ΤΕΙ Πατρών

Σχολή Διοίκησης Οικονομίας

Τμήμα Επιχειρηματικού Σχεδιασμού & Πληροφοριακών Συστημάτων

2009

Πτυχιακή Εργασία:

Ασφάλεια Δικτύων – Το Ηλεκτρονικό Ταχυδρομείο

Φοιτητές:

Θεολόγος Νικόλαος

Μπαδήμας Χρήστος

Σημηριώτης Ιωάννης

Εποπτεύων Καθηγητής:

Δρ. Μπακάλης Άρης

Περιεχόμενα

Ευχαριστίες

Ευχαριστούμε τον καθηγητή μας εκπαιδευτικό του ΤΕΙ Πάτρας κ. Άρη Μπακάλη, για την βοήθειά και την καθοδήγηση του η οποία ήταν πολύτιμη και καθοριστική για την διεκπεραίωση αυτής της εργασίας. Ευχαριστούμε επίσης, τον κ. Μάνο Κοκκολάκη, καθηγητή στο Αμερικάνικο Κολέγιο Ελλάδας (Deree) για τις συμβουλές του σε θέματα ασφάλειας, τον κ. Νικόλαο Μιχαλοδημητράκη, διαχειριστή συστήματος από το Τμήμα Βιολογίας του Πανεπιστημίου Κρήτης και τον κ. Νικόλαο Γιολδάση διαχειριστή συστήματος του ΤΕΙ Πατρών για τις απαντήσεις τους στα ερωτηματολόγια που τους αποστείλαμε για την μελέτη περίπτωσης.

Περίληψη

Από την αρχή της δημιουργίας του το Internet έπρεπε να παρέχει στους χρήστες του ασφάλεια για να μπορέσουν να το εμπιστευτούν και να το χρησιμοποιήσουν. Για τον λόγο αυτό συνεχώς αναπτύσσονταν και αναπτύσσονται διάφορα πρωτόκολλα με σκοπό να διασφαλίσουν την ακεραιότητα των δεδομένων που μεταδίδονται καθώς και πρωτόκολλα τα οποία θα εξυπηρετούν τον χρήστη στις ενέργειες που κάνει μέσω του Internet. Η υπηρεσία που ξεχώρισε και έφτασε σε σημείο σήμερα να θεωρείται αυτονόητο πως ο κάθε άνθρωπος που χρησιμοποιεί το Internet την χρησιμοποιεί είναι το ηλεκτρονικό ταχυδρομείο που στην ασφάλεια αυτής θα εστιάσουμε σε αυτή την εργασία.

Κατά τη διάρκεια αυτής της πτυχιακής περιγράφεται ο τρόπος λειτουργίας των σημαντικότερων και ευρέως χρησιμοποιούμενων πρωτοκόλλων για την μεταφορά της αλληλογραφίας μέσω του διαδικτύου, για πρωτόκολλα και εφαρμογές κρυπτογράφησης και για πρωτόκολλα ασφάλειας. Επίσης περιγράφονται και τα προβλήματα ασφάλειας που συναντάμε στο ηλεκτρονικό ταχυδρομείο καθώς και τα πρωτόκολλα και αλγόριθμοι για την αντιμετώπισή τους.

Κάνουμε αναφορά στις σημαντικότερες απειλές που συναντά ο μέσος χρήστης στο δίκτυο του και στο ηλεκτρονικό ταχυδρομείο, όπως είναι το spoofing, τα προγράμματα dialer, το phishing, τα e-mail bomb, τα hoaxes, οι ιοί, το sniffing και το spamming, καθώς και απλούς τρόπους αντιμετώπισης. Πραγματοποιήσαμε μέσω του προγράμματος Wireshark μια εικονική επίθεση sniffing μέσω πρωτοκόλλου HTTP για να διαπιστώσουμε πόσο εύκολο είναι να δει κάποιος 3ος δεδομένα που καταχωρούμε σε ιστοσελίδες κατά την περιήγησή μας αν το επιθυμεί.

Πραγματοποιήσαμε επίσης μια έρευνα πάνω στην υπηρεσία της ηλεκτρονικής αλληλογραφίας που προσφέρουν τα δύο εκπαιδευτικά ιδρύματα που συμμετείχαν για το επίπεδο ασφάλειας, τους τρόπους μεταφοράς της από τους mail servers στα mailbox των χρηστών, με σκοπό να διαπιστώσουμε πόσο αποδοτικά είναι.

Τέλος παρουσιάζουμε τρόπους – λύσεις για την ασφάλεια των δικτύων και των χρηστών όπως είναι τα Firewall, το Astaro Mail Gateway που απευθύνεται κυρίως σε επιχειρήσεις και το ESET Smart Security, μια εμπορική εφαρμογή για την προστασία προσωπικών υπολογιστών από τις περισσότερες απειλές που αναφέρουμε.

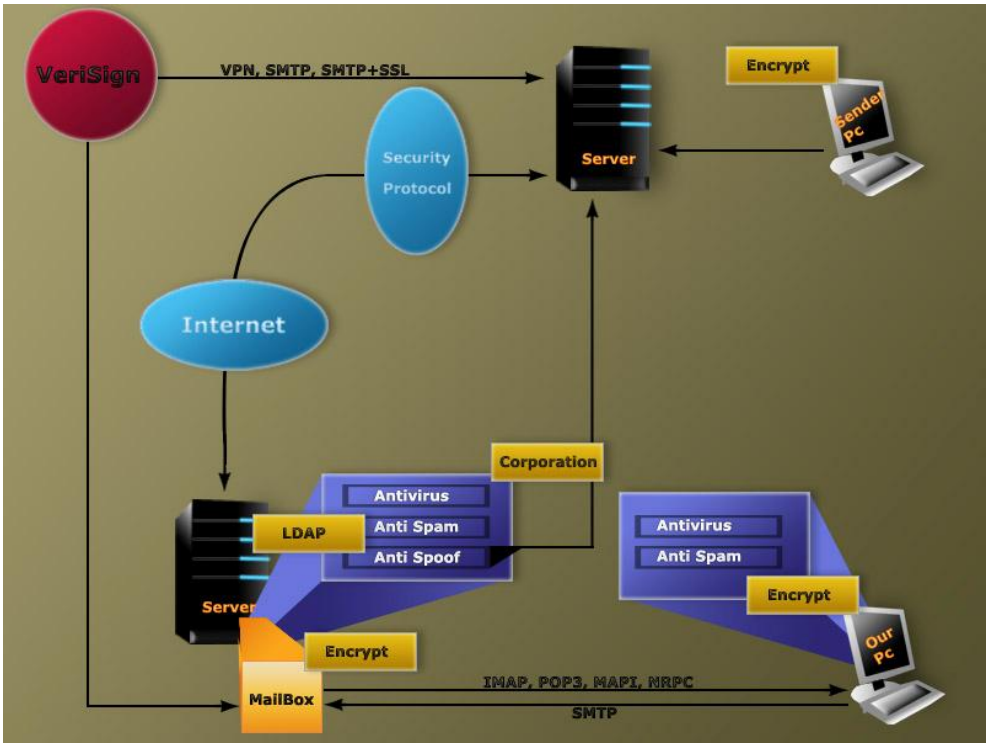
Εισαγωγή

Προτού αρχίσουμε να αναλύουμε την ασφάλεια των δικτύων – το ηλεκτρονικό ταχυδρομείο θα πρέπει να ορίσουμε τι είναι το e-mail, πως αποστέλλετε, και από ποιες διαδικασίες περνάει. Στα Ελληνικά το e-mail ορίζεται ως ηλεκτρονική αλληλογραφία και αποτελεί μια υπηρεσία του Internet, η οποία χρησιμοποιείται για την επικοινωνία των χρηστών και τη μεταφορά οποιουδήποτε ψηφιακού αρχείου. Όταν αποφασιστεί η έναρξη αποστολής ενός ηλεκτρονικού μηνύματος ακολουθούνται αρκετά στάδια μέχρις ότου καταλήξει στον τελικό παραλήπτη, τα οποία θα δούμε παρακάτω.

Πρώτα από όλα ο αποστολέας συντάσσει το ηλεκτρονικό μήνυμα στον προσωπικό του υπολογιστή μέσο ενός επεξεργαστή κειμένου, ύστερα από τον προσωπικό του υπολογιστή, μέσο μιας εφαρμογής αποστολής ηλεκτρονικής αλληλογραφίας, το αποστέλλει στο mail box «ηλεκτρονικό γραμματοκιβώτιο του», που φιλοξενείται στον server. Ο server είναι ο ενδιάμεσος που θα του προωθήσει το ηλεκτρονικό μήνυμα στο server του αποδέκτη. Κατά την αποστολή του e-mail ο χρήστης έχει τη δυνατότητα, ανάλογα με τη σημαντικότητα που κρίνει ότι έχει το μήνυμά του, να το κρυπτογράφηση ή όχι. Όταν φτάσει πλέον το μήνυμα από τον προσωπικό υπολογιστή στον server, ο server το προωθεί σε αυτόν του αποδέκτη. Στο στάδιο αυτό, εάν θέλει ο χρήστης έχει τη δυνατότητα να χρησιμοποιήσει encryption το pgp, s/mime κτλ. Επίσης μπορεί να χρησιμοποιήσει και ψηφιακό πιστοποιητικό από εταιρίες του χώρου όπως η VeriSign για να είναι ασφαλέστερη η μεταφορά.

Κατά τη διάρκεια που το e-mail ταξιδεύει στο διαδίκτυο υπάρχει περίπτωση να περάσει και από άλλους ενδιάμεσους servers, οι οποίοι δεν είναι οι τελικοί αποδέκτες, απλά χρησιμοποιούνται για να το προωθήσουν στον τελικό αποδέκτη ως διαμεσολαβητές. Ένας μεγάλος κίνδυνος στο στάδιο αυτό, είναι η υποκλοπή του μηνύματος αυτού από ενδιάμεσους κακόβουλους χρήστες. Εδώ χρησιμεύει η κρυπτογράφηση του μηνύματος, η οποία καθιστά αυτόματος το μήνυμα μη αναγνώσιμο από τρίτους. Όταν τελικά φτάσει στον τελικό server, ακολουθούνται αρκετές διαδικασίες ελέγχου στο περιεχόμενο του μηνύματος. Γίνεται έλεγχος για antivirus, antispam και antispoof. Στο τελευταίο πρέπει ο server αποδέκτης να επικοινωνήσει με το server αποστολέα για να κάνει την επιβεβαίωση. Τέλος θα σταλεί από τον server στο παραλήπτη με τα πρωτόκολλα POP3, IMAP κτλ. όπου εκεί

θα γίνει έλεγχος antivirus, antispamming και ύστερα θα αποκρυπτογραφηθεί (εάν είναι κρυπτογραφημένο) από τον τελικό χρήστη. Στο παρακάτω σχήμα φαίνεται η διαδικασία που αναλύσαμε παραπάνω.



Εικόνα 1 - Διαδικασία αποστολής e-mail

1. Υπηρεσίες ασφάλειας και διασφάλιση συστήματος

1.1. Υπηρεσίες ασφάλειας

Στο σημερινό κόσμο της δια-δικτύωσης και του ηλεκτρονικού εμπορίου κάθε υπολογιστικό σύστημα είναι ένας πιθανός στόχος. Σπάνια περνάει ένας μήνας χωρίς ειδήσεις που να αφορούν την "κατάληψη" και το "τρύπημα" των υπολογιστικών συστημάτων μεγάλων εταιριών και οργανισμών. Αν και λέγεται, από ορισμένους hackers, ότι τέτοιες επιθέσεις αποτελούν παιχνίδια κάποιων εφήβων το φαινόμενο έχει γίνει πιο μεθοδικό και απειλητικό τα τελευταία χρόνια.

Ακόμα και αν τίποτα δεν αλλάξει ή τίποτα δεν αφαιρεθεί οι διαχειριστές των συστημάτων πρέπει να ξοδεύουν ώρες ατελείωτες για την επανεγκατάσταση και επανα-ρύθμιση ενός τρυπημένου συστήματος για να είναι φτάσουν πάλι σε ένα ικανοποιητικό επίπεδο εμπιστοσύνης προς αυτό. Δεν υπάρχει κανένας τρόπος να γνωρίζουμε τα κίνητρα του εισβολέα και έτσι πρέπει να υποθέτουμε το χειρότερο.

Πολλοί διαφορετικοί τύποι ανθρώπων μπαίνουν σε υπολογιστικά συστήματα τρυπώντας την ασφάλειά τους. Άλλοι το κάνουν για πλάκα και άλλοι αποσκοπώντας σε κάποιο κέρδος. Υπάρχουν επίσης στοιχεία οργανωμένου εγκλήματος και κατασκοπευτικής δράσης οδηγούμενα από κυβερνήσεις, οργανισμούς, εταιρίες ή και τρομοκρατικές ομάδες. Οι πιο επικίνδυνοι από όλους, για κάποιο δίκτυο, είναι οι νυν και πρώην χρήστες του ίδιου του δικτύου διότι αυτοί γνωρίζουν τα συστήματα ασφάλειας και το που πρέπει να χτυπήσουν ώστε να προκαλέσουν ζημιά.

Παρά την ύπαρξη όλων αυτών των κινδύνων το ενδιαφέρον για τη δικτύωση των υπολογιστικών συστημάτων και για το Internet δεν υπήρξε ποτέ μεγαλύτερο. Ο αριθμός των υπολογιστών στο Internet διπλασιάζεται κάθε χρόνο για μια δεκαετία τώρα. Μέχρι αυτή τη στιγμή που συντάσσεται αυτή η πτυχιακή εργασία, το νούμερο των υπολογιστών που είναι στο διαδίκτυο ανά όλη την υφήλιο ξεπερνάει το ένα δισεκατομμύριο.

Όροι όπως ασφάλεια, προστασία και διασφάλιση του απορρήτου έχουν αποκτήσει παραπάνω από μία έννοιες. Ακόμα και οι επαγγελματίες του είδους δεν μπορούν να συμφωνήσουν στην ουσία αυτών των όρων. Μπορούμε, ωστόσο, να χρησιμοποιήσουμε μια πρακτική προσέγγιση και να πούμε ότι:

"ασφάλεια υπολογιστικού συστήματος έχουμε όταν μπορούμε να βασιστούμε σε αυτό και στο λογισμικό του στο να συμπεριφερθεί όπως περιμένουμε από αυτό".

Μέσα σε αυτόν τον πλατύ ορισμό υπάρχουν διαφορετικές μορφές ασφάλειας, οι οποίες πρέπει να απασχολούν τόσο τους διαχειριστές όσο και τους απλούς χρήστες των δικτύων και των συστημάτων τους όπως:

1.1.1. Εμπιστευσιμότητα (Confidentiality)

Είναι η διασφάλιση της πληροφορίας από οποιονδήποτε δεν έχει το δικαίωμα να την δει ή να κρατήσει αντίγραφό της. Αυτός ο τύπος ασφάλειας περιλαμβάνει τόσο την προστασία του συνόλου της πληροφορίας όσο και μέρους της το οποίο από μόνο του μπορεί να δείχνει άκακο αλλά που μπορεί να οδηγήσει στην αποκάλυψη άλλων σημαντικών πληροφοριών.

1.1.2. Ακεραιότητα δεδομένων (Data Integrity)

Είναι η προστασία της πληροφορίας, συμπεριλαμβανομένων των προγραμμάτων, από το σβήσιμό της ή την με οποιονδήποτε τρόπο αλλοίωσή της χωρίς την άδεια του ιδιοκτήτη της. Η υπό προστασία πληροφορία περιλαμβάνει επίσης αντικείμενα όπως backup ταινίες και αρχεία λογαριασμών.

1.1.3. Καταγραφή (Audit)

Ο διαχειριστής ενός δικτύου δεν πρέπει να ανησυχεί μόνο για τους χρήστες χωρίς άδεια πρόσβασης αλλά και για εκείνους που αν και νόμιμοι κάνουν λάθη ή προκαλούν σκόπιμα κάποιο πρόβλημα. Σε τέτοιες περιπτώσεις πρέπει να καθορισθεί τι έχει γίνει, από ποιόν και τι επηρεάστηκε. Ο μόνος τρόπος να επιτύχουμε όλα τα παραπάνω είναι να κάνουμε χρήση κάποιων αρχείων καταγραφής της δραστηριότητας στο σύστημα το οποίο να είναι ικανό να μας δώσει πληροφορίες για το ποιος και τι έκανε.

1.1.4. Διαθεσιμότητα (Availability)

Αφορά την προστασία των υπηρεσιών έτσι ώστε να μην υποβαθμιστεί η δυνατότητα παροχής τους. Εάν κάποια στιγμή ζητηθεί μια συγκεκριμένη υπηρεσία από νόμιμο χρήστη και δεν του δοθεί, αυτό ισοδυναμεί με την απώλεια της πληροφορίας που βρίσκεται στο σύστημα.

1.1.5. Συνέπεια (Consistency)

Η διασφάλιση ότι το σύστημα συμπεριφέρεται όπως αναμένεται από τους εξουσιοδοτημένους χρήστες του. Εάν το λογισμικό ή το υλικό μέρος του συστήματος αρχίσει να συμπεριφέρεται παράξενα, ειδικά μετά από κάποια αναβάθμιση ή μετατροπή τότε επίκειται καταστροφή. Τελικά η συνέπεια είναι η διασφάλιση της ορθότητας των δεδομένων και των προγραμμάτων που χρησιμοποιούμε.

1.1.6. Έλεγχος (Control)

Ο έλεγχος πρόσβασης στο σύστημα - παράνομοι χρήστες και λογισμικό μπορεί να δημιουργήσουν μεγάλα προβλήματα.

Αν και όλες οι παραπάνω μορφές / υπηρεσίες ασφάλειας είναι εξίσου σημαντικές, διαφορετικοί οργανισμοί δίνουν διαφορετική προτεραιότητα στη καθεμία διότι αντιμετωπίζουν διαφορετικού είδους απειλές. Για παράδειγμα:

- Σε ένα τραπεζικό περιβάλλον τα πιο σημαντικά είναι η ακεραιότητα της πληροφορίας και η καταγραφή των πράξεων των χρηστών και κατόπιν έρχονται εμπιστευσιμότητα και η διαθεσιμότητα της.
- Σε ένα περιβάλλον σχετιζόμενο με την εθνική ασφάλεια το οποίο επεξεργάζεται απόρρητες πληροφορίες, η εμπιστευσιμότητα έρχεται πρώτη και η διαθεσιμότητα τελευταία.

Σε ένα πανεπιστημιακό περιβάλλον πιο σημαντικά θεωρούνται η ακεραιότητα και η διαθεσιμότητα της πληροφορίας.

1.2. Βήματα Διασφάλισης ενός Συστήματος

1.2.1. Αξιολόγηση Απαιτήσεων και Κινδύνων

Το πρώτο βήμα στην εγκατάσταση ενός ασφαλούς συστήματος ή στην βελτίωση της ασφάλειας κάποιου είδη υπάρχοντος είναι η απάντηση των παρακάτω ερωτημάτων και η υλοποίηση των απαντήσεών τους:

- Τι προσπαθούμε να προστατεύσουμε; Καθορισμός του αντικειμένου της ασφάλειας
- Από ποιόν προσπαθούμε να το προστατέψουμε; Αναγνώριση των απειλών
- Πόσο χρόνο, προσπάθεια και τι κόστος προτιθέμεθα να αφιερώσουμε για να λύσουμε το πρόβλημα ασφάλειας που μας απασχολεί; Υπολογισμός του κόστους.

1.2.2. Ανάλυση Κόστους Απολαβής

Αφού ολοκληρώσουμε την αξιολόγηση των απαιτήσεών μας για ασφάλεια πρέπει να αντιστοιχίσουμε σε κάθε αντικείμενο που χρήζει της προστασίας μας και κάποιο κόστος που πρέπει να καταβάλουμε για να το προστατέψουμε αλλά και το κόστος με το οποίο θα επιβαρυνθούμε σε περίπτωση που το αφήσουμε απροστάτευτο και πάθουμε κάποια ζημιά εξαιτίας αυτής μας της επιλογής. Η επεξεργασία των στοιχείων που προκύπτουν από το σύνολο αυτών των διεργασιών μας δίνει κάποιο αποτέλεσμα που καθορίζει το βαθμό εφαρμογής λύσεων για την προστασία των δεδομένων μας.

1.2.3. Πολιτική Ασφάλειας

Στο τελευταίο βήμα ανήκει η αποδοχή μιας κοινής πολιτικής ασφάλειας. Η πολιτική ασφαλείας ενός δικτύου είναι αυτή που καθορίζει, εν τέλει, το γενικό πλαίσιο του τι προσπαθούμε να προστατέψουμε και γιατί. Δίνει γενικές γραμμές και κατευθύνσεις που θα πρέπει να ακολουθηθούν και υπαγορεύει το σκεπτικό λειτουργίας του δικτύου και τη θέση όλων των χρηστών αλλά και υπηρεσιών του.

Για την υλοποίηση λύσεων ασφάλειας στα δίκτυα έχουμε πολλά πρωτόκολλα, τεχνικές και εργαλεία, αντιπροσωπευτικά δείγματα των οποίων θα δούμε αναλυτικά στη συνέχεια αυτής της εργασίας.

2. SMTP - Simple Mail Transfer Protocol

Το SMTP είναι το καθιερωμένο πρωτόκολλο που χρησιμοποιείται στην μετάδοση των μηνυμάτων ηλεκτρονικού ταχυδρομείου στο διαδίκτυο. Ο λόγος δημιουργίας του πρωτοκόλλου ήταν στο να καταστεί δυνατή η επικοινωνία απομακρυσμένων χρηστών με διαφορετικά υπολογιστικά συστήματα. Αυτό έγινε αρχικά με τα πρωτόκολλα Mail Box Protocol το οποίο δημιουργήθηκε το 1971, το FTP Mail του 1973 και το Mail Protocol. Το 1982 δημιουργήθηκε το SMTP το οποίο σε αντίθεση με τα παραπάνω πρωτόκολλα, δεν βασιζόταν τόσο στο πρωτόκολλο FTP, αλλά ήταν ένας διαφορετικός μηχανισμός για την επικοινωνία του mail server με τον client. Για να πραγματοποιηθεί η επικοινωνία του προγράμματος μεταφοράς μηνυμάτων με τον απομακρυσμένο διακομιστή δημιουργείται μια TCP σύνδεση και στη συνέχεια τα δύο προγράμματα (πρόγραμμα μεταφοράς μηνυμάτων και διακομιστής) κάνουν χρήση του πρωτοκόλλου SMTP το οποίο επιτρέπει στον αποστολέα να δηλώνει την ταυτότητά του, να καθορίζει τον αποδέκτη και να μεταφέρει την ηλεκτρονική αλληλογραφία.

Το πρωτόκολλο SMTP εκτός από τα παραπάνω είναι υπεύθυνο για πολλές ακόμα λειτουργίες, όπως το να υπάρχει αντίγραφο των μηνυμάτων στον αποστολέα μέχρι να αποθηκευτεί το μήνυμα από τον παραλήπτη και είναι αυτό που χρησιμοποιείται για να ελέγχεται αν ένα ηλεκτρονικό γραμματοκιβώτιο υπάρχει σε κάποιον απομακρυσμένο διακομιστή.

Για την σωστή μετάδοση της ηλεκτρονικής αλληλογραφίας οι SMTP server θα πρέπει να έχουν ανοικτές κάποια από τις πόρτες 25 και 587 ή και τις δύο, αυτό για λόγους συμβατότητας ώστε να μπορούν να επικοινωνούν με τους άλλους SMTP servers.

3. Web Based e-mail

Web-based mail υπηρεσίες είναι e-mail accounts που φιλοξενούνται σε έναν web server. Οι ποιο δημοφιλείς εταιρίες για Web-based e-mail είναι:

- Hotmail (www.hotmail.com)
- Google (www.gmail.com)
- Yahoo (www.yahoo.com)

Καμία από αυτές τις υπηρεσίες δεν είναι καλύτερη ή χειρότερη από την άλλη, ειδικά όσο αναφορά την ασφάλεια. Όλες έχουν παρόμοια συστήματα για την αποφυγή επιθέσεων sniffing, cracking, social engineering και επιθέσεις βασισμένες σε κώδικα. Λόγο της μεγάλης δημοτικότητας το hotmail έχει δεχθεί τις περισσότερες επιθέσεις. Αυτό δεν σημαίνει όμως πως μία μικρή εταιρία είναι η λύση. Το πιθανότερο είναι πως δεν θα έχει την οικονομική δυνατότητα για τόσο καλό εξοπλισμό ώστε να αντιμετωπίσει και ποιο απλές επιθέσεις.

Για τη δημιουργία και τη σύνδεση στο web mail το μόνο που χρειάζεται είναι ένας browser όπως Internet Explorer, Safari, Opera, Chrome. Οι υπηρεσίες αυτές προτιμούνται για τους εξής λόγους:

- **Κόστος:** Τα περισσότερα web sites προσφέρουν αυτήν την υπηρεσία χωρίς κόστος.
- **Εύκολη πρόσβαση:** Τα web-based mails το μόνο που χρειάζονται όπως προαναφέραμε είναι έναν browser και πρόσβαση στο διαδίκτυο. Από εκεί και πέρα μπορούμε να έχουμε πρόσβαση στο e-mail μας από οπουδήποτε, οποιαδήποτε στιγμή και με οποιονδήποτε υπολογιστή. Η πρόσβαση στο e-mail είναι ιδιαίτερα εύκολη ζητώντας μόνο την ηλεκτρονική μας διεύθυνση και το password μας.
- **Φορητότητα:** για να έχουμε ένα server mail πρέπει να στήσουμε το πρόγραμμα στον υπολογιστή μας και μπορούμε να μπαίνουμε μόνο μέσο του υπολογιστή μας. Αντίθετα στα web mail μπορούμε να εισέλθουμε με οποιονδήποτε υπολογιστή. Άρα δεν είμαστε υποχρεωμένοι να μεταφέρουμε το laptop μας όπου και αν πάμε.
- **Ικανότητα ανάγνωσης του e-mail μας από διάφορους Servers:** κάθε web based mail υπηρεσία, μας επιτρέπει να κατεβάσουμε το e-mail μας και να το

διαβάσουμε μέσο του προγράμματος που χρησιμοποιούμε. Επίσης τώρα πια μας επιτρέπει να το διαβάσουμε χωρίς καν να κατεβάσουμε το αρχείο στον υπολογιστή μας. Εκτός αυτού το e-mail μπορούμε να το αφήσουμε στο διαθέσιμο χώρο που μας δίνει η εταιρία ώστε να έχουμε πρόσβαση και μετέπειτα από όπου και αν βρισκόμαστε.

- **Πολλαπλότητα εφαρμογών:** πολλά sites που έχουν web mail υπηρεσίες, μας επιτρέπουν να έχουμε περεταίρω εφαρμογές μέσα στην υπηρεσία που μας προσφέρουν όπως το να στείλουμε και φαξ μέσω Internet, με πολύ χαμηλό κόστος.
- **Εμπιστοσύνη:** ο χρήστης έχει πολύ μεγαλύτερη εμπιστοσύνη όταν κάνει hosting το e-mail του σε μία εταιρία όπως η Microsoft (Hotmail) ή η Google (Gmail), παρά σε μία μικρή εταιρία της χώρας του.

Όλες αυτές οι υπηρεσίες που προσφέρονται δωρεάν έχουν και αυτές κάποια αρνητικά στοιχεία. Τα οποία είναι:

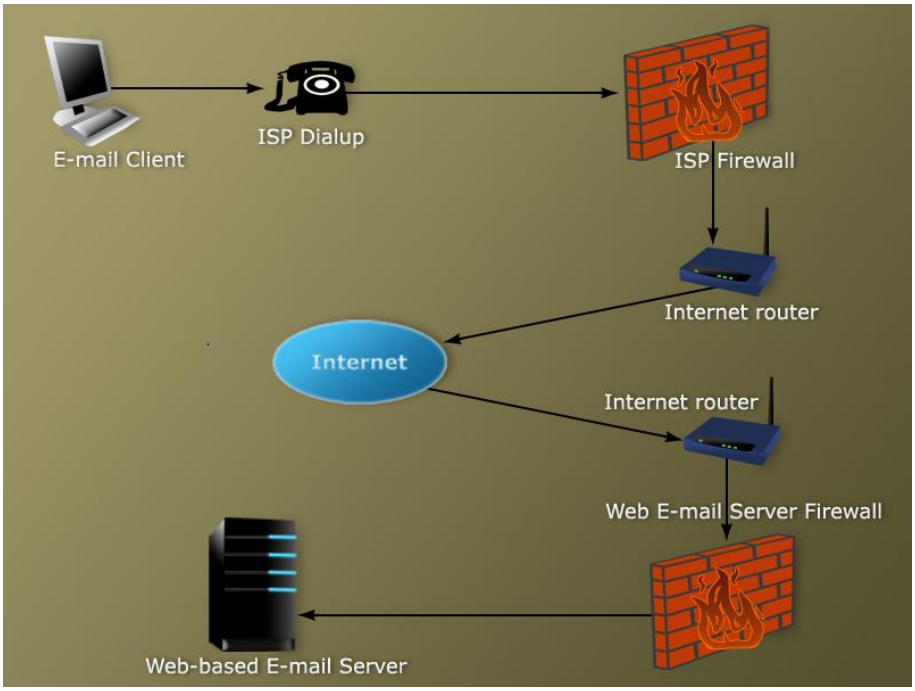
- **Junk mail:** παλαιότερα υπήρχε μεγάλο πρόβλημα με τα Junk mail πράγμα που στις μέρες μας έχει καταπολεμηθεί σε μεγάλο βαθμό.
- **Απώλεια πληροφοριών:** κανείς δεν δεσμεύεται ότι δεν θα χάσουμε τα e-mail μας που κάνουν hosting οι εταιρίες αυτές. Πάντως μέχρι τώρα δεν έχει ακουστεί τέτοιο πρόβλημα οπότε, αν και κανείς δεν μας εγγυάται πως δε θα τα χάσουμε το πιθανότερο είναι να μην τα χάσουμε.
- **Παροχή ευαίσθητων προσωπικών στοιχείων σε τρίτους:** Μέσο e-mail είναι πιθανό να ανταλλαγούν κωδικοί πρόσβασης, προσωπικά στοιχεία και άλλα έγγραφα που μπορεί να μη θέλουμε να πέσουνε σε χέρια τρίτων . Σε αυτή τη περίπτωση βασιζόμαστε στην σωστή λειτουργία της εταιρίας ώστε να φροντίσει να διαφυλάξει τα προσωπικά μας στοιχεία.

Στον παρακάτω πίνακα παρουσιάζουμε συνοπτικά τους δύο τύπους e-mail και τους συγκρίνουμε στους τομείς:

- Της ασφάλειας,
- Της ευκολίας,
- Της χρηστικότητας
- Και του κόστους

	Web based mail	Server mail
Ασφάλεια	Η ασφάλεια των Web mails υπόκειται στη κρίση τρίτων, δηλαδή του εκάστοτε φορέα που κάνει hosting το mail μας. Αν η εταιρία είναι μεγάλη όπως Mircrosoft, Google, Yahoo. Η ασφάλεια θα είναι τουλάχιστον ικανοποιητική. Μοναδικό πρόβλημα είναι πως επειδή αυτές οι εταιρίες είναι ιδιαίτερα δημοφιλείς στους χρήστες, άλλο τόσο δημοφιλείς είναι και στους Crackers. Πάντως τα επίπεδα ασφαλείας τους είναι ιδιαίτερα ικανοποιητικά.	Η διαχείριση της ασφάλειας των Server mail γίνεται υπό την αιγίδα της επιχείρησης. Μπορεί να φτάσει σε καλύτερα επίπεδα από ότι αυτή του Web mail, διότι μπορούν να χρησιμοποιηθούν εξεζητημένες λύσεις όπως Lotus (πρωτόκολλο κλειστό μιας και ανάγεται σε σουίτα προϊόντων), δακτυλικό αποτύπωμα για Authentication, hardware Firewalls κ.α.. Ο μέσος όρος όμως των επιχειρήσεων δεν χρησιμοποιεί καλύτερη ασφάλεια από ότι δίνουν οι λύσεις των Web - Mail.
Ευκολία	Η ευκολία χρήσης του είναι αναμφισβήτητη, χρειάζεται ο χρήστης μόνο την ηλεκτρονική του διεύθυνση να γράψει και το password που επιθυμεί να χρησιμοποιήσει για να δημιουργήσει λογαριασμό σε όποια εταιρία Web mail θέλει.	Χρειάζεται ξεχωριστό πρόγραμμα όπως Outlook Express, Outlook και σίγουρα κάποιον που να ξέρει να στήσει το e-mail. Οι γνώσεις του μέσου χρήστη ηλεκτρονικών υπολογιστών δεν αρκούν για να το στήσει, οπότε χρειάζεται και έναν τεχνικό για να κάνει αυτή τη δουλεία.
Χρηστικότητα	Και εδώ το Web Mail δείχνει την ανωτερότητα του καθώς το μόνο που χρειάζεται είναι ένας browser. Ακόμα και έγγραφο pdf, doc, docx, xls, jpg, png, να σταλεί από τον αποστολέα, ο χρήστης του Web mail μπορεί να το διαβάσει χωρίς να το κατεβάσει στον υπολογιστή του μέσο της εφαρμογής που του δίνει η υπηρεσία.	Σε αυτή τη περίπτωση πρέπει να κατεβάσει ο χρήστης το Attachment για να το ανοίξει μέσο της εφαρμογής που έχει εγκατεστημένη στον υπολογιστή του. Αυτή η λύση είχε ανακαλυφθεί όταν δεν υπήρχαν ευρυζωνικές συνδέσεις οπότε ο χρήστης έκανε σύνδεση στο Internet κατέβαζε την αλληλογραφία του και ύστερα με τον χρόνο του τη διάβαζε χωρίς να χρεώνετε περαιτέρω. Στη προκειμένη περίπτωση και με τη διάδοση των εβρυζωνικών συνδέσεων κάτι τέτοιο έχει καταστεί μη ευέλικτο. Επίσης ο χρήστης μπορεί να δει την αλληλογραφία του και να την αποθηκεύσει μόνο από τον υπολογιστή που έχει στήσει για να τη δέχεται και όχι από οποιονδήποτε όπως συμβαίνει στα Web mail.
Κόστος	Οι υπηρεσίες Web Mail για χρήστες είναι δωρεάν, ενώ για επιχειρήσεις που προσφέρει π.χ. η Google κυμαίνονται σε χαμηλά κόστη.	Είναι άμεσα εξαρτημένο με το μέγεθος της επιχείρησης και την ασφάλεια που επιζητά η επιχείρηση. Σε κάθε περίπτωση το κόστος είναι μεγαλύτερο από ότι το Web mail.

Στο παρακάτω σχήμα φαίνεται η γενική δομή του web based e-mail,από τον χρήστη μέχρι τον mail server.



Εικόνα 2 - Δομή Web Based e-mail

4. Πρωτόκολλα ηλεκτρονικής αλληλογραφίας

4.1. Πρωτόκολλα POP3 και IMAP.

Στην πλειονότητα των περιπτώσεων, οι περισσότεροι χρήστες ηλεκτρονικού ταχυδρομείου, κάνουν χρήση της υπηρεσίας αυτής διαθέτοντας τον προσωπικό τους λογαριασμό σε έναν διακομιστή ή αλλιώς mail server ο οποίος βρίσκεται κάπου στο Internet και ενός προγράμματος με το οποίο θα γίνεται η διαχείριση της αλληλογραφίας όπως είναι το Netscape Messenger, το Microsoft Outlook κ.α. και σε συνδυασμό παρέχουν την δυνατότητα στον χρήστη να:

- Έχει εύκολη και γρήγορη πρόσβαση στο ηλεκτρονικό γραμματοκιβώτιο του από οποιοδήποτε σημείο βρίσκεται και
- Να μπορεί να οργανώνει την αλληλογραφία του όπως επιθυμεί σε φακέλους για την καλύτερη διαχείρισή της.

Αυτό δηλαδή που πρέπει να παρέχεται στον χρήστη είναι η δυνατότητα να λαμβάνει και να αποστέλλει μηνύματα ηλεκτρονικού ταχυδρομείου ανεξάρτητα από την γεωγραφική του θέση και του τρόπου σύνδεσης του στο διαδίκτυο. Αυτές τις ανάγκες προσπάθησε να καλύψει το πρωτόκολλο POP3.

Το πρωτόκολλο POP3 (Post Office Protocol) είναι αυτό που αναλαμβάνει να μεταφέρει την ηλεκτρονική αλληλογραφία του χρήστη από τον διακομιστή στον προσωπικό υπολογιστή του χρήστη. Για να το επιτύχει αυτό, αντιγράφει την αλληλογραφία του χρήστη από τον διακομιστή στον οποίο βρίσκεται αποθηκευμένη, στον υπολογιστή που χρησιμοποιεί εκείνη την ώρα ο χρήστης και στη συνέχεια την διαγράφει από τον διακομιστή. Με αυτό τον τρόπο λειτουργίας του πρωτοκόλλου προκύπτουν κάποια βασικά μειονεκτήματα όπως είναι:

- Μεγάλη καθυστέρηση στην μεταφορά των δεδομένων η οποία εξαρτάτε από τον όγκο τους αλλά και από τον τύπο πρόσβασης που έχει ο χρήστης στο διαδίκτυο. Το μειονέκτημα αυτό ήταν πιο εμφανή παλαιότερα που οι περισσότεροι χρήστες συνδέονταν μέσω τηλεφωνικών κλήσεων (dial up). Αντίθετα σήμερα που οι γραμμές είναι κυρίως ADSL δεν υπάρχει αυτό το πρόβλημα.
- Έλλειψη ασφάλειας, καθώς, οποιοσδήποτε χρησιμοποιούσε τον υπολογιστή κάποιου που τον είχε χρησιμοποιήσει νωρίτερα για την ανάγνωση της

αλληλογραφίας του, θα είχε πρόσβαση στην αλληλογραφία του δεύτερου χρήστη εκτός αν αυτός κάθε φορά μετά την ανάγνωση της, την διέγραφε.

- Τέλος, το βασικό μειονέκτημα που προκύπτει από τα παραπάνω, είναι πως τα μηνύματα είναι διαθέσιμα μόνο στον υπολογιστή που τα είχε “κατεβάσει” ο χρήστης τελευταία φορά (και δεν τα είχε διαγράψει), άρα δεν καλύπτεται η ανάγκη το ηλεκτρονικό ταχυδρομείο του χρήστη να είναι διαθέσιμο από όπου και να βρίσκεται ο χρήστης.

Αυτά τα μειονεκτήματα είναι που προσπάθησε να καλύψει το πρωτόκολλο IMAP. Το IMAP (Internet Message Access Protocol) και αυτό κάνει σύνδεση με τον διακομιστή για την μεταφορά της αλληλογραφίας, αλλά σε αντίθεση με το POP3, δεν μεταφέρει όλη την αλληλογραφία από τον διακομιστή, αλλά μόνο τους τίτλους των μηνυμάτων και ο χρήστης μετά αποφασίζει ποια από τα μηνύματα θα διαβάσει ολόκληρα και ποια όχι. Με τον τρόπο αυτό, αυτό που κατάφερε να κάνει το IMAP είναι:

- Η γρήγορη μεταφορά των πληροφοριών από τον διακομιστή στον προσωπικό υπολογιστή του χρήστη, μιας και μεταφέρετε πολύ λιγότερη πληροφορία,
- Ασφάλεια στην ανάγνωση των μηνυμάτων, αφού τα μηνύματα υπάρχουν στον διακομιστή και μεταφέρονται μόνο προσωρινά στον υπολογιστή που θα χρησιμοποιήσει ο χρήστης και θα πρέπει κάθε φορά να γίνεται πιστοποίηση του ονόματος χρήστη και του προσωπικού κωδικού του και τέλος
- Διαθεσιμότητα της αλληλογραφίας από οπουδήποτε αφού όπως είπαμε και παραπάνω, τα μηνύματα παραμένουν στον διακομιστή.

Σήμερα, οι περισσότερες εφαρμογές αλλά και οι mail server υποστηρίζουν και τα δυο πρωτόκολλα, για λόγους συμβατότητας, αλλά η πραγματικότητα είναι πως το πρωτόκολλο IMAP έχει μεγαλύτερη δημοτικότητα μιας και καλύπτει καλύτερα τις απαιτήσεις των χρηστών.

4.2. Εμπορικές λύσεις ηλεκτρονικής αλληλογραφίας

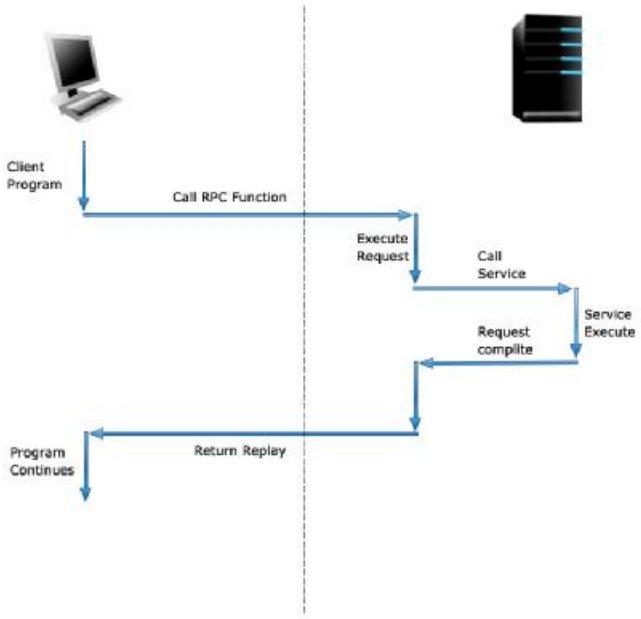
4.2.1. IBM Lotus Notes

Το Lotus Notes της IBM αποτελεί εδώ και χρόνια μια λύση ηλεκτρονικής αλληλογραφίας που απευθύνεται κυρίως σε επιχειρήσεις για να καλύπτεται η εσωτερική επικοινωνία και να διευκολύνεται η ηλεκτρονική συνεργασία. Η πλατφόρμα είναι τύπου διακομιστή – πελάτη (server - client) και παρέχει στους χρήστες επικοινωνία μέσω e-mail, ημερολόγιο και στην τελευταία της έκδοση (8.0) έχει

προστεθεί και το IBM Lotus Sametime που επιτρέπει στους χρήστες την ανταλλαγή άμεσων μηνυμάτων (Instant Messaging) και πραγματοποίηση τηλεδιασκέψεων με σκοπό την αύξηση της παραγωγικότητας των υπαλλήλων μιας επιχείρησης. Επίσης παρέχεται και η δυνατότητα του συγχρονισμού της πλατφόρμας με φορητές συσκευές για μεγαλύτερη ευκολία στην επικοινωνία και ευελιξία πρόσβασης.

Το Lotus Notes παρέχει αυξημένα επίπεδα ασφάλειας με χρήση των περισσότερο γνωστών και δοκιμασμένων πρωτοκόλλων ασφάλειας (SSL) και μεταφοράς της ηλεκτρονικής αλληλογραφίας (SMTP, POP, IMAP). Το Lotus Notes χρησιμοποιεί επίσης ένα πρωτόκολλο το οποίο ονομάζεται RPC ή NRPC (Notes Remote Procedure Calls) το οποίο βασίζεται σε client/server μοντέλο. Το RPC δίνει την δυνατότητα τα συστήματα που επικοινωνούν να μην βρίσκονται αναγκαστικά στον ίδιο χώρο αλλά και αν αυτά είναι διαφορετικών τεχνολογιών να μπορούν να επικοινωνούν μέσω του δικτύου της επιχείρησης. Επίσης δίνει πολλές δυνατότητες προγραμματισμού του μοντέλου client/server για όσο το δυνατόν καλύτερη επικοινωνία και γρηγορότερη απόκριση του συστήματος.

Πως λειτουργεί τώρα το NRPC. Όπως αναφέραμε βασίζεται στο μοντέλο client/server άρα όταν επιχειρείται μια αίτηση από τον πελάτη για κάποια υπηρεσία στον εξυπηρετητή, ο πρώτος περιμένει απάντηση από τον server για την εκτέλεση της εντολής. Όταν λάβει την απάντηση στέλνει την αίτηση για την υπηρεσία που θέλει. Όταν ολοκληρωθεί η αίτηση το πρόγραμμα του πελάτη συνεχίζει να εκτελείται και ο εξυπηρετητής είναι διαθέσιμος για άλλες αιτήσεις. Όπως φαίνεται το μοντέλο αυτό δίνει την δυνατότητα η εργασία να γίνεται κυρίως τοπικά δηλαδή στον υπολογιστή του κάθε χρήστη και να πραγματοποιούνται αιτήσεις στον εξυπηρετητή μόνο για υπηρεσίες προώθησης πληροφορίας με σκοπό ο server να μην είναι συνεχώς απασχολημένος για να μπορεί να ανταποκρίνεται ταχύτερα στις αιτήσεις.



Εικόνα 3 - Επικοινωνία Client-Server

Μία απομακρυσμένη διαδικασία ή όπως αναφέρθηκε παραπάνω αίτηση υπηρεσίας προσδιορίζεται μοναδικά από το τρίπτυχο:

- αριθμός προγράμματος (program number),
- αριθμός έκδοσης (version number),
- αριθμός διαδικασίας (procedure number).

Ένα πρόγραμμα μπορεί να αποτελείται από μία ή περισσότερες εκδόσεις. Κάθε έκδοση αποτελείται από μια συλλογή διαδικασιών που διατίθενται για απομακρυσμένη κλήση. Οι αριθμοί εκδόσεων κάνουν εφικτή την ταυτόχρονη διαθεσιμότητα πολλαπλών εκδόσεων πρωτοκόλλων RPC. Κάθε έκδοση περιέχει έναν αριθμό διαδικασιών που μπορούν να κληθούν από απόσταση. Κάθε διαδικασία διαθέτει ένα αριθμό διαδικασίας (procedure number).

4.2.2. Microsoft Exchange

Το Exchange είναι ένας διακομιστής συνεργατικής επικοινωνίας που έχει αναπτύξει η Microsoft. Βασίζεται στο ηλεκτρονικό ταχυδρομείο και προορίζεται κυρίως για επιχειρήσεις. Κάθε υπάλληλος ή χρήστης έχει τον δικό του λογαριασμό τον οποίο μπορεί να τον διαχειρίζεται μέσω του outlook και μπορεί να επικοινωνεί και εσωτερικά αλλά και εξωτερικά μέσω αυτού. Στις τελευταίες δυνατότητες έχει προστεθεί ο συγχρονισμός του λογαριασμού με φορητές συσκευές αλλά και η πρόσβαση από το Internet κάτι που στις αρχικές δεν υποστηριζόταν. Εκτός από την

επικοινωνία με e-mail υπάρχει και η δυνατότητα οι χρήστες να διατηρούν ημερολόγιο, τις επαφές τους και να προγραμματίζουν τις εργασίες τους.

Η πρώτη έκδοση της σουίτας κυκλοφόρησε τον Απρίλιο του 1993 και τον Ιανουάριο του 1995 είχε περίπου 500 χρήστες να χρησιμοποιούν την Beta 1. Η χρήση του διαδόθηκε πολύ γρήγορα και τον Απρίλιο του 1996 είχε 32000 χρήστες περίπου. Την ίδια χρονιά κυκλοφόρησε η έκδοση 4 η οποία ήταν και η πρώτη που μπορούσε να αγοραστεί από το ευρύ κοινό. Το 1997 κυκλοφόρησε η $5^{η}$ έκδοση η οποία αποτελούσε την πιο ολοκληρωμένη λύση καθώς έδινε την δυνατότητα της εγκατάστασης server τοπικά και παρείχε επικοινωνία μέσω SMTP στα δίκτυα. Οι εκδόσεις αυτές είχαν αρκετούς περιορισμούς στην χρήση όπως για παράδειγμα το μέγεθος των βάσεων δεδομένων που δεν μπορούσαν να ξεπερνάνε τα 16GB κάτι που σημαίνει και περιορισμό στους χρήστες.

Αυτοί οι περιορισμοί ξεπεράστηκαν με την έκδοση 6 αρχικά (Νοέμβριος 2000) και αργότερα με την 6.5 ή 2003, η οποία είχε μεγαλύτερες απαιτήσεις σε υπολογιστικό σύστημα, υποστήριζε βάσεις δεδομένων μέχρι 100GB (κάτι που σήμαινε και πολλούς χρήστες) και μπορούσε να εγκατασταθεί μόνο σε συστήματα με λειτουργικό Windows 2000 Server με SP4 ή Windows server 2003. Η έκδοση αυτή έδινε την δυνατότητα το σύστημα να μπορεί να τεθεί γρηγορότερα online και παρείχε και την δυνατότητα του συγχρονισμού με φορητές συσκευές. Είχε επίσης καλύτερη προστασία από ιούς και spam και έδινε και την δυνατότητα στον χρήστη να φιλτράρει τα εισερχόμενα e-mail μέσω της IP του αποστολέα. Η έκδοση αυτή ήταν προσανατολισμένη στην σχεδίαση του Microsoft Office 2003 κάτι που σημαίνει πως οι χρήστες είχαν ένα «κοινό» περιβάλλον εργασίας το οποίο και γνωρίζουν καλύτερα.

Το πρωτόκολλο που χρησιμοποιείται για την επικοινωνία με τον server είναι το RPC το οποίο έχει αναλυθεί στο Lotus Notes και το MAPI/RPC ή απλά MAPI (Messaging Application Programming Interface) που είναι το ενσωματωμένο πρωτόκολλο στο Outlook για την επικοινωνία του πελάτη – χρήστη με τον Exchange mail server. Το MAPI ουσιαστικά δεν έχει διαφορές από το RPC, απλά έχει διαφορετικό όνομα λόγω δικαστικών διαμαχών που είχε η Microsoft με άλλους οργανισμούς - εταιρίες. Ο τρόπος λειτουργίας είναι ο ίδιος.

Το RPC όπως και το MAPI είναι πρωτόκολλα τα οποία λειτουργούν σε LAN και WAN δίκτυα αλλά και σε VPN. Το RPC over HTTP είναι μια επέκταση του πρωτοκόλλου

μπορούμε να πούμε, το οποίο δίνει την δυνατότητα της επικοινωνίας με τον Microsoft Exchange Server μέσω του πρωτοκόλλου HTTP, δηλαδή την πρόσβαση μέσω browser από οποιονδήποτε υπολογιστή.

5. Κρυπτογραφία – Στεγανογραφία

Η **κρυπτογραφία** αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδομένων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη ή παραλήπτες. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε hardware λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου.

Η λογισμική κρυπτογραφία είναι φτηνότερη, πράγμα που την κάνει ευρέως αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια, δεν είναι το ίδιο γρήγορη με την εκτέλεση της σε hardware, αλλά η ολοένα αυξανόμενη ανάγκη για διασφάλιση των επικοινωνιών εδραίωσε την χρήση της. Εμείς, στις ακόλουθες σελίδες θα συζητήσουμε αποκλειστικά για την λογισμική κρυπτογραφία.

Στεγανογραφία είναι η τεχνική της απόκρυψης της ίδιας της ύπαρξης της πληροφορίας. Όπως για την κρυπτογραφία, έτσι και για την στεγανογραφία υπάρχουν δύο τρόποι υλοποίησης της: σε hardware και σε software. Η hardware εκτέλεση της είναι γρήγορη, αλλά πάρα πολύ ακριβή. Χρησιμοποιείται περισσότερο από κυβερνητικές υπηρεσίες και από τον στρατό, καθ' ότι οι τεχνολογίες που χρησιμοποιούνται είναι πολύ ανεπτυγμένες και καθόλου διαδεδομένες. Η εκτέλεση της σε software είναι πιο φθηνή και οι τεχνολογίες που απαιτούνται είναι σαφώς πιο εμπορικές. Στο Διαδίκτυο συναντάται η λογισμική στεγανογραφία για ευνόητους λόγους. Γι' αυτό το λόγο, θα σχολιάσουμε επί το πλείστον την λογισμική κρυπτογραφία παρακάτω.

5.1. Κρυπτογραφία

Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν. Κρυπτανάλυση (cryptanalysis) είναι η επίλυση

αυτών των προβλημάτων και κρυπτολογία (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτολογίας σε ένα ενιαίο επιστημονικό κλάδο.

Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο/συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους δεν έχουν πρόσβαση σε αυτά.

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, την χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν.

Στις μέρες μας κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός από την διασφάλιση του απόρρητου (privacy), η πιστοποίηση ταυτότητας (authentication) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητα μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας.

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουροι για το ποιος το έχει γράψει. Επίσης, μία ψηφιακή χρονοσφραγίδα (digital timestamp) συνδέει ένα έγγραφο με την ώρα της δημιουργίας του. Τέτοιοι μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση.

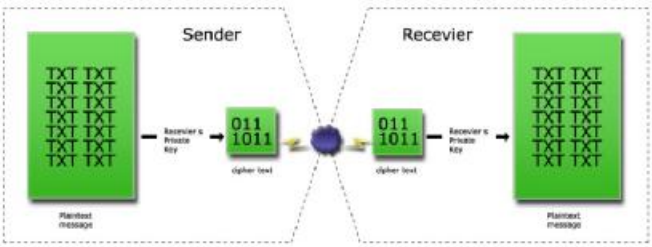
5.1.1. Είδη Κρυπτογραφίας

5.1.1.1. Ασύμμετρη Κρυπτογραφία (Public-Key Cryptography)

Η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική. Η ιδιωτική κλείδα δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνος που γνωρίζει την ιδιωτική κλείδα.

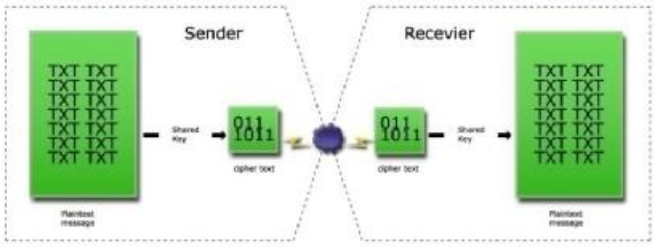


Εικόνα 4 - Ασύμμετρη κρυπτογραφία

Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

5.1.1.2. Συμμετρική Κρυπτογραφία (Symmetric Cryptography ή Secret-Key Cryptography)

Στην συνηθισμένη κρυπτογραφία, ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η Message Authentication Code (MAC).



Εικόνα 5 - Συμμετρική κρυπτογραφία

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

5.1.1.3. Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς

κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

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 περιβάλλοντα κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής

μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μιας και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι που θα αναλυθούν παρακάτω.

5.1.2. Κρυπτογραφικά Εργαλεία

Μέχρι τώρα αναφερθήκαμε στα δύο σημαντικότερα κρυπτοσυστήματα που ευρέως εφαρμόζονται σήμερα. Περιγράψαμε τις αρχές που τα διέπουν και το είδος των κλειδιών που χρησιμοποιούν (συμμετρικά ή ασύμμετρα). Στις ακόλουθες παραγράφους θα ασχοληθούμε με τους μηχανισμούς με τους οποίους εφαρμόζεται η κρυπτογραφία γενικότερα.

5.1.2.1. Block Ciphers

Block cipher είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα block μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε block κρυπτογραφημένου του ίδιου μήκους κειμένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται block size και για πολλούς ciphers είναι 64 bits. Στα μελλοντικά χρόνια το μήκος θα αυξηθεί στα 128 bits καθώς οι υπολογιστές γίνονται πιο ικανοί. Κάθε κείμενο δίνει διαφορετικό ciphertext.

Οι block ciphers λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα block διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα subkey. Το σύνολο των subkeys προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των subkeys καλείται key schedule.

Ο αριθμός των επαναλήψεων του επαναληπτικού cipher εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς ciphers ο αριθμός των επαναλήψεων για να επιτευχθεί ικανοποιητική ασφάλεια θα είναι πολύ μεγάλος για να πραγματοποιηθεί.

Οι Feistel ciphers είναι ειδικές περιπτώσεις επαναληπτικών ciphers όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής: το κείμενο χωρίζεται στο μισό. Η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός subkey και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό. Έπειτα, το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης X-OR. Η άλλη είσοδος της X-OR είναι το αποτέλεσμα του δεύτερου μετασχηματισμού, ο οποίος χρησιμοποιεί νέο subkey. Ο αλγόριθμος συνεχίζεται με το ίδιο τρόπο. Στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.

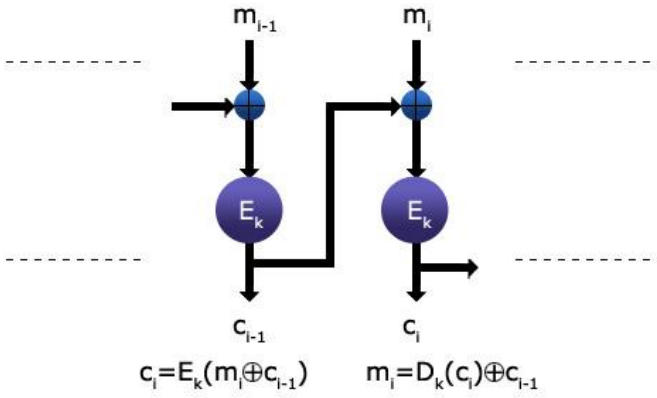
Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση. Τα subkeys χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση. Οι Feistel ciphers καλούνται και DES-like ciphers.

- **Τρόποι Λειτουργίας (Modes of Operation)**

Ένας αλγόριθμος τύπου block cipher έχει διάφορους τρόπους λειτουργίας. Κάθε τρόπος λειτουργίας μπορεί να έχει τις δικές του ιδιότητες εκτός από αυτές που κληρονομεί από τον βασικό cipher. Οι βασικοί τρόποι λειτουργίας είναι: ο Electronic Code Book (ECB), ο Cipher Block Chaining (CBC), ο Cipher Feedback (CFB) και ο Output Feedback (OFB).

Σε ECB mode, το κείμενο χωρίζεται σε ισομήκη block. Κάθε μη κρυπτογραφημένο block κρυπτογραφείται ανεξάρτητα από την συνάρτηση του βασικού block cipher. Μειονέκτημα αυτού του τρόπου είναι ότι ομοιότητες του plaintext δεν καλύπτονται. Τα plaintext block που είναι ταυτόσημα, δίνουν ταυτόσημα ciphertext block και το κείμενο μπορεί εύκολα να τροποποιηθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη των όμοιων ciphertext block. Η ταχύτητα της κρυπτογράφησης κάθε

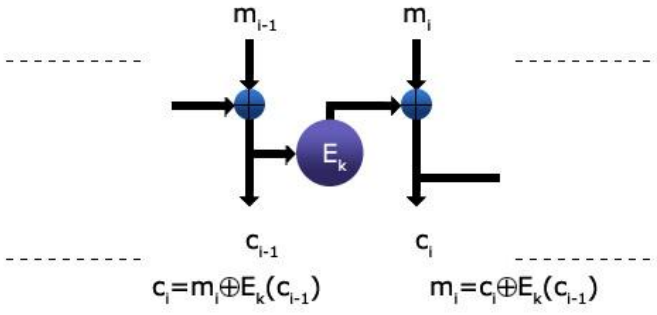
plaintext block είναι ίδια με την ταχύτητα του block cipher. Ο ECB επιτρέπει την παράλληλη παραγωγή των ciphertext blocks για καλύτερη απόδοση.



Εικόνα 6 - Cipher Block Chaining

Σε CBC mode, κάθε μη κρυπτογραφημένο block συνδυάζεται μέσω της λογικής πράξης X-OR με το πρωτύτερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη X-OR πράξη που καλείται Initialization Vector, c_0. Τα όμοια plaintext blocks καλύπτονται με την χρήση της λογικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρ' όλο που η αποκρυπτογράφηση μπορεί.

Σε CFB mode, το προηγούμενο ciphertext block κρυπτογραφείται και το αποτέλεσμα που παράγεται συνδυάζεται με το επόμενο plaintext block με χρήση μιας X-OR. Η έξοδος της X-OR αποτελεί το νέο ciphertext block που θα κρυπτογραφηθεί, συνεχίζοντας την διαδικασία. Γίνεται η ποσότητα που χρησιμοποιείται για ανάδραση (feedback) να μην είναι ένα πλήρες block. Απαιτείται ένας Initialization Vector c_0 για την πρώτη X-OR πράξη.

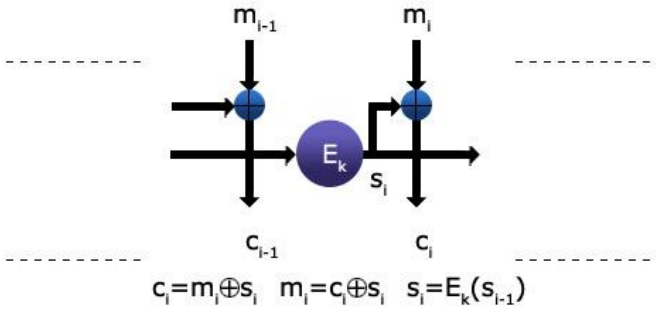


Εικόνα 7 - Cipher Block Chaining

Με αυτόν τον τρόπο καλύπτονται πιθανές ομοιότητες στα plaintext blocks μέσω της X-OR. Γίνεται, όμως, στην πλήρη ανάδραση τα c_i και c_{i-1} να είναι ταυτόσημα. Σαν συνέπεια και το επόμενο ζεύγος κρυπτογραφημένων block θα είναι ταυτόσημα μεταξύ τους. Αυτό το πρόβλημα λύνεται με την χρήση μερικής ανάδρασης. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher και δεν επιτρέπεται παράλληλη επεξεργασία.

Σε OFB mode, η διαδικασία είναι παρόμοια με αυτήν του CFB mode, με την διαφορά ότι η ποσότητα που συνδυάζεται με X-OR με κάθε plaintext block παράγεται ανεξάρτητα από τα plaintext και ciphertext. Ένας Initialization Vector s_0 χρειάζεται για να ξεκινήσει την διαδικασία και κάθε block s_i προκύπτει από την κρυπτογράφηση του προηγούμενου s_{i-1}. Η κρυπτογράφηση plaintext block γίνεται με τον συνδυασμό κάθε plaintext block μέσω μιας X-OR, με το κρυπτογραφημένο s.

Η ανάδραση με block όχι πλήρη δεν συνιστάται για λόγους ασφάλειας. Ο OFB mode έχει το εξής πλεονέκτημα σε σχέση με τον CFB. Τα πιθανά λάθη μετάδοσης δεν πολλαπλασιάζονται κατά την αποκρυπτογράφηση και έτσι δεν την επηρεάζουν. Το κείμενο, όμως, μπορεί εύκολα να αλλοιωθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη όμοιων ciphertext block. Δεν είναι δυνατή η παράλληλη επεξεργασία, αλλά η διαδικασία μπορεί να επιταχυνθεί με την παραγωγή των κρυπτογραφημένων s πριν τα δεδομένα να είναι διαθέσιμα για κρυπτογράφηση.



Εικόνα 8 - Output Feedback Mode

Άλλος ένας τρόπος λειτουργίας είναι ο Propagating Cipher Block Chaining (PCBC). Χρησιμοποιείται με πρωτόκολλα όπως το Kerberos version 4, ενώ δεν έχει επίσημα τυποποιηθεί ούτε χαίρει παγκόσμιας αναγνώρισης. Είναι παρόμοιος με το CBC και έχει σχεδιασθεί με σκοπό να αναπαράγει το πιθανό λάθος μετάδοσης έτσι ώστε να γίνεται αντιληπτό και το κείμενο που προκύπτει να απορρίπτεται.

5.1.2.2. Steam Ciphers

Stream cipher είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχύς αλγόριθμοι, κατά πολύ ταχύτεροι από τους block ciphers. Σε αντίθεση με τους block ciphers που λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks), οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν block cipher θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν stream cipher, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης.

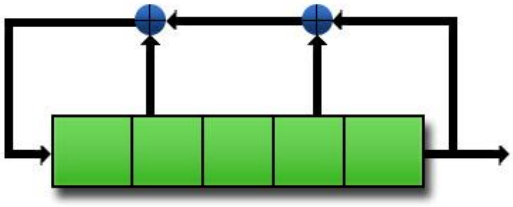
Ένας stream ciphers παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται keystream. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το plaintext, συνήθως μέσω X-OR πράξης. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του plaintext και του ciphertext (synchronous stream cipher) ή μπορεί να εξαρτάται από αυτά (self-synchronizing stream cipher). Οι περισσότεροι stream ciphers είναι synchronous.

5.1.2.3. One-time Pads

Οι stream ciphers βασίζονται στις θεωρητικές ιδιότητες ενός one-time pad. One-time pads (καμιά φορά καλούνται και Vernam ciphers) είναι ciphers που χρησιμοποιούν μια ακολουθία bits (keystream) που παράγεται τελείως στην τύχη. Το keystream είναι του ίδιου μήκους με το μη κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας X-OR πράξης με το αυτό για την παραγωγή του ciphertext. Επειδή του keystream είναι τελείως τυχαίο και είναι του ίδιου μήκους με το plaintext, η εύρεση του κειμένου είναι αδύνατη ακόμα και με την διάθεση τεράστιας υπολογιστικής ισχύς. Ένας τέτοιος cipher προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για την διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με του μήνυμα, εισάγει σημαντικό πρόβλημα στην διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη.

Οι stream ciphers αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Βέβαια δεν είναι σε θέση παρέχουν την θεωρητική ασφάλεια ενός time-pad είναι

τουλάχιστον πρακτικοί. Ο πιο ευρέως χρησιμοποιούμενος stream cipher είναι ο RC4. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα stream cipher όπως για παράδειγμα ο DES σε CFB και OFB modes. Ακόμα και έτσι, οι αυθεντικοί stream ciphers είναι αρκετά ταχύτεροι.



Εικόνα 9 - Linear Feedback Shift Register

Ένας μηχανισμός για την παραγωγή του keystream είναι ο Linear Feedback Shift Register (LFSR). Ο καταχωρητής αποτελείται από μία σειρά κελιών (cells) το καθένα από τα οποία αποτελείται από ένα bit. Τα περιεχόμενα των κελιών καθορίζονται από ένα Initialization Vector που λειτουργεί σαν το μυστικό κλειδί. Το keystream δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους του. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, την στιγμή που το X-OR αποτέλεσμα μερικών από αυτών τοποθετείται στο αριστερότερο κελί. Κάθε αλλαγή του ρολογιού δίνει ένα bit εξόδου.

Η κατασκευή των LFSR είναι εύκολη τόσο υπό μορφή software όσο και υπό μορφή hardware, ενώ η λειτουργία τους είναι ταχύτατη. Οι ακολουθίες bit, όμως, που δημιουργούνται από ένα και μοναδικό LFSR δεν είναι ασφαλής καθ' ότι τον τελευταίο καιρό έχει αναπτυχθεί μια δυνατή μαθηματική φόρμουλα που επιτρέπει την ανάλυση του μηχανισμού και εύρεση του keystream. Απαιτείται, λοιπόν, η συνδυασμένη χρήση πολλών LFSRs.

Ένας συνδυασμός LFSRs είναι ο Shift Register Cascade. Αποτελείται από εάν σύνολο από LFSRs που συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε η συμπεριφορά του ενός να εξαρτάται από την συμπεριφορά του άλλου. Αυτό επιτυγχάνεται συνήθως με την χρήση του ενός LFSR να ελέγχει το ρολόι του άλλου. Άλλο παράδειγμα τέτοιου συνδυασμού είναι ο Shrinking Generator που αναπτύχθηκε από τους Coppersmith, Krawczyk και Mansour. Βασίζεται στην αλληλεπίδραση των

εξόδων δύο LFSRs. Τα bits της μιας εξόδου χρησιμοποιούνται για να καθορίσουν, μέσω κατάλληλης τεχνικής, εάν τα bits της δεύτερης εξόδου θα συμπεριληφθούν στο keystream. Είναι απλός και έχει καλά χαρακτηριστικά ασφαλείας.

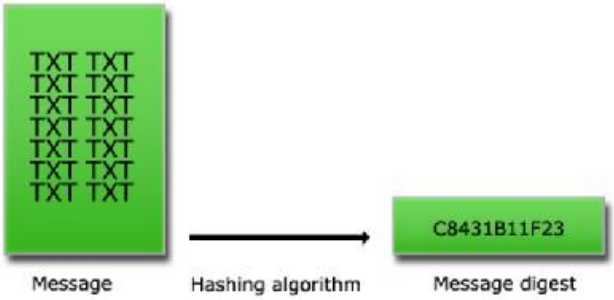
5.1.2.4. Hash Functions

Ο όρος hash function υποδηλώνει ένα μετασχηματισμό που παίρνει σαν είσοδο ένα μήνυμα *m* οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων *h* περιορισμένου μήκους που καλείται hash value, δηλαδή είναι $h = H(m)$. Οι hash functions είναι συναρτήσεις της μορφής $H(x)=y$, με τις εξής ιδιότητες:

- η είσοδος είναι οποιουδήποτε μήκους,
- η έξοδος έχει περιορισμένο μήκος,
- δεδομένου του x, ο υπολογισμός του y είναι εύκολος,
- η $H(x)$ είναι μη αντιστρέψιμη,
- η $H(x)$ είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

Λέγοντας μη αντιστρέψιμη συνάρτηση εννοούμε ότι δεδομένου ενός *y* είναι υπολογιστικά πολύ δύσκολο έως αδύνατο να βρεθεί ο *x*. Λέγοντας αμφιμονοσήμαντη εννοούμε ότι για δύο x_1, x_2 για τα οποία ισχύει ότι x_1, x_2 είναι πάντα $H(x_1),H(x_2)$. Σε καμία περίπτωση θα είναι $H(x_1) = H(x_2)$ όταν x_1, x_2.

Η hash value παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest). Μπορούμε να φανταστούμε την σύνοψη του μηνύματος σαν "ψηφιακό αποτύπωμα" ("digital fingerprint") του εγγράφου. Παραδείγματα γνωστών hash functions είναι οι MD2, MD5 και SHA.

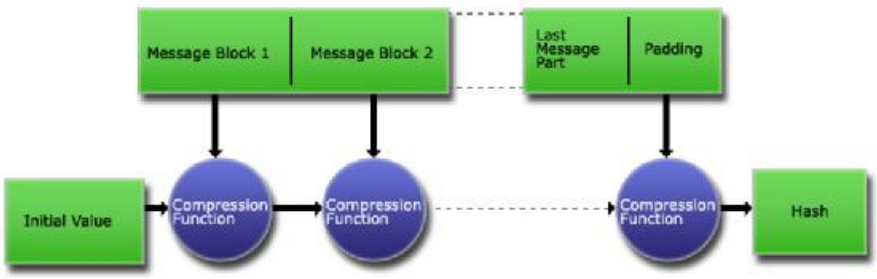


Εικόνα 10 - Hash Functions

Επειδή οι hash functions είναι πιο γρήγοροι από τους αλγόριθμους κρυπτογράφησης και ψηφιακών υπογραφών, συνηθίζεται να παράγεται η υπογραφή των μηνυμάτων

με την εφαρμογή κρυπτογραφικών διαδικασιών στο message digest, το οποίο είναι πιο μικρό και εύκολο στην διαχείριση. Επιπλέον ένα message digest μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου.

Οι Damgard και Merkle εισήγαγαν την έννοια του compression function. Αυτές οι συναρτήσεις παίρνουν είσοδο καθορισμένου μήκους και δίνουν έξοδο μικρότερου, περιορισμένου μήκους. Δεδομένου, λοιπόν, ενός compression function, ένας hash function μπορεί να πραγματοποιηθεί με την επανειλημμένη εφαρμογή του compression function έως ότου ολόκληρο το μήνυμα έχει επεξεργαστεί. Πιο αναλυτικά, το μήνυμα τεμαχίζεται σε blocks, των οποίων το μέγεθος εξαρτάται από τον compression function, και συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block. Το παρακάτω σχήμα επιδεικνύει την λογική της διαδικασίας.



Εικόνα 11 - Hash Functions

5.1.2.5. Message Authentication Code

Message Authentication Code είναι ένας κώδικας (καλείται και checksum) που συνοδεύει το μήνυμα και πιστοποιεί την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος. Για την παραγωγή τους εφαρμόζεται στο μήνυμα ένα από τα προαναφερθέντα κρυπτογραφικά εργαλεία σε συνδυασμό με ένα μυστικό κλειδί. Σε αντίθεση με τις ψηφιακές υπογραφές, τα MACs υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, έτσι ώστε να μπορούν να επαληθευθούν μόνο από τον προοριζόμενο παραλήπτη. Υπάρχουν τέσσερις τύποι MAC: (1) τα άνευ όρων ασφαλή, (2) τα βασιζόμενα σε hash functions, (3) τα βασιζόμενα σε stream ciphers και (4) τα βασιζόμενα σε block ciphers.

I. Οι Simmons και Stinson πρότειναν των άνευ όρων ασφαλή MAC που βασίζεται στην κρυπτογράφηση με ένα one-time pad. Όπως είπαμε, όμως,

επειδή το κλειδί ενός one-time pad είναι πολύ μεγάλο, δεν χρησιμοποιούνται στην πράξη.

II. Τα MACs που βασίζονται σε hash functions χρησιμοποιούν ένα μυστικό κλειδί σε συνδυασμό με ένα hash function για να παράγουν το checksum που συνοδεύει το μήνυμα. Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει το message digest του μηνύματος. Ο παραλήπτης του μηνύματος, που μοιράζεται με τον αποστολέα το ίδιο κλειδί, αποκρυπτογραφεί το message digest και έπειτα το συγκρίνει με ένα message digest που παράγει ο ίδιος από το μήνυμα. Εάν η σύγκριση είναι επιτυχής, τότε ο παραλήπτης σιγουρεύεται ότι τα δεδομένα δεν έχουν αλλοιωθεί. Ένα παράδειγμα είναι ο keyed-MD5.

III. Τα MACs που βασίζονται σε stream ciphers αναπτύχθηκαν από τους Lai, Rueppel και Woolven. Στο αλγόριθμο που ανέπτυξαν, ένας δοκιμασμένος για την ασφάλεια του stream cipher, εφαρμόζεται στα δύο μισά ενός μηνύματος. Τα δύο μισά τροφοδοτούν διαδοχικά το LFSR και η τελική κατάσταση του καταχωρητή αντιπροσωπεύει το checksum. Το μυστικό κλειδί που απαιτείται λειτουργεί σαν το Initialization Vector του LFSR.

IV. Τέλος, τα MAC μπορούν να δημιουργηθούν από block ciphers, όπως τον DES-CBC. Σε αυτήν την μέθοδο, το μήνυμα κρυπτογραφείται με εφαρμογή του αλγόριθμου block cipher. Το τελευταίο ciphertext block που δίνει ο αλγόριθμος αποτελεί το checksum του μηνύματος.

5.1.2.6. Μηχανισμοί Διαχείρισης και Ανταλλαγής Κλειδιών

Οι μηχανισμοί διαχείρισης κλειδιών (key management) και η ανταλλαγής κλειδιών (key exchange), ασχολούνται με την ασφαλή παραγωγή, διανομή και αποθήκευση των κλειδιών κρυπτογράφησης. Η εύρεση απρόσβλητων μεθόδων διαχείρισης και ανταλλαγής κλειδιών είναι πολύ σημαντική στην διατήρηση της ασφάλειας της επικοινωνίας.

Η έννοια της διαχείρισης κλειδιών αναφέρεται στα ασύμμετρα κρυπτοσυστήματα. Τα χαρακτηριστικά που πρέπει να έχει ένας μηχανισμός διαχείρισης κλειδιών είναι τα ακόλουθα. Οι χρήστες πρέπει να είναι σε θέση να μπορούν να αποκτήσουν με ασφάλεια ένα ζεύγος δημόσιας, □ ιδιωτικής κλείδας που θα ικανοποιεί τις ανάγκες τους για προστατευμένη επικοινωνία. Πρέπει να υπάρχει τρόπος αποθήκευσης και δημοσιοποίησης των δημόσιων κλειδιών, ενώ παράλληλα να είναι δυνατή η ανάκτηση τους όποτε χρειάζεται. Επίσης οι δημόσιες κλείδες θα πρέπει να

συσχετίζονται με σίγουρο τρόπο με την ταυτότητα του νόμιμου κατόχου. Έτσι, δεν θα μπορεί κάποιος να παρουσιάζεται σαν κάποιος άλλος, επιδεικνύοντας μία ψεύτικη δημόσια κλείδα. Τέλος οι χρήστες πρέπει να έχουν την δυνατότητα να φυλάσσουν τις ιδιωτικές τους κλείδες με ασφάλεια, οι οποίες θα είναι έγκυρες μόνο για συγκεκριμένο χρονικό διάστημα.

Η ανταλλαγή κλειδιών εφαρμόζεται στα συμμετρικά κρυπτοσυστήματα, όπου οι δύο επικοινωνούντες χρήστες πρέπει να αποφασίσουν για το κοινό μυστικό κλειδί και έπειτα να αποκτήσουν από ένα αντίγραφο αυτού, χωρίς κανένας άλλος να μάθει για αυτό.

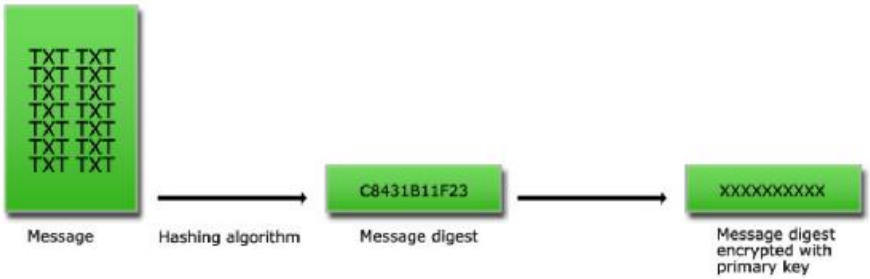
5.1.3. Απλές Εφαρμογές της Κρυπτογραφίας

5.1.3.1. Διαφύλαξη του Απορρήτου και Κρυπτογράφηση

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου (privacy) μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή την ιδιωτική κλείδα που αντιστοιχεί στην δημόσια κλείδα που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση.

Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί να είναι αδύνατη. Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι hash values των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν ακόμα να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

5.1.3.2. Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές



Εικόνα 12 - Κωδικοποίηση μηνύματος

Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει πιστοποίηση ταυτότητας (authentication). Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων (integrity) και την ταυτότητα ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία του αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας hash function και της ιδιωτικής κλείδας του αποστολέα.

Ας δούμε πως λειτουργεί μία ψηφιακή υπογραφή. Έστω δύο χρήστες, ο Α και ο Β. Όταν ο Α θέλει να στείλει ένα υπογεγραμμένο έγγραφο στον Β. Το πρώτο βήμα είναι η παραγωγή του message digest του μηνύματος. Το message digest είναι κατά κανόνα μικρότερο σε μέγεθος από το αρχικό μήνυμα. Στο δεύτερο βήμα, ο Α κρυπτογραφεί το message digest με την ιδιωτική του κλείδα. Τέλος, στέλνει το κρυπτογραφημένο message digest στον Β μαζί με το έγγραφο. Για να μπορέσει ο Β να επαληθεύσει την υπογραφή πρέπει να γνωρίζει την δημόσια κλείδα του Α και τον hash function που χρησιμοποίησε ο Α. Πρώτα θα αποκρυπτογραφήσει το message digest με την δημόσια κλείδα του Α και θα πάρει το message digest που παρήγαγε ο Α. Έπειτα, θα υπολογίσει το message digest του εγγράφου ξανά και θα το συγκρίνει με το παραληφθέν. Εάν τα δύο είναι ταυτόσημα τότε η υπογραφή επαληθεύτηκε επιτυχώς. Εάν δεν ταιριάζουν τότε ή κάποιος προσποιείται ότι είναι ο Α ή το μήνυμα τροποποιήθηκε κατά την μεταφορά του ή προέκυψε λάθος κατά την μετάδοση. Οποιοσδήποτε που γνωρίζει την δημόσια κλείδα του Α, την hash function και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε, μπορεί να επιβεβαιώσει το

γεγονός ότι το μήνυμα προέρχεται από τον Α και ότι δεν αλλοιώθηκε μετά την υπογραφή του.

Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις:

A. η hash function πρέπει να είναι όσο το δυνατόν περισσότερο μη αντιστρέψιμη και
B. τα ζεύγη δημόσιας ιδιωτικής κλείδας να είναι συσχετισμένα με τους νόμιμους κατόχους τους. Για την εξασφάλιση της δεύτερης προϋπόθεσης υπάρχουν ψηφιακά έγγραφα που καλούνται πιστοποιητικά (certificates) και συνδέουν ένα άτομο με μία συγκεκριμένη δημόσια κλείδα.

5.1.4. Μηχανισμοί και Αλγόριθμοι Κρυπτογραφίας

5.1.4.1. Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

- **RSA**

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA.

Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς *p, q* και υπολογίζουμε το γινόμενο τους *n = pq*. Το *n* καλείται *modulus*. Διαλέγουμε ένα αριθμό *e* μικρότερο του *n* και τέτοιο, ώστε *e* και *(p-1)(q-1)* να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό *d*, ώστε *(ed-1)* να διαιρείται από το *(p-1)(q-1)*. Τα ζευγάρια *(n,e)* και *(n,d)* καλούνται δημόσια κλείδα και ιδιωτική κλείδα, αντίστοιχα.

Είναι δύσκολο να βρεθεί η ιδιωτική κλείδα *d* από την δημόσια κλείδα *e*. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού *n*, δηλαδή των αριθμών *p* και *q*. Ο *n* είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το RSA.

Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς των κοινή χρήση ιδιωτικών κλείδων. Ο καθένας χρησιμοποιεί μόνο την δικιά του ιδιωτική κλείδα ή την δημόσια κλείδα οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος της σωστής ιδιωτικής κλείδας μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

- **Κρυπτογράφηση με το RSA**

Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο στον χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: $c = me \bmod n$, όπου (n,e) είναι η δημόσια κλείδα του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: $m = cd \bmod n$, όπου (n,d) η ιδιωτική κλείδα του Β. Η μαθηματική σχέση που το e και το d εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το d, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

- **Ψηφιακές Υπογραφές με το RSA**

Ας υποθέσουμε, τώρα, ότι ο Α θέλει να στείλει μήνυμα στον Β με τέτοιον τρόπο ώστε ο Β να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και δεν έχει μεταβληθεί. Ο Α υπογράφει το έγγραφο ως εξής: $s = md \bmod n$, όπου d και n είναι η ιδιωτική κλείδα του Α. Για να επαληθεύσει την υπογραφή ο Β εκτελεί την πράξη: $m = se \bmod n$, όπου e και n η δημόσια κλείδα του Α.

5.1.4.2. Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

- **DES (Data Encryption Standard)**

DES είναι το ακρωνύμιο των λέξεων Data Encryption Standard. Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος.

Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο

κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

- **Triple-DES**

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

- DES-EEE3 (Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με τρία διαφορετικά κλειδιά.
- DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

- **DESX**

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

- **AES (Advanced Encryption Standard)**

Το ακρωνύμιο AES προέρχεται από την φράση Advanced Encryption Standard. Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να

αντικαταστήσει τον DES. Ο DES βρίσκεται ήδη πολλά χρόνια σε χρήση και από το 1998 το NIST δεν τον ανανεώνει.

- **DSS (Digital Signature Algorithm)**

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί ως επίσημος αλγόριθμος παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α..

Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο. Η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

- **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 πολλές 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.

- **IDEA (International Data Encryption Algorithm)**

Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο σε hardware όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

- **Blowfish**

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. 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 ασφαλής αλγόριθμος.

5.1.4.3. Hash Functions

- **SHA και SHA-1 (Secure Hash Algorithm)**

Ο SHA, όπως και SHA-1, αναπτύχθηκε από το NIST. Ο SHA-1 αποτελεί επανέκδοση του SHA που διόρθωνε μια ατέλεια του τελευταίου. Ο SHA-1 είδε το φως της δημοσιότητας το 1994 και η δομή και λειτουργία του είναι παρόμοια με την αντίστοιχη του MD4 που αναπτύχθηκε από τον Ron Rivest. Είναι και αυτός μέρος του Capstone Project.

Ο SHA-1 παίρνει είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει message digest 160 bits. Είναι ελαφρά πιο αργός από τον MD5, αλλά το μεγαλύτερο message digest που παράγει τον κάνουν πιο ασφαλή απέναντι σε προσπάθειες αντιστροφής του.

- **MD2, MD4, MD5 (Message Digest)**

Όλοι αυτοί οι αλγόριθμοι είναι hash functions που έχουν αναπτυχθεί από τον Ron Rivest. Προορίζονται, κυρίως, για την παραγωγή ψηφιακών υπογραφών. Το μήνυμα πρώτα σμικρύνεται με έναν από αυτούς τους αλγόριθμους και έπειτα, το message digest του μηνύματος κρυπτογραφείται με την ιδιωτική κλείδα του αποστολέα. Και οι τρεις παίρνουν στην είσοδο μήνυμα αυθαίρετου μήκους και δίνουν στην έξοδο ένα message digest 128 bits. Παρ' όλο που η κατασκευή τους μοιάζει αρκετά, ο MD2 είχε σχεδιαστεί για μηχανές 8 bit, σε αντίθεση με τους MD4 και MD5 που προορίζονται για μηχανές 32 bits.

Ο MD2 αναπτύχθηκε το 1989. Το μήνυμα αρχικά συμπληρώνεται με κατάλληλο αριθμό bytes, ώστε το μήκος του σε bytes να είναι διαιρέσιμο από το 16. Ένα αρχικό checksum των 16 bits προστίθεται στο τέλος του μηνύματος και το τελικό message digest παράγεται από το αποτέλεσμα της προηγούμενης ενέργειας. Η κρυπτανάλυση του MD2 έδειξε ότι είναι δυνατόν να υπάρχουν μηνύματα που παράγουν το ίδιο message digest αν και μόνο αν παραλείπεται το βήμα πρόσθεσης του 16-byte checksum.

Ο MD4 αναπτύχθηκε το 1990. Το μήκος του μηνύματος συμπληρώνεται με κατάλληλο αριθμό bits, ώστε το μήκος του σε bits συν 448 να είναι διαιρέσιμο από το 512. Μια δυαδική αναπαράσταση του μηνύματος των 64 bits προστίθεται στο μήνυμα και το αποτέλεσμα επεξεργάζεται με compression function. Τα blocks που

διαχειρίζεται ο compression function έχουν μήκος 512 bits και κάθε block επεξεργάζεται πλήρως σε τρεις διακριτούς επαναληπτικούς γύρους. Ο MD4 έχει επανειλημμένα αναλυθεί με διάφορους τρόπους και δεν πρέπει να θεωρείται πλέον ασφαλής. Συγκεκριμένα, έχει αποδειχθεί ότι μπορεί να αντιστραφεί η διαδικασία και ότι υπό ορισμένες συνθήκες δεν είναι αμφιμονοσήμαντος.

Ο MD5 αναπτύχθηκε το 1991. Είναι μια κατά πολύ βελτιωμένη έκδοση του MD4, γι' αυτό είναι και λίγο πιο αργός. Η μόνη διάφορα είναι η χρήση τεσσάρων επαναλήψεων κατά την επεξεργασία του κάθε block. Οι απαιτήσεις σε μέγεθος block και μήκος μηνύματος παραμένουν οι ίδιες. Η κρυπτανάλυση του MD5 συνεχίζεται ακόμα, αλλά οι πρώτες εκτιμήσεις δείχνουν ότι έχει αρκετές αδυναμίες.

5.1.4.4. 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 $gk = n \bmod p$.

Ας υποθέσουμε τώρα ότι δύο χρήστες, ο Α και ο Β, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο Α παράγει μία τυχαία ιδιωτική τιμή *a* και ο Β μία τυχαία ιδιωτική τιμή *b*. Οι τιμές *a* και *b* διαλέγονται από το σύνολο [*1, p-1*]. Έπειτα δημιουργούν τις δημόσιες τιμές τους χρησιμοποιώντας τις παραμέτρους *p* και *g* και τις ιδιωτικές τους τιμές. Η δημόσια τιμή του Α είναι $ga \bmod p$ και του Β είναι $gb \bmod p$. Στην συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τέλος, ο Α κάνει τον υπολογισμό $gab = (gb)a \bmod p$ και Β κάνει με την σειρά του τον υπολογισμό $gba = (ga)b \bmod p$. Επειδή $gab = gba = k$, ο Α και Β έχουν τώρα ένα κοινό μυστικό κλειδί. Το πρωτόκολλο εξαρτάται από το γεγονός ότι είναι αδύνατον να υπολογιστεί το *κ* από τις δημόσιες τιμές $ga \bmod p$ και $gb \bmod p$ χωρίς την γνώση των *a* και *b* και όταν ο *p* είναι πολύ μεγάλος.

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.

- **Ψηφιακοί Φάκελοι (Digital Envelopes)**

Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί. Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με την δημόσια κλείδα της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

Ας υποθέσουμε ότι ο χρήστης B θέλει να στείλει μήνυμα στον χρήστη B. Ο A διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με την δημόσια κλείδα του B. Στέλνει στον B το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο B θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί την ιδιωτική του κλείδα για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ένος παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με την

δημόσια κλείδα του κάθε παραλήπτη. Και πάλι μεταδίδεται μόνο ένα κρυπτογραφημένο μήνυμα.

Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος συνδυασμός είναι το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

- **Πιστοποιητικά**

Τα πιστοποιητικά είναι ψηφιακά έγγραφα που αποδεικνύουν την σχέση μεταξύ μίας δημόσια κλείδας και μίας οντότητας. Επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι μία συγκεκριμένη δημόσια κλείδα ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικης κλείδας.

Ας υποθέσουμε ότι ο Α χρειάζεται την δημόσια κλείδα του Β για να μπορέσει να εγκαταστήσει μία ασφαλή συναλλαγή. Το να ζητήσει από τον Β να του στείλει την δημόσια κλείδα του μπορεί να θέσει την όλη επικοινωνία σε ρίσκο. Εκτός από την παρακολούθηση της συναλλαγής και αντικατάστασης της δημόσιας κλείδα του Β με την δημόσια κλείδα κάποιου άλλου (επίθεση man-in-the-middle), μπορεί οποιοσδήποτε να ξεγελάσει τον Α, όταν ο Α δεν γνωρίζει και δεν μπορεί να επικοινωνήσει τηλεφωνικός με τον Β, λέγοντας πως είναι ο Β και παρουσιάζοντας μία ψεύτικη δημόσια κλείδα. Δηλαδή, έστω ότι ο Β υποστηρίζει ότι είναι ο πρωθυπουργός της Ελλάδος. Τότε ο Α θα νομίζει ότι συνδιαλέγεται με τον πρωθυπουργό της Ελλάδος και χρησιμοποιεί την δημόσια κλείδα που του παρουσίασε ο Β για να στείλει στον δήθεν πρωθυπουργό εμπιστευτικά έγγραφα.

Ένα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

- το όνομα του κατόχου,
- το όνομα της του εκδοτικού οργανισμού CA,
- την δημόσια κλείδα του ονόματος που αναγράφεται στο πιστοποιητικό,
- την ημερομηνία λήξης του πιστοποιητικού,
- ένα σειριακό αριθμό (serial number),

- την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

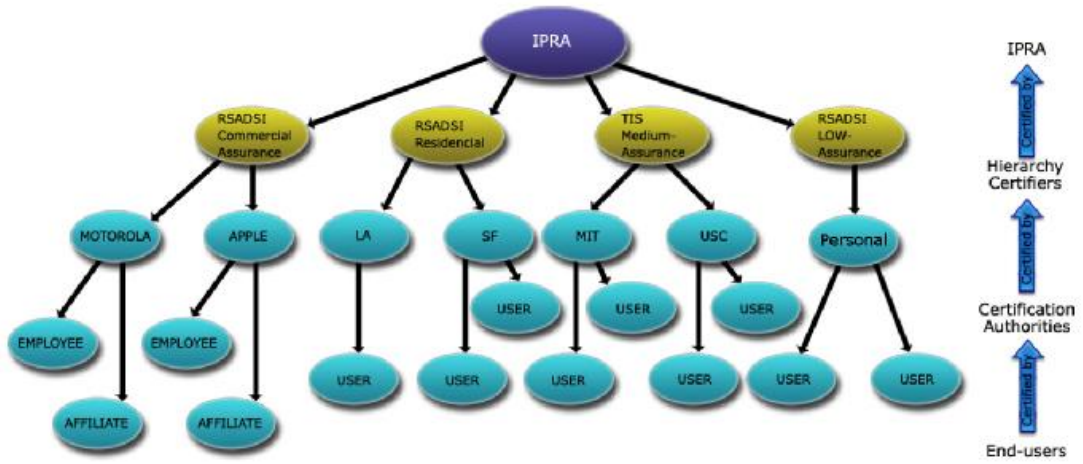
Η τυποποιημένη μορφή ενός πιστοποιητικού ακολουθεί το πρωτόκολλο X.509.

Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής ο παραλήπτης πρέπει να έχει την σωστή δημόσια κλείδα του αποστολέα. Επίσης, το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση της δημόσιας κλείδας κάθε πλευράς στην άλλη πλευρά και για την χρήση της στην κρυπτογράφηση της επικοινωνίας. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

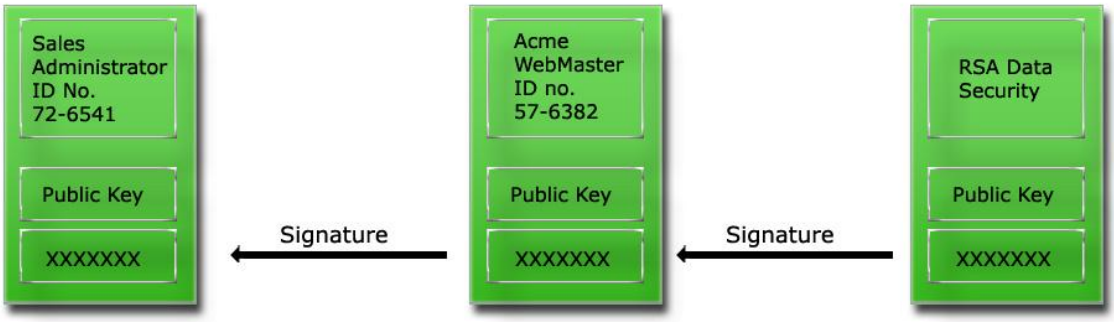
- **Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities)**

Τα πιστοποιητικά εκδίδονται από τις Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities CA), που μπορεί να είναι οποιοσδήποτε άξιος εμπιστοσύνης οργανισμός ικανός να εγγυηθεί για την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά. Ένας οργανισμός μπορεί να εκδίδει πιστοποιητικά για τους υπάλληλους του ή ένα Πανεπιστήμιο για τους σπουδαστές του ή ακόμα και μια πόλη για τους κατοίκους της. Η CA πρέπει να κατέχει ένα ζεύγος ιδιωτικής δημόσιας κλείδας. Με την ιδιωτική της κλείδα υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει, ενώ την εγκυρότητα της δημόσιας κλείδας πρέπει να επικυρώνει εκδοτικός οργανισμός σε υψηλότερη θέση στην ιεραρχία των CAs.

Η ιεραρχική κατάταξη που βλέπουμε στο ακόλουθο σχήμα, έχει στην κορυφή της τον οργανισμό Internet Policy Registration Authority (IPRA)και αμέσως μετά ακολουθούν οι Policy Certification Authorities (PCAs) που δημοσιοποιούν πολιτικές ασφάλισης και έκδοσης πιστοποιητικών. Ανάλογα με το είδος των πιστοποιητικών και περιορισμών που ασκούν όσο αναφορά την χρήση τους, οι Certification Authorities (CAs) που τα εκδίδουν κατατάσσονται σε μία από τις υψηλότερες σε επίπεδο, PCAs. Τέλος, έρχονται οι τελικοί χρήστες που ανάλογα με τις ανάγκες τους επιλέγουν την CA που θα πιστοποιήσει την δημόσια κλείδα τους. Οι ανάγκες κάθε χρήστη καθορίζονται στο αν κλείδα θα χρησιμοποιηθεί για εμπορικές συναλλαγές, για υπογραφή κυβερνητικών εγγράφων, για την απλή ανταλλαγή ηλεκτρονικού ταχυδρομείου ή ακόμα για την διασφάλιση τεχνολογικών επιτευγμάτων.



Εικόνα 13 - Ιεραρχία αρχών έκδοσης ψηφιακών υπογραφών



Εικόνα 14 - Εσωτερική ιεραρχική δομή εταιριών

Σ' αυτήν της ιεραρχία, οι οργανισμοί κάθε επιπέδου πιστοποιούν την δημόσια κλείδα και ταυτότητα του χαμηλότερου επιπέδου. Έτσι, πολλές φορές το πιστοποιητικό για έναν χρήστη μπορεί να συνοδεύεται από μία αλυσίδα πιστοποιητικών (certificates chain) που φθάνουν ως την κορυφή της ιεραρχίας. Σε κάθε πιστοποιητικό περιέχεται η υπογραφή του ανώτερου εκδοτικού οργανισμού που έχει δημιουργηθεί με την ιδιωτική κλείδα αυτού.

Από το σχήμα καταλαβαίνουμε ότι μια τέτοια ιεραρχική δομή μπορεί να εφαρμοστεί και στο εσωτερικό μεγάλων εταιριών. Η δημόσια κλείδα του ανώτερου εκδοτικού οργανισμού δεν μπορεί να πιστοποιηθεί από κανέναν. Ο οργανισμός εκδίδει πιστοποιητικό για τον εαυτό του που περιέχει την δημόσια κλείδα του και την υπογραφή του με την ιδιωτική του κλείδα, το οποίο καλείται root certificate. Αυτονόητο είναι, λοιπόν, ότι αυτός ο οργανισμός πρέπει να είναι απόλυτα έμπιστος.

Ο χρήστης που επιθυμεί να αποκτήσει ένα πιστοποιητικό, θα δημιουργήσει πρώτα ένα ζεύγος ιδιωτικής δημόσιας κλείδας και θα αποστείλει σε μία CA την δημόσια κλείδα μαζί με πληροφορίες που προσδιορίζουν την ταυτότητα του χρήστη. Η CA αφού επαληθεύσει την ταυτότητα του χρήστη και σιγουρευτεί ότι η αίτηση έκδοσης πιστοποιητικού προέρχεται από τον πραγματικό χρήστη, απαντά στον χρήστη με χρήστη το πιστοποιητικό του μαζί με τα ιεραρχικά δεμένα πιστοποιητικά που επιβεβαιώνουν την αυθεντικότητα την δημόσιας κλείδας της CA.

- **Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists)**

Μία λίστα ανάκλησης πιστοποιητικών περιέχει πιστοποιητικά που έχουν ακυρωθεί πριν από την προγραμματισμένη ημερομηνία λήξης. Υπάρχουν αρκετοί λόγοι γιατί ένα πιστοποιητικό μπορεί να ανακληθεί. Για παράδειγμα η κλείδα που ορίζεται στο πιστοποιητικό μπορεί να μην είναι ασφαλής ή το άτομο για το οποίο εκδόθηκε το πιστοποιητικό να μην έχει πια την δικαιοδοσία να το χρησιμοποιεί. Ας φανταστούμε την περίπτωση όπου ένας υπάλληλος μια εταιρείας έχει πιστοποιητικό που έχει εκδώσει για λογαριασμό του η εταιρεία. Εάν ο υπάλληλος απολυθεί, η εταιρεία θα ακυρώσει το πιστοποιητικό, ώστε να μην έχει την δυνατότητα να υπογράφει έγγραφα με αυτήν την κλείδα.

Κατά την επαλήθευση μιας υπογραφής, πρέπει κάθε χρήστης να συμβουλεύεται μία CRL για να διαπιστώσει εάν το εν λόγω πιστοποιητικό δεν έχει αποσυρθεί. Το αν αξίζει τον κόπο να πραγματοποιήσει τέτοιον έλεγχο, εξαρτάται από την σημασία του εγγράφου. Οι λίστες διατηρούνται και ανανεώνονται από τις CA, και κάθε CA διαχειρίζεται τις λίστες που παρέχουν πληροφορίες για τα ανακληθέντα πιστοποιητικά που είχαν εκδοθεί από την ίδια. Επίσης, οι λίστες περιέχουν τα πιστοποιητικά των οποίων δεν έχει περάσει η ημερομηνία λήξης. Αυτά τα πιστοποιητικά δεν γίνονται δεκτά σε καμία περίπτωση.

5.2. Στεγανογραφία

5.2.1. Ιστορική Αναδρομή

Σε όλη τη διαδρομή της ιστορίας ο άνθρωπος συνεχώς ανακάλυπτε νέες μεθόδους που του επέτρεπαν να κρύψει κάποια πολύτιμη πληροφορία. Ένα από τα πρώτα κείμενα που περιγράφουν τη στεγανογραφία έρχεται από τον Ηρόδοτο. Στην αρχαία Ελλάδα τα κείμενα γράφονταν σε πίνακες καλυμμένους με κερί. Σε μια αφήγηση ιστορικού γεγονότος αναφέρεται ότι ο Δημάρατος ήθελε να ειδοποιήσει τη Σπάρτη ότι

ο Ξέρξης προτίθετο να εισβάλει στην Ελλάδα. Για να αποφύγει την κλοπή του μηνύματος έγραψε το μήνυμά του σε ξύλινη πινακίδα, αφού έξυσε το κερί που αυτή είχε και την οποία μετά κάλυψε πάλι με κερί. Οι πινακίδες φαίνονταν λευκές και αχρησιμοποίητες και με αυτό το τρόπο πέρασαν κάθε έλεγχο.

Ακόμα μία μέθοδος ήταν το ξύρισμα του κεφαλιού του αγγελιοφόρου και το γράψιμο του μηνύματος στο κεφάλι του. Όταν πια τα μαλλιά μεγάλωναν αρκετά το μήνυμα δεν φαινόταν έως ότου το κεφάλι ξαναξυριζόταν.

Μια άλλη κοινή μορφή αόρατης γραφής επιτυγχάνεται με τη χρήση αόρατου μελανιού. Τέτοιου είδους μελάνια χρησιμοποιήθηκαν με επιτυχία μέχρι και στο δεύτερο παγκόσμιο πόλεμο. Ένα αθώο κατά τα φαινόμενα γράμμα μπορεί να περιέχει ένα πολύ διαφορετικό μήνυμα γραμμένο ανάμεσα στις γραμμές που φαίνονται. Την εποχή του δευτέρου παγκοσμίου πολέμου η τεχνολογία της στενογραφίας αποτελείτο κυρίως από αόρατα μελάνια. Η προέλευση αυτών των μελανιών είναι το γάλα, διάφορα φρούτα, το ξίδι και τα ούρα. Όλα τα παραπάνω συστατικά σκουραίνουν όταν θερμαίνονται και αυτό τους το χαρακτηριστικό εκμεταλλεύτηκε η κρυπτογραφία της εποχής. Με την ανάπτυξη της τεχνολογίας αναπτύχθηκαν νέα, χημικά, υλικά που κάνανε ακριβώς το ίδιο πράγμα αλλά ήθελαν συγκεκριμένη διαδικασία για να εμφανίσουν αυτά που κρύβανε.

Άλλη μέθοδος είναι αυτή των "Null ciphers" μη κρυπτογραφημένων μηνυμάτων. Υπήρχε τότε, όπως και σήμερα, η τεχνική της ανίχνευσης υπόπτων μηνυμάτων μέσω κάποιων ειδικών φίλτρων μιας αυτοματοποιημένης διαδικασίας. Ωστόσο, τα αθώα μηνύματα πέρναγαν ανενόχλητα. Το μόνο λοιπόν που είχε να κάνει κάποιος που ήθελε να στείλει κάποια κρυφή πληροφορία ήταν να την κάνει να φαίνεται αθώα. Έτσι έγραφε ένα τυχαίο κείμενο στο οποίο η πληροφορία βρισκόταν σε κάθε δεύτερο, για παράδειγμα, γράμμα των λέξεων του κειμένου.

Καθώς, όμως η τεχνολογία συνέχισε να αναπτύσσεται, βρέθηκαν τρόποι διακίνησης μεγαλύτερου όγκου πληροφορίας με ακόμα πιο αόρατο τρόπο. Οι Γερμανοί ανέπτυξαν τη τεχνολογία των μικροτελειών (microdots). Οι μικροτελείες είναι φωτογραφίες υψηλής ανάλυσης και ασήμαντου μεγέθους τελείες. Αυτό το σύστημα χρησιμοποιήθηκε από Γερμανούς κατασκόπους κατά τον δεύτερο παγκόσμιο πόλεμο.

5.2.2. Ορισμός - Ιδιότητες

Όπως καταλαβαίνουμε και από το όνομά της, η στεγανογραφία είναι η τέχνη, που στις μέρες μας έχει εξελιχθεί και σε τεχνική, της επικοινωνίας κατά τρόπο τέτοιο που να κρύβεται η ίδια η ύπαρξη της επικοινωνίας. Σε αντίθεση με τη κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει τη πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Στον παρακάτω πίνακα, που έχει συνταχθεί από τον David Kahn βλέπουμε τις διαφορές της στεγανογραφίας από τη κρυπτογραφία σε σχέση πάντα με τις μεθόδους και τους τύπους που η καθεμία χρησιμοποιεί. Εδώ με τον όρο "ασφάλεια" περιγράφουμε τις μεθόδους προστασίας των πληροφοριών ενώ με τον όρο "ανάκτηση" τις μεθόδους ανάκτησής τους.

Ασφάλεια Σήματος	**Ασφάλεια Ανάκτησης**
Ασφάλεια επικοινωνιών	**Ανάκτηση Επικοινωνιών**
Στεγανογραφία (αόρατα μελάνια, ανοικτοί κώδικες, μηνύματα σε "τρύπια τακούνια") και Ασφάλεια Εκπομπής (συστήματα εκπομπής ευρέως φάσματος)	Παρεμβολή και Ανίχνευση κατεύθυνσης
Κρυπτογραφία	***Κρυπτανάλυση***
Ασφάλεια κίνησης (σιγή ασυρμάτου, "χαζά" μηνύματα)	Ανάλυση κίνησης (ανίχνευση κατεύθυνσης, μελέτη ροής μηνυμάτων και αναγνώριση αποτυπωμάτων ασυρματικών επικοινωνιών)
Ηλεκτρονική Ασφάλεια	**Ηλεκτρονική Ανάκτηση**
Ασφάλεια Εκπομπής (μετατόπιση συχνοτήτων radar, ευρύ φάσμα)	Ηλεκτρονική Αναγέννηση (υποκλοπή εκπομπών radar)
Αντί Αντίμετρα (παρεμβολές radar)	Αντίμετρα (παρεμβολές σε radar και λανθασμένη ηχώ τους)

Ένα καλό στεγανογραφικό σύστημα πρέπει να εκπληρώνει τις προδιαγραφές που έθεσε η "Αρχή του Kerckhoff" στην κρυπτογραφία: *"Η ασφάλεια ενός συστήματος*

πρέπει να βασίζεται στο δεδομένο ότι ο "εχθρός" έχει πλήρη γνώση των σχεδιαστικών λεπτομερειών και της υλοποίησης ενός στεγανογραφικού συστήματος". Η μόνη πληροφορία που λείπει από τον "εχθρό" και που πρέπει να κρατηθεί μυστική από αυτόν είναι ένας μικρός και εύκολα ανταλλάξιμος τυχαίος αριθμός, το μυστικό κλειδί, χωρίς το οποίο δεν μπορεί να γνωρίζει εάν στο κανάλι επικοινωνίας διενεργείται κρυφή επικοινωνία. Η στεγανογραφία σχετίζεται άμεσα με το πρόβλημα των "κρυμμένων καναλιών" στο σχεδιασμό ενός ασφαλούς περιβάλλοντος επικοινωνίας, ένας ορισμός που αναφέρεται σε όλα τα μέσα επικοινωνίας που δεν μπορούν εύκολα να περιοριστούν από μηχανισμούς ελέγχου (π.χ. δύο εφαρμογές-διαδικασίες που επικοινωνούν διαμορφώνοντας και μετρώντας το φόρτο της CPU). Η στεγανογραφία σχετίζεται επιπλέον και με τη τεχνική εκπομπής ευρέως φάσματος η οποία επιτρέπει την λήψη μηνυμάτων που είναι εκατό φορές πιο αδύνατα από τον ατμοσφαιρικό θόρυβο, όπως επίσης και με την τεχνική TEMPEST που αναλύει εκπομπές RF των υπολογιστών και του επικοινωνιακού εξοπλισμού με στόχο την πρόσβαση σε στοιχεία που διακινούνται σε αυτά.

Τα περισσότερα κανάλια επικοινωνιών όπως οι τηλεφωνικές γραμμές και οι εκπομπές ράδιο εκπέμπουν σήματα που συνοδεύονται πάντα από κάποιο θόρυβο. Αυτός ο θόρυβος μπορεί να αντικατασταθεί από κάποιο μυστικό σήμα που έχει τη μορφή θορύβου για κάποιον που δεν γνωρίζει το μυστικό κλειδί.

Αυτή είναι και η βασική σχεδιαστική αρχή των στεγανογραφικών συστημάτων η αντικατάσταση του θορύβου υψηλής εντροπίας από μια εκπομπή υψηλής εντροπίας. Υπάρχουν πολλά προγράμματα που υλοποιούν κάποιου είδους στεγανογραφικό μηχανισμό. Ωστόσο, η πραγματικά καλή εφαρμογή της στεγανογραφίας είναι πολύ δύσκολη υπόθεση και για αυτό το λόγο η ανίχνευση της χρήσης της από μηχανισμούς ανάλυσης αποδίδει όταν πρόκειται για απλή εφαρμογή της. Ο θόρυβος των αναλογικών συστημάτων έχει ένα μεγάλο αριθμό ιδιοτήτων που είναι πολύ χαρακτηριστικές για το κανάλι και τον εξοπλισμό του επικοινωνιακού συστήματος. Ένα καλό στεγανογραφικό σύστημα πρέπει να παρακολουθεί το κανάλι, να χτίζει ένα μοντέλο του θορύβου που είναι παρόν και μετά να προσαρμόζει τις παραμέτρους των δικών του αλγορίθμων έτσι ώστε η αντικατάσταση του θορύβου του καναλιού με τεχνητό θόρυβο, που περιέχει την πληροφορία προς μετάδοση, να είναι επιτυχής. Το κατά πόσο το στεγανογραφικό σύστημα είναι ασφαλές εξαρτάται από τους μηχανισμούς ανάλυσης του θορύβου που έχει στη διάθεσή του ο "εχθρός".

Τα κοινά επικοινωνιακά συστήματα έχουν ένα μεγάλο αριθμό χαρακτηριστικών και μόνο ένα μικρό μέρος από αυτό που φαίνεται σαν θόρυβος μπορεί να αντικατασταθεί από τον στατιστικά πολύ καθαρό θόρυβο που δημιουργεί ένα σύστημα κρυπτογράφησης. Ο θόρυβος στις επικοινωνίες προκαλείται συχνά από τη διαμόρφωση, την κβάντιση και από άλλες διαδικασίες όπως κάθε είδους φίλτρα, συστήματα απαλοιφής της ηχούς, μετατροπείς δεδομένων κ. α..

Εάν κάποιος ήθελε να εξετάσει ένα αρχείο με κρυμμένες πληροφορίες θα μπορούσε να τις βρει. Στη χειρότερη περίπτωση θα μπορούσε να καταλάβει ότι αυτές υπάρχουν έστω και αν δεν τις έβλεπε. Εάν οι κρυμμένες πληροφορίες είναι κρυπτογραφημένες τότε σίγουρα θα φτάσει μέχρι αυτό το σημείο και θα σταματήσει. Ωστόσο εάν δεν είναι κρυπτογραφημένες τότε θα είναι σε θέση να εξετάσει όλο το "κρυμμένο" μήνυμα. Για το λόγο αυτό δεν θα πρέπει να θεωρούμε τη στεγανογραφία σαν αντικαταστάτη της κρυπτογραφίας αλλά σαν συμπλήρωμά της. Η στεγανογραφία γίνεται όλο και πιο σημαντική στο Κυβερνοχώρο εξαιτίας του ότι οι κυβερνήσεις του κόσμου απαγορεύουν τη χρήση κρυπτογράφησης από ιδιώτες, όπως στη Γαλλία και στη Ρωσία αλλά και στην Αμερική όπου υπάρχει ένας σχετικός πόλεμος της κυβέρνησης και του δημιουργού του PGP. Κάνοντας χρήση της στεγανογραφίας μπορούμε να συνεχίσουμε να στέλνουμε κρυπτογραφημένα μηνύματα χωρίς να τα βλέπει κανείς.

Η στεγανογραφία βασίζει την ασφάλειά της στο γεγονός ότι κάποιος δεν μπορεί να ψάξει για κάτι που δεν γνωρίζει εάν υπάρχει. Επιπλέον με όλες τις μετακινήσεις δεδομένων στο Internet, κανείς δεν έχει την απαιτούμενη υπολογιστική ισχύ για να περάσει από ανίχνευση όλες τις εικόνες και τα δεδομένα που διακινούνται.

Επίσης, είναι πολύ πιο εύκολο για έναν ιδιώτη να αρνηθεί την αποστολή ενός κρυπτογραφημένου και κρυμμένου, στεγανογραφικά, μηνύματος από το να το κάνει για ένα απλά κρυπτογραφημένο. Εάν κάποιος κρύψει πληροφορία σε μια εικόνα μπορεί εύκολα να το αρνηθεί λέγοντας ότι *"όπως την πήρα την έστειλα-δεν ήξερα τι είχε μέσα, κάποιος άλλος τα έβαλε"* και είναι πολύ δύσκολο για την αρχή που ψάχνει να αποδείξει το αντίθετο.

Οι παρούσες μέθοδοι παροχής πρακτικών στεγανογραφικών υπηρεσιών έχουν δύο κύριους άξονες κατευθύνσεων. Ο πρώτος, ο οποίος δεν είναι και τόσο αποδοτικός, απογυμνώνει τα κρυπτογραφημένα μηνύματα από οποιαδήποτε πληροφορία που

αναφέρεται στη ταυτότητά τους. Για παράδειγμα το πρόγραμμα Stealth επεξεργάζεται κατά τέτοιο τρόπο τα κρυπτογραφημένα με PGP μηνύματα που φαίνονται σαν σκουπίδια. Το πρόβλημα με αυτή τη μέθοδο είναι ότι η αναγνώριση ενός PGP μηνύματος είναι πολύ εύκολη υπόθεση ακόμα και αν έχουν αφαιρεθεί οι πληροφορίες αναγνώρισής του. Το Stealth μπορεί να παράσχει ασφάλεια κάποιου επιπέδου αλλά δεν μπορεί να αντιμετωπίσει κάποιον αποφασισμένο hacker.

Ο δεύτερος άξονας της στεγανογραφίας είναι η απόκρυψη δεδομένων μέσα σε άλλα αρχεία. Για παράδειγμα μπορούν να χρησιμοποιηθούν τα λιγότερο σημαντικά bits μιας bitmap εικόνας, μέσα στα οποία μπορεί να κρυφτεί η πληροφορία. Η αλλαγή αυτών των bits της εικόνας προκαλεί ανεπαίσθητες αλλαγές στη μορφή της. Χωρίς απευθείας σύγκριση με την αρχική εικόνα είναι πραγματικά αδύνατο να πει κανείς ότι κάτι άλλαξε.

Άλλος ένας τύπος αρχείων που μπορεί να χρησιμοποιηθεί για το κρύψιμο πληροφορίας μέσα του είναι τα ψηφιακά μουσικά αρχεία. Με την εισαγωγή του μηνύματος στα λιγότερο σημαντικά bits ενός μουσικού αρχείου κρύβεται η πληροφορία και ομοίως με τα αρχεία εικόνας δεν έχουμε αισθητές αλλοιώσεις στο τελικό, μουσικό, αποτέλεσμα.

Ένας τελευταίος και λόγω της φύσης του λιγότερο χρησιμοποιούμενος τρόπος, είναι αυτός της απόκρυψης δεδομένων στα μη χρησιμοποιούμενα sectors των δισκετών. Όπως βέβαια αντιλαμβανόμαστε αυτή η μέθοδος δεν μπορεί να χρησιμοποιηθεί σε δικτυακά σχήματα και εδώ απλά γίνεται αναφορά της ύπαρξής της σαν μία επιπλέον δυνατότητα.

5.2.3. Στεγανάλυση

Η στεγανάλυση είναι η τεχνική της ανίχνευσης της κρυμμένης πληροφορίας. Υπάρχουν δύο τύποι επιθέσεων κατά των στεγανογραφικά κρυμμένων μηνυμάτων: η ανίχνευση και η απόσπαση τους. Κάθε εικόνα μπορεί να τροποποιηθεί με στόχο τη καταστροφή κάποιας κρυμμένης πληροφορίας που πιθανόν να υπάρχει μέσα της. Η ανίχνευση της ύπαρξης κρυμμένης πληροφορίας εξοικονομεί χρόνο από τη διαδικασία καταστροφής ή ανάκτησής της αφού αυτή θα γίνεται μόνο όταν η πληροφορία βρεθεί.

Η ορολογία των στεγαναλυτικών τεχνικών είναι παρόμοια με αυτή των τεχνικών κρυπτανάλυσης, υπάρχουν ωστόσο και σημαντικές διαφορές. Ισχύει η παρακάτω, περιγραφική της λειτουργίας του συστήματος, εξίσωση:

μέσο μεταφοράς + μήνυμα + στεγο-κλειδί = στεγο-μέσο

όπου :

- μέσο μεταφοράς, εικόνα, ήχος, κείμενο ή κάποιος άλλος ψηφιακός κώδικας
- μήνυμα η πληροφορία που θέλουμε να κρύψουμε που μαζί με το μέσο μεταφοράς αποτελούν το στεγο-φορέα (stego-carrier)
- στεγο-κλειδί επιπλέον πληροφορία ασφάλειας

Όπως ακριβώς η κρυπτανάλυση εφαρμόζει διάφορες τεχνικές με σκοπό την αποκρυπτογράφηση της πληροφορίας, έτσι και η στεγανάλυση εφαρμόζοντας δικές της τεχνικές αποσκοπεί στην ανίχνευση της κρυμμένης πληροφορίας.

Ο στεγαναλυτής χρησιμοποιεί τεχνικές επίθεσης ανάλογα με το τι είδους πληροφορία έχει στα χέρια του. Μία μορφή επίθεσης είναι η "στεγο-αποκλειστική" (stego-only) όπου υπάρχει διαθέσιμη για ανάλυση μόνο η στεγανογραφικά κρυμμένη πληροφορία. Εάν τόσο η αρχική όσο και η κρυπτογραφημένη πληροφορία είναι διαθέσιμες τότε μιλάμε για επίθεση "γνωστού μέσου" (known cover). Η στεγανάλυση μπορεί να χρησιμοποιήσει επίθεση "γνωστού μέσου" όταν το κρυμμένο μήνυμα αποκαλυφθεί κάποια στιγμή αργότερα και ο στεγαναλυτής θέλει να το αναλύσει για την περίπτωση μελλοντικών επιθέσεων. Ωστόσο ακόμα και όταν το μήνυμα είναι διαθέσιμο η διαδικασία μπορεί να είναι εξίσου πολύπλοκη με αυτήν της "στεγ-αποκλειστικής" επίθεσης. Μια άλλη μορφή επίθεσης είναι η "επιλεκτική στεγο-επίθεση". Σε αυτήν τόσο το εργαλείο (αλγόριθμος) που χρησιμοποιήθηκε για τη στεγανογράφηση όσο και το στεγο-μέσο είναι γνωστά. Μια επίθεση επιλεγμένου μέσου είναι αυτή κατά την οποία ο στεγαναλυτής δημιουργεί το στεγο-μέσο από κάποιο στεγανογραφικό εργαλείο ή αλγόριθμο γνωστού μηνύματος. Ο στόχος μιας τέτοιας επίθεσης είναι ο καθορισμός συγκεκριμένων ιδιοτήτων του στεγο-μέσου που συγκλίνουν στη χρήση κάποιου στεγανογραφικού εργαλείου ή αλγορίθμου.

5.2.4. Τύποι Αρχείων - Στεγανογραφικά Προγράμματα

- **JPG**: Μέχρι στιγμής το μόνο στεγανογραφικό πρόγραμμα που κρύβει δεδομένα σε κωδικοποίηση JPEG είναι το Jpeg-Jsteg.

- **GIF**: Τα καλύτερα εργαλεία για στεγανογράφηση σε GIF μορφή είναι τα S-Tools4. Πρόκειται για ένα πρόγραμμα Windows95/NT το οποίο χρησιμοποιεί την τεχνική drag-and-drop.
- **BMP**: Στη περίπτωση αυτή η δουλειά μπορεί να γίνει με συνδυασμό των S-Tools4 και Hide4PGP.
- **WAV**: Ισχύει ότι και στη περίπτωση των αρχείων BMP.
- **VOC**: Μόνο το Hide4PGP μπορεί να επεξεργαστεί αρχεία φωνής.
- **GZ**: Ο τύπος αυτός αντιστοιχεί σε αρχεία που προκύπτουν από τον αλγόριθμο συμπίεσης του Linux και άλλων UNIX συστημάτων. Το GZ σημαίνει Gnu ZIP ή GZIP. Στα PC τα αρχεία που συμπιέζονται με το GZ διατηρούν τα πρώτα δύο γράμματα της κατάληξής τους και το τρίτο αντικαθίσταται με το γράμμα "z". Για παράδειγμα το αρχείο README.TXT θα γινότανε README.TXZ. Τέλος, το πρόγραμμα που χρησιμοποιείται είναι το GZSteg.
- **TXT**: Το "Texto" είναι ένα πρόγραμμα που παίρνει σαν είσοδο κρυπτογραφημένα με PGP (ASCII) αρχεία και παράγει ένα αρχείο αποτελούμενο από ακατανόητες φράσεις. Το "Snow" είναι ένα πρόγραμμα που κρύβει δεδομένα χρησιμοποιώντας tabs και κενά στο τέλος των γραμμών ενός αρχείου κειμένου.

6. Πρωτόκολλα ασφάλειας

6.1. Secure Shell - SSH

Το SSH είναι ένα σχετικά απλό πρόγραμμα το οποίο μπορεί να χρησιμοποιηθεί για την ασφαλή σύνδεση ενός τερματικού χρήστη με κάποιον απομακρυσμένο διακομιστή, να εκτελεί εντολές σε αυτόν και να μεταφέρει αρχεία από ένα διακομιστή σε έναν άλλο. Το SSH παρέχει ισχυρή αυθεντικοποίηση και ασφαλή επικοινωνία διαμέσου μη ασφαλών διαύλων. Υπάρχουν δύο εκδόσεις του SSH οι οποίες είναι διαθέσιμες σήμερα:

- Μια δημόσια έκδοση, η οποία είναι δωρεάν διαθέσιμη για διάφορα συστήματα UNIX από το 1995 και ο κώδικας, η τεκμηρίωση και τα αρχεία διαμόρφωσης είναι διαθέσιμα στο Internet.
- Μια εμπορική έκδοση, η οποία είναι διαθέσιμη για διάφορα συστήματα UNIX αλλά και για windows 95/NT, OS/2 και MacOS.

Η εμπορική έκδοση είναι εφοδιασμένη με πρόσθετα εργαλεία και χαρακτηριστικά. Για παράδειγμα ο Encrypting Data Dumper (EDD) μπορεί να χρησιμοποιηθεί για να κρυπτογραφεί διαφανώς ροές δεδομένων για την δημιουργία βοηθητικών αντιγράφων ασφαλείας. Επίσης στην εμπορική έκδοση παρέχεται και τεχνική υποστήριξη καθώς και συντήρηση.

Ο τρόπος λειτουργίας του πρωτοκόλλου έχει ως εξής.

- Ο πελάτης (εξυπηρετούμενος), αποστέλλει μια αίτηση αυθεντικοποίησης στον εξυπηρετητή.
- Ο εξυπηρετητής, επιστρέφει στον πελάτη το δικό του δημόσιο host key καθώς και ένα δημόσιο server key το οποίο αλλάζει εξ’ ορισμού κάθε 60 λεπτά. Σκοπός του host key είναι να καθορίζει την σύνδεση με τον επιλεγμένο server και η αλλαγή του server key να καθιστά αδύνατη την αποκρυπτογράφηση καταγεγραμμένης κυκλοφορίας ακόμα και στην περίπτωση που το host key δημοσιευθεί σε τρίτους.
- Στη συνέχεια ο πελάτης συγκρίνει το host key που έλαβε με την βάση δεδομένων του που περιέχει τα δημόσια host keys. Επίσης το αποθηκεύει στην δικιά του βάση δεδομένων αν δεν υπάρχει για μελλοντική χρήση.

- Αν τώρα ο πελάτης αποδεχθεί το host key, παράγει ένα τυχαίο αριθμό που χρησιμεύει ως κλειδί συνόδου (session key). Επιπλέων επιλέγει έναν αλγόριθμο κρυπτογράφησης μεταξύ εκείνων που υποστηρίζονται από τον εξυπηρετητή. Στη συνέχεια συμπληρώνει το κλειδί συνόδου με τυχαία byte, το κρυπτογραφεί διπλά με τα δημόσια server και host keys και αποστέλλει το αποτέλεσμα στον εξυπηρετητή.
- Ο εξυπηρετητής αποκρυπτογραφεί την διπλή κρυπτογράφηση και ανακτά το κλειδί συνόδου. Τώρα και τα δυο μέρη μπορούν να χρησιμοποιούν το κλειδί συνόδου για την κρυπτογράφηση της σύνδεσης. Ο εξυπηρετητής στέλνει μια κρυπτογραφημένη επιβεβαίωση στον πελάτη.
- Η λήψη αυτής της επιβεβαίωσης από τον πελάτη σημαίνει ότι ο εξυπηρετητής αποκρυπτογράφησε σωστά το κλειδί συνόδου και συνεπώς πρέπει να διατηρήσει τα ιδιωτικά του κλειδιά. Οπότε και ο εξυπηρετούμενος θεωρεί αξιόπιστο τον εξυπηρετητή, την κρυπτογράφηση επιπέδου μεταφοράς όσο και την προστασία ακεραιότητας.

Σε συγκεκριμένες περιπτώσεις ίσως απαιτείται και η πιστοποίηση ταυτότητας του χρήστη. Σε αυτή την περίπτωση η αντίστοιχη ανταλλαγή αρχίζει από τον εξυπηρετούμενο ο οποίος αποστέλλει μια αίτηση πιστοποίησης ταυτότητας στον εξυπηρετητή η οποία περιέχει το όνομα χρήστη που πρόκειται να συνδεθεί. Ανάλογα με την μέθοδο αυθεντικοποίησης, διαφοροποιείται ο “διάλογος” μεταξύ πελάτη – εξυπηρετητή.

Υπάρχουν δύο μέθοδοι αυθεντικοποίησης που υποστηρίζονται:

1. Στην περίπτωση της αυθεντικοποίησης με συνθηματικό (password), το συνθηματικό του χρήστη μεταδίδεται κρυπτογραφημένο διαφανώς από το SSH διαμέσου του διαύλου επικοινωνίας.
2. Στην περίπτωση αυθεντικοποίησης με κλειδί, ο εξυπηρετητής προσκαλεί τον πελάτη με ένα τυχαίο αριθμό, ο οποίος είναι κρυπτογραφημένος με το ιδιωτικό κλειδί του χρήστη. Σε αυτή την περίπτωση ο εξυπηρετητής πρέπει να έχει πρόσβαση σε κάποια βάση δεδομένων που θα κάνει την πιστοποίηση. Ο πελάτης μπορεί να αποκρυπτογραφήσει τον τυχαίο αριθμό μόνο αν γνωρίζει το ιδιωτικό κλειδί. Συνεπώς χρειάζεται κωδική φράση (passphrase) η οποία ξεκλειδώνει και αποκαλύπτει προσωρινά το ιδιωτικό κλειδί του χρήστη. Για να

ολοκληρωθεί η αυθεντικοποίηση ο πελάτης πρέπει να στείλει μια ορθή τιμή σύνοψης της αποκρυπτογραφημένης πρόσκλησης και κάποιων πρόσθετων δεδομένων που καθορίζουν την τρέχουσα σύνοδο.

Σε κάθε περίπτωση ο εξυπηρετητής θα πρέπει να ανταποκριθεί με κάποιο μήνυμα επιβεβαίωσης επιτυχημένης ή αποτυχημένης αυθεντικοποίησης.

6.2. Secure Sockets Layer – SSL

Το πρωτόκολλο SSL (Secure Sockets Layer) είναι ένα πρωτόκολλο που υλοποιείται στο επίπεδο μεταφοράς και παρέχει ασφάλεια μέσω συνδέσεων TCP/IP. Το πρωτόκολλο αυτό αναπτύχθηκε από την εταιρία Netscape Communications Corporation και έχει εξελιχθεί σε τρείς εκδόσεις μέχρι σήμερα. Η πρώτη έκδοση του SSL (SSL 1.0) χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της εταιρίας, η δεύτερη (SSL 2.0) ενσωματώθηκε στις εκδόσεις ένα (V.1.0) και δύο (V.2.0) του Netscape Navigator. Σε αυτή την έκδοση καθιερώθηκε και ως de facto πρότυπο για την κρυπτογράφηση της HTTP κυκλοφορίας. Η τρίτη έκδοση του πρωτοκόλλου (SSL 3.0) ήρθε για να καλύψει κάποια κενά της δεύτερης σε θέματα κρυπτογραφικής ασφάλειας αλλά και λειτουργικότητας. Το πρωτόκολλο SSL χρησιμοποιείται σε πολλές εφαρμογές σχετικές με το ηλεκτρονικό ταχυδρομείο, όπως είναι:

Όνομα	Θύρα	Περιγραφή
SSMTP	456	SMTP με υποστήριξη SSL
SPOP3	995	POP3 με υποστήριξη SSL
IMAPS	991	IMAP4 με υποστήριξη SSL

Το πρωτόκολλο SSL χωρίζεται σε δύο υπό-πρωτόκολλα. Το SSL Record Layer, το οποίο παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας των δεδομένων, προστασία από επιθέσεις με επανεκπομπή μηνυμάτων σε μια αξιόπιστη υπηρεσία μεταφοράς όπως το TCP, και το SSL Handshake Layer το οποίο είναι σημαντικότερο στη λειτουργία του καθώς είναι το πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών. Στη συνέχεια θα αναλυθούν περεταίρω.

Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης η οποία παρέχει συνοπτικά τρείς βασικές ιδιότητες:

1. Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.
2. Επιτυγχάνει εμπιστευτικότητα των μεταδιδόμενων δεδομένων μιας και η σύνδεση κρυπτογραφείται διαφανώς μετά την αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
3. Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται για την ακεραιότητα τους κατά την μετάδοση.

Αξίζει να αναφέρουμε ότι το πρωτόκολλο δεν παρέχει προστασία σε επιθέσεις ανάλυσης κυκλοφορίας (traffic analysis). Αν για παράδειγμα ένας αναλυτής κυκλοφορίας εξετάζει τις μη κρυπτογραφημένες IP διευθύνσεις αποστολέα και παραλήπτη και τις TCP θύρες, η παρακολουθεί τον όγκο της ροής των πληροφοριών του δικτύου, μπορεί τελικά να καταγράψει ποια μέρη αλληλεπιδρούν, ποιες υπηρεσίες χρησιμοποιούν και μερικές φορές να ανακτά και πληροφορίες από αυτές που μεταφέρονται. Το θετικό είναι ότι οι επιθέσεις αυτές σε επίπεδο χρηστών θεωρείται σχετικά ακίνδυνη λόγω της φύσης των πληροφοριών που μεταδίδονται.

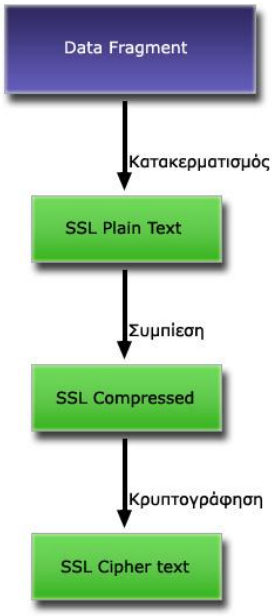
Για την λειτουργία του πρωτοκόλλου θα πρέπει να γνωρίζει τόσο ο εξυπηρετητής όσο και ο εξυπηρετούμενος, ότι η άλλη πλευρά επίσης χρησιμοποιεί SSL. Για να επιτευχθεί αυτό υπάρχουν τρείς δυνατές λύσεις που χρησιμοποιούνται:

1. Η πρώτη είναι να χρησιμοποιηθούν αφιερωμένοι αριθμοί θυρών σε κάθε πρωτόκολλο εφαρμογής που υποστηρίζει SSL.
2. Η δεύτερη είναι να χρησιμοποιηθεί ο κανονικός αριθμός θύρας για κάθε πρωτόκολλο εφαρμογής και να συμφωνούνται οι επιλογές ασφάλειας ως μέρος του πρωτοκόλλου εφαρμογής.
3. Η τρίτη είναι να χρησιμοποιείται μια επιλογή TCP για τη χρήση ενός πρωτοκόλλου ασφάλειας όπως το SSL, κατά τη διάρκεια της πραγματοποίησης της κανονικής TCP/IP σύνδεσης.

Αυτό που χρησιμοποιείται περισσότερο είναι η πρώτη μέθοδος, με τα πρωτόκολλα και τις θύρες που μέρος τους αναφέρονται παραπάνω.

6.2.1. SSL Record Protocol

Το πρωτόκολλο αυτό λαμβάνει δεδομένα από τα πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό τους, τη συμπίεσή τους, την αυθεντικοποίησή τους και την κρυπτογράφηση.



Εικόνα 15 - SSL Record Protocol

Κάθε εγγραφή SSL περιέχει τις ακόλουθες πληροφορίες:

- Τύπο περιεχομένου. Καθορίζει το πρωτόκολλο υψηλότερου επιπέδου που πρέπει να χρησιμοποιείται για την σειριακή επεξεργασία του ωφέλιμου φορτίου δεδομένων.
- Αριθμό έκδοσης πρωτοκόλλου. Ο αριθμός έκδοσης του πρωτοκόλλου SSL. Τυπικά είναι η έκδοση 3.
- Μήκος δεδομένων.
- Ωφέλιμο φορτίο δεδομένων, το οποίο προαιρετικά είναι κρυπτογραφημένο με τον τρέχων αλγόριθμο και συμπιεσμένο με την τρέχουσα μέθοδο συμπίεσης.
- Κώδικα αυθεντικοποίησης μηνύματος. Ο οποίος ουσιαστικά είναι ένας αύξον αριθμός μέσα στο μήνυμα.

6.2.2. SSL Handshake Protocol

Το SSL Handshake Protocol έχει σαν σκοπό να υποχρεώνει έναν εξυπηρετούμενο και έναν εξυπηρετητή να συμφωνούν για τα πρωτόκολλα που θα χρησιμοποιηθούν

κατά τη διάρκεια της επικοινωνίας, τις μεθόδους συμπίεσης και τις προδιαγραφές κρυπτογράφησης. Προαιρετικά γίνεται και αμοιβαία αυθεντικοποίηση, αλλά και δημιουργία ενός κύριου μυστικού κλειδιού (Master secret key), από το οποίο προκύπτουν τα διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων. Μια εφαρμογή του πρωτοκόλλου αυτού, συνήθως αρχίζει με μηνύματα χαιρετισμού ανάμεσα στις πλευρές που επικοινωνούν. Για την έναρξη μιας συνόδου ο εξυπηρετούμενος αποστέλλει ένα μήνυμα CLIENTHELLO στον εξυπηρετητή και αυτός με την σειρά του απαντά με ένα μήνυμα HELLOREQUEST. Το μήνυμα του εξυπηρετούμενου περιλαμβάνει:

- Τον αριθμό της υψηλότερης έκδοσης SSL που μπορεί να υποστηρίξει (συνήθως είναι η έκδοση 3).
- Μια τυχαία δομή που αποτελείται από 32 bit και μια από 28 byte που παράγεται από μια γεννήτρια τυχαίων αριθμών.
- Μια ταυτότητα αναγνώρισης συνόδου που επιθυμεί να χρησιμοποιηθεί για την σύνδεση αυτή.
- Έναν κατάλογο ο οποίος περιέχει τα περιβάλλοντα κρυπτογραφίας που υποστηρίζει.
- Και τέλος έναν κατάλογο με τις μεθόδους συμπίεσης που υποστηρίζει.

Αν ο εξυπηρετούμενος θέλει να ξεκινήσει μια νέα σύνοδο, τότε το πεδίο “ταυτότητα αναγνώρισης” πρέπει να είναι κενό. Σε αντίθετη περίπτωση σημαίνει ότι ο εξυπηρετούμενος επιθυμεί να πραγματοποιηθεί μια σύνοδος με καθορισμένες μεθόδους ασφάλειας οι οποίες προήλθαν από προηγούμενη σύνοδο μεταξύ των δυο μερών. Με την σειρά του ο εξυπηρετητής θα επιλέξει ένα περιβάλλον κρυπτογραφίας από αυτά που υποστηρίζει ο εξυπηρετούμενος, διαφορετικά θα στείλει ένα μήνυμα σφάλματος και θα τερματιστεί η σύνδεση. Από τη στιγμή που ο εξυπηρετούμενος στέλνει το μήνυμα CLIENTHELLO περιμένει ένα μήνυμα SERVERHELLO από τον εξυπηρετητή. Οποιοδήποτε άλλο μήνυμα λάβει εκτός του HELLOREQUEST ή SERVERHELLO αντιμετωπίζεται από τον εξυπηρετούμενο ως σφάλμα.

Το μήνυμα που αποστέλλετε από τον εξυπηρετητή (SERVERHELLO ή HELLOREQUEST) περιλαμβάνει:

- Έναν αριθμό έκδοσης του SSL του εξυπηρετητή, που περιλαμβάνει την χαμηλότερη έκδοση από αυτές που υποστηρίζει ο εξυπηρετούμενος και φαίνονται στο μήνυμα CLIENTHELLO που έχει λάβει και την υψηλότερη που υποστηρίζει ο εξυπηρετητής.
- Μια παραγόμενη από τον εξυπηρετητή τυχαία δομή, αντίστοιχη με αυτή του εξυπηρετούμενου.
- Μια ταυτότητα αναγνώρισης συνόδου που αντιστοιχεί στη συγκεκριμένη σύνδεση.
- Έναν κατάλογο από περιβάλλοντα κρυπτογράφησης ο οποίος επιλέγεται από τη λίστα με τα περιβάλλοντα που υποστηρίζονται από τον εξυπηρετούμενο.
- Την μέθοδο συμπίεσης που επιλέγει ο εξυπηρετητής από τις μεθόδους που υποστηρίζει ο εξυπηρετούμενος.

Αν η ταυτότητα μέσα στο μήνυμα CLIENTHELLO δεν είναι κενή, ο εξυπηρετητής ψάχνει στην δική του κρυφή μνήμη συνόδου την τιμή της ταυτότητας και αν βρεθεί κάποια αντίστοιχη τότε είναι έτοιμος να καθιερώσει μια νέα σύνοδο και απαντά στον εξυπηρετούμενο με την ίδια τιμή που έλαβε. Οπότε και προχωράνε στο “κλείσιμο” της συμφωνίας για την σύνοδο με τα μηνύματα CHANGECIPHERSPEC και FINISHED. Σε διαφορετική περίπτωση αποστέλλεται μέσα σε αυτό το πεδίο μια διαφορετική τιμή η οποία προσδιορίζει την νέα σύνοδο. Επίσης υπάρχει και η επιλογή να παραμείνει κενό αυτό το πεδίο κάτι το οποίο σημαίνει πως δεν θα γίνει αποθήκευση στην κρυφή μνήμη του εξυπηρετητή, οπότε και δεν θα μπορεί να συνεχιστεί αργότερα η σύνοδος. Ο εξυπηρετητής μπορεί να στέλνει και άλλα μηνύματα στον εξυπηρετούμενο, όπως για παράδειγμα αν θέλει να αυθεντικοποιηθεί, στέλνει ένα μήνυμα CERTIFICATE το οποίο περιέχει το πιστοποιητικό. Στην περίπτωση αυτή, ο εξυπηρετούμενος θα στείλει ένα μήνυμα CERTIFICATEVERIFY το οποίο θα επιβεβαιώνει ότι υποστηρίζεται το συγκεκριμένο πιστοποιητικό από τον ίδιο. Η ολοκλήρωση του πρωτοκόλλου SSL Handshake Protocol γίνεται με τον εξυπηρετητή να στέλνει ένα μήνυμα CHANGECIPHERSPEC και ένα αντίστοιχο FINISHED στον εξυπηρετούμενο.

Με την ολοκλήρωση της SSL χειραψίας, καθιερώνεται μια ασφαλής σύνδεση μεταξύ εξυπηρετητή και εξυπηρετούμενου, η οποία είναι διαθέσιμη να χρησιμοποιηθεί για μετάδοση δεδομένων εφαρμογών τα οποία ενθυλακώνονται στο SSL Record Protocol.

6.3. Πρότυπο MIME και S/MIME

6.3.1. MIME

Η ηλεκτρονική αλληλογραφία αρχικά έδινε την δυνατότητα στους χρήστες να μεταδίδουν μηνύματα τα οποία περιείχαν μόνο κείμενο σε χαρακτήρες ASCII 7-bit, κάτι το οποίο σημαίνει μόνο αγγλικούς χαρακτήρες. Η εξάπλωση του ηλεκτρονικού ταχυδρομείου έφερε την ανάγκη να μπορούν να μεταδίδονται και άλλες πληροφορίες μέσω αυτού, όπως προγράμματα, εικόνες, ήχος, βίντεο, οι οποίες με κάποιο τρόπο θα μπορούσαν να μετατραπούν από την μορφή που βρίσκονται σε μορφή κατάλληλη για την αποστολή τους. Για να γίνει αυτό επινοήθηκαν διάφορες μέθοδοι οι οποίες μετέτρεπαν τα δυαδικά δεδομένα σε κείμενο το οποίο εύκολα μεταφερόταν μέσω ηλεκτρονικού ταχυδρομείου. Μία από αυτές τις μεθόδους για παράδειγμα χρησιμοποιούσε μια δεκαεξαδική αναπαράσταση. Τα δυαδικά δεδομένα διαιρούνται σε μονάδες των τεσσάρων bit, κάθε μια από τις οποίες κωδικοποιείται σε έναν από τους δεκαέξι χαρακτήρες (0 έως 9 και A μέχρι F). Στη συνέχεια μεταφέρετε η πληροφορία μέσω ηλεκτρονικού ταχυδρομείου και ο παραλήπτης πρέπει να κάνει την αποκωδικοποίηση για να δει το περιεχόμενο του μηνύματος. Για να γίνει ευκολότερη η μετάδοση τέτοιων μηνυμάτων η IETF (Internet Engineering Task Force) δημιούργησε το πρότυπο MIME (Multipurpose Internet Mail Extensions), το οποίο δεν υποδείκνυε έναν συγκεκριμένο τρόπο για την κωδικοποίηση – αποκωδικοποίηση των μηνυμάτων, αλλά επέτρεπε στους χρήστες να επιλέγουν αυτοί ποια κωδικοποίηση θα χρησιμοποιούν ανάλογα με το περιεχόμενο του μηνύματος. Όταν χρησιμοποιείται το MIME, ο αποστολέας συμπεριλαμβάνει στην κεφαλίδα πρόσθετες γραμμές πληροφορίας που καθορίζουν ότι το μήνυμα που ακολουθεί είναι MIME, όπως και πρόσθετες πληροφορίες στον κορμό του μηνύματος που προσδιορίζουν τον τύπο των δεδομένων αλλά και την κωδικοποίηση που έχει χρησιμοποιηθεί.

Για να επιτευχθεί η σωστή κωδικοποίηση – αποκωδικοποίηση του μηνύματος, το MIME προσθέτει δυο γραμμές στην κεφαλίδα του μηνύματος, μία που δηλώνει ότι χρησιμοποιήθηκε το MIME για το μήνυμα, και άλλη μια που καθορίζει το περιεχόμενο του μηνύματος. Τον κορμό δηλαδή. Για παράδειγμα μια κεφαλίδα μπορεί να έχει την εξής μορφή:

```
MIME-Version: 1.0
Content-Type: Multipart/Mixed; Boundary= Mine_seperator
```

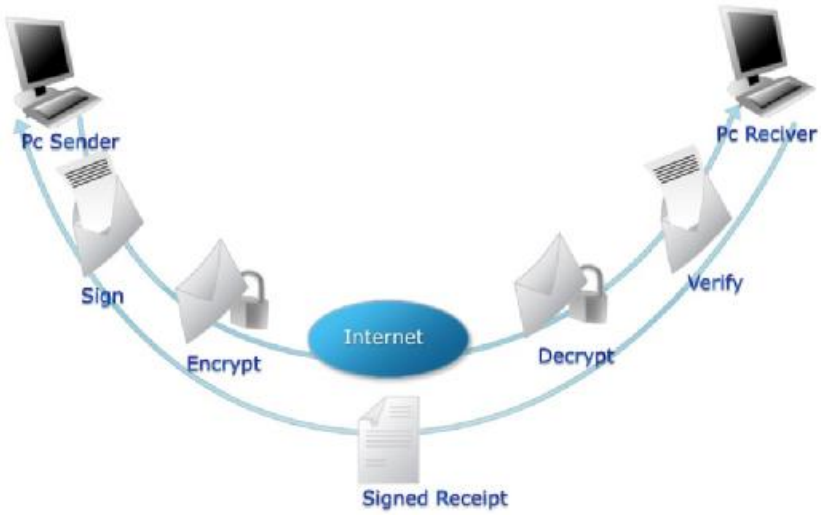
Όπως βλέπουμε, ορίζεται πως έχει χρησιμοποιηθεί η πρώτη έκδοση του MIME και θα εμφανίζεται στον κορμό μια γραμμή που θα περιέχει την φράση ”Mine_seperator” (διαχωριστικό MIME) πριν από κάθε μέρος του μηνύματος. Στην περίπτωση που το μήνυμα περιέχει απλό κείμενο τότε η δεύτερη γραμμή θα είναι:

```
Content-Type: text/plain
```

Συνοψίζοντας, το σημαντικότερο πλεονέκτημα του προτύπου MIME, είναι η ευελιξία του, καθώς το πρότυπο δεν ορίζει συγκεκριμένο τρόπο κωδικοποίησης, αλλά αφήνει την δυνατότητα στους χρήστες να επιλέγουν την κωδικοποίηση που τους βολεύει καλύτερα, αρκεί να ενημερώνεται ο παραλήπτης από τον αποστολέα για αυτή. Επίσης δεν ορίζεται κάποια συγκεκριμένη τιμή που θα χρησιμοποιηθεί για τον διαχωρισμό των μερών του μηνύματος αλλά θα πρέπει αν είναι μια φράση η οποία δεν περιέχετε στον κορμό του μηνύματος. Τέλος, το MIME είναι συμβατό με παλαιότερα συστήματα ηλεκτρονικού ταχυδρομείου, τα οποία αν λάβουν ένα μήνυμα τύπου MIME μεταφέρουν το μήνυμα χωρίς να ερμηνεύουν τις πρόσθετες γραμμές της επικεφαλίδας και αντιμετωπίζουν τον κορμό σαν απλό κείμενο.

6.3.2. S/MIME

Το πρότυπο S/MIME (Secure MIME) αποτελεί μια προέκταση του προτύπου MIME, το οποίο περιγράφει μια ασφαλή μέθοδο για την αποστολή των ηλεκτρονικών μηνυμάτων με την χρήση πιστοποιητικών, ψηφιακών υπογραφών και ψηφιακών φακέλων για την εξασφάλιση της αυθεντικότητας του αποστολέα. Στην περίπτωση που η αυθεντικότητα εξασφαλίζεται με πιστοποιητικά, γίνεται χρήση πιστοποιητικών της μορφής X.509 τα οποία περιλαμβάνουν έναν αριθμό έκδοσης, έναν σειριακό αριθμό, πληροφορίες ταυτότητας, πληροφορίες σχετικά με τον αλγόριθμο της κρυπτογράφησης και την υπογραφή της αρχής που το εκδίδει. Αν γίνεται χρήση ψηφιακών υπογραφών, είναι απαραίτητη η ύπαρξη ενός τουλάχιστον αλγόριθμου σύνοψης και ενός αλγορίθμου δημοσίου κλειδιού.



Εικόνα 16 - Κύκλος S/MIME μηνύματος

Από την μεριά του αποστολέα του μηνύματος η διαδικασία υπογραφής ενός MIME γίνεται ως εξής:

- Αρχικά ο αποστολέας κάνει χρήση μιας συνάρτησης για την δημιουργία της σύναψης του μηνύματος,
- Στη συνέχεια κρυπτογραφεί την σύνοψη που έχει είδη φτιάξει, χρησιμοποιώντας ένα από τα ιδιωτικά κλειδιά. Αυτό έχει σαν αποτέλεσμα την δημιουργία της ψηφιακής υπογραφής του μηνύματος MIME.
- Έπειτα προετοιμάζει ένα σύνολο πληροφοριών αποστολέα, που περιέχει το πιστοποιητικό με το δημόσιο κλειδί και έναν προσδιοριστή του αλγορίθμου σύνοψης που χρησιμοποιήθηκε για την δημιουργία της ψηφιακής υπογραφής.
- Το μήνυμα MIME και το παραπάνω σύνολο πληροφοριών συγχωνεύονται και αποτελούν ένα κρυπτογραφημένο – υπογεγραμμένο μήνυμα (CMS, Cryptographic Message Syntax).
- Το CMS περιγράφει μια μέθοδο ενθυλάκωσης για την κρυπτογραφική προστασία των MIME μηνυμάτων.

Στην μεριά του παραλήπτη για την ανάγνωση του μηνύματος, εκτελούνται οι εξής ενέργειες:

- Αρχικά γίνεται αποκρυπτογράφηση της ψηφιακής υπογραφής με την χρήση του κατάλληλου δημοσίου κλειδιού που έχει χρησιμοποιήσει ο αποστολέας και βρίσκεται στο σύνολο πληροφοριών που αναφέραμε πιο πάνω, για να αποκαλυφθεί η σύνοψη του αρχικού μηνύματος

- Στη συνέχεια δημιουργεί μια νέα σύνοψη του μηνύματος και συγκρίνεται με αυτή που παρέλαβε. Η αυθεντικοποίηση γίνεται αν οι συνόψεις ταυτίζονται, οπότε και το μήνυμα είναι αυθεντικό.

Αν η κρυπτογράφηση γίνεται με ψηφιακούς φακέλους, τότε, ο αποστολέας δημιουργεί μια τυχαία τιμή η οποία θα χρησιμοποιηθεί από τον αλγόριθμο κρυπτογράφησης ως συμμετρικό κλειδί και γίνεται κρυπτογράφηση του μηνύματος MIME με την χρήση αυτού του κλειδιού. Στη συνέχεια κρυπτογραφείται το συμμετρικό κλειδί με το δημόσιο κλειδί του παραλήπτη. Για κάθε παραλήπτη δημιουργείται ένα σύνολο πληροφοριών που περιλαμβάνουν το πιστοποιητικό με το δημόσιο κλειδί του αποστολέα, έναν προσδιοριστή του αλγορίθμου κρυπτογράφησης που χρησιμοποιήθηκε για την κρυπτογράφηση του συμμετρικού κλειδιού και το κρυπτογραφημένο συμμετρικό κλειδί. Όπως και στην περίπτωση των ψηφιακών υπογραφών, το κρυπτογραφημένο μήνυμα MIME και το σύνολο των πληροφοριών συνενώνονται για να αποτελέσουν ένα CMS μήνυμα.

Για να αναγνώσει τώρα ο παραλήπτης, αρχικά αποκρυπτογραφεί το σύνολο πληροφοριών που έλαβε χρησιμοποιώντας το ιδιωτικό του κλειδί και στη συνέχεια αποκρυπτογραφεί το περιεχόμενο του αρχικού μηνύματος χρησιμοποιώντας το συμμετρικό κλειδί που δημιουργήθηκε αρχικά.

6.4. PGP (Pretty Good Privacy)

6.4.1. Εισαγωγή

Το λογισμικό Pretty Good Privacy (PGP), το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες. Το PGP επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

Διασφάλιση του απορρήτου σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει.

Πιστοποίηση της ταυτότητας σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.

Ευκολία σημαίνει ότι η διασφάλιση του απόρρητου και η πιστοποίησης της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία. Δεν είναι αναγκαία ασφαλή κανάλια για την ανταλλαγή κλειδιών μεταξύ χρηστών κάτι που κάνει το PGP πολύ ευκολότερο στη χρήση από κάθε άλλο αντίστοιχο πακέτο. Αυτό συμβαίνει διότι το PGP είναι βασισμένο σε μια δυναμική νέα τεχνολογία που καλείται κρυπτογράφηση "δημοσίων κλειδιών" (public key).

Το PGP συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με:

- την ταχύτητα της συμβατικής κρυπτογράφησης
- περιλήψεις μηνυμάτων για ψηφιακές υπογραφές
- συμπίεση δεδομένων πριν την κρυπτογράφηση
- καλός εργονομικός σχεδιασμός
- και υψηλού επιπέδου διαχείριση κλειδιών

Επιπλέον το PGP εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες.

Σήμερα εάν η κυβέρνηση θελήσει να παραβιάσει το απόρρητο των πολιτών πρέπει να καταβάλλει ένα συγκεκριμένο ποσό χρημάτων και εργασίας για να υποκλέψει και να διαβάσει το συμβατικό ταχυδρομείο και να ακούσει ή να υποκλέψει τηλεφωνικές συνομιλίες. Αυτός ο τρόπος της παρακολούθησης δεν είναι πρακτικός σε μεγάλο επίπεδο. Αυτό συμβαίνει μόνο σε σημαντικές περιπτώσεις όπου φαίνεται ότι αξίζει.

Όλο και μεγαλύτερο ποσοστό από τις ιδιωτικές μας επικοινωνίες δρομολογείται μέσω ηλεκτρονικών καναλιών. Το ηλεκτρονικό ταχυδρομείο σταδιακά αντικαθιστά το συμβατικό ταχυδρομείο. Τα e-mail είναι πολύ εύκολο να υποκλαπούν και να περάσουν από διαδικασία ανίχνευσης βάσει καθορισμένων λέξεων-κλειδιών (keywords). Αυτό μπορεί να γίνει εύκολα, αυτόματα και χωρίς να πέσει στην αντίληψη κανενός σε μεγάλο επίπεδο. Οι διεθνείς συνδέσεις βρίσκονται ήδη κάτω από μια τέτοια διαδικασία παρακολούθησης από την NSA.

6.4.2. Λειτουργία του PGP

Για να κατανοήσουμε τη λειτουργία του PGP θα πρέπει να αναφέρουμε λίγα λόγια πάνω στην ορολογία που χρησιμοποιείται. Ας θεωρήσουμε ότι θέλει κάποιος να στείλει ένα μήνυμα αλλά δεν θέλει να το διαβάσει κανένας άλλος εκτός από τον παραλήπτη. Μπορεί να το κρυπτογραφήσει με τη χρήση ενός κλειδιού το οποίο θα πρέπει να χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος από τον παραλήπτη του, τουλάχιστον έτσι δουλεύει η συμβατική κρυπτογραφία ενός κλειδιού.

Στα συμβατικά κρυπτοσυστήματα, όπως το DES, ένα και μόνο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό σημαίνει ότι το κλειδί θα πρέπει να μεταδοθεί αρχικά μέσα από ένα ασφαλές κανάλι έτσι ώστε και τα δυο μέρη να το γνωρίζουν προτού αρχίσει η αποστολή κρυπτογραφημένων μηνυμάτων μέσω ασφαλών καναλιών. Αυτό δεν είναι και τόσο βολικό διότι αν έχεις ένα ασφαλές κανάλι για να ανταλλάζεις κλειδιά τότε τι χρειάζεσαι την κρυπτογραφία;

Στα κρυπτοσυστήματα δημοσίων κλειδιών ο καθένας έχει δυο συμπληρωματικά κλειδιά. Ένα που δίδεται δημόσια (public key) και ένα μυστικό (secret key ή private key). Το κάθε κλειδί ξεκλειδώνει τον κώδικα που το άλλο φτιάχνει. Η γνώση του δημοσίου κλειδιού δεν βοηθάει στην εξαγωγή του αντίστοιχου μυστικού κλειδιού. Το δημόσιο κλειδί μπορεί να διατεθεί σε ένα δίκτυο επικοινωνιών. Αυτό το πρωτόκολλο παρέχει διασφάλιση του απόρρητου χωρίς την ανάγκη ύπαρξης ασφαλών καναλιών, όπως απαιτεί η συμβατική κρυπτογραφία.

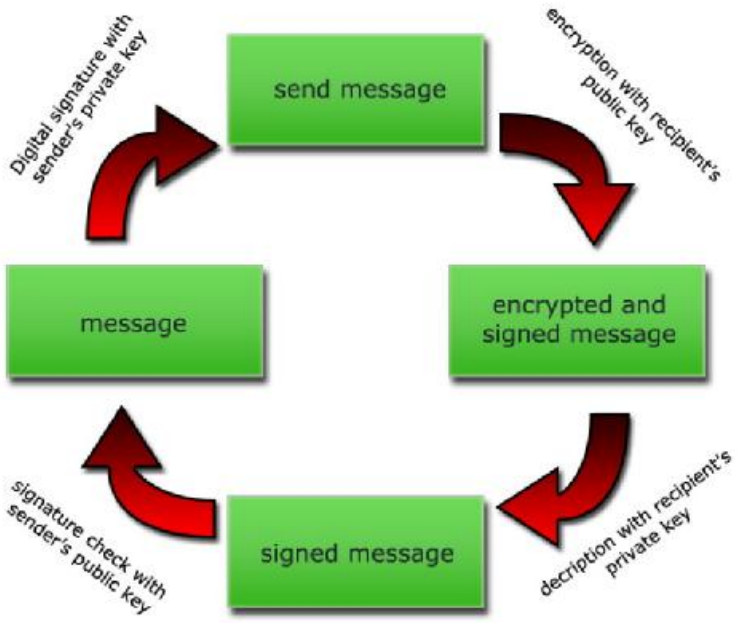
Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη ενός μηνύματος για να κρυπτογραφήσει ένα μήνυμα προς αυτό το άτομο ενώ ο παραλήπτης μπορεί να χρησιμοποιήσει με τη σειρά του το αντίστοιχο μυστικό κλειδί για να αποκρυπτογραφήσει το μήνυμα. Κανένας άλλος εκτός από τον παραλήπτη δεν μπορεί να το αποκρυπτογραφήσει διότι κανένας άλλος δεν έχει πρόσβαση στο μυστικό κλειδί - ακόμη και το άτομο που κρυπτογράφησε το μήνυμα.

Επίσης παρέχεται υπηρεσία πιστοποίησης του μηνύματος. Το μυστικό κλειδί του αποστολέα μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος άρα και για την υπογραφή του. Έτσι δημιουργείται μια ψηφιακή υπογραφή του μηνύματος την οποία ο παραλήπτης ή οποιοσδήποτε άλλος μπορεί να ελέγξει χρησιμοποιώντας

το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει. Αυτό αποδεικνύει ότι ο αποστολέας ήταν ο πραγματικός δημιουργός του μηνύματος και ότι το μήνυμα δεν αλλοιώθηκε από κάποιον άλλον διότι μόνο ο αποστολέας έχει στην κατοχή του το μυστικό κλειδί που έφτιαξε την υπογραφή. Η πλαστογράφηση ενός υπογεγραμμένου μηνύματος δεν είναι εφικτή και ο αποστολέας δεν μπορεί μετά να απαρνηθεί την υπογραφή του.

Αυτές οι δυο διαδικασίες μπορούν να συνδυαστούν για την παροχή τόσο διασφάλισης του απόρρητου όσο και πιστοποίησης της ταυτότητας αφού μπορεί κάποιος πρώτα να υπογράψει ένα μήνυμα με το μυστικό κλειδί του και μετά να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αντιστρέφει αυτά τα βήματα αποκρυπτογραφώντας πρώτα το μήνυμα με το μυστικό κλειδί του και κατόπιν ελέγχοντας την ψηφιακή υπογραφή που περιέχεται σε αυτό με το δημόσιο κλειδί του αποστολέα. Αυτές οι διαδικασίες γίνονται αυτόματα από το λογισμικό του παραλήπτη.

Επειδή ο αλγόριθμος της κρυπτογράφησης δημοσίων κλειδιών είναι πολύ πιο αργός από τη συμβατική κρυπτογράφηση ενός κλειδιού η κρυπτογράφηση επιτυγχάνεται καλύτερα με τη χρήση ενός υψηλής ποιότητας γρήγορου αλγόριθμου συμβατικής κρυπτογράφησης δηλαδή ενός κλειδιού για την κρυπτογράφηση του μηνύματος. Το αρχικό μη κρυπτογραφημένο μήνυμα καλείται "απλό κείμενο". Σε μια διαδικασία αόρατη στο χρήστη ένα προσωρινό τυχαίο κλειδί, το οποίο έχει δημιουργηθεί μόνο για τη συγκεκριμένη φορά, χρησιμοποιείται για να κρυπτογραφηθεί συμβατικά το αρχείο "απλό κείμενο". Μετά το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για να κρυπτογραφηθεί αυτό το προσωρινό κλειδί. Αυτό το συμβατικά δημιουργημένο κλειδί μιας φοράς (session key) το οποίο έχει κρυπτογραφηθεί και με τη διαδικασία του δημόσιου κλειδιού αποστέλλεται μαζί με το κρυπτογραφημένο κείμενο (κρυπτοκείμενο) στον παραλήπτη. Ο παραλήπτης χρησιμοποιεί το δικό του μυστικό κλειδί για να ανακτήσει το session key και μετά χρησιμοποιεί αυτό το κλειδί για να τρέξει τον γρήγορο συμβατικό αλγόριθμο ενός κλειδιού έτσι ώστε να αποκρυπτογραφήσει το κρυπτοκείμενο. Η όλη διαδικασία φαίνεται στο παρακάτω σχήμα:



Εικόνα 17 - Διαδικασία κρυπτογράφησης/αποκρυπτογράφησης με το PGP

Τα δημόσια κλειδιά φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών (key certificates) τα οποία περιλαμβάνουν:

- την ταυτότητα του ιδιοκτήτη τους (το όνομα του ιδιοκτήτη)
- μια σφραγίδα χρόνου που δείχνει πότε το ζεύγος των κλειδιών δημιουργήθηκε
- και τέλος το ίδιο το υλικό του κλειδιού.

Τα πιστοποιητικά δημοσίων κλειδιών περιλαμβάνουν το υλικό των δημοσίων κλειδιών ενώ τα πιστοποιητικά των μυστικών κλειδιών περιλαμβάνουν το υλικό των μυστικών κλειδιών. Κάθε μυστικό κλειδί κρυπτογραφείται επιπλέον με τον κωδικό του σε περίπτωση που κλαπεί. Ένα αρχείο κλειδιών ή ένα μπρελόκ κλειδιών (key ring) περιέχει ένα ή περισσότερα από αυτά τα πιστοποιητικά κλειδιών. Τα δημόσια μπρελόκ περιέχουν τα δημόσια πιστοποιητικά κλειδιών ενώ τα ιδιωτικά μπρελόκ περιέχουν τα ιδιωτικά πιστοποιητικά κλειδιά.

Τα κλειδιά χαρακτηρίζονται από ένα "key id" (ταυτότητα κλειδιού) η οποία είναι μια συντομογραφία του δημόσιου κλειδιού (τα 64 λιγότερο σημαντικά bits του δημοσίου κλειδιού). Όταν αυτή η ταυτότητα παρουσιάζεται μόνο τα 32 λιγότερο σημαντικά bits δίνονται για επιπλέον ελαχιστοποίηση του όγκου της ταυτότητας. Καθώς πολλά κλειδιά μπορεί να μοιράζονται το ίδιο user id (ταυτότητα χρήστη), για πρακτικούς λόγους κανένα κλειδί δεν μοιράζεται το ίδιο key id με κανένα άλλο.

Το PGP χρησιμοποιεί τις περιλήψεις μηνυμάτων (message digests) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολύ δυνατή μονόδρομη (hash) συνάρτηση 128 bit του μηνύματος. Είναι κάτι ανάλογο με το "check sum" ή CRC κώδικα ελέγχου στο ότι αντιπροσωπεύουν συμπαγώς το μήνυμα και χρησιμοποιούνται για την ανίχνευση αλλαγών σε αυτό. Αντίθετα βέβαια με το CRC είναι υπολογιστικά αδύνατο για κάποιον επιτιθέμενο να φτιάξει ένα υποκατάστατο μήνυμα το οποίο θα μπορούσε να παράγει την ίδια περίληψη μηνύματος. Η περίληψη μηνύματος κρυπτογραφείται με το μυστικό κλειδί και έτσι σχηματίζει την ψηφιακή υπογραφή.

Τα κείμενα υπογράφονται με την εισαγωγή στην αρχή τους ψηφιακών πιστοποιητικών υπογραφών οι οποίες περιέχουν το key id του κλειδιού που χρησιμοποιήθηκε για την υπογραφή τους, μια υπογεγραμμένη με το μυστικό κλειδί περίληψη του κειμένου και μια χρονική σφραγίδα της δημιουργίας της υπογραφής. Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο μπρελόκ δημοσίων κλειδιών που έχει στην κατοχή του ο παραλήπτης.

Τα κρυπτογραφημένα αρχεία περιέχουν στην αρχή τους το key id του δημοσίου κλειδιού που χρησιμοποιήθηκε στην κρυπτογράφησή τους. Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο μπρελόκ μυστικών κλειδιών του παραλήπτη.

Αυτοί οι δυο τύποι μπρελόκ κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών. Αντί να κρατάμε ξεχωριστά κλειδιά σε ξεχωριστά αρχεία κλειδιών τα μαζεύουμε σε μπρελόκ κλειδιών έτσι ώστε να διευκολύνουμε την αυτόματη ανεύρεσή τους είτε με τη χρήση του key id είτε με τη χρήση του user id. Κάθε χρήστης διατηρεί το δικό του ζεύγος μπρελόκ. Ένα ξεχωριστό δημόσιο κλειδί αποθηκεύεται προσωρινά σε ένα ξεχωριστό αρχείο μόνο για το χρόνο που χρειάζεται για την αποστολή του σε κάποιο φίλο ο οποίος κατόπιν θα το προσθέσει στο δικό του μπρελόκ κλειδιών.

6.4.3. Προστασία Δημοσίων Κλειδιών

Σε ένα κρυπτοσύστημα δημοσίων κλειδιών δεν υπάρχει ανάγκη προστασίας των δημοσίων κλειδιών, διότι το επιδιωκόμενο είναι η όσο το δυνατόν ευρύτερη διάδοσή τους. Το σημαντικό και αυτό που θα πρέπει να διασφαλίζεται είναι το να είμαστε σίγουροι ότι κάποιο δημόσιο κλειδί που φαίνεται ότι ανήκει σε κάποιον, όντως να ανήκει σε αυτόν. Αυτό μπορεί να είναι και το πιο σημαντικό μειονέκτημα του κρυπτοσυστήματος δημόσιων κλειδιών.

Κάποιο άτομο που τυγχάνει ευρείας εμπιστοσύνης θα μπορούσε να εξειδικευτεί στην παροχή αυτής της υπηρεσίας, δηλαδή της παροχής υπογραφών σε πιστοποιητικά δημοσίων κλειδιών άλλων χρηστών. Αυτό το κοινά αποδεκτό άτομο θα μπορούσε να είναι κάποιος "key server" ή κάποια υπηρεσία πιστοποίησης. Κάθε πιστοποιητικό δημόσιου κλειδιού που φέρει την υπογραφή αυτού του key server θα μπορεί να θεωρείται γνήσιο και έτσι άξιο της εμπιστοσύνης κάποιου. Το μόνο που χρειάζεται να κάνουν όσοι χρήστες θα ήθελαν να συμμετέχουν σε αυτή τη διαδικασία είναι να αποκτήσουν ένα καλό αντίγραφο του δημοσίου κλειδιού του key server έτσι ώστε να είναι σε θέση να επιβεβαιώσουν την υπογραφή αυτού. Κάποιος κεντρικός key server ή μια υπηρεσία πιστοποίησης, θα ήταν κατάλληλη για κάποια μεγάλη και απρόσωπη επιχείρηση ή κυβερνητική υπηρεσία.

Η αποκεντρωμένη έκδοση του σχήματος αυτού είναι εκείνη που επιτρέπει σε όλους τους χρήστες να δρουν σαν μεσάζοντες, ο ένας για τον άλλο, κάτι που έχει καλύτερα αποτελέσματα από έναν και μοναδικό key server. Το PGP τείνει προς αυτή τη κατεύθυνση διότι αντανακλά καλύτερα το φυσικό τρόπο με τον οποίο αλληλεπιδρούν μεταξύ τους οι άνθρωποι στις σχέσεις τους και ταυτόχρονα επιτρέπει σε αυτούς να διαλέξουν ποιόν εμπιστεύονται για τη διαχείριση των κλειδιών τους.

Αυτή ολόκληρη η διαδικασία της προστασίας των δημοσίων κλειδιών είναι το μοναδικό δύσκολο πρόβλημα στις πρακτικές εφαρμογές της κρυπτογράφησης δημοσίων κλειδιών. Θα μπορούσαμε να πούμε ότι είναι το αδύνατο σημείο της κρυπτογράφησης δημοσίων κλειδιών και έχει καταβληθεί μεγάλη προσπάθεια για τη λύση αυτού του προβλήματος.

Η χρήση ενός δημόσιου κλειδιού δεν θα πρέπει να ξεκινάει εάν δεν είμαστε σίγουροι ότι πρόκειται για ένα καλό δημόσιο κλειδί το οποίο ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει. Μπορούμε να είμαστε σίγουροι για την προέλευση του κλειδιού εάν έχουμε κάποιο πιστοποιητικό από τον ιδιοκτήτη του ή κάποιον άλλο που εμπιστευόμαστε, από τον οποίο όμως έχουμε ήδη ένα εγγυημένο δημόσιο κλειδί. Επιπλέον το user id θα πρέπει να έχει ολόκληρο το όνομα του ιδιοκτήτη και όχι απλά το μικρό του ή κάποιο άλλο ψευδώνυμο.

Δεν έχει σημασία πόσο σίγουροι μπορεί να αισθανόμαστε για κάποιο δημόσιο κλειδί που κατεβάσαμε από κάποιον ηλεκτρονικό πίνακα ανακοινωθέντων, ΠΟΤΕ δεν θα πρέπει να εμπιστευόμαστε οτιδήποτε δεν έχει την υπογραφή κάποιου που εμπιστευόμαστε. Ένα δημόσιο κλειδί που απλά κατεβάσαμε δίχως να το ελέγξουμε είναι πιθανόν να έχει αλλοιωθεί από κάποιον τρίτο, ακόμα και από το διαχειριστή του ηλεκτρονικού πίνακα. Εάν ποτέ μας ζητηθεί να υπογράψουμε το δημόσιο κλειδί κάποιου άλλου θα πρέπει να σιγουρευτούμε ότι αυτό πραγματικά του ανήκει. Αυτό πρέπει να γίνει διότι η υπογραφή μας στο δημόσιο κλειδί εγγυάται την αυθεντικότητά του. Εάν έχουμε κάνει λάθος, τότε όσοι μας εμπιστεύονται θα εμπιστευτούν και το κλειδί με αβέβαια αποτελέσματα. Ο κανόνας λέει ότι υπογράφουμε δημόσια κλειδιά για τα οποία έχουμε ιδία γνώση της αυθεντικότητάς τους. Για να αποκτήσουμε αυτή τη γνώση μπορούμε για παράδειγμα να μιλήσουμε στον ιδιοκτήτη του κλειδιού στο τηλέφωνο και να επιβεβαιώσουμε τα στοιχεία που έχουμε στα χέρια μας. Η εμπιστοσύνη δεν είναι αναγκαστικά κάτι μεταβιβάσιμο. Για παράδειγμα μπορεί έχουμε κάποιον φίλο που εμπιστευόμαστε και ξέρουμε ότι δεν λέει ψέματα. Αυτός μπορεί να εμπιστεύεται τον πρόεδρο της κυβέρνησης. Όπως είναι αυτονόητο αυτό δεν σημαίνει ότι και εμείς εμπιστευόμαστε τον πρόεδρο της κυβέρνησης.

Θα ήταν καλή ιδέα, οι χρήστες να κρατούσαν το δημόσιο κλειδί τους μαζί με ένα σύνολο από πιστοποιητικά για αυτούς από διαφόρους μεσάζοντες με την ελπίδα ότι οι περισσότεροι χρήστες εμπιστεύονται κάποιον από αυτούς. Μπορεί λοιπόν, κάποιος χρήστης να ανακοινώσει το δημόσιο κλειδί του μαζί με τη συλλογή των πιστοποιητικών που διαθέτει για αυτό. Όταν υπογράφουμε το δημόσιο κλειδί κάποιου πρέπει να του το επιστρέφουμε μαζί με την υπογραφή μας ώστε να την προσθέσουνε στη συλλογή πιστοποιητικών για το δημόσιο κλειδί τους.

Το PGP κρατάει στοιχεία για το ποια από τα δημόσια κλειδιά που έχουμε στην κατοχή μας είναι πιστοποιημένα με υπογραφές που εμπιστευόμαστε. Το μόνο που εμείς πρέπει να κάνουμε είναι να πούμε στο PGP ποιους εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας. Το PGP αναλαμβάνει από εκεί και πέρα να κρίνει αυτόματα κάποιο δημόσιο κλειδί ως έγκυρο ή όχι.

Το PGP γενικά θεωρεί ότι διατηρούμε το σύστημά μας, τα μπρελόκ και το PGP ασφαλές σε φυσικό επίπεδο. Εάν κάποιος έχει πρόσβαση στο σκληρό δίσκο του συστήματός μας τότε θεωρητικά μπορεί να αλλοιώσει το ίδιο το PGP έτσι ώστε αυτό να αδυνατεί να ανιχνεύσει οποιαδήποτε αλλοιώσει σε άλλα κλειδιά.

Ένας ακόμα τρόπος να προστατεύσουμε ολόκληρο το μπρελόκ με τα κλειδιά μας είναι να το υπογράψουμε ολόκληρο με το μυστικό μας κλειδί. Βέβαια θα έπρεπε πάλι να έχουμε κάπου αλλού προστατευμένο ένα αντίγραφο του δημοσίου κλειδιού μας για να είμαστε σε θέση να ελέγξουμε την υπογραφή μας. Όπως είναι φυσικό δεν μπορούμε να βασιστούμε στο δημόσιο κλειδί μας, που βρίσκεται στο μπρελόκ, για τον έλεγχο της υπογραφής μας διότι αυτό είναι μέρος αυτού που πάμε να προστατέψουμε.

6.4.4. Διαδικασία Αναγνώρισης Έγκυρων Κλειδιών

Το PGP παρακολουθεί ποια από τα κλειδιά που υπάρχουν στο μπρελόκ δημοσίων κλειδιών είναι πιστοποιημένα και ποια όχι με υπογραφές χρηστών που εμπιστευόμαστε. Το μόνο που πρέπει να κάνουμε είναι να "πούμε" στο PGP ποιους χρήστες εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας κλειδί. Το PGP αναλαμβάνει από εκεί να κινήσει αυτόματα διαδικασίες ελέγχου της εγκυρότητας κλειδιών που είναι υπογεγραμμένα από τους μεσάζοντες που εμείς ορίσαμε. Υπάρχει βέβαια πάντα η δυνατότητα να υπογράψουμε κλειδιά και εμείς οι ίδιοι.

Υπάρχουν δύο διαφορετικά κριτήρια βάση των οποίων το PGP κρίνει τη χρησιμότητα των κλειδιών και τα οποία δεν πρέπει να συγχέουμε:

1. Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει; (έχει πιστοποιηθεί από κάποιον του οποίου την υπογραφή εμπιστευόμαστε;)

2. Ανήκει σε κάποιον που μπορούμε να εμπιστευθούμε για την πιστοποίηση άλλων κλειδιών;

Το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση. Η απάντηση στη δεύτερη πρέπει να δοθεί αποκλειστικά από το χρήστη. Όταν ο χρήστης δώσει την απάντηση στην δεύτερη ερώτηση τότε το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση για άλλα κλειδιά τα οποία υπογράφονται από αυτόν που έχουμε ορίσει σαν έμπιστο. Κλειδιά τα οποία έχουν πιστοποιηθεί από κάποιον που έχουμε ορίσει ως έμπιστο θεωρούνται έγκυρα από το PGP. Τα κλειδιά που ανήκουν σε έμπιστους μεσάζοντες πρέπει να πιστοποιηθούν από είτε από εμάς τους ίδιους είτε από κάποιον άλλο που έχουμε ορίσει ως έμπιστο.

Το PGP δίνει επιπλέον τη δυνατότητα ορισμού διαφορετικών επιπέδων εμπιστοσύνης για διαφορετικούς μεσάζοντες. Το ότι εμπιστευόμαστε κάποιον να δράσει ως μεσάζοντας δεν σημαίνει μόνο ότι τον εμπιστευόμαστε αλλά επιπλέον ότι τον θεωρούμε αρκετά ικανό να διαχειριστεί κλειδιά επιλέγοντας ποια από αυτά πρέπει να υπογράψει και ποια όχι. Μπορεί να ορίσουμε έναν χρήστη - μεσάζοντα στο PGP σαν άγνωστο, μη έμπιστο, μερικώς έμπιστο και εντελώς έμπιστο για να πιστοποιεί δημόσια κλειδιά. Αυτή η πληροφορία, που αφορά το βαθμό εμπιστοσύνης κάποιου μεσάζοντα, περιέχεται στο μπρελόκ των κλειδιών μαζί με το αντίστοιχο κλειδί (του μεσάζοντα) και δεν αντιγράφεται σε καμία περίπτωση κατά την αντιγραφή κάποιου κλειδιού του μπρελόκ διότι θεωρείται εμπιστευτική πληροφορία μια και αντικατοπτρίζει την άποψη του κατόχου του για τους μεσάζοντες - απόλυτα προσωπικό στοιχείο.

Όταν το PGP ελέγχει την εγκυρότητα ενός κλειδιού αυτό που κάνει είναι να ελέγχει τον βαθμό εμπιστοσύνης όλων των συνημμένων υπογραφών πιστοποίησής του. Κατόπιν υπολογίζει ένα μέσο επίπεδο εμπιστοσύνης - για παράδειγμα δύο μερικώς έμπιστες υπογραφές ισοδυναμούν με μία πλήρως έμπιστη. Το σκεπτικό λειτουργίας του PGP προσαρμόζεται στις απαιτήσεις του χρήστη και ρυθμίζεται αναλόγως (για παράδειγμα μπορούμε να ρυθμίσουμε το PGP να θεωρεί ένα κλειδί έγκυρο μόνο εάν αυτό φέρει δύο πλήρως έμπιστες υπογραφές ή τρεις μερικώς έμπιστες).

Το δικό μας κλειδί θεωρείται έγκυρο από το PGP αξιωματικά και για αυτό το λόγο δεν χρειάζεται την πιστοποίηση από κανέναν. Το PGP γνωρίζει ποια δημόσια κλειδιά

είναι δικά μας κοιτάζοντας να βρει τα αντίστοιχα μυστικά κλειδιά στο μπρελόκ τους. Το PGP θεωρεί επιπλέον ότι εμπιστευόμαστε τους εαυτούς μας για να πιστοποιούν άλλα κλειδιά.

Όσο θα περνάει ο καιρός θα λαμβάνουμε όλο και περισσότερα κλειδιά από χρήστες που ίσως να θέλουμε να ορίσουμε ως μεσάζοντες. Κάθε ένας από αυτούς θα έχει τους δικούς του μεσάζοντες των οποίων τα πιστοποιητικά - υπογραφές θα μοιράζει μαζί με το κλειδί του με την ελπίδα ότι όποιος τα λάβει να εμπιστεύεται κάποιο από όλα. Έτσι δημιουργείται ένα αποκεντρωμένο δίκτυο εμπιστοσύνης για όλα τα δημόσια κλειδιά.

Αυτή η μοναδική προσέγγιση έρχεται σε αντίθεση με τα κατεστημένα κυβερνητικά σχήματα διαχείρισης κλειδιών, όπως το PEM (Internet Privacy Enhanced Mail), τα οποία βασίζονται σε συστήματα κεντρικού ελέγχου και υποχρεωτικής εμπιστοσύνης σε αυτά. Τα σχήματα αυτά απαρτίζονται από ιεραρχικές οντότητες που υπαγορεύουν ποιόν πρέπει να εμπιστευόμαστε. Αυτό είναι φανερό ότι έρχεται σε πλήρη αντίθεση με τη σχεδιαστική αρχή του PGP η οποία επιτρέπει στον καθένα και ανεξάρτητα από οποιονδήποτε και οτιδήποτε άλλο να καθορίσει ο ίδιος την πολιτική που θέλει να ακολουθήσει στη διαχείριση των κλαδιών του. Έτσι το PGP βάζει το χρήστη και όχι το σύστημα στην κορυφή της προσωπική του πυραμίδα πιστοποίησης.

6.4.5. Προστασία του Μυστικού Κλειδιού

Η προστασία του μυστικού κλειδιού και της φράσης-κλειδί του, είναι κάτι το αυτονόητο στο οποίο πρέπει να δοθεί μεγάλη προσοχή. Εάν ποτέ το μυστικό κλειδί πέσει σε λάθος χέρια τα οποία είναι οποιαδήποτε άλλα εκτός των δικών μας τότε θα πρέπει άμεσα, τόσο για τη δική μας ασφάλεια όσο και των άλλων, να ειδοποιήσουμε τους πάντες για το γεγονός προτού κάποιος αρχίσει να υπογράφει με το "όνομά" μας. Θα μπορούσε, για παράδειγμα, να υπογράψει ένα σύνολο από δημόσια κλειδιά δημιουργώντας έτσι πρόβλημα σε πολλούς χρήστες ειδικά εάν η υπογραφή μας τυγχάνει ευρείας εμπιστοσύνης και αποδοχής. Φυσικά, κίνδυνο διατρέχουμε και από το γεγονός της έκθεσης όλων των μηνυμάτων μας στα μάτια αυτού που έχει το προσωπικό μας κλειδί.

Η προστασία του μυστικού κλειδιού πρέπει να αρχίζει με τη φυσική του διασφάλιση. Μπορούμε να το κρατάμε σε κάποιο PC στο σπίτι ή κάποιο υπολογιστή notebook μια και αυτά τα έχουμε υπό την επίβλεψή μας συνεχώς. Εάν ποτέ υπάρξει ανάγκη χρησιμοποίησης υπολογιστή στο γραφείο ή οπουδήποτε αλλού τότε θα πρέπει να μεταφέρουμε το μυστικό κλειδί μας σε αυτόν μέσο κάποιας μνήμης USB ενδεχομένως και για όσο χρειάζεται ενώ όταν τελειώσουμε τη δουλεία μας δεν πρέπει να αφήσουμε πίσω οτιδήποτε μπορεί να οδηγήσει στην αποκάλυψη του. Δεν είναι επίσης σωστό να αφήνουμε το μυστικό κλειδί μας σε κάποιο απομακρυσμένο μηχάνημα διότι μπορεί κάποιος που παρακολουθεί τις επικοινωνίες να υποκλέψει τη μυστική φράση (pass phrase) και να αποκτήσει το μυστικό από το απομακρυσμένο σύστημα. Συμπερασματικά λέμε ότι θα πρέπει να γίνεται χρήση του μυστικού κλειδιού μόνο σε συστήματα στα οποία έχουμε φυσικό έλεγχο.

Επιπρόσθετα, πρέπει να προσέξουμε πού αποθηκεύουμε τη μυστική φράση-κλειδί. Δεν πρέπει ποτέ αυτή να βρίσκεται στον ίδιο υπολογιστή με αυτόν που έχει το αρχείο του μυστικού κλειδιού μας. Η αποθήκευση τόσο του μυστικού κλειδιού όσο και της μυστικής φράσης στον ίδιο υπολογιστή είναι το ίδιο επικίνδυνη με την φύλαξη του PIN ενός τραπεζικού ATM λογαριασμού στο ίδιο πορτοφόλι με την κάρτα ATM. Ένα πράγμα είναι σίγουρο - δεν θέλουμε σε καμία περίπτωση αυτός που θα έχει στα χέρια του τον σκληρό δίσκο με το μυστικό μας κλειδί να έχει στη διάθεσή του και τη μυστική φράση. Το ιδανικό θα ήταν να απομνημονεύαμε τη μυστική φράση και να μην την φυλάγαμε σε κανένα άλλο μηχάνημα εκτός του εγκεφάλου μας. Εάν, ωστόσο, νιώθουμε ότι πρέπει να τη γράψουμε κάπου θα πρέπει να την ασφαλίσουμε καλύτερα ίσως και από το ίδιο το μυστικό μας κλειδί.

Κάτι άλλο επίσης σημαντικό, που πρέπει να κάνουμε, είναι να παίρνουμε backup του μυστικού μπρελόκ μας διότι μόνο εμείς έχουμε το μοναδικό αντίγραφο αυτού και πιθανή απώλειά του θα ισοδυναμούσε με αχρήστευση όλων των δημοσίων κλειδιών που διανείμαμε στον κόσμο.

Το αποκεντρωτικό σχήμα φιλοσοφίας αλλά και λειτουργίας που έχει επιλέξει να χρησιμοποιήσει το PGP εκτός από τα πλεονεκτήματα στη διαχείριση των κλειδιών έχει και τα μειονεκτήματα του. Δεν υπάρχει μία κεντρική λίστα που να περιέχει τα μη έγκυρα κλειδιά κάνοντας πιο δύσκολη την γνώση τους. Έτσι αν κάτι πάει στραβά η διαδικασία γνωστοποίησής του είναι επίπονη. Εάν τελικά το μυστικό κλειδί και η

μυστική φράση πέσουν στα χέρια άλλων θα πρέπει να φτιάξουμε και να διανείμουμε ένα "πιστοποιητικό απολεσθέντος κλειδιού" (key compromise certificate). Αυτός ο τύπος πιστοποιητικού χρησιμοποιείται για να προειδοποιεί άλλους χρήστες να σταματήσουν να χρησιμοποιούν το αντίστοιχο δημόσιο κλειδί μας. Μπορούμε να χρησιμοποιήσουμε το PGP στη δημιουργία αυτού του πιστοποιητικού και κατόπιν να το στείλουμε σε όλους τους φίλους και συνεργάτες μας σε όλο τον κόσμο. Η έκδοση του PGP που τρέχει σε αυτούς θα αναλάβει να εγκαταστήσει το πιστοποιητικό του απολεσθέντος κλειδιού στα δημόσια μπρελόκ τους και από εκείνη τη στιγμή θα αποτρέπεται αυτόματα η επαναχρησιμοποίησή τους. Μπορούμε κατόπιν να δημιουργήσουμε ένα νέο ζεύγος μυστικού/δημοσίου κλειδιού και να αρχίσουμε πλέον να δουλεύουμε με αυτά.

7. Προβλήματα ασφάλειας του ηλεκτρονικού ταχυδρομείου

7.1. PEM - Privacy Enhanced Mail

Ένα ηλεκτρονικό μήνυμα του Internet, κατά την πορεία του από τον αποστολέα στον τελικό παραλήπτη, διανύει πολλά ενδιάμεσα συστήματα και δίκτυα. Δεν είναι δυνατόν να βασιστούμε στην αξιοπιστία όλων αυτών των οντοτήτων. Ένας εισβολέας μπορεί να κρύβεται οπουδήποτε και τα μηνύματα μπορούν εύκολα να διαβαστούν, να τροποποιηθούν και ακόμα να εμποδιστούν από το να φθάσουν στον τελικό τους προορισμό.

Το πρωτόκολλο Privacy-Enhanced Mail (PEM) προβλέπει για αυτή την αδυναμία του ηλεκτρονικού ταχυδρομείου του Internet, προσθέτοντας:

- την εφαρμογή των υπηρεσιών της απόρρητης συναλλαγής,
- της πιστοποίησης ταυτότητας,
- της ακεραιότητας των μηνυμάτων
- και την εξασφάλιση της μη αποκήρυξης της πηγής.

Οι υπηρεσίες αυτές προσφέρονται μέσω της χρήσης απ' άκρη σ' άκρη κρυπτογράφησης μεταξύ του αποστολέα και του παραλήπτη. Δεν απαιτούνται ειδικές ικανότητες επεξεργασίας στα συστήματα MTS (Message Transfer System) και υποστηρίζεται η συνεργασία με άλλα ταχυδρομικά συστήματα μεταφοράς.

7.1.1. Αρχές του PEM

Σημαντικότατο γεγονός (που έρχεται σε αντίθεση με το S/MIME) είναι ότι η εφαρμογή των υπηρεσιών ασφαλείας που παρέχει το PEM γίνεται στο σύνολο του σώματος του μηνύματος και δεν επιτρέπεται ούτε υποστηρίζεται η επιλεκτική χρήση των υπηρεσιών του PEM σε κομμάτια του μηνύματος.

Η ανάπτυξη του PEM στηρίχθηκε στις εξής βασικές αρχές:

1. Όλες προσθήκες ασφάλειας εφαρμόζονται στο Application Layer του OSI και είναι ανεξάρτητες από οποιαδήποτε χαρακτηριστικά ασφαλείας χαμηλότερων επιπέδων.
2. Οι προσθήκες ασφαλείας εφαρμόζονται μόνο από τους αποστολείς και τους τελικούς αποδέκτες των μηνυμάτων. Η λειτουργία των ενδιάμεσων συστημάτων που δεν υποστηρίζουν τις δυνατότητες του PEM δεν επηρεάζεται

από αυτή την συνθήκη. Παρ' όλα αυτά είναι απαραίτητο ο αποστολέας να γνωρίζει κατά πόσο ο προοριζόμενος παραλήπτης του μηνύματος εφαρμόζει τις υπηρεσίες ασφάλειας του PEM, ώστε να αποφευχθεί η άσκοπη κρυπτογράφηση και κωδικοποίηση του μηνύματος.

3. Οι καθορισμένοι μηχανισμοί είναι συμβατοί με μία μεγάλη ποικιλία ταχυδρομικών συστημάτων μεταφοράς (MTAs) και πρέπει να μπορούν να λειτουργούν πρωτόκολλα μεταφορά εκτός του SMTP (USENET, CSNET, BITNET).
4. Οι καθορισμένοι μηχανισμοί είναι συμβατοί με μεγάλη ποικιλία προγραμμάτων ηλεκτρονικού ταχυδρομείου (Mail User Agents MUAs). Επιπλέον οι μηχανισμοί του PEM διαλέγονται έτσι ώστε να μπορούν να χρησιμοποιηθούν με τα περισσότερα προγράμματα χρηστών.
5. Υποστηρίζεται μεγάλη ποικιλία τεχνικών διαχείρισης κλειδιών και διαφορετικές τεχνικές χρησιμοποιούνται με διαφορετικούς παραλήπτες. Διαφορετικές τεχνικές μπορούν να οριστούν ακόμα και με τους διαφορετικούς παραλήπτες ενός multicast μηνύματος. Για να συνεργαστούν δυο εφαρμογές PEM, πρέπει να μοιράζονται ένα τουλάχιστον κοινό μηχανισμό διαχείρισης κλειδιών.

7.1.2. Παραγωγή PEM Μηνυμάτων

Είδη κλειδιών και διαχείριση τους

Η περιγραφή του πρωτοκόλλου καθορίζει δύο τύπους κλειδιών:

1. Data Encrypting Keys (DEKs): Είναι κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των κειμένων των μηνυμάτων. Στην ασύμμετρη διαχείριση κλειδιών (asymmetric key management), στα PEM μηνύματα που εφαρμόζεται η υπηρεσία της διαφύλαξης του απόρρητου (ENCRYPTED μηνύματα βλέπε παρακάτω) τα DEKs χρησιμοποιούνται στην επιπλέον κρυπτογράφηση των Message Integrity Checks (MICs). Λέμε επιπλέον γιατί τα MICs, για την παραγωγή της υπογραφής του μηνύματος, κρυπτογραφούνται από το IK. Λέγοντας MICs εννοούμε το αποτέλεσμα που δίνει στην έξοδο του ένας digest ή hash algorithm όταν στην είσοδο εισάγουμε το μήνυμα. Τα κλειδιά DEKs παράγονται εκ νέου για κάθε μήνυμα προς μετάδοση.
2. Interchange Keys (IKs): Χρησιμοποιούνται για την κρυπτογράφηση των DEKs και MICs τα οποία μεταφέρονται μέσα στο μήνυμα. Κανονικά, το ίδιο IK θα

χρησιμοποιηθεί για όλα τα μηνύματα από έναν συγκεκριμένο αποστολέα σε έναν συγκεκριμένο παραλήπτη, για περιορισμένο χρονικό διάστημα. Η κρυπτογράφηση των DEKs και MICs μπορεί να γίνει είτε με συμμετρική κρυπτογραφία (συμμετρική διαχείριση κλειδιών), οπότε το IK είναι το ίδιο για αποστολέα και παραλήπτη, είτε με ασύμμετρη κρυπτογραφία (ασύμμετρη διαχείριση κλειδιών), οπότε η κρυπτογράφηση γίνεται με την δημόσια κλείδα του παραλήπτη. Στην ασύμμετρη κρυπτογράφηση των MICs χρησιμοποιείται η ιδιωτική κλείδα του αποστολέα.

Όταν ένα μήνυμα πρόκειται να επεξεργαστεί από το PEM, παράγεται ένα DEK για την κρυπτογράφηση του μηνύματος καθώς και απαραίτητοι παράμετροι (π.χ. Initialization Vectors) που εξαρτώνται από τους επιλεγμένους αλγόριθμους. Στην περίπτωση συμμετρικών IKs, χρησιμοποιούνται διαφορετικά κλειδιά για κάθε παραλήπτη του μηνύματος, για την προετοιμασία των κρυπτογραφημένων DEKs και MICs. Αντίθετα, στην περίπτωση των ασύμμετρων IKs, επειδή ο αποστολέας κατέχει ένα ζευγάρι δημόσιας - ιδιωτικής κλείδας, η κρυπτογράφηση των DEKs και MICs γίνεται για όλους τους παραλήπτες με την ίδια κλείδα.

Είναι δυνατόν ένα αφιερωμένο σύστημα (Key Distribution System) να δημιουργεί τα τυχαία DEKs. Τέτοια συστήματα μπορούν να εφαρμόζουν πιο ισχυρούς αλγόριθμους στην παραγωγή των τυχαίων DEKs, παρ' αυτά όμως η αποκέντρωση της παραγωγής επιτρέπει στα συστήματα των χρηστών να είναι αυτοσυντηρούμενα και απαλείφει την εμπιστοσύνη σε τρίτες οντότητες.

Η ασύμμετρη διαχείριση κλειδιών μπορεί να συνδυαστεί με την χρήση πιστοποιητικών για την επαλήθευσης της ταυτότητας του αποστολέα. Το πιστοποιητικό περιέχει, εκτός των πληροφοριών που σχετίζονται με τον εκδότη του (Certificate Authority CA) και την δημόσια κλείδα του αποστολέα.

7.1.3. Περιληπτική Παρουσίαση της Επεξεργασίας

Με σκοπό τα κρυπτογραφημένα μηνύματα να είναι παγκοσμίως αναγνωρίσιμα και να μπορούν να μεταφερθούν σε όλα τα περιβάλλοντα, απαιτείται ένας μετασχηματισμός τεσσάρων φάσεων. Αρχικά τα μηνύματα συντάσσονται σύμφωνα με τους τοπικούς κανόνες, χρησιμοποιώντας το σύνολο χαρακτήρων (character set) και τους χαρακτήρες ελέγχου του τοπικού συστήματος. Η αρχική αυτή μορφή μετατρέπεται σε κανονική μορφή (canonical form), η οποία αποτελεί είσοδο στις διαδικασίες της

κρυπτογράφησης και της παραγωγής MIC. Τέλος, το αποτέλεσμα της κρυπτογράφησης και / ή της παραγωγής του MIC κωδικοποιείται βάσει κατάλληλου μηχανισμού. Το σύνολο χαρακτήρων που χρησιμοποιεί ο μηχανισμός αυτός είναι παγκόσμια παρουσιάσιμο. Παρακάτω θα αναλύσουμε περισσότερο τα βήματα επεξεργασίας.

Η έξοδος του τέταρτου βήματος συνδυάζεται με κατάλληλες επικεφαλίδες που μεταφέρουν πληροφορίες ελέγχου της κρυπτογράφησης. Το PEM μήνυμα που προκύπτει περιλαμβάνεται στα περιεχόμενα ενός μηνύματος προς μετάδοση. Στα περιεχόμενα είναι δυνατόν να υπάρχει και απλό, μη προστατευμένο κείμενο.

Ο παραλήπτης του μηνύματος, αφού αφαιρέσει την κωδικοποίηση, εξετάζει τις πεδία ελέγχου της κρυπτογράφησης που του παρέχουν τις απαραίτητες πληροφορίες για να επαλήθευση την εγκυρότητα του MIC και για να αποκρυπτογραφήσει το κείμενο. Τέλος, το μήνυμα μετατρέπεται από την κανονική μορφή στην μορφή που αντιστοιχεί στα χαρακτηριστικά του τοπικού συστήματος του παραλήπτη.

Συντακτικά άκυρα PEM μηνύματα θα πρέπει να αναφερθούν μαζί με συλλογή διαγνωστικών πληροφοριών για να αντιμετωπιστούν προβλήματα ασυμβατότητας ή άλλων αιτιών. Τα PEM μηνύματα, όμως, που είναι συντακτικά έγκυρα αλλά παρουσιάζουν αποτυχημένη επαλήθευση του MIC πρέπει να αντιμετωπίζονται με προσοχή. Οι χρήστες θα πρέπει να ειδοποιούνται ότι το δεν μπορεί να εγγυηθεί η αυθεντικότητα και η ακεραιότητα των περιεχομένων του εν λόγω μηνύματος.

7.1.4. Τύποι Μηνυμάτων

Ανάλογα με το είδος της παρεχόμενης προστασίας και τις εφαρμοζόμενες υπηρεσίες, τα PEM μηνύματα διακρίνονται σε τέσσερα είδη:

- ENCRYPTED: Αναπαριστά ένα PEM μήνυμα στο οποίο έχουν εφαρμοστεί οι υπηρεσίες της διαφύλαξης του απόρρητου της συναλλαγής, της εξασφάλισης της ακεραιότητας των δεδομένων, της πιστοποίησης ταυτότητας και της εξασφάλισης της μη αποκήρυξης της πηγής.
- MIC-ONLY: Αναπαριστά ένα PEM μήνυμα στο οποίο παρέχονται όλες οι προηγούμενες υπηρεσίες εκτός της διαφύλαξης του απόρρητου. Μόνο οι UAs που ενσωματώνουν το PEM μπορούν να παρουσιάσουν το μήνυμα για ανάγνωση.

- MIC-CLEAR: Το μήνυμα είναι το ίδιο με προηγουμένως με την διαφορά ότι όλοι η UAs μπορούν να παρουσιάσουν το μήνυμα, αλλά μόνο οι συμβατοί με το PEM μπορούν να επαληθεύσουν την αυθεντικότητα και την ακεραιότητα του μηνύματος.
- CERTIFICATE REVOCATION: Μήνυμα που περιέχει μία ή περισσότερες λίστες ανάκλησης πιστοποιητικών (CRL).

7.1.5. Βήματα Επεξεργασίας

Η φιλοσοφία παραγωγής μηνυμάτων συμβατών με τις υποκείμενες τεχνολογίες και πρωτόκολλα περιλαμβάνει ένα βήμα κανονικοποίησης που αφαιρεί όλες τις τοπικές συμβάσεις, ακολουθούμενο από βήμα κωδικοποίησης για την προσαρμογή με μέσω μεταφοράς ηλεκτρονικού ταχυδρομείου (SMTP).

Το πρωτόκολλο SMTP έχει συγκεκριμένους περιορισμούς όσο αναφορά την μορφή του προς μετάδοση μηνύματος. Έτσι η προετοιμασία του μηνύματος έχει τις ακόλουθες απαιτήσεις:

1. Όλοι οι χαρακτήρες πρέπει να ανήκουν στο σύνολο χαρακτήρων 7-bit ASCII.
2. Οι γραμμές κειμένου πρέπει να διαχωρίζονται από το ζευγάρι <*CR*><*LF*> και το μήκος τους δεν πρέπει να ξεπερνά τους 1000 χαρακτήρες.
3. Λόγω του ότι η ακολουθία <*CR*><*LF*>.<*CR*><*LF*> σηματοδοτεί το τέλος του μηνύματος δεν πρέπει να συναντάται πουθενά πριν από το τέλος.

Τα τέσσερα βήματα του μετασχηματισμού παρουσιάζονται αναλυτικά παρακάτω:

- ***Βήμα 1: Local Form***

Το βήμα αυτό είναι εφαρμόσιμο στα PEM μηνύματα τύπου ENCRYPTED, MIC-ONLY, MIC-CLEAR. Το κείμενου του μηνύματος δημιουργείται βάσει των τοπικών συνόλων χαρακτήρων και των τοπικών χαρακτήρων ελέγχου.

- ***Βήμα 2: Canonical Form***

Το βήμα αυτό, όπως και το προηγούμενο, είναι εφαρμόσιμο στους τύπους ENCRYPTED, MIC-ONLY, MIC-CLEAR. Το κείμενο μετατρέπεται σε παγκόσμια αναγνωρίσιμη μορφή, την κανονικά μορφή. Όλες οι συμβάσεις του τοπικού συστήματος αφαιρούνται και το κείμενο υπόκειται στους περιορισμούς του SMTP. Το

μήκος των γραμμών μειώνεται, οι χαρακτήρες αλλαγής γραμμής γίνονται οι *<CR><LF>,* και το σύνολο χαρακτήρων ανάγεται στο 7-bit ASCII.

- ***Βήμα 3: Authentication and Encryption***

Το τρίτο βήμα περιλαμβάνει δύο ξεχωριστές ενέργειες: την παραγωγή MIC και την κρυπτογράφηση της κανονικής μορφής του προηγούμενου βήματος. Η κρυπτογράφηση εφαρμόζεται μόνο στα ENCRYPTED, ενώ η εφαρμόζεται και στους τρεις τύπους (ENCRYPTED, MIC-ONLY, MIC-CLEAR).

- ***Βήμα 4: Printable Encoding (base64)***

Η κωδικοποίηση του τέταρτου βήματος εφαρμόζεται στους τύπους ENCRYPTED και MIC-ONLY. Η ακολουθία bit του 3ου βήματος κωδικοποιείται σε χαρακτήρες που είναι παρουσιάσιμοι σε όλα τα sites.

Κάθε 3 bytes του επεξεργαζόμενου αρχείου, λαμβάνονται σαν ποσότητες των 24 bit και διαχωρίζονται σε 4 εξάδες bit. Έπειτα κάθε εξάδα αντιστοιχίζεται, βάσει ενός πίνακα 64 χαρακτήρων, με χαρακτήρα από συγκεκριμένο υποσύνολο του ASCII. Εάν δεν συμπληρώνονται 24 bit, τότε χρησιμοποιείται ο χαρακτήρα (=) σαν συμπλήρωμα.

7.1.6. Υποστηριζόμενοι Αλγόριθμοι

7.1.6.1. Αλγόριθμοι Κρυπτογράφησης

Ο μοναδικός αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση των περιεχομένων είναι ο DES σε CBC (Cipher Bloch Chaining) mode. Η είσοδος στον αλγόριθμο πολύ πιθανών να απαιτεί κατάλληλο συμπλήρωμα, ώστε το μήκος να είναι πολλαπλάσιο των 8 bytes. Επίσης απαιτεί έναν 64-bit Initialization Vector, ο οποίος είναι διαφορετικός για κάθε ENCRYPTED PEM μήνυμα.

Ο DES CBC απαιτεί ένα κλειδί κρυπτογράφησης των 64 bits. Από τα 64 bits, τα 56 χρησιμοποιούνται απευθείας για από τον DES CBC, ενώ τα υπόλοιπα 8 bits είναι bits περιττής ισοτιμίας. Για κάθε ENCRYPTED PEM μήνυμα παράγεται νέο τυχαίο κλειδί.

7.1.6.2. Αλγόριθμοι Παραγωγής MICs

Υπάρχουν δύο αλγόριθμοι σε αυτήν την κατηγορία, ο MD2 και ο MD5. Και οι δύο αλγόριθμοι δέχονται σαν είσοδο μήνυμα οποιουδήποτε μήκους και παράγουν στην έξοδο μια ακολουθία 16 bytes. Όταν χρησιμοποιείται συμμετρική διαχείριση κλειδιών,

το αποτέλεσμα των αλγορίθμων διασπάται στα δύο μισά των 8 bytes, τα οποία κρυπτογραφούνται ξεχωριστά και έπειτα συνενώνονται.

7.1.6.3. Αλγόριθμοι Συμμετρικής Διαχείρισης Κλειδιών

Οι αλγόριθμοι που χρησιμοποιούνται για την κρυπτογράφηση των DEKs και MICs είναι δύο παραλλαγές του DES: ο DES σε ECB (Electronic-Codebook) mode και ο DES σε EDE (Encrypt-Decrypt-Encrypt) mode. Και οι δύο απαιτούν IK κλειδιά μήκους 64 bits.

7.1.6.4. Αλγόριθμοι Ασύμμετρης Διαχείρισης Κλειδιών

Το ασύμμετρο ζευγάρι IK κλειδιών (δημόσια κλείδα ιδιωτική κλείδα) είναι της μορφής που καθορίζεται από το RSA μηχανισμό. Ομοίως, για την κρυπτογράφηση των DEKs και MICs ο μηχανισμός RSA εφαρμόζεται, κατά τον οποίο η ιδιωτική κλείδα κρυπτογραφεί το MICs παράγοντας έτσι ψηφιακές υπογραφές των μηνυμάτων και η δημόσια κλείδα κρυπτογραφεί το DEK.

Χρησιμοποιείται, επίσης, και ο MD2 σε συνδυασμό με τον RSA για την υπογραφή των πιστοποιητικών και των λιστών ανάκλησης πιστοποιητικών (CRL).

7.2. Ταυτοποίηση Αυθεντικοποίηση

Η ταυτοποίηση και αυθεντικοποίηση των χρηστών σε ένα πληροφοριακό σύστημα το οποίο μπορεί να είναι από έναν προσωπικό υπολογιστή μέχρι έναν διακομιστή ή ένα ολόκληρο δίκτυο, αποτελεί ένα πολύ σημαντικό θέμα στην ασφάλεια του ίδιου του πληροφοριακού συστήματος. Για αυτό τον λόγο υπάρχουν και διάφοροι τρόποι για να εξασφαλίζεται η ασφάλεια, ανάλογα με τις διαθέσιμες μεθόδους αλλά και το επίπεδο ασφάλειας που θέλουμε να έχουμε σε ένα πληροφοριακό σύστημα. Θα πρέπει να γίνει σαφές ότι η ταυτοποίηση δεν είναι το ίδιο με την αυθεντικοποίηση, καθώς η αυθεντικοποίηση έπεται της ταυτοποίησης. Πιο αναλυτικά:

- Η **ταυτοποίηση** (identification) είναι η διαδικασία κατά την οποία ένας χρήστης δίνει στο πληροφοριακό σύστημα τα στοιχεία πρόσβασης του με σκοπό να μπορέσει να χρησιμοποιήσει τις λειτουργίες που του παρέχονται από αυτό.
- Η **αυθεντικοποίηση** (authentication) είναι η διαδικασία κατά την οποία ο χρήστης πρέπει να επιβεβαιώσει ότι τα στοιχεία που έδωσε κατά την ταυτοποίηση είναι αληθή και σωστά.

Η διαδικασία της αυθεντικοποίησης περιλαμβάνει την υποβολή πληροφοριών στο σύστημα που είναι εκ των προτέρων γνωστές στον χρήστη αλλά και στο ίδιο το σύστημα. Ανάλογα με το είδος του συστήματος υπάρχουν τέσσερις (4) βασικοί τύποι για τον έλεγχο της αυθεντικοποίησης:

1. Αυθεντικοποίηση με κάτι που ο χρήστης γνωρίζει για παράδειγμα ένα συνθηματικό ή ένα pin.

Είναι ο τρόπος που χρησιμοποιείται περισσότερο σήμερα από τα συστήματα ηλεκτρονικού ταχυδρομείου, καθώς είναι ότι πιο εύκολο στον χρήστη να έχει μαζί του ή να γνωρίζει κάποιον κωδικό. Επίσης έχει την δυνατότητα να το αλλάζει συχνά για μεγαλύτερη ασφάλεια. Το βασικό μειονέκτημα της μεθόδου αυτής είναι ότι τρίτοι μπορούν συνήθως εύκολα να μαντέψουν τον κωδικό καθώς το μεγαλύτερο ποσοστό των χρηστών, χρησιμοποιεί για κωδικό είτε κάποια ημερομηνία, είτε έναν κωδικό για όλα.

2. Αυθεντικοποίηση με κάποια συσκευή που κατέχει ο χρήστης όπως είναι κάποια κάρτα, κάποια μαγνητική συσκευή ή κάποιο άλλο ψηφιακό πιστοποιητικό.

Ο τύπος αυτός απαιτεί την ύπαρξη εξειδικευμένων συσκευών και λογισμικού όπως είναι συσκευές RFID, τα οποία πρέπει να είναι εγκατεστημένα στον προσωπικό υπολογιστή που θα χρησιμοποιήσει ο χρήστης για την πρόσβασή του στο ηλεκτρονικό ταχυδρομείο του κάτι το οποίο είναι ασύμφορο και από θέμα χρηστικότητας αλλά και κόστους.

3. Αυθεντικοποίηση με βιομετρικά χαρακτηριστικά τα οποία είναι μοναδικά σε κάθε άνθρωπο και στο μεγαλύτερο μέρος τους δεν αντιγράφονται, όπως είναι δακτυλικά αποτυπώματα, ανάγνωση φωνής και ίριδας ματιού.

Και σε αυτή την περίπτωση απαιτείται εξειδικευμένος εξοπλισμός και λογισμικό το οποίο πρέπει να χρησιμοποιεί ο χρήστης όπως είναι οι αναγνώστες δακτυλικών αποτυπωμάτων (fingerprint reader) ή αναγνώστες ίριδος ματιών (core eye scanner). Να σημειώσουμε εδώ ότι αυτές οι συσκευές χρησιμοποιούν κάποιο λογισμικό το οποίο μετατρέπει τα δεδομένα του «σκαναρίσματος» σε δεκαεξαδικό συνήθως κωδικό ο οποίος είναι δύσκολος στην απομνημόνευση αλλά και στην εύρεση του και από ανθρώπους αλλά και από προγράμματα. Σε αυτό τον τύπο κυρίως

χρησιμοποιείται η αναγνώριση του δακτυλικού αποτυπώματος και στην εξάπλοση αυτής της μεθόδου συνέβαλλε το γεγονός ότι πολλές συσκευές, σήμερα, όπως φορητοί υπολογιστές, πληκτρολόγια κα, έχουν ενσωματωμένες τέτοιες συσκευές.

Εικόνα 18 - Mini Laptop με fingerprint reader

Εικόνα 19 - Core eye scanner

4. Αυθεντικοποίηση με βάση την τοποθεσία που βρίσκεται ο χρήστης, για παράδειγμα η IP διεύθυνση του.

Αυτόν τον τύπο αυθεντικοποίησης τον χρησιμοποιούν κυρίως εταιρίες, με σκοπό οι εργαζόμενοι να έχουν πρόσβαση στο ηλεκτρονικό τους ταχυδρομείο μόνο από υπολογιστές του intranet της εταιρίας με στατικές IP ή μέσω του domain που χρησιμοποιείται.

Οι τύποι αυθεντικοποίησης που χρησιμοποιούνται στο ηλεκτρονικό ταχυδρομείο συνήθως είναι ο πρώτος και ο τέταρτος για μεγαλύτερη ευκολία αλλά υπάρχει η δυνατότητα να χρησιμοποιηθούν και οι άλλοι με την χρήση ειδικών συσκευών και λογισμικού όπως αναφέραμε και παραπάνω, κάτι το οποίο είναι στην κρίση του χρήστη αν θα χρησιμοποιηθεί. Την μεγαλύτερη ασφάλεια μπορεί να την προσεγκίσει κάποιος με συνδυασμό μεθόδων, κάτι που γίνεται σπάνια, καθώς το ηλεκτρονικό ταχυδρομείο για τους περισσότερους χρήστες δεν απαιτεί μεγάλη ασφάλεια όπως για παράδειγμα ο τραπεζικός τους λογαριασμός και η διαχείριση του μέσω διαδικτύου.

Σε καμία περίπτωση δεν μπορούμε να πούμε ότι με κάποιον τρόπο θα διασφαλιστεί η μέγιστη ασφάλεια, καθώς αυτό είναι τελείως υποκειμενικό. Αν ένας κακόβουλος χρήστης θελήσει να αποκτήσει πρόσβαση στο ηλεκτρονικό ταχυδρομείο κάποιου χρήστη, μπορεί να το κάνει με διάφορους τρόπους και εργαλεία. Για παράδειγμα υπάρχουν εργαλεία τα οποία ψάχνουν για κωδικούς, και ανάλογα με το πόσο δύσκολος είναι ο κωδικός του χρήστη τον βρίσκουν και συνήθως γίνεται με δύο μεθόδους. Η μία είναι το «συστηματικό ψάξιμο» (brute force), στην οποία

δοκιμάζονται διάφοροι πιθανοί συνδυασμοί και το «έξυπνο ψάξιμο» που γίνεται δοκιμή συνδυασμών από πληροφορίες που σχετίζονται με τον χρήστη, όπως για παράδειγμα είναι το όνομα του, ημερομηνία γέννησης κ.α.. Ένα ακόμα εργαλείο που χρησιμοποιείται συχνά και είναι αρκετά εύκολο στην εύρεση του στο διαδίκτυο είναι τα key logger προγράμματα, τα οποία καταγράφουν το τι δακτυλογραφεί ο χρήστης κατά την είσοδό του στο ηλεκτρονικό ταχυδρομείο. Ένα έξυπνο και απλό εργαλείο-μέθοδος για την προστασία από τέτοιου είδους προγράμματα είναι η χρήση πληκτρολογίου οθόνης στο οποίο η χρήση γίνεται με το ποντίκι πατώντας πάνω στα γράμματα.

Το authentication στα e-mail χρησιμοποιείται όμως σε δύο φάσεις. Κατά την σύνδεση του χρήστη στο ηλεκτρονικό του ταχυδρομείο που αναλύσαμε παραπάνω και κατά την μεταφορά των ηλεκτρονικών μηνυμάτων από mail server σε mail server. Δεν μπορούμε να πούμε πως οι δύο αυτές φάσεις είναι ανεξάρτητες αλλά μας ενδιαφέρει κυρίως η δεύτερη. Αν δηλαδή ένα e-mail με διεύθυνση αποστολέα example@gmail.com έχει αποσταλεί από τον χρήστη “example” ο οποίος χρησιμοποιεί για mail server το “gmail.com” και δεν έχει αποσταλεί από κάποιον άλλο χρήστη ο οποίος χρησιμοποιεί σαν username το “example” και σαν mail server το “gmail.com” αλλά το “gmail.com” είναι ψεύτικο και όχι ο πραγματικός mail server. Το πρόβλημα εδώ είναι ότι ο παραλήπτης έχει λάβει ένα e-mail το οποίο θεωρεί από την διεύθυνση πως είναι από τον πραγματικό αποστολέα ενώ στην πραγματικότητα δεν είναι. Εδώ ακριβώς επεμβαίνει το authentication. Επειδή ο μόνος τρόπος να φανεί αν το e-mail προέρχεται από τον πραγματικό αποστολέα είναι από την IP διεύθυνση του η οποία είναι μοναδική. Το authentication αυτό που ουσιαστικά κάνει είναι να εξοπλίζει τα μηνύματα που αποστέλλονται με αρκετές επαληθεύσιμες πληροφορίες έτσι ώστε οι mail server’s και οι χρήστες να μπορούν να αναγνωρίζουν την φύση του κάθε εισερχόμενου μηνύματος αυτόματα. Η χρήση authentication βοηθά κυρίως στην καταπολέμηση της εξάπλωσης των SPAM και του Phishing.

Υπάρχουν διάφοροι τύποι authentication που χρησιμοποιούνται. Εμείς θα αναφέρουμε τους πιο δύο πιο διαδεδομένους μιας και οι υπόλοιποι αποτελούν παραλλαγές.

7.2.1. DomainKeys Identified Mail (DKIM)

Αυτός ο τύπος authentication αυτό που κάνει είναι να εξασφαλίζει πως η εισερχόμενη αλληλογραφία έχει προέλθει από κάποιον πιστοποιημένο mail server και το περιεχόμενό της δεν έχει μετατραπεί. Επίσης προστατεύει από μηνύματα διαφημιστικού χαρακτήρα και παραπλανητικά μηνύματα που σκοπό έχουν την υποκλοπή στοιχείων πιστωτικών καρτών, τραπεζικών λογαριασμών και γενικότερα ευαίσθητων πληροφοριών. Το DKIM χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού και επιτρέπει στον αποστολέα να υπογράφει ηλεκτρονικά τα e-mail που στέλνει και από τον παραλήπτη εξακριβώνεται η ταυτότητα του αποστολέα.

Πως ακριβώς λειτουργεί. Το DKIM προσθέτει μια κεφαλίδα με την ονομασία “DKIM-Signature” που περιέχει μια ψηφιακή υπογραφή των περιεχομένων (σώμα και κεφαλίδες) του μηνύματος. Οι προεπιλεγμένες παράμετροι για τους μηχανισμούς επαλήθευσης χρησιμοποιούν SHA-256 και κρυπτογράφηση Hash RSA base 64. Ο SMTP server τώρα, χρησιμοποιεί το όνομα του τομέα από τον οποίο προήλθε το e-mail (domain) και κάποια στοιχεία από την κεφαλίδα του μηνύματος για να επαληθεύσει μέσω του DNS server την αυθεντικότητα του αποστολέα. Ο DNS αυτό που επιστρέφει σαν απάντηση είναι ο τομέας και το αντίστοιχο δημόσιο κλειδί. Με αυτό το κλειδί στη συνέχεια ο παραλήπτης μπορεί να διαπιστώσει από την τιμή Hash του μηνύματος (κεφαλίδας και σώματος) αν το μήνυμα έχει ληφθεί ακέραιο ή έχει αλλοιωθεί κατά την μεταφορά του. Τέτοιο τύπο authentication χρησιμοποιούν φορείς όπως το Gmail και το Yahoo.

7.2.2. Sender Policy Framework (SPF)

Το πρόβλημα που έρχεται να λύσει το πρωτόκολλο SPF είναι η πλαστογράφηση της διεύθυνσης του αποστολέα. Σχεδόν σε όλες τις περιπτώσεις τα e-mail που έχουν σκοπό το να πάρουν ευαίσθητες πληροφορίες από τους χρήστες, έχουν σαν διεύθυνση αποστολέα μια ψεύτικη η οποία είναι τέτοια που μπορεί να ξεγελάσει κάποιον. Το πρωτόκολλο SPF ή Sender Policy Framework ξεκίνησε να αναπτύσσεται το καλοκαίρι του 2003 και έφτασε στην τελική του μορφή την άνοιξη του 2004 περνώντας από πολλά στάδια και αλλαγές στον τρόπο λειτουργίας του. Είναι ένα ανοικτό πρότυπο που προσδιορίζει κάποιες τεχνικές για την πρόληψη της πλαστογραφίας της διεύθυνσης του αποστολέα.

Όπως και στην κανονική αλληλογραφία έτσι και στα e-mail υπάρχουν τουλάχιστον δύο τύποι στοιχείων για τη διεύθυνση του αποστολέα. Η “Envelope sender address” ή “return-path” που είναι η διεύθυνση που χρησιμοποιείται για μεταφερθεί ένα ηλεκτρονικό μήνυμα από mail server σε mail server και για να μεταφερθεί πίσω στον αποστολέα αν αποτύχει η αποστολή και συνήθως δεν φαίνεται από τα προγράμματα ηλεκτρονικού ταχυδρομείου. Επίσης υπάρχει και η κεφαλίδα διεύθυνσης του αποστολέα ή “Header sender address” που είναι αυτό που φαίνεται από τα προγράμματα ηλεκτρονικού ταχυδρομείου για τον αποστολέα, δηλαδή η ετικέτα “From” ή “Sender”.

Το SPF συγκεκριμένα δίνει την δυνατότητα στον ιδιοκτήτη του domain να προσδιορίζει τους mail server που θα χρησιμοποιηθούν για την μετάδοση της αλληλογραφίας από τον συγκεκριμένο τομέα. Η τεχνολογία αυτή απαιτεί τις εξής λειτουργίες από δύο πλευρές. Πρώτα απ’ όλα ο ιδιοκτήτης του τομέα δημοσιεύει κάποιες πληροφορίες σε εγγραφές του SPF στον DNS που χρησιμοποιείται και στη συνέχεια ο server που παραλαμβάνει κάποιο e-mail που φαίνεται ότι προέρχεται από κάποιον συγκεκριμένο τομέα ελέγχει την εγκυρότητα του αποστολέα μέσω των στοιχείων που είναι καταχωρημένα στον DNS. Αν το μήνυμα προέρχεται τελικά από άγνωστο διακομιστή μπορεί να θεωρηθεί ψεύτικο. Στην αντίθετη περίπτωση το μήνυμα προωθείται στον τελικό παραλήπτη.

Για να καταλάβουμε καλύτερα το πώς χρησιμοποιείται το SPF πρωτόκολλο θα δώσουμε ένα παράδειγμα. Ας θεωρήσουμε πως ο Bob είναι ο ιδιοκτήτης του domain example.net. Ενίοτε στέλνει e-mail μέσω του λογαριασμού του στο Gmail και επικοινωνεί με το τμήμα υποστήριξης του Gmail για να μάθει την σωστή SPF εγγραφή για το domain του από το Gmail. Από τότε που άρχισε να λαμβάνει απαντήσεις σε μηνύματα που δεν είχε στείλει ο ίδιος αποφάσισε να φτιάξει την δική του SPF εγγραφή για να μειωθεί η πλαστογραφία του domain του. Η εγγραφή ήταν η εξής:

```
Example.net. TXT “v=spf1 mx a:Pluto.example.net include:aspmx.google-mail.com -all”
```

Τα στοιχεία αυτής της εγγραφής σημαίνουν:

v=spf1	SPF έκδοση 1
mx	Οι εισερχόμενοι mail servers (MXes) είναι εξουσιοδοτημένοι από το example.net
a:Pluto.example.net	Ο υπολογιστής Pluto.example.net είναι επίσης εξουσιοδοτημένος
include:aspmx.google-mail.com	Νόμιμα θεωρούνται και όσα προέρχονται από το google-mail.com
-all	Όλοι οι υπόλοιποι υπολογιστές δεν είναι εξουσιοδοτημένοι

8. Απειλές της ασφάλειας δικτύων και του ηλεκτρονικού ταχυδρομείου

8.1. Spoofing

Το spoofing χωρίζεται σε τέσσερεις κατηγορίες. IP spoofing, ARP spoofing, DNS spoofing και SMTP spoofing. Ο όρος spoofing αναφέρεται στην αλλαγή της διεύθυνσης IP (συνήθως), έτσι ώστε ο χρήστης που λαμβάνει ένα e-mail να νομίζει ότι το λαμβάνει από έναν έγκυρο χρήστη, ενώ στη πραγματικότητα δεν είναι έτσι. Το spoofing βασίζεται στο “social engineering” και ουσιαστικά ο “Hacker” προσπαθεί να χειραγωγήσει το θύμα του, δίνοντάς του τη ψευδαίσθηση ότι είναι κάποιος άλλος στον οποίο το θύμα θα εμπιστευόταν τα προσωπικά του δεδομένα. Εκτός αυτού το spoofing χρησιμοποιείται και για επιθέσεις άρνησης υπηρεσιών (DoS – Denial of Service), όπου οι επιθέσεις αυτού του είδους έχουν ως στόχο να γεμίσουν τον υπολογιστή-θύμα με πολλά πακέτα ώστε να τον αναγκάσουν να περιέλθει σε δυσλειτουργία και να μην μπορεί να εξυπηρετήσει σωστά τους νόμιμους χρήστες του. Τέλος ακόμα και για το σπάσιμο των μηχανισμών ασφαλείας δικτύων υπολογιστών, όπου σε πολλά εταιρικά δίκτυα είναι συνηθισμένο η αναγνώριση των χρηστών να γίνεται μέσω των IP διευθύνσεών τους. Στη συνέχεια θα αναφέρουμε μερικά παραδείγματα Spoofing για να κατανοήσουμε ακριβώς πως δουλεύει.

8.1.1. IP Spoofing

Όταν δύο υπολογιστές ανοίγουν μία σύνδεση μεταξύ τους χρησιμοποιώντας TCP/IP ακολουθείται η παρακάτω διαδικασία. Ο Πρώτος στέλνει ένα TCP πακέτο με έναν αρχικό ακέραιο αριθμό. Ο λαμβάνων υπολογιστής επιστρέφει ένα πακέτο το οποίο περιλαμβάνει έναν άλλο ακέραιο (οι αριθμοί αυτοί είναι γνωστοί ως αριθμοί ακολουθίας). Επίσης στέλνει μια επιβεβαίωση η οποία είναι ο αριθμός ακολουθίας του πρώτου συν ένα. Ο πρώτος στη συνέχεια πρέπει να επιστρέψει μια επιβεβαίωση η οποία περιλαμβάνει τον αριθμό ακολουθίας στον άλλο. Από τη στιγμή αυτή, ο πελάτης και ο διακομιστής στέλνουν πακέτα τα οποία περιέχουν αριθμούς ακολουθίας τους οποίους η άλλη πλευρά πρέπει να επιστρέψει για να πιστοποιήσει ότι είναι αυτή που ισχυρίζεται. Οι αριθμοί αυτοί προσδιορίζονται από έναν αλγόριθμο του TCP/IP. Ο εισβολέας για να πετύχει το IP spoofing πρέπει να γνωρίζει τους αριθμούς ακολουθιών που έχουν δημιουργηθεί από τους άλλους δύο υπολογιστές.

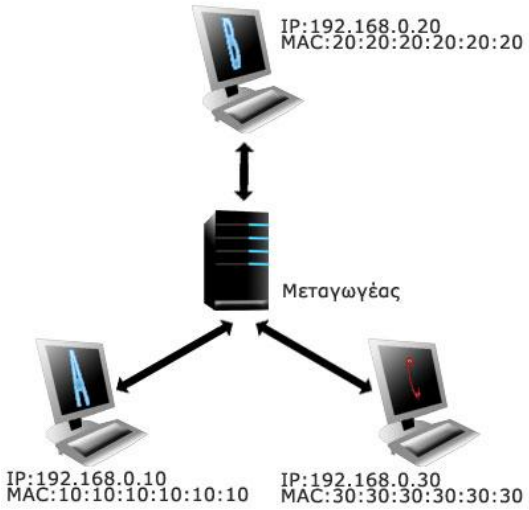
Οπότε για να αποδειχθεί επιτυχημένη μία τέτοια απόπειρα IP spoofing ο εισβολέας πρέπει να ξεπεράσει τα εξής εμπόδια:

- Ο πραγματικός υπολογιστής που θα προσποιηθεί ότι είναι, θα πρέπει να είναι εκτός λειτουργίας. Συνήθως αυτό το πετυχαίνει με μια επίθεση DoS (άρνησης υπηρεσιών).
- Ο υπολογιστής του εισβολέα θα πρέπει να πάρει τη διεύθυνση του υπολογιστή που θα προσποιηθεί και να συνδεθεί με τον διακομιστή για να ξεκινήσει έναν διάλογο προσποιούμενος ότι είναι κάποιος άλλος υπολογιστής.
- Ο εισβολέας πρέπει να ανακαλύψει τον αριθμό ακολουθίας που έχει δημιουργήσει ο διακομιστής.

Από τη στιγμή που κάνει τα παραπάνω η συνέχεια είναι πολύ πιο εύκολη.

8.1.2. ARP spoofing (Address Resolution Protocol)

Το ARP είναι το κομμάτι του TCP-IP, που συνδέει τις φυσικές διευθύνσεις των υπολογιστών (π.χ. της κάρτας δικτύου) με τις IP διευθύνσεις. Η επίθεση ARP spoofing πραγματοποιείται μεταβάλλοντας την ARP cache (τμήμα του λειτουργικού συστήματος το οποίο αποθηκεύει τα απαραίτητα στοιχεία για να γίνεται η μετατροπή των διευθύνσεων από φυσικές σε IP) ώστε η IP διεύθυνση ενός υπολογιστή που ο διακομιστής εμπιστεύεται στην πραγματικότητα να ισοδυναμεί με τη φυσική διεύθυνση του υπολογιστή του εισβολέα. Για να πραγματοποιηθεί όμως μια τέτοια επίθεση, ο Cracker θα πρέπει να βρίσκεται στο ίδιο δίκτυο με αυτόν που θέλει να εξαπατήσει.



Εικόνα 20 - Man-in-the-middle attack

Στο παραπάνω παράδειγμα βλέπουμε πως ο Cracker C προσπαθεί να εξαπατήσει τους χρήστες A και B. Σκοπός του C είναι να «μπει ανάμεσα» από τον A και τον B, όπου για να το πετύχει αυτό στέλνει πακέτα ARP στον A με διεύθυνση πρωτοκόλλου 192.168.0.20 και διεύθυνση MAC 30:30:30:30:30:30. Με τον ίδιο τρόπο εξαπατά και τον B. Οπότε όταν οι A και B θα θέλουν να ανταλλάξουν αρχεία θα χρησιμοποιούν τη διεύθυνση MAC του C (παράδειγμα ανταλλαγής μηνυμάτων μεταξύ A και B δηλαδή C, 192.168.0.20 **à** 30:30:30:30:30:30). Παρόλα αυτά για να μη γίνει αντιληπτός ο C θα πρέπει να προωθεί τα μηνύματα που δεν απευθύνονται σε αυτόν, στον νόμιμο παραλήπτη τους. Έτσι οι δύο χρήστες δεν θα καταλάβουν ότι η επικοινωνία τους παρακολουθείται.

8.1.3. DNS Spoofing

Η λιγότερο σημαντική επίθεση από όλες είναι η DNS Spoofing όπου ο Cracker μεταβάλει τα στοιχεία ενός DNS Server ώστε να αντιστοιχεί το συμβολικό όνομα κάποιου υπολογιστή που εμπιστεύονται οι χρήστες, στην IP διεύθυνση ενός υπολογιστή που χρησιμοποιείται από τον εισβολέα. Οπότε οι υπολογιστές που προσπαθούν να συνδεθούν με τον υπολογιστή που εμπιστεύονται θα συνδέονται στην πραγματικότητα με κάποιον άλλο υπολογιστή, κατά τη διάρκεια της επικοινωνίας με τον οποίο θα μπορούσαν να αντληθούν σημαντικά δεδομένα.

8.1.4. Spoofing μέσω SMTP

Το SMTP standard όσο παράξενο και αν φαίνεται, δεν παρέχει κάποια ασφάλεια (RFC 2821) και με αυτό τον τρόπο οποιοσδήποτε μπορεί να αλλάξει το πεδίο From: του ηλεκτρονικού μηνύματος. Τώρα θα δούμε την απλούστερη μορφή μιας τέτοιας επίθεσης σε βάθος. Για αρχή ο Cracker ανοίγει μια σύνδεση στην πόρτα επικοινωνίας του SMTP (tcp-25) server του θύματος και δίνει τις εξής εντολές:

```
[Cracker]   telnet victims.mailserver.org
[Server]    220 victims.mailserver.org
[Cracker]   hello asxeto.org
[Server]    250  victims.mailserver.org  Hello  asxeto.gr  [Crackers  IP
sender], pleased to meet you
[Cracker]   rcpt to:victim@mailserver.org
[Server]    250 victim@mailserver.org …Recipient ok
[Cracker]   data
[Server]    354 Enter mail, end with “.” On a line by itself
[Cracker]   From: your.boss@mailserver.org
```

```
[Cracker]   To: victim@mailserver.org
[Cracker]   Subject: Παρακαλώ στείλε μου το password
[Cracker]   <μια κενή γραμμή>
[Cracker]   Γεια σου εργαζόμενέ μου. Έξχασα το password για το banking
application και δεν έχω πρόσβαση στο εταιρικό δίκτυο. Παρακαλώ στείλε μου
το password στο hotmail account μου που είναι boss123@hotmail.com
[Cracker]   ευχαριστώ
[Cracker]   <CR><LF>.<CR><LF>
[Server]    250 Message accepted for delivery
(η τελευταία ακολουθία είναι ένα Enter, μία τελεία και μετά πάλι ένα
Enter.)
```

Μέσα από αυτό τον κώδικα βλέπουμε πως τα στοιχεία που εμφανίζονται στον mail client μας (π.χ. Outlook 2003) είναι αυτά που καταχωρήθηκαν μετά το **DATA**. Έτσι αφού ο Cracker άλλαξε το From: ώστε να φαίνεται το αφεντικό του θύματος προσέχοντας να βάλει το mailserver.org μιας και δεν θα μπορούσε να είναι άσχετο το e-mail του recipient (θα ήταν ανώφελο να προσπαθήσει να κάνει spoofing στον mail server της Microsoft και σαν παραλήπτη να έβαζε κάποιο χρήστη του οποίου το e-mail τελειώνει σε @asxeto.net) και επειδή δεν είναι σίγουρο αν θα μπορεί να διαβάσει τα μηνύματα που θα στείλει το θύμα στο «αφεντικό» του προσπαθεί να το εξαπατήσει ζητώντας να λάβει την απάντηση στο web mail του.

Ας δούμε τώρα τις πληροφορίες που προστίθενται στο Header ενός e-mail κατά την αποστολή του και τι σημαίνουν. Πριν όμως πάμε πρέπει να πούμε ότι αυτό είναι ένα απλουστευμένο παράδειγμα μιας και το e-mail είναι πολύ πιθανό να μη φτάσει από τον έναν υπολογιστή άμεσα στον άλλο και να πρέπει να περάσει από πολλούς mail servers μέχρι να καταλήξει στον τελικό, οπότε και θα έχει προστεθεί αρκετή παραπάνω πληροφορία. Το σημαντικό όμως είναι ότι τα σημαντικά στοιχεία που θα πούμε παραμένουν ίδια.

Ανάλυση του Internet Header (όλη τη δομή μαζί θα τη παρουσιάσουμε παρακάτω για να κάνουμε ένα συγκριτικό)

Microsoft Mail Internet Headers Version 2.0

Αυτός ο Header μπαίνει από το Outlook του αποστολέα

Received: from mail.litwareinc.com ([10.54.108.101]) by mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);

Wed, 15 Dec 2004 13:39:22 -0800

Αυτός ο Header μας ενημερώνει πως κάποιος υπολογιστής με όνομα mail.litwareinc.com πήρε μήνυμα από τον υπολογιστή με όνομα mail.proseware.com στις 13:39:22 την 15η Δεκεμβρίου 2004 (Λογικά αυτοί οι δύο υπολογιστές είναι mail servers).

Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com with Microsoft SMTPSVC(6.0.3790.0);

Wed, 15 Dec 2004 13:38:49 -0800

Αυτός ο header μας ενημερώνει πως με τη σειρά του, ο mail.litware.com πήρε το μήνυμα από κάποιον υπολογιστή με όνομα mail στις 13:38:49 την 15η Δεκεμβρίου 2004. Από τη στιγμή που στη συνέχεια δεν έχουμε κάποιο άλλο Header που να ξεκινάει με "Received:", θεωρούμε πως ο υπολογιστής με όνομα mail και διεύθυνση IP 10.54.108.23 είναι ο υπολογιστής από τον οποίο ξεκίνησε το μήνυμα (αν και αυτό δεν ισχύει πάντα μιας και υπάρχουν τρόποι απόκρυψης του υπολογιστή που αρχικοποιεί το μήνυμα).

From: "Kelly Weadock" kelly@litware.com

Ο συγκεκριμένος header μας ενημερώνει πως το μήνυμα φαίνεται να έχει έρθει από κάποιο χρήστη με διεύθυνση e-mail kelly@litware.com

To: <anton@proseware.com>

Εδώ βλέπουμε το όνομα του παραλήπτη του μηνύματος.

Subject: Review of staff assignments

Αυτός ο header περιέχει το subject του μηνύματος.

Date: Wed, 15 Dec 2004 13:38:31 -0800

Ο συγκεκριμένος header περιέχει την ημερομηνία που ο αποστολέας έστειλε το μήνυμα. Η ημερομηνία αυτή έγινε generate στον υπολογιστή του αποστολέα, έτσι αν ο αποστολέας είχε λανθασμένη ημερομηνία στον υπολογιστή του αυτό θα φανεί στο συγκεκριμένο header.

MIME-Version: 1.0

Αυτός ο header μπαίνει από το Outlook και περιγράφει την έκδοση του πρωτοκόλλου MIME που χρησιμοποίησε ο αποστολέας.

Content-Type: multipart/mixed;

Ο σκοπός του συγκεκριμένου header είναι να δώσει οδηγίες στον e-mail client του παραλήπτη για να μπορέσει να κάνει format το μήνυμα σωστά.

X-Mailer: Microsoft Office Outlook, Build 11.0.5510

Αυτός ο header αναφέρει την ακριβή έκδοση του Outlook που χρησιμοποιήθηκε για να σταλεί αυτό το μήνυμα.

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165

Περισσότερες πληροφορίες για τον e-mail client που χρησιμοποίησε ο αποστολέας.

Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==

Αυτός ο header χρησιμοποιείται για να γίνει λογική σύνδεση μηνυμάτων που ανήκουν στο ίδιο thread. Αυτό μπορεί να χρησιμοποιηθεί για παράδειγμα από το Outlook, όταν κάνουμε group τα μηνύματα βάση conversation (από το κεντρικό μενού του Outlook επιλέγουμε View – Arrange by – Conversation).

Return-Path: kelly@litware.com

Ο συγκεκριμένος header μας ενημερώνει για το πως μπορούμε να επικοινωνήσουμε με τον αποστολέα (π.χ. όταν επιλέγουμε να του στείλουμε ένα reply).

Message-ID: MAILbbnewS5TqCRL00000013@mail.litware.com

Κάθε μήνυμα παίρνει ένα message-ID από τον server του αποστολέα. Το μήνυμα κρατάει το ίδιο message id καθ' όλη τη διάρκεια της ζωής του. Επειδή ακριβώς το μήνυμα μπαίνει από τον originating mail server, συνήθως θα παρατηρήσουμε ότι διατηρεί και κάποιο χαρακτηριστικό γνώρισμα (πχ @mail.litware.com).

X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC) FILETIME=[2E0D4910:01C38DDC]

Αυτός είναι ένας header που μπαίνει στο μήνυμα την πρώτη φορά που θα περάσει από έναν Microsoft Exchange Server.

Εδώ έχουμε τη δομή του παραπάνω Header (από ένα κανονικό e-mail)

```
1) Microsoft Mail Internet Headers Version 2.0
2)    Received:    from    mail.litwareinc.com    ([10.54.108.101])    by
mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com
with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Kelly Weadock" kelly@litware.com
5) To: anton@proseware.com
6) Subject: Review of staff assignments
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
```

```
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Return-Path: kelly@litware.com
14) Message-ID: MAILbbnewS5TqCRL00000013@mail.litware.com
15)    X-OriginalArrivalTime:    15    Dec    2004    21:38:50.0145    (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

Και πάμε να δούμε τη δομή από ένα spoofed e-mail. Στη προκειμένη περίπτωση θα στείλουμε e-mail πάλι στον anton@proseware.com αλλά αυτή τη φορά ως ceo@proseware.com. Αυτό το οποίο θα πρέπει να ελέγξουμε είναι αν στους Internet Headers υπάρχουν πληροφορίες οι οποίες μοιάζουν ξένες ως προς το δικό μας δίκτυο.

```
1) Microsoft Mail Internet Headers Version 2.0
2)    Received:    from    mail.litwareinc.com    ([10.54.108.101])    by
mail.spoofers.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3)  Received:  from  spoofer  ([10.10.105.123])  by  mail.spoofers.com  with
Microsoft                                              SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Company CEO" ceo@proseware.com
5) To: anton@proseware.com
6) Subject: Please send me my dialup password at ceo@niamodekaf.com
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Message-ID: MAILbbnewS5TqCRL00000013@mail.spoofers.com
14)    X-OriginalArrivalTime:    15    Dec    2004    21:38:50.0145    (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

Εδώ παρατηρούμε ότι στις γραμμές δύο και τρία αναφέρουν δρομολόγηση από servers που δεν θα έπρεπε να βρίσκονται εκεί. Από τη στιγμή που το μήνυμα είναι εσωτερικό δεν θα έπρεπε να βλέπουμε ξένους servers. Επίσης στη γραμμή 13 έχουμε περιεχόμενο που είναι και αυτό «ξένο» ως προς το δίκτυό μας.

Παρόμοιο έλεγχο για spoofing μπορούμε να κάνουμε και από εξωτερική πηγή (δηλαδή από e-mails που προέρχονται από το Internet) και το Internet Header τους έχει ως εξής:

```
1) Microsoft Mail Internet Headers Version 2.0
2) Received: from mail.litwareinc.com ([10.54.108.101]) by
mail.spoofers.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:39:22 -0800
3) Received: from spoofer ([10.10.105.123]) by mail.spoofers.com with
Microsoft SMTPSVC(6.0.3790.0);
Wed, 15 Dec 2004 13:38:49 -0800
4) From: "Microsoft Technical Support" support@microsoft.com
5) To: anton@proseware.com
6) Subject: Change in security policy requires that you change your Hotmail
password to p@ssw0rd
7) Date: Wed, 15 Dec 2004 13:38:31 -0800
8) MIME-Version: 1.0
9) Content-Type: multipart/mixed;
10) X-Mailer: Microsoft Office Outlook, Build 11.0.5510
11) X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
12) Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+IPA==
13) Message-ID: MAILbbnewS5TqCRL00000013@mail.spoofers.com
14) X-OriginalArrivalTime: 15 Dec 2004 21:38:50.0145 (UTC)
FILETIME=[2E0D4910:01C38DDC]
```

8.2. Dialers

Οι Dialers στις μέρες μας δεν αποτελούν σοβαρό κίνδυνο. Μόνο για όσους χρήστες μπαίνουν στο διαδίκτυο με modem τύπου 56k. Αλλά ως φαίνεται σε λίγο καιρό κανένας χρήστης δεν θα αντιμετωπίζει τους Dialers ως απειλή. Παρόλα αυτά θα το αναφέρουμε διότι για αρκετά μεγάλο χρονικό διάστημα ήταν πολύ μεγάλη μάστιγα στο διαδίκτυο.

Οι Dialers είναι μικρά προγράμματα (50-80kb) τα οποία αποσυνδέουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Internet (ISP) και καλούν αυτόματα αριθμούς υψηλής χρέωσης (π.χ. 090, 901, 00xx κ.α.), οι οποίοι είναι για πρόσβαση σε συγκεκριμένες υπηρεσίες. Φυσικά αυτή η κίνηση γίνεται χωρίς τη συνειδητή συγκατάθεση του χρήστη. Η δημιουργία τους αρχικά ήταν για να γίνετε άμεσα η πληρωμή των συγκεκριμένων εταιριών οι οποίες χρησιμοποιούσαν τα dialers, με επίγνωση φυσικά του χρήστη. Η σωστή λειτουργία

τους έχει ως εξής: αν προσπαθήσουμε να επισκεφτούμε μια ιστοσελίδα η οποία προσφέρει ειδικό περιεχόμενο με αυτό τον τρόπο, θα εμφανιστεί στην οθόνη μας ένα παράθυρο διαλόγου το οποίο μας ρωτά αν θέλουμε να κατεβάσουμε το συγκεκριμένο πρόγραμμα dialer. Επίσης μας ενημερώνει για το είδος της υπηρεσίας την οποία πρόκειται να χρησιμοποιήσουμε και για τη χρέωσή της. Αν επιλέξουμε «yes», το λογισμικό του dialer εγκαθιστάτε στον υπολογιστή μας. Το λογισμικό αλλάζει τον αριθμό σύνδεσης στο διαδίκτυο με αυτόν της αυξημένης χρέωσης, ενώ εμείς έχουμε τη δυνατότητα πρόσβασης στο ειδικό περιεχόμενο εφόσον χρεωνόμαστε με αυξημένη τιμολόγηση. Καθ' όλη τη διάρκεια πρόσβασης στο ειδικό περιεχόμενο, υπάρχει στην οθόνη ένδειξη ότι χρησιμοποιείτε σύνδεση στο διαδίκτυο αυξημένης χρέωσης. Στη συνέχεια, μόλις αποσυνδεθούμε από τη συγκεκριμένη ιστοσελίδα, ο dialer αποκαθιστάται από τον υπολογιστή μας και η σύνδεση του modem επιστρέφει στον αριθμό του παρόχου Internet που χρησιμοποιούμε. Αυτό όμως άλλαξε λόγω του «εύκολου χρήματος» και για κάποιο διάστημα αποτέλεσαν μία από τις μεγαλύτερες απειλές στο χώρο του διαδικτύου (λέω αποτέλεσαν διότι τώρα ποια με τις ευρυζωνικές συνδέσεις δεν είναι δυνατό να απειληθούμε από dialers, όμως όσο η είσοδος στο διαδίκτυο γινόταν μέσο dial up και ISDN ήταν από τα ποιο επικίνδυνα προγράμματα, μιας και είχαν άμεσο αντίκτυπο στο λογαριασμό του τηλεφώνου).

Δύο είναι οι συνηθέστεροι τρόποι που δρουν οι dialers και είναι οι εξής:

1. Αλλάζουν τις ρυθμίσεις δικτύου μέσω τηλεφώνου (dial up networking) και μας υποχρεώνουν σαν χρήστη να καλέσουμε έναν συγκεκριμένο αριθμό (από αυτούς που έχουμε προαναφέρει) άγνωστο προς εμάς. Ύστερα διαγράφουν τον αριθμό του ISP που χρησιμοποιούμε και τοποθετούν το δικό τους. Από εκεί και πέρα κάθε φορά που μπαίνουμε μέσω dial up κάνει κλήση στον δικό τους πάροχο και φυσικά έχει και τις ανάλογες χρεώσεις.
2. Ο δεύτερος τρόπος είναι να αναγκάσουν τον υπολογιστή να παρακάμψει τις ρυθμίσεις του δικτύου μέσο τηλεφώνου και να καλέσει ένα συγκεκριμένο αριθμό. Έτσι παρόλο που μπορεί να εμφανίζονται οι προεπιλεγμένες ρυθμίσεις του χρήστη όταν συνδέεται στο Internet, θα καλείται ένας άλλος αριθμός που θα έχει οριστεί από τον dialer.

Οι dialers προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες. Οι οποίες μπορεί να είναι ιστοσελίδες που παρέχουν πειρατικό λογισμικό, πορνογραφικό

περιεχόμενο, ή ιστοσελίδες με αμφιλεγόμενο περιεχόμενο. Οι ιδιοκτήτες αυτών των ιστοσελίδων έχουν ενσωματώσει στο κώδικα της ιστοσελίδας τους τον dialer οπότε αυτός εγκαθίσταται αυτόματα με το που εισέρθουμε ως χρήστης στην ιστοσελίδα. Ο δεύτερος τρόπος που μας ενδιαφέρει κιόλας, είναι μέσο ηλεκτρονικής αλληλογραφίας. Με τη μορφή συνημμένου αρχείου (συνήθως με την ετικέτα ενός δημοφιλούς προγράμματος), όπου εάν το αποθηκεύσουμε και το εκτελέσουμε στον υπολογιστή μας εγκαθιστά εν άγνοιά μας τον dialer.

Η διαφορά του μεγέθους πληρωμής γίνεται αισθητή αν υποθέσουμε πως μία κανονική κλίση είναι 0,0058 ευρώ το λεπτό σε ώρες αιχμής και 0,0029 ευρώ σε μη ώρες αιχμής ενώ μέσο dialer μπορεί να φτάσει και τα 2 ευρώ το λεπτό δηλαδή 689 φορές ακριβότερη από τη χρέωση ΕΠΑΚ.

Υπαρκτά παραδείγματα διεθνών προορισμών από κλήσεις dialers είναι:

Nauru (00674), Solomon Islands (00677) και Wallis and Futuna (00 681). Για την αντιμετώπιση του συγκεκριμένου προβλήματος οι τηλεφωνικές εταιρίες αποφάσισαν να εξυπηρετούνται αυτές οι κλήσεις μέσο ενός «operator» του ΟΤΕ, ώστε να αποφεύγονται ακούσιες κλήσεις μέσω του υπολογιστή. Τέλος η λίστα αυτή ανανεώνεται και τροποποιείται από την ΕΕΤΤ με βάση τα στοιχεία που συλλέγονται.

Πώς μπορούμε να καταλαβαίνουμε ότι έχει εγκατασταθεί dialer στον Η/Υ

- Θα ακούσουμε το modem μας να αποσυνδέεται και να πραγματοποιεί νέα κλήση (βέβαια μερικοί dialers μπορούν να σιγήσουν τους ήχους κλήσης).
- Είναι πιθανό, η ταχύτητα της σύνδεσης μας στο Internet να είναι πολύ χαμηλότερη από ό, τι συνήθως. Μπορεί να υπάρχουν αρκετοί λόγοι που συμβαίνει αυτό αλλά καλό είναι να εξετάσουμε τα (dial up settings)
- Είναι πιθανό, παρά το γεγονός ότι βρισκόμαστε στο διαδίκτυο να μη μπορούμε να στείλουμε ηλεκτρονικά μηνύματα (e-mails)
- Θα λάβουμε λογαριασμό ο οποίος θα είναι απρόσμενα υψηλός και θα έχει κλήσεις σε αριθμούς εξωτερικού ή αυξημένης χρέωσης.

Τι μπορούμε να κάνουμε για να προφυλαχτούμε από τους dialers

- Να κλείσουμε τον υπολογιστή μας όταν δεν τον χρησιμοποιούμε.
- Ποτέ να μην ανοίγουμε συνημμένα αρχεία τρίτων αν δεν γνωρίζουμε τι είναι.

- Θα πρέπει να έχουμε εγκατεστημένο ένα Antivirus (π.χ. Nod32, AGV).
- Κατά καιρούς θα πρέπει να ελέγχουμε τον υπολογιστή μας για spyware.
- Πρέπει να εξετάζουμε συχνά τις παραμέτρους σύνδεσης του Η/Υ μας με το διαδίκτυο για να βεβαιωνόμαστε ποιους αριθμούς καλεί το modem μας.
- Να είμαστε επιφυλακτικοί με τα κλικ που κάνουμε σε «pop up windows» που εμφανίζονται ξαφνικά στην οθόνη μας.
- Να είμαστε ιδιαιτέρα προσεκτικοί στη περιήγηση μας στο διαδίκτυο.
- Να έχουμε δυνατά την ένταση στο modem μας ώστε να ακούσουμε αν πάει να κάνει ανάκληση.
- Να προσέχουμε την επιφάνεια εργασίας μας μήπως μας έχει σωθεί (μόνο του) κανένα εικονίδιο που μας φαίνεται άγνωστο.
- Να ενημερώνουμε όποιον είναι να χρησιμοποιήσει τον υπολογιστή μας, για το κακόβουλο λογισμικό που κυκλοφορεί.
- Να ενεργοποιήσουμε την υπηρεσία φραγής κλήσεων για κλήσεις εξωτερικού και αυξημένων χρεώσεων.

8.3. Phishing

Η λέξη phishing είναι παραλλαγή της λέξης Fishing (ψάρεμα) και η πράξη phishing κάνει αυτό ακριβώς που υποδηλώνει η λέξη. Επίσης το phishing είναι «υποενότητα του spam», αλλά είναι τόσο μεγάλη που αποτελεί απειλή από μόνη της.

Phishing είναι η πρακτική αποστολής ενός μηνύματος ηλεκτρονικού ταχυδρομείου ή ενός στιγμιαίου μηνύματος (εμάς μας αφορά το πρώτο κυρίως) που μοιάζει να προέρχεται από μία πραγματική εταιρία με καλή φήμη (όπως π.χ. τράπεζες, Pay pal, eBay κ.α.) αλλά δεν είναι. Σκοπό έχει να μας ξεγελάσει σαν χρήστες και να μας κάνει να αποκαλύψουμε ευαίσθητα προσωπικά στοιχεία όπως είναι ο αριθμός της πιστωτικής μας κάρτας, pin, ή οτιδήποτε άλλο μπορούν να εκμεταλλευτούν για να κάνουν στη συνέχεια συναλλαγές στις οποίες θα έχουν πρόσβαση σαν να ήταν οι νόμιμοι χρήστες. Υπάρχουν αρκετοί τρόποι για να κάνουν αυτή τη πράξη οι κακόβουλοι χρήστες. Θα παραθέσουμε ορισμένους τώρα και θα δούμε ποιοι είναι ποιο αποτελεσματικοί:

- Μπορούν να μας στείλουν ένα e-mail και να φαίνεται πως το στέλνει (π.χ. η τράπεζά μας) και να μας ζητάει να επαληθεύσουμε τα στοιχεία μας για λόγους ασφαλείας.

- Επίσης με e-mail που μας στέλνει «η τράπεζά μας» πάλι μπορεί να μας λέει ότι έχουμε πρόβλημα με το λογαριασμό μας και να πρέπει να δώσουμε άμεσα τα προσωπικά μας στοιχεία για να μη μας κλείσουν τον λογαριασμό μας. Με αυτό τον τρόπο ο κακόβουλος χρήστης προσπαθεί να μας αγχώσει ώστε να μη προλάβουμε να επαληθεύσουμε το ηλεκτρονικό μήνυμα.
- Μία άλλη ποιο έξυπνη λύση είναι, να μας στείλουν ένα e-mail το οποίο να μας προσφέρει (λέγοντάς μας πως κερδίσαμε) μία εκδρομή για παράδειγμα και να μας ζητάει τον αριθμό της πιστωτικής μας κάρτας για τα μεταφορικά και μόνο.
- Θα μπορούσε να είναι επίσης σαν χριστουγεννιάτικη προσφορά από κάποιον οργανισμό όπως το eBay και να πρέπει να βάλουμε τα προσωπικά μας στοιχεία για να μπούμε άμεσα σε αυτή τη προσφορά.

Υπάρχουν φυσικά και άλλες επιθέσεις, αλλά αυτές είναι οι πιο συχνές. Τώρα ας αναφέρουμε και ποιες μέθοδοι είναι οι ποιο αποτελεσματικές.

Σε γενικές γραμμές η δεύτερη τεχνική δεν είναι ιδιαίτερα αποτελεσματική διότι είναι δυσάρεστα νέα για εμάς ως αναγνώστες, οπότε θα το μελετήσουμε περισσότερο και πιθανό να τηλεφωνήσουμε στη τράπεζά μας για περαιτέρω πληροφορίες. Αυτό έχει ως συνέπεια να μας ενημερώσουνε ότι πρόκειται για εξαπάτηση και να το αποφύγουμε. Για να καταπολεμήσουν αυτό το πρόβλημα οι crackers μας δίνουν ένα πολύ μικρό χρονικό περιθώριο ώστε να μην μπορέσουμε να το σκεφτούμε ή να το μελετήσουμε και να προβούμε στις κινήσεις που μας ζητάνε. Η τρίτη λύση είναι η πιο έξυπνη από όλες διότι τα ευχάριστα νέα είναι πιο εύπεπτα και άμεσος εμείς ως χρήστες για να μη χάσουμε τη προσφορά «τρέχουμε» να δώσουμε τα προσωπικά μας στοιχεία. Αυτό επίσης έχει το καλό ότι μπορούμε να το διασταυρώσουμε πιο δύσκολα και είναι πολύ πιθανό να δώσουμε τα προσωπικά μας δεδομένα. Το πρώτο και το τέταρτο δεν έχουν καμία ιδιαιτερότητα αλλά από ότι βλέπουμε και από ότι θα δούμε από τα παραδείγματα στη συνέχεια λειτουργούν και αυτά εξ ίσου καλά.

Το phishing παλιά δεν αποτελούσε απειλή αλλά τα τελευταία χρόνια έχει αρχίσει να γίνετε μάστιγα αυτό επιβεβαιώνεται και από μία έρευνα που διεξήχθη το 2007 και έδειξε πως ένα στα 87 e-mails είναι phishing mail. Επίσης τα τελευταία χρόνια οι crackers έχουν καταφέρει να κάνουν πολύ πιστές αντιγραφές στα web sites με τα οποία έχουν σκοπό να «ψαρέψουν» και τρανταχτό παράδειγμα είναι το eBay όπου ένας hacker έστειλε ένα υποτιθέμενο χριστουγεννιάτικο e-mail σε χρήστες και όταν

ένας το έκανε προώθηση στο e-bay για να τους πει πως πρόκειται για phishing το eBay του είπε πως κάνει λάθος και όντως έστειλε στα μέλη του τέτοιο e-mail. Παρακάτω θα διαβάσετε την προσωπική εμπειρία του χρήστη:

Στα τέλη Νοεμβρίου, ο Richi Jennings, ανεξάρτητος ερευνητής που μελετά θέματα ασφαλείας και διαδικτυακής απάτης, έλαβε ένα e-mail με θέμα "Christmas is Coming on ebay.co.uk" (Τα Χριστούγεννα έρχονται στο ebay.co.uk). Το μήνυμα προσέφερε συμβουλές για επιτυχημένες χριστουγεννιάτικες αγορές και παρέπεμπε στο site ebaychristmas.net. Στο συγκεκριμένο site ο Jennings είδε ότι πρέπει να εισάγει το username και το password που χρησιμοποιεί στο eBay, καθώς και το όνομα και το password για το e-mail του.

Αντιλαμβανόμενος ότι η όλη κατάσταση φαινόταν τουλάχιστον ύποπτη, ο Jennings ανέφερε στο eBay την ύπαρξη του συγκεκριμένου e-mail στις 25 Νοεμβρίου. Η εταιρεία απάντησε τέσσερις μέρες αργότερα πως πρόκειται για πραγματικό e-mail που είχε σταλεί εκ μέρους της εταιρείας στον ίδιο. Ωστόσο, ο Jennings πεπεισμένος για την απάτη έστειλε νέο e-mail στο eBay τονίζοντας και πάλι την προσπάθεια εκμετάλλευσης αθώων χρηστών. Τη Δευτέρα 5 Δεκεμβρίου, εκπρόσωπος του eBay επιβεβαίωσε ότι πράγματι το συγκεκριμένο e-mail ήταν ψευδές, ωστόσο δεν μπόρεσε να δώσει ξεκάθαρη απάντηση για τους λόγους που δεν εντοπίστηκε η απάτη από το πρώτο e-mail του Richi Jennings.

Είναι πολύ πιθανό η ομάδα έρευνας απάτης του eBay να ξεγελάστηκε από άλλο παρόμοιο e-mail που είχε στείλει η εταιρεία και να μην έδωσε την απαιτούμενη προσοχή στην παρατήρηση του Jennings. Μάλιστα, το eBay τόνισε πως ήδη από τις 8 Νοεμβρίου - αρκετές ημέρες πριν την πρώτη επικοινωνία του Jennings - γνώριζε για το συγκεκριμένο site και είχε κινήσει διαδικασίες για την αναστολή λειτουργίας του.

Η αδυναμία του eBay να εντοπίσει μία phising απάτη, ακόμη και τη στιγμή που έλαβε στοιχεία για αυτήν, δείχνει πόσο προσεγμένες έχουν γίνει οι επιθέσεις του είδους και τη δυσκολία να τις εντοπίσει πλέον κάποιος από την πρώτη στιγμή. Όσο για τον Richi Jennings, παραθέτει την εκτεταμένη άποψή του για το θέμα στο blog του (http://richi.co.uk/blog/2005/12/ebays-anti-phishing-desk-sucks.html) και δηλώνει πρόθυμος να δώσει στο eBay μία δεύτερη ευκαιρία.

Ο λόγος που καταφέρνουν να κάνουν τόσο πιστές αντιγραφές είναι, ότι αντιγράφουν τον κώδικα της σελίδας και αλλάζουν μόνο τα σημεία τα οποία τους ενδιαφέρουν ώστε να πάρουν τα προσωπικά δεδομένα του χρήστη. Η Ελλάδα ευτυχώς λόγο της δυσκολίας που έχει η γλώσσα της είναι αρκετά προστατευμένη από τέτοιες επιθέσεις αλλά όχι απόλυτα. Αυτό δείχνει και η επίθεση ενός phishing mail που υποτίθεται ότι το έστελνε η City bank στους πελάτες της και ήταν το εξής:

```
Κλεισιματος των λογαριασμων και περιοριζοντας την προσβαση στο λογαριασμο Ο
λογαριασμος σας εχει Limited. Εμεις που αναθεωρηθηκε προσφατα στοιχεια της
πιστωτικης σας καρτας, και φαινεται οτι χρησιμοποιειτε την ιδια πιστωτικη
καρτα για 2 λογαριασμους. Οπως μπορειτε να διαβασετε και μας User Agreement
(τμημα 2.13) δημιουργια πολλαπλων λογαριασμων ειναι αυστηρα απαγορευμενη.
Ειστε τωρα καλειται να παρασχει πληροφοριες σχετικα με το λογαριασμο σας.
CitiBank θα διερευνησει το θεμα γρηγορα και αν η ερευνα ειναι υπερ σας, θα
αποκαταστησει το λογαριασμο σας.
Καντε κλικ εδω για να επαναφερετε το λογαριασμο σας
```

Η απαράδεκτη σύνταξη του κειμένου δείχνει πως το έγραψε κάποιος που δεν γνωρίζει καλά ελληνικά ή έγινε η μετάφραση από αυτόματο μεταφραστή. Επίσης στάλθηκε και σε χρήστες που δεν διαθέτουν λογαριασμό ούτε κάρτα σε αυτή την τράπεζα. Προφανώς κάποιοι έστειλαν δεκάδες χιλιάδες e-mail ελπίζοντας πως κάποιοι θα κάνουν click στην παραπομπή ώστε να επαναφέρουν το λογαριασμό τους, δίνοντας έτσι τα προσωπικά τους στοιχεία τους πονηρούς αποστολείς του μηνύματος.

Τη προηγούμενη μέρα ο ίδιος χρήστης έλαβε άλλο ένα παρόμοιο μήνυμα:

```
Αγαπητε πελατη
Μπορειτε εχουν βραβευθει με κουπονι για 100 eur.
Δωροεπιταγη code: 11245325932
για να συλλεξουμε παρακαλω συνδεθειτε και να εισαγετε το κωδικο κουπονιου
παραπανω.
Παρακαλω επιτρεψτε 3-5 μερες για μεταποιηση.
Copyright © winbank 2008
```

Ευτυχώς όπως βλέπουμε ακόμα είναι εύκολο να καταλάβουμε πότε είναι απάτη κυρίως από το συντακτικό και την ορθογραφία, το θέμα είναι για πόσο ακόμα?

Ένα τελευταίο παράδειγμα phishing είναι αυτό που είχαν κάνει χρησιμοποιώντας ως πρόφαση την Alpha bank και ήταν το εξής:

```
"Αγαπιτέ πελάτη της Ιντερνέτ-Τράπεζας!
Επειδή η κατάσταση με Online - Τράπεζες στη χώρα μας είναι σήμερα πολύ
δύσκολη, η κυβέπνιση της Ελλάδας παρακάλησέ μας να κάνουμε τον έλεγχο για
όλους τους Online - λογαριασμούς της δηκής ! μας τράπεζας να μάθουμε αν
υπάρχουν "λογαριασμοί μιας μέρας", τους οποίους χρησημοποιούν οι
εγκληματίες για να αποπλύνονται τα κλεμμένα λεφτά. Δια ταυτα σας
παρακαλούμε πολύ &sigm! a;οβαρά να συμ& pi;ληρώσετε το ερωτηματολόγιο της
επιβεβαιώσεις λόγαριασμού στη επίσημη μας Ιντερμετ-σελήδα.
Οι λογαριασμοί, που δε θα επιβεβαιοθούν ως της 27.11.05, θα παγώνονται για
ακαθόριστο καιρό πριν γίνει φανερό πως ακριβώς έχουν δημιουργηθεί και
εκμεταλευθεί. Ο έλεγχος αυτος είν&alph! a;ι επίκαιρος οχι μόνο για
ιδιωτικούς μας πελάτες, αλλα για όλους σας.
ΝΑ ΣΥΜΠΛΗΡΩΣΩ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ
Σας ζητούμε συγνώμη για τις ενοχλήσεις που προκύπται απο τη διαταγή της
παρούσες εκδήλωσης και ελπίζουμε για την κατανόηση και την βοήθειά σας.
Με σεβασμό,

Υπηρεσία ασφάλειος
Τράπεζα Alpha Bank"
```

Το link "ΝΑ ΣΥΜΠΛΗΡΩΣΩ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ" οδηγεί σε δικτυακό τόπο. Και εδώ φαίνεται η πολύ κακή μετάφραση από τους αυτόματους μεταφραστές που χρησιμοποιούνε οι crackers. Αυτό που ξανά τονίζουμε είναι πως οι μεταφραστές θα βελτιωθούν οπότε δεν πρέπει να επαναπαυόμαστε και πρέπει να βρούμε τρόπους για να αποφύγουμε το phishing.

Πως μπορούμε να προστατευθούμε από το phishing;

Δεν είναι καθόλου εύκολη και απλή υπόθεση να προστατευθεί κανείς από το phishing και αυτό έγκειται στο ότι το phising δεν πάει να χτυπήσει Hardware, δηλαδή σύστημα του υπολογιστή μας οπότε ένα καλό anti virus να μας προστατεύσει, αλλά χτυπάει κατευθείαν στον χρήστη και στη ψυχολογία του. Αυτό σημάνει πως το κρίσιμο σημείο ασφάλειας δεν βρίσκετε πια στον υπολογιστή αλλά βρίσκεται επάνω μας. **ΌΤΙ ΧΕΙΡΌΤΕΡΟ** και αυτό φαίνεται από τα λόγια ενός πολύ γνωστού social engineer hacker του Kevin Mitnick ο οποίος όταν βγήκε από τη φυλακή εξέδωσε ένα βιβλίο τονίζοντας την εξής φράση. *«Ο άνθρωπος είναι ο πιο αδύναμος κρίκος σε*

οποιοδήποτε σύστημα ασφαλείας». Παρόλα αυτά θα αναφέρουμε μερικούς τρόπους που μπορούν να μειώσουν τις πιθανότητες εξαπάτησής μας, αλλά σε αυτού του είδους τις απάτες το σημαντικότερο όλων είναι η σωστή ενημέρωσή μας και η αυτοσυγκράτησή μας.

Τρόποι αποφυγής εξαπάτησης phishing:

- Πρέπει να είμαστε σίγουροι ότι τα λειτουργικά μας συστήματα έχουν τις τελευταίες ενημερώσεις στα προγράμματα ασφαλείας αλλά και γενικότερα στα βασικά τους προγράμματα λειτουργίας όπως π.χ. στα windows είναι απαραίτητο το service pack 2 ή και 3, διότι εμποδίζει την εμφάνιση πλαστογραφημένων διευθύνσεων.
- Μπορούμε να ρυθμίσουμε τα φίλτρα του Outlook (αν χρησιμοποιούμε) ώστε να φιλτράρει τα phishing mails προτού φτάσουν σε εμάς. Φυσικά όπως προείπαμε επειδή είναι ιδιαίτερη η κατηγορία phishing ίσως τα φίλτρα να κριθούν ελαφρός αναποτελεσματικά.
- Το κυριότερο όλων να είμαστε ενήμεροι και να συνεχίζουμε να ενημερωνόμαστε, διότι με τον καιρό αλλάζει και ο τρόπος που γίνονται οι επιθέσεις.
- Να ελέγχουμε τις πηγές από όπου λαμβάνουμε τα e-mail μας και να ήμαστε πάντα υποψιασμένοι. Επίσης να κοιτάμε αν είναι secure οι διευθύνσεις στις οποίες μας πηγαίνουνε τα διάφορα links από τα e-mail και αυτό φαίνεται από το http**s** (το τελευταίο s υποδηλώνει το secure). Άλλο ένα είναι το «λουκέτο» που εμφανίζεται πάνω δεξιά στη διεύθυνση το οποίο δείχνει πως η ιστοσελίδα χρησιμοποιεί κάποιο πιστοποιητικό.

Τέλος για την ασφάλεια ψάχνουν τρόπο και οι μεγάλοι οργανισμοί όπως οι τράπεζες, Microsoft, eBay κ.α. διότι πια τα πλήγματα από το phishing αρχίζουν να διευρύνονται και χρειάζεται κινητοποίηση και από τους μεγάλους οργανισμούς.

8.4. E-mail bomb

Ο όρος e-mail bomb, αναφέρεται σε ένα είδος επίθεσης κατά την οποία ο επιτιθέμενος «βομβαρδίζει» (δηλαδή στέλνει τεράστιες ποσότητες ηλεκτρονικών μηνυμάτων) σε μία διεύθυνση ηλεκτρονικού ταχυδρομείου με σκοπό να γεμίσει το διαθέσιμο χώρο του δίσκου ή της εικονικής μνήμης του server και να προκαλέσει δυσλειτουργία στον server και στον ηλεκτρονικό υπολογιστή. Το e-mail bomb

διαφέρει από το spamming διότι όπως προείπαμε στέλνει ο “hacker” πολλά μηνύματα σε συγκεκριμένο υπολογιστή και όχι γενικός σε πληθώρα ηλεκτρονικών διευθύνσεων όπως συμβαίνει στα spam.

Υπάρχουν δύο τρόποι διακίνησης των e-mail bombs. Ο πρώτος τρόπος συνίσταται στη μαζική αποστολή μηνυμάτων από ένα πρόγραμμα που φτιάχνει ο ίδιος ο cracker (το οποίο είναι αρκετά απλό να φτιαχτεί) και το οποίο βομβαρδίζει τον εκάστοτε υπολογιστή. Αυτός ο τρόπος όμως δεν είναι ιδιαίτερα αποτελεσματικός αφού είναι εύκολο να εντοπιστεί η διαδικασία από έναν server και να την εντάξει στα spam. Ο δεύτερος τρόπος και αποτελεσματικότερος ονομάζεται DDoS – Distributed Denial of Service. Κατά την επίθεση αυτή ο cracker δίνει εντολή σε υπολογιστές «bots» ή «ζόμπι» να στείλουν μαζικά e-mails σε μία διεύθυνση. Η διαφορά τους έγκειται στο ότι στέλνονται τα e-mails από διαφορετικά ID οπότε και είναι δυσκολότερο στους Servers να διαπιστώσουν ότι είναι spam. Αυτός ο τρόπος όμως προϋποθέτει την εγγραφή του e-mail του θύματος σε διάφορες διαδικτυακές υπηρεσίες όπως (mailing lists, Newsletters κ.α.). Αν ο cracker καταφέρει να «γράψει» το θύμα σε πολλές τέτοιες υπηρεσίες τότε το θύμα θα παραλαμβάνει δεκάδες e-mails καθημερινά, γεμίζοντας με αυτό τον τρόπο τον σκληρό δίσκο του mail server του. Για την αποφυγή τέτοιων κρουσμάτων, είναι υποχρεωτικό πια να στέλνεται ένα e-mail επιβεβαίωσης ότι θέλουμε την εγγραφή σε μία τέτοια λίστα.

Επίσης μια παραλλαγή των e-mail bombs (και μάλιστα πιο δραστική) είναι οι ZIP Bombs. Ο τρόπος επίθεσης είναι όπως και παραπάνω δηλαδή στέλνονται εκατοντάδες, χιλιάδες ή ακόμα και εκατομμύρια e-mails σε έναν λογαριασμό, αλλά αυτή τη φορά έχουν συνημμένο ένα αρχείο το οποίο είναι σε μορφή ZIP, RAR, 7-ZIP (δηλαδή συμπιεσμένο) και περιλαμβάνει ένα έγγραφο κειμένου το οποίο έχει επαναλαμβανόμενο αρκετές φορές το γράμμα π.χ. «a» (διαλέγουν γράμματα τα οποία να δέχονται μεγάλη συμπίεση, διότι ως γνωστόν δεν συμπιέζονται όλα τα γράμματα το ίδιο). Όταν αυτό είναι συμπιεσμένο, το αρχείο πιάνει πολύ μικρό όγκο, όταν όμως ο mail server προσπαθήσει να αποσυμπιέσει τα e-mails για να ελέγξει για ιούς θα καταλήξει να αποσυμπιέζει έναν τεράστιο όγκο αρχείων τα οποία ενδέχεται να προκαλέσουν και το «πάγωμα» του mail server οπότε και τη γενικότερη δυσλειτουργία του συστήματος.

Αυτού του είδους οι επιθέσεις έχουν αρχίσει να μην είναι πια ιδιαίτερα απειλητικές διότι τα φίλτρα των e-mail servers είναι σε θέση να ξεχωρίσουν αρκετά καλά πότε δεχόμαστε e-mail bombs και ακόμα και όταν αποσυμπιέζουν τα zip bombs έχουν αρκετή μνήμη και δυνατούς επεξεργαστές ώστε να μην «παγώσει» το σύστημα.

Φυσικά όμως αν τελικά καταλήξουν στην ταχυδρομική μας θυρίδα τόσες εκατοντάδες e-mails θα μας είναι δυσάρεστο σαν χρήστες να πρέπει να δούμε ποια και πόσα e-mails πρέπει να διαγράψουμε από το «Inbox» μας.

8.5. Hoaxes ή Urban Legends

Η ονομασία Hoaxes προέρχεται από το Hocus Pocus (μία μαγική λέξη σαν το άμπρα κατάμπρα). Το Urban Legends σημαίνει αστικοί θρύλοι και δίνουν ακριβώς την ερμηνεία αυτών των e-mails, μιας και είναι φήμη ή θρύλος ο οποίος «περιφέρεται» στο διαδίκτυο. Το περιεχόμενο που έχουν συνήθως τα Hoaxes ή Urban Legends δεν διαφέρει πολύ από αυτό:

- *Διαμαρτυρία για την κακομεταχείριση των γυναικών στο Αφγανιστάν.*
- *Αποστολή χριστουγεννιάτικων καρτών σε ετοιμοθάνατα παιδιά.*
- *Προτάσεις φορολόγησης όσων δεδομένων διακινούνται μέσω Internet.*
- *Φυλακτά καλής τύχης ή κατάρες ακρωτηριασμού και καταστροφής.*

Τα hoaxes είναι e-mails που διακινούνται στο διαδίκτυο και δημοφιλέστερό τους θέμα είναι οι Ιοί (*π.χ. μη διαβάσετε e-mail με subject "Good Times" διότι θα καταστραφεί ο Η/Υ σας).*

Επίσης άλλες μεγάλες κατηγορίες τους είναι τα Συμπαράστασης τα οποία παρουσιάζουν προβλήματα κάποιου υποθετικά άρρωστου ανθρώπου και ζητούν τη μεγαλύτερη κινητοποίηση των χρηστών. Ενώ υπάρχει και η κατηγορία Εκφοβισμού τα οποία μπορεί να μας απειλεί ότι θα μας συμβεί κάτι τρομερό αν δεν το προωθήσουμε άμεσα.

Υπάρχουν αρκετοί τρόποι για να αναγνωρίσουμε τα Hoaxes και είναι οι εξής:

1. Οι συγγραφείς τους χρησιμοποιούν επιστημονικούς όρους για να γίνουν πιο πιστικοί στους αναγνώστες τους, αυτό εκ πρώτης όψεως μπορεί να δείχνει αρκετά σοβαροφανές αλλά στη συνέχεια μπορούμε να διαπιστώσουμε πως

δεν έχει κανένα νόημα. Ένα παράδειγμα που μας δίνει να το καταλάβουμε είναι αυτό π.χ.

```
"...if the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop which can severely damage the processor..."
```

αν το μελετήσουμε δεν υπάρχει κάτι που να αποκαλείται nth-complexity infinite binary loop και στη τελική οι επεξεργαστές είναι φτιαγμένοι για να κάνουν loops εβδομάδες χωρίς να παθαίνουν τίποτε.

2. Κάτι άλλο που κάνουν για να αυξήσουν την αξιοπιστία τους ως e-mails είναι να επικαλεσθούν οι συγγραφείς τους ότι αποτελούν e-mails που τους τα έστειλε μία επώνυμη εταιρία με κύρος όπως (π.χ. Microsoft, Yahoo, Aol). Πράγμα που είναι σχεδόν αδύνατο μιας και αυτές οι εταιρίες οτιδήποτε θέλουν να δημοσιεύσουν το δημοσιεύουν στο τύπο και δεν εμπιστεύονται τα e-mails.
3. Επόμενο και βασικότερο χαρακτηριστικό των Hoaxes είναι να ζητάει τη προώθηση του σε άλλους χρήστες. Αυτός είναι και ο σκοπός του και αν ένα e-mail ζητάει κάτι τέτοιο είναι σχεδόν σίγουρα Hoax.
4. Επίσης πολλοί χρησιμοποιούν και τον εκφοβισμό όπως *«Ψήφισε και εσύ κατά της φορολόγησης των πακέτων του Internet διαφορετικά σύντομα θα αρχίσουν να σε χρεώνουν».* Συνήθως έχουν κακή σύνταξη και είναι ανορθόγραφα αυτού του είδους τα Hoaxes.
5. Τέλος αν τελικά το κείμενο που έχει να σου πει στο e-mail είναι τόσο σημαντικό θα πρέπει τουλάχιστον να αναφέρει το site που έχει φτιαχτεί για αυτόν το λόγο. Και εδώ θα πρέπει να προσέξουμε αν όντως υπάρχει το site, να μην είναι ύποπτη η διεύθυνση (π.χ. η Cisco να έχει σελίδα στο Geocities).

Τρόποι για να αποφύγουμε και να μην επεκτείνουμε τη μάστιγα των hoaxes είναι οι ακόλουθοι. Πρώτον να έχουμε σωστή ενημέρωση, σοβαρότητα και αυτοσυγκράτηση. Όταν δεχόμαστε ένα τέτοιο e-mail να ελέγχουμε αν οι πηγές του είναι έγκυρες (δηλαδή θα πρέπει να ανατρέξουμε στην ιστοσελίδα που αναφέρεται το e-mail και να δούμε αν όντως ο συγγραφέας είναι έγκυρος). Ύστερα δεν πρέπει να παρασυρόμαστε από συναισθηματισμούς και τέλος δεν πρέπει να βιαζόμαστε, όσο

ποιο επείγον ισχυρίζεται ότι είναι το μήνυμα, τόσο ποιο προσεκτικά πρέπει να ασχοληθούμε μαζί του.

Δύο είναι τα μεγάλα προβλήματα που δημιουργούν τα Hoaxes. Το πρώτο είναι ότι ανεβάζουν πολύ τη κίνηση στο διαδίκτυο και τον χώρο στο e-mail μας και το δεύτερο είναι ότι δημιουργούνται e-mails με μεγάλες λίστες λογαριασμών τις οποίες κακόβουλοι χρήστες μπορούν να χρησιμοποιήσουν στο μέλλον για δική τους παράνομη χρήση.

Υποκατηγορία των Hoaxes είναι τα Chain Letters τα οποία όμως δηλώνουν ξεκάθαρα ότι είναι φτιαγμένα για να διακινηθούν σε όσο περισσότερους χρήστες γίνεται εντός διαδικτύου και συνήθως υπόσχονται καλή τύχη κ.α..

Τέλος τα Hoaxes εκτός από το διαδίκτυο έχουν αρχίσει και διαδίδονται μέσο κινητών τηλεφώνων. Παράδειγμα τους θα αναφέρουμε στη συνέχεια. Τώρα θα δούμε μερικά παραδείγματα από Hoaxes για να είμαστε ενημερωμένοι και να ξέρουμε τι πρέπει να αποφεύγουμε:

Παράδειγμα HOAX 1:

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

Παράδειγμα HOAX 2:

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

Φάρσα-ΗΟΑΧ για το κινητό τηλέφωνο:

Μια καινούργια φάρσα που σπέρνει την αμηχανία στους χρήστες κινητών τηλεφώνων είναι η ακόλουθη:

"Αν σας τηλεφωνήσουν στο κινητό σας από κάποιον που θα σας πει ότι είναι τεχνικός εταιρείας, και κάνουν έλεγχο στο τηλέφωνό σας και θα πρέπει να πατήσετε #90 ή 09# ή οποιοδήποτε άλλο νούμερο, ΚΛΕΙΣΤΕ ΤΟ ΤΗΛΕΦΩΝΟ ΧΩΡΙΣ ΝΑ ΠΑΤΗΣΕΤΕ ΚΑΠΟΙΟ ΑΡΙΘΜΟ. Πρόκειται για κάποια εταιρεία-απάτη που χρησιμοποιεί κάποια συσκευή, η οποία μόλις πατήσετε τα παραπάνω νούμερα, μπορεί να μπει στην κάρτα SIM και να παίρνουν τηλέφωνα με δική σας χρέωση. Προωθήστε το μήνυμα σε όσους περισσότερους μπορείτε."

Η παραπάνω φάρσα είχε εμφανιστεί για πρώτη φορά στη Γερμανία το 1999, με ακριβώς το ίδιο κείμενο. Η γερμανική εταιρία κινητής τηλεφωνίας T-Mobil (T-D1) τότε είχε δηλώσει επίσημα ότι κάτι τέτοιο δεν είναι δυνατόν τεχνικά στο δίκτυό της γιατί:

Στη Γερμανία δεν ισχύει το reverse charging, το δίκτυο δεν υποστηρίζει πρόσβαση σε κάρτα SIM κατά τη διάρκεια κλήσης. Επίσης υπάρχει μια λειτουργία για την πιστοποίηση του κινητού, η οποία μαζί με το κρυπτογραφικό κλειδί δεν επιτρέπει την πρόσβαση στην κάρτα με το συνδυασμό 9009. Η κάρτα SIM προστατεύεται από τον κωδικό PIN.

Έγινε ερώτηση και σε ελληνική τηλεφωνική εταιρία για τον ίδιο λόγο και η απάντηση της “Vodafone” ήταν η εξής:

"Αγαπητή κα Κοντίνη,
σε απάντηση του τελευταίου e-mail σας θα θέλαμε να σας ενημερώσουμε ότι, και στο παρελθόν έχει αναφερθεί κάτι ανάλογο το οποίο όταν διερευνήθηκε διαπιστώθηκε ότι δεν ήταν πραγματικό γεγονός, δεν έχει καταγραφεί και διαπιστωθεί γιατί απλά δεν ισχύει κάτι τέτοιο. Ήταν μια κακόγουστη φάρσα. Τεχνικά και δικτυακά δεν υπάρχει απολύτως καμία πρόσβαση στην κάρτα sim του συνδρομητή με οποιαδήποτε χρήση κωδικών ή άλλων ενεργειών εξ αποστάσεως έτσι όπως περιγράφεται. Σε καμία περίπτωση δεν ισχύει ότι αναφέρεται. Παρακαλούμε μην διστάσετε αν έχετε κάποια άλλη ερώτηση ή απορία. Στην διάθεση σας για οποιαδήποτε διευκρίνιση.
Ευχαριστούμε που επικοινωνήσατε μαζί μας.

8.6. Ιοι

Ιός πρόκειται για μία λέξη που απασχολεί έντονα όλους τους χρήστες Η/Υ. Η μορφή ηλεκτρονικού ιού έχει φυσικά διαφορά με τη μορφή ενός ιού που συναντάμε στη φύση, αλλά έχει και κοινά στοιχεία. Η διαφορά τους είναι η προφανής, ενώ ο ένας αποτελείτε από γενετικό κομμάτι στο DNA ο άλλος αποτελείτε από κομμάτι μέσα σε κώδικα. Το κοινό τους όμως είναι πως κάτω από ανάλογες συνθήκες και προϋποθέσεις μπορούν να διαδοθούν και να πολλαπλασιάσουν τον εαυτό τους πάρα πολλές φορές. Οι ιοί των υπολογιστών όπως και των ανθρώπων διακρίνονται σε κατηγορίες, δεν είναι όλοι το ίδιο επικίνδυνοι. Έτσι ένας ιός μπορεί να μας διαγράψει όλα τα δεδομένα από τον σκληρό μας δίσκο, μπορεί απλά να μας κάνει επανεκκινήσεις κάθε τόσο στον υπολογιστή, μπορεί να μας διαγράψει ορισμένα αρχεία ή ακόμα μπορεί απλά να μας ανοιγοκλείνει το πορτάκι του CD. Αυτό δείχνει πως οι ιοί μπορούν να είναι από φάρσα μέχρι και πολύ επικίνδυνοι, ανάλογα με το σκεπτικό που φτιάχτηκαν και το σκοπό για τον οποίο φτιάχτηκαν.

8.6.1. Τύποι Ιών και συνέπιες

8.6.1.1. Worms

Ένας Ιός τύπου worm όπως και οι άλλοι ιοί, έχει σχεδιαστεί για να αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλο. Η διαφορά του είναι ότι αυτός ο Ιός εκτελείται αυτόματα δηλαδή δεν χρειάζεται την ενεργοποίησή του από τον χρήστη, όπως χρειάζονται άλλοι που θα δούμε στη συνέχεια. Ο μεγάλος κίνδυνος του Ιού τύπου worm είναι η ικανότητά του να αναπαράγεται σε μεγάλο βαθμό. Έτσι για παράδειγμα μπορεί να αποσταλεί μόνος του σε όλες μας τις επαφές που έχουμε στο ηλεκτρονικό μας ταχυδρομείο, προκαλώντας υπερφόρτωση της δικτυακής κυκλοφορίας η οποία θα μπορούσε να προκαλέσει απλά επιβράδυνση στο διαδίκτυο ή και πάγωμα του διαδικτύου. Τρανταχτά παραδείγματα Ιών τύπου worm είναι ο Sasses και ο Blaster. Ο δεύτερος εκ των οποίων ανακαλύφθηκε στις 11 Αυγούστου 2003 και εκμεταλλευόταν το θέμα ευπάθειας που αναφερόταν στο ενημερωτικό δελτίο ασφάλειας MS03-026 (823980) της Microsoft για να μεταδοθεί μέσω δικτύων, χρησιμοποιώντας ανοικτές θύρες κλήσης απομακρυσμένης διαδικασίας (Remote Procedure Call) σε υπολογιστές στους οποίους εκτελούνταν κάποιο από τα προϊόντα που παρατέθηκαν από πάνω.

8.6.1.2. Δούρειος Ίππος (Trojan)

Όπως λέει και το όνομά του ο ιός δούρειος ίππος είναι ένας μεταμφιεσμένος ιός. Αυτό σημαίνει πως ενώ εμφανίζεται με το όνομα ενός έμπιστου αρχείου όπως για παράδειγμα οι τελευταίες ενημερώσεις ασφαλείας της Microsoft ή ποιο απλά Nero.exe. Στη πραγματικότητα το όνομα του τελευταίου αν είναι Trojan θα είναι Nero.exe.vbs, οπότε όταν πατήσουμε να τρέξουμε το αρχείο ή να δούμε την εικόνα (γιατί μπορεί να μεταμφιεστεί ακόμα και με κατάληξη .jpg), τότε ενεργοποιείται ο ιός και μπορεί για παράδειγμα να απενεργοποιήσει τα συστήματα ασφαλείας του υπολογιστή μας. Εκτός από συνημμένα αρχεία σε ηλεκτρονικό ταχυδρομείο μπορεί να έχουν ενσωματωθεί και σε κώδικα ενός κανονικού προγράμματος, οπότε εκεί είναι ακόμα πιο δύσκολο να το καταλάβουμε και το μόνο που μπορεί να μας βοηθήσει σε αυτή τη περίπτωση είναι ένα πρόγραμμα anti virus ή το να έχουμε σωστά ενημερωμένο τον υπολογιστή μας. Σε κάθε περίπτωση δεν πρέπει να ανοίγουμε e-mails από χρήστες τους οποίους δεν γνωρίζουμε και να μην κατεβάζουμε προγράμματα από μη έγκυρες πηγές.

8.6.1.3. Logical Bombs

Λογική βόμβα είναι τύπος Trojan το οποίο χρησιμοποιείται για την απελευθέρωση ενός Ιού ή ενός worm στο σύστημα που έχει εισβάλει. Η λογική βόμβα υπάρχει μέσα σε ένα σύστημα μέχρι κάτι να προκαλέσει την ενεργοποίησή της. Αυτό το κάτι μπορεί να είναι είτε εξωτερικός παράγοντας, είτε εσωτερικός παράγοντας παράδειγμα του οποίου είναι ικανοποίηση μιας προεπιλεγμένης συνθήκης από τον υπολογιστή μας. Αν και αυτός ο τρόπος δηλαδή οι Logical Bombs είναι πολύ αποτελεσματικός, δεν έχει βρεθεί έως τώρα αποτελεσματικός τρόπος για τον έλεγχό τους. Όταν αφεθεί ελεύθερος αυτός ο Ιός όσο πιθανό είναι να προσβάλει ένα εχθρικό πληροφοριακό σύστημα άλλο τόσο πιθανό είναι να προσβάλει και ένα φιλικό πληροφοριακό σύστημα. Τέλος έχουν και μια παραλλαγή τις χρονικές βόμβες (Time Bombs) οι οποίες πυροδοτούνται κάποια συγκεκριμένη ημερομηνία με τα ίδια αποτελέσματα.

8.6.1.4. Mail Bugs

Αυτούς τους Ιούς είναι αρκετά δύσκολο να τους καταλάβουμε, είναι σε μορφή HTML και μπορούν σε συνδυασμό με κάποιες άλλες παραμέτρους να παραβιάσουν το απόρρητο των πληροφοριών που έχουμε στον Η/Υ μας. Υπάρχουν επίσης και Micros Virus Scripts όπου είναι ιοί που αποστέλλονται μέσω του ηλεκτρονικού ταχυδρομείου όπου εκτός του κειμένου το μήνυμα συμπεριλαμβάνει και διάφορες εντολές ώστε ο

Ιός να εισβάλει στον Η/Υ. Οι εντολές αυτές είναι απλές προτάσεις όπως set DioM.JCD.exe_On.McSF. το οποίο σημαίνει, μόλις ανοίξουμε το e-mail να εκτελεστεί η εφαρμογή DioM.JCD.exe.

8.6.1.5. Άλλοι λιγότερο σημαντικοί ιοί:

Adware, Backdoors, Boot viruses, Bot-Net, EICAR test file, Exploit, Grayware, Honeypot, Keystroke logging, Polymorph viruses, Program viruses, Spyware, Zombie. Δεν θα κάνουμε περεταίρω αναφορά σε αυτούς τους Ιούς διότι θα ξεφύγουμε από τα πλαίσια της πτυχιακής μας εργασίας. Κάνουμε απλά τη γενική αναφορά διότι πιστεύουμε πως είναι απαραίτητη.

Τέλος ένα παράδειγμα ενός μολυσμένου αρχείου από τον Ιό ILOVEYOU είναι το εξής:

```
Όνομα αρχείου: ILOVEYOU.txt.vbs
Subject: ILOVEYOU
Message:
KINDLY CHECK THE ATTACHED LOVELETTER COMING FROM ME!!!
Attached: Love-Leter-for-you.txt.vbs
Size: 10.307 bytes
```

Στη συνέχεια έχουμε το αρχείο

```
Autoexec.bat
ECHO OFF
ECHO MORNING BABY, I NEVER LOVE ANY LIKE YOU.…NA
ECHO WHAT'VE EVER HAPPENED I STILL LOVE YOU….NA
ECHO SEE YOU AT THE MILKY WAY OR MOON RIVER.…NA
ECHO I WAITING FOR YOU. I LOVE YOU….NA NA NA NAAAA
CTTY NUL
FORMAT C:/AUTOTEST /Q/U
```

Actions

```
à \Windows\System\Mskernel32.vbs & LOVE-LETTER-FOR-YOU.txt.vbs
à \Windows Win32dll.vbs
à Search Winfat32.exe in \Windows\System
à HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX
```

```
New Registry Keys
à HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL
HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Run\ESKernel32
HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\RunServices\ES32DLL
HKEY_LOCALMACHINE\Sofware\Microsoft\Windows\CurrentVersion\Run\WINFAT32
à HKEY_USERS\<username>\Software\Microsoft\Windows\CurrentVersion\Run
Deleted Registry Keys
à HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Policies\Network\HideShare\Pwds
HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching
HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Policies\Network\HideShare\Pwds
HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching
```

8.7. Sniffing

Το sniffing εγκύπτει στα είδη των παθητικών επιθέσεων. Δηλαδή το sniffing δεν έχει σκοπό να βλάψει άμεσα τον στόχο του, αλλά έχει σαν σκοπό ο επιτιθέμενος να συλλέξει χρήσιμα στοιχεία και πληροφορίες ώστε να τα χρησιμοποιήσει μετέπειτα στην κύρια επίθεσή του. Ένα παράδειγμα είναι υποκλοπές passwords μέσω sniffing. Τα προγράμματα sniffers ή network analyzers είναι νόμιμα και χρησιμοποιούνται από τους διαχειριστές του δικτύου ώστε να διορθώσουν προβλήματα στη κίνησή του και άλλα παρόμοια, όμως δυστυχώς χρησιμοποιούνται και από τους crakers για τους παραπάνω λόγους.

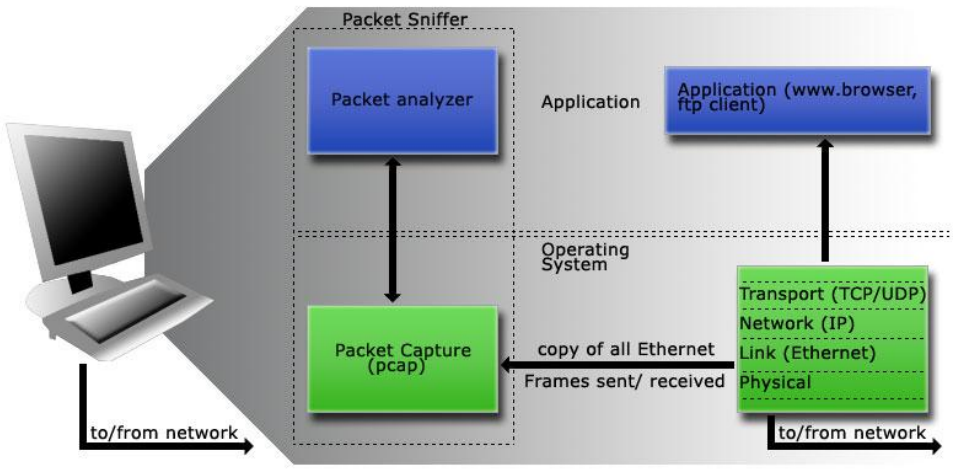
Ο τρόπος λειτουργίας αυτών των προγραμμάτων είναι ο εξής. Αφού οι περισσότεροι υπολογιστές συνδέονται με Lan δηλαδή μοιράζονται την ίδια σύνδεση με άλλους υπολογιστές και εάν το δίκτυο δεν χρησιμοποιεί switch, η κίνηση που προορίζεται για έναν τομέα μεταδίδεται σε κάθε μηχάνημα του δικτύου. Ο κάθε υπολογιστής όμως που περνάνε τα δεδομένα από την κάρτα δικτύου, αγνοεί όλα τα δεδομένα που δεν τον αφορούν δηλαδή που δεν προορίζονται για αυτόν. Το sniffer όμως αναγκάζει την κάρτα δικτύου του να αρχίσει να προσέχει και τα πακέτα που δεν προορίζονται για αυτόν, αλλά για τους υπόλοιπους υπολογιστές. Για να το πετύχει αυτό θέτει την

κάρτα δικτύου σε ειδική λειτουργία, γνωστή ως promiscuous mode. Όταν η κάρτα δικτύου βρίσκεται σε αυτή τη λειτουργία (μία κατάσταση που απαιτεί δικαιώματα ανώτερου χρήστη, root), τότε μπορεί το μηχάνημα να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του.

Για να αποφύγουμε το sniffing μπορούμε να χρησιμοποιήσουμε προγράμματα anti sniffing. Θα πρέπει όμως να αναφέρουμε τη δυσκολία ελέγχου του sniffing διότι μιας και είναι παθητική επίθεση, δηλαδή συλλέγει πληροφορίες, δεν κάνει καμία αλλοίωση ή δεν αφήνει καμία υπογραφή στη συνηθισμένη κίνηση του δικτύου για να φανεί η λειτουργία του. Παρόλα αυτά υπάρχουν τρόποι ώστε να γίνονται φανερές τέτοιου είδους επιθέσεις οι οποίες βρίσκονται σε promiscuous mode. Οι κύριοι μέθοδοι είναι Ping method, Arp method, local host και latency method. Πάντως η καλύτερη όλων για την αποφυγή του είναι η κρυπτογράφηση με SSL, PGP, SSH κ.α. έτσι ώστε και να αποκτήσει πρόσβαση στα δεδομένα μας ο cracker να μην μπορεί να τα αποκωδικοποιήσει.

Για να καταλάβουμε καλύτερα πως λειτουργεί το Sniffing θα δοκιμάσουμε να κάνουμε μία επίθεση σε έναν δικτυακό τόπο με το Wireshark και να υποκλέψουμε τους κωδικούς πρόσβασης. Το Wireshark οι περισσότεροι το γνωρίζουμε ως Ethereal, όμως επειδή ο σχεδιαστής του Ethereal προχώρησε σε μια νέα εταιρία αναγκάστηκε να εγκαταλείψει το σήμα κατατεθέν Ethereal και να το μετονομάσει σε Wireshark, κατά τα άλλα δουλεύουν με τον ίδιο ακριβώς τρόπο.

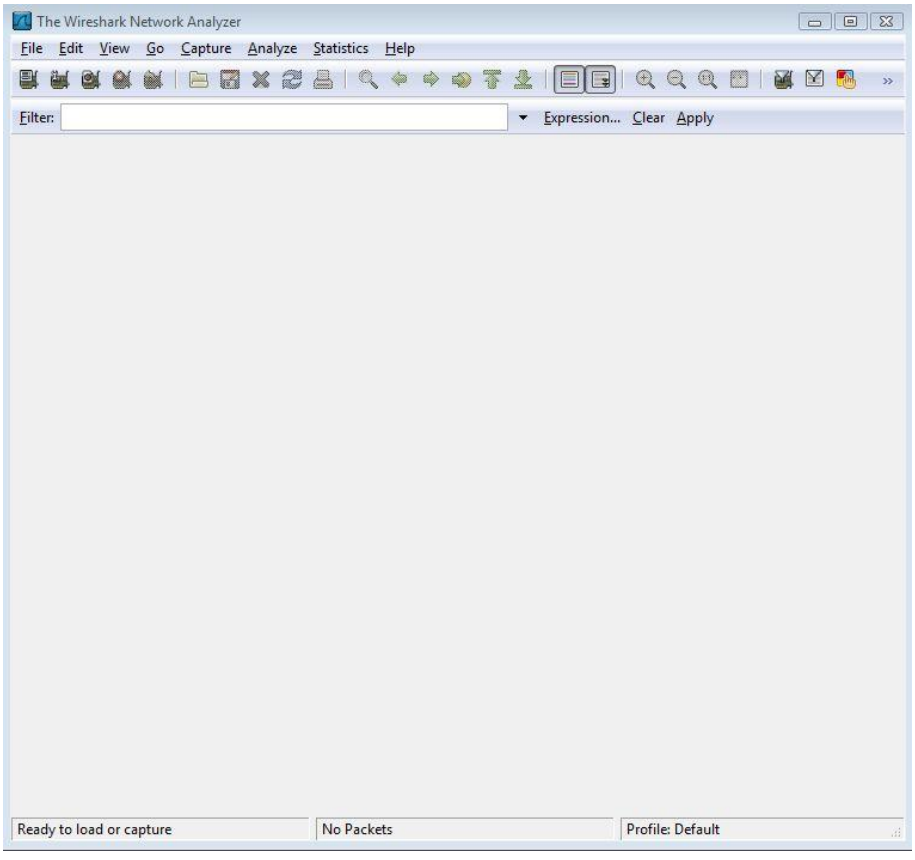
Στο σχήμα που ακολουθεί φαίνεται η δομή ενός packet Sniffer



Εικόνα 21 - Δομή Packet Sniffer

Όπου στο δεξί μέρος του Σχήματος φαίνονται τα πρωτόκολλα που τρέχουν κανονικά στον υπολογιστή μας. Μέσα στο παραλληλόγραμμο έχουμε τον packet Sniffer ο οποίος συνήθως είναι μία προσθήκη στο λογισμικό, που αποτελείται από δύο μέρη. Το πρώτο μέρος είναι η βιβλιοθήκη σύλληψης πακέτων η οποία λαμβάνει ένα αντίγραφο κάθε πλαισίου επιπέδου ζεύξης που στέλνεται ή λαμβάνεται από τον υπολογιστή μας. Ενώ το δεύτερο είναι ο αναλυτής πακέτων, ο οποίος απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Για το σκοπό αυτό, ο αναλυτής πακέτων πρέπει να «καταλαβαίνει» τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα.

Το πρόγραμμα Wireshark όταν το ανοίγουμε έχει αυτό το Interface (το οποίο και παραμετροποιείται, αλλά όπως θα δούμε είναι ικανοποιητικός και ο Default του χώρος)

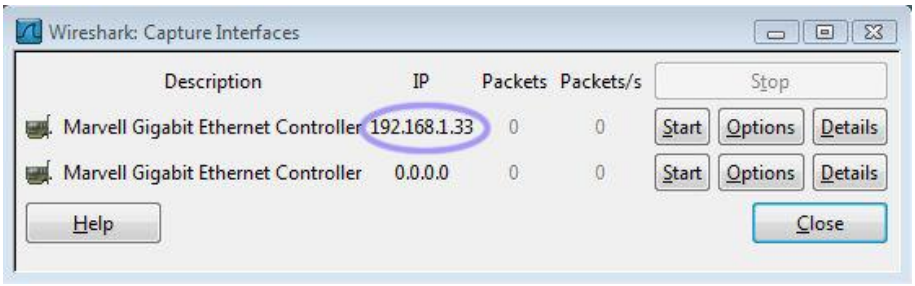


Εικόνα 22 - Wireshark Network Analyzer

Προτού αρχίσουμε το Capture πρέπει να ρυθμίσουμε τα Settings του προγράμματος. Οπότε από το Capture **à** Interfaces, ρυθμίζουμε ποια κάρτα δικτύου θα παρακολουθήσει (τα σημερινά PC έχουν πάνω από μια οπότε πρέπει να τη δηλώνουμε)

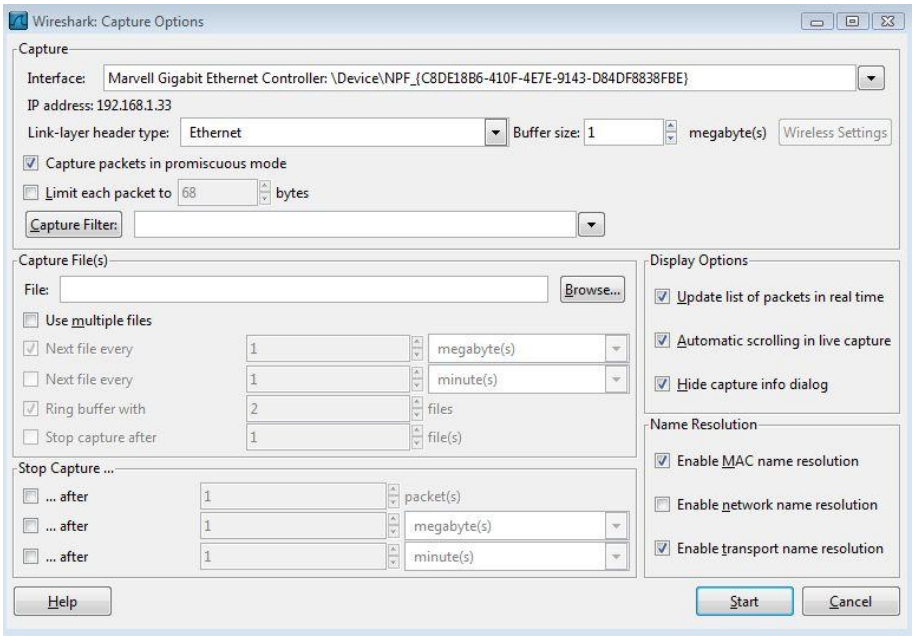
Εικόνα 23 - Capture Interfaces

Στην προκειμένη περίπτωση θα χρησιμοποιήσουμε την πρώτη από τις δύο Marvell



Εικόνα 24 - Capture Interfaces

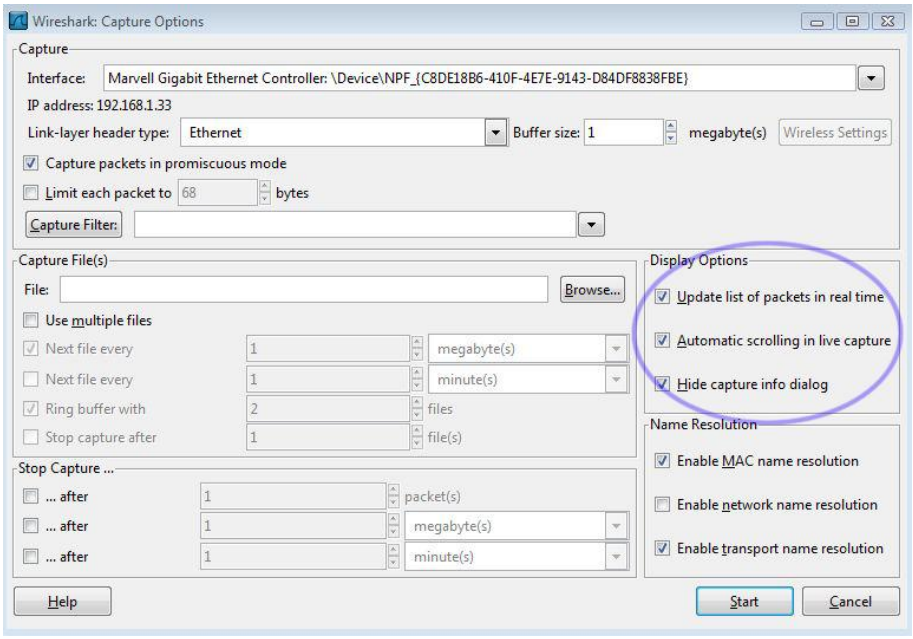
Ύστερα θα πάμε στο Capture **à** Options. Εδώ θα δούμε αν είναι κλικαρισμένα τα Checkboxes που μας ικανοποιούν



Εικόνα 25 - Capture options

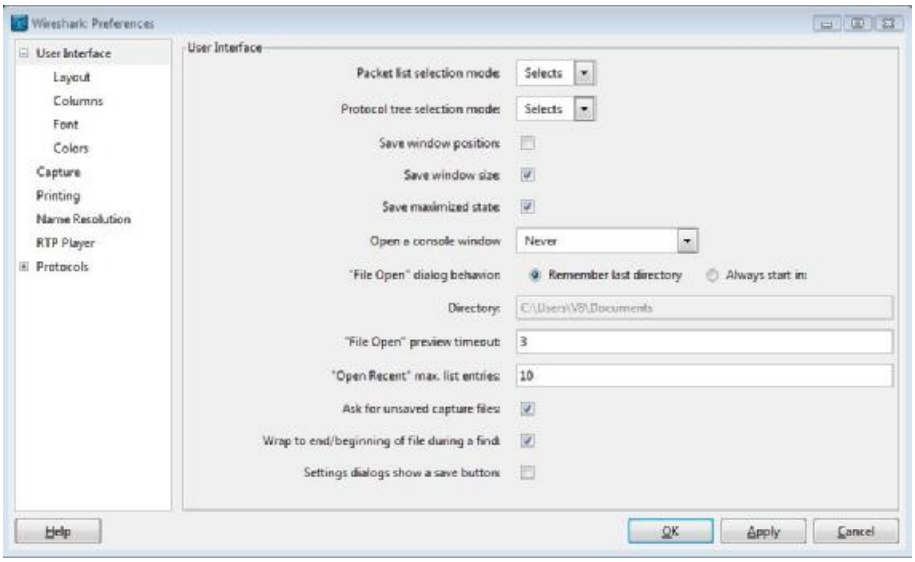
Κοιτάμε να κάνει Update σε real time. Δηλαδή να βλέπουμε τα δεδομένα τη στιγμή που τα λαμβάνουμε. Ύστερα να κάνει Automatic Scrolling in live Capture, δηλαδή να κατεβαίνει αυτόματα, έτσι ώστε να μας δείχνει το τελευταίο πακέτο που παραλάβαμε και Hide capture info dialog για να μην έχουμε πολύ πληροφορία τη στιγμή που

παίρνουμε τα πακέτα (στη συνέχεια αν θέλουμε το ανοίγουμε). Τα άλλα δεν μας αφορούν οπότε και συνεχίζουμε στο άλλο που πρέπει να ελέγξουμε



Εικόνα 26 - Capture Options

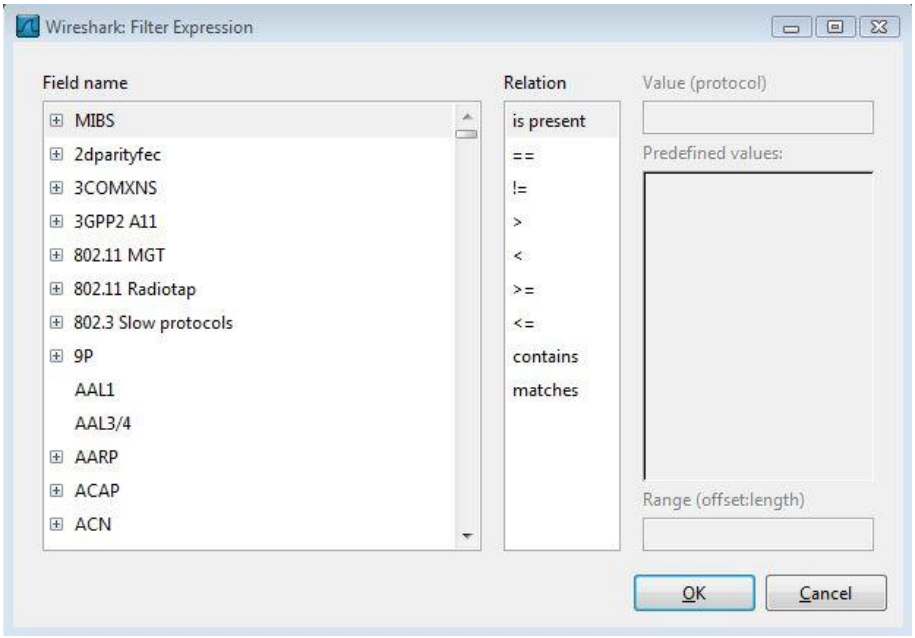
Από το μενού Edit **à** Preferences. Βρίσκουμε τη τοποθεσία που θέλουμε να μας σώζει τα αρχεία του (στη προκειμένη περίπτωση το έχουμε βάλει να τα σώζει στο MyDocuments



Εικόνα 27 - Preferences

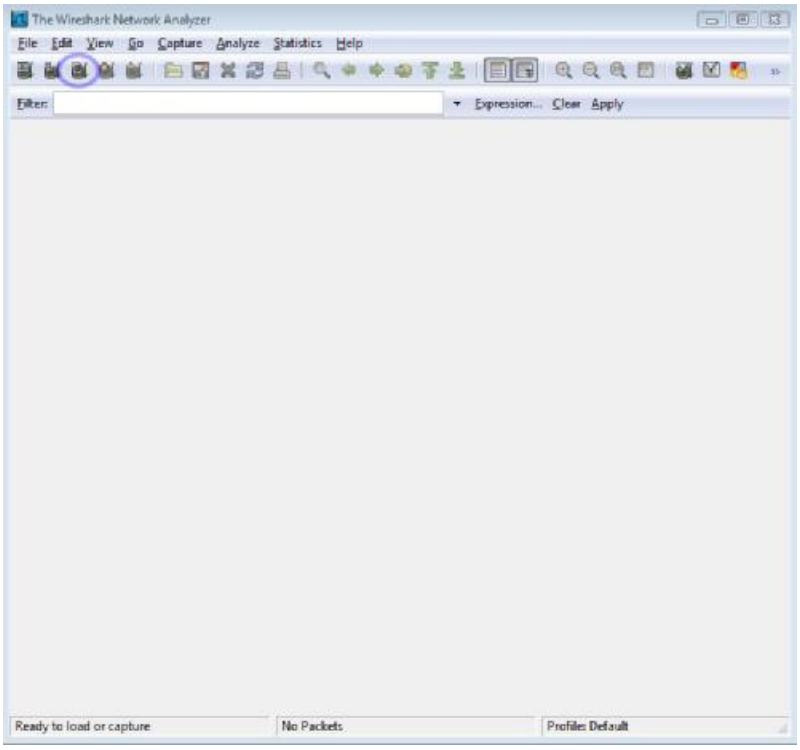
Ύστερα στο Filter **à** Expression. Ορίζουμε τα φίλτρα μας, δηλαδή ποια πακέτα δεν μας ενδιαφέρει να βλέπουμε, επίσης έχει ισότητες και ανοσιότητες για να τα προσδιορίσουμε με μεγαλύτερη ακρίβεια. Είναι πολύ βασικό στοιχείο τα φίλτρα, διότι

παίρνουμε πολύ μεγάλο όγκο δεδομένων και κάπως πρέπει να τον διαχειριστούμε. Για αρχή μπορούμε να μη βάλουμε μέχρι να δούμε τα αποτελέσματα και το πως θέλουμε να τα ορίσουμε



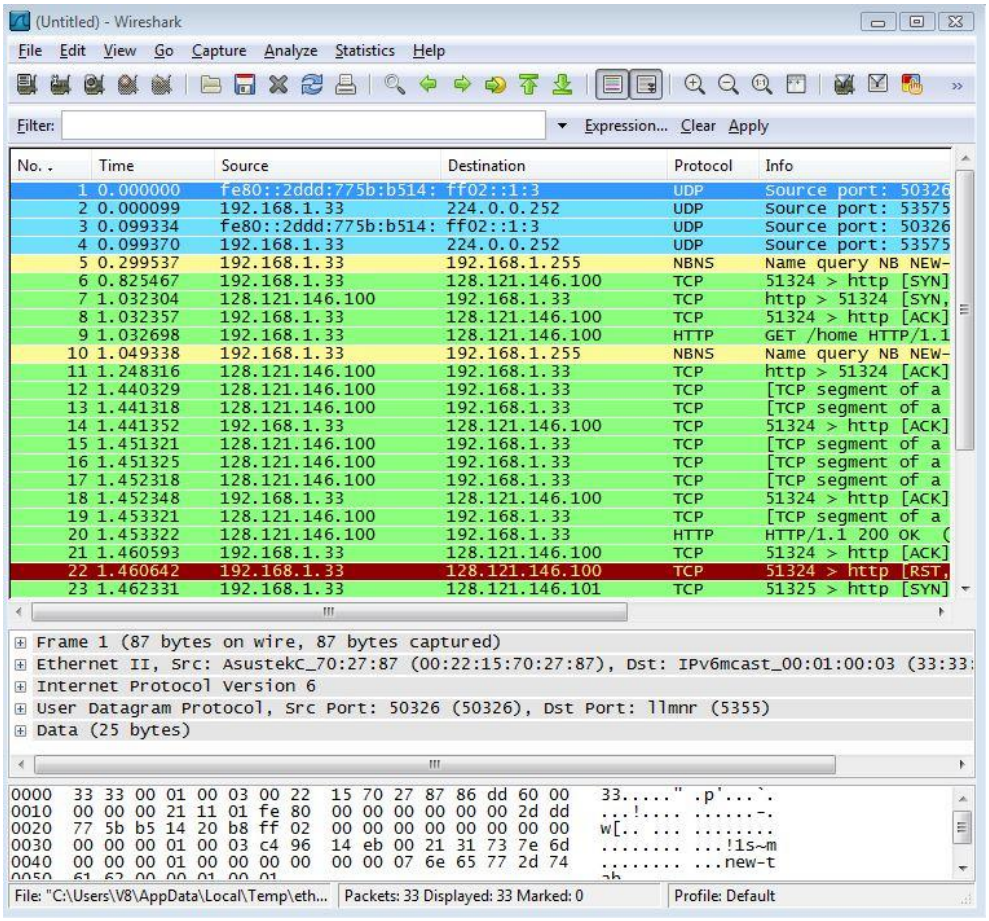
Εικόνα 28 - Filter Expression

Μετά τις απαραίτητες ρυθμίσεις, γυρνάμε στο κεντρικό Interface μας και πατάμε το κουμπί Start live Capture



Εικόνα 29 - Wireshark Network Analyzer

Όταν πια σταματήσουμε το Capture, το κεντρικό Interface θα έχει διαμορφωθεί και θα πρέπει να αρχίσουμε την αναζήτηση του πακέτου που μας ενδιαφέρει. Είτε χειροκίνητα (πράγμα που παίρνει πολύ ώρα), είτε με τη βοήθεια των φίλτρων.



Εικόνα 30 - Αρχική οθόνη μετά την χρήση

Πάνω στο ανοιχτό μπλε έχουμε το Μενού εντολών

Είναι συνηθισμένα πτυσσόμενα μενού που βρίσκονται στο επάνω μέρος του παραθύρου και μας δίνουν πρόσβαση στη διαχείριση του προγράμματος.

Στη συνέχεια έχουμε τον κατάλογο συλληφθέντων πακέτων

Παρουσιάζει μια περίληψη της μιας γραμμής για κάθε πακέτο που συλλαμβάνεται η οποία περιλαμβάνει τον αριθμό πακέτου, τον χρόνο σύλληψης του πακέτου, τις διευθύνσεις πηγής και προορισμού του πακέτου, το είδος του πρωτοκόλλου και πληροφορία σχετική με το πρωτόκολλο η οποία περιέχεται στο πακέτο.

Από κάτω έχουμε λεπτομέρειες επιλεγμένης επικεφαλίδας πακέτου

Παρέχει λεπτομέρειες σχετικά με το επιλεγμένο πακέτο στο παράθυρο packet-listing. Οι λεπτομέρειες αυτές περιλαμβάνουν πληροφορίες σχετικά με το πλαίσιο Ethernet και το IP datagram που περιέχουν αυτό το πακέτο. Το ποσό των λεπτομερειών που παρουσιάζεται για το Ethernet και το επίπεδο IP μπορεί να επεκταθεί ή ελαχιστοποιηθεί κάνοντας κλικ στο βέλος που δείχνει δεξιά ή προς τα κάτω και βρίσκεται στα αριστερά της γραμμής του πλαισίου Ethernet ή του IP datagram στο παράθυρο packet-header details.

Και τέλος έχουμε το Περιεχόμενο του πακέτου σε δεκαεξαδικό και ASCII

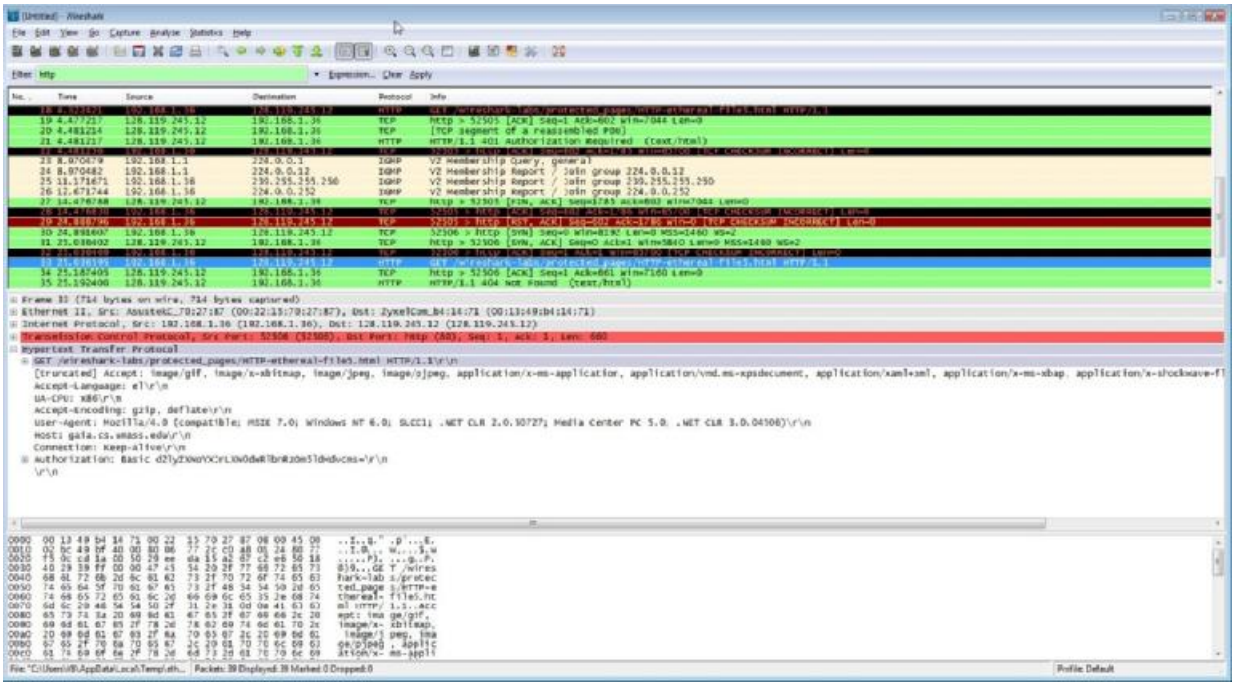
Παρουσιάζει ολόκληρο το περιεχόμενο ενός συλλαμβανομένου πλαισίου και σε μορφή ASCII και σε δεκαεξαδική μορφή.

Βασικό του στοιχείο είναι το πεδίο του φίλτρου παρουσίασης πακέτων στο οποίο μπορούμε να εισάγουμε το όνομα ενός πρωτοκόλλου ή άλλη πληροφορία έτσι ώστε να φιλτράρουμε την πληροφορία που παρουσιάζεται στο παράθυρο packet-listing.

Θα δοκιμάσουμε τώρα να υποκλέψουμε κωδικούς πρόσβασης από ένα Web Site (δοκιμάζουμε αυτή τη τεχνική διότι είναι παρόμοια με αυτή που υποκλέπτουμε μηνύματα ηλεκτρονικού ταχυδρομείου. Επειδή όμως λείπει ο κατάλληλος εξοπλισμός ο οποίος είναι τουλάχιστον 3 υπολογιστές, 1 router και 1 Server, το δοκιμάζουμε υποθετικά σε ένα website έτσι αλλάζοντας τις πόρτες που δουλεύει σε 145 για IMAP και 110 για POP3 και αναζητώντας στα official WebSites τους τη μορφή με την οποία αποστέλλονται τα δεδομένα, μπορούμε να πάρουμε ατόφιο το περιεχόμενο του e-mail). Ας δούμε όμως προς το παρόν το παράδειγμα υποκλοπής πακέτων από ένα website.

Αφού κάνουμε τη περιήγηση που θέλουμε στο διαδίκτυο (δηλαδή αφού εισάγουμε τους κωδικούς LogIn). Πηγαίνουμε στο Capture **à** Stop. Από εδώ και πέρα σταματάμε να λαμβάνουμε πακέτα και αρχίζουμε να εξερευνούμε για το πακέτο που χρειαζόμαστε. Στη δική μας περίπτωση το πακέτο που χρειαζόμαστε θα το βρούμε από τον κατάλογο συλληφθέντων πακέτων στο HTTP GET και στις λεπτομέρειες επιλεγμένης επικεφαλίδας πακέτου στο Authorization. Το μήνυμα που βλέπουμε δεν έχει καμία κωδικοποίηση απλώς είναι γραμμένο σε δεκαεξαδική μορφή αν κάνουμε την απαραίτητη αλλαγή σε ASCII (πράγμα που κάνει και από μόνο του το Wireshark,

στο Ethereal όμως δεν υπήρχε αυτή η επιλογή) όμως υπάρχουν και Websites που κάνουν το αναλαμβάνουν, θα καταφέρουμε να δούμε τους κωδικούς LogIn και password που εισαγάγαμε. Στην παρακάτω εικόνα φαίνεται το παράθυρο του προγράμματος μετά τη χρήση *(η εικόνα είναι σε ανάλυση 1920*1200 αν θέλετε να δείτε περισσότερες λεπτομέρειες).*



Εικόνα 31 - Αρχική οθόνη μετά την χρήση

8.8. Spam

Με τον όρο Spam χαρακτηρίζεται η αποστολή μεγάλου αριθμού αλληλογραφίας σε παραλήπτες οι οποίοι δεν έχουν ξανακάνει αλληλογραφία με το χρήστη που τους τη στέλνει. Το Spam ή UCE ή UBE (Αυτοκόλλητα εμπορικά μηνύματα, Αυτοκόλλητη ενοχλητικοί αλληλογραφία) συνήθως πραγματεύεται μηνύματα εμπορικού περιεχομένου, τα οποία προσφέρουν «επώνυμα» προϊόντα σε πολύ χαμηλές τιμές. Τώρα πια υπάρχουν και spams τα οποία πραγματεύονται υλικό πορνογραφικού περιεχομένου, περιέχουν επικίνδυνο λογισμικό ή χρησιμοποιούνται για απάτες επιφυλάσσοντας έτσι κινδύνους για τους χρήστες. Ο όρος spam προήλθε από την ταινία των Monty Pythons στην οποία αναφέρεται συνέχεια αυτός ο όρος ως κάτι βαρετό και επαναλαμβανόμενο. Στη ταινία ήταν ένα ζευγάρι το οποίο βρισκόταν σε ένα εστιατόριο και κατά την προσπάθειά του να παραγγείλει διαπιστώνει πως όλο το menu αποτελούταν από μια κονσέρβα Spam (special pork and meat). Παρόλο που το σκετς ήταν πολύ μικρό σε διάρκεια η λέξη Spam είχε ακουστεί πάνω από 94

φορές, πράγμα που δείχνει το κορεσμό της κοινωνίας από spam εκείνη την εποχή και μεταγενέστερα από το ψηφιακό spam. Η πρώτη αποπήρα spamming πραγματοποιήθηκε στις 3 Μαΐου του 1978 από τον manager της εταιρείας Digital Equipment Corporation που σήμερα δεν υπάρχει και αφορούσε τη διαφήμιση ενός νέου μοντέλου υπολογιστή. Στάλθηκε σε 393 επαφές, οι οποίες είχαν περαστεί με το χέρι. Η λήψη του μηνύματος προκάλεσε οργή στους χρήστες οι οποίοι το παρέλαβαν και τελικά έγινε επίπληξη στην εταιρία Digital Equipment Corporation. Το 1994 όμως έγινε η πρώτη πραγματικά μαζική αποστολή spam, από δύο δικηγόρους στην Αριζόνα, οι οποίοι τοποθέτησαν το μήνυμα των υπηρεσιών τους για τους μετανάστες σε 6 χιλιάδες συσκέψεις Usenet. Στην απάντηση είχαν λάβει πολλά εξοργισμένα μηνύματα. Τώρα πια το Spam αποτελεί το μεγαλύτερο μέρος της ηλεκτρονικής αλληλογραφίας το οποίο αποτελεί γύρο στο 8-9 στα 10 ηλεκτρονικά μηνύματα. Έχει εξελιχθεί σε μεγάλη μάστιγα της εποχής μας, έχουν εφευρεθεί νέοι τρόποι αποστολής spam όπως και μπλοκαρίσματός τους.

Καταρχήν το software που έχει εξελιχθεί για την καταπολέμησή τους χωρίζεται σε δύο κατηγορίες. Η πρώτη αφορά τους διακομιστές του ηλεκτρονικού ταχυδρομείου και η δεύτερη αφορά τους τελικούς χρήστες, δηλαδή εμάς. Για τους τελικούς χρήστες προγράμματα που βοηθούν στη καταπολέμηση του spam είναι το SpamFigter, McAfee, E-trust anti-spam κ.α. το κάθε ένα χρησιμοποιεί διαφορετικό τρόπο καταπολέμησης της ενοχλητικής αλληλογραφίας, αλλά τελικά όλα είναι αρκετά αποτελεσματικά. Οι διακομιστές τώρα κάνουν χρήση του SMTP server, χρησιμοποιούν προγράμματα όπως το Spam Assassin, Mail Scanner κ.α. τα οποία δουλεύουν διαφορετικά από τα προγράμματα που χρησιμοποιεί ο τελικός χρήστης και είναι περισσότερο αποτελεσματικά. Σε γενικές γραμμές πάντως για να αποφύγουμε με το καλύτερο τρόπο το Spam δεν πρέπει να βασιζόμαστε μόνο στους διακόμισες, αλλά πρέπει να έχουμε πάντα στον υπολογιστή μας ένα σύστημα anti-spamming και να φροντίζουμε να το κρατάμε ενημερωμένο.

Τώρα εκτός από το software για να αποφύγουμε το spam μπορούμε να κάνουμε και εμείς μερικές κινήσεις, οι οποίες αναφέρονται στη συνέχεια:

- Ποτέ δεν πρέπει να απαντάμε σε spam mails, με την απάντηση ή έστω και με ένα κλικ σε σύνδεσμο που μπορεί να περιέχεται στο e-mail, επιβεβαιώνουμε

τη διεύθυνση μας ότι αληθεύει και αυτόματος μπαίνει και σε άλλες λίστες για μαζικές αποστολές ενοχλητικής αλληλογραφίας.

- Ποτέ δεν πρέπει να ανταποκρινόμαστε στο Link “remove me from the mailing list”. Πρόκειται απλά και μόνο για ένα κόλπο το οποίο και πάλι ενημερώνει τον αποστολέα πως η διεύθυνση μας ισχύει με συνέπεια να αρχίσει να τη χρησιμοποιεί σε κάθε του πράξη.
- Ποτέ δεν πρέπει να γινόμαστε συνδρομητές σε sites που υπόσχονται πως θα αφαιρεθεί η διεύθυνση του e-mail μας από spam lists. Σπανίως είναι ειλικρινείς, ενώ στις περισσότερες περιπτώσεις είναι άλλο ένα trick των spammers.
- Πάντα να λαμβάνουμε μέτρα αντιμετώπισης του spam. Να ενημερώνουμε υπηρεσίες και αρμόδιους οργανισμούς όταν διαχειριζόμαστε spam από εμπορικές εταιρίες, να κάνουμε γνωστά τα παράπονά μας στις τελευταίες και φυσικά να αντιστεκόμαστε στον κατακλυσμό διαφημίσεων.
- Πάντα να διατηρούμε μια e-mail διεύθυνση αυστηρά και μόνο για τις πολύ στενές προσωπικές μας επαφές, φροντίζοντας να αποφεύγουμε τη δήλωσή της σε web υπηρεσίες.

9. Μελέτη περίπτωσης

Στα πλαίσια αυτής της πτυχιακής σκοπός μας εκτός από το να δούμε αν υπάρχει και πόση ασφάλεια στα δίκτυα και στο e-mail θελήσαμε να δούμε πόσο αποδοτικά είναι τα συστήματα e-mail που παρέχουν κάποια εκπαιδευτικά ιδρύματα. Τα ιδρύματα που συμμετείχαν και απάντησαν στην έρευνα μας ήταν το ΤΕΙ Πατρών και το τμήμα Βιολογίας του Πανεπιστημίου Κρήτης. Όπως θα δούμε από τις απαντήσεις των ερωτηματολογίων που αποστείλαμε υπάρχουν διαφορές στην υπηρεσία που προσφέρουν. Στον παρακάτω πίνακα φαίνονται οι απαντήσεις στο ερωτηματολόγιο μας.

Ερώτηση	ΤΕΙ Πατρών	Τμήμα Βιολογίας Κρήτης
Χρησιμοποιείτε κάποια λύση συνεργατικής επικοινωνίας που βασίζεται στην ηλεκτρονική αλληλογραφία όπως το MicrosoftExchange ή το LotusNotes;	ΟΧΙ	ΟΧΙ
Ποιο πρωτόκολλο μπορεί να χρησιμοποιήσει ο χρήστης για τη μεταφορά της ηλεκτρονικής αλληλογραφίας του, από τον διακομιστή στον υπολογιστή του; (IMAP, POP3, IMAP/SSL, POP3/SSL, MAPI, NRPC)	POP3	IMAP POP3 IMAP over SSL
Ο mailserver είναι ιδιόκτητος ή χρησιμοποιείται Outsourcing εταιρία. Στην περίπτωση της εταιρίας – οργανισμού, ποιας και γιατί έγινε η συγκεκριμένη επιλογή;	ΙΔΙΟΚΤΗΤΟΣ	Ο mailserver είναι ιδιόκτητος και επιλέχθηκε έπειτα από διαγωνισμό μειοδωτικών προσφορών
Αν είναι ιδιόκτητος ποια λύση Hardware ή software χρησιμοποιείται για την ασφάλεια σε επιθέσεις spoof;	ACCESS LISTS	Sender id filtering
Αν είναι ιδιόκτητος ποια λύση Hardware ή Software χρησιμοποιείται για την ασφάλεια σε επιθέσεις spam;	SPAMASSASSIN	SPAMASSASSIN
Αν είναι ιδιόκτητος ποια λύση Hardware ή Software χρησιμοποιείται για την ασφάλεια σε επιθέσεις virus;	CLAM-AntiVirus	Symantec Mail Security
Από τον client στον server τι σύστημα κρυπτογράφησης χρησιμοποιείται και γιατί επιλέχτηκε αυτό;	ΚΑΝΕΝΑ	SSL διότι είναι το standard της αγοράς
Στην περίπτωση του ιδιόκτητου mailserver τι μέθοδος κρυπτογράφησης χρησιμοποιείται για την επικοινωνία με άλλους mailservers;	------	Δεν χρησιμοποιούμε
Τι ποσοστά spamming δέχεστε (κατά μέσο όρο);	30.000 / ΜΕΡΑ	80%-90% εισερχόμενη, <1% καταλήγει στο mailbox
Έχει υπάρξει μέχρι τώρα επίθεση spoofing στο σύστημα σας;	ΟΧΙ	ΟΧΙ
Έχει πραγματοποιηθεί ποτέ, ενδοδικτυακή επίθεση, αν ναι πια ήταν (spamming, mailBombs, κτλ);	ΟΧΙ	ΟΧΙ
Τι άλλου είδους επιθέσεις έχει δεχτεί το σύστημά σας;	ΚΑΜΙΑ	Προσπάθεια σύνδεσης με κατηργημένους λογαριασμούς
Ο χρήστης μπορεί να διαχειριστεί το mailbox του μέσω κάποιου browser; Αν ναι ποιο πρωτόκολλο ασφαλείας χρησιμοποιείται για τη σύνδεση (SHTTP, SSL);	ΟΧΙ	SHTTP

Από τις απαντήσεις των διαχειριστών συστήματος των ιδρυμάτων, παρατηρούμε ότι και τα δύο δεν χρησιμοποιούν λύσεις για το e-mail όπως είναι το Exchange και το Lotusnotes κάτι που είναι λογικό μιας και είναι λύσεις προσανατολισμένες σε εταιρίες, καθώς προσφέρουν αρκετές παραπάνω υπηρεσίες εκτός του ηλεκτρονικού ταχυδρομείου και σίγουρα έχουν μεγαλύτερο κόστος.

Ένα σημαντικό ερώτημα ήταν ο τρόπος μεταφοράς της ηλεκτρονικής αλληλογραφίας στον χρήστη και βλέπουμε ότι το ΤΕΙ Πατρών υποστηρίζει μόνο σύνδεση POP3 ενώ το τμήμα Βιολογίας Κρήτης δίνει περισσότερες επιλογές στον χρήστη ο οποίος μπορεί να εκμεταλλευτεί τα πλεονεκτήματα των πρωτοκόλλων αυτών.

Σχετικά με τον mailserver, βλέπουμε πως και τα δύο ιδρύματα χρησιμοποιούν ιδιόκτητους mailserver. Αυτό σημαίνει πως η διαχείριση τους είναι στα χέρια των ιδρυμάτων και να επιλέγουν τις αλλαγές – αναβαθμίσεις που ίσως θέλουν να πραγματοποιήσουν.

Σχετικά με την προστασία τους από επιθέσεις Spoof τα δύο ιδρύματα έχουν επιλέξει διαφορετικές λύσεις προστασίας. Το ποια είναι αποδοτικότερη δεν μας απασχολεί σε αυτό το επίπεδο, το ότι υπάρχουν είναι το σημαντικό.

Κοινή επιλογή των ιδρυμάτων είναι το Spamassassin για την προστασία τους από Spam, κάτι που όπως διαπιστώσαμε έπειτα από ψάξιμο στο Internet είναι επιλογή συνηθισμένη για αυτή την χρήση.

Στην προστασία τους από ιούς χρησιμοποιούν διαφορετικές λύσεις. Το ClamAV που χρησιμοποιεί το ΤΕΙ Πατρών, είναι opensource λογισμικό το οποίο παρέχεται για συστήματα Windows αλλά και Linux, με συνεχείς ανανεώσεις του κώδικα και στην βάση δεδομένων των ιών του. Το τμήμα Βιολογίας Κρήτης έχει επιλέξει το MailSecurity της γνωστής εταιρίας στον χώρο Symantec, μια συσκευή η οποία εκτός από το antivirus προσφέρει και antispam.

Στο σημαντικότατο θέμα της κρυπτογράφησης από τον χρήστης στον server βλέπουμε ότι το ΤΕΙ Πατρών δεν παρέχει κρυπτογράφηση, σε αντίθεση με το τμήμα Βιολογίας Κρήτης που παρέχει SSL που όπως μας είπαν είναι Standard στην αγορά.

Στην επικοινωνία mailserver με mailserver που όπως έχουμε αναφέρει μπορεί να υπάρχει και εκεί κρυπτογραφία κανένα από τα ιδρύματα δεν την παρέχει.

Τα ποσοστά spam που δέχονται τα ιδρύματα από τις απαντήσεις βλέπουμε ότι είναι μεγάλα, χωρίς όμως να μας έχουν απαντήσει με ίδιο μέτρο. Αυτό που πρέπει να προσέξουμε είναι η απάντηση του τμήματος Βιολογίας που μας λέει ότι το <1% της αλληλογραφίας καταλήγει στα mailbox των χρηστών.

Βλέπουμε πως και τα δύο ιδρύματα δεν έχουν δεχτεί κάποια επίθεση spoof, ή ενδοδικτυακή επίθεση, κάτι που είναι λογικό καθώς τέτοιες επιθέσεις συναντάμε κυρίως σε εταιρίες και οργανισμούς που τα δεδομένα που μεταδίδονται είναι περισσότερο ευαίσθητα.

Τέλος σε μια ερώτηση που αφορά την ευκολία χρήσης του ηλεκτρονικού ταχυδρομείου από τον χρήστη, αν δηλαδή μπορεί να διαχειριστεί το mailbox του μέσω Internet με την χρήση κάποιου browser, βλέπουμε πως το e-mail του ΤΕΙ Πατρών δεν δίνει αυτή την δυνατότητα σε αντίθεση με το τμήμα Βιολογίας Κρήτης που την παρέχει και μάλιστα με την χρήση SHTTP, κάτι που σημαίνει αυξημένη ασφάλεια.

Ένα γενικό συμπέρασμα που βγαίνει από τις απαντήσεις των δύο ιδρυμάτων, είναι πως και τα δύο παρέχουν ηλεκτρονικό ταχυδρομείο με τις βασικές δικλείδες ασφάλειας και μπορούν να καλύψουν τις ανάγκες των χρηστών αλλά το τμήμα Βιολογίας Κρήτης μπορούμε να πούμε ότι ξεχωρίζει σε κάποια σημεία όπως είναι αυτό της χρηστικότητας, καθώς ο χρήστης έχει περισσότερες επιλογές για το πώς θα χρησιμοποιεί το ηλεκτρονικό του ταχυδρομείο, αν δηλαδή θα το χρησιμοποιεί μέσω κάποιου browser ή μόνο μέσω κάποιου προγράμματος διαχείρισης αλληλογραφίας όπως είναι το MicrosoftOutlook και τέλος παρέχει κωδικοποίηση SSL και SHTTP (στα αντίστοιχα σημεία) για αυξημένη ασφάλεια.

10. Λύσεις για την ασφάλεια του ηλεκτρονικού ταχυδρομείου

10.1. Firewalls

Εδώ θα κάνουμε μία αναφορά στα Firewalls και στη Hardware προστασία του υπολογιστή μας. Δεν είναι άμεση η επίδρασή τους με την ασφάλεια του e-mail αλλά διαδραματίζουν σημαντικό ρόλο στην ασφάλεια του δικτύου οπότε και του e-mail μας.

Υπάρχουν διάφορες απόψεις για το πώς προήλθε η ονομασία του Firewall, κάποιοι λένε πως προέρχεται από το μυθιστόρημα επιστημονικής φαντασίας του William Gibson “Newuromancer”, άλλοι λένε πως προέρχεται από τον χώρο του αυτοκινήτου μιας και Firewall λέγεται το προστατευτικό τοίχος που μπαίνει ανάμεσα στον κινητήρα και στον οδηγό έτσι ώστε εάν πάρει φωτιά ο κινητήρας να μην περάσει και στη καμπίνα του οδηγού, αλλά η πιο επιτυχημένη προσέγγιση πιστεύω πως είναι αυτή (το γιατί θα το καταλάβουμε στη συνέχεια που θα δούμε ακριβώς πως λειτουργεί) και λέει ότι πρωτοεμφανίστηκε στις αρχές του 20^{ου} αιώνα, όπου οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα για τους εσωτερικούς τοίχους ούτως ώστε να τα κάνουν ποιο ανθεκτικά στη διάδοση της φωτιάς. Σήμερα αυτός ο όρος πέρασε και στους υπολογιστές και κατέληξε να σημαίνει το software ή το Hardware το οποίο παρεμβάλλεται ανάμεσα στο Wan και στο δικό μας Lan και μας προστατεύει από κακόβουλες επιθέσεις.

Μέχρι τώρα τα Firewalls έχουν περάσει τρεις γενιές και βρίσκονται στην τέταρτη, να δούμε πως άρχισαν.

Πρώτη γενιά προέκυψε το 1988 όταν οι μηχανικοί της Digital Equipment Corporation ανέπτυξαν φίλτρα πακέτων δεδομένων, αυτά τα φίλτρα θεωρούνται η πρώτη γενιά Firewall. Τα φίλτρα λειτουργούσαν με την απλούστερη μορφή όπου, διάβαζαν τα πακέτα δεδομένων που διακινούνταν από το ένα δίκτυο στο άλλο, και εάν κάποιο πακέτο ταίριαζε με κάποιο συγκεκριμένο κανόνα τότε το απέρριπταν. Αυτή η επιλογή υπάρχει ακόμα και σήμερα στα Firewalls αλλά δεν θεωρείτε αξιόπιστη. Επειδή όμως δεν αποθήκευαν πληροφορίες σχετικά με την κατάσταση των διαφόρων συνδέσεων, δηλαδή δεν τα «ενδιέφερε» από ποιον στέλνονται τα πακέτα, βγήκε η δεύτερη γενιά Firewalls από τις εταιρίες Dave Presetto, Howard Trickey και Kshitij Nigam με ορισμένες λειτουργίες παραπάνω και με κύριά τους την εξέταση κατάστασης (state)

του κάθε πακέτου, δηλαδή την σύνδεση από την οποία προήλθε. Τα φίλτρα αυτά κρατούσαν ανά πάσα στιγμή πληροφορίες για τον αριθμό και το είδος των συνδέσεων μεταξύ των δύο δικτύων και επιπλέον μπορούσαν να ξεχωρίσουν εάν ένα πακέτο αποτελεί την αρχή ή το τέλος μιας νέας σύνδεσης ή μέρος μιας ήδη υπάρχουσας. Ύστερα η Τρίτη γενία Firewall βασιζόταν πλέον στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς Open Systems Interconnection. Το κύριο χαρακτηριστικό αυτής της γενιάς ήταν το ότι αντιλαμβανόταν ποια προγράμματα και πρωτόκολλα προσπαθούσαν να δημιουργήσουν μια νέα σύνδεση και με τον τρόπο αυτό μπορούσαν να εντοπίσουν εφαρμογές που προσπαθούσαν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτόκολλου ή μιας υπηρεσίας. Σήμερα στη τέταρτη γενιά Firewall έχουμε γραφικό περιβάλλον μέσο του οποίου εμείς σαν χρήστες μπορούμε να κάνουμε τις επιλογές μας όσον αφορά την ασφάλεια του δικτύου μας και να θέσουμε τους κανόνες βάση των οποίων θα απορρίπτονται κάποια πακέτα ή συνδέσεις.

Εδώ θα αναλύσουμε λίγο ποιο διεξοδικά τη λειτουργία του Firewall. Το Internet όπως όλοι ξέρουμε αποτελείτε από πολλά δίκτυα τα οποία χωρίζονται εκτός των άλλων και με το βαθμό εμπιστοσύνης δηλαδή, το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (Low level of trust), ένα περιμετρικό δίκτυο έχει μεσαίο επίπεδο εμπιστοσύνης (Medium level of trust), ενώ το δίκτυο του σπιτιού μας έχει υψηλό επίπεδο εμπιστοσύνης (High level of trust). Αυτό μας ενδιαφέρει να το γνωρίζουμε διότι ένα Hardware Firewall προστατεύει το εσωτερικό μας δίκτυο (δηλαδή το High level of trust) από εξωτερικές επιθέσεις. Δηλαδή μπαίνει ως ενδιάμεσο τοίχος ανάμεσα στο τοπικό μας δίκτυο και το διαδίκτυο. Το ίδιο κάνει και το software Firewall με μόνη διαφορά στο ότι μπαίνει ανάμεσα στον υπολογιστή μας και στο διαδίκτυο.

Μιλήσαμε παραπάνω για Hardware Firewall και Software Firewall ποιο είναι λοιπόν καλύτερο και γιατί υπάρχουν και τα δύο. Αρχικά τα δύο Firewalls φτιάχτηκαν για να εξυπηρετούν διαφορετικούς σκοπούς, το μεν Hardware Firewall δημιουργήθηκε κυρίως για επιχειρήσεις, οι οποίες έχουν ένα δικό τους τοπικό δίκτυο το οποίο θέλουν να το προστατέψουν από εξωτερικές υποθέσεις. Ενώ το software Firewall δημιουργήθηκε για τους Home Users οι οποίοι το μόνο που θέλουν είναι να προστατέψουν τον προσωπικό τους υπολογιστή. Η διαφορά στη λειτουργία τους είναι ότι το μεν Hardware Firewall δεν καταναλώνει πόρους από τον υπολογιστή μας, είναι σαφώς ποιο γρήγορο (οπότε μπορεί να αποφύγει μία επίθεση DOS) και

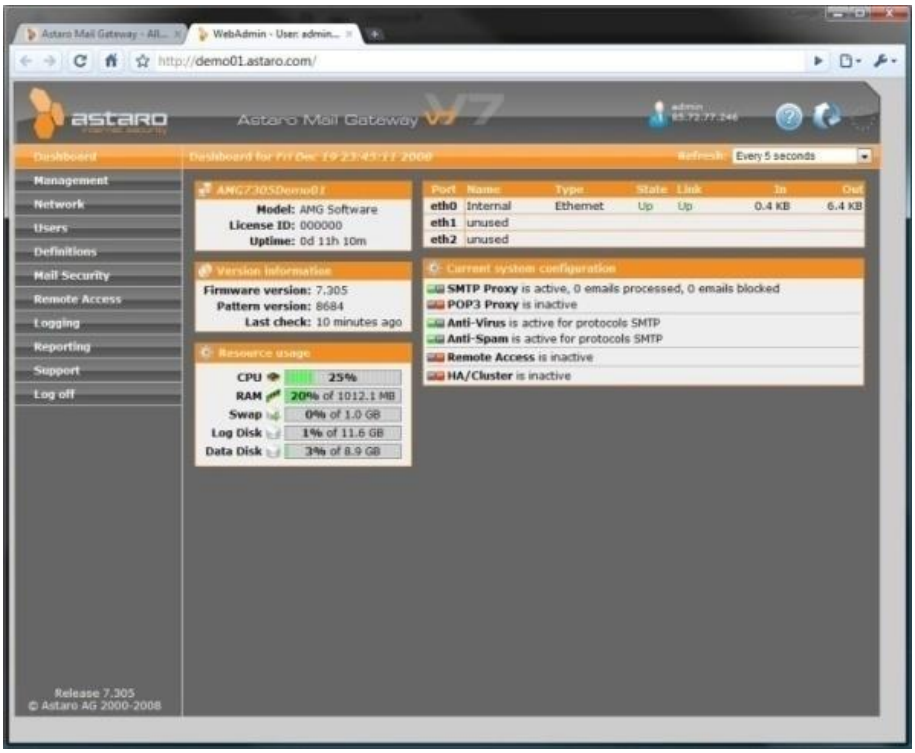
προστατεύει πολλούς υπολογιστές. Αντιθέτως το Software Firewall καταναλώνει πόρους από τον υπολογιστή μας. Το θετικό είναι ότι τώρα πια δέχεται και αυτό παραμετροποιήσεις από εμάς και προστατεύει τον υπολογιστή μας ακόμα και από επιθέσεις που βρίσκονται στο ίδιο τοπικό δίκτυο. Άρα από τα παραπάνω βλέπουμε πως πρέπει να υπάρχει μία συνεργασία Software και Hardware Firewall για να επιτύχουμε την αποτελεσματικότερη αντιμετώπιση κακόβουλων επιθέσεων. Πάντως σε γενικές γραμμές στον τρόπο λειτουργίας τους δεν έχουνε σημαντικές διαφορές.

10.2. Astaro mail gateway

Το Astaro mail gateway είναι μια λύση της εταιρίας Astaro Internet security για την προστασία του ηλεκτρονικού ταχυδρομείου επιχειρήσεων και οργανισμών. Το προϊόν αυτό παρέχεται και σαν υλικό (hardware) αλλά και σαν λογισμικό (software) με τις ίδιες γενικά δυνατότητες ασφάλειας και προστασίας. Η all in one λύση της εταιρίας μπορεί να υποστηρίξει από 1 χρήστη μέχρι 3.000 και να ελέγχει από 50.000 e-mails μέχρι 1.000.000 την ώρα ανάλογα το πακέτο, παρέχει την δυνατότητα φιλτραρίσματος των e-mail από απειλές όπως spam, ιούς και όλες τις γνωστές απειλές που έχουμε αναφέρει. Επίσης παρέχει κρυπτογραφία τύπου S/MIME και PGP, η διαχείρισή του συστήματος μπορεί να γίνει απομακρυσμένα και υπάρχει και η δυνατότητα ο τελικός χρήστης να ελέγχει ανά πάσα στιγμή το είδος του φιλτραρίσματος που θα γίνεται στο e-mail του, να καθορίζει αυτός τα κριτήρια, τους πιστοποιημένους αποστολείς, τις πιστοποιημένες IP διευθύνσεις αποστολής καθώς και τις επιτρεπόμενες επεκτάσεις αρχείων.

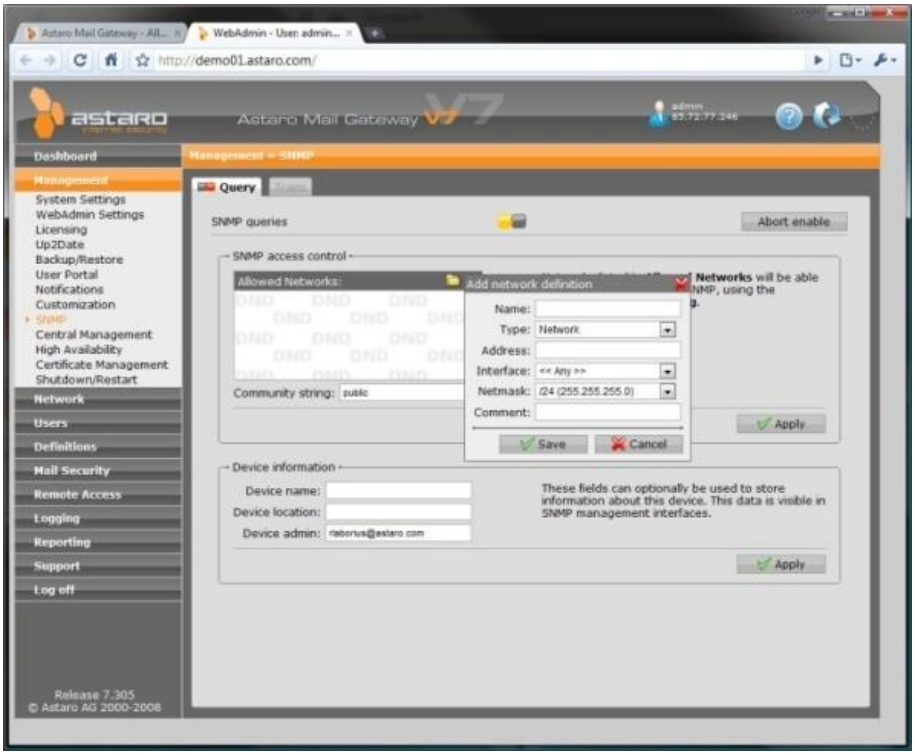
Στις ακόλουθες εικόνες βλέπουμε το περιβάλλον διαχείρισης και μερικές από τις ρυθμίσεις που μπορούμε να κάνουμε μέσα από το live demo της εφαρμογής που βρίσκεται δωρεάν στον ιστότοπο της εταιρίας.

Το αρχικό παράθυρο διαχείρησης του προγράμματος είναι το παρακάτω το οποίο περιέχει κάποιες πληροφορίες για την εφαρμογή, κάποια στατιστικά στοιχεία και την κατάσταση του συστήματος.



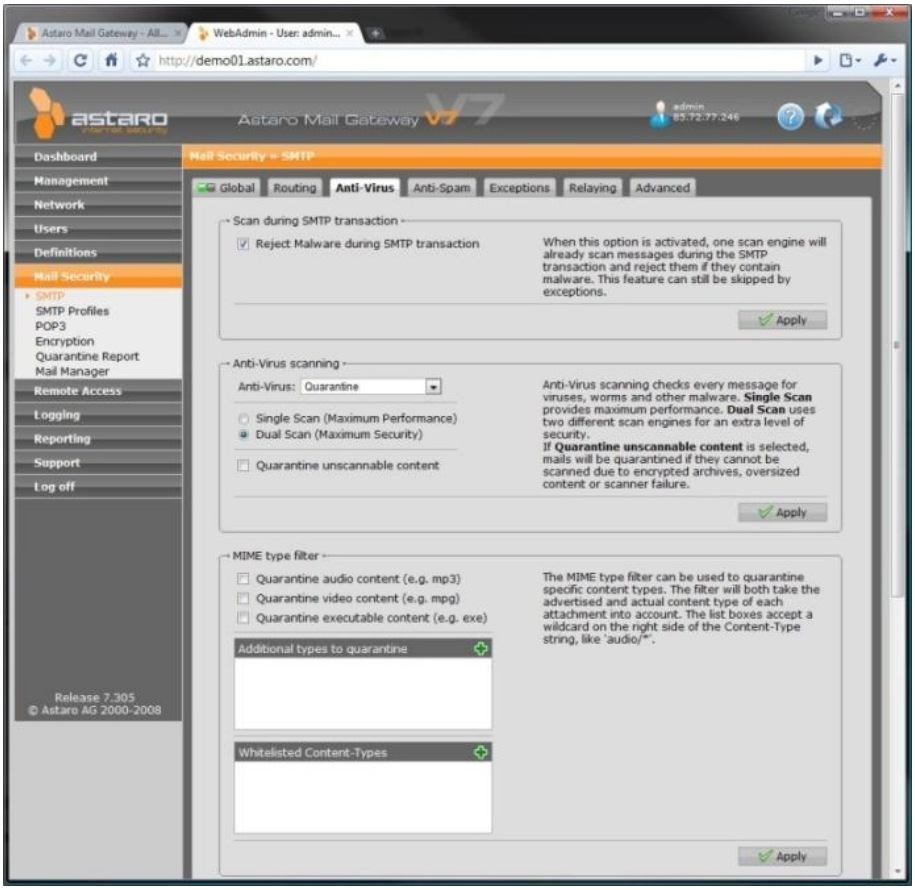
Εικόνα 32 - Astaro Mail Gateway

Στις ρυθμίσεις SNMP μπορεί ο χρήστης να ρυθμίσει τα επιτρεπόμενα δίκτυα από τα οποία το σύστημα θα κάνει προώθηση των e-mail, ρυθμίσεις των επιτρεπόμενων IP κ.α..



Εικόνα 33 - Ρυθμίσεις SNMP

Οι ρυθμίσεις ασφάλειας e-mail μπορεί να γίνει ξεχωριστά για τα πρωτόκολλα SMTP και POP3, οι οποίες θα είναι για anti-virus, anti-spam καθώς και φιλτράρισμα προεκτάσεων αρχείων.



Εικόνα 34 - Anti-Virus Settings

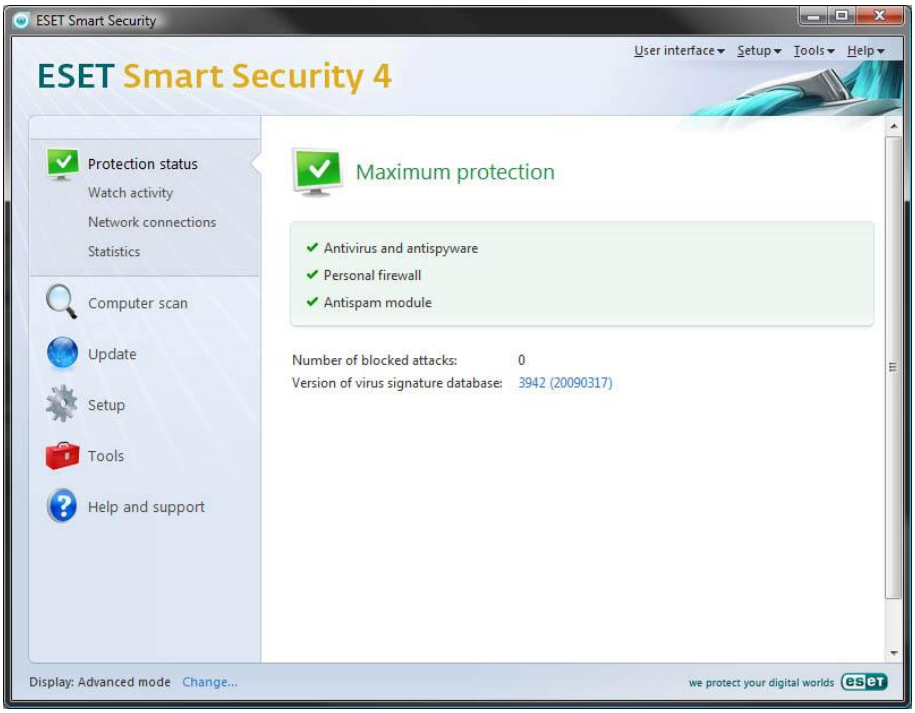
Γενικά, το Astaro mail gateway είναι μία λύση ασφάλειας e-mail η οποία με τις σωστές ρυθμίσεις σε πρωτόκολλα, κρυπτογραφία και φιλτράρισμα μπορεί να παρέχει στους τελικούς χρήστες την ασφάλεια που θέλουν από το ηλεκτρονικό τους ταχυδρομείο και να ελαχιστοποιηθεί ο χαμένος χρόνος του ξεκαθαρίσματος της ανεπιθύμητης αλληλογραφίας.

10.3. ESET Smart Security 4

Σήμερα στην αγορά υπάρχουν αρκετές λύσεις ολοκληρωμένης ασφάλειας, για antivirus, antispam, antispaware και firewall. Εμείς θα παρουσιάσουμε το Smart Security 4 της ESET το οποίο σήμερα θεωρείται από τα καλύτερα για τους λόγους ότι κάνει real time scan στα αρχεία του υπολογιστή και στα εισερχόμενα / εξερχόμενα πακέτα, είναι «ελαφρύ» πρόγραμμα (δεν απαιτεί δηλαδή πολλούς πόρους από το σύστημα) και κάνει συνεχώς update, μέχρι και 5 την μέρα.

Με τις σωστές ρυθμίσεις το Smart Security μπορεί να δουλέψει ικανοποιητικά και σχεδόν «αθόρυβα» παρέχοντας στον χρήστη την ασφάλεια που θέλει από το πρόγραμμα προστασίας του.

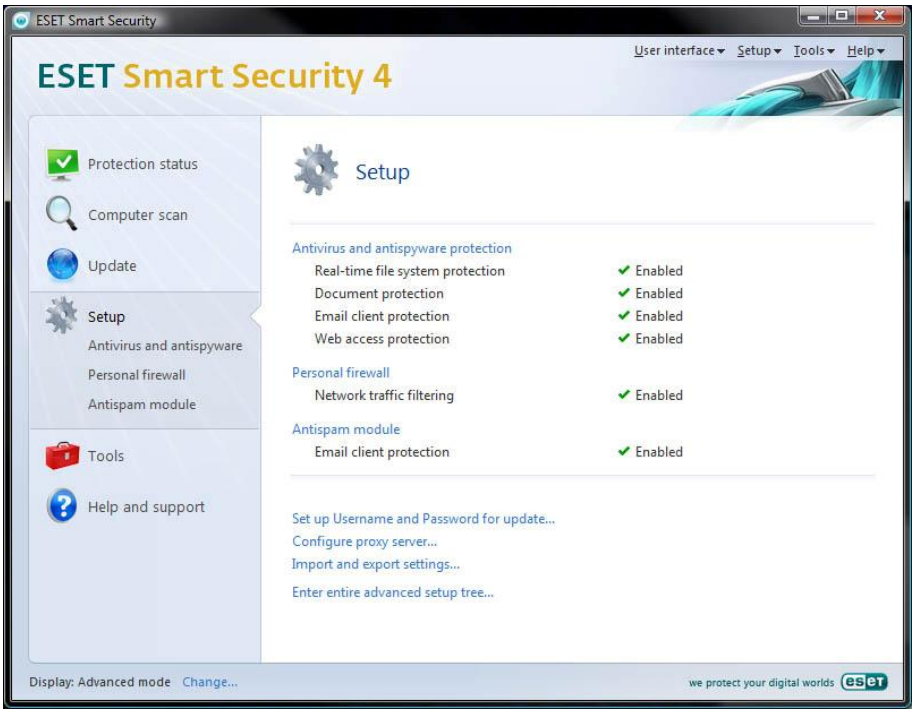
Μετά την εγκατάσταση του προγράμματος, η αρχική οθόνη είναι αυτή:



Εικόνα 35 - ESET Smart Security 4

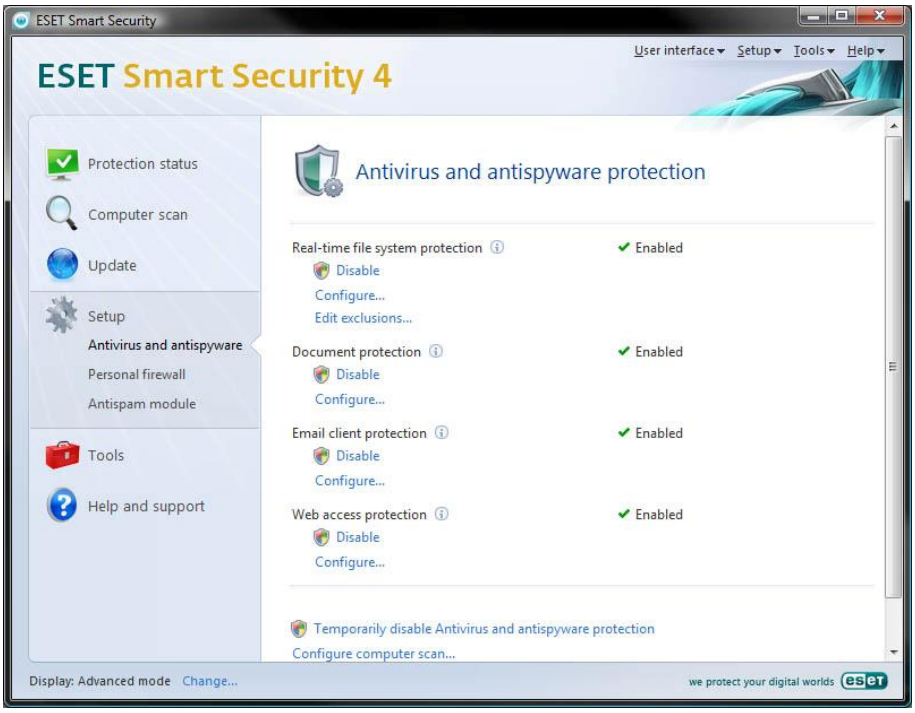
Όπως βλέπουμε είναι εξ' ορισμού ενεργοποιημένο το antivirus & antispyware, το firewall και το antispam. Στην αρχική οθόνη επίσης μας ενημερώνει για τις απειλές που έχει εντοπίσει και έχει μπλοκάρει καθώς και για την έκδοση του update που βρίσκεται αυτή τη στιγμή.

Για τις ρυθμίσεις του μας ενδιαφέρει κυρίως το menu Setup το οποίο φαίνεται στην παρακάτω εικόνα.



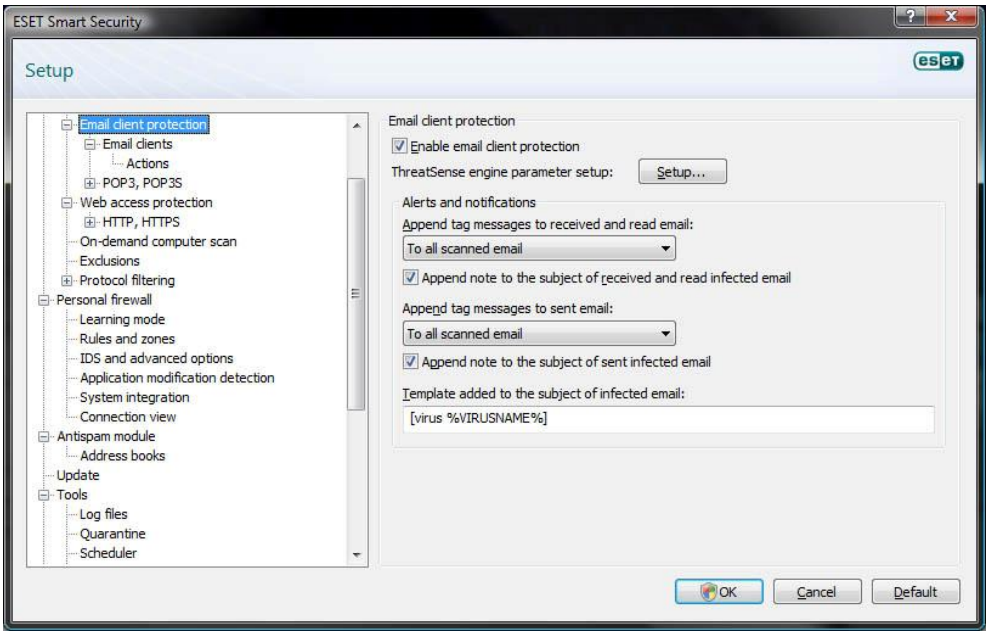
Εικόνα 36 - Setup

- *Antivirus & Antispyware.*



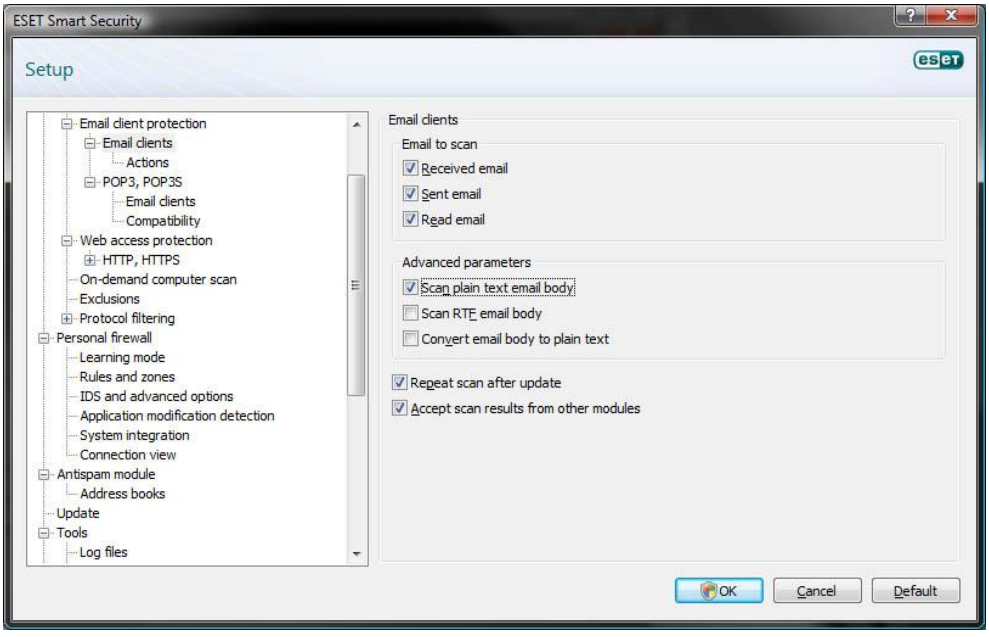
Εικόνα 37 - Antivirus & Antispyware

Εδώ αφήνουμε τις επιλογές Real-time system protection και Document protection όπως είναι και πάμε στις ρυθμίσεις για E-mail client protection που μας απασχολεί κυρίως.



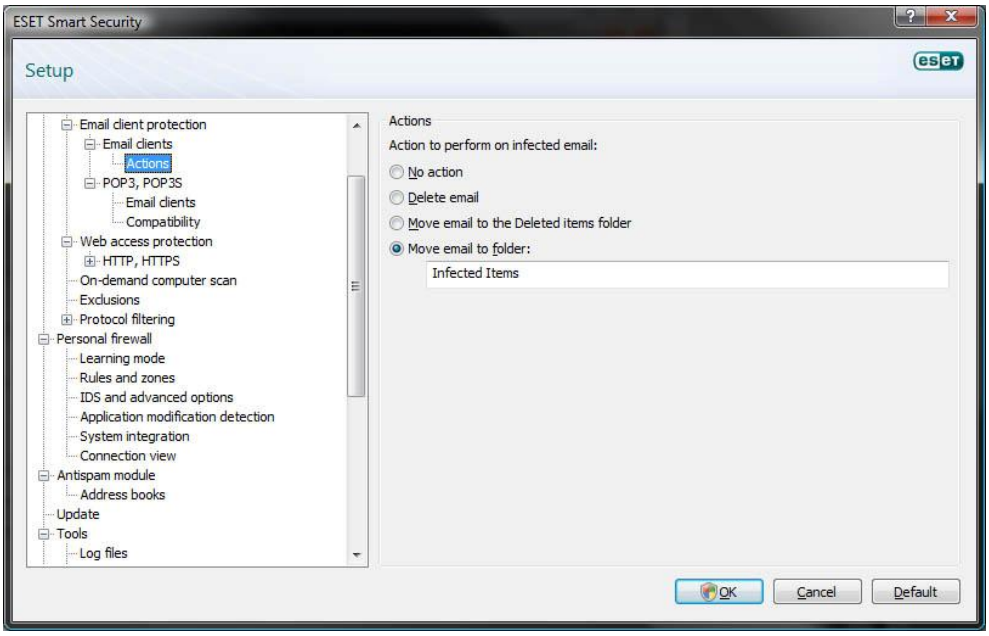
Εικόνα 38 - E-mail client protection

Στο menu E-mail clients επιλέγουμε ποια αλληλογραφία θα ελέγχει, εισερχόμενη, εξερχόμενη κλπ., και αν θέλουμε επιλέγουμε να ελέγχει και το κυρίως σώμα κειμένου του e-mail.



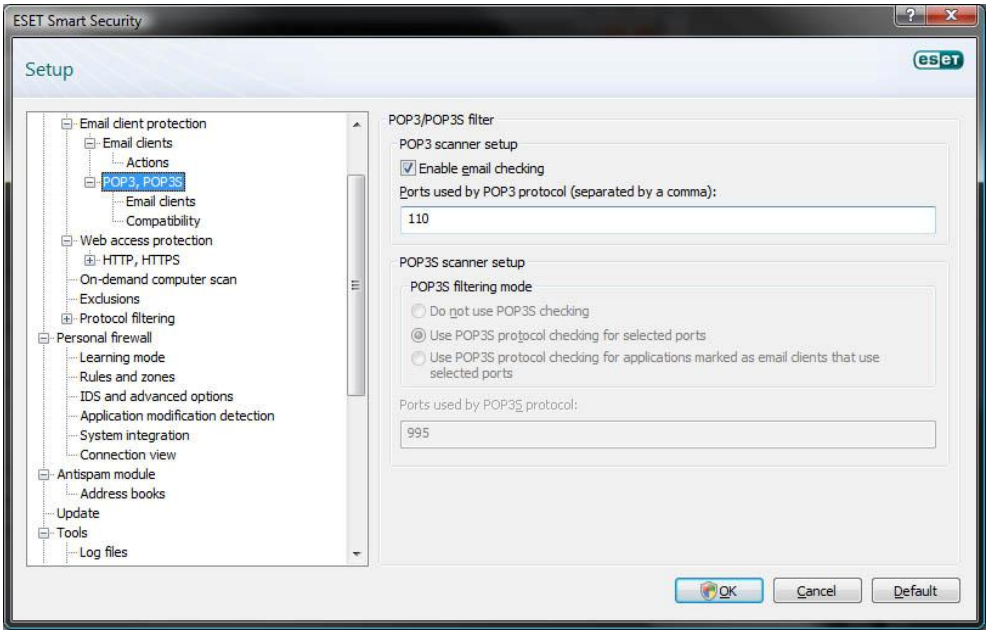
Εικόνα 39 - E-mail clients

Στη συνέχεια στο menu Action επιλέγουμε τι ενέργειες θα κάνει για τα e-mail που έχει εντοπίσει ως μολυσμένα. Εξ' ορισμού είναι επιλεγμένη η μεταφορά στον φάκελο Infected Items.



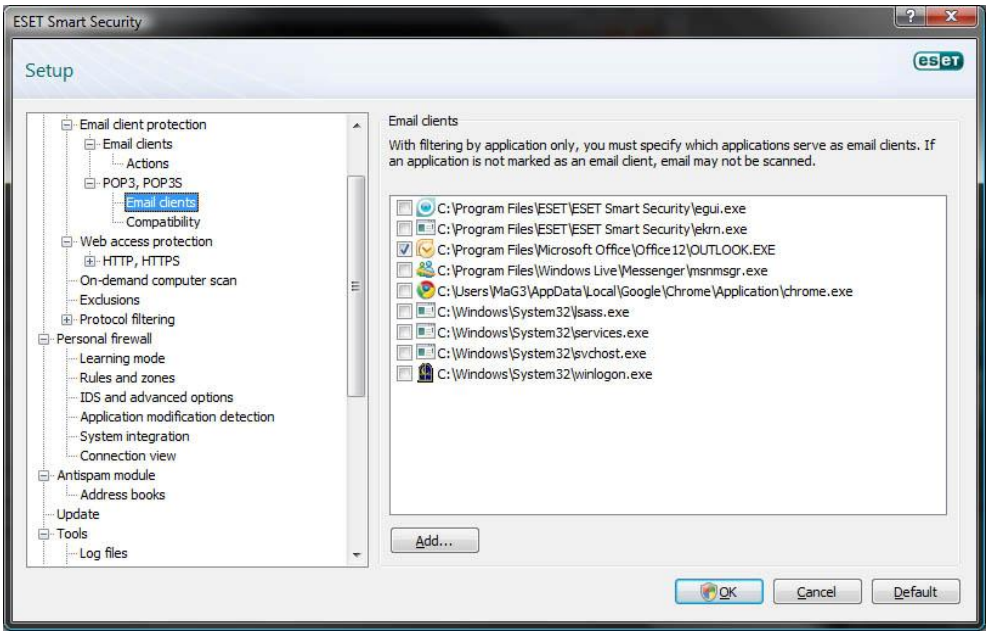
Εικόνα 40 - Actions

Έπειτα στο menu POP3, POP3S ρυθμίζουμε την πόρτα που χρησιμοποιούμε για την εισερχόμενη αλληλογραφία και αν χρησιμοποιούμε περισσότερες από μια, τις χωρίζουμε με κόμμα (,).



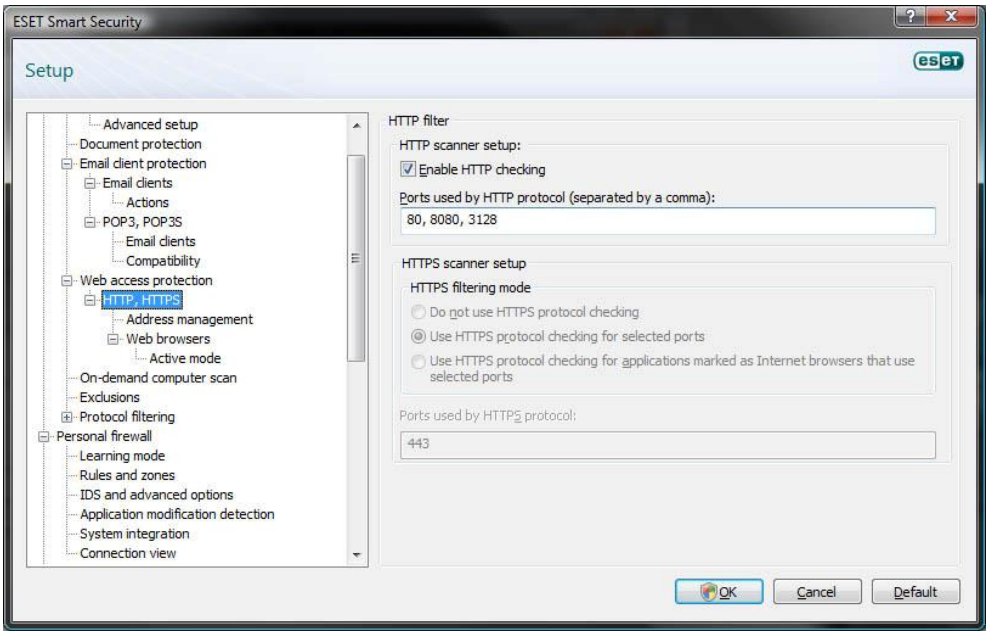
Εικόνα 41 - POP3/POP3S filter

Στο menu E-mail clients επιλέγουμε την εφαρμογή ή τις εφαρμογές που χρησιμοποιούμε για την αλληλογραφία μας. Στην περίπτωση μας είναι το Microsoft Outlook.



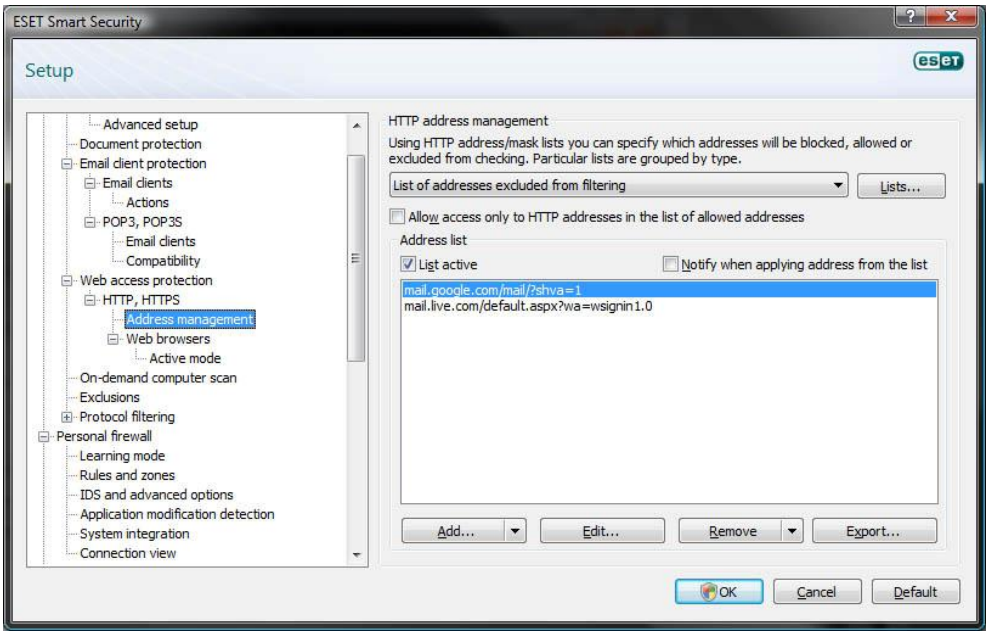
Εικόνα 42 - E-mail clients

Στη συνέχεια κάνουμε ρυθμίσεις για την αλληλογραφία που χρησιμοποιούμε μέσω πρόσβασης web για τα πρωτόκολλα HTTP και HTTPS. Ρυθμίζουμε τις πόρτες που θα ελέγχει το πρόγραμμα οι οποίες συνήθως είναι οι προκαθορισμένες 80, 8080, 3128.



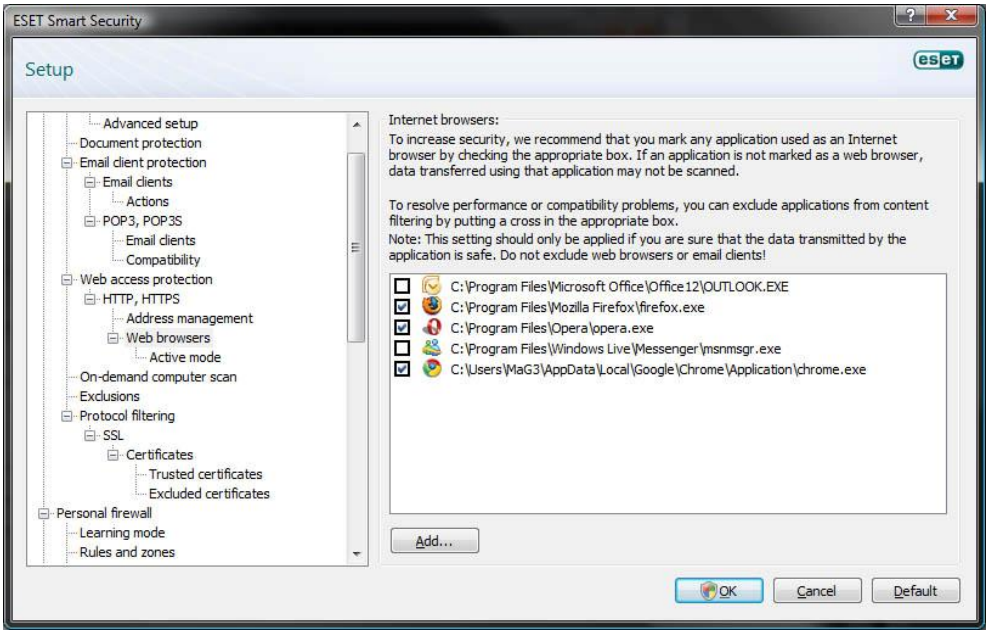
Εικόνα 43 - HTTP filter

Στο menu Address management προσθέτουμε τα URL των web mail μας. Εμείς έχουμε ένα λογαριασμό από το Gmail.com και ένα από το Hotmail.com. Τα URL αυτά είναι οι σελίδες που ανοίγουν στο web mail μας όταν έχουμε εισέλθει στην υπηρεσία.



Εικόνα 44 - HTTP address management

Στη συνέχεια επιλέγουμε τους browser που θέλουμε να ελέγχει το πρόγραμμα. Αυτούς δηλαδή που χρησιμοποιούμε συνήθως για την ανάγνωση της. Εμείς έχουμε επιλέξει τον Firefox, τον Chrome και τον Opera.



Εικόνα 45 - Web browsers

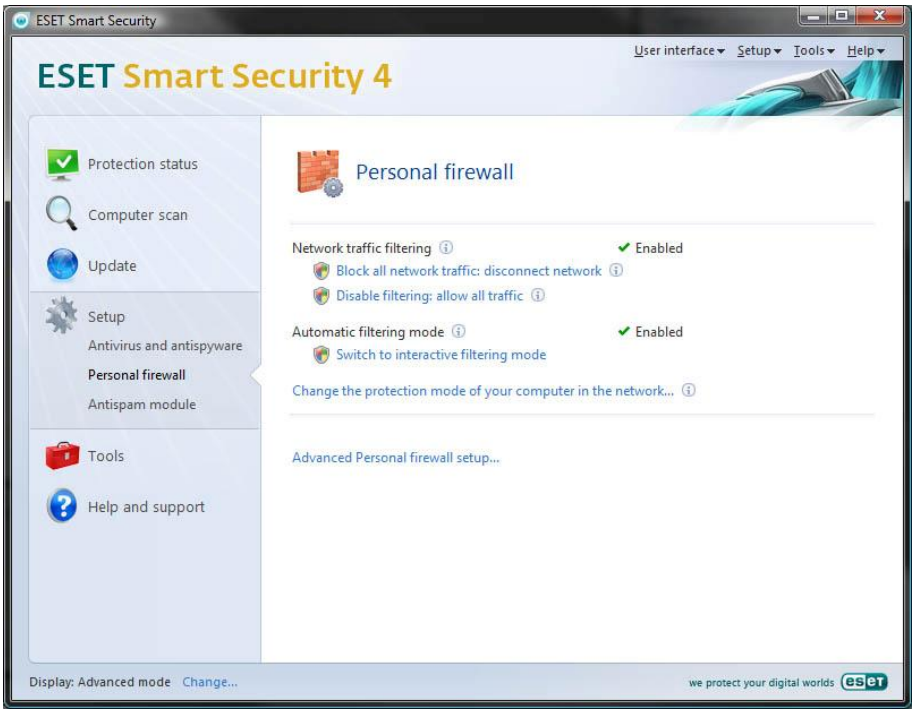
Τέλος από το Protocol filtering **à** SSL μπορούμε να ρυθμίσουμε το σύνολο των πρωτοκόλλων και των πιστοποιητικών που θα ελέγχει το πρόγραμμα.

Αυτές είναι οι βασικότερες ρυθμίσεις που πρέπει να κάνουμε για ένα ικανοποιητικό επίπεδο ασφάλειας στον υπολογιστή μας. Υπάρχουν βέβαια και άλλες οι οποίες

απαιτούν περισσότερο εξειδικευμένες γνώσεις πάνω σε πρωτόκολλα και πληροφορίες που θα πρέπει να γνωρίζουμε για τον mail server μας.

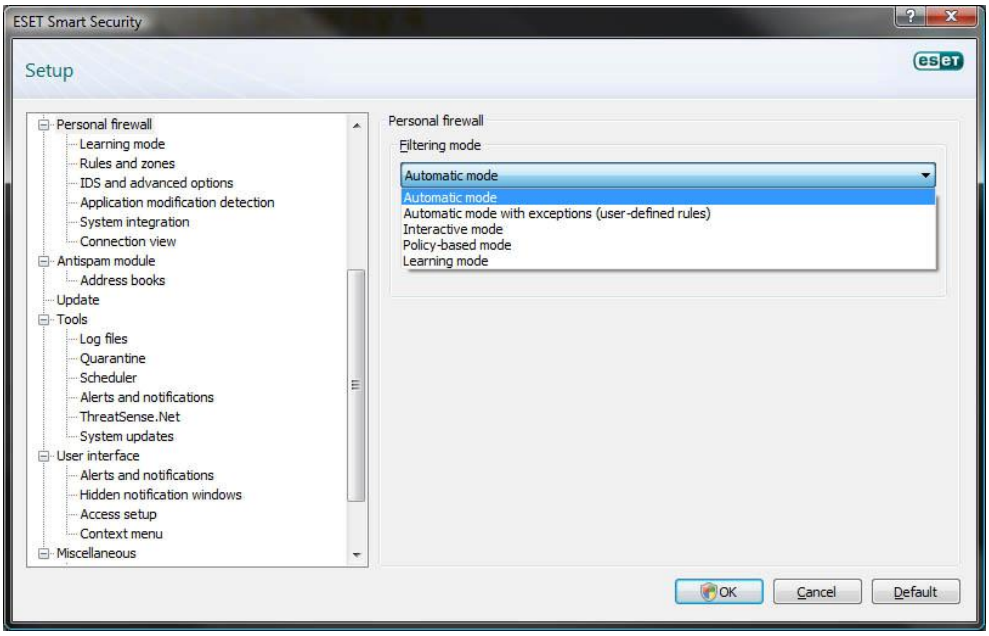
- *Personal Firewall*

Στο menu αυτό κάνουμε τις ρυθμίσεις για το Firewall, ποια προγράμματα δηλαδή θα επιτρέπουμε να μεταφέρουν δεδομένα ελεύθερα και ποια όχι. Η αρχική οθόνη των ρυθμίσεων του Firewall είναι αυτή.



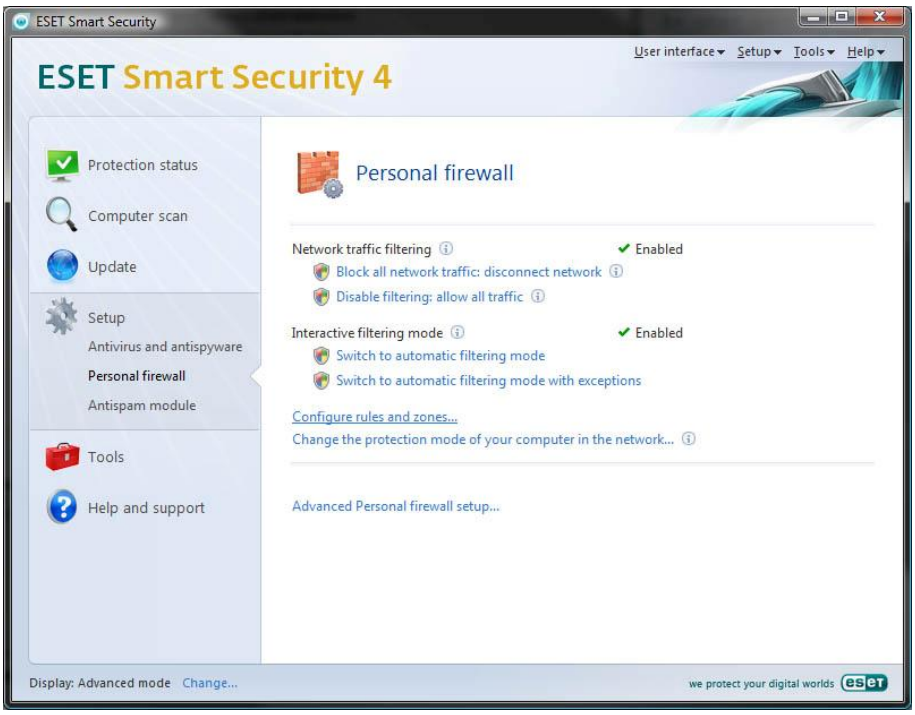
Εικόνα 46 - Personal firewall

Πατώντας στο Advanced Personal Firewall setup… μπορούμε να κάνουμε τις ρυθμίσεις που θέλουμε για το Firewall μας. Αν δεν έχουμε πολλές γνώσεις πάνω σε πρωτόκολλα και εφαρμογές καλύτερο είναι να επιλέξουμε το Automatic mode with exceptions (user-defined rules).

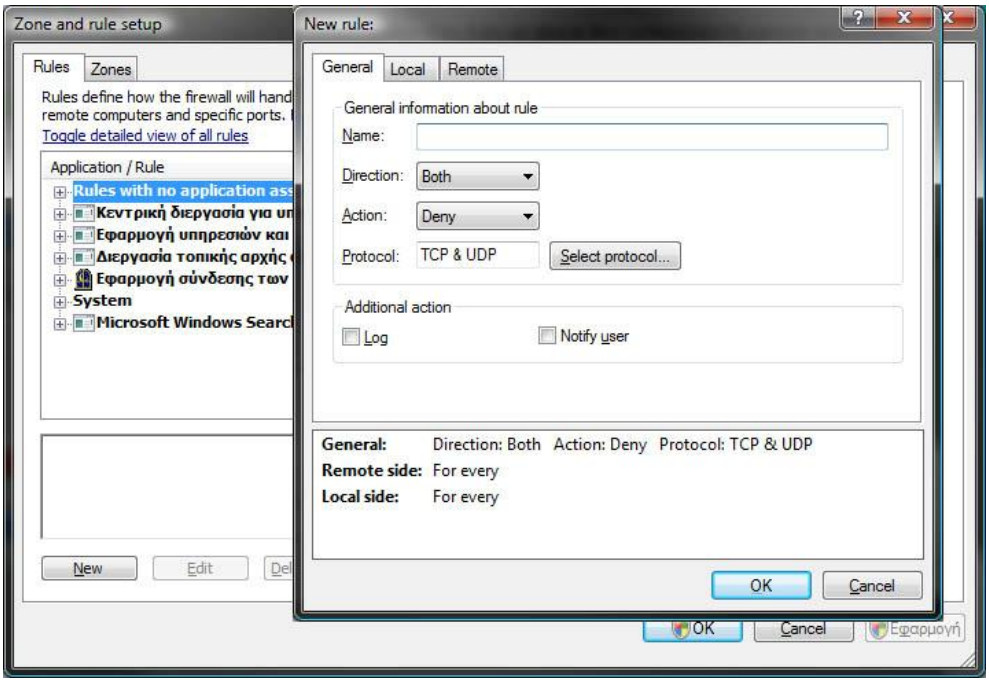


Εικόνα 47 - Personal firewall setup

Εξ' ορισμού όλες οι εφαρμογές που προσπαθούν να μεταφέρουν δεδομένα ελέγχονται από το πρόγραμμα. Στην επιλογή Configure rules and zones ορίζουμε ποια προγράμματα θα περνάνε ελεύθερα δεδομένα όπως είπαμε παραπάνω. Συνήθως εδώ ρυθμίζουμε προγράμματα p2p, torrent κλπ για να μπορούν να κατεβάζουν γρηγορότερα.



Εικόνα 48 - Personal firewall



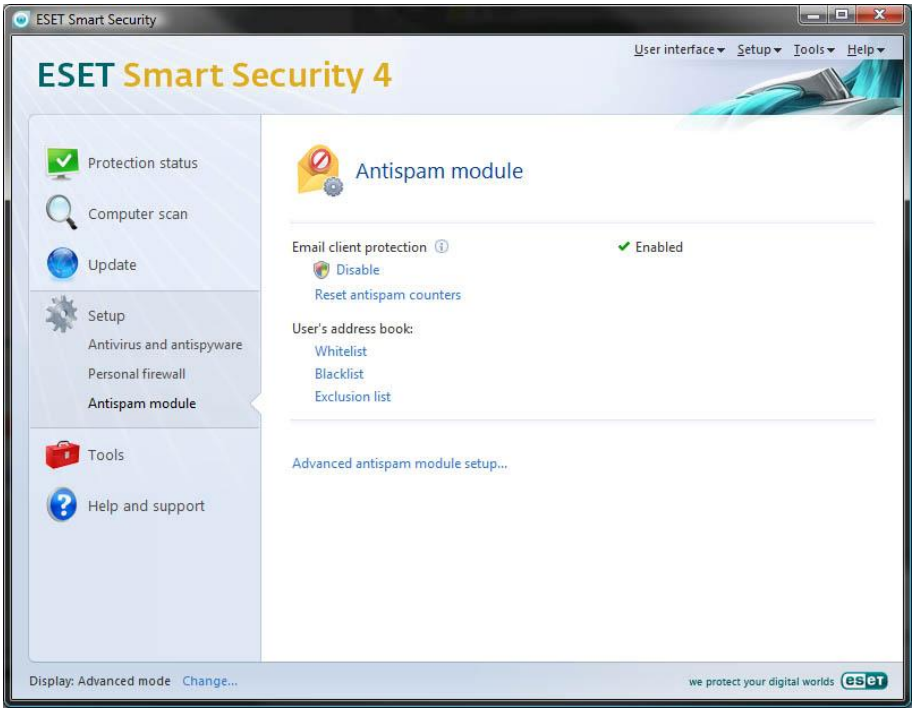
Εικόνα 49 - Zone and rule setup

Για να ορίσουμε ποια προγράμματα θα μεταφέρουν ελεύθερα δεδομένα πρέπει να ορίζουμε το όνομα της εφαρμογής και τις πόρτες που θα χρησιμοποιούν. Επίσης έχουμε και την επιλογή να ορίζουμε ποιες εφαρμογές θα μπλοκάρει το πρόγραμμα. Τέλος η επιλογή των κανόνων για τα προγράμματα μπορεί να γίνει και όταν κάποιο πρόγραμμα κάνει αίτηση για αποστολή δεδομένων στο Internet που το Smart Security θα εμφανίσει ένα pop up παράθυρο σαν αυτά για την επιλογή της ενέργειας.

Εικόνα 50 - Outbound traffic pop up

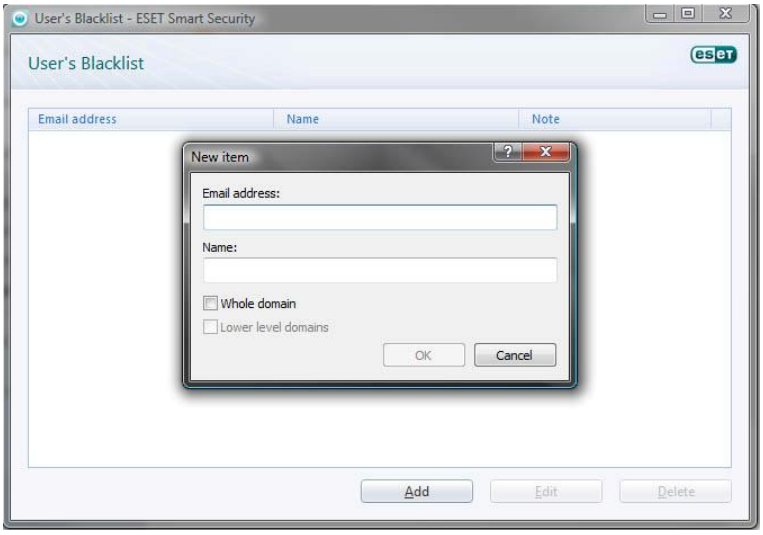
Εικόνα 51 - Inbound traffic pop up

- *Antispam module*



Εικόνα 52 - Antispam module

Εδώ έχουμε την δυνατότητα να επιλέξουμε διευθύνσεις χρηστών που θα επιτρέπονται (whitelist) και διευθύνσεις που θα απορρίπτονται (blacklist).



Εικόνα 53 - User's Blacklist

Αυτές είναι όλες οι βασικές ρυθμίσεις που πρέπει να γίνουν στο πρόγραμμα για τον έλεγχο της αλληλογραφίας, τους χρήστες και τις εφαρμογές. Υπάρχουν και άλλες ρυθμίσεις όπως αναφέραμε και παραπάνω αλλά απαιτούν εξειδικευμένες γνώσεις σε πρωτόκολλα και στον τρόπο λειτουργίας των mail servers.

Συμπεράσματα

Με την ολοκλήρωση αυτής της εργασίας καταλήξαμε στα εξής συμπεράσματα:

- Με την όλο και αυξανόμενη χρήση του Internet και των υπηρεσιών του, η ανάγκη για ασφάλεια όλο και μεγαλώνει καθώς συνεχώς οι crackers και οι hackers ανακαλύπτουν καινούριους τρόπους για την παραβίαση των συστημάτων ασφάλειας και κενά στα πρωτόκολλα που χρησιμοποιούνται. Οπότε αυτά με τη σειρά τους πρέπει να γίνονται περισσότερο ασφαλή και περίπλοκα. Δεν μπορούμε να πούμε πως ένα σύστημα είναι πλήρως ασφαλές αλλά η ικανοποιητική ασφάλεια μπορεί να προσεγγιστεί με συνδυασμό μεθόδων. Το διαδίκτυο συνεχώς θα εξελίσσεται και νέες απειλές θα εμφανίζονται. Η καταπολέμηση τους είναι θέμα χρόνου από την εμφάνιση τους.
- Το ηλεκτρονικό ταχυδρομείο που όπως έχουμε αναφέρει και πάλι αποτελεί μια από τις δημοφιλέστερες υπηρεσίες του Internet κρύβει κινδύνους και απειλές οι οποίες μέχρι ένα βαθμό μπορούν να καταπολεμηθούν, με την χρήση προγραμμάτων και συσκευών. Το ηλεκτρονικό ταχυδρομείο είναι μια υπηρεσία με τάση συνεχώς να αυξάνεται η δημοτικότητά της μιας και αποτελεί τον βασικό τρόπο ηλεκτρονικής επικοινωνίας. Άρα συνεχώς θα εξελίσσεται και θα προστατεύεται από εταιρίες και οργανισμούς με αυτόν το σκοπό. Αλλά αυτό που πρέπει να κάνει ο κάθε χρήστης για να προστατευθεί είναι να είναι ενήμερος και προσεκτικός στο πως την χρησιμοποιεί. Πρέπει να μπορεί να αναγνωρίζει πότε πρόκειται για αλληλογραφία η οποία είναι σημαντική για αυτόν και πότε είναι κακόβουλη ή απλά άχρηστη. Σε αυτό βοηθούν όσο μπορούν και οι ίδιοι οι πάροχοι της. Αυτό φαίνεται και από τα ποσοστά ανεπιθύμητης αλληλογραφίας που καταλήγει στα mail box των χρηστών σήμερα σε σχέση με το παρελθόν.

«Ο άνθρωπος είναι ο πιο αδύναμος κρίκος σε οποιοδήποτε σύστημα ασφαλείας»

Kevin David Mitnick

Παράρτημα

Ερωτηματολόγιο

Χρησιμοποιείτε κάποια λύση συνεργατικής επικοινωνίας που βασίζεται στην ηλεκτρονική αλληλογραφία όπως το Microsoft Exchange ή το Lotus Notes;

Ποιο πρωτόκολλο μπορεί να χρησιμοποιήσει ο χρήστης για τη μεταφορά της ηλεκτρονικής αλληλογραφίας του, από τον διακομιστή στον υπολογιστή του;

1. IMAP ☐
2. POP3 ☐
3. IMAP over SSL ☐
4. POP3 over SSL ☐
5. MAPI ☐
6. NRPC ☐

Ο mail server είναι ιδιόκτητος ή χρησιμοποιείται Outsourcing εταιρία. Στην περίπτωση της εταιρίας – οργανισμού, ποιας και γιατί έγινε η συγκεκριμένη επιλογή;

Αν είναι ιδιόκτητος ποια λύση Hardware ή software χρησιμοποιείται για την ασφάλεια σε επιθέσεις spoof;

Αν είναι ιδιόκτητος ποια λύση Hardware ή Software χρησιμοποιείται για την ασφάλεια σε επιθέσεις spam;

Αν είναι ιδιόκτητος ποια λύση Hardware ή Software χρησιμοποιείται για την ασφάλεια σε επιθέσεις virus;

Από τον client στον server τι σύστημα κρυπτογράφησης χρησιμοποιείται και γιατί επιλέχτηκε αυτό;

Στην περίπτωση του ιδιόκτητου mail server τι μέθοδος κρυπτογράφησης χρησιμοποιείται για την επικοινωνία με άλλους mail servers;

Τι ποσοστά spamming δέχεστε (κατά μέσο όρο);

Έχει υπάρξει μέχρι τώρα επίθεση spoofing στο σύστημα σας;

Έχει πραγματοποιηθεί ποτέ, ενδοδικτυακή επίθεση, αν ναι πια ήταν (spamming, mail Bombs, κτλ);

Τι άλλου είδους επιθέσεις έχει δεχτεί το σύστημά σας;

Ο χρήστης μπορεί να διαχειριστεί το mail box του μέσω κάποιου browser; Αν ναι ποιο πρωτόκολλο ασφαλείας χρησιμοποιείται για τη σύνδεση (SHTTP, SSL);

Ορολογία

ASCII	(American Standard Code for Information Interchange), Αμερικανικός Πρότυπος Κώδικας για Ανταλλαγή Πληροφοριών) είναι ένα κωδικοποιημένο σύνολο χαρακτήρων του λατινικού αλφάβητου όπως αυτό χρησιμοποιείται σήμερα στην Αγγλική γλώσσα και σε άλλες δυτικοευρωπαικές γλώσσες. Χρησιμοποιείται κυρίως στους υπολογιστές και άλλες συσκευές τηλεπικοινωνίας για αναπαράσταση κειμένου, καθώς επίσης για έλεγχο συσκευών που δουλεύουν με κείμενο.
Blacklist	Λίστες που περιέχουν τους χρήστες από τους οποίους **δεν** επιθυμούμε να λαμβάνουμε την ηλεκτρονική αλληλογραφία.
Block	Τμήμα κειμένου.
Browser	Φυλλομετρητής. Πρόγραμμα το οποίο επιτρέπει να βλέπουμε και να περιηγούμαστε σε ιστοσελίδες στο διαδίκτυο.
Ciphertext	Κείμενο το οποίο έχει υποστεί κρυπτογράφηση.
Client	Πελάτης ή εξυπηρετούμενος. Συνήθως είναι οι χρήστες. Αυτοί δηλαδή οι οποίοι κάνουν αιτήσεις στους εξυπηρετητές για την παροχή κάποιας υπηρεσίας.
CPU	Central processing unit. Κεντρική μονάδα επεξαιργασίας.
Cracker	Είναι ο άνθρωπος που χρησιμοποιώντας τα κενά ασφαλείας και διάφορα προγράμματα, καταφέρνει να κερδίζει πρόσβαση παράνομα ξεπερνώντας τα συστήματα ασφαλείας με σκοπό να βλάψει το λογισμικό ή το σύστημα το οποίο έχει στοχεύσει.
DDos	Distributed Denial of Service Attacks: είναι ένα είδος κατανεμημένων επιθέσεων που οφείλουν την αποτελεσματικότητά τους στο γεγονός ότι ένας τεράστιος αριθμός κόμβων επιτίθενται την ίδια χρονική περίοδο σε έναν μεμονωμένο host με σκοπό να εξαντλήσουν τους πόρους του συστήματός του και να τον αναγκάσουν να αρνηθεί τις υπηρεσίες του στους πελάτες του.
E-mail	Ηλεκτρονικό μήνυμα το οποίο έρχεται και στην ηλεκτρονική θυρίδα mailBox
Hacker	Είναι αυτός που συλλέγει γνώση για ένα λογισμικό, κερδίζει πρόσβαση σε σημεία που ένας χρήστης δεν ξέρει ή δεν μπορεί να έχει, και βάση των γνώσεων του το επεκτείνει δίνοντας του νέες δυνατότητες ή διορθώνοντας προβλήματά του (bugs).
Hardware	Είναι τα υλικά μέρη ενός υπολογιστικού συστήματος όπως σκληρός δίσκος, κάρτα γραφικών, μητρική, επεξεργαστής.
LAN	Local Area Network.
Mailbox	Το ηλεκτρονικό γραμματοκιβώτιο των χρηστών.
NIST	National Institute of Standards and Technology
Operator	Ο χείριστης ενός συστήματος.
OSI	Μοντέλο αναφοράς OSI. Περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων.
Plaintext	Είναι το μη διαμορφωμένο κείμενο το οποίο αποτελείται από ACSII 7 ή 8bit

	χαρακτήρες.
Server	Εξυπηρετητής. Το υπολογιστικό σύστημα που παρέχει υπηρεσίες στους εξυπηρετούμενους, για παράδειγμα υπηρεσίες web, mail κλπ..
Software	Είναι το λογισμικό ενός υπολογιστικού συστήματος όπως λειτουργικό σύστημα και τα προγράμματα.
WAN	Wide Area Network.
Whitelist	Λίστες που περιέχουν τους χρήστες από τους οποίους επιθυμούμε να λαμβάνουμε την ηλεκτρονική αλληλογραφία.
Bot	Είναι ή τα προγράμματα που χρησιμοποιούνται για να αυτοματοποιηθούν απλές διαδικασίες όπως οι αλλαγές στο περιεχόμενο των ιστοσελίδων (ώστε να τις βρίσκουν ποιο εύκολα τα προγράμματα αναζήτησης) ή αυτό που μας ενδιαφέρει περισσότερο, αν ένας υπολογιστής γίνει Bot ή ζόμπι από κάποιον Cracker τότε εκτελεί διαδικασίες κατά βούληση του Cracker και τις περισσότερες φορές χωρίς να τις καταλάβει ο νόμιμος χρήστης του υπολογιστή. Συνήθως η διαδικασίες αυτές είναι ή να στέλνεις spams ή επιθέσεις DDos.
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων. Ανεξάρτητη Αρχή η οποία αποτελεί τον Εθνικό Ρυθμιστή που ελέγχει, ρυθμίζει και εποπτεύει: (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφορά
ΕΠΑΚ	Ενιαίος Πανελλαδικός Αριθμός Κλήσης. Ειδικός αριθμός κλήσης για την σύνδεση στο Internet.
Πάγωμα	Χρησιμοποιείται ο όρος Πάγωμα, όταν κάτι έχει πάει στραβά με το λογισμικό του υπολογιστή μας και δεν μπορεί να ανταποκριθεί σε καμία κίνηση που του ζητάμε. Σε αυτή τη περίπτωση πρέπει να γίνει είτε επανεκκίνηση του συστήματος, είτε να αναμένουμε το "ξεπάγωμα" του συστήματος.

Βιβλιογραφία

Βιβλία:

Douglas E. Comer, *Δίκτυα και Διαδίκτυα Υπολογιστών – και εφαρμογές τους στο Internet*, Εκδόσεις Κλειδάριθμος.

James Stanger, *E-mail Virus Protection Handbook*, Εκδόσεις Syngress.

Joel Scambray – Stuart McClure – George Kurtz, *Χάκερ Επίθεση και Άμυνα - Τέταρτη Έκδοση 2003*, Εκδόσεις Μ. Γκιούρδας.

Στέφανος Γκρίτζαλης – Σωκράτης Κ. Κάτσικας, *Ασφάλεια Δικτύων Υπολογιστών – Τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης*, Εκδόσεις Παπασωτηρίου.

Σωκράτης Κ. Κάτσικας - Δημήτρης Γκρίτζαλης - Στέφανος Γκρίτζαλης, *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδόσεις Νέων Τεχνολογιών.

Internet:

http://blog.tech-spot.gr/2007/11/11/386/ - *21 Δεκεμβρίου 2008*
http://blogs.in.gr/gepitidios/archive/2008/02/01/624.aspx - *12 Νοεμβρίου 2008*
http://blogs.technet.com/pamal/archive/2006/02/10/419211.aspx - *12 Δεκεμβρίου 2008*
http://blogs.technet.com/user/Profile.aspx?UserID=6001 – *12 Δεκεμβρίου 2008*
http://chtsanti.net/Firewall.html - *7 Νοεμβρίου 2008*
http://el.wikipedia.org/wiki/E-mail_bomb - *28 Νοεμβρίου 2008*
http://el.wikipedia.org/wiki/Post_Office_Protocol - *20 Ιανουαρίου 2009*
http://el.wikipedia.org/wiki/SMTP - *5 Δεκεμβρίου 2008*
http://en.wikipedia.org/wiki/IBM_Lotus_Notes - *21 Ιανουαρίου 2009*
http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol – *20 Ιανουαρίου 2009*
http://en.wikipedia.org/wiki/Microsoft_Exchange_Server - *21 Ιανουαρίου 2009*
http://en.wikipedia.org/wiki/Pop3 - *5 Δεκεμβρίου 2008*
http://en.wikipedia.org/wiki/Sender_Policy_Framework - *22 Δεκεμβρίου 2008*
http://kameleon-nest.blogspot.com/2008/04/google-hacking-1.html - *22 Νοεμβρίου 2008*
http://mail.google.com/support/bin/answer.py?answer=25760 – *6 Νοεμβρίου 2008*
http://news.pramnos.net/story58-1239.html - *12 Νοεμβρίου 2008*
http://office.microsoft.com/el-gr/outlook/HA012316671032.aspx - *7 Νοεμβρίου 2008*
http://searchexchange.techtarget.com/sDefinition/0,,sid43_gci214084,00.html – *7 Νοεμβρίου 2008*
http://spamassassin.apache.org/doc.html - *19 Μαρτίου 2009*
http://spamassassin.apache.org/index.html - *19 Μαρτίου 2009*
http://techblog.gr/Internet/symantec-spam-report-july07/ - *8 Νοεμβρίου 2008*
http://tovima.dolnet.gr/print_article.php?e=B&f=15060&m=D22&aa=1 – *22 Νοεμβρίου 2008*
http://www.adslgr.com/forum/archive/index.php/t-26776.html - *6 Νοεμβρίου 2008*
http://www.adslgr.com/forum/archive/index.php/t-7270.html - *20 Δεκεμβρίου 2008*
http://www.akazoo.gr/Forum/Forum.aspx?node=forum&g=posts&t=1759 – *3 Δεκεμβρίου 2008*
http://www.astaro.com/our_products/astaro_mail_gateway - *25 Ιανουαρίου 2009*
http://www.astaro.com/our_products/astaro_mail_gateway/hardware_appliances - *25 Ιανουαρίου 2009*
http://www.astaro.com/our_products/astaro_mail_gateway/virtual_appliance - *25 Ιανουαρίου 2009*
http://www.chiosnews.com/cn1025200520027AM0.asp - *6 Νοεμβρίου 2008*
http://www.clamav.net/ - *19 Μαρτίου 2009*
http://www.clamav.net/about/ - *19 Μαρτίου 2009*

http://www.crestock.com/vector/padlock.aspx - *21 Δεκεμβρίου 2008*
http://www.dkim.org/#introduction – *11 Ιανουαρίου 2009*
http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL – *7 Δεκεμβρίου 2008*
http://www.eeei.gr/interbiz/articles/hoaxes.htm - *3 Δεκεμβρίου 2008*
http://www.eeei.gr/interbiz/articles/security.htm - *21 Δεκεμβρίου 2008*
http://www.epaggelmaties.com/writer/2001-2003/teyxos210.html - *28 Νοεμβρίου 2008*
http://www.e-pcmag.gr/modules/news/article.php?storyid=5106 – *11 Ιανουαρίου 2009*
http://www.e-yliko.gr/htmls/pc_use/smail.aspx - *6 Νοεμβρίου 2008*
http://www.faqs.org/rfcs/rfc821.html - *5 Δεκεμβρίου 2008*
http://www.forthnet.gr/templates/viewcontentTmArt.aspx?p=102396 – *3 Δεκεμβρίου 2008*
http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043 – *7 Δεκεμβρίου 2008*
http://www.freegr.gr/freenuke/modules.php?name=Forums&file=viewtopic&t=2828 – *28 Νοεμβρίου 2008*
http://www.freestuff.gr/forums/viewtopic.php?t=30605 – *12 Δεκεμβρίου 2008*
http://www.geocities.com/circuits01/spam.html - *8 Νοεμβρίου 2008*
http://www.go-online.gr/ebusiness/specials/article.html?article_id=1327 – *28 Νοεμβρίου 2008*
http://www.go-online.gr/ebusiness/specials/article.html?article_id=423 – *12 Δεκεμβρίου 2008*
http://www.imap.org/ - *20 Ιανουαρίου 2009*
http://www.imibo.com/delphi/mapiorcdo.html - *7 Νοεμβρίου 2008*
http://www.infopili.gr/content/view/493/93/lang,el/ - *10 Δεκεμβρίου 2008*
http://www.islab.demokritos.gr/gr/html/prixiaki_papapanos/kef_1.htm - *20 Δεκεμβρίου 2008*
http://www.itsecurity.gr/spam.html - *7 Νοεμβρίου 2008*
http://www.microsoft.com/exchange/default.MSPx - *20 Ιανουαρίου 2009*
http://www.microsoft.com/hellas/athome/security/quiz/default.mspx - *7 Δεκεμβρίου 2008*
http://www.microsoft.com/hellas/smallbiz/issues/sgcv2/security-guidance-centre/dont-get-hooked-by-phishing.mspx - *7 Δεκεμβρίου 2008*
http://www.microsoft.com/products/info/product.aspx?view=32&pcid=80821f49-e480-4b75-be73-24b6b32e72cb&type=ovr#Overview – *12 Φεβρουαρίου 2009*
http://www.openspf.org/Introduction - *12 Δεκεμβρίου 2008*
http://www.pare-dose.net/blog/?p=356 – *28 Νοεμβρίου 2008*
http://www.pcw.gr/Article/Security/browsers_security_IE8_Firefox_Opera_phishing/240-3368.html&pbreak=1 – *22 Νοεμβρίου 2008*
http://www.pcw.gr/forum/viewtopic.php?f=22&t=9579 – *10 Δεκεμβρίου 2008*
http://www.presspoint.gr/release.asp?id=83213 - *19 Μαρτίου 2009*
http://www.rmxsmania.com/Vb/archive/index.php/t-2202.html - *6 Νοεμβρίου 2008*
http://www.saferInternet.gr/Θέματα/ - *12 Δεκεμβρίου 2008*
http://www.securitylabs.gr/content/view/104/29/ - *12 Νοεμβρίου 2008*
http://www.securitylabs.gr/forum/showthread.php?t=12814 - *19 Μαρτίου 2009*
http://www.symantec.com/business/mail-security-for-smtp - *19 Μαρτίου 2009*
http://www.tm.teiher.gr/Portal/DesktopDefault.aspx?tabid=323 – *20 Ιανουαρίου 2009*
http://www.webz.gr/2008/04/18/αντιμετωπίστε-τα-spam-blogs/ - *10 Δεκεμβρίου 2008*
http://www.windowsvistaplace.com/intro-to-today - *20 Δεκεμβρίου 2008*
http://www.xblog.gr/?p=307 - *6 Νοεμβρίου 2008*
http://www-01.ibm.com/software/lotus/ - *21 Ιανουαρίου 2009*