
Ασφάλεια
στο Διαδίκτυο

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Διπλωματική Εργασία

Ασφάλεια στο διαδίκτυο
Web Security

Σπουδαστές:
Γεωργιάδου Μαρίνα ΑΕΜ:371
Ζιαζιάς Αθανάσιος ΑΕΜ:1035

Επιβλέπων Καθηγητής κ Εισηγητής:
ΚΑΤΣΑΡΟΣ ΠΑΝΑΓΙΩΤΗΣ

Θεσσαλονίκη, Ιούλιος 2007

Ευχαριστίες

Η συγκεκριμένη πτυχιακή εργασία ολοκληρώθηκε στα πλαίσια μελέτης για την Ασφάλεια στο διαδίκτυο.

Συνεπώς αισθανόμαστε την ανάγκη να ευχαριστήσουμε για το ιδιαίτερο ενδιαφέρον και ζήλο που μας έδειξε ο καθηγητής και εισηγητής κ. Κατσαρός Παναγιώτης του Αριστοτελείου Πανεπιστήμιου Θεσσαλονίκης Θετικών Επιστημών «Τμήμα Πληροφορικής», για την πολύτιμη καθοδήγηση του και την ευκαιρία που μας έδωσε να γνωρίσουμε από κοντά πολλές από τις βασικές τεχνολογίες του διαδικτύου και παράλληλα μας στάθηκε σε κάθε βήμα προς την ολοκλήρωση της διπλωματικής εργασίας αυτής.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Πρόλογος

Το Internet αρχικά ξεκίνησε και δημιουργήθηκε για ακαδημαϊκούς κυρίως σκοπούς έχει μεταβληθεί σε ένα παγκόσμιο δίκτυο αγοράς προϊόντων και συναλλαγών που ακόμα βρίσκεται σε εξέλιξη.

Η εξέλιξη του διαδικτύου, η τεράστια ανάπτυξη του οδηγεί καθημερινά στην μετατροπή των δεδομένων του φυσικού κόσμου σε ψηφιακή - ηλεκτρονική μορφή. Καθώς σχεδόν οποιαδήποτε υπηρεσία ή οργανισμός κτλ. χρησιμοποιούν υπολογιστές με πρόσβαση στο διαδίκτυο τις περισσότερες φορές για την διαχείριση των δεδομένων τους, η αξία της πληροφορίας που συγκεντρώνεται στο διαδίκτυο αποκτά τεράστιες διαστάσεις και γίνεται ένα θέμα που ολοένα και περισσότερο συζητιέται. Σε πολλές περιπτώσεις μάλιστα, ολόκληρη η πληροφορία είναι αποθηκευμένη σε ψηφιακά μέσα, χωρίς να υπάρχει σε έντυπη ή αναλογική μορφή.

Αν και έχουμε ακουστά πολλές περιπτώσεις παραβίασης της ασφάλειας συστημάτων και κλοπής δεδομένων, οι περισσότεροι χρήστες του Internet δεν έχουν δεχτεί μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια. Οι χρήστες του διαδικτύου βρίσκονται σε άγνοια όσον αφορά την ασφάλεια των δεδομένων τους, μην γνωρίζοντας τους κινδύνους και τις απειλές που αντιμετωπίζουν, ενώ οι εταιρείες παροχής υπηρεσιών -είτε πρόκειται για (ηλεκτρονική διεύθυνση) email, είτε για υποβολή φορολογικών δηλώσεων και web banking- εθίζουν τους χρήστες σε πρακτικές χαμηλής ασφάλειας και παρέχουν μια αίσθηση ότι ασχολούνται αποτελεσματικά με την ασφάλεια των δεδομένων τους.

Στο διαδίκτυο υπάρχουν διάφορες επιθέσεις που αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων.

Οι εισβολείς του διαδικτύου είναι ένας από τους σημαντικούς λόγους για να αυξηθεί η ασφάλεια στο διαδίκτυο και μεταξύ των χρηστών του. Αυτό περιλαμβάνει τη βελτίωση της ασφάλειας των συστημάτων που συνδέονται με το internet και την ενημέρωση και εκπαίδευση των χρηστών για τις απειλές. Αν και υπάρχει πολλή πληροφορία στο internet για την ασφάλεια δικτύων και συστημάτων, πολλές φορές δεν μπορεί να κατανοηθεί από χρήστες με λίγες γνώσεις. Άλλες φορές η πληροφορία δεν είναι συγκεκριμένη, δεν προχωράει σε μεγάλα επίπεδα λεπτομέρειας και καταλήγει ελλιπής.

Στο πρώτο κεφάλαιο παρουσιάζεται η αρχιτεκτονική ασφάλειας OSI/ISO. Το OSI αναφέρεται για τα συστήματα που είναι ανοικτά στην επικοινωνία με άλλα συστήματα και επίσης το ISO είναι Διεθνούς Οργανισμού Τυποποίησης, με στόχο την τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα επίπεδα των δικτύων.

Στο δεύτερο κεφάλαιο παρουσιάζεται και αναλύεται για τα βασικά θέματα της Κρυπτογραφίας. Η κρυπτογραφία χωρίζονται σε δυο κατηγορίες α)τα συμμετρικά κρυπτοσυστήματα(αναφορά σε αλγορίθμους όπως DES, AES κτλ..) και β) τα ασύμμετρα κρυπτοσυστήματα (αναφορά σε αλγορίθμους όπως Diffie-Hellman κτλ..).

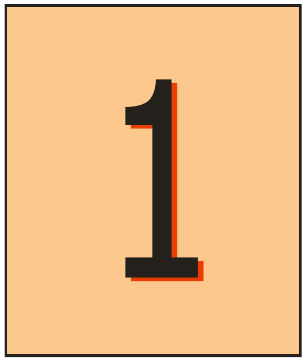
Στο τρίτο κεφάλαιο γίνεται περιγράφει με αναλυτικό τρόπο, ορισμός για το τι είναι το δημόσιο κλειδί και για διάφορα πιστοποιητικά, ένα από τα πιο ενδιαφέροντα είναι το πιστοποιητικό X.509 κτλ.

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Στο τέταρτο κεφάλαιο αναλύεται για το τι είναι ασφάλεια στο διαδίκτυο (Internet) , αναφέρεται σε τεχνικές που χρησιμοποιούνται για την διασφάλιση ότι τα δεδομένα που αποθηκεύονται σε ένα ηλεκτρονικό υπολογιστή δεν θα μπορούν να διαβαστούν ή να αλλοιωθούν από οποιονδήποτε δίχως εξουσιοδότησή. Αναφορά και στο SSL

Στο πέμπτο κεφάλαιο αναφερόμαστε στις κακόβουλες επιθέσεις στο Διαδίκτυο αυτό επικεντρώνεται στην ασφάλεια του διαδικτύου αρχίζοντας από την ευαισθησία των υποδομών του και προχωρώντας στους μηχανισμούς εκμετάλλευσης αυτών από τρίτους, στα ειδή επιθέσεων κτλ..

Συνοψίζοντας, η διπλωματική εργασία έχει στόχο να ενημερώσει για θέματα ασφάλειας δικτύων και να αυξήσει το ενδιαφέρον των χρηστών.



Κεφάλαιο

«Η Αρχιτεκτονική Ασφάλειας OSI/ISO»

1.1 Ορισμός του μοντέλου

1.2 Εισαγωγικά

1.3 Περιγραφή του μοντέλου

1.4 Υπηρεσίες Ασφάλειας της αρχιτεκτονικής OSI.

Κεφάλαιο 1 : Η αρχιτεκτονική Ασφάλειας OSI/ISO

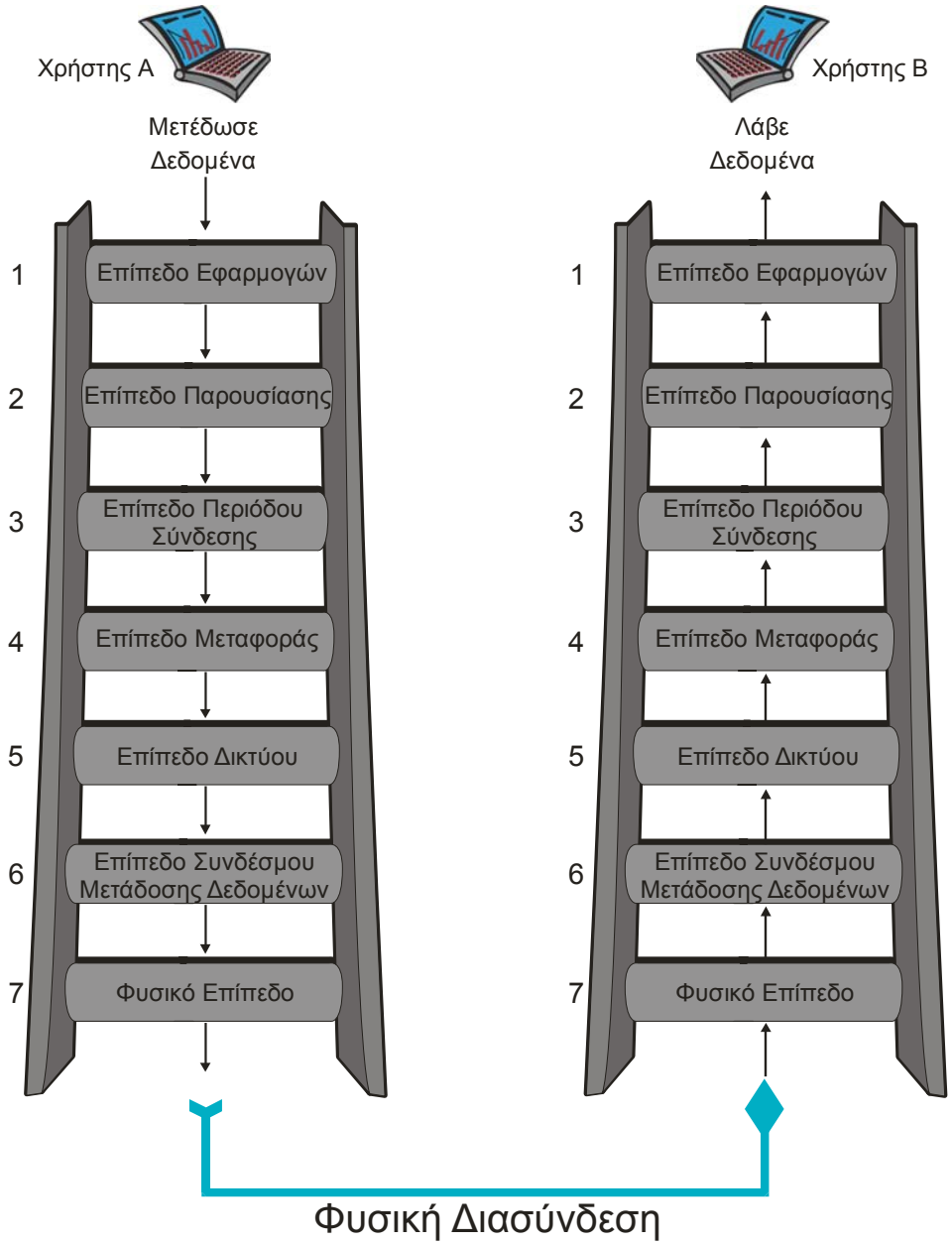
1.1 Ορισμός του μοντέλου

OSI : Open System Interconnection – Διασύνδεση Ανοικτού Συστήματος.

ISO : International Standards Organization – Διεθνής Οργανισμός Τυποποίησης.

Ο ορισμός αυτός δόθηκε μιας και το OSI ασχολείται με τη διασύνδεση ανοικτών συστημάτων, δηλαδή συστημάτων που είναι ανοικτά στην επικοινωνία με άλλα συστήματα.

Το μοντέλο OSI, ορίζει ένα πλαίσιο δικτύωσης (networking framework) για την υλοποίηση πρωτοκόλλων σε επτά στρώματα. Ο έλεγχος περνάει από το ένα στρώμα στο επόμενο, αρχίζοντας από το επίπεδο εφαρμογής (application layer) στον ένα σταθμό, προχωρώντας στο κατώτατο επίπεδο, μέσω του καναλιού προς τον επόμενο σταθμό και προς τα πίσω στην ιεραρχία.



Σχήμα 1.1

1.2 Εισαγωγικά

Το μοντέλο OSI οφείλει την ύπαρξή του σε εγχείρημα του Διεθνούς Οργανισμού Τυποποίησης, με στόχο την τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα επίπεδα των δικτύων.

Η παρουσίαση του μοντέλου OSI έγινε το έτος 1989 από τον Οργανισμό Προτυποποίησης ISO. Από τότε αποτελεί σημείο αναφοράς για τον τομέα σχετικά με θέματα ασφάλειας δικτύων.

Η αρχιτεκτονική ασφάλειας OSI 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 και μία γενική περιγραφή των υπηρεσιών και των αντίστοιχων μηχανισμών ασφάλειας για την περιγραφή των προβλημάτων ασφάλειας και των αντίστοιχων λύσεων.

1.3 Περιγραφή του μοντέλου

Το μοντέλο αυτό αποτελείται από επτά επίπεδα όπως φαίνεται στο Σχήμα 1.1. Για κάθε επίπεδο του μοντέλου δίνεται και η περιγραφή του, ξεκινώντας από το κατώτατο επίπεδο.

(1) Το Φυσικό Επίπεδο – Physical Layer :

Το **φυσικό επίπεδο** (physical layer) βρίσκεται πάνω από το φυσικό μέσο και ασχολείται με τη μετάδοση ανεπεξέργαστων (raw) δυαδικών ψηφίων μέσω ενός καναλιού επικοινωνίας. Τα ζητήματα σχεδίασης σχετίζονται με την εξασφάλιση του ότι, όταν η μία πλευρά στέλνει το bit 1, αυτό θα λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0. Ασχολείται κυρίως με τις μηχανικές, ηλεκτρονικές και χρονικές διασυνδέσεις όπως τα επίπεδα τάσης, τον χρονισμό κτλ, καθώς και με το φυσικό μέσο μετάδοσης, το οποίο βρίσκεται κάτω από αυτό.

(2) Το Επίπεδο Σύνδεσης Μετάδοσης Δεδομένων – Data Link Layer :

Η κύρια λειτουργία του, σε γενικές γραμμές είναι, ο έλεγχος και η διόρθωση σφαλμάτων. Πιο συγκεκριμένα, ο κυρίως στόχος του **επιπέδου σύνδεσης μετάδοσης δεδομένων** είναι να μετασχηματίζει μια υπηρεσία μετάδοσης ανεπεξέργαστων δεδομένων σε μια γραμμή η οποία να φαίνεται στο επίπεδο δικτύου ότι δεν έχει τον κίνδυνο μη εντοπισμένων σφαλμάτων μετάδοσης. Ο στόχος αυτός επιτυγχάνεται με το να βάζουμε τον αποστολέα να τεμαχίζει τα δεδομένα εισόδου σε πλαίσια δεδομένων (data frames) — με τυπικό μέγεθος λίγες εκατοντάδες ή λίγες χιλιάδες bytes, να οριοθετείται η αρχή και το τέλος του κάθε frame και να μεταδίδει τα πλαίσια με τη σειρά. Αν η υπηρεσία είναι αξιόπιστη, ο παραλήπτης επιβεβαιώνει την ορθή λήψη κάθε πλαισίου επιστρέφοντας ένα πλαίσιο επιβεβαίωσης (acknowledgment frame).

Ένα πρόβλημα που παρουσιάζεται στο επίπεδο σύνδεσης μετάδοσης δεδομένων (καθώς και στα περισσότερα ανώτερα επίπεδα) είναι το πώς μπορεί να αποτραπεί ένας γρήγορος αποστολέας από το να κατακλύσει με δεδομένα έναν αργό παραλήπτη. Συχνά απαιτείται κάποιος μηχανισμός ρύθμισης της κυκλοφορίας, έτσι ώστε ο αποστολέας να μαθαίνει πόσο χώρο προσωρινής αποθήκευσης διαθέτει ανά πάσα στιγμή ο παραλήπτης. Πολλές φορές οι μηχανισμοί ρύθμισης της κυκλοφορίας και διαχείρισης των σφαλμάτων είναι ενοποιημένοι.

(3) Το Επίπεδο Δικτύου – Network Layer :

Έχει ως κύρια λειτουργία του τον έλεγχο της λειτουργίας του υποδικτύου. Ένα βασικό ζήτημα σχεδίασης είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την προέλευση προς τον προορισμό τους. Τα δρομολόγια μπορεί να βασίζονται σε στατικούς πίνακες οι οποίοι είναι προσαρμοσμένοι στο δίκτυο και μεταβάλλονται σπάνια. Μπορεί επίσης να προσδιορίζονται στην αρχή κάθε συνόδου, για παράδειγμα, στην αρχή μιας περιόδου εργασίας τερματικού (δηλαδή, όταν πραγματοποιείται μια σύνδεση σε κάποια απομακρυσμένη μηχανή). Τέλος, μπορεί να είναι εντελώς δυναμικά, δηλαδή να καθορίζονται εκ νέου για κάθε πακέτο, έτσι ώστε να αντανακλούν το τρέχον φορτίο του δικτύου.

Αν υπάρχουν πάρα πολλά πακέτα στο υποδίκτυο την ίδια χρονική στιγμή, θα αρχίσουν να "παρεμποδίζουν" το ένα το άλλο, δημιουργώντας συμφόρηση. Ο έλεγχος της συμφόρησης ανήκει και αυτός στο επίπεδο δικτύου. Γενικότερα, η παρεχόμενη ποιότητα υπηρεσιών (καθυστέρηση, χρόνος διέλευσης, παραμόρφωση χρονισμού, κ.λπ.) είναι επίσης θέμα του επίπεδου δικτύου.

Όταν ένα πακέτο πρέπει να ταξιδέψει από ένα δίκτυο σε κάποιο άλλο προκειμένου να φτάσει στον προορισμό του, μπορεί να εμφανιστούν πολλά προβλήματα. Η διευθυνσιοδότηση που χρησιμοποιείται από το δεύτερο δίκτυο μπορεί να διαφέρει από εκείνη του πρώτου. Το δεύτερο δίκτυο μπορεί να μη δεχτεί καθόλου το πακέτο, αν αυτό είναι πολύ μεγάλο. Μπορεί ακόμα να διαφέρουν τα πρωτόκολλα, και ούτω καθεξής. Είναι θέμα του επιπέδου δικτύου να ξεπεράσει όλα αυτά τα προβλήματα, επιτρέποντας έτσι τη διασύνδεση ετερογενών δικτύων.

Στα δίκτυα εκπομπής (broadcast networks) το πρόβλημα της δρομολόγησης είναι απλό, έτσι το επίπεδο δικτύου είναι συνήθως υποτυπώδες ή ακόμη και ανύπαρκτο.

(4) Το Επίπεδο Μεταφοράς – Transport Layer :

Η βασική λειτουργία του **επιπέδου μεταφοράς** είναι να δέχεται δεδομένα από το ανώτερο επίπεδο (session layer), να τα τεμαχίζει αν χρειάζεται σε μικρότερα τμήματα, να τα μεταβιβάζει στο επίπεδο δικτύου (network layer), και να εξασφαλίζει ότι όλα αυτά τα τμήματα φτάνουν σωστά στο άλλο άκρο. Επιπρόσθετα, όλα αυτά πρέπει να γίνονται με αποδοτικό τρόπο και έτσι ώστε να απομονώνονται τα ανώτερα επίπεδα από τις αναπόφευκτες τεχνολογικές αλλαγές που προκύπτουν στο χρησιμοποιούμενο υλικό.

Επιπλέον, το επίπεδο μεταφοράς καθορίζει τον τύπο της υπηρεσίας που θα παρέχεται στο επίπεδο συνόδου και, τελικά, στους χρήστες του δικτύου. Ο πιο δημοφιλής τύπος σύνδεσης στο επίπεδο μεταφοράς είναι ένα «απαλλαγμένο από σφάλματα κανάλι» από σημείο σε σημείο, το οποίο παραδίδει μηνύματα ή byte με τη σειρά που στάλθηκαν. Άλλα πιθανά είδη υπηρεσίας μεταφοράς είναι η μεταφορά μεμονωμένων μηνυμάτων χωρίς εγγυήσεις για τη σειρά μετάδοσης τους, και η εκπομπή μηνυμάτων σε πολλαπλούς προορισμούς. Ο τύπος της υπηρεσίας καθορίζεται όταν εγκαθιδρύεται η σύνδεση.

Το επίπεδο μεταφοράς είναι ένα πραγματικό επίπεδο "απ' άκρου εις άκρο" (end-to-end), δηλαδή από την προέλευση έως τον προορισμό. Με άλλα λόγια, ένα πρόγραμμα στη μηχανή προέλευσης πραγματοποιεί σύνοδο με ένα παρόμοιο πρόγραμμα στη μηχανή προορισμού, χρησιμοποιώντας τις κεφαλίδες των μηνυμάτων και τα μηνύματα ελέγχου.

(5) Το Επίπεδο Συνόδου ή Επίπεδο Περιόδου Σύνδεσης – Session Layer :

Το **επίπεδο συνόδου** ή επίπεδο περιόδου σύνδεσης (session layer) έχει ως κύρια λειτουργία την αποκατάσταση συνόδων (sessions) μεταξύ χρηστών διαφορετικών μηχανών. Οι σύνοδοι προσφέρουν διάφορες υπηρεσίες, στις οποίες περιλαμβάνονται ο έλεγχος διαλόγου (dialog control, η παρακολούθηση του ποιος έχει σειρά να μεταδώσει), η διαχείριση σκυτάλης (token management, η αποτροπή των δύο πλευρών από το να επιχειρήσουν ταυτόχρονα την εκτέλεση της ίδιας κρίσιμης λειτουργίας), και ο συγχρονισμός (synchronization, η τήρηση σημείων ελέγχου σε μακρόχρονες μεταδόσεις έτσι ώστε αυτές να μπορούν να συνεχιστούν από το σημείο όπου διακόπηκαν, μετά από μια κατάρρευση του συστήματος).

(6) Το Επίπεδο Παρουσίασης – Presentation Layer :

Σε αντίθεση με τα κατώτερα επίπεδα, που ασχολούνται κυρίως με τη μεταφορά bit, το **επίπεδο παρουσίασης** ασχολείται με τη σύνταξη και τη σημασιολογία των μεταδιδομένων πληροφοριών. Για να είναι εφικτή η επικοινωνία μεταξύ υπολογιστών που χρησιμοποιούν διαφορετικές αναπαραστάσεις δεδομένων, μπορούν να οριστούν με αφαιρετικό τρόπο οι δομές δεδομένων που θα ανταλλάσσονται, μαζί με μια τυποποιημένη κωδικοποίηση που θα χρησιμοποιείται "μέσα στο καλώδιο". Το επίπεδο παρουσίασης διαχειρίζεται αυτές τις αφαιρετικές δομές δεδομένων και επιτρέπει τον ορισμό και την ανταλλαγή δομών δεδομένων υψηλού επιπέδου (για παράδειγμα, τραπεζικών εγγραφών). Ποιο απλά, η κύρια λειτουργία του είναι η παροχή γενικών η σταθερών λύσεων σε προβλήματα που συναντούν συχνά οι χρήστες του δικτύου, όπως η μετατροπή από ASCII σε Unicode.

(7) Το Επίπεδο Εφαρμογών – Application Layer :

Το **επίπεδο εφαρμογών** έχει ως κύριο σκοπό του την υποστήριξη μια ποικιλίας πρωτοκόλλων που χρησιμοποιούνται τακτικά από τους χρήστες. Ένα ευρέως χρησιμοποιούμενο πρωτόκολλο εφαρμογής είναι το Πρωτόκολλο Μεταφοράς Υπερ-κειμένου ή HTTP (HyperText Transfer Protocol), το οποίο είναι η βάση του Παγκόσμιου Ιστού. Όταν ένα πρόγραμμα πλοήγησης (browser) αιτείται πρόσβαση σε μια ιστοσελίδα, στέλνει το όνομα της επιθυμητής σελίδας στο διακομιστή χρησιμοποιώντας το πρωτόκολλο HTTP. Ο διακομιστής επιστρέφει στη συνέχεια τη σελίδα αυτή. Άλλα πρωτόκολλα εφαρμογών χρησιμοποιούνται για τη μεταφορά αρχείων, το ηλεκτρονικό ταχυδρομείο, και τις ομάδες ειδήσεων δικτύου.

Οι αρχές που εφαρμόστηκαν και προέκυψαν τα επίπεδα αυτά είναι:

1. Σε όποιο σημείο χρειαστεί μια διαφορετική λογική αφαίρεση πρέπει να δημιουργείται ένα επίπεδο.
2. Κάθε επίπεδο πρέπει να εκτελεί μια σαφώς καθορισμένη λειτουργία.
3. Η λειτουργία κάθε επιπέδου πρέπει να επιλέγεται με στόχο τον καθορισμό διεθνώς τυποποιημένων πρωτοκόλλων.
4. Τα σύνορα των επιπέδων πρέπει να επιλέγονται έτσι ώστε να ελαχιστοποιείται η ροή πληροφοριών μέσω της διασύνδεσης των επιπέδων.
5. Το πλήθος των επιπέδων πρέπει να είναι αρκετά μεγάλο έτσι ώστε να μη χρειάζεται να ανακατεύονται χωρίς λόγο διαφορετικές λειτουργίες στο ίδιο επίπεδο, και ταυτόχρονα αρκετά μικρό έτσι ώστε η αρχιτεκτονική να μη γίνεται άβολη.

1.3Υπηρεσίες Ασφάλειας της αρχιτεκτονικής OSI.

Οι υπηρεσίες ασφάλειας που προσφέρει η αρχιτεκτονική OSI διαχωρίζονται σε 5 κλάσεις (classes). Ο διαχωρισμός αυτό κινείται στο ίδιο πεδίο με τον παραπάνω διαχωρισμό σε επίπεδα. Έχει ως στόχο την επίτευξη της λειτουργικότητας του σχεδιασμού και της υλοποίησης των παρεχόμενων υπηρεσιών.

Ακολουθεί πίνακας περιγραφής των κλάσεων και επεξήγησης της κάθε μιας.

Πίνακας Περιγραφής των Κλάσεων Υπηρεσιών Ασφάλειας OSI			
1.	Αυθεντικοποίηση	⇨	1. Υπηρεσία Αυθεντικοποίησης Ομότιμης Οντότητας. 2. Υπηρεσία Αυθεντικοποίησης Προέλευσης των Δεδομένων.
2.	Έλεγχος Προσπέλασης	⇨	Υπηρεσία Ελέγχου Προσπέλασης.
3.	Εμπιστευτικότητα Δεδομένων	⇨	1. Υπηρεσία Εμπιστευτικότητας Συνόδου. 2. Υπηρεσία Εμπιστευτικότητας Μη Εγκατεστημένης Συνόδου. 3. Υπηρεσία Εμπιστευτικότητας Επιλεγμένου Πεδίου. 4. Υπηρεσία Εμπιστευτικότητας Ροής Κίνησης Δικτύου.
4.	Ακεραιότητα Δεδομένων	⇨	1. Υπηρεσία Ακεραιότητας Συνόδου με Αποκατάσταση. 2. Υπηρεσία Ακεραιότητας Συνόδου Χωρίς Αποκατάσταση. 3. Υπηρεσία Ακεραιότητας Συνόδου ς Επιλεγμένου Πεδίου. 4. Υπηρεσία Ακεραιότητας Μη Εγκατεστημένης Συνόδου 5. Υπηρεσία Ακεραιότητας Επιλεγμένου Πεδίου Μη Εγκατεστημένης Συνόδου.
5.	Μη Αποποίηση	⇨	1. Μη Αποποίηση Με Απόδειξη Προέλευσης. 2. Μη Αποποίηση Με Απόδειξη Παράδοσης.

Αναλυτική Παρουσίαση:

1) Η Αυθεντικοποίηση (authentication) ως στόχο της έχει την πιστοποίηση της ταυτότητας μιας οντότητας και την διασφάλιση της γνησιότητας των μηνυμάτων που ανταλλάσσονται μεταξύ των στελεχών μιας επικοινωνίας.

   Χωρίζεται σε 2 είδη υπηρεσιών:

   α) *Αυθεντικοποίηση Ομότιμης Οντότητας (Peer Entity Authentication):* Υπηρεσία που ελέγχει αν μια οντότητα που συμμετέχει σε μια επικοινωνία είναι αυτή που ισχυρίζεται πως είναι. Συγκεκριμένα, διασφαλίζει πως μια οντότητα δε θα προσπαθήσει να προσποιηθεί ότι είναι μία άλλη οντότητα ή να πραγματοποιήσει μία μη εξουσιοδοτημένη επανάληψη μηνύματος. Η αυθεντικοποίηση ομότιμης οντότητας λαμβάνει χώρα συνήθως είτε κατά τη διάρκεια της φάσης εγκατάστασης μιας συνόδου, είτε σπανιότερα κατά τη διάρκεια της φάσης μεταφοράς των δεδομένων.

   β) *Αυθεντικοποίηση Προέλευσης Δεδομένων (Data Origin Authentication):* Υπηρεσία που ως λειτουργία έχει την πιστοποίηση της πηγής προέλευσης ενός μηνύματος με βάση τον ισχυρισμό του. Αυτή η υπηρεσία δεν προσφέρει διασφάλιση έναντι επανάληψης ή

τροποποίησης των μηνυμάτων κατά τη μετάδοση. Τέτοιου είδους υπηρεσίες προσφέρονται συνήθως σε συνδυασμό με την ακεραιότητα δεδομένων. Η αυθεντικοποίηση προέλευσης δεδομένων συνήθως παρέχεται κατά τη διάρκεια της φάσης μεταφοράς δεδομένων.

2) Ο Έλεγχος Προσπέλασης (Access Control) είναι υπηρεσία που στοχεύει στην διασφάλιση της ακεραιότητας των πόρων του συστήματος και της προσπέλασης τους μόνο από 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.

3) Η Εμπιστευτικότητα Δεδομένων (Data Confidentiality) είναι υπηρεσία που στοχεύει στην πλήρη απόκρυψη δεδομένων από μη εξουσιοδοτημένες οντότητες. Οι λειτουργίες που παρέχει εφαρμόζονται σε μέρος του πακέτου ή σε ολόκληρο το πακέτο. Ποιο αναλυτικά οι υπηρεσίες που περιλαμβάνει είναι οι ακόλουθες:

   α) *Υπηρεσία Εμπιστευτικότητας Σύνδεσης (Connection Confidentiality Service)*: Η υπηρεσία παρέχει εμπιστευτικότητα των δεδομένων προς μετάδοση.

   β) *Υπηρεσία Εμπιστευτικότητας μη Εγκατεστημένης Σύνδεσης (Connectionless Confidentiality Service)*: Η υπηρεσία παρέχει εμπιστευτικότητα μεμονωμένων τμημάτων δεδομένων.

   γ) *Υπηρεσία Εμπιστευτικότητας Επιλεγμένου Πεδίου (Selected Field Confidentiality Service)*: Η υπηρεσία παρέχει εμπιστευτικότητα συγκεκριμένων πεδίων στα δεδομένα μιας σύνδεσης ή σε μεμονωμένα τμήματα αυτών.

   δ) *Υπηρεσία Εμπιστευτικότητας Ροής Κίνησης (Traffic Flow Confidentiality Service)*: Η υπηρεσία παρέχει προστασία πληροφοριών που μπορούν να αποκαλυφθούν ή να προκύψουν από επιθέσεις τύπου ανάλυσης κυκλοφορίας (traffic analysis).

4) Η Ακεραιότητα Δεδομένων (Data Integrity) εξασφαλίζει την ακεραιότητα των μεταδομένων δεδομένων κατά την μετάδοσή τους, δηλαδή ότι τα δεδομένα δεν έχουν τροποποιηθεί από μη-εξουσιοδοτημένους χρήστες. Οι λειτουργίες που παρέχει εφαρμόζονται σε μέρος του πακέτου ή σε ολόκληρο το πακέτο. Και σε αυτή την περίπτωση οι ανάλογοι μηχανισμοί μπορούν να εφαρμοστούν είτε σε ολόκληρο το μήνυμα ή σε ένα τμήμα του, όπως και παραπάνω.

   α) *Υπηρεσία Ακεραιότητας Σύνδεσης με Αποκατάσταση (Connection Integrity Service With Recovery):* Η υπηρεσία παρέχει ακεραιότητα των δεδομένων μιας σύνδεσης. Διασφαλίζει την δυνατότητα της πιθανής ανάκτησης των δεδομένων υπό ορισμένες συνθήκες.

   β) *Υπηρεσία Ακεραιότητας Σύνδεσης Χωρίς Αποκατάσταση (Connection Integrity Service Without Recovery):* Η υπηρεσία παρέχει επίσης ακεραιότητα των δεδομένων μιας σύνδεσης χωρίς να είναι εφικτή η ανάκτηση της ακεραιότητας σε περίπτωση απώλειας της.

   γ) *Υπηρεσία Ακεραιότητας Σύνδεσης Επιλεγμένου Πεδίου (Selected Field Connection Integrity Service):* Η υπηρεσία παρέχει ακεραιότητα μεμονωμένων πεδίων των δεδομένων μιας σύνδεσης.

   δ) *Υπηρεσία Ακεραιότητας Άνευ Εγκατάστασης Σύνδεσης (Connectionless Integrity Service):* Η υπηρεσία παρέχει ακεραιότητα μεμονωμένων τμημάτων δεδομένων.

δ) *Υπηρεσία Ακεραιότητας Επιλεγμένου Πεδίου Άνευ Εγκατάστασης Σύνδεσης (Selected Field Connectionless Integrity Service):* Η υπηρεσία παρέχει ακεραιότητα συγκεκριμένων πεδίων σε μεμονωμένα τμήματα δεδομένων.

5) Η Μη-Αποποίηση (non-repudiation) διασφαλίζει πως μια οντότητα δεν θα μπορέσει να αρνηθεί τόσο την αποστολή όσο και την παραλαβή κάποιου μηνύματος. Οι υπηρεσίες μη-αποποίησης είναι ιδιαίτερα σημαντικές στις συναλλαγές σε περιβάλλον ηλεκτρονικού επιχειρείν.

Χωρίζεται και αυτή σε 2 είδη υπηρεσιών:

α) *Μη Αποποίηση Με Απόδειξη Προελεύσεως (Non - Repudiation With Proof Of Origin)*: Η υπηρεσία αυτή παρέχει στον παραλήπτη πιστοποίηση της προέλευσης των μηνυμάτων που παραλαμβάνει.

β) *Μη αποποίηση με Απόδειξη Παραδόσεως (Non-Repudiation With Proof Of Delivery)*: Η υπηρεσία αυτή παρέχει στον αποστολέα πιστοποίηση της παράδοσης των μηνυμάτων που αποστέλλει.

Ακολουθεί μια παρουσίαση των κλάσεων και των επιπέδων OSI με ομαδοποίηση ως προς τα επίπεδα:

Αντιστοίχιση των Κλάσεων στα Επίπεδα			
	Επίπεδο – Layer		Υπηρεσία-ες
7.	Εφαρμογής (Application)	⇨	Αυθεντικοποίηση Έλεγχος Προσπέλασης Εμπιστευτικότητα Δεδομένων Ακεραιότητα Δεδομένων Μη Αποποίηση
6.	Παρουσίασης (Presentation)	⇨	Εμπιστευτικότητα Δεδομένων
5.	Συνόδου (Session)	⇨	-
4.	Μεταφοράς (Transport)	⇨	Αυθεντικοποίηση Έλεγχος Προσπέλασης Εμπιστευτικότητα Δεδομένων Ακεραιότητα Δεδομένων
3.	Δικτύου (Network)	⇨	Αυθεντικοποίηση Έλεγχος Προσπέλασης Εμπιστευτικότητα Δεδομένων Ακεραιότητα Δεδομένων
2.	Σύνδεσης Δεδομένων (Data Link)	⇨	Αυθεντικοποίηση Έλεγχος Προσπέλασης Εμπιστευτικότητα Δεδομένων Ακεραιότητα Δεδομένων

1.	Φυσικό (Physical) ⇨ Εμπιστευτικότητα Δεδομένων

Τεχνολογίες Ηλεκτρονικής Ασφάλειας

Οι τεχνολογίες ασφάλειας που προσφέρονται σε διάφορα επίπεδα του μοντέλου OSI-ISO είναι:

1) Επίπεδο εφαρμογής: Συμμετρική και Μη-συμμετρική κρυπτογραφία, Ψηφιακές Υπογραφές, Ψηφιακά Πιστοποιητικά και Αρχές Πιστοποίησης, Διαχείριση κλειδιών, Αλγόριθμοι Κρυπτογράφησης. Περιγράφονται στο κεφάλαιο 2.
2) Επίπεδο Σύνδεσης: S-HTTP, SSL, S-MIME, PGP, Firewalls

Περιγραφή των τεχνολογιών που προσφέρονται στο Επίπεδο Σύνδεσης, εν συντομία :

(1) S-HTTP (Secure Hyper-Text Transfer Protocol) : Πρόκειται για σύστημα ασφαλείας των πληροφοριών που υπάρχουν/μεταδίδονται μέσω WWW. Χρησιμοποιεί την μέθοδο δημόσιου-ιδιωτικού κλειδιού. Αποτελεί μια επέκταση του πρωτοκόλου HTTP και αναπτύχθηκε από τον οργανισμό CommerceNet. Προσφέρει διάφορες τεχνικές ασφαλείας όπως κρυπτογράφηση με βάση τους αλγόριθμους RSA που προβλέπεται να αποτελέσουν την βάση πολλών μεθόδων πληρωμής μέσω δικτύου.

(2) SSL (Secure Socket Layer) : Είναι ένα Internet socket-layer communication interface που επιτρέπει την ασφαλή επικοινωνία αγοραστή και πωλητή. Η τεχνολογία αυτή έχει αναπτυχθεί από την Netscape Communications Corporation. Πληρέστερη αναφορά του στο κεφάλαιο 4.

(3) S-MIME (Secure Multi-Purpose Internet Mail Extensions) : είναι μια ασφαλής μέθοδος για να στέλνει κάποιος μηνύματα χρησιμοποιώντας το σύστημα κρυπτογράφησης RSA (Rivest-Shamir-Adleman). Υποστηρίζεται από τις νεότερες εκδόσεις των browsers. Βασίζεται στη χρήση ενός ψηφιακού φακέλου (digital envelope). Το μήνυμα κρυπτογραφείται με ένα συμμετρικό αλγόριθμο, όπως DES ή RC2. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη και μαζί με το κρυπτογραφημένο μήνυμα τοποθετούνται στον ψηφιακό φάκελο για να σταλούν στον παραλήπτη.

(4) PGP (Pretty Good Privacy) : είναι ένα δημοφιλές πρόγραμμα που χρησιμοποιείται για να κρυπτογραφεί και να αποκρυπτογραφεί ηλεκτρονικά μηνύματα (e-mails). Πληρέστερη αναφορά του στο κεφάλαιο 3.

(5) Firewalls - Τείχος Προστασίας : Τα Firewalls είναι συστήματα που περιλαμβάνουν φίλτρα για μπλοκάρισμα και παρακολούθηση της μετάδοσης συγκεκριμένων πακέτων δεδομένων, gateways για προώθηση των αποδεκτών πακέτων και application proxies που εκτελούν έλεγχο ειδικής πρόσβασης σε εφαρμογές, παρακολούθηση και αναφορά. Γίνεται αναφορά του στο κεφάλαιο 5.

Κεφάλαιο

«Βασικά Θέματα Κρυπτογραφίας
-Συμμετρικά Κρυπτοσυστήματα
-Ασύμμετρα Κρυπτοσυστήματα»

«Ουδέν κρυπτόν υπό τον ήλιον»
Αρχαίο απόφθεγμα
Όχι πια...

«Τίποτα δε μένει κρυφό. Ή μήπως όχι; Εάν ίσχυε κάτι τέτοιο τότε όλοι αυτοί που ασχολούνται με θέματα κρυπτογραφίας θα έχαναν τη δουλειά τους. Το θέμα του απορρήτου (secrecy) είναι αρκετά επίκαιρο, μιας που όλο και περισσότερες συναλλαγές γίνονται από απόσταση – με το Internet να τείνει να αποκτήσει την πρωτοκαθεδρία- και επομένως όλο και περισσότερες ευαίσθητες πληροφορίες διακινούνται. Πολλές φορές η ασφάλεια στο δίκτυο ταυτίζεται με το απόρρητο, αλλά όχι και τόσο εύστοχα.»

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 Εισαγωγή

Από το μακρινό παρελθόν οι ασφαλές μεταδόσεις πληροφοριών και μηνυμάτων απασχόλησε τους ανθρώπους και εξακολουθούν να τους απασχολούν έως σήμερα δηλ. την μετάδοση πληροφοριών χωρίς να γίνεται αντιληπτή από τρίτους, η εξασφάλιση της δυνατότητας να μην μπορεί να διαβαστεί το μήνυμα στην περίπτωση που η μετάδοση γίνει αντιληπτή καθώς και η απόδειξη της αυθεντικής αποστολής ενός μηνύματος. Τα προβλήματα αυτά, θα εξακολουθούν να υπάρχουν, όσο θα υπάρχουν άνθρωποι που θα προσπαθούν να προστατέψουν τα δικαιώματά τους και κάποιοι που θα προσπαθούν να τα παραβιάσουν. Στη σύγχρονη εποχή, τα προβλήματα αυτά μεταφέρονται στο χώρο των ψηφιακών δεδομένων. Σύγχρονες υπολογιστικές μηχανές, με υψηλές δυνατότητες επεξεργασίας και αποθήκευσης πληροφοριών, χρησιμοποιούνται τόσο για να εξασφαλίζουν τη νομιμότητα όσο και για να την παρακάμπτουν.

Στην σημερινή εποχή η πραγματικότητα επιβάλλει την ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο, οι συναλλαγές και η μετάδοση εμπιστευτικών δεδομένων κτλ., και ειδικοτερα την ύπαρξη μηχανισμών προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των συναλλασσόμενων χρηστών. Επιβάλλει μηχανισμούς ασφάλειας στις συναλλαγές, ασφάλειας η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτοποίηση δηλαδή των συναλλασσόμενων.

Λόγοι οι οποίοι καθιστούν την ασφάλεια στην ηλεκτρονική επικοινωνία επιτακτική, είναι η ευκολία που παρέχεται μέσω ενός ανοικτού δικτύου, όπως είναι το Internet στην:

α) παρακολούθηση της επικοινωνίας από τρίτους- ωτακουστές (eavesdroppirs)

β) αλλοίωση του περιεχομένου του μεταφερόμενου μηνύματος-ψευδές μήνυμα (fake message)

γ) η όχι πάντα δυνατή εξακρίβωση της ταυτότητας των επικοινωνούντων μερών ιδιωτικότητα (privacy) καθιστά πιθανή μία επίθεση πλαστοπροσωπίας (impersonation).

Η κρυπτογραφία αποτέλεσε πανάρχαια μέθοδο εξασφάλισης της εμπιστευτικότητας των συναλλαγών, όπως θα δούμε παρακάτω στην ενότητα 2.3 ιστορική της διαδρομή. Μια από τις μεθόδους που χρησιμοποιούνται για την ασφαλή διακίνηση των πληροφοριών στο σύγχρονο περιβάλλον, είναι η κρυπτογραφία. Εξακολουθεί επίσης, έως και σήμερα να συμβάλλει στον παραπάνω στόχο, καθώς η ίδια αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet. Ειδικότερα, με τη χρήση της τεχνολογίας της κρυπτογραφίας, δημιουργούνται οι προηγμένες ηλεκτρονικές υπογραφές ή αλλιώς λεγόμενες ψηφιακές υπογραφές.

2.2 Ασφάλεια στο δίκτυο

Οι απειλές (threats) ασφάλειας δικτύου χωρίζονται σε δύο κατηγορίες. Οι παθητικές απειλές, που μερικές φορές αναφέρονται ως παρακολούθηση (eavesdropping)$_{\tau}$ περιλαμβάνουν απόπειρες από έναν επιτιθέμενο να αποκτήσει πληροφορία σχετικά με το μήνυμα που διακινείται σε μία επικοινωνία. Οι ενεργητικές απειλές περιλαμβάνουν κάποια τροποποίηση των μεταδιδόμενων δεδομένων ή τη δημιουργία ψεύτικων μεταδόσεων.

Το πιο σημαντικό αυτοματοποιημένο εργαλείο, με διαφορά, για ασφάλεια δικτύου και επικοινωνιών είναι η κρυπτογράφηση. Με συμβατική κρυπτογράφηση, τα δύο μέρη μοιράζονται ένα μοναδικό κλειδί κρυπτογράφησης/ αποκρυπτογράφησης. Η κυριότερη πρόκληση με τη συμβατική κρυπτογράφηση είναι η διανομή και η προστασία των κλειδιών. Ένα σχήμα κρυπτογράφησης δημόσιου κλειδιού περιλαμβάνει δύο

κλειδιά, ένα για κρυπτογράφηση και ένα για αποκρυπτογράφηση. Το ένα από τα κλειδιά διατηρείται από τον

ιδιοκτήτη κρυφό και το άλλο είναι δημόσιο.

Η συμβατική κρυπτογράφηση και η κρυπτογράφηση δημόσιου κλειδιού συχνά συνδυάζονται σε εφαρμογές ασφαλούς διαδικτύωσης. Η συμβατική κρυπτογράφηση χρησιμοποιείται για να κρυπτογραφεί δεδομένα, χρησιμοποιώντας ένα μίας χρήσης ή μικρής διάρκειας κλειδί συνόδου (session key). Το κλειδί συνόδου μπορεί να διανεμηθεί από ένα έμπιστο κέντρο διανομής κλειδιού ή να μεταδοθεί σε κρυπτογραφημένη μορφή χρησιμοποιώντας κρυπτογράφηση δημόσιου κλειδιού. Η κρυπτογράφηση δημόσιου κλειδιού διαθέτει την επιπλέον δυνατότητα να δημιουργεί ψηφιακές υπογραφές, οι οποίες μπορούν να πιστοποιήσουν την πηγή των μεταδομένων μηνυμάτων!

2.2.1 Απαιτήσεις ασφάλειας και επιθέσεις

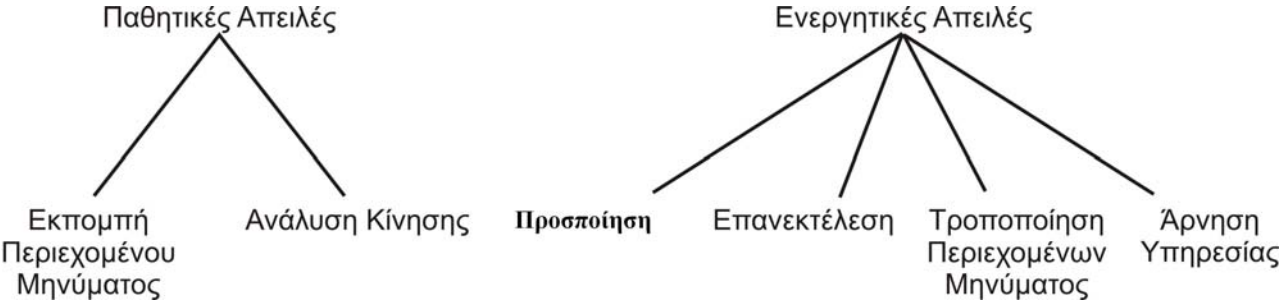
Για να καταλάβουμε τους τύπους των απειλών στην ασφάλεια, πρέπει να έχουμε έναν προσδιορισμό των απαιτήσεων ασφαλείας. Η ασφάλεια υπολογιστή και δικτύου απευθύνονται σε τρεις απαιτήσεις:

• Εμπιστευτικότητα: Απαιτεί τα δεδομένα να είναι προσβάσιμα για ανάγνωση μόνο από πιστοποιημένες ομάδες. Αυτός ο τύπος πρόσβασης περιλαμβάνει εκτύπωση, απεικόνιση και άλλες μορφές εμφάνισης.

• Ακεραιότητα: Απαιτεί τα δεδομένα να μπορούν να τροποποιηθούν μόνο από πιστοποιημένες ομάδες. Η τροποποίηση περιλαμβάνει εγγραφή, αλλαγή, αλλαγή κατάστασης, διαγραφή και δημιουργία.

• Διαθεσιμότητα: Απαιτεί τα δεδομένα να είναι διαθέσιμα μόνο σε πιστοποιημένες ομάδες

Μία χρήσιμη κατηγοριοποίηση των επιθέσεων στην ασφάλεια δικτύου αποτελούν τόσο οι παθητικές όσο και οι ενεργητικές απειλές (Σχήμα 2.1).



Σχήμα 2.1

Την ασφάλεια στο διαδίκτυο θα την ξανασυναντήσουμε στο τέταρτο κεφάλαιο για το πρωτόκολλο SSL (Secure Socket Layer) ή Ασφαλές Επίπεδο Υποδοχών. Το πρωτόκολλο αυτό είναι ένα από τα γνωστότερα πρωτόκολλα ασφαλείας που χρησιμοποιούνται για την διεκπεραίωση συναλλαγών στο Διαδίκτυο.

2.3 Κρυπτογραφία

Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη κρύπτο – κρυφός και την λέξη λόγος. Είναι ο τομέας που ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη.

2.3.1 Ιστορική αναδρομή κρυπτογραφίας

Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα που έχουμε αναφορές της στο ιστορικό Πολύβιο και συνεχίζεται στον Ιούλιο Καίσαρα. Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Ο πίνακας αντιστοιχίσεις των γραμμάτων, έχοντας ως κλειδί το 3, φαίνεται παρακάτω:

Το γράμμα	a	b	c	d	e	f	g	h	i	j	k	v	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Αντικαθίσταται από το γράμμα	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3

Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης. Η κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με σκοπό την διαφύλαξη εθνικών μυστικών και στρατηγικών. Όσο πιο πολύτιμα τα μυστικά τόσο πιο μεγάλη αξία αποκτούσε η ασφαλής φύλαξή τους. Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά.

Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών.

Δεν θα ήταν υπερβολή να πούμε ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξαιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA που χρησιμοποίησαν οι Άγγλοι για να αποκρυπτογραφούν τα μηνύματα του Γερμανικού επιτελείου προς τις αγέλες των υποβρυχίων τους στη Μεσόγειο αλλά και τον Ατλαντικό ωκεανό.

Από την δεκαετία του 60 και μετά η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω της ραγδαίας ανάπτυξης των υπολογιστών, αλλά και των τηλεπικοινωνιών. Έτσι λοιπόν, υπήρξε η ανάγκη για προστασία δεδομένων σε ψηφιακή μορφή. Αρχίζοντας με την εργασία του Feistel στην IBM στις αρχές της δεκαετίας του '70 και καταλήγοντας το 1977 με την υιοθέτηση του Αμερικανικού ομοσπονδιακού προτύπου για την επεξεργασία των πληροφοριών την κρυπτογράφηση των μη-διαβαθμισμένων πληροφοριών, τον αλγόριθμο DES. Παραμένει μέχρι σήμερα το τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα σε όλο τον κόσμο.

Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια τής κρυπτογραφίας δημοσίου κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό οι κρυπταναλυτές σήκωσαν τα μανίκια και άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα ασφαλές! Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν και η ψηφιακή υπογραφή.

2.3.2 Κρυπτολογία

Η Κρυπτολογία χωρίζεται σε 2 επιμέρους ενότητες:

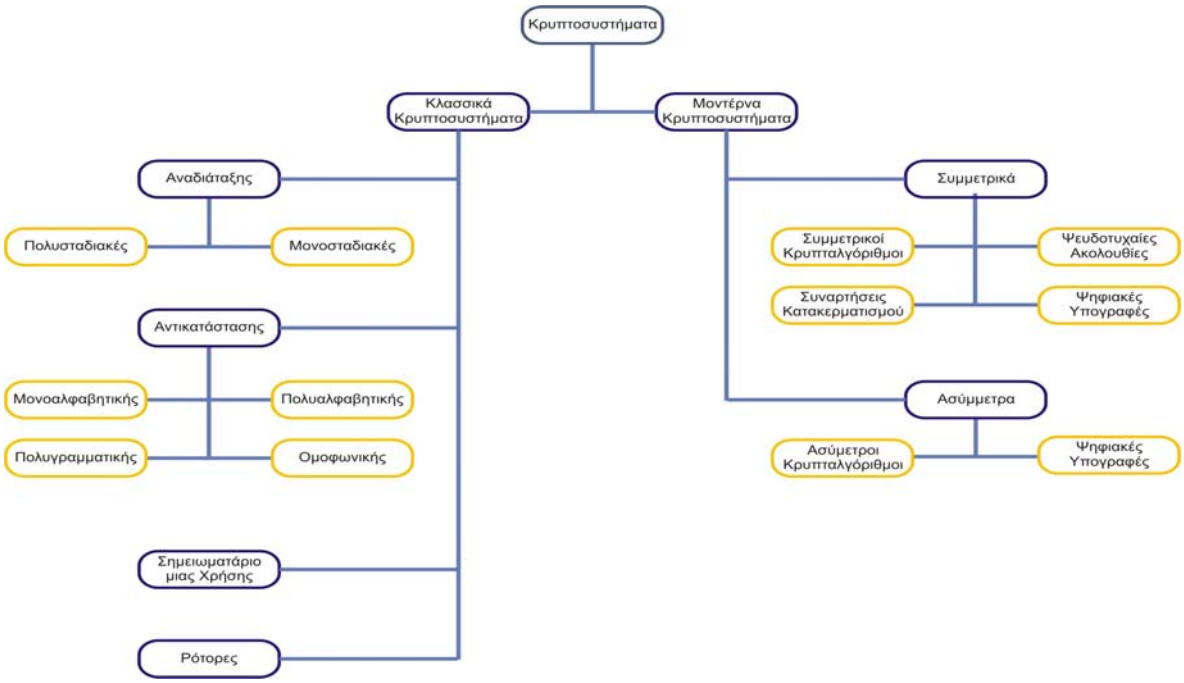
1. *Κρυπτογραφία*: η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας
2. *Κρυπτανάλυση*: η επιστήμη που ασχολείται με την ανάλυση και την διάσπαση των Κρυπτοσυστημάτων

1. Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

- *Εμπιστευτικότητα*: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- *Ακεραιότητα*: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- *Μη αποποίηση*: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- *Αυθεντικοποίηση*: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

2. Στην κρυπτανάλυση ασχολείται με τα κρυπτοσυστήματα που χωρίζονται σε 2 μεγάλες κατηγορίες τα οποία είναι τα εξής (Σχήμα 2.2):

- ✓ α) τα Κλασσικά Κρυπτοσυστήματα
- ✓ β) τα Μοντέρνα Κρυπτοσυστήματα

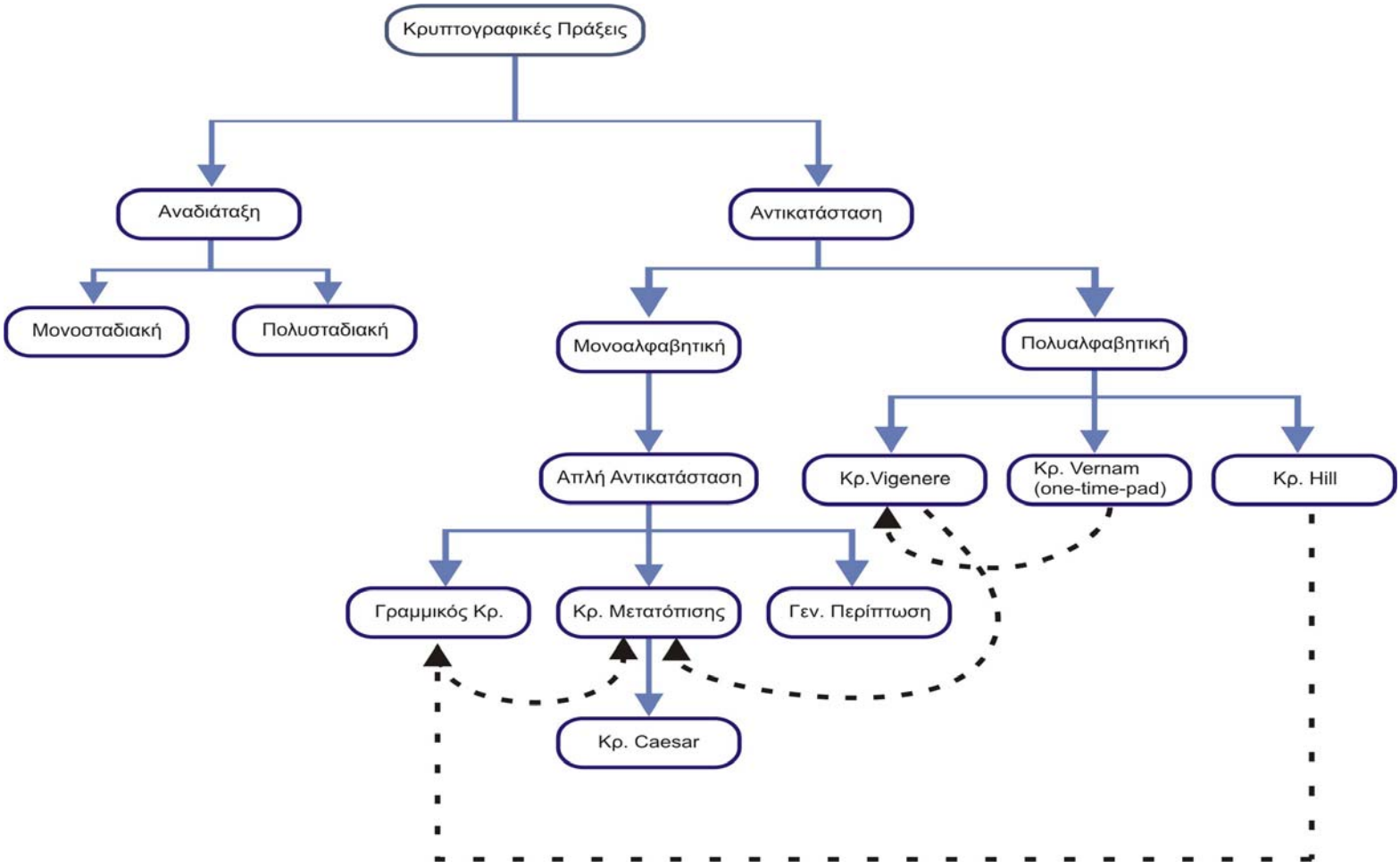


Σχήμα 2.2

2.4 Τα Κλασσικά Κρυπτοσυστήματα

Τα Κλασσικά Κρυπτοσυστήματα χωρίζονται σε 2 κατηγορίες οι οποίες είναι τα εξής (Σχήμα 2.3):

I. αναδιάταξη (α. Πολυσταδιακές και β. Μονοσταδιακές)
II. αντικατάσταση (α. Μονοαλφαβητικής, β. Πολυαλφαβητικής, γ. Πολυγραμματικής, δ. Ομοφωνικής)



Σχήμα 2.3

2.4.1 Κρυπτοσυστήματα Αναδιάταξης

Τα κρυπτογραφήματα αντικατάστασης διατηρούν τη σειρά των συμβόλων του καθαρού κειμένου αλλά παραποιούν τα ίδια τα σύμβολα. Τα κρυπτογραφήματα αναδιάταξης αλλάζουν τη σειρά των συμβόλων, χωρίς να τα παραποιούν.

Η κρυπτογράφηση γίνεται ως εξής:

Αρχικά τοποθετούμε το καθαρό κείμενο σε έναν πίνακα. Από κάθε γραμμή αντλούμε τα γράμματα που απαρτίζουν το κρυπτογραφημένο κείμενο με διαφορετική σειρά που γράφεται στο καθαρό κείμενο. Με τον τρόπο αυτό καταφέρνουμε να αναδιατάξουμε τα γράμματα του καθαρού κειμένου για τη παραγωγή του κρυπτογραφήματος. Το κλειδί σε αυτή τη περίπτωση είναι η σειρά με την οποία λαμβάνουμε τα κρυπτογραφημένα σύμβολα και ο αριθμός των στηλών του πίνακα. Ένας τρόπος με τον οποίο μπορούμε να καθορίσουμε το κλειδί είναι χρησιμοποιώντας κωδικές λέξεις ή φράσεις των οποίων τα γράμματα καθορίζουν τη σειρά ανάλογα με τη θέση τους στην αλφάβητο.

Η παραβίαση και αυτού του κρυπτογραφήματος γίνεται με χρήση των στατιστικών ιδιοτήτων της χρησιμοποιούμενης γλώσσας και με εύρεση του μέγεθους του κλειδιού.

2.4.1.2 Κρυπτοσυστήματα Αντικατάστασης

Σε ένα *κρυπτογράφημα αντικατάστασης* κάθε γράμμα ή ομάδα γραμμάτων αντικαθίσταται από ένα άλλο γράμμα ή ομάδα γραμμάτων. Το παλαιότερο γνωστό κρυπτογράφημα τέτοιου είδους είναι το *κρυπτογράφημα Καίσαρα*. Σύμφωνα μ' αυτή τη μέθοδο το αλφάβητο του κρυπτογραφημένου κειμένου ολισθαίνει κατά 3 γράμματα. Γενικότερα, μπορεί να γίνει ολίσθηση κατά *k* γράμματα.

Στη περίπτωση αυτή το *k* είναι το κλειδί του κρυπτογραφήματος. Μπορούμε να ορίσουμε τη μέθοδο κρυπτογράφησης αντικαθιστώντας κάθε γράμμα με ένα άλλο γράμμα χρησιμοποιώντας έναν οποιοδήποτε τυχαίο αλγόριθμο.

Στη περίπτωση αυτή η μέθοδος ονομάζεται *μονοαλφαβητική αντικατάσταση* και το κλειδί είναι η ακολουθία των γραμμάτων που αντιστοιχεί σε όλη την αλφάβητο. Ενώ η παραπάνω μέθοδος φαίνεται εκ πρώτης όψεως ασφαλής, εντούτοις, χρησιμοποιώντας τις στατιστικές ιδιότητας μιας γλώσσας μπορούμε εύκολα να σπάσουμε τον κώδικα.

2.5 ΤΑ ΜΟΝΤΕΡΝΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

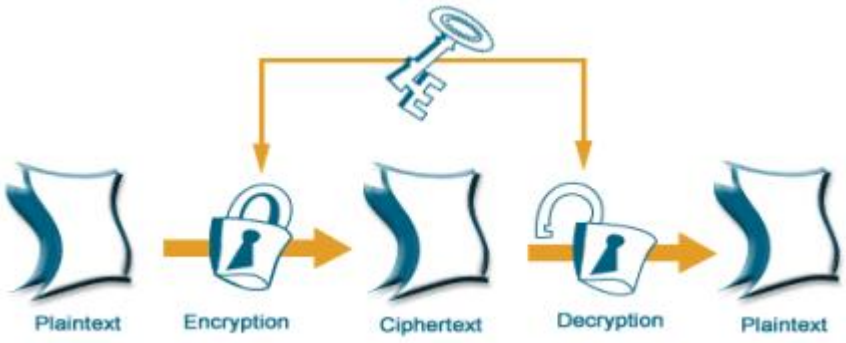
Τα Μοντέρνα Κρυπτοσυστήματα χωρίζονται σε 2 κατηγορίες οι οποίες είναι τα εξής:

I. Συμμετρικά Κρυπτοσυστήματα
II. Ασύμμετρα Κρυπτοσυστήματα

2.5.1 Συμμετρική κρυπτογραφία

Εισαγωγή για την Συμμετρική Κρυπτογραφία

Χρησιμοποιεί η συμμετρική κρυπτογραφία το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση (Σχήμα α). Αρχικά, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.



Σχήμα α : Συμμετρική Κρυπτογραφία

Στη συμμετρική Κρυπτογραφία υπάρχουν αρκετοί αλγόριθμοι, ο πιο γνωστός είναι ο Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών δηλ. αυτά που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT.

Κανόνες Συμμετρικής Κρυπτογραφίας

Η συμβατική κρυπτογραφία (conventional cryptography) αναφερόμενη ως συμμετρική κρυπτογραφία (symmetric cryptography) ή κρυπτογραφία μυστικού κλειδιού (secret key cryptography) αποτελούσε το μοναδικό τύπο κρυπτογράφησης δημόσιου κλειδιού. Ένα σχήμα συμβατικής κρυπτογραφίας αποτελείται από πέντε επιμέρους οντότητες όπως φαίνεται στο παραπάνω σχήμα (Σχήμα α):

- Αρχικό κείμενο (plaintext): Αποτελείται από τα αρχικά μηνύματα ή 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 (chiphertext): Αυτό είναι το μετασχηματισμένο μήνυμα του κειμένου 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): Αυτός είναι απαραίτητα ο αλγόριθμος κρυπτογράφησης εκτελεσμένος αντίστροφα την διαδικασία, δηλαδή λαμβάνει το κρυπτογραφημένο κείμενο και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.

Οι αλγόριθμοι Κρυπτογράφησης

Οι περισσότερο συχνά χρησιμοποιημένοι συμβατικοί αλγόριθμοι κρυπτογράφησης είναι οι κρυπτογραφήσεις τμημάτων. Μια κρυπτογράφηση τμήματος επεξεργάζεται την καθαρή είσοδο σε καθορισμένου μεγέθους τμήματα και παράγει ένα τμήμα κρυπτογραφημένου κειμένου ίσου μεγέθους με κάθε τμήμα καθαρού κειμένου. Παρακάτω θα δούμε τους πιο σημαντικούς αλγόριθμους

Γενικά για τον αλγόριθμο Data Encryption Standard

Το πρότυπο κρυπτογράφησης δεδομένων **Data Encryption Standard** (DES) είναι ένας αλγόριθμος συμμετρικής κρυπτογράφησης (είναι μια μέθοδος κρυπτογράφησης για τις πληροφορίες) που επιλέχθηκε επίσημα για την χρήση του από τον οργανισμό Federal Information Processing Standard (FIPS) στις Ηνωμένες Πολιτείες το 1976, και το οποίο στη συνέχεια χρησιμοποιήθηκε ευρέως διεθνώς. Ο αλγόριθμος αρχικά αμφισβητήθηκε, όσον αφορά σε απόρρητες πληροφορίες του σχεδιασμού στοιχείων, το σχετικά μικρό μήκος του κλειδιού (short key length) και την έμμεση ανάμειξη της Υπηρεσίας Εθνικής Ασφάλειας (National Security Agency NSA). Ο αλγόριθμος DES κατά συνέπεια έγινε αντικείμενο έντονης ακαδημαϊκής έρευνας, και παρακίνησε τη σύγχρονη κατανόηση του κρυπτογραφήματος (block ciphers) και της κρυπτολογικής ανάλυσής του.

Ο αλγόριθμος DES θεωρείται σήμερα επισφαλής για πολλές εφαρμογές. Αυτό οφείλεται κυρίως στο γεγονός ότι το μέγεθος του κλειδιού (56 bit) είναι πάρα πολύ μικρό. Κλειδιά του αλγορίθμου DES έχουν αποκωδικοποιηθεί σε λιγότερο από 24 ώρες. Υπάρχουν επίσης μερικά αναλυτικά αποτελέσματα τα οποία αποδεικνύουν θεωρητικές αδυναμίες του κρυπτογραφήματος, οι οποίες ωστόσο στην πράξη δεν μπορούν να αποδειχτούν. Ο αλγόριθμος πιστεύεται ότι στην πράξη είναι ασφαλής υπό την μορφή τριπλού DES (Triple DES), αν και υπάρχουν θεωρητικές αντιρρήσεις. Τα τελευταία χρόνια, η κρυπτογραφία έχει διαδεχθεί από προηγμένα πρότυπα κρυπτογράφησης, το πρότυπο Advanced Encryption Standard (AES).

Σε κάποια έγγραφα τεκμηρίωσης, γίνεται διάκριση ανάμεσα στο DES ως πρότυπο και στον αλγόριθμο που είναι γνωστός ως DEA (Data Encryption Algorithm – Αλγόριθμος Κρυπτογράφησης Δεδομένων).

Η ιστορία του αλγορίθμου Des

Ο αλγόριθμος DES δημιουργήθηκε στης αρχές της δεκαετίας του '70. Αργότερα το 1972, με την ολοκλήρωση μελέτης για τις ανάγκες ασφάλειας των υπολογιστών της Αμερικανικής Κυβέρνησης, το σώμα Αμερικανικών Προτύπων NBS (National Bureau of Standards) προσδιόρισε την ανάγκη ύπαρξης ενός κοινού πρότυπου για την κρυπτογράφηση των μη απόρρητων και ευαίσθητων πληροφοριών για όλη την

κυβέρνηση. Έτσι, στις 15 Μαΐου 1973, μετά από σύσκεψη με την NSA, το NBS ζήτησε τις προτάσεις για ένα πρότυπο κρυπτογράφησης που θα ικανοποιούσε τα αυστηρά κριτήρια σχεδιασμού του. Εντούτοις, καμία από τις υποβαλλόμενες προτάσεις δεν αποδείχθηκε κατάλληλη. Ένα δεύτερο αίτημα εκδόθηκε στις 27 Αυγούστου 1974. Αυτή τη φορά, η IBM υπέβαλε μία πρόταση που κρίθηκε αποδεκτή, και ένα πρότυπο κρυπτογράφησης αναπτύχθηκε κατά την διάρκεια της περιόδου 1973-1974 βασισμένο σε έναν προηγούμενο αλγόριθμο, το πρότυπο Horst Feistel's Lucifer. Η ομάδα της IBM για τον σχεδιασμό και την ανάλυση του κρυπτογραφήματος περιλάμβανε τους Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith, και Bryant Tuckerman.

Η συμμετοχή NSA για το σχεδιασμό του DES

Στις 17 Μαρτίου 1975, το προτεινόμενο τον αλγόριθμο DES δημοσιεύθηκε στον ομοσπονδιακό κατάλογο. Δημόσια σχόλια ζητήθηκαν, και μέσα στον επόμενο χρόνο διοργανώθηκαν δύο ανοικτά εργαστήρια προκειμένου να συζητηθούν τα προτεινόμενα πρότυπα. Κριτική εκφράστηκε από τα διάφορα συμβαλλόμενα μέρη, που περιλαμβάνουν τους πρωτοπόρους στα δημόσια κλειδιά (public-key) πρότυπα κρυπτογραφίας Martin Hellman και Whitfield Diffie, οι οποίοι ανέφεραν ένα περιορισμένο μήκος κλειδιού και μυστήριων «S-boxes» ως στοιχεία της ανάρμοστης παρέμβασης από το NSA.

Η υποψία ήταν ότι ο αλγόριθμος ήταν συγκαλυμμένα αποδυναμωμένος από την NSA έτσι ώστε αυτοί - αλλά κανένας άλλος - να μπορούν εύκολα να διαβάσουν τα κρυπτογραφημένα μηνύματα. Ο Alan Konheim (ένας από τους σχεδιαστές DES) σχολίασε «Στείλαμε τα S-boxes στην Ουάσιγκτον. Επέστρεψαν και ήταν όλα διαφορετικά». Η υπηρεσία United States Senate Select Committee on Intelligence κλήθηκε να ερευνήσει τις ενέργειες της NSA προκειμένου να καθορίσει εάν είχε υπάρξει οποιαδήποτε ανάρμοστη συμμετοχή. Στην αταξινόμητη περίληψη των συμπερασμάτων τους, που δημοσιεύθηκε το 1978,
η Επιτροπή έγραψε:

«Στην ανάπτυξη του DES, η NSA έπεισε την IBM ότι ένα μειωμένο βασικό μέγεθος κλειδιού θα ήταν ικανοποιητικό. Βοήθησε έμμεσα στην ανάπτυξη των S-box δομών και επιβεβαίωσε ότι το τελικό DES ήταν, στο καλύτερο της γνώσης τους, απαλλαγμένο από οποιαδήποτε στατιστική ή μαθηματική αδυναμία. »

Εντούτοις, βρήκε επίσης ότι

«Η NSA δεν πείραξε το σχέδιο του αλγορίθμου με κανένα τρόπο. Η IBM εφεύρε και σχεδίασε τον αλγόριθμο, έλαβε όλες τις σχετικές αποφάσεις σχετικά με αυτόν, και συμφώνησε ότι το επιλεγμένο βασικό μέγεθος ήταν περισσότερο από επαρκές για όλες τις εμπορικές εφαρμογές για τις οποίες το DES προορίστηκε. »

Ένα άλλο μέλος της ομάδας DES, ο Walter Tuchman, ανέφερε:

«Αναπτύξαμε τον αλγόριθμο DES εξ ολοκλήρου μέσα στην IBM χρησιμοποιώντας IBMers. Το NSA δεν παρενέβη στο ελάχιστο!»

Μερικές από τις υποψίες για τις κρυμμένες αδυναμίες των S-boxes καθησυχάστηκαν το 1990, με την ανεξάρτητη ανακάλυψη και την ανοικτή δημοσίευση από τους Eli Biham και Adi Shamir της διαφορικής κρυπτολογικής ανάλυσης, μια γενικής μεθόδου για το σπάσιμο κρυπτογραφικών block.

Τα S-boxes του DES ήταν ανθεκτικότερα στην επίθεση από εάν ήταν επιλεγμένα τυχαία, προτείνοντας έντονα ότι η IBM ήξερε για την τεχνική από τη δεκαετία του '70. Αυτό ήταν πράγματι η αλήθεια - το 1994, ο Don Coppersmith δημοσίευσε τα αρχικά κριτήρια σχεδιασμού για τα S-boxes. Σύμφωνα με το Steven Levy, οι ερευνητές της IBM Watson ανακάλυψαν τις διαφορικές κρυπταναλυτικές επιθέσεις το 1974 και κλήθηκαν από την NSA να κρατήσουν την τεχνική μυστική.

Ο Coppersmith εξηγεί:

«Αυτό έγινε επειδή η διαφορική κρυπτολογική ανάλυση μπορεί να είναι ένα πολύ ισχυρό εργαλείο, που χρησιμοποιείται ενάντια σε πολλά σχέδια, και υπήρξε ανησυχία ότι τέτοιες πληροφορίες γνωστές στο δημόσιο τομέα θα μπορούσαν να έχουν επιπτώσεις στην εθνική ασφάλεια.»

Ο Levy αναφέρει:

«Μας ζήτησαν να χαρακτηρίσουμε όλα τα έγγραφά μας εμπιστευτικά… Τα αριθμήσαμε και τα ασφαλίσαμε στα χρηματοκιβώτια, επειδή θεωρήθηκαν απόρρητα έγγραφα της Κυβέρνησης. Μας είπαν κάντε το. Έτσι το έκανα».

Ο ίδιος ο Shamir σχολίασε:

«Θα έλεγα ότι, αντίθετα προς αυτό που μερικοί άνθρωποι θεωρούν, δεν υπάρχει κανένα στοιχείο ότι το DES αλλοιώθηκε έτσι ώστε το βασικό σχέδιο να αποδυναμωθεί.»

Η άλλη κριτική - ότι το μήκος του κλειδιού ήταν πάρα πολύ σύντομο - υποστηρίχθηκε από το γεγονός ότι ο λόγος που δόθηκε από το NSA για τη μείωση του μήκους κλειδιού από 64 bit σε 56 ήταν ότι τα άλλα 8 bit θα μπορούσαν να χρησιμεύσουν ως τα κομμάτια ισότητας, τα οποία φάνηκαν κάπως αληθοφανή. Ευρέως θεωρήθηκε ότι η απόφαση της NSA παρακινήθηκε από την πιθανότητα ότι θα ήταν σε θέση να αντιμετωπίσουν μια επίθεση σε ένα κλειδί 56 bit αρκετά έτη σε προγενέστερο χρόνο πριν από τον υπόλοιπο κόσμο.

Ο αλγόριθμος ως πρότυπο

Παρά τις κριτικές, το DES εγκρίθηκε ως ομοσπονδιακά πρότυπο το Νοεμβρίου του 1976, και δημοσιεύθηκε στις 15 Ιανουαρίου 1977 ως FIPS PUB 46, κατάλληλο για χρήση σε όλα στα μη απόρρητα δεδομένα. Επιβεβαιώθηκε στη συνέχεια ως πρότυπο το 1983, το 1988 (που αναθεωρήθηκε ως FIPS-46-1), το 1993 (FIPS-46-2), και πάλι το 1998 (FIPS-46-3), τα τελευταία που ορίζουν «τριπλό DES».

Στις 26 Μαΐου 2002, το DES εκτοπίστηκε τελικά από το AES, το προηγμένο πρότυπο κρυπτογράφησης, μετά από έναν δημόσιο ανταγωνισμό. Ακόμη και το 2004, ωστόσο, το DES παραμένει σε διαδεδομένη χρήση. Στις 19 Μαΐου 2005, το FIPS 46-3 αποσύρθηκε επίσημα, αλλά η NIST έχει εγκρίνει το τριπλό DES έως το 2030 για τις ευαίσθητες κυβερνητικές πληροφορίες.

Μια άλλη θεωρητική επίθεση, η γραμμική κρυπτολογική ανάλυση, δημοσιεύθηκε το 1994, αλλά ήταν μια σφοδρή επίθεση το 1998 που κατέδειξε ότι το DES θα μπορούσε να πληγεί πρακτικά, και έδωσε έμφαση στην ανάγκη για έναν αλγόριθμο αντικατάστασης.

Η δημιουργία του DES θεωρείται καταλυτικής σημασίας για την ακαδημαϊκή μελέτη του συστήματος κρυπτογραφίας, ιδιαίτερα όσον αφορά στις μεθόδους για την αποκρυπτογράφηση το κρυπτογραφικών block. Σύμφωνα με μια δημοσκόπησης της NIST για τα DES:

Το DES μπορεί να θεωρηθεί ότι αποτέλεσε την αρχή για τη μη στρατιωτική μελέτη και την ανάπτυξη των αλγορίθμων κρυπτογράφησης. Στη δεκαετία του '70 υπήρχαν ελάχιστοι κρυπτογράφοι, εκτός από εκείνους στις στρατιωτικές ή στις υπηρεσίες νοημοσύνης, και λίγη ακαδημαϊκή μελέτη του συστήματος κρυπτογραφίας. Υπάρχουν τώρα πολλοί ακαδημαϊκά δραστήριοι κρυπτογράφοι, τμήματα μαθηματικών με ισχυρά προγράμματα στο σύστημα κρυπτογραφίας, και εμπορικές επιχειρήσεις και σύμβουλοι ασφάλειας πληροφοριών. Μια γενιά κρυπτοαναλυτών έχει αφιερώσει μεγάλη προσπάθεια για το σπάσιμο του αλγορίθμου DES.

Σύμφωνα με τα λεγόμενα του Bruce Schneier

«το DES έκανε περισσότερα για να δραστηριοποίηση τον τομέα της κρυπτολογικής ανάλυσης από οτιδήποτε άλλο. Τώρα υπάρχει ένας αλγόριθμος προς μελέτη.»

Ένα αρκετά μεγάλο μερίδιο της βιβλιογραφίας στο σύστημα κρυπτογραφίας στη δεκαετία του '70 και τη δεκαετία του '80 ασχολήθηκε με το DES, και το DES είναι το πρότυπα ενάντια στα οποία κάθε κλειδί συμμετρικό αλγόριθμο συγκρίνεται πάντα.

Παρακάτω θα δούμε το χρονολόγιο του αλγορίθμου DES

1. 15 Μαΐου 1973:	**Η NBS δημοσιεύει το πρώτο αίτημα για έναν τυποποιημένο αλγόριθμο κρυπτογράφησης**
2. 27 Αυγούστου 1974:	**Η NBS δημοσιεύει το δεύτερο αίτημα για τους αλγορίθμους κρυπτογράφησης**
3. 17 Μαρτίου 1975:	**Το DES δημοσιεύεται στον ομοσπονδιακό κατάλογο για σχολιασμό**
4. Αύγουστος 1976:	**Πρώτο εργαστήριο σχετικά με το DES**
5. Σεπτέμβριος 1976:	**Δεύτερο εργαστήριο, που συζητά τις μαθηματικές βάσεις του DES**
6. Νοέμβριος 1976:	**Το DES εγκρίνεται ως πρότυπο**
7. 15 Ιανουαρίου 1977:	**Το DES δημοσιεύεται ως FIPS πρότυπο FIPS ΜΠΑΡ 46**
8. 1983:	**Το DES επιβεβαιώνεται για πρώτη φορά**
9. 1986:	**Το Videocipher II, ένα δορυφορικό τηλεοπτικό σύστημα TV που βασίζεται σε DES αρχίζει να χρησιμοποιείται από την HBO**
10. 22 Ιανουαρίου 1988:	**το DES επιβεβαιώνεται για δεύτερη φορά ως FIPS 46-1, εκτοπίζοντας το FIPS PUB 46**
11. Ιούλιος 1990:	**Οι Biham και Shamir ανακαλύπτουν πάλι τη διαφορική κρυπτολογική ανάλυση, και την εφαρμόζουν σε ένα κρυπτογραφικό σύστημα DES.**
12. 1992:	**Οι Biham και Shamir δημοσιεύουν την διαφορική κρυπτολογική ανάλυση.**
13. 30 Δεκεμβρίου 1993:	**Το DES επιβεβαιώνεται για την τρίτη φορά ως FIPS 46-2**
14. 1994:	**Η πρώτη πειραματική κρυπτολογική ανάλυση DES εκτελείται χρησιμοποιώντας τη γραμμική κρυπτολογική ανάλυση (Matsui, 1994).**
15. Ιούνιος 1997:	**Το πρόγραμμα DESCHALL σπάζει ένα μήνυμα που κρυπτογραφείται με DES για πρώτη φορά στο κοινό.**
16. Ιούλιος 1998:	**Το DES Cracker της EFF (Deep Crack) σπάζει ένα κλειδί DES σε 56 ώρες.**
17. Ιανουάριος 1999:	**Μαζί, οι Deep Crack και distributed.net σπάνε ένα κλειδί DES σε 22 ώρες και 15 λεπτά.**
18. 25 Οκτωβρίου 1999:	**Το DES επιβεβαιώνεται για την τέταρτη φορά ως FIPS 46-3, που διευκρινίζει την προτιμημένη χρήση τριπλού DES**
19. 26 Νοεμβρίου 2001:	**Το AES δημοσιεύεται σε FIPS 197**
20. 26 Μαΐου 2002:	**Τα πρότυπα AES γίνονται αποτελεσματικά**
21. 26 Ιουλίου 2004:	**Η απόσυρση του FIPS 46-3 (και άλλων σχετικών προτύπων) προτείνεται στον ομοσπονδιακό κατάλογο**
22. 19 Μαΐου 2005:	**Η NIST αποσύρει το FIPS 46-3**
23. 13 Ιανουαρίου 2007:	**Η βασισμένη σε FPGA παράλληλη μηχανή COPACOBANA of the University of Bochum and Kiel της Γερμανία, σπάει το DES σε 7.2 ημέρες με κόστος υλικού $10.000**

Αλγόριθμοι αντικατάστασης

Οι ανησυχίες για την ασφάλεια και τη σχετικά αργή λειτουργία του DES στο λογισμικό παρακίνησαν τους ερευνητές να προτείνουν ποικίλα εναλλακτικά σχέδια για block cipher, τα οποία άρχισαν να εμφανίζονται προς το τέλος της δεκαετίας του '80 και τις αρχές τις δεκαετίας του '90. Τα περισσότερα από αυτά τα σχέδια κράτησαν ως μέγεθος του DES τα 64-bit, και θα μπορούσαν να ενεργήσουν ως αντικατάσταση, αν και χρησιμοποίησαν τυπικά ένα κλειδί 64-bit ή 124-bit. Στην USSR εισήχθη ο αλγόριθμος GOST 28147-89, με μέγεθος block 64-bit και ένα κλειδί 256-bit, το οποίο χρησιμοποιήθηκε επίσης στη Ρωσία αργότερα.

Το ίδιο το DES μπορεί να προσαρμοστεί και να επαναχρησιμοποιηθεί σε ένα ασφαλέστερο σχέδιο. Πολλοί πρώην χρήστες DES χρησιμοποιούν τώρα Triple DES (TDES) που περιγράφηκε και αναλύθηκε από έναν από τους σχεδιαστές του DES. Περιλαμβάνει την εφαρμογή του DES τρεις φορές με δύο (2TDES) ή τρία (3TDES) διαφορετικά κλειδιά. Το TDES θεωρείται επαρκώς ασφαλές, αν και είναι αρκετά αργό. Μια λιγότερο ακριβή εναλλακτική λύση είναι το DES-X, το οποίο αυξάνει το μέγεθος του κλειδιού από XORing το πρόσθετο κλειδί υλικό πριν και μετά από DES. Το GDES ήταν μια εναλλακτική του DES μεταβλητή που προτάθηκε ως τρόπος να επιταχυνθεί η κρυπτογράφηση, αλλά αποδείχθηκε ευαίσθητο στη διαφορική κρυπτολογική ανάλυση.

Το 2001, μετά από έναν διεθνή διαγωνισμό, η NIST επέλεξε ένα νέο κρυπτογραφικό πρότυπο: τα πρότυπα AES, ως αντικατάσταση. Ο αλγόριθμος που επιλέχτηκε ως AES υποβλήθηκε από τους σχεδιαστές του με το όνομα Rijndael. Οι άλλες συμμέτοχες στην NIST επικράτησε το AES συμπεριλαμβάνεται επίσης και οι αλγόριθμοι RC6, Serpent, MARS, και Towfish.

Το DES είναι ένας αρχετυπικός κρυπτογραφικό block - ένας αλγόριθμος που παίρνει μια καθορισμένου μήκους σειρά αρχικό κείμενο (plaintext) bits και την μετασχηματίζει μέσω μιας σειράς περίπλοκων διαδικασιών σε ένα άλλο κρυπτογραφημένο μήνυμα (ciphertext) του ίδιου μήκους. Στην περίπτωση του DES, το μέγεθος του block είναι 64 bit. Το DES χρησιμοποιεί επίσης ένα κλειδί για να προσαρμόσει το μετασχηματισμό, έτσι ώστε η αποκρυπτογράφηση να μπορεί να εκτελεσθεί μόνο από εκείνους που ξέρουν το ιδιαίτερο κλειδί που χρησιμοποιείται για να κρυπτογραφηθεί. Το κλειδί αποτελείται φαινομενικά από 64 bit. Ωστόσο, μόνο 56 bit από αυτά χρησιμοποιούνται πραγματικά από τον αλγόριθμο. Οκτώ bit χρησιμοποιούνται απλώς για τον έλεγχο της ισότητας, και απορρίπτονται μετά. Ως εκ τούτου το αποτελεσματικό βασικό μήκος είναι 56 bit, και αναφέρεται συνήθως υπό αυτήν τη μορφή.

Όπως άλλα block ciphers, το DES από μόνο του δεν είναι ένας ασφαλής τρόπος κρυπτογράφησης αλλά πρέπει αντ' αυτού να χρησιμοποιηθεί σε έναν τρόπο λειτουργίας. Το Fips-81 διευκρινίζουν διάφορους τρόπους για τη χρήση με DES.

Περιγραφή του Αλγορίθμου DES

Στο παρακάτω σχήμα 2.4(α) φαίνεται συνοπτικά ο τρόπος κρυπτογράφησης με τον αλγόριθμο DES. Το αρχικό κείμενο κρυπτογραφείται σε block των 64 bit, παράγοντας 64 bit κρυπτογραφημένου κειμένου. Ο αλγόριθμος που παραμετροποιείται με ένα κλειδί των 56 bit και έχει 19 διακεκριμένες φάσεις. Η πρώτη φάση είναι μια μετάθεση ανεξάρτητη από το κλειδί στο καθαρό κείμενο των 64 bit. Η τελευταία φάση είναι ακριβώς το αντίστροφο αυτής της μετάθεσης. Η προτελευταία φάση ανταλλάσσει τα 32 πιο αριστερά bit με τα 32 πιο δεξιά bit. Οι υπόλοιπες 16 φάσεις είναι λειτουργικά ταυτόσημες, αλλά παραμετροποιούνται με διαφορετικές συναρτήσεις του κλειδιού. Ο αλγόριθμος σχεδιάστηκε ώστε να επιτρέπει την πραγματοποίηση

της αποκρυπτογράφησης με το ίδιο κλειδί που γίνεται και η κρυπτογράφηση. Τα βήματα απλώς εκτελούνται με την αντίστροφη σειρά.

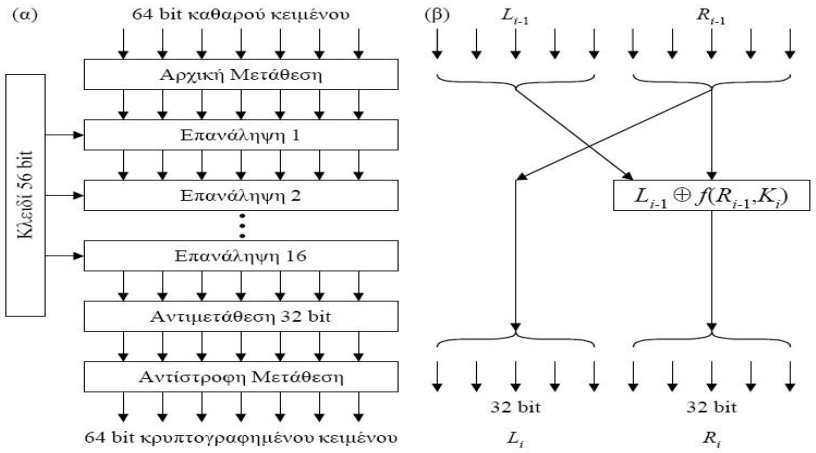
Η λειτουργία μιας από τις ενδιάμεσες φάσεις φαίνεται στο σχήμα 2.4(β). Κάθε τέτοια φάση παίρνει δύο εισόδους των 32 bit και παράγει δύο εξόδους των 32 bit. Η αριστερή έξοδος είναι απλώς ένα αντίγραφο της δεξιάς εισόδου. Η δεξιά έξοδος είναι η αποκλειστική διάζευξη (XOR) της αριστερής εισόδου και μιας συνάρτησης της δεξιάς εισόδου και του κλειδιού για αυτή τη φάση, K_i. Όλη η πολυπλοκότητα βρίσκεται σε αυτή τη συνάρτηση.

Συνοψίζοντας ακολουθούν οι παρακάτω τύποι:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

όπου $\oplus$ υποδηλώνει τη λογική XOR

Η συνάρτηση αποτελείται από τέσσερα στάδια τα οποία εκτελούνται σειριακά. Αρχικά, κατασκευάζεται ένας αριθμός E, μήκους 48 bit επεκτείνοντας τον R_{i-1} των 32 bit σύμφωνα με έναν σταθερό κανόνα μετάθεσης και επανάληψης. Στη συνέχεια, γίνεται αποκλειστική διάζευξη μεταξύ των E και K_i. Η έξοδος αυτή χωρίζεται έπειτα σε οκτώ ομάδες των 6 bit, που η κάθε μία τροφοδοτεί ένα διαφορετικό κουτί S. τα κουτιά S παράγουν 4 αντί για 6 bit εξόδου. Προφανώς διαφορετικές είσοδοι μπορούν να παράγουν την ίδια έξοδο. Το αποτέλεσμα είναι μια λίστα από 8 αριθμούς των 4 bit. Τέλος, αυτά τα 32 bit περνούν μέσω ενός κουτιού P. Σε κάθε μία από τις 16 επαναλήψεις χρησιμοποιείται και ένα διαφορετικό κλειδί. Πριν ξεκινήσει ο αλγόριθμος, εφαρμόζεται μια μετάθεση των 56 bit στο κλειδί. Ακριβώς πριν από μια επανάληψη, το κλειδί χωρίζεται σε δύο μονάδες των 28 bit, κάθε μία από αυτές περιστρέφεται αριστερά κατά έναν αριθμό από bit που εξαρτάται από τον αριθμό της επανάληψης. Το K_i προκύπτει από αυτό το περιστρεμμένο κλειδί εφαρμόζοντας σε αυτό μια μετάθεση των 56 bit.



Σχήμα: 2.4 Πρότυπο κρυπτογράφησης δεδομένων DES. (α) Γενική περιγραφή. (β) Λεπτομέρεια μιας επανάληψης.

Ο αλγόριθμος Triple Data Encryption Standard (TDES)

Ο αλγόριθμος **(TDES)** ονομάζεται **Triple Data Encryption Standard** σε συντομογραφία TDES ή TDEA ή συνηθέστερα 3DES προτάθηκε αρχικά από τον W. Tuchman. Το 1985 ο αλγόριθμος 3DES, για πρώτη φορά για χρήση σε οικονομικές εφαρμογές προτυποποιήθηκε στο πρότυπο ANSI X9.17. Το 1999, με τη δημοσίευση του ως FIPS PUB 46-3, το TDES ενσωματώθηκε ως τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES.

Ο αλγόριθμος TDES ακολούθησε το πρότυπο 2DES , ο οποίος δεν αξιοποιήθηκε ευρέως αφού θεωρήθηκε ευάλωτος στις κρυπταναλυτικές επιθέσεις τύπου ενδιάμεσου (man-in-the-middle attack). Το TDES χρησιμοποιεί τρία κλειδιά και τρεις εκτελέσεις του αλγορίθμου DES. Ο αλγόριθμος ακολουθεί τη διαδοχή: κρυπτογράφηση αποκρυπτογράφηση, κρυπτογράφηση (EDE -encryption - decryption -ecryption):

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

όπου:

C = κρυπτογράφημα
P = αρχικό κείμενο
$E_K[X]$ = κρυπτογράφηση του X χρησιμοποιώντας κλειδί K
$D_K[Y]$ = αποκρυπτογράφηση του X χρησιμοποιώντας κλειδί K.

Η αποκρυπτογράφηση ακολουθεί ακριβώς την ίδια διαδικασία με τα κλειδιά σε αντίστροφη χρήση

$$P = D_{K1}[E_{K2}[D_{K3}[C]]]$$

Δεν υπάρχει κρυπτογραφική σημασία στη χρήση της αποκρυπτογράφησης για δεύτερο στάδιο. Το μοναδικό πλεονέκτημα είναι ότι επιτρέπει στους χρήστες του τριπλού DES να αποκρυπτογραφούν δεδομένα από τους χρήστες του απλού DES:

$$C=E_{K1}[D_{K1}[E_{K1}[P]]]=E_{K1}[P]$$

Με τρία διαφορετικά κλειδιά το πρότυπο TDES, διαθέτει ένα ουσιαστικό μήκους κλειδιού των 168-bit. Στα πλαίσια του FIPS 46-3 επιτρέπεται, επίσης τη χρήση δύο κλειδιών με KI = K3. Το γεγονός αυτό εξασφαλίζει ένα μήκος κλειδιού 112-bit. Το FIPS 46-3 περιλαμβάνει τις ακόλουθες οδηγίες για το TDES:

- Το TDES αποτελεί τον εγκεκριμένο από το FIPS επιλεγμένο συμβατικό αλγόριθμο κρυπτογράφησης.
- Ο αρχικός DES, χρησιμοποιεί ένα μοναδικό κλειδί των 56-bit, επιτρέπεται κάτω από το πρότυπο μονό για κληροδοτούμενα συστήματα. Τα νέα συστήματα, όμως, πρέπει να υποστηρίζουν το TDES.
- Οι κυβερνητικοί οργανισμοί των ΗΠΑ χρησιμοποιούν τον αλγόριθμο DES για κληροδοτούμενα συστήματα ενθαρρύνονται για τη μετάβαση σε TDES.
- Είναι αναμενόμενο ότι το TDES και το Advanced Encryption Standard – AES θα συνυπάρξουν ως FIPS εγκεκριμένοι αλγόριθμοι, επιτρέποντας την σταδιακή μετάβαση στο AES.

Επιπλέον ο αλγόριθμος TDES έχει μήκος κλειδιού 168-bit και οι επιθέσεις του εξαντλητικής αναζήτησης είναι πρακτικά ατελέσφορες. Συνεπώς ο TDES αναμένεται ότι θα αξιοποιείται ολοένα και περισσότερο τα επόμενα χρόνια, μέχρι την ολοκληρωτική μετάβαση στις επερχόμενες υλοποιήσεις του AES.

Advanced Encryption Standard – *AES*

Στην κρυπτογραφία, το προηγμένο πρότυπο κρυπτογράφησης **Advanced Encryption Standard** (AES), επίσης γνωστό ως Rijndael, είναι ένα block cipher που έχει υιοθετηθεί ως πρότυπο κρυπτογράφησης από

την Αμερικανική Κυβέρνηση. Έχει αναλυθεί εκτενώς και χρησιμοποιείται τώρα ευρέως παγκοσμίως όπως συνέβη με τον προκάτοχό του, τα πρότυπα κρυπτογράφησης δεδομένων Data Encryption Standard (DES). Ο αλγόριθμος AES αναγγέλθηκε από το εθνικό ίδρυμα προτύπων και τεχνολογίας (NIST) ως Αμερικανικό FIPS PUB 197 (FIPS 197) στις 26 Νοεμβρίου 2001 μετά από μια πενταετή διαδικασία τυποποίησης. Έγινε αποτελεσματικό ως προτύπο στις 26 Μαΐου 2002. Από το 2006, ο αλγόριθμος AES είναι ένας από τους δημοφιλέστερους αλγορίθμους που χρησιμοποιούνται στο συμμετρικό σύστημα της κρυπτογραφίας. Η κρυπτογραφία αναπτύχθηκε από δύο βέλγους κρυπτογράφους (cryptographers), από τον Joan Daemen και Vincent Rijmen, και υποβλήθηκε στην διαδικασία επιλογής του AES με το όνομα «Rijndael», ένας συνδυασμός των ονομάτων των εφευρετών. (Rijndael προφέρεται (IPA), το οποίο ηχεί σχεδόν όπως τη "Rhine doll".

Ανάπτυξη

Ο αλγόριθμος Rijndael ήταν μία βελτίωση ενός προηγούμενου σχεδίου από τους Daemen και Rijmen, του Τετραγώνου. Το τετράγωνο ήταν μια ανάπτυξη του Shark (είναι ένα σύστημα κρυπτογραφίας, το σύστημα Shark είναι ένα block cipher που έχει ένα 64-bit block και ένα 128-bit key size. Αποτελείται από έξι στρογγυλούς SP-δικτύου που εναλλάσσει τα κλειδιά συνδυάζοντας τα γραμμικά και μη γραμμικά σήματα μετασχηματισμού. Ο γραμμικός μετασχηματισμός χρησιμοποιεί μια μήτρα MDS που αντιπροσωπεύει έναν κώδικα διόρθωσης λάθους Reed-Solomon error correcting code προκειμένου να εγγυηθεί η καλή διάδοση του).

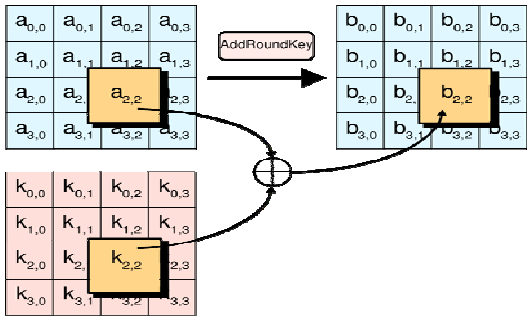
Αντίθετα από τον προκάτοχό του αλγορίθμου DES, ο Rijndael είναι ένα δίκτυο αντικατάσταση-μετάθεσης δικτύου, δηλ. όχι ένα δίκτυο του Feistel. Ο αλγόριθμος AES είναι γρηγορότερος στο λογισμικό και στο υλικό, είναι σχετικά εύκολο να εφαρμοστεί, και απαιτεί λίγη μνήμη. Σαν νέο πρότυπο κρυπτογράφησης, επεκτείνεται αυτήν την περίοδο σε μια ευρεία κλίμακα.

Περιγραφή του αλγορίθμου AES

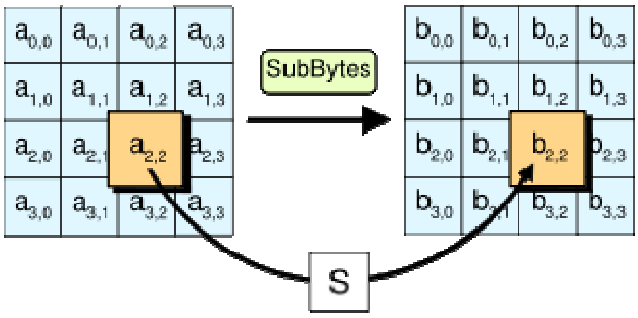
Για να κυριολεκτήσουμε, ο αλγόριθμος AES δεν είναι ακριβώς ο Rijndael (αν και στην πράξη χρησιμοποιούνται εναλλακτικά) δεδομένου ότι ο Rijndael υποστηρίζει μια μεγαλύτερη γραμμή του block και των key sizes; Ο αλγόριθμος AES έχει ένα block sizes των 128 bit και ένα key sizes 128, 192 ή 256 bits, ενώ ο Rijndael μπορεί να χρησιμοποιήσει μεγέθη κλειδιών (key sizes) και block σε ένα οποιοδήποτε πολλαπλάσιο του 32 bit, με ένα ελάχιστο των 128 bit και ένα μέγιστο 256 bit, αντίστοιχα. Το κλειδί επεκτείνεται χρησιμοποιώντας το βασικό πρόγραμμα του Rijndael. Οι περισσότεροι από τους υπολογισμούς του αλγορίθμου AES γίνονται σε έναν πρόσθετο πεπερασμένο πεδίο.

Ο αλγόριθμος AES λειτουργεί σε μια 4×4 γραμμή ψηφιολέξεων (bytes), χρησιμοποιώντας κατάλληλη συνθήκη (οι εκδόσεις Rijndael έχουν ένα μεγαλύτερο block μέγεθος τις πρόσθετες στήλες συνθηκών). Για την κρυπτογράφηση, κάθε κύκλος του αλγορίθμου AES (εκτός από τον τελευταίο κύκλο) αποτελείται από τέσσερα στάδια:

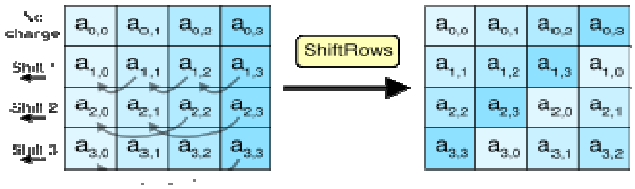
1. AddRoundKey - κάθε ψηφιολέξη(byte) της συνθήκης συνδυάζεται με το στρογγυλό κλειδί; Κάθε στρογγυλό κλειδί προέρχεται από το κρυπτογραφικό κλειδί χρησιμοποιώντας ένα κλειδί δρομολόγησης όπως βλέπουμε στο παρακάτω σχήμα.



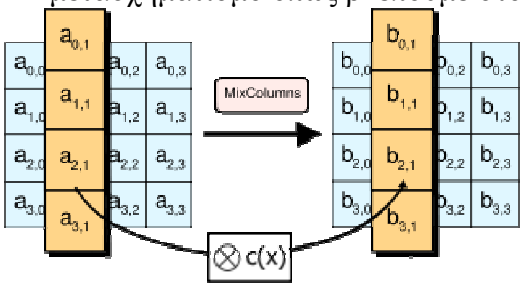
2. SubBytes - ένα μη γραμμικό βήμα αντικατάστασης όπου κάθε ψηφιολέξη αντικαθίσταται με άλλη σύμφωνα με έναν πρόγραμμα κλειδιών όπως βλέπουμε στο παρακάτω σχήμα.



3. ShiftRows - ένα βήμα αντικατάστασης-μετάθεσης όπου κάθε γραμμή των ψηφίων της συνθήκης μετατοπίζεται κυκλικά ορισμένα βήματα όπως βλέπουμε στο παρακάτω σχήμα.



4. MixColumns – η αντικατάσταση λειτουργεί όπως λειτουργεί στις στήλες της συνθήκης, που συνδυάζει τις τέσσερις ψηφιολέξεις (byte) σε κάθε στήλη χρησιμοποιώντας έναν γραμμικό μετασχηματισμό όπως βλέπουμε στο παρακάτω σχήμα.



Ο τελικός κύκλος αντικαθιστά το στάδιο MixColumns με μια άλλη περίπτωση στην χρονική περίοδο το AddRoundKey.

Ο αλγόριθμος Blowfish

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον από τον επιφανή κρυπτογράφο B.Schneier και καθιερώθηκε ως μία από τις δημοφιλέστερες εναλλακτικές λύσεις του DES. Είναι ένας Feistel cipher με μέγεθος block 64 bits και χαρακτηριστικό γνώρισμα του Blowfish αποτελεί το μήκος κλειδιού, το οποίο είναι μεταβλητό, μπορεί να λάβει τιμές έως 448-bit, αν και πρακτικά χρησιμοποιούνται κλειδιά των 128-bit. Ο Blowfish χρησιμοποιεί 16 γύρους.

Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα από τους ασφαλής αλγόριθμους.

RC2, RC4, RC5

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.

Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

Ο αλγόριθμος IDEA (International Data Encryption Algorithm)

Σε αυτό το σημείο αναρωτιόμαστε αφού το DES δεν είναι τόσο ασφαλές γιατί δεν ανακαλύφθηκαν νέοι αλγόριθμοι κρυπτογραφίας. Στη πραγματικότητα έχουν προταθεί πολύ νέοι αλγόριθμοι όπως BLOWFISH (Schneier, 1994), Crab (Kaliski και Robshaw, 1994), FEAL (Shimizu και Miyaguchi, 1988), KHAFRE (Merkle, 1991), LOKI91 (Brown et al., 1991), NEWDES (Scott, 1985), REDOC-II (Cusick και Wood,1991) και SAFER K64 (Massey, 1994). Ίσως ο πιο ενδιαφέρον και βασικός αλγόριθμος κρυπτογραφίας μετά το DES να είναι ο IDEA (international data encryption algorithm)
(Lai και Massey, 1990, και Lai, 1992).

Ο IDEA σχεδιάστηκε από δύο ερευνητές στην Ελβετία, οπότε δεν έχει την καθοδήγηση της NSA. Χρησιμοποιεί ένα κλειδί 128 bit οπότε δεν μπορεί να παραβιαστεί χρησιμοποιώντας μεγάλη υπολογιστική

ισχύ, για τα σημερινά δεδομένα αλλά και για τις επόμενες δεκαετίες. Σήμερα δεν υπάρχει γνωστός αλγόριθμος ή συσκευή που να μπορεί να παραβιάσει το IDEA.

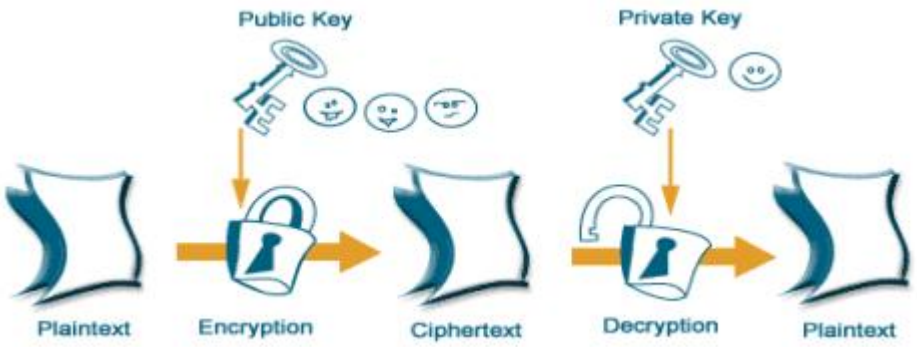
Η βασική δομή του αλγορίθμου μοιάζει με το DES στο γεγονός ότι στην είσοδο δέχεται 64 bit καθαρού κειμένου που παραμετροποιούνται με συνεχείς επαναλήψεις και στην έξοδο παράγει 64 bit κρυπτογραφημένου κειμένου. Επειδή η πολυπλοκότητα κάθε επανάληψης είναι μεγαλύτερη από το DES, ο IDEA χρειάζεται μόνο οκτώ επαναλήψεις. Ο αλγόριθμος μιας επανάληψης είναι ένας συνδυασμός πράξεων πάνω στις τέσσερις 16-αδες bit που αποτελούν μια είσοδο των 64 bit.

2.3.2.2 Ασύμμετρη Κρυπτογραφία

Εισαγωγή για την Ασύμμετρη Κρυπτογραφία

Διαφορετικά κλειδιά χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία, για την κρυπτογράφηση και την αποκρυπτογράφηση, το *δημόσιο* (public) και το *ιδιωτικό* (private) *κλειδί* αντίστοιχα (*Σχήμα β*). Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.



Σχήμα β: Ασύμμετρη κρυπτογραφία

Το 1976 οι Diffie και Hellman διατύπωσαν την βασική αρχή της κρυπτογραφίας δημόσιου κλειδιού, ενώ το 1977 οι Rivest, Shamir και Adleman δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων.

Για να αποκατασταθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν

το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης.

Ασύμμετρα Κρυπτοσυστήματα και Αυθεντικοποίηση Μηνυμάτων

Η κρυπτογράφηση έχει σαν σκοπό την προστασία από παθητικές επιθέσεις (passive attacks) και ενεργητικές επιθέσεις (active attacks). Οι παθητικές επιθέσεις στοχεύουν στην παραβίαση της εμπιστευτικότητας μηνυμάτων (eavesdropping) και οι ενεργητικές επιθέσεις κατά των μεταδιδόμενων δεδομένων και δοσοληψιών (falsification of data and transactions). Η υπηρεσία ασφάλειας η οποία παρέχει προστασία από τέτοιες κατηγορίες επιθέσεων, είναι γνωστή ως αυθεντικοποίηση μηνυμάτων (message authentication).

Η αυθεντικοποίηση μηνυμάτων είναι μία διαδικασία που επιτρέπει στους χρήστες μια ασφαλή ακεραιότητα (integrity), δηλαδή τη μη τροποποίηση των δεδομένων του μηνύματος, επισημαίνοντας την αυθεντικότητα (authenticity) της πηγής μετάδοσης. Αν το μήνυμα περικλείει και χρονοσήμανση (timestamp) διασφαλίζεται το γεγονός ότι το μήνυμα δεν έχει καθυστερήσει πέραν ενός "φυσιολογικού" ορίου και ότι δεν αποτελεί αναμετάδοση παλαιότερου μηνύματος. Υπάρχουν δυο περιπτώσεις στην αυθεντικοποίηση μηνυμάτων το πώς θα γίνει η μετάδοση του μηνύματος

1. Η Συμβατική Κρυπτογράφηση χρησιμοποιώντας την αυθεντικοποίηση είναι δυνατόν να επιτευχθεί απλώς με την χρήση της. Π.χ. έχουμε ένα μυστικό κλειδί το οποίο διαμοιράζονται ο αποστολέας και ο παραλήπτης τότε μονό ο αυθεντικός αποστολέας θα είναι σε θέση να κρυπτογραφήσει το μήνυμα επιτυχώς.
2. Αυθεντικοποίηση μηνυμάτων χωρίς κρυπτογράφηση παράγει μία ετικέτα μηνύματος (authentication tag), η οποία ενσωματώνει το μήνυμα προς μετάδοση το οποίο δεν είναι κρυπτογραφημένο μπορεί να είναι αναγνώσιμο στον προορισμό ανεξάρτητα από τη μέθοδο αυθεντικοποίησης στον προορισμό του.

Αλγόριθμοι για την Διαχείριση και Ανταλλαγή Κλειδιών

Diffie-Hellman

Το πρωτόκολλο *Diffie-Hellman* είναι ένας μηχανισμός ανταλλαγής κλειδιών και αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές δίκτυο.

Το πρωτόκολλο έχει δύο παραμέτρους: p και g.

Είναι και οι δύο δημοσιοποιημένοι και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες του συστήματος.

Η παράμετρος p είναι ένας πρώτος αριθμός και η παράμετρος g είναι ένας ακέραιος με την εξής ιδιότητα: για οποιοδήποτε ακέραιο αριθμό n στο διάστημα $[1, p-1]$,

υπάρχει αριθμός k τέτοιος ώστε $g^k = n \bmod p$.

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι πρώτες εκδόσεις του μηχανισμού Diffie-Hellman ήταν ευάλωτες σε επιθέσεις *man-in-the-middle*. Σε αυτή την επίθεση ο χρήστης C παρεμβάλλεται στην επικοινωνία των A και B και όταν ανταλλάσσουν τις δημόσιες τιμές τους τις αντικαθιστά με τις δικές του. Δηλαδή όταν ο A μεταδίδει την δημόσια τιμή του στον B, ο C την αντικαθιστά με την δικιά του και την στέλνει στον B. Ομοίως όταν ο B στέλνει την δημόσια τιμή του στον A. Σαν συνέπεια, οι C και A συμφωνούν για ένα μυστικό κλειδί και οι C και B συμφωνούν για ένα άλλο κλειδί. Έτσι ο C μπορεί να διαβάσει τα μηνύματα που μεταδίδουν ο A στον B και πιθανώς να τα τροποποιήσει πριν τα προωθήσει σε έναν από τους δύο.

Το 1992 αναπτύχθηκε μία ανανεωμένη έκδοση από τους Diffie, Van Oorschot και Wiener που υποστήριζε την πιστοποίηση της ταυτότητας των δύο πλευρών και είχε σαν σκοπό να καταπολεμήσει την επίθεση man-in-the-middle. Τα μηνύματα ανταλλάσσονται υπογεγραμμένα με τις ιδιωτικές κλείδες των A και B, ενώ χρησιμοποιούνται και πιστοποιητικά για την απόκτηση των σωστών δημοσίων κλείδων. Ο C ακόμα και αν είναι σε θέση να παρακολουθεί την επικοινωνία των A και B, δεν μπορεί να πλαστογραφήσει τα μηνύματα.

Αλγόριθμοι για Ασύμμετρα Κρυπτοσυστήματα

Οι πιο διαδεδομένοι αλγόριθμοι για ασύμμετρα κρυπτοσυστήματα είναι ο αλγόριθμος RSA και ο αλγόριθμος των Diffie-Hellman. Υπάρχουν επίσης και άλλοι δυο αλγόριθμοι ο Digital Signature Standard (DSS) και ο Elliptic- Curve Cryptography(ECC).

Αλγόριθμος RSA

Το 1977 αναπτύχθηκε ένα από τα πρώτα ασύμμετρα κρυπτοσυστήματα από τους R. Rivest, A. Shamir και L. Adleman στο MIT και το οποίο δημοσιεύτηκε για πρώτη φορά το 1978. Το RSA κυριάρχησε ως η πλέον μοναδική ευρέως αποδεκτή και εύκολα υλοποιημένη προσέγγιση για της κρυπτογράφησης των ασύμμετρων κρυπτοσυστήματων. Ο RSA είναι αλγόριθμος κρυπτογράφησης στον οποίο το αρχικό και το κρυπτογραφημένο κείμενο είναι ακέραιοι αριθμοί με τιμές μεταξύ 0 και n-1, για κάποιο *n*.

Η κρυπτογράφηση και η αποκρυπτογράφηση είναι της ακόλουθης μορφής για ένα αρχικό κείμενο M και για το αντίστοιχο κρυπτογραφημένο C συμβολίζονται ως ακολούθως:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Τόσο ο αποστολέας όσο και ο παραλήπτης θα πρέπει να γνωρίζουν τις τιμές των *n* και *e* και μόνον ο παραλήπτης πρέπει να γνωρίζει την τιμή του *d*. Ουσιαστικά ο RSA είναι ένας αλγόριθμος" για ασύμμετρο κρυπτοσύστημα με δημόσιο κλειδί KU={e,n} και ιδιωτικό κλειδί KR={d,n}. Για να είναι ικανοποιητικός αυτός ο αλγόριθμος για κρυπτογράφηση δημοσίου κλειδιού θα πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις:

- Είναι δυνατό να βρεθούν τιμές για τα e,d,n τέτοιες ώστε να ισχύει: $M^{ed} = M \bmod n$, για κάθε M<n.
- Είναι σχετικά εύκολο να υπολογιστούν τα M^e και C^d, για κάθε M<n.
- Είναι αδύνατο να προσδιοριστεί το *d*, δοθέντων των *e* και *n*.

Οι δύο πρώτες απαιτήσεις ικανοποιούνται εύκολα. Η τρίτη απαίτηση μπορεί να ικανοποιηθεί μόνο για μεγάλες τιμές των *e* και *n*.

Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς να διαρρεύσει σε τρίτους, είναι το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής καθώς οποιοσδήποτε γνωρίζει για την συναλλαγή και διαθέτει τα κατάλληλα μέσα, μπορεί να την καταγράψει και να αποκτήσει το κλειδί.

Κατέχοντας το κλειδί, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Η επικοινωνία για την μετάδοση του κλειδιού μπορεί να πραγματοποιηθεί με τη χρήση και άλλων μέσων (π.χ. τηλεφωνία), αλλά και πάλι δεν μπορεί να διασφαλιστεί η απόρρητη επικοινωνία των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" σ το δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Η παροχή ψηφιακών υπογραφών που δεν μπορούν να αποκηρυχθούν από την πηγή τους είναι ακόμη ένα από τα πλεονεκτήματα των ασύμμετρων κρυπτοσυστημάτων. Η πιστοποίηση ταυτότητας μέσω της συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Το αποτέλεσμα είναι ότι ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν υφίσταται τέτοιος κίνδυνος, καθώς μόνο ο ίδιος ο χρήστης γνωρίζει την ιδιωτική του κλείδα και είναι αποκλειστική ευθύνη του η φύλαξη της.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη. Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο.

Κεφάλαιο

«Δημόσιο Κλειδί»

3.1 Ορισμοί

3.2 Εισαγωγικά – Εισαγωγή βασικών όρων

3.3 Υπηρεσίες Διαχείρισης Πιστοποιητικών

3.4 Εφαρμογές της Υποδομής Δημόσιου Κλειδιού

3.1. Ορισμοί

Ακολουθούν ορισμοί όρων :

- Δημόσιο Κλειδί είναι ένα κλειδί γνωστό στον καθένα. Χρησιμοποιείται από τον αποστολέα για την κρυπτογράφηση του μηνύματος που πρόκειται να αποστείλει.
- Υποδομή Δημόσιων Κλειδιών – Public Key Infrastructure - PKI, σύμφωνα με την IETF (Internet Engineering Task Force), ορίζεται ως το σύνολο που απαρτίζεται από το λογισμικό, το υλισμικό, τους ανθρώπους, τις πολιτικές και τις διαδικασίες που απαιτούνται για τη δημιουργία, τη διαχείριση, την αποθήκευση, τη διανομή και την ανάκληση ψηφιακών πιστοποιητικών που περιέχουν Δημόσια Κλειδιά.
  - Ένα σύστημα Ψηφιακών Πιστοποιητικών, Υπηρεσιών Πιστοποίησης και άλλων Υπηρεσιών Καταγραφής που επιβεβαιώνουν και πιστοποιούν την αυθεντικότητα του κάθε συμμετέχοντος σε μια διαδικτυακή συναλλαγή και παράλληλα παρέχουν εγγύηση στην ασφάλεια της δραστηριότητας αυτής.
- Πιστοποίηση είναι η διαδικασία της επαλήθευσης ή της επιβεβαίωσης κάποιου αντικειμένου, δήλωσης, ή προσώπου όπως η αυθεντικότητα, δηλαδή ότι οι αξιώσεις που γίνονται από κάποιον ή για κάποιον είναι αληθινές. Στον τομέα της Ασφάλειας Υπολογιστικών Συστημάτων, πιστοποίηση είναι η διαδικασία επιβεβαίωσης της ψηφιακής ταυτότητας του αποστολέα ή παραλήπτη μιας επικοινωνίας, όπως π.χ. μιας αίτησης εισόδου σε ένα σύστημα. Το αντικείμενο της πιστοποίησης μπορεί να είναι ένα πρόσωπο, ένα υπολογιστικό σύστημα ή ένα υπολογιστικό πρόγραμμα.
- Υπηρεσίες Πιστοποίησης είναι εφαρμογές που παρέχουν την δυνατότητα πιστοποίησης της ταυτότητας κυριοτήτων σε ένα δίκτυο. Είναι χρήσιμες συνήθως σαν ένα πρώτο επίπεδο στην διαδικασία της εξουσιοδότησης, ορίζοντας αν ένας πελάτης μπορεί να χρησιμοποιήσει μια υπηρεσία και ποιο μέρος αυτής.

3.2 Εισαγωγικά – Εισαγωγή βασικών όρων

3.2.1 Παροχή Υπηρεσιών Πιστοποίησης (CSP), Αρχές Πιστοποίησης (CA) και Αρχές Καταχώρισης (RA).

Για τη διενέργεια ηλεκτρονικών συναλλαγών απαιτείται η οργάνωση και λειτουργία νέων φορέων παροχής επικοινωνιακών υπηρεσιών προστιθέμενης αξίας ώστε να επιτευχθεί ικανοποιητικό επίπεδο ασφάλειας. Οι φορείς αυτοί παλαιότερα αποκαλούνταν Έμπιστες Τρίτες Οντότητες (Trusted Third Parties – TTP) και σήμερα στη βιβλιογραφία αναφέρονται ως Παροχή Υπηρεσιών Πιστοποίησης (Certification Service Providers – CSP) αφού αξιοποιούν τις δυνατότητες, κυρίως των αλγορίθμων και αντιστοίχων ασύμμετρων κρυπτοσυστημάτων, με δημόσια κλειδιά τα οποία αποθηκεύονται σε Ψηφιακά Πιστοποιητικά (Digital Certificates).

Οι CSP παρέχουν τεχνική άλλα και νομική υποστήριξη για θέματα που σχετίζονται με την παραγωγή και διανομή των απαιτούμενων διακριτικών διασφάλισης και επαλήθευσης μιας ηλεκτρονικής δοσοληψίας. Το βασικό έργο των CSP αφορά την άρτια οργάνωση των μηχανισμών διαχείρισης ψηφιακών πιστοποιητικών ή απλώς πιστοποιητικών (certificates) για λόγους απλούστευσης. Οι CSP είναι οντότητες – φορείς που πρωταρχικό σκοπό έχουν να πιστοποιούν τεχνικά και νομικά την αντιστοίχηση της ταυτότητας (identity) μιας οντότητας (entity), όπως ενός φυσικού προσώπου, ενός εξυπηρέτη, μιας εφαρμογής, ή ενός ρόλου (role) με ένα δημόσιο κλειδί το οποίο περιέχεται σε ένα πιστοποιητικό. Ουσιαστικά οι CSP δραστηριοποιούνται για την παραγωγή,

αποθήκευση, αποστολή και ανάκληση πιστοποιητικών για την υποβοήθηση της επίτευξης μιας ασφαλούς ηλεκτρονικής επικοινωνίας.

Στα πλαίσια της λειτουργίας του, ένας CSP περιλαμβάνει τουλάχιστον μια Αρχή Πιστοποίησης και τουλάχιστον μια Αρχή Καταχώρισης :

1) Η Αρχή Πιστοποίησης – Certification Authority – CA :

Η CA αποτελεί ένα έμπιστο τμήμα του οργανισμού CSP και ασχολείται με την τεχνική διαχείριση των πιστοποιητικών για ολόκληρο τον κύκλο ζωής τους.

Οι βασικότερες λειτουργίες της CA, στα πλαίσια ενός CSP, περιλαμβάνουν την δημιουργία και διανομή των πιστοποιητικών, την αποθήκευση τους σε καταλόγους, τον έλεγχο των διαδικασιών ανάκλησης τους, καθώς και την επικοινωνία με άλλες CSP.

2) Η Αρχή Καταχώρισης – Registration Authority – RA :

Η RA ουσιαστικά παρέχει τη λειτουργική διεπαφή και επικοινωνία μεταξύ ενός χρήστη και του CSP. Είναι το τμήμα του οργανισμού CSP που είναι υπεύθυνο για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ταυτότητας ή του ρόλου ενός χρήστη ή μιας οντότητας, όπως μιας εφαρμογής ή ενός εξυπηρέτη. Η RA προωθεί προς τη CA τις έγκυρες υποβληθείσες προς αυτήν αιτήσεις για τη δημιουργία και περαιτέρω διαχείριση των αντίστοιχων πιστοποιητικών.

3.2.2 Πολιτική Πιστοποιητικών (CP) και Δήλωση Πρακτικών Πιστοποίησης (CPS).

Στα πλαίσια της λειτουργίας ενός CSP απαιτείται η ανάπτυξη και δημοσίευση δύο βασικών κειμένων : της Πολιτικής Πιστοποιητικών (CP) και Δήλωσης Πρακτικών Πιστοποίησης (CPS).

1. Πολιτική Πιστοποιητικών – Certificate Policy – CP

Είναι ένα σύνολο συγκεκριμένων κανόνων οι οποίοι εξασφαλίζουν την εφαρμοσιμότητα ενός πιστοποιητικού στα πλαίσια μιας συγκεκριμένης κοινότητας ή ενός συνόλου εφαρμογών με συγκεκριμένες απαιτήσεις ασφάλειας.

Όταν μια CA εκδίδει ένα πιστοποιητικό, ουσιαστικά δηλώνει προς το χρήστη του πιστοποιητικού ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί σε μία συγκεκριμένη οντότητα. Παρόλα αυτά, το όριο αποδοχής της διαβεβαίωσης της CA από το χρήστη πρέπει να αποτιμάται από αυτόν ανάλογα με το σκοπό και τις εφαρμογές που αυτό το πιστοποιητικό θα χρησιμοποιηθεί. Για παράδειγμα, ένα πιστοποιητικό X.509 v.3 (αναλύεται παρακάτω) μπορεί να περιέχει ένα δείκτη προς μια CP και ο δείκτης αυτός μπορεί να χρησιμοποιηθεί από το χρήστη για τη λήψη απόφασης αν πρέπει να εμπιστευθεί το συγκεκριμένο πιστοποιητικό για κάποιο συγκεκριμένο σκοπό. Η CP, η οποία πρέπει να γίνει αποδεκτή τόσο από το δημιουργό CSP όσο και από το χρήστη του πιστοποιητικού, αναπαριστάνεται στο πιστοποιητικό από ένα μοναδικά καταχωρημένο Προσδιοριστή Αντικειμένου (Object Identifier – OI). Η διαδικασία καταχώρισης περιλαμβάνει συγκεκριμένες διαδικασίες που έχουν καθοριστεί σε σχετικά πρότυπα των ISO/IEC και ITU. Ο φορέας ο οποίος καταχωρεί τον OI εκδίδει και το κείμενο που προσδιορίζει την CP, ώστε να μπορούν να το εξετάσουν οι χρήστες των πιστοποιητικών. Στη γενική περίπτωση, κάθε ξεχωριστό πιστοποιητικό μπορεί να υποδηλώσει μια ξεχωριστή συγκεκριμένη CP. Στις περισσότερες, όμως, περιπτώσεις ένας CSP έχει σε ισχύ ένα μικρό αριθμό διαφορετικών πολιτικών, εκφράζοντας τις πολιτικές σε υψηλότερο αφαιρετικό επίπεδο.

2. Δήλωση Πρακτικών Πιστοποίησης – Certification Practice Statement – CPS

Είναι μια δήλωση όπου καταγράφονται οι πρακτικές που ακολουθεί μια CA για τη διαχείριση των πιστοποιητικών. Αποτελεί ένα λεπτομερέστατο έγγραφο, όπου αναφέρεται ο τρόπος διεκπεραίωσης των λειτουργικών διαδικασιών των συστημάτων που υποστηρίζουν υπηρεσίες ασφάλειας, οι

ακολουθούμενες πρακτικές, καθώς και οι ενέργειες διανομής των πιστοποιητικών. Συνήθως αποτελεί τμήμα του συμβολαίου μεταξύ του CSP και του λήπτη των υπηρεσιών πιστοποίησης, ενώ μπορεί να περιλαμβάνει και κείμενα από ισχύοντες νόμους, ιδιωτικά συμφωνητικά και δηλώσεις βούλησης. Είναι επιθυμητό ένας CSP να περιλαμβάνει δείκτες προς ευρέως αποδεκτά πρότυπα με τα οποία συμμορφώνεται κατά τη λειτουργία του. Οι δείκτες προς τα πρότυπα πρέπει να καλύπτουν, με γενικό τρόπο, την καταλληλότητα των πρακτικών μιας CA σχετικά με τους σκοπούς μιας άλλης οντότητας, καθώς και την δυνητική τεχνολογική συμβατότητα των διανεμηθέντων πιστοποιητικών με το τεχνολογικό περιβάλλον διαφόρων συστημάτων, όπως συστήματα αποθήκευσης κτλ.

3.2.3 Υποδομή Δημόσιων Κλειδιών – Public Key Infrastructure – PKI

Στη γενική περίπτωση, ένας CSP μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον CSP. Οι CSP, λειτουργικά συνεργαζόμενοι διαμέσου Αλυσίδων Εμπιστοσύνης (Chains of Trust) για τη δημιουργία ενός γενικευμένου Ιστού Εμπιστοσύνης (Web of Trust), οδηγούν στην παροχή ολοκληρωμένων υπηρεσιών Υποδομής Δημόσιων Κλειδιών (PKI).

Μια PKI περιλαμβάνει έναν ή περισσότερους CSP και στοχεύει στην οργάνωση ενός ολοκληρωμένου περιβάλλοντος διαχείρισης πιστοποιητικών, με όρους τεχνικής επάρκειας και νομικής διασφάλισης κατά τη λειτουργία.

Η CP καθορίζει τη βάση για τη διαπίστευση μεταξύ διαφόρων CSP, στην κατεύθυνση της ανάπτυξης μιας αποτελεσματικής PKI : Όποτε μια CA διανέμει ένα πιστοποιητικό μιας CA προς μιας άλλη CA, πρέπει να αποτιμηθούν από τον παραλήπτη CA οι ξεχωριστές CP τις οποίες η CA αυτή εμπιστεύεται. Αμέσως μετά, για το σύνολο των αποδεκτών CP εγκαθίσταται, από τη CA που διένειμε το πιστοποιητικό, ένας δείκτης στο αποδεκτό πιστοποιητικό της CA.

Μια PKI πρέπει να λειτουργεί σε ένα αρκετά υψηλό επίπεδο ασφάλειας και σιγουριάς έτσι ώστε να ικανοποιούνται οι απαιτήσεις, σε ασφάλεια και διαχείριση κινδύνων, που έχουν τεθεί τόσο από την βιομηχανία όσο και από άλλους φορείς.

Ακολουθεί περιγραφή των βασικών υπηρεσιών ασφάλειας που μπορεί να προσφέρει μια PKI και είναι κοινές σε όλες τις Υπηρεσίες Υποδομής Δημόσιου Κλειδιού (ΥΥΔΚ)

1. Εμπιστευτικότητα – Confidentiality : διασφαλίζει ότι μόνο εξουσιοδοτημένα μέλη μπορούν να αναγνώσουν μια επικοινωνία, οι ωτακουστές όμως όχι.

   Ως εμπιστευτικότητα ορίζεται η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση αυτών. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή δεδομένων. Η Υποδομή Δημοσίου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από τον συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

   Η εμπιστευτικότητα μπορεί να παρομοιασθεί με έναν αδιαφανή φάκελο. Το μήνυμα που περιλαμβάνει δεν είναι άμεσα ορατό σε κανένα δίχως να ανοιχθεί ο φάκελος. Φυσικά, ο φάκελος μπορεί να ανοιχθεί από τον οποιονδήποτε και έτσι να παραβιασθεί το απόρρητο της αλληλογραφίας. Η κρυπτογραφία παρέχει ένα μεγάλο επίπεδο ασφάλειας στον φάκελος που πολύ δύσκολα, σχεδόν ακατόρθωτα, είναι εφικτό να ανοιχτεί από οποιονδήποτε άλλον εκτός από τον νόμιμο παραλήπτη.

2. Πιστοποίηση – Authentication : διασφαλίζει ότι ο δημιουργός μιας επικοινωνίας είναι το άτομο που υποτίθεται και όχι ένας πλαστός (απατεώνας).

Ως πιστοποίηση ορίζεται η επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Δηλαδή, το άτομο που επιθυμεί να επιβεβαιώσει την ταυτότητά ενός άλλου άτομου ή κάποιου εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση.

Η πιστοποίηση μπορεί να υλοποιηθεί με τρεις βασικές μεθόδους:

1. Με κάτι που γνωρίζει κανείς, π.χ. το PIN μιας πιστωτικής κάρτας ή το μυστικό κωδικό ενός λογαριασμού κτλ.
2. Με κάτι που έχει κανείς στην ιδιοκτησία του, π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα κτλ.
3. Με κάτι που έχει εκ γενετής, π.χ. δακτυλικά αποτυπώματα, φωνή κτλ.

Η Πιστοποίηση, πιο απλά, είναι ο τρόπος με τον οποίο δημοσιεύονται οι τιμές των δημόσιων κλειδιών και η πληροφορία που αντιστοιχεί στις τιμές αυτές. Ένα *πιστοποιητικό* (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημοσίου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών, ή πληροφορία που σχετίζεται με αυτά, ή και τα δύο. Γενικά, ένα πιστοποιητικό είναι μία συλλογή πληροφοριών που έχει υπογραφεί ψηφιακά από την οντότητα που το εκδίδει. Τα πιστοποιητικά αυτά χαρακτηρίζονται από το είδος της πληροφορίας που περιέχουν. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται *Αρχή Πιστοποίησης* (Certificate Authority - CA).

3. Ακεραιτότητα – Integrity : διασφαλίζει ότι το περιεχόμενο μιας επικοινωνίας δεν έχει μεταβληθεί, έχει δηλαδή διατηρήσει την ακεραιότητα του, κατά την μεταφορά του.

   Ακεραιότητα είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάσταση τους. Η υπηρεσία αυτή παρέχεται από μηχανισμούς κρυπτογραφίας όπως είναι οι ψηφιακές υπογραφές.

   Ας υποθέσουμε την ακεραιότητα ενός διαφανούς φακέλου. Το μήνυμα που περιέχει ο φάκελος μπορεί να διαβαστεί από τον οποιονδήποτε, οπότε και παραβιάζεται η εμπιστευτικότητα, όπως αυτή ορίστηκε παραπάνω. Ο φάκελος θεωρείται ενδεικτικό στοιχείο παραβίασης. Ο παραλήπτης βλέποντας τον φάκελο είναι σε θέση να επιβεβαιώσει ότι ο φάκελος δεν έχει ανοιχθεί, παραβιαστεί ή ακόμη και αντικατασταθεί.

4. Τεχνική Μη Αποποίηση – Technical Non-Repudiation : διασφαλίζει ότι ένα απεσταλμένο μήνυμα έχει αποσταλεί και παραληφθεί από τα μέλη που ισχυρίζονται ότι έχουν στείλει και λάβει το μήνυμα.

   Η μη-αποποίηση συνδυάζει τις υπηρεσίες της πιστοποίησης και της ακεραιότητας που παρέχονται σε μια τρίτη οντότητα. Έτσι, τα εμπλεκόμενα μέρη δεν μπορούν να αρνηθούν εκ τον υστέρων την συμμετοχή τους στη συναλλαγή (μη αποποίηση ευθύνης), δηλαδή ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί την δημιουργία και αποστολή του συγκεκριμένου μηνύματος καθώς και ο παραλήπτης ότι το έλαβε.

   Η ασύμμετρη κρυπτογραφία παρέχει ψηφιακές υπογραφές, τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει την συγκεκριμένη ψηφιακή υπογραφή, πρόκειται δηλαδή για μια αμφιμονοσήμαντη σχέση. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά και ο παραλήπτης του ψηφιακά υπογεγραμμένου μηνύματος μπορεί να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα.

   Το νομικό και πολιτικό περιβάλλον στο οποίο πραγματοποιείται η άρνηση αυτή παίζει επίσης ρόλο.

3.3 Υπηρεσίες Διαχείρισης Πιστοποιητικών

Η διασφάλισης της ταυτότητας κάθε οντότητας που βρίσκεται συνδεδεμένη στο χώρο του διαδικτύου είναι και αυτή μια από τις βασικές, άρα και σημαντικότερες, απαιτήσεις στον τομέα της ασφάλειας του Παγκόσμιου Ιστού.

Ένα ερώτημα που προκύπτει είναι τι είδους εργαλεία (όπως πρωτόκολλα), για την διασφάλιση αυτή, έχουμε στην διάθεσή μας σήμερα. Ποιο συγκεκριμένα, ποιες από τις υπηρεσίες πιστοποίησης χρησιμοποιούνται για την ανάπτυξη υποδομών δημόσιων κλειδιών;

Ως απάντηση, ακολουθεί αρχικά μια ονομαστική αναφορά των εργαλείων αυτών.

1. Πιστοποιητικά Μορφής PGP (Pretty Good Privacy)
2. Πιστοποιητικά X.509
3. Πιστοποιητικά SDI (Selective Dissemination of Information)
4. Επέκταση Ασφάλειας DNS

Ένα ψηφιακό πιστοποιητικό (digital certificate) ή πιστοποιητικό ταυτότητας (identity certificate) είναι ένα ηλεκτρονικό διακριτικό που αποδεικνύει την αντιστοίχηση μεταξύ μιας οντότητας και ενός δημόσιου κλειδιού. Ο κύριος σκοπός της υπηρεσίας διαχείρισης πιστοποιητικών (certificate management service) είναι να διαβεβαιώσει για την κατάσταση ενός πιστοποιητικού, το οποίο έχει ήδη εκδοθεί από έναν CSP. Αυτό επιτυγχάνεται με την αποτελεσματική διαχείριση των εκδοθέντων πιστοποιητικών σε όλη τη διάρκεια του κύκλου ζωής τους. Είναι αποκλειστική ευθύνη του CSP να υλοποιήσει όλες εκείνες τις διαδικασίες που βελτιώνουν τη διαχείριση της αποτελεσματικότητας και της ασφάλειας, με σκοπό την αύξηση της εμπιστοσύνης που οι χρήστες δείχνουν στον CSP.

Εκτός της προαναφερθείσας κατηγορίας πιστοποιητικών, ιδιαίτερη χρησιμότητα παρουσιάζουν και τα πιστοποιητικά χαρακτηριστικών (attribute certificates), τα οποία περιγράφουν τις ιδιότητες μιας συγκεκριμένης οντότητας, όπως δικαιώματα προσπέλασης ή συμμετοχή σε ομάδα χρηστών.

Ο κύκλος ζωής του πιστοποιητικού αποτελείται από τις εξής φάσεις – λειτουργίες :

1) Δημιουργία Πιστοποιητικού – Certificate Generation
2) Διανομή Πιστοποιητικών – Certificate Distribution
3) Αποθήκευση και Ανάκτηση Πιστοποιητικού – Certificate Storage and Retrieval
4) Ανάκληση Πιστοποιητικού – Certificate Revocation

Από αυτές θα επικεντρωθούμε στην 1^{η}, τη Δημιουργία Πιστοποιητικού :

Αφού ολοκληρωθεί η διαδικασία καταχώρισης του χρήστη στην RA, ο CA δημιουργεί ένα πιστοποιητικό και το παραδίδει στην αιτούσα οντότητα. Κατά τη φάση αυτή επιτυγχάνεται και η αντιστοίχηση μεταξύ οντότητας και δημόσιου κλειδιού. Για να είναι ασφαλής η αντιστοίχηση αυτή, θα πρέπει να έχουν ακολουθηθεί από την RA οι κατάλληλες διαδικασίες αυθεντικοποίησης και ταυτοποίησης από πλευράς CSP, κατά τη φάση της διαδικασίας καταχώρισης της αιτούσας οντότητας. Η ορθότητα της αντιστοίχησης αυτής αποτελεί το βασικό σημείο για την παροχή της υπηρεσίας αυθεντικοποίησης, από πλευράς του CSP, μεταξύ των χρηστών της. Τα πιστοποιητικά, αφού δημιουργηθούν, υπογράφονται ψηφιακά με χρήση του ιδιωτικού κλειδιού του CSP. Η

υπογραφή αυτή υποδηλώνει ότι ο CSP αναλαμβάνει την ευθύνη για την αυθεντικότητα των πληροφοριών που αναγράφονται στο πιστοποιητικό.

Έτσι έχουμε :

Είσοδος : Τα δεδομένα που αναφέρονται στην έγκυρη φόρμα εγγραφής

Έξοδος : Ένα έγκυρο πιστοποιητικό

Επεξεργασία : Το σημαντικότερο ζήτημα σε σχέση με αυτή τη διαδικασία είναι η μορφή του πιστοποιητικού. Παρότι αυτή η διαδικασία έχει αυτοματοποιηθεί από πολλά προϊόντα λογισμικού (π.χ. Netscape Certificate Server, Microsoft Certificate Server), δεν έχει υιοθετηθεί μία κοινή μορφή πιστοποιητικού. Στο παρελθόν έχουν προταθεί πολλά σχήματα καθένα από τα οποία χρησιμοποιεί ειδική μορφή για το πιστοποιητικό. Τα πιο σημαντικά από αυτά είναι αυτά που δόθηκαν παραπάνω : PGP, X.509, SDI και DNS.

Οι πιο ευρέως αναπτυσσόμενες μορφές πιστοποιητικών είναι αυτές του PGP και του X.509.

3.3.1 PGP – Pretty Good Privacy

Αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον Phil Zimmerman και χρησιμοποιεί τους αλγόριθμους RSA (Ron Rivest, Adi Shamir & Len Adleman) και IDEA (International Data Encryption Algorithm) για την κρυπτογράφηση και υπογραφή μηνυμάτων της ηλεκτρονικής αλληλογραφίας.

Το PGP είναι πολύ απλό και αποτελείται από ένα δημόσιο κλειδί, μία διεύθυνση ηλεκτρονικού ταχυδρομείου και ένα επίπεδο εμπιστοσύνης το οποίο τοποθετείται πάνω σε αυτό από τον παραλήπτη του μηνύματος.

Κάθε χρήστης του PGP διατηρεί μία λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί, η οποία καλείται keyring. Για την προστασία της λίστας, ο κάθε χρήστης την υπογράφει με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στην λίστα είναι δυνατό να φέρει έναν από τους εξής χαρακτηρισμούς:

- Απολύτως Έμπιστο (Completely Trusted)
- Μερικώς Έμπιστο (Marginally Trusted)
- Μη Έμπιστο (Untrusted)
- Άγνωστο (Unknown)

Το PGP επιτρέπει την ανταλλαγή keyrings, ενώ ο κάθε χρήστης έχει τη δυνατότητα να ρυθμίσει το επίπεδο εμπιστοσύνης για την αποδοχή ενός νέου κλειδιού. Δηλαδή, ο χρήστης μπορεί να θεωρήσει την οντότητα του κλειδιού έμπιστη, αν το κλειδί έχει ήδη υπογραφεί από δύο απολύτως έμπιστα (Completely Trusted) κλειδιά ή από τρία μερικώς έμπιστα (Marginally Trusted) κλειδιά.

Καθώς οι χρήστες ανταλλάσσουν keyrings σχηματίζουν έναν ιστό εμπιστοσύνης (web of trust). Κάθε χρήστης αποτελεί αρχή πιστοποίησης του εαυτού του και είναι υπεύθυνος για το μοντέλο εμπιστοσύνης που επιλέγει. Το απλό αυτό μοντέλο έχει επιτρέψει στο PGP να κερδίσει μία σχετικά μεγάλη αποδοχή στο Διαδίκτυο. Παρόλα αυτά, η Υποδομή Δημοσίου Κλειδιού του PGP δεν είναι κατάλληλη για εφαρμογές ηλεκτρονικού εμπορίου και για εφαρμογές που απαιτούν ισχυρή ταυτοποίηση.

Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηριστικό του βαθμού της

εμπιστοσύνης. Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει έναν ακριβή τρόπο του προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παρέχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας.

Το PGP δεν υποστηρίζει κάποια μέθοδο επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές πραγματοποιούνται μόνο μέσω άμεσης επικοινωνίας των χρηστών. Το PGP δεν παρέχει τη δυνατότητα ανωνυμίας, καθώς η χρήση μίας διεύθυνσης ηλεκτρονικής αλληλογραφίας που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

Παρότι, το πιστοποιητικό PGP είναι πολύ απλό, παρουσιάζει προβλήματα όταν απαιτείται να χρησιμοποιηθεί σε ανοιχτά κατανεμημένα περιβάλλοντα, αφού δεν παρουσιάζει ευελιξία σε περιβάλλοντα με απαιτήσεις κλιμάκωσης. Για το λόγο αυτό το ενδιαφέρον μετατοπίζεται στη χρήση του X.509 και ειδικά στα X.509 v3 πιστοποιητικά.

Παράδειγμα : «PGP και ο Ιστός Εμπιστοσύνης»

Εάν ο Α θέλει να χρησιμοποιήσει το PGP, θα πρέπει να δημιουργήσει ένα «δακτύλιο» δημόσιων-κλειδιών (public-key ring)που θα περιέχει τα δημόσια κλειδιά άλλων χρηστών. Υποθέστε ότι το βασικό δακτύλιο του Α περιέχει ένα δημόσιο κλειδί που αποδίδεται στον Β, αλλά πραγματικά ανήκει στον Γ. Ίσως ο Α να πήρε το κλειδί από έναν πίνακα ανακοινώσεων που χρησιμοποιήθηκε από τον Β για να στείλει το δημόσιο κλειδί του, το οποίο όμως έχει δεσμευθεί από τον Γ.

Υπάρχει ένας αριθμός πιθανών προσεγγίσεων με στόχο την ελαχιστοποίηση του κινδύνου ένα δακτύλιο κλειδιών να περιέχει ψεύτικα δημόσια κλειδιά.

1. Ο Α μπορεί φυσιολογικά να πάρει το δημόσιο κλειδί του Β από τον ίδιο τον Β. Αυτή είναι μια πολύ ασφαλής μέθοδος αλλά επίσης έχει και προφανείς φυσικούς περιορισμούς.
2. Ο Α μπορεί να επιβεβαιώσει τη γνησιότητα του κλειδιού τηλεφωνικώς. Εάν ο Α γνωρίζει τη φωνή του Β τότε μπορεί να ζητήσει από τον Β να του υπαγορεύσει το δημόσιο κλειδί του μέσω του τηλεφώνου. Εναλλακτικά, ο Β θα μπορούσε να κατακερματίσει (hash) το δημόσιο κλειδί του και να διαβάσει στον Α το πρώτο μέρος (ένα δείγμα) του κατακερματισμένου αυτού δημόσιου κλειδιού, έτσι ώστε ο Α να μπορέσει να επιβεβαιώσει ότι έχει το σωστό κλειδί (επιβεβαιώνοντας ότι το αυτό το δείγμα του κλειδιού όντως είναι του αυτό που έχει σημειώσει να είναι του Β).
3. Ο Α θα μπορούσε να πάρει το κλειδί από κάποιον άλλο που εμπιστεύεται. Εάν ο Δ ξέρει το δημόσιο κλειδί του Β, τότε μπορεί να το επιβεβαιώσει στον Α. Εάν ο Α εμπιστεύεται τον Δ, τότε εμπιστεύεται την γνησιότητα του δημόσιου κλειδιού του Β που δόθηκε από τον Δ. Στην ουσία, ο Δ υπογράφει το δημόσιο κλειδί του Β με το δικό του ιδιωτικό-προσωπικό κλειδί.
4. Ο Α μπορεί να λάβει το δημόσιο κλειδί του Β από μια εμπιστευμένη αρχή πιστοποίησης (trusted certification authority).

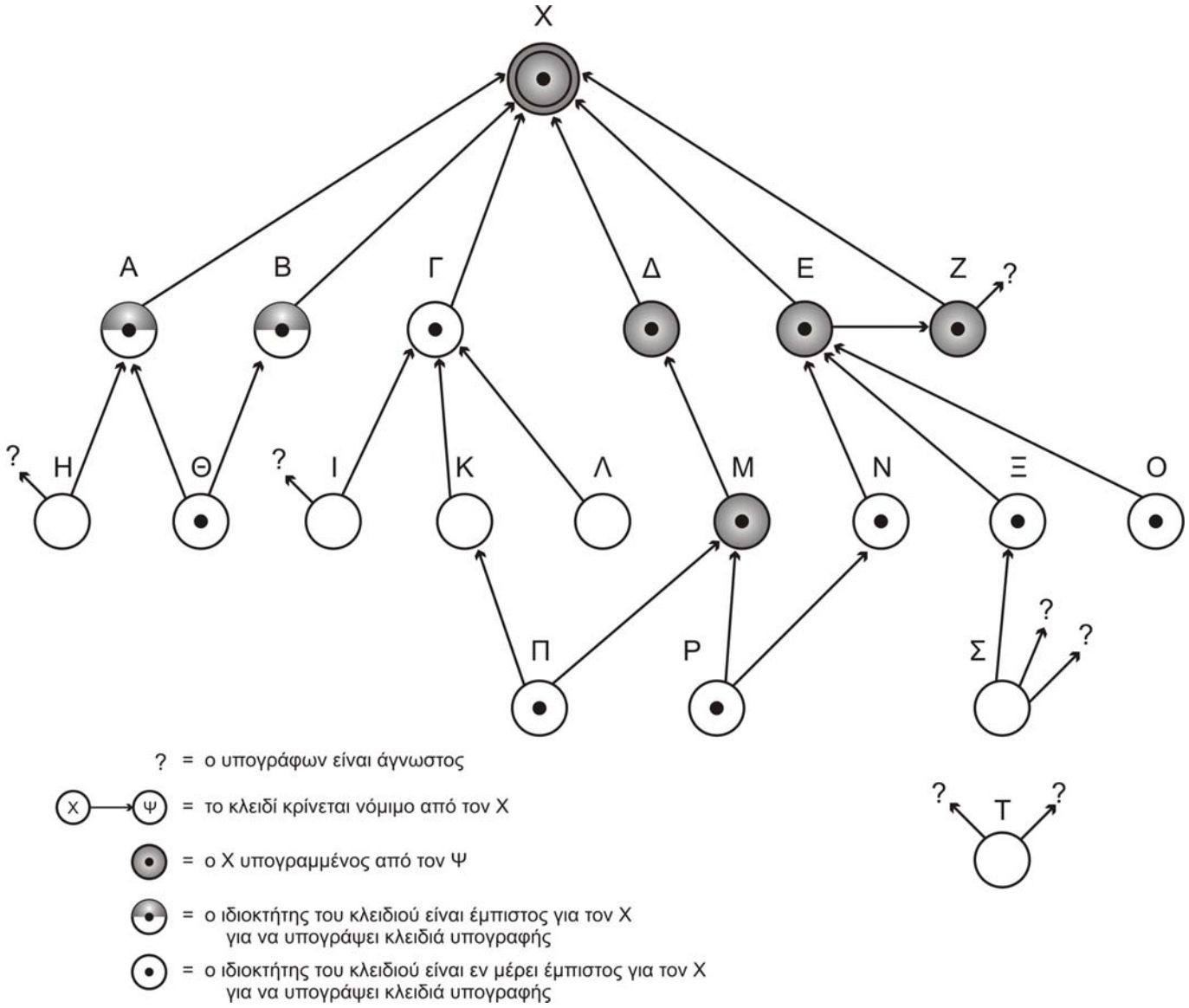
Το PGP συνδέει ένα επίπεδο εμπιστοσύνης (level of trust) με κάθε δημόσιο κλειδί ως εξής :

1. Όταν ο Α εισάγει ένα νέο δημόσιο κλειδί επάνω στο δικό του public-key ring, μπορεί να διευκρινίσει εάν αυτός ο χρήστης είναι άγνωστος (unknown), μη έμπιστος (untrusted), μερικά έμπιστος ή ολοκληρωτικά έμπιστος.

2. Το δημόσιο κλειδί μπορεί να συνδέεται με μία ή περισσότερες υπογραφές (δείτε το 3 πριν). Μια τιμή γνησιότητας (legitimacy value) δίνεται στο κλειδί αυτό, ανάλογα με ποιος το έχει υπογράψει, και κατά πόσο ο Α εμπιστεύεται τους υπογράφοντες αυτούς. Παραδείγματος χάριν, ένα κλειδί μπορεί να χρειαστεί να υπογραφεί από ένα εντελώς έμπιστο άτομο, ή δύο μερικώς έμπιστα ή 10 μη έμπιστα άτομα προτού του δοθεί μια τιμή γνησιότητας που θα δείχνει ότι ο Α εμπιστεύεται αυτό το κλειδί.

Το παρακάτω διάγραμμα επεξηγεί πώς συσχετίζονται η εμπιστοσύνη των υπογραφών και η γνησιότητά των κλειδιών. Το διάγραμμα παρουσιάζει ένα public-key ring. Κάθε κόμβος αντιπροσωπεύει ένα κλειδί, και το διάγραμμα παρουσιάζει τα διαφορετικά επίπεδα εμπιστοσύνης τα οποία συνδέονται με κάθε κλειδί. Ο ιδιοκτήτης του δακτύλιου των κλειδιών είναι ο «Χ» και ο κορυφαίος κόμβος είναι το δημόσιο-κλειδί του ιδιοκτήτη του δακτύλιου (key-ring owner) και έχει την μέγιστη εμπιστοσύνη.

Σε αυτό το παράδειγμα, ο ιδιοκτήτης έχει διευκρινίσει ότι εμπιστεύεται πάντα τους ακόλουθους χρήστες για να υπογράψουν άλλα κλειδιά : Δ, Ε, Ζ, Η. Ο ιδιοκτήτης εμπιστεύεται μερικώς τους χρήστες Α και Β να υπογράψουν άλλα κλειδιά. Η σκίαση των κόμβων δείχνει το επίπεδο εμπιστοσύνης που ορίζεται από τον ιδιοκτήτη του δακτύλιου των κλειδιών. Ένα σημείο στη μέση ενός κλειδιού δείχνει ότι το κλειδί θεωρείται γνήσιο.



Σχήμα 3.1 : Παράδειγμα του Μοντέλου Εμπιστοσύνης - Trust Model του PGP

Η δομή του δέντρου προσδιορίζει ποια κλειδιά έχουν υπογράψει άλλοι χρήστες. Ένα βέλος που δείχνει από ένα κλειδί σε ένα άλλο, σημαίνει ότι το πρώτο κλειδί έχει υπογραφεί από το δεύτερο. Παραδείγματος χάριν, το κλειδί Η έχει υπογραφεί από το Α. Ένα βέλος οδηγεί σε ένα αγγλικό ερωτηματικό εάν ένα κλειδί έχει υπογραφεί από κάποιον του οποίου το κλειδί δεν περιέχεται στον δακτύλιο, δείχνοντας έτσι ότι ο υπογράφων είναι άγνωστος στο ιδιοκτήτη του δακτύλιου. Παραδείγματος χάριν, το κλειδί Σ έχει υπογραφεί από το Ξ και επίσης από δύο άγνωστους υπογράφοντες.

Αξιοπρόσεχτα σημεία :

- Ο key-ring owner «Χ» έχει υπογράψει σχεδόν όλα τα κλειδιά που εμπιστεύεται πλήρως ή μερικώς. Στην πράξη, οι περισσότεροι χρήστες θα υπογράψουν τα κλειδιά άλλων χρηστών που εμπιστεύονται.

- Υποθέτουμε ότι δύο μερικώς έμπιστες υπογραφές είναι επαρκείς για να πιστοποιήσουν ένα κλειδί. Ως εκ τούτου, το κλειδί του χρήστη Θ κρίνεται νόμιμο από το PGP επειδή έχει υπογραφεί από τον Α και τον Β, οι οποίοι και οι δύο είναι μερικώς έμπιστοι.
- Ένα κλειδί μπορεί να καθοριστεί να είναι νόμιμο, αλλά ο ιδιοκτήτης του μπορεί να μην θεωρηθεί έμπιστος για να υπογράψει άλλα κλειδιά. Παραδείγματος χάριν, το κλειδί του Ξ είναι νόμιμο επειδή είναι υπογραμμένο από τον Ε, ο οποίος είναι έμπιστος, αλλά ο Ξ δεν είναι έμπιστος ώστε να υπογράψει άλλα κλειδιά. Ο key-ring owner εμπιστεύεται ότι έχει το σωστό δημόσιο κλειδί για τον Ξ αλλά δεν έχει πραγματικά καμιά εμπιστοσύνη στον Ξ. Επομένως το κλειδί του Σ δεν θεωρείται νόμιμο, παρόλο που έχει υπογραφεί από τον Ξ.
- Ο κόμβος Τ αποσυνδέεται από το δέντρο με δύο άγνωστες υπογραφές. Ένα τέτοιο κλειδί μπορεί να είχε αποκτηθεί από έναν βασικό κεντρικό υπολογιστή. Το PGP δεν μπορεί να υποθέσει ότι αυτό το κλειδί είναι νόμιμο εκτός και αν ο key-ring owner αποφασίσει ότι είναι νόμιμο και είτε υπογράψει αυτό το κλειδί, είτε δηλώσει ότι είναι πρόθυμος να εμπιστευθεί μια από τις υπογραφές του κλειδιού Τ.

3.3.2 X.509

Το X.509 σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου του X.500 (ldap). Η πρώτη έκδοση του X.509 δημοσιεύτηκε το 1988, καθιστώντας το έτσι την παλαιότερη πρόταση για μία παγκόσμια Υποδομή Δημοσίου Κλειδιού.

Το γεγονός αυτό σε συνδυασμό με την υποστήριξη του προτύπου από τον Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και την Διεθνή Ένωση Τηλεπικοινωνιών (Internation Telecommunications Union - ITU) έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών.

Η Visa και η Mastercard έχουν επιλέξει το X.509 για το Secure Electronic Transactions (SET) πρότυπο, και η Netscape υιοθέτησε το X.509 πρότυπο για την έκδοση των πιστοποιητικών που χρησιμοποιούνται στο Secure Sockets Layer πρωτόκολλο.

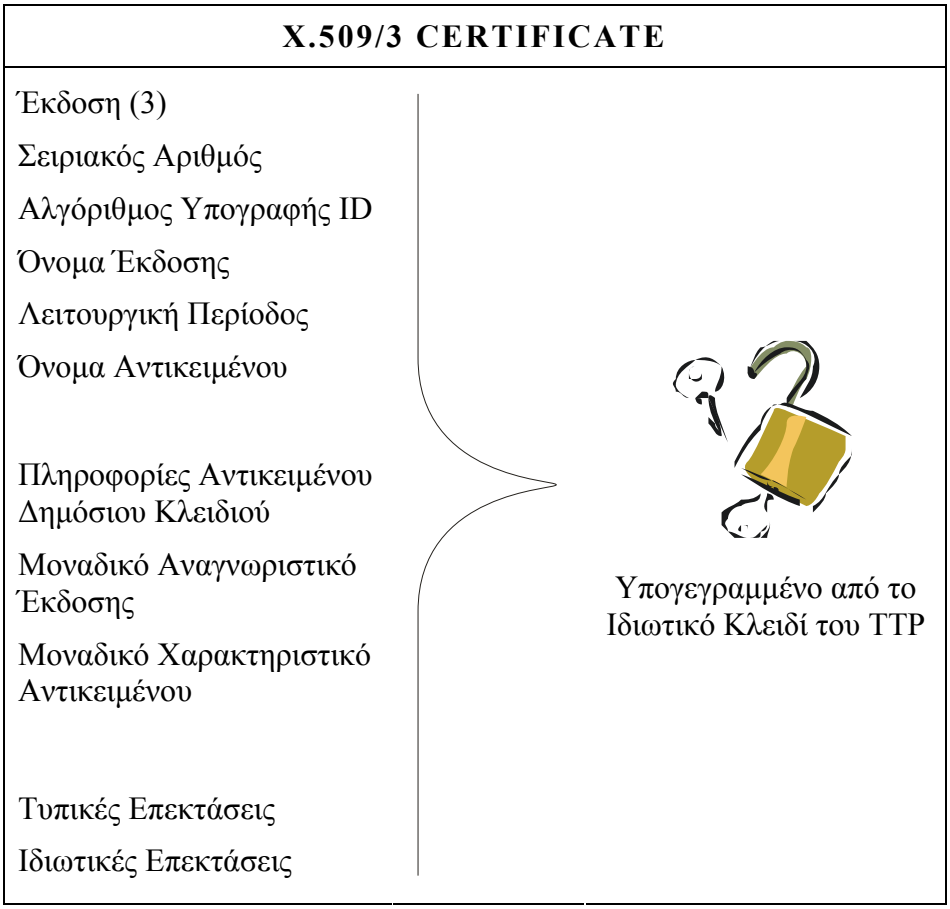
Τόσο το X.509 όσο και το X.500 αποτελούν τμήματα της σειράς προτύπων X που προτάθηκαν από τους οργανισμούς ISO και ITU. Το X.500 σχεδιάστηκε με σκοπό την παροχή υπηρεσιών καταλόγου παγκοσμίως και το X.509 με σκοπό την παροχή υπηρεσίας αυθεντικοποίησης στις υπηρεσίες του X.500.

Η έκδοση 3 του X.509 επεκτείνει σε μεγάλο βαθμό την λειτουργικότητα του προτύπου και γι αυτό είναι ιδιαίτερα διαδεδομένο και χρησιμοποιείται σε πλοηγητές ιστοσελίδων (web browsers), εξυπηρετητές και προγράμματα λογισμικού για την διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server/clients) κτλ από πολλές γνωστές εταιρίες ανάπτυξης λογισμικού.

Το X.500 (έκδοση 1) αναπτύχθηκε αρχικά το 1988. Για το λόγο αυτό αποτελεί το παλαιότερο πρότυπο για μία παγκόσμια PKI και υιοθετήθηκε από πολλές εταιρείες: οι Visa και MasterCard το υιοθέτησαν για το πρότυπο ασφαλών ηλεκτρονικών συναλλαγών (SET - Secure Electronic Transactions) και οι Microsoft και Netscape για την υλοποίηση των εξυπηρετών πιστοποιητικών (certificate servers). Έχοντας ήδη ευρεία διαδομένη εγκατεστημένη βάση, εκτιμάται ως ιδιαίτερα δύσκολο για το X.509 να αντικατασταθεί από άλλο πρότυπο. Παρά το γεγονός ότι το X.509 παρουσιάζει ατέλειες, ιδίως στο θέμα της διαλειτουργικότητας, αναμένεται ότι μόνο νέες εκδόσεις του προτύπου ή επεκτάσεις αυτού θα επικρατήσουν στις υλοποιήσεις των CSP και PKI.

Το X.509 βρίσκεται στην τρίτη του έκδοση και το βασικό πλεονέκτημα του έναντι των δύο προηγούμενων είναι η παροχή του μέσου για τη μετακίνηση πέρα από την ανάγκη της ιεραρχίας. Οι εκδόσεις 1 και 2 του X.509 είναι περισσότερο κατάλληλες για χρήση στο εσωτερικό των τμημάτων μιας επιχείρησης. Αυτό αποτελεί περιορισμό για την ανάπτυξη των προτύπων.

Η μορφή του X.509 απεικονίζεται στο ακόλουθο σχήμα :



Σχήμα 3.2 : Μορφή του πιστοποιητικού X.509

Ένα σημαντικό χαρακτηριστικό για τα πιστοποιητικά τύπου X.509 είναι η πρόσθετη λειτουργικότητα που προσφέρεται από τις τυπικές επεκτάσεις του (standard extensions). Οι επεκτάσεις αυτές είναι στην πραγματικότητα πεδία τα οποία παρέχουν διάφορους διοικητικούς και διαχειριστικούς ελέγχους, οι οποίοι είναι χρήσιμοι για αυθεντικοποίηση πολλαπλών σκοπών σε μεγάλης κλίμακας περιβάλλοντα.

Οι τυπικές επεκτάσεις προσφέρουν πληροφορίες που συνήθως σχετίζονται με πληροφορίες πολιτικής φύσης, χαρακτηριστικά του θέματος και του εκδότη, περιορισμούς σχετικά με το μονοπάτι του πιστοποιητικού καθώς και τη βελτιστοποιημένη λειτουργικότητα των CRL (Certificate Revocation Lists – Λίστες Ανάκλησης Πιστοποιητικών, σύντομη περιγραφή του στο Γλωσσάρι σελ. 2).

Οι τυπικές επεκτάσεις που έχουν προταθεί από τον ISO μπορούν να κατηγοριοποιηθούν σύμφωνα με:

- Πολιτικές Πιστοποιητικών και Χαρτογράφηση Πολιτικών (Certificate Policies and Policy Mapping). Αυτές οι επεκτάσεις βοηθούν τον CSP στην παροχή στους χρήστες των προδιαγραφών της πολιτικής που εφαρμόζεται στη διαχείριση του πιστοποιητικού. Η χαρτογράφηση των πολιτικών έχει ως σκοπό τον καθορισμό πολιτικών που θεωρούνται ισοδύναμες με πολιτικές άλλων CSP.
- Εναλλακτικές Ονομασίες (Alternative Names). Οι επεκτάσεις αυτές χρησιμοποιούνται με σκοπό τον καθορισμό εναλλακτικών διακριτικών ονομασιών για το θέμα ή τον εκδότη.
- Χαρακτηριστικά Καταλόγου Θέματος (Subject Directory Attributes). Χρησιμοποιώντας την επέκταση αυτή προσφέρεται η δυνατότητα στον ιδιοκτήτη ενός πιστοποιητικού να ορίσει επιπλέον πληροφορίες πέρα από την ονομασία του θέματος.
- Περιορισμοί Μονοπατιού Πιστοποιητικού (Certificate Path Constraints). Η επέκταση αυτή χρησιμοποιείται για να βοηθήσει τους CSP να συνδέσουν τις υποδομές τους με διάφορους τρόπους, επιβάλλοντας βασικούς κανόνες στους οποίους υπόκειται η σύνδεση αυτή.

Επιπλέον, έχουν οριστεί επεκτάσεις που αφορούν ειδικά τις CRL οι οποίες είναι:

- Αριθμοί και κωδικοί αιτιολογίας CRL
- Σημεία διανομής CRL
- Delta CRL
- Έμμεσες CRL.

Η v3 δεν παρέχει μόνο τις τυπικές επεκτάσεις, αλλά προσφέρει τη δυνατότητα ορισμού ιδιωτικών επεκτάσεων (private extensions). Χρησιμοποιώντας την ευκολία αυτή, οι χρήστες μπορούν να δημιουργήσουν τις δικές τους ιδιόκτητες επεκτάσεις με σκοπό την αύξηση της λειτουργικότητας του προτύπου. Προσφέροντας αυτή την ευελιξία στους χρήστες, τους δίνεται η ευκαιρία να προσαρμόσουν τα πιστοποιητικά τους στις ανάγκες τους.

Ένα ακόμη σημαντικό θέμα σχετικό με τις επεκτάσεις είναι εκείνο της κρισιμότητας. Η κρισιμότητα είναι μία δυαδική τιμή (αληθής ή ψευδής) που ανατίθεται σε κάθε επέκταση. Η ύπαρξη της τιμής "αληθές" στην επέκταση της κρισιμότητας, σημαίνει ότι οποιαδήποτε οντότητα ελέγχει την εγκυρότητα του πιστοποιητικού πρέπει να κατέχει τη γνώση των σκοπών και την πληροφορία χειρισμού για τη συγκεκριμένη επέκταση. Σε αντίθετη περίπτωση, το πιστοποιητικό θεωρείται άκυρο. Η τιμή "ψευδές" καθιστά την παραπάνω προϋπόθεση προαιρετική. Κάθε CSP αναθέτει την τιμή της κρισιμότητας κατά βούληση.

3.4 Εφαρμογές της Υποδομής Δημόσιου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού θα μπορούσε να έχει πολλές εφαρμογές σε ένα Ακαδημαϊκό Ίδρυμα για παράδειγμα. Όπως:

1. *Ασφαλές Ηλεκτρονικό Ταχυδρομείο*

   Ο χρήστης του ηλεκτρονικού ταχυδρομείου που έχει αποκτήσει προσωπικό ψηφιακό πιστοποιητικό από μια Αρχή Πιστοποίησης έχει τη δυνατότητα να ανταλλάσσει κρυπτογραφημένα μηνύματα, διαφυλάσσοντας έτσι την ασφάλεια των μηνυμάτων του και το απαραβίαστο της προσωπικής του ηλεκτρονικής αλληλογραφίας.

   Ο χρήστης κρυπτογραφεί το μήνυμα του με το δημόσιο κλειδί του παραλήπτη και το υπογράφει με την ψηφιακή του υπογραφή. Έτσι, μόνο ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα, με το ιδιωτικό του κλειδί, και να διαβάσει το περιεχόμενο του μηνύματος. Ακόμη, ο παραλήπτης είναι σίγουρος ότι ο αποστολέας είναι αυτός που δηλώνει ότι απέστειλε το μήνυμα, βασιζόμενος στην ψηφιακή υπογραφή που φέρει το μήνυμα, καθώς επίσης και ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί.

2. *Πρόσβαση σε Ασφαλείς Δικτυακούς Τόπους*

   Η αποδοχή της Αρχής Πιστοποίησης συνεπάγεται την προσθήκη ψηφιακών πιστοποιητικών στο λογισμικό πλοήγησης (browser) του χρήστη. Με βάση τα ιδιαίτερα χαρακτηριστικά του πιστοποιητικού αυτού, ο χρήστης έχει τη δυνατότητα να επισκεφτεί ασφαλείς δικτυακούς τόπους και να προσπελάσει δεδομένα, χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα.

3. *Προστασία Ευαίσθητων Δεδομένων σε Γραμματείες Τμημάτων και Διοικητικούς φορείς*

   Οι γραμματείες των τμημάτων ενός Ακαδημαϊκού Ιδρύματος καθώς επίσης και οι διοικητικές υπηρεσίες έχουν στη διάθεσή τους ιδιαίτερα ευαίσθητα δεδομένα που πρέπει να προστατευτούν.

   Η βαθμολογία φοιτητών, τα οικονομικά στοιχεία των εργαζομένων, τα διοικητικά έγγραφα, οι πρυτανικές αποφάσεις, είναι μερικά σημαντικά δεδομένα που δεν πρέπει να είναι κοινώς προσπελάσιμα, παρά μόνο από εξουσιοδοτημένα μέλη και επίσης πρέπει να προστατεύονται από παραβιάσεις και αλλοιώσεις.

   Η πιστοποίηση της ταυτότητας των χρηστών και η προστασία τέτοιου είδους δεδομένων μπορεί να επιτευχθεί με την Υποδομή Δημοσίου Κλειδιού. Με τα ψηφιακά πιστοποιητικά για τους χρήστες επιβεβαιώνεται η ταυτότητά τους και με τους μηχανισμούς κρυπτογράφησης βεβαιώνεται η ασφάλεια των δεδομένων.

4. *Προστασία Ερευνητικών Δεδομένων*

   Η προστασία ερευνητικών αποτελεσμάτων και μελετών είναι ιδιαίτερα σημαντική σε ένα ακαδημαϊκό ίδρυμα. Τα ευαίσθητα ερευνητικά δεδομένα που αποθηκεύονται σε εξυπηρετητές πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Επίσης, η δικτυακή μεταφορά τους σε εξουσιοδοτημένα μέλη της ακαδημαϊκής κοινότητας πρέπει να είναι ασφαλής.

   Η Υποδομή Δημοσίου Κλειδιού παρέχει μηχανισμούς ασφαλείας για αποθήκευση και μεταφορά ερευνητικών δεδομένων. Τα ερευνητικά δεδομένα κρυπτογραφούνται, έτσι ώστε μόνο εξουσιοδοτημένα μέλη να έχουν τη δυνατότητα να τα αποκρυπτογραφήσουν και να τα αποκτήσουν.

5. *Πρόσβαση σε Ηλεκτρονικές Βιβλιοθήκες*

Η πρόσβαση σε ηλεκτρονικές βιβλιοθήκες είναι ένα αναγκαίο εργαλείο για την ακαδημαϊκή έρευνα και μελέτη.

Στην πλειοψηφία, οι ηλεκτρονικές βιβλιοθήκες παρέχουν τη δυνατότητα σύνδεσης χρηστών που έχουν διεύθυνση δικτύου (IP) με συγκεκριμένη μορφή (π.χ. οι χρήστες του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης μπορούν να προσπελάσουν τα ψηφιακά δεδομένα της βιβλιοθήκης του Α.Π.Θ. μόνο αν έχουν διεύθυνση δικτύου της μορφής 155.207.x.y). Η λύση αυτή όχι μόνο δεν είναι ασφαλής, αλλά παρεμποδίζει και το έργο των ακαδημαϊκών μελών όταν αυτοί βρίσκονται εκτός του Ακαδημαϊκού Ιδρύματος ή συνδέονται μέσω κάποιου παροχέα δικτυακών υπηρεσιών (Internet Provider), οπότε και αποκτούν διεύθυνση δικτύου διαφορετικής μορφής.

Τα προβλήματα αυτά μπορούν να επιλυθούν με ένα πιο ευέλικτο σχήμα ταυτοποίησης των εξουσιοδοτημένων χρηστών. Η Υποδομή Δημοσίου Κλειδιού παρέχει ψηφιακά πιστοποιητικά για κάθε χρήστη, έτσι ώστε να επιβεβαιώνεται η ταυτότητά του και να έχει τη δυνατότητα πρόσβασης σε ηλεκτρονικές βιβλιοθήκες μόνο με βάση την ακαδημαϊκή του ιδιότητα.

6. *Πλέγμα Δεδομένων (Data GRID)*

Το Πλέγμα Δεδομένων είναι μια σχετικά νέα έννοια στην νέα ψηφιακή κοινωνία και αποδεικνύεται μια πολύ ουσιώδης δομή για τα Ακαδημαϊκά Ιδρύματα. Η δικτυακή αυτή δομή επιτρέπει σε ερευνητές, εργαστήρια και πανεπιστήμια από όλο τον κόσμο να συνενώνουν τις δυνάμεις τους για να έχουν μια δυναμική συνεργασία σε διάφορες ερευνητικές περιοχές.

Βασιζόμενοι σε μια κατανεμημένη δομή που περιλαμβάνει ηλεκτρονικές βιβλιοθήκες, δικτυακούς πόρους, χώρους αποθήκευσης ψηφιακών δεδομένων, υπολογιστικά συστήματα μεγάλης ισχύος ανά τον κόσμο, τα ακαδημαϊκά μέλη έχουν το δικαίωμα να χρησιμοποιήσουν τα μέσα αυτά, ανεξάρτητα από την φυσική τους τοποθεσία, με στόχο την έρευνα.

Για παράδειγμα χιλιάδες αστρονόμοι που ανήκουν σε διάφορα ακαδημαϊκά εργαστήρια του κόσμου και εστιάζουν σε μια ερευνητική περιοχή μπορούν να δημιουργήσουν ένα Πλέγμα Δεδομένων και να διαμοιράζονται όλα τα φυσικά μέσα που χρειάζονται για την έρευνα τους, ανεξάρτητα από την χωροταξική τους θέση.

Η πρόσβαση σε ερευνητικά δεδομένα, σε αποτελέσματα μελετών, σε δικτυακούς πόρους, σε χώρους αποθήκευσης δεδομένων και γενικότερα σε μέσα που χρησιμοποιούνται για έρευνα πρέπει να περιορίζεται μόνο σε εξουσιοδοτημένα μέλη της ακαδημαϊκής κοινότητας. Αυτό επιτυγχάνεται με την Υποδομή Δημοσίου Κλειδιού και με την αντιστοίχηση ψηφιακών πιστοποιητικών σε κάθε χρήστη, ώστε να επιβεβαιώνεται η ταυτότητάς τους.

7. *Δημιουργία Ερευνητικών Ιστοσελίδων με Δημόσια και Ιδιωτικά Τμήματα*

Πολλά ερευνητικά προγράμματα που εκπονούνται στα πλαίσια ακαδημαϊκών προγραμμάτων έχουν οργανωμένες ιστοσελίδες, όπου και δημοσιεύονται διάφορα στοιχεία και αποτελέσματα για το ερευνητικό έργο που επιτελείται.

Στα ερευνητικά αυτά έργα είναι πιθανό να συμμετέχουν επιστημονικοί συνεργάτες από άλλα ακαδημαϊκά ιδρύματα και να κρίνεται αναγκαία η απομακρυσμένη προσπέλαση συγκεκριμένων συνεργατών στα ερευνητικά δεδομένα. Έτσι δημιουργείται η ανάγκη να υπάρχουν ιστοσελίδες που να παρέχουν πληροφορίες και να παρουσιάζουν το ερευνητικό έργο σε κάθε ενδιαφερόμενο, αλλά παράλληλα να υπάρχει η δυνατότητα απομακρυσμένης πρόσβασης από συγκεκριμένα ακαδημαϊκά μέλη σε δεδομένα της έρευνας που δεν είναι προς κοινή δημοσίευση.

Η διάκριση των εξουσιοδοτημένων ακαδημαϊκών μελών που μπορούν να έχουν πρόσβαση σε όλα τα ερευνητικά δεδομένα και στους υπόλοιπους ενδιαφερόμενους που έχουν περιορισμένη

πρόσβαση, μπορεί να υλοποιηθεί με βάση την Υποδομή Δημοσίου Κλειδιού και την χρήση πιστοποιητικών. Ανάλογα με τα χαρακτηριστικά του πιστοποιητικού του χρήστη θα επιτρέπεται η αντίστοιχη προσπέλαση στην ερευνητική ιστοσελίδα.

8. *Υποβολή Ψηφιακά Υπογεγραμμένων Εργασιών*

Σε μερικά μαθήματα δίνεται η δυνατότητα υλοποίησης ή παράδοσης εργασιών μέσα από το περιβάλλον μιας ιστοσελίδας.

Η Υποδομή Δημοσίου Κλειδιού παρέχει έναν ασφαλή τρόπο να καθοριστεί ο αποστολέας της εργασίας, ότι η εργασία δεν έχει αλλοιωθεί και έχει υποβληθεί στο χρονικό διάστημα της ανάθεσης, όπως αυτό έχει αρχικά οριστεί (χρονοσφράγιση-timestamp).

9. *Υπογεγραμμένο Λογισμικό*

Η Υποδομή Δημοσίου Κλειδιού παρέχει ψηφιακά πιστοποιητικά σε χρήστες για να υπογράψουν το λογισμικό που αναπτύσσουν.

Οι ψηφιακές υπογραφές που συνοδεύουν το λογισμικό είναι τέτοιες ώστε οι αποδέκτες του λογισμικού να γνωρίζουν ποιος ανέπτυξε το λογισμικό καθώς επίσης και να είναι βέβαιοι ότι μπορούν να χρησιμοποιήσουν άμεσα το λογισμικό χωρίς να παρουσιαστούν προβλήματα ασφαλείας.

Κεφάλαιο

«Η Ασφάλεια στο Διαδίκτυο – Ι»

4.1 Τι είναι Ασφάλεια.

4.2 Εισαγωγικά.

4.3 Ιστορική Αναδρομή.

4.4 Αναλυτικά.

4.5 Αδυναμίες – Μειονεκτήματα του Πρωτοκόλλου SSL.

4.6 Επιθέσεις και Ανθεκτικότητα του πρωτοκόλλου SSL.

4.7 Σχέση του Πρωτοκόλλου SSL και του Μοντέλου OSI

4.8 Συνοπτικά.

4.1. Τι είναι Ασφάλεια

Ακολουθούν ορισμοί του όρου ασφάλεια:

- Ασφάλεια του Διαδικτύου είναι η άσκηση προφύλαξης και διατήρησης προσωπικών περιουσιών και πληροφοριών στο διαδίκτυο
- Στον τομέα της πληροφορικής, ο όρος ασφάλεια, αναφέρεται σε τεχνικές που χρησιμοποιούνται για την διασφάλιση ότι τα δεδομένα που αποθηκεύονται σε ένα ηλεκτρονικό υπολογιστή δεν θα μπορούν να διαβαστούν ή να αλλοιωθούν από οποιονδήποτε δίχως εξουσιοδότησή.
- Οι περισσότερες μετρήσεις ασφαλείας περιλαμβάνουν κρυπτογράφηση δεδομένων και κωδικούς.
- Κρυπτογράφηση δεδομένων είναι η διαδικασία μετατροπής του περιεχομένου του μηνύματος σε μορφή τέτοια που να είναι μη κατανοητή από μη εξουσιοδοτημένους αποδέκτες ή από αποδέκτες που δεν διαθέτουν το κατάλληλο εξοπλισμό αποκρυπτογράφησης.
- Κωδικός είναι μια κρυφή λέξη ή φράση που δίνει σε ένα χρήστη πρόσβαση σε ένα συγκεκριμένο πρόγραμμα ή σύστημα.

4.2 Εισαγωγικά

Η ασφαλής σύνδεση στο διαδίκτυο είναι μια από τις βασικές, άρα και σημαντικότερες, απαιτήσεις στον τομέα της ασφάλειας του Παγκόσμιου Ιστού. Το ερώτημα που προκύπτει είναι πως μπορεί να επιτευχθεί μια ασφαλής σύνδεση.

Ως απάντηση, μεταξύ άλλων, είναι και το πρωτόκολλο SSL (Secure Socket Layer) ή Ασφαλές Επίπεδο Υποδοχών. Το πρωτόκολλο αυτό είναι ένα από τα γνωστότερα πρωτόκολλα ασφαλείας που χρησιμοποιούνται για την διεκπεραίωση συναλλαγών στο Διαδίκτυο. Σε γενικές γραμμές, αυτό που ουσιαστικά κάνει, είναι σε κάθε μήνυμα να δημιουργείται ένα αποτύπωμα το οποίο, αν μεταβληθεί (παραδείγματος χάριν, αν κάποιος τρίτος προσπαθήσει να ανακτήσει απόρρητες πληροφορίες), τότε η συναλλαγή ματαιώνεται και ζητείται από το χρήστη να επανεισαγάγει τα στοιχεία του.

Το SSL χρησιμοποιεί κρυπτογράφηση με κοινό κλειδί, μια από τις ισχυρότερες μεθόδους κρυπτογράφησης

Σε απλά βήματα λειτουργεί ως εξής:

1°: Οι πληροφορίες κρυπτογραφούνται έτσι ώστε να μην είναι εφικτή η ανάγνωσή τους από τρίτους.

2°: Οι πληροφορίες ελέγχονται για την αυθεντικότητα τους με στόχο να μην είναι δυνατή η αποστολή και λήψη τους από και προς υπολογιστές που δεν είναι κατάλληλα εξουσιοδοτημένοι.

3°: Εξασφαλίζεται, με κατάλληλο τρόπο, η ακεραιότητα του μεταφερόμενου μηνύματος, έτσι ώστε κάποιος τρίτος να μη μπορεί να το αλλοιώσει.

4.3 Ιστορική αναδρομή

Όταν ο Παγκόσμιος Ιστός άρχισε να κάνει την δημόσια εμφάνισή του, χρησιμοποιήθηκε για την διάθεση στατικών σελίδων. Σύντομα όμως άρχισε να χρησιμοποιείται και για άλλους σκοπούς (κυρίως

εμπορικούς πλέον), όπως για την πραγματοποίηση χρηματικών συναλλαγών (e-banking, e-shopping, κ.α.). Ως επακόλουθο προέκυψε η ανάγκη για την ύπαρξη όχι απλά μιας σύνδεσης στο διαδίκτυο αλλά μιας ασφαλούς σύνδεσης σε αυτό.

Έτσι το 1995 η εταιρεία Netscape Communications, που ήταν ένας από τους δύο κορυφαίους δημιουργούς λογισμικού πλοήγησης, του Netscape Communicator, στην προσπάθεια να ανταποκριθεί στην παραπάνω ανάγκη, παρουσίασε το πακέτο ασφάλειας SSL.

Το πρωτόκολλο SSL σχεδιάστηκε και αναπτύχθηκε, αρχικά, για την χρήση του με την εφαρμογή Netscape Communicator. Όμως αργότερα χρησιμοποιήθηκε ευρέως, ακόμη και από τον φυλλομετρητή της Microsoft γνωστό ως Internet Explorer.

Όσων αφορά την ανάπτυξή του πρωτοκόλλου, η έκδοση 1.0 χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της Netscape. Με την έκδοση ν.2.0 ενσωματώθηκε στις εκδόσεις 1. και 2. του Netscape Navigator. Σε αυτή την μορφή ήταν που το SSL καθιερώθηκε ως αναπόσπαστο πρότυπο για την παροχή κρυπτογραφικής προστασίας στην κυκλοφορία δεδομένων μέσω HTTP. Ωστόσο, επειδή υπήρχαν αρκετοί περιορισμοί σε αυτή την έκδοσή του, τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητα του, προέκυψε η αναβάθμιση του στην έκδοση 3.0. Αξίζει να αναφερθεί πως στην υλοποίηση αυτή της έκδοσης υπήρξε σημαντική συνεισφορά από τη βιομηχανία και η αναθεώρηση έγινε δημόσια. Η έκδοση αυτή τέθηκε επισήμως σε κυκλοφορία στα τέλη του 1995. Η τελική του σύνθεση, με τις τελικές προδιαγραφές, κυκλοφόρησε τέλη του επόμενου έτους.

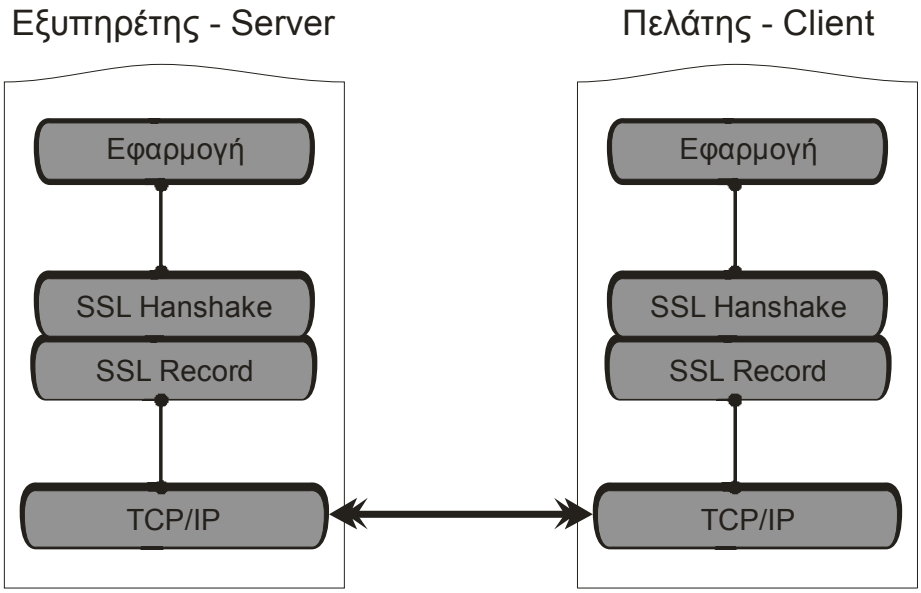
4.4 Αναλυτικά

Στο σχήμα που ακολουθεί (Σχήμα 4.1) φαίνεται η θέση του SSL στην στοίβα με τα συνηθισμένα πρωτόκολλα στα αντίστοιχα επίπεδα που αφορούν ένα τυπικό κοινό χρήστη που περιηγείται στον παγκόσμιο Ιστό με χρήση του πρωτοκόλλου SSL.

Πρωτόκολλο – Protocol
Εφαρμογών – HTTP (HyperText Transfer Protocol)
Ασφάλειας – SSL (Secure Socket Layer)
Μεταφοράς – TCP (Transmission Control Protocol)
Δικτύου – IP (Internet Protocol)
Συνδέσμου Μετάδοσης Δεδομένων – PPP (Point to Point Protocol)
Φυσικό Επίπεδο (Modem, PSTN/ISDN/ADSL, Καλωδιακή-Cable)

Σχήμα 4.1 : Επίπεδα & πρωτόκολλα για έναν τυπικό κοινό χρήστη που περιηγείται στον Ιστό μέσω SSL.

Στο επόμενο σχήμα (Σχήμα 4.2) απεικονίζεται η αρχιτεκτονική θεώρηση του SSL. Το SSL στρωματοποιείται στην κορυφή μίας αξιόπιστης υπηρεσίας μεταφοράς όπως εκείνη που παρέχεται από το TCP/IP και είναι σε θέση να παρέχει υπηρεσίες ασφάλειας για όλες τις TCP/IP εφαρμογές. Στην πραγματικότητα, ένα σημαντικό πλεονέκτημα της ασφάλειας επίπεδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς (transparently) σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιηθεί στην κορυφή του.



Σχήμα 4.2: Η αρχιτεκτονική τοποθέτηση του SSL.

Συνοπτικά, το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού.
- Επιτυγχάνεται η εμπιστευτικότητα των μεταδιδόμενων δεδομένων, αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μία αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs (**Message Authentication Codes**).

Είναι αξιοσημείωτο το γεγονός ότι το SSL πρωτόκολλο δεν παρέχει προστασία έναντι επιθέσεων ανάλυσης κυκλοφορίας (traffic analysis). Με την επίθεση αυτή ένας επιτεθείς (attacker) μπορεί να αποκτήσει σημαντικές πληροφορίες παρακολουθώντας, για παράδειγμα, τη συχνότητας και τον χρονισμό πακέτων στο δικτύου (network packets).

Για παράδειγμα, ένας αναλυτής κυκλοφορίας (ο επιτεθείς) εξετάζοντας τις μη κρυπτογραφημένες IP διευθύνσεις αποστολέα και παραλήπτη και τους TCP αριθμούς θυρών ή παρακολουθώντας τον όγκο της ροής κυκλοφορίας του δικτύου μπορεί εν τέλει να μάθει ποια μέρη αλληλεπιδρούν, ποιοι τύποι υπηρεσιών χρησιμοποιούνται, ή μερικές φορές να ανακτήσει πληροφορίες για επιχειρηματικές ή προσωπικές σχέσεις. Πάντως είναι γνωστό ότι η απειλή των επιθέσεων ανάλυσης κυκλοφορίας στην κοινότητα των χρηστών, σε γενικές γραμμές, θεωρείται σχετικά ακίνδυνη.

Για να χρησιμοποιηθεί το SSL θα πρέπει τόσο ο εξυπηρετούμενος όσο και ο εξυπηρέτης να γνωρίζουν ότι και η άλλη πλευρά χρησιμοποιεί επίσης το SSL. Γενικά, υπάρχουν τρεις δυνατές λύσεις για την αντιμετώπιση αυτού του ζητήματος :

1) Να χρησιμοποιηθούν αφιερωμένοι αριθμοί θυρών που δεσμεύονται από την IANA (**Internet Assigned Numbers Authority**). Θα πρέπει να ανατίθεται ένας ξεχωριστός αριθμός θύρας για κάθε πρωτόκολλο εφαρμογής που υποστηρίζει SSL.
2) Να χρησιμοποιείται ο κανονικός αριθμός θύρας για κάθε πρωτόκολλο εφαρμογής και να συμφωνούνται επιλογές ασφάλειας ως μέρος του πρωτοκόλλου εφαρμογής.
3) Να χρησιμοποιείται μία επιλογή TCP για τη χρήση ενός πρωτοκόλλου ασφάλειας, όπως το SSL, κατά τη διάρκεια της φάσης καθιέρωσης της κανονικής TCP/IP σύνδεσης.

Το μειονέκτημα που προκύπτει είναι πως η συμφωνία των επιλογών ασφάλειας, ανάλογα με την εφαρμογή, απαιτεί την τροποποίηση του κάθε πρωτοκόλλου εφαρμογής έτσι ώστε να προσαρμόζεται στην συμφωνημένη διαδικασία.

Στην πράξη, έχουν κρατηθεί και καθορισθεί από την IANA ξεχωριστοί αριθμοί θυρών για κάθε πρωτόκολλο εφαρμογής με υποστήριξη SSL. Αυτοί οι αριθμοί θυρών περιγράφονται στους πίνακες που ακολουθούν (Πίνακας 4.1 και 4.2).

Λέξη κλειδί	Θύρα	Περιγραφή
https	443	HTTP με υποστήριξη SSL
Ssmtp	465	SMTP με υποστήριξη SSL
Snntp	563	NNTP με υποστήριξη SSL
Sldap	636	LPAD με υποστήριξη SSL
Spop3	995	POP3 με υποστήριξη SSL

Πίνακας 4.1 : Αριθμοί Θυρών που έχουν ανατεθεί για Πρωτόκολλα Εφαρμογών με υποστήριξη SSL.

Λέξη κλειδί	Θύρα	Περιγραφή
FTP-DATA	889	FTP data με υποστήριξη SSL
FTPs	990	FTP control με υποστήριξη SSL
IMAPs	991	IMAP4 με υποστήριξη SSL
TELNETs	992	TELNET με υποστήριξη SSL
IRCs	993	IRC με υποστήριξη SSL

Πίνακας 4.2 : Αριθμοί Θυρών που χρησιμοποιούνται για Πρωτόκολλα Εφαρμογών με υποστήριξη SSL.

Αναλύοντας κατά βάση το πρωτόκολλο SSL και όπως αυτό απεικονίζεται, στο Σχήμα 4.2, αποτελείται από δύο επιμέρους πρωτόκολλα, το SSL Record Protocol (SSLRP) και το SSL Handshake Protocol (SSLHP). Ακολουθεί συνοπτική περιγραφή τους :

- Το Record Protocol παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων σε μία προσανατολισμένη στη σύνδεση αξιόπιστη υπηρεσία μεταφοράς, όπως αυτή που παρέχεται από το TCP. Το πρωτόκολλο αυτό λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό (fragmentation), τη συμπίεση, την αυθεντικοποίηση και την κρυπτογράφηση δεδομένων.
- Το Handshake Protocol, που αποτελεί το σημαντικότερο από τα πολλαπλά πρωτόκολλα SSL που μπορούν να τοποθετούνται πάνω από το Record Protocol, αποτελεί ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών το οποίο επίσης διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφάλειας και την αντίστοιχη κατάσταση στα δύο άκρα της σύνδεσης. Μετά την ολοκλήρωση αυτού, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του Record Protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας και κατάστασης. Σκοπός του SSL handshake protocol είναι να υποχρεώνει έναν εξυπηρετούμενο και έναν εξυπηρέτη να καθιερώνουν τα πρωτόκολλα που θα χρησιμοποιηθούν κατά τη διάρκεια της επικοινωνίας, να επιλέγουν τη μέθοδο συμπίεσης και την προδιαγραφή κρυπτογραφίας, προαιρετικά να αυθεντικοποιούνται αμοιβαία και να δημιουργούν ένα κύριο μυστικό κλειδί (master secret key), από το οποίο προκύπτουν τα διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων.

Μια απλή περιγραφή εφαρμογής τους ακολουθεί :

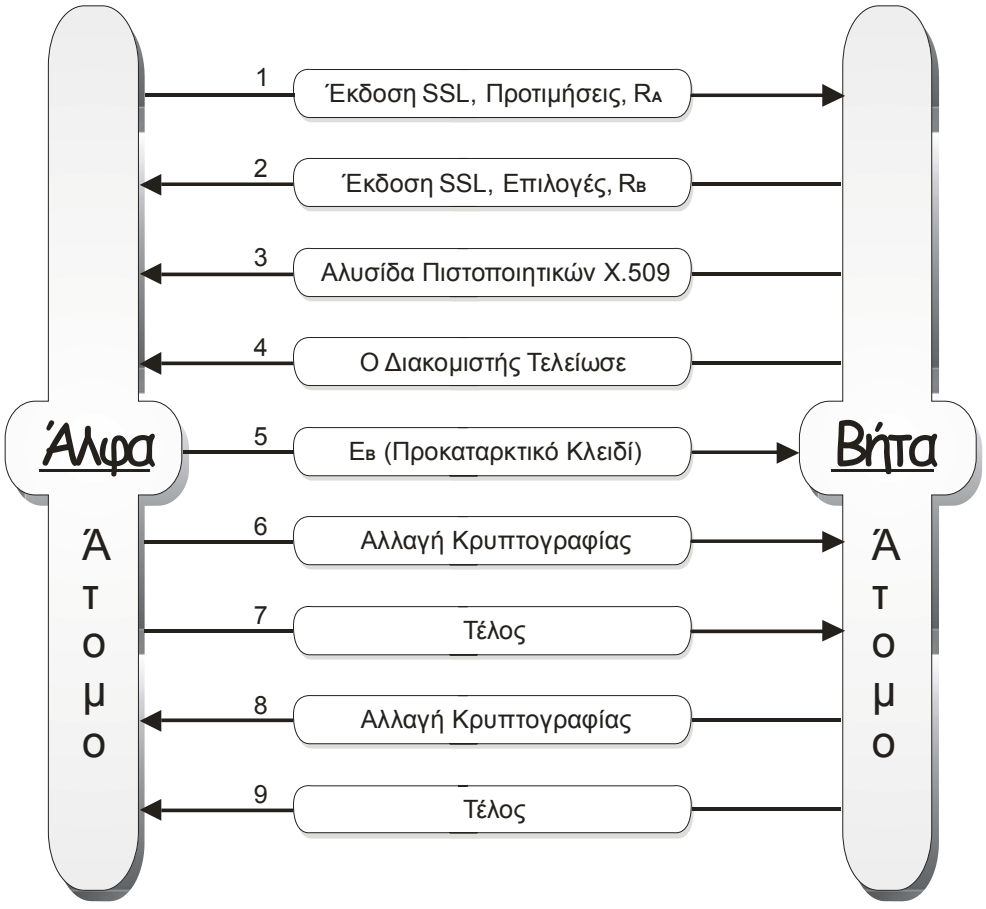
Ας αρχίσουμε με την εξέταση του τρόπου εγκαθίδρυσης ασφαλών συνδέσεων – Handshake Protocol. Το υποπρωτόκολλο εγκαθίδρυσης συνδέσεων φαίνεται στο Σχήμα 4.3. Ξεκινά με το μήνυμα 1, όταν ο Άλφα στέλνει μια αίτηση στον Βήτα για την εγκαθίδρυση μιας σύνδεσης. Η αίτηση καθορίζει την έκδοση SSL που έχει ο Άλφα και τις προτιμήσεις του σχετικά με τους αλγόριθμους συμπίεσης και κρυπτογραφίας. Περιέχει επίσης έναν αριθμό μίας χρήσης R_A, ο οποίος θα χρησιμοποιηθεί αργότερα.

Στη συνέχεια είναι η σειρά του Βήτα. Στο μήνυμα 2 ο Βήτα κάνει μια επιλογή ανάμεσα στους διάφορους αλγόριθμους που μπορεί να υποστηρίξει ο Άλφα και στέλνει το δικό του αριθμό μίας χρήσης R_B. Στη συνέχεια, στο μήνυμα 3, στέλνει ένα πιστοποιητικό που περιέχει το δημόσιο κλειδί του. Αν το πιστοποιητικό αυτό δεν υπογράφεται από κάποια ευρέως γνωστή αρχή, στέλνει επίσης και μια αλυσίδα πιστοποιητικών που μπορούν να ακολουθηθούν μέχρι μια τέτοια αρχή. Όλα τα προγράμματα πλοήγησης, συμπεριλαμβανομένου αυτού του Άλφα, έχουν προκαταβολικά εγκατεστημένα γύρω στα 100 δημόσια κλειδιά — έτσι, αν ο Βήτα μπορέσει να εγκαθιδρύσει μια αλυσίδα που να επικυρώνεται σε κάποιο από αυτά, ο Άλφα θα είναι σε θέση να επαληθεύσει το δημόσιο κλειδί του Βήτα. Στο σημείο αυτό ο Βήτα μπορεί να στείλει κάποια άλλα μηνύματα (όπως μια αίτηση για το πιστοποιητικό δημόσιου κλειδιού του Άλφα). Όταν ο Βήτα τελειώσει, στέλνει το μήνυμα 4 για να πει στον Άλφα ότι είναι η σειρά του.

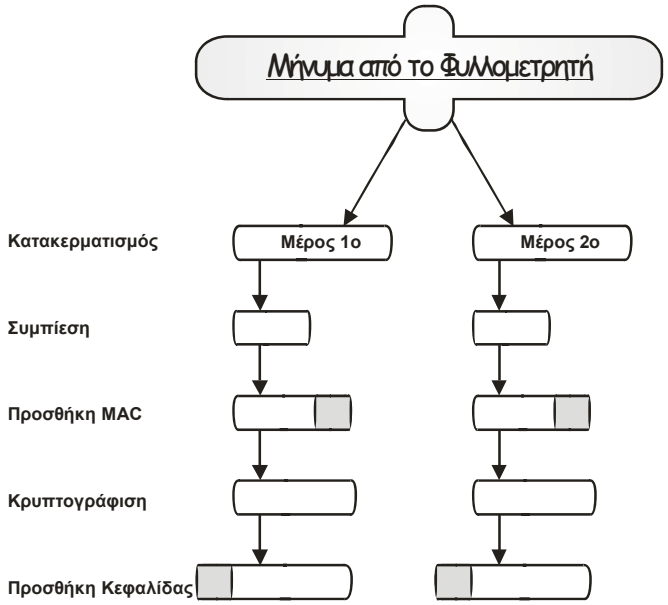
Ο Άλφα αποκρίνεται επιλέγοντας ένα τυχαίο προκαταρκτικό κλειδί (Premaster key) των 384 bit και στέλνοντας το στον Βήτα κρυπτογραφημένο με το δημόσιο κλειδί του (μήνυμα 5), Το πραγματικό κλειδί συνόδου που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων συνάγεται με περίπλοκο τρόπο από το προκαταρκτικό κλειδί σε συνδυασμό με τους δύο αριθμούς μίας χρήσης. Αφού ληφθεί το μήνυμα 5, τόσο ο Άλφα όσο και ο Βήτα είναι σε θέση να υπολογίσουν το κλειδί συνόδου. Για το λόγο αυτόν, ο Άλφα λέει στον Βήτα να μεταβεί στη νέα κρυπτογραφία (μήνυμα 6) και δηλώνει επίσης ότι έχει τελειώσει με το υποπρωτόκολλο εγκαθίδρυσης (μήνυμα 7). Ο Βήτα επιβεβαιώνει τότε τη λήψη των μηνυμάτων του (μηνύματα 8 και 9).

Ωστόσο, αν και ο Άλφα γνωρίζει ποιος είναι ο Βήτα, ο Βήτα δεν γνωρίζει ποιος είναι ο Άλφα (εκτός και αν ο Άλφα έχει ένα δημόσιο κλειδί και ένα αντίστοιχο πιστοποιητικό για αυτό, περίπτωση μάλλον απίθανη για έναν ιδιώτη). Έτσι, το πρώτο μήνυμα του Βήτα μπορεί να είναι μια αίτηση προς τον Άλφα να συνδεθεί χρησιμοποιώντας ένα εκ των προτέρων ορισμένο όνομα χρήστη και συνθηματικό. Το πρωτόκολλο σύνδεσης είναι, όμως, έξω από την εμβέλεια του SSL. Αφού επιτευχθεί, με οποιονδήποτε τρόπο, η σύνδεση μπορεί να αρχίσει η μετάδοση δεδομένων.

Για την πραγματική μεταφορά χρησιμοποιείται ένα δεύτερο υποπρωτόκολλο, όπως φαίνεται στο Σχήμα 4.4. Τα μηνύματα του προγράμματος πλοήγησης τεμαχίζονται αρχικά σε τμήματα μεγέθους μέχρι και 16 KB. Αν είναι ενεργοποιημένη η συμπίεση, κάθε τμήμα συμπιέζεται χωριστά. Μετά από αυτό το βήμα, ένα μυστικό κλειδί που συνάγεται από τους δύο αριθμούς μίας χρήσης και το προκαταρκτικό κλειδί συνενώνεται με το συμπιεσμένο κείμενο και το αποτέλεσμα κατακερματίζεται με το συμφωνημένο αλγόριθμο κατακερματισμού. Ο κατακερματισμός προσαρτάται σε κάθε τμήμα ως κωδικός πιστοποίησης ταυτότητας μηνύματος (MAC). Το συμπιεσμένο θραύσμα μαζί με τον κωδικό MAC κρυπτογραφείται στη συνέχεια με το συμφωνημένο συμμετρικό αλγόριθμο κρυπτογράφησης. Τέλος προστίθεται μια κεφαλίδα τμήματος, και το τμήμα μεταδίδεται μέσω της σύνδεσης TCP.



Σχήμα 4.3: Μια απλοποιημένη έκδοση του υποπρωτοκόλλου εγκαθίδρυσης σύνδεσης – handshake του SSL.



Σχήμα 4.4: Μετάδοση δεδομένων μέσω του πρωτοκόλλου SSL.

Συμπερασματικά, το πρωτόκολλο SSL μπορεί να χρησιμοποιείται για την εγκαθίδρυση ασφαλών συνδέσεων μεταξύ εξυπηρετουμένων και εξυπηρετών (clients – servers). Συγκεκριμένα, μπορεί να χρησιμοποιείται για να αυθεντικοποιεί έναν εξυπηρέτη και προαιρετικά τον εξυπηρετούμενο, να εκτελεί ανταλλαγή κλειδιών και να παρέχει αυθεντικοποίηση μηνυμάτων, καθώς επίσης και υπηρεσίες εμπιστευτικότητας και ακεραιότητας δεδομένων για αυθαίρετες TCP/IP εφαρμογές.

Μολονότι μπορεί να φαίνεται ότι η μη διασφάλιση αυθεντικοποίησης εξυπηρετούμενου αντιβαίνει τις αρχές που θα πρέπει να υιοθετούνται από ένα ασφαλές σύστημα, η απόφαση για προαιρετική υποστήριξη βοήθησε το πρωτόκολλο SSL να διαδοθεί ευρύτερα και το βοηθά ακόμη και σήμερα: η υποστήριξη της αυθεντικοποίησης εξυπηρετούμενου απαιτεί ξεχωριστά δημόσια κλειδιά και πιστοποιητικά για κάθε εξυπηρετούμενο και από τη στιγμή που η υποστήριξη για το SSL πρέπει να ενσωματώνεται στο αντίστοιχο λογισμικό εξυπηρετούμενου, όπως είναι ένα πρόγραμμα πλοήγησης, η απαίτηση για αυθεντικοποίηση εξυπηρετούμενου θα είχε ως συνέπεια τη διανομή δημόσιων κλειδιών και πιστοποιητικών για κάθε χρήστη στο Internet.

Βραχυπρόθεσμα, θεωρείται περισσότερο κρίσιμο οι τελικοί καταναλωτές σε περιβάλλον ηλεκτρονικού εμπορίου να μπορούν να ενημερώνονται σχετικά με την ταυτότητα των εμπόρων με τους οποίους συναλλάσσονται, παρά να απαιτείται ίδιος βαθμός ασφάλειας και από τους εμπόρους για τους καταναλωτές. Επιπλέον, αφού ο αριθμός των εξυπηρετών Internet είναι πολύ μικρότερος από τον αριθμό των

εξυπηρετούμενων, είναι ευκολότερο και πιο πρακτικό να εφοδιάζονται οι εξυπηρέτες με τα απαραίτητα δημόσια κλειδιά και πιστοποιητικά.

Σήμερα, το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το Internet γενικά και τον ιστό συγκεκριμένα. Παραδείγματα δημόσιων και δωρεάν διαθέσιμων SSL υλοποιήσεων είναι το SSLref που αναπτύχθηκε από τη Netscape Communications και το SSLeay που αναπτύχθηκε από τον E.Young, το OpenSSL αποτελεί μία ιδιαίτερα ενδιαφέρουσα υλοποίηση του SSL σε περιβάλλον ανοιχτού κώδικα.

Είναι επίσης ενδιαφέρον να σημειωθεί ότι οι περισσότερες Ελβετικές τράπεζες που προσφέρουν τις υπηρεσίες τους διαμέσου του Internet έχουν αναπτύξει την ασφάλεια των εφαρμογών ηλεκτρονικής τραπεζικής με βάση το πρωτόκολλο SSL. Αυτή η απόφαση είναι στην ίδια κατεύθυνση με τη στρατηγική της Ευρωπαϊκής Επιτροπής για Τραπεζικά Πρότυπα (European Committee for Banking Standards - ECBS).

Browsers – προγράμματα πλοήγησης, όπως ο Firefox της Mozila Foundation, έχουν επιλεγμένη από την αρχή την χρήση SSL 2.0 και 3.0.

Ωστόσο, οι ευρύτερα αναπτυγμένες και μαζικά χρησιμοποιούμενες εφαρμογές του SSL συναντώνται συνήθως σε HTTP προϊόντα εξυπηρετών και εξυπηρετούμενων. Για παράδειγμα, υπάρχουν αρκετοί HTTP εξυπηρέτες διαθέσιμοι οι οποίοι υποστηρίζουν το SSL. Συνήθως αυτοί οι εξυπηρέτες καλούνται ασφαλείς εξυπηρέτες (secure servers). Από την πλευρά του εξυπηρετούμενου, σήμερα, τα περισσότερα προγράμματα πλοήγησης ιστού υποστηρίζουν το SSL.

4.5 Αδυναμίες - Μειονεκτήματα του Πρωτοκόλλου SSL

Η μεγαλύτερη ίσως αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά.

Ένα άλλο μειονέκτημα της χρήσης του SSL πρωτοκόλλου αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του προγράμματος πλοήγησης του εξυπηρετούμενου με τον HTTPS εξυπηρέτη. Η καθυστέρηση οφείλεται στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίηση της SSL συνόδου. Πρακτικά, οι χρήστες αντιλαμβάνονται μικρή καθυστέρηση λίγων δευτερολέπτων μεταξύ της έναρξης συνόδου με τον HTTPS εξυπηρέτη και της ανάκτησης της πρώτης HTML σελίδας από αυτόν. Επειδή κατά τη σχεδίαση του SSL αποθηκεύεται το κύριο μυστικό κλειδί, η καθυστέρηση επηρεάζει μόνον την πρώτη SSL επικοινωνία μεταξύ προγράμματος πλοήγησης και HTTPS εξυπηρέτη.

Επίσης, μόνο στην έκδοση 2.0, υπάρχει αδυναμία που αφορά την επαναδιαπραγμάτευση κλειδιών συνόδου. Από τη στιγμή που μία σύνοδος δημιουργηθεί, το ίδιο κλειδί (master key) χρησιμοποιείται καθ' όλη τη διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνοδο (π.χ. μιας εφαρμογής TELNET), η αδυναμία αλλαγής του κλειδιού γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχούς «Ευθείας Επίθεσης» (Brute Force Attack).

4.6 Επιθέσεις και Ανθεκτικότητα του Πρωτοκόλλου SSL

Όπως συμβαίνει σε όλα τα πρωτόκολλα και υπηρεσίες δικτύων, έτσι και εδώ υπάρχουν συγκεκριμένες επιθέσεις που μπορούν να χρησιμοποιηθούν ενάντια στο πρωτόκολλο SSL ή σε εφαρμογές του. Ας σημειωθεί ότι η εύρεση μιας αδυναμίας σε μια συγκεκριμένη εφαρμογή του πρωτοκόλλου SSL δεν σημαίνει απαραίτητα ότι υπάρχει κάποιο ελάττωμα στο πρωτόκολλο SSL. Αυτό που τελικά προκύπτει είναι ότι η εφαρμογή μπορεί να είναι ευάλωτη σε μια συγκεκριμένη επίθεση ή λόγο κάποιας αδυναμίας, που όμως δεν εξυπακούεται πως όλες οι εφαρμογές υλοποιημένες με το πρωτόκολλο αυτό είναι τρωτές.

Ακολουθεί ένας κατάλογος αποτελούμενος από τις συχνότερα χρησιμοποιούμενες μεθόδους επίθεσης που θα μπορούσαν να χρησιμοποιηθούν για να παρακάμψουν το SSL πρωτόκολλο.

4.6.1 Επιθέσεις κρυπτογραφίας - Cipher Attacks ή Cracking Ciphers

Επειδή το πρωτόκολλο SSL χρησιμοποιεί πολλαπλές διαφορετικές τεχνολογίες για την εν δυνάμει κρυπτογράφηση (underlying encryption), οι επιθέσεις στην μηχανή κρυπτογράφησης ή στα κλειδιά είναι πιθανές. Εάν μια επίθεση, ενάντια σε οποιαδήποτε από τις διαθέσιμες μηχανές κρυπτογράφησης, βρεθεί να είναι επιτυχής, τότε το πρωτόκολλο SSL παύει να είναι ασφαλές.

Συνεπώς, οποιαδήποτε από τις διαθέσιμες μεθόδους κρυπτογραφικής ανάλυσης μπορούν να χρησιμοποιηθούν. Αυτό περιλαμβάνει την καταγραφή μιας συγκεκριμένης συνόδου - session επικοινωνίας και τη χρησιμοποίηση πολλών κύκλων επεξεργασίας από την ΚΜΕ (CPU) για να «σπάσει - crack» είτε την σύνοδο αυτή είτε το δημόσιο κλειδί που χρησιμοποιήθηκε.

Επειδή πολλές SSL σύνοδοι χρησιμοποιούν κλειδιά των 128 bit, το κόστος μιας επίθεσης ενάντια ενός τέτοιου κλειδιού είναι ακόμα αρκετά υψηλό. Καθώς νέα πρωτόκολλα και κλειδιά μεγαλύτερου μήκους υποστηρίζονται από το SSL πρωτόκολλο, ο απαιτούμενος φόρτος εργασίας για την αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος αυξάνεται.

4.6.2 Clear Text Attacks - Επίθεση Λεξικού (Dictionary Attack)

Οι επιθέσεις τύπου Clear Text (όπως auth challenge, fragmentation attack) αποτέλεσαν και αποτελούν γεγονός που αφορά το πρωτόκολλο SSL. Επειδή πολλά μηνύματα στο SSL είναι ίδια, όπως οι εντολές HTTP Get, ένας επιτιθέμενος μπορεί να υλοποιήσει ένα λεξικό όπου τα λήμματα είναι γνωστές τιμές συγκεκριμένων λέξεων ή φράσεων. Ο επιτιθέμενος έπειτα ωτακούει μια σύνοδο και συγκρίνει τα στοιχεία της συνόδου αυτής με το περιεχόμενο του λεξικού. Οποιαδήποτε αντιστοιχία δείχνει το κλειδί συνόδου που χρησιμοποιήθηκε και έτσι ολόκληρο το πακέτο δεδομένων μπορεί πλέον να αποκρυπτογραφηθεί.

Ο συντελεστής του όγκου εργασίας της clear text επίθεσης είναι αρκετά υψηλός. Για κάθε κομμάτι που προστίθεται στο κλειδί, το μέγεθος του λεξικού αυξάνεται με παράγοντα το δύο. Αυτό καθιστά ουσιαστικά αδύνατο το χτίσιμο ενός λεξικού με αρκετά λήμματα για την επιτυχή αποκρυπτογράφηση ενός κλειδιού μήκους 128 bit χρησιμοποιώντας μια clear text μεθοδολογία επίθεσης.

Λαμβάνοντας υπόψη τον υψηλό παράγοντα επεξεργασίας που απαιτείται από μια clear text επίθεση, μια «Ευθείας Επίθεσης» (Brute Force Attack), ακόμη και με τον υψηλό παράγοντα εργασίας αυτής, θεωρείται φθηνότερη από τις δύο αυτές. Εντούτοις, οι brute force επιθέσεις απαιτούν και αυτές υπερβολικά μεγάλη επεξεργαστική ισχύ της Κ.Μ.Ε. καθώς και χρόνο. Ακόμη και με το σημερινό διαθέσιμο εξοπλισμό μεγάλων υπολογιστικών μονάδων, ο παράγοντας εργασίας (work factor) που σχετίζεται με brute force επιθέσεις σε κλειδιά των 128 bit θεωρείται ακόμα ένα υπέρμετρα μεγάλο πρόβλημα.

Έτσι το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα (128 bits). Ακόμα και οι αλγόριθμοι σε προϊόντα για χρήση εκτός Η.Π.Α. υποστηρίζουν κλειδιά των 128 bits και παρόλο που τα 88 bits αυτών μεταδίδονται χωρίς κρυπτογράφηση, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών καθιστά την επίθεση εξαιρετικά δύσκολη.

4.6.3 «Ευθείας Επίθεσης» (Brute Force Attack)

Εν συντομία, η επίθεση αυτή θα δοκιμάσει όλους τους πιθανούς συνδυασμούς κάθε κλειδιού προκειμένου να «σπάσει» τον κωδικό πρόσβασης – password. Η μόνη προφύλαξη είναι είτε το μήκος του κλειδιού να είναι πολύ μεγάλο για να «σπασθεί» είτε να γίνεται συχνή αλλαγή αυτού.

Πραγματοποιείται με τη χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι μάταιη.

4.6.4 Επίθεση Επανάληψης (Replay Attack)

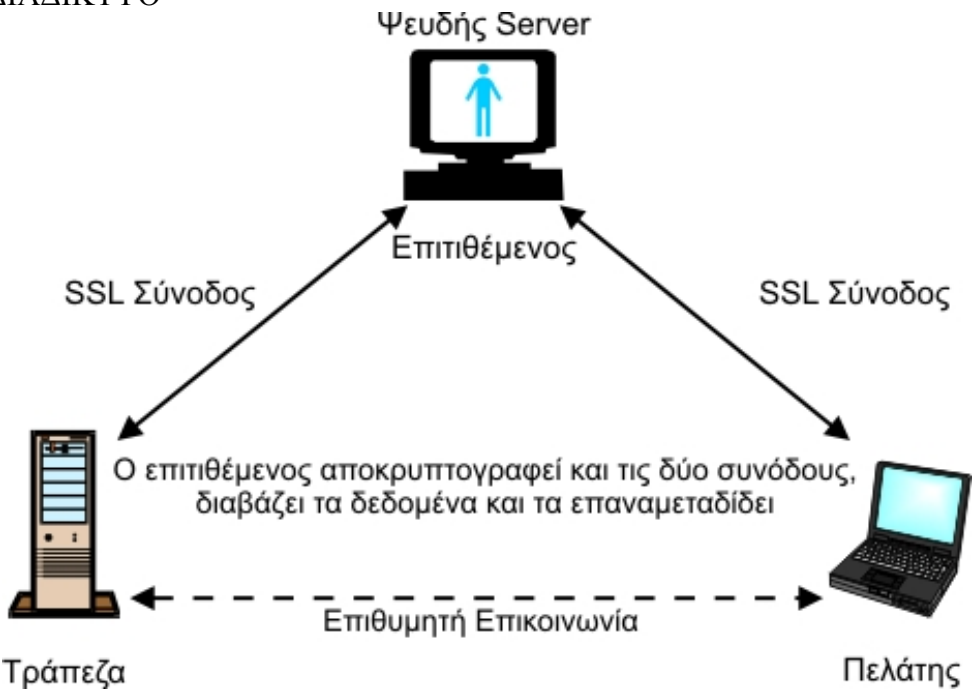
Οι επιθέσεις επανάληψης εμπλέκουν τον επιτιθέμενο που καταγράφει μια επικοινωνία μεταξύ του πελάτη και του κεντρικού υπολογιστή – εξυπηρέτη και αργότερα αυτός συνδέετε με τον κεντρικό υπολογιστή και του ξαναστέλνει τα καταγεγραμμένα μηνύματα. Ενώ μια επίθεση επανάληψης είναι εύκολο να δημιουργηθεί, το πρωτόκολλο SSL χρησιμοποιεί μια ταυτότητα – αναγνωριστικό σύνδεσης (connection ID) που παράγεται από τον εξυπηρέτη με τυχαίο τρόπο και ισχύει μόνο για εκείνη την σύνδεση. Συνεπώς, αφού δεν είναι ποτέ δυνατόν να υπάρχουν δύο ίδια αναγνωριστικά σύνδεσης, ο επιτιθέμενος δεν μπορεί επιτυχώς να χρησιμοποιήσει τις καταγεγραμμένες πληροφορίες. Επειδή η SSL χρησιμοποιεί μια 128 bit τιμή ταυτότητα σύνδεσης, ένας επιτιθέμενος θα έπρεπε να καταγράψει τουλάχιστον 2^{64} συνόδους για να έχει μια πιθανότητα 50% για την απόκτηση μιας έγκυρης ταυτότητας σύνδεσης.

4.6.5 Επίθεση Παρεμβολής (Man-ln-The-Middle Attack)

Η επίθεση τύπου Man-ln-The-Middle, όπως φαίνεται στο Σχήμα 4.5, υλοποιείται με την ύπαρξη ενός τρίτου ατόμου σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του εξυπηρέτη και του πελάτη, υποδυόμενος τον πραγματικό εξυπηρέτη.

Έχοντας πείσει τον πελάτη να πιστεύει πως έχει συνδεθεί με τον πραγματικό κεντρικό υπολογιστή, ο επιτιθέμενος μπορεί να αποκρυπτογραφήσει τα μηνύματα που στέλνονται από τον πελάτη, να συλλέξει τα δεδομένα, να τα τροποποιήσει όπως αυτός επιθυμεί, και στην συνέχεια να τα αναμεταδώσει στον πραγματικό κεντρικό υπολογιστή μέσω μιας SSL session μεταξύ του επιτιθεμένου και του πραγματικού κεντρικού υπολογιστή. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον εξυπηρέτη.

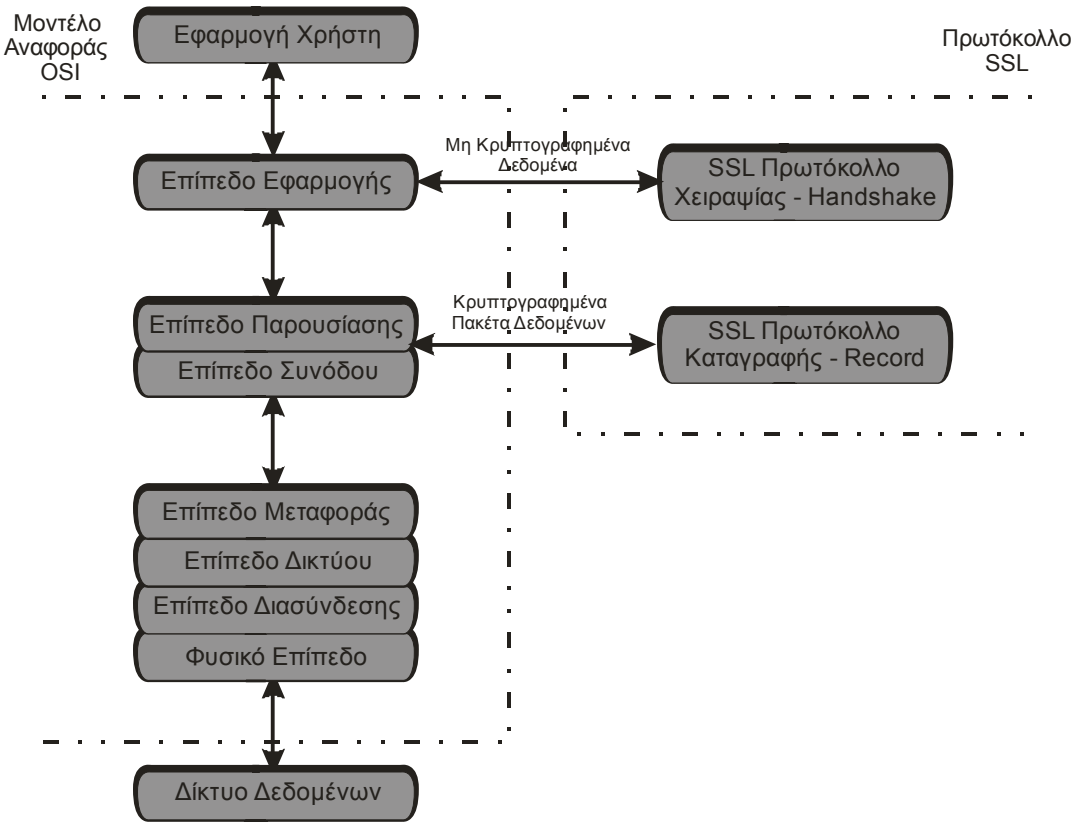
Η χρήση των πιστοποιητικών κεντρικών υπολογιστών καθιστά την επίθεση παρεμβολής δυσκολότερη. Εάν το πιστοποιητικό είναι πλαστογραφημένο έτσι ώστε να ταιριάξει με την ταυτότητα του πραγματικού κεντρικού υπολογιστή, η επαλήθευση υπογραφών θα αποτύχει. Εντούτοις, ο επιτιθέμενος θα μπορούσε να δημιουργήσει το δικό του/της έγκυρο πιστοποιητικό, αν και δεν θα ταίριαζε με το όνομα του πραγματικού κεντρικού υπολογιστή. Εάν το πιστοποιητικό ταιριάζει με τον επιτιθέμενο αλλά δεν ταιριάξει με το όνομα, ο χρήστης θα δει ένα σχετικό μήνυμα που θα του γνωστοποιεί το πρόβλημα. Εάν ο χρήστης αγνοήσει το μήνυμα αυτό, όπως πολλοί κάνουν, δεν γνωρίζει το πρόβλημα σύνδεσης.



Σχήμα 4.5: Επίθεση Παρεμβολής

4.7 Σχέση του Πρωτοκόλλου SSL και του μοντέλου OSI

Στο Σχήμα 4.6 παρουσιάζεται η σχέση του πρωτοκόλλου SSL και του μοντέλου διασύνδεσης ανοικτών συστημάτων – OSI.



Σχήμα 4.6: Σχέση των OSI και SSL

Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο **OSI,** έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Από το παραπάνω σχήμα (Σχήμα 4.6) παρατηρούμε πως το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του **OSI** και όχι ως πρωτόκολλο αντικατάστασης. Επίσης είναι φανερό ότι η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το SSL.

4.8 Συνοπτικά

Το SSL χρησιμοποιείται ευρύτατα ως βάση για σχεδόν όλη την κρυπτογραφημένη κυκλοφορία στον Ιστό προκειμένου για να αποτραπεί η απώλεια ευαίσθητων πληροφοριών σε ένα μη-ασφαλές δίκτυο. Μπορούμε να πούμε ότι το ηλεκτρονικό εμπόριο – e-commerce δεν θα ήταν όπου είναι σήμερα χωρίς το πρωτόκολλο SSL.

Το SSL παρέχει εμπιστευτικότητα δεδομένων και ακεραιότητας στοιχείων στη «χειραψία - handshake» για να αποφευχθεί η εκδήλωση επιτυχών επιθέσεων, αν και υπάρχει ένας ορισμένος βαθμός ανθρώπινης επέμβασης και κατανόησης που συνδέονται με την εφαρμογή της σωστή και κατάλληλης κίνησης την στιγμή που θα εμφανιστεί ένα πρόβλημα.

Επιπλέον, μόλις καθιερωθεί το SSL session, τα δεδομένα αυτά προστατεύονται από ωτακουστές – eavesdroppers, και δεν μπορούν να μεταβληθούν κατά τη διάρκεια της μετάδοσης μιας και τυχών αλλαγές θα οδηγήσουν στην αποτυχία της αποκρυπτογράφησης στον αποδέκτη, διατηρώντας την ακεραιότητα των δεδομένων.

Κεφάλαιο

«Κακόβουλες Επιθέσεις στο Διαδίκτυο»

5.1: Εισαγωγή

5.2: Ευαισθησίες και κίνδυνοι της ασφάλειας σε ένα δίκτυο

5.3: Είδη επιθέσεων στο διαδίκτυο

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

5.1 Εισαγωγή

Ένα δίκτυο συνίσταται από τη διασύνδεση δυο ή περισσοτέρων υπολογιστικών συστημάτων κατά τρόπο ώστε να παρέχεται η δυνατότητα στους χρήστες να επωφελούνται από ολόκληρο το υπολογιστικό δυναμικό. Αυτό πραγματοποιείται μέσω της ανταλλαγής πληροφοριών μεταξύ των χρηστών και της κοινής χρήσης των διαθέσιμων υπολογιστικών πόρων.

Το κεφάλαιο αυτό επικεντρώνεται στην ασφάλεια του διαδικτύου αρχίζοντας από την ευαισθησία των υποδομών του και προχωρώντας στους μηχανισμούς εκμετάλλευσης αυτών από τρίτους. Επίσης θα γίνει αναφορά στο κάθε εργαλείο-τεχνική και περιγραφή του μηχανισμού του καθενός ξεχωριστά.

Ένα εύλογο ερώτημα που απασχολεί τον σύγχρονο άνθρωπο ο οποίος βλέπει την τεχνολογία των ηλεκτρονικών υπολογιστών να καλπάζει και να αναπτύσσεται με γρήγορους ρυθμούς, είναι το γιατί οι υπολογιστές είναι ανασφαλείς. Από όσα βρέθηκαν σε Ελληνική αλλά και ξένη βιβλιογραφία η μεγάλη πλειοψηφία των περιπτώσεων εισβολών σχετίζεται με ένα από τα παρακάτω προβλήματα.

5.2 Ευαισθησίες και κίνδυνοι της ασφάλειας σε ένα δίκτυο

Αρχικά, ας αναλυθούν οι λόγοι της αυξημένης ευαισθησίας των δικτυακών υποδομών απέναντι σε μη εξουσιοδοτημένες προσπάθειες πρόσβασης που είναι οι ακόλουθοι :

- η επιθυμία πρόσβασης στα αποθηκευμένα αντικείμενα ενός κατανεμημένου συστήματος και η χρήση των παρεχομένων υπηρεσιών,
- η αυξανόμενη ποσότητα και αξία των πληροφοριών που διακινούνται μεταξύ των διασυνδεδεμένων υπολογιστικών συστημάτων (εξυπηρετητές, σταθμοί εργασίας),
- η ανάπτυξη και επέκταση ευρέων σε έκταση επικοινωνιακών υποδομών (INTERNET), που αυξάνει τη δυνατότητα πρόσβασης από μη εξουσιοδοτημένα άτομα.

Ένας εισβολέας μπορεί να περιλαμβάνεται, στο σύνολο των εξουσιοδοτημένων χρηστών (και να επιθυμεί πρόσβαση υψηλότερου του επιτρεπτού επιπέδου), αλλά είναι δυνατό να προέρχεται και εκτός του οργανισμού, που εξυπηρετείται από το σύστημα. Σκοπός μίας μη εξουσιοδοτημένης εισβολής είναι :

- η γνωστοποίηση πληροφοριών,
- η μεταβολή ή καταστροφή πληροφοριών,
- η μερική ή συνολική χρήση-καταστροφή των πόρων του συστήματος,
- η εισαγωγή προγραμμάτων καταστροφέων (ιών).

Οι πιο γνωστές εσκεμμένες απειλές που μπορούν να διαταράξουν την ασφάλεια ενός δικτύου είναι οι ακόλουθες:

1. Μη-εξουσιοδοτημένη χρήση ή προσποίηση κατά την οποία επιχειρείται προσπέλαση στα δεδομένα ή στις προαναφερόμενες υπηρεσίες του δικτύου από μη εξουσιοδοτημένους χρήστες.
2. Μη-ενεργή παρακολούθηση κατά την οποία απειλείται η εμπιστευτικότητα των ανταλλασσόμενων μηνυμάτων στο δίκτυο από μη-ενεργούς παρεμβολείς.
3. Ενεργή παρακολούθηση κατά την οποία επιχειρείται τροποποίηση ή εξαγωγή των ανταλασσομένων δεδομένων στο δίκτυο. Ο ενεργός παρεμβολέας μπορεί μεν να εντοπισθεί πιο εύκολα, αλλά μπορεί επίσης να προκαλέσει μεγαλύτερη ζημία στο δίκτυο.

4. Καταλογισμός ευθύνης, όπου ένας εξουσιοδοτημένος χρήστης μπορεί να αποποιηθεί την ευθύνη αποστολής ή παραλαβής ενός συγκεκριμένου μηνύματος ή ακόμη να κατασκευάσει ένα μη έγκυρο μήνυμα.
5. Άρνηση εξυπηρέτησης κατά την οποία το δίκτυο δεν ανταποκρίνεται στο απαιτούμενο επίπεδο εξυπηρέτησης ή και λειτουργικότητας.
6. Επανάληψη, όπου ένας εξουσιοδοτημένος χρήστης προβαίνει στην επανάληψη ενός μηνύματος με στόχο να θεωρηθεί από τον αποδέκτη του ως πρωτότυπο.
7. Ανάλυση επικοινωνίας κατά την οποία παρακολουθείται η μετάδοση των μηνυμάτων στο δίκτυο για τον εντοπισμό κυρίως της προέλευσή τους ή και της αποστολής τους.
8. Ιοί, σημαντικό πρόβλημα των υπολογιστικών συστημάτων. Δεν είναι τίποτα άλλο παρά λογισμικό που σχεδιάζεται για να προκαλέσει προβλήματα στην ομαλή λειτουργία του συστήματος. Ο τρόπος λειτουργίας τους είναι η επαναλαμβανόμενη αντιγραφή τους σε σημεία που ήδη βρίσκονται καταχωρημένα άλλα δεδομένα.

Η φύση και η αρχιτεκτονική των κατανεμημένων συστημάτων επαυξάνουν τους κινδύνους εισβολής και καθιστούν δυσκολότερη την υλοποίηση και εφαρμογή αποτρεπτικών μηχανισμών. Μερικοί από τους παράγοντες που χαρακτηρίζουν τη δυσκολία αυτή αναφέρονται στη συνέχεια.

- Τα δίκτυα και οι διασυνδεδεμένοι υπολογιστές είναι εκτεθειμένοι σε μεγάλο αριθμό χρηστών-πιθανών εισβολέων. Η γεωγραφική έκταση, που καλύπτουν τα δίκτυα, επεκτείνεται συνεχώς. Ανάλογα αυξάνει και η απόσταση, που χωρίζει το σταθμό πρόσβασης από τον εξυπηρετητή δεδομένων-επεξεργασίας, με αποτέλεσμα μεγάλος αριθμός δεδομένων να μεταφέρονται και μεγάλος αριθμός προγραμμάτων να εκτελούνται απομακρυσμένα από το σταθμό που τα ενεργοποιεί.
- Τα δίκτυα είναι δομημένα με πληθώρα φυσικών μέσων και συνδέσμων-συστατικών επικοινωνίας. Σε πολλές περιπτώσεις η φυσική πρόσβαση του εισβολέα είναι εξαιρετικά απλή, όπως η σύνδεση σε κάποιο εκτεθειμένο καλώδιο χαλκού ή σε μη προφυλαγμένο συγκεντρωτή, κατανεμητή. Η χρήση κρυπτογραφικών μεθόδων είναι, τις περισσότερες φορές μη οικονομική-αποτελεσματική, εξαιτίας του υψηλού υπολογιστικού φόρτου, που απαιτεί η διαχείριση των κλειδιών.
- Οι σημερινές επικοινωνιακές δομές διασυνδέουν ετερογενή δίκτυα και πρωτόκολλα. Η οικουμενική εφαρμογή ομογενών πρωτοκόλλων προστασίας - κρυπτογραφίας, είτε δεν είναι δυνατή λόγω της ετερογένειας των επικοινωνιακών πρωτοκόλλων, είτε όταν είναι δυνατή προκαλεί υψηλό υπολογιστικό - επικοινωνιακό φόρτο λόγω των αναγκαίων μετατροπών μηνυμάτων των ετερογενών πρωτοκόλλων.
- Η ταχύτατη επέκταση των ενοποιημένων επικοινωνιακών υπηρεσιών (ψηφιακά ολοκληρωμένα δίκτυα) σε πανεπιστημιακούς και οικιακούς χώρους, σε συνδυασμό με την χαλαρή διαχείρισή τους και τη διαρροή τεχνογνωσίας σε μη ειδικούς χρήστες έχει αυξήσει κατακόρυφα τους κινδύνους εισβολής.

5.3 Είδη επιθέσεων στο διαδίκτυο

Ας δούμε τις διάφορες τεχνικές που χρησιμοποιούν συνήθως οι «εισβολείς» με στόχο την απόκτηση πρόσβασης σε υπολογιστικά συστήματα, την παροχή δυνατότητας του πλήρους ελέγχου απομακρυσμένων συστημάτων και τέλος την πρόκληση ζημιών ή «τρώση» ενός συστήματος ανεξάρτητα των επιδόσεών αυτού.

5.3.1 Ανίχνευση δικτυακών υπηρεσιών συστημάτων (probes, scans)

Μια ανίχνευση ενός συστήματος χαρακτηρίζεται από ασυνήθιστες προσπάθειες για να αποκτήσει κάποιος πρόσβαση ή να ανακαλύψει πληροφορίες για το σύστημα αυτό. Το συνηθέστερο είναι το δεύτερο διότι αν κάποιος καταφέρει να ανακαλύψει πληροφορίες για ένα σύστημα είναι αρκετά πιθανό να καταφέρει να παραβιάσει την ασφάλειά του εκμεταλλευόμενος τις αδυναμίες που είναι ήδη γνωστές για το συγκεκριμένο σύστημα. Σαν παραδείγματα ανίχνευσης θα μπορούσαν να αναφερθούν η προσπάθεια για είσοδο στο σύστημα σε λογαριασμό χρήστη που δεν χρησιμοποιείται (όπως κάποιοι λογαριασμοί που υπάρχουν απλά για τις λειτουργίες των υπηρεσιών του συστήματος) και η σάρωση θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας Από τη στιγμή που ο επίδοξος εισβολέας μάθει ποιες υπηρεσίες προσφέρει το μηχάνημα-στόχος, μπορεί στη συνέχεια να σχεδιάσει την επίθεσή του βασιζόμενος σε γνωστές αδυναμίες των υπηρεσιών.

Επειδή μια διαδικασία port scanning αφήνει τα ίχνη της στα αρχεία καταγραφής (log files) του λειτουργικού συστήματος, ορισμένοι εισβολείς χρησιμοποιούν ορισμένες "ύπουλες" παραλλαγές. Μία από αυτές είναι η λεγόμενη "ημι-ανοιχτή σάρωση SYN" (half-open SYN scan). Κατά τη διάρκεια μιας τέτοιας σάρωσης, το πρόγραμμα συνδέεται στα port, αλλά τερματίζει καθεμία ακολουθία σύνδεσης, πριν αυτή ολοκληρωθεί. Από τη στιγμή, λοιπόν, που οι ακολουθίες σύνδεσης δεν ολοκληρώνονται, το λειτουργικό σύστημα στο μηχάνημα-στόχος συνήθως δεν τις καταγράφει, θεωρώντας ότι δεν συνέβησαν ποτέ.

Ωστόσο, το πρόγραμμα που κάνει τη σάρωση μπορεί να καταλάβει εάν κάποιο port είναι "ανοιχτό", κρίνοντας από την απάντηση του λειτουργικού συστήματος. Η διαδικασία της ανίχνευσης θα μπορούσε να παρομοιαστεί με τον έλεγχο των πορτών ενός δωματίου για να βρεθεί αν κάποια είναι ξεκλείδωτη και επιτρέπει την εύκολη πρόσβαση στους εσωτερικούς χώρους. Οι ανιχνεύσεις δικτυακών υπηρεσιών μερικές φορές ακολουθούνται από πιο σοβαρά περιστατικά έκθεσης της ασφάλειας αλλά μπορεί απλά να είναι το αποτέλεσμα απλής περιέργειας ή σύγχυσης.

Αξίζει να σημειωθεί ότι χρησιμοποιούνται και αυτοματοποιημένα εργαλεία για ανίχνευση συστημάτων που μπορούν να πραγματοποιήσουν ένα πολύ μεγαλύτερο αριθμό ανιχνεύσεων. Τέτοια εργαλεία εκτός από εισβολείς χρησιμοποιούνται και από διαχειριστές δικτύων για να μπορέσουν να διαπιστώσουν τυχόν αδυναμίες που παρουσιάζουν τα συστήματά τους.

5.3.2 Ανιχνευτές δικτυακών πακέτων (packet sniffers)

Πολλές δικτυακές εφαρμογές εκπέμπουν πακέτα που περιέχουν απλό κείμενο δηλ. η πληροφορία που στέλνεται στο δίκτυο δεν είναι κρυπτογραφημένη. Αφού τα πακέτα δεν είναι κρυπτογραφημένα μπορούν να επεξεργαστούν από οποιαδήποτε εφαρμογή που τα πιάνει από το δίκτυο.

Ένα πρωτόκολλο δικτύου περιγράφει πώς τα πακέτα ταυτοποιούνται και ποια πεδία περιέχουν, πράγμα που δίνει τη δυνατότητα στους υπολογιστές να καταλαβαίνουν ποια πακέτα προορίζονται για αυτούς. Με την ανοικτή διάδοση των προδιαγραφών των ευρέως χρησιμοποιούμενων πρωτοκόλλων όπως το TCP/IP, ο οποιοσδήποτε μπορεί να ερμηνεύσει πακέτα που πιάνει στο δίκτυο και να υλοποιήσει μια εφαρμογή ανιχνευτή δικτυακών πακέτων. Ένας ανιχνευτής πακέτων (packet sniffer) επομένως είναι μια εφαρμογή λογισμικού που μπορεί να συλλάβει όλα τα πακέτα που κυκλοφορούν στο δίκτυο. Αν τα πακέτα δεν είναι κρυπτογραφημένα μια τέτοια εφαρμογή μπορεί να δώσει χρήσιμες πληροφορίες σε εισβολείς, όπως στοιχεία και συνθηματικά λογαριασμών χρηστών, αριθμούς πιστωτικών καρτών, και διάφορα άλλα προσωπικά στοιχεία χρηστών.

Οι ανιχνευτές πακέτων μπορούν να δώσουν πληροφορίες σχετικά και με τις τοπολογίες δικτύων πράγμα που οι εισβολείς βρίσκουν ιδιαίτερα χρήσιμο. Τέτοιες πληροφορίες μπορεί να είναι ποιοι υπολογιστές παρέχουν συγκεκριμένες δικτυακές υπηρεσίες, πόσοι υπολογιστές βρίσκονται στο

τοπικό δίκτυο, ποιοι υπολογιστές έχουν πρόσβαση σε άλλους κλπ.. Όλα αυτά μπορούν να εξαχθούν από τα πακέτα που κυκλοφορούν στο δίκτυο λόγω των καθημερινών λειτουργιών.

Επιπλέον ένας ανιχνευτής δικτυακών πακέτων μπορεί να τροποποιηθεί για να εισάγει επιπλέον πληροφορία ή να τροποποιήσει ήδη υπάρχουσα στα πακέτα του δικτύου. Κάνοντας κάτι τέτοιο ένας εισβολέας μπορεί να κλείσει προώρα δικτυακές συνδέσεις ή και να αλλάξει κρίσιμες πληροφορίες που περιέχονται σε κάποιο πακέτο. Θα μπορούσαμε να φανταστούμε το μέγεθος της ζημιάς αν ένας εισβολέας τροποποιούσε πληροφορία που προοριζόταν για ένα λογιστικό σύστημα. Τα αποτελέσματα τέτοιων επιθέσεων είναι πολύ δύσκολα ανιχνεύσιμα και πολύ ακριβά στην επιδιόρθωσή τους.

5.3.3 Προσποίηση διεύθυνσης IP (IP Spoofing)

Μια επίθεση τέτοιου είδους συμβαίνει όταν κάποιος εισβολέας έξω από το δίκτυο που θέλουμε να προστατέψουμε προσποιείται ότι είναι μηχάνημα με διεύθυνση μέσα στο εύρος των διευθύνσεων που εμπιστευόμαστε (εσωτερικές του δικτύου ή κάποιες από εξωτερικές). Χρησιμοποιώντας διευθύνσεις που βρίσκονται σε εύρος που εμπιστευόμαστε ο επιτεθείς μπορεί να κερδίσει πρόσβαση σε δικτυακές υπηρεσίες που προορίζονται για έμπιστους χρήστες του δικτύου.

Ο εισβολέας αποστέλλει μηνύματα με διευθύνσεις IP που υποδεικνύουν ότι αυτά προέρχονται από ένα "έμπιστο" port. Ο επίδοξος εισβολέας αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μια διεύθυνση IP που αντιστοιχεί σε ένα τέτοιο port. Στη συνέχεια, τροποποιεί τα περιεχόμενα της κεφαλής των πακέτων που θα αποστείλει, ώστε να φαίνεται ότι προέρχονται από ένα έμπιστο port..

Ο μηχανισμός αυτός μπορεί να δώσει πρόσβαση σε κωδικούς και συνθηματικά λογαριασμών χρηστών αλλά μπορεί να χρησιμοποιηθεί και με άλλους τρόπους. Για παράδειγμα ο εισβολέας μπορεί να μιμηθεί κάποιον από τους εσωτερικούς χρήστες ενός φορέα με τρόπο που εκθέτει τον οργανισμό στον οποίο αυτός βρίσκεται (π.χ. αποστολή ενοχλητικού ηλεκτρονικού ταχυδρομείου). Τέτοιες επιθέσεις είναι πιο εύκολες όταν ο εισβολέας γνωρίζει κωδικό και συνθηματικό ενός έγκυρου χρήστη αλλά είναι δυνατές απλά και μόνο με τη γνώση των πρωτοκόλλων επικοινωνίας.

5.3.4 Άρνηση Υπηρεσίας (Denial of Service – DoS)

Μια από τις πλέον διάσημες αποτελεσματικές μεθόδους που χρησιμοποιούν οι εισβολείς για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές είναι οι επιθέσεις DoS (Denial of Service attacks). Το όνομα της τεχνικής (άρνηση εξυπηρέτησης) οφείλεται στο γεγονός ότι ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών (clients), εξαιτίας του τεράστιου πλήθους πλαστών αιτήσεων (bogus requests) που δέχεται από τον επιτεθεί.

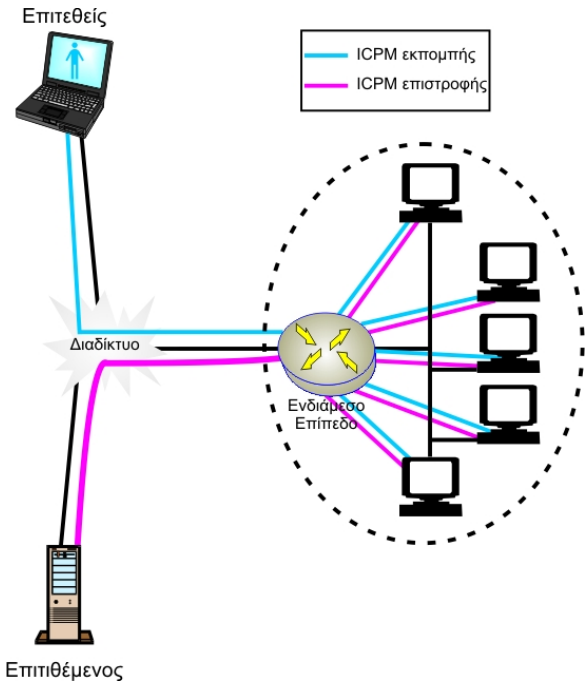
Οι επιθέσεις αυτού του τύπου είναι τελείως διαφορετικές από όλες τις άλλες τεχνικές λόγω του ότι δεν έχουν στόχο να αποκτήσουν πρόσβαση σε δικτυακούς πόρους ή πληροφορία που υπάρχει στο δίκτυο. Τέτοιου είδους επιθέσεις στοχεύουν στο να καταστήσουν μια υπηρεσία άχρηστη πράγμα που επιτυγχάνεται με την εξάντληση κάποιων περιορισμένων πόρων του δικτύου, του λειτουργικού συστήματος ή μιας εφαρμογής.

Υπάρχουν διάφορα και κατά καιρούς εφευρίσκονται νέα είδη ή παραλλαγές επιθέσεων DoS πολλά από τα οποία εκμεταλλεύονται εγγενείς αδυναμίες του ζεύγους πρωτοκόλλων TCP/IP. Οι τέσσερις από τις διασημότερες παραλλαγές είναι οι ακόλουθες:

(1) Ping of Death : Αίτηση PING ή, αλλιώς, αίτηση ICMP(Επέκταση του πρωτοκόλλου IP για την αποστολή μηνυμάτων λαθών και ελέγχου), προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) του τελευταίου (πάνω από 64Kb). Τέτοια "παράτυπα"

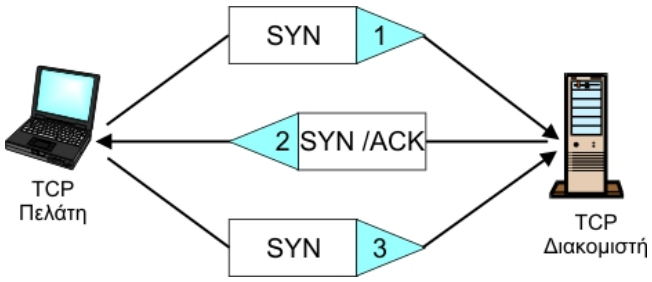
πακέτα μπορούν να "κρεμάσουν" υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.

(2) **Smurf Attack :** Επιτυγχάνεται αποστέλλοντας αιτήσεις ICMP σε μια διεύθυνση εκπομπής (broadcast address) στο υπό επίθεση δίκτυο ή σε κάποιο άλλο, ενδιάμεσο. Η διεύθυνση επιστροφής (return address) των πακέτων ICMP "πλαστογραφείται", ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου. Από τη στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου (subnet), λειτουργεί ενισχυτικά, δημιουργώντας από μία μόνο αίτηση ICMP δεκάδες ή και εκατοντάδες απαντήσεις, προκαλώντας με τον τρόπο αυτό καταιγίδα απαντήσεων. Ας σημειωθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί το πολύ σε 255 μηχανήματα (ανήκουν όλα στο ίδιο υποδίκτυο), επομένως κατά τη διάρκεια μιας επίθεσης Smurf, από κάθε αίτηση PING μπορούν να παραχθούν μέχρι και 255 απαντήσεις. Αντιλαμβάνεται κανείς, τον υπέρογκο αριθμό των άχρηστων πακέτων που δημιουργούνται, όταν ο επιτεθείς στέλνει εκατοντάδες ή ακόμη και χιλιάδες πακέτα ICMP. Στο παρακάτω σχήμα, Σχήμα 5.1, έχουμε μια τυπική αναπαράσταση της Smurf Attack**.**

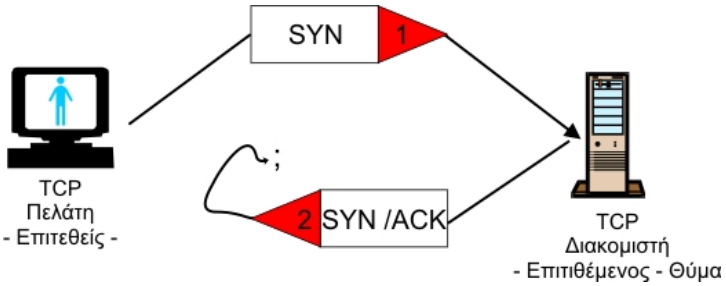


Σχήμα 5.1: Μια τυπική Smurf Attack Επίθεση

(3) **SYN Flood Attack** : Πριν εγκαθιδρυθεί μια συνεδρία (session) μεταξύ ενός πελάτη και ενός διακομιστή, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και ως "ακολουθία χειραψίας" (handshaking sequence). Εάν ο πελάτης αγνοήσει την τελευταία απάντηση SYN-ACK (SYNchronize -ACKnowledge) του διακομιστή, ο τελευταίος θα επιμένει για ένα προκαθορισμένο χρονικό διάστημα. Ένας εισβολέας μπορεί να εκμεταλλευτεί τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστή-θύμα ή ακόμα και για να τον «κρεμάσει». Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση (IP address), κρύβοντας με τον τρόπο αυτό τα ίχνη του. Στα παρακάτω σχήματα, Σχήμα 5.2.1 & 5.2.2, έχουμε μια τυπική αναπαράσταση της SYN Flood Attack**.**



Σχήμα 5.2.1: Μια τυπική SYN Flood Attack Επίθεση – Δίχως Επίθεση

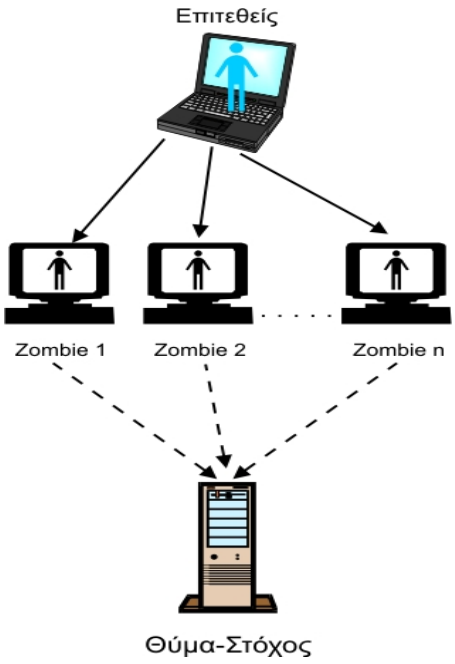


Σχήμα 5.2.2: Μια τυπική SYN Flood Attack Επίθεση – Με Επίθεση

(4) Teardrop Attack : Ο επιτεθείς εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP. Όταν ένα τέτοιο πακέτο αποστέλλεται στο Internet, ενδέχεται να ταξιδεύει σε επιμέρους, μικρότερα τμήματα (fragments). Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο (field), όπου εκεί περιγράφεται η θέση του στο αρχικό, "μεγάλο" πακέτο IP. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, ονόματι "Teardrop", το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο υπό συζήτηση πεδίο. Όταν ο υπολογιστής – στόχος προσπαθήσει να συναρμολογήσει τα "παραπλανητικά" αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει, εκτός και αν ο διαχειριστής συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch που διορθώνει το πρόβλημα.

Οταν σε μια επίθεση DoS συμμετέχουν περισσότερα του ενός μηχανήματα, που συνήθως ονομάζονται «zombies», έχουμε τις λεγόμενες κατανεμημένες επιθέσεις DoS (Distributed Denial of Service ή DDoS attacks). Στις επιθέσεις αυτού του είδους είναι δυνατόν να συμμετέχουν και προσωπικοί υπολογιστές – ακόμα και το PC στο σπίτι μας – χωρίς να το γνωρίζουν οι χρήστες τους. Στο σχήμα που ακολουθεί (Σχήμα 5.3) βλέπετε μια τυπική DDoS Επίθεση. Ο επιτεθείς εισβολέας κατορθώνει με κάποιον τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα - zombies που θα συμμετάσχουν – εν αγνοία τους – στην επίθεση.

Τη στιγμή που θα την εξαπολύσει, στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστής DDoS). Τότε, εκείνο ειδοποιεί μια συγκεκριμένη χρονική στιγμή καθέναν από τους υπόλοιπους υπολογιστές (πελάτες DDoS - zombies) και όλοι μαζί αρχίζουν να βάλλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να "πλημμυρίσει" και να μην μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών.



Σχήμα 5.3: Μια τυπική DDoS Επίθεση

5.3.5 Απρόσκλητοι Ωτακουστές - Eavesdroppers

Ένας ωτακουστής είναι ένας επιτεθείς ικανός να παρακολουθεί όλες τις πληροφορίες που είτε αποστέλλονται, είτε λαμβάνονται από ένα μέρος κάποιας επικοινωνίας, με σκοπό να ανιχνευθεί είτε ο ιδρυτής, είτε ο παραλήπτης. Οι ωτακουστές αντιμετωπίζονται δύσκολα, ακριβώς επειδή μπορούν να καταγράφουν και να συγκρίνουν όλα τα εισερχόμενα και εξερχόμενα μηνύματα.

Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά δικτύων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα «sniffer». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Εάν το δίκτυο είναι βασισμένο στο TCP/IP, τότε το sniffer που παρακολουθεί πακέτα IP, ονομάζεται και packet sniffer. Εξάλλου, σε ένα δίκτυο τοπολογίας αστέρα, όπως είναι κάποια τοπικά δίκτυα, τα πακέτα που φεύγουν από έναν κόμβο (υπολογιστή) εκπέμπονται προς όλους τους άλλους κόμβους του δικτύου. Ωστόσο, μόνο ο κόμβος για τον οποίο προορίζονται τα πακέτα θα τα χρησιμοποιήσει. Οι άλλοι θα τα αγνοήσουν. Εάν, τώρα, ένα πρόγραμμα sniffer είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου σε «αδιάκριτο» τρόπο λειτουργίας (promiscuous mode), τότε το μηχάνημα αυτό θα μπορεί να «βλέπει» όλα τα πακέτα που διακινούνται στο δίκτυο.

Οι διαχειριστές συστημάτων κάνουν χρήση των sniffer για να αναλύουν την κυκλοφορία των πακέτων σε ένα δίκτυο και να εντοπίζουν εστίες προβλημάτων. Επίσης, συχνά χρησιμοποιούν περισσότερα του ενός sniffer, τα οποία βρίσκονται στρατηγικά εγκατεστημένα σε διάφορους κόμβους του δικτύου, ώστε να εντοπίζουν εισβολές παρείσακτων. Με άλλα λόγια, τα sniffer μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών IDS (Intrusion Detection Systems).

Βλέπουμε, λοιπόν, ότι τα προγράμματα αυτά αποτελούν πολύτιμο εργαλείο για τους διαχειριστές συστημάτων. Ωστόσο, όπως έχει ήδη γίνει προφανές, τις υπηρεσίες τους μπορούν να εκμεταλλευτούν και οι εισβολείς για την υλοποίηση των παράνομων δραστηριοτήτων τους. Για παράδειγμα, ο εισβολέας μπορεί να χρησιμοποιεί ένα sniffer για να υποκλέπτει κωδικούς

πρόσβασης, αριθμούς πιστωτικών καρτών, διάφορα άλλα προσωπικά στοιχεία χρηστών, για να διαβάζει την ηλεκτρονική τους αλληλογραφία κ.λ.π.

Ο προφανής τρόπος για να προστατευτεί ένα δίκτυο από την επιβλαβή χρήση των sniffers είναι να υπάρχει αυστηρή επίβλεψη στα προγράμματα που εγκαθιστούν οι χρήστες στους υπολογιστές. Εάν ένας εισβολέας δε μπορεί να αποκτήσει φυσική πρόσβαση σε κάποιον υπολογιστή, τότε αδυνατεί να εγκαταστήσει ένα sniffer. Άλλος ένας τρόπος προστασίας είναι η αποστολή δεδομένων σε κρυπτογραφημένη μορφή. Ο sniffer θα εξακολουθεί να συλλαμβάνει τα πακέτα, μόνο που τώρα δε θα μπορεί να εξάγει κάποιο νόημα από το περιεχόμενο τους. Βεβαίως, στην περίπτωση αυτή υπάρχει πάντοτε ο κίνδυνος της αποκρυπτογράφησης. Για το λόγο αυτό, προτείνεται η χρήση ισχυρής κρυπτογραφίας, με το ανάλογο κόστος σε υπολογιστική ισχύ. Το ζητούμενο είναι η "χρυσή τομή" ανάμεσα στη δύναμη των μεθόδων κρυπτογράφησης από τη μία και στην ευκολία των χρηστών από την άλλη. Τέλος, υπάρχει μια ολόκληρη κατηγορία προγραμμάτων που μπορούν να εντοπίζουν ποιοι υπολογιστές σε ένα δίκτυο έχουν κάρτα δικτύου σε αδιάκριτο τρόπο λειτουργίας (promiscuous mode). Έτσι, ο διαχειριστής συστήματος μπορεί να ελέγξει εάν κάποιος υπολογιστής τρέχει ένα sniffer ή αν έχει δοθεί επίσημη άδεια για την εγκατάστασή του.

5.3.6 Κακοπροαίρετος Κώδικας Προγραμμάτων – Malicious Software

Τα κακοπροαίρετα προγράμματα (malicious code) είναι ένας γενικός όρος για προγράμματα που μόλις εκτελούνται προκαλούν ανεπιθύμητα αποτελέσματα σε ένα υπολογιστικό σύστημα. Οι χρήστες του συστήματος συνήθως δεν αντιλαμβάνονται την ύπαρξη ενός τέτοιου προγράμματος παρά μόνο αφού ανακαλύψουν τη ζημιά που έγινε.

Σε αυτή την κατηγορία προγραμμάτων ανήκουν οι δούρειοι ίπποι (trojan horses), οι ιοί (viruses) και τα σκουλήκια (worms). Οι δούρειοι ίπποι και οι ιοί είναι συνήθως κρυμμένοι σε νόμιμα προγράμματα ή αρχεία που οι εισβολείς έχουν παραλλάξει για να κάνουν περισσότερα πράγματα από όσα θα έπρεπε.

(1) **Worms – Σκουλήκια** : Είναι προγράμματα τα οποία διαδίδουν αυτόματα τον εαυτό τους στα άλλα συστήματα ενός δικτύου. Προχωρούν μέσα στο δίκτυο, εγκαθίστανται σε συνδεδεμένες μηχανές και στην συνέχεια, προσπαθούν από εκεί να βρουν επόμενους στόχους και τρόπο να τους προσβάλλουν. Το χαρακτηριστικό τους είναι ότι μπορούν να δρουν αυτόνομα και να έχουν ακόμα και την δυνατότητα να ξεχωρίζουν τους στόχους τους. Το πιο χαρακτηριστικό σκουλήκι είναι το Internet Worm που το βράδυ της 2ας Νοεμβρίου 1988, κατάφερε να διασπάσει το Διαδίκτυο στην Αμερική, προκαλώντας αντιδράσεις πανικού σε όλο τον κόσμο.

Πιο συγκεκριμένα, τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο Διαδίκτυο με ταχύτατο ρυθμό. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καλυμένα/παραλλαγμένα μηνύματα ηλεκτρονικού ταχυδρομείου σε όλη τη λίστα επαφών του χρήστη. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από κάποιο γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο με «οδυνηρές» συνέπειες για τον υπολογιστή του. Η μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, εκτός από την κατασπατάληση του εύρους ζώνης, επιβαρύνει δραματικά τους κεντρικούς εξυπηρέτες αλληλογραφίας του Διαδικτύου, με αποτέλεσμα να τίθενται συχνά εκτός λειτουργίας.

(2) **Trojan Horses – Δούρειοι Ίπποι** : Προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Δεν θα ήταν υπερβολή αν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών του Διαδικτύου, προέρχεται από τους "Δούρειους Ίππους".

Σε αντίθεση με τους ιούς, οι Δούρειοι ίπποι είναι αυτόνομα προγράμματα που απαιτούν την εκτέλεση τους από τον χρήστη για να ενεργοποιηθούν. Παριστάνουν ένα χρήσιμο πρόγραμμα που ο χρήστης επιθυμεί να εκτελέσει π.χ. μια ηλεκτρονική χριστουγεννιάτικη κάρτα, ένα παιχνίδι κλπ. Ενώ το πρόγραμμα φαίνεται να κάνει αυτό που θέλει ο χρήστης στην πραγματικότητα κάνει και κάτι άλλο άσχετο με τον διαφημιζόμενο σκοπό του όπως η διαγραφή του σκληρού δίσκου, η ενεργοποίηση ενός ιού που κουβαλάει μέσα του, η επιλεκτική διαγραφή αρχείων, η ανέυρεση της λίστας ονομάτων του προγράμματος αποστολής ηλεκτρονικού ταχυδρομείου του χρήστη, η ανέυρεση αριθμών πιστωτικών καρτών και η αποστολή τους στον δημιουργό του Δούρειου ίππου κ.α. Οι σύγχρονοι Δούρειοι Ίπποι μεταμφιέζονται τόσο καλά που μπορεί να παραπλανήσουν ακόμη και έναν έμπειρο χρήστη.Η αυξανόμενη δημοσιότητα και χρήση του παγκόσμιου ιστού (World Wide Web) και η αυξανόμενη απαίτηση για συμβατότητα μεταξύ διαφορετικών πλατφόρμων των διάσημων εργαλείων διαχείρισης γραφείου (π.χ. Microsoft Office) έχουν δημιουργήσει ένα περιβάλλον όπου οι μακρο-ιοί και οι Δούρειοι ίπποι μπορούν να ανθίσουν και να εξαπλωθούν πολύ εύκολα.

Συνήθως κρύβονται σε άλλα προγράμματα, αλλά μπορούν να βρίσκονται και μεμονωμένα. Πρόκειται για προγράμματα που στην σύγχρονη μορφή τους αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής "φωλιάζει" με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το Internet, το Trojan-διακομιστής, που τρέχει σιωπηρά στο περιθώριο – υπόβαθρο (background), στέλνει ένα σήμα το οποίο λαμβάνει το Trojan-πελάτης (στο μηχάνημα του θύτη). Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια σύνοδος και ο εισβολέας αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτεθείς στο άλλο μηχάνημα ποικίλλει, αναλόγως του Trojan. Ο πρώτος μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού CD-ROM ή εμφανίζοντας μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία. Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Ετσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη.

Πώς όμως μπορεί να «εισαχθεί» ένας «Δούρειος Ίππος» στον υπολογιστή; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι με ευρεία διάδοση, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λ.π. Υπάρχουν δύο τρόποι για την αποφυγή τους. Ο πρώτος είναι η χρησιμοποίηση προγραμμάτων γνωστά ως «Antivirus» και «AntiTrojan». Πολλά προγράμματα της κατηγορίας αυτής μπορούν να ανιχνεύουν ιούς και να διαγράφουν μολυσμένα αρχεία. Ο άλλος τρόπος είναι η χρησιμοποίηση ενός «φράγματος ασφάλειας» (firewall), είτε σε μορφή λογισμικού είτε υλισμικού. Κάθε φορά που ένας «Εξυπηρέτης Δούρειος Ίππος» θα προσπαθεί να «βγει» στο Διαδίκτυο, το φράγμα ασφάλειας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία.

(3) **Viruses – Ιοί** : Τα γνωστά προγράμματα που προσπαθούν (με πονηρές και συνήθως δόλιες τεχνικές) να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα

του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους, αφήνοντας μία υπογραφή-ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης - configuration του συστήματος).

Ένας πραγματικός ιός στην κλασσική του έννοια είναι ένα κομμάτι κώδικα που προσαρτάται σε κάποιο άλλο εκτελέσιμο κώδικα, έτσι ώστε όταν εκτελείται το "μολυσμένο" πρόγραμμα να εκτελείται και ο ιός μαζί του.

Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Διαδίκτυο. Αφού εκτελεστεί ο ιός μεταφέρεται στην κύρια μνήμη του ηλεκτρονικού υπολογιστή και μπορεί να έχει τον πλήρη έλεγχο του συστήματος. Συνήθως το πρώτο μέλημα του είναι να προσαρτήσει αντίγραφα του εαυτού του σε άλλα εκτελέσιμα προγράμματα με γεωμετρικό ρυθμό και με αυτόν τον τρόπο να εξαπλωθεί.

Οι ιοί δεν είναι αυτόνομα προγράμματα – δεν μπορούν να εκτελεστούν από μόνοι τους και απαιτούν για την ενεργοποίηση τους, την εκτέλεση κάποιου πρόγραμματος "ξενιστή" που περιέχει τον ιό μέσα στον κώδικα του.

Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι από μηδαμινές έως και καταστροφικές.

Υπάρχουν αρκετά είδη ιών, όπως:

α) Αυτοί που προσβάλλουν τον τομέα εκκίνησης μιας αποθηκευτικής μονάδας (boot sector viruses).

β) Αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/File viruses).

γ) Αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών (Macro viruses).

δ) Οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή και σε όλες τις προαναφερόμενες κατηγορίες.

Η κύρια διαφορά τους από τα σκουλήκια είναι ότι για να διαδοθούν χρειάζεται να γίνει κάποια ενέργεια από την πλευρά του χρήστη, η οποία γίνεται χωρίς ο χρήστης να το καταλάβει (π.χ. εκτέλεση αρχείων με παραπλανητική κατάληξη ενώ πρόκειται στην ουσία για εκτελέσιμα προγράμματα).

(4) **Back Doors – Πίσω Πόρτες** : Δεν αποτελεί κακόβουλο λογισμικό αυτό καθ'αυτό όμως είναι μια τροποποίηση νόμιμου λογισμικού με συχνά κακόβουλο σκοπό. Μερικές φορές ονομάζονται και trap doors ανάλογα με το ποιος τις δημιουργεί και επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε κάποιο σύστημα. Επίσης μπορούν να χρησιμοποιηθούν και από ειδικούς ασφαλείας σαν «δόλωμα – bait» για τον εντοπισμό και παγίδευση ιδιαίτερα ταλαντούχων εισβολέων.
Ορισμένες φορές οι σχεδιαστές λειτουργικών συστημάτων δημιουργούν σκόπιμα «πίσω πόρτες» που τους δίνουν την δυνατότητα να κάνουν αλλαγές σε οτιδήποτε θέλουν. Φυσικά, για τα στελέχη του τμήματος μηχανογράφησης ενός μεγάλου οργανισμού, αυτό το υψηλό επίπεδο ελέγχου είναι συχνά απαραίτητο.

(5) **Logic Bombs – Λογικές Βόμβες** : είναι κρυφά χαρακτηριστικά μέσα σε προγράμματα τα οποία μπορεί να παραμείνουν ανενεργά για πάρα πολύ καιρό μέχρι να ενεργοποιηθούν όταν συντρέξουν οι κατάλληλες συνθήκες. Πολλές φορές οι λογικές βόμβες ενσωματώνονται σε διάσημα εμπορικά προγράμματα από τους προγραμματιστές για τον έλεγχο της πειρατείας λογισμικού.

Υποκατηγορία αυτών των προγραμμάτων είναι η Time Bomb – Ωρολογιακή Βόμβα που χρησιμοποιεί το ρολόι του συστήματος και είναι ιδιαίτερα χρήσιμη όταν ο ένοχος δεν θέλει να είναι παρών όταν διαπράττεται το αδίκημα

(6) **Zombies, or Rabbit Programs - Ζόμπι ή Προγράμματα Λαγοί :** είναι προγράμματα που "κλωνοποιούν" τον εαυτό τους ατέρμονα, με στόχο να κατακλύσουν τους πόρους του "μολυσμένου" υπολογιστικού συστήματος με σκοπό την κατάρρευση του. Άλλα προγράμματα που εντάσσονται σε αυτήν την κατηγορία, επιτίθενται και κατακλύζουν τους εξυπηρετητές (servers) των διαφόρων τοποθεσιών του Web με χιλιάδες αιτήσης σύνδεσης, επιβραδύνοντας την λειτουργία αυτών με αποτέλεσμα την αδυναμία εξυπηρέτησης (denial-of-service).

5.3.7 Επιθέσεις για εύρεση συνθηματικών

Επιθέσεις για εύρεση συνθηματικών μπορούν να υλοποιηθούν με πολλές διαφορετικές μεθόδους συμπεριλαμβανομένων των απευθείας επιθέσεων (brute–force), προγραμμάτων δούρειων ίππων (trojan horse), IP spoofing και ελεγκτών πακέτων. Αν και οι τεχνικές προσποίησης IP διεύθυνσης (IP spoofing) και ελεγκτών πακέτων που αναλύονται ξεχωριστά μπορούν να δώσουν λογαριασμούς και συνθηματικά χρηστών, οι επιθέσεις για εύρεση συνθηματικών αναφέρονται συνήθως σε συνεχείς επανειλημμένες προσπάθειες για τον προσδιορισμό ενός λογαριασμού χρήστη και του συνθηματικού του. Τέτοιες επιθέσεις καλούνται "απευθείας" (brute force).

Συχνά μια απευθείας επίθεση διενεργείται με τη χρήση ενός προγράμματος που τρέχει πάνω στο δίκτυο και προσπαθεί να συνδεθεί σε ένα διαμοιραζόμενο πόρο όπως ένας εξυπηρετητής. Όταν ο εισβολέας κατορθώσει να αποκτήσει πρόσβαση, έχει τα ίδια δικαιώματα με τον χρήστη του οποίου ο λογαριασμός παραβιάστηκε για να αποκτηθεί η πρόσβαση στον πόρο. Αν ο λογαριασμός έχει επαρκή δικαιώματα, ο εισβολέας μπορεί να δημιουργήσει μια "πίσω πόρτα" για μελλοντική πρόσβαση χωρίς να ανησυχεί για αλλαγές στην κατάσταση ή το συνθηματικό του λογαριασμού που παραβίασε.

5.3.8 Επιθέσεις σε επίπεδο εφαρμογής

Οι επιθέσεις σε επίπεδο εφαρμογής μπορούν να γίνουν με πολλούς τρόπους ανάλογα με το πρωτόκολλο. Μια από τις πιο κοινές μεθόδους είναι η εκμετάλλευση αδυναμιών που ανακαλύπτονται σε εξυπηρετητές γνωστών δικτυακών υπηρεσιών όπως ηλεκτρονικού ταχυδρομείου (sendmail), μεταφοράς αρχείων (ftp), HTTP, NIS, NFS κλπ. Οπως έχει αναφερθεί και προηγούμενα, τέτοιες αδυναμίες μπορεί να υπάρχουν είτε από τη σχεδίαση των πρωτοκόλλων η οποία δεν είχε λάβει υπόψη της την ασφάλεια, είτε από την υλοποίησή τους. Κατά καιρούς αναφέρονται επιτυχείς επιθέσεις σε διάφορους εξυπηρετητές και αν αυτές εκμεταλλεύονται υλοποιήσεις βγαίνουν από τους κατασκευαστές νέες σταθερότερες εκδόσεις που επιλύουν τις συγκεκριμένες αδυναμίες που ανακαλύφθηκαν. Σαν ένα καλό παράδειγμα επίθεσης σε επίπεδο εφαρμογής θα μπορούσαν να αναφερθούν οι μαζικές αποστολές (πολλές χιλιάδες) μηνυμάτων ηλεκτρονικού ταχυδρομείου σε έναν συγκεκριμένο εξυπηρετητή (mail bombs). Τέτοιες επιθέσεις μπορεί να αντιμετωπίζονται απλά και μόνο με σωστότερη ρύθμιση των παραμέτρων των εξυπηρετητών. Ιδιαίτερη αναφορά πρέπει να γίνει στην υπηρεσία του παγκόσμιου ιστού WWW (World Wide Web) λόγω της τεράστιας διάδοσής της.

Η υπηρεσία του παγκόσμιου ιστού (WWW) βασίζεται σε ένα πρωτόκολλο επιπέδου εφαρμογής, το HTTP. Η υπηρεσία αυτή είναι η πλέον διαδεδομένη στο Διαδίκτυο σε σημείο μάλιστα που αρκετοί χρήστες έχουν ταυτίσει το Διαδίκτυο με αυτή. Οι επιθέσεις που γίνονται εδώ

εκμεταλλεύονται την ανοικτή φύση αρκετών νέων τεχνολογιών που αναπτύσσονται παράλληλα με την ανάπτυξη της υπηρεσίας: την γλώσσα προδιαγραφής υπερκειμένων HTML (Hypertext Markup Language), τη λειτουργία των προγραμμάτων πλοηγών Διαδικτύου (web browsers) αλλά και του ίδιου του HTTP.

Καθώς ο παγκόσμιος ιστός αναπτυσσόταν διαρκώς παρουσιάστηκαν ανάγκες για δημιουργία εφαρμογών που παράγουν δυναμικό περιεχόμενο και όχι μόνο απλές στατικές HTML σελίδες. Οι εφαρμογές αυτές μπορούν να εκτελούνται τόσο στην πλευρά του εξυπηρετητή όσο και στην πλευρά του πελάτη. Επιθέσεις μπορούν να συμβούν και στις δυο περιπτώσεις. Έτσι:

Στην πλευρά του εξυπηρετητή έχουμε εκτελέσιμα προγράμματα (cgi, servlets κλπ) που δημιουργούν το δυναμικό περιεχόμενο κάνοντας πρόσβαση σε ένα σωρό κρίσιμους πόρους όπως βάσεις δεδομένων. Αν αυτά τα προγράμματα δεν είναι προσεκτικά γραμμένα και δεν κάνουν απαραίτητους ελέγχους είναι δυνατόν να τα εκμεταλλευτεί ένας εισβολέας εκτελώντας τα με τρόπο διαφορετικό από αυτόν που είναι σχεδιασμένα (π.χ. κλήση τους με κακόβουλες παραμέτρους που δεν είχαν προβλεφθεί).

Στην πλευρά του πελάτη έχουν δημιουργηθεί τεχνολογίες που επιτρέπουν την εκτέλεση προγραμμάτων στον πλοηγό Διαδικτύου. Σαν τέτοιες τεχνολογίες θα μπορούσαν να αναφερθούν η JAVA, η JAVASCRIPT, τα ActiveX της Microsoft κλπ.

Τέτοια προγράμματα φορτώνονται και εκτελούνται τοπικά στο σύστημα του χρήστη ανάλογα με ετικέτες που υπάρχουν στις HTML σελίδες (<APPLET>, <OBJECT>, <SCRIPT>). Βέβαια οι γλώσσες αυτές παρέχουν μηχανισμούς ασφάλειας μέσα στη σχεδίασή τους αλλά έχουν αναφερθεί περιπτώσεις που οι μηχανισμοί αυτοί έχουν παρακαμφθεί δημιουργώντας προγράμματα που δρουν σαν δούρειοι ίπποι. Μάλιστα οι επιθέσεις αυτές προκαλούν ζημιές σε πληθώρα από συστήματα λόγω του γεγονότος ότι οι περισσότερες γλώσσες που χρησιμοποιούνται για την κατασκευή τέτοιων προγραμμάτων είναι ανεξάρτητες πλατφόρμας.

5.3.9 Οι κίνδυνοι του IRC

Το IRC (Internet Relay Chat) είναι μία από τις πιο ευρέως χρησιμοποιούμενες υπηρεσίες του Internet ανά την υφήλιο. Η δημοτικότητα αυτού του συστήματος επικοινωνίας έχει ξεπεράσει κάθε προσδοκία, και χρησιμοποιείται πλέον από εκατομμύρια χρήστες καθημερινά. Υπάρχουν χιλιάδες κανάλια συνομιλίας (chat channels) του IRC σε όλο τον κόσμο, τα οποία ειδικεύονται σε ξεχωριστούς τομείς: χόμπι, επαγγέλματα, ή ακόμη και διάφορα αμφιλεγόμενα θέματα. Δυστυχώς, όπως και οτιδήποτε άλλο, το IRC έχει και ορισμένα μειονεκτήματα. Κάποιος χρήστης, κάποτε, θεώρησε ότι το να ενοχλεί τους άλλους χρήστες είναι διασκεδαστικό. Από τότε υπήρξαν πολλοί άλλοι οι οποίοι ακολούθησαν τα βήματά του. Κατ' αυτό τον τρόπο προέκυψαν οι κίνδυνοι του IRC, οι οποίοι ουσιαστικά οφείλονται στον τρόπο λειτουργίας αυτής της υπηρεσίας. Όταν οι χρήστες τρέχουν ένα client πρόγραμμα IRC, στην πραγματικότητα ζητούν άδεια για να εισέλθουν σ' έναν IRC server, ο οποίος και περιέχει τους μηχανισμούς του συστήματος. Αυτός ο server πιστοποιεί την ταυτότητα των χρηστών, εμποδίζει δύο χρήστες να επιλέξουν την ίδια εικονική ταυτότητα (το ψευδώνυμο που χρησιμοποιεί κάθε χρήστης για να συνδεθεί σ' ένα κανάλι συνομιλίας), ελέγχει τον αριθμό των χρηστών, κ.α.

Επί του παρόντος, σε συγκεκριμένες συνθήκες ο server μπορεί να εκδιώξει έναν χρήστη από ένα κανάλι. Αυτό μπορεί να συμβεί όταν ένα client πρόγραμμα IRC στέλνει πολλές πληροφορίες στον server σε πολύ σύντομο χρονικό διάστημα, και για να αποφύγει τον κορεσμό του συστήματος ο server κλείνει αυτή την συγκεκριμένη σύνδεση. Το φαινόμενο αυτό αποτελεί την βάση των επιθέσεων που γίνονται μέσω του IRC. Ακολουθεί μία περιγραφή των πιο κοινών μορφών επίθεσης:

- **Nuke – Επίθεση «με Πυρηνικά»** : Μία τέτοια επίθεση εξαλείφει αμέσως έναν χρήστη από ένα κανάλι IRC. Αυτή η επίθεση εκτελείται στέλνοντας πλασματικά πακέτα δεδομένων στην διεύθυνση IP του χρήστη• ο υπολογιστής του χρήστη απαντά στέλνοντας ένα μεγάλο όγκο πληροφοριών στον IRC server και, σαν αποτέλεσμα, το IRC εκδιώκει τον χρήστη από το κανάλι. Υπάρχουν διάφορες μορφές επίθεσης nuke, αν και η πιο γνωστή είναι η αποκαλούμενη ICMP - μία επίθεση 'άρνησης εξυπηρέτησης (Denial of Service, DoS). Αυτή είναι η συνηθέστερη μορφή επιθέσεων μέσω IRC, καθώς υπάρχουν πολλά εργαλεία διαθέσιμα στο Internet για την εκκίνηση τέτοιων επιθέσεων.

- **Flood – «Πλημμύρα»** : Αυτό το είδος επιθέσεων είναι παρόμοιο με τις επιθέσεις nuke, αλλά επειδή είναι λιγότερο αποτελεσματικό δεν χρησιμοποιείται τόσο συχνά. Μία επίθεση flood εκτελείται στέλνοντας μεγάλες ποσότητες δεδομένων στον υπολογιστή-θύμα, έτσι ώστε όταν αυτός απαντήσει, να υπερβεί τον όγκο των δεδομένων που επιτρέπει ο server.

Ολοένα και περισσότεροι ιοί χρησιμοποιούν επίσης το IRC για να παρέχουν πρόσβαση σε υπολογιστές σε διάφορους εισβολείς. Αντιπροσωπευτικό παράδειγμα είναι ένα είδος Δούρειου Ίππου ο οποίος, όταν εγκαθίσταται σ' έναν υπολογιστή, συνδέεται σε συγκεκριμένα κανάλια IRC και περιμένει να λάβει εντολές από τον δημιουργό του.

5.3.10 Άλλοι τύποι απειλών

Κάποιοι άλλοι τύποι απειλών για την ασφάλεια, την ιδιωτικότητα και την ανωνυμία περιλαμβάνουν:

1) Επιθέσεις Αντίστροφης Πορείας,
2) Επιθέσεις από Εχθρικούς Συνεργάτες,
3) Επιθέσεις Κωδικοποίησης Μηνυμάτων,
4) Επιθέσεις Χρονοσήμανσης,
5) Επιθέσεις Υπερφόρτωσης Μηνυμάτων,
6) Επιθέσεις Περιόδων Σύνδεσης,
7) Επιθέσεις από Αξιοποίηση Cookies,
8) Επιθέσεις σε Υπηρεσίες Προσωποποίησης.

1) Επίθεση Αντίστροφης Πορείας – Trace Back Attack

Σε μία επίθεση αντίστροφης πορείας, ένας επιτεθείς ξεκινά από ένα γνωστό ανταποκριτή και ιχνηλατεί το μονοπάτι προς τον ιδρυτή είτε κατά το μονοπάτι προώθησης είτε κατά το αντίστροφο μονοπάτι. Αυτά τα δύο είδη αποτελούν τους δύο τύπους επιθέσεων αντίστροφης πορείας.

Σε μία ενεργή (active) επίθεση αντίστροφης πορείας, ο επιτεθείς διατηρεί τον έλεγχο της δικτυακής δομής και είναι ικανός να ακολουθήσει μία ενεργή και συνεχιζόμενη ροή πακέτων που διαπερνά το δίκτυο προς το σημείο προέλευσης τους.

Σε μία παθητική (passive) επίθεση αντίστροφης πορείας, ο επιτεθείς είναι με κάποιο τρόπο σε θέση να εξετάσει την κατάσταση δρομολόγησης των συμμετεχόντων μελών ενός πρωτοκόλλου και να ιχνηλατήσει αντίστροφα τη σύνδεση προς μία αποθηκευμένη πορεία.

2) Επίθεση από Εχθρικούς Συνεργάτες – Malicious Collaborators

Είναι δύσκολο να αποδειχθεί ένα σύστημα ασφαλές όταν αντιμετωπίζει ομάδα από συνεργαζόμενα μέλη. Αυτά τα μέλη είναι «εχθρικοί συμμετέχοντες» σε πρωτόκολλα που επικοινωνούν μεταξύ τους για να ανακαλύψουν την ταυτότητα κάποιου ιδρυτή. Στην ακραία περίπτωση, όταν όλοι πλην ενός αποτελούν εχθρικό συνεργάτη, οποιοδήποτε πακέτο που θα αποσταλεί προς τον έντιμο συμμετέχοντα διαμέσου ενός από τα περιγραφέντα συστήματα θα είναι αναγνώσιμο.

3) Επίθεση Κωδικοποίησης Μηνυμάτων – Message Coding Attack

Ένας επιτεθείς είναι σε θέση να πραγματοποιήσει μία επικοινωνία με ένα συγκεκριμένο εξυπηρετούμενο και έναν εξυπηρέτη. Επιπλέον μπορούν να ιχνηλατηθούν μηνύματα, εάν δεν τροποποιούν την κωδικοποίηση τους κατά τη διάρκεια της μετάδοσης. Παράλληλα, η αποτροπή επιθέσεων που βασίζονται στην ακριβή καταγραφή του όγκου των μηνυμάτων είναι αρκετά δύσκολη.

4) Επίθεση Χρονοσήμανσης – Timing Attack

Η απειλή των επιθέσεων χρονοσήμανσης περιγράφει την ανάλυση των πακέτων που μεταδίδονται και ανιχνεύει την πηγή τους εξαιτίας των συσχετισμένων χρόνων. Η αντιμετώπιση αυτής της απειλής είναι εξαιρετικά δύσκολη, διότι οποιοδήποτε σύστημα εκτός μιας ασφαλούς ομάδας υπολογιστών είναι ευπρόσβλητο σε επιθέσεις χρονοσήμανσης. Ως αποτέλεσμα, η πλειοψηφία των εργαλείων, υπηρεσιών και πρωτοκόλλων ανωνυμίας δεν μπορεί να προστατεύσει την ανωνυμία των χρηστών από αυτήν την επίθεση.

5) Επίθεση Υπερφόρτωσης Μηνυμάτων – Flooding Attack

Στην περίπτωση που κάποιος δρομολογητής υποστηρίζει n χρήστες, ένας επιτεθείς μπορεί να αποστείλει n-1 πακέτα και να ιχνηλατήσει το πρωταρχικό πακέτο προς την πηγή του. Ωστόσο, αυτή η επίθεση μπορεί να αποφευχθεί ζητώντας την αυθεντικοποίηση κάθε αποστολέα. Σημειώνεται ότι η αναγκαιότητα αυθεντικοποίησης δεν ταυτίζεται με την ανάγκη της ιδιωτικότητας και της ανωνυμίας. Πράγματι, μόνον οι δρομολογητές που ζητούν αυθεντικοποίηση, για παράδειγμα μέσω SSL, μπορούν να αντιμετωπίσουν τις επιθέσεις υπερφόρτωσης μηνυμάτων.

Η πλειοψηφία των εργαλείων, πρωτοκόλλων και υπηρεσιών ανωνυμίας στηρίζουν τη λειτουργία τους στην αμοιβαία εμπιστοσύνη μεταξύ των συμμετεχόντων τους.

6) Επίθεση Περιόδων Σύνδεσης – Connection Period Attacks

Ο τύπος αυτής της επίθεσης αναφέρεται στην απώλεια της ιδιωτικότητας μιας ομάδας και του επιπέδου ανωνυμίας της, με βάση το γεγονός ότι οι περισσότεροι χρήστες εγκαθιστούν έναν περιορισμένο αριθμό συνδέσεων και έχουν ένα συνήθη τύπο συμπεριφοράς στον ιστό. Ως αποτέλεσμα, ένας επιτεθείς μπορεί να αναλύσει κάποιες επαναλαμβανόμενες δραστηριότητες και να αποκτήσει ιδιωτικές πληροφορίες. Παρόλο που αυτό το είδος επίθεσης δεν αποκαλύπτει απαραιτήτως την ταυτότητα του χρήστη, μπορεί να μειώσει δραματικά το μέγεθος των ανώνυμων χρηστών μιας ομάδας.

7) Επίθεση από Αξιοποίηση cookies

Όπως είναι γνωστό, τα cookies αποτελούν αρχεία δεδομένων που τοποθετούνται στο σύστημα ενός χρήστη με σκοπό να παρέχουν προσωπικές πληροφορίες σε εξυπηρέτες, τους οποίους επισκέπτονται οι χρήστες. Η δομή των cookies μπορεί να απειλήσει την ιδιωτικότητα και ανωνυμία των χρηστών, επειδή τα προσωπικά δεδομένα ενδέχεται να γίνουν αντικείμενο επεξεργασίας από ποικίλες οντότητες του ιστού.

8) Επίθεση σε Υπηρεσίες Προσωποποίησης

Οι υπηρεσίες προσωποποίησης προσφέρονται κατά τη διαδικασία προσέλκυσης νέων χρηστών σε ένα περιβάλλον. Υπάρχει πάντοτε η απειλή αποκάλυψης προσωπικών πληροφοριών κατά τη διάρκεια της διαδικασίας εγγραφής. Η αυξανόμενη χρήση αυτών των υπηρεσιών οδηγεί στην ανάγκη αντιμετώπισης των σχετιζόμενων απειλών από εργαλεία, εφαρμογές και υπηρεσίες ανωνυμίας.

Επίλογος

Αδυναμίες των μέτρων προστασίας

Δυστυχώς, όσα μέτρα προστασίας και αν ληφθούν, πάντοτε τα χρησιμοποιούμενα προγράμματα θα είναι ατελή υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι αποφασισμένοι crackers. Πρόκειται για τα λεγόμενα «exploits», δηλαδή προγραμματιστικές αδυναμίες σε γνωστές και ευρέως χρησιμοποιούμενες εφαρμογές, τις οποίες μπορούν να αξιοποιούν οι εισβολείς για να αποκτούν μη εξουσιοδοτημένη πρόσβαση ή έλεγχο σε συστήματα ή απλά να προκαλούν ζημιές σε υπολογιστές-στόχους. Οι εταιρείες υπολογιστών προσπαθούν να αντιμετωπίσουν τα προβλήματα ασφάλειας παρέχοντας στους χρήστες αναβαθμίσεις ή διορθώσεις.

Συχνά, πάντως, οι εταιρείες κυκλοφορούν αναβαθμίσεις ή διορθώσεις (bug fixes, patches) προγραμμάτων με γνωστά προβλήματα. Σε κάθε περίπτωση, οι αναβαθμίσεις σίγουρα λύνουν κάποια προβλήματα, ωστόσο, αυτό δεν σημαίνει κατ' ανάγκη ότι αυξάνουν συνολικά την ασφάλεια του συστήματος μας. Είναι πιθανό ένα patch να κλείνει ορισμένα κενά ασφάλειας, αλλά ταυτόχρονα να δημιουργεί κάποια άλλα.

Γλωσσάρι – Βασικές Έννοιες

1. Βασικές έννοιες και όροι ασφάλειας στο επίπεδο του χρήστη

1.1 Ευρεία εκπομπή – Broadcasting : Μέθοδος αποστολής του ίδιου μηνύματος σε όλους τους υπολογιστές ενός υποδικτύου, ταυτόχρονα. Παρόμοια έννοια είναι το multicasting (πολλαπλή εκπομπή), μόνο που τώρα οι παραλήπτες του μηνύματος είναι προεπιλεγμένοι όχι κατ' ανάγκη όλοι οι υπολογιστές.

1.2 Φράγμα Ασφάλειας – Firewall : Μέθοδος προστασίας που υλοποιείται σε επίπεδο υλικού ή / και λογισμικού και χρησιμοποιείται για να αποτρέπει εξουσιοδοτημένη πρόσβαση από και προς ένα δίκτυο. Συχνά τα φράγματα ασφάλειας χρησιμοποιούνται για να εμποδίζουν χρήστες του Διαδικτύου να προσπελάζουν ιδιωτικά δίκτυα, τα οποία είναι και αυτά συνδεδεμένα με το Διαδίκτυο. Γενικά, μπορούμε να πούμε ότι ένα φράγμα ασφάλειας διαχωρίζει ένα δίκτυο από κάποιο άλλο.

1.3 Hub : Κοινό σημείο σύνδεσης για ένα πλήθος υπολογιστών σε ένα τοπικό δίκτυο (τοπολογία αστέρα). Ένα hub έχει πολλές θύρες (ports). Όταν ένα πακέτο φτάνει σε μία θύρα, αντιγράφεται σε όλες τις άλλες, με αποτέλεσμα όλοι οι υπολογιστές που είναι συνδεδεμένοι με το hub να "βλέπουν" όλα τα διακινούμενα πακέτα. Σε αντιδιαστολή βρίσκονται τα διασκεπτικά στοιχεία τοπικών υπολογιστών ή πλαισίων: κάθε φορά που ένα πακέτο φτάνει σε μία θύρα, διαβάζεται η διεύθυνση προορισμού στην κεφαλή του και το πακέτο προωθείται μόνο στη θύρα στην οποία αντιστοιχεί ο υπολογιστής με τη συγκεκριμένη διεύθυνση.

1.4 ICMP (Internet Control Message Protocol) : Επέκταση του πρωτοκόλλου IP για την αποστολή μηνυμάτων λαθών και ελέγχου. Χρησιμοποιείται από την εντολή Ping για να διαπιστώνεται, μεταξύ των άλλων, εάν ένα μηχάνημα είναι ενεργό, από δρομολογητές (routers), κάθε φορά που ειδοποιούν ένα μηχάνημα για τη μη διαθεσιμότητα ενός κόμβου στον οποίο απευθύνονται κτλ.

1.5 IP Spoofing : Τεχνική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε δικτυωμένα μηχανήματα. Ο εισβολέας αποστέλλει μηνύματα με διευθύνσεις IP που υποδεικνύουν ότι αυτά προέρχονται από ένα "έμπιστο" port. Ο επίδοξος cracker αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μια διεύθυνση IP που αντιστοιχεί σε μια τέτοια θύρα. Στη συνέχεια, τροποποιεί τα περιεχόμενα της κεφαλής των πακέτων που θα αποστείλει, ώστε να φαίνεται ότι προέρχονται από μια έμπιστη θύρα. Η κατάλληλη ρύθμιση δρομολογητών και φραγμάτων ασφάλειας μπορεί να αποτρέψει τις επιθέσεις του είδους.

1.6 PING (Packet InterNet Groper) : Εργαλείο για να διαπιστώνεται εάν μια δεδομένη διεύθυνση IP είναι προσβάσιμη. Το πρόγραμμα στέλνει ένα πακέτο σε μια διεύθυνση και στη συνέχεια αναμένει μια απάντηση από τον υπολογιστή στον οποίο αντιστοιχεί αυτή η διεύθυνση

1.7 Port Number – Αριθμός Θύρας : Αριθμός που αντιστοιχεί σε μια εφαρμογή στο ρόλο διακομιστή, σε ένα δίκτυο βασισμένο στο TCP/IP (όπως, π.χ., το Διαδίκτυο). Η θύρα μπορεί να θεωρηθεί ως το άκρο μιας λογικής σύνδεσης (δηλαδή μιας σύνδεσης όπως τη βλέπει ο χρήστης). Ένας αριθμός θύρας χρησιμοποιείται ώστε εισερχόμενα δεδομένα να αντιστοιχίζονται στην κατάλληλη υπηρεσία (service). Γνωστά παραδείγματα αποτελούν τα port 80, 25 και 20, που χρησιμοποιούνται από διακομιστές ιστοσελίδων, αλληλογραφίας και FTP, αντίστοιχα www.isi.edu/in-

notes/iana/assignments/port-numbers. Ο συνδυασμός μιας διεύθυνσης IP ενός μηχανήματος με έναν αριθμό port ονομάζεται Socket.

1.8 Promiscuous Mode – Αδιάκριτος Τρόπος Λειτουργίας : Δικτυωμένος υπολογιστής ρυθμισμένος ώστε να αναγνωρίζει και να δέχεται όλα τα πακέτα που φτάνουν ή περνούν από αυτόν, ανεξαρτήτως πρωτοκόλλου ή προορισμού. Κάθε εργαλείο λογισμικού που χρησιμοποιείται για το φιλτράρισμα δικτυακών πακέτων πρέπει να είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου και οδηγούς που του επιτρέπουν να βρίσκεται σε αδιάκριτο τρόπο λειτουργίας.

1.9 Subnet – Υποδίκτυο : Υποσύνολο ενός δικτύου που περιλαμβάνει υπολογιστές οι οποίοι έχουν διευθύνσεις με ένα κοινό τμήμα. Στα δίκτυα TCP/IP, οι υπολογιστές ενός υποδικτύου έχουν διευθύνσεις IP με κοινό πρόθεμα. Η υποδιαίρεση ενός δικτύου σε υποδίκτυα είναι χρήσιμη τόσο για λόγους ευκολίας διαχείρισης όσο και για λόγους ασφαλείας.

1.10 CRL (Certificate Revocation Lists – Λίστες Ανάκλησης Πιστοποιητικών, κεφ3 σελ12) : Είναι η μια από τις δύο συνηθισμένες μεθόδους που χρησιμοποιούνται για την διατήρηση πρόσβασης στους εξυπηρέτες ενός δικτύου στην περίπτωση μιας PKI. Η άλλη μέθοδος είναι η Online Certificate Status Protocol (OCSP). Η CRL είναι μια λίστα πιστοποιητικών που έχουν ανακληθεί πριν από τη προβλεπόμενη ημερομηνία λήξης τους. Το κυριότερο αρνητικό χαρακτηριστικό της είναι ότι πρέπει να «κατεβαίνουν» ενημερώσεις (updates) τακτικά έτσι ώστε να διατηρούνται οι λίστες έγκυρες. Σε αντίθεση, η OCSP, ξεπερνά αυτόν τον περιορισμό με το να ελέγχει την κατάσταση του πιστοποιητικού σε πραγματικό χρόνο.

1. Συγγραφείς-Προγραμματιστές Κακόβουλου Κώδικα – Malicious Code Authors

Δεν είναι γνωστά πολλά πράγματα για τους ανθρώπους που γράφουν και εγκαθιστούν προγραμματιζόμενες απειλές κυρίως γιατί ένα πολύ μικρό ποσοστό από τα σχετικά συμβάντα γίνονται γνωστά στην ευρύτερη κοινότητα. Παλιότερες μελέτες έδειξαν υψηλό ποσοστό προγραμματιστών ως εγκληματιών σε αντίθεση με σήμερα. Προφανώς η διάδοση των ηλεκτρονικών υπολογιστών δημιούργησε την δυνατότητα διάπραξης τέτοιων εγκλημάτων από το ευρύ κοινό. Βασιζόμενοι στους συγγραφείς που είναι γνωστοί στις αρχές και στα γεγονότα που τελικά αναδύθηκαν στην επιφάνεια, αυτοί μπορούν να χωριστούν στις ακόλουθες βασικές κατηγορίες:

2.1 Εργαζόμενοι :

Τα τρία συστατικά κάθε απάτης είναι η ανάγκη, η ευκαιρία και η γνώση. Με την πρόσληψη ενός υπαλλήλου, δύο από τα τρία στοιχεία, και συγκεκριμένα η ευκαιρία και η γνώση, υπάρχουν ήδη λόγω της φύσης του επαγγέλματος.

Μια από τις μεγαλύτερες κατηγορίες ατόμων που προκαλούν προβλήματα ασφαλείας περιλαμβάνει τους δυσαρεστημένους υπαλλήλους ή πρώην υπαλλήλους που νιώθουν ότι αδικήθηκαν ή φέρουν μια βαθιά αντιπάθεια για τους εργοδότες τους. Οι εργαζόμενοι ή πρώην εργαζόμενοι αποτελούν συνήθως τους πιο επικίνδυνους πληροφορικούς εγκληματίες αφού γνωρίζουν πολλούς από τους κωδικούς ασφαλείας και μέτρα προστασίας που είναι ήδη εγκατεστημένα. Ξέρουν σε ποιους υπολογιστές να επιτεθούν, ποια αρχεία θα δημιουργήσουν την μεγαλύτερη ζημιά αν σβηστούν και που βρίσκονται αποθηκευμένα τα αντίγραφα ασφαλείας.

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

2.2 Κλέφτες :

Μια δεύτερη κατηγορία περιλαμβάνει τους κλέφτες και τους παραχαράκτες. Αυτά τα άτομα θα μπορούσαν να εμποδίσουν την ομαλή λειτουργία ενός υπολογιστικού συστήματος για να εκμεταλλευθούν την κατάσταση που θα προκύψει ή να καλύψουν αποδείξεις της εγκληματικής τους δραστηριότητας.

2.3 Κατάσκοποι :

Βιομηχανική και πολιτική κατασκοπία ή σαμποτάζ είναι ένας άλλος λόγος συγγραφής κακόβουλου κώδικα. Οι προγραμματιζόμενες απειλές είναι ένα πολύ ισχυρό και δύσκολα εντοπίσιμο μέσο απόκτησης απόρρητων ή ευαίσθητων πληροφοριών, ή καθυστέρησης του ανταγωνισμού (σαμποτάζ).

2.4 Εκβιαστές :

Ο εκβιασμός μπορεί επίσης να αποτελέσει κίνητρο για την συγγραφή τέτοιου είδους λογισμικού. Σε αυτήν την περίπτωση οι εκβιαστές απειλούν να ενεργοποιήσουν καταστροφικό λογισμικό αν δεν πληρωθεί κάποιο ποσό ή αν δεν ικανοποιηθεί κάποια άλλη τους επιθυμία. Πολλές εταιρίες έχουν πέσει θύματα κάποιας μορφής εκβιασμού στην οποία έχουν συμφωνήσει να μην κινηθούν δικαστικά εναντίον των ατόμων που παραβίασαν την ασφάλεια των υπολογιστικών τους συστημάτων. Δεν είναι λίγες οι περιπτώσεις μάλιστα όπου οι εταιρίες έχουν προσλάβει στο προσωπικό τους τέτοιου είδους

άτομα. Σε αντάλλαγμα οι εκβιαστές συμφωνούν να μην φανερώσουν δημόσια τις ατέλειες των δικτύων των εταιριών που τους επέτρεψαν την παράνομη πρόσβαση.

Φυσικά ο σημαντικότερος λόγος για τον οποίο οι εταιρίες διστάζουν να οδηγήσουν σε δίκη κάποιο εκβιαστή είναι η δυσφήμιση που θα υποστούν σχετικά με την ασφάλεια τους και επίσης η απειλή περαιτέρω ζημιάς αν δεν ανακαλυφθούν και διορθωθούν οι αδυναμίες στην ασφάλεια.

2.5 Πειραματιστές :

Αναμφίβολα κάποιες προγραμματιζόμενες απειλές θα γραφτούν από πειραματιστές και περίεργους. Μερικές φορές τα άτομα αυτής της κατηγορίας μπορεί να δημιουργήσουν κάποιο πρόγραμμα που να αποβεί επικίνδυνο λόγω κάποιων προγραμματιστικών λαθών στον κώδικα του ή λόγω αφέλειας ή κακής κρίσης από μέρους τους.

2.5 Λαγωνικά Δημοσιότητας :

Άλλο μεγάλο κίνητρο για την συγγραφή ενός ιού ή σκουληκιού μπορεί να είναι το κέρδος, η φήμη ή απλά η ικανοποίηση του εγώ από το κυνηγητό. Σε αυτό το συχνό σενάριο, κάποιος θα συγγράψει έναν ιό, θα τον εξαπολύσει στο διαδίκτυο και μετά θα προσπαθήσει να κερδίσει δημοσιότητα σαν αυτός που τον ανακάλυψε, ή σαν ο πρώτος που θα δημιουργήσει κώδικα που τον απενεργοποιεί, ή απλά να κοκορευτεί για το δημιούργημα του σε κάποιο δημόσιο χώρο συνομιλιών στο διαδίκτυο. Αυτού του είδους το σενάριο εμφανίζεται με αυξημένη συχνότητα τελευταία αφού τώρα πια δίνεται μεγάλη έμφαση από τον δημοσιογραφικό τύπο και την τηλεόραση σε τέτοιου είδους γεγονότα.

2.6 Πολιτικοί ακτιβιστές :

Ένα στοιχείο με αυξανόμενη συχνότητα στον χώρο της συγγραφής ιών φαίνεται να είναι υποθάλπουσα πολιτική σκοπιμότητα. Οι ιοί σε αυτήν την κατηγορία μεταφέρουν κάποιο είδος πολιτικού μηνύματος είτε σαν κύριο λόγο ύπαρξης τους είτε για αντιπερισπασμό. Αυτό το στοιχείο αναγάγει την συγγραφή ιών σε ένα εργαλείο στα χέρια πολιτικών εξτρεμιστών που ζητάνε κάποιο κοινό ή ακόμη χειρότερα όταν επιθυμούν την παρενόχληση κυβερνητικών, κοινωνικών ή επιχειρησιακών ιδρυμάτων. Προφανώς η επίθεση στα υπολογιστικά δίκτυα τέτοιων ιδρυμάτων και οργανισμών εξυπηρετεί τους σκοπούς κάποιου μεγαλύτερου πολιτικού σκοπού.

Βιβλιογραφία – Ιστοσελίδες

1)Δημήτριος Μ. Πουλάκης, Κρυπτογραφία, η επιστήμη της ασφαλούς επικοινωνίας, Εκδόσεις Ζήτη, Δεκέμβριος 2005.
2)Nigel Smart, *Cryptography: An Introduction*, McGraw-Hill Education, November 2002.
3)Douglas Stinson, *Cryptography: Theory and Practice (Discrete Mathematics & Its Applications S.)*, CRC Press, February 27, 2002.

4)Richard A. Mollin, *An Introduction to Cryptography*, CRC Press, August 10, 2000.

5)Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 16, 1996. (Ελεύθερα διαθέσιμο στο http://www.cacr.math.uwaterloo.ca/hac/)

6)Δημήτρης Γκριτζαλης, Στέφανος Γκριτζαλης, Σωκράτη Κατσικα, Ασφάλεια Δικτύων υπολογιστών, Εκδόσεις Παπασωτηριου 2003

Web Security Privacy &
Commerce (2Nd Ed 2001)
- Simson Garfinkel
O'Reilly

7)Ασφάλεια Δικτύων Υπολογιστών - Πομπόρτσης Ανδρέας, Παπαδημητρίου Γεώργιος - Τζίολα - 2003 - ISBN 960-8050-88X

8)Ισόβια στους χάκερ; Απόψεις για το Ιντερνετ, την επιστήμη και όλα τα υπόλοιπα. Χρίστος Παπαδημητρίου, Εκδόσεις Καστανιώτη, 2004,

http://www.go-online.gr/ebusiness/specials/article.html?article_id=710
http://www.it.uom.gr/project/ergac/Cryptografisi/ERGASIA_C.htm
http://www.cacr.math.uwaterloo.ca/hac/
http://www.e21.gr/articles_full.asp?ArticleID=242#
http://www.techteam.gr/lofiversion/index.php/t9765.html
http://www.chi-publishing.com/samples/ISB0903HH.pdf
http://www.rsasecurity.com/rsalabs/node.asp?id=2125
http://www.kentlaw.edu/legalaspects/digital_signatures/tutorials/SSLD.html
http://www.minisoft.com/pages/connectivity/javelinHP/pages/encrypt.html
http://www.tech-invite.com/Ti-SSL.html
http://www.cs.bris.ac.uk/~bradley/publish/SSLP/chapter4.html

http://www.cisco.com/pcgi-bin/search/search.pl?siteToSearch=cisco.com&country=US&language=en&as_q=ssl&as_epq=&as_oq=&as_eq=&as_occt=any&location=en%7CUS&submit=Search
http://www.cisco.com/en/US/netsol/ns340/ns394/ns50/ns140/networking_solutions_white_paper09186a0080136858.shtml
http://www.webopedia.com/TERM/S/SSL.html

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

http://www.freesoft.org/CIE/Topics/121.htm
http://www.freesoft.org/CIE/Topics/ssl-draft/INDEX.HTM
http://www.webopedia.com/TERM/S/security.html
http://isp.webopedia.com/TERM/S/security.html
http://www.iec.org/online/tutorials/int_sec/
http://www.bitpipe.com/tlist/Internet-Security.html
http://www.albion.com/security/intro-4.html

http://67.18.47.148/com/index/about-internet/data/astinomia/asfaleia.asp
http://67.18.47.148/com/index/about-internet/data/astinomia/diadiktio_kai_dikaio.asp