ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Το ψηφιακό έγκλημα και η ανάσχεσή του. Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

Παρασκευή Δ. Καλομοίρη

Επιβλέποντες: **Δρακούλης Μαρτάκος,** Αναπληρωτής Καθηγητής

ΑΘΗΝΑ

ΦΕΒΡΟΥΑΡΙΟΣ 2014

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

Παρασκευή Δ. Καλομοίρη

Α.Μ.: M592

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Δρακούλης Μαρτάκος,** Αναπληρωτής Καθηγητής

ΦΕΒΡΟΥΑΡΙΟΣ 2014

ΠΕΡΙΛΗΨΗ

Στην ψηφιακή εποχή τα δεδομένα των υπολογιστικών συστημάτων μπορεί να έχουν ιδιαίτερη αξία και οι εγκληματίες εκμεταλλεύονται το γεγονός ότι οι εταιρείες και τα άτομα βασίζονται ολοένα και περισσότερο στους υπολογιστές. Οι οργανισμοί χρησιμοποιούν τους υπολογιστές για να αποθηκεύσουν όλα τα είδη πληροφορίας περιλαμβανομένων των οικονομικών και ιατρικών δεδομένων. Η έκθεση αυτής της πληροφορίας μπορεί να έχει σαν αποτέλεσμα οικονομικές απώλειες, κανονιστικές κυρώσεις ή βλάβη στην φήμη ενός οργανισμού.
Στην εργασία που ακολουθεί παρουσιάζονται τα είδη των ηλεκτρονικών επιθέσεων στους υπολογιστές και τα είδη του κακόβουλου λογισμικού. Η αντιμετώπιση των επιθέσεων και των εισβολών καθώς και η ανάκτηση των ψηφιακών δεδομένων γίνονται με τη δικανική ψηφιακή ανάλυση των υπολογιστών. Παρουσιάζονται οι τρόποι ανάκτησης και ανάλυσης των ψηφιακών δεδομένων, όπως επίσης και θέματα ιδιωτικότητας σε ειδικές περιοχές (ασύρματα και κινητά δίκτυα επικοινωνιών, ηλεκτρονική ψηφοφορία, ηλεκτρονική διακυβέρνηση). Τέλος παρουσιάζονται κάποια *projects* που είναι σε ερευνητικό στάδιο και προσπαθούν να αντιμετωπίσουν προβλήματα ιδιωτικότητας και διαχείρισης εμπιστοσύνης.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ψηφιακό έγκλημα και δικανική ψηφιακή ανάλυση

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ψηφιακό έγκλημα, δικανική ψηφιακή ανάλυση, ψηφιακά δεδομένα, προστασία της ιδιωτικότητας, κακόβουλο λογισμικό, διαχείριση εμπιστοσύνης

ABSTRACT

In the digital age, data on computer systems can have significant value, and criminals are taking advantage of the fact that businesses and individuals have become reliant on computers. Organizations use computers to store all forms of information including financial and medical data. The exposure of such information can result in financial loss, regulatory sanctions and reputational harm.

In the following chapters we present the various types of electronic attacks and the types of malware. Digital forensics analysis is the way to deal with the computer intrusions and to collect the digital evidence. We also present ways to retrieve and analyze digital evidence and ways to protect privacy regarding (on individual or organizational level) in many special cases (e.g. e-Government, e-voting, mobile communications). Finally, we present some projects in the field of research that try to deal with specific problems in the areas of privacy and trust management.

SUBJECT AREA: Cybercrime, Digital forensics analysis

KEYWORDS: cybercrime, digital forensics analysis, digital data, privacy protection, malware, trust management

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η εργασία αυτή διενεργήθηκε στην Αθήνα, το 2013. Ιδιαίτερες ευχαριστίες στον Καθηγητή, κο Δρακούλη Μαρτάκο.

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

Α΄ Μέρος, Οι Ηλεκτρονικές Επιθέσεις στον Ψηφιακό Κόσμο και η Αντιμετώπισή τους

1. Εισαγωγή - Το Ψηφιακό Έγκλημα (*Computer Crime)* και τα Θεμέλια της Δικανικής Ψηφιακής Ανάλυσης

Στην εποχή μας είναι πολύ δύσκολο να φανταστούμε ένα έγκλημα που δεν έχει ψηφιακές διαστάσεις. Οι εγκληματίες, βίαιοι και μη, χρησιμοποιούν την τεχνολογία για να διευκολυνθούν στις επιθέσεις τους και να αποφύγουν τη σύλληψη, δημιουργώντας έτσι προκλήσεις στις διωκτικές και δικαστικές αρχές αλλά και στους επαγγελματίες ασφάλειας των υπολογιστών. Σαν αποτέλεσμα της διακίνησης τεράστιων ποσοτήτων ναρκωτικών, της παιδικής πορνογραφίας, και άλλων παράνομων υλικών που διακινούνται μέσω διαδικτύου, το *U.S Customs Cybersmuggling Center* ελέγχει κάθε υπολογιστή στο διαδίκτυο στις ΗΠΑ ως σημείο εισόδου. Οι οργανωμένες ομάδες εγκληματιών παγκόσμια χρησιμοποιούν την τεχνολογία για να διατηρούν αρχεία, να επικοινωνούν και να κάνουν παράνομες πράξεις. Οι μεγαλύτερες ληστείες της εποχής μας έχουν καθοδηγηθεί μέσω δικτύων υπολογιστών.

Οι τρομοκράτες χρησιμοποιούν το διαδίκτυο για να επικοινωνούν, να στρατολογούν μέλη, να *«ξεπλένουν»* χρήματα, να κλέβουν πιστωτικές κάρτες, να ζητούν προσφορές και να δημοσιεύουν προπαγανδιστικό υλικό και εγχειρίδια εκπαίδευσης. Οι τρομοκράτες φθάνουν μέχρι το σημείο να αναπτύξουν οι ίδιοι τα εργαλεία που θα χρησιμοποιήσουν για να αποφύγουν την ανίχνευση και τη σύλληψη, όπως για παράδειγμα προγράμματα για την κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου και της υπηρεσίας άμεσων μηνυμάτων (*Instant Messaging, IM).* Επίσης η χρήση του διαδικτύου από τους τρομοκράτες εισάγει προκλήσεις για τους ψηφιακούς ερευνητές και απαιτεί διεθνή συνεργασία των διωκτικών αρχών και ανταλλαγή πληροφοριών.

Οι επιθέσεις σε δικτυακά συστήματα (*network based systems)* που έχουν σαν στόχο κρίσιμες υποδομές, όπως κυβερνητικές, υποδομές ενέργειας, υγείας, τηλεπικοινωνίες, οικονομικές και υπηρεσίες άμεσης βοήθειας προκαλούν μεγάλη ανησυχία και οι ομάδες που ασχολούνται με την αποτροπή αυτών των επιθέσεων έχουν αποκτήσει μεγάλη τεχνολογική εμπειρία. Τα τελευταία πέντε χρόνια, εισβολείς κατευθυνόμενοι από τις κυβερνήσεις κατάφεραν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε πολλά κυβερνητικά και εταιρικά δίκτυα στις ΗΠΑ και στη Ευρώπη. Μέχρι σήμερα, ο σκοπός αυτών των επιθέσεων ήταν η συλλογή πληροφοριών, αλλά υπήρχε πάντα η δυνατότητα της διατάραξης των κρίσιμων υποδομών.

Οι βίαιοι και κατ' εξακολούθηση εγκληματίες συνήθως ψάχνουν τα θύματά τους στο διαδίκτυο μέσω του οποίου είναι αόρατοι και συχνά κρύβουν τα ίχνη τους. Επίσης, αν και κανένας ποτέ δεν πέθανε από επίθεση σε ένα δίκτυο υπολογιστών, συχνά άνθρωποι (κυρίως έφηβοι) αυτοκτονούν αφού έχουν δεχτεί κάποια επίθεση ή προσβολή μέσω του διαδικτύου. Οι υπολογιστές επίσης χρησιμοποιούνται για να στοχεύσουν το σύστημα απόδοσης δικαιοσύνης, είτε μέσω απευθείας επιθέσεων στην υποδομή δικτύου και των υπολογιστών των διωκτικών αρχών είτε μέσω της απόκτησης προσωπικών πληροφοριών των εργαζομένων στις διωκτικές αρχές που μετά χρησιμοποιούνται για εκβίαση.

Νέοι όροι όπως ***κυβερνο-έγκλημα*** (*cybercrime*) και ***δικανική ψηφιακή ανάλυση*** *(digital forensics)*, έχουν δημιουργηθεί για να χαρακτηρίσουν τις εγκληματικές ενέργειες που εμπλέκουν υπολογιστές και τις νομικές και ερευνητικές τεχνολογίες που χρησιμοποιούνται για την επίλυσή τους.

Επειδή κάθε έγκλημα μπορεί να εμπλέκει υπολογιστές, δεν είναι καθαρό πώς θα γίνει ο διαχωρισμός ανάμεσα στα εγκλήματα που γίνονται χρησιμοποιώντας υπολογιστές και στα εγκλήματα που απλώς εμπλέκουν υπολογιστές. Αν και δεν υπάρχει συμφωνία για τον ορισμό του ψηφιακού εγκλήματος, ο όρος αυτός γίνεται με τα χρόνια όλο και πιο συγκεκριμένος. Το ψηφιακό έγκλημα αναφέρεται σε ένα περιορισμένο σύνολο επιθέσεων που έχουν οριστεί με σαφήνεια σε νόμους όπως στο *U.S. Computer Fraud and Abuse Act* και στο *UK Computer Abuse Act*. Αυτά τα εγκλήματα περιλαμβάνουν κλοπή υπηρεσιών υπολογιστών, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και υπολογιστικά συστήματα, πειρατεία λογισμικού και αλλοίωση ή κλοπή ηλεκτρονικά αποθηκευμένης πληροφορίας, εκβιασμό που γίνεται και διευκολύνεται με τη χρήση των υπολογιστών, μη εξουσιοδοτημένη πρόσβαση σε αρχεία τραπεζών, και αρχεία κατόχων πιστωτικών καρτών και τέλος κυκλοφορία κλεμμένων κωδικών πρόσβασης και μετάδοση καταστρεπτικών ιών ή εντολών.

Μια από τις κυριότερες δυσκολίες στον ορισμό του ψηφιακού εγκλήματος βρίσκεται στο γεγονός ότι υπάρχουν περιπτώσεις κατά τις οποίες οι υπολογιστές ή τα δίκτυα δεν εμπλέκονται απευθείας σε ένα έγκλημα, αλλά περιέχουν τις ψηφιακές αποδείξεις που σχετίζονται με το έγκλημα. Για να συμπεριλάβουμε και τέτοιου είδους περιπτώσεις, χρησιμοποιείται ο ευρύτερος όρος ***έγκλημα σχετιζόμενο με υπολογιστές*** *(computer related crime),* ο οποίος περιλαμβάνει κάθε έγκλημα που εμπλέκει υπολογιστές και δίκτυα. Με τον ίδιο τρόπο, υπάρχουν οργανισμοί όπως το Υπουργείο Δικαιοσύνης των *ΗΠΑ (U.S. Department of Justice, USDOJ)* και το Συμβούλιο της Ευρώπης *(Council of Europe*) που χρησιμοποιούν τον όρο ***κυβερνο-έγκλημα*** (*cybercrime*) για να χαρακτηρίσουν ένα ευρύ πεδίο εγκλημάτων που εμπλέκουν υπολογιστές και δίκτυα.

Στο παρελθόν, όταν οι βασικές πηγές των ψηφιακών αποδείξεων ήταν οι υπολογιστές, το πεδίο των ψηφιακών αποδείξεων καλυπτόταν από τον ορισμό ***δικανική ανάλυση υπολογιστών*** *(computer forensics, forensic computer analysis).* Από την εποχή που περισσότερες αποδείξεις μπορούσαν να βρεθούν στα δίκτυα υπολογιστών και στις κινητές συσκευές, και καθώς χρειαζόταν περισσότερο ειδικευμένη γνώση για την εξαγωγή από αυτά διαφόρων τύπων ψηφιακών αποδείξεων όπως είναι οι ψηφιακές φωτογραφίες ή το κακόβουλο λογισμικό, ο ορισμός αυτός έγινε προβληματικός. Αν και ο όρος ***δικανική ανάλυση υπολογιστών*** συνήθως αναφέρεται στην εξέταση των στοιχείων των υπολογιστών και των περιεχομένων τους (όπως είναι ο σκληρός δίσκος, οι φορητοί δίσκοι, οι εκτυπωτές), ο όρος αυτός έχει επίσης χρησιμοποιηθεί κάποιες φορές για να περιγράψει τη δικανική ανάλυση όλων των μορφών των ψηφιακών αποδείξεων, που περιλαμβάνουν και τις διαδρομές στα δίκτυα υπολογιστών, δηλαδή τη ***δικανική ανάλυση δικτύων*** *(network forensics*). Το 2001 στο πρώτο ετήσιο *Digital Forensic Research Workshop (DFRWS)* αναγνωρίστηκε η ανάγκη για μια αναθεώρηση του ορισμού αυτού και προτάθηκε ο όρος ***επιστήμη δικανικής ψηφιακής ανάλυσης*** *(digital and multimedia sciences)* για το νέο αυτό πεδίο της επιστήμης που περιλαμβάνει την δικανική ψηφιακή ανάλυση των υπολογιστικών συστημάτων όπως είναι οι ψηφιακές εικόνες, τα βίντεο, οι ηχητικές ηχογραφήσεις. Ο ορισμός ***ψηφιακή δικανική ανάλυση*** *(digital forensics)* προέκυψε σαν πρωταρχικός ορισμός που καλύπτει τις γενικές πρακτικές ανάλυσης όλων των μορφών των ψηφιακών αποδείξεων. Ειδικές περιπτώσεις στην δικανική ψηφιακή ανάλυση περιλαμβάνουν:

- ***Δικανική ανάλυση υπολογιστών (computer forensics)*****:** Διαφύλαξη και ανάλυση των υπολογιστών, που ονομάζεται επίσης ***δικανική ανάλυση αρχείων συστημάτων*** *(file system forensics),*
- ***Δικανική ανάλυση δικτύων (network forensics)*****:** Διαφύλαξη και ανάλυση της κίνησης και των αρχείων καταγραφής των δικτύων *(log files),*

- ***Δικανική ανάλυση κινητών συσκευών (mobile device forensics):*** Διαφύλαξη και ανάλυση των κινητών τηλεφώνων, των *«έξυπνων»* κινητών τηλεφώνων και των συστημάτων πλοήγησης *(Global Positioning System, GPS),*
- ***Δικανική ανάλυση κακόβουλου λογισμικού (malware forensics):*** Διατήρηση και ανάλυση του κακόβουλου λογισμικού όπως είναι οι ιοί (*virus*), τα *worms,* τα *trojan horses*.**[1]**

Τα θέματα αυτά που αφορούν στις επιθέσεις σε υπολογιστές και υπολογιστικά συστήματα καθώς και οι μέθοδοι δικανικής ψηφιακής ανάλυσης θα παρουσιαστούν στα επόμενα κεφάλαια.

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

2. Οι Ηλεκτρονικές Επιθέσεις και ο Τρόπος Δράσης τους

Τα συστήματα των υπολογιστών αποτελούν στόχο σε ένα ευρύ πεδίο ηλεκτρονικών επιθέσεων.

Η κατανόηση των επιθέσεων είναι μια βασική προϋπόθεση ώστε να σχεδιαστούν οι κατάλληλες δικανικές, ψηφιακές μέθοδοι για τη συλλογή και την ανάλυση των αποδείξεων των επιθέσεων. Η ανάλυση των αποδείξεων μιας επίθεσης δεν μπορεί να γίνει με σωστό τρόπο αν δεν γνωρίζουμε την συμπεριφορά της επίθεσης. Οι επιθέσεις μπορούν να θεωρηθούν σαν μια σειρά από βήματα αρχίζοντας από την αναγνώριση προς την πρόσβαση και τέλος προς την κάλυψη. Κάθε βήμα αφήνει ψηφιακές αποδείξεις για τους ελεγκτές.

Είναι δύσκολο να γίνουν προβλέψεις για τις μελλοντικές ηλεκτρονικές επιθέσεις, κυρίως επειδή οι ηλεκτρονικοί εγκληματίες δεν είναι προβλέψιμοι. Η συνεχής πάλη μεταξύ των κυβερνο-εγκληματιών και του νόμου, δείχνει ότι και οι δύο πλευρές συνεχώς εξελίσσονται και προσαρμόζονται. Η μια πλευρά συνεχώς εφευρίσκει νέους τρόπους επίθεσης και εργαλείων επίθεσης ενώ η άλλη πλευρά ακολουθεί και διορθώνει τις ατέλειες των υπολογιστικών συστημάτων. Με σιγουριά μπορούμε να πούμε τα παρακάτω:

- Οι επιθέσεις θα αυξάνονται με εξελιγμένο τρόπο και σε συνδυασμό μεταξύ τους, απαιτώντας ολοένα και περισσότερο εξελιγμένους τρόπους αντιμετώπισης,
- Οι επιθέσεις που σχεδιάζονται για κέρδος και για κλοπή προσωπικών δεδομένων θα αυξηθούν,
- Οι επιθέσεις κοινωνικής μηχανικής (*social engineering)* θα συνεχιστούν μέσω του ηλεκτρονικού ταχυδρομείου, λόγω της μεγάλης τους επιτυχίας,
- Το κακόβουλο λογισμικό αναπτύσσεται σε νέα μέσα όπως η υπηρεσία άμεσων μηνυμάτων (*Instant Messaging, IM)* και τα κινητά τηλέφωνα,
- Το κακόβουλο λογισμικό είναι η περισσότερο επικρατούσα επίθεση τα τελευταία χρόνια και θα συνεχίσει να είναι.

Η βελτίωση της ποιότητας των επιθέσεων, υπονοεί ότι τα ψηφιακά δικανικά μέσα θα έχουν αυξημένη σημασία στην έρευνα, διάγνωση και ανάλυση των κυβερνο-επιθέσεων. Οι ψηφιακές δικανικές τεχνικές θα αμφισβητούνται από επιτιθέμενους που θα έχουν πρόσβαση σε περισσότερα και πιο εξελιγμένα εργαλεία επίθεσης. Οι ερευνητές των κυβερνο-εγκλημάτων θα χρειάζονται καλύτερη γνώση των επιθέσεων και καλύτερα δικανικά εργαλεία για τη συλλογή και ανάλυση των ηλεκτρονικών αποδείξεων **[2]**.

Υπάρχουν τόσα διαφορετικά είδη επιτιθέμενων όσα είναι και τα διαφορετικά είδη των επιθέσεων. Οι επιτιθέμενοι μπορούν να κατηγοριοποιηθούν με διαφορετικούς τρόπους. Για παράδειγμα, μπορεί να είναι ***εσωτερικοί*** ή ***εξωτερικοί***, ανάλογα με τη σχέση που έχουν με το στόχο της επίθεσης. Την πενταετία 2000-2005 αναφέρθηκε ότι το ποσοστό των ηλεκτρονικών επιθέσεων εκ των έσω ήταν σχεδόν ίσο με το ποσοστό των εξωτερικών επιθέσεων. Οι εσωτερικοί επιτιθέμενοι δημιουργούν περισσότερες ανησυχίες γιατί έχουν συγκεκριμένα πλεονεκτήματα όπως είναι η εμπιστοσύνη και η γνώση του οργανισμού που στοχεύουν, τα οποία αυξάνουν τις πιθανότητες μιας επιτυχημένης επίθεσης. Επιπλέον, οι εσωτερικοί επιτιθέμενοι δεν χρειάζεται να παρακάμψουν την περίμετρο άμυνας, που έχει σχεδιαστεί από την ασφάλεια του κάθε συστήματος για να αποτρέψει τις εξωτερικές ηλεκτρονικές επιθέσεις.

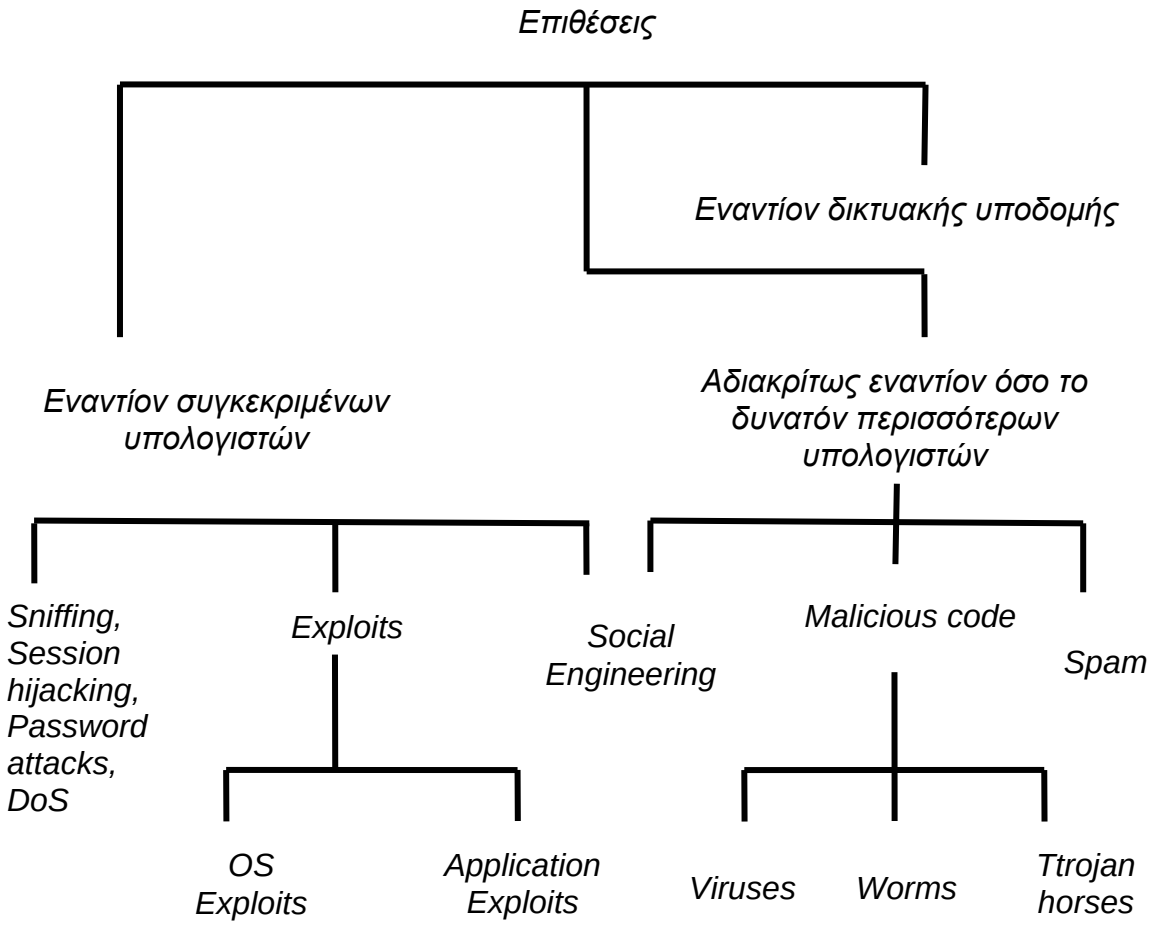
Επίσης οι επιτιθέμενοι μπορούν να κατηγοριοποιηθούν ως ***ερασιτέχνες*** ή ως ***επαγγελματίες***. Ο περισσότερος κόσμος φαντάζεται τους επιτιθέμενους σαν τον στερεοτυπικό έφηβο *hacker*, όπως συνήθως τους παρουσιάζουν τα μέσα ενημέρωσης. Αν και οι ερασιτέχνες *hackers* είναι υπεύθυνοι για ένα σημαντικό ποσοστό ιών (*virus*, *worm*) και άλλων βανδαλισμών, η ανάμιξη των επαγγελματιών και του οργανωμένου εγκλήματος χαρακτηρίζεται από την επιτήδευση των επιθέσεων και ο αριθμός των επιθέσεων συνήθως καθοδηγείται από το κίνητρο του κέρδους. Εκτός από τους επαγγελματίες *hackers*, άλλοι επαγγελματίες που αναμιγνύονται στις ηλεκτρονικές επιθέσεις περιλαμβάνουν εθνικές κυβερνήσεις, στρατιωτικά τμήματα και βιομηχανική κατασκοπία.

Το κίνητρο των ηλεκτρονικών επιθέσεων εξαρτάται από τον επιτιθέμενο. Ακριβώς επειδή υπάρχουν πολλοί διαφορετικοί τύποι επιτιθέμενων, τα κίνητρα μπορεί να περιλαμβάνουν οτιδήποτε, όπως διασκέδαση, φήμη, κέρδος, κατασκοπία, εκδίκηση ή κάποιο πολιτικό σκοπό.

Ο στερεοτυπικός έφηβος *hacker*, θεωρούμε συνήθως ότι ενδιαφέρεται να κερδίσει φήμη (θαυμασμό για τις τεχνικές του επιδόσεις ή φόβο για τις ζημιές που μπορεί να πετύχει). Από την άλλη μεριά, το οργανωμένο έγκλημα και οι επαγγελματίες επιτιθέμενοι ενδιαφέρονται κυρίως για το κέρδος. Οι επιθέσεις που προσανατολίζονται στην καταστρατήγηση της ιδιωτικότητας ή στην κλοπή εμπιστευτικών δεδομένων αποτελούν μια τάση που αυξάνεται. Επίσης οι κυβερνο-επιθέσεις για πολιτικούς σκοπούς αποκτούν αυξανόμενο ενδιαφέρον από τότε που η διεθνής προσοχή έχει στραφεί στην τρομοκρατία.

Μια ταξινόμηση των ηλεκτρονικών επιθέσεων παρουσιάζεται στο ***σχήμα 1***. Στο ψηλότερο επίπεδο, οι επιθέσεις μπορεί να στοχεύουν εναντίον συγκεκριμένων υπολογιστών, δικτυακής υποδομής ή αδιακρίτως εναντίον όσο το δυνατόν περισσότερων υπολογιστών.

Οι επιθέσεις που κατευθύνονται εναντίον συγκεκριμένων υπολογιστών περιλαμβάνουν *sniffing*, πειρατεία συνόδου (*session hijacking*), εκμετάλλευση ευπαθειών (*exploits of vulnerabilities*), επιθέσεις κωδικών πρόσβασης (*password attacks*), άρνηση παροχής υπηρεσίας (*Denial of Service, DoS*) και επιθέσεις κοινωνικής μηχανικής (*social engineering*). Η κοινωνική μηχανική μπορεί επίσης να χρησιμοποιηθεί σε επιθέσεις μεγάλης κλίμακας που γίνονται αδιακρίτως. Άλλες επιθέσεις μεγάλης κλίμακας περιλαμβάνουν κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*) και κακόβουλο λογισμικό (*malicious code, malware*) **[3]**.

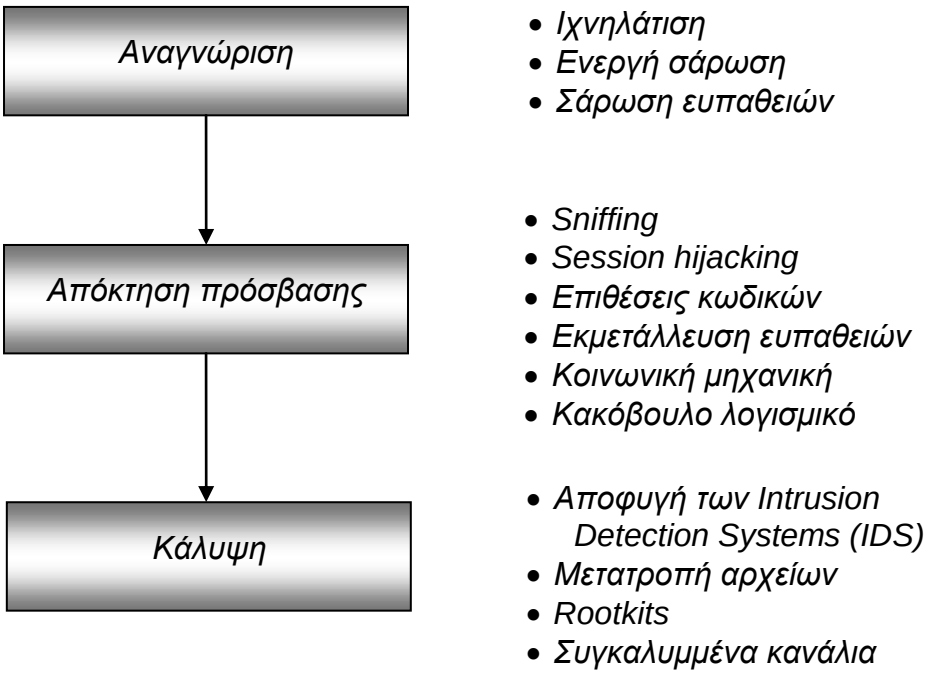


Σχήμα 1: Ταξινόμηση των ηλεκτρονικών επιθέσεων

2.1 Τα είδη των ηλεκτρονικών επιθέσεων

Οι διαφορετικές φάσεις των ηλεκτρονικών επιθέσεων παρουσιάζονται στο ***σχήμα 2***.

Μια επίθεση για να πετύχει ένα συγκεκριμένο στόχο, συνήθως εκτυλίσσεται μέσα από διαδοχικά στάδια, τα οποία είναι ανάλογα με τα στάδια που παρατηρούνται σε μια φυσική επίθεση. Όπως φαίνεται στο ***σχήμα 2***, το πρώτο στάδιο είναι ***η φάση της αναγνώρισης*** ώστε να συλλεχθεί πληροφορία για την προετοιμασία της επίθεσης. Η γνώση του στόχου και των αδυναμιών του μπορεί να είναι καθοριστικής σημασίας για την επιτυχία μιας επίθεσης. Το δεύτερο στάδιο είναι ***η απόκτηση πρόσβασης***, που θα μπορούσε να έχει πολλούς διαφορετικούς τελικούς στόχους, όπως τον έλεγχο, την κλοπή ή την καταστροφή. Κατά τη διάρκεια της επίθεσης αλλά και μετά την επίθεση, ο επιτιθέμενος είναι πιθανό να λάβει δράσεις ώστε να ***αποφύγει τον εντοπισμό (κάλυψη)***, όπως το να αλλάξει τα αρχεία καταγραφής του συστήματος (*system logs*) ή να εγκαταστήσει ένα *rootkit (βλ. κεφ.2.1.3.3)*.



Σχήμα 2: Τα βασικά στάδια των επιθέσεων εναντίον συγκεκριμένων στόχων

2.1.1 Η Φάση της Αναγνώρισης

Για την προετοιμασία μιας επιτυχημένης επίθεσης, είναι φυσικό ο επιτιθέμενος να προσπαθήσει πρώτα να μάθει όσο το δυνατόν περισσότερα σχετικά με το στόχο. Η φάση της αναγνώρισης είναι δυνατόν να αποκαλύψει έναν εκπληκτικό αριθμό πληροφοριών όπως ονόματα λογαριασμών, διευθύνσεις, λειτουργικά συστήματα και ακόμα και κωδικούς πρόσβασης (*passwords*). Επιπλέον οι περισσότερες τεχνικές αναγνώρισης δεν θεωρούνται κακόβουλες ή παράνομες και μπορούν να έρθουν εις πέρας με σχετική ασφάλεια. Οι τεχνικές της αναγνώρισης είναι τόσο κοινές και γνωστές ώστε οι πιθανοί στόχοι μπορεί να μην τεθούν σε συναγερμό.

Υπάρχουν πολλές διαφορετικές τεχνικές αναγνώρισης και οι επιτιθέμενοι δεν ακολουθούν μια συγκεκριμένη διαδοχή βημάτων. Θα αναφέρουμε τρία γενικά βήματα τα οποία προοδευτικά χρησιμοποιούνται για να ανακαλύψουν οι επιτιθέμενοι περισσότερη πληροφορία για τον πιθανό στόχο. Πρώτα, γίνονται προσπάθειες ιχνιλάτισης

(*footprinting*) από δημόσιους καταλόγους (*directories*) ώστε να γίνει γνωστή η θέση και η φύση του πιθανού στόχου. Στη συνέχεια, γίνεται σάρωση (*scanning*) η οποία παρέχει περισσότερο λεπτομερή πληροφορία για τον στόχο σε σχέση με την απευθείας ερώτηση (*active probing*).

2.1.1.1 Ιχνηλάτιση (*Footprinting*)

Το πρώτο βήμα στην ανακάλυψη είναι η ***ιχνηλάτιση*** (ανακάλυψη αποτυπώματος ή απαρίθμηση) με πρωταρχικό σκοπό τον εντοπισμό και την ανακάλυψη της φύσης των πιθανών στόχων. Για παράδειγμα, ένας επιτιθέμενος θα θέλει να γνωρίζει πόσοι πιθανοί υπολογιστές (*hosts*) είναι διαθέσιμοι και τις διαδικτυακές διευθύνσεις τους *(Internet Protocol addresses, IP addresses).*

Ένα πολύ μεγάλο ποσοστό πληροφορίας είναι διαθέσιμο στο διαδίκτυο (*web*) σε μεγάλες και δημόσιες βάσεις δεδομένων. Αυτές οι βάσεις δεδομένων μπορούν να ερωτηθούν από διάφορα προγράμματα όπως *nslookup, whois, dig*. Πολλές από αυτές τις βάσεις δεδομένων έχουν εύκολες στη χρήση διεπαφές (*interfaces*) και δεν απαιτούν εξειδικευμένη τεχνική γνώση. Γενικά, η πληροφορία που μπορεί να αντληθεί από την ιχνηλάτιση είναι κοινή, εύκολο να βρεθεί και αποτελεί μικρό κίνδυνο για τις εταιρείες, τις κυβερνήσεις και τις στρατιωτικές μονάδες.

Οι βάσεις δεδομένων *whois* περιέχουν δεδομένα σχετικά με την ανάθεση των διευθύνσεων *IP*, την καταχώρηση των ονομάτων των τομέων (*domain names*) και την πληροφορία επικοινωνίας. Τα ονόματα των τομέων (*domain names*) όπως για παράδειγμα το *www.company.com* καταχωρούνται μέσω του *Internet Network Information Center (InterNIC),* μια ένωση που αποτελείται από πολλές εταιρείες και την κυβέρνηση των ΗΠΑ. Για ένα συγκεκριμένο όνομα τομέα (*domain name*) η βάση δεδομένων *whois* μπορεί να προμηθεύσει το όνομα και τη διεύθυνση *IP*, τους εξυπηρετητές (*servers*) και την πληροφορία επικοινωνίας αυτού που καταχώρησε το όνομα του τομέα.

Η βάση δεδομένων *ARIN (American Registry for Internet Numbers)* παρέχει πληροφορίες σχετικές με την ιδιοκτησία συγκεκριμένου εύρους διευθύνσεων *IP (IP addresses)*. Επιτρέπει την απόκτηση πληροφοριών επικοινωνίας και καταχώρησης συμπεριλαμβανομένων των διευθύνσεων *IP*, αυτόνομων αριθμών συστήματος και καταχωρημένων οργανισμών στην Αμερικανική ήπειρο. Οι καταχωρήσεις των Ευρωπαϊκών *IP* διευθύνσεων μπορούν να βρεθούν από το *Reseaux IP Europeens Network Coordination Centre (RIPE NCC).* Αντίστοιχα, οι καταχωρήσεις *IP* διευθύνσεων στην Ασία διατηρούνται από το *Asia Pacific Network Information Center (APNIC).*

Μια άλλη πολύ γνωστή και χρήσιμη βάση δεδομένων είναι το σύστημα ονοματοδοσίας τομέων (*Domain Name System, DNS*). Το *DNS* είναι μια ιεραρχία εξυπηρετητών (*servers*) που χρησιμοποιούνται για να αντιστοιχίζουν ονόματα τομέων, *IP* διευθύνσεις και εξυπηρετητές ηλεκτρονικού ταχυδρομείου (*mail servers*). Για παράδειγμα, αναλύει ένα όνομα τομέα όπως το *www.company.com* στην *IP* διεύθυνση του σχετιζόμενου εξυπηρετητή. Η ιεραρχία εκτυλίσσεται από τους *root DNS* εξυπηρετητές ως τους *DNS* εξυπηρετητές για τον κάθε οργανισμό και δίκτυο. Αυτοί οι *DNS* εξυπηρετητές περιέχουν πληροφορία για άλλους χαμηλότερου επίπεδου *DNS* εξυπηρετητές και για διευθύνσεις *IP* συγκεκριμένων υπολογιστών.

Από την άποψη της δικανικής αντιμετώπισης του ψηφιακού εγκλήματος, η εξέταση του συστήματος του επιτιθέμενου θα πρέπει να επικεντρώνεται για αποδείξεις στο σκληρό δίσκο όπου φαίνονται οι ιστοσελίδες *(web sites)* και η πληροφορία που αντλήθηκε από

τη διαδικασία της ιχνηλάτισης. Αυτή η πληροφορία συχνά βρίσκεται στην ενεργή *cache* ή σαν απομεινάρια στο σκληρό δίσκο του υπολογιστή.

2.1.1.2 Ενεργή σάρωση (*Active Scanning*)

Η ιχνηλάτιση μπορεί να θεωρηθεί παρόμοια με το να ψάχνει κανείς ονόματα και αριθμούς σε ένα τηλεφωνικό κατάλογο. Η ***σάρωση*** αποτελεί ένα πιο ενεργό βήμα για να μάθει κανείς σχετικά με πιθανούς στόχους, από τις απαντήσεις τους σε διάφορες ερωτήσεις (*probes*). Υπάρχουν πολλοί διαφορετικοί τρόποι για να διεξάγει κάποιος σαρώσεις και οι περισσότεροι από αυτούς είναι αυτοματοποιημένοι για ευκολία και ταχύτητα.

Κατά τη διάρκεια μιας «κατόπιν εορτής» ψηφιακής εξέτασης του υπολογιστή ενός επιτιθέμενου, είναι πολύ σημαντικό να εξετάσουμε την ύπαρξη εργαλείων όπως αυτά που περιγράφονται πιο κάτω. Αυτό θα βοηθήσει έναν πεπειραμένο εξεταστή να καταλάβει το επίπεδο των ικανοτήτων του επιτιθέμενου. Αυτό το βήμα αποκτά ιδιαίτερα μεγάλη σημασία όταν προσπαθούμε να καταλάβουμε το εύρος μιας πιθανής απειλής σε επίπεδο οργανισμού. Οι επιτιθέμενοι γενικά αρέσκονται να χρησιμοποιούν τα ίδια εργαλεία συνέχεια, και σ' αυτό το αρχικό στάδιο ο επιτιθέμενος είναι πολύ πιθανό να χρησιμοποιήσει μερικά από τα παρακάτω εργαλεία και σε άλλους υπολογιστές στόχους.

2.1.1.2.1 Διάλογος Πολέμου (War Dialing)

Πρόκειται για μια παλιά και πρωτόγονη μέθοδο που όμως χρησιμοποιείται ακόμα. Πολλοί οργανισμοί επιτρέπουν σε απομακρυσμένους χρήστες (*remote users*) να έχουν πρόσβαση στο δίκτυό τους μέσω μετασχηματιστών σύνδεσης (*dial up modems)*. ***Οι war dialers*** είναι αυτοματοποιημένες μηχανές που επικοινωνούν συστηματοποιημένα με ένα σύνολο από τηλεφωνικές γραμμές μέχρι να βρουν προσπελάσιμους μετασχηματιστές (*modems*). Ένας τηλεφωνικός αριθμός ενός οργανισμού μπορεί εύκολα να βρεθεί μέσω του διαδικτύου ή των τηλεφωνικών καταλόγων. Έτσι ο επιτιθέμενος μπορεί να χρησιμοποιήσει το εύρος των αριθμών που είναι σχετικοί με τον αριθμό του οργανισμού που βρήκε, για να ανακαλύψει τηλεφωνικές γραμμές με *modems*. Κάποιοι *war dialers* περιλαμβάνουν και μια λειτουργία ώθησης που στέλνει ένα προκαθορισμένο σύνολο χαρακτήρων στο *modem* για να δει πώς θα αντιδράσει. Η απάντηση μπορεί να αποκαλύψει την απουσία κωδικού πρόσβασης, τον τύπο της πλατφόρμας και ίσως ένα πρόγραμμα απομακρυσμένης σύνδεσης (όπως το δημοφιλές *pcAnywhere*). Υπάρχουν πολλοί και δημοφιλείς *war dialers*, όπως *Toneloc, THC Scan, Phone Tag, Rasusers, Microsoft's Hyper-Terminal, PhoneSweep, Sandtrap, Procomm Plus*.

Αν και οι *war dialers* χρησιμοποιούνται εδώ και δεκαετίες, είναι ακόμα αποτελεσματικοί στις επιθέσεις όταν ένα *modem* δεν είναι ασφαλισμένο. Είναι φανερό ότι *modems* χωρίς προστασία κωδικού πρόσβασης είναι εντελώς ευάλωτα. Επίσης, μπορεί κάποιος να επιτεθεί σε *modems* μαντεύοντας τον κωδικό πρόσβασης. Μια επιτυχημένη επίθεση μέσω ενός μη ασφαλούς *modem*, μπορεί να οδηγήσει σε έκθεση του δικτύου ενός οργανισμού σε κίνδυνο, προσπερνώντας με μεγάλη αποτελεσματικότητα τείχη προστασίας (*firewalls*) και άλλες εξειδικευμένες μεθόδους άμυνας.

2.1.1.2.2 Σάρωση με Ανταλλαγή Μηνυμάτων ping (Ping Sweeps)

Το πρωτόκολλο ελέγχου μηνυμάτων του διαδικτύου *(Internet Control Message Protocol, ICMP)* αποτελεί ένα σημαντικό τμήμα του πρωτοκόλλου του διαδικτύου (*Internet Protocol, IP*) στο να ενεργοποιεί ειδοποιήσεις σε περιπτώσεις κινδύνου και άλλες λειτουργίες ελέγχου. Το *ICMP* περιέχει μια πολύ χρήσιμη λειτουργία που ονομάζεται

ping και τυπικά χρησιμοποιείται για να πιστοποιήσει ότι ένας συγκεκριμένος υπολογιστής είναι ενεργός στο δίκτυο. Τα μηνύματα *ping* αποτελούνται από ένα ζευγάρι μηνυμάτων που ονομάζονται *Echo Request* και *Echo Reply***.** Ένας υπολογιστής που λαμβάνει ένα μήνυμα *ICMP Echo Request* θα πρέπει να απαντήσει με ένα μήνυμα *ICMP Echo Reply*.

Τα μηνύματα *ping* συχνά χρησιμοποιούνται από τους επιτιθέμενους για να ανιχνεύσουν ή να σαρώσουν ένα σύνολο από διευθύνσεις *IP*, ώστε να βρουν ενεργούς υπολογιστές. Υπάρχουν πολλά εργαλεία που μπορούν να υλοποιήσουν αυτή τη διαδικασία. Ωστόσο, αυτά τα εργαλεία έχουν δύο μειονεκτήματα για τους επιτιθέμενους. Είναι δυνατόν να ανιχνευθούν και να ενεργοποιήσουν κατάσταση συναγερμού στους πιθανούς στόχους. Επίσης οι οργανισμοί έχουν σαν πολιτική κάποιες φορές να μην επιτρέπουν την ανταλλαγή μηνυμάτων *ICMP*. Για να καλύψουν την έλλειψη της χρήσης των μηνυμάτων *ICMP*, οι επιτιθέμενοι, χρησιμοποιούν τη λειτουργικότητα των πακέτων ελέγχου του πρωτοκόλλου ελέγχου μεταφοράς (*Transmission Control Protocol, TCP)* σε γνωστές θύρες. Ένα αρχικό *TCP SYN* πακέτο (που χρησιμοποιείται για να ζητήσει μια νέα σύνδεση *TCP*) στέλνεται στον παραλήπτη και θα ενεργοποιήσει ένα απαντητικό πακέτο *TCP SYN-ACK*.

2.1.1.2.3 Αποτύπωση του Δικτύου (Network Mapping)

Η σάρωση με ανταλλαγή μηνυμάτων *ping*, αποκαλύπτει τις διευθύνσεις ενεργών υπολογιστών αλλά δεν αποκαλύπτει πληροφορίες σχετικές με τα δίκτυά τους. ***Η ανίχνευση διαδρομής*** (*traceroute*) είναι μια λειτουργία που χρησιμοποιείται ευρέως για την αποτύπωση της τοπολογίας των δικτύων. Η μέθοδος αυτή χρησιμοποιεί το πεδίο *Time to Live (TTL)* που βρίσκεται στην κεφαλίδα του πακέτου *IP*. Όταν στέλνεται ένα *IP* πακέτο, η τιμή του πεδίου *TTL*, τίθεται στην μέγιστη επιτρεπόμενη τιμή χρόνου που επιτρέπεται για την μετάδοση του πακέτου. Ο καθορισμός του χρόνου στο πεδίο *TTL*, είναι απαραίτητος ώστε τα *IP* πακέτα να μην μεταφέρονται συνεχώς από κόμβο σε κόμβο σε ένα δίκτυο. Κάθε δρομολογητής (*router*) που λαμβάνει το *IP* πακέτο, μειώνει την τιμή του πεδίου *TTL* κατά τον χρόνο που ξοδεύτηκε για το *IP* πακέτο στο συγκεκριμένο δρομολογητή. Συνήθως οι δρομολογητές προωθούν τα *IP* πακέτα που λαμβάνουν πολύ γρήγορα και επομένως μειώνουν την τιμή του πεδίου *TTL* κατά την ελάχιστη τιμή δηλ. τη μονάδα. Με αυτό τον τρόπο τελικά το πεδίο *TTL* μπορεί να χρησιμοποιηθεί για μέτρηση αλμάτων (*hop count*). Όταν η τιμή του πεδίου *TTL* γίνει μηδέν, ο δρομολογητής θα πρέπει να αποβάλει το *IP* πακέτο και να επιστρέψει ένα μήνυμα *ICMP Time Exceeded* στην *IP* διεύθυνση πηγής *(source IP address*) του πακέτου που αποβλήθηκε.

Η λειτουργία της ανίχνευσης δρόμου αποστέλλει μια ακολουθία πακέτων του πρωτοκόλλου δεδομενογράμματος χρήστη *(User Datagram Protocol, UDP)*, ξεκινώντας με την τιμή του πεδίου *TTL* στην τιμή της μονάδας και αυξάνοντας την τιμή αυτή κατά μία μονάδα για κάθε επιτυχημένο πακέτο. Όταν επιστρέφουν τα μηνύματα *ICMP Time Exceeded*, ανακαλύπτονται οι διευθύνσεις των δρομολογητών σε διαδοχικά αυξανόμενες αποστάσεις. Ανάλογα, μπορούν να χρησιμοποιηθούν μηνύματα *ICMP*, αντί για πακέτα *UDP*.

2.1.1.2.4 Ανίχνευση Θυρών (Port Scanning)

Στις εφαρμογές που χρησιμοποιούν *TCP (Transmission Control Protocol*) και *UDP (User Datagram Protocol)* έχουν εκχωρηθεί αριθμοί θυρών, οι οποίοι μεταφέρονται στις κεφαλίδες των *TCP* ή *UDP* πακέτων. Οι κεφαλίδες επιτρέπουν ένα εύρος 65.535 θυρών

TCP και 65.535 θυρών *UDP*. Ορισμένοι αριθμοί θυρών είναι γνωστοί και εκχωρημένοι εκ των προτέρων σε κοινά πρωτόκολλα, όπως φαίνεται στον ***πίνακα 1***.

Πίνακας 1: Παραδείγματα γνωστών θυρών

ΘΥΡΑ	***ΠΕΡΙΓΡΑΦΗ***
TCP 20	*Δεδομένα πρωτοκόλλου μεταφοράς αρχείων (File Transfer Protocol, FTP)*
TCP 21	*Έλεγχος πρωτοκόλλου μεταφοράς αρχείων (File Transfer Protocol, FTP)*
TCP 23	*Telnet*
TCP 25	*Πρωτόκολλο μεταφοράς ηλεκτρονικού ταχυδρομείου (Simple Mail Transfer Protocol, SMTP)*
TCP 53	*Domain Name System*
TCP 80	*HTTP (Hypertext Transfer Protocol)*
TCP 161	*Πρωτόκολλο διαχείρισης δικτύου (Simple Network Management Protocol, SNMP)*
TCP 179	*Border Gateway Protocol*

Για παράδειγμα, οι εξυπηρετητές *web* «ακούν» τα αιτήματα *HTTP (Hypertext Transfer Protocol)* στην *TCP* θύρα 80. Οι άλλες θύρες μπορούν να χρησιμοποιηθούν δυναμικά, αν χρειαστεί.

Ένας επιτιθέμενος ενδιαφέρεται πάντα να ανακαλύψει ποιές θύρες είναι ανοιχτές (ή ποιές υπηρεσίες είναι ενεργές) σε έναν πιθανό στόχο. Ανοιχτή θύρα σημαίνει ότι ο στόχος θα είναι δεκτικός σε αυτή τη θύρα. Επίσης οι πιθανές επιθέσεις συχνά στοχεύουν σε αδυναμίες μιας συγκεκριμένης υπηρεσίας. Ωστόσο, η διερεύνηση κάθε μιας θύρας ξεχωριστά μπορεί να γίνει πολύ κουραστική. Ένας ανιχνευτής θυρών αποτελεί ένα αυτοματοποιημένο εργαλείο για την αποστολή ερωτήσεων σε ένα σύνολο από συγκεκριμένες θύρες, έτσι ώστε να ανιχνευθούν οι ανοιχτές θύρες.

Το πιο ευρέως διαδεδομένο εργαλείο για ανίχνευση θυρών, είναι το ανοιχτό λογισμικό *Nmap*. Το *Nmap* είναι πιθανώς ο πιο ικανός ανιχνευτής θυρών, παρέχει επιλογές για διαφορετικούς τύπους ανίχνευσης, οι οποίοι ποικίλουν στο βαθμό της απάτης και στην ικανότητα να περνούν μέσα από τείχη προστασίας (*firewalls*). Άλλα δημοφιλή εργαλεία περιλαμβάνουν το εργαλείο ανίχνευσης *Foundstone*, το *hping* και το *nemesis*.

2.1.1.2.5 Ανίχνευση Λειτουργικού Συστήματος (Operating System Detection)

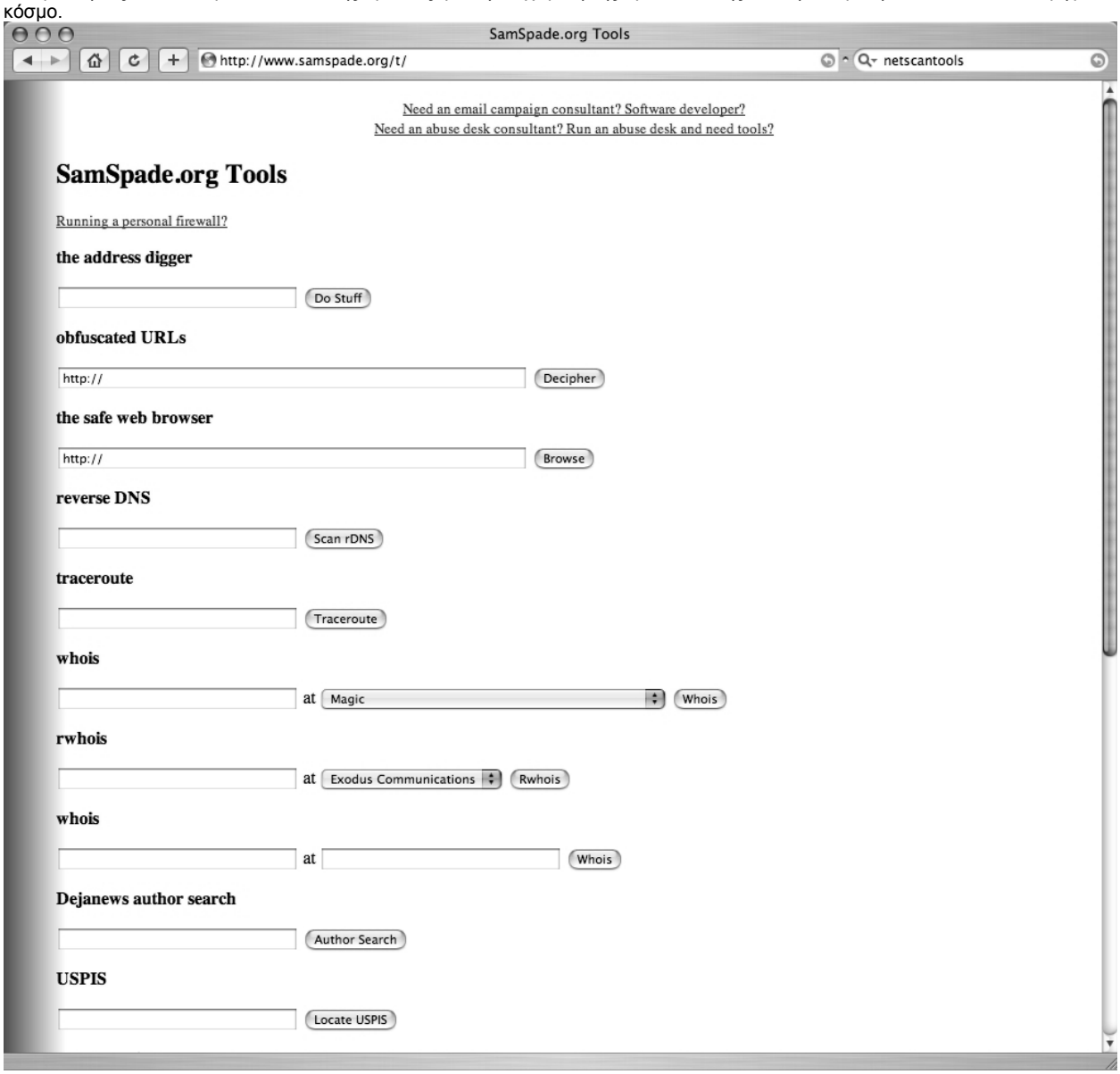
Ένας επιτιθέμενος ίσως προσπαθήσει να ανακαλύψει το λειτουργικό σύστημα του υπολογιστή στόχου, επειδή συγκεκριμένες αδυναμίες είναι γνωστές για διαφορετικά λειτουργικά συστήματα (όπως και για τις διαφορετικές τους εκδόσεις). Υποκλοπές της κίνησης του δικτύου με έναν *sniffer* είναι δυνατόν να αποκαλύψουν στοιχεία για το

λειτουργικό σύστημα ενός υπολογιστή. Για παράδειγμα, διαφορετικά λειτουργικά συστήματα επιδεικνύουν συγκεκριμένη συμπεριφορά στην ανάθεση τιμής στο πεδίο *TTL (Time to Live)* στην κεφαλίδα του *IP* πακέτου και στον καθορισμό του μεγέθους των παράθυρων *TCP*. Μια ενεργή τεχνική που χρησιμοποιούν οι επιτιθέμενοι είναι η ανίχνευση αποτυπωμάτων της σωρού *TCP (TCP stack*), τα οποία μπορούν να βρεθούν χρησιμοποιώντας το δημοφιλές εργαλείο *Nmap*. Η ανίχνευση των αποτυπωμάτων της σωρού *TCP*, εκμεταλλεύεται το γεγονός ότι ενώ το *TCP* πρωτόκολλο είναι τυποποιημένο ως προς την εγκαθίδρυση συνομιλίας με την τρίδρομη χειραψία (*3 way handshake*), η τυποποίηση δεν καλύπτει απαντήσεις σε διάφορους αθέμιτους συνδυασμούς των *TCP* πεδίων. Τα λειτουργικά συστήματα μπορεί να διαφέρουν στην υλοποίηση των απαντήσεών τους όταν λαμβάνουν αθέμιτα *TCP* πακέτα. Ερευνώντας αυτές τις διαφορές με διάφορα αθέμιτα *TCP* πακέτα, το λειτουργικό σύστημα και ακόμα και η συγκεκριμένη του έκδοση είναι δυνατόν να αναγνωριστούν. Μόλις ένα λειτουργικό σύστημα αναγνωριστεί, ο επιτιθέμενος μπορεί να εκμεταλλευτεί αδυναμίες γνωστές για αυτό το λειτουργικό σύστημα.

2.1.1.2.6 Ευέλικτα Εργαλεία Σάρωσης (Versatile Scanning tools)

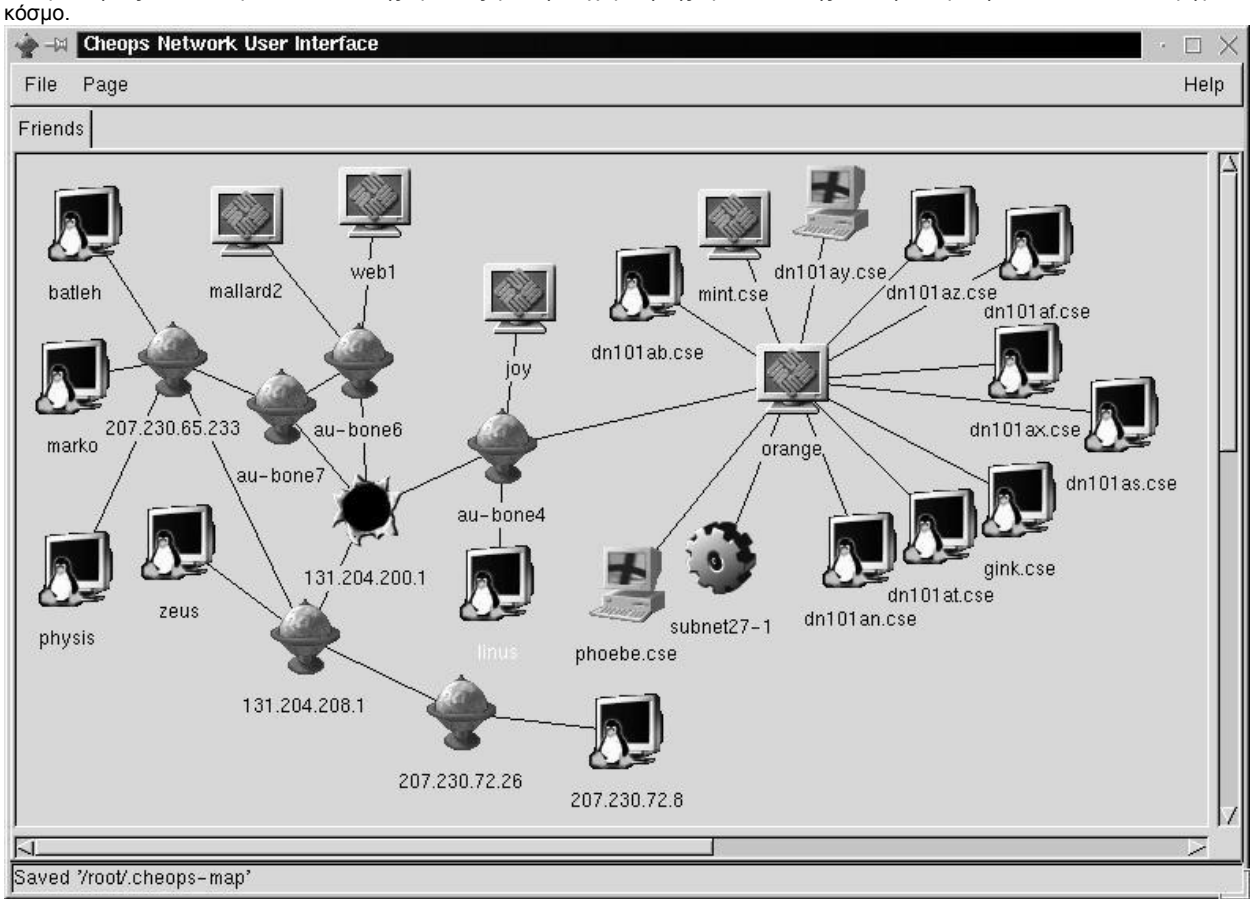
Είναι διαθέσιμος ένας μεγάλος αριθμός από ελεύθερα και εμπορικά εργαλεία σάρωσης. Πολλά από αυτά χρησιμοποιούνται για νόμιμους σκοπούς από τους διαχειριστές συστημάτων είτε για να αποκτήσουν γνώση είτε για να πιστοποιήσουν τις δυνατότητες των υπολογιστών στα δίκτυά τους. Θα απαριθμήσουμε κάποια από τα εργαλεία τα οποία είναι ιδιαίτερα δημοφιλή στους επιτιθέμενους, επειδή συνδυάζουν αρκετές από τις λειτουργίες σάρωσης και αποτύπωσης που αναφέρθηκαν παραπάνω.

Το *Sam Spade* είναι ένας συνδυασμός από χρήσιμα εργαλεία αναγνώρισης με γραφικό σύστημα *Windows*. Οι λειτουργίες του περιλαμβάνουν δυνατότητες *ping*, *whois, IP block whois* (με ερωτήσεις στη βάση δεδομένων *ARIN*), *nslookup, traceroute* και μια λειτουργία που αντιστοιχίζει διευθύνσεις ηλεκτρονικού ταχυδρομείου σε ένα συγκεκριμένο εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Μια έκδοση του *Sam Spade* είναι διαθέσιμη σαν εργαλείο βασισμένο σε *windows*, όπως φαίνεται στο παρακάτω ***σχήμα.***



Σχήμα 3: Αποτύπωση του *Sam Spade*

Άλλα παραδείγματα ελεύθερων εργαλείων σάρωσης περιλαμβάνουν το *CyberKit* και το *Cheops*. Το *Cheops* είναι ένα δημοφιλές και εύκολο στη χρήση εργαλείο για αποτύπωση δικτύου, και μπορεί αυτόματα να σχεδιάσει την τοπολογία ενός δικτύου βασισμένο σε υπολογιστές που έχει ανακαλύψει και στις μεταξύ τους αποστάσεις. Μπορεί επίσης να ανακαλύψει ενεργές υπηρεσίες μέσω της σάρωσης θυρών και να αναγνωρίσει λειτουργικά συστήματα μέσω του ελέγχου αποτυπωμάτων της σωρού *TCP*. Μια εικόνα του *Cheops* φαίνεται στο παρακάτω ***σχήμα***.



Σχήμα 4: Αποτύπωση του *Cheops*

Ένα άλλο παράδειγμα εργαλείου που υπάρχει στο εμπόριο είναι το *Northwest Performance Software's Netscan Tool Pro.* Περιλαμβάνει λειτουργίες *ping*, σάρωσης θυρών, γεννήτριας πακέτων *ICMP*, *whois, nslookup, traceroute*, αναγνώρισης λειτουργικού συστήματος και επικύρωσης διευθύνσεων ηλεκτρονικού ταχυδρομείου. Χρησιμοποιεί μια ασυνήθιστη μέθοδο για την αναγνώριση λειτουργικών συστημάτων βασισμένη στην παρατήρηση των απαντήσεων σε τέσσερεις τύπους μηνυμάτων *ICMP* και στις ποικιλίες τους.

Το *Nmap* αναφέρθηκε ήδη πιο πάνω σαν ένα εργαλείο σάρωσης θυρών, αλλά είναι κάτι περισσότερο από έναν απλό σαρωτή. Το *Nmap* επίσης περιλαμβάνει: σαρώσεις απομακρυσμένων κλήσεων λειτουργιών *RPC (Remote Procedure Calls),* αποστολή σαρώσεων με διαφορετικές επιλογές χρόνου ώστε να αποφευχθεί η ανίχνευση, αναγνώριση του λειτουργικού συστήματος ενός υπολογιστή από τον έλεγχο αποτυπωμάτων της σωρού *TCP*.

2.1.1.3 Σάρωση Ευπαθειών *(Vulnerability Scanning)*

Η ***ενεργή σάρωση*** *(active scanning*) είναι μια ανεκτίμητη μέθοδος ώστε να μάθει ο επιτιθέμενος πληροφορίες για έναν πιθανό στόχο, όπως τις διευθύνσεις *IP* των υπολογιστών, την τοπολογία του δικτύου, τις ανοιχτές θύρες και τα λειτουργικά συστήματα. Το επόμενο βασικό βήμα της αναγνώρισης είναι η σάρωση για την ανακάλυψη συγκεκριμένων αδυναμιών που μπορεί να χρησιμεύσουν σε μια επίθεση. Αν και κάποιος θα μπορούσε να σαρώσει ξεχωριστά κάθε υπολογιστή για να ανακαλύψει αδυναμίες, η μέθοδος αυτή δεν είναι πρακτική. Οι αυτοματοποιημένοι σαρωτές αδυναμιών είναι διαθέσιμοι και συχνά χρησιμοποιούνται από τους διαχειριστές συστημάτων για να εκτιμήσουν το ποσοστό ασφάλειας στα δίκτυά τους.

Τα εργαλεία των επιτιθέμενων έχουν γίνει ιδιαίτερα εκλεπτυσμένα με την πάροδο του χρόνου και συνδυάζουν πολλές λειτουργίες. Για παράδειγμα, πολλά εργαλεία προσφέρουν μαζί δυνατότητες ***ενεργής σάρωσης*** *(active scanning)* και ***σάρωσης αδυναμιών*** (*vulnerability scanning*). Οι σαρωτές εκτιμούν διαφορετικούς τύπους αδυναμιών, αναζητώντας μία από τις τρείς γενικές αδυναμίες των συστημάτων οι οποίες περιλαμβάνουν ***λανθασμένο κώδικα λειτουργικού συστήματος, λανθασμένο κώδικα εφαρμογής ή λανθασμένες διαμορφώσεις (configuration) του συστήματος.***

2.1.1.3.1 Αδυναμίες Συστήματος

Έχουν ανακαλυφθεί πολλές νέες αδυναμίες των λειτουργικών συστημάτων. Οι πιο σημαντικές αδυναμίες συνήθως δημοσιοποιούνται από τους δημιουργούς των λειτουργικών συστημάτων και η δημοσιοποίηση συνοδεύεται από τη διόρθωση της αδυναμίας με ένα διορθωτικό τμήμα κώδικα (*patch*). Στην πράξη οι οργανισμοί δυσκολεύονται να αφιερώσουν το χρόνο και την προσπάθεια που χρειάζεται για να είναι συνεπείς με τα ζητήματα ασφάλειας και τις διορθώσεις που χρειάζονται στον κώδικα. Ο χρόνος που μεσολαβεί από τη δημοσίευση μιας αδυναμίας μέχρι να εγκατασταθεί η διόρθωση του κώδικα, αφήνει ένα παράθυρο ευκαιρίας στους επιτιθέμενους να εκμεταλλευτούν αυτή την αδυναμία. Μια αναφορά του *Symantec* εκτίμησε ότι ο μέσος χρόνος μεταξύ της δημοσίευσης μιας αδυναμίας και της εμφάνισης μιας επίθεσης που σχετίζεται με αυτή την αδυναμία, είναι μικρότερος από μια εβδομάδα. Επομένως, οι οργανισμοί θα πρέπει να ασχολούνται επιμελώς με τις διορθώσεις του κώδικα.

2.1.1.3.2 Αδυναμίες Εφαρμογών

Αδυναμίες δεν υπάρχουν μόνο στα λειτουργικά συστήματα, αλλά υπάρχουν και στις εφαρμογές. Οι εφαρμογές εισάγουν νέους κινδύνους οι οποίοι θέτουν σε δοκιμασία τα λειτουργικά συστήματα, καθώς ανοίγουν νέες θύρες, εγκαθιστούν νέες υπηρεσίες και χρησιμοποιούν πλεονεκτικές διαδικασίες οι οποίες μερικές φορές έχουν λάθη ή είναι ευαίσθητες σε πειρατεία ή δημιουργούν υπερχείλιση της μνήμης. Οι εφαρμογές που συνήθως γίνονται στόχος, περιλαμβάνουν τους φυλλομετρητές (*web browsers)*, τις εφαρμογές υπολογιστή όπως το *Microsoft Word* και το *Excel*, που τρέχουν κώδικα τον οποίο έχουμε βρει από το διαδίκτυο και τον έχουμε «κατεβάσει» στον υπολογιστή. Για παράδειγμα, ένας *web browser* μπορεί να εκτελέσει ένα πρόγραμμα *javascript* από έναν ύποπτο εξυπηρετητή, ο οποίος μπορεί να οδηγήσει τον πελάτη να «κατεβάσει» και να εκτελέσει κακόβουλο λογισμικό.

2.1.1.3.3 Λάθη Διαμόρφωσης του Συστήματος

Ο εξοπλισμός του δικτύου απαιτεί τεχνικές δεξιότητες ώστε να διαμορφωθεί κατάλληλα. Η λανθασμένη διαμόρφωση λόγω άγνοιας ή λάθους μπορεί να θέσει σε αχρηστία τις δυνατότητες ασφάλειας που προσφέρονται μαζί με τα συστήματα του δικτύου. Για παράδειγμα, ένα λανθασμένα διαμορφωμένο τείχος προστασίας (*firewall*) είναι δυνατόν να επιτρέπει την είσοδο περισσότερων ειδών πακέτων. Επίσης, πολλά λειτουργικά συστήματα και υπηρεσίες εφαρμογών, περιλαμβάνουν σταθερούς λογαριασμούς και κωδικούς πρόσβασης (οι οποίοι είναι εύκολο να βρεθούν από το *web*). Αυτοί συνήθως σκοπό έχουν να βοηθήσουν την διαδικασία εγκατάστασης, ή να απλοποιήσουν την διαδικασία εύρεσης λαθών σε περίπτωση που χαθούν οι κωδικοί πρόσβασης. Οι σταθεροί κωδικοί πρόσβασης θα πρέπει να αλλάζουν, αλλά συνήθως αυτό παραμελείται. Οι επιτιθέμενοι συχνά ελέγχουν την ύπαρξη προεπιλεγμένων ρυθμίσεων

του συστήματος γιατί αυτές προσφέρουν έναν εύκολο τρόπο για να επιτεθούν στο σύστημα.

2.1.1.3.4 Σαρωτές Αδυναμιών

Οι περισσότεροι σαρωτές αδυναμιών ενεργούν με παρόμοιο τρόπο. Αρχικά, προσπαθούν να βρουν ενεργούς υπολογιστές ψάχνοντας σε ένα εύρος διευθύνσεων *IP* χρησιμοποιώντας τη λειτουργία *ping* ή άλλες παρόμοιες λειτουργίες. Στη συνέχεια, εκτελούν μια συγκεκριμένη ακολουθία από σαρώσεις για να ανακαλύψουν ανοιχτές θύρες και ενεργές υπηρεσίες που εκτελούνται στους υπολογιστές. Βασισμένοι σε αυτή την πληροφορία, προχωρούν σε περισσότερο προσαρμοσμένες ανιχνεύσεις προς τους υπολογιστές. Στο τελευταίο στάδιο, δημιουργούν ένα είδος αναφοράς (*report*). Κάποιοι σαρωτές αδυναμιών, περιλαμβάνουν επίσης λειτουργίες για την αποτύπωση του δικτύου.

Το *SATAN (Security Administrator's Tool for Analyzing Networks*) είναι ένας πολύ γνωστός σαρωτής αδυναμιών που αναπτύχθηκε το 1995. Το σύστημα αυτό έχει δύο μοντέρνους απογόνους, το ανοιχτό λογισμικό *SARA (Security Auditor's Research Assistant)* και το εμπορικό λογισμικό *SAINT(Security Administrator's Integrated Network Tool)*. Το λογισμικό *SARA* εμπλουτίζει τη μηχανή ασφάλειας και την αρχιτεκτονική προγράμματος του λογισμικού *SATAN* με ένα βελτιωμένο λογισμικό χρήστη και με επικαιροποιημένους ελέγχους αδυναμιών. Το λογισμικό *SARA* μπορεί να ανακαλύψει πληροφορία για υπολογιστές, εξετάζοντας διάφορες υπηρεσίες δικτύου. Μπορεί επίσης να ανακαλύψει πιθανά λάθη στην ασφάλεια, όπως λανθασμένα συσχετισμένες δικτυακές υπηρεσίες, γνωστές αδυναμίες συστημάτων, ή πολιτικές που επιλέχθηκαν με χαμηλού επιπέδου κριτήρια. Μπορεί να δημιουργήσει μια αναφορά με αυτά τα αποτελέσματα ή να εκτελέσει ένα πρόγραμμα για να ανακαλύψει πιθανά προβλήματα ασφάλειας.

Το *Nessus* είναι ένας δημοφιλής, ανοιχτού λογισμικού σαρωτής αδυναμιών. Βασίζεται σε μια αρχιτεκτονική πελάτη- εξυπηρετητή *(client-server),* όπου ο πελάτης και ο εξυπηρετητής μπορεί να λειτουργούν στην ίδια μηχανή. Ο πελάτης αποτελείται από ένα εργαλείο για συσχετισμούς στο χρήστη και από ένα εργαλείο για καταγραφή και αναφορά των αποτελεσμάτων. Ο εξυπηρετητής αποτελείται από μια βάση δεδομένων που περιέχει αδυναμίες συστημάτων, μια βάση για να διατηρεί τα βήματα του τρέχοντος σαρώματος και μια μηχανή σάρωσης. Επίσης, το λογισμικό *Nmap* περιλαμβάνεται, ως εργαλείο σαρώματος θυρών. Η βάση δεδομένων των αδυναμιών είναι σχεδιασμένη ώστε να αποτελείται από ξεχωριστά τμήματα, με *plug-ins*. Κάθε ένα *plug-in* είναι σχεδιασμένο ώστε να ελέγχει για την ύπαρξη μιας συγκεκριμένης αδυναμίας. Το λογισμικό *Nessus* περιλαμβάνει πάνω από 500 *plug-ins*, και οι χρήστες συνεχώς προσθέτουν καινούργια. Οι αδυναμίες βαθμολογούνται και κατατάσσονται σε κατηγορίες όπως για παράδειγμα αδυναμίες σχετικές με τα *windows*, αδυναμίες σχετικές με *CGI (Common Gateway Interface)*, λανθασμένοι συσχετισμοί των τειχών προστασίας (*firewalls*), αδυναμίες του πρωτοκόλλου μεταφοράς αρχείων *(File Transfer Protocol*, *FTP*), αδυναμίες του πρωτοκόλλου ηλεκτρονικού ταχυδρομείου *(Simple Mail Transfer Protocol , SMTP*).

Οι σαρωτές αδυναμιών που υπάρχουν στο εμπόριο περιλαμβάνουν τα λογισμικά *TigerTool's Tiger Suite Pro, McAfee's CyberCop AsaP, ISS's Internet Scanner*, *eEye Digital Security's Retina Network Security Scanner, Cisco System's Secure Scanner*.

2.1.2 Η Απόκτηση Πρόσβασης

Η φάση της επίθεσης για την απόκτηση πρόσβασης σε έναν στόχο, μπορεί να έχει πολλές διαφορετικές μορφές και να εξυπηρετεί διαφορετικούς σκοπούς, όπως το να κλέψει εμπιστευτικά δεδομένα, να αλλοιώσει δεδομένα, να επιτεθεί στην διαθεσιμότητα μιας πηγής ή να κερδίσει παράνομα πρόσβαση στο σύστημα. Όπως είδαμε παραπάνω στο ***σχήμα 1***, οι επιθέσεις μπορούν να αναλυθούν σε τρείς κατηγορίες: επιθέσεις που κατευθύνονται εναντίον συγκεκριμένων στόχων, επιθέσεις μεγάλης κλίμακας που κατευθύνονται αδιάκριτα εναντίον όσο το δυνατόν περισσότερων στόχων ή επιθέσεις που κατευθύνονται εναντίον της δομής του δικτύου. Οι δύο πρώτοι τύποι των επιθέσεων καλύπτονται σε αυτό το κεφάλαιο. Συχνά, οι μεγάλης κλίμακας επιθέσεις έχουν σαν συνέπεια την ευρεία διαταραχή των δικτυακών συστημάτων, άσχετα αν δεν είναι αυτός ο κύριος σκοπός τους.

Οι βασικότεροι τύποι επιθέσεων που θα αναφερθούν εδώ, περιλαμβάνουν *sniffing*, πειρατεία συνόδου (*session hijacking*), επιθέσεις κωδικών πρόσβασης (*password attacks*), εκμετάλλευση (*exploits*), επιθέσεις κοινωνικής μηχανικής *(social engineering), trojan horses, spyware,* ιούς *(viruses, worms),* κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου *(spam)* και επιθέσεις άρνησης παροχής υπηρεσίας (*Denial of Service, DoS*). Αυτή η λίστα των τύπων των επιθέσεων δεν είναι πλήρης, αλλά σκοπό έχει να τονίσει τους πιο κοινούς τύπους επιθέσεων που παρατηρούνται σήμερα και θα συνεχίσουν να υπάρχουν στο εγγύς μέλλον. Θα πρέπει να τονίσουμε ότι η ταξινόμηση δεν υπονοεί ότι αυτές οι μέθοδοι αποκλείουν η μία την άλλη. Συχνά, οι μέθοδοι επίθεσης συνδυάζονται. Για παράδειγμα, οι ιοί μπορεί να διασπαρθούν ταυτόχρονα από επιθέσεις κοινωνικής μηχανικής και αδυναμίες και να δημιουργήσουν άρνηση παροχής υπηρεσίας.

2.1.2.1 Sniffing

Το *sniffing* είναι μια παθητική επίθεση, η οποία προσπαθεί να καταστρατηγήσει την εμπιστευτικότητα της πληροφορίας. Θα μπορούσε να θεωρηθεί μέρος της φάσης της αναγνώρισης (για παράδειγμα μπορεί να χρησιμοποιηθεί για να γίνουν γνωστοί οι κωδικοί πρόσβασης του συστήματος) και να προετοιμάσει μια επίθεση, αλλά μπορεί επίσης να θεωρηθεί και η βασική επίθεση που προσπαθεί να κερδίσει πρόσβαση στην πληροφορία. Τα εργαλεία *sniffers* που παραδοσιακά χρησιμοποιούνται από τους διαχειριστές των δικτύων για την παρακολούθηση της κυκλοφορίας στο δίκτυο και για τον έλεγχο λαθών σε τοπικά δίκτυα *(Local Area Networks, LAN*), αποτελούν τα πιο κοινά εργαλεία επίθεσης. Σε ένα τοπικό δίκτυο κάθε υπολογιστής βλέπει όλη τη διασπορά κυκλοφορίας αλλά αγνοεί τα πακέτα που κατευθύνονται σε άλλους υπολογιστές του δικτύου. Έτσι ο *sniffer* μπορεί να υποκλέψει οτιδήποτε μεταδίδεται στο δίκτυο συμπεριλαμβανομένων των ονομάτων πρόσβασης *(user names*), των κωδικών πρόσβασης (*passwords*), των μηνυμάτων ηλεκτρονικού ταχυδρομείου και όλων των τύπων τα προσωπικά δεδομένα.

Υπάρχουν πολλά εργαλεία *sniffers*, ελεύθερου λογισμικού ή εμπορικά, όπως τα *tcpdump, windump, Snort, Ethereal, Sniffit, dsniff*.

2.1.2.2 Πειρατεία Συνόδου (*Session Hijacking*)

Η πειρατεία συνόδου είναι ένας συνδυασμός διαδικασίας *sniffing* και απάτης διευθύνσεων (*address spoofing)* που επιτρέπει την απομακρυσμένη σύνδεση ενός χρήστη, δίνοντας έτσι τη δυνατότητα σε έναν επιτιθέμενο να έχει μη εξουσιοδοτημένη πρόσβαση σε μια μηχανή, με όλα όμως τα δικαιώματα του νόμιμου χρήστη. Η διαδικασία απάτης των διευθύνσεων, αποστέλλει πακέτα με ψεύτικη διεύθυνση πηγής

(source IP address). Αυτό είναι πολύ απλό, γιατί ο αποστολέας ενός *IP* πακέτου μπορεί να γράψει στο πεδίο της διεύθυνσης πηγής *IP* στην κεφαλίδα του πακέτου. Η διαδικασία της απάτης των διευθύνσεων, επιτρέπει στους επιτιθέμενους να παραστήσουν άλλα πρόσωπα.

Αν ένας χρήστης είναι δεσμευμένος σε μία διαδραστική σύνοδο (για παράδειγμα μέσω *telnet, rlogin, FTP*), ένα εργαλείο πειρατείας συνόδου επιτρέπει στον επιτιθέμενο να κλέψει τη σύνοδο. Όταν τα περισσότερα θύματα πειρατείας βλέπουν ότι χάθηκε η σύνοδός τους, συνήθως υποθέτουν ότι υπάρχει πρόβλημα με το δίκτυο και προσπαθούν πάλι να συνδεθούν, αγνοώντας την επίθεση της πειρατείας.

Δημοφιλή εργαλεία πειρατείας συνόδου αποτελούν το *Juggernaut* και το *Hunt*. Η επίθεση της πειρατείας ξεκινάει με τη διαδικασία *sniffing* που κάνει ο επιτιθέμενος στα πακέτα μιας διαδραστικής συνόδου μεταξύ δύο υπολογιστών, σημειώνοντας προσεκτικά τους αριθμούς ακολουθίας των *TCP* πακέτων. Για να γίνει η πειρατεία στη σύνοδο, ο επιτιθέμενος «μολύνει» τα πακέτα με μία *IP* διεύθυνση πηγής παριστάνοντας τον έναν από τους δύο υπολογιστές της συνόδου. Για να επιτύχει η επίθεση θα πρέπει να χρησιμοποιηθούν οι σωστοί αριθμοί ακολουθίας *TCP*, για να πειστεί ο υπολογιστής που έχει μείνει στη σύνοδο και να δεχτεί τα πακέτα που του στέλνει ο επιτιθέμενος.

2.1.2.3 Επιθέσεις Κωδικών Πρόσβασης (*Password Attacks*)

Οι επιθέσεις κωδικών πρόσβασης επιχειρούν να επιτύχουν πρόσβαση σε έναν υπολογιστή ή σε μια υπηρεσία, έχοντας όλα τα δικαιώματα του κανονικού (νόμιμου) χρήστη. Οι κωδικοί πρόσβασης εξακολουθούν να χρησιμοποιούνται πολύ συχνά για έλεγχο πρόσβασης παρά τη μεγάλη τους αδυναμία: αν ένας κωδικός κλαπεί ή τον μαντέψουν, ο επιτιθέμενος μπορεί να αποκτήσει πλήρη πρόσβαση στο σύστημα. Τα καλύτερα προστατευμένα συστήματα είναι δυνατόν να μείνουν έκθετα εξαιτίας ενός αδύναμου κωδικού. Έτσι, πολλές επιθέσεις συχνά κατευθύνονται στο να μαντέψουν ή να υποκλέψουν τους κωδικούς.

Οι κωδικοί που είναι εύκολο να μαντέψει κάποιος, είναι οι προεπιλεγμένοι *(default)* κωδικοί που είναι εγκατεστημένοι από τα λειτουργικά συστήματα και τις εφαρμογές των υπηρεσιών. Για παράδειγμα, το λογισμικό *Cisco Works 2000* περιλαμβάνει έναν λογαριασμό διαχείρισης με κωδικό *cisco*. Κατάλογοι με προεπιλεγμένους λογαριασμούς και κωδικούς είναι εύκολο να βρεθούν ψάχνοντας στο διαδίκτυο και συχνά αγνοούνται από τους διαχειριστές των συστημάτων.

Οι πιο ισχυρές επιθέσεις κωδικών πρόσβασης, ονομάζονται ***σπάσιμο κωδικών πρόσβασης*** *(password cracking)* και συμβαίνουν σε περίπτωση που ο επιτιθέμενος αποκτήσει πρόσβαση στο αρχείο κωδικών. Τα συστήματα υπολογιστών αποθηκεύουν μια λίστα με λογαριασμούς χρήστη και κωδικούς πρόσβασης σε ένα αρχείο κωδικών και η πληροφορία αυτή είναι κωδικοποιημένη για λόγους προστασίας. Αν ένας επιτιθέμενος αποκτήσει το αρχείο κωδικών έχει το πλεονέκτημα του χρόνου ώστε να σπάσει τους κωδικούς χρησιμοποιώντας «ωμή βία» (για παράδειγμα δοκιμάζοντας όλους τους δυνατούς συνδυασμούς χαρακτήρων).

Η χρήση «ωμής βίας» στην προσπάθεια να μαντέψει κάποιος τους κωδικούς μπορεί να είναι πολύ χρονοβόρα και συχνά δεν είναι απαραίτητη. Το ανθρώπινο ένστικτο οδηγεί στο να διαλέγουμε κωδικούς βασισμένους σε κοινές λέξεις και ονόματα. Ένα λεξικό επίθεσης εκμεταλλεύεται αυτή την τάση μαντεύοντας ένα σύνολο από κοινές λέξεις και ονόματα. Ωστόσο, τα μοντέρνα συστήματα υπολογιστών συνήθως προγραμματίζονται με την πολιτική να αποτρέπουν τους χρήστες από το να διαλέγουν κωδικούς που

κάποιος μπορεί να τους μαντέψει εύκολα. Έτσι, η πιθανότητα να μαντέψει κάποιος τους κωδικούς πρόσβασης δεν είναι πια τόσο δυνατή όσο στο παρελθόν.

Περισσότερο εκλεπτυσμένα εργαλεία που μαντεύουν κωδικούς, συνδυάζουν επιθέσεις μέσω λεξικών με επιθέσεις «ωμής βίας». Ξεκινούν μαντεύοντας κοινές λέξεις και στη συνέχεια μεθοδικά προσθέτουν χαρακτήρες στις λέξεις για να δημιουργήσουν νέες λέξεις. Παραδείγματα εργαλείων που χρησιμοποιούνται για το σπάσιμο κωδικών είναι τα *John the Ripper, Cain and Abel, Crack, Lincrack, L0phtcrack, Nutcracker, PalmCrack και RainbowCrack.*

2.1.2.4 Εκμετάλλευση (*Exploits*)

Όπως αναφέραμε προηγουμένως, νέες αδυναμίες στα λειτουργικά συστήματα και στις εφαρμογές λογισμικού ανακαλύπτονται συνεχώς. Μια αδυναμία είναι η περιγραφή ενός κενού στην ασφάλεια, το οποίο δεν αποτελεί κίνδυνο από μόνο του. Ωστόσο, έχοντας τη γνώση μιας αδυναμίας και τον απαραίτητο χρόνο, οι επιτιθέμενοι μπορούν να δημιουργήσουν ένα λογισμικό για να εκμεταλλευτούν αυτή την αδυναμία. Ο κίνδυνος εμφανίζεται όταν παρουσιάζεται το κακόβουλο λογισμικό και το μοιράζονται πολλοί επιτιθέμενοι. Οι αδυναμίες σχετίζονται με διαφορετικά επίπεδα σοβαρότητας, όπου οι πιο σοβαρές αδυναμίες είναι δυνατόν να οδηγήσουν σε μια ολοκληρωτική καταστροφή του υπολογιστή στόχου.

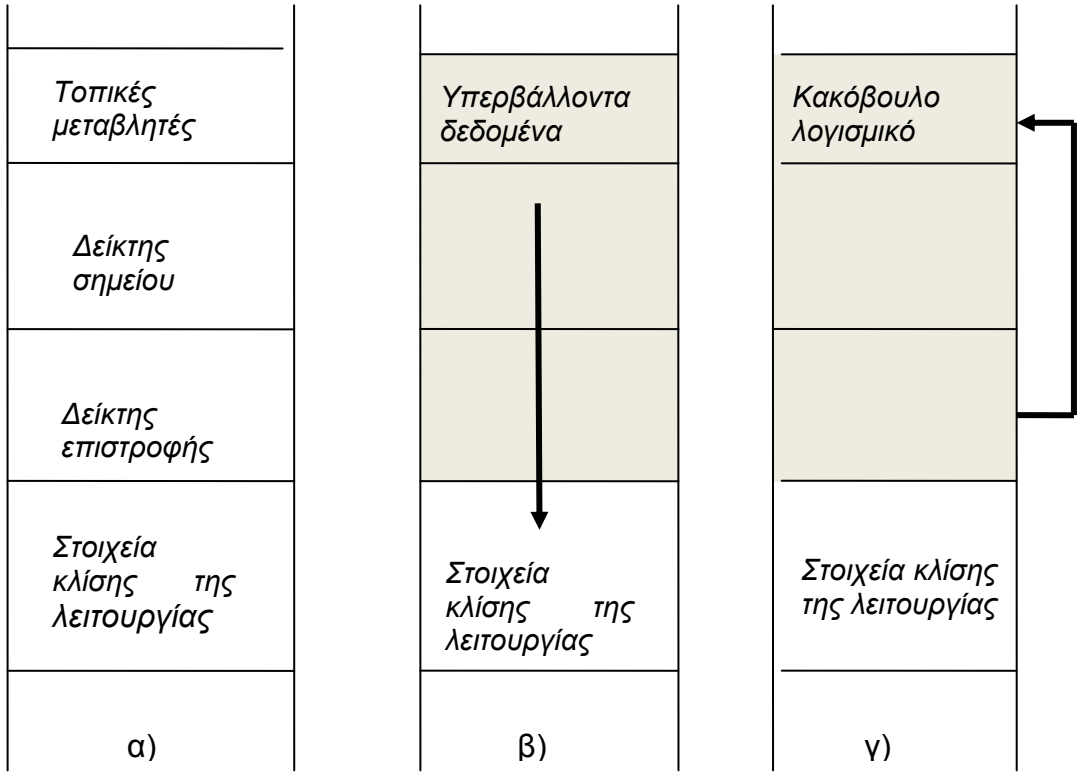
Ένας πάροχος συνήθως έχει γνώση των αδυναμιών του συστήματος, αλλά δεν δημοσιοποιεί αυτή την πληροφορία μέχρις ότου να υπάρξει λύση για το πρόβλημα. Έτσι οι υπάρχουσες αδυναμίες ανακοινώνονται ταυτόχρονα με το λογισμικό που τις διορθώνει. Δυστυχώς, τα λογισμικά που διορθώνουν αυτά τα προβλήματα χρειάζονται χρόνο για να φορτωθούν και να εφαρμοστούν, κυρίως σε μεγάλους οργανισμούς που έχουν πολλούς υπολογιστές. Για πρακτικούς λόγους, οι οργανισμοί συνήθως δυσκολεύονται στο να είναι ενημερωμένοι με τα λογισμικά που αντιμετωπίζουν αδυναμίες. Έτσι, αν ένας οργανισμός αργήσει να ανανεώσει τα συστήματά του με τα λογισμικά που αντιμετωπίζουν τις υπάρχουσες αδυναμίες, είναι πιθανό να εκτεθεί σε νέες επιθέσεις.

Το *SANS* (*The twenty most critical Internet security vulnerabilities*), διατηρεί μια λίστα από τις 20 περισσότερο επικίνδυνες αδυναμίες ασφάλειας στο διαδίκτυο. Η αδυναμία υπερχείλισης της μνήμης είναι μία από τις πιο κοινές που εντοπίζουν οι επιτιθέμενοι. Επιθέσεις υπερχείλισης της μνήμης συνήθως χρησιμοποιούνται από ιούς. Αυτός ο τύπος επίθεσης είναι ελκυστικός στους επιτιθέμενους γιατί πολλές εφαρμογές και λειτουργικά συστήματα δεν εκτελούν ελέγχους στα όρια της μνήμης και έτσι κινδυνεύουν από υπερχείλιση μνήμης. Επιπλέον, μια πετυχημένη επίθεση υπερχείλισης μνήμης μπορεί να οδηγήσει στην απόκτηση πλήρους ελέγχου του υπολογιστή στόχου.

Ένα γνωστό παράδειγμα, είναι η επίθεση εκχύλισης μνήμης που είναι βασισμένη σε σωρό (*stack*), γνωστή σαν ***σπάζοντας τη σωρό*** *(smashing the stack).* Κατά τη διάρκεια της κλίσης μιας λειτουργίας, διάφορα τμήματα δεδομένων σπρώχνονται στη σωρό του προγράμματος *(program stack*): πεδία της λειτουργίας, δείκτης επιστροφής, δείκτες σημείων, τοπικές μεταβλητές. Αυτή η κατάσταση φαίνεται στο ***σχήμα 5α***. Κανονικά, στο τέλος της κλήσης της λειτουργίας, τα δεδομένα πετιούνται έξω από τη σωρό και ο δείκτης επιστροφής χρησιμοποιείται για να συνεχιστεί η εκτέλεση του κυρίως προγράμματος. Η εκχύλιση της μνήμης που βασίζεται σε σωρό, εξαρτάται από την αποθήκευση περισσότερων δεδομένων από αυτά που πρέπει στις τοπικές μεταβλητές. Τα επιπλέον δεδομένα γράφονται στον δεδομένο χώρο της μνήμης και στη συνέχεια γράφονται επάνω από τον δείκτη επιστροφής και τον δείκτη σημείων, όπως φαίνεται στο ***σχήμα 5β***. Στα υπερβάλλοντα δεδομένα, ο επιτιθέμενος είναι δυνατόν να γράψει

στη θέση του δείκτη επιστροφής έναν άλλο δείκτη ο οποίος να δείχνει σε ένα σημείο της σωρού όπου ο επιτιθέμενος έχει γράψει το κακόβουλο λογισμικό (***σχήμα 5γ***). Έτσι, αντί να ξεκινήσει η εκτέλεση του κυρίως προγράμματος στο τέλος κλίσης της λειτουργίας, θα εκτελεστεί το κακόβουλο λογισμικό.

Είναι φανερό ότι η επίθεση εκχύλισης μνήμης απαιτεί προσεκτικό γράψιμο κώδικα και τεχνικές γνώσεις σχετικές με την αρχιτεκτονική του επεξεργαστή στόχου. Επομένως αυτού του είδους οι επιθέσεις δεν είναι εύκολο να σχεδιαστούν από τη αρχή. Γι αυτό το λόγο υπάρχουν ήδη γραμμένα κακόβουλα λογισμικά αυτού του είδους, που τα μοιράζονται οι επιτιθέμενοι και μπορούν να χρησιμοποιηθούν χωρίς να απαιτούν ιδιαίτερες τεχνικές γνώσεις.



Σχήμα 5: Επίθεση υπερχείλισης μνήμης

2.1.2.5 Κοινωνική Μηχανική *(Social Engineering)*

Οι επιθέσεις κοινωνικής μηχανικής έχουν το πλεονέκτημα της ανθρώπινης δράσης. Κοινωνικές ικανότητες χρησιμοποιούνται για να ξεγελάσουν το θύμα έτσι ώστε να αποκαλύψει προσωπικές πληροφορίες ή να ανοίξει ένα μολυσμένο μήνυμα ηλεκτρονικού ταχυδρομείου. Η κοινωνική μηχανική μπορεί να συνδυαστεί με πολλές άλλες μεθόδους επίθεσης. Αν και οι επιθέσεις κοινωνικής μηχανικής είναι απλές και δεν απαιτούν αυξημένες τεχνικές γνώσεις, μπορεί να είναι πολύ αποτελεσματικές αν εκτελεστούν σωστά.

Στο παρελθόν το τηλέφωνο αποτελούσε μια δημοφιλή μέθοδο για επιθέσεις κοινωνικής μηχανικής. Σήμερα, πολλές επιθέσεις κοινωνικής μηχανικής γίνονται μέσω του ηλεκτρονικού ταχυδρομείου, λόγω του μικρού κινδύνου και του μικρού κόστους που έχει

η μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Επίσης, το ηλεκτρονικό ταχυδρομείο είναι διαθέσιμο σε πολλές διαφορετικές πλατφόρμες υπολογιστών και σε διαφορετικούς τύπους συσκευών. Το ηλεκτρονικό ταχυδρομείο έγινε το αγαπημένο μέσο των επιτιθέμενων μετά την επιτυχία που είχε η μαζική αποστολή ιών μέσω ηλεκτρονικού ταχυδρομείου όπως οι ιοί *2000 Love Letter* και *2001 Anna Kournikova*. Οι ιοί του ηλεκτρονικού ταχυδρομείου τυπικά προσφέρουν έναν προκλητικό λόγο στον παραλήπτη για να τον δελεάσουν να ανοίξει το αρχείο που συνοδεύει το μήνυμα και έτσι να μολυνθεί ο υπολογιστής του. Πρόσφατα, τα ηλεκτρονικά μηνύματα μπορεί να παριστάνουν ότι αφορούν θέματα ασφάλειας, ειδοποιήσεις από τον πάροχο υπηρεσιών διαδικτύου (*Internet Service Provider*, *ISP)* ή από τον διαχειριστή του συστήματος ή άλλου είδους μηνύματα που μοιάζουν επίσημα.

Πρόσφατα, εμφανίστηκε ένας νέος τύπος επίθεσης κοινωνικής μηχανικής που ονομάζεται *phishing*. Οι επιθέσεις *phishing* ξεκινούν με ένα ηλεκτρονικό μήνυμα που μοιάζει να προέρχεται από μια εταιρεία πιστωτικών καρτών ή από έναν οικονομικό οργανισμό και ζητάει πληροφορίες λογαριασμού, αναφέροντας ότι υπάρχει ένα πρόβλημα με ένα λογαριασμό ή με μία συναλλαγή. Αυτά τα ηλεκτρονικά μηνύματα είναι πολύ προσεκτικά γραμμένα ώστε να μοιάζουν αληθινά και επίσης συχνά περιλαμβάνουν κλεμμένα γραφικά των εταιρειών. Επίσης περιλαμβάνουν και μία σύνδεση (*link*) που κατευθύνει το θύμα σε μία σελίδα διαδικτύου (*web*) η οποία φαίνεται αυθεντική, αλλά στην πραγματικότητα είναι ψεύτικη. Ο σκοπός της ψεύτικης σελίδας *web* είναι να συγκρατήσει οποιαδήποτε πληροφορία λογαριασμού ή προσωπική που θα συμπληρώσει το θύμα ή να εγκαταστήσει κακόβουλο λογισμικό στον υπολογιστή του θύματος.

2.1.2.6 Trojan Horses

Τα λεγόμενα *trojan horses* αποτελούν κακόβουλο λογισμικό το οποίο όμως εμφανίζεται ως καλοήθες. Ο σκοπός της μεταμφίεσης είναι να δελεάσει τον χρήστη ώστε να εγκαταστήσει και να εκτελέσει ένα πρόγραμμα. Αν εκτελεστούν, τα *trojan horses* μπορούν να κάνουν ότι κάνουν και τα άλλα προγράμματα που τρέχουν με τα δικαιώματα του χρήστη. Τα *trojan horses* μπορούν να συνδυαστούν με άλλα είδη επιθέσεων (όπως επιθέσεις κοινωνικής μηχανικής) και να δημιουργήσουν πρόβλημα στην ασφάλεια.

Ο όρος ***trojan horse*** περιλαμβάνει κάποιους τύπους λαθραίου κακόβουλου λογισμικού που προσπαθούν να κρύψουν την ύπαρξή τους στον υπολογιστή-θύμα. Αυτά τα *trojan horses* διανέμονται με διάφορους λαθραίους τρόπους, όπως με ιούς, με την μεταφορά αρχείων, με την φόρτωση σελίδων *web*. Τα θύματα συνήθως δεν αντιλαμβάνονται την εγκατάσταση των *trojan horses*.

Τα περισσότερο ανησυχητικά *trojan horses* είναι προγράμματα που ονομάζονται *trojan* απομακρυσμένης σύνδεσης (*Remote Access Trojans, RATs*), και επιτρέπουν στον επιτιθέμενο να αποκτήσει απομακρυσμένη πρόσβαση στην μηχανή του θύματος. Αυτά τα προγράμματα καταστρατηγούν τον συνηθισμένο έλεγχο ασφάλειας πρόσβασης (δηλ. την πρόσβαση με τη χρήση κωδικού πρόσβασης). Πολλά τέτοια προγράμματα *trojan* απομακρυσμένης σύνδεσης είναι γνωστά και χρησιμοποιούνται για νόμιμες διαχειριστικές χρήσεις.

2.1.2.7 Adware, Spyware

Το *Adware* είναι λογισμικό που χρησιμοποιείται για να παρακολουθεί και να καταγράφει την συμπεριφορά του χρήστη στον υπολογιστή, τυπικά για λόγους στοχευμένου *marketing*. Το *Adware* συνήθως εγκαθίσταται σε έναν υπολογιστή όπως και τα άλλα

λογισμικά χωρίς να το γνωρίζει ο χρήστης. Ακόμα και όταν ο χρήστης ειδοποιηθεί για την παρουσία λογισμικού *Adware*, αυτό το λογισμικό μπορεί να αποτελέσει μια επίθεση στην ιδιωτικότητα του χρήστη, όταν θα πρέπει να κοινοποιηθεί πληροφορία για το χρήστη προς τους οργανισμούς *marketing*. Βασικά, το *Adware* αποτελεί περισσότερο μια ενόχληση, εμφανίζοντας συχνά παράθυρα διαφημίσεων κατά τη διάρκεια περιήγησης στο διαδίκτυο.

Μια περισσότερο σοβαρή ανησυχία, αποτελεί ένας άλλος τύπος λογισμικού που παρακολουθεί και καταγράφει τις δραστηριότητες του χρήστη και ονομάζεται *Spyware*. Έχει υπολογιστεί ότι το 88% των προσωπικών υπολογιστών είχε μολυνθεί από *Spyware* και ότι 89.806 σελίδες *web* περιείχαν *Spyware* έτοιμο να φορτωθεί σε υπολογιστές, το πρώτο τετράμηνο του 2005. Αντίστοιχα με το *Adware*, το *Spyware* μπορεί να εγκατασταθεί σε έναν υπολογιστή εν γνώσει του χρήστη ή του διαχειριστή του συστήματος. Για παράδειγμα, εμπορικές εκδόσεις του *Spyware*, πωλούνται σαν μέσα για την παρακολούθηση των δραστηριοτήτων στον υπολογιστή των παιδιών ή των υπαλλήλων ενός οργανισμού. Ωστόσο, πολύ συχνά το *Spyware* εγκαθίσταται λαθραία σε έναν υπολογιστή σαν *trojan horse* ή σαν μέρος ενός ιού. Το *Spyware* καταγράφει τις σελίδες που επισκέπτεται ένας χρήστης στο διαδίκτυο, τους κωδικούς και οτιδήποτε γίνεται στον υπολογιστή. Αφού τα καταγράψει, το *Spyware* μεταφέρει τα κλεμμένα δεδομένα μέσα από διάφορα κανάλια (π.χ. ηλεκτρονικό ταχυδρομείο, *FTP*, φόρτωση σε σελίδα του διαδικτύου) στον επιτιθέμενο.

2.1.2.8 Ιοί *(Viruses, Worms)*

Οι ιοί αποτελούν λογισμικό που είναι σχεδιασμένο ώστε να επαναλαμβάνεται. Το είδος των ιών που ονομάζεται *virus*, αποτελείται από αποσπάσματα (*snippets)* προγράμματος που επαναλαμβάνονται μετατρέποντας ένα κανονικό πρόγραμμα ή αρχείο σε μια επανάληψή του. Δεν είναι αυτούσια προγράμματα υπολογιστών αλλά εξαρτώνται από την εκτέλεση των μολυσμένων προγραμμάτων. Όταν το βασικό πρόγραμμα εκτελείται, ο κώδικας του ιού εκτελείται επίσης και φτιάχνει ένα αντίγραφο του εαυτού του σε άλλα αρχεία.

Αντίθετα, το είδος των ιών που ονομάζονται *worms*, είναι αυτούσια προγράμματα που επαναλαμβάνονται, διασπείροντας αντίγραφα του εαυτού τους σε άλλα συστήματα μέσα στο δίκτυο. Τα *worms* έχουν επικρατήσει σε σχέση με τα *virus* τα τελευταία χρόνια λόγω της αύξησης των δικτύων υπολογιστών. Σήμερα, όλοι οι υπολογιστές είναι συνδεδεμένοι σε δίκτυο μέσω του διαδικτύου, το οποίο αποτελεί ένα πολύ φιλικό περιβάλλον για *worms*. Συγκεκριμένα, η μεγάλη εξάπλωση του ηλεκτρονικού ταχυδρομείου έχει διευκολύνει τα *worms* στο να εξαπλωθούν σε διαφορετικές πλατφόρμες υπολογιστών.

Τα *virus* έχουν εξελιχθεί με τα χρόνια σε πολυπλοκότητα. Στην αρχή απλά πρόσθεταν τον κώδικά τους στην αρχή ή στο τέλος του αρχείου του υπολογιστή (*host file*). Για να αποφύγουν την ανίχνευση στη συνέχεια, άρχισαν να διασπείρουν τον κώδικά τους σε όλο το αρχείο του υπολογιστή. Μια άλλη τεχνική που χρησιμοποιούν τα *virus* για να αποφύγουν την ανίχνευση είναι να κωδικοποιούν τον κώδικά τους μέσα σε κάθε εμφάνιση του αρχείου του υπολογιστή, κάνοντας έτσι πιο δύσκολη τη δημιουργία μιας υπογραφής για το συγκεκριμένο *virus*. Όταν τα αντιιϊκά προγράμματα άρχισαν να εμβαθύνουν στον αλγόριθμο αποκρυπτογράφησης για την υπογραφή, τα *virus* έγιναν πολυμορφικά, μεταβάλλοντας τον αλγόριθμο κρυπτογράφησης σε κάθε αντίγραφο. Επίσης κάποια *virus* μεταμορφώνονταν, αλλάζοντας τη λογική τους σε κάθε εμφάνιση της μόλυνσης.

Τα *worms* που διαδίδονται μέσω του δικτύου, δεν εξελίχθηκαν με τον ίδιο τρόπο όπως τα *virus* που μολύνουν αρχεία. Λειτουργικά, ένα πρόγραμμα *worm* θα πρέπει να ακολουθήσει κάποια συγκεκριμένα βήματα για να διαδοθεί σε έναν άλλο στόχο αφού μολύνει τον υπολογιστή-θύμα.

Αρχικά, ένας αλγόριθμος επιλέγει υποψήφιους για τους επόμενους στόχους. Ο απλούστερος αλγόριθμος που χρησιμοποιείται από αρκετά *worms*, είναι να επιλεγεί μια διεύθυνση *IP* (αριθμός 32-*bit*) τυχαία. Περισσότερο εξελιγμένοι αλγόριθμοι, επιλέγουν διευθύνσεις μέσα από το ίδιο δίκτυο, επειδή τα τοπικά δίκτυα έχουν μικρότερες καθυστερήσεις διάδοσης και επιτρέπουν την ταχύτερη διασπορά του ιού.

Στη συνέχεια, κάποια *worm* εκτελούν σάρωση των επιλεγμένων στόχων. Οι σαρώσεις παρουσιάζουν απαντήσεις από τους επιλεγμένους στόχους που δίνουν μια ένδειξη για το αν οι καταστροφές που έχουν προγραμματίσει τα *worm* μπορεί να είναι επιτυχημένες. Αυτή η διαδικασία, εμφανίζει τελικά τους πιο βολικούς στόχους μεταξύ των υποψηφίων.

Το τρίτο βήμα είναι η καταστροφή ή η επίθεση προς το στόχο. Μια συνηθισμένη επίθεση είναι η αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου προς το στόχο, που συνήθως μεταφέρει ένα μολυσμένο αρχείο που πρέπει να εκτελεστεί. Πιο εξελιγμένα μηνύματα ηλεκτρονικού ταχυδρομείου με *worm* ενεργοποιούνται όταν το μήνυμα ληφθεί ή διαβαστεί. Άλλα *worm* επιτίθενται μέσω αποστολής αρχείων ή εισαγωγής κωδικού πρόσβασης.

Το τέταρτο βήμα, μετά την απόκτηση πρόσβασης είναι η μεταφορά ενός αντιγράφου του *worm* στο στόχο. Ανάλογα με το είδος της επίθεσης, το αντίγραφο του *worm* μπορεί να έχει μεταφερθεί κατά τη διάρκεια της επίθεσης. Ωστόσο, κάποιες επιθέσεις δημιουργούν μόνο τα μέσα για την πρόσβαση. Τα *worm* εκμεταλλεύονται την πρόσβαση για να μεταφέρουν ένα αντίγραφο του εαυτού τους μέσα από διάφορα πρωτόκολλα όπως *FTP, HTTP, Trivial File Transfer Protocol (TFTP)*.

Ένα προαιρετικό, τελευταίο βήμα είναι η εκτέλεση του ωφέλιμου φορτίου του *worm*, αν υπάρχει. Αυτό είναι το μέρος του προγράμματος που απευθύνεται στο θύμα και δεν είναι σχετικό με τη διάδοση. Αυτό το ωφέλιμο φορτίο μπορεί να είναι για παράδειγμα λογισμικό που επιτρέπει την απομακρυσμένη σύνδεση, εγκαθιστά *spyware*, απενεργοποιεί αντιιϊκά προγράμματα ή φορτώνει κώδικα *worm* από το διαδίκτυο.

2.1.2.9 Κακόβουλα Μηνύματα Ηλεκτρονικού Ταχυδρομείου *(Spam)*

Τα *spam* είναι μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν «σκουπίδια» και αποτελούν ένα πρόβλημα το οποίο συνεχώς διογκώνεται. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου στις οποίες στέλνονται τα *spam*, βρίσκονται από το διαδίκτυο ή δημιουργούνται τυχαία. Συνήθως διαφημίζουν ένα προϊόν, μια υπηρεσία ή ένα είδος επένδυσης (η οποία συνήθως είναι απάτη). Το είδος αυτό της επίθεσης είναι ιδιαίτερα ελκυστικό γιατί κάποιος μπορεί να στείλει μεγάλους όγκους ηλεκτρονικών μηνυμάτων με πολύ μικρό κόστος. Επίσης τα εργαλεία που χρειάζονται είναι πολύ κοινά: ένας ηλεκτρονικός υπολογιστής, το κατάλληλο λογισμικό και μια σύνδεση διαδικτύου.

Μια πηγή ανησυχίας σχετική με τα *spam*, είναι το γεγονός ότι υπάρχει συνεργασία μεταξύ των επιτιθέμενων που στέλνουν *spam*, των επιτιθέμενων που γράφουν λογισμικό ιών και του οργανωμένου εγκλήματος. Ένας μεγάλος αριθμός από ιούς έχει χρησιμοποιηθεί σαν όχημα για τη μετάδοση *trojan horses* τα οποία δημιουργούν το φαινόμενο *bot* στα δίκτυα. Τα *bot* είναι προγράμματα τα οποία παίρνουν οδηγίες από έναν απομακρυσμένο χρήστη (επιτιθέμενο) ή επιτρέπουν να γίνει μια σύνδεση που

όμως την αγνοεί ο χρήστης του υπολογιστή. Συνήθως τα *bot* χρησιμοποιούνται για κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσίας ή για αποστολή *spam*.

2.1.2.10 Άρνηση Παροχής Υπηρεσίας (*Denial of Service, DoS)*

Πολλοί θεωρούν τις επιθέσεις άρνησης παροχής υπηρεσίας σαν ένα είδος πλημμύρας, αλλά υπάρχουν τουλάχιστον 4 τύποι τέτοιων επιθέσεων:

- Εξάντληση των πόρων μιας μηχανής (π.χ. κύκλων της Κεντρικής Μονάδας Επεξεργασίας (*Central Processing Unit*,*CPU)*, της μνήμης),
- Αποτυχία των εφαρμογών και των λειτουργικών συστημάτων να χειριστούν εξαιρετικές συνθήκες, λόγω αποτυχίας των προγραμμάτων,
- Επιθέσεις στη δρομολόγηση και στο *DNS,*
- Αδυναμία σύνδεσης με το δίκτυο καταναλώνοντας το εύρος ζώνης με πλημμύρα κίνησης.

Υπάρχουν πάρα πολλά παραδείγματα επιθέσεων άρνησης παροχής υπηρεσίας. Ένα παράδειγμα εξάντλησης είναι η επίθεση εδάφους *(land attack*). Σε μηχανές που χρησιμοποιούσαν *Windows NT* (πριν το πακέτο 4), η επίθεση εδάφους μπορούσε να κάνει τη μηχανή να καταναλώνει συνεχώς κύκλους *CPU*. Το *ping* του «θανάτου» είναι ένα *ICMP Echo request* μήνυμα που ξεπερνάει το μέγιστο επιτρεπτό μέγεθος των 65.536 *bytes*. Μπορούσε να κάνει παλαιότερα λειτουργικά συστήματα να καταρρεύσουν ή να παγώσουν (στα νεότερα λειτουργικά συστήματα αυτό έχει διορθωθεί).

Η επίθεση *Smurf* είναι ένα παράδειγμα έμμεσης επίθεσης πλημμύρας, όπου το πρωτόκολλο *ICMP* παραβιάζεται ώστε να προκαλέσει την αποστολή πολλών πακέτων απάντησης στη μηχανή-θύμα σε απάντηση ενός πακέτου αναμετάδοσης (*broadcast*). Αποτελεί έμμεση επίθεση γιατί η πραγματική διεύθυνση του επιτιθέμενου δεν εμφανίζεται στα πακέτα. Επίσης είναι ιδιαίτερα ενδιαφέρουσα, καθώς ένα πακέτο επίθεσης πολλαπλασιάζεται σε πολλά πακέτα από τους αποδέκτες της διασποράς.

Οι περισσότερο επικίνδυνες επιθέσεις πλημμύρας εκμεταλλεύονται τη διεύρυνση μέσα σε ένα κατανεμημένο δίκτυο. Παραδείγματα αυτοματοποιημένων, κατανεμημένων εργαλείων άρνησης παροχής υπηρεσίας είναι τα *Trin00*, *TFN (tribe flood network), TFN2K*, *Stachelbrat*.

Οι κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσίας αποτελούνται από δύο φάσεις. Στην πρώτη φάση έχουμε την προετοιμασία του δικτύου της κατανεμημένης άρνησης παροχής υπηρεσίας *(Distributed Denial of Service*, *DdoS)*. Ο επιτιθέμενος προσπαθεί να μολύνει ένα μεγάλο αριθμό από υπολογιστές, συνήθως προσωπικούς υπολογιστές με μια σύνδεση αναμετάδοσης, εγκαθιστώντας ένα *DoS agent* (π.χ. ένα *trojan horse*). Τα κατανεμημένα εργαλεία όπως το *Trin00* και το *TFN* εγκαθιστούν ένα δίκτυο δύο επιπέδων. Ένας μικρός αριθμός μολυσμένων μηχανημάτων που ονομάζονται *masters*, περιμένουν εντολές από τον επιτιθέμενο. Οι υπόλοιπες μηχανές αποτελούν τους *daemons* και παίρνουν εντολές από τους *masters*. Οι *daemons* είναι τελικά αυτοί που εκτελούν την επίθεση στους συγκεκριμένους στόχους.

2.1.3 Η Κάλυψη

Το τελευταίο στάδιο μιας επίθεσης είναι η κάλυψη. Στη φάση της αναγνώρισης ή της επίθεσης, είναι φυσικό ο επιτιθέμενος να επιθυμεί να αποφύγει την αναγνώρισή του, η οποία θα προκαλέσει και κινήσεις άμυνας.

Μετά από μια πετυχημένη επίθεση, την απόκτηση της πρόσβασης ή την απόκτηση του ελέγχου, ο επιτιθέμενος επιθυμεί να κρύψει τα ίχνη της επίθεσης. Η αναγνώριση μιας επίθεσης μπορεί να προκαλέσει αμυντικές ενέργειες για να αποφευχθεί η επίθεση, ενέργειες ιχνηλάτισης ώστε να βρεθεί ο επιτιθέμενος και ενδυνάμωση των συστημάτων άμυνας.

2.1.3.1 Αποφυγή των Συστημάτων Ανίχνευσης Επίθεσης *(Intrusion Detection Systems, IDS)*

Τα συστήματα *IDS* έχουν σχεδιαστεί για να ειδοποιούν τους διαχειριστές συστημάτων για σημάδια ύποπτων ενεργειών. Αποτελούν κάτι ανάλογο με τους συναγερμούς και είναι σχεδιασμένα για να αντιδρούν σε εισβολείς που είναι ικανοί να καταστρατηγήσουν τις άμυνες των υπολογιστών (π.χ. τείχη προστασίας). Τα δικτυακά συστήματα *IDS (network based)* παρακολουθούν την κίνηση στο δίκτυο και μπορούν να υλοποιηθούν σε μία μηχανή ή να ενσωματωθούν σε τείχη προστασίας και σε δρομολογητές (*routers*). Τα υπολογιστικά συστήματα *IDS (host based*) είναι διεργασίες που εκτελούνται στους υπολογιστές και παρακολουθούν τις δραστηριότητες του συστήματος. Τα συστήματα *IDS* έχουν ευρεία χρήση από τους οργανισμούς. Οι επιτιθέμενοι συνήθως θέλουν να αποφύγουν την αναγνώριση από αυτά τα συστήματα.

Αν δεν πάρει ιδιαίτερες προφυλάξεις, ένας επιτιθέμενος μπορεί εύκολα να αναγνωριστεί από ένα σύστημα *IDS* κατά τη φάση της αναγνώρισης, επειδή τα εργαλεία σάρωσης προκαλούν αρκετό θόρυβο. Η σάρωση θυρών (*port scanning)* είναι δυνατόν να εμπλέκει χιλιάδες πακέτα, ενώ η σάρωση αδυναμιών *(vulnerability scanning)* μπορεί να εμπλέκει εκατοντάδες χιλιάδες πακέτα. Αυτές οι σαρώσεις έχουν μια αξιοσημείωτη επίδραση στην κανονική κίνηση μέσα στο δίκτυο. Επιπλέον, τα συστήματα *IDS* είναι σχεδιασμένα για να αναζητούν αυτών των ειδών τις σαρώσεις.

Τα περισσότερα εμπορικά συστήματα *IDS* προσπαθούν να αντιστοιχίσουν την κυκλοφορία στο δίκτυο με μια βάση δεδομένων που περιέχει υπογραφές επιθέσεων. Αυτή η προσέγγιση ονομάζεται ***κακή χρήση*** ή ***αναγνώριση βασισμένη σε υπογραφές*** *(signature-based detection).* Έτσι, ένας επιτιθέμενος θα προσπαθούσε να αποφύγει το ταίριασμα των υπογραφών αλλάζοντας τα πακέτα ή το πρότυπο κίνησης μιας επίθεσης. Μια προσέγγιση για να αλλάξει την εμφάνιση μιας επίθεσης, είναι να εκμεταλλευτεί τον κατακερματισμό των *IP* πακέτων *(IP fragmentation*). Ένα σύστημα *IDS* θα πρέπει να επανασυναρμολογεί τα κομμάτια για να μπορεί να ανιχνεύσει μια επίθεση. Ένα σύστημα *IDS* χωρίς τη δυνατότητα να επανασυναρμολογεί τα κομμάτια θα μπορούσε να αποφευχθεί με το σπάσιμο των πακέτων της επίθεσης.

Η αποφυγή των συστημάτων *IDS* είναι πιθανή και στο επίπεδο εφαρμογών (*application layer)*. Για παράδειγμα, ένα σύστημα *IDS* μπορεί να έχει μια υπογραφή για επιθέσεις σε γνωστά και αδύναμα προγράμματα του *Common Gateway Interface* (*CGI)* στον εξυπηρετητή *web*. Ένας επιτιθέμενος θα μπορούσε να προσπαθήσει να αποφύγει αυτή την υπογραφή στέλνοντας μια αίτηση *Hypertext Transfer Protocol* (*HTTP)* για ένα πρόγραμμα *CGI*, προσαρμόζοντας κατάλληλα την αίτηση *HTTP* ώστε η υπογραφή να μην ταιριάζει, αλλά η αίτηση να γίνεται δεκτή στον εξυπηρετητή *web*.

Μια άλλη στρατηγική για να αποφευχθεί η ανίχνευση από ένα σύστημα *IDS*, είναι να υπερφορτώσουμε το σύστημα με κοινά και μη σημαντικά γεγονότα ώστε να καλυφθεί η πραγματική επίθεση. Το «πέταγμα κάτω από το ραντάρ» του *IDS* είναι κάτι εύκολο να γίνει όταν χιλιάδες ανώφελες σαρώσεις θυρών και σαρώσεις *ping* γεμίζουν τις κονσόλες των χρηστών και τα αρχεία, ενώ παράλληλα εκτελείται μια πιο εξειδικευμένη επίθεση.

2.1.3.2 Μετατροπή Αρχείων Καταγραφής (*Logs)*

Η κάλυψη των αποδείξεων μετά από μια επίθεση είναι πολύ σημαντική αν ο επιτιθέμενος θέλει να διατηρήσει τον έλεγχο των συστημάτων των θυμάτων. Έτσι δημιουργείται η ανάγκη να αλλάξει τα αρχεία συστήματος στους υπολογιστές των θυμάτων. Οι μηχανές *UNIX* διατηρούν ένα αρχείο συστήματος για όλες τις ενέργειες του συστήματος, το οποίο μπορούν να βλέπουν οι διαχειριστές του συστήματος για να ανιχνεύσουν σημάδια εισχώρησης στο σύστημα.

Ένας επιτιθέμενος χρειάζεται να αποκτήσει επαρκή δικαιώματα πρόσβασης, όπως αυτά του διαχειριστή για να αλλάξει τα αρχεία του συστήματος. Οι επιτιθέμενοι δεν σβήνουν τα αρχεία του συστήματος, γιατί η απουσία αυτών των αρχείων θα επισημανθεί από τους διαχειριστές του συστήματος και θα θεωρηθεί ύποπτη. Αντίθετα, ένας εξειδικευμένος επιτιθέμενος θα προσπαθήσει να γράψει στα αρχεία του συστήματος για να σβήσει ύποπτα γεγονότα, όπως αποτυχημένες προσπάθειες πρόσβασης, συνθήκες λάθους και προσβάσεις σε αρχεία.

2.1.3.3 Rootkits

Τα *rootkits* είναι γνωστά σαν τα πιο επικίνδυνα μέσα για να καλύπτουν οι επιτιθέμενοι τα ίχνη τους. Έχουν ονομαστεί έτσι από την πρόσβαση στον βασικό λογαριασμό *(root account)* που είναι ο σημαντικότερος στόχος στα *UNIX* συστήματα γιατί ο βασικός χρήστης *(root user*) έχει πλήρη πρόσβαση στο σύστημα. Αν ένας επιτιθέμενος αποκτήσει τη βασική πρόσβαση, είναι πιθανό να εγκαταστήσει ένα *rootkit* σχεδιασμένο να κρύβει σημάδια επίθεσης αλλάζοντας επιλεκτικά τα στοιχεία του συστήματος. Το *rootkit* δεν μπορεί να ανιχνευθεί σαν μια επιπλέον εφαρμογή ή διεργασία. Είναι μια αλλαγή στο ίδιο το λειτουργικό σύστημα. Για παράδειγμα, τα συστήματα *UNIX* περιλαμβάνουν ένα πρόγραμμα *ifconfig* που δείχνει την κατάσταση των διεπαφών του δικτύου, περιλαμβάνοντας και τις ανάμεικτες διεπαφές. Ένα *rootkit* μπορεί να αλλάξει το πρόγραμμα *ifconfig*, έτσι ώστε ποτέ να μην αποκαλύπτει τις ανάμεικτες διεπαφές και με αυτό τον τρόπο να κρύβει την παρουσία ενός *sniffer*. Ένα άλλο πρόγραμμα, το *find*, είναι χρήσιμο στο να βρίσκει αρχεία και καταλόγους (*directories*). Ένα *rootkit*, μπορεί να αλλάξει το πρόγραμμα *find* ώστε να κρύβει τα αρχεία ενός επιτιθέμενου.

Τα *rootkits* σε επίπεδο πυρήνα (*Kernel)* έχουν εξελιχθεί από τα παραδοσιακά *rootkits*. Στα περισσότερα λειτουργικά συστήματα, το *Kernel* είναι ο πυρήνας του συστήματος που ελέγχει τις διεργασίες, τη μνήμη του συστήματος, την πρόσβαση στο δίσκο και άλλες βασικές λειτουργίες του συστήματος. Όπως υπονοεί ο όρος, τα *rootkit* επιπέδου *Kernel* μετατρέπουν το ίδιο το *Kernel*. Έτσι η επίθεση γίνεται στον πυρήνα του συστήματος, ώστε κανένα πρόγραμμα και καμία λειτουργία να μην είναι ανόθευτη. Τα *rootkit* επιπέδου *Kernel* είναι πιθανό να μην είναι δυνατόν να ανακαλυφθούν.

2.1.3.4 Συγκαλυμμένα Κανάλια (*Covert Channels)*

Αν και τα αρχεία του συστήματος και τα λειτουργικά συστήματα μπορούν να μετατραπούν ώστε να αποκρύψουν κάποια επίθεση, η παρουσία ενός κινδύνου στο σύστημα μπορεί να αποκαλυφθεί από τις επικοινωνίες. Για παράδειγμα, οι διαχειριστές του συστήματος μπορεί να αναγνωρίσουν πακέτα από έναν επιτιθέμενο με τα οποία προσπαθεί να αποκτήσει πρόσβαση μέσω μιας συγκεκριμένης θύρας. Επομένως, ένας επιτιθέμενος συνήθως προσπαθεί να κρύψει τις κινήσεις του μέσω συγκαλυμμένων καναλιών.

Η μέθοδος *tunneling* είναι μια γνωστή μέθοδος για να κρύψει κάποιος τις επικοινωνίες του. Με τη μέθοδο αυτή ένα πακέτο ενθυλακώνεται στο ωφέλιμο φορτίο ενός άλλου πακέτου. Το εξωτερικό πακέτο είναι το όχημα για τη μεταφορά μέσα στο δίκτυο. Ο

παραλήπτης απλά πρέπει να βγάλει το εσωτερικό πακέτο το οποίο μεταφέρεται στο δίκτυο χωρίς να αλλοιωθεί. Το εξωτερικό πακέτο είναι συνήθως ένα πακέτο *IP* για δρομολόγηση μέσα στο διαδίκτυο. Επίσης συχνά χρησιμοποιούνται *ICMP* και *HTTP* μηνύματα. **[4]**

2.2 *Malware* – Μια απειλή που Εξελίσσεται

Το κακόβουλο λογισμικό (*malware*), όπως είναι οι ιοί (*worm, virus, trojan horse*) συγκαταλέγεται στις περισσότερο αναγνωρίσιμες απειλές για τα υπολογιστικά συστήματα. Το κακόβουλο λογισμικό υπήρξε το μεγαλύτερο πρόβλημα ασφάλειας για τους προσωπικούς υπολογιστές, και συνέχισε να είναι από τότε που το διαδίκτυο υιοθετήθηκε μαζικά στα μέσα της δεκαετίας του 1990. Ωστόσο, η αρχή του προβλήματος του κακόβουλου λογισμικού ξεκίνησε πολύ πιο πριν. Για παράδειγμα, αν και οι αρχικές ρίζες των προγραμμάτων *trojan horse* είναι άγνωστες, η άφιξη των ιών (*worm, virus*) μπορεί να συνδεθεί με την αρχική ιδέα των αυτό-επαναλαμβανόμενων συστημάτων, όπως ήταν τα κυψελωτά αυτόματα *(cellular automata, von Neumann, 1948)*. Αυτού του είδους τα αυτόματα, εισάγουν την ιδέα ότι η πληροφορία μπορεί να κωδικοποιηθεί με απλούς κανόνες έτσι ώστε να είναι δυνατόν να επαναληφθεί και να διασκορπισθεί στο σύστημα. Αυτή η ιδέα χρησιμοποιήθηκε από τους *Watson* και *Crick* όταν, πέντε χρόνια μετά, δημοσίευσαν τη δομή του *DNA*, το μόριο το οποίο κωδικοποιεί την πληροφορία και χρησιμοποιείται για να επαναλάβει τις οργανικές μορφές της ζωής. Μετά από 30 χρόνια, ο ερευνητής ασφάλειας *Frederick Cohen* πρώτος χρησιμοποίησε τον όρο ***ιός υπολογιστή*** (*computer virus*) για να περιγράψει ένα αυτό-επαναλαμβανόμενο κομμάτι κώδικα μέσα σε ένα πληροφοριακό σύστημα *(Information Technology system, IT system)* (*Cohen, 1994*). Σε μια ενδιαφέρουσα παράλληλη ανάπτυξη το βιβλίο του *Richard Dawkin "The Selfish Gene" (1996),* εισήγαγε την ιδέα ότι όλοι οι ζωντανοί οργανισμοί είναι μαριονέτες αυτό-επαναλαμβανόμενων τμημάτων κώδικα. Αυτές είναι και οι ιδέες που βρίσκονται πίσω από την εξέταση της εξέλιξης της απειλής του κακόβουλου λογισμικού.

2.2.1 Εισαγωγή

Σε γενικό επίπεδο, ο όρος κακόβουλο λογισμικό (*malware*) υποδηλώνει οποιοδήποτε τμήμα κώδικα υπολογιστή που μπορεί να έχει κακόβουλη και ανεπιθύμητη επίδραση σε ένα πληροφοριακό σύστημα *(IT system)* ή σε ένα δίκτυο. Αν και υπάρχουν χιλιάδες παραδείγματα κακόβουλου λογισμικού, οι βασικές κατηγορίες θεωρούνται ότι είναι οι παρακάτω:

- ***Virus:*** Ένα επαναλαμβανόμενο πρόγραμμα το οποίο εισάγεται σε ένα σύστημα μολύνοντας τα φέροντα υλικά, όπως είναι οι δίσκοι, τα αρχεία, τα έγγραφα. Το λογισμικό *virus* είναι δυνατό να μεταφέρει ένα ωφέλιμο φορτίο, το οποίο ενεργοποιείται κάποια στιγμή μετά τη μόλυνση, και προκαλεί ανεπιθύμητα και συχνά καταστροφικά αποτελέσματα. Θα πρέπει να σημειωθεί ότι ο όρος *virus* συχνά χρησιμοποιείται λανθασμένα σαν ένας γενικός όρος για να περιγράψει όλα τα είδη του κακόβουλου λογισμικού.
- ***Worm:*** Αν και μοιράζεται μια επιφανειακή ομοιότητα με το λογισμικό *virus* επειδή επαναλαμβάνεται μέσα στα δικτυακά συστήματα, το λογισμικό *worm* διαφέρει ως προς το ότι μπορεί να εξαπλώνεται αυτόνομα χωρίς να χρειάζεται να μολύνει κάποιο φέρων υλικό του συστήματος. Το λογισμικό *worm* επωφελείται από την δικτυακή σύνδεση μεταξύ των συστημάτων και μπορεί να εξαπλωθεί σαν αποτέλεσμα αυτόνομης δραστηριότητας (όπως η σάρωση τυχαίων διευθύνσεων *IP* και η εκμετάλλευση αδυναμιών ώστε να επιτευχθεί είσοδος σε απομακρυσμένα συστήματα) ή σαν αποτέλεσμα δραστηριότητας ενός χρήστη (όπως ανοίγοντας ένα αρχείο ηλεκτρονικού ταχυδρομείου που είναι κακόβουλο ή κατά την ανταλλαγή αρχείων από σύστημα σε σύστημα).

- ***Trojan Horse*:** Αυτή η κατηγορία του κακόβουλου λογισμικού αναφέρεται σε προγράμματα που ξεγελούν τους χρήστες παριστάνοντας πως έχουν κάποια συγκεκριμένη λειτουργία έτσι ώστε να τα εκτελέσουν, ενώ στην πραγματικότητα κάνουν κάτι άλλο (είτε αντί, είτε επιπλέον της λειτουργίας που διαφημίζουν) και έχουν σαν αποτέλεσμα αναπάντεχα και συχνά ανεπιθύμητα αποτελέσματα.

Υπάρχουν επίσης και πολλοί άλλοι όροι που χρησιμοποιούνται για να περιγράψουν ένα επικίνδυνο και κακόβουλο λογισμικό όπως *backdoors* (θύρες που ανοίγουν από τους επιτιθέμενους για να επιτρέψουν μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα), *trapdoors* (σημεία εισόδου μη εξουσιοδοτημένα, που έχουν αφεθεί από λάθος ανοιχτά από τους προγραμματιστές), *time bombs* (κώδικας που ενεργοποιείται μετά από κάποια χρονική περίοδο ή σε κάποια συγκεκριμένη ημερομηνία), *logic bombs* (κώδικας που ενεργοποιείται από ένα συγκεκριμένο γεγονός ή από μια σειρά γεγονότων που συμβαίνουν σε ένα σύστημα).

Ανεξάρτητα από το όνομά του, το κακόβουλο λογισμικό αποτελεί ένα από τα πιο σημαντικά θέματα ασφάλειας. Στον ***πίνακα 2*** φαίνονται τα αποτελέσματα ερευνών οι οποίες δείχνουν ότι το κακόβουλο λογισμικό αποτελεί την περισσότερο σημαντική κατηγορία περιστατικών.

Πίνακας 2: Αποτελέσματα ερευνών περιστατικών κακόβουλου λογισμικού

Έρευνα	***Κατηγορία***	***Σχετιζόμενη στατιστική***	***Βασική κατηγορία***
KPMG Global Information Security Survey 2002 (KPMG, 2002)	*Περιστατικά ιών*	*61% πάσχουν από παραβάσεις*	*NAI*
DTI Information Security Breaches Survey 2004 (DTI, 2004)	*Μόλυνση από ιούς και διασπαστικό λογισμικό*	*50% των αποδεκτών μολύνθηκαν*	*NAI*
Ernst & Young Global Information Security Survey 2004 (Ernst & Young 2004)	*Virus, Trojan Horse, Internet Worm*	*68% των περιστατικών οδηγούν σε απώλεια διαθεσιμότητας*	*OXI*
CSI/FBI Computer Crime &Security Survey 2005 (Gordon et al. 2005)	*Virus*	*75% των εκτεθειμένων μολύνθηκαν*	*NAI*

Θα πρέπει να σημειώσουμε ότι αν και το κακόβουλο λογισμικό δεν ήταν στην κορυφή των περιστατικών στην έρευνα των *Ernst & Young* (η αποτυχία του υλικού (*hardware)* κατείχε τα πρωτεία, επηρεάζοντας το 72% των ερωτηθέντων), τοποθετήθηκε σαν

πρώτη ανησυχία όταν οι ερωτηθέντες κλήθηκαν να δηλώσουν το θέμα ασφάλειας που τους ανησυχούσε περισσότερο τον επόμενο χρόνο, με το 77% να απαντά καταφατικά.

Όπως θα περίμενε κανείς, το κακόβουλο λογισμικό εκτός από επικρατούσα απειλή είναι και η περισσότερο δαπανηρή. Μια ένδειξη γι' αυτό δίνεται από την έρευνα των *CSI/BI Computer Crime & Security Survey 2005*, στην οποία 639 ερωτηθέντες δήλωσαν απώλειες πάνω από 42,5 εκατομμυρίων δολαρίων εξαιτίας περιστατικών κακόβουλου λογισμικού. Αυτό, τοποθέτησε το κακόβουλο λογισμικό πολύ μπροστά από όλες τις άλλες 12 κατηγορίες παραβιάσεων για τις οποίες οι ερωτηθέντες κλήθηκαν να απαντήσουν (σ' αυτές περιλαμβάνονταν μη εξουσιοδοτημένη πρόσβαση, κλοπή ιδιωτικής πληροφορίας και άρνηση παροχής υπηρεσίας) και αντιπροσώπευσε το ένα τρίτο των απωλειών σε όλη την έρευνα.

Ένα άλλο σημαντικό θέμα, είναι ότι οι χρήστες έχουν πολύ μικρές πιθανότητες να αποφύγουν μια συμπλοκή με κακόβουλο λογισμικό. Ο λόγος οφείλεται σε μεγάλο βαθμό σε ολοένα και πιο εφευρετικούς μηχανισμούς διάδοσης και στη χρήση του διαδικτύου ως μέσου μεταφοράς. Σαν αποτέλεσμα, η διάδοση του κακόβουλου λογισμικού έγινε πιο γρήγορη, πιο εκτενής και επηρέασε πολύ περισσότερους χρήστες. Σαν μια ένδειξη γι' αυτό μπορούμε να θεωρήσουμε τη σημαντική αύξηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου που είναι μολυσμένα με κακόβουλα αρχεία, στην οποία συνέβαλλε σε σημαντικό βαθμό η χρήση του διαδικτύου. Σύμφωνα με μια έρευνα, το 2000, κατά μέσο όρο ένα στα 790 μηνύματα ηλεκτρονικού ταχυδρομείου περιείχε ιό. Η κατάσταση αυτή με τα χρόνια άλλαξε, ώστε το 2004 ένα στα 16 μηνύματα περιείχε ιό. Έτσι, οι πιθανότητες να αποφύγει κάποιος τα μολυσμένα μηνύματα είναι πολύ μικρές.

Είναι φανερό ότι όσοι δημιουργούν το κακόβουλο λογισμικό, πετυχαίνουν μεγαλύτερα επίπεδα επιτυχιών δίνοντας έμφαση στις στρατηγικές ανίχνευσης και προστασίας.

2.2.2 Τα κίνητρα της απάτης

Πριν εξετάσουμε τι μπορεί να κάνει το κακόβουλο λογισμικό, είναι λογικό να εξετάσουμε το ρόλο όσων γράφουν και ελευθερώνουν τέτοιου είδους λογισμικό. Μια εκτίμηση των εξελισσόμενων τεχνικών τους και των κινήτρων τους μπορεί να συμβάλλει στην κατανόηση αυτής της απειλής.

Τυπικά, τα κίνητρα των επιτιθέμενων μπορούν να κατηγοριοποιηθούν σύμφωνα με έναν ή περισσότερους από τους παρακάτω λόγους:

- Να δουν πόσο μπορεί να εξαπλωθεί η δημιουργία τους ή πόση προσοχή μπορεί να προσελκύσει,
- Να προκαλέσουν ζημιά ή αναστάτωση (το κίνητρο θα μπορούσε να είναι εκδίκηση ή ιδεολογία), που μπορεί να πάρει τη μορφή μιας στοχευμένης επίθεσης εναντίον ενός ατόμου, ενός οργανισμού ή ενός συστήματος,
- Να κατακτήσουν το αίσθημα της δύναμης ή της ανωτερότητας απέναντι στα θύματά τους,
- Να χρησιμοποιήσουν το κακόβουλο λογισμικό σαν ένα μέσον για προσωπικό κέρδος,
- Να δώσουν στους χρήστες ένα μάθημα ασφάλειας, προσφέροντας πρακτικά μια επίδειξη αδυναμίας ασφάλειας στους χρήστες και στους παρόχους,
- Να κάνουν ένα πείραμα για να διαπιστώσουν τι μπορούν να πετύχουν με το μοντέρνο λογισμικό, την τεχνολογία δικτύων κ.λπ.

Αν και οι συνεντεύξεις με δημιουργούς κακόβουλου λογισμικού είναι σπάνιες, υπάρχουν κάποια σχόλια δημοσιευμένα που δίνουν μια εικόνα της νοοτροπίας τους. Κάποιοι σύγχρονοι δημιουργοί κακόβουλου λογισμικού ισχυρίζονται ότι ο σκοπός τους είναι να ερευνήσουν την τεχνική σκοπιμότητα νέων προσεγγίσεων, ή να επιδείξουν την αδυναμία των συστημάτων τα οποία στοχεύουν. Για παράδειγμα, σε μια δημοσιευμένη συνέντευξη του δημιουργού ιών *Marek "Benny" Strihavka*, πρώην μέλους της ομάδας 29 A, όταν τέθηκε το ερώτημα για το σκοπό της ομάδας και τα κίνητρά του, απάντησε:

Ο σκοπός της ομάδας 29 A ήταν πάντα η τεχνολογική πρόοδος, η εφεύρεση και η καινοτομία νέων και τεχνικά ώριμων και ενδιαφερόντων ιών… Πάντα προσπαθούσα να φέρω κάτι καινούργιο, που δεν υπήρχε ως τότε. Δημιούργησα λογισμικό ιών για πλατφόρμες που θεωρούνταν ανθεκτικές σε ιούς…. Αυτό δεν είχε να κάνει με κάποιο είδος «κυβερνο-τρομοκρατίας».

Μια περισσότερο άμεση αιτιολόγηση ειπώθηκε από τον *Onel de Guzman*, έναν κατά παραδοχή δημιουργό κακόβουλου λογισμικού ο οποίος ισχυρίστηκε ότι δημιούργησε τον κακόφημο ιό *Loveletter*. Η άποψη του *de Guzman* ήταν ότι θα έπρεπε να κατηγορηθεί η ίδια η *Microsoft* για τα περιστατικά πειρατείας, επειδή ο ιός εκμεταλλεύτηκε μια αδυναμία του ηλεκτρονικού ταχυδρομείου του *Outlook*.

Για προγραμματιστές σαν κι εμάς αυτό δεν είναι λάθος… Είμαι ο χρήστης, αγοράζω το προϊόν. Αν το χρησιμοποιώ με λάθος ή αδόκιμο τρόπο, γιατί πρέπει να κατηγορηθώ εγώ γι' αυτό;

Αντίστοιχα, μπορεί κάποιος να πάρει μια ένδειξη για τα κίνητρα του δημιουργού ενός ιού από μηνύματα τα οποία συνήθως κρύβουν μέσα στις δημιουργίες τους. Δεδομένων των εγωκεντρικών κινήτρων πολλών δημιουργών ιών, μια από τις πιο κοινές μορφές μηνυμάτων σχετίζεται με την καυχησιολογία και την κομπορρημοσύνη για τις ικανότητές τους. Σαν παράδειγμα μπορούμε να θεωρήσουμε το παρακάτω μήνυμα το οποίο μένει στον κατάλογο του συστήματος (*system directory)* στο αρχείο *msg15.txt*, εξ' αιτίας της μόλυνσης με μια παραλλαγή του ιού *Mydoom*.

Ο συγγραφέας αναλαμβάνει την υπηρεσία ασφάλειας του συστήματος (IT security) και θα δουλέψουμε με το Mydoom, με ιούς P2P (peer to peer) και με κώδικες που εκμεταλλεύονται αδυναμίες. Επίσης θα επιτεθούμε στην ασφάλεια των αρχείων (f-secure), στο Symantec, στο mcafee κ.λπ. Η 11η Μαρτίου είναι η μέρα. Πού είναι τώρα το SkyNet? Lol

Στην περίπτωση αυτή, το κείμενο περιγελά τον αντίπαλο ιό *NetSky* (ο συγγραφέας του οποίου αναφέρεται στη δημιουργία του σαν *SkyNet*) και εκπέμπει μια φανερή απειλή στις διάφορες εταιρείες αντιιϊκής προστασίας.

Είναι επίσης σύνηθες στους δημιουργούς ιών να μεταφέρουν μηνύματα τα οποία προσπαθούν να δικαιολογήσουν ή να αποδώσουν κατηγορίες για τις πράξεις τους. Για παράδειγμα, ο κώδικας του ιού *Blaster* τον Αύγουστο του 2003 περιείχε το παρακάτω μήνυμα, το οποίο δεν εμφανιζόταν στην οθόνη:

Θέλω απλά να σου πω ότι Σ' ΑΓΑΠΩ SAN!!

Billy gates γιατί το κάνεις αυτό να συμβαίνει; Σταμάτα να βγάζεις λεφτά και φτιάξε το λογισμικό σου!!

Εντωμεταξύ το ενσωματωμένο μήνυμα στον κώδικα του ιού *Klez*, φαινόταν να είναι μια έκκληση για βοήθεια από τον Οκτώβριο του 2001 και περιείχε το ακόλουθο μήνυμα:

Λυπάμαι που το κάνω αυτό, αλλά δεν έχει και νόημα να ζητάω συγγνώμη.

Θέλω μια καλή δουλειά, γιατί πρέπει να ενισχύσω του γονείς μου.

Τώρα είδατε τις τεχνικές μου δυνατότητες.

Πόσο θα είναι ο ετήσιος μισθός μου; ΟΧΙ περισσότερο από 5.500 $.

Τι πιστεύετε γι' αυτό;

Μη με βρίζετε, δεν έχω καμία εχθρότητα.

Μπορείτε να με βοηθήσετε;

Είναι φανερό από αυτά τα λίγα παραδείγματα ότι τα ισχυριζόμενα κίνητρα μπορεί να διαφέρουν αρκετά. Ωστόσο, μπορούμε να σταχυολογήσουμε ενδείξεις για τα κίνητρα των δημιουργών των ιών, από το τι προσπαθούν να κάνουν με το κακόβουλο λογισμικό. Για παράδειγμα, όπως έδειξαν πρόσφατες συζητήσεις, υπήρξε μια αύξηση στο ποσοστό των ιών που προσπαθούν να ανοίξουν μια θύρα του συστήματος, γεγονός που θα διευκολύνει διάφορες εγκληματικές δράσεις. Συγκεκριμένα, για κάθε σύστημα που εκτίθεται με αυτό τον τρόπο, ο εισβολέας αποκτά ένα εκμεταλλεύσιμο περιουσιακό στοιχείο. Καθώς αυξάνεται ο αριθμός τους, αυτά τα συστήματα αντιπροσωπεύουν έναν τεράστιο πόρο σε όρους συλλογικής υπολογιστικής ισχύος και δικτυακού εύρους ζώνης. Με κακόβουλο λογισμικό που επαναλαμβάνεται με επιτυχία, χιλιάδες προσωπικοί υπολογιστές εκτίθενται, προσδένονται και λειτουργούν σαν εντεταλμένο δίκτυο (*botnet*) κάτω από τον έλεγχο του εισβολέα (σαν παράδειγμα της απειλής, τους πρώτους έξι μήνες του 2004 ο αριθμός των μηχανικών δικτύων (*botnet*) που παρακολουθούνταν από τη *Symantec* αυξήθηκε από τις 2.000 σε περισσότερα από 30.000). Έχοντας αποκτήσει τέτοιους πόρους, οι εισβολείς μπορούν να τους μετατρέψουν σε οικονομικά πλεονεκτήματα με πολλούς τρόπους. Μια καθιερωμένη προσέγγιση είναι η πώληση ή η ενοικίαση του εντεταλμένου δικτύου σε εισβολείς που το χρησιμοποιούν σαν μέσο για να στέλνουν άχρηστα μηνύματα ηλεκτρονικού ταχυδρομείου και για να παρακάμπτουν τις «μαύρες» λίστες των διευθύνσεων *IP*, χρησιμοποιώντας αναφορές που προτείνουν την ενοικίαση με λιγότερο από 100$ την ώρα. Μια άλλη αποδεδειγμένη επιλογή είναι ο εκβιασμός, βασισμένος στην απειλή χρήσης της συλλογικής δύναμης πυρός των εκτεθειμένων συστημάτων να προωθήσουν μια επίθεση κατανεμημένης άρνησης παροχής υπηρεσίας. Σημαντικά θύματα εν προκειμένω, περιλαμβάνουν διαδικτυακά χαρτοπαίγνια, τα οποία έχουν αναφερθεί ότι είναι στόχοι διεκδικήσεων από ρωσικά συνδικάτα οργανωμένου εγκλήματος.

Δυστυχώς, δεν είναι μόνο τα κίνητρα που μπορεί να διαφέρουν. Οι δημιουργοί κακόβουλου λογισμικού έχουν αναπτύξει χιλιάδες τεχνικές για να στοχεύουν και να επιτίθενται σε συστήματα, και αυτές είναι το κλειδί για να εκτιμήσουμε πώς οι απειλές έχουν εξελιχθεί στην τρέχουσα μορφή τους παρά την αυξημένη προσοχή των πιθανών θυμάτων.

2.2.3 Η Εξελισσόμενη Απειλή

Έχοντας τεκμηριώσει την ύπαρξη του προβλήματος του κακόβουλου λογισμικού, θα εξετάσουμε πώς εξελίχθηκε στο χρόνο η φύση της απειλής. Αναφερόμενοι στις κατηγορίες του κακόβουλου λογισμικού, θα εστιάσουμε σε ιούς δηλ. *worm* και *virus*, καθώς αυτά αποτελούν τις μορφές του κακόβουλου λογισμικού που έχουν υποστεί τις

πιο δραματικές αλλαγές. Αν και τα προγράμματα τύπου *trojan horse* εξακολουθούν να έχουν μια σημαντική παρουσία, η φύση της απειλής τους δεν έχει εξελιχθεί θεμελιωδώς- πάντα μπορούσαν να κάνουν σχεδόν οτιδήποτε μπορούσε να γίνει με το λογισμικό (μολονότι ενδεχομένως περιορίζονται από τα δικαιώματα πρόσβασης που έχουν στη διάθεσή τους). Μια από τις πιο αξιοσημείωτες αλλαγές αποτελεί η οδός μέσω της οποίας μπορούν να εισέλθουν σε ένα σύστημα. Ενώ η εγκατάσταση του λογισμικού *trojan horse* παλαιότερα γινόταν μηχανικά από έναν χρήστη υπεράνω υποψίας, σήμερα οι ιοί τύπου *worm* χρησιμοποιούνται συχνά σαν μηχανισμοί για να τα ρίχνουν μέσα στα συστήματα με αυτοματοποιημένο τρόπο. Έτσι η πραγματική αλλαγή μπορεί να αποδοθεί στην εξέλιξη των τεχνικών των ιών τύπου *worm*.

Κοιτάζοντας την ιστορία των ιών (*worm, virus*) αποκαλύπτεται μια καθαρή εξέλιξη όσον αφορά στη σχετιζόμενη μόλυνση και στους μηχανισμούς διάδοσης, όπως και στα αποτελέσματα στα συστήματα που στοχεύουν. Εκτός από μια βαθύτερη ριζική αλλαγή, που μετακίνησε τον τρόπο διάδοσης του κακόβουλου λογισμικού από την ανταλλαγή δίσκων στη χρήση του διαδικτύου, τα τελευταία χρόνια υπάρχουν κάποιες φάσεις των τρόπων μόλυνσης που ξεχωρίζουν:

- **Αρχές του 1990:** βασίστηκε σε ανθρώπους που αντάλλασαν δίσκους στα συστήματα για τη διάδοση των ιών των αρχείων,
- **Μέσα του 1990:** μετακίνηση προς μακρο-ιούς, που έδωσε τη δυνατότητα στο κακόβουλο λογισμικό να ενσωματωθεί σε αρχεία που είχαν μεγάλες πιθανότητες να ανταλλαγούν μεταξύ των χρηστών,
- **Τέλη του 1990:** εμφάνιση της αυτοματοποιημένης λειτουργίας μαζικού ηλεκτρονικού ταχυδρομείου, αφαιρώντας την εξάρτηση από τους χρήστες για να μεταφέρουν τα μολυσμένα αρχεία,
- **Σήμερα:** αποφεύγεται η ανάγκη να κοροϊδέψουν ένα χρήστη για να ανοίξει το μολυσμένο αρχείο ενός ηλεκτρονικού μηνύματος, με την αξιοποίηση αδυναμιών που επιτρέπουν τη μόλυνση χωρίς τη μεσολάβηση του χρήστη.

Ωστόσο το πρόβλημα του κακόβουλου λογισμικού συναντιέται πολύ παλιότερα. Για παράδειγμα, το πρώτο γνωστό περιστατικό ιού μπορεί να ανιχνευθεί το 1982, με την απελευθέρωση του *ElkCloner* στα συστήματα *Apple II*. Γραμμένο από τον 15-χρονο *Richard Skrenta*, το πρόγραμμα έμοιαζε με τους ιούς που θα ακολουθούσαν: διαδιδόταν μεταξύ των μηχανημάτων μολύνοντας τις δισκέττες (*floppy disk*) και φορτώνονταν στη μνήμη όποτε ένα σύστημα αρχικοποιούνταν από μια μολυσμένη δισκέττα. Μετά από την 50-κοστή αρχικοποίηση αυτού του είδους ο ιός εμφάνιζε το παρακάτω μήνυμα:

Elk Cloner: The program with a personality – ElkCloner: Το πρόγραμμα με προσωπικότητα

It will get on all your disks – Θα μπει σε όλους τους δίσκους σας

It will infiltrate your chips – θα διεισδύσει σε όλα τα chips σας

Yes, it's Cloner

It will stick to you like glue – Θα κολλήσει πάνω σας σαν κόλλα

It will modify ram too – Θα τροποποιήσει και τη ram

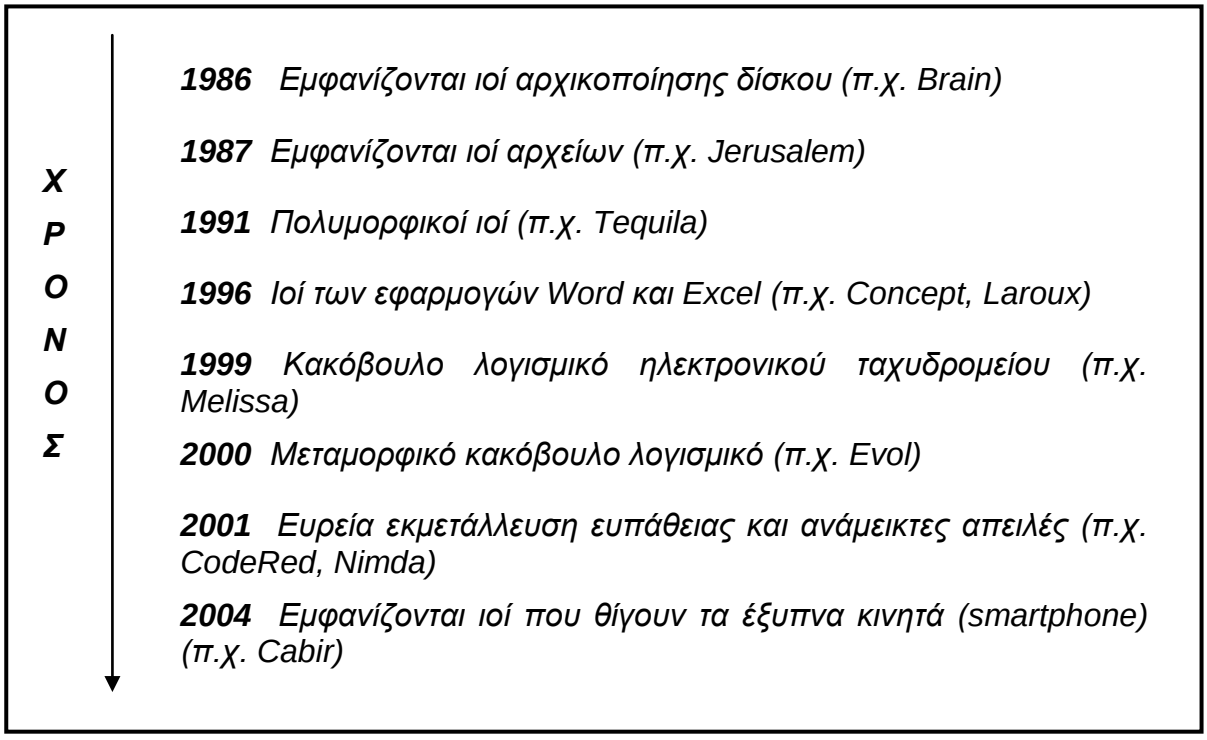
Send in the Cloner! – Στείλτε τον Cloner!

Εκτός από αυτή την ενόχληση, ο ιός *ElkCloner* δεν έκανε τίποτα άλλο για να αναστατώσει το χρήστη ή για να βλάψει το σύστημα (αν και υπήρχε ενδεχόμενο να καταστραφούν τα δεδομένα αν το πρόγραμμα προσπαθούσε να γραφτεί σε ένα δίσκο που δεν περιείχε το λειτουργικό σύστημα).

Αν και σήμερα αναφέρεται σαν ιός, αυτός ο όρος δεν είχε επινοηθεί στις μέρες του *ElkCloner*. Ήταν μόλις μετά από δύο χρόνια που η συμπεριφορά αυτού του τύπου λογισμικού ονομάστηκε από τη μελέτη του *Fred Cohen* με τίτλο «Ιοί Υπολογιστών-Θεωρία και Πειραματισμοί» (*Cohen, 1984*).

Ο όρος ιός σήμερα χρησιμοποιείται γενικευμένα για να περιλάβει όλα τα είδη του κακόβουλου λογισμικού, και μαζί με τους εισβολείς η απειλή του ιού είναι το θέμα ασφάλειας που έχει εισδύσει περισσότερο στο μυαλό των χρηστών. Πράγματι, αν και άλλοι τύποι κακόβουλου λογισμικού όπως τα *worm* και τα *trojan horse* είχαν προκύψει πολύ πριν τη μελέτη του *Cohen*, ήταν από αυτή τη μελέτη που η βιολογική αναλογία προέκυψε και αυτή υπήρξε η διαρκής συνεισφορά στον τρόπο που οι επόμενες μελέτες αντιμετώπισαν το κακόβουλο λογισμικό.

Στο παρακάτω ***σχήμα*** φαίνεται το χρονικό μερικών από τα πιο σημαντικά δημιουργήματα κακόβουλου λογισμικού από τις ημέρες του *ElkCloner* και της μελέτης του *Cohen*.



Σχήμα 6: Η εξέλιξη των ιών *(virus, worm)*

Θα πρέπει να σημειωθεί, ότι το τελευταίο πεδίο δηλώνει την εμφάνιση του κακόβουλου λογισμικού σε μια νέα πλατφόρμα, αντανακλώντας τις αυξημένες δυνατότητες των συσκευών κινητής τηλεφωνίας και ως εκ τούτου την παρουσία τους σαν πρόκληση για τους δημιουργούς κακόβουλου λογισμικού.

Στις δύο δεκαετίες από τότε που η μελέτη του *Cohen* υποδήλωσε την πιθανή απειλή, ο κίνδυνος που περιέγραψε εμφανίστηκε και γιγαντώθηκε. Ωστόσο, αν και υπάρχουν

χιλιάδες προσπάθειες εισβολής, θα πρέπει να τονίσουμε ότι δεν θέτουν όλες ισοδύναμη απειλή. Πράγματι, σε ορισμένες περιπτώσεις, νέο κακόβουλο λογισμικό αναγνωρίζεται και περιέχεται στα προϊόντα των εργαστηρίων αντιιϊκών προγραμμάτων, πριν προλάβει να βλάψει και να διαδοθεί. Επίσης, παλαιότεροι τύποι απειλής τελικά αποδυναμώνονται σαν αποτέλεσμα ανίχνευσης και εξάλειψης από το αντιιϊκό λογισμικό. Έτσι, από τους χιλιάδες τύπους γνωστών εισβολών, μόνο ένα ποσοστό αντιπροσωπεύει μια ενεργή απειλή σε κάθε εποχή. Τέτοιου είδους κακόβουλο λογισμικό ορίζεται ως «σε άγρια κατάσταση», και η έκταση του προβλήματος μπορεί να υπολογιστεί από τον οργανισμό *The WildList Organization*, που συντάσσει μια μηνιαία λίστα βασισμένη σε αναφορές έγκυρων ερευνητών αντιιϊκών και οργανισμών από όλο τον κόσμο. Η κατάταξη αποδίδεται σε έναν ιό, αν επαληθευμένα έχει παρουσιαστεί σε δύο ή περισσότερους ανταποκριτές της λίστας μέσα σε μια συγκεκριμένη περίοδο αναφοράς. Δυστυχώς, αν και αυτή η πρακτική κρατάει τη λίστα σε επίπεδο εκατοντάδων και όχι χιλιάδων αναφερόμενων εισβολών, ο αριθμός τους παραμένει ένα σημαντικό πρόβλημα.

Ένα άλλο σημαντικό στοιχείο εξέλιξης, όπως φαίνεται και στο ***σχήμα 6***, είναι η εμφάνιση των ανάμεικτων απειλών, που συνδυάζουν τα χαρακτηριστικά του κακόβουλου λογισμικού με αδυναμίες του εξυπηρετητή και του διαδικτύου. Σύμφωνα με τον ορισμό του *Symantec*, το κακόβουλο λογισμικό μπορεί να χαρακτηριστεί σαν ***ανάμεικτη απειλή*** αν συνδυάζει δύο ή περισσότερα από τα παρακάτω χαρακτηριστικά:

- Να προκαλέσει ζημιά (π.χ. να δρομολογήσει επίθεση άρνησης παροχής υπηρεσίας, να εγκαταστήσει ένα *trojan horse* για μελλοντική χρήση),
- Να διαδοθεί μέσω διάφορων μεθόδων (π.χ. με μαζικές αποστολές ηλεκτρονικών μηνυμάτων, μολύνοντας τους επισκέπτες των εκτεθειμένων ιστοσελίδων),
- Να έχει πολλά σημεία επίθεσης (π.χ. προσθέτοντας κώδικα σε αρχεία *HTML (Hypertext Markup Language)*, μολύνοντας τα αρχεία τύπου *.exe*, κάνοντας αλλαγές στις εγγραφές),
- Να διαδίδεται αυτόματα (π.χ. με σάρωση του διαδικτύου και άλλων προσπελάσιμων δικτύων με αδύναμα συστήματα),
- Να εκμεταλλεύεται αδυναμίες (π.χ. υπερχείλιση μνήμης, απουσία κωδικών, αδυναμίες επικύρωσης δεδομένων *HTTP*).

Οι περισσότεροι τύποι κακόβουλου λογισμικού που εμφανίστηκαν από το 2000 και μετά έχουν τα χαρακτηριστικά της ***ανάμεικτης απειλής*** και ο αποτελεσματικός συνδυασμός τεχνικών είναι υπεύθυνος για την παρατηρημένη έξαρση στον όγκο και στο κόστος των περιστατικών.

Έχοντας αποδείξει ότι η φύση της απειλής έχει εξελιχθεί, αξίζει να μελετήσουμε περισσότερο την συμπεριφορά του κακόβουλου λογισμικού. Εν προκειμένω, σημαντικά σημεία είναι τα εξής:

- ***Η διάδοση*****:** Πώς εξαπλώνεται το κακόβουλο λογισμικό,
- ***Το ωφέλιμο φορτίο*****:** Τι προκαλεί σε ένα μολυσμένο στόχο,
- ***Η συντήρηση*****:** Πώς διατηρεί την ύπαρξή του.

Αν και τα αναφέραμε σαν ξεχωριστά σημεία, υπάρχει κάποιες φορές η πιθανότητα να αντιληφθούμε μια επικάλυψη μεταξύ αυτών των στοιχείων (π.χ. σαν αποτέλεσμα της διαδικασίας διάδοσης μπορεί να προκληθούν επιβλαβείς συνέπειες και να θεωρηθούν

ως ωφέλιμο φορτίο του κακόβουλου λογισμικού). Τα τρία αυτά στοιχεία θα αναλυθούν πιο κάτω.

2.2.3.1 Μηχανισμοί Διάδοσης

Όλα τα είδη κακόβουλου λογισμικού χρειάζονται κάποιο τρόπο για να εισέλθουν στο σύστημα του θύματος. Στην περίπτωση των ιών (*virus, worm*), η ικανότητα διάδοσης είναι σύμφυτη με την λειτουργικότητά τους, με την αντιγραφή τους μέσα στο ίδιο σύστημα ή μεταξύ των συστημάτων να αποτελεί το κλειδί για περαιτέρω μολύνσεις. Γενικά, μια ποικιλία από τεχνικές μπορούν να χρησιμοποιηθούν και οι καθιερωμένες μέθοδοι περιλαμβάνουν:

- Μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (σε κάποιες περιπτώσεις η συγκομιδή των διευθύνσεων ηλεκτρονικού ταχυδρομείου γίνεται από το σύστημα του θύματος),
- Εκμετάλλευση αδυναμιών,
- Επιλογή και χρήση μη προστατευμένων κοινών δικτυακών τμημάτων,
- Επιλογή χρηστών κοινωνικής μηχανικής που φορτώνουν ή τρέχουν το κακόβουλο λογισμικό στο σύστημά τους.

Όταν λαμβάνουμε υπόψη τους πιθανούς φορείς μόλυνσης, είναι σημαντικό να αναγνωρίζουμε ότι οι δημιουργοί κακόβουλου λογισμικού είναι πιστοί οπαδοί της μόδας – τουλάχιστον όσον αφορά στο να παρακολουθούν τις τεχνολογίες που χρησιμοποιούν οι άλλοι, και μετά κάνοντας πειρατεία στις πιο δημοφιλείς να τις χρησιμοποιούν σαν πλατφόρμες για να αναπτύξουν νέο κακόβουλο λογισμικό. Κάποια σημαντικά παραδείγματα γι' αυτό περιλαμβάνουν:

- ***Ηλεκτρονικό Ταχυδρομείο***: Από τα τέλη του '90, το ηλεκτρονικό ταχυδρομείο αποδείχτηκε ότι είναι μια εξαιρετικά δυνατή μέθοδος διανομής του κακόβουλου λογισμικού. Αν και αρχικά ήταν ένας ακόμα τρόπος με τον οποίο οι ανύποπτοι χρήστες μπορούσαν να ανταλλάξουν αρχεία μολυσμένα με μακρο-ιούς, η χρήση του ηλεκτρονικού ταχυδρομείου συνδυάστηκε γρήγορα με αυτοματοποιημένα χαρακτηριστικά και λογισμικό ώστε να κάνει δυνατή τη μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε πολλούς παραλήπτες και να κάνει αποτελεσματική την ακαριαία και καθολική διανομή. Από τα πολλαπλά παραδείγματα που μπορούν να παρατεθούν, περιστατικά ορόσημο που χρησιμοποίησαν αυτή την τεχνική περιλαμβάνουν τον *Melissa* (έναν μακρο-ιό της εφαρμογής *Word 97*) το 1999, και τον *LoveLetter* (έναν ιό *worm* βασισμένο σε ένα κακόβουλο λογισμικό της *Visual Basic*) τον επόμενο χρόνο. Μια συνέπεια της μαζικής αποστολής μολυσμένων αρχείων με μηνύματα ηλεκτρονικού ταχυδρομείου, είναι η καθιερωμένη πια συμβουλή προς τους χρήστες να είναι ιδιαίτερα προσεκτικοί και καχύποπτοι όταν λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν αρχεία.
- ***Δίκτυα Ομότιμων (Peer-to-Peer)****:* Στις αρχές του 2000 γίναμε μάρτυρες της διαδεδομένης εμφάνισης και δημοτικότητας των δικτύων *Peer-to-Peer* (*P2P)*, βασισμένων σε λογισμικό όπως το *KaZaA* και το *Morpheus*, τα οποία έγιναν ιδιαίτερα σημαντικά σαν πηγές παράνομου λογισμικού, μουσικών και άλλων πειρατικών αρχείων μέσων διασκέδασης. Με χιλιάδες χρήστες να έχουν προσελκυστεί από αυτά τα δίκτυα, αυτά τελικά έγιναν ένας φυσικός στόχος του κακόβουλου λογισμικού του οποίου οι δημιουργοί συνειδητοποίησαν ότι τα δίκτυα *P2P* μπορούσαν να χρησιμοποιηθούν σαν κανάλια διανομής

συγκαλύπτοντας το κακόβουλο λογισμικό σαν άλλο περιεχόμενο και έτσι ξεγελώντας τους χρήστες και κάνοντάς τους να το φορτώσουν στον υπολογιστή τους νομίζοντας ότι είναι κάτι άλλο. Παραδείγματα που έχουν χρησιμοποιήσει την διανομή αρχείων *P2P* ως όχημα, περιλαμβάνουν τους ιούς *worm Benjamin, Kwbo, t* και *Mant*.

- ***Υπηρεσία Άμεσων Μηνυμάτων* (*Instant Messaging, IM*)**: Η υπηρεσία άμεσων μηνυμάτων (*IM*) έγινε μια δημοφιλής εφαρμογή τελικού χρήστη τόσο στο οικιακό όσο και στο επαγγελματικό πεδίο, κάνοντας δυνατή τη συνομιλία αλλά και την επαφή και ανταλλαγή πληροφοριών μέσα στους οργανισμούς. Από την πλευρά του κακόβουλου λογισμικού, άνοιξε ένα νέο κανάλι προς τα συστήματα των χρηστών και τα δίκτυα των οργανισμών. Παραδείγματα ιών *worm* βασισμένων στην υπηρεσία άμεσων μηνυμάτων περιλαμβάνουν το *Choke* και το *Kelvir*, τα οποία στόχευσαν το *Microsoft MSN Messenger*.
- ***Σελίδες Δικτύωσης (Blog)***: Καθώς αυξήθηκε η δημοτικότητα των σελίδων δικτύωσης, οι εισβολείς θέσπισαν ψεύτικες σελίδες δικτύωσης, στις οποίες τα συστήματα των επισκεπτών εκτίθενται σε κίνδυνο κακόβουλου λογισμικού. Οι χρήστες δελεάζονται από τους τίτλους και τα διαφημιζόμενα περιεχόμενα για να επισκεφτούν αυτές τις σελίδες δικτύωσης και όταν το κάνουν καθιστούν τα συστήματά τους ευάλωτα στο κακόβουλο λογισμικό το οποίο μπορεί να περιέχει η σελίδα.

Όλα τα παραπάνω, απεικονίζουν την καιροσκοπική φύση των δημιουργών κακόβουλου λογισμικού και το γεγονός ότι είναι προσαρμοσμένοι στο να βρίσκουν νέους τρόπους για να ξεγελούν τα θύματά τους. Πράγματι, σε ότι θα μπορούσε να θεωρηθεί ως ευφυία και αναισθησία, οι δημιουργοί του κακόβουλου λογισμικού έχουν επίσης εντοπίσει την ευκαιρία να χρησιμοποιούν την κακή φήμη των δημιουργημάτων τους σαν ένα επιπλέον μέσο για να τα καθιστούν ικανά να διαδίδονται. Καιροφυλακτώντας με τις ανησυχίες των χρηστών μπροστά στην απειλή, το κακόβουλο λογισμικό συχνά φτάνει μασκαρεμένο σαν ενημέρωση ασφάλειας, ειδοποίηση εναντίον ενός ιού, ή σαν εργαλείο που μπορεί να εξολοθρεύσει μια απειλή που είναι πολύ δημοφιλής. Τυπικά παραδείγματα περιλαμβάνουν, τους ιούς *worm Gibe* και *Qint*, που εμφανίστηκαν και οι δύο σαν μηνύματα προερχόμενα από τη *Microsoft*, μεταφέροντας ψεύτικα αρχεία τα οποία υποτίθεται ότι ήταν λογισμικό ασφάλειας.

2.2.3.2 Πιθανότητες Ωφέλιμου Φορτίου

Ο όρος ***ωφέλιμο φορτίο*** *(payload)* αναφέρεται στο τι μπορεί να κάνει το κακόβουλο λογισμικό όταν ενεργοποιηθεί. Θεωρητικά, θα μπορούσε να είναι οτιδήποτε μπορεί να γίνει με τον έλεγχο του λογισμικού. Ωστόσο, στην πραγματικότητα τα ωφέλιμα φορτία του κακόβουλου λογισμικού έτειναν να ακολουθούν έναν αριθμό από αναγνωρίσιμα θέματα, με κάποια κοινά και δημοφιλή αποτελέσματα όπως η διαγραφή ή μετατροπή αρχείων, η υποβίβαση των επιδόσεων του συστήματος, η αστάθεια του συστήματος και η έκθεση σε κίνδυνο της ασφάλειας δημιουργώντας θύρες που παραβιάζονται ή αποκαλύπτοντας εμπιστευτικές πληροφορίες.

Όλα τα είδη κακόβουλου λογισμικού επηρεάζουν την ακεραιότητα του μολυσμένου συστήματος, αφού και μόνο η παρουσία του κάνει μια αλλαγή στην κατάσταση νομιμότητας. Ιδιαίτερα οι μολύνσεις από ιούς έχουν σαν αποτέλεσμα την μη εξουσιοδοτημένη μετατροπή του φορέα του συστήματος (π.χ. ένα πρόγραμμα εκτελέσιμο, ένα αρχείο ή έναν τομέα του δίσκου αρχικοποίησης). Ωστόσο, εκτός από αυτά, μπορεί να υπάρχουν περισσότερες και πιο ουσιώδεις επιρροές στην ακεραιότητα του συστήματος, όπως η μεταβολή ή η καταστροφή των δεδομένων και η καταστροφή

της λειτουργίας του συστήματος. Επιπλέον, οι δράσεις του ωφέλιμου φορτίου μπορούν να επηρεάσουν και τις κεντρικές ιδιότητες ασφάλειας του συστήματος, όπως την εμπιστευτικότητα (π.χ. κλέβοντας ή αποκαλύπτοντας πληροφορίες) και την διαθεσιμότητα (π.χ. παρεμποδίζοντας ή απαγορεύοντας την πρόσβαση στο σύστημα ή στα δεδομένα του σε νόμιμες οντότητες). Μερικά παραδείγματα του εύρους των πιθανών δραστηριοτήτων του ωφέλιμου φορτίου αναφέρονται στον ***πίνακα 3***, μαζί με την ένδειξη των περιοχών ασφάλειας που αυτές οι δραστηριότητες εκθέτουν σε κίνδυνο. Η λίστα αυτή αναφέρει τις καθιερωμένες δραστηριότητες που έχουν ανιχνευθεί σε πολυάριθμες περιπτώσεις κακόβουλου λογισμικού.

Πίνακας 3: Παραδείγματα ωφέλιμου φορτίου κακόβουλου λογισμικού και των απειλών τους

Ωφέλιμο φορτίο	***Εμπιστευτικότητα***	***Ακεραιότητα***	***Διαθεσιμότητα***
Παραβίαση θύρας	*ΝΑΙ*	*ΝΑΙ*	*ΟΧΙ*
Keystroke logging	*ΝΑΙ*	*ΟΧΙ*	*ΝΑΙ*
Καταστροφή του BIOS (Basic Input Output System)	*ΟΧΙ*	*ΝΑΙ*	*ΝΑΙ*
Καταστροφή δεδομένων και αρχείων	*ΟΧΙ*	*ΝΑΙ*	*ΝΑΙ*
Εγκατάσταση άρνησης παροχής υπηρεσίας	*ΟΧΙ*	*ΟΧΙ*	*ΝΑΙ*
Ενοχλητικές επιπτώσεις και μηνύματα	*ΟΧΙ*	*ΝΑΙ*	*ΝΑΙ*
Απατεωνίστικα μηνύματα ηλεκτρονικού ταχυδρομείου	*ΟΧΙ*	*ΝΑΙ*	*ΟΧΙ*
Απενεργοποίηση αντιιϊκού λογισμικού	*ΟΧΙ*	*ΝΑΙ*	*ΟΧΙ*
Εγκατάσταση trojan horse	*ΟΧΙ*	*ΝΑΙ*	*ΟΧΙ*

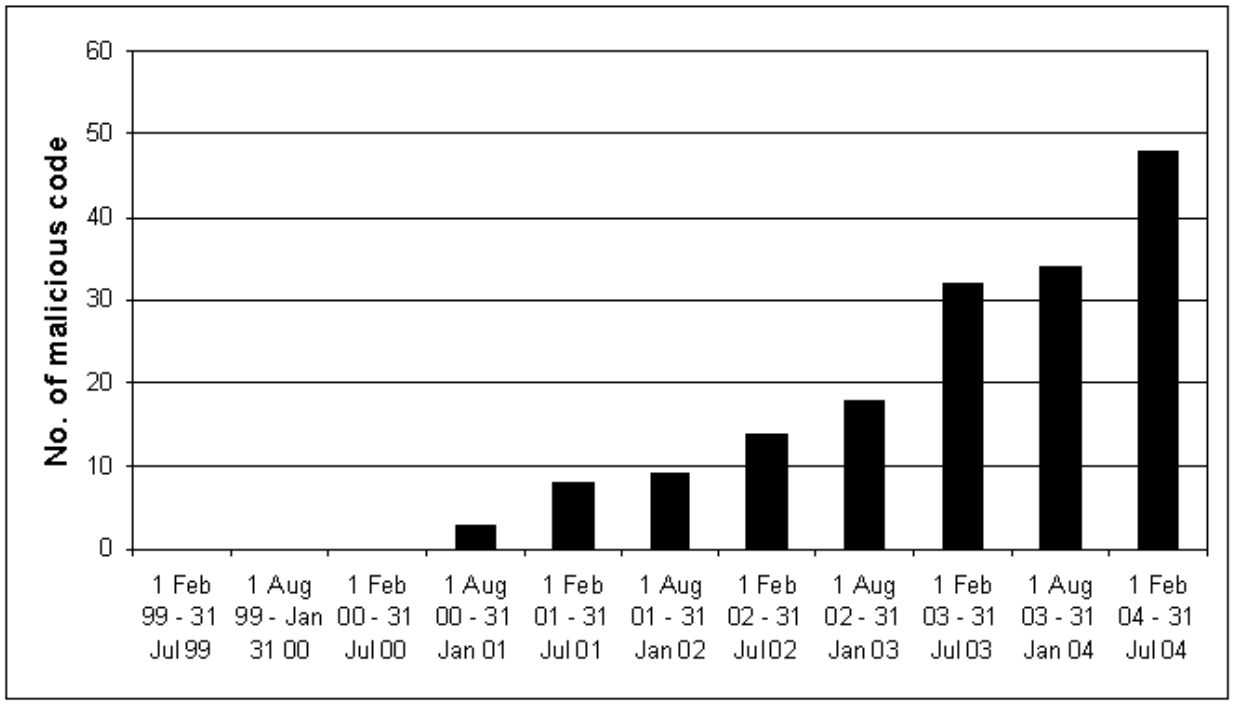
Υπάρχουν βεβαίως και επιπλέον επιπτώσεις που μπορεί να προκύψουν σαν συνέπεια των αποτελεσμάτων του ωφέλιμου φορτίου, όπως αποδιοργάνωση δραστηριοτήτων και οικονομικό κόστος σχετιζόμενο με την απώλεια δεδομένων και την αναδιοργάνωση του συστήματος. Επίσης μπορούν να υπάρχουν επιδράσεις και πέραν του μολυσμένου συστήματος. Για παράδειγμα, όπως ακριβώς προκαλεί άρνηση παροχής υπηρεσίας σε έναν τοπικό χρήστη, το ωφέλιμο φορτίο μπορεί να επηρεάσει το σύστημα ώστε να εγκαταστήσει άρνηση παροχής υπηρεσίας προς έναν απομακρυσμένο χρήστη.

Όταν αναλύουμε το κακόβουλο λογισμικό, η κατανόηση του ωφέλιμου φορτίου αποτελεί ένα σημαντικό βήμα προς την κατανόηση της απειλής. Από την άλλη μεριά, ένα ωφέλιμο φορτίο δεν είναι πάντοτε παρόν- κι αυτή είναι μια πολύ συχνή κατάσταση όταν

έχει ως στόχο να παρέχει απόδειξη της έννοιας για νέο μηχανισμό διάδοσης. Δυστυχώς, αυτό σημαίνει επίσης ότι η απειλή εξακολουθεί να υφίσταται. Ένα πολύ καλό παράδειγμα μπορεί να δοθεί από την περίπτωση του ιού *worm Slammer*, ο οποίος εμφανίστηκε τον Ιανουάριο του 2003 και διαδόθηκε στα συστήματα εκμεταλλευόμενος μια γνωστή αδυναμία του λογισμικού των *Microsoft SQL Server 2000* και *Microsoft SQL Server Desktop Engine (MSDE) 2000*. Παρά την απουσία ωφέλιμου φορτίου, ο ιός ήταν αρκετά ικανός να προκαλέσει σε σημαντικό βαθμό αναστάτωση σαν αποτέλεσμα της ταχύτητας διάδοσής του και της απορρέουσας κυκλοφορίας που δημιούργησε στα εκτεθειμένα συστήματα μέσα στο διαδίκτυο. Στα αποτελέσματα μπορούμε να περιλάβουμε την κατάρρευση του δικτύου τηλεπικοινωνιών της Νότιας Κορέας, την αποδιοργάνωση 13.000 μηχανημάτων ανάληψης χρημάτων της *Bank of America* και την βλάβη σε πέντε από τους δεκατρείς εξυπηρετητές ονομάτων βάσης του διαδικτύου. Γενικά, οι παρενέργειες του ιού εκτιμάται ότι κόστισαν μεταξύ 950 εκ. $ και 1,2 δις. $ σε χαμένη παραγωγικότητα.

Αν και τα παλαιότερα προγράμματα ήταν συχνά καταστρεπτικά, μια βασική διαφορά με τα σημερινά κακόβουλα λογισμικά είναι ότι ακόμα και όταν το ωφέλιμο φορτίο ενεργοποιείται, οι χρήστες παραμένουν επιλήσμονες. Πράγματι, ενώ η αντίληψη για το κακόβουλο λογισμικό των περισσότερων χρηστών εξακολουθεί να βασίζεται στην ιδέα ότι είναι κάτι που μολύνει το σύστημα και μετά αναστατώνει τις λειτουργίες ή καταστρέφει τα δεδομένα με κάποιο τρόπο, είναι σημαντικό να αναγνωρίσουμε ότι η πραγματική απειλή συχνά δεν βρίσκεται στην αρχική μόλυνση αλλά σ' αυτό που αφήνει πίσω της. Αντί να διαλύσει το σύστημα, μια ολοένα και πιο συχνή πρακτική είναι να ανοίγει μια θύρα (*backdoor*) έτσι ώστε να μπορέσει να εκμεταλλευτεί το σύστημα με πολλούς ύπουλους τρόπους.

Επιπλέον, η αυξανόμενη τάση που παρατηρείται να μην περιέχει το κακόβουλο λογισμικό καταστρεπτικό ωφέλιμο φορτίο φαίνεται στο ***σχήμα 7***, το οποίο παρουσιάζει ανά έξι μήνες συνολικά τα νέα λογισμικά που παρουσιάζονται και δεν περιέχουν καταστρεπτικό ωφέλιμο φορτίο (δηλ. αυτά που ανοίγουν κάποια θύρα – *backdoor*, ή δεν έχουν φανερή λειτουργικότητα στο ωφέλιμο φορτίο) και επίσης τα ποσοστά που αυτά τα λογισμικά αντιπροσωπεύουν στις εμφανίσεις κακόβουλου λογισμικού γενικά. Αν και τα είδη που προκαλούν καταστροφές κυριαρχούν στο σύνολο, το ποσοστό των μη καταστρεπτικών κακόβουλων λογισμικών είναι σημαντικό και επίσης ολοένα αυξάνεται.



Σχήμα 7: Η αυξητική τάση του μη καταστρεπτικού κακόβουλου λογισμικού

Η φύση της δράσης του ωφέλιμου φορτίου και το σημείο στο οποίο ενεργοποιείται αποτελούν σημαντικά χαρακτηριστικά στον καθορισμό της διάρκειας ζωής του κακόβουλου λογισμικού μέσα στο σύστημα πριν ανακαλυφθεί. Αν το ωφέλιμο φορτίο είναι ιδιαίτερα ακραίο, ακόμα κι ένας χρήστης χωρίς αντιιϊκή προστασία θα τεθεί σε συναγερμό από το πρόβλημα και αν η δράση είναι καταστρεπτική και αχρηστεύσει το σύστημα (π.χ. καταστρέφοντας το *BIOS* όπως ο ιός *CIH-Chernobyl*), τότε χάνεται η ευκαιρία για περαιτέρω επανάληψη αν το κακόβουλο λογισμικό είναι ιός – *worm* ή *virus*. Όμοια, αν το ωφέλιμο φορτίο ενεργοποιείται πολύ γρήγορα μετά τη μόλυνση, επιπλέον ευκαιρίες για διάδοση μπορεί να χαθούν. Έτσι η ικανότητα να προστατέψει την ύπαρξή του αποτελεί ένα σημαντικό συστατικό του κακόβουλου λογισμικού.

2.2.3.3 Τεχνικές Αυτοσυντήρησης

Ένα από τα επιθυμητά χαρακτηριστικά του κακόβουλου λογισμικού είναι να είναι δύσκολο να ανακαλυφθεί και να καταστραφεί. Κυνηγώντας αυτό το στόχο, οι δημιουργοί του κακόβουλου λογισμικού έχουν επινοήσει έναν αριθμό από τεχνικές σχεδιασμένες για να αποκρύπτουν τα δημιουργήματά τους μέσα σε ένα σύστημα και να περιπλέκουν το έργο των αντιιϊκών πακέτων.

- **Λαθραίες Τεχνικές:** Το κακόβουλο λογισμικό μπορεί να χρησιμοποιήσει λαθραίες μεθόδους για να κρύψει τις αποδείξεις της ύπαρξής του, και να αυξήσει τις πιθανότητες να μην αποκαλυφθεί. Για παράδειγμα, αν ένας ιός έχει μολύνει ένα εκτελέσιμο πρόγραμμα, σαν αποτέλεσμα θα αλλάξει αναπόφευκτα το μέγεθος του μολυσμένου αρχείου. Αυτό μπορεί να πραγματοποιηθεί αν ο ιός αναχαιτίζει τις αιτήσεις που γίνονται για την πρόσβαση του δίσκου.
- ***Πολυμορφισμός:*** Το πολυμορφικό κακόβουλο λογισμικό έχει σχεδιαστεί για να περιπλέκει το έργο των αντιιϊκών πακέτων. Αναγνωρίζοντας ότι η βασική μέθοδος που χρησιμοποιείται από μηχανές ανίχνευσης είναι το ταίριασμα της υπογραφής, το πολυμορφικό κακόβουλο λογισμικό κρυπτογραφεί τον εαυτό του διαφορετικά για κάθε μόλυνση, έτσι ώστε να αποφεύγει να αφήνει μια

σταθερή και ανιχνεύσιμη υπογραφή. Ένα μικρό κομμάτι του κώδικα αποκρυπτογραφεί τα υπόλοιπα όταν το κακόβουλο λογισμικό ενεργοποιηθεί. Αυτή η τακτική εμφανίστηκε με τον ιό *Tequila* το 1991 και από τότε έγινε πολύ δημοφιλής.

- ***Μεταμόρφωση:*** Αν και το πολυμορφικό κακόβουλο λογισμικό μπορεί να υιοθετήσει διαφορετικές μεταμφιέσεις, ο βασικός του κώδικας παραμένει ο ίδιος όταν αποκρυπτογραφηθεί. Σε αντίθεση, το μεταμορφικό κακόβουλο λογισμικό έχει την ικανότητα να ξαναγράφει τον εαυτό του, έτσι ώστε οι διαδοχικές μολύνσεις εμπλέκουν πραγματικά ξεχωριστό κώδικα που όμως κάνει την ίδια λειτουργία. Η μεταμορφική μηχανή, αποσυναρμολογεί τον κώδικα, μεταθέτει με κάποιο τρόπο τις εντολές (π.χ. διαιρώντας ή αναδιατάσσοντας τις αρχικές εντολές σε διαφορετικά μέρη του κώδικα, τα οποία συνδέονται με άλματα) και στη συνέχεια επανασυναρμολογεί το αποτέλεσμα για να παράξει τη νέα μορφή του κακόβουλου λογισμικού. Ένα γνωστό παράδειγμα είναι ο ιός *worm Evol* ο οποίος επηρεάζει συστήματα που χρησιμοποιούν διάφορες πλατφόρμες των *Windows*.
- ***Ασφάλεια Επίθεσης:*** Γνωρίζοντας ότι πολλά συστήματα είναι σήμερα εξοπλισμένα με αντιιϊκά πακέτα και άλλες μορφές προστασίας, το κακόβουλο λογισμικό συχνά επιχειρεί μια προληπτική επίθεση εναντίον αυτών των προγραμμάτων. Πολλές τεχνικές έχουν επινοηθεί. Για παράδειγμα ο ιός *worm Gaobot* επιχειρεί να απαγορεύσει την πρόσβαση σε πάνω από 35 ιστοσελίδες που σχετίζονται με την ασφάλεια (και ανήκουν σε εταιρείες όπως *F-Secure, McAfee, Symantec, Sophos, Trend Micro*), έτσι ώστε να εμποδίσει το μολυσμένο σύστημα από το να αποκτήσει τις ενημερώσεις ασφάλειας για την ανίχνευση και την αποπομπή του ιού. Επίσης διατηρεί μια λίστα από 420 και περισσότερες διεργασίες (π.χ. που σχετίζονται με αντιιϊκά πακέτα και με λογισμικό τείχους προστασίας) οι οποίες τερματίζονται αν βρεθεί ότι εκτελούνται στο σύστημα. Εντωμεταξύ, μία από τις παραλλαγές του ιού *worm Beagle* επιχειρεί να διαγράψει μια ποικιλία από αρχεία εγγραφής των *Windows*, ώστε να εμποδίσει να εκτελεστεί το σχετιζόμενο λογισμικό όταν το σύστημα αρχικοποιείται.

2.2.3.4 Παραδείγματα Περιστατικών

Έχοντας αναγνωρίσει διάφορες τεχνικές, θα πρέπει να επισημάνουμε πώς αυτές εκδηλώνονται σε σημαντικές εκρήξεις κακόβουλου λογισμικού. Θα παρουσιάσουμε τα πιο σημαντικά στελέχη κακόβουλου λογισμικού από το 1998 ως το 2004. Όλα αυτά είχαν σαν στόχο το λειτουργικό σύστημα *Windows*, με την πλειοψηφία να επηρεάζει όλες τις εκδόσεις από το *Windows 95* και μετά. Ένας άλλος κοινός παράγοντας όλων των ιών εκτός από τον *CIH* ήταν η δυνατότητα να διαδίδεται μέσα στα συστήματα. Κοιτάζοντας τις εμφανίσεις των ιών στη διάρκεια των χρόνων μπορούμε να παρατηρήσουμε κάποια σημαντικά στοιχεία όσον αφορά στην εξέλιξη των τεχνικών τους. Για παράδειγμα οι αποστολείς μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου εξελίχθηκαν και πέρασαν από τη χρήση του *Outlook* στις δικές τους *SMTP (Simple Mail Transfer Protocol)* μηχανές και έγιναν περισσότερο εφευρετικοί όσον αφορά στην εφαρμογή της τεχνικής των μαζικών μηνυμάτων. Αντί να χρησιμοποιούν διευθύνσεις από τοπικά βιβλία διευθύνσεων, οι σύγχρονοι ιοί ενσωμάτωσαν τεχνικές για την συγκομιδή διευθύνσεων από ένα αυξανόμενο εύρος αρχείων και χρησιμοποιούν αυτές τις διευθύνσεις και σαν στόχους και σαν ψεύτικες διευθύνσεις αποστολής για επόμενα μηνύματα.

Τα σημερινά συστήματα έχουν να ασχοληθούν με ένα αυξανόμενο σημαντικό πεδίο απειλών και η συζήτηση κατευθύνεται προς τα βήματα που πρέπει να γίνουν για να προστατευθούν.

- ***1998, Ιός Virus, CIH***: Εγκαθίσταται στη μνήμη των υπολογιστών και μολύνει τα εκτελέσιμα αρχεία του υπολογιστή όταν ανοίγουν ή όταν αντιγράφονται. Χειροκίνητες ενέργειες, όπως η ανταλλαγή μολυσμένων αρχείων μεταξύ των χρηστών κάνουν δυνατή τη διάδοση μεταξύ των συστημάτων.

  Ενεργοποιείται στις 26 του μήνα (στις 26 Απριλίου ενεργοποιούνται μόνο οι αυθεντικές εκδοχές). Γράφει πάνω στο σκληρό δίσκο του υπολογιστή τυχαία δεδομένα και προσπαθεί να φθείρει το *Flash* του *BIOS*.

  Δεν υπάρχουν δυνατότητες αυτοσυντήρησης του ιού.

- ***1999, Μακρο-ιός του Ms-Word, MelissaA:*** Μολύνει τα αρχεία *Ms-Word* και τα αντίστοιχα πρότυπα. Εκτελεί αυτόματη αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας το *Microsoft Outlook* στις 50 πρώτες εγγραφές του βιβλίου διευθύνσεων. Όλα τα μηνύματα παρουσιάζονται ως *Important message from USERNAME,* όπου το *USERNAME* έχει επιλεγεί από τις αρχικοποιήσεις του *MS word* του μολυσμένου συστήματος και έχουν το ίδιο μήνυμα στο σώμα του μηνύματος: "*Here is that document you asked for…don't show anyone else"*.

  Προσαρτά το ενεργό κείμενο στα μηνύματα ηλεκτρονικού ταχυδρομείου που μοιάζει με γνωστοποίηση ευαίσθητης και εμπιστευτικής πληροφορίας. Ανοίγοντας ή κλείνοντας ένα μολυσμένο αρχείο σε κάποια χρονική στιγμή όπου τα λεπτά της ώρας είναι τα ίδια με τον αριθμό της ημέρας του μήνα (π.χ. 10 λεπτά μετά τις 8, στις 10 του μήνα), έχει σαν αποτέλεσμα να μπουν τα ακόλουθα στο κείμενο:*Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here*.

  Για να αυτοσυντηρηθεί, μετατρέπει τις αρχικοποιήσεις ασφάλειας και απενεργοποιεί τις ειδοποιήσεις του συστήματος.

- ***2000, Ιός Worm, KakWorm:*** Διαχέεται χρησιμοποιώντας εκδόσεις του *Microsoft Outlook Express*, προσαρτώμενος σε εξερχόμενα μηνύματα χρησιμοποιώντας τη λειτουργία *Signature*.

  Ενεργοποιείται στις 5 το απόγευμα της πρώτης μέρας του μήνα και κλείνει το σύστημα.

  Δεν υπάρχουν δυνατότητες αυτοσυντήρησης του ιού.

- ***2001, Ιός Virus/Worm, Nimda****:* Μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας ιδιωτική μηχανή *SMTP*. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου συλλέγονται από τα *.htm* και τα *.html* αρχεία και επίσης από μηνύματα που διατηρούνται μέσα στο σύστημα. Μπορεί επίσης να διαδοθεί μέσω ανταλλαγών στα δίκτυα.

  Ενεργοποιεί το δίσκο *C* του συστήματος σαν ένα σημείο του δικτύου επιτρέποντας έτσι πρόσβαση στο σύστημα. Επίσης δημιουργεί έναν λογαριασμό επισκέπτη με δικαιώματα διαχειριστή. Μολύνει εκτελέσιμα αρχεία και αντικαθιστά πολλά νόμιμα αρχεία του συστήματος. Μπορεί να υποβαθμίσει την απόδοση και να προκαλέσει αστάθεια στο μολυσμένο σύστημα.

  Δεν υπάρχουν δυνατότητες αυτοσυντήρησης του ιού.

- ***2002, Ιός Worm, Klez-H****:* Μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας ιδιωτική μηχανή *SMTP*. Προσπαθεί να συλλέξει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από περισσότερους από 20 τύπους αρχείων. Σπρώχνει την διεύθυνση του αποστολέα σε μαζικές αποστολές μηνυμάτων.

  Προσαρτά ένα αρχείο τυχαία επιλεγμένο από το τοπικό σύστημα το οποίο στέλνεται σαν προσάρτημα στη μαζική αποστολή μαζί με τον ιό. Μολύνει εκτελέσιμα αρχεία (κρύβοντας τα αυθεντικά και αντικαθιστώντας τα με αντιγραφές του εαυτού του). Βάζει τον ιό *Elkem* στους φακέλους των αρχείων προγραμμάτων και τον εκτελεί.

  Απομακρύνει τα κλειδιά αρχικοποίησης των προϊόντων *AV* και διαγράφει τα αρχεία *checksum*.

- ***2003, Ιός Worm, Sobig.F****:* Μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας ιδιωτική μηχανή *SMTP*. Συλλέγει μηνύματα από τα αρχεία τύπου *.dbx, .eml, .hlp, .htm, .html, .mht, .wab* και *.txt.* Στέλνει μηνύματα με ένα από εννέα πιθανά θέματα, δύο πιθανά σώματα μηνύματος και εννέα πιθανά ονόματα προσαρτημάτων. Χρησιμοποιεί τις λεπτομέρειες από μηνύματα του αποστολέα χρησιμοποιώντας τυχαία επιλεγμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου από το τοπικό σύστημα και από τις αποστολές μηνυμάτων (από το πεδίο "*From*"). Επίσης προσπάθησε να διαδοθεί μέσω ανταλλαγών του δικτύου αλλά δεν τα κατάφερε λόγω μιας αβλεψίας του κώδικά του.

  Έχει τη δυνατότητα να φορτώνει και να εκτελεί αρχεία τύπου *trojan horse* στο τοπικό σύστημα. Έχει δυναμική να κλέψει πληροφορία από το τοπικό σύστημα.

  Δεν υπάρχουν δυνατότητες αυτοσυντήρησης του ιού.

- ***2004, Ιός Worm, Netsky.P****:* Μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας ιδιωτική μηχανή *SMTP*. Συλλέγει διευθύνσεις ηλεκτρονικού ταχυδρομείου από αρχεία στα τοπικά μέσα αντιγραφής αρχείων. Χρησιμοποιεί πολλαπλά θέματα μηνυμάτων και προσαρτήματα. Αντιγράφει τον εαυτό του σε φακέλους ανταλλαγής αρχείων ομότιμων (*peer to peer, P2P*) και χρησιμοποιεί διάφορα ονόματα για να ξεγελάσει το σύστημα.

  Δεν υπάρχουν ενέργειες του ωφέλιμου φορτίου και επιδράσεις*.*

  Δεν υπάρχουν δυνατότητες αυτοσυντήρησης του ιού.

2.2.4 Στρατηγικές Ανίχνευσης και Πρόληψης

Η βιομηχανία ασφάλειας απάντησε στις απειλές με ένα εύρος από τεχνολογίες πρόληψης, ανίχνευσης και «εμβολιασμού». Τα αντιιϊκά λογισμικά είναι σήμερα ένα από τα πιο ευρέως χρησιμοποιημένα αντίμετρα ασφάλειας, καθώς χρησιμοποιούνται από το 96% των χρηστών. Η ανάπτυξη του αντιιϊκού λογισμικού πρέπει να είναι γρήγορη ώστε να καλύψει το ρυθμό της εξελισσόμενης απειλής. Τα μοντέρνα αντιιϊκά συστήματα πρέπει να είναι ιδιαίτερα πολύπλοκα, για να αντιμετωπίσουν την πολυπλοκότητα της απειλής. Σ' αυτό το κεφάλαιο θα συνοψίσουμε τις κύριες στρατηγικές που χρησιμοποιούνται.

2.2.4.1 Αναγνώριση του Κακόβουλου Λογισμικού και Απολύμανση

Τα περισσότερα συστήματα αντιιϊκού λογισμικού έχουν βασιστεί σε μεθοδολογίες αναγνώρισης του κακόβουλου λογισμικού μέσω τεχνικών σάρωσης *(scanning),* στη συνέχεια απομόνωσης του ιού και απολύμανσης του συστήματος. Οι σαρωτές που

χρησιμοποιούνται από τους αντιιϊκούς μηχανισμούς μπορούν να έχουν τις παρακάτω μορφές:

- ***Απλή Σάρωση (Simple Scanning)***: Ανιχνεύει αλυσίδες από *bytes* που χρησιμοποιούνται από ήδη γνωστούς τύπους κακόβουλου λογισμικού,
- ***Πολύπλοκη Σάρωση (Complex Scanning)***: Βασίζεται στην απλή σάρωση για να βελτιώσει την ανίχνευση και να αναγνωρίσει ακριβείς αντιστοιχίες, επιτρέποντας την πρόληψη των παραλλαγών που είναι ένα χαρακτηριστικό του κακόβουλου λογισμικού,
- ***Αλγοριθμική Σάρωση(Algorithmic Scanning)***: Δημιουργεί έναν αλγόριθμο που μπορεί να χρησιμοποιηθεί για να ταιριάξει και να ανιχνεύσει έναν συγκεκριμένο ιό,
- ***Ανάλυση του Κώδικα (Code Emulation)***: Βασίζεται στη χρήση μιας εικονικής μηχανής για την ανάλυση του περιβάλλοντος. Ο ιός εκτελείται σε αυτό το εικονικό περιβάλλον, όπου μπορεί να γίνει κατανοητός και έτσι να ανιχνευθεί και να απομακρυνθεί από το πραγματικό σύστημα,
- ***Ευρετική Ανάλυση (Heuristic Analysis):*** Ελέγχει για ύποπτους συνδυασμούς κώδικα και συχνά χρησιμοποιείται σαν φίλτρο για τους αλγοριθμικούς σαρωτές,
- ***Νευρονικά Δίκτυα (Neural Networks):*** Μπορούν να χρησιμοποιηθούν για να μειώσουν τον αριθμό των θετικών αλλά λανθασμένων ευρημάτων από την ευρετική ανάλυση. Ένα νευρονικό δίκτυο μπορεί να εκπαιδευθεί να ανιχνεύει μόνο αυτούς τους συνδυασμούς κώδικα που είναι πραγματικά κακόβουλοι.

Μόλις αναγνωριστεί με την χρήση ενός συνδυασμού των μεθόδων σάρωσης που αναφέρθηκαν πιο πάνω, το κακόβουλο λογισμικό θα πρέπει να απομονωθεί και αν χρειάζεται το μολυσμένο σύστημα θα πρέπει να «απολυμανθεί» και να διορθωθεί**.** Σε γενικές γραμμές, τα αντιιϊκά συστήματα βασίζονται στη γνώση που υπάρχει σχετικά με τη θέση και το μέγεθος του κακόβουλου λογισμικού έτσι ώστε να απενεργοποιήσουν τη διαδικασία απολύμανσης και να απομακρύνουν τον ιό από τον μολυσμένο υπολογιστή, από το πρόγραμμα ή από άλλο μέσο. Αν το κακόβουλο λογισμικό είναι πολυμορφικό, θα πρέπει πρώτα να αποκρυπτογραφηθεί και τα περισσότερα μοντέρνα αντιιϊκά συστήματα έχουν ένα γενικό αποκρυπτογραφητή που βασίζεται στην μέθοδο της ανάλυσης κώδικα που αναφέραμε πιο πάνω.

Παρά την επιτήδευση και την πολυπλοκότητα των τεχνικών ανίχνευσης και «απολύμανσης» που χρησιμοποιούν τα αντιιϊκά συστήματα, αυτά περιορίζονται σε μεγάλο βαθμό στο να αναγνωρίζουν μόνο γνωστές απειλές. Έτσι, η διαρκής ενημέρωση των αντιιϊκών προϊόντων με νέες υπογραφές είναι ζωτικής σημασίας για να είναι βιώσιμη η προστασία από το κακόβουλο λογισμικό. Επιπλέον, το αντιιϊκό λογισμικό βασίζεται στην ικανότητα των τελικών χρηστών να ακολουθούν τις βέλτιστες πρακτικές της ασφάλειας και να τις χρησιμοποιούν κατάλληλα για να ανιχνεύουν τα άγνωστα στοιχεία που εισέρχονται στο σύστημά τους. Η ακατάλληλη χρήση του αντιιϊκού λογισμικού μπορεί να υπονομεύσει σε σημαντικό βαθμό την ικανότητά του να προσφέρει προστασία έναντι των απειλών του κακόβουλου λογισμικού.

2.2.4.2 Τεχνικές Μετρίασης του Κακόβουλου Λογισμικού

Διαφορετικοί μηχανισμοί μπορούν να χρησιμοποιηθούν για να μετριάσουν την απειλή του κακόβουλου λογισμικού. Αυτοί περιλαμβάνουν:

- Συστήματα ελέγχου πρόσβασης,
- Έλεγχος ακεραιότητας,
- Κλείδωμα συμπεριφοράς,
- «Άμμος πυγμαχίας» (*Sand boxing*),
- Εκπαίδευση του χρήστη.

Οι έλεγχοι πρόσβασης χτίζονται στα λειτουργικά συστήματα για να περιορίσουν τα δικαιώματα των χρηστών και των εφαρμογών. Ο σκοπός τους είναι να εξασφαλίσουν την εμπιστευτικότητα των δεδομένων σε ένα σύστημα. Ωστόσο, από τη φύση του το κακόβουλο λογισμικό αντιπροσωπεύει την έκθεση σε κίνδυνο περισσότερο της ακεραιότητας των δεδομένων παρά της εμπιστευτικότητας και έτσι είναι ικανό να εισέλθει σε ένα σύστημα με όλα τα κατάλληλα δικαιώματα του χρήστη ή της εφαρμογής. Επομένως το κακόβουλο λογισμικό μπορεί να ελεγχθεί περιορίζοντας την λειτουργικότητα του συστήματος σε βασικές εφαρμογές που δεν είναι στόχοι μόλυνσης, απομονώνοντας το σύστημα από την επαφή με πιθανές πηγές κακόβουλου λογισμικού, ή περιορίζοντας τη ροή των δεδομένων έτσι ώστε να σπάσει η αλυσίδα της μολυσματικότητας.

Αντίθετα με τους ελέγχους πρόσβασης, ***ο έλεγχος της ακεραιότητας*** βασίζεται στο γεγονός ότι το κακόβουλο λογισμικό θέτει σε κίνδυνο την ακεραιότητα ενός προγράμματος. Δυστυχώς, η ικανότητα του συστήματος να ελέγξει ότι όλα τα εγκατεστημένα προγράμματα δεν έχουν αλλάξει, έχει μειωμένη χρησιμότητα – δεδομένου ότι οι εφαρμογές συχνά αλλάζουν και έτσι δεν είναι δυνατό να αναγνωριστεί ένα πρόγραμμα που είναι ήδη μολυσμένο και επίσης ένας τέτοιος μηχανισμός θα απασχολούσε πολλούς πόρους του συστήματος. Ωστόσο, ο έλεγχος της ακεραιότητας μπορεί να γίνει σε συνδυασμό με τα συστήματα ανίχνευσης που αναλύθηκαν πιο πάνω και θα μπορούσε να είναι περισσότερο χρήσιμος μελλοντικά με ανάπτυξη κώδικα στην αρχιτεκτονική των προσωπικών υπολογιστών που θα κάνουν τις εφαρμογές εγγενώς πιο ασφαλείς.

Το κλείδωμα της συμπεριφοράς βασίζεται στο γεγονός ότι το κακόβουλο λογισμικό συχνά ξεκινάει δράσεις τις οποίες ο χρήστης αγνοεί, όπως το να καλέσει μια εφαρμογή ή ένα εκτελέσιμο αρχείο. Τα συστήματα που κλειδώνουν συμπεριφορές, αναγνωρίζουν τέτοιου είδους δράσεις και ρωτούν το χρήστη αν θέλει να εκτελεστούν αυτές οι ενέργειες. Το πρόβλημα με ένα τέτοιο σύστημα είναι ότι οι περισσότεροι χρήστες αγνοούν αν η ενέργεια είναι επιθυμητή ή όχι και θα θεωρήσουν αυτά τα συχνά μηνύματα ενοχλητικά. Τα συστήματα αυτά μπορούν να παρακαμφθούν από κακόβουλο λογισμικό που προκαλεί «αργή μόλυνση» και εκτελείται όταν ένας χρήστης άθελά του επιτρέπει να εκτελεστεί μια ενέργεια και από κακόβουλο λογισμικό του οποίου ο κώδικας μολύνει απ' ευθείας μια ενέργεια την οποία ένα τέτοιο σύστημα επέτρεψε να εκτελεστεί.

Ωστόσο, το κλείδωμα της συμπεριφοράς μπορεί να έχει κάποια βάση, ειδικά όταν χρησιμοποιείται σε συνδυασμό με την ***ευρετική ανάλυση***. Σε τέτοιες περιπτώσεις η ενέργεια του κλειδώματος είναι διαφανής για τον χρήστη. Πράγματι, η πιθανή ταχύτητα της μόλυνσης αυτοδιαδίδοντας κακόβουλο λογισμικό ηλεκτρονικού ταχυδρομείου (το οποίο συχνά αναφέρεται ως ***μαζικοί αποστολείς μηνυμάτων***) είχε σαν αποτέλεσμα την ανάπτυξη ειδικών συστημάτων κλειδώματος συμπεριφοράς και εργαλείων άμυνας βασισμένων σε υπολογιστές. Αυτά μπορούν να δράσουν αποτελεσματικά σαν συστήματα ανίχνευσης, διείσδυσης και πρόληψης βασισμένα σε υπολογιστές, για να αναγνωρίσουν τη συμπεριφορά πολλών τύπων ιών όπως των *Slammer, Blaster,*

Mydoom, Netsky και *Sobig*. Για να το θέσουμε απλά, η τεχνική αυτή κλειδώνει κάθε προσπάθεια του κακόβουλου λογισμικού να εκτελέσει μια εντολή σε ένα απομακρυσμένο σύστημα.

***Η «άμμος πυγμαχίας»* (*sand boxing*)** είναι μια σχετικά πρόσφατη έννοια που επιτρέπει μόνο σε έμπιστα προγράμματα να τρέξουν σε ένα σύστημα. Όλα τα άλλα προγράμματα τρέχουν σε απομονωμένα εικονικά υποσυστήματα *(virtual subsystems*). Κάθε μόλυνση επομένως, δεν θα επηρεάσει το πραγματικό σύστημα και μπορεί να ανιχνευθεί και να απομονωθεί στο αντίστοιχο υποσύστημα. Η τεχνική αυτή έχει πολυάριθμα πιθανά μειονεκτήματα, όπως οι δυσκολίες να αναλυθούν όλες οι εφαρμογές σε εικονικά υποσυστήματα, οι περιορισμοί που τίθενται από το δίκτυο και η πιθανότητα το έμπιστο σύστημα τελικά να αποτύχει. Είναι επίσης πιθανό μερικοί τύποι κακόβουλου λογισμικού να μολύνουν το πραγματικό σύστημα και να αποφύγουν την «άμμο πυγμαχίας». Ωστόσο, είναι πιθανό η «άμμος πυγμαχίας» να βρει κάποια εφαρμογή σε συνδυασμό με άλλες λύσεις ασφάλειας.

Η εκπαίδευση του χρήστη είναι απλή, αλλά ζωτικής σημασίας και στην πρώτη γραμμή άμυνας για την μετρίαση του κακόβουλου λογισμικού. Είναι σημαντικό, όλοι οι χρήστες ενός συστήματος να συνειδητοποιήσουν ότι οι ενέργειες που κάνουν μπορεί να έχουν μια σημαντική επίδραση στην ασφάλεια του συστήματος. Θα πρέπει να είναι γνώστες των κινδύνων όταν ανοίγουν ή κοιτάζουν προσαρτήματα μηνυμάτων ηλεκτρονικού ταχυδρομείου που προέρχονται από μη έμπιστες πηγές και επίσης των κινδύνων όταν εγκαθιστούν μη έμπιστο λογισμικό και όταν δεν διατηρούν ενημερωμένο το αντιιϊκό λογισμικό τους. Επίσης οι διαχειριστές των συστημάτων θα πρέπει να είναι γνώστες των κινδύνων όταν συνδέουν έναν υπολογιστή με μη ενημερωμένη αντιιϊκή προστασία σε ένα παραγωγικό σύστημα.

2.2.4.3 Τεχνικές Επιπέδου Δικτύου

Σε επίπεδο δικτύου, οι άμυνες έναντι του κακόβουλου λογισμικού περιλαμβάνουν τη χρήση λιστών δρομολογητών ελέγχου πρόσβασης *(Access Control List, ACL),* το κλείδωμα θυρών σε τείχη προστασίας (*firewalls*), την ανάπτυξη συστημάτων ανίχνευσης διείσδυσης σε δίκτυα και τη χρήση συστημάτων παγίδας (*honeypots)* και συστημάτων έγκαιρης προειδοποίησης.

Οι δρομολογητές δικτύων *(network routers)* μπορούν να θεωρηθούν σαν την πρώτη γραμμή άμυνας απέναντι στο κακόβουλο λογισμικό. Είναι χρήσιμοι στην πρόληψη των επιθέσεων άρνησης παροχής υπηρεσίας και των προσπαθειών διάδοσης του κακόβουλου λογισμικού, χρησιμοποιώντας φιλτράρισμα εισερχόμενης και εξερχόμενης κίνησης και λίστες ελέγχου πρόσβασης έτσι ώστε να αρνούνται την κίνηση από/προς συγκεκριμένα υποδίκτυα ή θύρες. Στην πράξη, αυτά τα συστήματα προσομοιάζουν με τη λειτουργία των τειχών προστασίας αν και δεν είναι τόσο εξελιγμένα. Αντίθετα με το τείχος προστασίας, ένας δρομολογητής δεν προορίζεται αρχικά να λειτουργήσει ως συσκευή ασφάλειας, ο σκοπός του είναι να βοηθά τη συνδεσιμότητα. Είναι επίσης σημαντικό να τονιστεί ότι οι δρομολογητές έχουν ως συσκευές κάποιες αδυναμίες οι οποίες πρέπει να διορθώνονται με κώδικα (*patch*). Στο μέλλον, είναι πιθανό οι επιθέσεις να στοχεύουν συγκεκριμένους δρομολογητές, με δυνητικά καταστρεπτικά αποτελέσματα.

Τα τείχη προστασίας (*firewalls*) είναι μια ζωτικής σημασίας άμυνα έναντι του κακόβουλου λογισμικού. Με τη χρήση των κατάλληλων τειχών προστασίας μπορούν να αποφευχθούν πολλές επιθέσεις κακόβουλου λογισμικού. Ειδικά, με το να κλειδώνουμε τις θύρες σε όλες τις μη χρησιμοποιημένες υπηρεσίες εμποδίζουμε ένα σημαντικό ποσοστό κίνησης κακόβουλου λογισμικού, ειδικά την προσπέλαση αφύλακτων θυρών.

Για παράδειγμα το κλείδωμα της θύρας *TCP 3127* εμποδίζει τη λειτουργία του ιού *Mydoom* και το κλείδωμα της θύρας *UDP 1434* (που σχετίζεται με τον *Microsoft SQL Server)* εμποδίζει τον ιό *Slammer* να διαδοθεί. Ωστόσο, τα τείχη προστασίας δεν μπορούν εύκολα να κλειδώσουν την κίνηση σε χρησιμοποιημένες υπηρεσίες, όπως η θύρα *TCP 80* η οποία χρησιμοποιείται από τους εξυπηρετητές *web*. Είναι σημαντικό να γνωρίζουμε ότι τα τείχη προστασίας πρέπει να αποτελούν μέρος ενός πολυεπίπεδου συστήματος άμυνας. Για παράδειγμα πολλοί οργανισμοί ενθαρρύνουν τους υπαλλήλους που εργάζονται από το σπίτι και τους απομακρυσμένους συνεργάτες να συνδέονται με το δίκτυο χρησιμοποιώντας ιδιωτικά εικονικά δίκτυα *(Virtual Private Network, VPN)*. Αυτοί οι πελάτες εισέρχονται στο δίκτυο πίσω από την περίμετρο του τείχους προστασίας και έτσι καθιστούν αμέσως το δίκτυο ευάλωτο, εκτός και αν έχουν προμηθευτεί τα δικά τους τείχη προστασίας. Είναι επίσης απαραίτητο να θυμόμαστε ότι τα τείχη προστασίας έχουν αδυναμίες και γίνονται ολοένα και περισσότερο στόχοι των εισβολέων. Επομένως το λογισμικό των τειχών προστασίας θα πρέπει απαραίτητα να διατηρείται ενημερωμένο.

Τα συστήματα ανίχνευσης και παρεμπόδισης εισβολής *(network intrusion detection and prevention systems)* σε δίκτυα μπορούν να χρησιμοποιηθούν για να παράγουν ειδοποιήσεις όταν αναγνωρίζεται ο τύπος της κίνησης που παράγεται από μια κακόβουλη εισβολή. Σε ***κατάσταση εργασίας*** *(logging mode)* παράγεται μόνο μια ειδοποίηση και επιτρέπει στον διαχειριστή του συστήματος να κάνει τις ανάλογες ενέργειες. Σε ***κατάσταση κλειδώματος*** (*blocking mode)* η κακόβουλη κίνηση θα ελεγχθεί και θα απαγορευθεί πριν φτάσει στον επιθυμητό στόχο. Η ανίχνευση της εισβολής μπορεί να χρησιμοποιήσει μηχανές για να προσδιορίσει ανωμαλίες στη ροή της κίνησης πρωτοκόλλου και επίσης συστήματα που βασίζονται σε υπογραφές για να αναγνωρίσει συγκεκριμένους τύπους επίθεσης. Τα περισσότερο αποτελεσματικά συστήματα συνδυάζουν και τους δύο τύπους.

Τα συστήματα παγίδας *(honeypot)* έχουν σχεδιαστεί για να δελεάζουν τους εισβολείς παρέχοντας ένα εικονικό σύστημα το οποίο φαίνεται ευάλωτο και μπορούν εύκολα να του επιτεθούν. Σε ένα παραγωγικό σύστημα, ο γενικός ρόλος του συστήματος είναι να αποσπά την προσοχή των εν δυνάμει εισβολέων, να επισημαίνει τις λεπτομέρειες μιας επίθεσης και να τις κατευθύνει σε ένα αρχείο καταγραφής (*log)*. Περισσότερο εξελιγμένα είδη τέτοιων συστημάτων που συλλέγουν πιο εκτενείς πληροφορίες, μπορούν να χρησιμοποιηθούν στην έρευνα που αφορά στα αντιιϊκά λογισμικά για να συλλέξουν και να αναλύσουν νέους τύπους ιών. Τα συστήματα παγίδας (*honeypot*) είναι επομένως μια πολύ χρήσιμη προσθήκη στο οπλοστάσιο της άμυνας. Επιπλέον, μια παρόμοια αλλά λιγότερο εξελιγμένη εκδοχή αυτού του συστήματος εφαρμόζεται με τις τεχνολογίες παγίδας των ψεύτικων ηλεκτρονικών μηνυμάτων (*spamtrap*), που χρησιμοποιούνται για να προσελκύσουν κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*) χρησιμοποιώντας ψεύτικες διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Τα συστήματα έγκαιρης ειδοποίησης *(early warning systems)* είναι ικανά να συλλέξουν δεδομένα από έναν αριθμό από διαφορετικούς αισθητήρες *(sensors).* Συσχετίζοντας τα αρχεία καταγραφής δεδομένων των τειχών προστασίας, τις πληροφορίες από τα συστήματα ανίχνευσης των εισβολών (και στους υπολογιστές και στο δίκτυο) και από τα συστήματα παγίδας (*honeypots*), μπορούν να προμηθεύσουν τον τύπο της λεπτομερούς ανάλυσης της κακόβουλης κυκλοφορίας στο δίκτυο η οποία θα παράξει μια ειδοποίηση και θα επιτρέψει να γίνουν αποτελεσματικά και εγκαίρως ενέργειες άμυνας. Αυτά τα συστήματα είναι καλύτερα αν η πληροφορία μπορεί να συλλεχθεί από αισθητήρες τοποθετημένους σε πολλές θέσεις μέσα στο διαδίκτυο (*web*).

Τέτοια συστήματα είναι ικανά να αναγνωρίσουν και να ανιχνεύσουν τις αναπτυσσόμενες απειλές καθώς αυτές διαχέονται μέσα στο διαδίκτυο.

Συμπερασματικά, η άμυνα ενάντια στο κακόβουλο λογισμικό θα πρέπει να είναι δομημένη σε επίπεδα και να εφαρμόζεται σε βάθος. Θα πρέπει να εμπλέκει αντιιϊκά συστήματα ικανά να αναπτύξουν εξ ολοκλήρου την πανοπλία των τεχνικών ανίχνευσης και ανάλυσης. Αυτά τα συστήματα θα πρέπει να χρησιμοποιούνται τόσο στην πύλη (*gateway*) όσο και στον υπολογιστή (*host*) και θα πρέπει να παραμένουν ενημερωμένα για να εξασφαλιστεί η ικανότητά τους στην αντιμετώπιση των συνεχώς μεταβαλλόμενων απειλών του κακόβουλου λογισμικού. Η πολυεπίπεδη άμυνα θα πρέπει επίσης να εμπλέκει δρομολογητές (*routers*) με καλά ρυθμισμένες τις λίστες πρόσβασης και τείχη προστασίας με πολιτικές ενημέρωσης, τόσο στο δίκτυο όσο και στον υπολογιστή (*host*). Η ανίχνευση εισβολής στα δίκτυα μπορεί να είναι πολύ σημαντική, αν αναπτύσσεται και παρακολουθείται κατάλληλα όπως γίνεται με τα συστήματα παγίδας (*honeypots*) και με τα συστήματα έγκαιρης ειδοποίησης. Η εκπαίδευση του χρήστη στα θέματα ασφάλειας, δεν θα πρέπει να παραμεληθεί, καθώς η ασφαλής συμπεριφορά του χρήστη διαμορφώνει μια σημαντική πρώτη γραμμή άμυνας.

Πάνω απ' όλα, είναι ζωτικής σημασίας να αναγνωρίζονται και να διορθώνονται όσο το δυνατόν γρηγορότερα οι κρίσιμες αδυναμίες. Πράγματι, το χρονικό διάστημα που μεσολαβεί από την αποκάλυψη της αδυναμίας μέχρι την εκδήλωση της απειλής από κακόβουλο λογισμικό έχει μειωθεί δραματικά. Για παράδειγμα, το 2001 χρειάστηκαν 330 ημέρες από την δημοσιοποίηση μιας αδυναμίας μέχρι να εκδηλωθεί αντίστοιχη επίθεση από τον ιό *worm Nimda*, γεγονός που έδωσε άπλετο χρόνο στους διαχειριστές που ήταν προσηλωμένοι σε θέματα ασφάλειας να διορθώσουν τα συστήματά τους. Το καλοκαίρι του 2003 τα κρούσματα εισβολής είχαν αυξηθεί σημαντικά, με το ιό *worm Blaster* να παρουσιάζεται μόλις 27 ημέρες από την αποκάλυψη της αδυναμίας. Ωστόσο, η πρόκληση για τους διαχειριστές συστήματος αυξήθηκε ακόμα περισσότερο και κατά τη διάρκεια των τελευταίων έξι μηνών του 2004 παρατηρήθηκε μέσος όρος 5.8 ημερών μεταξύ της δημοσιοποίησης μιας αδυναμίας και της επίθεσης από το κακόβουλο λογισμικό. Επιπλέον, υπάρχει μεγάλη ανησυχία για τις πιθανές επιθέσεις μηδενικής μέρας, που συνεπάγονται την εκμετάλλευση μιας αδυναμίας που δεν έχει ακόμα δημοσιοποιηθεί. Έτσι, είναι σημαντικότερο από ποτέ να δοθεί ιδιαίτερη προσοχή στο θέμα της ανίχνευσης και της αποφυγής των απειλών του κακόβουλου λογισμικού.

2.2.5 Επίλογος

Η παραπάνω συζήτηση ανέδειξε ότι αν και το κακόβουλο λογισμικό έχει αναγνωριστεί εδώ και 20 χρόνια, συνεχίζει να αποτελεί μια σημαντική και εξελισσόμενη απειλή. Οι έρευνες ασφάλειας μιας μεγάλης ποικιλίας πηγών μεταφέρουν την ανησυχητική εντύπωση ότι το κακόβουλο λογισμικό δεν είναι μόνο η πιο επιφανής απειλή, αλλά και ότι η επικράτηση και οι επιπτώσεις του αυξάνονται συνεχώς. Έτσι, τώρα θεωρείται μεγαλύτερο πρόβλημα αντί να ελαττώνεται.

Η συζήτηση ανέδειξε την αυξανόμενη πολυπλοκότητα της δράσης του κακόβουλου λογισμικού, όσον αφορά στη διάδοση, στο ωφέλιμο φορτίο και στις τεχνικές συντήρησης. Με ένα πλήθος νέων παραγόντων μόλυνσης, μαζί με ένα μεγαλύτερο εύρος κακόβουλων δράσεων που μπορούν να εκτελεστούν όταν συμβεί η μόλυνση, το σημερινό κακόβουλο λογισμικό είναι περισσότερο προβληματικό από τις προηγούμενες γενιές του. Αυτό σχετίζεται κατά πολύ, με τις επιπλέον ευκαιρίες μόχλευσης και εκμετάλλευσης της υποκείμενης τεχνολογίας ειδικότερα για την αξιοποίηση της συνδεσιμότητας του δικτύου. Ωστόσο, υπάρχει μια καθαρή σύνδεση στα άτομα που είναι υπεύθυνα για τη δημιουργία και την απελευθέρωση του κακόβουλου λογισμικού.

Το ευρύ φάσμα των πιθανών κινήτρων σημαίνει ότι δεν υπάρχει ένα συγκεκριμένο προφίλ των πιθανών υπόπτων και ότι οι ευκαιρίες οικονομικού οφέλους προσελκύουν τώρα πολλούς που πριν δεν ενδιαφέρονταν γι' αυτό.

Το κακόβουλο λογισμικό θα συνεχίσει να αναπτύσσεται. Η απειλή που θα αντιμετωπίσουμε στο μέλλον έχει τη δυναμική να είναι χειρότερη από τη σημερινή, με περαιτέρω στόχους μόλυνσης (όπως τα κινητά τηλέφωνα) που ήδη αυξάνονται. Αυτή η κατάσταση έχει προκύψει παρά την εμφανή βελτίωση των τεχνολογιών προστασίας. Ωστόσο, αυτές οι τεχνολογίες θα συνεχίσουν να αποτυγχάνουν όχι λόγω σύμφυτων αδυναμιών αλλά λόγω αναποτελεσματικής και ανεπαρκούς ανάπτυξης ή επειδή πολλές αδυναμίες παραμένουν «ανοιχτές» ενώ θα έπρεπε να εμποδιστούν με το κατάλληλο λογισμικό. Η εξελισσόμενη απειλή απαιτεί αυξημένη προστασία σε πολλά μέτωπα και μπορεί να αντιμετωπιστεί μόνο με κατάλληλους συνδυασμούς τεχνολογίας και επαγρύπνηση των πιθανών θυμάτων. **[5]**

3. Δικανική Αντιμετώπιση των Ηλεκτρονικών Επιθέσεων

3.1 Ενσωματώνοντας την Ιδιωτικότητα στη Σχεδίαση των Πληροφοριακών Συστημάτων

Στα σύγχρονα ψηφιακά περιβάλλοντα, κάθε χρήστης πρέπει να παρέχει κάποια δεδομένα με βάση τα οποία αποκτά πρόσβαση στις ηλεκτρονικές υπηρεσίες που του προσφέρονται και διευκολύνουν κατά πολύ την προσωπική και επαγγελματική του ζωή. Τα δεδομένα αυτά, όμως, συχνά περιέχουν προσωπικές πληροφορίες για το χρήστη, όπως αριθμό φορολογικού μητρώου, αριθμό πιστωτικής κάρτας, αριθμό ταυτότητας κ.λπ. Σχετικές έρευνες υποδεικνύουν ότι οι χρήστες των ηλεκτρονικών υπηρεσιών θεωρούν ότι τα δεδομένα τους δεν προστατεύονται επαρκώς και ότι ο κίνδυνος παραβίασης της ιδιωτικότητάς τους είναι σημαντικός. Τα παραπάνω έχουν αρνητικό αντίκτυπο στην εμπιστοσύνη των χρηστών στα πληροφοριακά συστήματα που χρησιμοποιούν.

Ως αποτέλεσμα, η προστασία της ιδιωτικότητας αποτέλεσε τον κεντρικό στόχο πρόσφατων ερευνών στον τομέα της ανάπτυξης πληροφοριακών συστημάτων. Αρχικά οι προσπάθειες εστιάστηκαν στην ανάπτυξη τεχνικών λύσεων που διασφαλίζουν την ιδιωτικότητα των χρηστών και εφαρμόζονται στη φάση της υλοποίησης του συστήματος. Οι τεχνολογίες αυτές οι οποίες αναφέρονται και ως ***τεχνολογίες βελτίωσης της ιδιωτικότητας*** (*Privacy enhancing technologies),* είναι αρκετά γενικές και δεν λαμβάνουν υπόψη το επιχειρησιακό πλαίσιο στο οποίο θα λειτουργεί το πληροφοριακό σύστημα και τις ανάγκες του. Συνεπώς, η επιλογή της κατάλληλης λύσης δεν είναι προφανής και είναι πολύ πιθανό η εφαρμογή κάποιας λύσης τελικά να μην ανταποκρίνεται στις ανάγκες των χρηστών του συστήματος. Αυτό έστρεψε το ενδιαφέρον σε μεθόδους ανάλυσης απαιτήσεων πληροφοριακών συστημάτων που εστιάζουν σε θέματα ασφάλειας (συμπεριλαμβανομένης της ιδιωτικότητας) ήδη από τη φάση της σχεδίασης και όχι κατά τη φάση της υλοποίησης των πληροφοριακών συστημάτων.

Τα βασικά ερωτήματα που προκύπτουν είναι κατά πόσο οι υπάρχουσες μέθοδοι ανάλυσης απαιτήσεων αντιμετωπίζουν ως ξεχωριστό κριτήριο την ιδιωτικότητα και κατά πόσο μεθοδεύουν την προστασία της στο υπό ανάπτυξη σύστημα.

3.1.1 Ιδιωτικότητα και Απαιτήσεις Ιδιωτικότητας

Όταν ένας χρήστης χρησιμοποιεί μια τυπική εφαρμογή ηλεκτρονικής επεξεργασίας κειμένου, συνήθως δεν σκέφτεται αν κάποιος βρίσκεται κοντά του και παρακολουθεί το κείμενο που παράγεται. Όταν ο ίδιος χρήστης περιηγείται το διαδίκτυο, είναι σαν να βρίσκεται στο κέντρο μιας συνομιλίας όπου εκατοντάδες άνθρωποι μπορούν να δουν τι κάνει ή και να ακούσουν τι ακριβώς αναφέρει.

Οι περισσότεροι χρήστες Η/Υ χρησιμοποιούν το διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου για επαγγελματικούς και προσωπικούς σκοπούς. Οι υπηρεσίες του ηλεκτρονικού ταχυδρομείου και του διαδικτύου προσφέρονται από παρόχους υπηρεσιών διαδικτύου *(ISPs),* και ειδικά συστήματα που αναφέρονται ως εξυπηρετητές (*servers*) διεκπεραιώνουν τις αιτήσεις υπηρεσιών των χρηστών. Οι εξυπηρετητές διατηρούν δεδομένα των χρηστών που τους επισκέπτονται για διάφορους λόγους, όπως καλύτερη και γρηγορότερη παροχή υπηρεσίας την επόμενη φορά που θα ζητηθούν οι ίδιες υπηρεσίες, διευκόλυνση των χρηστών στον τρόπο πρόσβασης στις υπηρεσίες αυτές (διατηρώντας τα στοιχεία αναγνώρισής τους) κ.α. Τα στοιχεία αυτά διατηρούνται αποθηκευμένα για σημαντικό χρονικό διάστημα σε αρχεία καταγραφής

(*log files*), τα οποία είναι στη διάθεση του διαχειριστή των συστημάτων αυτών, τόσο για ανάγνωση όσο και για επεξεργασία.

Η χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου είναι δύο από τις πολλές υπηρεσίες που προσφέρονται σήμερα στους διάφορους χρήστες, μέσω των οποίων αυτοί αφήνουν εν αγνοία τους σημαντικό αριθμό των προσωπικών τους δεδομένων, με αποτέλεσμα να παραβιάζεται η ιδιωτικότητά τους. Κατά πόσο όμως γνωρίζουν οι σημερινοί χρήστες τον κίνδυνο της αποκάλυψης όλων αυτών των δεδομένων, των προσωπικών τους δεδομένων, σε τρίτους μη έμπιστους γι' αυτούς χρήστες;

Η ιδιωτικότητα, ως ένα ζήτημα κοινωνικό και νομικό, έχει απασχολήσει εδώ και καιρό κοινωνικούς επιστήμονες, φιλόσοφους και νομικούς. Με την αξιοποίηση των Η/Υ και τις ολοένα αυξανόμενες δυνατότητες που πρόσφεραν τα σύγχρονα πληροφοριακά συστήματα και τα δίκτυα επικοινωνιών, η ιδιωτικότητα των χρηστών άρχισε να κινδυνεύει.

Στην πορεία για τη δημιουργία μιας παγκόσμιας κοινωνίας της πληροφορίας και με την ύπαρξη ολοένα και περισσότερων προγραμμάτων ανάπτυξης των δικτύων τηλεπικοινωνιών μεταξύ των κρατών, δημιουργούνται ποικίλοι κίνδυνοι όσον αφορά στη διαφύλαξη της ιδιωτικότητας των χρηστών που χρησιμοποιούν ή θα χρησιμοποιήσουν τα δίκτυα αυτά.

Η ιδιωτικότητα, ως βασικό ανθρώπινο δικαίωμα αναγνωρισμένο από τη δήλωση του Οργανισμού Ηνωμένων Εθνών για την προστασία των ανθρώπινων δικαιωμάτων, αλλά και από πολλές διεθνείς και τοπικές συνθήκες, πρέπει να προστατεύεται σε μια δημοκρατική κοινωνία. Αυτό μπορεί να επιτευχθεί με έναν από τους παρακάτω τρόπους:

- Θέσπιση νόμων για την ιδιωτικότητα και την προστασία δεδομένων,
- Εφαρμογή τεχνολογιών ενίσχυσης της ιδιωτικότητας που επιλέγονται και εφαρμόζονται από τους χρήστες,
- Εκπαίδευση των χρηστών και των επαγγελματιών πληροφορικής σε θέματα ιδιωτικότητας,
- Τήρηση επιχειρησιακών κανονισμών (κώδικες δεοντολογίας) που αφορούν πρακτικές εφαρμογής και υλοποίησης της ιδιωτικότητας.

Ο πρώτος ορισμός της ιδιωτικότητας δόθηκε από τους *Warren* και *Brandeis* στο άρθρο τους «Το δικαίωμα στην ιδιωτικότητα» *(The right to privacy).* Οι δύο αυτοί Αμερικανοί δικηγόροι όρισαν την ιδιωτικότητα ως ***το δικαίωμα του να είναι κανείς μόνος του.***

Πιο πρόσφατα ο *Alen Westin* απέδωσε τον όρο ιδιωτικότητα ως ***το δικαίωμα κάθε ανθρώπου ή ομάδας ατόμων ή οργανισμών να καθορίζουν από μόνοι τους πότε, πώς και σε ποιό βαθμό οι προσωπικές τους πληροφορίες θα γίνονται γνωστές σε τρίτους***. Ως ομάδες ατόμων ή οργανισμούς αναφερόμαστε σε νομικά πρόσωπα.

Η ιδιωτικότητα ως έννοια, προσεγγίζεται από τρείς πλευρές:

- ***Χωρική Ιδιωτικότητα (Territorial Privacy):*** Αναφέρεται στην προστασία της ιδιωτικότητας του ατόμου στο φυσικό χώρο που τον περιβάλλει, π.χ. να μην μπορούν τρίτοι να παρατηρήσουν τις εργασίες που κάνει ένα άτομο στο γραφείο του,
- ***Ιδιωτικότητα του Ατόμου (Privacy of the Person):*** Αναφέρεται στην προστασία του ατόμου από αναίτιες παρεμβάσεις τρίτων σε αυτό π.χ. φυσική

έρευνα χωρίς δικαιολογία, έλεγχο για κατοχή φαρμάκων, ανήθικη και παράνομη έρευνα για την απόκτηση προσωπικών πληροφοριών κ.λπ.

- ***Πληροφοριακή Ιδιωτικότητα (Informational Privacy):*** Αναφέρεται στο δικαίωμα του κάθε ατόμου να ελέγχει αν και με ποιό τρόπο τα προσωπικά του δεδομένα συλλέγονται, αποθηκεύονται, υφίστανται επεξεργασία και διαμοιράζονται σε τρίτους.

Ο όρος ***προσωπικά δεδομένα*** *(personal data*) αφορά κάθε πληροφορία που προσδιορίζει την προσωπικότητα ενός ατόμου. Ο όρος ***προστασία δεδομένων*** (*data protection*) αναφέρεται στην προστασία των προσωπικών δεδομένων με σκοπό τη διαφύλαξη της ιδιωτικότητας και αποτελεί μέρος της γενικής έννοιας της ιδιωτικότητας. Ωστόσο, η ιδιωτικότητα, δεν μπορεί να αποτελεί δικαίωμα απόλυτο, για όλες τις περιπτώσεις, μια και πολλές φορές η προστασία της έρχεται σε αντίθεση με άλλα δικαιώματα ή νόμους. Επίσης είναι γενικά αποδεκτό ότι κανένας δεν μπορεί να είναι αναγνωρίσιμο μέλος σε μια κοινωνία χωρίς να αποκαλύπτει μέρος των προσωπικών του δεδομένων.

Σε μια κοινωνία αρκετά δικτυακή όπως η σημερινή, η ιδιωτικότητα δεν μπορεί να προστατευτεί μόνο από νόμους και κανονισμούς. Τα πληροφοριακά συστήματα που συλλέγουν προσωπικά δεδομένα θα πρέπει επίσης να αποτρέπουν την παραβίαση της ιδιωτικότητας. Για το λόγο αυτό, οι υπεύθυνοι για την προστασία δεδομένων απαιτούν από τους αναλυτές και τους προγραμματιστές πληροφοριακών συστημάτων να συμπεριλαμβάνουν την ιδιωτικότητα ως τεχνική απαίτηση που πρέπει να λαμβάνεται υπόψη στο υπό ανάπτυξη σύστημα και πιο συγκεκριμένα θα πρέπει να λαμβάνεται υπόψη από τη φάση της σχεδίασης του συστήματος αποτελώντας ξεχωριστό κριτήριο που πρέπει να υλοποιηθεί.

Για να επιτευχθεί ο παραπάνω στόχος και να μπορέσει η ιδιωτικότητα από μια γενική έννοια να μετατραπεί σε γενική απαίτηση, ορίστηκε μια σειρά από επιμέρους απαιτήσεις, που λέγονται ***απαιτήσεις ιδιωτικότητας*** (*privacy requirements*) και είναι οι ακόλουθες:

- Αυθεντικοποίηση (*Authentication*)
- Εξουσιοδότηση *(Authorization*)
- Αναγνώριση (*Identification)*
- Προστασία δεδομένων *(Data Protection*)
- Ανωνυμία (*Anonymity*)
- Ψευδωνυμία *(Pseudonymity*)
- Μη συνδεσιμότητα *(Unlikability*)
- Μη παρατηρησιμότητα (*Unobservability)*

Οι απαιτήσεις αυτές καλύπτουν διάφορες όψεις της ιδιωτικότητας κατά τη χρήση ενός πληροφοριακού συστήματος. Ανάλογα με τον τρόπο προστασίας της ιδιωτικότητας σε ένα πληροφοριακό σύστημα, υλοποιείται μία ή περισσότερες από αυτές.

3.1.1.1 Αυθεντικοποίηση

Η αυθεντικοποίηση είναι η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Σε ιδιωτικά και δημόσια δίκτυα, η αυθεντικοποίηση υλοποιείται συνήθως με τη χρήση κωδικών πρόσβασης (*passwords*).

Η αυθεντικοποίηση αποτελεί κυρίως απαίτηση ασφάλειας παρά ιδιωτικότητας ενός συστήματος.

Έτσι όταν μια οντότητα αιτείται τη χρήση μιας υπηρεσίας από ένα πληροφοριακό σύστημα, θα πρέπει να εξετάζεται η υπηρεσία αυτή και ανάλογα να ζητείται η αυθεντικοποίηση ή μη της συγκεκριμένης οντότητας. Με αυτό τον τρόπο προστατεύονται και η ιδιωτικότητα της οντότητας και τα ευαίσθητα δεδομένα του συστήματος.

3.1.1.2 Εξουσιοδότηση

Η εξουσιοδότηση είναι η διαδικασία μέσω της οποίας μια οντότητα αποκτά δικαιώματα (π.χ. χρήση, τροποποίηση, προσπέλαση κ.λπ.) σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος. Σε ένα σύστημα που υπάρχουν πολλοί χρήστες ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους στο σύστημα.

Η εξουσιοδότηση όπως και η αυθεντικοποίηση, αποτελεί κυρίως απαίτηση ασφάλειας. Η εξουσιοδότηση, όμως, συντελεί στην ικανοποίηση της ιδιωτικότητας, μια και τα ευαίσθητα προσωπικά δεδομένα των χρηστών που βρίσκονται αποθηκευμένα σε ένα σύστημα πρέπει να μπορούν να τα προσπελάσουν μόνο εξουσιοδοτημένοι χρήστες. Προστατεύοντας τα προσωπικά δεδομένα των χρηστών ενός συστήματος, προστατεύεται εν μέρει η ιδιωτικότητά τους.

Η εξουσιοδότηση συχνά έπεται της αυθεντικοποίησης, αφού πρώτα πρέπει να αναγνωριστεί θετικά μια οντότητα και μετά να της ανατεθούν τα αντίστοιχα δικαιώματα ανάλογα με το ρόλο της στο σύστημα.

3.1.1.3 Αναγνώριση

Η αναγνώριση έχει οριστεί ως απαίτηση που ικανοποιεί την ιδιωτικότητα, αφενός μεν της εξωτερικής οντότητας που ζητά να αποκτήσει πρόσβαση σε μια υπηρεσία ή να προσπελάσει ένα σύνολο δεδομένων αυτής, αφετέρου των οντοτήτων των οποίων τα προσωπικά δεδομένα είναι αποθηκευμένα στο σύστημα.

Συγκεκριμένα, από την πλευρά της εξωτερικής οντότητας, η διαδικασία της αναγνώρισης ελέγχει αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια, εξουσιοδότησή της ή όχι. Σε περίπτωση που δεν απαιτείται, προστατεύεται η ιδιωτικότητά της αφού επιστρέφονται τα αντίστοιχα δεδομένα ή η υπηρεσία που ζητήθηκε δίχως την παροχή προσωπικών δεδομένων από αυτή.
Από την πλευρά της προστασίας δεδομένων που είναι αποθηκευμένα σε ένα σύστημα, η διαδικασία της αναγνώρισης φροντίζει να μην επιτραπεί σε κανέναν μη εξουσιοδοτημένο χρήστη η πρόσβαση σε αυτά, προφυλάσσοντας έτσι την ιδιωτικότητα των κατόχων τους.

3.1.1.4 Προστασία Δεδομένων

Σκοπός της συγκεκριμένης απαίτησης είναι η ***προστασία των προσωπικών δεδομένων από επεξεργασία*** η οποία έρχεται σε αντίθεση με την ισχύουσα νομοθεσία.

Οι βασικές αρχές της ιδιωτικότητας που εκφράζονται από αντίστοιχους νόμους είναι οι ακόλουθες:

- ***Αρχή της νομιμότητας και της δικαιοσύνης (Principle of Lawfulness and Fairness):*** Τα προσωπικά δεδομένα πρέπει να συλλέγονται με νόμιμο και δίκαιο τρόπο.
- ***Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν (Principle of the Purpose Specification and Purpose Building):*** Ο σκοπός που συλλέγονται τα προσωπικά δεδομένα πρέπει να είναι σαφώς καθορισμένος και να συνάδει με τη νομοθεσία. Η επεξεργασία των δεδομένων πρέπει να διεξάγεται μόνο για το σκοπό για τον οποίο συγκεντρώθηκαν.
- ***Αρχή της Αναγκαιότητας της Συλλογής και της Επεξεργασίας των Δεδομένων (Principle of Necessity of Data Collection and Processing***): Η συλλογή και η επεξεργασία των προσωπικών δεδομένων πρέπει να επιτρέπονται μόνο στις περιπτώσεις που ο συλλέγων πράττει ενέργειες αντίστοιχες με το σκοπό συλλογής των δεδομένων, αποδεικνύοντας έτσι την αναγκαιότητα, αφού για την εκτέλεση των ενεργειών χρειάζεται τα δεδομένα αυτά.
- ***Παροχή Πληροφόρησης, Ενημέρωσης και Πρόσβασης στα Υποκείμενα των ευαίσθητων Δεδομένων (Information, Notification and Access Rights of the Data Subjects):*** Τα υποκείμενα των δεδομένων πρέπει να έχουν το δικαίωμα της πληροφόρησης και της ενημέρωσης για τα προσωπικά τους δεδομένα, καθώς και το δικαίωμα της πρόσβασης, της διόρθωσης, της διαγραφής ή και του αποκλεισμού των δεδομένων τους σε περιπτώσεις που εκείνα κρίνουν αναγκαίο.
- ***Αρχή της Ασφάλειας και της Ακρίβειας (Principle of Security and Accuracy***): Επιβάλλει την ύπαρξη κατάλληλων μηχανισμών και τεχνολογιών για τη διασφάλιση της εμπιστευτικότητας, της ακρίβειας και της διαθεσιμότητας των προσωπικών δεδομένων, ούτως ώστε να παραμένουν ασφαλή, ενημερωμένα και ακέραια.
- ***Εποπτεία και Κύρωση (Supervision and Sanctions):*** Προβλέπει τη σύσταση Ανεξάρτητης Αρχής Προστασίας Δεδομένων, με σκοπό την επίβλεψη και την παρατήρηση της εφαρμογής των κανόνων ιδιωτικότητας. Η ίδια Αρχή θα είναι υπεύθυνη και για την επιβολή κυρώσεων στις περιπτώσεις που σημειώνονται αποκλίσεις από τη νομιμότητα.

3.1.1.5 Ανωνυμία

Μια από τις βασικές απαιτήσεις προστασίας της ιδιωτικότητας ενός χρήστη είναι η δυνατότητά του να μπορεί να παραμένει ανώνυμος. Η ***ανωνυμία*** διασφαλίζει ότι ένας χρήστης μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει την ταυτότητά του.

Ανάλογα με το ρόλο που έχει ο χρήστης σε κάθε επικοινωνία έχουν καθοριστεί δύο μορφές υλοποίησης της ανωνυμίας: ***η ανωνυμία του αποστολέα*** (*sender anonymity*) και ***η ανωνυμία του παραλήπτη*** (*receiver anonymity*). Η ανωνυμία του αποστολέα σημαίνει ότι σε μια επικοινωνία, ο χρήστης που έχει το ρόλο του αποστολέα παραμένει ανώνυμος, ενώ ο παραλήπτης όχι. Αντίστοιχα, η ανωνυμία του παραλήπτη σημαίνει τη διαφύλαξη της ανωνυμίας του παραλήπτη παρά του αποστολέα.

Για το χρήστη που στέλνει/λαμβάνει σε μια επικοινωνία υπάρχει ο όρος της ***τέλειας ανωνυμίας αποστολέα/παραλήπτη*** (*perfect sender/receiver anonymity*), που σημαίνει

ότι ο επιτιθέμενος δεν έχει τη δυνατότητα να ξεχωρίσει πότε ο αποστολέας/παραλήπτης συμμετέχει σε μια επικοινωνία και πότε όχι.

Το 2007 ο *Pfitzmann* όρισε λεπτομερέστερα την ανωνυμία ως ακολούθως: ***Ανωνυμία μιας οντότητας σημαίνει ότι αυτή δεν είναι αναγνωρίσιμη μέσα σε ένα σύνολο οντοτήτων, το σύνολο ανώνυμων οντοτήτων.*** Το σύνολο αυτό περιλαμβάνει όλες τις οντότητες που συμμετέχουν σε μια επικοινωνία και που πιθανόν θα μπορούσαν να αναγνωριστούν από διάφορους επιτιθέμενους.

3.1.1.6 Ψευδωνυμία

Η απαίτηση της ψευδωνυμίας έχει παρόμοια χαρακτηριστικά με αυτά της ανωνυμίας. Με την ***ψευδωνυμία*** προστατεύεται η αναγνώριση των χρηστών από τρίτες οντότητες. Στην ψευδωνυμία οι χρήστες χρησιμοποιούν ψευδώνυμα για να προστατέψουν την αποκάλυψη της ταυτότητάς τους. Το ψευδώνυμο είναι ένα αναγνωριστικό μιας οντότητας, διαφορετικό από το πραγματικό της όνομα.

Η ψευδωνυμία ορίζεται ως ***η απαίτηση που διασφαλίζει την απόκρυψη της ταυτότητας του χρήστη όταν αυτός ενεργεί στα πλαίσια μιας επικοινωνίας χρησιμοποιώντας ένα ή περισσότερα ψευδώνυμα.*** Η ψευδωνυμία υλοποιείται όταν δεν μπορεί να υλοποιηθεί η ανωνυμία, όπως σε περιπτώσεις όπου ο χρήστης πρέπει να είναι υπόλογος των πράξεών του.

Οι *Pfitzmann* και *Waidner* κατηγοριοποίησαν τα ψευδώνυμα σε δύο κατηγορίες: στα προσωπικά ψευδώνυμα (*personal pseudonyms*) και στα ψευδώνυμα ρόλων (*role pseudonyms*).

Ένα ψευδώνυμο αποκαλείται προσωπικό όταν ανήκει σε κάποιο χρήστη, ο οποίος το χρησιμοποιεί για προσωπική του χρήση σε διάφορες συναλλαγές για κάποια χρονική περίοδο. Άρα στην ουσία ένα προσωπικό ψευδώνυμο αντικαθιστά το όνομα του χρήστη.

Ένα ψευδώνυμο αποκαλείται ψευδώνυμο ρόλου, όταν σε αντίθεση με το προσωπικό ψευδώνυμο, δεν συνδέεται με το όνομα του χρήστη, αλλά με το ρόλο που αυτός έχει στα πλαίσια μιας συναλλαγής ή επικοινωνίας. Τα ψευδώνυμα αυτά προσφέρουν μεγαλύτερη προστασία από ότι τα προσωπικά, αφού ισχύουν για ένα συγκεκριμένο ρόλο του χρήστη που μετέχει σε μια συγκεκριμένη επικοινωνία.

3.1.1.7 Μη Συνδεσιμότητα

Η απαίτηση της ***μη συνδεσιμότητας*** προστατεύει την ιδιωτικότητα των χρηστών από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, κάτι που θα μπορούσε να οδηγήσει στην αποκάλυψη της ταυτότητας των πρώτων.

Το 2007 ο *Pfitzmann* όρισε τη μη συνδεσιμότητα ως ακολούθως: ***Δύο ή περισσότερες οντότητες (π.χ. χρήστες, μηνύματα, ενέργειες) είναι μη συνδέσιμες, από την πλευρά του επιτιθέμενου, αν μέσα στο ίδιο σύνολο οντοτήτων (ή στο ίδιο περιβάλλον που διεξάγεται η επικοινωνία) ο επιτιθέμενος δεν μπορεί να ξεχωρίσει αν αυτές οι οντότητες σχετίζονται μεταξύ τους ή όχι.***

3.1.1.8 Μη Παρατηρησιμότητα

Η απαίτηση της ***μη παρατηρησιμότητας*** προστατεύει την ιδιωτικότητα των χρηστών από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν τα ίχνη των πρώτων τη στιγμή που περιηγούνται το διαδίκτυο ή χρησιμοποιούν μια υπηρεσία.

Ο ορισμός της μη παρατηρησιμότητας είναι ο ακόλουθος (*Pfitzmann*): ***Μια οντότητα (π.χ. χρήστης, μήνυμα, ενέργεια) είναι μη παρατηρήσιμη σε ένα σύνολο οντοτήτων όταν: ο επιτιθέμενος δεν μπορεί να εντοπίσει την οντότητα αυτή και όταν ο κάτοχος της οντότητας αυτής παραμένει ανώνυμος σε σχέση με τους άλλους κατόχους των υπολοίπων οντοτήτων.***

3.1.2 Μέθοδοι Ανάλυσης Απαιτήσεων Ιδιωτικότητας

Οι επόμενες ενότητες περιγράφουν γνωστές μεθόδους ανάλυσης απαιτήσεων ιδιωτικότητας που έχουν προταθεί στους τομείς της ***τεχνολογίας των απαιτήσεων*** *(requirements engineering*) και της ***ασφάλειας πληροφοριακών συστημάτων*** *(information systems security*). Στην πλειονότητά τους μπορούν να θεωρηθούν γενικές μέθοδοι ανάλυσης απαιτήσεων, οι οποίες υποστηρίζουν τον προσδιορισμό και τη διαχείριση τόσο των λειτουργικών όσο και των μη λειτουργικών απαιτήσεων στα πρώτα στάδια της διαδικασίας σχεδίασης ενός συστήματος.

Ο λόγος που εστιάζουμε στις συγκεκριμένες μεθόδους είναι ότι εμπεριέχουν κατάλληλες έννοιες για τη σαφή αναπαράσταση των απαιτήσεων ασφάλειας (στις οποίες συμπεριλαμβάνονται και οι απαιτήσεις ιδιωτικότητας), καθώς και για τον τρόπο που οι απαιτήσεις αυτές μεταφράζονται σε συγκεκριμένες λειτουργίες του υπό ανάπτυξη συστήματος.

Οι μέθοδοι που θα εξεταστούν είναι:

- Η μέθοδος *NFR (Non-Functional Requirement Framework)*
- Η μέθοδος *i*
- Η μέθοδος *Tropos*
- Η μέθοδος *KAOS*
- Η μέθοδος *GBRAM (Goal-Based Requirements Analysis Method)*
- Η μέθοδος *RBAC (Role-Based Access Control)*
- Η μέθοδος *M-N (Moffet-Nusseibeh Framework)*
- Η μέθοδος *B-S (Bellotti-Sellen Framework)*
- Η μέθοδος *STRAP (STRuctured Analysis for Privacy)*
- Η μέθοδος *PriS (Privacy Safeguard)*

3.1.2.1 Η Μέθοδος *NFR*

Στόχος της *NFR* είναι η συστηματική καταγραφή της διαδικασίας σχεδίασης ενός συστήματος, μέσω των αλληλένδετων σχεδιαστικών αποφάσεων σχετικών με τον τρόπο της βέλτιστης ικανοποίησης των μη λειτουργικών του απαιτήσεων (*non-functional requirements*) όπως είναι η ασφάλεια, η ακρίβεια και το κόστος. Η μέθοδος *NFR* μπορεί να εφαρμοστεί σε όλες τις φάσεις της ανάπτυξης ενός συστήματος, κατά κύριο λόγο όμως έχει χρησιμοποιηθεί στα αρχικά στάδια της ανάλυσης απαιτήσεων.

Ο τρόπος που η *NFR* διαχειρίζεται τις απαιτήσεις ασφάλειας βασίζεται στην έννοια του στόχου. Συγκεκριμένα, η *NFR* αναπαριστά τις απαιτήσεις ασφάλειας ως ανεκτικούς στόχους (*softgoals*) που πρέπει να ικανοποιηθούν ώστε το σύστημα να θεωρηθεί ασφαλές. Η διαδικασία ικανοποίησης των στόχων αυτών μπορεί να ιδωθεί σαν τη σταδιακή κατασκευή, αποσαφήνιση και αναθεώρηση ενός γραφήματος που απεικονίζει τους στόχους αυτούς και τις μεταξύ τους αλληλεξαρτήσεις. Οι αλληλεξαρτήσεις αυτές

εκφράζουν την ιεραρχική εκλέπτυνση των γενικών (στρατηγικών) στόχων σε πιο συγκεκριμένους (λειτουργικούς) στόχους, οι οποίοι τελικά συνδέονται με συγκεκριμένες λειτουργίες του συστήματος. Επίσης, εκφράζουν την επίδραση, θετική ή αρνητική που μπορεί να έχει η ικανοποίηση ενός στόχου στην ικανοποίηση άλλων στόχων που βρίσκονται στο ίδιο επίπεδο. Μέσω της ανάλυσης αυτής επιδιώκεται η βέλτιστη ικανοποίηση όλων των στόχων που έχουν τεθεί μέσω των λειτουργιών του συστήματος. Για τον υπολογισμό του συνολικού βαθμού ικανοποίησης των στόχων λαμβάνονται υπόψη τόσο οι συσχετίσεις μεταξύ των στόχων όσο και οι εκτιμήσεις των σχεδιαστών του συστήματος.

Ένα σημαντικό γνώρισμα της μεθόδου *NFR* είναι ότι η κατασκευή του γραφήματος των ανεκτικών στόχων καθοδηγείται από έτοιμους καταλόγους που καταγράφουν προκαθορισμένους τρόπους εκλέπτυνσης των στρατηγικών ανεκτικών στόχων σε λειτουργικούς, τις πιθανές αλληλεξαρτήσεις μεταξύ διαφόρων στόχων, καθώς και εναλλακτικούς τρόπους υλοποίησης των ανεκτικών στόχων από λειτουργίες του συστήματος. Οι κατάλογοι αυτοί έχουν προκύψει από την εμπειρία της εφαρμογής της μεθόδου *NFR* σε διαφορετικές περιπτώσεις ανάπτυξης συστημάτων. Παράλληλα με τη μέθοδο, έχει φτιαχτεί εργαλείο λογισμικού το *Organization Model Environment (OME)*, το οποίο παρέχει ένα γραφικό περιβάλλον που βοηθά στην εφαρμογή της μεθόδου.

3.1.2.2 Η Μέθοδος *i*

Η μέθοδος *i* εφαρμόζεται στα αρχικά στάδια της σχεδίασης συστημάτων με σκοπό την αποτύπωση της λογικής και του περιεχομένου ενός οργανισμού, εστιάζοντας στις δρώσες οντότητες του οργανισμού (*agents*) και στις μεταξύ τους αλληλεξαρτήσεις. Η μέθοδος αναπτύχθηκε αρχικά σαν ένα εργαλείο μοντελοποίησης, ανάλυσης και επανασχεδιασμού των επιχειρηματικών διαδικασιών. Πρόσφατα χρησιμοποιήθηκε και για τη μοντελοποίηση απαιτήσεων ασφάλειας και ιδιωτικότητας. Οι απαιτήσεις ασφάλειας στη μέθοδο αυτή αναπαρίστανται ως ανεκτικοί στόχοι, έννοια η οποία αναφέρεται και στη μέθοδο *NFR*. Αντίθετα όμως με την *NFR*, η μέθοδος *i* δεν επικεντρώνεται σε καθολικούς στόχους του οργανισμού, αλλά στους επιμέρους στόχους που έχουν οι δρώσες οντότητες του συστήματος. Συγκεκριμένα, οι δρώσες οντότητες είναι αλληλοσχετιζόμενες υπό την έννοια ότι για να πετύχουν τους στόχους τους εξαρτώνται από εργασίες που εκτελούνται από άλλες δρώσες ή από πόρους που μοιράζονται με άλλες δρώσες οντότητες.

Μετά την αρχική κατασκευή ενός μοντέλου πεδίου *(domain model*) όπου απεικονίζονται οι εμπλεκόμενες δρώσες οντότητες και οι μεταξύ τους αλληλεξαρτήσεις, αναλύεται η ασφάλεια του συστήματος με τη χρήση διαφορετικών τεχνικών. Αυτές στοχεύουν στην αναγνώριση των πιθανών επιτιθέμενων και των κινδύνων που παρουσιάζουν, στον προσδιορισμό των αδυναμιών που προκύπτουν από τις αλληλεξαρτήσεις μεταξύ των οντοτήτων, καθώς και στην αναγνώριση των πιθανών λύσεων για την αντιμετώπιση των κινδύνων και των αδυναμιών. Αποτέλεσμα της παραπάνω ανάλυσης είναι η εκλέπτυνση και η προσαρμογή των ανεκτικών στόχων των οντοτήτων. Αφού ολοκληρωθεί η παραπάνω διαδικασία για όλες τις δρώσες οντότητες, αξιολογείται κατά πόσο ο συνολικός βαθμός ασφάλειας είναι ικανοποιητικός. Τέλος, γίνεται ανάλυση των ρόλων που έχουν οι δρώσες οντότητες με βάση τις εργασίες που εκτελούν και τους πόρους που χρησιμοποιούν καταλήγοντας έτσι σε ένα μοντέλο που περιγράφει τη λειτουργία του συστήματος. Η μέθοδος *i* χρησιμοποιεί όπως και η *NFR* το εργαλείο *OME*.

3.1.2.3 Η Μέθοδος *TROPOS*

Η μέθοδος αυτή βοηθά στην περιγραφή των πληροφοριακών συστημάτων και του εργασιακού περιβάλλοντος του οργανισμού στον οποίο εντάσσονται και λειτουργούν.

Εφαρμόζεται σε όλες τις φάσεις ανάπτυξης ενός συστήματος, υιοθετώντας έναν ομοιογενή τρόπο εργασίας από τη φάση της ανάλυσης απαιτήσεων ως τη φάση του σχεδιασμού και της υλοποίησης του συστήματος. Το μοντέλο περιγραφής του οργανισμού βασίζεται σε αυτό της μεθόδου *i*, υιοθετώντας τις βασικές έννοιες όπως δρώντες, στόχοι, εργασίες, πόροι και εξαρτήσεις. Επιπλέον χρησιμοποιεί τον όρο ασφαλής οντότητα για να περιγράψει κάθε στόχο ή εργασία που σχετίζεται με την ασφάλεια του συστήματος. Οι ασφαλείς στόχοι αναπαριστούν τις απαιτήσεις ασφάλειας των οντοτήτων. Μια ασφαλής εργασία περιγράφει έναν τρόπο ικανοποίησης του ασφαλούς στόχου. Τέλος, μια ασφαλής εξάρτηση ορίζει έναν περιορισμό στη σχέση μεταξύ δύο οντοτήτων.

Η μέθοδος διαχειρίζεται τις απαιτήσεις ασφάλειας σε όλες τις φάσεις ανάπτυξης λογισμικού με τον ακόλουθο τρόπο. Στη φάση της ανάλυσης των απαιτήσεων παράγεται το μοντέλο του οργανισμού, το οποίο περιγράφει τους δρώντες, τις συσχετίσεις τους και τους περιορισμούς ασφάλειας που εφαρμόζονται σε αυτές. Στη συνέχεια, στη φάση του σχεδιασμού της αρχιτεκτονικής του συστήματος, περιγράφονται οι ασφαλείς οντότητες που εγγυώνται την ικανοποίηση των παραπάνω περιορισμών και προδιαγράφονται τα υποσυστήματα που υλοποιούν τις ασφαλείς οντότητες. Τέλος, στη φάση της λεπτομερούς σχεδίασης, κάθε μέρος της αρχιτεκτονικής ορίζεται και αναλύεται σε βάθος, μαζί με τις εισόδους, τις εξόδους και τις παραμέτρους ασφάλειας.

3.1.2.4 Η Μέθοδος *KAOS*

Είναι μια μέθοδος εύρεσης και τεκμηρίωσης απαιτήσεων που βασίζεται στην έννοια του στόχου. Συγκεκριμένα, ξεκινά με τον προσδιορισμό των αφηρημένων- υψηλού επιπέδου στόχων του οργανισμού, οι οποίοι στη συνέχεια αναλύονται σε πιο συγκεκριμένους, κάποιες φορές εναλλακτικούς υποστόχους, καταλήγοντας έτσι στην κατασκευή μιας δενδρικής δομής στόχων, τα φύλλα της οποίας είναι στόχοι που μπορούν να ανατεθούν σε δρώσες οντότητες του υπό ανάπτυξη συστήματος.

Παράλληλα, αναγνωρίζονται τα εμπόδια (*obstacles*) τα οποία εντοπίζουν την υλοποίηση ενός ή περισσότερων στόχων ασφάλειας του οργανισμού. Όπως οι στόχοι, έτσι και τα εμπόδια αναλύονται με τη λογική του δέντρου δημιουργώντας ένα δέντρο εμποδίων. Με τον τρόπο αυτό μπορεί να εξαλειφθεί ένα εμπόδιο ευκολότερα, αφού είναι γνωστά τα υποεμπόδια από τα οποία αποτελείται. Επίσης τα εμπόδια που εντοπίζονται κατηγοριοποιούνται όπως επίσης και οι στόχοι του οργανισμού. Μέσω της κατηγοριοποίησης διευκολύνεται ο τρόπος εύρεσης των συσχετίσεων μεταξύ των εμποδίων και των στόχων που επηρεάζουν. Τέλος, αποφασίζεται ο τρόπος αντιμετώπισης των εμποδίων σε σχέση με τους στόχους που επηρεάζονται. Συγκεκριμένα, εξετάζονται τα εμπόδια του κάθε στόχου οι οποίοι αναπροσαρμόζονται ώστε να μπορέσουν να υλοποιηθούν χωρίς να απειλούνται από τα συγκεκριμένα εμπόδια. Η προσαρμογή μπορεί να σημαίνει τον επαναπροσδιορισμό των στόχων, των οντοτήτων που βρίσκονται σε δράση, την εισαγωγή νέων στόχων ή ακόμα και τον επανασχεδιασμό όλου του συστήματος. Σκοπός είναι η εξάλειψη όλων των εμποδίων που εντοπίστηκαν.

Η μέθοδος προσφέρει στους σχεδιαστές συστημάτων μια γλώσσα μοντελοποίησης, στρατηγικές επεξεργασίας απαιτήσεων, καθώς και υποστήριξη με τη μορφή εργαλείου λογισμικού.

3.1.2.5 Η Μέθοδος *GBRAM*

Είναι μια μέθοδος που επίσης βασίζεται στην ανάλυση των στόχων. Παρέχει ένα συστηματικό τρόπο καθορισμού και εκλέπτυνσης των στόχων που πρέπει να ικανοποιεί

ένα σύστημα, καθώς και για το χειρισμό των σχέσεων μεταξύ τους και για τη μετατροπή τους σε λειτουργικές απαιτήσεις.

Η μέθοδος αυτή έχει χρησιμοποιηθεί και για την ανάλυση των πολιτικών ιδιωτικότητας ηλεκτρονικών υπηρεσιών και το συστηματικό εντοπισμό απαιτήσεων ιδιωτικότητας που υπαγορεύονται από τις πρακτικές προστασίας της ιδιωτικότητας του οργανισμού. Η διαδικασία αυτή αναφέρεται ως *εξόρυξη των στόχων* (*goal mining*) και οι απαιτήσεις που προκύπτουν κατατάσσονται είτε ως στόχοι προστασίας (*protection goals*) είτε ως αδυναμίες (*vulnerabilities*). Οι στόχοι προστασίας εκφράζουν τις προσπάθειες του οργανισμού να σεβαστούν την ιδιωτικότητα των πελατών του, ενώ οι αδυναμίες αντικατοπτρίζουν τους πιθανούς κινδύνους της ιδιωτικότητας των πελατών που προκύπτουν από τις πρακτικές συλλογής και αποθήκευσης προσωπικών δεδομένων. Στη συνέχεια οι στόχοι της ιδιωτικότητας μετατρέπονται σε λειτουργικές απαιτήσεις, χρησιμοποιώντας κατάλληλες τεχνικές, όπως η ανάλυση σεναρίων, ο εντοπισμός εμποδίων και περιορισμών καθώς και στρατηγικές εκλέπτυνσης όπως εμπειρικοί κανόνες, οδηγίες και επαναλαμβανόμενοι τύποι ερωτήσεων. Τέλος, αξιολογείται η συνέπεια ανάμεσα στις απαιτήσεις του συστήματος και στις εκφρασμένες πολιτικές του οργανισμού, ενώ πιθανές αναντιστοιχίες εντοπίζονται και επιλύονται.

3.1.2.6 Η Μέθοδος *RBAC*

Έχει στόχο τον εντοπισμό των απαιτήσεων ιδιωτικότητας ενός οργανισμού. Συγκεκριμένα, στοχεύει στη μετατροπή των απαιτήσεων ιδιωτικότητας ενός οργανισμού σε ***πολιτικές ελέγχου πρόσβασης*** (*access control policies*) γεφυρώνοντας έτσι το κενό μεταξύ των «γενικών» απαιτήσεων και των «συγκεκριμένων» πολιτικών υλοποίησής τους, δηλαδή συγκεκριμένων ενεργειών που πρέπει να υλοποιηθούν προκειμένου να ικανοποιηθεί κάποια απαίτηση.

Η *RBAC* αναπαριστά τις απαιτήσεις ιδιωτικότητας ως εργασίες που πρέπει να υλοποιήσουν οι δρώσες οντότητες του οργανισμού. Για τον εντοπισμό των απαιτήσεων ιδιωτικότητας η μέθοδος συνδυάζει τεχνικές ανάλυσης στόχων και καθορισμού ρόλων ως εξής: Πρώτα δημιουργείται ένα μοντέλο βασισμένο στο περιεχόμενο του οργανισμού στο οποίο περιγράφονται οι δρώσες οντότητες του οργανισμού. Έπειτα, αναγνωρίζονται οι ρόλοι που αυτές επιτελούν. Για τον κάθε ρόλο εντοπίζονται οι στόχοι που αυτός επιτελεί. Για την επίτευξη ενός στόχου ορίζονται οι συνθήκες που πρέπει να ισχύουν. Οι πολιτικές ιδιωτικότητας ορίζονται βάσει των συνθηκών που πρέπει να ισχύουν ώστε μια οντότητα να μπορέσει να επιτελέσει ένα συγκεκριμένο στόχο μέσα από ένα ρόλο της σε σχέση με μια άλλη οντότητα ή έναν πόρο του οργανισμού.

Η *RBAC* δεν υποστηρίζεται από φορμαλιστικά μοντέλα.

3.1.2.7 Η Μέθοδος *M-N*

Στόχος της μεθόδου αυτής είναι η εύρεση και η ανάλυση των απαιτήσεων ασφάλειας στα πρώτα βήματα της σχεδίασης συστημάτων. Χρησιμοποιεί ένα μεταμοντέλο βασισμένο στο εννοιολογικό μοντέλο της μεθόδου *KAOS* που περιγράφηκε προηγουμένως, αλλά προτείνει έναν διαφορετικό τρόπο εργασίας. Επιπλέον, από το χώρο της ασφάλειας υιοθετεί τις έννοιες του αγαθού (*asset*) καθώς και της απειλής (*threat*) που στοχεύει στην ολική ή μερική καταστροφή του αγαθού. Οι στόχοι ασφάλειας αποσκοπούν στην προστασία των αγαθών και τις απειλές.

Η εφαρμογή της μεθόδου περιλαμβάνει δύο βήματα. Στο πρώτο, εφαρμόζονται τεχνικές ανάλυσης και διαχείρισης της επικινδυνότητας με σκοπό τον εντοπισμό των αγαθών και των πιθανών απειλών σε αυτά. Στη συνέχεια ορίζονται οι γενικοί στόχοι ασφάλειας του συστήματος που αντιστοιχούν στις απειλές που αναγνωρίστηκαν προηγουμένως. Η

ανάλυση των στόχων αυτών και η μετατροπή τους σε περιορισμούς των λειτουργικών απαιτήσεων του συστήματος γίνονται με βάση τη μέθοδο *KAOS*. Η συγκεκριμένη μέθοδος δεν υποστηρίζεται από φορμαλιστικά μοντέλα ή από εργαλεία λογισμικού.

3.1.2.8 Η Μέθοδος *B-S*

Οι *Bellotti* και *Sellen* ανέπτυξαν τη μέθοδο *B-S*, σκοπός της οποίας είναι η εύρεση των απαιτήσεων ιδιωτικότητας στη φάση της σχεδίασης συστημάτων και συγκεκριμένα στα αρχικά στάδια της φάσης του καθορισμού των απαιτήσεων ενός οργανισμού.

Οι απαιτήσεις ιδιωτικότητας περιγράφονται στη μέθοδο αυτή με τη μορφή κριτηρίων ιδιωτικότητας που θα πρέπει να ακολουθεί ο σχεδιαστής για να καθορίσει τις αδυναμίες του εκάστοτε οργανισμού προτείνοντας στη συνέχεια πιθανές λύσεις για την αντιμετώπιση των αδυναμιών.

Ο τρόπος εντοπισμού των απαιτήσεων ιδιωτικότητας στην μέθοδο αυτή είναι ο ακόλουθος. Οι σχεδιαστές αξιολογούν τον εκάστοτε οργανισμό βάσει της λίστας κριτηρίων ιδιωτικότητας που ορίζει η μέθοδος. Η μέθοδος ορίζει επίσης μια σειρά ερωτημάτων που μπορεί να κάνει ο σχεδιαστής στο προσωπικό του οργανισμού, ώστε να μπορέσει ευκολότερα να αποτυπώσει και να αξιολογήσει την κατάσταση του οργανισμού. Αφού ληφθούν οι απαντήσεις, καταγράφονται οι αδυναμίες του οργανισμού και αποφασίζει ο σχεδιαστής τον τρόπο αναπαράστασής τους.

Η μέθοδος αυτή δεν υποστηρίζεται από φορμαλιστικά μοντέλα ή από κάποιο εργαλείο λογισμικού.

3.1.2.9 Η Μέθοδος *STRAP*

Αναπτύχθηκε με σκοπό την εύρεση και την ανάλυση των απαιτήσεων ιδιωτικότητας στη φάση της σχεδίασης ενός συστήματος. Χαρακτηριστικό της συγκεκριμένης μεθόδου είναι η χρήση διάφορων τεχνικών από το χώρο της σχεδίασης και της ασφάλειας των συστημάτων.

Οι απαιτήσεις ιδιωτικότητας στη *STRAP* αναπαρίστανται με τη μορφή αδυναμιών. Η *STRAP* χρησιμοποιεί την έννοια του στόχου για την αποτύπωση των λειτουργικών απαιτήσεων του οργανισμού. Στο μοντέλο των στόχων που δημιουργείται αποτυπώνονται οι αδυναμίες με τη μορφή εμποδίων ανάμεσα στους στόχους και στους υποστόχους.

Ο τρόπος που ακολουθεί η μέθοδος για τον εντοπισμό και την αποτύπωση των απαιτήσεων ιδιωτκότητας αναλύεται στα ακόλουθα βήματα: ***Ανάλυση*** (*Analysis),* ***Επαναπροσδιορισμός*** (*Refinement*), ***Αξιολόγηση*** (*Evaluation),* και ***Επανάληψη*** (*Iteration*). Αρχικά πραγματοποιείται ***ανάλυση των στόχων του συστήματος***. Αποτέλεσμα αυτής της ανάλυσης είναι η αναγνώριση των στόχων, των ενεργών οντοτήτων καθώς και των βασικών συστατικών του συστήματος. Επίσης συγκεντρώνονται πληροφορίες σχετικές με το περιεχόμενο του υπό ανάπτυξη συστήματος και καταγράφονται οι πρώτες απαιτήσεις σχετικά με τη διαφύλαξη της ιδιωτικότητας. Οι αδυναμίες καταγράφονται στο διάγραμμα των στόχων με τη μορφή εμποδίων και κατηγοριοποιούνται με βάση τις βέλτιστες πρακτικές χρήσης υπηρεσιών πληροφορικής (*fair information practices).*

Στη φάση του επαναπροσδιορισμού λαμβάνεται η απόφαση εξάλειψης και μείωσης των αδυναμιών, οι οποίες αν και αναγνωρίστηκαν έχουν λύσεις τόσο απλές ώστε δεν απαιτείται να συνεχίσουν να απασχολούν τους σχεδιαστές. Για τις αδυναμίες αυτές καταγράφονται οι λύσεις υλοποίησής τους και διαγράφονται από τη λίστα αδυναμιών του συστήματος.

Στη φάση της αξιολόγησης, αξιολογούνται τα διάφορα προτεινόμενα σενάρια σχεδίασης του συστήματος. Πρώτα αξιολογείται ο τρόπος που κάθε πρόταση σχεδίασης του συστήματος αναφέρει για την αντιμετώπιση των αδυναμιών του συστήματος. Το σενάριο που μειώνει περισσότερο την επικινδυνότητα, διασφαλίζοντας όσο γίνεται καλύτερα την ιδιωτικότητα, θεωρείται αποδοτικότερο σε σχέση με άλλα σενάρια. Η *STRAP* προτείνει μια σειρά από κριτήρια που καθοδηγούν τη φάση της αξιολόγησης.

Στη φάση της επανάληψης, επαναλαμβάνονται τα προηγούμενα βήματα για να μελετηθεί εκ νέου η σχεδίαση του συστήματος. Μελετάται εκ νέου η δομή των στόχων, γίνονται οι απαραίτητες αλλαγές, επαναπροσδιορίζονται οι αδυναμίες, αξιολογούνται τα νέα σενάρια μείωσης της επικινδυνότητας κ.λπ. Η φάση της επανάληψης ολοκληρώνεται όταν δεν υπάρχουν πλέον αλλαγές/βελτιώσεις στις προηγούμενες τρεις φάσεις.

3.1.2.10 Η Μέθοδος *PriS*

Η μέθοδος αυτή περιλαμβάνει μια σειρά από έννοιες που σκοπό έχουν την εφαρμογή των απαιτήσεων ιδιωτικότητας στις δραστηριότητες ενός οργανισμού και στην παροχή ενός συστηματικού τρόπου εύρεσης ορθών μοντέλων συστημάτων που να υλοποιούν τις απαιτήσεις αυτές.

Η μέθοδος αυτή συμβολίζει τις απαιτήσεις της ιδιωτικότητας ως έναν ειδικό τύπο στόχου, τον στόχο της ιδιωτικότητας (*privacy goal*).

Οι στόχοι ιδιωτικότητας δημιουργούνται από διάφορα ζητήματα προστασίας της ιδιωτικότητας και αντιστοιχούν στις οχτώ βασικές παραμέτρους ιδιωτικότητας που αναφέρθηκαν στην ***ενότητα 3.1.1***. Οι στόχοι πραγματοποιούνται από τις διεργασίες του οργανισμού. Η διαδικασία μετάβασης από τους στόχους στις διεργασίες περιλαμβάνει το μετασχηματισμό των γενικών στόχων του οργανισμού σε έναν ή περισσότερους υποστόχους οι οποίοι αποτελούν το μέσο για να αποκτηθεί η σύνδεση μεταξύ των γενικών στόχων και των διεργασιών. Η μεθοδολογική προσέγγιση της μεθόδου περιλαμβάνει τέσσερα στάδια. ***Στο πρώτο στάδιο*** γίνεται η καταγραφή των απόψεων από επιλεγμένα στελέχη του οργανισμού που έχουν την ευθύνη λήψης αποφάσεων με στόχο την ανάλυση των απόψεων σχετικά με τη λειτουργία του οργανισμού, τον καθορισμό των ζητημάτων που αφορούν την ιδιωτικότητα και τον εντοπισμό των απαιτήσεων ιδιωτικότητας που πρέπει να ληφθούν υπόψη για τη σωστή λειτουργία του οργανισμού. ***Το δεύτερο στάδιο*** περιλαμβάνει δύο φάσεις. Στην πρώτη φάση αναγνωρίζεται η επίδραση των απαιτήσεων ιδιωτικότητας στους γενικότερους στόχους του οργανισμού, ενώ στη δεύτερη φάση αναλύεται η επίδραση των αλλαγών των διεργασιών που τις υλοποιούν εξαιτίας των απαιτήσεων ιδιωτικότητας. ***Στο τρίτο στάδιο*** και μετά τον εντοπισμό των διεργασιών που επηρεάζονται από τις απαιτήσεις ιδιωτικότητας, ακολουθεί η διαμόρφωση των συγκεκριμένων διεργασιών με βάση τα πρότυπα (*patterns*) ιδιωτικότητας. Τα πρότυπα αυτά είναι γενικευμένα μοντέλα διεργασιών τα οποία περιέχουν ενέργειες, καθώς και ροές δεδομένων μεταξύ των ενεργειών και παρουσιάζουν τον τρόπο με τον οποίο θα πρέπει να λειτουργεί ένας οργανισμός σε συγκεκριμένο, κάθε φορά, τμήμα του. ***Στο τελευταίο στάδιο*** προσδιορίζεται ποιά είναι η πιο ενδεδειγμένη τεχνολογία που μπορεί να υλοποιήσει τις διεργασίες που επηρεάζονται από τις παραμέτρους της ιδιωτικότητας, όπως αυτές έχουν ήδη οριστεί από τα προηγούμενα στάδια.

Η *Pris* βοηθά τόσο στην εφαρμογή των απαιτήσεων στις δραστηριότητες ενός οργανισμού όσο και στην παροχή ενός συστηματικού τρόπου εύρεσης ορθών μοντέλων συστημάτων για την υλοποίηση των απαιτήσεων. Ο τρόπος λειτουργίας της *Pris*

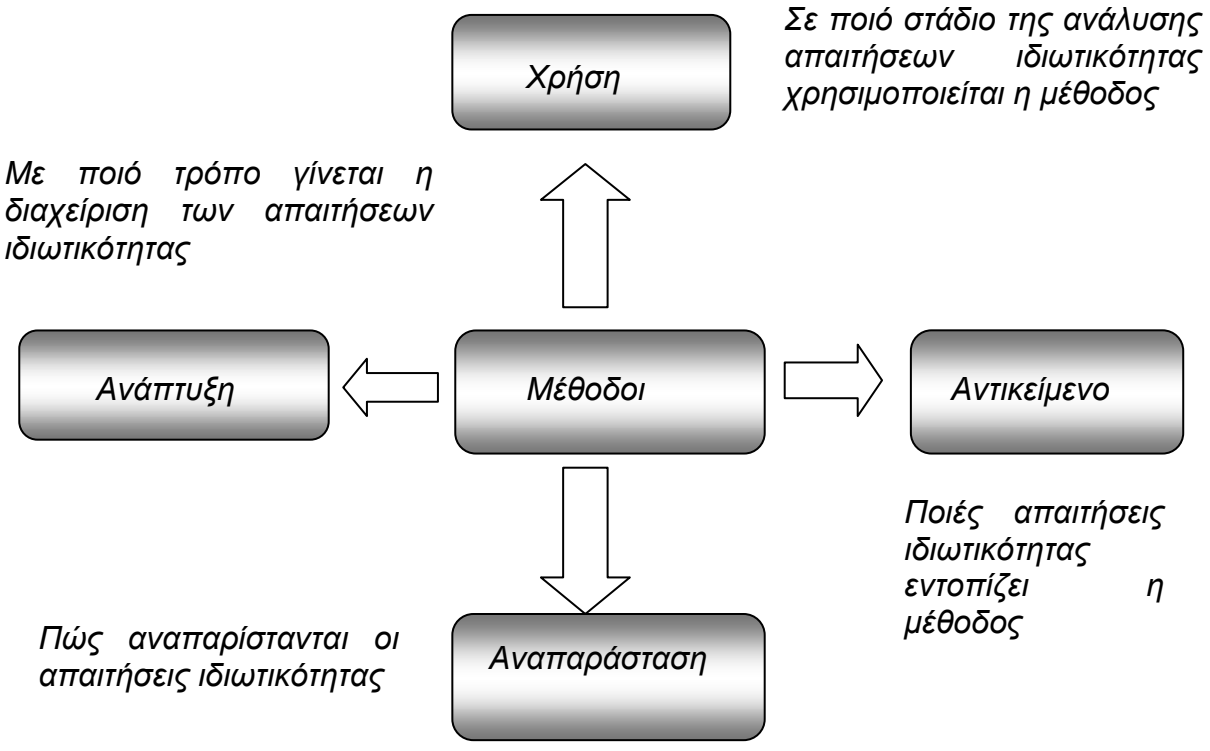
υποθέτει ότι οι στόχοι ιδιωτικότητας αποτελούν στρατηγικούς στόχους του οργανισμού και άρα εμφανίζονται στο υψηλότερο επίπεδο της ιεραρχίας των στόχων. Η μέθοδος απεικονίζεται φορμαλιστικά και διαγραμματικά. Επίσης, έχει κατασκευαστεί εργαλείο λογισμικού για την καθοδήγηση των σχεδιαστών και την αυτοματοποίηση του τρόπου λειτουργίας της.

3.1.3 Σύγκριση των Μεθόδων Ανάλυσης Απαιτήσεων Ιδιωτικότητας

Στην παρούσα ενότητα αναλύονται οι παραπάνω μέθοδοι, με σκοπό την ανάδειξη των χαρακτηριστικών τους όσον αφορά στη σχεδίαση και στην υλοποίηση των απαιτήσεων της ιδιωτικότητας σε ένα σύστημα.

Για το σκοπό της ανάλυσης, χρησιμοποιείται ένα πλαίσιο ***(σχήμα 8)*** που εξετάζει τις μεθόδους υπό τέσσερις οπτικές, οι οποίες βασίζονται στις τέσσερις βασικές παραμέτρους που συμμετέχουν στην σχεδίαση συστημάτων:

- ***Χρήση:*** Σε ποιό στάδιο της ανάλυσης απαιτήσεων χρησιμοποιείται η μέθοδος,
- ***Αντικείμενο:*** Ποιές κατηγορίες απαιτήσεων ιδιωτικότητας εντοπίζονται**,**
- ***Αναπαράσταση:*** Πώς αναπαρίστανται οι απαιτήσεις ιδιωτικότητας,
- ***Ανάπτυξη:*** Με ποιό τρόπο γίνεται η διαχείριση των απαιτήσεων ιδιωτικότητας.



Σχήμα 8: Πλαίσιο σύγκρισης μεθόδων

Κάθε παράμετρος αναλύεται σε περαιτέρω κριτήρια. Συγκεκριμένα, στην κατηγορία της χρήσης εξετάζονται τα ακόλουθα: **α)** Εύρεση των απαιτήσεων ιδιωτικότητας, **β)** Διαχείριση απαιτήσεων ιδιωτικότητας**, γ)** Επαλήθευση των απαιτήσεων ιδιωτικότητας. Αναλυτικότερα εξετάζεται αν οι μέθοδοι χρησιμοποιούν ή όχι κάποιες τεχνικές για την ανακάλυψη/συλλογή των απαιτήσεων ιδιωτικότητας, κατά πόσο ορίζουν συγκεκριμένες διαδικασίες εκλέπτυνσης των απαιτήσεων ιδιωτικότητας και ανάλυσης των μεταξύ τους σχέσεων, καθώς και αν γίνεται επαλήθευση των απαιτήσεων αυτών.

Στη δεύτερη κατηγορία εξετάζεται το αντικείμενο των μεθόδων υπό τα ακόλουθα τρία κριτήρια: **α)** Απαιτήσεις ιδιωτικότητας του οργανισμού, **β)** Πολιτικές ασφάλειας και **γ)** Τεχνολογίες υλοποίησης ασφάλειας. Πολλές μέθοδοι εστιάζουν μόνο στον προσδιορισμό των απαιτήσεων ιδιωτικότητας. Άλλες όμως προχωρούν και στον καθορισμό πολιτικών ιδιωτικότητας, δηλαδή στον καθορισμό συγκεκριμένων δικαιωμάτων πρόσβασης στα δεδομένα. Τέλος, κάποιες εστιάζουν στον εντοπισμό κατάλληλων τεχνικών λύσεων για την υλοποίηση των απαιτήσεων.

Η κατηγορία της αναπαράστασης εξετάζει τον τρόπο με τον οποίο εκφράζονται οι έννοιες της ιδιωτικότητας. Συνήθως υπάρχουν δύο τρόποι αναπαράστασης: η διαγραμματική και η φορμαλιστική. Από αυτούς τους τρόπους προκύπτουν και τα κριτήρια της κατηγορίας αυτής: **α)** Διαγραμματική αναπαράσταση**, β)** Φορμαλιστική γλώσσα.

Τέλος η κατηγορία της ανάπτυξης εξετάζει την ύπαρξη κατάλληλων βοηθημάτων εφαρμογής των μεθόδων. Δηλαδή εξετάζονται η ύπαρξη εργαλείων μοντελοποίησης, καθώς και η παροχή καθοδήγησης για την διαδικασία μοντελοποίησης των απαιτήσεων ιδιωτικότητας. Τα κριτήρια της κατηγορίας αυτής είναι: **α)** Καθοδήγηση και **β)** Εργαλεία.

3.1.4 Επίλογος

Η ιδιωτικότητα είναι διεθνώς αναγνωρισμένη ως ανθρώπινο δικαίωμα που πρέπει να προστατεύεται από τις κοινωνίες στις οποίες συμμετέχουν και δραστηριοποιούνται οι άνθρωποι. Καθημερινά, όλο και περισσότεροι χρήστες αξιοποιούν το διαδίκτυο, αφού οι υπηρεσίες που προσφέρει διευκολύνουν κατά πολύ τον τρόπο και την ποιότητα ζωής τους. Η ραγδαία αύξηση των χρηστών οδήγησε τους παρόχους διαδικτυακών υπηρεσιών, με σκοπό την καλύτερη εξυπηρέτηση των χρηστών και την καθιέρωση και καταξίωσή τους με στόχο το κέρδος.

Η γρήγορη αυτή εξέλιξη, σε συνδυασμό με την αυξανόμενη χρήση των υπηρεσιών που παρέχονται από το διαδίκτυο, οδήγησε στη δημιουργία επισφαλών πληροφοριακών συστημάτων και εφαρμογών καθώς και επισφαλών διαύλων επικοινωνίας μεταξύ των εφαρμογών αυτών και των χρηστών.

Τα ζητήματα της ιδιωτικότητας δε λαμβάνονται υπόψη εξίσου σε όλες τις φάσεις της σχεδίασης συστημάτων. Οι απαιτήσεις ασφάλειας και ιδιωτικότητας πρέπει να αναλύονται εκτενώς κατά τη φάση της σχεδίασης ώστε οι αδυναμίες να εντοπιστούν έγκαιρα και όχι κατά την υλοποίηση του συστήματος, όπου ο χρόνος και το κόστος επίλυσης των αδυναμιών είναι πολλαπλάσια. **[6]**

3.2 Η Διατήρηση των Δεδομένων Επικοινωνίας και η Διασφάλιση του Απορρήτου και της Ιδιωτικότητας

Ο όρος ***ηλεκτρονικές επικοινωνίες*** (*electronic communications*) καλύπτει ένα ευρύ φάσμα τηλεπικοινωνιακών τεχνολογιών, οι οποίες περιλαμβάνουν την παραδοσιακή σταθερή τηλεφωνία, την κινητή τηλεφωνία 2^{ης} γενιάς μέσω του Παγκόσμιου Συστήματος Κινητών Επικοινωνιών *(Global System for Mobile Communications, GSM)* και την κινητή τηλεφωνία 3^{ης} γενιάς μέσω του Ενοποιημένου Συστήματος Κινητών Τηλεπικοινωνιών (*Universal Mobile Telecommunication System, UMTS*). Επιπρόσθετα η εξέλιξη του διαδικτύου έχει οδηγήσει στη ραγδαία εξάπλωση τεχνολογιών επικοινωνίας, όπως είναι το σύστημα ηλεκτρονικού ταχυδρομείου καθώς και περισσότερο πρόσφατες τεχνολογίες τηλεφωνίας διαδικτύου, κυρίως μέσω του Πρωτοκόλλου Αρχικοποίησης Συνόδου (*Session Initiation Protocol, SIP*) και του Πρωτοκόλλου Φωνής μέσω Διαδικτύου (*Voice over the Internet Protocol, VoIP).*

Για τη διασφάλιση του απορρήτου και της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες απαιτείται η προστασία δύο κατηγοριών δεδομένων επικοινωνίας:

- ***Των εσωτερικών δεδομένων (content data):*** Αποτελούν το πραγματικό περιεχόμενο της επικοινωνίας. Για παράδειγμα, στην περίπτωση διαδικτυακής επικοινωνίας μέσω του πρωτοκόλλου *TCP/IP*, τα εσωτερικά δεδομένα περιλαμβάνουν τα πραγματικά δεδομένα που ανταλλάσσονται και τα οποία περιλαμβάνονται στο πεδίο φορτίου δεδομένων (*payload field*).
- ***Των εξωτερικών δεδομένων (context data):*** Αποτελούν τα δεδομένα τα οποία χρησιμοποιούνται για τον έλεγχο και τη διευθυνσιοδότηση της επικοινωνίας. Στο προηγούμενο παράδειγμα της διαδικτυακής επικοινωνίας, τα εξωτερικά δεδομένα περιλαμβάνουν, μεταξύ άλλων, τη διεύθυνση *IP* της πηγής και του προορισμού, τον τύπο της επικοινωνίας κ.λπ.

Η αποκάλυψη των εσωτερικών δεδομένων της επικοινωνίας οδηγεί εξ ορισμού στην παραβίαση του απορρήτου της επικοινωνίας και της ιδιωτικότητας των μερών της επικοινωνίας. Όμως, η αποκάλυψη των εξωτερικών δεδομένων επίσης επηρεάζει το απόρρητο της επικοινωνίας, εφόσον μπορεί να οδηγήσει στην αποκάλυψη της ταυτότητας των μερών της επικοινωνίας, της χρονικής στιγμής που πραγματοποιήθηκε, της τοποθεσίας στην οποία βρίσκονται τα μέρη της επικοινωνίας, ενώ σε μερικές περιπτώσεις μπορεί να αποκαλύψει και πληροφορία η οποία σχετίζεται με το πραγματικό περιεχόμενο της επικοινωνίας. Στο διαδίκτυο για παράδειγμα, τα εξωτερικά δεδομένα μπορεί να αποκαλύψουν πληροφορία που σχετίζεται με το πραγματικό περιεχόμενο της επικοινωνίας, εφόσον η διεύθυνση *IP* του προορισμού είναι δυνατόν πολύ εύκολα να αποκαλύψει την ιστοσελίδα που προσπέλασε ο χρήστης και συνεπώς και το περιεχόμενο της επικοινωνίας.

Στις σύγχρονες κοινωνίες η διασφάλιση του απορρήτου και της ιδιωτικότητας στις τηλεπικοινωνίες προστατεύεται μέσω της νομοθεσίας. Πολλές χώρες της Ευρωπαϊκής Ένωσης έχουν αναθέσει σε Ανεξάρτητες Αρχές την ευθύνη για την κανονιστική ρύθμιση και τον έλεγχο του απορρήτου των επικοινωνιών (στην Ελλάδα αυτή η αρμοδιότητα έχει ανατεθεί στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, ΑΔΑΕ). Από την άλλη πλευρά, δημιουργούνται σταδιακά εθνικές και διακρατικές νομικές υποχρεώσεις προς τους παρόχους δικτύων ηλεκτρονικών επικοινωνιών, ώστε να διατηρούν τα δεδομένα επικοινωνίας των συνδρομητών τους για ορισμένο χρονικό διάστημα. Η συλλογή και η καταγραφή των δεδομένων θα πρέπει να γίνονται με βάση συγκεκριμένες πολιτικές ιδιωτικότητας οι οποίες συμβαδίζουν με το νομοθετικό πλαίσιο και έχουν κοινοποιηθεί από τους παρόχους στους συνδρομητές μέσω της γνωστοποίησης του

είδους των εξωτερικών δεδομένων που συλλέγονται και του τρόπου που αυτά θα υποστούν επεξεργασία. Η έναρξη οποιασδήποτε επικοινωνίας προϋποθέτει την συγκατάθεση και την συμφωνία του καταναλωτή με τους όρους που θέτουν οι συγκεκριμένες πολιτικές.

Ο σκοπός της διατήρησης επικεντρώνεται κατά κύριο λόγο στη δυνατότητα διερεύνησης εγκληματικών ενεργειών. Με αυτό τον τρόπο η διατήρηση των δεδομένων επιτρέπει στις διωκτικές αρχές να αιτούνται την άρση του απορρήτου των εξωτερικών δεδομένων επικοινωνίας των συνδρομητών για το χρονικό διάστημα κατά το οποίο διατηρούνται τα δεδομένα, ώστε να διεξαχθούν οι απαιτούμενες για τη διερεύνηση πιθανών εγκληματικών πράξεων έρευνες. Είναι προφανές ότι για τη διασφάλιση της ιδιωτικότητας των συνδρομητών απαιτείται σε πρώτη φάση ο καθορισμός των κανόνων και των προϋποθέσεων βάσει των οποίων ένας πάροχος ηλεκτρονικών επικοινωνιών θα παραδίδει τα διατηρούμενα δεδομένα ενός συνδρομητή του σε μια διωκτική αρχή, η οποία αιτείται αυτής της πρόσβασης. Σε δεύτερη φάση απαιτείται ο καθορισμός και η κοινοποίηση συγκεκριμένων πολιτικών ιδιωτικότητας από μέρους των παρόχων, οι οποίες θα προσδιορίζουν τους όρους με τους οποίους πραγματοποιείται μια επικοινωνία λαμβάνοντας υπόψη τους προσδιοριζόμενους κανόνες και προϋποθέσεις.

3.2.1 Διατήρηση Δεδομένων στις Ηλεκτρονικές Επικοινωνίες

Ο όρος ***διατήρηση δεδομένων*** αναφέρεται στην αποθήκευση, από την πλευρά των παρόχων δικτύων ηλεκτρονικών επικοινωνιών (*electronic communication network providers*), των εξωτερικών δεδομένων επικοινωνίας των συνδρομητών τους, ώστε να διασφαλίζεται η διαθεσιμότητα των δεδομένων αυτών για το σκοπό της διερεύνησης, της ανίχνευσης και της δίωξης σοβαρών εγκλημάτων, όπως αυτά ορίζονται από τη νομοθεσία. Ο όρος ***πάροχος δικτύου ηλεκτρονικών επικοινωνιών*** περιλαμβάνει τους παρόχους σταθερής και κινητής τηλεφωνίας και τους παρόχους υπηρεσιών διαδικτύου (*ISP*). Στην τελευταία κατηγορία περιλαμβάνονται και οι πάροχοι υπηρεσιών πρόσβασης διαδικτύου, ηλεκτρονικού ταχυδρομείου *(e-mail*) και φωνής μέσω διαδικτύου (*VoIP*).

Είναι προφανές ότι κάθε πάροχος ήδη διατηρεί και επεξεργάζεται τα δεδομένα επικοινωνίας των συνδρομητών του για ορισμένο χρονικό διάστημα, για την υποστήριξη διαδικασιών χρέωσης και επίλυσης προβλημάτων σύνδεσης. Για παράδειγμα, το τμήμα χρέωσης ενός παρόχου τηλεφωνίας έχει πρόσβαση στα αρχεία δεδομένων κλήσεων (*call data records, CDRs*) τα οποία περιλαμβάνουν δεδομένα όπως η πηγή και ο προορισμός μιας κλήσης καθώς και η διάρκεια της κλήσης. Αντίστοιχα ένας πάροχος διαδικτύου διατηρεί δεδομένα διακίνησης ηλεκτρονικού ταχυδρομείου, όπως είναι η πηγή και ο προορισμός κάθε ηλεκτρονικού μηνύματος, για λόγους διασφάλισης και ελέγχου της ορθής λειτουργίας της υπηρεσίας.

Ανάλογα με τον τύπο της επικοινωνίας μπορεί να διατηρηθούν διάφορα δεδομένα. Για παράδειγμα, όπως φαίνεται και στο ***σχήμα 9***, στην περίπτωση των παρόχων κινητής τηλεφωνίας, η διατήρηση δεδομένων μπορεί να περιλαμβάνει τους αριθμούς τηλεφώνου του καλούντος και του καλούμενου μαζί με δεδομένα φυσικής ταυτοποίησης, όπως είναι τα ονόματα και οι διευθύνσεις τους. Επίσης περιλαμβάνει τους διεθνείς αριθμούς αναγνώρισης κινητών συνδρομητών *(International Mobile Subscriber Identification Numbers, IMSI*) οι οποίοι είναι μοναδικοί αριθμοί σε παγκόσμια κλίμακα και αντιστοιχούν ένας σε κάθε κάρτα σύνδεσης συνδρομητή *(Subscriber Identity Module, SIM).* Επιπλέον, η διατήρηση δεδομένων κινητής τηλεφωνίας περιλαμβάνει τους διεθνείς αριθμούς αναγνώρισης κινητού εξοπλισμού *(International Mobile Equipment Numbers, IMEI)*, οι οποίοι είναι μοναδικοί αριθμοί σε παγκόσμια

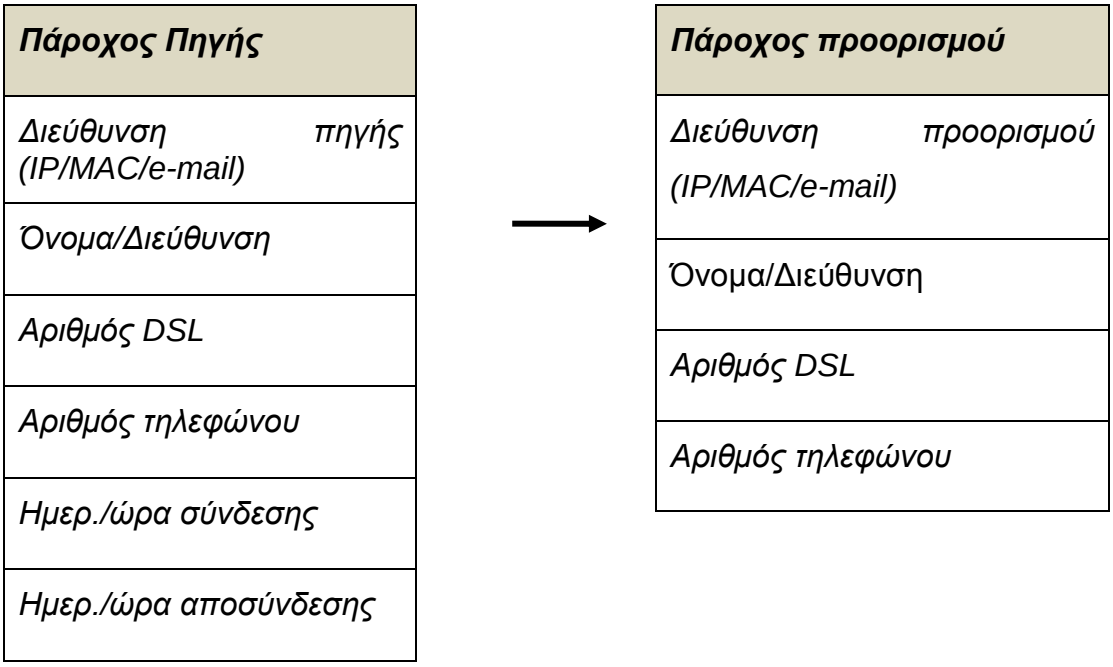
κλίμακα και χαρακτηρίζουν μοναδικά κάθε συσκευή κινητής τηλεφωνίας. Άλλα εξωτερικά δεδομένα μπορεί να περιλαμβάνουν την ημερομηνία/ώρα εκκίνησης και τερματισμού μιας κλίσης, καθώς και τους προσδιοριστές των σταθμών βάσης στους οποίους ήταν συνδεδεμένες οι κινητές συσκευές κατά την εκκίνηση της κλήσης. Τα δεδομένα αυτά αποτελούν πληροφορία τοποθεσίας, η οποία αποκαλύπτει, με σχετική ακρίβεια, τη φυσική τοποθεσία των χρηστών.

Πάροχος Πηγής
Αριθμός Καλούμενου
Όνομα/Διεύθυνση
Αριθμός IMSI
Αριθμός IMEI
Ημερ./ώρα έναρξης
Ημερ./ώρα λήξης
Σταθμός βάσης-Cell ID

Πάροχος προορισμού
Αριθμός καλούντος
Όνομα/Διεύθυνση
Αριθμός IMSI
Αριθμός IMEI

Σχήμα 9: Εξωτερικά δεδομένα στις κινητές επικοινωνίες

Στην περίπτωση των παρόχων διαδικτύου, όπως φαίνεται και στο ***σχήμα 10***, τα διατηρούμενα δεδομένα περιλαμβάνουν δεδομένα αναγνώρισης της ταυτότητας της πηγής και του προορισμού της επικοινωνίας, όπως είναι η διεύθυνση διαδικτύου *(IP address)* ή η διεύθυνση της κάρτας δικτύου (*Media Access Control address*, *MAC address*). Τα διατηρούμενα δεδομένα εξαρτώνται και από τον τύπο της επικοινωνίας. Για παράδειγμα, μπορεί να περιλαμβάνει τη διεύθυνση ηλεκτρονικού ταχυδρομείου της πηγής και του προορισμού (*e-mail address*), καθώς επίσης και άλλα στοιχεία αναγνώρισης των συνδρομητών, όπως είναι ονόματα και διευθύνσεις, ο αριθμός τηλεφωνικής σύνδεσης κ.λπ.



Σχήμα 10: Εξωτερικά δεδομένα στις διαδικτυακές επικοινωνίες

3.2.2 Απειλές Ασφάλειας και Ιδιωτικότητας

Τα εξωτερικά δεδομένα επικοινωνίας περιλαμβάνουν πληροφορία η οποία σχετίζεται με την ταυτότητα και την τοποθεσία των μερών της επικοινωνίας, τη χρονική στιγμή και σε ορισμένες περιπτώσεις με το ίδιο το περιεχόμενο της επικοινωνίας. Συνεπώς η διατήρηση αυτών των δεδομένων ευνοεί την εκδήλωση διαφόρων απειλών ασφάλειας οι οποίες σχετίζονται με το απόρρητο της επικοινωνίας και την ιδιωτικότητα των συνδρομητών. Οι απειλές αυτές περιλαμβάνουν:

- ***Αποκάλυψη δεδομένων:*** Η αποκάλυψη των διατηρούμενων δεδομένων σε μη εξουσιοδοτημένους χρήστες, είτε αυτοί είναι εξωτερικοί είτε εσωτερικοί χρήστες του παρόχου χωρίς τα απαιτούμενα δικαιώματα πρόσβασης, μπορεί να οδηγήσει σε άμεση ή έμμεση παραβίαση του απορρήτου.
- ***Τροποποίηση δεδομένων:*** Μια τυχαία τροποποίηση των δεδομένων ενδέχεται να επηρεάσει την αξιοπιστία τους. Όμως μια εσκεμμένη τροποποίηση ενδέχεται να οδηγήσει σε κατάχρηση των δεδομένων. Σε μια ακραία περίπτωση θα μπορούσαν να χρησιμοποιηθούν δεδομένα επικοινωνίας, τα οποία κακόβουλα έχουν τροποποιηθεί για τη νομική δίωξη κάποιου ανυποψίαστου συνδρομητή.
- ***Μη εξουσιοδοτημένη πρόσβαση:*** Η απειλή αυτή σχετίζεται με τις δύο προηγούμενες, εφόσον μια μη εξουσιοδοτημένη πρόσβαση ανάγνωσης θα οδηγούσε σε αποκάλυψη των δεδομένων, ενώ μια μη εξουσιοδοτημένη πρόσβαση εγγραφής θα μπορούσε να οδηγήσει σε τροποποίηση των δεδομένων.

- ***Παράνομη καταγραφή δεδομένων:*** Σχετίζεται με τη συλλογή δεδομένων πέρα από αυτά που έχουν καθοριστεί στις πολιτικές ιδιωτικότητας των παρόχων. Οι επικοινωνίες που εκτελούνται από τους συνδρομητές πραγματοποιούνται με βάση συγκεκριμένες πολιτικές ιδιωτικότητας, οι οποίες καθορίζουν το είδος των προς συλλογή δεδομένων. Η καταγραφή δεδομένων που δεν περιέχονται στις πολιτικές ιδιωτικότητας αποτελεί σημαντική παραβίαση της ιδιωτικότητας των συνδρομητών.
- ***Παράνομη χρήση δεδομένων:*** Περιλαμβάνει την επεξεργασία των δεδομένων για σκοπούς που δεν περιλαμβάνονται στους νόμιμους σκοπούς της διατήρησης, όπως καθορίζονται στις πολιτικές ιδιωτικότητας. Για παράδειγμα, πρόσβαση σε δεδομένα επικοινωνίας χρηστών διαδικτύου με σκοπό την κατηγοριοποίηση των αγοραστικών τους συνηθειών ή παρακολούθηση των δραστηριοτήτων τους.
- ***Παρατεταμένη διατήρηση δεδομένων:*** Αφορά στη διατήρηση των δεδομένων για χρονικά διαστήματα μεγαλύτερα από αυτά που ορίζονται από τη νομοθεσία και αναφέρονται στις κοινοποιήσιμες πολιτικές ιδιωτικότητας. Παρόλο που η παρατεταμένη διατήρηση δεν αποτελεί από μόνη της άμεση παραβίαση του απορρήτου και της ιδιωτικότητας, παρατείνει την έκθεση των δεδομένων σε πιθανές επιθέσεις και αδυναμίες.
- ***Αδυναμία καταλογισμού ευθύνης:*** Σε περίπτωση που οι πράξεις των χρηστών με νόμιμα δικαιώματα πρόσβασης στα δεδομένα δεν είναι καταλογίσιμες σε αυτούς, πιθανοί κακόβουλοι εξωτερικοί χρήστες θα μπορούσαν να προβούν σε παράνομη χρήση ή κατάχρηση των δεδομένων. Για παράδειγμα, τα δεδομένα επικοινωνίας των συνδρομητών θα μπορούσαν να διαρρεύσουν σε μη εξουσιοδοτημένους χρήστες ή να αποτελέσουν αντικείμενο συναλλαγής ή εκβιασμού συνδρομητών. Επιπλέον, θα ήταν δυνατό να δοθεί πρόσβαση σε δεδομένα σε κάποια διωκτική αρχή, η οποία δεν θα είχε εξασφαλίσει την απαιτούμενη δικαστική άδεια.

3.2.3 Κοινωνικές Αρχές για τη Διατήρηση Δεδομένων

Επειδή η διατήρηση των δεδομένων αυξάνει τους κινδύνους για το απόρρητο και την ιδιωτικότητα των συνδρομητών, θα πρέπει κατ' ελάχιστο, να εφαρμοστούν ορισμένες κοινωνικές αρχές πριν από οποιαδήποτε υλοποίηση και εφαρμογή της διατήρησης των δεδομένων επικοινωνίας. Οι βασικές κοινωνικές αρχές που αφορούν στη διατήρηση δεδομένων επικοινωνίας είναι οι ακόλουθες:

- ***Αρχή της αναλογικότητας:*** Με βάση αυτή την αρχή, η διατήρηση των δεδομένων δεν θα πρέπει να επηρεάζει την ιδιωτικότητα των πολιτών σε βαθμό δυσανάλογο με την προστασία που παρέχει η διατήρηση των δεδομένων επικοινωνίας στο κοινωνικό σύνολο. Με άλλα λόγια οι περιορισμοί που εισάγονται από τη διατήρηση δεδομένων δεν θα πρέπει να υπερβαίνουν το θεμελιώδες δικαίωμα της ελευθερίας στην επικοινωνία.
- ***Αρχή της αναγκαιότητας:*** Η αρχή αυτή ορίζει ότι η διατήρηση των δεδομένων θα πρέπει να καλύπτει τα ελάχιστα δυνατά στοιχεία τα οποία είναι απολύτως αναγκαία για το σκοπό της προστασίας του κοινωνικού συνόλου και για το ελάχιστο δυνατό χρονικό διάστημα.
- ***Αρχή της αποτελεσματικότητας*****:** Με βάση αυτή την αρχή, η διατήρηση των δεδομένων επικοινωνίας θα πρέπει να προστατεύει αποτελεσματικά το

κοινωνικό σύνολο από εγκληματικές ενέργειες που σχετίζονται με την κατάχρηση των ηλεκτρονικών επικοινωνιών.

Είναι φανερό ότι θα πρέπει να βρεθεί το κατάλληλο σημείο ισορροπίας μεταξύ των αρχών της αναλογικότητας από τη μια πλευρά και της αρχής της αποτελεσματικότητας από την άλλη.

3.2.4 Απαιτήσεις Ασφάλειας για τη Διατήρηση Δεδομένων

Για την ελαχιστοποίηση των απειλών ασφάλειας που προκύπτουν από τη διατήρηση των δεδομένων και για την επίτευξη της βέλτιστης ισορροπίας μεταξύ των κοινωνικών αρχών που σχετίζονται με τη διατήρηση των δεδομένων, είναι αναγκαία η διασφάλιση ορισμένων θεμελιωδών απαιτήσεων ασφάλειας. Οι απαιτήσεις αυτές περιλαμβάνουν τα ακόλουθα:

- ***Εμπιστευτικότητα των δεδομένων****:* Τα διατηρούμενα δεδομένα θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη σε εσωτερικούς και εξωτερικούς χρήστες κατά την αποθήκευση ή την επεξεργασία τους.
- ***Ακεραιότητα των δεδομένων:*** Η ακεραιότητα των δεδομένων θα πρέπει να διασφαλίζεται έναντι τυχαίας ή εσκεμμένης τροποποίησης από εσωτερικούς ή εξωτερικούς χρήστες. Σε περίπτωση που δεν είναι δυνατή η πρόληψη κάθε πιθανής τροποποίησης των δεδομένων, θα πρέπει τουλάχιστον να διασφαλίζεται η ανίχνευσή της.
- ***Ελεγχόμενη πρόσβαση:*** Πρόσβαση στα δεδομένα θα πρέπει να δίνεται μόνο σε εξουσιοδοτημένους χρήστες με την εφαρμογή μιας αυστηρής πολιτικής πρόσβασης.
- ***Καταγραφή, ανίχνευση και έλεγχος****:* Η οποιαδήποτε πρόσβαση ή επεξεργασία των δεδομένων θα πρέπει να καταγράφεται με ασφαλή και μη τροποποιήσιμο τρόπο, ώστε κάθε παράνομη πρόσβαση ή κατάχρηση των δεδομένων επικοινωνίας να είναι ανιχνεύσιμη.
- ***Ασφαλής καταστροφή των δεδομένων:*** Τα δεδομένα θα πρέπει να καταστρέφονται με ασφαλή και μη αναστρέψιμο τρόπο, μετά τη λήξη της νόμιμης περιόδου διατήρησης, ώστε να μην είναι δυνατές η κατάχρηση των δεδομένων και η παραβίαση της ιδιωτικότητας των συνδρομητών.

Δεδομένου ότι οι τεχνολογίες και οι αρχιτεκτονικές δικτύου διαφέρουν από πάροχο σε πάροχο, η υλοποίηση των απαιτήσεων αυτών δεν είναι πάντοτε προφανής. Για την επίτευξη των απαιτήσεων ασφάλειας απαιτείται η σχεδίαση ενός γενικού μοντέλου ασφάλειας των διατηρούμενων δεδομένων επικοινωνίας.

3.2.5 Ένα Γενικό Μοντέλο για την Ασφαλή Διατήρηση των Δεδομένων Επικοινωνίας

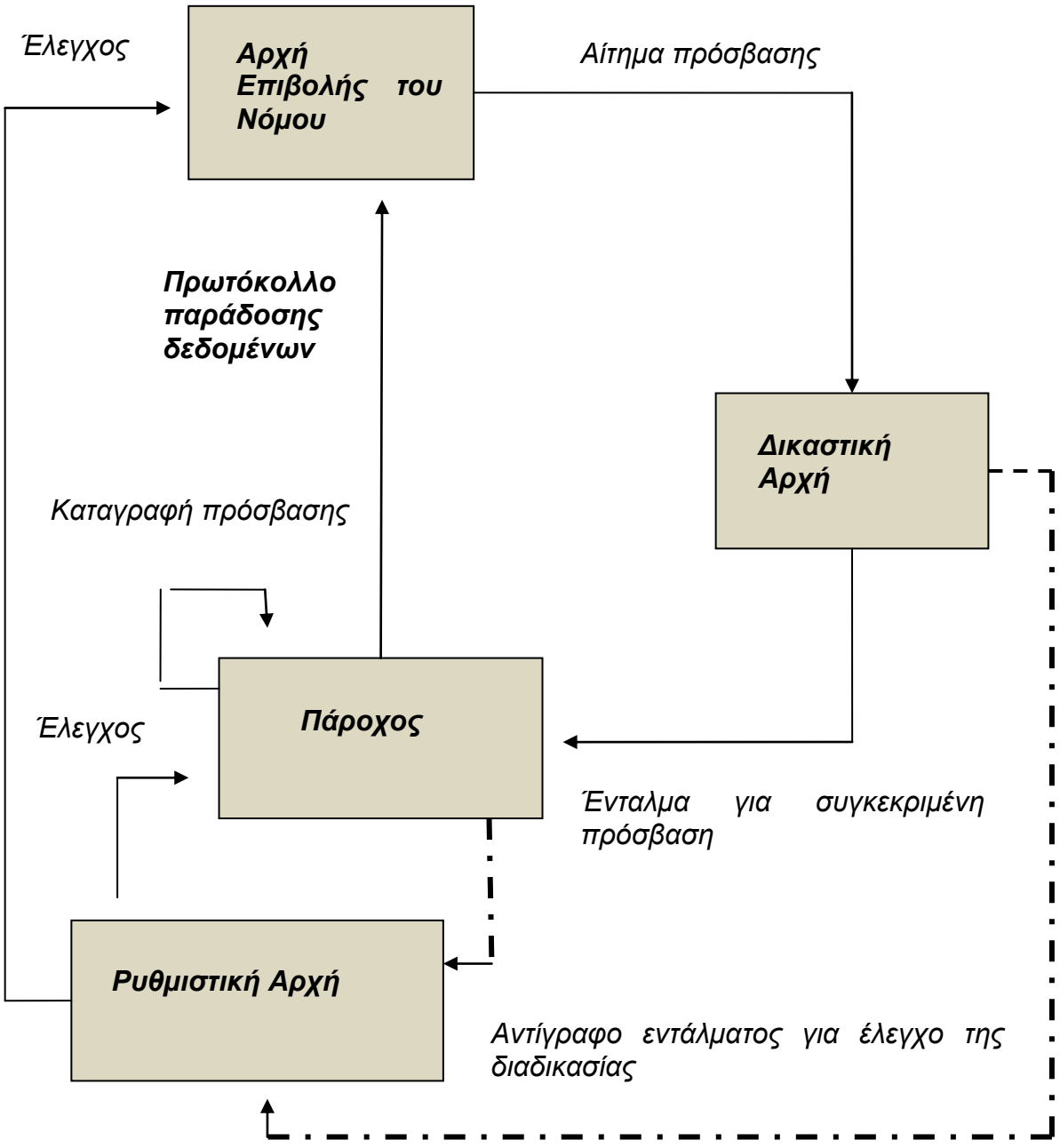
Ένα γενικό μοντέλο για την ασφαλή διατήρηση των δεδομένων επικοινωνίας θα πρέπει να καλύπτει στο μεγαλύτερο δυνατό βαθμό τόσο τις τεχνικές απαιτήσεις ασφάλειας όσο και τις κοινωνικές αρχές που απαιτούνται. Στο ***σχήμα 11*** παρουσιάζεται ένα γενικό μοντέλο το οποίο περιλαμβάνει τέσσερις λογικές οντότητες:

- ***Τον Πάροχο Ηλεκτρονικών Επικοινωνιών:*** Μπορεί να είναι ένας πάροχος διαδικτύου ή ένας πάροχος τηλεπικοινωνιών. Κάθε πάροχος είναι υπεύθυνος για τον καθορισμό συγκεκριμένων πολιτικών ιδιωτικότητας που περιγράφουν τους όρους υπό τους οποίους πραγματοποιείται μια επικοινωνία και φέρουν

την ευθύνη για την τήρησή της. Ευθύνονται, λοιπόν, για ένα σύνολο ζητημάτων που αφορούν στην ασφαλή αποθήκευση δεδομένων, στη διατήρηση των δεδομένων για το αναμενόμενο χρονικό διάστημα και στην ασφαλή καταστροφή τους μετά τη λήξη της περιόδου διατήρησης.

- ***Την Αρχή Επιβολής του Νόμου:*** Αναφέρεται σε κάθε διωκτική αρχή με δικαίωμα αίτησης για παροχή πρόσβασης σε δεδομένα επικοινωνίας που διατηρεί ο πάροχος, με σκοπό τη δίωξη πιθανών εγκληματικών ενεργειών.
- ***Την Δικαστική Αρχή:*** Είναι η αρχή η οποία ελέγχει την πρόσβαση στα διατηρούμενα δεδομένα. Ο πάροχος δίνει πρόσβαση σε δεδομένα σε κάποια αρχή επιβολής του νόμου, μόνο μετά την έκδοση δικαστικής εντολής και μόνο για το συγκεκριμένο συνδρομητή στον οποίο αναφέρεται η δικαστική εντολή.
- ***Την Ρυθμιστική Αρχή:*** Είναι μια ανεξάρτητη αρχή η οποία λειτουργεί ως έμπιστη τρίτη οντότητα. Έχει την ευθύνη να ελέγχει την τήρηση των διαδικασιών που ακολουθούν οι εμπλεκόμενοι φορείς για την ασφαλή αποθήκευση, επεξεργασία και πρόσβαση στα δεδομένα.

Οι βασικές αρχές ασφάλειας στις οποίες στηρίζεται αυτό το μοντέλο είναι η διάκριση καθηκόντων (*separation of duties*) και ο διπλός έλεγχος *(dual control*).



Σχήμα 11: Ένα γενικό μοντέλο για την ασφαλή διατήρηση δεδομένων επικοινωνίας

3.2.5.1 Μέτρα Ασφάλειας

Η προστασία των δεδομένων επικοινωνίας είναι αναγκαία προϋπόθεση για τη διασφάλιση της ιδιωτικότητας των συνδρομητών. Για το σκοπό αυτό απαιτείται ο συνδυασμός μέτρων πρόληψης και μέτρων ανίχνευσης για την εμπιστευτικότητα, την ακεραιότητα, την διαθεσιμότητα, τον έλεγχο πρόσβασης και τον έλεγχο χρήσης των

δεδομένων. Παρακάτω, περιγράφονται ορισμένα βασικά μέτρα ασφάλειας τα οποία μπορούν να εφαρμοστούν στα πλαίσια του γενικού μοντέλου ασφάλειας κατά τη διατήρηση των δεδομένων επικοινωνίας.

3.2.5.1.1 Κρυπτογράφηση

Για την εμπιστευτικότητα των δεδομένων μπορούν να εφαρμοστούν κατάλληλοι μηχανισμοί κρυπτογράφησης, ώστε ακόμα και στην περίπτωση που παραβιαστούν οι μηχανισμοί πρόσβασης σε ένα σύστημα, να μην αποκαλύπτεται το πραγματικό περιεχόμενο της πληροφορίας. Η κρυπτογράφηση των δεδομένων μπορεί να υλοποιηθεί χρησιμοποιώντας ***συμμετρική κρυπτογραφία*** (*symmetric cryptography*) – για παράδειγμα τον αλγόριθμο *Advanced Encryption Standard* (*AES)*. Σε αυτή την περίπτωση όμως, κάθε χρήστης που έχει πρόσβαση στο κλειδί κρυπτογράφησης, έχει ταυτόχρονα και τη δυνατότητα αποκρυπτογράφησης των δεδομένων. Συνεπώς δεν εξασφαλίζεται η αρχή του διπλού ελέγχου της πληροφορίας (*dual control*).

Ο διπλός έλεγχος μπορεί να εξασφαλιστεί με τη χρήση ***κρυπτογραφίας δημόσιου κλειδιού*** (*public key cryptography*) – για παράδειγμα με τη χρήση του κρυπτοσυστήματος *RSA* – σε συνδυασμό με τεχνικές διαμοίρασης κλειδιού (*key sharing*). Σε αυτή την περίπτωση, σε κάθε πάροχο ανατίθεται ένα μοναδικό ζεύγος δημόσιου/ιδιωτικού κλειδιού. Ο πάροχος μπορεί αυτόνομα να κρυπτογραφήσει τα διατηρούμενα δεδομένα με τη χρήση του δημόσιου κλειδιού. Όμως, το αντίστοιχο ιδιωτικό κλειδί αποκρυπτογράφησης διαμοιράζεται μεταξύ του παρόχου και της Ρυθμιστικής Αρχής με τη χρήση τεχνικών διαμοίρασης κλειδιού. Είναι προφανές ότι τα ζητήματα που αφορούν τη δημιουργία, την πιστοποίηση και τη διαχείριση των κλειδιών, όπως επίσης και τη διαμοίραση και την αποστολή των μεριδίων του ιδιωτικού κλειδιού είναι πολύ σημαντικά και απαιτείται η πλήρης επίλυσή τους, πριν από την υιοθέτηση οποιασδήποτε υλοποίησης του γενικού μοντέλου ασφάλειας.

Εκτός από τις τεχνικές κρυπτογραφίας δημόσιου κλειδιού οι οποίες απαιτούν υψηλό υπολογιστικό κόστος, ιδίως για μεγάλες ποσότητες δεδομένων, μπορεί να εφαρμοστεί και η τεχνική ***της υβριδικής κρυπτογραφίας*** (*hybrid encryption*).

Η χρήση των μηχανισμών κρυπτογράφησης είναι μεν αναγκαία αλλά όχι και ικανή συνθήκη για την προστασία των δεδομένων από κάποιον κακόβουλο εσωτερικό χρήστη από την πλευρά του παρόχου, ο οποίος έχει τη δυνατότητα να διατηρεί αντίγραφα του κλειδιού κρυπτογράφησης ή των ίδιων των δεδομένων πριν από την κρυπτογράφησή τους. Η αντιμετώπιση τέτοιων προβλημάτων απαιτεί το συνδυασμό τεχνικών και διαδικαστικών μέτρων ασφάλειας. Για παράδειγμα, ένα διαδικαστικό μέτρο πρόληψης τέτοιων επιθέσεων κατάχρησης είναι η διαρκής εποπτεία των συστημάτων κρυπτογράφησης από δύο τουλάχιστον διαχειριστές. Ένα πιθανό μέτρο ανίχνευσης από την πλευρά του παρόχου είναι η εφαρμογή ενός ασφαλούς και μη τροποποιήσιμου συστήματος καταγραφής (*logging*), με σκοπό τον έλεγχο όλων των ενεργειών σε κρίσιμα συστήματα, και η διατήρηση μη τροποποιήσιμων αρχείων καταγραφής συστήματος και εντολών. Ένα τέτοιο μέτρο θα επέτρεπε στη Ρυθμιστική Αρχή να πραγματοποιεί εξωτερικούς ελέγχους ασφάλειας σε προγραμματισμένες ή τυχαίες περιόδους, έτσι ώστε να διαπιστωθεί η ορθή υλοποίηση των διαδικασιών κρυπτογράφησης.

3.2.5.1.2 Ακεραιότητα Δεδομένων

Η ακεραιότητα των δεδομένων μπορεί να ελεγχθεί με τη χρήση γνωστών κρυπτογραφικών συναρτήσεων κατακερματισμού (*hash functions),* π.χ. των *SHA, MD5*

κ.λπ. Κάθε αντικείμενο δεδομένων περνά ως είσοδος από μία τέτοια συνάρτηση και στη συνέχεια η τιμή κατακερματισμού κρυπτογραφείται μαζί με το αντίστοιχο αντικείμενο δεδομένων, χρησιμοποιώντας τους μηχανισμούς κρυπτογράφησης. Συνεπώς, κάθε κρυπτογραφημένο αντικείμενο δεδομένων περιλαμβάνει όχι μόνο τον έλεγχο ακεραιότητας αλλά και οποιαδήποτε τροποποίηση των αποθηκευμένων δεδομένων γίνει αντιληπτή.

Με τη μέθοδο αυτή όμως, δεν είναι δυνατή η ανίχνευση επιθέσεων τροποποίησης κατά τις οποίες έχουν διαγραφεί ορισμένα από τα αποθηκευμένα δεδομένα, μαζί με τους αντίστοιχους ελέγχους ακεραιότητας των δεδομένων αυτών. Μια εξελιγμένη τεχνική για αυτή την περίπτωση είναι η χρήση κρυπτογραφικών συνδέσμων μεταξύ κάθε γειτονικού αντικειμένου δεδομένων. Με αυτή τη μέθοδο, σε περίπτωση διαγραφής ενός αντικειμένου δεν θα είναι δυνατή η επαλήθευση του επόμενου στη σειρά αντικειμένου δεδομένων.

3.2.5.1.3 Έλεγχοι Πρόσβασης

Διάφορες κατηγορίες εσωτερικών χρηστών του παρόχου μπορεί να χρειάζονται πρόσβαση στα διατηρούμενα δεδομένα επικοινωνίας για λόγους περαίωσης των εργασιών τους. Για παράδειγμα, το τμήμα χρεώσεων χρειάζεται πρόσβαση στα δεδομένα επικοινωνίας με σκοπό την επεξεργασία τους για τον υπολογισμό των λογαριασμών των συνδρομητών. Η πρόσβαση των εσωτερικών χρηστών του παρόχου μπορεί να ελεγχθεί με μηχανισμούς όπως οι ***λίστες ελέγχου πρόσβασης*** (*access control lists*) και οι ***ρόλοι*** (*roles*). Με τον έλεγχο πρόσβασης βάσει ρόλων (*role based access control)* το εξουσιοδοτημένο προσωπικό του τμήματος χρεώσεων λογαριασμών του παρόχου μπορεί να έχει λάβει ένα συγκεκριμένο ρόλο, ο οποίος ενεργοποιείται μόνο συγκεκριμένες ώρες της ημέρας και για συγκεκριμένα τμήματα των δεδομένων. Είναι προφανές ότι εφόσον τα διατηρούμενα δεδομένα επικοινωνίας βρίσκονται σε κρυπτογραφημένη μορφή, η πρόσβαση στην πραγματική πληροφορία απαιτεί επίσης την συνεργασία των μερών που κατέχουν τα απαραίτητα κλειδιά αποκρυπτογράφησης. Με αυτό τον τρόπο επιτυγχάνεται διπλός έλεγχος για την εσωτερική πρόσβαση των δεδομένων. Επιπρόσθετα, με τη χρήση μηχανισμών καταγραφής (*logging*) σε επίπεδο συστήματος και εφαρμογής, είναι δυνατή η ανίχνευση πιθανής κατάχρησης των δεδομένων.

Η πρόσβαση στα δεδομένα από μια εξωτερική αρχή (π.χ. μια Αρχή Επιβολής του Νόμου) θα πρέπει να ελέγχεται μέσω της Δικαστικής Αρχής. Σε περίπτωση που μια Αρχή Επιβολής αιτείται πρόσβαση σε διατηρούμενα δεδομένα θα πρέπει να αποστείλει ένα αίτημα άρσης απορρήτου για τα συγκεκριμένα δεδομένα του συγκεκριμένου χρήστη στη Δικαστική Αρχή, στο οποίο να αναγράφεται και το συγκεκριμένο χρονικό διάστημα για την άρση του απορρήτου. Σε περίπτωση που το αίτημα γίνει αποδεκτό από τη Δικαστική Αρχή, εκδίδεται ένταλμα το οποίο μπορεί να είναι σε ηλεκτρονική μορφή και να περιγράφει τα συγκεκριμένα δικαιώματα πρόσβασης που δίνονται στην Αρχή Επιβολής. Με αυτό τον τρόπο εξασφαλίζονται ο διπλός έλεγχος και η διάκριση καθηκόντων μεταξύ των εμπλεκόμενων αρχών.

3.2.5.1.4 Ψηφιακές Υπογραφές

Για την διασφάλιση της ακεραιότητας και της αυθεντικότητας των ηλεκτρονικών ενταλμάτων απαιτείται η χρήση ***ψηφιακών υπογραφών*** (*digital signatures*). Η Δικαστική Αρχή χρησιμοποιώντας ένα πιστοποιημένο κλειδί υπογραφής μπορεί να υπογράψει ψηφιακά τα εντάλματα τα οποία περιλαμβάνουν την ταυτότητα του στόχου της άρσης, τον τύπο των δεδομένων που αιτούνται πρόσβαση, τη συγκεκριμένη

χρονική περίοδο της άρσης του απορρήτου και μια χρονοσφραγίδα της χρονικής στιγμής έκδοσης του εντάλματος. Ο πάροχος θα μπορεί με την χρήση του αντίστοιχου δημόσιου κλειδιού της Δικαστικής Αρχής να επαληθεύσει την αυθεντικότητα του εντάλματος.

Το δημόσιο κλειδί της Δικαστικής Αρχής, αλλά και κάθε άλλο δημόσιο κλειδί, θα πρέπει να είναι πιστοποιημένο μέσα από ένα έγκυρο ψηφιακό πιστοποιητικό (*digital certificate*). Η πιστοποίηση των δημόσιων κλειδιών μπορεί να πραγματοποιηθεί μέσω μιας υποδομής δημόσιου κλειδιού (*Public Key Infrastructure, PKI*), η οποία εκδίδει, δημοσιεύει και διαχειρίζεται τα πιστοποιητικά. Προτείνεται η χρήση μιας εξωτερικής, ανεξάρτητης υποδομής δημόσιου κλειδιού. Με αυτό τον τρόπο κανένα από τα άμεσα εμπλεκόμενα μέρη δεν θα έχει τις αυξημένες αρμοδιότητες αλλά και το διαχειριστικό κόστος που συνεπάγεται η λειτουργία μιας υποδομής δημόσιου κλειδιού.

3.2.5.1.5 Μετάδοση Δεδομένων

Μετά τη λήψη ενός εντάλματος, ο πάροχος θα πρέπει να μεταδώσει τα ζητούμενα δεδομένα στην αιτούσα Αρχή. Τα δεδομένα, αφού αποκρυπτογραφηθούν με τη συνεργασία των μερών που κατέχουν τα μερίδια του κλειδιού αποκρυπτογράφησης, θα πρέπει να αποσταλούν με ασφαλή τρόπο. Αυτό μπορεί να εξασφαλιστεί με την εφαρμογή ενός ασφαλούς πρωτοκόλλου μετάδοσης, για παράδειγμα με βάση τα πρότυπα του Ευρωπαϊκού Ινστιτούτου Τεχνικών Προτύπων (*European Technical Standardization Institution, ETSI)*. Ο πάροχος και η αιτούσα Αρχή μπορούν να στείλουν ένα αντίγραφο του εντάλματος στη Ρυθμιστική Αρχή με σκοπό τη διευκόλυνση των εξωτερικών ελέγχων που θα πραγματοποιηθούν στον πάροχο σε μελλοντικό χρόνο.

3.2.5.1.6 Καταγραφή Ενεργειών (Logging)

Σε συνδυασμό με τα μέτρα πρόληψης, θα πρέπει να εγκατασταθούν και μηχανισμοί ανίχνευσης κακόβουλων ενεργειών στα διατηρούμενα δεδομένα επικοινωνίας. Αυτό μπορεί να υλοποιηθεί με μηχανισμούς καταγραφής ενεργειών με ασφαλή και μη τροποποιήσιμο τρόπο, ώστε να είναι δυνατή η μελλοντική ανίχνευση των προσβάσεων στα δεδομένα.

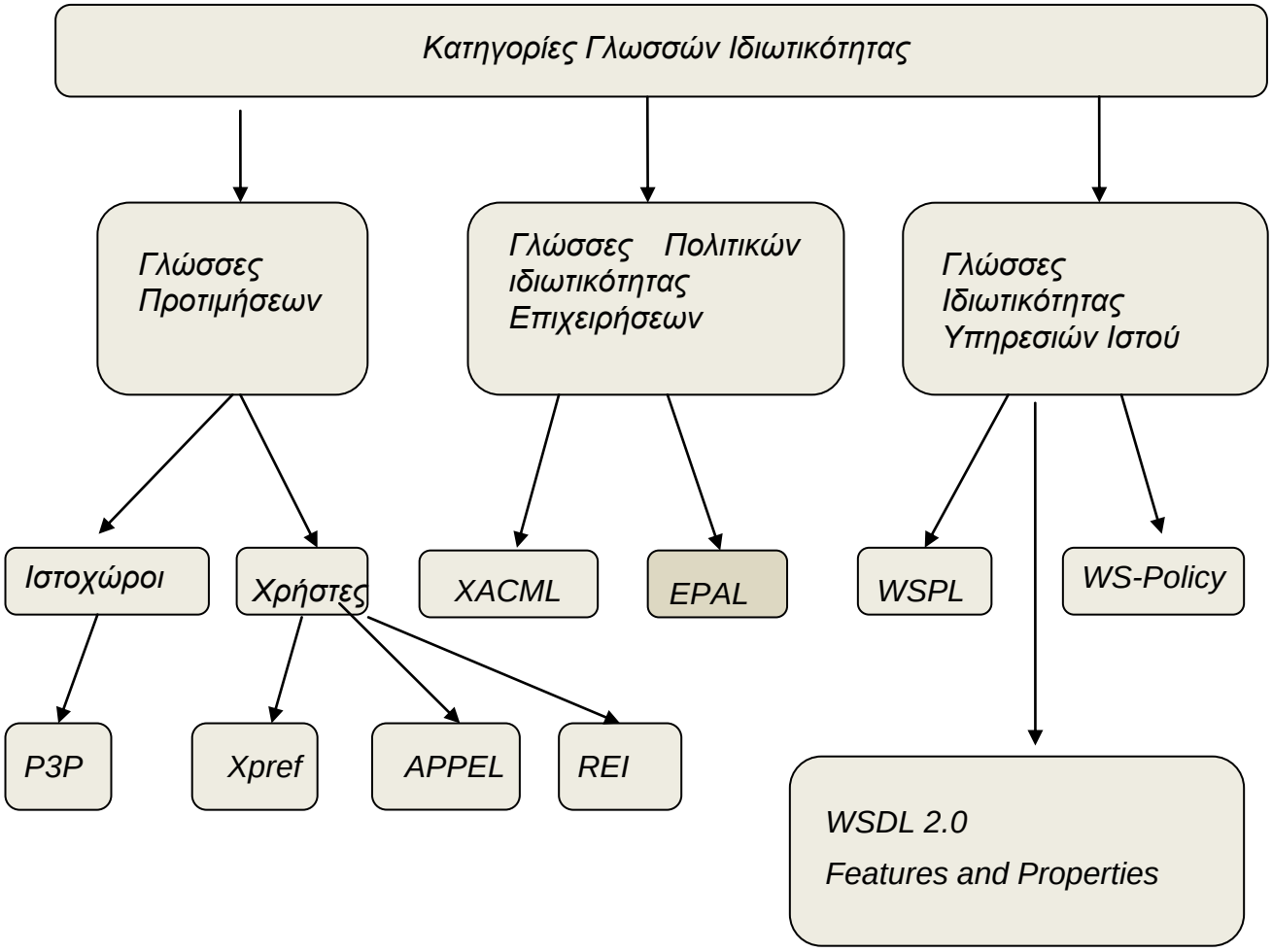
Ένας τέτοιος μηχανισμός είναι η χρήση ασφαλούς συστήματος καταγραφής ενεργειών (*secure log servers*), που συνδυάζει κρυπτογραφικούς μηχανισμούς, όπως είναι οι ψηφιακές υπογραφές και οι συναρτήσεις κατακερματισμού. Για να επιτευχθεί η διάκριση των καθηκόντων, ο διαχειριστής του συστήματος καταγραφής δεν θα πρέπει να έχει δικαιώματα πρόσβασης στα διατηρούμενα δεδομένα. Με την εφαρμογή ενός τέτοιου διαχωρισμού, καθίσταται δυσκολότερη η παράνομη πρόσβαση στα δεδομένα επικοινωνίας ή η τροποποίησή τους.

Η Ρυθμιστική Αρχή μπορεί να αξιοποιεί τα στοιχεία καταγραφής πρόσβασης κατά την διάρκεια των εξωτερικών ελέγχων ασφάλειας που θα πραγματοποιεί στον πάροχο και να επιβεβαιώνει τη λήψη των απαραίτητων μέτρων προστασίας των δεδομένων.

3.2.5.2 Μέτρα Ιδιωτικότητας

Οι ρυθμιστικές και νομικές απαιτήσεις για την προστασία της ιδιωτικότητας των συνδρομητών έχουν τροφοδοτήσει την ανάγκη για δημιουργία, επιβολή και εποπτεία πολιτικών ιδιωτικότητας από μέρους των παρόχων. Οι πολιτικές αυτές εκφράζονται με την ανάπτυξη ποικίλων ***γλωσσών πολιτικών ιδιωτικότητας*** (*privacy policy languages*), καθεμιά από τις οποίες αποσκοπεί στην κάλυψη μιας συγκεκριμένης ανάγκης ιδιωτικότητας.

Οι γλώσσες πολιτικών ιδιωτικότητας μπορούν να ταξινομηθούν σε τρείς βασικές κατηγορίες, όπως φαίνεται στο ***σχήμα 12***, στο οποίο και παρατίθενται οι πιο αντιπροσωπευτικές γλώσσες κάθε κατηγορίας. Η κατηγοριοποίηση που λαμβάνει χώρα γίνεται με βάση το σκοπό της υλοποίησης αλλά και της χρήσης κάθε γλώσσας. Στην ***πρώτη κατηγορία*** περιλαμβάνονται γλώσσες που δίνουν την δυνατότητα έκφρασης συγκεκριμένων προτιμήσεων από μέρους των συμβαλλόμενων μερών. Στη ***δεύτερη κατηγορία*** ανήκουν γλώσσες που χρησιμοποιούνται για τον καθορισμό των πολιτικών ιδιωτικότητας ενός παρόχου, περιγράφοντας το επίπεδο πρόσβασης στα δεδομένα που έχουν συλλεγεί. Τα τελευταία χρόνια έχουν προταθεί ορισμένες γλώσσες για υπηρεσίες ιστού. Οι γλώσσες αυτές αποτελούν την ***τρίτη κατηγορία*** και παρουσιάζουν ποικίλους βαθμούς εκφραστικότητας και πολυπλοκότητας.



Σχήμα 12: Κατηγοριοποίηση γλωσσών πολιτικών ιδιωτικότητας

3.2.5.2.1 Γλώσσες Προτιμήσεων

Η *Platform for Privacy Preferences 1.0 (P3P)* αποτελεί την πιο αντιπροσωπευτική γλώσσα της κατηγορίας αυτής. Η *P3P* έχει καθιερωθεί ως το πρότυπο για την έκφραση

του είδους των δεδομένων αλλά και του σκοπού συλλογής των δεδομένων από μέρους των ιστοχώρων. Η μέθοδος κωδικοποίησης των πρακτικών συλλογής και χρήσης των δεδομένων που παρέχεται είναι σε μορφή *XML*, στοιχείο που την καθιστά αυτόματα ανεξάρτητη πλατφόρμας και υπολογιστικού συστήματος.

Στο πλαίσιο της προδιαγραφής *P3P* μέσω του καθορισμού της γλώσσας προτιμήσεων *P3P Preference Exchange Language (APPEL)* παρέχεται η δυνατότητα και στο χρήστη να εκφράσει τις προτιμήσεις ιδιωτικότητάς του. Ο στόχος της χρήσης αυτής της γλώσσας προτιμήσεων είναι οι προτιμήσεις που εκφράζονται σε *APPEL* να συγκριθούν με εκείνες που εκφράζονται σε *P3P* προκειμένου ένας χρήστης να αποφασίσει αν είναι διατεθειμένος να αποκαλύψει τα δεδομένα που του ζητούνται από τον ιστοχώρο, ώστε να ανακτήσει πρόσβαση σε αυτόν. Παρά το γεγονός όμως ότι η προδιαγραφή *P3P* επιτρέπει τόσο στο χρήστη όσο και στους ιστοχώρους να εκφράσουν τις προτιμήσεις τους, το μοντέλο αυτό δεν έχει βρει ακόμα ευρεία αποδοχή.

Προκειμένου να καλυφθεί ένα μέρος ή το σύνολο των αδυναμιών που προκύπτουν από τη χρήση της *APPEL*, έχουν προταθεί ορισμένες νέες γλώσσες πολιτικών ιδιωτικότητας όπως η *Xpref* και η *REI*.

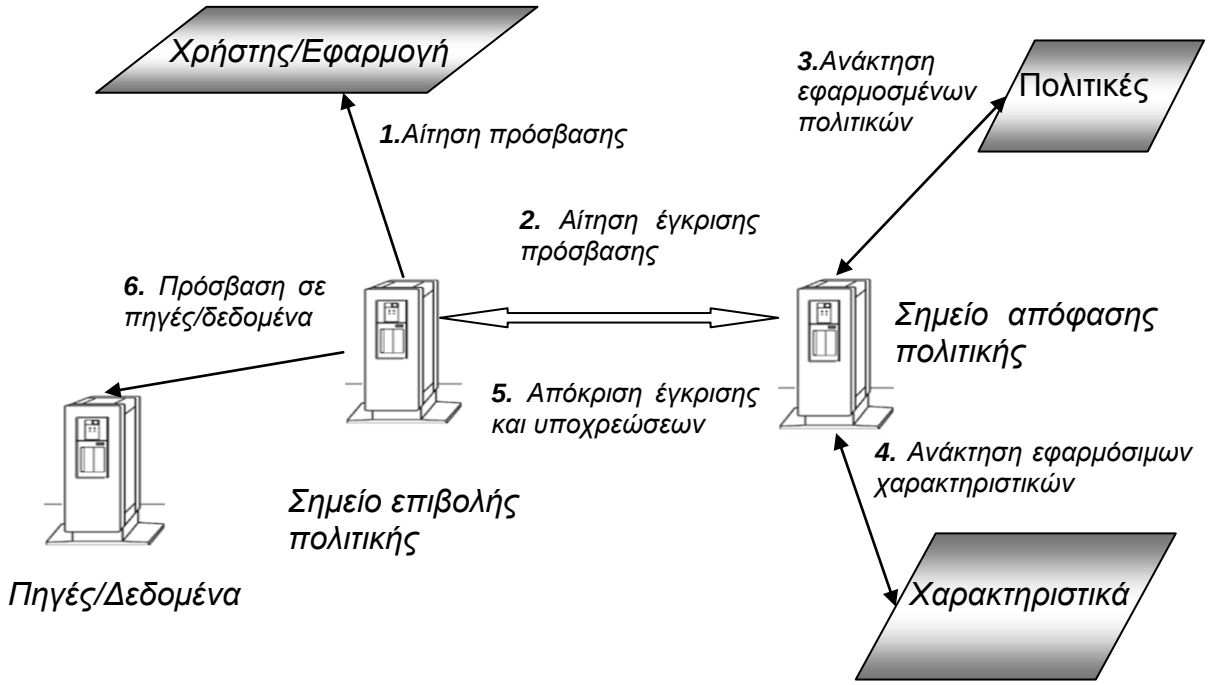
3.2.5.2.2 Γλώσσες Πολιτικών Ιδιωτικότητας Επιχειρήσεων

Οι δύο πιο διαδεδομένες γλώσσες που περιλαμβάνονται στην κατηγορία αυτή είναι η *Enterprise Privacy Authorization Language (EPAL)* της *IBM* και η *eXtensible Access Control Markup Language (XACML)* του *OASIS*. Βασικό χαρακτηριστικό γνώρισμα και των δύο γλωσσών αποτελεί το γεγονός ότι είναι ανεξάρτητες πλατφόρμας, στοιχείο που οφείλεται στην αναπαράστασή τους μέσω της *XML*.

Η *XACML* αποτελεί ένα πρότυπο του *OASIS* και η χρήση της συνοψίζεται σε δύο βασικές κατευθύνσεις: ως μία γλώσσα πολιτικών και ως μία γλώσσα ελέγχου πρόσβασης αίτησης/απόκρισης. Στην πρώτη περίπτωση στόχος είναι η περιγραφή των γενικών απαιτήσεων ελέγχου πρόσβασης, ενώ στη δεύτερη περίπτωση η χρήση της αποσκοπεί στη δημιουργία αιτήσεων λαμβάνοντας υπόψη ορισμένα χαρακτηριστικά, ώστε να ελεγχθεί αν μια ενέργεια πάνω σε ένα σύνολο δεδομένων ή πηγών πρέπει να επιτραπεί ή όχι. Την αίτηση αυτή ακολουθεί μια απόκριση που ενημερώνει το αποτέλεσμα της αίτησης.

Η *EPAL* αποτελεί μια γλώσσα που αναπτύχθηκε από την *IBM* και έχει προταθεί για προτυποποίηση στον *W3C* από το Νοέμβριο του 2003. Οι αντικειμενικοί της στόχοι είναι δύο: η παροχή της δυνατότητας κωδικοποίησης των πολιτικών και η εισαγωγή μιας γλώσσας επιβολής των επιλεγμένων πολιτικών.

Τόσο η *XACML* όσο και η *EPAL* χρησιμοποιούν το ίδιο μοντέλο επιβολής πολιτικών που απεικονίζεται και στο ***σχήμα 13***.



Σχήμα 13: Μοντέλο επιβολής πολιτικών

Στο μοντέλο αυτό ένας χρήστης/εφαρμογή επιδιώκει να αποκτήσει πρόσβαση σε ένα σύνολο πηγών/δεδομένων, υποβάλλοντας ένα αίτημα στο ***Σημείο Επιβολής Πολιτικής*** (*Policy Enforcement Point, PEP*) ***(ενέργεια 1).*** Το συστατικό αυτό διαμορφώνει μια αίτηση που περιέχει τα χαρακτηριστικά της αίτησης του χρήστη/εφαρμογής. Τα χαρακτηριστικά που περιέχονται στη νέα αίτηση είναι η ταυτότητα του αιτούντος, η πηγή για την οποία ζητείται η πρόσβαση, η ενέργεια που θα εκτελεστεί στην πηγή και ο σκοπός πρόσβασης. Η αίτηση έγκρισης της πρόσβασης υποβάλλεται στο ***Σημείο Απόφασης Πολιτικής*** (*Policy Decision Point, PDP*) ***(ενέργεια 2).*** Το συστατικό αυτό, μόλις λάβει την αίτηση, ανακτά τις εφαρμόσιμες πολιτικές ***(ενέργεια 3),*** μαζί με τα πρόσθετα στοιχεία που απαιτούνται για την αξιολόγηση των πολιτικών ***(ενέργεια 4)*** και αξιολογεί τις πολιτικές, ώστε να καθορίσει την απόφαση έγκρισης. Η ληφθείσα απόφαση επιστρέφεται στο ***Σημείο Επιβολής Πολιτικής (ενέργεια 5),*** το οποίο επιτρέπει ή απαγορεύει την πρόσβαση στο χρήστη/εφαρμογή ***(ενέργεια 6).***

Οι δύο γλώσσες παρουσιάζουν μια σειρά από ομοιότητες αλλά και μια σειρά από διαφορές, όμως σε γενικές γραμμές μπορεί να θεωρηθεί ότι η *EPAL* προσφέρει ένα υποσύνολο της λειτουργικότητας της *XACML*. Η *XACML* στην ουσία αναπτύχθηκε για να προσφέρει έλεγχο επιχειρηματικής πρόσβασης διευθετώντας ζητήματα τα οποία προέκυπταν στα διανεμημένα συστήματα. Επίσης περιέχει ένα σύνολο από στοιχεία τα οποία δεν περιέχονται στην *EPAL*, περιορίζοντας τη δυνατότητά της να εκφράσει ευέλικτες και εξελικτικές πολιτικές.

3.2.5.2.3 Γλώσσες Ιδιωτικότητας Υπηρεσιών Ιστού

Οι υπηρεσίες ιστού προκειμένου να επικοινωνήσουν μεταξύ τους απαιτούν επιμέρους πληροφορίες που αφορούν ζητήματα όπως είναι ο καθορισμός των απαιτούμενων μηχανισμών εμπιστευτικότητας και των απαραίτητων στοιχείων αυθεντικοποίησης, ποιότητας υπηρεσιών και ιδιωτικότητας. Οι γλώσσες ιδιωτικότητας των υπηρεσιών

ιστού αποτελούν την τρίτη κατηγορία και έχουν απώτερο στόχο την περιγραφή του συνόλου των στοιχείων των υπηρεσιών ιστού που απαρτίζουν τα μη λειτουργικά χαρακτηριστικά μιας υπηρεσίας, διευκολύνοντας με αυτό τον τρόπο τη διαλειτουργικότητα, την προσβασιμότητα και την αξιοπιστία των υπηρεσιών.

Οι πιο ευρέως γνωστές και χρησιμοποιούμενες γλώσσες ακολουθούν την εξής δομή: Μια πολιτική αποτελεί ένα συνδυασμό κατηγορημάτων ή ισχυρισμών, οι οποίοι διευκρινίζουν τις αποδεκτές τιμές για ένα ή περισσότερα χαρακτηριστικά. Οι πιο αντιπροσωπευτικές γλώσσες της κατηγορίας αυτής ποικίλουν ως προς την εκφραστικότητα και την πολυπλοκότητα και μπορούν να συνοψιστούν στη *Web Service Policy Language (WSPL)*, στην πρόταση της *Oracle "Features and Properties*" για προσθήκη «συνθετικών» (λογικών συνδέσμων) στην *WSDL 2.0* και τέλος στο *Web Service Policy Framework (WS-Policy)*.

Η *WSPL* αναπτύχθηκε από την Τεχνική Επιτροπή *OASIS XACML* και το συντακτικό της αποτελεί ένα υποσύνολο του προτύπου *XACML*. Η χρήση της εστιάζεται στον καθορισμό των πολιτικών των υπηρεσιών ιστού, χρησιμοποιώντας πρότυπους τύπους δεδομένων και τελεστών για την έκφραση των παραμέτρων. Ιδιαίτερα σημαντικό είναι το γεγονός ότι επιτρέπει τη συγχώνευση δύο πολιτικών, δημιουργώντας μια τρίτη πολιτική η οποία ικανοποιεί τις απαιτήσεις των δύο αρχικών, υποθέτοντας βέβαια ότι μια τέτοια πολιτική υφίσταται.

Η πρόταση *Features and Properties* έχει στόχο να ενισχύσει το τμήμα των χαρακτηριστικών γνωρισμάτων που είναι διαθέσιμα στην *WSDL 2.0*, ώστε να διευθετηθούν πλήρως οι ανάγκες των υπηρεσιών ιστού για γνωστοποίηση των απαιτήσεών τους. Με την ενίσχυση αυτή επιτρέπεται στις υπηρεσίες ιστού να κοινοποιήσουν τα χαρακτηριστικά τους χωρίς όμως να παρέχεται σημαντική εκφραστικότητα εξαιτίας της έλλειψης τελεστών για το συνδυασμό των ισχυρισμών.

Το *Web Service Policy Framework* (*WS-Policy)* παρέχει μια εύκαμπτη και εκτενή γραμματική για την έκφραση των ικανοτήτων, των απαιτήσεων και των γενικών χαρακτηριστικών των οντοτήτων ενός υπηρεσιοστρεφούς συστήματος βασισμένου στην *XML*. Η *WS-Policy* καθορίζει το πλαίσιο για την έκφραση αυτών των ιδιοτήτων ως πολιτικών. Κάθε πολιτική αποτελεί μια συλλογή εναλλακτικών πολιτικών, ενώ κάθε εναλλακτική πολιτική αποτελεί μια συλλογή πολιτικών ισχυρισμών. Η *WS-Policy* προκειμένου να δηλώσει τους ισχυρισμούς αυτούς χρησιμοποιεί λεξιλόγιο το οποίο δανείζεται από γλώσσες όπως είναι η *WS-Security Policy*, η *WS-ReliableMesaging Policy* και η *WS-Trust* για να περιγράψει τους ισχυρισμούς που αντιστοιχούν σε καθένα από τα πεδία που περιγράφουν οι συγκεκριμένες γλώσσες.

3.2.6 Επίλογος

Καθώς η διατήρηση των δεδομένων επικοινωνίας αυξάνει τις απειλές κατά της ιδιωτικότητας των συνδρομητών υπηρεσιών ηλεκτρονικών επικοινωνιών, δημιουργείται μια ολοένα και μεγαλύτερη ανάγκη για την επίτευξη μιας αποδεκτής ισορροπίας μεταξύ των αρχών της αναλογικότητας και της αποτελεσματικότητας. Μια βασική παράμετρος γι' αυτή την ισορροπία είναι ο καθορισμός του επιτρεπτού χρόνου διατήρησης. Μια εκτεταμένη περίοδος διατήρησης των δεδομένων αυξάνει την έκθεσή τους σε απειλές ασφάλειας, ενώ μια πάρα πολύ μικρή περίοδος ενδέχεται να καταστήσει τη διατήρηση των δεδομένων αναποτελεσματική. Αν και το χρονικό διάστημα διατήρησης διαφέρει από χώρα σε χώρα, διαφαίνεται ότι η μακρά περίοδος διατήρησης δεν καλύπτει τις αρχές της αναλογικότητας και της αναγκαιότητας ή ακόμα και της αποτελεσματικότητας,

εφόσον τα πολύ παλαιά δεδομένα επικοινωνίας σπανίως αποδεικνύονται χρήσιμα σε έλεγχο επιβολής του νόμου.

Το απόρρητο των επικοινωνιών και η ιδιωτικότητα των συνδρομητών υπηρεσιών ηλεκτρονικών επικοινωνιών αποτελούν, σε μια σύγχρονη κοινωνία, θεμελιώδη ανθρώπινα δικαιώματα. Προς αυτή την κατεύθυνση η διατήρηση των δεδομένων επικοινωνίας θα πρέπει να βασίζεται σε καλά ορισμένες αρχές ασφάλειας, όπως είναι ο διπλός έλεγχος και η διάκριση καθηκόντων. Η εφαρμογή διακριτών Αρχών οι οποίες θα ελέγχουν την πρόσβαση στα δεδομένα και την τήρηση διαδικασιών και το επίπεδο ασφάλειας των παρόχων σε συνδυασμό με μηχανισμούς επιβολής πολιτικών ιδιωτικότητας από την πλευρά των παρόχων αποτελούν ορισμένα βήματα προς την ισορροπία ανάμεσα στην ανάγκη επιβολής του νόμου και στην προστασία της ιδιωτικότητας των συνδρομητών. **[7]**

3.3 Η Ασφαλής Ανάκτηση και Ανάλυση των Ψηφιακών Δεδομένων

Η επιστήμη που έχει αντικείμενο την έρευνα και την ανάλυση των ψηφιακών δεδομένων ενός υπολογιστή με σκοπό την εξαγωγή ακέραιων, αδιάβλητων και νομικά έγκυρων ηλεκτρονικών στοιχείων ονομάζεται περιφραστικά ***Ασφαλής Ανάκτηση και Ανάλυση Ψηφιακών Δεδομένων*** *(Computer Forensics*) ή ***Συστηματική Διερεύνηση Υπολογιστών***. Περιλαμβάνει επιπλέον τη μελέτη ειδικών προβλημάτων ασφάλειας, όπως οι τεχνικές ανάκτησης και ανάλυσης πληροφοριακών στοιχείων από οποιονδήποτε τύπο φυσικού φορέα δεδομένων και λειτουργικών συστημάτων, καθώς επίσης και την αναλυτική διερεύνηση των υπολογιστών, όπως και την αποκωδικοποίηση των ενεργειών που πραγματοποιούνται στον υπολογιστή. Η επιστημονική αυτή περιοχή έγινε ιδιαίτερα δημοφιλής στις μέρες μας γιατί έχει συσχετιστεί σε μεγάλο βαθμό με την εξιχνίαση ηλεκτρονικών εγκλημάτων.

Ως ***Ασφαλή Ανάκτηση και Ανάλυση Ψηφιακών Δεδομένων*** ορίζουμε την επιστήμη που έχει αντικείμενο την εφαρμογή μιας μοντελοποιημένης διαδικασίας για την απόκτηση, ανάκτηση, διατήρηση και παρουσίαση των στοιχείων που έχουν υποστεί ηλεκτρονική επεξεργασία ή έχουν αποθηκευτεί σε ένα ηλεκτρονικό μέσο. Είναι μια σύγχρονη επιστημονική περιοχή που εξελίσσεται ταχύτατα και σχετίζεται άμεσα με τον τομέα της ασφάλειας των πληροφοριακών συστημάτων.

Η συστηματική διερεύνηση υπολογιστών περιλαμβάνει την ανάκτηση δεδομένων που έχουν διαγραφεί εσκεμμένα ή μη, έχουν υποστεί βλάβη, είναι κρυφά, είναι προστατευμένα με κωδικούς ή είναι κρυπτογραφημένα, έχουν προσβληθεί από κάποιον ιό ή έχουν καταστραφεί ολοκληρωτικά.

Είναι σημαντικό να αναφέρουμε ότι το αποτέλεσμα μιας συστηματικής διερεύνησης είναι πάντα τεκμηριωμένο και στηρίζεται σε ένα αυστηρά καθορισμένο μοντέλο διερεύνησης και ανάλυσης ψηφιακών δεδομένων, καθιστώντας το αδιαμφισβήτητο ενώπιον ενός οργανισμού ή μιας δικαστικής αρχής. Σημαντικές διαδικασίες της αποτελούν αυτές της διατήρησης, του προσδιορισμού, της εξαγωγής, της τεκμηρίωσης και της ερμηνείας των στοιχείων που διατηρούνται σε ηλεκτρονικά μέσα.

Η διαδικασία αναλυτικής διερεύνησης βασίζεται στην ανάκτηση και ανάλυση των ψηφιακών στοιχείων και δεδομένων που βρίσκονται σε υπολογιστές, στο Διαδίκτυο, καθώς και σε άλλο σχετικό τεχνικό εξοπλισμό και συσκευές. Η επεξεργασία των ψηφιακών δεδομένων γίνεται με βάση ένα αυστηρό μεθοδολογικό πλαίσιο που περιλαμβάνει κανόνες και τεχνικές και πραγματοποιείται με τη βοήθεια ειδικού υλικού και λογισμικού προηγμένης τεχνολογίας και διακρίνεται στα παρακάτω στάδια:

- ***Αποτίμηση:*** Αποτελεί το πρώτο στάδιο στο οποίο πραγματοποιούνται η συγκέντρωση όλων των ψηφιακών δεδομένων και ο προσεκτικός διαχωρισμός τους σ' αυτά που παρουσιάζουν ενδιαφέρον για τη διερεύνηση.
- ***Ανάκτηση*****:** Στο στάδιο αυτό λαμβάνεται ιδιαίτερη μέριμνα για την προστασία των δεδομένων από αλλοιώσεις. Μια αποδεκτή διαδικασία για τη συστηματική διερεύνηση περιλαμβάνει την ακριβή αντιγραφή των δεδομένων και έπειτα τον διεξοδικό έλεγχο του αντιγράφου των δεδομένων.
- ***Εξέταση:*** **Τ**ο στάδιο της εξέτασης περιλαμβάνει αρχικά την διαδικασία άντλησης των δεδομένων από ψηφιακά μέσα αποθήκευσης και την συστηματική ανάλυσή τους και τη μετατροπή τους σε αξιοποιήσιμη μορφή.
- ***Καταγραφή και στοιχειοθέτηση:*** Οι ενέργειες που πραγματοποιούνται και οι παρατηρήσεις καταγράφονται αναλυτικά. Τέλος, η αναλυτική διερεύνηση

ολοκληρώνεται με τη δημιουργία μιας συνολικής αναφοράς που περιλαμβάνει όλα τα ευρήματα.

Η αναζήτηση των ψηφιακών δεδομένων πραγματοποιείται σε ηλεκτρονικές συσκευές που χρησιμοποιούμε καθημερινά ακόμη και αν αυτές δεν έχουν ως κύρια χρήση τους την αποθήκευση δεδομένων. Προσωπικοί υπολογιστές, κινητά τηλέφωνα, φορητά μέσα αποθήκευσης (π.χ. εξωτερικοί σκληροί δίσκοι, *USB drives*), *PDA*, δικτυακός ενεργός εξοπλισμός (*routers, switches)* είναι μερικές συσκευές στις οποίες συνήθως εφαρμόζονται οι τεχνικές *forensics* προκειμένου να βρεθούν τα ζητούμενα στοιχεία.

Σε μια ολοκληρωμένη θεώρηση της συστηματικής διερεύνησης υπολογιστών είναι σημαντικό να αναφέρουμε τις εξής έννοιες:

- ***Φυσικές αποδείξεις (Physical evidence***): Αποτελούν τα φυσικά αντικείμενα που καταδεικνύουν ένα έγκλημα και συνδέουν ένα θύμα με ένα έγκλημα ή ένα έγκλημα με ένα θύτη. Αποτελούνται από τον ίδιο τον υπολογιστή σκληρούς δίσκους, *PDA, CD-ROM* κ.α.
- ***Ψηφιακές αποδείξεις (Digital evidence***): Αποτελούν τα ηλεκτρονικά δεδομένα που επαληθεύουν την προηγούμενη σχέση μεταξύ θύτη, θύματος και εγκλήματος. Είναι τα δεδομένα που βρίσκονται στη μνήμη του υπολογιστή, στο σκληρό δίσκο, σε ένα κινητό τηλέφωνο κ.α.
- ***Η φυσική σκηνή του εγκλήματος (Physical crime scene):*** Αποτελεί το φυσικό περιβάλλον όπου βρίσκονται οι φυσικές αποδείξεις. Το περιβάλλον στο οποίο έγινε η εγκληματική πράξη ορίζεται ως η πρωτεύουσα φυσική σκηνή του εγκλήματος, ενώ οι σχετιζόμενοι υποχώροι ονομάζονται δευτερεύουσες φυσικές σκηνές.
- ***Η ψηφιακή σκηνή του εγκλήματος (Digital crime scene):*** Αποτελεί το εικονικό περιβάλλον που δημιουργήθηκε από υλικό και λογισμικό, όπου υπάρχουν οι ψηφιακές αποδείξεις.
- ***Διερευνητής (Investigator):*** Είναι το φυσικό πρόσωπο (ή ομάδα) που διεξάγει μια έρευνα και διαθέτει την ανάλογη πιστοποίηση γνώσεων και τεχνικών των διαδικασιών ασφαλούς ανάκτησης και ανάλυσης ψηφιακών δεδομένων.
- ***Περιστατικό (Incident):*** Θεωρείται οτιδήποτε μπορεί να αποτελέσει αφορμή για την παρέμβαση μιας ομάδας δράσης και συλλογής ηλεκτρονικών στοιχείων.

3.3.1 Διαδικασία Διερεύνησης Περιστατικών

Η διαδικασία της διερεύνησης και της απόκρισης σε ένα περιστατικό παραβίασης πληροφοριακών συστημάτων θα πρέπει να εξασφαλίζει την ακεραιότητα των δεδομένων κατά την ανάκτησή τους, ώστε να είναι δυνατή η αξιοποίηση των συμπερασμάτων σε μια νομική διαδικασία.

Προκειμένου η διαδικασία της διερεύνησης να είναι αποδεκτή από οργανισμούς, υπηρεσίες, εταιρείες αλλά και πολίτες θα πρέπει να δίνεται ιδιαίτερη προσοχή στα παρακάτω στοιχεία της έρευνας:

- ***Διαφύλαξη:*** Είναι πολύ σημαντικό να μπορεί να αποδειχθεί ότι τα δεδομένα πέρασαν από όλες τις διαδικασίες της έρευνας χωρίς να έχουν υποστεί αλλαγές.

- ***Απόκτηση:*** Η απόκτηση των δεδομένων είναι μια σαφής και καθορισμένη διαδικασία σύμφωνα με την οποία διασφαλίζεται ότι τα δεδομένα δεν έχουν επηρεαστεί από εξωτερικούς, ανθρώπινους ή τεχνολογικούς παράγοντες.
- ***Ανάλυση:*** Αποτελεί την εξαγωγή συμπερασμάτων που σχετίζονται με τις πληροφορίες που μελετήθηκαν.
- ***Ανακάλυψη:*** Είναι η διαδικασία απομόνωσης των στοιχείων που παρουσιάζουν ενδιαφέρον και συσχετίζονται με το προς διερεύνηση περιστατικό.
- ***Τεκμηρίωση:*** Είναι η απόδειξη ότι ακολουθήθηκε με επιμέλεια η καθορισμένη διαδικασία διερεύνησης από την αρχή ως το τέλος της υπόθεσης.
- ***Παρουσίαση:*** Αποτελεί την μετατροπή των συμπερασμάτων της έρευνας σε ένα πλαίσιο κατανοητό και αξιοποιήσιμο από την εταιρεία, την εκτελεστική ή τον ιδιώτη.

Η εξέλιξη της έρευνας που διεξάγει μια διαδικασία συστηματικής διερεύνησης και ανάλυσης ψηφιακών δεδομένων επηρεάζεται, μεταξύ άλλων, από τη φύση του περιστατικού, από τους χρονικούς περιορισμούς για τη διαλεύκανση της υπόθεσης και από το ποιος τελικά παραγγέλνει την έρευνα και για ποιο σκοπό.

Ανάλογα με το περιβάλλον που αιτείται την διερεύνηση μιας υπόθεσης διακρίνουμε τρείς κατηγορίες:

- ***Την εγκληματική διερεύνηση*** που εξετάζει περιπτώσεις παραβίασης νομοθεσίας όπως παιδική πορνογραφία, υπεξαίρεση χρημάτων, παράνομη πρόσβαση σε δεδομένα και απάτη ή δόλο.
- ***Την εταιρική διερεύνηση*** που εξετάζει ενέργειες παραβίασης της πολιτικής ασφάλειας μιας εταιρείας ή ενός οργανισμού, όπως παράνομη πρόσβαση, υποθέσεις εταιρικής απάτης, κατάχρησης υπολογιστικών πόρων, περιπτώσεις πιθανής βιομηχανικής κατασκοπίας, φιλοξενίας περιεχομένου που δεν εμπίπτει στις αρχές του οργανισμού ή ειδικές περιπτώσεις, όπως, για παράδειγμα, όταν κάποιος δυσαρεστημένος υπάλληλος μπορεί να έχει κρύψει σημαντικά αρχεία και πληροφορίες χωρίς να γνωστοποιεί τους κωδικούς πρόσβασης με σκοπό να προκαλέσει ζημιά στην εταιρεία.
- ***Την ιδιωτική διερεύνηση*** που εξετάζει περιπτώσεις υποθέσεων πολιτών, όπως για να διαπιστωθεί μια παράβαση νόμου, είτε περιπτώσεις ανάκτησης δεδομένων, κωδικών και άλλων ευαίσθητων πληροφοριών.

Θα πρέπει να τονίσουμε ότι πολλές φορές το αρχικό περιστατικό, μετά από έρευνα, μεταπίπτει σε άλλη κατηγορία από αυτή που ξεκίνησε. Η αρχική διάκριση καθορίζει κυρίως την πρώτη αντίδραση του διερευνητή, ενώ η μεθοδολογία που χρησιμοποιείται διασφαλίζει πάντα ότι η μετάπτωση από την μια κατηγορία στην άλλη δεν θα επιφέρει απώλεια σημαντικών στοιχείων.

Τέλος, τα υπολογιστικά συστήματα μπορεί να αποτελούν αντικείμενο έρευνας στα πλαίσια μιας διαδικασίας συστηματικής διερεύνησης και ανάλυσης ψηφιακών δεδομένων σε τρία επίπεδα:

- ***Επίπεδο στόχου:*** Το υπολογιστικό σύστημα εκτέθηκε σε παράνομη δραστηριότητα μετά από επίθεση, κατάληψη και χρησιμοποίησή του από τρίτους, συνήθως εν αγνοία του διαχειριστή/ χειριστή του συστήματος.

- ***Επίπεδο φορέα:*** Το υπολογιστικό σύστημα χρησιμοποιήθηκε για να υλοποιήσει στόχους παράνομης ή μη ορθής δραστηριότητας από χρήστες που είχαν πρόσβαση σε αυτό.
- ***Επίπεδο ενδιάμεσου:*** Όταν το υπολογιστικό σύστημα δεν χρησιμοποιήθηκε ακριβώς σε κάποια διαδικασία αλλά σ' αυτό μπορούμε να εντοπίσουμε ενδιαφέροντα στοιχεία όπως σε *firewall logs*, *intrusion detection logs* κ.α.

3.3.2 Μοντέλα Ασφαλούς Ανάκτησης και Ανάλυσης Ψηφιακών Δεδομένων

Σε μια διαδικασία ασφαλούς ανάκτησης και ανάλυσης ψηφιακών δεδομένων υπάρχει η ανάγκη ύπαρξης ενός καθορισμένου μεθοδολογικού πλαισίου που θα εξασφαλίζει για κάθε υπόθεση που διερευνάται την εγκυρότητα των αποτελεσμάτων προκειμένου να κατατεθούν σε δικαστικούς ή άλλους φορείς. Επομένως η αναγκαιότητα εφαρμογής κατάλληλων μοντέλων κατά την διαδικασία διερεύνησης δεν προκύπτει μόνο ως μια επιστημονική αναγκαιότητα που εξυπηρετεί τους μελετητές και την μεταξύ τους επικοινωνία, αλλά πολύ περισσότερο εξασφαλίζει την εγκυρότητα των στοιχείων και ενισχύει την αποδεικτική τους ισχύ.

Ένα μοντέλο ασφαλούς ανάκτησης και ανάλυσης ψηφιακών δεδομένων πρέπει να ικανοποιεί τις παρακάτω αρχές:

- Το μοντέλο θα πρέπει να βασίζεται στις καλώς ορισμένες αρχές της κλασσικής έρευνας των φυσικών παραβιάσεων.
- Το μοντέλο θα πρέπει να είναι εφαρμόσιμο και να ακολουθεί διαδικασίες, όπως αυτές ορίζονται και σε μια διερεύνηση εγκληματικής ενέργειας του φυσικού κόσμου.
- Το μοντέλο θα πρέπει να αξιοποιεί το υφιστάμενο τεχνολογικό πλαίσιο, αλλά να είναι ανεξάρτητο από συγκεκριμένα προϊόντα και διαδικασίες.
- Το μοντέλο θα πρέπει να έχει εκείνο τον βαθμό λεπτομέρειας ώστε σε κάθε φάση του οι τεχνολογικές απαιτήσεις που θέτει να μπορούν να ικανοποιηθούν.
- Το μοντέλο θα πρέπει να διαθέτει τον απαραίτητο βαθμό γενίκευσης ώστε να μπορεί να χρησιμοποιηθεί τόσο σε έρευνες παραβίασης του νόμου όσο και σε επιχειρησιακές υποθέσεις, αλλά και στις περιπτώσεις διαχείρισης ενός περιστατικού παραβίασης ασφάλειας.

Έως σήμερα έχει προταθεί μια πληθώρα μοντέλων ασφαλούς ανάκτησης και ανάλυσης ψηφιακών δεδομένων, που έχουν τη βάση τους σε τρία κύρια διαδικαστικά μοντέλα, τα οποία παρουσιάζονται πιο κάτω.

3.3.2.1 Το Μοντέλο Διαδικασίας Ψηφιακής Δικανικής Ανάλυσης (*Forensics Process)*

Το *Forensic Process Model* έχει προταθεί από το *National Institute of Standards and Technology (NIST)*, έχει υιοθετηθεί από το Υπουργείο Δικαιοσύνης των ΗΠΑ και αποτελεί ένα γενικό διαδικαστικό μοντέλο οδηγό, που πρέπει να τηρείται σε κάθε περιστατικό διερεύνησης παραβιάσεων ασφάλειας.

Αποτελείται από τέσσερις βασικές φάσεις:

- ***Την συλλογή:*** Αποτελεί την αρχική φάση του μοντέλου και περιλαμβάνει την αναγνώριση, την ταξινόμηση, την καταγραφή και την απόκτηση δεδομένων από τις πιθανές πηγές, ακολουθώντας πάντα διαδικασίες που εξασφαλίζουν την ακεραιότητα των δεδομένων. Η συλλογή διενεργείται πάντα σε συνάρτηση

με το χρόνο εξαιτίας της πιθανότητας απωλειών δυναμικών στοιχείων όπως οι τρέχουσες διαδικτυακές συνδέσεις, καθώς επίσης και η απώλεια δεδομένων από ηλεκτρικές συσκευές (π.χ. κινητά τηλέφωνα, *PDAs*).

- ***Την εξέταση:*** Είναι η φάση που σχεδιάστηκε για να ενισχύσει τη διαφάνεια των στοιχείων, ενημερώνοντας κάθε φορά για την προέλευσή τους αλλά και την σπουδαιότητά τους. Περιλαμβάνει την επεξεργασία μεγάλου όγκου δεδομένων χρησιμοποιώντας συνδυασμούς αυτοματοποιημένων και μη διαδικασιών για την αξιολόγηση και την εξαγωγή δεδομένων ιδιαίτερου ενδιαφέροντος κι έχει πάντα κύριο μέλημά της την ακεραιότητα των δεδομένων που επεξεργάζεται.
- ***Την ανάλυση:*** Η επόμενη φάση της διαδικασίας είναι η ανάλυση και η αξιολόγηση των συμπερασμάτων που προέκυψαν από την φάση της εξέτασης. Από την αξιολόγηση αυτή κρίνεται αν τα στοιχεία που έχουν ανακτηθεί είναι επαρκή ώστε να επιτευχθεί ο στόχος που τέθηκε στην αρχή της έρευνας ή εάν η έρευνα πρέπει να συνεχιστεί σε μεγαλύτερο βάθος.
- ***Την αναφορά:*** Η τελική φάση είναι η καταγραφή των αποτελεσμάτων της ανάλυσης, η οποία περιλαμβάνει την περιγραφή των ενεργειών που πραγματοποιήθηκαν, την καταγραφή των εργαλείων που χρησιμοποιήθηκαν κατά την έρευνα και τον τρόπο χρήσης τους, ενώ προσδιορίζει ποιές άλλες ενέργειες απαιτούνται (π.χ. εξέταση επιπλέον πηγών δεδομένων, εξασφάλιση των καταγεγραμμένων ευπαθειών, ισχυροποίηση υφιστάμενων ελέγχων ασφάλειας). Τέλος, παρέχει οδηγίες για τη βελτίωση πολιτικών, οδηγιών, διαδικασιών, εργαλείων και άλλων θεμάτων για την αποφυγή στο μέλλον παραβιάσεων παρόμοιων με το προς εξέταση περιστατικό.

3.3.2.2 Το Μοντέλο Αποσπάσματος Ψηφιακής Δικανικής Ανάλυσης (*Abstract Digital Forensics)*

Το μοντέλο *Abstract Digital Forensics* προτείνει μια αυστηρά καθορισμένη διαδικασία, η οποία περιλαμβάνει τα παρακάτω εννιά στάδια:

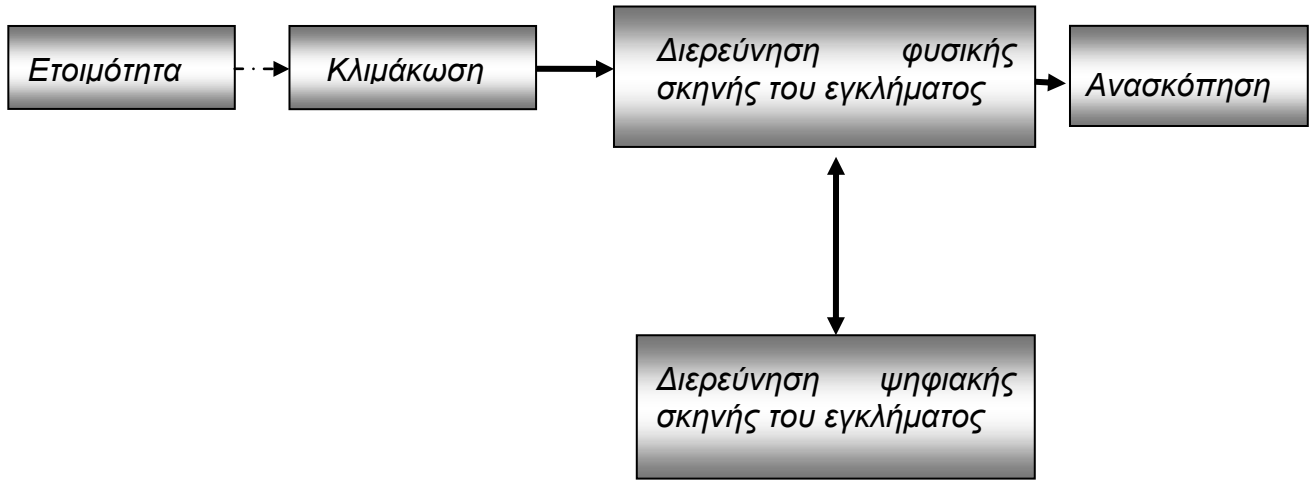
- ***Προσδιορισμός:*** Ανάλογα με τις ενδείξεις που υπάρχουν, προσδιορίζεται ο τύπος του περιστατικού που πρόκειται να διερευνηθεί.
- ***Προετοιμασία:*** Περιλαμβάνει την προετοιμασία των απαιτούμενων ενταλμάτων και εξουσιοδοτήσεων έρευνας, των εργαλείων και των τεχνικών που πρόκειται να χρησιμοποιηθούν, αλλά και την οργάνωση της τεχνικής υποστήριξης.
- ***Στρατηγική προσέγγισης:*** Αναπτύσσει την κατάλληλη διαδικασία βάσει της οποίας η έρευνα θα μεγιστοποιήσει τον αριθμό των αποδείξεων στον ελάχιστο δυνατό χρόνο, ελαχιστοποιώντας τις επιπτώσεις στο θύμα.
- ***Διατήρηση:*** Περιλαμβάνει την απομόνωση, την διασφάλιση και την διατήρηση της κατάστασης στην οποία εντοπίστηκαν τόσο τα φυσικά όσο και τα ψηφιακά στοιχεία.
- ***Συλλογή:*** Περιλαμβάνει την καταγραφή της φυσικής σκηνής του προς διερεύνηση γεγονότος, αλλά και την αντιγραφή όλων των ψηφιακών μέσων και στοιχείων, σύμφωνα πάντα με γενικά αποδεκτές και πλήρως καθορισμένες διαδικασίες.
- ***Εξέταση:*** Περιλαμβάνει την διεξοδική και συστηματική έρευνα για δεδομένα που συσχετίζονται με το περιστατικό που διερευνάται.

- ***Ανάλυση:*** Έχει βασικό σκοπό τον καθορισμό της σπουδαιότητας κάθε δεδομένου ή στοιχείου που εντοπίστηκε, την ανακατασκευή κατακερματισμένων δεδομένων αλλά και την εξαγωγή συμπερασμάτων βασισμένων στα στοιχεία που ανακτήθηκαν.
- ***Παρουσίαση:*** Περιλαμβάνει την περίληψη αλλά και την επεξήγηση των συμπερασμάτων της έρευνας που διενεργήθηκε.
- ***Επιστροφή των στοιχείων:*** Εξασφαλίζει την επιστροφή τόσο των φυσικών όσο και των ψηφιακών στοιχείων στο νόμιμο κάτοχό της.

3.3.2.3 Το Μοντέλο Ολοκληρωμένης Ψηφιακής Διερεύνησης (*Integrated Digital Investigation)*

Αποτελεί ένα ολοκληρωμένο μοντέλο το οποίο οργανώνει τις διαδικασίες διερεύνησης σε πέντε ξεχωριστές ομάδες που αποτελούνται συνολικά από δεκαεπτά φάσεις.

Οι διακριτές αυτές ομάδες είναι **η ετοιμότητα, η κλιμάκωση, η διερεύνηση της φυσικής σκηνής του εγκλήματος, η διερεύνηση της ψηφιακής σκηνής του εγκλήματος και η ανασκόπηση.** Η σειρά εκτέλεσής τους διακρίνεται στο ***σχήμα*:**



Σχήμα 14: Ομάδες ενεργειών και η συσχέτισή τους

3.3.2.3.1 Ετοιμότητα

Οι φάσεις που περιλαμβάνονται στην ομάδα της ετοιμότητας (*readiness*) έχουν στόχο να πιστοποιήσουν ότι οι διαδικασίες και η υποδομή είναι ικανές να υποστηρίξουν την έρευνα στο σύνολό της.
Η συγκεκριμένη ομάδα περιλαμβάνει ξεχωριστή φάση που αναφέρεται στις διαδικασίες *(operations readiness phase)* και ξεχωριστή φάση που αναφέρεται στην υποδομή *(infrastructure readiness phase).*
Η ***φάση της ετοιμότητας των διαδικασιών*** προβλέπει την κατάλληλη εκπαίδευση στα άτομα που θα ασχοληθούν με τη διερευνητική διαδικασία, την επιβεβαίωση της καταλληλότητας του λογισμικού και του υλικού που θα χρησιμοποιηθούν και την ετοιμότητα του εργαστηριακού εξοπλισμού για την περαιτέρω ανάλυση των ευρημάτων που θα προσκομισθούν.

Η δεύτερη ***φάση της ετοιμότητας των υποδομών*** διασφαλίζει ότι τα δεδομένα που θα πρέπει να αναλυθούν υπάρχουν και θα υπάρχουν σε φυσικό επίπεδο. Η φάση αυτή περιλαμβάνει, μεταξύ άλλων, και την τοποθέτηση καμερών ή και υλικού αναγνώρισης του εισερχόμενου προσωπικού στην περιοχή που θα γίνει η συλλογή των στοιχείων.

3.3.2.3.2 Κλιμάκωση

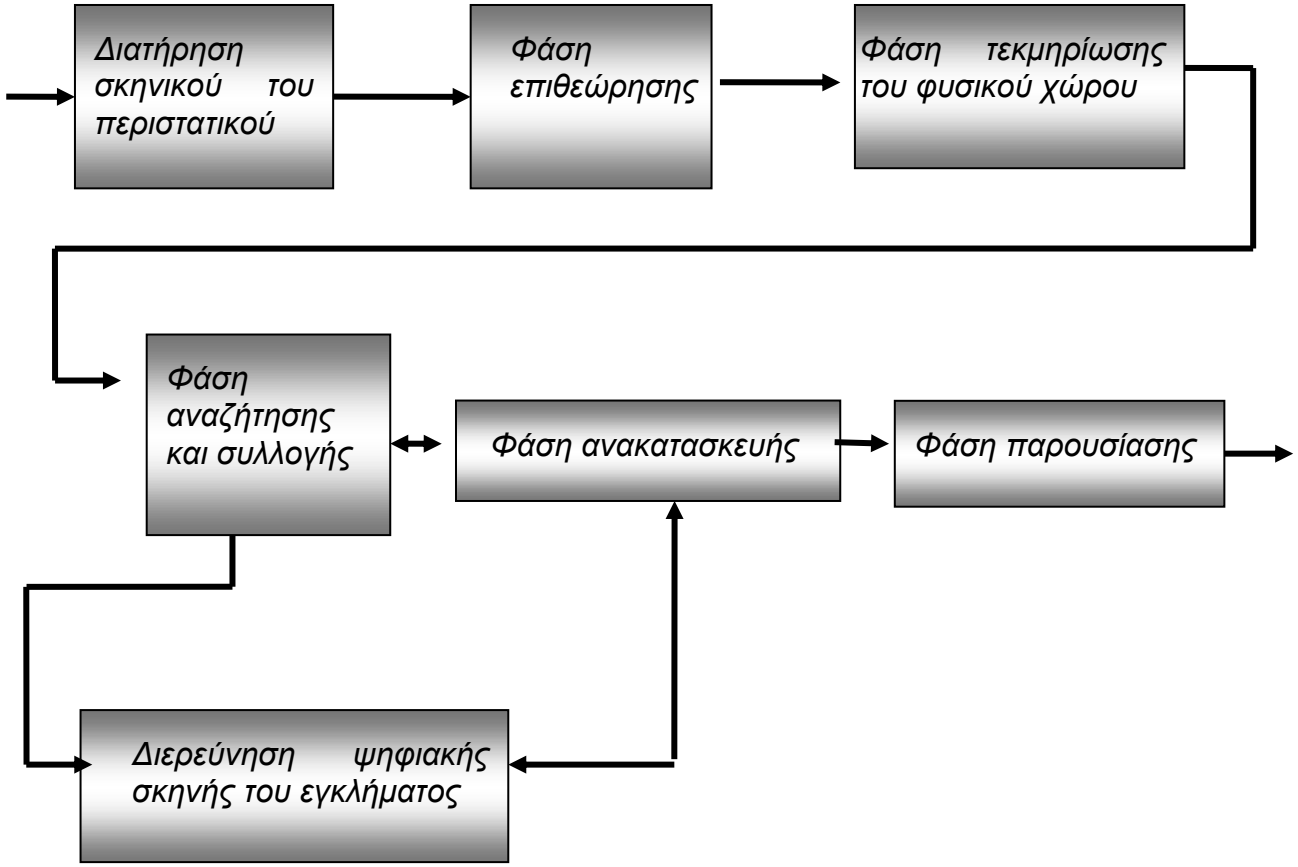
Η ομάδα της ***κλιμάκωσης*** (*deployment*) της διερευνητικής διαδικασίας πιστοποιεί την αναγνώριση και την εξακρίβωση ενός περιστατικού και διαμορφώνεται ανάλογα με την φύση του περιστατικού.

Υπάρχουν δύο φάσεις και σε αυτή την κατηγορία:

- Κατά την πρώτη φάση της ***αναγνώρισης και κοινοποίησης*** *(detection and notification phase)* εντοπίζεται το περιστατικό ενώ ειδοποιούνται τα κατάλληλα για τη διαδικασία άτομα. Ο εντοπισμός μπορεί να προέρχεται από μια ποικιλία τρόπων όπως, για παράδειγμα, από μια καταγγελία ή ένα σύστημα ανίχνευσης εισβολής (*IDS*). Με αυτή τη φάση καθορίζεται και η έναρξη της διαδικασίας διερεύνησης του περιστατικού.
- Η δεύτερη φάση της ***εξακρίβωσης και εξουσιοδότησης*** *(confirmation and authorization phase)* περιλαμβάνει τη διαδικασία απόκτησης εξουσιοδοτήσεων για την διεξαγωγή της έρευνας και διαφοροποιείται για περιπτώσεις επιβολής του νόμου σε σχέση με επιχειρησιακά περιστατικά. Στην πρώτη περίπτωση απαιτείται ένταλμα έρευνας, ενώ στην δεύτερη συνήθως αρκεί να μην παραβιάζονται πολιτικές προστασίας δικαιωμάτων όπως έχουν θεσμοθετηθεί από την εταιρεία.

3.3.2.3.3 Διερεύνηση της Φυσικής Σκηνής του Εγκλήματος

Η ομάδα διερεύνησης της ***φυσικής σκηνής του εγκλήματος*** *(physical crime scene)* έχει στόχο την συλλογή και την ανάλυση των ***φυσικών στοιχείων*** (*physical evidence)* με σκοπό να εξαχθούν συμπεράσματα για την χρονική σειρά των γεγονότων που έλαβαν χώρα ώστε να ανακατασκευαστεί η αλληλουχία τους που κατέληξε στο περιστατικό. Διακρίνεται, όπως φαίνεται και στο ***σχήμα 15***, στις παρακάτω φάσεις:



Σχήμα 15: Διερεύνηση της φυσικής σκηνής του εγκλήματος

1. Αρχικά στη ***διατήρηση του σκηνικού του περιστατικού*** (*preservation phase*), διαδικασία η οποία είναι όμοια με αντίστοιχη μη ηλεκτρονικού περιστατικού. Σε αυτή διατηρούμε τη σκηνή καθαρή και ασφαλή ώστε σε επόμενη φάση να μπορεί να γίνει συλλογή των στοιχείων χωρίς αυτά να έχουν αλλοιωθεί.
2. Ακολουθεί η φάση της ***επιθεώρησης*** *(survey phase)* η οποία συντελεί στη διατύπωση μιας αρχικής θεωρίας για το περιστατικό. Συνήθως περιλαμβάνει μια περιήγηση στους χώρους που μπορεί να υπάρχουν στοιχεία που σχετίζονται με το περιστατικό, εντοπίζονται *PDA* και άλλες ηλεκτρονικές συσκευές που πιθανόν να χρησιμοποιήθηκαν, κομμάτια χαρτιού με κωδικούς πρόσβασης και άλλες σημειώσεις, δωμάτια με *servers*, το δίκτυο γενικότερα και οι υπολογιστές, η φυσική τους διασύνδεση κ.α.
3. Στη συνέχεια υλοποιείται η φάση της ***τεκμηρίωσης φυσικού χώρου*** *(documentation phase*), η οποία σε αντιστοιχία με τη διαδικασία των μη ηλεκτρονικών περιστατικών περιλαμβάνει φωτογραφήσεις του χώρου, βίντεο, σκίτσα και επιπλέον καταγραφή και φωτογράφηση των συνδέσεων στον υπολογιστή, καθώς και πλήρη καταγραφή της κατάστασης στην οποία βρίσκονται τα μηχανήματα (π.χ. το πλήθος και το μέγεθος των σκληρών δίσκων, το μέγεθος της μνήμης κ.α.).
4. Η επόμενη φάση είναι αυτή της ***αναζήτησης και συλλογής*** *(search and collection)*, η οποία περιλαμβάνει τη διεξοδική αναζήτηση και συλλογή από την

σκηνή του περιστατικού όσο το δυνατόν περισσότερων φυσικών στοιχείων, τα οποία θα μπορούσαν να βοηθήσουν στην ηλεκτρονική διαλεύκανση της υπόθεσης.

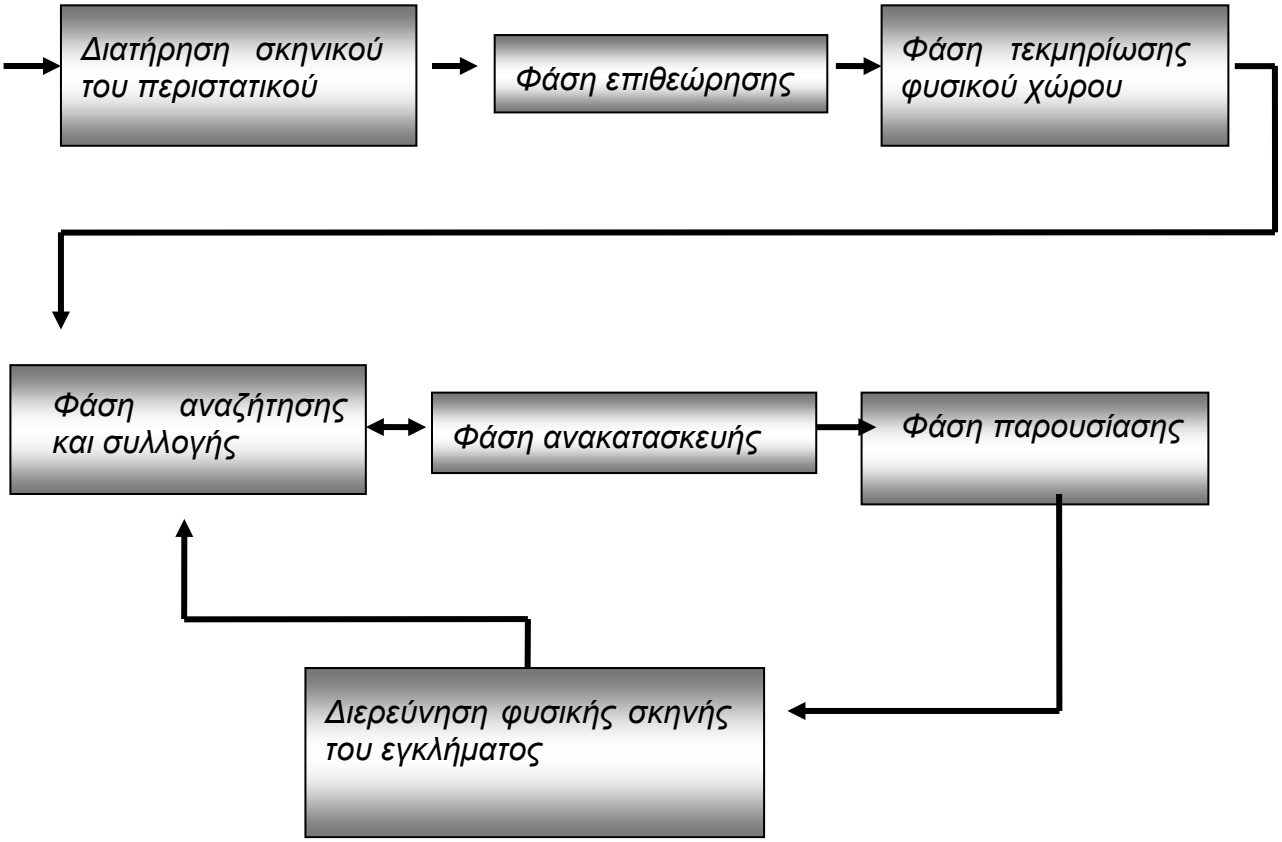
5. Στην αμέσως επόμενη φάση της ***ανακατασκευής*** (*reconstruction*) γίνονται η οργάνωση και η ομαδοποίηση των αποτελεσμάτων ύστερα από την ανάλυσή τους έτσι ώστε αυτά να χρησιμοποιηθούν κατάλληλα για τη δημιουργία μιας θεωρίας σχετικά με το γεγονός.
6. Τέλος, η φάση της ***παρουσίασης*** (*presentation*) έχει σκοπό την παρουσίαση των φυσικών και ψηφιακών στοιχείων στο δικαστήριο ή στη διοίκηση της εταιρείας που ζήτησε την έρευνα.

3.3.2.3.4 Διερεύνηση της Ψηφιακής Σκηνής του Εγκλήματος

Η ομάδα διερεύνησης της ψηφιακής σκηνής του εγκλήματος *(digital crime scene)* έχει στόχο την συλλογή και την ανάλυση των ψηφιακών στοιχείων (*digital evidence)* με σκοπό να εξαχθούν συμπεράσματα για την χρονική σειρά των ηλεκτρονικών δραστηριοτήτων που έλαβαν χώρα ώστε να ανακατασκευαστεί η αλληλουχία τους που κατέληξε στο περιστατικό.

Οι φάσεις από τις οποίες διέρχεται η παραπάνω συστηματική διερεύνηση είναι οι εξής:

1. Η ***διατήρηση του σκηνικού του περιστατικού*** (*preservation phase)* στην οποία διατηρούμε την ηλεκτρονική σκηνή του συμβάντος ανεπηρέαστη από εξωτερικούς παράγοντες, ώστε σε επόμενη φάση να μπορούν να γίνουν συλλογή και ανάλυση στοιχείων χωρίς αυτά να έχουν αλλοιωθεί.
2. Η φάση της ***επιθεώρησης*** (*survey phase)* στην οποία όλα τα συσχετιζόμενα με την έρευνα δεδομένα μεταφέρονται σε ελεγχόμενο χώρο για κατάλληλη επεξεργασία.
3. Η φάση της ***τεκμηρίωσης φυσικού χώρου*** κατά την οποία γίνεται πλήρης καταγραφή των ψηφιακών στοιχείων όταν αυτά εντοπιστούν. Η καταγραφή αυτή είναι πολύ χρήσιμη κατά τη φάση της παρουσίασης (*presentation*).
4. Η φάση της ***αναζήτησης και συλλογής*** *(search and collection*), η οποία περιλαμβάνει διεξοδική ανάλυση των ψηφιακών στοιχείων. Ειδικό λογισμικό χρησιμοποιείται για την αποκάλυψη κρυφών, διαγραμμένων ή αρχείων με βλάβη που είχαν χρησιμοποιηθεί, ενώ παράλληλα δίνονται στοιχεία όπως ημερομηνίες, διάρκεια χρήσης κ.α. Γίνεται επίσης μια αδρή χρονολογική καταγραφή για τον εντοπισμό δραστηριότητας και ταυτότητας.
5. Η φάση της ***ανακατασκευής*** (*reconstruction*) κατά την οποία πραγματοποιούνται οργάνωση και ομαδοποίηση των ψηφιακών αποτελεσμάτων ύστερα από την ανάλυσή τους, έτσι ώστε αυτά να χρησιμοποιηθούν κατάλληλα για τη δημιουργία μιας υπόθεσης σχετικά με την αιτία πρόκλησης του συμβάντος.
6. Τέλος, η φάση της ***παρουσίασης*** (*presentation*) έχει σκοπό την παρουσίαση των ψηφιακών στοιχείων στην ομάδα διερεύνησης της φυσικής σκηνής του εγκλήματος.



Σχήμα 16: Διερεύνηση της ψηφιακής σκηνής

3.3.2.3.5 Ανασκόπηση

Περιλαμβάνει μια γενική αλλά ταυτόχρονα συνολική ανασκόπηση της έρευνας εντοπίζοντας σημεία στα οποία θα μπορούσε να υπάρξει βελτίωση της απόδοσης. Τονίζονται όλα εκείνα τα στοιχεία και τα γεγονότα τα οποία αναδομήθηκαν με σκοπό την επίτευξη του στόχου της έρευνας έτσι ώστε σε παρόμοιες υποθέσεις να χρησιμοποιηθεί η ήδη υπάρχουσα γνώση.

3.3.3 Διαδικασίες Διαχείρισης Παραβιάσεων

Διακρίνουμε δύο κατηγορίες διαδικασιών διαχείρισης περιστατικών ανάλογα με το αν τα συστήματα που πιθανόν συμμετείχαν στο περιστατικό συνεχίζουν να είναι σε λειτουργία ή όχι.

Η ***εν λειτουργία διερεύνηση ή ενεργητική διερεύνηση*** *(live forensics response*), αφορά στην κατάσταση κατά την οποία τα μηχανήματα που θεωρείται ότι πήραν μέρος στο περιστατικό βρίσκονται εν λειτουργία. Η ***εκτός λειτουργίας διερεύνηση ή παθητική διερεύνηση*** *(incident postmortem*) αφορά στην περίπτωση κατά την οποία τα μηχανήματα βρίσκονται εκτός λειτουργίας. Η διάκριση αυτή επηρεάζει άμεσα την απόφαση για το πώς θα γίνει ο χειρισμός του περιστατικού.

Οι δύο αυτές κατηγορίες αναφέρονται στη φάση της απόκτησης, της συλλογής και της ανάλυσης των στοιχείων, όπως αυτές περιγράφονται, ίσως με μικρές διαφοροποιήσεις

στα μοντέλα που αναφέραμε. Στην πραγματικότητα όταν το σύστημα είναι ενεργό, τότε εκτελούνται και οι δύο διαδικασίες, πρώτα η ενεργητική διερεύνηση και μετά η παθητική διερεύνηση. Η διαφορά είναι ότι, όταν το σύστημα είναι σε λειτουργία, ποτέ δεν το απενεργοποιούμε πριν εκτελέσουμε τις κατάλληλες διαδικασίες, ενώ όταν είναι απενεργοποιημένο, δεν το ανοίγουμε αν δεν εξασφαλίσουμε τρόπους που διατηρούν την ακεραιότητα των στοιχείων.

3.3.3.1 Εν Λειτουργία Διερεύνηση *(Live Forensics)*

Ενεργητική ή εν λειτουργία διερεύνηση *(live forensics response*) είναι η διαδικασία συλλογής στοιχείων από ένα μηχάνημα το οποίο βρίσκεται σε λειτουργία (είναι ενεργό). Τα στοιχεία που συλλέγονται σε αυτή τη διαδικασία χωρίζονται σε ευμετάβλητα (*volatile*) και μη ευμετάβλητα (*non-volatile*). Πιο συγκεκριμένα:

- ***Ευμετάβλητα*** (*volatile*) είναι τα στοιχεία που μπορεί να εξαφανιστούν όπως τα στοιχεία που υπάρχουν στους διάφορους καταχωρητές, στην *cache*, στη *RAM*, η κατάσταση του δικτύου και οι διεργασίες που εκτελούνται εκείνη τη στιγμή.
- ***Μη ευμετάβλητα*** *(non-volatile)* είναι τα στοιχεία που μπορούμε να ανακτήσουμε και αργότερα κατά την ανάλυση, προτιμούμε όμως να αποκτηθούν κατά την εν λειτουργία διερεύνηση, καθώς η διαδικασία ανάκτησής τους γίνεται πολύ πιο σύνθετη στην περίπτωση της εκτός λειτουργίας διερεύνησης. Για παράδειγμα, θα μπορούσαν να ανακτηθούν τα αρχεία συμβάντων *(event logs)* αργότερα, αλλά η *raw binary* μορφή τους θα έκανε τη διαδικασία πολύ πιο επίπονη. Μη ευμετάβλητα στοιχεία θεωρούνται, εκτός των αρχείων συμβάντων, τα *MAC* δεδομένα για αρχεία, τα *alternate data streams (ADS),* συνηθισμένα αρχεία ή δεδομένα που παρουσιάζουν ενδιαφέρον, αντίγραφο της *registry* κ.α.

Κατά την εν λειτουργία διερεύνηση δίνεται προτεραιότητα στο να καταγραφεί και να στοιχειοθετηθεί οτιδήποτε αποτελεί ευμετάβλητο στοιχείο, ενώ γίνεται προσπάθεια να αποκτηθούν όσο το δυνατόν περισσότερα μη ευμετάβλητα στοιχεία χωρίς να επηρεαστεί η κατάσταση του συστήματος.

Η εν λειτουργία διερεύνηση στοιχείων θα πρέπει να έχουμε υπόψη ότι διακρίνεται για τη μεγάλη και αποτελεσματική συμβολή στη διαδικασία διερεύνησης, αλλά έχει και σημαντικά μειονεκτήματα τα οποία θα πρέπει να αξιολογούμε κάθε φορά.

Πλεονεκτήματα

Πολλά στοιχεία μπορεί να βρίσκονται σε μέρη του υπολογιστικού συστήματος που όταν τίθενται εκτός λειτουργίας καταστρέφονται, όπως για παράδειγμα η μνήμη *RAM*. Από τη μνήμη *RAM* ανακτώνται πολλές πληροφορίες όπως κωδικοί πρόσβασης (*passwords)*, τα περιεχόμενα του *clipboard* ή *sessions* από προγράμματα ανταλλαγής μηνυμάτων κ.α. Δεν υπάρχει τρόπος να ανακατασκευαστούν αυτά τα δεδομένα από τη στιγμή που θα κλείσει το σύστημα, συμπεριλαμβανομένων πληροφοριών όπως η ώρα και η μέρα του συστήματος ή ποιές συνδέσεις και ποιές θύρες επικοινωνίας είναι ανοιχτές.

Τα συμπεράσματα που προκύπτουν από το συνδυασμό των ευμετάβλητων και μη στοιχείων αποτελούν μια καλή αρχή για την έναρξη των υποθέσεων του διερευνητή ώστε να αποφασίσει σε ποιό βαθμό έχει εξελιχθεί ένα συμβάν και να εκτιμήσει ποιά είναι τα ορθότερα μέτρα για την αντιμετώπιση ή τη διερεύνηση.

Μειονεκτήματα

Όλες οι ενέργειες που γίνονται κατά τη διάρκεια μιας ερευνητικής διαδικασίας, όπως έχει συζητηθεί και προηγουμένως, πρέπει να γίνονται με σεβασμό της αρχής της

διατήρησης των στοιχείων και του σκηνικού του συμβάντος που χρήζει έρευνας. Η διαδικασία της εν λειτουργίας διερεύνησης δεν ανταποκρίνεται με τον καλύτερο τρόπο σε αυτή την αρχή, καθώς επηρεάζει πολλές φορές το υπό εξέταση υπολογιστικό σύστημα. Για παράδειγμα, τα εργαλεία ή οι εντολές που θα χρησιμοποιηθούν για να αποκτηθούν τα περιεχόμενα της *RAM* είναι φυσικό ότι θα την αλλάξουν σε ένα μικρό βαθμό, καθώς αυτά τα εργαλεία θα φορτωθούν στη μνήμη κατά την εκτέλεσή τους.

Τα εργαλεία που θα χρησιμοποιηθούν θα πρέπει να είναι εγκεκριμένα και να τεκμηριώνεται ότι δεν αλλοιώνουν τα δεδομένα και τα στοιχεία του συστήματος. Επίσης όταν έχει ολοκληρωθεί η διαδικασία συλλογής των στοιχείων, επιλέγουμε να τεθεί εκτός λειτουργίας το σύστημα, μέσω της διακοπής ηλεκτροδότησης του συστήματος και όχι μέσω της τυπικής διαδικασίας σβησίματος που υποστηρίζουν τα περισσότερα λειτουργικά συστήματα.

Τέλος, ένα ακόμα μεγάλο μειονέκτημα που έχει η εν λειτουργία διερεύνηση είναι ότι σε περίπτωση που το σύστημα που μελετάται έχει μολυνθεί από κακόβουλο λογισμικό (ιδιαίτερα από κώδικα που μπορεί να επηρεάζει και να αλλοιώνει τα δεδομένα), τότε μπορεί να έχουν διαγραφεί πληροφορίες και στοιχεία που ενοχοποιούν το χρήστη και να επηρεάζουν την ίδια τη διαδικασία της διερεύνησης.

3.3.3.2 Εκτός Λειτουργίας Διερεύνηση

Ως ***εκτός λειτουργίας διερεύνηση ή παθητική διερεύνηση*** *(incident postmortem forensics)* χαρακτηρίζουμε τη διαδικασία συλλογής στοιχείων από ένα μηχάνημα το οποίο βρίσκεται εκτός λειτουργίας.

Η κατηγορία αυτή εντάσσεται στο πλαίσιο της εξέτασης των δεδομένων, αφού αυτά προσδιοριστούν κατά το στάδιο της αναζήτησης και συλλογής. Για να εξασφαλιστεί η ακεραιότητα των στοιχείων, θα πρέπει να προηγηθεί μια σειρά ενεργειών. Πιο συγκεκριμένα:

Είναι πιο ασφαλές και δόκιμο υπό το πρίσμα της επιστήμης της διερεύνησης ηλεκτρονικών στοιχείων, τα δεδομένα από όλα τα συστήματα να αναλύονται σε ένα κατάλληλο εργαστήριο. Για το λόγο αυτό θα πρέπει τα στοιχεία να αντιγραφούν *bit* προς *bit* δημιουργώντας ακριβές αντίγραφο (*image*) όλων των αποθηκευτικών μέσων, κάτι που εξασφαλίζει ότι όλα τα δεδομένα του αποθηκευτικού μέσου έχουν αντιγραφεί επακριβώς σε καινούργιο μέσο το οποίο έχει πρώτα τεχνικά αποστειρωθεί. Η αποστείρωση περιλαμβάνει τον τρόπο με τον οποίο κάνουμε ένα μέσο «καθαρό» από κάθε είδους δεδομένα που φιλοξενούνται σε αυτό, ή από υπολείμματα παλαιότερων δεδομένων.

Πλεονεκτήματα

Επειδή τα αποθηκευτικά μέσα υποβάλλονται στη διαδικασία του *imaging*, ενώ το υπολογιστικό σύστημα είναι κλειστό, η αλλοίωση των δεδομένων πάνω στο σύστημα που θα διερευνηθεί είναι ανύπαρκτη. Η μελέτη των δεδομένων περιλαμβάνει περιοχές που θα ήταν αδύνατο να ερευνηθούν σε ένα ενεργό σύστημα υπό την προστασία του λειτουργικού του συστήματος. Τα συμπεράσματα που προκύπτουν μπορούν να θεωρηθούν περισσότερο ασφαλή, κάτι που κάνει τη διαδικασία της ανάλυσης και της εξακρίβωσης του περιστατικού πολύ πιο συνεπή. Η διαδικασία του *imaging* περιλαμβάνει τρόπους, όπως το *hash-copy-hash*, οι οποίοι αποδεικνύουν με αδιαμφισβήτητο τρόπο ότι τα δεδομένα δεν επηρεάστηκαν ούτε μορφοποιήθηκαν. Η διαδικασία αυτή περιλαμβάνει τη χρήση συναρτήσεων σύνοψης (*hashes*) στον αρχικό τόμο και στον τελικό μετά την *bit* προς *bit* αντιγραφή του, για να αποδειχθεί ότι κανένα δεδομένο δεν τροποποιήθηκε.

Επίσης η μέθοδος αυτή είναι πιο ασφαλής από την επιρροή ιομορφικού λογισμικού (κάτι που δεν ισχύει στην εν λειτουργία διερεύνηση), αφού η ανάλυση γίνεται σε ένα «νεκρό» σύστημα στο οποίο απλώς εξάγονται τα δεδομένα με συγκεκριμένες τεχνικές σε χαμηλό επίπεδο και δεν είναι ενεργές πιθανώς μολυσμένες διεργασίες.

Μειονεκτήματα

Τα μειονεκτήματα αυτής της μεθόδου είναι κυρίως η έλλειψη των πλεονεκτημάτων της εν λειτουργία διερεύνησης. Δηλαδή το γεγονός ότι από τη στιγμή που θα τεθεί εκτός λειτουργίας ένα σύστημα χάνονται δεδομένα τα οποία συμβαίνουν εκείνη τη στιγμή, όπως διεργασίες που τρέχουν, χρήστες οι οποίοι είναι ενεργοί μέσα στο σύστημα τη στιγμή του περιστατικού, αρχικοποιημένες συνδέσεις και συγκεκριμένη δικτυακή κίνηση.

3.3.4 Τεχνικές Ανάκτησης και Ανάλυσης Αρχείων

3.3.4.1 Απόκρυψη Αρχείων – Κατάλοιπα Δεδομένων

Οι τεχνικές απόκρυψης αρχείων (*data hiding*) είναι αρκετές και ένας διερευνητής πρέπει να τις γνωρίζει προκειμένου να μην παραβλέψει σημεία του υπολογιστικού συστήματος στα οποία θα μπορούσαν να βρεθούν στοιχεία.

Η απόκρυψη δεδομένων μπορεί να πραγματοποιηθεί σε τρία επίπεδα:

- ***Στο επίπεδο διαχείρισης αποθηκευτικών μέσων*** *(media management layer),*
- ***Στο επίπεδο συστήματος αρχείων*** *(file system layer),*
- ***Στο επίπεδο εφαρμογών*** *(application layer).*

Στο επίπεδο ***διαχείρισης αποθηκευτικών μέσων*** (*media management layer*), το αποθηκευτικό μέσο χωρίζεται από φυσική άποψη σε μικρότερα τμήματα, τα *partitions* ή τους τόμους (*volumes*). Σε αυτό το επίπεδο οι τεχνικές συγκάλυψης αρχείων εκμεταλλεύονται χώρους που το λειτουργικό σύστημα είτε δεν γνωρίζει είτε θεωρεί μη δεσμευμένους.

Στο επίπεδο ***συστήματος αρχείων*** *(file system layer*) οι τεχνικές απόκρυψης χρησιμοποιούν τις δομές των συστημάτων αρχείων (*file systems*), εκμεταλλευόμενες τις αδυναμίες και τα χαρακτηριστικά της εκάστοτε έκδοσης. Σε αυτή την κατηγορία εμπίπτουν οι τεχνικές που χρησιμοποιούν οποιουδήποτε είδους αδρανείς περιοχές (*slack space)*, τα *alternate data streams (ADS* του *NTFS*), τα *reserved inodes των Unix file systems* όπως το *EXT2/3* και η χρήση ειδικών ονομάτων αρχείων *(file names*), τα οποία προσποιούνται αρχεία του συστήματος.

Στο επίπεδο ***εφαρμογών*** *(application layer*), ανήκουν πιο γνωστές τεχνικές, όπως αυτές της στεγανογραφίας, που εμφωλιάζουν μέσα σε ένα αναμενόμενο αρχείο ένα άλλο που παραμένει κρυμμένο.

Με τον όρο ***κατάλοιπα δεδομένων***, εννοούμε τα δεδομένα τα οποία δεν είναι ενεργά σε ένα πληροφοριακό σύστημα. Τα κατάλοιπα δεδομένων περιλαμβάνουν:

- Τα δεδομένα τα οποία βρίσκονται σε ελεύθερο χώρο πάνω στο αποθηκευτικό μέσο,
- Τα δεδομένα που βρίσκονται σε αδρανείς περιοχές *(slack spaces),*

- Τα δεδομένα που περιέχονταν μέσα σε αρχεία τα οποία έχουν διαγραφεί στο παρελθόν και δεν είναι εμφανή με χρήση των εφαρμογών που τα έχουν δημιουργήσει.

Οι κυριότερες περιοχές όπου μπορεί να βρεθούν κατάλοιπα δεδομένων, μεταξύ άλλων είναι:

- ***File slack*:** Είναι ο χώρος που δεν χρησιμοποιείται μεταξύ του λογικού τέλους του αρχείου σε σχέση με το φυσικό.
- ***Volume slack*:** Είναι ο μη χρησιμοποιούμενος χώρος μεταξύ του τέλους *ενός file system* και του τέλους του *partition* που το περιέχει. Το μέγεθος των δεδομένων που κρύβονται στο *volume slack* μπορεί να είναι πολύ μεγάλο.
- ***File system slack*:** Είναι ο χώρος στο τέλος ενός συστήματος αρχείων (*file system*) στον οποίο δεν έχει ανατεθεί κανένα *cluster*.
- ***Partition gap*:** Όταν κάποιος σκληρός δίσκος μορφοποιείται με παραπάνω από ένα *partitions*, τότε είναι πιθανό να υπάρχουν κενά μεταξύ των *partitions* τα οποία μπορούν να χρησιμοποιηθούν για να κρυφτούν δεδομένα.
- ***Swap file*:** Εδώ μπορεί να βρεθούν δεδομένα της *RAM* και επειδή τα συγκεκριμένα αποθηκεύονται στο δίσκο, είναι δυνατό να ανακτηθούν και να δώσουν δεδομένα όπως πληροφορίες για αρχεία κ.α.
- ***Unallocated space*:** Είναι ένα ακόμα μη χρησιμοποιούμενο μέρος του δίσκου, που δεν ελέγχεται από το λειτουργικό σύστημα.
- ***Host protected area*:** Μερικοί σκληροί δίσκοι δεσμεύουν μια ειδική περιοχή που λέγεται *προστατευμένη περιοχή υπολογιστή (host protected area*). Σε αυτό τον χώρο αποθηκεύονται διαγνωστικά εργαλεία και εργαλεία αρχικοποίησης (*booting*), προαποθηκευμένο λειτουργικό σύστημα για εγκατάσταση και επαναφορά σε περίπτωση βλάβης κ.α.

3.3.4.2 Ανάλυση Συστήματος Αρχείων

Είναι πολύ σημαντικό για ένα διερευνητή να γνωρίζει και να κατανοεί σε μεγάλο βαθμό τις βασικές αρχές των διαφόρων συστημάτων αρχείων *(FAT, NTFS, EXT2/3),* γιατί ένα μεγάλο μέρος της ανάκτησης και ανάλυσης των δεδομένων σε μια έρευνα είναι κάπου «κρυμμένο» στο σύστημα.

Τα αποτελέσματα της ανάλυσης ενός συστήματος αρχείων μπορούν δώσουν πολύτιμα στοιχεία σε μια έρευνα. Οι πληροφορίες που ενδεχομένως θα προκύψουν θα μπορούσε να είναι τα περιεχόμενα ενός καταλόγου αρχείων ή η ανάκτηση δεδομένων. Για παράδειγμα, όταν δημιουργείται ένα καινούργιο αρχείο, το λειτουργικό σύστημα ψάχνει για μη δεσμευμένο χώρο (*unallocated*) και τον αναθέτει στο αρχείο αυτό και θέτει το χώρο σε κατάσταση δεσμευμένη (*allocated*). Όταν το αρχείο διαγραφεί, ο χώρος αλλάζει κατάσταση σε μη δεσμευμένη ώστε να μπορεί, σε περίπτωση που χρειαστεί να φιλοξενήσει νέα δεδομένα, όμως μέχρι να φτάσει αυτή η στιγμή, τα διαγραμμένα δεδομένα του προηγούμενου αρχείου υπάρχουν ακόμη, κι επομένως μπορούν ανά πάσα στιγμή να ανακληθούν (*undelete*).

3.3.5 Πλαίσιο Οδηγιών για την Ασφαλή Ανάκτηση και Ανάλυση Ψηφιακών Δεδομένων

Στην προσπάθεια για την προτυποποίηση των διαδικασιών σε μια αναλυτική διερεύνηση υπολογιστών αναπτύχθηκαν σημαντικές πρωτοβουλίες. Θα παρουσιάσουμε

δύο σημαντικά πλαίσια οδηγιών που αντανακλούν την προσέγγιση της περιοχής της δικανικής ανάλυσης υπολογιστών (*computer forensics*) από τους φορείς που τα προτείνουν.

Το πρώτο πλαίσιο αναπτύχθηκε από το *National Institute of Standards and Technology (NIST)* με το *Guide to Integrating Forensic Techniques Into Incident Response*. Ο οδηγός αυτός παρουσιάζει τη διαδικασία διερεύνησης από την τεχνολογική πλευρά και όχι από τη νομική, παρέχοντας ένα πλαίσιο για τη συστηματική ανάκτηση και ανάλυση ψηφιακών δεδομένων. Παρέχει οδηγίες και συμβουλές για τη συλλογή, την ανάκτηση, την ανάλυση και την τεκμηρίωση δεδομένων που προέρχονται από διάφορες πηγές δεδομένων, συμπεριλαμβανομένων αρχείων, λειτουργικών συστημάτων, δικτυακής κίνησης και εφαρμογών.

Το δεύτερο πλαίσιο οδηγιών είναι το *Good Practice Guide for Computer-Based Electronic Evidence*, προέρχεται από τη Μεγάλη Βρετανία και συγκεκριμένα από τον οργανισμό *Association of Chief Police Officers (ACPO*). Ο οδηγός αυτός παρουσιάζει ιδιαίτερο ενδιαφέρον για τις συστηματικές οδηγίες που παρέχει για το χειρισμό περιστατικών οικιακών δικτύων και ασύρματων επικοινωνιών, τον έλεγχο του παιδοφιλικού περιεχομένου, την ανάκτηση αποδείξεων προερχόμενων από βίντεο και ηχογραφημένο υλικό και αποδείξεων προερχόμενων από κινητά τηλέφωνα.

3.3.6 Ανοιχτά Ερευνητικά Θέματα

Στην περιοχή της συστηματικής διερεύνησης των υπολογιστών υπάρχει ήδη σημαντική ερευνητική και επιστημονική δραστηριότητα. Για παράδειγμα, τα τελευταία χρόνια πραγματοποιούνται πλήθος από συνέδρια, γίνονται δημοσιεύσεις και γράφονται βιβλία στην ευρύτερη περιοχή της δικανικής ανάλυσης υπολογιστών.

Η δικανική ανάλυση υπολογιστών αποτελεί μια πολύ δυναμικά εξελισσόμενη ερευνητική περιοχή. Τις τρέχουσες ερευνητικές δραστηριότητες τροφοδοτεί μια σειρά νέων προκλήσεων, οι οποίες πραγματοποιούνται στα παρακάτω πεδία:

- ***Ποικιλομορφία των συσκευών:*** Οι συσκευές και τα δεδομένα που αποθηκεύονται αλλάζουν δυναμικά και χρήζουν ιδιαίτερης μελέτης, π.χ. *USB drive, iPod, cell phone/PDA*, ψηφιακή κάμερα, απομακρυσμένες συσκευές αποθήκευσης, συστήματα *voIP (voice over IP*).
- ***Αποθήκευση δεδομένων και απομακρυσμένη χρήση υπηρεσιών:*** Η έννοια της τοπικής αποθήκευσης δεδομένων και υπηρεσιών αλλάζει με την εξάπλωση της απομακρυσμένης φιλοξενίας δεδομένων σε ξένους πόρους (*google docs, yahoo photo album, Microsoft skydrive, photosynthesis* κ.α.), τη δημοσίευση πληροφοριών στο δίκτυο (κοινωνική δικτύωση), την ανταλλαγή αρχείων (*peer-to-peer*) και τέλος τη δυναμική εμφάνιση του *cloud computing*.
- ***Ακριβής αντιγραφή και επεξεργασία τεράστιου όγκου δεδομένων – ενεργές συστοιχίες δίσκων:*** Η ύπαρξη μιας «φάρμας» ενεργών δίσκων που αποθηκεύουν τεράστιο όγκο δεδομένων (π.χ. *amazon, ebay*) δημιουργεί ιδιαίτερα προβλήματα στην ακριβή αντιγραφή τους (*imaging*) και στην επεξεργασία των δεδομένων τους.
- ***Anti-forensics:*** Ιδιαίτερη πρόκληση στη διερεύνηση αποτελούν οι τεχνικές απόκρυψης πληροφοριών, όπως η κρυπτογραφία, η στεγανογραφία και οι άλλες τεχνικές απόκρυψης που εφαρμόζονται στα αρχεία εικόνων και ήχου, στις εφαρμογές (π.χ. *file slack*), στη γεωμετρία δίσκων (π.χ. κρυμμένα *partitions*),

στις επικοινωνίες (π.χ. πρωτόκολλα), στις μνήμες, στις δομές δεδομένων (*heap space*) και στα λειτουργικά συστήματα.

- ***Εμπιστοσύνη των αρχείων καταγραφής και ελέγχου****:* Είναι πιθανό ένας εισβολέας να μπορεί να τροποποιεί τα αρχεία καταγραφής συμβάντων συσκευών και εφαρμογών. Επίσης αναπτύσσονται όλο και πιο εξελιγμένα *rootkits* και σαν αποτέλεσμα χάνονται πολύτιμες αποδείξεις σε μια διαδικασία διερεύνησης.
- ***Δοκιμασία και αξιολόγηση των εργαλείων συστηματικής διερεύνησης:*** Είναι σημαντικό να προταθούν πλαίσια ανάπτυξης δικανικών εργαλείων (εμπορικά ή ανοιχτού κώδικα) καθώς και μέθοδοι αξιολόγησης της εγκυρότητας των αποτελεσμάτων τους. **[8]**

3.4 Υπολογιστές και Δίκτυα: Πώς αντιμετωπίζουν τις Απειλές

Η ευρεία χρήση των προσωπικών υπολογιστών από ιδιώτες και οργανισμούς που αναπτύχθηκε τα τελευταία χρόνια, είχε σαν αποτέλεσμα την ηλεκτρονική αποθήκευση ενός μεγάλου ποσοστού πληροφορίας. Ένας αυξανόμενος αριθμός εγκληματιών χρησιμοποιεί την ανίχνευση μέσω *pager*, τα κινητά τηλέφωνα, τους φορητούς υπολογιστές και τους εξυπηρετητές δικτύου ως μέσα για εγκλήματα και παραβατική συμπεριφορά. Οι υπολογιστές χρησιμοποιούνται στο ηλεκτρονικό έγκλημα με διαφορετικούς τρόπους. Σε ορισμένες περιπτώσεις, οι ίδιοι οι υπολογιστές παρέχουν τα μέσα για τη διάπραξη του εγκλήματος. Για παράδειγμα, το διαδίκτυο μπορεί να χρησιμοποιηθεί για να εγκατασταθούν επιθέσεις *hackers* σε ένα αδύναμο δίκτυο υπολογιστών, ή για τη μετάδοση ακατάλληλων εικόνων. Με άλλα λόγια οι υπολογιστές απλώς χρησιμοποιούνται σαν βολικές μηχανές αποθήκευσης των αποδείξεων του εγκλήματος. Αυτό το ηλεκτρονικό υλικό, σε ορισμένες περιπτώσεις, μπορεί να αποτελέσει κρίσιμο στοιχείο της εγκληματικής δραστηριότητας.

Οι διωκτικές και δικαστικές αρχές χρειάζεται να γνωρίζουν πώς να ανακτήσουν τις ηλεκτρονικές αποδείξεις που είναι αποθηκευμένες στους υπολογιστές. Οι ψηφιακές αποδείξεις είναι πιθανό να βρεθούν σε μαγνητικά μέσα αποθήκευσης όπως είναι οι σκληροί δίσκοι, οι δισκέττες (*floppy disks*), τα *flash*, η μνήμη τυχαίας προσπέλασης (*random access memory, RAM)* κ.λπ. Τα ηλεκτρονικά αρχεία όπως τα αρχεία καταγραφής των δικτύων υπολογιστών (*log*), τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα αρχεία επεξεργασίας κειμένου και τα αρχεία εικόνων, παρέχουν στις διωκτικές αρχές σημαντικές και συχνά ουσιώδεις αποδείξεις και στοιχεία εγκληματικής δραστηριότητας. Η χειρονακτική ανάλυση αυτών των δεδομένων είναι αδύνατη. Οι διαδικασίες σωστής συλλογής και αυτοματοποιημένης ανάλυσης είναι ουσιώδεις για τη διατήρηση των δεδομένων και την παρουσίασή τους σαν στοιχεία αποδείξεων στις δικαστικές αρχές. Η δικανική αντιμετώπιση του ηλεκτρονικού εγκλήματος (*computer forensic)* σχετίζεται με τη συντήρηση, αναγνώριση, εξαγωγή, καταγραφή και ερμηνεία των μέσων πληροφορικής για τη συλλογή αποδείξεων και την εύρεση των αιτίων *(root cause analysis)*.

Η ανάγκη για καλά ορισμένες διαδικασίες για την απόκτηση και ανάλυση αποδείξεων χωρίς την πρόκληση της καταστροφής τους και η παροχή αποδεικτικών στοιχείων που να μπορούν να γίνουν δεκτά από τις δικαστικές αρχές, συζητήθηκε στο *First Digital Forensics Workshop*. Εκεί προτάθηκε ένα γενικό πλαίσιο δικανικής επιστήμης για την αντιμετώπιση ψηφιακών εγκλημάτων. Το πλαίσιο αυτό καθόρισε μια γραμμική διαδικασία έρευνας, η οποία εμπεριέχει τα ακόλουθα στάδια: αναγνώριση, συντήρηση, συλλογή, εξέταση, ανάλυση, παρουσίαση και απόφαση. Βασισμένες σε αυτό το πλαίσιο έρευνας, αναπτύχθηκαν δομημένες προσεγγίσεις όπως για παράδειγμα η *Ψηφιακή Ανάλυση από Άκρο σε Άκρο* (*End-to-End Digital Investigation, EEDI*) οι οποίες διευκολύνουν περίπλοκες έρευνες.

Η δικανική αντιμετώπιση του δικτυακού εγκλήματος *(network forensic)* σχετίζεται με τον προσδιορισμό του τρόπου με τον οποίο πραγματοποιήθηκε η μη εξουσιοδοτημένη πρόσβαση σε έναν απομακρυσμένο υπολογιστή. Επίσης παρέχει πληροφορίες σχετικές με την εισβολή σε υπολογιστικά συστήματα. Τα αρχεία καταγραφής *(log files)* που τηρούνται στον υπολογιστή που έπεσε θύμα εισβολής, όπως επίσης οι δρομολογητές (*routers*) και οι πάροχοι διαδικτυακών υπηρεσιών *(Internet Service Providers-ISP)* χρησιμοποιούνται για να εντοπίσουν τα ίχνη του εισβολέα.

Πολλά εξειδικευμένα εργαλεία έχουν αναπτυχθεί, για να διευκολύνουν τη δικανική αντιμετώπιση ηλεκτρονικών και δικτυακών παραβάσεων. Οι *Mohay, Anderson, Collie,*

McKemmish, et al. (2003) προσδιορίζουν τρείς βασικές κατηγορίες δικανικής λειτουργίας: ***απεικόνιση, ανάλυση και οπτικοποίηση***. ***Η απεικόνιση*** αποτελεί το πρώτο βήμα, όπου δημιουργείται ένα αντίγραφο των αποδείξεων για περαιτέρω ανάλυση έτσι ώστε να αποφευχθεί ο κίνδυνος αλλοίωσης των πρωτότυπων. Μερικά εργαλεία που χρησιμοποιούνται ευρέως για σκοπούς απεικόνισης είναι τα *Norton Ghost, Safeback, Encase, Linux dd*. Μια πλήρης δικανική ανάλυση της εικόνας είναι απαραίτητη ώστε να βρεθεί πληροφορία σχετική με κάθε συγκεκριμένη περίπτωση. Η ψηφιακή πληροφορία δεν είναι πάντοτε διαθέσιμη και έτοιμη να διαβαστεί. Κάποια αρχεία μπορεί να έχουν σβηστεί, αλλοιωθεί ή να είναι κρυμμένα. ***Η δικανική ανάλυση*** επιτρέπει την ανάκτηση των αρχείων που μπορεί να είναι διαγραμμένα, κρυμμένα, προστατευμένα από κωδικούς ή κρυπτογραφημένα. Κάποια πολύ γνωστά εργαλεία είναι τα *Sleuthkit* και *WinInterrogate*. ***Η οπτικοποίηση*** περιλαμβάνει την χρονική απεικόνιση της δραστηριότητας του υπολογιστή χρησιμοποιώντας την πληροφορία που βρέθηκε στα αρχεία καταγραφής (*log files).*

Η δικανική αντιμετώπιση του δικτυακού εγκλήματος *(network forensic*) μπορεί να επιτευχθεί χρησιμοποιώντας εργαλεία όπως τα *Snort, TcpDump,* και *BlackIce*. Τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν τα αρχεία καταγραφής του συστήματος *(system log)* και τα *audit trails* που βρίσκονται στον υπολογιστή όπως και την πληροφορία που βρίσκεται στους δρομολογητές και στους μεταγωγείς (*switches*). Πολλές προσεγγίσεις έχουν προταθεί για την ανίχνευση εισβολών και την αναζήτηση της πηγής της εισβολής.

Οι περισσότεροι πάροχοι δικανικών ψηφιακών εργαλείων προσφέρουν ποικίλα εργαλεία και κάποιοι προσφέρουν πλήρη απεικονιστική λειτουργικότητα. Για παράδειγμα, το *Computer Forensic Investigative Toolkit (CFIT)* που αναπτύχθηκε από *τον Defence Science and Technology Organization (DSTO)* του υπουργείου άμυνας της Αυστραλίας παρέχει εργαλεία για την ανάλυση διαφόρων ειδών ροών δεδομένων: δικτυακά δεδομένα, δεδομένα τηλεπικοινωνιακών κλήσεων ή δεδομένα δίσκων υπολογιστών. Άλλα εργαλεία τα οποία χρησιμοποιούνται ευρέως είναι το *The Coroner's Toolkit (TCT)* και το *ForensiX*.

Τα εργαλεία λογισμικού θα πρέπει να ικανοποιούν τα κριτήρια του *Daubert*: τα εργαλεία λογισμικού θα πρέπει να έχουν ελεγχθεί ως προς την ακρίβεια, την αξιοπιστία και την επαναληψιμότητα και να έχουν μια γενικά αποδεκτή μεθοδολογία. Η αξιοπιστία των εργαλείων δικανικής αντιμετώπισης των ηλεκτρονικών εγκλημάτων είναι σημαντική για τις διωκτικές αρχές. Αρχές, όπως το *National Institute of Standards and Technology (NIST)* και το *National Institute of Justice (NIJ)* έχουν αναπτύξει προγράμματα για τον έλεγχο και την επικύρωση του δικανικού λογισμικού.

3.4.1 Δικανικές Αναλύσεις Υπολογιστών

Σύμφωνα με μία μελέτη του Πανεπιστημίου του *Berkeley* της Καλιφόρνια που έγινε το 2001, το 93% της πληροφορίας που δημιουργήθηκε εκείνη την εποχή ήταν σε ψηφιακή μορφή. Οι υπολογιστές εμπλέκονται στα σημερινά εγκλήματα με πολλαπλούς τρόπους, όπως αναφέρεται στο *President's Working Group*. Οι υπολογιστές μπορούν να αποτελούν το στόχο του εγκλήματος, όπου η καταστροφή επιτελείται στην ακεραιότητα, στην ιδιωτικότητα και στη διαθεσιμότητα της πληροφορίας που είναι αποθηκευμένη. Η μη εξουσιοδοτημένη πρόσβαση επιτυγχάνεται σε ένα σύστημα που αποτελεί στόχο με σκοπό την απόκτηση πληροφορίας που είναι αποθηκευμένη σε αυτό ή την διαταραχή των λειτουργιών του. Επίσης οι υπολογιστές μπορούν να χρησιμοποιηθούν ως συσκευές αποθήκευσης, όπου μπορούν να αποθηκευτούν κλεμμένοι αριθμοί πιστωτικών καρτών, αριθμοί ασφάλισης, ιατρικά αρχεία, πληροφορίες ιδιοκτησίας κ.α.

Τέλος οι υπολογιστές μπορούν να χρησιμοποιηθούν ως εργαλεία επικοινωνίας όπου μηνύματα ηλεκτρονικού ταχυδρομείου και σύνοδοι συζήτησης (*chat sessions*) είναι δυνατό να ενεργοποιήσουν το σχεδιασμό και το συντονισμό πολλών εγκλημάτων. Επίσης κάποιες φορές οι υπολογιστές μπορούν να χρησιμοποιηθούν για να αποστείλουν απειλές ή εκβιαστικά μηνύματα.

Σε περίπτωση που υπάρχει υποψία περιστατικού ασφάλειας ή ηλεκτρονικού εγκλήματος, ο ερευνητής χρησιμοποιεί τα εργαλεία δικανικής αντιμετώπισης για να ερευνήσει για αποδείξεις σε έναν ιδιαίτερα μεγάλο όγκο δεδομένων. Η δικανική αντιμετώπιση του ηλεκτρονικού εγκλήματος είναι μια μεθοδολογία μέσω της οποίας αποκτώνται και αναλύονται οι αποδείξεις σε ψηφιακή μορφή. Θα πρέπει να σημειωθεί ότι είναι τέτοια η φύση των ψηφιακών αποδείξεων ώστε χρειάζονται ειδικές διαδικασίες για την απόκτηση και το χειρισμό τους. Οι ηλεκτρονικές αποδείξεις είναι πολύ εύκολο να μεταβληθούν εκτός και αν ακολουθηθούν αυστηρές διαδικασίες. Για παράδειγμα, η αρχικοποίηση ενός συστήματος μπορεί να προκαλέσει την απώλεια πληροφορίας μνήμης του υπολογιστή και να καταστρέψει πολύτιμα ίχνη εγκλήματος.

Στη συνέχεια, θα περιγραφούν τα βασικά βήματα που χρειάζονται κατά την εκτέλεση της δικανικής ανάλυσης και επίσης θα περιγραφούν κάποια εργαλεία που χρησιμοποιούνται συχνά στην έρευνα του ηλεκτρονικού εγκλήματος.

3.4.1.1 Πού χρησιμοποιούνται οι Δικανικές Αναλύσεις

Οι τεχνικές δικανικής αντιμετώπισης του ηλεκτρονικού εγκλήματος είναι ουσιώδεις για την επιτυχή αποφυγή, ανίχνευση, έρευνα και δίωξη του ηλεκτρονικού εγκλήματος. Καθώς η εγκληματική χρήση των υπολογιστών ολοένα αυξάνεται, η επιβολή του νόμου βασίζεται σε μεγάλο βαθμό στις δικανικές αναλύσεις των υπολογιστών για να τεκμηριώσει τις διώξεις. Η ανάλυση των αιτίων (*root cause analysis)* είναι απαραίτητη ώστε να αποφευχθεί η επανεμφάνιση του προβλήματος και οι δικανικές αναλύσεις βοηθούν στην κατανόηση της πλήρους έκτασης του προβλήματος. Τα εργαλεία της δικανικής ανάλυσης υπολογιστών αποτελούν ένα βασικό συστατικό ώστε να εξασφαλιστεί μια επιτυχής διαιτησία.

Οι οργανισμοί ολοένα και περισσότερο ενσωματώνουν μεθόδους με τις οποίες αποθηκεύεται πληροφορία, ώστε να ενεργοποιούνται επιτυχώς οι δικανικές αναλύσεις. Είναι πολύ σημαντικό να προστατεύεται η πνευματική ιδιοκτησία των εταιρειών από τις πιθανές ηλεκτρονικές κλοπές ιδιόκτητων στοιχείων. Η απώλεια εταιρικών μυστικών, εμπιστευτικών δεδομένων πελατών, οικονομικών πληροφοριών και της ιδιωτικής πληροφορίας αποτελεί ένα κύμα εγκλήματος της τάξης δισεκατομμυρίων δολαρίων. Ενώ οι εταιρείες εστιάζουν στην αποφυγή της κλοπής πληροφοριών και εταιρικών μυστικών από εξωτερικούς εισβολείς (*hackers*), οι υπάλληλοι αυτών των εταιρειών και συχνά οι πρώην υπάλληλοί τους έχουν την πιο απρόσκοπτη πρόσβαση σε πολύτιμα εταιρικά δεδομένα. Οι κατάλληλες διαδικασίες δικανικής ανάλυσης υπολογιστών μπορούν να βοηθήσουν τις εταιρείες στην ιχνηλάτιση των ηλεκτρονικών εγκλημάτων.

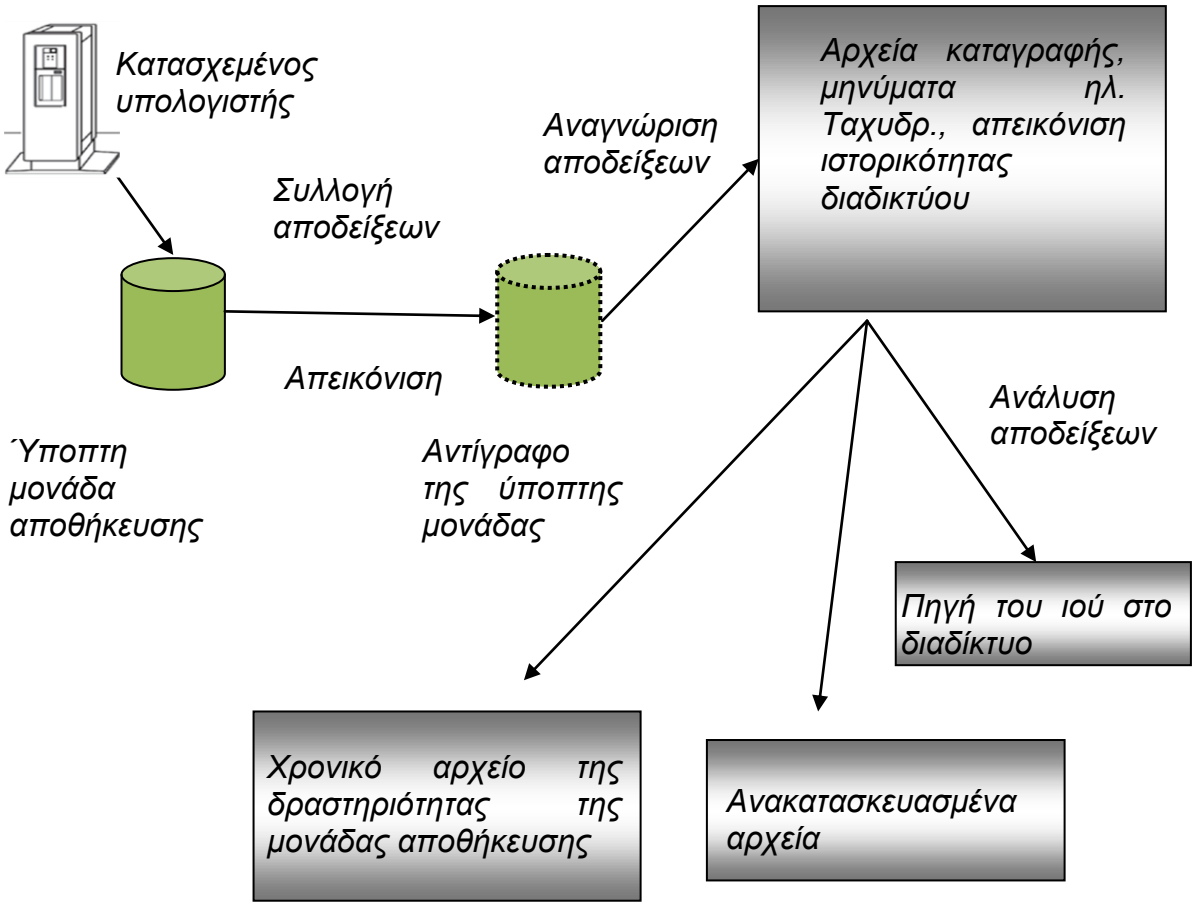
3.4.1.2 Τα Βήματα της Δικανικής Ανάλυσης Υπολογιστών

Υπάρχουν πολλά βήματα που εμπλέκονται στην ανάκτηση και ανάλυση των ψηφιακών αποδείξεων, σε μια έρευνα μέσα σε υπολογιστικά συστήματα. Γενικά, στη διαδικασία έρευνας έχουν προσδιοριστεί τρία βασικά βήματα, που ονομάζονται τα τρία ***Α. Απόκτηση, Αυθεντικοποίηση και Ανάλυση***. Αυτά τα τρία βήματα, όπως και το τέταρτο βήμα της ***Παρουσίασης*** θα παρουσιαστούν παρακάτω. Όταν ένας ύποπτος δίσκος κατάσχεται από έναν υπολογιστή, δημιουργείται αμέσως ένα αντίγραφο του δίσκου. Στη συνέχεια, το αντίγραφο αναλύεται έτσι ώστε να προσδιοριστούν πολύτιμες

αποδείξεις όπως είναι τα αρχεία καταγραφής (*log files),* τα διαγραμμένα αρχεία κ.λπ. Η ανάλυση των αναγνωρισμένων αποδείξεων έχει ως αποτέλεσμα την απόδοση των ανακατασκευασμένων αρχείων ή άλλη χρήσιμη πληροφορία.

3.4.1.2.1 Η Απόκτηση των Αποδείξεων

Η διαδικασία απόκτησης ηλεκτρονικών αποδείξεων μπορεί να διαφέρει από περίπτωση σε περίπτωση. Μια πρόκληση στην εύρεση αποδείξεων βρίσκεται στο πού θα τις αναζητήσουμε. Για παράδειγμα, κάποιες έρευνες μπορεί να απαιτούν την εξέταση των δεδομένων που είναι αποθηκευμένα στον σκληρό δίσκο του υπολογιστή ενώ σε ορισμένες περιπτώσεις εισβολής στα δίκτυα, οι αποδείξεις μπορεί να βρίσκονται μόνο στην μνήμη τυχαίας προσπέλασης (*Random Access Memory, RAM*). Επομένως, δεν υπάρχει μια μοναδική διαδικασία για τη συλλογή αποδείξεων, και η χρήση της κατάλληλης μεθοδολογίας για την εξασφάλιση των ψηφιακών αποδείξεων εξαρτάται από τον τύπο των αποδείξεων που αναζητούνται και από την διαθέσιμη τεχνολογία τη δεδομένη στιγμή. Ο ερευνητής θα πρέπει να γνωρίζει ποιό εργαλείο να χρησιμοποιήσει έτσι ώστε να ανακαλύψει τις αποδείξεις. Επίσης είναι σημαντικό να ανακαλύψουμε και να κατοχυρώσουμε τις αποδείξεις, χωρίς αυτές να χάσουν την ακεραιότητα και την αξία τους ώστε να είναι αποδεκτές από τις δικαστικές αρχές. Υπάρχουν αρκετά βήματα που εμπλέκονται στην απόκτηση των αποδείξεων και τα κυριότερα αναφέρονται πιο κάτω:



Σχήμα 17: Μια τυπική δικανική ανάλυση υπολογιστή

- ***Αλυσίδα Επιτήρησης (Chain of Custody):*** Για να προστατευθεί η ακεραιότητα των αποδείξεων και να υποστηριχθεί ότι αυτές δεν αλλοιώθηκαν για όσο διάστημα βρίσκονταν σε επιτήρηση, είναι κριτικής σημασίας η διατήρηση μιας αλυσίδας επιτήρησης των αποδείξεων που συγκεντρώθηκαν. Η αλυσίδα επιτήρησης είναι μια διαδικασία που διατηρεί και καταγράφει την χρονολογική ιστορία της έρευνας. Το έγγραφο παρακολούθησης της αλυσίδας επιτήρησης για μια απόδειξη, καταγράφει πληροφορίες όπως για παράδειγμα ποιός χειρίστηκε την απόδειξη, ποιές διεργασίες ακολουθήθηκαν για τη συλλογή της απόδειξης, πότε συλλέχθηκε και αναλύθηκε η απόδειξη, πού βρέθηκε και πού αποθηκεύθηκε, γιατί αυτό το υλικό θεωρήθηκε ότι αποτελεί απόδειξη και τέλος με ποιό τρόπο έγινε η συλλογή και η διατήρηση της απόδειξης.
- ***Αναγνώριση:*** Για να αναγνωρίσει πιθανές αποδείξεις, ο ερευνητής θα πρέπει να έχει εκτενή γνώση της αρχιτεκτονικής και του λογισμικού του υπολογιστή (*hardware, software*), τα οποία περιλαμβάνουν το λειτουργικό σύστημα, το σύστημα αρχείων και τους αλγόριθμους κρυπτογράφησης. Οι αποδείξεις θα πρέπει να αναγνωριστούν μέσα σε κανονικά αρχεία και μπορεί να βρεθούν σε χαλαρό χώρο, σε μη κατανεμημένο χώρο, σε κρυμμένα ή κρυπτογραφημένα αρχεία, σε αρχεία προστατευμένα με κωδικό, σε αρχεία καταγραφής κ.λπ. Οι αποδείξεις μπορεί να βρεθούν σε οποιαδήποτε πηγή δεδομένων όπως είναι ο σκληρός δίσκος, οι δισκέττες, τα *flash*, τα κινητά τηλέφωνα, το *CD-ROM* κ.α.
- ***Συλλογή/Διατήρηση****:* Οι αναγνωρισμένες αποδείξεις θα πρέπει να συλλεχθούν από τα διαθέσιμα συστατικά. Η συλλογή τους δεν θα πρέπει να καθυστερήσει, γιατί σε αυτή την περίπτωση μπορεί να χαθεί πολύτιμη πληροφορία λόγω της παρατεταμένης χρήσης του υπολογιστή. Σε κάποιες περιπτώσεις, οι αποδείξεις θα πρέπει να αντιγραφούν για ανάλυση. Η αντιγραφή αυτή πραγματοποιείται ανά *bit* με τη χρήση ειδικών δικανικών εργαλείων λογισμικού. Αυτή η διεργασία που δημιουργεί ένα ακριβές αντίγραφο του πρωτότυπου της απόδειξης ονομάζεται απεικόνιση. Η αστάθεια των δεδομένων δημιουργεί έναν αριθμό από εμπόδια στη διεργασία της απεικόνισης. Οι αποδείξεις είναι πολύ εύκολο να τροποποιηθούν καθώς δημιουργείται το αντίγραφο των αποδείξεων. Η χρήση της απεικόνισης δεν θα πρέπει να εισάγει νέα δεδομένα στην πρωτότυπη απόδειξη ή στο αντίγραφό της. Ο ερευνητής θα πρέπει να είναι σε θέση να αποδείξει στις δικαστικές αρχές ότι το αντίγραφο είναι έγκυρο και να δείξει ότι η διαδικασία της απεικόνισης είναι επαναλαμβανόμενη.
- ***Μεταφορά και Αποθήκευση:*** Όλα τα δεδομένα που έχουν ανακτηθεί από ένα εκτεθειμένο σύστημα θα πρέπει να ασφαλιστούν. Αποδεικτικά στοιχεία όπως είναι οι σκληροί δίσκοι μπορεί να καταστραφούν αν κάποιος δεν τα χειριστεί σωστά. Αυτού του είδους τα μαγνητικά μέσα αποθήκευσης πρέπει να προστατεύονται από μηχανικές και ηλεκτρομαγνητικές καταστροφές. Το υλικό θα πρέπει να σφραγίζεται ώστε να αποδεικνύεται ότι δεν αλλοιώθηκε κατά τη μεταφορά του. Ένα έγγραφο αλυσίδας επιτήρησης θα πρέπει να σχετίζεται με κάθε αποδεικτικό στοιχείο.

Η πρόκληση στην απόκτηση των ψηφιακών αποδείξεων βρίσκεται στο γεγονός ότι είναι οικονομικά ασύμφορη η παύση όλων των διαθέσιμων πόρων ενός συστήματος για περαιτέρω έρευνα στη σημερινή ψηφιακή εποχή, όπου η πληροφορία δημιουργείται, αποθηκεύεται και μεταφέρεται σε ηλεκτρονική μορφή.

3.4.1.2.2 Η Αυθεντικοποίηση των Αποδείξεων

Έχει ζωτική σημασία οι αποδείξεις που συλλέγονται να είναι ένα ακριβές αντίγραφο των πρωτότυπων, κατά τη χρονική στιγμή που συντελείται το έγκλημα. Ο ερευνητής θα πρέπει να είναι ικανός να αποδείξει με πειστικό τρόπο ότι οι αποδείξεις προήλθαν από τον υπολογιστή στόχο. Μόλις συλλεχθούν οι αποδείξεις θα πρέπει να διασφαλιστεί ότι αυτές δεν θα καταστραφούν, μεταβληθούν ή αλλοιωθούν.

Η αυθεντικοποίηση των αποδείξεων χρησιμοποιώντας απλές τεχνικές χρονοσήμανσης (*time stamping)* είναι ένας αποτελεσματικός τρόπος για να συγκρίνουμε το αντίγραφο με το πρωτότυπο. Μία συνάρτηση κατακερματισμού (*hash function) H* είναι η μετατροπή που παίρνει μια είσοδο *m* και επιστρέφει μια σειρά χαρακτήρων σταθερού μήκους, που ονομάζεται τιμή κατακερματισμού (*hash value) h* (δηλαδή *h=H[m]).* Μπορούμε να θεωρήσουμε την τιμή κατακερματισμού σαν ένα ***ψηφιακό αποτύπωμα***. Δύο πολύ δημοφιλείς αλγόριθμοι κατακερματισμού είναι οι *MD5* και *SHA*. Όταν οι ψηφιακές αποδείξεις συλλεχθούν και αντιγραφούν, οι τιμές κατακερματισμού των πρωτότυπων και των αντιγράφων υπολογίζονται και καταγράφονται. Τελικά οι δύο αυτές τιμές κατακερματισμού θα πρέπει να είναι πανομοιότυπες.

3.4.1.2.3 Η Ανάλυση των Αποδείξεων

Είναι πιθανό να απαιτούνται πολλαπλά εργαλεία για να αναλυθούν πλήρως οι κατασχεμένες αποδείξεις. Θα πρέπει να χρησιμοποιούνται ελεγμένα και επικυρωμένα εργαλεία, ενώ στην περίπτωση που χρησιμοποιούνται άλλα εργαλεία ο ερευνητής θα πρέπει να επιβεβαιώσει ότι οι αποδείξεις δεν είναι κατεστραμμένες. Στην ανάλυση εμπεριέχονται δραστηριότητες που περιλαμβάνουν την ανάγνωση του *partition table*, την αναζήτηση σε υπάρχοντα αρχεία για σχετικές πληροφορίες όπως είναι λέξεις κλειδιά, αλλαγές καταστάσεων του συστήματος ή γραμματοσειρές, την ανάκτηση πληροφοριών από διαγραμμένα αρχεία, τον έλεγχο για δεδομένα που είναι κρυμμένα σε *boot record*, σε μη διανεμημένο χώρο μνήμης ή σε κομμάτια του δίσκου που είναι κατεστραμμένα, το σπάσιμο των κωδικών κ.α. Η διαδικασία της ανάλυσης ενός συστήματος που είναι σε λειτουργία, έχοντας υπόψη ότι τα χαρακτηριστικά αυτού του συστήματος μπορεί να έχουν μεταβληθεί από τον εισβολέα, είναι μια δραστηριότητα που εισάγει πολλές προκλήσεις. Σε κάποιες περιπτώσεις, η πολύπλοκη δραστηριότητα του υπολογιστή και των δικτύων μπορεί να μεταβάλλει τα αποδεικτικά στοιχεία σε δυναμικά δεδομένα που δεν είναι εύκολο να αναπαραχθούν.

Ακόμα και διαγραμμένα αρχεία μπορούν να ανακτηθούν από ένα δίσκο, από έναν εκπαιδευόμενο ερευνητή δικανικών αναλύσεων και μόνο η πλήρης αντικατάσταση (*overwrite*) ενός αρχείου είναι δυνατόν να το κάνει μη προσπελάσιμο από τα μέσα. Για να ανακτηθούν τα δεδομένα που έχουν αντικατασταθεί (*overwrite*) μπορούν να χρησιμοποιηθούν εξελιγμένες τεχνικές όπως τα *Scanning Tunneling Microscopy (STM), Magnetic Force Microscopy*. Αυτές οι τεχνικές εκμεταλλεύονται το γεγονός ότι είναι πρακτικώς αδύνατο να γράφονται τα δεδομένα στην ίδια περιοχή κάθε φορά εξαιτίας των φυσικών περιορισμών των μηχανισμών καταγραφής. Αυτές οι συσκευές επιβαρύνουν με τεράστιο κόστος σε χρόνο και χώρο αποθήκευσης και επομένως δεν χρησιμοποιούνται ευρέως. Άλλες τεχνικές που βασίζονται στα αρχεία καταγραφής *(log based techniques)* όπως η *Byteprints* έχουν προταθεί για την ανάκτηση σταθερών απεικονίσεων των αρχείων ακόμα κι αν αυτά έχουν αντικατασταθεί (*overwrite*). Αυτές οι τεχνικές δεν χρειάζονται εξελιγμένο και ιδιαίτερα ακριβό υλικό.

Η ερμηνεία των αποτελεσμάτων μιας ανάλυσης εξαρτάται σε μεγάλο βαθμό από την ικανότητα του ερευνητή. Σε αυτό το στάδιο, ο ερευνητής μπορεί να στοιχειοθετήσει το

νόημα και τη συνάφεια των επεξεργασμένων δεδομένων και να λύσει θέματα όπως η ταυτότητα του χρήστη του υπολογιστή, ο σκοπός των δεδομένων κ.α.

3.4.1.2.4 Η Δημιουργία Αναφοράς

Ένα κρίσιμο στάδιο της ανάλυσης αποτελεί η παρουσίαση ή η δημιουργία μιας αναφοράς των αποτελεσμάτων της ανάλυσης. Κάθε βήμα στην δικανική ανάλυση θα πρέπει να καταγράφεται λεπτομερώς. Ο ερευνητής θα πρέπει να είναι σε θέση να εξηγεί τα περίπλοκα τεχνολογικά θέματα με απλούς όρους. Επίσης, το νόημα και η σημαντικότητα των αποτελεσμάτων που έχουν αποκτηθεί θα πρέπει να μεταφερθούν με σαφήνεια.

3.4.1.3 Εργαλεία Δικανικής Ανάλυσης Υπολογιστών

Τα εργαλεία δικανικής ανάλυσης έχουν αναπτυχθεί για να καλύψουν τα διάφορα στάδια της δικανικής ανάλυσης που περιγράφηκαν προηγουμένως. Δεν υπάρχει μία μοναδική λύση που να καλύπτει τις ποικίλες απαιτήσεις μιας δικανικής ανάλυσης υπολογιστών. Τα δικανικά εργαλεία ανάλυσης έχουν αναπτυχθεί για να καλύπτουν διαφορετικές λειτουργικές πλατφόρμες. Κάποια από αυτά είναι ελεύθερης χρήσης και άλλα είναι περιορισμένης και πρέπει να αγοραστούν. Επίσης, υπάρχουν διαφορετικά εργαλεία για την απόκτηση των αποδείξεων και για την ανάλυσή τους από συστήματα που είναι σε λειτουργία *(live system).* Κάποια από τα πιο γνωστά εργαλεία δικανικής ανάλυσης που βασίζονται στις πιο πάνω κατηγορίες είναι:

- **Εργαλεία απεικόνισης:** *dd, EnCase, Safeback, Norton Ghost, iLook, Mares, SMART, ByteBack, SnapBack, Drive Image, X-Ways Forensics*
- **Εργαλεία Ανάλυσης:** *Sleuthkit, WinInterrogate, ForensiX, SMART, DriveSpy, iLook, DiskSig Pro, Quick View, Thumbs Plus, CompuPic, Hex Editor, dtSearch, NTA Stealth, PDA Seizure*
- **Συστήματα Δικανικής Ανάλυσης (Toolkits):** *Corener's Toolkit (TCT), Forensic Toolkit (FTK).*

Τα διαθέσιμα εργαλεία δικανικής ανάλυσης αξιολογούνται λαμβάνοντας υπόψη διάφορα κριτήρια όπως είναι η πληρότητα της λειτουργικότητας του εργαλείου, ο χρόνος που χρειάζεται το εργαλείο για να εκτελέσει τη λειτουργία του, η ευκολία στη χρήση του εργαλείου, το κόστος του, η παραδοχή του από τις δικαστικές αρχές κ.α. Ενδεικτικά περιγράφουμε κάποια από τα εργαλεία δικανικής ανάλυσης.

3.4.1.3.1 Εργαλεία Απεικόνισης

Η διαδικασία της απεικόνισης ενός σκληρού δίσκου εμπλέκει την αντιγραφή ανά *bit* του δίσκου σε ένα αρχείο εικόνας που ονομάζεται δίσκος ανάλυσης. Η απεικόνιση του σκληρού δίσκου ενός υπολογιστή ύποπτου για εισβολή, είναι μία από τις πιο σημαντικές λειτουργίες στη διαδικασία της δικανικής ανάλυσης. Είναι ιδιαίτερα σημαντικό να μην γραφτούν άλλα δεδομένα στον ύποπτο σκληρό δίσκο κατά τη διαδικασία αυτή. Για το σκοπό αυτό, χρησιμοποιείται τεχνολογία εμπλοκής εγγραφής *(write blocker technology*). Οι τεχνολογίες αυτές εξασφαλίζουν ότι εμποδίζεται οποιαδήποτε προσπάθεια εγγραφής στο δίσκο όπου γίνεται προσπάθεια απεικόνισης. Είναι επίσης επιτακτικής σημασίας κάθε *bit* που αντιγράφεται στο δίσκο ανάλυσης να είναι ακριβώς το ίδιο με κάθε αντίστοιχο *bit* του ύποπτου δίσκου. Η ακεραιότητα του αντιγράφου μπορεί να πιστοποιηθεί με την αναπαραγωγή αποτυπωμάτων των περιεχομένων του ύποπτου δίσκου και των περιεχομένων του δίσκου ανάλυσης με τη χρήση λειτουργιών

κατακερματισμού (*hash functions*) όπως είναι η *MD5* και με τη σύγκριση αυτών των αποτυπωμάτων.

Για να διευκολυνθεί η διαδικασία της δικανικής ανάλυσης έχουν αναπτυχθεί πολλά εργαλεία απεικόνισης. Οι ερευνητές έχουν επίσης στη διάθεσή τους, εκτός από εργαλεία λογισμικού και εργαλεία *hardware* για να αποκτούν αντίγραφα των εικόνων του συστήματος.

- ***dd:*** Η λειτουργικότητα *dd* δημιουργεί ανά *bit* ένα αντίγραφο αρχείου, μέρους ενός αρχείου, φυσικής μνήμης, ενός λογικού δίσκου ή ολόκληρου του φυσικού δίσκου. Μπορεί να χρησιμοποιηθεί και να εγκατασταθεί σε υπολογιστές ελεύθερα και είναι διαθέσιμο για συστήματα βασισμένα σε *Unix* και σε *Windows*. Περιέχει ένα ενσωματωμένο υπολογιστή υπόλοιπου (*checksum*) χρησιμοποιώντας *MD5* και έναν ελεγκτή ακεραιότητας που μπορεί να συγκρίνει τα υπόλοιπα των δεδομένων και τα υπόλοιπα των απεικονίσεων και να υποδείξει αν είναι διαφορετικά.
- ***SafeBack:*** Πρόκειται για ένα βιομηχανικό αυτό-αυθεντικοποιημένο εργαλείο δικανικής ανάλυσης που χρησιμοποιείται από διωκτικές αρχές σε όλο τον κόσμο. Είναι μια λειτουργία βασισμένη σε *DOS* και χρησιμοποιείται για να δημιουργήσει αποτυπώματα των αποδείξεων από τους σκληρούς δίσκους σε υπολογιστικά συστήματα βασισμένα σε *Intel*. Το εργαλείο αυτό αντιγράφει όλες τις περιοχές του σκληρού δίσκου με μεγάλη ακρίβεια. Απομακρυσμένη λειτουργία μέσω μιας σύνδεσης παράλληλης θύρας επιτρέπει να διαβαστεί ή να γραφτεί ο σκληρός δίσκος σε έναν απομακρυσμένο υπολογιστή. Στην έκδοση *SafeBack 3.0*, χρησιμοποιούνται δύο ξεχωριστές μαθηματικές διαδικασίες κατακερματισμού που κάνουν χρήση του αλγόριθμου *SHA256* για να υποστηρίξουν την ακεραιότητα των *SafeBack* αρχείων.
- ***Norton Ghost*:** Το εργαλείο αυτό αποτελεί μια λειτουργικότητα αντιγραφής και αποκατάστασης και χρησιμοποιείται σε συστήματα *Windows, NT, Linux* και *DOS.* Επιτρέπει την δημιουργία αντιγράφων σε εικόνες χωρίς να χρειάζεται η επανεκκίνηση του υπολογιστή. Εξοικονομεί χώρο μνήμης και χρόνο δημιουργώντας τεράστια αντίγραφα και μπορεί να προγραμματίσει την αυτόματη δημιουργία αντιγράφων για ενημερωμένες εικόνες.

3.4.1.3.2 Εργαλεία Ανάλυσης

Οι δραστηριότητες δικανικής ανάλυσης διαφέρουν ανάλογα με τον τύπο του μέσου που αναλύεται, το σύστημα αρχείων που χρησιμοποιείται κ.λπ. Κάποια δημοφιλή εργαλεία ανάλυσης είναι:

- ***DriveSpy*:** Πρόκειται για ένα εργαλείο ανάλυσης σε *DOS*. Είναι σχεδιασμένο ώστε να επεκτείνει τις δυνατότητες του *DOS* για να ικανοποιούνται οι ανάγκες δικανικής ανάλυσης. Μπορεί να εξετάσει αρχεία που είτε είναι είτε δεν είναι *DOS*. Στο εργαλείο αυτό περιλαμβάνονται δυνατότητες καταγραφής ώστε να αποτυπώνονται όλες οι δραστηριότητες της έρευνας. Το *DriveSpy* μπορεί να σώσει και να αποκαταστήσει συμπιεσμένες εικόνες δικανικής ανάλυσης ενός σκληρού δίσκου και επίσης να αποκτήσει ένα μέρος από επιλεγμένα αρχεία. Χρησιμοποιώντας το *DriveSpy* μπορεί να αποκτηθούν εκτεταμένη αρχιτεκτονική πληροφορία των σκληρών δίσκων και συγκεκριμένα μέρη τους.
- ***dtSearch:*** Πρόκειται για ένα γρήγορο και ακριβές εργαλείο ανάκτησης κειμένου το οποίο είναι πολύ χρήσιμο στην έρευνα της δικανικής ανάλυσης.

Μπορεί να ερευνήσει άμεσα *gigabytes* κειμένου σε έναν υπολογιστή, στο δίκτυο, στο διαδίκτυο ή στο *intranet*. Επιτρέπει την αναζήτηση στοιχείων με δείκτη (*indexed*), χωρίς δείκτη (*unindexed*), την αναζήτηση μέσα σε ένα ολόκληρο κείμενο και χρησιμοποιείται από τους ερευνητές της δικανικής ανάλυσης στο φιλτράρισμα των μηνυμάτων ηλεκτρονικού ταχυδρομείου και στην ανάλυση της αποκτηθείσας δικανικής απόδειξης. Τα προϊόντα *dtSearch* λειτουργούν σε πλατφόρμες *Windows* και *NET*. Επίσης είναι διαθέσιμη μια έκδοση *Linux* της μηχανής *dtSearch* για προγραμματιστές.

- ***Sleuth Kit (TSK):*** Πρόκειται για μια συλλογή από εργαλεία εντολών βασισμένα σε *UNIX* που χρησιμοποιούνται για τη δικανική ανάλυση και βασίζονται στο σχεδιασμό και τον κώδικα του *The Coroner's Toolkit (TCT).* Περιλαμβάνει εργαλεία διαχείρισης αρχείων συστήματος και εργαλεία διαχείρισης μέσων. Τα εργαλεία διαχείρισης των αρχείων συστήματος όπως *fsstat, fls, ffind, icat, dcat* κ.α. χρησιμοποιούνται στην ανάλυση των αρχείων του συστήματος που βρίσκονται στο σκληρό δίσκο, με μη παρεμβατικό τρόπο. Τα εργαλεία διαχείρισης των μέσων χρησιμοποιούνται για την εξέταση της μορφής των δίσκων και των άλλων μέσων. Μερικά παραδείγματα εργαλείων διαχείρισης μέσων είναι τα *mmls* και *img_stat*.

3.4.1.3.3 Συστήματα Δικανικής Ανάλυσης (Toolkits)

Τα συστήματα δικανικής ανάλυσης συνήθως παρέχουν εργαλεία για την εκτέλεση πολλών δραστηριοτήτων στην έρευνα της δικανικής ανάλυσης. Δεν έχει αναπτυχθεί ένα μοναδικό σύστημα που να περικλείει όλες τις δικανικές δραστηριότητες που απαιτεί μια έρευνα.

- ***Το σύστημα The Coroner's (The Coroner's Toolkit, TCT):*** Πρόκειται για μια συλλογή από εργαλεία που χρησιμοποιούνται για την δικανική ανάλυση που γίνεται εκ των υστέρων σε ένα σύστημα *UNIX*. Τα εργαλεία που περιλαμβάνει το σύστημα «αιχμαλωτίζουν» πληροφορίες με βάση τη σειρά της μεταβλητότητας των αποδείξεων, συλλέγουν λεπτομέρειες σχετικές με τη μνήμη και τις ενεργές διεργασίες πριν η μνήμη επανεγγραφεί και οι διαδικασίες τελειώσουν. Επίσης χρησιμοποιούνται για τη συλλογή αποδείξεων σε συγκεκριμένο χρόνο, για την ανάκτηση σβησμένων αρχείων από μη χρησιμοποιημένα σημεία του σκληρού δίσκου. Και τέλος, ανακτούν κρυπτογραφημένα κλειδιά από ενεργές διεργασίες ή από αρχεία.
- ***Δικανικό Σύστημα (Forensic Toolkit, FTK):*** Το σύστημα αυτό έχει μια διεπαφή που είναι ευκολονόητη και εύχρηστη. Ανακτά και ταξινομεί με αυτόματο τρόπο τα σβησμένα και μερικώς επανεγραμμένα αρχεία. Επίσης ενσωματώνει το εργαλείο *dtSearch*, μια μηχανή ανάκτησης κειμένου που παρέχει μια δυνατή και εκτεταμένη λειτουργία αναζήτησης κειμένου. Τα φίλτρα του συστήματος επιτρέπουν την ταξινόμηση μέσω χιλιάδων αρχείων ώστε να βρεθούν γρήγορα οι απαιτούμενες αποδείξεις. Το *FTK* μπορεί επίσης να χρησιμοποιηθεί για την ανάλυση των μηνυμάτων ηλεκτρονικού ταχυδρομείου.

3.4.2 Δικανικές Αναλύσεις Δικτύων

Η γιγάντωση της χρήσης του διαδικτύου είχε σαν αποτέλεσμα την αύξηση των ηλεκτρονικών επιθέσεων και των ρηγμάτων στην ασφάλεια της επικοινωνίας. Οι υπάρχουσες μέθοδοι όπως η εξέταση των αρχείων καταγραφής (*log files)* των

εξυπηρετητών, των αρχείων των τειχών προστασίας, των γεγονότων ανίχνευσης των εισβολών, ο έλεγχος του λογισμικού κ.α. δεν επαρκούν για να αναγνωρίσουν τους εξελιγμένους εισβολείς που χρησιμοποιούν εργαλεία όπως η κρυπτογραφία. Τα εργαλεία δικανικής ανάλυσης δικτύων είναι ειδικευμένες μηχανές ανάλυσης ικανές να «αιχμαλωτίσουν» και να συσχετίσουν δεδομένα από πολλαπλές οντότητες δικτύων.

3.4.2.1 Κοινές Δραστηριότητες Δικανικής Ανάλυσης Δικτύων

Όταν ανιχνευθεί μια εισβολή σε ένα δίκτυο, το πρώτο βήμα που πρέπει να γίνει είναι η αναγνώριση και η συλλογή των δεδομένων. Επομένως, η προσεκτική ανάγνωση των αρχείων καταγραφής με τη χρήση εργαλείων δικανικής ανάλυσης μπορεί να αποδώσει πληροφορίες σχετικές με την εισβολή, όπως είναι το σημείο εισόδου, η αδυναμία την οποία εκμεταλλεύτηκε ο εισβολέας κ.α. Θα πρέπει να υπάρχει ιδιαίτερη προσοχή στα χρονικά αποτυπώματα του συστήματος ειδικά στην περίπτωση όπου τα πρωτόκολλα χρονικού συγχρονισμού όπως το πρωτόκολλο χρόνου δικτύου *(Network Time Protocol*, *NTP)* ή οι εξωτερικές πηγές χρόνου δεν έχουν χρησιμοποιηθεί. Πιο κάτω αναφέρονται μερικές σχετικές δραστηριότητες δικανικής ανάλυσης δικτύων.

3.4.2.1.1 Παρακολούθηση Δικτύων και Καταγραφή Αρχείων Δικτύων

Η ενεργητική διατήρηση των αρχείων καταγραφής αποτελεί πολύτιμη πληροφορία. Επίσης η παρακολούθηση του δικτύου για την ανακάλυψη ύποπτων συνδέσεων ή νέων διεργασιών σε πραγματικό χρόνο είναι ένας αποτελεσματικός τρόπος ανακάλυψης και αποφυγής των εισβολών. Οι ειδοποιήσεις εισβολών από συστήματα ανίχνευσης εισβολών (*IDS*) ενεργοποιούν την δικανική ανάλυση αλλά δεν παρέχουν πληροφορίες σχετικές με το τι συνέβη μετά την επίθεση. Η αύξηση του αριθμού των υπολογιστών που βρίσκονται σε δίκτυα και το μέγεθος του διαδικτύου κάνουν το έργο της παρακολούθησης της κίνησης του δικτύου μια πολύ ενδιαφέρουσα και γεμάτη προκλήσεις δραστηριότητα. Δεν είναι ακόμα καθαρά καθορισμένη η χρονική διάρκεια κατά την οποία θα πρέπει να διατηρούνται τα αρχεία καταγραφής στα διάφορα σημεία του δικτύου. Ο χρόνος αυτός εξαρτάται άμεσα από το μέγεθος της διαθέσιμης μνήμης. Η απόκτηση αρχείων καταγραφής των δικτύων, από πηγές διαφορετικής αρμοδιότητας είναι δύσκολη εξαιτίας της έλλειψης συνεργασίας.

3.4.2.1.2 Ιχνηλασία Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου

Τα μηνύματα του ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται συχνά στην τέλεση εγκλημάτων. Αν ένα ηλεκτρονικό μήνυμα (*e-mail*) σχετίζεται με ένα έγκλημα, θα πρέπει να καταγραφεί σαν απόδειξη και η επικεφαλίδα του μηνύματος (*header*) μπορεί να είναι χρήσιμη στην αναζήτηση του ύποπτου. Η διαδικασία ιχνηλάτισης των ηλεκτρονικών μηνυμάτων απαιτεί γνώση του τρόπου με τον οποίο δουλεύει το ηλεκτρονικό μήνυμα. Μερικά από τα στοιχεία των ηλεκτρονικών μηνυμάτων, όπως για παράδειγμα ο τελευταίος εξυπηρετητής από τον οποίο πέρασε το ηλεκτρονικό μήνυμα, δεν μπορούν να αποκρυβούν. Τα αρχεία καταγραφής των δρομολογητών και των τειχών προστασίας είναι δυνατό να βοηθήσουν στην επαλήθευση του μονοπατιού που ακολούθησε το ηλεκτρονικό μήνυμα. Οι εξυπηρετητές των ηλεκτρονικών ταχυδρομείων συνήθως διατηρούν αρχεία καταγραφής όλων των ηλεκτρονικών μηνυμάτων που έχουν επεξεργαστεί, και επομένως ακόμα και αν κάποιος χρήστης διαγράψει ένα ηλεκτρονικό μήνυμα, αυτό μπορεί να ανακτηθεί από τους εξυπηρετητές των ηλεκτρονικών ταχυδρομείων. Τα διάφορα νομικά θέματα και τα θέματα δικαιοδοσίας δημιουργούν προκλήσεις στην επιτυχή αναζήτηση των ιχνών των ηλεκτρονικών μηνυμάτων. Πολλές φορές τα αρχεία καταγραφής δεν διατηρούνται σωστά από τους *Internet Service Providers (ISP)* και από την άλλη μεριά κρυπτογραφημένα ηλεκτρονικά μηνύματα ή

μηνύματα με απογυμνωμένες επικεφαλίδες εισάγουν δυσκολίες στη διαδικασία ιχνηλάτισης των ηλεκτρονικών μηνυμάτων.

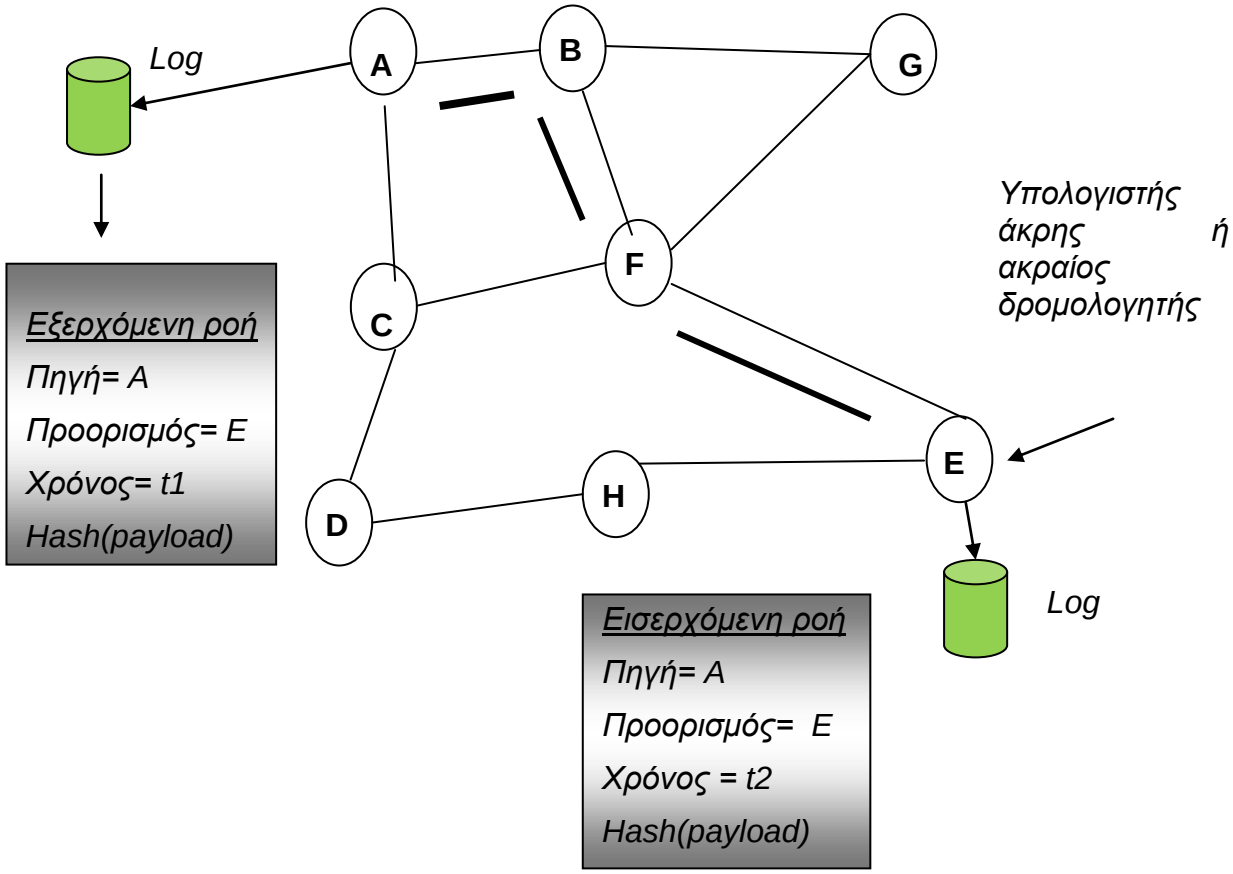
3.4.2.1.3 IP Traceback

Οι περισσότερες επιθέσεις άρνησης παροχής υπηρεσίας *(DoS)* συνεπάγονται έναν αριθμό πακέτων που στέλνονται στο σύστημα στόχο. Όλα τα σχετικά πακέτα έχουν προφανώς έγκυρες διευθύνσεις *IP*, ενώ δεν έχουν πληροφορία που θα μπορούσε να καθορίσει τον υπολογιστή από τον οποίο προήλθαν. Η διαδικασία *IP Traceback* συνεπάγεται την αναγνώριση της πηγής αυτών των πακέτων επίθεσης. Κάποιες τεχνικές *IP Traceback* περιλαμβάνουν άμεσες ερωτήσεις προς τους δρομολογητές του δικτύου σχετικά με την κίνηση που εξυπηρετούν, δημιουργία εικονικού υπερκείμενου δικτύου με τη χρήση μηχανισμών καταγραφής για την επιλεκτική παρακολούθηση της ροής των πακέτων και την αναγνώριση του μονοπατιού επίθεσης με ανακατασκευή, χρησιμοποιώντας μια συλλογή πακέτων σημειωμένων ή ειδικά παραγμένων από τους δρομολογητές διαμέσου του μονοπατιού επίθεσης. Θα πρέπει να σημειώσουμε ότι δεν υπάρχει κάποια λύση που να αναγνωρίζει με επιτυχία την πηγή σε όλες τις επιθέσεις.

3.4.2.1.4 Ανίχνευση της Επίθεσης προς την Πηγή (traceback) και Ανακατασκευή

Οι επιθέσεις που γίνονται μέσω διαδικτύου όπως είναι οι ιοί *(worm, virus)* γίνονται ολοένα και πιο εξελιγμένες και διαδίδονται πολύ γρήγορα με αυτοματοποιημένο τρόπο. Οι ιοί δεν χρειάζονται την ανθρώπινη αλληλεπίδραση για να διαδοθούν, είναι αυτόνομα και αυτό-μεταδιδόμενα κομμάτια κώδικα. Η ιχνηλάτιση της πραγματικής πηγής της κακόβουλης ροής πληροφοριών είναι ιδιαίτερα σημαντική ως δραστηριότητα δικανικής ανάλυσης δικτύων. Στο ***σχήμα 18*** βλέπουμε το μονοπάτι επικοινωνίας μεταξύ δύο κόμβων σε ένα δίκτυο. Οι λεπτομέρειες της ροής διατηρούνται και από τους δύο κόμβους, τον κόμβο πηγής *A* και τον κόμβο προορισμού *E*. Αν μια κακόβουλη ροή πληροφορίας ανιχνευθεί στον κόμβο *E*, ο κόμβος αυτός εξετάζει τον πίνακα των εισερχόμενων ροών για να διαπιστώσει την πηγή της κακόβουλης ροής. Ο κόμβος *E* μπορεί τότε να χρησιμοποιήσει ένα πρωτόκολλο ερωτήσεων-απαντήσεων για να διαπιστώσει την πηγή της ροής. Οι λεπτομέρειες της ροής μπορούν εναλλακτικά να αποθηκευτούν στους ακραίους δρομολογητές αντί για τους υπολογιστές των άκρων αποφεύγοντας έτσι μεταβολές σε όλους τους υπολογιστές των άκρων.

Η ανακατασκευή της επίθεσης θα επιτρέψει στους διαχειριστές του συστήματος να κατανοήσουν τους μηχανισμούς της διάδοσης και έτσι να μπορέσουν να διορθώσουν τα αδύναμα συστήματα και να αποφύγουν μελλοντικές επιθέσεις. Η ανίχνευση της πηγής μιας επίθεσης μέσω διαδικτύου είναι χρήσιμη για τη δίωξη αλλά και για τον περιορισμό των ζημιών.



Σχήμα 18: Ανίχνευση της πηγής ενός *worm* διαδικτύου

3.4.2.2 Εργαλεία Δικανικής Ανάπτυξης Δικτύων

Έχουν αναπτυχθεί διάφορα εργαλεία για την εκτέλεση των δραστηριοτήτων της δικανικής ανάλυσης των δικτύων, όπως είναι τα *Snort, BlackIce, TcpDump, Paraben's Network e-mail Examiner, NetAnalysis* κ.α. Τα εργαλεία δικανικής ανάλυσης δικτύων μπορούν να κατηγοριοποιηθούν σε εργαλεία βασισμένα σε υπολογιστή *(host based)* ή σε εργαλεία βασισμένα στο δίκτυο *(network wide).* Τα εργαλεία που βασίζονται στον υπολογιστή ελέγχουν τα πακέτα που εισέρχονται σε έναν συγκεκριμένο υπολογιστή (*host*) και παρουσιάζουν στον ερευνητή στατιστικά στοιχεία σχετικά με την κίνηση στον υπολογιστή. Τα εργαλεία που βασίζονται στο δίκτυο, έχουν πολλαπλά συστατικά που βρίσκονται σε διαφορετικά μέρη του δικτύου και επικοινωνούν μεταξύ τους έτσι ώστε να παρουσιάσουν τη συνολική πληροφορία του δικτύου. Ενδεικτικά παρουσιάζουμε κάποια από αυτά τα εργαλεία:

Εργαλεία Δικανικής Ανάλυσης βασισμένα σε Υπολογιστή (*host based*)

Αυτά τα εργαλεία εγκαθίστανται σε έναν υπολογιστή του δικτύου και βοηθούν στην κατανόηση της δραστηριότητας του δικτύου συλλέγοντας και αναλύοντας τα πακέτα που φθάνουν σε αυτόν τον υπολογιστή. Αυτά τα εργαλεία συνήθως παρέχουν πολλή πληροφορία στη μορφή αρχείων καταγραφής.

- ***TcpDump:*** Πρόκειται για ένα εργαλείο εντολών (*command line)* που χρησιμεύει στην παρακολούθηση του δικτύου, στην εύρεση λαθών των πρωτοκόλλων και στην απόκτηση δεδομένων. Τυπώνει τις επικεφαλίδες των πακέτων στη

διεπαφή του δικτύου οι οποίες ταιριάζουν με μια συγκεκριμένη δυαδική έκφραση. Είναι διαθέσιμο για χρήση σε πολλές λειτουργικές πλατφόρμες όπως *Linux, Windows95, 98, NT, 2000, XP, Vista*. Για να ελέγχει την κίνηση από και προς άλλους υπολογιστές, το εργαλείο θα πρέπει να λειτουργεί σε ένα δίκτυο κατανεμημένης πρόσβασης.

- ***Snort*:** Πρόκειται για ένα εργαλείο ασφάλειας ανοιχτό στη χρήση που αρχικά αναπτύχθηκε για την πλατφόρμα *UNIX* του 1998 και στη συνέχεια μεταφέρθηκε σε πλατφόρμα *Win32*. Είναι ένα απλό εργαλείο εντολών που χρησιμοποιείται για να παρακολουθεί την κίνηση του δικτύου, ελέγχει βάσει κανόνων την ύπαρξη υπογραφών εισβολής, ειδοποιεί και καταγράφει σε περίπτωση που ανακαλύψει κάποια ταυτοποίηση σε υπογραφές εισβολής, πραγματοποιεί ανάλυση πρωτοκόλλου, ελέγχει το δίκτυο για λάθη (*troubleshoot*) και ελέγχει την ύπαρξη μη εξουσιοδοτημένων εφαρμογών. Απαιτεί μικρή χωρητικότητα μνήμης και καταναλώνει πολύ λίγη διαχειριστική ισχύ. Μπορεί στην ουσία να ακούσει όλη την κίνηση σε έναν υπολογιστή ή με τον κατάλληλο μετασχηματιστή να ακούσει όλη την κίνηση στο δίκτυο.

Εργαλεία Δικανικής Ανάλυσης βασισμένα σε Δίκτυο (*network based*)

Τα δικτυακά εργαλεία δικανικής ανάλυσης αποτελούνται από πολλές συσκευές παρακολούθησης που μπορούν να εγκατασταθούν σε διαφορετικά σημεία του δικτύου και χρησιμοποιούνται για κατανεμημένη επιτήρηση στο δίκτυο. Η πληροφορία που απαιτείται για να εκτελεστούν συγκεκριμένες δραστηριότητες δικανικής ανάλυσης όπως *IP traceback*, η ανακατασκευή της επίθεσης, η ιχνηλάτιση των μηνυμάτων ηλεκτρονικού ταχυδρομείου πρέπει να συλλεχθεί από τους υπολογιστές που βρίσκονται στο ίδιο δίκτυο (*domain*) όπου βρίσκεται και ο υπολογιστής στόχος ή από συνεργαζόμενους υπολογιστές που βρίσκονται έξω από το δίκτυο (*domain*). Τέτοιου είδους εργαλεία παρακολούθησης ενσωματώνουν δεδομένα από διαφορετικά συστήματα παρακολούθησης και παρέχουν μια πλήρη και περιεκτική εικόνα της δραστηριότητας του δικτύου. Ένα δημοφιλές εργαλείο δικανικής ανάλυσης δικτύου περιγράφεται στη συνέχεια:

- ***Niksun NetDetector 2005*:** Αποτελεί μια πλήρη λειτουργική εφαρμογή για επιτήρηση ασφάλειας, ανίχνευση, ανάλυση και δικανική ανάλυση δικτύων. Μπορεί να ανιχνεύσει ανωμαλίες σε περιπτώσεις υπογραφών και στατιστικών και αιχμαλωτίζει και αποθηκεύει τα συμβάντα στο δίκτυο. Το εργαλείο αυτό, χρησιμοποιώντας ένα δυνατό *GUI* μπορεί να ανακατασκευάσει επιτυχώς εφαρμογές *web*, ηλεκτρονικά μηνύματα, *FTP, Telnet, VoIP* και να κάνει υψηλού επιπέδου δικανική ανάλυση σε επίπεδο πακέτου.

3.4.3 Σύνοψη Εργαλείων Δικανικής Ανάλυσης

Υπάρχουν διαθέσιμα πλέον πολλά εργαλεία δικανικής ανάλυσης, τόσο ανοιχτού κώδικα όσο και εμπορικά, τα οποία μπορούμε να διακρίνουμε ανάλογα με τη χρήση τους στις παρακάτω κατηγορίες: ***ανάκτησης δεδομένων, διαχείρισης αποθηκευτικών μέσων και αρχείων, ανάλυσης εφαρμογών και ανάλυσης δικτυακής κίνησης***. Μία λίστα διαθέσιμου λογισμικού μπορεί να αναζητηθεί στο δικτυακό τόπο του *Open Source Digital Forensics (www.opensourceforensics.org).*

3.4.3.1 Εργαλεία Ανάκτησης Δεδομένων

Παρουσιάζουμε μια ενδεικτική λίστα του διαθέσιμου ελεύθερου λογισμικού ή ανοιχτού κώδικα με κύριο αντικείμενο την ανάκτηση δεδομένων.

Τίτλος	***Περιγραφή***	***Πηγή αναφοράς***
Forensic Acquisition Utilities	Μία συλλογή από εργαλεία για *Windows όπως dd.exe, md5sum.exe, wipe.exe, nc.exe*	*http://users.erols.com/gmgarner/forensics/*
Ftimes	Είναι ένα σύστημα βασικών εργαλείων συλλογής και ανάλυσης. Ο κύριος σκοπός του είναι να συλλέγει και να παράγει πληροφορίες για καταλόγους και αρχεία με έναν τρόπο όπως τα συστήματα προσδιορισμού εισβολέων. Υπάρχουν εκδόσεις για περιβάλλον *Windows* και *Unix*.	*http://ftimes.sourceforge.net/Ftimes/index.shtml*
liveview	Είναι ένα *java-based* εργαλείο σε γραφικό περιβάλλον το οποίο δημιουργεί μια *Vmware* εικονική μηχανή για να επεξεργαστεί ένα πλήρες αντίγραφο του δίσκου. Υπάρχουν εκδόσεις για περιβάλλον *Windows* και *Unix*.	*http://liveview.sorceforge.net/*
netcat	Είναι ένα απλό εργαλείο το οποίο διαβάζει και γράφει δεδομένα σε μια δικτυακή επικοινωνία, χρησιμοποιώντας *TCP* ή *UDP* πρωτόκολλο. Υπάρχουν εκδόσεις για περιβάλλον *Windows* και *Unix*.	*http://www.atstake.com/research/tools/network_utilities/*
ProDiscover DFT	Παρέχει σε έναν ερευνητή μια ολοκληρωμένη εφαρμογή σε *Windows* περιβάλλον για τη συλλογή, την ανάλυση, τη διαχείριση και την καταγραφή ενός δίσκου.	*http://techpathways.com*
psloggedon	Είναι ένα *applet* το οποίο παρουσιάζει τους χρήστες ενός συστήματος περιγράφοντας τη φυσική τους θέση.	*http://www.sysinternals.com/ntw2k/freeware/psloggedon.shtml*
TULP2G	Είναι ένα λογισμικό που επιτρέπει εύκολα την εξαγωγή και την αποκωδικοποίηση δεδομένων από ψηφιακές συσκευές (κινητά τηλέφωνα, *SIM* κάρτες κ.α.)	*http://sourceforge.net/projects/tulp2g/*
Webjob	Κατεβάζει ένα πρόγραμμα πάνω σε *HTTP/HTTPS*, το εκτελεί σε	*http://webjob.sourcefotge.net/*

	ένα προστατευμένο πλαίσιο. Το αποτέλεσμα, αν υπάρχει, το κατευθύνει σε *stdout/stderr* ή σε μια *Web* διεύθυνση.	*Webjob/index.shtml*
Automated Imange and Restore (AIR)	Είναι ένα *GUI front-end* για *dd/dcfldd* και σχεδιάστηκε για την εύκολη δημιουργία *bit* αντιγράφων.	*http://air-imager-sourceforge.net/*
Dcfl-dd	Αποτελεί τροποποίηση του *dd*, ενισχύοντάς το με μηχανισμό *MD5* κατά την αντιγραφή δεδομένων.	*http://sourceforge.net/projects/biatchux*
Unhide	Χρησιμοποιείται στην αποκάλυψη διεργασιών και *TCP/UDP* συνδέσεων από *rootkits/LKMs* ή από άλλες τεχνικές απόκρυψης.	*http://www.security-projects.com/?Unhide*

3.4.3.2 Εργαλεία Διαχείρισης Αποθηκευτικών Μέσων και Αρχείων

Ακολουθεί μια ενδεικτική λίστα ελεύθερου λογισμικού ή ανοιχτού κώδικα που χρησιμοποιείται σε μια διαδικασία διερεύνησης για την αποτύπωση αποθηκευτικών μέσων (κλωνοποίηση δίσκων, ανάλυση) και τη διαχείριση αρχείων (εμφάνιση κρυφών, αποκατάσταση από καταστροφή, διαγραφή κ.α.).

Τίτλος	***Περιγραφή***	***Πηγή αναφοράς***
TestDisk	Εργαλείο για τον έλεγχο και την ακύρωση διαγραφής ενός *partition*. Λειτουργεί με τα συστήματα αρχείων *FAT, Linux EXT2/3, Linux SWAP, NTFS, Netware, BeFS (BeOS), ReiserFS*.	*http://www.cgsecurity.org/testdisk.html*
Explore2fs	Βλέπει τα περιεχόμενα ενός *Ext2FS partition* από *Windows* περιβάλλον.	*http://uranus.it.swin.edu.au/~jn/linux/explore2fs.htm*
CDfs	Είναι ένα σύστημα αρχείων για *Linux* το οποίο εξάγει όλα τα *traks* και τα *boot images* σε ένα *CD*, σαν κανονικά αρχεία.	*http://www.elis.rug.ac.be/~ronsse/cdfs/*
gpart	Είναι ένα εργαλείο που προσπαθεί να μαντέψει το *primary partition table* από ένα σκληρό δίσκο στην περίπτωση που το *primary partition table*	*http://www.stud.uni-hannover.de/user/76201/gpart/*

	στον *sector* 0 είναι κατεστραμμένο ή σβησμένο.	
The Sleuth Kit	Μια συλλογή από εργαλεία *command line* για την ανάλυση συστημάτων αρχείων τύπου *NTFS, FAT, FFS, EXT2FS και για DOS, BSD, Sun* και *MAC partitions*. Τα εργαλεία επιτρέπουν την ανάκτηση και την ανάλυση σβησμένων δεδομένων, και την επεξεργασία διαφόρων άλλων δεδομένων.	*http://www.sleuthkit.org/sleuthkit/*
Disk Investigator	Ανιχνεύει και αποκαλύπτει ό,τι είναι κρυμμένο σε σκληρό δίσκο. Βοηθά στην ανάκτηση χαμένων δεδομένων. Παρακάμπτει το λειτουργικό σύστημα και εμφανίζει το πραγματικό περιεχόμενο του συστήματος αρχείων. Επαναφέρει σβησμένα αρχεία.	*http://www.theabsolute.net/sware/dskinv.html*

3.4.3.3 Εργαλεία Ανάλυσης Εφαρμογών

Ακολουθεί μια ενδεικτική λίστα λογισμικού ανοιχτού κώδικα που χρησιμοποιείται σε μια διαδικασία διερεύνησης για την ανάλυση δεδομένων και ενεργειών που προκύπτουν από υφιστάμενες εφαρμογές των πληροφοριακών συστημάτων.

Τίτλος	***Περιγραφή***	***Πηγή αναφοράς***
Event Log Parser	Ένα *PHP script* για την ανάλυση αρχείων καταγραφής γεγονότων (*event logs*) σε *Windows*.	*http://www.whitehats.ca/main/members/Malik/malik_eventlogs/malik_eventlogs.html*
Microsoft Log Parser	Παρέχει ένα περιβάλλον για αναζήτηση πληροφοριών σε *text-based data* όπως τα αρχεία καταγραφής (*log files), Event log, Registry, Active Directory*.	*http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx*
LibPST	Παρέχει λειτουργίες για πρόσβαση σε *Outlook's Personal Folders*.	*http://sourceforge.net/projects/ol2mbox*

3.4.3.4 Εργαλεία Ανάλυσης Δικτυακής Κίνησης

Ακολουθεί μια ενδεικτική λίστα λογισμικού ανοιχτού κώδικα που χρησιμοποιείται σε μια διαδικασία διερεύνησης περιστατικών δικτύων.

Τίτλος	***Περιγραφή***	***Πηγή αναφοράς***
Wireshark	Αποτελεί ένα *network analyzer* και είναι η συνέχεια του *Ethereal*. Καταγράφει όλη τη δικτυακή επικοινωνία που διέρχεται από το σημείο εφαρμογής του.	http://www.wireshark.org
tcpflow	Είναι μια εφαρμογή η οποία καταγράφει όλες τις *TCP* συνδέσεις, τις αποθηκεύει και τις αναλύει.	*http://www.circlemud.org/~jelson/software/tcpflow*
tcpreplay	Πραγματοποιεί επαναποστολή *tcpdump* αρχείων για την ανίχνευση *sniffers* αλλά και δρομολογητών (*routers*), τειχών προστασίας (*firewalls*) και *IDS*.	http://tcpreplay.sourceforge.net/

3.4.4 *National Software Reference Library* (*NSLR)*

Η βιβλιοθήκη αυτή έχει σχεδιαστεί για να παρέχει δεδομένα σε διεθνές επίπεδο τα οποία είναι αποδεκτά από τις δικαστικές αρχές και μπορούν να τα χρησιμοποιήσουν οι ερευνητές και οι σχεδιαστές δικανικών εργαλείων. Η βιβλιοθήκη αυτή έχει σχεδιαστεί και αναπτύσσεται στα πλαίσια ενός έργου που υποστηρίζεται από το Υπουργείο Δικαιοσύνης των ΗΠΑ και από διωκτικές αρχές. Συλλέγει λογισμικό από διάφορες πηγές και ενσωματώνει προφίλ αρχείων που έχουν εξαχθεί από αυτό το λογισμικό σε ένα αρχείο πληροφοριών που ονομάζεται *Reference Data Set (RDS*). Το *RDS* περιλαμβάνει γνωστές ψηφιακές υπογραφές, ανιχνευμένες κακόβουλες εφαρμογές λογισμικού. Οι κρυπτογραφικές λειτουργίες όπως η *SHA1* και η *MD5* χρησιμοποιούνται για την παραγωγή του ψηφιακού αποτυπώματος.

Το *RDS* μπορεί να χρησιμοποιηθεί για να ελέγξει αρχεία ενός υπολογιστή και να τα ταυτοποιήσει με δικά του προφίλ αρχείων και έτσι να πιστοποιήσει ποιά αρχεία είναι σημαντικά στοιχεία αποδείξεων. Με τη χρήση των υπογραφών, οι ερευνητές των αρχών δίωξης αγνοούν τα καλοήθη αρχεία στους υπολογιστές που έχουν κατασχεθεί, οι διαχειριστές των συστημάτων μπορούν να αναγνωρίσουν τα σημαντικά αρχεία του συστήματος που έχουν διαταραχθεί όπως επίσης να ξεχωρίσουν τις εφαρμογές από τα δεδομένα που έχουν δημιουργηθεί από χρήστες. Το *NSLR* μπορεί να χρησιμοποιηθεί για τη δίωξη εγκλημάτων πνευματικής ιδιοκτησίας.

3.4.5 Επίλογος

Έχει ήδη αναγνωριστεί εδώ και χρόνια η ανάγκη για μέτρα ασφάλειας που θα θωρακίσουν τους υπολογιστές και τα δίκτυα από τις επιθέσεις μέσω διαδικτύου και από το κυβερνο-έγκλημα. Τη λύση για την εύρεση του δράστη ενός εγκλήματος που τελείται μέσω υπολογιστή (μετά το συμβάν) την παρέχει η δικανική ανάλυση η οποία συλλέγει πληροφορίες ώστε να αποτρέπει παρόμοιες επιθέσεις στο μέλλον. Αν και υπάρχουν πολλά εργαλεία που βοηθούν στην δικανική ανάλυση, πολύ λίγα από αυτά παρέχουν αποδείξεις οι οποίες είναι ιδιαίτερα χρήσιμες στις δικαστικές αρχές. Έτσι εκτός από το πεδίο της ανάπτυξης περισσότερο εξελιγμένων εργαλείων δικανικής ανάλυσης, η

έρευνα στο μέλλον θα εστιάσει στην ενσωμάτωση δικανικών τεχνικών σε υπολογιστές *mainstream* και τεχνικών ασφάλειας δικτύου. **[9,10]**

3.5 Η Αξιολόγηση των Δικανικών Ψηφιακών Εργαλείων

Οι δικανικές ψηφιακές τεχνικές και τα δικανικά εργαλεία θα πρέπει να πληρούν τα βασικά αποδεικτικά και επιστημονικά πρότυπα ώστε να μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία στις νομικές διαδικασίες. Στις ΗΠΑ, το ανώτατο δικαστήριο γνωμοδότησε ότι μια απόδειξη ή γνώμη που αντλείται από επιστημονικές ή τεχνικές δραστηριότητες πρέπει να προέρχεται από μεθόδους που είναι επιστημονικά αξιόπιστες για να είναι αποδεκτή από τις δικαστικές αρχές. Ο όρος ***επιστημονικά αξιόπιστες*** υποδηλώνει ότι τα εργαλεία και οι τεχνικές θα πρέπει να αποδεικνύονται ότι λειτουργούν σωστά με τον εμπειρικό έλεγχο. Στην περίπτωση της ψηφιακής δικανικής ανάλυσης, αυτό συνεπάγεται ότι τα εργαλεία και οι τεχνικές που χρησιμοποιούνται στη συλλογή και ανάλυση των ψηφιακών αποδείξεων πρέπει να αξιολογηθούν και να αποδειχτεί ότι πληρούν τα επιστημονικά πρότυπα.

Ο παραδοσιακός έλεγχος επικύρωσης (*validation*) του λογισμικού εκτελείται ως μία δραστηριότητα ρουτίνας σε κάθε προσπάθεια ανάπτυξης λογισμικού. Υπάρχουν πολλές αναφορές και πρότυπα που αναλύουν το ρόλο του ελέγχου επικύρωσης κατά την διάρκεια της ανάπτυξης λογισμικού.

Συχνά δημιουργείται μια σύγχυση μεταξύ των όρων ***επικύρωση*** *(validation)* και ***επαλήθευση*** *(verification)* όσον αφορά στη χρήση τους στον έλεγχο του λογισμικού. Οι ορισμοί που παρέχονται από το *General Principles of Software validation, Final Guidance for Industry and FDA staff* είναι οι ακόλουθοι:

- ***Η επαλήθευση του λογισμικού*** παρέχει αντικειμενικές αποδείξεις ότι τα αποτελέσματα της σχεδίασης μιας συγκεκριμένης φάσης του κύκλου ανάπτυξης του λογισμικού, ικανοποιεί όλες τις απαιτήσεις της συγκεκριμένης φάσης. Η επαλήθευση του λογισμικού, ελέγχει τη συνοχή, την πληρότητα και την ορθότητα του λογισμικού και της υποστηρικτικής τεκμηρίωσης. Ο έλεγχος του λογισμικού αποτελεί μία από τις πολλές δραστηριότητες επαλήθευσης και προσβλέπει στο να επιβεβαιώσει ότι η ανάπτυξη του λογισμικού πληρεί τις απαιτήσεις που έχουν δοθεί.
- ***Η επικύρωση του λογισμικού*** αποτελεί μέρος της επαλήθευσης. Είναι η επιβεβαίωση μετά από έλεγχο και η παροχή αντικειμενικών αποδείξεων, ότι οι προδιαγραφές του λογισμικού συμμορφώνονται με τις απαιτήσεις του χρήστη και την προτιθέμενη χρήση και ότι οι συγκεκριμένες απαιτήσεις που υλοποιήθηκαν μέσω του λογισμικού μπορεί να θεωρηθούν ότι έχουν εκπληρωθεί. Οι δραστηριότητες της επικύρωσης του λογισμικού μπορεί να συμβούν τόσο κατά τη διάρκεια όσο και στο τέλος του κύκλου ζωής της ανάπτυξης λογισμικού, ώστε να επιβεβαιώσουν ότι όλες οι απαιτήσεις έχουν υλοποιηθεί.

3.5.1 Επικύρωση των Εργαλείων Ψηφιακής Δικανικής Ανάλυσης

Συνήθως οι τελικοί χρήστες ενός προϊόντος λογισμικού δεν μπορούν να προσφέρουν αποδείξεις ή μαρτυρία στις δικαστικές αρχές για να πιστοποιήσουν ότι το λογισμικό που χρησιμοποιήθηκε σε μια συγκεκριμένη έρευνα λειτούργησε σύμφωνα με τις απαιτήσεις. Κάποιες εταιρείες παρέχουν εκπροσώπους οι οποίοι δίνουν την εξειδικευμένη μαρτυρία τους στις δικαστικές αρχές, σχετικά με την εγκυρότητα του λογισμικού τους, αλλά αυτό δεν ακολουθείται σαν πρακτική στις περισσότερες έρευνες.

Ένας αρκετά μεγάλος αριθμός προϊόντων λογισμικού δικανικής ανάλυσης παράγεται *ad hoc*, από μικρά εργαστήρια ή μεμονωμένους σχεδιαστές λογισμικού οι οποίοι

αναγνωρίζουν την ανάγκη για δικανική ανάλυση και παρέχουν ένα προϊόν για να την ικανοποιήσουν. Εξ αιτίας της *ad hoc* φύσης τους, τα προϊόντα αυτά συχνά δεν υποβάλλονται σε εκτεταμένο έλεγχο. Αυτό το λογισμικό, πολλές φορές μοιράζεται μεταξύ των επαγγελματιών ή παρέχεται σαν λογισμικό ελεύθερης χρήσης (*open source software*). Οι επαγγελματίες που θα χρησιμοποιήσουν αυτό το λογισμικό στις έρευνές τους, απαιτείται να εκτελέσουν οι ίδιοι τους ελέγχους επικύρωσης του λογισμικού, ώστε να είναι σε θέση να επιβεβαιώσουν στον εαυτό τους αλλά και στις δικαστικές αρχές για την καταλληλότητα των εργαλείων τους και των αποτελεσμάτων.

Οι περισσότεροι επαγγελματίες έχουν πολύ μικρή εμπειρία στην διαδικασία επικύρωσης του λογισμικού. Επομένως, υπάρχουν πολλά πρακτικά ζητήματα που περιορίζουν τους επαγγελματίες των διωκτικών αρχών ή των βιομηχανιών στο να τελέσουν την επικύρωση του λογισμικού με την ίδια επιτυχία όπως οι επαγγελματίες σχεδιαστές λογισμικού και μηχανικοί. Επιπλέον οι επαγγελματίες των διωκτικών αρχών και των βιομηχανιών χρειάζονται απαραίτητα τεκμηρίωση που να ικανοποιεί το επίπεδο της εμπειρίας που έχουν στην ψηφιακή δικανική ανάλυση. Και τέλος στην πράξη, συνήθως υπάρχουν χρονικοί περιορισμοί που περιορίζουν τους επαγγελματίες στο να επικυρώσουν μόνο ένα υποσύνολο των λειτουργιών του εργαλείου που θα χρησιμοποιηθεί για την τρέχουσα έρευνα.

Στην πράξη, υπάρχουν πολύ λίγες πιθανότητες να μπορέσουν οι επαγγελματίες της δικανικής ψηφιακής ανάλυσης να τελέσουν πλήρεις και εξαντλητικούς ελέγχους επικύρωσης. Ο ένας λόγος είναι ο χρόνος: συχνά οι υποθέσεις που αναφέρονται στις διωκτικές αρχές παραμένουν για μήνες μέχρι να γίνει η ψηφιακή δικανική ανάλυση. Αυτό που χρειάζεται είναι να υπάρχει μια διαδικασία που θα μειώσει το χρόνο που ξοδεύεται κατά την εξέταση ενός συστήματος, ενώ θα διατηρεί ένα υψηλό επίπεδο ποιότητας. Μια τέτοια διαδικασία θα είναι πολύ χρήσιμη τόσο στους επαγγελματίες της ψηφιακής δικανικής ανάλυσης όσο και στις δικαστικές αρχές.

3.5.1.1 Μέθοδοι Ελέγχου Επικύρωσης

Θα περιγράψουμε μεθόδους επικύρωσης οι οποίες χρησιμοποιούνται από τους επαγγελματίες. Οι μέθοδοι αυτές πληρούν τις ανάγκες των επαγγελματιών γιατί: **α)** είναι απλές αλλά αποτελεσματικές μέθοδοι και απαιτούν μικρή γνώση της διαδικασίας ελέγχου επικύρωσης του λογισμικού και **β)** είναι αποτελεσματικές γιατί επιτρέπουν στον ελεγκτή να ελέγξει μόνο εκείνες τις λειτουργίες που θα χρησιμοποιηθούν στην τρέχουσα περίπτωση.

3.5.1.1.1 Έλεγχος Λευκού Κουτιού (White Box Testing)

Ο έλεγχος του λευκού κουτιού περιλαμβάνει εξέταση του πηγαίου κώδικα πάνω στον οποίο έχει δημιουργηθεί η εφαρμογή, και επίσης ελέγχους που συγκρίνουν την απόδοση του λογισμικού σε σχέση με τις απαιτήσεις. Η απαίτηση αποτελεί την προδιαγραφή αυτού που θα πρέπει να κάνει το λογισμικό. Οι απαιτήσεις αναπτύσσονται κατά τη διάρκεια των φάσεων ανάπτυξης των απαιτήσεων του λογισμικού που αποτελεί μια από τις αρχικές φάσεις στην διαδικασία ανάπτυξης λογισμικού.

Μια επίσημη εξέταση του πηγαίου κώδικα ονομάζεται ***περιδιάβαση κώδικα*** (*code walkthrough*) και περιλαμβάνει δύο βασικές απαιτήσεις. Πρώτα, ο πηγαίος κώδικας πάνω στον οποίο έχει αναπτυχθεί η εφαρμογή θα πρέπει να είναι διαθέσιμος για εξέταση. Οι περισσότεροι εμπορικοί προμηθευτές κώδικα είναι απρόθυμοι στο να διαθέσουν τον πηγαίο κώδικα σε εξωτερικούς εξεταστές εξ αιτίας των θεμάτων κατοχύρωσης πνευματικής ιδιοκτησίας. Έτσι, η περιδιάβαση κώδικα από εξωτερικούς

εξεταστές που δεν ανήκουν στις εταιρείες που σχεδιάζουν τον κώδικα, δεν αποτελεί κοινή πρακτική.

Η δεύτερη απαίτηση είναι τα μέλη της ομάδας που εξετάζουν τον κώδικα να έχουν στέρεες τεχνικές γνώσεις και εμπειρία σε δύο περιοχές. Κάποια μέλη της ομάδας, όπως οι προγραμματιστές και οι μηχανικοί λογισμικού θα πρέπει να έχουν εμπειρία στον προγραμματισμό και στην ανάπτυξη λογισμικού. Επιπλέον, η περιδιάβαση του κώδικα απαιτεί συμμετοχή ατόμων με γνώση του δικτύου και των έργων που εκτελούνται με το λογισμικό που ελέγχεται. Έτσι, στο πλαίσιο της δικανικής ψηφιακής ανάλυσης αυτή η απαίτηση εμπλέκει και τους αντίστοιχους εμπειρογνώμονες με γνώση στη σύνθεση των μέσων επικοινωνίας, στα συστήματα αρχείων, στις δραστηριότητες της δικανικής ανάλυσης κ.α.

Η περιδιάβαση του κώδικα αποτελεί μια ιδιαίτερα εντατική εργασία – ενδεικτικά οι μεσαίες σε μέγεθος εφαρμογές περιλαμβάνουν, χιλιάδες ή ακόμα και εκατομμύρια γραμμές κώδικα – και χρειάζεται ακόμα και μήνες για να ολοκληρωθεί. Η περιδιάβαση του κώδικα, αν και είναι εξονυχιστική, είναι περιορισμένης χρήσης από τα μέλη της επιστημονικής κοινότητας που ασχολούνται με την ψηφιακή δικανική ανάλυση και αντιμετωπίζουν τις ταχύτατες αλλαγές του περιβάλλοντος του λογισμικού που σχετίζεται με τα εργαλεία ανακάλυψης ψηφιακών αποδείξεων.

3.5.1.1.2 Έλεγχος Μαύρου Κουτιού (Black Box Testing)

Ο έλεγχος του μαύρου κουτιού αξιολογεί το λογισμικό συγκρίνοντας την πραγματική του συμπεριφορά με την αναμενόμενη συμπεριφορά. Αντίθετα από τον έλεγχο του λευκού κουτιού, ο έλεγχος του μαύρου κουτιού δεν κάνει καμιά υπόθεση σχετικά με την εσωτερική δομή της εφαρμογής (δηλ. για τον πηγαίο κώδικα). Στη μέθοδο αυτή το λογισμικό θεωρείται ως μαύρο κουτί και η απόδοση της εφαρμογής αξιολογείται σχετικά με τις λειτουργικές απαιτήσεις.

Στο πεδίο της δικανικής ψηφιακής ανάλυσης, η μέθοδος εκτελείται χρησιμοποιώντας ένα εργαλείο που παρέχει δραστηριότητες δικανικής ψηφιακής ανάλυσης κάτω από διάφορες συνθήκες όπως είναι τα διαφορετικά συστήματα αρχείων, το υλικό των υπολογιστών (*hardware*), οι διαφορετικές παράμετροι του λογισμικού. Τα αποτελέσματα αυτών των ελέγχων που έχουν τελεστεί σε διαφορετικές συνθήκες συγκρίνονται με τις απαιτήσεις σχεδίασης του λογισμικού. Αν το εργαλείο λειτουργεί όπως περιγράφουν οι απαιτήσεις, τότε υπάρχει ένα επίπεδο εμπιστοσύνης ότι το εργαλείο αυτό θα λειτουργήσει με τον αναμενόμενο τρόπο και σε άλλες παρόμοιες συνθήκες. Ένα θετικό αποτέλεσμα, δηλώνει ότι έχουμε επικυρώσει το εργαλείο για τη συγκεκριμένη δραστηριότητα και τις συγκεκριμένες συνθήκες μόνο. Ωστόσο, αυτή η εμπιστοσύνη στο εργαλείο δεν εκτείνεται σε συνθήκες που δεν έχουν καλυφθεί κατά την επικύρωση του ελέγχου. Για παράδειγμα, μία μελέτη επικύρωσης μπορεί να αποδείξει ότι ένα εργαλείο περνάει τον έλεγχο για αναζήτηση κωδικοποιημένων, μη κατακερματισμένων (*non fragmented*) λέξεων *ASCII*. Αυτό το συμπέρασμα όμως, δεν γενικεύεται και σε άλλες κωδικοποιήσεις κειμένου όπως *UNICODE*, *UTF-8* ή ακόμα και κατακερματισμένο (*fragmented*) κείμενο *ASCII* διαμέσου μη συνεχόμενων *clusters*. Οι παρουσιάσεις σχετικά με τις ικανότητες ενός εργαλείου εκτείνονται μόνο ως εκεί που ο έλεγχος του εργαλείου καλύπτει κάποιες συγκεκριμένες συνθήκες.

Η μέθοδος αυτή μπορεί να εκτελεστεί πιο γρήγορα από τη μέθοδο του λευκού κουτιού, επειδή δεν περιλαμβάνει και την περιδιάβαση του κώδικα. Ωστόσο, μπορεί και αυτή να είναι μια χρονοβόρα διαδικασία καθώς ένας εκτεταμένος έλεγχος επικύρωσης μπορεί να περιλαμβάνει δεκάδες και εκατοντάδες σενάρια ελέγχου, καθένα από τα οποία μπορεί

να έχει διαφορετικούς συνδυασμούς *hardware*, μονάδων επικοινωνίας και παραμέτρων λογισμικού. Σε μια τυπική και εκτεταμένη διαδικασία επικύρωσης, είναι σημαντικό να ελέγχουμε το εργαλείο στο πλήρες εύρος των παραμέτρων που επιλέγονται από το χρήστη και με έναν αριθμό από διαφορετικές ομάδες δεδομένων ή δείγματα ελέγχου. Αν και ένας ή δύο έλεγχοι είναι δυνατό να παράγουν θετικά αποτελέσματα, πάντα υπάρχουν συνθήκες όπου το εργαλείο μπορεί να αποτύχει, συνθήκες οι οποίες ωστόσο είναι ασυνήθιστο να μην έχουν ελεγχθεί ή να μην έχουν προταθεί από τους σχεδιαστές λογισμικού. Κάποιες περίεργες συνθήκες αρχικοποίησης παραμέτρων, λειτουργικά κριτήρια κ.α. είναι δυνατό να αποκαλύψουν ένα κρυμμένο λάθος (π.χ. ένα λάθος στο λογισμικό), το οποίο αν και μπορεί να συμβεί σπάνια, στην ουσία ακυρώνει τη λειτουργία ενός εργαλείου για το δεδομένο συνδυασμό ή ομάδα δεδομένων.

3.5.1.1.3 Έγκαιρη Επικύρωση (Just-in-time Validation)

Πρόκειται για μια μεθοδολογία ελέγχου που περιλαμβάνει εργαλεία ελέγχου λογισμικού που χρησιμοποιούν μόνο αυτές τις παραμέτρους που θα χρησιμοποιηθούν και στην πραγματική συλλογή και ανάλυση των αποδείξεων (όπως είναι τα αρχεία συστήματος, οι τύποι των αρχείων, το *hardware*, οι μεταγωγείς (*switches)* λογισμικού κ.α.). Για παράδειγμα, αν ένας δικανικός ψηφιακός ελεγκτής χρησιμοποιήσει το εργαλείο *X* για να αναγνωρίσει γραφικά σε ένα μορφοποιημένο μέσο *NTFS (New Technology File System)*, τότε ο έλεγχος του εργαλείου επικύρωσης θα πρέπει να χρησιμοποιήσει αυτές τις παραμέτρους (δηλαδή *file system = NTFS, file types = graphics*). Η ομάδα των παραμέτρων που χρησιμοποιούνται για τον έλεγχο θα πρέπει να είναι ένα υποσύνολο των παραμέτρων που είναι διαθέσιμες για έλεγχο. Ωστόσο, ο έλεγχος μόνο των συνθηκών που χρειάζονται στη δεδομένη στιγμή μπορεί να γλιτώσει από προσπάθεια και χρόνο που χρειάζεται για να ελεγχθούν σενάρια ελέγχου που δεν είναι σχετικά για τη δεδομένη στιγμή.

Η μέθοδος αυτή μπορεί να διεξαχθεί με τη χρήση επικυρωμένων δεδομένων αναφοράς ή με την συγκριτική ανάλυση (*comparative analysis*) που θα περιγραφούν πιο κάτω.

3.5.2 Οδηγίες για τον Έλεγχο Επικύρωσης

Μια καλή πηγή οδηγιών για την επικύρωση των εργαλείων ψηφιακής δικανικής ανάλυσης αποτελεί το *Scientific Working Group for Digital Evidence (SWGDE) Recommended Guidelines for Validation*. Το *SWGDE* αποτελείται από μέλη διωκτικών αρχών, υπαλλήλους βιομηχανίας και μέλη ακαδημαϊκών σχολών και ο σκοπός του είναι να δημιουργήσει πρότυπα για την εύρεση και ανάλυση ψηφιακών αποδείξεων.

Οι οδηγίες του *SWGDE* περιγράφουν τις διαδικασίες που πρέπει κάποιος να ακολουθήσει κατά τη διαδικασία επικύρωσης του λογισμικού δικανικής ανάλυσης. Οι οδηγίες αυτές ορίζουν ότι η επικύρωση των εργαλείων περιλαμβάνει τη δημιουργία ενός πλάνου ελέγχου (*test plan*), την εκτέλεση των ελέγχων που ορίζονται στο πλάνο ελέγχου και την τεκμηρίωση των αποτελεσμάτων. Στη συνέχεια θα περιγράψουμε τις οδηγίες που θα ακολουθηθούν για να πιστοποιηθεί η έγκαιρη επικύρωση ενός εργαλείου για την αναγνώριση και την ανάκτηση διαγραμμένων αρχείων από την δισκέτα του υπολογιστή.

Πρώτο βήμα αποτελεί ***η ανάπτυξη του πλάνου ελέγχου***. Το πλάνο ελέγχου ορίζει το εργαλείο και τη λειτουργικότητα που θα πρέπει να ελεγχθεί και επίσης τον τρόπο με τον οποίο θα ελεγχθεί το εργαλείο. Επίσης περιλαμβάνει μια περιγραφή του σκοπού του ελέγχου, τις απαιτήσεις δηλ. τη λειτουργικότητα του εργαλείου που θα ελεγχθεί, μια

περιγραφή της μεθοδολογίας ελέγχου, τα αναμενόμενα αποτελέσματα, μια περιγραφή των σεναρίων ελέγχων και μια περιγραφή των δεδομένων ελέγχου.

Στο παράδειγμά μας, θα ελεγχθεί η δυνατότητα του εργαλείου *X* να αναγνωρίσει και να ανακτήσει τα διαγραμμένα αρχεία, που αποτελεί μια πολύ κοινή διαδικασία δικανικής ανάλυσης. Έτσι ο σκοπός του ελέγχου μπορεί να περιγραφεί ως εξής: ***να επικυρωθεί ότι το εργαλείο X έχει τη δυνατότητα να αναγνωρίσει και να ανακτήσει τα διαγραμμένα αρχεία σε μια formatted δισκέττα του υπολογιστή.***

Οι τρείς απαιτήσεις που ο έλεγχος αυτός θα πρέπει να έχει είναι:

1. Το εργαλείο θα πρέπει να μπορεί να αναγνωρίσει τα διαγραμμένα αρχεία και να τα σημειώσει με έναν τρόπο αναμφίβολο, έτσι ώστε ο ελεγκτής να μπορεί να διαχωρίσει τα διαγραμμένα από τα μη διαγραμμένα αρχεία.
2. Το εργαλείο θα πρέπει να μπορεί να αναγνωρίσει και να εμφανίσει *metadata* για τα διαγραμμένα αρχεία, ώστε να συμπεριλάβει τα μεγέθη των αρχείων, και τους χρόνους μετατροπής, πρόσβασης και δημιουργίας.
3. Το εργαλείο θα πρέπει να μπορεί να ανακτήσει και να εξάγει τα λογικά περιεχόμενα των διαγραμμένων αρχείων στον υπολογιστή του συστήματος αρχείων.

Βασισμένοι στις παραπάνω απαιτήσεις μπορούμε να προσδιορίσουμε τα αναμενόμενα αποτελέσματα του ελέγχου:

1. Το εργαλείο θα σημειώσει κάθε διαγραμμένο αρχείο, ώστε να διαχωρίσει τα διαγραμμένα από τα μη διαγραμμένα αρχεία.
2. Το εργαλείο θα πρέπει να εμφανίσει και να σημειώσει χωρίς αμφιβολία τα *metadata* των διαγραμμένων αρχείων.
3. Το εργαλείο θα γράψει τα περιεχόμενα των διαγραμμένων αρχείων στο σύστημα αρχείων του υπολογιστή χρησιμοποιώντας μοναδικά ονόματα για κάθε αρχείο που ανακτάται.
4. Το αποτέλεσμα της λειτουργίας κατακερματισμού (*hash*) των αρχείων που έχουν ανακτηθεί θα πρέπει να ταιριάζει με το αντίστοιχο αποτέλεσμα κατακερματισμού του πρωτότυπου αρχείου. Αυτό αποτελεί διαβεβαίωση ότι το ανακτώμενο αρχείο είναι ίδιο με το πρωτότυπο.

Στη συνέχεια θα παραθέσουμε τα σενάρια ελέγχου. Ένα σενάριο ελέγχου προσδιορίζει τις συνθήκες κάτω από τις οποίες θα ελεγχθεί το εργαλείο, όπως επίσης και τα κριτήρια επιτυχίας/αποτυχίας για κάθε σενάριο ελέγχου.

Τέλος θα πρέπει να περιγραφούν τα δεδομένα ελέγχου. Στην περίπτωσή μας, το μέσο που θα ελέγξουμε είναι μια δισκέττα μεγέθους 1,4*MB*, που είναι μορφοποιημένη (*formatted*) με το σύστημα αρχείων *FAT12*. Τα ψηφιακά στοιχεία που θα πρέπει να ανακτηθούν περιλαμβάνουν δύο είδη αρχείων: μια μη διαγραμμένη και μια διαγραμμένη έκδοση του αρχείου *A* (ένα μικρό αρχείο μεγέθους < 1K) και μια μη διαγραμμένη και μια διαγραμμένη έκδοση του αρχείου *B* (ένα μεσαίου μεγέθους αρχείο ~ 60K). Στα επόμενα βήματα θα προετοιμάσουμε τα μέσα ελέγχου που θα χρησιμοποιηθούν για τον έλεγχο.

Για να εξασφαλιστεί ένας επιστημονικά αυστηρός έλεγχος θα πρέπει πρώτα να εξασφαλίσουμε ότι το μέσο ελέγχου που θα χρησιμοποιήσουμε δεν περιέχει υπολείμματα τα οποία θα αλλοιώσουν τα αποτελέσματα. Η μεθοδολογία ελέγχου των μέσων περιλαμβάνει τα ακόλουθα:

1. Αποστείρωση του μέσου ελέγχου γράφοντας μια σειρά από χαρακτήρες πάνω σε όλη την εγγράψιμη περιοχή του μέσου, από τον πρώτο μέχρι τον τελευταίο τομέα (*sector*). Τυπικά, σε όλο το δίσκο γράφεται «0» (μηδέν), και αυτό αποτελεί μια καλή πρακτική που πιστοποιεί ότι όλος ο δίσκος είναι αποστειρωμένος.
2. Μορφοποίηση (*format*) του δίσκου, ώστε να δημιουργηθεί ένα σύστημα αρχείων.
3. Αντιγραφή των αρχείων ελέγχου στο μέσο.
4. Διαγραφή ορισμένων από τα αρχεία.
5. Φραγμό σε δυνατότητα εγγραφής στο μέσο ώστε να εξασφαλιστεί ότι τα δεδομένα του δεν θα αλλάξουν ακούσια.
6. Δημιουργία ενός ακριβούς δικανικού αντιγράφου (*forensic duplicate*) της εικόνας.
7. Υπολογισμός του αποτελέσματος της λειτουργίας κατακερματισμού (*hash*) και για το αντίγραφο και για το πρωτότυπο. Αυτές οι τιμές κατακερματισμού θα πρέπει να είναι ίδιες.

3.5.3 Συγκριτική Ανάλυση (*Comparative analysis)*

Η μέθοδος αυτή είναι χρήσιμη στην περίπτωση που μια επικυρωμένη πηγή αναφοράς δεδομένων είτε είναι μη διαθέσιμη, είτε η δημιουργία της απαιτεί μια σημαντική επένδυση σε χρόνο και πόρους που ακούσια θα καθυστερήσει την πραγματική εξέταση των αποδείξεων. Θα πρέπει να σημειώσουμε ότι η συγκριτική ανάλυση χρησιμοποιεί την ανάλυση του μαύρου κουτιού σαν μέθοδο ελέγχου του σχεδιασμού.

Το κλειδί στην συγκριτική ανάλυση είναι η σύγκριση των αποτελεσμάτων διαμέσου πολλαπλών ανεξάρτητων εργαλείων. Τα εργαλεία αυτά είναι ανεξάρτητα με την έννοια ότι έχουν σχεδιαστεί από διαφορετικές και ανεξάρτητες ομάδες προγραμματιστών και είναι λογισμικά ανοιχτά στη χρήση ή έχουν σχεδιαστεί από διαφορετικούς εμπορικούς οργανισμούς. Θα πρέπει να σημειώσουμε ότι οι εκδόσεις 1.0 και 1.1. του ίδιου εργαλείου δεν αποτελούν ανεξάρτητα εργαλεία. Αν τρία διαφορετικά εργαλεία δίνουν τα ίδια αποτελέσματα, έχουμε ισχυρές αποδείξεις ότι το λογισμικό λειτουργεί με τον τρόπο που πρέπει. Έχουμε μια ισχυρότερη αξίωση για επικύρωση, όταν ένα ή περισσότερα από τα εργαλεία έχουν επικυρωθεί χρησιμοποιώντας ένα σύνολο δεδομένων αναφοράς. Για παράδειγμα, αν τα εργαλεία *Y* και *Z* έχουν επικυρωθεί χρησιμοποιώντας ένα σύνολο δεδομένων αναφοράς, τότε έχουμε ισχυρότερη απόδειξη της επικύρωσης όταν το εργαλείο *X* παράγει τα ίδια αποτελέσματα όπως τα εργαλεία *Y* και *Z*. Αν κανένα από τα άλλα εργαλεία δεν έχει επικυρωθεί, η εμπιστοσύνη είναι πολύ αδύναμη παρά το γεγονός ότι και τα τρία εργαλεία που έχουν σχεδιαστεί από διαφορετικές ομάδες προγραμματιστών δίνουν τα ίδια αποτελέσματα.

Η πραγματική διαδικασία ελέγχου είναι ίδια όπως και στη μέθοδο του μαύρου κουτιού. Δημιουργείται ένα πλάνο ελέγχου και κάθε ένα από τα εργαλεία ελέγχεται, ακολουθώντας το πλάνο ελέγχου και χρησιμοποιώντας τα μέσα ελέγχου. Στη συνέχεια συγκρίνουμε τα αποτελέσματα των ελέγχων.

3.5.4 Η Αναγνώριση των Περιπτώσεων Λαθών στον Έλεγχο Επικύρωσης

Όταν ο έλεγχος μιας εφαρμογής λογισμικού αποτυγχάνει το πιο σημαντικό έργο είναι η προσπάθεια καθορισμού των αιτίων της αποτυχίας του ελέγχου. Θα πρέπει να

σημειώσουμε ότι ένας περιορισμένος αριθμός αποτυχιών δεν αποκλείει εντελώς την χρήση του συγκεκριμένου λογισμικού ελέγχου. Η αποτυχία θα πρέπει να ερμηνευτεί ανάλογα με τα συνολικά αποτελέσματα του ελέγχου και τη φύση των λαθών. Ανάλογα με τον τρόπο με τον οποίο θα χρησιμοποιηθεί το εργαλείο, ένα συγκεκριμένο ποσοστό λαθών μπορεί να είναι αποδεκτό αν αυτό το ποσοστό λαθών και οι τύποι των λαθών είναι γνωστά στοιχεία και λαμβάνονται υπόψη κατά την ανάλυση των δεδομένων που πρέπει να ανακτηθούν.

3.5.5 Επίλογος

Καθώς αυξάνεται συνεχώς ο αριθμός των δικανικών εφαρμογών λογισμικού και όσο το περιβάλλον όπου τα εργαλεία θα πρέπει να λειτουργήσουν συνεχώς εξελίσσεται με την ανάπτυξη νέων λειτουργικών συστημάτων και εφαρμογών υπολογιστών, η παραδοσιακή, εντατική επικύρωση του λογισμικού θα συνεχίσει να μην μπορεί να συμβαδίσει με τις απαιτήσεις της δικανικής κοινότητας για επικυρωμένο λογισμικό. Οι επαγγελματίες της δικανικής ανάλυσης του λογισμικού, όπως και τα μεγάλα εργαστήρια θα πρέπει να πραγματοποιούν την επικύρωση των εργαλείων με κάποιο βαθμό αυστηρότητας αν θέλουν τα αποτελέσματα αυτών των εργαλείων να συνεχίσουν να γίνονται δεκτά ως αποδείξεις από τις διωκτικές αρχές. Οι προσεγγίσεις που παρουσιάστηκαν, όταν εφαρμόζονται με την δέουσα επιμέλεια και την τεκμηρίωση, θα χρησιμοποιούνται ολοένα και περισσότερο για να παρέχουν την απαιτούμενη επικύρωση και διαβεβαίωση ότι οι δικανικές αναλύσεις του λογισμικού γίνονται με τον τρόπο που πρέπει. **[11]**

3.6 Συσχετισμός Αρχείων Καταγραφής (*log*): Τα Εργαλεία και οι Τεχνικές

Οι δικανικές λειτουργίες είναι στην ουσία ανεξάρτητες πλατφόρμας, αν και δεν μπορούμε να πούμε το ίδιο για τα αρχεία συστήματος και τα αρχεία καταγραφής (*log files*). Αρχικά, θα κατανοήσουμε την έννοια της ***διαδικασίας έρευνας*** στο περιβάλλον της ψηφιακής δικανικής ανάλυσης. Αυτή η διαδικασία αποτελείται από μια ακολουθία δραστηριοτήτων τις οποίες θα πρέπει να εκτελέσει ο δικανικός εξεταστής για να επιβεβαιώσει τη συμμόρφωση με τις δικανικές απαιτήσεις που τώρα είναι κοινές σε όλες τις χώρες.

Η διαδικασία της έρευνας αποτελείται από έξι στάδια, όπως φαίνεται στο ***σχήμα 19*****.**

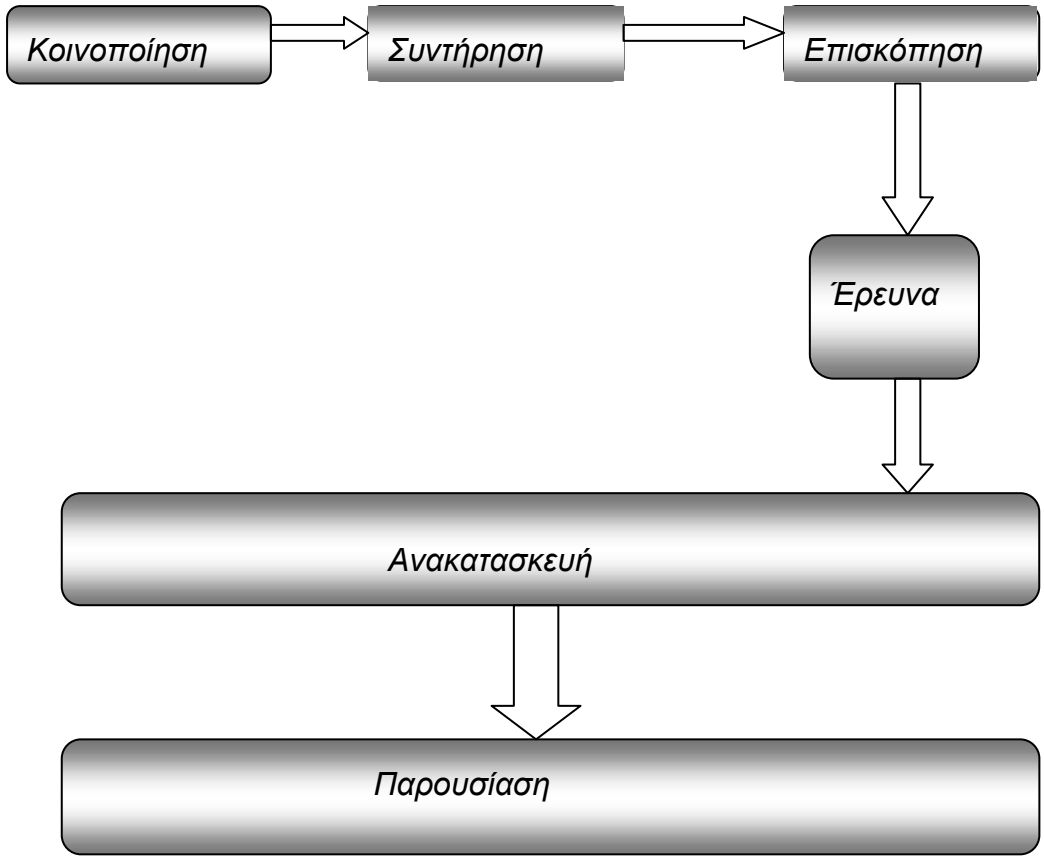
- ***Κοινοποίηση:*** Όταν μια επίθεση ανιχνευθεί από μια αυτόματη μηχανή, το εσωτερικό προσωπικό ή από μια εξωτερική πηγή (π.χ. από έναν διαχειριστή συστήματος που ανήκει σε άλλη εταιρεία ή από μια άλλη μονάδα εργασίας μέσα στην ίδια εταιρεία) δημιουργείται μια πρώτη αναφορά. Η επόμενη κίνηση συνήθως συνεπάγεται τη δημιουργία και την ανάπτυξη μιας ομάδας απόκρισης, της οποίας το πρώτο έργο είναι να πιστοποιήσει ότι η επίθεση πραγματικά έγινε.
- ***Συντήρηση:*** Αυτό το σημαντικό βήμα απόκρισης αντιπροσωπεύει την πρώτη ψηφιακή δικανική δραστηριότητα. Ο βασικός σκοπός εδώ είναι να επιβεβαιώσουμε ότι δεν έχουν γίνει διαφοροποιήσεις στη σκηνή του εγκλήματος έτσι ώστε να μην αποκλειστούν μελλοντικά ερευνητικά και αναλυτικά μέτρα. Η σκηνή του ψηφιακού εγκλήματος συνήθως αναπαράγεται με την δημιουργία μιας εικόνας του δίσκου έτσι ώστε να μπορούν να γίνουν λεπτομερείς αναλύσεις σε σωστά εξοπλισμένα εργαστήρια.
- ***Επισκόπηση:*** Αυτό είναι το πρώτο βήμα για τη συλλογή αποδείξεων. Η σκηνή του εγκλήματος ελέγχεται για φανερές ψηφιακές αποδείξεις και δημιουργούνται υποθέσεις για να οριοθετήσουν την περαιτέρω έρευνα.
- ***Έρευνα:*** Οι υποθέσεις που αναπτύχθηκαν στο στάδιο της επισκόπησης ελέγχονται με τη βοήθεια των εργαλείων ανάλυσης. Σε αυτό το στάδιο συλλέγονται περισσότερο λεπτομερείς αποδείξεις, επιτρέποντας στους ερευνητές να επικεντρωθούν στα σημεία ελέγχου που είναι άξια προσοχής.
- ***Αναδόμηση:*** Στο στάδιο αυτό γίνεται λεπτομερής έλεγχος για να συνδεθούν τα στοιχεία των αποδείξεων και να ανακατασκευαστεί το γεγονός. Πολύ συχνά σε αυτό το στάδιο ανακαλύπτονται νέες αποδείξεις.
- ***Παρουσίαση:*** Στο στάδιο αυτό, τα ευρήματα συναρμολογούνται σε ένα συμπαγές υλικό και παρουσιάζονται σε αυτούς που παράγγειλαν την έρευνα.

Υπάρχουν δύο βασικές περιπτώσεις που απαιτούν δικανική ανάλυση:

- Ανασχηματισμός μιας επίθεσης *(post mortem analysis),*
- Έλεγχος του υπολογιστή που μπορεί να χρησιμοποιήθηκε για να εκτελέσει μια εγκληματική πράξη.

Στην πρώτη περίπτωση, ο υπολογιστής που ελέγχεται αποτελεί το στόχο της επίθεσης, ενώ στη δεύτερη περίπτωση είναι το εργαλείο για τη διάπραξή της.

Τα αρχεία καταγραφής *(log files)* υπόκεινται στους ίδιους κανόνες όπως και η ανάλυση του συστήματος αρχείων.



Σχήμα 19: Η διαδικασία έρευνας

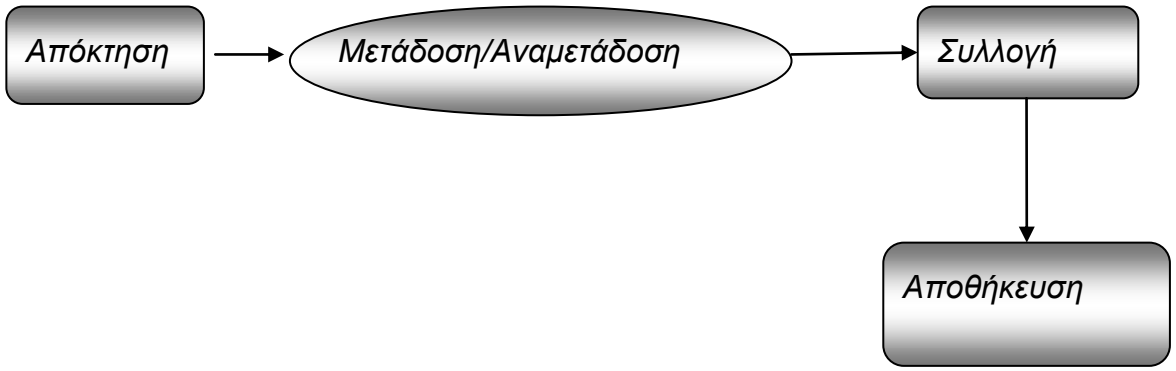
3.6.1 Χαρακτηριστικά και Προϋποθέσεις των Αρχείων Καταγραφής

Τα αρχεία καταγραφής έχουν κάποιες θεμελιώδεις προϋποθέσεις, όταν χρησιμοποιούνται για δικανικούς σκοπούς. Αυτές οι προϋποθέσεις είναι:

- ***Ακεραιότητα:*** Το αρχείο καταγραφής θα πρέπει να έχει παραμείνει αναλλοίωτο και να μην έχουν γίνει σε αυτό τροποποιήσεις από χρήστες μη εξουσιοδοτημένους.
- ***Χρονική επισήμανση:*** Το αρχείο καταγραφής θα πρέπει να σηματοδοτεί με σαφήνεια το χρόνο που έγινε ένα συγκεκριμένο γεγονός. Αυτό είναι ουσιώδες για να γίνουν οι απαραίτητοι συσχετισμοί μετά το γεγονός.
- ***Κανονικοποίηση και μείωση των δεδομένων:*** Η κανονικοποίηση αναφέρεται στην εξαγωγή δεδομένων από το πρωτότυπο αρχείο καταγραφής χωρίς να δημιουργείται πρόβλημα ακεραιότητας των δεδομένων. Αυτά τα δεδομένα είναι δυνατόν μετά να συσχετιστούν με άλλα δεδομένα διαφορετικού τύπου. Η μείωση των δεδομένων είναι μια διαδικασία για την αναγνώριση σχετικών γεγονότων και το συσχετισμό τους σύμφωνα με επιλεγμένα κριτήρια.

3.6.2 Η Ακεραιότητα των Αρχείων Καταγραφής

Η ακεραιότητα των αρχείων καταγραφής θα πρέπει να είναι εγγυημένη από τη στιγμή που αυτά δημιουργούνται. Ανεξάρτητα από τον τρόπο με τον οποίο αποκτώνται τα αρχεία καταγραφής, έχουν την παρακάτω ροή:



Σχήμα 20: Η ροή των αρχείων καταγραφής

Όταν ένας *sniffer* δικτύου, ένας πράκτορας του συστήματος (*system agent*) ή ένας δαίμονας (*daemon*) αποκτά ένα αρχείο καταγραφής γεγονότων το μεταδίδει σε μια μηχανή η οποία συνήθως είναι διαφορετική από αυτή στην οποία συνέβει το γεγονός. Μόλις το αρχείο φτάσει στη μηχανή προορισμού (που ονομάζεται μηχανή καταγραφής) μπορεί να αποθηκευτεί προσωρινά σε ένα *slot* που έχει εκχωρηθεί από πριν ή να εισαχθεί σε μια βάση δεδομένων ώστε να ελεγχθεί αργότερα. Η χωρητικότητα του δίσκου της μηχανής καταγραφής είναι καθορισμένη από την πολιτική του συστήματος και μόλις καταστεί πλήρης, τα πρωτότυπα αρχεία καταγραφής αποθηκεύονται σε άλλα μέσα και διαγράφονται ώστε να δημιουργηθεί χώρος για νέα αρχεία. Αυτή η μέθοδος ονομάζεται ***περιστροφή των αρχείων*** (*log rotation*).

Η ακεραιότητα των αρχείων καταγραφής μπορεί να παραβιαστεί με διάφορους τρόπους. Ένας εισβολέας μπορεί να εκμεταλλευτεί ένα μη κρυπτογραφημένο κανάλι μετάδοσης για να υποκλέψει και να μεταβάλλει το μεταδιδόμενο αρχείο. Θα μπορούσε επίσης να υποκλέψει μια *IP* διεύθυνση και να στέλνει αρχεία καταγραφής ώστε να νομίζει η μηχανή ότι λαμβάνει αρχεία από διαφορετική πηγή.

3.6.2.1 Προβλήματα Ακεραιότητας

Ένα βασικό πρόβλημα ακεραιότητας έχει σχέση με τον τρόπο που αντιμετωπίζονται τα αρχεία μόλις φθάσουν στη μηχανή καταγραφής. Αν η μηχανή καταγραφής έχει υποστεί επίθεση, η ακεραιότητα του αρχείου είναι σε κίνδυνο. Το περιεχόμενο μεμονωμένων αρχείων μπορεί να έχει μεταβληθεί ή να έχει διαγραφεί. Το ζήτημα της ακεραιότητας ασχολείται επίσης με το πώς γίνεται ο χειρισμός της πατρότητας των αρχείων καταγραφής. Κατά την παρουσίαση των αποδεικτικών στοιχείων θα πρέπει να υπάρχει βεβαιότητα σχετικά με το ποιά μηχανή δημιούργησε τα αρχεία καταγραφής και ποιός έκανε την έρευνα.

Υπάρχουν πολλές μέθοδοι που λύνουν αυτά τα προβλήματα. Η πρώτη ορίζεται στο *RFC 3195*, που προσδιορίζει μια πιθανή μέθοδο για αξιόπιστη μετάδοση των *Syslog*

μηνυμάτων. Είναι εξαιρετικά χρήσιμη όταν υπάρχουν πολλοί ενδιάμεσοι κόμβοι (*relays*) μετάδοσης μεταξύ της πηγής και της μηχανής καταγραφής.

Οι περισσότεροι διαχειριστές συστημάτων και αναλυτές ασφάλειας θεωρούν το *SCP (secure copy)* σαν μια ασφαλή λύση. Η πιο εμφανής αντίφαση είναι η ακαταλληλότητά του σε περιπτώσεις ανίχνευσης εισβολής, επειδή ο χρόνος της εισβολής δεν είναι δυνατόν να ανιχνευθεί από το αρχείο καταγραφής. Και επίσης παραμένει και το πρόβλημα της ασφάλειας της μετάδοσης μεταξύ των σημείων απόκτησης και συλλογής. Σαν απάντηση σε αυτό το πρόβλημα, τουλάχιστον στις αρχιτεκτονικές *UNIX*, χρησιμοποιείται κρυπτογράφηση ώστε να εγκατασταθεί ένα σχετικά ασφαλές κανάλι που να συνδέει τις μηχανές. Έτσι δημιουργείται μια κρυπτογραφημένη σύνδεση μεταξύ των κόμβων μετάδοσης.

3.6.3 Διαχείριση Χρονικής Επισήμανσης *(Time Stamping)*

Η διαχείριση χρονικής επισήμανσης των αρχείων καταγραφής είναι ένα πολύ σημαντικό ζήτημα. Κάθε αναφορά θα πρέπει να είναι 100% αξιόπιστη, όχι μόνο από άποψη ακεραιότητας με την αυστηρή έννοια (*IP*, θύρες, ωφέλιμα φορτία κ.α.) αλλά και ως προς την ημερομηνία και την ώρα που αναφέρθηκε ένα γεγονός. Η χρονική επισήμανση είναι ζωτικής σημασίας για δύο λόγους: εξατομίκευση της αναφοράς και συσχετισμό. Τα πιο κοινά προβλήματα σε αυτή την περίπτωση είναι η απουσία συγχρονισμού και η απουσία ομοιομορφίας της ζώνης ώρας.

Η απουσία συγχρονισμού συμβαίνει όταν τα σημεία απόκτησης (αισθητήρες του δικτύου και συσκευές *Syslog*) δεν είναι συγχρονισμένα με ένα διεθνές πρότυπο, αλλά μόνο μεταξύ τους. Σε αυτή την περίπτωση, βασιζόμαστε στο πρωτόκολλο ώρας δικτύου *(Network Time Protocol, NTP)*, το οποίο όμως παρουσιάζει κάποιες αδυναμίες, ειδικά σε κατανεμημένες αρχιτεκτονικές συνδεδεμένες με το δημόσιο δίκτυο. Επιπλέον το *NTP* δεν εγγυάται ομοιομορφία εκτός εάν έχουν υιοθετηθεί μια σειρά από μέτρα που προτείνονται από συγκεκριμένα *RFC* για συγκεκριμένους τύπους αρχείων, όπως περιγράφουμε πιο κάτω. Ορισμένοι κατασκευαστές έχουν δημιουργήσει συσκευές εξοπλισμένες με ιδιαίτερα αξιόπιστους επεξεργαστές οι οποίοι σηματοδοτούν χρονικά κάθε είσοδο και συγχρονίζουν οποιαδήποτε δραστηριότητα με ατομικά ρολόγια κατανεμημένα σε όλο τον κόσμο. Αυτή η λύση, μολονότι προσφέρει σε ένα βαθμό αξιοπιστία αυξάνει το κόστος σχεδιασμού και κάνει τη διαχείριση περισσότερο πολύπλοκη. Σε μια κατανεμημένη αρχιτεκτονική, αυτή η λύση παρουσιάζεται με τη μορφή μιας συσκευής που αλληλεπιδρά με ένα *PKI* το οποίο πιστοποιεί την αυθεντικότητα των κόμβων μετάδοσης ώστε να εμποδίσει την αλλοίωση της αναφοράς.

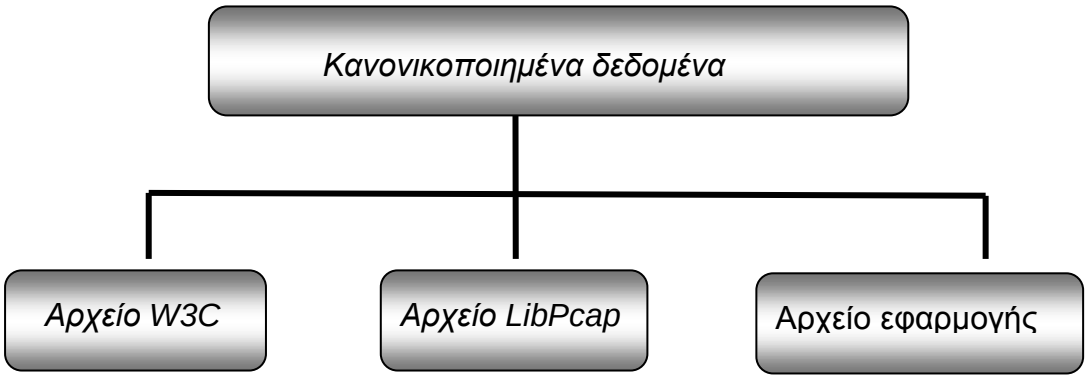
Αυτός ο τύπος αρχιτεκτονικής απαιτεί έναν βαρύ προϋπολογισμό, αλλά υπάρχουν και λιγότερο εκτενείς δυνατότητες αρχιτεκτονικής που τηρούν τη βέλτιστη πρακτική.

Δεδομένου ότι μια από τις πιο κοινές μορφοποιήσεις αρχείων καταγραφής είναι το *Libpcap* (που χρησιμοποιείται από τα *TcpDump* και *Ethereal*) πάνω σε συνδέσεις *TCP* (δηλ. συνδέσεις τριών δρόμων), είναι πιθανό να αποδοθεί επιπλέον επίπεδο χρονικής επισήμανσης, όπως για τα *RFC 1072* και *2018*, ενεργοποιώντας την δυνατότητα *SACK OK (Selective Acknowledgement OK*). Αυτή η επιλογή μπορεί να επιστρέψει ακόμα και μια τιμή χρονικής επισήμανσης (*time stamp)* μήκους 32 *bit* στα πρώτα τέσσερα *bytes* κάθε πακέτου, έτσι ώστε οι αναφορές μεταξύ κόμβων συνδιαλλαγής (*transaction*) όταν η επιλογή *SACK OK* είναι ενεργοποιημένη, να είναι συγχρονισμένες και να μπορούν να συσχετιστούν. Αυτή η προσέγγιση είναι αποτελεσματική μόνο όταν ολόκληρο το σύστημα και το δίκτυο έχουν αρχικοποιηθεί ως προς αυτή.

Όσον αφορά στις ***ζώνες ωρών***, στις διεθνώς κατανεμημένες αρχιτεκτονικές, κάποιοι διαχειριστές πληροφοριών ασφάλειας πιστεύουν ότι είναι συνετό να διατηρείται η τοπική ζώνη ώρας στο σύστημα ή στο αντικείμενο του δικτύου. Το μειονέκτημα σε αυτή την προσέγγιση είναι ότι περιπλέκει το συσχετισμό των αρχείων καταγραφής. Σήμερα, ολοένα και περισσότερες ζώνες ώρας βασίζονται στο *GM*T. Αυτό απλοποιεί τη διαχείριση, αλλά η όποια επιλογή θα πρέπει να ενσωματωθεί σε μία γενική πολιτική.

3.6.3.1 Κανονικοποίηση και Μείωση των Δεδομένων

Αν όλες οι αναφορές είχαν την ίδια μορφοποίηση, δεν θα υπήρχε ανάγκη για κανονικοποίηση. Σε ετερογενείς αρχιτεκτονικές δεν ισχύει αυτό. Η κανονικοποίηση είναι επίσης γνωστή σαν ***ενοποίηση γεγονότων*** *(event unification)* και υπάρχει έντονη ανάγκη γι' αυτή τη λειτουργία σε κατανεμημένες αρχιτεκτονικές. Ας υποθέσουμε, για παράδειγμα μια αρχιτεκτονική στην οποία θα πρέπει να συσχετίσουμε γεγονότα που έχουν καταγραφεί από μια σελίδα διαδικτύου, από έναν *sniffer* δικτύου και από μια ιδιωτική εφαρμογή. Η σελίδα διαδικτύου καταγράφει τα γεγονότα σε μορφοποίηση *w3c*, ο *sniffer* δικτύου σε μορφοποίηση *LibPcap*, και η ιδιωτική εφαρμογή σε κάποια άλλη μορφοποίηση. Αυτές οι αναφορές θα πρέπει να ενωθούν με κάποιο τρόπο. Η λύση δίνεται με την εύρεση κοινών σημείων μεταξύ των διαφορετικών μορφοποιήσεων και τη δημιουργία ενός επιπέδου αφαίρεσης, όπως φαίνεται στο παρακάτω ***σχήμα***.

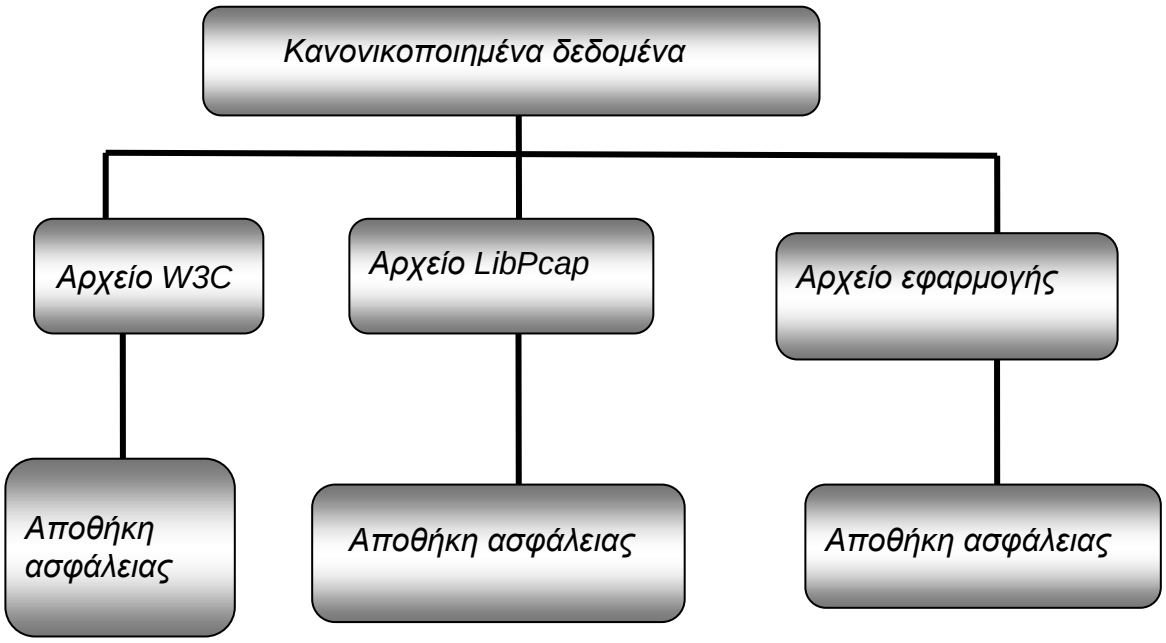


Σχήμα 21: Κανονικοποίηση αρχείων καταγραφής

Ένας εισβολέας, μπορεί να προσπαθήσει να παραβιάσει την ακεραιότητα των αρχείων καταγραφής στρέφοντας το ενδιαφέρον του στις συνδέσεις (*links*) μεταξύ των σημείων απόκτησης και των σημείων κανονικοποίησης. Το σημείο της κανονικοποίησης και το σημείο του συσχετισμού των αρχείων συνήθως βρίσκονται στην ίδια μηχανή. Αυτό, από την πλευρά της δικανικής ανάλυσης δικτύων θεωρείται πιθανό σημείο αποτυχίας και επομένως θα πρέπει να το χειριστούμε με τέτοιο τρόπο ώστε να εξασφαλίσουμε την ακεραιότητα και να μειώσουμε πιθανές απώλειες δεδομένων κατά τη διάρκεια της κανονικοποίησης των διαφορετικών μορφών αρχείων. Η πιο σύγχρονη πρακτική σε αυτή την περίπτωση, απαιτεί τη χρήση των *MD5* και *SHA-1* για να εξασφαλιστεί η ακεραιότητα, ενώ παράλληλα ένας σε βάθος έλεγχος της μηχανής κανονικοποίησης χρησιμεύει στο θέμα της απώλειας δεδομένων, διατηρώντας τα αρχεία καταγραφής της

πηγής σε κανονικοποιημένη μορφή. Στο ***σχήμα 22*****,** κάθε αρχείο καταγραφής της πηγής αποθηκεύεται σε στηρίγματα που δημιουργούνται γι' αυτό το σκοπό.

Για να διαχειριστούμε το θέμα των αποθηκών ασφάλειας (*secure repository*) και να έχουμε αρχεία καταγραφής που είναι αξιόπιστα, οι μηχανές στη δεύτερη γραμμή του ***σχήματος 22*** θα πρέπει να είναι έμπιστες, και να έχουν κρυπτοσυστήματα που να μπορούν να διαχειριστούν την αυθεντικοποίηση, τη λειτουργία του κατακερματισμού και την αξιόπιστη μετάδοση.



Σχήμα 22: Πολυεπίπεδη αρχιτεκτονική αρχείων καταγραφής

3.6.4 Συσχετισμός και Φιλτράρισμα

Για την εκτέλεση του συσχετισμού των αρχείων καταγραφής και του φιλτραρίσματος, θα πρέπει ο διαχειριστής του συστήματος και ο μηχανικός ασφάλειας να αντιμετωπίσουν τα προβλήματα που περιγράψαμε παραπάνω από την πλευρά της αρχιτεκτονικής του συστήματος.

3.6.4.1 Συσχετισμός

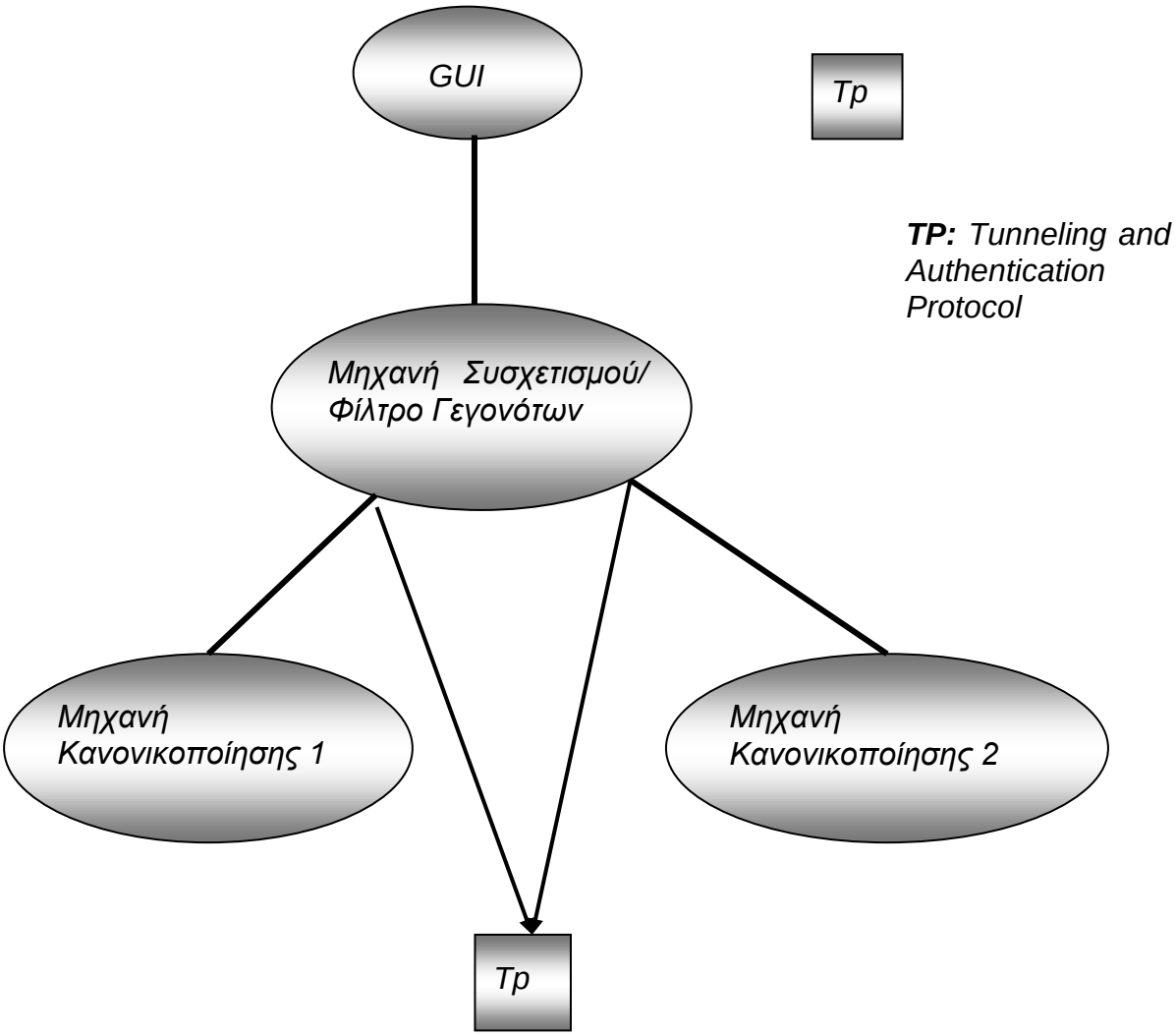
Ο συσχετισμός ορίζεται ως μια τυχαία, συμπληρωματική, παράλληλη ή αμοιβαία σχέση και ειδικά μια δομημένη, λειτουργική ή ποιοτική αντιστοιχία μεταξύ δύο συγκρίσιμων οντοτήτων.

Σε αυτή την ενότητα, χρησιμοποιούμε τον όρο ***συσχετισμό*** *(correlation)* για να περιγράψουμε την δραστηριότητα που εκτελείται από μία ή περισσότερες μηχανές για να ανακατασκευάσει ένα γεγονός το οποίο σχετίζεται με κάποιου είδους βιαιότητα.

Το ***φιλτράρισμα*** *(filtering)*, είναι η εξαγωγή και η διευθέτηση των δεδομένων (ανά τύπο πρωτοκόλλου, χρόνο, διεύθυνση *IP* και διεύθυνση *MAC* κ.α.). Μπορεί να γίνει από τις ίδιες μηχανές που κάνουν και το συσχετισμό.

Μια σχετικά πολύπλοκη αρχιτεκτονική μπορεί να έχει συσταθεί όπως φαίνεται στο ***σχήμα 23.***

Αν η *SCP* ή κάποια παρόμοια μέθοδος χρησιμοποιείται για να συλλέξει δεδομένα από τα σημεία απόκτησης (πριν να εισαχθούν τα αρχεία καταγραφής στις μηχανές κανονικοποίησης), είναι πιθανό να καθυστερήσουν τα επόμενα βήματα τα οποία είναι και πιο περίπλοκα από την σχετικά απλή διαδικασία απόκτησης και δημιουργίας των αρχείων καταγραφής. Επομένως, χρειάζεται ένα σύστημα *Tunneling and Authentication* (*Tp*) που να βασίζεται σε ένα ασφαλές πρωτόκολλο επικοινωνίας όπως το *ISO/OSI* επιπέδου 3.



Σχήμα 23: Συσχετισμός κανονικοποιημένων γεγονότων

3.6.4.2 Ερμηνεία των Αρχείων Καταγραφής

Συνήθως, όταν ένας διαχειριστής ασφάλειας διαβάζει το αποτέλεσμα ενός συσχετισμού που εκτελέστηκε από ένα συγκεκριμένο εργαλείο, μπορούμε να πούμε ότι βλέπει μόνο την κορυφή του παγόβουνου. Υπάρχει ένα πολύ περίπλοκο σύνολο διαδικασιών στο

γραφικό περιβάλλον χρήστη (*Graphical User Interface, GUI)*. Υπάρχουν δύο βασικές προσεγγίσεις στην ανάλυση των αρχείων καταγραφής.

Προσέγγιση από Πάνω προς τα Κάτω

'Ενας δικανικός ερευνητής ο οποίος δουλεύει με ένα αυτοματοποιημένο εργαλείο καταγραφής και συσχετισμού γεγονότων συνήθως χρησιμοποιεί αυτή την προσέγγιση. Κατά τη διάρκεια ανίχνευσης μιας εισβολής, η προσέγγιση από πάνω προς τα κάτω σημαίνει ότι ξεκινάμε από την επίθεση και ακολουθούμε τα ίχνη προς τα πίσω δηλαδή προς την πηγή της επίθεσης. Στη δικανική ανάλυση δικτύων, σημαίνει ότι ξεκινάμε από την οθόνη *GUI* του γεγονότος και πηγαίνουμε προς το αρχείο πηγής με σκοπό:

- Να επικυρωθεί η διαδικασία συσχετισμού που χρησιμοποιήθηκε από το αυτοματοποιημένο εργαλείο καταγραφής και συσχετισμού γεγονότων,
- Να βρεθούν τα αρχεία καταγραφής πηγής που θα χρησιμοποιηθούν σαν αποδείξεις στις δικαστικές αρχές ή για περαιτέρω ανάλυση.

Το ***σχήμα 23*** αντιπροσωπεύει μια προσέγγιση από πάνω προς τα κάτω, ώστε να φτάσουμε στα αρχεία πηγής. Όταν ανιχνευθούν, τα αρχεία καταγραφής εγγράφονται σε *CD-ROM* ή σε *DVD*, και ο χρήστης τους αποδίδει μια ψηφιακή υπογραφή.

Προσέγγιση από Κάτω προς τα Πάνω

Αυτή η προσέγγιση εφαρμόζεται από ένα εργαλείο ξεκινώντας από το αρχείο πηγής ώστε να φτάσουμε στο επίπεδο παρουσίασης της διαδικασίας έρευνας. Ένα σύστημα ανίχνευσης εισβολής (*IDS*) ακολουθεί αυτή την προσέγγιση για να αναγνωρίσει μια επίθεση που εξελίσσεται μέσω μιας ανάλυσης γεγονότων σε πραγματικό χρόνο. Σε ένα περιβάλλον κατανεμημένης ασφάλειας η μηχανή *IDS* μπορεί να βρίσκεται στην ίδια μηχανή που βρίσκεται και η μηχανή κανονικοποίησης. Στην περίπτωση αυτή, η μηχανή *IDS* θα χρησιμοποιήσει το εργαλείο δικανικής ανάλυσης του δικτύου για να εμφανίσει το πρόβλημα στο *GUI*.

Αυτή η προσέγγιση χρησιμοποιείται, όταν η ανάλυση των αρχείων και ο συσχετισμός γίνεται χωρίς τη χρήση αυτοματοποιημένων εργαλείων. Σε αυτή την περίπτωση χρησιμοποιούνται διαπεραστές των αρχείων καταγραφής (*log parsers)* για να αναλύσουν τα αρχεία πηγής στο συσχετισμό από κάτω προς τα πάνω. Ο διαπεραστής συνήθως είναι γραμμένος σε μια γλώσσα όπως *Perl* ή *Python*, αν και υπάρχουν και διαπεραστές γραμμένοι σε *Java* που επιτρέπουν προσέγγιση που διασχίζει τις πλατφόρμες.

3.6.5 Προϋποθέσεις των Εργαλείων Απόκτησης των Αρχείων Καταγραφής

Για να εξασφαλιστούν συσχετισμοί συνεπείς με τις δικανικές απαιτήσεις, η υποδομή της διαδικασίας καταγραφής θα πρέπει να ικανοποιεί τις παρακάτω προϋποθέσεις:

- Υποστήριξη *TCPdump* και στην είσοδο και στην έξοδο,
- Σύγχρονοι αλγόριθμοι κατακερματισμού (*hash algorithms*),
- Δυνατότητες μείωσης των δεδομένων,
- Ανακατασκευή δεδομένων: εξαγωγή των συνδέσεων και του ωφέλιμου φορτίου από κίνηση που ανακόπτεται για την ερμηνεία της μορφοποίησης των αρχείων που εμπλέκονται στη σύνοδο *(transaction),*
- Συγκεκαλυμμένη δυνατότητα αναγνώρισης καναλιών (όχι απαραίτητη),

- Δυνατότητα μόνο ανάγνωσης κατά τη διάρκεια συλλογής και εξέτασης: Αυτό αποτελεί μια απαραίτητη λειτουργικότητα για τον τύπο του εργαλείου.
- Πλήρης συλλογή: Αποτελεί μια από τις πιο σημαντικές προϋποθέσεις. Όλα τα πακέτα θα πρέπει να συλλεχθούν ή τουλάχιστον όλες οι απώλειες θα πρέπει να ελαχιστοποιηθούν και να καταγραφούν.
- Ουσιαστική ασφάλεια ειδικά για τις συνδέσεις μεταξύ των σημείων των αποκτήσεων, των αποθηκών των συλλογών, των χρηστών διαχείρισης κ.α.

3.6.6 Η Χρήση Εργαλείων *GPL (General Public License)* για Έρευνα και Συσχετισμό

Υπάρχει ένας αριθμός εργαλείων *GPL (General Public License)* που παρέχουν τα βασικά για την χρήση της τεχνικής από κάτω προς τα πάνω. Η προσέγγιση αυτή είναι πιο απλή και λιγότερο δαπανηρή από την προσέγγιση από πάνω προς τα κάτω που βασίζεται σε τεχνικές αυτοματοποιημένου συσχετισμού και προβολής σε *GUI*. Κάποια από αυτά τα εργαλεία και τα αντίστοιχα έργα (*projects*) θα αναλυθούν πιο κάτω.

3.6.6.1 Το *IRItaly Project*

Το *IRItaly (Incident Response Italy)* είναι ένα έργο που αναπτύχθηκε στο Πανεπιστήμιο του Μιλάνο. Το έργο αφορά πληροφορίες επιθέσεων, αμυντικά συστήματα, δικανικές αναλύσεις υπολογιστών και δικτύων και μεθόδους ανάκτησης των δεδομένων. Ο βασικός σκοπός του έργου είναι να ενημερώσει και να ευαισθητοποιήσει την επιστημονική κοινότητα και τις επιχειρήσεις της Ιταλίας, όπως και τους ιδιωτικούς και δημόσιους οργανισμούς σχετικά με τα ζητήματα απόκρισης σε περιστατικά εισβολής και επίθεσης.

Είναι οργανωμένο σε δύο τμήματα, όπου το ένα τμήμα παρέχει λεπτομερείς οδηγίες και καθοδήγηση και το άλλο παρέχει ένα *bootable CD-ROM*. Οι καλύτερες πρακτικές απόκρισης σε περιστατικά παρουσιάζονται για να αναλύσουν τις μηχανές στόχους και να ανακατασκευάσουν τον τρόπο που έγινε η επίθεση. Ο τελικός σκοπός ασφαλώς, είναι να προμηθεύσει μεθόδους για οχύρωση του συστήματος και αποφυγή μελλοντικών επιθέσεων.

Όλες οι λειτουργίες έχουν σχεδιαστεί με ιδιαίτερη προσοχή για να καταγράφουν τις μεθόδους αναγνώρισης και αποθήκευσης ώστε να ισχυροποιήσουν την αξιοπιστία τους ως αποδεικτικά στοιχεία. Το *CD-ROM* παρέχει ένα σύνολο δραστηριοτήτων για να αναλάβει δράση ως απάντηση σε μια εισβολή, μαζί με μια λεπτομερή ανάλυση των εξής στοιχείων:

- Προετοιμασία της απάντησης σε μια εισβολή,
- Ανάλυση της διαθέσιμης πληροφορίας που σχετίζεται με την εισβολή,
- Συλλογή και αποθήκευση πληροφορίας (αποδείξεων),
- Ελαχιστοποίηση των ενδιάμεσων εργαλείων (*rootkit*), τα οποία χρησιμοποιούνται για να πετύχουν παράνομη πρόσβαση σε μια μηχανή,
- Αποκατάσταση της λειτουργίας των συστημάτων στις κανονικές συνθήκες λειτουργίας.

Επιπλέον, παρέχεται λεπτομερής πληροφορία σχετικά με:

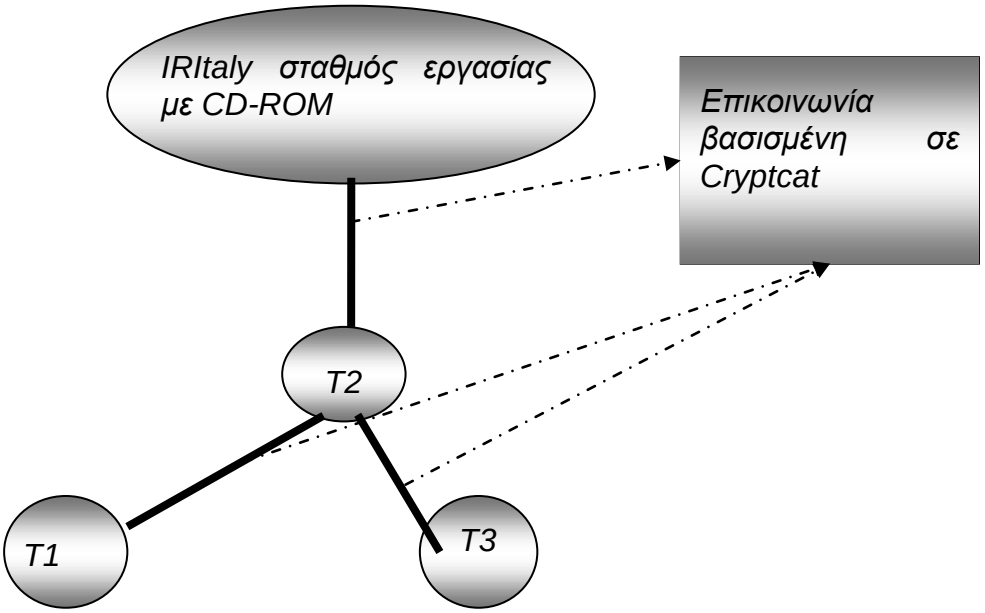
- Διαχείριση των διαφορετικών συστημάτων αρχείων,
- Διαδικασίες ανάκτησης δεδομένων,

- Αντιγραφή με απεικόνιση των δίσκων του συστήματος,
- Ασφαλείς ηλεκτρονικές επικοινωνίες,
- Αλγόριθμους κρυπτογράφησης,
- Εργαλεία απόκτησης, ανάλυσης και ασφαλούς αποθήκευσης των αρχείων καταγραφής.

Το *CD* επίσης παρέχει ένα μοντέλο για αναφορά του περιστατικού και όλες τις φόρμες για τη σημαντική αλυσίδα επιτήρησης *(chain of custody),* για να βελτιώσει την οργάνωση και να διευκολύνει τις αλληλεπιδράσεις μεταξύ των οργανισμών που εμπλέκονται στην ανάλυση του περιστατικού.

Το *CD-ROM* του *IRItaly* έργου, μπορεί να χρησιμοποιηθεί για να φέρει εις πέρας έναν αρχικό έλεγχο του υπολογιστή στόχου. Περιλαμβάνει εργαλεία για την ανάλυση δίσκων, τη δημιουργία εικόνων αντιγράφων των δίσκων και για τον έλεγχο των αρχείων καταγραφής. Μετά την εκκίνηση (*booting*) του *CD-ROM*, εγκαθίσταται μια διεπαφή τερματικού την οποία ο εξεταστής μπορεί να χρησιμοποιήσει για να εκκινήσει συγκεκριμένες εφαρμογές των *TCPDump, Ethereal, Snort, Swatch* κ.α.

Η διαδικασία συσχετισμού περιλαμβάνει την σύγκριση των αρχείων καταγραφής που βρίσκονται στον υπολογιστή στόχο με αυτά που βρίσκονται σε άλλες μηχανές. Σε αυτή την περίπτωση, το *CD* λειτουργεί αποτελεσματικά σε πολύ μικρά περιβάλλοντα ή ακόμα και σε περιπτώσεις πλαισίου ένα-προς-ένα, όπως φαίνεται και στο παρακάτω ***σχήμα.***



Σχήμα 24: Χρήση του *IRItaly CD-ROM*

Στο σχήμα αυτό τα *T1, T2* και *T3* αποτελούν στόχους που πρέπει να εκκινηθούν με το *CD* και να συνδεθούν με το βασικό σταθμό εργασίας της δικανικής ανάλυσης μέσω *Netcat* ή *Cryptcat*. Ο μόνος περιορισμός του *CD* είναι ότι δεν μπορεί να χρησιμοποιηθεί σε κατανεμημένες αρχιτεκτονικές. Ωστόσο, όπως θα αναφέρουμε πιο κάτω, γίνεται έργο

για την ανάπτυξη μιας νέας έκδοσης του *CD* με επιπλέον εργαλεία που θα ξεπεράσουν έναν αριθμό από περιορισμούς.

3.6.6.2 Νεότερες Αναπτύξεις: Η έκδοση 2 του έργου *IRItaly*

Η νέα έκδοση του *CD-ROM* λύνει κάποιους περιορισμούς της παλιάς έκδοσης και περιέχει πλήρη εφαρμογή του νέου *Python FLAG*.

Το αρχικό *FLAG* είχε σχεδιαστεί για να απλοποιεί τη διαδικασία της ανάλυσης των αρχείων καταγραφής και τις δικανικές έρευνες. Οι μεγάλες υποθέσεις συνήθως σημαίνουν πάρα πολλά δεδομένα που θα πρέπει να αναλυθούν και να συσχετιστούν. Το *FLAG* χρησιμοποιεί μια βάση δεδομένων σαν *backend* ώστε να χειριστεί τον μεγάλο όγκο των δεδομένων.

Επειδή το *FLAG* είναι βασισμένο στο *web*, μπορεί να αναπτυχθεί σε έναν εξυπηρετητή και να το μοιραστούν πολλοί χρήστες. Τα δεδομένα είναι οργανωμένα για την καλύτερη λειτουργία. Επίσης χρησιμοποιούνται «σελιδοδείκτες» (*bookmarks*) ώστε να γίνονται καλύτερα η οργάνωση και η αναφορά των ευρημάτων.

Το *FLAG* ξεκίνησε σαν έργο από το Υπουργείο Άμυνας της Αυστραλίας. Το *PyFLAG* είναι η *Python* ανάπτυξη του *FLAG*, που αποτελεί μια από την αρχή ανάπτυξη του *FLAG* σε μια αποτελεσματικότερη γλώσσα προγραμματισμού. Μερικές από τις λειτουργικότητες που προστέθηκαν στην πρώτη έκδοση είναι:

Δικανικές αναλύσεις δίσκων

- Υποστήριξη *NTFS, Ext2, FFS, FAT,*
- Υποστήριξη πολλών διαφορετικών μορφοποιήσεων αρχείων περιλαμβανομένων των συμπιεσμένων μορφών, όπως και τα παραδοσιακά *dd* αρχεία,
- Προηγμένη επισήμανση χρόνου για πολύπλοκες αναζητήσεις,
- Υποστήριξη της λειτουργίας κατακερματισμού *NSRL (National Software Reference Library)* για γρήγορη αναγνώριση αρχείων,
- Υποστήριξη των *Windows*, των διάφορων εκδόσεων του *win98* όπως και της έκδοσης *Windows NT*,
- Δυνατότητα αναδόμησης των αρχείων από κατεστραμμένες εικόνες αρχείων.

Δικανικές αναλύσεις δικτύων

- Αποθήκευση της κίνησης ενός *tcpdump* σε μια βάση *SQL*,
- Εκτέλεση πλήρους αναδόμησης μιας ακολουθίας *TCP*,
- Δυνατότητα δημιουργίας ενός διαγράμματος δικτύου βασισμένου στο *TCPDump*, σε πραγματικό χρόνο.

Ανάλυση αρχείων καταγραφής

- Επιτρέπει σε αρχεία καταγραφής με τυχαίες μορφοποιήσεις να μπορούν να φορτωθούν στη βάση δεδομένων με ευκολία,
- Παρέχει μια προηγμένη μορφή *GUI*,

Επίσης η νέα έκδοση του *CD-ROM* περιέχει νέες δυνατότητες ανάλυσης των αρχείων καταγραφής με τη μορφή *SecSyslog*. Το *SecSyslog* παρουσιάζει προβλήματα ακεραιότητας. Η ακεραιότητα μπορεί να παραβιαστεί όταν δεν γίνεται αυθεντικοποίηση

μεταξύ των μηχανών, όταν γίνονται απάτες με διευθύνσεις ή όταν υποκλέπτεται κίνηση στο δίκτυο. Το *SecSyslog* αναζητεί μια λύση σε αυτό το πρόβλημα μέσω της χρήσης των συγκαλυμμένων καναλιών *(covert channels*):

- Χρησιμοποιεί *TCP* μαζί με τη χρήση του απλού και επαρκούς *UDP* για να εγκαταστήσει τη σύνδεση μεταξύ των μηχανών,
- Τα πακέτα του *SecSyslog* είναι κρυπτογραφημένα και έγκλειστα μέσα στα *UDP* πακέτα. Έτσι όταν κάποιος υποκλέπτει την μετάδοση δεν μπορεί να καταλάβει τι είδους κίνηση περνάει στη γραμμή,
- Μόλις φτάσουν στον προορισμό τους, τα πακέτα *SecSyslog* αποκρυπτογραφούνται από τον *SecSyslog* daemon και τα μηνύματα αναλύονται.

Το *SecSyslog* μπορεί να λύσει κάποια προβλήματα ακεραιότητας και εμπιστευτικότητας που σχετίζονται με την έλλειψη ασφάλειας και δικανικής συμμόρφωσης σε πολλές αρχιτεκτονικές καταγραφής αρχείων.

3.6.7 *SecSyslog* και Συγκαλυμμένα Κανάλια

Σύμφωνα με τον ορισμό, ένα ***συγκαλυμμένο κανάλι είναι οποιοδήποτε τηλεπικοινωνιακό κανάλι που μπορεί να χρησιμοποιηθεί για να μεταδώσει πληροφορία χρησιμοποιώντας μεθόδους που παραβιάζουν τις υπάρχουσες πολιτικές ασφάλειας*.**

Ένας άλλος ορισμός περιγράφει ένα συγκαλυμμένο κανάλι σαν ***μια οποιαδήποτε μέθοδο που επιτρέπει την μετάδοση της πληροφορίας μέσω μιας ή περισσότερων μεταβλητών συστήματος που δεν είναι όμως σχεδιασμένες γι' αυτό το σκοπό.***

3.6.7.1 Κατηγορίες

Τα συγκαλυμμένα κανάλια μπορούν να χωριστούν σε δύο βασικές κατηγορίες: ***κανάλια αποθήκευσης*** *(storage channels*) και ***κανάλια χρονοδιαγράμματος*** *(timing channels*). Ο σκοπός τους βασικά είναι ο ίδιος και διαφέρουν μόνο στον τρόπο με τον οποίο είναι διαθέσιμη η πληροφορία. ***Η πρώτη κατηγορία*** χρησιμοποιεί μια καθολική μεταβλητή *(global variable*) που δρα σαν ένα κανάλι μετάδοσης στο οποίο ένα από τα δύο μέρη που θέλουν να επικοινωνήσουν μπορούν να κάνουν αλλαγές οι οποίες διαβάζονται από το άλλο μέρος. Αυτή η μεταβλητή μπορεί να είναι μια περιοχή μνήμης για ειδικούς *IT*. ***Η άλλη κατηγορία*** μας επιτρέπει να μεταδώσουμε πληροφορία διαμορφώνοντας τη χρήση ειδικών πόρων του συστήματος (χρόνος *CPU*, παραλαβή ενός πακέτου και απόκριση κ.α.), έτσι ώστε να εκμεταλλευτούν τις διαφορές από την κανονική λειτουργία σαν ένα μέσο κωδικοποίησης της μεταδιδόμενης πληροφορίας. Υβριδικά συγκαλυμμένα κανάλια που συνδυάζουν και τις δύο κατηγορίες είναι πιθανό να κάνουν ένα κανάλι ακόμα πιο δύσκολο να ανιχνευθεί.

Ενώ παλιότερα η έρευνα για τα συγκαλυμμένα κανάλια εστίαζε στη ροή της πληροφορίας μεταξύ διαφορετικών διεργασιών στο ίδιο σύστημα, το ενδιαφέρον έχει τώρα μετατοπιστεί στην πληροφορία που στέλνεται από τον ένα υπολογιστή στον άλλο χρησιμοποιώντας τα νεώτερα πρωτόκολλα δικτύου και το διαδίκτυο.

3.6.7.2 Η χρήση των συγκαλυμμένων καναλιών δικτύων

Τα πρωτόκολλα *TCP/IP* προσφέρουν πολλούς τρόπους για την δημιουργία συγκαλυμμένων καναλιών και για να μεταφέρουν δεδομένα μεταξύ υπολογιστών ώστε:

- Να αποφύγουν συσκευές ασφάλειας που έχουν εγκατασταθεί περιμετρικά στο δίκτυο,
- Να αποφύγουν τους *sniffers* δικτύου,
- Να συμπυκνώσουν πληροφορία, κρυπτογραφημένη ή μη, μέσα σε κανονικά πακέτα για μυστική μετάδοση σε δίκτυα τα οποία απαγορεύουν τέτοια συμπεριφορά.

Θα παρουσιάσουμε τεχνικές παραποίησης των κεφαλίδων *TCP/IP*, όπως και τεχνικές που χρησιμοποιούνται σε *επίπεδο ICMP (Internet Control Message Protocol*) και σε υψηλότερα επίπεδα όπως *το HTTP (Hyper Text Transfer Protocol*) και το *DNS (Domain Name Service).*

3.6.7.2.1 Κωδικοποίηση Πληροφορίας στις κεφαλίδες IP/TCP

Οι κεφαλίδες *TCP* και *IP* παρέχουν πολλά πεδία στα οποία η πληροφορία μπορεί να μεταφερθεί μυστικά. Στο ***σχήμα 25***, παρουσιάζεται η μορφή της κεφαλίδας για το πρωτόκολλο *IP*.

0	***4***	***8***	***16***	***19***	***24***	***32***
VERS | ***HLEN*** | ***Service Type*** |				***Total Length***		
Identification			| ***Flags*** |		***Fragment Offset***	
Source IP Address						
Destination IP Address						
IP Options					| ***Padding***	
Data						

Σχήμα 25: Κεφαλίδα πρωτοκόλλου *IP*

Στην περίπτωση αυτή το μόνο πεδίο που μπορεί να χρησιμοποιηθεί για να συστήσει ένα συγκαλυμμένο κανάλι που δεν θα ανιχνευτεί εύκολα, είναι το ***πεδίο Αναγνώρισης*** *(Identification field).*

Η κεφαλίδα του πρωτοκόλλου *TCP* ***(σχήμα 26)*** παρέχει αρκετές δυνατότητες, αλλά και πάλι το συγκαλυμμένο κανάλι θα είναι συγκαλυμμένο μόνο αν είναι δύσκολο να ανιχνευθεί, και έτσι το καλύτερο πεδίο που μπορούμε να χρησιμοποιήσουμε γι' αυτό το λόγο είναι το πεδίο ***Αριθμός Ακολουθίας*** (*Sequence Number, SN*). Το πεδίο *SN* μπορεί να χρησιμοποιηθεί *ως Initial Sequence Number* ή ως *Acknowledgement Sequence Number.*

0	***4***	***8***	***16***	***19***	***24***	***32***
Source Port			***Destination Port***			
Sequence Number						
Acknowledgement Number						
HLEN	***Reserved***		***Code Bits***		***Window***	
Checksum				***Urgent Pointer***		
Options				***Padding***		
Data						

Σχήμα 26: Κεφαλίδα πρωτοκόλλου *TCP*

3.6.7.2.2 Η παραποίηση του πεδίου Identification (IP πρωτόκολλο)

Το ***πεδίο ID*** *(Identification)* του *IP* πρωτοκόλλου περιέχει μια μοναδική τιμή ώστε οι δρομολογητές και οι υπολογιστές να μπορούν να επανασυναρμολογήσουν τα κατακερματισμένα πακέτα που λαμβάνουν. Αυτό το πεδίο μπορεί να παραποιηθεί αντικαθιστώντας μια τιμή (π.χ. μια *ASCII* τιμή) στο *ID* πεδίο που περιέχει κωδικοποιημένη πληροφορία. Ο μηχανισμός μετάδοσης δεν αλλάζει σε καμία περίπτωση και ο παραλήπτης αρκεί να διαβάσει το *ID* πεδίο και να χρησιμοποιήσει έναν αλγόριθμο αποκωδικοποίησης για να μεταφράσει το πεδίο στην τιμή *ASCII* που ο αποστολέας ήθελε να στείλει.

Αυτή η μέθοδος χρησιμοποιεί ειδικά γι' αυτό το σκοπό ένα πλαστό πακέτο με σωστά πεδία προορισμού και πηγής και την κωδικοποιημένη μορφή στο πεδίο *ID*. Ο απομακρυσμένος χρήστης λαμβάνει τα δεδομένα «ακούγοντας» την θύρα 80 με έναν δαίμονα που μπορεί να ξεχωρίσει τα συγκαλυμμένα πακέτα από τα κανονικά *HTTP* πακέτα, να αποκωδικοποιήσει τα πρώτα και να στείλει τα δεύτερα στον εξυπηρετητή *web*.

Αυτή η μέθοδος είναι αρκετά αξιόπιστη και εύκολη στην υλοποίηση, παρόλο που υπάρχει κίνδυνος να αποτύχει αν υπάρχει τείχος προστασίας (*firewall*) ή μετάφραση διευθύνσεων δικτύου *(Network Address Translation, NAT*) μεταξύ των δύο υπολογιστών.

3.6.7.2.3 Η Μέθοδος Initial Sequence Number (ISN)

Στο πρωτόκολλο *TCP* η τιμή του *Initial Sequence Number* εγγυάται την αξιοπιστία και τον έλεγχο της ροής των δεδομένων. Κάθε *byte* που μεταδίδεται από την ροή των *TCP* δεδομένων έχει έναν εκχωρημένο αριθμό ακολουθίας. Κάθε σύνδεση (κάθε συνδεδεμένο ζευγάρι *sockets*) μπορεί να χρησιμοποιηθεί από τις ροές και όσο πιο αξιόπιστος είναι ο αλγόριθμος υπολογισμού του *ISN* τόσες περισσότερες ροές είναι διαθέσιμες. Όταν δημιουργηθεί η σύνδεση, ο υπολογιστής πελάτης (*client host*) θα πρέπει να καθορίσει την τιμή του *ISN* και να εκκινήσει την τρίδρομη χειραψία (*three way handshake)*.

Το πεδίο *ISN* είναι ιδανικό για μετάδοση μυστικής πληροφορίας, εξ αιτίας του μεγέθους του (32 *bits*). Οι αλγόριθμοι υπολογισμού του *ISN* μπορούν να χρησιμοποιηθούν έτσι ώστε με 32 *bits* διαθέσιμα, να μπορούν να παραχθούν περισσότερα διασπαρμένα αποτελέσματα και να κάνουν το συγκαλυμμένο κανάλι δύσκολο να ανιχνευθεί.

3.6.7.2.4 Η Μέθοδος Acknowledge Sequence Number (ASN)

Αυτή η μέθοδος βασίζεται στην εξαπάτηση του *IP* ώστε να επιτρέψει στον αποστολέα να προωθήσει ένα πακέτο από έναν απομακρυσμένο εξυπηρετητή προς το σωστό προορισμό. Η τεχνική αυτή ξεγελάει τον παραλήπτη ώστε να νομίζει ότι ο εξυπηρετητής από τον οποίο ήρθε το πακέτο είναι η πραγματική πηγή. Έτσι η πραγματική πηγή παραμένει ανώνυμη. Αυτός ο τύπος συγκαλυμμένου καναλιού είναι πολύ δύσκολο να ανιχνευθεί, ειδικά αν ο εξυπηρετητής που στέλνει τα πακέτα είναι υπερφορτωμένος.

Αυτή η τεχνική εκμεταλλεύεται μια λειτουργικότητα των πρωτοκόλλων *TCP/IP* με την οποία ο εξυπηρετητής προορισμού απαντά στο αίτημα σύνδεσης στέλνοντας ένα πακέτο με ένα *ISN* αυξημένο κατά μία μονάδα. Ο αποστολέας πρέπει να στείλει ένα ψεύτικο πακέτο και να έχει αλλάξει τα παρακάτω πεδία:

- Το *IP* πηγής,
- Τη θύρα πηγής,
- Το *IP* προορισμού,
- Τη θύρα προορισμού,
- Το *ISN* με τα κωδικοποιημένα δεδομένα.

Η επιλογή των θυρών πηγής και προορισμού είναι εντελώς τυχαία. Το *IP* προορισμού θα πρέπει να είναι αυτό του εξυπηρετητή που προωθεί το πακέτο και το *IP* πηγής να είναι του υπολογιστή προορισμού. Έτσι το πακέτο στέλνεται από τον πελάτη στον εξυπηρετητή που θα το προωθήσει, ο οποίος το προωθεί στη μηχανή προορισμού (με το *ISN* αυξημένο κατά μία μονάδα), η οποία θα το αποκωδικοποιήσει.

Ένας καλά ρυθμισμένος δρομολογητής ή ένα τείχος προστασίας δεν θα πρέπει να επιτρέψει να περάσει ένα πακέτο με ενεργό *ACK flag*, εκτός και αν αναγνωρίζει ότι ο υπολογιστής προορισμού είναι υπεύθυνος για την εγκαθίδρυση της σύνδεσης.

3.6.7.2.5 Συγκαλυμμένα Κανάλια με τη χρήση ICMP Tunnel

Αν και η τεχνική αυτή αναπτύχθηκε το 1996, πολλά συστήματα ακόμα και σήμερα είναι ευπαθή σε συγκαλυμμένα κανάλια που χρησιμοποιούν *ICMP*. Η μόνη απαίτηση είναι να επιτρέπει το σύστημα την κίνηση *ICMP_ECHO*.

Πολλοί θεωρούν την κίνηση *ICMP* καλοήθη, και αυτό ισχύει γιατί ο σκοπός της είναι να αναφέρει προβλήματα παράδοσης. Τα πακέτα *ICMP* είναι ενθυλακωμένα σε *IP* δεδομενογράμματα (*datagrams*). Τα πρώτα 32 *bits* της κεφαλής του *ICMP* πακέτου είναι πάντοτε τα ίδια και η υπόλοιπη κεφαλή μπορεί να περιέχει οποιονδήποτε από 15 διαφορετικούς τύπους μηνύματος που επιτρέπονται από το πρωτόκολλο.

Τα μηνύματα *ICMP* που είναι ευπαθή στο να χρησιμοποιηθούν σαν συγκαλυμμένα κανάλια είναι τα *ICMP_ECHO* (ερώτηση) και *ICMP_ ECHOREPLY* (απάντηση). Εφόσον μπορούμε να στείλουμε ερωτήσεις και να πάρουμε απαντήσεις, το πρωτόκολλο είναι ένα πιθανό όχημα για κρυμμένες ακολουθίες δεδομένων. Η λειτουργικότητα *ping*, για παράδειγμα στέλνει και παίρνει μόνο τέτοια μηνύματα.

Τα μηνύματα *ICMP_ECHO* επιτρέπουν την εισαγωγή πληροφορίας στο πεδίο δεδομένων *(data field)*, που συνήθως κρατάει πληροφορία για το χρόνο καθυστέρησης. Ωστόσο το πεδίο δεδομένων δεν ελέγχεται από κάποια συσκευή και μπορεί να χρησιμοποιηθεί για να στείλει τυχαία δεδομένα, δημιουργώντας έτσι ένα συγκαλυμμένο κανάλι.

3.6.7.2.6 HTTP/S Tunnel

Υπάρχουν διάφοροι τρόποι για να σχεδιάσουμε ένα συγκαλυμμένο κανάλι βασισμένο σε *HTTP*. Ένας τρόπος είναι να εξετάσουμε τι τύπος εξυπηρετητή θα υλοποιηθεί (*http daemon, proxy* ή *CGI*), πώς θα πρέπει να χειριστούμε την κίνηση για να επιτύχουμε τη μεταμφίεση του καναλιού (αλυσίδες *proxy*, δημιουργία θορύβου κ.α.) ή τι είδους λειτουργίες χρειάζονται. Αφού εξεταστούν αυτά τα θέματα, επιλέγουμε τη μέθοδο που θα χρησιμοποιήσουμε (*GET, CONNET, POST…)* και τον τρόπο που θα εφαρμόσουμε το μοντέλο στην πράξη.

Όπως με κάθε συγκαλυμμένο κανάλι, οι στεγανογραφικές και κρυπτογραφικές τεχνικές είναι επίσης χρήσιμες για να δημιουργήσουν επιπλέον σύγχιση σε όποιον παρατηρεί την κίνηση.

Αυτά τα κανάλια απαιτούν γενικά δύο συγχρονισμένες οντότητες. Μία μέσα στο δίκτυο στόχο και μία άλλη έξω από αυτό. Ο εξωτερικός εξυπηρετητής θα πρέπει να είναι προσβάσιμος εκ των έσω και όταν προσπελαύνεται δεν θα πρέπει να δημιουργεί υποψίες κάποιου μηχανήματος ελέγχου, αυτοματοποιημένου ή μη. Ο εξυπηρετητής θα πρέπει να ενεργεί σαν να είναι ικανός να χειριστεί τις *HTTP* αιτήσεις και ο πελάτης θα πρέπει να στέλνει κατάλληλα κωδικοποιημένη πληροφορία με το πρόσχημα των κανονικών *HTTP* αιτήσεων.

Επομένως τα συγκαλυμμένα κανάλια που βασίζονται σε *HTTP* μπορούν να πάρουν μια μεγάλη ποικιλία φορμών, γεγονός που τα κάνει ένα ελκυστικό όχημα για όσους θέλουν να αποκρύψουν αθέμιτη κίνηση.

Πολλά εργαλεία ανοιχτού και κλειστού λογισμικού, χρησιμοποιούν τα *HTTP* κανάλια για διάφορους σκοπούς. Για παράδειγμα, εργαλεία που έχουν σχεδιαστεί για να ανιχνεύσουν ένα κλεμμένο υπολογιστή μόλις αυτός συνδεθεί στο δίκτυο, μπορούν να στείλουν την πληροφορία θέσης αθέατα μέσω μηνύματος ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας ένα *HTTP* κανάλι. Το πρωτόκολλο *SOAP* (*Simple Object Access Protocol*) και η *Remote Procedure Call (RPC)* πάνω σε *HTTP*, βασίζονται σε *HTTP* κανάλια.

3.6.7.2.7 DNS (Domain Name System)

Η πιθανότητα χρήσης κανονικών αιτήσεων/απαντήσεων *DNS* για τη μετάδοση των δεδομένων έχει κινήσει το ενδιαφέρον τα τελευταία χρόνια.

Το *DNS* χρησιμοποιεί ένα ιεραρχικό σύστημα ονοματοδοσίας *(.com, .bar.com, .foo.bar.com)* και αυτό είναι πολύ χρήσιμο. Αν μπορέσουμε να ελέγξουμε έναν εξυπηρετητή *DNS* με την χρήση ενός συγκεκριμένου ονόματος *domain*, μπορούμε να αλλάξουμε τους πίνακες που παρέχουν την απαραίτητη πληροφορία για την ικανοποίηση των αιτήσεων των πελατών. Μπορούμε τότε να δημιουργήσουμε ένα συγκαλυμμένο κανάλι χρησιμοποιώντας κάποια πεδία από τον πίνακα *DNS*. Με αυτό τον τρόπο κερδίζουμε αρκετό εύρος ζώνης *(bandwidth).* Χρησιμοποιώντας το πεδίο *CNAME* για να κωδικοποιήσουμε μεταδιδόμενη πληροφορία, μπορούμε να στείλουμε και να πάρουμε μέχρι 110 *bytes* ανά πακέτο, ενώ με τη χρήση του πεδίου *TXT*

κερδίζουμε 220 *bytes* ανά πακέτο. Πρόκειται για ένα πολύ μεγάλο όγκο δεδομένων συγκρίνοντας με αυτά που έχουμε στις κεφαλίδες *TCP* και *IP*.

Το πρωτόκολλο *DNS* είναι παρόμοιο σε πολλούς τρόπους με το *HTTP*:

- Λειτουργεί σε κομμάτια (*blocks*) από δεδομένα,
- Δεν κάνει τίποτα μέχρι να πάρει μια αίτηση από τον πελάτη,
- Λειτουργεί σε *set* χαρακτήρων (*Base32/Base64*)

Πολλά εργαλεία έχουν αναπτυχθεί για την εκμετάλλευση *HTTP* καναλιών. Δεδομένων των ομοιοτήτων μεταξύ *DNS* και *HTTP*, υπάρχουν πολλοί τρόποι για τη χρήση του *DNS*. Αντίστοιχα, μπορούν να χρησιμοποιηθούν και πολλά εργαλεία που χρησιμοποιούν *HTTP*.

Θα πρέπει να αναφέρουμε ότι ενώ τα πρώτα εργαλεία φιλτραρίσματος είναι διαθέσιμα για το *HTTP* καθώς και για άλλα πρωτόκολλα, δεν ισχύει το ίδιο για το *DNS*. Επίσης, η έντονη κίνηση στο *DNS* είναι δυνατό να τραβήξει την υποψία και αυτή η πιθανότητα μόνο εν μέρει αντισταθμίζεται από το υψηλό εύρος ζώνης που προσφέρει η μέθοδος. Έτσι είναι περισσότερο αποτελεσματικό να χρησιμοποιήσουμε ένα *HTTP* κανάλι όταν δεν υπάρχουν ιδιαίτερες απαιτήσεις για εύρος ζώνης.

3.6.8 Επίλογος

Σε αυτό το κεφάλαιο παρουσιάστηκε ο συσχετισμός των αρχείων καταγραφής και των γεγονότων. Για να υπάρχει συμμόρφωση με τις γενικές αρχές της ψηφιακής δικανικής ανάλυσης, τα εργαλεία που χρησιμοποιούνται θα πρέπει να ικανοποιούν κάποιες προϋποθέσεις. Το *project IRItaly* αναπτύσσεται προς αυτή την κατεύθυνση. Το πιο σημαντικό πρόβλημα προς επίλυση σχετίζεται με τον τρόπο αντιμετώπισης των κατανεμημένων αρχιτεκτονικών, και ειδικότερα με τις προσεγγίσεις ***από πάνω προς τα κάτω*** και ***από κάτω προς τα πάνω***. Για την ώρα, υπάρχει ένα κενό μεταξύ των δύο προσεγγίσεων. Ο σκοπός είναι να δοθεί αυτονομία στους διαχειριστές οι οποίοι δεν μπορούν να επενδύσουν μεγάλα ποσά σε πολύπλοκα κατανεμημένα συστήματα. **[12]**

3.7 Η Πολιτική Ασφάλειας, η Διατήρηση της Ετοιμότητας και η Απάντηση στις Ηλεκτρονικές Επιθέσεις

Στις 12 Απριλίου 2005, η εταιρεία LexisNexis διαπίστωσε ότι υπήρχαν ενδείξεις κλοπής από τις βάσεις δεδομένων της, των προσωπικών πληροφοριών περίπου 310.000 κατοίκων των ΗΠΑ. Η εταιρεία είχε ανακοινώσει από το Μάρτιο του ίδιου έτους ότι είχαν κλαπεί πληροφορίες για περίπου 30.000 άτομα, αλλά μια εσωτερική έρευνα αύξησε κατά πολύ αυτό τον αριθμό. Η εταιρεία ενημέρωσε μέσω του ηλεκτρονικού ταχυδρομείου τα άτομα, ότι υπήρχε η ένδειξη κλοπής των προσωπικών τους δεδομένων από αγνώστους οι οποίοι προσπέλασαν παράνομα τους κωδικούς και τις προσωπικές πληροφορίες των πελατών της εταιρείας *Seisint*, την οποία είχε αγοράσει η *LexisNexis* το 2004.

Η πληροφορία είναι ένα πολύ κρίσιμο δεδομένο. Όποιος έχει την πληροφορία έχει την δυνατότητα να προσφέρει τεράστιο καλό ή να κάνει μεγάλη ζημιά. Οι εταιρείες και οι οργανισμοί που διατηρούν προσωπικές, ευαίσθητες ή ιδιωτικές πληροφορίες δεν μπορούν πλέον να τηρούν παθητική στάση όσον αφορά στα δίκτυα υπολογιστών και στην ασφάλεια των δεδομένων. Καθώς οι εταιρείες προσπαθούν να εφαρμόσουν το εξελισσόμενο πεδίο της δικανικής ψηφιακής ανάλυσης στο πεδίο ασφάλειας ολόκληρου του δικτύου τους, οι εξωτερικές και εσωτερικές απειλές προς την εταιρική ψηφιακή ασφάλεια αυξάνονται με ταχείς ρυθμούς. Οι εξωτερικές απειλές αποτελούνται από το κακόβουλο λογισμικό (*malware*) όπως είναι οι ιοί (*virus, worm, trojan horse, spyware, adware).* Άλλες εξωτερικές απειλές αποτελούν τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*), οι απειλές στο πεδίο κοινωνικής μηχανικής *(social engineering*), η παραβίαση των κωδικών ενός υπολογιστή ή συστήματος (*hacking*). Οι εσωτερικές απειλές προέρχονται από θυμωμένους υπαλλήλους και από υπαλλήλους που δεν ανταποκρίνονται στις απαιτήσεις της εργασίας και οι οποίοι δεν μπορούν να θεωρηθούν κακόβουλοι. Οι δραστηριότητες των υπαλλήλων αυτών (κακόβουλων ή μη) μπορούν να οδηγήσουν σε απώλεια της ακεραιότητας του συστήματος και απώλεια δεδομένων. Το χειρότερο είναι ότι οι πιθανοί εισβολείς μπορεί να χρησιμοποιήσουν τα ιδιωτικά δεδομένα του οργανισμού για έναν αριθμό επικίνδυνων και παράνομων δραστηριοτήτων, όπως είναι η εκβίαση, η απάτη, η κλοπή ή οι απειλές εθνικής ασφάλειας.

Επιπλέον προκλήσεις στο πεδίο της ασφάλειας προέρχονται από την εγκατάσταση ασύρματων δρομολογητών (*routers*), από μη εγκεκριμένες εγκαταστάσεις λογισμικού, από την κλοπή ή απώλεια υπολογιστών (φορητών ή μη) και φορητών μέσων αποθήκευσης *(USB, flash* κ.α.). Η κλοπή υλικού υπολογιστών ή μέσων αποθήκευσης μπορεί να προκαλέσει μεγάλη ζημιά στην υπόληψη των οργανισμών. Το 2005, η *Bank of America* ανακάλυψε ότι το Δεκέμβρη του 2004, έχασε τις ταινίες αποθήκευσης που περιείχαν σε κρυπτογραφημένη μορφή τους αριθμούς κοινωνικής ασφάλισης και άλλα προσωπικά δεδομένα που ανήκαν σε κυβερνητικούς υπαλλήλους και βασίζονταν σε 1,2 εκατομμύρια πιστωτικές κάρτες. Τη χρονική στιγμή της ανακοίνωσης δεν υπήρχε ένδειξη ότι έγινε κάποια παράνομη δραστηριότητα με τη χρήση της πληροφορίας που υπήρχε στα μέσα αποθήκευσης που χάθηκαν.

Η απώλεια ευαίσθητων και ιδιωτικών δεδομένων από εγκληματικές και παράνομες ομάδες θα πρέπει να είναι το πρωταρχικό μέλημα κάθε οργανισμού. Οι εισβολές στα δίκτυα, οι παραβιάσεις ασφάλειας και τα συμβάντα ασφάλειας σχετίζονται με τη μη

εξουσιοδοτημένη πρόσβαση στα δεδομένα των υπολογιστών και στα συστήματα. Τα συμβάντα ασφάλειας αποτελούνται από τρείς διαφορετικούς τύπους δραστηριοτήτων:

- Κάθε παραβίαση ή μη εξουσιοδοτημένη πρόσβαση σε εταιρικά δεδομένα, άσχετα με το αν έχουν σαν αποτέλεσμα απώλειες ή ζημιές. Πιθανούς στόχους αποτελούν οι προσωπικοί υπολογιστές, τα μέσα αποθήκευσης και ακόμα ολόκληρο το δίκτυο του συστήματος,
- Κάθε χρήση των εταιρικών υπολογιστικών συστημάτων για κακόβουλη δραστηριότητα από εσωτερικές ή εξωτερικές δυνάμεις,
- Κάθε γεγονός, κακόβουλο ή ατύχημα, που έχει σαν αποτέλεσμα ζημιές ή απώλειες.

Παραδείγματα των απειλών στα δίκτυα, περιλαμβάνουν παραβίαση κωδικών από εσωτερικούς ή εξωτερικούς παράγοντες, μη εξουσιοδοτημένη πρόσβαση, κακόβουλο λογισμικό και άρνηση παροχής υπηρεσίας. Αυτές οι εισβολές στα δίκτυα των υπολογιστών μπορεί να προκαλέσουν την κακή λειτουργία των εφαρμογών λογισμικού, την κλοπή κωδικών για την αποστολή κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου, την καταστροφή ή το σβήσιμο των λειτουργικών συστημάτων και των αρχείων υπολογιστών. Το οικονομικό κόστος που υφίσταται ένας οργανισμός για να αντιμετωπίσει μία μόνο εισβολή στους υπολογιστές του και την αντίστοιχη ζημιά, υπερβαίνει τον ετήσιο προϋπολογισμό ασφάλειας του οργανισμού (*CIO Magazine*, 2004). Αυτές οι απειλές δεν αποτελούν πλέον μια μικρή ενόχληση. Μπορούν να γίνουν καταστρεπτικές και δαπανηρές και οι οργανισμοί παίρνουν μέτρα για να εμποδίσουν και να μειώσουν τα αποτελέσματά τους. Η διαδικασία της δικανικής ανάλυσης που συλλέγει, εξετάζει, αναλύει και καταγράφει τις προσπάθειες εισβολής θα πρέπει να ενσωματωθεί στην πολιτική δικτυακής ασφάλειας της εταιρείας μέσω της ανίχνευσης της εισβολής, της πρόληψης της εισβολής και του ελέγχου των εφαρμογών.

3.7.1 Διάφορα Θέματα και Προβλήματα

Τα ποσά που ξοδεύουν οι οργανισμοί για να διαφυλάξουν την δικτυακή ασφάλεια και η πολυπλοκότητα των λύσεων που επιλέγουν, διαφέρει πολύ μεταξύ των οργανισμών. Κάποιοι οργανισμοί επιλέγουν περιεκτικά συστήματα πρόληψης και ανίχνευσης παραβιάσεων, με ένα φυσικό διαχωρισμό των συστημάτων που περιλαμβάνουν και τη χρήση *Demilitarized Zone (DMZ)* για πρόσβαση στο διαδίκτυο. Άλλοι οργανισμοί βασίζονται στο *hardware* και σε συστήματα για άμεση σύνδεση με τον έξω κόσμο. Επίσης υπάρχει μεγάλη ποικιλία στις πολιτικές ασφάλειας και στις σχεδιασμένες απαντήσεις/συλλογές δεδομένων των οργανισμών. Οι λόγοι για την ύπαρξη της ποικιλίας και της μεταβλητότητας περιλαμβάνουν το μέγεθος των οργανισμών, την έκθεση στο διαδίκτυο. Οι εταιρείες που αποτρέπουν τη λήψη εξωτερικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και την περιήγηση στο διαδίκτυο, έχουν μικρότερες πιθανότητες να δεχθούν επιθέσεις εισβολής. Άλλοι λόγοι που ευθύνονται για την ποικιλία των πολιτικών ασφάλειας, είναι οι απαιτήσεις συμμόρφωσης με συγκεκριμένους νομικούς κανόνες. Επίσης είναι το ρίσκο της καταστροφής, αν δηλαδή οι επιπτώσεις μιας εισβολής θα είναι καταστρεπτικές ή μηδαμινές, αν ο οργανισμός διαθέτει συστήματα ανάνηψης από καταστροφές και πόσο γρήγορα θα μπορέσει να ανανήψει.

3.7.1.1 Πρόληψη και Ανίχνευση Παραβάσεων

Οι οργανισμοί που θέλουν να μεγιστοποιήσουν την προστασίας τους απέναντι σε παραβιάσεις των υπολογιστικών συστημάτων θα πρέπει πρώτα να κάνουν αυτό-αξιολογήσεις ώστε να διαπιστώσουν πόσο ελκυστικοί είναι σαν στόχοι, και να

προσδιορίσουν τα πρωταρχικά στοιχεία που θα ήθελαν να προστατεύσουν. Οι εταιρείες θα πρέπει να αναρωτηθούν: «*Τι είδους στόχος είμαι;».* Οι οικονομικοί οργανισμοί, οι κυβερνητικοί οργανισμοί, οι οργανισμοί που υποστηρίζουν κυβερνητικές λειτουργίες θα πρέπει να προσεγγίσουν το θέμα της ασφάλειας από διαφορετική πλευρά, σε σχέση με μικρότερους οργανισμούς ή τοπικές επιχειρήσεις. Παρόμοια, οι οργανισμοί θα πρέπει να προσδιορίσουν τα βασικά στοιχεία που θέλουν να προστατεύσουν. Είναι για έναν οργανισμό, η συλλογή και προστασία των δεδομένων περισσότερο σημαντική ή η προστασία των υπαρχόντων δεδομένων; Η απάντηση σε αυτή την ερώτηση βοηθά την εταιρεία να καθορίσει τον τρόπο με τον οποίο θα γίνει η διάθεση των πόρων της. Αυτή η ανάλυση περιλαμβάνει τις πραγματικές παραβιάσεις και επίσης την ανίχνευση και καταγραφή των προσπαθειών παραβίασης που απέτυχαν. Η συλλογή αυτών των πληροφοριών βοηθά τον οργανισμό να καταλάβει τις πραγματικές απειλές και να ανιχνεύσει πρότυπα επιθέσεων. Για παράδειγμα, το 2003 οι ειδικοί μπόρεσαν να προβλέψουν τον ιό *blaster*, από πρότυπα επιθέσεων κακόβουλου λογισμικού που είχαν ανιχνεύσει και αποτρέψει.

Αναφορικά με την παραβίαση ασφάλειας στην εταιρεία *LexisNexis* που παρουσιάσαμε, ο *Avivah Litan (Gartner Group, 2003*), προτείνει τρείς δραστηριότητες που πρέπει να υλοποιηθούν άμεσα από εταιρείες οι οποίες διαχειρίζονται ευαίσθητα προσωπικά δεδομένα πολιτών:

- Υλοποίηση διαδικασίας αυθεντικοποίησης δύο παραγόντων, για πρόσβαση στα συστήματα και τις βάσεις δεδομένων. Έτσι θα αποτραπεί η μη εξουσιοδοτημένη ανταλλαγή των κωδικών (*password*) και των ονομάτων πρόσβασης *(user Identification, ID)* στους οργανισμούς που έχουν πρόσβαση σε τέτοια δεδομένα,
- Υλοποίηση εργαλείων παρακολούθησης δραστηριότητας, στο επίπεδο των εφαρμογών ή της βάσης δεδομένων, ώστε να είναι δυνατό να ανιχνευθούν πρότυπα ή ασυνήθιστη δραστηριότητα που μπορεί να υποδηλώνει απάτη ή προσπάθεια εισβολής,
- Θεώρηση των πρακτικών ασφάλειας ως βασικό κριτήριο κατά την επιλογή παρόχων των υπηρεσιών πληροφόρησης.

3.7.1.2 Η Πολιτική Ασφάλειας *(Security Policy)*

Η ***πολιτική ασφάλειας ενός οργανισμού*** θα πρέπει να απευθύνεται κατ' ελάχιστο στα παρακάτω στοιχεία*:*

- Πώς θα πρέπει να χειριστεί την ευαίσθητη πληροφορία,
- Πώς θα διατηρήσει με ασφάλεια τους κωδικούς και τα ονόματα πρόσβασης, όπως επίσης και άλλα δεδομένα,
- Πώς θα απαντήσει σε μια πιθανή προσπάθεια εισβολής,
- Πώς θα χρησιμοποιήσει τα υπολογιστικά συστήματα και τις συνδέσεις στο διαδίκτυο με ασφαλή τρόπο,
- Πώς θα χρησιμοποιήσει με ασφάλεια το εταιρικό σύστημα ηλεκτρονικού ταχυδρομείου.

Η *Cisco Systems*, που είναι προμηθευτής δικτυακών λύσεων βασισμένων στο *Internet Protocol*, αναγνωρίζει τρείς τύπους ***καταστάσεων πολιτικής*** *(policy statements)* που θα πρέπει να καλύπτουν όλα τα δικτυακά συστήματα και δεδομένα μέσα σε έναν οργανισμό. Την ***κατάσταση πολιτικής χρήσης*** (*usage policy statement*), ***την κατάσταση αποδεκτής χρήσης από εταίρο*** *(partner acceptable use statement*) και

την ***κατάσταση αποδεκτής χρήσης από διαχειριστή*** (*administrator acceptable use statement*), *(Network Security Policy: Best Practices White Paper, 2003)*. Προτείνει ***η κατάσταση πολιτικής χρήσης***, να περιγράφει τους ρόλους και τις υπευθυνότητες των χρηστών και να παρέχει πειθαρχικές δράσεις απέναντι σε υπαλλήλους. ***Η κατάσταση αποδεκτής χρήσης από εταίρο***, θα πρέπει να περιγράφει τη χρήση των δεδομένων και την κατάλληλη διεξαγωγή, όπως επίσης τι αποτελεί προσπάθεια εισβολής ασφάλειας και ποιές ενέργειες θα πρέπει να γίνουν όταν αυτή συμβεί***. Η κατάσταση αποδεκτής χρήσης από διαχειριστή,*** θα πρέπει να περιγράφει την διαχείριση του δικτύου, την επανεξέταση των προνομίων και την επιβολή της πολιτικής.

Κάθε μια από αυτές τις καταστάσεις πολιτικής θα πρέπει να συμπληρώνει την άλλη, χωρίς συγκρούσεις και ασάφειες. Σημαντική βοήθεια στην ανάπτυξη αυτών των καταστάσεων και της πολιτικής ασφάλειας του δικτύου αποτελεί η καταγραφή της εμπειρίας των οργανισμών που τις έχουν ήδη εφαρμόσει.

3.7.1.3 Η Σχεδιασμένη Απάντηση *(Planned Response)*/Η Συλλογή Δεδομένων *(Data Collection)*

Οι μεγαλύτερες εταιρείες θα πρέπει να έχουν στο προσωπικό τους πιστοποιημένους δικανικούς αναλυτές, για να παρακολουθούν οποιαδήποτε ασυνήθιστη δραστηριότητα και να εξάγουν τις κατάλληλες πληροφορίες. Οι μικρότερες εταιρείες θα πρέπει να χρησιμοποιούν ειδικό λογισμικό για δικανική ανάλυση για να διατηρούν τις ηλεκτρονικές αποδείξεις, να τις αναλύουν και να τις καταγράφουν. Κάθε οργανισμός θα πρέπει να προσπαθεί να διώκει με νομικά μέσα αυτές τις εισβολές. Επειδή όμως η νομική δίωξη αυτών των επιθέσεων απαιτεί συλλογή δεδομένων, καταγραφή και παρουσίαση, οι περισσότεροι οργανισμοί αρκούνται στη συλλογή των πληροφοριών και στην δράση ως προς την επίθεση, ανεξάρτητα από τη νομική δίωξη.

Στη συνέχεια θα παρουσιάσουμε τον τρόπο με τον οποίο τρείς διαφορετικοί οργανισμοί προετοιμάστηκαν και αντιμετώπισαν παραβιάσεις ασφάλειας.

3.7.1.3.1 Περίπτωση 1: Εταιρεία Υπηρεσιών Υγείας

Στις αρχές του 2005, μια εταιρεία υπηρεσιών υγείας μπήκε σε κατάσταση συναγερμού λόγω μιας διακοπής στη λειτουργία ενός εσωτερικού τείχους προστασίας (*firewall*). Το συγκεκριμένο τείχος προστασίας ήταν μεταξύ του απομακρυσμένου δικτύου της εταιρείας και του δικτύου των κύριων εγκαταστάσεων. Το εσωτερικό τείχος προστασίας σταμάτησε να απαντά στις αιτήσεις διαχείρισης και σε κάθε τύπο ηλεκτρονικής επικοινωνίας.

Τα αρχικά βήματα αναγνώρισης του προβλήματος έδειξαν ότι πιθανόν να υπήρχε σφάλμα υλικού (*hardware)* στο ίδιο το τείχος προστασίας. Μηχανικοί της εταιρείας και του προμηθευτή του *hardware* προσπάθησαν να ανακαλύψουν το πρόβλημα και μετά από πολλές ώρες, αποφάσισαν ότι υπήρξε πλημμύρα (*flood*) πακέτων δεδομένων, που έκανε το τείχος προστασίας να χρησιμοποιήσει το 100% των πόρων του. Η χρήση ήταν τόσο εντατική και σαν αποτέλεσμα λειτουργίες όπως η αποθήκευση πακέτων (*packet dumps*) και η διαχειριστική ανάλυση (*management analysis*) δεν ήταν δυνατόν να γίνουν. Έπρεπε να γίνει φυσική αποσύνδεση όλων των διεπαφών, ώστε να διαπιστωθεί ποιά ήταν η πηγή της εισερχόμενης κίνησης. Αργότερα βρέθηκε ότι ήταν ένας μόνο υπολογιστής ο οποίος έστελνε εξαιρετικά μεγάλο αριθμό από πολύ μικρά πακέτα, και σαν αποτέλεσμα προκαλούσε επίθεση άρνησης παροχής υπηρεσίας στο τείχος προστασίας. Η επίθεση αυτή δεν κατευθυνόταν ειδικά στο τείχος προστασίας, αλλά καθώς αυτό ήλεγχε κάθε εισερχόμενο πακέτο, υπερφόρτωσε τη λειτουργία του. Αν και

οι ικανότητες εύρους ζώνης του τείχους προστασίας δεν επηρεάστηκαν, η χρήση της διαδικασίας έφτασε στο 100%.

Η υπηρεσία δικτύου υποβαθμίστηκε για τρείς μέρες. Αργότερα βρέθηκε ότι ο υπολογιστής συνδέθηκε με το δίκτυο μέσω τηλεφωνικής σύνδεσης (*dial up connection*) σε έναν απομακρυσμένο εξυπηρετητή πρόσβασης. Επιπλέον η έρευνα απέδειξε ότι ο υπολογιστής δεν ήταν ξένος αλλά ανήκε στην εταιρεία και είχε δοθεί σε έναν εργαζόμενο. Στον υπολογιστή αυτό ήταν εγκατεστημένη μια μεγάλη ποσότητα από λογισμικό που δεν χρειάζονταν στη λειτουργία της εταιρείας και το οποίο μπορεί να προκάλεσε τη διακοπή του δικτύου, αλλά δεν ήταν γνωστό ποιά εφαρμογή λογισμικού ήταν κακόβουλη. Μετά τη σύγκριση των δεδομένων με τα αρχεία καταγραφής του τείχους προστασίας και με τις συσκευές ασφάλειας, αποδείχτηκε ότι η πιο ύποπτη εφαρμογή ονομαζόταν *view toolbar*.

Το προσωπικό της εταιρείας μελέτησε την εφαρμογή *view toolbar* και ανακάλυψε ότι πρόκειται για μια άκακη εφαρμογή η οποία εγκαταστάθηκε μαζί με τις καθορισμένες λειτουργίες *adware*. Η εταιρεία δημιούργησε ένα περιβάλλον για να εγκαταστήσει την εφαρμογή και να συνεχίσει την έρευνα. Χρησιμοποιώντας το *Google* με το λεκτικό *view toolbar download*, οι τεχνικοί είδαν μια οθόνη γεμάτη με σελίδες διαδικτύου (*web*) από της οποίες μπορούσαν να εγκαταστήσουν την εφαρμογή. Όταν επιχείρησαν να εγκαταστήσουν την εφαρμογή, στα πρώτα δευτερόλεπτα της προσπέλασης στη σελίδα *web*, και καθώς άνοιγαν τη συγκεκριμένη σελίδα, ο υπολογιστής «κρέμασε» δηλαδή σταμάτησε να δουλεύει και το τείχος προστασίας του εργαστηρίου τέθηκε εκτός λειτουργίας. Το προσωπικό κατάλαβε ότι επρόκειτο για μια κακόβουλη σελίδα *web* και όχι για κακόβουλη εφαρμογή. Στη συνέχεια του ελέγχου, ανακάλυψαν ότι τα πρώτα πέντε αποτελέσματα της ερώτησης *Google* για την εφαρμογή, ήταν κακόβουλες *web* σελίδες.

Η εταιρεία επικοινώνησε με εταιρείες ασφάλειας υπολογιστών της *Symantec*, *Microsoft* και *Checkpoint* για να ανακαλύψει αν αυτό που βρήκε ήταν μια γνωστή αδυναμία. Καμιά εταιρεία δεν την είχε υπόψη της.

Στη συνέχεια, η εταιρεία υπηρεσιών υγείας, επικοινώνησε με την εταιρεία *SecureWave* στο Λουξεμβούργο. Η εταιρεία αυτή διαφήμιζε ένα προϊόν που έδινε στους διαχειριστές πλήρη έλεγχο του *hardware* και του λογισμικού. Τον Ιανουάριο του 2005, η εταιρεία *SecureWave* έκανε μια επίδειξη του λογισμικού της στη διοίκηση της εταιρείας. Αν και τα αποτελέσματα ήταν εντυπωσιακά, οι μηχανικοί της εταιρείας θέλησαν να ελέγξουν οι ίδιοι το προϊόν στο εργαστήριο. Ενημέρωσαν τον εκπρόσωπο της *SecureWave* για την ανακάλυψη της αδυναμίας ασφάλειας και τον ρώτησαν αν θα ήθελε η *SecureWave* να εγκαταστήσουν το προϊόν στο εργαστήριο και να επισκεφθούν την κακόβουλη *web* σελίδα. Η *SecureWave* συμφώνησε και ο εκπρόσωπός της είπε ότι*, αν υπάρχει κάποια αδυναμία σε ένα λειτουργικό σύστημα που το προϊόν μας δεν μπορεί να σταματήσει θα θέλαμε να το γνωρίζουμε.*

Οι συνθήκες στο εργαστήριο αρχικοποιήθηκαν και το λογισμικό της *SecureWave* εγκαταστάθηκε σε έναν υπολογιστή. Επαναλήφθηκε η διαδικασία με το ψάξιμο στη σελίδα της *Google* για τις *web* σελίδες που περιέχουν το *view toolbar*. Στη συνέχεια επιλέχθηκε η κακόβουλη σελίδα *web* και τα αποτελέσματα ήταν εκπληκτικά. Το λογισμικό *SecureWave* όχι μόνο σταμάτησε την αδυναμία αλλά έδωσε και μια ένδειξη για τον τρόπο λειτουργίας της κακόβουλης σελίδας *web*. Τα αρχεία καταγραφής του *SecureWave* περιείχαν λεπτομέρειες σχετικά με τα βήματα λειτουργίας της σελίδας, περιλαμβανομένων των αρχείων που τοποθετούσε στον υπολογιστή και των αλλαγών στα αρχεία (*registry*) που έκανε στη μονάδα του υπολογιστή. Αρχικά έτρεχε ένα *java*

script το οποίο απενεργοποιούσε όλα τα *Active X* ασφάλειας του *browser*. Τότε ξεκινούσε μια *Active X* σύνοδος (*session*) και εννιά *DLL (Dynamic Link Library)* αρχεία εφαρμογών εγκαθίσταντο σε διάφορους καταλόγους (*directories*) του υπολογιστή. Το *SecureWave* σταμάτησε όλες τις αλλαγές αρχείων (*registry)*.

Οι πληροφορίες που υπήρχαν στα αρχεία καταγραφής του *SecureWave* δόθηκαν στις εταιρείες ασφάλειας. Τρείς βδομάδες αργότερα η *Microsoft* δημοσίευσε εννέα σημαντικά διορθωτικά προγράμματα (*patch)* αλλαγών για τα λειτουργικά συστήματα και για τους *explorers*, τα οποία συνδέθηκαν με τον τρόπο που δούλευε η κακόβουλη σελίδα, όπως αποκάλυψαν τα αρχεία καταγραφής του *SecureWave.*

Αν και η εταιρεία υπηρεσιών υγείας είχε ένα ατύχημα στην ασφάλεια του δικτύου, η ιστορία αυτή θεωρείται ιστορία επιτυχούς κατάληξης. Τελικά βρήκαν λογισμικό προστασίας για τους υπολογιστές και τα δεδομένα των εξυπηρετητών και βέβαια για τα δεδομένα των πελατών τους.

3.7.1.3.1.1 Πολιτική Ασφάλειας *(Security Policy)*

Η εταιρεία υπηρεσιών υγείας χρησιμοποιεί έξι τεχνικές για να αποτρέψει την παραβίαση και να την ανιχνεύσει: **1)** Παρατάσσονται τείχη προστασίας (*firewalls*) σε όλες τις διεπαφές μεταξύ του ιδιωτικού δικτύου και του δημόσιου διαδικτύου (*internet*). Όλη η κίνηση και οι προσπάθειες παραβίασης καταγράφονται και αποθηκεύονται σε έναν εξυπηρετητή ασφάλειας για ιστορική αξιολόγηση. Όλοι οι υπολογιστές που είναι δυνατόν να βγουν από το δίκτυο, όπως οι φορητοί υπολογιστές θα πρέπει να έχουν λογισμικό τείχους προστασίας εγκατεστημένο σε αυτούς, το οποίο θα αποτρέπει και θα καταγράφει τις προσπάθειες εισβολής. Επίσης θα πρέπει να γίνεται έλεγχος της κίνησης από τα τείχη προστασίας ώστε να επιτρέπουν αυτά που η κίνηση θα πρέπει να κάνει και να αποτρέπουν αυτά που δεν πρέπει να κάνει. Η εταιρεία υπηρεσιών υγείας χρησιμοποιεί την πληροφορία που αποθηκεύει από τον έλεγχο της κίνησης στα τείχη προστασίας, για να συγκεντρώσει πληροφορίες σχετικά με τις δικτυακές συνήθειες των υπαλλήλων και τη χρήση του εύρους ζώνης. Αυτές οι πληροφορίες εξετάζονται ανά μήνα ώστε να αποφασιστεί ποιές *web* σελίδες θα πρέπει να απαγορευθούν ανάλογα με το μέγεθος της κίνησης και τη χρήση του εύρους ζώνης. **2)** Τα συστήματα ανίχνευσης εισβολών (*IDS*) τοποθετούνται σε στρατηγικές θέσεις σε όλο το δίκτυο. Τα συστήματα αυτά ελέγχουν για υπογραφές με αδυναμίες και οι βάσεις δεδομένων που διατηρούν με πρότυπα εισβολών ενημερώνονται περιοδικά ώστε να εξασφαλίσουν τα δίκτυα απέναντι στις νεότερες επιθέσεις εισβολής. **3)** Η λειτουργία καταγραφής των συστημάτων *IDS,* καταγράφει τα δεδομένα σε αρχεία και προετοιμάζει ανακοινώσεις ανά ημέρα, εβδομάδα ή μήνα. Αυτές οι ανακοινώσεις αναλύονται για πρότυπα κίνησης ή πολιτικές παραβίασης. **4)** Οι ενημερώσεις αποτυχίας των δρομολογητών (*routers*) και των μεταγωγέων (*switches*) χρησιμοποιούνται για να ενημερώσουν το προσωπικό ασφάλειας όταν ένας δρομολογητής ή ένας μεταγωγέας παρουσιάσει τρείς ή περισσότερες αποτυχημένες προσπάθειες αρχικοποίησης. Οι ενημερώσεις αυτές καταγράφονται και στέλνονται στο προσωπικό ασφάλειας μέσω του ηλεκτρονικού ταχυδρομείου. **5)** Φίλτρα δικτύου τοποθετούνται σε όλες τις απομακρυσμένες συσκευές του δικτύου. Οι συσκευές αυτές έχουν τα φίλτρα για να περιορίζουν την κίνηση του δικτύου. Για παράδειγμα, τα μηνύματα *Internet Control Message Protocol (ICMP*) ή *ping* χρησιμοποιούνται συχνά από το προσωπικό υποστήριξης. Το *ICMP* επιτρέπεται από το υποδίκτυο του προσωπικού υποστήριξης αλλά δεν επιτρέπεται από κανένα άλλο δίκτυο. Οι εισβολείς (*hackers*) χρησιμοποιούν συχνά το *ICMP* για να βοηθηθούν στην ανίχνευση ενός δικτύου και να δημιουργήσουν επιθέσεις άρνησης παροχής υπηρεσίας. Το πρόβλημα με το *ping* είναι ότι ένα άτομο εκτός δικτύου μπορεί να μαντέψει την

τοπολογία του δικτύου. Με τη χρήση εργαλείων που χρησιμοποιούν το *ping*, όπως είναι το *traceroute* ή το *tracert* για τα *Windows*, κάποιος μπορεί να διαπιστώσει πόσα άλματα (*hops),* δηλαδή πόσοι *firewalls* και *routers* υπάρχουν στο δίκτυο. Αν και οι οργανισμοί μπορούν να απαγορεύσουν τα εξωτερικά *ICMP*, τα εσωτερικά *ICMP* μπορούν να πραγματοποιηθούν από επισκέπτες του οργανισμού αν τους έχει δοθεί πρόσβαση στο δίκτυο για να εκτυπώνουν, για να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο, για περιήγηση στο διαδίκτυο ή για προσπέλαση αρχείων. **6)** Το κλείδωμα του *hardware* ή του λογισμικού του λειτουργικού συστήματος αποτελεί ένα κλειδί για τη διασφάλιση του δικτύου. Το λογισμικό *SecureWave* είναι ένα λογισμικό ελέγχου εισόδου/εξόδου *(I/O control*) που μπορεί να κλειδώσει οποιαδήποτε συσκευή εισόδου/εξόδου έτσι ώστε οι φυσικές συσκευές παραβίασης ασφάλειας να μπλοκάρουν. Επίσης το λογισμικό *SecureWave* επιτρέπει έλεγχο του λογισμικού του συστήματος, ώστε μόνο τα εγκεκριμένα αρχεία να αποθηκεύονται στη μνήμη. Αυτό απαγορεύει τους τύπους κακόβουλου λογισμικού (όπως *trojan horse, worm, virus, spyware*) από το να αποθηκευτούν στην μνήμη του υπολογιστή.

Ως προληπτικό εργαλείο ανίχνευσης εισβολών, η εταιρεία υπηρεσιών υγείας χρησιμοποιεί τα συστήματα παγίδας (*honeypots*) σε κάποια μη ασφαλή περιοχή του διαδικτύου. Ένα σύστημα παγίδας (*honeypot*) είναι ένας υπολογιστής ο οποίος αφήνεται επίτηδες χωρίς προστασία και με ένα πολύ μικρό επίπεδο ασφάλειας ώστε να δελεάσει τον εισβολέα. Οι τεχνικές των εισβολέων και οι δραστηριότητες των ιών παρακολουθούνται και σε απάντηση γίνονται διορθώσεις στο δίκτυο.

Η προσέγγιση του δικτύου που χρησιμοποιεί συστήματα παγίδας (*honeypots*) για την ανίχνευση των εισβολών, έχει γίνει μια από τις πιο σημαντικές τάσεις στη βιομηχανία της ασφάλειας πληροφοριών. Για να δημιουργήσουν ένα δίκτυο-παγίδα, οι διαχειριστές του συστήματος σχεδιάζουν ένα τμήμα του δικτύου της εταιρείας ώστε να το κάνουν ελκυστικό στους εισβολείς. Αυτό το τμήμα θα περιέχει ψεύτικη πληροφορία, για παράδειγμα κώδικα εφαρμογών ή μελλοντικά σχέδια της εταιρείας. Μόλις ο εισβολέας μπει σε αυτή την περιοχή, στην οποία ένας εξουσιοδοτημένος χρήστης δεν έχει κανένα λόγο να μπει, το σύστημα ειδοποιεί αυτόματα το προσωπικό ασφάλειας, που αρχίζει να παρακολουθεί τις δραστηριότητες του εισβολέα και πιθανόν να του δώσει και επιπλέον λανθασμένες πληροφορίες για να μάθει περισσότερα για την ταυτότητα και την θέση του.

Είναι πολύ σημαντική η κατανόηση της φύσης και των κινήτρων των προσπαθειών εισβολής, ώστε να εμπλουτιστούν οι διαδικασίες της ασφάλειας πληροφοριών. Μια παραβίαση από έναν έφηβο που θέλει να εντυπωσιάσει τους φίλους του, μπορεί να έχει σοβαρές επιπτώσεις για έναν οργανισμό, αλλά συνήθως αποτελεί μικρότερο πρόβλημα από την εταιρική κατασκοπία ή από τους «πληροφορικούς τρομοκράτες» που έχουν πολιτικά κίνητρα.

3.7.1.3.1.2 Η Σχεδιασμένη Απάντηση *(Planned Response)/*Η Συλλογή Δεδομένων *(Data Collection)*

Το κλειδί στην ασφάλεια των δικτύων αποτελεί το πλάνο αντιμετώπισης και απάντησης στις επιθέσεις. Αν και κάθε παραβίαση είναι διαφορετική, τα απλά και περιεκτικά πλάνα μπορούν να μειώσουν τις παραβιάσεις ή και να τις συμπεριλάβουν.

Η εταιρεία υπηρεσιών υγείας συμπεριέλαβε την δυνατότητα αναφορών και τα σχήματα αναφορών, σαν μέρος των σχεδιασμένων δραστηριοτήτων για την απάντηση και τη συλλογή δεδομένων. Το είδος της παραβίασης και τα δεδομένα που προσέγγισε θα πρέπει να εξεταστούν ώστε να καθοριστεί η φύση της αναφοράς που απαιτείται. Η

χρήση των αναφορών ενθαρρύνεται και πολλές φορές απαιτείται από την διαχείριση κινδύνου των εταιρειών, από τις κυβερνήσεις, από τα τμήματα δίωξης των εγκλημάτων. Σε περίπτωση που οι προσωπικές τους πληροφορίες αποκαλύπτονται, οι ασθενείς θα πρέπει να ειδοποιούνται.

Επίσης η νομική δίωξη των παραβιάσεων ενθαρρύνεται, παρόλο που το κόστος είναι ένα εμπόδιο, κυρίως για μικρές εταιρείες. Η δικανική ανάλυση, η ανίχνευση των δεδομένων, η αντιγραφή των στοιχείων με την απεικόνιση (*imaging*) του *hardware* που έχει προσβληθεί μπορεί να είναι πολυδάπανες. Οι περισσότεροι οργανισμοί δεν μπορούν να αντέξουν το κόστος μιας πλήρους ανάλυσης που θα χρησιμοποιηθεί για τη δίωξη και γι' αυτό αρκούνται στην κάλυψη του κενού ασφάλειας. Η δίωξη είναι γενικά ένα πολύπλοκο θέμα λόγω των πολλαπλών δικαιοδοσιών και της φύσης αυτών των εγκλημάτων. Αυτά τα εγκλήματα συνήθως συμβαίνουν από απόσταση, πολλές φορές σε διεθνές επίπεδο. Η συλλογή πιστευτών αποδείξεων είναι ένα σημαντικό εγχείρημα για κάθε εγκληματική δραστηριότητα μέσω παραβίασης δικτύου. Τα συγκεκριμένα βήματα που διατηρούν τις αποδείξεις κατά τη συλλογή δεδομένων είναι:

1. ***Η σχεδιασμένη απάντηση (Planned Response)****:* Η εταιρεία υπηρεσιών υγείας έχει μια ομάδα επείγουσας απάντησης (*Emergency Response Team, ERT*) που αποτελείται από προσωπικό τεχνικών πληροφορικής και απαντά στις παραβιάσεις ασφάλειας. Επειδή κάθε παραβίαση είναι διαφορετική, η ομάδα αναλύει την επίδραση και τη σοβαρότητα της παραβίασης ώστε να καθορίσει την κατάλληλη αντίδραση. Μέσα στην ομάδα έχουν τεθεί κάποιες γενικές οδηγίες για να καθοδηγήσουν την αντίδραση σε γενικές γραμμές. Μια τέτοια οδηγία είναι «***αν η επίθεση αφορά άρνηση παροχής υπηρεσίας, αλλά η ασφάλεια και τα δεδομένα είναι άθικτα, θα πρέπει να παρθούν μέτρα φιλτραρίσματος, ώστε να εμποδιστεί η διεύθυνση πηγής του εισβολέα να περάσει μέσα στο σύστημα».***

   Μια άλλη οδηγία είναι ***«να απομονώνονται και να αποσυνδέονται τα συστήματα που έχουν μολυνθεί, και να απενεργοποιούνται οι θύρες αν είναι απαραίτητο. Ελέγξτε το σύστημα για να διαπιστωθεί αν ο ιός συνεχίζει να διαδίδεται».***

   Η ομάδα αυτή έχει την εξουσιοδότηση από τη διοίκηση να κλείσει και να απομονώσει τα συστήματα που αυτή κρίνει, έτσι ώστε να εμποδίσει την πρόσβαση σε προστατευμένες πληροφορίες υγείας και σε οικονομικά δεδομένα. Κανονικά, κάθε σχεδιασμένη διακοπή θα πρέπει να εξουσιοδοτείται, αλλά κατά τη διάρκεια κρίσεων η ομάδα *ERT*, έχει την πλήρη εξουσία να σταματήσει κάθε αδυναμία και να σώσει τις σημαντικές πληροφορίες.

2. ***Η συλλογή δεδομένων (Data Collection)***

   Η συλλογή δεδομένων αποτελεί ένα σημαντικό κομμάτι στην εκτίμηση της αδυναμίας και στην ανάνηψη. Κάθε φορά που υπάρχει η υποψία ότι το σύστημα έχει παραβιαστεί, η μηχανή απομονώνεται και δημιουργείται ένα αντίγραφο *bit* προς *bit*. Το αντίγραφο δημιουργείται ώστε το προσωπικό των τεχνικών ή οι ερευνητές να μπορούν ελέγξουν τις πληροφορίες χωρίς να καταστρέψουν αποδεικτικά στοιχεία της παραβίασης. Επίσης τα αρχεία καταγραφής δικτύου από τα τείχη προστασίας και από τα συστήματα *IDS* αντιγράφονται για να εξεταστούν.

   Τα δεδομένα εξετάζονται για τους παρακάτω λόγους:

   - Την ανακάλυψη της μεθόδου παραβίασης,

- Την ανακάλυψη των πληροφοριών που αποκαλύφθηκαν,
- Την ανακάλυψη της ίδιας αδυναμίας σε διαφορετικά συστήματα,
- Την ανακάλυψη ενός *rootkit* ή ενός ιού *trojan horse* σαν κατάλοιπο της παραβίασης. Ένα *rootkit* είναι ένα σύνολο από εργαλεία που επιτρέπουν στον εισβολέα να συλλέξει ονόματα πρόσβασης (*user ID*) και κωδικούς πρόσβασης (*password*).

Αυτά τα ευρήματα χρησιμοποιούνται για να καθοριστεί το επόμενο βήμα. Για παράδειγμα, αν έχει παραβιαστεί κάποιος νόμος, θα πρέπει να ειδοποιηθούν οι αρχές. Αν έχουν παραβιαστεί πληροφορίες ασθενών, οι ασθενείς αυτοί θα πρέπει να ειδοποιηθούν άμεσα.

Η καταγραφή των περιστατικών είναι επίσης πολύ σημαντική, όχι μόνο σαν μια βοήθεια για τη λύση του προβλήματος της παραβίασης, αλλά και για την ανάπτυξη μιας διαδρομής ελέγχου που θα μπορούσε να χρησιμοποιηθεί κατά την εξέταση των εγκληματιών. Είναι κρίσιμο να βρεθεί όσο το δυνατόν περισσότερη πληροφορία και να δημιουργηθούν φόρμες που θα βοηθήσουν τους χρήστες που δεν είναι ειδικοί πληροφορικής να παρέχουν ακριβείς πληροφορίες. Κάποια σημαντικά θέματα που σχετίζονται με τις φόρμες αναφοράς περιστατικών είναι:

- Τα στοιχεία επικοινωνίας των ανθρώπων που ανακάλυψαν το πρόβλημα και των υπεύθυνων,
- Τα συστήματα και τα δίκτυα που αποτελούν στόχο. Η γνώση όσο το δυνατόν περισσότερων πληροφοριών σχετικά με τα δίκτυα που υφίστανται την επίθεση, όπως η έκδοση του λειτουργικού συστήματος, οι διευθύνσεις διαδικτύου (*IP addresses*) κ.α.,
- Ο σκοπός των συστημάτων που υφίστανται την επίθεση. Γιατί χρησιμοποιούνται αυτά τα συστήματα (μισθοδοσία, έρευνα και σχεδιασμό, διατηρούν αρχεία ασθενών κ.α.) όπως επίσης και μια κατάταξη της σπουδαιότητας του κάθε συστήματος,
- Οι αποδείξεις της παραβίασης, δηλαδή η ανακάλυψη όλων των στοιχείων σχετικά με την εισβολή,
- Οι μέθοδοι της επίθεσης που χρησιμοποιήθηκαν,
- Η διεύθυνση πηγής (*source IP address*) του εισβολέα,
- Τα στοιχεία επικοινωνίας του δικτύου γι’ αυτή τη διεύθυνση,
- Η λίστα των μερών που ειδοποιήθηκαν. Μπορεί να περιλαμβάνει τεχνικούς, νομικούς συμβούλους της εταιρείας και ίσως τις αρχές δίωξης εγκλημάτων.

Τα δίκτυα της εταιρείας υπηρεσιών υγείας μολύνθηκαν το 2002 από τον ιό *Nimda-D*, που δημιούργησε μια πλήρη διακοπή του δικτύου για πέντε μέρες. Το κόστος επισκευής της ζημιάς που προκάλεσε ο ιός, αν εξαιρέσουμε την απώλεια παραγωγικότητας και εσόδων, ανήλθε στα 150.000$. Το κόστος αυτό ήταν 2,5 φορές ο προϋπολογισμός ασφάλειας του οργανισμού για το 2002.

3.7.1.3.2 Περίπτωση 2: Η κοινότητα των σχολείων

Η ασφάλεια του δικτύου στην κοινότητα των σχολείων κλίνει προς τον τελικό χρήστη και την αποκεντρωμένη διαχείριση της κάθε περιοχής (σχολείου). Κάθε περιοχή μπορεί να αγοράζει υλικό και λογισμικό και να εγκαθιστά ηλεκτρονικό ταχυδρομείο και πρόσβαση στο διαδίκτυο και συνήθως χωρίς να ακολουθούνται οι οδηγίες των τμημάτων τεχνολογίας. Ένα σχολείο εγκατέστησε το δικό του σύστημα ηλεκτρονικού ταχυδρομείου, το οποίο υπέστη εισβολή και μετατράπηκε σε υπηρεσία προώθησης κακόβουλων ηλεκτρονικών μηνυμάτων. Αφού τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*) εμποδίζονται χρησιμοποιώντας την διεύθυνση *IP* από την οποία στέλνονται, η χρήση της διεύθυνσης του σχολείου επέτρεψε στον εισβολέα να παρακάμψει το λογισμικό φιλτραρίσματος του ηλεκτρονικού ταχυδρομείου. Όταν έγινε αντιληπτή η προώθηση αυτών των μηνυμάτων και το σύστημα έκλεισε από τους τεχνικούς, ο εισβολέας μπόρεσε να χρησιμοποιήσει το σύστημα του ηλεκτρονικού ταχυδρομείου σαν διακομιστή (*proxy*) για να μεταδώσει πορνογραφικό υλικό. Αν τεχνικοί πληροφορικής είχαν αναμιχθεί από την αρχή στην εγκατάσταση του συστήματος ηλεκτρονικού ταχυδρομείου, θα το είχαν εγκαταστήσει με τα πρότυπα ενός πιο ασφαλούς συστήματος.

3.7.1.3.2.1 Πολιτική Ασφάλειας *(Security Policy)*

Η κοινότητα των σχολείων δεν έχει μια επίσημη πολιτική ασφάλειας των δικτύων και των υπολογιστών. Οι ανεπίσημες πολιτικές της καθοδηγούνται από την χρηματοδότηση και τη νομιμότητα. Οι παράνομες ανταλλαγές αρχείων μέσω του *Napster* και του *Kazaa* απαγορεύονται. Ενώ ο διαχειριστής των τεχνολογικών θεμάτων έγραψε και προώθησε για έγκριση προς τους διαχειριστές μια μέθοδο πολιτικής ασφάλειας, αυτή γύρισε για διευκρινήσεις. Μετά από επιπλέον διορθώσεις και νέες υποβολές, που συνοδεύτηκαν από πρόσθετες αιτήσεις για διευκρίνιση από τους διαχειριστές, τελικά η πολιτική ασφάλειας εγκαταλείφθηκε από τον διαχειριστή τεχνολογίας.

Το προσωπικό διαχείρισης των σχολείων αναγνώρισε ότι η πολιτική ασφάλειας που θα ακολουθούσαν θα περιείχε στοιχεία όπως: **1)** Μια παράκαμψη της υπάρχουσας διαχείρισης του δικτύου, **2)** Εγκατάσταση μιας ζώνης *DMZ (Demilitarized Zone)*, **3)** Κεντρική αγορά και τυποποίηση των εφαρμογών και του υλικού (*hardware*) **4)** Έλεγχο των ασύρματων σημείων πρόσβασης και **5)** Πρόσβαση στο δίκτυο του σχολείου μόνο από τα δικά του συστήματα.

3.7.1.3.2.2 Η Σχεδιασμένη Απάντηση *(Planned Response)/*Η Συλλογή Δεδομένων *(Data Collection)*

Η κοινότητα των σχολείων δεν μελέτησε μια σχεδιασμένη απάντηση στην εισβολή του συστήματος ή τον τρόπο με τον οποίο θα μπορούσε να συλλέξει δεδομένα. Αντίθετα με την περίπτωση του οργανισμού υπηρεσιών υγείας, η κοινότητα των σχολείων (με πάνω από 100 σχολεία) ξοδεύει για την ασφάλεια του δικτύου της ανά έτος κάτι περισσότερο από το μισθό του διαχειριστή ασφάλειας. Η απάντηση στο γιατί η ασφάλεια ενός οργανισμού είναι πιο περιεκτική από την ασφάλεια ενός άλλου, μπορεί να καταδειχθεί σε τέσσερις περιοχές: **1)** Την ευθύνη**, 2)** Τον κίνδυνο της καταστροφής, δηλαδή τις επιπτώσεις της προσπάθειας εισβολής, **3)** Την ύπαρξη ανάκαμψης από την καταστροφή, και **4)** Το ιστορικό των σοβαρών προσπαθειών εισβολής. Ακόμα και αν το δίκτυο των σχολείων μολυνθεί και αχρηστευθεί, τα σχολεία θα συνεχίσουν να λειτουργούν και ο κίνδυνος της καταστροφής από εισβολή είναι μηδαμινός. Τα σχολεία έχουν μικρή έκθεση στον κίνδυνο, λόγω της μη κερδοσκοπικής τους οργανωτικής δομής.

3.7.1.3.3 Περίπτωση 3: Η Πολιτεία

Λόγω των αυξημένων απαιτήσεων ασφάλειας, οι Πολιτείες δεν αποκαλύπτουν τις λεπτομέρειες σχετικά με τα συμβάντα εισβολής. Αυτό που είναι γνωστό, είναι ότι σε επίπεδο Πολιτείας δόθηκε μικρή προσοχή στη σπουδαιότητα της ασφάλειας των δικτύων, μέχρι τη στιγμή που εμφανίστηκε ένα σημαντικό συμβάν ασφάλειας στο οποίο οι προσωπικές πληροφορίες και οι πληροφορίες μισθοδοσίας 600 υπαλλήλων και 7 συμβούλων χάθηκαν. Μια συσκευή αποθήκευσης δεδομένων κλάπηκε από ένα γραφείο, και αυτή η συσκευή είχε αποθηκευμένες τις παραπάνω πληροφορίες.

3.7.1.3.3.1 Πολιτική Ασφάλειας *(Security Policy)*

Τη χρονική στιγμή της κλοπής, η πολιτεία δεν διέθετε μια αποτελεσματική, γραπτή πολιτική. Η Πολιτεία εφάρμοσε την πολιτική ασφάλειας δύο μήνες μετά την παραβίαση της ασφάλειας.

3.7.1.3.3.2 Η Σχεδιασμένη Απάντηση (*Planned Response*)/Η Συλλογή Δεδομένων *(Data Collection)*

Η Πολιτεία δεν διέθετε ένα σχέδιο απάντησης ή ένα πλάνο συλλογής δεδομένων. Η ύπαρξη μιας αποτελεσματικής πολιτικής ασφάλειας θα μπορούσε να αποτρέψει την απώλεια των δεδομένων και τις επακόλουθες ευθύνες που υπέστη η Πολιτεία.

3.7.1.4 Συμπεράσματα

Από τον τρόπο με τον οποίο οι τρείς διαφορετικοί οργανισμοί προετοιμάστηκαν και αντιμετώπισαν τις απειλές ασφάλειας, διαφάνηκαν τρία συμπεράσματα: ***να υπάρχει μια καθαρή πολιτική, να υπάρχει άσκηση συνεχών επανεκτιμήσεων, να γίνεται χρήση των προηγούμενων λαθών για μάθηση και βελτίωση.***

3.7.1.4.1 Καθαρή Πολιτική (Clear Policy)

Είναι απαραίτητη μια διαυγής και αποτελεσματική πολιτική η οποία θα είναι ευρέως διαδεδομένη και οικεία στους υπαλλήλους. Η καθαρά ορισμένη πολιτική της εταιρείας υπηρεσιών υγείας την βοήθησε να απαντήσει αποτελεσματικά στην εισβολή στο δίκτυό της. Η πολιτική της είναι η ακόλουθη:

1. Τα ονόματα πρόσβασης (*user ID*) και οι κωδικοί πρόσβασης (*password*) είναι εμπιστευτικά και δεν πρέπει να εμφανίζονται πουθενά.
2. Οι υπάλληλοι δεν πρέπει να συνδέουν τα συστήματα της εταιρείας με άλλα δίκτυα ή με ασύρματα δίκτυα χωρίς την ανάμειξη των τεχνικών πληροφορικής.
3. Η εγκατάσταση λογισμικού στους υπολογιστές της εταιρείας ή στο δίκτυο χωρίς την ανάμειξη των τεχνικών πληροφορικής, μπορεί να προκαλέσει δυσλειτουργία στο δίκτυο ή απώλεια παραγωγικότητας και δεδομένων. Τέτοιες μη εξουσιοδοτημένες ενέργειες είναι παράνομες και υπόκεινται σε χρηματικές ποινές.
4. Προσωπικό λογισμικό, μη εξουσιοδοτημένο λογισμικό ή παράνομο λογισμικό δεν πρέπει να εγκαθίσταται στα μηχανήματα της εταιρείας.
5. Δεν πρέπει να δημιουργούνται αντίγραφα του λογισμικού της εταιρείας ή αυτό το λογισμικό να εγκαθίσταται σε προσωπικούς υπολογιστές.
6. Η φόρμα του ***χρήστη πληροφοριακού συστήματος*** (*IT*) θα πρέπει να συμπληρώνεται για όλους τους υπαλλήλους που χρησιμοποιούν το λογισμικό.

7. Αν ένας υπάλληλος διατηρεί αρχεία πληροφοριών ασθενών, εταιρικές πληροφορίες ή αρχεία με πληροφορίες υπαλλήλων σε κινητές συσκευές όπως φορητοί υπολογιστές, *PDA*, *USB* ή σε μέσα αποθήκευσης όπως *CD* ή δισκέττες, τα αρχεία θα πρέπει να είναι προστατευμένα με κωδικό ή κρυπτογραφημένα.
8. Τα αρχεία πληροφοριών ασθενών, οι εταιρικές πληροφορίες και τα αρχεία με πληροφορίες υπαλλήλων δεν θα πρέπει να διατηρούνται σε προσωπικούς υπολογιστές που δεν ανήκουν στην εταιρεία.
9. Οι υπάλληλοι δεν πρέπει να απενεργοποιούν το λογισμικό προστασίας από ιούς ή οποιοδήποτε άλλο λογισμικό χωρίς την ανάμειξη των τεχνικών πληροφορικής.
10. Οι υπολογιστές, το λογισμικό του συστήματος και το *hardware* θα πρέπει να αγοράζεται μόνο μέσω του τμήματος *IT*.
11. Οι προϊστάμενοι και η διοίκηση θα πρέπει να φροντίζουν ώστε οι υπάλληλοι να τηρούν αυτή την πολιτική.

Ωστόσο, παρόλο που υπάρχει γραπτή πολιτική που είναι συγκεκριμένη και καλύπτει πολλά θέματα, μικρές είναι οι επιπτώσεις για τους υπαλλήλους που δεν την ακολουθούν πλήρως. Μια γραπτή πολιτική που όμως δεν ακολουθείται είναι το ίδιο αναποτελεσματική όσο και η απουσία πολιτικής.

3.7.1.4.2 Συνεχής Επανεκτίμηση (Continuous Reassessment)

Καθώς οι απειλές εξελίσσονται συνεχώς ώστε να παρακάμπτουν την άμυνα που αναπτύσσεται, η ασφάλεια των υπολογιστικών συστημάτων απαιτεί συνεχή έλεγχο και εκτίμηση των υπαρχόντων συστημάτων. Η σχολική περιφέρεια ανέφερε μόνο το συμβάν ασφάλειας που περιλάμβανε την παραβίαση του εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Έτσι η ευθύνη τους είναι μηδαμινή, δεδομένης της απουσίας γραπτής πολιτικής ασφάλειας και της μη αποτελεσματικής τοπολογίας. Ενώ συνεχίζουν την υπάρχουσα πολιτική διαχείρισης *IT* και αγοράζουν *hardware* και λογισμικό αποκεντρωμένα και ανεξάρτητα, η περιφέρεια των σχολείων προχωρά προς την ολοκλήρωση των συστημάτων της. Καθώς τα συστήματά της γίνονται πιο εύκολα προσπελάσιμα, μέσω του διαδικτύου, περιμένουμε ότι αυτό θα αυξήσει δραματικά τον αριθμό και τη σοβαρότητα των προσπαθειών εισβολής και από εξωτερικούς αλλά και από εσωτερικούς παράγοντες. Καθώς προσπαθούν να βελτιώσουν την τοπολογία του δικτύου τους προσθέτοντας *DMZ* και πρόσθετα συστήματα ανίχνευσης εισβολών, η απουσία πολιτικής ασφάλειας πιθανώς θα οδηγήσει σε νέες και πιο σοβαρές παραβιάσεις ασφάλειας.

Όταν το σύστημά τους επηρεάστηκε από την εγκατάσταση μη εξουσιοδοτημένου και κακόβουλου λογισμικού, η εταιρεία υπηρεσιών υγείας μπόρεσε να αντιδράσει γρήγορα, αναγνώρισε το πρόβλημα και αναγνώρισε και ανέφερε ένα νέο τύπο αδυναμίας. Οι επανεκτιμήσεις της ασφάλειας του δικτύου είναι μια διαρκής προσπάθεια, στην πολιτική ασφάλειας των οργανισμών.

3.7.1.4.3 Η Μάθηση από Προηγούμενα Λάθη

Η εταιρεία υπηρεσιών υγείας έχει σαν πρακτική, να εξετάζει παραβιάσεις δικτύων και μελέτες περιπτώσεων από άλλες εταιρείες. Επίσης καταγράφει μια λεπτομερή αναφορά κάθε παραβίασης του συστήματος και χρησιμοποιεί αυτές τις πληροφορίες για να βελτιώσει μακροπρόθεσμα την ασφάλεια του συστήματος. Ο σκοπός της εταιρείας είναι

να μάθει από τα λάθη της και να βρει τρόπους να καλύψει τα κενά της ασφάλειας. Ο υπάλληλος που εγκατέστησε ένα μη εξουσιοδοτημένο λογισμικό το οποίο τελικά αποδείχτηκε κακόβουλο, δεν είχε τελικά κυρώσεις και αυτό δημιουργεί ένα μεγάλο κενό στην πολιτική της εταιρείας. Η εταιρεία γνωρίζει πολύ καλά ότι η απειλή των κυρώσεων και των τιμωριών όταν δεν υπάρχει συμβατότητα με την πολιτική της ασφάλειάς της, δεν είναι συνεπής με τις ποινές που επιβάλλονται και οι οποίες θα έπρεπε να περιλαμβάνουν αυστηρές επιπλήξεις και απόλυση. Όσο αναγνωρίζουν ότι η πολιτική της εταιρείας είναι αναποτελεσματική ως προς την τιμωρία των υπαλλήλων, δεν μπορούν να κάνουν κάτι γι' αυτό το θέμα.

Το συμβάν ασφάλειας της Πολιτείας, δηλαδή ένας κλεμμένος φορητός υπολογιστής με τα προσωπικά δεδομένα των υπαλλήλων, ήταν ένα συμβάν πολυδάπανο από άποψη χρημάτων και φήμης. Σε απάντηση η Πολιτεία δημιούργησε την δική της πολιτική ασφάλειας. Η πολιτική αυτή παρέχει λεπτομέρειες σχετιζόμενες με τη φυσική ασφάλεια και την διαχείριση των δεδομένων, την πρόσβαση και τον έλεγχο των λογαριασμών, την προσωπική χρήση και τις περιπτώσεις απαγόρευσής της, όπως επίσης συγκεκριμένες επιβολές και κυρώσεις. Όταν άρχισε αυτή η πολιτική να εφαρμόζεται, σταμάτησαν και τα συμβάντα κενών ασφάλειας.

3.7.2 Λύσεις και Προτάσεις

Η αποτελεσματική ετοιμότητα και αντίδραση στις εισβολές βασίζεται σε ένα συνδυασμό πολιτικών και διαδικασιών, δέσμευσης της εταιρείας και διάθεσης συνεργασίας από τους υπαλλήλους. Μια ιδεατή πολιτική ασφάλειας και μια ιδεατή τοπολογία ασφάλειας αποτελούν το ιδανικό μοντέλο της εταιρικής ασφάλειας.

3.7.2.1 Η Ιδεατή Πολιτική Ασφάλειας *(Ideal Security Policy)*

Υπάρχουν πολλές προκλήσεις στην προσπάθεια διαμόρφωσης μιας στέρεας και αποτελεσματικής πολιτικής ασφάλειας των υπολογιστών και των δικτύων. Στην προσπάθεια αυτή θα πρέπει να εξεταστούν οι εξωτερικοί πελάτες, οι εσωτερικοί πελάτες και οι υπάλληλοι, οι στόχοι της εταιρείας και οι αναδυόμενες απειλές της ασφάλειας. Οι οργανισμοί θα πρέπει να σταθμίσουν το κόστος της προστασίας του δικτύου τους απέναντι στην πιθανότητα σοβαρών συμβάντων ασφάλειας. Επίσης θα πρέπει να ληφθούν υπόψη και οι παράγοντες της εσωτερικής πολιτικής της εταιρείας. Για παράδειγμα, η εταιρεία υπηρεσιών υγείας είχε να αντιμετωπίσει το πρόβλημα της ανισότητας ανάμεσα στις ανάγκες και στις επιθυμίες της διοίκησης και στην ασφάλεια λειτουργίας. Η διοίκηση και το ανώτερο προσωπικό απαιτούν ηλεκτρονικό ταχυδρομείο βασισμένο στο *web*, όπως είναι το *HotMail* ή το *Yahoo*, παρόλο που οι διαδρομές αυτών των ηλεκτρονικών ταχυδρομείων παραμένουν απροστάτευτες από τα φίλτρα ηλεκτρονικού ταχυδρομείου του οργανισμού. Θα πρέπει επίσης να σταθμιστούν και άλλοι παράγοντες πολιτικής, όπως είναι ο τρόπος με τον οποίο θα ξοδευτεί ο προϋπολογισμός ασφάλειας του τεχνολογικού τμήματος. Θα πρέπει δηλαδή ο οργανισμός να αγοράσει νέους υπολογιστές ή να αναβαθμίσει την αντιιϊκή προστασία; Αν το δίκτυο παραβιαστεί από έναν εισβολέα, το τμήμα *IT* μπορεί να αποφασίσει να απαγορεύσει την πρόσβαση σε άλλες εφαρμογές ή συστήματα, έτσι ώστε να παρατηρήσει την εισβολή καθώς αυτή εξελίσσεται για να βρει τρόπους να θωρακίσει το σύστημα στο μέλλον. Αυτή η διερεύνηση είναι απαραίτητη, ειδικά όταν αφορά σε μια νέου είδους απειλή, παρόλο που η διοίκηση της εταιρείας μπορεί να την αποδοκιμάζει. Πιο κάτω θα αναλύσουμε το πλαίσιο ή το μοντέλο για την ιδεατή πολιτική ασφάλειας.

3.7.2.1.1 Σκοπός (Purpose)/Στόχος (Goal)

Ο σκοπός της πολιτικής ασφάλειας είναι να δηλώσει με επίσημο τρόπο ***«τους σκοπούς, τους στόχους, τους κανόνες και τις επίσημες διαδικασίες που βοηθούν στον ορισμό της ασφάλειας και της αρχιτεκτονικής του οργανισμού»*** (*Robert Shimonski, 2004).* Επιπλέον με αυτό το πλαίσιο, οι πολιτικές ασφάλειας θα πρέπει να απευθύνονται σε επτά βασικές λειτουργίες: **1)** Θα πρέπει να είναι κατανοητές, **2)** Θα πρέπει να είναι ρεαλιστικές, **3)** Θα πρέπει να είναι συνεπείς, **4)** Θα πρέπει να είναι δυνατόν να επιβληθούν, **5)** Θα πρέπει να έχουν καταγραφεί, διανεμηθεί και να έχουν γίνει κατανοητές, **6)** Θα πρέπει να είναι ευέλικτες και **7)** Θα πρέπει περιοδικά να αναθεωρούνται.

3.7.2.1.2 Παραμετροποίηση (Customization)

Η πολιτική ασφάλειας θα πρέπει να παραμετροποιείται ανάλογα με τα χαρακτηριστικά του κάθε οργανισμού. Η πολιτική ασφάλειας θα πρέπει να παρέχει λογικές προσδοκίες για ιδιωτικότητα από τους υπαλλήλους. Θα πρέπει να υπάρχουν λίστες διαδικασιών που θα ακολουθούνται σε περιπτώσεις που ελέγχεται η ασφάλεια από το τμήμα *IT*, ειδικά όταν προσκρούει στην παραγωγικότητα ή στην ιδιωτικότητα των υπαλλήλων. Για παράδειγμα, θα πρέπει να περιλαμβάνονται τα συγκεκριμένα άτομα που θα ειδοποιούνται όταν γίνεται έλεγχος στον υπολογιστή ενός υπαλλήλου (ο προϊστάμενος του υπαλλήλου και άλλοι στην αλυσίδα της διοίκησης) ή σε ένα σύστημα αρχείων που χρησιμοποιείται από πολλούς υπαλλήλους.

3.7.2.1.3 Ορισμός των Κεφαλαίων (Assets) του Οργανισμού/Η Ανάλυση του Κινδύνου (Risk Analysis)

Ο *Danchev* (2003) προτείνει μια στρατηγική για να καθοριστούν τα κεφάλαια (*assets*) ενός οργανισμού και η ανάλυση του κινδύνου. Προτείνει αναγνώριση των κεφαλαίων της εταιρείας, προσδιορισμό των πιθανών κινδύνων και μια διαρκή διαδικασία. Τα κεφάλαια του οργανισμού θα πρέπει να καθοριστούν ώστε να είναι βέβαιη η προστασία τους. Θα πρέπει να εξεταστεί από ποιόν πρέπει να προστατευθούν τα κεφάλαια της εταιρείας και στη συνέχεια να προσδιοριστούν οι πιθανοί κίνδυνοι. Τέλος, να οριστεί μια διαδικασία για συνεχή ή τουλάχιστον περιοδική επανεξέταση ώστε να καθορίζονται νέα κεφάλαια.

Επίσης πρέπει να γίνει απαρίθμηση και να δοθεί προτεραιότητα στα κρίσιμα κεφάλαια του οργανισμού (κατηγορίες, συστήματα, διαδικασίες). Το *hardware*, τα δίκτυα και το λογισμικό, θα πρέπει να συμπεριληφθούν στη διαδικασία ανάλυσης κινδύνου. Κατά την εξέταση του *hardware*, θα πρέπει να συμπεριληφθούν όλοι οι εξυπηρετητές, οι υπολογιστές (φορητοί και μη) τα φορητά μέσα αποθήκευσης *(CD, USB*).

Τα δίκτυα που παρέχουν πρόσβαση έξω από την εταιρεία για τους υπαλλήλους, τους πελάτες και τους συνεργάτες, θα πρέπει να ληφθούν υπόψη. Θα πρέπει να εξεταστεί η ασφάλεια του σημείου εισόδου, είτε αυτό είναι *VPN (Virtual Private Network*) είτε τηλεφωνική σύνδεση. Διάφορες μέθοδοι για τη διασφάλιση της ασφάλειας είναι η απαγόρευση πρόσβασης σε συγκεκριμένες εφαρμογές ή συστήματα και οι περιορισμοί στη διάρκεια κατά την οποία είναι ενεργός ένας κωδικός πρόσβασης.

Το απαρχαιωμένο λογισμικό και οι διορθώσεις λογισμικού, αποτελούν αδυναμίες και πρέπει να προσδιορίζονται. Επίσης λογισμικό που δεν είναι κρυπτογραφημένο και οι εφαρμογές ανταλλαγής αρχείων *(Kazaa, Sharereactor, E-Donkey*) είναι πιθανές αδυναμίες, όπως και το λογισμικό *Messaging*, το λογισμικό διασκέδασης ή και το ελεύθερο λογισμικό που έρχεται από άγνωστες πηγές.

3.7.2.1.4 Η Διαχείριση της Απειλής (Threat Management)

Ο οργανισμός θα πρέπει να εκτελέσει μια ανάλυση κινδύνων *(risk analysis)*, προσδιορίζοντας τα κεφάλαια του οργανισμού και καθορίζοντας ποιοί θα θέλουν πρόσβαση σε αυτά, χρησιμοποιώντας την ***αρχή του ελάχιστου προνομίου*** *(principal of least privilege)*, ή αλλιώς δίνοντας τη μικρότερη δυνατή πρόσβαση που χρειάζεται για να εκτελεστούν οι αντίστοιχες δραστηριότητες. Τα κεφάλαια του οργανισμού μπορεί να περιλαμβάνουν προσωπικές πληροφορίες, δεδομένα πελατών, πνευματική ιδιοκτησία ή πρόσβαση σε ηλεκτρονικό ταχυδρομείο ή στο διαδίκτυο. Αυτά τα κεφάλαια συνήθως χρησιμοποιούνται από υπαλλήλους, συνεργάτες (για παράδειγμα ένα εξωτερικό δίκτυο), πωλητές, πελάτες (χρήστες που λαμβάνουν υπηρεσίες πληροφορίας ή αναβαθμίσεις) ή γενικά χρήστες του διαδικτύου. Η πολιτική πρόσβασης θα πρέπει να ορίζει αυτές τις ομάδες και να προσδιορίζει ρόλους μέσα σε αυτές τις ομάδες. Για παράδειγμα, ένας υπάλληλος μπορεί να έχει το ρόλο του προϊστάμενου, του διαχειριστή ή του λογιστή. Η πρόσβαση προς τα κεφάλαια της εταιρείας θα πρέπει να οριστεί για κάθε ρόλο, συμπεριλαμβανομένης της πρόσβασης στο ηλεκτρονικό ταχυδρομείο και στο διαδίκτυο. Τα εργαλεία επιβολής της πολιτικής συνήθως ελέγχουν: **1)** Ποιος είσαι (αυθεντικοποίηση/*authentication*), **2)** Τι θέλεις να κάνεις (εξουσιοδότηση/*authorization*), **3)** Γιατί θέλεις να το κάνεις (ο ρόλος που έχεις).

Η διαχείριση της απειλής χωρίζεται σε ***φυσικές απειλές ασφάλειας*** *(on-site physical security threats)* που συμβαίνουν στο δίκτυο του οργανισμού και τις ***απειλές του διαδικτύου*** *(internet threats)*. Οι φυσικές απειλές ασφάλειας εκμεταλλεύονται τους κωδικούς πρόσβασης, την προστασία από ιούς, τα φορητά μέσα αποθήκευσης και την διαχείριση των συμβάντων. Η δημιουργία των κωδικών πρόσβασης είναι ένα σημαντικό έργο στο οποίο συνήθως δεν δίνεται μεγάλη σημασία, λόγω της αύξησης των συστημάτων και των λογαριασμών που χρειάζονται προστασία με κωδικούς. Θα πρέπει να υπάρχει η πολιτική, ώστε κάθε λογαριασμός να αποτελείται από έναν κωδικό που να είναι μοναδικός. Δεν θα πρέπει να χρησιμοποιείται ο ίδιος κωδικός δια μέσου των συστημάτων, καθώς αν ένας κωδικός κλαπεί, θα είναι διαθέσιμη πλήρης πρόσβαση. Επίσης δεν θα πρέπει να χρησιμοποιούνται κοινές και γνωστές λέξεις σαν κωδικοί πρόσβασης, όπως ονόματα παιδιών, γενέθλια ή αριθμός κοινωνικής ασφάλισης και θα πρέπει να περιλαμβάνουν αριθμούς και σύμβολα.

Η αυτόματη γήρανση των κωδικών πρόσβασης θα πρέπει να χρησιμοποιείται για κάθε εφαρμογή του συστήματος. Οι χρήστες ενθαρρύνονται να αλλάζουν τους κωδικούς πρόσβασης πριν εκπνεύσει η διάρκεια των κωδικών. Θα τους επιτρέπεται να χρησιμοποιούν πάλι τον ίδιο κωδικό, μετά από την πέμπτη φορά που αλλάζουν τον κωδικό πρόσβασης. Όσο είναι πρακτικό, οι οργανισμοί θα πρέπει να εξετάσουν τη χρήση μηχανισμών αυθεντικοποίησης δύο παραγόντων όπως *RSA SecureID* για την ασφάλεια των *VPN* και να απαιτούν υπογραφές δημόσιου κλειδιού για την αυθεντικοποίηση της πηγής των ηλεκτρονικών μηνυμάτων.

Ο *Danchev* (*2003*) προτείνει ότι οι οργανισμοί θα πρέπει να δομήσουν την πολιτική ασφάλειας στην αποκλειστική καθοδήγηση των υπαλλήλων στον τρόπο που πρέπει να δουλέψουν με τους υπολογιστές και μέσα στον ψηφιακό κόσμο, ώστε να αποφύγουν την έκθεση στους ιούς υπολογιστών. Προτείνει να μην ανοίγουν οι υπάλληλοι αρχεία τα οποία έρχονται από άγνωστες πηγές. Κατ' ελάχιστο, όλα τα αρχεία και τα προγράμματα θα πρέπει να ελέγχονται από ένα ενημερωμένο λογισμικό ελέγχου ιών, πριν τα ανοίξουν οι υπάλληλοι, ανεξάρτητα από τον τύπο αυτών των αρχείων (π.χ. *.exe, .bat,.com,.doc)*. Οι πλήρεις έλεγχοι των δίσκων θα πρέπει να προγραμματίζονται και να γίνονται τουλάχιστον μια φορά την εβδομάδα, χρησιμοποιώντας ενημερωμένες

υπογραφές ιών. Η προστασία από τους ιούς δεν θα πρέπει να απενεργοποιείται για κανένα λόγο, παρά μόνο σαν απόφαση του τμήματος *IT* ή του τμήματος ασφάλειας.

Τα φορητά μέσα αποθήκευσης (*CD, USB*, δισκέττες) θα πρέπει να ελέγχονται ώστε η χρήση τους να πρέπει να περιορίζεται μόνο στα μηχανήματα της εταιρείας. Δεν θα πρέπει να επιτρέπεται η πρόσβαση στα μέσα αποθήκευσης που έρχονται από έξω. Αν είναι απαραίτητο να χρησιμοποιηθούν τέτοια μέσα, θα πρέπει να υπάρχει μέριμνα ώστε να ελεγχθούν για την ύπαρξη κακόβουλου λογισμικού. Επίσης στην πολιτική ασφάλειας θα πρέπει να περιλαμβάνεται μια περιοδική αποθήκευση του συστήματος, ο έλεγχος και η συντήρηση του συστήματος.

Εφόσον κάθε κατάσταση παραβίασης της ασφάλειας διαφέρει, οι οργανισμοί θα πρέπει να προκαθορίσουν και να δημιουργήσουν ένα πλάνο απάντησης στις εισβολές, που θα παρέχει μια γενική επισκόπηση για τον τρόπο αντίδρασης στις αδυναμίες. Μέσα στο πλάνο απάντησης θα πρέπει να υπάρχει εξουσιοδότηση για κλείσιμο των συστημάτων στην περίπτωση που πρέπει να προστατευθούν σημαντικά δεδομένα και συστήματα. Ο οργανισμός θα πρέπει να έχει σε ετοιμότητα εκπαιδευμένο προσωπικό ικανό να χρησιμοποιήσει την τεχνολογία δικανικής ανάλυσης για την ανίχνευση των βημάτων μιας εισβολής. Ο οργανισμός θα πρέπει επίσης να χρησιμοποιεί τα συμβάντα ασφάλειας ως εργαλείο εκπαίδευσης, ανανεώνοντας την πολιτική ασφάλειας και την τοπολογία αν χρειάζεται.

Ο *Danchev (2003)* αναγνώρισε τις απειλές που προέρχονται από το διαδίκτυο και περιλαμβάνουν την εμφάνιση *web* σελίδων, το ηλεκτρονικό ταχυδρομείο, τα άμεσα μηνύματα (*Instant Messaging, IM*), την εγκατάσταση μη εξουσιοδοτημένου λογισμικού και το άνοιγμα αρχείων που προέρχονται από άγνωστες πηγές. Προτείνει να καθορίσουν οι οργανισμοί την αποδεκτή χρήση αυτών των δραστηριοτήτων, ώστε να μην οδηγούνται σε παραβιάσεις ασφάλειας. Οι οργανισμοί πρέπει να καθορίζουν πότε και πώς θα επιτρέπεται οι υπάλληλοι να βλέπουν σελίδες *web*, να εγκαθιστούν και να ανοίγουν αρχεία, να επικοινωνούν με το ηλεκτρονικό ταχυδρομείο και το *IM*. Οι πιθανές απειλές που υπάρχουν πίσω από αυτές τις δραστηριότητες θα πρέπει να εξηγούνται με σαφήνεια στους υπαλλήλους και να συμβαδίζουν πάντα με την παρακολούθηση για παράνομες δραστηριότητες.

Επιπλέον απειλές μέσω του διαδικτύου, περιλαμβάνουν τα εργαλεία συζήτησης μέσω *web*, η απομακρυσμένη σύνδεση υπολογιστή και τα υπολογιστικά συστήματα που ανήκουν στους υπαλλήλους. Τα εργαλεία συζήτησης μέσω *web* και τα εργαλεία που χρησιμοποιούνται για απομακρυσμένη σύνδεση εκθέτουν τους οργανισμούς σε αδυναμίες. Τα δίκτυα θα πρέπει να απαγορεύουν την πρόσβαση σε εργαλεία συζήτησης και σε εφαρμογές απομακρυσμένες, γιατί έτσι υπάρχει η πιθανότητα να εμπλακούν εισβολείς και να δημιουργήσουν απομακρυσμένη σύνδεση στο δίκτυο του οργανισμού.

Η απομακρυσμένη σύνδεση μπορεί να πάρει τη μορφή του *Virtual Private Network (VPN)* ή της πρόσβασης μέσω ασύρματης σύνδεσης. Οι λύσεις *VPN* αποτελούν μια καλή λύση για την παραγωγικότητα, αλλά δεν έχουν έλεγχο στην πρόσβαση στο δίκτυο. Τα συστήματα που χρησιμοποιούν *VPN* είναι συνδεδεμένα στο διαδίκτυο και οι δραστηριότητες μέσω διαδικτύου θα πρέπει να εξορθολογιστούν, έχοντας υπόψη τις πιθανότητες εισβολής. Τα συστήματα αυτά θα πρέπει να προστατεύονται από τείχη προστασίας, γιατί χωρίς αυτά θα είναι εκτεθειμένα σε εισβολές.

Η χρήση του *Wi-Fi*, μπορεί να δημιουργήσει προβλήματα ασφάλειας στους χρήστες των φορητών υπολογιστών, καθώς εισβολείς μπορεί να κλέψουν δεδομένα, να εγκαταστήσουν ιούς, κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*) ή μέσω

αυτών να επιτεθούν σε άλλους υπολογιστές. Το 2005 ο συνολικός αριθμός των δημόσιων σημείων εισόδου στο διαδίκτυο ξεπέρασε τις 50.000 διεθνώς, όπου περίπου τα μισά από αυτά τα σημεία βρίσκονταν στις ΗΠΑ. Καθώς ο αριθμός τους αυξάνεται με ραγδαίο ρυθμό, οι απειλές μέσω *Wi-Fi* θα αυξηθούν και αυτές σημαντικά.

3.7.2.1.5 Ισορροπία

Η ασφάλεια του οργανισμού θα πρέπει να εξισορροπήσει απέναντι στις ανάγκες των εξωτερικών πελατών, στις απαιτήσεις των εσωτερικών πελατών και στα θέματα ιδιωτικότητας των υπαλλήλων. Την ίδια στιγμή, οι οργανισμοί θα πρέπει να προσδιορίσουν τον κίνδυνο παραβίασης της ασφάλειας και να τον σταθμίσουν σε σχέση με τα ποσά που είναι διατεθειμένοι να ξοδέψουν για να εμποδίσουν και να ανιχνεύσουν εισβολές. Επίσης ένα άλλο θέμα ισορροπίας αποτελεί η ανάγκη να επιτρέπεται η πρόσβαση στους παρόχους του λογισμικού για δραστηριότητες συντήρησης, διατηρώντας ταυτόχρονα το δίκτυο και τα συστήματα ασφαλή. Η απόφαση απόδοσης πρόσβασης σε πελάτες, υπαλλήλους και εσωτερικούς πελάτες θα πρέπει να εξεταστεί με προσοχή προς όφελος της ασφάλειας του οργανισμού. Οι αποφάσεις αυτές δεν θα είναι πάντα δημοφιλείς και θα πρέπει να επανεξετάζονται περιοδικά.

3.7.2.1.6 Εκτέλεση/Διανομή

Η πολιτική ασφάλειας του οργανισμού θα πρέπει να είναι διαθέσιμη σε όλους τους υπαλλήλους, σε ηλεκτρονική και σε γραπτή μορφή. Η πολιτική θα πρέπει να επανεξετάζεται σε τακτική βάση και αν χρειάζεται να γίνονται αλλαγές. Οι σημαντικές αλλαγές, οι προσθήκες και οι διαγραφές της πολιτικής ασφάλειας είναι απαραίτητο να γίνονται γνωστές στους υπαλλήλους.

Η πολιτική της εταιρείας δεν θα πρέπει μόνο να γίνεται γνωστή στους υπαλλήλους, αλλά οι υπάλληλοι θα πρέπει να δίνουν τη συγκατάθεσή τους για την τήρηση αυτής της πολιτικής, δραστηριότητα που θα πρέπει να ανανεώνεται μια φορά το χρόνο.

3.7.2.1.7 Επιβολή και Κυρώσεις

Απαραίτητη είναι η δημιουργία μιας λίστας κυρώσεων και η επιβολή αυτών των κυρώσεων σε περιπτώσεις παραμέλησης της πολιτικής ασφάλειας. Είναι απαραίτητο να οριστούν με σαφήνεια η κατάλληλη χρήση, η απαγορευμένη χρήση και η προσωπική χρήση, μαζί με τους τύπους των δραστηριοτήτων που απαιτούν έγκριση από τους διαχειριστές του συστήματος, ή έγκριση από την ιεραρχία. Στη συνέχεια να ορίζονται με σαφήνεια οι πειθαρχικές δράσεις σε περιπτώσεις παραβίασης της πολιτικής ασφάλειας, όπως επίσης και οι κυρώσεις και οι νομικές διαδικασίες για τέτοιου είδους παραβιάσεις που γίνονται από τους παρόχους.

Οι προϊστάμενοι είναι υπεύθυνοι για τη διασφάλιση της συγκατάθεσης των υπαλλήλων σχετικά με την τήρηση της πολιτικής ασφάλειας. Η χρήση που κάνουν οι υπάλληλοι είναι δυνατόν να παρακολουθείται, μετά από αίτημα του προϊστάμενου, της διεύθυνσης ή του τμήματος ανθρώπινων πόρων και σε περίπτωση που υπάρχουν υπόνοιες ύποπτης συμπεριφοράς ο λογαριασμός του χρήστη θα πρέπει να απενεργοποιείται. Στην συνέχεια θα πρέπει να αναλύονται τα αρχεία του συγκεκριμένου λογαριασμού, ώστε να διαπιστωθεί το εύρος της παραβίασης της ασφάλειας και να ακολουθείται η διαδικασία των κυρώσεων.

3.7.2.1.8 Επανεξέταση (Revision)

Θέτουμε το στόχο να επανεξετάζουμε ανά έτος την πολιτική ασφάλειας. Η κατανόηση και η γνώση των αδύναμων σημείων του συστήματος, η δημιουργία στόχων για τη διόρθωση των αδυναμιών και την ανακάλυψη πιθανών νέων αδυναμιών, η μάθηση από παλαιότερα συμβάντα και από τις διορθωτικές κινήσεις που έγιναν και τέλος η δημιουργία και η υλοποίηση πολιτικών ελέγχου και εξέτασης είναι απαραίτητα βήματα στην επανεξέταση της πολιτικής ασφάλειας.

3.7.2.2 Ιδεατή Τοπολογία Ασφάλειας *(Ideal Security Topology)*

Αν και κάθε δίκτυο είναι μοναδικό, υπάρχουν βασικές τεχνικές που μπορούν να χρησιμοποιηθούν για να ελαχιστοποιήσουν τις παραβιάσεις. Οι εισβολείς και τα λογισμικά ιών χρησιμοποιούν τις τεχνικές, όχι μόνο για να εισδύσουν στα δίκτυα αλλά και για να συλλέξουν πληροφορίες που θα τις χρησιμοποιήσουν για να αποδυναμώσουν τα δίκτυα. Υπάρχουν βασικά μέτρα που μπορούν να υλοποιηθούν τα οποία ενισχύουν την προστασία του δικτύου και αποθαρρύνουν τους εισβολείς. Αν μια εταιρεία δεν έχει υπαλλήλους για την ενασχόληση με τα θέματα ασφάλειας του δικτύου, θα πρέπει να προσλάβει μια εταιρεία ή έναν πάροχο που θα βοηθήσει στην ασφάλιση του δικτύου. Τα βασικά μέτρα που θα πρέπει να ακολουθηθούν στην δημιουργία μιας ιδεατής τοπολογίας δικτύου είναι:

1. ***Edge Network***

   I. ***Πάροχοι υπηρεσιών :*** Πολλοί πάροχοι υπηρεσιών διαδικτύου παρέχουν επιθέσεις άρνησης παροχής υπηρεσίας (*DoS)* και πρότυπα ειδοποίησης. Αν και τα τείχη προστασίας έχουν σχεδιαστεί για να απομακρύνουν τις επιθέσεις *DoS*, αυτή η προσφορά επιτρέπει στα τείχη προστασίας να λειτουργήσουν χωρίς τον πρόσθετο φόρτο των επιθέσεων *DoS*. Περιορίζοντας οποιαδήποτε περιττή κίνηση στα συστήματα του δικτύου ενισχύεται η ποιότητα των υπηρεσιών προς τον οργανισμό και τους πελάτες. Η λήψη ειδοποιήσεων για πιθανές αδυναμίες μπορεί να βοηθήσει στην έγκαιρη λήψη ενεργειών ασφάλισης του δικτύου.

   II. ***Περιφερειακά συστήματα:*** Θα πρέπει να υλοποιείται διαχωρισμός της λειτουργίας του τείχους προστασίας από τους περιφερειακούς δρομολογητές. Ένας περιφερειακός δρομολογητής θα πρέπει να έχει έναν ελάχιστο αριθμό υπηρεσιών. Υπηρεσίες όπως *FTP*, *TFTP*, *Telnet* θα πρέπει να χρησιμοποιούνται μόνο όταν είναι απόλυτα απαραίτητο. Η πρόσβαση στην κονσόλα (*console access*) αποτελεί τον πιο σίγουρο τρόπο για τη διαχείριση μιας συσκευής δικτύου, ελαχιστοποιώντας την δυνατότητα πρόσβασης στο διαδίκτυο. Εφαρμογές όπως η *IP-Reach*, επιτρέπουν την διαχείριση ενός σημείου πρόσβασης που μπορεί να συνδέεται με φυσικό τρόπο με τον δρομολογητή.

      - ***Ασφάλεια:*** Οι περιφερειακοί δρομολογητές θα πρέπει να περιέχουν λίστες πρόσβασης και φίλτρα ώστε να επιτρέπουν τη διαχείριση σε μικρό εύρος διευθύνσεων *IP*, κατά προτίμηση από την πλευρά του ιδιωτικού δικτύου του οργανισμού. Αν η απομακρυσμένη σύνδεση είναι απαραίτητη, θα πρέπει να χρησιμοποιούνται κρυπτογραφημένες επικοινωνίες, όπως *SSH (secure shell)*. Τα φίλτρα θα απομονώνουν τις θύρες που κινδυνεύουν περισσότερο από παραβιάσεις και δεν χρησιμοποιούνται. Για παράδειγμα, κάποιες εταιρείες χρησιμοποιούν στην πραγματικότητα τις θύρες *TCP* και *UDP* 135 ως 139 για πρόσβαση στο διαδίκτυο. Τα φίλτρα θα πρέπει να

απομονώσουν αυτές τις θύρες. Επίσης το *ICMP* θα πρέπει να χρησιμοποιείται μόνο όταν είναι απαραίτητο. Η απομόνωση του *ICMP* θα βοηθήσει περισσότερο στην απομόνωση του δικτύου από μερικές από τις πιο σοβαρές παραβιάσεις.

III. ***Τείχος προστασίας:*** Ένα τείχος προστασίας θα πρέπει να μπορεί να ελέγχει τα πακέτα, να ανιχνεύει κάθε σύνδεση, να διαπερνάει όλες τις διεπαφές του τείχους προστασίας και να επιβεβαιώνει ότι αυτές είναι έγκυρες. Αυτή η διαδικασία επιτρέπει έλεγχο των πακέτων για αδυναμίες και προβλήματα ασφάλειας.

- Το δίκτυο ανάμεσα στα τείχη προστασίας και τους περιφερειακούς δρομολογητές θα πρέπει να είναι όσο το δυνατόν ελαχιστοποιημένο. Αν υπάρχει μόνο ένας δρομολογητής και ένα τείχος προστασίας, θα πρέπει να χρησιμοποιηθεί μια μάσκα των 30 *bits* (255.255.255.252) για να ελαχιστοποιήσει το διαθέσιμο χώρο του δικτύου μέσα σε αυτή τη ζώνη.
- ***Ασφάλεια:*** Οι εξερχόμενες θύρες θα πρέπει να ελαχιστοποιηθούν. Πολλές εταιρείες ασφαλίζουν τις εσωτερικές συνδέσεις, αλλά έχουν ανοιχτές τις εξωτερικές θύρες. Αυτού του είδους η τοπολογία είναι πιθανό να ανοίξει κενά στην ασφάλεια. Μόνο οι εξωτερικές θύρες που είναι απαραίτητες για νόμιμους σκοπούς της εταιρείας θα πρέπει να είναι ανοιχτές. Σε αυτή την περίπτωση μεγάλη βοήθεια δίνουν η καταγραφή και ο έλεγχος της κίνησης.

IV. Παρακολούθηση της κίνησης/IDS/IPS:

- Υπηρεσίες όπως η *Websense* θα πρέπει να παρακολουθούν και να αναφέρουν την *web* κίνηση και να απαγορεύουν γνωστούς κακόβουλους ιστοχώρους που μεταφέρουν κώδικα στους υπολογιστές μέσω της περιήγησης στο διαδίκτυο. Τα λογισμικά *Spyware* και *Adware* μπορεί να έχουν αντίθετη επίδραση στα λειτουργικά συστήματα και να δώσουν χρήσιμη πληροφορία στους πιθανούς εισβολείς. Επίσης γενικευμένες αναφορές μπορούν να χρησιμοποιηθούν από τους διαχειριστές για να ενδυναμώσουν τις πολιτικές της εταιρείας σχετικά με την περιήγηση στο διαδίκτυο και σε αντάλλαγμα να παρέχουν υπηρεσίες με καλύτερη ποιότητα στους πελάτες και στους υπαλλήλους.
- Τα συστήματα *IDS* και *IPS* αποτελούν ένα ακέραιο κομμάτι στην ασφάλεια του δικτύου. Η τοποθέτηση συστημάτων *IDS* και *IPS,* αν γίνει σε στρατηγικά σημεία μέσα στο δίκτυο επιτρέπει στον οργανισμό να δει ποιές αδυναμίες είναι πιθανό να περάσουν από το τείχος προστασίας. Υπάρχουν ελεύθερα διαθέσιμα συστήματα *IDS*, όπως το *snort* που επιτρέπουν παρακολούθηση των δεδομένων σε πραγματικό χρόνο.

2. DMZ

I. Επιβάλλεται η χρήση μιας ζώνης *DMZ*. Μια ζώνη που έχει φυσική ή εικονική ξεχωριστή εκχώρηση με δομημένη τοπολογία ώστε να περιορίσει τις επικοινωνίες της με άλλα συστήματα της εταιρείας. Η *DMZ* ή οι εκτεθειμένοι υπολογιστές θα πρέπει να παρακολουθούνται πολύ στενά. Κάθε εξυπηρετητής ή υπολογιστής που έχει μια στατική διεύθυνση *IP*, θα

πρέπει να έχει απενεργοποιημένες όλες τις περιττές υπηρεσίες. Ο υπολογιστής θα πρέπει να έχει έναν ελάχιστο σκοπό και η επιτρεπτή κίνηση προς αυτό τον υπολογιστή θα πρέπει επίσης να ελαχιστοποιηθεί.

II. Θα πρέπει να χρησιμοποιούνται δύο διαφορετικοί υπολογιστές για το εσωτερικό και το εξωτερικό ηλεκτρονικό ταχυδρομείο. Επιτρέποντας σε έναν μόνο υπολογιστή να δρα ως εσωτερική και εξωτερική πύλη (*gateway)*, υπάρχει η πιθανότητα να χρησιμοποιηθούν ως πύλες για ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου.

3. Υπολογιστές με Σύνδεση στο Διαδίκτυο και Τοπολογία Δικτύου

I. Δεν θα πρέπει να αγνοήσουμε τους εξυπηρετητές και τους υπολογιστές. Ένα σημαντικό βήμα για την ασφάλιση του δικτύου αποτελούν τα κομμάτια κώδικα ασφάλειας και η σωστή σύνθεση του δικτύου. Έχοντας ένα τείχος προστασίας και ένα *IDS*, καλύπτουμε ένα κομμάτι μόνο του πάζλ. Ένας υπολογιστής που δεν είναι σωστά διαμορφωμένος είναι πιθανό να παραβιάσει όλους τους κανόνες ασφάλειας και να εκθέσει το δίκτυο σε κακόβουλες επιθέσεις.

- ***Διαχείριση των τμημάτων κώδικα:*** Διατηρώντας τους εξυπηρετητές και τους υπολογιστές επικαιροποιημένους με τμήματα κώδικα που διορθώνουν σφάλματα (*patch*), μπορεί να μειωθούν οι πιθανότητες έκθεσης σε κίνδυνο. Δυστυχώς πολλά τέτοια τμήματα κώδικα δίνονται στη δημοσιότητα από τους πωλητές των λειτουργικών συστημάτων εβδομάδες ή και μήνες αφού ανακαλυφθεί η αδυναμία.
- ***Εγκατάσταση lockdown:*** Οι συνηθισμένοι χρήστες δεν είναι διαχειριστές των υπολογιστών. Οι λειτουργίες του επιπέδου διαχείρισης θα πρέπει να είναι μόνο ευθύνη του τμήματος *IT*. Επιπλέον, οι μη εξουσιοδοτημένες εφαρμογές και οι συσκευές εισόδου/ εξόδου θα πρέπει να ελέγχονται.
    - Το *SecureWave* διαθέτει ένα προϊόν που επιτρέπει πλήρη έλεγχο των εφαρμογών και των συσκευών εισόδου/εξόδου. Αυτό επιτρέπει στους διαχειριστές να αρνηθούν συσκευές όπως *CD-ROM* και δισκέτες. Το *SecureWave* επιτρέπει την κρυπτογράφηση συγκεκριμένων συσκευών εισόδου/εξόδου και επίσης επιτρέπει τη χρησιμοποίηση μόνο ορισμένων τύπων συσκευών. Επίσης επιτρέπει τον έλεγχο των εφαρμογών. Κανένα αρχείο δεν επιτρέπεται να εγκατασταθεί στη μνήμη του υπολογιστή αν δεν ανήκει στην λίστα επιτρεπόμενων εφαρμογών του εργαλείου (λευκή λίστα). Έτσι έχουμε πλήρη προστασία από *adware*, *spyware, trojan horses* και ανεπιθύμητες εφαρμογές. Πολλά προϊόντα προσφέρουν έλεγχο και διαθέτουν μια λίστα από μη αποδεκτές εφαρμογές και αρχεία. Η λευκή λίστα, είναι μια λίστα αποδεκτών εφαρμογών και αρχείων. Έτσι προσφέρεται μια μικρότερη και πιο εύκολα διαχειρίσιμη λίστα.

- ***Κρυπτογράφιση Αρχείου:*** Η κρυπτογράφιση σε σκληρούς δίσκους των εξυπηρετητών και των υπολογιστών της σημαντικής ή ιδιωτικής πληροφορίας μπορεί να αποτρέψει την κλοπή πληροφορίας σε περίπτωση που κάποιος υπολογιστής κλαπεί. Οι πληροφορίες αυτές μπορούν εύκολα να προσπελαστούν χωρίς να χρειάζεται κωδικός πρόσβασης. Ακόμα και οι κωδικοί *bios* δεν μπορούν να προστατεύσουν τα δεδομένα, όπως προστατεύονται στο σκληρό δίσκο.

II. Τα εσωτερικά πρωτόκολλα και η διαχείριση του δικτύου θα πρέπει να είναι όσο το δυνατόν περιορισμένα. Για παράδειγμα, το *ICMP* θα πρέπει να επιτρέπεται από ένα υποδίκτυο προσδιορισμένο από το τμήμα *IT*. Ο λόγος είναι ότι το *ICMP* χρησιμοποιείται από πολλούς ιούς σαν ένας τρόπος ανακάλυψης, για να εισάγουν ευπάθειες σε μεγάλη κλίμακα.

3.7.3 Επίλογος

Ένα σημαντικό στοιχείο της δικανικής ψηφιακής ανάλυσης, αποτελεί η προστασία των εταιρικών δεδομένων. Όταν η προστασία αυτή αποτυγχάνει, είναι πιθανό να υπάρξει κλοπή προσωπικών δεδομένων, τεχνολογίας, *monetization*, απάτη, εκβιασμός και ακόμα απειλές εθνικής ασφάλειας. Για να διατηρήσουμε την ασφάλεια απέναντι στις απειλές εισβολής στα δίκτυα, χρειάζεται συνεχής επαγρύπνηση των οργανισμών. Ένας ιδιοκτήτης εταιρείας, διευθυντής ή διαχειριστής της ασφάλειας του δικτύου διαθέτει πολλά εργαλεία που του επιτρέπουν να προστατεύσει επαρκώς τα υπολογιστικά συστήματα και τις βάσεις δεδομένων. Δυστυχώς, συχνά οι οργανισμοί και οι άνθρωποι που δουλεύουν σε αυτούς δεν δρουν πάντα όπως πρέπει. Οι εταιρείες, αποφεύγουν να αναπτύξουν, να δημιουργήσουν και να επιβάλλουν μια πολιτική ασφάλειας. Οι υπάλληλοι των εταιρειών καταστρατηγούν τις καθιερωμένες διαδικασίες και το υλικό συχνά χάνεται. Η δημιουργία μιας αποτελεσματικής τοπολογίας δικτύου και πολιτικής ασφάλειας, όπως και η χρησιμοποίηση τεχνικών από τις εταιρείες είναι δυνατό να εμποδίσουν την απώλεια δεδομένων και τις εισβολές στα δίκτυα. Η διαφύλαξη των εταιρικών δεδομένων αποτελεί στοιχείο κλειδί στην δικανική εφαρμογή της ψηφιακής τεχνολογίας, δεδομένων των κινδύνων που απειλούν την προσωπική, εταιρική και εθνική ασφάλεια. **[13]**

3.8 Η Εκπαίδευση των Ψηφιακών Ερευνητών

Η διατήρηση των λειτουργιών σε ένα περιβάλλον έρευνας αποτελεί μια χρονοβόρα διαδικασία. Η διαδικασία αυτή επιδεινώνεται με την προσθήκη της τεχνολογίας, είτε στην εκτέλεση των ερευνών είτε όταν η ίδια η τεχνολογία είναι το αντικείμενο της έρευνας. Όταν αναλογιστούμε το ρυθμό με τον οποίο εξελίσσεται η τεχνολογία, το φορτίο της έρευνας επιδεινώνεται εκθετικά.

Τα ζητήματα με τα οποία θα ασχοληθούμε αφορούν στην εκπαίδευση και επηρεάζουν τους τομείς του προσωπικού και του προϋπολογισμού των οργανισμών. Αυτοί οι δύο τομείς είναι στενά συνδεδεμένοι και σε επίπεδο οργανισμών αλλά και σε επίπεδο υπηρεσιών προς τους πολίτες. Ο διευθυντής κάθε ομάδας και η οργανωτική δομή του οργανισμού στον οποίο ενσωματώνεται αυτή η ομάδα, καθορίζουν την πιθανότητα επιτυχίας της κάθε ψηφιακής μονάδας. Η επιτυχία της κάθε ψηφιακής μονάδας δεν εξαρτάται μόνο από το διευθυντή, αλλά και από τους διοικητικούς διαχειριστές οι οποίοι παίρνουν μέρος στη διαδικασία των αποφάσεων που αφορούν σε θέματα προϋπολογισμού, εκπαίδευσης και στελέχωσης.

Οι λόγοι για τη σωστή διαδικασία εκπαίδευσης είναι προφανείς: η αποτελεσματική και επαρκής απόδοση στο επαγγελματικό επίπεδο εξαρτάται από το ανάλογο επίπεδο εκπαίδευσης που έχει παρασχεθεί. Η αποτυχία παροχής επαρκούς εκπαίδευσης θα αφήσει τα άτομα και τους οργανισμούς έκθετους (ειδικά στην περίπτωση της συλλογής των ψηφιακών δικανικών αποδείξεων, θα τους αφήσει έκθετους σε διωκτικές και δικαστικές αρχές). Η αποτυχία επεξεργασίας των ηλεκτρονικών αποδείξεων μπορεί να έχει ως αποτέλεσμα την αθώωση ενός ύποπτου ή την αποτυχία παροχής επαρκούς προστασίας σε έναν οργανισμό κατά τη διάρκεια μιας επίθεσης. Αυτό θα επηρεάσει τα άτομα που είναι τα υποκείμενα μιας διαδικασίας έρευνας και επίσης τους οργανισμούς για τους οποίους δουλεύουν.

3.8.1 Οι Ρόλοι

Αν αγνοήσουμε τα θέματα του προϋπολογισμού, οι απαιτήσεις στελέχωσης και εκπαίδευσης περιστρέφονται γύρω από την ερώτηση:

Ποια είναι τα έργα για τα οποία απαιτούμε εκπαίδευση;

Μια πολύ γενική περιγραφή αναφέρει ότι οι ειδικοί της ψηφιακής δικανικής ανάλυσης, ***αποκτούν, αρχειοθετούν, αναλύουν*** και ***επικυρώνουν*** τις ψηφιακές αποδείξεις.

Μακροσκοπικά, μια μέθοδος καθορισμού των εκπαιδευτικών αναγκών, είναι να κατηγοριοποιήσουμε τις απαιτούμενες και επιθυμητές ικανότητες και γνώσεις, σύμφωνα με τα επίπεδα εξειδίκευσης και προαπαιτούμενης γνώσης που θα πρέπει να έχει ο εκπαιδευόμενος. Οι *Yasinsac, Erbacher, Marks, Pollitt & Sommer (2003)* πρότειναν ένα πλαίσιο *Computer/Network Forensics (CNF)* βασισμένο στα επίπεδα εξειδίκευσης κατ' αντιστοιχία με τα έργα που απαιτούνται από τον επαγγελματία. Οι συγγραφείς πρότειναν τη χρήση αυτού του πλαισίου σαν μια βάση για τον καθορισμό του βιογραφικού ψηφιακής δικανικής ανάλυσης σε επίπεδο Πανεπιστημιακής εκπαίδευσης. Το πλαίσιο *CNF* μπορεί να είναι κατάλληλο για πολλές από τις λειτουργίες που απαιτούνται από έναν επαγγελματία δικανικής ψηφιακής ανάλυσης.

Σύμφωνα με το πλαίσιο *CNF*, υπάρχει μια εξέλιξη των ικανοτήτων που απαιτούνται από τους διάφορους ρόλους, οι οποίες περιλαμβάνουν ***ικανότητες τεχνικές***, ***επαγγελματικές***, ***διαμόρφωσης πολιτικής*** και ***ικανότητες ερευνητή.*** Είναι πιθανόν ότι μπορούν να εφαρμοστούν και παρόμοια μοντέλα που καθορίζουν τις εκπαιδευτικές απαιτήσεις μιας μονάδας που ασχολείται με τις ψηφιακές έρευνες. Το πλαίσιο που

παρουσιάζουμε είναι βασισμένο σε ρόλους (*role based)* και επομένως επιτρέπει σε έναν διευθυντή να καθορίσει τα κατάλληλα επίπεδα εκπαίδευσης ή γνώσης για κάθε λειτουργικό ρόλο μέσα στη μονάδα του. Το πλαίσιο *CNF* παρουσιάζεται στον ***πίνακα 4***.

Πίνακας 4: Το πλαίσιο *CNF*

Ρόλος	***Μορφωτικό Επίπεδο***	***Εκπαίδευση***
Τεχνικός CNF	*Εισαγωγικό επίπεδο: Επιστήμη πληροφορικής, Hardware, Λειτουργικά Συστήματα, Δικανική επιστήμη, Αστικό και Ποινικό Δίκαιο*	*Εκπαίδευση σε Hardware, Δίκτυα, Ανάκτηση βασικών δεδομένων και Αναπαραγωγή Δεδομένων*
Διαμορφωτής Πολιτικής CNF	*Information Management, Δικανική επιστήμη, Assurance Knowledge Management, Enterprise Architecture*	*Εκπαίδευση σε Information Assurance, Νομικές Τεχνικές και Τεχνικές CNF*
Επαγγελματίας CNF	*Επίπεδο Τεχνικού CNF, μαθήματα υψηλού επιπέδου σε IS, Δίκτυα, Αρχιτεκτονική υπολογιστών και Δίκαιο (αστικό, ποινικό και ανάλογες διαδικασίες)*	*Εκπαίδευση Τεχνικού CNF, εκπαίδευση σε προηγμένη ανάκτηση δεδομένων και εκπαίδευση σε Νομικές διαδικασίες*
Ερευνητής CNF	*Επίπεδο Μεταπτυχιακού ή Διδακτορικού, εκτεταμένη εμπειρία σε ψηφιακή δικανική ανάλυση*	*Ειδική εκπαίδευση για συγκεκριμένες περιοχές έρευνας*

Οι τεχνικοί CNF *(CNF technicians)* είναι ικανοί να δρούν σαν ***πρώτη γραμμή πυρός*** για τα διάφορα περιστατικά και διενεργούν ***κατάσχεση, αναπαραγωγή και ανάκτηση*** των ψηφιακών αποδείξεων. Θα πρέπει να τονίσουμε ότι η γνώση γι' αυτό το ρόλο μπορεί να αποκτηθεί μέσω ενός εκπαιδευτικού οργανισμού.

Ο διαμορφωτής πολιτικής CNF *(CNF policy maker)* χρειάζεται γνώση σε ένα ευρύτερο πλαίσιο για να μπορεί να ανταπεξέλθει ως διαχειριστής (*manager*). Αν και το πλαίσιο *CNF* είναι προσανατολισμένο σε τεχνικό επίπεδο, ο ρόλος αυτός δεν είναι απαραίτητο να απαιτεί διαχειριστικές ικανότητες, για τη διαχείριση του τεχνικού προσωπικού.

Ο επαγγελματίας CNF *(CNF professional)* χρειάζεται να έχει μεγαλύτερο εύρος γνώσεων και ικανοτήτων από τον τεχνικό *CNF* σε επίπεδο επιστήμης υπολογιστών, πληροφοριακών συστημάτων και σχετικών νομικών ζητημάτων. Όταν ο τεχνικός *CNF* αντιμετωπίσει δυσκολίες στην ανάκτηση των δεδομένων, είναι αναμενόμενο ότι ο επαγγελματίας *CNF* επειδή διαθέτει περισσότερες δεξιότητες, εμπειρία και γνώσεις θα βοηθήσει στην ανάκτηση των δεδομένων. Επίσης σε αυτό το επίπεδο, σύμφωνα με τους συγγραφείς του πλαισίου *CNF*, οι νομικές γνώσεις περιλαμβάνουν ποινικό, αστικό δίκαιο και γνώσεις των δικανικών διαδικασιών.

Τέλος, ***ο ερευνητής CNF*** *(CNF researcher)* επεκτείνει το σώμα των γνώσεων σε αυτό το πεδίο. Το άτομο αυτό θα πρέπει να είναι γνώστης της περιοχής της ψηφιακής δικανικής ανάλυσης. Θα πρέπει να σημειώσουμε ότι δεν υπάρχει συγκεκριμένη εκπαίδευση εκτός από αυτήν που απαιτείται για να επιδιωχθεί μια συγκεκριμένη γραμμή έρευνας.

Ιδιαίτερη σημασία θα πρέπει να δοθεί στο να συμπεριληφθεί όλο το εύρος των δεξιοτήτων και των γνώσεων, για τα οποία η εκπαίδευση είναι απαραίτητη. Μολονότι τα έργα που συνήθως γίνονται από έναν ειδικό ψηφιακής δικανικής ανάλυσης (τεχνικό) μπορεί να περιλαμβάνουν μόνο μια όψη από τα χαρακτηριστικά ***«αποκτώ, αρχειοθετώ, αναλύω και επικυρώνω»***, συχνά μια αποτυχία της πλήρους εκτίμησης της φύσης της τεχνολογίας μπορεί να καταστήσει την ψηφιακή έρευνα ατελή και λανθασμένη.

Σε πολλά περιστατικά ανάλυσης, δεν υπήρχε πλήρης γνώση του συστήματος μέχρι τη στιγμή που άρχισε να εμβαθύνει η έρευνα. Μόλις αρχίσει η αντιμετώπιση του προβλήματος στο σύστημα, μπορεί να χρειαστεί πρόσθετη βοήθεια από έμπειρο προσωπικό για να διεκπεραιωθούν οι εργασίες ανάλυσης. Επομένως, το θέμα είναι ότι η περισσότερη γνώση (και άρα εκπαίδευση) από τους αναλυτές επιτρέπει αποτελεσματικότερη αντιμετώπιση των συμβάντων.

Μια μακροσκοπική ματιά στις δεξιότητες εστιάζει στα διακριτά έργα που εμπλέκονται σε κάθε ρόλο του πλαισίου *CNF*. Μια λίστα των θεωρήσεων και των έργων του ειδικού της δικανικής ψηφιακής ανάλυσης θα πρέπει να περιέχει:

1. Προστασία του υπολογιστή από τροποποίηση, καταστροφή, αλλοίωση των δεδομένων ή εισαγωγή κάποιου ιού,
2. Ανακάλυψη όλων των αρχείων στο υπολογιστικό σύστημα, συμπεριλαμβανομένων των κανονικών αρχείων, των διαγραμμένων, των κρυφών, των αρχείων του συστήματος, των κρυπτογραφημένων και των αρχείων που προστατεύονται από κωδικούς πρόσβασης,
3. Ανάκτηση των διαγραμμένων αρχείων που βρέθηκαν (ολική ή μερική),
4. Αποκάλυψη των περιεχομένων των κρυμμένων αρχείων, των αρχείων *swap* και *temp*,
5. Προσπέλαση (αν είναι πιθανή και κατάλληλη) των περιεχομένων των κωδικοποιημένων και προστατευμένων αρχείων,
6. Προσπέλαση των δεδομένων σε ειδικές περιοχές του δίσκου, συμπεριλαμβανομένων του χώρου του δίσκου που δεν έχει διατεθεί και του *slack space*.
7. Παροχή μιας αναφοράς ανάλυσης του συστήματος που εξετάζεται, η οποία θα περιέχει όλα τα σχετικά αρχεία και τα δεδομένα των αρχείων που ανακαλύφθηκαν. Παροχή γνωμάτευσης για το πλαίσιο του συστήματος, τη δομή των αρχείων και των δεδομένων που ανακαλύφθηκαν. Παροχή πληροφορίας πρόσβασης και ιδιοκτησίας. Παροχή γνωμάτευσης για τις προσπάθειες απόκρυψης, διαγραφής, μετατροπής, προστασίας ή κωδικοποίησης των δεδομένων. Προσθήκη οποιασδήποτε σχετικής πληροφορίας που ανακαλύφθηκε κατά την αξιολόγηση του συστήματος.
8. Παροχή δικαστικής κατάθεσης, βεβαίωσης ή διαβούλευσης αν χρειαστεί.

Θα πρέπει βέβαια να είμαστε ενήμεροι σχετικά με τη διαφορά μεταξύ της δικανικής ανάλυσης υπολογιστών και της δικανικής ανάλυσης δικτύων *(Berghel, 2003*). Η διαφορά αυτή μπορεί να δημιουργήσει προβλήματα στην παροχή της απαιτούμενης εκπαίδευσης, καθώς η παραμέληση της μιας συνιστώσας είναι πιθανό να αφήσει την εκπαίδευση του προσωπικού ατελή. Ίσως ένας καλύτερος ορισμός θα ήταν κυβερνο-δικανική ανάλυση *(cyberforensics),* καθώς η φύση των συστημάτων που εμπλέκονται περιλαμβάνει και τους υπολογιστές και τα δίκτυα. Πραγματικά, τα δεδομένα μπορεί να βρίσκονται σε ένα ευρύ φάσμα συσκευών οι οποίες μπορεί να βρίσκονται μέσα ή έξω από τον οργανισμό. Σε πολλές περιπτώσεις είναι απαραίτητη η γνώση των νομικών ζητημάτων για να διεκπεραιωθεί η ψηφιακή έρευνα. Αυτός είναι και ένας από τους λόγους που το πεδίο της ψηφιακής δικανικής ανάλυσης θεωρείται διεπιστημονικό πεδίο.

3.8.2 Η Επιλογή του Προσωπικού

Όπως είναι προφανές, ένας διευθυντής προσπαθεί να γεμίσει τον κάθε ρόλο με άτομα που έχουν τα κατάλληλα προσόντα. Ένα μέρος από αυτές τις θεωρήσεις θα πρέπει να λαμβάνει υπόψη και τις απαιτούμενες δεξιότητες που θα πρέπει ήδη να έχει κατακτήσει ο εκπαιδευόμενος, πριν ξεκινήσει την εκπαίδευσή του.

Η επιλογή προσωπικού για μια μονάδα ψηφιακής ανάλυσης είναι προβληματική: είτε η πρωταρχική οδηγία της διεύθυνσης σε αυτή τη μονάδα είναι η έρευνα και η δίωξη των επιθέσεων, είτε αυτές οι ερευνητικές εργασίες υπόκεινται σε μια ήδη καθιερωμένη περιγραφή εργασίας. Σε κάθε περίπτωση, η αξιολόγηση των γνώσεων και των ικανοτήτων του προσωπικού θα πρέπει να γίνει, ώστε να προσδιοριστεί αν υπάρχουν ελλείψεις σύμφωνα με τους ρόλους που πρέπει να εκτελεστούν για το σχεδιασμό της εκπαίδευσης.

Στο κόσμο των οργανισμών, συχνά αυτές τις εργασίες διεκπεραιώνει ο διαχειριστής του συστήματος ή του δικτύου. Στον κόσμο της παροχής υπηρεσιών στους πολίτες (ειδικότερα στην επιβολή του νόμου) οι πιθανότητες είναι πολύ πιο περιορισμένες. Εξαιτίας των νόμων και των κανονισμών που ισχύουν στους τίτλους του προσωπικού και στα έργα που εκτελούν, συχνά ο συσχετισμός του τίτλου και των απαιτούμενων δεξιοτήτων είναι αδύνατος.

Το δίλλημα που υπάρχει είναι ότι οι ερευνητές οι οποίοι παραδοσιακά ασχολούνται με την έρευνα μπορεί να μην έχουν βασικές δεξιότητες στους υπολογιστές. Ωστόσο, αυτή η τάση αλλάζει καθώς νεότεροι ερευνητές, οι οποίοι έχουν μεγαλώσει στην εποχή των υπολογιστών, γίνονται το μεγαλύτερο μέρος της δύναμης των ερευνητών. Το επίπεδο αυτών των δεξιοτήτων είναι βασικό: για παράδειγμα, ένας ερευνητής μπορεί να έχει τις δεξιότητες που απαιτούνται για να περιηγηθεί στο διαδίκτυο, να διαβάσει μηνύματα ηλεκτρονικού ταχυδρομείου και να παράγει τα βασικά έγγραφα γραφείου.

Σε πολλές περιπτώσεις, ο διευθυντής δεν έχει την πολυτέλεια να επιλέγει προσωπικό από μια ομάδα ειδικευμένων τεχνικών δικανικής ανάλυσης. Επομένως, ο διευθυντής θα πρέπει να βρει τα πρόσωπα που διαθέτουν τις καλύτερες δεξιότητες για τα έργα που θα πρέπει να εκτελέσουν.

Οι διευθυντές ίσως προτιμούν τη στελέχωση με άτομα που έχουν πιστοποιήσεις ή εμπειρία στο αντικείμενο σαν τεχνικοί. Τα άμεσα πλεονεκτήματα μπορεί να βρίσκονται στην απόκτηση μιας συγκεκριμένης ομάδας ικανοτήτων για ένα σύνολο εργασιών που απαιτούνται για το ρόλο που πρέπει να στελεχωθεί.

Οι υποψήφιοι που έχουν ένα πτυχίο είτε σε πληροφοριακά συστήματα είτε στην επιστήμη υπολογιστών έχουν ένα πλεονέκτημα καθώς καταλαβαίνουν σε μεγάλο βαθμό την υποκείμενη τεχνολογία. Αυτή η εκπαίδευση λειτουργεί σαν ένα θεμέλιο για τα

μαθήματα που είναι προσανατολισμένα στα έργα ή για την εκπαίδευση που χρειάζεται σαν συμπλήρωμα της βασικής μόρφωσης. Σε κάθε περίπτωση, όταν υπάρχει κάποια έλλειψη στη βασική εκπαίδευση θα γίνεται αποκατάσταση.

Όσον αφορά στις υπηρεσίες του πολίτη, όσοι είναι έμπειροι στην τεχνολογία υπολογιστών έχουν συνήθως τίτλους σπουδών στα πληροφοριακά συστήματα και αποτελούν ιδιωτικό προσωπικό των εταιρειών. Το προσωπικό που ασχολείται με τα πληροφοριακά συστήματα συχνά δεν έχει τίτλους έρευνας και δεν είναι σε θέση να διεξάγει μια έρευνα στον πραγματικό κόσμο. Γι' αυτό το λόγο και η προσπάθεια στελέχωσης μιας ομάδας έρευνας μοιάζει με το αίνιγμα «η κότα έκανε το αυγό ή…» στον προσδιορισμό του τι ακριβώς είναι το σημαντικότερο στην προσπάθεια της στελέχωσης. Ένας διευθυντής θα πρέπει να καθορίσει ποιές δεξιότητες είναι άμεσα απαραίτητες για τη διενέργεια μιας ψηφιακής ανάλυσης και να βρει τα καταλληλότερα άτομα για να στελεχώσει τους ρόλους και να τους δώσει την κατάλληλη εκπαίδευση.

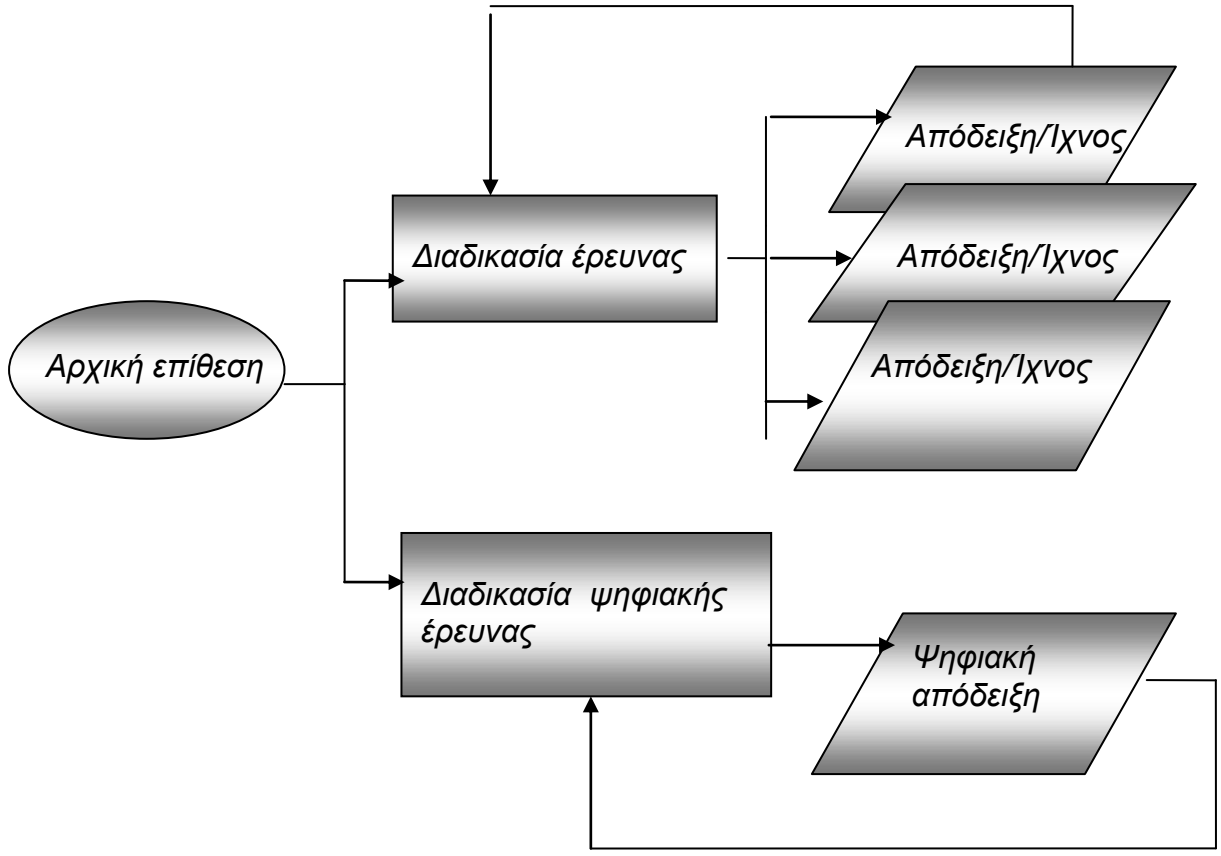
Μια έρευνα μπορεί να ξεκινήσει από μια ψηφιακή επίθεση, που μπορεί να είναι μια επίθεση *DoS* (άρνηση παροχής υπηρεσίας), μια μη εξουσιοδοτημένη πρόσβαση, μια επίθεση εισβολής στην ασφάλεια του συστήματος κ.α. Η επιλογή του προσωπικού (και η παροχή της κατάλληλης εκπαίδευσης) βασίζεται στην πρωταρχική ώθηση των ερευνών: οι έρευνες των εγκλημάτων απαιτούν πρότυπες τεχνικές έρευνας κατά την εμφάνιση του εγκλήματος, ενώ για τις ψηφιακές έρευνες μπορεί να μην χρειαστεί το προσωπικό να βγει έξω από τον ψηφιακό κόσμο. Στις ψηφιακές έρευνες η έναρξη μπορεί να γίνει είτε από την πλευρά της τεχνολογίας είτε παραδοσιακά (όπως και στα κοινά εγκλήματα). Για παράδειγμα, ένας εκβιασμός που γίνεται μέσω τηλεφώνου μπορεί να αντιμετωπιστεί με παραδοσιακό τρόπο, αντίθετα από έναν εκβιασμό που γίνεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η γνώση της λειτουργίας των τηλεπικοινωνιών δεν χρειάζεται στην αντιμετώπιση της πρώτης περίπτωσης, ενώ στη δεύτερη περίπτωση απαιτείται γνώση της διαδικασίας των μηνυμάτων του ηλεκτρονικού ταχυδρομείου και ως προς το πρωτόκολλο αλλά και ηλεκτρονικά και φυσικά. Τελικά, η αποκάλυψη του χρήστη ενός μηνύματος ηλεκτρονικού ταχυδρομείου μπορεί να οδηγήσει στον εντοπισμό ενός ατόμου ή μιας τοποθεσίας. Ωστόσο, οι ερευνητές θα πρέπει να είναι προσεκτικοί στα συμπεράσματα που βγάζουν. Η γνώση ότι ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να είναι "*spoofed*" (δηλαδή παραποιημένο για να διαστρεβλώσει την ταυτότητα του αποστολέα), δεν θα παρέχει τη δυνατότητα στον ερευνητή να προσδιορίσει το ***πώς, πού και ποιός*** έκανε την παραποίηση. Είναι απαραίτητη μια βαθύτερη γνώση των υποκείμενων πρωτοκόλλων για να προσδιοριστεί τι ακριβώς συνέβη. Η αποτυχία της κατανόησης του πώς έγινε η παραποίηση μπορεί να έχει σαν αποτέλεσμα την αποτυχία αναγνώρισης των ιχνών και την εξαγωγή λάθος συμπερασμάτων.

Όπως φαίνεται στο ***σχήμα 27***, οι εξειδικευμένες οδηγίες και οι αποδείξεις απαιτούν εξειδικευμένη γνώση ώστε να βρεθεί περισσότερη πληροφορία. Σαν αποτέλεσμα, πραγματοποιείται μια επαναληπτική διαδικασία *IPO (input-process-output)* η οποία προσθέτει στοιχεία στην παραγόμενη πληροφορία, μέχρις ότου η πληροφορία είναι επαρκής και παραχθεί κάποιο συμπέρασμα. Ο τελικός στόχος είναι να βρεθεί κάποιο πρότυπο που τελικά να οδηγεί στα πραγματικά αίτια ή στον ένοχο. Όπως φαίνεται και στο ***σχήμα 27***, προσδοκούμε ότι η αποκάλυψη μιας ψηφιακής απειλής όταν τεθεί σαν είσοδος στη διαδικασία έρευνας θα οδηγήσει τελικά σε ένα αποτέλεσμα στον «πραγματικό κόσμο».

Ο ρόλος του ερευνητή είναι να πάρει τα ανόμοια κομμάτια μιας πληροφορίας και να τα συνδέσει δημιουργώντας μια αλυσίδα αιτιότητας. Καθώς οι έρευνες επικαλύπτονται μεταξύ του ψηφιακού και του πραγματικού κόσμου, τα ευρήματα θα πρέπει να

καταγράφονται και να αξιολογούνται ώστε να χρησιμοποιηθούν σαν βάση για τη δίωξη του εγκληματία ή για να υποστηρίξουν την απομόνωση ενός εσωτερικού εισβολέα.

Δυσκολίες δημιουργούνται όταν οι επιπλέον δυσκολίες των συμβάντων που ερευνώνται εισέρχονται στην ροή των εργασιών. Οι τεχνικές έρευνας στον πραγματικό κόσμο τελικά ενώνουν τις τεχνικές έρευνας στον ψηφιακό κόσμο και γίνονται επιπρόσθετες απαιτήσεις εκπαίδευσης. Ο ρόλος του ψηφιακού ερευνητή είναι να αποκαλύψει τα ίχνη που δείχνουν το ***πώς*** και το ***ποιός*** ενός ψηφιακού εγκλήματος. Ωστόσο σε πολλές περιπτώσεις, τα ίχνη που βρίσκονται από κάποιον ψηφιακό ερευνητή δηλώνουν μόνο τις πιθανότητες που απαντούν στην ερώτηση ***ποιός***. Ενώ ένας ψηφιακός ερευνητής μπορεί να κατέχει τις δεξιότητες για να εξάγει και να εμφανίσει την πληροφορία από ψηφιακές πηγές, τα τεχνολογικά ζητήματα θα πρέπει να κατανοηθούν με προσοχή έτσι ώστε να μην αποκλειστούν οι πιθανές αιτίες της επίθεσης.



Σχήμα 27: Η ανάμειξη των ψηφιακών και μη ψηφιακών δεξιοτήτων

Για παράδειγμα, ένας ερευνητής μπορεί να βρει δικτυακά μηνύματα που παραδόθηκαν σε μια συγκεκριμένη διεύθυνση *MAC* στο δίκτυο και να βασίσει τις περαιτέρω έρευνες εστιασμένος σε αυτόν τον κόμβο του δικτύου. Σε περίπτωση που ο ερευνητής δεν λάβει υπόψη του τον τρόπο με τον οποίο οι διευθύνσεις *MAC* μπορεί να πλαστογραφηθούν, θα παραπλανηθεί και θα οδηγηθεί σε λάθος στόχους (δηλ. δεν θα αναγνωρίσει ανεπιθύμητα *ARP (Address Resolution Protocol)* μηνύματα που τροποποιούν τους *ARP* πίνακες).

Επίσης, ακολουθώντας τα ίχνη ένας ψηφιακός ερευνητής μπορεί να καταλήξει σε έρευνες στον πραγματικό κόσμο, όπως είναι η παρακολούθηση τηλεφωνικών ή οικονομικών αρχείων των υπόπτων. Οι έμπειροι διαχειριστές δικτύων οι οποίοι είναι προσανατολισμένοι στην εξέταση των δικτύων, δύσκολα ακολουθούν τα ίχνη στον πραγματικό κόσμο.

Εξ αιτίας της φύσης των ερευνών, η εκπαίδευση του προσωπικού απαιτεί την συμπλήρωση των δεξιοτήτων των μελλοντικών ερευνητών, καθώς είναι μάλλον απίθανο οι ερευνητές να διαθέτουν ικανότητες και γνώσεις διερεύνησης τόσο στον ψηφιακό, όσο και στον πραγματικό κόσμο. Επομένως, η στελέχωση παίζει σημαντικό ρόλο, και για την αναγνώριση των άμεσων διαθέσιμων δεξιοτήτων αλλά και για την επισήμανση μελλοντικών εκπαιδευτικών αναγκών του προσωπικού. Το επόμενο βήμα, αφορά στο πώς γίνεται ο προσδιορισμός των κατάλληλων δεξιοτήτων. Αν ξαναδούμε τους ρόλους *CNF*, μπορεί να φτάσουμε στο συμπέρασμα ότι οι ανάγκες της εκπαίδευσης μπορεί να αλλάζουν δυναμικά.

3.8.3 Ο Σκοπός των Λειτουργιών (Ρόλων)

Δυστυχώς, η φύση της ψηφιακής έρευνας δεν την περιορίζει σε ένα στενό πλαίσιο ερευνών. Αν ένας διευθυντής είναι αρκετά τυχερός ώστε να έχει αρκετό προσωπικό, μπορεί να μοιράσει τη δουλειά πράγμα που επιτρέπει την εκπλήρωση συγκεκριμένων έργων που δεν βασίζονται σε άλλα συστατικά της έρευνας.

Για παράδειγμα, όταν φαίνεται ότι τα δεδομένα είναι κωδικοποιημένα, ένας τεχνικός μπορεί να έχει την δυνατότητα να επεξεργαστεί αυτά τα δεδομένα. Στην ιδεατή κατάσταση, ένας εκπαιδευμένος αναλυτής θα πρέπει να έχει τα προσόντα να αναγνωρίζει την πιθανότητα παρουσίας κρυμμένων δεδομένων (κωδικοποιημένων, στεγανογραφίας κ.α.). Ο αναλυτής θα πρέπει επίσης να είναι εκπαιδευμένος σε μεθόδους αποκρυπτογράφησης παρά να δώσει την έρευνα σε ένα άλλο μέλος της ομάδας.

Για διάφορους λόγους δεν είναι επιθυμητό να εισάγουμε περισσότερα άτομα στην διαδικασία της έρευνας. Ένας λόγος είναι ότι επιπρόσθετες συνδέσεις μπορεί να αλλοιώσουν την αλυσίδα της επιτήρησης (*chain of custody)* και επίσης να βάλουν και άλλους ανθρώπινους παράγοντες στην έρευνα, χωρίς στην πραγματικότητα να χρειάζεται. Αυτό μπορεί να οδηγήσει σε προβλήματα καταγραφής, όπως επίσης και εισαγωγής νέων έργων και πόρων στον κύκλο ζωής του *project* της έρευνας. Σύμφωνα με το πλαίσιο *CNF*, ο διευθυντής θα πρέπει να διασφαλίσει το απαραίτητο επίπεδο εκπαίδευσης του προσωπικού, έτσι ώστε να αποφευχθεί η κατάσταση κατά την οποία πολλά άτομα είναι υπεύθυνα για τα τελικά αποτελέσματα μιας έρευνας. Η ιδανική κατάσταση κάθε ερευνητικής μονάδας είναι να υπάρχει ένα *cross trained* προσωπικό που να μπορεί να απαντά αποτελεσματικά σε κάθε περίπτωση επίθεσης και να διεξάγει τις έρευνες.

3.8.4 Τυποποίηση Εκπαίδευσης

Υπάρχουν τουλάχιστον τρία παραδείγματα εκμάθησης: ένα ***τυπικό μοντέλο εκπαίδευσης, η εμπειρία που αποκτάται με τη δουλειά (on the job training) και η επαγγελματική εκπαίδευση.*** Μέχρι πρόσφατα, το τυπικό μοντέλο εκπαίδευσης υστερούσε σε πολλά σημεία, καθώς τα πανεπιστήμια μόλις πρόσφατα άρχισαν να προσφέρουν μαθήματα ψηφιακής δικανικής ανάλυσης και ασφάλειας. Επιπλέον, στις θεματικές περιοχές που καλύπτονται, οι περισσότεροι φοιτητές δεν έχουν πρακτική εμπειρία.

Η εμπειρία από τον πραγματικό κόσμο συχνά υπερβαίνει το επίπεδο της λεπτομέρειας μιας τυπικής εκπαίδευσης. Ενώ είναι ανεκτίμητη, η ευρύτητα της γνώσης μπορεί να είναι σποραδική και να απαιτεί χρόνο αλλά και τις κατάλληλες συνθήκες για να αποκτηθεί περισσότερη γνώση.

Το μοντέλο της επαγγελματικής εκπαίδευσης επίσης εστιάζει σε συγκεκριμένες θεματικές περιοχές και συχνά δεν ψάχνει σε υποκείμενες αρχές και θεωρίες. Για παράδειγμα, το επαγγελματικό μοντέλο εκπαίδευσης μπορεί να προσφέρει μαθήματα και σεμινάρια από έναν πάροχο λογισμικού ή από έναν επαγγελματία εκπαιδευτή για ένα συγκεκριμένο προϊόν. Οι γενικές αρχές μπορεί να καλυφθούν στο βαθμό που αποτελούν τη βάση της εφαρμογής ενός προϊόντος λογισμικού, ωστόσο ο πάροχος μπορεί να υποθέσει ότι οι συμμετέχοντες έχουν ένα συγκεκριμένο επίπεδο γνώσης.

Μια λύση εκπαίδευσης μπορεί να υπάρξει όταν οι δεξιότητες αντιπαραβάλλονται με τα προσφερόμενα μαθήματα στο πλαίσιο της τυπικής εκπαίδευσης. Τα κενά στις δεξιότητες είναι ασφαλώς οι περιοχές για τις οποίες θα πρέπει να παρασχεθεί εκπαίδευση. Όπως αναφέραμε προηγουμένως, αυτές οι δεξιότητες του τεχνικού *CNF* προτιμώνται έναντι ενός τυπικού υπόβαθρου εκπαίδευσης.

Η παραδοσιακή επιστήμη των υπολογιστών και των πληροφοριακών συστημάτων έχει προσφέρει στους σπουδαστές το υπόβαθρο και τις δεξιότητες σε προγραμματισμό, ανάλυση, βασικά στοιχεία βάσεων δεδομένων, διαχείριση δικτύων και σε άλλες γνωστικές περιοχές ώστε να ανταπεξέλθουν στο εργασιακό περιβάλλον ενός εργοστασίου ή ενός εργαστηρίου. Ένα από τα πιο κοινά παράπονα που συνήθως ακούγονται για τα μορφωτικά ινστιτούτα είναι η έλλειψη πρακτικής εκπαίδευσης. Στην ουσία πολλοί οργανισμοί αναπτύσσουν εκπαιδευτικά προγράμματα ώστε να συμπληρώσουν τις βασικές δεξιότητες που παρέχονται από ένα τυπικό μορφωτικό ινστιτούτο. Το δίλλημα περιστρέφεται γύρω από το θέμα ***εκπαίδευση έναντι πρακτικής εκπαίδευσης.*** Πολλά τυπικά συστήματα εκπαίδευσης δείχνουν να απαξιώνουν την πρακτική εκπαίδευση επικαλούμενα ότι αυτού του είδους τα μαθήματα ανήκουν σε τάξεις ***δια βίου μάθησης*** ή σε κάποιο επαγγελματικό εκπαιδευτικό *forum*. Έτσι η τυπική εκπαίδευση σχετίζεται με την υποκείμενη θεωρία και παρέχει τις βασικές γνώσεις και δεξιότητες, όπως επίσης και με τις ικανότητες του φοιτητή να επεκτείνει τις γνώσεις του.

Για πάρα πολλούς λόγους, σπάνια το προσωπικό μπορεί να ανταπεξέλθει με τα έργα που απαιτούνται σε ένα δικανικό πλαίσιο (νομικό) το οποίο υπερβαίνει το παραδοσιακό μοντέλο πληροφοριακού συστήματος που διδάσκεται σε μια τάξη. Μόνο πρόσφατα, τα πανεπιστήμια άρχισαν να προσφέρουν μαθήματα σχετικά με τη δικανική ανάλυση.

Αυτό σημαίνει ότι οι τεχνικοί μπορεί να είναι οικείοι με τις βασικές αρχές των δικτύων αλλά δεν έχουν εμπειρία σε θέματα ασφάλειας παρά μόνο τις βασικές αρχές. Ανάλογα με το ρόλο που απαιτείται, η εκπαίδευση θα πρέπει να συμπληρώνεται με μια τυπική εκπαίδευση ή να ικανοποιείται από ένα μάθημα που καλύπτει συγκεκριμένα, τεχνικά θέματα.

3.8.5 Η Τυπική Εκπαίδευση

Μια εξέταση μιας παραδοσιακής εκπαίδευσης στην επιστήμη των υπολογιστών, μπορεί να περιέχει κάποιες δεξιότητες ή γνωστικές περιοχές που απαιτούνται για τη δικανική ανάλυση υπολογιστών. Οι γνωστικές περιοχές θα πρέπει τουλάχιστον να περιλαμβάνουν μια βασική κατανόηση της τεχνολογίας για να προσφέρουν στον ερευνητή τις δεξιότητες που χρειάζεται ως ***ερευνητής ή ως τεχνικός πρώτης ανάγκης***. Κάποια από τα μαθήματα θα πρέπει να περιλαμβάνουν τα παρακάτω:

- ***Γνώσεις γραφής σε υπολογιστή*** και εργαλεία παραγωγής προϊόντων γραφείου, που επιτρέπουν στον εκπαιδευόμενο να χειριστεί διάφορα έγγραφα χρησιμοποιώντας *OTS (Off the shelf)* προγράμματα λογισμικού. Επιπλέον, ο εκπαιδευόμενος θα πρέπει να αποκτήσει δεξιότητες στη χρήση των τυπικών εφαρμογών δικτύου, όπως είναι το ηλεκτρονικό ταχυδρομείο, οι φυλλομετρητές *web*, η μεταφορά αρχείων, όπως και άλλων εφαρμογών *peer-to-peer*.

- ***Λειτουργικά συστήματα:*** Παροχή μιας επισκόπησης των διαθέσιμων λειτουργικών συστημάτων και των διαθέσιμων εντολών για την εκτέλεση εργασιών σε επίπεδο χρήστη και διαχειριστή. Επιπλέον ο εκπαιδευόμενος μπορεί να κατανοήσει τις δομές δεδομένων σε επίπεδο συστήματος *(partition tables, file tables, directories),* όπως επίσης και δομές που σχετίζονται με την ασφάλεια *(system, group, user tables).*

- ***Με τον πολλαπλασιασμό των γραφικών διεπαφών χρηστών*** *(Graphical User Interface, GUI),* που επιτρέπουν στους χρήστες να καλούν λειτουργίες του συστήματος, πολλοί χρήστες δεν είναι πια οικείοι με τις αλληλεπιδράσεις της γραμμής εντολών. Σε πολλές περιπτώσεις όμως, η διεπαφή της γραμμής εντολών *(command line)* μπορεί να είναι η μόνη σίγουρη και ασφαλής μέθοδος για την απόκτηση των δικανικών δεδομένων από ένα σύστημα και αυτό αποτελεί μια κρίσιμη δεξιότητα του ερευνητή.

- ***Εισαγωγικός προγραμματισμός και προγραμματισμός του GUI*****:** Παρέχει τη δυνατότητα κατανόησης του κώδικα και επιτρέπει στον εκπαιδευόμενο να αναπτύξει δικές του λύσεις, όταν οι έρευνες απαιτούν λύσεις που δεν υπάρχουν στα προγράμματα *OTS*.

- ***Δομές δεδομένων και αλγόριθμοι:*** Ενισχύουν την ικανότητα του χρήστη να παρέχει λύσεις και ενισχύουν τις γνώσεις του αναλυτή για πιθανές αποδεικτικές δομές που μπορεί να εμφανιστούν κατά τη διάρκεια της έρευνας.

- ***Βασικές αρχές βάσεων δεδομένων:*** Επιτρέπουν στον ερευνητή να χειρίζεται τα δεδομένα ώστε να αναπτύξει συσχετισμούς των αποδείξεων, ή να αναπτύξει δικές του βάσεις δεδομένων για να υποστηρίξει την έρευνα.

- ***Δίκτυα και επικοινωνία δεδομένων:*** Βοηθά τον ερευνητή να αναπτύξει μια γνώση της κατάστασης των ψηφιακών σκηνών, και να παρέχει κατανόηση των πιθανών μηχανισμών που αναμιγνύονται κατά τη διάρκεια της επίθεσης. Επιπλέον οι ερευνητές πρέπει να καταλάβουν πώς θα γίνει η μόχλευση της τεχνολογίας κατά τη διάρκεια κάθε φάσης της έρευνας.

Τα μαθήματα της τυπικής εκπαίδευσης για διάφορους λόγους, είναι ατελή σε περιοχές γνώσης σχετικές με την ψηφιακή δικανική ανάλυση. Η επιλογή πρόσθετων μαθημάτων μπορεί να συμπληρώσει τα βασικά μαθήματα της επιστήμης υπολογιστών και των πληροφοριακών συστημάτων.

Τα πιο χρήσιμα μαθήματα που θα προστεθούν στο πρόγραμμα σπουδών είναι αυτά που απευθύνονται σε θέματα δικανικής ανάλυσης υπολογιστών και δικτύων. Συχνά τα θέματα αυτών των μαθημάτων, αποτελούνται από συστατικά που μαζί δημιουργούν μαθήματα σχετικά με την ανάκτηση, την ανίχνευση εισβολής, ή κάποια παρόμοια θεματική περιοχή. Αυτά τα μαθήματα δεν προσφέρονται σαν μέρος της γενικής εκπαίδευσης στην επιστήμη των υπολογιστών. Συχνά τα βρίσκουμε σαν ελεύθερα μαθήματα ή σαν μέρος της εκπαίδευσης των οργανισμών ή των βιομηχανιών.

3.8.6 Επαγγελματική Εκπαίδευση

Υπάρχουν δύο μέθοδοι μέσω των οποίων μπορούν να αποκτηθούν οι δεξιότητες για πραγματική απόκτηση, αρχειοθέτηση και ανάλυση. Η μία εμπλέκει τη μάθηση των μεθοδολογιών και των πρωτοκόλλων της ψηφιακής δικανικής ανάλυσης. Η άλλη μέθοδος επικεντρώνεται σε ένα συγκεκριμένο προϊόν, όπως είναι το *Guidance Software's EnCase.*

Τα γενικά μαθήματα παρέχουν στον ερευνητή τις τρέχουσες μεθοδολογίες και τα πρωτόκολλα της βιομηχανίας. Τα μαθήματα θα πρέπει να παρουσιάζουν παραδείγματα εργαλείων που μπορούν να χρησιμοποιηθούν, αναφέροντας τις δυνατότητές τους όπως και τους περιορισμούς τους. Επομένως, ο εκπαιδευόμενος θα πρέπει να έχει κάποια ιδέα για το ποιά εργαλεία θα πρέπει να χρησιμοποιήσει ανάλογα με την κάθε περίπτωση. Σε αυτές τις περιπτώσεις, ο ερευνητής έχει τις δικές του συσκευές για να καταγράψει την υπόθεση και να διατηρήσει την αλυσίδα επιτήρησης (*chain of custody)*.

Σε περίπτωση που οι έρευνες διεξάγονται με ένα συγκεκριμένο προϊόν, όπως το *EnCase, Ilook, FTK, SMART* ή κάποιο άλλο παρόμοιο προϊόν, η επιθυμητή εκπαίδευση θα πρέπει να παρέχεται από τον πάροχο του προϊόντος ή από έναν εξουσιοδοτημένο πάροχο. Σε πολλές περιπτώσεις αυτά τα μαθήματα έχουν σαν αποτέλεσμα την παροχή πιστοποίησης στη χρήση του προϊόντος.

Μια λίστα από παραδείγματα μαθημάτων που προσφέρονται στους επαγγελματίες αναλυτές είναι (*SANS Institute, 2005):*

- ***SEC401:*** *SANS Security Essentials Bootcamp*
- ***SEC502****: Firewalls, Perimeter Protection and VPNs*
- ***SEC503:*** *Intrusion Detection in Depth*
- ***SEC504:*** *Hacker Techniques, Exploits and Incident Handling*
- ***SEC505:*** *Securing Windows*
- ***SEC506:*** *Securing UNIX/Linux*
- ***AUD507:*** *Auditing Networks, Perimeters and Systems*
- ***SEC508:*** *System Forensics, Investigation and Response*
- ***SEC309:*** *Intro to Information Security*
- ***AUD410:*** *IT Security Audit Essentials*
- ***MGT512:*** *SANS Security Leadership Essentials for Managers*
- ***MGT414:*** *SANS + S Training Program for the CISSP Certification Exam*
- ***SEC616****: NET Security*
- ***SEC617****: Linux Administration Bootcamp*

Όπως βλέπουμε τα μαθήματα εστιάζουν σε συγκεκριμένες περιοχές. Τέτοιου είδους μαθήματα έχουν το πλεονέκτημα να περιορίζουν το πεδίο εφαρμογής του θέματος και να παρέχουν εργαλεία ή δεξιότητες ειδικά γι' αυτό το θέμα.

3.8.7 Πιστοποιήσεις

Ένα από τα θέματα που απασχολούν, είναι αν ένας ερευνητής θα πρέπει να είναι πιστοποιημένος ή όχι. Οι πιστοποιήσεις δίνονται από οργανισμούς ή εταιρείες και είτε

είναι συγκεκριμένες για ένα συγκεκριμένο προϊόν ή υπηρεσία, ή μπορεί να είναι γενικές. Τα πλεονεκτήματα της πιστοποίησης μπορούν να προσδιοριστούν από την εξέταση της αποδοχής τους στην βιομηχανία. Οι πιστοποιήσεις δεν ενσωματώνονται στην τυπική εκπαίδευση, αλλά μπορούν να εκδοθούν σαν μέρη μιας εκπαίδευσης που δίνεται από επαγγελματικά ινστιτούτα ή από μια τάξη δια βίου μάθησης. Οι διευθυντές θα πρέπει να γνωρίζουν ότι η εκπαίδευση μπορεί να αντληθεί και από τα μαθήματα της τυπικής εκπαίδευσης και από τις τάξεις εκπαίδευσης και να προσαρμόσουν ανάλογα την πολιτική τους.

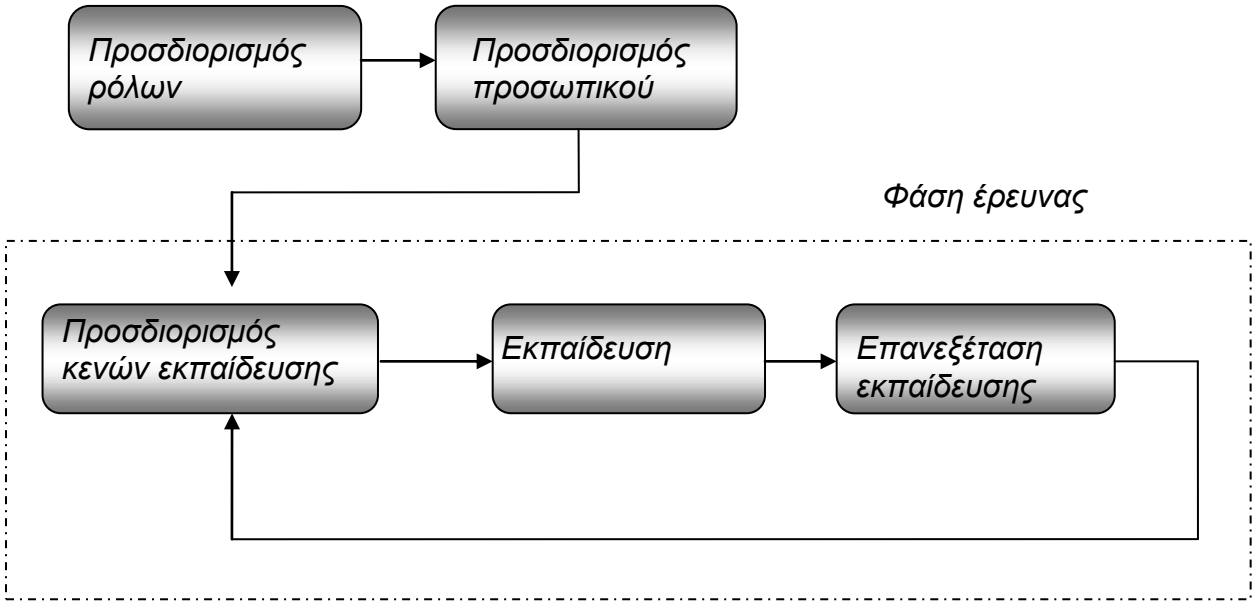
Η *CISSP (Certified Information Systems Security Professional)* πιστοποίηση *(CISSP, 2005)* καλύπτει δέκα περιοχές γνώσης και πιστοποιεί ότι ο εκπαιδευόμενος έχει τις βασικές γνώσεις σε αυτές τις περιοχές. Αυτές οι περιοχές είναι:

- Συστήματα ελέγχου πρόσβασης και μεθοδολογία,
- Ανάπτυξη εφαρμογών και συστημάτων,
- Ανάπτυξη πλάνου συνοχής επιχειρήσεων,
- Κρυπτογραφία,
- Νόμος, έρευνα και δεοντολογία,
- Ασφάλεια λειτουργιών,
- Φυσική ασφάλεια,
- Αρχιτεκτονική ασφάλειας και μοντέλα,
- Πρακτικές διαχείρισης ασφάλειας,
- Τηλεπικοινωνίες, δίκτυα και ασφάλεια διαδικτύου.

Ενώ η *CISSP* είναι μια γενική πιστοποίηση γνώσεων, η σειρά πιστοποιήσεων *GIAC (Global Information Assurance Certification)* παρέχει ικανότητες σε συγκεκριμένες περιοχές (όπως τα τείχη προστασίας).

3.8.8 Η Αναγνώριση των Αναγκών Εκπαίδευσης

Καθώς έχουμε εστιάσει στην εκπαίδευση του τεχνικού προσωπικού, χρειάζεται να διατηρήσουμε μια προοπτική για το ***πότε*** μπορεί να γίνει η εκπαίδευση στη διάρκεια του κύκλου ζωής μιας έρευνας. Στο ***σχήμα 28*** φαίνεται ο σχεδιασμός της εκπαίδευσης σε έναν επαναληπτικό κύκλο επιτρέποντας μια συνεχή κατάσταση εκπαίδευσης.



Σχήμα 28: Η επαναληπτική διαδικασία της εκπαίδευσης

Στην ουσία ένας διευθυντής θα πρέπει να αναγνωρίζει το γεγονός ότι η εκπαίδευση είναι στην πραγματικότητα μια διαρκής διαδικασία, αν κάποιο στοιχείο από το περιβάλλον αλλάξει. Αλλαγές προσωπικού, νέες τεχνολογίες, νέες διαδικασίες ή νόμοι ή και μια αύξηση του όγκου της δουλειάς που απαιτείται, μπορεί να οδηγήσουν σε νέες απαιτήσεις εκπαίδευσης.

Για να καθοριστεί το επίπεδο της εκπαίδευσης, θα πρέπει να σκεφτούμε το ρόλο που θα πρέπει να εκτελεστεί. Άλλοι παράγοντες που μπορεί να μην είναι φανεροί αμέσως, απαιτούν θεώρηση κάθε απόφασης. Μερικοί από αυτούς τους παράγοντες έχουν να κάνουν με θέματα προσωπικού, όπως είναι το επίπεδο του προσωπικού και η στελέχωση των ρόλων που ίσως απαιτήσουν εκπαίδευση του προσωπικού.

3.8.9 Επίλογος

Μια πρόταση που θα μπορούσε να κάνει κάποιος είναι να επεκτείνει τα χαρακτηριστικά ***απόκτηση, αρχειοθέτηση, ανάλυση και βεβαίωση*** που υπάρχουν στην διαδικασία της έρευνας, έτσι ώστε να περιλαμβάνουν και την ***πρόληψη***. Ο ερευνητής θα πρέπει να προβλέπει και να ενεργεί πρώτος (αν είναι δυνατόν) και να απαντά στις επιθέσεις που γίνονται στα πρωτόκολλα και στις μεθοδολογίες.

Ενώ το πλαίσιο *CNF* παρέχει μια δομή με την οποία μπορούμε να καθορίσουμε ποιές είναι οι ανάγκες σε μόρφωση και εκπαίδευση που απαιτούνται για ένα συγκεκριμένο ρόλο, οι διευθυντές θα πρέπει να γνωρίζουν ότι το πλαίσιο έχει μεγαλύτερη σημασία αν οι ρόλοι μπορούν να δομηθούν όπως ακριβώς εμφανίζονται στο πλαίσιο *CNF*. Πολλές φορές οι ανάγκες ενός οργανισμού μπορεί να αποκλείουν την προσκόλληση σε ένα τέτοιο πλαίσιο.

Άλλες φορές, η πραγματικότητα καθορίζει ποιός ρόλος απαιτείται, παρά τις ικανότητες του προσωπικού. Υπάρχουν κάποιοι άλλοι λόγοι για τους οποίους κάποιος δεν μπορεί

να εκπαιδευτεί: οι αναλυτές έχουν μεγάλη πιθανότητα να καταθέσουν σε ένα δικαστήριο (επομένως υπάρχει ανάγκη για εκπαίδευση νομικού περιεχομένου), ωστόσο κάποιοι τεχνικοί πολύ έμπειροι δεν μπορούν να είναι και οι καλύτεροι μάρτυρες στο δικαστήριο. Αυτοί οι παράγοντες θα πρέπει να ληφθούν υπόψη κατά την επιλογή του προσωπικού, αφού συχνά η αξιοπιστία του παραγόμενου έργου (αναφορά της ανάλυσης) δεν είναι τόσο σημαντική όσο η αξιοπιστία του αναλυτή.

Η εκπαίδευση είναι απαραίτητα μια διαρκής διαδικασία και πρέπει να διαχειρίζεται προληπτικά και να μην αφήνεται στη διακριτικότητα και υπόδειξη των τεχνικών. Καθώς ο διευθυντής δεν χρειάζεται να έχει σε βάθος τεχνικές γνώσεις, η θέση αυτή απαιτεί ευρεία γνώση όχι περιορισμένη στο τεχνικό επίπεδο: επιθυμητή είναι η εκπαίδευση στη διαχείριση προσωπικού, στη διαχείριση έργων, στη διαχείριση κρίσεων και στη διαχείριση προϋπολογισμού. Οι διευθυντές επίσης θα πρέπει να έχουν υπόψη τους ότι συχνά οι αποστολές αλλάζουν αφού τα σχέδια έχουν διαμορφωθεί και υλοποιηθεί, και ότι η εκπαίδευση θα πρέπει να θεωρείται απαραίτητη για πιθανές και μελλοντικές απαιτήσεις ώστε να ακολουθεί την τεχνολογία. **[14]**

4. Ειδικά Θέματα

4.1 Απειλές και Μηχανισμοί Προστασίας της Ιδιωτικότητας στα Ασύρματα και Κινητά Δίκτυα Επικοινωνιών

Ο *Alan F. Westin* ορίζει ως ***ιδιωτικότητα*** (*privacy*): ***την αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν για τον εαυτό τους πότε, πώς και σε ποιό ακριβώς βαθμό οι πληροφορίες για τα άτομά τους γνωστοποιούνται στους υπόλοιπους με τους οποίους επικοινωνούν.*** Βασιζόμενοι στον παραπάνω ορισμό, στα πλαίσια του παρόντος κεφαλαίου, θεωρούμε ως ιδιωτικότητα την αξίωση και την ικανότητα οποιουδήποτε ατόμου, που χρησιμοποιεί κάποια κινητή συσκευή, να ελέγχει την αποκάλυψη των προσωπικών του πληροφοριών στους υπόλοιπους, με τους οποίους ενδέχεται να επικοινωνεί. Συνεπώς, η ανωνυμία (*anonymity*) του χρήστη αποτελεί αναγκαιότητα για την εξασφάλιση της ιδιωτικότητας.

Σε ένα περιβάλλον κινητών (*mobile*) επικοινωνιών η ιδιωτικότητα των χρηστών και άρα η ανωνυμία τους αποτελεί σημαντικό ζήτημα. Αναλογιζόμενοι ένα τέτοιο περιβάλλον διαπιστώνουμε εύκολα ότι διάφορες πληροφορίες τυγχάνουν επεξεργασίας από κινητές ή φορητές συσκευές των χρηστών, οι οποίοι μετακινούνται από δίκτυο σε δίκτυο ανάλογα με τις εκάστοτε ανάγκες τους. Το γεγονός αυτό οδηγεί σε ένα διαρκώς μεταβαλλόμενο περιβάλλον, όπου διαρκώς συσκευές –άρα και χρήστες- συνδέονται και αποσυνδέονται. Μια συσκευή που εισέρχεται στην περιοχή ραδιοκάλυψης ενός ασύρματου δικτύου ενδέχεται να συνδεθεί σε αυτό αυτομάτως, αν βέβαια αυτό επιτρέπεται. Όμως από την άλλη πλευρά, οι διαχειριστές και οι υπόλοιποι χρήστες του δικτύου μπορεί να μην ενδιαφέρονται ιδιαίτερα για τη διασφάλιση του απορρήτου των επικοινωνιών και την προστασία της ιδιωτικότητας της νεοεισερχόμενης συσκευής, άρα και του χρήστη. Η μέθοδος *open authentication* που προσφέρεται από τα δίκτυα *IEE 802.11* αποτελεί χαρακτηριστικό παράδειγμα της εν λόγω περίπτωσης. Ακόμα όμως και αν το δίκτυο χρησιμοποιεί κάποιους μηχανισμούς ασφάλειας, δεν είναι δεδομένο ότι αυτοί εξασφαλίζουν την ιδιωτικότητα των χρηστών και σε ποιό ακριβώς βαθμό. Ενώ λοιπόν οι νέες ασύρματες τεχνολογίες πρόσβασης και τύποι δικτύων υπόσχονται καινοτόμες εφαρμογές που είναι πιθανό να βελτιώσουν την ποιότητα της ζωής μας, έχουν τη δυνατότητα να βλάψουν σε σημαντικό βαθμό την ιδιωτικότητα των χρηστών τους. Όλες οι σύγχρονες μορφές και τεχνολογίες ασύρματων δικτύων, όπως είναι τα αδόμητα ασύρματα δίκτυα (*Mobile ad hoc Networks, MANET*), τα ασύρματα δίκτυα αισθητήρων *(Wireless Sensor Networks, WSN)*, τα οχηματικά δίκτυα *(Vehicular ad hoc Networks, VANET)* και γενικά ότι περιλαμβάνεται στο γενικό όρο ***διάχυτη υπολογιστική*** (*ubiquitous/pervasive computing*) είναι δυνατό να χρησιμοποιηθεί για την παρακολούθηση των χρηστών και των συνηθειών τους. Η συνεχής παρακολούθηση των δραστηριοτήτων και της κίνησης των χρηστών στο χώρο και στο χρόνο μπορεί να καταλήξει με τη σειρά της στη σύνθεση λεπτομερών προφίλ ανά χρήστη, οδηγώντας έτσι σε πλήρη παραβίαση της ιδιωτικότητάς του. Μέχρι στιγμής, πολλοί μηχανισμοί εξασφάλισης της ανωνυμίας έχουν προταθεί στη βιβλιογραφία ιδιαίτερα για τα ενσύρματα δίκτυα, οι περισσότεροι όμως από αυτούς απαιτούν τη χρήση πολύπλοκων υποδομών και τεχνολογιών. Στην περίπτωση των κινητών δικτύων επικοινωνιών η χρήση παρόμοιων υποδομών ενδέχεται να οδηγήσει σε υψηλά υπολογιστικά κόστη για τις συσκευές και σε συμφόρηση του ίδιου του δικτύου.

Θα παραθέσουμε δύο παραδείγματα στα οποία διακρίνονται ξεκάθαρα οι απειλές για την ιδιωτικότητα ενός χρήστη που περιάγει (*roam*) σε κάποιο ασύρματο δίκτυο επικοινωνιών.

Στο πρώτο παράδειγμα ένας χρήστης επισκέπτεται μια καφετέρια στην οποία συχνάζουν άνθρωποι που ενδιαφέρονται για τις νέες τεχνολογίες. Χρησιμοποιώντας τεχνολογία *Mobile IP* ο χρήστης συνδέεται στο διαδίκτυο (*mobile internet*) μέσω του νέου του κινητού τηλεφώνου. Ακολούθως, φορτώνει από το διαδίκτυο ένα βίντεο (*streaming video*) από έναν εξυπηρετητή ασύρματου πρωτόκολλου εφαρμογών (*Wireless Application Protocol, WAP*). Ας υποθέσουμε ότι ο χρήστης ενδιαφέρεται για το χρηματιστήριο και το βίντεο αυτό αφορά τις τελευταίες τιμές ή εξελίξεις.

Στο δεύτερο παράδειγμα μπορούμε να υποθέσουμε ότι ο χρήστης αισθάνεται μοναξιά. Ενώ στην καφετέρια υπάρχουν πολλοί θαμώνες, ο χρήστης χρησιμοποιεί μέσω του κινητού τηλεφώνου την υπηρεσία κοινωνικής δικτύωσης *Instant Mobile Dating*, στην οποία έχει γίνει συνδρομητής. Μόλις συνδεθεί, ανακαλύπτει ότι το προφίλ κάποιου άλλου συνδρομητή (του άλλου φύλλου) που βρίσκεται στον ίδιο χώρο ταιριάζει με το δικό του προφίλ και χωρίς να το σκεφτεί αρχικοποιεί μια σύνοδο συνομιλίας *(chat session)* με αυτόν. Αφού συνομιλούν για μερικά λεπτά ανταλλάσσοντας απόψεις για κοινά θέματα, αποφασίζουν να συνεχίσουν αυτοπροσώπως τη συνομιλία τους σε κάποιο τραπέζι.

Αναλύοντας τα παραπάνω παραδείγματα, διαπιστώνουμε ότι υπάρχουν αρκετά ζητήματα ιδιωτικότητας που θα έπρεπε να απασχολήσουν το χρήστη. Συγκεκριμένα στο πρώτο παράδειγμα, ο χρήστης νιώθει άβολα όταν αποκαλύπτει σε άλλους ανθρώπους το ενδιαφέρον του για τη χρηματιστηριακή αγορά. Ανησυχεί ότι κάποιος μπορεί να χρησιμοποιήσει αυτή την πληροφορία και να συμπεράνει ότι είναι ευκατάστατος. Κάποιος θα μπορούσε επίσης, έχοντας αυτό στο μυαλό του, να τον ακολουθήσει για να δει πού μένει. Επίσης, ο χρήστης δεν εμπιστεύεται πλήρως την εταιρεία από την οποία φορτώνει τα βίντεο. Φοβάται ότι η εν λόγω εταιρεία έχει τη δυνατότητα να συλλέγει στοιχεία για τον ίδιο, επιδιώκοντας να δημιουργήσει ένα λεπτομερές προφίλ και αργότερα να το διαθέσει σε διαφημιστικές εταιρείες με σκοπό το κέρδος.

Στο δεύτερο παράδειγμα, ο χρήστης αισθάνεται άβολα όταν αποκαλύπτεται στους άλλους θαμώνες της καφετέριας ότι χρησιμοποιεί αυτή την υπηρεσία ραντεβού. Επίσης ανησυχεί για το ενδεχόμενο οι συνομιλητές του στην υπηρεσία αυτή να είναι φαρσέρ, οι οποίοι θα ήταν δυνατό να διαπιστώσουν την ταυτότητά του και να τον περιγελάσουν.

Φυσικά εκτός των παραπάνω ζητημάτων, μια σειρά από άλλα προβλήματα σχετικά με την ιδιωτικότητα του χρήστη θα μπορούσαν να αναλυθούν. Όπως για παράδειγμα το ζήτημα της ***ιδιωτικότητας της γεωγραφικής θέσης*** (*location privacy).* Είναι πιθανό ο οικείος πάροχος (*home*) των υπηρεσιών κινητών επικοινωνιών δεύτερης ή και τρίτης γενιάς *(2G/3G*), αλλά και άλλοι που συνεργάζονται με αυτόν να παρακολουθούν συνεχώς πού κινείται και τι είδους υπηρεσίες χρησιμοποιεί. Το πρωτόκολλο κινητών υπηρεσιών *(Mobile IP)* για παράδειγμα, χρησιμοποιεί την οντότητα του δρομολογητή-πράκτορα *(home agent)* για να επιτρέπει στους χρήστες να επικοινωνούν ενώ περιάγουν εκτός του οικείου δικτύου τους. Ο *home agent* είναι μια στατική οντότητα, αποτελεί τμήμα της υποδομής του οικείου παρόχου υπηρεσιών διαδικτύου και γι’ αυτό είναι σε θέση να παρακολουθεί συνεχώς τις κινήσεις των χρηστών που περιάγουν εκτός του οικείου δικτύου. Οι πληροφορίες δηλαδή που συλλέγονται από αυτόν είναι ευαίσθητες, αφού η αποθήκευση και η εκ των υστέρων επεξεργασία τους μπορεί να οδηγήσουν μεσοπρόθεσμα ή μακροπρόθεσμα σε δημιουργία λεπτομερών προφίλ σχετικά με το πού συνηθίζει να κινείται ο χρήστης αλλά και πού βρίσκεται ανά πάσα στιγμή.

Η ίδια ανησυχία υφίσταται για κάθε άτομο που χρησιμοποιεί μια κινητή συσκευή, εφόσον αυτή μπορεί εν δυνάμει να λειτουργεί ως πομπός, ο οποίος είναι δυνατό να

χρησιμοποιηθεί κακόβουλα ώστε να αποκαλύψει την τρέχουσα γεωγραφική θέση του χρήστη, αλλά και άλλες πληροφορίες , όπως με ποιούς συναναστρέφεται, τις συνήθειές του κ.λπ. Συνεπώς θα μπορούσαμε να πούμε ότι το ζήτημα της ιδιωτικότητας είναι περισσότερο σύνθετο από ότι το αντιλαμβάνεται κάποιος με την πρώτη ματιά, συνήθως δεν βρίσκεται πλήρως υπό την εποπτεία του ίδιου του χρήστη και περιλαμβάνει αρκετές συνιστώσες που χρήζουν περαιτέρω ανάλυσης και περιγραφής.

4.1.1 Μηχανισμοί Προστασίας της Ιδιωτικότητας στα δίκτυα *2G/3G*

4.1.1.1 Προστασία της Ταυτότητας των χρηστών στο *GSM*

Το Πανευρωπαϊκό Σύστημα Κινητών Επικοινωνιών *(Global System For Mobile Communications, GSM)* αποτελεί το δημοφιλέστερο σύστημα κινητών επικοινωνιών δεύτερης γενιάς (*2G*). Σύμφωνα με πρόσφατα στοιχεία ο αριθμός των συνδρομητών του ξεπέρασε τα τρία δισεκατομμύρια στο τέλος του 2008. Κάθε χρήστης στο σύστημα *GSM* διαθέτει μια ***μόνιμη (permanent) ταυτότητα***, η οποία είναι γνωστή ως ***IMSI*** *(International Mobile Subscriber Identity*). Η εν λόγω ταυτότητα αποτελείται από τρία διαφορετικά πεδία, όπως φαίνεται στο ***σχήμα 29***. Η ενδεχόμενη αποκάλυψη της ταυτότητας αυτής σε τρίτους και η συσχέτισή της με το συνδρομητή ως φυσικό πρόσωπο αποτελούν άμεση ή έμμεση απειλή για την ιδιωτικότητά του. Για παράδειγμα, οι κινήσεις του συνδρομητή στο χώρο είναι δυνατό να παρακολουθούνται ανά πάσα στιγμή, εφόσον αναγνωρίζεται μοναδικά από το *IMSI* του. Σημειώνεται ότι η ταυτότητα *IMSI* δεν θα πρέπει να συγχέεται με το διεθνή τηλεφωνικό αριθμό κλήσης του συνδρομητή *(Mobile Station International Number, MSISDN).* Το *MSISDN*, όπως και το *IMSI*, βρίσκεται αποθηκευμένο στην έξυπνη κάρτα *(Universal Integrated Circuit Card, UICC)* που δίνεται από τον εκάστοτε πάροχο υπηρεσιών στο συνδρομητή κατά την εγγραφή του στο δίκτυο.

Το σύστημα λοιπόν θα πρέπει να προστατεύει τη μόνιμη ταυτότητα των χρηστών από τυχόν ωτακουστές (*eavesdroppers*), περιορίζοντας τις περιπτώσεις όπου αυτή χρειάζεται να μεταδοθεί απροστάτευτη, δηλαδή σε μορφή αρχικού κειμένου (*cleartext*). Έτσι στο *GSM* αντί του *IMSI* χρησιμοποιούνται ***προσωρινές ταυτότητες χρηστών*** που ονομάζονται ***TMSI*** *(Temporary Mobile Subscriber Identity).* Η προσωρινή ταυτότητα του χρήστη μεταβάλλεται συνήθως κάθε φορά που αυτός αυθεντικοποιείται από το δίκτυο και μεταδίδεται σε αυτόν κρυπτογραφημένη. Επίσης η τεχνολογία *General Packet Radio Service (GPRS)* χρησιμοποιεί παρόμοιες ***προσωρινές ταυτότητες συνδρομητών*** που καλούνται ***P-TMSI*** *(Packet TMSI).* Αυτές αποδίδονται στον κάθε χρήστη που χρησιμοποιεί κάποια υπηρεσία *GPRS* από τον αντίστοιχο κόμβο εξυπηρέτησης *(Serving GPRS Support Node, SGSN)* και ανεξάρτητα από το *TMSI*.

IMSI =	**MCC +**	**MNC +**	**MSIN**
International Mobile Subscriber Identity (Ταυτότητα συνδρομητή)	*Mobile Country Code (Κωδικός χώρας)*	*Mobile Network Code (Κωδικός δικτύου)*	*Mobile Subscriber Identification Number (Κωδικός συνδρομητή)*
15 αριθμητκοί χαρακτήρες	*3 χαρακτήρες*	*2 χαρακτήρες*	*Μέγιστο 10 χαρακτήρες*

Σχήμα 29: Τα πεδία από τα οποία αποτελείται το *IMSI*

4.1.1.2 Προστασία της Ιδιωτικότητας των χρηστών στο *UMTS*

Το *Universal Mobile Telecommunications Service (UMTS)* αποτελεί ένα σύστημα κινητών επικοινωνιών τρίτης γενιάς (*3G*) που προτυποποιείται από τον οργανισμό *3rd Generation Partnership Project (3GPP).* Για λόγους συμβατότητας με το *GSM*, η μόνιμη ταυτότητα ενός συνδρομητή στο *UMTS* παραμένει ο αριθμός *IMSI*. Όμως σε όλες σχεδόν τις περιπτώσεις επικοινωνίας του χρήστη με το δίκτυο χρησιμοποιούνται προσωρινές τους ταυτότητες γνωστές ως *TMSI*, για το υποσύστημα μεταγωγής κυκλώματος *(Circuit Switched, CS)* και *P-TMSI* για το υποσύστημα μεταγωγής πακέτων *(Packet Switched, PS),* ανάλογα με την έκδοση του *UMTS* που υλοποιεί ο εκάστοτε πάροχος υπηρεσιών.

Κάθε τερματική συσκευή μπορεί να βρίσκεται σε δύο καταστάσεις: ***αδρανής*** (*idle*) ή ***συνδεδεμένη*** (*connected*) καθ' όλη τη διάρκεια που ο χρήστης επικοινωνεί με το δίκτυο. Συγκεκριμένα μόλις ο χρήστης ενεργοποιήσει τη συσκευή του, αυτή μεταβαίνει στην κατάσταση αδράνειας. Αμέσως μόλις εγκαθιδρυθεί μια σύνδεση, η κατάσταση της συσκευής μεταβάλλεται σε συνδεδεμένη. Στην κατάσταση αδράνειας η συσκευή μπορεί να αναγνωριστεί μόνο με τη χρήση ταυτοτήτων του δικτύου κορμού *(Core Network, CN)* δηλαδή με τα *IMSI, TMSI, P-TMSI*. Όμως στην κατάσταση συνδεδεμένη, η συσκευή μπορεί να αναγνωριστεί με τη χρήση ταυτοτήτων *επιπέδου UMTS Terrestrial Radio Access Network (UTRAN),* οι οποίες καλούνται προσωρινές ταυτότητες ραδιοδικτύου *(Radio Network Temporary Identity, RNTI).* Εξυπακούεται ότι το δίκτυο οφείλει να διατηρεί και αντίστοιχη συσχέτιση μεταξύ της ταυτότητας *CN* και αυτής του επιπέδου *UTRAN*.

Με αυτό τον τρόπο, η ταυτότητα του χρήστη προστατεύεται σε όλες σχεδόν τις περιπτώσεις από παθητικού τύπου επιθέσεις ωτακουστών.

Όπως ήδη ειπώθηκε μια προσωρινή ταυτότητα ισχύει μόνο ***τοπικά***. Έτσι, όταν ο χρήστης περιάγει στην περιοχή ευθύνης ενός νέου *Visitor Location Register(VLR)/Serving GPRS Support Node (SGSN)*, αυτό θα πρέπει να είναι σε θέση να αντιληφθεί την προσωρινή του ταυτότητα, η οποία όμως έχει αποδοθεί από το προηγούμενο *VLR/SGSN*. Αυτό επιτυγχάνεται με την προσάρτηση της ταυτότητας της περιοχής στην οποία κινείται ο συνδρομητής στην προσωρινή ταυτότητά του. Με αυτό τον τρόπο σε κάθε συνδρομητή αποδίδεται πάντοτε διαφορετική προσωρινή ταυτότητα από οποιονδήποτε άλλο. Σε περίπτωση που η επικοινωνία μεταξύ παλιού και νέου *VLR/SGSN* είναι αδύνατη, το *IMSI* του χρήστη πρέπει να χρησιμοποιηθεί, παραβιάζοντας την ιδιωτικότητά του.

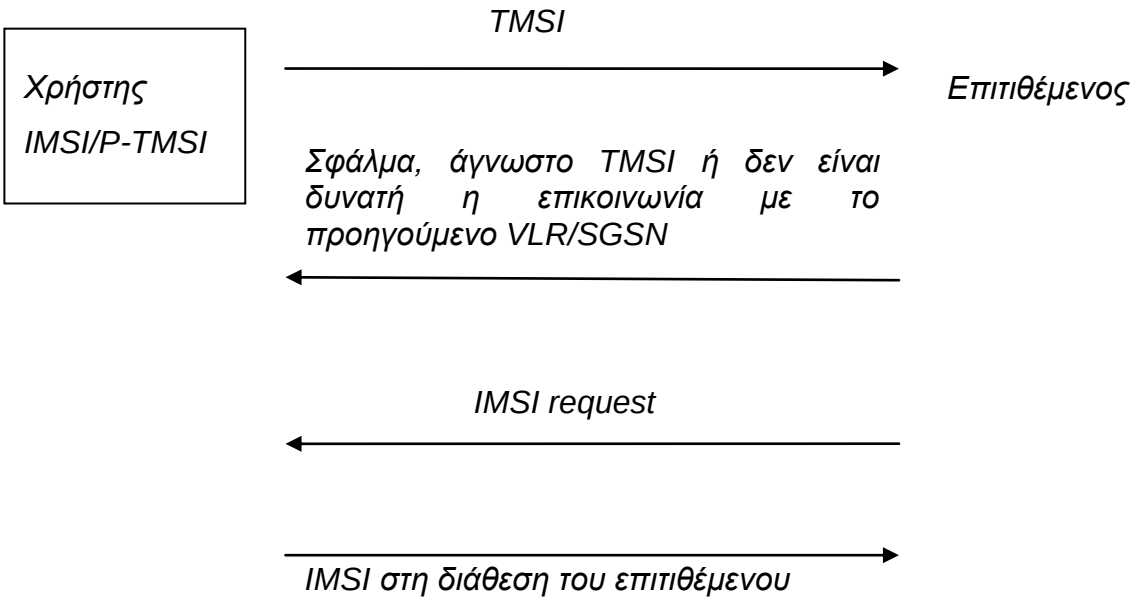
Ένας άλλος έμμεσος μηχανισμός προστασίας της ταυτότητας των χρηστών και της θέσης που περιάγουν έχει ενσωματωθεί στο πρωτόκολλο πιστοποίησης της ταυτότητας των χρηστών του *UMTS*. Το εν λόγω πρωτόκολλο πιστοποίησης της ταυτότητας μεταξύ συνδρομητή και δικτύου, γνωστό και ως *Authentication and Key Agreement (AKA),* είναι σχεδιασμένο στα πρότυπα του αντίστοιχου μηχανισμού που υπάρχει και στο *GSM*. Η διαδικασία αυθεντικοποίησης βασίζεται σε ένα συμμετρικό κλειδί μήκους 128 *bits*, το οποίο είναι αποθηκευμένο στην κάρτα *UICC* του συνδρομητή και στον *αντίστοιχο Home Subscriber Server (HSS)* του οικείου δικτύου. Το κλειδί αυτό θεωρείται μυστικό. Η διαδικασία αυθεντικοποίησης, αποτελεί συνδυασμό του γνωστού πρωτοκόλλου πρόκλησης-απόκρισης *(challenge-response*) του *GSM* και του γενικού (*generic*) μηχανισμού αυθεντικοποίησης που βασίζεται σε αριθμούς ακολουθίας *(sequence numbers)*.

4.1.1.3 Απειλές

Όπως ήδη αναφέραμε σε ορισμένες περιπτώσεις το σύστημα επιτρέπει την εκπομπή της ταυτότητας *IMSI* από το τερματικό στο δίκτυο σε μορφή αρχικού κειμένου (*cleartext*). Η διαδικασία μπορεί να ξεκινήσει από το οικείο δίκτυο ή το δίκτυο εξυπηρέτησης στις ακόλουθες περιπτώσεις: **α)** Όταν ο συνδρομητής εγγράφεται για πρώτη φορά στο δίκτυο, **β)** μετά από μεγάλο χρονικό διάστημα κατά το οποίο η συσκευή του συνδρομητή ήταν απενεργοποιημένη, **γ)** όταν ο συνδρομητής περιάγει εκτός οικείου δικτύου και **δ)** όταν το δίκτυο δεν είναι ικανό να ανακτήσει το *IMSI* του συνδρομητή. Αυτό είναι πιθανό να συμβεί, όταν κατά τη διαδικασία διαπομπής (*handover*) από κυψέλη σε κυψέλη ή από δίκτυο σε δίκτυο, το ζεύγος *IMSI/P-TMSI* πρέπει να μεταδοθεί από το προηγούμενο *SGSN* στο νέο, αλλά η διεύθυνση του προηγούμενου *SGSN* δεν μπορεί να βρεθεί. Επίσης, σε περίπτωση κατά την οποία το προηγούμενο *SGSN* δεν αποκρίνεται εξαιτίας κάποιας βλάβης.

Η προαναφερόμενη διαδικασία είναι προφανώς ευάλωτη σε παθητικού τύπου επιθέσεις, όπου ο επιτιθέμενος αναμένει για πιθανές εκπομπές απροστάτευτων *IMSI*. Γενικά, η εκπομπή του *IMSI* αποτελεί κυρίως απειλή εναντίον της εμπιστευτικότητας της ταυτότητας του χρήστη *(identity confidentiality)* και της θέσης στην οποία κινείται *(location privacy).* Επιπλέον όμως η γνώση του *IMSI* είναι δυνατό να επιτρέψει την πλαστογράφηση της ταυτότητας του χρήστη. Δεν είναι βέβαια σαφές πώς ένας επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή τη δυνατότητα πλαστογράφησης, εκτός από το να προκαλέσει γενική αναστάτωση στο σύστημα. Αξίζει όμως να σημειωθεί ότι η γνώση του *IMSI* σε συνδυασμό με το αντίστοιχο κλειδί (που βρίσκεται αποθηκευμένο στη κάρτα *UICC*), μπορεί να οδηγήσει στην κλωνοποίηση της τελευταίας.

Γενικότερα βέβαια υπάρχουν τοποθεσίες ή σημεία στα οποία πολλά *IMSI* εκπέμπονται συνεχώς. Σε αυτές περιλαμβάνονται αεροδρόμια, λιμάνια κ.λπ., όπου οι χρήστες ενεργοποιούν τα κινητά τερματικά τους μετά από το ταξίδι τους. Αυτό σημαίνει ότι ο επιτιθέμενος που γνωρίζει το *IMSI* κάποιου ή κάποιων συνδρομητών είναι σε θέση να τους αναγνωρίσει. Από την άλλη πλευρά αυτό είναι επίσης δυνατό παρατηρώντας απλώς ποιοί αποβιβάζονται. Σε κάθε περίπτωση όμως, ο μηχανισμός πιστοποίησης ταυτότητας του *UMTS* δεν είναι ιδιαίτερα αποτελεσματικός σε ενεργές επιθέσεις ενδιάμεσου. Συγκεκριμένα ο επιτιθέμενος μπορεί να προσποιηθεί το δίκτυο εξυπηρέτησης με αποτέλεσμα να καταφέρει σχετικά εύκολα να αποσπάσει το *IMSI* του χρήστη θύματος. Η κατάσταση αυτή περιγράφεται στο ***σχήμα 30***.



Σχήμα 30: Ενεργητικού τύπου επίθεση με στόχο την απόκτηση του *IMSI*

4.1.2 Ιδιωτικότητα Χρηστών και Υπηρεσίες Εντοπισμού Θέσης στα Κινητά Δίκτυα *2G/3G*

Τα τελευταία χρόνια η ανάπτυξη υπηρεσιών που βασίζονται στον εντοπισμό της θέσης ενός κινητού συνδρομητή *(Location Based Services, LBS)* αποτελεί μια πραγματικότητα με αυξανόμενες τάσεις στον τομέα των κινητών επικοινωνιών. Οι υπηρεσίες αυτές βασίζονται στον εντοπισμό της θέσης κάποιου κινητού συνδρομητή με όσο το δυνατόν μεγαλύτερη ακρίβεια. Με αυτό τον τρόπο κάθε χρήστης μπορεί να αποκτά πρόσβαση σε υπηρεσίες προσαρμοσμένες στις εκάστοτε συνθήκες και απαιτήσεις του, ιδιαίτερα σε ώρα ανάγκης. Για παράδειγμα, υπηρεσίες όπως η καθοδήγηση σε διανυκτερεύοντα φαρμακεία, νοσοκομεία ή πρατήρια καυσίμων ενδέχεται να αποδειχτούν πολύτιμες, ενώ πληροφορίες που έχουν να κάνουν με τη διασκέδαση βελτιώνουν απλώς το επίπεδο διαβίωσης των συνδρομητών. Έτσι, οι διάφορες υπηρεσίες *LBS* δίνουν στο χρήστη την δυνατότητα να αξιοποιήσει στο έπακρο τις δυνατότητες της κινητής συσκευής του, κάνοντας τη ζωή του ευκολότερη. Στις ΗΠΑ για παράδειγμα εφαρμόζονται ήδη προγράμματα χρέωσης των κλήσεων με βάση τον καθορισμό της θέσης της κινητής συσκευής, αφού οι συνδρομητές μπορούν να ορίσουν τις περιοχές στις οποίες θα απολαμβάνουν χαμηλότερη χρέωση. Επίσης, η υπηρεσία εντοπισμού θέσης χρησιμοποιείται από τις υπηρεσίες έκτακτης ανάγκης, για τον εντοπισμό ενός συνδρομητή που κινδυνεύει (κλήση 911 για ΗΠΑ ή 112 για Ευρώπη).

Όπως συμβαίνει με κάθε τεχνολογική καινοτομία, οι υπηρεσίες εντοπισμού θέσης παρουσιάζουν και αυτές ορισμένα μειονεκτήματα. Το σημαντικότερο πρόβλημα με τις υπηρεσίες αυτού του είδους είναι η δυνατότητα παρακολούθησης της θέσης και της κίνησης του κινητού τερματικού, άρα και του χρήστη. Αυτό μπορεί να γίνει αντικείμενο εκμετάλλευσης, κυρίως για διαφημιστικούς σκοπούς, και συνεπώς παραβίασης του απορρήτου της θέσης και πιθανώς της ταυτότητας του χρήστη. Η αποστολή διαφημίσεων από διάφορα καταστήματα, όταν είναι γνωστό μέσω *LBS* ότι ο χρήστης

περιάγει πλησίον αυτών, είναι τουλάχιστον ενοχλητική με αποτέλεσμα οι ρόλοι να αντιστρέφονται. Αντί ο χρήστης να χρησιμοποιεί προς όφελός του τις υπηρεσίες *LBS*, ουσιαστικά γίνεται ο ίδιος εύκολο θύμα εκμετάλλευσης από αυτές.

Με βάση τα παραπάνω, η προστασία των δεδομένων που αφορούν στη θέση του κάθε συνδρομητή που εντοπίζεται από ένα σύστημα *LBS*, όταν αυτός προσπαθεί να χρησιμοποιήσει κάποια σχετική υπηρεσία, αποτελεί επιτακτική ανάγκη. Η δυνατότητα πλήρους και άμεσου ελέγχου της ιδιωτικότητας με διαφανή τρόπο, θα πρέπει να αποτελεί ευθύνη του συνδρομητή και σε καμιά περίπτωση του παρόχου υπηρεσιών. Στη Μεγάλη Βρετανία, για παράδειγμα, η καταχώρηση και η αποθήκευση προσωπικών δεδομένων των χρηστών στα οποία περιλαμβάνονται και πληροφορίες θέσης που συγκεντρώνονται γι' αυτούς, επιβάλλεται να γίνονται ύστερα από ρητή συγκατάθεση των χρηστών αυτών. Κάθε φορά λοιπόν που κάποιος χρήστης εγγράφεται σε μια υπηρεσία *LBS* θα πρέπει να είναι βέβαιος ότι δεν θα ενοχλείται ή δεν θα τυγχάνει εκμετάλλευσης από υπηρεσίες όπως το *junk mail.*

Το απόρρητο της θέσης και γενικότερα η ιδιωτικότητα του χρήστη είναι ένα σύνθετο ζήτημα, ειδικά όταν αυτός περιάγει από δίκτυο σε δίκτυο. Ανέκαθεν οι πάροχοι είναι σε θέση να συλλέγουν και να καταγράφουν τις πληροφορίες θέσης των συνδρομητών που κινούνται εντός του δικτύου τους. Με την ανάπτυξη της περιαγωγής των υπηρεσιών *LBS*, οι πληροφορίες θέσης των συνδρομητών διαρρέουν πλέον και εκτός των δικτύων στα οποία αυτοί είναι εγγεγραμμένοι. Βεβαίως υπάρχει σχετική νομολογία που θέτει περιορισμούς και επιχειρεί να προστατεύσει τα προσωπικά δεδομένα των συνδρομητών, ωστόσο το νομικό πλαίσιο ενδέχεται να διαφέρει σημαντικά από χώρα σε χώρα. Για το λόγο αυτό, ειδικά για διεθνείς περιαγωγές, αποκτά μεγάλη σημασία η θέσπιση συμφωνιών και κανόνων μεταξύ των διαφόρων παρόχων ως προς τις γενικές απαιτήσεις ιδιωτικότητας, ούτως ώστε να καθιερωθεί στο μέλλον η περιαγωγή *LBS* ως μια αξιόπιστη και προπαντός ασφαλής υπηρεσία.

4.1.2.1 Απαιτήσεις

Οι παρακάτω βασικές απαιτήσεις μπορούν να εφαρμοστούν σε όλες τις περιπτώσεις υπηρεσιών *LBS*:

1. Ο χρήστης θα έχει τον πλήρη έλεγχο των εφαρμογών που μπορούν να εντοπίσουν τη θέση του. Υπάρχει η δυνατότητα να προσφερθούν διαφορετικά επίπεδα ελέγχου: **α)** στατικός έλεγχος από το χρήστη για κάθε εφαρμογή, **β)** δυναμικός έλεγχος ανά εφαρμογή και **γ)** δυναμικός έλεγχος ανά αίτηση εντοπισμού θέσης.
2. Ο χρήστης θα πρέπει να ενημερώνεται για το πότε αναζητείται η θέση του. Μπορούν έτσι να προσφερθούν διαφορετικά επίπεδα γνωστοποίησης: **α)** καμιά γνωστοποίηση, **β)** γνωστοποίηση ανά αίτηση και **γ)** αρχείο ιστορικού, π.χ. δημιουργείται μια καταχώρηση στη βάση δεδομένων του παρόχου για το ποιός ακριβώς αιτείται για τον εντοπισμό της θέσης κάποιου συνδρομητή.
3. Να είναι σε θέση ο χρήστης να ελέγξει το επίπεδο ακρίβειας στον εντοπισμό της θέσης του με σκοπό την προστασία της ιδιωτικότητας της θέσης στην οποία βρίσκεται. Για παράδειγμα, μια εφαρμογή *LBS* θα είναι ικανή να εντοπίζει το ακριβές σημείο που βρίσκεται ο χρήστης, ενώ κάποια άλλη απλώς θα αναφέρει την πόλη ή τη γειτονιά στην οποία κινείται.

4. Στις υπηρεσίες ανίχνευσης (*tracking*) οι θέσεις των χρηστών καταχωρίζονται για να αναπαραστήσουν την κίνηση. Τέτοιες πληροφορίες θα πρέπει να αποθηκεύονται για σύντομο χρονικό διάστημα και αμέσως μετά να διαγράφονται.

Όπως ήδη αναφέρθηκε η ιδιωτικότητα του χρήστη απειλείται από την αποκάλυψη της μόνιμης ταυτότητάς του. Αυτή εξάλλου είναι πάντοτε γνωστή στον οικείο πάροχο υπηρεσιών και πιθανώς σε άλλους παρόχους, όταν ο συνδρομητής περιάγει. Η μόνιμη ταυτότητα λοιπόν του συνδρομητή, όπως για παράδειγμα το *MSISDN* που χρησιμοποιείται στις υπηρεσίες *LBS*, δεν θα πρέπει να αποκαλύπτεται στον εκάστοτε πάροχο υπηρεσιών, αν ο χρήστης δεν το επιθυμεί, αλλά να γίνεται πάντοτε χρήση της προσωρινής ταυτότητάς του.

4.1.2.2 Εξασφάλιση Ανωνυμίας στις υπηρεσίες *LBS*

Γενικά η μόνιμη ταυτότητα του συνδρομητή γνωστοποιείται στον πάροχο υπηρεσιών κατά την πρόσβαση του πρώτου στην υπηρεσία *LBS*. Ωστόσο, σε ορισμένες περιπτώσεις, η διαδικασία αυτή δεν είναι και η πλέον κατάλληλη. Σε αυτές τις περιπτώσεις το δίκτυο κρυπτογραφεί (ή καθιστά ανώνυμη) την ταυτότητα του συνδρομητή σε μια σκοπίμως ασαφή αντίστοιχη, γνωστή ως *Opaque ID*. Η μέθοδος κρυπτογράφησης ή ανωνυμοποίησης που χρησιμοποιείται είναι στην ευχέρεια του εκάστοτε παρόχου. Με αυτό τον τρόπο οι εφαρμογές *LBS* μπορούν να αναφέρονται στο συνδρομητή χωρίς να γνωρίζουν την πραγματική (μόνιμη) ταυτότητά του.

4.1.2.2.1 Συσκευή Μεσολάβησης (Mediation Device)

Στη γενικότερη αρχιτεκτονική *LBS* εντάσσεται η συσκευή διαμεσολάβησης *(Mediation Device, MD)*, η οποία τοποθετείται εντός του δικτύου του παρόχου που κάθε φορά κάνει αίτηση για κάποια υπηρεσία *LBS*. Η εν λόγω συσκευή είναι υπεύθυνη για την κρυπτογράφηση και την αποκρυπτογράφηση του *MSISDN*. Συγκεκριμένα, το δίκτυο που κάνει την αίτηση καθορίζει αν το *MSISDN* θα κρυπτογραφηθεί βάσει συγκεκριμένης συμφωνίας που υφίσταται μεταξύ αυτού και του παρόχου υπηρεσιών *LBS*. Καθώς, όπως είπαμε, οι μέθοδοι κρυπτογράφησης ή ανωνυμοποίησης της προσωρινής ταυτότητας *Opaque ID* του συνδρομητή ενδέχεται να διαφέρουν από δίκτυο σε δίκτυο, πρέπει επίσης να είναι δυνατός ο προσδιορισμός του δικτύου που αρχικά το παρήγαγε, έτσι ώστε το *Opaque ID* να δρομολογηθεί στο σωστό δίκτυο και να αποκρυπτογραφηθεί. Επομένως, το *Opaque ID* ενδέχεται να πρέπει να εμπεριέχει τα *MCC* και *MNC.*

4.1.2.2.2 Χρήση του Opaque ID

Το *Opaque ID* μπορεί να χρησιμοποιηθεί σε πολλές διαφορετικές περιπτώσεις: **α)** όταν ο συνδρομητής προσπελαύνει κάποια υπηρεσία *LBS*, **β)** όταν ο πάροχος υπηρεσιών αιτείται για την εύρεση της θέσης του συνδρομητή και **γ)** όταν ο πάροχος υπηρεσιών προβαίνει σε άλλες ενέργειες που απαιτούν την ταυτότητα του συνδρομητή.

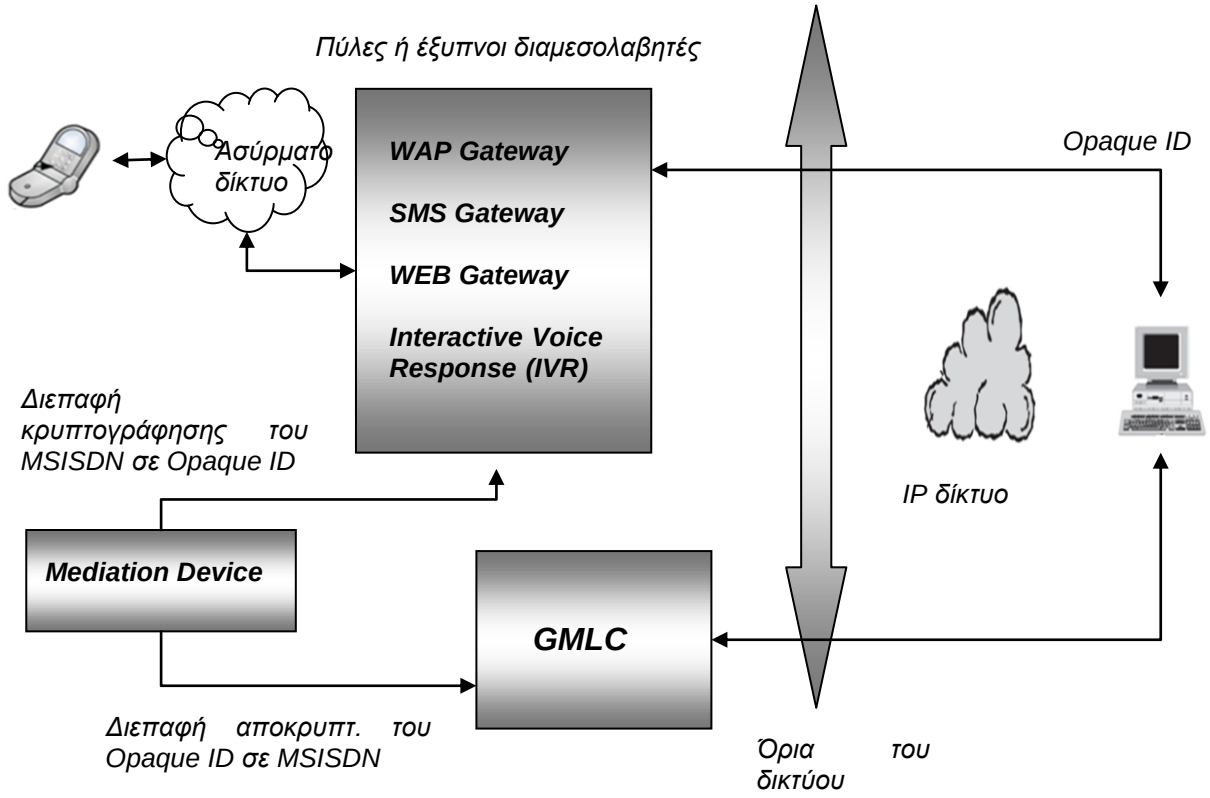
Η συσκευή διαμεσολάβησης επομένως θα πρέπει να είναι προσβάσιμη από:

1. Το *Gateway Mobile Location Centre (GMLC)* του δικτύου κινητών επικοινωνιών που κάνει την αίτηση. Σημειώστε ότι το *GMLC* είναι ο πρώτος κόμβος που συναντά ένας εξωτερικός *πελάτης Location Services (LCS)* σε ένα *GSM* ή *UMTS* δίκτυο. Ακολούθως το *GMLC* μπορεί να ζητήσει πληροφορίες δρομολόγησης από το οικείο δίκτυο του συνδρομητή. Μετά την ολοκλήρωση της καταχώρισης και της

εξουσιοδότησης, το *GMLC* αποστέλλει αιτήσεις εντοπισμού θέσης και λαμβάνει τις τελευταίες εκτιμήσεις θέσης από το δίκτυο στο οποίο περιάγει ο συνδρομητής.

2. Οποιαδήποτε πύλη (*gateway*) χρησιμοποιήθηκε για την πρόσβαση στην *LBS*.

Στο ***σχήμα 31*** περιγράφεται η διαδικασία κρυπτογράφησης της μόνιμης ταυτότητας του συνδρομητή, όταν γίνεται μια αίτηση *LBS*, και η αντίστοιχη της αποκρυπτογράφησης, όταν ο πάροχος υπηρεσιών ζητά τη θέση του συνδρομητή.



Σχήμα 31: Χρήση του *Opaque ID*

Το *Opaque ID* μπορεί να ισχύει για μια μόνο σύνοδο, να είναι στατικό ή να εκτείνεται πέραν της μιας συνόδου. Αναλυτικότερα, ένα ***Opaque ID συνόδου*** (*Session Opaque ID)* ανατίθεται όταν ο συνδρομητής ξεκινά να προσπελαύνει μια *LBS* και διαρκεί μέχρι το πέρας της πρόσβασής του σε αυτό. Για παράδειγμα, ένα *Session Opaque ID* μπορεί να ανατεθεί στην αρχή μιας *WAP (Wireless Application Protocol)* συνόδου και να διαγραφεί στο τέλος της. Στην περίπτωση αυτή θα μπορούσε να χρησιμοποιηθεί για οποιαδήποτε *LBS*, η οποία προσπελάστηκε κατά τη διάρκεια της ίδιας *WAP* συνόδου.

Ένα ***στατικό Opaque ID*** *(Static Opaque ID)* ανατίθεται όταν ο συνδρομητής ξεκινά να προσπελαύνει μια *LBS* και διατηρείται για όλες τις μελλοντικές προσβάσεις του στην ίδια *LBS*. Αυτό, για παράδειγμα, ενδέχεται να είναι ιδιαίτερα χρήσιμο στην περίπτωση που μια *LBS* χρειάζεται να εντοπίζει τη θέση των συνδρομητών σε συνεχόμενη βάση, όπως είναι η σταθμοσκόπηση (*polling*), και μπορεί να χρησιμοποιηθεί από τον πάροχο υπηρεσιών διαφανώς, δηλαδή χωρίς την ενεργή συμμετοχή του συνδρομητή.

Ένα ***εκτεταμένο Opaque ID*** *(Extended Opaque ID)* ανατίθεται όταν ο συνδρομητής ξεκινά να προσπελαύνει μια *LBS* και διαρκεί μέχρι την ολοκλήρωση της συνόδου, για συγκεκριμένο χρονικό διάστημα ή μέχρι να λάβει χώρα ένας συγκεκριμένος αριθμός χρήσεων. Έτσι ένα *Extended Opaque ID* είναι δυνατό να ανατεθεί στην αρχή μιας *WAP* συνόδου με την *LBS*, αλλά η επίδοση της πληροφορίας να γίνεται μετά το πέρας της συνόδου. Ως παράδειγμα αναφέρουμε την περίπτωση που ένας συνδρομητής προσπελαύνει μια *LBS* για να αποκτήσει πληροφορίες σχετικά με κάποιο δρομολόγιο, αλλά λαμβάνει τις πληροφορίες αυτές σε μορφή κειμένου αργότερα, ενώ ήδη ταξιδεύει προς τον προορισμό του.

4.1.3 Προστασία της Ιδιωτικότητας στο *Bluetooth*

Όπως είδαμε στα ασύρματα και κινητά δίκτυα επικοινωνιών, όπου οι χρήστες περιάγουν ανάμεσα σε διαφορετικούς ασύρματους τομείς (*domains*) ανακύπτει το ζήτημα της ιδιωτικότητας της γεωγραφικής θέσης στην οποία βρίσκονται ανά πάσα στιγμή. Εφ' όσον η τεχνολογία *Bluetooth* απευθύνεται σε προσωπικές κινητές συσκευές, όπως κινητά τηλέφωνα, *PDA*, φορητοί υπολογιστές κ.α., το ζήτημα αυτό αναδεικνύεται σε ιδιαίτερα σημαντικό. Η απειλή του εντοπισμού της γεωγραφικής θέσης είναι ανεξάρτητη από το εάν το *Bluetooth* θα χρησιμοποιηθεί για κάποια τοπική σύνδεση ή ως τεχνολογία πρόσβασης. Εφόσον λοιπόν κάποιος χρήστης μεταφέρει και χρησιμοποιεί τη συσκευή του, ελλοχεύει πάντοτε ο κίνδυνος εντοπισμού της μέσω των ραδιοσημάτων που αυτή εκπέμπει.

Από την άλλη πλευρά, για να είναι σε θέση ο επιτιθέμενος να εντοπίσει τις κινήσεις κάποιου χρήστη, θα πρέπει να υπάρχει κάποιο σταθερό αναγνωριστικό της συσκευής. Αν ο επιτιθέμενος κατορθώσει να αντιστοιχίσει την ταυτότητα μιας συσκευής στην ταυτότητα του κατόχου της, τότε η απειλή πραγματοποιείται. Κατά συνέπεια, όλα τα σταθερά αναγνωριστικά μιας συσκευής *Bluetooth* αποτελούν πιθανή απειλή για την ιδιωτικότητα του κατόχου της. Για παράδειγμα, η διεύθυνση της συσκευής *Bluetooth* ή οποιαδήποτε τιμή προέρχεται μονοσήμαντα από αυτήν και εκπέμπεται στο δίκτυο απροστάτευτη είναι ο προφανής στόχος μιας επίθεσης εντοπισμού της θέσης. Όμως, ακόμη και το όνομα της συσκευής ή οποιαδήποτε εφαρμογή που εκτελείται στη συσκευή και μπορεί να χρησιμοποιηθεί για την αποκάλυψη της ταυτότητας του χρήστη αποτελεί απειλή για την ιδιωτικότητά του.

Για να προστατευθεί μια συσκευή από επιθέσεις εντοπισμού θέσης, θα πρέπει να δημιουργηθεί μια ***κατάσταση ανωνυμίας*** *(anonymity state)*. Οι συσκευές που βρίσκονται σε κατάσταση ανωνυμίας επιβάλλεται να ανανεώνουν τακτικά τη διεύθυνση της συσκευής τους, επιλέγοντας μια τυχαία διεύθυνση.

4.1.3.1 Διεύθυνση Συσκευής και Εντοπισμός της Θέσης

Η σημαντικότερη απειλή εντοπισμού θέσης εκμεταλλεύεται τη διεύθυνση των συσκευών *Bluetooth*. Η δομή της διεύθυνσης ακολουθεί το πρότυπο *IEEE 802* και είναι μοναδική για κάθε συσκευή. Έτσι, η διεύθυνση των συσκευών *Bluetooth* μήκους 48 *bits* αποδίδεται στη συσκευή κατά τη φάση κατασκευής της και είναι γνωστή ως *BD_ADDR (Bluetooth Device Address).* Η εν λόγω διεύθυνση αποτελείται από τρία διαφορετικά τμήματα: **α)** κατώτερο τμήμα διεύθυνσης *(Lower Address Part, LAP*), **β)** ανώτερο τμήμα διεύθυνσης *(Upper Address Part, UAP)* και **γ)** μη σημαντικό τμήμα διεύθυνσης *(Non-significant Address Part, NAP).* Τα τμήματα *LAP* και *UAP* αποτελούν το σημαντικό τμήμα *(significant part)* της διεύθυνσης της συσκευής. Η *BD_ADDR* χρησιμοποιείται για την αναγνώριση των συσκευών όταν έχουν εγκατασταθεί συνδέσεις. Η δομή της διεύθυνσης *BD_ADDR* περιγράφεται στο ***σχήμα 32***. Η πλευρά που θέλει να εγκαταστήσει μια σύνδεση θα πρέπει να γνωρίζει τη διεύθυνση *BD_ADDR* της

συσκευής με την οποία θέλει να επικοινωνήσει, πριν από την εγκατάσταση της σύνδεσης. Έτσι η πλευρά που θέλει να εγκαταστήσει μια σύνδεση είναι αναγκαίο την πρώτη φορά να συλλέξει τις διευθύνσεις όλων των γειτονικών της συσκευών και στη συνέχεια να επιλέξει τη διεύθυνση της συσκευής που την ενδιαφέρει. Το βήμα αυτό είναι γνωστό ως ***διαδικασία διερεύνησης*** *(inquiry procedure).* Οι πληροφορίες από την προαναφερθείσα διαδικασία μπορούν να ξαναχρησιμοποιηθούν για τις επόμενες συνδέσεις με ήδη γνωστές συσκευές, χωρίς να απαιτούνται εκ νέου διαδικασίες διερεύνησης.

Σε ορισμένες περιπτώσεις, ολόκληρη η διεύθυνση της *Bluetooth* συσκευής αποστέλλεται μέσω ενός ειδικού ***πακέτου συγχρονισμού αναπήδησης συχνότητας*** *(Frequency Hop Synchronization, FHS*). Το γεγονός αυτό πιθανόν να τύχει εκμετάλλευσης από διάφορους τύπους επιθέσεων. Όμως αυτή δεν είναι και η μοναδική απειλή. Συγκεκριμένα, οποιαδήποτε τιμή προέρχεται αιτιοκρατικά από ολόκληρη ή από κάποιο τμήμα της διεύθυνσης μιας συσκευής μπορεί να χρησιμοποιηθεί για τον ίδιο σκοπό. Αυτό συμβαίνει στην περίπτωση του ***κώδικα πρόσβασης*** *(access code)* του *Bluetooth*. Ο κώδικας αυτός αποτελεί το πρώτο τμήμα κάθε πακέτου που μεταδίδει κάθε συσκευή *Bluetooth*. Υπάρχουν τρείς διαφορετικοί κώδικες πρόσβασης: **α) *Ο κώδικας πρόσβασης στο κανάλι*** *(Channel Access Code, CAC),* ο οποίος προέρχεται από το *LAP* της κύριας συσκευής, **β) *ο κώδικας πρόσβασης συσκευής*** (*Device Access Code, DAC*), ο οποίος προέρχεται από το *LAP* κάποιας συγκεκριμένης εξαρτημένης συσκευής και **γ) *ο κώδικας πρόσβασης διερεύνησης*** *(Inquiry Access Code, IAC),* ο οποίος είναι δυνατό να λάβει δύο μορφές, αλλά προέρχεται από ειδικές τιμές *LAP* που δεν σχετίζονται με καμία συγκεκριμένη *BD_ADDR.* Επομένως, μόνο οι *CAC* και *DAC* μπορούν να χρησιμοποιηθούν για τον εντοπισμό της θέσης ενός συγκεκριμένου χρήστη.

MSB ***LSB***

BD_ADDR (48 bits)

NAP (16 bits)	***UAP (8 bits)***	***LAP (24 bits)***
Non-significant Address Part	***Upper Address Part***	***Lower Address Part***

Σχήμα 32: Η δομή της διεύθυνσης μιας συσκευής *Bluetooth*

4.1.3.2 Επιθέσεις Εντοπισμού Θέσης

Όπως είδαμε, άμεσα ή έμμεσα η χρήση μιας σταθερής διεύθυνσης συσκευής παρέχει τη δυνατότητα σε κακόβουλους χρήστες να εντοπίζουν τη θέση των συσκευών *Bluetooth*. Ο *CAC* ή ο *DAC* είναι δυνατό να χρησιμοποιηθούν για την αναγνώριση μιας συγκεκριμένης συσκευής. Επιπλέον, το όνομα μιας συσκευής είναι επίσης πιθανό να χρησιμοποιηθεί για την παρακολούθηση της θέσης της.

4.1.3.2.1 Επίθεση Παρακολούθησης Κίνησης (Traffic Monitoring Attack)

Η επίθεση παρακολούθησης κίνησης ενδέχεται να είναι επιτυχής ακόμη και αν η συσκευή του θύματος έχει τεθεί σε μη ανιχνεύσιμη κατάσταση. Ο επιτιθέμενος απλώς παρακολουθεί τις επικοινωνίες μεταξύ δύο έμπιστων συσκευών που ανήκουν στο θύμα. Οι συσκευές αυτές επικοινωνούν, χρησιμοποιώντας κάποιο συγκεκριμένο κώδικα

πρόσβασης στο κανάλι *CAC*. Ο συγκεκριμένος *CAC* υπολογίζεται από τη διεύθυνση συσκευής της κύριας συσκευής του μικροδικτύου. Συνεπώς, ο επιτιθέμενος μπορεί να ανακαλύψει τις κύριες συσκευές που υπάρχουν στην περιοχή, απλώς παρακολουθώντας τη δικτυακή κίνηση. Αν και ο *CAC* δεν προσδιορίζει μοναδικά μια συσκευή, ο επιτιθέμενος έχει τη δυνατότητα να είναι σχεδόν σίγουρος ότι ο συγκεκριμένος CAC ανήκει σε μία μοναδική συσκευή, επειδή υπάρχει πολύ μικρή πιθανότητα σε μια μικρή περιοχή να υπάρχουν δύο συσκευές που έχουν τον ίδιο *CAC*. Ακόμα, εφόσον αποστέλλεται ολόκληρη η διεύθυνση με τα πακέτα *FHS* των συσκευών, ο επιτιθέμενος είναι σε θέση να προσδιορίσει μοναδικά την ταυτότητα κάθε συσκευής. Η επίθεση που βασίζεται στην παρακολούθηση του *DAC* ή των πακέτων *FHS* δεν είναι τόσο αποτελεσματική όσο εκείνη που βασίζεται στην παρακολούθηση του *CAC*, αφού τα πακέτα *FHS* ή τα πακέτα που περιέχουν *DAC* χρησιμοποιούνται μόνο κατά την εγκατάσταση συνδέσεων και επομένως είναι σχετικά σπάνια.

4.1.3.2.2 Επίθεση Διερεύνησης (Inquiry Attack)

Στην εν λόγω επίθεση ο επιτιθέμενος έχει διασκορπίσει συσκευές *Bluetooth* στην περιοχή που επιθυμεί να είναι ικανός να εντοπίζει χρήστες *Bluetooth*. Το απαιτούμενο κόστος είναι σχετικά μικρό, αφού σήμερα οι συσκευές *Bluetooth* είναι αρκετά φθηνές. Το δίκτυο που δημιουργείται είναι δυνατό να χρησιμοποιείται και για νόμιμους σκοπούς, όπως ένα δημόσιο περίπτερο πληροφοριών, συνεπώς θα μπορούσε ακόμα και να προϋπάρχει. Θεωρούμε επίσης ότι το θύμα της επίθεσης έχει αφήσει τη συσκευή του σε ανιχνεύσιμη κατάσταση. Στην περίπτωση αυτή η επιτιθέμενη συσκευή απλώς σαρώνει την περιοχή, εκπέμποντας συχνά μηνύματα διερεύνησης για συσκευές, και καταγράφει όλες τις διευθύνσεις συσκευών που ανακαλύπτει. Αν συσχετιστούν χρονικά τότε τα δεδομένα αυτά είναι δυνατό να παράξουν μια λεπτομερή καταγραφή των κινήσεων του θύματος καθώς και των συναναστροφών του, αφού, για παράδειγμα, αν δύο άνθρωποι πηγαίνουν συχνά στα ίδια μέρη, ενδέχεται να έχουν κάποια σχέση μεταξύ τους.

4.1.3.2.3 Επίθεση Σελιδοποίησης (Paging Attack)

Το πρώτο βήμα για την ανεύρεση άλλων συσκευών είναι η αποστολή ενός μηνύματος διερεύνησης. Το μήνυμα αυτό εκπέμπεται κατ' εξακολούθηση μέσω μιας καλά ορισμένης και μικρής σειράς 32 συχνοτήτων *(hop sequence).* Συνεπώς, κάθε συσκευή, η οποία επιθυμεί να είναι προσπελάσιμη από τις άλλες, ελέγχει συχνά τις συχνότητες αυτές για τυχόν μηνύματα διερεύνησης. Η διαδικασία αυτή ονομάζεται ***έλεγχος διερεύνησης*** *(inquiry scan).* Μια συσκευή που ελέγχει για μηνύματα διερεύνησης θα απαντήσει στα ερωτήματα αυτά, αποστέλλοντας τη διεύθυνσή της και την τιμή του τοπικού της ρολογιού. Το μήνυμα διερεύνησης είναι ανώνυμο και δεν υπάρχουν μηνύματα επιβεβαίωσης (*ACK*) για την απάντηση. Άρα η συσκευή που ελέγχει για μηνύματα διερεύνησης δεν γνωρίζει ποιός έκανε τη διερεύνηση ούτε και αν ο δεύτερος έλαβε σωστά την απάντησή της. Η συσκευή που προχωρά σε διερεύνηση συλλέγει τις απαντήσεις για κάποιο διάστημα και μπορεί, αν θέλει, να προσεγγίσει μια συγκεκριμένη συσκευή μέσω ενός ***μηνύματος σελίδας*** *(page message).* Το μήνυμα αυτό αποστέλλεται μέσω μιας άλλης σειράς συχνοτήτων, η οποία επίσης αποτελείται από 32 συχνότητες και ορίζεται από τα τελευταία 24 *bits* της *BD_ADDR* της διεύθυνσης της συσκευής προορισμού, δηλαδή της *LAP*. Μία συσκευή λαμβάνει τα μηνύματα σελίδας όταν βρίσκεται σε ***κατάσταση ελέγχου σελίδας*** *(page scan state).*

Η εν λόγω επίθεση εκμεταλλεύεται την προαναφερθείσα κατάσταση και επιτρέπει στον επιτιθέμενο να διακριβώσει αν μια συσκευή με γνωστή *BD_ADDR* ή *DAC* βρίσκεται σε μια συγκεκριμένη περιοχή. Προϋπόθεση για την επιτυχία της επίθεσης είναι η συσκευή

του θύματος να είναι σε ***κατάσταση σύνδεσης***. Η συσκευή που φέρει ο επιτιθέμενος εκπέμπει μηνύματα σελίδας στη συσκευή-στόχο, περιμένει να της επιστραφεί ένα πακέτο *ID* και στη συνέχεια δεν αποκρίνεται. Αν λάβει πακέτο *ID*, ο επιτιθέμενος γνωρίζει ότι το θύμα βρίσκεται στην περιοχή. Η συσκευή-θύμα από την πλευρά της, αφού δεν θα πάρει απάντηση, δεν θα αναφέρει το γεγονός στο επίπεδο αναφοράς.

4.1.3.2.4 Επίθεση που Βασίζεται στο User-friendly Όνομα των Συσκευών

Η *Link Manager Protocol (LMP)* εντολή του *Bluetooth, LMP name req* είναι δυνατό να χρησιμοποιηθεί για να ζητήσει το φιλικό *(user-friendly)* όνομα μιας συσκευής οποιαδήποτε στιγμή μετά την επιτυχή διαδικασία σελιδοποίησης του *baseband*. Έτσι, η εν λόγω εντολή ενδέχεται να χρησιμοποιηθεί για να υποβληθεί ερώτηση στα πλαίσια επίθεσης εντοπισμού θέσης. Η επίθεση θα είναι επιτυχής, αν η συσκευή-θύμα είναι σε κατάσταση σύνδεσης και έχει ένα μοναδικό *user-friendly* όνομα.

4.1.3.2.5 Επίθεση Αναπήδησης Συχνοτήτων (Frequency Hopping Attack)

Το σχήμα αναπήδησης συχνοτήτων *(frequency hopping scheme)* που χρησιμοποιείται στο *Bluetooth* καθορίζεται από μία επαναλαμβανόμενη ακολουθία αναπηδήσεων. Η σειρά των αναπηδήσεων υπολογίζεται με βάση διάφορες παραμέτρους, όπως μια διεύθυνση και το ρολόι της κύριας συσκευής. Σε κατάσταση σύνδεσης χρησιμοποιούνται η *LAP* και τα τέσσερα λιγότερο σημαντικά *bits (Least Significant Bits, LSB)* της *UAP* της κύριας συσκευής. Σε κατάσταση σελίδας *(page state)* χρησιμοποιείται η *LAP/UAP* της συσκευής που έχει δεχτεί το μήνυμα σελίδας. Έτσι, θεωρητικά, υπάρχει το ενδεχόμενο υποκλοπής πληροφοριών για τη *LAP* καθώς και για τα τέσσερα σημαντικά *bits* της *UAP* από κάποιον επιτιθέμενο, ο οποίος παρατηρεί τη σειρά αναπηδήσεων συχνότητας.

4.1.4 Ζητήματα Ιδιωτικότητας σε Οχηματικά Δίκτυα

Τα οχηματικά δίκτυα ή *VANET (Vehicular Ad-Hoc Networks)* λαμβάνουν όλο και μεγαλύτερη προσοχή τα τελευταία χρόνια από το χώρο της βιομηχανίας και της εκπαίδευσης. Ουσιαστικά, αποτελούν ***αδόμητα ασύρματα δίκτυα*** (*MANETs*) όπου οι κινητοί κόμβοι είναι οχήματα (αυτοκίνητα, φορτηγά ή μοτοσυκλέτες) και όχι, για παράδειγμα, κινητές συσκευές. Στο όχι και τόσο μακρινό μέλλον αναμένεται ότι κάθε είδους όχημα θα είναι εξοπλισμένο με αισθητήρες και θα έχει υπολογιστικές ικανότητες που θα του επιτρέπουν να επικοινωνεί με άλλα οχήματα αλλά και με την εκάστοτε υποδομή των οδικών δικτύων.

Οι εφαρμογές των οχηματικών δικτύων είναι πολλές και σημαντικές. Τα οχήματα είναι δυνατό να μεταδίδουν πληροφορίες σχετικά με ατυχήματα και επικίνδυνες οδικές συνθήκες ή να προειδοποιούν τα οχήματα που τα ακολουθούν για την κίνηση στους δρόμους. Μηνύματα επίσης μπορούν να μεταδίδονται από και προς την υπάρχουσα οδική υποδομή, τα οποία σχετίζονται με την ασφάλεια του οδικού δικτύου, την πιθανή κίνηση σε διάφορα σημεία του, την πληρωμή διοδίων ή ακόμα και με εφαρμογές που έχουν να κάνουν με τη διασκέδαση των οδηγών.

Τα ειδικά χαρακτηριστικά των οχηματικών δικτύων που τα διαφοροποιούν από τα *MANETs* είναι το μεγάλο πλήθος των μελών που τα αποτελούν, καθώς και η μεγάλη ταχύτητα με την οποία οι κόμβοι, δηλαδή τα οχήματα, κινούνται. Είναι σαφές επομένως ότι τα οχηματικά δίκτυα είναι πολύ ευπαθή σε παθητικές και ενεργητικές επιθέσεις. Το γεγονός αυτό σε συνδυασμό με το μεγάλο εύρος εφαρμογών των οχηματικών δικτύων κάνει επιτακτική την ανάγκη υιοθέτησης μηχανισμών ασφάλειας που θα ικανοποιούν

βασικές ιδιότητες όπως η πιστοποίηση μηνυμάτων, η διαθεσιμότητα του δικτύου, η εμπιστευτικότητα και η ιδιωτικότητα. Το ζήτημα που ερευνητικά παρουσιάζει μεγάλο ενδιαφέρον είναι η υλοποίηση μηχανισμών που θα είναι ικανοί να προστατεύουν την ιδιωτικότητα των οχημάτων (έτσι ώστε για παράδειγμα, να μην μπορεί κάποιος να παρακολουθεί τη διαδρομή ενός οχήματος), ενώ ταυτόχρονα θα είναι σε θέση να εντοπίσουν τα οχήματα που έχουν προκαλέσει κάποιο ατύχημα ή η οδική τους συμπεριφορά είναι επικίνδυνη.

Τέλος σημειώνεται, ότι για την ομαλή λειτουργία ενός οχηματικού δικτύου θα πρέπει τα οχήματα να ανταλλάσσουν συχνά μηνύματα μεταξύ τους. Κάθε κόμβος του δικτύου (δηλαδή κάθε όχημα) επιβάλλεται να στέλνει κάθε τόσο ένα μήνυμα (*hello beacon)* προς τους γειτονικούς του κόμβους και την υποδομή του οδικού δικτύου, που θα περιέχει (τουλάχιστον) έναν κωδικό ταυτοποίησης (*identifier*) και τη γεωγραφική του θέση.

4.1.4.1 Η Σημασία της Ιδιωτικότητας στα Οχηματικά Δίκτυα

Τα οχήματα αποτελούν για κάθε άνθρωπο σημαντικό κομμάτι της προσωπικής του ιδιοκτησίας και οι περισσότεροι από εμάς έχουμε το ίδιο αυτοκίνητο για αρκετά χρόνια. Στις περισσότερες κοινωνικές ομάδες, τα αυτοκίνητα αποτελούν σύμβολα κύρους και πλούτου, ενώ πολλά χαρακτηριστικά της προσωπικότητας ενός ατόμου μπορούν να αποκαλυφθούν βάσει του αυτοκινήτου που οδηγεί. Επιπλέον, τα μελλοντικά οχήματα θα είναι εξοπλισμένα με συστήματα πλοήγησης και έτσι θα υπάρχει η δυνατότητα να συγκεντρώνουν στοιχεία για συγκεκριμένες διαδρομές που ακολουθεί ο οδηγός τους. Το γεγονός αυτό σε συνδυασμό με τις μελλοντικές δυνατότητες επικοινωνίας που θα διαθέτει κάθε όχημα, όπως, για παράδειγμα, συστήματα ηλεκτρονικής πληρωμής διοδίων, πρόσβαση στο διαδίκτυο και δυνατότητα λήψης λογισμικού και αρχείων, κάνει την ανάγκη για ιδιωτικότητα ιδιαίτερα επιτακτική.

Στη συνέχεια παρουσιάζουμε διάφορες καταστάσεις όπου η ιδιωτικότητα των χρηστών των οχηματικών δικτύων μπορεί να παραβιαστεί. Επίσης, θα σημειώσουμε ότι σε πολλές περιπτώσεις δεν είναι επιθυμητό να πετύχουμε τέλεια ιδιωτικότητα. Θα πρέπει να αποφασιστεί τι βαθμός ιδιωτικότητας απαιτείται σε κάθε περίπτωση και ανάλογα να σχεδιαστεί το σύστημά μας. Πιθανά σενάρια που θα δημιουργούσαν προβλήματα στην ιδιωτικότητα των οχηματικών δικτύων είναι τα εξής:

- Η αστυνομία θα μπορούσε να εκπέμψει κατάλληλα σήματα (*hello beacons)* για να προσδιορίσει την ταχύτητα των οχημάτων σε οποιοδήποτε σημείο του οδικού δικτύου και ακολούθως να στείλει κλήσεις για παραβίαση του ορίου ταχύτητας,
- Κάποιος ωτακουστής εργοδότης θα είχε τη δυνατότητα να παρακολουθεί τα μηνύματα που ανταλλάσσουν τα αυτοκίνητα στο χώρο στάθμευσης της εταιρείας και προσδιορίζοντας ποιό αυτοκίνητο ανήκει σε κάθε εργαζόμενο, να γνωρίζει κάθε ημέρα το χρόνο άφιξης και αναχώρησής του από την εταιρεία,
- Ένας ιδιωτικός αστυνομικός θα μπορούσε να παρακολουθήσει ένα όχημα από τα μηνύματα που αυτό στέλνει είτε σε άλλα αυτοκίνητα ή στη δικτυακή υποδομή του οδικού δικτύου,
- Ασφαλιστικές εταιρείες μπορούν να συλλέγουν λεπτομερή στατιστικά στοιχεία για τον τρόπο οδήγησης και τις διαδρομές που ακολουθούν συνήθως οι οδηγοί. Τα στοιχεία αυτά θα ήταν δυνατό να τα χρησιμοποιήσουν είτε για την καταδίκη ενός οδηγού για κάποιο ατύχημα ή για να μην καταβάλλουν κάποια αποζημίωση (γιατί τα στοιχεία τους αποδεικνύουν, για παράδειγμα, ότι ο κάτοχος του οχήματος οδηγεί επικίνδυνα),

- Επίσης ωτακουστές θα μπορούσαν να συλλέγουν παρόμοια στατιστικά στοιχεία με σκοπό το κέρδος. Για παράδειγμα, τα συλλεχθέντα στοιχεία ίσως πωληθούν σε διαφημιστικές εταιρείες, οι οποίες θα ενοχλούν συνεχώς τους οδηγούς με διαφημίσεις,
- Μια ομάδα εγκληματιών ενδεχομένως να έχει πρόσβαση στην υποδομή του οδικού δικτύου και να χρησιμοποιεί τις πληροφορίες που υποκλέπτονται για να προσδιορίσει τη θέση των οχημάτων της αστυνομίας.

Όπως φαίνεται από τα παραπάνω παραδείγματα, τα περισσότερα ζητήματα που σχετίζονται με την ιδιωτικότητα αφορούν στη θέση του οχήματος ή στην ταυτότητά του. Αναλύοντας τις σχέσεις που μπορούν να προκύψουν μεταξύ ζευγαριών {θέσης, ταυτότητας} πιθανόν να συντελεστούν μια σειρά από επιθέσεις.

Στο πρώτο σενάριο είναι πολύ εύκολο να προκύψει λύση λόγω του ότι στις περισσότερες χώρες ένας κατηγορούμενος θεωρείται αθώος μέχρι να αποδειχθεί το αντίθετο. Στην περίπτωση του παραδείγματός μας, αυτό σημαίνει ότι η αστυνομία θα πρέπει να είναι σε θέση να αποδείξει ότι ο κατηγορούμενος είναι πραγματικά αυτός που ξεπέρασε το όριο ταχύτητας. Άρα, για να ξεπεραστεί η απειλή αυτή ως προς την ιδιωτικότητα των οδηγών, αρκεί από το σύστημα να χρησιμοποιείται ένα ψευδώνυμο αντί της πραγματικής ταυτότητας του οδηγού ή του οχήματος. Προφανώς, αν δεν είναι εύκολο να αποκαλυφθεί η αντιστοίχιση ενός ψευδωνύμου με την πραγματική ταυτότητα του χρήστη, η αστυνομία δεν θα μπορεί εύκολα να στέλνει κλήσεις στους οδηγούς.

Στο δεύτερο σενάριο η λύση της χρήσης ενός ψευδωνύμου ίσως να μην είναι αρκετή. Ο λόγος είναι ότι ένας εργοδότης που απασχολεί περιορισμένο αριθμό εργαζομένων μπορεί με μεγαλύτερη ευχέρεια να συσχετίσει πρόσωπα με οχήματα. Στην περίπτωση αυτή, μια αποδοτική λύση θα ήταν η αλλαγή του ψευδωνύμου ενός οχήματος ανά τακτά χρονικά διαστήματα.

Στις τέσσερις τελευταίες περιπτώσεις, ακόμα και η συχνή αλλαγή ψευδωνύμων δεν θα ήταν αρκετή. Για να αποτραπεί η παρακολούθηση ενός οχήματος, θα πρέπει το ψευδώνυμό του να αλλάζει ενώ το όχημα κινείται. Μια λύση είναι τα λεγόμενα ***ψευδώνυμα geobound***, δηλαδή ***τα ψευδώνυμα που εξαρτώνται από τη γεωγραφική θέση***. Αναλυτικότερα, σε κάθε γεωγραφική θέση υπάρχει διαθέσιμο ένα συγκεκριμένο σύνολο ψευδώνυμων. Έτσι, κάθε φορά που κάποιο όχημα διέρχεται από αυτή τη θέση λαμβάνει με τυχαίο τρόπο κάποιο από τα ψευδώνυμα του συνόλου. Παρά τα πλεονεκτήματα που προσφέρουν τα ψευδώνυμα *geobound*, η υιοθέτησή τους μπορεί να μειώσει τη συνολική απόδοση του συστήματος λόγω των πιθανών συγκρούσεων (*collisions*) και του αυξημένου φόρτου σηματοδοσίας *(signaling overhead).*

Τέλος, υπάρχουν περιπτώσεις όπου η πραγματική ταυτότητα του οχήματος πρέπει να γίνεται γνωστή. Για παράδειγμα, όταν ένα όχημα επικοινωνεί με ένα οικείο όχημα, σταθμό ή διόδια. Επομένως, για να προστατευθεί η ιδιωτικότητα του συγκεκριμένου χρήστη απαιτείται η προστασία της πραγματικής του ταυτότητας από τα μη εξουσιοδοτημένα γειτονικά οχήματα που πιθανόν να ακούν την επικοινωνία και παθητικά ή ενεργητικά υποκλέπτουν τα μηνύματα που ανταλλάσσει.

4.1.4.2 Απαιτήσεις για την Επίτευξη της Ιδιωτικότητας

Οδηγούμενοι από τις επιθέσεις κατά της ιδιωτικότητας που αναφέρθηκαν στην προηγούμενη ενότητα και από τις λύσεις που προτάθηκαν, ορισμένες βασικές απαιτήσεις για την επίτευξη ενός ικανοποιητικού βαθμού ιδιωτικότητας μπορούν να αποτυπωθούν:

- Είναι χρήσιμο να χρησιμοποιούνται ψευδώνυμα αντί των πραγματικών ταυτοτήτων των οδηγών ή των οχημάτων,
- Τα ψευδώνυμα θα πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα ανάλογα με τις απαιτήσεις του συστήματος,
- Η συχνότητα αλλαγής των ψευδωνύμων εξαρτάται από την εκάστοτε εφαρμογή και το βαθμό ιδιωτικότητας που απαιτείται,
- Τα ψευδώνυμα που χρησιμοποιούνται κατά τη διάρκεια μιας συγκεκριμένης επικοινωνίας θα πρέπει να μπορούν να συσχετιστούν με την πραγματική ταυτότητα του χρήστη. Αυτό είναι απαραίτητο σε ειδικές περιπτώσεις που απαιτείται, π.χ. κατόπιν εισαγγελικής άδειας η άρση της ανωνυμίας του.

Αυτό που έχει μεγάλη σημασία στο σχεδιασμό των οχηματικών δικτύων επικοινωνιών είναι η επίτευξη μιας καλής ισορροπίας μεταξύ της ιδιωτικότητας και της υποχρέωσης λογοδοσίας (*accountability*). Αυτό που προτείνεται στις περισσότερες πρόσφατες επιστημονικές εργασίες για την καλύτερη διαχείριση του συγκεκριμένου προβλήματος είναι η χρήση κρυπτογραφικών τεχνικών. Για παράδειγμα, μπορούν να χρησιμοποιηθούν ψηφιακές υπογραφές για την πιστοποίηση μηνυμάτων σε συνδυασμό με τη χρήση ψευδωνύμων που αλλάζουν συχνά, με σκοπό την επίτευξη εξαρτημένης (*conditional*) ανωνυμίας.

Τέλος, ένα ερώτημα που προκύπτει είναι πώς θα μοιράζονται τα ψευδώνυμα στα οχήματα. Για τη λύση του προβλήματος αυτού προτείνεται η χρήση μιας έμπιστης τρίτης οντότητας *(Trusted Third Party, TTP)* που θα αποθηκεύει τις πραγματικές ταυτότητες των χρηστών και των οχημάτων και θα αντιστοιχίζει σε κάθε οντότητα ένα σύνολο ψευδωνύμων. Η απεικόνιση αυτή θα πρέπει να κρατείται μυστική και να αποκαλύπτεται μόνο σε συγκεκριμένες, ειδικές περιπτώσεις. Αναλυτικότερα, κατά τη φάση της κατασκευής του οχήματος, η έξυπνη κάρτα που θα εγκαθίσταται σε αυτό θα αποστέλλει την ταυτότητα του οχήματος στην έμπιστη οντότητα. Η τελευταία θα παράγει με βάση κάποιες κρυπτογραφικές αρχές ένα σύνολο ψευδωνύμων, έχοντας ως είσοδο τη μοναδική ταυτότητα του οχήματος και πιθανώς κάποιες άλλες παραμέτρους. Τα ψευδώνυμα αυτά θα μεταφέρονται στη συνέχεια πίσω στο ασφαλές περιβάλλον *(tamper resistant)* της έξυπνης κάρτας.

4.1.5 Επίλογος

Οι μηχανισμοί προστασίας της **ι**διωτικότητας που μελετήθηκαν, έχουν στόχο την προστασία της ταυτότητας και της γεωγραφικής θέσης των χρηστών στο ασύρματο περιβάλλον. Η ανάλυση επικεντρώνεται σε ασύρματα δικτυακά περιβάλλοντα *UMTS*, *Bluetooth* και *VANET*. Παρ' όλα αυτά τα περισσότερα ζητήματα που αναπτύχθηκαν αφορούν οποιαδήποτε ασύρματη δικτυακή τεχνολογία πρόσβασης.

Οι μηχανισμοί αυτοί και οι τεχνολογίες θα αποκτούν ολοένα και μεγαλύτερη σημασία τα επόμενα χρόνια, όσο οδεύουμε προς το ενοποιημένο *(all-IP)* δικτυακό περιβάλλον τέταρτης γενιάς *(4G).* Η εισαγωγή του πρωτοκόλλου *IP* στα δίκτυα κορμού των παρόχων υπηρεσιών, το ολοένα αυξανόμενο πλήθος των συνδρομητών χρηστών, οι πολύπλοκες σχέσεις που αναμένεται να αναπτυχθούν μεταξύ των παρόχων, η διασύνδεση των δικτύων αυτών με το διαδίκτυο και το ετερογενές περιβάλλον πρόσβασης είναι μερικοί από τους λόγους που τα ζητήματα ασφάλειας και ιδιωτικότητας αναμένεται να αναθεωρηθούν. **[15]**

4.2 Μέλη Ψηφιακών Κοινοτήτων και Προστασία της Ιδιωτικότητας

Οι τεχνολογίες πληροφορικής και επικοινωνιών που στηρίζονται στη χρήση του διαδικτύου ευνοούν την ανάπτυξη νέων τρόπων και πρακτικών επικοινωνίας μεταξύ των ανθρώπων. Παραδοσιακά, η δημιουργία μιας κοινότητας είναι συνυφασμένη με τη φυσική αλληλεπίδραση των ανθρώπων, που συναντώνται πρόσωπο με πρόσωπο. Οι ψηφιακές κοινότητες *(Digital Communities)* γνωστές επίσης και ως διαδικτυακές κοινότητες, εικονικές κοινότητες ή κοινωνικά δίκτυα είναι ομάδες ανθρώπων που μοιράζονται κοινά ενδιαφέροντα και επικοινωνούν μεταξύ τους μέσω του διαδικτύου. Σύμφωνα με έναν από τους πιο δημοφιλείς ορισμούς, οι ***ψηφιακές κοινότητες*** είναι «…***κοινωνικές συναθροίσεις που προκύπτουν στο διαδίκτυο, όταν αρκετοί άνθρωποι εμπλέκονται σε δημόσιες συζητήσεις για αρκετό διάστημα, με επαρκές συναίσθημα, ώστε να δημιουργηθούν δίκτυα προσωπικών σχέσεων στον κυβερνοχώρο»***. Σε αντίθεση με τις παραδοσιακές κοινότητες, που συνήθως περιορίζονται σε μια τοποθεσία, οι ψηφιακές κοινότητες δεν έχουν γεωγραφικούς περιορισμούς. Επίσης οι παραδοσιακές κοινότητες είναι γενικά πολύ μικρότερες από τις ψηφιακές. Τα σύγχρονα διαδικτυακά κοινωνικά δίκτυα παρουσιάζουν αλματώδη αύξηση των μελών τους, ορισμένα μάλιστα αριθμούν εκατοντάδες χιλιάδες μέλη.

Καθώς η ύπαρξη των ψηφιακών κοινοτήτων εξαρτάται από την αλληλεπίδραση και την επικοινωνία των μελών τους μέσω του διαδικτύου, το άγραφο κοινωνικό συμβόλαιο μεταξύ των μελών και τα ιδιαίτερα πολιτισμικά χαρακτηριστικά κάθε κοινότητας καθορίζουν τις αποδεκτές συμπεριφορές και διαμορφώνουν τις σχέσεις μεταξύ των χρηστών. Οι διαδικτυακές σχέσεις αναπτύσσονται διαφορετικά από τις σχέσεις πρόσωπο-με-πρόσωπο. Η απουσία φυσικής συνύπαρξης επιτρέπει στα άτομα να αλλάζουν την ταυτότητά τους και μειώνει την επίδραση που έχουν κανόνες και νόρμες στην ατομική συμπεριφορά και που συνήθως καθορίζουν τις κοινωνικές σχέσεις. Για να αντισταθμίσουν την έλλειψη αυτή, οι περισσότερες ψηφιακές κοινότητες χρησιμοποιούν μέσα όπως ***forum συζητήσεων*** με διαχειριστή, κανόνες ασφάλειας και εχεμύθειας, κώδικες συμπεριφοράς και πολιτικές λειτουργίας.

Τα μέλη των ψηφιακών κοινοτήτων συνήθως μοιράζονται προσωπικές πληροφορίες και ανάλογα με το είδος της κοινότητας στην οποία ανήκουν, ενδέχεται να κοινοποιούν και πληροφορίες που είναι εξαιρετικά αποκαλυπτικές, όπως προβλήματα υγείας ή οικογενειακά προβλήματα, ερωτικές προτιμήσεις, μύχιες σκέψεις τους κ.λπ. Δεδομένου ότι τα ζητήματα διαφύλαξης της ιδιωτικότητας απασχολούν τους χρήστες του διαδικτύου σε σημαντικό βαθμό, και μάλιστα θεωρείται ότι αποτελούν έναν από τους βασικούς παράγοντες ανάσχεσης του ηλεκτρονικού εμπορίου, το σχετικά νέο αυτό φαινόμενο ατόμων που ανταλλάσσουν προσωπικές πληροφορίες μέσω του διαδικτύου χωρίς να γνωρίζονται απαιτεί διεξοδική διερεύνηση. Επίσης, η δυνατότητα που δίνεται σε άτομα και ομάδες να αλληλεπιδρούν από μεγάλη απόσταση δημιουργεί και άλλα ζητήματα που χρειάζονται περαιτέρω διερεύνηση, όπως είναι η προστασία της προσωπικής ταυτότητας *(personal identity)* κάθε χρήστη.

Άραγε η εκθετική αύξηση του αριθμού των μελών ψηφιακών κοινοτήτων (όπως το *MySpace.com*) φανερώνει ότι οι χρήστες δεν ανησυχούν για την προστασία της ιδιωτικότητάς τους; Ή, αν κάτι τέτοιο δεν συμβαίνει, ποιούς προβληματισμούς έχουν και πώς αντιλαμβάνονται τους κινδύνους κατά της ιδιωτικότητας; Χρησιμοποιούν μέσα και τρόπους προστασίας και, εάν ναι, ποιά είναι αυτά;

4.2.1 Ψηφιακές Κοινότητες

4.2.1.1 Αναγνωρίζοντας τις Ψηφιακές Κοινότητες

Οι ψηφιακές κοινότητες συχνά περιγράφονται ως φανταστικές και όχι ως πραγματικές, λόγω της απουσίας της φυσικής συνύπαρξης των μελών τους. Ο *Anderson* χρησιμοποίησε πρώτος τον όρο ***φανταστική κοινότητα***, υποστηρίζοντας ότι τα μέλη μιας τέτοιας κοινότητας διατηρούν στο μυαλό τους την εικόνα της σχέσης και ότι ***«…ποτέ δε θα γνωρίσουν τα περισσότερα μέλη της κοινότητας στην οποία ανήκουν, δεν θα τα συναντήσουν ούτε θα τα ακούσουν, ωστόσο στο μυαλό κάθε μέλους υπάρχει η εικόνα της κοινωνίας τους»***. Μόνο πρόσφατα άρχισε να αμφισβητείται η έως τώρα παγωμένη άποψη ότι βασική προϋπόθεση για την ύπαρξη μιας κοινωνίας είναι η συνύπαρξη των μελών της, μέσα από την έρευνα και τη σχετική βιβλιογραφία στο θέμα των ψηφιακών κοινοτήτων.

Εφόσον η συνύπαρξη δεν θεωρείται πλέον αναγκαία προϋπόθεση, τι είναι τότε αυτό που καθορίζει μια κοινότητα; Έχουν προταθεί πολλές και διαφορετικές απαντήσεις στο ερώτημα αυτό. Οι ψηφιακές κοινότητες μπορούν, σύμφωνα με μια προσέγγιση, να κατηγοριοποιηθούν σε **α)** κοινότητες συναλλαγών *(Communities of Transactions*), **β)** κοινότητες κοινού ενδιαφέροντος *(Communities of Interest*), **γ)** κοινότητες σχέσεων ή κοινής πρακτικής *(Communities of Practice or Relations)* και **δ)** κοινότητες φαντασίας *(Communities of Fantasy)*. Οι κοινότητες συναλλαγών αποτελούνται κατά κύριο λόγο από άτομα που μετέχουν σε συναλλαγές ηλεκτρονικού εμπορίου (αγοραστές-πωλητές), ενώ τα μέλη μιας κοινότητας ενδιαφέροντος μοιράζονται ένα κοινό ενδιαφέρον ή πάθος, όπως για παράδειγμα, ένα άθλημα, μουσική ή κηπουρική. Τα μέλη μιας τέτοιας κοινότητας ανταλλάσσουν ιδέες σχετικά με το κοινό τους ενδιαφέρον και ταυτόχρονα μπορεί να ανταλλάσσουν και κάποιες προσωπικές πληροφορίες. Οι κοινότητες κοινής πρακτικής αποτελούνται από άτομα με κοινές ιδέες και αντιλήψεις, τα οποία συνήθως ασκούν παρόμοιες επαγγελματικές δραστηριότητες και μέσα από τη συμμετοχή τους και τη συνεργασία στο πλαίσιο της ψηφιακής κοινότητας στοχεύουν στην αλληλοϋποστήριξη, στην πληροφόρηση και στη διερεύνηση των γνώσεών τους. Τα μέλη μιας κοινότητας πρακτικής, αναπτύσσουν δεσμούς κοινών εμπειριών και δημιουργούν κοινωνικά δίκτυα, τα οποία συχνά αναπτύσσονται και εκτός διαδικτύου. Τέλος, τα μέλη μιας κοινότητας φαντασίας, τα ενώνει το κοινό ενδιαφέρον για τα παιχνίδια φαντασίας και την επιστημονική φαντασία. Ειδική περίπτωση αποτελούν οι κοινότητες παικτών διαδικτυακών παιχνιδιών, όπως τα δημοφιλή διαδικτυακά παιχνίδια πόλων πολλών παικτών *(Massively Multiplayer Online Role-Playing Games-MMORPG's)* που αριθμούν πλέον μερικά εκατομμύρια εγγεγραμμένων παικτών παγκοσμίως.

Αναφέρονται επίσης και άλλες κατηγορίες ψηφιακών κοινοτήτων, όπως, για παράδειγμα **α)** ***οι κοινότητες σκοπού*** *(Communities of Purpose),* τα μέλη των οποίων βρίσκονται σε παρόμοιες καταστάσεις ή προσπαθούν να επιτύχουν αντίστοιχους σκοπούς και μοιράζονται εμπειρίες και πληροφορίες, **β)** ***οι κοινότητες ανάπτυξης λογισμικού***, τα μέλη των οποίων συνεργάζονται για την ανάπτυξη λογισμικού ανοιχτού κώδικα, καθώς και **γ)** ***περιστασιακές κοινότητες***, που αποτελούνται από άτομα που αντιμετωπίζουν ιδιαίτερες προσωπικές καταστάσεις, όπως μια ασθένεια, ένα διαζύγιο ή ένα θάνατο. Τέλος, τα ιστολόγια (*blogs*) θεωρούνται η πιο πρόσφατη μορφή ψηφιακών κοινοτήτων, ενώ ως ψηφιακές κοινότητες θα μπορούσαν να χαρακτηριστούν επίσης δραστηριότητες όπως η ανάπτυξη ψηφιακού περιεχομένου από χρήστες, π.χ. *Wikipedia*, και τα εικονικά περιβάλλοντα.

Τέλος, η επικοινωνία των μελών μιας ψηφιακής κοινότητας είναι ηλεκτρονική, οι σημαντικότεροι παράγοντες για την ανάπτυξή της είναι οι κοινοί πόροι, οι κοινές αρχές και οι επαναλαμβανόμενοι τύποι συμπεριφοράς. Άλλες ενδιαφέρουσες πτυχές των ψηφιακών κοινοτήτων που έχουν κατά καιρούς ερευνηθεί περιλαμβάνουν κοινωνικούς, πολιτικούς και οικονομικούς παράγοντες . Αντικείμενο μελέτης σχετικών ερευνών έχουν αποτελέσει επίσης ζητήματα όπως τα κίνητρα που ωθούν κάποιον να γίνει μέλος μιας ψηφιακής κοινότητας, η αλληλεπίδραση μεταξύ των μελών στο πλαίσιο της κοινότητας, η ανάπτυξη σχέσεων εμπιστοσύνης, η χρήση απάτης, η διαχείριση της ψηφιακής ταυτότητας των μελών καθώς και το ζήτημα του ψηφιακού χάσματος. Μόνο πολύ πρόσφατα, τα ζητήματα προστασίας της ιδιωτικότητας και ο τρόπος που τα μέλη των κοινοτήτων αυτών τα αντιλαμβάνονται, προσέλκυσαν το ενδιαφέρον της επιστημονικής κοινότητας και των ερευνητών.

4.2.1.2 Μέλη Ψηφιακών Κοινοτήτων

Από την άποψη της επικοινωνίας μεταξύ των μελών, όλα τα μέλη μιας ψηφιακής κοινότητας έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους σε ισότιμη βάση, καθώς ακολουθείται η αρχιτεκτονική της ***επικοινωνίας μεταξύ ομότιμων*** *(peer-to-peer).* Η αρχιτεκτονική αυτή, που παρέχεται στα μέλη των κοινοτήτων μέσω του διαδικτύου, τους δίνει τη δυνατότητα να εκκινούν την επικοινωνία με οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, καθώς και να δημοσιεύουν και να αναζητούν πληροφορίες. Κάθε ψηφιακή κοινότητα χαρακτηρίζεται από διαφορετικούς τύπους αλληλεπίδρασης και διαφορετικό βαθμό συμμετοχής των μελών τους. Εξάλλου, στο πλαίσιο της ίδιας κοινότητας διαφορετικά μέλη έχουν διαφορετικό βαθμό εμπλοκής σε αυτή, από τον απλό σχολιασμό των αναρτήσεων σε ένα ιστολόγιο έως τη συμμετοχή σε διαδικτυακά παιχνίδια ως αντίπαλοι ή σύμμαχοι άλλων μελών. Όπως συμβαίνει και στις παραδοσιακές κοινότητες, τα μέλη μιας ψηφιακής κοινότητας συχνά χωρίζονται σε υποομάδες ή κλίκες στο πλαίσιο της ίδιας κοινότητας, ή ακόμα αποχωρούν για να δημιουργήσουν νέες κοινότητες.

Για ποιούς λόγους μετέχει κάποιος σε μια ψηφιακή κοινότητα; Η σχετική βιβλιογραφία καταγράφει μια πληθώρα κινήτρων. Κατ' αρχάς οι άνθρωποι εντάσσονται σε μια κοινότητα, ψηφιακή ή όχι, για να αποκτήσουν αυτό που ονομάζεται αίσθημα της κοινωνίας. Επίσης, ένας σημαντικός λόγος για τον οποίο προσφέρουν προσωπικές πληροφορίες στο πλαίσιο μιας κοινότητας είναι ότι αναμένουν, σε αντάλλαγμα, να αντλήσουν και αυτοί με τη σειρά τους χρήσιμες πληροφορίες ή άλλη βοήθεια μέσα από τη συμμετοχή τους στην κοινότητα. Σύμφωνα με έρευνες, τα ενεργά μέλη των ψηφιακών κοινοτήτων λαμβάνουν περισσότερες απαντήσεις και σε συντομότερο χρονικό διάστημα στις ερωτήσεις τους, σε σχέση με μέλη που είναι λιγότερο γνωστά μέσα στην κοινότητα. Η αναγνωρισιμότητα είναι επίσης ένας λόγος για τον οποίο πολλοί άνθρωποι μετέχουν σε ψηφιακές κοινότητες. Έχει βρεθεί, μάλιστα, σε έρευνα σχετικά με την παραβατική συμπεριφορά με χρήση υπολογιστών, ότι συχνά, άτομα που εμπλέκονται σε μη νόμιμες δραστηριότητες, διατηρούν το ίδιο ψευδώνυμο ή αναγνωριστικό, ώστε να διατηρηθεί η συσχέτιση των πράξεών τους με το αναγνωριστικό τους, παρά το γεγονός ότι η πρακτική αυτή μπορεί να οδηγήσει στον εντοπισμό και στην αποκάλυψή τους.

4.2.2 Ιδιωτικότητα στις Ψηφιακές Κοινότητες

Γενικά τα μέλη μιας ψηφιακής κοινότητας αντιλαμβάνονται την έννοια της ιδιωτικότητας ως το βαθμό στον οποίο οι προσωπικές τους πληροφορίες και τα μηνύματα που ανταλλάσσουν μένουν μεταξύ των μελών της κοινότητας στην οποία ανήκουν. Η έννοια της ιδιωτικότητας θεωρείται από πολλούς ασύμβατη με την έννοια της κοινωνίας. Εφόσον ένα από τα ισχυρότερα κίνητρα για τη συμμετοχή σε μια κοινότητα είναι η

ανάγκη των ατόμων να αποτελούν μέρος ενός ευρύτερου συνόλου και να μοιράζονται πληροφορίες, πού βρίσκονται τα όρια της προστασίας της ιδιωτικότητάς τους; Επιθυμούν, και εάν ναι, σε ποιό βαθμό, τα μέλη μιας ψηφιακής κοινότητας να προστατεύσουν την ιδιωτικότητά τους; Για να απαντήσουμε στο ερώτημα αυτό, θα πρέπει, κατ' αρχάς να εξετάσουμε τις σχέσεις μεταξύ των μελών και της κοινότητας. Εάν τα μέλη μιας κοινότητας μετέχουν σε αυτήν προκειμένου να λαμβάνουν κάποιες υπηρεσίες ή να επιτύχουν συγκεκριμένους στόχους, τότε είναι πιθανό να επιθυμούν την προστασία της ιδιωτικότητάς τους. Εάν, όμως, η συμμετοχή στην κοινότητα αποτελεί κομμάτι της κοινωνικής τους ζωής, τότε η στάση τους απέναντι στην ιδιωτικότητα μπορεί να μην είναι η ίδια με την προηγούμενη περίπτωση.

Η παραπάνω διαφοροποίηση ενδεχομένως εξηγεί το γεγονός ότι, ενώ γενικά οι χρήστες του διαδικτύου ανησυχούν για την προστασία της ιδιωτικότητάς τους, ταυτόχρονα η συμμετοχή τους στις ψηφιακές κοινότητες αυξάνει εκθετικά. Σύμφωνα με πρόσφατη έρευνα, άτομα που δεν ανήκαν σε μια συγκεκριμένη ψηφιακή κοινότητα ανησυχούσαν σε μεγαλύτερο βαθμό για την προστασία της ιδιωτικότητάς τους σε σχέση με τα μέλη της κοινότητας, ωστόσο δεν φαίνεται ότι η ανησυχία αυτή αποτέλεσε σημαντικό αποτρεπτικό παράγοντα για τη συμμετοχή τους στην κοινότητα. Επίσης, σύμφωνα με άλλη έρευνα, στο χώρο του ηλεκτρονικού εμπορίου, η ευκολία και το κέρδος που προσφέρουν οι διαδικτυακές υπηρεσίες φαίνεται ότι μπορεί να αντισταθμίσουν τους φόβους σχετικά με την προστασία της ιδιωτικότητας των χρηστών του διαδικτύου.

Θα πρέπει, τέλος, να παρατηρήσουμε ότι, υπάρχει διαφορά μεταξύ του πραγματικού κινδύνου και του τρόπου με τον οποίο τα άτομα αντιλαμβάνονται τον κίνδυνο. Αυτή η διαφορά θα μπορούσε να ερμηνεύσει τον τρόπο με τον οποίο αναλαμβάνουν κινδύνους οι χρήστες του διαδικτύου. Οι άνθρωποι γενικά υπερεκτιμούν ή υποτιμούν έναν κίνδυνο, διότι τείνουν να: **α)** αντιδρούν υπερβολικά απέναντι σε εσκεμμένες πράξεις, **β)** αντιδρούν με πιο έντονο τρόπο σε καταστάσεις που προσβάλλουν τις ηθικές τους αξίες, **γ)** αντιδρούν περισσότερο έντονα απέναντι σε άμεσες απειλές από ότι σε απειλές που είναι μακροπρόθεσμες, και **δ)** υποτιμούν αλλαγές που συμβαίνουν αργά στο πέρασμα του χρόνου.

4.2.2.1 Είδη Ιδιωτικότητας

Η έννοια της ιδιωτικότητας είναι περιεκτική και συχνά χρησιμοποιείται για να περιγράψει διαφορετικές καταστάσεις. Σύμφωνα με μια προσέγγιση, μπορούμε να διακρίνουμε τα ακόλουθα διαφορετικά είδη ιδιωτικότητας:

1. ***Η Χωρική Ιδιωτικότητα (Territorial Privacy)*** ή αλλιώς απομόνωση, είναι η κατάσταση διατήρησης της ιδιωτικότητας στην οποία τα άτομα δεν υπόκεινται σε ανεπιθύμητη παρατήρηση ή παραβίαση του χώρου τους.
2. ***Η Πληροφοριακή Ιδιωτικότητα (Informational Privacy)*** ή αλλιώς ανωνυμία, είναι η δυνατότητα των ατόμων να ελέγχουν τις συνθήκες κάτω από τις οποίες τα προσωπικά τους δεδομένα κοινοποιούνται.
3. Η ***Ψυχολογική Ιδιωτικότητα (Psychological Privacy),*** ορίζεται ως ο έλεγχος της κοινοποίησης ή της παρακράτησης προσωπικών πληροφοριών για την προστασία των πεποιθήσεων και της προσωπικότητας των ατόμων.
4. Τέλος, ***η Ιδιωτικότητα των Σχέσεων (Interactional Privacy)*** ή αλλιώς οικειότητα, αφορά σχέσεις στο πλαίσιο κοινωνικών ομάδων και αναφέρεται στην επικοινωνία μεταξύ των μελών της ομάδας.

4.2.3 Προβληματισμοί των Μελών Ψηφιακών Κοινοτήτων για την Ιδιωτικότητα

4.2.3.1 Στοιχεία για την Έρευνα

Προκειμένου να διερευνήσουμε τη στάση και τις αντιλήψεις μελών ψηφιακών κοινοτήτων στο ζήτημα της ιδιωτικότητας, χρησιμοποιήσαμε ένα ερωτηματολόγιο που αποτελείται από ερωτήσεις κλειστού και ανοικτού τύπου. Με βάση το ερωτηματολόγιο αυτό ελήφθησαν συνεντεύξεις από δεκατέσσερα άτομα, όλα μέλη της δημοφιλούς ψηφιακής κοινότητας *MySpace.com*. Τα μέλη του *MySpace.com* χρησιμοποιούν τα μέσα που τους παρέχει ο δικτυακός τους τόπος για να δημιουργήσουν το δικό τους κοινωνικό δίκτυο που αποτελείται από φίλους, να ανταλλάξουν και να μοιραστούν πληροφορίες, να συμμετάσχουν σε ομάδες κοινού ενδιαφέροντος και να αναρτήσουν υλικό που τους αφορά, όπως φωτογραφίες, *video*, σχόλια κ.λπ. Η συμμετοχή στην κοινότητα του *MySpace.com* γίνεται χωρίς κόστος, και κάθε νέο μέλος μπορεί να δημιουργήσει το προφίλ του που περιλαμβάνει προσωπικές πληροφορίες, να στείλει μηνύματα σε άλλα μέλη και να αναρτήσει εγγραφές στο ιστολόγιο. Στη συνέχεια έχει τη δυνατότητα να προσκαλέσει φίλους να μετάσχουν στο δίκτυό του, ενώ μπορεί επίσης να λάβει μηνύματα από μέλη της κοινότητας *MySpace.com* τα οποία δεν ανήκουν στο κοινωνικό του δίκτυο, ή όπως αλλιώς ονομάζεται, στο δίκτυο των φίλων του.

Τα μέλη της κοινότητας αλληλεπιδρούν στέλνοντας μηνύματα, ενώ μηνύματα ηλεκτρονικού ταχυδρομείου γενικά δεν ανταλλάσσονται, καθώς η διεύθυνση ηλεκτρονικού ταχυδρομείου *(email address)* δεν περιλαμβάνεται στα προσωπικά στοιχεία που είναι διαθέσιμα στα άλλα μέλη της κοινότητας. Στα προσωπικά στοιχεία που μπορούν να δουν τα μέλη της κοινότητας ανήκουν συνήθως η φωτογραφία του μέλους, η ηλικία, η περιγραφή φυσικών χαρακτηριστικών, όπως το ύψος, το βάρος και το χρώμα των ματιών, ο τόπος καταγωγής ή κατοικίας, οι μουσικές προτιμήσεις, αγαπημένοι καλλιτέχνες κ.λπ. Κατά το διάστημα που διεξήχθη η έρευνα, στα τέλη του 2006, το *MySpace.com* αριθμούσε περισσότερα από 50 εκατομμύρια εγγεγραμμένα μέλη, από όλες σχεδόν τις χώρες του κόσμου. Αξίζει να σημειωθεί ότι μέσω της εισαγωγικής σελίδας του ιστότοπου του *MySpace* μπορεί κανείς να έχει πρόσβαση στην πολιτική του *MySpace* σχετικά με την προστασία της ιδιωτικότητας των μελών του.

Η επιλογή των μελών του *MySpace* που συμμετείχαν στη μελέτη περίπτωσης έγινε σε εθελοντική βάση. Χρησιμοποιώντας τη δυνατότητα αποστολής μηνυμάτων που παρέχει το *MySpace*, επικοινωνήσαμε με εκατό μέλη, έπειτα από τυχαία επιλογή. Η αρχική επιλογή έγινε μελετώντας τα προφίλ διαφορετικών χρηστών, ώστε να συμπεριλαμβάνονται άτομα και των δύο φύλων, όλων των ηλικιακών ομάδων και διαφορετικών προελεύσεων. Από τα δεκαέξι άτομα που απάντησαν στο μήνυμά μας, τα δεκατέσσερα συμφώνησαν να μετάσχουν στην έρευνα και τα δύο αρνήθηκαν, εκφράζοντας τη δυσαρέσκειά τους για την ενόχληση. Ο ***πίνακας 5*** περιλαμβάνει τα στοιχεία των μελών που τελικά απάντησαν στις ερωτήσεις της έρευνας. Αξίζει να σημειωθεί ότι ο αριθμός των γυναικών που συμφώνησαν να μετάσχουν στην έρευνα είναι σημαντικά μεγαλύτερος από τον αριθμό των αντρών. Αυτό μπορεί να είναι τυχαίο ή μπορεί να αποδοθεί στη μεγαλύτερη ευαισθητοποίηση των γυναικών σε ζητήματα προστασίας της ιδιωτικότητας, ή ακόμα, θα μπορούσε να αποδοθεί στο γεγονός ότι ο αποστολέας των μηνυμάτων ήταν άντρας.

Πίνακας 5: Στοιχεία ερωτηθέντων

Πλήθος ατόμων	*14 άτομα*
Ηλικία	*Από 16 έως 27 ετών*
Φύλο	*4 άνδρες, 10 γυναίκες*
Χώρες προέλευσης	*Ηνωμένο Βασίλειο, Αυστραλία, Λιθουανία, Ελλάδα, Λίβανος, Περού, ΗΠΑ, Ολλανδία, Ρουμανία, Ουρουγουάη*

Πρέπει να σημειωθεί επίσης ότι για τη διερεύνηση των αντιλήψεων των μελών των ψηφιακών κοινοτήτων σχετικά με την προστασία της ιδιωτικότητάς τους, η έρευνα με χρήση του διαδικτύου είναι μια εύλογη επιλογή. Ο *Stanton* διαπίστωσε ότι δεδομένα που είχαν συλλεχθεί μέσω του διαδικτύου οδήγησαν σε συμπεράσματα ανάλογα με εκείνα στα οποία είχε καταλήξει εξετάζοντας δείγμα ατόμων που συμπλήρωσαν το ίδιο ερωτηματολόγιο με χαρτί και μολύβι. Ωστόσο χαρακτηριστικό των ερευνών μέσω του διαδικτύου είναι το χαμηλό ποσοστό των απαντήσεων που λαμβάνονται, καθώς και ότι συχνά θεωρούνται ανεπιθύμητα μηνύματα (*spam*). Καθώς επίσης, στόχος της έρευνας ήταν να μελετηθούν οι αντιλήψεις μελών ψηφιακών κοινοτήτων, επιλέχθηκε η προσέγγιση της αποστολής ερωτηματολογίου μέσω μηνυμάτων σε επιλεγμένο δείγμα μελών τέτοιων κοινοτήτων. Οι ερωτήσεις στις οποίες κλήθηκαν να απαντήσουν τα μέλη περιλαμβάνονται στον ***πίνακα 6***.

4.2.3.2 Ανάλυση και Συμπεράσματα

Σύμφωνα με τις απαντήσεις τους, όλα τα μέλη που απάντησαν στο ερωτηματολόγιο ήταν ενήμερα ότι ο ιστότοπος *MySpace* διαθέτει πολιτική για την ιδιωτικότητα των στοιχείων των μελών του. Ωστόσο, μόνο τέσσερις ανέφεραν ότι τη διάβασαν πριν γίνουν μέλη του *MySpace* και δημιουργήσουν το προφίλ τους. Ένα από τα μέλη αυτά, σε επόμενη ερώτηση σχετικά με τα μέσα διαφύλαξης της ιδιωτικότητας που θεωρεί κατάλληλα, ανέφερε ότι πρέπει να ***«διαβάζει κανείς την πολιτική για την ιδιωτικότητα πριν γίνει μέλος και να έχει εγκατεστημένο στον υπολογιστή πρόγραμμα προστασίας από ιούς που να είναι πρόσφατα ενημερωμένο».*** Είναι πάντως, αξιοσημείωτο το γεγονός ότι τα περισσότερα από τα μέλη που απάντησαν δεν ενδιαφέρθηκαν να διαβάσουν την πολιτική της ιδιωτικότητας.

Οι περισσότεροι από τους ερωτώμενους (έντεκα στους δεκατέσσερις) απάντησαν ότι δεν αισθάνονται ανασφάλεια σε σχέση με τη χρήση των προσωπικών τους δεδομένων. Στην ερώτηση ωστόσο για το εάν ανησυχούν ιδιαίτερα για κάποιο από τα δημοσιευμένα στοιχεία του προφίλ τους, δύο από αυτούς που απάντησαν ότι δεν αισθάνονται ανασφάλεια ανέφεραν ότι τους απασχολεί το πώς θα μπορούσε κάποιος τρίτος να χρησιμοποιήσει τις προσωπικές τους φωτογραφίες, τα βίντεο και τις εγγραφές του ιστολογίου τους. Τα άτομα που εξέφρασαν ανασφάλεια ανέφεραν ότι ανησυχούν ιδιαίτερα για την προστασία της ιδιωτικότητας της τοποθεσίας στην οποία βρίσκονται και της *IP* διεύθυνσης που χρησιμοποιούν. Είναι επίσης ενδιαφέρον ότι ένα από τα άτομα που απάντησαν ότι νιώθουν ανασφάλεια δεν εξέφρασε καμιά ιδιαίτερη ανησυχία για τα στοιχεία του προφίλ του και μάλιστα ανέφερε ότι δίνει αληθή στοιχεία σχετικά με το πού βρίσκεται.

Ως πηγές της ανασφάλειάς τους σχετικά με την προστασία της ιδιωτικότητάς τους, τρία άτομα ανέφεραν την πιθανή κακόβουλη χρήση από τρίτους, ενώ ένας από τους

ερωτώμενους απάντησε ότι ***«…βασική ανησυχία μου είναι ότι άλλοι θα σχηματίσουν λάθος άποψη για μένα».*** Επίσης, ένα άτομο ανέφερε ότι η ανασφάλειά του πηγάζει από το γεγονός ότι ***«… δεν είμαι ειδικός σε θέματα του internet»*** ενώ σε μια άλλη απάντηση διατυπωνόταν η άποψη ότι ***«… γενικά δεν μπορείς να εμπιστεύεσαι τους ανθρώπους»*.**

Στην ερώτηση για το τι κάνουν όταν έχουν ενδοιασμούς σχετικά με τη χρήση των προσωπικών τους στοιχείων οι περισσότεροι από τους ερωτώμενους απάντησαν ότι θα απέφευγαν να δημοσιοποιήσουν τα στοιχεία αυτά στο διαδίκτυο, ενώ ένα άτομο απάντησε ότι θα έδινε ψεύτικα δεδομένα. Αντίθετα, τρεις άλλοι ερωτώμενοι υποστήριξαν ότι δίνουν πάντα τα αληθινά στοιχεία τους στο διαδίκτυο, ακόμα και όταν αμφιβάλλουν για την προστασία της ιδιωτικότητάς τους. Ακόμα, στην ερώτηση για τους λόγους για τους οποίους θα περιλάμβαναν ψευδή στοιχεία στο προφίλ τους, εκτός από εκείνους που δήλωσαν ότι πάντα δίνουν αληθή στοιχεία, οι υπόλοιποι ανέφεραν ότι προκειμένου να αποφύγουν πιθανή ανεπιθύμητη αλληλογραφία και ενόχληση από τρίτους θα έδιναν ψεύτικα στοιχεία σχετικά με την τοποθεσία που βρίσκονται και την ηλικία τους. Χαρακτηριστικά, το νεαρότερο άτομο που συμμετείχε στην έρευνα απάντησε ότι θα έδινε ψεύτικα στοιχεία έως ότου ***«… γνωρίσει τα άλλα μέλη καλά»*.**

Ορισμένα μέλη του *MySpace* ανέφεραν επίσης περιστατικά παραβίασης της ιδιωτικότητάς τους. Ένα μέλος, ειδικότερα περιέγραψε ότι είχε πέσει θύμα κλοπής ταυτότητας, καθώς ανακάλυψε προσωπικές του φωτογραφίες να χρησιμοποιούνται στο προφίλ άλλων ατόμων. Σχετικά με το περιστατικό αυτό, το ίδιο πρόσωπο σχολίασε ότι ***«… αναλαμβάνουμε τον κίνδυνο αυτό και πιστεύω ότι οι περισσότεροι άνθρωποι γνωρίζουν ότι πάντα θα υπάρχουν κακοπροαίρετοι».*** Ωστόσο, κανένας από τους ερωτώμενους δεν αξιολόγησε ως πάρα πολύ υψηλό το αίσθημα ανασφάλειάς του σχετικά με την προστασία της ιδιωτικότητας των στοιχείων του. Οι περισσότεροι ερωτώμενοι απάντησαν ότι δεν αισθάνονται ανασφάλεια ή βαθμολόγησαν το αίσθημα ανασφάλειάς τους ως μέτριο, ενώ τρεις το χαρακτήρισαν χαμηλό. Ενδιαφέρον παρουσιάζει το γεγονός ότι το άτομο που ανέφερε ότι είχε πέσει θύμα κλοπής ηλεκτρονικής ταυτότητας, ανακαλύπτοντας προσωπικές φωτογραφίες στο προφίλ άλλων ατόμων σε δύο περιπτώσεις, σημείωσε ότι ανησυχεί σε χαμηλό βαθμό για την ιδιωτικότητα των δεδομένων του, ενώ το άτομο που ανέφερε ότι είχε δεχτεί παρενόχληση απάντησε ότι ανησυχεί σε μέτριο βαθμό.

Απαντώντας στην ερώτηση ***«πώς νομίζετε ότι κάποιος τρίτος θα μπορούσε να εκμεταλλευτεί τις προσωπικές πληροφορίες που είναι διαθέσιμες για εσάς;»,*** τα μέλη του *MySpace* ανέφεραν την παρενόχληση, τη λήψη ανεπιθύμητης ηλεκτρονικής αλληλογραφίας και μηνυμάτων, απειλών, την κλοπή της ψηφιακής τους ταυτότητας και τη χρήση των προσωπικών τους δεδομένων από άλλους. Ένας ερωτώμενος σχολίασε ότι προσέχει ποιά προσωπικά δεδομένα του δημοσιοποιεί στο διαδίκτυο, ώστε να μην μπορεί να τα εκμεταλλευτεί κάποιος τρίτος, ενώ άλλο μέλος του *MySpace* ανέφερε ότι φοβάται το ενδεχόμενο να πέσει θύμα απαγωγής. Αρκετοί από τους ερωτηθέντες δεν απάντησαν στην ερώτηση αυτή, ενώ ενδιαφέρον είναι το γεγονός ότι πολλοί κατονόμασαν πιθανές απειλές κατά της ιδιωτικότητας, αν και οι ίδιοι είχαν απαντήσει ότι δεν ανησυχούν ιδιαίτερα για το ζήτημα αυτό.

Όλα τα μέλη του *MySpace* που μετείχαν στην έρευνα απάντησαν ότι σε περίπτωση κατάχρησης των προσωπικών τους στοιχείων, η πρώτη τους πράξη θα ήταν να αναφέρουν τους κακόβουλους χρήστες στη σχετική υπηρεσία του ιστότοπου που τους φιλοξενεί. Ένα από τα μέλη πρόσθεσε επίσης ότι θα διερευνούσε τη δυνατότητα ανάληψης νομικών μέσων, ενώ δύο άλλα δήλωσαν ότι θα διέγραφαν τα προφίλ τους. Μόνο ένα μέλος εξέφρασε την πρόθεση να αφήσει την κοινότητα στην οποία ανήκει,

στην περίπτωση ενός τέτοιου περιστατικού. Ενδιαφέρον παρουσιάζει το γεγονός ότι κανένα από τα δύο μέλη που είχαν, σε προηγούμενη ερώτηση αναφέρει ότι έχουν υποστεί παραβίαση της ιδιωτικότητάς τους (παρενόχληση και χρήση προσωπικών φωτογραφιών από τρίτους) δεν δήλωσε πρόθεση να αποχωρήσει από την κοινότητα, έπειτα από τα περιστατικά αυτά. Αντίθετα, και οι δύο σημείωσαν ότι σε παρόμοια περίπτωση, στο μέλλον, θα ανέφεραν τους κακόβουλους χρήστες στους διαχειριστές του ιστότοπου. Συμπεραίνουμε επομένως ότι, για τους χρήστες αυτούς, η συμμετοχή στην κοινότητα έχει μεγαλύτερη βαρύτητα από την αντίληψη του κινδύνου για την παραβίαση της ιδιωτικότητάς τους.

Στην ερώτηση σχετικά με τα μέσα που θα χρησιμοποιούσαν για την προστασία της ιδιωτικότητάς τους, οχτώ μέλη απάντησαν ότι ο κύριος τρόπος με τον οποίο προστατεύονται είναι η επιλογή των ατόμων (φίλων) που απαρτίζουν το προσωπικό τους δίκτυο, ενώ τρία από τα μέλη αυτά πρόσθεσαν ότι επιλέγουν προσεκτικά τις προσωπικές πληροφορίες που δημοσιοποιούν στο διαδίκτυο. Τρία άλλα μέλη απάντησαν ότι προστατεύουν την ιδιωτικότητά τους επιλέγοντας να είναι ορατά τα προσωπικά τους στοιχεία μόνο στα άτομα που μετέχουν στο προσωπικό τους δίκτυο φίλων. Αξίζει να σημειωθεί ότι αυτή η δυνατότητα παρέχεται από το *MySpace* σε όλα τα μέλη του, κάτι που δε συμβαίνει με όλα τα περιβάλλοντα κοινωνικής δικτύωσης *(Social Networking)*. Δύο άλλοι ερωτηθέντες ισχυρίστηκαν ότι η λήψη μέτρων προστασίας της ιδιωτικότητας είναι μάταιη. Ένας εξ' αυτών μάλιστα, που συμβαίνει να είναι και ο μεγαλύτερος σε ηλικία από όσους απάντησαν στις ερωτήσεις της έρευνας, δήλωσε ότι στο διαδίκτυο δεν υφίσταται αποτελεσματικός τρόπος προστασίας της ιδιωτικότητας, ενώ ο δεύτερος σχολίασε ότι ***«… εάν κάποιος αναζητά προσωπικές πληροφορίες για σένα θα βρει τρόπο να τις ανακαλύψει».***

Πίνακας 6: Ερωτήσεις συνεντεύξεων στα μέλη του *MySpace*

1. Διαβάσατε την πολιτική ιδιωτικότητας του ιστότοπου πριν δημιουργήσετε το προφίλ σας;
2. Αισθάνεστε φόβο ή ανασφάλεια σχετικά με τη χρήση των προσωπικών σας πληροφοριών;
3. Αισθάνεστε ανασφάλεια για κάποια από τα στοιχεία του προφίλ σας; I. Όχι II. Ναι, για τα βίντεο και της φωτογραφίες μου III. Ναι, για την ηλικία μου IV. Ναι, για την τοποθεσία μου V. Ναι, για …. (περιγράψτε)
4. Εάν απαντήσατε ότι αισθάνεστε ανασφάλεια στην προηγούμενη ερώτηση, ποιοί είναι οι σημαντικότεροι λόγοι γι' αυτό;
5. Όταν έχετε ενδοιασμούς για το εάν πρέπει να αναρτήσετε στο διαδίκτυο προσωπικά σας στοιχεία… I. Δίνετε τα στοιχεία σας II. Δίνετε ψεύτικα στοιχεία

III. Δεν δίνετε καθόλου στοιχεία IV. Κάνετε κάτι άλλο (περιγράψτε)
6. Για ποιους λόγους θα αναγράφατε ψεύτικα στοιχεία στο προφίλ σας;
7. Σε τι βαθμό σας ανησυχεί πιθανή κατάχρηση των προσωπικών στοιχείων του προφίλ σας; I. Σε υψηλό βαθμό II. Σε μέτριο βαθμό III. Σε χαμηλό βαθμό IV. Δεν με ανησυχεί
8. Με ποιό τρόπο πιστεύετε ότι θα μπορούσε κάποιος να χρησιμοποιήσει τα προσωπικά σας στοιχεία που βρίσκονται στο διαδίκτυο;
9. Εάν ανακαλύπτατε ότι ένα άλλο μέλος έχει χρησιμοποιήσει τα προσωπικά σας στοιχεία, τι θα κάνατε; I. Θα ανέφερα το χρήστη στο διαχειριστή του ιστότοπου II. Θα διέγραφα το προφίλ μου και θα αποσυρόμουν από την κοινότητα/ομάδα III. Θα διέγραφα το προφίλ μου και θα δημιουργούσα νέο IV. Άλλο (εξηγείστε)
10. Με ποιό τρόπο πιστεύετε ότι μπορείτε να διαφυλάξετε την ιδιωτικότητα των προσωπικών σας στοιχείων στο διαδίκτυο; I. Επιλέγοντας το δίκτυο των φίλων/κοινωνικό δίκτυο II. Περιορίζοντας το πλήθος των φίλων/μελών του δικτύου III. Με άλλο τρόπο (περιγράψτε)

Συμπερασματικά, από την ανάλυση των απαντήσεων που έδωσαν τα μέλη του *MySpace* στην έρευνα αυτή, προκύπτουν τα ακόλουθα:

4.2.3.2.1 Αντιλήψεις των μελών ψηφιακών κοινοτήτων σχετικά με την ιδιωτικότητα

Παρά το γεγονός ότι οι περισσότεροι ερωτηθέντες απάντησαν αρνητικά στην ερώτηση για το εάν νιώθουν ανασφάλεια σχετικά με τη διαφύλαξη της ιδιωτικότητάς τους, εντούτοις περιέγραψαν υποθετικά σενάρια παραβίασης και κατάχρησης των προσωπικών τους δεδομένων. Σε συνδυασμό με το γεγονός ότι κανείς από τους ερωτηθέντες δεν εξέφρασε πρόθεση να αποχωρήσει από την ψηφιακή κοινότητα στην οποία ανήκει, σε περίπτωση που το υποθετικό σενάριο γίνει πραγματικότητα, μπορούμε να συμπεράνουμε ότι τα μέλη αυτά ανησυχούν σχετικά με την προστασία της ιδιωτικότητάς τους, ωστόσο οι ανησυχίες αυτές είναι σε χαμηλό επίπεδο. Η διαπίστωση αυτή ενισχύει την ανάγκη για περαιτέρω διερεύνηση των παραγόντων οι οποίοι αντισταθμίζουν τους φόβους για την παραβίαση της ιδιωτικότητας, ιδιαίτερα μάλιστα στις περιπτώσεις που τα άτομα έχουν ήδη υποστεί ένα τέτοιο περιστατικό. Θα πρέπει ωστόσο, να παρατηρήσουμε ότι έως κάποιο βαθμό, ο προβληματισμός για την

προστασία της ιδιωτικότητάς τους επηρεάζει τη συμπεριφορά των μελών των ψηφιακών κοινοτήτων, αφού όπως απάντησαν πολλοί από τους ερωτηθέντες, μπορεί να οδηγήσει σε απόκρυψη κάποιων προσωπικών στοιχείων ή ακόμα και στη δημοσιοποίηση ψευδών. Τέλος, τα μέλη των ψηφιακών κοινοτήτων που ερωτήθηκαν δήλωσαν ότι ανησυχούν περισσότερο για την προστασία της ιδιωτικότητάς τους σε σχέση με τις αναρτήσεις στο ιστολόγιό τους, τα προσωπικά τους βίντεο και τις φωτογραφίες, την τοποθεσία που βρίσκονται και την ηλικία τους.

4.2.3.2.2 Σημασία των σχέσεων εμπιστοσύνης

Γενικά, η ανάλυση των απαντήσεων των μελών του *MySpace* που μετείχαν στην έρευνα υποδεικνύει ότι οι ερωτώμενοι δεν θεωρούν σημαντική πηγή κινδύνου κατά της ιδιωτικότητάς τους τα υπόλοιπα μέλη της ευρύτερης κοινότητας στην οποία ανήκουν. Θεωρούν επομένως, ότι η ιδιωτικότητά τους εξασφαλίζεται μέσα από τις σχέσεις εμπιστοσύνης που αναπτύσσονται μεταξύ των μελών της κοινότητας. Όπως χαρακτηριστικά ανέφερε ένα από τα μέλη που ρωτήθηκαν ***«…πρώτα γνωρίζεις καλά τα άτομα με τα οποία μιλάς και στη συνέχεια αποκαλύπτεις προσωπικές σου πληροφορίες».*** Εξάλλου, ως βασικό μέσο προστασίας της ιδιωτικότητας τα περισσότερα μέλη ανέφεραν την επιλογή των ατόμων που απαρτίζουν το προσωπικό τους δίκτυο. Ωστόσο, δεν είναι προφανές πώς αυτό υλοποιείται στην πράξη, καθώς η ανάπτυξη διαπροσωπικών σχέσεων, και μέσα από το διαδίκτυο, απαιτεί μακρό χρονικό διάστημα και εξαρτάται από την κουλτούρα της κοινότητας στο πλαίσιο της οποίας οι σχέσεις αυτές υφίστανται. Πάντως, σε όλες σχεδόν τις απαντήσεις διαφαίνεται ο διαχωρισμός των τρίτων σε άτομα που ανήκουν στο ίδιο κοινωνικό δίκτυο (εσωτερικοί, *insiders*) και σε ξένους (*outsiders*).

4.2.3.2.3 Χρήση παραπλανητικών στοιχείων

Γενικά, με την έννοια της παραπλάνησης υπονοείται είτε η εμπρόθετη παραπληροφόρηση είτε η απόκρυψη πληροφοριών. Τα μέλη των ψηφιακών κοινοτήτων αναφέρουν ότι ακολουθούν και τις δύο αυτές πρακτικές, προκειμένου να προστατευτούν από απειλές που προέρχονται από το διαδίκτυο, όπως η παρενόχληση. Στο πλαίσιο αυτό, τα μέλη χρησιμοποιούν δικαιολογημένα ψεύδη για την προστασία της ιδιωτικότητας.

4.2.3.2.4 Ενδιαφέρον για διαφορετικούς τύπους ιδιωτικότητας

Σύμφωνα με τις απαντήσεις που λάβαμε, τα μέλη των ψηφιακών κοινοτήτων ενδιαφέρονται κυρίως για την ιδιωτικότητα του χώρου τους. Χαρακτηριστικά, κάποια μέλη δήλωσαν ότι θα έδιναν ψεύτικα στοιχεία για το πού βρίσκονται. Αντίθετα, η ιδιωτικότητα των πληροφοριών δεν φαίνεται να απασχολεί σε υψηλό βαθμό τα μέλη του *MySpace*, καθώς όπως απάντησαν, επιλέγουν το δίκτυο των φίλων τους και ελέγχουν τις προσωπικές πληροφορίες που δημοσιοποιούν στο διαδίκτυο. Η ψυχολογική ιδιωτικότητα από την άλλη πλευρά, ανήκει στα ζητήματα ιδιωτικότητας που τους απασχολούν, καθώς σύμφωνα με κάποιες απαντήσεις, προβληματίζονται για την εικόνα που σχηματίζουν οι τρίτοι μέσα από τις πληροφορίες που τους αφορούν. Τέλος, η ιδιωτικότητα των σχέσεων απασχολεί επίσης τα μέλη των ψηφιακών κοινοτήτων και για το λόγο αυτό φαίνεται ότι χρησιμοποιούν τα μέσα που τους παρέχονται από τον ιστότοπο που φιλοξενεί το κοινωνικό τους δίκτυο, στην περίπτωση της έρευνας το *MySpace*, προκειμένου να περιορίσουν την πρόσβαση στα προσωπικά τους δεδομένα μόνο στα άτομα που ανήκουν στο δικό τους δίκτυο.

4.2.4 Επίλογος και Περαιτέρω Έρευνα

Η διερεύνηση του τρόπου με τον οποίο αντιλαμβάνονται την ιδιωτικότητά τους τα μέλη των ψηφιακών κοινοτήτων είναι σημαντικό ζήτημα, καθώς οι κοινότητες αυτές αποτελούν πλέον όχι μόνο κοινωνικό φαινόμενο, αλλά και αναδυόμενο επιχειρηματικό μοντέλο. Αν και γενικά τα ζητήματα ιδιωτικότητας απασχολούν τους χρήστες του διαδικτύου, η έρευνα για το ποιά ακριβώς είναι τα ζητήματα αυτά, είναι πολύ περιορισμένη. Ένα γενικό συμπέρασμα στο οποίο καταλήγει η έρευνα είναι ότι η ιδιωτικότητα γίνεται αντιληπτή με διαφορετικό τρόπο από τους χρήστες του διαδικτύου. Διαφορετικές ομάδες χρηστών, όπως τα μέλη των ψηφιακών κοινοτήτων αντιλαμβάνονται με διαφορετικό τρόπο τι συνιστά απειλή κατά της ιδιωτικότητάς τους και χρησιμοποιούν διαφορετικά μέσα προστασίας. Κατά συνέπεια, απαιτούνται διαφορετικές προσεγγίσεις στην προστασία της ιδιωτικότητας, τόσο σε τεχνικό όσο και σε οργανωτικό επίπεδο. Στα βασικά ζητήματα που ανέδειξε η έρευνα που παρουσιάστηκε περιλαμβάνονται τα ακόλουθα:

1. Τα μέλη των ψηφιακών κοινοτήτων ανησυχούν για την προστασία της ιδιωτικότητάς τους σε διαφορετικό βαθμό και για διαφορετικούς λόγους. Κάποιοι αναφέρουν ότι δεν έχουν φόβους, ενώ η πλειονότητα των μελών εκφράζει μέτριο επίπεδο ανησυχίας, αναφέροντας τις διαφορετικές πηγές για την ανησυχία αυτή, κυρίως την τοποθεσία στην οποία βρίσκονται, την ηλικία τους, τις προσωπικές φωτογραφίες και τα βίντεο και τις εγγραφές στο ιστολόγιο.
2. Χρειάζεται να διακρίνουμε τα διαφορετικά είδη ιδιωτικότητας, όπως τα αντιλαμβάνονται τα μέλη των ψηφιακών κοινοτήτων. Η προστασία της ιδιωτικότητας του χώρου και των σχέσεων φαίνεται να απασχολεί περισσότερο τα μέλη των ψηφιακών κοινοτήτων σε σχέση με την προστασία της ψυχολογικής ιδιωτικότητας και της ιδιωτικότητας των πληροφοριών.
3. Τα μέλη των ψηφιακών κοινοτήτων δεν υφίστανται μόνο απειλή από ενδεχόμενη παραπλάνηση, αλλά τη χρησιμοποιούν και τα ίδια ως μέσο προστασίας της ιδιωτικότητάς τους.

Τα παραπάνω ζητήματα χρειάζονται περαιτέρω διερεύνηση. Τα συμπεράσματα της έρευνας που παρουσιάστηκε, ενισχύουν τα συμπεράσματα άλλων ερευνών ότι τα μέλη των ψηφιακών κοινοτήτων ανησυχούν για την προστασία της ιδιωτικότητάς τους, ωστόσο η ανησυχία αυτή δεν είναι αρκετή ώστε να αποτρέψει τη συμμετοχή τους. Επιπλέον, στο πλαίσιο της έρευνας που παρουσιάστηκε έγινε διαχωρισμός των διαφορετικών τύπων της ιδιωτικότητας που επιθυμούν να προστατεύσουν τα μέλη των ψηφιακών κοινοτήτων. **[16]**

4.3 Η Χρήση του *Internet* ως Εργαλείο Έρευνας

Μια σημαντική παράμετρος στον έλεγχο των ιχνών σε μια έρευνα αποτελεί ο έλεγχος για τις σχετικές πληροφορίες στο διαδίκτυο, όπως είναι οι ιστοσελίδες που επισκέφθηκε κάποιος ή τα μηνύματα τα οποία δεν στάλθηκαν, η διεύθυνση του ηλεκτρονικού ταχυδρομείου του εισβολέα ή ο αριθμός τηλεφώνου του και τέλος τα προσωπικά δεδομένα που υπάρχουν σε βάσεις δεδομένων. Επειδή το διαδίκτυο περιέχει μεγάλο όγκο πληροφοριών οι οποίες είναι πολύ χαλαρά συνδεδεμένες, είναι πολύ δύσκολο να ερευνήσει κάποιος για συγκεκριμένα στοιχεία. Γι' αυτό και είναι ιδιαίτερα κρίσιμο, να μάθουν οι ερευνητές να αναζητούν στο διαδίκτυο αποτελεσματικά. Επίσης για να εξοικειωθούν οι ερευνητές με εργαλεία έρευνας θα πρέπει να αναπτύξουν στρατηγικές έρευνας.

Δεδομένης της δημοτικότητας των κοινωνικών δικτύων, όπως είναι το *Facebook* και του πλούτου των προσωπικών πληροφοριών που περιέχει, οι ψηφιακοί ερευνητές συχνά βρίσκουν χρήσιμη πληροφορία σε αυτές τις ιστοσελίδες. Κάποιες πληροφορίες στις κοινωνικές ιστοσελίδες είναι δυνατόν να αναζητηθούν και να προσπελαστούν από οποιονδήποτε στο διαδίκτυο, αλλά υπάρχει και σημαντική πληροφορία σε αυτές τις ιστοσελίδες με περιορισμένη πρόσβαση που περιλαμβάνει μόνο φίλους και οικογένεια. Σε κάποιες περιπτώσεις οι ψηφιακοί ερευνητές είναι δυνατόν να αποκτήσουν πληροφορία, περιλαμβανομένων των *backups* παλαιότερων ιστοσελίδων και επικοινωνιών, από τον πάροχο της κοινωνικής ιστοσελίδας.

Μια άλλη μέθοδος αναζήτησης ψηφιακών αποδείξεων στο διαδίκτυο είναι ο έλεγχος για πόρους που είναι σε σύνδεση μέσα σε μια συγκεκριμένη γεωγραφική περιοχή. Για παράδειγμα, αν το θύμα μιας επίθεσης ζει στο *San Francisco*, είναι πολύ πιθανό να υπάρχει μεγαλύτερη συγκέντρωση σχετικής πληροφορίας σε αυτή την περιοχή. Ο έλεγχος των *online* τηλεφωνικών καταλόγων, των αρχείων των εφημερίδων, των *chat rooms* και άλλων πόρων που βρίσκονται στη συγκεκριμένη περιοχή μπορεί να αποκαλύψουν άγνωστες πτυχές των *online* δραστηριοτήτων του θύματος και να οδηγήσουν στην ταυτότητα του εγκληματία. Οι μηχανές αναζήτησης *(search engines*) που εστιάζουν σε μια συγκεκριμένη χώρα (για παράδειγμα *www.google.it, ie.altavista.com)* είναι επίσης χρήσιμες για γεωγραφικά εστιασμένη έρευνα.

Μια άλλη στρατηγική είναι η έρευνα σε ένα συγκεκριμένο οργανισμό. Για παράδειγμα, αν το θύμα είναι συνδεδεμένο με μια συγκεκριμένη εταιρεία ή σχολείο, είναι πιθανό να υπάρχει μεγαλύτερη συγκέντρωση προσωπικών πληροφοριών σε σχετικούς *online* πόρους. Όπως και με την έρευνα που είναι εστιασμένη γεωγραφικά, η εξέταση ενός *online* αρχείου τηλεφώνων του οργανισμού, του εσωτερικού του ταχυδρομείου, των λιστών του ηλεκτρονικού ταχυδρομείου και άλλων προσβάσιμων *online* πόρων μπορεί να οδηγήσει σε χρήσιμες πληροφορίες. Επιπλέον, είναι δυνατόν να εξεταστούν τα συστήματα στο δίκτυο του οργανισμού για να βρεθεί πληροφορία σχετική με τους χρήστες. Αν και είναι επιτρεπτή η πρόσβαση στην πληροφορία των συστημάτων υπολογιστών ενός οργανισμού με μη επεμβατικούς τρόπους, θα πρέπει να υπάρχει προσοχή από τους ερευνητές ώστε να μην επιχειρήσουν κάποια μη εξουσιοδοτημένη πρόσβαση.

Εκτός από την αναζήτηση ονομάτων, ψευδωνύμων, ολόκληρων διευθύνσεων ηλεκτρονικού ταχυδρομείου ή τμημάτων διευθύνσεων ηλεκτρονικού ταχυδρομείου, μπορεί να είναι παραγωγικό να εστιάσει ο ερευνητής σε έρευνες σχετικές με ασυνήθιστα ενδιαφέροντα, ελέγχοντας περιοχές στο διαδίκτυο στις οποίες σύχναζε το θύμα ή ο ύποπτος. Δεδομένης της δυσκολίας να γίνουν επίσημες εικασίες σχετικά με τις ιστοσελίδες που επισκέφθηκε το θύμα ή ο ύποπτος στο διαδίκτυο, αυτού του είδους η

έρευνα αναπτύσσεται από την αρχή. Για παράδειγμα, συνεντεύξεις με την οικογένεια και φίλους ή μια εξέταση του υπολογιστή του θύματος μπορεί να αποκαλύψουν ότι εγγράφηκε σε κάποια ψηφιακή κοινότητα και σύχναζε σε κάποιο συγκεκριμένο *chat room*. Ο εισβολέας ή το θύμα μπορεί να έχουν αφήσει ίχνη σχετικά με τις δραστηριότητές τους σε αυτές τις περιοχές. Η έρευνα στις περιοχές αυτές μπορεί να είναι ιδιαίτερα αποδοτική αν ο εισβολέας και το θύμα επικοινώνησαν σε μια δημόσια περιοχή του διαδικτύου, αποκαλύπτοντας τις συνδέσεις μεταξύ τους.

Επιπρόσθετα με τα ίχνη των δραστηριοτήτων στο διαδίκτυο, *online* μάρτυρες που χρησιμοποίησαν τις ίδιες περιοχές μπορεί να έχουν κρατήσει αρχεία καταγραφής *(log files)* από τις δραστηριότητες αυτές στους υπολογιστές τους.

Οι στρατηγικές έρευνας δεν αποκλείουν η μια την άλλη και μπορούν να συνδυαστούν αποτελεσματικά έτσι ώστε να εντοπίσουν όσο το δυνατόν περισσότερη πληροφορία στο διαδίκτυο σχετικά με το αντικείμενο έρευνας. Ανεξάρτητα από τον συνδυασμό των στρατηγικών έρευνας, οι ερευνητές θα πρέπει να καταγράψουν τα στοιχεία με έμφαση στο πότε, πώς και πού βρέθηκαν αυτά. Οι σημειώσεις του ερευνητή οι οποίες θα συνδυαστούν με την ιστορία του *web* φυλλομετρητή (*browser*) είναι γενικά αρκετή για να καταδείξει πότε, πού και πώς βρέθηκε η πληροφορία. Επίσης, επειδή η πληροφορία που βρίσκεται στο διαδίκτυο μπορεί κάθε στιγμή να αλλάξει ή και να σβηστεί, θα πρέπει να αποθηκεύονται εικόνες (*screenshots*) από τις ιστοσελίδες στις οποίες οι ερευνητές βρήκαν τις πληροφορίες που έψαχναν. Μερικά εργαλεία που αιχμαλωτίζουν αποτελεσματικά τη μορφή των ιστοσελίδων *web* είναι τα παρακάτω:

- *Web Whacker: www.webwhacker.com,*
- *Adobe Acrobat: www.adobe.com,*
- *Teleport: www.tenmax.com/teleport/pro/home.htm,*
- *Httrack: www.httrack.com*,
- *Web Copier: www.maximumsoft.com,*
- *Snagit: www.techsmith.com,*
- *Anawave's Websnake: http://www.websnake.com,*
- *Htdig: http://www.htdig.org,*
- *Surfsaver: http://www.surfsaver.com,*
- *Wget: http://www.gnu.org/software/wget/wget.html,*
- *Black Window: http://www.softbytelabs.com/us/bw*.

Κάποια από αυτά τα εργαλεία δεν αντιγράφουν τις υποσελίδες *(subpages)* ενός ιστοχώρου, αν οι συνδέσεις (*links*) σε αυτές τις υποσελίδες είναι κωδικοποιημένες σε μια γλώσσα που τα εργαλεία δεν μπορούν να καταλάβουν. Επομένως, προτείνεται να ελέγχεται πρώτα ένα εργαλείο για να επιβεβαιωθεί ότι είναι επαρκές για το σκοπό που χρειάζεται και επίσης να ελέγχονται τα αρχεία που παράγει το εργαλείο για να επιβεβαιώνεται ότι είναι σε ικανοποιητική μορφή. Όλα τα αρχεία που παράγονται κατά τη διάρκεια της διαδικασίας αναζήτησης θα πρέπει να καταγράφονται μαζί με τα ονόματα αρχείων, τις *MD5* τιμές και τις σφραγίδες ημερομηνίας και χρόνου.

4.3.1.1 Μηχανές Αναζήτησης

Οι μηχανές αναζήτησης είναι ανάμεσα στα πιο σημαντικά εργαλεία για την εύρεση πληροφορίας μέσα στο διαδίκτυο. Αν και οι μηχανές αναζήτησης δεν είναι ιδιαίτερα

δύσκολες στη χρήση, είναι απαραίτητες κάποιες επιδεξιότητες για να χρησιμοποιηθούν αποτελεσματικά. Κάθε μηχανή αναζήτησης έχει διαφορετικά περιεχόμενα, διαφορετικές μεθόδους αρχειοθέτησης, διαφορετικά εργαλεία αναζήτησης και διαφορετικούς περιορισμούς στη χρήση. Επομένως, είναι σημαντικό να καταλάβουμε τον τρόπο με τον οποίο δουλεύει κάθε μηχανή αναζήτησης και ποιές από αυτές είναι κατάλληλες κάθε φορά για το συγκεκριμένο σκοπό.

Πολλές μηχανές αναζήτησης όπως η *Altavista*, ενημερώνουν τον εαυτό τους κατά τη διάρκεια της αναζήτησης εκτελώντας προγράμματα που ψάχνουν ακατάπαυστα στο *web* για νέα δεδομένα. Σαν αποτέλεσμα, μπορούν να βρουν τα πιο πρόσφατα στοιχεία αλλά να χάσουν τα παλαιότερα «απαρχαιωμένα» δεδομένα. Το *Google* αντισταθμίζει αυτό το κενό διατηρώντας ένα αντίγραφο από σελίδες *web* που βρήκε (αυτή η πληροφορία είναι χρήσιμη όταν η αρχική έχει πια χαθεί). Επίσης το *Google* μπορεί να αναζητά αρχεία *Word* και *PDF* που άλλες μηχανές αναζήτησης παραβλέπουν. Επίσης το *Google* διατηρεί ένα αρχείο μη σταλμένων μηνυμάτων που χρονολογούνται από το 1981 και στο οποίο μπορεί να εκτελέσει αναζητήσεις. Ένα άλλο μοναδικό εργαλείο του *Google* είναι ο αλγόριθμος αναζήτησης που έχει (*PageRank*), ο οποίος μπορεί να εκτιμήσει τη σχετικότητα και την ποιότητα των δεδομένων, βασισμένος σε έναν αριθμό από συνδέσεις (*links*) στα δεδομένα αυτά από τις πηγές του *web*. Είναι σημαντικό να είμαστε ενήμεροι για τον τρόπο που μια μηχανή αναζήτησης προσπαθεί να «βοηθήσει» (*help*) στην αναζήτηση, έτσι ώστε αυτή η βοήθεια να μπορεί να χρησιμοποιηθεί όταν είναι χρήσιμο και να αποφεύγεται όταν δεν είναι χρήσιμο.

Οι ερευνητές μπορούν να χρησιμοποιήσουν τη γλώσσα των μηχανών αναζήτησης για να δημιουργήσουν περισσότερο εστιασμένες αναζητήσεις. Για παράδειγμα, κάποιες μηχανές αναζήτησης καταλαβαίνουν λέξεις όπως *AND, OR, NOT* και *NEAR*. Κάποιες μηχανές αναζήτησης επίσης επιτρέπουν σύμβολα όπως '-' για να αποκλείουν ορισμούς από την αναζήτηση και αντίστοιχα '+' για να περικλείουν ορισμούς. Για παράδειγμα στην *Altavista*, μπορούν να χρησιμοποιηθούν οι παρακάτω εντολές για να βρεθούν αρχεία που περιέχουν τις λέξεις '*unsolved'* (άλυτος) και '*homicide'* (ανθρωποκτονία) αλλά όχι τις λέξεις '*mystery'* (μυστήριο) και *'mysteries'* (μυστήρια):

+homicide+unsolved-mystery-mysteries

Homicide AND unsolved AND NOT myster*

Κάποιοι εισβολείς προστατεύουν τους εαυτούς τους χρησιμοποιώντας «έξυπνα» ψευδώνυμα, όπως για παράδειγμα το *En0ch|an* αντί για το *Enochian*. Η χρήση του «0» αντί για το «ο» και του « |» αντί για το «i», μπερδεύουν τους αλγόριθμους αναζήτησης. Σε τέτοιου είδους περιπτώσεις, απαιτείται έξυπνη χρήση σύνταξης του τρόπου αναζήτησης (για παράδειγμα με χρήση *AND, OR, NOT, NEAR*). Οι μηχανές αναζήτησης μπορεί να είναι επίσης χρήσιμες για την αναζήτηση συνδέσεων στο *web*. Για παράδειγμα, σελίδες που περιέχουν συνδέσεις σε ιστοσελίδες ενός ύποπτου μπορεί να βρεθούν ψάχνοντας στο *Altavista* και στο *Google* χρησιμοποιώντας τη σύνταξη *link:www.suspectswebpage.com*.

Θα πρέπει να έχουμε υπόψη μας ότι ψάχνοντας για φανερά παράνομους ορισμούς, σπάνια θα βρούμε κάτι πραγματικά παράνομο. Πολλές ιστοσελίδες χρησιμοποιούν παράνομους ορισμούς για να προσελκύσουν το ενδιαφέρον, αλλά οι πραγματικοί εγκληματίες κάνουν προσπάθεια για να κρύψουν τις δραστηριότητές τους χρησιμοποιώντας ευφημισμούς. Για παράδειγμα, κάποιοι εγκληματίες χρησιμοποιούν τους όρους *lolita* ή *nature shots* (λήψεις στη φύση) για να αναφερθούν σε φωτογραφίες παιδιών, ή τον όρο *family fun* (διασκέδαση στην οικογένεια) για να

αναφερθούν σε αιμομιξία. Τέτοιου είδους ευφημισμοί μπορεί να εμφανιστούν στις αρχικές αναζητήσεις, οπότε και θα πρέπει να επεκταθεί η αναζήτηση χρησιμοποιώντας αυτή τη γνώση και εμβαθύνοντας στην αναζήτηση. Επίσης, χρήστες οι οποίοι θέλουν να αποκλείσουν τις ιστοσελίδες τους από τις μηχανές αναζήτησης μπορούν να τοποθετήσουν αρχεία τύπου *robots.txt* στους ιστοχώρους τους.

Οι μηχανές μετα-αναζήτησης (*metasearch*) όπως το *Copernic* και το *Metacrawler*, επιτρέπουν στους χρήστες να αναζητούν πολλαπλές μηχανές αναζήτησης ταυτόχρονα από ένα συγκεκριμένο ιστοχώρο. Επειδή χρησιμοποιούν τις μηχανές αναζήτησης, οι μηχανές μετα-αναζήτησης είναι χρήσιμες για ανάλυση δεδομένων ή για να βρεθούν πολύ συγκεκριμένα στοιχεία. Ωστόσο, καθώς οι μηχανές μετα-αναζήτησης τείνουν να σφετεριστούν τον έλεγχο της αναζήτησης, τα αποτελέσματά τους μπορεί να μην είναι πλήρη και να περιέχουν άσχετα στοιχεία. Επομένως αυτές οι μηχανές, προκαλούν μεγαλύτερη δυσκολία στο να προσδιορίσουν γιατί συγκεκριμένες σελίδες συμπεριλαμβάνονται στα αποτελέσματα της αναζήτησης, και επίσης πώς βρέθηκαν αυτές οι σελίδες. Τα αποτελέσματα της αναζήτησης μπορεί να περιέχουν σελίδες που είναι άσχετες με το αντικείμενο της έρευνας αλλά ωστόσο περιέχουν κάποιες από τις λέξεις κλειδιά που χρησιμοποιήθηκαν από τη μηχανή αναζήτησης. Η αποτυχία εξήγησης για το πώς βρέθηκε ένα συγκεκριμένο στοιχείο απόδειξης, αποδυναμώνει την προσπάθεια έρευνας. Επιπλέον ο μεγάλος αριθμός ελέγχων που είναι κοινοί στις μηχανές μετα-αναζήτησης μπορεί να είναι δυσβάσταχτος και να εμποδίσει την έρευνα.

Αν και οι μηχανές μετα-αναζήτησης μπορεί να είναι χρήσιμες στην αναζήτηση πολύ συγκεκριμένων λεπτομερειών (για παράδειγμα, εμφανίσεις ενός συγκεκριμένου αριθμού τηλεφώνου σε μια ιστοσελίδα), είναι επίσης σημαντικό να γίνεται αναζήτηση σε ειδικευμένες μηχανές ή βάσεις δεδομένων όταν αναζητούμε συγκεκριμένες λεπτομέρειες.

4.3.1.2 *Online* Βάσεις Δεδομένων (Το Αόρατο *web*)

Υπάρχουν πολλές βάσεις δεδομένων στο *web* που περιέχουν δεδομένα με συγκεκριμένη θεματική περιοχή. Για παράδειγμα, *online* βάσεις δεδομένων περιέχουν πληροφορίες σχετικές με εγκλήματα σεξουαλικού περιεχομένου, με εξαφανισμένα παιδιά, με περιουσιακά στοιχεία ή στοιχεία πιστωτικών καρτών και με ιατρικές πληροφορίες χρηστών. Πολλές από αυτές τις βάσεις δεδομένων μπορεί να εντοπιστούν με τη χρήση μηχανών αναζήτησης αλλά οι πληροφορίες που περιέχουν θα πρέπει να αναζητηθούν απ' ευθείας. Για παράδειγμα, χρησιμοποιώντας το *Google* ή το *Altavista* για αναζήτηση του "*sex AND offender AND database*" μπορούμε να πάρουμε πολλές διαφορετικές εγγραφές σχετικές με σεξουαλικά εγκλήματα στις ΗΠΑ. Κάποιες βάσεις δεδομένων είναι οργανωμένες σαν ιστοσελίδες όπως το *JournalismNe*t (http://www.journalismnet.com) και έτσι είναι πιο εύκολο να βρεθούν.

Υπάρχουν επίσης και *online* βάσεις δεδομένων, όπως είναι το *AutoTrack* και το *KnowX*, που περιέχουν μεγάλη ποικιλία πληροφοριών σχετικές με χρήστες, αλλά αυτές οι βάσεις δεδομένων ζητούν συνδρομή για να προσπελαστούν.

Οι βάσεις δεδομένων τύπου *whois* είναι ιδιαίτερα χρήσιμες για αναζητήσεις που εμπλέκουν το διαδίκτυο. Αυτές οι βάσεις δεδομένων διατηρούνται από το διαδίκτυο και περιέχουν ονόματα και πληροφορία επικοινωνίας με χρήστες που είναι υπεύθυνοι για τα υπολογιστικά συστήματα που αποτελούν το διαδίκτυο. Αυτές οι βάσεις δεδομένων, μπορεί να αποκαλύψουν την ταυτότητα του υπεύθυνου ενός ιστοχώρου, περιλαμβάνοντας το όνομα, τον αριθμό τηλεφώνου και τη διεύθυνση. Υπάρχουν ξεχωριστές βάσεις δεδομένων *whois* για τις διαφορετικές χώρες και οι περισσότερες μπορούν να βρεθούν στη βάση *Allwhois*:

- United States (NetSol): http://www.netsol.com/cgi-bin/whois/whois
- United States (ARIN): http://www.whois.arn.met/whois/index.html
- Europe: http://www.ripe.net/db/whois.html
- Asia: http://www.apnic.net/

Κάποιες από αυτές τις βάσεις δεδομένων, περιέχουν πληροφορία μόνο σε υψηλό επίπεδο τομέων (*domains*), ενώ άλλες έχουν πληροφορία σε επίπεδο διευθύνσεων *IP*. Για παράδειγμα, για να βρεθεί η πληροφορία επικοινωνίας για το www.wsex.com, θα πρέπει να γίνει αναζήτηση στη βάση *NetSol,* ενώ για να βρεθεί πληροφορία επικοινωνίας για τη διεύθυνση *IP* 207.42.132.101, θα πρέπει να γίνεται αναζήτηση στη βάση *ARIN.* Θα πρέπει να επισημανθεί ότι αυτές οι βάσεις δεδομένων έχουν ελαφρώς διαφορετική πληροφορία επικοινωνίας για το *World Sports Exchange.*

Ιστοσελίδες όπως η *Geektools* διευκολύνουν τον έλεγχο προσφέροντας μια μοναδική διεπαφή σε πολλές βάσεις δεδομένων *whois.* Επίσης είναι δυνατό να κάνουμε αναζητήσεις σε αυτές τις βάσεις δεδομένων και για άλλα πεδία, όπως είναι τα ονόματα και οι διευθύνσεις ηλεκτρονικού ταχυδρομείου. Κάποιοι χρήστες, χρησιμοποιούν υπηρεσίες όπως είναι η *Domain by Proxy* για να εμποδίσουν τη δημοσίευση της πληροφορίας επικοινωνίας τους στις βάσεις δεδομένων *whois.*

4.3.2 *Online* Ανωνυμία και Αυτό-προστασία

Είναι πολύ σημαντικό για τους ερευνητές να αποκτήσουν οικειότητα με την χρήση της *online* ανωνυμίας για να προστατευτούν, και να κατανοήσουν τον τρόπο με τον οποίο χρησιμοποιούν την ανωνυμία οι εγκληματίες και οι εισβολείς ώστε να αποφύγουν την ανίχνευση. Εκτός από την απόκρυψη των προσωπικών πληροφοριών όπως είναι το όνομα, η διεύθυνση και ο αριθμός τηλεφώνου, κάποιοι εισβολείς χρησιμοποιούν διευθύνσεις *IP* οι οποίες δεν μπορούν να συνδεθούν με αυτούς. Τέτοιου είδους διευθύνσεις *IP* μπορεί να αποκτηθούν χρησιμοποιώντας δωρεάν *ISP (Internet Service Providers*) που επιτρέπουν στους χρήστες να μπουν στο διαδίκτυο χωρίς να πρέπει να δώσουν την ταυτότητά τους. Άλλοι *ISP* προσφέρουν υπηρεσία ανωνυμίας όταν ένας από τους λογαριασμούς των πελατών τους έχει κλαπεί και χρησιμοποιείται από τον σφετεριστή, ώστε να αποκαλυφθεί η ταυτότητά του καθώς είναι *online* και προσπαθεί να παρανομήσει. Τα δημόσια τερματικά υπολογιστών και τα *Internet café* αποτελούν επίσης δημοφιλείς τρόπους σύνδεσης με το διαδίκτυο ανώνυμα.

Οι ερευνητές θα πρέπει να χρησιμοποιούν την ανωνυμία για να προφυλαχθούν καθώς αναζητούν πληροφορίες για εγκληματίες στο διαδίκτυο, ιδιαίτερα όταν διεξάγουν μια μυστική έρευνα. Οι *online* μυστικές έρευνες μπορούν να χρησιμοποιηθούν σε πολλούς τύπους εγκληματικής δραστηριότητας συμπεριλαμβανομένων των *online* τυχερών παιχνιδιών. Όταν διερευνώνται περιπτώσεις *online* τυχερών παιχνιδιών είναι απαραίτητο να δημιουργηθούν διάφορες μυστικές ταυτότητες έτσι ώστε να γίνουν σύνοδοι και να συγκεντρώσουν πληροφορίες για τους οργανισμούς και τα δίκτυα. Οι μυστικές ταυτότητες χρησιμοποιούνται επίσης για τη διακίνηση ναρκωτικών στο διαδίκτυο και κλεμμένου υλικού μέσω ιστοχώρων δημοπρασιών.

4.3.2.1 Proxies

Ένας τρόπος απόκρυψης μιας διεύθυνσης *IP* καθώς κάποιος περιηγείται στο διαδίκτυο είναι να διευθύνει όλες τις αιτήσεις ιστοσελίδων μέσω *proxy*. Οι εξυπηρετητές *web* που προσπελαύνονται μέσω *proxy* καταγράφουν τη διεύθυνση *IP* του *proxy* παρά τη διεύθυνση του υπολογιστή. Τα εμπορικά *web proxy* όπως είναι το *Anonymizer.com* είναι

διαθέσιμα και υπάρχουν πολλές μηχανές στο διαδίκτυο που δρουν σαν *proxy* είτε από λάθος είτε από το σχεδιασμό τους. Πληροφορίες για τους *web proxy* μπορούν να βρεθούν στα:

- http://www.all-nettools.com/privacy/anon.htm
- http://www.inetprivacy.com/a4proxy/
- http://www.anon.inf.tu-dresden.de/

Όταν οι εισβολείς χρησιμοποιούν *web proxy* για να κρύψουν την ταυτότητά τους, δυσκολεύεται περισσότερο η ανίχνευση γιατί οι ερευνητές θα πρέπει να πάρουν πληροφορία από τον εξυπηρετητή στον οποίο βρίσκεται ο διακομιστής (*proxy)* για να διαπιστώσουν την πραγματική διεύθυνση *IP* των εισβολέων. Αυτά τα αρχεία θα πρέπει να είναι διαθέσιμα σε συστήματα που έχουν σχεδιαστεί ειδικά για να προφυλάσσουν την ταυτότητα των χρηστών.

Οι χρήστες που θέλουν να κρύψουν την *IP* διεύθυνσή τους στα δίκτυα συνομιλίας (*chat*) βρίσκουν υπολογιστές που δεν έχουν ρυθμιστεί σωστά, με ανοιχτά *proxy* και τους χρησιμοποιούν χωρίς εξουσιοδότηση. Είναι δύσκολο να πάρει κανείς αρχεία καταγραφής (*log files*) από τέτοιους *proxy*, όταν βρίσκονται σε άλλες χώρες. Για να λύσουν αυτό το πρόβλημα, πολλά δίκτυα *IRC (Internet Relay Chat)* δεν επιτρέπουν σύνδεση με υπολογιστές που βρίσκονται σε έναν εξυπηρετητή *proxy*.

4.3.2.2 Κωδικοποίηση

Για να προστατεύσουν τις διαδικτυακές επικοινωνίες τους, κάποιοι χρήστες κωδικοποιούν τα δεδομένα τους χρησιμοποιώντας *PGP (Pretty Good Privacy)* ή ειδικές υπηρεσίες ηλεκτρονικού ταχυδρομείου όπως το *Hushmail*. Άλλοι χρησιμοποιούν το ασφαλές πρότυπο ηλεκτρονικού ταχυδρομείου (*S/MIME*) που είναι ενσωματωμένο σε πολλούς πελάτες ηλεκτρονικού ταχυδρομείου. Τα κλειδιά κωδικοποίησης που χρησιμοποιούνται στο *S/MIME* συνήθως αποθηκεύονται στο σύστημα ενός χρήστη και προστατεύονται με κωδικό πρόσβασης. Για παράδειγμα, το *Netscape* αποθηκεύει αυτά τα κλειδιά σε ένα αρχείο που ονομάζεται *key3.db*. Ωστόσο, αυτά τα κλειδιά μπορούν να παραχθούν και να αποθηκευθούν σε μια συσκευή *hardware* όπως είναι το *iButton*.

Κάποιοι χρήστες *IRC* υποστηρίζουν την κωδικοποίηση και προκαλούν μεγαλύτερη δυσκολία στους ερευνητές να παρακολουθήσουν επικοινωνίες και να ανακτήσουν ψηφιακές αποδείξεις.

Επιπλέον, τα προγράμματα *trojan horse* μπορούν να διαμορφωθούν ώστε να κωδικοποιούν την κυκλοφορία μεταξύ του πελάτη και του εξυπηρετητή. Για παράδειγμα, κάθε πακέτο που στέλνεται μεταξύ ενός *Back Orifice* πελάτη και του εξυπηρετητή υφίσταται επεξεργασία *X-OR* με ένα γνωστό υπόδειγμα. Ωστόσο, αυτά τα πακέτα ξεκινούν με το ίδιο υπόδειγμα από *bytes*, και τα συστήματα ανίχνευσης εισβολών μπορούν να διαμορφωθούν ώστε να αναγνωρίζουν το κλειδί και να αποκωδικοποιούν την κυκλοφορία.

Γενικά, δεν είναι εφικτό να αποκωδικοποιηθεί η κυκλοφορία του δικτύου και είναι περισσότερο αποτελεσματική η αναζήτηση και ανάκτηση ψηφιακών αποδείξεων από τα ακραία σημεία της επικοινωνίας. Οι εισβολείς των υπολογιστικών συστημάτων το έχουν κατανοήσει αυτό, και αντί να προσπαθούν να κλέψουν πιστωτικές κάρτες καθώς τα δεδομένα μεταδίδονται από τον πελάτη προς τον εξυπηρετητή μέσα από μια κρυπτογραφημένη σύνδεση *SSL (Secure Sockets Layer),* στοχεύουν προς τα τελικά σημεία της σύνδεσης. Οι εισβολείς των υπολογιστικών συστημάτων συνήθως κλέβουν πιστωτικές κάρτες εγκαθιστώντας ένα πρόγραμμα *trojan horse* στο σύστημα του

θύματος και παρακολουθώντας την πληκτρολόγηση ή εισβάλοντας στον εξυπηρετητή και κλέβοντας το αρχείο ή τη βάση δεδομένων που περιέχει τις πληροφορίες της πιστωτικής κάρτας. Παρόμοια, όταν οι εισβολείς δεν μπορούν να αποκτήσουν τους κωδικούς πρόσβασης με τη χρήση ενός *sniffer* επειδή η κίνηση είναι κωδικοποιημένη με *SSH*, στοχεύουν τα ακραία σημεία της κίνησης αντικαθιστώντας το λογισμικό του *SSH* εξυπηρετητή με μια έκδοση που γράφει τους κωδικούς πρόσβασης σε ένα αρχείο.

4.3.2.3 Ανώνυμα και Ψευδώνυμα *E-mail*

Οι χρήστες οι οποίοι έχουν τεχνικές γνώσεις και ενδιαφέρονται να διαφυλάξουν την ταυτότητά τους, στέλνουν μηνύματα μέσω ανώνυμων και ψευδώνυμων υπηρεσιών. Για παράδειγμα, όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου στέλνεται μέσω ενός ανώνυμου *remailer* (ενδιάμεσος εξυπηρετητής που λαμβάνει ένα *e-mail* και το προωθεί), η πληροφορία της ταυτότητας αφαιρείται από την κεφαλίδα του *e-mail* πριν αυτό σταλθεί στον προορισμό του. Οι πιο αποτελεσματικοί ανώνυμοι *remailers* (για παράδειγμα *Mixmaster* και *Cyberpunk*) είναι εξαιρετικά εξελιγμένοι και με αυτούς είναι πολύ δύσκολο να βρεθεί ποιός έστειλε το μήνυμα.

Ωστόσο, ακόμα κι όταν χρησιμοποιούνται αυτοί οι *remailers,* μπορεί να συμβεί η μετάδοση των αποδείξεων καθώς ο αποστολέας μεταφέρει κάτι μέσα στο μήνυμα, το μήνυμα αφήνει ίχνη πίσω του και οι ενδιάμεσες μηχανές που χειρίζονται το μήνυμα μπορεί να έχουν χρήσιμες πληροφορίες. Ο αποστολέας μπορεί να συμπεριλάβει κάτι προσωπικό ή το μήνυμα μπορεί να περιέχει χαρακτηριστικά τα οποία δίνουν μια ένδειξη για την πηγή του. Ο υπολογιστής του αποστολέα μπορεί να διατηρεί τμήματα του μηνύματος, το κλειδί κωδικοποίησης με το οποίο υπέγραψε το μήνυμα ή μια καθαρή σύνδεση προς τον *remailer* που χρησιμοποιήθηκε.

Οι ενδιάμεσοι εξυπηρετητές μπορεί να περιέχουν αρχεία καταγραφής με χρονική σφραγίδα που δείχνουν από πού λήφθηκαν τα δεδομένα και προς τα πού κατευθύνονται. Χρησιμοποιώντας αυτά τα τμήματα της πληροφορίας, είναι δυνατό να περιοριστούν οι πιθανοί ύποπτοι και τελικά η έρευνα να εστιάσει σε λίγους χρήστες. Κάποιοι *remailers* προσπαθούν να ελαχιστοποιήσουν τη μετάδοση της πληροφορίας που θα μπορούσε να χρησιμοποιηθεί για να συνδέσει ένα μήνυμα με τον αποστολέα του, αλλά καμιά μηχανή δεν είναι τέλεια.

Οι πραγματικά ανώνυμοι *remailers* δεν αναγκάζουν τον αποστολέα να λάβει απάντηση στο μήνυμά του επειδή δεν είναι δυνατό να συνδέσουν το μήνυμα με αυτόν που το έστειλε. Για το λόγο αυτό, οι πραγματικά ανώνυμες υπηρεσίες είναι χρήσιμες όταν ο χρήστης δεν ενδιαφέρεται για να διατηρήσει μια σύνδεση δύο δρόμων. Ανωνυμία σημαίνει ότι δεν υπάρχει ταυτότητα και δεν είναι δυνατό να διατηρηθεί μακράς διάρκειας σύνδεση με το αντικείμενο.

Η ψευδωνυμία, δηλαδή η δημιουργία ταυτοτήτων που δεν μπορούν να συνδεθούν με την αληθινή ταυτότητα του χρήστη, επιτρέπουν την πλήρη πρόσβαση στο διαδίκτυο και την εγκαθίδρυση συνδέσεων μακράς διάρκειας χωρίς να κινδυνεύει η ιδιωτικότητα του χρήστη. Επειδή οι περισσότεροι άνθρωποι που χρησιμοποιούν *e-mail* θέλουν να πάρουν απάντηση, χρησιμοποιούν ψευδώνυμους εξυπηρετητές για να αποκρύψουν την πραγματική τους ταυτότητα.

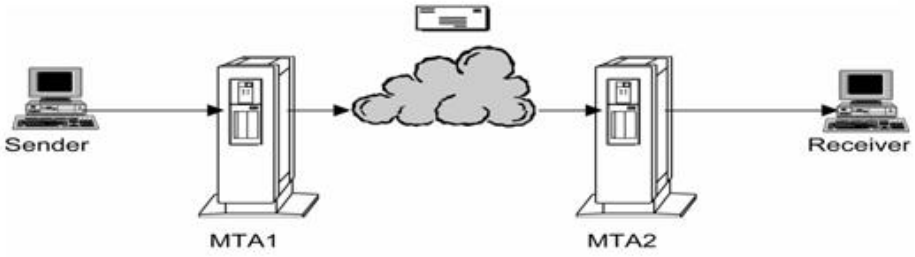
Κάποιοι *remailers* διατηρούν αρχεία καταγραφής με τις πραγματικές *IP* διευθύνσεις των χρηστών, αλλά οι περισσότεροι *remailers* δεν παραχωρούν τα δικαιώματά τους ακόμα και όταν υπάρχει υποψία παρανομίας. Υπάρχει πιθανότητα οι ερευνητές να αναγκάσουν το *remailer* να αποκαλύψει την ταυτότητα του αποστολέα, αλλά αυτό

απαιτεί επιπλέον προσπάθεια καθώς ο σκοπός του *remailer* είναι να προστατεύει την ταυτότητα των αποστολέων.

4.3.3 Πλαστογραφία *e-mail* και Ανίχνευση

Είναι συχνά πιθανό να ανιχνευθεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου πίσω προς την πηγή του και να αναγνωριστεί ο αποστολέας χρησιμοποιώντας τις πληροφορίες που βρίσκονται στην κεφαλίδα του *e-mail*. Εκτός από την εξαγωγή πληροφορίας από την κεφαλίδα του *e-mail*, είναι σημαντικό να καταλάβουμε πώς πλαστογραφούνται τα μηνύματα ηλεκτρονικού ταχυδρομείου. Η βασική χρήση των πλαστογραφημένων *e-mail* είναι να δώσουν στον παραλήπτη λάθος εντύπωση. Για παράδειγμα ο αποστολέας μπορεί να παραστήσει τον προϊστάμενο του παραλήπτη ή ένα φίλο του. Κάποιοι εισβολείς πλαστογραφούν τα *e-mail* σε μια προσπάθεια να καλύψουν την ταυτότητά τους. Ωστόσο, αυτή η προσέγγιση της ανωνυμίας δεν είναι αποτελεσματική γιατί οι πλαστογραφίες συνήθως περιέχουν τη διεύθυνση *IP* του αποστολέα.

Πριν ασχοληθούμε με το θέμα της πλαστογραφίας και της ανίχνευσης *e-mail,* θα πρέπει να καταλάβουμε πώς ένα μήνυμα δημιουργείται και μεταδίδεται. Υπάρχουν υπολογιστές στο διαδίκτυο, που ονομάζονται *Message Transfer Agents (MTA*) που είναι το αντίστοιχο των ταχυδρομείων για τα ηλεκτρονικά μηνύματα (***σχήμα 33***). Όταν στέλνεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου, πρώτα πηγαίνει στο τοπικό *MTA*. Όπως και ένα ταχυδρομικό γραφείο βάζει γραμματόσημα στα γράμματα, έτσι και το τοπικό *MTA* τοποθετεί την τρέχουσα ώρα και το όνομα του *MTA* μαζί με κάποια τεχνική πληροφορία στην κορυφή του *e-mail*. Αυτά τα στοιχεία αποτελούν την κεφαλίδα λήψης. Το μήνυμα τότε περνάει σε έναν άλλο *MTA* μέχρι που φθάνει στον προορισμό του.



Σχήμα 33: ***Message Transfer Agent***

Κάθε *MTA* που λαμβάνει το μήνυμα βάζει μια κεφαλίδα λήψης στην κορυφή του μηνύματος. Αυτό σημαίνει ότι ο τελευταίος υπολογιστής που θα χειριστεί το μήνυμα βρίσκεται στην κορυφή της κεφαλίδας και ο πρώτος βρίσκεται στο τέλος. Έτσι για να ανιχνεύσουμε ένα μήνυμα προς τον αποστολέα του, θα πρέπει να ακολουθήσουμε το δρόμο στον οποίο ταξίδεψε το *e-mail* διαβάζοντας την κεφαλίδα του από πάνω προς τα κάτω.

Όταν ένα *e-mail* πλαστογραφείται, η πλαστογραφημένη κεφαλίδα λήψης δεν είναι συνεπής με τις άλλες κεφαλίδες. Η σφραγίδα ημερομηνίας και ώρας στην πλαστογραφημένη κεφαλίδα είναι διαφορετική από τις υπόλοιπες σφραγίδες χρόνου. Επιπλέον, η πλαστογραφημένη κεφαλίδα δηλώνει ότι το μήνυμα λήφθηκε από το *“mta.nonexistent.com”* και σ’ αυτή την περίπτωση η επόμενη κεφαλίδα λήψης θα

έπρεπε να δείχνει ότι το μήνυμα πέρασε από το *"mta.nonexistent.com"* στο *"mta.sending.com".* Ωστόσο, η επόμενη κεφαλίδα δεν έχει καμιά αναφορά σε *"mta.nonexistent.com*" και αντί γι' αυτό αποκαλύπτει την πραγματική *IP* διεύθυνση του αποστολέα. Ο *ISP* που είναι υπεύθυνος για την *IP* διεύθυνση του αποστολέα μπορεί να χρησιμοποιήσει αυτή την πληροφορία για να διαπιστώσει ποιός κωδικός χρήστη χρησιμοποιήθηκε για να σταλθεί το μήνυμα. Για να κρύψουν την διεύθυνση *IP*, κάποια *e-mail* πλαστογραφούν τα σταλμένα μηνύματα με σύνδεση σε ένα *SMTP* μέσω ενός *proxy*. Αυτή η προσέγγιση κάνει πιο δύσκολη την εύρεση της *IP* διεύθυνσης της πηγής επειδή ο *web proxy* μπορεί να αποκρύψει αποτελεσματικά αυτή την πληροφορία.

4.3.3.1 Μεταφράζοντας τις Κεφαλίδες των *e-mail*

Εκτός κι αν έχει χρησιμοποιηθεί ένας *remailer* ή μια προηγμένη τεχνική πλαστογραφίας, μια σημαντική πληροφορία που μπορεί να οδηγήσει στην ταυτότητα του αποστολέα θα έχει αποθηκευτεί κάπου μέσα στο μήνυμα. Ο σκοπός είναι να βρεθεί αυτή η πληροφορία-κλειδί μέσα σε πολλές και παραπλανητικές πληροφορίες. Για σκοπούς ανίχνευσης του *e-mail*, οι δύο πιο χρήσιμες κεφαλίδες είναι οι "*Message-ID"* και *"Received".* Ένα *Message-ID* θα πρέπει να είναι μοναδικό, δεν πρέπει να υπάρχουν δύο μηνύματα που να έχουν το ίδιο *Message-ID*. Κάποια *MTA* κατασκευάζουν το *Message-ID* χρησιμοποιώντας την τρέχουσα ημερομηνία και ώρα, το όνομα τομέα *(domain name)* του *MTA* και το όνομα χρήστη του αποστολέα.

Δεν μπορούμε πάντοτε να βασιζόμαστε στη μοναδικότητα του *Message-ID,* καθώς αυτό μπορεί να πλαστογραφηθεί. Αν και οι κεφαλίδες *Received* μπορεί να πλαστογραφηθούν και να εισαχθούν μέσα στο μήνυμα για να μπερδέψουν τους ερευνητές, κάποιες κεφαλίδες στην κορυφή του μηνύματος θα πρέπει να είναι έγκυρες γιατί προστέθηκαν από τα *MTA* που παρέδωσαν το μήνυμα.

Σε κάποιες περιπτώσεις, μια κεφαλίδα *Received* θα περιέχει την *e-mail* διεύθυνση του αποστολέα. Σε άλλες περιπτώσεις, μια κεφαλίδα *Received* θα περιέχει την διεύθυνση *IP* του υπολογιστή πηγής και μπορεί να είναι απαραίτητο να επικοινωνήσουμε με κάποιον υπεύθυνο για τις διευθύνσεις *IP* στο *ISP*, ώστε να βρεθεί ποιός χρησιμοποιούσε το συγκεκριμένο υπολογιστή όταν στάλθηκε το μήνυμα. Για παράδειγμα, πολλοί χρησιμοποιούν διευθύνσεις *e-mail* χωρίς ταυτότητα (με χρήση ψευδωνύμων) αλλά δεν γνωρίζουν ότι οι κεφαλίδες *e-mail* αυτών των μηνυμάτων περιέχουν την διεύθυνση *IP* του υπολογιστή πηγής.

Το *Hotmail* και άλλες παρόμοιες υπηρεσίες διατηρούν αρχεία καταγραφής τα οποία είναι χρήσιμα για την αναγνώριση του αποστολέα. Μπορεί να χρησιμοποιηθεί κάποιος *web proxy* για να κρύψει την διεύθυνση *IP* του υπολογιστή πηγής, κάνοντας πιο δύσκολο τον καθορισμό της πραγματικής πηγής του μηνύματος. Όταν χρησιμοποιείται ένας *proxy*, η κεφαλίδα του μηνύματος θα περιέχει την διεύθυνση *IP* του εξυπηρετητή *proxy* και είναι απαραίτητο να αποκτηθούν τα αρχεία καταγραφής πρόσβασης από τον εξυπηρετητή *proxy* ώστε να βρεθεί η αρχική πηγή του μηνύματος.

4.3.4 Επίλογος

Η εγκληματική δραστηριότητα στο διαδίκτυο, μπορεί να δημιουργήσει ένα σημαντικό αριθμό πληροφορίας στο επίπεδο εφαρμογών, συμπεριλαμβανόμενων των ιστοσελίδων *web*, των μηνυμάτων ηλεκτρονικών ταχυδρομείων και των αρχείων καταγραφής *IRC.* Εκτός από την εξαγωγή πληροφοριών από αυτές τις πηγές ψηφιακών αποδείξεων, εξίσου σημαντική είναι η έρευνα στα σχετικά αρχεία των εξυπηρετητών και η παρακολούθηση της κυκλοφορίας στο δίκτυο, για την εγκαθίδρυση μιας συνέχειας στην άμυνα και για τον εντοπισμό των επιτιθέμενων. Επίσης πρέπει απαραίτητα να

ελέγχεται η μεταφορά των ψηφιακών αποδείξεων μεταξύ του υπολογιστή του επιτιθέμενου και των άλλων συστημάτων στο διαδίκτυο, που βοηθά την απόδοση των *online* δραστηριοτήτων στον επιτιθέμενο. Είναι πολύ πιο δύσκολο να εγκαθιδρύσουμε την συνέχεια στην άμυνα, όταν οι επιτιθέμενοι προσπαθούν να κρύψουν τις δραστηριότητές τους ή την ταυτότητά τους στο διαδίκτυο.

Όταν ακολουθούμε τα ψηφιακά ίχνη, θα πρέπει να έχουμε υπόψη μας ότι ένας από τους κυριότερους περιορισμούς του διαδικτύου σαν πηγή αποδείξεων, είναι ότι γενικά το διαδίκτυο έχει την τελευταία έκδοση της πληροφορίας. Αν μια σελίδα *web* τροποποιηθεί, οι παλιές πληροφορίες συνήθως έχουν χαθεί. Επειδή δεν μπορούμε να υποθέσουμε ότι οι αποδείξεις θα μείνουν στο διαδίκτυο για κάποια χρονική διάρκεια, θα πρέπει να τις συλλέγουμε όσο το δυνατόν πιο γρήγορα. Επίσης είναι σημαντικό να θυμόμαστε ότι δεν αρχειοθετούνται αυτόματα όλες οι δραστηριότητες που γίνονται στο διαδίκτυο. Αν ο ερευνητής είναι αρκετά τυχερός ώστε να είναι στο σωστό μέρος τη σωστή ώρα, η έρευνα των αλληλεπιδράσεων *online* μπορεί να βοηθήσει πολύ τις έρευνες, όπως και τα αρχεία καταγραφής συζητήσεων (*chat logs*). Με κάθε τρόπο, αυτές οι αλληλεπιδράσεις *online* περιέχουν έναν θησαυρό πληροφοριών συμπεριφοράς των ατόμων που εμπλέκονται στις επιθέσεις. **[17]**

4.4 Προστασία της Ιδιωτικότητας στην Ηλεκτρονική Ψηφοφορία

Η έννοια της προστασίας της ιδιωτικότητας αναφέρεται γενικά στη θέσπιση του κατάλληλου νομικού πλαισίου, καθώς και στην εφαρμογή ειδικών τεχνικών και τεχνολογιών για την προφύλαξη του πολίτη από την αποκάλυψη σε μη εξουσιοδοτημένες οντότητες, πληροφοριών και δεδομένων που τον αφορούν.

Η έννοια αυτή, όμως, αποκτά κάποιες ιδιαιτερότητες όταν αναφέρεται σε μια διαδικασία ψηφοφορίας, στα πλαίσια της λειτουργίας ενός δημοκρατικού πολιτεύματος. Τώρα η έννοια της προστασίας της ιδιωτικότητας γίνεται πολυδιάστατη και δεν περιορίζεται απλά και μόνο στην προφύλαξη του πολίτη από την αποκάλυψη προσωπικών δεδομένων, π.χ. αποκάλυψη στοιχείων τόπου διαβίωσης, τηλεφώνου επικοινωνίας ή ευαίσθητων προσωπικών δεδομένων σε μη εξουσιοδοτημένες οντότητες.

Για παράδειγμα, σε μια διαδικασία ψηφοφορίας, δεν υπάρχει η έννοια της ***εξουσιοδοτημένης οντότητας*** (*authorized entity).* Καμιά οντότητα δεν θα πρέπει να έχει δικαίωμα ανάγνωσης της ψήφου του πολίτη σε οποιαδήποτε χρονική στιγμή, ανεξάρτητα από τη θεσμική της θέση σε ένα πολίτευμα. Ως άλλο παράδειγμα, ενώ στην κλασσική έννοια της προστασίας της ιδιωτικότητας υπάρχει το στοιχείο της προστασίας από πώληση προσωπικών δεδομένων (π.χ. στοιχεία διαβίωσης ή οικονομικής κατάστασης) από οποιονδήποτε οργανισμό (π.χ. τράπεζα), στο πλαίσιο μιας ψηφοφορίας έχουμε την αποτροπή από πώληση της ψήφου, που είναι και αυτό ένα προσωπικό δεδομένο, από τον ίδιο τον κάτοχο. Επίσης σε μια διαδικασία ψηφοφορίας θα πρέπει ο ψηφοφόρος να προστατεύεται από εξαναγκασμό, καθώς κάτι τέτοιο αποτελεί σοβαρή παραβίαση της ιδιωτικότητάς του (μυστικότητα της ψήφου).

Ως πρόσθετη ειδική παράμετρος στο θέμα της προστασίας της ιδιωτικότητας είναι και το γεγονός ότι θα πρέπει να παρέχονται στον ψηφοφόρο εγγυήσεις ότι η ψήφος του δεν έχει παραλλαχθεί μετά την ψηφοφορία και, επιπλέον ότι είναι το ίδιο σημαντική όσο και οποιουδήποτε άλλου στη διαμόρφωση του τελικού αποτελέσματος. Επιπρόσθετα, όταν αναφερόμαστε σε ηλεκτρονική ψηφοφορία ή ψηφοφορία από απόσταση, εμφανίζεται ένα άλλο σύνολο παραμέτρων προστασίας της ιδιωτικότητας οι οποίες, ενώ δεν σχετίζονται άμεσα με τη διαδικασία της ψηφοφορίας, εντούτοις αποτελούν πηγή σημαντικών κινδύνων για την παραβίαση της ιδιωτικότητας του ψηφοφόρου. Παραδείγματα τέτοιων παραμέτρων είναι το διαδίκτυο, η ορθότητα του λογισμικού που χρησιμοποιείται στο σύστημα υποστήριξης της ηλεκτρονικής ψηφοφορίας, το κακόβουλο λογισμικό στον υπολογιστή του χρήστη κ.α.

Όλα τα παραπάνω συνιστούν ένα ιδιαίτερα πολυσύνθετο πρόβλημα προστασίας της ιδιωτικότητας, το οποίο μάλιστα γίνεται ακόμη πιο πολύπλοκο με τη χρήση νέων τεχνολογιών, οι οποίες έχουν τα δικά τους δύσκολα προβλήματα παραβίασης της ιδιωτικότητας του ατόμου, για την υποστήριξη διαδικασιών ψηφοφορίας ηλεκτρονικά και από απόσταση.

4.4.1 Απαιτήσεις Ασφάλειας και Ζητήματα Ιδιωτικότητας για τα Συστήματα Ηλεκτρονικής Ψηφοφορίας

Θα παρουσιάσουμε τις βασικές απαιτήσεις ασφάλειας για ένα σύστημα ηλεκτρονικής ψηφοφορίας με στόχο την ανάδειξη της συνθετότητας του προβλήματος της προστασίας της ιδιωτικότητας σε αυτό το πεδίο εφαρμογής. Το πρόβλημα ξεφεύγει από τα στενά πλαίσια της απλής προστασίας προσωπικών δεδομένων (που μπορεί να λυθεί με διάφορους τρόπους, όπως με κρυπτογράφηση) και περιλαμβάνει απαιτήσεις επαληθευσιμότητας της ψήφου από τον ψηφοφόρο αλλά και την εκλογική αρχή, προστασίας του ψηφοφόρου από εξαναγκασμό και αποτροπής από πώληση ψήφου.

4.4.1.1 Συστήματα Ηλεκτρονικής Ψηφοφορίας

Η ηλεκτρονική ψηφοφορία *(e-voting)* είναι η ψηφοφορία με τη χρήση ηλεκτρονικών μέσων, δηλαδή στην ουσία ηλεκτρονική άσκηση του δικαιώματος της ψήφου. Τα ηλεκτρονικά μέσα μπορεί να περιλαμβάνουν συστήματα υπολογιστών, δίκτυα επικοινωνίας, ειδικό ηλεκτρονικό εξοπλισμό κ.λπ. Η ψηφοφορία είναι δυνατό να διεξάγεται από συγκεκριμένα σημεία (εκλογικά κέντρα ή άλλα ελεγχόμενα μέρη) ή απομακρυσμένα, από οποιοδήποτε σημείο μέσω του διαδικτύου, τηλεφώνων, ψηφιακής διαδραστικής τηλεόρασης κ.λπ. Για να είναι ασφαλής η διαδικασία χρησιμοποιούνται κρυπτογραφικές τεχνικές και πρωτόκολλα.

Ένα σύστημα ηλεκτρονικής ψηφοφορίας είναι ένα σύνθετο πληροφοριακό σύστημα που περιλαμβάνει:

- Συστήματα υλικού και λογισμικού:
    - Εξυπηρετητές και σταθμούς εργασίας, συστήματα βάσεων δεδομένων κ.λπ., που επικοινωνούν μέσα από μια ασφαλή υποδομή επικοινωνίας
    - Κρυπτογραφικά πρωτόκολλα, λειτουργικά συστήματα, προγράμματα *middleware*, εφαρμογές πελάτη.
- Ένα σύνολο εξουσιοδοτημένων οντοτήτων που εμπλέκονται στη διεξαγωγή της ψηφοφορίας, όπως ψηφοφόροι, ελεγκτικές αρχές, συντονιστές της ψηφοφορίας, εξωτερικοί παρατηρητές /επιθεωρητές, διαχειριστές των συστημάτων.
- Ένα σύνολο διαδικασιών και κανόνων που καθορίζουν τον τρόπο διεξαγωγής της ψηφοφορίας και παρακολουθούν και ελέγχουν όλα τα επιμέρους στάδια διασφαλίζοντας έτσι την ακεραιότητα της ψηφοφορίας και την εγκυρότητα του τελικού αποτελέσματος.

Κάθε πληροφοριακό σύστημα που χρησιμοποιείται για να υποστηρίξει μια διαδικασία ψηφοφορίας θα πρέπει:

1. Να υποστηρίζει όλες εκείνες τις διαδικασίες που απαιτούνται για την ομαλή οργάνωση και διεξαγωγή της ψηφοφορίας.
2. Να υποστηρίζει τη χρήση ψηφοδελτίων διαφορετικής μορφής και να μπορεί να προσαρμόζεται σε διαφορετικούς τύπους ψηφοφοριών.
3. Να υποστηρίζει όλους τους διαφορετικούς ρόλους που εμπλέκονται στο σύστημα ως χρήστες και να εγγυάται προσβασιμότητα σε όσο το δυνατό μεγαλύτερο αριθμό πολιτών.
4. Να προστατεύει θεμελιώδεις δημοκρατικές αρχές όπως η ελευθερία της ψήφου και της ψηφοφορίας ή η μυστικότητα της ψήφου σε κάθε στάδιο της διαδικασίας ψηφοφορίας.
5. Να υποστηρίζει τη διαφάνεια και την ελεγξιμότητα όλης της διαδικασίας.
6. Να είναι πρακτικό στην υλοποίησή του και αποδοτικό.

4.4.1.2 Θεμελιώδεις Απαιτήσεις Ασφάλειας

Η ψηφοφορία δεσμευτικού χαρακτήρα όπως μία εκλογή ή ένα δημοψήφισμα για παράδειγμα, διέπεται από συνταγματικά κατοχυρωμένες καταστατικές αρχές, οι οποίες τυγχάνουν εφαρμογής στο σύνολο των δημοκρατικών πολιτευμάτων. Το 2002 το Συμβούλιο της Ευρώπης υιοθέτησε έναν κώδικα καλής πρακτικής για εκλογικά θέματα ο οποίος αναγνωρίζει πέντε θεμελιώδεις αρχές για τη διενέργεια δημοκρατικών εκλογών:

1. ***Καθολική ψηφοφορία (universal suffrage):*** Κάθε πολίτης έχει το δικαίωμα ψήφου και εκλογής εφόσον πληρεί τις προϋποθέσεις που ορίζει ο νόμος (π.χ. ηλικία, εθνικότητα κλπ).
2. ***Ισότητα της ψήφου και των ψηφοφόρων (equal suffrage):*** Κάθε πολίτης δικαιούται μια ψήφο και όλες οι ψήφοι είναι μεταξύ τους ισοδύναμες.
3. ***Ελευθερία της ψήφου και της ψηφοφορίας (free suffrage):*** Ο ψηφοφόρος έχει το δικαίωμα να εκφράσει τη βούλησή του ελεύθερα και χωρίς κανένα εξαναγκασμό ή άσκηση πίεσης.
4. ***Μυστικότητα της ψήφου (secret suffrage):*** Ο ψηφοφόρος έχει το δικαίωμα να ψηφίσει μυστικά.
5. ***Αμεσότητα της ψήφου και της ψηφοφορίας (direct suffrage):*** Οι ψήφοι που έχουν υποβληθεί από τους ψηφοφόρους καθορίζουν απευθείας το εκλογικό αποτέλεσμα.

Σε ένα σύστημα ηλεκτρονικής ψηφοφορίας, η εφαρμογή των πέντε καταστατικών αρχών προσδιορίζει ένα σύνολο θεμελιωδών απαιτήσεων (ιδιοτήτων) ασφάλειας που θα πρέπει να ικανοποιούνται. Οι απαιτήσεις αυτές είναι:

4.4.1.2.1 Δημοκρατικότητα (Democracy)

Ένα σύστημα χαρακτηρίζεται δημοκρατικό αν και μόνο αν νόμιμοι (εξουσιοδοτημένοι) ψηφοφόροι δικαιούνται να ψηφίσουν. Κανένας ψηφοφόρος δεν μπορεί να ψηφίσει περισσότερες από μία φορές εκτός εάν το σύστημα λαμβάνει υπόψη μόνο μία από τις ψήφους (συνήθως την τελευταία). Επιπλέον, κανένας δεν μπορεί να ψηφίσει στη θέση κάποιου άλλου.

4.4.1.2.2 Ορθότητα – Ακρίβεια (Accuracy)

Η ορθότητα απαιτεί ότι το αποτέλεσμα της ψηφοφορίας που ανακοινώνεται είναι το πραγματικό αποτέλεσμα των εκλογών όπως προκύπτει από το στάδιο της καταμέτρησης των ψήφων. Αυτό πρακτικά σημαίνει ότι κανένας δεν είναι σε θέση να αλλοιώσει ή να διαγράψει την ψήφο κάποιου άλλου, όλες οι έγκυρες ψήφοι έχουν υπολογιστεί στο τελικό αποτέλεσμα μία φορά η κάθε μια και καμιά μη έγκυρη ψήφος δεν έχει συμπεριληφθεί.

4.4.1.2.3 Μυστικότητα (Secrecy)

Η συγκεκριμένη απαίτηση σχετίζεται με το γεγονός ότι όλες οι ψήφοι παραμένουν μυστικές σε όλη τη διάρκεια της ψηφοφορίας αλλά και μετά τη λήξη της, ενώ κανένας δεν μπορεί να συνδέσει την ταυτότητα ενός ψηφοφόρου με την ψήφο του.

4.4.1.2.4 Μη Αναγκαιότητα Έκδοσης Απόδειξης (Receipt-freeness)

Το κρυπτογραφικό πρωτόκολλο που χρησιμοποιεί το σύστημα είναι σε θέση να πείθει τον ψηφοφόρο ότι η ψήφος του καταμετρήθηκε στο τελικό αποτέλεσμα χωρίς όμως να μπορεί να παρέχει απόδειξη γι' αυτό. Έτσι, ο ψηφοφόρος δεν μπορεί με οποιονδήποτε τρόπο να πείσει έναν τρίτο για το αληθινό περιεχόμενο της ψήφου του, ακόμα κι αν επιθυμεί κάτι τέτοιο. Η ιδιότητα της μη αναγκαιότητας έκδοσης απόδειξης χρησιμοποιείται στη διεθνή βιβλιογραφία ως το κυριότερο μέσο για να επιτευχθεί η ασφάλεια του συστήματος ηλεκτρονικής ψηφοφορίας συνεισφέροντας στην αποτροπή φαινομένων πώλησης ψήφου.

4.4.1.2.5 Προστασία από Εξαναγκασμό (Uncoercibility)

Κανένας ψηφοφόρος δεν κατέχει ούτε είναι σε θέση να δημιουργήσει μια απόδειξη που να δείχνει το περιεχόμενο της ψήφου του. Η έννοια της προστασίας από εξαναγκασμό είναι περισσότερο ισχυρή από την έννοια της μη αναγκαιότητας της έκδοσης απόδειξης, παρ' όλα αυτά στη βιβλιογραφία χρησιμοποιούνται και οι δύο για να δηλώσουν την προστασία από επιθέσεις πώλησης της ψήφου ή/και του εξαναγκασμού και επιβολής ψήφου.

4.4.1.2.6 Δικαιοσύνη (Fairness)

Η απαίτηση αυτή διασφαλίζει ότι κανείς δεν μπορεί να μάθει το αποτέλεσμα της ψηφοφορίας πριν από την τελική καταμέτρηση των ψήφων και την επικύρωση του αποτελέσματος. Αυτό πρακτικά σημαίνει ότι αυτοί που ψηφίζουν προς το τέλος της περιόδου υποβολής των ψήφων δεν θα επηρεαστούν από την ανακοίνωση μιας εκτίμησης του αποτελέσματος.

4.4.1.2.7 Επαληθευσιμότητα (Verifiability)

Η επαληθευσιμότητα σχετίζεται με την ύπαρξη μηχανισμών ελέγχου της διαδικασίας ψηφοφορίας προκειμένου αυτοί να εξασφαλίσουν ότι όλες οι ψήφοι παραλήφθηκαν κανονικά και καταμετρήθηκαν σωστά. Η επαληθευσιμότητα μπορεί να είναι ***οικουμενική*** (*universal*) όπου όλοι (ψηφοφόροι, αρχές ελέγχου, παρατηρητές κ.λπ.) είναι σε θέση να επιβεβαιώσουν το αποτέλεσμα μετά την καταμέτρηση των ψήφων, ή ***ατομική*** (*individual*) που είναι πιο ασθενής και επιτρέπει σε κάθε ψηφοφόρο να επιβεβαιώσει ότι η ψήφος του καταμετρήθηκε σωστά.

4.4.1.2.8 Επαληθεύσιμη Συμμετοχή (Verifiable Participation)

Η ιδιότητα αυτή διασφαλίζει ότι υπάρχει δυνατότητα να βρεθεί αν ένας συγκεκριμένος πολίτης συμμετείχε ή όχι στη ψηφοφορία. Αυτό είναι αναγκαίο στις περιπτώσεις όπου η συμμετοχή στην ψηφοφορία είναι υποχρεωτική ή σε περιπτώσεις οργανισμών, συλλόγων όπου το ποσοστό αποχής μπορεί να έχει συγκεκριμένο νόημα.

4.4.1.2.9 Ανθεκτικότητα (Robustness)

Η απαίτηση αυτή εγγυάται ότι δεν μπορεί να λάβει χώρα μια προσωρινή συνεργασία (νόμιμη ή κακόβουλη) είτε ψηφοφόρων, είτε αρχών, είτε εσωτερικών/εξωτερικών εχθρών η οποία θα μπορούσε να διακόψει τη διαδικασία ψηφοφορίας. Αυτό πρακτικά σημαίνει ότι η δυνατότητα αποχής των ψηφοφόρων δεν θα δημιουργήσει προβλήματα, καθώς επίσης και ότι αποτρέπονται παράνομες ενέργειες οι οποίες ενδέχεται να ακυρώσουν το αποτέλεσμα της ψηφοφορίας. Η απαίτηση της ανθεκτικότητας αφορά επίσης και στο ότι η ασφάλεια του συστήματος πρέπει να ικανοποιείται παρά τα όποια τυχαία σφάλματα ή εξωτερικές απειλές και επιθέσεις.

Ένα σύστημα ηλεκτρονικής ψηφοφορίας θα πρέπει να ικανοποιεί όσο το δυνατό περισσότερες από τις παραπάνω απαιτήσεις, αν όχι όλες. Είναι δυνατόν κάποιες απαιτήσεις να συνυπάρχουν, αφού η ύπαρξη της μιας υπονοεί την ύπαρξη κάποιας άλλης ή πολλές φορές να ενισχύει η μια την άλλη. Είναι όμως επίσης δυνατόν κάποιες από τις απαιτήσεις να συγκρούονται ή να μην μπορούν να συνυπάρξουν ή ακόμη και να μη μπορούν να ικανοποιηθούν από το χρησιμοποιούμενο κρυπτογραφικό πρωτόκολλο.

4.4.1.3 Ασφάλεια Απέναντι στους Κινδύνους του Διαδικτύου

Η ασφάλεια στο διαδίκτυο έχει τρία επίπεδα: **α)** ασφάλεια των κεντρικών *web* εξυπηρετητών και των δεδομένων που αποθηκεύονται σε αυτούς, **β)** ασφάλεια κατά την επικοινωνία των δεδομένων μεταξύ εξυπηρετητών και των συστημάτων των χρηστών και **γ)** ασφάλεια των υπολογιστών των χρηστών. Επιπλέον, απαιτούνται η ταυτοποίηση στην επικοινωνία χρήστη – εξυπηρετητή και η τήρηση της κατάλληλης πληροφορίας σε αρχεία καταγραφής συναλλαγών *(transaction logs)* για λόγους μη αποποίησης της ευθύνης στην εκτέλεση μιας συναλλαγής.

Πολλοί ίσως θεωρούν ότι η δυνατότητα εκτέλεσης ηλεκτρονικών συναλλαγών στο διαδίκτυο με χρήση πρωτοκόλλων όπως το *SSL (Secure Sockets Layer)* καθώς και πιστοποίησης των υπολογιστών μπορεί να είναι αρκετή για να προστατευθεί η ιδιωτικότητα του ψηφοφόρου. Όμως η θεώρηση αυτή είναι λανθασμένη, αφού η ψηφοφορία μέσω του διαδικτύου είναι από πολλές απόψεις διαφορετική σε σχέση με τις ηλεκτρονικές διαδικασίες, όπως αυτή του ηλεκτρονικού εμπορίου *(e-commerce*):

1. Οι ηλεκτρονικές συναλλαγές στο διαδίκτυο απαιτούν ταυτοποίηση του χρήστη μέσω *password*, ψηφιακών υπογραφών ή βιομετρικών δεδομένων. Ο ψηφοφόρος όμως θα πρέπει να ταυτοποιηθεί μόνο αφού προηγουμένως έχει εγγραφεί σε κάποιου είδους εκλογικό κατάλογο ενώ ταυτόχρονα η ψήφος του απαιτείται να είναι ανώνυμη.
2. Το να εκτελέσει κάποιος μια συναλλαγή χρησιμοποιώντας την πιστωτική κάρτα της συζύγου του δεν θεωρείται πρόβλημα ασφάλειας στο χώρο του *e-commerce* ενώ το δικαίωμα της ψήφου είναι γενικά μη μεταφέρσιμο.
3. Μια επίθεση στην ασφάλεια ενός συστήματος *e-commerce* μπορεί να έχει ως αποτέλεσμα αδυναμία εκτέλεσης μιας συναλλαγής. Στην περίπτωση αυτή όμως υπάρχει αρκετός χρόνος για την ανίχνευση και την αντιμετώπιση της επίθεσης ώστε το σύστημα να καταστεί και πάλι λειτουργικό. Μια αντίστοιχη επίθεση σε ένα σύστημα ηλεκτρονικής ψηφοφορίας μπορεί να οδηγήσει σε αδυναμία υποβολής της ψήφου κάποιου ψηφοφόρου κι επομένως παραβίαση της ακεραιότητας της διαδικασίας σε περίπτωση που δεν υπάρχει διαθέσιμο εναλλακτικό κανάλι επικοινωνίας.

Το τελευταίο σημείο είναι αρκετά σημαντικό. Πολλά από τα ζητήματα που καλούνται να επιλύσουν τα διαδικτυακά συστήματα ηλεκτρονικής ψηφοφορίας οφείλονται στην ίδια την αρχιτεκτονική του διαδικτύου και στην έλλειψη εγγενών μηχανισμών αυστηρής ρύθμισης των επικοινωνιών πάνω από αυτό. Το διαδίκτυο είναι ένα ανοικτό περιβάλλον με αποτέλεσμα οι επιθέσεις στην ασφάλειά του να είναι γρήγορες και ανέξοδες. Οι επιθέσεις αυτές μπορούν με πολλούς τρόπους να υπονομεύσουν την ψηφοφορία.

4.4.1.3.1 Κίνδυνοι για την Ηλεκτρονική Ψηφοφορία από το Διαδίκτυο

Μια πρώτη κατηγορία επιθέσεων που έχουν στόχο απευθείας τους κεντρικούς εξυπηρετητές ή τους υπολογιστές των χρηστών είναι οι λεγόμενες ***επιθέσεις διείσδυσης*** *(penetration attacks).* Οι επιθέσεις αυτές αποτελούν ευθεία προσπάθεια παραβίασης της ιδιωτικότητας του ψηφοφόρου καθώς είναι δυνατό να εγκατασταθούν κακόβουλα προγράμματα που υποκλέπτουν τα προσωπικά στοιχεία του ψηφοφόρου ή ακόμη και το περιεχόμενο της ψήφου του. Χαρακτηριστικά παραδείγματα είναι όπως παρουσιάσαμε στο *κεφάλαιο 2.2* τα προγράμματα *trojan horse* ή απομακρυσμένου ελέγχου *(remote control programs)* τα οποία μεταδίδονται μέσα από ένα κανάλι διανομής και μπορούν να παρακολουθούν το περιεχόμενο των ψήφων, να

παρεμποδίσουν έναν ψηφοφόρο να υποβάλλει την ψήφο του και να αλλοιώσουν το περιεχόμενο της ψήφου πριν αυτή κρυπτογραφηθεί.

Οι επιθέσεις δεν είναι απαραίτητο να κατευθύνονται σε συγκεκριμένους ή τυχαίους ψηφοφόρους, αλλά μπορεί να έχουν στόχο μια συγκεκριμένη ομάδα πληθυσμού. Επιθέσεις τέτοιου τύπου είναι ιδιαίτερα σοβαρές, επειδή δεν είναι εύκολα ανιχνεύσιμες δεδομένου ότι τα συνήθη πρωτόκολλα ασφαλείας όπως το *SSL* και το *HTTPS* λειτουργούν σε υψηλότερο επίπεδο από αυτό του υπολογιστή – στόχου της επίθεσης δηλ. σε επίπεδο λειτουργικού συστήματος ή σε επίπεδο φυλλομετρητή (*browser*).

Γενικά η ηλεκτρονική ψηφοφορία από συγκεκριμένα σημεία (κιόσκια) είναι λιγότερο ευάλωτη σε τέτοιου είδους επιθέσεις σε σχέση με τη διαδικτυακή. Το λογισμικό στους υπολογιστές που χρησιμοποιούνται για την ψηφοφορία ελέγχεται και επιβλέπεται από εξουσιοδοτημένους υπαλλήλους και μπορεί να ρυθμιστεί με τρόπο που να αποτρέπει την επικοινωνία με οποιονδήποτε διαδικτυακό υπολογιστή εκτός από τους νόμιμους εξυπηρετητές που υποστηρίζουν την ψηφοφορία.

Μια άλλη κατηγορία επιθέσεων στοχεύει στην επικοινωνία μεταξύ των συστημάτων των χρηστών (υπολογιστές απ' όπου υποβάλλεται η ηλεκτρονική ψήφος) και των εξυπηρετητών (π.χ. το σύστημα που διενεργεί την καταμέτρηση). Στην ψηφοφορία μέσω του διαδικτύου, το κανάλι μεταφοράς των ψήφων στα κεντρικά συστήματα πρέπει να είναι έμπιστο. Αυτό προϋποθέτει την αυθεντικοποίηση του καναλιού καθώς και την κρυπτογράφηση των δεδομένων για να διασφαλιστεί η εμπιστευτικότητά τους.

Οι πιο γνωστές επιθέσεις αυτού του τύπου είναι οι επιθέσεις άρνησης παροχής υπηρεσίας οι οποίες δημιουργούν υπερφόρτωση στον υπολογιστή – στόχο διακόπτοντας έτσι την επικοινωνία του με το υπόλοιπο σύστημα. Συγκεντρώνοντας τις επιθέσεις αυτές σε συγκεκριμένες περιοχές όπου, για παράδειγμα, οι ψηφοφόροι είναι γνωστό ότι προτιμούν ένα συγκεκριμένο πολιτικό κόμμα, είναι δυνατό να επιτευχθεί σοβαρή αλλοίωση του αποτελέσματος της ψηφοφορίας ή και κατάρρευση ολόκληρου του συστήματος.

Ένα άλλο είδος επιθέσεων παραβίασης της ιδιωτικότητας του ψηφοφόρου είναι οι επιθέσεις πλαστοπροσωπίας (*spoofing*) όπου οι επιτιθέμενοι προσποιούνται ότι είναι εξουσιοδοτημένες οντότητες και κατευθύνουν τον ανυποψίαστο ψηφοφόρο να συνδεθεί με ένα μη νόμιμο ιστότοπο αντί για τον πραγματικό εξυπηρετητή του συστήματος. Το ίδιο μπορεί να συμβεί αν κάποιος κακόβουλος χρήστης πειράξει, για παράδειγμα, την υπηρεσία ονοματολογίας (*DNS*). Οι επιθέσεις αυτές μπορεί να οδηγήσουν σε μη ανιχνεύσιμη απώλεια μιας ψήφου και φυσικά να αλλοιώσουν το αποτέλεσμα της ψηφοφορίας. Στην χειρότερη περίπτωση ένας μη νόμιμος ιστότοπος μπορεί να ενεργήσει ως ενδιάμεσος μεταξύ του ψηφοφόρου και του νόμιμου ιστότοπου αλλάζοντας το περιεχόμενο της ψήφου.

4.4.1.3.2 Προστασία από Εξαναγκασμό και Επαληθευσιμότητα

Η ψηφοφορία μέσω του διαδικτύου είναι ευάλωτη σε επιθέσεις εξαναγκασμού, οι οποίες αποτελούν και μεγάλο κίνδυνο εναντίον της ιδιωτικότητας του ψηφοφόρου. Οι υπεύθυνοι για την άσκηση πολιτικής αλλά και ειδικοί της ασφάλειας συνήθως αγνοούν τον μη εξαναγκασμό με το βασικό επιχείρημα ότι αν οι ψηφοφόροι μπορούν να ψηφίσουν μέσα από έναν υπολογιστή στο σπίτι τους, δεν υπάρχει τρόπος που εγγυάται ότι κάποιος τρίτος δεν τους παρακολουθεί την ώρα που υποβάλλουν την ψήφο τους. Στην περίπτωση του διαδικτύου ο εξαναγκασμός είναι αναπόφευκτος, αλλά θεωρείται αποδεκτός λόγω της μειωμένης πιθανότητας επηρεασμού του τελικού αποτελέσματος. Ωστόσο, ο κίνδυνος μαζικού εξαναγκασμού ή εξαγοράς ψήφων είναι αρκετά

μεγαλύτερος, αφού οι αποδείξεις των ψήφων μπορούν να συγκεντρωθούν *off-line* και να σταλούν σε έναν τρίτο για την άσκηση εξαναγκασμού. Η απαίτηση μη αναγκαιότητας έκδοσης απόδειξης είναι απαραίτητη προκειμένου να αποτραπεί ο μαζικός και όχι ο μεμονωμένος εξαναγκασμός. Δυστυχώς, σε ένα σύστημα απομακρυσμένης ηλεκτρονικής ψηφοφορίας είναι δύσκολο να αντιμετωπιστεί επαρκώς η απειλή του εξαναγκασμού, η οποία είναι μια σοβαρή προσπάθεια παραβίασης της ιδιωτικότητας του ψηφοφόρου.

4.4.2 Βασικές Τεχνικές Προσεγγίσεις για την Προστασία της Ιδιωτικότητας στην Ηλεκτρονική Ψηφοφορία

Θα αναφερθούμε στα βασικά εργαλεία και πρωτόκολλα προστασίας της ιδιωτικότητας όσον αφορά στα συστήματα ηλεκτρονικής ψηφοφορίας. Όπως ήδη είπαμε, η έννοια της ιδιωτικότητας σε μια διαδικασία ψηφοφορίας είναι πολυδιάστατη και ξεφεύγει από τη συνήθη έννοια της ιδιωτικότητας στην καθημερινότητα, η οποία περιορίζεται στην προφύλαξη προσωπικών δεδομένων από μη εξουσιοδοτημένη προσπέλαση. Αυτός είναι και ο λόγος για τον οποίο οι τεχνικές που θα παραθέσουμε είναι πολύπλοκες και προχωρούν πέρα από μια απλή κρυπτογράφηση της ψήφου (όπως θα γινόταν με μια απλή κρυπτογράφηση ενός ιατρικού φακέλου).

Υπάρχουν δύο βασικές προσεγγίσεις για την προστασία της ιδιωτικότητας σε ένα σύστημα ηλεκτρονικής ψηφοφορίας. Η υποβολή της ψήφου μέσω ενός καναλιού ανώνυμης επικοινωνίας, όπου είναι δυνατή η ύπαρξη της ψήφου σε αναγνώσιμη από όλους μορφή (καθώς δεν υπάρχουν στοιχεία για το ποιός την υπέβαλε) και η υποβολή της ψήφου απευθείας σε κρυπτογραφημένη μορφή, όπου μαζί με την ψήφο πλέον μπορούν να αποθηκευτούν χωρίς πρόβλημα και τα στοιχεία του ψηφοφόρου, ενώ για τη διαδικασία της καταμέτρησης δεν απαιτείται η αποκρυπτογράφηση των ψήφων. Η πρώτη προσέγγιση υλοποιείται με ειδικές διατάξεις δικτύων που ονομάζονται *mix-nets* ενώ η δεύτερη με μια κατηγορία συναρτήσεων κρυπτογράφησης που ονομάζονται ομομορφικές συναρτήσεις.

4.4.2.1 Κανάλια Ανώνυμης Επικοινωνίας – *Mix-nets*

Ένα κανάλι ανώνυμης επικοινωνίας επιτρέπει σε έναν αποστολέα ενός μηνύματος να κρατήσει μυστική την ταυτότητά του από τον παραλήπτη του μηνύματος. Αυτό στην περίπτωση της ηλεκτρονικής ψηφοφορίας, έχει ως αποτέλεσμα την αποσύνδεση της ψήφου από τον ψηφοφόρο, καθώς επίσης και τη δυνατότητα ελέγχου ότι η ψήφος του ψηφοφόρου είναι νόμιμη (καθώς η ψήφος μπορεί να υποβληθεί σε αναγνώσιμη από τον καθένα μορφή).

Ένας τρόπος υλοποίησης ενός καναλιού ανώνυμης επικοινωνίας είναι και τα *mix-nets* όπου *m* εξυπηρετητές που ονομάζονται *mix-servers*, ακολουθιακά αποκρυπτογραφούν και μεταθέτουν τα ψηφοδέλτια που λαμβάνουν ως είσοδο, ώστε με καμιά συνομωσία των *mix servers*, εκτός κι αν όλοι μετέχουν σε αυτή, να μην είναι δυνατή η συσχέτιση μιας ψήφου με έναν ψηφοφόρο. Με άλλα λόγια ο ρόλος ενός *mix-net* είναι η απάλειψη της σχέσης ψήφου-ψηφοφόρου με μια διαδικασία τυχαίας κρυπτογράφησης και μετάθεσης των ψήφων που εισέρχονται σε αυτό. Κάποιες υποδομικές εργασίες που αφορούν πρωτόκολλα ψηφοφορίας που χρησιμοποιούν *mix-nets* παρουσιάζονται συνοπτικά στη συνέχεια.

Στο μοντέλο ψηφοφορίας της εργασίας του *Abe* ορίζονται τέσσερις βασικές οντότητες. ***Οι ψηφοφόροι-χρήστες*****, *ένας πίνακας ανακοινώσεων*****, *οι mix-servers*** και ***οι επαληθευτές*****.** Οι χρήστες κρυπτογραφούν την ψήφο τους σε ψηφοδέλτια με χρήση του κρυπτογραφικού σχήματος *ElGamal* και του διαμοιραζόμενου κλειδιού των *mix-servers*.

Μετά αναρτούν το ψηφοδέλτιο στον πίνακα ανακοινώσεων και όταν ολοκληρωθεί η ψηφοφορία, η λίστα με τα *ballots* περνά στον έλεγχο του *mix-net.*

Η λειτουργία ενός γενικού *mix-net* χωρίζεται σε δύο φάσεις. Τη φάση της ***τυχαιοποίησης*** *(randomization)* ***και μετάθεσης*** (*permutation*) και τη φάση της ***αποκρυπτογράφησης***. Κατά την πρώτη φάση, η ακολουθία των *mix-servers* τυχαιοποιεί και μεταθέτει την είσοδό τους βάσει τυχαίων παραγόντων και μεταθέσεων ξεχωριστών και μυστικών για κάθε *mix-server*. Οι *mix-servers* συνεργάζονται για να εκδώσουν από κοινού μια ***απόδειξη μηδενικής γνώσης*** *(zero knowledge proof*), που καλείται *Proof-P*, η οποία παρέχεται ως απόδειξη εγκυρότητας της διαδικασίας αυτής. Ο κάθε *mix-server* επικυρώνει την απόδειξη αυτή ξεχωριστά για να ανιχνευτούν και να απομακρυνθούν τυχόν κακόβουλοι *mix-servers.* Κατά τη δεύτερη φάση, μια ομάδα από *mix-servers* συνεργάζονται για την αποκρυπτογράφηση της εξόδου της προηγούμενης φάσης με χρήση τεχνικών *threshold decryption*. Και σε αυτή τη φάση οι *mix-servers* συνεργάζονται και εκδίδουν από κοινού μια *zero knowledge* απόδειξη, οποία καλείται τώρα *Proof-D,* ως απόδειξη της εγκυρότητας της αποκωδικοποίησης. Σε περίπτωση αποτυχίας της απόδειξης, εντοπίζονται και απομακρύνονται τυχόν κακόβουλοι *mix-servers* και η διαδικασία επαναλαμβάνεται από μια νέα ομάδα από *mix-servers*. Στο τέλος τα αποκωδικοποιημένα μηνύματα της εξόδου καταγράφονται μαζί με τις αποδείξεις *Proof-D* και *Proof-P* στον πίνακα ανακοινώσεων και μπορούν να επαληθευτούν από οποιονδήποτε ενδιαφερόμενο.

Στο παραπάνω μοντέλο για τη διασφάλιση της ιδιωτικότητας και της ανωνυμίας των ψηφοφόρων, η εργασία καθενός από τους *m mix-servers* επαληθεύεται ξεχωριστά, ώστε να είναι βέβαιο ότι δεν έχει διαρρεύσει μυστική πληροφορία τυχαιοποίησης ή μετάθεσης και ότι κανένας *mix-server* δεν εργάζεται κακόβουλα ακυρώνοντας την εργασία των προηγούμενων. Επίσης, το μοντέλο ορίζει αυστηρά ότι η μετάβαση στην επόμενη φάση πραγματοποιείται μόνο σε περίπτωση επιτυχίας της απόδειξης που αντιστοιχεί στην τρέχουσα φάση. Η ενδεχόμενη αποτυχία στις αποδείξεις *Proof-D* και *Proof-P* στο τέλος κάθε φάσης υποδεικνύει άμεσα και τους μη νόμιμους *mix-servers*, οι οποίοι απομακρύνονται και το *mix-net* αναδιοργανώνεται για να επαναλάβει με ορθό τρόπο την προβληματική φάση.

Η εργασία των *Abe και Hoshino* αποτελεί κριτική σε προηγούμενη εργασία του *Abe* που περιείχε την αρχική πρόταση για την υλοποίηση *mix-net* πάνω σε δίκτυα μεταθέσεων. Αυτή η αρχική πρόταση αποδεικνύεται ότι δίνει μη ισοπίθανες μεταθέσεις τις οποίες μπορούν να εκμεταλλευτούν κακόβουλες αρχές για να παραβιάσουν το σύστημα. Στη συγκεκριμένη εργασία των *Abe και Hoshino* προτείνεται μια λύση γι' αυτό το πρόβλημα, ώστε το υποκείμενο δίκτυο μετάθεσης να δίνει ισοπίθανες μεταθέσεις για τις εισόδους του. Παράλληλα, προτείνονται κάποιες πρόσθετες βελτιώσεις για να είναι πιο αποδοτικό το μοντέλο από την άποψη της υπολογιστικής και επικοινωνιακής πολυπλοκότητας για τους επαληθευτές και τους *mix-servers.*

4.4.2.2 Ομομορφικές Συναρτήσεις Κρυπτογράφισης

Η βασική ιδέα των σχημάτων αυτής της κατηγορίας στηρίζεται στη χρήση εγγράψιμων ψηφοδελτίων *(write-in-ballots).* Στα εγγράψιμα ψηφοδέλτια ο ψηφοφόρος μπορεί να εισάγει ένα μήνυμα της επιλογής του, δικαίωμα που παρέχεται σε νομοθεσίες αρκετών κρατών. Συγκεκριμένα, ο κάθε ψηφοφόρος λαμβάνει ένα κρυπτογραφημένο διαπιστευτήριο ψηφοφορίας *(voting credential)* από τις εκλογικές αρχές, το οποίο συνδυάζει μαζί με την ψήφο του, αξιοποιώντας τις ομομορφικές ιδιότητες ορισμένων πιθανοτικών κρυπτοσυστημάτων. Κάθε διαπιστευτήριο αποτελείται από τυχαίους

αριθμούς, έναν από κάθε εκλογική αρχή και λαμβάνεται υπόψη κατά τη φάση της καταμέτρησης, ώστε να εξασφαλίζεται η ορθότητα του αποτελέσματος.

4.4.2.2.1 Μερικά Ομομορφικά Σχήματα Ψηφοφορίας

Το πρωτόκολλο του *Acquisti* που εξετάζεται παρακάτω εξασφαλίζει ιδιωτικότητα, καθολική επαληθευσιμότητα, μη αναγκαιότητα έκδοσης και προστασία από εξαναγκασμό χωρίς τη χρήση διαδικαστικών περιορισμών ή φυσικών υποθέσεων (όπως χρήση *smart cards*, κανάλια επικοινωνίας που δεν παρακολουθούνται, κιόσκια ψηφοφορίας, τυχαιοποιητές κ.λπ.). Η λύση που προτείνουν οι *Juels και Jakobsson* βασίζεται επίσης σε ένα σύνολο αρχών που εκδίδουν διαπιστευτήρια. Η διαφορά είναι ότι το πρωτόκολλο των *Juels και Jakobsson* χρησιμοποιεί τη μέθοδο αναδιάταξης και απόκρυψης των διαπιστευτηρίων, ενώ το πρωτόκολλο του *Acquisti* αξιοποιεί αναδιάταξη και ομομορφικές ιδιότητες. Το πρωτόκολλο του *Chaum* ικανοποιεί αρκετές από τις απαιτήσεις, αλλά στηρίζεται σε συγκεκριμένη φυσική υλοποίηση. Οι χρήστες ψηφίζουν σε ειδικό κιόσκι και παραλαμβάνουν έντυπη απόδειξη, κρυπτογραφημένη με χρήση οπτικής κρυπτογραφίας. Στην εργασία προτείνεται ένα σχήμα που επιτρέπει εγγράψιμα ψηφοδέλτια και βασίζεται σε μια νέα τεχνική για την αναδιάταξη, η οποία είναι πιο αποδοτική από τα απλά *mix-nets* (πρωτόκολλο *shuffle mix-net)*. Για να διασφαλιστεί όμως η μη αναγκαιότητα έκδοσης απόδειξης απαιτούνται πάλι διαδικαστικοί περιορισμοί (χρήση εκλογικών θαλάμων με συνεχή επιτήρηση).

Στην εργασία προτείνεται μια νέα προσέγγιση με χρήση ψηφοδελτίων-διανυσμάτων *(vector ballots),* η οποία επιτρέπει τη χρήση ομομορφικών συναρτήσεων κρυπτογράφησης και εγγράψιμων ψηφοδελτίων (προαιρετικά). Τα ψηφοδέλτια διανύσματα έχουν τρεις συντεταγμένες: **α)** το κρυπτογράφημα, που περιλαμβάνει μια από τις επιτρεπόμενες επιλογές ψήφου, **β)** ένα κρυπτογράφημα-σημαία *(flag)* που δίνει κρυπτογραφημένη την πληροφορία εάν ο ψηφοφόρος επιλέγει εγγράψιμο ψηφοδέλτιο ή όχι, και **γ)** την εγγράψιμη επιλογή. Για την ικανοποίηση όμως της ιδιότητας της μη αναγκαιότητας έκδοσης απόδειξης απαιτείται χρήση τυχαιοποιητή. Η εκλογική αρχή που συντονίζει τη διαδικασία της ψηφοφορίας αποτελείται από ανεξάρτητους εξυπηρετητές (επιμέρους αρχές) που επιβλέπουν την εγγραφή και την καταμέτρηση των ψήφων μέσω ενός πίνακα ανακοινώσεων.

Καθεμιά από τις αρχές αυτές δημιουργεί μια σειρά τυχαίων αριθμών (έναν για κάθε νόμιμο ψηφοφόρο), οι οποίοι αποτελούν μερίδια του διαπιστευτηρίου ψηφοφορίας που ο χρήστης πρέπει να συνδυάσει με την ψήφο του, ώστε αυτή να ληφθεί υπόψη. Κάθε αρχή δημοσιεύει στον πίνακα ανακοινώσεων αντίγραφα των μεριδίων των διαπιστευτηρίων που δημιουργεί, κρυπτογραφημένα με ένα ζευγάρι δημοσίων παραμέτρων *Paillier*, ενώ η υλοποίηση με *ElGamal* κρυπτογράφηση είναι επίσης δυνατή. Επίσης, κάθε αρχή στέλνει σε κάθε ψηφοφόρο τα ίδια μερίδια διαπιστευτηρίων, κρυπτογραφημένα με ένα διαφορετικό ζευγάρι δημοσίων παραμέτρων *Paillier*, επισυνάπτοντας στο μήνυμά της μια καθορισμένη απόδειξη της ισοδυναμίας μεταξύ του κρυπτογραφημένου μεριδίου που υπάρχει στον πίνακα και αυτού που έχει λάβει ο ψηφοφόρος.

Κάθε αρχή δημιουργεί επίσης τυχαίους αριθμούς που χρησιμεύουν ως μερίδια για τα επιτρεπόμενα ψηφοδέλτια (π.χ. ναι/όχι, πολλαπλών υποψηφίων, 1 από *t* επιλογές κ.λπ.). Και αυτά τα μερίδια κρυπτογραφούνται με τα δύο διαφορετικά ζευγάρια δημόσιων παραμέτρων *Paillier*. Και τα δύο σύνολα κρυπτογραφημένων μεριδίων των επιτρεπτών ψηφοδελτίων δημοσιεύονται στον πίνακα ανακοινώσεων μαζί με αποδείξεις μηδενικής γνώσης και υπογράφονται από την αρχή (εγγράψιμα ψηφοδέλτια).

Χρησιμοποιώντας κρυπτογράφηση *Paillier*, ο ψηφοφόρος πολλαπλασιάζει τα μερίδια που έχει λάβει από κάθε αρχή με τα κρυπτογραφημένα μερίδια του ψηφοδελτίου που έχει επιλέξει από τον πίνακα. Λόγω των ομομορφικών ιδιοτήτων των κρυπτοσυστημάτων *Paillier*, το κρυπτογράφημα που προκύπτει περιλαμβάνει το άθροισμα αυτών των μεριδίων (που αποτελεί το διαπιστευτήριο ψηφοφορίας του ψηφοφόρου) και των μεριδίων των ψηφοδελτίων (που αποτελεί την ψήφο του). Αυτό το κρυπτογράφημα αποστέλλεται στον πίνακα ανακοινώσεων.

Μετά τη λήξη της προθεσμίας ψήφου, όλα τα κρυπτογραφήματα που έχουν τοποθετηθεί από τους νόμιμους ψηφοφόρους αναδιατάσσονται από τις αρχές, χρησιμοποιώντας *mix-nets* του *Chaum*. Τα μερίδια των διαπιστευτηρίων που έχουν τοποθετηθεί από τις αρχές επίσης συνδυάζονται για κάθε ψηφοφόρο και μετά αναδιατάσσονται.

Έτσι, οι αρχές έχουν αποκτήσει δύο λίστες: **α)** μια λίστα με τα κρυπτογραφημένα και αναδιατεταγμένα διαπιστευτήρια που οι ίδιες είχαν δημοσιεύσει στον πίνακα ανακοινώσεων και **β)** μια λίστα από κρυπτογραφημένα και αναδιατεταγμένα αθροίσματα διαπιστευτηρίων και ψηφοδελτίων, που τοποθετήθηκαν στον πίνακα από τους ψηφοφόρους. Οι δύο λίστες έχουν κρυπτογραφηθεί με διαφορετικές δημόσιες παραμέτρους *Paillier*. Χρησιμοποιώντας κρυπτογραφία κατωφλίου *(threshold cryptography)* για τα αντίστοιχα ιδιωτικά κλειδιά, οι αρχές αποκρυπτογραφούν τα στοιχεία κάθε λίστας και τα συγκρίνουν μέσω ενός απλού αλγόριθμου αναζήτησης. Για κάθε διαπιστευτήριο που γνωρίζουν ότι είναι έγκυρο, αναζητούν ποιό μήνυμα (εάν υπάρχει) που τοποθετήθηκε από έναν ψηφοφόρο περιέχει αυτό το διαπιστευτήριο και έχει συνδυαστεί με επιτρεπτή ψήφο.

4.4.3 Μελέτη Περίπτωσης: Το Ολοκληρωμένο Σύστημα Ηλεκτρονικής Ψηφοφορίας ΠΝΥΚΑ

Θα παρουσιάσουμε συνοπτικά τις βασικές αρχές σχεδίασης, υλοποίησης και αξιολόγησης του διαδικτυακού συστήματος ηλεκτρονικής ψηφοφορίας ΠΝΥΚΑ που αναπτύχθηκε από το Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών (ΕΑ ΙΤΥ) σε συνεργασία με την εταιρεία *EXPERTNET Προηγμένες Εφαρμογές ΑΕ* στο πλαίσιο ενός ερευνητικού προγράμματος. Στόχος της παρουσίασης αυτής είναι να δείξουμε πως τα όσα αναφέρθηκαν σε σχέση με την προστασία της ιδιωτικότητας του ψηφοφόρου υλοποιήθηκαν στην πράξη.

Το σύστημα ΠΝΥΚΑ υποστηρίζει όλα τα στάδια μιας ηλεκτρονικής ψηφοφορίας όπως εγγραφή/πιστοποίηση, υποβολή ψήφου, καταμέτρηση αποτελεσμάτων και επαλήθευση. Για τη μεγιστοποίηση του βαθμού προστασίας της ιδιωτικότητας του ψηφοφόρου, το σύστημα ενσωματώνει πολλές τεχνολογικές καινοτομίες, όπως πλήρως κατανεμημένη αρχιτεκτονική, ομομορφική κρυπτογράφηση κατωφλίου, συσκευές υλικού για την αποθήκευση των κλειδιών κ.λπ. Και έχει αναπτυχθεί εξ ολοκλήρου με εργαλεία ανοικτού κώδικα έτσι ώστε να διευκολύνεται η επαληθευσιμότητά του. Μπορεί επίσης να παραμετροποιηθεί για να υποστηρίξει διαφορετικές μορφές ψηφοφορίας, από απλές διαδικασίες έκφρασης γνώμης μέχρι εκλογές και δημοψηφίσματα μεγάλης κλίμακας.

Ο σχεδιασμός του συστήματος έγινε με τη χρήση τυπικών μεθόδων ανάλυσης και διαχείρισης κινδύνων όπως το πλαίσιο *CORAS*, δίνοντας έτσι έμφαση στην προσέλκυση της δημόσιας εμπιστοσύνης. Το σύστημα εφαρμόστηκε με επιτυχία σε μια δοκιμαστική ηλεκτρονική ψηφοφορία μεταξύ των μελών του ΤΕΕ Δυτικής Ελλάδας ενώ συμμετείχε παράλληλα στο διαγωνισμό *e-voting* που διοργάνωσε το *Competence Center for Electronic Voting and Participation.*

4.4.3.1 Μεθοδολογία Σχεδίασης

Η έννοια της εμπιστοσύνης είναι ιδιαίτερα σημαντική σε σχέση με τον τρόπο που οι πολίτες – χρήστες αντιμετωπίζουν ένα πληροφοριακό σύστημα. Η γενικότερη έλλειψη εμπιστοσύνης στις νέες τεχνολογίες και στη χρήση του διαδικτύου έχει αρνητικές επιπτώσεις σε οποιαδήποτε προσπάθεια μετάβασης από τις παραδοσιακές μορφές ψηφοφορίας σε ηλεκτρονικά συστήματα, δεδομένου ότι η ψηφοφορία αποτελεί μια ιδιαίτερα ευαίσθητη διαδικασία.

Βασική λοιπόν αρχή στην ανάπτυξη ενός πετυχημένου συστήματος ηλεκτρονικής ψηφοφορίας είναι η προσέλκυση της δημόσιας εμπιστοσύνης. Για να επιτευχθεί αυτό απαιτείται μια συστηματική προσέγγιση που καλύπτει όλα τα στάδια σχεδίασης, υλοποίησης και ελέγχου του συστήματος.

Στο σύστημα ΠΝΥΚΑ, η προσέγγιση αυτή περιλάμβανε δύο βασικές συνιστώσες:

I. Την υιοθέτηση μιας αρχιτεκτονικής οικοδόμησης εμπιστοσύνης

II. Την εφαρμογή μιας τυπικής μεθοδολογίας ανάλυσης και διαχείρισης κινδύνων.

4.4.3.1.1 Αρχιτεκτονική Εμπιστοσύνης

Η αρχιτεκτονική εμπιστοσύνης έχει προταθεί από το ΕΑ ITY ως μια γενική μεθοδολογία οικοδόμησης εμπιστοσύνης σε ένα σύστημα όπου η ασφάλεια είναι κρίσιμη, έτσι ώστε να:

1. Αντιμετωπίζει το σύστημα ως μια ολοκληρωμένη εφαρμογή λογισμικού/υλικού και εφαρμόζοντας μεθόδους που εξασφαλίζουν την ορθότητα της λειτουργίας σε όλες τις φάσεις του κύκλου ζωής της.
2. Αναλύει το σύστημα σε διάφορα επίπεδα αρχιτεκτονικής τα οποία περικλείουν το περιβάλλον του, τους χρήστες, τους διαχειριστές και γενικά όλα τα τεχνικά και κοινωνικά ζητήματα που έχουν κάποια αλληλεπίδραση με αυτό.

Η βασική ιδέα είναι κατάτμηση της διαδικασίας σχεδίασης σε ***διακριτά στρώματα εμπιστοσύνης*** *(layers of trust).* Μια ποικιλία από εργαλεία και τεχνικές μπορεί να εφαρμοστεί σε καθένα από τα στρώματα για να εξασφαλιστεί ότι κάθε στρώμα ικανοποιεί τις απαιτήσεις και τις προδιαγραφές εμπιστοσύνης. Στο ***σχήμα 34*** φαίνονται τα στρώματα της αρχιτεκτονικής.

Ο ρόλος των στρωμάτων είναι ο ακόλουθος:

1. ***Επιστημονική πληρότητα (scientific soundness):*** Όλα τα επιμέρους τμήματα του συστήματος πρέπει να κατέχουν κάποιο τύπο διαβεβαίωσης της ασφάλειας και να είναι ευρέως αποδεκτά στην επιστημονική κοινότητα.
2. ***Πληρότητα υλοποίησης (implementation soundness):*** Θα πρέπει να υιοθετηθεί μια μεθοδολογία που θα οδηγεί στην επαλήθευση της υλοποίησης των ξεχωριστών τμημάτων του συστήματος ως συνόλου. Επιπρόσθετα, μια τέτοια μεθοδολογία επαλήθευσης θα πρέπει να εφαρμόζεται περιοδικά στο σύστημα.

   Το στρώμα αυτό αντιμετωπίστηκε με την υιοθέτηση και την εφαρμογή της μεθοδολογίας ανάλυσης κινδύνων *CORAS* σε όλα τα στάδια σχεδιασμού και ανάπτυξης του συστήματος.
3. ***Πληρότητα εσωτερικών λειτουργιών (internal operation soundness):*** Ο σχεδιασμός και η υλοποίηση πρέπει να προσφέρουν υψηλή διαθεσιμότητα και

ανοχή σε σφάλματα και να υποστηρίζουν διαδικασίες αυτοπαρακολούθησης, αυτοεξέτασης και αυτοανάκαμψης από βλάβες.

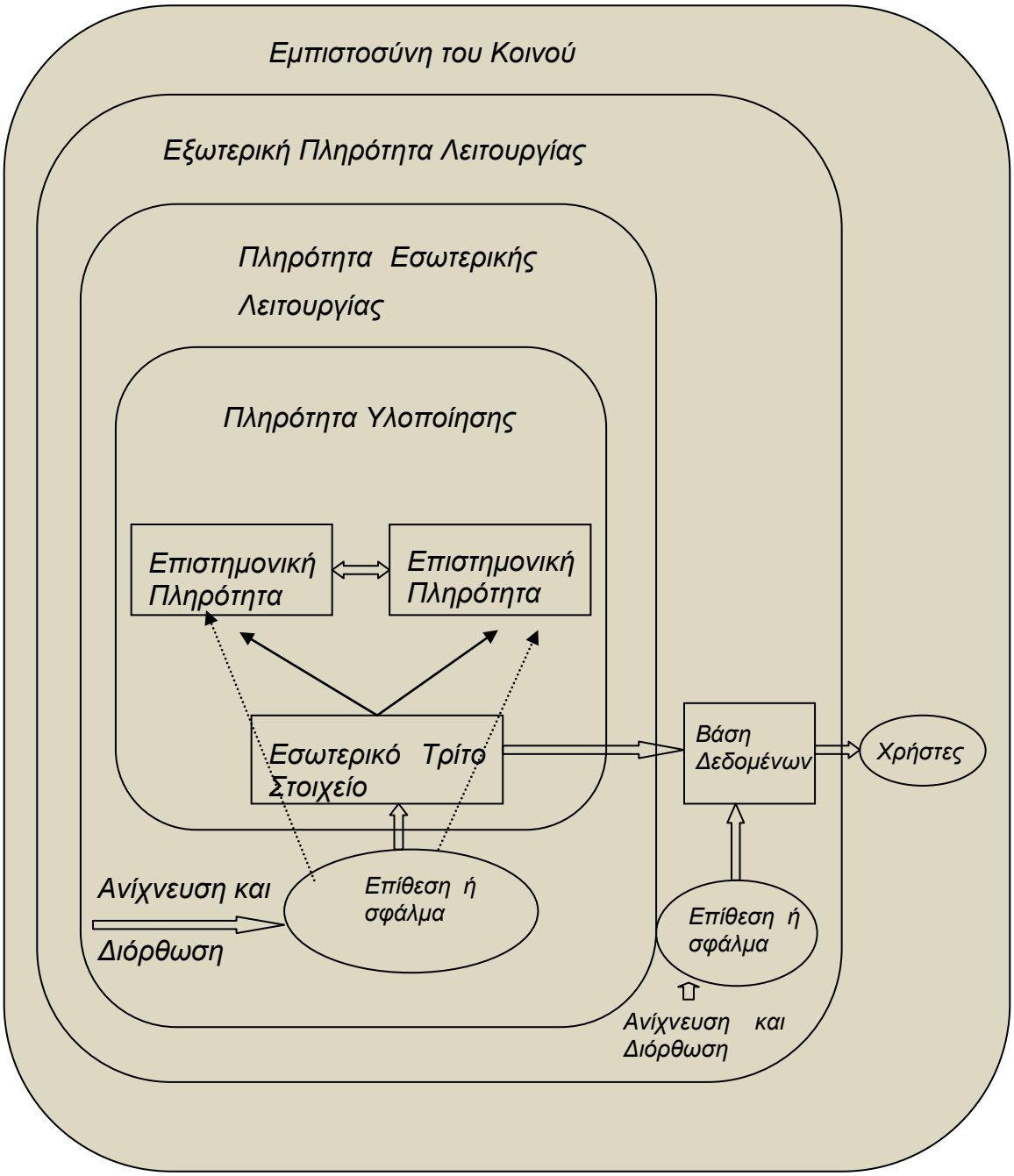
Το κρυπτογραφικό πρωτόκολλο περιλαμβάνει δικλίδες ασφαλείας για λάθη από την πλευρά του χρήστη καθώς και από την πλευρά του συστήματος. Η χρήση δημόσιου πίνακα ανακοινώσεων (*bulletin board,* π.χ. μια δημόσια προσβάσιμη ιστοσελίδα) καθιστά δυνατή την επαλήθευση των αποθηκευμένων δεδομένων (ψήφων) από το κοινό. Όσον αφορά στην έμπιστη Τρίτη Αρχή, αυτή είναι συνδυασμός δύο βασικών οντοτήτων του πρωτόκολλου που είναι η εκλογική αρχή (ΕΑ) και οι κάτοχοι των κλειδιών κρυπτογράφησης/αποκρυπτογράφησης (*keyholders*).

4. ***Πληρότητα λειτουργιών που είναι ορατές εξωτερικά (externally visible operational soundness):*** Θα πρέπει να είναι αδύνατο για κάποιον έξω από το σύστημα να αλλοιώσει την κανονική λειτουργία του συστήματος. Αν πραγματοποιηθεί μια τέτοια απειλή, θα πρέπει να είναι γρήγορα ανιχνεύσιμη.

   Στο στρώμα αυτό έχουμε τη χρήση του δημοσίου πίνακα ανακοινώσεων για την επαλήθευση των δεδομένων, ενώ όλη η λειτουργία του συστήματος επιβλέπεται από ειδικό σύστημα ανίχνευσης και αντιμετώπισης εισβολών.

5. ***Η διαδικασία να πειστεί το κοινό (κοινωνική πλευρά εμπιστοσύνης):*** Για την επιτυχή εφαρμογή του συστήματος σε μεγάλη κλίμακα είναι πολύ σημαντικό το σύστημα να έχει την εμπιστοσύνη του κοινού, όσον αφορά στην προστασία της ιδιωτικότητάς του.

Αυτή η εμπιστοσύνη μπορεί γενικά να ενισχυθεί αν ο οργανισμός που διαχειρίζεται το σύστημα επιτρέψει τη διάθεση των λεπτομερειών σχεδιασμού και λειτουργίας του σε δημόσιο διάλογο, ενισχύοντας με τον τρόπο αυτό τη διαφάνεια και την αξιοπιστία του. Παράλληλα, θα πρέπει να υπάρξει και μια οργανωμένη προσπάθεια εισαγωγής και χρήσης του συστήματος σε περιορισμένους κύκλους χρηστών στην αρχή και σε εθελοντική βάση με στόχο τη δημιουργία της κρίσιμης μάζας που μπορεί να χρησιμοποιήσει το σύστημα για ψηφοφορίες μεγαλύτερης κλίμακας πείθοντας ταυτόχρονα και άλλους για την ορθότητα του συστήματος.



Σχήμα 34: Αρχιτεκτονική εμπιστοσύνης ενός πληροφοριακού συστήματος

4.4.3.1.2 Ανάλυση και Διαχείριση Κινδύνων

Κατά το σχεδιασμό του συστήματος εφαρμόστηκε η *CORAS* που αποτελεί μια δομημένη μεθοδολογία για τη διαχείριση της ασφάλειας σε ένα σύστημα από τα αρχικά στάδια σχεδιασμού. Αναπτύχθηκε στο πλαίσιο ενός ευρωπαϊκού ερευνητικού *IST* έργου *(IST-2000-25031)* στο οποίο συμμετείχε το ΕΑ-ΙΤΥ, βρίσκεται ήδη στη δεύτερη έκδοσή του και διατίθεται δωρεάν προς χρήση.

Για την αρχικοποίηση της εφαρμογής *CORAS* στο σύστημα ΠΝΥΚΑ επιλέχθηκε η διενέργεια μιας προκαταρτικής μελέτης *HAZOP (Hazard and Operability Study)* για την αποτίμηση της ασφάλειας της αρχιτεκτονικής του συστήματος. Από τη μελέτη *HAZOP* προέκυψε ένα σύνολο από πίνακες που δείχνουν εποπτικά τις κρίσιμες οντότητες του συστήματος και κάποια σενάρια απειλών που θα πρέπει να ληφθούν υπόψη και να αντιμετωπιστούν κατάλληλα. Οι οντότητες και οι απειλές αυτές μπορούν στη συνέχεια να εισαχθούν σε αναλύσεις *Fault Tree Analysis (FTA)* και *Failure Mode Effects Criticality Analysis (FMECA)*, που έπονται στα βήματα εφαρμογής της *CORAS*, και να μελετηθούν διεξοδικά.

Στη συνέχεια η *CORAS* εφαρμόστηκε στο κρυπτογραφικό πρωτόκολλο που είναι και το πλέον κρίσιμο από πλευράς ασφάλειας. Ακολουθήθηκαν τα παρακάτω βήματα:

1. Προσδιορισμός Περιβάλλοντος *(Identify context)*
2. Προσδιορισμός Επικινδυνότητας *(Identify risks)*
3. Ανάλυση Επικινδυνότητας *(Analyze risks)*
4. Αξιολόγηση Επικινδυνότητας *(Evaluate risks)*
5. Αντιμετώπιση Κινδύνων *(Threat risks)*

Η ανάλυση επικινδυνότητας του συστήματος έγινε με τη μορφή συναντήσεων εργασίας *(working sessions).* Στις συναντήσεις αυτές υπήρχε ανταλλαγή απόψεων μεταξύ των διαφόρων ειδικών (μηχανικοί ασφάλειας, προγραμματιστές, μηχανικοί δικτύων κ.λπ.), επιτρέποντας έτσι την κάλυψη όλων των πλευρών του συστήματος. Το αποτέλεσμα από την εφαρμογή της *CORAS* ήταν ένα σύνολο *UML (Unified Modeling Language)* μοντέλων (διαγράμματα δραστηριοτήτων, διαγράμματα χρονικών ακολουθιών, *fault tree* διαγράμματα κ.λπ.) και εκτεταμένη τεκμηρίωση για τις απειλές και τα μέτρα προστασίας του συστήματος. Η τεκμηρίωση αυτή θα μπορεί να χρησιμοποιηθεί, επιπρόσθετα και για την υποστήριξη του ελέγχου του συστήματος από κάθε ενδιαφερόμενο.

4.4.3.2 Αρχιτεκτονική Συστήματος

4.4.3.2.1 Οντότητες Συστήματος

Το σύστημα απαρτίζεται από ένα σύνολο διακριτών οντοτήτων *(agents, actors)* οι οποίες εμπλέκονται με διάφορους τρόπους στα επιμέρους στάδια μιας ψηφοφορίας, όπως εγγραφή, πιστοποίηση, υποβολή ψήφου, επαλήθευση, καταμέτρηση και ανακοίνωση αποτελέσματος.

Οι οντότητες αυτές είναι:

- ***Υποψήφιοι (Candidates):*** Είναι οι υποψήφιοι της εκλογικής διαδικασίας, που μπορεί να είναι 1 (δημοψήφισμα Ναι/Όχι) έως n.
- ***Ψηφοφόροι (Voters):*** Είναι οι ψηφοφόροι που συμμετέχουν στη διαδικασία.
- ***Εκλογικές Αρχές (Election Authorities):*** Είναι οι Αρχές που έχουν την ευθύνη για τη διεξαγωγή της ψηφοφορίας.

Κάθε Εκλογική Αρχή επιτελεί πολλές λειτουργίες και αποτελείται από επιμέρους οντότητες οι οποίες αλληλοελέγχονται ώστε να αποτρέπεται η αλλοίωση του αποτελέσματος της ψηφοφορίας.

Έτσι η Εκλογική Αρχή περιλαμβάνει:

- ***Γραμματεία (Registar):*** Δημιουργεί και διαχειρίζεται τον εκλογικό κατάλογο των νόμιμων ψηφοφόρων και τις εκλογικές περιοχές.
- ***Διαχειριστές (Administrators):*** Είναι υπεύθυνοι για την αρχικοποίηση του συστήματος και τον καθορισμό των σχετικών παραμέτρων.
- ***Κάτοχοι Κλειδιών (Keyholder*s):** Είναι οι κάτοχοι των μερών των κλειδιών κρυπτογράφησης, όπως ορίζονται από το χρησιμοποιούμενο πρωτόκολλο ψηφοφορίας.
- ***Διαχειριστές Ψήφων (Vote Managers):*** Είναι υπεύθυνοι για την ασφαλή επικοινωνία μεταξύ ψηφοφόρου και Εκλογικής Αρχής (κρυπτογράφηση, ψηφιακή υπογραφή, έλεγχοι κ.λπ.) και για την αποθήκευση των ψήφων στη βάση δεδομένων του συστήματος.
- ***Καταμετρητές (Talliers)****:* Αναλαμβάνουν την καταμέτρηση των ψήφων και την εξαγωγή του τελικού αποτελέσματος.
- ***Καταγραφείς (Loggers):*** Καθ' όλη τη διάρκεια της διαδικασίας, καταγράφουν τα στοιχεία που απαιτούνται ώστε να μπορούν να πραγματοποιηθούν ο εκ των υστέρων έλεγχος και η επαλήθευση της διαδικασίας.
- ***Χειριστές των Πινάκων Ανακοινώσεων (Bulletin Boards – BB)****:* Οι οντότητες αυτές αναλαμβάνουν την ανάρτηση των απαιτούμενων πληροφοριών σε δημόσιους πίνακες ανακοινώσεων, ώστε να είναι προσβάσιμες από κάθε ενδιαφερόμενο.
- ***Ελεγκτές (Auditors):*** Ελέγχουν την ορθότητα του τελικού αποτελέσματος και τη συμμόρφωση της διαδικασίας με τους ισχύοντες κανόνες. Μπορεί να είναι εσωτερικοί υπάλληλοι ή εξωτερικοί ελεγκτές μιας τρίτης Ελεγκτικής Αρχής ή μιας Αρχής Πιστοποίησης.
- ***Επαληθευτές (Verifiers):*** Πρόκειται για εξωτερικούς ελεγκτές οι οποίοι έχουν τη δικαιοδοσία να πιστοποιήσουν την ορθότητα του αποτελέσματος της ψηφοφορίας και την ακεραιότητα της συνολικής διαδικασίας.
- ***Εχθροί (Adversaries) και Εξαναγκαστές (Coersers):*** Πρόκειται για κακόβουλες οντότητες που έχουν στόχο να πλήξουν τη διαδικασία της ψηφοφορίας.

4.4.3.2.2 Αρχιτεκτονική

Με βάση τα όσα αναφέρθηκαν παραπάνω, η υψηλού επιπέδου αρχιτεκτονική του συστήματος μπορεί να περιγραφεί ως εξής:

Οι ψηφοφόροι συνδέονται στο σύστημα ηλεκτρονικής ψηφοφορίας μέσω του διαδικτύου, χρησιμοποιώντας τον προσωπικό υπολογιστή τους ή κάποιο άλλο σταθερό σημείο πρόσβασης (π.χ. *voting kiosk).* Η σύνδεση γίνεται μέσω του *SSL* πρωτοκόλλου. Καθεμιά από τις τοπικές εκλογικές αρχές ΕΑ, αναλαμβάνει την εξυπηρέτηση των ψηφοφόρων μιας συγκεκριμένης εκλογικής περιφέρειας. Μεταξύ των ΕΑ αποκαθίστανται ένα ιδιωτικό εικονικό δίκτυο *(Virtual Private Network, VPN)* και όλα τα δεδομένα που ανταλλάσσονται πάνω από αυτό είναι ισχυρά κρυπτογραφημένα, όπως υπαγορεύει το πρωτόκολλο ψηφοφορίας. Η διαχείριση κάθε *VPN* γίνεται από την αντίστοιχη τοπική ΕΑ. Για τη σύνδεση ενός ψηφοφόρου σε αυτό το *VPN* πραγματοποιείται μια σύντομη ανταλλαγή κατάλληλων μηνυμάτων μεταξύ της εφαρμογής που εκτελείται στο σταθμό του ψηφοφόρου *(client module)* και της εφαρμογής εξυπηρέτησης ψηφοφόρων που

εκτελείται στον εξυπηρετητή της τοπικής ΕΑ. Η πιστοποίηση της ταυτότητας του ψηφοφόρου στο σύστημα μπορεί να γίνεται με τις συνήθεις μεθόδους ταυτοποίησης (π.χ. *login* και *password*, ή με χρήση *PKI*).

Η αρχιτεκτονική της κεντρικής ΕΑ και εκείνη των τοπικών ΕΑ είναι παρόμοιες με την εξής διαφοροποίηση. Η κεντρική ΕΑ δεν συναλλάσσεται απευθείας με τους ψηφοφόρους αλλά μόνο με τις επιμέρους ΕΑ. Η κεντρική ΕΑ διατηρεί τις βασικές ρυθμίσεις της ψηφοφορίας, εκδίδει ψηφιακά πιστοποιητικά και στέλνει μηνύματα συγχρονισμού και ελέγχου στις επιμέρους ΕΑ. Επιπρόσθετα, λαμβάνει από τις τοπικές ΕΑ τα τοπικά αποτελέσματα των εκλογών μαζί με την απαραίτητη πληροφορία αποκρυπτογράφησής τους και προβαίνει στην επαλήθευσή τους και στον υπολογισμό του τελικού αποτελέσματος.

Σε κάθε τοπική ΕΑ βρίσκονται συγκεντρωμένες πολλές επιμέρους οντότητες του συστήματος. Οι οντότητες αυτές τρέχουν σε εξυπηρετητές οι οποίοι είναι συνδεδεμένοι σε ένα μικρό τοπικό δίκτυο που προστατεύεται από το διαδίκτυο με κάποιο *firewall* και ένα σύστημα ανίχνευσης επιθέσεων (*IDS*). Επιπλέον, υπάρχει πρόβλεψη για τη χρησιμοποίηση τεχνικών που εξασφαλίζουν την υψηλή διαθεσιμότητα *(high availability)* των εξυπηρετητών στις ΕΑ, όπως *clustering* και *failover*, ενώ επιπρόσθετα προβλέπονται και μέτρα τήρησης αντιγράφων ασφάλειας.

4.4.3.2.3 Περιβάλλον Ανάπτυξης

Στην ανάπτυξη του συστήματος χρησιμοποιήθηκαν παντού εργαλεία ανοικτού κώδικα ώστε να είναι περισσότερο διάφανη η λειτουργία του συστήματος.

Ως κύρια γλώσσα προγραμματισμού επιλέχθηκε η αντικειμενοστραφής γλώσσα *Java*. Χρησιμοποιήθηκε επίσης το περιβάλλον ανάπτυξης *NetBeans 5.5*. Για την υλοποίηση των επιμέρους *modules* κρυπτογραφικού πρωτοκόλλου επιλέχθηκε η βιβλιοθήκη κρυπτογραφικών εργαλείων και αλγορίθμων *Bouncy Castle της Java.* Η διαχείριση των κλάσεων και των συναρτήσεων που παρέχει η βιβλιοθήκη γίνεται από το *NetBeans*. Για τη βάση δεδομένων επιλέχθηκε η *PostgreSQL*. Κάθε βάση δεδομένων σε μια τοπική εκλογική αρχή έχει ακριβώς την ίδια δομή με αυτή της κεντρικής και αποθηκεύει μόνο τα στοιχεία για τους ψηφοφόρους που αυτή εξυπηρετεί.

Ο εξυπηρετητής δικτύου *(web server)* αναλαμβάνει να εξυπηρετήσει το διαδικτυακό ιστότοπο της εκλογικής αρχής και ο εξυπηρετητής εφαρμογών *(application server)* επεξεργάζεται τις αιτήσεις που δέχεται από τον εξυπηρετητή διαδικτύου. Και οι δύο αυτοί εξυπηρετητές βρίσκονται στο επίπεδο εφαρμογών *(application tier)* της εκλογικής αρχής. Το λογισμικό που επιλέχθηκε για τους εξυπηρετητές αυτούς είναι ο *Apache Tomcat.* Όλη η υλοποίηση αξιοποιεί το λειτουργικό σύστημα *Linux Ubuntu.*

4.4.3.2.4 Εξωτερικά Συστήματα Λογισμικού

Στο σύστημα ολοκληρώνονται κι ένα σύνολο από εξωτερικές τεχνολογίες υλικού και λογισμικού, όπως περιγράφεται στη συνέχεια.

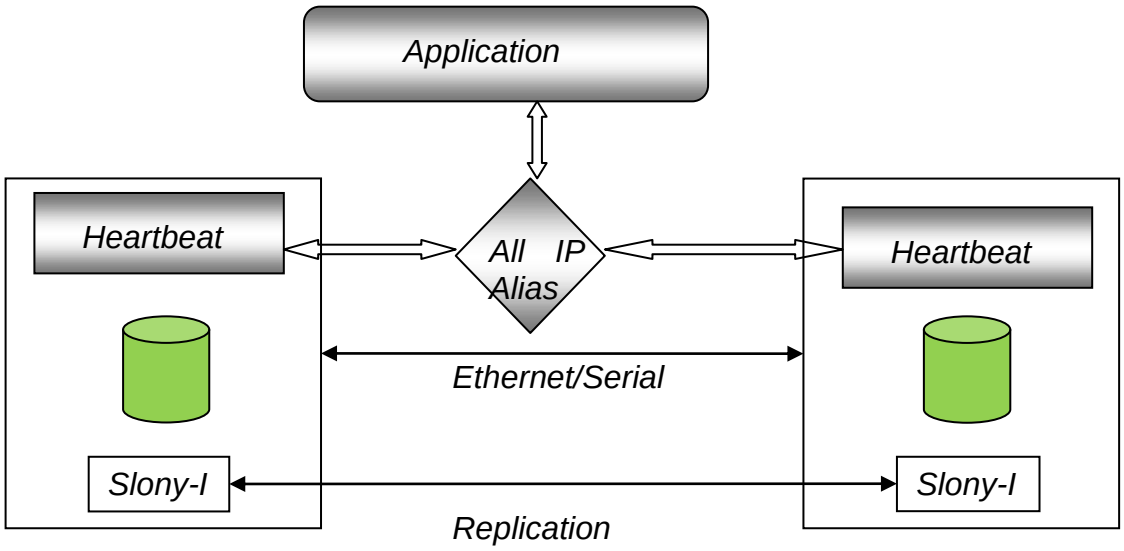
Για την εγκατάσταση ασφαλών *VPN* συνδέσμων μεταξύ των τοπικών εκλογικών αρχών με την κεντρική επιλέχθηκε το εργαλείο ανοικτού κώδικα *OpenVPN* το οποίο βασίζεται στο πρωτόκολλο *SSL/TLS*. Ακολουθεί το μοντέλο πελάτη-εξυπηρετητή και οι συνδέσεις που αποκαθίστανται για τα ασφαλή κανάλια *(secure tunnels)* είναι *UDP* συνδέσεις για λόγους ευελιξίας και ταχύτητας.

Η *PKI* υποδομή που χρησιμοποιείται είναι ιεραρχική, διαχωρίζεται δηλαδή σε διαφορετικά επίπεδα εμπιστοσύνης τα οποία οργανώνονται με τη μορφή δένδρου. Για

το σκοπό αυτό αξιοποιείται το εργαλείο ανοικτού κώδικα *OpenCA*. Για την πιστοποίησή του ο χρήστης υποβάλλει αίτηση για τη λήψη πιστοποιητικού από την *OpenCA*. Στη συνέχεια μπορεί να προσπελάσει το *web interface* της εκλογικής αρχής στην οποία ανήκει και να καταθέσει, μέσω *SSL* την ψήφο του.

Για την περιμετρική ασφάλεια, χρησιμοποιείται το σύστημα ανίχνευσης επιθέσεων (*IDS*) *HELENA*, το οποίο αναπτύχθηκε από το ΕΑ ΙΤΥ. Πρόκειται για ένα κατανεμημένο σύστημα εντοπισμού εισβολών το οποίο μπορεί να προσαρμοστεί ως εξωτερική εφαρμογή σε οποιαδήποτε δικτυακή εφαρμογή.

Για το σύστημά μας είναι επιθυμητό να υπάρχει σε κάθε εκλογική αρχή ένας εξυπηρετητής (ενεργή ΕΑ) που να εξυπηρετεί τους ψηφοφόρους και ένας εξυπηρετητής (εφεδρική ΕΑ) που να βρίσκεται σε αναμονή για να αναλάβει την εξυπηρέτηση των ψηφοφόρων σε περίπτωση που τεθεί εκτός λειτουργίας η ενεργή ΕΑ (επίτευξη υψηλής διαθεσιμότητας και αντοχής σε σφάλματα). Για να επιτευχθεί αυτό έγινε χρήση του εργαλείου *HeartBeat* και εφαρμόστηκε το σενάριο που προτείνει το ερευνητικό έργο ανοικτού λογισμικού *UltraMonkey.* Για να αποτελέσει η βάση δεδομένων της εφεδρικής ΕΑ ακριβές και ενημερωμένο αντίγραφο της βάσης δεδομένων της ενεργής ΕΑ χρησιμοποιήθηκε το εργαλείο *Slonyl*, ένα ασύγχρονο *master-slave* σύστημα αντιγραφής για την *PostgreSQL* που παρέχει υποστήριξη για *cascading* και για *failover*. Στο παρακάτω ***σχήμα*** φαίνεται μια τυπική υλοποίηση ενός σεναρίου που συνδυάζει τα δύο εργαλεία.



Σχήμα 35: Συνδυασμός των εργαλείων *Heartbeat* και *Slony-I*

Το εργαλείο *Slonyl* χρησιμοποιείται επίσης για την ασύγχρονη αντιγραφή των βάσεων δεδομένων των τοπικών ΕΑ στη βάση της κεντρικής ΕΑ.

Τέλος χρησιμοποιήθηκε ο 8-*bit* μικροελεγκτής *AVR Atmega8* της *ATMEL* μαζί με το αναπτυξιακό σύστημα μικροελεγκτών *AVR STL500/STK501* για την ασφαλή αρχικοποίηση και εκκίνηση της ψηφοφορίας. Η κεντρική εκλογική αρχή δημιουργεί τον

κώδικα εκκίνησης της ψηφοφορίας ο οποίος συμπεριλαμβάνει και τα δεδομένα που απαιτούνται για την πραγματοποίηση της εκκίνησης.

4.4.4 Επίλογος

Τα όσα αναφέραμε καταδεικνύουν τον πολυσύνθετο χαρακτήρα της ηλεκτρονικής ψηφοφορίας καθώς εμπλέκονται σε αυτή πολλά διαφορετικά συστήματα λογισμικού και υλικού, το καθένα με τα δικά του ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας του ψηφοφόρου. Σε πολλά από τα ζητήματα που προκύπτουν καλούνται να δώσουν λύσεις οι ειδικοί της πληροφορικής και της ασφάλειας. Σε άλλα πάλι καλείται το νομικό σύστημα να παράσχει τις απαραίτητες ρυθμίσεις που θα διασφαλίζουν τα δημοκρατικά δικαιώματα. Οι δύο αυτές ομάδες ειδικών μπορούν να δώσουν ισχυρές λύσεις στα ζητήματα που ανακύπτουν στην ηλεκτρονική ψηφοφορία και να τη θωρακίσουν σε μεγάλο βαθμό, απέναντι σε προσπάθειες αμφισβήτησης και διαφθοράς. Σημαντικό ρόλο όμως, έχει τελικά η ίδια η πολιτεία, η οποία είναι ο τελικός αποδέκτης των ευεργετημάτων της ηλεκτρονικής ψηφοφορίας. Η πολιτεία οφείλει να αναλάβει πρωτοβουλία για να συνεργαστεί με τους ειδικούς τεχνολόγους και νομικούς, προσδιορίζοντας το κατάλληλο οργανωτικό και λειτουργικό πλαίσιο για τη βαθμιαία εισαγωγή της ηλεκτρονικής ψηφοφορίας σε διάφορες διαδικασίες έκφρασης γνώμης πολιτών, αξιολογώντας στη συνέχεια τον κοινωνικό/πολιτικό αντίκτυπο από την εφαρμογή της. Εάν δεν γίνει το σημαντικό αυτό βήμα, θα είναι εξαιρετικά δύσκολο να καταστεί η ηλεκτρονική ψηφοφορία αποδεκτή από πλατιές μάζες ψηφοφόρων και τελικά να γίνει μια καθολικά αποδεκτή μέθοδος έκφρασης γνώμης. Οι σημερινές εξελίξεις στο χώρο της τεχνολογίας και της νομοθεσίας για την προστασία της ιδιωτικότητας του πολίτη απέναντι στη χρήση σύγχρονων τεχνολογιών, έχουν πλέον δημιουργήσει ένα αρκετά ώριμο πλαίσιο για να γίνει το βήμα αυτό. **[18]**

4.5 Προστασία της Ιδιωτικότητας στην Ηλεκτρονική Διακυβέρνηση

Η συνεισφορά των νέων τεχνολογιών της πληροφορικής και των επικοινωνιών στον εκσυγχρονισμό και στην αναδιοργάνωση της δημόσιας διοίκησης είναι εξαιρετικά σημαντική, καθώς στις σύγχρονες κοινωνίες όπου είναι αναπόφευκτη η ύπαρξη γραφειοκρατικού μηχανισμού, η λειτουργία της διοίκησης έχει φτάσει στα όριά της, με αποτέλεσμα την παροχή χαμηλής ποιότητας υπηρεσιών στους διοικούμενους. Το γεγονός αυτό αναγνωρίζεται και από την ελληνική πολιτεία, αφού η ανάπτυξη υπηρεσιών ηλεκτρονικής διακυβέρνησης εντάσσεται σε μια σειρά από πολιτικές για την ανάπτυξη υποδομών της κοινωνίας της πληροφορίας, όπως είναι το Επιχειρησιακό Πρόγραμμα για την Κοινωνία της Πληροφορίας και τα σχέδια δράσης «Ψηφιακή Στρατηγική 2006-2013» και «Ψηφιακή Σύγκλιση», αλλά και το επιχειρησιακό πρόγραμμα «Πολιτεία».

Η ηλεκτρονική διακυβέρνηση, ειδικότερα, χρησιμοποιείται ως συνώνυμο για την εισαγωγή των νέων τεχνολογιών στη δημόσια διοίκηση. Συγκεκριμένα, αναφέρεται στις εφαρμογές της σύγχρονης τεχνολογίας της πληροφορικής και των επικοινωνιών για την παροχή υπηρεσιών στους πολίτες και στις επιχειρήσεις από τη δημόσια διοίκηση, κυρίως μέσω του διαδικτύου και του παγκόσμιου ιστού (*web*). Οι εφαρμογές αυτές αφορούν στην παροχή πληροφοριών σχετικά με τις διοικητικές διαδικασίες, όπως και των αναγκαίων αιτήσεων για την έναρξη της διοικητικής διαδικασίας, αλλά και την αυτοματοποιημένη διεκπεραίωση των διαδικασιών αυτών, με την ηλεκτρονική συμπλήρωση και αποστολή αιτήσεων και εγγράφων, την υποστήριξη των συναλλαγών με τη διοίκηση (π.χ. πληρωμή τελών) και τέλος την αυτοματοποιημένη έκδοση διοικητικών αποφάσεων.

Οι υπηρεσίες ηλεκτρονικής διακυβέρνησης εν γένει παρουσιάζουν μια σειρά από θετικά αποτελέσματα, όπως είναι η βελτίωση της ποιότητας των υπηρεσιών του δημόσιου τομέα, η αύξηση της υπευθυνότητας των αρμοδίων υπαλλήλων, η παροχή υπηρεσιών με μεγαλύτερη ακρίβεια και αποτελεσματικότητα, η μείωση διοικητικών εξόδων και χρόνου για την εκτέλεση τυποποιημένων διαδικασιών, η επίτευξη μεγαλύτερης διαφάνειας στην εκτέλεση διαδικασιών και η παροχή ευρύτερης πρόσβασης στις υπηρεσίες λόγω της συνεχούς διαθεσιμότητας του διαδικτύου.

Οι εφαρμογές της ηλεκτρονικής διακυβέρνησης διακρίνονται ανάλογα με τις σχέσεις που αναπτύσσουν μεταξύ των διαφόρων φορέων. Έτσι, έχουμε εφαρμογές που αφορούν στις σχέσεις *μεταξύ* ***φορέων του δημόσιου τομέα*** *(Government-to-Government, G2G),* εφαρμογές που αφορούν στις συναλλαγές ***μεταξύ δημόσιου τομέα και επιχειρήσεων*** *(Government-to-Business, G2B),* όπως είναι οι ηλεκτρονικές δημόσιες προμήθειες, ενώ η κατηγορία της οποίας οι εφαρμογές παρουσιάζουν τη μεγαλύτερη διάδοση είναι αυτή που διέπει τις σχέσεις ***μεταξύ δημοσίου και πολιτών*** *(Government-to-Citizen, G2C)*.

Στη χώρα μας, οι κυριότερες ηλεκτρονικές υπηρεσίες είναι οι φορολογικές ηλεκτρονικές υπηρεσίες της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (**www.taxisnet.gr**, **www.gsis.gov.gr**), οι ηλεκτρονικές υπηρεσίες του ΙΚΑ (**www.ika.gr**) και οι υπηρεσίες των ΚΕΠ, στις οποίες δίνεται πλέον η δυνατότητα πρόσβασης μέσω διαδικτύου (**www.kep.gov.gr**). Ιδίως ο δικτυακός τόπος των ΚΕΠ αποτελεί πύλη για την παροχή διαφόρων ηλεκτρονικών υπηρεσιών και λειτουργεί ως μονοαπευθυντικός χώρος (*one-stop-shop*). Το ελληνικό πλαίσιο παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης ολοκληρώνεται με τη δημιουργία της πύλης «ψηφιακή Ελλάδα». Τέλος, στον τομέα των σχέσεων μεταξύ διοικητικών αρχών (*G2G*), πολύπλευρη υποστήριξη παρέχεται μέσω του έργου «Σύζευξις». Αντικείμενο του έργου αυτού είναι η ανάπτυξη και ο εκσυγχρονισμός της τηλεπικοινωνιακής υποδομής του δημόσιου τομέα, ενώ μέσω του

έργου αυτού υλοποιείται η υποδομή δημόσιου κλειδιού (*PKI*) που καλύπτει το δημόσιο τομέα.

4.5.1 Ζητήματα Προστασίας Προσωπικών Δεδομένων

Η επιτυχία της ηλεκτρονικής διακυβέρνησης εξαρτάται σε μεγάλο βαθμό από την προστασία των προσωπικών δεδομένων, από την αντιμετώπιση, δηλαδή των προβλημάτων προστασίας της ιδιωτικότητας, τα οποία αναγράφονται κατά την ανάπτυξη των ηλεκτρονικών υπηρεσιών από τη δημόσια διοίκηση. Τα προβλήματα αυτά είτε είναι εγγενή, αφορούν δηλαδή τη χρήση του διαδικτύου ως μέσου επικοινωνίας, είτε αφορούν συγκεκριμένα ειδικά ζητήματα, όπως είναι η χρήση ενός μοναδικού αναγνωριστικού αριθμού, η διασύνδεση αρχείων της διοίκησης κ.ο.κ.

Ειδικότερα, η χρήση του διαδικτύου συνεπάγεται την αποκάλυψη προσωπικών δεδομένων και τούτο σε αντίθεση με την παραδοσιακή επίσκεψη σε μια δημόσια υπηρεσία. Ο χρήστης του διαδικτύου σε κάθε επίσκεψή του σε δικτυακούς τόπους αποκαλύπτει εν γνώσει του ή μη πληροφορίες που αφορούν στο άτομό του. Οι πληροφορίες αυτές μπορεί να χρησιμοποιηθούν στη συνέχεια, για τη δημιουργία προφίλ προσωπικότητας των χρηστών. Γενικότερα, κατά τη χρήση των διαδικτυακών υπηρεσιών είναι δυνατές η συλλογή και η συγκέντρωση προσωπικών πληροφοριών για τη συμπεριφορά και τις προτιμήσεις των χρηστών. Στην περίπτωση των πληροφοριών που κατέχουν οι δημόσιες υπηρεσίες και οι διοικητικοί οργανισμοί, είναι δυνατόν οι πληροφορίες που αυτοί διαθέτουν για τους διοικούμενους να συγκεντρωθούν σε ένα ενιαίο σύνολο.

Συνέπεια της συγκέντρωσης ενός τέτοιου όγκου πληροφοριών που αφορούν στο άτομο και στη δημιουργίας προφίλ προσωπικότητας γι' αυτό είναι ότι καθίσταται ο πολίτης διαφανής και ως εκ τούτου, χειραγωγήσιμος. Επίσης, η συγκέντρωση μεγάλου πληροφοριακού όγκου- στην προκειμένη περίπτωση από τις δημόσιες αρχές- οδηγεί στη συρρίκνωση της ιδιωτικής σφαίρας του ατόμου, όπως και στην αδυναμία του να γνωρίζει ποιός, τι, από πού και για ποιό σκοπό γνωρίζει γι' αυτό.

Πέραν τούτου, η καθιέρωση ενός αναγνωριστικού αριθμού για την πρόσβαση σε διάφορες ηλεκτρονικές υπηρεσίες γεννά προβλήματα, καθώς καθιστά ευχερή την ταυτοποίηση του ατόμου, και κατά συνέπεια, πιο εύκολη την πρόσβαση στα προσωπικά του δεδομένα. Επίσης, η διασύνδεση αρχείων του δημόσιου τομέα δημιουργεί παρόμοια προβλήματα, καθώς είναι δυνατή η αποκάλυψη πλήθους προσωπικών δεδομένων που σε συνδυασμό με άλλα δεδομένα μπορεί να έχουν αρνητικές συνέπειες για τους πολίτες.

Όπως και στην περίπτωση του ηλεκτρονικού εμπορίου, έτσι και εν προκειμένω, για να πετύχει τους στόχους της η εισαγωγή της ηλεκτρονικής διακυβέρνησης, είναι αναγκαία η διασφάλιση των χρηστών των σχετικών υπηρεσιών ότι τα προσωπικά τους δεδομένα θα προστατεύονται αποτελεσματικά. Η παρούσα περίπτωση παρουσιάζει την ιδιαιτερότητα ότι τα προσωπικά δεδομένα των χρηστών είναι πιο ευαίσθητα σε σχέση με τα δεδομένα του ηλεκτρονικού εμπορίου, καθώς αφορούν σε σημαντικές πτυχές της προσωπικής ζωής του ατόμου, τις οποίες το άτομο εμπιστεύεται στην πολιτεία και έχει την αξίωση της προστασίας τους.

4.5.2 Εφαρμογή της Νομοθεσίας για την Προστασία Προσωπικών Δεδομένων στην Ηλεκτρονική Διακυβέρνηση

Σύμφωνα με το θεμελιώδη κανόνα του άρθρου 3 παρ.1 ν. 2472/1997, οι διατάξεις του εν λόγω νόμου εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία

καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο. Στην περίπτωση των αμφίδρομων ηλεκτρονικών υπηρεσιών που παρέχονται από τη διοίκηση έχουμε να κάνουμε με αυτοματοποιημένη επεξεργασία δεδομένων, οπότε βρίσκει σαφώς εφαρμογή ο ν. 2472/1997. Στην περίπτωση των υπηρεσιών ηλεκτρονικής διακυβέρνησης που εξαντλούνται στην παροχή πληροφόρησης στους πολίτες δεν υφίσταται καμιά επεξεργασία προσωπικών δεδομένων και ο παραπάνω νόμος δεν εφαρμόζεται.

Καθοριστική σημασία για την εφαρμογή του ν. 2472/1997 έχουν τα δεδομένα που υπόκεινται σε επεξεργασία, να είναι δεδομένα προσωπικού χαρακτήρα. Σύμφωνα με το νόμο αυτό, ως προσωπικά δεδομένα νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, στο φυσικό πρόσωπο, δηλαδή, στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί. Από τον ορισμό αυτό εξαιρούνται τα στατιστικής φύσεως συγκεντρωτικά δεδομένα, από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα των δεδομένων.

Τα δεδομένα που δεν παρουσιάζουν σχέση με φυσικά πρόσωπα είναι ανώνυμα και σε αυτά δεν εφαρμόζεται ο ν. 2472/1997. Ως ανώνυμα μπορεί να γίνουν νοητά τα δεδομένα που αναφέρονται μεν σε πρόσωπα, τα οποία όμως δεν μπορούν να συσχετιστούν με κάποιο συγκεκριμένο πρόσωπο. Τα ανώνυμα δεδομένα ομοιάζουν με τα δεδομένα στα οποία είναι δυνατή η ταυτότητα του υποκειμένου, με τη διαφορά ότι αυτό δεν είναι πλέον εφικτό.

Ιδιαίτερη περίπτωση είναι τα ψευδώνυμα δεδομένα, όσα δηλαδή αντιστοιχούν σε ένα υποκείμενο δεδομένων, η ταυτότητα του οποίου συγκαλύπτεται με ένα ψευδώνυμο. Και στην περίπτωση αυτή, κατά την ορθότερη άποψη, δεν εφαρμόζεται ο ν. 2472/1997, αφού τα δεδομένα αυτά δεν σχετίζονται με κάποιο φυσικό πρόσωπο.

Οι δύο παραπάνω κατηγορίες δεδομένων παίζουν σημαντικό ρόλο στο πλαίσιο της προστασίας δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Σύμφωνα με το άρθρο 5 παρ.7 του ν. 3471/2006, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει, στο βαθμό που αυτό είναι τεχνικώς εφικτό, να καθιστά δυνατές τη χρήση και την πληρωμή των υπηρεσιών αυτών ανώνυμα ή με ψευδώνυμο.

4.5.2.1 Η Νομιμότητα της Επεξεργασίας Δεδομένων

Οι υπηρεσίες ηλεκτρονικής διακυβέρνησης, στις οποίες λαμβάνει χώρα επεξεργασία προσωπικών δεδομένων, υπόκεινται στις διατάξεις του δικαίου προστασίας των προσωπικών δεδομένων. Και τούτο, διότι κάθε επεξεργασία προσωπικών δεδομένων συνιστά επέμβαση στο συνταγματικό δικαίωμα προστασίας των προσωπικών δεδομένων, στο δικαίωμα προστασίας της ιδιωτικής ζωής, όπως γενικότερα και στα θεμελιώδη δικαιώματα.

Κατ' αρχάς θα πρέπει να τηρείται η αρχή της νομιμότητας (άρθρο 4 παρ.1 ν. 2472/1997), σύμφωνα με την οποία η συλλογή δεδομένων πρέπει να γίνεται κατά νόμιμο τρόπο και αυτά να υφίστανται νόμιμη επεξεργασία, ενόψει των σκοπών αυτών. Για να είναι, συνακόλουθα νόμιμη η επεξεργασία προσωπικών δεδομένων πρέπει να πληρείται μία από τις προϋποθέσεις του άρθρου 5 ν. 2472/1997. Εν προκειμένω, δύο είναι οι διατάξεις που βρίσκουν εφαρμογή. Κατά πρώτον, η επεξεργασία προσωπικών δεδομένων θα είναι νόμιμη, υπό την προϋπόθεση ότι αυτή είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο

επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα. Για να συντρέχει αυτή η προϋπόθεση απαιτείται, κατ' αρχάς να έχουμε έργο δημοσίου συμφέροντος, δηλαδή έργο που εξυπηρετεί λόγους δημοσίου συμφέροντος, το οποίο εξειδικεύεται με την αναφορά στις ειδικότερες εκφάνσεις του, όπως είναι το συμφέρον της εθνικής οικονομίας κ.α., ή έργο που εμπίπτει στην άσκηση δημόσιας εξουσίας. Επιπλέον πρέπει το έργο να εκτελείται από δημόσια αρχή ή από υπεύθυνο επεξεργασίας κατόπιν αναθέσεως από δημόσια αρχή.

Σύμφωνα με τα παραπάνω, η επεξεργασία δεδομένων στο πλαίσιο των υπηρεσιών διοικητικής διακυβέρνησης που εμπίπτουν στη δραστηριότητα της δημόσιας διοίκησης ανήκει στην παραπάνω διάταξη και συνεπώς είναι νόμιμη. Εξάλλου, η παροχή πληροφόρησης είναι υποχρέωση του κράτους που απορρέει από το Σύνταγμα, το οποίο κατοχυρώνει το δικαίωμα πληροφόρησης και την υποχρέωση της διοίκησης να απαντά σε αιτήματα για παροχή πληροφοριών και χορήγηση εγγράφων. Σε συνδυασμό με τη διάταξη 5^{A} παρ.2 του Συντάγματος, που θεμελιώνει το δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας, γίνεται σαφές ότι η παροχή πληροφόρησης και η υποχρέωση απάντησης στα αιτήματα των πολιτών μπορεί και πρέπει να λαμβάνουν χώρα και με ηλεκτρονικά μέσα.

Περαιτέρω, η χρήση ηλεκτρονικών μέσων για τη διεκπεραίωση διοικητικών διαδικασιών προβλέπεται ρητά στον νόμο και συγκεκριμένα στο άρθρο 8 του ν.3242/2004, στο οποίο ορίζεται ότι οι διοικητικές συναλλαγές που συνδέονται με την έκδοση ατομικής πράξης φορέων του δημόσιου τομέα που αφορούν στην έκδοση πιστοποιητικών ή άλλων εγγράφων με τα οποία βεβαιώνονται πραγματικά περιστατικά, στοιχεία ή έννομες σχέσεις, διενεργούνται και ολοκληρώνονται από την υπηρεσία που είναι αρμόδια για την έκδοση της τελικής πράξης και με χρήση ηλεκτρονικών μέσων και ιδίως προηγμένων πληροφοριακών συστημάτων διαλειτουργικότητας.

Σε ιδιαίτερες περιπτώσεις, όπου δεν πληρείται η προϋπόθεση που θέτει η διάταξη του άρθρου 5 του ν. 2472/1997, θα πρέπει να παρέχεται η συγκατάθεση από το υποκείμενο των δεδομένων. Η συγκατάθεση μπορεί εφόσον αφορά σε απλά και όχι σε ευαίσθητα δεδομένα, να παρέχεται ηλεκτρονικά, για παράδειγμα με την συμπλήρωση τετραγωνιδίου κατά την επίσκεψη ιστοσελίδας του διαδικτύου.

4.5.2.2 Γενικές Αρχές της Προστασίας Προσωπικών Δεδομένων

Σύμφωνα με το άρθρο 4 παρ.1 του ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται ενόψει των σκοπών της επεξεργασίας. Από τη διάταξη αυτή, με την οποία θεμελιώνεται η γενική αρχή της αναγκαιότητας της επεξεργασίας, προκύπτουν επιμέρους αρχές, οι οποίες διέπουν την επεξεργασία προσωπικών δεδομένων. Κατ' αρχάς τα προσωπικά δεδομένα πρέπει να είναι συναφή, δηλαδή σχετικά με το σκοπό της επεξεργασίας, αλλά και κατάλληλα για την εξυπηρέτηση του σκοπού αυτού, ενώ επιπλέον δεν πρέπει να είναι περισσότερα από όσα κάθε φορά απαιτούνται ενόψει των σκοπών της επεξεργασίας.

Η αρχή της αναγκαιότητας της επεξεργασίας χαράσσει τα όρια για τη νόμιμη επεξεργασία δεδομένων από δημόσιες αρχές. Συγκεκριμένα, η αρχή αυτή σημαίνει ότι πρέπει να τυγχάνουν επεξεργασίας μόνο τα δεδομένα που είναι αναγκαία για την εκπλήρωση του σκοπού της επεξεργασίας, ενώ η επεξεργασία δεδομένων θα πρέπει να πραγματοποιείται μόνο εφόσον τούτο είναι αναγκαίο. Ως εκ τούτου, τα δεδομένα που συλλέγονται για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης θα πρέπει να περιορίζονται στα αναγκαία μόνο για το σκοπό αυτό δεδομένα.

Αξίζει να σημειωθεί εδώ ότι με βάση την αρχή της αναγκαιότητας, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έκρινε σε πολλές περιπτώσεις ως μη νόμιμη την επεξεργασία δεδομένων από δημόσιες αρχές. Ενδεικτικά αναφέρεται η υπ' αριθ. 510/17/15.5.2000 απόφαση της Αρχής, που αφορούσε στην αναγραφή προσωπικών δεδομένων στις αστυνομικές ταυτότητες και στην οποία η Αρχή έκρινε ότι ορισμένα από τα αναφερόμενα στις ταυτότητες στοιχεία δεν ήταν αναγκαία για την επίτευξη του σκοπού της επεξεργασίας που είναι η βεβαίωση της ταυτότητας του υποκειμένου. Μεταξύ αυτών περιλαμβάνονται το δακτυλικό αποτύπωμα, το ονοματεπώνυμο του/της συζύγου, το επάγγελμα, η υπηκοότητα, η κατοικία και το θρήσκευμα. Παρομοίως, στην υπ' αριθ. 1446/10.11.2000 απόφαση της Αρχής κρίθηκε ότι η αναγραφή του θρησκεύματος επί του πιστοποιητικού γεννήσεως που εκδίδουν οι Δήμοι θα πρέπει να γίνεται μόνο στην περίπτωση που το θρήσκευμα σύμφωνα με το νόμο αποτελεί προϋπόθεση εξασκήσεως δικαιώματος, όπως για παράδειγμα χρήση του πιστοποιητικού για την εγγραφή σε ιερατική σχολή, άλλως θα πρέπει να παραλείπεται, διότι δεν είναι απαραίτητο για το σκοπό της επεξεργασίας, δηλαδή, για την πιστοποίηση των δεδομένων γεννήσεως.

Σημαντικές είναι επίσης οι αρχές της δεσμευτικότητας του σκοπού και του καθορισμένου σκοπού, οι οποίες διέπουν την επεξεργασία προσωπικών δεδομένων. Σύμφωνα με το άρθρο 4 παρ.1 του ν. 2472/1997, τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.

Συνακόλουθα, ο σκοπός της επεξεργασίας πρέπει να είναι καθορισμένος και η επεξεργασία δεδομένων να πραγματοποιείται για το συγκεκριμένο σκοπό, αποκλειόμενης της πολυλειτουργικής συλλογής και χρήσης των προσωπικών δεδομένων. Η στόχευση αυτή του δικαίου της προστασίας των προσωπικών δεδομένων είναι ιδιαίτερα σημαντική στο πλαίσιο της ηλεκτρονικής διακυβέρνησης, καθώς και με την εφαρμογή της αρχής της δεσμευτικότητας του σκοπού καθίσταται σαφές ότι τα δεδομένα που συλλέγονται με αφορμή την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας δεν πρέπει να χρησιμοποιούνται αργότερα από τη διοίκηση και να λαμβάνει χώρα συσχέτιση ή συνδυασμός με άλλα δεδομένα.

4.5.2.3 Άλλες Ασφαλιστικές Δικλίδες Προστασίας

Η προστασία των προσωπικών δεδομένων του διοικούμενου διασφαλίζεται με τις διατάξεις του ν. 2472/1997 που κατοχυρώνουν τα δικαιώματα των υποκειμένων των δεδομένων. Ο νόμος αυτός κατοχυρώνει ορισμένα δικαιώματα, από τα οποία τα δύο πρώτα αφορούν την πληροφόρηση του υποκειμένου των δεδομένων και τα υπόλοιπα τη δυνατότητα προβολής αντιρρήσεων και δικαστικής προστασίας. Έτσι, στο άρθρο 11 ρυθμίζεται το δικαίωμα ενημέρωσης και συγκεκριμένα προβλέπεται η υποχρέωση του υπεύθυνου της επεξεργασίας για ενημέρωση των υποκειμένων, ήδη κατά το στάδιο της συλλογής προσωπικών δεδομένων. Στην περίπτωση που τα δεδομένα δεν συλλέγονται απ' ευθείας από το υποκείμενο ή με τη συνδρομή του, πρέπει το υποκείμενο να ενημερώνεται (άρθρο 11 παρ.3).

Περαιτέρω, αναγνωρίζεται το δικαίωμα πρόσβασης (άρθρο 12), δηλαδή το δικαίωμα του υποκειμένου των δεδομένων να γνωρίζει εάν τα δεδομένα προσωπικού χαρακτήρα που το αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Ακολούθως, προβλέπεται το δικαίωμα προβολής αντιρρήσεων για την επεξεργασία δεδομένων, οι οποίες απευθύνονται στον υπεύθυνο επεξεργασίας και περιέχουν υποχρεωτικό αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση,

μη διαβίβαση ή διαγραφή. (άρθρο 13). Και ακόμα, το υποκείμενο των δεδομένων έχει το δικαίωμα προσωρινής δικαστικής προστασίας, μπορεί δηλαδή να ζητήσει από το αρμόδιο δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που το θίγει, όταν αυτή έχει ληφθεί αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της οικονομικής φερεγγυότητας και της αξιοπιστίας του (άρθρο 14 του ν. 2472/1997).

Πέρα από τα παραπάνω, στη διασφάλιση της προστασίας των προσωπικών δεδομένων συμβάλλουν η αρχή της αποφυγής και η αρχή της οικονομίας της επεξεργασίας. Όπως αναφέρθηκε παραπάνω, ο νομοθέτης προβλέπει τη δυνατότητα χρήσης και πληρωμής των υπηρεσιών ηλεκτρονικών επικοινωνιών ανώνυμα ή με ψευδώνυμο. Περαιτέρω, και ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατό λιγότερων δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τη διάταξη του άρθρου 5 παρ.6 του ν.3471/2006.

Σημαντικό είναι, ακόμα να λαμβάνεται πρόνοια για τη λήψη των κατάλληλων οργανωτικών και τεχνικών μέτρων για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας (άρθρο 10 παρ.3 του ν. 2472/1997).

Επιπλέον είναι δυνατή η λήψη μέτρων αυτοπροστασίας των χρηστών του διαδικτύου. Η προσέγγιση αυτή ισοδυναμεί με μια προτροπή για τη χρήση τεχνολογιών όπως είναι η κρυπτογραφία και η στενογραφία που σκοπό έχουν την προστασία της ανωνυμίας των χρηστών. Αυτό βέβαια, δεν θα είναι δυνατό στις περιπτώσεις όπου η χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης γίνεται μόνο μετά από εξουσιοδοτημένη πρόσβαση, πράγμα που αποτελεί μάλλον τον κανόνα όταν πρόκειται για αμφίδρομες υπηρεσίες.

4.5.3 Επίλογος

Με την εξέλιξη των ηλεκτρονικών υπηρεσιών της δημόσιας διοίκησης αναμένεται να ανακύψουν καινοφανή ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα. Ένα τέτοιο ζήτημα για παράδειγμα, αποτελεί και η διαχείριση της ηλεκτρονικής ταυτότητας, για το οποίο περιέχονται ειδικές ρυθμίσεις σε αλλοδαπές νομοθεσίες. Είναι όμως αναγκαία η ρύθμιση των σχετικών ζητημάτων με ειδικές νομοθετικές ρυθμίσεις, καθώς η εφαρμογή των γενικών διατάξεων του ν. 2472/1997 δεν θα οδηγεί πάντοτε στην επίλυσή τους. **[19]**

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

Β' Μέρος, Η Διαχείριση της Εμπιστοσύνης και η Προστασία της Ιδιωτικότητας στο Πεδίο της Έρευνας

5. Ηλεκτρονικό Έγκλημα και Θέματα Ιδιωτικότητας

Το κυβερνο-έγκλημα *(cybercriminality)* τείνει να γίνει η κατάρα της σημερινής κοινωνίας και επηρεάζει κάθε έναν, σε εθνικό και διεθνές επίπεδο. Οι χρήστες, οι εταιρείες, τα ιδρύματα, οι κυβερνήσεις μπορεί να γίνουν θύματα ή ακόμα και βοηθοί των κυβερνο-εγκληματιών (άθελά τους). Άρρηκτα συνδεδεμένη με το κυβερνο-έγκλημα είναι η αντανάκλαση της εξέλιξης των πρακτικών του εγκλήματος που έχουν προσαρμοστεί στον κόσμο των τεχνολογιών της πληροφορίας και της επικοινωνίας.

Λόγω της παγκόσμιας φύσης της κατανομής του διαδικτύου, της δομής του, των υπηρεσιών και των ομάδων χρηστών του, οι εγκληματίες που το χρησιμοποιούν για τις δραστηριότητές τους, διαμορφώνουν μια σοβαρή πρόκληση: Αυτή περιλαμβάνει (χωρίς όμως να περιορίζεται σε αυτά), την συλλογή πληροφοριών για συμβάντα που σχετίζονται με κυβερνο-εγκλήματα την αναγνώριση των κατάλληλων ατόμων και των κατάλληλων νόμων για τη δίωξή τους.

Τα ίδια ισχύουν και για την ιδιωτικότητα: Μια ποικιλία κουλτούρας, διαφορετικών νόμων και γνωμών δυσκολεύουν τη συμφωνία σε πρότυπα προσεγγίσεων που θα χρησιμοποιηθούν διεθνώς. Θα πρέπει επίσης να σημειώσουμε ότι η ιδέα της ψηφιακής ιδιωτικότητας συχνά «υποφέρει» στα χέρια των τεχνολογιών της πληροφορίας και των τηλεπικοινωνιών και ότι τα προσωπικά δεδομένα είναι άυλα αγαθά μεγάλης αξίας, τόσο για τις νομικές υπηρεσίες όσο και για τους εγκληματίες.

Θα αναφέρουμε στη συνέχεια κάποια ερευνητικά *projects* που αγγίζουν τα προβλήματα της ψηφιακής ιδιωτικότητας και προσπαθούν να συνεισφέρουν στον καλύτερο χειρισμό των αδυναμιών που μπορεί να τις εκμεταλλευτούν για κακόβουλους λόγους. Στην πραγματικότητα, η *ψηφιακή ασφάλεια (cybersecurity)* αποτελεί ένα νέο και ξεχωριστό πεδίο έρευνας που βασίζεται στις γνώσεις και τεχνικές που υπάρχουν στα πεδία του νόμου, της εγκληματολογίας, της κοινωνιολογίας, της ανθρωπολογίας, των οικονομικών, της πολιτικής επιστήμης και των ψηφιακών τεχνολογιών. Τα *projects* που αναφέρονται στη συνέχεια δίνουν μεγαλύτερη έμφαση στο πεδίο των ψηφιακών τεχνολογιών.

5.1 *SysSec:* Η Διαχείριση των Απειλών και των Αδυναμιών στο Μελλοντικό Διαδίκτυο

Για πολλά χρόνια οι εισβολείς των πληροφοριακών συστημάτων βρίσκονταν ένα βήμα μπροστά από τους αμυνόμενους. Η ασύμμετρη φύση της απειλής οδήγησε σε ένα φαύλο κύκλο όπου τελικά οι επιτιθέμενοι έβγαιναν νικητές. Το *SysSec (Systems Security)* προσπαθεί να σπάσει αυτόν τον φαύλο κύκλο στο πεδίο της ασφάλειας των συστημάτων και ενθαρρύνει τους ερευνητές να επικεντρωθούν στις μελλοντικές απειλές και όχι στις επιθέσεις του χτες, έτσι ώστε να είναι καλά προετοιμασμένοι και να προλάβουν τις επόμενες κινήσεις των επιτιθέμενων.

Την περασμένη δεκαετία παρατηρήθηκε ένας μεγάλος αριθμός επιθέσεων στο διαδίκτυο. Κινούμενοι από οικονομικά και πολιτικά κίνητρα, οι επιτιθέμενοι διενεργούσαν επιθέσεις οι οποίες έμεναν όσο το δυνατόν αθέατες, ήταν δύσκολο να ανιχνευθούν και εκμεταλλεύονταν τον πιο αδύναμο κρίκο, δηλ. το χρήστη. Η πηγή του προβλήματος βρίσκονταν στην ίδια τη φύση της ασφάλειας στο διαδίκτυο. Στην τρέχουσα πρακτική της ασφάλειας του διαδικτύου, οι περισσότερες άμυνες έχουν την μορφή της αντίδρασης ενώ οι επιτιθέμενοι είναι εξ ορισμού ενεργητικοί. Οι ερευνητές της ασφάλειας του

διαδικτύου, συνήθως κυνηγούν τους επιτιθέμενους προσπαθώντας να βρουν έναν μηχανισμό άμυνας για κάθε νέα επίθεση. Έτσι αντιμετωπίζουμε μια ασύμμετρη απειλή: ενώ οι επιτιθέμενοι έχουν όλο το χρόνο να διαλέξουν πότε και πού θα χτυπήσουν ελαχιστοποιώντας το κόστος, οι αμυνόμενοι πρέπει να απαντήσουν άμεσα μέσα σε στενά χρονικά πλαίσια και με μεγαλύτερο κόστος. Κάθε νέος γύρος επίθεσης-άμυνας απομυζά ενέργεια από τους αμυνόμενους, τραβώντας τους σε ένα φαύλο κύκλο που τελικά τους αποδυναμώνει. Φαίνεται ότι ο μόνος τρόπος να χτίσουμε αποτελεσματικές άμυνες είναι να σπάσουμε αυτό τον κύκλο, αλλάζοντας τους κανόνες του παιχνιδιού, προλαμβάνοντας τις κινήσεις των επιτιθέμενων έτσι ώστε να είμαστε πάντα ένα βήμα μπροστά από αυτούς. Αυτό μπορεί να γίνει με τους εξής τρόπους:

- Αναγνωρίζοντας τις αναδυόμενες αδυναμίες,
- Εργαζόμενοι προς την κατεύθυνση της απάντησης των πιθανών επιθέσεων πριν αυτές εμφανιστούν.

Προς αυτή την κατεύθυνση, το πρόσφατα δημιουργημένο *SysSec Network of Excellence* προσπαθεί να αλλάξει την προσέγγιση στην ασφάλεια του διαδικτύου. Αντί να κυνηγάμε τους επιτιθέμενους αφού γίνει η επίθεση, το *SysSec* μελετά εκ των προτέρων τις επείγουσες απειλές και αδυναμίες. Η βασική εργασία του *SysSec* είναι να προσδιορίσει έναν οδικό χάρτη για την αντιμετώπιση των απειλών και το χτίσιμο μιας υποδομής για την ενίσχυση της εκπαίδευσης στην ασφάλεια των συστημάτων – έτσι ώστε να παρέχει την εμπειρία που χρειάζεται για να αντιμετωπιστούν οι αναδυόμενες απειλές.

5.1.1 Οδικός Χάρτης

Με την συνεργασία της ερευνητικής κοινότητας, το *SysSec* έχει ήδη παράξει έναν ερευνητικό οδικό χάρτη (http://syssecproject.eu/roadmap1) ο οποίος περιγράφει κάποιες σημαντικές περιοχές στις οποίες θα πρέπει να εστιάσουμε. Στον πρώτο χρόνο της δοκιμασίας του, αυτό το *project* επέλεξε πέντε κατηγορίες:

1. ***Ιδιωτικότητα:*** Το *SysSec* προτρέπει τους ερευνητές να εξετάσουν πώς θα προστατέψουν τους χρήστες από τις εξελιγμένες απειλές που τείνουν να αποκαλύψουν τις προσωπικές τους πληροφορίες. Για παράδειγμα, είναι σημαντικό να ανιχνεύσουν λειτουργίες που έχουν αδυναμίες και μπορεί να αποκαλύψουν προσωπικά δεδομένα χρηστών ή λογαριασμούς πρόσβασης σε *online* υπηρεσίες.
2. ***Στοχευμένες επιθέσεις:*** Είναι σημαντικό να αναπτύξουν οι ερευνητές νέες τεχνικές για τη συλλογή και την ανάλυση δεδομένων που σχετίζονται με στοχευμένες επιθέσεις. Η έλλειψη διαθέσιμων δεδομένων, σε συνδυασμό με τον περιορισμό της παραδοσιακής ανάλυσης και των τεχνικών προστασίας, αποτελεί ένα από τα αδύνατα σημεία στον πόλεμο κατά των *malware*. Επίσης οι ερευνητές θα πρέπει να εστιάσουν σε νέες προσεγγίσεις άμυνας που λαμβάνουν υπόψη τους εναλλακτικούς παράγοντες (όπως τις αναβαθμίσεις) και μεγάλης κλίμακας πρόληψη (για παράδειγμα στους *ISP*).
3. ***Ασφάλεια των αναδυόμενων τεχνολογιών:*** Η ασφάλεια σε νέες, αναδυόμενες τεχνολογίες (όπως τα κοινωνικά δίκτυα, οι έξυπνες μηχανές κ.λπ.) είναι μια από τις προτεραιότητες της περιοχής της ασφάλειας του συστήματος. Σε αυτή την κατεύθυνση είναι σημαντικό να ενισχυθεί η συνεργασία μεταξύ της ακαδημαϊκής κοινότητας και της βιομηχανίας για να

μεγιστοποιηθούν οι επιπτώσεις της έρευνας και να ελαττωθεί ο χρόνος που χρειάζεται για την ανάλυση και τις δοκιμές.

4. ***Κινητικότητα:*** Ανάπτυξη νέων εργαλείων και τεχνικών που θα μπορούν να εφαρμοστούν σε υπάρχοντα συστήματα *smartphone* για την ανίχνευση και πρόληψη επιθέσεων έναντι των συσκευών και των εφαρμογών τους.
5. ***Χρησιμοποιήσιμη ασφάλεια:*** Είναι απαραίτητη μια μελέτη της χρήσης των μέτρων ασφάλειας και θα γίνει περισσότερο κρίσιμη στο μέλλον. Αν θέλουμε να προχωρήσουμε προς αυτή την κατεύθυνση, θα πρέπει να γίνουν προσπάθειες που θα ενώσουν τους ειδικούς από διάφορες τεχνικές περιοχές (μηχανικούς, τεχνικούς ασφάλειας συστημάτων, ψυχολόγους, νομικούς κ.λπ.)

Με τη βοήθεια των τεχνικών που έχουν οργανωθεί σε ομάδες εργασίας, το *SysSec* ενημερώνει τον οδικό χάρτη σε τακτά χρονικά διαστήματα, ώστε να περιλαμβάνει νέες απειλές και προτεραιότητες.

5.1.2 Εκπαίδευση

Έχοντας αναγνωρίσει την έλλειψη εκπαιδευτικού υλικού στην περιοχή της ασφάλειας των συστημάτων, το *SysSec* σκοπεύει να εγκαταστήσει ένα κέντρο ακαδημαϊκής υποστήριξης και έχει αρχίσει να σχεδιάζει ένα κοινό εκπαιδευτικό πρόγραμμα για την ασφάλεια συστημάτων, εστιάζοντας κυρίως στην παραγωγή *slides* και εργαστηριακών ασκήσεων. Αυτό το πρόγραμμα θα διατίθεται στα Πανεπιστήμια της Ευρώπης και σκοπεύει να αποτελέσει ένα υψηλού επιπέδου εκπαιδευτικό πρόγραμμα για την ασφάλεια των συστημάτων. **[20]**

5.2 Η Κατανόηση του Ρόλου των *Malware* στο κυβερνο-έγκλημα

Στον πυρήνα κάθε λειτουργίας κυβερνο-εγκλήματος είναι η ικανότητα του επιτιθέμενου να εγκαταστήσει *malware* στους υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο χωρίς να το ξέρουν οι χρήστες τους. Το *project MALICIA* έχει σκοπό να μελετήσει τον κρίσιμο ρόλο των *malware* στο κυβερνο-έγκλημα και την πρόσφατη ανάπτυξη μιας υπόγειας οικονομίας που σχετίζεται με το *malware* και την υπονόμευση των υπολογιστών που είναι συνδεδεμένοι στο διαδίκτυο.

Το κυβερνο-έγκλημα και η εγκληματική δραστηριότητα που διενεργείται μέσω υπολογιστών συνδεδεμένων στο διαδίκτυο αποτελεί μια διογκούμενη απειλή για τις αναπτυγμένες περιοχές, όπως είναι η Ευρώπη όπου σχεδόν τα τρία τέταρτα των νοικοκυριών και ένας μεγάλος αριθμός των υποδομών είναι συνδεδεμένα στο διαδίκτυο και επίσης ένας αυξανόμενος αριθμός υπηρεσιών και συναλλαγών γίνονται *online*.

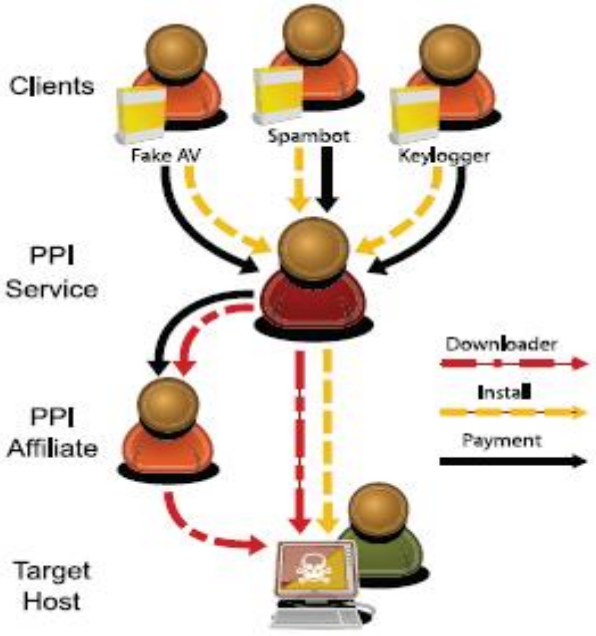
Στον πυρήνα των περισσότερων λειτουργιών κυβερνο-εγκλήματος βρίσκεται η ικανότητα του επιτιθέμενου να εγκαταστήσει κακόβουλα προγράμματα (*malware*) σε υπολογιστές συνδεδεμένους στο διαδίκτυο, χωρίς να το καταλάβουν οι χρήστες τους. Το *malware* περιλαμβάνει *bots, trojan horses, rootkits,* ιούς, ψεύτικο λογισμικό και *spyware*. Το *malware* επιτρέπει στους επιτιθέμενους να εγκαταστήσουν μια μόνιμη παρουσία σε έναν υπολογιστή και να τον χρησιμοποιήσουν για τις δικές τους λειτουργίες. Ο σκοπός τους μπορεί να είναι οι ίδιοι οι υπολογιστές, δηλ. η κλοπή της πνευματικής ιδιοκτησίας ενός οργανισμού, ή οι κωδικοί πρόσβασης λογαριασμών μιας τράπεζας. Πολλές φορές οι επιτιθέμενοι χρησιμοποιούν τους υπολογιστές σαν αποδέκτες των κακόβουλων δραστηριοτήτων, στέλνοντας σε αυτούς *spam*, κάνοντας επιθέσεις άρνησης παροχής υπηρεσίας (*DoS*).

Ο σκοπός του *project MALICIA (IMDEA Software Institute)* είναι να μελετήσει τον κρίσιμο ρόλο του *malware* στο κυβερνο-έγκλημα και την πρόσφατη άνοδο της

εκτεταμένης υπόγειας οικονομίας που σχετίζεται με το *malware* και την υπονόμευση των υπολογιστών που είναι συνδεδεμένοι στο διαδίκτυο. Οι μέρες που οι επιτιθέμενοι δημιουργούσαν κακόβουλο λογισμικό και το εγκαθιστούσαν σε υπολογιστές για να δείξουν τις ικανότητές τους, έχουν πια περάσει. Σήμερα, το οικοσύστημα που σχετίζεται με το *malware* περιστρέφεται περισσότερο γύρω από το κυβερνο-έγκλημα και την αποκόμιση οικονομικών ωφελειών.

Καθώς το οικοσύστημα του *malware* έχει αυξηθεί και είναι πιο επικερδές, έχει εξελιχθεί και τεχνικά. Οι επιτιθέμενοι έχουν καταλάβει ότι η αντιμετώπιση ολόκληρης της αλυσίδας από τη δημιουργία του *malware* μέχρι το *monetization* είναι ένα αποθαρρυντικό έργο γιατί απαιτεί υψηλού επιπέδου δεξιότητες και πόρους. Σαν αποτέλεσμα, έχουν δημιουργηθεί ειδικευμένες υπηρεσίες σε όλα τα στάδια της αλυσίδας *malware-monetization*, όπως *toolkits* που αυτοματοποιούν την κατασκευή των *malware*, εργαλεία κωδικοποίησης προγραμμάτων για την αποφυγή του αντιϊϊκού λογισμικού.

Σαν ένα πρώτο βήμα στο *project MALICIA*, υπήρξε συνεργασία με ερευνητές του Πανεπιστημίου *Berkeley* και του *International Computer Science Institute*, για να διερευνήσουν την εμπορευματοποίηση της διανομής του *malware* στην μορφή *pay-per-install (PPI)* υπηρεσιών, όπως φαίνεται στο ***σχήμα 36***. Οι *PPI* υπηρεσίες προσφέρουν στους εγκληματίες έναν απλό τρόπο να αναθέτουν την διανομή του *malware* που έχουν δημιουργήσει. Οι πελάτες προσφέρουν το *malware* στην υπηρεσία *PPI* και επιλέγουν τον αριθμό των επιθυμητών εγκαταστάσεων σε κάθε γεωγραφική περιοχή. Η υπηρεσία *PPI* φροντίζει να εγκαταστήσει το *malware* στους υπολογιστές-θύματα με αντάλλαγμα ένα μικρό ποσό που ποικίλει από 180$ για μερικές χιλιάδες υπολογιστών σε Ευρωπαϊκές χώρες και τις ΗΠΑ, μέχρι 7$ για χιλιάδες υπολογιστές στην Ασία.



Σχήμα 36: Η υπηρεσία *Pay-per-Install*

Για να ικανοποιήσουν τις ανάγκες των πελατών για εγκαταστάσεις, ο πάροχος *PPI* τυπικά αναθέτει την διανομή του *malware* σε τρίτες οντότητες που ονομάζονται θυγατρικές (*affiliates*). Οι πάροχοι *PPI* πληρώνουν τις θυγατρικές για κάθε υπολογιστή στον οποίο επιτίθενται, ενεργώντας σαν ενδιάμεσος που πουλάει εγκαταστάσεις σε πελάτες και αγοράζει εγκαταστάσεις από θυγατρικές. Κάθε θυγατρική μπορεί να ειδικεύεται σε κάποια συγκεκριμένη μέθοδο διανομής *malware* (για παράδειγμα μέσω

κάλυψης του *malware* με ένα πρόγραμμα καλοήθες και διανομή του μέσα από δίκτυα που μοιράζονται αρχεία, ή μέσω κοινωνικής μηχανικής, ή μέσω εκμετάλλευσης των φυλλομετρητών *web* μέσω της φόρτωσης διάφορων ιστοσελίδων ή εφαρμογών). Η υπηρεσία *PPI* δίνει σε κάθε θυγατρική ένα πρόγραμμα φόρτωσης ιστοσελίδων (*downloader*) προσαρμοσμένο με ένα μοναδικό αναγνωριστικό θυγατρικής. Όταν η θυγατρική εγκαθιστά τον *downloader* σε έναν υπολογιστή-θύμα, ο *downloader* συνδέεται με την υπηρεσία *PPI* για να φορτώσει τα προγράμματα του πελάτη. Αφού εγκαταστήσει τα προγράμματα στον υπολογιστή, αναφέρει στην θυγατρική το αναγνωριστικό που έχει και η θυγατρική πιστώνεται με μια εγκατάσταση.

Για να καταλάβουμε την αγορά *PPI*, θα φιλτράρουμε τέσσερις υπηρεσίες *PPI*. Γι' αυτό τον λόγο αναπτύξαμε μια υποδομή που μας επιτρέπει: **α)** να αλληλεπιδρούμε με *PPI* υπηρεσίες μιμούμενοι το πρωτόκολλο επικοινωνίας που περιμένουν από τις θυγατρικές και **β)** να συλλέγουμε και να ταξινομούμε το *malware* που διανέμεται με τις *PPI* υπηρεσίες. Χρησιμοποιώντας αυτή την υποδομή συλλέξαμε πάνω από ένα εκατομμύριο προγράμματα *malware* και τα ταξινομήσαμε ανάλογα ανά ομάδα όπως και τις μεθόδους *monetization*. Η ανάλυση αυτή αποκάλυψε ότι από τις είκοσι πιο δημοφιλείς ομάδες *malware*, οι δώδεκα απασχολούσαν υπηρεσίες *PPI* για την διανομή τους. Επίσης αποκαλύφθηκε ότι κάποιες ομάδες *malware* στόχευαν αποκλειστικά τις ΗΠΑ και κάποιες Ευρωπαϊκές χώρες. Οι μέθοδοι *monetizatio*n περιλαμβάνουν: *spam*, εγκατάσταση ψεύτικου αντιιϊκού λογισμικού, την κλοπή πληροφορίας, την άρνηση παροχής υπηρεσίας, το *adware*.

Πολλά ακόμα πρέπει να μάθουμε για το οικοσύστημα του *malware* και την οικονομία που υποστηρίζει το κυβερνο-έγκλημα. Ένας στόχος είναι να εξελίξουμε την ανάλυση του *malware* κατανοώντας τι κάνει το πρόγραμμα του *malware*, γιατί το κάνει, δηλαδή ποιό ρόλο παίζει το *malware* στην λειτουργία του κυβερνο-εγκλήματος. **[21]**

5.3 Η Προστασία των Δεδομένων στα *Android Smartphones*

Το *Android* είναι το λειτουργικό σύστημα για τις κινητές συσκευές. Λόγω της γρήγορης και ευρείας υιοθέτησής του, έγινε ο στόχος κακόβουλων εφαρμογών που συνεχώς αυξάνουν. Αυτή η αύξηση είναι ανησυχητική δεδομένου ότι ολοένα και περισσότεροι άνθρωποι βασίζονται σε αυτές τις συσκευές και για προσωπικούς και για επαγγελματικούς λόγους. Ένα σύστημα προστασίας είναι ουσιώδες, αλλά δυστυχώς, οι υπάρχοντες μηχανισμοί αποτυγχάνουν στο να προστατεύσουν τα ευαίσθητα δεδομένα που βρίσκονται σε ένα *smartphone*. Οι διαρροές αυτές, σχετίζονται με εγγενείς περιορισμούς των μηχανισμών ασφάλειας του *Android* που βασίζονται πολύ σε συστήματα ελέγχου πρόσβασης και επομένως δεν προσφέρουν έλεγχο πρόσβασης πάνω σε τμήματα δεδομένων, αφού αυτά έχουν φύγει από την πηγή τους.

Στο *CIDRe*, που είναι μια ομάδα *project* από τα *SUPELEC* και *INRIA*, σχεδιάστηκε και υλοποιήθηκε το *Blare*, ένα σύστημα ανίχνευσης εισβολής *(Intrusion Detection System-IDS)* σε *Linux*. Το *Blare* παρακολουθεί τη ροή της πληροφορίας και αναγνωρίζει παράνομα στοιχεία σε ένα γενικό πλαίσιο μιας προκαθορισμένης πολιτικής ασφάλειας. Το *Blare* βασίζεται στο πλαίσιο *LSM*, ένα διορθωτικό τμήμα προγράμματος (*patch*) για τον πυρήνα του *Linux (kernel)* που εισάγει «αγκίστρια» σε κάθε σημείο του πυρήνα όπου μια κλήση του επιπέδου χρήστη του συστήματος δημιουργεί μια ροή πληροφορίας. Γνωστά μοντέλα ασφάλειας, όπως το *SELinux, AppArmor, Smack, TOMOYO* επίσης βασίζονται στο *LSM*. Το *Blare* διατηρεί δύο ετικέτες ασφάλειας για κάθε αντικείμενο του λειτουργικού συστήματος (αρχεία, διεργασίες κ.λπ.). Η πρώτη ετικέτα καταγράφει τα ευαίσθητα δεδομένα που χρησιμοποιήθηκαν για τη δημιουργία του περιεχομένου του συγκεκριμένου αντικειμένου. Η δεύτερη ετικέτα αναφέρει τις

αναμίξεις δεδομένων που επιτρέπεται να ρέουν μέσα στο αντικείμενο (δηλ. περιγράφει την πολιτική ασφάλειας που εφαρμόζεται στο αντικείμενο). Έτσι είναι εύκολο να αποδειχθεί η νομιμότητα μιας ροής πληροφορίας, συγκρίνοντας τις τιμές των ετικετών. Όταν οι τιμές δεν ταιριάζουν, το *Blare* δημιουργεί μια ειδοποίηση.

Έχοντας μια αποτελεσματική *Linux* υλοποίηση του εργαλείου, μελετήθηκε η εφαρμογή του στο πλαίσιο του *Android*. Προτάθηκε μια συνολική πολιτική της ροής πληροφορίας προσανατολισμένη στην προστασία των δεδομένων που συνήθως υπάρχουν σε ένα *smartphone* (για παράδειγμα λίστα επαφών, γεωπληροφορία κ.λπ.) και υλοποιήθηκε μια *Android* έκδοση του *Blare*. Οι μετρήσεις που έγιναν για την επιβάρυνση που δημιούργησε η εφαρμογή έδωσαν ενθαρρυντικά αποτελέσματα και έγινε δυνατή η αναγνώριση επιθέσεων ακεραιότητας ή εμπιστευτικότητας των δεδομένων.

Για να ελεγχθεί η δυνατότητα αναγνώρισης των επιθέσεων έναντι της ακεραιότητας, χρησιμοποιήθηκε το *BaseBridge*, ένα *Android malware* που ο σκοπός του είναι να εγκαταστήσει τις κακόβουλες εφαρμογές στο τηλέφωνο, και έτσι να παραβιάσει την ακεραιότητα του συστήματος. Όπως ήταν αναμενόμενο, δημιουργήθηκαν ειδοποιήσεις από το *Blare*. Με την χρήση των ειδοποιήσεων, δημιουργήθηκε ένα γράφημα που περιέγραφε την διάδοση των μολυσμένων δεδομένων μέσα στο σύστημα, λαμβάνοντας υπόψη τη χρονική ετικέτα του κάθε συναγερμού. Το γράφημα έδειξε ότι η εφαρμογή που επρόκειτο να εγκατασταθεί δημιουργήθηκε από ένα αρχείο του *BaseBridge* και ότι το περιεχόμενό της προσπελάστηκε και αποθηκεύτηκε από διαφορετικά αντικείμενα, με έναν τρόπο που υποδείκνυε την εγκατάσταση και την εκτέλεσή της.

Για να ελεγχθεί η ικανότητα ανίχνευσης έναντι της εμπιστευτικότητας των δεδομένων, χρησιμοποιήθηκαν δύο πολύ γνωστές αδυναμίες. Η πρώτη σχετίζεται με τον *browser* του *Android* και επιτρέπει τη διαρροή των δεδομένων έξω από τη συσκευή. Η δεύτερη σχετίζεται με την *Android* εφαρμογή *Skype* που διαρρέει δεδομένα του χρήστη. Χρησιμοποιήθηκαν αυτές οι δύο αδυναμίες για τη διαρροή των *Skype* δεδομένων μέσω του *browser* προς μία απομακρυσμένη οντότητα. Τοποθετήθηκαν ετικέτες στα αρχεία με τα ευαίσθητα δεδομένα πριν από την επίθεση. Μόλις έγινε η επίθεση, το *Blare* δημιούργησε τις αντίστοιχες ειδοποιήσεις. Οι ειδοποιήσεις έδειξαν καθαρά ότι ο *browser* διάβασε αρχεία με ευαίσθητα δεδομένα και επίσης ότι διέρρευσε αυτά τα ευαίσθητα δεδομένα προς μια απομακρυσμένη οντότητα. Με τη χρησιμοποίηση των ειδοποιήσεων, χτίζεται ένα γράφημα που περιγράφει πώς διέρρευσαν τα ευαίσθητα δεδομένα στα οποία έχουν τοποθετηθεί ετικέτες. Το γράφημα έδειξε ότι ο *browser* πρώτα προσπέλασε τα ευαίσθητα δεδομένα που είχαν αποθηκευτεί στον φάκελο (*directory*) του *Skype* και μετά έγραψε αυτά τα δεδομένα σε ένα *socket* και τα έστειλε στην απομακρυσμένη οντότητα.

Συμπερασματικά, το *Blare* αποδείχτηκε αποτελεσματικό στην αναγνώριση των επιθέσεων και ειδικά στην διαρροή των δεδομένων στο πλαίσιο του *Android*. **[22]**

5.4 *I-Code:* Η Αναγνώριση Κακόβουλου Κώδικα σε Πραγματικό Χρόνο (*Real-time)*

Τα δίκτυα συνήθως μαστίζονται από κακόβουλα προγράμματα που μεταδίδονται από τον έναν υπολογιστή στον άλλο. Αυτά τα προγράμματα που ονομάζονται *worms, viruses, shellcodes* προσπαθούν να εισδύσουν και να εκθέσουν σε κίνδυνο απομακρυσμένους υπολογιστές, ανακαλύπτοντας τις αδυναμίες τους. Μόλις ένας υπολογιστής υποστεί επίθεση, μπορεί να χρησιμοποιηθεί σε ένα ευρύ πεδίο παράνομων ενεργειών που περιλαμβάνουν τον εκβιασμό, τις επιθέσεις άρνησης παροχής υπηρεσίας (*DoS*), την αποστολή *spam* και ψεύτικου λογισμικού (*fraud*), την εγκατάσταση στον υπολογιστή παράνομου υλικού.

Το *i-Code* είναι ένα διετές *project* έρευνας που αποσκοπεί στην υλοποίηση ενός ενσωματωμένου εργαλείου ανίχνευσης και αναγνώρισης του κακόβουλου λογισμικού σε πραγματικό χρόνο *(real time).* Το εργαλείο (που ολοκληρώνεται με μια ενσωματωμένη κονσόλα) μπορεί να βοηθήσει τους διαχειριστές δικτύων και τους δικανικούς αναλυτές που θέλουν να ερευνήσουν ένα περιστατικό που εμπλέκει κακόβουλο λογισμικό.

Έχοντας αναγνωρίσει την πρόκληση που δημιουργούν οι αυξημένες ταχύτητες των δικτύων στην ανίχνευση των επιθέσεων, το *i-Code* αντιμετωπίζει αυτή την πρόκληση υλοποιώντας μια αρχιτεκτονική *I/O* που αποφεύγει κοινές περιπτώσεις συνωστισμού, αναμορφώνοντας την λογική της ροής δεδομένων στον χρόνο φόρτωσης της εφαρμογής ώστε να ταιριάξει με το φόρτο έργου και να εκμεταλλευτεί υλικό ειδικού σκοπού. Τα δύο συστατικά της αρχιτεκτονικής *I/O* που είναι σημαντικά για την απόδοση είναι ***η επεξεργασία*** *(processing)* και ***η αποθήκευση*** *(buffering)*. Για την επεξεργασία, *το i-Code* επαναχρησιμοποιεί το γνωστό μοντέλο των *streams* και των φίλτρων. Για την αποθήκευση, χρησιμοποιεί ένα σύστημα διαχείρισης *buffers* στο οποίο όλα τα ζωντανά δεδομένα φυλάσσονται σε κυκλικούς *buffers* και οι *buffers* μοιράζονται μεταξύ των τομέων προστασίας *(protection domains).*

Η προσέγγιση ανίχνευσης του *i-Code* έχει τρείς άξονες, με δύο ανιχνευτές επιπέδου δικτύου *(NEMU* και *Argos)* και έναν ανιχνευτή σε επίπεδο υπολογιστή *(AccessMiner),* ενσωματωμένους σε μια κονσόλα η οποία επίσης συσχετίζει τα αποτελέσματα μαζί με μια ανάλυση *shellcode* που δίνεται από τον «σάκο πυγμαχίας» (*sandbox*) *Anubis*.

Το *NEMU* είναι ένα εργαλείο που διενεργεί *emulation* σε επίπεδο δικτύου, μια ευρετική μέθοδος ανίχνευσης *(κεφ. 2.2.4)* που σαρώνει την κυκλοφορία του δικτύου για να ανιχνεύσει πολυμορφικές επιθέσεις. Το *NEMU* χρησιμοποιεί έναν *CPU emulator* για να αναλύει δυναμικά κάθε πιθανή ακολουθία εντολών στην ελεγχόμενη κυκλοφορία και προσπαθεί να αναγνωρίσει την συμπεριφορά εκτέλεσης συγκεκριμένων ομάδων κακόβουλου λογισμικού, όπως το αυτοαποκρυπτογραφημένο πολυμορφικό *shellcode*. Οι επιτιθέμενοι που προσπαθούν να κρύψουν το *malware* μέσα σε εισερχόμενα δικτυακά πακέτα που φαίνονται φυσιολογικά, αποκαλύπτονται εύκολα από το *NEMU*. Συμπληρωμένο με το *Anubis*, που είναι ένας «σάκος πυγμαχίας» δυναμικής ανάλυσης *malware*, το *NEMU* είναι ικανό όχι μόνο να ανιχνεύσει αλλά και να αξιολογήσει με ακρίβεια τις εισερχόμενες επιθέσεις.

Το *Argos* είναι ένας πλήρης και ασφαλής *system emulator* σχεδιασμένος για χρήση σε συστήματα παγίδας (*honeypots*). Βασίζεται στο *Qemu*, αλλά έχει επεκταθεί για να ανιχνεύει απομακρυσμένες προσπάθειες επίθεσης σε λειτουργικά συστήματα. Χρησιμοποιώντας δυναμική ανάλυση, ανιχνεύει δικτυακά δεδομένα κατά τη διάρκεια της εκτέλεσης και αναγνωρίζει κάθε προσπάθεια να χρησιμοποιηθούν με παράνομο τρόπο.

Το *AccessMiner* είναι ένα εργαλείο για την ανάλυση κλήσεων συστήματος που συλλέγονται σε υπολογιστές που εκτελούν εφαρμογές χρηστών και διαφοροποιούνται από τις κλήσεις συστημάτων *malware*. Έχει σχεδιαστεί για μεγάλης κλίμακας συλλογή και κεντρική ανάλυση σε πραγματικά δίκτυα.

Το *Anubis* είναι ένα σύστημα δυναμικής ανάλυσης *malware* βασισμένο σε έναν *emulator Qemu*. Προσφέρεται σαν μια ανοιχτή υπηρεσία μέσω ενός δημόσιου ιστοχώρου, όπου οι χρήστες μπορούν να υποβάλλουν εκτελέσιμα για ανάλυση, και λαμβάνουν μια αναφορά που περιγράφει τη συμπεριφορά του δείγματος με έναν αναγνώσιμο τρόπο. Για το *i-Code*, το *Anubis* έχει επεκταθεί ώστε να υποστηρίζει ανάλυση και αξιολόγηση του *shellcode*.

Η κονσόλα είναι σχεδιασμένη για να συλλέγει γεγονότα που παράγονται από αυτά τα συστήματα, περνούν για ανάλυση το *shellcode* που δημιουργείται στο «σάκο πυγμαχίας» του *Anubis* και ενσωματώνει τα αποτελέσματα σε μια μορφή εύκολη στη χρήση. Είναι επίσης σχεδιασμένο να επεκτείνεται εύκολα με άλλα συστήματα ανίχνευσης με χρήση προτύπων ανοιχτής επικοινωνίας.

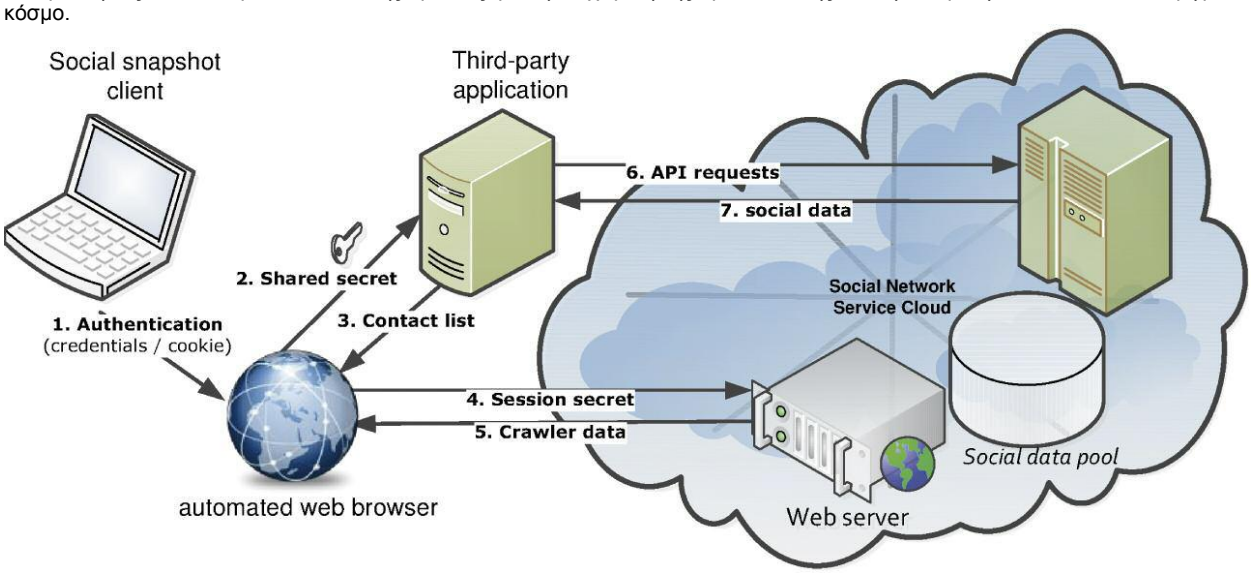
Τα τελικά αποτελέσματα αυτού του *project* παρουσιάστηκαν στις Βρυξέλες το 2012 σε ένα συνέδριο, που το παρακολούθησαν πάνω από 40 μέλη δικανικής ψηφιακής ανάλυσης της Ευρωπαϊκής κοινότητας. **[23]**

5.5 Η Αναζήτηση Ηλεκτρονικών Εγκλημάτων σε *Online* Κοινωνικά Δίκτυα

Τα τελευταία χρόνια τα *online* κοινωνικά δίκτυα *(Online Social Networks, OSN)* αποτελούν τους μεγαλύτερους και ταχύτερα αναπτυσσόμενους ιστοχώρους στο διαδίκτυο. Τα *OSN*, όπως το *Facebook* ή το *LinkedIn* περιέχουν ευαίσθητα και προσωπικά δεδομένα εκατοντάδων εκατομμυρίων ανθρώπων και ενσωματώνονται σε εκατομμύρια άλλους ιστοχώρους. Τα *OSN* συνεχίζουν να αντικαθιστούν τους παραδοσιακούς τρόπους ψηφιακής αποθήκευσης, ανταλλαγής και επικοινωνίας. Η συλλογή αυτού του τύπου των δεδομένων είναι επομένως ένα σημαντικό πρόβλημα στο πεδίο της δικανικής ψηφιακής ανάλυσης. Ενώ η παραδοσιακή ψηφιακή δικανική ανάλυση βασίζεται στην ανάλυση των αρχείων συστήματος, της δικτυακής κυκλοφορίας και των αρχείων καταγραφής, απαιτούνται νέες προσεγγίσεις για την εξαγωγή δεδομένων από τα *OSN* ή από τις υπηρεσίες *cloud*.

Η προσέγγιση που θα περιγράψουμε βασίζεται σε ένα υβριδικό σύστημα που χρησιμοποιεί έναν αυτοματοποιημένο *web browser* σε συνδυασμό με μια εφαρμογή *OSN* τρίτου μέρους *(third party application).* Το σύστημα αυτό μπορεί να χρησιμοποιηθεί αποτελεσματικά για να συλλέξει «κοινωνικά στιγμιότυπα», ακολουθίες δεδομένων οι οποίες περιλαμβάνουν δεδομένα του χρήστη και σχετικές πληροφορίες από το κοινωνικό δίκτυο. Οι ακολουθίες δεδομένων που συλλέγει το εργαλείο περιέχουν πληροφορίες προφίλ (δεδομένα του χρήστη, ιδιωτικά μηνύματα, φωτογραφίες κ.λπ.) και σχετιζόμενα *meta-data* (εσωτερικές ετικέτες χρόνου και μοναδικά αναγνωριστικά-*identifiers*). Υλοποιήθηκε ένα πρωτότυπο για το *Facebook* και αξιολόγησε το σύστημα με έναν αριθμό εθελοντών.

Το ***σχήμα 37*** παρουσιάζει τις βασικές εφαρμογές του πλαισίου του κοινωνικού στιγμιότυπου. **(1)** Ο πελάτης του κοινωνικού στιγμιότυπου αρχικοποιείται παρέχοντας τα διαπιστευτήρια του χρήστη (*credentials*). Το εργαλείο που δημιουργήθηκε ξεκινάει σε αυτό το σημείο τον αυτοματοποιημένο *browser* με το δεδομένο μηχανισμό αυθεντικοποίησης. **(2)** Ο αυτοματοποιημένος *browser* προσθέτει την εφαρμογή στιγμιότυπου στο προφίλ του χρήστη που αποτελεί στόχο και στέλνει το κοινό μυστικό *Application Programming Interface* (*API)* στον εξυπηρετητή της εφαρμογής. **(3)** Το στιγμιότυπο της εφαρμογής απαντά με τη λίστα επαφών του χρήστη. **(4)** Ο αυτοματοποιημένος *web browser* ζητάει συγκεκριμένες ιστοσελίδες από το προφίλ του χρήστη και από τη λίστα επαφών του. **(5)** Τα λαμβανόμενα δεδομένα διαπερνώνται και αποθηκεύονται. **(6)** Καθώς ο αυτοματοποιημένος *browser* ζητάει συγκεκριμένες ιστοσελίδες, η εφαρμογή του στιγμιότυπου συλλέγει προσωπικές πληροφορίες μέσω του *OSN API*. **(7)** Τελικά τα δεδομένα που έχουν συλλεχθεί από την εφαρμογή τρίτου μέρους αποθηκεύονται στον εξυπηρετητή της εφαρμογής του στιγμιότυπου.



Σχήμα 37: Συλλογή ψηφιακών αποδείξεων μέσω του πλαισίου κοινωνικού στιγμιότυπου

Για να αποκτηθεί πρόσβαση στο πλήρες περιεχόμενο του λογαριασμού του χρήστη του κοινωνικού δικτύου, τα κοινωνικά στιγμιότυπα βασίζονται στη συλλογή του αρχικού σημείου αυθεντικοποίησης *(authentication token).* Στη συνέχεια θα αναφερθούν τρία σενάρια ψηφιακής δικανικής ανάλυσης, αντιπροσωπευτικά περιπτώσεων που βρίσκονται στον πραγματικό κόσμο που απεικονίζουν την συλλογή του *authentication token.*

Συναίνεση: Αυτή η αφελής προσέγγιση απαιτεί την συναίνεση από το πρόσωπο του οποίου αναλύεται το κοινωνικό δικτυακό προφίλ. Ένα άτομο θα μπορούσε να δώσει σε έναν ψηφιακό δικανικό αναλυτή προσωρινή πρόσβαση στο λογαριασμό κοινωνικής δικτύωσης που διατηρεί, για να δημιουργήσει ένα στιγμιότυπο. Αυτή θα μπορούσε επίσης να είναι η προτιμώμενη μέθοδος ώστε να διενεργηθεί η έρευνα με ηθικό τρόπο και σύμφωνα με τους νόμους περί ιδιωτικότητας.

***Πειρατεία συνόδων κοινωνικής δικτύωσης*:** Η εφαρμογή του κοινωνικού στιγμιότυπου που παρουσιάστηκε, παρέχει μια μονάδα για πειρατεία εγκατεστημένων συνόδων κοινωνικής δικτύωσης. Ένας ερευνητής θα μπορούσε να παρακολουθεί τη σύνδεση δικτύου του χρήστη για έγκυρα *authentication tokens*, για παράδειγμα μη κρυπτογραφημένες συνδέσεις *WiFi* ή *LAN*. Μόλις η μονάδα πειρατείας βρει ένα έγκυρο *authentication token*, η εφαρμογή στιγμιότυπου παράγει μια ξεχωριστή σύνοδο για να αντιγράψει τον λογαριασμό του χρήστη.

Εξαγωγή από την εικόνα δικανικής ανάλυσης: Τελικά, θα μπορούσε να χρησιμοποιηθεί η φυσική πρόσβαση στον υπολογιστή του χρήστη για να εξαχθούν τα έγκυρα *authentication cookies* από τους *web browsers*. Τα αποθηκευμένα *authentication cookies* μπορούν να βρεθούν αυτόματα ψάχνοντας στην εικόνα ενός σκληρού δίσκου ή σε τεχνικές ανάλυσης.

Τα κοινωνικά στιγμιότυπα ερευνούν νέες τεχνικές αυτοματοποιημένης συλλογής ψηφιακών αποδείξεων από υπηρεσίες κοινωνικής δικτύωσης. Συγκρινόμενες με τις τεχνικές *web crawling*, η προσέγγιση που παρουσιάστηκε μειώνει σημαντικά την κυκλοφορία στο δίκτυο, συντηρείται πιο εύκολα και έχει πρόσβαση σε πρόσθετη και κρυμμένη πληροφορία. Εκτεταμένες αξιολογήσεις αυτών των τεχνικών έδειξαν ότι είναι πρακτικές και αποτελεσματικές στη συλλογή πλήρους πληροφορίας από έναν συγκεκριμένο λογαριασμό κοινωνικής δικτύωσης, σχετικά γρήγορα και χωρίς να ανιχνευθούν από τους παρόχους του κοινωνικού δικτύου. Οι τεχνικές αυτές μπορούν να

χρησιμοποιηθούν όπου δεν υπάρχει νόμιμη συνεργασία με τους παρόχους του κοινωνικού δικτύου. Το εργαλείο και οι τεχνικές που παρουσιάστηκαν, παρέχονται ως ανοικτό λογισμικό για να βοηθήσουν στη συλλογή ψηφιακών αποδείξεων από κοινωνικά δίκτυα. **[24]**

5.6 Σύστημα Απεικόνισης των Γεγονότων Ασφάλειας στα Δίκτυα Υπολογιστών

Η απεικόνιση παρέχει τα μέσα για αναπαράσταση και κατανόηση μεγάλου όγκου δεδομένων με ένα σύνθετο και καλαίσθητο τρόπο, επιτρέποντας στους χειριστές να χειρίζονται μεγάλους όγκους δεδομένων πιο εύκολα. Στο πεδίο της παρακολούθησης των γεγονότων δικτυακής ασφάλειας, η απεικόνιση παρέχει πλεονεκτήματα για τις παρακάτω δραστηριότητες:

Εποπτεία σε πραγματικό χρόνο *(real time supervision):* ***Τα εργαλεία απεικόνισης*** *(visualization tools)* δίνουν έμφαση και προτεραιότητα στα κακόβουλα γεγονότα που έχουν ανιχνευθεί. Επίσης παρέχουν επίγνωση της κατάστασης, δηλ. γενική πληροφορία για το τι συμβαίνει στο σύστημα. Στην περίπτωση αυτή, η απεικόνιση σπάνια παρέχει πληροφορίες αλλά αντίθετα παρέχει μια γενική εικόνα του συστήματος.

Δικανική ανάλυση: Τα εργαλεία απεικόνισης επιτρέπουν στους χειριστές να ψάχνουν διάφορες πηγές δεδομένων για πληροφορίες σχετικά με το τι έγινε στο σύστημα. Τα απεικονιστικά εργαλεία εξόρυξης δεδομένων συχνά χρησιμοποιούνται σε ένα υποσύνολο δεδομένων, όπου αυτό το υποσύνολο έχει επιλεγεί βάσει της ανίχνευσης κακόβουλων και ανώμαλων δραστηριοτήτων.

Γρήγορη αντίδραση: Τα εργαλεία απεικόνισης βοηθούν το διαχειριστή να αντιδράσει γρήγορα όταν αντιμετωπίσει γεγονότα ασφάλειας, δηλ. αναμορφώνοντας ένα τείχος προστασίας ή αναπτύσσοντας αυτόματα ένα διορθωτικό τμήμα κώδικα (*patch*) σε αδύναμα συστήματα. Η απεικόνιση για γρήγορη αντίδραση, συχνά παρέχει συμπληρωματική πληροφορία σχετικά με την κατάσταση του δικτύου και των πολιτικών ασφάλειας.

Επικοινωνία: Τα εργαλεία απεικόνισης βοηθούν τους διαχειριστές να εξηγήσουν τις καταστάσεις με μεγαλύτερη σαφήνεια. Οι παραγόμενες απεικονίσεις μπορούν να χρησιμοποιηθούν για εσωτερικούς σκοπούς (για ενίσχυση των συστημάτων *ticketing*) ή για εξωτερικούς σκοπούς (βελτίωση των επικοινωνιών).

Πολλά εργαλεία απεικόνισης μπορούν να χρησιμοποιηθούν για την παρακολούθηση των γεγονότων δικτυακής ασφάλειας. Κάποια από αυτά είναι πολύ γενικά και προσφέρουν αναπαραστάσεις παρόμοιες με αυτές που χρησιμοποιούνται στα παραδοσιακά φύλλα λογισμικού (*spreadsheet*) δηλ. *bar charts, pie charts, radar graphs, tree maps* κ.λπ. Άλλα εργαλεία, είναι πολύ συγκεκριμένα, και λαμβάνουν υπόψη τους ειδικούς τύπους δεδομένων για να προσφέρουν περισσότερο εξειδικευμένες αναπαραστάσεις. Για παράδειγμα, το *Network Visualizer (TVN)* χρησιμοποιεί αρχεία σύλληψης πακέτων (*pcap*) για να αναπαραστήσει ροές δικτυακής επικοινωνίας.

Κατά συνέπεια, οι διαχειριστές που παρακολουθούν τα δίκτυα ή οι αναλυτές που εκτελούν δικανική ανάλυση δεσμεύονται είτε να χρησιμοποιήσουν συγκεκριμένα εργαλεία και να ελπίζουν ότι θα ικανοποιήσουν τις ανάγκες τους, είτε να χρησιμοποιήσουν πολύ γενικά εργαλεία και να θυσιάσουν την ακρίβεια και το γενικό πλαίσιο. Για να εκτελεστεί σωστά, η δεύτερη λύση απαιτεί ο χρήστης να έχει εξειδίκευση όχι μόνο στην ασφάλεια των δικτύων αλλά επίσης και στην ανάλυση δεδομένων και στον οπτικό σχεδιασμό πληροφορίας. Στην πραγματικότητα, η εύρεση της κατάλληλης απεικόνισης για ένα συγκεκριμένο σύνολο δεδομένων απαιτεί την επιλογή της καλύτερης οπτικής απεικόνισης του πλαισίου των δεδομένων και των αντικειμένων. Η

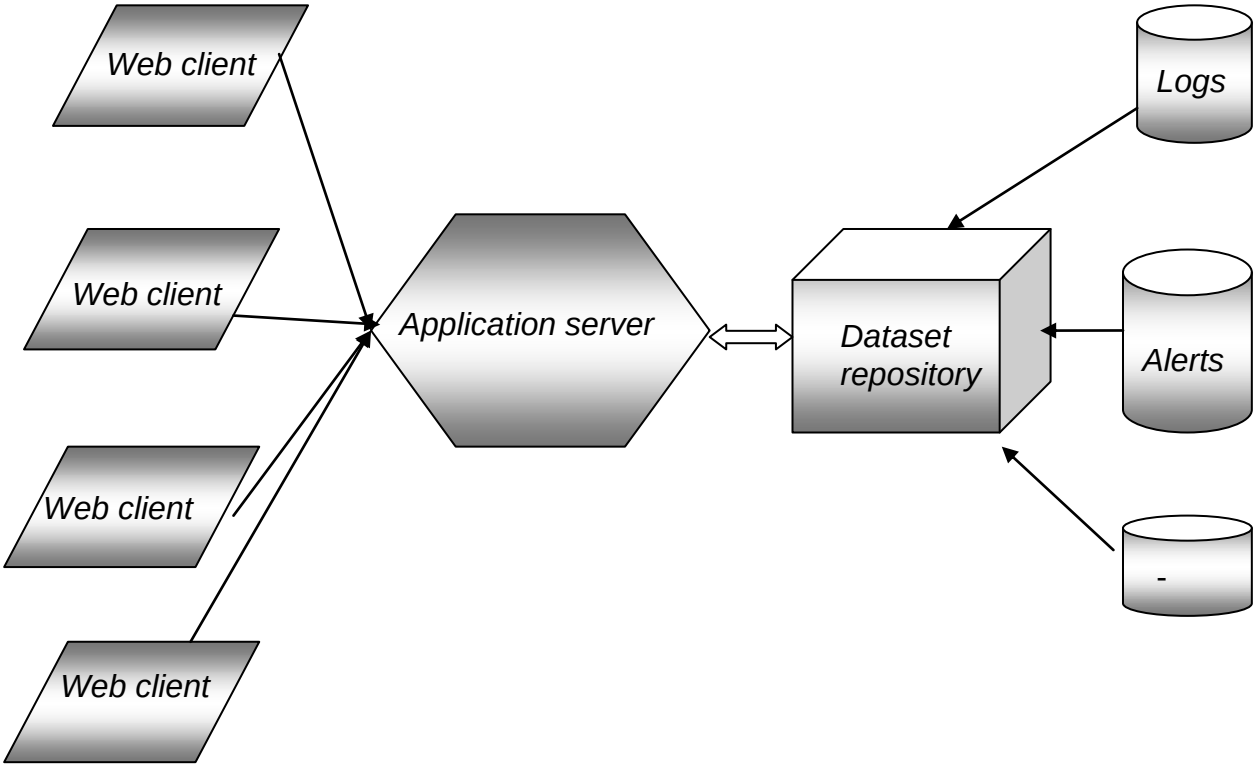
επιλογή της σωστής αναπαράστασης απαιτεί πολύ χρόνο και εμπειρία για τους ειδικούς της ασφάλειας, ειδικά όταν δεν υπάρχει υπόβαθρο στην απεικόνιση ή στα στατιστικά.

Η ομάδα εργασίας της απεικόνισης της ασφάλειας στην *CIDre* ομάδα, εργάζεται σε ένα σύστημα που βοηθά τους ειδικούς ασφάλειας στη διαχείριση και διερεύνηση των δεδομένων που σχετίζονται με την ασφάλεια. Ο σκοπός είναι να επιτρέψουν στους χρήστες να παρακολουθούν και να ερευνούν τα δεδομένα με έναν τρόπο όσο το δυνατόν φιλικό στο χρήστη. Στην ιδεατή κατάσταση, ο χρήστης δεν χρειάζεται απαραίτητα να είναι ειδικός στο σχεδιασμό ή στην απεικόνιση. Ένας από τους σκοπούς, είναι να επιτρέψουν στο σύστημα να παράγει αυτόματα τις επαρκείς απεικονίσεις σύμφωνα με τα τρέχοντα δεδομένα και τα οπτικά πλαίσια και τους σκοπούς του χρήστη. Μόνο ο χρήστης γνωρίζει τις διαθέσιμες πηγές των δεδομένων και δρα με αυτά με φυσικό τρόπο. Επομένως, λεπτομέρειες σχετικά με τις αιτήσεις που γίνονται στα σύνολα των δεδομένων θα πρέπει να αποκρυβούν. Προς αυτή την κατεύθυνση, γίνονται αυτοματοποιημένες μεταφράσεις των στόχων και των προθέσεων από το χρήστη σε παραδοσιακές εντολές των βάσεων δεδομένων, όπως για παράδειγμα της *SQL*. Το σύστημα που δημιουργήθηκε επίσης επιλέγει αυτόματα τις αναπαραστάσεις που ταιριάζουν καλύτερα στους σκοπούς του χρήστη. Τέλος, επειδή η δικανική ψηφιακή επιστήμη είναι μια διαδραστική διεργασία από τη φύση της, δίνεται ιδιαίτερη σημασία στις αλληλεπιδράσεις μεταξύ του χρήστη και των δεδομένων μέσω δυναμικών τρόπων αναπαράστασης.

Μολονότι η αποτελεσματική απεικόνιση είναι συχνά ένα πρόβλημα που έχει επίκεντρο το χρήστη, είναι σημαντικό να χτιστεί ένα απαντητικό και αποδοτικό σύστημα, όταν έχουμε να κάνουμε με μεγάλο αριθμό δεδομένων ασφάλειας. Σχετικά με αυτό το θέμα, παρουσιάζεται η αρχιτεκτονική του ***σχήματος 38***, που είναι προσανατολισμένη στο *web*:

1. ***Η αποθήκη των δεδομένων (dataset repository),*** συλλέγει, αποθηκεύει, κατατάσσει και εξυπηρετεί τις απαιτούμενες αιτήσεις πάνω σε αυτά τα δεδομένα (αρχεία καταγραφής, *snort alert* κ.λπ.),
2. ***Ο εξυπηρετητής της εφαρμογής (application server),*** προσπελαύνει την αποθήκη δεδομένων και εξυπηρετεί τις εφαρμογές *web* και δίνει στοιχεία σε πολλούς τελικούς χρήστες,
3. ***Η εφαρμογή web*** διατηρεί συστατικά δικτύου για αιτήσεις δεδομένων και μόνιμες συνδέσεις και έχει τις ίδιες ικανότητες αποθήκευσης (*caching*) και επεξεργασίας.
4. Στο τελικό επίπεδο, μετά την κύρια λογική της εφαρμογής, βρίσκονται ***τα συστατικά της απεικόνισης (visualization contents)*** που χρησιμοποιούνται για την αναπαράσταση και την αλληλεπίδραση με τα δεδομένα.

Προτείνοντας νέους τρόπους αλληλεπίδρασης με τα δεδομένα ασφάλειας μαζί με μια αποτελεσματική αρχιτεκτονική, είναι πιθανό να προσφερθεί μια επιλογή απεικόνισης περισσότερο αποδοτική και ευέλικτη που θα ερευνά και θα παρακολουθεί τα γεγονότα που σχετίζονται με την ασφάλεια. **[25]**



Σχήμα 38: Η αρχιτεκτονική του συστήματος απεικόνισης

5.7 *Domain-Specific* Γλώσσες Προγραμματισμού (*DSL*) για Χρήση Δικανικών Ψηφιακών Εργαλείων

Ένα σημαντικό μέρος της ψηφιακής δικανικής ανάλυσης αποτελεί η ανάκτηση των αποδείξεων από τις ψηφιακές συσκευές. Αυτό περιλαμβάνει, ανάκτηση εικόνων, εγγράφων *text* και μηνυμάτων ηλεκτρονικού ταχυδρομείου σχετικών με την δικανική έρευνα. Τέτοιου είδους έρευνες βασίζονται πολύ σε λογισμικό φτιαγμένο για πελάτες, το οποίο συχνά πρέπει να μετατραπεί ανάλογα με την περίπτωση. Επιπλέον, πρέπει να αναβαθμιστεί για να μπορέσει να χειριστεί όγκο δεδομένων που πλησιάζει το *terabyte*. Το *CWI* εφαρμόζει υψηλού επιπέδου εργαλεία δημιουργίας γλώσσας και τεχνικές για την κατασκευή και την συντήρηση τέτοιου λογισμικού, που θα έχει λιγότερα λάθη και θα είναι λιγότερο χρονοβόρο.

Μια περιοχή εφαρμογής του λογισμικού της δικανικής ψηφιακής ανάλυσης, είναι η ***αναπαράσταση των αρχείων*** *(file carving),* δηλαδή η διεργασία ανάκτησης των αρχείων από μια ψηφιακή συσκευή χωρίς τη χρήση μεταδεδομένων (*metadata*) του συστήματος αρχείων. Η αναπαράσταση των αρχείων χρησιμοποιείται, για παράδειγμα, για την ανάκτηση φωτογραφιών παιδικής πορνογραφίας, ακόμα κι αν ο ύποπτος έχει προσπαθήσει να τις σβήσει. Επίσης, εξ αιτίας του κατακερματισμού (*fragmentation*), ένα αρχείο μπορεί να έχει διανεμηθεί μέσω μιας συσκευής σε πολλαπλά τμήματα. Τα εργαλεία αναπαράστασης των αρχείων, ταιριάζουν τις ακολουθίες των *bytes* ενός τύπου αρχείου και προσπαθούν να ανακατασκευάσουν το αρχικό αρχείο.

Οι τύποι των αρχείων *(file formats),* όπως *JPEG* (εικόνες), *ZIP* (αρχειοθετημένα, συμπιεσμένα) και *DOC* (έγγραφα) παίζουν σημαντικό ρόλο στην αναπαράσταση των αρχείων. Ορίζουν τη δομή που είναι απαραίτητη για να καθοριστεί αν ένα ακατέργαστο τμήμα αρχείου μπορεί να αποτελεί μέρος ενός πλήρους αρχείου ενός συγκεκριμένου τύπου. Οι τύποι των αρχείων υπάρχουν σε πολλές εκδόσεις και παραλλαγές ανάλογα με τον πάροχο. Η γνώση του τύπου του αρχείου είναι συνήθως συνυφασμένη με πολύπλοκους, βελτιστοποιημένους αλγόριθμους επανασυναρμολόγησης των τμημάτων των αρχείων.

Η *Derric*, είναι μια γλώσσα *domain-specific* σχεδιασμένη από το *CWI* που μπορεί να χρησιμοποιηθεί για να περιγράψει τύπους αρχείων. Αυτές οι περιγραφές χρησιμοποιούνται ως είσοδος σε μια γεννήτρια κώδικα, που παράγει αναπαραστάσεις αρχείων υψηλής απόδοσης. Αυτός ο τρόπος γνώσης των τύπων των αρχείων είναι απομονωμένος από τον αλγοριθμικό κώδικα αναπαράστασης του αρχείου. Οι ψηφιακοί δικανικοί αναλυτές μπορούν να εστιάσουν στην συντήρηση και εξέλιξη των περιγραφών των τύπων αρχείων, ενώ οι μηχανικοί λογισμικού εστιάζουν στην βελτιστοποίηση του συστήματος στο οποίο εκτελούνται οι περιγραφές.

Μια περιγραφή *Derric*, αποτελείται από τρία μέρη: την ***κεφαλίδα διαμόρφωσης*** *(configuration header),* ***το τμήμα ακολουθίας*** *(sequence section)* και μια ***λίστα ορισμών δομών*** *(structure definitions).* Η κεφαλίδα διαμόρφωσης δηλώνει τα *metadata* του τύπου του αρχείου όπως την έλλειψη τέλους (*endianness*), την έλλειψη σήματος (*signedness*) και τις κωδικοποιήσεις χαρακτήρων. Το τμήμα ακολουθίας περιγράφει τη δομή του αρχείου σε υψηλό επίπεδο χρησιμοποιώντας κανονική έκφραση. Τέλος, οι ενδείξεις (*tokens*) που χρησιμοποιούνται στην κανονική έκφραση αποτελούν το τμήμα δομών. Κάθε δομή προσδιορίζεται από ένα όνομα και περιέχει ένα ή περισσότερα πεδία. Τα περιεχόμενα και το μήκος κάθε πεδίου μπορεί να περιορίζονται αυθαίρετα ώστε να δρομολογήσουν τη διαδικασία ταιριάσματος. Το *Derric* είναι αρκετά εκφραστικό στην περιγραφή ενός μεγάλου πεδίου τύπων αρχείων.

Το *Derric* αξιολογήθηκε συγκρίνοντας παραγόμενες αναπαραστάσεις αρχείων με τις αληθινές αναπαραστάσεις που χρησιμοποιούνται στη δικανική πρακτική. Τα αποτελέσματα έδειξαν ότι οι αναπαραστάσεις αρχείων που έγιναν από το *Derric* είχαν απόδοση εξίσου καλή με τις αναπαραστάσεις άλλων εργαλείων. Το *Derric* έχει υλοποιηθεί σε *Rascal*, μια γλώσσα μεταπρογραμματισμού (*metaprogramming*) και η υλοποίησή του είναι σχετικά μικρή. Περίπου 2000 γραμμές *Rascal* και μια βιβλιοθήκη 4200 γραμμών σε κώδικα *Java*. Έτσι, το κόστος συντήρησης της υλοποίησης της *DSL (Domain Specific Language)* είναι αποδεκτό.

Ένα πρόσθετο πλεονέκτημα της περιγραφής τύπων αρχείων με ορισμούς χρησιμοποιώντας το *Derric*, είναι ότι οι περιγραφές μπορούν να μετασχηματιστούν πριν περάσουν στη γεννήτρια κώδικα. Έχουν υλοποιηθεί τρεις μετασχηματισμοί για την διαδοχική προμήθεια αναπαραστάσεων που είναι πιο αποδοτικοί. Σε κάποιες περιπτώσεις δικανικής ανάλυσης, είναι πιο αποτελεσματικό να γίνει κάποιος συμβιβασμός σε επίπεδο ακρίβειας για να πάρουμε τα αποτελέσματα πιο γρήγορα. Εφόσον οι μετασχηματισμοί είναι αυτοματοποιημένοι, αυτή η συναλλαγή μπορεί να γίνει χωρίς να αλλάξει ο κώδικας. Η αξιολόγηση της επίδρασης των μετασχηματισμών έγινε σε μια εικόνα δοκιμής μεγέθους 1*TB*. Τα αποτελέσματα έδειξαν ότι η απόδοση αυξάνεται με έναν παράγοντα 3, όταν μειώνεται η ακρίβεια κατά 8%.

Οι ψηφιακές δικανικές αναλύσεις, βασίζονται σημαντικά στο λογισμικό. Οι *DSL* μπορούν να βοηθήσουν στο πεδίο των δικανικών αναλύσεων. Το *Derric* είναι ένα σημαντικό βήμα προς αυτή την κατεύθυνση: διαχωρίζοντας την περιγραφή του τύπου των αρχείων από

τον τρόπο που χρησιμοποιούνται στην υλοποίηση, τα δικανικά εργαλεία γίνονται πιο εύκολα μετατρέψιμα. Επιπλέον, το μοντέλο του μετασχηματισμού παρέχει ευκαιρίες για διαμόρφωση συναλλαγών που μπορούν να βοηθήσουν στην δικανική ανάλυση. **[26]**

5.8 Η Διατήρηση των Ευαίσθητων προσωπικών Δεδομένων κάτω από τον Έλεγχο του Ενδιαφερόμενου

Ένας μεγάλος αριθμός προσωπικών δεδομένων συλλέγεται σε εξυπηρετητές από διοικήσεις, νοσοκομεία, εταιρείες ασφάλειας κ.λπ. Επίσης οι έξυπνες συσκευές που υπάρχουν παντού γύρω μας παράγουν διαφανώς ευαίσθητες χωροχρονικές πληροφορίες (π.χ. η παρακολούθηση της υγείας, τα έξυπνα κτήρια, τα διόδια). Στο μεταξύ, ολοένα και περισσότερα ψηφιοποιημένα δεδομένα παραδίδονται στο χρήστη (φόρμες μισθοδοσίας, δελτία τηλεφωνικής εταιρείας, δελτία τραπεζών κ.α.). Ενώ τα πρωτότυπα αυτών των δεδομένων φυλάσσονται στα πληροφοριακά συστήματα του εκδότη, οι πολίτες συχνά βασίζονται στις εταιρείες διαδικτύου για να αποθηκεύσουν με αξιοπιστία ένα δεύτερο αντίγραφο και να το έχουν *online*. Δυστυχώς υπάρχουν πολλά παραδείγματα παραβίασης της ιδιωτικότητας ξεκινώντας από αμέλεια, κατάχρηση ή επίθεση και τελικά κανένας εξυπηρετητής δεν είναι ασφαλής.

Θα παρουσιαστεί εδώ μια όψη της διαχείρισης των προσωπικών δεδομένων ριζικά διαφορετική και ιδιαίτερα αποκεντρωμένη. Σχεδιάστηκε πάνω στην εμφάνιση νέων συσκευών που ονομάζονται *Secure Tokens* και συνδυάζουν την ασφάλεια των έξυπνων καρτών και την ικανότητα αποθήκευσης των *NAND Flash chips* (δηλ. *SIM* καρτών υψηλής χωρητικότητας, ασφαλών *USB sticks*). Ο πρωτοφανής συνδυασμός φορητότητας, ασφάλειας και μαζικής χωρητικότητας δίνει τα εχέγγυα για μια πραγματική επανάσταση στη διαχείριση των προσωπικών δεδομένων.

Η ιδέα είναι να ενσωματωθούν μέσα στα *Secure Tokens*, στοιχεία λογισμικού ικανά να αποκτήσουν, να αποθηκεύσουν και να διαχειριστούν με ασφάλεια τα προσωπικά δεδομένα. Αυτό δημιουργεί έναν πλήρη εξυπηρετητή προσωπικών δεδομένων (*Personal Data Server, PDS)* που παραμένει κάτω από τον έλεγχο του κατόχου. Το *PDS* δεν είναι απλά μια αποθήκη (*repository*) προσωπικών δεδομένων. Θα πρέπει να επιτρέπει την ανάπτυξη δυνατών εφαρμογών που επιπλέον είναι επικεντρωμένες στο χρήστη και διατηρούν την ιδιωτικότητα των προσωπικών δεδομένων. Τα παραπάνω απαιτούν μια καλά οργανωμένη αναπαράσταση των δεδομένων που μπορεί να αποκτηθεί με ερωτήσεις (*queries*). Θα πρέπει επίσης να παρέχει στον κάτοχο των δεδομένων, έναν φιλικό τρόπο ελέγχου των συνθηκών διαμοιρασμού που σχετίζονται με τα δεδομένα του. Τα *PDS* θα πρέπει επίσης να παρέχουν τις παραδοσιακές υπηρεσίες βάσεων δεδομένων, όπως είναι η αντοχή και οι δυνατότητες ερωτήσεων (*queries*) και θα πρέπει να είναι ικανά να λειτουργήσουν μαζί με εξωτερικές πηγές δεδομένων με έναν ασφαλή τρόπο.

Με την κατάλληλη υποδομή, τα *PDS* παρουσιάζουν την εικόνα που βλέπουμε στο ***σχήμα 39***. Τα προσωπικά δεδομένα του ιδιώτη, που έχουν παραδοθεί και πιστοποιηθεί από διαφορετικές πηγές, στέλνονται στο *PDS* του, το οποίο μπορεί να εξυπηρετεί αιτήσεις από διάφορες εφαρμογές. Ενώ η προστασία των προσωπικών δεδομένων στην πλευρά του εκδότη θα παραμένει ανοιχτό πρόβλημα, τα *PDS* επιτρέπουν την εκτέλεση των εφαρμογών κάτω από τον πλήρη έλεγχο του ιδιώτη.

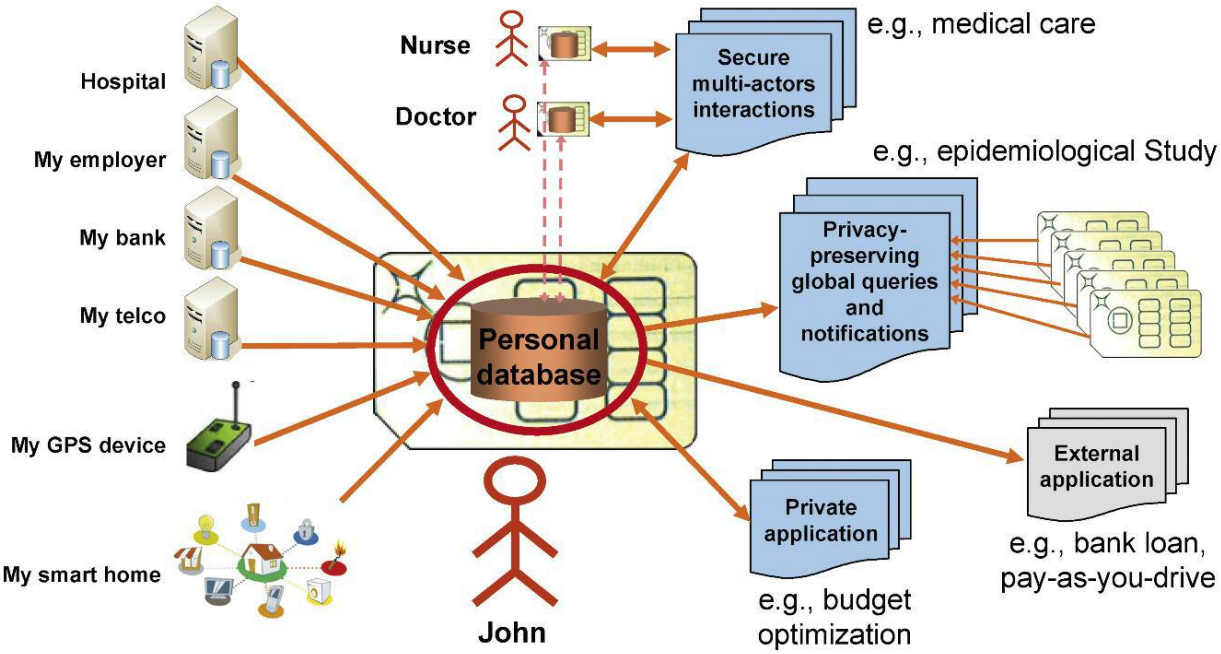
Οι ιδιωτικές εφαρμογές εκτελούνται από τον ίδιο τον κάτοχο και διατηρούν τα δικαιώματά του. Οι εξωτερικές εφαρμογές/υπηρεσίες δηλώνουν κανόνες συλλογής που ορίζουν ποιά δεδομένα απαιτούνται από τους κανόνες εταιρειών (για παράδειγμα μισθοδοσία και φορολογική πληροφορία για ένα δάνειο τράπεζας, στοιχεία από *GPS* για το σύστημα *PayAsYoyDrive).* Το *PDS* υπολογίζει το ελάχιστο ποσό δεδομένων που θα

πρέπει να σταλεί και το δείχνει στον κάτοχο ο οποίος τελικά μπορεί να δεχτεί ή να μη δεχτεί την υπηρεσία αυτή. Αντίστοιχα, η προέλευση των δεδομένων πιστοποιείται από το *PDS* και ελέγχεται από την υπηρεσία. Οι καθολικοί υπολογισμοί που διατηρούν την ιδιωτικότητα είναι διεργασίες μεγάλης κλίμακας στον πληθυσμό των *PDS* (για παράδειγμα, ένα σύνολο από ερωτήσεις για μια επιδημιολογική έρευνα), παρέχουν εγγυήσεις ιδιωτικότητας (για παράδειγμα διαφορική ιδιωτικότητα, κ-ανωνυμία) και επιβάλλονται από όλα τα *PDS* με έναν ασφαλή τρόπο πολλαπλών μερών (*multi party).* Τέλος, οι εφαρμογές που συνεργάζονται μπορούν να ανταλλάξουν προσωπικά δεδομένα μεταξύ των *PDS* (π.χ. ιατρικά δεδομένα των ασθενών ανταλλάσσονται μεταξύ των γιατρών, προσωπικοί φάκελοι ανταλλάσσονται μέσα σε μια κοινότητα συναδέλφων). Η κατάσταση διαμοιρασμού μπορεί να οριοθετείται στο χρόνο χάρη στους κανόνες κράτησης δεδομένων και να ελέγχεται αργότερα. Μπορούν να επιτευχθούν ασφαλή σενάρια συνεργασίας γιατί όλα τα *PDS* είναι έμπιστα και ανθεκτικά στις παραποιήσεις.

Η μετατροπή του οράματος των *PDS* σε πραγματικότητα εισάγει τρείς βασικές επιστημονικές προκλήσεις:

1. Θα πρέπει να σχεδιαστούν νέες τεχνικές βάσεων δεδομένων, που να χειρίζονται με αποτελεσματικό τρόπο τα ενσωματωμένα δεδομένα και να αντιμετωπίζουν τους περιορισμούς του υλικού (*hardware*) που είναι σύμφυτοι με τα *Secure Tokens,*
2. Θα πρέπει να παρέχεται ένα πλήρες και διαισθητικό μοντέλο που θα βοηθάει τους χρήστες να προστατεύσουν όλες τις πλευρές της ιδιωτικότητάς τους και να παρέχει αποδείξεις νομιμότητας για όλα τα δεδομένα που εισέρχονται ή φεύγουν από τα *PDS*,
3. Οι παραδοσιακές λειτουργίες ενός κεντρικού εξυπηρετητή θα πρέπει να εγκατασταθούν από την αρχή σε ένα άτυπο περιβάλλον συνδυάζοντας έναν μεγάλο αριθμό υψηλής ασφάλειας αλλά χαμηλής ισχύος *Secure Tokens* με μια ισχυρή αλλά χαμηλής ασφάλειας υποδομή.

Η προσέγγιση των *PDS* παρέχει μια αξιόπιστη εναλλακτική μέθοδο στη συστηματική συγκέντρωση των προσωπικών δεδομένων σε εξυπηρετητές και δείχνει το δρόμο σε νέες αρχιτεκτονικές που παρέχουν ιδιωτικότητα βάσει του σχεδιασμού. **[27]**



Σχήμα 39: Η αρχιτεκτονική του προσωπικού εξυπηρετητή δεδομένων

6. Ασφάλεια και Διαχείριση Εμπιστοσύνης

Η μοντέρνα κοινωνία βασίζεται ολοένα και περισσότερο στην αποθήκευση, επεξεργασία και μετάδοση πληροφοριών. Η διασφάλιση της ακεραιότητας, της ασφάλειας και της ιδιωτικότητας των πληροφοριών είναι πολύ σημαντική, ανεξάρτητα αν η πληροφορία βρίσκεται στο επίπεδο του πολίτη ή σε ένα εθνικό ή διεθνές επίπεδο. Επιπλέον, οι μελλοντικές τάσεις στον λεγόμενο ***Περιβάλλοντα Έξυπνο Χώρο*** *(Ambient Intelligent Space, AmI)* θα ενισχύσουν το ρόλο της πληροφορίας και την εξάρτησή μας από αυτή. Αυτή η κατάσταση φέρνει μεγάλες ευκαιρίες στην ενίσχυση της ποιότητας της ζωής μας, αλλά την ίδια στιγμή, παρουσιάζει μεγάλες προκλήσεις όσον αφορά στην ιδιωτικότητα και στην ακεραιότητα των προσωπικών πληροφοριών.

Υπάρχει μια κοινή αίσθηση ότι επιτυγχάνοντας μεγαλύτερη ασφάλεια στην τεχνολογία της πληροφορίας και των επικοινωνιών *(Information and Communication Technology, ICT)*, αυξάνονται η ανάπτυξη και η διάδοσή τους, με συνακόλουθα αποτελέσματα σε πολλά πεδία. Καθώς αυτή η τεχνολογία εξαπλώνεται ραγδαία, θα είναι δυνατό να μεταφράζουμε τις φυσικές μας αλληλεπιδράσεις με ηλεκτρονικές αν υπάρχει αρκετή εμπιστοσύνη και αυτοπεποίθηση στα συστήματα που επεξεργάζονται την πληροφορία.

Η ακεραιότητα, η ασφάλεια και η ιδιωτικότητα της πληροφορίας είναι επομένως σημαντικές, σε οτιδήποτε, από την μετάδοση της προσωπικής πληροφορίας μέχρι τις κυβερνητικές και βιομηχανικές υποδομές. Η απουσία της εμπιστοσύνης στα συστήματα θα επηρεάσει την διάδοσή της. Επομένως, η υλοποίηση και η ανάπτυξη συστημάτων με δυνατή και αποτελεσματική ασφάλεια είναι ζωτικής σημασίας.

Επιπρόσθετα, τα μοντέρνα συστήματα *ICT* μπορεί να αποτελούνται από αρκετούς (χιλιάδες και περισσότερους) υπολογιστικούς και επικοινωνιακούς πόρους των οποίων ο αριθμός αλλάζει δυναμικά και έτσι συχνά ομοιάζουν και ονομάζονται εικονικές κοινότητες. Σε αυτό το νέο πλαίσιο, η ικανότητα αναπαράστασης, δημιουργίας, διαπραγμάτευσης, παρακολούθησης και εξέλιξης σχέσεων εμπιστοσύνης με έναν ασφαλή τρόπο, γίνεται υποχρεωτική.

Η εμπιστοσύνη και η ασφάλεια στην κοινωνία της πληροφορίας, αποτελεί ένα ευρύ πεδίο έρευνας παγκόσμια. Στη συνέχεια θα παρουσιαστούν κάποια *projects* που έχουν αναπτυχθεί στον τομέα αυτό.

6.1 Η Ασφάλεια των Εγγράφων

Ο σκοπός αυτού του ερευνητικού *project* είναι η ανάπτυξη πρακτικών και περιεκτικών τεχνικών μέτρων για την ασφάλεια των εγγράφων. Ξεκίνησε το Σεπτέμβρη του 2003 και διενεργείται από το *Zurich Information Security Center (ZISC).*

Η ασφάλεια των εγγράφων έχει ως κίνητρο το γεγονός ότι οι εταιρείες θα πρέπει να ασφαλίζουν πολλά από τα έγγραφα που επεξεργάζονται επειδή αυτά περιέχουν ιδιωτικά στοιχεία των πελατών τους που προστατεύονται από το νόμο και επίσης μυστικά των επιχειρήσεων που δεν πρέπει να τα γνωρίζουν ανταγωνιστές. Αυτές οι επιχειρήσεις θα πρέπει να καταφεύγουν σε οργανωτικά μέτρα, αφού τα τεχνικά μέτρα δεν είναι πρακτικά, δεν είναι αρκετά περιεκτικά ή απουσιάζουν εντελώς.

Ο (μακροπρόθεσμος) σκοπός της ασφάλειας των εγγράφων, είναι να επιβεβαιώσει ότι η πληροφορία στα έγγραφα μπορεί να προστατευθεί από μηχανισμούς που επιβάλλουν μια πολιτική ασφάλειας και ιδιωτικότητας, και ότι αυτοί οι μηχανισμοί δεν περιορίζονται σε μια συγκεκριμένη πλατφόρμα ή σε έναν επεξεργαστή εγγράφων. Το ***μοντέλο απειλής*** *(threat model)* θεωρεί ότι τα ενδιαφερόμενα μέρη μιας εταιρείας (υπάλληλοι,

σύμβουλοι, συνεργάτες κ.λπ.) που έχουν πρόσβαση σε ευαίσθητα έγγραφα δεν είναι έμπιστα γιατί:

- Μπορεί να είναι αμελείς με τη χρήση και διανομή των δεδομένων,
- Το λογισμικό που χρησιμοποιούν μπορεί να μην είναι έμπιστο (για παράδειγμα να έχει μολυνθεί από ιό),
- Κάποιοι μπορεί να έχουν κακές προθέσεις.

Η έλλειψη εμπιστοσύνης σημαίνει ότι απαιτείται σοβαρός έλεγχος από την πλευρά του πελάτη που προωθεί την ασφάλεια των εγγράφων στην περιοχή της διαχείρισης των δικαιωμάτων και της ασφάλειας των συστημάτων πληροφορικής.

Από το σκοπό και το μοντέλο απειλής, εξάγεται ο σκοπός του *project* **της *Ασφάλειας των Εγγράφων***: οι πρωταρχικοί σκοποί είναι *η* ***ικανοποίηση της εμπιστευτικότητας*** (δηλαδή η προστασία των μυστικών των επιχειρήσεων) και μια ***πολιτική ακεραιότητας*** (ώστε να περιορίζει τους επιτιθέμενους από το να παίρνουν αυθαίρετα δικαιώματα). Η *Microsoft* δημιούργησε τον όρο ***επιχειρησιακή διαχείριση δικαιωμάτων*** *(enterprise rights management)*, αφού ο πρώτος σκοπός διαφέρει από το σκοπό της ***διαχείρισης ψηφιακών δικαιωμάτων*** *(digital rights management, DRM)* ο οποίος τυπικά περιλαμβάνει πληρωμή για πρόσβαση σε μη έμπιστα δεδομένα (π.χ. ταινίες). Η ιδιωτικότητα είναι έξω από το σκοπό αυτού του *project*.

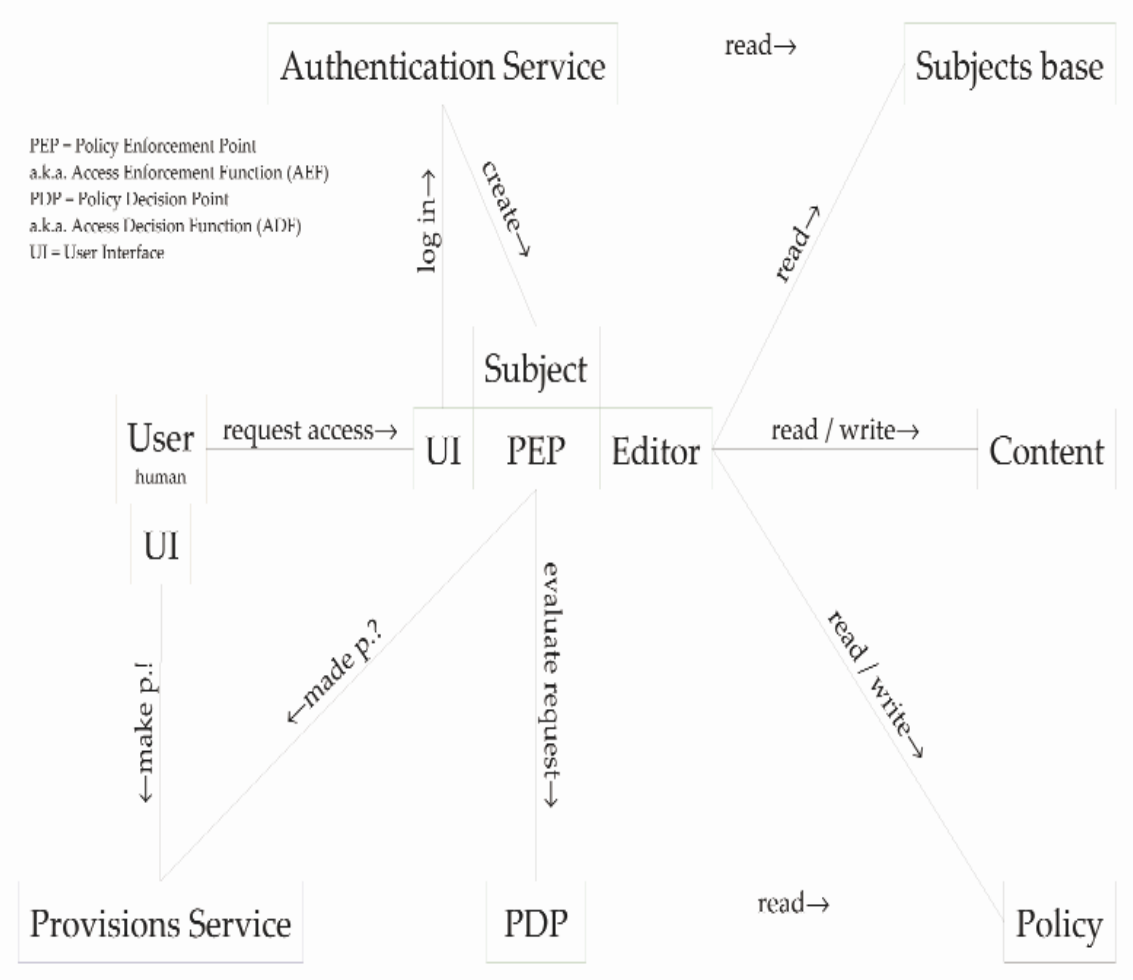
Θα πρέπει να αναφερθεί ότι οι απαιτήσεις δεν προέρχονται από αυτά που θεωρούν οι επιστήμονες πληροφορικής ενδιαφέροντα και άξια έρευνας, αλλά από πραγματικές περιπτώσεις που συνέβησαν σε μια Ελβετική τράπεζα. Για παράδειγμα, οι χρήστες θα πρέπει να είναι ικανοί να ορίσουν διαφορετικούς κανόνες (πολιτική) για διαφορετικά τμήματα (περιεχόμενα) στο ίδιο έγγραφο, έτσι ώστε να μην είναι υποχρεωμένοι να δημιουργήσουν πολλές εκδόσεις του ίδιου εγγράφου με διαφορετική λογοκρισία σε κάθε μια. Ένα άλλο παράδειγμα είναι ότι θα πρέπει να μπορούμε να ορίσουμε ότι κάποιοι χρήστες έχουν την άδεια να αναθέτουν άδειες σε άλλους χρήστες ώστε οι τελευταίοι να μπορούν να επεξεργαστούν τα έγγραφα.

Τα έγγραφα που χρησιμοποιήθηκαν από το *project* είναι ένα υπερσύνολο των εγγράφων *XML*. Αναπτύχθηκε ένα μαθηματικό μοντέλο αυτού του υπερσυνόλου. Τελικά, ορίστηκε με τρόπο φορμαλιστικό η σημασιολογία μιας γλώσσας πολιτικής που ονομάζεται το παράδειγμα της «κολλώδους» πολιτικής. Αυτό σημαίνει ότι η πολιτική κολλάει με την πληροφορία και παραμένει όταν η πληροφορία μεταφέρεται μεταξύ εγγράφων (δηλ. μέσω *cut* και *paste*). Τα υποκείμενα είναι βασικά ομάδες ιδιοτήτων (δηλ. ζευγάρια όνομα-τιμή) που μπορούν να χρησιμοποιηθούν σε ρόλους μοντελοποίησης για (ιεραρχικό) έλεγχο πρόσβασης ***βασισμένο σε ρόλους*** *(role-based access control)*. Η βαρύτητα των αντικειμένων είναι αυτή των ιδιοτήτων και των κόμβων. Το σύνολο των δραστηριοτήτων δεν περιλαμβάνει μόνο δράσεις πάνω στο περιεχόμενο (ειδικά «διάβασμα»), αλλά επίσης και πάνω στην πολιτική («πρόσθεσε κανόνα», «ανέθεσε άδειες»). Επιπλέον, και πρόσθετα με τις συνθήκες, υποστηρίζονται οι προβολές και έτσι επιτρέπεται οι αποφάσεις πρόσβασης να γίνονται ανάλογα με αυτές (για παράδειγμα υπογράφοντας μια συμφωνία μη δημοσιοποίησης ή πρόσβασης με λογαριασμό).

Το επόμενο βήμα είναι η θεώρηση πλαισίων που είναι διαφορετικά από τα έγγραφα (π.χ. μια βάση δεδομένων). Όταν η πληροφορία προέρχεται από έναν άλλο τύπο πλαισίου, το έγγραφο θα λάβει υπόψη του την πολιτική αυτού του πλαισίου, σε συμφωνία με τη σημασιολογία πολιτική-συνδυασμός ή πολιτική-ταίριασμα (π.χ. τη διατομή των περιορισμών).

Σαν πρωτότυπο, σχεδιάστηκε ένα σύστημα πελάτη *(client system)* (αντιληπτό από το χρήστη όπως ο επεξεργαστής κειμένου) που θα υλοποιηθεί από φοιτητές. Το περιεχόμενο και η πολιτική είναι στοιχεία μιας πλειάδας εγγράφων όπως φαίνεται στο ***σχήμα 40***. Καθώς ο χρήστης δεν είναι μέρος μιας έμπιστης βάσης, η ακεραιότητα του συστήματος πελάτη – ειδικά η εμπιστευτικότητα των μυστικών κλειδιών- θα πρέπει να επιβεβαιωθεί είτε από τους μηχανισμούς του λειτουργικού συστήματος (αν τους υπολογιστές τους διαχειρίζονται έμπιστοι υπάλληλοι του οργανισμού) είτε από μηχανισμούς βασισμένους στο υλικό (*hardware*). Καθώς η υπηρεσία προβολής είναι τμήμα της έμπιστης βάσης, αποτελεί μόνο ένα τοπικό στέλεχος. Αλλιώς, οι παράνομοι χρήστες θα μπορούσαν να κάνουν τον υπολογιστή τους να καταστρέψει τα αρχεία πρόσβασης ή τη συμφωνία μη δημοσιοποίησης.

Η ασφάλεια των εγγράφων είχε σαν αποτέλεσμα κάποια άλλα *projects* όπως τον *emulator* για *Linux*, *Trusted Platform Module (TPM)* και έναν αξιολογητή αλγόριθμων *XML*. Επίσης θέτει ενδιαφέροντα ζητήματα στο πεδίο της χρηστικότητας και της ασφάλειας. **[28]**



Σχήμα 40: Η αρχιτεκτονική του συστήματος ασφάλειας εγγράφων

6.2 *iWatch*: Προηγμένη Παρακολούθηση Βασισμένη σε Αισθητήρες Οργανωμένους σε Δίκτυα και σε Αυτόνομα Κινητά Οχήματα

Πρόσφατα γεγονότα και αλλαγές στην κοινωνία έχουν δημιουργήσει μια αυξανόμενη απαίτηση για ασφάλεια, που έχει ωθήσει τις κυβερνήσεις και τους οργανισμούς να κάνουν προτεραιότητα την προσωπική ασφάλεια και την ασφάλεια των αγαθών. Για παράδειγμα, στο Λονδίνο, τη μεγαλύτερη πληθυσμιακά πρωτεύουσα της Ευρώπης, έχουν συσταθεί τεράστια προγράμματα ασφάλειας, που βασίζονται σε προγράμματα επιτήρησης (καταγραφικά καμερών, *Closed Circuit Television, CCTV)*. Λόγω αυτών των προγραμμάτων, χιλιάδες κάμερες *CCTV* εγκαταστάθηκαν για επιτήρηση σε πολλές περιοχές ενδιαφέροντος (π.χ. περισσότερες από 10.000 κάμερες στο μετρό του Λονδίνου και στο αεροδρόμιο του Χήθροου). Ωστόσο οι κάμερες έχουν μικρή χρησιμότητα χωρίς να υπάρχει κάποιου είδους ανάλυση των δεδομένων που καταγράφουν. Μια έρευνα του 2002 από το αρμόδιο γραφείο της Βρετανικής κυβέρνησης, βρήκε ότι οι κάμερες έχουν πολύ μικρή επίδραση στο έγκλημα και καμία στην πρόληψη της τρομοκρατίας. Η αστυνομία του Λονδίνου παραδέχτηκε ότι σχετικά με τη χρήση των δεδομένων των αισθητήρων, το εργατικό δυναμικό αποτελεί έναν σημαντικό περιορισμό. Για να αποβούν χρήσιμες οι κάμερες στην πρόληψη της τρομοκρατίας, χρειάζεται ένας ολόκληρος στρατός αστυνομικών που θα εξετάζει λεπτομερώς τις εικόνες.

Τα συστήματα που υπάρχουν μέχρι σήμερα βασίζονται σε στατικούς αισθητήρες όπως είναι οι κάμερες και οι αισθητήρες κίνησης για επιτήρηση και παρακολούθηση. Κάθε ανάπτυξη, επεκτασιμότητα και δυνατότητα προσαρμογής είναι επίσης πολύ σημαντικά θέματα για τα συστήματα ασφάλειας. Για αυτό το λόγο, στα επόμενα χρόνια η τάση που θα επικρατήσει θα είναι να βγουν οι δυνατότητες επεξεργασίας, επικοινωνίας και αίσθησης από τους σταθμούς εργασίας και σταδιακά να ενσωματωθούν στους ίδιους τους αισθητήρες. Σε μακροπρόθεσμο ορίζοντα, ο υπολογιστής θα δώσει τις αρμοδιότητές του σε μικρότερες συσκευές που θα ενσωματώνονται κατ' ουσίαν οπουδήποτε στο περιβάλλον. Συνήθως αυτοί οι αισθητήρες δεν κατεργάζονται κάποια επεξεργαστική ισχύ και δεν υπάρχει επικοινωνία μεταξύ τους. Εκτός από τους αισθητήρες, μικρές ετικέτες πληροφορίας χρησιμοποιούνται για την αναγνώριση των προϊόντων και των ατόμων όπως γίνεται και στα συστήματα αποτροπής των κλοπών.

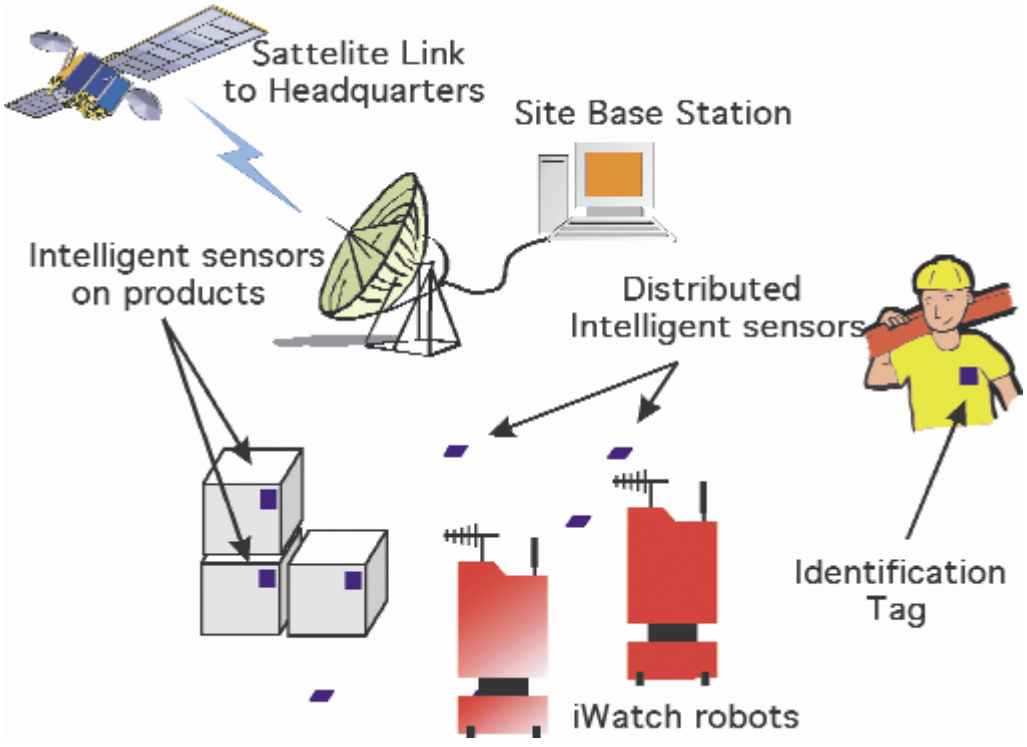
Το *i-Watch* είναι μια διεπιστημονική δραστηριότητα στην *FORTH-ICS.* Προτίθεται να χρησιμοποιήσει υπάρχουσα τεχνολογία υψηλού επιπέδου και εμπειρία σε αυτό το σημαντικό πεδίο εφαρμογής και αντίστροφα, να χρησιμοποιήσει το συγκεκριμένο πεδίο εφαρμογής για να εκτελέσει περαιτέρω εργασία στην υποκείμενη τεχνολογία. Το *i-Watch* εστιάζει στο πώς θα μπορέσει να βελτιωθεί η ευαισθητοποίηση των κρατών και η ασφάλεια σε μεγάλης κλίμακας κτίρια και αγαθά, ενσωματώνοντας διάφορες συσκευές κάτω από ένα κοινό πλαίσιο που περιλαμβάνει:

- Έξυπνους αισθητήρες χαμηλού κόστους με *RF (Radio Frequency)* επικοινωνία, μνήμη και δυνατότητες επεξεργασίας, οι οποίοι μπορούν να αναπτυχθούν σε μεγάλη κλίμακα ώστε: **α)** να διευκολύνουν τη δημιουργία δικτύων αισθητήρων υψηλής πυκνότητας για την παρακολούθηση μεγάλων περιοχών, **β)** να δρουν σαν συσκευές παρακολούθησης για φυσικά αγαθά και εμπορεύματα ενδιαφέροντος, και **γ)** να αναγνωρίζουν το εξουσιοδοτημένο προσωπικό,
- Αυτόνομα ρομποτικά οχήματα μπορούν να παρέχουν έναν αυτοματοποιημένο μηχανισμό για παρακολούθηση θέσης και συνεχή χαρτογράφηση όπως επίσης για επιτήρηση και για ειδικευμένες δυνατότητες αίσθησης κατά τη διάρκεια

περιπολίας ή σε περίπτωση έκτακτων περιστατικών. Εκτός από την προσφορά λειτουργιών ειδικευμένης επιτήρησης, οι κινητές ρομποτικές πλατφόρμες μπορούν κάθε στιγμή να καταγράψουν πληροφορίες από τους έξυπνους αισθητήρες και να τροποποιήσουν τη βάση δεδομένων με την ιστορικότητα των δεδομένων των αισθητήρων. Επίσης μπορούν να βελτιώσουν τις εκτιμήσεις των αισθητήρων θέσης, και έτσι να ξεπεράσουν τους βασικούς περιορισμούς που υπάρχουν στην επικοινωνία και στην τοποθέτηση μεταξύ των αισθητήρων.

- Οι λειτουργικότητες θα μεταφερθούν κάτω από ένα κοινό λειτουργικό περιβάλλον, προσφέροντας πλήρη και συγκεντρωμένη επίγνωση της κατάστασης, υποστηριζόμενη από τεχνολογία δορυφορικής επικοινωνίας.

Το *i-Watch project*, υποστηρίζει την ανάπτυξη υπαρχόντων στελεχών υλικού (*hardware*) με το αντίστοιχο *middleware*, όπως και την ανάπτυξη εφαρμογών ασφάλειας αισθητήρων, που βασίζονται στο ενσωματωμένο σύστημα δικτύου και τις δυνατότητες που αυτό προσφέρει. Τελικά, το *i-Watch* θα προσφέρει ολοκλήρωση υψηλού επιπέδου σε επικεντρωμένες περιοχές, προσβλέποντας σε πλήρη επίγνωση κατάστασης μεταξύ κατανεμημένων γεωγραφικών περιοχών. Η ***εικόνα τακτικής επιτήρησης και ελέγχου*** που παράγεται από το πεδίο κάθε εφαρμογής μπορεί να μεταδοθεί από αξιόπιστα μέσα ανεξάρτητα θέσης, όπως είναι οι δορυφόροι και να συνδυαστεί σε ένα συγκεκριμένο σταθμό επιλογής ώστε να δημιουργηθεί ένα ενοποιημένο περιβάλλον λειτουργιών. Αυτό το περιβάλλον που παρουσιάζεται ως ***τοίχος πληροφορίας*****,** είναι το θεμελιώδες μέσο για την επίτευξη της επίγνωσης της κατάστασης. Τέλος, το *i-Watch* συγκεντρώνει ερευνητές αυτόνομων οχημάτων, έξυπνων αισθητήρων, δικτύων και επεξεργασίας σήματος και κεφαλαιοποιεί την υπάρχουσα εμπειρία και τεχνολογία για να παρέχει αυτοματοποιημένη ανίχνευση, αναγνώριση, χαρτογράφηση και έλεγχο απογραφής των αγαθών και των ανθρώπων όπως επίσης και περιπολία από αυτόνομα κινητά οχήματα σε κτήρια μεγάλης κλίμακας. **[29]**



Σχήμα 41: Το πεδίο δράσης και τα συστατικά συστήματος του *i-Watch*

6.3 *JAFAR*: Ένα Αρχιτεκτονικό Πλαίσιο για Εφαρμογές Ηλεκτρονικού Εμπορίου

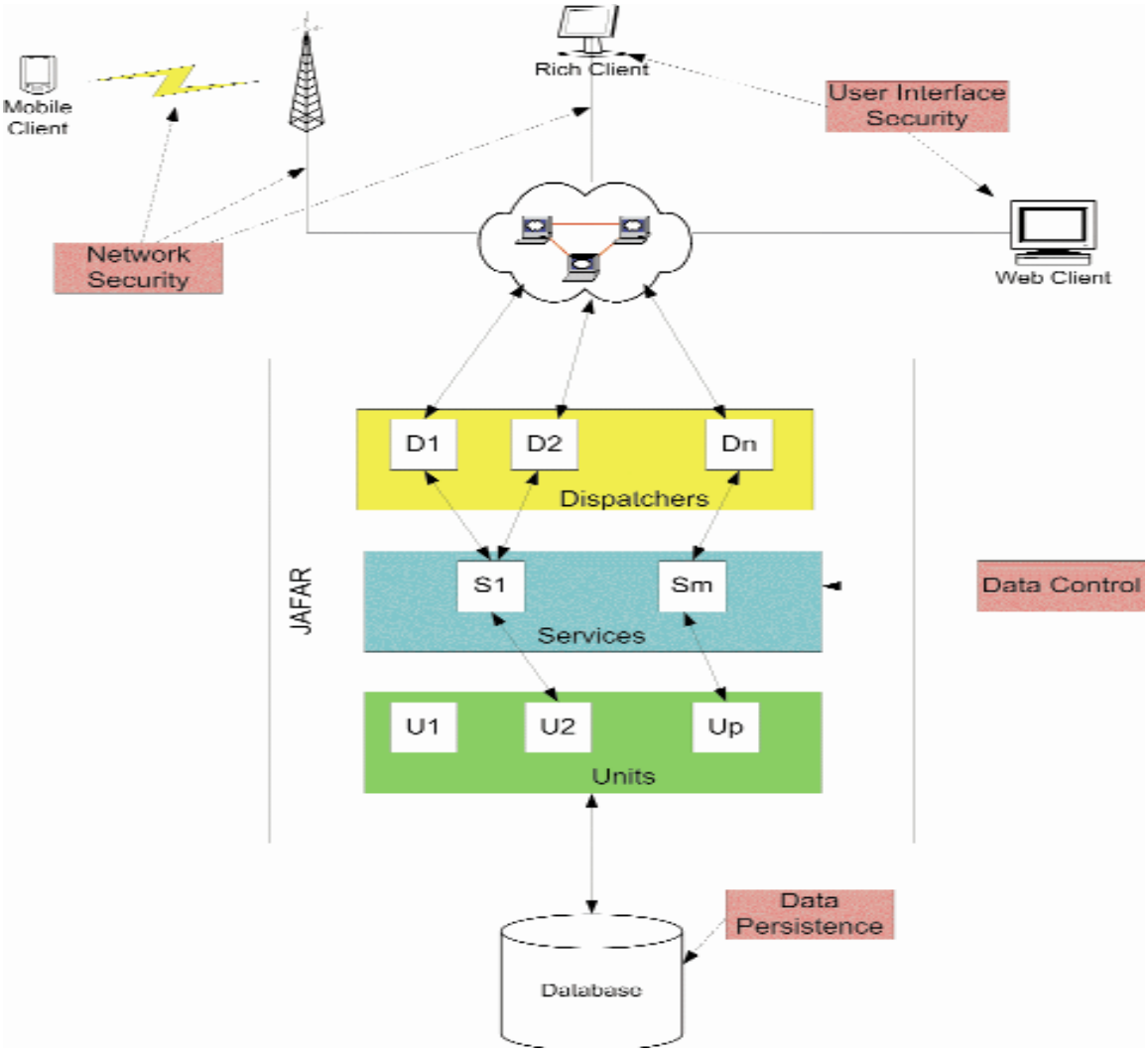
Από τις αρχές του 1990 και την έλευση του ***κατανεμημένου ηλεκτρονικού εμπορίου*** *(e-commerce)*, η επιστήμη των υπολογιστών αντιμετώπισε προβλήματα σχετιζόμενα με την ασφάλεια, στα πεδία της ανταλλαγής δεδομένων και του χειρισμού δεδομένων στην περιοχή του εξυπηρετητή. Το κλειδί της επιτυχίας για τις εφαρμογές του *e-commerce* βρίσκεται στην απόκτηση της εμπιστοσύνης από τους πιθανούς χρήστες. Επομένως, οι εφαρμογές θα πρέπει να αναπτύσσονται έτσι ώστε να προσφέρουν επαρκή επίπεδα ασφάλειας. Η ομάδα *ADS (Architecture Engineering for Dependable Distributed Systems)* του *SE2C* ενδιαφέρεται για βασικά προβλήματα ασφάλειας και διαχείρισης εμπιστοσύνης που υπάρχουν στην ανάπτυξη και χρήση των εφαρμογών ***κατανεμημένου e-commerce*** *(distributed e-commerce)*.

Κατ' αρχήν στα μάτια των χρηστών, η εμπιστευτικότητα των δεδομένων κατά την ανταλλαγή στοιχείων μεταξύ της εφαρμογής του πελάτη και του εξυπηρετητή συνιστά το πιο κρίσιμο σημείο της ασφάλειας. Αυτό το φαινόμενο, που παραμένει καθαρά πρόβλημα δικτύου, απέκτησε μεγαλύτερη σημασία με την έλευση των τηλεπικοινωνιακών δικτύων τρίτης γενιάς και την εμφάνιση του παραδείγματος του κινητού εμπορίου *(m-commerce)*. Η χρήση ενός αρχιτεκτονικού πλαισίου όπως είναι το *JAFAR* επιτρέπει στους προγραμματιστές κατανεμημένων εφαρμογών να λαμβάνουν υπόψη τους και να λύνουν πιο εύκολα, σε επίπεδο λογισμικού, το πρόβλημα της ανταλλαγής δεδομένων. Αυτό επιτυγχάνεται ειδικότερα, μέσω της χρήσης λύσεων ασφάλειας που έχουν ήδη υλοποιηθεί στην καρδιά του σχεδιασμού του πλαισίου (π.χ. διεπαφές επικοινωνίας που υποστηρίζουν το πρωτόκολλο *TLS (Transport Layer Security),* χρήση πιστοποιητικών για την κρυπτογράφηση των δεδομένων κ.λπ.). Επίσης, στις περιπτώσεις που το επίπεδο της εμπιστευτικότητας το απαιτεί, το πλαίσιο ενισχύεται με την ανάπτυξη και άλλων συστατικών που ενσωματώνουν περισσότερο ισχυρά μέσα κρυπτογράφησης. Ακόμα, σημαντικά είναι τα πιστοποιητικά ασφάλειας για την αυθεντικοποίηση του ιστοχώρου του *e-commerce* στους χρήστες. Σε εξέλιξη είναι η έρευνα των διαφόρων λύσεων ασφάλειας που μπορούν να χρησιμοποιηθούν στο πεδίο του *e-commerce* και να ενσωματωθούν στο *JAFAR*, κυρίως πάνω από δίκτυα *UMTS*.

Δεύτερον, η σταθερότητα και η διαθεσιμότητα των δεδομένων αποτελούν σημαντικά σημεία της επιτυχίας των εφαρμογών *e-commerce*. Λαμβάνοντας υπόψη την εταιρεία *Amazon*, μια διακοπή των *web* διεπαφών της θα είχε σημαντική επίδραση στον κύκλο εργασιών της. Έτσι, οι εφαρμογές θα πρέπει να σχεδιαστούν ώστε να αποτρέπουν τις απομακρυσμένες επιθέσεις όπως είναι οι επιθέσεις άρνησης παροχής υπηρεσίας, που στοχεύουν την διαθεσιμότητα των πόρων. Κατά την ανάπτυξη του *JAFAR*, μελετήθηκαν οι πιθανότητες ανίχνευσης τέτοιων τύπων επιθέσεων, όπως επίσης και τα μέτρα που θα πρέπει να παρθούν όταν ένας σημαντικός πόρος δεν είναι πια διαθέσιμος. Ειδικότερα, γίνεται έρευνα για την αποκέντρωση των πόρων, ώστε να μειωθεί όσο είναι δυνατόν ο χρόνος κατά τον οποίο οι πόροι δεν είναι διαθέσιμοι. Ωστόσο, προβλέπεται η ενσωμάτωση των απόψεων προσαρμογής και ελαστικότητας του συστήματος στο άμεσο μέλλον, μέσω άλλων *projects* όπως είναι το *CORRECT*.

Τέλος, εφόσον η ασφάλεια αποθήκευσης σχετίζεται με την εφαρμογή των επιχειρήσεων και την υποστηρικτική της δομή αποθήκευσης, μια μεθοδολογία μείωσης του κινδύνου αποτελεί έναν υγιή τρόπο ενδυνάμωσης της διαθεσιμότητας αποθήκευσης, της αξιοπιστίας και της ιδιωτικότητας. Αυτός είναι και ο λόγος που η αποθήκευση και η πρόσβαση σε αποθηκευμένα δεδομένα είναι τα τελικά σημαντικά σημεία που επηρεάζουν τη σχεδίαση των εφαρμογών *e-commerce*. Η αρχιτεκτονική επιπέδων του *JAFAR* έχει σχεδιαστεί με έναν αυστηρό τρόπο και καθορίζει τα δικαιώματα που δίνονται στους χρήστες μετά την αναγνώρισή τους. Επίσης, το *JAFAR* αναπτύχθηκε για

να προσφέρει μια πλειονότητα υπηρεσιών στους χρήστες μειώνοντας ταυτόχρονα τον αριθμό των διεπαφών που κάνουν πιθανή την κατάσχεση πληροφοριών και την εισαγωγή λανθασμένων δεδομένων. Ειδικά η τελευταία περίπτωση, περιλαμβάνει κώδικα που μεταφράζεται από το σύστημα, όπως είναι η *SQL* ή η *HTML*, που μπορεί να έχει καταστρεπτικά αποτελέσματα στα αποθηκευμένα δεδομένα. Μελετώνται τρόποι για τον ορισμό κανόνων ασφάλειας που θα ελέγχονται σε πραγματικό χρόνο και που θα μπορεί να αλλάξουν σε ένα παραγωγικό σύστημα για να αντιδράσουν σε παρατηρημένα πρότυπα επίθεσης. Επίσης το *JAFAR* ενσωματώνει μια μονάδα (*module*) που κάνει δυνατό έναν αυστηρό έλεγχο των δεδομένων που πρόκειται να αποθηκευτούν ανιχνεύοντας πιθανά τμήματα κακόβουλου κώδικα. **[30]**



Σχήμα 42: Η αρχιτεκτονική του *Jafar*

6.4 *PRIME:* Η Διαχείριση της Ταυτότητας ως προς την Ασφάλεια

Στις μέρες μας μια παγκόσμια υποδομή πληροφοριών, συνδέει απομακρυσμένα μέρη σε όλο τον κόσμο μέσω της χρήσης δικτύων μεγάλης κλίμακας, βασιζόμενη σε πρωτόκολλα επιπέδου εφαρμογής και υπηρεσίες όπως το *World Wide Web*. Οι ανθρώπινες δραστηριότητες βασίζονται ολοένα και περισσότερο στη χρήση απομακρυσμένων πόρων και υπηρεσιών και στις αλληλεπιδράσεις μεταξύ μερών που είναι σε απομακρυσμένες τοποθεσίες και συχνά ξέρουν πολύ λίγα το ένα για το άλλο. Λόγω της τεράστιας προσωπικής πληροφορίας που είναι διαθέσιμη, αυξάνονται οι

ανησυχίες σχετικά με την ιδιωτικότητα των χρηστών: η αποτελεσματική ανταλλαγή και διάδοση πληροφοριών μπορεί να γίνει μόνο όταν οι χρήστες έχουν κάποια διαβεβαίωση ότι δεν υπάρχει κίνδυνος αποκάλυψης ευαίσθητης πληροφορίας. Επομένως είναι πολύ σημαντική η ψηφιακή διαχείριση ταυτότητας για την υποστήριξη ασφαλών αλληλεπιδράσεων. Μια περιεκτική λύση διαχείρισης ταυτότητας θα πρέπει να παρέχει πλήρη υποστήριξη στον ορισμό και στη διαχείριση του κύκλου ζωής των ψηφιακών ταυτοτήτων και των προφίλ, όπως και υποδομή για ανταλλαγή και επικύρωση αυτών των πληροφοριών.

Αναδυόμενα σενάρια των αλληλεπιδράσεων χρήστη-υπηρεσίας στον ψηφιακό κόσμο πιέζουν προς την ανάπτυξη ισχυρών και ευέλικτων μοντέλων και γλωσσών ελέγχου πρόσβασης με βελτιωμένες δυνατότητες απορρήτου. Η ανάγκη για ιδιωτικότητα σημαίνει ότι οι πολιτικές ελέγχου πρόσβασης και τα μοντέλα θα πρέπει να επαναπροσδιοριστούν, και να αναπτυχθούν νέες μορφές ορισμού εξουσιοδότησης και ενίσχυσης. Ειδικότερα, ισχύουν δύο σοβαρά θέματα: **α)** ο έλεγχος της πρόσβασης θα πρέπει να λειτουργεί ακόμα και όταν τα μέρη που αλληλεπιδρούν προτιμούν να μείνουν ανώνυμα ή να αποκρύψουν μόνο συγκεκριμένα χαρακτηριστικά για τον εαυτό τους, **β)** τα δεδομένα που συλλέγονται κατά τον έλεγχο της πρόσβασης όπως και τα δεδομένα που αποθηκεύονται από τα διαφορετικά μέρη μπορεί να περιέχουν ευαίσθητες πληροφορίες για τις οποίες θα πρέπει να εφαρμοστούν οι πολιτικές ιδιωτικότητας.

Στο πλαίσιο του *PRIME project*, το κύριο έργο είναι η ανάπτυξη της μονάδας (*module*) *Access Control Decision Function* (*ACDF*), μαζί με τον ορισμό ενός μοντέλου και μιας γλώσσας προστασίας της ιδιωτικότητας, που θα ορίζουν και θα ενδυναμώνουν τις απαιτήσεις προστασίας της προσωπικής αναγνωριστικής πληροφορίας *(Personal Identifiable Information, PPI).*

Το συστατικό ελέγχου πρόσβασης βασίζεται σε μια απλή και εκφραστική γλώσσα της οποίας τα κύρια χαρακτηριστικά είναι τα παρακάτω:

- ***Ευέλικτοι και εκφραστικοί κανόνες ελέγχου πρόσβασης (Flexible and expressive access control rules)***: Οι κανόνες ελέγχου πρόσβασης χρησιμοποιούν επιμέρους ταυτότητες που σχετίζονται με τους χρήστες. Είναι επίσης δυνατό να οριστούν κανόνες ελέγχου πρόσβασης σχετικά με αντικείμενα πρόσβασης πληροφορίας και με πόρους που προσπελαύνονται.
- ***Ενίσχυση αλληλεπίδρασης (Interactive enforcement):*** Ένα συστατικό ελέγχου πρόσβασης μπορεί να μην έχει όλη την πληροφορία που χρειάζεται για να αποφασίσει αν θα πρέπει ή όχι να δοθεί πρόσβαση. Από την άλλη πλευρά, οι αιτούντες μπορεί να μην ξέρουν εκ των προτέρων ποιά πληροφορία θα πρέπει να παρουσιάσουν για να πάρουν πρόσβαση. Σαν αποτέλεσμα, η διαδικασία ελέγχου πρόσβασης είναι ένας τρόπος διαπραγμάτευσης με τον αιτούντα την πρόσβαση, της αποκάλυψης πρόσθετης προσωπικής πληροφορίας ώστε να επιτευχθεί η τελική απόφαση πρόσβασης.
- ***Περιορισμοί από την πλευρά του πελάτη (Client-side restrictions):*** Επιπρόσθετα με τους παραδοσιακούς κανόνες ελέγχου πρόσβασης της πλευράς του εξυπηρετητή, οι χρήστες θα πρέπει να μπορούν να θέσουν περιορισμούς της χρήσης των προσωπικών τους πληροφοριών μόλις αυτές δοθούν σε κάποια τρίτη οντότητα. Για το λόγο αυτό, εισάγεται η έννοια ότι η απελευθέρωση των πολιτικών διέπουν την απελευθέρωση των συστατικών, των πιστοποιητικών και των *PII* στην πλευρά της τρίτης οντότητας.

- ***Ανωνυμία και έλεγχος του τελικού χρήστη (Anonymity and end-user control):*** Το σύστημα ελέγχου πρόσβασης επιτρέπει τον πλήρη έλεγχο του τελικού χρήστη πάνω στην ψηφιακή ταυτότητα που θα χρησιμοποιηθεί. Με άλλα λόγια, ο έλεγχος της πρόσβασης πρέπει να λειτουργεί όταν οι οντότητες που αλληλεπιδρούν επιθυμούν να μείνουν ανώνυμες ή να αποκαλύψουν μόνο συγκεκριμένα συστατικά τους.
- ***Ανταλλάξιμη πολιτική μορφοποίησης (Interchangeable policy format):*** Οι οντότητες θα πρέπει να καθορίσουν τις απαιτήσεις προστασίας στα δεδομένα που έχουν διαθέσιμα, χρησιμοποιώντας μια μορφοποίηση που είναι αναγνώσιμη από ανθρώπους και από μηχανήματα, και επίσης είναι εύκολο να ελεγχθεί και να ανταλλαχθεί. Επομένως η γλώσσα θα πρέπει να έχει μια απλή δηλωτική μορφή.

Η μονάδα *ACDF* είναι υπό ανάπτυξη και θα ενσωματωθεί με την αρχιτεκτονική *PRIME*. **[31]**

6.5 Η Ασφάλεια και η Δικτύωση των Εφαρμογών Υγείας

Η ανακάλυψη των πόρων και η επικοινωνία μεταξύ τους αποτελούν βασικά προβλήματα στην δικτύωση των συσκευών και των υπηρεσιών. Το *Universal Plug and Play (UpnP)* είναι μια λύση ευρείας αποδοχής για την ανακάλυψη, τον έλεγχο και την παρακολούθηση των δικτυωμένων συσκευών. Η εγκατάσταση του δικτύου γίνεται απλή. Επιπλέον, τα δίκτυα μπορούν να δομηθούν με τέτοιο τρόπο ώστε ένα τερματικό να ελέγχει όλες τις συσκευές και κάθε συσκευή να ελέγχεται από πολλά διαφορετικά σημεία ελέγχου. Ωστόσο, το *UpnP* δεν ορίζει ικανοποιητικούς μηχανισμούς ασφάλειας. Το ασφαλές *UpnP* αναπτύχθηκε για να εξασφαλίσει ότι μόνο εξουσιοδοτημένοι κόμβοι μπορούν να ελέγχουν και να παρακολουθούν συσκευές.

6.5.1 Η Λύση της Ασφάλειας

Το ασφαλές *UpnP* παρέχει αυθεντικοποίηση στους υπολογιστές, εμπιστευτικότητα και ακεραιότητα των δεδομένων, όπως και διαχείριση κλειδιού. Χρησιμοποιούνται γνωστά και αποδεδειγμένα ασφαλή συστατικά, δηλαδή *Secure Sockets Layer (SSL)* και πιστοποιητικά *X.509.*

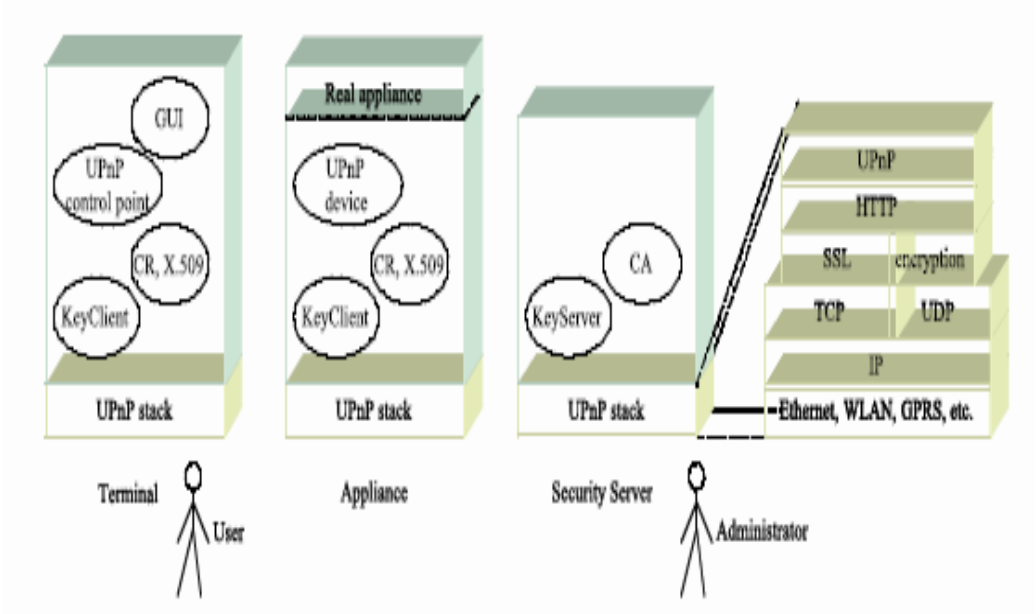
Το *SSL* χρησιμοποιείται ευρέως, για παράδειγμα, για να ασφαλίσει την πρόσβαση σε τραπεζικούς λογαριασμούς μέσω του διαδικτύου. Το *SSL* χρησιμοποιήθηκε για να ασφαλίσει την κυκλοφορία *TCP*, που μεταφέρει τα περισσότερα *UpnP* μηνύματα. Για να εγκατασταθεί μια *SSL* σύνοδος, κάθε κόμβος θα πρέπει να έχει ένα πιστοποιητικό αυθεντικοποίησης *X.509.* Τα πιστοποιητικά δίνονται από μια τοπική Αρχή Πιστοποιητικών *(Certificate Authority, CA)* αλλά μόνο αφού ο διαχειριστής έχει αποδεχτεί τον νέο κόμβο. Η φάση ανακάλυψης του *UpnP* χρησιμοποιεί *UDP*, στο οποίο δεν είναι δυνατό να χρησιμοποιηθεί *SSL*, οπότε τα *UDP* δεδομένα κρυπτογραφούνται. Το κλειδί κρυπτογράφησης του *UDP* μοιράζεται από όλο το δίκτυο και διανέμεται με τη χρήση *SSL*.

6.5.2 Περιοχές Εφαρμογής

Το ασφαλές *UpnP* κάνει δυνατό το χτίσιμο ασφαλών δικτύων που είναι εύκολα στην εγκατάσταση και έχουν πολλαπλά τερματικά ελέγχου. Μπορούν να χρησιμοποιηθούν ποικίλα φυσικά δίκτυα και να μοιραστούν με τις εφαρμογές. Οι περιοχές των εφαρμογών περιλαμβάνουν την υγειονομική περίθαλψη στα σπίτια, στα νοσοκομεία, στα γυμναστήρια και τους εξωτερικούς χώρους άθλησης, στα οικιακά δίκτυα, στα κτηριακά

δίκτυα, στον βιομηχανικό αυτοματισμό, στα δίκτυα αισθητήρων και στα τηλεματικά δίκτυα μεταφορών.

Το ***δικτυακό σύστημα υγειονομικής περίθαλψης*** *(Networked Health Care system)* του *VTT (Technical Research Centre of Finland)* πρωτοστάτησε στην ιδέα του ***συστήματος της ολικής προσωπικής πληροφορίας υγειονομικής περίθαλψης***. Η δικτυακή υγειονομική περίθαλψη μπορεί να χρησιμοποιηθεί σε πολλά όργανα υγειονομικού ενδιαφέροντος, όπως σε *steppers* αδυνατίσματος, ποδήλατα γυμναστικής, ζυγαριές που βελτιώνουν την υγεία. Το έργο χρησιμοποιεί πολλά προσωπικά σενάρια που έχουν σαν στόχο τον αποτελεσματικό έλεγχο του σωματικού βάρους και την βελτίωση της σωματικής διάπλασης. Η εστίαση της σχεδίασης γίνεται στο επίπεδο *middleware* και στις λύσεις επικοινωνίας. Οι χρήστες λαμβάνουν συμβουλές και πληροφορίες και την εναλλακτική των μαθημάτων εκγύμνασης με προσωπικό καθοδηγητή. Η παροχή λεπτομερούς ανατροφοδότησης των ασκήσεων αποτελεί μια καλή πρακτική εμψύχωσης των συμμετεχόντων, ώστε να διαχειρίζονται προσωπικά την φροντίδα της υγείας τους (το ασφαλές *UpnP* φαίνεται στο ***σχήμα 43***).



Σχήμα 43: Η αρχιτεκτονική του ασφαλούς *UpnP*

Το ***δικτυακό σύστημα υγειονομικής περίθαλψης*** μπορεί να ενσωματωθεί με έναν αριθμό συσκευών. Για παράδειγμα, με ένα ποδήλατο γυμναστικής που επιτρέπει στο χρήστη να διαλέξει την αντίσταση. Προσωπική πληροφορία υγείας, όπως οι παλμοί της καρδιάς, η κατανάλωση θερμίδων κ.α. συλλέγονται απευθείας από τις συσκευές που είναι συνδεδεμένες με το σύστημα ή από το προφίλ του χρήστη (π.χ. συνήθειες διατροφής). Τέτοιες πληροφορίες βοηθούν στην παρακολούθηση και στον έλεγχο του βάρους και στην βελτίωση της υγείας και ενθαρρύνουν την φυσική άσκηση και τη βελτίωση της υγείας του χρήστη.

Το ***δικτυακό σύστημα υγειονομικής περίθαλψης*** παρέχει ασφαλή επικοινωνία μεταξύ των συσκευών, όπως φαίνεται στο ***σχήμα 44*** και μόνο αυθεντικοποιημένες συσκευές μπορούν να συνδεθούν στο δίκτυο *UpnP*. Το δίκτυο αποτελεί ένα αυτοοργανωμένο σύστημα, που επιτρέπει δυναμικά συσχετισμούς μεταξύ των οντοτήτων εφαρμογών και των πόρων του δικτύου χωρίς πολύπλοκη διαμόρφωση.

Η μελλοντική ανάπτυξη του συστήματος θα επικεντρωθεί στην προσθήκη νέων συσκευών. Επίσης προβλέπεται η παροχή απομακρυσμένου ελέγχου μεταξύ των ιδιωτικών δικτύων. **[32]**

Σχήμα 44: Το δικτυακό σύστημα υγειονομικής περίθαλψης

6.6 Η Διαχείριση της Εμπιστοσύνης στις Εικονικές Κοινότητες

Οι εικονικές κοινότητες *(Virtual Communities, VC)* είναι ένας τρόπος σύνδεσης των ανθρώπων με κοινά χαρακτηριστικά, επαγγελματικό προσανατολισμό ή κοινές συνήθειες. Ήδη υπάρχουν πολλές εικονικές κοινότητες - *Kazaa, Bittorrent, Facebook* – και προσελκύουν εκατομμύρια χρηστών του διαδικτύου. Σαν μέλος της εικονικής κοινότητας, κάποιος μπορεί να έχει πρόσβαση σε πόρους της κοινότητας οι οποίοι είναι προστατευμένοι από εξωτερικούς χρήστες. Η πρόκληση βρίσκεται στην αναγνώριση κάποιου χρήστη ως μέλους της κοινότητας, αφού οι κοινότητες μεγαλώνουν και συρρικνώνονται δυναμικά και στην καθιέρωση εμπιστοσύνης μεταξύ των χρηστών που θα βασίζεται στη βάση της περιορισμένης γνώσης μεταξύ των μερών. Οι υπάρχουσες εικονικές κοινότητες κάνουν λίγα για να προστατεύσουν τα μέλη τους από κακόβουλους εσωτερικούς και εξωτερικούς χρήστες και επομένως δεν είναι αποδεκτές για εμπορική χρήση.

Οι εικονικές κοινότητες παρέχουν μηχανισμούς που βοηθούν στην αποτελεσματική υλοποίηση ασφαλούς πρόσβασης σε εμπιστευτικά δεδομένα ή προστατευμένους πόρους. Ένα μέλος εικονικής κοινότητας μπορεί να προσπελάσει πόρους της κοινότητας οι οποίοι δεν είναι προσπελάσιμοι από εξωτερικούς χρήστες. Για παράδειγμα, η *Apple* θα μπορούσε να χτίσει μια κοινότητα χρηστών που επιθυμούν να «φορτώσουν» ταινίες υψηλής ποιότητας από τους ασφαλείς εξυπηρετητές του *iTunes*. Δεν θα πρέπει να υπάρχει κάποιο κεντρικό σημείο πρόσβασης, έτσι ώστε το σύστημα να είναι περισσότερο επεκτάσιμο και εύκολο στη διαχείριση. Επίσης διαφορετικά μέλη της κοινότητας θα μπορούν να έχουν διαφορετικά δικαιώματα, συμπεριλαμβανομένων εκείνων της μεταπώλησης μουσικής σε άλλα μέλη της κοινότητας *iTunes*. Η πραγματική ποιότητα και οι ακριβείς περιορισμοί στον όγκο των μουσικών θεμάτων που είναι προσπελάσιμοι στα μέλη της κοινότητας ανάλογα με το ποσό που επιθυμούν να πληρώσουν. Με αυτό το σενάριο οι εξωτερικοί χρήστες είναι όλοι οι χρήστες του διαδικτύου που δεν πληρώνουν για την πρόσβαση. Καθώς δεν είναι μέλη της κοινότητας *iTunes*, δεν μπορούν να προσπελάσουν κανένα αρχείο εκεί και δεν μπορούν να εμβάλλουν ψεύτικη μουσική στο δίκτυο. Επιπλέον, τέτοιου είδους ελεγχόμενη

πρόσβαση σε πόρους κοινοτήτων βοηθά όχι μόνο στην προστασία εμπιστευτικής πληροφορίας αλλά επίσης και στο σχεδιασμό της χρήσης του εύρους ζώνης και του φόρτου των παρόχων της υπηρεσίας.

Η διαχείριση της εμπιστοσύνης κάνει την ασφάλεια διάφανη στους τελικούς χρήστες, ώστε να μην απαιτείται ουσιώδης γνώση των μηχανισμών ασφάλειας. Επίσης υπάρχουσες προσεγγίσεις της διαχείρισης ασφάλειας απαιτούν μια συγκεντρωτική αρχιτεκτονική και έτσι δεν ταιριάζουν στην κατανεμημένη φύση του διαδικτύου. Επομένως στην παρούσα έρευνα, που ξεκίνησε το 2004, συνδυάζεται η κατανεμημένη διαχείριση εμπιστοσύνης και οι εικονικές κοινότητες σε μία λύση που είναι κατάλληλη για εμπορική και ιδιωτική χρήση.

Τα θέματα που εξετάστηκαν είναι:

- Πώς επισημοποιείται η υποστήριξη των *VC* σε ένα σύστημα διαχείρισης εμπιστοσύνης,
- Εξαιτίας της κατανεμημένης φύσης του διαδικτύου, χρειάζεται να ερευνηθούν οι συνθήκες υπό τις οποίες είναι διαθέσιμη πληροφορία απαραίτητη για ασφαλή αυθεντικοποίηση του χρήστη,
- Ο σχεδιασμός του συστήματος θα πρέπει να παρέχει ασφάλεια διάφανη για τον τελικό χρήστη.

Κάθε μέλος της κοινότητας θα πρέπει να αποδεικνύει την θέση του στην ομάδα της κοινότητας πριν πάρει συγκεκριμένη άδεια πρόσβασης. Μια τέτοια απόδειξη μπορεί να εκληφθεί σαν ένα ***set κατανεμημένων υπογεγραμμένων εγγράφων που ονομάζονται πιστοποιητικά.*** Ο εκδότης και το υποκείμενο της πιστοποίησης αντιπροσωπεύουν χρήστες του διαδικτύου. Ο αριθμός των *VC* στα οποία μπορεί κάποιος χρήστης να είναι μέλος είναι απεριόριστος και επομένως ένας χρήστης μπορεί να είναι υποκείμενο πολλών πιστοποιητικών την ίδια στιγμή.

Σαν ένα τυπικό σενάριο, μπορούμε να φανταστούμε ότι ο χρήστης Α θέλει να μοιραστεί τα *video* των διακοπών του. Ο χρήστης δεν θέλει να δει τα *video* του ο κόσμος , αλλά θέλει να περιορίσει τους θεατές στους φίλους του. Έτσι ο χρήστης Α φτιάχνει μια εικονική κοινότητα που περιέχει μόνο τους φίλους του. Για να την υλοποιήσει, δημιουργεί πιστοποιητικά, ένα για κάθε φίλο, καθορίζοντας τον κάθε ένα σαν φίλο της κοινότητας. Στην πράξη, ο χρήστης Α δεν χρειάζεται να επικοινωνήσει προσωπικά με τους φίλους του, αλλά η διαδικασία μπορεί να γίνει χρησιμοποιώντας *agents* λογισμικού που θα αναπαριστούν τον Α και τους φίλους του. Επίσης οι φίλοι του Α μπορεί και να μην γνωρίζουν καθόλου τη διαδικασία και να βλέπουν τα *video* σαν να είναι δικά τους.

Όταν κάποιος φίλος του Α, έστω Β, θέλει να δει τα *video* του Α, το *agent* λογισμικού του Β επικοινωνεί με το *agent* λογισμικού του Α για να ελέγξει αν τα πιστοποιητικά που παρέχονται από τον *agent* λογισμικού του Β είναι έγκυρα. Ο έλεγχος της εγκυρότητας των πιστοποιητικών δεν είναι το μόνο έργο που θα πρέπει να κάνει ο *agent*. Αν ο agent λογισμικού του Α ανακαλύψει ότι τα πιστοποιητικά που έλαβε από τον Β δεν είναι επαρκή για να του δώσει την πρόσβαση να δει τα *video*, θα ζητήσει από τον *agent* του Β να του παρέχει επιπλέον πιστοποιητικά. Καθώς όλα τα πιστοποιητικά αποθηκεύονται με έναν κατανεμημένο τρόπο, η δουλειά του *agent* του Β είναι να εντοπίσει τα κατάλληλα πιστοποιητικά. Η δυσκολία είναι να εντοπίσει όλα τα απαραίτητα πιστοποιητικά αποτελεσματικά.

Ας υποθέσουμε ότι αργότερα ο Β θέλει να μοιραστεί τα δικά του *video* με τον Α. Θα δημιουργήσει έτσι την δική του κοινότητα φίλων και κάθε μέλος της κοινότητας θα

μπορεί να βλέπει τα *video* του. Επιπλέον, εφόσον ο Β εμπιστεύεται τον Α μπορεί να αποφασίσει ώστε όλα τα μέλη της κοινότητας του Α να έχουν πρόσβαση και στα δικά του *video*. Έτσι λοιπόν ο Β αναθέτει την εξουσιοδότηση στα μέλη της κοινότητας του Α.

Θα μπορούσαν να υπάρχουν και πιο εξεζητημένα σενάρια. Έτσι ο σκοπός είναι να σχεδιαστεί και να υλοποιηθεί ένα εξελιγμένο πλαίσιο διαχείρισης εμπιστοσύνης που απλοποιεί την προστασία των εμπιστευτικών πόρων σε εικονικές κοινότητες. Χρησιμοποιήθηκε μια προσέγγιση της διαχείρισης εμπιστοσύνης που είναι βασισμένη σε ρόλους για να μοντελοποιήσει την εμπιστοσύνη και τις εικονικές κοινότητες. Στην προσέγγιση αυτή χρησιμοποιήθηκε η λογική και ο λογικός προγραμματισμός για την αναπαράσταση πολύπλοκων σχέσεων εμπιστοσύνης που μπορεί να εμφανιστούν στην πραγματική ζωή. Τέλος προτάθηκε μια γλώσσα διαχείρισης εμπιστοσύνης με ένα τυπικό και δηλωτικό νόημα βασισμένο στη σημασιολογία (*semantics*) των λογικών προγραμμάτων. Η έρευνα αυτή διεξάγεται από το *project I-SHARE*. **[33]**

6.7 Χτίζοντας ένα Στοχαστικό Μοντέλο ως προς την Ασφάλεια και την Αξιολόγηση της Εμπιστοσύνης

Η ευρεία χρήση των υπολογιστών και ο μεγάλος όγκος των δεδομένων που μεταφέρονται έχουν καταστήσει το διαδίκτυο σαν την κύρια περιοχή για ανταλλαγή πληροφοριών και ηλεκτρονικό εμπόριο. Οι επιθέσεις στα δίκτυα υπολογιστών που χρησιμοποιούνται για επικοινωνιακούς και οικονομικούς σκοπούς, είναι πιθανό να απειλήσουν την οικονομική και φυσική ευμάρεια των ανθρώπων και των οργανισμών. Για τα σημερινά συστήματα υπολογιστών και επικοινωνίας *(Information and Communication Technology*, *ICT*) χρειάζεται μια συνεχής εκτίμηση του κινδύνου, και επομένως υπάρχει έντονη η ανάγκη για μοντέλα που θα παρέχουν πιθανολογικά μέτρα της λειτουργικής ασφάλειας.

6.7.1 Στοχαστικό Μοντέλο

Κατά τη διάρκεια της τελευταίας δεκαετίας, έγινε σημαντική έρευνα στην εφαρμογή παραδοσιακών και εξαρτώμενων τεχνικών για την ποσοτικοποίηση των χαρακτηριστικών ασφάλειας των συστημάτων *ICT*. Ειδικότερα, οι τεχνικές στοχαστικών μοντέλων όπως οι αλυσίδες *Markov* ή τα στοχαστικά *Petri nets* θεωρήθηκαν ιδιαίτερα υποσχόμενες προσεγγίσεις. Σε ένα εξαρτώμενο πλαίσιο, ένα σύστημα θα είναι συνεχώς ευαίσθητο σε αποτυχίες λογισμικού και υλικού, που μπορεί να μεταφέρουν το σύστημα από μια καλή κατάσταση σε μια κατάσταση αποτυχίας. Συνήθως, αυτές οι μέθοδοι δεν υπολογίζουν τις αποτυχίες από τις κακόβουλες ενέργειες. Ωστόσο, χρησιμοποιώντας την αναλογία μεταξύ της αποτυχίας του συστήματος και ενός ρήγματος της ασφάλειας, είναι πιθανό να μοντελοποιηθεί μια απόπειρα εισβολής με τη μορφή μιας ή περισσότερων αλλαγών κατάστασης που μεταφέρουν το σύστημα σε κατάσταση ρήγματος δηλ. σε μια κατάσταση που αποκλίνει από την ορισμένη πολιτική ασφάλειας. Η χρήση ενός στοχαστικού μοντέλου, που συνδυάζει επιθέσεις ασφάλειας με την παραδοσιακή εξάρτηση των πηγών των λαθών, έχει ένα μεγάλο εύρος εφαρμογών:

- ***Να ποσοτικοποιήσει την ασφάλεια:*** Χρησιμοποιώντας την στατική κατάσταση πιθανοτήτων ενός στοχαστικού μοντέλου, μπορεί κάποιος να υπολογίσει λειτουργικά στοιχεία όπως «τη μέση τιμή προς το συμβιβασμό ασφάλειας» του συστήματος,
- ***Για ανάλυση κύκλου εργασιών:*** Κάποιος μπορεί να αξιολογήσει την πιθανή επίδραση των αντιμέτρων ασφάλειας, πριν τα υλοποιήσει,

- Σαν μια μέθοδο που βοηθάει τους διαχειριστές να βρουν ***βέλτιστες στρατηγικές άμυνας*** και να υπολογίσουν τις αναμενόμενες απώλειες που σχετίζονται με τις στρατηγικές.

Ωστόσο, οι επιθέσεις δεν χαρακτηρίζονται πάντα από μοντέλα τυχαίας φύσης. Οι περισσότεροι επιτιθέμενοι δρουν από πρόθεση και υπολογίζουν τις πιθανές συνέπειες (ικανοποίηση, όφελος και κατάσταση ενάντια στην προσπάθεια και τον κίνδυνο των ενεργειών τους) πριν γίνουν οι ενέργειες. Μια από τις προκλήσεις που απομένουν αφορά στο πώς θα ενσωματωθεί η συμπεριφορά του επιτιθέμενου μέσα στα στοχαστικά μοντέλα.

6.7.2 Το Μοντέλο του Παιχνιδιού

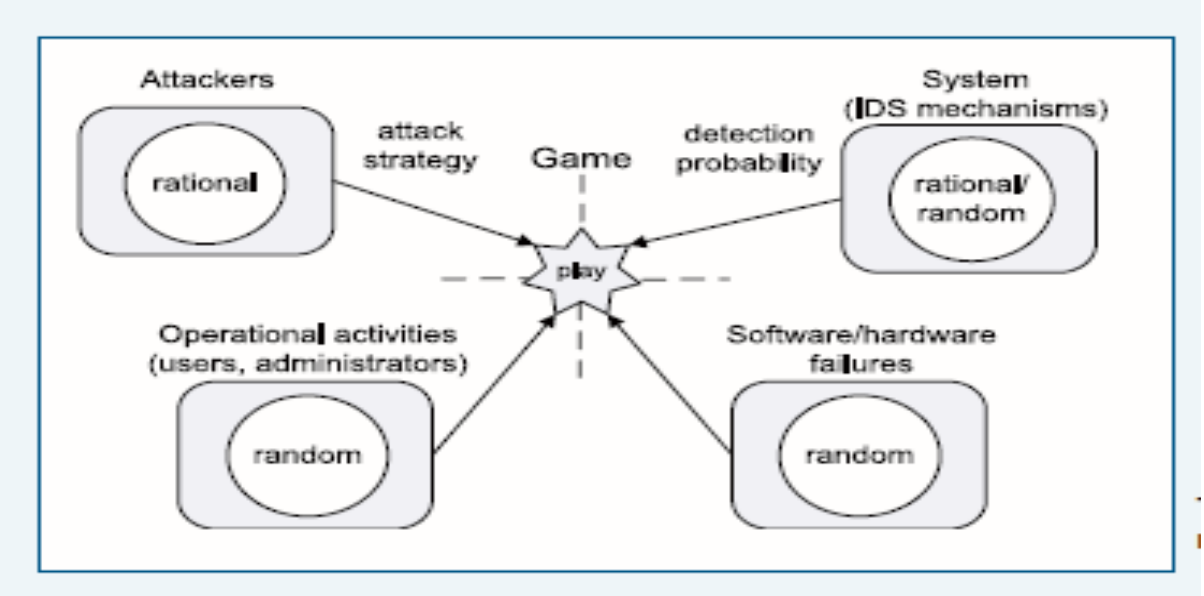
Στο κέντρο *Q2S* στο *NTNU* (Νορβηγία) υλοποιείται ένα στοχαστικό μοντέλο που μπορεί να χρησιμοποιηθεί για να αξιολογήσει την ασφάλεια και την αξιοπιστία των *ICT*. Το μοντέλο αυτό θεωρεί όλα τα στοιχεία που μπορεί να επηρεάσουν τα χαρακτηριστικά της ασφάλειας ή της εξάρτησης του συστήματος, που περιλαμβάνουν:

- Την φυσιολογική συμπεριφορά του χρήστη,
- Τις δραστηριότητες διαχείρισης,
- Τις τυχαίες αποτυχίες του λογισμικού και του υλικού,
- Τις εκ προθέσεως επιθέσεις.

Για να ενσωματωθούν οι εκ προθέσεως επιθέσεις στο μοντέλο, θα πρέπει να προβλεφθεί η συμπεριφορά του επιτιθέμενου. Χρησιμοποιώντας ένα στοχαστικό μοντέλο παιχνιδιού, μπορούμε να υπολογίσουμε την αναμενόμενη συμπεριφορά των επιτιθέμενων για ένα διαφορετικό αριθμό προφίλ επιτιθέμενων.

Το μοντέλο παιχνιδιού που φαίνεται στο ***σχήμα 45*** βασίζεται στην έννοια ***ανταμοιβή/κόστος***. Αυτό θεωρεί ότι οι επιτιθέμενοι θα υπολογίσουν την ανταμοιβή των πετυχημένων ενεργειών τους έναντι του πιθανού κόστους της ανίχνευσης πριν δράσουν και ότι πάντα θα προσπαθούν να μεγιστοποιήσουν το αναμενόμενο αποτέλεσμα της επίθεσης. Οι δυναμικές των καταστάσεων των στοχαστικών παιχνιδιών διαμορφώνουν μια αλυσίδα *Markov*, υποθέτοντας ότι οι επιτιθέμενοι, οι χρήστες και οι διαχειριστές δεν αλλάζουν την συμπεριφορά τους στο χρόνο. Έχοντας λύσει το στοχαστικό παιχνίδι, η αναμενόμενη συμπεριφορά του επιτιθέμενου μπορεί να αντικατοπτριστεί στις μεταβάσεις μεταξύ των καταστάσεων του μοντέλου του συστήματος, ζυγίζοντας το κόστος της μετάδοσης σύμφωνα με μια διανομή πιθανότητας. Στο τελικό στάδιο, η αντίστοιχη στοχαστική διαδικασία χρησιμοποιείται για να μετρήσει τα μέτρα ασφάλειας του συστήματος, με έναν όμοιο τρόπο με την κοινή ανάλυση διαθεσιμότητας και αξιοπιστίας των συστημάτων *ICT*.

Οι προηγούμενες έρευνες έχουν δείξει ότι τα στοχαστικά μοντέλα μπορούν να χρησιμοποιηθούν για να μοντελοποιήσουν και να αναλύσουν την αξιοπιστία των συστημάτων *ICT* με όρους χαρακτηριστικών ασφάλειας και εξάρτησης. Η έρευνα, δηλώνει ότι η θεωρία των παιχνιδιών αποτελεί ένα βολικό εργαλείο για ενσωμάτωση της αναμενόμενης συμπεριφοράς των επιτιθέμενων σε τέτοια μοντέλα. Ωστόσο, η επαλήθευση της ικανότητας της μεθόδου να προβλέψει τις επιθέσεις της πραγματικής ζωής θα χρειαστεί περαιτέρω έρευνα, περιλαμβάνοντας την αξιολόγηση του μοντέλου έναντι στα εμπειρικά δεδομένα. **[34]**



Σχήμα 45: Οι αλληλεπιδράσεις μεταξύ του επιτιθέμενου και του συστήματος μοντελοποιημένων σαν ένα στοχαστικό παιχνίδι

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Αντίθετα με τα αναλογικά δεδομένα, όπως είναι η υποκειμενική ανάμνηση ενός μάρτυρα του οποίου η πειστικότητα και η αξιοπιστία διερευνώνται σε βάθος, τα ψηφιακά δεδομένα τα οποία μπορούν να πάρουν μόνο μία από δυο αδιαμφισβήτητες τιμές (μηδέν ή ένα) μπορούν να παρερμηνευθούν από το μέσο άνθρωπο ως προικισμένα με εγγενή και αδιαφιλονίκητη αλήθεια.

Στην πραγματικότητα συμβαίνει το ακριβώς αντίθετο. Αντίθετα με τα παραδοσιακά, αναλογικά δεδομένα και τις αποδείξεις των οποίων οι αλλοιώσεις μπορεί να ανιχνευθούν από τους ειδικούς με τον κατάλληλο εξοπλισμό, τα ψηφιακά δεδομένα είναι δυνατόν να παραποιηθούν και ανάλογα με την εξειδίκευση του παραποιητή, η αλλαγή μπορεί να μην είναι ανιχνεύσιμη ανεξάρτητα από τις ικανότητες των δικανικών ψηφιακών αναλυτών και από τον εξοπλισμό που χρησιμοποιούν.

Ο λόγος είναι απλός: Τα «μηδέν» και «ένα» των ψηφιακών δεδομένων μπορεί να αλλάξουν και αν έχουν ληφθεί κάποιες ελάχιστες προφυλάξεις από τον παραποιητή, δεν θα υπάρχουν ίχνη είτε της αλλαγής είτε της ταυτότητας του ανθρώπου που την έκανε.

Η δικανική ψηφιακή ανάλυση μπορεί να καθορίσει τι υπάρχει στα ψηφιακά μέσα αποθήκευσης του υπόπτου τη στιγμή της δικανικής έρευνας, αλλά δεν μπορεί να καθορίσει ποιός τα έβαλε εκεί και επίσης πότε και με ποιό τρόπο, όπως δεν μπορεί να προσδιορίσει αν τα δεδομένα έχουν αλλάξει. Η μόνη εξαίρεση μπορεί να προέλθει από την ομολογία ενός υπόπτου, αλλά ακόμα κι αυτή δεν αποτελεί απόδειξη, δεδομένων των πολλών «λανθασμένων» ομολογιών στην ιστορία της δίωξης του εγκλήματος.

Η πιθανότητα μη απόδοσης δικαιοσύνης είναι επομένως πολύ μεγάλη, δεδομένου ότι πολλοί δικηγόροι, δικαστές και ένορκοι δεν είναι γνώστες των εσωτερικών λεπτομερειών της επιστήμης των υπολογιστών. Επιπλέον, οι κατήγοροι των κακόβουλων εισβολέων εκμεταλλεύονται αυτή την άγνοια και ισχυρίζονται ψευδώς ότι οι ψηφιακές αποδείξεις αποτελούν απόδειξη της ενοχής των κατηγορούμενων.

Το μυστικό αυτό που αφορά στις ψηφιακές αποδείξεις, δεν κοινολογείται ανοιχτά από την βιομηχανία της δικανικής ψηφιακής ανάλυσης και από τους κατήγορους, αφού και οι δύο αυτές πλευρές επικεντρώνονται στα θέματα της συλλογής, της διατήρησης και της παρουσίασης των ψηφιακών αποδείξεων που μπορεί πράγματι να είναι απρόσβλητες αν όλα τα παραπάνω γίνουν σωστά, όπως η διαδικασία της αλυσίδας επιτήρησης (*chain of custody*).

Ας θεωρήσουμε ένα παράδειγμα ψηφιακής απόδειξης. Ο σκληρός δίσκος ενός υπόπτου έχει κατασχεθεί, είναι υποκείμενος σε δικανική ψηφιακή ανάλυση και έχει δημιουργηθεί μια αναφορά για το δικαστήριο η οποία αναφέρει ότι ο σκληρός δίσκος περιέχει τα εξής αρχεία και ότι τα αρχεία αυτά είχαν μετονομαστεί ή τυπωθεί σε μια συγκεκριμένη ημερομηνία, αντικρούοντας έτσι τα επιχειρήματα του ύποπτου ότι δεν γνώριζε την ύπαρξη αυτών των αρχείων.

Ένα τυπικό δικαστήριο θα δεχτεί την αναφορά που έχει ετοιμάσει η δικανική ανάλυση. Στην πραγματικότητα δεν θα πρέπει να την δεχτεί αψήφιστα για τους παρακάτω λόγους:

1. Τα δεδομένα που βρίσκονται στο σκληρό δίσκο κάποιου, μπορεί να έχουν μπει στο δίσκο (ή σε κάποιο άλλο μέσο αποθήκευσης) με κάποιον από τους παρακάτω τρόπους, χωρίς να το γνωρίζει ο ύποπτος. Όλα αυτά τα μονοπάτια λαθραίας εισόδου δεδομένων είναι πολύ γνωστά και χρησιμοποιούνται σε καθημερινή βάση. Καταστάσεις στις οποίες αυτό συμβαίνει περιλαμβάνουν:

I. Ο σκληρός δίσκος δεν ήταν καινούργιος όταν τον απέκτησε ο ύποπτος και περιείχε αρχεία από προηγούμενο ιδιοκτήτη ή χρήστη. Αυτό μπορεί να συμβεί ακόμα και στις περιπτώσεις που κάποιος αγοράζει έναν καινούργιο υπολογιστή, ο οποίος μπορεί να έχει επιστραφεί από τον προηγούμενο αγοραστή. Ακόμα και αν ο σκληρός δίσκος έχει καθαριστεί από τον πωλητή και το λογισμικό του έχει εγκατασταθεί εκ νέου, δεν υπάρχει καμιά εγγύηση ότι δεν έχουν αφεθεί κάποια υπολείμματα δεδομένων. Γι αυτό και υπηρεσίες στρατού και ασφάλειας στις περισσότερες χώρες καταστρέφουν τους δίσκους όταν δεν τους χρησιμοποιούν πια, αντί να σβήνουν τα δεδομένα τους.

II. Ένας μεγάλος αριθμός από πακέτα λογισμικού (που αναφέρονται ως *adware* και *spyware*- ***κεφ. 2.2***) αναλαμβάνουν να εγκαταστήσουν χωρίς την άδεια και τη γνώση του χρήστη αρχεία με διαφημίσεις και την δυνατότητα για το δημιουργό του λογισμικού να εισδύσει στον υπολογιστή του χρήστη μέσω του διαδικτύου ή άλλου δικτύου. Αν αυτή η δυνατότητα διείσδυσης ανακαλυφθεί από μια τρίτη οντότητα που μπορεί να είναι κάποιος εισβολέας ο οποίος ψάχνει συστηματικά για υπολογιστές που περιέχουν ***«μια είσοδο πίσω πόρτας»*** *(back door entry),* είναι εύκολο να εισαχθούν αρχεία στο σκληρό δίσκο του ύποπτου χωρίς να το γνωρίζει.

III. Η απόκτηση πλήρους ελέγχου ενός υπολογιστή μέσω του διαδικτύου δεν απαιτεί καν την εγκατάσταση λογισμικού *adware* ή *spyware*. Η *Microsoft* αναγνωρίζει και δημοσιοποιεί σε σχεδόν εβδομαδιαία βάση έναν αριθμό από «τρύπες» ασφάλειας στα λειτουργικά της συστήματα και στις εφαρμογές της. Αυτό ισχύει ειδικότερα για τον *Internet Explorer* που επιτρέπει στον καθένα να αποκτήσει τον πλήρη έλεγχο του υπολογιστή ενός χρήστη που είναι συνδεδεμένος στο διαδίκτυο και να εισάγει εν αγνοία του χρήστη αρχεία στον υπολογιστή του. Ανακαλύψεις τέτοιου είδους ***«εισόδων πίσω πόρτας»*** στους υπολογιστές εμφανίζονται κατά μέσο όρο μία κάθε εβδομάδα, τα τελευταία χρόνια.

IV. Κατά την αναζήτηση σελίδων στο διαδίκτυο, συχνά λόγω λάθους στην πληκτρολόγηση της διεύθυνσης, μπορεί να βρεθούμε σε κάποια σελίδα ύποπτη. Επίσης οι εισβολείς συχνά παραποιούν τις εισόδους στα ονόματα τομέων (*Domain Name Servers, DNS*) έτσι ώστε να παραποιούν έναν φάκελο ο οποίος προσπελαύνεται κάθε φορά που πληκτρολογούμε το όνομα μιας σελίδας διαδικτύου που θέλουμε να δούμε.

V. Ακόμα κι αν δεν συμβεί κάτι από τα παραπάνω, θα πρέπει να δεχτούμε το γεγονός ότι το διαδίκτυο χρησιμοποιείται δωρεάν από το χρήστη. Εφόσον όμως τίποτα στη ζωή μας δεν είναι πραγματικά δωρεάν, η πηγή εσόδων για πολλές σελίδες *web* προέρχεται από διαφημίσεις, με τη μορφή αναδυόμενων διαφημίσεων, εικόνων, κειμένου κ.λπ. Μπορεί να συμβεί αυτές οι εικόνες να μην αφορούν σε καλλυντικά ή άλλα είδη αλλά να είναι εικόνες γυμνών ανήλικων ατόμων. Και μόνο η ύπαρξή τους στον υπολογιστή ενός ατόμου, είναι αρκετή για να τον ελέγξουν οι διωκτικές αρχές ή και να τον κλείσουν στη φυλακή σε πολλές χώρες. Ενώ κάποιος περιηγείται το διαδίκτυο και επισκέπτεται διαφορετικές σελίδες *web,* οι εικόνες των σελίδων που επισκέπτεται αποθηκεύονται στο σκληρό δίσκο του εκτός εάν ο χρήστης αλλάξει τις ρυθμίσεις του *web browser* ώστε να

μην αποθηκεύει τίποτα στην *cache*. Σαν αποτέλεσμα, μπορεί να είναι πολύ δύσκολο να πειστεί ένας δικαστής ή οι ένορκοι για το γεγονός ότι ο κατηγορούμενος δεν γνωρίζει πώς βρέθηκαν αυτές οι εικόνες στον υπολογιστή του.

VI. Πολύ συχνά, το συγγενικό περιβάλλον του χρήστη ενός υπολογιστή είναι πιθανό να χρησιμοποιεί τον ίδιο υπολογιστή. Στην περίπτωση αυτή είναι πολύ πιθανό αυτά τα άτομα να έχουν επισκεφτεί σελίδες *web* που δεν εγκρίνει ο χρήστης του υπολογιστή. Οι εικόνες από τέτοιου είδους σελίδες παραμένουν στον υπολογιστή, μέχρι να γράψουμε πάνω από αυτά τα αρχεία των οποίων την ύπαρξη δεν γνωρίζουμε.

VII. Τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (*spam*) είναι πάρα πολύ κοινά. Πολλά από αυτά χρησιμοποιούν «κάλυψη» διαφημίζοντας εύκολο πλουτισμό, χάσιμο βάρους, συνταγές αιώνιας νεότητας, σεξ και άλλα είδη που τραβούν το ενδιαφέρον. Οι περισσότεροι τα σβήνουν αμέσως ή τα αγνοούν. Αλλά εδώ βρίσκεται και το πρόβλημα. Παρά το γεγονός ότι σβήνοντας τα *spam* δεν σβήνουμε τα πάντα (απλώς λέμε στον υπολογιστή ότι ο χώρος που καταναλώνεται στον δίσκο από αυτό το *email*, το οποίο στην πραγματικότητα δεν σβήνεται ποτέ, μπορεί να το χρησιμοποιήσει ο υπολογιστής στο μέλλον όπως θέλει). Σχεδόν κανένας από εμάς δεν κάνει τον κόπο να σβήσει και τα προσαρτήματα αυτών των *email* και ακόμα και αν το κάνουμε αυτά τα προσαρτήματα στην πραγματικότητα δεν σβήνονται από το δίσκο, όπως αναφέρθηκε και πιο πάνω. Τελικά μόνο οι ειδικοί των υπολογιστών, θα γράψουν πάνω από το ενοχλητικό προσάρτημα, επειδή τα *Windows* δεν προσφέρουν αυτή την δυνατότητα. Θα πρέπει κάποιος να αγοράσει ειδικό λογισμικό για να το πετύχει αυτό. Και ακόμη και αν κάποιος αγοράσει λογισμικό για να γράψει πάνω από το προσάρτημα, το όνομα του αρχείου που από μόνο του μπορεί να είναι ένα ενοχοποιητικό στοιχείο, και το οποίο αποθηκεύεται σε μια διαφορετική περιοχή του σκληρού δίσκου από το ίδιο το αρχείο δεν αντικαθίσταται και παραμένει προς μεγάλη ικανοποίηση των δικανικών ψηφιακών ερευνητών που ίσως ερευνήσουν μελλοντικά το σκληρό δίσκο. Έτσι και πάλι, ένας ενδιαφερόμενος θα δυσκολευτεί πολύ να πείσει έναν δικαστή που δεν έχει τεχνικές γνώσεις, για το πώς μπορεί να βρέθηκαν στο δίσκο του τα αρχεία ή έστω και τα ονόματά τους που τον ενοχοποιούν.

VIII. Η ασύρματη πρόσβαση έχει αυξηθεί με έναν εκρηκτικό τρόπο παγκόσμια και σήμερα υπάρχει σχεδόν παντού, σε δημόσιους χώρους (εστιατόρια, ξενοδοχεία, αεροδρόμια κ.λπ.) όπως και στα περισσότερα σπίτια. Επίσης παντού υπάρχουν αναφορές για το πόσο ανασφαλές είναι αυτό το πρότυπο. Το υλικό του *Wi-Fi* είναι διαμορφωμένο ώστε να μην απαιτεί κωδικό πρόσβασης, κρυπτογράφηση και γενικά κάποιου είδους ασφάλεια. Οι περισσότεροι χρήστες δεν ασχολούνται με τη διόρθωση αυτής της ατέλειας και χρησιμοποιούν τις συσκευές *Wi-Fi* όπως είναι. Επίσης σήμερα ένα οικιακό *Wi-Fi* μπορεί να προσπελαστεί ακόμα και 5 μίλια μακριά από το σπίτι. Αν κάποιος εισβολέας συνδεθεί σε κάποιο οικιακό *Wi-Fi*, εφόσον δεν υπάρχει καμιά ασφάλεια, ο μη εξουσιοδοτημένος χρήστης έχει πλήρη πρόσβαση στον υπολογιστή και στη σύνδεση διαδικτύου του θύματος. Αυτό σημαίνει ότι είναι δυνατό να τοποθετηθούν αρχεία στον δίσκο του θύματος χωρία να το γνωρίζει και

επίσης να μείνουν στα αρχεία του *ISP* ίχνη παράνομης διαδικτυακής δραστηριότητας. Σαν αποτέλεσμα ο χρήστης του υπολογιστή ενοχοποιείται για παράνομες δραστηριότητες τις οποίες όμως δεν έχει κάνει.

IX. Αργά ή γρήγορα όλοι οι υπολογιστές παθαίνουν βλάβη. Η τυπική διαδικασία είναι να δώσουμε τον υπολογιστή για επισκευή σε κάποιον ειδικό. Οι τεχνικοί έχουν έτσι τη δυνατότητα να βάλουν πιθανά ενοχοποιητικά δεδομένα στον υπολογιστή (όπως για παράδειγμα εργαλεία *hacking* τα οποία τα χρησιμοποιούν για διάγνωση ή για επισκευή του υπολογιστή). Είναι λοιπόν πιθανό, καιρό αργότερα να βρεθούν αυτά τα ενοχοποιητικά στοιχεία στον υπολογιστή του χρήστη χωρίς αυτός να μπορεί να τα δικαιολογήσει (συχνά δεν θυμάται και την επισκευή που έκανε).

2. Οι δικανικοί ψηφιακοί αναλυτές θέλουν να τεκμηριώνουν τα ευρήματά τους επισημαίνοντας την χρονοσήμανση *(date/time stamp)* που σχετίζεται με τα διαφορετικά αρχεία του υπολογιστή, σαν να είναι αυτή η πληροφορία απρόσιτη από οποιονδήποτε. Στην πραγματικότητα αυτό είναι εντελώς λάθος. Η χρονοσήμανση, όπως και κάθε άλλο *bit* πληροφορίας που βρίσκεται στα μαγνητικά μέσα του υπολογιστή, μπορεί να αλλάξει (χωρίς να υπάρχουν ίχνη της αλλαγής) έτσι ώστε η «απόδειξη» που έχει βρεθεί από τον δικανικό ψηφιακό αναλυτή να τεκμηριώσει αυτό που στην πραγματικότητα θέλει κάποιος άλλος να τεκμηριωθεί. Αυτό που χρειάζεται είναι ένα έτοιμο λογισμικό γνωστό σαν *disk editor*, το οποίο μπορεί να αλλάξει τα ***μεταδεδομένα*** (*metadata*) δηλ. δεδομένα του τύπου ποιος έκανε κάτι και πότε, όπως τη χρονοσήμανση.

3. Αντίθετα με τις παραδοσιακές φωτογραφίες για τις οποίες ένας έμπειρος ερευνητής μπορεί να προσδιορίσει αν έχουν παραποιηθεί, οι ψηφιακές φωτογραφίες μπορεί να παραποιηθούν με τρόπο ώστε κανένας ειδικός να μην μπορεί να το αντιληφθεί. Έτσι, το γνωμικό ότι οι φωτογραφίες δεν ψεύδονται, στην ψηφιακή εποχή δεν ισχύει.

4. Όπως και με την ψηφιακή φωτογραφία, τα ίδια ισχύουν και με τον ψηφιακό ήχο. Αντίθετα με τον αναλογικό ήχο, τα ψηφιοποιημένα αρχεία του ήχου μπορεί εύκολα να παραποιηθούν. Πολλές φορές οι δικανικοί ψηφιακοί αναλυτές δεν είναι αρκετά έμπειροι ώστε να αντιληφθούν την παραποίηση.

Συμπερασματικά, στα δικαστήρια σήμερα βιώνουμε ένα νέο φαινόμενο σε σχέση με το ψηφιακό έγκλημα. Όλοι αποθηκεύουμε ολοένα και περισσότερες πληροφορίες στους υπολογιστές μας οι οποίες είναι σχετικές με τη ζωή και τις δραστηριότητές μας. Αυτό έχει σαν αποτέλεσμα μια μεγάλη αύξηση των δικανικών αναλύσεων υπολογιστών σε κατασχεμένους και ύποπτους υπολογιστές, βασισμένη στη (λάθος) υπόθεση ότι «στον υπολογιστή βρίσκονται αυτά που βάλαμε εμείς μέσα».

Το νομικό και κοινωνικό πρόβλημα σχετικά με αυτό το θέμα, είναι ότι τα περισσότερα άτομα που ασχολούνται στα επαγγέλματα δίωξης των εγκλημάτων δεν είναι σχετικά με τα θέματα που παρουσιάστηκαν πιο πάνω, σύμφωνα με τα οποία τα δεδομένα που βρίσκονται σε έναν υπολογιστή και παρουσιάζονται σαν αποδείξεις, στην πραγματικότητα δεν είναι πάντα αποδείξεις αλλά μπορεί να έχουν βρεθεί στον υπολογιστή με κάποιο άλλο τρόπο.

Επίσης οι αποδείξεις που έχουν βρεθεί στον *ISP* ενός ύποπτου, μπορεί να μην είναι αποδείξεις στην πραγματικότητα καθώς ο διαδικτυακός λογαριασμός ενός χρήστη είναι εύκολο να προσπελαστεί από τρίτα άτομα, χωρίς να το γνωρίζει ο χρήστης.

Οι ψηφιακές αποδείξεις θα πρέπει να ελέγχονται εξονυχιστικά, ανεξάρτητα από τις δυνατότητες και την εμπειρία του δικανικού ψηφιακού αναλυτή ο οποίος ενδιαφέρεται κυρίως να τις παρουσιάσει. Ενώ το τμήμα της αλυσίδας επιτήρησης *(chain of custody)* που σχετίζεται με τον τρόπο χειρισμού των αποδείξεων, είναι πιθανό να είναι άψογο, τα ψηφιακά δεδομένα πάνω στα οποία έγινε η δικανική ανάλυση μπορεί να έχουν αλλοιωθεί εύκολα από κάποιον τρίτο και χωρίς να υπάρχουν ίχνη αυτής της αλλοίωσης. Έτσι, πολύ συχνά οι ψηφιακές αποδείξεις στην ουσία δεν αποδεικνύουν κάτι. Αυτό το γεγονός όμως αποτελεί και τη μεγαλύτερη πρόκληση. Οι ψηφιακές αποδείξεις θα πρέπει να συλλέγονται και να αξιολογούνται σύμφωνα με τους κανόνες της δικανικής ψηφιακής ανάλυσης από ερευνητές με ισχυρό προφίλ στην επιστήμη των υπολογιστών αλλά και με επαρκείς γνώσεις σε νομικά θέματα. Από την άλλη μεριά, η ραγδαία διάδοση των ασύρματων δικτύων και του *internet* και η ευρεία χρήση των υπολογιστών τόσο σε οικιακό επίπεδο όσο και σε επίπεδο οργανισμών και υπηρεσιών, εισάγουν προκλήσεις για εκμετάλλευση από το οργανωμένο έγκλημα αλλά και προκλήσεις στο πεδίο της επιστήμης για την ανάσχεση των επιθέσεων και τη διαφύλαξη της ιδιωτικότητας της ψηφιακής επικοινωνίας. Οι οργανισμοί και οι κυβερνήσεις έχουν καταλάβει την αναγκαιότητα αυτή και χρηματοδοτούν και ενθαρρύνουν την έρευνα στο πεδίο της ιδιωτικότητας των ψηφιακών επικοινωνιών και της διαχείρισης της εμπιστοσύνης.

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Asset	Αγαθό
Slack space	Αδρανής περιοχή
Chain of custody	Αλυσίδα επιτήρησης
Sand boxing	Άμμος πυγμαχίας
Identification	Αναγνώριση
Signature based detection	Αναγνώριση βασισμένη σε υπογραφές
Analysis	Ανάλυση
Root cause analysis	Ανάλυση αιτίων
Code emulation	Ανάλυση κώδικα
Broadcast	Αναμετάδοση
Tracerouting	Ανίχνευση διαδρομής
Port scanning	Ανίχνευση θυρών
Operating system detection	Ανίχνευση λειτουργικού συστήματος
Anonymity	Ανωνυμία
Sender anonymity	Ανωνυμία αποστολέα
Receiver anonymity	Ανωνυμία παραλήπτη
Evaluation	Αξιολόγηση
Privacy requirements	Απαιτήσεις ιδιωτικότητας
Address spoofing	Απάτη διευθύνσεων
Imaging	Απεικόνιση
Threat	Απειλή
Remote user	Απομακρυσμένος χρήστης
Data hiding	Απόκρυψη αρχείων
Abstract digital forensics	Απόσπασμα ψηφιακής δικανικής ανάλυσης
Snippets	Αποσπάσματα προγράμματος
Network mapping	Αποτύπωση δικτύου
Sequence number	Αριθμός ακολουθίας
Denial of service	Άρνηση παροχής υπηρεσίας
Log file	Αρχείο καταγραφής
System log	Αρχείο καταγραφής συστήματος
Host file	Αρχείο οικείου υπολογιστή
Information systems security	Ασφάλεια πληροφοριακών συστημάτων
Authentication	Αυθεντικοποίηση
Root account	Βασικός λογαριασμός
Root user	Βασικός χρήστης
Fair information practices	Βέλτιστες πρακτικές χρήσης υπηρεσιών πληροφορικής
Privacy policy language	Γλώσσα πολιτικής ιδιωτικότητας
Graphical user interface	Γραφικό περιβάλλον χρήστη
Call data records	Δεδομένα κλήσεων
Forensic process	Διαδικασία ψηφιακής δικανικής ανάλυσης
Internet protocol address	Διαδικτυακή διεύθυνση
War dialing	Διάλογος πολέμου
Key sharing	Διαμοίραση κλειδιού

Configuration	Διαμόρφωση
Management analysis	Διαχειριστική ανάλυση
International mobile equipment number	Διεθνής αριθμός αναγνώρισης κινητού εξοπλισμού
International mobile subscriber identification number	Διεθνής αριθμός αναγνώρισης κινητών συνδρομητών
Interface	Διεπαφή
Investigator	Διερευνητής
Source IP address	Διεύθυνση IP πηγής
File system forensics	Δικανική ανάλυση αρχείων συστημάτων
Network forensics	Δικανική ανάλυση δικτύων
Malware forensics	Δικανική ανάλυση κακόβουλου λογισμικού
Mobile device forensics	Δικανική ανάλυση κινητών συσκευών
Computer forensics	Δικανική ανάλυση υπολογιστών
Forensic computer analysis	Δικανική ανάλυση υπολογιστών
Network based systems	Δικτυακά συστήματα
Web	Διαδίκτυο
Floppy disk	Δισκέττα
Router	Δρομολογητής
Network router	Δρομολογητής δικτύου
Just in time validation	Έγκαιρη επικύρωση
Computer related crime	Έγκλημα σχετιζόμενο με υπολογιστές
Virtual private network	Εικονικό ιδιωτικό δίκτυο
Virtual subsystems	Εικονικό υποσύστημα
Hacker	Εισβολέας σε υπολογιστή
Exploit of vulnerabilities	Εκμετάλλευση ευπαθειών/αδυναμιών
Incident postmortem forensics	Εκτός λειτουργίας ή παθητική διερεύνηση
White box testing	Έλεγχος λευκού κουτιού
Black box testing	Έλεγχος μαύρου κουτιού
Role based access control	Έλεγχος πρόσβασης βάσει ρόλων
Active scanning	Ενεργή σάρωση
Live forensics	Εν λειτουργία ή ενεργητική διερεύνηση
Event unification	Ενοποίηση γεγονότων
Goal mining	Εξόρυξη στόχων
Authorization	Εξουσιοδότηση
Server	Εξυπηρετητής
Mail server	Εξυπηρετητής ηλεκτρονικού ταχυδρομείου
Exploits of vulnerabilities	Εκμετάλλευση ευπαθειών (αδυναμιών)
Context data	Εξωτερικά δεδομένα
Iteration	Επανάληψη
Refinement	Επαναπροσδιορισμός
Password attacks	Επιθέσεις κωδικών πρόσβασης
Verification	Επαλήθευση
Validation	Επικύρωση
Media management layer	Επίπεδο διαχείρισης αποθηκευτικών μέσων
Application layer	Επίπεδο εφαρμογών
File system layer	Επίπεδο συστήματος αρχείων
Digital and multimedia sciences	Επιστήμη δικανικής ψηφιακής ανάλυσης

Content data	Εσωτερικά δεδομένα
Readiness	Ετοιμότητα
Versatile scanning tools	Ευέλικτα εργαλεία σάρωσης
Volatile	Ευμετάβλητα
Heuristic analysis	Ευρετική ανάλυση
Electronic communications	Ηλεκτρονικές υπηρεσίες
Privacy of the person	Ιδιωτικότητα του ατόμου
Virtual private network	Ιδιωτικό εικονικό δίκτυο
Virus, Worm, Trojan horse	Ιός
Web site	Ιστοσελίδα
Footprinting	Ιχνηλάτιση
Malware, Malicious code	Κακόβουλο λογισμικό
Spam	Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου
Subscriber Identity number	Κάρτα σύνδεσης συνδρομητή
Fragmentation	Κατακερματισμός
Directory	Κατάλογος
System directory	Κατάλογος συστήματος
Administrator acceptable use statement	Κατάσταση αποδεκτής χρήσης από διαχειριστή
Partner acceptable use statement	Κατάσταση αποδεκτής χρήσης από εταίρο
Usage policy statement	Κατάσταση πολιτικής χρήσης
Central processing unit	Κεντρική μονάδα επεξεργασίας
Deployment	Κλιμάκωση
Social engineering	Κοινωνική μηχανική
Cybercrime	Κυβερνο-έγκλημα
Cellular automata	Κυψελωτά αυτόματα
Password	Κωδικός πρόσβασης
Operating system	Λειτουργικό σύστημα
Access control list	Λίστα ελέγχου πρόσβασης
Switch	Μεταγωγέας
Dial up modem	Μετασχηματιστής σύνδεσης
Network address translation	Μετάφραση διευθύνσεων δικτύου
Hop count	Μέτρηση αλμάτων
Unobservality	Μη παρατηρησιμότητα
Unlikability	Μη συνδεσιμότητα
Domain model	Μοντέλο πεδίου
Format	Μορφοποίηση
Neural networks	Νευρονικά δίκτυα
Integrated digital investigation	Ολοκληρωμένη ψηφιακή έρευνα
Emergency response team	Ομάδα επείγουσας απάντησης
User name	Όνομα πρόσβασης
Domain name	Όνομα τομέα
Agent	Οντότητα
Global system for mobile communications	Παγκόσμιο σύστημα κινητών επικοινωνιών
Universal mobile telecommunication system	Παγκόσμιο σύστημα κινητών επικοινωνιών $4^{ης}$ γενιάς
Electronic communication network provider	Πάροχος δικτύου ηλεκτρονικών επικοινωνιών

Internet service provider	Πάροχος υπηρεσιών διαδικτύου
Identification field	Πεδίο αναγνώρισης
Session hijacking	Πειρατεία συνόδου
Client	Πελάτης
Code walkthrough	Περιδιάβαση κώδικα
Incident	Περιστατικό
Test plan	Πλάνο ελέγχου
Flood	Πλημμύρα
Informational privacy	Πληροφοριακή ιδιωτικότητα
Information technology system	Πληροφοριακό σύστημα
Access control policy	Πολιτική ελέγχου πρόσβασης
Default	Προεπιλεγμένο
Data protection	Προστασία δεδομένων
Personal data	Προσωπικά δεδομένα
Personal pseudonyms	Προσωπικά ψευδώνυμα
Session initiation protocol	Πρωτόκολλο αρχικοποίησης συνόδου
User datagram protocol	Πρωτόκολλο δεδομενογράμματος χρήστη
Internet Protocol	Πρωτόκολλο διαδικτύου
Simple Network Management System	Πρωτόκολλο Διαχείρισης Δικτύου
Transmission control protocol	Πρωτόκολλο ελέγχου μεταφοράς
Internet Control Message Protocol	Πρωτόκολλο ελέγχου μηνυμάτων διαδικτύου
File transfer protocol	Πρωτόκολλο μεταφοράς αρχείων
Simple mail transfer protocol	Πρωτόκολλο μεταφοράς ηλεκτρονικού ταχυδρομείου
Voice over the internet protocol	Πρωτόκολλο φωνής μέσω διαδικτύου
Network time protocol	Πρωτόκολλο ώρας δικτύου
Pattern	Πρότυπο
Gateway	Πύλη
Kernel	Πυρήνας
Scanning	Σάρωση
Vulnerability scanning	Σάρωση ευπαθειών
Blog	Σελίδα δικτύωσης
Policy decision point	Σημείο απόφασης πολιτικής
Policy enforcement point	Σημείο επιβολής πολιτικής
Password cracking	Σπάσιμο κωδικών πρόσβασης
Privacy goal	Στόχος ιδιωτικότητας
Protection goal	Στόχος προστασίας
Covert channel	Συγκαλυμμένο κανάλι
Comparative analysis	Συγκριτική ανάλυση
Symmetric cryptography	Συμμετρική κρυπτογραφία
Hash function	Συνάρτηση κατακερματισμού
Link	Σύνδεση
Chat session	Σύνοδος συζήτησης
Intrusion detection system	Σύστημα ανίχνευσης εισβολών
Early warning system	Σύστημα έγκαιρης ειδοποίησης
Peer-to-Peer system	Σύστημα ομότιμων
Domain name system	Σύστημα ονοματοδοσίας τομέα
Honeypot	Σύστημα παγίδας

Geographical positioning system	Σύστημα πλοήγησης
Computer related	Σχετιζόμενο με υπολογιστές
Stack	Σωρός
Program stack	Σωρός προγράμματος
Firewall	Τείχος προστασίας
Requirements engineering	Τεχνολογία απαιτήσεων
Privacy enhancing technologies	Τεχνολογίες βελτίωσης της ιδιωτικότητας
Dial up connection	Τηλεφωνική σύνδεση
Sector	Τομέας
Local area network	Τοπικό δίκτυο
3 way handshake	Τρίδρομη χειραψία
Hybrid cryptography	Υβριδική κρυπτογραφία
Hardware	Υλικό
Instant messaging	Υπηρεσία άμεσων μηνυμάτων
Public key infrastructure	Υποδομή δημόσιου κλειδιού
Host	Υπολογιστής (οικείος)
Detection and notification phase	Φάση αναγνώρισης και κοινοποίησης
Search and collection phase	Φάση αναζήτησης και συλλογής
Reconstruction phase	Φάση ανακατασκευής
Preservation phase	Φάση διατήρησης
Confirmation and authorization phase	Φάση εξακρίβωσης και εξουσιοδότησης
Survey phase	Φάση επιθεώρησης
Presentation phase	Φάση παρουσίασης
Documentation phase	Φάση τεκμηρίωσης
Web browser	Φυλλομετρητής
Physical evidence	Φυσική απόδειξη
Physical crime scene	Φυσική σκηνή του εγκλήματος
Territorial privacy	Χωρική ιδιωτικότητα
Role based pseudonyms	Ψευδώνυμα ρόλων
Pseudonymity	Ψευδωνυμία
Digital evidence	Ψηφιακή απόδειξη
Digital forensics	Ψηφιακή δικανική ανάλυση
Computer/Digital crime	Ψηφιακό έγκλημα
Digital certificate	Ψηφιακό πιστοποιητικό
Digital crime scene	Ψηφιακή σκηνή του εγκλήματος
Digital signature	Ψηφιακή υπογραφή
Payload	Ωφέλιμο φορτίο
Editor	Επιμελητής
Recommendations	Υποδείξεις

Το ψηφιακό έγκλημα και η ανάσχεσή του.
Οι προκλήσεις που εισάγει στο πεδίο της έρευνας για τη διαχείριση της εμπιστοσύνης και την ασφαλή επικοινωνία στον ψηφιακό κόσμο.

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

ACK	Acknowledgment
ACL	Access Control List
ACPO	Association of Chief Police Officers
ADS	Alternate Data Streams
ADS	Architecture Engineering for Dependable Distributed Systems
AKA	Authentication and Key Agreement
API	Application Programming Interface
APNIC	Asia Pacific Network Information Center
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Acknowledge Sequence Number
BB	Bulletin Boards
BD_ADDR	Bluetooth Device Address
BIOS	Basic Input Output System
BSD	Berkeley Software Distribution
CAC	Common Access Card
CCTV	Closed Circuit Television
CISSP	Certified Information Systems Security Professional
CDR	Call Data Record
CD-ROM	Compact Disk Read Only Memory
CFIT	Computer Forensic Investigative Toolkit
CGI	Common Gateway Interface
CN	Core Network
CNF	Computer Network Forensics
CPU	Central Processing Unit
CS	Circuit Switched
DDOS	Distributed Denial of Service
DFRWS	Digital Forensic Research Workshop
DLL	Dynamic Link Library

DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DSL	Domain Specific Language
DSTO	Defence Science and Technology Organization
EEDI	End-to-End Digital Investigation
EPAL	Enterprise Privacy Authorization Language
ERT	Emergency Remote Team
ETSI	European Technical Standardization Institute
FHS	Frequency Hop Synchronization
FMECA	Failure Mode Effects Criticality Analysis
FTA	Fault Tree Analysis
FTK	Forensic Toolkit
FTP	File Transfer Protocol
GBRAM	Global Based Requirements Analysis Method
GMLC	Gateway Mobile Location Centre
GPL	General Public License
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HAZOP	Hazard and Operability Study
HSS	Home Subscriber Server
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IM	Instant Messaging

IMEI	International Mobile Equipment Number
IMSI	International Mobile Subscriber Identity
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPO	Input Process Output
IRC	Internet Relay Chat
IRItaly	Incident Response Italy
IS	Information System
ISN	Initial Sequence Number
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LAP	Lower Address Part
LBS	Location Based Service
LCS	Location Services
LMP	Link Manager Protocol
LSB	Least Significant Bit
LSM	Linux Security Modules
MAC	Media Access Control
MANET	Mobile ad hoc Networks
MCC	Mobile Country Code
MMORPG	Massively Multiplayer Online Role Playing Games
MNC	Mobile Network Code
MSB	Most Significant Bit
MSDE	Microsoft SQL Server Desktop Engine
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Station International Number
MSN	Microsoft Network
MTA	Message Transfer Agents
NAP	Non-significant Address Part
NAT	Network Address Translation

NFR	Non Functional Requirement Framework
NIC	Network Information Center
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NSLR	National Software Reference Library
NTFS	New Technology File System
NTP	Network Time Protocol
OME	Organization Model Environment
OS	Operating System
OSI	Open Systems Interconnection
OSN	Online Social Network
OTS	Off the shelf
PDA	Personal Data Assistant
PDP	Policy Decision Point
PDS	Personal Data Server
PEP	Policy Enforcement Point
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PS	Packet Switched
P2P	Peer to Peer
PPI	Pay per Install
PRIS	Privacy safeguard
P-TMSI	Packet TMSI
RAM	Random Access Memory
RAT	Remote Access Trojan
RBAC	Role Based Access Control
RDS	Reference Data Set
RF	Radio Frequency
RFC	Remote Function Call
RIPE NCC	Reseaux IP Europeens Network Coordination Centre
RNTI	Radio Network Temporary Identity
RPC	Remote Procedure Call

SAINT	Security Administrator's Integrated Network Tool
SARA	Security Auditor's Research Assistant
SATAN	Security Administrator's Tool for Analyzing Networks
SCP	Secure Copy
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SN	Sequence Number
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SQL	Structured Query Language
STM	Scanning Tunneling Microscopy
STRAP	Structured Analysis for Privacy
SWGDE	Scientific Working Group for Digital Evidence
SysSec	Systems Security
TCP	Transmission Control Protocol
TCT	The Coroner's Toolkit
TFN	Tribe Flood Network
TFTP	Trivial File Transfer Part
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TPM	Trusted Platform Module
TTL	Time to Live
TTP	Trusted Third Party
UAP	Upper Address Part
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UK	United Kingdom
UML	Unified Modeling Language

UMTS	Universal Mobile Telecommunication System
US	United States
USB	Universal Serial Bus
USDOJ	United States Department of Justice
UTF	UCS Transformation Format
UTRAN	UMTS Terrestrial Radio Access Network
VANET	Vehicular ad hoc Networks
VLR	Visitor Location Register
VOIP	Voice over the Internet Protocol
VPN	Virtual Private Network
WS	Web Service
WSN	Wireless Sensor Networks
WSPL	Web Service Policy Language
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
ZISC	Zurich Information Security Center
3GPP	3rd Generation Partnership Project
ΑΔΑΕ	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
ΕΑ	Εκλογική Αρχή
ΙΤΥ	Ινστιτούτο Τεχνολογίας Υπολογιστών
ΤΕΕ	Τεχνικό Επιμελητήριο Ελλάδος

ΑΝΑΦΟΡΕΣ

[1] Eoghan Casey, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Third Edition, 2011, pp.3-9
[2] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, pp. 23-24
[3] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, pp. 2-3
[4] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch.1
[5] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch.2
[6] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 14
[7] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 3
[8] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 17
[9] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch. 3
[10] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 17, pp 409-412
[11] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch. 5
[12] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch. 6
[13] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch. 10
[14] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital Crime and Forensic Science in Cyberspace*, IDEA Group, 2006, ch. 14
[15] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 6
[16] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 15
[17] Eoghan Casey, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Third Edition, 2011, ch. 23.3
[18] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 18
[19] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, 2010, ch. 22
[20] ERCIM News 90, July 2012, pp 13-14
[21] ERCIM News 90, July 2012, pp 15-16
[22] ERCIM News 90, July 2012, pp 18
[23] ERCIM News 90, July 2012, pp 19-20
[24] ERCIM News 90, July 2012, pp 28-29
[25] ERCIM News 90, July 2012, pp 31-32
[26] ERCIM News 90, July 2012, pp 34
[27] ERCIM News 90, July 2012, pp 39-40
[28] ERCIM News 63, October 2005, pp 14-15
[29] ERCIM News 63, October 2005, pp 17-18
[30] ERCIM News 63, October 2005, pp 18-19
[31] ERCIM News 63, October 2005, pp 23-24
[32] ERCIM News 63, October 2005, pp 25-26
[33] ERCIM News 63, October 2005, pp 29-30
[34] ERCIM News 63, October 2005, pp 42-43