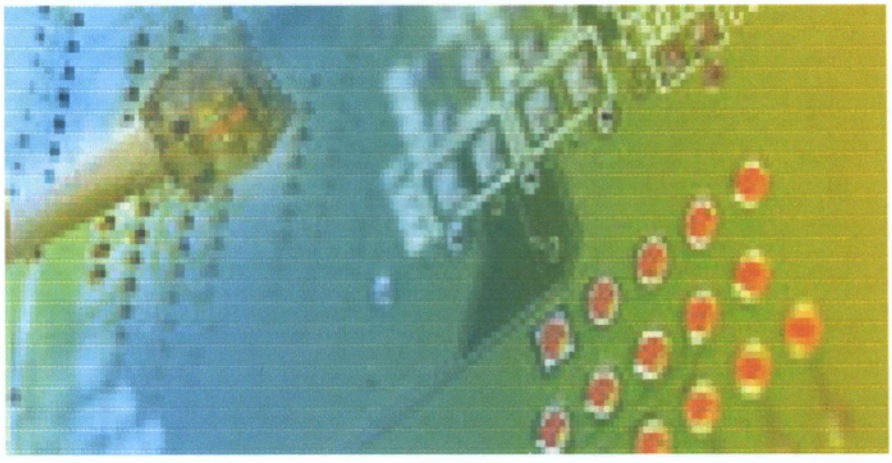
ΑΤΕΙ ΚΑΛΑΜΑΤΑΣ
ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΤΗΛΕΠΟΙΚΟΙΝΩΝΙΩΝ



Ασφάλεια Και Προστασία Προσωπικών Δεδομένων Στις Ηλεκτρονικές Επικοινωνίες

ΣΠΟΥΔΑΣΤΡΙΑ: Σούρσου Αθηνά
ΑΜ: 2006238
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Κ. Μακροδημήτρης Γεώργιος

ΣΠΑΡΤΗ 2012

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Διαδίκτυο

Το Διαδίκτυο είναι ένα δημόσιο δίκτυο παγκόσμιας εμβέλειας το οποίο παρέχει άμεση διασύνδεση σε οποιοδήποτε χρησιμοποιεί ένα τοπικό δίκτυο (LOCAL AREA NETWORK) ή πάροχο υπηρεσιών σύνδεσης με το διαδίκτυο (INTER SERVICE PROVIDER ISP).Το διαδίκτυο είναι ένα δίκτυο δημόσιας χρήσης το οποίο συνδέεται και δρομολογείται μέσω πυλών (gateways).Οι τελικοί χρήστες συνδέονται με παρόχους τοπικής πρόσβασης (LAN ή ISP), που συνδέονται με παρόχους πρόσβασης δικτύου και τελικά με τον δικτυακό κορμό του Internet. Εφόσον η πρόσβαση στο διαδίκτυο είναι ελεύθερη σε όλους, είναι ευνόητο ότι υπάρχει έλλειψη ελέγχου η οποία μπορεί να έχει σαν αποτέλεσμα μια ακανόνιστη και ανεξέλεγκτη διάχυση της πληροφορίας. Οι χρήστες χρειάζονται αποτελεσματικές και εύχρηστες μηχανές αναζήτησης για να «ταξιδέψουν στην θάλασσα των πληροφοριών».

Το Διαδίκτυο αποτελεί παράδειγμα συστήματος τύπου open system interconnection. Καλείται ανοιχτό σύστημα (open system), γιατί σε αντίθεση με προηγούμενα επικοινωνιακά συστήματα ανεπτυγμένα από ιδιωτικές εταιρίες, η περιγραφή του είναι δημόσια διαθέσιμη. Έτσι, οποιοσδήποτε μπορεί να γράψει λογισμικό που να συμβαδίζει με τις προδιαγραφές του συστήματος.

Αποτελεί ένα συνεχώς διευρυνόμενο και οικουμενικό μέσο, στο οποίο οι χρήστες διασκεδάζουν, εκπαιδεύονται, πληροφορούνται και διεξάγουν τις όποιες οικονομικές ή επιχειρηματικές δραστηριότητες. Δυστυχώς, δεν είναι ασφαλές και αυτή η αλόγιστη και αφελής χρήση του οδηγεί τις περισσότερες φορές σε κάθε είδους ηλεκτρονικές απάτες, όπως είναι και η υποκλοπή των προσωπικών δεδομένων των χρηστών. Η ασφάλεια της επικοινωνίας μεταξύ δύο ή περισσότερων επικοινωνούντων μερών μπορεί να διακυβευτεί με ποικίλους τρόπους.

Ασφαλής επικοινωνία μεταξύ δύο μερών νοείται κάθε μορφής επικοινωνία που γίνεται με χρήση ψηφιακής τεχνολογίας, και εξασφαλίζει την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών που διακινούνται μέσω ενός τηλεπικοινωνιακού δικτύου. Ποια είναι, λοιπόν, τα αρνητικά ή έστω ανησυχητικά φαινόμενα που προκύπτουν από την εξάπλωση του Διαδικτύου; Και ποιου είδους ηλεκτρονικές απειλές ελοχεύονται μέσα στις διαδικτυακές δραστηριότητες των χρηστών.

Το Διαδίκτυο δεν αποτελεί μόνο πηγή πληροφόρησης, διασκέδασης ή εκπαίδευσης. Αποτελεί ένα εξαιρετικά πολύτιμο εργαλείο για το επιχειρείν. Το ηλεκτρονικό επιχειρείν (γνωστό και ως e-επιχειρείν) σημαίνει ακριβώς αυτό που υποδεικνύει ο όρος: ανάπτυξη επιχειρηματικών διαδικασιών και υπηρεσιών μέσω του Διαδικτύου. Μέσω του e-επιχειρείν δίνεται η δυνατότητα σε οποιαδήποτε επιχείρηση, οργανισμό, αλλά και σε οποιονδήποτε επαγγελματία να παρέχει τις υπηρεσίες του και να ικανοποιεί τις απαιτήσεις και επιθυμίες των πελατών του γρήγορα και απλά, μέσω του Διαδικτύου, όπως και να συναλλάσσεται με τους προμηθευτές και τους συνεργάτες του.

Το e-επιχειρείν ενσωματώνει δραστηριότητες (υπηρεσίες προστιθέμενης αξίας) για το ηλεκτρονικό εμπόριο, το λεγόμενο e-commerce: Ιδιώτες και εταιρίες έχουν τη δυνατότητα να πραγματοποιούν αγορές προϊόντων από όλο τον κόσμο. Τα οφέλη είναι πολλαπλά: Εύκολη αναζήτηση και σύγκριση προσφερόμενων προϊόντων και τιμών εντός και εκτός των φυσικών συνόρων, μικρότερο κόστος αγοράς σε πολλές περιπτώσεις, δυνατότητα αγορών 24 ώρες το 24ωρο. Μέσα από το e-επιχειρείν αναδεικνύεται και το e-government, δηλαδή η ηλεκτρονική διακυβέρνηση: Ο κάθε πολίτης μπορεί να πραγματοποιεί συναλλαγές με το δημόσιο και τους οργανισμούς τοπικής αυτοδιοίκησης γρήγορα και αποτελεσματικά, αποφεύγοντας τη γραφειοκρατία και τις ουρές, με λίγα μόνο «κλικ» από τον υπολογιστή του. Το e-banking αποτελεί επίσης ένα ανεκτίμητο εργαλείο στα χέρια των χρηστών του Διαδικτύου. Μέσα από ειδικές ασφαλείς πλατφόρμες που οι περισσότερες έγκυρες τράπεζες παρέχουν σήμερα στου πελάτες τους, μπορούν να πραγματοποιηθούν άπειρες τραπεζικές συναλλαγές, που παλαιότερα απαιτούσαν την φυσική μας παρουσία στην τράπεζά. Επίσης, μέσω του e-banking πολλοί καθημερινοί λογαριασμοί (τηλεφώνου, ηλεκτρικού ρεύματος, ΕΥΔΑΠ, κ.λπ.). Και η λίστα των δυνατοτήτων διευρύνεται συνεχώς. Παρά τις καταπληκτικές δυνατότητες που διανοίγονται, στην Ελλάδα παρατηρείται μια διστακτικότητα στην αξιοποίηση των νέων εφαρμογών του Διαδικτύου.

Ο Παγκόσμιος Ιστός (World Wide Web) είναι μια από τις σημαντικότερες υπηρεσίες του Internet και προσφέρει στους χρήστες του τη δυνατότητα πρόσβασης στη μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο. Πρόκειται για μια τεράστια συλλογή εγγράφων, τα οποία είναι αποθηκευμένα σε εκατομμύρια υπολογιστές στον κόσμο και η οποία εμπλουτίζεται συνεχώς από όλους τους χρήστες οι οποίοι αποφασίζουν να ανεβάσουν στο χώρο του τις σελίδες τους. Η πλοήγηση στις σελίδες του παγκοσμίου ιστού πραγματοποιείται μέσω ειδικών προγραμμάτων πλοήγησης –browsers- («Internet Explorer και ο Netscape Navigator») και απαιτεί ιδιαίτερη προσοχή από τον χρήστη, διότι εγκυμονεί πολλαπλούς

κινδύνους, τόσο για την ασφάλεια του υπολογιστή του, όσο και για την ασφάλεια των προσωπικών του δεδομένων. Τα μέτρα τα οποία μπορεί να ληφθούν για να εξασφαλίσουν κατά το δυνατόν ασφαλή πλοήγηση στις σελίδες του παγκοσμίου ιστού εξαρτώνται α) από τις υπηρεσίες που μπορεί να προσφέρει ο παροχέας σύνδεσης (internet provider) και β) από τις ενέργειες που κάνει ο ίδιος ο χρήστης.

Το Internet (ή Διαδίκτυο) παρουσιάζει μεγάλη αποδοχή, πράγμα που οδηγεί στην συνεχή εξέλιξη και αναδιαμόρφωση του. Ένα από τα μεγαλύτερα προβλήματα που έπρεπε να λυθούν ώστε το Διαδίκτυο να γίνει πραγματικότητα, ήταν η ύπαρξη πολλών τεχνολογιών δικτύων, καθεμιά από τις οποίες εξυπηρετεί μια συγκεκριμένη ομάδα ανθρώπων. Οι χρήστες του δικτύου διαλέγουν την τεχνολογία που είναι κατάλληλη για τις επικοινωνιακές τους ανάγκες. Η χρήση μίας και μόνο τεχνολογίας για την δημιουργία ενός παγκόσμιου δικτύου είναι αδύνατη, γιατί δεν υπάρχει τεχνολογία που να ικανοποιεί όλες τις απαιτήσεις. Για παράδειγμα, μερικοί χρήστες χρειάζονται δίκτυα υψηλών ταχυτήτων που καλύπτουν μικρές αποστάσεις. Για άλλους πάλι, πιο εξαπλωμένα δίκτυα, χαμηλών ταχυτήτων είναι πιο χρήσιμα.

Το Διαδίκτυο, παρ' όλα αυτά, καταφέρνει να συνενώσει όλες αυτές τις διαφορετικές τεχνολογίες, παρέχοντας ένα σύνολο συμβάσεων. Κρύβει τις λεπτομέρειες της υποκείμενης δικτυακής τεχνολογίας και επιτρέπει σε υπολογιστές από όλο τον κόσμο να βρίσκονται σε επαφή ανεξάρτητα από το δίκτυο στο οποίο συνδέονται. Το Διαδίκτυο βασίζεται σε μια συλλογή από τυποποιήσεις που καλούνται πρωτόκολλα. Τα πρωτόκολλα (π.χ. TCP και IP) παρέχουν τους κανόνες για την επικοινωνία. Περιέχουν τις λεπτομέρειες των ανταλλασσόμενων μηνυμάτων, περιγράφουν πως ανταποκρίνεται ο υπολογιστής όταν λαμβάνει κάποιο μήνυμα και ορίζει πως διαχειρίζεται ο υπολογιστής τις καταστάσεις λάθους. Κατά μία έννοια, τα πρωτόκολλα είναι για την επικοινωνία ότι είναι οι αλγόριθμοι για τον προγραμματισμό. Ένας αλγόριθμος επιτρέπει την κατανόηση της λογικής του προγράμματος, χωρίς να χρειάζεται να ξέρει την δομή και κατασκευή της CPU. Ομοίως, ένα πρωτόκολλο επιτρέπει στον χρήστη να καταλάβει τα δεδομένα χωρίς να έχει γνώση του δικτυακού υλικού.

ΚΕΦΑΛΑΙΟ 1°

1.1 Η ΕΝΝΟΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Προσωπικά δεδομένα είναι , σύμφωνα με τον Νόμο 2472/1997 και την Οδηγία 95 / 46/ ΕΚ κάθε πληροφορία που αναφέρεται στο πρόσωπό του κάθε ατόμου, π.χ. το όνομα και το επάγγελμά του ατόμου, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες.

1.2 Προστασία Προσωπικών Δεδομένων

Αναγνωρίζοντας ότι η συλλογή, η επεξεργασία και, ιδιαίτερα, η διαβίβαση ή κοινοποίηση προσωπικών δεδομένων μέσω των νέων τεχνολογιών πληροφοριών, και, συγκεκριμένα των λεωφόρων πληροφοριών, διέπονται από τις διατάξεις της Συνθήκης για την Προστασία του Ατόμου από την Αυτόματη Επεξεργασία Προσωπικών Δεδομένων (Στρασβούργο 1981, Σειρά Ευρωπαϊκών Συνθηκών Αρ. 108) και από επιμέρους συστάσεις για την προστασία δεδομένων και κυρίως τη Σύσταση Αρ. R(90)19 για την προστασία των προσωπικών δεδομένων που χρησιμοποιούνται στην εξόφληση λογαριασμών και άλλες συναφείς εργασίες. Χρησιμοποιώντας το Διαδίκτυο οι χρήστες επιφορτίζονται με ευθύνες όσον αφορά στη δράση τους και θέτουν σε κίνδυνο την ιδιωτικότητά τους. Είναι σημαντικό να συμπεριφέρονται με τρόπο που να τους εξασφαλίζει προστασία και να προάγει τις αγαθές σχέσεις με τα άλλα πρόσωπα. Οι παρούσες κατευθυντήριες γραμμές προτείνουν ορισμένους πρακτικούς τρόπους για τη διασφάλιση της ιδιωτικότητας, αλλά πρέπει επίσης να γνωρίζουν τα δικαιώματα και τις υποχρεώσεις τους που απορρέουν από τον νόμο. Πρέπει να έχουν υπόψη τους ότι ο σεβασμός της ιδιωτικότητας αποτελεί θεμελιώδες δικαίωμα για κάθε άτομο και τυγχάνει προστασίας από αντίστοιχη νομοθεσία. Παρακάτω ακολουθούν κάποιες κατευθυντήριες γραμμές που περιγράφουν τις αρχές της ορθής πρακτικής, σε ότι αφορά στην ιδιωτικότητα, για χρήστες και παροχείς υπηρεσιών Διαδικτύου (ISP).[28]

1.3 Προς χρήστες

1. Το Διαδίκτυο δεν είναι ασφαλές. Ωστόσο, υπάρχουν, και διαρκώς αναπτύσσονται, διάφορα μέσα τα οποία σας επιτρέπουν να βελτιώσετε την προστασία των δεδομένων σας. Είναι σκόπιμο να χρησιμοποιούνται όλα τα διαθέσιμα μέσα για την προστασία των δεδομένων και των επικοινωνιών , όπως τη νόμιμη κρυπτογράφηση για τα εμπιστευτικού

χαρακτήρα ηλεκτρονικά μηνύματά καθώς και κωδικούς πρόσβασης για κάθε προσωπικό υπολογιστή.

2. Να θυμάστε ότι κάθε συναλλαγή , κάθε επίσκεψή στο Διαδίκτυο, αφήνει ίχνη. Αυτά τα «ηλεκτρονικά ίχνη» μπορούν να χρησιμοποιηθούν, εν αγνοία σας, για να διαμορφωθεί ένα προφίλ για το άτομό σας και τα ενδιαφέροντα του κάθε χρήστη. Αν δεν επιθυμείτε να συμβεί αυτό, σας παροτρύνουμε να χρησιμοποιείτε τα τελευταία τεχνικά μέσα, τα οποία περιλαμβάνουν τη δυνατότητα ενημέρωσής κάθε φορά που αφήνετε ίχνη, ώστε να τα σβήνετε. Μπορείτε να ενημερώνεστε για την πολιτική ιδιωτικότητας που ακολουθούν διάφορα προγράμματα και ηλεκτρονικοί τόποι Διαδικτύου και να προτιμάτε εκείνα που καταγράφουν τα λιγότερα δεδομένα ή εκείνα που προσφέρουν πρόσβαση με ταυτόχρονη διατήρηση της ανωνυμίας.

3. Η ανώνυμη πρόσβαση και χρήση υπηρεσιών, καθώς και τα ανώνυμα μέσα εξόφλησης λογαριασμών, αποτελούν την καλύτερη προστασία της ιδιωτικότητάς . Αναζητήστε τα τεχνικά μέσα που διασφαλίζουν την ανωνυμία σας όπου χρειάζεται.

4. Η πλήρης ανωνυμία ίσως να μην επιτρέπεται λόγω νομικών περιορισμών. Σε αυτές τις περιπτώσεις και εφόσον επιτρέπεται από τον νόμο, μπορείτε να χρησιμοποιείτε ψευδώνυμο ώστε μόνο ο Παροχέας Υπηρεσιών Διαδικτύου να γνωρίζει την ταυτότητά σας.

5. Να δίνετε στον Παροχέα Υπηρεσιών Διαδικτύου, ή κάθε άλλο πρόσωπο, μόνο τα δεδομένα που είναι απαραίτητα για την εκπλήρωση συγκεκριμένου σκοπού για τον οποίο έχετε ενημερωθεί. Δίνετε ιδιαίτερη προσοχή στους αριθμούς των πιστωτικών καρτών και των τραπεζικών λογαριασμών σας, επειδή η χρήση και η κατάχρηση αυτών στο χώρο του Διαδικτύου ενδεχομένως γίνεται πολύ εύκολα.

6. Η ηλεκτρονική διεύθυνση αποτελεί προσωπικό δεδομένο και ότι άλλα πρόσωπα μπορεί να επιθυμούν να το χρησιμοποιήσουν για διαφορετικούς σκοπούς, όπως είναι η εισαγωγή της σε καταλόγους ή σε λίστες χρηστών. Μη διστάζετε να ρωτάτε για το σκοπό του καταλόγου ή άλλης χρήσης. Μπορείτε να ζητήσετε την παράλειψη των στοιχείων σας εφόσον δεν επιθυμείτε να εγγραφείτε σε μια τέτοια λίστα.

7. Απαιτείται επιφυλακτικότητα με τόπους Διαδικτύου όπου ζητούνται περισσότερα στοιχεία από όσα είναι απαραίτητα για την πρόσβαση ή την ολοκλήρωση μιας συναλλαγής, ή όταν δεν εξηγείται ο λόγος για τον οποίο ζητούνται τόσες πληροφορίες.

8. Φέρνουμε πλήρη ευθύνη έναντι του νόμου για την επεξεργασία των δεδομένων, για παράδειγμα, αν φορτώνουμε παράνομα στοιχεία από το διαδίκτυο στον υπολογιστή σας ή

αντίστροφα, και ότι τα ίχνη σας μπορούν να βρεθούν ακόμα και στην περίπτωση που χρησιμοποιούμε ψευδώνυμο.

9. Η κακόβουλη αλληλογραφία. μπορεί να στραφεί εναντίον μας και, επιπλέον, να υποστούμε τις συνέπειες του νόμου.

10. Ο Παροχέας Υπηρεσιών Διαδικτύου που χρησιμοποιείτε είναι υπεύθυνος για την ορθή χρήση των δεδομένων που του παρέχετε. Ρωτήστε τον/την τι είδους δεδομένα συλλέγει, επεξεργάζεται και αποθηκεύει, με ποιον τρόπο και για ποιο σκοπό. Να επαναλαμβάνετε την ερώτηση αυτή κατά διαστήματα. Να επιμένετε για την αλλαγή τους αν είναι λανθασμένα ή για τη διαγραφή τους αν είναι υπερβολικά, «ξεπερασμένα» ή περιττά. Να ζητάτε από τον Παροχέα σας να ενημερώνει τρίτους, στους οποίους έχει διαβιβάσει ή κοινοποιήσει τα δεδομένα σας για τυχόν τροποποιήσεις.

11. Αν δεν είστε ικανοποιημένος/η με τον τρόπο με τον οποίο ο Παροχέας σας συλλέγει, χρησιμοποιεί, αποθηκεύει, διαβιβάζει ή κοινοποιεί δεδομένα και αρνείται να αλλάξει τη συμπεριφορά του/της, τότε εξετάστε ενδεχόμενη αλλαγή Παροχέα. Αν πιστεύετε ότι ο Παροχέας σας δεν συμμορφώνεται με τους κανόνες προστασίας δεδομένων, μπορείτε να ενημερώσετε τις αρμόδιες αρχές ή να προβείτε σε ενέργειες σύμφωνα με το νόμο.

12. Να ενημερώνεστε για τους κινδύνους που σχετίζονται με την ασφάλεια και την ιδιωτικότητα στο Διαδίκτυο, καθώς και για τις διαθέσιμες μεθόδους και τεχνικές για τη μείωση αυτών των κινδύνων.

13. Αν σκοπεύετε να στείλετε δεδομένα σε άλλη χώρα, πρέπει να γνωρίζετε ότι ενδέχεται να παρέχεται μικρότερη προστασία εκεί. Αν τα εν λόγω δεδομένα αφορούν εσάς, είστε σαφώς ελεύθερος να τα διαβιβάσετε/κοινοποιήσετε. Ωστόσο, οφείλετε να συμβουλευτείτε, για παράδειγμα, την αρμόδια αρχή στη χώρα σας, προκειμένου να βεβαιωθείτε ότι επιτρέπεται η διαβίβαση δεδομένων, πριν αποστείλετε δεδομένα άλλων προσώπων στο εξωτερικό. Ίσως χρειαστεί να ζητήσετε από τον αποδέκτη να παράσχει τις απαραίτητες εγγυήσεις για την προστασία των δεδομένων.

1.4 Προς παρόχους υπηρεσιών Διαδικτύου

1. Οι κατάλληλες διαδικασίες που είναι διαθέσιμες πρέπει συνοδεύονται από πιστοποίηση, προκειμένου να προστατεύσετε την ιδιωτικότητα των ενδιαφερομένων (ακόμα και στην περίπτωση που δεν είναι χρήστες του Διαδικτύου), ιδιαίτερα, όσον αφορά στη

διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, καθώς και της φυσικής και λογικής ασφάλειας του δικτύου και των αντιστοίχων παρεχομένων υπηρεσιών.

2. Να πληροφορείτε τους χρήστες για τους κινδύνους, σχετικά με την ιδιωτικότητα, που παρουσιάζονται λόγω χρήσης του Διαδικτύου, προτού ολοκληρώσουν την εγγραφή τους ή αρχίσουν να χρησιμοποιούν τις προσφερόμενες υπηρεσίες. Οι κίνδυνοι αυτού του είδους μπορεί να αφορούν στην ακεραιότητα και την εμπιστευτικότητα των δεδομένων, στην ασφάλεια του δικτύου ή σε άλλους κινδύνους σχετικά με την ιδιωτικότητα, όπως η κρυφή συλλογή ή καταγραφή δεδομένων.

3. Να πληροφορείτε τους χρήστες για τα τεχνικά μέσα τα οποία μπορούν να χρησιμοποιούν νόμιμα προκειμένου να μειώνουν τους κινδύνους για την ασφάλεια των δεδομένων και των επικοινωνιών, όπως είναι η νόμιμα διαθέσιμη κρυπτογράφηση και οι ψηφιακές υπογραφές. Να προσφέρετε τέτοιου είδους τεχνικά μέσα σε τιμή κόστους, όχι σε απαγορευτική τιμή.

4. Προτού αποδεχθείτε την εγγραφή και τη σύνδεση χρηστών στο Διαδίκτυο, να τους πληροφορείτε για τις δυνατότητες ανώνυμης πρόσβασης, καθώς και για τις δυνατότητες χρήσης και εξόφλησης υπηρεσιών, με τρόπους που παρέχουν τη δυνατότητα διατήρησης της ανωνυμίας, όπως οι προπληρωμένες κάρτες πρόσβασης. Σε περιπτώσεις όπου η πλήρης ανωνυμία ενδεχομένως να μην επιτρέπεται λόγω νομικών περιορισμών, μπορείτε, εφόσον το επιτρέπει ο νόμος, να τους προσφέρετε τη δυνατότητα χρήσης ψευδωνύμων. Να πληροφορείτε τους χρήστες για την ύπαρξη προγραμμάτων τα οποία τους επιτρέπουν την ανώνυμη έρευνα και φυλλομέτρηση ιστοσελίδων στο Διαδίκτυο. Σχεδιάστε το σύστημά σας κατά τέτοιον τρόπο ώστε να παρακάμπτεται ή να ελαχιστοποιείται η χρήση προσωπικών δεδομένων.

5. Μη διαβάζετε, τροποποιείτε ή διαγράφετε μηνύματα που έχουν αποσταλεί σε τρίτα πρόσωπα.

6. Μην επιτρέπετε οποιαδήποτε παρεμβολή που αφορά στο περιεχόμενο της επικοινωνίας, εκτός εάν η εν λόγω παρεμβολή προβλέπεται από τον νόμο και εκτελείται από δημόσια αρχή.

7. Η συλλογή, η επεξεργασία και η αποθήκευση δεδομένων των χρηστών είναι θεμιτή μόνο όταν κρίνεται απαραίτητη για σαφείς, συγκεκριμένους και νόμιμους σκοπούς.

8. Μη διαβιβάζετε ή κοινοποιείτε δεδομένα εκτός εάν η επικοινωνία προβλέπεται από τον νόμο 8.

9. Μην αποθηκεύετε δεδομένα για χρονικό διάστημα μεγαλύτερο από αυτό που είναι απαραίτητο για να επιτευχθεί ο σκοπός της επεξεργασίας.

10. Μη χρησιμοποιείτε δεδομένα για ιδιοτελείς σκοπούς προώθησης/πώλησης υπηρεσιών ή/και αγαθών εκτός εάν το ενδιαφερόμενο άτομο έχει ενημερωθεί και δεν έχει εκφράσει αντίρρηση ή, στην περίπτωση της επεξεργασίας δεδομένων κίνησης ή ευαίσθητων δεδομένων, το ενδιαφερόμενο άτομο έχει δώσει τη ρητή συγκατάθεσή του.

11. Εσείς φέρετε την ευθύνη για την ορθή χρήση των δεδομένων. Στην εισαγωγική σας σελίδα τονίστε με σαφήνεια τη φράση «Πολιτική ιδιωτικότητας». Η φράση, αντίστοιχα, πρέπει να παραπέμπει σε ιστοσελίδα με αναλυτική επεξήγηση της πρακτικής ιδιωτικότητας που τηρείτε. Να ενημερώστε τους χρήστες για την ταυτότητά σας, το είδος των δεδομένων που συλλέγετε, επεξεργάζεστε και αποθηκεύετε, τον τρόπο, το σκοπό και το χρονικό διάστημα τήρησης των δεδομένων προτού αρχίσουν να χρησιμοποιούν τις υπηρεσίες, κατά τη διάρκεια της επίσκεψής τους στον τόπο σας και οποτεδήποτε ρωτηθείτε. Εάν είναι απαραίτητο, να ζητάτε τη συγκατάθεσή τους. Να διορθώνετε άμεσα ανακριβή δεδομένα κατόπιν αιτήσεως των χρηστών. Να διαγράφετε δεδομένα εάν αυτά είναι υπερβολικά, «ξεπερασμένα» ή περιττά και να σταματάτε την εκτέλεση της επεξεργασίας εάν υπάρχουν αντιρρήσεις εκ μέρους των χρηστών. Να ειδοποιείτε τα τρίτα πρόσωπα προς τα οποία έχουν διαβιβαστεί ή κοινοποιηθεί τα δεδομένα για τυχόν τροποποιήσεις. Αποφύγετε την κρυφή συλλογή δεδομένων.

12. Οι πληροφορίες που δίνονται στους χρήστες πρέπει να είναι ακριβείς και ενημερωμένες.

13. Σκεφτείτε το καλά προτού δημοσιεύσετε δεδομένα στον διαδικτυακό σας τόπο! Η δημοσίευση μπορεί να καταπατά την ιδιωτικότητα άλλων προσώπων και ενδέχεται να απαγορεύεται από τον νόμο. Επίσης η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί μια από τις σημαντικότερες παραμέτρους της ανάπτυξης του ηλεκτρονικού εμπορίου. Σε κάθε συναλλαγή ηλεκτρονικού εμπορίου συγκεντρώνονται πληροφορίες για τον πελάτη. Όμως, με την καταγραφή των προσωπικών δεδομένων του πελάτη, που γίνεται κατά εκούσιο τρόπο, ο φορέας παροχής υπηρεσιών έχει αυτόματα δημιουργήσει εικόνα για τα ενδιαφέροντα και τις συνήθειες του πελάτη. Τότε υπάρχει κίνδυνος να κάνει χρήση των δεδομένων αυτών με οποιοδήποτε τρόπο και για οποιοδήποτε σκοπό. Η οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των

των αυτων. και η οδηγια 97/96/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικου χαρακτηρα και την προστασια της ιδιωτικης ζωης στον τηλεπικοινωνιακό τομέα.[1]

1.5 Προστασία Προσωπικών Δεδομένων Στην Ελλάδα.

"Κάθε πολίτης πρέπει να είναι σε θέση να γνωρίζει κάθε στιγμή ποιος, πού, πότε, πώς και γιατί επεξεργάζεται τα προσωπικά του στοιχεία".

Στην Ελλάδα έχει ιδρυθεί και λειτουργεί από το Νοέμβριο του 1997 ως ανεξάρτητη διοικητική υπηρεσία η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με βάση το Νόμο 2472/97. Αποστολή της Αρχής Προστασίας Δεδομένων είναι η εποπτεία της εφαρμογής των νόμων και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Τα δεδομένα που συλλέγουν οι οργανισμοί ηλεκτρονικού εμπορίου για τους πελάτες τους, στα πλαίσια πραγματοποίησης ηλεκτρονικών συναλλαγών, αποτελούν προσωπικά δεδομένα και συνεπώς προστατεύονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Συγκεκριμένα κάθε οργανισμός ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την εν λόγω Αρχή.

Η Αρχή αυτή έχει τις εξής αρμοδιότητες:

- ✓ Να εκδίδει οδηγίες και κανονιστικές πράξεις για την εφαρμογή των διατάξεων που αφορούν στην προστασία προσωπικών δεδομένων και να γνωμοδοτεί για σχετικά θέματα.
- ✓ Να απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και να επιβάλλει/βοηθάει όσους διατηρούν αρχεία να καταρτίζουν κώδικες δεοντολογίας.
- ✓ Να καταγγείλει τις παραβάσεις στις αρμόδιες διοικητικές και δικαστικές αρχές αλλά και να επιβάλει κυρώσεις.
- ✓ Να ενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, ελέγχους σε κάθε αρχείο.

Στην χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την

επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/97),ενώ ο Νόμος 2774/1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα καταργήθηκε στις 29 Ιουλίου 2006

Ο Νόμος 2472/97 ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ και αναφέρεται στην "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Με λίγα λόγια καθορίζει τις υποχρεώσεις των φορέων και των υπηρεσιών που "εκτελούν την επεξεργασία" και θέτει τα δικαιώματα προστασίας των ατόμων, όσον αφορά την προστασία και διαφύλαξη των προσωπικών τους δεδομένων.

Με βάση το νόμο 2472/97:

- ✓ Η επεξεργασία προσωπικών πληροφοριών είναι επιτρεπτή μόνο στις περιπτώσεις που ο νόμος προσδιορίζει περιοριστικά και δεσμευτικά.
- ✓ Η επεξεργασία επιτρέπεται μόνο για νόμιμους ,θεμιτούς και εξειδικευμένους σκοπούς που είναι γνωστοί στον πολίτη.
- ✓ Αναγνωρίζονται και κατοχυρώνονται νέα δικαιώματα των πολιτών για να αμύνονται έναντι των προσβολών της ιδιωτικής ζωής και της προσωπικότητάς τους (δικαίωμα προηγούμενης πληροφόρησης, διόρθωσης, αποζημίωσης).

Οι ρυθμίσεις του νόμου 2472/97 συμπληρώθηκαν από το Νόμο 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών). Ο νόμος αυτός κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών.

1.6 Κανονισμοί Α.Δ.Α.Ε..

Η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) είναι ένας νέος φορέας που λειτουργεί με βάσει το Ν. 3115/2003 με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών.

Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαμβάνει διοικητικής αυτοτέλειας. Έδρα της ΑΔΑΕ είναι η Αθήνα, αλλά μπορεί με απόφαση της να εγκαθιστά και να λειτουργεί

γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της κοινοποιούνται στον Υπουργό Δικαιοσύνης και στο τέλος κάθε χρόνου υποβάλλεται έκθεση των πεπραγμένων της στη Βουλή. Η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον κανονισμό της Βουλής. Η ΑΔΑΕ για την εκπλήρωση της αποστολής της έχει τις ακόλουθες αρμοδιότητες:

- ✓ Διενέργεια αυτεπάγγελτων ελέγχων σε επιχειρήσεις και υπηρεσίες που έχουν γενικό αντικείμενο την επικοινωνία.
- ✓ Κατάσχεση ψηφιακών πειστηρίων, καταστροφή στοιχείων που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.
- ✓ Εξέταση καταγγελιών σχετικά με την προστασία των δικαιωμάτων των αιτούντων.
- ✓ Συνεργασία με άλλες αρχές της χώρας και με αντίστοιχες αρχές άλλων κρατών, για θέματα ασφάλειας επικοινωνιών.
- ✓ Έκδοση κανονισμού εσωτερικής λειτουργίας, ο οποίος δημοσιεύεται στην εφημερίδα της Κυβέρνησης.
- ✓ Έκδοση κανονιστικών πράξεων, μέσω των οποίων ρυθμίζεται κάθε δικαιοδοσία και λεπτομέρεια σε σχέση με τις αρμοδιότητες της Αρχής.
- ✓ Σύνταξη, μια φορά τον χρόνο, έκθεσης πεπραγμένων, στην οποία περιγράφεται το έργο της Αρχής, διατυπώνονται παρατηρήσεις και προτείνονται νομοθετικές μεταβολές στον τομέα διασφάλισης του απορρήτου των επικοινωνιών.

Το ηλεκτρονικό εμπόριο βασίζεται στην επικοινωνία των πελατών με τους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου. Για να γίνει μια ηλεκτρονική συναλλαγή, πρέπει πρώτα να επικοινωνήσει ο πελάτης με τον έμπορα, να δώσει τα προσωπικά του στοιχεία, τον αριθμό της πιστωτικής του κάρτας και να λάβει πληροφορίες σχετικές με τη συναλλαγή. Είναι προφανές ότι η επικοινωνία αυτή πρέπει να είναι απόρρητη, αφού σε καμιά περίπτωση τα προσωπικά στοιχεία του πελάτη και ιδιαίτερα οι αριθμοί των πιστωτικών του καρτών δεν πρέπει να γνωστοποιούνται σε τρίτους. Όπως αναφέρθηκε πιο πάνω, σκοπός της ΑΔΑΕ είναι η προστασία του απορρήτου των επικοινωνιών. Συνεπώς κάθε οργανισμός ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την ΑΔΑΕ. Η ΑΔΑΕ έχει εκδώσει κάποιους κανονισμούς για τη διασφάλιση του απορρήτου των επικοινωνιών και κάθε οργανισμός ηλεκτρονικού εμπορίου, σύμφωνα με τα παραπάνω, πρέπει να τους ακολουθεί. Η

ΑΔΑΕ ελέγχει τους οργανισμούς ηλεκτρονικού εμπορίου για την τήρηση των κανόνων, και η ίδια ελέγχεται από το κράτος.

Η ΑΔΑΕ έχει εκδώσει και δημοσιεύσει στην εφημερίδα της κυβερνήσεως κανονισμούς ασφαλείας για το διαδίκτυο, τη διασφάλιση απορρήτου τηλεπικοινωνιακής υποδομής, την κινητή και σταθερή τηλεφωνία, το θεσμικό πλαίσιο για την ασφάλεια, καθώς και την ασφάλεια για αυτόματες τραπεζικές συναλλαγές. Με δεδομένο ότι το μεγαλύτερο μέρος του ηλεκτρονικού εμπορίου πραγματοποιείται μέσω του διαδικτύου, κάθε οργανισμός ηλεκτρονικού εμπορίου πρέπει να συμμορφώνεται και να τηρεί τους κανονισμούς ασφαλείας για το διαδίκτυο. Συγκεκριμένα θα πρέπει να ακολουθεί τουλάχιστον τους κανονισμούς που περιγράφονται στη συνέχεια με λεπτομέρεια, οι οποίοι δημοσιεύθηκαν στις 26 Ιανουαρίου 2005 στην εφημερίδα της κυβερνήσεως.[3], [2]

1.7 Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις Συναφείς Υπηρεσίες και Εφαρμογές

Σκοπός του συγκεκριμένου Κανονισμού είναι:

- ✓ Η διασφάλιση του απορρήτου των διαδικτυακών επικοινωνιών.
- ✓ Η ασφάλεια των διαδικτυακών τηλεπικοινωνιακών φορέων και Δημοσίων οργανισμών.
- ✓ Η θέσπιση των υποχρεώσεων των εν λόγο φορέων αναφορικά με την ασφάλεια και το απόρρητο των επικοινωνιών.
- ✓ Ο έλεγχος στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα οι :

- ✓ Πάροχοι πρόσβασης στο Διαδίκτυο (σταθεροί και κινητοί τηλεπικοινωνιακοί πάροχοι, Internet, Servise Providers κτλ.).
- ✓ Πάροχοι διαδικτυακών υπηρεσιών.
- ✓ Πάροχοι διαδικτυακών υπηρεσιών προστιθέμενης αξίας.

Οι οργανισμοί ηλεκτρονικού εμπορίου είναι πάροχοι διαδικτυακών υπηρεσιών, αφού οι ηλεκτρονικές συναλλαγές πραγματοποιούνται μέσω του διαδικτύου. Συνεπώς οι οργανισμοί αυτοί πρέπει να εφαρμόζουν τον συγκεκριμένο Κανονισμό. Η ΑΔΑΕ ελέγχει του οργανισμούς αυτούς για την τήρηση του εν λόγω, και όχι μόνο, Κανονισμού.

ΚΕΦΑΛΑΙΟ 2ο

2.1 ΙΟΜΟΡΦΟΛΟΓΙΚΟ ΥΛΙΚΟ

2.1.1 Εισαγωγή

Το 1986 , οι Basit και Amjad Alvi, στην Λαχώρη του Πακιστάν, διέθεταν ένα κατάστημα εμπορίας λογισμικού στο οποίο πουλούσαν δικές τους εφαρμογές. Ανακάλυψαν, όμως, ότι οι χρήστες έκαναν πειρατεία του λογισμικού τους-απλά αντιγράφοντας το- και έτσι οι πωλήσεις τους έπεφταν με τον καιρό. Απάντησαν με το να γράψουν τον πρώτο ιό στην ιστορία των υπολογιστών, με το όνομα "brain",ο οποίος αντέγραψε τον εαυτό του σε κάθε δισκέτα ενώ παράλληλα έδειχνε ένα μήνυμα περί πνευματικής ιδιοκτησίας του λογισμικού που είχε αντιγράψει, στην , οθόνη του υπολογιστή.

Από αυτή την απλή αρχή ,η οποία δεν είχε καθόλου κακά κίνητρα, εξελίχθηκε μια ολόκληρη κουλτούρα ιών που αποτελεί μια από τις μάστιγες ενάντια στην ασφάλεια των υπολογιστικών συστημάτων και δικτύων. Φτάνουμε σήμερα να έχουμε κώδικες ιών που ελέγχουν εκατοντάδες χιλιάδες υπολογιστικά συστήματα για αδυναμίες τις οποίες εκμεταλλεύονται προκειμένου να εξαπλωθούν, δημιουργώντας αναρίθμητες απώλειες πληροφοριών αλλά και κεφαλαίων που δαπανούνται για την «ίαση» των προσβεβλημένων συστημάτων.

« Ένας υπολογιστικός ιός (computer virus) πρόκειται για ένα αυτόνομο εκτελεστικό πρόγραμμα, το οποίο προσκολλά –και αντιγράφει/εξαπλώνει τον εαυτό του- σε ένα υπολογιστικό σύστημα χωρίς την εξουσιοδότηση του διαχειριστή/χρήστη του. Το πρόγραμμα αυτό είναι γραμμένο με τέτοιο τρόπο, ώστε να εκτελείται μόνο του σε κάποια προγραμματισμένη στιγμή ή οποία από κάποιο γεγονός έναρξης (trigger) ,εξαπολύει τις εντολές που έχει γραμμένες στο σύστημα το οποίο εκτελείται.»

2.2 Δομή ιών

Η δομή λειτουργίας των ιών χωρίζεται σε τρεις κύριους τύπους, που και αυτοί –με την σειρά τους- χωρίζονται σε αρκετές υποκατηγορίες.:

- ✓ Ιούς τομέα εκκίνησης (boot record) ,οι οποίοι προσκολλώνται στο μέρος εκείνο των μαγνητικών μέσων (πχ δισκέτα ,σκληρό) που χρησιμοποιείται για να «φορτωθεί» το λειτουργικό σύστημα και να δοθεί ο έλεγχος στον χρήστη. Μέχρι τα τέλη της δεκαετίας του 80 η εκκίνηση του λειτουργικού συστήματος γινόταν κυρίως από δισκέτες, οπότε αποτελούσε και τον κύριο τρόπο διάδοσής τους.

Στους σκληρούς δίσκους, που μέχρι και σήμερα αποτελούν το κύριο μέσο εκκίνησης του λειτουργικού συστήματος, ένας τέτοιος ιός μπορεί να μολύνει το ενεργό διαμέρισμα (active partition) του δίσκου ή τον τομέα εκκίνησης (boot record) που εκτελείται κατά την αρχή της διαδικασίας εκκίνησης (boot) του συστήματος.

- ✓ Ιούς προγραμμάτων-αρχείων, οι οποίοι -συνήθως- μολύνουν εκτελέσιμα –και άλλα σημαντικά- αρχεία, τα οποία χρησιμοποιούνται για την εκτέλεση μιας εφαρμογής και έχουν τις παρακάτω καταλήξεις: COM, EXE, SYS, DLL, OVL κτλ.
- ✓ Μακρό-ιούς, οι οποίοι εμφανίστηκαν στα μέσα της δεκαετίας του 90 και μολύνουν αρχεία κειμένων ή άλλα εκτελέσιμα, τα οποία πιο πριν θεωρούνταν ως τα πιο ασφαλή από μόλυνση μια και δεν περιείχαν εκτελέσιμο ή προγραμματισμένο κώδικα.

2.2.1 Ιοί τομέα εκκίνησης

Μια δισκέτα ή ένα σκληρός δίσκος, δεν χρειάζεται να είναι εκκινήσιμος(bootable) για να μπορέσει να εξαπλώσει ένα τέτοιο ιό. Όλες οι δισκέτες έχουν κατάλληλα προγράμματα φόρτωσης του λειτουργικού συστήματος, τα οποία δημιουργούνται κατά την διαμόρφωσή τους (system format). Εάν μια δισκέτα έχει μολυνθεί από έναν τέτοιο ιό, τότε αυτός ενεργοποιείται όταν το σύστημα θα προσπαθήσει να εκκινήσει από την δισκέτα ή από τον σκληρό.

Ακόμα και αν το σύστημα δεν καταφέρει να εκκινήσει από μια μολυσμένη δισκέτα-δίσκο, ο ιός προσπαθεί να τρέξει την αυτοδύναμη ρουτίνα (bootstrat routine) που περιέχεται μέσα στην δισκέτα ή το δίσκο, καθώς αυτό είναι το μόνο που χρειάζεται για να ενεργοποιηθεί. Όπως ένα TSR (terminate and stay resident) πρόγραμμα, οι πιο πολλοί ιοί αυτού του είδους εγκαθιστούν τους εαυτούς τους στην μνήμη του συστήματος και επικάθονται στις διάφορες υπηρεσίες που προσφέρει το BIOS και το λειτουργικό σύστημα του χρήστη.

Ακόμη, παραμένουν ενεργοί στη μνήμη για όσο χρόνο το σύστημα λειτουργεί. Σ' αυτή την διάρκεια θα συνεχίζουν να μολύνουν τα καθαρά αρχεία εγγραφής εκκίνησης όποιων δισκετών εισέλθουν για οποιδήποτε σκοπό. Αυτό το είδος ιών αποτελεί μόλις το 5% της

συλλογής ιών των IBM PC, αλλά είναι υπεύθυνο για το 85% των μολύνσεων που αναφέρονται κάθε χρόνο.

2.2.2 Ιοί τομέα εκκίνησης δισκέτας

Οι περισσότεροι ιοί τομέα εκκίνησης δισκέτας μπορούν να μολύνουν τον κύριο τομέα εκκίνησης(boot sector) του σκληρού δίσκου που πιθανόν να υπάρχει στο σύστημα, ή το τμήμα εκκίνησης του ενεργού διαμερίσματος(active partition) του δίσκου. Μια δισκέτα αποτελεί κυρίως τον φορέα του ιού, που επιτρέπει την εξάπλωση σε «καθαρά» μηχανήματα καθώς και σε άλλες «καθαρές» δισκέτες ,οι οποίες με την σειρά τους θα συνεχίζουν το έργο της μόλυνσης. Βλέπουμε ,λοιπόν πως οι «ηλεκτρονικοί» ιοί μιμούνται πολύ την αρχιτεκτονική των βιολογικών ιών για την εξάπλωση τους.

2.2.3 Ιοί κύριου τομέα εκκίνησης σκληρού δίσκου

Η πλειοψηφία των ιών τμήματος εκκίνησης δισκέτας μολύνουν την κύρια εγγραφή εκκίνησης του σκληρού δίσκου. Ο ιός του κύριου τομέα εκκίνησης είναι μια άλλη μορφή των ιών που μολύνει την δισκέτα και επικάθεται -απλά- στην αντίστοιχη περιοχή του σκληρού δίσκου. Όπως και με τις άλλες μορφές του συγκεκριμένου είδους, το κύριο τμήμα εκκίνησης πρέπει να φορτωθεί από το σύστημα στην μνήμη πριν μπορέσει ο ιός να εκτελεστεί και να ενεργοποιηθεί.

Το λογισμικό που περιέχεται στον τομέα εκκίνησης ενός σκληρού, δισκέτας κτλ. είναι το πρώτο που φορτώνεται σε ένα σύστημα μια και η ευθύνη του προγράμματος αυτού είναι να φορτώσει λογισμικό υψηλού επιπέδου. Χωρίς αυτή την «αρχική φόρτωση δεν μπορεί να εκτελεστεί λειτουργικό σύστημα και κατά συνέπεια δεν μπορεί να λειτουργήσει ένας υπολογιστής.

Εάν αυτό το είδος ιών εισαχθεί στο σύστημα μετά την εκκίνηση του, δεν μπορεί να μολύνει το σύστημα. Πρέπει λοιπόν –οπωσδήποτε- να γίνει (τουλάχιστον μια φορά)εκκίνηση του υπολογιστή από μολυσμένο δίσκο ή δισκέτα. Ένα γνωστό παράδειγμα τέτοιου ιού είναι ο ιός Form ο οποίος όταν μόλυνε έκανε ένα "click" κάθε φορά και που πατιόταν ένα πλήκτρο σε ένα σύστημα, ενώ μπορούσε –επίσης- να εμποδίσει την εκκίνηση των υπολογιστών με λειτουργικό σύστημα Windows NT

2.2.4 Προγραμματιστικοί/Παρασιτικοί ιοί

Μια άλλη μεγάλη οικογένεια ιών, οι οποίοι προσαρτούν τον εαυτό τους σε άλλα συνήθως –εκτελέσιμα- προγράμματα είναι οι παρασιτικοί ιοί, Όταν ένας χρήστης εκτελέσει

ένα πρόγραμμα που έχει μολυνθεί από έναν τέτοιο ιό , τότε ο ιός επεμβαίνει και εκτελεί πρώτος τον εαυτό του. Για να αποκρύψει, όμως την παρουσία του και αν αποτρέψει τον χρήστη να καταλάβει ότι κάτι δεν πάει καλά, δίνει το δικαίωμα εκτέλεσης και στο πρόγραμμα που έχει ζητήσει ο χρήστης.

Από εκεί και πέρα, μια και το λειτουργικό σύστημα τον εκλαμβάνει σαν έγκυρο μέρος του προγράμματος που εκτέλεσε ο χρήστης του δίνονται τα ίδια δικαιώματα πρόσβασης που δίνονται και στο εκτελέσιμο πρόγραμμα του χρήστη, επιτρέποντας του να εγκατασταθεί στην μνήμη, να μολύνει και τα άλλα προγράμματα που θα εκτελεστούν έπειτα, ή/ και να αδειάσει το φορτίο του (payload).

Ένας τέτοιος, διάσημος, ιός είναι ο "Jerusalem" που εμφανίστηκε στις αρχές της δεκαετίας του 90. Αυτός ο ιός είχε σαν αποστολή να κάνει το σύστημα πιο αργό, καθώς και να διαγράφει κάθε αρχείο που εκτελούσε ο χρήστης(μετά την ενεργοποίηση του).

Ένας άλλος ιός, που πραγματικά συγκλόνισε και τρόμαξε την κοινότητα των χρηστών ήταν ένας ιός που πήγε τα πράγματα παραπέρα. Μέχρι τον Μάιο του 1998 ,ξέραμε πως το μεγαλύτερο κακό που θα μπορούσε να μας κάνει ένας ιός ήταν να διαγράψει όλα τα περιεχόμενα ενός σκληρού δίσκου. Μικρό το κακό εάν ο χρήστης μπορούσε να διατηρεί αντίγραφα ασφαλείας. Τον Ιούνιο του 1998,αυτό δεν αρκούσε πλέον, γιατί εμφανίστηκε ο ιός CIH .Πρόκειται για τον πρώτο ιό ο οποίος μπορούσε να κάνει πραγματική ζημιά , στον υπολογιστή που κανένα αντίγραφο ασφαλείας δεν θα μπορούσε να θεραπεύσει. Ο συγκεκριμένος ιός μπορεί να σβήσει το BIOS της μητρικής πλακέτας καθιστώντας τον άχρηστο και να ανίκανο να λειτουργήσει.!

Ο CIH γράφτηκε από τον Chen Ing-Hau και ενεργοποιείται στις 26 κάθε μήνα (ή στις 26 Ιουνίου κάθε χρόνου –ανάλογα με την έκδοση που έχει μολύνει το σύστημα) διαγράφοντας το BIOS και τον σκληρό δίσκο του συστήματος που βρίσκεται.

2.2.5 Κρυφοί ιοί

Οι κρυφοί ιοί, αποτελούν εξέλιξη των παρασιτικών ιών και προσπαθούν να κρύψουν την παρουσία τους από τον χρήστη. Οι περισσότεροι κρυφοί ιοί κρύβουν τον εαυτό τους μόνο όταν ο ιός είναι ενεργός στη μνήμη, ενώ εκτελείται σαν διεργασία του λειτουργικού συστήματος. Αυτοί οι ιοί, όταν καταλαβαίνουν ότι υπάρχουν αιτήσεις του συστήματος που μπορεί να αποκαλύψουν την παρουσία τους, επεμβαίνουν και τις αλλάζουν (ώστε να παραμένουν κρυφοί,) ενώ καταχωρούνται σαν να έχουν κρυφό μέγεθος ή δυνατότητες

κρυφής ανάγνωσης δεδομένων (ή και τα δύο).Το κρυφό μέγεθος έχει να κάνει αποκλειστικά με τους ιούς που μολύνουν τα αρχεία.

Όταν ένας τέτοιος μολύνει ένα εκτελέσιμο αρχείο, τότε συνήθως προσαρτά σε αυτό ένα αντίγραφο του εαυτού του. Αυτό έχει σαν αποτέλεσμα την αύξηση του μεγέθους του αρχείου (όσο είναι και το μέγεθος του ιού).Επειδή ο χρήστης μπορεί να καταλάβει την διαφορά η τεχνική απόκρυψης δείχνει να μην έχει μεταβληθεί το μέγεθος του αρχείου.

Με την εξέταση των περιεχομένων ενός μολυσμένου αρχείου, ένας έμπειρος χρήστης θα μπορούσε να καταλάβει την παρουσία ενός τέτοιου ιού καθώς και τις αλλαγές που έχει κάνει στο πρόγραμμα. Τότε ο ιός χρησιμοποιεί ένα είδος «κρυφτού», όπου προσπαθεί να κρύψει την παρουσία του μέσα στο αρχείο. Παρόλα αυτά είναι πολύ δύσκολο για ένα χρήστη να καταλάβει τις αλλαγές που έχουν γίνει σε ένα εκτελέσιμο πρόγραμμα(σε δεκαεξαδική ή δυαδική μορφή), καθώς οι πιο πολλοί ούτε καν μπαίνουν στον κόπο να το κάνουν.

Η μέθοδος κρυφής ανάγνωσης βοηθάει τον ιό (όταν πχ το λειτουργικό ή ένα άλλο πρόγραμμα ζητήσει να διαβάσει το –μολυσμένο- τμήμα εκκίνησης του υπολογιστή),να διαβάσει όλες του τις αιτήσεις ενώ, ενώ όταν εμφανιστεί κάτι τέτοιο, εμφανίζει στον χρήστη μια καθαρή έκδοση του τμήματος εκκίνησης (που έχει αποθηκευτεί πριν το μολύνει) κρύβοντας έτσι το πραγματικό. Αυτό μπορεί να ανιχνευτεί από κατάλληλα προγράμματα ανίχνευσης ιών .(Virus scanners).

2.2.6 Κρυπτογραφημένοι ιοί

Σε απάντηση και προσπάθεια αποφυγής των προγραμμάτων προστασίας από ιούς (signature scanning), οι κατασκευαστές των ιών άρχισαν να κρυπτογραφούν τους ιούς που δημιούργησαν. Η ιδέα ήταν να κρυφτεί και να παραμείνει αμετάβλητη η ταυτότητα του ιού με την κρυπτογράφηση του, ώστε να μη φαίνεται παρών σε ένα πρόγραμμα ανίχνευσης ιών.

Ένας κρυπτογραφημένος ιός αποτελείται από το κρυπτογραφημένο –κύριο- μέρος του ιού και μια αντίστοιχη ρουτίνα αποκρυπτογράφησης. Εάν ένας χρήστης εκτελέσει ένα μολυσμένο πρόγραμμα, τότε η ρουτίνα αποκρυπτογράφησης του ιού παίρνει τον έλεγχο του υπολογιστή και τον αποκρυπτογραφεί ενώ ο έλεγχος περνά πλέον στον ιό.

Ένας κρυπτογραφημένος ιός μολύνει τα προγράμματα όπως ένας απλός παρασιτικός ιός, με την διαφορά ότι, κάθε φορά που μολύνει ένα νέο πρόγραμμα, δημιουργεί ένα αντίγραφο του κύριου μέρους του αλλά και της ρουτίνας αποκρυπτογράφησης, τα οποία προσαρτά στο πρόγραμμα.

Για την κρυπτογράφηση του αντιγράφου του ιού χρησιμοποιείται ένα κλειδί κρυπτογράφησης το οποίο είναι προγραμματισμένο να αλλάζει, η κρυπτογράφηση του ιού γίνεται με διαφορετικό τρόπο, κάνοντας τον ιό να φαίνεται διαφορετικός από αρχείο σε αρχείο.

Το γεγονός αυτό καθιστά πολύ δύσκολη την ανίχνευση του από τα προγράμματα ανίχνευσης ιών, μια και κάθε φορά αλλάζει, χωρίς κα διατηρεί κάτι (που θα τον προδίδει) σταθερό. Παρόλα αυτά, οι ρουτίνες αποκρυπτογράφησης παραμένουν ίδιες από γενιά σε γενιά, γεγονός που αποτελεί χαρακτηριστική αδυναμία έναντι των προγραμμάτων προστασίας.

2.2.7 Πολυμορφικοί ιοί

Οι –απλοί- παρασιτικοί ιοί λειτουργούν με την δημιουργία και την προσκόλληση αντιγράφων τους σε κάθε αρχείο που μολύνουν .Με αυτή τη μέθοδο είναι πολύ εύκολο να ανιχνευτεί η ταυτότητα του ιού σε κάθε αρχείο, μια και θα βρίσκεται σε κάθε μολυσμένο αρχείο. Όπως είδαμε προηγουμένως, για να καταπολεμηθεί το γεγονός αυτό(από τους κατασκευαστές ιών) δημιουργήθηκαν οι κρυφοί και οι κρυπτογραφημένοι ιοί, αλλά και πάλι βρέθηκαν τρόποι και αδυναμίες στην κατασκευή τους.

Έτσι οι κατασκευαστές των ιών πέρασαν στην πιο εξελιγμένη μορφή παρασιτικών ιών, τους πολυμορφικούς, όπου πλέον όχι μόνο χρησιμοποιούνται τεχνικές stealth για την απόκρυψη ενός ιού μέσα στα αρχεία, όχι μόνο κρυπτογραφείται ο ιός για να μην ανιχνεύεται, αλλά πλέον ο ιός –μετά από κάθε μόλυνση-δημιουργείται και μια νέα ρουτίνα κρυπτογράφησης.

Κάθε αρχείο που μολύνεται με ένα τέτοιο ιό αποτελεί μια δεινή πρόκληση για τα προγράμματα ανίχνευσης ιών. Ο πρώτος πολυμορφικός ιός εμφανίστηκε το 1990, με το όνομα «1260» και γράφτηκε από τον Mark Washburn.

2.2.8 Ιοί Ρετρό

Όπως και στους αντίστοιχους βιολογικούς ιούς το αντικείμενο αυτών των ιών είναι να επιτεθούν στην απειλή της ύπαρξης τους, που δεν είναι άλλη από το πρόγραμμα ανίχνευσης τους. Ένας τέτοιος ιός ψάχνει να βρει αντίστοιχα προγράμματα ανίχνευσης ιών, από τα οποία προσπαθεί να διαγράψει συγκεκριμένα αρχεία(πχ τα αρχεία που περιέχουν τις ταυτότητες των ιών, αρχεία με τα αθροίσματα ελέγχου –checksums- διαφόρων αρχείων),ώστε να μην μπορούν αυτά να λειτουργήσουν ή να υπολειτουργούν. Ακόμα προσπαθούν να διαγράψουν

αυτήν την TSR (terminate and stay resident) εφαρμογή από την μνήμη, ώστε να μείνει το σύστημα χωρίς συνεχή προστασία, δίνοντας του την δυνατότητα να επεκταθεί άφοβα.

2.2.9 Ιοί συνδέσμων

Αυτή η κατηγορία ιών αποτελεί άλλον ένα πονοκέφαλο, μια και οι ιοί δεν επεμβαίνουν –άμεσα- στα αρχεία (σαν παρασιτικοί), αλλά δημιουργούν συνδέσμους μέσα σε καταλόγους οι οποίοι ενεργοποιούν την εκτέλεσή τους, χωρίς φυσικά αυτό να φαίνεται στον χρήστη.

2.2.10 Πολύ - διαχωρισμένοι Ιοί

Οι συγκεκριμένοι ιοί μολύνουν τόσο το τμήμα εκκίνησης του δίσκου, όσο και εκτελέσιμα προγράμματα. Δρουν δηλαδή και σαν τους ιούς του τομέα εκκίνησης και σαν τους παρασιτικούς, καθώς –όταν πρωτοέλθουν σε επαφή με ένα μηχάνημα- πρώτα μολύνουν το τμήμα εκκίνησης και έπειτα αρχίζουν και εξαπλώνονται –παράλληλα- και στα εκτελέσιμα αρχεία(που θα εκτελεστούν μετά την εκκίνηση του συστήματος)

2.2.11 Macro Ιοί

Οι μακρό ιοί στοχεύουν σε αρχεία δεδομένων με δυνατότητες εκτέλεσης μακροεντολών και έκαναν την εμφάνιση τους -σχετικά- πρόσφατα. Μέχρι σήμερα, αυτοί οι ιοί επηρεάζουν και μολύνουν αρχεία που προέρχονται από την σουίτα προγραμμάτων Office της εταιρείας Microsoft(κυρίως από τις εφαρμογές Word και Excel που προσφέρουν δημιουργία αρχείων με τέτοιες δυνατότητες).Παρόλα αυτά, αποτελούν απειλή για οποιαδήποτε εφαρμογή η οποία υποστηρίζει δυνατότητες εκτέλεσης και δημιουργίας μακροεντολών.

Μια μακροεντολή είναι μια συλλογή από ενέργειες οι οποίες εκτελούνται αυτόματα με την ίδια σειρά. Ας φανταστούμε μια μακροεντολή σαν ένα bach αρχείο(π.χ. autoexec.bat) το οποίο εκτελεί αυτόματα τα περιεχόμενα του όταν κληθεί ώστε να μην χρειάζεται κάθε φορά να το κάνει ο χρήστης

Οι μακρο-ιοί είναι ιοί που πολλαπλασιάζονται μόνοι τους. Εάν ένας χρήστης «ανοίξει» ένα κείμενο και εκτελέσει μία μακρο-εντολή που περιέχει έναν μακρο-ιό , τότε ο ιός αντιγράφει αυτόματα τον εαυτό του στα αρχεία εκκίνησης αυτής της εφαρμογής. Τώρα, ο υπολογιστής είναι μολυσμένος, μια και ένα αντίγραφο αυτού του ιού βρίσκεται σε ένα στρατηγικό σημείο του.

Εάν πρόκειται για κάποιο σύστημα που βρίσκεται σε ένα δίκτυο υπολογιστών, τότε είναι πολύ πιθανό να επεκταθεί η μόλυνση σε όλο το δίκτυο. Αυτή τη φορά, ο φορέας του ιού είναι αρχεία με μακροεντολές που μεταφέρονται με διάφορους τρόπους(π.χ. e-mail).

Ένα κακό, με αυτούς τους ιούς, είναι ότι μπορούν να γραφτούν χωρίς ιδιαίτερες γνώσεις, μια και δεν πρόκειται για προγραμματισμό σε γλώσσα μηχανής, αλλά για απλή αλληλουχία εντολών σε ψευδό-γλώσσα. Ένα άλλο κακό είναι ότι δεν επηρεάζονται από τις διαφορές στα λειτουργικά συστήματα (εκτελούνται σε επίπεδο εφαρμογής).

Όλα δείχνουν πως αυτό το είδος ιών πρόκειται να αυξηθεί στα επόμενα χρόνια, μια και ο φορέας τους (Internet) είναι αρκετά δημοφιλής, ενώ –επίσης-μολύνουν τα αρχεία, ειδικά στους χώρους εργασίας.

2.3 Πόσο εύκολα δημιουργείται ένας ιός

Εκτός από τον πηγαίο κώδικα διαφόρων τύπων που κυκλοφορεί ελεύθερα στο Internet,ένας χρήστης μπορεί να βρει επίσης έτοιμες σουίτες δημιουργίας ιών, μέσα από τις οποίες μπορεί να δημιουργήσει τον ιό της αρεσκείας του, επιλέγοντας τα χαρακτηριστικά του, τον τρόπο λειτουργίας του, ακόμα και το μέγεθος της ζημιάς που θέλει να προκαλέσει.

Από την άλλη πλευρά, ένας έμπειρος προγραμματιστής ,χρησιμοποιώντας μοντέρνα προγραμματιστικά εργαλεία σε συνδυασμό με πάγιες προγραμματιστικές ρουτίνες, μπορεί να δημιουργήσει ένα νέο ιό, βασιζόμενος σε κάποιον παλαιότερο.

2.4 Το μέλλον

Οι ιοί ολοένα και περισσότερο θα απασχολούν τους ειδικούς στην ασφάλεια των πληροφοριών. Οι τάσεις εξάπλωσης και εξέλιξής τους δείχνουν πως θα γίνονται ολοένα και πιο δραστικοί, ενώ θα μπορούσαν να διαδίδονται χωρίς καν να δρα ο δράστης.

Επίσης, η σύγκλιση της τεχνολογίας των υπολογιστών με την τεχνολογία των κινητών τηλεφώνων φέρνει τους ιούς ακόμα πιο κοντά στον μέσο χρήστη. Δεδομένου δε ότι οι «έξυπνες (οικιακές) συσκευές» αποτελούν πραγματικότητα στις αναπτυγμένες χώρες του δυτικού κόσμου, τα αποτελέσματα εξάπλωσης των ιών τείνουν να γίνουν ακόμα περισσότερο ενοχλητικά. Τέλος η γιγαντιαία υπολογιστική ισχύς η οποία βρίσκεται κατανεμημένη σε εκατομμύρια ψηφιακές συσκευές στον πλανήτη πιθανόν να αποτελέσει στόχο ενός ιού. Τα αποτελέσματα μιας τέτοιας περίπτωσης ξεπερνούν ακόμα και τα όρια της φαντασίας.

Στην αντίπερα όχθη, οι συνδυασμένες λύσεις είναι ίσως το μόνο πιθανό αντίμετρο. Ένα antivirus scanner δεν είναι ποτέ αρκετό από μόνο του. Στις περισσότερες περιπτώσεις

απαιτούνται συνδυασμένες λύσεις, οι οποίες πρέπει να περιγράφονται σε μια κατάλληλη πολιτική αντιμετώπισης και καταπολέμησης τέτοιων επιθέσεων.

Είναι σκόπιμο επίσης να παραδεχτούμε πως, τις περισσότερες φορές ,θεραπεύουμε – παρά προλαμβάνουμε- μια τέτοια επίθεση. Ίσως λοιπόν είναι κρισιμότερο να εστιάζουμε την προσοχή μας στην ανάκαμψη ενός μολυσμένου συστήματος, περιορίζοντας τις συνέπειες και εμποδίζοντας την εξάπλωση ενός ιού. [4]

2.5 Άλλες μορφές κακού κώδικα

2.5.1 Σκουλήκια (worms)

Ένα σκουλήκι (worm) είναι ένα αυτόνομο πρόγραμμα ή ομάδα προγραμμάτων το οποίο μπορεί να εξαπλωθεί από ένα σύστημα σε ένα άλλο. Αντίθετα με τους ιούς, ένα «σκουλήκι» δεν χρειάζεται να αλλάξει ένα πρόγραμμα(δρώντας παρασιτικά) για να εξαπλωθεί, καθώς είναι από μόνο του ένα πρόγραμμα το οποίο χρησιμοποιεί το δίκτυο, ψάχνοντας για μηχανήματα με «τρύπες» και exploits εφαρμογών, οι οποίες θα του επιτρέψουν να εξαπλωθεί ταχύτατα.

Το «πρόβλημα» με τους ιούς είναι ότι χρειάζεται λίγο και η «βοήθεια» του χρήστη για να εξαπλωθούν. Αντίθετα, ένα σκουλήκι, από την στιγμή που θα ενεργοποιηθεί θα κάνει όλη την δουλειά μόνο του(π.χ. θα ψάξει για «τρύπες» ,θα τις χρησιμοποιήσει, θα εξαπλωθεί σε νέα μηχανήματα Κ.Ο.).

Το 1988 εμφανίστηκε το πρώτο σκουλήκι με το όνομα «Internet worm» το οποίο είχε πολύ μεγάλη εξάπλωση και προκάλεσε μεγάλη ζημία. Η συγγραφή ενός σκουληκιού είναι ιδιαίτερα δύσκολη, καθότι έχει την δυνατότητα να προκαλέσει μεγάλη ζημιά. Επίσης η ανάγκη για συμβατότητα μεταξύ των υπολογιστικών συστημάτων και εφαρμογών κάνει ευκολότερη την διάδοσή τους .Ένα σκουλήκι μπορεί να είναι ένα απλό batch αρχείο (αρχείο εκτέλεσης εντολών) ή ένα πλήρες πρόγραμμα(π.χ. σε γλώσσα C) ή τέλος ένα script μιας γλώσσας προγραμματισμού (π.χ. Visual Basic).

Χαρακτηρίζονται συνήθως από την δυνατότητά τους να εξαπολύουν ταυτόχρονα πολλές και διαφορετικές επιθέσεις ,μια και η δομή τους έχει να κάνει με την ανίχνευση και την εκμετάλλευση αρκετών exploits που μπορεί να υπάρχουν σε ένα σύστημα, οι οποίες του δίνουν την δυνατότητα να επιτύχει παραπάνω από ένα αποτέλεσμα.[4]

2.5.2 Δούρειοι ίπποι (Trojan Horses)

Είναι προγράμματα που φαίνεται να κάνουν μια χρήσιμη εργασία για τον χρήστη ενώ στην πραγματικότητα επιτελούν μυστικά μια άλλη με απώτερο σκοπό την κατάλυση της ασφάλειας. Οι Δούρειοι ίπποι βρίσκονται σε μεγάλη εξάπλωση σήμερα, εκμεταλλευόμενοι της τρωικής αφέλειας των άπειρων χρηστών των ηλεκτρονικών υπολογιστών.

2.5.3 Προγράμματα Ζόμπι (Zombies)

Είναι προγράμματα που καταλαμβάνουν κρυφά κάποιον υπολογιστή που είναι συνδεδεμένος στον Διαδίκτυο και μετά χρησιμοποιούν αυτόν τον υπολογιστή για να εκκινήσουν επιθέσεις εναντίον υπολογιστών - στόχων. Συνήθως οι στόχοι τους είναι servers του Παγκόσμιου Ιστού με χιλιάδες αιτήσεις σύνδεσης, επιβραδύνοντας την λειτουργία αυτών με αποτέλεσμα την αδυναμία εξυπηρέτησης (Denial –of-service).Τα ζόμπι εμφυτεύονται σε εκατοντάδες υπολογιστές ανυποψίαστων χρηστών και ξεκινούν από εκεί τις επιθέσεις τους. Διατηρούν κρυφή ταυτότητα του δημιουργού τους.

2.5.4 Προγράμματα λαγοί (Rabbit programs)

Είναι προγράμματα που δεν έχουν σαν βασικό στόχο να προκαλέσουν ζημιά σε αρχεία αλλά να κλωνοποιήσουν τον εαυτό τους ατέρμονα ή να διατάξουν τον υπολογιστή να εκτελεί ενέργειες χωρίς νόημα, με στόχο να καταλύσουν τους πόρους (κεντρική και περιφερειακή μνήμη, επεξεργαστική ισχύ) του «μολυσμένου» υπολογιστικού συστήματος, και να προκαλέσουν την κατάρρευση του. Αυτή η επίθεση είναι από τις αρχαιότερες μορφές προγραμματιζόμενης απειλής.

2.5.5 Λογικές βόμβες (Logic Bombs)

Η λογική βόμβα ή σκουριασμένος κώδικας (slag code) είναι ένας κώδικας προγράμματος ο οποίος έχει εισαχθεί –συνήθως- εσκεμμένα σε ένα σύστημα είναι σχεδιασμένη να εκτελεστεί/εκραγεί κάτω από συγκεκριμένες συνθήκες λειτουργίας(π.χ. συγκεκριμένη χρονική στιγμή)που θα της επιτρέψουν να έχει τα επιθυμητά αποτελέσματα. Ουσιαστικά είναι ένας ιός με καθυστερημένη δράση και όταν εκραγεί μπορεί να έχει οποιασδήποτε μορφής αποτελέσματα(π.χ. διαγραφή αρχείων, αλλαγή στοιχείων, εμφάνιση μηνυμάτων).

Κάποιες μπορούν να ανιχνευτούν και να εξουδετερωθούν πριν την έκρηξή τους, μέσω περιοδικών ελέγχων όλων των αρχείων του συστήματος. Υποκατηγορία αυτών των προγραμμάτων είναι η ωρολογιακή βόμβα(Time bomb) που χρησιμοποιεί το εσωτερικό ρολόι

του υπολογιστή και είναι ιδιαίτερα χρήσιμη καθώς επιτρέπει να διαπραχθεί το αδίκημα ενώ ο ένοχος δεν είναι παρών.

2.5.6 Πίσω πόρτες (back doors or trap doors)

Είναι κομμάτια κώδικα που γράφονται σε εφαρμογές ή λειτουργικά συστήματα έτσι ώστε να δώσουν στους προγραμματιστές πρόσβαση σε προγράμματα χωρίς να χρειάζεται αυτοί να περάσουν από τις συνήθεις χρονοβόρες διαδικασίες ασφάλειας της πρόσβασης. Στην ουσία είναι τρύπες' ασφάλειας που δημιουργούνται εσκεμμένα. Ο όρος υιοθετήθηκε αργότερα από τους εισβολείς πληροφοριακών συστημάτων για να περιγράψει οποιοδήποτε μηχανισμό με τον οποίο θα μπορούσαν να αποκτήσουν πρόσβαση ξανά σε ένα ήδη παραβιασμένο σύστημα χωρίς να χρειαστεί να επαναλάβουν όλες τις διαδικασίες εισβολής που χρησιμοποίησαν πρώτη φορά. Ένα δημοφιλές πρόγραμμα για την εγκατάσταση πίσω πόρτας σε παραβιασμένο σύστημα είναι το Net cat.Οι πίσω πόρτες υφίστανται από τότε που άρχισαν να φτιάχνονται προγράμματα για υπολογιστές. Τυπικά φτιάχνονται από προγραμματιστές εφαρμογών που χρειάζονται κάποιο μέσο εκσφαλμάτωσης ή ελέγχου του κώδικα που αναπτύσσουν. Αρκετά συχνά αποτελούν τροποποίηση νόμιμου λογισμικού με κακόβουλο σκοπό.

Οι πίσω πόρτες μετατρέπονται σε απειλές όταν χρησιμοποιούνται από ασυνείδητους προγραμματιστές που θέλουν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Αποτελούν επίσης πρόβλημα όταν ο αρχικός προγραμματιστής της εφαρμογής ξεχάσει να αφαιρέσει την πίσω πόρτα όταν πια η εφαρμογή έχει διορθωθεί από όλα τα σφάλματα και κάποιος άλλος ανακαλύψει την ύπαρξή της.[5],[6],[7].

2.5.7 Μηνύματα απατηλού περιεχομένου (hoaxes) ή ειδήσεις μαϊμού!

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου : **«Προειδοποιητικά»**:είτε ειδοποιούν τον χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλή στο λειτουργικό του σύστημα και παροτρύνουν να προβεί σε συγκεκριμένες ενέργειες ή προειδοποιούν για πιθανές επιθέσεις, στην πραγματικότητα είναι ακίνδυνα.

«Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου και ζητούν την κινητοποίηση όσο περισσοτέρων χρηστών γίνεται. **«Εκφοβισμού»** αλυσιδωτές επιστολές στον χρήστη ότι θα του συμβεί κάτι κακό εάν δεν προωθήσει το μήνυμα σε άλλους χρήστες. Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοση τους το χάσιμο χρόνου απασχολούμενοι με αυτά και κυρίως η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. [29]

2.5.8 Spam: Η κατάρα του Διαδικτύου

Το spam συνήθως ορίζεται σαν «αυτόκλητο e-mail» και έχει ομοιότητες με τα διαφημιστικά φυλλάδια των καταστημάτων που κατακλύζουν τα ταχυδρομικά μας κουτιά. Ωστόσο το spam είναι πολύ περισσότερο από αυτό. Ανάλογα με τον ποιόν θα ρωτήσετε, μπορεί να περιλαμβάνει τα παρακάτω :

- ✓ Αυτόκλητο e-mail από νόμιμες επιχειρήσεις που προσπαθούν να προωθήσουν τα προϊόντα τους σε ένα ευρύτερο κοινό.
- ✓ Μαζικό e-mail από οργανισμούς που ανακοινώνουν νέες υπηρεσίες στις οποίες μπορεί να ενδιαφέρονται οι χρήστες.
- ✓ Απατηλό e-mail που προσπαθεί να προωθήσει διάφορα 'γίνετε πλούσιος' σενάρια τα οποία στην πραγματικότητα κάνουν πλούσιους τους δράστες και όχι τους παραλήπτες.
- ✓ Προσβλητικό e-mail που προσκαλεί τους χρήστες να γίνουν συνδρομητές πορνογραφικού περιεχομένου
- ✓ Πονηρό e-mail που περιλαμβάνει μικρά ενσωματωμένα (script code) και το οποίο όταν ανοιχτεί από τον παραλήπτη, ειδοποιείται αυτόματα ο αποστολέας, επιτρέποντας του να στείλει στην διεύθυνση του παραλήπτη μεγάλες ποσότητες spam.

Ένας περισσότερο επίσημος ορισμός του spam είναι οποιαδήποτε μορφή e-mail που προσπαθεί να αποκρύψει την διεύθυνση του αποστολέα έτσι ώστε να μην μπορεί να ανιχνευτεί ή που χρησιμοποιεί δόλο στην αναγραφή του θέματος του e-mail για να προκαλέσει τον παραλήπτη να το ανοίξει.

Το πρόβλημα με το spam έχει να κάνει εν μέρει με την ελευθερία του λόγου και εν μέρει με την φύση του Διαδικτύου: ένα κατανεμημένο σύστημα που στην ουσία δεν ελέγχει κανείς και που αναπτύχθηκε μέσω μιας σειράς από ηθελημένες αποφάσεις σε τεχνικά ζητήματα. Το spam διασχίζει εθνικά σύνορα και είναι δύσκολο να ξεχωριστεί από το νόμιμο e-mail. Σε λίγο καιρό το e-mail μια από τις σημαντικότερες και αρχαιότερες υπηρεσίες που προσφέρει το Διαδίκτυο, μπορεί να μετατραπεί σε ένα άχρηστο μέσο για νόμιμη επικοινωνία αν δεν γίνει κάτι να σταματήσει η τρικυμιώδης τάση του .

Η αυστηρή επιβολή κατάλληλης νομοθεσίας μπορεί να είναι η μόνη απάντηση ή πιο συγκεκριμένα ,οι μυνήσεις. Η νομοθεσία του spam έχει αρχίσει να κάνει την εμφάνιση της

,και κάνοντας χρήση αυτής, ίσως είναι δυνατόν να εναχθούν spammers σε διαφορετικές τοποθεσίες αφού το spam διασχίζει όλα τα σύνορα. Σχεδόν 9 στους 10 υπαλληλικούς χρήστες μιας έρευνας υποστήριξαν την νομοθεσία κατά του spam. [9]

2.5.9 Κακός σχεδιασμός ιστοσελίδων

Πολλές εταιρείες τώρα πουλάνε τα προϊόντα και τις υπηρεσίες τους μέσω του Διαδικτύου σε οποιονδήποτε διαθέτει ένα πρόγραμμα φυλλομετρητή. Όμως ο κακός σχεδιασμός του μηχανισμού για το καλάθι αγορών που διαθέτουν τα πολλά on line καταστήματα, μπορεί να επιτρέψει σε εισβολείς να αλλάξουν διάφορα πεδία της ιστοσελίδας, όπως για παράδειγμα η τιμή κάποιου προϊόντος. Πολλές μικρές κυρίως εταιρείες κάνουν ένα στοιχειώδες λάθος στον προγραμματισμό της ιστοσελίδας τους χρησιμοποιούν κρυμμένα HTML tags σαν τον μοναδικό μηχανισμό ανάθεσης τιμής σε κάθε προϊόν. Σε αποτέλεσμα αυτού, μόλις οι εισβολείς ανακαλύψουν αυτή την τρωτότητα, μπορούν να τροποποιήσουν την τιμή που βρίσκεται αποθηκευμένη στο κρυμμένο tag και να την μειώσουν δραματικά.

Για παράδειγμα, ας πούμε ότι κάποια εμπορική ιστοσελίδα έχει τον ακόλουθο κώδικα

HTML:

<FORM ACTION=http://192.168.51.101/cgi-bin/order.pl method="post"

<input type=hidden name="price" value=199.99">

< input type=hidden name="prd_id" value="X190"

QUANTITY :<input type=text name="quant" size=3 maxlength=3 value=1>.

Μετά μια απλή αλλαγή της τιμής με κάποιο απλό πρόγραμμα κειμενογράφου θα επιτρέψει στον εισβολέα να εισάγει την τιμή 1.99 αντί για 199.99(η τιμή που ίσχυε κανονικά):

<input type=hidden name="price" value"1.99">

Αν νομίζεται ότι αυτού του είδους οι προγραμματιστικές τρωτότητες είναι σπάνιες, δεν έχετε παρά να πληκτρολογήσετε στο πεδίο αναζήτησης της ιστοσελίδας:

http://www.google.com το εξής "type=hidden name=price", και θα ανακαλύψετε μερικές εκατοντάδες τέτοιες σελίδες.

2.5.10 Cookies (Λίγα κουλουράκια ;)

Ένα αδύνατο σημείο στο θέμα της ασφάλειας είναι τα cookies, μια λειτουργία η οποία έχει σαν στόχο να κάνει τη ζωή των χρηστών του Διαδικτύου ευκολότερη. Στον Παγκόσμιο Ιστό χρειάζεται να υπάρχει κάποιος τρόπος αποθήκευσης των προτιμήσεων των χρηστών. Τα cookies είναι ο λόγος που όταν κάποιος επιστρέφει ξανά σε κάποια ιστοσελίδα, η σελίδα τον «αναγνωρίζει».

Τα cookies είναι μικρά αρχεία δεδομένων, που αποθηκεύονται στους υπολογιστές των χρηστών. Ο σκοπός αυτών των αρχείων είναι να παρέχουν πληροφορίες για τους χρήστες, στους web servers που αυτοί συχνάζουν. Τα cookies μπορούν να απειλήσουν την ιδιωτικότητα και ανωνυμία των χρηστών αφού προσωπικά δεδομένα μπορούν να επεξεργαστούν από διάφορους ιστοχώρους και να δημιουργηθεί το προφίλ (web profile) του χρήστη με ευκολία.

Ένα cookie είναι ένα κομμάτι κειμένου το οποίο στέλνεται από έναν web server στον υπολογιστή μέσω του προγράμματος πλοήγησης που αυτός χρησιμοποιεί. Μόλις ληφθεί , το πρόγραμμα πλοήγησης ή φυλλομετρητής στέλνει αυτό το cookie κάθε φορά που ο χρήστης ζητάει κάποιο καινούργιο έγγραφο από τον web server.

Τα cookies μπορούν να χρησιμοποιηθούν για να αφαιρέσουν την ανωνυμία από τους χρήστες ή να την ενισχύσουν. Δυστυχώς η επιλογή βρίσκεται κάτω από τον έλεγχο του web server.Επιπλέον , μπορεί να είναι δύσκολο να κατανοήσει για ποιόν λόγο χρησιμοποιείται κάθε cookie.Τυπικές εφαρμογές των cookie είναι:

- ✓ Ένας ιστοχώρος με εμπορικά προϊόντα μπορεί να χρησιμοποιεί κάποιο cookie για να υλοποιεί ένα ηλεκτρονικό «καλάθι προϊόντων».
- ✓ Ένας ιστότοπος με νέα μπορεί να χρησιμέψει cookies για να παρέχει στους συνδρομητές της τοπικά νέα και πρόγνωση καιρού.
- ✓ Ένας ιστόχωρος που παρέχει υπηρεσίες μόνο σε συνδρομητές, μπορεί να χρησιμοποιεί cookies για να αποθηκεύει πληροφορίες σχετικές με τον συνδρομητή έτσι ώστε κάθε φορά που κάποιος συνδρομητής που μπαίνει στον ιστοχώρο να μην χρειάζεται να πληκτρολογεί το συνθηματικό του.

Μερικές ιστοσελίδες είναι με τέτοιο τρόπο ρυθμισμένες έτσι ώστε αν κάποιος χρήστης έχει ήδη κάποιο cookie ,να του παρέχει πλήρη πρόσβαση στις πληροφορίες του λογαριασμού του. Άλλοι ιστόχωροι όμως απαιτούν από τον χρήστη να εισάγει κάποιον

κωδικό ακόμα και αν ο υπολογιστής του έχει το κατάλληλο cookie .Γενικά αυτοί οι ιστόχωροι είναι πιο ασφαλείς. Αυτό οφείλεται στο γεγονός ότι κάποιο cookie ενός χρήστη μπορεί εύκολα να καταλήξει στον υπολογιστή κάποιου άλλου για παράδειγμα αν κάποιος χρήστης μπει στον ιδιωτικό λογαριασμό του χρησιμοποιώντας κάποιον κοινόχρηστο υπολογιστή (π.χ. κάποια σχολή) ή τον υπολογιστή κάποιου φίλου του. Όσο αφορά αυτούς που αναπτύσσουν εφαρμογές από τον Παγκόσμιο Ιστό, δεν θα πρέπει ποτέ να κάνουν το λάθος να νομίσουν ότι τα cookie είναι ασφαλή.[10]

2.5.11 Δηλητηριασμένα cookie.

Στο Microsoft Encyclopedia of Security του Mitch Tulloch, γίνεται μια πολύ σύντομη αναφορά στην τεχνική των δηλητηριασμένων cookies(cookie poisoning,cookie hijacking, cookie snarfing) είναι μια μορφή επίθεσης που περιλαμβάνει την μη εξουσιοδοτημένη τροποποίηση των cookies στους υπολογιστές των χρηστών. Πολύ περιληπτικά, ο εισβολέας τροποποιεί ένα συγκεκριμένο cookie στον υπολογιστή του χρήστη για να αποκτήσει την ταυτότητα του (identify theft) .Χρησιμοποιώντας το τροποποιημένο cookie ,ο εισβολέας μπορεί να επισκεφθεί ιστοχώρους που έχει ήδη επισκεφθεί ο χρήστης και να προσπαθήσει να αποκτήσει πρόσβαση σε προσωπικές πληροφορίες για τον χρήστη που έχουν αποθηκευμένες αυτοί οι ιστοχώροι, όπως ο αριθμός πιστωτικής κάρτας του χρήστη. [11]

Η καλύτερη προστασία σε τέτοιες επιθέσεις είναι η χρήση κρυπτογράφησης στα cookies από τους ιστοχώρους που τα χρησιμοποιούν έτσι ώστε οι εισβολείς να μην μπορούν να διαβάσουν ή να τροποποιήσουν πληροφορίες που βρίσκονται αποθηκευμένες σε αυτά.

2.6 Στεγανογραφία που χρησιμοποιείται για κακόβουλο σκοπό

Όπως μας πληροφορούν οι Edward Skoudis - Lenny Zeltser στο βιβλίο τους "Malware: Fifhting Malicious Code ",οι εισβολείς μπορούν τώρα να ενσωματώσουν κρυφά μηνύματα μέσα στον κώδικα προγραμμάτων .Το πρόγραμμα μπορεί να μοιάζει σαν ένα κανονικό εκτελέσιμο αρχείο το οποίο κάνει την δουλειά του απρόσκοπα αλλά μέσα στον κώδικα υπάρχει διάσπαρτο κάποιο μήνυμα. Σε αυτήν την περίπτωση το αρχείο αυτό μπορεί να λειτουργήσει σαν ένα μυστικό κανάλι επικοινωνίας μεταξύ εισβολέων. Η τέχνη και επιστήμη της κρυφής δημιουργίας μηνυμάτων ονομάζεται στεγανογραφία.[12]

Η παραδοσιακή κρυπτογράφηση μετατρέπει με μαθηματικό τρόπο ένα μήνυμα σε μια μορφή που δεν μπορεί να διαβαστεί άμεσα, ωστόσο ο εχθρός ξέρει ότι κάποιου είδους

επικοινωνία τελείται. Η στεγανογραφία αποκρύπτει το μήνυμα έτσι ώστε ο αντίπαλος δεν ξέρει καν ότι γίνεται επικοινωνία.

Στεγανογραφικές τεχνικές υπάρχουν εδώ και χιλιάδες χρόνια. Στον χώρο της επιστήμης των υπολογιστών, τους δόθηκε μεγάλη σημασία μόλις τα τελευταία χρόνια. Τυπικές τεχνικές στεγανογραφίας μπορούν να κρύψουν μηνύματα μέσα σε αρχεία εικόνων όπως: BMP, JPEG ή GIF.Άλλες τεχνικές κρύβουν πληροφορίες μέσα σε αρχεία ήχου όπως MP3 και WAV. Ωστόσο νεότερες τεχνικές που έκαναν την εμφάνιση τους μόλις το 2003, μπορούν να εσωκλείουν πληροφορία μέσα σε εκτελέσιμα προγράμματα χωρίς να τροποποιήσουν την λειτουργία η το μέγεθος των αρχείων τους!

Η στεγανογραφία επινοήθηκε στους αρχαίους καιρούς. Σύμφωνα με τον Ηρόδοτο, το μήνυμα, ένα τατουάζ στο κρανίο ενός δούλου, κρυβόταν με την επανάπτυξη των τριχών της κεφαλής.[12]

ΚΕΦΑΛΑΙΟ 3ο

3.1 ΑΣΦΑΛΕΙΑ ΠΕΡΙΜΕΤΡΟΥ

Ένα σύστημα firewall καλείται να λειτουργήσει ως ένας μηχανισμός «περιμετρικής άμυνας», ο οποίος δρα συμπληρωματικά με τους υπόλοιπους μηχανισμούς ασφάλειας. Σκοπός του είναι ο έλεγχος και η καταγραφή όλων των προσπαθειών προσπέλασης οι οποίες κατευθύνονται προς το προστατευόμενο σύστημα, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του.

Τα συστήματα ανίχνευσης εισβολών (IDS) προσπαθούν να ανιχνεύσουν οποιαδήποτε παράνομη δραστηριότητα στοχεύει σε δικτυακούς και υπολογιστικούς πόρους. Τα συστήματα αυτά συλλέγουν πληροφορίες από μια πληθώρα δικτυακών πηγών και συστημάτων και στη συνέχεια αναλύουν τις πληροφορίες για ενδείξεις εισβολής, προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης. Τα firewalls και τα IDS αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο. Στη συνέχεια του κεφαλαίου αυτού γίνεται μια αναλυτική περιγραφή των δυνατοτήτων και των περιορισμών των δύο αυτών σημαντικών τεχνολογιών για την ασφάλεια περιμέτρου, των firewalls και των IDS.

Ένα firewall είναι ουσιαστικά ένα «τείχος» ασφάλειας μεταξύ του μη ασφαλούς δημόσιου δικτύου και του ιδιόκτητου δικτύου που θεωρείται ασφαλές και αξιόπιστο. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν στο «απέναντι» δίκτυο. Ένα firewall δεν μπορεί να λειτουργήσει σωστά, ανεξαρτήτως του πως έχει σχεδιαστεί ή υλοποιηθεί, εάν δεν έχει καθοριστεί μια σαφής πολιτική ασφάλειας. Το firewall που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφάλειας που βρίσκεται κάθε φορά σε ισχύ και πρέπει να είναι συγκεκριμένη και σαφής. Το firewall αποτελεί την πρώτη γραμμή άμυνας του οργανισμού απέναντι στους επίδοξους εισβολείς, αλλά ποτέ τη μοναδική.

Η χρήση ενός φράγματος ασφάλειας δεν αποτελεί πανάκεια για την ασφάλεια του δικτύου. Όπως όλα τα συστήματα ασφάλειας μπορεί να παραβιαστεί από κάποιον ικανό εισβολέα. Επιπλέον το firewall αλληλεπιδρά με το διαδίκτυο και χρειάζεται ιδιαίτερη προσοχή στην εγκατάσταση του και την σωστή διαμόρφωσή του.

Τέλος, υπάρχουν και οι υβριδικές μορφές firewall, οι οποίες συνήθως συνδυάζουν τις λειτουργίες ενός proxy server με εκείνες ενός stateful inspection firewall. Τα περισσότερα προιόντα firewall είναι υβριδικά, συνδυάζοντας δύο η και περισσότερες τεχνολογίες, επωφελούμενα από τα προνόμια που προσφέρει η κάθε μία.

Οι επικριτές των firewalls συνήθως επικαλούνται τη δυσκολία της χρήσης τους καθώς απαιτούν πολλές συνδέσεις και μηχανισμούς. Τους καταλογίζουν επίσης ότι αποτελούν εμπόδια στην ελεύθερη χρήση του Διαδικτύου. Ακόμη υποστηρίζουν ότι τα firewalls δημιουργούν μια ψευδαίσθηση ασφάλειας, οδηγώντας σε χαλάρωση των μέτρων ασφάλειας εντός του προστατευόμενου δικτύου. Ωστόσο, όλοι συμφωνούν ότι τα firewalls είναι ισχυρά εργαλεία για την ασφάλεια των δικτύων, αλλά δεν αποτελούν πανάκεια για όλα τα προβλήματα ασφάλειας των δικτύων. Συνεπώς, δεν πρέπει να θεωρούνται ως υποκατάστατο μιας προσεκτικής διαχείρισης ασφάλειας μέσα σε ένα εσωτερικό δίκτυο.

Κάθε οργανισμός ηλεκτρονικού εμπορίου οφείλει να διαφυλάσσει τα προσωπικά δεδομένα των πελατών του και να λαμβάνει μέτρα ώστε αυτά να μην εκτίθενται σε μη εξουσιοδοτημένη πρόσβαση. Μπορούν να προσφέρουν αποτελεσματικές υπηρεσίες ελέγχου πρόσβασης για τα εσωτερικά δίκτυα των οργανισμών ηλεκτρονικού εμπορίου καθώς αποτελούν την πρώτη γραμμή άμυνας απέναντι σε εξωτερικές επιθέσεις. Συνεπώς τα firewalls αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο.

Πολλοί οργανισμοί ηλεκτρονικού εμπορίου έχουν συνδέσει τα εσωτερικά τους δίκτυα με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών, αλλά και για τη λήψη χρήσιμων πληροφοριών από τον παγκόσμιο ιστό. Η σύνδεση όμως ενός συστήματος στο διαδίκτυο (δημόσιο δίκτυο) δίνει τη δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό.

Τύποι firewalls

- ✓ Φιλτραρίσματος πακέτων(packet filter).
- ✓ Εξέτασης κατάστασης (stateful inspection).
- ✓ Επιπέδου κυκλώματος (circuit level-getaway).
- ✓ Επιπέδου εφαρμογής (application level -gateway).

3.1.2 Firewall φιλτραρίσματος πακέτων

Η συγκεκριμένη κατηγορία επιτρέπει (by default) σε κάθε εισερχόμενο/εξερχόμενο πακέτο να περάσει προς το εσωτερικό/εξωτερικό δίκτυο αντίστοιχα (και το Internet).Η διέλευση του απαγορεύεται μόνο εάν υπάρχει ενεργοποιημένος κάποιος κανόνας. Οι κανόνες αυτοί εξετάζονται με βάση ποιος ταιριάζει πρώτος (first fit basis)

Οι firewall της συγκεκριμένης τεχνολογίας δεν γνωρίζουν τίποτα για την σύνοδο(session) που έχει δημιουργηθεί στα παραπάνω επίπεδα, ούτε για τις δραστηριότητες των εφαρμογών, ενώ παράλληλα δεν πιστοποιούν την ταυτότητα των χρηστών, αλλά ούτε και των υπηρεσιών που χρησιμοποιεί το σύστημα. Τέλος, παρέχουν ελάχιστη καταγραφή γεγονότων(logging), η οποία περιορίζεται στις πληροφορίες που παρέχονται από την IP επικεφαλίδα στο εκάστοτε IP πακέτο.

3.1.3 Firewall εξέτασης κατάστασης

Τα συστήματα firewall εξέτασης κατάστασης (stateful inspection) λειτουργούν επίσης στο επίπεδο 3 του OSI, εξετάζοντας την IP επικεφαλίδα κάθε πακέτου, με τρόπο παρόμοιο ενός firewall φιλτραρίσματος πακέτων. Επιπλέον, όμως, διατηρούν μια λίστα με τα δεδομένα κατάστασης (state data) των προηγούμενων πακέτων.

Αυτά τα συστήματα συγκρίνουν το πρώτο πακέτο με μια ομάδα κανόνων. Εάν το πακέτο επιτρέπεται να «περάσει», τα δεδομένα κατάστασης του προστίθενται σε μια εσωτερική βάση δεδομένων, επιτρέποντας έτσι στα επόμενα πακέτα –μιας συνόδου- να τύχουν πιο γρήγορης επεξεργασίας. Η καταγραφή τους είναι παρόμοια με εκείνη που παρέχουν τα firewalls φιλτραρίσματος πακέτων.

3.1.4 Firewall κυκλώματος

Τα συστήματα firewall της συγκεκριμένης κατηγορίας λειτουργούν στο επίπεδη 4 του OSI, ελέγχοντας την TCP επικεφαλίδα κάθε πακέτου σύμφωνα με μια ομάδα κανόνων (ελέγχουν, επίσης, την πόρτα προέλευσης/ προορισμού).

Η αρχή λειτουργίας των συστημάτων αυτών βασίζεται στον έλεγχο της δραστηριότητας μιας δικτυακής συνόδου. Θεωρεί πως η κάθε πόρτα, η οποία περιγράφεται σε κάθε εισερχόμενο/εξερχόμενο πακέτο, αντιστοιχεί σε κάποια εφαρμογή, ενώ οι δυνατότητες καταγραφής γεγονότων (logging) είναι παρόμοιες με εκείνες των firewalls φιλτραρίσματος πακέτων. Γενικότερα, στο επίπεδο μεταφοράς (transport layer), ο firewall δρα σαν μια και μοναδική αρχή ελέγχου, καθώς αποσυναρμολογεί και συναρμολογεί κάθε

πακέτο που διέρχεται μέσα από αυτόν, εξασφαλίζοντας έτσι μια μοναδική εξουσιοδοτημένη ροή πληροφοριών, προστατεύοντας το δίκτυο και τα εσωτερικά συστήματα από επιθέσεις κατακερματισμένων IP πακέτων(IP fragmentation).

3.1.5 Firewall επιπέδου εφαρμογής (application –level gateway)

Τα συστήματα αυτά λειτουργούν στο επίπεδο 7 του OSI ελέγχοντας την TCP επικεφαλίδα του κάθε διερχόμενου πακέτου, σε σχέση με μια ομάδα κανόνων, ελέγχοντας ταυτόχρονα την ροή των δεδομένων σαν μια σύνδεση στο επίπεδο εφαρμογής. Αναγνωρίζουν, επίσης τις εντολές των υπηρεσιών-εφαρμογών και επιτρέπουν ή απαγορεύουν συγκεκριμένες πλέον εντολές, προσφέροντας εκλεπτυσμένο έλεγχο πάνω στην ροή των πληροφοριών

Ένα άλλο προνόμιο που προσφέρουν τα firewall αυτά είναι η λεγόμενη «μετάφραση διεύθυνσης δικτυού» ή «απόκρυψη δικτύου» (Network Address Translation (Network Hiding)-NAT). Σε ένα τέτοιο σενάριο, ο firewall είναι η μοναδική δίοδος από/προς το δίκτυο, καθώς λαμβάνει μια IP διεύθυνση, η οποία είναι και η μόνη που φαίνεται στο INTERNET,κρύβοντας έτσι τις εσωτερικές διευθύνσεις του δικτύου.

Επιπλέον, η λειτουργία του NAT προσφέρει ακόμα μια υπηρεσία την λεγόμενη «ανακατεύθυνση υπηρεσίας» με την οποία προστατεύονται συγκεκριμένα τμήματα του δικτύου που χρήζουν ιδιαίτερης προστασίας από τον «έξω κόσμο».Για παράδειγμα αν μια τοπολογία έχει στο εσωτερικό της μια βάση δεδομένων (ή όποιο άλλο σύστημα) η οποία δεν πρέπει να είναι προσπελάσιμη εξωτερικά τότε δημιουργείται μια εικονική βάση που φαίνεται στον «έξω κόσμο», ενώ ο firewall φροντίζει να ανακατευθύνει τις αιτήσεις από την εικονική στην πραγματική βάση, προσφέροντας ένα μεγαλύτερο επίπεδο ασφάλειας και ελέγχου.

3.2 Αδυναμίες των firewall

Η τεχνολογία των firewall δεν θα πρέπει να θεωρείται πανάκεια, μια και δεν είναι τίποτα άλλο παρά ένα πλέγμα, στο οποίο ρυθμίζουμε εμείς το μέγεθος των οπών του (καθορίζοντας έτσι τι μπορεί να περάσει και τι όχι).Τα firewall δεν μπορούν να εμποδίσουν μια σειρά από περιστατικά και ενέργειες, όπως:

- ✓ Την πειρατεία συνόδου ,όπου ο επιτιθέμενος παίρνει τον έλεγχο μιας συνόδου από ένα νόμιμο χρήστη (δηλ. έναν χρήστη που έχει πιστοποιήσει την ταυτότητα του).

- ✓ Το network data sniffing (ή snooping)
- ✓ Την παραποίηση δικτυακών δεδομένων
- ✓ Την επαναδρομολόγηση δικτυακών δεδομένων
- ✓ Την μεταμφίεση δικτυακών δεδομένων
- ✓ Τη διαρροή πληροφοριών, σε τρίτους, από νόμιμα εξουσιοδοτημένους χρήστες
- ✓ Την σύνδεση modems se συστήματα του εσωτερικού δικτύου για σύνδεση με εξωτερικά δίκτυα.
- ✓ Τις επιθέσεις social engineering.
- ✓ Την αποδοχή «μολυσμένων» αρχείων, χωρίς προηγούμενο έλεγχο τους
- ✓ Τις εσωτερικές επιθέσεις.

Για να θεωρείται επιτυχημένη η υλοποίηση και η χρήση ενός firewall ,θα πρέπει να υποστηρίζει μια γενικότερη –συνεπή και ολοκληρωμένη-λύση ασφάλειας, λειτουργικούς ελέγχους καθώς και συχνούς ελέγχους για την αποτίμηση του επιπέδου ασφάλειας στην δικτυακή δομή του οργανισμού. Τέλος δεν θα πρέπει να ξεχάσουμε πως οι κανόνες ελέγχου ενός συστήματος firewall πρέπει να καθορίζονται από μια συγκεκριμένη πολιτική ασφάλειας.

Πιο συγκεκριμένα, ένας ειδικευμένος μηχανικός ασφάλειας θα πρέπει να έχει πάντοτε στο μυαλό του τους παρακάτω πέντε κανόνες για την σωστή λειτουργία ενός firewall:

1. Δημιουργία μιας κατάλληλης πολιτικής ασφάλειας, η οποία θα ακολουθείται κατά γράμμα, δημιουργώντας ένα ασφαλές εσωτερικό δίκτυο(αποφεύγοντας πολλά από τα προβλήματα που αναφέραμε παραπάνω),αφήνοντας –αποκλειστικά-στο firewall την προστασία από εξωτερικές επιθέσεις.

2. Αντιμετώπιση του συστήματος από την σκοπιά ενός «επιτιθέμενου» (και όχι ενός «αμυνόμενου»).ώστε να μπορεί πρώτος να εξάγει συμπεράσματα ως προς τις ρυθμίσεις και την γενικότερη διάρθρωση (configuration) του firewall .

3. Εκπαίδευση και σωστή διαχείριση, ώστε όλοι οι χρήστες να γνωρίζουν τους κινδύνους και τις απειλές που μπορεί να αντιμετωπίσουν, καθώς και -στοιχειώδεις- ενέργειες αντιμετώπισης όταν κάτι κακό συμβεί, αποφεύγοντας καταστάσεις πανικού όταν εκδηλωθεί ή όταν αποκαλυφθεί μια επίθεση.

4. Χρήση ενεργητικής (proactive) ασφάλειας για την πλήρη ασφάλιση όλων των συστημάτων όπως π.χ.:

- ✓ Ασφαλή ρύθμιση (hardening) του λειτουργικού συστήματος στο οποίο εγκαθίσταται η εφαρμογή του firewall.
- ✓ Απενεργοποίηση ΟΛΩΝ των μη απαραίτητων υπηρεσιών.
- ✓ Χρήση μηχανισμών ισχυρής πιστοποίησης (strong authentication) ,όπου αυτό είναι απαραίτητο
- ✓ Έλεγχο για ύπαρξη back doors
- ✓ Έλεγχο για –μη εξουσιοδοτημένες- μεταβολές στις ρυθμίσεις των κρίσιμων συστημάτων.
- ✓ Υλοποίηση και χρήση ενός συστήματος ανίχνευσης εισβολής (Intrusion Detection System),για την έγκαιρη ανακάλυψη και αντιμετώπιση «ύποπτων» γεγονότων.
- ✓ Σχεδιασμό και υλοποίηση μιας πολιτικής αντιμετώπισης περιστατικών ασφάλειας(Incident Handling Response).

Συμπεράσματα

Τα μοντέρνα συστήματα firewalls είναι ουσιαστικά «υβρίδια» όλων των κατηγοριών που περιγράφηκαν παραπάνω και υλοποιούνται με συνδυασμό κατάλληλου υλικού και λογισμικού. Αν και η συγκεκριμένη τεχνολογία δεν μετρα περισσότερα από 10 χρόνια ζωής, η εκτεταμένη χρήση τους δείχνει πως το μέλλον θα αποτελέσουν βασικό και αναπόσπαστο κομμάτι κάθε δικτυακής αρχιτεκτονικής.

Η τάση σήμερα είναι ο συνδυασμός της χρήσης της ισχύος του υλικού (hardware)και της ευφυΐας του λογισμικού (software), δίνοντας έτσι το μεγάλο δυνατό αποτέλεσμα. Παράλληλα, σε εργαστηριακό επίπεδο ακόμη, γίνονται προσπάθειες ενσωμάτωσης τεχνικής νοημοσύνης (Artificial Intelligence-AI) ώστε να μπορούν τα συστήματα αυτά να αυτοδιαχειρίζονται.

Επίσης, τα πρώτα συστήματα τα οποία ενσωματώνουν την τεχνολογία ενός Δικτυακού Συστήματος Ανίχνευσης Εισβολών (Network Intrusion Detection System-NID) είναι πλέον πραγματικότητα, αν και παραμένει ανοιχτό το ζήτημα της απόδοσης. Ωστόσο,

με την ταχύτατη εξέλιξη της υπολογιστικής ισχύος, το τελευταίο θα πρέπει να θεωρηθεί απλά θέμα χρόνου.

Η εκτεταμένη χρήση της τεχνολογίας broadband συνδέσεων, καθιστά ένα firewall το απαραίτητο συμπλήρωμα κάθε οικιακού (προσωπικού) ή επαγγελματικού (σταθμού εργασίας) υπολογιστή. Μια και με την συγκεκριμένη τεχνολογία κάθε χρήστης θα μπορεί να είναι συνδεδεμένος στο παγκόσμιο δίκτυο 24 ώρες το 24ωρο, οι κίνδυνοι που κάποτε φαίνονταν μακρινοί τώρα χτυπούν - πραγματικά- την πόρτα μας.

Οι υποστηρικτές των firewalls τα θεωρούν σημαντικά, ως πρόσθετα μέτρα ασφάλειας, επειδή συγκεντρώνουν λειτουργίες ασφάλειας σε ένα και μόνο σημείο, απλοποιώντας την εγκατάσταση, τη ρύθμιση και τη διαχείριση.[13]

3.3 Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems)

Μια αναφορά

Τα συστήματα ανίχνευσης εισβολής (Intrusion Detection System-IDS) είναι προϊόντα με μορφή λογισμικού ή και υλικού, τα οποία αυτοματοποιούν την διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και αντίδρασης σε «ύποπτες» δραστηριότητες, οι οποίες στοχεύουν σε δικτυακούς και υπολογιστικούς πόρους. Τα συστήματα αυτά συλλέγουν πληροφορίες από μια πληθώρα δικτυακών πηγών και συστημάτων και στην συνέχεια, αναλύουν τις πληροφορίες τόσο για ενδείξεις εισβολής (επιθέσεις που προέρχονται εκτός εταιρικού δικτύου), όσο και για ενδείξεις κακής μεταχείρισης (επιθέσεις που έρχονται μέσα από εταιρικό δίκτυο), προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης.

Όταν ένα IDS ελέγχει για τέτοιου είδους ενδείξεις το δίκτυο λέγεται «σύστημα ανίχνευσης εισβολής δικτύου» ενώ όταν ελέγχει αρχεία καταγραφής (Long files) σε ένα συγκεκριμένο σύστημα τότε λέγεται «σύστημα ανίχνευσης εισβολής μεμονωμένου συστήματος»(Host based IDS) .Μια πραγματικά αποτελεσματική αρχιτεκτονική περιλαμβάνει και τις δυο τεχνολογίες.

3.3.1 Εσωτερική αρχιτεκτονική των IDS

Ένα απλοποιημένο μοντέλο ενός IDS συστήματος μπορεί να καθοριστεί σαν μια ομάδα από διάφορα αλληλεξαρτώμενα μέρη. Αυτά τα μέρη μπορεί να είναι:

- ✓ Συλλογή πρωτογενών δεδομένων από κατάλληλους αισθητήρες.
- ✓ Ανίχνευση και ενημέρωση του κατάλληλου προσωπικού για τα γεγονότα.

- ✓ Ανάλυση των δεδομένων.
- ✓ Αποθήκευση των δεδομένων σε μια αντίστοιχη βάση .
- ✓ Αντίδραση στα γεγονότα.
- ✓ Γραφικό περιβάλλον εργασίας για την διεπαφή με τον διαχειριστή.

Αυτές οι λειτουργίες μπορούν να υλοποιηθούν σε ξεχωριστά συστήματα, παρουσιάζοντας όμως το τελικό αποτέλεσμα σε ένα κεντρικό σταθμό διαχείρησης.

Ο σκοπός λειτουργίας των αισθητήρων (sensor) είναι η συλλογή των πληροφοριών σχετικά με συγκεκριμένα γεγονότα, καθώς και η προώθηση αυτών των πληροφοριών στα υπόλοιπα μέρη, αφού γίνει το σχετικό φιλτράρισμα από περιττά στοιχεία, μειώνοντας έτσι τον όγκο τους, καθώς και η παρουσίαση μόνο των σχετικών πληροφοριών.

Η λειτουργία μηχανής ανάλυσης έχει να κάνει με την πιο διεξοδική ανάλυση των στοιχείων που παρέχονται από την προηγούμενη λειτουργία της συλλογής καθώς και την εξαγωγή συμπερασμάτων για την απόπειρα ή πραγματοποίηση μιας επίθεσης στο παρελθόν ή στο μέλλον. Η μηχανή αυτή μπορεί να δημιουργήσει μεγάλο όγκο πληροφοριών, για αυτό συνίσταται ο καθορισμός του εύρους της ανάλυσης σε σχέση με το φιλτράρισμα των δεδομένων .Η καλή διαχείριση των πληροφοριών αυτών μπορεί να συμβάλλει στην αποτελεσματικότητα και την ταχύτατη λειτουργία του IDS.

Η λειτουργία της αποθήκευσης δεδομένων του IDS καθορίζει το μέσο στο οποίο αποθηκεύονται οι πληροφορίες που αφορούν στην ασφάλεια ενός συστήματος, ώστε να μπορούν αργότερα να χρησιμοποιηθούν από το προσωπικό για περαιτέρω ανάλυση.

Τέλος η αρχιτεκτονική των IDS ,περιλαμβάνει τη γεννήτρια αντιδράσεων σε γεγονότα(response generator) , η οποία αναλαμβάνει να προειδοποιεί το κατάλληλο προσωπικό για ένα περιστατικό ασφάλειας αλλά και να δράσει δυναμικά από μια συγκεκριμένη IP διεύθυνση ρύθμιση των δρομολογητών ή και του firewall για μπλοκάρισμα όλων των συνδέσεων από την συγκεκριμένη IP που προήλθε η επίθεση.

Έτσι ώστε να προστατευθεί το δίκτυο και τα συστήματα από περαιτέρω επιθέσεις μέχρι να γίνει ανάλυση των γεγονότων. Παρόλα αυτά, η συγκεκριμένη λειτουργία δεν περιλαμβάνεται σε όλα τα IDS.

Τι δεν μπορούν να κάνουν τα IDS?

Όπως και οι firewalls ,έτσι και τα IDS δεν είναι «μαγικά κουτιά» για να μπορούν να κάνουν τα πάντα. Αναλυτικότερα τα συστήματα αυτά:

- ✓ ΔΕΝ μπορούν να καλύψουν τα προβλήματα τυχόν ασθενών μηχανισμών πιστοποίησης ταυτότητας των χρηστών ενός οργανισμού.
- ✓ ΔΕΝ μπορούν να διεξάγουν έρευνες για επιθέσεις που συνέβησαν χωρίς την ανθρώπινη συμμετοχή και βοήθεια, ειδικότερα αν αναζητείται φυσικό πρόσωπο για απόδοση κατηγοριών.
- ✓ ΔΕΝ μπορούν να «διαισθανθούν »την καλύτερη δυνατή πολιτική ασφάλειας για ένα οργανισμό. Αυτό είναι μια δύσκολη και πολύπλευρη ανθρώπινη λειτουργία που τα IDS μπορούν να βοηθήσουν έμμεσα, παρέχοντας χρήσιμες πληροφορίες από την ανάλυση των στοιχείων που λαμβάνουν.
- ✓ ΔΕΝ μπορούν να καλύψουν τις αδυναμίες ασφάλειας των δικτυακών πρωτοκόλλων μια και τα πρωτόκολλα δρουν σαν ένα layer-below στο οποίο στηρίζονται τα IDS για να λειτουργήσουν αποτελεσματικά. Φυσικά, δεν ευθύνονται άμεσα όταν λόγω της έλλειψης ασφάλειας από τα πρωτόκολλα, περιορίζονται οι δυνατότητες τους.
- ✓ ΔΕΝ μπορούν να καλύψουν προβλήματα στην ποιότητα και ακεραιότητα των πληροφοριών που λαμβάνουν από τα άλλα συστήματα, μια και η λειτουργία τους στηρίζεται σε μια διαφορετική βάση (πχ λειτουργικό σύστημα),Αν η βάση είναι «αλλοιωμένη»(πχ bugs του λειτουργικού συστήματος),τότε κι τα IDS θα παρουσιάζουν αλλοιωμένα στοιχεία.
- ✓ ΔΕΝ μπορούν ακόμα να αντιμετωπίσουν αρχιτεκτονικές πρωτοκόλλων υψηλών ταχυτήτων, τα οποία χρησιμοποιούν κατακερματισμό πακέτων για να επιτύχουν καλύτερη απόδοση και ταχύτητα. Το IDS εκλαμβάνει το συγκεκριμένο γεγονός σαν επίθεση και είναι ιδιαίτερα δύσκολο να διαχωρίζει πότε πρόκειται για επίθεση και πότε κανονική ροή, ειδικά εάν αυτό γίνεται σε πολύ μεγάλες ταχύτητες.

Φυσικά, ακόμα και με τα παραπάνω μειονεκτήματα, η χρήση τους στα μοντέρνα IT περιβάλλοντα κρίνεται επιτακτική.

3.3.2 Ανίχνευση παρουσίας ενός IDS και επίθεση

Όπως προαναφέραμε, τα IDS έχουν το ρόλο του «ενεργού φύλακα» σε ένα δίκτυο, κοιτώντας συνεχώς για απόπειρες επίθεσης τόσο στο ίδιο το δίκτυο όσο και στα συστήματα του, προχωρώντας σε ανάλογη δράση όταν ανιχνεύσουν κάτι. Για ένα επιτιθέμενο, το IDS είναι ότι είναι ένα φυσικό σύστημα συναγερμού για ένα κλέφτη ο οποίος προσπαθεί να μπει σε ένα σπίτι, χωρίς να πιαστεί από το σύστημα αυτό.Στην περίπτωση αυτή, ένας «οργανωμένος» επιτιθέμενος πρέπει πρώτα να ψάξει να βρει και να απενεργοποιήσει το IDS (=συναγερμό) για να αποφύγει την ανίχνευση της παρουσίας του και την ειδοποίηση των διαχειριστών (=ιδιοκτήτη).Για τον λόγο αυτό, έχουν δημιουργηθεί και εξελίχθη πολλές τεχνικές για την ανίχνευση, επίθεση ή και αποφυγή ενός συστήματος IDS, οι οποίες συνήθως εκμεταλλεύονται γνωστά ελαττώματα σε πρωτόκολλα ή εσωτερικά bugs και αδυναμίες.

3.3.3 Αντί επιλόγου

Οι οργανισμοί θα πρέπει να καταλάβουν ότι η υλοποίηση και χρήση ενός συστήματος IDS είναι μια μακρόχρονη, σύνθετη και επίπονη διαδικασία η οποία κρύβει πολλές προκλήσεις. Εάν οι διαχειριστές νομίζουν ότι βάζοντας ένα IDS «στην πρίζα» θα δουλέψει σωστά χωρίς προηγούμενο σχεδιασμό και λεπτομερείς ρυθμίσεις, τότε όχι μόνο θα απομακρύνουν τους χρήστες (αλλά και τους ίδιους τους διαχειριστές) από την ιδέα και την χρήση των IDS ,αλλά – παράλληλα θα φέρουν τους επιτήδειους που θα θέλουν να επωφεληθούν από μια τέτοια κατάσταση. Εάν όμως μια τέτοια εγκατάσταση αντιμετωπιστεί σωστά ,θα αποτελέσει μια τεχνολογική πρόοδο, που θα μπορεί να αναβαθμίσει αρκετά τη γενική εικόνα και το επίπεδο της ασφάλειας ενός οργανισμού.[14]

ΚΕΦΑΛΑΙΟ 4°

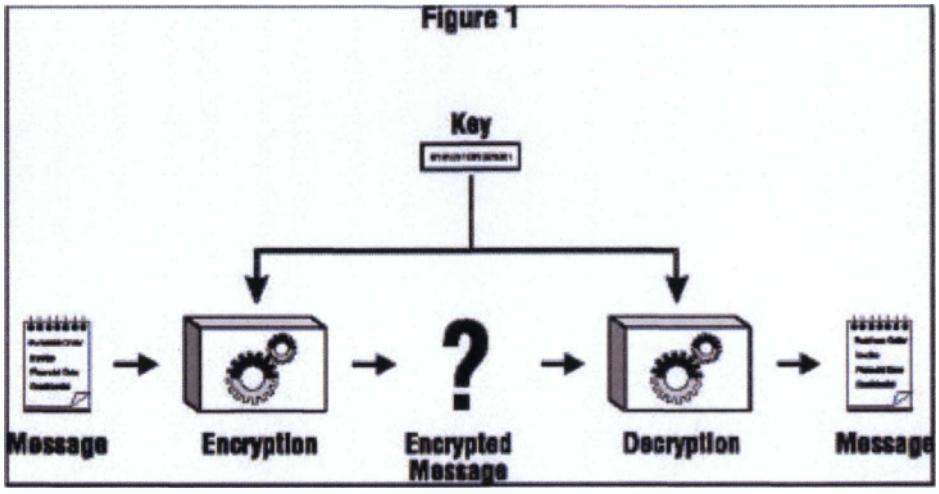
4.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

4.1.1 Τι είναι η κρυπτογράφηση

Κρυπτογράφηση είναι μια διεργασία μέσα από την οποία ένα μήνυμα (plaintext) μετατρέπεται σε ένα άλλο μήνυμα (cipher text) χρησιμοποιώντας μια μαθηματική συνάρτηση (αλγόριθμος κρυπτογράφησης) και ένα ειδικό password κρυπτογράφησης που ονομάζεται κλειδί.

Αποκρυπτογράφηση είναι η ανάποδη διεργασία: το cipher text μετατρέπεται στο αρχικό κείμενο (plaintext) χρησιμοποιώντας μια άλλη μαθηματική συνάρτηση και ένα άλλο κλειδί. Σε μερικά κρυπτογραφικά συστήματα το κλειδί κρυπτογράφησης και το κλειδί αποκρυπτογράφησης μπορεί να είναι το ίδιο.

Η διεργασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στην παρακάτω εικόνα:



Τι μπορούμε να επιτύχουμε με την κρυπτογράφηση

- ✓ Η κρυπτογράφηση μπορεί να παίξει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες:
- ✓ Μπορεί να προστατεύσει πληροφορίες αποθηκευμένες στον υπολογιστή μας από πρόσβαση ενός τρίτου, με ή χωρίς άδεια.
- ✓ Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες κατά την διάρκεια της μεταφοράς από το ένα υπολογιστικό σύστημα στο άλλο.

- [illegible] να χρησιμοποιηθεί για να εμποδίσει και να εντοπίσει τυχαίες ή σκόπιμες [illegible] στα δεδομένα μας.
- ✓ Μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού του.

Πέρα από πλεονεκτήματα, υπάρχουν και κάποια όρια τα οποία πρέπει να γνωρίζουμε για να αποφεύγουμε τα ανεπιθύμητα αποτελέσματα:

Η κρυπτογράφηση δεν μπορεί να προφυλάξει τα δεδομένα μας από κάποιον εισβολέα που θέλει να σβήσει τα δεδομένα μας.

- ✓ Ένας εισβολέας μπορεί να έχει τροποποιήσει και να εκθέτει ένα πρόγραμμα κρυπτογράφησης από μόνος του, έτσι ώστε να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα με το δικό του κλειδί. Ή μπορεί να κρατάει σε ένα αρχείο όλα τα κλειδιά για να τα χρησιμοποιεί αργότερα.
- ✓ Ένας εισβολέας μπορεί να έχει πρόσβαση στα αρχεία μας πριν τα κρυπτογραφήσουμε και αφού τα αποκρυπτογραφήσουμε.
- ✓ Ένας ίσως βρει έναν άγνωστο προηγούμενα και σχετικά εύκολο τρόπο να αποκρυπτογραφεί τα μηνύματα που εμείς κρυπτογραφούμε με έναν αλγόριθμο.

Για όλους αυτούς τους λόγους, η κρυπτογράφηση θα πρέπει να θεωρείται σαν ένα μέρος της ολιστικής στρατηγικής ασφάλειας που έχουμε, όπως είναι ο κατάλληλος έλεγχος πρόσβασης στον υπολογιστή μας.

4.1.2 Στοιχεία κρυπτογράφησης

4.1.2.1 Plaintext

Η πληροφορία την οποία θέλουμε να κρυπτογραφήσουμε.

4.1.2.2 Ciphertext

Η πληροφορία αφού αυτή κρυπτογραφήθηκε.

4.1.2.3 Αλγόριθμος κρυπτογράφησης

Ο αλγόριθμος κρυπτογράφησης είναι μια συνάρτηση,μαθηματικών αρχών, η οποία εκτελεί το έργο της κρυπτογράφησης και της αποκτυπτογράφησης των δεδομένων μας.

4.1.2.4 Κλειδιά κρυπτογράφησης

Τα κλειδιά κρυπτογράφησης χρησιμοποιούνται από τον αλγόριθμο κρυπτογράφησης για να ορίσουν πως τα δεδομένα είναι κρυπτογραφημένα ή αποκρυπτογραφημένα.Τα κλειδιά είναι παρόμοια με τα password των υπολογιστών: όταν ένα κομμάτι πληροφορίας κρυπτογραφήται, πρέπει να έχουμε το σωστό κλειδί για να έχουμε πρόσβαση πάλι σε αυτό.Αλλά αντίθετα με ένα πρόγραμμα που χρησιμοποιεί password, ένα πρόγραμμα κρυπτογράφησης δεν συγκρίνει το κλειδί που δίνουμε με το κλειδί που αρχικά χρησιμοποιούμε για να κρυπτογραφήσουμε το αρχείο, και μετά μας παρέχει πρόσβαση εάν τα δύο κλειδιά ταιριάζουν.Αντίθετα ένα πρόγραμμα κρυπτογράφησης χρησιμοποιεί το κλειδί μας για να μετατρέψει το ciphertext στο αρχικό κείμενο.Εαν δώσουμε το σωστό κλειδί θα πάρουμε το αρχικό μήνυμα.Εαν προσπαθήσουμε να αποκρυπτογραφήσουμε ένα αρχείο με λάθος κλειδί, θα πάρουμε σκουπίδια.

4.1.2.5 Μήκος κλειδιών

Όπως και με password, τα κλειδιά κρυπτογράφησης έχουν έν προκαθορισμένο μήκος Τα μακρύτερα κλειδιά είναι δυσκολότερο να τα μαντέψει κάποιος από τα μικρότερα γιατί υπάρχουν περισσότερα πιθανά κλειδιά που πρέπει να δοκιμάσει κάποιος επιτιθέμενος, για να βρεί το σωστό.Μερικά συστήματα κρυπτογράφησης μας επιτρέπουν να χρησιμοποιούμε διαφορετικό μήκος κλειδιών και μερικά μας επιτρέπουν μεταβλητού μήκους κλειδιών.

Η δύναμη και αντοχή ενός κρυπτογραφικού συστήματος εξαρτάται από τους εξής παράγοντες:

- ✓ Η μυστικότητα του κλειδιού
- ✓ Η δυσκολία να μαντέψουμε το κλειδί, ή να δοκιμάσουμε όλα τα πιθανά κλειδιά.
- ✓ Μακρύτερα κλειδιά είναι γενικά δυσκολότερο να βρεις.
- ✓ Η δυσκολία να αναστρέφουμε έναν αλγόριθμο κρυπτογράφησης χωρίς να γνωρίζουμε το κλειδί.
- ✓ Η ύπαρξη άλλων δρόμων, όπως λέμε «πίσω πόρτα» με τους οποίους μπορούμε να αποκρυπτογραφήσουμε πιο εύκολα ένα αρχείο χωρίς να γνωρίζουμε το κλειδί κρυπτογράφησης.
- ✓ Η ικανότητα να αποκρυπτογραφήσεις ένα ολόκληρο κρυπτογραφημένο μήνυμα γνωρίζεις τον τρόπο με τον οποίο αποκρυπτογραφήθηκε ένα μέρος αυτού.

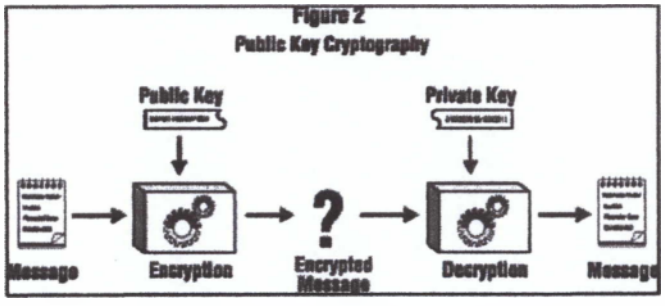
- ✓ Η ιδιοκτησία και η γνώση των χαρακτηριστικών του plaintext από ένα επιτιθέμενο.

4.2 Ευρέως διαδεδομένοι αλγόριθμοι κρυπτογράφησης και συναρτήσεις

Υπάρχουν δυο βασικά είδη κρυπτογραφικών αλγόριθμων σε χρήση σήμερα:

Κρυπτογραφία προσωπικού κλειδιού, η οποία χρησιμοποιεί το ίδιο κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσει το μήνυμα. Αυτός ο τύπος είναι επίσης γνωστός σαν κρυπτογραφία συμμετρικού κλειδιού.

Κρυπτογραφία δημοσίου κλειδιού, η οποία χρησιμοποιεί ένα δημόσιο κλειδί(public key) για να κρυπτογραφήσει το μήνυμα ,και ένα προσωπικό κλειδί για να το αποκρυπτογραφήσει. Το όνομα «δημόσιο κλειδί» οφείλεται στο γεγονός ότι μπορούμε να κάνουμε το κλειδί αυτό δημοσίως γνωστό χωρίς να διακινδυνεύουμε την μυστικότητα του μηνύματος ή του κλειδιού αποκρυπτογράφησης .Τα συστήματα δημοσίου κλειδιού είναι γνωστά σαν κρυπτογραφία ασύμμετρου κλειδιού.Μια παράσταση κρυπτογραφίας δημοσίου κλειδιού φαίνεται στην παρακάτω εικόνα:



Συναρτήσεις αποσύνθεσης μηνύματος

Μια συνάρτηση αποσύνθεσης μηνύματος δημιουργεί ένα μοναδικό πρότυπο από bits για μια δοσμένη είσοδο.Η τιμή αποσύνθεσης υπολογίζεται με τέτοιο τρόπο ώστε να είναι αδύνατο να υπολογιστεί μια είσοδος από ένα τεμαχισμένο μήνυμα χρησιμοποιώντας την ίδια τιμή της αποσύνθεσης.Οι αποσυνθέσεις μηνυμάτων θεωρούνται συχνά σαν δακτυλικά αποτυπώματα για αρχεία.

4.2.1 Αλγόριθμοι συμμετρικού κλειδιού

Οι αλγόριθμοι αυτοί χρησιμοποιούνται για μεγάλο όγκο δεδομένων ή επίσεις για δεδομένα με συνεχή ροή. Είναι σχεδιασμένοι να εκτελούνται με ταχύτητα και έχουν μεγάλο αριθμό πιθανων κλειδιών.Οι καλύτεροι αλγόριθμοι συμμετρικού κλειδιού φτάνουν το τέλειο: αν ένα δεδομένο κρυπτογραφηθεί με το δημόσιο κλειδί, δεν υπάρχει τρόπος να το αποκρυπτογραφήσεις χωρίς να έχεις το ίδιο κλειδί. Οι κατηγορίες των αλγόριθμων συμμετρικού κλειδιού είναι δυο: Σε αυτούς που κρυπτογραφούν ένα κομμάτι δεδομένων μονομιάς ή αλγόριθμους «μπλόκ»,και σε αυτούς που κάνουν την κρυπτογράφηση byte παρά byte σε δεδομένα συνεχής ροής ή αλγόριθμους «συρμού».

DES (Data encryption Standard) Εφαρμόστηκε από την κυβέρνηση των ΗΠΑ το 1997 και σαν ANSI πρότυπο το 1981 .Είναι ένας bloc αλγόριθμος που χρησιμοποιεί κλειδί 56-bit και έχει πολλούς τύπους λειτουργιών ανάλογα με τον σκοπό που χρησιμοποιείται. Είναι ένας δυνατός αλγόριθμος, αλλά πιθανολογείται ότι μια μηχανή που μπορεί να σπάσει ένα κρυπτογραφημένο μήνυμα σε μερικές ώρες μπορεί να κατασκευαστεί για περισσότερα από 1.000.000.Τέτοιες μηχανές ίσως υπάρχουν αν και καμία κυβέρνηση ή επίσημη εταιρεία δεν παραδέχεται ότι έχει.

DESX. Είναι μια απλή μετατροπή του DES αλγόριθμου για να βελτιώνει την ασφάλεια και να κάνει την αναζήτηση του κλειδιού δυσκολότερη. Περισσότερες πληροφορίες υπάρχουν στην RSA Data Security: http://www.rsa.com/rsalabs/newfaq.

TRIPLE DES.Είναι ένας τρόπος να κάνεις τον DES τουλάχιστον δυο φορές ποιο ασφαλές χρησιμοποιώντας τον DES αλγόριθμο τρείς φορές με τρία διαφορετικά κλειδιά.

IDEA. Αναπτύχθηκε στην Ζυρίχη από τους Massey-Lai και δημοσιεύτηκε το1990.Χρησιμοποιεί κλειδί 128-bit και θεωρείται ότι είναι πολύ ασφαλής. Ο IDEA χρησιμοποιείται από το πρόγραμμα PGP.

RC2 Είναι «bloc» αλγόριθμος και αναπτύχθηκε από τον RIVEST και κρατείται σαν επαγγελματικό μυστικό από την RSA. Αυτός ο αλγόριθμος ανακαλύφθηκε από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet. ΤΟ 1996 ο RC2 πωλείται με μια λειτουργία όπου μπορείς να χρησιμοποιήσεις κλειδιά από 1-2048-bit Συχνά το μήκος όμως φτάνει στα 40-bit, σε εφαρμογές που εξάγονται, και αυτό είναι πολύ ευάλωτο στην επίθεση έρευνας κλειδιού.

RC4 Είναι αλγόριθμος 'συρμού' και αναπτύχθηκε από τον RIVEST και κρατείται μυστικό από την RCA Επίσης αυτός ο αλγόριθμος ανακαλύφθηκε με τον ίδιο τρόπο το 1994

και εμφανίζεται αρκετά ασφαλής. Χρησιμοποιεί κλειδιά μήκους 1-bit -2048-bit ,και συχνά περιορίζεται σε 40-bit κλειδιά για προγράμματα που εξάγονται.

RC5 Είναι αλγόριθμος bloc, αναπτύχθηκε από τον Rivest και δημοσιεύτηκε το 1994.Ο RC5 επιτρέπει από τον χρήστη να ορίζει το μήκος του κλειδιού, το μέγεθος του bloc δεδομένων και το πόσες φορές θα γίνει η κρυπτογράφηση.

4.2.3 Αλγόριθμοι δημοσίου κλειδιού(public key)

Η ύπαρξη κρυπτογραφίας δημοσίου κλειδιού πρωτοπαρουσιάστηκε το φθινόπωρο του 1975 από τους Diffie-Helman. Οι δύο ερευνητές τότε στο Stanford University έγραψαν ένα έγγραφο στο οποίο υποστήριζαν την ύπαρξη μιας κρυπτογραφικής τεχνικής με την οποία μια πληροφορία που κρυπτογραφούταν με ένα κλειδί μπορούσε να αποκρυπτογραφηθεί από ένα δεύτερο, χωρίς να έχουν σχέση τα δυο αυτά κλειδιά. Μέχρι τότε μια ποικιλία από κρυπτογραφικά συστήματα είχαν αναπτυχθεί.Δυστιχώς υπήρχαν σημαντικά λιγότερα κρυπτογραφικά συστήματα δημοσίου κλειδιού από ότι συμετρικού. Η αιτία είχε να κάνει με τον τρόπο που είχαν σχεδιαστεί οι αλγόριθμοι.Καλοί συμετρικοί αλγόριθμοι απλά αλλάζουν την είσοδο ανάλογα με το κλειδί. Για να αναπτύξουμε ένα καινούργιο αλγόριθμο συμετρικού κλειδιού θα πρέπει να βρούμε έναν ασφαλή τρόπο να αλλάζουμε την είσοδο. Οι αλγόριθμοι δημοσίου κλειδιού στηρίζονται στα μαθηματικά. Αναπτύσοντας έναν τέτοιο αλγόριθμο απαιτείται να λυθεί ένα μαθηματικό πρόβλημα με ειδικές ιδιότητες.

Diffie-Hellman key exchange .Ένα σύστημα για ανταλλαγή κρυπτογραφικών κλειδιών ανάμεσα σε ενεργα μέρη.Το Diffie-Hellman δεν είναι ακριβώς μια μεθοδος κρυπτογράφησης –αποκρυπτογράφησης, αλλά μια μέθοδος ανάπτυξης και ανταλλαγής ενός μοιρασμένου κλειδιού σε ένα δημόσιο κανάλι επικοινωνίας. Στην πραγματικότητα τα δυο μέρη συμφωνούν σε μερικές κοινές αριθμητικές πράξεις, και τότε το κάθε μέρος δημιουργεί ένα κλειδί. Οι μαθηματικοί μετασχηματισμοί των κλειδιών ανταλλάσονται. Κάθε μέρος μπορεί να υπολογίσει ένα τρίτο κλειδί συνόδου το οποίο δεν μπορεί εύκολα να παραχθεί από έναν επιτιθέμενο που γνωρίζει και των δυο τις αριθμητικές τιμές.

RSA.Ο RSA είναι ένα πολύ γνωστό κρυπτογραφικό σύστημα αναπτυγμένο από τους καθηγητές του MIT. Ο RSA μπορεί να χρησιμοποιήθεί και για να κρυπτογραφεί πληροφορίες αλλά και σαν βάση του συστήματος ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για να αποδείξουν την πατρότητα και την γνησιότητα της ψηφιακής πληροφορίας. Το κλειδί μπορεί να είναι οποιουδήποτε μήκους, ανάλογα με την εφαρμογή που χρησιμοποιείται

ELGamal. Ο δημιουργός αυτού του αλγόριθμου είναι ο Taher ELGamal,ε είναι ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού που είναι βασισμένο στο πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman. Ο ELGamal χρησιμοποιείται για κρυπτογράφηση και για ψηφιακές υπογραφές με τον ίδιο τρόπο που χρησιμοποιείται ο RSA.

DSS. (Digital Signature Standard). Αναπτύχθηκε από την National Security Agency και εφαρμόστηκε σαν ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών.Είναι βασισμένος στον αλγόριθμο των ψηφιακών υπογραφών (DSA).Αν και ο DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, μόνο κλειδιά ανάμεσα σε 512 και 1024 bits επιτρέπονται.Κυρίως χρησιμοποιείται για ψηφιακές υπογραφές.

4.2.4 Συναρτήσεις αποσύνθεσης μηνυμάτων(Message digest functions)

Μια αποσύνθεση μηνύματος δεν είναι τίποτε άλλο από έναν αριθμό , έναν ειδικό αριθμό που βγαίνει από έναν ανακατεμένο κώδικα(hash code) ο οποίος προέρχεται από μια συνάρτηση που είναι δύσκολο να αντιστραφεί.Ο μοναδικός αυτός αριθμός έχει συνήθως 128 με 256 bits μήκος.Μια καλή συνάρτηση αποσύνθεσης μηνύματος πρέπει να συνδυάζει μερικές μαθηματικές ιδιότητες:

- ✓ Κάθε bit από την συνάρτηση αποσύνθεσης μηνύματος επηρεάζεται από κάθε bit της εισόδου της συνάρτησης.
- ✓ Εάν κάθε δοσμένο bit της εισόδου της συνάρτησης αλλάζει, τότε κάθε bit εξόδου έχει ποσοστό πιθανότητας αλλαγής 50%.
- ✓ Έχοντας ένα αρχείο εισόδου και την ανάλογη συνάρτηση αποσύνθεσης του,θα πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί κάποιο άλλο αρχείο που θα βγάλει τον ίδιο βαθμό αποσύνθεσης..

Οι συναρτήσεις αποσύνθεσης μηνυμάτων ονομάζονται επίσης και συναρτήσεις (hash functions) μιας κατεύθυνσης γιατί παράγουν τιμές που είναι δύσκολο να αντιστραφούν,ανθεκτικές στην επίθεση και μοναδικές ως επι τον πλείστον.

4.3 Υποδομή δημοσίου κλειδιού

Το τελευταίο κομμάτι του puzzle της κρυπτογραφίας είναι ένα σύστημα για να αποδεικνύει την ταυτότητα των ανθρώπων που κρατούν κρυπτογραφικά κλειδιά. Τα τελευταία χρόνια ένα τέτοιο σύστημα ονομάζεται υποδομή δημοσίου κλειδιού.

Στην κρυπτογράφηση δημοσίου κλειδιού κάθε χρήστης απαιτείται να φτιάξει δυο κλειδιά:

- ✓ Ένα δημόσιο κλειδί, το οποίο χρησιμοποιείται για να στέλνουμε κρυπτογραφημένα μηνύματα στον παραλήπτη, και για να επικυρώνουμε την ψηφιακή υπογραφή του αποστολέα.
- ✓ Ένα προσωπικό κλειδί, το οποίο χρησιμοποιείται από τον παραλήπτη για να αποκωδικοποιήσει τα κρυπτογραφημένα μηνύματα που λαμβάνει και για να υπογράψει με την ψηφιακή υπογραφή του ο αποστολέας.

Ενώ τα προσωπικά κλειδιά είναι σχεδιασμένα να κρατιούνται μυστικά, τα δημόσια κλειδιά είναι σχεδιασμένα να δημοσιεύονται και να διανέμονται ευρέως.

Ένας απλός τύπος δημοσίου και προσωπικού κλειδιού περιέχει ελάχιστη πληροφορία εκτός από τις πραγματικές τιμές που χρειάζονται για να γίνει η κρυπτογράφηση και αποκρυπτογράφηση. Θα μπορούσαμε να πούμε ότι χρειαζόμαστε περισσότερες πληροφορίες να αποθηκεύονται σε κάθε δημόσιο κλειδί. Μαζί με την πληροφορία κρυπτογράφησης, ίσως επιθυμούμε να αποθηκεύσουμε το όνομα του χρήστη ή κάποια άλλη πληροφορία ταυτότητας. Για παράδειγμα αν έχουμε τρία δημόσια κλειδιά για τρεις ανθρώπους είναι δύσκολο να τα ξεχωρίσουμε. Αν όμως αποθηκεύσουμε περισσότερη πληροφορία στου καθένα το προσωπικό κλειδί, θα έχουμε τρόπο να ξέρουμε ποιο προσωπικό κλειδί ανήκει σε ποιανού το δημόσιο κλειδί.

Η περιοχή του ονόματος μπορεί να συμπληρωθεί με οποιοδήποτε στοιχείο που θέλουμε. Άπαξ και το κλειδί δημιουργηθεί με ένα όνομα, αυτό μπορεί να υπογραφεί από ένα τρίτο πρόσωπο. Τα τρίτα πρόσωπα που επικυρώνουν την πληροφορία του κλειδιού πριν αυτό υπογραφεί αυτό ονομάζονται αρχές πιστοποίησης. [15],[16].

ΚΕΦΑΛΑΙΟ 5°

5.1 Κρυπτογραφία στο Web

5.2 Λειτουργίες της κρυπτογράφησης

Οι επαγγελματίες που ασχολούνται με την ασφάλεια έχουν ταυτίσει τέσσερις λέξεις για να περιγράφουν όλες τις λειτουργίες που εκτελεί η κρυπτογραφία στα σύγχρονα πληροφοριακά συστήματα. Οι διαφορετικές λειτουργίες είναι:

5.2.1 Confidentiality-Εμπιστευτικότητα

Η κρυπτογραφία χρησιμοποιείται για να μεταμορφώνει την πληροφορία που στέλνεται μέσω Internet και αποθηκεύεται στους servers, έτσι ώστε να μην μπορούν να δουν το περιεχόμενο των δεδομένων αυτοί που κρυφοκοιτάνε.. Μερικοί ονομάζουν αυτή τη ιδιότητα μυστικότητα (privacy) αλλά οι περισσότεροι χρησιμοποιούν αυτή την λέξη για να αναφέρονται στην προστασία της ατομικής πληροφορίας.

5.2.2 Authentication-Επικύρωση-Απόδειξη γνησιότητας

Οι Ψηφιακές Υπογραφές χρησιμοποιούνται για να εξακριβώνουν την ταυτότητα του αποστολέα ενός μηνύματος. Οι παραλήπτες ενός μηνύματος μπορούν να ελέγξουν την ταυτότητα του αποστολέα, ο οποίος υπέγραψε ψηφιακά το μήνυμα. Μπορούν να χρησιμοποιηθούν σε συνδυασμό με τα password ή και να τα αντικαταστήσουν.

5.2.3 Integrity-Ακεραιότητα

Υπάρχουν μέθοδοι που ελέγχουν αν ένα μήνυμα έχει μεταβληθεί την στιγμή την στιγμή της μεταφοράς. Συχνά αυτό γίνεται με τους κώδικες αποσύνθεσης μηνυμάτων ψηφιακά υπογεγραμμένων.

5.2.4.No repudiation-Απαγόρευση απάρνησης

Οι κρυπτογραφημένες αποδείξεις δημιουργούνται έτσι ώστε ο αποστολέας να μην μπορεί να απαρνηθεί το γεγονός της αποστολής του μηνύματος του.

5.3 Κρυπτογραφικά συστήματα που χρησιμοποιούνται σήμερα

Τα τελευταία χρόνια έχουν αναπτυχθεί και χρησιμοποιηθεί αρκετά κρυπτογραφικά συστήματα για το Internet.Μπορούμε να τα χωρίσουμε σε δύο κατηγορίες: Η πρώτη είναι

προγράμματα και πρωτόκολλα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mail).Τα ποιο δημοφιλή είναι τα παρακάτω:

- ✓ PGP
- ✓ S/MIME

Η δεύτερη κατηγορία είναι πρωτόκολλα δικτύου που χρησιμοποιούνται για να παρέχουν εμπιστευτικότητα, ακεραιότητα, αναγνώριση ταυτότητας σε περιβάλλον δικτύου. Τέτοια συστήματα χρειάζονται αλληλεπίδραση πραγματικού χρόνου ανάμεσα στο client και σε ένα server για να δουλέψουν σωστά. Τα πιο δημοφιλή είναι τα παρακάτω:

- ✓ SSL
- ✓ PCT
- ✓ S-HTTP
- ✓ SET and CyberCash
- ✓ DNSSEC
- ✓ IPsec and IPv6
- ✓ KERBEROS
- ✓ SSH

5.3.1 PGP (Pretty Good Privacy)

Το PGP είναι το πρώτο πρόγραμμα κρυπτογράφησης δημοσίου κλειδιού, γραμμένο από τον Zimmerman και κυκλοφόρησε στο Internet τον Ιούνιο του 1991. Το PGP είναι ένα ολοκληρωμένο σύστημα που προσφέρει κρυπτογραφική προστασία των e-mails και των αρχείων γενικότερα. Το PGP επίσης είναι ένα σύνολο από standards που περιγράφουν τα formats των κρυπτογραφημένων μηνυμάτων, των κλειδιών και των ψηφιακών υπογραφών.

Είναι ένα κρυπτογραφικό σύστημα που χρησιμοποιεί τον RSA αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού για την διαχείριση των κλειδιών και τον IDEA συμμετρικό αλγόριθμο για την κύρια κρυπτογράφηση των δεδομένων.

Το PGP προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος που χρησιμοποιεί είναι ο IDEA.Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης που χρησιμοποιεί είναι ο MD5.Προσφέρει αναγνώριση γνησιότητας με την

χρήση των δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

Το PGP είναι διαθέσιμο με δύο τρόπους, σαν μία μεμονωμένη εφαρμογή και σαν ένα ολοκληρωμένο πρόγραμμα ηλεκτρονικού ταχυδρομείου διαθέσιμο από την PGP Inc.

Το μεμονωμένο πρόγραμμα τρέχει σε πολύ περισσότερα προγράμματα από ότι το ολοκληρωμένο πρόγραμμα, αλλά είναι περισσότερο δύσχρηστο. Ένα τέτοιο παράδειγμα που ήταν πολύ διαδεδομένο είναι οι εκδόσεις του PGP για περιβάλλον DOS. Επίσης η PGP Inc αναπτύσσει διάφορα plug-ins για δημοφιλή προγράμματα ηλεκτρονικού ταχυδρομείου για να επιτρέψει σε αυτά να στέλνουν και να λαμβάνουν κρυπτογραφημένα μηνύματα με το PGP.

Ένα πρόβλημα με το PGP είναι η διαχείριση και πιστοποίηση των δημοσίων κλειδιών. Τα δημόσια κλειδιά δεν έχουν ημερομηνία λήξης, αντί αυτού, όταν τα κλειδιά εκτεθούν, εξαρτάται από τον ιδιοκτήτη εάν αυτός θέλει να διανέμει σε όλους αυτούς με τους οποίους ηχεί επικοινωνία μια ειδική PGP πιστοποίηση απόσυρσης(ακύρωσης). Οι ανταποκριτές που δεν μαθαίνουν το γεγονός αυτό και χρησιμοποιούν το εκτεθειμένο κλειδί για εβδομάδες, μήνες και χρόνια αργότερα, για να στείλουν κρυπτογραφημένα μηνύματα ρισκάρουν την ασφάλεια των μηνυμάτων. Αυτό έχει σαν αποτέλεσμα, εάν δημιουργήσουμε και διανέμουμε ένα δημόσιο κλειδί, πρέπει να κρατήσουμε το μυστικό κλειδί για πάντα επειδή αυτό το κλειδί δεν λήγει ποτέ.

Η πρόσφατη έκδοση του PGP5 χρησιμοποιεί ένα νέο τύπο κλειδιών με κρυπτογραφικούς αλγόριθμους τον DSS και τον Diffie-Helman.

5.3.2 S/MIME (Multipurpose Internet Mail Extentions)

Το MIME είναι ένα standard για αποστολή αρχείων με binary attachments μέσω του Internet .Το Secure/MIME είναι μια επέκταση του MIME standard για την αναγνώριση των κρυπτογραφημένων e-mail.Αντίθετα από το PGP το S/MIME δεν εφαρμόστηκε σαν ένα αυτόνομο πρόγραμμα, αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου. Επειδή αυτό το εργαλείο προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγόριθμους και όλες τις πατέντες, και επειδή οι μεγαλύτερες εταιρίες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security, είναι πιθανό το S/MIME να υιοθετηθεί περισσότερο από το PGP, από τους πωλητές e-mail προγραμμάτων.

Το S/MIME προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα ,εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων. Το σύστημα μπορεί να χρησιμοποιηθεί με δυνατή ή αδύνατη κρυπτογράφηση.

Για να στείλουμε κρυπτογραφημένα μηνύματα σε κάποιον με το S/MIME, πρέπει να έχουμε ένα αντίγραφο του δημοσίου κλειδιού του. Τα περισσότερα προγράμματα που χρησιμοποιούν το S/MIME κάνουν χρήση των X.509 v3 Public key infrastructures σαν και αυτές που δημιουργούνται από την VeriSign και από άλλες αρχές πιστοποίησης

5.3.3 SSL (Secure Socket Layer)

Το SSL είναι ένα κρυπτογραφικό πρωτόκολλο για ασφαλή κανάλια επικοινωνίας διπλής κατεύθυνσης .Το SSL χρησιμοποιείται συχνά με το TCP/IP πρωτόκολλο του Internet.Το SSL είναι το κρυπτογραφικό σύστημα που χρησιμοποιείται από τους web browsers όπως είναι ο Netscape Navigator και ο Microsoft Internet Explorer,αλλά μπορεί να χρησιμοποιηθεί σε οποιαδήποτε υπηρεσία TCP/IP.

Οι SSL συνδέσεις συχνά ξεκινούν από την πλευρά του web browser εξαιτίας της χρήσης ενός ειδικού προθέματος στην URL διεύθυνση. Για παράδειγμα το πρόθεμα:http//:χρησιμοποιείται για να υποδείξει μια SSL-κρυπτογραφημένη HTTP σύνδεση, ενώ " snews://" χρησιμοποιείται για να υποδείξει μια SSL-κρυπτογραφημένη NNT σύνδεση.

Το SSL προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

5.3.4 PCT Private Communications Technology)

Το PCT είναι ένα ασφαλές πρωτόκολλο επιπέδου μεταφοράς, παρόμοιο με το SSL, το οποίο αναπτύχθηκε από την Microsoft.Το PCT αναπτύχθηκε σαν απάντηση στα προβλήματα που παρουσίαζε το SSL 2.0 αλλά και στο SSL 3.0.

Αν και η Microsoft υποστηρίζει το SSL 3.0 και το TLS το καινούργιο Transport Layer Security μοντέλο, η Microsoft σκοπεύει να συνεχίσει να υποστηρίζει το PCT γιατί χρησιμοποιείται από μεγάλους πελάτες της Microsoft στα εταιρικά τους δίκτυα.

5.3.5 S-HTTP

Το S-HTTP είναι ένα σύστημα για υπογραφή και κρυπτογράφηση πληροφοριών που στέλνονται μέσω του HTTP πρωτοκόλλου. Το S-HTTP σχεδιάστηκε πριν να κυκλοφορήσει δημόσια το SSL .Περιλαμβάνει μερικά κομψά χαρακτηριστικά όπως η ικανότητα να έχει προϋπογράψει κείμενα που βρίσκονται σε έναν web server.

Αλλά το S-HTTP είναι ένα νεκρό πρωτόκολλο επειδή η Netscape και η Microsoft έχουν αποτύχει να το εφαρμόσουν στους browsers.

5.3.6 SET

Το SET είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο για την αποστολή κρυπτογραφημένων αριθμών πιστωτικών καρτών μέσω του Internet.Το πρωτόκολλο αυτό βρίσκεται υπό ανάπτυξη.

Υπάρχουν τρία μέρη που αποτελούν το SET : ένα "ηλεκτρονικό πορτοφόλι" που υπάρχει στον υπολογιστή του χρήστη, ένας server που τρέχει στα εμπορικά web sites, και ο SET server πληρωμής που τρέχει στις διάφορες τράπεζες των εμπόρων.

Για να χρησιμοποιήσουμε το SET σύστημα, πρέπει να εισάγουμε πρώτα τον αριθμό της πιστωτικής μας κάρτας μέσα στο πρόγραμμα του "ηλεκτρονικού πορτοφολιού" .Οι περισσότερες εφαρμογές αποθηκεύουν τον αριθμό της πιστωτικής σε ένα κρυπτογραφημένο αρχείο στον σκληρό δίσκο ή σε μια κάρτα (smart card).Το πρόγραμμα επίσης δημιουργεί ένα δημόσιο και ένα μυστικό κλειδί για την κρυπτογράφηση διάφορων οικονομικών πληροφοριών μας που θα σταλούν μέσω του Internet.

Όταν εμείς θελήσουμε να αγοράσουμε κάτι, ο αριθμός της πιστωτικής μας κάρτας κρυπτογραφείται και στέλνεται στον έμπορο. Το πρόγραμμα του εμπόρου υπογράφει ψηφιακά το μήνυμα πληρωμής και το προωθεί στην τράπεζα όπου επεξεργάζεται. Έτσι ο SET server πληρωμής αποκρυπτογραφεί όλες τις πληροφορίες και χρεώνει την κάρτα. Τελικά, μια απόδειξη είσπραξης στέλνεται πίσω σε μας, αλλά και στον έμπορο.

Οι τράπεζες που επεξεργάζονται τις πιστωτικές κάρτες είναι ενθουσιασμένες για το SET επειδή αυτές κρατούν τους αριθμούς των πιστωτικών καρτών μακριά από τους

εμπόρους. Αυτό θα περιόριζε σημαντικά τις απάτες που γίνονται, γιατί είναι έμποροι ,και όχι hackers, που αυτοί είναι υπεύθυνοι για τις απάτες των πιστωτικών καρτών σήμερα.

Το SET προσφέρει εμπιστευτικότητα για τους αριθμούς των πιστωτικών καρτών, καθώς κρυπτογραφούνται χρησιμοποιώντας το RSA αλγόριθμο. Αλλά δεν προσφέρει εμπιστευτικότητα (και κατά συνέπεια μυστικότητα)για τα υπόλοιπα στοιχεία της συναλλαγής του χρήστη. Αυτή ήταν μια αναγκαία συμβιβαστική λύση για να κερδηθεί η έγκριση για εξαγωγή του SET προγράμματος χωρίς περιορισμούς. Το SET παρέχει ακεραιότητα, αναγνώριση ταυτότητας και απαγόρευση απάρνησης χρησιμοποιώντας συναρτήσεις αποσύνθεσης μηνύματος και ψηφιακές υπογραφές.

5.3.7 CyberCash

Το CyberCash είναι ένα πρωτόκολλο ηλεκτρονικής πληρωμής παρόμοιο στον σκοπό με τον SET.Στην πραγματικότητα μέρη του SET είναι μοντέλα ανάπτυξης στο CyberCash.

5.3.8 DNSSEC (Domain Name System Security)

Το Domain Name System Security standard είναι ένα σύστημα που σχεδιάστηκε για να φέρει ασφάλεια στο Domain Name System Security(DNS). Το DNSSEC δημιουργεί ένα δημόσιο παράλληλο κλειδί υποδομής χτισμένο πάνω στο DNS σύστημα. Κάθε DNS domain καθορίζεται από ένα δημόσιο κλειδί. Ένα τέτοιο δημόσιο κλειδί μπορούμε να το αποκτήσουμε με ένα έμπιστο τρόπο από το εν λόγω domain ή αυτό μπορεί να φορτωθεί από πριν μέσα σε έναν DNS server χρησιμοποιώντας το αρχείο "boot" του server.

Το DNSSEC αναγνωρίζεται για τις ασφαλής ανανεώσεις πληροφοριών στους DNS servers, κάνοντας το ιδανικό για απομακρυσμένη διαχείριση. Εφαρμογές που δουλεύουν είναι διαθέσιμες για download από την Trust Information System(http//:www.tis.com) και από την CyberCash(http//:www.cybercash.com) .

5.3.9 IPsec και IPv6

Το IPsec είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο από το Internet Engineering Task Force για την παροχή πέρα για πέρα εμπιστευτικότητας για τα πακέτα που ταξιδεύουν στο Internet.Το IPsec δουλεύει με το IPv4 ,την έκδοση του IPstandart που χρησιμοποιείται σήμερα στο Internet.Το IPv6,είναι η επόμενη γενιά IP,περιλαμβάνει το IPSec.

Το IPSec δεν προσφέρεται για την ακεραιότητα, την αναγνώριση, ή την απαγόρευση απάρνησης, αλλά αφήνει αυτά τα χαρακτηριστικά για τα άλλα πρωτόκολλα. Πρόσφατα, η

κύρια χρήση του IPsec φαίνεται να είναι ένα πρωτόκολλο για την δημιουργία εικονικών προσωπικών δικτύων(VPN) μέσω του Internet.Αλλά το IPsec έχει την ικανότητα να παρέχει αναγνώριση ταυτότητας, ακεραιότητα, και προεραιτικά την εμπιστοσύνη των δεδομένων για όλες τις επικοινωνίες που παίρνουν μέρος πάνω στο Internet,έχοντας ευρέως διαδεδομένες εφαρμογές του πρωτοκόλλου και επίσης την άδεια για χρήση από τις κυβερνήσεις.

5.3.10 Kerberos

Ο Kerberos είναι ένα σύστημα ασφάλειας δικτύου που αναπτύχθηκε από το MIT και χρησιμοποιήθηκε από την αρχή στις Ηνωμένες Πολιτείες. Αντίθετα με τα άλλα συστήματα που αναφέρθηκαν στο κεφάλαιο αυτό, ο Kerberos δεν χρησιμοποιεί τεχνολογία δημοσίου κλειδιού. Αντί αυτού, ο Kerberos είναι βασισμένος σε συμμετρικά κρυπτογραφήματα που μοιράζονται μεταξύ του Kerberos server και κάθε ξεχωριστού χρήστη. Κάθε χρήστης έχει το δικό του password ,και ο Kerberos server χρησιμοποιεί αυτό το password για να κρυπτογραφήσει μηνύματα που στέλνονται σε αυτόν τον χρήστη έτσι ώστε να μην μπορούν να διαβαστούν από κανέναν άλλον.

Υποστήριξη με τον Kerberos πρέπει να προστίθεται σε κάθε πρόγραμμα που χρειάζεται προστασία. Συνήθως 'Kerberized"εκδόσεις προγραμμάτων όπως το Telnet, FTP, POP, Sun RPC χρησιμοποιούνται σήμερα. Ένα σύστημα που χρησιμοποιούσε τον Kerbero για να αποδώσει εμπιστευτικότητα στο HTTP πρωτόκολλο αναπτύχθηκε αλλά ποτέ δεν βγήκε από το εργαστήριο.

Ο Kerberos είναι ένα δύσκολο σύστημα για να διαμορφωθεί και να διαχειριστεί. Για να λειτουργήσει η κάθε πλευρά θα πρέπει να έχει ένα Kerberos server που θα είναι φυσικά ασφαλές. Ο Kerberos server διατηρεί ένα αντίγραφο των password κάθε χρήστη .Σε περίπτωση που ο Kerberos server εκτίθεται, κάθε password χρήστη πρέπει να αλλάζει.

5.3.11 SSH (Secure Shell)

Το SSH είναι το ασφαλές κέλυφος (Secure Shell).Παρέχει κρυπτογραφικά εικονικά τερματικά(Telnet) και λειτουργίες μεταφοράς αρχείων(rcp) .Μη εμπορικές εκδόσεις του SSH είναι διαθέσιμες από πολλές εκδόσεις UNIX συστημάτων. Το SSH είναι διαθέσιμο για UNIX ,Windows, Macintosh συστήματα από την Data Fellows(http://www.datafellows.com) [15],[16].

ΚΕΦΑΛΑΙΟ 6^{ο}

6.1 Ψηφιακά πιστοποιητικά

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να πιστοποιήσουν ότι το άτομο που στέλνει πληροφορίες ή τον αριθμό της πιστωτικής του κάρτας ή ένα μήνυμα είναι πραγματικά αυτό που δηλώνει ότι είναι. Τα πιστοποιητικά αποθηκεύονται στον σκληρό δίσκο του χρήστη και χρησιμοποιούν τεχνολογία απόκρυψης για να δημιουργήσουν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη. Όταν κάποιος που διαθέτει ένα ψηφιακό πιστοποιητικό επισκεφθεί κάποιο site ή στείλει ένα e-mail το πιστοποιητικό αυτό βεβαιώνει την ταυτότητα του χρήστη.

Τα ψηφιακά πιστοποιητικά είναι αρκετά ασφαλή επειδή χρησιμοποιούν ισχυρή τεχνολογία απόκρυψης. Στην πραγματικότητα είναι πιο ασφαλή ακόμα και από τις υπογραφές. Τα ψηφιακά πιστοποιητικά εκδίδονται έναντι χρεώσεως από ιδιωτικές εταιρίες και ονομάζονται Digital Authorities.Μια τέτοια είναι η VeriSign.Τα ψηφιακά πιστοποιητικά περιλαμβάνουν πληροφορίες όπως : το όνομα του χρήστη, το όνομα της εταιρίας που το εκδίδει, σειριακό αριθμό. Οι πληροφορίες έχουν κωδικοποιηθεί με έναν μοναδικό τρόπο. Στην περίπτωση των ψηφιακών πιστοποιητικών υπάρχει ένα γνωστό πρότυπο το X.509.

6.2 Χρησιμότητα των ψηφιακών πιστοποιητικών

Η κρυπτογράφηση δημοσίου κλειδιού από μόνη της δεν μπορεί να εγγυηθεί την αυθεντικότητα των επικοινωνούντων μελών .Το μόνο που πραγματικά διασφαλίζει είναι ότι το δημόσιο και το ιδιωτικό κλειδί του αποστολέα είναι συμπληρωματικό ζευγάρι κλειδιών. Δεν υπάρχει καμία εγγύηση για το ποιος είναι αυτός που κρατά το ιδιωτικό κλειδί. Λύση στο πρόβλημα της αυθεντικότητας δίνει η Αρχή Πιστοποίησης (Certificate Authority CA).Η CA είναι μια έμπιστη οντότητα η οποία εκδίδει πιστοποιητικά υπογεγραμμένα με το ιδιωτικό κλειδί της, τα οποία περιέχουν το όνομα και το δημόσιο κλειδί κάποιας οντότητας. Όταν ένας χρήστης θέλει να στείλει το δημόσιο κλειδί του σε κάποιον άλλον χρήστη στέλνει το πιστοποιητικό αυτό. Ο παραλήπτης του πιστοποιητικού, γνωρίζοντας το δημόσιο κλειδί της CA επιβεβαιώνει ότι το πιστοποιητικό είναι πράγματι υπογεγραμμένο από την CA, από το δημόσιο κλειδί πρέπει να είναι όντως του συγκεκριμένου αποστολέα. Έτσι δεν είναι απαραίτητο ένας χρήστης να γνωρίζει όλα τα δημόσια κλειδιά των άλλων χρηστών. Αρκεί να γνωρίζει αυτή τα δημόσια κλειδιά κάποιων αρχών πιστοποίησης(CA) ώστε να είναι σε θέση να επιβεβαιώνει την γνησιότητα των πιστοποιητικών που είναι υπογεγραμμένα από αυτές.

Η διαδικασία αυτής της αντιστοίχησης –δέσμευσης ενός δημοσίου κλειδιού σε μια οντότητα, καλείται πιστοποίηση.(Certification) Κατ'επέκταση, καλούνται πιστοποιητικά δημοσίου κλειδιού, ή απλά πιστοποιητικά τα ηλεκτρονικά έγγραφα που χρησιμοποιούνται για την αναγνώριση μιας οντότητας και την συσχέτιση της με ένα δημόσιο κλειδί.

Τα πιστοποιητικά αυτά είναι τυποποιημένες ηλεκτρονικές βεβαιώσεις που εκδίδονται και υπογράφονται ηλεκτρονικά από την Αρχή Πιστοποίησης με σκοπό να πιστοποιήσουν την κατοχή του συγκεκριμένου ζεύγους(ασύμμετρων) κρυπτογραφικών κλειδιών από ένα υποκείμενο και περιγράφουν στοιχεία ταυτοποίησης του υποκειμένου αυτού. Επαληθεύουν τον ισχυρισμό ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει στην συγκεκριμένη οντότητα.

Ένα ψηφιακό πιστοποιητικό είναι μια δομή δεδομένων η οποία περιέχει:

- ✓ Το όνομα και πληροφορίες αναγνώρισης του υποκειμένου του πιστοποιητικού.
- ✓ Το δημόσιο κλειδί του υποκειμένου, δηλαδή του κατόχου του πιστοποιητικού.
- ✓ Ένα μοναδικό αριθμό (serial number).
- ✓ Το όνομα της CA του πιστοποιητικού.
- ✓ Την ψηφιακή υπογραφή της CA και τον αλγόριθμο που χρησιμοποίησε.
- ✓ Την ημερομηνία έκδοσης και λήξης της ισχύος του πιστοποιητικού.

Υπάρχουν 4 είδη πιστοποιητικών:

<u>Πιστοποιητικά Αρχών Πιστοποίησης</u>

Αυτά τα πιστοποιητικά περιλαμβάνουν το δημόσιο κλειδί της αρχής πιστοποίησης και είτε το όνομα της συγκεκριμένης υπηρεσίας που πιστοποιεί. Αυτά μπορούν να υπογραφούν από μόνα τους ή αλλιώς να υπογραφούν από CA.Αυτά συνηθίζεται να πιστοποιούν άλλα είδη πιστοποιητικών.

<u>Πιστοποιητικά server</u>

Αυτά τα πιστοποιητικά περιλαμβάνουν το δημόσιο κλειδί ενός SSL Server,το όνομα του οργανισμού που 'τρέχει' τον Server, το όνομα της Internet διεύθυνσης του, και το δημόσιο κλειδί του server.

πλεκτρονική διεύθυνση του ατομου ,η οτιοπποτε αλλο.

Πιστοποιητικα εκδοτων λογισμικου

Αυτα τα πιστοποιητικα χρησιμοποιουνται για να υπογραψουν προγραμματα που προκειται να διανεμηθούν.

6.3 Υποδομή των ψηφιακών πιστοποιητικών

Για να λειτουργησει αποτελεσματικα η διαδικασια εκδοσης, υπογραφης, και δημοσίευσης των ψηφιακών πιστοποιητικών είναι απαραίτητη μια υποδομή.

Χωρις την υποδομη αυτή είναι αμφίβολο αν οι κάτοχοι ψηφιακών πιστοποιητικών που χρησιμοποιούν άλλους αλγόριθμους και πρότυπα θα μπορούσαν να επικοινωνήσουν μεταξύ τους. Η υποδομή αυτή ονομάζεται Υποδομή Δημοσίου Κλειδιού. Η Υ.Δ.Κ ενσωματώνει ψηφιακά πιστοποιητικά ,κρυπτογραφία δημοσίου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση της Υποδομής Δημοσίου Κλειδιού περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, σε εξυπηρετητές, σε λογισμικό χρηστών, καθώς επίσης και εργαλείων για την διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών αυτών. Υπάρχουν κάποιες βασικές λειτουργίες-υπηρεσίες που είναι βασικές σε όλες τις Υ.Δ.Κ :

Εμπιστευτικότητα

Μη άρνηση Αποδοχής (non repudiation)

Πιστοποίηση

6.4 Διαδικασια Δημιουργίας Ψηφιακών Πιστοποιητικών

Η πρώτη διαδικασία που πραγματοποιείται σε μια τυπική εφαρμογή είναι η δημιουργία του ζεύγους κλειδιών της CA και η δημοσίευση του πιστοποιητικού της. Κατά δεύτερο λόγο, λαμβάνει χώρα η διαδικασία ενός ζεύγους δημοσίου και ιδιωτικού κλειδιού του χρήστη. Το δημόσιο κλειδί θα κατατεθεί στην Αρχή Εγγραφής μαζί με τα στοιχεία του χρήστη. Υπάρχουν δυο εναλλακτικές που μπορεί να δημιουργηθεί το ζεύγος κλειδιών:

1. Στο περιβάλλον του χρήστη. Στην περίπτωση αυτή το ρίσκο να αποκαλυφθεί το ιδιωτικό κλειδί είναι ελάχιστο, αφού ο μόνος γνώστης του κλειδιού είναι ο χρήστης

2. της Αρχής Εγγραφής ή Πιστοποίησης : Η δημιουργία του ζεύγους κλειδιών σε τοποθεσία διαφορετική από τον νόμιμο κάτοχο του ιδιωτικό κλειδιού έχει επίπτωση στην αυξημένη πολυπλοκότητα του μοντέλου επικοινωνίας. Αρχικά θα πρέπει να υπάρχει ένα ασφαλές κανάλι από το οποίο θα μεταφερθεί το ιδιωτικό κλειδί του χρήστη. Ο βαθμός εμπιστοσύνης και οι απαιτήσεις της ασφάλειας της Αρχής Εγγραφής, θα είναι πολύ μεγαλύτερες, γιατί σε περίπτωση επιτυχούς επίθεσης εκτίθενται τα ιδιωτικά κλειδιά των χρηστών. Το πλεονέκτημα στην περίπτωση αυτή είναι η ασφαλής αποθήκευση του ιδιωτικού κλειδιού για να υπάρχει δυνατότητα ανάκτησης του σε περίπτωση που ο χρήστης χάσει αυτό. Επιπλέον πολλοί χρήστες δεν έχουν την μαθηματική ικανότητα να δημιουργήσουν μόνοι τους ένα τέτοιο ζεύγος κρυπτογραφικών κλειδιών και η Αρχη Εγγραφής το δημιουργήσει για αυτούς.

Όποια εναλλακτική και αν ακολουθήσει, το ιδιωτικό κλειδί καταλήγει στο ασφαλές προσωπικό περιβάλλον του χρήστη το οποίο μπορεί να είναι ο σκληρός δίσκος, αποσπώμενος δίσκος ή η έξυπνη κάρτα. Από τα τρία ασφαλέστερα είναι η έξυπνη κάρτα η οποία θεωρείται ανθεκτική σε εξωτερικές επιθέσεις και έχει την δυνατότητα να δημιουργεί τις ψηφιακές υπογραφές χωρίς να απαιτείται το ιδιωτικό κλειδί να μεταφερθεί σε λιγότερο ασφαλές περιβάλλον, όπως ο προσωπικός υπολογιστής του χρήστη.

6.5 Διαδικασία ανάκλησης ψηφιακών Πιστοποιητικών

Εκτός από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού μπορεί οποτεδήποτε να ανακληθεί οριστικά (revocation) ύστερα από αίτημα του ίδιου του τελικού χρήστη ή και από σχετική απόφαση του εκδότη τους. Η ανάκληση ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του σειριακού αριθμού του πιστοποιητικού σε μια λίστα ανακληθέντων Πιστοποιητικών η οποία δημοσιεύεται τακτά χρονικά διαστήματα από την υπηρεσία Ανάκλησης Πιστοποιητικών, αφού πρώτα υπογραφεί από τον ίδιο τον εκδότη(CA)των πιστοποιητικών. Κάθε CA υπογράφει τις λίστες που παρέχουν πληροφορίες για τα ανακληθέντα πιστοποιητικά που είχαν εκδοθεί από την ίδια.

Η ανάκληση ενός πιστοποιητικού γίνεται σε δυο περιπτώσεις:

1) Στην περίπτωση που ο χρήστης υποψιαστεί ότι το ιδιωτικό κλειδί έχει εκτεθεί και έχει γίνει γνωστό σε τρίτους.

2) Στην περίπτωση που γίνει κακή χρήση του πιστοποιητικού από τον χρήστη, Κακή χρήση ορίζεται η οποιαδήποτε χρήση του πιστοποιητικού πέραν της προβλεπόμενης.

Η CA καθορίζει την χρήση των πιστοποιητικών. Όταν η CA κρίνει ότι απαιτείται ανάκληση του πιστοποιητικού ενός χρήστη, η Υπηρεσία Ανάκλησης ανανεώνει τη λίστα ανακληθέντων πιστοποιητικών και την δημοσιεύει. Κατά την επαλήθευση μιας υπογραφής πρέπει κάθε χρήστης να συμβουλεύεται μια CRL για να διαπιστώσει εάν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Το αν αξίζει τον κόπο να πραγματοποιήσει τέτοιον έλεγχο, εξαρτάται από την σημασία του εγγράφου.[16]

6.6 Το πιστοποιητικό X.509

Το X.509 είναι το πιο διαδεδομένο διεθνώς πρότυπο το οποίο σχεδιάστηκε για την σύνταξη ενός ψηφιακού πιστοποιητικού και να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου X.500 (LDAP).Το πρωτόκολλο X.500 αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων(καταλόγων), η οποία σχεδιάστηκε από τον Διεθνή Οργανισμό Τυποποίησης(ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lighweight Directory Access Protocol).Η πρώτη έκδοση του X.509 δημοσιεύτηκε το 1988,καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημοσίου Κλειδιού.Το γεγονός αυτό, σε συνδιασμό με την υποστήριξη του πρωτύπου από τον ISO και ότι αποτελεί Σύσταση της Διεθνούς Ένωσης Τηλεπικοινωνιών(ITU) , έχουν οδηγήσει στην υοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών.Αρκετά χρηματοπιστοτικά ιδρύματα χρησιμοποιούν το X.509 για το πρώτυπο ασφαλών συναλλαγών SET(Secure Electronic Transactions).Χρησιμοποιείται επίσης σε φυλλομετρητές ιστοσελίδων(browsers),εξυπηρετητές(servers) και προγράμματα λογισμικού για διαχείρηση ηλεκτρονικού ταχυδρομείου κτλ.,από πολλές γνωστές εταιρείες ανάπτυξης λογισμικού.Το πρότυπο αυτό χρησιμοποιείται de facto στις περισσότερες εφαρμογές που κάνουν χρήση ψηφιακών πιστοποιητικών.Η Netscape υοθετησε το X.509 πρότυπο για την έκδοση πιστοποιητικών που χρησιμοποιούνται στο SSL πρωτόκολλο.

Διαθέτει αρκετά προκαθορισμένα πεδία για την αναγραφή των απαραίτητων πληροφοριών(εκδότης,δημόσιο κλειδί υποκειμένου, δειάρκεια ισχύος, κ.α.) καθώς και την δυνατότητα να συμπεριλάβει επιπλέον εκτεταμένα πεδία(extensions) που καθορίζονται από τον εκδότη των πιστοποιητικών.

ΚΕΦΑΛΑΙΟ 7°

7.1 Ψηφιακές υπογραφές

7.2 Η έννοια της ψηφιακής υπογραφής

Με τον όρο ηλεκτρονική υπογραφή δεν εννοούμε την αποτύπωση της ιδιόχειρης υπογραφής ούτε την μεταβίβασή της με ηλεκτρονικά μέσα, αλλά ένα ευρύτερο σύνολο μεθόδων υπογραφής για τον προσδιορισμό του συντάκτη του ηλεκτρονικού μηνύματος. Είναι μια μέθοδος τεκμηρίωσης με ηλεκτρονικά μέσα, που χρησιμοποιείται σε συγκεκριμένες μηχανικές απεικονίσεις, με σκοπό την διασφάλιση αφενός της γνησιότητας και της ακρίβειας του περιεχομένου του ηλεκτρονικού εγγράφου και αφετέρου της εξατομίκευσης του εκδότη του εγγράφου αυτού. Για την δημιουργία και τις εφαρμογές της ηλεκτρονικής υπογραφής είναι δυνατόν να χρησιμοποιούνται σύγχρονες τεχνολογίες είτε υλικού είτε λογισμικού ηλεκτρονικών υπολογιστών, που επιλέγονται συνήθως από το πρόσωπο που επιδιώκει να αποκτήσει ηλεκτρονική υπογραφή, ώστε να προσδιορίζεται αξιόπιστα η ταυτότητά του στις ηλεκτρονικές συναλλαγές. Η ιδιόχειρη υπογραφή, που δεν είναι τεχνικά δυνατή στα ηλεκτρονικά έγγραφα, διότι λείπει η υλική ενσωμάτωση, υποκαθίσταται στην ηλεκτρονική επικοινωνία από την ηλεκτρονική υπογραφή. Υπάρχουν πολλοί τρόποι ηλεκτρονικής υπογραφής από την απλούστερη μορφή κωδικών (password) και των μυστικών κωδικών αριθμών (PIN) μέχρι τις πιο σύνθετες περιπτώσεις με χρήση κρυπτογραφικών ή βιομετρικών μεθόδων. Στην έννοια της ηλεκτρονικής υπογραφής περιλαμβάνεται και η ψηφιακή υπογραφή, η οποία δεν αποτελεί τίποτα περισσότερο από μια ασφαλή μέθοδο διαπίστωσης τόσο του εκδότη ηλεκτρονικού κειμένου, όσο και της γνησιότητας και του αναλλοίωτου αυτού. Τα συστήματα παραγωγής ψηφιακής υπογραφής διαθέτουν τους κατάλληλους μηχανισμούς, ώστε να διασφαλίζεται ότι ένα έγγραφο είναι γνήσιο, ότι δημιουργήθηκε από τον υπογράφοντα και ότι ο χρόνος σύνταξή του είναι ο αναφερόμενος. Τα κρυπτογραφικά συστήματα αποτελούνται από κρυπτογραφικούς αλγόριθμους δηλαδή ένα σύνολο μαθηματικών συναρτήσεων, που χρησιμοποιούνται για κρυπτογράφηση-αποκρυπτογράφηση των δεδομένων.

Τα κυριότερα συστήματα κρυπτογράφησης είναι δυο: Το συμμετρικό και το ασύμμετρο. Το σύστημα που χρησιμοποιεί συμμετρικούς αλγόριθμους, διαθέτει το ίδιο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση, το οποίο είναι γνωστό και στον αποστολέα και παραλήπτη. Γιατί το εν λόγω σύστημα είναι πρόσφορο για κλειστή ομάδα συναλλασσομένων και όχι για συναλλακτική επαφή με μεγάλο αριθμό συναλλασσομένων.

Το δεύτερο κρυπτογραφικό σύστημα, αυτό της ασύμμετρης κρυπτογράφησης, χρησιμοποιεί ασύμμετρους αλγόριθμους. Για την θέση της ψηφιακής υπογραφής εφαρμόζεται ένας συνδυασμός δημοσίου και μυστικού κλειδιού. Με την βοήθεια ενός ειδικού προγράμματος παράγεται μια συμτηξη του μεταβιβαζόμενου κειμένου, ένα είδος περίληψης του. Το συντετμημένο αυτό κείμενο σφραγίζεται με το μυστικό κλειδί. Το μυστικό ιδιωτικό κλειδί είναι γνωστό μόνο στον αποστολέα του μηνύματος, ο οποίος το χρησιμοποιεί για την κρυπτογράφηση του μηνύματος. Το κλειδί αυτό αποθηκεύεται στον σκληρό δίσκο του υπολογιστή ή σε ειδική κάρτα ηλεκτρονικού υπολογιστή με έναν αριθμό PIN .Ο συνδυασμός του μηνύματος με το μυστικό κλειδί αποτελεί την ψηφιακή υπογραφή του αποστολέα. Κατόπιν παραδίδεται το κρυπτογραφημένο κείμενο στον παραλήπτη, ο οποίος το αποκρυπτογραφεί με την χρήση του δημοσίου κλειδιού του συντάκτη, το οποίο είτε αποστέλλεται στον παραλήπτη μαζί με το κρυπτογραφημένο κείμενο είτε ξεχωριστά είτε δημοσιεύεται σε έναν on line κατάλογο. Έτσι ένα πρόγραμμα ελέγχου του παραλήπτη ξεκλειδώνει με το δημόσιο κλειδί το συντετμημένο κείμενο και παράγει συγχρόνως μια δεύτερη σύντμηση του παραληφθέντος ηλεκτρονικού κειμένου. Αν τα δύο αυτά συντετμημένα κείμενα είναι όμοια, πιστοποιείται η προέλευση του κειμένου από τον υπογράφοντα. Η ασύμμετρη κρυπτογραφική μέθοδος είναι προσφορότερη για τα ανοιχτά δίκτυα, όπως το Internet ωστόσο δεν είναι κατάλληλη για μεταβίβαση εκτενών μηνυμάτων, επειδή είναι χρονοβόρα. Για τον λόγο αυτό για την αποστολή εκτενών μηνυμάτων ακολουθείται μια διαφορετική διαδικασία, κατά την οποία δημιουργείται πρώτα το «δακτυλικό αποτύπωμα» του κειμένου, εξάγεται δηλαδή το άθροισμα των bits ,εκ των οποίων συγκροτείται το περιεχόμενο του κειμένου. Αυτό το «δακτυλικό αποτύπωμα» υπογράφεται στην συνέχεια, κρυπτογραφείται δηλαδή με την διαδικασία RSA .Ο αποστολέας κρυπτογραφεί την περίληψη του κειμένου αυτού μαζί με τα άλλα πρόσθετα δεδομένα, όπως ο τόπος και ο χρόνος της υπογραφής, με την χρήση του μυστικού κλειδιού. Ο παραλήπτης με την χρήση του δημοσίου κλειδιού αποκρυπτογραφεί το «δακτυλικό αποτύπωμα»,ώστε να διαπιστώσει αν το περιεχόμενο του παρέμεινε αναλλοίωτο.

7.3 Η ψηφιακή ως υποκατάστατο της ιδιόχειρης υπογραφής στις ηλεκτρονικές συναλλαγές

Για να θεωρηθεί η ψηφιακή υπογραφή ως υποκατάστατο της ιδιόχειρης, πρέπει να εξετασθεί αν αυτή πληρεί τις βασικές λειτουργίες της ιδιόχειρης υπογραφής, δηλαδή την αποδεικτική λειτουργία προσδιορισμού της ταυτότητας του εκδότη και την λειτουργία επιβεβαίωσης της ταυτότητας του εγγράφου.

Η ψηφιακή υπογραφή δύναται να αναπληρώσει την ιδιόχειρη υπογραφή στις ηλεκτρονικές συναλλαγές, καθώς πληρεί τις βασικές λειτουργίες που πληρεί και η τελευταία,:

Α) την αποδεικτική λειτουργία, στο μέτρο που συμπεραίνεται ότι το έγγραφο προέρχεται από τον υπογράφοντα με την βοήθεια του πιστοποιητικού που παρέχεται από τους παρόχους υπηρεσιών πιστοποίησης. Λειτουργίες πιστοποίησης επιτελούν οι πάροχοι υπηρεσιών πιστοποίησης, οι οποίες υπηρεσίες συνίστανται στην επιβεβαίωση της αυθεντικότητας του ιδιοκτήτη και των χαρακτηριστικών ενός δημοσίου κλειδιού με την έκδοση ενός πιστοποιητικού, μιας ηλεκτρονικής βεβαίωσης σχετικά με την ταυτότητα ενός ατόμου. Το παρεχόμενο πιστοποιητικό πρέπει να περιλαμβάνει ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό, τα στοιχεία αναγνώρισης του Παρόχου Υπηρεσιών Πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος, το όνομα του υπογράφοντος ή το ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο, πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί, εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος, ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού, τον κωδικό ταυτοποίησης του, την προηγμένη ηλεκτρονική υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που το εκδίδει, τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού και τυχόν όρια στο ύψος των συναλλαγών, για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

Β) την λειτουργία προσδιορισμού της ταυτότητας του εκδότη, καθόσον τα κλειδιά της ψηφιακής υπογραφής παρέχονται από τους Παρόχους Υπηρεσιών Πιστοποίησης σε συγκεκριμένα πρόσωπα, με τα οποία, συνδέονται συμβατικά.

Γ) την λειτουργία επιβεβαίωσης της ταυτότητας του εγγράφου, καθώς με την διαδικασία επαλήθευσης της ψηφιακής υπογραφής είναι δυνατή η διαπίστωση της αλλοίωσης ή όχι του περιεχομένου του ηλεκτρονικού εγγράφου

Δ) την εγγυητική λειτουργία, επειδή ο αποστολέας ενός ηλεκτρονικού εγγράφου με την ψηφιακή του υπογραφή αναλαμβάνει την εύθηνη για την γνησιότητα και την ακρίβεια του περιεχομένου του εγγράφου. [18].[19] [20]

ΚΕΦΑΛΑΙΟ 8ο

8.1 ΠΙΣΤΟΠΟΙΗΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

8.2 Υποδομή Δημοσίου κλειδιού

Ένα σημαντικό πρόβλημα που παρουσιάζεται στο ηλεκτρονικό εμπόριο και γενικά στις ηλεκτρονικές συναλλαγές πληρωμής είναι η πιστοποίηση της ταυτότητας των οντοτήτων που λαμβάνουν μέρος στην συναλλαγή.

Σε μια συναλλαγή, τόσο ο πελάτης όσο και ο έμπορος πρέπει να είναι σε θέση να επιβεβαιώνουν ταυτότητα του άλλου μέρους με το οποίο συναλλάσσεται. Δηλαδή πρέπει να είναι σε θέση να επιβεβαιώνουν ότι το άλλο μέλος είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Στις ηλεκτρονικές συναλλαγές, όμως, η πιστοποίηση δεν είναι τόσο απλή. Στις ηλεκτρονικές συναλλαγές μέσω διαδικτύου, η πιστοποίηση βασίζεται σε μια εφαρμογή της κρυπτογραφίας, την «βεβαίωση».Η βεβαίωση αποτελεί ένα σχήμα σύμφωνα με το οποίο έμπιστοι αντιπρόσωποι, όπως είναι οι αρχές πιστοποίησης, βεβαιώνουν την αυθεντικότητα αγνώστων αντιπροσώπων, ώστε αυτοί να θεωρούνται πλέον ως πιστοποιημένοι χρήστες. Η παραπάνω διαδικασία στηρίζεται στην έκδοση ψηφιακών πιστοποιητικών από την πλευρά των έμπιστων αντιπροσώπων. Η συγκεκριμένη τεχνική αναπτύχθηκε με σκοπό να καταστεί δυνατή η διαδικασία αναγνώρισης και πιστοποίησης σε μεγάλη κλίμακα.

Η κρυπτογραφία είναι στις μέρες μας κοινά αποδεκτή σαν το πλέον απαραίτητο εργαλείο ασφάλειας στο ηλεκτρονικό εμπόριο. Σημαντικές εφαρμογές της κρυπτογραφίας είναι οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά. Οι ψηφιακές υπογραφές βοηθούν την επικύρωση της προέλευσης δεδομένων και επιβεβαιώνουν αν τα δεδομένα έχουν αλλοιωθεί. Περαιτέρω δυνατότητες προσφέρονται μέσω των υποδομών δημοσίου κλειδιού οι οποίες ενσωματώνουν τα ψηφιακά πιστοποιητικά σε ένα ασφαλές αρχιτεκτονικό σχήμα και αποδεικνύονται έτσι ικανές να υποστηρίξουν με ασφάλεια τις συναλλαγές ηλεκτρονικού εμπορίου που λαμβάνουν μέρος στο διαδίκτυο.

8.3 Πρωτόκολλα Πιστοποίησης Αυθεντικότητας

Πιστοποίηση αυθεντικότητας είναι η τεχνική με την οποία κάποιος πιστοποιεί ότι αυτός με τον οποίο επικοινωνεί είναι αυτός και όχι κάποιος άλλος. Κατά την ίδρυση μιας συνόδου επικοινωνίας απαιτείται η αυθεντικοποίηση των ταυτοτήτων των επικοινωνούντων μελών, δηλαδή το κάθε μέλος αποδεικνύει την ταυτότητα του, προτού αρχίσει η ανταλλαγή πληροφοριών. Συγκεκριμένα στο ηλεκτρονικό εμπόριο είναι αναγκαίο να εξακριβωθεί η

ταυτότητα του αποστολέα ενός ηλεκτρονικού εγγράφου. Όμως η εξακρίβωση της ταυτότητας μιας απομακρυσμένης οντότητας είναι δύσκολη και απαιτεί σύνθετα πρωτόκολλα βασισμένα στην κρυπτογραφία. Όταν ένας χρήστης επιθυμεί να εγκαταστήσει μια ασφαλή σύνδεση με ένα δεύτερο χρήστη, εκτελείται ένα πρωτόκολλο πιστοποίησης αυθεντικότητας και μόλις το πρωτόκολλο ολοκληρωθεί, ο κάθε χρήστης είναι σίγουρος για την ταυτότητα του άλλου.

Στα περισσότερα πρωτόκολλα εγκαθίσταται μεταξύ δυο χρηστών ένα μυστικό κλειδί συνόδου (session key) για χρήση στην επερχόμενη συνομιλία. Στην πράξη, για λόγους απόδοσης, όλη η κίνηση δεδομένων κρυπτογραφείται χρησιμοποιώντας κρυπτογραφία μυστικού κλειδιού, ενώ η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται στα πρωτόκολλα πιστοποίησης αυθεντικότητας καθώς και για την κρυπτογράφηση των κλειδιών συνόδου.

Τα περισσότερα πρωτόκολλα πιστοποίησης αυθεντικότητας βασίζονται στην εξής αρχή: ο ένας χρήστης στέλνει στον άλλον ένα τυχαίο αριθμό, τον οποίο μετασχηματίζει με ένα ειδικό τρόπο και επιστρέφει το αποτέλεσμα. Τα πρωτόκολλα αυτά ονομάζονται πρωτόκολλα πρόκλησης –απόκλισης (challenge-response).

8.4 Εγκατάσταση Μοιραζόμενου κλειδιού

Σε περίπτωση που δυο χρήστες δεν έχουν μυστικό κλειδί και επιθυμούν να επικοινωνήσουν με ασφάλεια μέσω του δικτύου , μπορούν να καθιερώσουν ένα τέτοιο κλειδί. Ένας τρόπος για να επιτευχθεί αυτό, θα ήταν να τηλεφωνήσει ο χρήστης Α στον χρήστη Β και να του δώσει το κλειδί του Αλλά στην περίπτωση αυτή ο Β δεν είναι σίγουρος ότι πρόκειται για τον Α και όχι για τον εισβολέα. Θα μπορούσαν βέβαια να κανονίσουν από κοινού μια συνάντηση , όπου ο καθένας θα έφερνε το διαβατήριο του για πιστοποίηση της ταυτότητας του, συνήθως όμως κάτι τέτοιο δεν είναι εφικτό.

Υπάρχει ένα πρωτόκολλο που επιτρέπει σε δυο ξένους να επικοινωνήσουν με ασφάλεια εγκαθιστώντας ένα κοινό μυστικό κλειδί. Το πρωτόκολλο αυτό ονομάζεται ανταλλαγή μυστικού κλειδιού των Diffie-Hellman και λειτουργεί ως εξής:

Οι χρήστες Α και Β έχουν συμφωνήσει σε δυο μεγάλους πρώτους αριθμούς n και g, όπου (n-1)/2 είναι επίσης πρώτος αριθμός. Οι αριθμοί αυτοί μπορεί να είναι δημόσιοι, έτσι είτε ο ένας χρήστης είτε ο άλλος μπορούν απλά να επιλέξουν τα n ,g και να τα πουν στον άλλο ανοιχτά....

Στην συνέχεια ο Α επιλέγει ένα μεγάλο αριθμό ,x , και τον κρατάει μυστικό. Όμοια ο Β επιλέγει ένα μεγάλο αριθμό ,y .

Ο χρήστης Α ξεκινάει στέλνοντας στον Β ένα μήνυμα που περιέχει τους έξεις αριθμούς(n,g,g^x, mod n),

Ο χρήστης Β απαντά στέλνοντας στον Α ένα μήνυμα που περιέχει τον αριθμό g^y mod n.

Ο Α υψώνει τον αριθμό που πήρε από τον Β στην x-οστή δύναμη και παίρνει τον όρο (g^y mod n)^x.

Ο χρήστης Β εκτελεί παρόμοια λειτουργία και παίρνει το (g^x mod n)^y.Σύμφωνα με τους κανόνες της αριθμητικής modulo και οι δυο υπολογισμοί παράγουν το g^{xy} mod n. Έτσι ο Α και ο Β μοιράζονται το μυστικό κλειδί. Υπάρχει περίπτωση ένας εισβολέας να δεί και τα δύο μηνύματα. Έτσι θα γνωρίσει τα n και τα g όμως δεν θα μπορεί να υπολογίσει τα x και y.Με δεδομένο μόνο το g^x mod n δεν μπορεί να βρει το x.Δεν υπάρχουν πρακτικοί αλγόριθμοι για τον υπολογισμό διακριτών αλγορίθμων modulo.

Ο αλγόριθμος αυτός παρουσιάζει ένα μεγάλο πρόβλημα. Όταν ο χρήστης Β λαμβάνει την τριάδα (n, g, g^x, mod n) δεν μπορεί να είναι σίγουρος ότι το μήνυμα αυτό προέρχεται από τον Α. Ένας εισβολέας μπορεί να εκμεταλλευτεί αυτό το γεγονός και να εξαπατήσει και τους δυο χρήστες Α και Β .Ο Α στέλνει κανονικά το μήνυμα 1 που προορίζεται για τον Β .Ο εισβολέας υποκλέπτει το μήνυμα αυτό και στέλνει αντί αυτού στον Β το μήνυμα 2 (n, g, g^z, mod n) όπου z είναι ο μυστικός αριθμός που επέλεξε ο εισβολέας. Επιπλέον ο εισβολέας στέλνει και ένα μήνυμα 3 πίσω στον Α .Αργότερα ο Β στέλνει το μήνυμα 4 προς τον Α, το οποίο ο εισβολέας επίσης υποκλέπτει και κρατάει.

Έτσι ο Α υπολογίζει το μυστικό κλειδί g^{xz} mod n, το ίδιο κάνει και ο εισβολέας. Ο Β υπολογίζει το g^{yz} mod.Όμοια και ο εισβολέας. Οπότε ο Α νομίζει ότι μιλάει με τον Β και ο Β νομίζει ότι μιλάει με τον Α. Κάθε μήνυμα που στέλνεται από τον Α συλλαμβάνεται από τον εισβολέα ,τροποποιείται και στέλνεται στον Β. Παρόμοια διαδικασία γίνεται για μήνυμα που στέλνεται από τον Β. Ο εισβολέας βλέπει τα πάντα και μπορεί να τροποποιήσει όλα τα μηνύματα, ενώ οι χρήστες Α και Β έχουν την εντύπωση ότι έχουν ένα ασφαλές κανάλι επικοινωνίας. Η επίθεση αυτή λέγεται bucket brigate.

8.5 Πιστοποίηση Αυθεντικότητας με χρήση Κέντρου Διανομής Κλειδιών.

Για να επικοινωνήσει κάποιος με n άτομα χρειάζεται να έχει n κλειδιά, όμως για μεγάλο επικοινωνιακό φόρτο η διαχείριση κλειδιών είναι πρόβλημα.

Ένας διαφορετικός τρόπος προσέγγισης είναι η εισαγωγή ενός έμπιστου κέντρου διανομής κλειδιών(Key Distribution Center KDC). Στο μοντέλο αυτό κάθε χρήστης έχει ένα απλό κλειδί το οποίο μοιράζεται με το κέντρο διανομής κλειδιών. Η πιστοποίηση αυθεντικότητας και η διαχείριση των κλειδιών συνόδου γίνεται με την μεσολάβηση του κέντρου διανομής κλειδιών. Αυτό είναι ένα πρωτόκολλο.

Ο χρήστης Α επιλέγει ένα κλειδί συνόδου Κ και λέει στο KDC ότι θέλει να μιλήσει στο χρήστη Β χρησιμοποιώντας το K_S. Το μήνυμα αυτό είναι κρυπτογραφημένο με ένα μυστικό κλειδί K_A που μοιράζεται ο Α μόνο με το κέντρο διανομής κλειδιών (KDC).

Το κέντρο διανομής κλειδιών (KDC) αποκρυπτογραφεί το μήνυμα αυτό και εξάγει την ταυτότητα του Β και το κλειδί συνόδου. Στην συνέχεια κατασκευάζει ένα νέο μήνυμα που περιέχει την ταυτότητα του Α και το κλειδί συνόδου, το κρυπτογραφεί με το μυστικό κλειδί K_B που μοιράζεται με τον Β και το στέλνει στον Β.

Όταν ο Β αποκρυπτογραφήσει το μήνυμα, μαθαίνει ότι ο Α επιθυμεί να μιλήσει με αυτόν και επίσης γνωρίζει και το κλειδί συνόδου που ο Α θέλει να χρησιμοποιήσει.

Με τον παραπάνω τρόπο η πιστοποίηση αυθεντικότητας πραγματοποιείται αξιόπιστα. Το κέντρο διανομής κλειδιών γνωρίζει ότι το μήνυμα 1 προέρχεται από τον χρήστη Α, εφόσον κανένας άλλος δεν είναι ικανός να το κρυπτογραφήσει με το μυστικό κλειδί του Α. Όμοια ο Β γνωρίζει ότι το μήνυμα 2 προέρχεται από το κέντρο διανομής κλειδιών, το οποίο εμπιστεύται και επιπλέον κανένας άλλος δεν γνωρίζει τι μυστικό κλειδί.

Το πρωτόκολλο αυτό παρουσιάζει ένα σημαντικό μειονέκτημα: Ένας εισβολέας μπορεί να αντιγράψει τα μηνύματα που αποστέλλονται μεταξύ των δύο χρηστών και να τα αναμεταδώσει. Το πρόβλημα αυτό ονομάζεται επίθεση επανάληψης(replay attack).Μια λύση είναι η τοποθέτηση ενός τυχαίου αριθμού nonce σε κάθε μήνυμα. Ο αριθμός αυτός είναι μοναδικός σε κάθε μήνυμα. Ο χρήστης με αυτόν τον τρόπο μπορεί να απορρίπτει κάθε μήνυμα που περιέχει ένα παλαιότερα χρησιμοποιούμενο nonce.Σε αυτή την προσέγγιση χρειάζεται μια λίστα που να αποταμιεύει όλα τα nonce για πάντα, γιατί κάποιος εισβολέας μπορεί να επιχειρήσει να επαναλάβει ένα μήνυμα που είχε σταλεί πριν από μεγάλο χρονικό διάστημα. Αυτή η λίστα θα μεγαλώνει συνεχώς δημιουργώντας πρόβλημα στην αποθήκευσή της. Μπορούν βέβαια να συνδυαστούν οι χρονοσφραγίδες με τα nonce ,έτσι ώστε να υπάρχει όριο στα αποθηκευμένα nonce ,αλλά με τον τρόπο αυτό το πρωτόκολλο γίνεται περισσότερο σύνθετο.

8.6 Πιστοποίηση Αυθεντικότητας με χρήση Κρυπτογραφίας Δημόσιου κλειδιού

Η πιστοποίηση της αμοιβαίας αυθεντικότητας μπορεί να επιτευχθεί και με την χρήση κρυπτογραφίας δημοσίου κλειδιού. Δυο χρήστες, ο Α και ο Β, γνωρίζουν ο ένας το δημόσιο κλειδί του άλλου, και θέλουν να εγκαταστήσουν μια σύνοδο. Στην συνέχεια στη σύνοδο αυτή, θέλουν να χρησιμοποιήσουν κρυπτογραφία μυστικού κλειδιού που είναι πολύ γρηγορότερη σε σχέση με την κρυπτογραφία δημοσίου κλειδιού. Για τον λόγο αυτό εκτελείται μια αρχική συναλλαγή όπου πιστοποιείται η αυθεντικότητα και των δυο πλευρών και επιπλέον καθορίζεται ένα κοινό μυστικό κλειδί συνόδου.

Ο χρήστης Α ξεκινάει κρυπτογραφώντας την ταυτότητά του και έναν τυχαίο αριθμό R_A χρησιμοποιώντας το δημόσιο κλειδί E_B του χρήστη Β.

Όταν ο Β λάβει το μήνυμα δε γνωρίζει αν προέρχεται από τον Α ή από κάποιον εισβολέα. Ο Β απαντάει στέλνοντας ένα μήνυμα που περιέχει τον R_A ,και ένα δικό του τυχαίο αριθμό R_B και ένα προτεινόμενο κλειδί συνόδου K_S .Το μήνυμα αυτό, πριν το στείλει, το κρυπτογραφεί με το δημόσιο κλειδί E_A του Α.

Όταν ο Α πάρει το μήνυμα 2,το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Μόλις δει τον R_A είναι σίγουρος ότι το μήνυμα προέρχεται από τον Β, διότι κανένας άλλος δε θα μπορούσε να αποκρυπτογραφήσει το μήνυμα 1, και να καθορίσει τον R_A . Επιπλέον το μήνυμα πρέπει να είναι καινούργιο και όχι επανάληψη, εφόσον ο Α μόλις έστειλε στον Β τον R .

Ο Α συμφωνεί για την σύνοδο και στέλνει στον Β το μήνυμα 3.

Όταν ο Β δει το R_B κρυπτογραφημένο με το K_S καταλαβαίνει ότι σίγουρα ο Α πήρε το μήνυμα 2.Ένας εισβολέας δε μπορεί να κατασκευάσει το μήνυμα 3 εφόσον δε γνωρίζει ούτε το R_B K_S και ούτε μπορεί να τα καθορίσει χωρίς το ιδιωτικό κλειδί του Α.[21]

ΚΕΦΑΛΑΙΟ 9°

9.1 Τάσεις επιθέσεων στο Internet.

9.1.2 ΕΠΙΣΗΜΑΝΣΕΙΣ-ΠΡΟΤΡΟΠΕΣ

9.1.3 Ο δρόμος για την online ασφάλεια.

Η επίτευξη της ασφάλειας σε όλες τις διαδικτυακές δραστηριότητές δεν είναι καθόλου δύσκολη υπόθεση. Το μόνο που απαιτείται είναι να τηρούν οι χρήστες με σχεδόν θρησκευτική ευλάβεια μια σειρά κανόνων, οι οποίοι θα τους απαλλάξουν και θα τους προστατεύουν από κάθε λογής κίνδυνο που μπορεί να συναντήσουν στο Παγκόσμιο Διαδίκτυο. Patches, updates και συνεχής ενημέρωση.

Ανά τακτά χρονικά διαστήματα (όχι μεγαλύτερα του ενός μήνα) πρέπει να γίνεται ένας έλεγχος στο Διαδίκτυο ή σε άλλες πηγές ενημέρωσης για την ύπαρξη ή τη διάθεση patches τόσο για το λειτουργικό σύστημα όσο και για το software που χρησιμοποιεί ο χρήστης. Για την ενημέρωση των Windows (98 και μεταγενέστερα) με τα τελευταία security fixes, καλύτερα είναι να προτιμά την λειτουργία Windows Update - που θα τον γλιτώσει από το μπελά του ψαξίματος, με μόνο αντίτιμο ίσως μια επιπλέον ολιγόλεπτη καθυστέρηση στα κατεβάσματα των updates. Το Microsoft Critical Update Notification, μια υπηρεσία που προσφέρεται για download στα Windows 2000 και είναι ενσωματωμένη στα Windows XP, ενημερώνει ανά πάσα στιγμή για το πότε ζωτικά updates είναι διαθέσιμα, αυτοματοποιώντας ως ένα βαθμό, μάλιστα, την ενημέρωση του συστήματος (one click download). Για άλλα σημαντικά patches ασφαλείας από την Microsoft η πιο έγκυρη πηγή ενημέρωσης είναι το Microsoft TechNet (www.microsoft.com/technet).

9.1.4 Σωστή και "προσεγμένη" χρήση των δικτυακών εφαρμογών.

Το πρώτο μέλημα θα πρέπει να είναι η σωστή ρύθμιση των δικτυακών εφαρμογών που χρησιμοποιεί ο κάθε χρήστης. Οι περισσότεροι Web browsers διαθέτουν μερικές δεκάδες ρυθμίσεων ασφαλείας που καθορίζουν σε αρκετά μεγάλο βαθμό ποια components, ποια Java applets ή άλλα κοινά πλέον στοιχεία των web sites μπορούν να "εκτελεστούν" από τον browser, ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies (επιτρέποντας την αποθήκευσή τους στο σύστημα ή τη χρήση τους από τρίτα web sites μόνο όταν αυτό δεν συνιστά κίνδυνο για τα προσωπικά δεδομένα). Μια καλή αρχή για την δοκιμή των ρυθμίσεων του browser είναι το online test Qualys's Free Browser Checkup (http://browsercheck.qualys.com/), το οποίο κατά πάσα πιθανότητα θα αποκαλύψει στο

χρήστη μερικές από τις αδυναμίες του browser του. Οι χρήστες των Windows μπορούν να στραφούν επιπλέον στη χρήση του Microsoft Baseline Security Analyzer. Πρόκειται για ένα δωρεάν διαθέσιμο από το TechNet εργαλείο που ελέγχει το σύστημά του για κακές ρυθμίσεις . Τέλος, αν χρησιμοποιεί instant messengers (κατηγορία προγραμμάτων που αποτελεί έως ένα βαθμό "κερκόπορτα" στην ασφάλεια των υπολογιστικών συστημάτων), πρέπει να αποφεύγει να συνομιλεί με ξένους .

Στην πλειοψηφία τους δημοφιλείς εφαρμογές, όπως ο AIM, το ICQ, το Trillian, ο Yahoo! και ο MSN Messenger, οι instant messengers συνήθως αποκαλύπτουν την IP διεύθυνση του συστήματος του κάθε χρήστη, ακόμα και σε ορισμένες περιπτώσεις που ο χρήστης έχει ζητήσει την απόκρυψή της, επιτρέποντας συνδέσεις peer to peer (απευθείας σύνδεση δύο υπολογιστικών συστημάτων). Επιπλέον, χρησιμοποιούν αρκετά ports (συμπεριλαμβανομένου και του 80 - του port που χρησιμοποιούν οι Web Browsers) αποτελώντας έτσι μια δημοφιλή "τρύπα" ασφαλείας για τους hackers. Ενδεικτικό, άλλωστε, για του λόγου το αληθές είναι ο μεγάλος αριθμός exploits που υπάρχουν για τους πιο δημοφιλείς instant messaging clients.

9.1.5 Σοφή χρήση Antivirus και Firewalls.

Ο χρήστης θα πρέπει πάντα να κάνει την καλύτερη επιλογή ενός ή και περισσότερων πακέτων antivirus και να φροντίζει να το ενημερώνει σε τακτική βάση με virus definition updates. Ακόμα και η πιο αποτελεσματική μηχανή αντιμετώπισης ιών, εάν δεν ενημερώνεται διαρκώς είναι τελείως άχρηστη. Στην πλειοψηφία τους, τα antivirus ελέγχουν όλα τα νέα αρχεία και τα νέα προγράμματα που εγκαθίστανται στον υπολογιστή για ιούς, ωστόσο όπως και να 'χει θα πρέπει ο χρήστης να προγραμματίζει ένα εβδομαδιαίο πλήρη έλεγχο του συστήματος για κάθε ενδεχόμενο.

Αναφορικά τώρα με τα firewalls, θα πρέπει να έχει κατά νου ότι οι εξ' ορισμού ρυθμίσεις των περισσοτέρων προγραμμάτων firewall θα επιτρέπουν απεριόριστη πρόσβαση στο Internet για μερικές χιλιάδες εφαρμογών. Δεν πρέπει να εμπιστευθεί με κλειστά μάτια σε αυτά την ασφάλεια του PC του. Αντιθέτως, πρέπει να ενεργοποιήσει τις μέγιστες ρυθμίσεις ασφαλείας και μέσα από μια συνεχή διαδικασία "δοκιμής και διαπίστωσης", να δώσει δικαιώματα χρήσης του Internet μόνο σε όσες εφαρμογές θέλει ο χρήστης. Αρχικά θα πρέπει να αρνηθεί την χρήση/ πρόσβαση του Internet σε όλες τις εφαρμογές (πλην του Web Browser/ e-mail client και οποιασδήποτε p2p file sharing εφαρμογής χρησιμοποιεί). Αν κάποια από αυτές δεν ανταποκρίνεται σωστά (στο σύνολο ή σε μέρος των λειτουργιών της)

λόγω της μη πρόσβασης στο Internet, τότε πρέπει να δημιουργήσει ένα κανόνα εξαίρεσης στο πρόγραμμα firewall που χρησιμοποιεί

9.1.6 Διατήρηση της ανωνυμίας.

Πρώτο βήμα στην διατήρηση της ανωνυμίας του χρήστη δεν είναι άλλο από την ενημέρωση του browser που χρησιμοποιεί. Αρχικά θα πρέπει να προτιμά την πιο πρόσφατη έκδοση και φυσικά να φροντίζει να την ενημερώνει τακτικά με όλα τα security patches. Ο Internet Explorer 6 και ο Netscape 7 περιλαμβάνουν νέα χαρακτηριστικά που επιτρέπουν στο χρήστη ως ένα βαθμό να προστατέψει το απόρρητο των προσωπικών δεδομένων του και να διατηρεί την ανωνυμία του στο Διαδίκτυο. Τα νέα χαρακτηριστικά των browser εντοπίζονται κυρίως στην έξυπνη διαχείριση των cookies και στην αποτροπή εκτέλεσης "ύποπτου" κώδικα (malware). Στον Internet Explorer, για να απενεργοποιηθούν τα third party cookies (τα cookies που "φυτεύονται" στο σύστημα όχι από τα sites που επισκέπτεστε αλλά από τριτογενείς φορείς), τότε ο χρήστης θα πρέπει να κάνει την ακόλουθη διαδικασία. Να επιλέξει Tools → Internet Options και στην συνέχεια Privacy. Στη συνέχεια, να πάει στην ενότητα επιλογών Advanced και να ενεργοποιήσει την επιλογή "Override automatic Cookie Handling". Γενικότερα είναι προτιμότερο να επιτρέπονται τα πρωτογενή cookies, να μπλοκάρονται τα third party cookies και τέλος να επιτρέπονται τα session cookies (που συνήθως αφορούν σε μια περίοδο χρήσης/ επίσκεψης σε μια online υπηρεσία - webmail κτλ).

Επόμενο βήμα στην προστασία της ανωνυμίας του δεν είναι άλλο από την χρήση ενός προγράμματος αποτροπής / παρεμπόδισης της λειτουργίας spyware λογισμικού.

9.1.7 Κρυπτογράφηση και περιορισμός των υπηρεσιών.

Ο καθορισμός των υπηρεσιών (services) που θα είναι ενεργές σε ένα σύστημα με Windows XP (ή προγενέστερα NT based λειτουργικά συστήματα) είναι ίσως ένα από τα πιο κρίσιμα στάδια στην δημιουργία μιας ζώνης ασφαλείας για τον προσωπικό υπολογιστή ή το εταιρικό δίκτυο. Υπηρεσίες όπως Remote Registry, Remote Desktop , Remote Access μπορεί να είναι αρκετά χρήσιμα εργαλεία για διαχειριστές μεγάλων εταιρικών δικτύων. Ωστόσο είναι απίθανο το αν και πότε θα φανούν χρήσιμα σε ένα home user. Για να νιώθει περισσότερη ασφάλεια ο χρήστης, αλλά και για να μη βρεθεί προ εκπλήξεων αφού κάθε μια από αυτές δίνει σχεδόν απεριόριστη πρόσβαση στον υπολογιστή του, τότε αυτό που είναι απαραίτητο να κάνει είναι να τις απενεργοποιήσει.

Επιπλέον, αν όντως τα δεδομένα που διατηρεί στο σκληρό δίσκο ή στο ηλεκτρονικό του ταχυδρομείο είναι τόσο "ευαίσθητα" και "προσωπικά" που δεν θέλει να τα δει κανείς

[illegible] όλων των δικτυακών τυπών στην ασφάλεια δεν είναι αρκετό. Για [illegible] προτείνεται η χρηση κρυπτογραφησης στα οεοομενα συγκεκριμενων φακέλων (π.χ. σε αυτούς που αποθηκεύει τα προσωπικά δεδομένα του), η οποία θα δυσκολέψει επιπρόσθετα το έργο των όποιων καλοθελητών. Για να κρυπτογραφήσει τα εμπεριεχόμενα αρχεία ενός καταλόγου στα Windows XP, μέσα από ένα παράθυρο του Windows Explorer, τότε πρέπει να επιλέξει τον κατάλογο και με δεξί κλικ Properties . Στην συνέχεια να πάει στην σελίδα General και κατόπιν να επιλέξει Advanced και ακολούθως "Encrypt".

9.1.8 Παρακολούθηση της δικτυακής δραστηριότητας.

Η παρακολούθηση και ο έλεγχος της εισερχόμενης/ εξερχόμενης δικτυακής κίνησης packets δεδομένων (outbound/ inbound traffic) μπορεί να αποκαλύψει στο χρήστη αρκετά πράγματα για την παρασκηνιακή δραστηριότητα εφαρμογών που υπό άλλες συνθήκες θα περνούσε απαρατήρητη. Πρόκειται ίσως για μια πιο μακρόχρονη διαδικασία εύρεσης και αντιμετώπισης trojan και spyware εφαρμογών που ωστόσο μπορεί να δώσει λύσεις εκεί που ένα antivirus ή anti spyware πρόγραμμα ενδεχομένως να αποτύχει. Πέρα από τη μη εγκεκριμένη εκροή packets από το σύστημα προς τον "έξω κόσμο" του Διαδικτύου, η παρακολούθηση της δικτυακής δραστηριότητας μπορεί να αποκαλύψει τον τρόπο δράσης κάποιων hackers, δίνοντας του εμμέσως πλην σαφώς κατευθυντήριες γραμμές για την περαιτέρω προάσπιση του συστήματός η του δικτύου του. Παρότι τα Windows XP διαθέτουν κάποιες απλοϊκές λειτουργίες επισκόπησης της δικτυακής δραστηριότητας, συνιστάται ανεπιφύλακτα η χρήση εξειδικευμένου εργαλείου (μερικές καλές επιλογές σε αυτήν την κατηγορία προγραμμάτων βρίσκονται στη σελίδα

http://www.billssoftwarepicks.com/software/connectivity/network_monitors/.

9.2 Ανωνυμία στο διαδίκτυο.

9.2.3 Τεχνικές και λύσεις διατήρησης της ανωνυμίας στο Διαδίκτυο:

9.2.3.1 Proxy και Proxy Chains.

Η αρχαιότερη τεχνολογία και η βάση όλων των ανώνυμων επικοινωνιών στο Διαδίκτυο είναι ο proxy. Ο proxy είναι ένας υπολογιστής στο δίκτυο, ο οποίος αναλαμβάνει να προωθήσει ένα "μήνυμα" που αποστέλλει ένας υπολογιστής Α σε ένα υπολογιστή Β, φροντίζοντας έτσι ώστε να μην αποκαλυφθεί ποτέ η πηγή του μηνύματος. Ένας τέτοιος

proxy, δηλαδή ένας proxy που κατορθώνει επιτυχώς να αποκρύψει την ταυτότητα του αποστολέα του μηνύματος καλείται "anonymizer".

Οι "anonymizer" προέκυψαν ως απομιμήσεις τις καθημερινής ζωής, π.χ. στην συχνή περίπτωση που ένας δημοσιογράφος μεταφέρει μια είδηση αρχίζοντας με την φράση "Σύμφωνα με πηγές" και άλλα τετριμμένα χωρίς ωστόσο να κατονομαστεί η πηγή του μηνύματος, τότε έχουμε να κάνουμε με ένα "anonymizer". Όταν ένα μήνυμα περνάει από μια αλυσίδα anonymizers, περνάει μέσα από ένα σύστημα υπολογιστών που καλείται proxy chains (αλυσίδα από proxies) Πιο αποτελεσματικοί proxy chains είναι αυτοί που υποστηρίζουν ισχυρή κρυπτογράφηση δεδομένων.

9.2.3.2 Mixnets και Mixnet Reply Blocks.

Τα Mixnets πρωτοεμφανίστηκαν το 1981 από τον David Chaum. Βασική έννοια στα Mixnets είναι ο MIX, ο οποίος είναι ένας proxy που αποδέχεται τα κρυπτογραφημένα μηνύματα με το Public key (μέθοδος πιστοποίησης ταυτότητας που λειτουργεί ως κλειδί για την αποκρυπτογράφηση της πληροφορίας), τα αποκωδικοποιεί, τα ταξινομεί και τα προωθεί στον τελικό τους αποδέκτη, διαγράφοντας όλες τις πληροφορίες για την πηγή τους. Επιπλέον, ο Chaum, καθόρισε τον τρόπο με το οποίο η χρήση αλυσίδων από Mix μπορεί να οδηγήσει στην τελική διαγραφή όλων των στοιχείων που αποδεικνύουν την ταυτότητα του αποστολέα. Ένα mixnet τώρα συνιστά ένα κόμβο υπολογιστών, καθένας από τους οποίους έχουν ένα ζεύγος public/secret keys.

Το μήνυμα φθάνει κρυπτογραφημένο στο πρώτο MIX, αποκρυπτογραφείται, κρυπτογραφείται και στην συνέχεια περνάει στο επόμενο MIX όπου ακολουθείται πάλι η ίδια διαδικασία μέχρι να φθάσει στον τελικό MIX και να ανακατευθυνθεί στον τελικό αποδέκτη. Όσο πιο μεγάλη είναι η αλυσίδα των MIX τόσο πιο δύσκολο είναι για κάποιον να εντοπίσει την πηγή του μηνύματος. Η πολυπλοκότητα των MIXnets καθώς επίσης και η δεδομένη καθυστέρηση που παρατηρείται στην αποστολή του μηνύματος, τα καθιστούν μη πρακτικά για χρήσεις όπως Web browsing ή και συμμετοχή σε chat rooms και σε άλλα μέρη όπου υπάρχει απαίτηση για συνεχή διάδραση. Τα MIXnets Reply Blocks, καθορίζουν πέρα από την αποστολή του μηνύματος και τη διαδρομή της απάντησης σε αυτό, αναγκάζουν, δηλαδή, τον αποδέκτη του μηνύματος να απαντήσει χρησιμοποιώντας την ίδια ή παρεμφερή ασφαλή διαδικασία.

9.2.3.3 Remailers.

Τα προγράμματα που χρησιμοποιούνται για την ανωνυμία στο e-mail είναι ευρύτατα γνωστά ως remailers. Όπως σε όλες τις κατηγορίες των εργαλείων διατήρησης της ανωνυμίας (anonymity tools), τα remailers χρησιμοποιούν και τις δύο προαναφερόμενες τεχνολογίες (Proxy/ Mixnets) και διακρίνονται σε τρεις κατηγορίες:

τύπου 0: remailers που χρησιμοποιούν έναν μόνο proxy

τύπου 1: remailers που χρησιμοποιούν ένα mixnet

τύπου 2: remailers που χρησμοποιούν mixnets με reply blocks

Τύπος Remailer:

0: anon.penet.fi

Χαρακτηριστικά: Διατηρεί πίνακες με πλασματικές και πραγματικές e-mail διευθύνσεις. Υπάρχει μόνο ένα σημείο που "κλειδώνει" την επικοινωνία.

Τύπος Remailer:

1: cypherpunks

Χαρακτηριστικά: Χρησιμοποιούν τα δοσμένα public keys για να κρυπτογραφήσουν τα εισερχόμενα μηνύματα, ενώ παρέχουν anonymous e-mail μέσα από την χρήση των reply blocks.

Τύπος Remailer:

2: mixmaster

Χαρακτηριστικά: Διακρίνονται από όλα τα χαρακτηριστικά των cypherpunks σε συνδυασμό με:

- το καθορισμένο σταθερό μέγεθος των μηνυμάτων
- την ανακατανομή τους
- τη μη σταθερή καθυστέρηση κατά την μεταφορά τους από hop σε hop

Καθένας από αυτούς τους τύπους απευθύνεται σε ξεχωριστό κοινό. Συγκεκριμένα, ο πρώτος απευθύνεται κυρίως σε αρχάριους χρήστες που επιθυμούν μία μέθοδο επικοινωνίας ασφαλέστερη εκείνης που προσφέρει ο mail server του ISP τους (ή οι παροχείς Web mail), ο δεύτερος σε κοινό με μεγαλύτερες απαιτήσεις σε θέματα ασφαλείας και ο τρίτος στους σκληροπυρηνικούς θιασώτες της ασφάλειας και της ανωνυμίας στο Internet.

9.2.3.4 Ανώνυμο Web surfing.

Μια σειρά από ολοκληρωμένες προτάσεις, που ξεφεύγουν από την δυνατότητα αποστολής ανώνυμου e-mail λύνουν τα χέρια σε όλους τους χρήστες δίνοντάς τους όλα τα απαραίτητα μέσα για ανώνυμο web surfing. Αυτές οι υπηρεσίες αναλαμβάνουν το σύνολο των λειτουργιών ενός proxy server, αποκρύπτοντας την IP διεύθυνση που χρησιμοποιείται και δεχόμενες τα cookies και μια σειρά άλλα δεδομένα για λογαριασμό τους. Οι σημαντικότερες υπηρεσίες αυτής της κατηγορίας είναι:

Anonymizer http://www.anonymizer.com/

Κατά πάσα πιθανότητα, το Anonymizer είναι το πιο γνωστό από όλες αυτές τις υπηρεσίες, αποτελώντας για πολλούς χρήστες την πρώτη γνωριμία με το "ανώνυμο Web". Η εταιρεία, ανάλογα με το κόστος συνδρομής, προσφέρει διάφορα πακέτα υπηρεσιών και δωρεάν χρήση της υπηρεσίας για Web surfing. Στο πλαίσιο της δωρεάν παρεχόμενης υπηρεσίας συμπληρώνει ο χρήστης μια απλή φόρμα στο site του Anonymizer, προκειμένου να επιτραπεί η εισαγωγή μιας Web διεύθυνσης (URL - Uniform Resource Locator) και η θέασή της μέσω του δικτύου του Anonymizer. Ωστόσο, αν κάνει κλικ μέσα στον browser παρακάμπτεται η χρήση του anonymizer (θα πρέπει να βλέπει διαδοχικά τις σελίδες μέσα από την φόρμα του anonymizer). Η συνδρομή στο βασικό πακέτο Anonymous Surfing τον απαλλάσσει από αυτό το πρόβλημα, ενώ για μερικά χρήματα παραπάνω το anonymizer προσφέρει και κρυπτογράφηση δεδομένων (με χρήση 128 bit κρυπτογράφησης SSL3). Το πλήρες πακέτο υπηρεσιών (dial up) , περιλαμβάνει IP masking, κρυπτογράφηση αλλά και αυξημένη ταχύτητα αφού αποκτά απευθείας πρόσβασης στο δίκτυο του Anomymizer. Από τα βασικότερα μειονεκτήματα του Anonymizer είναι η έλλειψη της υποστήριξης Java (γλώσσα προγραμματισμού ανεξάρτητη από πλατφόρμες, αρχιτεκτονικές και λειτουργικά συστήματα).

9.2.3.5 Freedom

http://www.freedom.net/

Το Freedom φαντάζει και είναι πιο ελκυστικό από οικονομικής απόψεως από το Anonymizer, αφού το κόστος του δεν υπερβαίνει τα €50 ετησίως. Με αυτά τα λεφτά δίνει πρόσβαση στο χρήστη, στις υπηρεσίες του μεσαίου πακέτου του Anonymizer (anonymous proxy, πρόσβαση στο Internet και κρυπτογράφηση δεδομένων), ενώ για την αξιοποίηση της υπηρεσίας απαιτείται η χρήση ειδικού προγράμματος clients. Το Freedom διαφοροποιείται σε σχέση με το Anonymizer στη χρήση πολλαπλών nyms, δηλαδή στη χρήση εναλλακτικών προσωπικοτήτων κάθε μια από τις οποίες μπορεί να προσαρμόσει σε διαφορετικές ανάγκες.

Για παράδειγμα, ένα nym που χρησιμοποιείται κυρίως για επιχειρηματικούς σκοπούς μπορεί να φανερώνει στοιχεία της επαγγελματικής του ιδιότητας, ενώ ένα άλλο που χρησιμοποιείται για. κοινωνικούς σκοπούς να αποκαλύπτει το φύλο του, χωρίς ωστόσο να είναι δυνατή σε οποιοδήποτε σημείο χρήσης της υπηρεσίας η διασταύρωση και η ταυτοποίηση αυτών των δύο nyms.

9.2.3.6 FreeNet

http://freenet.sourceforge.net/

Το 1999 στο καταστατικό λειτουργίας της υπηρεσίας διαφαινόταν κάτι το πραγματικό επαναστατικό, δεδομένου ότι τότε το θέμα "ανωνυμία στο Διαδίκτυο" ήταν επίκαιρο όσο και σήμερα. Δυστυχώς, για διάφορους λόγους, η εξέλιξη του προγράμματος δεν ήταν η αναμενόμενη, ενώ ποτέ δεν έτυχε της δημοτικότητας που του άξιζε. Πλέον από κάτι που θα έφερνε τα πάνω - κάτω στο Διαδίκτυο, το FreeNet έχει εξελιχθεί σε μια άρτια υπηρεσία anonymous web surfing/file sharing, δημοφιλή κυρίως μεταξύ των κλειστών underground κοινοτήτων διακίνησης λογισμικού και mp3 αρχείων. Το FreeNet χαίρει της υποστήριξης της κοινότητας του open source, ενώ το επίπεδο των υπηρεσιών είναι πολύ καλύτερο από αυτό των συνδρομητικών υπηρεσιών, αφού ουσιαστικά έχουμε να κάνουμε με ένα δίκτυο μέσα στο δίκτυο.

9.3 Τεχνικές Προστασίας σε περιπτώσεις δημοσίευσης προσωπικών δεδομένων.

Τηλεφωνικοί κατάλογοι του Διαδικτύου, υπηρεσίες αναζήτησης προσώπων και άλλοι κατάλογοι του Διαδικτύου καθιστούν σχεδόν αδύνατη τη διατήρηση των προσωπικών δεδομένων επικοινωνίας ενός χρήστη εκτός του Web. Είναι αρκετά εύκολο για τον οποιονδήποτε να βρει το όνομά, τον αριθμό τηλεφώνου, τη διεύθυνση οικίας ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη και να χρησιμοποιήσει τις πληροφορίες αυτές για επιχειρηματικούς ή κοινωνικούς σκοπούς, για διαφήμιση ή μάρκετινγκ ή ακόμη και με εγκληματική πρόθεση. Παρακάτω περιγράφουμε ορισμένους τρόπους που σκοπό έχουν να βοηθήσουν τον έλεγχο της ποσότητας των προσωπικών στοιχείων που δημοσιοποιεί ο οποιοσδήποτε χρήστης στον κόσμο, ενώ παράλληλα μπορεί να συνεχίσει να απολαμβάνει όλα τα οφέλη που του προσφέρει το Διαδίκτυο.

Να είστε εκλεκτικοί. Από την πρώτη κιόλας στιγμή, περιορίστε την ποσότητα των προσωπικών στοιχείων που δίνετε σε μια τοποθεσία. Αποκαλύψτε τη διεύθυνση

ηλεκτρονικού ταχυδρομείου σας μόνον σε πρόσωπα που γνωρίζετε και αποφύγετε να καταχωρείται οποιαδήποτε πληροφορία σε μεγάλους καταλόγους του Διαδικτύου.

Όταν κάνετε αγορές μέσω Διαδικτύου, θα πρέπει να γνωρίζετε τις πηγές από τις οποίες προμηθεύεστε προϊόντα. Οι προμηθευτές που πωλούν ηλεκτρονικές συσκευές με πολύ μεγάλη έκπτωση τείνουν να διαφέρουν από εκείνους που πωλούν, για παράδειγμα, είδη πλεξίματος. Όταν αγοράζετε ακριβά, δημοφιλή αντικείμενα, να τα αγοράζετε από διακεκριμένες εταιρείες που διαθέτουν σαφείς πολιτικές απορρήτου. Και μάθετε τι λένε οι άλλοι για τους πωλητές και τις διαδικτυακές τους τοποθεσίες, ανατρέχοντας σε παρατηρήσεις πωλητών και αγοραστών και ελέγχοντας διαδικτυακές τοποθεσίες σύγκρισης όπως, για παράδειγμα, το Epinions.com ή το Bizrate.com.

Διαβάστε προσεκτικά τη δήλωση για την προστασία των προσωπικών δεδομένων της εκάστοτε τοποθεσίας Web. Η δήλωση αυτή θα πρέπει να αναφέρει τον τρόπο με τον οποίο συλλέγονται τα προσωπικά σας στοιχεία από μια εταιρεία, καθώς και το σκοπό για τον οποίο συλλέγονται. Εάν κάτι δεν σας φαίνεται σωστό, επικοινωνήστε με την εταιρεία για να απαντήσουν στις ερωτήσεις σας, προτού αποκαλύψετε οποιαδήποτε προσωπικά στοιχεία. Εάν στην τοποθεσία δεν δημοσιοποιείται πολιτική προστασίας προσωπικών δεδομένων, τότε αναζητήστε άλλη τοποθεσία για να κάνετε τη δουλειά σας.

Δημοσιεύστε το βιογραφικό σας μόνο σε διακεκριμένες τοποθεσίες απασχόλησης. Βεβαιωθείτε ότι οι τοποθεσίες απασχόλησης που χρησιμοποιείτε διαθέτουν πολιτικές προστασίας προσωπικών δεδομένων οι οποίες επιτρέπουν την πρόσβαση στα προσωπικά σας στοιχεία μόνο από πιστοποιημένα γραφεία ευρέσεως εργασίας. Μην δημοσιοποιείτε το βιογραφικό σας στη δική σας τοποθεσία Web.

Βγείτε από τους καταλόγους

- Μάθετε τις τοποθεσίες στις οποίες είστε καταχωρημένοι την τρέχουσα χρονική περίοδο, κάνοντας τη δική σας έρευνα στο Διαδίκτυο. Κάντε αναζήτηση του ονόματός σας στις δημοφιλείς μηχανές αναζήτησης αλλά και σε καταλόγους του Διαδικτύου όπως, για παράδειγμα, εκείνους που αναγράφονται στο πλευρικό κείμενο, στο δεξί μέρος της οθόνης σας.
- Ζητήστε να διαγραφεί το όνομά σας από καταλόγους του Διαδικτύου. Εάν δεν είναι ξεκάθαρο το πώς μπορείτε να το κάνετε αυτό σε μια τοποθεσία Web, τότε χρησιμοποιήστε το σύνδεσμο "Contact Us" (Επικοινωνήστε μαζί μας) ή τη διεύθυνση στο κάτω μέρος της διαδικτυακής τοποθεσίας του καταλόγου.

- Προμηθευτείτε έναν απόρρητο αρ θμό τηλεφώνου ή τουλάχιστον φροντίστε ώστε να διαγραφούν οι καταχωρίσεις που αφορούν τη διεύθυνσή σας. Επίσης, δώστε εντολή στον πάροχο του τηλεφώνου σας και στον πάροχο των υπηρεσιών Διαδικτύου σας να αφαιρέσουν οποιαδήποτε προσωπικά σας στοιχεία από όλους τους καταλόγους τους.
- Δημιουργήστε μια ειδική ηλεκτρονική διεύθυνση αποκλειστικά για τις δραστηριότητες στο Διαδίκτυο όπως, για παράδειγμα, για τις αγορές και τις ομάδες ενημέρωσης. Με αυτόν τον τρόπο, μπορείτε να την κλείσετε, εάν χρειάζεται, και να ανοίξετε μια νέα χωρίς να προκαλέσετε αναστάτωση στην εταιρεία σας ή στην προσωπική σας αλληλογραφία μέσω ηλεκτρονικού ταχυδρομείου.
- Κρατήστε αρχείο, κάθε φορά που δίνετε τα προσωπικά σας στοιχεία σε μια εταιρεία, ούτως ώστε να μπορείτε να τους ζητήσετε να τα διαγράψουν αργότερα, εάν είναι απαραίτητο.

9.4 Μέτρα για την ασφάλεια του ηλεκτρονικού υπολογιστή.

Σημαντικό για την ασφάλεια του ηλεκτρονικού υπολογιστή είναι τα ειδικά προϊόντα ασφαλείας, που καλύπτουν τόσο σε επίπεδο hardware (ο «ορατός» εξοπλισμός ενός συστήματος)όσο και σε επίπεδο λογισμικού (software). Επίσης το επισφαλές ενός υπολογιστή καθορίζεται από το διάστημα που είναι συνδεδεμένος όπως επίσης και από την ταχύτητα της σύνδεσής του. Η χρήση firewalls, antivirus (αντιβιοτικών) προγραμμάτων και λογισμικού προστασίας προσωπικών δεδομένων είναι υποχρεωτική. Για να είναι ολοκληρωμένη η προστασία εκτός από την εγκατάσταση των προγραμμάτων απαιτείται διαρκής ενημέρωση. Ένα από τα πιο σημαντικά κριτήρια επιλογής Internet firewall θα πρέπει να είναι οι λεγόμενες λειτουργίες ελέγχου της εξερχόμενης κυκλοφορίας (traffic), δίνοντάς στο χρήστη επιλογές αποδοχής, απόρριψης της αποστολής των packets (Κάθε αρχείο που αποστέλλεται μέσω του δικτύου τεμαχίζεται σε packets - έτσι ώστε να είναι πιο γρήγορη και πιο ευέλικτη η μεταφορά τους που επιχειρεί να στείλει μια εφαρμογή). Ακόμα και τα πιο ακραία μέτρα ασφαλείας δεν μπορούν να εγγυηθούν την απόλυτη ασφάλεια. Έτσι, για την επίτευξη της σχετικής ασφάλειας απαιτείται η τήρηση μια σειρά κανόνων, συγκεκριμένα:

1. Επιλογή ενός καλού antivirus προγράμματος.

2. Τακτική ανίχνευση όλου του δίσκου με το antivirus.

3. Συνεχής ανανέωση (update) του.

4. Έλεγχος κάθε δισκέτας/cd με το antivirus πριν την ανοίξει ο χρήστης.

5. Τήρηση αντιγράφων ασφαλείας όλων των αρχείων του σε cd ή δισκέτα.

6. Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού του. Η πιο έγκυρη πηγή ενημέρωσης είναι το Microsoft TechNet (www.microsoft.com/technet). Μπορεί ο κάθε χρήστης να το επισκεφθεί και να κάνει κλικ στο Click on Hotfix & Bulletin Search για να δει για ποια προγράμματα χρειάζεται patches και ποια όχι.

7. Ανίχνευση μέσω του αντιβιοτικού κάθε νέου αρχείου που «κατεβάζει» από το Internet.

8. Αν χρησιμοποιεί irc chat, τότε να απενεργοποιήσει την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που του στέλνουν.

9. Να επιλέξει την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ του. Ίσως κάποιος να του στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχει την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσει το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.

10. Να διατηρεί και να ανανεώνει συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.

11. Διατήρηση της ανωνυμίας του με την ενημέρωση του browser που χρησιμοποιεί. Να προτιμάτε πάντα την πιο πρόσφατη έκδοση και φυσικά να φροντίζει να την ενημερώνει τακτικά με όλα τα security patches.

12. Σωστή ρύθμιση των δικτυακών εφαρμογών. Οι περισσότεροι Web browsers διαθέτουν ρυθμίσεις ασφαλείας που καθορίζουν ποια components, ποια Java applets ή άλλα στοιχεία των web sites μπορούν να «εκτελεστούν» από τον browser, ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies. Οι χρήστες των Windows μπορούν να στραφούν επιπλέον στη χρήση του Microsoft Baseline Security Analyzer. Πρόκειται για ένα δωρεάν διαθέσιμο από το TechNet εργαλείο που ελέγχει το σύστημά για κακές ρυθμίσεις.

13. Αν χρησιμοποιεί instant messengers, να αποφεύγει να συνομιλεί με ξένους.

14. Εδώ πρέπει να επισημανθεί πως όσο πιο αυστηρές ρυθμίσεις ασφαλείας ενεργοποιούνται στον υπολογιστή, τόσο πιο δύσκολη γίνεται και η πρόσβαση σε σελίδες του Διαδικτύου. Η συνήθης ρύθμιση ασφαλείας στους φυλλομετρητές είναι η «μεσαία».

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), (2006),« Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις Συναφείς Υπηρεσίες και Εφαρμογές».

[2] Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), (2006), «Κανονισμός για τη Διασφάλιση του Απορρήτου Διδικτυακών Υποδομών».

[3] Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), (2006), «Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου».

[4] Ασφάλεια της πληροφορίας (Σουρής-Πάτσιος-Γρηγοριάδης) Εκδόσεις Ν.Τεχνολογίες.

[5] Garfinkel Simson and Stafford Gene (Practical Unix and Internet Security O'Reilly and Associates second edition 1996.

[6] STALLINGS WILLIAM :" Operating systems internal and desing principles". Prentice Hall fourth edition 2000.

[7] Clough Bryan and Mungo Paul: "Approaching Zero" Data crime computer underworld Faber and Faber 1992.

[8] WWW..go –online.gr/ebusines/specials/articles htm/ article_id=410

[9] Tulloch Mitch "Microsoft encyclopedia of security, "Microsoft Press 2003.

[10] Mansfield Richard Haker Attack-Sybex 2000

[11] Γκρίτζαλης Σέφανος Enhancing Web Privacy and Anonimity in the Digital era

[12] Skoudis Edward with Zelter Lenny Malware: Fithing Malicious code P.Hall S.edition 2002

[13] ΑΣΦΑΛΕΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ (ΣΟΥΡΗΣ-ΠΑΤΣΙΟΣ-ΓΡΗΓΟΡΙΑΔΗΣ) ΕΚΔΟΣΕΙΣ Ν.ΤΕΧΝΟΛΟΓΙΕΣ.

[14] ΑΣΦΑΛΕΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ (ΣΟΥΡΗΣ –ΠΑΤΣΙΟΣ-ΓΡΗΓΟΡΙΑΔΗΣ)Ν.ΤΕΧΝΟΛΟΓΙΕΣ

[15] Simson Garfinkel-Gene Stafford:Web security and commerce .First edition June 1997

[16] Simson Garfinkel –Gene Stafford :Practikal Unix and Internet security 1996 second edition

[17] ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

[18] www.de sch.gr/~antoniou/My page/safe/internet/intro.htm(IOII)

[19] Stallings Williams(2003) Cryptography and NetworkSecurity:principles and practice

[20] ΚΟΜΝΗΝΟΣ-ΣΠΥΡΑΚΗ:Ασφάλεια δικτύωνκαι υπολογιστικών συστημάτων.

[21] ΚΑΤΣΙΚΑΣ ΣΩΚ.: Ο ρόλος της υποδομής του δημοσίου κλειδιού στην ανάπτυξη των ηλεκτρονικών αγορών,Πανεπιστήμιο Αιγαίου.