ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ: ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ.

ΜΕΛΕΤΗ ΕΠΙΣΦΑΛΩΝ ΣΗΜΕΙΩΝ ΚΑΙ ΒΕΛΤΙΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ INTERNET HOSTS

Ζάχος Αντώνιος-Λάζου Ολυμπία

Περιεχόμενα

Πρόλογος ……...

Κ Ε Φ Α Λ Α Ι Ο 1

ΑΣΦΑΛΕΙΑ ΣΤΟΥΣ ΗΛΕΚΤΡΟΝΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

1.1 ΕΙΣΑΓΩΓΗ……..
1.2 ΕΞΕΛΙΞΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ…….....
1.3 ΕΝΝΟΙΑ ΑΣΦΑΛΕΙΑΣ…….....
1.4 ΤΑ ΤΡΩΤΑ ΣΗΜΕΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ…….....
1.5 ΓΙΑΤΙ ΤΟΣΟ ΕΝΔΙΑΦΕΡΟΝ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ…….....
1.6 ΓΙΑΤΙ ΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΤΡΩΤΟ……...
1.6.1 ΤΥΠΟΙ ΤΡΩΤΩΝ……
1.6.2 ΕΛΑΤΤΩΜΑΤΑ ΣΤΟ ΛΟΓΙΣΜΙΚΟ Η ΣΤΟ ΣΧΕΔΙΑΣΜΟ ΠΡΩΤΟΚΟΛΛΩΝ……...
1.6.3 ΑΔΥΝΑΜΙΕΣ ΣΤΗΝ ΥΛΟΠΟΙΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ Η ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ…….....
1.6.4 ΑΔΥΝΑΜΙΕΣ ΣΤΗ ΔΙΑΜΟΡΦΩΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ……..

1.7 ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ……
1.7.1 ONLINE SCANNERS……...
1.7.2 ΠΡΟΓΡΑΜΜΑΤΑ ANTIVIRUS……..
1.7.3 ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΠΡΟΓΡΑΜΜΑΤΑ……..
1.7.4 ΠΡΟΓΡΑΜΜΑΤΑ ΚΑΤΑΠΟΛΕΜΗΣΗΣ Spyware……

1.8 DIALERS.……
1.9 SPAM……...
1.9.1 ΔΙΑΦΗΜΙΣΗ……
1.9.2 ΔΙΑΔΟΣΗ Malware……
1.9.3 ΕΞΑΚΡΙΒΩΣΗ Email……..
1.9.4 ΑΠΑΤΗ – Phishing…….
1.9.5 ΦΑΡΣΑ – Hoax…….
1.9.6 Flooding……
1.9.7 ΠΩΣ ΝΑ ΑΠΟΦΕΥΓΕΤΕ ΤΑ SPAM……
1.9.8 ΠΡΟΣΤΑΤΕΥΕΣΤΕ ΤΑ E-MAIL ΤΩΝ ΦΙΛΩΝ ΣΑΣ……
1.9.9 ΕΛΛΗΝΕΣ Spammers…….

1.10 ΠΡΟΤΕΙΝΟΜΕΝΗ ΜΕΘΟΔΟΛΟΓΙΑ ΒΕΛΤΙΩΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ……

1.10.1 ΑΠΟΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ……
1.10.2 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ ΠΟΡΩΝ……..
1.10.3 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ……...
1.10.4 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ……..
1.10.5 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ……..
1.10.6 ΠΟΙΟΙ ΘΑ ΕΜΠΛΑΚΟΥΝ ΣΤΟ ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΗΣ ΠΟΛΙΤΙΚΗΣ….
1.10.7 ΤΑ ΣΥΣΤΑΤΙΚΑ ΤΗΣ ΚΑΛΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ……..
1.10.8 ΚΑΝΟΝΕΣ ΑΣΦΑΛΕΙΑΣ……..

1.11 Internetworking Protocols – ΣΥΓΧΡΟΝΗ ΚΡΥΠΤΟΓΡΑΦΙΑ……...

1.11.1 ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΗΣ……
1.11.2 Software Engineering ΚΑΙ ΙΚΑΝΟΤΗΤΑ ΕΠΙΒΙΩΣΗΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ…….
1.11.3 ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΙΣΤΟΣΕΛΙΔΩΝ ΚΑΙ ΓΛΩΣΣΕΣ ΚΕΙΜΕΝΟΥ (scripting languages)……..
1.11.4 ΝΟΗΜΟΝΕΣ ΑΥΤΟΜΑΤΟΙ ΜΕΣΑΖΟΝΤΕΣ ……

Κ Ε Φ Α Λ Α Ι Ο 2

<u>ΜΟΝΤΕΛΑ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ:</u>

1. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ
2.ΕΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

2.1 ΕΙΣΑΓΩΓΗ……

2.1.1 ΕΞΑΚΡΙΒΩΣΗ ΤΑΥΤΟΤΗΤΑΣ…….
2.1.2 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ……...

2.2 ΤΑΥΤΟΠΟΙΗΣΗ ΜΕ ΚΩΔΙΚΟΥΣ ΠΡΟΣΒΑΣΗΣ…….

2.2.1 ΑΠΕΙΛΕΣ……...
2.2.2 ΤΑΥΤΟΠΟΙΗΣΗ ΜΕ ΒΙΟΜΕΤΡΙΚΕΣ ΜΕΘΟΔΟΥΣ .....
2.2.3 ΔΙΑΧΕΙΡΙΣΗ ΜΗΧΑΝΙΣΜΟΥ ΣΥΝΘΗΜΑΤΙΚΩΝ……
2.2.4 ΕΠΙΛΟΓΟΣ…….
2.2.5 ΠΑΡΑΡΤΗΜΑ……

ΕΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ

2.3 ΕΙΣΑΓΩΓΗ……

2.3.1 ΕΝΝΟΙΕΣ……
2.3.2 ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ……

2.4 ΜΟΝΤΕΛΑ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ…….
2.5 ΜΗΧΑΝΙΣΜΟΙ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ……
2.6 ΕΠΙΛΟΓΟΣ……..
2.7 ΠΑΡΑΡΤΗΜΑ…….

Κ Ε Φ Α Λ Α Ι Ο 3

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

3.1 ΕΙΣΑΓΩΓΗ…….

3.1.1 ΠΟΤΕ ΕΝΑ ΛΟΓΙΣΜΙΚΟ ΛΕΓΕΤΑΙ ΚΑΚΟΒΟΥΛΟ……

3.2 ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ……..

3.2.1 ΤΥΠΟΙ ΙΩΝ…….
3.2.2 ΜΑΚΡΟ-ΙΟΙ…….
3.2.3 ΠΡΟΣΤΑΣΙΑ……

3.3 ΜΗ ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ……..

3.3.1 ΚΕΡΚΟΠΟΡΤΕΣ……
3.3.2 ΛΟΓΙΚΗ ΒΟΜΒΑ…….
3.3.3. ΔΟΥΡΕΙΟΣ ΙΠΠΟΣ……..
3.3.4 WORMS……
3.3.5 ΒΑΚΤΗΡΙΑ……
3.3.6 ΑΛΛΕΣ ΣΗΜΑΝΤΙΚΕΣ ΑΠΕΙΛΕΣ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ……..

3.4 ΧΑΚΕΡ ……..…….

3.4.1 ΕΤΥΜΟΛΟΓΙΑ ΚΑΙ ΟΡΙΣΜΟΣ …….
3.4.2 ΗΛΕΚΤΡΟΝΙΚΗ ΚΟΥΛΤΟΥΡΑ- Underground groups
- "ΥΠΟΓΕΙΕΣ ΟΜΑΔΕΣ"……..
3.4.3 Defcon- ΠΑΓΚΟΣΜΙΟ ΣΥΝΕΔΡΙΟ ΧΑΚΕΡ …….
3.4.4 ΣΥΝΕΙΣΦΟΡΑ ΤΩΝ ΧΑΚΕΡ ΣΤΗΝ ΠΑΓΚΟΣΜΙΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΑΣΦΑΛΕΙΑ…….

3.4.5 Η ΠΡΟΣΩΠΙΚΟΤΗΤΑ ΤΟΥ ΧΑΚΕΡ……..

3.5 ΣΟΒΑΡΑ ΠΕΡΙΣΤΑΤΙΚΑ …….

3.5.1 ΤΟ «ΣΚΟΥΛΗΚΙ» ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ (Internet Worm)…..…..…..…
3.5.2 ΟΙ ΟΛΛΑΝΔΟΙ *hackers* (Dutch Hackers)……
3.5.3 ΟΙ ΔΑΝΟΙ *hackers*.……...
3.5.4 ΕΠΙΘΕΣΗ ΜΕΣΩ ΤΟΥ IRC……
3.5.5 ΠΟΛΕΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ……
3.5.6 ΚΛΟΠΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ…….
3.5.7 ΑΠΟ ΤΙΣ ΦΙΛΙΠΠΙΝΕΣ ΜΕ ΑΓΑΠΗ…….
3.5.8 ΕΠΙΘΕΣΗ ΣΤΗΝ MICROSOFT …….

3.6 ΙΟΙ ΣΥΝΕΧΕΙΑ ……

3.6.1 ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ MICROSOFT……
3.6.2 ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ GOOGLE……..
3.6.3 ΑΝΑΛΥΣΗ ΖΗΜΙΑΣ…….
3.6.4 ΕΠΙΛΟΓΟΣ……..
3.6.5 ΠΑΡΑΡΤΗΜΑ…….

ΒΙΒΛΙΟΓΡΑΦΙΑ …….

Πρόλογος

Στην πτυχιακή εργασία μας έχουμε ως στόχο να προσδιορίσουμε τους όρους, να κατανοήσουμε στις σχέσεις μεταξύ των διαφορών τους που συσχετίζονται με την περιοχή της ασφάλειας του η/υ και να θεμελιώσουμε απόψεις για το πώς θα πρέπει να χρησιμοποιούνται οι όροι αυτοί. Στην αρχή της εργασίας θα έχουμε μια ιστορική αναδρομή που θα αναφέρει την εξέλιξη τόσο του η/υ – διαδίκτυο όσο και της ασφάλειας. Επίσης θα ερμηνευτούν και κάποιες βασικές έννοιες για τη καλύτερη και γρηγορότερη κατανόηση τους Στην ουσία θα ανοίξουμε το μεγάλο κεφάλαιο της ασφάλειας του η/υ . Θα αναλύσουμε και θα «σταθούμε» στις βασικές απειλές της τις οποίες θα τις αναπτύξουμε ξεχωριστά σε κάθε κεφάλαιο. Πιο αναλυτικά, η έννοια της ασφάλειας έχει πολλές ερμηνείες γι διαφέρον και σπουδαιότητα. Οι βασικές απαιτήσεις της είναι η εμπιστευτικότητα, η εγκυρότητα,και η διαθεσιμότητα. Οι απαιτήσεις αυτές απειλούνται από εξωτερικές και εσωτερικές αδυναμίες, τεχνικές ή ανθρώπινες, τυχαίες ή εσκεμμένες. Θα αναπτύξουμε διάφορες επιθέσεις όπως π.χ. ιοί, επίθεση σε ιστοσελίδα, κ.α. και θα δούμε τις συνέπειες τους. Θα δώσουμε συμβουλές για την ασφαλέστερη λειτουργία του η/υ, θα ελέγξουμε κάποια εργαλεία απομάκρυνσης και antivirus και φυσικά που απευθυνόμαστε σε περίπτωση απειλής. Στη συνέχεια θα αναπτύξουμε την μεγαλύτερη απειλή το κακόβουλο λογισμικό, την ερμηνεία του, τα είδη του, το ρυθμό εξάπλωσης του και τα μέτρα αντιμετώπισης του. Κάποια φυσικά τείχη της ασφάλειας είναι τα μοντέλα εξουσιοδότησης, δηλαδή ο έλεγχος πρόσβασης και ο έλεγχος προσπέλασης, κ.α.. Ο έλεγχος πρόσβασης στην ουσία είναι η ταυτοποίηση και η αυθεντικοποιήση του χρήστη απέναντι στο λειτουργικό σύστημα και στην εξάλειψη των απειλών. Βέβαια, με τους ρυθμού ανάπτυξης οι μέθοδοι πρόσβασης έχουν αλλάξει, έχουν γίνει βιομετρικοί, γι'αυτό στο τέλος του κεφαλαίου θα υπάρξει μια σύγκριση ανάμεσα στο παραδοσιακό τρόπο κωδικό/pin και στις βιομετρικές μεθόδους καθώς και το συμπέρασμα. Μετά τον έλεγχο πρόσβασης έχουμε τον έλεγχο προσπέλασης τη δυνατότητα δηλαδή χρήσης και το περιορισμό της δυνατότητας προσπέλασης στις πληροφορίες παρά μόνο από εξουσιοδοτημένους χρήστες. Τέλος, θα «δώσουμε» κάποια κολπάκια για τη δημιουργία ενός ασφαλούς η/υ και θα καταλήξουμε σε συμπέρασμα.

ΚΕΦΑΛΑΙΟ 1 :

ΑΣΦΑΛΕΙΑ ΣΤΟΥΣ ΗΛΕΚΤΡΟΝΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

1.1 ΕΙΣΑΓΩΓΗ

«Γενικά αυτος που
καταλαμβάνει το πεδίο της μάχης,
Έχει το πλεονέκτημα» Sun Tzu

Ένας τυπικός και ενδεικτικός ορισμός όχι όμως πλήρης και εκτεταμένος - του όρου «Ασφάλεια Υπολογιστών και Δικτύων» είναι: η αποτροπή επιθέσεων με σκοπό την αποφυγή μη εξουσιοδοτημένης εκμετάλλευσης υπολογιστικών και δικτυακών πόρων και δεδομένων.

Το πρώτο δίκτυο, το ARPANET είχε αρχικά σχεδιαστεί με σκοπό την ευελιξία. Με την πάροδο του χρόνου και όσο προσθέτονταν κόμβοι, άρχισαν τα πρώτα βήματα του hacking. Αρχικά οι ερευνητές που χρησιμοποιούσαν το δίκτυο αντάλλασσαν αστεία και ενοχλητικά μμηνύματα. Ήταν σπάνιο εκείνο τον καιρό μία προσπάθεια απομακρυσμένης σύνδεσης σε ένα άλλο κόμβο να θεωρηθεί επίθεση, κύρια λόγω του ότι οι χρήστες του δικτύου, ήταν μία μικρή ομάδα ανθρώπων που γνώριζαν προσωπικά ο ένα τον άλλο. Τα πρώτα πραγματικά προβλήματα ασφάλειας εμφανίστηκαν γύρω στο 1980 κύρια λόγω της χρησιμοποίησης των υπολογιστών για διαχείριση απόρρητων δεδομένων και συγκεκριμένα δεδομένων που σχετίζονταν με την περιοχή των στρατιωτικών πληροφοριών. Η αποκορύφωση ήρθε το 1986, που εξαιτίας ενός λογιστικού λάθους που παρατήρησε ο Cliff Stoll, σε ένα τηλεφωνικό λογαριασμό που σύνδεε τους υπολογιστές στο ARPANET, του Lawrence Berkeley National Laboratory στην Βόρεια Καλιφόρνια, ανακάλυψε πως γινόταν μία διεθνής προσπάθεια μέσω του δικτύου να κλαπούν πληροφορίες από στρατιωτικούς κόμβους στην Αμερική.

Η διαμοιραζόμενη χρήση υπολογιστικών και δικτυακών πόρων και πληροφοριών αυξάνεται με εκθετικούς ρυθμούς και στα 1980 είναι αναγκαία η χρήση λειτουργικών συστημάτων που να αποτρέπουν τους χρήστες από ανεπιθύμητη - σκόπιμη ή μη - αλληλεπίδραση καθώς και θωράκιση των δικτύων απέναντι στην ανασφαλή τους φύση. Παράλληλα με τη δυνατότητα απόκρυψης της πληροφορίας (που απαιτείται σε περιπτώσεις μετάδοσης διαβαθμισμένης πληροφορίας), επιβάλλεται και η διατήρηση της ορθότητάς της κατά τη μμεταφορά και την ανάκτησή της (που είναι απαίτηση των επιχειρήσεων και των οργανισμών). Οι υπολογιστές αποτελούν ταυτόχρονα μέσα και στόχους επιθέσεων και η ασφάλεια τους δεν αντιμετωπίζεται ως αυτοσκοπός αλλά σαν το βασικό στοιχείο της διασφάλισης πληροφοριών.

Προκειμένου να διασαφηνιστεί ο όρος ασφάλεια είναι αναγκαίο να οριστούν α) ποιοι πόροι πρέπει να «προστατεύονται» και β) απέναντι σε ποιες «απειλές».

Ως πόροι που πρέπει να προστατεύονται θεωρούνται διεργασίες καθώς και αρχεία ή δεδηγμένα που αποθηκεύονται ή μμεταφέρονται σε υπολογιστές ή δίκτυα υπολογιστών.

Ως απειλές για την ασφάλεια πληροφοριών θεωρούνται διάφορες μορφές αναπαραγμένου κώδικα, όπως ιοί (virus) και σκουλήκια (worms), εκτελέσιμα αρχεία εντολών (shell scripts) που μπορούν να χρησιμοποιήσουν ατέλειες του λογισμικού (bugs) προκειμένου να αλλοιώσουν τα δικαιώματα προσπέλασης διεργασιών, κενά στην διαμόρφωση λογισμικού και των λειτουργικών συστημάτων.

Στα πλαίσια μιας γενικότερης θεώρησης, ασφάλεια θεωρείται η επιτυχής εξουδετέρωση απειλών όπως κλοπή, απάτη, κατασκοπεία, εκβιασμός, τρομοκρατία.

Με βάση το κίνητρο της επίθεσης, που μπορεί να είναι απλή επιθυμία απόκτησης πρόσβασης σε απαγορευμένους πόρους μέχρι την ανορθόδοξη επίτευξη πολιτικών και οικονομικών στόχων, διακρίνονται οι ακόλουθες κατηγορίες εισβολέων:

- Hackers: επεμβαίνουν παράνομα σε υπολογιστές επειδή απλά αντιμετωπίζουν τη διαδικασία της προσβολής της ασφάλειας υπολογιστών και δικτύων σαν πρόκληση για τις προγραμματιστικές του ικανότητες.

- Κατάσκοποι (Spies): επιδιώκουν την παράνομη απόκτηση πληροφοριών με απώτερο στόχο το πολιτικό όφελος.

- Τρομοκράτες (Terrorists): σκοπεύουν να διασπείρουν φόβο σχετικά με πολιτικά ζητήματα χρησιμοποιώντας πληροφορίες που έχουν αποκτήσει με παράνομο τρόπο.

- Βιομηχανικοί κατάσκοποι (Corporate Raiders): επιδιώκουν την απόκτηση πρόσβασης σε πληροφορίες και συστήματα ανταγωνιστικών εταιριών και επιχειρήσεων με σκοπό το οικονομικό όφελος εις βάρος τους.

- Επαγγελματίες εγκληματίες (Professional Criminals): στοχεύουν στην ικανοποίηση προσωπικών οικονομικών οφελών μέσω παράνομης απόκτησης πληροφοριών ή παραποίησής του.

- Βάνδαλοι (Vandals): έχουν ως μόνο στόχο την πρόκληση ζημιάς με οποιοδήποτε τρόπο και χωρίς κάποιο συγκεκριμένο προσωπικό όφελος.

Ανεξάρτητα από την κατηγοριοποίηση των επιτιθεμένων σε ένα σύστημα, κύριο πρόβλημα που πρέπει να αντιμετωπιστεί είναι ο έγκαιρος προσδιορισμός των τρωτών και η βελτίωση της ασφάλειας των συστημάτων πριν από τους επιτιθέμενους.

1.2 Η ΕΞΕΛΙΞΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

«Πάντα να εξετάζεις το
περιβάλλον σου» - Miyamoto Musashi

Πολλή συζήτηση έχει γίνει και πολλά άρθρα έχουν γραφεί για την εξέλιξη του διαδικτύου και την κατηγοριοποίησή του ανάλογα με τα δικαιώματα προσπέλασης, σε Internet, Intranet και Extranet. Από την απόλυτη ελευθερία της διακίνησης της πληροφορίας στις λεωφόρους του Internet, μέχρι τις κλειστές στους εξωτερικούς χρήστες, ομάδες των Intranets και την ελεγχόμενη πρόσβαση χρηστών στα extranets, ο σκοπός είναι ο ίδιος: η μεταφορά πληροφορίας με έναν ομοιόμορφο τεχνολογικά τρόπο για την προσέγγιση ανθρώπων και αγορών. Η διαφορά έγκειται στον ορισμό της περιμέτρου. Στο ποιοι θα είναι μέσα και ποιοι θα μείνουν απ' έξω.

Όσο όμως η τεχνολογία αυξάνει τα πλεονεκτήματα που προσφέρονται σε χρήστες από την συμμετοχή τους στην κοινωνία της πληροφορίας, μειώνοντας ταυτόχρονα το κόστος, τόσο αυξάνει και ο κίνδυνος στον οποίο εκτίθενται. Οι «έξω» πάντα θα προσπαθούν να μπουν «μέσα».

1.3 ΕΝΝΟΙΑ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια ενός συστήματος είναι ένα θέμα που αργά η γρήγορα θα απασχολήσει όλους τους χρήστες των Η/Υ, του Ίντερνετ αλλά και οποιουδήποτε μέσου ανταλλαγής πληροφοριών, όπως τα κινητά τηλέφωνα. Πολλοί αποφεύγουν να ασχοληθούν έστω και λίγο με το θέμα πιστεύοντας είτε ότι δεν είναι σημαντικό, είτε ότι η μελέτη του απαιτεί ειδικές, τεχνικές γνώσεις πληροφορικής. Γενικά ο μέσος χρήστης του ίντερνετ δεν είναι ευαισθητοποιημένος σχετικά με αυτό το θέμα και/ή τρέφει ένα φόβο προς την τεχνολογία.

Το πρόβλημα της ασφάλειας όμως είναι πάρα πολύ σπουδαίο και η ανάγκη για προστασία μεγάλη. Συνήθως συνειδητοποιούμε το μέγεθος της σπουδαιότητας όταν καταστραφούν ή κλαπούν τα δεδομένα μας από βλαβερά προγράμματα ή μη εξουσιοδοτημένους εισβολείς του συστήματός μας. Όταν η επίδοση του Η/Υ μειωθεί κατακόρυφα και η σύνδεση στο ίντερνετ γίνει πολύ αργή (με dial up modem φαίνεται αυτό). Η καταστροφή των δεδομένων ήταν η κλασσική απειλή των παλιότερων ιών. Αν και ακόμη και σήμερα υπάρχουν καταστροφικοί ιοί, ο στόχος των μοντέρνων ιών είναι τα προσωπικά δεδομένα και οι ευαίσθητες πληροφορίες που είναι αποθηκευμένες στον Η/Υ. Οι συνέπειες των σύγχρονων κακόβουλων προγραμμάτων δεν είναι τόσο "φανερές", είναι όμως πολύ πιο επικίνδυνες.

Καθοριστικό ρόλο παίζει η γνώση του εργαλείου που έχουμε μπροστά μας. Οι περισσότεροι χρήστες που πέφτουν θύματα ηλεκτρονικής απάτης δε γνωρίζουν τα πιο βασικά πράγματα του Η/Υ, του περιηγητή και κατά συνέπεια του διαδικτύου. Είναι πολύ εύκολο για τον καθένα να αγοράσει έναν υπολογιστή και να μπει στο ίντερνετ, πόσοι όμως γνωρίζουν πραγματικά έστω και ένα μέρος του δυναμικού του Η/Υ και του Ίντερνετ;

Τελικά όμως, πέρα από τις τεχνικές γνώσεις είναι ο τεχνολογικός τρόπος σκέψης. Από τι στιγμή που καταλάβει ο χρήστης ότι όλα τα συστήματα και προγράμματα διέπονται από τις ίδιες αρχές λειτουργίας, θα μπορέσει να προσεγγίσει την ασφάλεια άφοβα και με μεγάλη ευκολία.

<u>Πρακτικές Συμβουλές:</u>

- Καχυποψία

Η πρόληψη είναι η καλύτερη προστασία και επιτυγχάνεται με έναν πάρα πολύ απλό τρόπο: Την καχυποψία! Αρκεί ο χρήστης να μάθει να μην εμπιστεύεται ότι βλέπει στην οθόνη του και να μην κάνει κλικ σε οτιδήποτε του τραβάει την προσοχή, πριν αξιολογήσει τη σοβαρότητά του.

Στην αρχή είναι δύσκολο να ξεχωρίσει κανείς τις σοβαρές από τις πιθανον επικίνδυνες ιστοσελίδες. Γενικά, οι ιστοσελίδες με παράνομο υλικό, σε οποιαδήποτε μορφή, είναι πιθανόν να περιέχουν ιούς. Επίσης, σελίδες που μιμούνται γνωστές εταιρίες επίσης μπορεί να κρύβουν κινδύνους. Τέτοιες σελίδες διαφημίζονται συχνά σε email (spam).

- Opera

Αποφεύγετε τον internet explorer και χρησιμοποιείτε ένα άλλο περιηγητή όπως η Opera.

- Έλεγχος με antivirus

Ένας χρυσός κανόνας είναι ο έλεγχος του κάθε αρχείου που κατεβαίνει από το ίντερνετ στον Η/Υ με το antivirus πριν εκτελεστεί!

- Email

Με τα email πρέπει να είναι κανείς προσεκτικός και ποτέ να μην ανοίγονται συννημένα από αμφιβόλου προελεύσεως διευθύνσεις. Και εδώ ισχύει ο χρυσός κανόνας του ελέγχου με antivirus πριν την εκτέλεση. Ένα πιο ασφαλές πρόγραμμα email είναι το thunderbird.

- Προγράμματα Προστασίας

Ένα καλό Antivirus, ένα Firewall και ένα Antispyware δεν πρέπει να λείπουν από κανένα υπολογιστή.

- Updates - Ενημερώσεις

Όσο πιο νέα και ενημερωμένα είναι τα λογισμικά που χρησιμοποιείτε τόσο πιο ασφαλή είναι. Πολύ σημαντική είναι η τακτική ενημέρωση του λειτουργικού (windows) και των προγραμμάτων προστασίας (antivirus, antispyware).

- Τακτικός Έλεγχος

Τουλάχιστον μια φορά το μήνα συνιστάται να γίνεται έλεγχος του σκληρού δίσκου για ιούς και κατασκοπευτικά προγράμματα (αυτό αφορά αρχάριους χρήστες και όχι διαχειριστές συστημάτων που τα παρακολουθούν συχνά και γνωρίζουν ακριβώς τι περιέχουν).

Τελικά, η Διαδικτυακή Ασφάλεια πρέπει να κατανοηθεί ως έννοια. Όσα μέτρα προστασίας και να λάβουμε, απόλυτη ασφάλεια δεν μπορεί να εγγυηθεί κανένα πρόγραμμα όσο ο Η/Υ μας στέλνει και λαμβάνει πληροφορίες με οποιοδήποτε τρόπο. Ο μεγαλύτερος κίνδυνος είναι η κακή χρήση του υπολογιστή από το χρήστη και ο καλύτερος τρόπος προστασίας του συστήματός μας είναι η περιήγηση στο ίντερνετ μέσα σε λογικά πλαίσια.

1.4 ΤΑ ΤΡΩΤΑ ΣΗΜΕΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

«Πότε ένα υπολογιστικό σύστημα δεν είναι ασφαλές;
Όταν λειτουργεί!» - hacker

Ένα σύστημα είναι ασφαλές τόσο, όσο οι άνθρωποι που το χρησιμοποιούν. Κανείς δεν νοιάζεται για την ασφάλεια ενός συστήματος που λειτουργεί συνεχώς και έχει τα απαραίτητα backup για να επανέλθει στην κανονική λειτουργία του, αν συμβεί πρόβλημα στο υλικό.

Το πρόβλημα προκύπτει όταν μία λειτουργική ανάγκη (όπως η εμπιστευτικότητα) πρέπει να υλοποιηθεί. Από την στιγμή που θα αρχίσουν η υλοποιήσεις συστημάτων ασφαλείας, δεν υπάρχει ορατό τέλος στην βελτίωση της ασφάλειας. Όποιος δεν έχει προσπέλαση στο σύστημα, θα προσπαθεί να βρει τρωτό σημείο στην ασφάλεια.

Τρωτό είναι ένα αδύναμο (ασθενικό) σημείο που εκμεταλλεύεται κάποιος που θέλει να βρει ένα τρόπο να εισβάλει, χωρίς εξουσιοδότηση, σε ένα υπολογιστικό/δικτυακό σύστημα. Όταν με χρήση του τρωτού σημείου γίνει εισβολή, τότε μιλάμε για περιστατικό παραβίασης της ασφάλειας. Τα τρωτά σημεία οφείλονται σε σχεδιαστικά και κατασκευαστικά λάθη.

1.5 ΓΙΑΤΙ ΤΟΣΟ ΕΝΔΙΑΦΕΡΟΝ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ

Είναι χαρακτηριστικά εύκολο να αποκτήσει κάποιος μη εξουσιοδοτημένη προσπέλαση σε ένα περιβάλλον με χαλαρή ασφάλεια και ταυτόχρονα να μην γίνει ποτέ αντιληπτός. Ακόμα και αν χρήστες του δικτύου δεν έχουν κάτι χρήσιμο σε ένα υπολογιστή, αυτός μπορεί να γίνει η κεκρόπορτα για την εισβολή σε ένα δίκτυο.

Ακόμα και η πιο «αθώα» πληροφορία, όπως τι προγράμματα τρέχουν οι υπολογιστές, τι πρωτόκολλα χρησιμοποιούνται είναι πολύ σημαντικά στοιχεία για τους hackers. Με τη γνώση αυτή μπορούν να δοκιμάσουν γνωστά τρωτά σημεία τους και να αποκτήσουν πρόσβαση σε σημαντικές πληροφορίες.

Το διαδίκτυο είναι ένα μέσο διάδοσης πληροφοριών. Αυτό όμως ισχύει και για τους hackers που μεταδίδουν πληροφορίες για τις αδυναμίες που βρίσκουν σε λειτουργικά συστήματα, πρωτόκολλα και εφαρμογές. Στο διαδίκτυο υπάρχει ένας ανταγωνισμός ταχύτητας, ανάμεσα στο πόσο γρήγορα θα ανηδράσουν οι κατασκευαστές και οι διαχειριστές των υπολογιστικών συστημάτων για να διορθώσουν ένα νέο αδύνατο σημείο στο σύστημά τους, πριν δεχθούν εισβολή και των hackers που θέλουν να εκμεταλλευτούν το αδύνατο σημείο για να εισβάλουν στο σύστημα. Σύμφωνα με στοιχεία του CERT/CC και τα καθημερινά κρούσματα επιθέσεων, κανένας στο διαδίκτυο δεν μπορεί να θεωρηθεί ασφαλής.

Οι επιπτώσεις μίας παραβίασης στην ασφάλεια μπορεί να είναι ο χαμένος χρόνος για την ανάκτηση της λειτουργικότητας των συστημάτων, η απώλεια χρημάτων και αξιοπιστίας, η αδυναμία συνέχισης της εργασίας, τα νομικά προβλήματα και σε εξαιρετικά σπάνιες περιπτώσεις ο κίνδυνος της ίδιας της ζωής.

Συνήθως οι περιπτώσεις επίθεσης έχουν σκοπό την επίθεση κατά της αξιοπιστίας, της φήμης και της λειτουργικότητας των οργανισμών με αποτέλεσμα την άμεση ή έμμεση χρηματική επιβάρυνση.

Επιθέσεις έχουν παρουσιαστεί και σε sites του Ελληνικού χώρου κύρια σε κρατικούς οργανισμούς με σκοπό την δυσφήμησή τους. Στο παράρτημα υπάρχουν εικόνες με τις σελίδες διαφόρων κόμβων μετά από επίθεση.

1.6 ΓΙΑΤΙ ΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΤΡΩΤΟ

Πολλά από τα πρωταρχικά δικτυακά πρωτόκολλα, που τώρα αποτελούν μέρος της υποδομής του διαδικτύου, δεν σχεδιάστηκαν έχοντας κατά νου την ασφάλεια. Χωρίς μία θεμελιώδη ασφαλή υποδομή, η άμυνα του δικτύου γίνεται πιο δύσκολη. Επιπλέον, το διαδίκτυο είναι ένα δυναμικό περιβάλλον. τόσο στην τοπολογία του, όσο και στην τεχνολογία.

Ο στόχος κατά το σχεδιασμό του IP ήταν η δημιουργία ενός πρωτοκόλλου που να διασυνδέει ετερογενή δίκτυα με τέτοιο τρόπο ώστε όλοι οι υπολογιστές να είναι μοναδικά προσδιορισμένοι, να μπορούν να ανταλλάσσουν δεδομένα με μία κοινή μορφοποίηση (format) και τέλος να μεταδώσουν δεδομένα χωρίς να γνωρίζουν στοιχεία για τη δομή και τη μορφή των δικτύων που ανήκουν οι παραλήπτες. Τα διασυνδεόμενα δίκτυα αρχικά αφορούσαν πανεπιστήμια ή ερευνητικά ιδρύματα και στόχος ήταν η διαπανεπιστημιακή συνεργασία. Για αυτόν το λόγο ουδέποτε τέθηκε θέμα ασφάλειας στο σχεδιασμό του IP. Μοιραία λοιπόν οι μηχανισμοί της ασφάλειας απουσιάζουν από εκεί που θα έπρεπε να ήταν ενσωματωμένοι, στο επίπεδο του δικτύου. Όταν αργότερα με την τεράστια εξάπλωση του διαδικτύου και τη χρήση του για εμπορικούς σκοπούς εμφανίστηκε το θέμα της ασφάλειας, έπρεπε αναγκαστικά να αντιμετωπιστεί σε ένα υψηλότερο επίπεδο, όπως στο επίπεδο εφαρμογής ή σπανιότερα στο επίπεδο μεταφοράς. Για παράδειγμα το πρωτόκολλο Secure Sockets Layer (SSL) λειτουργεί στο επίπεδο μεταφοράς, ενώ το πρωτόκολλο Secure HTTP (SHTTP) λειτουργεί στο επίπεδο εφαρμογής.

Εξαιτίας του κληρονομούμενου ανοικτού περιβάλλοντος του διαδικτύου και του αρχικού σχεδιασμού των πρωτοκόλλων, οι επιθέσεις γενικά είναι γρήγορες, εύκολες, ανέξοδες και μπορεί να μην είναι δυνατόν να ανακαλυφθούν ή να ανιχνευτούν. Ο εισβολέας δεν χρειάζεται να είναι παρών στο site που επιτίθεται, αλλά αντίθετα μπορεί να βρίσκεται οπουδήποτε στον κόσμο και μάλιστα είναι δυνατό να αποκρυφτεί και το σημείο που βρίσκεται.

Μία άλλη μέθοδος ενίσχυσης της ασφάλειας που εμφανίστηκε τελευταία και χρησιμοποιείται όλο και πιο συχνά είναι αυτή της δημιουργίας ιδεατών ιδιωτικών δικτύων (VPNs) με χρήση κατάλληλου λογισμικού η υλικού. Η βασική φιλοσοφία αυτών των μεθόδων είναι η κωδικοποίηση του πακέτου που πρόκειται να μεταδοθεί και κατόπιν η ενσωμάτωσή του σε ένα νέο πακέτο που αποστέλλεται στον προορισμό. Η μετατροπή δηλαδή του αρχικού IP πακέτου σε δεδομένα ενός άλλου IP πακέτου όπου τα πεδία που αφορούν τις διευθύνσεις αποστολέα και παραλήπτη είναι διαφορετικά από ότι στο αρχικό πακέτο (tunneling).

Παρά τις επιτυχημένες προσπάθειες σε όλες αυτές τις μέθοδες εξακολουθεί να υπάρχει ένα σοβαρό πρόβλημα. Αν χρησιμοποιείται ασφάλεια στο επίπεδο εφαρμογής τότε υπάρχει αρκετή πληροφορία που περιέχεται στην επικεφαλίδα του πακέτου στο οποίο ενσωματώνεται το κωδικοποιημένο πακέτο, που είναι ευάλωτη σε επιθέσεις26. Με χρήση προγραμμάτων ανάλυσης της δικτυακής κυκλοφορίας (sniffers) είναι δυνατόν να αποκαλυφθούν οι διεργασίες και τα συστήματα που ανταλλάσσουν πληροφορίες. Επίσης το κόστος της υποστήριξης της ασφάλειας από κάθε εφαρμογή χωριστά στοιχίζει αρκετά σε σχέση με το να παρέχονταν η ασφάλεια στο επίπεδο του δικτύου και κάθε εφαρμογή να έκανε χρήση αυτής.

Αν χρησιμοποιείται ασφάλεια στο επίπεδο μεταφοράς, τότε αυτό σημαίνει ότι οι εφαρμογές που χρησιμοποιούν αυτή τη μέθοδο πρέπει να ξαναγραφτούν, ώστε τόσο ο εξυπηρετητής όσο και ο πελάτης να κάνουν χρήση αυτής της ασφάλειας. Τέλος η χρήση πρωτοκόλλων tunneling έχει μέτρια απόδοση, αλλά επιπλέον πάσχει από έλλειψη κάποιου πρότυπου που θα μπορέσει να ακολουθηθεί.

Είναι πάντως κοινό στους οργανισμούς να δείχνουν μία ατεκμηρίωτη εμπιστοσύνη στο διαδίκτυο, έχοντας άγνοια των κινδύνων που παραμονευτούν. Πιστεύουν πως το site τους δεν είναι στόχος ή πως έχουν πάρει όλα τα απαραίτητα μέσα για την προστασία τους. Όμως η τεχνολογία αλλάζει ταχύτατα και το ίδιο τα εργαλεία που καιοσκευάζουν οι εισβολείς. Έτσι τα μέτρα που λαμβάνονται δεν ισχύουν μετά την πάροδο σύντομου χρονικού διαστήματος .

Εξαιτίας του ότι το μεγαλύτερο μέρος της κυκλοφορίας στο διαδίκτυο δεν είναι κρυπτογραφημένο, δεν είναι εφικτή η εμπιστευτικότητα και ακεραιότητα των πληροφοριών. Σαν αποτέλεσμα ένα site μπορεί να δεχθεί επιθέσεις από άλλο με χρήση εργαλείων, όπως ένας packet sniffer, που μπορεί να είναι εγκατεστημένος στο ένα και να μαζεύει στοιχεία για άλλο.

Ένας άλλος παράγοντας που συνεισφέρει στην επιδείνωση του προβλήματος είναι η ραγδαία ανάπτυξη των υπηρεσιών πάνω από το διαδίκτυο. Με χρήση πολύπλοκων εφαρμογών, που δυστυχώς δεν σχεδιάζονται, εγκαθίστανται και συντηρούνται με προσοχή, μένουν τρωτά σημεία στον κώδικα των προγραμμάτων και των λειτουργικών.

Η επιλογή του λειτουργικού συστήματος που εγκαθίσταται στον εξοπλισμό πρέπει να γίνεται με κριτήριο την ενίσχυση της ασφάλειας, και όχι με κριτήριο την ταχύτητα, τις επιδόσεις, την τιμή, την ευκολία χρήσης, την διαχείριση, και την υποστήριξη.

Συνήθως η στάνταρτ διαμόρφωση του λειτουργικού, όπως έρχεται από τον κατασκευαστή δεν είναι η κατάλληλη για την διασφάλιση και ενίσχυση της ασφάλειας, δίνοντας την δυνατότητα στους γνώστες να επιχειρήσουν επίθεση αμέσως μετά την πρώτη εγκατάσταση.

Τέλος πρέπει να τονιστεί, πως με την εξέλιξη του διαδικτύου υπάρχει η ανάγκη για εξειδικευμένους τεχνικούς σε θέματα ασφάλειας που θα αναλύουν, σχεδιάζουν, εγκαθιστούν και συντηρούν την ασφάλεια ενός site.

1.6.1 ΤΥΠΟΙ ΤΡΩΤΩΝ

Η ακόλουθη ταξινόμηση είναι χρήσιμη για να καταλάβουμε τους τεχνικούς λόγους, πίσω από επιτυχείς τεχνικές παραβίασης της ασφάλειας και να βοηθήσει τους ειδικούς να προσδιορίσουν γενικές λύσεις για τον ίδιο τύπο προβλημάτων.

1.6.2 ΕΛΑΤΤΩΜΑΤΑ ΣΤΟ ΛΟΓΙΣΜΙΚΟ Η ΣΤΟ ΣΧΕΔΙΑΣΜΟ ΠΡΩΤΟΚΟΛΛΩΝ

Τα πρωτόκολλα ορίζουν του κανόνες και τις μεθόδους για να μπορούν οι υπολογιστές να επικοινωνούν μεταξύ τους στο δίκτυο. Αν το πρωτόκολλο έχει σχεδιαστικό λάθος είναι επισφαλές σε εκμετάλλευση του τρωτού σημείου ανεξάρτητα από το πόσο καλά υλοποιήθηκε. Ένα τέτοιο παράδειγμα είναι το Network File System (NFS), που επιτρέπει στα συστήματα να μοιράζουν αρχεία. Το πρωτόκολλο αυτό δεν περιλαμβάνει έναν τρόπο πιστοποίησης, έτσι ώστε ο χρήστης που συνδέεται δεν πιστοποιείται για το αν είναι αυτό που διατείνεται. Οι NFS servers είναι στόχος για την κοινότητα των εισβολέων.

Όταν σχεδιάζεται το λογισμικό χωρίς η ασφάλεια να συμπεριλαμβάνεται στις αρχικές προδιαγραφές, υπάρχει το ενδεχόμενο το επιπλέον τμήμα που προστίθεται για την ενίσχυση της ασφάλειας, να μην αλληλεπιδρά όπως είχε αρχικά σχεδιαστεί και να προκύπτουν απρόσμενα τρωτά σημεία.

1.6.3 ΑΔΥΝΑΜΙΕΣ ΣΤΗΝ ΥΛΟΠΟΙΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ Η ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ

Ακόμα και αν ένα πρωτόκολλο έχει σχεδιαστεί σωστά και προσεχτικά, μπορεί να έχει τρωτά σημεία από τον τρόπο υλοποίησής του. Για παράδειγμα, ένα πρωτόκολλο για ηλεκτρονικό ταχυδρομείο, μπορεί να υλοποιηθεί με τέτοιο τρόπο που να επιτρέπει την σύνδεση στο mail port του συστήματος που θα γίνει η επίθεση και να ζητήσει να εκτελέσει συγκεκριμένες εντολές. Έτσι ο εισβολέας μπορεί να γράψει στο πεδίο «Το:», αντί την σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου, συγκεκριμένες εντολές και να ζητήσει το password file του συστήματος, χωρίς να χρειάζεται καν λογαριασμός στο σύστημα.

Το λογισμικό μπορεί να έχει τρωτά σημεία, επειδή δεν βρέθηκαν πριν την τελική έκδοση. Οι εισβολείς ψάχνουν και βρίσκουν τα ελαττώματα αυτά με δικά τους εργαλεία. Για παράδειγμα ψάχνουν για ελαττώματα σε περιπτώσεις όπως:

1. Ανταγωνιστικές καταστάσεις στην προσπέλαση αρχείων
2. Ανυπαρξία ελέγχων για το περιεχόμενο και το μέγεθος των δεδομένων.
3. Ανυπαρξία ελέγχων γω την ανημετώπιση εσωτερικών λαθών
4. Αδυναμία προσαρμογής σε εξάντληση πόρων
5. Ελλιπή έλεγχο του λειτουργικού περιβάλλοντος
6. Ανάρμοστη χρήση κλήσεων του συστήματος
7. Χρήση τμημάτων του λογισμικού για άλλο σκοπό από αυτό που σχεδιάστηκαν.

Κάνοντας χρήση αδυναμιών στο λογισμικό οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε πόρους, χωρίς να χρειάζονται την απαραίτητη εξουσιοδότηση από το σύστημα

1.6.4 ΑΔΥΝΑΜΙΕΣ ΣΤΗ ΔΙΑΜΟΡΦΩΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Τρωτά σημεία σε αυτή την κατηγορία δεν προέρχονται από προβλήματα στα πρωτόκολλα ή το λογισμικό. Αντίθετα τα προβλήματα αυτά προέρχονται από τον τρόπο που αυτά τα δομικά στοιχεία,

εγκαθίστανται και χρησιμοποιούνται Τα προϊόντα παραδίδονται και συνήθως εγκαθίστανται με προκαθορισμένες παραμέτρους, που οι εισβολείς μπορούν να εκμεταλλευτούν. Οι διαχειριστές συστημάτων και οι χρήστες μπορεί να μην αλλάξουν ης προκαθορισμένες παραμέτρους, με αποτέλεσμα το σύστημα να εμφανίζει τρωτά.

Ένα παράδειγμα λανθασμένης διαμόρφωσης που συχνά εκμεταλλεύονται Οι εισβολείς είναι η ανώνυμη χρήση της υπηρεσίας File Transfer Protocol (FTP). Οι οδηγίες για την ασφαλή διαμόρφωση αυτής της υπηρεσίας τονίζουν την ανάγκη το password file, τα βοηθητικά προγράμματα και τα αρχεία δεδομένων να βρίσκονται σε άλλη θέση στο σύστημα από το υπόλοιπο λειτουργικό σύστημα και αυτό να μην μπορεί να προσπελαστεί από τον χώρο αποθήκευσης του FTP. Όταν τα sites δεν προσέξουν την διαμόρφωση του ftp server τότε μη εξουσιοδοτημένοι χρήστες μπορούν να βρουν πληροφορίες πιστοποίησης και να τις εφαρμόσουν για να αποκτήσουν προσπέλαση.

1.7 ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ

Όταν λέμε τείχος προστασίας σε προσωπικούς υπολογιστές, εννοούμε ένα πρόγραμμα που ελέγχει την κυκλοφορία στη διασταύρωση του Η/Υ σας και του διαδικτύου. Το τείχος προστασίας θα ελέγξει και θα σας αναφέρει ποια προγράμματα του Η/Υ θέλουν να επικοινωνήσουν με το ίντερνετ. Επίσης θα σας αναφέρει αν κάποιος / κάτι προσπαθεί να επικοινωνήσει με το κομπιούτερ σας. Βέβαια εκτός του ότι θα το αναφέρει, θα σας δώσει τη δυνατότητα να επιτρέψετε ή να απαγορεύσετε την είσοδο ή έξοδο πληροφοριών προγραμμάτων από το κομπιούτερ σας.

Το Firewall δεν προστατεύει από ιούς! Αυτό που πετυχαίνει μέσα από τον έλεγχο της κυκλοφορίας των πληροφοριών είναι κυρίως την προστασία από προγράμματα τύπου backdoor που χρησιμοποιούν οι ερασιτέχνες hackers. Οι πραγματικά ικανοί εισβολείς ενός συστήματος βρίσκουν τρόπους να ξεγελάσουν το firewall οπότε δεν πρέπει να το αντιμετωπίζουμε σαν τη λύση για όλα τα προβλήματα ασφάλειας. Υπάρχουν μάλιστα και ορισμένοι φανατικοί υποστηρικτές της άποψης ότι το firewall είναι περιττό. Πέρα από κάθε φανατισμό όμως, είναι γενικότερα αποδεκτό ότι το firewall βοηθάει σημαντικά και επίσης μας προστατεύει από διάφορα σκουλήκια που μεταδίδονται μέσω του διαδικτύου.

Το τείχος προστασίας είναι πολύ σημαντικό να υπάρχει, μπορεί βέβαια να σας προβληματίσουν λίγο μερικά μηνύματα που θα σας στέλνει ζητώντας την άδειά σας για πρόσβαση των προγραμμάτων. Όταν δεν ξέρετε το πρόγραμμα, να του αρνείστε πάντα την πρόσβαση! Αν κάτι δε λειτουργεί σωστά και έχετε απαγορεύσει την είσοδο / έξοδο ενός σημαντικού προγράμματος του συστήματος μπορείτε ανά πάσα στιγμή να αλλάξετε την εντολή. Πραγματικά δεν είναι τόσο πολύπλοκο όσο ακούγεται, απλά προσπαθώ να εξηγήσω εδώ κάπως αναλυτικά τι συμβαίνει. Κατά τη διάρκεια της λειτουργίας του firewall γίνονται αντιληπτά τα λεγόμενα port scans. Μπορούμε να φανταστούμε ότι ο Η/Υ έχει πολλές θύρες / πόρτες (ports) που χρησιμοποιούνται για την επικοινωνία με το διαδίκτυο. Υπάρχουν πολλοί λόγοι για τους οποίους μπορεί κάποιος ή κάτι να "χτυπήσει μια πόρτα" του υπολογιστή σας.

Όταν όμως λειτουργεί το firewall δεν υπάρχει λόγος ανησυχίας το οποίο αυτόματα προστατεύει και είναι σπάνιο έως απίθανο να κρύβεται πίσω από όλα τα port scans ένας hacker!

Υπάρχουν διάφορα προγράμματα (τείχη προστασίας) συνήθως συνιστάτε το SYGATE για αρχάριους χρήστες.
Το τείχος προστασίας μας επιτρέπει να μάθουμε τον Η/Υ μας καλύτερα και να δούμε πόσα και ποιά προγράμματα θέλουν να βγουν στο ίντερνετ και να επικοινωνήσουν πχ με τον κατασκευαστή τους. Λοιπόν, δε χρειάζεται να επικοινωνούν, γιατί δηλαδή το Word να θέλει να στέλνει πληροφορίες στη microsoft? Δυστυχώς υπάρχουν υποψίες ότι ακόμα και η microsoft μας κατασκοπεύει μέσω των windows. Συγκεκριμένα είναι δύο οι πιο σημαντικές εφαρμογές που το κάνουν αυτό. Υπάρχει όμως τρόπος να τις απενεργοποιήσουμε κατεβάζοντας δύο καταπληκτικά προγράμματα. Είναι πολύ μικρά σε μέγεθος και αξίζει να τα κατεβάσετε!

1.7.1 ONLINE SCANNERS

1. Disk Scanners

Τα παρακάτω online antivirus ελέγχουν όλο τον σκληρό δίσκο για ιούς. Συνήθως απαιτείται η χρήση Internet Explorer με active x για τη χρήση τους. Πριν τη χρήση τους να απενεργοποιείτε το δικό σας on access scan (guard) antivirus.

- TRENDMICRO
- F SECURE
- BITDEFENDER
- McAfee

2. File Scanners

Οι παρακάτω σελίδες προσφέρουν δωρεάν φυσικά έλεγχο απομωνομένων αρχείων. Είναι πολύ χρήσιμη αυτή η υπηρεσία για γρήγορο έλεγχο κάποιου ύποπτου αρχείου. Δεν χρειάζεται να απενεργοποιήσετε το antivirus για αυτό τον έλεγχο αφού απλά ανεβάζετε το αρχείο και ο έλεγχος γίνεται online και όχι στον υπολογιστή σας.

- KASPERSKY
- RAV ANTIVIRUS
- JOTTI MALWARE SCAN
- VIRUSTOTAL

Τακτική Ενημέρωση (Update)

Η τακτική ενημέρωση του Antivirus είναι υποχρεωτική, διαφορετικά δεν θα είμαστε προστατευμένοι από νέες απειλές που δημιουργούνται καθημερινά. Η ενημέρωση πρέπει να γίνεται τουλάχιστον μια φορά τη βδομάδα και συχνότερα αν είμαστε πολλές ώρες στον ίντερνετ. Επίσης συνιστάται να ανοίγουμε το κυρίως πρόγραμμα περιοδικά και να ελέγχουμε (scan) τον σκληρό δίσκο για ιούς τουλάχιστον μια φορά το μήνα. Καμιά φορά μπορεί να συμβεί να περάσει ένας ιός στο κομπιούτερ χωρίς να τον εντοπίσει ο φύλακας αλλά να τον βρει το κυρίως πρόγραμμα σε ένα έλεγχο.

Προσοχή: Μην εγκαθιστάτε περισσότερα από ένα Antivirus στο σύστημά σας γιατί η ταυτόχρονη λειτουργία τους μπορεί να οδηγήσει σε τρομερές αστάθειες και μεγάλα προβλήματα. Δύο Antivirus μπορούν να καταστρέψουν τον υπολογιστή σας σε τέτοιο βαθμό που μόνο ένα format μπορεί να τον επαναφέρει. Τα δεδομένα σας όμως θα έχουν χαθεί!

1.7.2 ΠΡΟΓΡΑΜΜΑΤΑ ANTIVIRUS

Στο ίντερνετ υπάρχουν διαθέσιμες δωρεάν εκδόσεις κάποιων αρκετά καλών προγραμμάτων. Βέβαια τα εμπορικά προγράμματα είναι πάντα καλύτερα ή τουλάχιστον πιο φιλικά στο χρήστη λόγω αυτόματων ενημερώσεων κτλ. Παρόλαυτά, θεωρώ ότι τα δωρεάν προγράμματα είναι υπεραρκετά για τον απλό χρήστη. Το πρόγραμμα που ξεχωρίζω και συνιστώ είναι ένα πολύ καλό γερμανικό προϊόν, το Antivir.

- Antivir

Το Antivir είναι πολύ δημοφιλές στη Γερμανία αλλά και στον υπόλοιπο κόσμο. Χρησιμοποιεί ελάχιστους από τους πόρους του υπολογιστή και είναι ιδανικό για αργούς υπολογιστές με λιγότερη μνήμη RAM. Συγκεκριμένα χρειάζεται μόνο 14 MB ελεύθερης μνήμης και 15 MB ελεύθερου χώρου στο σκληρό δίσκο. Πλέον οι ενημερώσεις του είναι πολύ μικρές σε μέγεθος και καθιστούν αυτό το πρόγραμμα ιδανικό. Επίσης αναγνωρίζει πάνω από 228.632 ιούς! Ερωτήσεις και θέματα σχετικά με το Antivir μπορείτε να συζητάτε στο νέο φόρουμ υποστήριξης Antivir Forum στην αγγλική ενότητα (και στη γερμανική φυσικά).

Σημείωση: Το Antivir διατίθεται δωρεάν μόνο για προσωπικούς υπολογιστές για ιδιωτική χρήση και όχι για υπολογιστές σε χώρους εργασίας. Η Premium έκδοση, που κοστίζει 20 Ευρώ, είναι και αυτή για προσωπικούς υπολογιστές έχει όμως κάποιες περισσότερες λειτουργίες όπως email scanning, αναγνώριση spyware κα. Εταιρίες και δημόσιοι οργανισμοί θα πρέπει να αγοράζουν την ανάλογη άδεια. Περισσότερες πληροφορίες στο http://antivir.de. Απαγορεύεται η επανεκπομπή του, σε οποιοδήποτε μέσο, μετά ή άνευ επεξεργασίας, χωρίς γραπτή άδεια του συγγραφέα.

1.7.3 ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΠΡΟΓΡΑΜΜΑΤΑ

Τα κατασκοπευτικά προγράμματα είναι μικρά προγραμματάκια που μπαίνουν στον Η/Υ χωρίς να το καταλαβαίνουμε. Πολλές φορές συμπεριλαμβάνονται μέσα σε άλλα προγράμματα που κατεβάζουμε από το ίντερνετ, όπως δωρεάν screensavers, παιχνίδια, messengers αλλά και σε δωρεάν cd που διανέμονται με περιοδικά. Η λειτουργία αυτών των εφαρμογών (προγράμματα) μοιάζει λίγο με τους δούρειους ίππους, εγκαθιστόνται χωρίς την άδεια και γνώση του χρήστη και αρχίζουν να κατασκοπεύουν τις ιντερνετικές μας συνήθειες. Ίσως πολλά από αυτά τα κατασκοπευτικά προγράμματα να μην είναι βλαβερά, γιατί δεν καταστρέφουν αρχεία όπως οι ιοί, όμως "κρυφακούγοντας" στέλνουν πληροφορίες για το λειτουργικό μας σύστημα, τί είδους ιστοσελίδες επισκεπτόμαστε, αν χρησιμοποιούμε το ίντερνετ για αγορές, πως λέγεται ο Η/Υ μας κτλ. Αυτό βέβαια στη καλύτερη περίπτωση, γιατί στη χειρότερη διαβάζουν ότι πληκτρολογούμε, σαρώνουν τα αρχεία μας για κωδικούς, αριθμούς πιστωτικών καρτών και για ηλεκτρονικές διευθύνσεις. Ακόμα, ένα είδος κατασκοπευτικών προγραμμάτων μπορεί να αλλάξει την αρχική σελίδα του Internet Explorer και να "πετάει" διαφημίσεις.

Ακόμα και τα πιο ήπιας μορφής spyware, όπως έχει καθιερωθεί να λέγονται στα αγγλικά, τα θεωρώ ιδεολογικά ανήθικα γιατί εκτός του ότι εισβάλλουν στην ιδιωτική μας ζωή, λειτουργούν συνέχεια κάνοντας το σύστημα του Η/Υ ασταθές και αργό. Και φυσικά, τις πληροφορίες που συλλέγουν τις στέλνουν αδιάκοπα στο ίντερνετ καθυστερώντας τις σελίδες μας να φορτώσουν. Ορισμένα από αυτά τα κατασκοπευτικά προγράμματα έχουν κατασκευαστεί με τέτοιο ύπουλο τρόπο ώστε να κάνουν την απεγκατάστασή τους πολύ δύσκολη έως και αδύνατη.

Προστασία Προσωπικών Δεδομένων

Εξετάζοντας το θέμα της εισβολής της ιδιωτικής μας ζωής από τη νομική του πλευρά, τα κατασκοπευτικά προγράμματα παραβιάζουν την Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα. "Ο σεβασμός και η προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας αποτελούν πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας.

Η τεράστια πρόοδος της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους έχουν σαν συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να δημιουργήσει προβλήματα στην ιδιωτική ζωή του πολίτη."

1.7.4 ΠΡΟΓΡΑΜΜΑΤΑ ΚΑΤΑΠΟΛΕΜΗΣΗΣ Spyware

Ένα από τα καλύτερα προγράμματα που εμποδίζουν την εγκατάσταση κατασκοπευτικών και παρόμοιων εμπορικών προγραμμάτων είναι το Spyware Blaster που δεν πρέπει να λείπει από κανέναν υπολογιστή! Αυτό βέβαια δε σημαίνει (και αυτό ισχύει για όλα τα προγράμματα) ότι εγκαθιστώντας το spyware blaster μπορεί ο καθένας ασύστολα να επισκέπτεται επικίνδυνες σελίδες χωρίς να πάθει τίποτα!

Ακόμα υπάρχουν δυο πολύ δημοφιλή προγράμματα που σαρώνουν τον Η/Υ, εντοπίζουν τα κατασκοπευτικά προγράμματα και τα εξοντώνουν! :) Αυτά είναι το Adaware και το Spybot Search and Destroy . Πριν σας δώσω τις σελίδες που θα τα κατεβάσετε δωρεάν, θέλω να πώ κάτι που ισχύει για όλα αυτά τα προγράμματα. Αφού τα κατεβάσετε πριν τα χρησιμοποιήσετε την πρώτη φορά πρέπει να τα ενημερώσετε (update). Μετά συνιστάτε να σκανάρετε τον Η/Υ τακτικά (μια φορά τη βδομάδα ή το μήνα ανάλογα με το πόσο είστε στο ίντερνετ). Το πιο σημαντικό πράγμα είναι να τα ενημερώνετε (update) επίσης τακτικά, γιατί διαφορετικά δεν θα μπορούν να σας προστατεύσουν από καινούργιες απειλές.

Προσοχή!: Στο αχανές διαδίκτυο προσφέρονται δωρεάν προγράμματα που υποστηρίζουν ότι καταπολεμούν τα spyware ενώ στην πραγματικότητα περιέχουν και διαδίδουν κακόβουλα προγράμματα! Για αυτό το λόγο να εμπιστεύεστε μόνο γνωστές και δοκιμασμένες ιστοσελίδες που προσφέρουν δωρεάν τέτοια προγράμματα.

1.8 DIALERS

Οι Dialers είναι προγράμματα που χρησιμοποιούνται από διάφορες ιστοσελίδες ως τρόπος πληρωμής για το περιεχόμενο που προσφέρουν. Για να λειτουργήσουν πρέπει ο χρήστης συνειδητά να συμφωνήσει στο κατέβασμα του Dialer πληκτρολογώντας συνήθως τη λέξη "OK". Ο dialer μετά χρησιμοποιεί την τηλεφωνική γραμμή για να πάρει τηλέφωνο έναν αριθμό που δημιουργεί υψηλότερα κόστη (πχ 090) ώστε να πληρωθεί η εταιρία για τις υπηρεσίες που προσφέρει.

Σημείωση: Οι dialers είναι μια απειλή που δεν αφορά το γρήγορο ίντερνετ ADSL. Εκτός αν υπάρχει ακόμα στον Η/Υ συνδεδεμένο dial up modem.

Αυτό το είδος dialer είναι νόμιμο από τη στιγμή που η εταιρία και το πρόγραμμα της είναι δηλωμένα στην κατάλληλη κρατική υπηρεσία της εκάστοτε χώρας, και εφόσον εξηγούν στον χρήστη το κόστος που προκύπτει και φυσικά του δίνουν τη δυνατότητα να επιλέξει αν θα κατεβάσει το πρόγραμμα ή όχι. Προβλήματα δημιουργούνται όταν οι dialer είναι παράνομοι, κατεβάζονται και εκτελούνται χωρίς την άδεια του χρήστη και χρεώνουν υπέρογκα ποσά. Πολλοί θα αναρωτηθούν: "Είναι δυνατόν να κατεβεί ένα πρόγραμμα χωρίς να κάνω εγώ αυτή την ενέργεια;". Και η απάντηση είναι ναι, εφόσον ο internet explorer δεν έχει ρυθμιστεί κατάλληλα σχετικά με την εκτέλεση active x. Τα active x είναι μια τεχνική που υποστηρίζεται μόνο από τον internet explorer και επιτρέπει την εκτέλεση και το κατέβασμα κώδικα. Άν ο Internet Explorer έχει ενεργοποιημένα τα active x και δεν έχει ρυθμιστεί έτσι ώστε να προειδοποιεί τον χρήστη για την εκτέλεση και το κατέβασμα αρχείων, τότε μπορεί ένας dialer να κατεβεί χωρίς να το καταλάβουμε. Άλλοι dialers που δίνουν τη δυνατότητα στο χρήστη να τον ακυρώσει, δεν εξηγούν με σαφήνεια τι είναι το πρόγραμμα που προτρέπουν να κατεβεί ή εμφανίζουν δηλώσεις τους τύπου: "πατήστε οκ και θα έχετε άμεση πρόσβαση σε όλες τις υπηρεσίες". Η φράση που περιέχει το OK με μεγάλα γράμματα είναι πολύ συχνή στους dialer. Σε μερικές περιπτώσεις αντί για OK, υπάρχει το NAI.

Εφόσον ο Internet explorer είναι ο μοναδικός περιηγητής που χρησιμοποιεί active x (ο firefox χρησιμοποιεί active x μόνο μέσα από ένα plug in που πρέπει να εγκατασταθεί με γνώση του χρήστη), είναι αυτονόητο ότι είναι πολύ πιο ασφαλή η περιήγηση στο διαδίκτυο με την Opera. Μια πολύ καλή συμβουλή είναι να μη κάνετε κλικ σε οτιδήποτε εμφανίζεται. Πάντα να ελέγχετε τί κατεβάζετε και να μην εμπιστεύεστε εύκολα τα διάφορα sites.

Το Antivirus Antivir δίνει ευτυχώς (και μετά από κερδισμένες νομικές μάχες στη Γερμανία) τη δυνατότητα προστασίας του Η/Υ και από dialers. Κατά την εγκατάσταση ρωτάει τον χρήστη αν επιθυμεί την ανίχνευση και προστασία τυχόν dialers στον Η/Υ. Παράλληλα μπορείτε να πάτε στον ΟΤΕ και να κάνετε φραγή όλων των εξερχόμενων κλήσεων σε νούμερα τύπου 090.

Πως να αναγωρίζετε τους Dialer

Αν κατεβάσετε έναν dialer είτε γιατί δεν το καταλάβετε είτε γιατί δεν διαβάσατε με λεπτομέρεια τους όρους χρήσης μιας ιστοσελίδας ή προγράμματος, τότε υπάρχουν κάποια τρικ για να τον αναγνωρίσετε πριν ενεργοποιηθεί. Καταρχήν πριν το κατέβασμα, αν δείτε ΟΚ στη σελίδα με μεγάλα γράμματα, 99% προκειται για Dialer. Μετά το κατέβασμα, μην εκτελέσετε το αρχείο αν δεν το τσεκάρετε με το antivirus. Αν το εκτελέσετε ενώ είστε online θα ακούσετε τον κλασσικό ήχο του modem αν δεν έχετε χαμηλώσει την ένταση του μεγαφώνου. Για αυτό το λόγο συνιστάται να μην χαμηλώνετε την ένταση του modem.

Από τη στιγμή που ακούτε ένα τέτοιο ήχο, καλό είναι να τραβήξετε το καλώδιο του modem ή του υπολογιστή αμέσως! (Μου έχει τύχει και έκανα άμεσο reset πριν ο dialer ολοκληρώσει την κλήση).

Αυτός είναι ένας πολύ καλός τρόπος αναγνώρησης ενός dialer αλλά δεν είναι 100% ασφαλής γιατί υπάρχουν dialer που επεμβαίνουν στις ρυθμίσεις ήχου του modem και χαμηλώνουν την ένταση του μεγαφώνου!

Τι να κάνετε σε περίπτωση που έχετε πέσει θύμα ενός παράνομου Dialer.

Καταρχήν μην πανικοβληθείτε και κρατήστε την ψυχραιμία σας!
Βγείτε άμεσα από το ίντερνετ.
Μην σβήσετε τίποτα από τον υπολογιστή σας.
Δημιουργήστε ένα image του σκληρού δίσκου σας.
Διαμαρτυρηθείτε στον ΟΤΕ με αποδεικτικό στοιχείο το image που φτιάξετε και μην πληρώσετε τους απατεώνες.

1.9 SPAM

Spam είναι μια δικτυακή κατάχρηση, φάρσα ή ακόμα και απάτη. Με τον όρο Spam μπορούμε να χαρακτηρίσουμε ενέργειες που σχετίζονται με κατάχρηση email (spam email), messengers (spim), blogs (sblogs), forum, κινητά τηλέφωνα, μηχανές αναζήτησης κτλ. Η κατάχρηση αυτή γίνεται συνήθως, αλλά όχι αποκλειστικά, με σκοπό να διαφημιστούν ιστοσελίδες, προϊόντα ή υπηρεσίες και έχει κριθεί παράνομη για διάφορους λόγους. Πρώτον είναι ενοχλητική και επίμονη. Οι όγκοι τέτοιων διαφημίσεων είναι μεγάλοι και σπαταλούν τον πολύτιμο χρόνο μας. Ενώ μπορεί να περιμένουμε σημαντικά email, τα spam καθιστούν δύσκολο να ξεχωρίσουμε τα χρήσιμα από τις διαφημίσεις και χρεώνεται ο λογαριασμός μας στον ΟΤΕ περισσότερο, αφού αναγκαζόμαστε να μένουμε online περισσότερο. Επίσης, τέτοια email μπορεί να περιέχουν κακόγουστες φάρσες, επικίνδυνες απάτες, κακόβουλα προγράμματα (ιοί, σκουλήκια κτλ) και άλλο παράνομο υλικό.

Αυτή η ενοχλητική αλληλογραφία αποτελείται από emails που στέλνονται μαζικά σε χιλιάδες διευθύνσεις email ανά τον κόσμο. Οι spammer, αυτοί που στέλνουν τα email δηλαδή, χρησιμοποιούν διάφορους τρόπους, κυρίως βασιζόμενη στην τεχνολογία, για να εντοπίσουν διευθύνσεις email που υπάρχουν στον ίντερνετ. Σαρώνουν λοιπόν το διαδίκτυο με ειδικά προγράμματα που συλλέγουν διευθύνσεις και τις αποθηκεύουν σε μεγάλες λίστες. Ακόμα και emails που χρησιμοποιούνται στις λίστες των DNS μπορούν να εντοπισθούν. Εκτός από αυτούς τους τρόπους όμως, μπορεί και να μαντεύουν το email βασιζόμενοι σε ένα domain όνομα ή σε εφαρμογές που χρησιμοποιούν λεξικά. Οι λίστες των spammer μπορεί να πουληθούν και σε άλλους επαγγελματίες του είδους.

Για τους αρχάριους του ίντερνετ είναι μερικές φορές δύσκολο να συνειδητοποιήσουν ότι αυτά τα email δεν απευθύνονται σε αυτούς προσωπικά και πέφτουν πιο εύκολα θύματα σε τέτοιες ηλεκτρονικές

απάτες. Γι'αυτό χρησιμοποιώντας το ίντερνετ δε πρέπει να ξεχνάμε την κοινή λογική που θα μας συνόδευε σε οποιαδήποτε άλλη μας δραστηριότητα.

Σκοπός των email spam και μερικά από τα είδη που έχω δει μέχρι στιγμής, είναι τουλάχιστον ένας από τους παρακάτω:

Είδη ηλεκτρονικού spam

Διαφήμιση	Διάδοση Malware	Εξακρίβωση email
Phishing	Φάρσα-Hoax	Προσηλυτισμός
Nigeria C.	Flooding	DoS

1.9.1 ΔΙΑΦΗΜΙΣΗ

Τα spam email που περιέχουν διαφημίσεις είναι τα πιο συνηθισμένα και ονομάζονται επίσημα "μη ζητηθείσα εμπορική επικοινωνία" (unsolicited email) . Είναι ενοχλητικά γιατί φουσκώνουν το inbox μας με περιττές διαφήμισης ιστοσελίδων ή προϊόντων και επίσης καταλαμβάνουν χώρο, χρόνο και bandwidth καθώς κατεβαίνουν στον υπολογιστή μας. Η μη ζητηθείσα εμπορική αλληλογραφία είναι παράνομη σύμφωνα με το νόμο για την «Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα». Αυτός ο νόμος προβλέπει (άρθρο 9 του Ν.2774/1999):

Η με οποιοδήποτε τηλεπικοινωνιακό μέσο απ΄ ευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών επιτρέπεται μόνον στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους.

Αυτό σημαίνει ότι και η τακτική telemarketing ορισμένων εταιριών, όπως κάποιων τραπεζών που προσπαθούν να πουλήσουν πιστωτικές κάρτες από το τηλέφωνο, είναι παράνομη και θα έπρεπε να τιμωρείται. Την επόμενη φορά λοιπόν που κάποιος πωλητής θα σας πάρει τηλέφωνο χωρίς τη ρητή συγκατάθεσή σας, επικαλεστείτε τον νόμο προστασίας προσωπικών δεδομένων και μη τον αφήσετε να σπαταλήσει τον χρόνο σας. :) Επίσης να προσέχετε που δίνετε τα στοιχεία σας, γιατί πολλές εταιρίες τα πουλάνε σε άλλες για να σας ενοχλούν με διαφημίσεις. Όταν όμως τα δίνετε από μόνοι σας από το τηλέφωνο, είναι σας να δίνετε τη "ρητή συγκατάθεσή σας".

1.9.2 ΔΙΑΔΟΣΗ Malware

Ιοί και άλλα προγράμματα που περιέχουν βλαβερό κώδικα στέλνονται συννημένα σε email. Θα έχετε ακούσει τη συνηθισμένη συμβουλή "μην ανοίγετε συννημένα από ανθρώπους που δε γνωρίζετε". Πρέπει κανείς να λάβει υπόψη του ότι είναι πολύ εύκολο να παραποιηθεί και να πλαστογραφηθεί η διεύθυνση του πραγματικού αποστολέα.

"Θα πλαστογραφούσε ένας spammer τη διεύθυνση ενός φίλου μου;"

Ναι! Έχει συμβεί και δεν είναι σπάνιο φαινόμενο. Πιό πιθανό όμως είναι να έχει κολλήσει κάποιος φίλος σας ένα σκουλήκι (worm) το οποίο στέλνει τον εαυτό του αυτόματα σε όλες τις αποθηκευμένες επαφές του προγράμματος αλληλογραφίας (outlook express, outlook, thunderbird κτλ).

Κακόβουλα προγράμματα μπορούν να περιέχονται και στο κώδικα HTML του email με τη μορφή κάποιου script. Σε αυτή την περίπτωση αρκεί η απλή προεπισκόπιση του email για να κολλήσει κανείς ιό. Η λύση είναι να απενεργοποιήσουμε τον κώδικα HTML στο πρόγραμμα αλληλογραφίας.

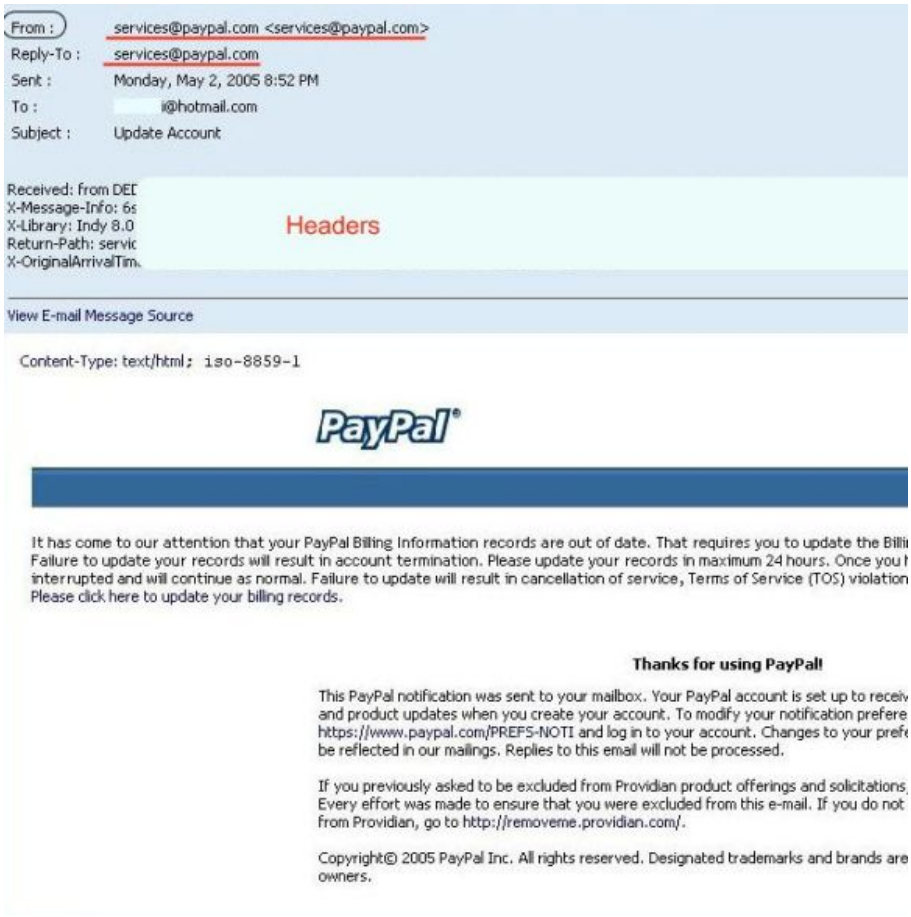
1.9.3 ΕΞΑΚΡΙΒΩΣΗ Email

Οι spammers στέλνουν συχνά emails τα οποία περιέχουν ένα πρόγραμμα που ενημερώνει τον αποστολέα αν ο λογαριασμός email είναι ενεργός. Όταν σιγουρευτούν συνεχίζουν να στέλνουν SPAM emails και κρατάνε τη διεύθυνση email στα αρχεία τους. Για αυτό τον σκοπό χρησιμοποιούνται και τα αρχεία εικόνας. Ο τρόπος αντιμετώπισης είναι πάλι η απενεργοποίηση του κώδικα HTML και το μπλοκάρισμα της εμφάνισης των εικόνων.

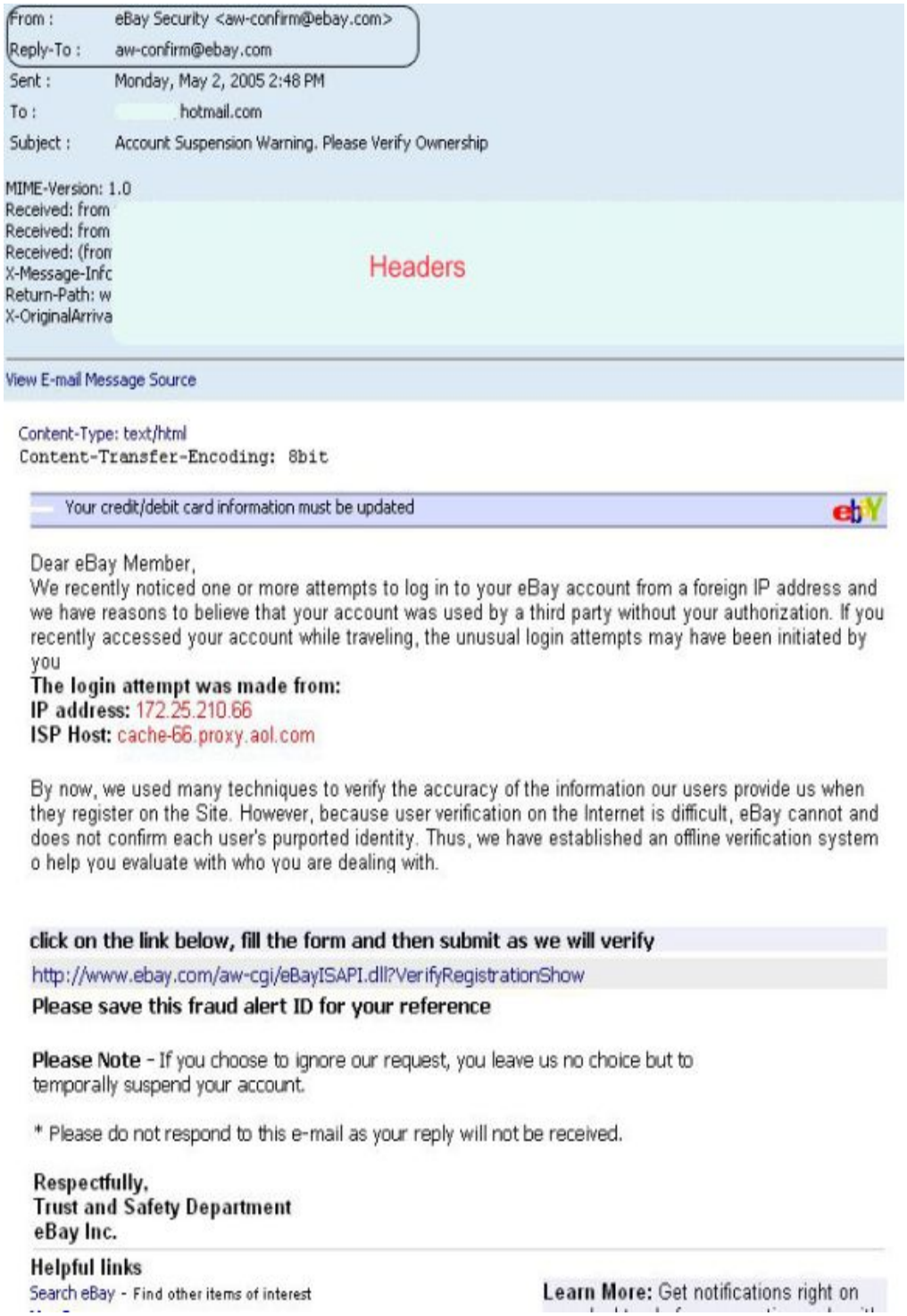
1.9.4 ΑΠΑΤΗ – Phishing

Phishing = Ψάρεμα! Emails που φαίνονται να προέρχονται από μεγάλες και γνωστές εταιρίες, με όλα τα γραφικά και το κατάλληλο επίσημο κείμενο, προσπαθούν να σας ψαρέψουν και να σας πείσουν ότι πρέπει να εισάγετε τα στοιχεία του λογαριασμού σας για εξακρίβωση ή για να αποφευχθεί κάποιο σοβαρό πρόβλημα. Αυτό το είδος απάτης είναι πολύ καλά σχεδιασμένο και στοχεύει σε κωδικούς από πελάτες των amazon, ebay, citybank, paypal και άλλων μεγάλων εταιριών. Δυστυχώς πολλοί αφελείς έχουν πέσει θύμα τέτοιων Phishing email με αποτέλεσμα να αδειάσουν οι λογαριασμοί τους από τους ηλεκτρονικούς εγκληματίες! Η επιτυχία των phishing email βασίζεται σε ψυχολογικούς τρόπους παραπλάνησης ανθρώπων που είναι αφελείς και δεν έχουν τις κατάλληλες γνώσεις. Αυτός ο ψυχολογικός τρόπος παραπλάνησης και καθοδήγησης των θυμάτων λέγεται "κοινωνική μηχανική" (social engineering) και έχει χρησιμοποιηθεί κατά καιρούς από hackers με διάφορες παραλλαγές. Πολλές φορές μάλιστα η κοινωνική μηχανική αποδεικνύεται πιο αποτελεσματική από τεχνολογικά μέσα (κατασκοπευτικά προγράμματα και ιούς) γιαυτό και χρησιμοποιείται ευρέως.

Παράδειγμα PHISHING που μιμείται την εταιρία Paypal:



PHISHING που μιμείται την εταιρία Ebay:



1.9.5 ΦΑΡΣΑ – Hoax

Ένα ακόμα επικίνδυνο spam το οποίο είναι δυστυχώς αρκετά διαδεδομένο είναι το HOAX. Αυτά είναι email που φαίνεται να περιέχουν πληροφορίες για τον πιο επικίνδυνο ιό και μας καλούν να προωθήσουμε το μήνυμα σε όλα τα άτομα στη λίστα μας. Τέτοια hoax στέλνονται συχνά και μέσω των

messengers, δεν περιέχουν ποτέ αξιόπιστες πληροφορίες και σκοπό έχουν να σπείρουν τον τρόμο και τον πανικό ανάμεσα σε άπειρους χρήστες. Να βασίζεστε μόνο σε επίσημες πληροφορίες που μπορείτε να βρείτε σε επίσημες και γνωστές ιστοσελίδες κατασκευαστών antivirus. Εκτός του ότι δεν είναι αστείο να σπέρνουμε τον πανικό με το να προωθούμε τέτοια γελοία email, μαζικές προωθήσεις δημιουργούν μεγάλα προβλήματα και αστάθειες στα δίκτυα.

Παράδειγμα HOAX 1:

A MEMBER OF AOL BY THE SCREEN NAME OF ZZ331MIGHT TRY TO SEND YOU A VIRUS WHICH COULD CRASH YOUR COMPUTER SYSTEM. HIS TRICK: HE INNOCENTLY IM's YOU HELLO, WAITS 30 SECONDS, THEN IM's YOU AGAIN, WAITS ANOTHER 30 SECONDS, AND THEN WRITES... "WHAT THE FU**, WHY AREN'T YOU ANSWERING"DO NOT REPLY TO HIS IM's, NOR READ ANY OF HIS E-MAIL BECAUSE ONCE YOU REPLY, YOUR COMPUTER WILL FREEZE AND THATS HOW YOU KNOW YOUR HARD DRIVE IS BEING WIPED OUT. SO PLEASE BE VERY VERY CAREFUL!!!!
PLEASE PASS THIS ON TO EVERY ONE YOU KNOW!!!

Παράδειγμα HOAX 2:

Outbreak: I'm infecting you with t-virus, my code is <random numbers>. Forward this to <phone number> to get your own code and chance to win prizes. More at <website URL>

1.9.6 Flooding

Flooding σημαίνει πλημμυρίζω και είναι ένας όρος που χρησιμοποιείται για να περιγράψει το πλημμύρισμα των λογαριασμών email. Στόχος τους είναι να παραλύσουν ένα δίκτυο ή έναν email provider και τα email που στέλνονται είναι συνήθως άδεια, χωρίς κανένα περιεχόμενο.

1.9.7 ΠΩΣ ΝΑ ΑΠΟΦΕΥΓΕΤΕ ΤΑ SPAM

Για να αποφεύγουμε το spam πρέπει να προστατεύουμε το email μας και να προσέχουμε να μη το δημοσιεύουμε σε σελίδες του ίντερνετ. Οι spammers χρησιμοποιούν "διαδικτυακά ρομπότ" που σκανάρουν το διαδίκτυο για ηλεκτρονικές διευθύνσεις και τις αποθηκεύουν στα αρχεία τους. Αυτές τις διευθύνσεις μετά τις πουλάνε σε άλλους spammers. Αν παρατηρήσετε προσεκτικά την ιστοσελίδα μου, δε θα βρείτε πουθενά το email μου σαν link παρά μόνο σαν αρχείο εικόνας. Ένας άλλος τρόπος προστασίας του email είναι να μη χρησιμοποιείτε το σύμβολο @ αλλά να περιγράφετε το email όπως ακούγεται (ηχητικά) πχ "myemail at yahoo dot com" όπου at=@, dot=. Ένα άλλο πρόβλημα είναι ότι αν ο ηλεκτρονικός υπολογιστής ενός φίλου σας μολυνθεί από κάποιο κατασκοπευτικό πρόγραμμα, το πιό πιθανό είναι να καταγράψει όλα τα email που έχει ο φίλος σας αποθηκευμένα στον Η/Υ του και να τα ενσωματώσει στις "διευθνείς" spam λίστες. Έτσι δε φτάνει να προστατεύετε εσείς το email σας. Πρέπει να μάθουμε όλοι να σεβόμαστε το απόρρητο της ηλεκτρονικής διεύθυνσης email και να το διαχειριζόμαστε σαν ένα νούμερο τηλεφώνου που δε θα αποκαλύπταμε πουθενά χωρίς την άδεια του ιδιοκτήτη.

1.9.8 ΠΡΟΣΤΑΤΕΥΕΣΤΕ ΤΑ E-MAIL ΤΩΝ ΦΙΛΩΝ ΣΑΣ

Σαν απλοί χρήστες μη στέλνετε email μαζικά σε λίστες φίλων σας χωρίς να χρησιμοποιείτε την επιλογή bcc. Θα το έχετε παρατηρήσει ότι στην αποστολή ενός email έχετε το πεδίο ΠΡΟΣ, ΘΕΜΑ, αλλά και τα πεδία cc, bcc. CC (carbon copy) σημαίνει δηλαδή καρμπόν αντίγραφο και BCC (blind carbon copy) σημαινει "τυφλό" καρμπόν αντίγραφο. Στο πεδίο bcc μπορείτε να γράφετε τη λίστα με τα email των φίλων σας, έτσι ώστε να μην είναι ορατά για τα υπόλοιπα μέλη και να προστατεύονται έτσι τα δεδομένα τους. Ένας ακόμα τρόπος που ακολουθούν πολλοί είναι το να έχουμε μια απλή δωρεάν ηλεκτρονική διεύθυνση (webmail: yahoo, hotmail, gmx κτλ) που χρησιμοποιείται σε εγγραφές στο ιντερνετ (messenger,

message boards, φόρουμ, clubs κτλ) και το επίσημο email το οποίο προστατεύουμε. Αυτή είναι μια πολύ καλή τακτική. Διαφορετικά, ο μόνος τρόπος να προστατευτούμε από το spam και μια τακτική που αναγκάζονται να χρησιμοποιούν εταιρίες των οποίων το email είναι πολύ γνωστό, είναι τα διάφορα εμπορικά και μη προγράμματα anti-spam.

Παρόλαυτά, εγώ εδώ δε θα προτείνω κάποια προγράμματα Antispam γιατί ούτε μέσα από αυτά μπορεί κανείς να εγγυηθεί ότι δε θα λάβει ανεπιθύμητη αλληλογραφία ή το οτι θα λειτουργίσουν σωστά τα φίλτρα του και δεν θα εμποδίσει χρήσιμη αλληλογραφία να κατεβεί. Όπως και να το κάνουμε το spam δε μπορούμε τα το αποφύγουμε τελείως με κανένα τρόπο, όσο δεν υπάρχουν αυστηροί νόμοι για τη καταπολέμησή του και όσο δεν εφαρμόζονται . Αν και σε πολλές χώρες υπάρχουν τέτοιοι νόμοι, δυστυχώς δεν εφαρμόζονται. Ακόμα χειρότερα οι περισσότεροι internet providers δεν συμβάλλουν στον αγώνα κατά του spam και δεν προσφέρουν abuse email διευθύνσεις καταγγελιών. Το 90% από τις φορές που έχω προσπαθήσει να καταδιώξω και να εντοπίσω αυτούς που στέλνουν τα spam, σκοντάφτω σε ασιατικούς providers που δεν έχουν δεσμεύσεις και δεν υπόκειται (?) σε Antispam νόμους. Όπως φαίνεται υπάρχει μια μεγάλη μερίδα ανθρώπων ανά τον κόσμο που στη κυριολεξία ζει και πλουτίζει από την ανεπιθύμητη αλληλογραφία και ίσως αυτός να είναι ο μεγαλύτερος λόγος για τον οποίο δεν υπάρχουν αποτελεσματικά μέτρα κατά της.

1.9.9 ΕΛΛΗΝΕΣ Spammers

Το ίντερνετ στην Ελλάδα αναπτύσσεται συνεχώς, ακόμα όμως δεν μπορεί, εκ των πραγμάτων, να συγκριθεί με το αμερικάνικο, το γερμανικό και το αγγλικό ίντερνετ. Όπως έχουν δείξει έρευνες που δημοσιεύονται κατά καιρούς στις αθηναϊκές εφημερίδες, το ποσοστό των ελλήνων που χρησιμοποιούν το διαδίκτυο είναι πολύ μικρό σε σχέση με την Ευρώπη. Πραγματικά δεν θα περίμενε κανείς να υπάρχουν έλληνες spammers, απο ότι φαίνεται όμως υπάρχουν αρκετοί webmasters και άλλοι επαγγελματίες που καταφεύγουν σε μεθόδους spam για να διαφημίσουν την ιστοσελίδα και τα προϊόντα τους. Έχω βάσιμες υποψίες ότι ήδη υπάρχουν κάποια ελληνικά φόρουμ, τα οποία πουλάνε τις βάσεις δεδομένων τους και συνεργάζονται με spammers! Πίστευα για πολύ καιρό ότι το email αποθηκεύεται κρυπτογραφημένο στις βάσεις δεδομένων των φόρουμ, όμως κάτι τέτοιο ισχύει μόνο για τους κωδικούς (passwords) και όχι πάντα (εξαρτάται από το λογισμικό).

1.10 ΠΡΟΤΕΙΝΟΜΕΝΗ ΜΕΘΟΔΟΛΟΓΙΑ ΒΕΛΤΙΩΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

«Απέναντι στους έμπειρους στην επίθεση,
ο εχθρός δεν ξέρει πώς να αμυνθεί.
Απέναντι στους επιδέξιους στην άμυνα
ο εχθρός δεν ξέρει που να επιτεθεί» -Sun Tzu

Η ύπαρξη ασφάλειας στο intranet και το extranet απαιτεί την δημιουργία εμποδίων στην φυσική προσπέλαση του εξοπλισμού, το δίκτυο, αλλά και τις εφαρμογές. Τι είναι όμως αυτό που θέλουμε να διαφυλάξουμε; Μία γενική απάντηση της μορφής «τον οργανισμό ή εταιρία μου από αυτούς που θέλουν να χρησιμοποιήσουν την τεχνολογία για να κάνουν κακό», αφήνει περιθώρια για μία μόνο λύση στο πρόβλημα: μην χρησιμοποιείτε υπολογιστές. Αυτή την στιγμή δεν υπάρχει 100% ασφαλές σύστημα προστασίας ενός intranet ή extranet. Μάλιστα όσο πλησιάζουμε προς την απόλυτη ασφάλεια το ίδιο ασυμπτωτικά διογκώνεται το κόστος για την δημιουργία ενός τέτοιου συστήματος ασφάλειας.

Για να είναι εφικτή μια υλοποίηση, δηλαδή το κόστος υλοποίησης του συστήματος ασφάλειας να είναι μικρότερο από το κόστος μιας επίθεσης, πρέπει να γίνουν μία σειρά από ενέργειες που έχουν σκοπό την ανάλυση, τον σχεδιασμό, την υλοποίηση και την λειτουργία του συστήματός μας, για την αντιμετώπιση περιστατικών επιθέσεων.

Έτσι Χρειάζεται:

1. Να γίνει ανάλυση των κινδύνων που έχουμε να αντιμετωπίσουμε και καταγραφή των πόρων που πρέπει να διαφυλάξουμε,

2. να προσδιοριστεί η πολιτική ασφάλειας που θα εφαρμόσουμε,

3. να σχεδιάσουμε την αρχιτεκτονική του υπολογιστικού και πληροφοριακού συστήματος που θα αναπτύξουμε,

4. να αποφασίσουμε για τις υπηρεσίες ασφάλειας που θα υιοθετήσουμε για την προστασία του intranet/extranet,

5. να γνωρίζουμε τα εργαλεία και τις μεθόδους επιθέσεων καθώς και τα αντίμετρα που πρέπει να εφαρμόζονται,

6. να έχουμε σχεδιάσει τον τρόπο αντιμετώπισης ενός περιστατικού επίθεσης

7. να ενημερώνουμε τους χρήστες μας

8. να είμαστε πάντα ενήμεροι για τα τελευταία νέα σε θέματα ασφάλειας παρακολουθώντας λίστες και ανακοινώσεις κατασκευαστών υπολογιστικών συστημάτων, οργανισμών ασφάλειας, χρηστών, ακόμα και hackers.

Για να έχουμε ένα ικανοποιητικό επίπεδο ασφάλειας πρέπει να αναλύσουμε τα παραπάνω για να ικανοποιήσουμε την ύπαρξη έξι βασικών σημείων της ασφάλειας 22,49:

- Την εμπιστευτικότητα της πληροφορίας: διασφαλίζοντας πως η πληροφορία είναι προσπελάσιμη από τους σωστούς χρήστες (π.χ. τα σχέδια για το νέο προϊόν είναι προσπελάσιμα σε ορισμένους μόνο χρήστες)

- Την πιστοποίηση αυθεντικότητας: επαληθεύοντας την αυθεντικότητα ενός χρήστη ή υπολογιστικού συστήματος (π.χ. πως είναι πράγματι ο χρήστης που ζητά προσπέλαση)

- Την αποφυγή άρνησης πράξεων: εξασφαλίζοντας πως οι χρήστες δεν μπορούν να αρνηθούν τις ηλεκτρονικές πράξεις τους (π.χ. ότι αντέγραφαν ένα αρχείο)

- Την ακεραιότητα των δεδομένων: διασφαλίζοντας πως τα δεδομένα δεν έχουν αλλάξει και είναι τα ίδια με αυτά που αρχικά τοποθετήθηκαν (π.χ. τα περιεχόμενα της μελέτης δεν έχουν αλλάξει από κάποιο τρίτο)

- Τον έλεγχο προσπέλασης: διασφαλίζοντας πως οι πόροι βρίσκονται κάτω από τον αποκλειστικό έλεγχο εξουσιοδοτημένων χρηστών, βεβαιώνοντας πως ο χρήστης που ζητά την προσπέλαση έχει την άδεια να το κάνει (π.χ. η αλλαγή στο αρχείο ενός υπαλλήλου επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα)

- Την διαθεσιμότητα των πόρων: εξασφαλίζοντας πως τα δεδομένα οι υπηρεσίες και οι εξυπηρετητές είναι διαθέσιμα όποτε ζητηθούν (π.χ. άμεση αποκατάσταση δεδομένων και υπηρεσιών μετά από επίθεση).

1.10.1 ΑΠΟΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ

Γενικά

Είναι πολύ σημαντικό να καταλάβουμε πως στην υλοποίηση της ασφάλειας δεν μπορεί κανείς να κάνει την ερώτηση «ποιο είναι το καλύτερο firewall, να το εγκαταστήσω». Υπάρχουν δύο άκρα: απόλυτη ασφάλεια και απόλυτη ελευθερία πρόσβασης. Μία καλή προσέγγιση προς την απόλυτη ασφάλεια έχουμε όταν ο υπολογιστής μας δεν είναι συνδεμένος με το δίκτυο, δεν είναι συνδεμένος στο ηλεκτρικό ρεύμα, είναι κλειστός, κλειδωμένος σε ένα χρηματοκιβώτιο, κτισμένο με τεράστιες ποσότητες τσιμέντου σε πολύ μεγάλο βάθος, με μοναδική είσοδο που φυλάσσεται από ακριβοπληρωμένους φρουρούς. Δυστυχώς έτσι δεν είναι και τόσο χρήσιμος.

Από την άλλη πλευρά ένας υπολογιστής με πλήρη ελευθερία πρόσβασης είναι μεν τρομερά εύχρηστος, αλλά μπορεί να καταλήξει άχρηστος αφού χωρίς κανόνες χρήσης ο καθένας μπορεί να κάνει ότι θέλει καταστρέφοντας την λειτουργικότητά του είτε εσκεμμένα, είτε από άγνοια.

Οι περισσότεροι άνθρωποι έχουν μία εικόνα για το ανεκτό επίπεδο κινδύνου γ-ια κάθε ενέργειά τους (όσο και αν είναι προσιτό δεν πηδάμε από το παράθυρο του σπιτιού μας για να κατέβουμε γρήγορα στο δρόμο να προλάβουμε το λεωφορείο για την δουλειά, ενώ μπορεί να το επιχειρήσουμε αν κινδυνεύει η ζωή μας).

Ο κάθε οργανισμός λοιπόν πρέπει να αποφασίσει για τα συστήματά του, το σημείο που χρειάζεται να βρίσκεται, ανάμεσα στην απόλυτη ασφάλεια και την απόλυτη ευκολία προσπέλασης. Μία πολιτική ασφάλειας πρέπει να προσδιορίσει τους πόρους που έχουν αξία για τον οργανισμό, τις πιθανές απειλές και κατόπιν να προτείνει ων κατάλληλη πολιτική ασφάλειας για το πως θα διασφαλιστούν οι πόροι από τις πιθανές απειλές.

1.10.2 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ ΠΟΡΩΝ

Είναι σημαντικό να προσδιοριστούν όλοι οι πόροι που θα πρέπει να προστατευθούν. Η κατηγοριοποίηση των πόρων που θα προστατευθούν έχει ως εξής44,45:

Υλικό: Κεντρική Μονάδα Επεξεργασίας, τερματικοί σταθμοί εργασίας, προσωπικοί υπολογιστές, εκτυπωτές, δίσκοι, γραμμές επικοινωνίας, εξυπηρετητές, δρομολογητές.

Λογισμικό: Πηγαίος κώδικας, αντικείμενος κώδικας, εργαλεία, διαγνωστικά προγράμματα, λειτουργικά συστήματα, προγράμματα επικοινωνίας.

Δεδομένα: Αρχειοθετημένα off-line, αποθηκευμένα on-line, κατά την διάρκεια ως επεξεργασίας τους, αντίγραφα ασφαλείας.

Ανθρώπινο δυναμικό: Χρήστες, διαχειριστές, τεχνικοί κ.λπ.
Τεκμηρίωση: Προγραμμάτων, υλικού, συστημάτων, τοπικών διαδικασιών διαχείρισης.

Υλικό Υποστήριξης: Δημοσιεύσεις, φόρμες, μαγνητικά μέσα κ.α.

1.10.3 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Αφού καταγραφούν οι πόροι που πρέπει να προστατευτούν θα πρέπει να προσδιοριστούν πιθανές απειλές τους. Κλασικές απειλές που μπορεί να δεχθεί ένα σύστημα είναι οι ακόλουθες:

1. Σκόπιμη απειλή (Hacking, Denial of Service, κατασκοπία)
2. Απροσχεδίαστη απειλή (π.χ. λανθασμένη αποστολή με mail κρίσιμων στοιχείων σε μια ομάδα αποδεκτών)
3. Φυσικές περιβαλλοντικές απειλές (σεισμός)
4. Μη φυσικές απειλές (εμπρησμός, διακοπή ρεύματος)
5. Μη εξουσιοδοτημένη προσπέλαση των μέσων και / ή της πληροφορίας.
6. Αγνώστου ταυτότητας και / ή μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας.
7. Κατάργηση / άρνηση των προσφερόμενων υπηρεσιών.
8. Η εμπιστοσύνη παίζει σημαντικό ρόλο στην υλοποίηση της πολιτικής ασφάλειας. Το πρώτο βήμα είναι να αποφασιστεί ποιος έχει προσπέλαση, σε ποιους πόρους, τι είδους (διαχειριστή, απλού χρήστη, χειριστή) και να περιγραφεί το μοντέλο υλοποίησης με ομάδες χρηστών.

1.10.4 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Τι είναι πολιτική ασφάλειας και γιατί πρέπει να έχω

Η πολιτική ασφάλειας είναι το σύνολο των κανόνων που ρυθμίζουν την πρόσβαση που έχει κάθε χρήστης στα πληροφοριακά συστήματα ενός οργανισμού.

Χωρίς την ύπαρξη πολιτικής ασφάλειας δεν υπάρχει ένα γενικό πλαίσιο για την ασφάλεια. Με την πολιτική ορίζουμε ποια συμπεριφορά είναι επιτρεπόμενη μέσα στον οργανισμό ως προς την χρήση των προσφερόμενων υπηρεσιών, μέσα από διαδικασίες που πρέπει να ακολουθηθούν από όλους.

Η πολιτική ασφάλειας είναι μία καλή μέθοδος για την δημιουργία συναντίληψης ανάμεσα στα στελέχη του οργανισμού.

Οι χρήστες ανημετωπίζουν τις πολιτικές σαν ένα φρένο της παραγωγικότητας ή ένα τρόπο να ελέγχεται η συμπεριφορά των εργαζομένων, αρνούμενοι να υποκύψουν στην παρακολούθηση (σύνδρομο του Μεγάλου Αδελφού).

1.10.5 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Οι αποφάσεις που λαμβάνονται για την ασφάλεια ενός δικτύου από τον διαχειριστή του, καθορίζουν το πόσο ασφαλές είναι ένα δίκτυο καθώς και την ευκολία στη χρήση του.

Καταρχήν θα πρέπει να αποφασιστεί τι είναι σκόπιμο να διαφυλαχτεί.

Όταν γίνει αυτό θα πρέπει να οριστούν οι περιορισμοί που θα πρέπει να τεθούν ώστε να έχουμε το επιθυμητό αποτέλεσμα.

Οι στόχοι καθορίζονται από τους ακόλουθους παράγοντες:

1. Προσφερόμενες υπηρεσίες σε σχέση με την ασφάλεια του δικτύου. Υπάρχουν περιπτώσεις που η χρήση κάποιων υπηρεσιών αυξάνει τον κίνδυνο για την άρση της ασφάλειας ενός δικτύου, με αποτέλεσμα το κόστος των υπηρεσιών αυτών να είναι μεγαλύτερο από τα οφέλη τους. Σε τέτοιες περιπτώσεις είναι προτιμότερη η κατάργηση της υπηρεσίας.

2. Ευκολία χρήσης σε σχέση με τη προσφερόμενη ασφάλεια. Το ευκολότερο σύστημα στη χρήση είναι αυτό που προσφέρει άμεση πρόσβαση χωρίς την ύπαρξη συνθηματικών. Παρόλα αυτά ένα τέτοιο σύστημα δεν προσφέρει καμία απολύτως ασφάλεια. Με την χρήση συνθηματικών (password) το σύστημα γίνεται λίγο πιο δύσκολο αφού κάθε χρήστης θα πρέπει να θυμάται τον κωδικό του, αλλά ταυτόχρονα γίνεται και πιο ασφαλές.

3. Κόστος ασφάλειας ενάντια στον κίνδυνο απώλειας.
Υπάρχουν διάφορα είδη που προσδιορίζουν το κόστος της ασφάλειας όπως :

- Κόστος αγοράς υλικού ή λογισμικού, όπως firewalls και on-time password generators
- Απόδοση (η κωδικοποίηση και η αποκωδικοποίηση χρειάζονται κάποιο χρόνο) καθώς και ευκολία στην χρήση.

Υπάρχουν επίσης διάφορα επίπεδα κινδύνου όπως :

- Άρση του απορρήτου (π.χ. ανάγνωση πληροφορίας από τρίτους),
- Απώλεια δεδομένων (διαγραφή δεδομένων) ή
- Απώλεια υπηρεσιών (χρήση των πηγών του δικτύου, άρνηση πρόσβασης στο δίκτυο κ.α.).
- Για την υλοποίηση της ασφάλειας του δικτύου θα πρέπει να ληφθούν υπόψη όλα τα παραπάνω.

1.10.6 ΠΟΙΟΙ ΘΑ ΕΜΠΛΑΚΟΥΝ ΣΤΟ ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Μια πολιτική ασφάλειας για να είναι κατάλληλη για τον οργανισμό θα πρέπει να είναι αποδεκτή από όλους τους εργαζομένους. Επίσης θα πρέπει να υπάρχει υποστήριξη της πολιτικής και από τη διεύθυνση του οργανισμού ώστε να επιτύχει στους στόχους της. Οι ομάδες εργαζομένων που εμπλέκονται σε μια πολιτική ασφάλειας είναι:

1. Απλοί χρήστες - η πολιτική ασφάλειας αφορά αυτούς ως επί το πλείστον
2. Προσωπικό υποστήριξης - είναι αυτοί που θα υλοποιήσουν και θα υποστηρίξουν την πολιτική ασφάλειας
3. Διοικητικό προσωπικό - καθορίζουν το βαθμό προστασίας των περισσότερων δεδομένων και αναλαμβάνουν το οικονομικό κόστος της πολιτικής που θα υλοποιηθεί
4. Νομικοί σύμβουλοι - που ενδιαφέρονται για την φήμη και την νομική κάλυψη του οργανισμού

1.10.7 ΤΑ ΣΥΣΤΑΤΙΚΑ ΤΗΣ ΚΑΛΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Μια πολιτική ασφάλειας θα πρέπει να είναι:

- Υλοποιήσιμη: Να υπάρχουν ρεαλιστικοί κανόνες διαχείρισης των συστημάτων για κάθε τμήμα του οργανισμού, οδηγίες χρήσης των διάφορων πόρων, εγκατεστημένα συστήματα ασφάλειας.

- Θα πρέπει να ακολουθείται απ' όλους: Οι χρήστες θα πρέπει να κατανοήσουν πως δε γίνονται παρακάμψεις για τη διευκόλυνσή τους. Θα πρέπει οι ίδιοι να προσαρμόσουν τις καθημερινές δραστηριότητές τους στους κανόνες ασφάλειας. Δεν θα πρέπει όμως να είναι και υπερβολικά αυστηροί γιατί τότε οι χρήστες θα προσπαθούν να βρουν τρόπους για να ξεπεράσουν τους κανόνες.

- Ευέλικτη: Για να είναι βιώσιμη μια πολιτική ασφάλειας θα πρέπει να εξαρτάται από το υλικό και το λογισμικό που υπάρχει, ώστε να μπορεί να αναπροσαρμόζει τους κανόνες της σύμφωνα με τις προδιαγραφές τους. Επίσης θα πρέπει να αναγνωρίζει τις εξαιρέσεις που είναι δυνατό να γίνουν στους κανόνες ασφάλειας ανάλογα με τις ανάγκες που θα παρουσιαστούν. Για παράδειγμα ο διαχειριστής ενός συστήματος μπορεί να χρειαστεί τον κωδικό πρόσβασης κάποιου χρήστη για ένα σύστημα.

- Θα πρέπει να ισοσταθμίζει την προστασία του οργανισμού με την παραγωγικότητα. Αν οι κανόνες είναι πολύ αυστηροί οι χρήστες θα βρουν τρόπους να μην τους εφαρμόζουν. Οι τεχνικοί έλεγχοι δεν είναι πάντα εφικτοί.

- Αναβαθμίσιμη: Οι κανόνες που τίθενται θα πρέπει να αναπροσαρμόζονται και να ακολουθούν την εξέλιξη του οργανισμού.

Την πολιτική ασφάλειας που θα εφαρμόσουμε πρέπει να έχουν την ευκαιρία να την σχολιάσουν και όσοι θα δεχτούν τις επιπτώσεις της. Πολλά παραδείγματα πολιτικής μπορούν να βρεθούν στις ιστοσελίδες:

http://www.eff.orglpub/CAF/policies
http://www.gatech.edu/itis/policy/usage/contents.html
http://csrc.ncsl.nisiogov/secplcy/

1.10.8 ΚΑΝΟΝΕΣ ΑΣΦΑΛΕΙΑΣ

1. Κανόνες ασφάλειας για το δίκτυο

-Η πολιτική ασφάλειας για το δίκτυο καθορίζει:
-Ποιος εγκαθιστά καινούριες συσκευές στο δικτυο
-Ποιος ειδοποιείται για κάθε τέτοια εγκατάσταση
-Πώς τεκμηριώνεται μια τέτοια αλλαγή
-Ποιες είναι οι αλλαγές στο «χάρτη» του δικτύου
-Ποιες οι νέες απαιτήσεις σε ασφάλεια
-Πώς αντιμετωπίζονται μη ασφαλείς συσκευές

2. Κανόνες ασφάλειας για την προστασία των δεδομένων

-Η πολιτική ασφάλειας για την προστασία των δεδομένων - πληροφοριών του οργανισμού, καθορίζει:

-Επίπεδα κρισιμότητας των πληροφοριών που κυκλοφορούν
-Ποιος έχει πρόσβαση σε ευαίσθητες πληροφορίες
-Τα επίπεδα πρόσβασης σε τέτοιες πληροφορίες που έχουν οι ομάδες των χρηστών
-Πώς αποθηκεύεται και μεταδίδεται τέτοιου είδους πληροφορία
-Σε ποια συστήματα αποθηκεύεται τέτοια πληροφορία
-Σε ποια συστήματα εκτυπώνονται τέτοια δεδομένα

3. Κανόνες ασφάλειας των χρηστών

-Η πολιτική ασφάλειας για τους χρήστες θα πρέπει να καθορίζει:

-Την ευθύνη των χρηστών για την προστασία των δεδομένων που έχουν στους προσωπικούς λογαριασμούς τους

-Αν οι χρήστες μπορούν διαβάζουν και να αντιγράφουν αρχεία που δεν τους ανήκουν αλλά έχουν πρόσβαση

-Αν οι χρήστες μπορούν να μεταβάλλουν αρχεία που δεν τους ανήκουν αλλά έχουν δικαίωμα εγγραφής σ' αυτά

Αν οι χρήστες μπορούν να πάρουν αντίγραφα βασικών αρχείων (configuration files) από τα βασικά συστήματα του οργανισμού

-Αν οι χρήστες μπορούν να μοιράζουν αρχεία για κοινή χρήση
-Αν οι χρήστες μπορούν να δημιουργούν αντίγραφα νόμιμα αγορασμένου λογισμικού
-Το επίπεδο χρήσης του Mail, Web, News από τους χρήστες ή από ομάδες χρηστών

4. Κανόνες ασφάλειας των λογαριασμών των χρηστών

-Η πολιτική ασφάλειας για τους λογαριασμούς των χρηστών θα πρέπει να καθορίζει:

-Ποιος έχει τη δικαιοδοσία να δέχεται αιτήσεις ανοίγματος λογαριασμών

-Ποιος επιτρέπεται να κάνει χρήση των πόρων του οργανισμού

-Αν οι χρήστες μοιράζονται το λογαριασμό τους με άλλους ή αν έχουν περισσότερους από έναν λογαριασμούς σε συστήματα του οργανισμού

-Τα δικαιώματα και τις υπευθυνότητες των χρηστών για τη χρήση των πόρων που τους διατίθενται

-Πότε ο λογαριασμός ενός χρήστη απενεργοποιείται

-Τους κανόνες που ακολουθούν οι κωδικοί πρόσβασης των χρηστών

5. Κανόνες ασφάλειας για την απομακρυσμένη πρόσβαση

-Η πολιτική ασφάλειας για την απομακρυσμένη πρόσβαση θα πρέπει να καθορίζει:

-Ποιος έχει το δικαίωμα της απομακρυσμένης πρόσβασης (Authentication)

-Ποιες είναι οι επιτρεπόμενες μέθοδοι για απομακρυσμένη πρόσβαση

-Αν επιτρέπονται dial-out modems

-Αν θα υπάρχει καταγραφή των χρηστών που χρησιμοποιούν την υπηρεσία αυτή

-Αν θα δίνεται η δυνατότητα για callback

-Σε ποια δεδομένα επιτρέπεται η απομακρυσμένη πρόσβαση

6. Διαδικασία Configuration Management

-Η πολιτική ασφάλειας στη διαδικασία του configuration management καθορίζει:

-Πώς ελέγχεται και εγκαθίσταται καινούριο υλικό και λογισμικό στα συστήματα του οργανισμού

-Πώς τεκμηριώνονται οι αλλαγές σε υλικό και λογισμικό

-Ποιος ενημερώνεται για τυχόν αλλαγές σε υλικό και λογισμικό

-Ποιος έχει τη δικαιοδοσία να κάνει αλλαγές στο υλικό ή το λογισμικό των συστημάτων του οργανισμού

-Με ποια διαδικασία μπορεί να υπάρξει εξαίρεση σε ένα κανόνα για ορισμένο χρονικό διάστημα

-Πως γίνεται η διαχείριση των firewalls, πως ζητούνται αλλαγές και πως εγκρίνονται.

7. Διαδικασία αντιμετώπισης προβλημάτων

-Η πολιτική ασφάλειας στην περίπτωση που παρουσιαστεί κάποιο πρόβλημα (εισβολή) καθορίζει:

-Διαδικασία άμεσης υποστήριξης από εξειδικευμένο προσωπικό
-Τις πρώτες, άμεσες ενέργειες που πρέπει να γίνουν
-Τον τρόπο που θα αντιμετωπιστεί μια εισβολή
-Ποιες πληροφορίες θα πρέπει να καταγραφούν για να χρησιμοποιηθούν αργότερα
-Ποιος θα πρέπει να ενημερωθεί και πότε

8. Διαδικασία Backup

-Η πολιτική ασφάλειας για τη διαδικασία του backup καθορίζει:

-Ποια είναι τα αρχεία τα οποία παίρνονται backup (αρχεία συστήματος, αρχεία χρηστών)
-Πόσο συχνά πραγματοποιείται η διαδικασία του backup
-Αν υπάρχει Disaster Recovery το όποιο είναι άμεσα εκτελέσιμο μετά από κάποια δυσλειτουργία.
-Που φυλάγονται τα μαγνητικά μέσα.

Δέκα εντολές για την ασφάλεια των ηλεκτρονικών υπολογιστών σας

1. Μην προβαίνετε σε υποθέσεις. Αφιερώστε χρόνο από τον χρόνο σας στην εκμάθηση τρόπων και πρακτικών που θα κάνουν τον υπολογιστή σας πιο ασφαλή.

2. Αποκτήστε και χρησιμοποιήστε κάποια αξιόπιστη antivirus εφαρμογή. Επιλέξτε μία εφαρμογή η οποία διαθέτει αξιόπιστο και σταθερό παρελθόν. Οι Checkmark, AV-Test.org και TuV ανήκουν στους πλέον αξιόπιστους ανεξάρτητους ερευνητικούς οργανισμούς οι οποίοι δοκιμάζουν και αξιολογούν τις antivirus εφαρμογές.

3. Αποκτήστε και χρησιμοποιήστε κάποια αξιόπιστη firewall εφαρμογή. Για άλλη μια φορά, οι ανεξάρτητοι οργανισμοί δοκιμής και αξιολόγησης είναι το καλύτερό σας στοίχημα για λογικές επιλογές. Ορισμένα λειτουργικά συστήματα έρχονται με προ-εγκατεστημένο firewall που ωστόσο φιλτράρει μόνο την εισερχόμενη κίνηση των δεδομένων. Χρησιμοποιείστε ένα firewall που μπορεί να ελέγξει τόσο την εισερχόμενη όσο και την εξερχόμενη διακίνηση των δεδομένων με το Διαδίκτυο.

4. Μην ανοίγετε μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που προέρχονται από άγνωστη πηγή, ή πηγή που δεν εμπιστεύεστε. Πολλοί ιοί διακινούνται χάρη σε μηνύματα ηλεκτρονικού ταχυδρομείου. Για το λόγο αυτό, εάν για οποιονδήποτε λόγο είστε διστακτικοί, παρακαλούμε να ζητήσετε μία πρόσθετη επιβεβαίωση από τον αποστολέα.

5. Μην ανοίγετε συνημμένα αρχεία σε μηνύματα με ύποπτο ή απροσδόκητο τίτλο. Εάν θέλετε να τα ανοίξετε, αποθηκεύστε τα πρώτα στον σκληρό σας δίσκο και εν συνεχεία σκανάρετέ τα με μία ενημερωμένη antivirus εφαρμογή.

6. Διαγράψτε οποιοδήποτε ανεπιθύμητο μήνυμα ή μήνυμα τύπου αλυσίδας. Μην τα προωθήσετε και μην προσπαθήσετε να απαντήσετε στους αποστολείς τους. Αυτού του είδους η αλληλογραφία θεωρείται ως spam, διότι έρχεται αυτόκλητη, είναι ανεπιθύμητη και υπερφορτώνει την διακίνηση των δεδομένων στο Διαδίκτυο.

7. Αποφύγετε την εγκατάσταση διεργασιών και/ή εφαρμογών που δεν είναι αναγκαίες στις καθημερινές εργασίες, όπως για παράδειγμα εξυπηρετητές διανομής και διαμοιρασμού αρχείων, εξυπηρετητές απομακρυσμένης πρόσβασης, κ.ο.κ. Αυτά τα προγράμματα αποτελούν εν δυνάμει απειλές και δεν θα πρέπει να εγκαθίστανται εκτός των περιπτώσεων που η χρήση τους κρίνεται απολύτως απαραίτητη.

8. Αναβαθμίστε το σύστημα και τις εφαρμογές όσο πιο συχνά μπορείτε. Κάποια λειτουργικά συστήματα και εφαρμογές προσφέρουν δυνατότητα αυτοματοποίησης της διαδικασίας λήψης και εγκατάστασης των αναβαθμίσεων. Κάντε πλήρη χρήση αυτής της δυνατότητας. Τυχόν αδυναμία επιδιόρθωσης του συστήματός σας σε αρκετά συχνά χρονικά διαστήματα μπορεί να το αφήσει ευάλωτο σε απειλές για τις οποίες αναβαθμίσεις ασφάλειας είναι ήδη διαθέσιμες.

9. Μην αντιγράφετε οποιοδήποτε αρχείο αν δεν γνωρίζετε ή δεν εμπιστεύεστε την πηγή του. Ελέγξτε την πηγή προέλευσης των αρχείων που κατεβάζετε βεβαιωθείτε ότι τα αρχεία έχουν πιστοποιηθεί από κάποια antivirus εφαρμογή στην τοποθεσία προέλευσή τους.

10. Κρατήστε αντίγραφα ασφαλείας των σημαντικών προσωπικών σας αρχείων (αλληλογραφία, έγγραφα, φωτογραφίες, κ.α.) σε τακτά χρονικά διαστήματα. Αποθηκεύστε τα αντίγραφα σε κινητές μονάδες μνήμης όπως ένας δίσκος CD ή DVD. Κρατήστε το αρχείο σας σε διαφορετική τοποθεσία από εκείνη που στεγάζει τους υπολογιστές σας.

Κοιτώντας στο μέλλον

Υπάρχει μεγάλη ερευνητική και αναπτυξιακή προσπάθεια ώστε στο μέλλον οι κρίσιμες εφαρμογές να μπορούν να εκτελούνται σε ένα ασφαλέστερο περιβάλλον από ότι σήμερα. Τα παρακάτω αποτελούν μια ματιά στο κοντινό μέλλον. Γενικά, το κοντινό μέλλον ισχυροποιεί την σημασία της Κρυπτογραφίας

1.11 Internetworking Protocols - Σύγχρονη Κρυπτογραφία

Τα περισσότερα από τα πρωτόκολλα που χρησιμοποιούνται σήμερα δεν έχουν αλλάξει από τότε που ορίστηκαν, την εποχή του ARPA του ερευνητικού και εκπαιδευτικού δικτύου, που η εμπιστοσύνη ήταν ο κανόνας. Για να έχουμε μία ασφαλή βάση για τις κρίσιμες μελλοντικές εφαρμογές του διαδικτύου, πρέπει να αντιμετωπιστούν τα σοβαρά ελαττώματα που υπάρχουν σήμερα. Κύρια η έλλειψη της απόκρυψης (encryption) για την ασφαλή μετάδοση δεδομένων και την διασφάλιση της αυθεντικότητας της πληροφορίας, η έλλειψη της κρυπτογραφικής πιστοποίησης για την διασφάλιση της αυθεντικότητας της πηγής που προέρχεται η πληροφορία και η έλλειψη της δυνοτότητας cryptographic checksum για την διασφάλιση της ακεραιότητας των αποθηκευμένων δεδομένων, αλλά και της ίδιας της πληροφορίας δρο-μολόγησης. Τα νέα πρωτόκολλα που προτείνονται από την IETF (lnternet Engineering Task Force), όπως το Ipng ή αλλιώς Ιρν6 μπορούν να οδηγήσουν σε δημιουργία ασφαλέστερου περιβάλλοντος. Στο μέλλον, τα πρωτόκολλα πιστοποίησης θα υπόστηρίζονται σταδιακά από τεχνολογίες που σήμερα πιστοποιούν άτομα (π.χ. στο εργασιακό τους περιβάλλον), με την χρήση έξυπνων καρτών, αναγνώστες δακτυλικών αποτυπωμάτων, αναγνώριση προσώπου, ίριδας, φωνής κλπ.

Ο σχεδιασμός, η ανάλυση και η υλοποίηση πρωτοκόλλων θα είναι το αντικείμενο συνεχούς έρευνας. Ο στόχος, που είναι ένα 100% ασφαλές πρωτόκολλο (ασφαλές όσο και ο κρυπτογραφικός αλγόριθμος που το υποστηρίζει), δεν είναι μακριά.

1.11.1 Ανίχνευση Εισβολής

Η έρευνα σε αυτό τον τομέα διεξάγεται για την βελτίωση της δυνατότητας των δικτυακών συστημάτων να διακρίνουν πως δέχτηκαν επίθεση. Η ανίχνευση των παραβιάσεων αναγνωρίζεται σαν μια

δύσκολη ερευνητική περιοχή που βρίσκεται ακόμα στην αρχή της. Υπάρχουν δύο περιοχές στον τομέα αυτό, η ανίχνευση ανωμαλιών και η αναγνώριση προτύπων.

Η έρευνα στην ανίχνευση ανωμαλιών βασίζεται στον ορισμό προτύπων «κανονικής» συμπεριφοράς, σε δίκτυα, εξυπηρετητες, χρήστες και στην ανίχνευση συμπεριφορών που είναι κατά πολύ διαφορετικές (ανωμαλία). Τα πρότυπα της κανονικής συμπεριφοράς συνήθως προσδιορίζονται συγκεντρώνοντας στοιχεία για ένα χρονικό διάστημα κατάλληλο για την εξασφάλιση ενός τυπικού δείγματος συμπεριφοράς των εξουδιοδοτημένων χρηστών και των διαδικασιών (processes) των συστημάτων. Η βασική δυσκολία που πρέπει να αντιμετωπιστεί, είναι πως η κανονική συμπεριφορά είναι ευμετάβλητη εξαιτίας πληθώρας αβλαβών ενεργειών που μπορούν να επιτρέψουν παραβιάσεις. Πολλές από τις ενέργειες ενός εισβολέα δεν διαφοροποιούνται από τις ενέργειες εξουσιοδοτημένων χρηστών.

Η δεύτερη μεγάλη περιοχή είναι η αναγνώριση προτύπων. Ο στόχος εδώ είναι να αναγνωριστούν ακολουθίες γεγονότων στην συμπεριφορά του δικτύου, των εξυπηρετητών και των χρηστών,που προέρχονται από γνωστά σενάρια επιθέσεων. Ένα πρόβλημα σε αυτή την προσέγγιση είναι η πληθώρα των διαφορετικών σεναρίων που προκύπτουν από την διαφοροποίηση της στρατηγικής που εφαρμόζει ο κάθε εισβολέας κάνοντας χρήση της ίδιας μεθόδου. Ένα δεύτερο πρόβλημα είναι πως νέα είδη επιθέσεων που δεν είναι γνωστά τα μοτίβα επίθεσης, δηλαδή η «υπογραφή» τους, δεν μπορουν να αντιμετωπιστούν με αυτή την προσέγγιση.

Τέλος πρέπει να αναφερθεί πως υπάρχει ανάγκη να βρεθούν εργαλεία και τεχνικές για την αναγνώριση επιθέσεων που προέρχονται από διαφορετικά μέρη του Internet αλλά συντονίζονται από ένα σημείο (Distributed Denial of Service-DdoS), καθώς και πρωτόκολλα που να επιτρέπουν την ιχνηλασία της αρχής των επιθέσεων.

1.11.2 Software Engineering και ικανότητα επιβίωσης των συστημάτων

Οι τρέχουσες μέθοδοι δημιουργίας λογισμικού δεν έχουν να επιδείξουν αξιόλογα επιτεύγματα, σε ότι αφορά θέματα ασφάλειας. Τις περισσότερες φορές το θέμα της ασφάλειας είναι μεταγενέστερο του βασικού σχεδιασμού του λογισμικού. Η δημιουργία ασφαλών λογισμικών, πρέπει να έχει την δυνατότητα να επιδεικνύει το λογισμικό συμπεριφορά που συνεισφέρει στην ικανότητα επιβίωσης του συστήματος παρά τις επιθέσεις που δέχεται.

Σαν ικανότητα επιβίωσης, ορίζεται η ικανότητα ενός συστήματος να συνεχίζει να εκτελεί τις κρίσιμες λειτουργίες ,με τον χρονοπρογραμματισμό που έχει οριστεί ,ακόμα και αν μέρος των πόρων του συστήματος έχουν δεχτεί επίθεση ή έχουν βλάβη .Ο όρος σύστημα έχει ευρεία έννοια και περιλαμβάνει και συστάδες από συστήματα και δίκτυα.

Αν και αρχές και μεθόδοι που έχουν να κάνουν με την ικανότητα επιβίωσης είναι χαρακτηριστικά των έμβιων όντων ,μπορούν να υλοποιηθούν με παραδοσιακές τεχνικές της περιοχής της δημιουργίας λογισμικού και των υπολογιστικών συστημάτων ,όπως αξιοπιστία ,αντιμετώπιση σφαλμάτων ,επιβεβαίωση ορθότητας ,απόδοση και ασφάλεια συστημάτων .Η έρευνα κατευθύνεται σε δημιουργία μεθόδων ανοσοποίησης που θα διακινούν αυτόματα τις διορθώσεις των τρωτών ,σε ένα ολόκληρο δίκτυο ,για να διαφυλαχτούν όλα τα συστήματα από ένα νέο πρόβλημα ασφάλειας .Η έννοια της ανοσοποίησης μπορεί να γενικευθεί ώστε να συμπεριλάβει προσαρμόσιμα δίκτυα ,που αποτελούνται από κατανεμημένα συνεργαζόμενα δικτυακά στοιχεία ,που ανταλλάσουν πληροφορίες για προβλήματα ασφαλείας και δραστικά αλλάζουν και προσαρμόζονται σαν αντίδραση απειλών εναντίον της ασφάλειας

1.11.3 Προγραμματισμός ιστοσελίδων και γλώσσες κειμένου (scripting languages)

Το να «κατεβάσεις» ενδιαφέρον ,πληροφοριακό και ψυχαγωγικό περιεχόμενο από τις σελίδες κόμβων του διαδικτύου ,τοπικά στον υπολογιστή είναι μία κύρια ενέργεια του net surfing .Το περιεχόμενο που έχει ενδιαφέρον από τη πλευρά της ασφάλειας έχει να κάνει με το «κατέβασμα»κώδικα που εκτελείται τοπικά .Το εκτελέσιμο περιεχόμενο μπορεί να παρέχει την αναμετάδοση μίας συνάντησης ,μουσική ,τρισδιάστατα γραφικά ή επικίνδυνο κώδικα που μπορεί να διαγράψει τα περιεχόμενα του δίσκου από τον

σταθμό εργασίας .Ο κώδικας είναι γραμμένος σε JAVA ή ActiveX και ονομάζεται applet(JAVA) ή Control Panel(ActiveX).

Οι γλώσσες προγραμματισμού για web,εισάγουν νέα προβλήματα στην ασφάλεια του διαδικτύου ,γιατί «κατεβαίνουν» ,αποθηκεύονται και εκτελούνται χωρίς να ελέγξεις το source code .Αυτό γίνεται απλά «σερφάροντας» στο διαδίκτυο ,χωρίς πολλές φορές ο χρήστης να αντιλαμβάνεται το γεγονός .Η JAVA έχει εσωτερικούς μηχανισμούς ασφάλειας ,αλλά οι ειδικοί στην ασφάλεια γνωρίζουν πώς να τους ξεπερνούν .Ο μηχανισμός για την εξασφάλιση του κώδικα είναι η κρυπτογράφηση του checksum του κώδικα και η πιστοποίηση του από τον κατασκευαστή .Πάντως τα επόμενα χρόνια το πρόβλημα αυτό θα ενταθεί και ο μόνος εμφανής τρόπος προφύλαξης είναι η κρυπτογράφηση και η ετοιμότητα των χρηστών .

1.11.4 Νοήμονες αυτόματοι μεσάζοντες

(Intelligent Autonomous Agents) –
Ένας νέος τρόπος υπολογιστικής συμπεριφοράς

Το μελλοντικό περιβάλλον του διαδικτύου θα εξαρτάται κύρια από το μοντέλο επεξεργασίας των ΄μεσαζόντων΄ ,με σημαντηκές επιπτώσεις στην ασφάλεια .Οι μεσάζοντες είναι εκτελέσιμα τμήματα λογισμικού ,που δεν εξαρτώνται από το λειτουργικό σύστημα ,τους πόρους το υλικό ή την γεωγραφική κατανομή του εξοπλισμού για να εκτελεστούν .Οι μεσάζοντες εκτελούν τους υπολογισμούς και κάνουν τις επικοινωνίες που ένας χρήστης του έχει ορίσει ,αλλά το περιβάλλον εκτέλεσης του κώδικα είναι έξω από το περιβάλλον που διαχειρίζεται ο χρήστης .Η βασική θεωρία γύρο από τους νοήμονες αυτόματους μεσάζοντες είναι η ακόλουθη :ο μεσάζοντας ,με την εντολή του χρήστη ,προωθείται σε ένα ή περισσότερους απομακρυσμένους κόμβους εκτελεί έναν υπολογισμό ή συγκεντρώνει πληροφορίες και επιστρέφει με ταποτελέσματα στον χρήστη .Ο τρόπος λειτουργίας του μεσάζοντα μπορεί να είναι από μερικώς ως τελείως αυτόνομος και ο βαθμός της αυτονομίας μπορεί να διαρκεί για όλο το διάστημα που υπάρχει .

Ένα μελλοντικό υπολογιστικό περιβάλλον βασισμένο σε μεσάζοντες μπορεί να έχει τα ακόλουθα χαρακτηριστικά :

- Οι μεσάζοντες μοιράζονται πληροφορίες και συνεργάζονται για να ολοκληρώσουν το έργο του χρήστη
- Οι μεσάζοντες προφυλάσσονται με εγγενείς μηχανισμούς προστασίας αλλά και από ορισμένα εξωτερικά στοιχεία ασφαλείας που παρέχονται από την υποδομή και άλλους μεσάζοντες
- Από την στιγμή που η δράση του μεσάζοντα είναι κύρια έξω από το περιβάλλον της υποδομής του χρήστη ,σε άλλα sites (και άρα έξω από κάθε firewall που σχεδιάστηκε για να προστατεύει τον χρήστη), τα παραδοσιακά firewalls δεν έχουν να προσφέρουν κάτι στην ασφάλεια
- Η αναπαραγωγή και η ποικιλία των μεσαζόντων παρέχει αυξημένη ικανότητα επιβίωσης όταν το σύστημα που βρίσκονται δέχεται επίθεση ή δεν έχει την υποστήριξη που χρειάζεται από τους πόρους του συστήματος
- Οι μεσάζοντες επικοινωνούν για να ενισχύσουν την ικανότητα ανίχνευσης παραβιάσεων .Ειδικευμένοι μεσάζοντες-αισθητήρες ,είναι σχεδιασμένοι να ανιχνεύουν συγκεκριμένους τύπους απειλών και ομάδες διαφορετικών μεσαζόντων παρέχουν στην «κοινωνία» των μεσαζόντων μια πλήρη εικόνα των τρεχουσών απειλών
- Η υποδομή που υποστηρίζεται από μεσάζοντες αυτοπροστατεύεται και ενεργεί για την άμυνα χωρίς την παρέμβαση του χρήστη .

ΚΕΦΑΛΑΙΟ 2 :

ΜΟΝΤΕΛΑ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ:

1. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

2.1 ΕΙΣΑΓΩΓΗ

Ένα ασφαλές σύστημα οπωσδήποτε πρέπει, με κάποιον τρόπο, να γνωρίζει ποιοι ζητούν και χρησιμοποιούν τις υπηρεσίες του. Για να γίνει αυτό, πρέπει να υπάρχει κάποιος τρόπος διαχωρισμού των χρηστών και εξακρίβωσης, κατά το δυνατόν χωρίς αμφιβολία, της ταυτότητάς τους. Η εξακρίβωση αυτή συνήθως ακολουθεί δύο στάδια: το στάδιο της ταυτοποίησης, δηλαδή της διαδικασίας αναγνώρισης της ταυτότητας του χρήστη, και το στάδιο της αυθεντικοποίησης, δηλαδή της διαδικασίας επαλήθευσης της ταυτότητάς του.

Μια από τις πιο σοβαρές επιθέσεις εναντίον πληροφοριακών συστημάτων είναι η αντιποίηση ταυτότητας, κατά την οποία κάποιος χρήστης κατορθώνει να πείσει το σύστημα ότι είναι κάποιος άλλος. Ο σκοπός είναι να χρησιμοποιήσει πόρους του συστήματος που με την πραγματική του ταυτότητα δεν είναι εξουσιοδοτημένος να προσπελάσει και, επίσης, να παραπλανήσει το σύστημα καταγραφής συμβάντων (log system) στο ίχνος ελέγχου (audit trail) του συστήματος. Συμπεραίνουμε, λοιπόν, ότι υπάρχουν δύο σημαντικοί λόγοι που επιβάλλουν την εξακρίβωση της ταυτότητας ενός χρήστη: Ο πρώτος είναι ότι η ταυτότητα του χρήστη είναι παράμετρος σε αποφάσεις ελέγχου προσπέλασης και ο δεύτερος ότι η ταυτότητα του χρήστη καταγράφεται από το μηχανισμό καταγραφής συμβάντων στο ίχνος ελέγχου.

Σε πολλές καταστάσεις της καθημερινής ζωής συχνά ζητείται εξακρίβωση της ταυτότητας ανθρώπων. Οι τραπεζικοί υπάλληλοι συνήθως ζητούν την ταυτότητα του

πελάτη πριν εξαργυρώσουν μια επιταγή, ενώ οι βιβλιοθηκάριοι μιας πανεπιστημιακής βιβλιοθήκης κανονικά πρέπει να ζητήσουν τη φοιτητική ταυτότητα κάποιου πριν του δανείσουν κάποιο βιβλίο. Τα πανεπιστήμια δεν αποκαλύπτουν βαθμούς από το τηλέφωνο, επειδή οι υπάλληλοι της γραμματείας δεν μπορούν να γνωρίζουν αν τους καλεί ο ίδιος ο φοιτητής. Ωστόσο, ο καθηγητής, που πιθανόν γνωρίζει τη φωνή του φοιτητή του, μπορεί να του πει το βαθμό του τηλεφωνικά. Οι άνθρωποι, λοιπόν, έχουν αναπτύξει συστήματα εξακρίβωσης ταυτότητας βασισμένα σε έγγραφα, σε αναγνώριση φωνής ή άλλα έμπιστα μέσα.

Προφανώς με τους υπολογιστές τα πράγματα είναι αρκετά διαφορετικά και σίγουρα λιγότερο ασφαλή. Οποιοσδήποτε μπορεί να προσπαθήσει να συνδεθεί με ένα υπολογιστικό σύστημα και, σε αντίθεση με τον καθηγητή που αναγνωρίζει τη φωνή του φοιτητή του, ο υπολογιστής δεν είναι δυνατόν να διακρίνει αν τα ηλεκτρικά σήματα που δέχεται παράγονται από τον Α ή από κάποιο άλλο πρόσωπο που ισχυρίζεται πως είναι ο Α.

Η πρώτη γραμμή άμυνας ενός οποιουδήποτε υπολογιστικού συστήματος είναι το σύστημα εξακρίβωσης ταυτότητας χρηστών που χρησιμοποιεί. Συνήθως η γραμμή

αυτή άμυνας είναι και η πιο ισχυρή, αν δεν είναι (σε μη ασφαλή συστήματα) και η μοναδική. Είναι, λοιπόν, φανερή η μεγάλη σημασία της.

Το κεφάλαιο αυτό είναι οργανωμένο σε δύο ενότητες, από τις οποίες η πρώτη αναφέρεται γενικά στην εξακρίβωση ταυτότητας χρηστών, ενώ η δεύτερη αναφέρεται σε έκταση στον πιο συνηθισμένο μηχανισμό αυθεντικοποίησης υπολογιστικών συστημάτων: στα συνθηματικά.

2.1.1 ΕΞΑΚΡΙΒΩΣΗ ΤΑΥΤΟΤΗΤΑΣ

Από την πρώτη στιγμή που το ανθρώπινο είδος συγκρότησε οργανωμένες κοινωνίες κάποιου μεγέθους δημιουργήθηκε η ανάγκη για διαφοροποίηση και αναγνώριση της ταυτότητας των ατόμων της ομάδας. Το πρόβλημα αρχικά λύθηκε με τη χρήση (μικρών, βαφτιστικών) ονομάτων, αλλά, καθώς οι πληθυσμοί άρχισαν να γίνονται μεγαλύτεροι, το ένα όνομα έπαψε να έχει τη δυνατότητα να είναι μοναδικό χαρακτηριστικό κάποιου ατόμου. Τότε άρχισαν να χρησιμοποιούνται και άλλα, επιπρόσθετα, ονόματα, όπως το πατρώνυμο, ο τόπος καταγωγής και –πολύ αργότερα– το επώνυμο ως στοιχεία ταυτοποίησης ατόμων.

Οποιοσδήποτε μπορεί να ισχυριστεί ότι η ταυτότητά του είναι διαφορετική από την πραγματική, ιδιαίτερα αν ο αποδέκτης του ισχυρισμού δεν είχε προηγούμενη γνωριμία με τον ταυτοποιούμενο. Αν ο βιβλιοθηκάριος γνωρίζει εξ όψεως το φοιτητή που ζητάει να δανειστεί κάποιο βιβλίο, είναι δυνατόν να αρκεστεί σ' αυτή τη γνώση και να μη ζητήσει να δει τη φοιτητική του ταυτότητα, η οποία και θα αποδείξει τον ισχυρισμό του. Η πιο συνηθισμένη όμως περίπτωση είναι, μετά την ταυτοποίηση, να ζητείται και αυθεντικοποίηση, δηλαδή απόδειξη της ταυτότητας.

Στην ενότητα αυτή θα ασχοληθούμε με το πώς μπορούμε να πετύχουμε την ταυτοποίηση και την αυθεντικοποίηση ατόμων σε υπολογιστικά συστήματα.

2.1.2 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Έλεγχος πρόσβασης

Ο όρος παραπέμπει σε ένα σύνολο λογικών ή φυσικών μηχανισμών ασφάλειας που σχεδιάζονται-εφαρμόζονται για να προστατέψουν από τη μη εξουσιοδοτημένη πρόσβαση (π.χ. είσοδος στο σύστημα, ανάγνωση, εγγραφή, είσοδος στο δίκτυο, κ.α.), στους πόρους-αγαθά του συστήματος.

Κατηγορία Ελέγχου	Πρόληψη	Ανίχνευση	Αντιμετώπιση
Φυσικής πρόσβασης (παραδείγματα			
Φράχτες	**X**		**X**
Προσωπικό Ασφαλείας	**X**	**X**	**X**
Έξυπνες Κάρτες (smartcards)	**X**		
Διαχειριστικός (παραδείγματα)			
Πολιτικές Ασφάλειας	**X**	**X**	**X**
Έλεγχος και Εποπτεία	**X**	**X**	
Εκπαίδευση υπαλλήλων	**X**	**X**	**X**
Λογικής Πρόσβασης (παραδείγματα)			
Λίστες Ελέγχου Πρόσβασης (ACLs), MAC, RBAC,…	**X**		
Λογισμικό Antivirus, Anti-Spyware,..	**X**	**X**	**X**
Κρυπτογράφηση Δεδομένων και Επικοινωνιών	**X**		
Firewalls (Packet Filters, Application Gateways)	**X**	**X**	
Συστήματα Ανίχνευσης & Αποτροπής Εισβολών (IDS/IPS)	**X**	**X**	**X**

Ο όρος «έλεγχος πρόσβασης», συχνά χρησιμοποιείται για να περιγράψει ένα σύνολο διαδικασιών στο οποίο συμμετέχουν άνθρωποι, ηλεκτρονικές διατάξεις, προγράμματα, και άλλος ηλεκτρονικός ή μη εξοπλισμός, με σκοπό:

α) Ο εξουσιοδοτημένος χρήστης να έχει πρόσβαση στο σύστημα
β) Οι μη εξουσιοδοτημένοι χρήστες να μην έχουν πρόσβαση στο σύστημα.

Το αντιστάθμισμα (trade-off) μεταξύ ασφάλειας και λειτουργικότητας καθιστά σαφές, πως,

1. Η υιοθέτηση πολύπλοκων και εξεζητημένων μέτρων ασφαλείας επιτυγχάνει το στόχο Β, αλλά δυσχεραίνει την υλοποίηση του στόχου Α,
2. Η υιοθέτηση «χαλαρών» μέτρων ασφάλειας επιτυγχάνει το στόχο Α, ωστόσο καθιστά δύσκολη και επίφοβη την υλοποίηση του στόχου Β.

Ταυτοποιήση ένος χρήστη

Υπάρχουν πολλές μέθοδοι αναγνώρισης της ταυτότητας ενός ατόμου. Για το σκοπό αυτό μπορεί να χρησιμοποιηθεί:

- Η εμφάνιση, δηλαδή το ύψος, το βάρος, το φύλο, η όψη.
- Η κοινωνική συμπεριφορά, δηλαδή ο τρόπος αλληλεπίδρασης με τους άλλους.
- Το όνομα.
- Κάποιος κωδικός, όπως, π.χ., ένας αριθμός μητρώου.
- Η γνώση που έχει το άτομο σχετικά με κάτι.
- Η κατοχή κάποιου αντικειμένου.
- Η βιοδυναμική, δηλαδή πώς εκτελεί κάτι το άτομο.
- Η φυσιολογία του, όπως αυτή προκύπτει από –για παράδειγμα– τα χαρακτηριστικά του.
- Ξένα επιβληθέντα χαρακτηριστικά, όπως, π.χ., βραχιόλια, ταυτότητες κτλ.

Όλοι οι παραπάνω τρόποι χρησιμοποιούνται σήμερα στην καθημερινή ζωή, όπως και διάφοροι συνδυασμοί τους. Ωστόσο, ο συντριπτικά πιο διαδεδομένος τρόπος ταυτοποίησης ατόμων από υπολογιστικά συστήματα είναι με τη χρήση κάποιου κωδικού, που συνήθως αναφέρεται ως όνομα χρήστη (username).

Αυθεντικοποιήση

Υπάρχουν τέσσερις μέθοδοι για να αποδείξει κάποιος την ταυτότητά του:

- Με κάτι που ξέρει.
- Με κάτι που έχει.
- Με κάτι που αποτελεί μοναδικό ατομικό χαρακτηριστικό του.

Η πρώτη μέθοδος είναι ίσως και η ευκολότερη για χρήση όταν στη διαδικασία αυθεντικοποίησης εμπλέκονται μηχανές. Παραδείγματα σχετικών μέσων αυθεντικοποίησης είναι τα συνθηματικά, τα PINs (Personal Identification Numbers), οι συνθηματικές φράσεις, και πληροφορίες σχετικές με το άτομο ή την οικογένεια κάποιου που δεν είναι ευρέως γνωστές.

Τα πλεονεκτήματα της μεθόδου αυτής είναι:

• Το μέσο αυθεντικοποίησης είναι πάντα στην κατοχή του χρήστη.
• Το μέσο αυθεντικοποίησης μπορεί να αλλάξει εύκολα.
• Η προστασία του μέσου αυθεντικοποίησης είναι σχετικά εύκολη.

Το μέσο αυθεντικοποίησης εισάγεται εύκολα στο μηχανισμό αυθεντικοποίησης μέσω πληκτρολογίου, χωρίς να υπάρχει ανάγκη προσθήκης εξειδικευμένου υλικού.

Ωστόσο, η μέθοδος έχει και μειονεκτήματα. Το βασικότερο είναι ότι η φιλοσοφία της στηρίζεται στο ότι ο αυθεντικοποιούμενος γνωρίζει κάτι, κάτι που βέβαια μπορεί να ξεχαστεί, να αντιγραφεί ή ακόμη και να εικαστεί από κάποιον άλλο, μη εξουσιοδοτημένο να το κάνει. Σε πολλές περιπτώσεις χρήσης τέτοιου μηχανισμού δεν είναι ιδιαίτερα δύσκολο για κάποιον επιτιθέμενονα μάθει το μέσο αυθεντικοποίησης, απλώς παρακολουθώντας τον εξουσιοδοτημένο χρήστη να το εισάγει στο σύστημα. Επιπλέον, δεν απαιτούνται ειδικά εργαλεία, γνώσεις ή μέθοδοι για να αντιγράψει κανείς το μέσο αυθεντικοποίησης. Παρ' όλο, λοιπόν, που η μέθοδος αυτή είναι σε ευρύτατη χρήση σήμερα σε υπολογιστές, αυτόματες τραπεζικές μηχανές, τηλεφωνικές κάρτες κτλ., εκτιμάται ως ατελής.

Η δεύτερη μέθοδος δεν είναι τόσο επιρρεπής σε αντιγραφή όσο η πρώτη. Η μέθοδος αυτή βασίζεται στην κατοχή από τον αυθεντικοποιούμενο ενός αντικειμένου, π.χ. μιας κάρτας (απλής, μαγνητικής, έξυπνης), ενός κλειδιού ή μιας γεννήτριας πρόκλησης απάντησης. Είναι φανερό ότι ο ιδιοκτήτης των αντικειμένων αυτών πρέπει να καταβάλει προσπάθεια να τα προστατεύσει από κλοπή η απώλεια. Ακριβώς αυτά τα δύο προβλήματα είναι και τα βασικά μειονεκτήματα αυτής της μεθόδου αυθεντικοποίησης.

Από την άλλη πλευρά, τέτοια αντικείμενα δεν είναι εύκολο να αντιγραφούν, χωρίς ωστόσο να είναι και εντελώς αδύνατη η αντιγραφή τους. Για να αποφύγουμε εκτεταμένο κίνδυνο αντιγραφής, θα πρέπει το κόστος της να είναι αρκετά μεγαλύτερο από το αναμενόμενο όφελος. Αν και η πρακτική αυτή αποτρέπει τον ευκαιριακό επιτιθέμενο, δεν αποτελεί ωστόσο σοβαρό εμπόδιο για τον αποφασισμένο.

Η τρίτη μέθοδος βασίζεται στην αναγνώριση και επαλήθευση ατομικών χαρακτηριστικών του αυθεντικοποιούμενου. Χαρακτηριστικά που έχουν κατά καιρούς προταθεί ως πιθανά για τέτοια χρήση κατηγοριοποιούνται σε φυσιολογικά (ή ανθρωπομετρικά) χαρακτηριστικά και σε χαρακτηριστικά συμπεριφοράς.

Τα ανθρωπομετρικά χαρακτηριστικά που έχουν χρησιμοποιηθεί περιλαμβάνουν:

• Δακτυλικό αποτύπωμα.
• Ίριδα.
• Φυσιογνωμία προσώπου.
• Γεωμετρία χειρός – φλεβικά πρότυπα.
• Αμφιβληστροειδής χιτώνας.
• Δομή DNA.
• Κατανομή ιδρωτοποιών πόρων στο δάκτυλο.
• Σχήμα και μέγεθος αυτιών.
• Οσμή.
• Ηλεκτρική αγωγιμότητα σώματος.

Ενώ τα χαρακτηριστικά συμπεριφοράς που έχουν χρησιμοποιηθεί περιλαμβάνουν:
• Χαρακτηριστικά χειρόγραφης υπογραφής.
• Χαρακτηριστικά φωνής.
• Χαρακτηριστικά τρόπου πληκτρολόγησης.

Η μέθοδος αυτή είναι πολύ αποτελεσματικότερη από τις άλλες δύο και πλησιάζει περισσότερο στον ανθρώπινο τρόπο της επαλήθευσης της ταυτότητας κάποιου. Ωστόσο, έχει το μειονέκτημα ότι απαιτεί ειδικό εξοπλισμό, ο οποίος μάλιστα κοστίζει πολύ, ενώ επίσης υποβάλλει τους χρήστες σε ελέγχους που μπορεί να μην είναι εύκολα αποδεκτοί.

2.2 ΤΑΥΤΟΠΟΙΗΣΗ ΜΕ ΚΩΔΙΚΟΥΣ ΠΡΟΣΒΑΣΗΣ

Η επαλήθευση ταυτότητας με τη χρήση κωδικών πρόσβασης αποτελεί την πλέον δημοφιλή μέθοδο ταυτοποίησης. Τα παραδείγματα είναι πολλά:

• Πρόσβαση σε Η/Υ (π.χ. log-on στα Windows, Unix,..): Χρήση ενός ονόματος χρήστη (username) και ενός κωδικού για την πρόσβαση στον Η/Υ
• Πρόσβαση στον server του δικτύου (π.χ. Domain Server, Unix server): Χρήση ενός ονόματος χρήστη και ενός κωδικού για την πρόσβαση στο χώρο του δίσκου που έχει εκχωρηθεί στον χρήστη από τον server.
• Πρόσβαση στον mail server για την αποστολή, λήψη και διαχείριση e-mail:

Χρήση ενός ονόματος χρήστη και ενός κωδικού για την πρόσβαση στην ταχυδρομική θυρίδα του διακομιστή εισερχόμενης αλληλογραφίας (incoming mail server) ή για την αποστολή e-mail μέσω του διακομιστή εξερχόμενης αλληλογραφίας (outgoing mail server).

• Πρόσβαση στην κάρτα SIM του κινητού τηλεφώνου, στην κάρτα ανάληψης (ATM): Χρήση ενός αριθμού PIN (Personal Identification Number).

Κατά πάσα πιθανότητα, η πρώτη επαφή που είχατε με την ασφάλεια υπολογιστών ήταν όταν προσπαθήσατε να συνδεθείτε με έναν υπολογιστή, ο οποίος σας ζήτησε να του δώσετε το όνομα χρήστη και το συνθηματικό σας. Τώρα ξέρετε ήδη ότι το πρώτο βήμα (δηλαδή η αίτηση για το όνομα χρήστη) στοχεύει στην αναγνώριση της ταυτότητάς σας, όπου ανακοινώνετε ποιος είστε. Το δεύτερο βήμα (δηλαδή η αίτηση για το συνθηματικό) στοχεύει στην επαλήθευση της ταυτότητάς σας, όπου αποδεικνύετε ότι είστε αυτός που ισχυρίζεστε πως είστε.

Αφού δώσετε το όνομα χρήστη και το συνθηματικό σας, ο υπολογιστής θα τα συγκρίνει με τις εγγραφές ενός αρχείου συνθηματικών. Η σύνδεση θα πετύχει αν δώσετε ένα έγκυρο όνομα χρήστη και το αντίστοιχο, επίσης έγκυρο, συνθηματικό. Αν, όμως, είτε το όνομα χρήστη είτε το συνθηματικό είναι λανθασμένα, η απόπειρα σύνδεσης θα αποτύχει. Συνήθως σε μια τέτοια περίπτωση η οθόνη θα καθαριστεί και θα σας ζητηθεί να ξαναπροσπαθήσετε. Ωστόσο, κάποια συστήματα μετρούν τις αποτυχημένες προσπάθειες σύνδεσης για κάθε χρήστη και κλειδώνουν τον αντίστοιχο λογαριασμό όταν το πλήθος των αποτυχημένων προσπαθειών ξεπεράσει κάποιο προκαθορισμένο όριο. Κάποια άλλα συστήματα μπορεί και να μην επιτρέψουν, με μικρή πιθανότητα, τη σύνδεση στο χρήστη, ακόμη και αν το ζεύγος (όνομα χρήστη, συνθηματικό) που εισήχθη ήταν έγκυρο.

Για να ελαττωθεί η πιθανότητα κάποιος επιτιθέμενος να χρησιμοποιήσει ένα τερματικό ή υπολογιστή που έχει αφεθεί χωρίς επιτήρηση ενώ κάποιος χρήστης παραμένει συνδεμένος, η επαλήθευση ταυτότητας μπορεί να γίνεται όχι μόνο στην αρχή της συνόδου, αλλά και σε διαστήματα κατά τη διάρκεια της συνόδου. Μπορεί, επίσης, να κλειδώνει η οθόνη όσο δε χρησιμοποιείται ή να τερματίζεται μια σύνοδος αν δεν υπάρξει επικοινωνία για κάποιο διάστημα.

Κάποτε δίναμε το όνομα χρήστη και το συνθηματικό σε απάντηση μιας οθόνης που περιείχε ένα φιλικό καλωσόρισμα και πληροφορίες για το σύστημα στο οποίο προσπαθούσαμε να συνδεθούμε. Σήμερα, ως άλλο σημάδι των καιρών, το φιλικό καλωσόρισμα έχει αντικατασταθεί με ένα μήνυμα που προειδοποιεί τους μη εξουσιοδοτημένους χρήστες να μην επιχειρήσουν πρόσβαση. Όλοι οι χρήστες πρέπει να δηλώσουν ότι διάβασαν το μήνυμα αυτό πριν τους επιτραπεί να επιχειρήσουν να συνδεθούν με το σύστημα.

Τα περισσότερα σύγχρονα υπολογιστικά συστήματα χρησιμοποιούν την ταυτοποίηση και αυθεντικοποίηση – μέσω ονομάτων χρηστών και συνθηματικών– ως την πρώτη γραμμή άμυνάς τους. Για τους περισσότερους χρήστες, οι μηχανισμοί αυτοί αποτελούν αναπόσπαστο τμήμα της διαδικασίας σύνδεσης με το σύστημα. Έχουμε, λοιπόν, εδώ ένα μηχανισμό που είναι ευρύτατα αποδεκτός και σχετικά εύκολος στην υλοποίησή του. Από την άλλη μεριά, η πρόσκτηση ενός έγκυρου ζεύγους ονόματος χρήστη και συνθηματικού είναι ένας κοινότατος τρόπος επίτευξης μη εξουσιοδοτημένης πρόσβασης σε ένα υπολογιστικό σύστημα. Έχει ενδιαφέρον, λοιπόν, να εξετάσουμε την πραγματική ασφάλεια των συνθηματικών ως μηχανισμού αυθεντικοποίησης. Θα το κάνουμε αυτό αναπτύσσοντας τις απειλές εναντίον συνθηματικών. Οι τρεις ποιο σημαντικές είναι:

- Εικασία συνθηματικού
- Υποκλοπή συνθηματικού
- Παραβίαση αρχείου συνθηματικών

Μη ξεχνάτε ότι ο χρήστης παίζει ένα σημαντικό ρόλο στην προστασία των συνθηματικών. Η αυθεντικοποίηση αποτυγχάνει όταν δίνετε σε άλλους το συνθηματικό σας, είτε λέγοντάς το σε κάποιον είτε γράφοντας το κάπου και αφήνοντας το σημείωμα κολλημένο πάνω στον υπολογιστή ή μέσα στο ξεκλείδωτο συρτάρι του γραφείου σας.

2.2.1 ΑΠΕΙΛΕΣ

1. <u>Το πρόβλημα με τους κωδικούς πρόσβασης</u>.

Συχνά τίθεται το εξής ερώτημα: «Πώς θα επιτύχουμε την εύρεση ενός κωδικού πρόσβασης που θα είναι α) δύσκολο να παραβιαστεί από κάποιον τρίτο (επομένως, αρκετά τυχαίος – random), και ταυτόχρονα β) αρκετά εύκολος ώστε να τον θυμόμαστε; Αρχικά, οι δύο αυτές απαιτήσεις φαντάζουν ως αντιφατικές.

2. <u>Πώς θυμάται ο χρήστης τον κωδικό πρόσβασης;</u>

- Ένας «δύσκολος» κωδικός που χρησιμοποιείται συχνά είναι εύκολο να απομνημονευτεί
- Ένας «εύκολος» κωδικός που χρησιμοποιείται σπάνια είναι δύσκολο να

απομνημονευτεί

- Λάθος τακτική: επιλογή ενός «δύσκολου» κωδικού, και στη συνέχεια χρήση του σε περισσότερα του ενός περιβάλλοντα (δικτυακοί τόποι, συστήματα ελέγχου πρόσβασης, πρόσβασης σε Η/Υ κλπ).

Η χρήση κωδικών πρόσβασης, παρά τις αδυναμίες της, αποτελεί τον πλέον δημοφιλή τρόπο ταυτοποίησης για συστήματα που απαιτούν χαμηλό έως μέσο
επίπεδο ασφάλειας.

Ο χρήστης μπορεί να «χάσει» την αποκλειστικότητα του κωδικού του πρόσβασης όταν:

• Χρησιμοποιεί τον ίδιο κωδικό σε πολλά συστήματα
• Αποκαλύψει τον κωδικό του σε κάποιον τρίτο (για διευκόλυνση – π.χ. «θέλω να δω κάτι στον υπολογιστή σου», τυχαία – π.χ. «σε είδα την ώρα που πληκτρολογούσες το PIN σου», ή ως αποτέλεσμα παραπλάνησης – τεχνικές phishing).

Όσο πιο «δύσκολος» είναι ο κωδικός πρόσβασης, τόσο πιο υψηλή είναι η πιθανότητα:

- Να ξεχαστεί
- Να σημειώσει ο χρήστης τον κωδικό του σε ένα χαρτί.

Όσο πιο «εύκολος» είναι ο κωδικός πρόσβασης τόσο πιο εύκολη είναι η απομνημόνευση του, επομένως τόσο πιο υψηλή είναι η πιθανότητα:

- Κάποιος τρίτος να «σπάσει» τον κωδικό χρησιμοποιώντας εξειδικευμένα εργαλεία
- Κάποιος τρίτος να υποθέσει τον κωδικό, αξιοποιώντας προσωπικές ή άλλες πληροφορίες που γνωρίζει για τον χρήστη.

Η μελέτη αυτή περίπτωσης καταδεικνύει πως: το ποσοστό όσων εξαπατώνται από
επιθέσεις τύπου phishing είναι αρκετά υψηλό. Σήμερα, το ποσοστό αυτό είναι σαφώς μικρότερο. Ωστόσο, αν υποθέσουμε π.χ. ένα ποσοστό εξαπάτησης. 1/1000, και το ίδιο mail φθάσει σε 1.000.000 ανθρώπους, τότε κατά μέσο όρο θα εξαπατηθούν 1000 άνθρωποι. Επίσης, λόγω της υψηλής διείσδυσης του Internet, ένα μεγάλο ποσοστό των ανθρώπων που λαμβάνουν τέτοιου είδους αλληλογραφία δεν είναι ενημερωμένοι σχετικά με τους κινδύνους που ελλοχεύουν (security awareness).

Το γεγονός αυτό αυξάνει τις πιθανότητες εξαπάτησης. Το πρόβλημα της απομνημόνευσης των κωδικών πρόσβασης δεν περιορίζεται στην πρόσβαση σε Ηλεκτρονικούς Υπολογιστές. Καθημερινά χρησιμοποιούμε συσκευές που απαιτούν τη χρήση ενός συνθηματικού πρόσβασης (π.χ. PIN σε κινητά τηλέφωνα, συσκευές ATM κ.λ.π).

3. <u>Λάθη στη σχεδίαση (design errors).</u>

Ένα σύνηθες λάθος είναι η χρήση μιας ή περισσότερων προσωπικών πληροφοριών ως κωδικών πρόσβασης. Η χρήση τέτοιων συνθηματικών, ναι μεν είναι αποδεκτή σε συστήματα που απαιτούν χαμηλό επίπεδο ασφάλειας (π.χ. ερώτηση για τον υπολειπόμενο χρόνο ομιλίας στο τμήμα Εξυπηρέτησης Πελατών του Παρόχου Κινητής Τηλεφωνίας), δε συμβαίνει όμως το ίδιο σε συστήματα μέσου και υψηλού επιπέδου ασφαλείας. Σε αυτές τις περιπτώσεις, το σύστημα θα πρέπει να ελέγχει την εγκυρότητα των κωδικών που επιλέγονται ώστε να αποφεύγονται παρόμοιες καταστάσεις.

4. <u>Λάθη χρηστών</u>.

Κατά τη διαχείριση πολλών συσκευών ή προγραμμάτων απαιτείται η εισαγωγή κωδικού πρόσβασης. Κατά την πρώτη σύνδεση ενδέχεται να υπάρχει προεγκατεστημένος ένας αρχικός (default) κωδικός, ο οποίος α) είναι εύκολος στην απομνημόνευση, και β) συνήθως είναι ο ίδιος για όλα τα προϊόντα της εταιρίας. Συχνά οι χρήστες αμελούν ή αποφεύγουν να αλλάξουν τους αρχικούς κωδικούς. Σε αυτήν την περίπτωση, οι κίνδυνοι είναι προφανείς, π.χ. απομακρυσμένη διαχείριση
router, πρόσβαση dial-up, πρόσβαση στο voice mail, κ.α.. Το μοντέλο απειλών καθορίζει και την πολιτική ασφάλειας που πρέπει να ακολουθηθεί:

- Απειλή 1. Επίθεση σε έναν (συγκεκριμένο) λογαριασμό**.** Οι επιθέσεις τέτοιου τύπου είναι απόλυτα στοχευμένες. Ο στόχος είναι ένα συγκεκριμένο μηχάνημα ή χρήστης.
- Απειλή 2. Επίθεση σε οποιονδήποτε λογαριασμό του συστήματος. Ο στόχος του εισβολέα είναι η είσοδος στο σύστημα με οποιονδήποτε τρόπο. Συνήθως, οι επιθέσεις τέτοιου τύπου είναι στοχευμένες (π.χ. στόχος: η Microsoft) και κλιμακωτές, όταν δηλαδή χρησιμοποιούνται ως προθάλαμος μιας γενικότερης επίθεσης στο σύστημα. (π.χ. «θέλω να συνδεθώ ως οποιοσδήποτε χρήστης στο microsoft.com, και στη συνέχεια να αποκτήσω δικαιώματα Διαχειριστή»). Σε πολλά συστήματα τα δικαιώματα πρόσβασης που εκχωρούνται στους εσωτερικούς χρήστες (insiders) του συστήματος είναι σημαντικά περισσότερα σε σχέση με αυτά που εκχωρούνται σε εξωτερικούς χρήστες (outsiders). Έτσι, το πιο σημαντικό (άρα, και το πιο δύσκολο) βήμα που έχει να διανύσει ο «εισβολέας» είναι η επιτυχής πρόσβαση σε κάποιον (οποιονδήποτε) λογαριασμό χρήστη του συστήματος (ακόμα και αν ο λογαριασμός αυτός έχει περιορισμένα δικαιώματα). Στη συνέχεια ο εισβολέας θα χρησιμοποιήσει έξυπνες τεχνικές-εργαλεία για να αυξήσει ακόμα περισσότερο τα δικαιώματα που του παρέχει το σύστημα.
- Απειλή 3. Επίθεση σε οποιονδήποτε λογαριασμό οποιουδήποτε συστήματος. Π.χ. για την αποθήκευση-διακίνηση παρανόμως διακινούμενου υλικού (λογισμικό, παιχνίδια, ταινίες κ.λ.π). Ο λογαριασμός αυτός μπορεί να χρησιμοποιηθεί αργότερα στα πλαίσια μιας επίθεσης DOS ή DDOS σε κάποιο άλλο σύστημα (π.χ. ως zombie σε δίκτυα BotNet).

Η ταξινομία αυτή είναι χρήσιμη γιατί μας βοηθάει να θέσουμε χρήσιμα ερωτήματα όταν επιλέγουμε ή σχεδιάζουμε ένα σύστημα ασφάλειας με κωδικούς πρόσβασης. Έτσι, αξιολογούνται οι εξής περιπτώσεις: α) όταν η επιλογή ενός «εύκολου» κωδικού από έναν χρήστη δυνητικά θα βλάψει μόνον το χρήστη και β) όταν η επιλογή ενός «εύκολου» κωδικού από έναν χρήστη δυνητικά βλάπτει άλλους χρήστες ή το πληροφοριακό σύστημα της Επιχείρησης/Οργανισμού. Στην δεύτερη περίπτωση, η πολιτική ασφάλειας της επιχείρησης πρέπει να τροποποιηθεί ώστε οι

χρήστες του συστήματος να υποχρεώνονται (στο βαθμό που αυτό είναι εφικτό) να επιλέξουν κωδικούς χαμηλής προβλεψιμότητας.

5. Εικασία συνθηματικών

Η επιλογή των συνθηματικών είναι ένα κρίσιμο ζήτημα για την ασφάλεια. Αν και

δεν είναι δυνατόν να αποτραπεί τελείως ένας επιτιθέμενος από το να εικάσει τυχαία ένα έγκυρο συνθηματικό, μπορούμε να προσπαθήσουμε να κρατήσουμε την πιθανότητα να συμβεί ένα τέτοιο γεγονός πολύ χαμηλή. Για να δούμε πώς, πρέπει να πούμε ότι οι επιτιθέμενοι χρησιμοποιούν κυρίως δύο τεχνικές όταν προσπαθούν να εικάσουν συνθηματικά:

- Εξαντλητική έρευνα (brute force): συνίσταται στη δοκιμή όλων των δυνατών συνδυασμών έγκυρων συμβόλων δεδομένου μήκους.(βλέπε παράρτημα,2)
- Έξυπνη έρευνα: συνίσταται στη δοκιμή συνδυασμών έγκυρων συμβόλων επιλεγμένων να ανήκουν σε κάποιον περιορισμένο χώρο έρευνας. Παραδείγματα αποτελούν η δοκιμή συνθηματικών που με κάποιον τρόπο σχετίζονται με το όνομα χρήστη, με ονόματα φίλων και συγγενών του χρήστη, με τη μάρκα αυτοκινήτου του χρήστη, με τον αριθμό κυκλοφορίας του αυτοκινήτου του χρήστη, με τον αριθμό τηλεφώνου του χρήστη, με τον τόπο καταγωγής του χρήστη ή η δοκιμή συνθηματικών που είναι γενικώς δημοφιλή. Τυπικό παράδειγμα μιας τέτοιας επίθεσης είναι η λεξικογραφική επίθεση, κατά την οποία δοκιμάζονται όλες οι λέξεις που περιέχονται σε κάποιο (ή σε περισσότερα από ένα) ηλεκτρονικό λεξικό.

Έχουμε άραγε μέσα άμυνας; Ευτυχώς ναι, μερικά από τα οποία μπορεί να φαίνονται προφανή, αλλά δυστυχώς δεν τηρούνται πάντα. Μπορούμε να κάνουμε τα εξής:

- Να βάλουμε συνθηματικό στο λογαριασμό μας. Αν ο διαχειριστής του συστήματος ή ο χρήστης ξεχάσει να καθορίσει συνχρήστη, ο επιτιθέμενος δε χρειάζεται καν να μπει στον κόπο να εικάσει το συνθηματικό.
- Να αλλάξουμε τα προκαθορισμένα συνθηματικά. Όταν παραδίδεται ένα σύστημα, συνήθως έχει προκαθορισμένους λογαριασμούς (π.χ. system), με προκαθορισμένα συνθηματικά (π.χ. manager). Η πρακτική αυτή βοηθάει τους μηχανικούς που κάνουν συνθηματικό για το λογαριασμό του την εγκατάσταση, αλλά, αν το συνθηματικό παραμείνει αναλλοίωτο, είναι εύκολη υπόθεση για τον επιτιθέμενο να αποκτήσει πρόσβαση στο σύστημα.

Στο συγκεκριμένο παράδειγμα, μάλιστα, ο επιτιθέμενος αποκτά πρόσβαση σε λογαριασμό με ιδιαίτερα προνόμια. Να καθορίσουμε ελάχιστο μήκος συνθηματικού, προκειμένου να αντιμετωπίσουμε επιθέσεις εξαντλητικής έρευνας. Δυστυχώς, πολλά συστήματα καθορίζουν και μέγιστο μήκος συνθηματικού, περιορίζοντας το μήκος των συνθηματικών σε οκτώ χαρακτήρες. Να καθορίσουμε μια μορφή συνθηματικού επιβάλλοντας συνθηματικά που περιέχουν μικρά και κεφαλαία γράμματα, αριθμητικούς και μη αλφαριθμητικούς χαρακτήρες.

Να αποφύγουμε τα προφανή συνθηματικά. Μην παραξενευτείτε αν διαπιστώσετε ότι οι επιτιθέμενοι είναι εφοδιασμένοι με λίστες δημοφιλών συνθηματικών και να ξέρετε ότι οι λεξικογραφικές επιθέσεις έχουν επεκτείνει πολύ την έννοια του προφανούς. Σήμερα μπορείτε να βρείτε ηλεκτρονικά λεξικά για σχεδόν όλες τις γλώσσες. Να καθορίσουμε, αν το σύστημά μας το επιτρέπει, ημερομηνία λήξης για κάθε συνθηματικό, αναγκάζοντας έτσι τους χρήστες να αλλάζουν συνθηματικά σε τακτά διαστήματα. Μπορούμε, επιπλέον, να έχουμε και μηχανισμούς που απαγορεύουν στους χρήστες να ξαναχρησιμοποιήσουν παλιά συνθηματικά, όπως, π.χ., μια λίστα των τελευταίων δέκα συνθηματικών. Φυσικά, οι αποφασιστικοί χρήστες μπορούν πάντα να επαναφέρουν το παλιό αγαπημένο τους συνθηματικό κάνοντας τον απαραίτητο αριθμό αλλαγών.

Να διαμορφώσουμε το σύστημά μας έτσι ώστε να παρακολουθεί τις αποτυχημένες απόπειρες σύνδεσης και να αντιδρά κλειδώνοντας τελείως ή για κάποιο χρόνο ένα λογαριασμό χρήστη αν το πλήθος τους ξεπεράσει κάποιο όριο, ώστε να αποτρέψει περαιτέρω απόπειρες. να διαμορφώσουμε το σύστημά μας έτσι ώστε, μετά από κάθε επιτυχημένη σύνδεση, να αναφέρει πότε έγινε η τελευταία επιτυχής σύνδεση και το πλήθος των αποτυχημένων προσπαθειών σύνδεσης από τότε, ώστε ο χρήστης να προειδοποιείται για πρόσφατες απόπειρες επίθεσης εναντίον του λογαριασμού του.

Από τα παραπάνω φαίνεται πόσο σημαντική είναι η σωστή επιλογή των συνθηματικών. Το ιδανικό συνθηματικό είναι πολύ δύσκολο να εικαστεί και εύκολο να απομνημονευτεί. Μετά απ' αυτά που είπαμε, φαίνεται ότι πετυχαίνουμε την καλύτερη ασφάλεια αν οι χρήστες διαλέγουν μακρά συνθηματικά, που περιέχουν μικρά και κεφαλαία γράμματα, αριθμούς και σύμβολα, τα οποία πιθανόν δημιουργούνται για λογαριασμό τους από το σύστημα και αλλάζουν τακτικά. Είναι όμως ρεαλιστική η προσέγγιση αυτή; Θα πετύχουμε έτσι στην πράξη το επιθυμητό επίπεδο ασφάλειας;

Μάλλον όχι. Κι αυτό γιατί είναι απίθανο οι χρήστες να καταφέρουν να απομνημονεύσουν πολύπλοκα συνθηματικά μεγάλου μήκους (ιδιαίτερα στην περίπτωση που έχουν συνθηματικά για τραπεζικούς λογαριασμούς, κ.τ.λ). Έτσι, είναι πολύ πιθανό να αναγκαστούν να καταγράψουν κάπου το συνθηματικό και να το φυλάξουν κοντά στο υπολογιστικό τους σύστημα, όπου μπορούν να το προσπελάσουν εύκολα, τόσο οι ίδιοι όσο και οι πιθανοί επιτιθέμενοι. Ένα από τα καθήκοντα των υπεύθυνων ασφάλειας είναι και το να ψάχνουν για χαρτάκια με συνθηματικά κολλημένα πάνω σε οθόνες τερματικών.

Από την άλλη μεριά, αν απαιτούμε τα συνθηματικά να αλλάζουν τακτικά και συχνά, είναι πολύ πιθανό οι χρήστες να τείνουν να χρησιμοποιούν ευκολομνημόνευτα συνθηματικά και κατά συνέπεια πιο εύκολα να τα εικάσει κάποιος. Μπορεί να επαναχρησιμοποιούν το αγαπημένο τους συνθηματικό ή να κάνουν προβλέψιμες αλλαγές στο συνθηματικό τους. Αν είσαι υποχρεωμένος να αλλάξεις το συνθηματικό σου κάθε μήνα, η πρόσθεση του μήνα (δύο ψηφία 1–12 ή τρεις χαρακτήρες JAN–DEC) στο συνθηματικό σου παράγει συνθηματικά τα οποία μπορείς να θυμάσαι εύκολα. Φυσικά, ο επιτιθέμενος που βρήκε ένα από αυτά τα συνθηματικά μπορεί εύκολα να προβλέψει το επόμενο.

Υπάρχει και κάτι άλλο που πρέπει να σκεφτούμε: Υποθέστε ότι οι χρήστες του συστήματος παίρνουν όλοι την υπόθεση ασφάλειας πολύ σοβαρά, αποφεύγουν αδύναμα συνθηματικά που μπορούν να εικαστούν εύκολα, δεν καταγράφουν τα συνθηματικά τους, αλλά, αναπόφευκτα, πού και πού τα ξεχνούν. Αυτό θα τους εμποδίσει στην εργασία τους και θα τους αναγκάσει να ζητήσουν τη συνδρομή του διαχειριστή του συστήματος προκειμένου να αποκτήσουν καινούριο συνθηματικό και να μπορέσουν να συνδεθούν με το σύστημα. Η αναγκαστική αυτή ενέργεια θα διακόψει την εργασία του διαχειριστή και θα ανοίξει το δρόμο για μια νέα επίθεση: Αν ο χρήστης και ο διαχειριστής δεν μπορούν να συναντηθούν πρόσωπο με πρόσωπο,

μπορεί να πρέπει να συμφωνήσουν το νέο συνθηματικό τηλεφωνικά. Είναι σε θέση ο διαχειριστής να επαληθεύσει την ταυτότητα του χρήστη πλήρως; Η παραπλάνηση ενός διαχειριστή

συστήματος προκειμένου να αποκαλύψει τηλεφωνικά κάποιο συνθηματικό είναι παλιά, δοκιμασμένη και προσφιλής μέθοδος πολλών επιτιθέμενων.

Άλλωστε, οι επιτυχείς επιθέσεις τις περισσότερες φορές είναι μάλλον αποτέλεσμα καλής κοινωνικής μηχανικής παρά αυξημένης τεχνικής ικανότητας.Πέρα λοιπόν από τη σωστή εκπαίδευση των χρηστών και την παραίνεση να επιλέγουν συνθηματικά με κάποια επιθυμητά χαρακτηριστικά και να αποφεύγουν κάποια άλλα, μήπως το ίδιο το σύστημα μπορεί να βοηθήσει ώστε να βελτιωθεί ακόμη περισσότερο ή ασφάλεια των συνθηματικών;

Υπάρχουν τρεις βασικές τεχνικές που μπορούν να χρησιμοποιηθούν για να το πετύχουμε αυτό:

- Αυτόματη δημιουργία συνθηματικών από το σύστημα
- Προληπτικός έλεγχος συνθηματικών
- Κατασταλτικός έλεγχος συνθηματικών

Μη νομίσετε όμως ότι τα συνθηματικά που δημιουργούνται αυτόματα δεν έχουν και αυτά προβλήματα. Αν είναι αρκετά τυχαία, οι χρήστες δεν μπορούν να τα απομνημονεύσουν. Ακόμη και αν το συνθηματικό μοιάζει με πραγματική λέξη, ο χρήστης μπορεί να δυσκολεύεται να το απομνημονεύσει και συνεπώς μπαίνει στον πειρασμό να το καταγράψει κάπου. Γενικά, τα συστήματα αυτόματης δημιουργίας συνθηματικών δεν έχουν τύχει καλής αποδοχής από τους χρήστες.

Ο κατασταλτικός έλεγχος συνθηματικών συνίσταται στην περιοδική εκτέλεση από το ίδιο το σύστημα ενός προγράμματος διάρρηξης συνθηματικών με σκοπό τον εντοπισμό εύκολων να εικαστούν συνθηματικών. Το σύστημα ακυρώνει αμέσως όσα τέτοια συνθηματικά βρει και ενημερώνει τους αντίστοιχους χρήστες. Τα μειονεκτήματα της τακτικής αυτής είναι καταρχήν ότι απαιτεί πολλούς πόρους αν θέλουμε να γίνει σωστά και, επίσης, ότι στο μεσοδιάστημα μεταξύ των ελέγχων τα αδύναμα συνθηματικά παραμένουν ενεργά στο σύστημα.

Η πιο πολλά υποσχόμενη τακτική είναι αυτή του προληπτικού ελέγχου, κατά την οποία ο κάθε χρήστης επιλέγει το συνθηματικό του, το οποίο όμως υπόκειται σε έλεγχο καταλληλότητας κατά τη στιγμή της επιλογής του. Αν βρεθεί ακατάλληλο, ο χρήστης ειδοποιείται και του ζητείται να επιλέξει νέο. Η φιλοσοφία της τακτικής αυτής βασίζεται στην ιδέα ότι οι χρήστες, με την κατάλληλη υποβοήθηση από το σύστημα, μπορούν να επιλέξουν καλά συνθηματικά, τα οποία θα τους είναι και εύκολο να απομνημονεύσουν.

Το κλειδί της επιτυχίας της τακτικής αυτής είναι να βρεθεί το σημείο ισορροπίας ανάμεσα στην αποδοχή των χρηστών και στην ισχύ του συνθηματικού. Μια τέτοια απλή τακτική θα μπορούσε να είναι, για παράδειγμα, να γίνονται αποδεκτά συνθηματικά μόνο αν έχουν μήκος τουλάχιστον οκτώ χαρακτήρων και περιέχουν, στους πρώτους οκτώ χαρακτήρες, τουλάχιστον ένα κεφαλαίο, ένα μικρό, έναν αριθμό και ένα σημείο στίξης. Μια άλλη τέτοια τακτική θα μπορούσε να κάνει αποδεκτά μόνο τα συνθηματικά που δεν περιέχονται σε κάποιο λεξικό κακών συνθηματικών. Πέρα από τη δυσκολία κατάρτισης ενός τέτοιου λεξικού, δυσκολία που ωστόσο έχει ήδη αποτελέσει αντικείμενο ερευνητικών εργασιών, υπάρχουν δύο προβλήματα στην εφαρμογή της τακτικής αυτής. Το πρώτο είναι ο χώρος, αφού ένα καλό λεξικό καταλαμβάνει αρκετό χώρο μνήμης. Το δεύτερο είναι ο χρόνος, αφού όσο πιο μεγάλο είναι το λεξικό, τόσο περισσότερος χρόνος απαιτείται για τον έλεγχο των συνθηματικών που υποβάλλει ο χρήστης.

6. <u>Υποκλοπή συνθηματικών</u>

Η αναγνώριση και η επαλήθευση ταυτότητας μέσω ονόματος χρήστη και συνθηματικού παρέχουν μονομερή αυθεντικοποίηση. Ο χρήστης εισάγει ένα όνομα και ένα συνθηματικό και ο υπολογιστής επαληθεύει την ταυτότητα του χρήστη. Αλλά ξέρει ο χρήστης ποιος έχει λάβει το συνθηματικό του; Μέχρι τώρα η απάντηση είναι όχι. Ο χρήστης δεν έχει καμιά ένδειξη, πόσο μάλλον εγγύηση, για την ταυτότητα του

μέρους που βρίσκεται στην άλλη άκρη της γραμμής.

Αυτό είναι πραγματικό πρόβλημα και οδηγεί στη δεύτερη μέθοδο παραβίασης συνθηματικών. Σε μια επίθεση υποκλοπής, ο επιτιθέμενος, που μπορεί να είναι νόμιμος χρήστης, τρέχει ένα πρόγραμμα που παρουσιάζει μια ψεύτικη οθόνη σύνδεσης σε κάποιο τερματικό. Ένας ανυποψίαστος χρήστης έρχεται στο τερματικό αυτό και προσπαθεί να συνδεθεί. Το θύμα οδηγείται μέσω του κανονικού μενού σύνδεσης

και του ζητείται το όνομα χρήστη και το συνθηματικό του. Αυτά αποθηκεύονται σε χώρο προσπελάσιμο από τον επιτιθέμενο. Στη συνέχεια, ο έλεγχος είτε περνά στο χρήστη ή εμφανίζεται ένα ψεύτικο μήνυμα λάθους σύνδεσης και το πρόγραμμα υποκλοπής τερματίζει. Ο έλεγχος μεταφέρεται στο λειτουργικό σύστημα, που τώρα παρουσιάζει στο χρήστη την αληθινή οθόνη σύνδεσης. Ο χρήστης ξαναπροσπαθεί, πετυχαίνει και μπορεί να μείνει με παντελή άγνοια του γεγονότος ότι το συνθηματικό του υποκλάπηκε.

Τι μπορούμε να κάνουμε για να αντιμετωπίσουμε μια τέτοια επίθεση υποκλοπής;

- Η επίδειξη του πλήθους των αποτυχημένων προσπαθειών σύνδεσης μπορεί να δείξει στο χρήστη ότι έγινε τέτοια επίθεση. Αν η πρώτη προσπάθεια σύνδεσης αποτύχει, αλλά στη δεύτερη (και πετυχημένη) απόπειρα το σύστημά σας πει ότι δεν υπήρξαν αποτυχημένες προσπάθειες σύνδεσης, πρέπει να αρχίσετε να υποψιάζεστε ότι κάτι συμβαίνει.
- Η παροχή κάποιου είδους εγγύησης ότι ο χρήστης επικοινωνεί με το λειτουργικό σύστημα και όχι με ένα πρόγραμμα υποκλοπής επίσης βοηθά. Στα Windows NT, για παράδειγμα, αυτό μπορεί να γίνει με το ταυτόχρονο πάτημα των πλήκτρων CTRL+ALT+DEL.
- Αν οι χρήστες απαιτούν μεγαλύτερες εγγυήσεις για την ταυτότητα του συστήματος με το οποίο επικοινωνούν, όπως, για παράδειγμα, μπορεί να συμβαίνει σε κατανεμημένα συστήματα, είναι δυνατόν το σύστημα να απαιτείται να αυθεντικοποιήσει τον εαυτό του στο χρήστη. Η διαδικασία αυτή της αμοιβαίας αυθεντικοποίησης μπορεί να υλοποιηθεί με αρκετούς τρόπους, ένας από τους οποίους είναι και η χρήση κρυπτογραφημένων πρωτοκόλλων περιορισμένης ή μηδενικής γνώσης.

Πέρα από τις επιθέσεις υποκλοπής, ένας επιτιθέμενος είναι δυνατόν να έχει στη διάθεσή του και άλλους τρόπους για να βρει ένα συνθηματικό, ειδικά σε περιπτώσεις κατανεμημένων συστημάτων, όπου τα συνθηματικά μεταδίδονται (κρυπτογραφημένα ή όχι) μέσω δικτυακών συνδέσεων. Στις περιπτώσεις αυτές συνηθισμένη είναι και η χρήση συνθηματικών μιας χρήσης.

Συνθηματικά μιας χρήσης είναι αυτά που αλλάζουν κάθε φορά που χρησιμοποιούνται. Αντί ο κάθε χρήστης να χρησιμοποιεί μια στατική λέξη (ή φράση), χρησιμοποιεί μια στατική μαθηματική συνάρτηση. Το σύστημα παρέχει ένα μοντέλο στη συνάρτηση και ο χρήστης υπολογίζει και επιστρέφει την τιμή της συνάρτησης. Τα συστήματα αυτά αναφέρονται και ως συστήματα πρόκλησης απάντησης, γιατί το σύστημα προκαλεί το χρήστη και επαληθεύει ή όχι την ταυτότητά του με βάση την απάντησή του.

Τα συνθηματικά μιας χρήσης παρέχουν αρκετή προστασία εναντίον υποκλοπών, γιατί η υποκλοπή τους δεν προσφέρει τίποτα στον επιτιθέμενο. Ωστόσο, η χρησιμότητά τους περιορίζεται από την υπολογιστική πολυπλοκότητα των αλγόριθμων που ένας άνθρωπος μπορεί να απομνημονεύσει και να χρησιμοποιήσει. Και αυτή η δυσκολία όμως αντιμετωπίζεται, αν οι υπολογισμοί αυτοί εκτελεστούν από μια υπολογιστική μηχανή (π.χ. μια κάρτα) αντί από έναν άνθρωπο.

7. Παραβίαση αρχείου συνθηματικών

Για να επαληθεύσει την ταυτότητα ενός χρήστη, το σύστημα πρέπει να συγκρίνει το συνθηματικό που εισάγει ο χρήστης με μια τιμή που είναι αποθηκευμένη σε κάποιο αρχείο, αναφερόμενο συνήθως ως αρχείο συνθηματικών. Ένα τέτοιο αρχείο είναι, φυσικά, πολύ ελκυστικός στόχος για υποψήφιους επιτιθέμενους. Η αποκάλυψη, λοιπόν, σε μη κρυπτογραφημένη μορφή ή η τροποποίηση των περιεχομένων του αρχείου συνθηματικών αποτελούν έναν τρίτο πιθανό τρόπο παραβίασης συνθηματικών. Αναφέρθηκαμε σε αποκάλυψη περιεχομένων σε μη κρυπτογραφημένη μορφή. Αυτό δε σημαίνει ότι δε θα πρέπει να μας απασχολεί και η αποκάλυψη κρυπτογραφημένων συνθηματικών. Πράγματι, αν αυτό συμβεί, τίποτε δεν μπορεί να αποκλείσει την εκδήλωση μιας λεξικογραφικής επίθεσης σε μη πραγματικό χρόνο, οπότε μέτρα προστασίας όπως περιορισμός του πλήθους των αποτυχημένων προσπαθειών σύνδεσης καθίστανται μη εφαρμόσιμα. Καταλήγουμε, λοιπόν, ότι η προστασία του αρχείου συνθηματικών αποτελεί ακρογωνιαίο λίθο της ασφάλειας του μηχανισμού αυθεντικοποίησης του συστήματός μας. Για να προστατεύσουμε το αρχείο συνθηματικών, έχουμε τις εξής επιλογές:

- Να το αποθηκεύουμε σε κρυπτογραφημένη μορφή.
- Να ελέγχουμε την πρόσβαση σ' αυτό μέσω του λειτουργικού συστήματος.

- Να συνδυάσουμε τα δύο παραπάνω και πιθανόν να τα ενισχύσουμε με άλλα μέτρα που στοχεύουν στην αποτροπή ή την καθυστέρηση λεξικογραφικών επιθέσεων.

Η εφαρμογή κρυπτογραφικής προστασίας δεν απαιτεί καν τη χρήση αλγόριθμου κρυπτογράφησης, αφού αρκεί μια μονόδρομη συνάρτηση. Μονόδρομη συνάρτηση είναι μια συνάρτηση που είναι σχετικά εύκολο να υπολογιστεί αλλά πολύ δύσκολο να αντιστραφεί. Δηλαδή, δοθέντος του x είναι πολύ εύκολο να υπολογιστεί το f(x), αλλά

δοθέντος του f(x) είναι πολύ δύσκολο να υπολογιστεί το x. Τέτοιες συναρτήσεις έχουν χρησιμοποιηθεί από παλιά για την προστασία αποθηκευμένων συνθηματικών. Αντί για το συνθηματικό x, φυλάσσεται στο αρχείο συνθηματικών η τιμή f(x). Όταν κάποιος χρήστης προσπαθήσει να συνδεθεί και εισάγει ένα συνθηματικό x΄, το σύστημα υπολογίζει την τιμή f(x΄) και τη συγκρίνει με την αποθηκευμένη τιμή f(x). Αν αυτές οι δύο είναι ίδιες, ο χρήστης αυθεντικοποιείται επιτυχώς.

Αν χρησιμοποιήσουμε μια τέτοια τεχνική, το αρχείο συνθηματικών μπορεί να παραμείνει αναγνώσιμο αν δε μας απασχολούν ιδιαίτερα οι λεξικογραφικές επιθέσεις.

Αν η f είναι καλή μονόδρομη συνάρτηση, δεν είναι εφικτό να ανακατασκευαστεί το

συνθηματικό x από την f(x). Σε μια λεξικογραφική επίθεση, ο επιτιθέμενος κωδικοποιεί όλες τις λέξεις ενός λεξικού και συγκρίνει τα αποτελέσματα με τις κωδικοποιημένες εγγραφές του αρχείου συνθηματικών. Αν βρεθεί κάποια που ταιριάζει, ο επιτιθέμενος βρήκε ένα συνθηματικό. Μήπως η μονόδρομη συνάρτηση μπορεί να σχεδιαστεί έτσι ώστε να καθυστερεί τέτοιες επιθέσεις; Η απάντηση είναι, βέβαια, ναι, αν η συνάρτηση αυτή είναι αρκετά πολύπλοκη να υπολογιστεί. Φυσικά, όσο πιο πολύπλοκος γίνεται ο υπολογισμός της μονόδρομης συνάρτησης, τόσο μεγαλώνει η καθυστέρηση στην αυθεντικοποίηση των νόμιμων χρηστών. Από την άλλη πλευρά, αν βελτιστοποιήσουμε τη μονόδρομη συνάρτηση ως προς την ταχύτητά της, διευκολύνουμε τις λεξικογραφικές επιθέσεις. Όπως σχεδόν πάντα, καλούμαστε να βρούμε το σημείο ισορροπίας.

Οι μηχανισμοί ελέγχου προσπέλασης του λειτουργικού συστήματος περιορίζουν την πρόσβαση σε αρχεία και άλλους πόρους σ' εκείνους μόνο τους χρήστες που είναι προς τούτο εξουσιοδοτημένοι. Μόνο εξουσιοδοτημένοι (και μάλιστα προνομιούχοι) χρήστες πρέπει να μπορούν να έχουν πρόσβαση εγγραφής στο αρχείο συνθηματικών, αλλιώς ο κάθε επιτιθέμενος θα μπορούσε να αποκτήσει πρόσβαση στα αρχεία χρηστών απλώς αλλάζοντας το συνθηματικό τους, ακόμα και αν αυτό προστατεύεται κρυπτογραφικά. Αν περιοριστεί και η πρόσβαση ανάγνωσης, θεωρητικά τα συνθηματικά θα μπορούσαν να αποθηκευτούν ακόμη και σε μη κρυπτογραφημένη μορφή. Αν, όμως, το αρχείο συνθηματικών περιέχει πληροφορίες που είναι απαραίτητες και σε μη προνομιούχους χρήστες, τότε πρέπει τα συνθηματικά να είναι κρυπτογραφημένα. Ωστόσο, ακόμη και ένα τέτοιο αρχείο, τυπικό παράδειγμα του οποίου είναι το /etc/passwd του Unix, μπορεί να αποτελέσει στόχο λεξικογραφικής επίθεσης. Γι' αυτό το λόγο, οι πιο πρόσφατες εκδόσεις του Unix αποθηκεύουν τα κρυπτογραφημένα συνθηματικά σε ένα αρχείο που δεν είναι δημόσια διαθέσιμο. Τέτοια αρχεία ονομάζονται σκιώδη αρχεία συνθηματικών. Για παράδειγμα, το HP–UX μπορεί να χρησιμοποιήσει ένα σκιώδες αρχείο συνθηματικών, το /.secure/etc/passwd.

Ένα άλλο, όχι τόσο ισχυρό, μέτρο προστασίας ανάγνωσης αρχείου είναι να το αποθηκεύσουμε με κάποια ειδική, ιδιωτική και μη δημόσια γνωστή μορφοποίηση. Για παράδειγμα, τα Windows NT αποθηκεύουν τα κρυπτογραφημένα συνθηματικά με μια ιδιωτική δυαδική μορφοποίηση. Το μέτρο αυτό μπορεί να είναι αρκετό για να αντιμετωπίσει τον άπειρο επιτιθέμενο, αλλά ο αποφασισμένος επιτιθέμενος θα αποκτήσει ή θα συμπεράνει την απαραίτητη πληροφορία για να ανιχνεύσει τη θέση των δεδομένων των σχετικών με την ασφάλεια. Το συμπέρασμα; Από μόνη της η ασφάλεια μέσω αδιαφάνειας δεν είναι ισχυρός μηχανισμός προστασίας. Αυτό δε σημαίνει ότι η αδιαφάνεια δεν μπορεί να αποδειχθεί χρήσιμη, σε συνδυασμό με άλλα μέτρα ασφάλειας.

Αν ανησυχούμε για λεξικογραφικές επιθέσεις, αλλά δεν μπορούμε, για κάποιο λόγο, να κρύψουμε το αρχείο συνθηματικών, μπορεί να χρησιμοποιήσουμε μια άλλη τεχνική, γνωστή ως επέκταση του συνθηματικού (salting). Όταν ένα συνθηματικό κρυπτογραφείται πριν από την αποθήκευση, κάποια επιπλέον πληροφορία (ή επέκταση) προστίθεται σ' αυτό πριν από την κρυπτογράφηση. Στη συνέχεια, η επέκταση απόθηκεύεται (σε μη κρυπτογραφημένη μορφή) μαζί με το συνθηματικό. Για παράδειγμα, στο Unix ο μηχανισμός επέκτασης λειτουργεί ως εξής: Ο χρήστης επιλέγει ένα συνθηματικό μήκους μέχρι οκτώ εκτυπώσιμων χαρακτήρων. Το συνθηματικό αυτό μετατρέπεται, χρησιμοποιώντας ASCII 7 bit, σε μια λέξη μήκους 56 bit, που με τη σειρά της χρησιμοποιείται ως έντελο σε μια μονόδρομη συνάρτηση.

Η συνάρτηση αυτή, γνωστή ως crypt(3), βασίζεται στο DES. Ο πίνακας Ε του DES τροποποιείται χρησιμοποιώντας επέκταση μήκους 12 bit, του οποίου η τιμή σχετίζεται με την ώρα της δημιουργίας του συνθηματικού. Ο τροποποιημένος αλγόριθμος DES εφαρμόζεται σε είσοδο που αποτελείται από ένα block 64 μηδενικών. Η έξοδος του αλγόριθμου στη συνέχεια χρησιμοποιείται ως είσοδος στην ίδια συνάρτηση, για δεύτερη κρυπτογράφηση. Η διαδικασία αυτή επαναλαμβάνεται συνολικά 25 φορές. Η τελική έξοδος, μήκους 64 bit, μετατρέπεται σε ακολουθία 11 χαρακτήρων. Το κρυπτογραφημένο συνθηματικό αποθηκεύεται στη συνέχεια μαζί με τη μη κρυπτογραφημένη, επέκταση στο αρχείο συνθηματικών.

Τι σκοπούς εξυπηρετεί η επέκταση;

- Εμποδίζει την ανάγνωση ταυτόσημων συνθηματικών στο αρχείο συνθηματικών. Ακόμη και αν δύο χρήστες επιλέξουν το ίδιο συνθηματικό, αυτά τα συνθηματικά θα δημιουργηθούν σε διαφορετικούς χρόνους, επομένως η επέκταση θα είναι διαφορετική για κάθε συνθηματικό και, επομένως, οι κρυπτογραφημένες μορφές των συνθηματικών θα είναι διαφορετικές.
- Επιμηκύνει το μήκος του συνθηματικού χωρίς να απαιτείται ο χρήστης να θυμάται επιπλέον δύο χαρακτήρες. Επομένως, το πλήθος των πιθανών συνθηματικών αυξάνεται κατά έναν παράγοντα ίσο με 4096, αυξάνοντας έτσι τη δυσκολία να εικαστεί το συνθηματικό.

Αποκλείει τη χρήση υλικού για την υλοποίηση του DES, πράγμα που θα διευκόλυνε την εκδήλωση επίθεσης εξαντλητικής έρευνας.

2.2.2 ΤΑΥΤΟΠΟΙΗΣΗ ΜΕ ΒΙΟΜΕΤΡΙΚΕΣ ΜΕΘΟΔΟΥΣ

Βιομετρία. Είναι η επιστήμη μέτρησης και στατιστικής ανάλυσης βιολογικών
δεδομένων. Στο γνωστικό αντικείμενο της Ασφάλειας, ο όρος αναφέρεται σε τεχνολογικές μεθόδους που επιτρέπουν τη συλλογή και ανάλυση χαρακτηριστικών του ανθρώπινου σώματος ή/και της ανθρώπινης συμπεριφοράς, με σκοπό τον έλεγχο πρόσβασης στους πόρους του συστήματος, ή στα πλαίσια της φυσικής ασφάλειας (physical security) σε σημεία ενδιαφέροντος.

Επαλήθευση Ταυτότητας (Identity Verification): Σύγκριση ενός χαρακτηριστικού με ένα χαρακτηριστικό της βάσης δεδομένων, με σκοπό την εύρεση
«ταιριάσματος» (matching). Υποερώτημα που απαντάται:

Είναι ο Α όντως ο Α;

Ταυτοποίηση (Identification): Σύγκριση ενός χαρακτηριστικού με όλα τα χαρακτηριστικά της βάσης δεδομένων, με σκοπό την εύρεση ενός «ταιριάσματος». Υποερώτημα που απαντάται:
Ποια είναι η ταυτότητα του υποκειμένου;

Η έννοια της ταυτοποίησης παρουσιάζει το μεγαλύτερο τεχνολογικό και ερευνητικό ενδιαφέρον σε σχέση με την επαλήθευση ταυτότητας. Σε περιπτώσεις κατά τις οποίες το μέγεθος της βάσης είναι ιδιαίτερα μεγάλο, η ταυτοποίηση καθίσταται μια πολύ δύσκολη διαδικασία. Στην πράξη, οι βιομετρικές μέθοδοι χρησιμοποιούνται κυρίως για την επαλήθευση ταυτότητας (identity verification) των χρηστών ενός συστήματος, στα πλαίσια της ταυτοποίησης SYA (Something You Are).

Απαιτήσεις Συστήματος
Ένα σύστημα (ή συσκευή) βιομετρίας συνήθως αποτελείται από:

- Διαδικασίες και συσκευές εισόδου και εξαγωγής χαρακτηριστικών από το αρχικό δείγμα,
- Έναν αποθηκευτικό χώρο (π.χ. μια Βάση Δεδομένων- ΒΔ) με τα χαρακτηριστικά που έχουν εξαχθεί,
- Διαδικασίες αναγνώρισης (σύγκρισης και εξαγωγής αποτελέσματος).

Λήψη δείγματος: Κατά το στάδιο της εγγραφής, λαμβάνεται το πρώτο δείγμα από ένα υποκείμενο. Η ποιότητα του πρώτου δείγματος είναι σημαντική για τη μετέπειτα αναγνώριση του υποκειμένου. Εάν η ποιότητα δεν είναι ικανοποιητική, τότε η διαδικασία λήψης πρέπει να επαναληφθεί.

Συνήθως, η λήψη του πρώτου δείγματος, πραγματοποιείται υπό την καθοδήγηση ειδικού προσωπικού. Στη συνέχεια θαακολουθήσει η ψηφιοποίηση του δείγματος και η εξαγωγή χαρακτηριστικών.

Εξαγωγή χαρακτηριστικών: Το δείγμα που αποκτάται κατά το στάδιο της εγγραφής, δεν αποθηκεύεται στη ΒΔ με την αρχική του μορφή. Το πρώτο δείγμα περιέχει ορισμένη ποσότητα πληροφορίας που δεν είναι χρήσιμη, και επομένως πρέπει να απομονωθεί. Ένα πολύ μικρό υποσύνολο του δείγματος που αποκτάται, θεωρείται ως μοναδικό για το υποκείμενο, και παρουσιάζει το μεγαλύτερο ενδιαφέρον (άρα είναι χρήσιμο) κατά τον έλεγχο πρόσβασης. Η ποιότητα και η ποσότητα των χαρακτηριστικών του δείγματος που παρουσιάζουν το μεγαλύτερο ενδιαφέρον, εξαρτώνται από το είδος της βιομετρικής μεθόδου.

Σημείωση: Η διαδικασία της εξαγωγής χαρακτηριστικών είναι απωλεστική (lossy): αυτό σημαίνει ότι τα χαρακτηριστικά που εξάγονται, δεν είναι ικανά να οδηγήσουν στην τέλεια αναδημιουργία του αρχικού δείγματος.

Ένα βιομετρικό χαρακτηριστικό δε μπορεί ποτέ να είναι 100% ίδιο με το χαρακτηριστικό που ελήφθη κατά την εγγραφή. Αυτό συμβαίνει επειδή το περιβάλλον ή/και άλλοι εξωγενείς παράγοντες (ζέστη, φωτισμός, υγρασία, σκόνη, συναισθηματική/πνευματική κατάσταση, κόπωση, ασθένεια κ.λ.π) επηρεάζουν τη διαδικασία. Επομένως, ένα σύστημα που ελέγχει (και απαιτεί) 100% ταύτιση για να επιτρέψει την πρόσβαση, θα ήταν πρακτικά άχρηστο, αφού θα απέρριπτε πολλούς εξουσιοδοτημένους χρήστες (Λανθασμένη Απόρριψη – False Rejection). Ανάλογα προβλήματα εντοπίζονται σε περιπτώσεις όπου, ένα σύστημα είναι πολύ «χαλαρό», δηλαδή αποφαίνεται θετικά ακόμα και στην περίπτωση όπου το ποσοστό ομοιότητας είναι χαμηλό. Το σύστημα αυτό θα ήταν επίσης πρακτικά άχρηστο, αφού θα επέτρεπε την πρόσβαση σε πολλούς μη εξουσιοδοτημένους χρήστες (Λανθασμένη Αποδοχή - False Acceptance).

Είναι σαφές ότι τα ποσοστά FRR και FAR είναι αντιστρόφως ανάλογα. Το σημείο ισορροπίας (security threshold) είναι το σημείο εκείνο κατά το οποίο έχουμε αποδεκτά ποσοστά FAR και FRR, και εξαρτάται από την πολιτική ασφάλειας του συστήματος. Το σημείο ισορροπίας απεικονίζει την ακρίβεια του συστήματος, και συγκεκριμένα το ποσοστό διαφοροποίησης που επιτρέπεται μεταξύ του αρχικού και του τελικού δείγματος: αν η διαφοροποίηση είναι μικρότερη του σημείου ισορροπίας,
τότε ο χρήστης γίνεται αποδεκτός, αλλιώς ο χρήστης απορρίπτεται.

- Σε συστήματα υψηλού επιπέδου ασφάλειας, όπου η ασφάλεια είναι πιο σημαντική από τη λειτουργικότητα, το FAR διατηρείται σε πολύ μικρά επίπεδα με συνέπεια το ποσοστό εξουσιοδοτημένων χρηστών που απορρίπτονται από το σύστημα να είναι υψηλό. Σε αυτήν την περίπτωση συνήθως χρησιμοποιούνται συμπληρωματικές διαδικασίες, π.χ. προσωπικό ασφάλειας για τον φυσικό έλεγχο της ταυτότητας όσων το σύστημα απορρίπτει.
- Σε συστήματα χαμηλού-μέσου επιπέδου ασφαλείας, όπου η λειτουργικότητα είναι πιο σημαντική από την ασφάλεια, το FRR διατηρείται σε πολύ μικρά επίπεδα, με συνέπεια το ποσοστό εξουσιοδοτημένων χρηστών που γίνονται αποδεκτοί από το σύστημα να είναι υψηλό. Για παράδειγμα, ο μηχανισμός ελέγχου πρόσβασης σε ένα φωτοτυπικό μηχάνημα θα πρέπει να έχει χαμηλό FRR.

1. <u>Δακτυλικό αποτύπωμα</u>

Ο έλεγχος πρόσβασης με τη χρήση δαχτυλικών αποτυπωμάτων είναι από τις πλέον κλασσικές τεχνικές ταυτοποίησης. Οι πρώτες αυτοματοποιημένες μέθοδοι χρησιμοποιήθηκαν κατά τη δεκαετία του 60 στις ΗΠΑ για την διαλεύκανση εγκλημάτων.

<u>Λήψη δείγματος</u>**:** Οι παραδοσιακές μέθοδοι κάνουν χρήση μελάνης για την αποτύπωση του δείγματος σε χαρτί. Στη συνέχεια χρησιμοποιείται ένας σαρωτής για την ψηφιοποίηση του δείγματος. Τα σύγχρονα συστήματα περιλαμβάνουν αναγνώστες (readers) βασισμένους σε:

- Τεχνολογίες φωτός (οπτικοί – optical): Η εξαγωγή των χαρακτηριστικών βασίζεται στις διαφοροποιήσεις της αντανάκλασης του φωτός (χρήση LED) ανάλογα με το είδος της επιφάνειας στην οποία προσκρούει. Ένα μειονέκτημα των οπτικών αναγνωστών είναι ότι η ακρίβεια τους επηρεάζεται από τη σκόνη και τις ακαθαρσίες.
- Σιλικόνη (Silicon): Το δάχτυλο τοποθετείται σε μια επιφάνεια σιλικόνης που αποτελείται από μικροσκοπικά στοιχεία (pixels) - Όσο μεγαλύτερος είναι ο αριθμός των pixels (μεγαλύτερη ανάλυση) τόσο πιο ακριβή είναι τα αποτελέσματα (π.χ 500 dpi). Με τη χρήση ειδικών αισθητήρων μετρώνται

χαρακτηριστικά όπως η πίεση ή/και η απόσταση μεταξύ της επιφάνειας του δαχτύλου και των pixels. Οι αναγνώστες που βασίζονται στη χρήση ολοκληρωμένων (chips) σιλικόνης, χαρακτηρίζονται από το χαμηλό τους μέγεθος και ως εκ τούτου χρησιμοποιούνται σε περιβάλλοντα όπου το μικρό μέγεθος είναι σημαντικό (π.χ. κινητή τηλεφωνία, φορητοί Η/Υ κ.λ.π).

- Υπέρηχοι (ultrasonic): Η χρήση υπέρηχων εξάγει τα χαρακτηριστικά του δέρματος που βρίσκεται κάτω από την επιφάνεια του δάχτυλου (η οποία μπορεί να επηρεάζεται από σκόνη ή αμυχές). Θεωρούνται περισσότερο ακριβή (και ακριβά) από τους οπτικούς αναγνώστες.

Στις περισσότερες των περιπτώσεων, τα χαρακτηριστικά που εξάγονται είναι οι γραμμές και οι καμπύλες (τα σημεία «Minutiae») από τις οποίες αποτελείται κάθε δαχτυλικό αποτύπωμα, και οι οποίες (στο σύνολο τους) είναι μοναδικές για κάθε υποκείμενο. Περίπου 30 τέτοια σημεία εξάγονται από κάθε αποτύπωμα, ενώ το συνολικό μέγεθος του αποτυπώματος που εξάγεται δεν ξεπερνάει το 1 KB. Η πιθανότητα δύο άτομα να έχουν περισσότερα από 8-10 τέτοια σημεία, θεωρείται πάρα πολύ μικρή.

Πλεονεκτήματα: Η αναγνώριση δαχτυλικού αποτυπώματος είναι γνωστή και γρήγορη μέθοδος, εμφανίζει σχετικά υψηλή ακρίβεια κατά την επαλήθευση ταυτότητας & την ταυτοποίηση. Επιπλέον, τα χαρακτηριστικά που εξάγονται είναι πλούσια σε πληροφορία (δηλαδή, υπάρχουν σημαντικές διαφορές μεταξύ δύο υποκειμένων).

Μειονεκτήματα: Η αναγνώριση δαχτυλικού αποτυπώματος επηρεάζεται συχνά από αλλαγές στο περιβάλλον, όπως η ηλικία, η σκόνη, η υγρασία, η καταπόνηση του χεριού λόγω εργασίας κ.λ.π. Επίσης, όταν το δαχτυλικό αποτύπωμα είναι χαμηλής ποιότητας, η εξαγωγή των χαρακτηριστικών είναι δύσκολη.

2. Αναγνώριση Ίριδας (Iris Recognition)

Η ίριδα είναι η κυκλική επιφάνεια που περικλείει την κόρη του ματιού. Η ίριδα του ματιού περιέχει ένα πλούσιο και πολύπλοκο μωσαϊκό γραμμών και σχημάτων (υπάρχουν περίπου 200 τέτοια σημεία), τα οποία είναι μοναδικά για κάθε υποκείμενο.

Οι μέθοδοι αναγνώρισης που βασίζονται στην ίριδα θεωρούνται από τις πλέον ακριβείς (accurate) μεθόδους: Η έρευνα έχει δείξει ότι ο έλεγχος πρόσβασης με τη χρήση του αποτυπώματος της ίριδας εμφανίζει ποσοστά ακρίβειας μεγαλύτερα και από τις μεθόδους αναγνώρισης DNA.

Λήψη Δείγματος: Πραγματοποιείται λήψη φωτογραφίας (με τη χρήση υπέρυθρης ακτινοβολίας) από κοντινή απόσταση. Η φωτογραφία θα πρέπει να έχει υψηλή ανάλυση, ώστε να μην απωλεστούν τα χαρακτηριστικά της ίριδας.

Ανίχνευση ζωής: Ορισμένα τερματικά ανιχνεύουν τις περιοδικές διακυμάνσεις του μεγέθους της κόρης του ματιού, ώστε να αποφευχθούν επιθέσεις επανάληψης (replay attacks) – π.χ. τοποθέτηση φωτογραφίας της ίριδας μπροστά στην κάμερα.

Πλεονεκτήματα: Το αποτύπωμα της ίριδας παραμένει αναλλοίωτο στη διάρκεια ζωής του ανθρώπου. Τα χαρακτηριστικά που εξάγονται είναι αρκετά πλούσια, το μέγεθος του αποτυπώματος είναι μικρό, ενώ η διαδικασία είναι ιδιαίτερα γρήγορη, τόσο κατά τον έλεγχο πρόσβασης όσο και κατά την ταυτοποίηση.

Μειονεκτήματα: Η μέθοδος απαιτεί τη λήψη φωτογραφίας από πολύ κοντινή απόσταση και σε υψηλή ανάλυση. Αυτό μπορεί να θεωρηθεί ενοχλητικό για πολλούς χρήστες του συστήματος. Επίσης, η μέθοδος δεν ενδείκνυται για ταυτοποίηση σε πολυσύχναστους χώρους, σε αντίθεση με άλλες μεθόδους (π.χ. αναγνώριση προσώπου).

3. Αναγνώριση Αμφιβληστροειδούς (Retina)

Η μέθοδος αυτή ανιχνεύει και καταγράφει το πλέγμα των αιμοφόρων αγγείων στον αμφιβληστροειδή του ματιού. Η ρέτινα δεν είναι άμεσα ορατή. Επομένως, ή λήψη του δείγματος απαιτεί τη χρήση ακτινοβολίας (υπέρυθρη, ή laser) για να φωτιστεί αναδειχθεί ο αμφιβληστροειδής. Στη συνέχεια αποκτάται η εικόνα της ρέτινας η οποία και αναλύεται για την εύρεση και εξαγωγή των μοναδικών χαρακτηριστικών.

Τα χαρακτηριστικά που εξάγονται περιέχονται στο πλέγμα των αιμοφόρων αγγείων που ξεκινούν από το οπτικό νεύρο και διατρέχουν τη ρέτινα, που είναι διαφορετικά σε κάθε άνθρωπο. Η ακρίβεια της μεθόδου είναι πάρα πολύ υψηλή, και τα χαρακτηριστικά που εξάγονται είναι πλούσια. Ως εκ τούτου μπορεί να χρησιμοποιηθεί για επαλήθευση ταυτότητας αλλά και για ταυτοποίηση. Στην πράξη χρησιμοποιείται για επαλήθευση ταυτότητας σε συστήματα πολύ υψηλού επιπέδου ασφαλείας.

Πλεονεκτήματα: Το αποτύπωμα της ρέτινας παραμένει αναλλοίωτο στη διάρκεια ζωής του ανθρώπου (με εξαιρέσεις, π.χ. λόγω ασθενειών του ματιού). Τα χαρακτηριστικά που εξάγονται είναι αρκετά πλούσια (περίπου 400 χαρακτηριστικά), το μέγεθος του αποτυπώματος είναι μικρό (<100 Β), ενώ η διαδικασία είναι ιδιαίτερα γρήγορη, τόσο κατά την επαλήθευση ταυτότητας όσο και κατά την ταυτοποίηση

4. Αναγνώριση Προσώπου (Facial Recognition)

Λήψη Δείγματος: Σε ιδανικές συνθήκες, ο χρήστης στέκεται σε συγκεκριμένη απόσταση από την κάμερα και κοιτάζει προς την κάμερα.

Εξαγωγή χαρακτηριστικών: Αρχικά, το λογισμικό αναλαμβάνει να εντοπίσει το πρόσωπο ή τα πρόσωπα στη φωτογραφία. Στη συνέχεια εξάγονται τα χαρακτηριστικά
του προσώπου (π.χ. θέση ματιών, μύτης, στόματος, καθώς και η απόσταση μεταξύ τους). Τα συστήματα αναγνώρισης προσώπου ενδείκνυνται κυρίως για έλεγχο πρόσβασης χρηστών σε συστήματα χαμηλού-μέσου επιπέδου ασφαλείας, καθώς τα χαρακτηριστικά που εξάγονται δεν είναι πλούσια.

Πλεονεκτήματα: Τα τελευταία χρόνια, η ακρίβεια των συστημάτων αναγνώρισης προσώπου έχει αυξηθεί σημαντικά, ωστόσο υπολείπεται άλλων μεθόδων.

Μειονεκτήματα: Δυσκολία διάκρισης μεταξύ ατόμων με υψηλό ποσοστό ομοιότητας
(π.χ. δίδυμα). Η ακρίβεια του συστήματος επηρεάζεται από εξωγενείς (π.χ. φωτισμός)
και άλλους παράγοντες (π.χ. ηλικία, πληγές, αλλαγή μαλλιών, γυαλιά, κ.λ.π). Επιπλέον, τα συστήματα αναγνώρισης προσώπου συχνά εγείρουν αντιδράσεις καθώς
η λήψη του αποτυπώματος μπορεί να γίνει και χωρίς τη συγκατάθεση του υποκειμένου.

Ανίχνευση ζωής: Σε περιπτώσεις όπου το σύστημα αναγνώρισης δεν επικουρείται από προσωπικό ασφάλειας, το σύστημα είναι ευπαθές σε επιθέσεις επανάληψης (π.χ. επίδειξη φωτογραφίας). Στα πλαίσια ενός μηχανισμού ανίχνευσης ζωής συνήθως ζητείται από το χρήστη να μεταβάλλει κάποιο από τα χαρακτηριστικά του προσώπου
του (π.χ. κλείσιμο ματιών, κίνηση στόματος, μορφασμοί). Εναλλακτικά μπορεί να χρησιμοποιηθεί και δεύτερη κάμερα με σκοπό τη φωτογράφηση του προφίλ του υποκειμένου.

5. Αναγνώριση Φωνής (Voice Recognition)

Η αναγνώριση φωνής (ή αλλιώς αναγνώριση ομιλούντος – speaker recognition) διαφέρει από την αναγνώριση ομιλίας. Τα συστήματα αναγνώρισης ομιλίας έχουν ως στόχο την αναγνώριση του περιεχομένου της ομιλίας (π.χ. συστήματα φωνητικής υπαγόρευσης), ενώ τα συστήματα αναγνώρισης φωνής έχουν ως στόχο την αναγνώριση του υποκειμένου που ομιλεί.

Λήψη Δείγματος: Η λήψη του φωνητικού δείγματος είναι μια απλή διαδικασία η οποία συνήθως χρησιμοποιεί ένα μικρόφωνο, συνδεδεμένο με έναν πολυμεσικό Η/Υ. Κατά την εγγραφή το σύστημα ζητεί από το χρήστη να εκφωνήσει μια ή περισσότερες λέξεις/φράσεις). Αργότερα, κατά την αναγνώριση, το σύστημα θα ζητήσει από το χρήστη να εκφωνήσει την ίδια φράση.

Εξαγωγή χαρακτηριστικών: Στη συνέχεια γίνεται εξαγωγή ορισμένων φωνητικών χαρακτηριστικών της ανθρώπινης φωνής, τα οποία σχετίζονται με τη φωνητική οδότου ατόμου (φωνητική οδός: αρχίζει από το άνοιγμα των φωνητικών χορδών περιλαμβάνει τον φάρυγγα, τη στοματική και ρινική κοιλότητα και έχει μέσο μήκος για τους άνδρες 17 cm)

Πλεονεκτήματα: Σε αντίθεση με άλλα βιολογικά χαρακτηριστικά, η φωνή ενός ανθρώπου δε «χάνεται». Η μέθοδος είναι η πλέον αποδεκτή από τους χρήστες του συστήματος, λόγω ευκολίας (και διακριτικότητας) στον τρόπο λήψης του αποτυπώματος. Επίσης η μέθοδος είναι ιδανική για

απομακρυσμένη πρόσβαση (π.χ. μέσω ενός τηλεφώνου). Η μέθοδος εμφανίζει καλή αναλογία κόστους/απόδοσης, εφόσον δεν απαιτείται ιδιαίτερος εξοπλισμός, παρά μόνον ειδικό λογισμικό.

Μειονεκτήματα: Η ακρίβεια της μεθόδου αναγνώρισης μπορεί να επηρεαστεί από εξωγενείς (π.χ. θόρυβος) ή άλλους παράγοντες (συναισθηματική φόρτιση, ηλικία ομιλούντος, ασθένεια κ.λ.π).

Ανίχνευση ζωής: Τα συστήματα που ζητούν από το χρήστη τη διατύπωση συγκεκριμένης λέξης/φράσης, είναι ευπαθή σε επιθέσεις επανάληψης. Αρκετά συστήματα αναγνώρισης κάνουν χρήση ενός μηχανισμού πρόκλησης-απάντησης (challenge-response): Κατά την εγγραφή ζητείται από το χρήστη η διατύπωση περισσότερων από μία λέξεων/φράσεων (π.χ. η εκφώνηση μιας λίστας από αριθμούς).

Κατά την αναγνώριση, το σύστημα ζητάει (ή δείχνει) μια λέξη και ο χρήστης καλείται να την εκφωνήσει.

6. Άλλες Κατηγορίες

- Αναγνώριση Αποτυπώματος παλάμης Αποτελεί διαφοροποίηση της μεθόδου αναγνώρισης δαχτυλικού αποτυπώματος. Χρησιμοποιεί οπτικούς αναγνώστες.
- Αναγνώριση Αγγείων χεριού - Βασίζεται στο γεγονός ότι το πλέγμα των αιμοφόρων αγγείων στο ανθρώπινο χέρι (στο πίσω τμήμα του χεριού) είναι μοναδικό. Η λήψη του αποτυπώματος γίνεται με μια κάμερα και τη χρήση υπέρυθρης ακτινοβολίας: Τα αγγεία του χεριού απορροφούν την υπέρυθρη ακτινοβολία και κατ' αυτόν τον τρόπο η παρουσία τους απεικονίζεται στη φωτογραφία που λαμβάνεται. Η τεχνική βρίσκεται ακόμα στο στάδιο της έρευνας.
- Αναγνώριση δέρματος νυχιού. Σύμφωνα με αυτήν τη μέθοδο, αναγνωρίζονται οι γραμμές και οι κοιλότητες στην επιφάνεια του δέρματος, κάτω από το νύχι του δαχτύλου. Διαφοροποιείται ελαφρά από τη μέθοδο αναγνώρισης δαχτυλικού αποτυπώματος. Χρησιμοποιεί οπτικούς αναγνώστες.
- Αναγνώριση DNA. Είναι μία από τις πλέον ακριβείς μεθόδους

αναγνώρισης. Η αναγνώριση μέσω του DNA απαιτεί την ύπαρξη δειγμάτων αίματος, ιστού κ.λ.π και ως εκ τούτου δεν ευνοείται η ευρεία χρήση της σε συστήματα πρόσβασης. Η ταχύτητα αναγνώρισης δεν είναι μεγάλη (στο εργαστήριο, οι βέλτιστοι χρόνοι που επιτυγχάνονται είναι της τάξης των 10 λεπτών).

- Αναγνώριση σχήματος αυτιού. Χρησιμοποιεί εξοπλισμό που ενσωματώνεται σε ακουστικά τηλεφώνου. Η τεχνολογία βρίσκεται σε πρώιμο στάδιο.
- Αναγνώριση οσμής σώματος. Η τεχνολογία βρίσκεται σε πρώιμο στάδιο.

7. Αναγνώριση Υπογραφής

Κατά την εγγραφή ο χρήστης καλείται να υπογράψει (περισσότερες από μια φορές π.χ. 3-10 φορές) ένα κείμενο. Στη συνέχεια με τη χρήση ειδικού λογισμικού εξάγονται τα ειδικά χαρακτηριστικά της υπογραφής. Τα συστήματα αναγνώρισης υπογραφής βασίζονται περισσότερο στη δυναμική (dynamics) της υπογραφής και όχι στην σύγκριση της εικόνας της υπογραφής με την εικόνα που είναι αποθηκευμένη.

Δηλαδή εξετάζονται χαρακτηριστικά όπως η πίεση του υπογράφοντος,τη φορά, η επιτάχυνση, η χρονική διάρκεια κ.λ.π. Ένα πλεονέκτημα της μεθόδου αυτής είναι πως η γνώση της εικόνας μιας υπογραφής δεν καθιστά ικανή την κλοπή της ταυτότητας του υπογράφοντος. Ορισμένα συστήματα εξετάζουν (κάποια από) τα παραπάνω χαρακτηριστικά, σε συνδυασμό με την εμφάνιση της υπογραφής.

Στην πράξη η αναγνώριση υπογραφής χρησιμοποιείται για την επαλήθευση ταυτότητας και μόνον. Τα χαρακτηριστικά που εξάγονται δεν είναι ιδιαίτερα πλούσια,
ενώ το γεγονός ότι είναι συμπεριφοριστική μέθοδος (μια υπογραφή δεν επαναλαμβάνεται ποτέ με τον ίδιο ακριβώς τρόπο) την καθιστά αυτόματα ανεπιθύμητη μέθοδο πρόσβασης για συστήματα υψηλής ασφάλειας. Συνήθως χρησιμοποιείται ως μια συμπληρωματική μέθοδος αναγνώρισης, σε συστήματα χαμηλού- μέσου επιπέδου ασφάλειας.

Σημείωση: Διαφορά με ψηφιακή υπογραφή – Σε αντίθεση με την φυσική υπογραφή, η ψηφιακή υπογραφή είναι μια ντετερμινιστική διαδικασία. Αυτό σημαίνει, πως εφόσον δοθεί το ίδιο (ιδιωτικό) κλειδί ως είσοδος στον αλγόριθμο ψηφιακής υπογραφής, το αποτέλεσμα θα είναι πάντα το ίδιο.

2.2.3 ΔΙΑΧΕΙΡΙΣΗ ΜΗΧΑΝΙΣΜΟΥ ΣΥΝΘΗΜΑΤΙΚΩΝ

Όσα τεχνικά μέτρα και αν πάρει κανείς, ο μηχανισμός αυθεντικοποίησης με συνθηματικά δε θα είναι αρκετά ασφαλής, παρά μόνο αν υπάρχει και σωστή διαχείρισή του. Η εξασφάλιση ότι οι χρήστες θα έχουν συνθηματικά δύσκολα να εικαστούν είναι μια μόνο πλευρά της όλης διαδικασίας διαχείρισης των συνθηματικών. Η διαχείριση αυτή περιλαμβάνει όλες τις πολιτικές και διαδικασίες που χρησιμοποιούνται για τη διασφάλιση της ασφάλειας των συνθηματικών. Αν και το θέμα είναι μεγάλο και έχει αποτελέσει αντικείμενο αρκετών προσπαθειών προτυποποίησης, θα περιοριστώ εδώ να παραθέσω μερικές βασικές οδηγίες για την αποτελεσματική διαχείριση του μηχανισμού αυτού:

• Η σύνθεση, το μήκος, η διάρκεια ζωής, ο εκδότης του συνθηματικού είναι σαφώς καθορισμένα και καταγραμμένα χαρακτηριστικά του συστήματος, η δε επιλογή των παραμέτρων τους γίνεται σύμφωνα με τις απαιτήσεις ασφάλειάς του.

• Η μέθοδος μετάδοσης του συνθηματικού προς τον ιδιοκτήτη του και προς όπου αλλού απαιτείται είναι ασφαλής.

• Η μέθοδος αποθήκευσης του συνθηματικού κατά τη διάρκεια της ζωής του είναι ασφαλής.

• Η μέθοδος εισαγωγής του συνθηματικού στο σύστημα είναι ασφαλής.

• Η μέθοδος μετάδοσης του συνθηματικού από το σημείο εισαγωγής του στο σημείο ελέγχου του είναι ασφαλής.

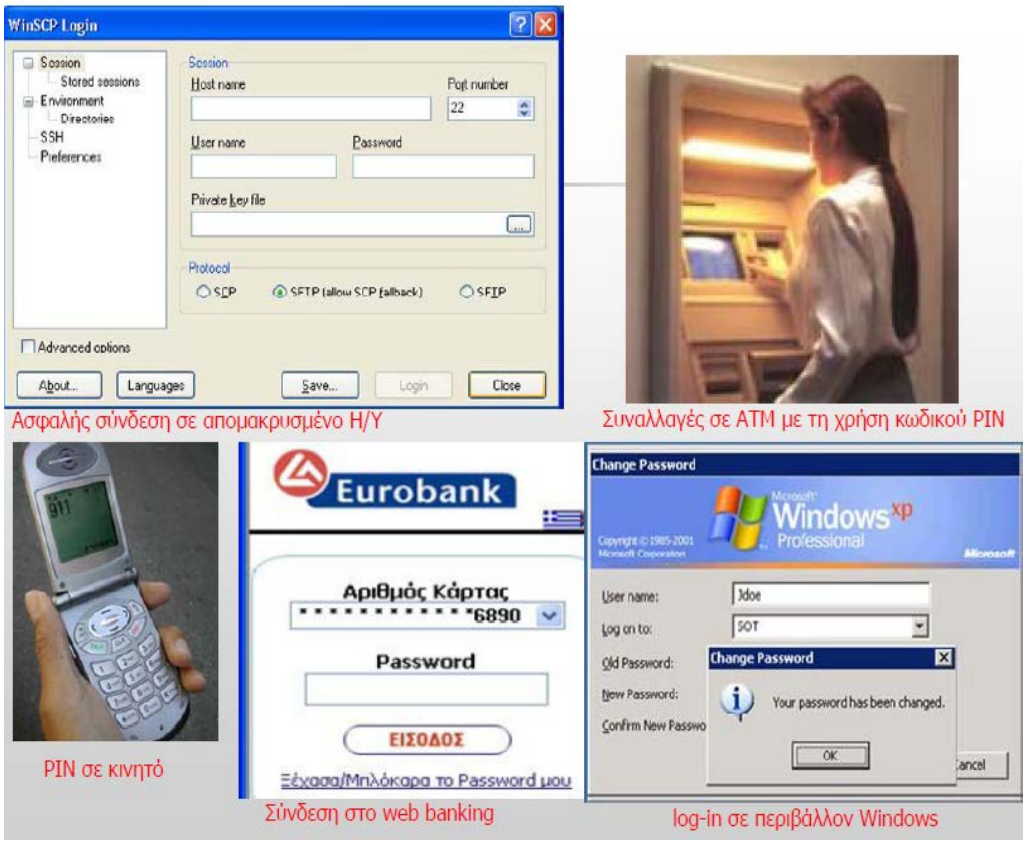
• Η αυθεντικοποίηση του χρήστη δε γίνεται μόνο κατά τη φάση σύνδεσής του στο σύστημα, αλλά και κατά τη διάρκεια της συνόδου, σε διαστήματα που καθορίζονται ανάλογα με τις απαιτήσεις ασφάλειας του συστήματος.

2.2.4 ΕΠΙΛΟΓΟΣ

Στο κεφάλαιο αυτό ασχοληθήκαμε με τις έννοιες της ταυτοποίησης και αυθεντικοποίησης χρήστη. Αρχικά αναφέραμε τις δύο έννοιες και τις ορίσαμε ως τις διαδικασίες αναγνώρισης και επαλήθευσης, αντίστοιχα, της ταυτότητας του χρήστη. Στη συνέχεια, αφού πρώτα αναφερθήκαμε γενικά σε μεθόδους ταυτοποίησης και αυθεντικοποίησης, επικεντρώσαμε το ενδιαφέρον μας στον πιο συνηθισμένο σε υπολογιστικά συστήματα μηχανισμό ταυτοποίησης και αυθεντικοποίησης του ονόματος χρήστη και συνθηματικού. Αναφερθήκαμε με λεπτομέρεια στις απειλές που αντιμετωπίζει ο μηχανισμός αυτός, καθώς και στα μέσα άμυνας που μπορούμε εμείς, ως διαχειριστές ενός συστήματος, να αντιτάξουμε. Τα μέσα αυτά περιλαμβάνουν τεχνικά και διαχειριστικά μέτρα, τα κυριότερα από τα οποία είναι η σωστή επιλογή και διαχείριση συνθηματικών, η υποβοήθηση του χρήστη στην αναγνώριση αποπειρών παραβίασης του συνθηματικού του και η προστασία του αρχείου συνθηματικών μέσω ισχυρής κρυπτογράφησης και ελέγχου της πρόσβασης σ’ αυτό.

2.2.5 ΠΑΡΑΡΤΗΜΑ

1.



2. Πόσοι κωδικοί υπάρχουν;

Αυτό εξαρτάται από το αλφάβητο εισόδου και το μέγεθος (μήκος) του κωδικού πρόσβασης.

Παράδειγμα
Έστω ότι το αλφάβητο εισόδου είναι το [a,b] και το μήκος του κωδικού 2, τότε οι πιθανοί κωδικοί είναι:

aa, ab, ba, bb → 4

Εάν το μήκος του κωδικού είναι 3, τότε οι πιθανοί κωδικοί είναι:

aaa, aab, aba, abb, baa,bab, bba, bbb → 8

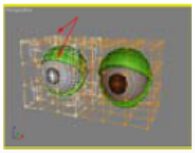
Εάν το αλφάβητο εισόδου έχει μέγεθος 26 (π.χ. τα πεζά γράμματα της λατινικής αλφαβήτου), τότε:

Για κωδικούς μήκους 2 → 26 X 26 = 676 πιθανοί κωδικοί
Για κωδικούς μήκους 3 → 26 X 26 X 26 = 17576 πιθανοί κωδικοί

Εάν το αλφάβητο εισόδου έχει μήκος 96 (π.χ. πεζά και κεφαλαία γράμματα της λατινικής αλφαβήτου : 52, αριθμητικοί χαρακτήρες : 10, σύμβολα και σημεία στίξης από το πληκτρολόγιο : 34), τότε
Για κωδικούς μήκους 8 → 96^8 = 7213895789838336 πιθανοί κωδικοί.

3.

Εκπαίδευση των χρηστών – Μία μελέτη περίπτωσης

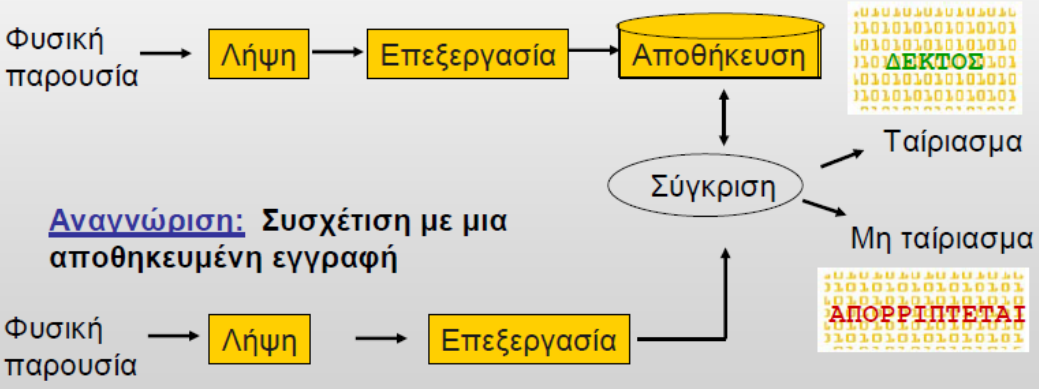


- 100 φοιτητές χωρίστηκαν σε 3 ομάδες (Anderson, 2001)
  - Στην «κόκκινη» ομάδα δόθηκαν οι συνήθεις οδηγίες για την επιλογή σωστού password
    - (τουλάχιστον 6 χαρ., & ένας μη αλφαριθμητικός χαρ.)
  - Στην «πράσινη» ομάδα ζητήθηκε να σκεφθούν μια φράση (passphrase) και να επιλέξουν γράμματα από αυτή
    - π.χ "It's 12 noon and I am hungry" → I'S12&IAH
  - Στην «κίτρινη» ομάδα δόθηκε ένας πίνακας χαρακτήρων (γράμματα & αριθμοί): «Επιλέξτε 8 χαρακτήρες. Γράψτε τον κωδικό σε ένα χαρτί. Καταστρέψτε το χαρτί 1 εβδομάδα μετά...»

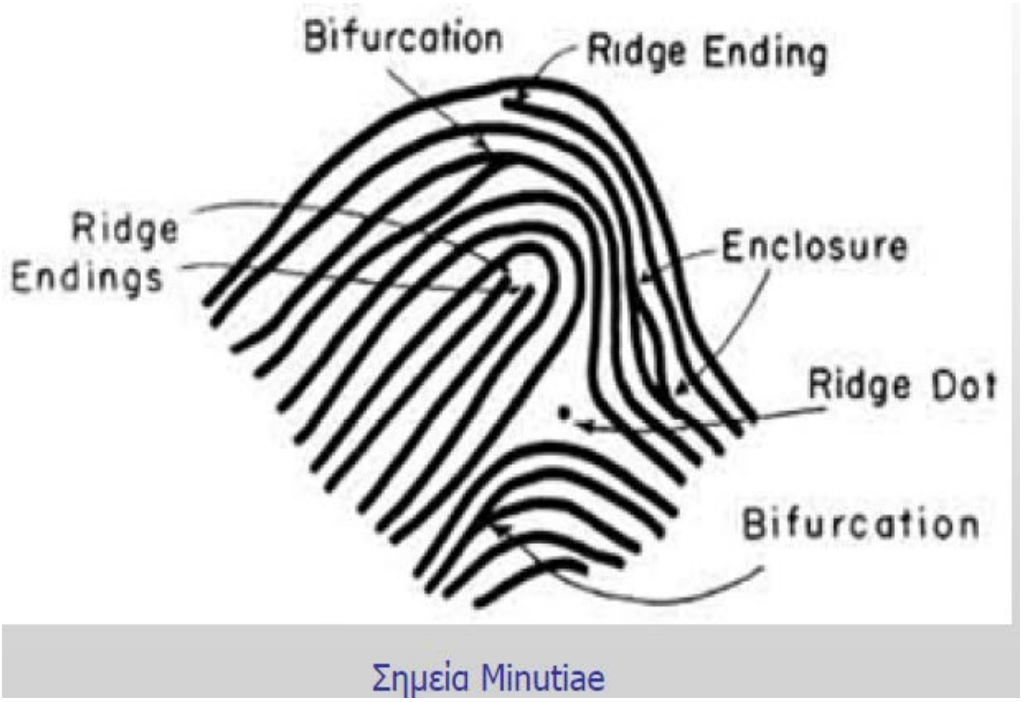
4.

Συστήματα Βιομετρίας Διαδικασίες - βήματα

Εγγραφή: **Αποθήκευση ενός χαρακτηριστικού σε μια βάση δεδομένων**



5.



Σημεία Minutiae

www.cis.rit.edu

2.ΕΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ

2.3 ΕΙΣΑΓΩΓΗ

Όπως έχουμε ξανά αναφέρει στην πρώτη γραμμή άμυνας του υπολογιστικού συστήματος είναι *η* αναγνώριση και η επαλήθευση της ταυτότητας των χρηστών. Το γεγονός ότι κάποιος είναι εξουσιοδοτημένος να συνδεθεί με ένα υπολογιστικό σύστημα δε σημαίνει ότι είναι και εξουσιοδοτημένος να κάνει ό, τι θέλει σ' αυτό! Γι' αυτό το λόγο πρέπει να υπάρχει κάποιος μηχανισμός που ελέγχει τη δυνατότητα κάποιου να χρησιμοποιεί πληροφορίες ή υπολογιστικούς πόρους, στο πλαίσιο ενός πληροφοριακού συστήματος. Ο μηχανισμός αυτός είναι γνωστός με το όνομα έλεγχος προσπέλασης. Παρ' όλο που είναι διαισθητικά προφανής η ανάγκη για την ύπαρξη ενός μηχανισμού ελέγχου προσπέλασης σε κάθε υπολογιστικό σύστημα, δεν είναι εξίσου προφανείς και όλοι οι σκοποί που αυτός εξυπηρετεί. Στην συνέχεια του κεφαλαίου θα αναπτύξουμε τους σκοπούς που εξυπηρετεί ο έλεγχος προσπέλασης, κάποιους ορισμούς και έννοιες βασικές για την κατανόηση. Στη συνέχεια θα αναπτύξουμε κάποιες πολιτικές ελέγχου προσπέλασης, θα αναφέρουμε συνοπτικά κάποια μοντέλα περιγραφής πολιτικών ελέγχου προσπέλασης, ενώ στο τέλος θα περιγράψουμε κάποιους μηχανισμούς υλοποίησης πολιτικών έλεγχων προσπέλασης.

2.3.1 ΕΝΝΟΙΕΣ

Όπως είπαμε και παραπάνω αν έχουμε εξουσιοδοτήσει ένα χρήστη να προσπελάζει πληροφορίες ή υπολογιστικούς πόρους, δεν εννοούμε απαραίτητα ότι ο χρήστης έχει απεριόριστη (με τη χρονική ή τη χωρική έννοια) πρόσβαση σ' αυτά. Ακόμη, μπορεί κάποτε να θελήσουμε να αφαιρέσουμε το προνόμιο αυτό του χρήστη, και μάλιστα να εμποδίσουμε κάθε περαιτέρω προσπέλαση αμέσως μετά την αφαίρεση της εξουσιοδότησης. Αυτά μπορούν να γίνουν μόνον αν ελέγχεται κάθε προσπέλαση κάθε χρήστη σε κάθε πληροφορία ή υπολογιστικό πόρο.

Οι σκοποί που εξυπηρετεί ο έλεγχος προσπέλασης είναι δυο και είναι αλληλοσυμπληρούμενοι.

- <u>Η εφαρμογή της αρχής του ελάχιστου προνομίου.</u>

Η αρχή του ελάχιστου προνομίου λέει ότι κάθε χρήστης πρέπει να έχει πρόσβαση μόνο στο μικρότερο δυνατό πλήθος πληροφοριών και υπολογιστικών πόρων που είναι απαραίτητοι προκειμένου να εκτελεστεί μια εργασία. Ακόμη και αν οι επιπλέον πληροφορίες ή πόροι είναι άχρηστοι για το χρήστη, πάλι δεν επιτρέπεται η παραπανίσια προσπέλαση. Ο λόγος που επιβάλλουμε αυτή την αρχή είναι ότι η απαγόρευση προσπέλασης σε μη απαραίτητες πληροφορίες ή υπολογιστικούς πόρους μας προφυλάσσει από πιθανά ρήγματα ασφάλειας αν αστοχήσει κάποιο τμήμα του μηχανισμού προστασίας.

- <u>Επαλήθευση αποδεκτής χρήσης</u>.

Η απόφαση χορήγησης δυνατότητας προσπέλασης είναι δίτιμη: επιδέχεται μόνο τις τιμές «ναι – επιτρέπεται η προσπέλαση» και «όχι – απαγορεύεται η προσπέλαση». Πέρα όμως από το αν επιτρέπουμε σε κάποιο χρήστη να προσπελάσει μια πληροφορία ή έναν υπολογιστικό πόρο, μας ενδιαφέρει να ξέρουμε και τι κάνει με την πληροφορία ή τον πόρο, προκειμένου να διαπιστώσουμε αν οι ενέργειές του είναι νόμιμες.

Εννοιολογικά, η λέξη προσπέλαση υποδηλώνει ότι υπάρχει ένα ενεργό υποκείμενο που προσπελάζει ένα παθητικό αντικείμενο με σκοπό την εκτέλεση κάποιας συγκεκριμένης λειτουργίας.

Ένα παράδειγμα υποκειμένων είναι οι χρήστες και οι διεργασίες, ενώ ένα παράδειγμα αντικειμένων είναι τα αρχεία και ο εκτυπωτής δικτύου. Μη νομίσετε όμως ότι κάθε οντότητα μέσα σ' ένα σύστημα κατηγοριοποιείται μοναδικά ως υποκείμενο ή αντικείμενο. Ανάλογα με τις συνθήκες, μια οντότητα μπορεί να είναι υποκείμενο σε μια αίτηση προσπέλασης και αντικείμενο σε μια άλλη. Επομένως, οι όροι υποκείμενο και αντικείμενο απλώς διακρίνουν την ενεργό και την παθητική οντότητα σε μια αίτηση προσπέλασης. Για το λόγο αυτό, οι έννοιες υποκείμενο και αντικείμενο μας προσφέρουν δύο βασικές επιλογές για την πολιτική μας ελέγχου προσπέλασης: Μπορούμε είτε να καθορίσουμε *τι* επιτρέπεται *να κάνει* κάθε υποκείμενο ή τι επιτρέπεται *να* πάθει κάθε αντικείμενο.

Λοιπόν αφού το σύστημα έχει εξακριβώσει την ταυτότητα του χρήστη, αποδίδει σ' αυτόν συγκεκριμένα προνόμια για την εργασία του μέσα στο σύστημα, όπως καθορίζονται από την πολιτική ασφάλειας. Τα προνόμια αυτά χωρίζονται σε δύο κύριες κατηγορίες:

- προνόμια επί του συστήματος.

Τα προνόμια αυτά καθορίζουν τις γενικές δυνατότητες που έχει ο χρήστης σε σχέση με το σύστημα. Τέτοια προνόμια μπορεί να καθορίζουν τη δυνατότητα χρήσης πόρων, κ.α..

- προνόμια επί συγκεκριμένων αντικειμένων.

Τα προνόμια αυτά καθορίζουν τι δικαιώματα έχει ο χρήστης πάνω σε συγκεκριμένα αντικείμενα. Για τα προνόμια αυτά υπάρχουν δύο βασικές στρατηγικές ορισμού των, ο κατ' επιλογήν έλεγχος προσπέλασης και ο υποχρεωτικός έλεγχος προσπέλασης.

2.3.2 ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ

Σύμφωνα με τον ISO, ο έλεγχος προσπέλασης αποτελείται από δύο τμήματα: αντικείμενα (Access Control Decision Facility) σύμφωνα με καθορισμένους κανόνες και ένα μηχανισμό που επιβάλλει την απόφαση (Access Control Enforcement Facility). Το σύνολο των κανόνων με βάση τους οποίους λειτουργεί ο μηχανισμός απόφασης είναι γνωστό ως πολιτική ελέγχου προσπέλασης.

Υπάρχουν διάφορες τέτοιες πολιτικές, που έχουν αναπτυχθεί για να καλύψουν τις ανάγκες διαφορετικών χώρων λειτουργίας πληροφοριακών συστημάτων. Ο πρώτος χώρος λειτουργίας πληροφοριακών συστημάτων που ασχολήθηκε με την
ασφάλεια ήταν, για προφανείς λόγους, ήταν ο στρατιωτικός. Η πολιτική ελέγχου προσπέλασης σε στρατιωτικής φύσης πληροφοριακά συστήματα βασίζεται στην ευαισθησία της πληροφορίας που περιέχεται στις πληροφορίες– αντικείμενα και στο
βαθμό εμπιστοσύνης που έχουμε στους χρήστες. Η απόφαση χορήγησης άδειας προσπέλασης βασίζεται στο αποτέλεσμα της σύγκρισης μεταξύ του βαθμού εμπιστοσύνης που έχουμε στο χρήστη και της ευαισθησίας της πληροφορίας.

Το βασικό χαρακτηριστικό της πολιτικής αυτής, γνωστής ως πολιτική Υποχρεωτικού Ελέγχου Προσπέλασης (Mandatory Access Control – **MAC**) είναι ότι η εφαρμογή της είναι υποχρεωτική για όλους τους χρήστες του συστήματος.

Είναι λοιπόν, ο τρόπος περιορισμού της προσπέλασης σε αντικείμενα με βάση την ευαισθησία της πληροφορίας που περιέχεται σ' αυτά και της εμπιστευτικότητας που χαρακτηρίζει τα υποκείμενα, προκειμένου να τους επιτραπεί η προσπέλαση σε πληροφορίες τέτοιας ευαισθησίας. Αυτό το μοντέλο παρέχει ένα σύστημα ασφάλειας που βασίζεται στη χρήση ετικετών ασφάλειας που αποδίδονται τόσο στα υποκείμενα όσο και στα αντικείμενα. Η ετικέτα ασφάλειας ενός υποκειμένου καλείται εξουσιοδότηση χρήσης ενώ η αντίστοιχη ετικέτα του αντικειμένου ονομάζεται βαθμός ασφάλειας. Έτσι, ανάλογα με την εξουσιοδότηση χρήσης που κατέχει το υποκείμενο μπορεί να αποκτήσει πρόσβαση στα αντίστοιχα αντικείμενα. Γίνεται διεξοδική χρήση της ιδιότητας απλής ασφάλειας και της ιδιότητας του μοντέλου Bell-LaPadula.

Ας ξαναγυρίσουμε στο παράδειγμα μας στο στρατιωτικό χώρο και ας ψάξουμε για την ανάγκη αυτή που πηγάζει από το γεγονός ότι στα συστήματα αυτά υπάρχουν πληροφορίες που, αν γίνουν

γνωστές στον εχθρό, μπορούν να βλάψουν την εθνική ασφάλεια. Επειδή η προστασία των πληροφοριών αυτών κοστίζει και επειδή δεν είναι ίση η ευαισθησία όλων αυτών των πληροφοριών, διαχωρίζουμε διάφορους βαθμούς ευαισθησίας της πληροφορίας. Οι συνήθως χρησιμοποιούμενοι βαθμοί ευαισθησίας της πληροφορίας, σε σειρά αύξουσας σημασίας για την εθνική ασφάλεια, είναι αδιαβάθμιστη, εμπιστευτική, απόρρητη και άκρως απόρρητη. Πληροφορία της οποίας ο βαθμός ευαισθησίας είναι ένας από τους τρεις τελευταίους ονομάζεται και διαβαθμισμένη.

Από την άλλη μεριά, οι χρήστες χαρακτηρίζονται από ένα βαθμό εμπιστοσύνης, ο οποίος μετριέται όπως και η ευαισθησία της πληροφορίας. Ο βαθμός αυτός εμπιστοσύνης καθορίζεται μετά από εκτέλεση σειράς ελέγχων σχετικών με το πρόσωπο του χρήστη. Η σχέση μεταξύ βαθμού ευαισθησίας και βαθμού εμπιστοσύνης είναι ότι κάθε χρήστης με βαθμό εμπιστοσύνης *α* θεωρείται έμπιστος να χειρίζεται πληροφορίες με βαθμό ευαισθησίας μικρότερο ή ίσο με *α*.

Όσο μικρότερος είναι ο αριθμός των χρηστών που χειρίζονται μια πληροφορία, τόσο ευκολότερος είναι ο έλεγχος της διάχυσής της. Η διαπίστωση αυτή, σε συνδυασμό με τη διαπίστωση ότι είναι πολύ λίγοι οι χρήστες που χρειάζεται να χειρίζονται όλες τις πληροφορίες ενός δεδομένου βαθμού ευαισθησίας, οδηγεί στη λεγόμενη αρχή της ανάγκης για γνώση σύμφωνα με την οποία ένας χρήστης δεν πρέπει να έχει άδεια προσπέλασης σε μια πληροφορία, παρά μόνο αν τη χρειάζεται για να εκτελέσει κάποια εργασία (εννοείται, βέβαια, ότι θα πρέπει να έχει και τον κατάλληλο βαθμό εμπιστοσύνης). Οδηγούμαστε, λοιπόν, στον ορισμό διαμερισμάτων πληροφορίας, στα οποία κατατάσσεται κάθε πληροφορία ανάλογα με τη φύση της. Τα διαμερίσματα αυτά μπορεί να είναι και επικαλυπτόμενα. Ο συνδυασμός του βαθμού ευαισθησίας μιας πληροφορίας και του συνόλου των διαμερισμάτων στα οποία αυτή ανήκει (που μπορεί να είναι και το κενό σύνολο) συγκροτεί τη διαβάθμιση της πληροφορίας. Κατ' αντιστοιχία, ο βαθμός εμπιστοσύνης κάθε χρήστη συσχετιζόμενος με διαμερίσματα συγκροτεί τη διαβάθμιση του χρήστη. Είναι, ελπίζω, φανερό ότι η διαβάθμιση ενός χρήστη μπορεί να είναι διαφορετική για διαφορετικά διαμερίσματα, αφού είναι δυνατό να διαφέρουν οι αντίστοιχοι βαθμοί εμπιστοσύνης.

Άδεια προσπέλασης χορηγείται αν:

- ο βαθμός εμπιστοσύνης του χρήστη που τη ζητάει είναι τουλάχιστον ίσος με το βαθμό ευαισθησίας της πληροφορίας για τουλάχιστον όλα τα διαμερίσματα στα οποία ανήκει η προς προσπέλαση πληροφορία και
- δε δημιουργεί δυνατότητα υποβιβασμού του βαθμού ευαισθησίας μιας πληροφορίας μέσω εγγραφής σε πληροφορία χαμηλότερου βαθμού ευαισθησίας.

Σε αντίθεση με άλλες πολιτικές έλεγχου προσπέλασης, ο MAC παρέχει πιο ρωμαλέους μηχανισμούς ασφάλειας των δεδομένων και μπορεί να ανταπεξέλθει σε πιο συγκεκριμένες απαιτήσεις ασφάλειας, όπως είναι ο έλεγχος της ροής της πληροφορίας, ενώ το κύριο μειονέκτημά του είναι η μικρή ευελιξία.

Ο Προαιρετικός/Διακριτικός Έλεγχος Προσπέλασης (Discretionary Access Control - **DAC**) βασίζεται στην ιδέα των δικαιωμάτων προσπέλασης σε αντικείμενα (αρχεία, υπολογιστικοί πόροι) του συστήματος, καθώς και σε μηχανισμούς για την εκχώρηση και ανάκλησή τους. Το υποκείμενο (χρήστης, διεργασία) που δημιουργεί ένα αντικείμενο είναι ο ιδιοκτήτης του. Ο ιδιοκτήτης έχει τη δυνατότητα να αναθέτει ή να ανακαλεί δικαιώματα προσπέλασης σε άλλα υποκείμενα πάνω στο αντικείμενο που κατέχει.

Πλεονέκτημα αυτού του τύπου πολιτικής ελέγχου προσπέλασης είναι ότι υποστηρίζεται ευρέως στα υπάρχοντα υπολογιστικά συστήματα, ενώ μειονέκτημά του είναι ότι δεν παρέχει υψηλά επίπεδα ασφάλειας.

Ας το εξετάσουμε όμως και αυτό με παράδειγμα. Στον αντίποδα ενός στρατιωτικού περιβάλλοντος, σε ένα ακαδημαϊκό περιβάλλον, όπου οι πληροφορίες δεν έχουν και μεγάλη σχέση με την εθνική ασφάλεια και όπου η βασική αρχή που πρέπει να διέπει τη λειτουργία των πληροφοριακών συστημάτων είναι η διατήρηση της ακαδημαϊκής ελευθερίας. Υπάρχουν όμως και πληροφορίες (π.χ. βαθμοί) όπου η προσπέλαση πρέπει να είναι αυστηρά περιορισμένη.

Σε ένα τέτοιο περιβάλλον η διακίνηση της πληροφορίας είναι βασικά ελεύθερη, οι δε κανόνες της διακίνησης αυτής καθορίζονται αποκλειστικά και μόνο από τους ιδιοκτήτες (ή παραγωγούς) της πληροφορίας. Επειδή οι χρήστες σε ένα τέτοιο περιβάλλον ανήκουν συνήθως σε ομάδες (ερευνητικές ομάδες, τμήματα, τομείς κτλ.), η απόφαση χορήγησης ή όχι άδειας προσπέλασης βασίζεται μόνο στην ταυτότητα των χρηστών ή/και των ομάδων στις οποίες αυτοί ανήκουν. Επιπλέον, η παροχή και ανάκληση δικαιωμάτων προσπέλασης, όπως και η δυνατότητα ενός χρήστη που έχει ήδη κάποιο συγκεκριμένο δικαίωμα προσπέλασης να το μεταβιβάσει σε έναν άλλο χρήστη (πιθανόν έμμεσα), επαφίεται στη διακριτική ευχέρεια του χρήστη, χωρίς να απαιτείται η διαμεσολάβηση του διαχειριστή συστήματος.

Ο Έλεγχος Προσπέλασης Βασισμένος σε Ρόλους (Role Based Access Control - **RBAC**) αποτελεί μια πιο γενική προσέγγιση του ελέγχου προσπέλασης. Απαιτεί τη χαρτογράφηση διαφορετικών ρόλων και τον καθορισμό μιας κατανομής δικαιωμάτων προσπέλασης στους πόρους του συστήματος για κάθε ρόλο. Κατόπιν σε κάθε χρήστη εκχωρούνται ένας ή περισσότεροι ρόλοι, παραχωρώντας του, τα δικαιώματα προσπέλασης που καθορίζονται απ' αυτούς τους ρόλους .

Εικόνα 1. Έλεγχος Προσπέλασης Βασισμένος σε Ρόλους.

Σε κάθε χρήστη ορίζονται ένας ή περισσότεροι ρόλοι και σε κάθε ρόλο ορίζονται ένα ή περισσότερα δικαιώματα προσπέλασης, τα οποία μπορούν να δοθούν στους χρήστες που ανήκουν στους συγκεκριμένους ρόλους .

Η ιδιότητα μέλους των χρηστών στους ρόλους μπορεί να ανακληθεί εύκολα και νέες ιδιότητες μέλους να εκχωρηθούν όπως απαιτείται. Έτσι απλοποιείται η διοίκηση και η διαχείριση των δικαιωμάτων, καθώς οι ρόλοι μπορούν να ενημερωθούν χωρίς να χρειάζεται ενημέρωση των δικαιωμάτων για κάθε χρήστη ξεχωριστά. Επιπλέον, η χρήση ιεραρχιών ρόλου μπορεί να παρέχει πρόσθετα πλεονεκτήματα, δεδομένου ότι ένας ρόλος μπορεί εν δυνάμει να περιλαμβάνει τις λειτουργίες που συνδέονται με έναν άλλο ρόλο.

Ο RBAC έχει πρόσφατα προταθεί ως πρότυπο NIST. Υποστηρίζει ένα μεγάλο σύνολο από εμπορικές απαιτήσεις ασφάλειας, γι' αυτό οι τύποι RBAC ευρέως χρησιμοποιούνται σε πολλές εφαρμογές, όπως λειτουργικά συστήματα και συστήματα διαχείρισης βάσεων δεδομένων. Ο Microsoft Authorization Manager, ο οποίος περιλαμβάνεται στα MS-Windows Server 2003, είναι παράδειγμα RBAC υλοποίησης.

Πλεονεκτήματα αυτού του τύπου πολιτικής ελέγχου προσπέλασης είναι η ευκολία στη διαχείριση (λιγότερες οντότητες που διαχειρίζονται), η ισχυρότερη ασφάλεια, η γρηγορότερη ανάθεση και ανάκληση προνομίων, ενώ μειονέκτημά του είναι το γεγονός ότι πρέπει να αποφασιστεί πάνω σε ποιο προϊόν ή τεχνολογία θα βασιστεί η ανάθεση ρόλου. Ο τύπος RBAC είναι ευέλικτος και ουδέτερος ως προς την πολιτική που εφαρμόζεται, δίνοντας του ένα πλεονέκτημα απέναντι στους τύπους MAC και DAC. Συμπερασματικά ο RBAC αποτελεί μια ελπιδοφόρο εναλλακτική λύση έναντι των πρότυπων MAC και DAC.

Όμως ο παραδοσιακός τύπος RBAC δεν είναι ικανός να ορίσει μια πολιτική εξουσιοδότησης με περιορισμούς περιβάλλοντος οι οποίοι πρέπει να εφαρμοστούν σε μια πολιτική προσπέλασης.

Ερευνητές προσπάθησαν να βελτιώσουν το παραδοσιακό μοντέλο RBAC προτείνοντας καινούργιους τύπους οι οποίοι λαμβάνουν υπόψη περιορισμούς περιβάλλοντος (χρόνος, χώρος). Οι τελευταίες προεκτάσεις του RBAC, για να υποστηρίξουν περιορισμούς περιβάλλοντος βελτιώσαν το παραδοσιακό μοντέλο, αλλά αυτοί οι τύποι είναι στατικοί, με μικρή ευελιξία και καθόλου επεκτασιμότητα.

Ο Έλεγχος Προσπέλασης Βασισμένος στο Περιβάλλον (Context-Based Access Control - **CBAC**) λαμβάνει υπόψην όχι μόνο το πρόσωπο που προσπαθεί να έχει προσπέλαση στα δεδομένα και τον τύπο των δεδομένων που προσπελαύνονται, αλλά και το περιβάλλον της συναλλαγής στο οποίο γίνεται η προσπάθεια προσπέλασης.

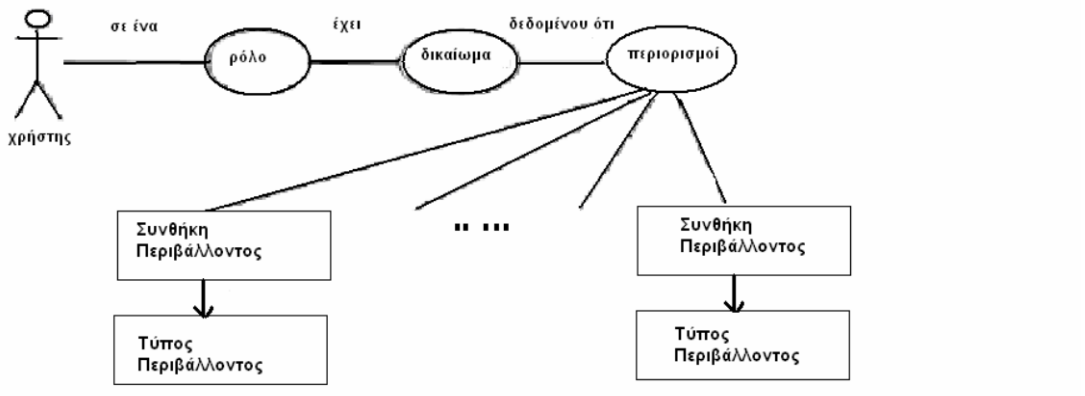
Ένα σύστημα που δεν επιτρέπει σε έναν χρήστη να έχει προσπέλαση σε έναν συγκεκριμένο πόρο περισσότερο από 100 φορές ημερησίως, είναι ένα CBAC σύστημα, δεδομένου ότι μετρά τον αριθμό των προσπελάσεων που διενεργήθηκαν και αποτρέπει όλες τις προσπελάσεις πέρα από τις πρώτες 100, άσχετα από το γεγονός ότι ο χρήστης και ο πόρος είναι οι ίδιοι.

Όπως σημειώνεται από άλλους ερευνητές ποικίλοι παράγοντες και πληροφορίες περιβάλλοντος πρέπει να εξεταστούν κατά τον επηρεασμό της επιθυμητής συμπεριφοράς ενός CBAC συστήματος κατά τη διάρκεια του χρόνου εκτέλεσης. Αυτό που απαιτείται είναι ένα ενεργό σύστημα ελέγχου προσπέλασης που υποστηρίζει εξουσιοδότηση δικαιώματος βασισμένη στο περιβάλλον.

Αν και είναι δύσκολο να δοθεί ένας ακριβής ορισμός του περιβάλλοντος, μπορεί γενικά να οριστεί ως «οποιαδήποτε πληροφορία που μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει την κατάσταση οποιασδήποτε οντότητας. Μια οντότητα είναι ένα πρόσωπο, θέση ή αντικείμενο που θεωρείται σχετικό με την αλληλεπίδραση μεταξύ ενός χρήστη και μιας εφαρμογής». Χρησιμοποιώντας αυτόν τον ορισμό, το «περιβάλλον» θα μπορούσε να είναι ο χρόνος ή ο χώρος της πρόσβασης, μια αίτηση υπό-ρόλου (π.χ., όχι μόνο ένας παθολόγος, αλλά και ένας χειρούργος), κάποια ειδική σχέση (π.χ., όχι απλά ένας παθολόγος, αλλά αυτός ο συγκεκριμένος παθολόγος του ασθενή), ή κάποιος παρόμοιος περιορισμός. Η βασική ιδέα του CBAC είναι να συνδέσει τους σχετικούς με το περιβάλλον περιορισμούς με το κάθε συστατικό του προτύπου RBAC (εικόνα 2), έτσι ώστε οι αποφάσεις εξουσιοδότησης να μπορούν να ληφθούν κατά το χρόνο εκτέλεσης, βασισμένες στις δυναμικές πληροφορίες περιβάλλοντος, παρά στο χρόνο σχεδίασης όταν μια πολιτική εξουσιοδότησης καθορίζεται αρχικά.

Μοντέλο CBAC

Οι περίπλοκες σχέσεις χρήστη-δεδομένων μέσα στα συστήματα απαιτούν μια εύκαμπτη επιβολή πολιτικής. Στο σύστημα, ο καθορισμός πολιτικής και η επιβολή πολιτικής είναι ανεξάρτητα. Ο σχεδιαστής της εφαρμογής δεν χρειάζεται να ξέρει στο χρόνο κωδικοποίησης της εφαρμογής ποιες πολιτικές προσπέλασης θα χρησιμοποιηθούν. Η υποδομή μας θα επιβάλει απλά στο χρόνο εκτέλεσης όποιες πολιτικές είναι αυτήν την περίοδο ενεργές.



Πολυάριθμοι τύποι περιβαλλόντων είναι πιθανοί, αλλά μας ενδιαφέρει κυρίως η κατάσταση του χρήστη που υποβάλλει ένα αίτημα, η κατάσταση του αντικείμενου που ζητείται και το πότε και που δημιουργείται το αίτημα. Με την προσθήκη των περιορισμών περιβάλλοντος στην πολιτική εξουσιοδότησης, η εξουσιοδότηση καθορίζεται δυναμικά βασισμένη στο τρέχον περιβάλλον του αιτήματος και όχι μόνο στο ρόλο του χρήστη.

Όπως φαίνεται και στην εικόνα, ένας περιορισμός αποτελείται από πολλαπλούς περιορισμούς, που αποκαλούνται συνθήκες περιβάλλοντος. Μια συνθήκη περιβάλλοντος ορίζεται ως ένα κατηγόρημα πάνω σε κάποιον τύπο περιβάλλοντος, η τιμή του οποίου καθορίζει εάν μια συγκεκριμένη συνθήκη ικανοποιείται. Ο τύπος περιβάλλοντος ορίζεται ως μια ιδιότητα της κατάστασης κάτω από την οποία η αίτηση προσπέλασης εκδίδεται. Σε απλές περιπτώσεις, ο τύπος περιβάλλοντος μπορεί να είναι ο χρόνος ή ο χώρος. Σε ένα πιο περίπλοκο σενάριο, ο τύπος περιβάλλοντος μπορεί επίσης να χρησιμοποιηθεί για να περιγράψει μια ιδεώδης αρχή όπως το έμπιστο επίπεδο αυθεντικοποίησης.

Στον παρακάτω πίνακα παρουσιάζονται παραδείγματα εφαρμογής των βασικών τύπων πολιτικής ελέγχου προσπέλασης σε διάφορους τομείς.

Setting	**User/Role Based**	**Context Based**	**Mandatory/ Discretionary**
ATM	Τα προνόμια συνδέονται συγκεκριμένα στο λογαριασμό του ιδιοκτήτη.	Δεν μπορείτε να αποσύρετε περισσότερο από $2500 ανά 24 ώρες	Ο λογαριασμός ιδιοκτήτη δεν μπορεί να χορηγήσει σε άλλους δικαίωμα για πρόσβαση στο λογαριασμό με την κάρτα τους
Firewall	Η πρόσβαση χορηγείται μέσω ρόλου, π.χ. υπάλληλος, υπεργολάβος, πελάτης.	Δεν επιτρέπει πρόσβαση σε εσωτερικούς πόρους δικτύου ως ότου αυθεντικοποιηθεί ο χρήστης	Ένας εσωτερικός χρήστης δεν μπορεί να χορηγήσει την πρόσβαση στα δεδομένα μέσω firewall.
Σύστημα Βάσης δεδομένων νοσοκομείου	Η πρόσβαση χορηγείται μέσω ρόλου, π.χ. Γιατρός, Νοσοκόμα,	Κανένα κατάλληλο παράδειγμα.	Ένας γιατρός ή νοσοκόμα μπορεί να χορηγήσει σε έναν συνάδελφο πρόσβαση στο αρχείο ενός ασθενή για να πάρει την άποψη του.

Λειτουργικά Συστήματα-File Servers	Η πρόσβαση στα δεδομένα χορηγείται είτε μέσω κανόνα ή συγκεκριμένα σε ένα χρήστη.	Οι χρήστες δεν μπορούν να σώσουν ένα άλλο αρχείο στον κοινό file server όταν έχουν υπερβεί την ποσόστωση τους.	Ο ιδιοκτήτης του αρχείου μπορεί συνήθως να χορηγήσει πρόσβαση στα δεδομένα του σε καθένα, ανεξάρτητα από πολιτική της επιχείρησης.

Φανταστείτε μια εταιρεία συμβούλων. Η εταιρεία αυτή παρέχει συμβουλές επιχειρηματικής φύσης σε μια σωρεία εταιρειών, διαφορετικής φύσης, καθεμία από τις οποίες έχει και το πληροφοριακό της σύστημα. Για να είναι αποτελεσματική η εταιρεία συμβούλων, πρέπει προφανώς να έχει πρόσβαση στις επιχειρηματικές πληροφορίες των πελατών της. Από την άλλη μεριά, αν έχει ήδη ως πελάτη μια εταιρεία καλλυντικών, δεν πρέπει να έχει ταυτόχρονα ως πελάτη και μια άλλη, ανταγωνιστική της πρώτης, εταιρεία του ίδιου κλάδου. Ακόμη και για κάποιο χρονικό διάστημα μετά τη λήξη της πελατειακής σχέσης, η εταιρεία συμβούλων δε θα πρέπει να μπορεί να έχει πρόσβαση σε επιχειρηματικές πληροφορίες άλλων εταιρειών καλλυντικών.

Η πολιτική του Σινικού Τείχους (Chinese Wall Access Control – **CWAC**) διαμορφώθηκε για να καλύψει την ανάγκη αυτή. Σύμφωνα με την πολιτική αυτή, η πληροφορία διακρίνεται σε δημόσια και εταιρική. Ενώ η ανάγνωση δημόσιας πληροφορίας είναι βασικά ελεύθερη, η ανάγνωση εταιρικής πληροφορίας υπόκειται σε υποχρεωτικούς ελέγχους. Η απόφαση για χορήγηση άδειας εγγραφής δημόσιας ή εταιρικής πληροφορίας προκύπτει, όπως και στην πολιτική MAC, από τις συνέπειες της πιθανής παροχής έμμεσης προσπέλασης ανάγνωσης, που παραβιάζει τους κανόνες προσπέλασης ανάγνωσης.

Ένα πληροφοριακό σύστημα που χρησιμοποιείται για υπηρεσίες συμβούλου αναπόφευκτα θα χρησιμοποιεί μεγάλες δημόσιες βάσεις δεδομένων. Επιπλέον, η ύπαρξη δημόσιας πληροφορίας επιτρέπει στο πληροφοριακό σύστημα να παρέχει διάφορες δημοφιλείς υπηρεσίες, όπως δημόσιους πίνακες ανακοινώσεων και ηλεκτρονικό ταχυδρομείο, υπηρεσίες που οι χρήστες περιμένουν να βρουν διαθέσιμες σε κάθε σύγχρονο πληροφοριακό σύστημα. Η δημόσια πληροφορία μπορεί να αναγνωστεί απ' όλους τους χρήστες, με μόνη επιφύλαξη την εφαρμογή της πολιτικής DAC.

Η εταιρική πληροφορία κατηγοριοποιείται σε μη αλληλοκαλυπτόμενες κλάσεις αντικρουόμενων συμφερόντων. Κάθε εταιρεία ανήκει σε ακριβώς μία κλάση αντικρουόμενων συμφερόντων. Η πολιτική του Σινικού Τείχους απαιτεί ότι ένας σύμβουλος δε θα πρέπει να μπορεί να διαβάσει πληροφορίες για περισσότερες από μία εταιρείες σε κάθε δεδομένη κλάση αντικρουόμενων συμφερόντων. Για να γίνει πιο κατανοητή η απαίτηση αυτή, ας υποθέσουμε ότι μια κλάση αποτελείται από τράπεζες και μια άλλη κλάση από εταιρείες καλλυντικών. Η απαίτηση της πολιτικής είναι ότι ο ίδιος σύμβουλος δεν πρέπει να έχει προσπέλαση ανάγνωσης πληροφοριών σε πληροφοριακά συστήματα περισσότερων από μία τραπεζών ή περισσότερων από μία εταιρειών καλλυντικών.

Η πολιτική Σινικού Τείχους είναι μείγμα ελεύθερης επιλογής και υποχρεωτικών περιορισμών. Όσο ένας σύμβουλος δεν έχει ακόμη διαβάσει καθόλου εταιρική πληροφορία σχετική με τράπεζες, έχει τη δυνατότητα να διαβάσει εταιρική πληροφορία για οποιαδήποτε τράπεζα. Τη στιγμή όμως που ο σύμβουλος θα διαβάσει πληροφορίες για μια συγκεκριμένη τράπεζα, θα πρέπει να του απαγορευτεί η προσπέλαση σε εταιρική πληροφορία οποιασδήποτε άλλης τράπεζας. Η ελεύθερη επιλογή της πρώτης εταιρείας σε μια κλάση αντικρουόμενων συμφερόντων μπορεί να ασκηθεί μόνο μια φορά και μετά χάνεται για πάντα (ή, τουλάχιστον, για κάποιο μεγάλο χρονικό διάστημα).

Συνοπτικά, οι κανόνες απόφασης για τη χορήγηση άδειας προσπέλασης στην πολιτική CWAC μπορούν να διατυπωθούν ως εξής. Άδεια προσπέλασης χορηγείται αν:

- η πληροφορία την οποία αφορά ανήκει στην ίδια κλάση αντικρουόμενων συμφερόντων με κάποια άλλη πληροφορία που ήδη έχει προσπελάσει ο ίδιος χρήστης ή σε κλάση αντικρουόμενων συμφερόντων για την οποία ο χρήστης δεν έχει ακόμη αποκτήσει άδεια προσπέλασης και

- δεν είναι δυνατόν να αναγνωστεί πληροφορία που ανήκει σε διαφορετική κλάση αντικρουόμενων συμφερόντων απ' αυτή για την οποία ζητείται άδεια εγγραφής.

2.4 ΜΟΝΤΕΛΑ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ

Μέχρι στιγμής είδαμε πέντε διαφορετικές πολιτικές ελέγχου προσπέλασης. Αναφερθήκαμε στις πολιτικές αυτές περιγραφικά. Μερικές φορές είναι όμως χρήσιμο, ή και απαραίτητο, να μπορούμε να εκφράσουμε τις πολιτικές και με
μαθηματικό φορμαλισμό, επειδή, για παράδειγμα, θέλουμε να μπορούμε να αποδείξουμε κάποιες ιδιότητές τους.

Για το λόγο αυτό αναπτύχθηκαν, κατά καιρούς, αρκετά φορμαλιστικά μοντέλα πολιτικών ελέγχου προσπέλασης. Τα μοντέλα αυτά μπορούν να κατηγοριοποιηθούν με διάφορους τρόπους. Ο τρόπος που θα τα κατηγοριοποιήσουμε είναι ανάλογα με το μαθηματικό τους υπόβαθρο και ανάλογα με τη λειτουργικότητά τους. Δεδομένο ότι τα φορμαλιστικά μοντέλα αποδεικνύονται μόνο με μαθηματικούς τύπους, εδώ θα γίνει μια αναφορά μόνο στη σπουδαιότητα του καθενός.

1. Μοντέλο Bell–LaPadula

Την ασφαλή ροή πληροφορίας την εξασφαλίζουν δυο ιδιότητες με αυτό το μοντέλο. Η πρώτη, γνωστή και ως απλή ιδιότητα ασφάλειας, ορίζει ότι ένα υποκείμενο μπορεί να αποκτήσει άδεια προσπέλασης ανάγνωσης ενός αντικειμένου. Η δεύτερη, γνωστή και ως ιδιότητα, ορίζει ότι ένα υποκείμενο που έχει άδεια προσπέλασης ανάγνωσης σε ένα αντικείμενο μπορεί να αποκτήσει άδεια προσπέλασης εγγραφής σε άλλο αντικείμενο.

Το μοντέλο Bell–LaPadula μπορεί να περιγράψει φορμαλιστικά την πολιτική MAC ως προς την εμπιστευτικότητα.

2. Μοντέλο Biba

Το μοντέλο Bell–LaPadula αναφέρεται μόνο στην εμπιστευτικότητα της πληροφορίας. Ο Biba κατασκεύασε ένα αντίστοιχο μοντέλο που αναφέρεται στην ακεραιότητα της πληροφορίας. Το μοντέλο Biba είναι δυϊκό του μοντέλου Bell–LaPadula, με την έννοια ότι ορίζει βαθμούς ακεραιότητας της πληροφορίας ανάλογους με τους βαθμούς ευαισθησίας.

Το μοντέλο Biba μπορεί να περιγράψει φορμαλιστικά την πολιτική MAC ως προς την ακεραιότητα.

3. Μοντέλο Σινικού τείχους

Αν και η αρχική διατύπωση του μοντέλου αυτού δεν έγινε φορμαλιστικά, ο Sandhu απέδειξε ότι ένα δικτύωμα μπορεί να χρησιμοποιηθεί για το σκοπό αυτό.

Το μοντέλο Σινικού τείχους απέδειξε ότι μη συμβατοί βαθμοί ασφάλειας δεν
μπορούν να συνδυαστούν στην πολιτική CWAC.

4. Μοντέλο Clark–Wilson

Το μοντέλο αυτό χρησιμοποιήθηκε για να περιγράψει μη στρατιωτικές πολιτικές ελέγχου προσπέλασης, όπως είναι η πολιτική DAC, αναφέρεται δε στην ακεραιότητα της πληροφορίας. Πιο συγκεκριμένα, ο σκοπός του μοντέλου είναι να εξασφαλίσει ότι η εσωτερική πληροφορία του συστήματος είναι συνεπής σε σχέση με τις προσδοκίες των εξωτερικών χρηστών.

Στα, μη στρατιωτικά, εμπορικά περιβάλλοντα η ακεραιότητα είναι τουλάχιστον εξίσου σημαντική με την εμπιστευτικότητα. Οι Clark και Wilson πρότειναν ένα μοντέλο πολιτικής ελέγχου προσπέλασης βασισμένο σ' αυτό που ονομάζουν καλά σχηματισμένη συναλλαγή, η οποία είναι μια ολοκληρωμένη ενέργεια, που αποτελείται από βήματα τα οποία εκτελούνται επακριβώς και με τη σωστή σειρά από κατάλληλα εξουσιοδοτημένους και ταυτοποιημένους χρήστες.

Η πολιτική παρουσιάζεται συναρτήσει δεδομένων υπό περιορισμούς, τα οποία υφίστανται επεξεργασία από διαδικασίες μετασχηματισμού. Οι διαδικασίες αυτές μοιάζουν με μηχανισμούς παρακολούθησης, με την έννοια ότι εκτελούν μόνο συγκεκριμένες λειτουργίες επί συγκεκριμένων δεδομένων, τα οποία μπορούν να τύχουν επεξεργασίας μόνο από τέτοιες διαδικασίες. Οι διαδικασίες επαλήθευσης ακεραιότητας εξασφαλίζουν τη διατήρηση της ακεραιότητας των δεδομένων. Οι Clark και Wilson πρότειναν τον ορισμό της πολιτικής συναρτήσει τρισδιάστατων διανυσμάτων προσπέλασης, που αποτελούνται από την ταυτότητα χρήστη, τη διαδικασία μετασχηματισμού και τα δεδομένα.

Το μοντέλο χρησιμοποιεί πέντε κανόνες πιστοποίησης:

- Οι διαδικασίες επαλήθευσης ακεραιότητας πρέπει να εξασφαλίζουν το γεγονός ότι όλα τα δεδομένα υπό περιορισμούς βρίσκονται σε έγκυρη κατάσταση, όταν εκτελείται η διαδικασία επαλήθευσης ακεραιότητας.
- Οι διαδικασίες μετασχηματισμού πρέπει να είναι πιστοποιημένα έγκυρες, δηλαδή έγκυρα δεδομένα υπό περιορισμούς πάντα μετασχηματίζονται σε έγκυρα δεδομένα υπό περιορισμούς. Κάθε διαδικασία μετασχηματισμού είναι πιστοποιημένη προσπέλαση ενός συγκεκριμένου συνόλου δεδομένων υπό περιορισμούς.
- Οι κανόνες προσπέλασης πρέπει να ικανοποιούν τις απαιτήσεις της αρχής διαχωρισμού καθηκόντων.
- Όλες οι διαδικασίες μετασχηματισμού πρέπει να κάνουν προσθετικές μόνο εγγραφές σε ένα ημερολόγιο.
- Κάθε διαδικασία μετασχηματισμού που παίρνει δεδομένα χωρίς περιορισμούς ως είσοδο πρέπει είτε να τα μετατρέψει σε δεδομένα υπό περιορισμούς είτε να απορρίψει τα δεδομένα χωρίς περιορισμούς και να μην κάνει κανένα μετασχηματισμό.

5. Μοντέλο Graham–Denning

Το μοντέλο αυτό χρησιμοποιεί οκτώ βασικές πράξεις για να ελέγξει τη ροή πληροφοριών μεταξύ υποκειμένων και αντικειμένων σ' ένα σύστημα:

- Δημιουργία αντικειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο αντικείμενο.
- Δημιουργία υποκειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο υποκείμενο.
- Διαγραφή υποκειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να διαγράψει ένα υποκείμενο.
- Διαγραφή αντικειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να διαγράψει ένα αντικείμενο.

➢ Ανάγνωση δικαιώματος προσπέλασης. Με την πράξη αυτή ένα υποκείμενο μπορεί να πληροφορηθεί τα δικαιώματα ανάγνωσης ενός άλλου υποκειμένου (ή του εαυτού του) σε κάποιο αντικείμενο.

➢ Παραχώρηση δικαιώματος προσπέλασης. Με την πράξη αυτή ο ιδιοκτήτης ενός αντικειμένου καθορίζει τα δικαιώματα προσπέλασης οποιουδήποτε άλλου υποκειμένου στο αντικείμενο.

➢ Ανάκληση δικαιώματος προσπέλασης. Με την πράξη αυτή ο ιδιοκτήτης ενός αντικειμένου αίρει τα δικαιώματα προσπέλασης οποιουδήποτε άλλου υποκειμένου στο αντικείμενο.

➢ Μεταβίβαση δικαιώματος προσπέλασης. Με την πράξη αυτή ένα υποκείμενο μπορεί να μεταβιβάσει τα δικαιώματα προσπέλασης που έχει σε κάποιο αντικείμενο σε άλλο υποκείμενο. Τα δικαιώματα που μεταβιβάζονται μπορούν να είναι περαιτέρω μεταβιβάσιμα ή όχι.

6. Μοντέλο Harrison–Ruzzo–Ullman

Το μοντέλο αυτό αποτελεί γενίκευση του προηγούμενου και βασίζεται σε έξι βασικές πράξεις:

➢ Δημιουργία αντικειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο αντικείμενο.

➢ Δημιουργία υποκειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο υποκείμενο.

➢ Διαγραφή υποκειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να διαγράψει ένα υποκείμενο.

➢ Διαγραφή αντικειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να διαγράψει ένα αντικείμενο.

➢ Παραχώρηση δικαιώματος προσπέλασης. Με την πράξη αυτή ο ιδιοκτήτης ενός αντικειμένου καθορίζει τα δικαιώματα προσπέλασης οποιουδήποτε άλλου υποκειμένου στο αντικείμενο.

➢ Ανάκληση δικαιώματος προσπέλασης. Με την πράξη αυτή ο ιδιοκτήτης ενός αντικειμένου αίρει τα δικαιώματα προσπέλασης οποιουδήποτε άλλου υποκειμένου στο αντικείμενο.

7. Μοντέλο Take–Grant

Το μοντέλο υποστηρίζει τις εξής πράξεις:

➢ Δημιουργία αντικειμένου. Με την πράξη αυτή ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο αντικείμενο.

➢ Ανάκληση δικαιώματος προσπέλασης. Με την πράξη αυτή αίρονται τα δικαιώματα προσπέλασης οποιουδήποτε υποκειμένου σε οποιοδήποτε αντικείμενο.

➢ Παραχώρηση δικαιώματος προσπέλασης. Με την πράξη αυτή το υποκείμενο που έχει δικαίωμα προσπέλασης σε ένα αντικείμενο παραχωρεί σ' αυτό (που τώρα γίνεται υποκείμενο) το δικαίωμα προσπέλασης που έχει σε άλλο αντικείμενο.

➢ Ανάκληση δικαιώματος προσπέλασης. Με την πράξη αυτή αναιρείται η παραχώρηση δικαιώματος προσπέλασης.

2.5 ΜΗΧΑΝΙΣΜΟΙ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Αφού αναφέραμε τις διάφορες πολιτικές ελέγχου προσπέλασης και τα φορμαλιστικά μοντέλα που τις περιγράφουν, τώρα μπορούμε να παρουσιάσουμε τους μηχανισμούς που μπορούμε να χρησιμοποιήσουμε για να υλοποιήσουμε κάποια, οποιαδήποτε, πολιτική ελέγχου προσπέλασης. Η παρουσίαση αυτή θα γίνει σε σειρά αύξουσας πολυπλοκότητας, αλλά και ταυτόχρονα αύξουσας λειτουργικότητας των μηχανισμών.

Μια απλή δομή ελέγχου προσπέλασης λειτουργεί όπως ένα **ευρετήριο**. Φανταστείτε ότι το σύνολο των αντικειμένων είναι αρχεία και το σύνολο των υποκειμένων χρήστες ενός υπολογιστικού συστήματος. Κάθε αρχείο έχει ένα μοναδικό ιδιοκτήτη, ο οποίος έχει το δικαίωμα να καθορίζει τα δικαιώματα προσπέλασης, συμπεριλαμβανομένου του δικαιώματος να καθορίζει ποιος έχει ποια δικαιώματα και να αφαιρεί το δικαίωμα προσπέλασης από οποιονδήποτε, όποτε θέλει. Κάθε χρήστης έχει ένα ευρετήριο αρχείων, που περιέχει κατάλογο όλων των αρχείων για τα οποία ο χρήστης έχει κάποιο δικαίωμα προσπέλασης.

Προφανώς σε κανένα χρήστη δεν μπορεί να επιτρέπεται να κάνει εγγραφή στο ευρετήριο αρχείων, γιατί έτσι θα μπορούσε να παραχαράξει δικαιώματα προσπέλασης

σε κάποιο αρχείο. Επομένως, το λειτουργικό σύστημα πρέπει να επιτρέπει την εκτέλεση πράξεων σε όλα τα ευρετήρια αρχείων μόνο με εντολές των ιδιοκτητών των αρχείων. (Αυτό μπορεί να γίνει προσθέτοντας στα γνωστά δικαιώματα προσπέλασης αρχείων (read – R, write – W, execute – X) ένα ακόμη δικαίωμα, το owner – O, που δίνεται στον ιδιοκτήτη και του επιτρέπει να χορηγεί και να αφαιρεί δικαιώματα προσπέλασης (βλέπε παράρτημα).

Η προσέγγιση αυτή υλοποιείται εύκολα, γιατί χρησιμοποιεί μια λίστα ανά χρήστη, λίστα που έχει καταγραμμένα όλα τα αντικείμενα τα οποία ο χρήστης επιτρέπεται να προσπελάσει. Ωστόσο, η λίστα γίνεται πολύ μεγάλη αν υπάρχουν πολλά αντικείμενα που πρέπει να είναι προσπελάσιμα από όλους τους χρήστες, όπως, για παράδειγμα, βιβλιοθήκες υποπρογραμμάτων. Τότε, το ευρετήριο κάθε χρήστη πρέπει να έχει μια εγγραφή για κάθε τέτοιο αντικείμενο, ακόμη και αν ο χρήστης δεν έχει την πρόθεση να το προσπελάσει.

Μια άλλη δυσκολία είναι η αφαίρεση δικαιωμάτων προσπέλασης. Αν κάποιος ιδιοκτήτης ενός αρχείου έχει χορηγήσει σ' ένα χρήστη δικαίωμα ανάγνωσης ενός αρχείου, θα γίνει μια εγγραφή για το αρχείο στο ευρετήριο του χρήστη. Η πράξη αυτή σημαίνει ότι υπάρχει κάποια εμπιστοσύνη ανάμεσα στον ιδιοκτήτη και στο χρήστη. Αν, όμως, αργότερα ο ιδιοκτήτης χάσει την εμπιστοσύνη αυτή, μπορεί να θελήσει να αφαιρέσει το δικαίωμα προσπέλασης του χρήστη στο αρχείο. Το λειτουργικό σύστημα μπορεί εύκολα να ικανοποιήσει τη μοναδική αίτηση διαγραφής του δικαιώματος κάποιου χρήστη να προσπελάζει κάποιο αρχείο, γιατί αυτό απλώς σημαίνει τη διαγραφή μιας εγγραφής από ένα συγκεκριμένο ευρετήριο. Μέχρι εδώ, λοιπόν, κανένα πρόβλημα.

Αν, όμως, ο ιδιοκτήτης θελήσει να αφαιρέσει το δικαίωμα προσπέλασης από όλους όσοι έχουν το δικαίωμα να προσπελάζουν το αρχείο, το λειτουργικό σύστημα πρέπει να ψάξει μέσα σε όλα τα ευρετήρια, πράγμα που μπορεί να πάρει πάρα πολύ χρόνο σε ένα μεγάλο σύστημα. Για να γίνουν τα πράγματα χειρότερα, σκεφτείτε ότι ο ιδιοκτήτης δεν έχει τρόπο να γνωρίζει αν ο χρήστης μεταβίβασε το δικαίωμα προσπέλασης του αρχείου και σε κάποιον άλλο. Το πρόβλημα αυτό είναι εντονότερο σε κατανεμημένα συστήματα. Μια τρίτη δυσκολία είναι τα ψευδώνυμα.

Θεωρήστε δύο ιδιοκτήτες, Α και Β, που έχουν δύο διαφορετικά αρχεία τα οποία συμβαίνει να έχουν το ίδιο όνομα, Γ, και που θέλουν να παραχωρήσουν δικαίωμα προσπέλασης σ' αυτά στο χρήστη Δ. Προφανώς το ευρετήριο του Δ δεν μπορεί να περιέχει δύο εγγραφές με το ίδιο όνομα αρχείου. Επομένως, ο Δ πρέπει ναείναι σε θέση να ξεχωρίσει το Γ του Α από το Γ του Β. Μια λύση σ' αυτό είναι να συμπεριλάβει κανείς και το όνομα του ιδιοκτήτη στο πλήρες όνομα του αρχείου, για παράδειγμα χρησιμοποιώντας το συμβολισμό Α:Γ και Β:Γ.

Ας υποθέσουμε όμως ότι ο Δ έχει αδύνατη μνήμη κάτι πολύ συνηθισμένο και δεν μπορεί να θυμηθεί τι περιέχει το αρχείο μόνο από το όνομά του (Γ). Θα πρέπει, για να μην απογοητεύσουμε τέτοιους χρήστες, να επιτρέψουμε στον Δ να ονομάσει το Γ με κάποιο άλλο όνομα, μοναδικό στο δικό του ευρετήριο, που να θυμίζει με κάποιον τρόπο τα περιεχόμενά του. Αν, όμως, το κάνουμε αυτό, τότε το Γ του Α μπορεί να ονομάζεται Ε στο ευρετήριο του Δ. Ο Δ όμως μπορεί να ξεχάσει ότι το Ε ανήκει στον Α και μπορεί να ξαναζητήσει δικαιώματα προσπέλασης του Γ από τον Α. Αλλά, στο μεταξύ, λόγω καλής συμπεριφοράς, ο Α εμπιστεύεται τον Δ περισσότερο, οπότε του δίνει περισσότερα δικαιώματα προσπέλασης στο Γ από πριν. Τι έχει γίνει τώρα; Ο ίδιος χρήστης έχει δύο διαφορετικά σύνολα δικαιωμάτων προσπέλασης για το ίδιο αρχείο! Βλέπουμε, λοιπόν, ότι, επιτρέποντας τη χρήση ψευδωνύμων, κινδυνεύουμε να καταλήξουμε σε πολλαπλά δικαιώματα προσπέλασης, όχι απαραίτητα συμβατά μεταξύ τους.

Μετά απ' όλ' αυτά, θα πρέπει, φοβάμαι, να συμπεράνουμε ότι η προσέγγιση του ευρετηρίου είναι πολύ απλοϊκή για να αποτελέσει σοβαρό υποψήφιο υλοποίησης
πολιτικών ελέγχου προσπέλασης.

Η επόμενη δομή που θα κοιτάξουμε είναι η **λίστα ελέγχου προσπέλασης**. Ορίζεται μια τέτοια λίστα για κάθε αντικείμενο και περιέχει όλα τα υποκείμενα που έχουν δικαιώματα προσπέλασης στο αντικείμενο και τα δικαιώματα του καθενός. Η δομή αυτή διαφέρει από το ευρετήριο, γιατί υπάρχει μια λίστα ανά αντικείμενο, ενώ το ευρετήριο κατασκευάζεται ανά υποκείμενο. Αν και η διαφορά μοιάζει μικρή, υπάρχουν ωστόσο σημαντικές διαφορές.(βλέπε παράρτημα παράδειγμα λίστας ελέγχου προσπέλασης).

Για παράδειγμα, αν δύο υποκείμενα έχουν δικαίωμα προσπέλασης σε κάποιο αντικείμενο, το λειτουργικό σύστημα θα κρατήσει μόνο μία λίστα για το αντικείμενο που περιέχει τα δικαιώματα προσπέλασης και για τα δύο υποκείμενα. Η λίστα μπορεί,
μάλιστα, να έχει γενικές προκαθορισμένες εγγραφές για οποιοδήποτε υποκείμενο. Με τον τρόπο αυτό συγκεκριμένα υποκείμενα μπορούν να έχουν ρητά καθορισμένα δικαιώματα και όλα τα άλλα υποκείμενα ένα σύνολο προκαθορισμένων δικαιωμάτων. Με την οργάνωση αυτή ένα δημόσιο αρχείο ή πρόγραμμα μπορεί να διαμοιράζεται ανάμεσα σε όλους τους δυνατούς χρήστες του συστήματος χωρίς να χρειάζεται να γίνει εγγραφή για το αντικείμενο στο ατομικό ευρετήριο κάθε χρήστη.

Η λίστα ελέγχου προσπέλασης λύνει τα προβλήματα των ευρετηρίων, αλλά δημιουργεί ένα άλλο: το να βρούμε όλα τα δικαιώματα που έχει ένα υποκείμενο (κάτι
που θα χρειαστούμε αν, για παράδειγμα, θελήσουμε να τα αφαιρέσουμε) είναι πολύ
δύσκολο, αφού θα πρέπει να ψάξουμε στις λίστες προσπέλασης όλων των αντικειμένων του συστήματός μας.

Το ευρετήριο και η λίστα ελέγχου προσπέλασης είναι στην ουσία ισοδύναμες δομές (περιέχουν την ίδια πληροφορία) που διαφέρουν μόνο ως προς την οργάνωσή τους. Το μεν ευρετήριο είναι οργανωμένο ως προς τα υποκείμενα, ενώ η λίστα ελέγχου προσπέλασης είναι οργανωμένη ως προς τα αντικείμενα. Η διαφοροποίηση αυτή κάνει τη χρήση τους ευκολότερη σε διαφορετικές καταστάσεις. Μια εναλλακτική λύση είναι ο **πίνακας ελέγχου προσπέλασης**. Αυτός είναι ένας πίνακας του οποίου κάθε γραμμή αντιπροσωπεύει ένα υποκείμενο και κάθε στήλη ένα αντικείμενο. Κάθε εγγραφή είναι το σύνολο των δικαιωμάτων προσπέλασης που έχει το υποκείμενο στο αντικείμενο. (βλέπε παράρτημα ένα παράδειγμα πίνακα ελέγχου προσπέλασης).

Γενικά, οι πίνακες αυτοί είναι αραιοί, επειδή τα περισσότερα υποκείμενα δεν έχουν δικαιώματα προσπέλασης στα περισσότερα αντικείμενα. Ο πίνακας αυτός μπορεί να αναπαρασταθεί ως ένα σύνολο τριάδων της μορφής {υποκείμενο, αντικείμενο, δικαιώματα}. Η έρευνα σ' ένα μεγάλο αριθμό τέτοιων τριάδων είναι τόσο αναποτελεσματική, που η δομή αυτή σπάνια χρησιμοποιείται.

Δυνατότητα είναι ένα αντικείμενο που δεν μπορεί να παραχαραχθεί και δίνει στον κάτοχό του δικαιώματα επί ενός αντικειμένου. Η δυνατότητα είναι το ηλεκτρονικό ανάλογο του εισιτηρίου κινηματογράφου ή του δελτίου ταυτότητας, που θεωρητικά δεν μπορεί να αντιγραφεί.

Η ιδέα για τη χρήση δυνατοτήτων οφείλεται στη διαπίστωση ότι θεωρητικά ένα υποκείμενο πρέπει να μπορεί να δημιουργήσει νέα αντικείμενα και να μπορεί να

καθορίσει τι λειτουργίες επιτρέπονται πάνω σ' αυτά τα αντικείμενα. Είναι βέβαιο ότι κάθε υποκείμενο ενός συστήματος μπορεί να δημιουργήσει νέα αντικείμενα, όπως αρχεία, τμήματα δεδομένων ή υποδιεργασίες, και να καθορίσει τις επιτρεπόμενες λειτουργίες στα δημιουργήματά του, λειτουργίες όπως read, write, execute. Αλλά κάθε υποκείμενο θα πρέπει να μπορεί επίσης να δημιουργήσει εντελώς νέα αντικείμενα (όπως νέες δομές δεδομένων) και να ορίσει τρόπους προσπέλασης που

δεν ήταν μέχρι τότε γνωστές στο σύστημα. Ο χειρισμός αυτών των καταστάσεων δεν είναι δυνατόν να γίνει με στατικές δομές ελέγχου προσπέλασης, όπως αυτές που

μέχρι τώρα έχουμε αναφέρει.

Όπως είπαμε, μια δυνατότητα είναι ένα εισιτήριο που δίνει την άδεια σε ένα υποκείμενο να προσπελάσει με ένα συγκεκριμένο τρόπο ένα αντικείμενο. Οι δυνατότητες δημιουργούνται μόνο μετά από ειδική αίτηση ενός υποκειμένου προς το λειτουργικό σύστημα. Για να είναι αποτελεσματική η δυνατότητα, πρέπει να μην είναι δυνατόν να πλαστογραφηθεί. Ένας τρόπος για να γίνει αυτό είναι να δώσουμε τη δυνατότητα κατευθείαν στο υποκείμενο. Εναλλακτικά, το λειτουργικό σύστημα μπορεί να κρατάει όλες τις δυνατότητες για λογαριασμό των υποκειμένων και να επιστρέφει στο υποκείμενο ένα δείκτη σε μια δομή δεδομένων του λειτουργικού συστήματος, που επίσης συνδέεται με το υποκείμενο.

Ένα από τα δικαιώματα προσπέλασης αντικειμένων είναι το δικαίωμα μεταβίβασης *ή* διάδοσης. Υποκείμενα που έχουν αυτό το δικαίωμα μπορούν να μεταβιβάσουν αντίγραφα των δυνατοτήτων τους σε άλλα υποκείμενα. Θυμηθείτε ότι καθεμιά απ' αυτές τις δυνατότητες περιέχει μια λίστα δικαιωμάτων προσπέλασης, ένα από τα οποία μπορεί να είναι επίσης το δικαίωμα μεταβίβασης. Αν είναι έτσι, μια διεργασία μπορεί να μεταβιβάσει ένα αντίγραφο δυνατότητας σε μια άλλη διεργασία, που με τη σειρά της μπορεί να τη μεταβιβάσει σε μια τρίτη. Η δεύτερη διεργασία μπορεί να απαγορεύσει περαιτέρω διανομή της δυνατότητας (και, κατά συνέπεια, περαιτέρω διάχυση του δικαιώματος προσπέλασης) παραλείποντας το δικαίωμα μεταβίβασης από τα δικαιώματα που μεταβιβάζει στη δυνατότητα για την τρίτη διεργασία. Έτσι, η δεύτερη διεργασία μπορεί ακόμη να μεταβιβάσει κάποια δικαιώματα στην τρίτη διεργασία, αλλά όχι το δικαίωμα να διαδώσει δικαιώματα προσπέλασης σε άλλα υποκείμενα.

Επιχειρησιακά, οι δυνατότητες μας επιτρέπουν να κρατάμε εύκολα λογαριασμό των δικαιωμάτων υποκειμένων σε αντικείμενα κατά τη διάρκεια της εκτέλεσης. Οι δυνατότητες συνήθως υποστηρίζονται και από ένα πιο εύληπτο πίνακα, όπως είναι ένας **πίνακας ελέγχου προσπέλασης** ή μια **λίστα ελέγχου προσπέλασης.** Κάθε φορά που μια διεργασία ζητάει να χρησιμοποιήσει ένα νέο αντικείμενο, το λειτουργικό σύστημα εξετάζει την κύρια λίστα αντικειμένων και υποκειμένων για να καθορίσει αν το αντικείμενο είναι προσπελάσιμο. Αν ναι, το λειτουργικό σύστημα δημιουργεί μια δυνατότητα για το αντικείμενο. Προκειμένου να προστατευτεί η μνήμη, κατά την εκτέλεση μόνο οι δυνατότητες αντικειμένων που έχουν ήδη προσπελαστεί από την τρέχουσα διεργασία κρατιούνται έτοιμες για χρήση. Ο περιορισμός αυτός βελτιώνει την ταχύτητα ελέγχου προσπέλασης.

Οι δυνατότητες μπορούν και να ανακαλούνται. Όταν το υποκείμενο που εξέδωσε μια δυνατότητα την ανακαλεί, δεν πρέπει να επιτρέπεται περαιτέρω προσπέλαση με βάση τη δυνατότητα αυτή. Αυτό μπορεί να εξασφαλιστεί κρατώντας έναν πίνακα δυνατοτήτων με δείκτες προς τις ενεργές δυνατότητες, έτσι ώστε το λειτουργικό σύστημα να μπορεί να ιχνηλατήσει ποια δικαιώματα προσπέλασης πρέπει να αναιρεθούν αν ανακληθεί μια δυνατότητα. Παρόμοιο είναι και το πρόβλημα της διαγραφής δυνατοτήτων μη ενεργών υποκειμένων.

Ένας στόχος του ελέγχου προσπέλασης είναι να περιορίσουμε όχι μόνο ποια υποκείμενα έχουν πρόσβαση σε ένα αντικείμενο, αλλά και τι κάνουν με το αντικείμενο αυτό. Η προσπέλαση ανάγνωσης ή εγγραφής μπορεί εύκολα να ελεγχθεί από τα περισσότερα λειτουργικά συστήματα, αλλά πιο πολύπλοκος έλεγχος είναι δύσκολο να επιτευχθεί.

Με τον όρο **έλεγχος προσπέλασης μέσω διαδικασίας** εννοούμε ότι υπάρχει μια διαδικασία που ελέγχει την προσπέλαση σε αντικείμενα. Νοητά, η διαδικασία αυτή σχηματίζει μια προστατευτική κάψουλα γύρω από το αντικείμενο και επιτρέπει μόνο συγκεκριμένους και καθορισμένους τύπους προσπέλασης σ' αυτό. Οι διαδικασίες μπορούν να εξασφαλίσουν ότι οι προσπελάσεις σε ένα αντικείμενο θα γίνονται μόνο μέσω μιας έμπιστης διεπαφής.

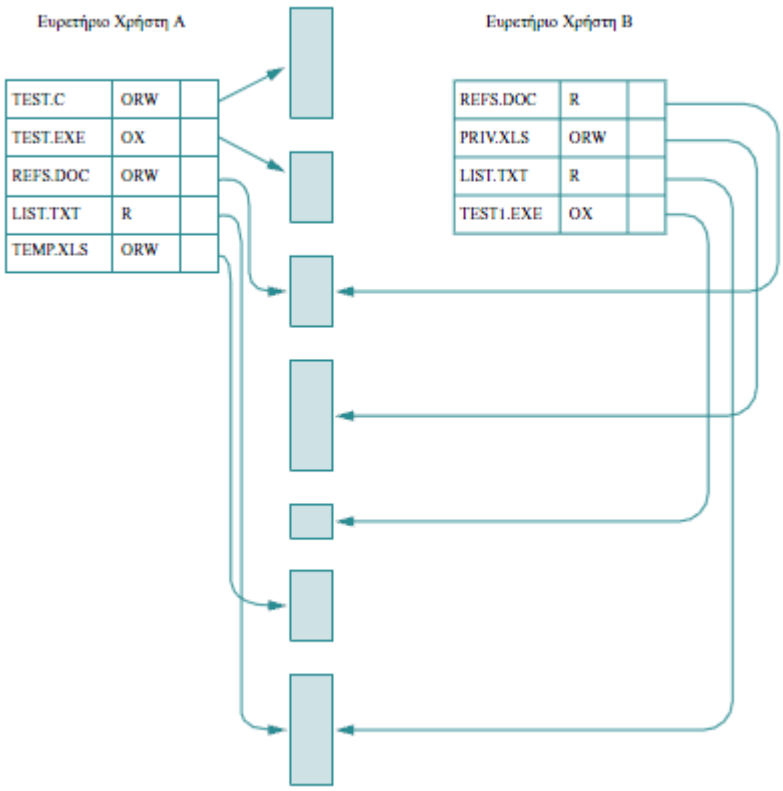
Για παράδειγμα, ούτε χρήστες ούτε γενικές ρουτίνες του λειτουργικού συστήματος επιτρέπεται να έχουν απευθείας πρόσβαση στον πίνακα έγκυρων χρηστών. Οι μόνες προσπελάσεις μπορούν να γίνουν μέσω τριών διαδικασιών, μία για να προσθέτει ένα χρήστη, μία για να διαγράφει ένα χρήστη και μία για να ελέγχει αν ένα συγκεκριμένο όνομα αντιστοιχεί σε έγκυρο χρήση. Οι διαδικασίες αυτές μπορεί να χρησιμοποιούν τους δικούς τους ελέγχους για να διαπιστώσουν αν οι κλήσεις που τους γίνονται είναι νόμιμες. Ο μηχανισμός αυτός αποτελεί υλοποίηση της ιδέας της ασφάλειας μέσω απόκρυψης πληροφορίας, επειδή ο τρόπος υλοποίησης ενός αντικειμένου είναι γνωστός μόνο στη διαδικασία ελέγχου του αντικειμένου. Φυσικά, υπάρχει και τίμημα αποτελεσματικότητας: δεν είναι δυνατόν να υπάρξει απλή, γρήγορη προσπέλαση, ακόμη και αν το αντικείμενο χρησιμοποιείται συχνά.

2.6 ΕΠΙΛΟΓΟΣ

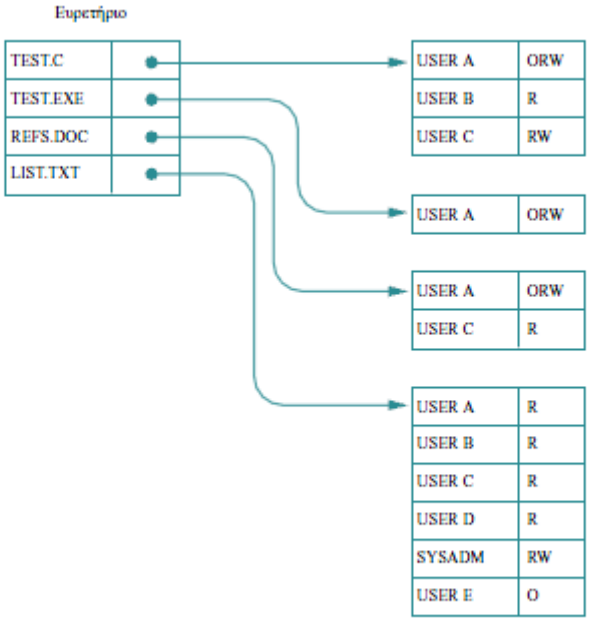
Στο κεφάλαιο αυτό ασχοληθήκαμε με τον έλεγχο προσπέλασης. Αφού πρώτα αναφέραμε γιατί είναι απαραίτητη η ύπαρξη ενός μηχανισμού ελέγχου προσπέλασης σε κάθε υπολογιστικό σύστημα, επεκτείναμε το πεδίο εφαρμογής του μηχανισμού αυτού από τους «χρήστες» και τις «πληροφορίες» στα «υποκείμενα» και τα «αντικείμενα» ενός συστήματος. Έχοντας διακρίνει τις έννοιες αυτές, προχωρήσαμε να δούμε πέντε διαφορετικές πολιτικές ελέγχου προσπέλασης, καθεμιά από τις οποίες αναπτύχθηκε για να καλύψει τις ανάγκες ενός διαφορετικού τύπου περιβάλλοντος. Συγκεκριμένα, αναπτύξαμε την πολιτική υποχρεωτικού ελέγχου προσπέλασης, την πολιτική διακριτικού ελέγχου προσπέλασης, τον έλεγχο προσπέλασης βασισμένο στο περιβάλλον, τη ρολοκεντρική πολιτική ελέγχου προσπέλασης και την πολιτική Σινικού Τείχους. Στη συνέχεια είδαμε πώς αυτές οι πολιτικές μπορούν να περιγραφούν και φορμαλιστικά, χρησιμοποιώντας μαθηματικά μοντέλα, και περιγράψαμε τα πιο σημαντικά απ' αυτά, δηλαδή τα μοντέλα Bell–LaPadula, Biba, Σινικού Τείχους, Clark–Wilson, Graham–Denning, Harrison–Ruzzo–Ullman και Ανάκλησης–Παραχώρησης. Τέλος κλείσαμε με μια αναφορά σε μια ποικιλία μηχανισμών που μπορούν να χρησιμοποιηθούν για να υλοποιηθεί μια πολιτική ελέγχου προσπέλασης, οι κυριότεροι από τους οποίους είναι τα ευρετήρια, οι λίστες ελέγχου προσπέλασης, οι πίνακες ελέγχου προσπέλασης, οι δυνατότητες και ο έλεγχος προσπέλασης μέσω διαδικασίας.

2.7 ΠΑΡΑΡΤΗΜΑ

1. ΕΥΡΕΤΗΡΙΑ



2. ΛΙΣΤΑ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ



3. ΠΙΝΑΚΑΣ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ

	TEST.C	TEST.EXE	REFS.DOC	LIST.TXT
USER A	ORW	ORW	ORW	R
USER B	R	—	—	R
USER C	RW	—	R	R
USER D	—	—	—	R
USER E	—	—	—	O
SYSADM	—	—	—	RW

ΚΕΦΑΛΑΙΟ 3 :

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

3.1 ΕΙΣΑΓΩΓΗ

Η έννοια του κακόβουλου λογισμικού είναι σύνθετη δεδομένου ότι ένα λογισμικό δεν παράγεται να έχει βούληση. Αλλά για να εξερευνήσουμε όλες τις πιθανές ερμηνείες του κακόβουλου καλό θα ήταν να αρχίζαμε πρώτα από το λογισμικό. Συνάμα 'Με τον όρο λογισμικό υπολογιστών, ή λογισμικό (software) ορίζεται η συλλογή από προγράμματα υπολογιστών, διαδικασίες και οδηγίες χρήσης που εκτελούν ορισμένες εργασίες σε ένα υπολογιστικό σύστημα. Το λογισμικό συστήματος επιβοηθά τη λειτουργία του υλικού του υπολογιστή και του υπολογιστικού συστήματος. Περιλαμβάνει λειτουργικά συστήματα, οδηγούς συσκευών (drivers), διαγνωστικά εργαλεία, servers, βοηθητικά προγράμματα και άλλα. Σκοπός του λογισμικού συστήματος είναι η απομάκρυνση του προγραμματιστή όσο το δυνατόν περισσότερο από την διαχείριση των πολύπλοκων στοιχείων του υπολογιστή, π.χ. η κύρια μνήμη και άλλα χαρακτηριστικά του υλικού, αλλά και από περιφερειακές συσκευές όπως εκτυπωτές, αναγνώστες, οθόνες, πληκτρολόγια, κ.α.'. Με τον όρο κακόβουλο λογισμικό δεν εννοούμε μόνο το λογισμικό που παράχθηκε για να καταστρέψει ή να αλλοιώσει κάποια αρχεία με διάφορες επιθέσεις αλλά και οποιοδήποτε λογισμικό που δεν πλήρη ακριβής εμπιστευτικότητα και εγκυρότητα. Γι'αυτό τον λόγο σε αυτό το κεφάλαιο θα οριοθετήσουμε τον όρο και θα τον κατηγοριοποιήσουμε σύμφωνα με τα είδη του.

3.1.1 ΠΟΤΕ ΕΝΑ ΛΟΓΙΣΜΙΚΟ ΛΕΓΕΤΑΙ ΚΑΚΟΒΟΥΛΟ

Όπως αναφέρθηκε και στην αρχή το λογισμικό δεν έχει δική του βούληση. Η κακή βούληση στην προκειμένη περίπτωση εξαρτάται από τον προγραμματιστή ὁ έχοντας γνώση των πράξεων του παράγει ένα λογισμικό με επιβλαβείς συνέπειες για δόλιους σκοπούς. Από την άλλη μεριά όμως μπορεί ο προγραμματιστής να έχει άγνοια όσον αφορά στον τρόπο παραγωγής ασφαλούς λογισμικού με αποτέλεσμα να μη γνωρίζει τόσο τις επιβλαβείς συνέπειες όσο και ότι το προϊόν του μπορεί να επιφέρει τέτοιες καταστροφές. Φυσικά στα κακόβουλα λογισμικά δεν συγκαταλέγονται μόνο τα παραγμένα λογισμικά. Κακόβουλο μπορεί να θεωρηθεί και μια σωρός από κατεστραμμένα αρχεία ενός παιχνιδιού. Όπως γνωρίζουμε τα παιχνίδια αποτελούνται από πολλούς φακέλους με αρχεία. Πολύ πριν την εκκίνηση του παιχνιδιού κάποια αρχεία έχουν ήδη καταστραφεί χωρίς αυτό να σημαίνει ότι δεν θα τρέξει το παιχνίδι ή θα έχει κάποια επίπτωση (σε κάποιες περιπτώσεις μπορεί το παιχνίδι να είναι λίγο πιο αργό). Επίσης, κακόβουλο λογισμικό θεωρείται και ένα ήδη υπάρχον λογισμικό που δεν πληροί την απαιτούμενη εμπιστευτικότητα και εγκυρότητα. Δηλαδή κάποιος μπορεί να ¨περάσει¨ ένα πρόγραμμα στον ηλεκτρονικό του υπολογιστή που να μην είναι έγκυρο και να μην έχει κάποια αυθεντικοποιήση ή πιστοποίηση να είναι ¨σπασμένο¨ είναι και αυτό κακόβουλο γιατί δεν δέχεται update και δεν μπορεί να δέχεται οποιαδήποτε καινούρια ενημέρωση.

Αυτό που δεν πρέπει να παραλειφθεί είναι οι αδυναμίες, οι απειλές και οι επιθέσεις. Λέγοντας αδυναμίες μπορεί να είναι τεχνικές ή ανθρώπινες, τυχαίες ή εσκεμμένες και τέλος εσωτερικές ή εξωτερικές. Ας πάρουμε για παράδειγμα μια μεσαία εταιρεία που απασχολεί κάποιο προσωπικό, αν κάποιος από αυτούς τους εργαζόμενους απολυθεί και νοιώθει μεγάλη αδικία ή βαθειά αντιπάθεια απέναντι στους εργοδότες του αποτελεί συνήθως έναν τους πιο επικίνδυνους πληροφορικούς εγκληματίες αφού γνωρίζει πολλούς από τους κωδικούς ασφαλείας και μέτρα προστασίας που είναι ήδη εγκατεστημένα. Ξέρει σε ποιους υπολογιστές να επιτεθεί, ποια αρχεία θα δημιουργήσουν την μεγαλύτερη ζημιά αν σβηστούν και που

βρίσκονται αποθηκευμένα τα αντίγραφα ασφαλείας. Αυτή είναι μια γνωστή τεχνική που έχει χρησιμοποιηθεί από υπαλλήλους οικονομικών και πιστωτικών οργανισμών είναι η *τεχνική του σαλαμιού (salami technique)* κατά την οποία η κατάλληλη τροποποίηση ενός η περισσοτέρων προγραμμάτων, προκαλεί τον υπολογιστή να στρογγυλοποιεί τις συναλλαγές προς τα κάτω κατά πολύ ασήμαντα χρηματικά ποσά, που μεταφέρονται στους λογαριασμούς των ένοχων υπαλλήλων. Οι παθόντες μπορεί να είναι χιλιάδες, επομένως μη προσδιορίσιμοι (άδηλοι).

Στις εξωτερικές αδυναμίες περιλαμβάνονται οι εκβιαστές, πειραματιστές, και πολιτικοί ακτιβιστές. Πιο αναλυτικά οι εκβιαστές είναι η πιο συνηθισμένη κατηγορία εξωτερικής ανθρώπινης εσκεμμένης απειλής . Οι εκβιαστές απειλούν να ενεργοποιήσουν καταστροφικό λογισμικό αν δεν πληρωθεί κάποιο ποσό ή αν δεν ικανοποιηθεί κάποια άλλη τους επιθυμία. Πολλές εταιρίες έχουν πέσει θύματα κάποιας μορφής εκβιασμού στην οποία έχουν συμφωνήσει να μην κινηθούν δικαστικά εναντίον των ατόμων που παραβίασαν την ασφάλεια των υπολογιστικών τους συστημάτων. Δεν είναι λίγες οι περιπτώσεις μάλιστα όπου οι εταιρίες έχουν προσλάβει στο προσωπικό τους τέτοιου είδους άτομα. Σε αντάλλαγμα οι εκβιαστές συμφωνούν να μην φανερώσουν δημόσια τις ατέλειες των δικτύων των εταιριών που τους επέτρεψαν την παράνομη πρόσβαση. Φυσικά ο σημαντικότερος λόγος για τον οποίο οι εταιρίες διστάζουν να οδηγήσουν σε δίκη κάποιο εκβιαστή είναι η δυσφήμιση που θα υποστούν σχετικά με την ασφάλεια τους και επίσης η απειλή περαιτέρω ζημιάς αν δεν ανακαλυφθούν και διορθωθούν οι αδυναμίες στην ασφάλεια. Άλλο μεγάλο κίνητρο για την συγγραφή ενός ιού ή σκουληκιού μπορεί να είναι το κέρδος, η φήμη ή απλά η ικανοποίηση του εγώ από το κυνηγητό. Αναμφίβολα κάποιες προγραμματιζόμενες απειλές θα γραφτούν από πειραματιστές και περίεργους. Σε αυτό το συχνό σενάριο, κάποιος θα συγγράψει έναν ιό, θα τον εξαπολύσει στο διαδίκτυο και μετά θα προσπαθήσει να κερδίσει δημοσιότητα σαν αυτός που τον ανακάλυψε, ή σαν ο πρώτος που θα δημιουργήσει κώδικα που τον απενεργοποιεί, ή απλά να κοκορευτεί για το δημιούργημα του σε κάποιο δημόσιο χώρο συνομιλιών στο διαδίκτυο. Ένα στοιχείο με αυξανόμενη συχνότητα στον χώρο της συγγραφής ιών φαίνεται να είναι υποθάλπουσα πολιτική σκοπιμότητα. Οι ιοί σε αυτήν την κατηγορία μεταφέρουν κάποιο είδος πολιτικού μηνύματος είτε σαν κύριο λόγο ύπαρξης τους είτε για αντιπερισπασμό. Αυτό το στοιχείο αναγάγει την συγγραφή ιών σε ένα εργαλείο στα χέρια πολιτικών εξτρεμιστών που ζητάνε κάποιο κοινό ή ακόμη χειρότερα όταν επιθυμούν την παρενόχληση κυβερνητικών, κοινωνικών ή επιχειρησιακών ιδρυμάτων. Προφανώς η επίθεση στα υπολογιστικά δίκτυα τέτοιων ιδρυμάτων και οργανισμών εξυπηρετεί τους σκοπούς κάποιου μεγαλύτερου πολιτικού σκοπού.

Θέλοντας να οριοθετήσουμε και να κατηγοριοποιήσουμε τον όρο ¨κακόβουλο λογισμικό¨ θα τολμήσουμε κάτι το έχοντας ήδη γνώση ότι οι ειδικοί στον χώρο της ασφάλειας της πληροφορικής και πρόληψης της ηλεκτρονικής απάτης δεν συμφωνούν όλοι στους κοινούς ορισμούς. Τα βασικά κριτήρια κατηγοριοποίησης είναι η αυτονομία και η αναπαραγωγή. Η αυτονομία για να μπορούμε να διαχωρίσουμε το κακόβουλο λογισμικό με βάση ύπαρξης ή μη του λογισμικού-ξενιστή (Ξενιστής : λογισμικό σε βάρος του οποίου επιβιώνει το ¨παράσιτο¨) και η αναπαραγωγή (αυτό αναπαραγωγή ή μη) γιατί δεν αναπαράγονται όλα. Περιληπτικά ισχύει όποιο κακόβουλο λογισμικό απαιτεί λογισμικό-ξενιστή δεν αναπαράγεται, ενώ αντίθετα το λογισμικό που δεν απαιτεί ξενιστή αναπαράγεται. Κάποια βασικά είδη από το λογισμικό που απαιτεί ξενιστή και δεν αναπαράγεται είναι οι κερκόπορτες, οι λογικές βόμβες, οι δούρειοι ίπποι και οι ιοί. Από την άλλη μεριά χαρακτηριστικά είδη του λογισμικό που δεν απαιτεί ξενιστή και αναπαράγεται είναι οι ιοί, τα βακτήρια και οι αναπαραγωγοί. Από τα παραπάνω μπορούμε να καταλάβουμε ότι ένα λογισμικό τέτοιου τύπου μπορούμε να το χωρίσουμε σε ιομορφικό και μη. Ας αρχίσουμε λοιπόν αναλύοντας τι είναι ιομορφικό λογισμικό.

3.2 ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ

Ίος (virus) γνωστά προγράμματα που προσπαθούν (με πονηρές και συνήθως δόλιες τεχνικές) να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους, αφήνοντας μία υπογραφή-ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης - configuration του συστήματος). Ένας κλασικός τρόπος είναι μετά την εγκατάσταση του και την εισαγωγή του στο πρόγραμμα είναι να το μολύνει ενώ αντίγραφα του ίου να συνεχίζουν τη διαδικασία μολύνοντας άλλα προγράμματα.

Ο πρώτος που μελέτησε σε βάθος τη συμπεριφορά των ίων συστηματικά ήταν ο Fred Cohen ο οποίος απέδειξε ότι η μόλυνση είναι δυνατόν να υπάρξει όταν υπάρχει διαμοίραση της πληροφορίας ή μη ελεγχόμενη ροή. Κάποια από τα βασικά πορίσματα του ήταν :

1. η ένωση οπουδήποτε συνόλου ιομορφικών είναι ιομορφική,
2. το πλήθος των διαφορετικών ίων σε μια υπολογιστική μηχανή είναι άπειρο,
3. κάθε πρόγραμμα που αντιγράφει τον εαυτό του είναι ιός,
4. μια δεδομένη ακολουθία συμβόλων που είναι ιός μπορεί να παραχθεί από μια άλλη δεδομένη ακολουθία συμβόλων που είναι επίσης ιός είναι μη επιλύσιμο πρόβλημα,
5. δεν υπάρχει πρόγραμμα το οποίο μπορεί να ανιχνεύσει όλους τους ιούς μιας συγκεκριμένης υπολογιστικής μηχανής,
6. δεν υπάρχει πρόγραμμα το οποίο να μπορεί να εντοπίσει από ποιο πρόγραμμα- φορέα προκλήθηκε η προσβολή ενός αρχικά απρόσβλητου προγράμματος.

(πηγή: ΕΑΠ Ασφάλεια η/υ)

Ένας ιός μπορεί να κάνει οτιδήποτε και οποιοδήποτε άλλο πρόγραμμα. Η μοναδική διαφορά είναι ότι προσαρτάται σε ένα άλλο πρόγραμμα και εκτελείται κρυφά, όταν εκτελείται το πρόγραμμα-φορέας. Από την στιγμή που εκτελείται ένας ιός, μπορεί να εκτελέσει οποιαδήποτε λειτουργία, π.χ. αλλοίωση ή διαγραφή αρχείων.

Ένας ιός έχει τέσσερις φάσεις κατά την διάρκεια της ζωής του την φάση ύπνωσης, την φάση διάδοσης, την φάση ενεργοποίησης και την φάση εκτέλεσης. Στην φάση ύπνωσης ο ιός είναι ανενεργός. Η φάση αυτή δεν είναι απαραίτητο να υπάρχει σε όλους τους ιούς. Στην ουσία περιμένει να ενεργοποιηθεί από κάποιο γεγονός. Στην συνέχεια αφού περάσουμε στην επόμενη φάση, ο ιός τοποθετεί ακριβές αντίγραφο του εαυτού του σε άλλα προγράμματα. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν κλώνο του ιού, ο οποίος με την σειρά του θα ενεργοποιηθεί και θα αρχίσει την λειτουργία για την οποία έχει σχεδιαστεί. Η λειτουργία προβλέπεται από τον κώδικα, μπορεί να είναι αβλαβής όπως π.χ. απλή εμφάνιση ενός μηνύματος ή με επιβλαβείς συνέπιες όπως π.χ. καταστροφή αρχείων.

3.2.1 ΤΥΠΟΙ ΙΩΝ

Από το 1984 που εμφανίστηκε ο πρώτος ιός οι ιοί έχουν αναπτυχθεί ραγδαία. Αυτό οφείλεται στα αποτελεσματικά αντιβιοτικά ενάντια σε συγκεκριμένους τύπους ιών που τους ωθούν να αναπτυχτούν νέοι τύποι για να υπερνικήσουν τα αντίμετρα. Κάποιοι από τους βασικούς τύπους είναι οι :

- παρασιτικοί ο παραδοσιακός τύπος ιού, προσαρτάται σε εκτελέσιμα αρχεία, αναπαράγεται και όταν εκτελεστεί μολύνει το πρόγραμμα, στη συνέχεια βρίσκει άλλα εκτελέσιμα αρχεία.
- παραμένοντας στη μνήμη, εγκαθίστανται στην μνήμη ως τμήματα προγραμμάτων και στην συνέχεια μολύνουν κάθε πρόγραμμα που εκτελείται
- τομέα εκκίνησης οι ιοί αυτοί μολύνουν τον τομέα εκκίνησης του δίσκου.
- δυσανιχνεύσιμο σχεδιασμένοι να αποφεύγουν την ανίχνευση από ειδικό αντιβιοτικό
- πολυμορφικοί έχουν τη δυνατότητα να μεταλλάσσονται σε κάθε μόλυνση.

Ένα παράδειγμα δυσανιχνεύσιμου ιού είναι ο ιός που χρησιμοποιεί συμπίεση για να αποφύγει την αύξηση του μεγέθους του μολυσμένου αρχείου.

Ο πολυμορφικός ιός δημιουργεί κατά την αναπαραγωγή του αντίγραφα που είναι λειτουργικά ισοδύναμα με το πρωτότυπο, αλλά περιέχουν σαφώς διαφορετικές ακολουθίες ψηφίων. Όπως και με το δυσανιχνεύσιμο ιό, ο σκοπός είναι να εξαπατηθεί το αντιβιοτικό λογισμικό. Στην περίπτωση αυτή, η υπογραφή του ιού θα διαφέρει από αντίγραφο σε αντίγραφο. Για να πετύχει αυτήν τη διαφοροποίηση, ο ιός μπορεί να εισάγει τυχαίες περιττές εντολές ή να αλλάζει τη σειρά εμφάνισης ανεξάρτητων μεταξύ τους εντολών. Όμως, μια πιο αποτελεσματική τακτική είναι να χρησιμοποιηθεί κρυπτογράφηση. Στην τακτική αυτή, ένα τμήμα του ιού, που συνήθως ονομάζεται μηχανή μετάλλαξης, δημιουργεί ένα τυχαίο κλειδί κρυπτογράφησης και κρυπτογραφεί τον υπόλοιπο κώδικα του ιού. Το κλειδί αποθηκεύεται μαζί με τον ιό και η μηχανή μετάλλαξης μεταλλάσσεται η ίδια. Όταν κληθεί το μολυσμένο πρόγραμμα, ο ιός χρησιμοποιεί

το αποθηκευμένο κλειδί για να αυτοαποκρυπτογραφηθεί. Όταν ο ιός αναπαραχθεί, δημιουργείται νέο κλειδί.

3.2.2 ΜΑΚΡΟ-ΙΟΙ

Πρόσφατα παρατηρήθηκε ότι αυξήθηκε ο αριθμός των ιών που ανευρίσκονται σε επιχειρηματικά συστήματα. Η αύξηση αυτή οφείλεται, κατά κύριο λόγο, σε ένα νέο τύπο ιού, το μακρο–ιό (macro–virus), οι οποίοι συνιστούν σήμερα τα δύο τρίτα του συνόλου των ιών. Οι ιοί αυτοί είναι επικίνδυνοι γιατί:

1. Είναι ανεξάρτητοι από πλατφόρμες υλικού. Σχεδόν όλοι τους μολύνουν αρχεία Microsoft. Κάθε πλατφόρμα υλικού και λειτουργικό σύστημα που υποστηρίζει το Word μπορεί να μολυνθεί.
2. Μολύνουν αρχεία κειμένου και όχι εκτελέσιμα προγράμματα.
3. Διαδίδονται εύκολα. Μια πολύ συνηθισμένη μέθοδος είναι με το ηλεκτρονικό ταχυδρομείο.

Οι μακρο– ιοί εκμεταλλεύονται τις μακρο– εντολές του Word, οι οποίες υπάρχουν και σε άλλα προγράμματα εφαρμογών γραφείου (π.χ. Excel). Η μακρο–εντολή είναι στην ουσία ένα εκτελέσιμο πρόγραμμα ενσωματωμένο σε ένα αρχείο κειμένου ή ένα λογιστικό φύλλο γραμμένο συνήθως σε κάποια μορφή της Basic. Ο βασικός λόγος της δημοτικότητάς τους είναι ότι οι χρήστες τις χρησιμοποιούν προκειμένου να αυτοματοποιήσουν λειτουργίες που εκτελούν συχνά και να μειώσουν έτσι την απαιτούμενη πληκτρολόγηση. Από τη στιγμή που τρέχει η μακρο–εντολή, μπορεί να αντιγράψει τον εαυτό της σε άλλα αρχεία, να διαγράψει αρχεία ή να προκαλέσει άλλου είδους ζημιές. Στο Microsoft Word υπάρχουν τρία είδη αυτοεκτελούμενων μακρο– εντολών:

- Autoexecute. Αν υπάρχει μακρο–εντολή με το όνομαAutoExec στο αρχείο normal.dot ή σε κάποιο ολικό πρότυπο που είναι αποθηκευμένο στο ευρετήριο εκκίνησης του Word, εκτελείται οποτεδήποτε εκκινεί το Word.
- Automacro. Μια τέτοια μακρο–εντολή εκτελείται όταν συμβεί κάποιο καθορισμένο γεγονός, όπως το άνοιγμα ή κλείσιμο κάποιου εγγράφου, η δημιουργία ενός νέου εγγράφου ή το κλείσιμο του Word.
- Command macro. Αν μια μακρο–εντολή που προσαρτάται σε ολικό μακρο–αρχείο ή σε έγγραφο έχει το όνομα μιας υπάρχουσας εντολής του Word, εκτελείται όποτε ο χρήστης ενεργοποιήσει την εντολή αυτή.

Μια συνηθισμένη τακτική διάδοσης ενός μακρο–ιού είναι η ακόλουθη: Μια automacro ή command macro προσαρτάται σε ένα έγγραφο Word, που εισάγεται στο σύστημα μέσω ηλεκτρονικού ταχυδρομείου ή με μεταφορά αρχείου. Κάποια στιγμή, μετά το άνοιγμα του εγγράφου, εκτελείται η μακρο–εντολή, η οποία αντιγράφει τον εαυτό της στο ολικό αρχείο μακρο–εντολών. Όταν επανεκκινήσει το Word, το αρχείο αυτό ενεργοποιείται. Μόλις ενεργοποιηθεί η συγκεκριμένη αυτή μακρο–εντολή, αφενός μεν αναπαράγεται, αφετέρου δε μπορεί να προκαλέσει ζημιά. Ευτυχώς, οι πρόσφατες εκδόσεις του Word παρέχουν κάποια αυξημένη (αν και όχι απόλυτη) προστασία έναντι μακρο–ιών. Για παράδειγμα, η Microsoft προσφέρει ένα προαιρετικό εργαλείο προστασίας από

μακρο–ιούς που ανιχνεύει ύποπτα αρχεία Word και επισημαίνει στο χρήστη τους κινδύνους που διατρέχει ανοίγοντάς τα.

3.2.3 ΠΡΟΣΤΑΣΙΑ

Πρέπει να γίνει κατανοητό ότι η ιδανική λύση εναντίον των ιών είναι η πρόληψη της εισαγωγής τους στο σύστημα. Δυστυχώς, αυτός ο στόχος είναι γενικά αδύνατον να επιτευχθεί, αν και η πρόληψη μπορεί να ελαττώσει το πλήθος των επιτυχών επιθέσεων ιών. Δεδομένο, λοιπόν, ότι δεν μπορούμε να αποφύγουμε τελείως την εισαγωγή ιών στο σύστημά μας, οι αμέσως καλύτερες επιλογές μας είναι οι εξής:

- **Ανίχνευση** για να εντοπιστεί ο ιός.
- **Αναγνώριση** αφού επιτεύχθηκε η ανίχνευση, να αναγνωριστεί ο ιός που μόλυνε το πρόγραμμα.
- **Απομάκρυνση** των ιχνών του ιού από το μολυσμένο πρόγραμμα για να αποκατασταθεί η κατάσταση και να μην προλάβει να εξαπλωθεί.

Όπως έχουμε ήδη πει, οι τεχνολογίες των ιών και των αντιβιοτικών προχωρούν παράλληλα. Οι πρώτοι ιοί ήταν σχετικά απλά προγράμματα και μπορούσαν να ανιχνευτούν και να απομακρυνθούν με σχετικά απλά αντιβιοτικά. Όμως, σήμερα, τόσο οι ιοί όσο και τα αντιβιοτικά έχουν εξελιχθεί σε πολυπλοκότητα.

Μπορούμε λοιπόν να χωρίσουμε το αντιβιοτικό λογισμικό σε τέσσερις γενιές:

- **Πρώτη γενιά.** Απλοί σαρωτές
- **Δεύτερη γενιά**. Ευρεστικοί σαρωτές
- **Τρίτη γενιά**. Παγίδες δραστηριότητας
- **Τέταρτη γενιά**. Πλήρης προστασία

Περιληπτικά οι σαρωτές της πρώτης γενιάς απαιτούσαν την παρουσία της υπογραφής του ιού για να 0τον αναγνωρίσουν. Η τεχνική αυτή βασίζεται στο γεγονός ότι ο ιός μπορεί να περιέχει χαρακτήρες μπαλαντέρ, αλλά βασικά είναι ο ίδιος ως προς τη δομή του και τις ακολουθίες των bit που περιέχει. Είναι όμως φανερό ότι οι δυνατότητες ανίχνευσης που έχουν τέτοιοι σαρωτές περιορίζονται σε γνωστούς ιούς.

Οι σαρωτές δεύτερης γενιάς δε βασίζονται στην ύπαρξη συγκεκριμένης υπογραφής. Οι σαρωτές αυτοί χρησιμοποιούν ευρεστικούς κανόνες για να εντοπίσουν προγράμματα πιθανόν μολυσμένα από ιούς. Μια κλάση τέτοιων σαρωτών αναζητά τμήματα κώδικα που συχνά σχετίζονται με ιούς. Τα αντιβιοτικά τρίτης γενιάς είναι προγράμματα που παραμένουν στη μνήμη και ανιχνεύουν τους ιούς από τη δράση τους και όχι από τη δομή των μολυσμένων προγραμμάτων. Το πλεονέκτημα των προγραμμάτων αυτών είναι ότι δεν απαιτούν την ανάπτυξη υπογραφών και ευρεστικών κανόνων ανίχνευσης για μια μεγάλη ποικιλία ιών. Τα προϊόντα τέταρτης γενιάς είναι πακέτα που αποτελούνται από διάφορες τεχνικές αντιβίωσης, οι οποίες χρησιμοποιούνται ταυτόχρονα. Οι τεχνικές αυτές συμπεριλαμβάνουν σάρωση και παγίδευση δραστηριοτήτων. Επιπλέον, τα πακέτα αυτά περιλαμβάνουν και έλεγχο προσπέλασης, που περιορίζει την ικανότητα των ιών να προσβάλουν ένα σύστημα και στη συνέχεια περιορίζει την ικανότητα του ιού να τροποποιήσει αρχεία, περιορίζοντας έτσι τις ικανότητες επέκτασής του.

3.3 ΜΗ ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ

Όπως έχουμε ήδη αναφέρει παραπάνω το κακόβουλο λογισμικό έχει δυο μορφές το ιομορφικό και το μη ιομορφικό λογισμικό. Οι μορφές του μη ιομορφικού λογισμικού είναι οι κερκόπορτες, οι λογικές βόμβες, οι Δούρειοι Ίπποι, οι έλικες και τα βακτήρια ή αλλιώς έλικας ή αναπαραγωγός.

Αν και το ιομορφικό λογισμικό είναι η πιο διαδεδομένη και, συνεπώς, γνωστότερη μορφή κακόβουλου λογισμικού, οι άλλες μορφές κακόβουλου λογισμικού που θα μας απασχολήσουν στην ενότητα αυτή είναι εξίσου επικίνδυνες για την ασφάλεια πληροφοριακών συστημάτων.

3.3.1 ΚΕΡΚΟΠΟΡΤΕΣ

Κερκόπορτα (trapdoor) είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης.

Οι κερκόπορτες χρησιμοποιήθηκαν νόμιμα για πολλά χρόνια από τους προγραμματιστές, για να εκσφαλματώσουν και να δοκιμάσουν προγράμματα. Αυτό συνήθως συμβαίνει όταν ο προγραμματιστής αναπτύσσει μια εφαρμογή που περιέχει μια διαδικασία αυθεντικοποίησης η οποία απαιτεί από το χρήστη την εισαγωγή πολλών διαφορετικών τιμών πριν εκτελεστεί η εφαρμογή. Για να εκσφαλματώσει το πρόγραμμα, ο προγραμματιστής μπορεί να θέλει να έχει ειδικά προνόμια ή να αποφύγει όλη την απαραίτητη διαδικασία εγκατάστασης και αυθεντικοποίησης. Επίσης μπορεί να θέλει να είναι βέβαιος ότι θα υπάρχει τρόπος ενεργοποίησης του προγράμματος ακόμη και αν κάτι δεν πάει καλά με τη διαδικασία αυθεντικοποίησης που είναι ενσωματωμένη στην εφαρμογή.

Η κερκόπορτα είναι κώδικας που αναγνωρίζει κάποια συγκεκριμένη ειδική ακολουθία εισόδου ή ενεργοποιείται με το να τρέξει από κάποιο συγκεκριμένο χρήστη ή με τη συγκυρία μιας απίθανης ακολουθίας γεγονότων. Ως εδώ τίποτε δε φαίνεται κακό. Ωστόσο, οι κερκόπορτες μεταβάλλονται σε απειλές, όταν χρησιμοποιούνται από κακόβουλους προγραμματιστές που θέλουν να αποκτήσουν μη εξουσιοδοτημένη προσπέλαση σε κάποιο σύστημα. Είναι δύσκολο να υλοποιήσουμε ελέγχους μέσω του λειτουργικού συστήματος για προστασία από τις κερκόπορτες. Τα όποια αντίμετρα πρέπει μάλλον να επικεντρωθούν στις διαδικασίες ανάπτυξης και συντήρησης λογισμικού.

3.3.2 ΛΟΓΙΚΗ ΒΟΜΒΑ

Μια από τις παλιότερες μορφές κακόβουλου λογισμικού, που εμφανίστηκε πριν ακόμη και από τους ιούς και τους έλικες, είναι η λογική βόμβα.

Η λογική βόμβα (logic bomb) είναι κώδικας ενσωματωμένος σε κάποιο νόμιμο πρόγραμμα εφαρμογής και ρυθμισμένος να ≪εκραγεί≫, όταν εκπληρωθούν κάποιες συγκεκριμένες συνθήκες. Παραδείγματα τέτοιων συνθηκών είναι η παρουσία ή απουσία συγκεκριμένων αρχείων, η έλευση μιας συγκεκριμένης μέρας της εβδομάδας ή μιας ημερομηνίας, ή η εκτέλεση της εφαρμογής από ένα συγκεκριμένο χρήστη. Σε μια περίπτωση, γνωστή στη βιβλιογραφία, η βόμβα ήταν ρυθμισμένη να εκραγεί, αν ο αριθμός ταυτότητας ενός συγκεκριμένου υπαλλήλου (αυτού που έβαλε τη βόμβα) δεν εμφανιζόταν σε δύο συνεχόμενες –χρονικά– καταστάσεις μισθοδοσίας, οπότε η πιθανότητα να είχε απολυθεί ο υπάλληλος ήταν μεγάλη. Από τη στιγμή που θα ενεργοποιηθεί, η βόμβα μπορεί να τροποποιήσει ή να διαγράψει δεδομένα ή και ολόκληρα αρχεία, να προκαλέσει το σταμάτημα ενός συστήματος ή να κάνει οποιαδήποτε άλλη ζημιά.

3.3.3 ΔΟΥΡΕΙΟΣ ΙΠΠΟΣ

Ο Δούρειος Ίππος (Trojan Horse) είναι, ή φαίνεται πως είναι, ένα χρήσιμο πρόγραμμα, που περιέχει κρυμμένο κώδικα ο οποίος, όταν εκτελεστεί, εκτελεί κάποια ανεπιθύμητη ή επιβλαβή λειτουργία.

Οι Δούρειοι Ίπποι μπορούν να χρησιμοποιηθούν για να πραγματοποιήσουν έμμεσα λειτουργίες που ο μη εξουσιοδοτημένος χρήστης δεν μπορεί άμεσα να εκτελέσει. Για παράδειγμα, προκειμένου να αποκτήσει πρόσβαση στα αρχεία ενός άλλου χρήστη σε ένα διαμοιραζόμενο σύστημα, ένας χρήστης θα μπορούσε να δημιουργήσει ένα Δούρειο Ίππο που, όταν εκτελείται, αλλάζει τις παραμέτρους προστασίας των αρχείων του χρήστη που το εκτελεί έτσι ώστε τα αρχεία να είναι αναγνώσιμα από όλους. Ο δημιουργός μπορεί μετά να παρασύρει τους άλλους χρήστες να χρησιμοποιήσουν το Δούρειο Ίππο βάζοντάς τον σε ένα κοινό ευρετήριο και ονομάζοντάς τον έτσι ώστε να φαίνεται σαν ένα χρήσιμο πρόγραμμα, όπως, π.χ., ένα πρόγραμμα που εμφανίζει τα αρχεία ενός χρήστη σε μια επιθυμητή και βολική μορφή. Παράδειγμα ενός Δούρειου Ίππου που είναι δύσκολο να ανιχνευτεί είναι ένας μεταφραστής που έχει τροποποιηθεί και εισάγει επιπλέον κώδικα σε συγκεκριμένα προγράμματα, καθώς αυτά μεταφράζονται. Ένα τέτοιο πρόγραμμα μπορεί να είναι και αυτό που καθορίζει τις διαδικασίες εισόδου στο σύστημα, στο οποίο ο κώδικας που εισάγεται επιπλέον επιτρέπει στο δημιουργό να αποκτήσει πρόσβαση στο σύστημα χρησιμοποιώντας ένα ειδικό συνθηματικό. Αυτός ο Δούρειος Ίππος,που δημιουργεί μια κερκόπορτα, δεν είναι ποτέ δυνατόν να αποκαλυφθεί με ανάγνωση του πηγαίου κώδικα του προγράμματος εισόδου.

Ένα άλλο συνηθισμένο κίνητρο για να γράψει κάποιος Δούρειο Ίππο είναι η καταστροφή δεδομένων. Το πρόγραμμα φαινομενικά εκτελεί μια χρήσιμη λειτουργία
(π.χ. ένα πρόγραμμα αριθμομηχανής), αλλά επίσης, σιωπηρά, διαγράφει τα αρχεία του χρήστη.

3.3.4 WORMS

Τα σκουλήκια (worms) χρησιμοποιούν δικτυακές συνδέσεις για να εξαπλωθούν από σύστημα σε σύστημα. Από τη στιγμή που θα ενεργοποιηθεί μέσα σ' ένα σύστημα, ο έλικας μπορεί να συμπεριφερθεί ως ιός ή ως βακτήριο ή να εισαγάγει Δούρειους Ίππους ή να εκτελέσει οποιαδήποτε καταστροφική ενέργεια.

Για να αναπαραχθεί, ο έλικας χρησιμοποιεί κάποιο δικτυακό όχημα. Παραδείγματα τέτοιων οχημάτων είναι:

• **Υπηρεσία ηλεκτρονικού ταχυδρομείου.** Ο έλικας ταχυδρομεί ένα αντίγραφο του
εαυτού του σε άλλα συστήματα.

• **Υπηρεσία από απόσταση εκτέλεσης.** Ο έλικας εκτελεί ένα αντίγραφο του εαυτού του σε κάποιο άλλο σύστημα.

• **Υπηρεσία από απόσταση σύνδεσης.** Ο έλικας συνδέεται με ένα απομακρυσμένο σύστημα ως χρήστης και μετά χρησιμοποιεί εντολές για να αντιγράψει τον
εαυτό του από ένα σύστημα σε άλλο.

Το νέο αντίγραφο του έλικα εκτελείται στη συνέχεια στο απομακρυσμένο σύστημα, όπου, εκτός των άλλων λειτουργιών που εκτελεί στο σύστημα αυτό, συνεχίζει να εξαπλώνεται και σ' άλλα συστήματα, με τον ίδιο τρόπο.

Οι έλικες έχουν τα ίδια χαρακτηριστικά με τους ιούς: μια φάση ύπνωσης, μια φάση διάδοσης, μια φάση ενεργοποίησης και μια φάση εκτέλεσης.

Κατά τη φάση ύπνωσης ο έλικας είναι ανενεργός. Κάποτε όμως θα ενεργοποιηθεί από κάποιο γεγονός, όπως την έλευση μιας ημερομηνίας, την παρουσία ενός άλλου προγράμματος ή αρχείου ή την υπέρβαση κάποιου αποθηκευτικού ορίου στο δίσκο. Η φάση αυτή δεν είναι απαραίτητο να υπάρχει σε όλους τους έλικες. Κατά τη φάση διάδοσης εκτελούνται οι εξής λειτουργίες:

1. Αναζήτηση άλλων συστημάτων προς μόλυνση, με εξέταση των πινάκων που περιέχουν διευθύνσεις απομακρυσμένων συστημάτων.
2. Εγκατάσταση σύνδεσης με απομακρυσμένο σύστημα.
3. Αντιγραφή του έλικα στο απομακρυσμένο σύστημα και εκτέλεσή του.

Ο έλικας μπορεί, επίσης, να επιχειρήσει να καθορίσει αν το σύστημα έχει προηγουμένως μολυνθεί πριν αντιγράψει τον εαυτό του εκεί. Σε ένα πολυπρογραμματιζόμενο σύστημα μπορεί, επίσης, να μεταμφιεστεί παίρνοντας το όνομα μιας διεργασίας συστήματος ή κάποιο άλλο όνομα που είναι δύσκολο να εντοπιστεί από το διαχειριστή συστήματος.

Όπως και με τις ιομορφές, οι έλικες δικτύων είναι δύσκολο να αντιμετωπιστούν. Ωστόσο, υπάρχουν αντίμετρα προστασίας δικτύων και υπολογιστικών συστημάτων που, αν εφαρμοστούν σωστά, ελαχιστοποιούν τους κινδύνους επίθεσης από έλικες.

3.3.5 ΒΑΚΤΗΡΙΑ

Τα βακτήρια (bacteria) είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα πολυπρογραμματιζόμενο σύστημα ή πιθανόν να δημιουργεί δύο νέα αρχεία, καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές κ.ο.κ. Τα βακτήρια αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες.

3.3.6 ΑΛΛΕΣ ΣΗΜΑΝΤΙΚΕΣ ΑΠΕΙΛΕΣ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ

Σύμφωνα με τη Symantec στο δεύτερο εξάμηνο του 2007 ανακαλύφθηκαν 499.811 κακόβουλοι κώδικες λογισμικού. Καθ' όλη τη διάρκεια του 2007 οι νέοι ιοί έφτασαν τους 711.912. Η πλειονότητα των ιών προορίζεται για υπολογιστικά συστήματα που τρέχουν Microsoft Windows, μια και αυτά είναι πιο διαδεδομένα και πιο εύκολα προσβάσιμα.

1. Επίθεση άρνησης υπηρεσιών γνωστή και ως Dos. Στην ουσία υπερφορτώνει τον server web ή mail με ψεύτικες ανάγκες ή μηνύματα για να γίνει διακοπή παροχής πληροφοριών στους εξουσιοδοτημένους χρήστες.
2. Λογισμικό παρακολούθησης Η/Υ (Spyware). Γνωστό και ως adware, το spyware είναι λογισμικό που συγκεντρώνει πληροφορίες μέσω της σύνδεσης που διαθέτει ο χρήστης χωρίς τη συγκατάθεσή του, συνήθως για διαφημιστικούς λόγους. Το spyware παρακολουθεί τις κινήσεις του χρήστη στο Internet και αποστέλλει τις πληροφορίες σε τρίτους.
3. Keyloggers : ανήκουν στην κατηγορία των spyware, καταγράφουν την αλληλουχία πληκτρολόγησης χαρακτήρων καθώς και την κίνηση του ποντικιού στην οθόνη. Για παράδειγμα να

αποσπάσουν ένα password, και να τα αποστείλουν σε τρίτο πρόσωπο ηλεκτρονικά. Λύση για τα keyloggers αποτελούν αφενός τα anti-spyware εργαλεία, αφετέρου τα εικονικά πληκτρολόγια (virtual keyboards).

4. Ransom-ware : μια ακόμη ηλεκτρονική απειλή έχει κάνει την εμφάνιση της. Ανήκει στην κατηγορία των Δούρειών ίππων. Αφού καταφέρει να διεισδύσει στον υπολογιστή του θύματος «κλειδώνει» με κωδικό κάποια από τα αρχεία υπολογιστή και πλέον εμφανίζονται στο κάτοχο τους ως κρυπτογραφημένα. Στη συνέχεια ο επιτήδειός ζητά «λύτρα» για την «απελευθέρωση» των αρχείων, επιτρέποντας την είσοδο σε αυτά από τον ιδιοκτήτη τους, μόνο στην περίπτωση που πληρωθούν. Αν τα λεφτά δεν σταλούν ο εκβιαστής θα αρχίσει να διαγράφει τα αρχεία κάθε 30 λεπτά, αντίθετα αν σταλούν στέλνει και αυτός με την σειρά του κωδικό απενεργοποίησης για τον ιό.

5. Scareware : γνωστού και ως Antivirus2010, επιχειρεί να τρομοκρατήσει τους χρήστες, προσπαθώντας να τους πείσει ότι έχουν μολυνθεί από κάποιον ιό (χωρίς βέβαια να ισχύει κάτι τέτοιο) και πρέπει άμεσα να προχωρήσουν στη χρήση μιας συγκεκριμένης εφαρμογής για την αντιμετώπιση του προβλήματος. Παραδείγματος χάριν"ντύνει" την ιστοσελίδα όπου εμφανίζεται με τα λογότυπα γνωστών και έγκυρων sites, έτσι, είναι εύκολο για τον ανυποψίαστο χρήστη να ξεγελαστεί και να θεωρήσει ότι η προτροπή που βλέπει προέρχεται όντως από τη γνωστή ιστοσελίδα. Φυσικά, σε περίπτωση που κάποιος εγκαταστήσει τη δήθεν εφαρμογή, το μόνο που καταφέρνει είναι να μολύνει τον υπολογιστή του. Σε άλλες περιπτώσεις, οι κατασκευαστές των συγκεκριμένων ιστοσελίδων, τρομοκρατώντας τους χρήστες, επιτυγχάνουν να τους πείσουν ότι πρέπει να αγοράσουν κάποιο αντιικό πρόγραμμα ή να πληρώσουν για online (και φυσικά πρακτικά ανύπαρκτες) υπηρεσίες "καθαρισμού" του υπολογιστή τους.(παράρτημα 1,2)

6. Security tools and toolkits (εργαλεία ασφάλειας): τα οποία συνήθως είναι σχεδιασμένα για να προστατέψουν τα δίκτυα στα οποία εργάζονται, αλλά μπορούν επίσης να χρησιμοποιηθούν από μη εξουσιοδοτημένους χρήστες στην έρευνα τους για αδυναμίες στην ασφάλεια.

7. Back doors (πίσω πόρτες), Δεν αποτελεί κακόβουλο λογισμικό αυτό καθ' αυτό όμως είναι μια τροποποίηση νόμιμου λογισμικού με συχνά κακόβουλο σκοπό. Ορισμένες φορές οι σχεδιαστές λειτουργικών συστημάτων δημιουργούν σκόπιμα «πίσω πόρτες» που τους δίνουν την δυνατότητα να κάνουν αλλαγές σε οτιδήποτε θέλουν.

8. Zombies : είναι προγράμματα που "κλωνοποιούν" τον εαυτό τους, με στόχο με σκοπό την κατάρρευση του υπολογιστικού συστήματος. Άλλα προγράμματα που εντάσσονται σε αυτήν την κατηγορία, επιτίθενται και κατακλύζουν τους εξυπηρετητές (servers) των διαφόρων τοποθεσιών του Web με χιλιάδες αιτήσης σύνδεσης, επιβραδύνοντας την λειτουργία αυτών με αποτέλεσμα την αδυναμία εξυπηρέτησης (denial-of-service).

3.4 Χάκερ

Η ταυτότητα, το αντικείμενο και ο μύθος των χάκερ.

3.4.1 Ετυμολογία και Ορισμός

Οι χάκερ έχουν συνδεθεί με το ηλεκτρονικό έγκλημα, σε ορισμένες περιπτώσεις μάλιστα εύστοχα. Η κλασσική έννοια του χακερ όμως δεν έχει σχέση με την παρανομία. Η λέξη προέρχεται από την αγγλική ρίζα hack που σημαίνει το κόψιμο και την επεξεργασία ξύλου. Ο χάκερ έχει τη δυνατότητα να «πελεκεί» εφαρμογές, προγράμματα και δίκτυα με πολύ περίτεχνο και έξυπνο τρόπο.

Στο ίντερνετ υπάρχουν αρκετές διαφωνίες για τον ορισμό της λέξης χάκερ. Έχουν όμως όλες κάποια κοινά στοιχεία:

- Οι χάκερ έχουν βαθιές γνώσεις σχετικά με τον προγραμματισμό ή/και σχετικά με τη λειτουργία δικτύων.
- Πρόκειται για πολύ ευφυή άτομα.

Γενικά υπάρχουν 3 κατηγορίες χάκερ:

1. White Hat - Hackers
2. Black Hat - Hackers

3. Grey Hat - Hackers

White Hat-Hackers

White hat-hackers είναι οι χάκερ με το άσπρο καπέλο! Το χρώμα του καπέλου είναι συμβολικό και περιγράφει την «αγνότητα» των προθέσεων αυτού του είδους των χάκερ. Στόχος τους είναι να καταπολεμήσουν το ηλεκτρονικό έγκλημα και τους Black Hat-Hackers. Οι grey hats τους ταυτίζουν με τους ειδικούς ασφάλειας και διαχειριστές συστημάτων. Πολλοί τέτοιοι χάκερ δουλεύουν για μεγάλες εταιρίες λογισμικών και λειτουργικών συστημάτων. Η ηλικία τους μάλλον κυμαίνεται από 25-40 χρονών. Μερικές φορές οι Grey hats μετατρέπονται σε white hats όταν μεγαλώσουν.

Black Hat-Hackers

Οι black hat των χάκερ είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα. Χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνοντας παράνομα προγράμματα, όπως ηλεκτρονικούς ιούς και κατασκοπευτικά προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν, σπάνε κωδικούς από ιστοσελίδες και τις καταστρέφουν ή αλλάζουν την αρχική σελίδα (deface). Το deface χρήσιμοποιείται και από grey hats αλλά σε σπάνιες περιπτώσεις και μόνο για να μεταδώσουν κάποια μηνύματα ασφάλειας. Το κίνητρο των black hats είναι χρηματικό στις περισσότερες περιπτώσεις και όχι ιδεολογικό. Όταν μιλάμε για το οργανωμένο ηλεκτρονικό έγκλημα, πίσω του κρύβονται συνήθως εταιρίες και οργανωμένες ομάδες από έμπειρους προγραμματιστές και όχι μεμωνομένα άτομα.

Grey Hat- Hackers

Εδώ μπαίνουμε στη γκρίζα ζώνη του ίντερνετ. Σε αυτή τη κατηγορία ανοίκουν χάκερ που παραβιάζουν το νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Μπορεί να ανακαλύψουν κενά ασφάλειας ξένων δικτύων ή προγραμμάτων και να τα σπάσουν για να αποδείξουν την αδυναμία τους. Αυτοί οι χάκερ είναι ως επί το πλείστον νεαροί σε ηλικία, ξεκινούν το hacking γύρω στα 15 και φτάνουν στο αποκορύφωμα των γνώσεών τους ως φοιτητές. Δουλεύουν μόνοι τους χωρίς να επιδιώκουν την εκμετάλλευση των γνώσεών τους με εμπορικό τρόπο και καταδικάζουν τους black hats σαν εγκληματίες. Οι ίδιοι δεν θεωρούν τον εαυτό τους εγκληματίες ακόμα και αν παραβιάζουν νόμους γιατί δεν καταστρέφουν ούτε δημιουργούν ζημιές στα συστήματα που εισβάλλουν. Θεωρούν τον ευατό τους ερευνητές της τεχνολογίας και σε κάποιες περιπτώσεις ενημερώνουν ακόμα και το κοινό ή τους διαχειριστες συστημάτων για τυχόν προβλήματα ασφάλειας.

Black Hat Hacker - Cracker - Spammer

Κράκερ είναι οι προγραμματιστές που σπάνε παράνομα την προστασία εφαρμογών και κατά κανόνα δεν είναι χάκερ (software cracker). Το σπάσιμο των κωδικών ενός προγράμματος μπορεί να αποτελεί μια τεχνολογική πρόκληση για τους ειδήμονες των Η/Υ, όμως σε καμιά περίπτωση δεν δικαιολογείται ειδικά αν δημοσιευτούν τα σπασμένα προγράμματα! Όπως οι κράκερ έτσι και οι σπάμερ δεν είναι black-hat χάκερ αλλά ανοίκουν όλοι στο ηλεκτρονικό έγκλημα και συχνά συνεργάζονται.

Script Kiddies

Script Kiddies είναι ένας όρος που με σαρκαστικό τρόπο αναφέρεται στον «παιδικό» τρόπο που χρησιμοποιούν απλοί χρήστες για να υποδυθούν τους χάκερ. Οι αληθινοί χάκερ τους υποτιμούν γιατί χρησιμοποιούν έτοιμα προγράμματα από το ίντερνετ χωρίς να τα κατασκευάζουν οι ίδιοι, και το κίνητρο τους είναι η επίδειξη ικανοτήτων και όχι η μάθηση.

3.4.2 Ηλεκτρονική Κουλτούρα - Underground groups - "Υπόγειες Ομάδες"

Η «υπόγεια» κοινότητα των χάκερ ήταν πολύ πιο ανοιχτή στα πρώτα χρόνια του ίντερνετ. Σήμερα είναι πολύ πιο δύσκολο να βρεθεί κανείς ανάμεσα σε αυθεντικούς χάκερ. Αυτό οφείλεται σε ένα μεγάλο βαθμό στην αυξημένη δημοτικότητα του διαδικτύου, στην εμπορευματοποίηση του μύθου των χάκερ και κυρίως στους νομικούς κινδύνους. Το να είναι κανείς χάκερ προϋποθέτει πολλές ώρες απομόνωσης, μάθησης και προσωπικής έρευνας χωρίς να είναι σημαντική η επικοινωνία. Όταν υπάρχει επικοινωνία, γίνεται μόνο σε τεχνικό επίπεδο πάνω σε συγκεκριμένα θέματα. Στην αρχή μπορεί να νομίζει κανείς ότι οι άνθρωποι που ασχολούνται σε βάθος με τους υπολογιστές και το ίντερνετ είναι απότομοι και αντικοινωνικοί. Η πραγματικότητα όμως είναι ότι ενδιαφέρονται περισσότερο για την ουσία παρά την εμφάνιση των πραγμάτων. Χάκερ θα βρει κανείς σε φόρουμ σχετικά με την ασφάλεια, οι λιτές αλλά ουσιαστικές απαντήσεις τους προδίδουν τις γνώσεις τους. Δυστυχώς όμως, ίσως η μεγαλύτερη μερίδα των χάκερ δεν ασχολούνται με δημόσιες συζητήσεις και κατά κανόνα δεν ενδιαφέρονται για επικοινωνία σε προσωπικό επίπεδο. Οι σημερινοί χάκερ είναι πολύ προσεκτικοί, μεθοδικοί και δεν αποκαλύπτουν τις δραστηριότητες τους ούτε σε φίλους.

3.4.3 Defcon - παγκόσμιο συνέδριο χάκερ

Η Defcon είναι το μεγαλύτερο παγκόσμιο συνέδριο χάκερ που λαβαίνει χώρα κάθε χρόνο στο Λας Βέγκας της Αμερικής. Ιδρύθηκε το 1993 και έχει περίπου 5000 άτομα συμμετοχή κάθε χρόνο. Κατά τη διάρκεια του τριήμερου συνεδρίου παρουσιάζονται ομιλίες πάνω σε τεχνικά θέματα για υπολογιστές. Το κοινό που παρακολουθεί περιλαμβάνει χάκερ (επίδοξους και μη), ειδικούς ασφάλειας, στελέχη σοβαρών επιχειρήσεων αλλά και πράκτορες του FBI! Ο μύθος που έχει δημιουργηθεί στο ίντερνετ για το συνέδριο της Defcon οφείλεται ανάμεσα σε άλλα, και στο γεγονός ότι κάποιες ιστοσελίδες περιγράφουν με πολύ κωμικό τρόπο την διαφορετική συμπεριφορά των συμμετεχόντων, με χαρακτηριστικό παράδειγμα το ότι σχεδόν όλοι βάφουν τα μαλλιά τους μπλε!

Defcon ονομαζόταν ένα από τα πρώτα πιο ισχυρά προγράμματα που χρησιμοποίησαν οι χάκερ. Ο προγραμματιστής του ήταν γνωστός με το ψευδώνυμο Force.

3.4.4 Συνεισφορά των χάκερ στην παγκόσμια ηλεκτρονική ασφάλεια

Πολλά έχουν συνεισφέρει οι χάκερ, στην παγκόσμια ηλεκτρονική ασφάλεια. Ανακαλύπτουν κενά ασφάλειας και τα δημοσιεύουν πριν αυτά τα εκμεταλλευτούν συγγραφείς ιών και black hats. Ενημερώνουν τους διαχειριστές και το κοινό για αυτά τα κενά και ευαισθητοποιούν τον κόσμο σχετικά με την ασφάλεια. Αποδεικνύουν ότι με την έρευνα και τις γνώσεις μπορούμε να βελτιώσουμε την τεχνολογία σε βαθμό που παλιά θεωρούταν αδύνατος και με ταχύτατους ρυθμούς.

Η παλιά φιλοσοφία ασφάλειας που βασίζεται στην ασάφεια «Security through obscurity» δεν είναι αποτελεσματική τακτική την εποχή του ίντερνετ και της παγκοσμιοποίησης. Το να κρύβει κανείς τις αδυναμίες ενός συστήματος για να αποτρέπει επίδοξους εισβολείς είναι σαν να κλείνει τα μάτια για να μη τον δουν. Ο μόνος πρακτικά αποτελεσματικός τρόπος αντιμετώπισης είναι η έγκαιρη ανακάλυψη των προβλημάτων και η ενημέρωση τους μέσω update και patches.

Τα κενά ασφάλειας που ανακαλύπτονται από τους χάκερ αναγκάζουν τις εταιρίες λογισμικών και λειτουργικών συστημάτων να ενημερώνουν πολύ πιο τακτικά τα προϊόντα τους και έτσι να βελτιώνουν την ασφάλεια. Η τεχνολογία αναπτύσσεται με ραγδαίους ρυθμούς όταν υπάρχουν τακτικές ενημερώσεις. Δυστυχώς όμως βλέπουμε εταιρίες να τους ενδιαφέρει περισσότερο το να φέρουν ένα προϊόν όσο το δυνατόν πιο γρήγορα στην αγορά, χωρίς να ελέγχουν λάθη στον προγραμματισμό και τυχόν προβλήματα που μπορεί να παρουσιαστούν. Το αποτέλεσμα είναι μια γενιά προγραμμάτων με bugs και κενά ασφάλειας, τα οποία ίσως να σπεύσουν να τα διορθώσουν όταν θα είναι πολύ αργά.

Η ιστορία αποδεικνύει ότι αντί να εκτιμηθεί η συνεισφορά των εκάστοτε χάκερ στην παγκόσμια ασφάλεια και την εξέλιξη τις τεχνολογίας είχαμε συλλήψεις και άδικες ποινές φυλάκισης. Εδώ τίθεται ένα τεράστιο ηθικό θέμα για το αν η δημοσιοποίηση κενών ασφάλειας, ακόμα και αν περιλαμβάνει μη εξουσιοδοτημένη εισχώρηση σε ξένα συστήματα, πρέπει να τιμωρείται ή όχι.

Το hacking που βασίζεται στην εξερεύνηση ξένων συστημάτων χωρίς να βλάπτεται με οποιοδήποτε τρόπο το σύστημα δεν θα έπρεπε να είναι σοβαρό αδίκημα. Οι περισσότεροι χάκερ είναι ανήλικοι ή νέοι φοιτητές με μοναδικό κίνητρό τους τη μάθηση. Πρόκειται για παιδιά με υψηλό δείκτη νοημοσύνης που για κοινωνικούς και ψυχολογικούς λόγους καταφεύγουν στο hacking. Είναι πραγματικά τραγικό να δικάζονται σαν κοινοί εγκληματίες και να τους τοποθετούν σε φυλακές δίπλα σε δολοφόνους και βιαστές.

3.4.5 Η προσωπικότητα του χάκερ

Η συμπεριφορά των χάκερ έχει τα χαρακτηριστικά του τύπου INTP του διάσημου Τεστ προσωπικότητας Myers-Brigg (βασισμένο στην τυπολογία Γιούνγκ.) Σε αυτή την απόπειρα περιγραφής των βασικών στοιχείων του χάκερ θα περιοριστούμε στην ομάδα των grey hats.

Μικροί σε ηλικία, με κίνητρό τους τη γνώση αλλά και την ανάγκη για δημιουργία προσπαθούν να ανακαλύψουν τα μυστικά πολύπλοκων συστημάτων. Συνήθως το σχολείο δεν τους δίνει τα κατάλληλα ερεθίσματα για να ικανοποιήσουν τη δίψα τους για μάθηση και στρέφονται σε πιο ενδιαφέροντα πράγματα όπως την τεχνολογία. Κάθε μυστήριο τους ελκύει, κάθε πρόβλημα που φαίνεται αδύνατο να λυθεί. Οι ηλεκτρονικοί υπολογιστές είναι γεμάτοι τέτοιες προκλήσεις και αποτελούν το ιδανικό παζλ ή σταυρόλεξο για τέτοια άτομα. Σύντομα το ενδιαφέρον τους για την τεχνολογία αυξάνεται και αφιερώνουν όλο και περισσότερο χρόνο στη διαδικασία επίλυσης των μικρών και μεγάλων προβλημάτων που αντιμετωπίζουν καθώς χειρίζονται τους Η/Υ και το Ίντερνετ.

Φυσικά δεν έχουν όλοι οι χάκερ την ίδια προσωπικότητα και συμπεριφορά. Μερικοί έχουν και μια κανονική κοινωνική ζωή παράλληλα με τις ηλεκτρονικές δραστηριότητές τους. Ο λόγος που η πλειοψήφία δεν έχει πολλές κοινωνικές επαφές είναι απλός: οι άνθρωποι που συναντούν δεν τους ερεθίζουν πνευματικά και θεωρούν χάσιμο πολύτιμου χρόνου την επικοινωνία με άτομα που δεν εκτιμούν τη γνώση. Ένας άλλος λόγος είναι τα πιθανά οικογενειακά ή ψυχολογικά προβλήματα. Ένα μεγάλο ποσοστό χάκερ προέρχονται από προβληματικές οικογένειες και/ή έχουν κάποια μικρά, που στη πορεία μπορεί να γίνουν μεγάλα, ψυχολογικά προβλήματα.

Η εξερεύνηση του ηλεκτρονικού κόσμου απαιτεί αφοσίωση και συγκέντρωση στο αντικείμενο. Οι ώρες που πρέπει να διαθέσει κανείς είναι πάρα πολλές με αποτέλεσμα να κάνει την εμφάνισή του ο εθισμός. Η γραμμή μεταξύ του εθισμού, της εμμονής και της αφοσίωσης στους Η/Υ είναι πολύ λεπτή. Ο υπερβολικός ζήλος μετατρέπεται πολύ εύκολα σε εθισμό. Όταν αρχίσει κανείς το hacking και μετά από τις πρώτες επιτυχείς εισβολές σε συστήματα, είναι πολύ δύσκολο να σταματήσει. Το αίσθημα που έχει ο χάκερ είναι μιας βαθιάς ικανοποίησης και αποδεικνύει την ανωτερότητά του και τις γνώσεις που έχει. Ίσως τελικά το hacking να είναι απλά ένα θέμα εγωισμού για αυτό και μερικοί χάκερ υποσυνείδητα έως και συνειδητά θέλουν να συλλυφθούν για να μάθει το ευρή κοινό τα κατορθώματά τους. Αυτή είναι μια από τις αυτοκαταστροφικές τάσεις που έχουν. Υπάρχουν όμως και χάκερ που δεν είναι τόσο επιφανειακοί. Σαν INTP δεν τους αφορά να είναι κοινωνικά αποδεκτοί (ακόμα και με την αρνητική φήμη), αλλά να μπορούν να χτίζουν και να δημιουργούν νέες τεχνολογικές προσεγγίσεις και πραγματικότητες. Η ικανοποίηση που νιώθουν με την εισβολή τους σε ξένα συστήματα προέρχεται από το αίσθημα επιτυχίας σαν μια επιβράβευση. Μέσα από αυτές τις εμπειρίες μαθαίνουν όλο και περισσότερα. Το γεγονός ότι ο απλός υπολογιστής που έχουν στο σπίτι τους έχει τη δυνατότητα να συνδεθεί με όλα τα μεγάλα δίκτυα τους συναρπάζει. Είναι κάτι που στη φαντασία των χάκερ, που ξέρουν να θαυμάζουν το αυτονόητο, φαίνεται μαγικό. Οι τεχνολογικές προκλήσεις γίνονται όλο και μεγαλύτερες και πάντα υπάρχουν προβλήματα να λύσουν. Το hacking τους δίνει ένα σκοπό και νόημα ύπαρξης.

Οι πιο ταλαντούχοι χάκερ αναγκάζονται βίαια να εγκαταλήψουν το hacking αν αντιμετωπίσουν προβλήματα με τη δικαιοσύνη. Έχουμε πολλά παραδείγματα χάκερ που σταμάτησαν απότομα το hacking και μετανιώνουν για τις ατέλειωτες ώρες που επένδυσαν σε αυτό. Η αποστροφή που νιώθουν οι πρώην χάκερ προς το hacking οφείλεται στο γεγονός ότι συνειδητοποιούν την επικινδυνότητα του ηλεκτρονικού εθισμού. Οι πιο τυχεροί γίνονται ειδικοί ασφάλειας ή έχουν μια καλή καριέρα σε όποιο επάγγελμα θα ακολουθήσουν. Οι πιο άτυχοι αντιμετωπίζουν προβλήματα με τη στάση ζωής που έχουν (αμφισβήτηση της εξουσίας, δεν βρίσκουν κάτι πιο ενδιαφέρον από το hacking) και ίσως αντιμετωπίζουν ψυχολογικά προβλήματα και τάσεις φυγής.

Το hacking εκφράζει μια βαθιά εσωτερική ανάγκη που δεν έχει σχέση με την τεχνολογία. Είναι η ανάγκη για γνώση, για περιπέτεια, για εξερεύνηση και ανακαλύψεις. Οι χακερ μοιάζουν πολύ με τους δημοσιογράφους που διψούν για αποκλειστικότητα και μυστικά. Η τεχνολογία είναι μόνο η αφορμή για την αναζήτηση αυτού που ούτε οι χάκερ μπορούν να ορίσουν. Αν αυτά τα ταλαντούχα και ανήσυχα πνεύματα καταφέρουν να διοχετεύσουν την ενέργειά τους σε άλλους τομείς, έχουν όλες τις δυνατότητες να διαπρέψουν. Αν τελικά καταφέρουν να καταπολεμήσουν τον κυνισμό και την απαισιοδοξία που πολλές φορές τους διακατέχει.

Η παραπάνω περιγραφή βασίζεται σε αληθινές ιστορίες χάκερ από διάφορες πηγές. Σίγουρα όμως η προσωπικότητα του κάθε ανθρώπου είναι μοναδική και ειδικά του κάθε χάκερ. Η περιγραφή αυτή δεν θα αντιπροσωπεύει όλους τους χάκερ και σε καμία περίπτωση τους black hats.

3.5 Σοβαρά περιστατικά

Θα προσπαθήσουμε να παρουσιάσουμε μερικά σοβαρά περιστατικά όπως τα κατέγραψε το CERT/CC. Η επιλογή των σοβαρών περιστατικών έγινε με βάση την διάρκεια, το πλήθος των στόχων, τον τρόπο δράσης και την πρωτοτυπία της επίθεσης.

Έμφαση θα δοθεί σε δύο από αυτά: το Internet Worm (Νοέμβριος 988), το οποίο αν και δεν καταγράφεται στο CERT®/CC, αποτελεί το ορόσημο της ίδρυσής του, και στην δράση των Ολλανδών hackers (Απρίλιος 1990-Μάρτιος 1992), τόσο για την σημασία τους όσο και για να παρουσιαστεί ο τρόπος δράσης τους. Για μία εκτενέστερη καταγραφή των συμβάντων και κατηγοριοποίηση ανάλογα με τον αριθμό των εμπλεκομένων sites, τον χρόνο εξέλιξης του συμβάντος και τα εργαλεία που χρησιμοποιήθηκαν ο αναγνώστης μπορεί να ανατρέξει στο "An Analysis Of Security Incidents On The Internet".

3.5.1 Το «σκουλήκι» του διαδικτύου (Internet Worm)

Πρόκειται για μία από τις πρώτες μεγάλες επιθέσεις που δέχθηκε το Internet από Worm. Τα worms ("σκουλήκια") είναι προγράμματα τα οποία προχωρούν μέσα στο δίκτυο, εγκαθίστανται σε συνδεδεμένες μηχανές και στην συνέχεια, προσπαθούν από εκεί να βρουν επόμενους στόχους και τρόπο να τους προσβάλλουν. Το χαρακτηριστικό τους είναι ότι μπορούν να δρουν αυτόνομα και να έχουν ακόμα και την δυνατότητα να ξεχωρίζουν τους στόχους τους.

Το Internet Worm (όπως επικράτησε να λέγεται) εμφανίστηκε το βράδυ ης 2ας Νοεμβρίου 1988 και μέσα σε ελάχιστες ώρες προσέβαλε μηχανήματα VAX και Sun-3 που έτρεχαν λειτουργικό Berkeley UNIX ή παρόμοια (Π.Χ. SunOS) σε ολόκληρη την έκταση των Ηνωμένων Πολιτειών. Η επόμενη μέρα (που χαρακτηριστικά ονομάστηκε Μαύρη Πέμπτη) βρήκε τους διαχειριστές των συστημάτων να προσπαθούν μάταια να επανεκκινήσουν τους υπολογιστές τους ενώ ένα κλίμα πανικού επεκτάθηκε όπου είχε προηγουμένως περάσει το Worm.

Προτού αναλυθεί ο τρόπος δράσης του Internet Worm, παρατίθενται χρονολογικά τα γεγονότα.

2/11/88,

18.00 Η ακριβής ώρα δράσης δεν έγινε ποτέ γνωστή ,αλλά αυτή αναφέρεται ως επικρατέστερη . Το VAX11/750 του MIT Artificial Intelligence Lab,με όνομα prep.ai.mit.edu,γίνεται ο πρώτος στόχος .Στο μηχάνημα αυτό δεν υπήρχε τακτική μέθοδος λήψης αντιγράφων (backup),ούτε μηχανισμός accounting,γι΄αυτό και τα ίχνη του Worm δεν εντοπίστηκαν ποτέ .Το Worm μπήκε στο σύστημα χρησιμοποιώντας κάποιους από τους πολλούς δημόσιους λογαριασμούς του συστήματος.

18.24 Ο πρώτος επίσημος στόχος : rand.org (Rand Copr., Santa Monica)

19.04 Προσβάλλεται το csgw.berkeley.edu. Το μηχάνημα αυτό ελναι και το gateway του Πανεπιστημίου του Berkeley. Γίνεται άμεσα αντιληπτό από τους administrators.

19.54 Χτυπάει τον finger server του mimsy.umd.edu στο τμήμα Υπολογιστικών Υπηρεσιών του Πανεπιστημίου του Maryland.

20.00 Έχουν χτυπηθεί τα Sun του MIT AI Lab

20.40 Το Berkeley ανακαλύπτει επιθέσεις από το sendmail και το rsh. Περίεργη συμπεριφορά των finger και telnet. Αναγκάζονται να κατεβάσουν (shutdown) συστήματα.

20.49 Προσβάλλεται ο cs.utah.edu, ο κεντρικός εξυπηρετητής του τμήματος Υπολογιστικών Υπηρεσιών του Πανεπιστημίου της Utah. (Τα γεγονότα παρακάτω είναι καταγεγραμμένα από την Utah και είναι παρόμοια και σύγχρονα με άλλα αμερικανικά Πανεπιστήμια).

21.09 Επίθεση από sendmail στον cs.utah.edu.

21.21 Ο μέσος φόρτος (διεργασίες στην ουρά το λεπτό) του cs.utah.edu φθάνει το 5. Πριν τις 21.00 ήταν 0.2-2, ενώ μια τιμή 20 μπορούσε να φορτώσει τόσο πολύ το σύστημα που θα ήταν άχρηστο για οτιδήποτε άλλο.

21.41 Ο μέσος φόρτος στο cs.utah.edu φθάνει το 7.

22.01 Ο μέσος φόρτος στο cs.utah.edu φθάνει το 16.

22.06 Το cs.utah.edu τρέχει ταυτόχρονα 100 διαδικασίες (το μέγιστό του). Πλέον καθίσταται άχρηστο.

22.20 Καταφέρνουν να καθαρίσουν το Worm στο cs.utah.edu. Ωστόσο έχουν προσβληθεί όλα τα υπόλοιπα μηχανήματα Sun του Utah.

22.41 Προσβάλλεται πάλι το cs.utah.edu. Ο μέσος φόρτος φθάνει το 27.

22.49 Οι διαχειριστές του cs.utah.edu αναγκάζονται να κλείσουν (shutdown) προσωρινά το σύστημα, μέχρι να βρεθεί η αιτία.

23.21 Στην επανεκκίνηση, ο μέσος φόρτος φθάνει το 37.

23.28 Ο Peter Yee από την NASA στέλνει το ακόλουθο μήνυμα στην λίστα TCP-IP:

«Δεχόμαστε επίθεση από ένα ιό του διαδικτύου. Έχει προσβάλει ήδη τα UC Berkeley, UC San Diego, Lawrence Livermore, Stanford και NASA Ames»

Συμβουλεύει την απενεργοποίηση των telnet, ftp, finger, rsh και SNMP, αλλά δεν αναφέρει το rexec.

3/11/88,

00.34 Andy Sudduth του Harvard στέλνει ανώνυμα mail στην λίστα TCP-IP, περιγράφοντας για πρώτη φορά πως γίνεται η επίθεση από το finger, πως να αποτραπεί η επίθεση από το sendmail, ενώ αναφέρει για πρώτη φορά και τις επιθέσεις από το rexec. Δυστυχώς το μήνυμα δεν παραδίδεται στην λίστα παρά 2 μέρες αργότερα, επειδή ο relay.cs.net έχει βγει εκτός λειτουργίας, προσβεβλημένος από το Worm.

02.54 Στέλνεται στην λίστα TCP-IP καθώς και στο newsgroup comp.bugs.4bsd.ucb-fixes ένα fix για το sendmail.

Νωρίς το πρωί το wtmp session log χάνεται μυστηριωδώς από το prep.ai.mit.edu.

05.07 Από το Berkeley στέλνεται αναφορά για την επίθεση από το finger, αλλά το μήνυμα δεν γίνεται αντιληπτό για τις επόμενες 12 ώρες.

09.00 Αρχίζει το ετήσιο Berkeley Unix Workshop στο Πανεπιστήμιο του Berkeley. Παραπάνω από 40 διαχειριστές σημαντικών συστημάτων βρίσκονταν στην California την ώρα που ξεσπούσε η κρίση (πολλοί που πετούσαν Πέμπτη πρωί αναγκάστηκαν λόγω της κατάστασης να ακυρώσουν τις πτήσεις τους!).

15.00 Μία ομάδα από το MIT ανακαλύπτει το bug του finger.

16.26 Απομονώνεται το Worm και αρχίζει η προσπάθεια για disassemble και decompile στο Berkeley.

18.00 Παράλληλη δουλειά και στο MIT. Οι δύο ομάδες ανταλλάσσουν κώδικα.

4/11/88,

06.00 Η ομάδα του Berkeley καταφέρνει να αποκωδικοποιήσει το Worm.

12.36 Ανακοίνωση από το MIT ότι οι ομάδες Berkeley και MIT κατάφεραν να αποκωδικοποιήσουν το Worm.

17.00 Γίνεται μικρή παρουσίαση του Worm στο τέλος του Berkeley UNIX Workshop

8/11/88 Το National Computer Security Center των ΗΠΑ συναντάται για να συζητήσει το Worm. Παραβρίσκονται 50 άτομα.

11/11/88 Παρουσιάζεται η πλήρως αποκωδικοποιημένη έκδοση του Worm με σχολιασμένο κώδικα.

Είναι προφανής ο πανικός που δημιούργησε η επίθεση του Worm, ενός καλογραμμένου προγράμματος για το οποίο αρχικά δεν υπήρχε καμία ένδειξη της λειτουργίας του. Όπως φάνηκε αργότερα, αποτελούταν από 99 γραμμές κώδικα αρχικοποίησης (bootstrap) σε γλώσσα προγραμματισμού C κι έναν επιπλέον μεγάλο μεταγλωττισμένου κώδικα (object code) που κυκλοφορούσε σε διάφορες εκδόσεις (ανάλογα αν ο στόχος ήταν VAX ή Sun-3). Η αποκωδικοποίηση (decompilation) αυτού του κώδικα έδωσε 3200 γραμμές προγράμματος C.

Η δράση του Worm περιελάμβανε 2 κατηγορίες την επίθεση και την άμυνα. Στον τομέα της επίθεσης, αρχικά προσπαθούσε να εισέλθει στο σύστημα χρησιμοποιώντας τρύπες γνωστών δικτυακών προγραμμάτων. Στην συνέχεια χρησιμοποιώντας διάφορα συνηθισμένα αρχεία του συστήματος (/etc/hosts.equiv, ~ /.rhosts, κλπ.) προσπαθούσε να εντοπίσει νέους πιθανούς στόχους. Προσπαθούσε

επίσης στο εκάστοτε σύστημα που βρισκόταν να μαντέψει λογαριασμούς χρηστών ώστε να μπορέσει να χρησιμοποιήσει την κοινή πρόσβαση (μέσω των rsh και rexec) για να προχωρήσει και σε άλλα συστήματα.

Η τακτική άμυνας του Worm περιελάμβανε μηχανισμούς για την αποτροπή εντοπισμού της επίθεσης, δυσκολίες στην ανάλυση των δεδομένων, και την κλωνοποίηση του Worm. Αρχικά άλλαζε την ταυτότητά του στο όνομα sh, του πιο συνηθισμένου (και αθώου) μεταγλωττιστή εντολών στο unix. Αλλάζοντας συνέχεια και γρήγορα process Ids (μέσω του fork()), απέτρεπε την καταστροφή του με την kill. Επίσης, είχε απενεργοποιήσει εντελώς την δημιουργία core αρχείων (σε περίπτωση που κάτι δεν πήγαινε καλά). Όλα του τα αρχεία έμεναν για ελάχιστο χρονικό διάσημα στο δίσκο, ενώ ακόμα κι αν εντοπίζονταν είχαν δυσνόητα ονόματα συναρτήσεων ώστε να μην είναι άμεσα ορατή η λειτουργία τους. Οι εναλλακτικές ευκαιρίες εντοπισμού νέων στόχων ήταν τόσες, που δύσκολα μπορούσε να περιοριστεί.

Το Worm ωστόσο, δεν είχε σκοπό την καταστροφή των συστημάτων που προσέβαλε. Για το λόγο αυτό, δεν έσβηνε αρχεία συστήματος, ούτε τροποποιούσε υπάρχοντα αρχεία με κανένα τρόπο και για κανένα σκοπό (π.χ. για την εγκατάσταση δούρειων ίππων). Επίσης, για την εύρεση κωδικών πρόσβασης, δεν κρατούσε για μελλοντική χρήση κωδικούς του συστήματος που είχε ήδη προσβάλει Πάντα χρησιμοποιούσε το δικό του λεξιλόγιο. Για την μεταφορά του χρησιμοποιούσε μόνο το TCP/IP και δεν προσπαθούσε να εισβάλει μέσω UUCP (Unix-to-Unix CoPy) ή των δικτύων X.25 και (του τότε) BITNET. Τέλος, δεν προσπαθούσε να αποκτήσει πρόσβαση διαχειριστή (root access) μιας και δεν του ήταν απαραίτητο προκειμένου να πετύχει τους στόχους του.

Σε υπολογιστικούς όρους, το Worm πέτυχε επίθεση τύπου denial-of service (DoS, άρνηση υπηρεσίας). Στην προκειμένη περίπτωση, η υπηρεσία που χτυπήθηκε ήταν το ίδιο το μηχάνημα που πλέον δεν μπορούσε να εξυπηρετήσει τις δουλειές των χρηστών λόγω του αυξημένου αριθμού των Worms που συναγωνίζονταν για CPU. Όμως κι ένα ακόμα πιο παράξενο είδος DoS παρουσιάστηκε με το Worm: οι διαχειριστές των συστημάτων πανικόβλητοι και φοβούμενοι την μόλυνση από το Worm, δεν δίσταζαν να βγάλουν τα μηχανήματά τους εκτός λειτουργίας. Αγνοούσαν όμως έτσι ότι αποκόπτονταν από τις συντονισμένες προσπάθειες όλων των άλλων να θέσουν σε έλεγχο την κατάσταση, ενώ, ακόμα χειρότερα, απόκοπταν την επικοινωνία σε άλλους ενδιαφερόμενους (στην περίπτωση που οι ίδιοι ήταν gateways). Αυτό στην πράξη δημιούργησε αρκετές ώρες καθυστέρησης στην επίλυση του προβλήματος.

Η βιβλιογραφία για το Internet Worm που μέσα σε ένα βράδυ κατάφερε να οδηγήσει στην κατάρρευση το μεγαλύτερο δίκτυο υπολογιστών της Αμερικής είναι αρκετά μεγάλη. Ήταν το πρώτο θέμα ασφάλειας υπολογιστών που αποτέλεσε πρωτοσέλιδο των New York Times (5/11/88) και έδειξε την τρωτότητα του δικτύου σε απλές (σχετικά) επιθέσεις ("It has raised the public awareness to a considerable degree"). Πολλά έχουν ειπωθεί επίσης και για τους σκοπούς του. Τ ο σίγουρο είναι ότι η καταστροφή θα μπορούσε να είναι πολύ μεγαλύτερη, αν αυτός ήταν ο σκοπός του. Δόθηκε επίσης και η εκδοχή (από μικροατέλειες στον προγραμματισμό του) ότι ήταν ένα καλοσχεδιασμένο πείραμα που όμως ξέφυγε εκτός ελέγχου. Σε κάθε περίπτωση, έδειξε την ετοιμότητα στην οποία θα πρέπει να βρίσκονται όλοι ώστε να αντι-μετωπιστεί μία παρόμοια κατάσταση στο μέλλον.

Αξίζει, τέλος, να σημειωθεί ότι το Internet Worm υπήρξε και το γεγονός που θεμελίωσε το CERT/CC το 1988.

3.5.2 ΟΙ Ολλανδοί hackers (Dutch Hackers)

Η ιστορία των Ολλανδών hackers είναι το πιο μεγάλο σε διάρκεια περιστατικό, όπως καταγράφεται στο CERT®/CC. Ξεκίνησε την 1η Απριλίου 1990 με την προσπάθεια εισβολής σε μηχανήματα του domain .mil (Αμερικανικός Στρατός). Η διάρκειά του ήταν σχεδόν δύο χρόνια και αναφέρθηκαν ως προσβεβλημένα 383 sites σε όλο τον κόσμο (ένα και στην Ελλάδα). Η ιστορία αυτή γίνεται παράλληλα με τον Πόλεμο του Κόλπου και κάποιες προεκτάσεις του είχαν σχέση που θα μπορούσε να δημιουργήσει σημαντικά προβλήματα στην αποστολή.

Οι hackers κατάφεραν και εισέβαλαν σε 34 αμερικάνικα στρατιωτικά sites στο Internet, συμπεριλαμβανομένων και sites που συμμετείχαν στην υποστήριξη της επιχείρησης "Desert Storm/Shield"40. Έψαξαν αρχεία και ηλεκτρονικό ταχυδρομείο για την αναζήτηση λέξεων όπως «πυρηνικά», «όπλα», «πύραυλοι», "desert shield", "desert storm". Βρήκαν πληροφορίες για την ακριβή θέση των αμερικανικών στρατευμάτων, τον τύπο των όπλων που είχαν, τις δυνοτότητες των πυραύλων Patriot και τις κινήσεις των αμερικανικών πλοίων στον Κόλπο. Όταν μάζεψαν τις πληροφορίες έσβησαν τα ίχνη τους.

Σύμφωνα με τον Jim Christy, έναν από τους υπεύθυνους του προγράμματος για την ανακάλυψη εγκλημάτων σε θέματα πολέμου των πληροφοριών, του γραφείου της αμερικάνικης αεροπορίας (Air Force Office of Special Investigations), οι επιθέσεις αφορούσαν και συστήματα τροφοδοσίας των στρατευμάτων στον Κόλπο. «Θα μπορούσαν αντί για πυρομαχικά να είχαν στείλει οδοντόβουρτσες», είπε χαρακτηριστικά στο ABCNews.

Οι hackers είχαν τόση πληροφορία που γέμιζαν τους δίσκους τους, τις δισκέτες, και φύλαξαν μέρος της λείας τους σε χώρο των υπολογιστικών συστημάτων στο Bowling Green University και στο University of Chicago. Κατά πληροφορί$_{ες}$40, οι εισβολείς επιχείρησαν να πουλήσουν πληροφορίες στο Ιράκ κατά την διάρκεια του πολέμου. Η πληροφορία μεταδόθηκε από το BBC, που είχε την πληροφορία από κυβερνητικούς αξιωματούχους στο Ιράκ, αλλά ο Σαντάμ Χουσεΐν αρνήθηκε την προσφορά του ενδιάμεσου των hackers, γιατί φοβήθηκε παγίδα.

Ακόμα και όταν οι εισβολείς εντοπίστηκαν δεν μπορούσαν να τους συλλάβουν γιατί εκείνο τον καιρό οι επιθέσεις σε υπολογιστές δεν ήταν παράνομες. Το FBI προσπάθησε να φέρει τον κύριο εμπνευστή της ομάδας των εισβολέων στην Αμερική, για μία συνέντευξη για δουλειά από μεγάλη αεροναυπηγική εταιρία στην Florida, αλλά αθέλητα ειδοποιήθηκε και το κατάλαβε. Τελικά δύο από τους εισβολείς συλλαμβάνονται και οδηγούνται στην φυλακή για παραποίηση στοιχείων και χρήση πιστωτικής κά$_{ρτας}$40.

χρονολογικά, η επίθεση εξελίχθηκε ως εξή$_{ς}$38:

1/4/1990 Απόπειρα εισβολής σε .mil site από .edu site. Όπως όμως αποδείχθηκε αργότερα, η επίθεση ξεκίνησε από μία ομάδα 4 νεαρών Ολλανδών από μία επαρχιακή πόλη της Ολλανδίας.

5/1990 Αποκαλύπτεται ο τρόπος δράσης των εισβολέων: Πρώτα,
επιλέγουν ένα site στο οποίο αποκτούν πλήρη πρόσβαση διαχειριστή (συνήθως μέσα στις ΗΠΑ), στην συνέχεια, χτυπούν το στόχο τους. Εντοπίζονται από το FBI και ειδοποιούνται οι τοπικές αρχές. Έλλειψη όμως νόμου περί του παρανόμου των πράξεών τους δεν επιτρέπει την σύλληψή τους. Ανακαλύπτεται ο τρόπος που άφηναν backdoor στα συστήματα (άφηναν εξυπηρετητή στο port 87)

5/1990 Οι hackers κάνουν μάλιστα και ανοικτή επίδειξη των δυνά-
μεών τους, εισβάλλοντας επί τόπου σε sites στην Γαλλία και στις ΗΠΑ. Μάλιστα χρησημοποιούν διάφορα τεχνάσματα ώστε να επιτύχουν και δωρεάν τηλεφωνήματα για τις συνδέσεις τους (in-band signaling). Τα επιτεύγματά τους τα κάνουν και γνωστά στα newsgroups, Χρησημοποιώντας το κωδικό όνομα rchack.

8/1990 Εξαφανίζονται όλα τα αρχεία σε Υπολογιστικό Κέντρο Πανεπιστημίου της Ολλανδίας.

30/12/1990 Στέλνουν μήνυμα σε πολλά Internet sites, ζητώντας λογαριασμό για πρόσβαση. Το μήνυμα έλαβε και το CERT®/CC το οποίο και ερεύνησε το θέμα. Ο hacker αυτός αναγνωρίστηκε από το login name που είχε σε κάποιο σύστημα στις ΗΠΑ (fidelio). Προφανώς, δεν έκανε καμία προσπάθεια για να αλλάξει τη πραγματική του ταυτότητα .

1/1991-4/1991 Μία από ης πιο έντονες περιόδους δραστηριότητας των Ολλανδών hackers. Τ ο θέμα άρχισε να παίρνει ανησυχητικές διαστάσεις και έγινε γνωστό στο ευρύ κοινό (μέσω των NY Times). Αδυναμία εύρεσης νομικού πλαισίου για εγκλήματα μέσω υπολογιστών στην Ολλανδία (δεν καταλάβαιναν τι σημαίνει "computer crime").

2/1991 Επίθεση σε site το οποίο κρατούσε πληροφορίες και παρακολούθηση της δράσης τους. Αμέσως ακολουθούν επιθέσεις και προς την ομάδα που προσπαθούσε να τους εντοπίσει και προς άλλες κατευθύνσεις.

21/4/1991 Σε άρθρο των NY Times γίνεται αναφορά για πρώτη φορά στους Ολλανδούς hackers42.

5/199-7/1991 Ύφεση της δράσης τους.

10/1991 -αρχές 1992 Επανάληψη των επιθέσεων. Προσπάθεια για την θωράκιση των μηχανημάτων που χρησιμοποιούσαν οι Ολλανδοί hackers (υπήρξαν αντιδράσεις γιατί αναιρούνταν πολιτικές διαχείρισης) .

27/1/1992 Δύο από τους Ολλανδούς hackers συλλαμβάνονται από την Ολλανδική Αστυνομία. Οι κατηγορίες βασίζονταν στον ήδη υπάρχοντα νόμο και αφορούσαν σε πλαστογραφία (παραποίηση πληροφοριών με σκοπό την απόκτηση πρόσβασης διαχειριστή), βανδαλισμό (κάνοντας άχρηστα τα υπολογιστικά συστήματα) και λοιπές απάτες (χρήση κλεμμένων κωδικών πρόσβασης και χρήση πιστωτικών καρτών).

17/2/1992 Εκδίδεται από το CERT®/CC οδηγία με τίτλο "Internet Intruder Activity" περιγράφοντας τις λεπτομέρειες της δράσης των Ολλανδών hackers.

3/1992 Δημοσιοποιείται και στο CERT®/CC τα αποτέλεσμα της ανάκρισης των 2 συλληφθέντων hackers, οι οποίοι και υπέδειξαν ότι ήταν αναμεμειγμένοι άλλοι 2. Με αυτήν την αναφορά, έκλεισε και τυπικά, 2 χρόνια μετά την έναρξή του, το περιστατικό των Ολλανδών hackers.

Οι Ολλανδοί hackers χρησιμοποίησαν διάφορες μεθόδους προκειμένου να πετύχουν τους σκοπούς τους. Για τον λόγο αυτό αναφέρονται οι Μέθοδοι Δράσης του CERT®/CC με τις οποίες συσχετίστηκαν: weak passwords, no passwords, password files, password cracking, Trojan login, FTP, deleted files, open servers, social engineering, user accounts, system accounts, login attempts, hosts.equiv, .rhosts, sendmail attacks, debug, chsh/chfn, mail spoofing, rm -rf /, 87 socket, software piracy.

Όλα τα παραπάνω τα κατάφεραν, είτε χρησιμοποιώντας απλές εντολές που έδιναν με το χέρι, είτε με χρήση απλών προγραμμάτων (scripts). Ιδιαίτερο ενδιαφέρον παρουσιάζει η αναφορά στο "socket 87" που ήταν η «πίσω πόρτα» για να επανέρχονται σε συστήματα που είχαν ήδη χτυπήσει.

Η επίθεση των Ολλανδών hackers, απέδειξε την αδυναμία των sites να θωρακιστούν απέναντι σε μία απειλή που συνεχώς άλλαζε πρόσωπο και τρόπους δράσης. Είναι αμφίβολο αν η δράση τους θα σταματούσε στις αρχές του 1992 αν δεν είχε επέμβει η Ολλανδική Αστυνομία. Σε κάθε περίπτωση, η επίθεση αυτή θα μείνει ως η πιο μεγάλη σε διάρκεια (712 μέρες) και σφοδρότητα (για την εποχή της).

3.5.3 Οι Δανοί hackers

Είναι μία παρόμοια επίθεση με αυτή των Ολλανδών hackers, αυτή τη φορά όμως από την Δανία. Είχε διάρκεια από τον Αύγουστο του 1993 ως και τον Δεκέμβριο του ίδιου έτους (οπότε και επενέβη η Δανική Αστυνομία).

Τα χαρακτηριστικά της επίθεσης, με βάση τους τρόπους δράσης που καταγράφηκαν στο CERT®/CC είναι τα εξής: sendmail, ISS attack, password files, password cracking, files deleted, mail spoofing, Trojan horses.

Όπως φαίνεται, η δράση τους αποτελεί ένα μικρό υποσύνολο της δράσης των Ολλανδών hackers. Ένα νέο χαρακτηριστικό της επίθεσης ήταν η χρήση του εργαλείου ISS (lnternet Security Scanner), το οποίο μπορεί και ανιχνεύει για παραλείψεις στην ασφάλεια των συστημάτων ενός υποδικτύου.

Αν και αρχικά προοριζόταν για χρήση από τους διαχειριστές συστημάτων, σύντομα ξέφυγε από το έλεγχο κι έγινε όπλο στις επιθέσεις των hackers.

Η επίθεση των Δανών hackers, το δεύτερο εξάμηνο το 1993, είχε ως στόχο και 2 Ελληνικά sites.

3.5.4 Επίθεση μέσω του IRC

Το IRC (lnternet Relay Chat) αποτελεί τον κυριότερο και παλιότερο τρόπο επικοινωνίας των χρηστών του Internet. Σε διάφορους χώρους (κανάλια, όπως ονομάζονται στην ορολογία του IRC) μπορεί κανείς να μπει και να δει συζητήσεις σε θέματα διάφορων ενδιαφερόντων (από πολιτική μέχρι hacking).

Το «Περιστατικό #18» του CERT®/CC αφορά σε επιθέσεις μέσω του IRC. Χρησιμοποιώντας μεθόδους social engineering, hackers έπειθαν τους απλούς και αφελείς χρήστες να εκτελούν εντολές (τις λεγόμενες *DCC* εντολές) ώστε να αποκτούν πρόσβαση στο λογαριασμό τους. Στην συνέχεια, με χρήση κλασικών μεθόδων συνέχιζαν τις επιθέσεις τους. Η πιο χαρακτηριστική περίπτωση ήταν να πείθουν αρχάριους χρήστες να τρέξουν την εντολή "rm -rf / &" από το λογαριασμό τους, με τα γνωστά καταστροφικά αποτελέσματα.

Ένα επίσης σοβαρό περιστατικό, το «Περιστατικό #16», έχει καταγραφεί ως ένα από τα σφοδρότερα στα αρχεία του CERT®/CC. Η διάρκειά του ήταν 224 μέρες (μέσα 1994-μέσα 1995) και χτυπήθηκαν 515 sites. Οι μέθοδοι δράσης που καταγράφηκαν αφορούσαν: rootkit, sniffer, user accounts, system accounts, crack, login attempts, NIS attack, rdist, social engineering, system files deleted, Trojan IRC, Trojan Is, Trojan ifconfig, Trojan ps, Trojan login, Trojan mail, weak password, password file, password cracking, **TFTP** attack, uudecode alías, sendmail attack, IRC abuse, IRC flooding, password -f, mail spoofing, mail bombs, DOS attack, guest account, no password, **FTP** abuse, software piracy, telnet connections, rlogin connections, mailrace, NFS attack, halt system, chain letter, lpr print, expreserve, SATAN, configuraton, gopher, httpd, uucp, rexd attack, warez, open servers.

Χαρακτηριστικά αναφέρεται ότι από τα 515 sites που χτυπήθηκαν σε όλον το κόσμο, 2 ήταν και στην Ελλάδα. Το περιστατικό αυτό παρουσιάζει για πρώτη φορά μία ευρεία γεωγραφική κατανομή στην επιλογή των στόχων (χτυπήθηκαν 41 top-level domains) .

3.5.5 Πόλεμος στο διαδίκτυο

Τη στιγμή που στην Δυτική όχθη οι Ισραηλινοί και οι Παλαιστίνιοι ανέβαζαν τους τόνους της αντιπαράθεσης, hackers επιτέθηκαν (6 Νοεμβρίου 2000) σε κόμβους του American Israelí Publíc Affairs Committee και έκλεψαν 700 φακέλους υποστηρικτών των Ισραηλιτών. Ακόμα 50 περίπου sites, που είχαν σχέσεις με τους Ισραηλίτες, δέχτηκαν επιθέσεις, ενώ άγνωστος είναι ο αριθμός των αντίστοιχων sites των Παλαιστινίων που δέχτηκαν επίθεση τις ημέρες εκείνες.

Είναι φανερό πως ο πόλεμος συνεχίζεται και στον κυβερνοχώρο, πιθανά με θύματα ανθρώπινες ζωές, αφού τα αρχεία που κλάπηκαν είχαν στοιχεία που τις βάζουν σε κίνδυνο.

3.5.6 Κλοπές προσωπικών δεδομένων

Το 2000 ήταν το έτος που έγιναν γνωστές αρκετές περιπτώσεις κλοπής απόρρητων προσωπικών δεδομένων. Στην αρχή του χρόνου ένας δεκαοκτάχρονος Ρώσος με το ψευδώνυμο Maxus, εισέβαλε στο ηλεκτρονικό κατάστημα πώλησης μουσικής CDUniverse και έκλεψε τα στοιχεία των πελατών του. Όταν η εταιρία που εξυπηρετούσε ηλεκτρονικά (hosting) ης υπηρεσίες της CDUniverse αρνήθηκε να πληρώσει $100,000 σαν λύτρα στον κλέφτη, αυτός δημοσίευσε 25,000 πιστωτικές κάρτες στο Internet, ενώ ισχυρίστηκε πως είχε άλλες 300,000.

Τον Σεπτέμβρη 2000 εκλάπησαν 15,700 πιστωτικές κάρτες από την Western Union. Η μητρική εταιρία First Data προσφέρει ένα δίκτυο ηλεκτρονικών οικονομικών συναλλαγών στο 75% του κόσμου παρέχοντας υπηρεσίες με πιστωτικές κάρτες σε 1,400 οργανισμούς και 343 εκατομμύρια καταναλωτές παγκοσμίως.

Σης αρχές του Δεκεμβρίου 2000, ένας κυβερνοκλέφτης από την Ρωσία, έκλεψε 55,000 πιστωτικές κάρτες από την CreditCards.com, μία εταιρία που επεξεργάζεται και επιβεβαιώνει την ακρίβεια των στοιχείων πιστωτικών καρτών για μικρομεσαίες επιχειρήσεις στο διαδίκτυο. Δύο μέρες αργότερα ένας άλλος εισέβαλε και έκλεψε τα ηλεκτρονικά αρχεία 5,000 ασθενών του Washington University Hospital, με το ιατρικό ιστορικό και τους αριθμούς κοινωνικής ασφάλισής τους.

3.5.7 Από τις Φιλιππίνες, με αγάπη

Τον Μάιο του 2000, εμφανίστηκε ο ιός των ερωτικών γραμμάτων, γνωστός σαν ILOVEYOU. Ο ιός αυτός είχε πολλά κοινά στοιχεία με τον Melissa και δημιούργησε αρκετά προβλήματα, αφήνοντας πίσω του χαλασμένα αρχεία και χάος. Το FBI ανίχνευσε και βρήκε πως ο ιός προερχόταν από τον Onel de Guzman, έναν 22χρονο μαθητή στα προάστια της Μανίλα στις Φιλιππίνες.

Αν και δεν υπήρχαν εθνικοί νόμοι για αυτού του είδους τα αδικήματα, βρήκαν τρόπο να τον καταδικάσουν για πλαστογραφία πιστωτικών καρτών. Μετά από αυτό το περιστατικό, σύμφωνα με μία μελέτη της McConnell International, οι Φιλιππίνες είναι το μοναδικό κράτος που έχει ολοκληρωμένη κάλυψη για 10 διαφορετικές κρίσιμες περιοχές ηλεκτρονικών εγκλημάτων.

3.5.8 Επίθεση στην Microsoft

Το φθινόπωρο του 2000 έγινε ένα σοβαρό περιστατικό εισβολής σε ένα από τα πλέον γνωστά δίκτυα, αυτό της Microsoft[45],46. Χωρίς να έχουν δοθεί πολλά στην δημοσιότητα σχετικά με το τι έκαναν οι εισβολείς το διάστημα που είχαν προσπέλαση στα συστήματα της εταιρίας (πιθανόν ποτέ δεν θα μάθουμε αν κατάφεραν να πάρουν ή να αλλάξουν τον κώδικα γνωστών προγραμμάτων) είναι σίγουρο πως η φήμη της εταιρίας δέχτηκε ένα καίριο πλήγμα.

Πέρα όμως από αυτό ο κώδικας των προϊόντων της Microsoft είναι πολύτιμος για αρκετούς ανταγωνιστές της, που θα ήθελαν πολύ να τον έχουν στα χέρια τους. Το ζήτημα είναι πως το χτύπημα αυτό ήταν αφορμή για να χάσει η εταιρία τμήμα της πνευματικής ιδιοκτησίας της και πιθανόν της τεχνολογίας που χρησιμοποιεί. Αν πάντως οι hackers πήραν κώδικα τότε σε λίγο καιρό ή θα τον δούμε δημοσιευμένο κάπου στο διαδίκτυο ή θα πωληθεί σε όποιον δώσει τα περισσότερα.

Η επίθεση φαίνεται πως ξεκίνησε από τον υπολογιστή στο σπίτι ενός υπαλλήλου που συνδεόταν με το δίκτυο της εταιρίας. Από εκεί ένας Δούρειος Ίππος με όνομα QAZ μεταφέρθηκε στο εσωτερικό δίκτυο της εταιρίας. Ο δούρειος ίππος μεταδίδεται μέσω ηλεκτρονικού ταχυδρομείου και αυτόματης αντιγραφής του μέσω διαμοιρασμένων φακέλων μέσα στο δίκτυο, αλλάζοντας την γνωστή εφαρμογή Notepad με τον εαυτό του.

Με την ενεργοποίησή του ο QAZ.trojan (W32.HLLW.QAZ.A) ψάχνει για την εφαρμογή Notepad.exe και αντιγράφει τον εαυτό του στην θέση του, μετονομάζοντας το αυθεντικό σε note.exe. Κάθε φορά που κάποιος τρέχει το μεταλλαγμένο notepad.exe, εκτελείται και το note.exe, ώστε ο χρήστης να μην διαπιστώνει κάποιο πρόβλημα. Κατόπιν ψάχνει στο δίκτυο για να μολύνει και άλλα αντίγραφα του notepad.exe. Από την στιγμή που μολύνει ένα σταθμό, στέλνει με email στον hacker την IP διεύθυνσή του, ενεργοποιεί το WinSock για την επικοινωνία του και περιμένει σύνδεση στο Port 7597. Απλά ο hacker ελέγχει το ηλεκτρονικό ταχυδρομείο του μέσω web, (που προφανώς έχει ανοιχτεί σε μία δωρεάν υπηρεσία με λάθος στοιχεία), και κάνει telnet από ένα άλλο κόμβο κρύβοντας με τους γνωστούς τρόπους την πραγματική του IP.

Χωρίς να έχουν δοθεί στην δημοσιότητα αρκετά στοιχεία για την δράση των εισβολέων και με αντικρουόμενες πληροφορίες για το χρονικό διάστημα που είχαν προσπέλαση στο δίκτυο (λέχθηκε για ένα μήνα ή στην καλύτερη περίπτωση για 9 μέρες), συνηθίζεται από τους hackers, τις πρώτες μέρες, να αντιγράφεται ή να αποστέλλεται με email ότι φαίνεται χρήσιμο, από τον φόβο να γίνουν αντιληπτοί (χωρίς βέβαια να μπορεί κανείς να πει πως έγινε έτσι σε αυτή την περίπτωση).

Έχει ενδιαφέρον να αναλογιστούμε πως κατάφερε ο ιός και πέρασε τα συστήματα ελέγχου της εταιρίας. Εδώ μάλλον η απάντηση βρίσκεται στον τρόπο που τα προγράμματα προστασίας ελέγχουν για ιούς. Στην πλειοψηφία τους τα προγράμματα αυτά έχουν αρχεία με τις υπογραφές των ιών που έχουν βρεθεί σε κανονική και συμπιεσμένη μορφή. Έτσι, αν για παράδειγμα συμπιεστεί ένα αρχείο που περιέχει ιό με ένα πρόγραμμα συμπίεσης, όχι ευρέως γνωστό (π.χ. NeoLite) σε αυτό-αποσυμπιεζόμενο αρχείο, τότε τα συστήματα προστασίας δεν το αντιλαμβάνονται αφού το αρχείο είναι εκτελέσιμο (.exe) και η υπογραφή του δεν υπάρχει μέσα σε αυτό.

Είναι λοιπόν εύκολο για οποιονδήποτε, χωρίς ιδιαίτερες γνώσεις, να συλλέξει τις πληροφορίες που χρειάζονται και να προσπαθήσει να κάνει μια επιτυχή επίθεση σε ένα site. Για να μπορέσει όμως να παραμείνει άγνωστη η ταυτότητά του, χρειάζεται περισσότερη εμπειρία και χρόνος.

Την επόμενη χρονιά η Microsoft ήταν πάλι στόχος των hackers. Αυτή τη φορά η επίθεση αφορούσε τα στοιχεία για το DNS της εταιρίας . Για λίγες ώρες τα στοιχεία για το DNS είχαν αλλάξει και εκατομμύρια χρήστες για δύο μέρες δεν μπορούσαν να προσπελάσουν τους web servers της.

3.6 Ιοί συνέχεια

Στις 19 Ιουλίου 2001 το CERT/CC εκδίδει οδηγία (CA-2001-13) που αφορά το Code Red Worm. Πρόκειται για μια επίθεση κινέζων hackers που δημιούργησε τεράστια προβλήματα τόσο σε κόμβους όσο και σε δίκτυα, δημιουργώντας μεγάλη κυκλοφορία και denial of service σε πολλά δίκτυα υπολογιστών. Ο ιός εύρισκε ένα τρωτό στον IIS 4.0 και 5.0 της Microsoft που επέτρεπε την απομακρυσμένη εκτέλεση κώδικα. Ο κώδικας αυτός μόλυνε τα συστήματα και προσπαθούσε να επεκτείνει την επίθεση και σε άλλα πλησίον του. Σε λίγες μέρες και πριν προλάβουν να κυκλοφορήσουν τα προγράμματα προστασίας τα γνωστά «αντιβιοτικά», 300,000 κόμβοι μολύνθηκαν δημιουργώντας πανικό στο διαδίκτυο. Ο ιός αυτός είχε και «μεταλλάξεις», αφού παρουσιάστηκε και σε έκδοση ΙΙ ως απάντηση από Αμερικανούς hackers, με βελτιωμένο τον κώδικα ώστε να βρίσκει τα συστήματα που είχαν πρόβλημα και να διαδίδεται με μεγαλύτερη ταχύτητα. Ο ιός αυτός τοποθετούσε «κερκόπορτες» (backdoors) και είχε μέθοδο να εξετάζει τα συστήματα μέσα στο τοπικό δίκτυο αλλάζοντας το τελευταίο τμήμα της IP διεύθυνσης.

Ένας άλλος ιός ο W32/Sircam worm εμφανίστηκε ιδιαίτερα απειλητικός, αφού διαδιδόταν μέσω ηλεκτρονικού ταχυδρομείου με την χρήση Outlook και μέσω διαμοιρασμένων καταλόγων (shared directories) σε συστήματα που έτρεχαν Windows. Η ευρεία διάδοσή του οφείλεται στο ότι χρησιμοποιούσε τον διευθυνσιογράφο (address book) του Outlook και έστελνε αντίγραφα σε γνωστούς με θέμα «Γεια. Πως είσαι;» και κείμενο «σου στέλνω αυτό το αρχείο και θέλω τα σχόλιά σου». Ο παραλήπτης ανυποψίαστος άνοιγε το mail και το συνημμένο αρχείο με αποτέλεσμα να μολυνόταν το σύστημά του. Επίσης όταν ο κώδικας του ιού διαπίστωνε πως υπήρχε στο τοπικό δίκτυο και άλλο σύστημα με διαμοιρασμένους καταλόγους, αντέγραφε τον κώδικά του σε διάφορα σημεία του νέου συστήματος και κύρια στο βασικό αρχείο rund1l32.exe και στην registry του συστήματος. Το αποτέλεσμα στα συστήματα που είχαν μολυνθεί ήταν να μην υπάρχει διασφάλιση του απορρήτου, να υπάρχει άρνηση λειτουργίας (denial of service) και απώλεια της ακεραιότητας του συστήματος. Αποτέλεσμα αυτών ήταν να αντιγραφούν παράνομα εμπιστευτικά αρχεία εταιρειών με passwords, αριθμούς πιστωτικών καρτών πελατών, σχέδια προϊόντων κλπ.

Τέλος μία παραλλαγή των προηγούμενων ιών ήταν το W32/Nimda@MM γνωστός απλά σαν Nimda worm. Το «σκουλήκι» αυτό χρησιμοποιούσε όλους τους τρόπους επίθεσης μέσω ταχυδρομείου, IIS web server, μόλυνση αρχείων σε file shares, ακόμα και κατεβάζοντας τον κώδικα μέσα από μολυσμένες ιστοσελίδες με απλό web-browsing. Μάλιστα όπου εύρισκε τους προηγούμενους ιούς χρησιμοποιούσε τα τρωτά που είχαν δημιουργήσει και αφού μόλυνε τα συστήματα έκλεινε τις «τρύπες» των άλλων ιών για να μην γίνεται αντιληπτός. Ο ιός αυτός είχε σαν αποτέλεσμα την κατάρρευση πολλών δικτύων διεθνών τραπεζών. Πολλές εταιρίες προϊόντων αντιμετώπισης ιών ισχυρίζονται πως ο Nimda και SirCam ήταν πάνω από το 50% των ιών που εμφανίστηκαν το 2001.

Τέλος το Δεκέμβριο του 2001 έκανε την εμφάνισή του ο ιός Pentagon (ή Goner) worm γραμμένος σε Visual Basic Script (VBS), σαν screen saver που προσπαθούσε να απενεργοποιήσει τα προγράμματα προστασίας από ιούς που «έτρεχαν» στα συστήματα. Η εταιρία MessageLabs ισχυρίζεται πως σε 24 ώρες από την εμφάνιση του ιού εντόπισε 40,000 μολυσμένα συστήματα. Το αντίστοιχο για τον SirCam τον Νοέμβριο ήταν 50,000 συστήματα σε 24 ώρες.

Φαίνεται πως οι δημιουργοί των ιών προχωρούν σε μεθόδους που δεν απαιτούν την βοήθεια του χρήστη για να εξαπλωθούν και αυτό γεμίζει με ανησυχία τους υπεύθυνους των εταιριών που κατασκευάζουν συστήματα προστασίας από ιούς.

Στον Πίνακα φαίνονται οι 24 ιοί της τελευταίας διετίας που προκάλεσαν την μεγαλύτερη κινητοποίηση ή μόλυναν τα περισσότερα συστήματα.

Όνομα ιού	Ημερομηνία Ανακάλυψης	Τύπος ιού	Μέθοδος Μετάδοσης	Επικινδυνότητα
W32/SirCam@MM	7/17/2001	Ιός	E-mail	Μεσαία
W32/Navidad@M	1/3/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32/Hybris.gen@MM	10/16/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32!Nimda.gen@MM	9/18/2001	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
JS/Kak@M	10/22/1999	Ιός	VBScript Σκουλήκι	Μεσαία
VBS/VBSWG.gen@MM	2/11/2001	Ιός	VbScript	Μεσαία
W95/MTX.gen@M	8/23/2000	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32/Magistr.a@MM	3/12/2001	Ιός	Σκουλήκι	Μεσαία
VBS/Loveletter@MM	5/4/2000	Ιός	VbScript	Μεσαία
W32!Naked@MM	3/6/2001	Ιός	E-mail	Μεσαία
W32/ProLin@MM	11/30/2000	Διαδικτυακό Σκουλήκι	MAPI	Χαμηλή
W32/CodeRed.a.	7/17/2001	Ιός	Διαδικτυακό Σκουλήκι	-
W32/FunLove.4099	1/9/1999	Ιός	Win32	Μεσαία
BackDoor-G	4/15/1999	Δούρειος Ίππος	Remote Access	Μεσαία
VBS/VBSWG.Z@MM	5/16/2001	Ιός	VbScript	Μεσαία

BackDoor-Sub7	12/16/1999	Δούρειος Ίππος	Remote Access	Μεσαία
W32/CodeRed.c. Σκουλήκι	8/4/2001	Ιός	Διαδικτυακό Σκουλήκι	-
VBS/SST.gen@MM	5/9/2001	Ιός	VBScript Σκουλήκι	Μεσαία
APStrojan.qa@MM	1/18/2000	Δούρειος Ίππος	AOL Password	Μεσαία
W32/APost@MM	9/3/2001	Ιός	E-mail Σκουλήκι	Μεσαία
W32/QAZ.Σκουλήκι	8/7/2000	Δούρειος Ίππος	Διαδικτυακό Σκουλήκι	Μεσαία
IRC/Stages. Σκουλήκι	5/26/2000	Ιός	VBScript Σκουλήκι	Μεσαία
W32/Badtrans@MM	4/11/2001	Ιός	Διαδικτυακό Σκουλήκι	Μεσαία
W32/Pretty . Σκουλήκι .unp	2/15/2000	Δούρειος Ίππος	Σκουλήκι	Μεσαία

3.6.1 ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ MICROSOFT

Στόχος των εγκληματιών που δρουν μέσω του internet είναι να μπορούν να χρησιμοποιούν ένα ιό και να αποκτήσουν τον έλεγχο σ'ένα μεγάλο αριθμό υπολογιστών, να τους μετατρέψουν δηλαδή σε ζόμπι. Με αυτόν τον τρόπο θα αποκτήσουν δύναμη δημιουργώντας ένα ισχυρό δίκτυο ελεγχόμενων υπολογιστών που εκτελεί κακόβουλες ενέργειες. Χαρακτηριστικά που μαρτυρούν ότι ο υπολογιστής έχει μολυνθεί είναι η μείωση της ταχύτητας, περίεργα μηνύματα, ο υπολογιστής κολλάει, κάνει επανεκκινήσεις συνέχεια κάθε λίγα λεπτά, αφού τις εκτελεί από μόνος του δεν λειτουργεί καλά, οι δίσκοι και οι μονάδες δίσκων δεν είναι προσβάσιμοι, ασυνήθιστα μηνύματα σφαλμάτων και τέλος παραμορφωμένα παράθυρα διαλόγου και μενού. Σε αυτές τις περιπτώσεις πρέπει να υπάρχει ένα εργαλείο διαγραφής κακόβουλου λογισμικού και είναι ενημερωμένο. Κάποια βήματα για να μην μετατραπεί ο υπολογιστής σε ζόμπι σύμφωνα πάντα με την Microsoft είναι :

1. να προσέχετε τα e-mail και κυρίως τα συννημένα
2. χρησιμοποιείται το τείχος προστασίας στο internet
3. μείνετε ενημερωμένοι
4. ενεργοποιείστε τις αυτόματες ενημερώσεις
5. χρησιμοποιήστε γνήσια προϊόντα
6. antivirus

Βασικά η επίτευξη της σχετικής ασφάλειας στο internet σ'όλες τις διαδικτυακές δραστηριότητες δεν είναι καθόλου δύσκολη υπόθεση. Ο μόνο που χρειάζεται είναι σχεδόν θρησκευτική ευλάβεια σε μια σειρά από κανόνες που θα σας προστατεύσουν από κάθε λογής κίνδυνο που μπορείτε να συναντήσετε στο Παγκόσμιο Διαδίκτυο.

- Patches, updates και συνεχής ενημερώσεις ανά τακτά διαστήματα να μην ξεπερνούν όμως τον ένα μήνα. Ελέγξτε στο διαδίκτυο ή σε άλλη πηγή ενημέρωσης την ύπαρξη ή την διάθεση των patches για το λειτουργικό σύστημα. Μια έγκυρη πηγή για patches ασφαλείας είναι η πιο έγκυρη ενημέρωση το microsoft technet.
- Σωστή προσέγγιση και χρήση διαδικτυακών εφαρμογών, οι περισσότεροι web browsers διαθέτουν δεκάδες χιλιάδες ρυθμίσεις ασφαλείας και επιτρέπουν πλέον και μια έξυπνη διαχείριση των cookies. Μια καλή αρχή για δοκιμή των ρυθμίσεων του browsers είναι το online test qualys's free browser check up το οποίο θα σας αποκαλύψει κάποια αδυναμία του browser σας.
- Σοφή χρήση των antivirus και των firewalls. Φροντίστε να έχετε ένα ή περισσότερα πακέτα antivirus και να το ενημερώνετε συχνά με virus definition updates. Ακόμα και η αποτελεσματική μηχανή αντιμετώπισης ιών αν δεν ενημερώνεται διαρκώς είναι παντελώς άχρηστη. Όσο αφορά τα firewallsπρέπει να έχετε κατά νου ότι οι εξ'ορισμού ρυθμίσεις των περισσότερων προγραμμάτων firewall θα επιτρέπουν την απεριόριστη πρόσβαση στο internet για μερικές χιλιάδες εφαρμογές. Με άλλα λόγια δεν πρέπει να εμπιστευτείτε με κλειστά μάτια σε αυτό την ασφάλειά σας.
- Διατηρείστε την ανωνυμία σας, ενημέρωση του browser που χρησιμοποιείται, επιτρέπεται τα πρωτογενή cookies και μπλοκάρεται third party cookies, πρόγραμμα αποτροπής και εμπόδισης της λειτουργίας spyware λογισμικού.
- Κρυπτογράφηση και περιορισμός των υπηρεσιών
- Παρακολούθηση της διαδικτυακής δραστηριότητας.

3.6.2 ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ GOOGLE

Κακόβουλο λογισμικό:

Εάν ξαφνικά εμφανιστεί μία νέα γραμμή εργαλείων στο πρόγραμμα περιήγησης ιστού του υπολογιστή σας ή εάν οι αναζητήσεις σας μέσω Toolbar ανακατευθυνθούν σε κάποια διαφορετική μηχανή αναζήτησης, ενδέχεται να έχει εγκατασταθεί κακόβουλο λογισμικό στον υπολογιστή σας. Το κακόβουλο λογισμικό (γνωστό και ως spyware, adware ή scumware) συμπεριλαμβάνει μερικές φορές, χωρίς να το γνωρίζετε, δωρεάν στοιχεία λήψης. Μετά την εγκατάστασή του, μπορεί να ενεργοποιήσει αναδυόμενες διαφημίσεις, να σας ανακατευθύνει σε ανεπιθύμητους ιστότοπους ή ακόμα και να αλλάξει την εμφάνιση και λειτουργία της Αναζήτησης ιστού Google στον υπολογιστή σας. Σας διαβεβαιώνουμε ότι το Toolbar δεν συνεργάζεται κατά οποιονδήποτε τρόπο με κακόβουλα λογισμικά και δεν πραγματοποιείται εγκατάσταση λογισμικού τρίτου μέρους μέσω του Toolbar.

Λήψη λογισμικού προστασίας

Μπορείτε να πραγματοποιήσετε λήψη δωρεάν λογισμικού που ανιχνεύει και καταργεί κακόβουλα λογισμικά από τον υπολογιστή σας. Οι χρήστες του Toolbar αναφέρουν ότι ενδέχεται να

πρέπει να εγκαταστήσετε όλα τα παρακάτω προγράμματα για να καταργήσετε τις πιο συνηθισμένες κακόβουλες εφαρμογές:

- Lavasoft Ad-Aware (Μόνο στα Αγγλικά)
- CWShredder (Μόνο στα Αγγλικά)
- Spybot Search and Destroy (Μόνο στα Αγγλικά)

Η Google δεν συνδέεται με κανέναν τρόπο με αυτά τα εργαλεία κατάργησης κακόβουλων λογισμικών και δεν μπορεί να εγγυηθεί για την αποτελεσματικότητά τους.

3.6.3 ΑΝΑΛΥΣΗ ΖΗΜΙΑΣ

Η ζημιά που κάνουν οι προγραμματιζόμενες απειλές ποικίλει από τις απλά ενοχλητικές μέχρι τις απόλυτα καταστροφικές. Η ζημιά μπορεί να προκληθεί από επιλεκτικές διαγραφές συγκεκριμένων αρχείων ή στιγμιαίες μετατροπές που ανταλλάσουν τις τιμές τυχαίων ψηφίων. Πολλές απειλές μπορεί να στοχεύουν συγκεκριμένους στόχους - οι συγγραφείς τους μπορεί να επιθυμούν να προκαλέσουν ζημιά στα αρχεία ενός συγκεκριμένου χρήστη ή εταιρίας ή την καταστροφή μιας συγκεκριμένης βάσης δεδομένων.

Η αποκάλυψη διάφορων πληροφοριών είναι ένας άλλος τρόπος ζημιάς που μπορεί να προκληθεί από τις προγραμματιζόμενες απειλές. Αντί απλά να τροποποιεί πληροφορίες σε ένα σκληρό δίσκο, μια απειλή μπορεί να φανερώσει κάποιες άκρως απόρρητες και ευαίσθητες πληροφορίες, να τις στείλει στην άλλη άκρη του κόσμου μέσω του ηλεκτρονικού ταχυδρομείου, να τις δημοσιοποιήσει σε ένα δημόσιο πίνακα ανακοινώσεων (public bulletin board). Οι πληροφορίες αυτές μπορούν να είναι στρατιωτικά ή βιομηχανικά μυστικά, τα σχέδια μιας καινούργιας εφεύρεσης, κωδικοί πρόσβασης σε κάποιο ακαδημαϊκό ίδρυμα, το μισθολόγιο των υπαλλήλων μιας εταιρίας, οι κωδικοί πιστωτικών καρτών των πελατών μιας εταιρίας κλπ. Η λίστα φαίνεται πραγματικά ατελείωτη. Είναι φανερό ότι το είδος της ζημιάς ποικίλει ανάλογα με τα κίνητρα των ανθρώπων που γράφουν τον υπεύθυνο κώδικα.

3.6.4 ΕΠΙΛΟΓΟΣ

Στην τεχνολογική εποχή που ζούμε, η σημασία της ασφάλειας των ηλεκτρονικών υπολογιστών και δικτύων είναι μέγιστη για τα προσωπικά δεδομένα του καθημερινού ανθρώπου. Πρώτον, ένα μεγάλο μέρος των προσωπικών μας πληροφοριών είναι αποθηκευμένο σε υπολογιστές. Αν αυτοί οι υπολογιστές δεν είναι ασφαλείς από περίεργα μάτια, τότε ούτε και τα δεδομένα που περιέχουν είναι. Ακόμη χειρότερα, μερικές από τα πιο ευαίσθητες πληροφορίες - χρεωστικά & πιστωτικά ιστορικά, λογαριασμοί τραπεζών, στοιχεία κατόχων πιστωτικών καρτών κλπ. - ζούνε σε μηχανήματα που είναι συνδεδεμένα σε πολύ μεγάλα δίκτυα.

Δεύτερον, όλο και μεγαλύτερο μέρος της σημερινής κοινωνίας εξαρτάται από τους υπολογιστές, και την ακμαιότητα των προγραμμάτων και των δεδομένων που αυτά περιέχουν. Αυτά περιλαμβάνουν τα προφανή (οικονομικά δεδομένα), τα πανταχού παρόντα (το τηλεφωνικό δίκτυο ελέγχεται από τεράστια δίκτυα ηλεκτρονικών υπολογιστών), τα ζωτικής σημασίας (ιατρικές συσκευές ελεγχόμενες από υπολογιστές και ηλεκτρονικά συστήματα αποθήκευσης και επεξεργασίας ιατρικών δεδομένων). Τα προβλήματα που προκαλούνται από λάθη σε τέτοια συστήματα είναι μνημειώδη. Ο νους

τρομάζει από τον συλλογισμό του τι κακό θα μπορούσε να δημιουργηθεί - ηθελημένα ή μη!- από μη εξουσιοδοτημένες αλλαγές. Οι άνθρωποι αποτελούν ένα πολύ μεγάλο μέρος του προβλήματος αλλά και της λύσης. Έτσι λοιπόν οποιαδήποτε μελέτη των επιπτώσεων στο μέλλον πρέπει να συμπεριλαμβάνει τεχνολογικούς και μη τεχνολογικούς παράγοντες. Η κατάσταση που επικρατεί στον χώρο της ασφάλειας των πληροφοριακών συστημάτων και δικτύων σίγουρα θα αλλάζει ανά τα χρόνια. Είναι όμως σίγουρο ότι απόλυτη ασφάλεια δεν είναι δυνατόν να υπάρξει ποτέ. Η πληροφορική ασφάλεια είναι τόσο σημαντική στην σημερινή κοινωνία της πληροφορίας όσο σημαντικά ήταν και τα τείχη για τις πόλεις μια χιλιετηρίδα πρίν.

"ed quis custodiet ipsos custodes?"

(Μα ποιος θα φυλάει τους ίδιους τους φύλακες?)

Satires, VI, γραμμή 347

-JUVENAL, C.100 C.E

3.6.5 ΠΑΡΑΡΤΗΜΑ

1 «Αν και δεν εμπίπτει στην κατηγορία του κακόβουλου λογισμικού θα παρουσιάσω μία μορφή scareware που δεν έχει σχέση με ιούς αλλά με αναφορά μέσω email της επικείμενης αγοράς domain name παραπλήσιου με αυτό της εταιρίας σας. Οι επιτήδειοι βρίσκουν εταιρικά emails όπου αποστέλλουν ένα κείμενο όπως το παρακάτω προσπαθώντας να πείσουν τον ιδιοκτήτη του e-forum.gr για παράδειγμα ότι κάποιος στην Κίνα προσπαθεί να αγοράσει το e.forum.cn, e.forum.cn.hk κτλ. αφήνοντας να πλανάται στον αέρα η πιθανότητα ότι κάποιος στην Ασία προσπαθεί να εκμεταλλευτεί το εμπορικό σας όνομα. Αν και δεν προτρέπουν άμεσα το υποψήφιο θύμα να κάνει κάποια αγορά, δηλώνουν (ψευδώς) ότι αν δεν προβεί ο παραλήπτης σε κάποια κίνηση άμεσα τότε σε 7 ημέρες θα επιτρέψουν να αγοραστούν τα αναφερόμενα domain names. Σε εμφανή σημεία του email υπάρχει το link του site της εταιρίας η οποία πουλάει στην ουσία domain names. Προσοχή καθώς πρόκειται για καλοστημένη δουλειά που κινείται στα όρια της παρανομίας και που δεν προκαλεί έυκολα υποψίες (όπως για παράδειγμα η περίφημη νιγηριανή απάτη στην οποία έχει γίνει εκτενής αναφορά στο e-forum.gr:

viewtopic.php?f=20&t=129&start=0&hilit=%CE%BD%CE%B9%CE%B3%CE%B7%CF%81%CE%AF%CE%B1).

From: steven [mailto:steven@qipeng.org.cn]
Sent: Wednesday, March 18, 2009 1:37 PM
Subject: Urgently-Domain Issue
Importance: High

(If you are not the person who is in charge of this, please transfer to the right person/department. Thank you.)

Dear CEO,

We , a registrar organization in China, have something to check with you. We received an application this morning. One company called "Cinemo Trading Co. Ltd" is applying for " e-forum " as internet brand and following Asian/.CN domain names to use.
e-forum.asia

e-forum.com.cn
e-forum.com.hk
e-forum.com.tw
e-forum.hk
e-forum.net.cn
e-forum.org.cn
e-forum.tw
After checking, we found the internet brand and keyword of these domain names are as same as your company's names, so we need to check this with your company.If the aforesaid company is your subsidiary company or your business partner, please DO NOT reply us, we will approve the application automatically. If you have no any relationship with this company, please contact us within 7 workdays. If out of the deadline, we will approve the application submitted by " Cinemo Trading Co. Ltd " unconditionally.
Please forward the email to your decision maker,and let them contact me in time,so that we can handle this in reasonable.Look forwarding to hearing from you.
Best Regards,
Steven Zhou Lead Checker

Shanghai QiPeng Network Information Technology Co.,Ltd
Tel $B!' (B +86-21-6992-9440 Fax $B!' (B +86-21-6992-9447
Mobile:13764008659
Postal Code $B!' (B 201803
website:http://www.qipeng.org.cn

Shanghai QiPeng Network Information Technology Co.,Ltd is a comprehensive company engaged in the Internet intellectual property services that mainly provides network-based service, network intellectual property service.
Company objective: The good faith first, the customer is supreme.

---

steven $B!$ (Bsteven@qipeng.org.cn »

(ΠΗΓΗ : e-foroum.gr, θέμα κακόβουλο λογισμικό)

2 «Εκατομμύρια χρήστες σε όλο τον κόσμο εκτιμάται ότι έπεσαν θύματα εταιρειών που πουλούν στο Διαδίκτυο ψεύτικα αντι-ιικά προγράμματα. Η αμερικανική κυβέρνηση κατάφερε τώρα να μπλοκάρει με δικαστική εντολή τις παραπλανητικές διαφημίσεις.

Η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) εξασφάλισε εντολή περιοριστικών μέτρων και συνεχίζει τη δικαστική διαμάχη για να πετύχει την οριστική απαγόρευση του λογισμικού «scareware» («λογισμικό τρόμου» σε ελεύθερη απόδοση), όπως αναφέρει τη Δευτέρα το BBC.

Τα έγγραφα που υπέβαλε η FTC στο δικαστήριο δείχνουν ότι οι απατεώνες καταχωρούσαν διαφημίσεις ακόμα και σε αξιόπιστους κατά τα άλλα δικτυακούς τόπους.

Οι χρήστες που έκαναν κλικ στις διαφημίσεις δρομολογούνταν σε ιστοσελίδες ανύπαρκτων εταιρειών ασφάλειας οι οποίες προχωρούσαν σε σάρωμα των υπολογιστών για τον εντοπισμό ιών και spyware. Το

σάρωμα πάντοτε αποκάλυπτε δήθεν προβλήματα και οι απατεώνες παρότρυναν τους χρήστες να αγοράσουν άχρηστο λογισμικό προστασίας.

Τα περιοριστικά μέτρα αφορούν τα ψεύτικα αντι-ιικά προγράμματα WinFixer, WinAntivirus, DriveCleaner, ErrorSafe και XP Antivirus, τα οποία προωθούσαν οι εταιρείες Innovative Marketing Inc. και ByteHosting Internet Services LLC.

Περισσότεροι από ένα εκατομμύριο χρήστες στις ΗΠΑ και πολλοί ακόμα σε όλο τον κόσμο εκτιμάται ότι είχαν πέσει θύματα της απάτης.Τα περιουσιακά στοιχεία των δύο εταιρειών πάγωσαν ώστε να καταστεί δυνατή η αποζημίωση των πελατών τους.» Πηγή: in.gr (Δεκέμβριος 2008)

ΒΙΒΛΙΟΓΡΑΦΙΑ

Gollmann D, *computer security,* John Wiley & sons,1999.

Γκρίτζαλης Δ. *Ασφάλεια Πληροφοριακών Συστημάτων*, Αθήνα, Ελληνική εταιρία Επιστημόνων Η/Υ & Πληροφορικής(ΕΠΥ),1989.

Κιουντούζης Ε. *Ασφάλεια Πληροφοριακών Συστημάτων,* Αθήνα Εκδόσεις Ευγ. Μπένου,1993.

Νόμος 2472/97 περί «Προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ΦΕΚ αρ. 50, 10/4/1997.

Χαλαζωνίτης Κ., « Οι ευαίσθητες πληροφορίες», στο *Ασφάλεια Πληροφοριών*: *Τεχνικά, Νομικά και Κοινωνικά Θέματα*, Ν. Αλεξανδρή, Ε. Κιουντουζή, Β Τραπεζάνογλου(επιμέλεια έκδοσης), Αθήνα, Ελληνική Εταιρία Επιστημόνων Η/Υ & Πληροφορικής (ΕΠΥ), 1995.

Γκρίτζαλης Δ., *Ασφάλεια στις τεχνολογίες πληροφοριών και επικοινωνιών: Εννοιολογική θεμελίωση,* (μτφρ. Σ. Κοκολάκης), Αθήνα, Εκδόσεις Νέων Τεχνολογιών,1996.

Κάτσικας Σ. Κ., «Διαχείριση Κινδύνων Πληροφοριακών Συστημάτων» *στο Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ,1995.

Γκρίτζαλης Δ. Γκρίτζαλης Σ., *Ασφάλεια Λειτουργικών Συστημάτων,* Εκπαιδευτική Εταιρία Νέων Τεχνολογιών, Αθήνα,1991.

Tanenbaum A. S. (επιμέλεια μετάφρασης Π. Γεωργιάδη), *Σύγχρονα Λειτουργικά Συστήματα,* Εκδόσεις Παπασωτηρίου, Αθήνα, 1993.

Denning P.(Ed), *Computers under attack: Intruders, Worms and Viruses,* Addison-Wesley, 1990.

Κάτσικας Σ. Κ., «Προστασία και ασφάλεια Συστημάτων Υπολογιστών», τόμος Α'& Β' στο *Ασφάλεια Υπολογιστών*, ΕΑΠ, 2001.

Μάγκος Εμμ., *«Ασφάλεια υπολογιστών και προστασία Δεδομένων»* ,2008.

http://www.Microsoft.com/Hellas/athome/security/viruses
http://www.asxetos.gr
http://www.virus.gr
http://www.itsecurity.gr