Τ.Ε.Ι ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σπουδαστές :

Κοσμά Παρασκευή
Α.Μ 3397
Καραγιάννη Αιμιλία
Α.Μ 3416

Με θέμα:

ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΗΣ ΔΙΑΚΙΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Εισηγητής:Καθηγητής
Τσιαντής Λεωνίδας

Άρτα – Νοέμβριος

ΠΡΟΛΟΓΟΣ

Η ανάγκη για ασφαλή διακίνηση πληροφοριών που επιτυγχάνεται με την λήψη αντίστοιχων μέτρων για την προστασία των συνεχώς αναπτυσσόμενων και αυξανόμενων WWW εφαρμογών και υπηρεσιών, έχει αρχίσει να γίνεται επιτακτική για τις επιχειρήσεις και γενικότερα για κάθε χρήστη.

Όταν μία επιχείρηση συνδέει το προσωπικό της δίκτυο στο internet δεν προσφέρει απλά στους υπαλλήλους της πρόσβαση σε πληροφορίες ή διαδικτυακές υπηρεσίες, αλλά επιπλέον δίνει τη δυνατότητα σε εξωτερικούς χρήστες να προσεγγίσουν τις ιδιωτικές πληροφορίες της επιχείρησης. Έτσι λοιπόν καλείται να πάρει τα απαραίτητα μέτρα για την ομαλή λειτουργία της σε θέματα που αφορούν την ασφάλεια.

Σκοπός αυτής της πτυχιακής εργασίας είναι η παρουσίαση του προβλήματος της ασφάλειας, γνωρίζοντας κάποιες από τις αρχές και τις τεχνικές ηλεκτρονικής κρυπτογραφίας και ασφάλειας που εφαρμόζονται στα διεθνή δίκτυα Η/Υ.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΑΠΕΙΛΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ

Τα υπολογιστικά συστήματα είναι ευάλωτα σε πολλές απειλές που επιφέρουν διάφορους τύπους βλαβών με αποτέλεσμα σημαντικές απώλειες. Οι βλάβες αυτές ποικίλουν από λάθη επιβλαβή στην ακεραιότητα των βάσεων δεδομένων μέχρι πυρκαγιές που μπορούν να καταστρέψουν ολόκληρα υπολογιστικά κέντρα. Οι απώλειες μπορούν να προέρχονται για παράδειγμα από τις πράξεις υποτιθέμενων έμπιστων υπαλλήλων που εξαπατούν ένα σύστημα, από εξωτερικούς hackers ή από απρόσεχτους υπαλλήλους που εισάγουν δεδομένα. Ακρίβεια στην εκτίμηση των απωλειών σχετιζομένων με την ασφάλεια υπολογιστών δεν είναι δυνατή εξαιτίας του γεγονότος ότι πολλές απώλειες ποτέ δεν ανακαλύπτονται, και άλλες συγκαλύπτονται για να αποφευχθεί δυσάρεστη δημοσιότητα. Τα αποτελέσματα των ποικίλων απειλών διαφέρουν αισθητά. Μερικά επηρεάζουν την αίσθηση εμπιστοσύνης ή την ακεραιότητα των δεδομένων ενώ άλλα επηρεάζουν την διαθεσιμότητα ενός συστήματος.

Εικόνα 1.1

1.1 Απάτες και κλοπές

Η χρήση των υπολογιστικών συστημάτων είναι δυνατή για απάτες και για κλοπή. Για παράδειγμα, άτομα μπορούν να χρησιμοποιήσουν ένα υπολογιστή για να καταχραστούν μικρά ποσά από ένα μεγάλο αριθμό λογαριασμών, υποθέτοντας ότι τα μικρά αυτά ποσά ποτέ δεν θα γίνουν αντιληπτά ότι καταχράστηκαν. Τα οικονομικά συστήματα δεν είναι τα μόνα που ριψοκινδυνεύουν. Συστήματα τα οποία ελέγχουν την πρόσβαση σε οποιουσδήποτε πόρους είναι και αυτά στόχοι (π.χ. συστήματα απογραφών, συστήματα που κρατούν την βαθμολογία στα σχολεία, μεγάλων αποστάσεων τηλεφωνικά συστήματα κ.α).

Η ηλεκτρονική απάτη μπορεί να γίνει είτε από άτομα που έχουν σχέση με το σύστημα είτε από αυτά που δεν έχουν. Τα άτομα που έχουν κάποια σχέση είναι αυτά που ευθύνονται για το μεγαλύτερο ποσοστό απάτης. Αφού τα άτομα αυτά έχουν πρόσβαση και γνωρίζουν καλύτερα το θύμα-υπολογιστικό σύστημα, είναι σε καλύτερη θέση να προκαλέσουν εγκλήματα. Τα άτομα που έχουν σχέση με το υπολογιστικό σύστημα μπορεί να είναι είτε χρήστες είτε τεχνικό προσωπικό. Ένας πρώην υπάλληλος του οργανισμού με γνώσεις για τις λειτουργίες του οργανισμού μπορεί επίσης να είναι μία απειλή ιδιαίτερα αν η συνεργασία του με τον οργανισμό δεν έχει τερματιστεί με τον καλύτερο τρόπο

1.2 Εχθρικοί κώδικες

Με τον όρο αυτό αναφερόμαστε στους ιούς, τα ‘σκουλίκια’ (worms), τους Δούρειους Ίππους και διάφορους άλλους κώδικες που μπορούν να εισέλθουν ‘απροσκάλεστα’ στα υπολογιστικά συστήματα.

Τα **σκουλήκια** είναι αυτό-αναπαραγόμενα προγράμματα τα οποία δρουν από μόνα τους και δεν χρειάζονται πρόγραμμα ξενιστή (host). Τα προγράμματα αυτά δημιουργούν ένα αντίγραφο του εαυτού τους και το εκτελούν, χωρίς να χρειάζεται η μεσολάβηση του χρήστη. Τα σκουλήκια συχνά χρησιμοποιούν τις υπηρεσίες του δικτύου για να διαδοθούν στους υπόλοιπους υπολογιστές.

Ένας **ιός** είναι ένα τμήμα κώδικα το οποίο αναπαράγεται με το να προσαρτήσει αντίγραφά του σε εκτελέσιμα αρχεία που υπάρχουν. Το νέο αντίγραφο του ιού εκτελείται όταν ο χρήστης εκτελέσει το νέο φορέα πρόγραμμά. Ο ιός μπορεί να περιέχει ένα επιπρόσθετο φορτίο το οποίο ενεργοποιείται όταν κάποιες συγκεκριμένες υποθέσεις ικανοποιούνται. Για παράδειγμα, ορισμένοι ιοί εμφανίζουν ένα γραπτό μήνυμα σε συγκεκριμένες ημερομηνίες. Υπάρχουν πολλοί τύποι ιών όπως αυτοί που μένουν μόνιμα στην μνήμη και αυτοί που είναι πολυμορφικοί. Θα πρέπει να τονίσουμε πως οι ιοί εισέρχονται μέσω cd, δισκέτας, σύνδεσης, e-mail, site.

Εικόνα 1.2

Οι ιοί κατατάσσονται στις εξής κατηγορίες:

1. Ιοί- καταστροφείς

Αυτού του είδους οι ιοί εισέρχονται σε ένα σύστημα και καταστρέφουν αρχεία και δεδομένα

2. Εικονικοί ιοί (φορείς)

Αυτοί οι ιοί εικονικά έχουν προκαλέσει κάποια ζημιά στο πρόγραμμα χωρίς να το έχουν κάνει.

3. Αυτοαναπαραγόμενοι ιοί

Εισέρχονται κάποια χρονική στιγμή στο σύστημα και μπαίνουν από μόνοι τους σε λειτουργία (κάποιες συγκεκριμένες ημερομηνίες).

4. Δούρειος Ίππος (κλοπή δεδομένων)

Τα δεδομένα που μπορούν να κλαπούν είναι στοιχεία τηλεφωνικού λογαριασμού.

5. Ιοί Μακροεντολών

Είναι οι ιοί οι οποίοι αλλάζουν ως προς το χειρότερο, εν ολίγοις καταστρέφουν την λειτουργία των μακροεντολών.

6. Ιοί Παρεμβολής Εκτέλεσης

Χαρακτηριστικό αυτής της κατηγορίας είναι ότι αυτοί οι ιοί παρεμβάλλονται κατά την εκτέλεση ενός προγράμματος.

7. Ιοί Μικροεφαρμογών

Είναι κάποιοι ιοί οι οποίοι χτυπάνε κάποια μικροπρογράμματα (π.χ όταν βάζουμε μία δισκέτα και αυτή έχει προσβληθεί από κάποιο ιό)

8. Ιοί στον έλεγχο λήψης αποφάσεων

Αυτοί οι ιοί έχουν την δυνατότητα να ανοίγουν και να κλείνουν τον υπολογιστή σε ακαθόριστες στιγμές του υπολογιστή.

Αντιβιοτικά για την προστασία κατά των ιών

- Dr Solomons Anti- virus

- McAfee

- Norton Anti- virus

Εικόνα 1.3

Δούρειος Ίππος είναι ένα πρόγραμμα το οποίο εκτελεί μία συγκεκριμένη αποστολή, αλλά και που επίσης περιέχει μη αναμενόμενες και ανεπιθύμητες λειτουργίες. Ένα παράδειγμα είναι ένα πρόγραμμα διόρθωσης σε ένα πολυχρηστικό σύστημα. Αυτό το πρόγραμμα μπορεί να τροποποιηθεί έτσι ώστε να διαγράφει τυχαία ένα από τα αρχεία κάποιου χρήστη κάθε φορά που θα εκτελεί μία χρήσιμη λειτουργία (διόρθωση).

1.3Hackers

Hackers ονομάζονται αυτοί που εισέρχονται μέσα σε συστήματα των υπολογιστών χωρίς εξουσιοδότηση. Μπορεί να συμπεριλαμβάνουν άτομα που έχουν σχέση με το σύστημα ή άτομα του εξωτερικού περιβάλλοντος.

Η απειλή των hackers πρέπει να θεωρηθεί ως περασμένη ή ενδεχόμενη μελλοντική ζημιά. Παρόλο που οι σύγχρονες απώλειες, που οφείλονται στους hackers, είναι σημαντικά μικρότερες από τις απώλειες που οφείλονται στους κλέφτες που έχουν σχέση με το σύστημα, το πρόβλημα των hackers έχει εξαπλωθεί και είναι σοβαρό. Ένα παράδειγμα δραστηριότητας hackers είναι η υποκλοπή του δημόσιου τηλεφωνικού συστήματος.

Οι hackers συχνά λαμβάνουν περισσότερης προσοχής από τις κοινές και επικίνδυνες απειλές. Το αμερικάνικο υπουργείο δικαιοσύνης προτείνει τρεις λόγους γι αυτό.

- Οι οργανισμοί δεν γνωρίζουν τις προθέσεις του hacker, οπότε μερικοί hackers απλώς μπαίνουν, άλλοι κλέβουν και άλλοι προκαλούν άλλου είδους ζημιά. Αυτή η αδυναμία του προσδιορισμοί των προθέσεων του hacker δείχνει ότι οι επιθέσεις τους δεν έχουν όρια.

- Οι επιθέσεις των hackers κάνουν τους ανθρώπους να νιώθουν αδύναμοι, επειδή η ταυτότητα των hackers είναι άγνωστη. Για παράδειγμα, η υπόθεση του κάποιος να προσλάβει έναν βαφέα να του βάψει το σπίτι και αυτός όταν είναι μέσα να κλέψει κάτι από το σπίτι. Οι υπόλοιποι ιδιοκτήτες στην γειτονιά δεν θα νιώσουν απειλή από αυτό το έγκλημα και θα προσπαθήσουν να προστατεύσουν τους εαυτούς τους με το να μην συνεργαστούν με αυτόν το βαφέα.

Αντίθετα, αν ένας διαρρήκτης μπει στο ίδιο σπίτι και κλέψει, τότε ολόκληρη η γειτονιά θα νιώσει ευάλωτη και ανήσυχη.

- Όλοι γνωρίζουμε πως η απειλή των hackers είναι η πιο πρόσφατη. Διάφοροι οργανισμοί πάντα έπρεπε να ανησυχούν για τις ενέργειες των υπαλλήλων τους και να λαμβάνουν διάφορα μέτρα πειθαρχίας για να μειώσουν τις απειλές που προέρχονται από αυτούς. Ωστόσο, αυτά τα μέτρα είναι μη αποτελεσματικά γι αυτούς που δεν ανήκουν στον οργανισμό αυτόν και δεν υποκύπτουν στους κανόνες που επιβάλει σε υπαλλήλους.

Εικόνα 1.4

1.4Κατασκοπεία

Υπάρχουν δύο είδη κατασκοπείας : αυτή που έχει σχέση με την πολιτική και λέγεται διεθνής **κυβερνητική κατασκοπεία** και αυτή που έχει σχέση με τις βιομηχανίες και λέγεται **βιομηχανική κατασκοπεία** (industrial espionage).

Η βιομηχανική κατασκοπεία είναι η συλλογή ιδιοκτησιακών δεδομένων από εταιρείες ή από κυβερνήσεις που αποσκοπούν στην αρωγή άλλων εταιριών. Αυτού του είδους λοιπόν η κατασκοπεία μπορεί να διαπραχτεί είτε από εταιρίες που αποσκοπούν στην βελτίωση των συγκριτικών πλεονεκτημάτων τους είτε από κυβερνήσεις που επιδιώκουν να βοηθήσουν τις εγχώριες βιομηχανίες. Η ξένη βιομηχανική κατασκοπεία που διαπράττεται από μία κυβέρνηση συχνά αναφέρεται ως **οικονομική κατασκοπεία.** Μέχρι η πληροφορία να επεξεργασθεί και να αποθηκευτεί σε υπολογιστικά συστήματα, η ασφάλεια των υπολογιστών μπορεί να βοηθήσει στην προστασία κατά τέτοιων απειλών. Όμως μπορεί να κάνει ελάχιστα για να μειώσει την απειλή εξουσιοδοτημένων εργαζομένων που θα πουλήσουν αυτήν την πληροφορία.

Η βιομηχανική κατασκοπεία είναι σε άνθηση. Μία έρευνα υποστήριξε ότι το 58% των ‘κλοπών’ διεπράχθησαν από νυν ή πρώην υπαλλήλους. Οι τρεις πιο καταστροφικές κατηγορίες κλεμμένων πληροφοριών ήταν πληροφορίες τιμολόγησης, πληροφορίες βιομηχανικής διαδικασίας και πληροφορίες ανάπτυξης κα προδιαγραφών προϊόντων.

Σε μερικές περιπτώσεις απειλές που τέθηκαν από αλλοδαπές κρατικές υπηρεσίες πληροφοριών μπορεί να είναι παρούσες. Επιπρόσθετα, σε πιθανή οικονομική κατασκοπεία, οι αλλοδαπές υπηρεσίες πληροφοριών μπορεί να

στοχεύουν σε μη απόρρητα συστήματα για να διευρύνουν τις αποστολές πληροφοριών. Μερικές μη απόρρητες πληροφορίες οι οποίες μπορεί να τις ενδιαφέρουν περιλαμβάνουν ταξιδιωτικά σχέδια ανώτερων αξιωματούχων, σχέδια εκτάκτου ανάγκης και πολιτικής άμυνας, δορυφορικά δεδομένα, δεδομένα επιβολής νόμου, ανακρίσεων, αρχείων ασφαλείας κ.ά. Μία καθοδήγηση θα πρέπει να αναζητηθεί από ένα ενήμερο γραφείο ασφαλείας αναφορικά με τέτοιου είδους απειλές.

Εικόνα 1.5

1.5Απειλές στην προσωπική ζωή

Η συσσώρευση τεράστιων ποσών από ηλεκτρονικές πληροφορίες από κυβερνήσεις για άτομα, πιστωτικά γραφεία και ιδιωτικές επιχειρήσεις, συνδυασμένες με την ικανότητα των υπολογιστών να παρακολουθούν, να επεξεργάζονται και να αθροίζουν τεράστια ποσά πληροφοριών για άτομα

έχουν δημιουργήσει μία απειλή στην ιδιωτική ζωή του ατόμου. Η πιθανότητα ότι όλες αυτές οι πληροφορίες και η τεχνολογία μπορεί να συνδεθούν μεταξύ τους ίπταται σαν φάντασμα πάνω από την σύγχρονη εποχή πληροφοριών.

Η απειλή στην προσωπική ζωή καταφθάνει από πολλές πηγές. Σε αρκετές περιπτώσεις κυβερνητικοί υπάλληλοι πούλησαν προσωπικές πληροφορίες σε ιδιωτικούς αστυνομικούς ή σε άλλους 'χρηματιστές' της πληροφορίας.

Ενόσω η σπουδαιότητα και το κόστος της απειλής της ιδιωτικής ζωής στην κοινωνία είναι δύσκολο να αποτιμηθούν, είναι πασιφανές ότι η τεχνολογία της πληροφορίας γίνεται αρκετά ισχυρή να δικαιολογήσει τους κυβερνητικούς φόβους. Γι αυτό, απαιτείται αυξημένη αφύπνιση γύρω από το πρόβλημα.

Εικόνα 1.6

1.6Υπηρεσίες και Μηχανισμοί Ασφάλειας του OSI/ISO

Η αρχιτεκτονική ασφάλειας OSI παρουσιάστηκε για πρώτη φορά το 1989 από τον Οργανισμό Προτυποποίησης ISO με σκοπό να επεκτείνει τη χρήση του μοντέλου αναφοράς ISO/OSI. Από τότε αποτελεί σημείο αναφοράς για όσους ασχολούνται με θέματα ασφάλειας δικτύων.

Αυτή λοιπόν η αρχιτεκτονική προσφέρει μία γενική περιγραφή των υπηρεσιών ασφάλειας και των αντίστοιχων μηχανισμών, πραγματοποιώντας μία αντιστοίχηση των υπηρεσιών στα επίπεδα του μοντέλου OSI. Ενδιαφέρον σημείο αποτελεί το γεγονός ότι η αρχιτεκτονική ασφάλειας OSI δεν προτείνει λύσεις σε προβλήματα ασφάλειας, αλλά παρέχει ένα ολοκληρωμένο πλαίσιο ορολογίας κα μία γενική περιγραφή των υπηρεσιών και των αντίστοιχων μηχανισμών ασφάλειας για την περιγραφή των προβλημάτων ασφάλειας κα των αντίστοιχων λύσεων.

1.6.1Υπηρεσίες ασφάλειας

Στην αρχιτεκτονική ασφάλειας OSI οι υπηρεσίες διαχωρίζονται σε πέντε κλάσεις (classes). Οι κλάσεις αυτές, περιλαμβάνουν υπηρεσίες αυθεντικοποίησης, ελέγχου πρόσβασης, εμπιστευτικότητας, ακεραιότητας δεδομένων και μη αποποίησης.

Η **αυθεντικοποίηση** (authentication) στοχεύει να αποδεικνύει την ταυτότητα μιας οντότητας και να εξασφαλίζει τη γνησιότητα των μηνυμάτων που ανταλλάσσονται σε μία επικοινωνία. Διακρίνονται δύο είδη αυθεντικοποίησης:

- Αυθεντικοποίηση Ομότιμης Οντότητας (Peer Entity Authentication)

- Αυθεντικοποίηση Προέλευσης Δεδομένων (Data Origin Authentication

Ο **έλεγχος Προσπέλασης** (Access Control) είναι η υπηρεσία που παρέχει προστασία από τη χρήση πόρων του συστήματος από μη εξουσιοδοτημένες οντότητες. Οι υπηρεσίες ελέγχου πρόσβασης συνεργάζονται με τις υπηρεσίες αυθεντικοποίησης, αφού για να παραχωρηθούν τα κατάλληλα δικαιώματα πρόσβασης σε κάποιους πόρους θα πρέπει να έχει προηγηθεί κατάλληλη αυθεντικοποίηση.

Η **εμπιστευτικότητα δεδομένων** (Data Confidentiality) είναι υπηρεσία που εγγυάται ότι τα δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες. Οι μηχανισμοί που παρέχει μπορούν να εφαρμοστούν είτε σε ολόκληρο το μήνυμα, είτε σε τμήμα του. Συγκεκριμένα οι επιμέρους υπηρεσίες περιλαμβάνουν:

- Υπηρεσία Εμπιστευτικότητας Σύνδεσης (connection confidentiality service)

- Υπηρεσία Εμπιστευτικότητας μη Εγκατεστημένης Σύνδεσης (connectionless confidentiality service)

- Υπηρεσία Εμπιστευτικότητας Επιλεγμένου Πεδίου (selected field confidentiality service)

- Υπηρεσία Εμπιστευτικότητας Ροής Κίνησης (traffic flow confidentiality service)

Η **ακεραιότητα δεδομένων** (Data Integrity) εξασφαλίζει ότι τα μεταδιδόμενα δεδομένα δεν έχουν τροποποιηθεί από μη-εξουσιοδοτημένους χρήστες. Και σε αυτή την περίπτωση οι ανάλογοι μηχανισμοί μπορούν να εφαρμοστούν είτε σε ολόκληρο το μήνυμα ή σε ένα τμήμα του.

- Υπηρεσία Ακεραιότητας Σύνδεσης με Αποκατάσταση (connection integrity service with recovery)

- Υπηρεσία Ακεραιότητας Σύνδεσης Χωρίς Αποκατάσταση (connection integrity service without recovery)

- Υπηρεσία Ακεραιότητας Σύνδεσης Επιλεγμένου Πεδίου (selected field connection integrity service)

- Υπηρεσία Ακεραιότητας Άνευ Εγκατάστασης Σύνδεσης (connectionless integrity service)

- Υπηρεσία Ακεραιότητας Επιλεγμένου Πεδίου Άνευ Εγκατάστασης Σύνδεσης (selected field connectionless integrity service)

Η **μη-αποποίηση** (non-repudiation) εγγυάται ότι μία οντότητα δεν μπορεί να αποποιηθεί την αποστολή ή την παραλαβή ενός μηνύματος. Υπάρχουν δύο επιμέρους υπηρεσίες:

- Μη αποποίηση με Απόδειξη Προελεύσεως (Non-Repudiation With Proof Of Origin)

- Μη αποποίηση με Απόδειξη Παραδόσεως (Non-Repudiation With Proof Of Delivery)

Εικόνα 1.7

1.6.2Μηχανισμοί Ασφάλειας

Η αρχιτεκτονική ασφάλειας του OSI απαριθμεί οκτώ διαφορετικούς μηχανισμούς ασφάλειας.

- Η **κρυπτογραφία** (Encipherment) χρησιμοποιείται για να προσφέρει εμπιστευτικότητα στα δεδομένα και να υποστηρίξει ή να συμπληρώσει άλλους μηχανισμούς ασφάλειας.

- Οι **Μηχανισμοί Ψηφιακών Υπογραφών** (Digital signature Mechanisms), με τεχνικούς όρους, παρέχουν το ηλεκτρονικό αντίστοιχο της ιδιόχειρης, υπογραφής σε ψηφιακά έγγραφα. Η ψηφιακή υπογραφή επικυρώνει την ακεραιότητα ενός εγγράφου και αποτρέπει τον υπογράφοντα να αποποιηθεί την αποστολή του.

- Οι **Μηχανισμοί Ελέγχου Πρόσβασης** (Access Control Mechanisms) χρησιμοποιούν τους μηχανισμούς αυθεντικοποίησης για να προσφέρουν έλεγχο προσπέλασης σε πόρους ενός συστήματος ή δικτύου. Τέτοιου είδους μηχανισμοί αποτρέπουν:

    1. Μία μη-εξουσιοδοτημένη οντότητα να προσπελάσει πόρους του δικτύου.

    2. Μία εξουσιοδοτημένη οντότητα να προσπελάσει πόρους στους οποίους δεν της έχει παραχωρηθεί δικαίωμα πρόσβασης.

- Οι **Μηχανισμοί Ακεραιότητας δεδομένων** (Data Integrity Mechanisms) χρησιμοποιούνται για να διαφυλάξουν την ακεραιότητα των δεδομένων που μεταδίδονται, δηλαδή τη μη τροποποίησή τους. Σημειώνεται ότι αυτοί οι μηχανισμοί δεν προστατεύουν από επιθέσεις τύπου επανεκπομπής μηνυμάτων (replay attacks).

- Οι **Μηχανισμοί Ανταλλαγής Αυθεντικοποίησης** (Authentication Exchange Mechanisms) χρησιμοποιούνται για να επιβεβαιώσουν την ταυτότητα των οντοτήτων. Σύμφωνα με τη σύσταση X.509 των ISO και ITU-T χρησιμοποιείται ο όρος ισχυρός (strong) για να χαρακτηριστεί ένας μηχανισμός ανταλλαγής αυθεντικοποίησης όταν χρησιμοποιεί κρυπτογραφικές τεχνικές για να προστατεύει τα μηνύματα που ανταλλάσσονται. Αντίστοιχα, ο όρος ασθενής (weak) χρησιμοποιείται για να χαρακτηρισθεί ένας μηχανισμός ανταλλαγής αυθεντικοποίησης ο οποίος δεν κάνει χρήση παρόμοιων τεχνικών. Οι ασθενείς μηχανισμοί είναι ευπαθείς σε παθητικές επιθέσεις υποκλοπής και επιθέσεις τύπου επανεκπομπής μηνυμάτων.

- Οι **Μηχανισμοί επιπρόσθετης Κίνησης (**Traffic Padding Mechanisms) χρησιμοποιούνται για να προστατέψουν από επιθέσεις ανάλυσης κίνησης (traffic analysis). Δεν πρέπει να αποκαλύπτεται η πληροφορία αν τα δεδομένα που μεταδίδονται αναπαριστούν πραγματικές πληροφορίες.

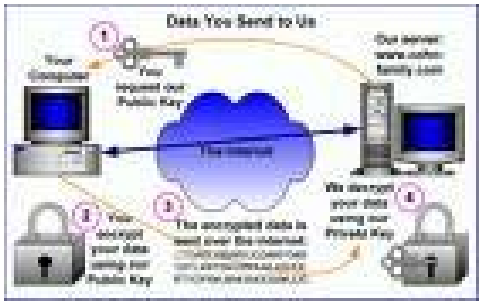
- Οι **Μηχανισμοί Ελέγχου Δρομολόγησης** (Routing Control Mechanisms) χρησιμοποιούνται ώστε να είναι δυνατή η επιλογή συγκεκριμένης πορείας για τα μεταδιδόμενα δεδομένα. Η πορεία αυτή είναι δυνατόν είτε να είναι προεπιλεγμένη, είτε να επιλέγεται με κριτήριο την ανίχνευση κάποιου εισβολέα. Για το λόγο αυτό είναι δυνατό να αποφεύγονται κάποιες διαδρομές των οποίων η ασφάλεια έχει παραβιαστεί.

- Οι **Μηχανισμοί Συμβολαιογράφου** (Notarisation Mechanisms) χρησιμοποιούνται για να διασφαλίσουν ιδιότητες των μεταδιδόμενων δεδομένων όπως ακεραιότητα, προέλευση και προορισμός. Η διασφάλιση παρέχεται από μία Έμπιστη τρίτη Οντότητα (Trusted Third Party –TTP).

ΚΕΦΑΛΑΙΟ 2

ΓΝΩΣΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Κρυπτογραφία είναι η επιστήμη και η ικανότητα να γράφεις με μυστικότητα κρατώντας τις πληροφορίες μυστικές. Όταν αναφερόμαστε σε υπολογιστές, η κρυπτογραφία προστατεύει δεδομένα έναντι της αποκάλυψης αυτών χωρίς άδεια. Μπορεί να αναγνωρίσει την ταυτότητα του χρήστη και φανερώνει την πλαστογραφία χωρίς άδεια. Η κρυπτογραφία είναι ένα αναπόφευκτο μέρος της μοντέρνας ασφάλειας υπολογιστών.

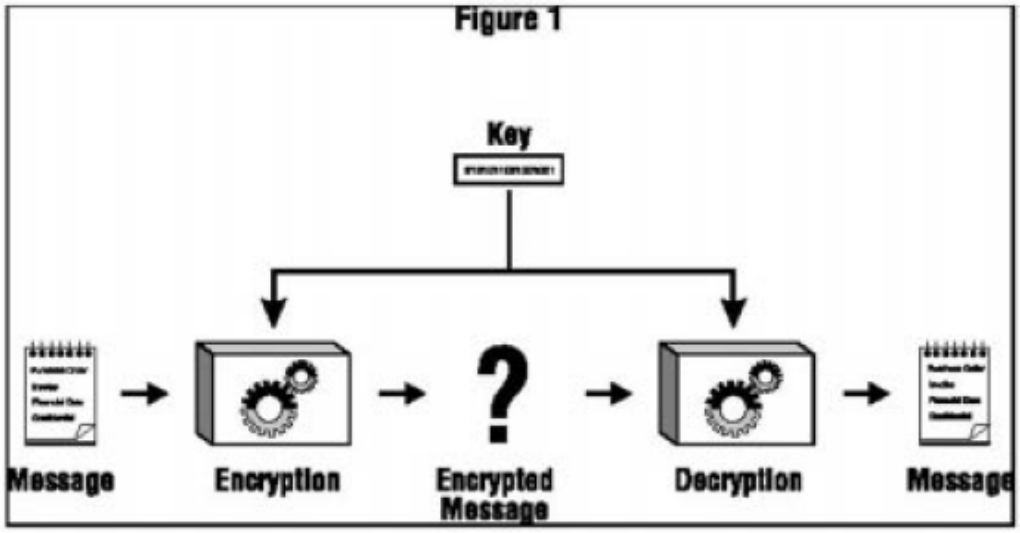


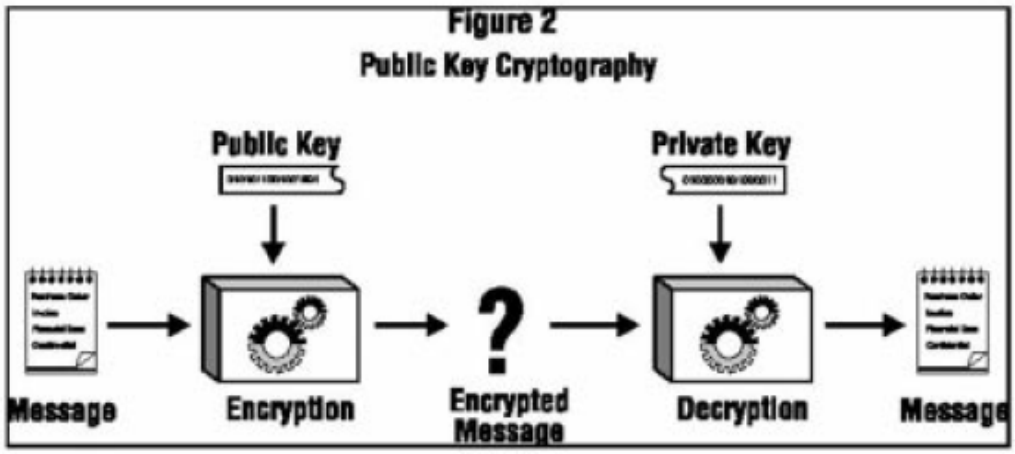
Εικόνα 2.1

2.1 Τι είναι κρυπτογράφηση;

Κρυπτογράφηση είναι μία διεργασία με την οποία ένα μήνυμα (που ονομάζεται plaintext) μετατρέπεται σε ένα άλλο μήνυμα (που ονομάζεται ciphertext) χρησιμοποιώντας μία μαθηματική συνάρτηση (αλγόριθμος κρυπτογράφησης) και ένα ειδικό password κρυπτογράφησης, που ονομάζεται κλειδί.

Αποκρυπτογράφηση είναι η ανάποδη διεργασία: το ciphertext μετατρέπεται στο αρχικό κείμενο (plaintext) χρησιμοποιώντας μία 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.





Εικόνα 2.2

2.2 Η χρησιμότητα της κρυπτογράφησης

Η κρυπτογράφηση μπορεί να παίξει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες:

- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες αποθηκευμένες στον υπολογιστή μας από πρόσβαση ενός τρίτου, με ή χωρίς άδεια.

- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να εμποδίσει και για να εντοπίσει τυχαίες ή σκόπιμες αλλαγές στα δεδομένα μας.

- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες κατά την διάρκεια της μεταφοράς από ένα υπολογιστικό σύστημα στο άλλο.

- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού.

Πέρα από αυτά τα 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 όπως είναι.

- Ένας εισβολέας μπορεί να έχει πρόσβαση στα αρχεία μας πριν τα κρυπτογραφήσουμε και αφού τα αποκρυπτογραφήσουμε.

- 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. Η μπορεί να κρατά σε ένα αρχείο όλα τα κλειδιά για να τα χρησιμοποιήσει αργότερα.

- Ένας εισβολέας ίσως βρει έναν άγνωστο προηγούμενα και σχετικά εύκολο τρόπο να αποκρυπτογραφεί τα μηνύματα που εμείς κρυπτογραφούμε με κάποιο αλγόριθμο.

Για αυτούς τους λόγους η κρυπτογράφηση θα πρέπει να θεωρείται σαν ένα μέρος της ολικής στρατηγικής ασφάλειας που έχουμε, και όχι σαν υποκατάστατο άλλων μέτρων ασφαλείας που πρέπει να έχουμε, όπως είναι ο κατάλληλος έλεγχος πρόσβασης στον υπολογιστή μας.

2.3 Στοιχεία της κρυπτογράφησης

Υπάρχουν πολλοί διάφοροι τρόποι με τους οποίους μπορούμε να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε μία πληροφορία με έναν υπολογιστή. Παρ' όλα, αυτά όλα αυτά τα συστήματα κρυπτογράφησης μοιράζονται κοινά στοιχεία:

Plaintext

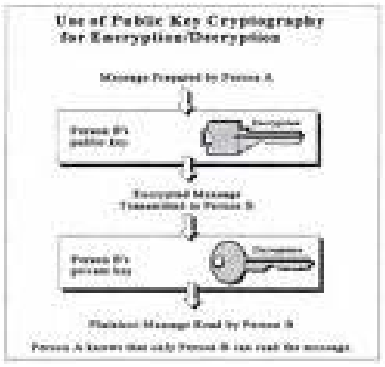
Η πληροφορία την οποία επιθυμούμε να κρυπτογραφήσουμε.

Ciphertext

Η πληροφορία αφού αυτή κρυπτογραφήθηκε.

Αλγόριθμος κρυπτογράφησης

Ο αλγόριθμος κρυπτογράφησης είναι μία συνάρτηση, συνήθως μαθηματικών αρχών, η οποία εκτελεί το έργο της κρυπτογράφησης και της αποκρυπτογράφησης των δεδομένων μας.



Εικόνα 2.3

Κλειδιά κρυπτογράφησης

Τα κλειδιά κρυπτογράφησης χρησιμοποιούνται από τον αλγόριθμο κρυπτογράφησης για να ορίσουν πώς τα δεδομένα είναι κρυπτογραφημένα ή

αποκρυπτογραφημένα. Τα κλειδιά είναι παρόμοια με τα password των υπολογιστών: όταν ένα κομμάτι πληροφορίας κρυπτογραφείται, 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. Εάν δώσουμε το σωστό κλειδί θα πάρουμε το αρχικό μήνυμα. Εάν προσπαθήσουμε να αποκρυπτογραφήσουμε ένα αρχείο με λάθος κλειδί, θα πάρουμε σκουπίδια.

Μήκος κλειδιών

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

Εικόνα 2.4

2.4 Συμμετρική Κρυπτογράφηση

Στην συμμετρική κρυπτογράφηση (symmetric key encryption) ή συμβατική κρυπτογράφηση ή κρυπτογράφηση Ιδιωτικού κλειδιού (secret key encryption) και τα δύο συναλλασσόμενα μέρη θα πρέπει να συμφωνήσουν για ένα κοινό μυστικό κλειδί και να εξασφαλισθεί η ασφαλής μετάδοση του. Επιπλέον, κάθε χρήστης θα πρέπει να έχει τόσα μυστικά κλειδιά όσα και τα μέλη με τα οποία συναλλάσσεται. Τέλος δεν ικανοποιείται η απαίτηση για αυθεντικότητα, γιατί δεν μπορεί να αποδειχθεί η ταυτότητα των συναλλασσόμενων μερών. Από την στιγμή που δύο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δύο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε το άλλο άτομο. Κατά συνέπεια η μη –αποποίηση ευθύνης για τη αποστολή ενός μηνύματος καθίσταται και αυτή αδύνατη. Το πρόβλημα αυτό επιλύεται με την κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση.

2.4.1 Κανόνες Συμμετρικής Κρυπτογράφησης

Ένα σχήμα συμβατικής κρυπτογραφίας αποτελείται από πέντε επιμέρους οντότητες.

- *Αρχικό κείμενο (plaintext*): Αποτελεί το αρχικό μήνυμα ή τα αρχικά δεδομένα που εισάγονται στον αλγόριθμο κρυπτογράφησης.
- *Αλγόριθμος κρυπτογράφησης (encryption algorithm)*: Πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος.

- *Μυστικό κλειδί (secret key)*: Αποτελεί το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί.

- *Κρυπτογράφημα ή Κρυπτογραφημένο μήνυμα (ciphertext):* Είναι το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης. Το κρυπτογράφημα αυτό εξαρτάται τόσο από το αρχικό μήνυμα όσο και από το μυστικό κλειδί, συνεπώς δοθέντος ενός μηνύματος διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.

- *Αλγόριθμος αποκρυπτογράφησης (decryption algorithm):*Πρόκειται για έναν αλγόριθμο που πραγματοποιεί την αντίστροφη διαδικασία, δηλαδή λαμβάνει το κρυπτογράφημα και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.

Για την ασφαλή χρήση της συμβατικής κρυπτογραφίας πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις:

- Απαιτείται η ύπαρξη ενός ισχυρού (strong) αλγορίθμου κρυπτογράφησης. Ως ελάχιστη απαίτηση αναφέρεται η ύπαρξη αλγορίθμου για τον οποίο ακόμη κι εάν αυτός είναι γνωστός στο

δυνητικό επιτιθέμενο και υπάρχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφήματα, αυτός δε δύναται ούτε να υπολογίσει το μυστικό κλειδί, ούτε να συμπεράνει το αρχικό κείμενο, δηλαδή δε δύναται να κρυπταναλύσει το κρυπτογράφημα. Αυτή η απαίτηση δηλώνεται αυστηρότερα ως ακολούθως: ο επιτιθέμενος πρέπει να είναι αδύνατο να κρυπταναλύσει το κρυπτογράφημα ή να ανακαλύψει το κλειδί, ακόμη και αν κατέχει κάποια κρυπτογραφήματα μαζί μα τα αντίστοιχα αρχικά μηνύματα, από τα οποία παράχθηκε καθένα από αυτά τα κρυπτογραφήματα.

- Ο πομπός και ο δέκτης πρέπει να έχουν παραλάβει τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να διαφυλάσσουν αυτό το μυστικό κλειδί σε ασφαλές μέρος. Εάν κάποιος γνωρίζει τον αλγόριθμο και ανακαλύψει το κλειδί, τότε όλη η επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη, συνεπώς παραβιάζεται η εμπιστευτικότητα.

2.4.2 Αλγόριθμοι Συμμετρικοί Κλειδιού (Symmetric Key or Private Key)

Οι αλγόριθμοι αυτοί χρησιμοποιούνται για μεγάλο όγκο δεδομένων ή επίσης για δεδομένα με συνεχή ροή. Είναι σχεδιασμένοι να εκτελούνται με ταχύτητα και έχουν μεγάλο αριθμό πιθανόν κλειδιών. Οι καλύτεροι αλγόριθμοι συμμετρικού κλειδιού φτάνουν το τέλειο: αν ένα δεδομένο κρυπτογραφηθεί με

ένα δοσμένο κλειδί, δεν υπάρχει τρόπος να το αποκρυπτογραφήσεις χωρίς να έχεις το ίδιο κλειδί.

Οι αλγόριθμοι συμμετρικοί κλειδιού μπορούν να χωριστούν σε δύο κατηγορίες. Σε αυτούς που κρυπτογραφούν ένα κομμάτι δεδομένων μόνο μιας ή αλγόριθμους ‘μπλοκ’, (block algorithms), και σε αυτούς που κάνουν την κρυπτογράφηση byte παρά byte σε δεδομένα συνεχής ροής ή αλγόριθμους ‘συρμού’, (stream algorithms).

Υπάρχουν πολλοί αλγόριθμοι συμμετρικού κλειδιού σε χρήση σήμερα. Μερικοί από αυτούς που συναντάμε συνήθως για την ασφάλεια του web είναι οι παρακάτω.

DES. (Data Encryption Standard) Εφαρμόστηκε από την κυβέρνηση των Ηνωμένων πολιτειών το 1977 και σαν ANSI πρότυπο το 1981. Είναι ένας ‘μπλοκ’ αλγόριθμος που χρησιμοποιεί κλειδί 56-bit και έχει πολλούς τύπους λειτουργιών ανάλογα με τον σκοπό που χρησιμοποιείται. Είναι ένας δυνατός αλγόριθμος, αλλά πιθανολογείται ότι μία μηχανή που θα είναι ικανή να σπάσει ένα κρυπτογραφημένο μήνυμα σε μερικές ώρες μπορεί να κατασκευαστεί για περισσότερα από 1.000.000 δολάρια. Τέτοιες μηχανές ίσως υπάρχουν αν και καμία κυβέρνηση ή επίσημη εταιρία δεν παραδέχεται ότι έχει.

DESX. Είναι μία απλή μετατροπή του DES αλγόριθμου για να βελτιώσει την ασφάλεια και να κάνει την αναζήτηση κλειδιού δυσκολότερη.

Triple – DES. Είναι ένας τρόπος να κάνεις το DES τουλάχιστον δυο φορές ποιο ασφαλές χρησιμοποιώντας τον DES αλγόριθμο τρεις φορές με τρία διαφορετικά κλειδιά.

IDEA. (International Data Encryption Algorithm). Αναπτύχθηκε στην Ζυρίχη της Ελβετίας, από τους James L. Massey και τον Xuejia Lai και δημοσιεύτηκε το 1990. Χρησιμοποιεί κλειδί 128 – bit και θεωρείται ότι είναι πολύ ασφαλής. Ο IDEA χρησιμοποιείται και από το πρόγραμμα PGP.

RC2. Είναι 'μπλοκ' αλγόριθμος και αναπτύχθηκε από τον Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Αυτός ο αλγόριθμος ανακαλύφθηκε από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet το 1996. Ο RC2 πωλείται με μία λειτουργία όπου μπορείς να χρησιμοποιήσεις κλειδιά από 1-bit έως 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 Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Επίσης αυτός ο αλγόριθμος ανακαλύφθηκε από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet το 1994 και εμφανίζεται αρκετά ασφαλής. Χρησιμοποιεί κλειδιά μήκους 1-bit έως 2048-bit, και συχνά περιορίζεται σε 40-bit κλειδιά για προγράμματα που εξάγονται.

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

2.5 Ασύμμετρη Κρυπτογράφηση

Η ασύμμετρη κρυπτογράφηση (Asymmetric Key Encryption) ή κρυπτογράφηση δημόσιου κλειδιού (Public Key Encryption) προτάθηκε το 1976 από τους W.Diffie και M.Hellman και υπήρξε ένα εξόχως σημαντικό βήμα στην περαιτέρω διάδοση της κρυπτογραφίας. Οι δύο ερευνητές τότε στο Stanford University, έγραψαν ένα έγγραφο στο οποίο υποστήριζαν την ύπαρξη μιας κρυπτογραφικής τεχνική, η οποία βασίζεται σε ένα ζεύγος κλειδιών εκ των οποίων το ένα είναι δημόσια γνωστό, ενώ το άλλο είναι ιδιωτικό. Σε αυτού του είδους την κρυπτογράφηση οτιδήποτε κρυπτογραφείται με το ένα κλειδί, μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί. Οι αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις και όχι σε απλές πράξεις με bits.

Το κύριο πλεονέκτημα που προσφέρει η κρυπτογράφηση δημόσιου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει. Η κρυπτογράφηση δημοσίου κλειδιού θεωρείται κατάλληλη για το ηλεκτρονικό εμπόριο για τους εξής λόγους:

- Εξασφαλίζει εμπιστευτικότητα του μηνύματος

- Παρέχει πιο ευέλικτα μέσα ελέγχου της ταυτότητας των χρηστών (authentication)

- Υποστηρίζει ψηφιακές υπογραφές (ακεραιότητα μηνύματος)

2.5.1 Δομή δημοσίου κλειδιού

Μία δομή δημοσίου κλειδιού αποτελείται από τις ακόλουθες συνιστώσες:

- *Αλγόριθμος κρυπτογράφησης (encryption algorithm):* Ο αλγόριθμος με τον οποίον πραγματοποιούνται οι διάφοροι μετασχηματισμοί στο αρχικό μήνυμα.

- *Αρχικό κείμενο (plaintext):* Είναι το μη κρυπτογραφημένο μήνυμα που αποτελεί στοιχείο εισόδου στον αλγόριθμο κρυπτογράφησης.

- *Ζεύγος δημόσιου (public) και ιδιωτικού (private) κλειδιού:*Ζεύγος κλειδιών, που έχει επιλεγεί με τρόπον ώστε, το δημόσιο κλειδί του παραλήπτη να χρησιμοποιηθεί για κρυπτογράφηση και το ιδιωτικό κλειδί του παραλήπτη για αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί πραγματοποιούνται από τον αλγόριθμο κρυπτογράφησης/ αποκρυπτογράφησης, εξαρτώμενοι από τις τιμές του δημόσιου και του ιδιωτικού κλειδιού που παρέχονται ως είσοδοι.

- *Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext):* Είναι το μήνυμα που παράγεται από τον αλγόριθμο κρυπτογράφησης ως

έξοδος. Εξαρτάται από το αρχικό μήνυμα και το δημόσιο κλειδί του παραλήπτη. Για ένα συγκεκριμένο μήνυμα από δύο διαφορετικά κλειδιά παράγονται από τη συνάρτηση κρυπτογράφησης δύο διαφορετικά κρυπτογραφημένα κείμενα.

- *Αλγόριθμος αποκρυπτογράφησης (decryption algorithm):* Είναι ο αλγόριθμος που δέχεται ως είσοδο το κρυπτογραφημένο μήνυμα και το ιδιωτικό κλειδί και παράγει το πρωτότυπο αρχικό μήνυμα

2.5.2 Αλγόριθμοι δημόσιου κλειδιού (public key)

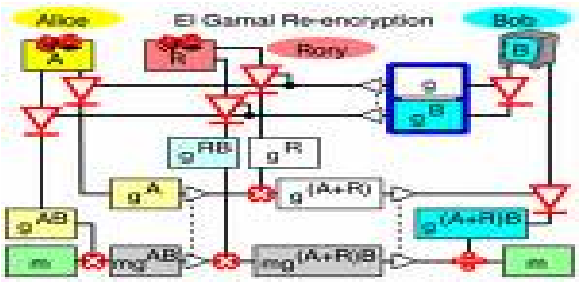
Μία ποικιλία από κρυπτογραφικά συστήματα δημόσιου κλειδιού είχαν αναπτυχθεί. Δυστυχώς υπήρχαν σημαντικά λιγότερα κρυπτογραφικά συστήματα δημόσιου κλειδιού από ότι συμμετρικού κλειδιού. Η αιτία έχει να κάνει με τον τρόπο που έχουν σχεδιαστεί οι αλγόριθμοι. Καλοί συμμετρικοί αλγόριθμοι απλά αλλάζουν την είσοδο ανάλογα με το κλειδί. Για να αναπτύξουμε ένα καινούριο αλγόριθμο συμμετρικού κλειδιού θα πρέπει να βρούμε έναν νέο ασφαλή τρόπο να αλλάζουμε την είσοδο. Οι αλγόριθμοι δημοσίου κλειδιού στηρίζονται στα μαθηματικά. Αναπτύσσοντας έναν τέτοιο αλγόριθμο απαιτείται να λυθεί ένα μαθηματικό πρόβλημα με ειδικές ιδιότητες.

Diffie-Hellman key exchange. Ένα σύστημα για ανταλλαγή κρυπτογραφικών κλειδιών ανάμεσα σε ενεργά μέρη. Το Diffie-Helman δεν είναι ακριβώς μια μέθοδος κρυπτογράφησης και αποκρυπτογράφησης, αλλά μία μέθοδος ανάπτυξης και ανταλλαγής ενός μοιρασμένου μυστικού κλειδιού σε ένα δημόσιο κανάλι επικοινωνίας. Στην πραγματικότητα, τα δύο μέρη συμφωνούν

σε μερικές κοινές αριθμητικές τιμές, και τότε το κάθε μέρος δημιουργεί ένα κλειδί. Οι μαθηματικοί μετασχηματισμοί των κλειδιών ανταλλάσσονται. Κάθε μέρος μπορεί τότε να υπολογίσει ένα τρίτο κλειδί συνόδου (session key) το οποίο δεν μπορεί εύκολα να παραχθεί από έναν επιτιθέμενο που γνωρίζει και των δύο τις αριθμητικές τιμές.

RSA. Ο RSA είναι πολύ γνωστό κρυπτογραφικό σύστημα αναπτυγμένο από καθηγητές του MIT, τους Ronald Rivest, Adi Shamir και Leonard Adleman. Ο RSA μπορεί να χρησιμοποιηθεί 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 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, είναι ένα κρυπτογραφικό σύστημα δημόσιου κλειδιού που είναι βασισμένο στο πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Helman. Ο ELGamal χρησιμοποιείται για κρυπτογράφηση και για ψηφιακές υπογραφές με τον ίδιο τρόπο όπως ο RSA.



Εικόνα 2.5

DSS. (Digital Signature Standard). Αναπτύχθηκε από την National Security Agency (NSA) και εφαρμόστηκε σαν ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών FIPS (Federal Information Processing Standard) από την NIST (National Institute for Standards and Technology). Ο DSS είναι βασισμένος στον αλγόριθμο ψηφιακών υπογραφών(DSA). Αν και ο DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, μόνο κλειδιά ανάμεσα σε 512 και 1024 bits επιτρέπονται στον DSS. Όπως αναφέρθηκε, ο DSS μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές αν και είναι πιθανό να χρησιμοποιήσει DSA εφαρμογές για την κρυπτογράφηση επίσης.

2.6 Αντοχή κρυπτογράφησης

Όλοι οι τύποι της κρυπτογραφίας δεν είναι ίδιοι. Μερικά συστήματα παρακάμπτονται εύκολα ή ‘σπάζονται’. Άλλα αντιστέκονται αρκετά ακόμα και στις ποιο καλές επιθέσεις. Η ικανότητα ενός κρυπτογραφικού συστήματος να προστατεύσει την πληροφορία από μία επίθεση ονομάζεται η αντοχή του. Η αντοχή εξαρτάται από πολλούς παράγοντες περιλαμβάνοντας:

- Η μυστικότητα του κλειδιού

- Η δυσκολία να μαντέψουμε το κλειδί, ή να δοκιμάσουμε όλα τα πιθανά κλειδιά. Μακρύτερα κλειδιά είναι γενικά δυσκολότερο να μαντέψεις ή να βρεις.

- Η δυσκολία να αναστρέψουμε έναν αλγόριθμο κρυπτογράφησης χωρίς να γνωρίζουμε το κλειδί (σπάσιμο του αλγόριθμου κρυπτογράφησης).

- Η ύπαρξη άλλων δρόμων, όπως λέμε ‘πίσω πόρτα’ με τους οποίους μπορούμε να αποκρυπτογραφήσουμε ποιο εύκολα ένα αρχείο χωρίς να γνωρίζουμε το κλειδί κρυπτογράφησης.

- Η ικανότητα να αποκρυπτογραφήσεις ένα ολόκληρο κρυπτογραφημένο μήνυμα εάν γνωρίζεις τον τρόπο με τον οποίον αποκρυπτογραφήθηκε ένα μέρος αυτού (known text attack).

- Η ιδιοκτησία και η γνώση των χαρακτηριστικών του plaintext από τον επιτιθέμενο. (Για παράδειγμα, ένα κρυπτογραφικό σύστημα είναι ευπρόσβλητο σε επίθεση εάν όλα τα μηνύματα που κρυπτογραφούνται με αυτό, αρχίζουν και τελειώνουν με ένα γνωστό κομμάτι κειμένου.)

Ο στόχος στον σχεδιασμό κρυπτογραφικών συστημάτων είναι η δημιουργία ενός αλγόριθμου που θα είναι πολύ δύσκολο να αναστραφεί χωρίς το κλειδί. Η δυσκολία της αναστροφής αυτής πρέπει να είναι σχεδόν ισοδύναμη με την προσπάθεια που απαιτείται για να μαντέψουμε το κλειδί προσπαθώντας με πιθανές λύσεις κάθε φορά. Για να μπορέσουμε να κρατήσουμε την διαδικασία αναστροφής του αλγόριθμου πολύ δύσκολη χρειάζεται να χρησιμοποιηθούν μαθηματικά υψηλού επιπέδου.

Εικόνα 2.6

2.7Υποδομή δημόσιου κλειδιού (Public Key Infrastructure)

Ένα σύστημα που αποδεικνύει τη ταυτότητα των ανθρώπων που κρατούν κρυπτογραφικά κλειδιά, ονομάζεται υποδομή δημόσιου κλειδιού.

Στην κρυπτογράφηση δημόσιου κλειδιού κάθε χρήστης απαιτείται να φτιάξει δύο κλειδιά:

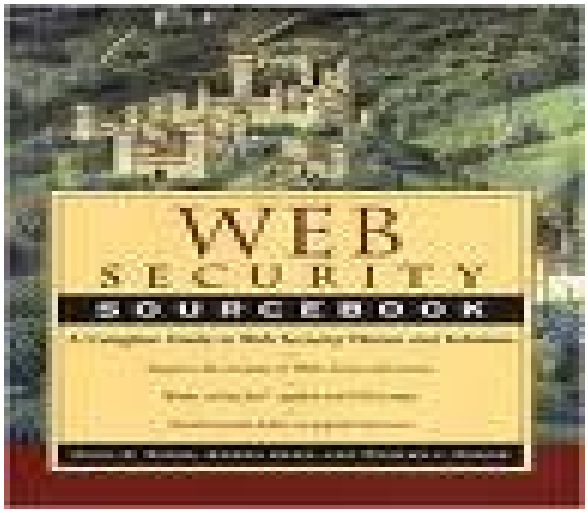
- Ένα δημόσιο κλειδί, το οποίο χρησιμοποιείται για να στέλνουμε κρυπτογραφημένα μηνύματα στον παραλήπτη, και για να επικυρώνουμε την ψηφιακή υπογραφή του αποστολέα.

- 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.

Σημείωση: Τα προσωπικά κλειδιά είναι σχεδιασμένα να κρατιούνται μυστικά, τα δημόσια κλειδιά είναι σχεδιασμένα να δημοσιεύονται και να διανέμονται ευρέως.

ΚΕΦΑΛΑΙΟ 3

ΑΣΦΑΛΕΙΑ ΣΤΟ WEB



Εικόνα 3.1

Ο παγκόσμιος ιστός είναι βασικά μία εφαρμογή πελάτη/ διακομιστή που παρέχει πολλές ευκολίες σε επιχειρήσεις, κυβερνήσεις και γενικότερα σε όποιον έχει πρόσβαση σε αυτόν. Το περιεχόμενο του διαδικτύου είναι πολύ εύκολο να εξελιχτεί, το λογισμικό που αποτελεί την βάση του, είναι πολύπλοκο. Αυτό λοιπόν το περίπλοκο λογισμικό μπορεί να κρύβει σοβαρές ατέλειες όσον αφορά την ασφάλεια.

Η μικρή ιστορία του διαδικτύου είναι γεμάτη με παραδείγματα νέων και εκσυγχρονισμένων συστημάτων εγκατεστημένα κατάλληλα, που είναι

επιρρεπή σε επιθέσεις. Όταν ένας web server υπονομευτεί, ένας εισβολέας μπορεί εύκολα να κερδίσει πρόσβαση σε δεδομένα και συστήματα που δεν ανήκουν στο δίκτυο αυτό καθεαυτό αλλά συνδεόμενος με τον server σε τοπική σελίδα. Χρήστες οι οποίοι δεν γνωρίζουν την αναγκαιότητα της ασφάλειας εξαιτίας έλλειψης γνώσεων ή και ακόμα μέσων, δεν είναι σε θέση να πάρουν τα κατάλληλα μέτρα για την προστασία του διαδικτύου.

3.1 Απειλές Ασφάλειας στο Web

Οι απειλές που μπορεί να δεχτεί το διαδίκτυο χωρίζονται σε δύο κατηγορίες: τις παθητικές και τις ενεργητικές. Στις παθητικές, ο εισβολέας σε περίπτωση σύγχυσης του δικτύου βρίσκει την ευκαιρία να κάνει επιτυχή την πρόσβαση σε ιστοσελίδες που υποτίθεται ότι δεν παραβιάζονται δηλαδή αυτές οι επιθέσεις περιλαμβάνουν την υποκλοπή (eavesdropping) στη δικτυακή κίνηση μεταξύ του browser και του server και την πρόσβαση σε ένα web site που υποτίθεται ότι είναι περιορισμένη. Οι ενεργητικές επιθέσεις περιλαμβάνουν την προσωποποίηση, άλλου χρήστη αλλάζοντας τα μηνύματα μεταξύ πελάτη και εξυπηρετητή και αλλάζοντας πληροφορία στην ιστοσελίδα.

Πιο συγκεκριμένα λόγοι που καθιστούν αναγκαία την ύπαρξη ασφάλειας στο world wide web είναι οι εξής:

1. Απώλεια πληροφορίας από:

    - Τροποποίηση δεδομένων και μνήμης.

- Trojan horse browser.

- Κλοπή της πληροφορίας από τον server.

- Κλοπή των δεδομένων από τον πελάτη.

- Τροποποίηση της κίνησης των μηνυμάτων κατά την μεταφορά

2. Καταπάτηση προσωπικών δεδομένων

3. Η μη σωστή παρουσίαση του χρήστη ο οποίος μπορεί να έχει υποστεί απομίμηση.

4. Παρεμπόδιση του χρήστη να κάνει σωστά την δουλειά του, κάτι το οποίο είναι ιδιαίτερα ενοχλητικό και διασπαστικό, και μπορεί να οφείλεται στο:

    - Γέμισμα του δίσκου ή της μνήμης

    - Κατακλυσμό του συστήματος από ψεύτικες απειλές

    - Απομόνωση μηχανής από επιθέσεις DNS

    - Καταστροφή των user threads

5. Δημιουργείται η ψευδαίσθηση ότι η πληροφορία που δέχεται ο χρήστης είναι αξιόπιστη ενώ στην ουσία αυτό που έχει προηγηθεί είναι η πλαστογραφία, παραχάραξη των δεδομένων. Αυτό βέβαια αντιμετωπίζεται με κατάλληλες κρυπτογραφικές τεχνικές σε αντίθεση με τα προηγούμενα που είναι αρκετά δύσκολο να αντιμετωπιστούνε.

6. Απώλεια χρημάτων.

Ένας τρόπος για να πραγματοποιηθεί ασφάλεια στο διαδίκτυο είναι η χρησιμοποίηση της υπηρεσίας IP, ένας άλλος είναι η επίτευξη ασφάλειας μέσω του TCP πρωτοκόλλου. Το πιο χαρακτηριστικό παράδειγμα αυτής της προσέγγισης του TCP είναι το Secure Socket Layer (SSL) και το ακόλουθό του TLS.

3.2 Λειτουργίες της κρυπτογράφησης

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

Εμπιστευτικότητα- Confidentiality

Η κρυπτογραφία χρησιμοποιείται για να μεταμορφώσει την πληροφορία που στέλνεται μέσω του internet και αποθηκεύεται στους servers , έτσι ώστε να μην μπορούν να δουν το περιεχόμενο των δεδομένων αυτοί που θέλουνε να παρέμβουνε. Μερικοί ονομάζουν αυτή την ιδιότητα *μυστικότητα (privacy)* αλλά

οι περισσότεροι χρησιμοποιούν αυτή τη λέξη για να αναφέρονται στην προστασία της ατομικής πληροφορίας.

Ακεραιότητα- Integrity

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

Απόδειξη γνησιότητας – Επικύρωση – Authentication

Οι ψηφιακές υπογραφές χρησιμοποιούνται για να εξακριβώσουν την ταυτότητα του αποστολέα ενός μηνύματος. Οι παραλήπτες ενός μηνύματος μπορούν να ελέγξουν την ταυτότητα του αποστολέα, ο οποίος υπέγραφε ψηφιακά το μήνυμα. Μπορούν να χρησιμοποιηθούν σε συνδυασμό με τα password ή και να τα αντικαταστήσουν.

Απαγόρευση απάρνησης - Nonrepudiation

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

3.3 Κρυπτογραφικά Συστήματα

Πολλά είναι τα κρυπτογραφικά συστήματα που χρησιμοποιούνται για το internet, τα τελευταία χρόνια. Χωρίζονται σε δύο κατηγορίες. Η πρώτη είναι

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

- SSH
- SSL
- PCT
- TLS
- S-HTTP
- SET and CyberCash
- DNSSEC
- IPsec and IPv6
- Kerberos

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

- PGP
- S/ MIME

3.4 Secure Shell – SSH

Το Secure Shell- SSH είναι ένα σχετικά απλό πρόγραμμα το οποίο μπορεί να χρησιμοποιηθεί για να συνδεθεί μία οντότητα ασφαλώς με μία απομακρυσμένη μηχανή, να εκτελεί εντολές σε αυτήν και να μεταφέρει αρχεία από μία μηχανή σε μία άλλη. Το SSH παρέχει ισχυρή αυθεντικοποίηση, αλλά και ασφαλή επικοινωνία διαμέσου μη ασφαλών διαύλων.

Το SSH δημιουργήθηκε από τον T.Ylonen από το Helsinki University of Technology , Finland. Σήμερα υπάρχουν διαθέσιμες δύο εκδόσεις του SSH:

- Μία εμπορική έκδοση, η οποία είναι διαθέσιμη στην έκδοση 3.2 για διάφορα συστήματα UNIX , καθώς επίσης και για Windows 95/NT, OS/2, MacOS.

3.4.1 Το Πρωτόκολλο Επιπέδου Μεταφοράς SSH

Το πρωτόκολλο επιπέδου μεταφοράς SSH (SSH Transport Layer Protocol) παρέχει κρυπτογραφημένη αυθεντικοποίηση host, καθώς επίσης και

εμπιστευτικότητα και προστασία ακεραιότητας δεδομένων, ενώ δεν παρέχει αυθεντικοποίηση χρήστη.

Αυτό λοιπόν το πρωτόκολλο υποστηρίζει διάφορους τρόπους ανταλλαγής κλειδιών, μυστικά και δημόσια κλειδιά, αλγόριθμους σύνοψης και αυθεντικοποίησης μηνυμάτων που συμφωνούνται κατά τη φάση εγκατάστασης μιας σύνδεσης. Υπάρχουν υποχρεωτικοί αλγόριθμοι τους οποίους πρέπει να υποστηρίζουν όλες οι υλοποιήσεις, αλλά και άλλοι αλγόριθμοι που ορίζονται στις προδιαγραφές του πρωτοκόλλου αλλά είναι προαιρετικοί.

3.4.2 Το SSH πρωτόκολλο αυθεντικοποίησης

Το SSH πρωτόκολλο αυθεντικοποίησης (SSH Authentication Protocol) σχεδιάστηκε να εκτελείται πάνω από το πρωτόκολλο επιπέδου μεταφοράς SSH για να παρέχει αυθεντικοποίηση χρήστη. Το αντίστοιχο όνομα υπηρεσίας είναι ssh-userauth. Στην αυθεντικοποίηση χρήστη ο εξυπηρετούμενος πρώτος δηλώνει το όνομα υπηρεσίας και το όνομα του χρήστη ο οποίος επιθυμεί να έχει πρόσβαση στην υπηρεσία. Ο εξυπηρέτης, με την σειρά του, απαντά με το σύνολο των μεθόδων αυθεντικοποίησης που είναι αποδεκτές για αυτή την υπηρεσία και ο εξυπηρετούμενος επιστρέφει μια αντίστοιχη αίτηση αυθεντικοποίησης στον εξυπηρέτη. Ο διάλογος συνεχίζεται, έως ότου η πρόσβαση επιτραπεί ή απορριφθεί.

3.5 SSL (Secure Socket Layer)

Το SSL (Secure Socket Layer) είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω του Internet. Αναπτύχθηκε από την Netscape και έγινε προσιτό από το πλατύ κοινό από τον Web browser και server της Netscape. Η ιδέα ήταν να μιμηθούν τις πωλήσεις μιας εταιρίας με κρυπτογραφικά ενεργοποιημένους web servers διανέμοντας έναν free client ο οποίος εφάρμοζε τα ίδια κρυπτογραφικά πρωτόκολλα.

Το Internet Engineering Task Force (IETF) είναι τώρα στη διαδικασία της δημιουργίας ενός Transport Layer Security (TLS) πρωτοκόλλου. Αυτό το πρωτόκολλο είναι βασισμένο στο SSL 3.0, με μικρές αλλαγές στις επιλογές αλγόριθμων.

Εικόνα 3.2

3.5.1 Τι είναι το SSL

Το SSL είναι ένα επίπεδο (layer) που υπάρχει ανάμεσα στη σειρά του TCP/IP πρωτοκόλλου και στο επίπεδο εφαρμογής. Ενώ το κανονικό TCP/IP πρωτόκολλο απλά στέλνει ένα ανώνυμο free-error ρεύμα πληροφοριών ανάμεσα στους δύο υπολογιστές, το SSL προσθέτει πολυάριθμες λειτουργίες σε αυτό το ρεύμα, περιλαμβάνοντας:

- Απόδειξη γνησιότητας και απαγόρευση απάρνησης του client, χρησιμοποιώντας ψηφιακές υπογραφές

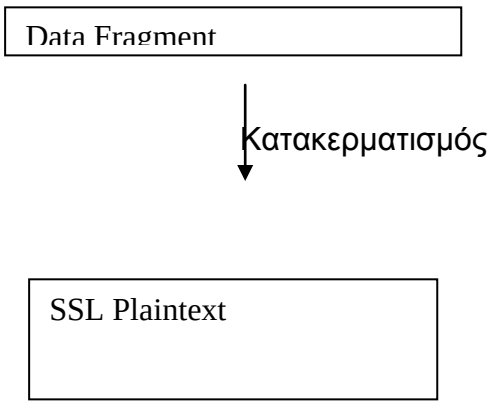
- Απόδειξη γνησιότητας και απαγόρευση απάρνησης του server, χρησιμοποιώντας ψηφιακές υπογραφές

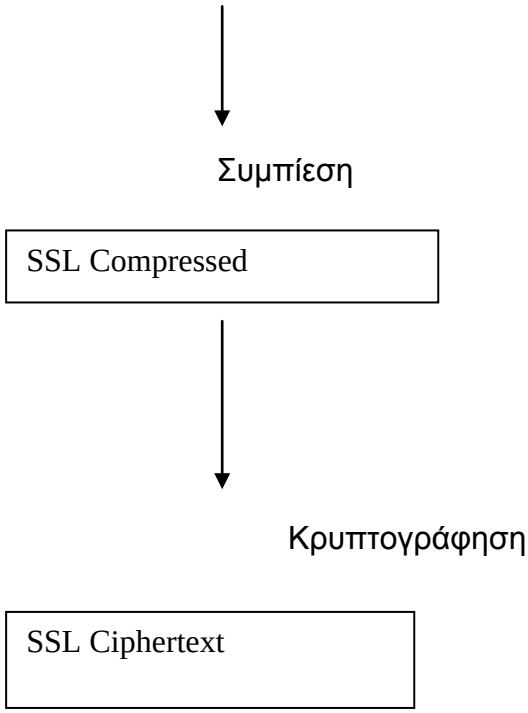
- Εμπιστοσύνη δεδομένων μέσω της χρήσης της κρυπτογραφίας

- Ακεραιότητα δεδομένων μέσω της χρήσης κωδικών απόδειξης γνησιότητας μηνυμάτων

3.5.1.1 SSL Record Protocol

Το SSL record protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό (fragmentation), τη συμπίεση, την αυθεντικοποίηση και την κρυπτογράφηση δεδομένων. Πιο συγκεκριμένα το πρωτόκολλο δέχεται ως είσοδο ένα τμήμα δεδομένων αυθαίρετου μεγέθους και παράγει ως έξοδο μία σειρά από SSL εγγραφές με μέγιστο μέγεθος 16.383 bytes η καθεμία





Σχήμα 3.2.2 :Τα βήματα του SSL record protocol

Όπως φαίνεται και στο πιο πάνω σχήμα τα βήματα που ακολουθεί το SSL κατά την επεξεργασία είναι:

1. Κατάτμηση των δεδομένων.

2. Συμπίεση, η οποία δεν πρέπει να αυξάνει το μήκος του περιεχομένου πάνω από 1024 bytes.

3. Υπολογισμός ενός κωδικού αυθεντικότητας μηνύματος πάνω στα συμπιεσμένα δεδομένα.

4. Το συμπιεσμένο μήνυμα μαζί με το MAC κρυπτογραφούνται χρησιμοποιώντας συμμετρική κρυπτογράφηση.

Το πρωτόκολλο αυτό παρέχει δύο υπηρεσίες:

Α. Το απόρρητο: Το Handshake protocol ορίζει ένα μυστικό κλειδί που χρησιμοποιείται για συμβατική κρυπτογράφηση.

Β. Ακεραιότητα μηνύματος . Το Handshake protocol ορίζει επίσης ένα μυστικό κλειδί το οποίο σχηματίζει έναν κώδικα αυθεντικότητας μηνύματος Message authentication code (MAC).

Διάφορα πρωτόκολλα SSL μπορούν να στρωματοποιούνται στην κορυφή του SSL record protocol. Κάθε πρωτόκολλο SSL μπορεί να αναφέρεται σε συγκεκριμένους τύπους μηνυμάτων τα οποία αποστέλλονται χρησιμοποιώντας το SSL record protocol. Οι προδιαγραφές SSL 3.0 καθορίζουν τα ακόλουθα τρία πρωτόκολλα SSL:

- Πρωτόκολλο προειδοποίησης (SSL Alert Protocol).
- Πρωτόκολλο χειραψίας (SSL Handshake Protocol).
- Πρωτόκολλο Αλλαγής Προδιαγραφών Κρυπτογραφίας (SSL Change Cipher Spec Protocol).

Το SSL alert protocol χρησιμοποιείται για να μεταβιβάζει προειδοποιήσεις (alerts) μέσω του SSL record protocol. Οι προειδοποιήσεις αποτελούν ένα συγκεκριμένο τύπο μηνύματος που αποτελείται από μέρη: ένα επίπεδο προειδοποίησης και μία περιγραφή προειδοποίησης. Το πρωτόκολλο χειραψίας θα το περιγράψουμε μετέπειτα. Το πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας χρησιμοποιείται για την αλλαγή μιας προδιαγραφής κρυπτογραφίας με μία άλλη. Αποτελείται από ένα απλό μήνυμα μήκους ενός byte με τιμή ίση με 1. Ο μόνος σκοπός αυτού του μηνύματος είναι να προκαλέσει την εκκρεμή κατάσταση να αντιγραφεί στην τρέχουσα κατάσταση που ενημερώνει το cipher suite να χρησιμοποιηθεί σε αυτή τη σύνδεση. Τέλος, θα πρέπει να επισημάνουμε ότι το SSL record protocol μπορεί επίσης να χρησιμοποιηθεί για να σταλούν αυθαίρετα δεδομένα του χρήστη.

Γενικά η βασική ιδέα του SSL είναι:

Α. Τα bytes έχουν μία αλληλουχία και επιλέγονται από τον πελάτη και τον διακομιστή.

Β. Το secret Key (μυστικό κλειδί) το οποίο χρησιμοποιείται σε MAC χειρισμούς δεδομένων στέλνεται από τον server.

Γ. Το συμβατικό κλειδί κρυπτογράφησης για τα δεδομένα κρυπτογραφείται από τον server και αποκρυπτογραφείται από τον client.

Δ. Το συμβατικό κλειδί κρυπτογράφησης για τα δεδομένα κρυπτογραφείται από τον client και αποκρυπτογραφείται από τον server.

3.5.1.2 SSL Handshake Protocol

Το SSL handshake protocol είναι το κύριο πρωτόκολλο που στρωματοποιείται στην κορυφή το SSL record protocol.Έτσι, τα μηνύματα SSL handshake προωθούνται στο SSL record επίπεδο όπου ενθυλακώνονται εντός μιας ή περισσοτέρων SSL εγγραφών, οι οποίες επεξεργάζονται και μεταδίδονται όπως καθορίζεται από τη μέθοδο συμπίεσης και την προδιαγραφή κρυπτογραφίας της τρέχουσας κατάστασης συνόδου και σύνδεσης.

Γενικά, το Handshake Protocol επιτρέπει στον πελάτη και στον διακομιστή να κάνουν ορατή την αυθεντικότητά τους ο ένας στον άλλον δηλαδή τους επιτρέπει να εξακριβώσουν την γνησιότητα του άλλου. Επίσης διαπραγματεύονται κάποιες λειτουργίες, την κρυπτογράφηση, τον Mac αλγόριθμο και τα κλειδιά κρυπτογράφησης τα οποία θα χρησιμοποιηθούν για την προστασία δεδομένων στο SSL record. Το Handshake protocol χρησιμοποιείται πριν μεταδοθούν τα δεδομένα Αποτελείται από μια σειρά μηνυμάτων που ανταλλάσσονται μεταξύ του client και του server. Κάθε μήνυμα έχει τρία πεδία:

- Τύπος (1 byte),

- Μήκος (3 bytes)

- Περιεχόμενο (>1 byte).

3.5.2 Εκδόσεις του SSL

Το SSL πρωτόκολλο σχεδιάστηκε από την Netscape για χρήση με τον Netscape Navigator. Η έκδοση 1.0 του πρωτοκόλλου χρησιμοποιήθηκε μέσα στο Netscape. Η έκδοση 2.0 συμπεριλήφθηκε με το Netscape Navigator 1 και 2. Αφού το SSL 2.0 δημοσιεύτηκε, η Microsoft δημιούργησε ένα παρόμοιο secure link πρωτόκολλο, ονομαζόμενο PCT,το οποίο ξεπέρασε μερικές αδυναμίες του SSL 2.0. Τα πλεονεκτήματα του PCT ενσωματώθηκαν στο SSL 3.0. Το SSL 3.0 πρωτόκολλο χρησιμοποιήθηκε σαν την βάση για το Transport Layer Security (TLS) πρωτόκολλο που αναπτύχθηκε από την IETF.

3.5.3 Κλειδιά στο SSL

Υπάρχει ένας αριθμός από κλειδιά που χρησιμοποιούνται: το **δημόσιο κλειδί** του server, το **server-write-key**, και το **client-write-key**. Το server-write-key, και το client-write-key παράγονται μέσω μιας hash από το master key, ένα ordinal χαρακτήρα, την πρόκληση και το id της σύνδεσης.

3.6 PCT (Private Communication Technology

Το Σεπτέμβριο του 1995 η Microsoft corporation εξέδωσε ένα Internet Draft στο οποίο πρότεινε μία ελαφρώς βελτιωμένη έκδοση του SSL 2.0 που

ονομάσθηκε Private Communication Technology (PCT) έκδοση 1.0. Όπως συμβαίνει και με το SSL, το PCT 1.0 εκτελείται στην κορυφή μιας αξιόπιστης και προσανατολισμένης σε σύνδεση υπηρεσίας μεταφοράς, όπως εκείνη που παρέχεται από το TCP/IP και μπορεί να χρησιμοποιείται για να παρέχει ασφάλεια σε οποιοδήποτε TCP/IP πρωτόκολλο εφαρμογών στρωματοποιείται στην κορυφή του. Επίσης, όπως συμβαίνει και στο SSL, το PCT 1.0 διαιρείται σε δύο υποπρωτόκολλα που ονομάζονται PCT record protocol και PCT handshake protocol:

- Το PCT record protocol χρησιμοποιείται για την ενθυλάκωση δεδομένων χειραψιών και εφαρμογών μέσα σε PCT εγγραφές.

- Το PCT handshake protocol στρωματοποιείται στην κορυφή του PCT record protocol και χρησιμοποιείται για να αυθεντικοποιήσει τον εξυπηρέτη στον εξυπηρετούμενο (και, προαιρετικά, αντιστρόφως) και για να συμφωνεί τους αλγορίθμους MAC και κρυπτογράφησης καθώς και τα αντίστοιχα κλειδιά.

3.7 Transport Layer Security Protocol – TLS

Το TLS πρωτόκολλο δημιουργήθηκε τον Απρίλιο του 1996 από το IETF για την περιοχή ασφάλειας επιπέδου μεταφοράς. Αποτελεί μία τυποποίηση IETF της οποίας στόχος είναι να παρέχει μία έκδοση του SSL. Η κανονική έκδοσή του μοιάζει με του SSL. Αρχικά αναπτύχθηκε βασιζόμενο στις πρόσφατες διαθέσιμες προδιαγραφές του SSL (2.0 και 3.0), του PCT (1.0) και του SSH

(2.0)_,και διαπιστώθηκε πως ήταν ουσιαστικά ίδιο με τις προδιαγραφές του SSL 3.0. Άλλωστε η στρατηγική της ομάδας εργασίας για τις προδιαγραφές του TLS 1.0 ήταν να βασίζονται στο SSL 3.0, παρά στα SSL 2.0, PCT 1.0, SSH 2.0 ή οποιαδήποτε άλλη πρόταση πρωτοκόλλου ασφάλειας επιπέδου μεταφοράς.

3.8 S-HTTP

Το S- HTTP είναι ένα σύστημα για υπογραφή και κρυπτογράφηση πληροφοριών μέσω του HTTP πρωτοκόλλου. Το S-HTTP σχεδιάστηκε πριν να κυκλοφορήσει δημόσια το SSL. Περιλαμβάνει μερικά χαρακτηριστικά, όπως είναι 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.

3.9 Πληρωμές μέσω Ηλεκτρονικών Πιστωτικών Καρτών

Εισαγωγή

Στο πρόσφατο παρελθόν τα συστήματα πληρωμής μέσω πιστωτικών καρτών προτιμήθηκαν από τους πελάτες και τους χρήστες του internet. Υπάρχουν διάφορες απαιτήσεις ασφάλειας τις οποίες πρέπει να ικανοποιούν τα συστήματα αυτά. Για παράδειγμα, πρέπει να παρέχεται ένας μηχανισμός που να επικυρώνει τα διάφορα μέρη που εμπλέκονται, όπως τους πελάτες και τους εμπόρους, καθώς και τις τράπεζες που συμμετέχουν. Επιπλέον, πρέπει

να παρέχεται ένας μηχανισμός που να προστατεύει πληροφορίες σχετικές με την πιστωτική κάρτα και την πληρωμή κατά τη μετάδοση μέσω του internet. Επίσης, πρέπει να καθιερωθεί μία διαδικασία που να επιλύει τις διαφορές όσον αφορά στην πληρωμή με πιστωτική κάρτα ανάμεσα στα διάφορα μέρη που εμπλέκονται.

Υπάρχουν πέντε εμπλεκόμενα μέρη σε ένα ασφαλές πρόγραμμα ηλεκτρονικής πληρωμής μέσω πιστωτικής κάρτας:

- Ο κάτοχος πιστωτικής κάρτας
- Ο έμπορος
- Η τράπεζα του εμπόρου
- Το κέντρο διαχείρισης πιστοποιητικών
- Η τράπεζα έκδοσης πιστωτικών καρτών

Ο κάτοχος της πιστωτικής κάρτας χρησιμοποιεί την πιστωτική κάρτα για να αγοράσει αγαθά ή υπηρεσίες από τον έμπορο. Ο έμπορος, με τη σειρά του, αλληλεπιδρά με την τράπεζά του η οποία ονομάζεται τράπεζα του εμπόρου, τράπεζα εγγύησης (acquirer bank) ή απλά εγγυητής (acquirer). Σε ένα πρόγραμμα ηλεκτρονικής πληρωμής μέσω πιστωτικής κάρτας, ο εγγυητής τυπικά αναφέρεται σε έναν οικονομικό οργανισμό, ο οποίος έχει ένα

λογαριασμό με έναν έμπορο και προωθεί σε αυτόν τις εξουσιοδοτήσεις πιστωτικών καρτών και τις αντίστοιχες πληρωμές. Σε αυτή τη ρύθμιση, μία πύλη πληρωμής είναι μία συσκευή την οποία διευθύνει ο εγγυητής προκειμένου να χειριστεί τα εμπορικά μηνύματα πληρωμών. Ένα πολύ σημαντικό μέρος για ένα ασφαλές σύστημα ηλεκτρονικών πληρωμών με πιστωτική κάρτα είναι το κέντρο διαχείρισης πιστοποιητικών (certificate management center), το οποίο εκδίδει και αποσύρει πιστοποιητικά δημοσίων κλειδιών στα εμπλεκόμενα μέλη. Επιπλέον, υπάρχουν συνήθως δύο εμπλεκόμενα δίκτυα σε ‘ένα πρόγραμμα ηλεκτρονικών πληρωμών μέσω πιστωτικών καρτών:

- Ένα δημόσιο δίκτυο, συνήθως το Internet

- Ένα ιδιωτικό δίκτυο, το τραπεζικό δίκτυο, το οποίο ανήκει στην τραπεζική κοινότητα η οποία έχει και την ευθύνη χειρισμού του.

3.9.1Secure Electronic Transaction - SET

Το SET είναι μία ανοιχτή κρυπτογράφηση και ένας προσδιορισμός της ασφάλειας που έχει σχεδιαστεί για την προστασία συναλλαγών με πιστωτικές κάρτες μέσω internet. Η τρέχουσα έκδοση Setv1 για ασφάλεια προβλήθηκε από την Mastercard και την Visa τον Φεβρουάριο του 1996. Πολλές εταιρίες

ασχολήθηκαν με την εξέλιξη της πρωταρχικής περιγραφής του. Ανάμεσα σε αυτές είναι η IBM , Microsoft, Netscape, Terisa και η Verisign.

Το SET δεν είναι από μόνο του ένα σύστημα πληρωμής. Είναι μία σειρά από πρωτόκολλα ασφάλειας και σχημάτων που διευκολύνουν τους χρήστες να χρησιμοποιήσουν το υπάρχων σύστημα πληρωμής με πιστωτικές κάρτες μέσω του διαδικτύου, χρησιμοποιώντας τεχνικές ασφάλειας.

3.9.1.1 Οι απαιτήσεις των επιχειρήσεων για ασφάλεια στην διαδικασία πληρωμής και η χρησιμότητα του SET

1. Παροχή εμπιστοσύνης όσον αφορά το σύστημα πληρωμής και παραγγελία πληροφορίας.

Είναι βασικό να συνειδητοποιήσουν οι χρήστες ότι αυτή η πληροφορία είναι ασφαλής και αποδεκτή μόνο για τον παραλήπτη. Αυτό το απόρρητο που υπάρχει μειώνει τον κίνδυνο της απάτης. Το SET χρησιμοποιεί την κρυπτογράφηση.

2. Παροχή ακεραιότητας για όλα τα μεταδιδόμενα δεδομένα.

Εδώ πρέπει να υπάρχει εγγύηση ότι δεν θα υπάρχουν αλλαγές στο περιεχόμενο κατά την διάρκεια της μεταφοράς ενός Set μηνύματος. Ψηφιακές υπογραφές χρησιμοποιούνται για να αποδείξουν την ακεραιότητα.

3. Παροχή αυθεντικότητας ότι ο κάτοχος μιας πιστωτικής κάρτας είναι ένας νόμιμος χρήστης του λογαριασμού.

Ένας μηχανισμός αντιστοιχεί τον κάτοχο μιας πιστωτικής κάρτας με έναν συγκεκριμένο αριθμό λογαριασμού. Έτσι μειώνεται ο κίνδυνος απάτης και το ολικό κόστος της διαδικασίας που απαιτεί η πληρωμή. Ψηφιακές υπογραφές και πιστοποιητικά χρησιμοποιούνται για να επιβεβαιώσουν ότι ο κάτοχος είναι νόμιμος χρήστης του αξιοποιήσιμου λογαριασμού.

4. Παροχή αυθεντικότητας ότι ένας έμπορος μπορεί να δεχτεί συναλλαγές με πιστωτικές κάρτες.

Οι κάτοχοι πιστωτικής κάρτας έχουν την ανάγκη να γνωρίζουν τους εμπόρους με τους οποίους έρχονται σε επαφή μέσα από ασφαλείς διαδικασίες. Ψηφιακές υπογραφές και πιστοποιητικά χρησιμοποιούνται για άλλη μια φορά και εδώ.

5. Εγγύηση ότι χρησιμοποιούνται οι καλύτερες τεχνικές ασφαλείας και σχεδίασης συστήματος έτσι ώστε να προστατευτούν όλες οι νόμιμες ομάδες που παίρνουν μέρος σε μία ηλεκτρονική συναλλαγή εμπορίου.

Το Set είναι το πιο χαρακτηριστικό παράδειγμα χρησιμοποίησης αλγορίθμων και πρωτοκόλλων που παρέχουν ασφάλεια.

3.9.1.2Τα χαρακτηριστικά του SET

1. Ο λογαριασμός του κατόχου πιστωτικής κάρτας και η πληροφορία για την πληρωμή είναι ασφαλείς καθώς ρέουν στο δίκτυο.

Το SET δεν κάνει γνωστό τον αριθμό πιστωτικής κάρτας του κατόχου στον έμπορο, μόνο η τράπεζα από την οποία εξήλθε ο συγκεκριμένος αριθμός τον γνωρίζει. Εδώ βλέπουμε την χρήση του απόρρητου. Συμβατική κρυπτογράφηση από την DES χρησιμοποιείται για την παροχή εμπιστοσύνης που επιθυμεί ο κάθε χρήστης από το διαδίκτυο στο οποίο έχει πρόσβαση.

2. Η πληροφορία για την πληρωμή που στέλνεται από τον κάτοχο στον έμπορο περιέχει δεδομένα προσωπικά, στοιχεία για τη παραγγελία κ.τ.λ.

Το SET εγγυάται ότι το περιεχόμενο του μηνύματος δεν θα παραποιηθεί κατά την μεταφορά του. Την ακεραιότητα του μηνύματος την παρέχουν οι RSA ψηφιακές υπογραφές που χρησιμοποιούν SHA-1 κωδικούς. Συγκεκριμένα μηνύματα προστατεύονται επίσης από το HMAC χρησιμοποιώντας SHA-1.

3. Το SET δίνει την δυνατότητα στους εμπόρους να επιβεβαιώσουν ότι ένας κάτοχος πιστωτικής κάρτας είναι νόμιμος χρήστης με έγκυρο αριθμό λογαριασμού.

Το SET χρησιμοποιεί X.509v3 ψηφιακά πιστοποιητικά με RSA υπογραφές γι αυτόν τον σκοπό.

4. Το SET παρέχει την ευκολία στους κατόχους πιστωτικής κάρτας να επιβεβαιώσουν ότι ένας έμπορος έχει σχέση με έναν οργανισμό οικονομικής φύσεως, ο οποίος του επιτρέπει να δέχεται κάρτες στις συναλλαγές που κάνει. Το SET χρησιμοποιεί επίσης X.509v3 ψηφιακά πιστοποιητικά και RSA υπογραφές για αυτόν τον λόγο.

<u>Σημείωση</u>

Θα πρέπει να τονίσουμε πως σε αντίθεση με την IP security και τα πρωτόκολλα SSL/ TLS το SET παρέχει μόνο μία επιλογή για κάθε αλγόριθμο κρυπτογράφησης. Αυτό γίνεται κατανοητό γιατί το Set είναι μία μοναδική εφαρμογή με έναν απλό αριθμό απαιτήσεων, ενώ η IP security και τα SSL/ TLS έχουν σαν στόχο να ενισχύσουν έναν μεγάλο αριθμό εφαρμογών.

3.9.2 CyberCash

Το CyberCash ιδρύθηκε για να παρέχει λύσεις λογισμικού και υπηρεσιών σε όλους τους τύπους των οικονομικών συναλλαγών και πληρωμών μέσω internet. Εδώ πρέπει να αναφέρουμε τα CyberCoin της CyberCash και PayNow συστήματα.

Το CyberCash έχει αναπτύξει ένα σύστημα πληρωμών βασισμένο σε πιστωτικές κάρτες για το internet.Το σύστημα αυτόπληρωμής του CyberCash, χρησιμοποιεί ειδικό λογισμικό πορτοφολιού (wallet software) για την πλευρά του πελάτη, ώστε να παρέχεται η δυνατότητα στους πελάτες να πραγματοποιήσουν ασφαλείς αγορές από εμπόρους που συνδέονται με αυτό, χρησιμοποιώντας πιστωτικές κάρτες.

Στο σύστημα πληρωμής CyberCash που δε βασίζεται σε πιστωτικές κάρτες, ο εξυπηρέτης του CyberCash λειτουργεί ως πύλη εξυπηρέτη που συνδέει το πορτοφόλι του πελάτη με το λογισμικό του εμπόρου στην υπάρχουσα οικονομική υποδομή. Έτσι, ο εξυπηρέτης του CyberCash από την μία πλευρά είναι συνδεδεμένος με το internet και από την άλλη με πολλές τράπεζες και τραπεζικά συστήματα συναλλαγών. Τα μηνύματα αγορών που

περιέχουν πληροφορίες για την πιστωτική κάρτα ενός πελάτη προωθούνται μέσω αυτής της πύλης τη στιγμή της αγοράς. Τα αποτελέσματα της συναλλαγής επιστρέφονται στον έμπορο διαμέσου του CyberCash εξυπηρέτη.

3.10 DNSSEC (Domain Name System Security)

Το Domain Name Security Standard είναι ένα σύστημα που σχεδιάστηκε για να προσφέρει ασφάλεια στο Domain Name System Security (DNS). Το DNSSEC δημιουργεί ένα παράλληλο δημόσιο κλειδί υποδομής πάνω στο DNS σύστημα. Κάθε DNS domain καθορίζεται από ένα δημόσιο κλειδί. Ένα τέτοιο δημόσιο κλειδί μπορούμε να το αποκτήσουμε με έναν έμπιστο τρόπο από το εν λόγο domain ή αυτό μπορεί να φορτωθεί από πριν μέσα σε ένα DNS server χρησιμοποιώντας το αρχείο ‘ boot ’ του server. Τέλος το DNSSEC αναγνωρίζεται για τις ασφαλής ανανεώσεις πληροφοριών στους DNS servers, κάνοντας το ιδανικό για απομακρυσμένη διαχείριση.

3.11 IPsec και IPv6

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

Θα πρέπει να σημειωθεί πως το Ipsec δεν προσφέρεται για την ακεραιότητα, την αναγνώριση ταυτότητας, 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 (Virtual Private Networks –VPNs) μέσω του internet. Αλλά το Ipsec έχει την ικανότητα να παρέχει αναγνώριση ταυτότητας, ακεραιότητας, και προαιρετικά την εμπιστοσύνη των δεδομένων για όλες τις επικοινωνίες που παίρνουν μέρος πάνω στο internet, έχοντας ευρέως διαδεδομένες εφαρμογές του πρωτοκόλλου και επίσης την άδεια χρήσης αυτών από τις κυβερνήσεις.

3.12 Kerberos

Ο Kerberos είναι ένα σύστημα ασφάλειας δικτύου που αναπτύχθηκε από το MIT και χρησιμοποιήθηκε από την αρχή στις Ηνωμένες Πολιτείες. Οι εκδόσεις v.1 έως v.3 του Kerberos χρησιμοποιούνται μόνον εσωτερικά στο MIT, αλλά η v.4 διατέθηκε δημόσια και χρησιμοποιήθηκε ευρύτατα.

Αυτό λοιπόν το σύστημα είναι βασισμένο 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 άλλο.

Ο Kerberos είναι ένα δύσκολο σύστημα στο να διαμορφωθεί και να διαχειριστεί. Για να λειτουργήσει ένα τέτοιο σύστημα θα πρέπει η κάθε μεριά 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 αλλάζεται.

3.13 PGP (Pretty Good Privacy)

Το PGP είναι το πρώτο πρόγραμμα κρυπτογράφησης δημόσιου κλειδιού, γραμμένο από τον Phil Zimmerman που κυκλοφόρησε στο internet τον Ιούνιο toy 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.

Το PGP είναι ένα κρυπτογραφικό σύστημα διασταύρωσης που χρησιμοποιεί τον RSA αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού για την διαχείριση των κλειδιών και τον IDEA συμμετρικό αλγόριθμο για την κύρια κρυπτογράφηση των δεδομένων.

Το PGP προσφέρει εμπιστευτικότητα, εξαιτίας του ο κρυπτογραφικός αλγόριθμος που χρησιμοποιεί είναι ο IDEA. Προσφέρει ακεραιότητα εξαιτίας του ότι, η συνάρτηση αποσύνθεσης που χρησιμοποιεί είναι η MD5. Προσφέρει αναγνώριση γνησιότητας με την χρήση του δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

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

3.14 S/MIME (Multipurpose Internet Mail Extensions)

Το MIME χρησιμοποιείται για αποστολή αρχείων με binary attachments μέσω του internet. Το Secure /MIME είναι μία επέκταση του MIME standard για τη 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.

ΚΕΦΑΛΑΙΟ 4

ΑΝΑΧΩΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

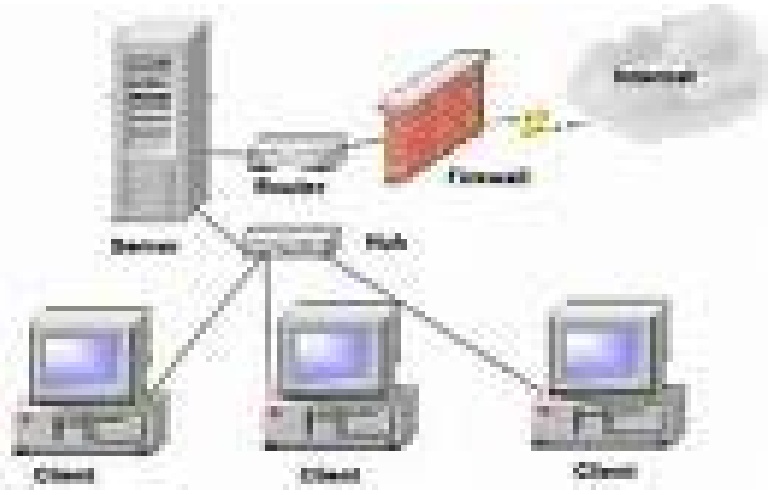
Εικόνα 4.1

4.1 Ορισμός

Πολλοί οργανισμοί και επιχειρήσεις έχουν συνδέσει τα εσωτερικά τους δίκτυα με το internet , ενδιαφερόμενοι για λήψη χρήσιμων πληροφοριών από τον παγκόσμιο ιστό , αλλά και προσανατολισμένοι στις δυνατότητες του ηλεκτρονικού επιχειρείν και των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Με τον τρόπο αυτό, όμως , τα εσωτερικά τους συστήματα γίνονται ευπρόσβλητα σε κακόβουλη χρήση και επίθεση από εξωτερικούς χρήστες. Απαραίτητη φραγή της εισερχόμενης επιβουλής συνιστά ένα ανάχωμα ασφάλειας (firewall) , δηλαδή μια διάταξη εξειδικευμένων μηχανισμών ασφάλειας που ελέγχει την πρόσβαση και τη μετακίνηση της πληροφορίας μεταξύ ενός δικτύου που εμπιστευόμαστε και ενός δικτύου που δεν εμπιστευόμαστε απαραίτητα .Πιο συγκεκριμένα:

- Με τον όρο ανάχωμα ασφάλειας (firewall) εννοούμε συστήματα τα οποία υλοποιούν τους κανόνες μιας πολιτικής ασφάλειας μεταξύ δύο δικτύων . Τις περισσότερες φορές το ένα από τα δύο δίκτυα είναι το internet , αλλά ένα ανάχωμα ασφάλειας , στη γενική περίπτωση , μπορεί να τοποθετηθεί και μεταξύ δύο τυχαίων δικτύων υπολογιστών.

Ο ρόλος του αναχώματος ασφάλειας μπορεί να είναι τόσο η αποτροπή μη εξουσιοδοτημένων προσβάσεων σε μια ασφαλή περιοχή, όσο και η αποτροπή μη εξουσιοδοτημένης εξόδου πληροφορίας από μια περιοχή. Μπορεί δηλαδή να λειτουργήσει ως θύρα ελέγχου της κίνησης και προς τις δύο κατευθύνσεις.



Εικόνα 4.2

4.2 Δυνατότητες ενός αναχώματος ασφαλείας

Η λειτουργικότητα των αναχωμάτων ασφάλειας εκτείνεται στα ακόλουθα:

- Το ανάχωμα ασφάλειας αποτελεί το επίκεντρο των αποφάσεων που σχετίζονται με θέματα ασφάλειας

Το ανάχωμα ασφάλειας επιτρέπει στο διαχειριστή του δικτύου να ορίσει ένα κεντρικό σημείο ελέγχου (choke point) , το οποίο αποτρέπει την προσπέλαση μη εξουσιοδοτημένων χρηστών στο προστατευμένο δίκτυο. Το ανάχωμα ασφάλειας απλοποιεί τη διαχείριση ασφάλειας, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο, το οποίο συνδέει τον οργανισμό με τον εξωτερικό κόσμο και όχι στον κάθε υπολογιστή χωριστά μέσα σε ολόκληρο το δίκτυο.

- Το ανάχωμα ασφάλειας εφαρμόζει έλεγχο προσπέλασης (access control) από και προς το δίκτυο , υλοποιώντας και υποστηρίζοντας την πολιτική ασφάλειας του οργανισμού.

Η μια από τις δυνατές πολιτικές ενός αναχώματος ασφάλειας βασίζεται ακριβώς στην άρνηση σε οποιαδήποτε πρόσβαση η οποία δεν έχει σαφώς επιτραπεί. Χωρίς το ανάχωμα ασφάλειας, κάθε υπολογιστής στο εσωτερικό δίκτυο ενός οργανισμού είναι εκτεθειμένος σε προσβολές από άλλους υπολογιστές του internet. Αυτό σημαίνει ότι η όλη ασφάλεια του εσωτερικού δικτύου εξαρτάται από το πόσο ισχυρά είναι τα χαρακτηριστικά ασφάλειας κάθε υπολογιστή του εσωτερικού δικτύου και άρα είναι τόσο ισχυρή όσο το πιο αδύνατο σύστημα.

- Το ανάχωμα ασφάλειας προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο (network activity logging)

Εφόσον όλη η κίνηση διέρχεται από το ανάχωμα ασφάλειας, αυτό μπορεί να αποτελέσει ένα καλό σημείο για τη συλλογή πληροφορίας σχετικά με τη χρήση τόσο των συστημάτων όσο και του δικτύου. Ένα αξιόπιστο ανάχωμα ασφάλειας καταγράφει όλες τις επιτρεπόμενες και μη δραστηριότητες σε ένα αρχείο συμβάντων (activity log – audit log), το οποίο είναι διαθέσιμο στο διαχειριστή του δικτύου. Μερικά αναχώματα ασφάλειας επίσης, προσφέρουν και μηχανισμούς συναγερμού (alarms) ώστε να βοηθήσουν στον έγκαιρο εντοπισμό μιας ύποπτης δραστηριότητας τη στιγμή που αυτή λαμβάνει χώρα και στην άμεση πληροφόρηση του διαχειριστή.

- Το ανάχωμα ασφάλειας έχει τη δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης.

Το ανάχωμα ασφάλειας έχει τη δυνατότητα να ενσωματώνει το NAT (Network Address Translator) , το οποίο μεταφράζει τις εσωτερικές διευθύνσεις σε πραγματικές και να αντιμετωπίζει το πρόβλημα της έλλειψης ή της αλλαγής διευθύνσεων στην περίπτωση που ένας οργανισμός αλλάζει παροχέα υπηρεσιών internet. Και αυτό γιατί έχει διαπιστωθεί πως τα τελευταία χρόνια το internet αντιμετωπίζει πρόβλημα διαθέσιμων IP διευθύνσεων, με αποτέλεσμα οργανισμοί που επιθυμούν να αποκτήσουν αρκετές πραγματικές IP , να μην μπορούν.

- Το ανάχωμα ασφάλειας προστατεύει τα διαφορετικά δίκτυα εντός του ίδιοι του οργανισμού

Το ανάχωμα ασφάλειας χρησιμοποιείται για την προστασία ευαίσθητων περιοχών του δικτύου απέναντι στην πρόσβαση από άλλα σημεία μέσα στο ίδιο δίκτυο. Πολλές φορές το ανάχωμα χρησιμοποιείται για να διαχωρίσει ένα τμήμα του δικτύου από κάποιο άλλο .Έτσι αποφεύγεται εξάπλωση τυχόν προβλήματος σε ολόκληρο το δίκτυο την στιγμή που ξεκίνησε από ένα συγκεκριμένο τμήμα.

4.3 Αδυναμίες ενός αναχώματος ασφαλείας

Ένα ανάχωμα ασφάλειας προστατεύει το δίκτυο από πιθανές απειλές αλλά δεν εγγυάται ολοκληρωμένη ασφάλεια. Αυτό έχει σαν αποτέλεσμα να απαιτούνται άλλες ενέργειες όπως , εκπαίδευση των χρηστών (user education) στα πλαίσια του συνολικού πλάνου ασφάλειας (security plan) , μηχανισμοί

φυσικής προστασίας (physical security) , ενσωμάτωση ασφάλειας σε επίπεδο εξυπηρέτη (server security).

Πιο συγκεκριμένα οι αδυναμίες που παρουσιάζει ένα ανάχωμα είναι οι εξής :

- Το ανάχωμα ασφάλειας δεν μπορεί να προστατεύσει από προγράμματα – ιούς

Ανακριβή δεδομένα και ιομορφικό λογισμικό (viral software) δεν μπορούν να ελεγχθούν. Και αυτό γιατί τα αναχώματα ασφάλειας ανιχνεύουν την κίνηση που έχει να κάνει με τις διευθύνσεις και τις θύρες πηγής και προορισμού (source and destination addresses and port numbers) αλλά δεν εξετάζουν τις λεπτομέρειες των δεδομένων. Έτσι σε κάθε προσωπικό υπολογιστή κάθε οργανισμού είναι απαραίτητο να χρησιμοποιείται λογισμικό αντιμετώπισης ιομορφών και κυρίως στους εξυπηρέτες του.

- Το ανάχωμα ασφάλειας δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού

Οι εσωτερικοί χρήστες μπορούν να υποκλέψουν και να καταστρέψουν υλικό και λογισμικό καθώς και να τροποποιήσουν προγράμματα χωρίς να έρθουν σε επαφή με το ανάχωμα ασφάλειας. Το ανάχωμα δεν είναι σε θέση να προστατεύσει τον οργανισμό από επιθέσεις όταν υπάλληλοι πείθονται από κακόβουλα άτομα και τους παραδίνουν άδεια εισόδου στο σύστημα προσποιούμενοι ίσως το διαχειριστή του δικτύου (social engineering attacks) . Σε αυτήν την περίπτωση η ενημέρωση είναι απαραίτητη για τις διάφορες

απειλές . Οι χρήστες πρέπει να κατανοήσουν την σημασία της διατήρησης της μυστικότητας του συνθηματικού τους και της περιοδικής αλλαγής του διότι αν διαρρεύσει η πρόσβαση στο σύστημα θα είναι εύκολη. Τέλος πρέπει να σημειωθεί πως όταν έχουμε να κάνουμε με τέτοιες απειλές απατούνται εσωτερικά μέτρα ασφάλειας όπως ασφάλεια σε επίπεδο ξενιστή (host security) και εκπαίδευση χρηστών (user education).

- Το ανάχωμα δεν μπορεί να προστατεύσει από συνδέσεις οι οποίες δε διέρχονται από αυτό

Ένα ανάχωμα προστατεύει ένα περιβάλλον μόνον αν ελέγχει ολόκληρη την περίμετρο του περιβάλλοντος. Συνδέσεις που δε διέρχονται από το σημείο που βρίσκεται το ανάχωμα ασφάλειας δεν μπορούν να διασφαλιστούν από αυτό. Εν ολίγοις ένα ανάχωμα δεν μπορεί να αντιμετωπίσει επιθέσεις που δε σχετίζονται με αυτό, ελέγχει αποτελεσματικά μόνο την κίνηση που διέρχεται μέσα από αυτό.

- Το ανάχωμα ασφάλειας δεν μπορεί να προστατέψει τον οργανισμό απέναντι σε επιθέσεις συσχετιζόμενες με δεδομένα (data driven attacks)

Αυτές οι επιθέσεις κάνουν αισθητή την παρουσία τους όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρέτες του οργανισμού και εξαπολύουν επίθεση εναντίον του συστήματος. Αυτό πραγματοποιείται είτε διαμέσου του ηλεκτρονικού ταχυδρομείου , είτε διαμέσου της αντιγραφής από δισκέτα για παράδειγμα. Με αποτέλεσμα μια τέτοιου είδους επίθεση να οδηγεί στη μεταβολή των αρχείων που σχετίζονται

με τα προνόμια προσπέλασης ενός εξυπηρέτη , και τότε η πρόσβαση στο σύστημα καθίσταται εύκολη από έναν μη εξουσιοδοτημένο χρήστη.

- Το ανάχωμα ασφάλειας δεν μπορεί να προστατεύσει τον οργανισμό από απειλές άγνωστου τύπου

Το ανάχωμα ασφάλειας μπορεί να προστατεύσει το δίκτυο από γνωστές απειλές που έχουν αντιμετωπιστεί στο παρελθόν , εφόσον βέβαια διαθέτει την απαραίτητη τεχνολογία , αλλά δεν μπορεί να ανταποκριθεί αυτομάτως σε νέες απειλές οι οποίες προκύπτουν κατά καιρούς.

- Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του αναχώματος ασφάλειας

Ένα ανάχωμα το οποίο έχει ρυθμιστεί με πολύ αυστηρό τρόπο είναι δυνατόν να προκαλέσει δυσαρέσκεια στους χρήστες , και αυτό εξαιτίας των πολλών ελέγχων , των πολλαπλών επιπέδων ασφάλειας και κατά συνέπεια της συνολικής ελαττωμένης φιλικότητας και μειωμένης ευχρηστίας που εισάγει. Ένα τέτοιο ανάχωμα μπορεί επίσης να εμποδίσει την διαδικτύωση.

4.4 Εγκατάσταση ενός αναχώματος ασφαλείας

Η εγκατάσταση ενός αναχώματος ασφάλειας αποτελεί σημαντική σχεδιαστική απόφαση για τους εξής λόγους :

- Κατά την εγκατάσταση ενός αναχώματος ασφάλειας , η άρνηση παροχής υπηρεσιών για περιορισμένο χρονικό διάστημα μπορεί να προκαλέσει προβλήματα.

- Η εγκατάσταση ενός αναχώματος ασφάλειας επιφέρει καθυστέρηση στο χρόνο απόκρισης των προγραμμάτων που υλοποιούν τις υπηρεσίες που παρέχει η ιστοθέση.

- Η συνεχής συντήρηση και ενημέρωση ενός αναχώματος ασφάλειας είναι απαραίτητη, καθώς προστίθενται νέες υπηρεσίες και απαξιώνονται παλαιότερες .

- Όλες ανεξαιρέτως οι υπηρεσίες δεν υλοποιούνται διαμέσου του αναχώματος ασφάλειας με διαφανή (transparent) τρόπο ως προς το χρήστη. Αυτό έχει σαν αποτέλεσμα η εγκατάσταση του αναχώματος να επιφέρει αναστάτωση στο προσωπικό του οργανισμού μέχρι αυτό να εξοικειωθεί με τις ήδη υπάρχουσες υπηρεσίες , που όμως τώρα θα υλοποιούνται με διαφορετικό τρόπο.

Συμπεραίνουμε λοιπόν πως η εγκατάσταση ενός αναχώματος ασφάλειας δεν πρέπει να αντιμετωπίζεται ως ο μοναδικός τρόπος εξασφάλισης της γενικότερης πολιτικής ασφάλειας της ιστοθέσης αλλά να αποτελεί μια συνιστώσα στα πλαίσια αυτής της πολιτικής. Όταν ληφθεί απόφαση για την εγκατάσταση ενός αναχώματος ασφάλειας , υπάρχουν ορισμένα σχεδιαστικά ζητήματα τα οποία θα πρέπει να αντιμετωπιστούν. Τα ζητήματα αυτά περιλαμβάνουν τα εξής :

- Εκτίμηση του κινδύνου (risk assessment)

Απαιτείται , η εκτίμηση της επίδρασης που θα έχει η εισβολή μιας εξωτερικής οντότητας που αποκτά πρόσβαση στο δίκτυο γιαυτό η σχεδίαση του αναχώματος ασφάλειας θα πρέπει να γίνεται με τέτοιο τρόπο ώστε να προστατεύονται διαφορετικά ζώνες διαφορετικού κινδύνου.

- Εκτίμηση των απειλών (threat assessment)

Ένα πρόκειται για διασύνδεση με ένα δημόσιο δίκτυο , υπάρχουν σοβαρές απειλές. Εάν όμως πρόκειται για διασύνδεση με το εξωτερικό τμήμα ενός οργανισμού, το επίπεδο των απειλών είναι χαμηλό εφόσον βέβαια έχουμε να κάνουμε με έμπιστους συνεργάτες. Από αυτά καταλαβαίνουμε πως απαιτείται η εκτίμηση των απειλών κατά την διασύνδεση του δικτύου ενός οργανισμού με άλλα δίκτυα.

- Εκτίμηση του κόστους (cost assessment)

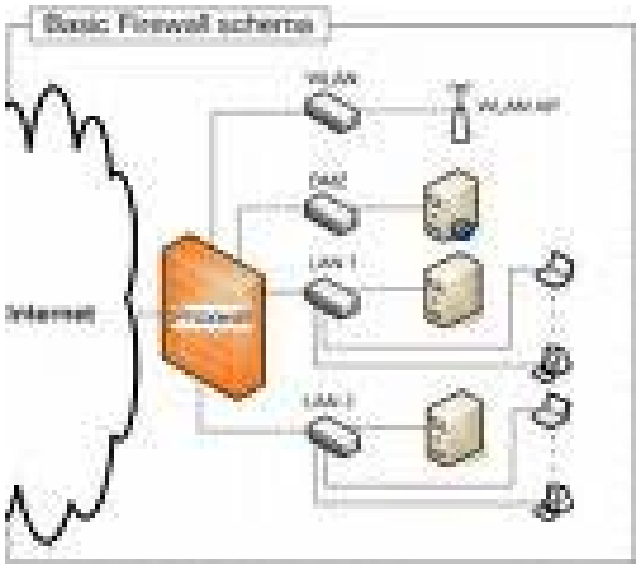
Προκειμένου να ληφθεί ορθή απόφαση , είτε για αγορά ενός εμπορικού προϊόντος , είτε για κατασκευή αναχώματος ασφάλειας από τον ίδιο τον οργανισμό θα πρέπει να υπολογιστεί ακριβώς το κόστος υλοποίησης ενός αναχώματος ασφάλειας. Απαραίτητο είναι επίσης , να εκτιμηθεί και το κόστος της μετέπειτα διαρκούς υποστήριξης του αναχώματος ασφάλειας.

- Τύπος του αναχώματος ασφάλειας (firewall type)

Θα πρέπει να επιλεγεί εκείνος ο τύπος αναχώματος που ικανοποιεί τις ανάγκες και τις απαιτήσεις του εκάστοτε οργανισμού.

- Χρηστικότητα (usability) του αναχώματος ασφάλειας

Πρέπει να γίνουν συμβιβασμοί μεταξύ χρηστικότητας και ασφάλειας ώστε να μπορούν οι χρήστες να συνδεθούν στο δίκτυο του οργανισμού μέσω modem για παράδειγμα .Αυτό δεν θα συνέβαινε εάν το ανάχωμα ασφάλειας είναι προσανατολισμένο στην παρεμπόδιση των εξωτερικών εισβολών. Ο πιο ασφαλής τρόπος είναι ένα δίκτυο να μην συνδέεται με κανένα άλλο δίκτυο είναι προφανές όμως πως ένα τέτοιο δίκτυο δεν θα ήταν καθόλου αποδοτικό.



Εικόνα 4.3

4.5 Απαιτήσεις σχεδίασης αναχώματος ασφάλειας

Οι λειτουργικές απαιτήσεις σχεδίασης αναχώματος ασφάλειας είναι οι ακόλουθες :

- Ένας μηχανισμός όπως θα μπορούσε να θεωρηθεί το ανάχωμα ασφάλειας , θα πρέπει να είναι αδιάβλητος (tamperproof).Το ανάχωμα εγκαθίσταται χωρίς πολλές λειτουργίες χρήστη , με απευθείας σύνδεση προς τα εξωτερικά αλλά και τα εσωτερικά δίκτυα, δηλαδή εγκαθίσταται σε ξεχωριστό υπολογιστικό σύστημα.

- Να είναι απλός και μικρός σε μέγεθος , ώστε να μπορεί να αναλυθεί. Στους σχεδιαστές αναχωμάτων ασφάλειας συνίσταται η απλή και όσο το δυνατό μικρή σε μέγεθος υλοποίησης τους

- Να αναμειγνύεται σε οποιαδήποτε συνομιλία. Η σωστή τοποθέτηση του αναχώματος ασφάλειας είναι εκείνη που μπορεί να μας εξασφαλίσει ότι όλη η κίνηση θα περνά μέσα από αυτή.

4.6 Πολιτική σχεδίασης αναχώματος ασφάλειας

Από τα προηγούμενα γίνεται κατανοητό ότι, το ανάχωμα ασφάλειας αποτελεί μια φιλοσοφία ασφάλειας και βοηθά στην υλοποίηση μιας ευρύτερης πολιτικής ασφάλειας που καθορίζει τις υπηρεσίες και την πολιτική προσπέλασης σε ένα δίκτυο. Πρόκειται , δηλαδή , για ένα ή περισσότερα συστήματα ή δρομολογητές σε συνδυασμό με άλλα μέτρα ασφάλειας , όπως ,για παράδειγμα , εξειδικευμένους τρόπους αυθεντικοποίησης αντί για στατικά συνθηματικά. Υπάρχουν δύο επίπεδα της πολιτικής ασφάλειας ενός δικτύου τα οποία επηρεάζουν άμεσα τη σχεδίαση , την εγκατάσταση και τη χρήση ενός αναχώματος ασφάλειας .

- Πολιτική Υπηρεσίας Πρόσβασης στο Δίκτυο (Network Service Access Policy)

Αυτού του είδους η πολιτική, προσδιορίζει εκείνες τις υπηρεσίες που θα επιτρέπονται ή ρητά θα απαγορεύονται από το δίκτυο , καθώς και τον τρόπο με τον οποίο αυτές οι υπηρεσίες θα χρησιμοποιούνται. Τέλος καθορίζει τις συνθήκες υπό τις οποίες θα επιτρέπονται εξαιρέσεις σ αυτή την ίδια την πολιτική. Πρόκειται για πολιτική υψηλού επιπέδου.

- Πολιτική Σχεδίασης του αναχώματος ασφάλειας (Firewall Design Policy)

Αυτή η πολιτική περιγράφει τους τρόπους με τους οποίους το ανάχωμα ασφάλειας θα επιβάλλει περιορισμό της πρόσβασης και φιλτράρισμα των υπηρεσιών , κατά τον τρόπο που αυτά έχουν ρητά διατυπωθεί στην Πολιτική Υπηρεσίας Πρόσβασης στο Δίκτυο. Γενικά τα αναχώματα ασφάλειας υλοποιούν μία από τις δύο παρακάτω βασικές πολιτικές σχεδίασης που είναι οι εξής :

- Πολιτική προκαθορισμένης άδειας χρήσης (Default permit stance): Επιτρέπεται κάθε υπηρεσία, εκτός και αν έχει ρητά απαγορευθεί.

- Πολιτική προκαθορισμένης απαγόρευσης χρήσης (Default deny stance): Απαγορεύεται κάθε υπηρεσία, εκτός και αν έχει ρητά επιτραπεί.

Για να οδηγηθεί μια επιχείρηση σε μια πολιτική σχεδίασης του αναχώματος ασφάλειας και, τελικά, σε ένα ολοκληρωμένο σύστημα που υλοποιεί την πολιτική αυτή, καλό θα ήταν να ξεκινήσει από την πολιτική προκαθορισμένης απαγόρευσης χρήσης. Μετέπειτα ο σχεδιαστής ασφάλειας πρέπει να κατανοήσει και να καταγράψει τα εξής:

- Ποιες υπηρεσίες του Internet σχεδιάζει ο οργανισμός να χρησιμοποιήσει (π.χ. Telnet, ftp).

- Τι επιπρόσθετες ανάγκες και υπηρεσίες (π.χ. κρυπτογραφία) μπορούν να υποστηριχτούν.

- Πως θα γίνεται η χρήση των υπηρεσιών (π.χ. σε τοπική βάση, διαμέσου του internet, με χρήση dial-up υπηρεσίας από το σπίτι ή από απομακρυσμένες θέσεις).

- Τι κίνδυνοι παραμονεύουν αν παρασχεθούν αυτές οι υπηρεσίες με τους συγκεκριμένους τρόπους πρόσβασης.

- Ποιο είναι το κόστος, σε όρους συντηρησιμότητας και επίδρασης στη λειτουργικότητα του δικτύου, της παροχής προστασίας διαμέσου του αναχώματος ασφάλειας.

- Πως προσδιορίζεται η σχέση που συνδέει την ασφάλεια με τη λειτουργικότητα. Σε περίπτωση σύγκρουσης, σε ποια από τις δύο έννοιες δίνεται προτεραιότητα.

4.7 Εγκατάσταση

Η εγκατάσταση ενός αναχώματος ασφάλειας περιλαμβάνει σειρά διαδοχικά εκτελούμενων φάσεων. Αυτές, σε μία τυπική περίπτωση εγκατάστασης περιλαμβάνουν:

- Απόκτηση υλικού και λογισμικού
- Απόκτηση τεκμηρίωσης, εκπαίδευσης και υποστήριξης
- Εγκατάσταση υλικού και λογισμικού
- Ρύθμιση της δρομολόγησης
- Ρύθμιση των κανόνων φιλτραρίσματος πακέτων
- Ρύθμιση μηχανισμών καταγραφής και έγκυρης προειδοποίησης
- Δοκιμαστικός έλεγχος του συστήματος
- Εγκατάσταση

ΚΕΦΑΛΑΙΟ 5

ΨΗΦΙΑΚΕΣ ΤΕΧΝΙΚΕΣ ΑΝΑΓΝΩΡΙΣΗΣ ΤΑΥΤΟΤΗΤΑΣ

5.1 Αναγνώριση ταυτότητας

Η αναγνώριση ταυτότητας είναι ένα απαραίτητο στοιχείο της σημερινής ζωής, αλλά και της μελλοντικής επίσης. Μεγάλοι οργανισμοί χρησιμοποιούν ειδικά διακριτικά σήματα (κονκάρδες) αναγνώρισης ταυτότητας για τους εργαζομένους, για να βοηθούν τους φύλακες στο να αποφασίζουν ποιους θα αφήνουν να μπαίνουν στα κτίρια και ποιοι θα μένουν έξω. Κυβερνήσεις χρησιμοποιούν διαφορετικά είδη συστημάτων για να καθορίσουν την

ταυτότητα των χρηστών τους, και για να ελέγχουν την πρόσβαση των πληροφοριών τους και των υπηρεσιών τους.

5.1.1 Συστήματα αναγνώρισης ταυτότητας βασισμένα σε πιστοποιητικά ιδιότητας.

Ένας αποδεδειγμένος τρόπος να αποδεικνύουμε την ταυτότητα μας στον φυσικό κόσμο είναι η μεταφορά πιστοποιητικών ιδιότητας από μια έμπιστη αρχή. Πιστοποιητικά ιδιότητας είναι ένα διαβατήριο, μια αστυνομική ταυτότητα , ένα δίπλωμα αυτοκινήτου, ακόμα και μια κάρτα μέλους ενός γυμναστηρίου, τα οποία πιστοποιούν την ταυτότητα μας.

Τα καλά πιστοποιητικά ιδιότητας είναι κατασκευασμένα με κατάλληλο τρόπο ώστε να μην είναι εύκολη η μεταποίηση των στοιχείων τους (tamper-proof), έτσι ώστε να μην μπορεί ο ιδιοκτήτης να τα ανταλλάξει με κάποιον άλλο. Επίσης θα πρέπει να μην είναι δυνατόν να πλαστογραφηθούν (forgery-proof), έτσι ώστε να μην εκδίδονται από κανέναν άλλον εκτός από τις νόμιμες αρμόδιες αρχές. Για παράδειγμα η αστυνομική ταυτότητα πρέπει να εκδίδεται μόνο από τις αστυνομικές αρχές και δεν μπορεί να την χρησιμοποιήσει άλλος εκτός από τον νόμιμο κάτοχο της.

5.1.2 Τεχνικές αναγνώρισης ταυτότητας στους Η/Υ

Οι προσωπικοί υπολογιστές δεν συνηθίζεται να αναγνωρίζουν την ταυτότητα των χρηστών τους. Τα παραδοσιακά PC δίνουν πλήρη πρόσβαση σε κάθε πρόσωπο που μπορεί να χειριστεί το πληκτρολόγιο. Γι αυτό το λόγο

ονομάζονται και προσωπικοί υπολογιστές επειδή είναι φτιαγμένοι να μην μοιράζονται με διαφορετικούς χρήστες. Αλλά αυτή την εποχή που ένας προσωπικός υπολογιστής μπορεί να προσεγγιστεί από ένα δίκτυο, ή όταν ο υπολογιστής περιέχει ευαίσθητες πληροφορίες
που ίσως μοιράζονται από μια ομάδα προσώπων, τότε είναι απαραίτητη η χρήση αναγνώρισης της ταυτότητας των χρηστών για να αποκτήσουν το δικαίωμα των υπηρεσιών του υπολογιστή.

Πολλοί χρήστες υπολογιστών ήδη έχουν υπό την κατοχή τους πολλούς τύπους ID. Γιατί απλά δεν τους χρησιμοποιούν; ή γιατί ο υπολογιστής δεν αναγνωρίζει τα χαρακτηριστικά του προσώπου μας για να αποφασίσει ποιοι είμαστε.

Δυστυχώς, οι περισσότεροι υπολογιστές δεν μπορούν να κοιτάξουν το πρόσωπο μας, και μετά με μια βιαστική ματιά στην φωτογραφία της αστυνομικής μας ταυτότητας να αποφασίσουν αν πρέπει να μας επιτραπεί η είσοδος ή όχι. Διαδικασία που κάνει με ευκολία κάθε δημόσιος υπάλληλος όπου :

- Οι περισσότεροι υπολογιστές δεν έχουν κάμερες

- Ακόμα και οι υπολογιστές που διαθέτουν κάμερες δεν έχουν το κατάλληλο λογισμικό για να τους επιτρέψει να αναγνωρίσουν την ταυτότητα ενός ανθρώπου με αξιοπιστία.

- Ακόμα και οι υπολογιστές που μπορούν να αναγνωρίσουν την ταυτότητα ανθρώπων από εικόνες βίντεο, δεν έχουν την «κοινή λογική» για να ξέρουν αν κοιτούν σε μια εικόνα βίντεο (πραγματικού χρόνου) του προσώπου, ή αν κοιτούν σε μια εικόνα βιντεοταινίας του προσώπου που έχει αντιγραφθεί προηγουμένως.

- Και εάν ακόμη είχαν κοινή λογική, δεν θα είχαν τα χέρια, δάχτυλα, και ούτω καθ' εξής για να κοιτάξουν την αστυνομική ταυτότητα του προσώπου και να αποφασίσουν εάν είναι αληθινή ή απομίμηση.

Αν και υπάρχει μια συνεχής προσπάθεια έρευνας για την χρήση των φυσικών χαρακτηριστικών όπως είναι το ανθρώπινο πρόσωπο, ή η φωνή για την αναγνώριση της ταυτότητας, πολύ ποιο απλά και φθηνότερα συστήματα χρησιμοποιούνται εδώ και χρόνια. Αλλά υπάρχει μια μικρή διαφορά ανάμεσα σε αυτά τα συστήματα των υπολογιστών και στα συστήματα αναγνώρισης ταυτότητας που βασίζονται σε έγγραφα στον φυσικό μας κόσμο. Τα περισσότερα συστήματα αναγνώρισης ταυτότητας στους υπολογιστές σχεδιάζονται για να μπορεί ο υπολογιστής να καθορίσει εάν το πρόσωπο που κάθεται στο πληκτρολόγιο είναι το ίδιο με αυτοί που καθόταν εκεί την προηγούμενη μέρα, παρά για να αποδείξει ότι το πρόσωπο αυτό είναι κάποιο συγκεκριμένο πρόσωπο. Αυτά τα συστήματα νοιάζονται περισσότερο για το αδιάκοπο της αναγνώρισης ταυτότητας. Μια εταιρία, η Miros, έχει αναπτύξει ένα σύστημα ελέγχου πρόσβασης στο web που χρησιμοποιεί μια μικρή βιντεοκάμερα για να παρέχει την web πρόσβαση με ασφάλεια.

5.1.2.1 Συστήματα βασισμένα σε password:

Τα πρώτα ψηφιακά συστήματα αναγνώρισης της ταυτότητας του χρήστη ήταν βασισμένα σε συνθηματικές λέξεις (password). Κάθε χρήστης ενός συστήματος έχει το όνομα του (username) και την συνθηματική λέξη του. Για να αποδείξεις την ταυτότητα σου στον υπολογιστή, απλά εισάγεις το password. Εάν το password που εισάγεις ταιριάζει με αυτό που είναι αποθηκευμένο στον υπολογιστή, τότε πρέπει να είσαι αυτός που ισχυρίζεσαι ότι είσαι.

Επειδή είναι απλά στην χρήση, γνωστά, και δεν απαιτούν ειδικό hardware, τα passwords συνεχίζουν να είναι τα ποιο δημοφιλή συστήματα αναγνώρισης ταυτότητας που χρησιμοποιούνται σε υπολογιστές σήμερα στον κόσμο. Δυστυχώς υπάρχουν πολλά προβλήματα χρησιμοποιώντας passwords για την αναγνώριση της ταυτότητας. Σχεδόν όλα περιστρέφονται γύρω από πέντε παράγοντες, οι οποίοι είναι οι εξής:

I. Ο υπολογιστής πρέπει να έχει το password σου μέσα σε ένα αρχείο πριν προσπαθήσει να αποδείξει την ταυτότητα σου.

II. Οι άνθρωποι ξεχνούν τα password.

III. Οι άνθρωποι διαλέγουν εύκολα και αδύναμα passwords.

IV. Το password σου όταν το στέλνεις στον Η/Υ μπορεί να υποκλαπεί.

V. Οι άνθρωποι λένε τα δικά τους passwords σε φίλους και συνεργάτες.

5.1.2.2 Φυσικά κουπόνια (tokens):

Ένας άλλος τρόπος με τον οποίο οι άνθρωποι μπορούν να αποδείξουν την ταυτότητά τους είναι μέσω της χρήσης ενός κουπονιού – φυσικού αντικειμένου που μεταφέρεις μαζί σου, το οποίο με κάποιο τρόπο αποδεικνύει την ταυτότητα σου και σου παρέχει πρόσβαση.

Οι κάρτες πρόσβασης είναι τυπικά κουπόνια που χρησιμοποιούνται για να αποδεικνύουν την ταυτότητα στον επιχειρηματικό κόσμο. Για να ανοίξεις μια πόρτα απλά περνάς μια κάρτα στον ειδικό αναγνώστη. Κάθε κάρτα έχει έναν μοναδικό αριθμό. Το σύστημα από την άλλη, έχει μια λίστα των καρτών που είναι εξουσιοδοτημένες να ανοίγουν τις κατάλληλες πόρτες στην κατάλληλη χρονική στιγμή. Με σκοπό την αποτελεσματικότητα του συστήματος, οι κάρτες δεν πρέπει να δανείζονται σε άλλους.

Τα φυσικά κουπόνια έχουν και αυτά κάποια προβλήματα όπου είναι τα εξής:

I. Αν ένα πρόσωπο χάσει το κουπόνι, δεν μπορεί να μπει στην περιορισμένη περιοχή, αν και η ταυτότητα του δεν αλλάξει.

II. Δεν μπορούν να αποδείξουν ποιος πραγματικά είσαι. Όποιος και να έχει στην ιδιοκτησία του ένα κουπόνι μπορεί να έχει πρόσβαση σε μια περιορισμένη περιοχή.

III. Κάποια από τα κουπόνια είναι εύκολο να πλαστογραφηθούν.

Επομένως τα συστήματα που βασίζονται σε κουπόνια δεν αναγνωρίζουν την ταυτότητα ενός προσώπου αλλά ενός κουπονιού. Για το λόγο αυτό, τα συστήματα αυτά συνδυάζονται με συστήματα που βασίζονται σε passwords. Για να αποκτήσεις πρόσβαση σε ένα δωμάτιο ή έναν Η/Υ, χρειάζεται να παρουσιάσεις και ένα κουπόνι και να εισάγεις το password. Αυτή η τεχνική χρησιμοποιείται από τις αυτόματες ταμειολογιστικές μηχανές (Automatic Teller Machines, ATMs) για να αναγνωρίζουν τους ιδιοκτήτες των τραπεζικών λογαριασμών.

5.1.2.3 Βιομετρήσεις

Μια τρίτη τεχνική συχνά χρησιμοποιούμενη από τους υπολογιστές για να καθορίσουν την ταυτότητα ενός προσώπου είναι να γίνει μια φυσική μέτρηση αυτού του προσώπου και να συγκριθεί αυτή η φυσική μέτρηση με μια προηγούμενη η οποία είναι καταγραμμένη. Αυτή η τεχνική ονομάζεται βιομετρική, επειδή βασίζεται πάνω σε μια μέτρηση κάποιου στοιχείου ενός ζωντανού προσώπου.

Υπάρχουν δύο τρόποι με τους οποίους τα βιομετρικά αυτά τα συστήματα μπορούν να χρησιμοποιηθούν.

Ο πιο απλός και ο αξιόπιστος τρόπος είναι να συγκρίνεις τις μετρήσεις ενός προσώπου με τις αντίστοιχες αποθηκευμένες. Η δεύτερη τεχνική είναι να εξερευνηθεί μια μεγάλη βάση δεδομένων αποθηκευμένων μετρήσεων, αναζητώντας μια συγκεκριμένη μέτρηση. Η δεύτερη τεχνική είναι περισσότερο επιρρεπής σε λάθη σύγκρισης από ότι η πρώτη.

Πολλά είδη από Βιομετρήσεις είναι πιθανά:

- Δακτυλικά αποτυπώματα.
- Αποτυπώματα πατήματος (footprints) ή τρόπος περπατήματος.
- Μια φωτογραφία ενός ανθρώπινου προσώπου.
- DNA διατάξεις.
- Σχήμα και μέγεθος χεριού.
- Τύπος αιμοφόρων αγγείων στον αμφιβληστροειδή χιτώνα.
- Αποτυπώματα φωνής.
- Γραφικό χαρακτήρα.
- Χαρακτηριστικά δακτυλογράφησης.

Επίσης οι βιομετρήσεις μπορούν να γίνουν αξιόπιστα εργαλεία για την εξακρίβωση ταυτότητας, αλλά έχουν τόσα πολλά προβλήματα που δεν χρησιμοποιούνται συχνά σήμερα.

Μερικά από αυτά τα προβλήματα περιλαμβάνουν:

- ✓ Αυτή η τεχνική απαιτεί ακριβό και ειδικού σκοπού εξοπλισμό για την μέτρηση που η κάθε βιομετρική τεχνική απαιτεί.

- ✓ Ένα βιομετρικό αποτύπωμα ενός προσώπου πρέπει να είναι σε ένα αρχείο μέσα στην τράπεζα δεδομένων του υπολογιστή πριν αυτό το πρόσωπο μπορεί να αναγνωρισθεί.

- ✓ Σε περίπτωση που ο εξοπλισμός μετρήσεων δεν είναι ειδικά προστατευμένος, ο εξοπλισμός είναι εκτεθειμένος σε δολιοφθορά και απάτη. Για παράδειγμα ένας έξυπνος κλέφτης μπορεί να ανατρέψει ένα σύστημα αναγνώρισης φωνής εάν έχει πρόσβαση στα καλώδια που συνδέουν το μικρόφωνο του συστήματος με το τμήμα επεξεργασίας φωνής. Ο κλέφτης με αυτή την πρόσβαση μπορεί να αντιγράψει απλά την φωνή ενός προσώπου που έχει πρόσβαση στο σύστημα και μετά απλά να ξαναπαίξει τον ήχο της φωνής όταν χρειάζεται.

Λόγω της πιθανής λάθους σύγκρισης, οι βιομετρήσεις συνδυάζονται με τις προηγούμενες τεχνικές (password-tokens). Στην περίπτωση των

passwords ζητείται από τον χρήστη να εισάγει έναν μυστικό αριθμό αναγνώρισης (Personal Identification Number, PIN), και μετά να δώσει ένα δείγμα βιομέτρησης, όπως είναι ένα αποτύπωμα φωνής. Το σύστημα χρησιμοποιεί τον αριθμό PIN για να βρει την κατάλληλη αποθηκευμένη μέτρηση η οποία μετά συγκρίνεται με το δείγμα που έχει ήδη αποκτηθεί.

5.1.3 Χρησιμοποιώντας τις Ψηφιακές Υπογραφές για Αναγνώριση Ταυτότητας

Πολλά από τα συστήματα αναγνώρισης ταυτότητας που αναφέρθηκαν παραπάνω μπορούν να βελτιωθούν με την χρήση των ψηφιακών υπογραφών.

Με λίγα λόγια, κάθε χρήστης ενός συστήματος που χρησιμοποιεί ψηφιακές υπογραφές δημιουργεί ένα ζεύγος κλειδιών:

- ***Ένα προσωπικό κλειδί***

Χρησιμοποιείται για να υπογράψει κάποιος με την υπογραφή του ένα κομμάτι δεδομένων, όπως είναι ένα Html κείμενο, ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ή μια φωτογραφία.

- ***Ένα δημόσιο κλειδί***

Χρησιμοποιείται για την επικύρωση της ψηφιακής υπογραφής αφού αυτή έχει υπογραφεί.

5.1.3.1 Κρυπτογράφηση και αποθήκευση του κλειδιού στον σκληρό δίσκο

Ο πιο απλός τρόπος να προστατεύσουνε ένα προσωπικό κλειδί είναι να το κρυπτογραφήσουμε χρησιμοποιώντας μια μυστική φράση (passphrase). Με αυτόν τον τρόπο τα προγράμματα όπως το PGP και ο Netscape Navigator προστατεύουν τα προσωπικά κλειδιά. Αυτή η τεχνική είναι προσωρινή λύση. Το μειονέκτημα είναι ότι αν κάποιος έχει και το προσωπικό κλειδί σου. Επίσης το κλειδί πρέπει να αποκρυπτογραφείται από τον υπολογιστή και αντιγράφεται στην μνήμη του για να μπορεί να χρησιμοποιηθεί, είναι ευπρόσβλητη η επίθεση μέσα στην μνήμη του υπολογιστή με ένα κακοποιό πρόγραμμα ή ένα «δούρειο ίππο»(Trojan horse).

5.1.3.2 Κρυπτογράφηση και αποθήκευση του κλειδιού σε ένα μεταφερόμενο μέσο

Ένας λίγο ποιο ασφαλής τρόπος να αποθηκεύσουμε το προσωπικό κλειδί μας είναι να το αποθηκεύσουμε κρυπτογραφημένο σε ένα μαλακό δίσκο, ή σε ένα CD-ROM, ή άλλο αποθηκευτικό μέσο. Μ ε αυτή την τεχνική ο επιτιθέμενος χρειάζεται και την μυστική φράση αλλά και το αποθηκευμένο κρυπτογράφημα για να αποκτήσει το προσωπικό μας κλειδί. Δυστυχώς όταν χρησιμοποιούμε το προσωπικό μας κλειδί, ο υπολογιστής αποκρυπτογραφεί το κλειδί και τοποθετεί ένα αντίγραφο στην μνήμη του. Αυτό αφήνει πάλι το

κλειδί ευπρόσβλητο σε μια επίθεση από κάποιον ιό ή άλλο κακοποιό πρόγραμμα.

5.1.3.3 Αποθήκευση του κλειδιού σε μια “Smart Card” ή άλλη έξυπνη συσκευή

Αυτή είναι ένας από τους περισσότερο ασφαλής τρόπους να προστατεύσουμε το προσωπικό μας κλειδί. Η έξυπνη κάρτα έχει έναν μικροεπεξεργαστή και στην πραγματικότητα δημιουργεί το δημόσιο/προσωπικό ζεύγος κλειδιών. Η έξυπνη κάρτα μπορεί να μεταφέρει το δημόσιο κλειδί στον “host” υπολογιστή και έχει έναν περιορισμένο αριθμό αποθηκευτικού χώρου για να κρατά 10 ή 20 πιστοποιητικά δημόσιου κλειδιού. Θεωρητικά το προσωπικό κλειδί δεν απομακρύνεται από την κάρτα. Έτσι οι επιτιθέμενοι δεν μπορούν να χρησιμοποιήσουν το προσωπικό κλειδί μας, εκτός αν έχουν στην κατοχή τους την κάρτα μας. Και αντίθετα από την περίπτωση αποθήκευσης του κλειδιού σε μια δισκέτα, ένα κακοποιό πρόγραμμα που ίσως τρέξει στον υπολογιστή μας δεν θα μπορέσει να μας κλέψει ένα αντίγραφο του προσωπικού μας κλειδιού επειδή αυτό δεν τοποθετείται ποτέ στην μνήμη του υπολογιστή μας.

Οι έξυπνες κάρτες έχουν και μειονεκτήματα όπου είναι τα εξής:

- ✓ Μερικές από αυτές είναι εύθραυστες και λεπτεπίλεπτες, έτσι ώστε με την συχνή χρήση τους αχρηστεύονται.

- ✓ Αν μια κάρτα χαθεί, κλαπεί ή καταστραφεί τα κλειδιά που περιέχει χάνονται και δεν είναι ποια διαθέσιμα στον χρήστη. Έτσι είναι απαραίτητο να υπάρχει σύστημα αναπαραγωγής καρτών και ένα

σύστημα ακύρωσης του κλειδιού σε περίπτωση απώλειας. Αυτό είναι ιδιαίτερα σημαντικό για κλειδιά που χρησιμοποιούνται για να κρυπτογραφούν αποθηκευμένα δεδομένα.

- ✓ Επίσης υπάρχει περίπτωση και να πλαστογραφηθούν.

5.2Public Key Infrastructure (PKI)

Όσα συστήματα αναγνώρισης ταυτότητας αναφέρθηκαν προηγουμένως έχουν ένα μειονέκτημα: Επιτρέπουν στους ανθρώπους να δημιουργούν προσωπικές ιδιωτικές σχέσεις ανάμεσα στους εαυτούς τους και ενός συγκεκριμένου υπολογιστικού συστήματος, αλλά δεν επιτρέπουν αυτές οι σχέσεις να σχηματίζονται στο πλαίσιο μιας μεγαλύτερης κοινωνίας.

Για παράδειγμα ο Νίκος Παπαδόπουλος γίνεται μέλος με μια πανεθνική online service και δημιουργεί έναν email λογαριασμό. Όταν δημιουργεί τον λογαριασμό, παίρνει ένα username: nikopap και ένα password:pnk32s. Όταν ο Νίκος επιθυμεί να δει τι email του, χρησιμοποιεί το password για να αποδείξει την ταυτότητα του. Ο Νίκος ίσως δημιουργήσει ένα προσωπικό κλειδί για να αποδείξει την ταυτότητα του και δώσει ένα αντίγραφο του δημοσίου κλειδιού του στην online service.

Αν ο Νίκος χάσει το password του το πρώτο που θα κάνει είναι να πάει πίσω στην πανεθνική υπηρεσία και να δημιουργήσει ένα καινούριο username:npapad, και ένα καινούργιο password:aoek4444. Ο Νίκος όμως θα είχε κάποιο πρόβλημα με την αλλαγή του username που άλλαξε στο να πείσει τους ανθρώπους που αντάλλαζε μηνύματα ότι ο nikpap και ο npapad είναι στην πραγματικότητα το ίδιο πρόσωπο.

Ο πρώτος τρόπος για να αποδείξει ότι ο Νίκος την ταυτότητά του είναι να στείλει email, τον αριθμό του τηλεφώνου του στους φίλους του και να τους ζητήσει να τον πάρουν τηλέφωνο. Αυτό ίσως και «δουλέψει» για αυτούς που έχουν ξανακούσει την φωνή του. Όλοι οι άλλοι όμως δεν έχουν τρόπο να ξέρουν αν η φωνή του Νίκου στο τηλέφωνο ανήκει όντως στον Νίκο ή σε κάποιον άλλο απατεώνα. Αν ο Νίκος αλληλογραφούσε με χιλιάδες ανθρώπους(Usenet), αυτή η τεχνική δεν θα ίσχυε.

Ένας δεύτερος τρόπος θα ήταν ο Νίκος να καταφύγει σε ένα τρίτο πρόσωπο εμπιστοσύνης να του εγγυηθεί την ταυτότητα του. Για παράδειγμα αυτός θα μπορούσε να «σαρώσει» την άδεια οδήγησης του αυτοκινήτου του, και να τοποθετήσει την εικόνα στο web site του. Το πρόβλημα με αυτήν την τεχνική είναι ότι οι επισκέπτες της ιστοσελίδας αυτής δεν θα έβλεπαν στην πραγματικότητα την άδεια οδήγησης του Νίκου, αλλά μια ψηφιακή αναπαράσταση αυτής. Αν το πρόσωπο που χρησιμοποιούσε σαν username το npapad ήταν στην αλήθεια απατεώνας, αυτό το πρόσωπο θα μπορούσε εύκολα να «σαρώσει» την δική του άδεια οδήγησης, και με το πρόγραμμα PhotoShop να άλλαζε το όνομα του με το ονοματεπώνυμο του Νίκου.

Αυτό που χρειάζεται ο Νίκος είναι να τοποθετήσει μια ψηφιακή υπογραφή στην άδεια οδήγησης του(όπως το σύστημα Veritas). Αυτή η ψηφιακή υπογραφή θα πιστοποιούσε τα περιεχόμενα της άδειας οδήγησης του, και αυτοί που θα κατέβαζαν την φωτογραφία του από το θα γνώριζαν ότι το όνομα ή η διεύθυνση του είναι η ίδια.

Η ψηφιακή υπογραφή πιστοποιητικών ιδιότητας είναι μόνο η λύση του μισού προβλήματος. Όσοι αλληλογραφούν με τον Νίκο θα είναι ικανοί να δουν την φωτογραφία άδειας οδήγησης του Νίκου και να γνωρίζουν την εμφάνιση

του Νίκου Παπαδόπουλου. Πώς όμως θα γνωρίζουν ότι ο npapad είναι στην πραγματικότητα ο Νίκος Παπαδόπουλος; Αντί να υπογραφεί ψηφιακά η φωτογραφία του Νίκου, σε αυτή την περίπτωση χρειάζεται να υπογραφεί ψηφιακά το δημόσιο κλειδί του. Ο Νίκος τότε μπορεί να υπογράψει όλα τα μηνύματα του με το προσωπικό του κλειδί.

Όποιος τώρα επιθυμεί να επιβεβαιώσει ότι τα μηνύματα του Νίκου στην πραγματικότητα του ανήκουν, θα πρέπει να πάρει ένα αντίγραφο του ψηφιακά υπογεγραμμένου δημοσίου κλειδιού του Νίκου και αν επικυρώσει την υπογραφή του που βρίσκεται εκεί.

5.3Αρχές Πιστοποίησης (Certification Authorities)

Μια αρχή πιστοποίησης (CA) είναι ένας οργανισμός που εκδίδει πιστοποιητικά δημοσίου κλειδιού. Αυτά τα πιστοποιητικά μοιάζουν με κάρτες κρυπτογραφικά υπογεγραμμένου περιεχομένου. Τα πιστοποιητικά υπογράφονται από τα προσωπικά κλειδιά που ανήκουν στην αρχή πιστοποίησης, και περιέχουν το όνομα του προσώπου, το δημόσιο κλειδί αυτού του προσώπου, έναν serial number, και άλλες πληροφορίες. Το πιστοποιητικό επιβεβαιώνει ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε έναν συγκεκριμένο οργανισμό ή άτομο.

Έχουμε πολλούς διαφορετικούς τρόπους με τους οποίους μια αρχή πιστοποίησης μπορεί να προσφέρει υπηρεσίες:

- ***Εσωτερική αρχή (Internal CA)***

Ένας οργανισμός μπορεί να λειτουργεί μια CA για να πιστοποιεί στους εργαζόμενους του, τις θέσεις τους, και το επίπεδο της εξουσίας τους. Μια

τέτοια ιεραρχία πιστοποίησης μπορεί να χρησιμοποιηθεί για τον έλεγχο πρόσβασης στις εσωτερικές πηγές πληροφοριών του οργανισμού.

- ***Εξωτερικής προέλευσης υπαλλήλου αρχή (Outsourced employee CA)***

Μια εταιρεία ίσως συμφωνήσει με μια εξωτερική φίρμα να παρέχει υπηρεσίες πιστοποίησης για τους δικούς της εργαζομένους, όπως μια εταιρία ίσως συμφωνήσει με ένα εργαστήριο φωτογραφίας για να κατασκευάσει ταυτότητες.

- ***Εξωτερικής προέλευσης πελάτη αρχή (Outsourced customer CA)***

Μια εταιρία ίσως συμφωνήσει με μια εξωτερική φίρμα να διευθύνει μια αρχή πιστοποίησης η οποία να λειτουργήσει για τους τρέχων ή για τους πιθανούς πελάτες της εταιρίας. Βασιζόμενη στις μεθόδους πιστοποίησης της εξωτερικής φίρμας, η εταιρία θα γλιτώσει την δαπάνη της δημιουργίας δικών της διαδικασιών πιστοποίησης.

- ***Έμπιστου τρίτου προσώπου αρχή (Trusted third-party CA)***

Μια εταιρία ή μια κυβέρνηση μπορεί να λειτουργήσει μια CA η οποία να συνδέει τα δημόσια κλειδιά με τα νόμιμα ονόματα ανθρώπων ή επιχειρήσεων. Μια τέτοια CA μπορεί να χρησιμοποιηθεί για να επιτρέπει σε άτομα χωρίς καμία προηγούμενη σχέση να αποδεικνύουν ο ένας στον άλλο την ταυτότητα του και να μετέχουν σε νόμιμες συναλλαγές. Για να

χρησιμοποιήσουμε τα πιστοποιητικά που έχει εκδώσει μια CA, πρέπει να έχουμε αντίγραφο του δημοσίου κλειδιού της CA.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. **Simson Garfinkel and Gene Spafford. PRACTICAL UNIX & INERNET SECURITY, second edition: April 1996.**
   O' Reilly & Associates, Inc

2. **Network and Internet work Security**
   W. Stallings, Prentice Hall

3. **Web Security &Commerce**
   O'Reilly & Associates, Inc

4. **DigiCrime**
http: // www.digicrime.com/

5. **RSA – security Protocols Overview –Ipsec**
http: // www.rwa.com/standardw/protocols/ipsec.html

6. **http: // www.cisco.com**

7. **What is … IPSec (a definition):**
http: // www.whatis.com/IPSec.htm

8. **Applied Cryptography**
http: // www.openmarket.com/techinfo/applied.htm

9. **RSA Data Security**
http: // www.rsa.com