(10)

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ

(ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ)

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΑΠΕΙΛΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΠΟΥΔΑΣΤΗΣ : ΚΟΛΑΤΣΗΣ ΗΛΙΑΣ

ΕΙΣΗΓΗΤΗΣ : ΜΗΛΙΩΝΗΣ ΜΑΤΘΑΙΟΣ

ΙΟΥΝΙΟΣ 2010
ΣΠΑΡΤΗ

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΚΙΝΔΥΝΟΙ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ ΜΕΣΟ E-MAIL ΚΑΙ ΜΕΘΟΔΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥΣ

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες, Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του *Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Τ.Ε.Ι Καλαμάτας Παραρτήματος Σπάρτης.*

ΚΕΦΑΛΑΙΟ 1

ΚΙΝΔΥΝΟΙ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ ΜΕΣΟ E-MAIL ΚΑΙ ΜΕΘΟΔΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥΣ

1.1 Ιστορία

Στα τέλη του 1971 ο μηχανικός υπολογιστών **Ray S. Tomlinson**, δούλευε στο πανεπιστήμιο **Cambridge (Massachusetts)**, για την εταιρεία **BBN** (Bolt Beranek & Newman), η οποία είχε προσληφθεί από την Αμερικάνικη κυβέρνηση για να φτιάξει το **APRANET**. Εκείνο τον καιρό πειραματιζόταν με τα προγράμματα SENDMSG και READMAIL τα οποία λειτουργούσαν μόνο στον ίδιο υπολογιστή και πρακτικά το μόνο που έκαναν ήταν να προσθέτουν μηνύματα σε ένα τοπικό αρχείο. Έτσι όποιος καθόταν σε ένα μηχάνημα, μπορούσε να "στείλει" μηνύματα στους υπόλοιπους χρήστες, χρησιμοποιώντας το username τους σαν διεύθυνση, ενώ μπορούσε να διαβάσει και να σβήσει τα μηνύματα που απευθύνονταν στον ίδιο.

Ο Tomlinson είχε δουλέψει πιο παλιά σε ένα πρωτόκολλο ανταλλαγής αρχείων με το όνομα CPYNET. Με τη βοήθεια αυτού, οι χρήστες του ARPANET (περίπου 15 υπολογιστές ως τότε) μπορούσαν να ανταλλάζουν αρχεία. Με το συνδυασμό των προγραμμάτων **SENDMSG/READMAIL**και του πρωτοκόλλου **CPYNET**, κάνοντας τις κατάλληλες τροποποιήσεις ώστε να υπάρχει η δυνατότητα προσθήκης δεδομένων στο τέλος του αρχείου, πέτυχε αποστολή μηνυμάτων μεταξύ υπολογιστών που η μόνη τους σύνδεση ήταν μέσω του πανεπιστημιακού δικτύου.

Για τον καθορισμό των διευθύνσεων πλέον χρειαζόταν κάτι παραπάνω από ένα απλό username. Έτσι, διάλεξε το χαρακτήρα **@ (at)** για να χωρίσει το όνομα χρήστη από το όνομα υπολογιστή, ώστε να είναι εμφανές σε ποιο μηχάνημα πρέπει να καταλήξει το μήνυμα και σε ποιο χρήστη του μηχανήματος απευθυνόταν.

Θα μπορούσαμε να θεωρήσουμε πως το πρώτο e-mail ήταν τα πειραματικά μηνύματα που έστειλε ο εφευρέτης στον εαυτό του, μεταξύ δύο υπολογιστών μοντέλου PDP-10 που βρίσκονταν μεν στο ίδιο δωμάτιο, αλλά ήταν συνδεδεμένοι μόνο μέσω ARPANET. Ο ίδιος ο Tomlinson λέει πως δε θυμάται ακριβώς τι είχε γράψει όμως νομίζει πως ήταν κάτι σαν "**QWERTYUIOP**", δηλαδή η πρώτη σειρά του πληκτρολογίου γραφομηχανής, με κεφαλαία γράμματα (οι PDP-10 έγραφαν μόνο κεφαλαία). Αφού αντάλλαξε αρκετά μηνύματα σιγουρεύοντας πως το πρόγραμμα που είχε φτιάξει λειτουργούσε σωστά, έστειλε μήνυμα, μέσω e-mail, στους υπολογιστές των άλλων συναδέλφων του για να τους ενημερώσει σχετικά με τη νέα αυτή υπηρεσία και πως μπορούσαν να τη χρησιμοποιήσουν.

Το 2002 ο Tomlinson δέχθηκε το πρώτο βραβείο "**Κατόρθωμα Ζωής**" που έδωσε ποτέ η Διεθνής Ακαδημία Ψηφιακών Τεχνών και Επιστημών, στα πλαίσια των πέμπτων Webby Awards. Το επίτευγμά του σίγουρα επηρέασε ριζικά την παγκόσμια κοινότητα, καθώς το ηλεκτρονικό ταχυδρομείο είναι από τα πιο διαδεδομένα προγράμματα του Διαδικτύου.

Ήδη όμως από τα τέλη της δεκαετίας του 1960 είχε αρχίσει η ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου μεταξύ χρηστών. Καθώς ο αριθμός των χρηστών και των υπολογιστών αυξανόταν, έγινε φανερή η ανάγκη δημιουργίας ενός πρωτοκόλλου για την ανταλλαγή ηλεκτρονικών μηνυμάτων μεταξύ χρηστών που χρησιμοποιούσαν διαφορετικά συστήματα υπολογιστών. Εξέλιξη των αρχικών πρωτοκόλλων που αναπτύχθηκαν την εποχή (δεκαετία του 1970) αυτή αποτελεί το SMTP. Συγκεκριμένα οι ρίζες του SMTP εντοπίζονται στα πρωτόκολλα Mail Box Protocol (1971), FTP Mail (1973) και Mail Protocol. Όταν όμως άρχισε να σχηματίζεται το διαδίκτυο (1980), ο *Jon Postel* πρότεινε την δημιουργία ενός νέου πρωτοκόλλου για την ανταλλαγή ηλεκτρονικών μηνυμάτων, το οποίο δεν θα βασιζόταν τόσο πολύ στο FTP όπως έκαναν οι πρόγονοί του. Έτσι λοιπόν το 1982 γεννήθηκε το SMTP.

Το πρόγραμμα send mail ήταν ένα από τα πρώτα προγράμματα που υλοποίησε το SMTP, ενώ σήμερα υπάρχει μία πληθώρα τέτοιων προγραμμάτων όπως για παράδειγμα τα Postfix, qmail, Novell Group Wise, Exim, Novell NetMail και άλλα. Σε μία μέτρηση που έγινε το 2001 βρέθηκαν τουλάχιστον 50 προγράμματα τα οποία υλοποιούσαν το πρωτόκολλο SMTP είτε ως client (δηλαδή αποστολείς ηλεκτρονικών μηνυμάτων) είτε ως server (δηλαδή παραλήπτες ηλεκτρονικών μηνυμάτων).

Το αρχικό SMTP υποστήριζε κατά βάση μονάχα μηνύματα απλού κειμένου και όχι μετάδοση αρχείων (πχ. εικόνες, εκτελέσιμα, μουσική κοκ). Στην συνέχεια όμως αναπτύχθηκαν διάφορα standards που επέτρεπαν την εισαγωγή αρχείων στα ηλεκτρονικά μηνύματα. Ένα από αυτά τα standards είναι και το Multipurpose Internet Mail Extensions (MIME), το οποίο κωδικοποιεί τα αρχεία με τέτοιον τρόπο ούτως ώστε να μπορούν να μεταδοθούν σε απλά μηνύματα SMTP.

1.2 Βασικές Έννοιες Ασφάλειας Πληροφοριών

- **Εμπιστευτικότητα:** όταν στα δεδομένα έχουν πρόσβαση (ανάγνωση, εμφάνιση κτλ) μόνο εξουσιοδοτημένα άτομα (ή οντότητες).
- **Ακεραιότητα:** όταν τα δεδομένα δεν αλλοιώνονται (αλλάζουν) με μη εξουσιοδοτημένο τρόπο ή από μη εξουσιοδοτημένα άτομα (ή οντότητες).
- **Διαθεσιμότητα:** όταν τα δεδομένα (ή οι υπηρεσίες) είναι διαθέσιμες προς χρήση όταν αυτό απαιτηθεί και με ικανοποιητική ποιότητα υπηρεσίας.

i) Αποκάλυψη πληροφοριών (Εμπιστευτικότητα)

- Είσοδος ή αποκάλυψη δεδομένων:
  - Απόρρητα Οικονομικά στοιχεία
  - Ευαίσθητα προσωπικά δεδομένα
  - Αλληλογραφία (εταιρική προσωπική)

- Οι αιτίες:
  - Λάθος ρύθμιση ACLs σε κάποιο «φάκελο» επιτρέπει σε λάθος ανθρώπους πρόσβαση
  - Κακή πιστοποίηση ταυτότητας ενός χρήστη. (πχ με κωδικό ο οποίος όμως είναι ίδιο με το Login ή είναι υπερβολικά απλός)
  - Μη ύπαρξη κανενός μέτρου για πιστοποίηση ταυτότητας χρηστών
  - Κακόβουλη ενέργεια από άτομο (π.χ. το pop3 mail μπορεί να υποκλαπεί με έναν απλό sniffer, Μια γραμματέας προωθεί αλληλογραφία της εταιρίας σε ανταγωνιστή)
  - Ανθρώπινο Λάθος (ένας χρήστης ξεχνά μία «ευαίσθητη» παρουσίαση σε κοινόχρηστο φάκελο)
  - Κλοπή ενός εταιρικού Laptop ή ακόμα και ενός USB Flash
  - Πλημμελής φύλαξη αντιγράφων ασφαλείας

- Άμεσες συνέπειες (παραδείγματα)
  - Οι ανταγωνιστές έχουν στα χέρια τους οικονομικές προσφορές σε μεγάλους διαγωνισμούς (μπορούν τώρα να κατέβουν στους ίδιους με μικρότερο κόστος)
  - Hacker's παίρνουν στα χέρια τους αριθμούς πιστωτικών καρτών και πελατών της εταιρίας. Έπειτα του χρεώνουν υπέρογκα ποσά.

- Έμμεσες συνέπειες (παραδείγματα)
  - Κάποιος υπάλληλος αποκτά πρόσβαση στα αρχεία του HR τμήματος και αποκαλύπτει την μισθοδοσία. Αποτέλεσμα δυσαρέσκεια και αναταραχή μεταξύ στο προσωπικού (αποχωρίσεις, αιτήματα για αύξηση κτλ)
  - Η άσχημη οικονομική κατάσταση της εταιρίας διαρρέει στον τύπο από αποχωρούντα δυσαρεστημένο υπάλληλο που όμως φρόντισε να αποκτήσει πρόσβαση στο λογιστήριο της εταιρίας.
  - Ένα ευαίσθητο πρόβλημα υγείας ενός υπαλλήλου γίνεται γνωστό και αυτός απομονώνεται από τους υπολοίπους.

ii) Αλλαγή – τροποποίηση πληροφοριών (Ακεραιότητα)

- Άμεσες συνέπειες
  - Ένας hacker αλλάζει την εμφάνιση του web site της εταιρίας εισάγοντας άσεμνο περιεχόμενο. Η άμεση συνέπεια είναι ότι οι χρήστες δεν μπορούν να χρησιμοποιήσουν το site σωστά.
  - Ένας Hacker αλλάζει επιμελώς συγκεκριμένα σημεία του web site μιας εταιρίας αυξάνοντας τις τιμές. Στους επισκέπτες η εταιρία δείχνει λιγότερο ανταγωνιστική
  - Ένας φοιτητής παίρνει πτυχίο αλλάζοντας την βαθμολογία του.
- Έμμεσες συνέπειες
  - Ένας hacker αλλάζει την εμφάνιση του web site της εταιρίας εισάγοντας άσεμνο περιεχόμενο. Η ηθική ζημιά γοήτρου για την εταιρία είναι μεγάλη
  - Η ηθική ζημιά ενός *defacement* δεν υπολογίζεται εύκολα. Σκεφτείτε τις επιπτώσεις για μία τράπεζα αν γίνει defacement στο web site για Online Transactions

iii) Άρνηση Εξυπηρέτησης (DoS, DDoS) (Διαθεσιμότητα)

- Άρνηση Εξυπηρέτησης (DoS, DDoS)
  - Συνήθως προκαλούνται από
    - ✓ αστοχία υλικού λογισμικού («κάψιμο» τροφοδοτικού στο Mail Server, ελαττωματικό καλώδιο, καταστροφή του λειτουργικού συστήματος ενός server)
    - ✓ ανθρώπινου λάθους (λάθος ρυθμίσεις – προγραμματισμός)
    - ✓ κακόβουλες ενέργειες όπως Viruses (Blaster, Watchi)
    - ✓ Κακόβουλοι χρήστες ή Cracker (hackers) προγράμματα όπως Smurf attack, SynFloods κτλ

- Κόστος
  - Τις περισσότερες φορές το κόστος δεν μπορεί να εκτιμηθεί.
  - Άμεσες συνέπειες. Χαμένες ανθρωποώρες υπάλληλων πελατών. Απασχόληση επιπλέον τεχνικού προσωπικού
  - Έμμεσες συνέπειες Δυσαρεστημένοι πελάτες, μείωση αποδοτικότητας υπαλλήλων – ανταγωνιστικότητας εταιρίας
  - Δύσκολο να αντιμετωπισθεί πλήρως.

1.2.1 Κρυπτογραφία

Καιρό τώρα έχει γίνει πολύς λόγος τόσο για το Carnivore όσο και για το Echelon, συστήματα που – μεταξύ άλλων – παρακολουθούν την ηλεκτρονική αλληλογραφία των χρηστών για λέξεις – κλειδιά που οι μυστικές υπηρεσίες θεωρούν επικίνδυνες. Όλα ξεκίνησαν από το carnivore στην Αμερική, για να συνεχιστούν και στην Ευρώπη με τη μορφή του Echelon, που ήδη χρησιμοποιείται στην Αγγλία και την Γερμανία, με προοπτικές να επεκταθεί και σε άλλες χώρες – μέλη του NATO. Το Carnivore έχει τη δυνατότητα να καταγράφει την ηλεκτρονική αλληλογραφία και στη συνέχεια να την ελέγχει και να φυλάσσει τα στοιχεία εκείνα που ενδιαφέρουν τις μυστικές υπηρεσίες και την αστυνομία.

Το Carnivore και το Echelon, όμως, δεν είναι το μόνο πρόβλημα σχετικά με την ηλεκτρονική αλληλογραφία. Σε γραφεία και επιχειρήσεις όπου χρησιμοποιείται ένας mail server για την ηλεκτρονική αλληλογραφία του προσωπικού, μπορούν να εγκατασταθούν φίλτρα τα οποία θα προωθούν μηνύματα που περιέχουν συγκεκριμένες λέξεις σε κάποιον χρήστη. Αυτός ο χρήστης συνήθως είναι ο ιδιοκτήτης ή ο διευθυντής της εταιρίας ή κάποιο άλλο πρόσωπο της απολύτου εμπιστοσύνης του. Είτε χρησιμοποιείται Exchange είτε κάποιο Unix based mail server, είναι δυνατό να εγκατασταθούν φίλτρα που παρακολουθούν τα μηνύματα των χρηστών. Φυσικά, αυτό είναι παράνομο, αφού το απόρρητο της ηλεκτρονικής αλληλογραφίας προστατεύεται όπως και το απόρρητο της φυσικής αλληλογραφίας.

Αν θέλουμε να κρατήσουμε την αλληλογραφία μας μυστική, ο μόνο τρόπος να το επιτύχουμε είναι να χρησιμοποιήσουμε κάποιο πρόγραμμα κρυπτογράφησης, από τα αρκετά που κυκλοφορούν στην αγορά. Κρυπτογράφηση είναι η μετατροπή των δεδομένων σε μορφή η οποία δεν είναι δυνατό να διαβαστεί. Τα προγράμματα αυτά χρησιμοποιούν ένα μοναδικό κλειδί για να κρυπτογραφήσουν το εκάστοτε αποστελλόμενο μήνυμα, το οποίο κλειδί ο παραλήπτης πρέπει να χρησιμοποιήσει προκειμένου να διαβάσει το μήνυμα που του έχει αποσταλεί. Οποιοσδήποτε αγνοεί το συγκεκριμένο κλειδί δεν είναι σε θέση να διαβάσει το μήνυμα. Ανάλογα με τον αλγόριθμο που χρησιμοποιείται, το κλειδί κρυπτογράφησης και αποκρυπτογράφησης μπορεί να είναι είτε το ίδιο είτε διαφορετικό.

Η πραγματική επανάσταση στην κρυπτογράφησης ήρθε με τη δημιουργία της τεχνικής Public Key. Η τεχνική αυτή χρησιμοποιεί δύο κλειδιά με το ένα κλειδί να είναι Public και γνωστό σε όλους και το άλλο Private και γνωστό μόνο στον κάτοχό του. Αν ένας χρήστης θέλει να στείλει ένα κρυπτογραφημένο μήνυμα σε κάποιον άλλο, τότε χρησιμοποιεί το Public Key για να το κρυπτογραφήσει και ο άλλος χρήστης το δικό του Private Key για να το αποκρυπτογραφήσει. Το βασικό πλεονέκτημα αυτής της μεθόδου είναι το ότι δε μεταφέρεται με καμία μορφή επικοινωνία το Private Key, άρα δεν υπάρχει περίπτωση υποκλοπής του. Ένα μειονέκτημα είναι η ταχύτητα, αφού αρκετά συστήματα Secret Key είναι πιο γρήγορα από τα συστήματα που χρησιμοποιούν Public Key.

Εκτός, όμως, από το να κρατήσουμε μυστικό το περιεχόμενο του μηνύματος που στέλνουμε, υπάρχει και η δυνατότητα να στείλουμε ανώνυμα e-mail χρησιμοποιώντας κάποιον από τους mailers που υπάρχουν είτε online είτε σε μορφή προγράμματος που μπορούμε να εγκαταστήσουμε στον υπολογιστή μας. Βέβαια, τα ανώνυμα e-mails συνεπάγονται ότι δεν θα λάβουμε ποτέ απάντηση, ενώ χρησιμεύουν περισσότερο σε όσους θέλουν να κάνουν κακόγουστες φάρσες ή να στέλνουν spam mails.

1.3 Λειτουργία

Για να την αποστολή ενός ηλεκτρονικού μηνύματος θα πρέπει ο χρήστης να έχει πρόσβαση σε έναν SMTP Server. Όλα τα προγράμματα ηλεκτρονικής αλληλογραφίας (πχ Mozilla Thunderbird, Microsoft Outlook κ.α.) θα πρέπει να ρυθμιστούν κατάλληλα από τον χρήστη για να λειτουργήσουν σωστά. Συγκεκριμένα ο χρήστης θα πρέπει να καθορίσει τον SMTP server που θα χρησιμοποιήσει για να στείλει και να παραλάβει ηλεκτρονική αλληλογραφία. Με τον τρόπο αυτό μπορεί για παράδειγμα ένας χρήστης να ανταλλάξει ηλεκτρονικά μηνύματα χωρίς να είναι συνδεδεμένος στο διαδίκτυο, εάν χρησιμοποιεί έναν τοπικό SMTP server.

Οι SMTP servers θα πρέπει να έχουν ανοιχτή μία τουλάχιστον από τις πόρτες 25 και 587, ούτως ώστε να μπορούν να επικοινωνήσουν με άλλους SMTP servers για την αποστολή ή παραλαβή ηλεκτρονικών μηνυμάτων. Πολλοί SMTP servers χρησιμοποιούν και τις δύο πόρτες για λόγους συμβατότητας.

Μία τυπική παραλαβή ηλεκτρονικού μηνύματος από έναν SMTP server έχει ως εξής: Αρχικά δημιουργείται μία σύνδεση μεταξύ του SMTP server που έχει τον ρόλο του αποστολέα και του SMTP Server που έχει τον ρόλο του παραλήπτη. Στην συνέχεια οι δύο SMTP servers "συνομιλούν" ούτως ώστε να επιτευχθεί χωρίς προβλήματα η ανταλλαγή του μηνύματος.

1.4 Τι είναι SPAM

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις σημαντικότερες υπηρεσίες που προσφέρει το διαδίκτυο. Το κυριότερο ίσως πλεονέκτημα της υπηρεσίας είναι ότι παρέχεται δωρεάν, αν εξαιρέσει κανείς τη χρέωση πρόσβασης στο διαδίκτυο. Η έλλειψη χρέωσης, όμως, είναι και η πηγή του προβλήματος της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spam): καθότι δωρεάν, πολλοί χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο για να αποστέλλουν διαφημιστικά και συνήθως ανεπιθύμητα μηνύματα σε χιλιάδες ή εκατομμύρια χρήστες. Υπολογίζεται ότι τα ανεπιθύμητα αυτά μηνύματα αποτελούν περίπου το 60% της διακινούμενης ηλεκτρονικής αλληλογραφίας.

Τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου σπαταλούν τους πόρους του διαδικτύου αλλά και το το χρόνο των χρηστών, αφού τους υποχρεώνουν να τα αφαιρούν χειρωνακτικά από τα εισερχόμενα μηνύματά τους.

Η αντιμετώπιση του προβλήματος, που πλέον έχει λάβει διαστάσεις επιδημίας, αποτελεί στόχο πολλών ερευνητών και εταιρειών. Μια από τις πιο επιτυχημένες μεθόδους που έχουν προταθεί είναι η χρήση προγραμμάτων αυτόματης ταξινόμησης μηνυμάτων σε κατηγορίες, που χρησιμοποιούν συνήθως αλγορίθμους μηχανικής μάθησης. Στην προκειμένη περίπτωση, τα προγράμματα αυτά χρησιμοποιούνται ως φίλτρα που ταξινομούν τα εισερχόμενα μηνύματα ως επιθυμητά (ham) ή ανεπιθύμητα

(spam), αφού εκπαιδευθούν σε παλαιότερα μηνύματα που έχουν ταξινομηθεί χειρωνακτικά.

Ο όρος spam χρησιμοποιήθηκε για πρώτη φορά σ' ένα τραγούδι των Monty Python τη δεκαετία του 1970. Αργότερα, τη δεκαετία του 1980, στα πρώτα chat rooms του Internet, η λέξη spam χρησιμοποιήθηκε στην αργκό των χρηστών για εκείνες τις πληροφορίες που ήταν άσχετες με την συζήτηση και συνεπώς άχρηστες. Το πρώτο μήνυμα spam εμφανίσθηκε το 1985 στην ομάδα συζήτησης (newsgroup) net.general και διαφήμιζε μια τραπεζαρία.

Με τον όρο spam εννοούμε την απρόκλητη, εμπορική και μαζική αποστολή μεγάλου αριθμού μηνυμάτων, τα οποία απευθύνονται σ' ένα σύνολο χρηστών του Internet, χωρίς αυτοί να έχουν ζητήσει ή να επιθυμούν κάτι τέτοιο και χωρίς να έχουν συνειδητά προκαλέσει την επικοινωνία με τον αποστολέα των μηνυμάτων.

Τα μηνύματα των spam e-mails είναι συνήθως ενημερωτικού ή διαφημιστικού περιεχομένου για προϊόντα ή και υπηρεσίες αμφίβολης ποιότητας και πιο σπάνια σεξουαλικού περιεχομένου και τα οποία φθάνουν στο γραμματοκιβώτιο μας, χωρίς εμείς να έχουμε ζητήσει την εν λόγω πληροφόρηση.

Έτσι, με μια σύντομη απόδοση, ο όρος spam μπορεί να χαρακτηρισθεί ως απρόκλητη ή αυτόκλητη ή ανεπιθύμητη αλληλογραφία ή και ανεπιθύμητα ηλεκτρονικά μηνύματα. Η επίσημη απόδοση στα ελληνικά του αγγλικού όρου spam είναι μη ζητηθείσα εμπορική επικοινωνία.

Το πλήθος τους τείνει να ξεπεράσει αυτό των χρήσιμων και νόμιμων μηνυμάτων. Υπολογίζεται ότι το 40% των ηλεκτρονικών μηνυμάτων που λαμβάνουν οι χρήστες του Internet θεωρούνται spam e-mails. Τα μηνύματα αυτά μπορεί να διαφημίζουν φάρμακα για οτιδήποτε μπορεί να φαντασθεί κανείς ή να εγγυώνται την απόκτηση πλαστών πτυχίων πανεπιστημίου ή δωρεάν εκδρομών στα πιο απίθανα μέρη του κόσμου.

Η σχετική νομοθεσία, που έχει αναπτυχθεί, κυρίως στις ΗΠΑ και τη Βρετανία, ενδιαφέρεται κυρίως για τα παραπλανητικά μηνύματα, που εκτιμάται ότι αποτελούν τα 2/3 όλων των ανεπιθύμητων μηνυμάτων.

Οι εταιρείες που στέλνουν μαζικά διαφημιστικά e-mails αποκαλούνται spammers και μερικές δεκάδες απ' αυτές διακινούν το 90% των spam e-mails. Έχουν τη δυνατότητα να στείλουν πολλά εκατομμύρια e-mails με μια κίνηση, ενώ οι εταιρείες που διαφημίζονται μέσω από τα μηνύματα αυτά πληρώνουν βάσει συμφωνίας κάποια ποσά για κάθε παραγγελία που δέχονται.

Αν και μόλις ένας στο εκατομμύριο από τους παραλήπτες «τσιμπήσουν» στο δόλωμα και κάνουν παραγγελίες, αυτός ο τρόπος διαφήμισης θεωρείται αρκετά αποδοτικός. Οι πιο χαρακτηριστικές λέξεις που εμφανίζονται συνήθως στο κείμενο των μηνυμάτων αυτών είναι οι εξής : one time offer, you are very lucky, a very special offer for you κ.ά.

1.4.1 Τα χαρακτηριστικά του Spam

Τα κυριότερα χαρακτηριστικά του spam μπορούν να συνοψιστούν στα ακόλουθα σημεία :

- **Απρόκλητο :** Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν έχει προϋπάρξει κάποια σχέση ή άλλη επικοινωνία μεταξύ του παραλήπτη και του αποστολέα, που θα μπορούσε να δικαιολογήσει ή να προκαλέσει την επικοινωνία αυτή.

- **Εμπορικό :** Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών και με τελική επιδίωξη την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.

- **Μαζικό :** Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σ' ένα πολύ μεγάλο πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σ' ένα μεγάλο πλήθος παραληπτών.

1.4.2 Οι συνέπειες από το Spam

Οι συνέπειες από την αχαλίνωτη χρήση του ηλεκτρονικού ταχυδρομείου από τους κάθε λογής διαφημιστές είναι καταστροφικές τόσο για τον απλό χρήστη όσο και για τις μεγάλες εταιρείες Οι εργαζόμενοι θα είναι αναγκασμένοι να ξοδεύουν όλο και περισσότερο χρόνο για να διαβάσουν αλλά και να διαγράψουν τα άχρηστα αυτά μηνύματα.
Επίσης, όλο και περισσότεροι πόροι από την επεξεργαστική ισχύ των διακομιστών (servers) θα πρέπει να δεσμεύονται για να απασχοληθούν με μια ανεπιθύμητη διαδικασία.
Είναι τόσο πολλά σε αριθμό αυτά τα μηνύματα που μπορούν ακόμη και να μπλοκάρουν το παγκόσμιο σύστημα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου και να οδηγήσουν το Internet σε κατάρρευση.
Ο λόγος είναι ότι φορτώνουν το δίκτυο και τα κεντρικά συστήματα δεν μπορούν να τα βγάλουν πέρα με την υπερβολική κίνηση που δημιουργείται.
Σύμφωνα με πρόσφατες έρευνες, το 1/3 των χρηστών του Internet αντιμετωπίζει μεγάλη δυσχέρεια στη χρήση της ηλεκτρονικής τους αλληλογραφίας καθώς τα χρήσιμα και επείγοντα μηνύματα από τους φίλους και τους συνεργάτες τους χάνονται μέσα στην πλημμυρίδα των spam e-mail.

1.4.3 Πώς δουλεύουν οι spammers

Η δουλειά των spammers χωρίζεται σε διαφορετικές κατηγορίες:

- **Harvest**: βρίσκουν έγκυρες email διευθύνσεις και φτιάχνουν βάσεις δεδομένων με τους στόχους.
- **Εύρεση open proxies**: μέσω αυτών στέλνουν τα email και παραμένουν ανώνυμοι.
- **Εύρεση open mail relay servers**: ώστε να μπορούν να στέλνουν τα email, μέσω των open relay servers που τα προωθούν παντού.

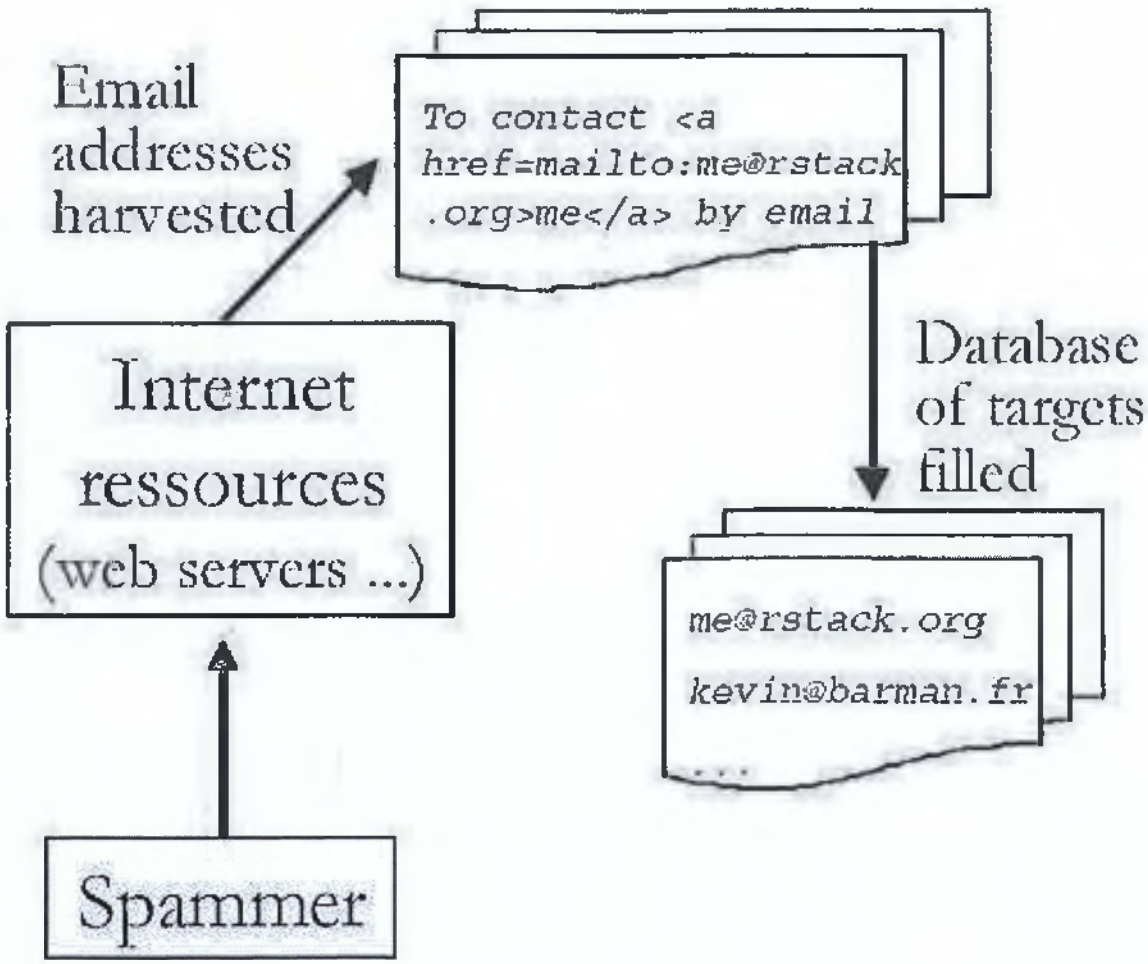
Για να αποσπάσουν έγκυρες email διευθύνσεις οι spammers συνεργάζονται με διάφορα άτομα που κάνουν αυτή τη δουλειά. Μάλιστα, στο internet χρησιμοποιείται ο όρος spaker, για να περιγράψει τους hacker οι οποίοι κάνουν hacking ώστε να προμηθεύσουν τους spammers με έγκυρες διευθύνσεις, επί πληρωμής φυσικά. Ο όρος spaker είναι πολύ απαξιωτικός και τα άτομα που κάνουν αυτή τη δουλειά δεν το περηφανεύονται.
Οι spakers εισβάλουν σε e-commerce web sites και γενικά σε ιστοσελίδες οι οποίες περιέχουν βάσεις δεδομένων με πολλές χιλιάδες ή και εκατομμύρια άτομα ανά τον

κόσμο που έχουν κάνει αγορές. Όσο πιο συγκεκριμένο είναι το target group που θα αποσπάσει ο spaker τόσο καλύτερη θα είναι και η αμοιβή του.

Εκτός όμως από εμπορικά sites, οι spammers βρίσκουν έγκυρες email διευθύνσεις σε πολλά σημεία στο internet-public lists, forums, κοινότητες όπως τα hotmail.com, aol.com κα.

Μια ακόμα τεχνική για να αποσπάσουν email διευθύνσεις βασίζεται σε προγράμματα που ψάχνουν ιστοσελίδες στο internet και ελέγχουν για τη σύνταξη mailto:username@site.com. Όταν βρίσκουν τη σύνταξη αυτή, αποθηκεύουν τη διεύθυνση email και η αναζήτηση συνεχίζεται. Σαν προστασία σε αυτή την τεχνική προτείνεται να μην υπάρχει πουθενά email με την παραπάνω σύνταξη, αλλά να γράφεται mailto: username at site dot com.

Βέβαια τα πιο προχωρημένα εργαλεία για αναζήτηση μπορούν να το καταλάβουν αυτό. Το google.com, η μεγαλύτερη μηχανή αναζήτησης στο internet είναι σύμμαχος για τους spammers και συνήθως τα προγράμματα που χρησιμοποιούν για αναζήτηση email βρίσκουν τις ιστοσελίδες μέσα από το google.



1.4.4 Αντιμετώπιση του Spam

Οι ηλεκτρονικές διευθύνσεις των χρηστών στους οποίους στέλνονται τέτοια μηνύματα εντοπίζονται με ειδικά προγράμματα από τις υπάρχουσες ιστοσελίδες του

Internet. Ένας άλλος ιδιαίτερα αποτελεσματικός τρόπος συγκέντρωσης διευθύνσεων e-mails ανύποπτων χρηστών, που στη συνέχεια θα βομβαρδιστούν με διαφημίσεις, είναι οι φάρσες, όπως για ένα καημένο κοριτσάκι που κινδυνεύει από καρκίνο ή για έναν πολύ καταστροφικό ιό και οδηγίες για το πώς να τον αποφύγετε.

Η φράση «στείλτε αυτό το μήνυμα σ' όσους περισσότερους χρήστες μπορείτε» είναι συνήθως η παγίδα που χρησιμοποιούν οι επιτήδειοι, καθώς τα e-mails με τις εκατοντάδες διευθύνσεις στις οποίες προωθούνται θα επιστρέψουν κάποια στιγμή στον αρχικό συντάκτη τους για να κάνει κι αυτός τη με τη σειρά την δουλειά του. Οι προσπάθειες που έχουν κάνει μέχρι στιγμής οι εταιρείες παροχής υπηρεσιών Internet (ISPs - Internet Service Providers) και υπηρεσιών ηλεκτρονικού ταχυδρομείου με τη χρήση ειδικών προγραμμάτων-φίλτρων για την αυτόματη απόρριψη τέτοιων μηνυμάτων πριν αυτά φθάσουν στον υπολογιστή του χρήστη δεν έχουν επιφέρει θεαματικά αποτελέσματα.

Στην Ελλάδα υπάρχει νόμος που απαγορεύει την μη ζητηθείσα εμπορική επικοινωνία, ενώ το spam αντιμετωπίζεται ποινικά στη Μεγάλη Βρετανία και στις ΗΠΑ.

Όλα αυτά βέβαια τα μέτρα που λαμβάνουν διάφορες χώρες και φορείς έχουν να αντιμετωπίσουν κάποιες δυσκολίες, όπως το ότι οι spammers (οι αποστολείς των ενοχλητικών αυτών μηνυμάτων) ενδέχεται να χρησιμοποιούν ISP's σε χώρες όπου υπάρχει χαλαρό νομικό προστατευτικό καθεστώς, ώστε να μην κινδυνεύουν από διώξεις.

Επίσης, η έννοια του spam είναι σχετική, καθώς κάτι που είναι ενοχλητικό για κάποιον μπορεί να είναι χρήσιμο και ενδιαφέρον για κάποιον άλλον, ένα γεγονός που κάνει πολύ δύσκολη την κατάταξη και τον διαχωρισμό των χρήσιμων από τα άχρηστα μηνύματα

1.4.5 Χρήση open proxies

Οι spammers μπορούν είτε να συνδεθούν απευθείας στον απομακρυσμένο mail relay server που θα στείλει το spam τους, είτε να συνδεθούν μέσω open proxies και έτσι να μην μπορούν να εντοπιστούν εύκολα, πετυχαίνοντας να μένουν συνέχεια ανώνυμοι. Ένας open proxy είναι μια υπηρεσία ανοικτή στον κόσμο που προωθεί οποιαδήποτε σχεδόν αίτηση, επιτρέποντας έτσι σε κάποιον να παραμένει ανώνυμος. Οι proxy servers χρησιμοποιούνται ιδιαίτερα από τους spammers και γενικότερα από το internet undergroung. Συνήθως οι spammers θα χρησιμοποιήσουν περισσότερους από ένα proxy servers για να καλύψουν τα ίχνη τους. Όσο περισσότερα ενδιάμεσα σημεία υπάρχουν, τόσο πιο δύσκολη θα είναι η ανίχνευσή τους. Οι spammers φοβούνται την πιθανότητα να εντοπιστούν, καθώς ξέρουν ότι οι δραστηριότητες τους είναι παράνομες και μπορούν να καταδικαστούν σε μεγάλα πρόστιμα και ποινές. Όσο πιο μεγάλη είναι η αλυσίδα των proxies στους οποίους συνδέονται τόσο καλύτερη ανωνυμία θα έχουν, αν και η ταχύτητα μειώνεται, αφού τα δεδομένα ταξιδεύουν περισσότερο.

1.4.6 Χρήση open relays

Οι open relays είναι mail transfer agents (MTA's) που δέχονται να προωθήσουν email μηνύματα ακόμα και αν δεν προορίζονται για το δικό τους domain. Οι spammers χρησιμοποιούν open relays για να προωθήσουν τα email τους σε οποιαδήποτε διεύθυνση θέλουν. Οι MTA's είναι συνήθως mail servers που έχουν

ρυθμιστεί λάθος, γιαυτό και επιτρέπουν την προώθηση μηνυμάτων από οποιονδήποτε host επικοινωνεί.

1.4.7 BOTs

Τα BOTs είναι ειδικό λογισμικό που εγκαθίσταται σε PC ανυποψίαστων χρηστών (σαν ιό, τον κολλάμε κάποιες φορές, πχ ανοίγουμε κάποιο attachment που δεν έπρεπε, ή μας ξεγελάνε ότι είναι χρήσιμο πρόγραμμα.). Στην πραγματικότητα το BOT, που εγκαθίσταται στο PC εκτελεί εντολές αυτού που το ελέγχει. Μια από αυτές τις λειτουργίες είναι να στείλει SPAM email από το λογαριασμό του μολυσμένου PC.

Η μέθοδος αυτή έχει πλεονεκτήματα, έναντι των Open relays. Ένα open relay γρήγορα θα το μάθουν τα antispam φίλτρα και θα τον κόψουν. Τα bots είναι πιο πολλά και δεν στέλνουν το email απευθείας τα ίδια αλλά χρησιμοποιούν το smpt του provider του μολυσμένου PC, πχ έχουμε OTENET και το email μας είναι elias@otenent.gr. Αν κολλήσουμε BOT αυτό θα αρχίσει να στέλνει emails τα οποία «Φεύγουν» μέσω του mail server της otenet. Οι RBL δεν μπορούν να κόψουν την OTENET. Συνήθως βέβαια σε κόβει έμας η OTENET, αλλά κάποιες χιλιάδες email έχουν είδη φύγει.

Τα BOTs επίσης ψάχνουν στις σελίδες του Internet και όπου συναντούν e-mail διεύθυνση την προσθέτουν στη λίστα τους. Αργότερα ο spammer έχει έτοιμους «πελάτες» για τα ενοχλητικά spam που θέλει να στείλει.

Γενικά το e-mail μας δεν πρέπει να φαίνεται πουθενά online. Όμως αν έχουμε κάποιο website και πρέπει να εμφανίζουμε την διεύθυνση, μπορούμε να την κωδικοποιήσουμε με τέτοιο τρόπο ώστε να μπορεί να λειτουργεί και να φαίνεται, αλλά παράλληλα να μην μπορεί κανένα bot να το υποκλέψει.

Μια τέτοια μέθοδος είναι η χρήση scripting γλώσσας (javascript) με την οποία σπάμε την διεύθυνση σε κομμάτια με τη χρήση του document write.

Έτσι με 3 document write μπορούμε να προβάλλουμε κανονικά την διεύθυνση μας, χωρίς όμως να φαίνεται μέσα στον κώδικα της σελίδας (εκεί που ψάχνουν τα spambots):

mailto:User
@
Domain.com

Έτσι το bot θα υποκλέψει μόνο την γραμμή με το @.
Ο κώδικας που πρέπει να βάζετε αντί για το email σας είναι:

```
<scriptlanguage=»javascript»type=»text/javascript»>
document.write('<ahref=»mailto:user');
document.write('@server.com»>user');
document.write('@server.com</a>');
</script>
```

1.4.8 Registration emails

Κλασσική περίπτωση που κάποιο email account μας γίνονται στόχος και περνάνε σε μια λίστα υποψηφίων αποδεκτών χιλιάδων spam mails, είναι η χρήση των εταιρικών

αυτών emails σε διάφορα διαφημιστικά forums ή σε άλλες ιστοσελίδες αμφιβόλου προέλευσης και ασφάλειας (commercial, warez , torrents, porn sites, etc.)

Οι μηχανές ανίχνευσης εντοπίζουν τα emails αυτά και τα περνάνε στους μηχανισμούς τους για μελλοντικές αποστολές. Καλό είναι για τέτοιες εγγραφές να έχουμε ένα email account σε κάποιον πάροχο όπως το Hotmail που ναι μεν δέχονται την spam-επίθεση αλλά έχουν άλλες δικλείδες ασφαλείας και αντιμετώπισης σε ανάλογες καταστάσεις. Χώρια που εκεί μπορούμε μέσω web να κάνουμε πολλαπλές διαγραφές και όχι πάνω στο δικό μας μηχάνημα με τους περιορισμένα διαθέσιμους πόρους.

Με απλά λόγια είναι πολύ πιο εύκολο να φιλτράρουμε 200 spam mails την μέρα σε ένα hotmail account , μέσα από ένα browser, παρά να τα κατεβάζουμε τοπικά στο μηχάνημα μας, να κάνουμε διαλογή και μετά να σβήνουμε χειροκίνητα.

1.4.9 Honeyd vs spammers

Το honeyd μπορεί να χρησιμοποιηθεί για να καταλάβουμε πώς λειτουργούν οι spammers, να τους κάνουμε να σπαταλήσουν χρόνο και πόρους και τελικά να ενημερώσουμε κάποιες black lists. Η αρχιτεκτονική που προτείνει ο δημιουργός του honeyd είναι η εξής: Δημιουργούμε διάφορα δίκτυα με virtual hosts που περιέχουν open proxies και open mail relays.

Με τη χρήση GRE tunneling που παρέχει το honeyd κατευθύνουμε την κίνηση που δέχονται σε κάποιο κεντρικό host και ο οποίος λειτουργεί σαν παγίδα για spam, στον οποίο προωθείται όλη η δραστηριότητα των spammers και το spam email. Αυτός ο host αναλαμβάνει να στείλει το συγκεντρωμένο spam σε κάποιο διεθνές φίλτρο spam.

Ο συγγραφέας του honeyd υποστηρίζει ότι η παραπάνω αρχιτεκτονική μέχρι στιγμής έχει δεχτεί πάνω από 6 εκατομμύρια email από περισσότερες από 1500 διευθύνσεις.

1.4.10 Chain mails

Μια ασθένεια των τελευταίων χρόνων , είναι μια διαδικασία μαζικών αποστολών chain mails που αποστέλλονται σε δεκάδες άτομα , περιεχόμενα σε mail lists, εντός ή και εκτός εργασιακών χώρων. Πρόκειται για κάτι φαινομενικά, μόνο , αθώο. Κάθε μαζική αποστολή , στα SMTP Headers του μηνύματος περιέχει όλα τα email addresses που το έχουν αποστείλει. Έτσι το email σας κάνει μια διαδρομή σε όλο το WEB και φυσικά μπορεί να χρησιμοποιηθεί για όποιο σκοπό.

Το δεύτερο σημείο προσοχής, είναι πως ανάλογα και αντίστοιχα emails είναι εκείνα που επιβαρύνουν το εταιρικό δίκτυο σας ή ακόμα και εκείνο του ISP. Για αυτό και πολλοί IT διαχειριστές πλέον , αν δουν πολλαπλές αιτήσεις SMTP (mail send πρωτόκολλο) από μια και μόνο IP διεύθυνση , προχωρούν μέχρι και σε ban (απαγόρευση) της συγκεκριμένης IP του τερματικού, με ειδικό κανόνα για το δίκτυο. Επιπλέον το domain που φαίνεται να είναι συνδεδεμένο με αυτή την IP , περνάει σε ένα "blacklist" και κανένας mail server από εκεί και πέρα δεν κάνει αποδεκτή SMTP αίτηση του. Για να αρθεί αυτή η απαγόρευση , χρειάζεται ειδική αίτηση προς τον ISP σας που με την σειρά του μεταφέρει το αίτημα σε άλλους φορείς.

Με λίγα λόγια τα chain emails δεν είναι τίποτα παραπάνω από μια μορφή spam που ακόμα και αν γίνεται με καλό σκοπό , κάνει την ίδια χρήση πόρων και παραβίαση φίλτρων όπως και τα κακόβουλα spam προγράμματα.

1.4.11 Πώς να χειριστούμε τα ανεπιθύμητα μηνύματα Spam

- **Διαγράφουμε τα άχρηστα μηνύματα e-mail χωρίς να τα ανοίξουμε.** Μερικές φορές, απλά ανοίγοντας ένα μήνυμα spam ειδοποιούμε τον αποστολέα του.

- **Δεν απαντάμε σε μηνύματα spam**, εκτός εάν είμαστε βέβαιοι ότι το μήνυμα προέρχεται από νόμιμη πηγή. Δεν απαντάμε καν σε μηνύματα που μας δίνουν τη δυνατότητα να "διαγραφείτε από τη λίστα μας".

- **Δεν αποκαλύπτουμε προσωπικά στοιχεία με μηνύματα e-mail ή άμεσα μηνύματα.** Πιθανόν να πρόκειται για απάτη. Οι περισσότερες αξιόπιστες εταιρείες δεν πρόκειται να μας ζητήσουν να αποκαλύψουμε προσωπικά στοιχεία μέσω e-mail. Εάν μια εταιρεία που εμπιστευόμαστε, όπως η τράπεζά μας ή η εταιρεία της πιστωτικής μας κάρτας, φαίνεται να μας ζητά προσωπικά στοιχεία, εξετάζουμε προσεκτικά το αίτημα αυτό. Καλούμε την εταιρεία στον αριθμό που αναγράφεται στο πίσω μέρος της πιστωτικής μας κάρτας, σε ένα λογαριασμό, στον τηλεφωνικό κατάλογο ή κάτι ανάλογο - και όχι στον αριθμό που περιέχεται στο e-mail. Εάν το αίτημα είναι γνήσιο, τότε το τμήμα εξυπηρέτησης πελατών της εταιρείας θα πρέπει να είναι σε θέση να μας βοηθήσει.

- **Σκεφτόμαστε προσεκτικά προτού ανοίξουμε συνημμένα αρχεία και προτού κάνουμε κλικ σε συνδέσμους που περιέχονται σε μηνύματα e-mail ή άμεσα μηνύματα,** ακόμη κι αν γνωρίζουμε τον αποστολέα. Εάν δεν μπορούμε να ζητήσουμε από τον αποστολέα να επιβεβαιώσει ότι το συνημμένο ή ο σύνδεσμος είναι ασφαλής, διαγράφουμε το μήνυμα. (Εάν πρέπει οπωσδήποτε να ανοίξουμε ένα συνημμένο αρχείο για το οποίο δεν είμαστε βέβαιοι, το αποθηκεύουμε πρώτα στο σκληρό μας δίσκο ώστε να μπορέσουμε να το ελέγξουμε με το πρόγραμμα προστασίας από τους ιούς, προτού το ανοίξουμε).

- **Δεν αγοράζουμε τίποτε και δεν συνεισφέρουμε σε εράνους που προωθούνται μέσω μηνυμάτων spam.** Οι αποστολείς μηνυμάτων spam συχνά ανταλλάσσουν ή πωλούν τις διευθύνσεις όσων έχουν αγοράσει κάτι από αυτούς - συνεπώς, εάν αγοράσουμε κάτι μέσω spam, πιθανόν να αρχίσουμε να λαμβάνουμε ακόμα περισσότερα ανεπιθύμητα μηνύματα. Επιπλέον, πολλοί αποστολείς τέτοιων μηνυμάτων κερδίζουν ένα αρκετά υψηλό εισόδημα από αυτούς που αγοράζουν τα προϊόντα τους. Αποφεύγουμε τον πειρασμό να αγοράσουμε προϊόντα μέσω ανεπιθύμητων μηνυμάτων, ώστε να βοηθήσουμε στον αγώνα κατά των αποστολέων τους. Κάποιοι εγκληματίες χρησιμοποιούν μηνύματα spam για να εκμεταλλευτούν την επιθυμία των ανθρώπων να βοηθήσουν τους άλλους. Εάν λάβουμε ένα μήνυμα e-mail από κάποια φιλανθρωπική οργάνωση που επιθυμούμε να υποστηρίξουμε, αποφεύγουμε τις απάτες συνεισφορών και καλούμε απευθείας την οργάνωση για να μάθουμε πώς μπορούμε να βοηθήσουμε.

- **Δεν προωθούμε αλυσιδωτά μηνύματα e-mail.** Με τα μηνύματα αυτά, όχι μόνον αποκαλύπτετε τη διεύθυνση e-mail μας σε άγνωστα άτομα, αλλά

πιθανόν να διασπείρουμε μια απάτη ή να μεταδώσουμε κάποιον ιό. Επιπλέον, έχει αναφερθεί ότι οι αποστολείς μηνυμάτων spam χρησιμοποιούν αλυσιδωτά μηνύματα ειδικά για να συλλέξουν διευθύνσεις e-mail.

1.4.12 Χρήσιμες συμβουλές

- Να μην απαντάμε ποτέ σε ένα spam e-mail και να μην κάνουμε πουθενά κλικ, γιατί απλούστατα η απάντησή μας ή και η άρνησή μας θα επιβεβαιώσει την εγκυρότητα του δικού μας e-mail και έτσι το e-mail μας θα γίνει μια πολύτιμη πληροφορία για πολλούς spammers.

- Να έχουμε μια πρόχειρη και μη συχνά χρησιμοποιούμενη ηλεκτρονική διεύθυνση, εκτός φυσικά από την κανονική, και να την δίνουμε σε πρώτη ζήτηση έτσι ώστε να πηγαίνουν εκεί όλα τα ανεπιθύμητα e-mails.

- Προσπαθούμε να γράφουμε το e-mail μας με τέτοιο τρόπο ώστε να μην περιέχει το σύμβολο @ και να είναι έτσι δύσκολη η αναγνώρισή του από τα προγράμματα των spammers. Για παράδειγμα, γράφουμε XXXXXX at hotmail com αντί για το κανονικό και εύκολα εντοπισμό XXXXX@hotmail.com

- Αναζητάμε και εγκαθιστάμε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails. Να ελέγχουμε πάντα αν αυτά τα προγράμματα-φίλτρα κάνουν σωστά το μπλοκάρισμα των spam e-mails.

- Δεν κάνουμε ποτέ προώθηση (forward) των spam e-mails σε φίλους ή και τρίτους, γιατί κι αυτοί θα προστεθούν στην λίστα αποδοχής.

- Δεν παρασυρόμαστε ποτέ από δελεαστικούς τίτλους, όπως a very special message for you, earn money easily, urgent and confidential κ.ά.

1.4.13 Τελικά για τα Spam

Ως απλοί χρήστες του Internet και του e-mail (ηλεκτρονικό ταχυδρομείο) σίγουρα έχουμε αισθανθεί την ενόχληση από την αποστολή τέτοιων απρόκλητών και ενοχλητικών μηνυμάτων.

Ιδιαίτερο πρόβλημα αντιμετωπίζουν οι χρήστες που χρησιμοποιούν μεγάλα διαστήματα της μέρας το ηλεκτρονικό ταχυδρομείο και είναι αναγκασμένοι να σβήνουν όλη αυτή την ανεπιθύμητη αλληλογραφία.

Τα μηνύματα αυτά για αρκετούς χρήστες μπορεί να είναι πολλές φορές και μερικές δεκάδες σε μια ημέρα. Η αναγκαιότητα για την αντιμετώπιση του spam εντοπίζεται στα ακόλουθα σημεία.

Πρόκειται για φαινόμενο πολύ ενοχλητικό και απαράδεκτο από τους παραλήπτες, καθώς ένας τακτικός χρήστης του Internet μπορεί να λαμβάνει εκατοντάδες τέτοια μηνύματα σε καθημερινή βάση. Πολλές φορές προβάλλονται αμφίβολης ποιότητας προϊόντα και υπηρεσίες ενώ συνηθισμένη είναι και η προβολή ύποπτων οικονομικών δραστηριοτήτων τύπου πυραμίδων ή άλλων μηνυμάτων που περιέχουν ή διαφημίζουν σεξουαλικό περιεχόμενο.

Κάνει κατάχρηση των πόρων του Internet, δηλ. επιβαρύνει πάρα πολύ τους e-mail servers, χωρίς να προσφέρει κάτι ουσιαστικό. Η κατάχρηση αυτή επιβαρύνει τα δίκτυα με κατανάλωση εύρους ζώνης, αποθηκευτικών και υπολογιστικών πόρων στα κεντρικά συστήματα διανομής αλληλογραφίας (e-mail servers). Αντίστοιχα προβλήματα προκαλεί στην πρόσβαση και τα συστήματα των χρηστών.

Θέτει σε κίνδυνο την ασφάλεια και την αξιοπιστία του Internet, καθώς πολλά τέτοια μηνύματα περιέχουν επικίνδυνους ιούς ή μπορεί και τα ίδια τα ανεπιθύμητα μηνύματα να είναι αποτέλεσμα δράσης ιών.

Οι spammers βρίσκονται σε συνεχή αναζήτηση συστημάτων τα οποία θα μπορούσαν να χρησιμοποιήσουν για την αποστολή των μηνυμάτων τους. Πολλά μηνύματα αυτής της κατηγορίας μεταφέρουν συνημμένα αρχεία τα οποία μπορεί να είναι ιοί (virus) ή σκουλήκια (worms) ή δούρειοι ίπποι (trojan horses) και τα οποίοι θέτουν σε κίνδυνο την ασφάλεια των συστημάτων. Το τελευταίο διάστημα μεγάλο ποσοστό ανεπιθύμητης και επικίνδυνης αλληλογραφίας είναι αποτέλεσμα της δράσης ιών που έχουν προσβάλει διάφορα συστήματα διασυνδεμένα στο Διαδίκτυο.

1.5 Αντίμετρα

1.5.1 RBL

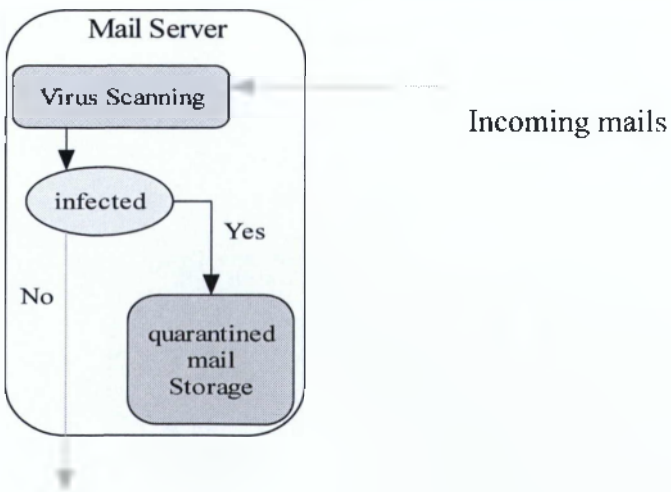
Η RBL είναι μια λίστα με καταγραφές συστημάτων που αποστέλλουν ανεπιθύμητα μηνύματα (SPAM/ virus) με σκοπό να αποτρέπεται η παραλαβή ανεπιθύμητων μηνυμάτων από συστήματα που έχουν καταχωρηθεί στην RBL .

Η RBL ζώνη περιέχει IP διευθύνσεις από μολυσμένους Η/Υ και ενημερώνεται αυτόματα από ένα μηχανισμό που εκτελείται στους κατά τόπους mail server(+antivirus).

Με αυτόν τον τρόπο ο παραπάνω μηχανισμός εκτελεί τις παρακάτω λειτουργίες:

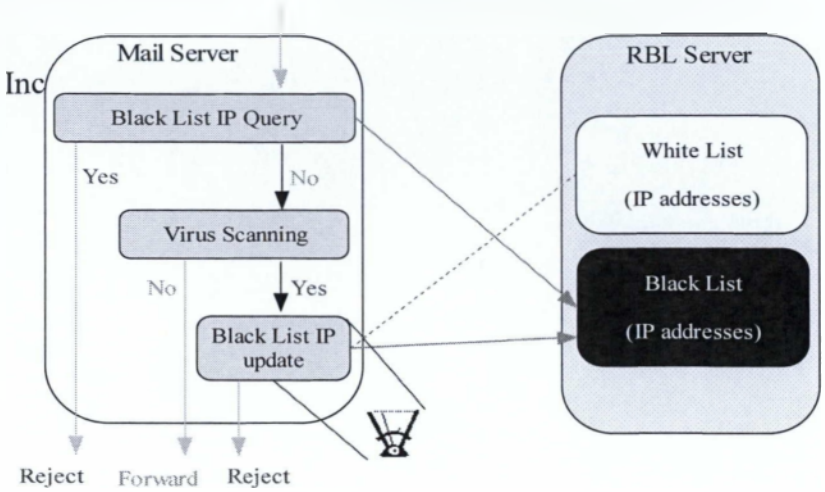
α. Αναλύει τους Headers των quarantined emails

Ο μηχανισμός αναλαμβάνει να ελέγξει τα headers των email που έχουν ιούς (quarantined) και να εξάγει το IP του αρχικού αποστολέα.



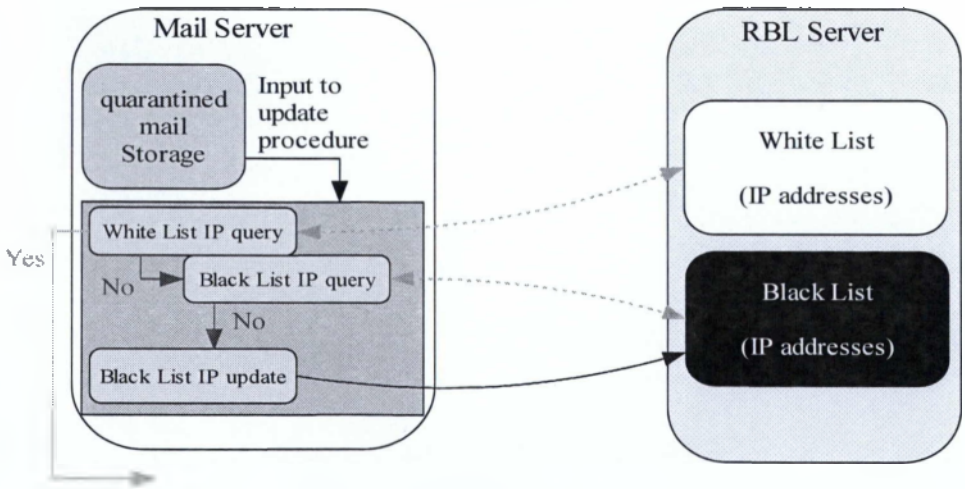
β. Ελέγχει τις εξαγόμενες IP διευθύνσεις βάση ενός whitelist

Ελέγχει αν το IP του αποστολέα βρίσκεται στην whitelist και αν όχι θα το συμπεριλάβει σε ένα αρχείο όπου θα υπάρχουν τα IP όλων των αποστολέων.



γ. Ενημερώνει την RBL ζώνη με τις IP διευθύνσεις

Όταν ο αριθμός των email με ιούς που αποστέλλονται ξεπεράσει κάποιο ρυθμιζόμενο αριθμό τότε η IP του αποστολέα εισάγεται στην blacklist .



Adding IP address

Forward

Με την RPL πετυχαίνουμε:

- Προστατεύουμε τα ιδρύματα που τυχόν δεν έχουν antivirus στον boundary mail server τους.
- Εμποδίζουμε αποτελεσματικά συνδέσεις από μολυσμένα συστήματα.
- Αυτοματοποιούμε τη διαδικασία reporting.

- Φτιάχνουμε ένα κατανεμημένο σύστημα αξιοποιώντας την πληροφορία από τους κατά τόπους mailserver.

1.5.2 Digital Signatures

Οι ψηφιακές πιστοποιήσεις και υπογραφές είναι ένας επιπλέον τρόπος για να φέρει το κάθε ηλεκτρονικό μήνυμα που στέλνετε προς τρίτους. Τα ψηφιακά αυτά μέσα , δημιουργούνται από διάφορες εταιρίες και προστίθενται σαν αρχεία σε κάθε απεσταλμένο email , σαν ενός είδους ειδική σφραγίδα γνησιότητας προέλευσης. Για την έκδοση τέτοιας ψηφιακής σφραγίδας μπορεί ο κάθε χρήστης με μια αίτηση και μια διαδικασία λίγων δευτερολέπτων , να αποκτήσει με δικά του στοιχεία την αντίστοιχη. Η ψηφιακή σφραγίδα που θα εκδοθεί θα περιέχει την διεύθυνση ηλεκτρονικού ταχυδρομείου , για την οποία και θα εκδοθεί και μερικά ακόμα στοιχεία που θα έχει τοποθετήσει ο χρήστης.
Με αυτό τον τρόπο θα γίνεται η εξακρίβωση της αυθεντικότητας προέλευσης και περιεχομένου από τον επονομαζόμενο αποστολέα και δεν θα απορρίπτεται από τα ειδικά φίλτρα spam. Μάλιστα η διαδικασία έκδοσης ψηφιακών στοιχείων πιστοποίησης, φέρει και ειδικά στοιχεία αυθεντικοποιήσης του αιτούντα, έτσι ώστε κανένας spam μηχανισμός να μπορεί να εκδόσει ανάλογο ψηφιακό έγγραφο ταυτότητας , για να προχωρήσει στο να ξεγελάσει φίλτρα , servers και χρήστες.
Για οικιακούς χρήστες, υπάρχουν αρκετές εταιρίες στο web που δωρεάν και μετά από αίτηση θα μπορέσουν να παρέχουν ανάλογο έγγραφο (π.χ. thatwee.com). Μέσα από την ίδια την σουίτα του MS Outlook να προχωρήσει κάποιος στην δημιουργία και προσθήκη μιας παρόμοιας δικλείδας.
Μέσω του Microsoft Outlook 2007, μπορεί ο χρήστης να πάει στο toolbar>tools>trust center>Email Security>get a Digital ID και να προχωρήσει μετά βήμα,βήμα στην δημιουργία και απόκτηση μιας ψηφιακής ταυτότητας που θα πρέπει να συνδεθεί με μια μόνο διεύθυνση ηλεκτρονικού ταχυδρομείου.

1.5.3 Bayesian Spam Filters

Φίλτρα Spam που βασίζονται στο Θεώρημα του Bayes. Τα Spam είναι ανεπιθύμητα e-mails που κατακλύζουν τα ηλεκτρονικά mailboxes δημιουργώντας προβλήματα στους χρήστες ηλεκτρονικού ταχυδρομείου αλλά και στα συστήματα διαχείρισης ηλεκτρονικού ταχυδρομείου. Προέκυψε έτσι η ανάγκη ανάπτυξης εργαλείων λογισμικού τα οποία να φιλτράρουν τα εισερχόμενα e-mails και να απορρίπτουν τα Spam. Πολλά από τα εργαλεία που αναπτύχθηκαν για το σκοπό αυτό (όπως το SpamAssassin ή το ASSP) βασίζονται στο Θεώρημα του Bayes1.Ας δούμε πώς.
Η βασική ιδέα για την ανάπτυξη αυτών των φίλτρων είναι ότι κάποιες λέξεις όπως «opportunity», «offer», «special», ή συνδυασμοί λέξεων όπως «enhance performance», μπορεί να μαρτυρούν ότι ένα μήνυμα που περιέχει κάποια ή κάποιες από αυτές τις λέξεις είναι Spam. Αν επομένως απαντηθεί το ερώτημα *«ποια είναι η πιθανότητα, να είναι Spam ένα μήνυμα που διαπιστώσαμε ότι περιέχει μια ή περισσότερες τέτοιες λέξεις»* και βρεθεί ότι η πιθανότητα αυτή είναι μεγάλη (μεγαλύτερη από κάποιο επίπεδο που θέτουμε π.χ. 95 %) τότε ένα τέτοιο μήνυμα μπορεί να απορριφθεί από το φίλτρο, δηλαδή, να θεωρηθεί Spam.
Βέβαια, ένα τέτοιο φίλτρο μπορεί να κάνει λάθη. Δηλαδή, μπορεί ένα μήνυμα να το θεωρήσει Spam ενώ δεν είναι, καθώς επίσης ένα μήνυμα να μην το θεωρήσει Spam ενώ είναι. Αυτό που επιδιώκεται είναι να ελαχιστοποιείται η πιθανότητα να θεωρηθεί

ένα μήνυμα Spam ενώ δεν είναι. Είναι προφανές ότι τέτοια φίλτρα μπορούν να βασίζονται σε μία ή περισσότερες λέξεις ή σε έναν ή περισσότερους συνδυασμούς λέξεων.

Ας δούμε ένα απλό φίλτρο που βασίζεται σε μια μόνο λέξη. Έστω «w» μια τέτοια λέξη και ας υποθέσουμε ότι σε μια χρονική περίοδο φθάνει σε έναν mail server ένα σύνολο μηνυμάτων. Κάθε μήνυμα από αυτά είναι ή δεν είναι Spam. Έτσι, αν *S* είναι το υποσύνολο των μηνυμάτων που είναι Spam τότε προφανώς το *S΄* είναι το υποσύνολο των μηνυμάτων που δεν είναι Spam. Μπορούμε να μετρήσουμε σε πόσα από τα μηνύματα του υποσυνόλου *S* και σε πόσα από τα μηνύματα του υποσυνόλου *S΄* εμφανίζεται η λέξη «w» και έτσι να εκτιμήσουμε αφενός την πιθανότητα: *ένα μήνυμα που είναι Spam να περιέχει τη λέξη «w»* και αφετέρου την πιθανότητα: *ένα μήνυμα που δεν είναι Spam να περιέχει τη λέξη «w»*.

Επίσης, μπορούμε να εκτιμήσουμε την πιθανότητα: *ένα μήνυμα που φθάνει στον mail server είναι Spam* και την πιθανότητα: *ένα μήνυμα που φθάνει στον mail server δεν είναι Spam*.

Συνήθως τα Bayesian, βάζουν ένα σκορ, πχ αν έχει την λέξει sex +10, αλλά αν έχει τη λέξη doctor -5 (μήπως είναι ιατρικό sex). Στο τέλος παίρνει μια βαθμολογία, πχ +40. Ανάλογα το όριο που βάζουμε (ευαίσθητο φίλτρο το κόβουμε πχ στο +20, αναίσθητο στο +100). Μια μέθοδος που χρησιμοποιούσαν οι spammers για να ΜΗΝ λειτουργούν τα score tests είναι να γράφουν επίμαχες λέξεις με letter substitution (υποκαταστάσεις γραμμάτων). Πχ αντί VIAGRA γράφουν VI4GR4, το sex το γράφουν s3x κτλ (αντί A, 4, αντί S, $ κτλ). Άλλοτε τα γράφουν ανορθόγραφα πχ αντί offer, γράφουν offer κτλ. Βέβαια αυτό καταντά αστείο καθώς στην προσπάθεια τους οι spammers να φτιάξουν ένα mail που δεν το πιάνουν τα φίλτρα καταντούν να φτιάχνουν ένα email που ούτε ο παραλήπτης μπορεί να διαβάσει με ευκολία.

1.5.4 Source URL (SURLS)

Σε αντίθεση με τις RBL λίστες οι SURLS είναι πιο αποδοτικές. Ουσιαστικά ο μηχανισμός AntiSPAM που χρησιμοποιεί SURLS δεν τον ενδιαφέρει από ποιον έρχεται το SPAM email. Αν δηλαδή το στέλνει κάποιος «γνωστός» spamer (αυτό το κάνουν οι RBL). Άλλωστε όπως έχουμε πει οι μολυσμένοι με BOTs υπολογιστές στέλνουν email από 1000άδες ανυποψίαστους χρήστες μέσω των δικών τους «καθαρών» λογαριασμών email τα οποία δεν είναι σε κάποια RBL.

Στις τεχνικές που χρησιμοποιούν SURLs ο αλγόριθμος του φίλτρου κοιτάει μέσα στο email να βρει αναφορές σε URLs από Spamers. Η λογική είναι απλή. Συνήθως ένας SPAMMER ενσωματώνει κάποια URL την οποία προτρέπει τον παραλήπτη να επισκεφτεί. Αν πουλάει πχ VIAGRA τον προτρέπει να επισκεφτεί κάποιο site πχ το www.pharmachy.com. Το site αυτό και άλλα κατηγοριοποιούνται ότι ανήκουν σε spammers, οπότε όποιο email περιέχει αναφορά σε αυτά (surl) απορρίπτεται ως spam.

1.5.5 Τεχνικές παράκαμψης φίλτρων

Καθώς τα πιο πολλά αντίμετρα στηρίζονται στην επεξεργασία και ανάλυση, του κειμένου ενός email μια εποχή ήταν της μόδας να στέλνουν όλα το email σαν εικόνα. Με άλλα λόγια ο spammer μετέτρεπε όλο το email σε jpg εικόνα ή οποία διαβάζεται από άνθρωπο, αλλά δεν μπορεί να αναλυθεί από πρόγραμμα. Για να αντιμετωπιστεί η κατάσταση πολλοί mail server έκοβαν έτσι και αλλιώς email που αποτελούνταν από μια μόνο εικόνα.

Οι spammers την συνέχεια άρχισαν να συνδυάζουν λέξεις και προτάσεις (συνήθως άσχετες με το spam) με εικόνες (οι οποίες περιείχαν το spam). Αυτό δεν αντιμετωπίστηκε ποτέ επιτυχώς από μόνο του. Κατάλοιπο αυτού είναι, ακόμα και σήμερα, οι πιο πολύ mail clients αλλά και webmail (όπως hotmail), να ΜΗΝ δείχνουν εξορισμού εικόνες σε ένα mail αλλά να πρέπει ο χρήστης να ζητήσει να το δει..

1.6 Μηνύματα οικονομικής εξαπάτησης (phishing)

Το phishing (αγγλικός νεολογισμός βασιζόμενος στη λέξη fishing=ψάρεμα) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπεραιώσουν μία συναλλαγή.

Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια «μοναδική ευκαιρία» και ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση url μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης όψεως, φαίνεται σωστή, όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου. Είτε χρησιμοποιούνται εντολές javascript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστοχώρο, είτε χρησιμοποιούνται τα ίδια τα scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο.

Παρόλο που οι περισσότεροι browsers έχουν ήδη αναπτύξει τεχνολογία anti-phishing προκειμένου να ανιχνεύουν τις σελίδες που ανοίγει ο χρήστης και να τον ειδοποιούν για το αν βρίσκεται σε σελίδα phishing, τα θύματα από τέτοιες επιθέσεις αυξάνονται ανησυχητικά σε όλον τον κόσμο. Ο χρήστης πρέπει να είναι ιδιαίτερα καχύποπτος απέναντι σε τέτοια μηνύματα και να επαληθεύει το περιεχόμενό τους επικοινωνώντας με την εταιρεία ή την τράπεζα που το έστειλε, όχι μέσω του μηνύματος, αλλά με τον τρόπο που χρησιμοποιούσε ως τώρα. Γενικά, οι αξιόπιστες εταιρείες και τράπεζες δεν καταφεύγουν σε γενικόλογα μηνύματα προκειμένου να εξυπηρετήσουν τους πελάτες τους, ούτε τους ζητούν να αποκαλύψουν τους κωδικούς τους.

Σήμερα κυκλοφορούν αρκετά προγράμματα anti-phishing, τα οποία είτε ελέγχουν το περιεχόμενο των ιστοσελίδων που διατρέχει ο χρήστης, είτε το περιεχόμενο των e-mail που λαμβάνει, προκειμένου να διαπιστώσουν αν πρόκειται για phishing, ενώ αποκαλύπτουν και το πραγματικό όνομα του ιστοχώρου που επισκέπτεται ο χρήστης.

1.6.1 Ενδείξεις πως ένα ηλεκτρονικό μήνυμα είναι πιθανόν πλαστό

- Ως spam μηνύματα, χρησιμοποιούν συνήθως γενικές προσφωνήσεις, όπως "Αγαπητέ πελάτη", αντί για το πραγματικό όνομα του παραλήπτη.

- Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο δήθεν πρόβλημα ή κάποια "μοναδική ευκαιρία" και, χρησιμοποιώντας φρασεολογία που δημιουργεί την αίσθηση του επείγοντος, ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

- Συνήθως ζητούν την παραχώρηση απορρήτων προσωπικών στοιχείων οικονομικού χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, όπως το Όνομα Χρήστη (username) και τον Κωδικό Πρόσβαση (password).

1.6.2 Εναλλακτικές μορφές

Spear Phishing: Πρόκειται για στοχευόμενα μηνύματα που μοιάζουν αυθεντικά για κάποιες ομάδες ανθρώπων. Για παράδειγμα, στους υπαλλήλους μιας εταιρίας μπορεί να φτάσει μήνυμα με αποστολέα τον εργοδότη τους, στο οποίο τους απευθύνεται προσωπικά και τους ζητά όνομα χρήστη και κωδικούς πρόσβασης. Απαντώντας κανείς σε ένα μήνυμα spear phishing θέτει προσωπικές και συχνά απόρρητες πληροφορίες στη διάθεση των απατεώνων.

Vishing: Σε αυτή την εκδοχή του phishing, για να πειστεί ευκολότερα το θύμα, του δίνεται τηλεφωνικός αριθμός εξυπηρέτησης ή του ζητείται το δικό του τηλέφωνο ώστε να μπορούν να επικοινωνήσουν μαζί του οι υποτιθέμενοι εκπρόσωποι της εταιρίας. Η πρακτική αυτή στηρίζεται στις τεχνολογίες Voip που προσφέρει το Διαδίκτυο.

Social Networking Phishing: Αντλώντας πληροφορίες και πολλά προσωπικά δεδομένα από τα προφίλ των χρηστών των ιστοσελίδων κοινωνικής δικτύωσης, οι απατεώνες στέλνουν εξατομικευμένα μηνύματα. Η επιτυχία της μεθόδου είναι μεγάλη. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες το 70% όσων έλαβαν το εξατομικευμένο παραπλανητικό μήνυμα πάτησε το σύνδεσμο που περιέχετε σε αυτό και συμπλήρωσε τα στοιχεία του στο εικονικό site.

1.6.3 Phishing mules

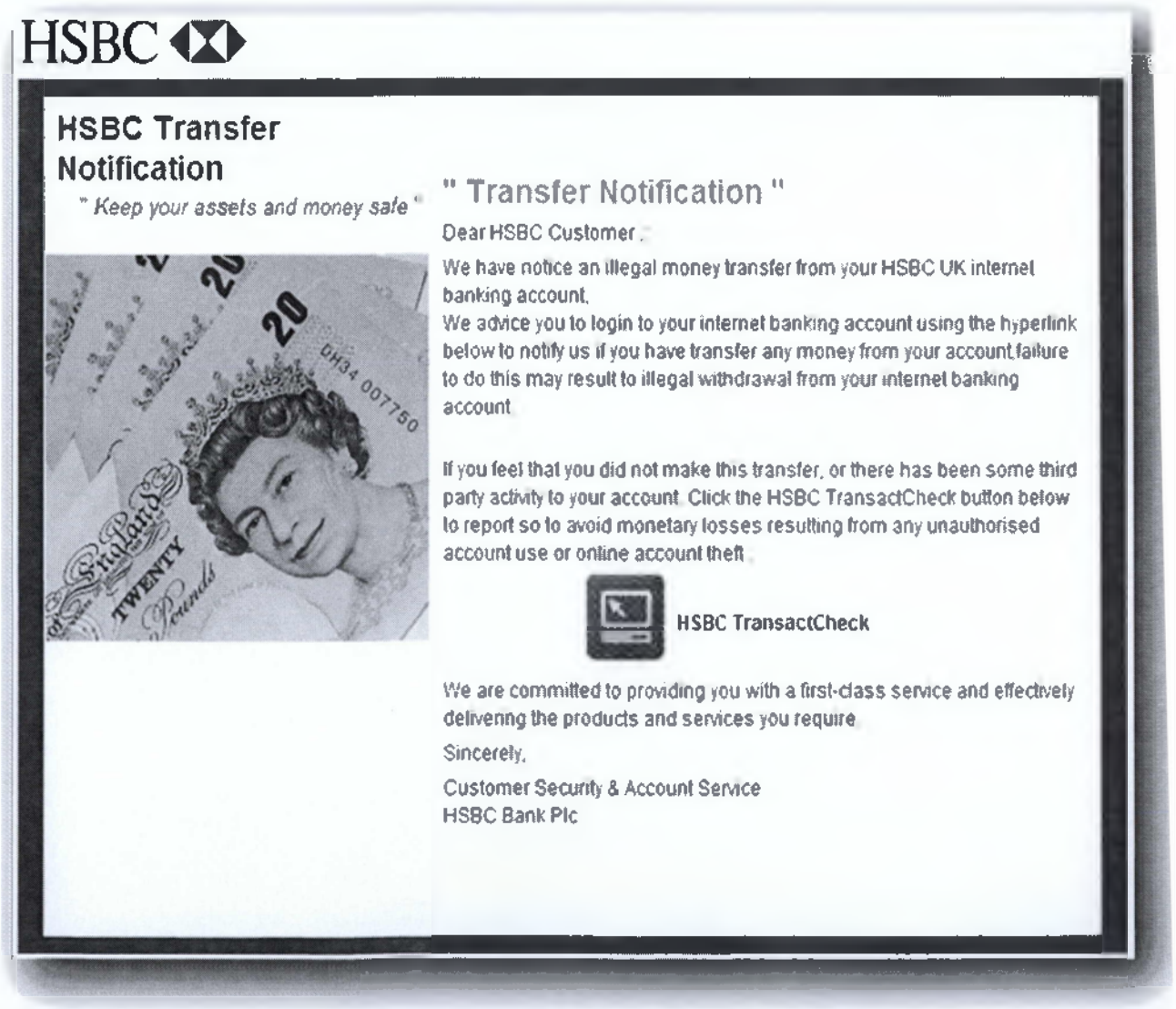
Οι εγκέφαλοι της απάτης συγκεντρώνουν τα οικονομικά στοιχεία ατόμων μέσω phishing, και έτσι είναι σε θέση να καταχραστούν τα στοιχεία αυτά και να υποκλέψουν χρήματα από τους εκτεθειμένους λογαριασμούς. Για να καλύψουν όμως τα ίχνη τους, αναθέτουν σε ανυποψίαστα άτομα να παίξουν το ρόλο μεσολαβητών, δημοσιεύοντας διάφορες δελεαστικές αγγελίες εργασίας στο Internet που υπόσχονται στους ενδιαφερόμενους ότι θα κερδίσουν χρήματα γρήγορα και με λίγη προσπάθεια. Τα άτομα αυτά είναι γνωστά ως «mules».

Οι τραπεζικοί λογαριασμοί των mules χρησιμοποιούνται για την παραλαβή εμβασμάτων από τους εκτεθειμένους λογαριασμούς. Στη συνέχεια, τους ζητείται να αποσύρουν τα χρήματα από το λογαριασμό τους σε μετρητά και να τα αποστείλουν στους εγκέφαλους της απάτης, μείον την προμήθειά τους, χρησιμοποιώντας μια υπηρεσία διεθνών εμβασμάτων. Οι εγκέφαλοι της απάτης διατηρούν έτσι την ανωνυμία τους, αφήνοντας εκτεθειμένους τους phishing mules, τους οποίους μπορούν να παρακολουθήσουν οι αρχές.

Προσέχετε ιδιαίτερα αγγελίες εργασίας που προβλέπουν την είσπραξη και την αποστολή χρημάτων σε τραπεζικούς λογαριασμούς και η αμοιβή είναι με τη μορφή προμήθειας. Τα άτομα που προσλαμβάνουν οι εγκέφαλοι της απάτης διαπράττουν ξέπλυμα χρήματος και μπορεί να αντιμετωπίσουν ποινικές κυρώσεις.

1.6.4 Phishing attack σε τράπεζες

i) Το μήνυμα προέρχεται από έναν αποστολέα ο οποίος έχει χρησιμοποιήσει ένα πετυχημένο πλαστό "περιβάλλον" της HSBC Αγγλίας για να στήσει την απάτη του (το περιβάλλον διαθέτει μέχρι και απεικόνιση της Αγγλικής Λίρας!):

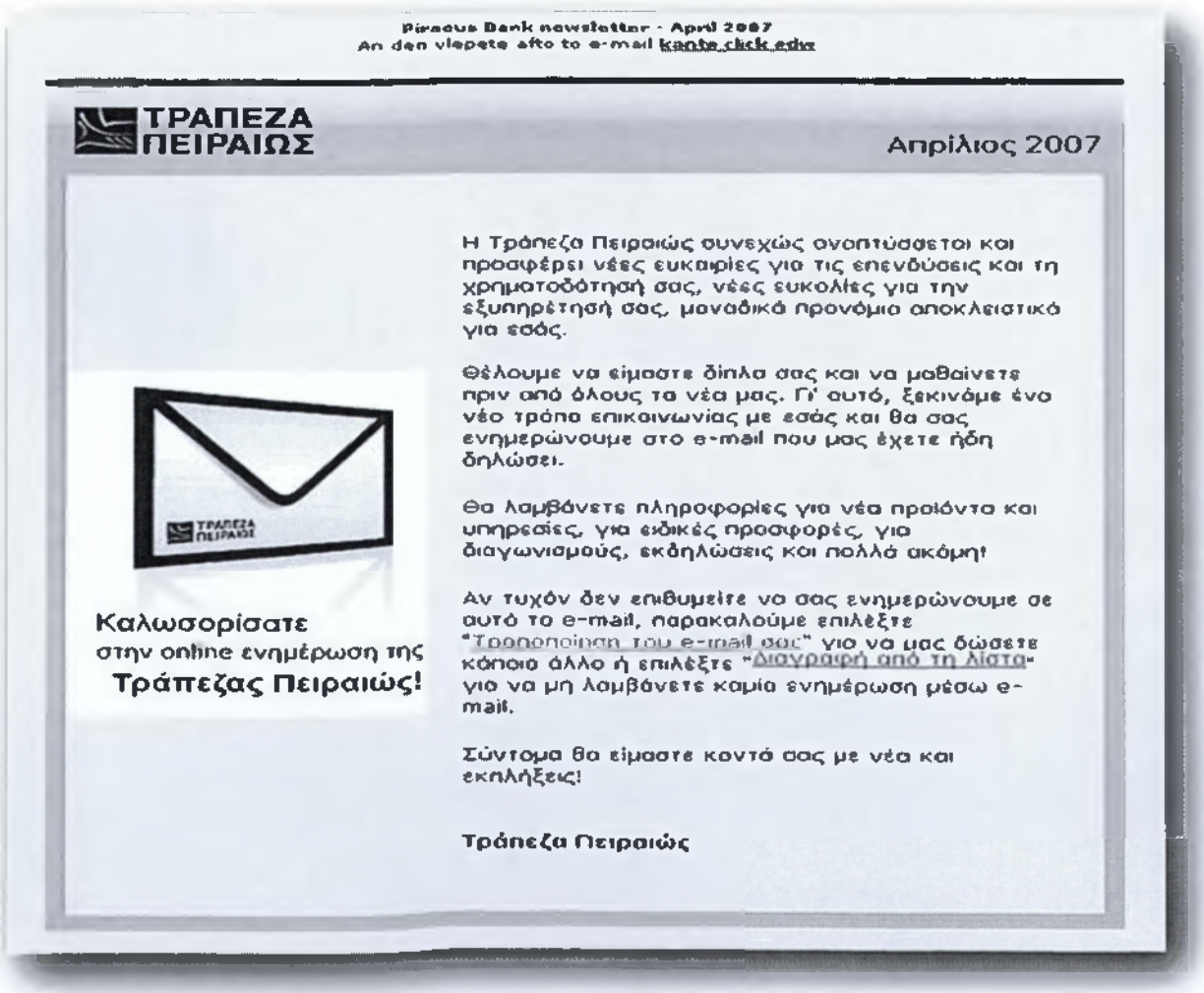


Το πλαστό μήνυμα πληροφορεί τον πιθανό Πελάτη και χρήστη της Υπηρεσίας e-Banking της Τράπεζας, ότι έχει παρατηρηθεί ασυνήθιστη κινητικότητα στον λογαριασμό του και τον προτρέπει να κάνει login στην Υπηρεσία e- Banking, για να ελέγξει την κίνηση του λογαριασμού του και για να αναφέρει στην Τράπεζα πιθανά προβλήματα.

Κατά την διάρκεια του login, το οποίο πραγματοποιείται στο ίδιο πλαστό περιβάλλον, οι κωδικοί εισόδου του χρήστη φυσικά υποκλέπτονται.
Θα πρέπει να γνωρίζουμε, ότι στον Ελληνικό χώρο ουδεμία Ελληνική Τράπεζα έχει νομιμοποιήσει κάποια ανάλογη διαδικασία, ώστε σε παρόμοιες περιπτώσεις να επικοινωνεί με τον Πελάτη της για λόγους ενημέρωσης κατά αυτό τον τρόπο.
Όλες οι Ελληνικές Τράπεζες υποχρεώνονται από την Τράπεζα της Ελλάδος να αναρτούν συγκεκριμένες οδηγίες στις επίσημες εμπορικές ιστοσελίδες τους (καθώς και στις εφαρμογές Ηλεκτρονικής Τραπεζικής), τις οποίες μπορούμε να συμβουλευόμαστε σε κάθε περίπτωση και οι οποίες αφορούν σε γενικούς και ειδικούς κανόνες ασφαλείας και σε κανόνες περί εμπιστοσύνης τρίτων, οι οποίοι επικοινωνούν κακόβουλα με τον Πελάτη για "λογαριασμό" της Τράπεζας.

ii)

Phishing επίθεση που στοχεύει τους πελάτες του τραπεζικού ιδρύματος Τράπεζα Πειραιώς, έλαβαν τα εργαστήρια του SecurityLabs.gr. Η επίθεση χρησιμοποιεί τεχνικές κοινωνικής μηχανικής με σκοπό να ξεγελάσει τους παραλήπτες και να τους πείσει να εισάγουν μία e-mail διεύθυνσή τους στα πλαίσια ενός νέου –υποτιθέμενου- προγράμματος επικοινωνίας του τραπεζικού ιδρύματος με τους πελάτες του.


Piraeus Bank newsletter - April 2007
An den vlepete afto to e-mail kante click edw

ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ

Απρίλιος 2007

Καλωσορίσατε στην online ενημέρωση της Τράπεζας Πειραιώς!

Η Τράπεζα Πειραιώς συνεχώς αναπτύσσεται και προσφέρει νέες ευκαιρίες για τις επενδύσεις και τη χρηματοδότησή σας, νέες ευκολίες για την εξυπηρέτησή σας, μοναδικά προνόμια αποκλειστικά για εσάς.

Θέλουμε να είμαστε δίπλα σας και να μαθαίνετε πριν από όλους τα νέα μας. Γι' αυτό, ξεκινάμε ένο νέο τρόπο επικοινωνίας με εσάς και θα σας ενημερώνουμε στο e-mail που μας έχετε ήδη δηλώσει.

Θα λαμβάνετε πληροφορίες για νέα προϊόντα και υπηρεσίες, για ειδικές προσφορές, για διαγωνισμούς, εκδηλώσεις και πολλά ακόμη!

Αν τυχόν δεν επιθυμείτε να σας ενημερώνουμε σε αυτό το e-mail, παρακαλούμε επιλέξτε "Τροποποίηση του e-mail σας" για να μας δώσετε κάποιο άλλο ή επιλέξτε "Διαγραφή από τη λίστα" για να μη λαμβάνετε καμία ενημέρωση μέσω e-mail.

Σύντομα θα είμαστε κοντά σας με νέα και εκπλήξεις!

Τράπεζα Πειραιώς

Πιο συγκεκριμένα, το κείμενο του phishing μηνύματος αναφέρει χαρακτηριστικά:

«Η Τράπεζα Πειραιώς συνεχώς αναπτύσσεται και προσφέρει νέες ευκαιρίες για τις επενδύσεις και τη χρηματοδότησή σας, νέες ευκολίες για την εξυπηρέτησή σας, μοναδικά προνόμια αποκλειστικά για εσάς. Θέλουμε να είμαστε δίπλα σας και να μαθαίνετε πριν από όλους τα νέα μας. Γι' αυτό, ξεκινάμε ένα νέο τρόπο επικοινωνίας με εσάς και θα σας ενημερώνουμε στο e-mail που μας έχετε ήδη δηλώσει. Θα λαμβάνετε πληροφορίες για νέα προϊόντα και υπηρεσίες, για ειδικές προσφορές, για διαγωνισμούς, εκδηλώσεις και πολλά ακόμη! Αν τυχόν δεν επιθυμείτε να σας ενημερώνουμε σε αυτό το e-mail, παρακαλούμε επιλέξτε «Τροποποίηση του e-mail σας» για να μας δώσετε κάποιο άλλο ή επιλέξτε «Διαγραφή από τη λίστα» για να μη λαμβάνετε καμία ενημέρωση μέσω e-mail. Σύντομα θα είμαστε κοντά σας με νέα και εκπλήξεις!»

Ιδιαίτερο ενδιαφέρον παρουσιάζει η στροφή στην τακτική των κακόβουλων χρηστών. Αυτή τη φορά η επίθεση δεν ζητά επαλήθευση των στοιχείων που αφορούν τους τραπεζικούς λογαριασμούς των χρηστών, αλλά «εγκαινιάζει» έναν - υποτιθέμενο- νέο τρόπο επικοινωνίας μεταξύ του πελάτη και του τραπεζικού ιδρύματος. Ενδεχόμενα, η επίθεση προετοιμάζει το έδαφος για μία ή περισσότερες μελλοντικές επιθέσεις (επαληθεύει λογαριασμούς ηλεκτρονικού ταχυδρομείου, «ψαρεύει» νέους) ενώ προσπαθεί να πείσει τους χρήστες πως το τραπεζικό ίδρυμα όντως επικοινωνεί μέσω ηλεκτρονικού ταχυδρομείου με τους πελάτες του - κάτι που θα διευκολύνει την μετέπειτα αποδοχή των μελλοντικών επιθέσεων.

1.6.5 Τρόποι προφύλαξης από το Phishing

- Να είμαστε γενικά καχύποπτοι και να μην απαντάμε σε μηνύματα ηλεκτρονικού ταχυδρομείου που μας ζητούν να αποκαλύψουμε αξιοποιήσιμα προσωπικά στοιχεία οικονομικού χαρακτήρα. Οι αξιόπιστες εταιρείες δεν συνηθίζουν να ζητούν από τους πελάτες τους να ενημερώσουν ή να επαληθεύσουν τέτοια απόρρητα στοιχεία με ένα απλό email.

- Ακόμη και σε περιπτώσεις που όλα δείχνουν ότι το μήνυμα είναι γνήσιο, είναι προτιμότερο να επικοινωνήσουμε με την εταιρία που παρουσιάζεται ως αποστολέας, για να επιβεβαιώσουμε ότι πράγματι αυτή μας έστειλε το μήνυμα και ότι δεν πρόκειται για περίπτωση απάτης.

- Φροντίζουμεε, όμως, να επικοινωνήσουμε με την εταιρεία αυτή με τον τρόπο που χρησιμοποιούμε συνήθως, και όχι σύμφωνα με τις οδηγίες που περιέχει το email ή απαντώντας σε αυτό.

- Δεν παραχωρούμε ευαίσθητα προσωπικά δεδομένα μέσω του διαδικτύου προσέχουμε την ηλεκτρονική διεύθυνση στην οποία βρισκόμαστε. Αντί για το απλό «http://», θα πρέπει να αρχίζει με «https://». Έτσι διασφαλίζουμε ότι χρησιμοποιούμε ασφαλή σύνδεση web (http secure).

- Γενικότερα, αγνοούμε ηλεκτρονικά μηνύματα που λαμβάνουμε από άγνωστες πηγές και αποφεύγουμε να συμπληρώνουμε ηλεκτρονικές φόρμες που παραλαμβάνουμε μέσω ηλεκτρονικού ταχυδρομείου.

- Ελέγχουμε συχνά τους online λογαριασμούς μας, εξετάζουμε προσεκτικά τόσο την συνολική κίνησή τους όσο και κάθε συναλλαγή ξεχωριστά, ώστε να είμαστε βέβαιοι ότι εγκρίνουμε όλα τα ποσά που έχει χρεωθεί.

- Χρησιμοποιούμε πάντα λογισμικό προστασίας από ιούς (antivirus). Παρόλο που τα antivirus δεν μπορούν να μας αποτρέψουν να ανοίξουμε ένα πλαστό ηλεκτρονικό μήνυμα, μπορούν εντούτοις να μας προστατεύσουν από ιούς ή λογισμικά υποκλοπής (spyware) που θα προέλθουν από τέτοιες ενέργειες. Πολλά Phishing μηνύματα οδηγούν σε διαδικτυακές τοποθεσίες που εγκαθιστούν στον υπολογιστή μας spywares τα οποία συνεχίζουν να καταγράφουν κάθε πληροφορία που εισάγουμε -πιθανότατα και αριθμούς λογαριασμών και πιστωτικών καρτών, και κωδικούς πρόσβασης- για πολύ καιρό μετά την αποχώρηση μας από τον συγκεκριμένο διαδικτυακό τόπο, ενώ μπορεί να περιέχει ακόμη και κάποιον ιό.

- Εγκατασουμε ψηφιακό φίλτρο που μπλοκάρει τα spam emails (antispam). Μας προσφέρει πλήρη ασφάλεια μέσω της προ-ενεργοποιημένης υπηρεσίας Email Antispamming, δίνοντάς μας επιπλέον τη δυνατότητα ενεργοποίησης ή απενεργοποίησης της υπηρεσίας καθώς και της διαμόρφωσής της σύμφωνα με τις ανάγκες μας.

1.7 Μηνύματα απατηλού περιεχομένου (hoaxes)

Αν κοιτάξει κανείς σε ένα λεξικό θα δει ότι hoax σημαίνει φάρσα, εξαπάτηση, κακόγουστο αστείο, κόλπο, μαϊμού, ξεγελώ, απομίμηση. Σαν όρος του διαδικτύου δεν διαφέρει καθόλου από τις λέξεις που προαναφέρθηκαν αφού δεν είναι τίποτε άλλο παρά φάρσες που κάνουν διάφοροι επιτήδειοι προειδοποιώντας μας συνήθως με email, για ιούς υπολογιστών που είναι ανύπαρκτοι. Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

1. **Προειδοποιητικά**: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα
2. **Συμπαράστασης**: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται
3. **Εκφοβισμού**: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.

Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος. Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ

λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

1.7.1 Οι λόγοι που γράφονται τα hoaxes

- Για ψυχαγωγία του συντάκτη τους που "σπάει πλάκα" με την διάδοση του μηνύματος του.
- Για να παρενοχλήσουν κάποιο άτομο
- Για να αποκτήσουν χρήματα συνήθως από οικονομικές "πυραμίδες".
- Για να σταματήσουν κάποιο άλλο hoax.
- Για να βλάψουν κάποιο συγκεκριμένο πρόσωπο ή την φήμη κάποιου οργανισμού ή εταιρείας

Δεν θα προσπαθήσουμε να μπούμε περισσότερο στον ψυχικό κόσμο των δημιουργών των hoaxes γιατί όσο δύσκολο είναι να ψυχολογήσει κανείς έναν hacker, cracker ή δημιουργό πραγματικών ιών το ίδιο δύσκολο είναι να είναι κανείς σίγουρος για το τι νοιώθει πραγματικά ένας δημιουργός ενός hoax και τι είναι αυτό που το παρακινεί πραγματικά να γράψει ένα virus hoax.

Το ευχάριστο σε αντίθεση με τις υπόλοιπες κατηγορίες είναι ότι τα hoaxes δεν διαγράφουν συνήθως τα κρίσιμα αρχεία του συστήματος και στο εδώ που τα λέμε καμιά φορά είναι τόσο πρωτότυπα που αν πραγματικά κάποιος τα καλοδιαβάσει όλο και θα χαμογελάσει, έστω και στα κλεφτά.

1.7.2 Πότε ένα email είναι hoax ή πραγματικότητα

Υπάρχουν κάποια χαρακτηριστικά από τα οποία μπορεί κάποιος να διακρίνει αν πρόκειται για πραγματική είδηση ή για hoax τα οποία αναφέρουμε παρακάτω:

- Σχεδόν σε όλα τα hoaxes γίνεται προτροπή από τον παραλήπτη να στείλει το μήνυμα που έλαβε και σε όλους τους φίλους και γνωστούς του προειδοποιώντας τους για τον επικίνδυνο ιό.
- Συνήθως σε αντίθεση με τους ιούς στα hoaxes δεν υπάρχει συνημμένο αρχείο.
- Τις περισσότερες φορές δεν υπάρχουν τρίτες έγκυρες πηγές που να μπορούν να επικυρώσουν την προειδοποίηση ή γενικότερα κάποιες διευθύνσεις από web sites όπου θα βρει κανείς αναλυτικότερες περιγραφές.
- Αρκετές φορές ξεχωρίζουν από το "ύφος" γραφής τους που δεν εμπνέει εμπιστοσύνη.
- Πολλές φορές υποστηρίζουν πως το μήνυμα τους έχει έρθει από πασίγνωστες εταιρείες όπως για παράδειγμα την Microsoft ή την Compaq αν πρόκειται για αλήθεια τότε σίγουρα θα υπάρχει σχετική αναφορά στα επίσημα sites των εταιρειών στο διαδίκτυο. Αν και μερικά "πετυχημένα" hoaxes χρησιμοποιούν το κόλπο του ψεύτικου URL που στηρίζεται σε έναν αποτυχημένο χειρισμό του χαρακτήρα AT (@) στο URL.
- Μερικές φορές για να μπερδέψουν τον παραλήπτη χρησιμοποιούνται τεχνικοί όροι που δεν υπάρχουν σε κανένα λεξικό.
- Χρησιμοποιούν απειλές του τύπου "αν δεν στείλεις αυτό το μήνυμα σε άλλους 15 θα σου χαλάσω τον υπολογιστή".

- Η εκφοβισμό του τύπου "αν δεν στείλεις αυτό το μήνυμα στους φίλους σου θα έχεις κακή τύχη για τα επόμενα 3 χρόνια".
- Αναφορές σε κακόβουλο κώδικα ή ιούς
- Ιστορίες με εταιρείες που μοιράζουν δωρεάν αντικείμενα (π.χ. κινητά) και άλλες που λένε ότι κερδίσατε ταξίδια και δώρα
- Αναφορές σε γεγονότα που έγιναν στο παρελθόν και πλέον δεν ισχύουν
- Γράμματα ένδειξης συμπαράστασης, συμπάθειας κλπ προς ασθενείς και άλλα πρόσωπα που έχουν κάποιο πρόβλημα
- Τα γνωστά chain letters που προσφέρουν συνήθως τύχη και ευτυχία σε όσους τα στείλουν στους γνωστούς και φίλους τους.
- Εταιρείες μαϊμούδες και απατεώνες που προσπαθούν να πείσουν για την επιχειρηματική τους δραστηριότητα
- Εντελώς αστεία, έως και γελοία μηνύματα που είναι σχεδόν αδύνατο να γίνουν πιστευτά
- Γεγονότα που έχουν αλλαχθεί ώστε να προβάλουν ή να δυσφημίζουν πρόσωπα και καταστάσεις.
- Τέλος υπάρχουν και οι αληθινοί μύθοι που κάνουν τον γύρο του internet και καταντούν και αυτοί hoaxes.

1.7.3 Τρόπο προστασίας από τα hoaxes

- Δεν ανοίγουμε συνημμένα αρχεία από αγνώστους, κάτι που ασφαλώς ισχύει και για τους ιούς.
- Ποτέ δεν ανακυκλώνουμε τα μηνύματα που μας καλούν να τα στείλουμε σε φίλους και γνωστούς αν πρώτα δεν σιγουρευτούμε ότι είναι πραγματικά από διαφορετικές πηγές.
- Διαβάζουμε προσεχτικά το κείμενο που μας έχουν στείλει και προσπαθούμε να διασταυρώσουμε αυτά που αναφέρει και από τρίτες πηγές.
- Δεν παρασυρόμαστε από συναισθηματισμούς ακόμα και αν το μήνυμα που μας έχουν στείλει μιλάει για παιδιά με ανίατες αρρώστιες ή άσχημα παιχνίδια της τύχης.

1.8 Απειλές ιών μέσω email

Έχει γίνει πλέον συνήθεια οι ιοί να στέλνονται σαν attachments σε ηλεκτρονικά ταχυδρομεία, ιδιαίτερα από γνωστούς και φίλους. Οι μοντέρνες μέθοδοι που χρησιμοποιούν τα προγράμματα των ιών είναι να δημιουργούν αυτόματα πληθώρα ηλεκτρονικών ταχυδρομείων από το Email address book (λίστα με διευθύνσεις) ενός χρήστη που έχει μολυνθεί και να τα στέλνουν σε όλους τους φίλους και γνωστούς με τους οποίους αυτός επικοινωνεί.

Το κείμενο που περιέχεται στο Email με το μολυσμένο attachment, πολλές φορές είναι γνώριμο στον παραλήπτη μιας και περιέχει την υπογραφή ενός φίλου, οδηγώντας το υποψήφιο θύμα να ανοίξει το attachment χωρίς να υποψιαστεί τίποτε.

Ιδιαίτερη προσοχή χρειάζεται στο άνοιγμα αρχείων (attachments) με EXE extension που είναι εκτελούμενα προγράμματα, χωρίς αυτό να σημαίνει ότι τα υπόλοιπα αρχεία είναι λιγότερο επικίνδυνα. Αν νομίζετε ότι αρχεία με extension.PIF,.GIF, ακόμη και.TXT είναι ασφαλή έχετε λάθος. Ακόμη και τέτοια αρχεία μπορεί να μεταφέρουν ιούς. Ας μην ξεχνάμε πόσο εύκολο είναι να γίνει rename ένα αρχείο exe σε txt για παράδειγμα.

Έχουμε την περίπτωση κατά την οποία το σύστημά σας θα μολυνθεί απο κάποιον ιό, trojans, worm. Η μόλυνση με αυτή την μορφή γίνεται ως εξής: Εάν λάβετε ένα e-mail με άγνωστο αποστολέα, πιθανόν το e-mail αυτό να περιέχει και κάποιο επισυναπτόμενο μολυσμένο αρχείο ή πρόγραμμα. Εάν εσείς αποφασίσετε να ανοίξετε το αρχείο αυτό ή να κάνετε εγκατάσταση το πρόγραμμα τότε ο ιός που είναι καμουφλαρισμένος μέσα σε αυτό θα αρχίσει να μολύνει τον υπολογιστή σας.

Μην ανοίγετε αρχεία αν δεν τα έχετε προηγουμένως ελέγξει με τον anti-virus scanner. Τα σύγχρονα προγράμματα anti-virus μπορεί να ρυθμιστούν για να ανιχνεύουν ιούς στα Emails που λαμβάνονται.

Η λαϊκή φαντασία επιμένει ότι οι ιοί δημιουργούνται από τις εταιρείες κατασκευής anti-virus software, οι οποίες με τον τρόπο αυτό διατηρούν και επαυξάνουν συνεχώς την πελατεία τους. Στην πραγματικότητα, όμως, οι εταιρείες αυτές δεν έχουν κανένα λόγο να μπουν στον κόπο της δημιουργίας ιών, αφού η παγκόσμια παραγωγή είναι αρκετή για να τις κρατήσει απασχολημένες για πολλά χρόνια ακόμη.

Κατά καιρούς, διάφοροι δημοσιογράφοι και κοινωνιολόγοι έχουν προσπαθήσει να έρθουν σε επαφή με τους ανθρώπους οι οποίοι δημιουργούν ιούς, σε μια προσπάθεια να κατανοήσουν τον τρόπο σκέψης και τα κίνητρά τους.

Σύμφωνα με όλες τις ενδείξεις η πρώτη επιτυχημένη επαφή αυτής της μορφής πραγματοποιήθηκε από τη Sarah Gordon, συνεργάτιδα της IBM, η οποία κατάφερε να επικοινωνήσει με τον Dark Avenger, έναν Βούλγαρο συγγραφέα ιών, η φήμη του οποίου είχε πάρει μυθικές διαστάσεις μεταξύ των ανθρώπων του χώρου.

Η εμπειρία της "προσωπικής επαφής" (μέσω chat room) έδειξε ότι ο άνθρωπος αυτός αποτελεί ένα τυπικό δείγμα συγγραφέα ιών και μπορεί να περιγραφεί με τη φράση "νέος και τσαντισμένος" (young and seething). Στην περίπτωση του Dark Avenger η οργή του προερχόταν από το γεγονός ότι ήταν εγκλωβισμένος στη Βουλγαρία και είχε στη διάθεσή του πολύ φτωχό εξοπλισμό. Έτσι, γι' αυτόν οι ιοί αποτελούσαν την εκδίκησή του εναντίον όσων διέθεταν καλύτερα μηχανήματα, αλλά δεν ήξεραν πώς να τα χρησιμοποιήσουν. Επίσης, επειδή οι ιοί του κυκλοφορούσαν σε ολόκληρο τον κόσμο η επιτυχία τους του έδινε ένα αίσθημα ελευθερίας, αφού χάρη σε αυτούς "ταξίδευε" παντού και ο ίδιος.

Έρευνες οι οποίες έγιναν παρατηρώντας τα λεγόμενα ανθρώπων όπως ο Dark Avenger ή η ομάδα Cult of the Dead Cow, έδειξαν ότι οι συγγραφείς ιών είναι συνήθως φυσιολογικοί άνθρωποι (σχεδόν πάντοτε άντρες) οι οποίοι βρίσκουν βαρετή την καθημερινή τους ζωή και χρησιμοποιούν τη δημιουργία ιών ως έναν τρόπο για να της δώσουν περισσότερο ενδιαφέρον.

Η μεγαλύτερη απειλή από τους ιούς προέρχεται απο την ηλεκτρονική αλληλογραφία. Το e-mail είναι μια απλή και αποδοτική μέθοδος για όποιον θέλει να διασπείρει κακόβουλο κώδικα σε μεγάλο αριθμό υπολογιστών. Αρκούν μερικά λεπτά για να κάνει ένας ιός το γύρο του κόσμου. Είτε πρόκειται για ιούς, Trojans, το Inbox είναι το πρώτο μέρος στο οποίο θα στοχεύσει κάποιος κακόβουλος χρήστης στην προσπάθειά του να μολύνει τον υπολογιστή σας.

1.9 Εμπορικές εφαρμογές για ασφάλεια email

I) Symantec Mail Security 8100 Series

Συσκευή ασφαλείας ηλεκτρονικής αλληλογραφίας που ελέγχει την κίνηση των μηνυμάτων spam εμποδίζοντας την αλληλογραφία spam από το σημείο προέλευσής της.

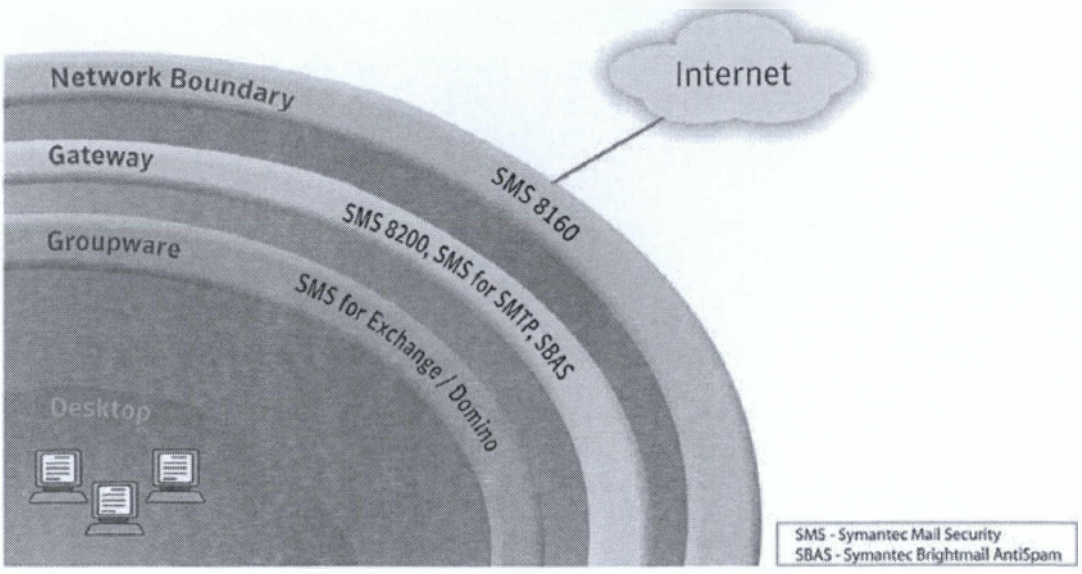
Η συσκευή Symantec Mail Security 8100 Series μειώνει το συνολικό όγκο της ηλεκτρονικής αλληλογραφίας σε ποσοστό έως και 50% εμποδίζοντας την αλληλογραφία spam πριν εισέλθει στο δίκτυο διασφαλίζοντας ταυτόχρονα τη συνεχή ροή της σημαντικής αλληλογραφίας. Έτσι υπάρχει σημαντική μείωση στα διαχειριστικά έξοδα, στην πρόκληση προβλημάτων συμφόρησης στο δίκτυο και στο κόστος υποδομής, διαμορφώνει την κίνηση της αλληλογραφίας στο επίπεδο TCP εμποδίζοντας τους αποστολείς αλληλογραφίας spam να προωθούν μηνύματα ηλεκτρονικής αλληλογραφίας σε προστατευμένα δίκτυα.

Επεκτείνεται εύκολα ώστε να ανταποκρίνεται στις ανάγκες των αναπτυσσόμενων επιχειρήσεων και μπορεί να συνδυαστεί με οποιαδήποτε λύση προστασίας από αλληλογραφία spam σε επίπεδο gateway, συμπεριλαμβανομένων των συσκευών Symantec Mail Security 8200 Series, για την παροχή μιας ολοκληρωμένης προσέγγισης πολλαπλών επιπέδων για την αντιμετώπιση της αλληλογραφίας spam. Χρησιμοποιεί την τεχνολογία Symantec Brightmail AntiSpam για την αντιμετώπιση των νέων τεχνικών αποστολής spam και των χαρακτηριστικών προτύπων κίνησης.

Symantec Mail Security 8160 – συσκευή 1U για εγκατάσταση σε rack

➢ *Χαρακτηριστικά και πλεονεκτήματα*

• Μειώνει το συνολικό όγκο της ηλεκτρονικής αλληλογραφίας σε ποσοστό έως και 50% εμποδίζοντας την αλληλογραφία spam πριν εισέλθει στο δίκτυο διασφαλίζοντας ταυτόχρονα τη συνεχή ροή της σημαντικής αλληλογραφίας.
• Περιορίζει το αυξανόμενο κόστος της υποδομής αλληλογραφίας και μειώνει το κόστος του υλικού, της αποθήκευσης και του δικτύου διαχείρισης.
• Διαμορφώνει την κίνηση στο επίπεδο TCP εμποδίζοντας τους αποστολείς αλληλογραφίας spam να προωθούν μηνύματα ηλεκτρονικής αλληλογραφίας σε προστατευμένα δίκτυα. Έτσι η αλληλογραφία παραμένει στους διακομιστές των αποστολέων αλληλογραφίας spam με αποτέλεσμα η δική τους υποδομή, αντί για τη δική σας, να λαμβάνει το φόρτο της αλληλογραφίας spam.
• Εύκολη στην εγκατάσταση, συμβατή με οποιονδήποτε διακομιστή μηνυμάτων και λειτουργεί διαφανώς στο δίκτυο
• Επεκτείνεται εύκολα ώστε να ανταποκρίνεται στις ανάγκες των αναπτυσσόμενων επιχειρήσεων. Μία μόνο συσκευή διαχειρίζεται έως 750.000 λογαριασμούς χρηστών και φόρτο αλληλογραφίας που υπερβαίνει τα 30 εκατομμύρια μηνύματα ημερησίως.
• Μπορεί να συνδυαστεί με οποιαδήποτε λύση προστασίας από αλληλογραφία spam σε επίπεδο gateway, συμπεριλαμβανομένων των συσκευών Symantec Mail Security 8200 Series, για την παροχή μιας ολοκληρωμένης προσέγγισης πολλαπλών επιπέδων για την αντιμετώπιση της αλληλογραφίας spam.
• Βασίζεται στην τεχνολογία Symantec Brightmail AntiSpam, με την οποία προστατεύονται περισσότεροι από 300 εκατομμύρια λογαριασμοί. Παρακολουθεί, εντοπίζει και ανταποκρίνεται στις νέες τεχνικές αποστολής spam και στα χαρακτηριστικά πρότυπα κίνησης.



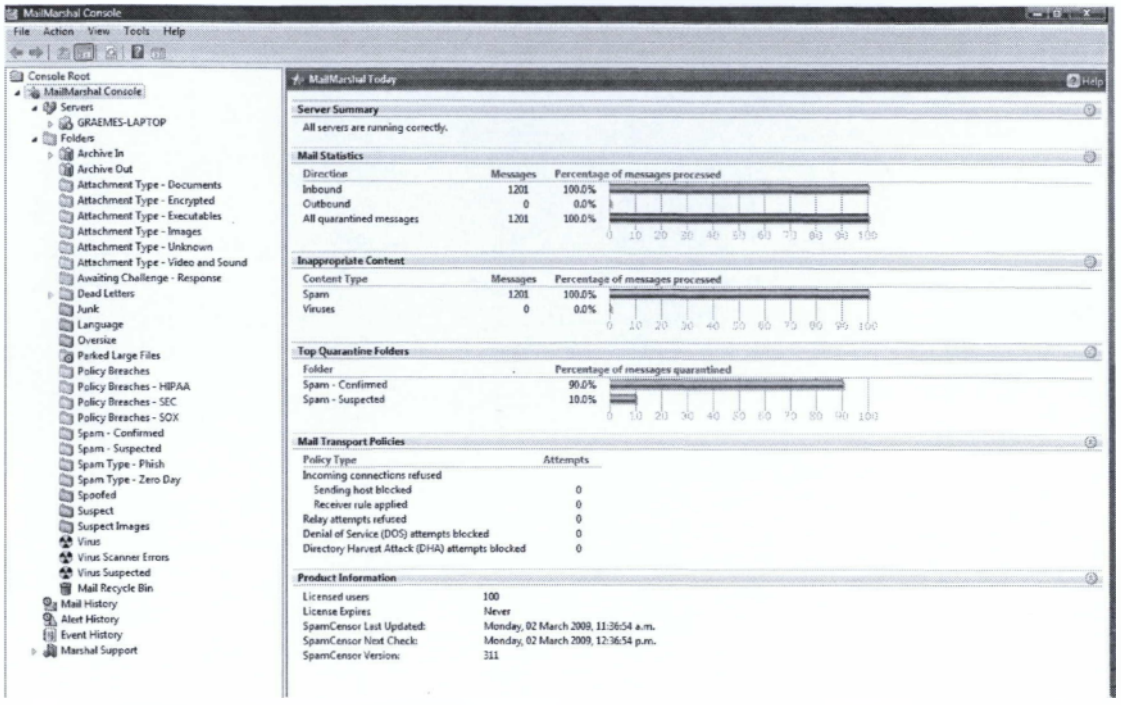
ii) MailMarshal SMTP 6.7

Το MailMarshal SMTP συμβάλει στην προστασία στο εταιρικό περιβάλλον του ηλεκτρονικού ταχυδρομείου κατά των spam και του κακόβουλο λογισμικό, όπως επίσης διαχειρίζεστε πολύπλοκες πολιτικές ασφαλείας κα αποτρέπει διαρροή εμπιστευτικών δεδομένων. Αναστέλλει εισερχόμενα κακόβουλα e-mail όπως το spam, phishing, ιοί, malware. Μπορεί να χρησιμοποιηθεί ως αυτόνομη λύση ή μαζικά, οι MailMarshal διακομιστές μπορούν να ρυθμιστούν εύκολα σε μια σειρά και να υποστηρίξουν τα μεγαλύτερα δίκτυα με κεντρική διαχείριση για την απλοποίηση των διοικητικών διαδικασιών.

➢ *Χαρακτηριστικά και πλεονεκτήματα*

- Εξασφαλίζει την e-mail πύλη σας ενάντια σε όλες τις απειλές.

Το Threats Mail Marshal αποκαθιστά την πραγματική αξία του ηλεκτρονικού ταχυδρομείου των επιχειρήσεων, καθιστώντας ασφαλή και αποτελεσματική τη χρήση του. Προστατεύει από όλα τα email, συμπεριλαμβανομένων των απειλών spam, phishing, ιούς, κακόβουλα προγράμματα, επιθέσεις DoS και πλαστογραφημένα μηνύματα.



- Ταχεία απόδοση της επένδυσης

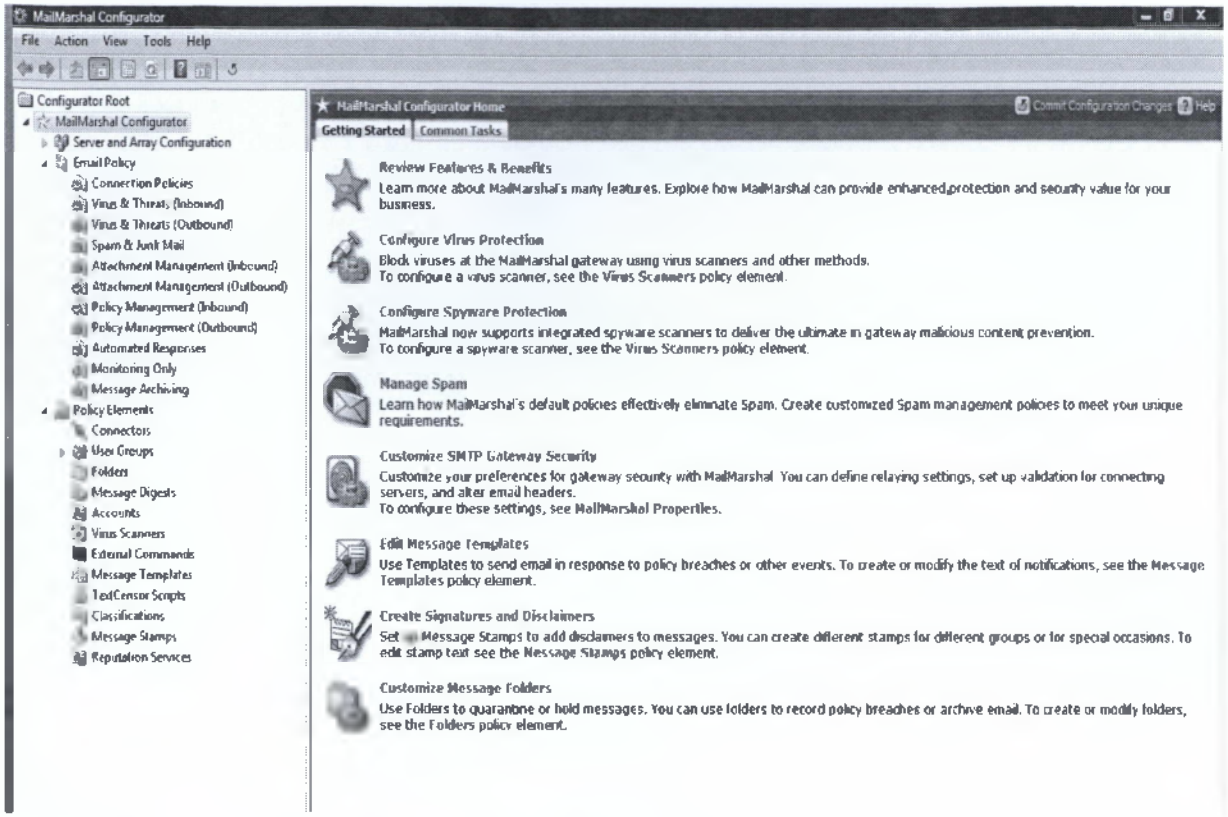
Χρήσιμα εκθέσεις ενημερώνουν για την αποτελεσματικότητα της ασφάλειας, όπως επίσης εντοπισμό απόπειρα παραβίασης της πολιτικής. Επιτρέπει στους διαχειριστές συστημάτων να αποδείξει την ταχεία απόδοση της επένδυσης στους ενδιαφερόμενους φορείς και στελέχη.

- Χαμηλό συνολικό κόστος της εγκατάστασης

Εύκολη εγκατάσταση, ελάχιστη διαχειριστική διοίκηση, η ενοποίηση όλων των λειτουργιών ασφαλείας του ηλεκτρονικού ταχυδρομείου σε ένα ενιαίο περιβάλλον διαχείρισης , anti-spam ενημερώσεις.

- Αποτρέπει την διαρροή των δεδομένων μέσω των πολιτικών πρόληψης

Επιτρέπει στους οργανισμούς να θέτουν περιορισμούς σχετικά με το ποιος μπορεί να στείλει εμπιστευτικές πληροφορίες μέσω του ηλεκτρονικού ταχυδρομείου και ποια δεδομένα μπορούν να σταλούν. Διασφαλίζει ότι οι ευαίσθητες επικοινωνίες προστατεύονται από αδιάκριτα μάτια. Παρέχει επίσης context-sensitive email αρχειοθέτηση, όπως η αποθήκευση όλων των μηνυμάτων σε ένα συγκεκριμένο θέμα.



- Παρέχει ολοκληρωμένο νομική προστασίας

Ακατάλληλο / προσβλητικό περιεχόμενο φιλτράρεται από τα εισερχόμενα και εξερχόμενα e-mail ελέγχονται αυτόματα για την τήρηση της ασφάλειας. Επιτρέπει στους οργανισμούς να αποδείξει ότι όλα τα εύλογα μέτρα για την προστασία των εργαζομένων και τη δίκαιη εφαρμογή των πολιτικών ασφαλείας χρησιμοποιούνται.

- Βελτιώνει την απόδοση δικτύων και εξοικονομεί της δαπάνες

Με τον έλεγχο της κατανάλωση το MailMarshal διατηρεί συνεπή και αξιόπιστη την απόδοση του δικτύου και παρεμποδίζει την υπερβολική μη επιχειρηματική χρήση του ηλεκτρονικού ταχυδρομείου.

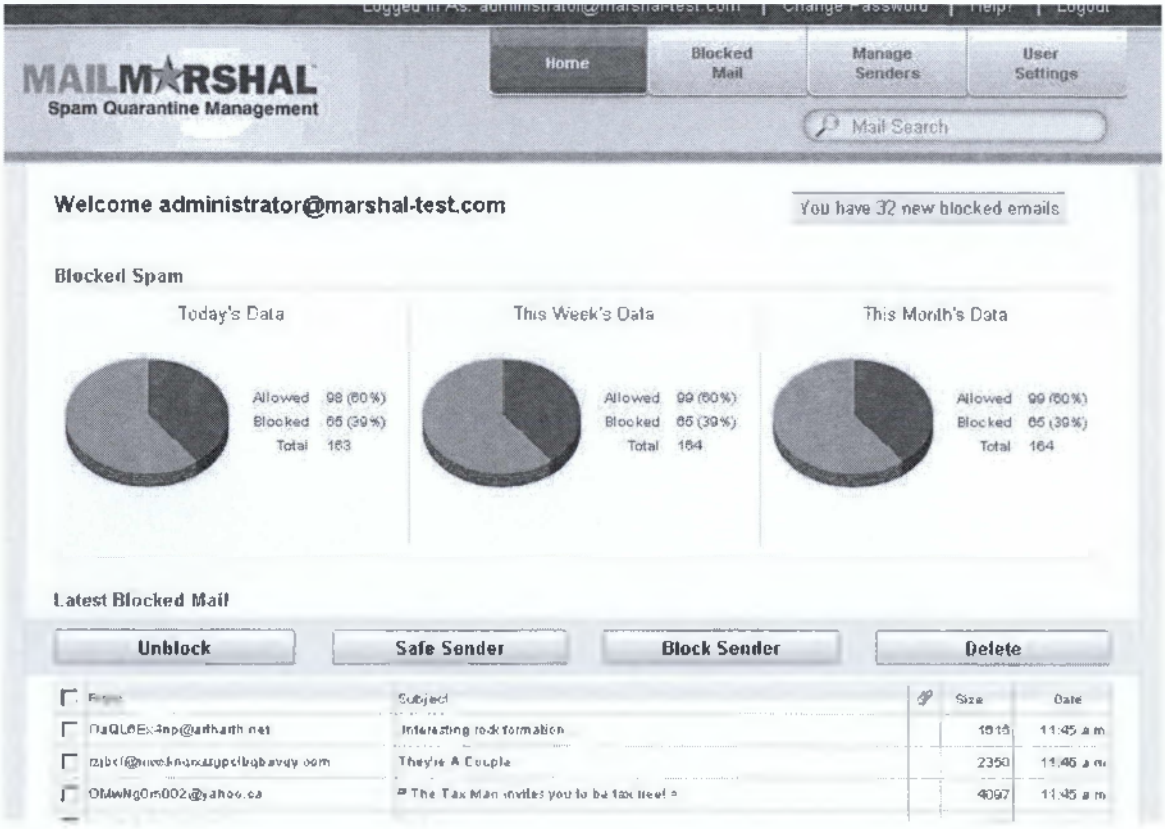
- Διασφαλίσει της εταιρίας και των εργαζομένων

Το MailMarshal εμποδίζει την παράνομη διανομή εμπιστευτικών ή ευαίσθητων πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου και διασφαλίζει ότι οι χρήστες δεν είναι σε θέση να φέρουν σε δύσκολη θέση την εταιρεία μέσα από τη διακίνηση ακατάλληλο περιεχόμενο ή προσβλητική συμπεριφορά. Μέσω της συνεχούς και σχολαστικής εφαρμογής της ασφάλειας και τις αποδεκτές πολιτικές χρήσης, θέματα όπως η σεξουαλική ή φυλετικής παρενόχληση μέσω του ηλεκτρονικού ταχυδρομείου μπορούν να προληφθούν.

➢ *Προστασία απο Spam & Phishing*

Η anti-spam μηχανή του MailMarshal συνδυάζει πρωτόκολλα και φίλτρα anti-spam για αξεπέραστη προστασία, απόδοση και ακρίβεια. Επιτυγχάνει σε ποσοστό 99,5% το ποσοστό την αλίευση ψευδούς θετικών δειγμάτων χωρίς ειδικές ρυθμίσεις. Δυναμικές anti-spam ενημερώσεις παρέχονται μέσω της *M86 Labs* υπηρεσίας ασφαλείας, καθώς και ενημέρωση κάθε 60 δευτερόλεπτα μαζί με την εβδομαδιαία ενημέρωση φίλτρου. Περιλαμβάνει επίσης την *Marshal IP Reputation Service*,, η οποία είναι μια υπηρεσία που μπορεί να απορρίψει πάνω από το 50% των

εισερχόμενων spam, επιτρέποντας σημαντική εξοικονόμηση bandwidth. Παρέχει την τεχνολογία *Automated Adaptive Whitelist* για την παρακολούθηση των e-mail των συνεργατών και εξασφαλίζει ότι τα μηνύματα που προέρχονται από αξιόπιστες πηγές δεν αποκλείονται ως spam. Επιβάλλει οποιαδήποτε πολιτική βασισμένο σε σχεδόν κάθε χαρακτηριστικό του μηνύματος.
Τα μηνύματα ελέγχονται με βάση:
• Ποιόν περιλαμβάνει το μήνυμα (αποστολέας, παραλήπτης, διεύθυνση IP)
• Τι περιέχει το μήνυμα (spam, malware, λέξεις-κλειδιά και φράσεις, το μέγεθος των μηνυμάτων, συνημμένα αρχεία, αλφαριθμητικά πρότυπα)
• Οι ενέργειες που θα θέλατε να πάρετε (μπλοκ, διαγραφή, καθυστέρηση, κρυπτογράφηση, αντίγραφο αρχείου, ειδοποίηση για μια διεύθυνση ηλεκτρονικού ταχυδρομείου, κατατάσει το μήνυμα για υποβολή εκθέσεων)

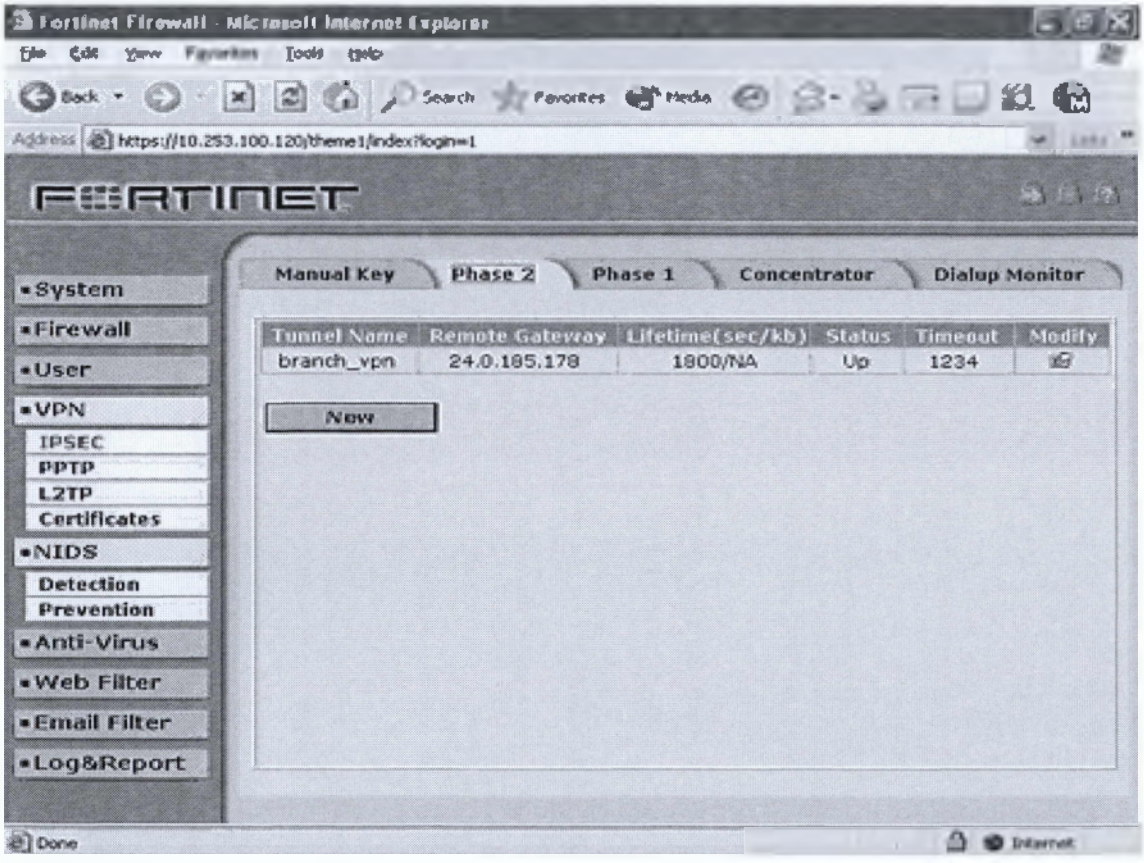


➢ *Προστασία απο Virus, Malware*

Παρέχει αδιάλειπτη ενσωματωμένη αντιοικη προστασία μέσω μιας σειράς απο υποστηρικτές, συμπεριλαμβανομένων της *McAfee, Norman, Sophos*, και *Symantec* και για αυτο το λόγο έχει ενσωμάτωμένο ειδικό anti-spyware ανιχνευτή, όπως των *CounterSpy* και *CA Anti-Malware* Ανιχνεύει και αποσυμπιέζει τύπους αρχείων, και εντοπίζει τους ιούς στα συνημμένα αρχεία. Προσδιορίζει και μπλοκάρει επικίνδυνους τύπους αρχείων από το περιεχόμενό τους και τον τύπο MIME. Τέλος παρέχει βαθιά ανάλυση του περιεχομένου του ηλεκτρονικού ταχυδρομείου όλων των στοιχείων για τον εντοπισμό και την απομόνωση μηνύματα που περιέχουν δυνητικά επιβλαβή κώδικα ή URL συνδέσμους με γνωστούς κακόβουλους δικτυακούς τόπους.

iii) Fortinet

Η τεχνολογία Fortinet antispam προσφέρει μια πληθώρα χαρακτηριστικών για την ανίχνευση, απομόνωση, και το μπλοκάρισμα των μηνυμάτων spam και κακόβουλων συνημμένων τους. Οι FortiGate, FortiWifi και FortiClient πλατφόρμες προσφέρουν ολοκληρωμένη antispam λειτουργικότητα ως μέρος των πολλαπλών επιπέδων προστασίας υποστηριζόμενη από το FortiGuard Antispam Service. FortiMail συσκευές συμπληρώσει αυτή τη λειτουργία με επιπλέον δυνατότητες που προσφέρει ακόμη πιο αποτελεσματικό φραγμό ενάντια του διαρκώς αυξανόμενου όγκου των spam, και παρέχουν μέγιστο επίπεδο προστασίας από τις επιθέσεις εξελιγμένων ηλεκτρονικών μηνυμάτων.

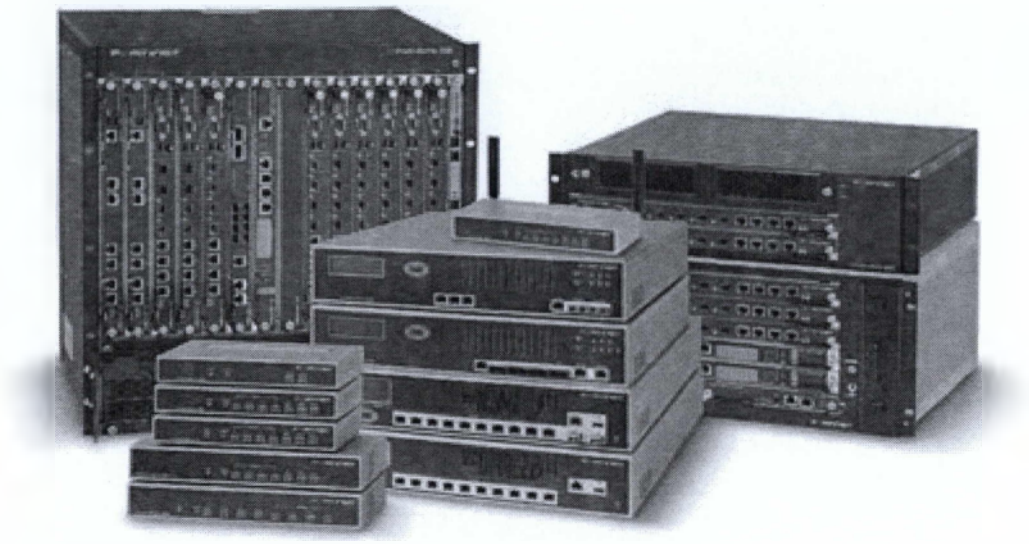


➢ *Οφέλη Fortinet Antispam Τεχνολογίας*

- ✓ Κλιμακούμενες λύσεις σχεδιασμένες για τις μικρές και πολλών gigabit δίκτυα.
- ✓ Δυνατότητες e-mail server για τη λειτουργικότητα SMB / SOHO εφαρμογών.
- ✓ Με βάση τις IP πολιτικές, ολιστική σάρωση εικόνας, και η κεντρική υπηρεσία FortiGuard συνδυάσει με διάφορες άλλες μεθόδους αναγνώρισης spam να παρέχει τα υψηλότερα επίπεδα της ακρίβειας, όπως πιστοποιείται από ICSA Labs.
- ✓ Το FortiClient επεκτείνει την antispam προστασίας σε απομακρυσμένους υπολογιστές desktop, φορητούς υπολογιστές, και smartphones που λειτουργούν εκτός της ζώνης του δικτύου.
- ✓ Διαθέσιμη κεντρική διαχείριση και υποβολή εκθέσεων, καθώς και ασφαλείς ζώνη όπως και γραφικά που παρέχουν πληροφορίες με τα χαρακτηριστικά

γνωρίσματα του συστήματος, μείωση του κεφαλαίου και των λειτουργικών δαπανών για την antispam προστασία

- ✓ Η παροχή ανά συσκευή απεριόριστη αδειών χρήσης απλοποιεί γενικά διοικητικά έξοδα και επιτρέπει στους οργανισμούς να επεκτείνουν την προστασία σε νέους χρήστες χωρίς να υποστεί πρόσθετες επιβαρύνσεις

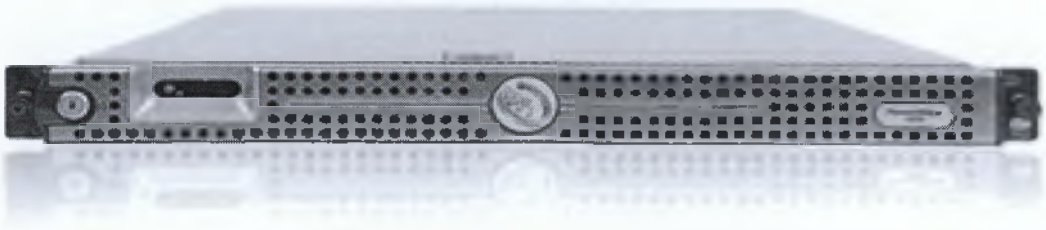


iv) MIME sweeper for SMTP

Το MIME sweeper για SMTP προσφέρει την ευελιξία να ορίζουν, να διαχειρίζονται και να εκτελούνται τα email με βάση την επικοινωνιακή δομή, χωρίς να τα επηρεάζει η οποία πολυπλοκότητα. Το εξαιρετικά ευέλικτο πλαίσιο πολιτικής που ενσωματώνει το περιεχόμενο του MIME sweeper καθώς και τα πολλαπλά στρώματα ασφάλειας εξασφαλίζει τον υψηλότερο βαθμό ασφάλειας των πληροφοριών των e-mail σας.

Η αρχιτεκτονική σχεδίαση ενθαρρύνει επίσης σημαντική εξοικονόμηση κόστους, δεδομένου ότι επιτρέπει την απλή ενοποίηση των πολλαπλών πυλών ηλεκτρονικού ταχυδρομείου και τομείς, σε συνδυασμό με την υψηλή επεκτασιμότητα. Πρόσθετα χαρακτηριστικά όπως η πολύ-γλωσσική υποστήριξη και πολλαπλών επιπέδων διοίκηση μπορεί εύκολα να φιλοξενήσει μεγάλες ομάδες επιχειρήσεων και να επιτρέπει με ασφάλεια την ταυτόχρονη διαχείριση του ηλεκτρονικού ταχυδρομείου σε πολλές περιοχές.

Επιπλέον το MIME sweeper για SMTP παρέχει CONTENT safe (πρόληψη απώλειας δεδομένων), EXCHANGE manager (εσωτερική ασφάλεια e-mail) και IMAGE manager (ασφάλεια εικόνας) για να προσφέρει την απόλυτη πλατφόρμα e-mail επικοινωνίας.

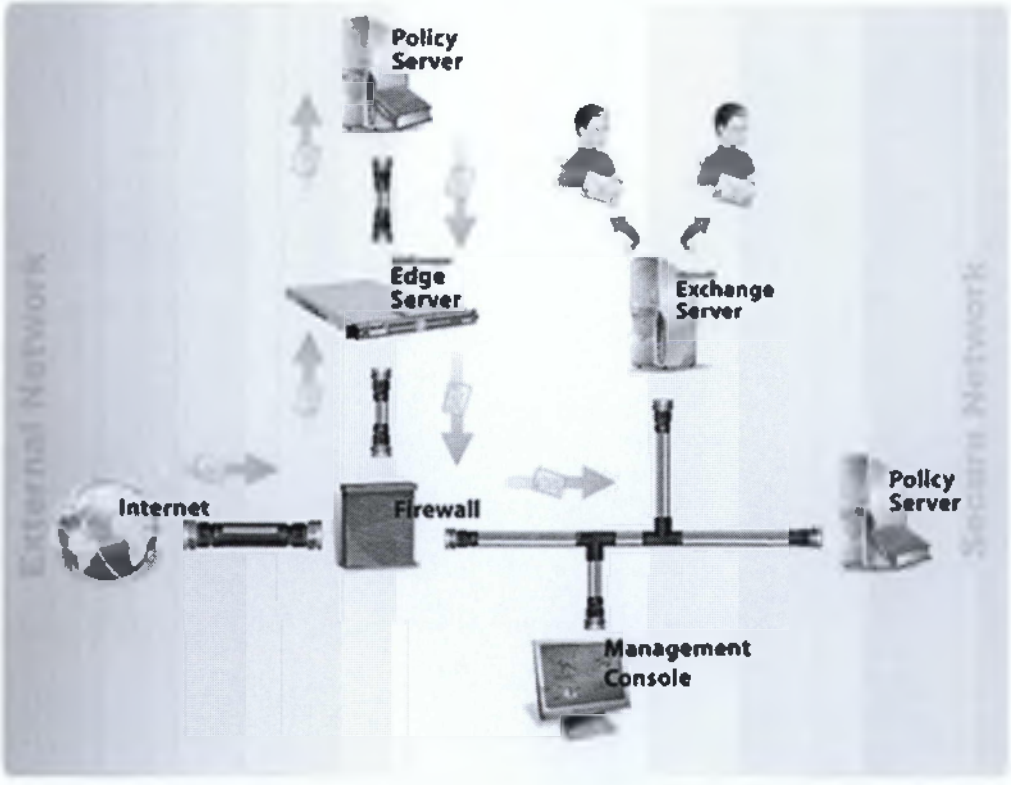


- *Χαρακτηριστικά και πλεονεκτήματα*

Καθορίζει τους κανόνες της πολιτικής και τα όρια, όπως απαιτείται από την υπηρεσία, ανάλογα με την τοποθεσία την ομάδα χρηστών των αποστολέα τον παραλήπτη τον τύπο του αρχείου το μέγεθος του αρχείου την ώρα την ημέρα. Η πολιτική εφαρμόζεται αυτόματα σύμφωνα με τις προδιαγραφές, περιλαμβάνοντας κλείδωμα, απομόνωση, προώθηση, διαγραφή, μετατροπή, αρχειοθέτηση και κρυπτογράφηση.

Επιπλέον περιλαμβάνει MS Exchange που διασφαλίζει ότι όλα τα εσωτερικά mail είναι σαρωμένα για τυχόν κακόβουλο λογισμικό ή για παραβιάσεις της πολιτικής (με EXCHANGE manager).

Επιλογή των anti-virus πωλητών όπως Kaspersky επιλογή για τον Edge-Server ή των εγκεκριμένων εκδόσεων του Authentium, Avira, Command, F-Secure, Norman, Sophos και της Symantec για την πολιτική ανάπτυξης Server.



Πλήρης κάλυψη των μηνυμάτων εξασφαλίζει τη μη απόκρυψη των αρχείων ή πληροφοριών. Περιλαμβάνει αναγνώριση φακέλων, αρχειοθέτηση, streaming media και εκατοντάδες άλλους παρόμοιους τύπους αρχείων ανάλογα με τη πηγή, τον τύπο και την κατανάλωση εύρους ζώνης. Άγνωστα αρχεία μπορεί να αποκλειστούν και στη συνέχεια να μπουν σε καραντίνα ή να διαγραφούν, σύμφωνα με την πολιτική ασφάλειας.

Αυτόματη ενημέρωση για τη διαχείριση των καταλόγων των πολύγλωσσων βωμολοχιών και επεξεργάσιμο λεξικά συμμόρφωσης (Gramm Leach Bliley Act (GLBA), Health Insurance Portability και Accountability Act (HIPAA).

Ενσωματωμένο με CONTENT safe για την προληπτική προστασία και τον εντοπισμό των ευαίσθητων πληροφοριών.

Ο Edge-Server ενημερώνεται αυτόματα σε διαστήματα 15 λεπτών εξασφαλίζοντας τη βέλτιστη ασφάλεια.

Περιεκτικά back-up και δυνατότητα επαναφοράς στην περίπτωση αποτυχίες του server ή του συστήματος.

Παρέχονται εύκολα προσαρμοσμένα πρότυπα αναφοράς. Επιλέξτε τη συχνότητα έκθεσης και του καταλόγου κυκλοφορίας για εύκολη αποστολή σε ανθρώπινο δυναμικό, επικεφαλής υπηρεσιών.

Η αρχιτεκτονική του επιτρέπει περισσότερους από 100.000 χρήστες και το καθιστά εύκολο να διαχειρίζεται πολλαπλές πύλες ηλεκτρονικού ταχυδρομείου.

Υποστηρίζει Windows 2003 και Windows Server 2008, είτε με ειδικό υλικό ή σε ένα VMware ESX / ESXi εικονικό περιβάλλον.

ΚΕΦΑΛΑΙΟ 2

ΠΡΩΤΟΚΟΛΛΑ ΠΑΡΑΛΗΨΕΙΣ – ΕΛΗΨΕΙΣ

2.1 Post Office Protocol (POP)

Το **Post Office Protocol (POP),** επίσης γνωστό και ως **POP3** είναι ένα πρωτόκολλο που χρησιμοποιείται για την παραλαβή των ηλεκτρονικών μηνυμάτων (email) από έναν απομακρυσμένο εξυπηρετητή (server) χρησιμοποιώντας σύνδεση TCP/IP.

Η μεταφορά αυτή γίνεται από ένα άλλο πρόγραμμα που υποστηρίζει το πρωτόκολλο POP3 το οποίο ονομάζεται **POP3 server**. Πάλι ο χρήστης χρειάζεται έναν **Mail client** που να διαθέτει το πρωτόκολλο POP3 για να επικοινωνήσει με τον POP3 server που διαχειρίζεται την εισερχόμενη αλληλογραφία του.

Όταν συνδεθεί ο χρήστης και ζητήσει από τον POP3 client να μεταφέρει τα εισερχόμενα μηνύματά του ο client συνδέεται με τον POP3 server και μεταφέρει τα μηνύματα που υπάρχουν στο γραμματοκιβώτιό του, στο δίσκο του υπολογιστή του χρήστη. Οι POP3 clients μεταφέρουν όλα τα μηνύματα του χρήστη χωρίς να υπάρχει η δυνατότητα ανάγνωσης συγκεκριμένων μόνο μηνυμάτων. Μετά την ανάγνωση των μηνυμάτων αυτά διαγράφονται από το γραμματοκιβώτιο του **Mail server**.

Ορισμένοι clients μπορούν να διαβάσουν την εισερχόμενη αλληλογραφία του χρήστη χωρίς να διαγράψουν τα μηνύματα από τον server.

Για ανάγνωση μηνυμάτων που έχουμε λάβει στη θυρίδα μας μπορούμε να χρησιμοποιούμε το πρωτόκολλο POP3 με δυνατότητα χρήσης SSL. Αυτό επιτυγχάνεται μέσο σύνδεσης με τον διακομιστεί **pop3.isc.tuc.gr** και της ταυτόχρονης ενεργοποίησης της δυνατότητας χρήσης ασφαλούς σύνδεσης SSL μέσο του port (θύρα) **995 TCP**.

Το POP3 αποτελεί εξέλιξη των προηγούμενων μορφών του πρωτοκόλλου, τα οποία ονομαζόταν ανεπίσημα POP1 και POP2. Ο όρος Post Office Protocol είναι πλέον συνώνυμος με το POP3, καθώς οι προηγούμενες μορφές του πρωτοκόλλου έχουν πλέον καταργηθεί στην πράξη.

Το POP3 είναι σχεδιασμένο με τέτοιον τρόπο ούτως ώστε να επιτρέπει στους χρήστες του διαδικτύου που έχουν προσωρινές συνδέσεις (πχ dial-up) να παραλαμβάνουν την ηλεκτρονική τους αλληλογραφία, να την αποθηκεύουν στον τοπικό σκληρό δίσκο και στην συνέχεια να την διαβάζουν χωρίς να χρειάζεται να παραμένουν συνδεδεμένοι στο διαδίκτυο. Παρόλο που υπάρχει η δυνατότητα τα μηνύματα να παραμείνουν στον server ηλεκτρονικού ταχυδρομείου, οι περισσότερες εφαρμογές POP3 συνδέονται με τον server, λαμβάνουν όλα τα ηλεκτρονικά μηνύματα, τα αποθηκεύουν στον υπολογιστή του χρήστη, τα σβήνουν από τον server και αποσυνδέονται.

Σε αντίθεση με το POP3, το πρωτόκολλο **Internet Message Access Protocol (IMAP)** που εμφανίστηκε αργότερα υποστηρίζει τόσο την online όσο και την offline ανάγνωση μηνυμάτων. Επίσης αφήνει τα μηνύματα στον server έως ότου ο χρήστης αποφασίσει να τα διαγράψει. Η τακτική αυτή δίνει την δυνατότητα σε έναν χρήστη να διαβάζει τα email του από διάφορους υπολογιστές. Αντίθετα, το POP3 επιτρέπει την ανάγνωση των email μονάχα από τον υπολογιστή στον οποίο έχουν κατέβει.

Τα περισσότερα προγράμματα διαχείρισης ηλεκτρονικής αλληλογραφίας (Mozilla Thunderbird, Microsoft Outlook κοκ) υποστηρίζουν και τα δύο πρωτόκολλα και δίνουν στον χρήστη την δυνατότητα να επιλέξει ποιό ταιριάζει καλύτερα στις ανάγκες του. Παρόλα αυτά όμως, το πρωτόκολλο IMAP υποστηρίζεται από λιγότερους servers σε σχέση με το πρωτόκολλο POP3.

Το POP3 χρησιμοποιεί την πόρτα 110 για να εγκαθιδρύσει μία σύνδεση TCP με τον mail server. Πολλά προγράμματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν κρυπτογράφηση ούτως ώστε τα δεδομένα που διακινούνται στην σύνδεση αυτή να

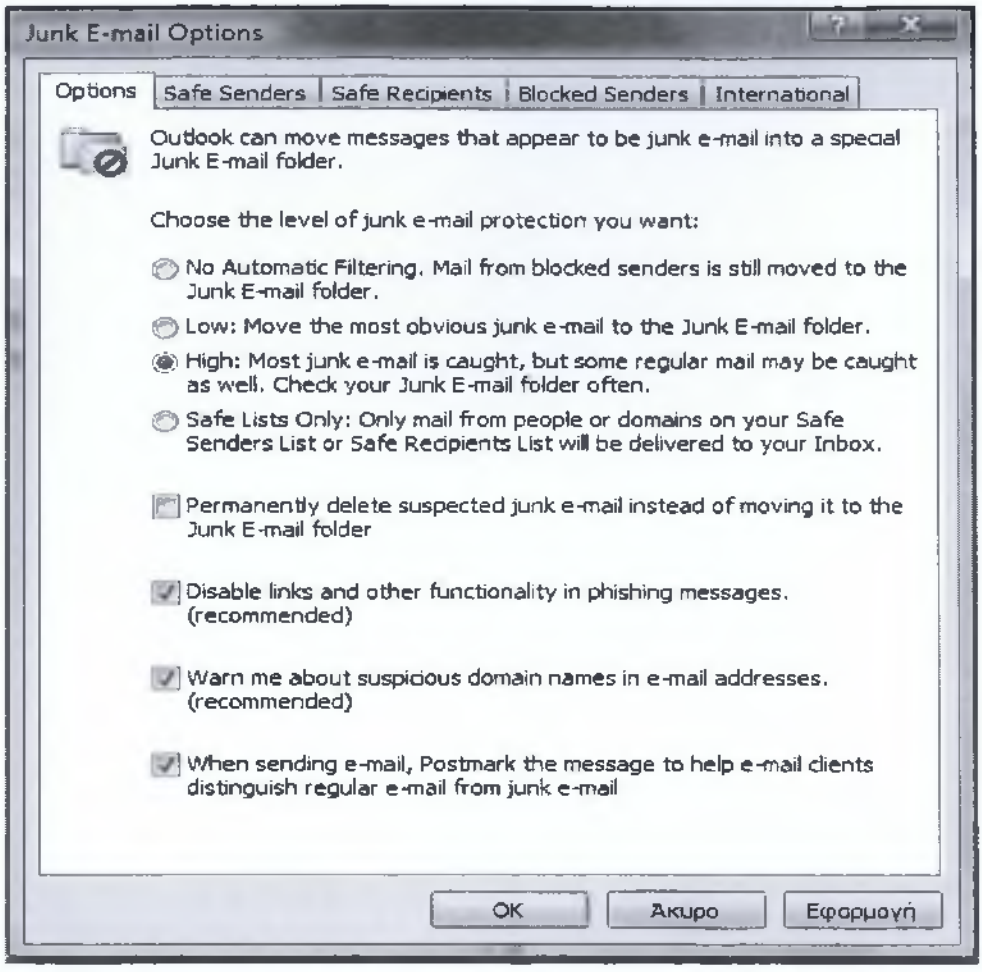
μην είναι αναγνώσιμα από άλλους. Για να αποδεχθεί ο mail server την σύνδεση, θα πρέπει ο χρήστης να δώσει το όνομα χρήστη και τον κωδικό πρόσβασής του.

Η αρχική έκδοση του POP3 μετέδιδε τα ευαίσθητα αυτά δεδομένα σε μορφή απλού κειμένου, οπότε οποιοσδήποτε μπορούσε να τα διαβάσει. Στην συνέχεια όμως το πρωτόκολλο βελτιώθηκε και πλέον παρέχει την δυνατότητα κρυπτογραφημένης μετάδοσης του ονόματος χρήστη και του κωδικού. Παρόλα αυτά όμως, πολλοί χρήστες δεν γνωρίζουν αυτήν την δυνατότητα και συνεπώς δεν την χρησιμοποιούν.

2.1.2 POP3 – Outlook ρυθμίσεις

Η φυσική αποθήκευση μηνυμάτων στο outlook , είναι μια επιλογή από χρήστες που θέλουν να αποφύγουν την συνεχή ταλαιπωρία επίσκεψης του webmail interface σε κάποια ιστοσελίδα για να δουν και να διαχειριστούν τα μηνύματα τους. Σε αυτή την περίπτωση , μαζί με τα μηνύματα που θέλει ο χρήστης, είναι αναπόφευκτο να έρθουν και τα spam , αφού η υπηρεσία spam filter είναι πάντα συνδεδεμένη με το mailbox του χρήστη και δεν γίνεται εντός του POP3 Server. Ο τρόπος αντιμετώπισης εδώ διαφέρει , ανάλογα με την σουίτα email client που χρησιμοποιεί ο χρήστης (outlook express, MS outlook, thunderbird κτλ.) Μπορεί να γίνει είτε μέσω κάποιου τρίτου προγράμματος που θα το ρυθμίσει ο χρήστης , σύμφωνα με τις οδηγίες , είτε μέσω των κανόνων junk/spam (π.χ. MS Outlook) για το φιλτράρισμα των εισερχομένων

Στον email client MS outlook , οι κανόνες του Junk filter, βρίσκονται στην διαδρομή: στο toolbar του client > actions>junk email>junk email options όπου και μια πολύ καλή ρύθμιση είναι να μπει στο "High" και μαζί με αυτό να ενεργοποιηθούν οι επιλογές «Disable links and other functionalities in phishing messages." , "Warn me about suspicious domains in email addresses" και τελευταία την επιλογή "postmark the message…" Ο λόγος που ενεργοποιούνται αυτές οι επιλογές είναι στο πρώτο για προστασία από Phishing messages, για ενημέρωση πιθανού ψεύτικου ή πλαστού domain και η τελευταία για να μην απορρίπτονται εύκολα τα δικά σας μηνύματα σαν spam καθώς θα περιέχουν ειδική σήμανση από το mailbox σας για ταυτοποίηση



2.1.3 Τα μειονεκτήματα του POP3 σε σύγκριση με το IMAP

Το POP δημιουργήθηκε για την επεξεργασία των μηνυμάτων τοπικά. Στο πρότυπο αυτό, ο χρήστης ελέγχει ανά χρονικά διαστήματα το mailbox του για νέα μηνύματα, τα οποία αν υπάρχουν κατεβαίνουν στο σύνολο του μεγέθους τους στον υπολογιστή του. Από εκεί και πέρα η επεξεργασία είναι τοπική, δηλαδή ότι Replies, Forwards, Moves κλπ. γίνουν, αποθηκεύονται ως ενέργειες τοπικά στον συγκεκριμένο υπολογιστή. Είναι προφανής λοιπόν η αδυναμία του πρωτοκόλλου να δώσει στο χρήστη τη δυνατότητα να ελέγξει ποια μηνύματα θα κατεβάσει, καθώς και να διατηρήσει το ιστορικό των ενεργειών του, κατά την πιθανή του μετάβαση σε άλλον υπολογιστή. Αν και υπάρχει η δυνατότητα για κατακράτηση αντιγράφων, αυτή κρίνεται στο σύνολο της ως μη λειτουργική σε σύγκριση με την αντίστοιχη του πρωτοκόλλου IMAP.

Αντίθετα στο πρωτόκολλο IMAP η επεξεργασία των μηνυμάτων γίνεται, κατά βάση, απ' ευθείας στο mailserver. Υπάρχει δηλαδή συνεχής αλληλεπίδραση μεταξύ του υπολογιστή του χρήστη και του mailserver κατά την επεξεργασία των μηνυμάτων, που έχει σαν αποτέλεσμα την διατήρηση του ιστορικού των ενεργειών σε ένα κεντρικό σημείο για να είναι διαθέσιμο από παντού. Αυτό δεν σημαίνει βέβαια ότι το IMAP αδυνατεί να λειτουργήσει όταν ο χρήστης είναι offline: ο χρήστης μπορεί να προβεί σε τοπική επεξεργασία και να συγχρονίσει την τοπική κατάσταση του λογαριασμού του με το mailserver, την επόμενη φορά που θα είναι σε σύνδεση με το δίκτυο. Όλα αυτά βέβαια, εξαρτώνται σε μεγάλο βαθμό και από τις ρυθμίσεις που

έχουν γίνει στο τοπικό πρόγραμμα mail του χρήστη.
Λόγω λοιπόν της φύσης του πρωτοκόλλου, που στην ουσία χρησιμοποιεί τον "απομακρυσμένο" λογαριασμό του χρήστη σαν να είναι τοπικός, προκύπτουν μια σειρά από δυνατότητες που δεν καλύπτονται απ' το πρωτόκολλο POP:

- Προεπισκόπηση Μηνυμάτων.
  Χρήσιμο σε συνδέσεις περιορισμένου bandwidth, όπως το dialup, όπου ο χρήστης έχει τη δυνατότητα να επιλέξει τι θα κατεβάσει.

- Διατήρηση ιστορικού ενεργειών στο λογαριασμό
  Δυνατότητα χρήσης του λογαριασμού από διαφορετικούς υπολογιστές ή HTTP clients (my.ntua.gr) με πλήρη συγχρονισμό.

- Μεταφορά τοπικών μηνυμάτων, αρχείων, usenet news, ή μηνυμάτων από άλλους λογαριασμούς στο mailbox του χρήστη.
  Δυνατότητα μελλοντικής επεξεργασίας από οπουδήποτε, με οποιονδήποτε υπολογιστή.

- Δημιουργία και δυνατότητα χρήσης πολλαπλών mailboxes
  Κατηγοριοποίηση μηνυμάτων, συνεργασία με server-side φίλτρα, όπως αυτά που παρέχονται από τις υπηρεσίες διαχείρισης λογαριασμού.

- Υποστήριξη ταυτόχρονης χρήσης κοινών λογαριασμών
  Πλήρης υποστήριξη σε λογαριασμούς που πρέπει να παρακολουθούνται ταυτόχρονα από πολλά άτομα.

2.2 Simple Mail Transfer Protocol (SMTP)

Το πρωτόκολλο **SMTP (Simple Mail Transfer Protocol = Πρωτόκολλο μεταφοράς απλού ταχυδρομείου)** αποτελεί το βασικό πρωτόκολλο του ηλεκτρονικού ταχυδρομείου του Internet. Με αυτό γίνεται όλη η μεταφορά των μηνυμάτων μεταξύ των διαφόρων υπολογιστών του Internet. Τόσο ο υπολογιστής που στέλνει μηνύματα όσο και ο υπολογιστής που τα λαμβάνει πρέπει να τρέχει **SMTP**.
Για να στείλει ένας χρήστης ένα μήνυμα χρησιμοποιεί έναν **mail client** δηλαδή ένα πρόγραμμα όπως π.χ ο Communicator της Netscape, ο Explorer της Microsoft, το Eudora, το οποίο δίνει τη δυνατότητα στον χρήστη με τη βοήθεια εντολών να συντάξει το μήνυμά του και στη συνέχεια να το στείλει.
Όταν ο **client** πάρει την εντολή από τον χρήστη να στείλει το μήνυμα συνδέεται με τον **Mail server** του τοπικού δικτύου (τον υπολογιστή που έχει διαμορφωθεί ώστε να χειρίζεται την αλληλογραφία των χρηστών του δικτύου) και του στέλνει το μήνυμα. Ο **Mail server** φροντίζει από εκεί και πέρα για την αποστολή του μηνύματος στον τελικό παραλήπτη του μηνύματος. Το μήνυμα δεν φθάνει κατ' ευθείαν στον υπολογιστή του παραλήπτη αλλά στον **Mail server** του τοπικού δικτύου του παραλήπτη, ο οποίος το τοποθετεί στο γραμματοκιβώτιο του χρήστη και παραμένει εκεί έως ότου ο παραλήπτης παραλάβει το ταχυδρομείο του.
Όλα τα προγράμματα ηλεκτρονικής αλληλογραφίας (πχ Mozilla Thunderbird, Microsoft Outlook κ.α.) θα πρέπει να ρυθμιστούν κατάλληλα από τον χρήστη για να λειτουργήσουν σωστά.

Συγκεκριμένα ο χρήστης θα πρέπει να καθορίσει τον SMTP server που θα χρησιμοποιήσει για να στείλει και να παραλάβει ηλεκτρονική αλληλογραφία. Με τον τρόπο αυτό μπορεί για παράδειγμα ένας χρήστης να ανταλλάξει ηλεκτρονικά μηνύματα χωρίς να είναι συνδεδεμένος στο διαδίκτυο, εάν χρησιμοποιεί έναν τοπικό SMTP server.

Οι SMTP servers θα πρέπει να έχουν ανοιχτή μία τουλάχιστον από τις πόρτες 25 και 587, ούτως ώστε να μπορούν να επικοινωνήσουν με άλλους SMTP servers για την αποστολή ή παραλαβή ηλεκτρονικών μηνυμάτων. Πολλοί SMTP servers χρησιμοποιούν και τις δύο πόρτες για λόγους συμβατότητας.

Μία τυπική παραλαβή ηλεκτρονικού μηνύματος από έναν SMTP server έχει ως εξής: Αρχικά δημιουργείται μία σύνδεση μεταξύ του SMTP server που έχει τον ρόλο του αποστολέα και του SMTP Server που έχει τον ρόλο του παραλήπτη. Στην συνέχεια οι δύο SMTP servers "συνομιλούν" ούτως ώστε να επιτευχθεί χωρίς προβλήματα η ανταλλαγή του μηνύματος. Στην συνέχεια παρατίθεται ως παράδειγμα μία υποτυπώδης συνομιλία μεταξύ του αποστολέα (Α) και του παραλήπτη (Π) του μηνύματος.

Η παραπάνω εντολή δημιουργεί μία TCP σύνδεση από τον αποστολέα προς τον παραλήπτη (www.example.com) στην πόρτα 25. Αφού γίνει η σύνδεση, ακολουθεί η εξής συνομιλία μεταξύ των δύο υπολογιστών:

Π: 220 www.example.com ESMTP Postfix
Α: HELO mydomain.com
Π: 250 Hello mydomain.com
Α: MAIL FROM:<sender@mydomain.com>
Π: 250 Ok
Α: RCPT TO:<friend@example.com>
Π: 250 Ok
Α: DATA
Π: 354 End data with <CR><LF>.<CR><LF>
Α: Subject: test message
Α: From: sender@mydomain.com
Α: To: friend@example.com
Α:
Α: Hello,
Α: This is a test.
Α: Goodbye.
Α: .
Π: 250 Ok: queued as 12345
Α: QUIT
Π: 221 Bye

Ουσιαστικά η παραπάνω συνομιλία χρησιμοποιείται για να στείλει το ακόλουθο μήνυμα από τον SMTP Server mydomain.com (ηλεκτρονική διεύθυνση sender@mydomain.com) στον SMTP Server example.com (ηλεκτρονική διεύθυνση friend@example.com):

Hello,
This is a test.
Goodbye.

Υπάρχουν φυσικά και αρκετές άλλες επιλογές στην συνομιλία, οι οποίες δεν παρουσιάζονται στο παραπάνω παράδειγμα. Ενδεικτικά αξίζει να αναφερθεί η λέξη SIZE που χρησιμοποιείται από τον αποστολέα για να μάθει το μέγιστο μέγεθος μηνύματος που μπορεί να παραλάβει ο παραλήπτης. Επίσης η λέξη EHLO (αναγραμματισμένο HELO) χρησιμοποιείται αντί της HALLO στην παραπάνω συνομιλία για να ξεκινήσει μία σύνοδο Extended SMTP (ESMTP) αντί για μία σύνοδο απλού SMTP. Παρακάτω φαίνεται ένα παράδειγμα όπου χρησιμοποιούνται οι δύο προαναφερθείσες επιλογές.

Π: 220-serverdomain.com ESMTP {postfix version and date}
Π: 220 NO UCE. {etc., terms of service}
A: EHLO mydomain.com
Π: 250-serverdomain.com Hello mydomain.com [127.0.0.1]
Π: 250-SIZE 14680064
Π: 250-PIPELINING
Π: 250 HELP

Στο παράδειγμα αυτό ο SMTP Server serverdomain.com (Παραλήπτης) χρησιμοποιεί την λέξη SIZE για να ενημερώσει τον SMTP Server mydomain.com (Αποστολέας) ότι δεν πρόκειται να δεχθεί μηνύματα το μέγεθος των οποίων υπερβαίνει κάποια προκαθορισμένη τιμή. Στην συγκεκριμένη τιμή το μέγεθος αυτό είναι 14,680,064 bytes ή 14 MB. Εάν το μήνυμα που προσπαθεί να μεταδώσει ο αποστολέας είναι μεγαλύτερο από 14MB, τότε δεν θα γίνει αποδεκτό και η μετάδοση θα αποτύχει.

2.2.1 Πρόβλημα ασφαλείας SMTP

Το πρόβλημα ασφαλείας οφείλεται στα εξής: Τα SMTP πακέτα είναι ευαίσθητα σε **sniffing** και **μη κρυπτογραφημένα**. Εργαλεία του είδους είναι διαθέσιμα στο Διαδίκτυο και μάλιστα οποιοσδήποτε μπορεί να τα βρει σχετικά εύκολα. Βασική λειτουργία των sniffers είναι η υποκλοπή των πακέτων που διέρχονται από έναν κόμβο του δικτύου. Πολλά εργαλεία του είδους είναι ικανά να υποκλέπτουν πακέτα των περισσότερων δικτυακών πρωτοκόλλων, συμπεριλαμβανομένων των SMTP, POP και IMAP.

Έτσι, ένας "αδιάκριτος" χρήστης μπορεί να υποκλέψει την ηλεκτρονική αλληλογραφία, χρησιμοποιώντας ένα πρόγραμμα για «sniffing». Συνεπώς ο υποκλοπέας μπορεί να αντλήσει πληροφορίες σχετικά με το περιεχόμενο των μηνυμάτων ηλεκτρονικού ταχυδρομείου που απέστειλε ή έλαβε ο ανύποπτος χρήστης, καθώς και τον κωδικό πρόσβασης που χρησιμοποιεί για την πρόσβαση στον εξυπηρέτητη ηλεκτρονικού ταχυδρομείου, όπως επίσης και τη δυνατότητα χρήσης password για αποστολή με «κλεμμένο» account => πλαστοπροσωπία

Η **εμπιστευτικότητα** χρησιμεύει στη προστασία του μηνύματος από μη εξουσιοδοτημένους χρήστες. Επιτυγχάνεται με κρυπτογράφηση των μηνυμάτων με συμμετρικούς ή ασύμμετρους αλγορίθμους

Η **πιστοποίηση της πηγής** ενός μηνύματος επιτυγχάνετε με τον καθορισμός του αποστολέα του μηνύματος και γίνεται με χρήση ψηφιακών υπογραφών. Είναι, αυστηρά προσωπικές, μοναδικές και είναι δύσκολη η πλαστογράφησή τους. Η χρήση τους επιτρέπει την επιβεβαίωση της αυθεντικότητας του μηνύματος. Ωστόσο ακόμα και αν το περιεχόμενο του μηνύματος δεν μπορεί να αλλοιωθεί, τα πεδία Date και Subject στην επικεφαλίδα του μηνύματος παραμένουν ευάλωτα

Η **ψηφιακή υπογραφή και η κρυπτογράφηση** μπορούν να συνδυασθούν με τρεις τρόπους, 1. τη κωδικοποίηση του περιεχομένου του μηνύματος και στη συνέχεια υπογραφή του, 2. την υπογραφή του κειμένου και κρυπτογράφηση μόνο του περιεχομένου, και 3. την υπογραφή του κειμένου και κρυπτογράφηση τόσο του περιεχομένου όσο και της ψηφιακής του υπογραφής. Αξίζει να σημειωθεί ότι μόνο η τρίτη μέθοδος παρέχει λύση στο πρόβλημα της πατρότητας του μηνύματος προστατεύοντας ταυτόχρονα και το πηγαίο κείμενο και την ψηφιακή υπογραφή.

Η **ακεραιότητα περιεχομένου** διασφαλίζει ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί, σχετίζεται άμεσα με την πιστοποίηση ταυτότητας του αποστολέα, δεν έχει ιδιαίτερη αξία η διατήρηση της ακεραιότητας του περιεχομένου αν ταυτόχρονα δεν έχει πιστοποιηθεί η ταυτότητα του αποστολέα, όπως δεν έχει αξία και η πιστοποίηση της ταυτότητας του αποστολέα αν δε μπορεί να διατηρηθεί η ακεραιότητα του κειμένου.

Η **μη απόρριψη υποχρέωσης ή οφειλής**, με αυτόν τον τρόπο ο παραλήπτης μπορεί να αποδείξει την αποστολή του μηνύματος από τον αποστολέα ακόμα και αν ο αποστολέας του αρνείται ότι το έχει στείλει.

2.3 *S/MIME Πρωτόκολλο*

Το S/MIME είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλοντα μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων. Η δεύτερη έκδοση του S/MIME είναι επί του παρόντος ενσωματωμένη σε πολλά δημοφιλή προϊόντα, όπως τα *Lotus Domino, Netscape Communicator, Novell GroupWise* και *Microsoft Exchange*. Το S/MIME δίνει την δυνατότητα σε εταιρίες που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.

Η ομάδα *Internet Engineering Task Force (IETF)* αναπτύσσει την 3η έκδοση του S/MIME που περιλαμβάνει την εξειδίκευση *Cryptographic Message Syntax (CMS)* που ορίζει μια τυποποιημένη σύνταξη για την επικοινωνία των κρυπτογραφικών πληροφοριών που είναι ανεξάρτητες από την μορφή των ενθυλακωμένων περιεχομένων ή από τον μηχανισμό μεταφοράς. Κάθε τύπος δεδομένων μπορεί να προστατευθεί από το CMS. Εκτός από τις εφαρμογές S/MIME, το CMS μπορεί να χρησιμοποιηθεί με τα πρωτόκολλα HTTP, X.400, FTP, SSL και SET. Η στρατηγική ανάπτυξης της τρίτης έκδοσης είναι τέτοια ώστε να διατηρείται η συμβατότητα με την προηγούμενη έκδοση (version 2). Αυτό επιτυγχάνεται με την πρόσθεση νέων, προαιρετικών στοιχείων στην νέα έκδοση, των οποίων η απουσία στις επικεφαλίδες επιτρέπει την συνεργασία των δύο εκδόσεων.

Επίσης, η έκδοση 3 του S/MIME απαιτεί την ύπαρξη ενός ελάχιστου συνόλου κρυπτογραφικών αλγορίθμων που διασφαλίζουν την συνεργασίας μεταξύ διαφορετικών εφαρμογών.

Η περιγραφή του S/MIME v3, που αναπτύχθηκε από την ομάδα IETF περιλαμβάνει τα εξής έγγραφα:

- *Cryptographic Message Syntax (CMS)*: Όπως προείπαμε, το CMS ορίζει ένα τυποποιημένο τρόπο σύνταξης για την ανταλλαγή κρυπτογραφικών πληροφοριών που σχετίζονται με τα προστατευμένα περιεχόμενα. Το CMS βασίζεται στο PKCS #7 Version 1.5 που χρησιμοποιείται στα τρέχοντα

προϊόντα S/MIME. στο τελευταίο έχουν ενσωματωθεί προαιρετικά χαρακτηριστικά ασφάλειας όπως η ακεραιότητα δεδομένων (integrity), η πιστοποίηση ταυτότητας (authentication), η εξασφάλιση της μη αποκήρυξης της προέλευσης (non- repudiation of origin) και της διασφάλισης του απόρρητου (privacy)

- *S/MIME Version 3 Message Specification*: Ορίζει την MIME κωδικοποίηση που χρησιμοποιείται για την μεταφορά περιεχομένων προστατευμένων από το CMS. Συγκεκριμένα, καθορίζει τις διάφορες επιλογές για την ενθυλάκωση αυτών των περιεχομένων στα MIME μηνύματα και προστίθενται οι νέοι τύποι περιεχομένων multipart/signed και application/pkcs7-siganture. Όλα τα προγράμματα με εφαρμοσμένο το S/MIME πρέπει να συμμορφώνονται με αυτό το έγγραφο.

- *S/MIME Version 3 Certificate Handling System*: Υποχρεώνει την υποστήριξη των πιστοποιητικών X.509, που μαζί με τις Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists) χρησιμοποιούνται για την πιστοποίηση ταυτότητας και την διαχείριση κλείδων.

- *Enhanced Security Services*: Το έγγραφο αυτό περιγράφει προαιρετικές υπηρεσίες ασφάλειας που μπορούν να παρέχονται σε συνδυασμό με την CMS προστασία. Οι προβλεπόμενες προαιρετικές υπηρεσίας είναι:

1. *Υπογεγραμμένες αποδείξεις (Signed Receipts): παρέχει αυθεντικές αποδείξεις παραλαβής μηνυμάτων.*
2. *Ετικέτες Ασφαλείας (Security Labels): παρέχει την δυνατότητα ιεράρχησης των επιπέδων ασφάλειας, συνδέοντας τα δεδομένα με ετικέτες ευαισθησίας.*
3. *Ταχυδρομικές Λίστες (Mail Lists): επιτρέπει στις ταχυδρομικές λίστες να διαχειρίζονται ασφαλισμένα μηνύματα.*
4. *Υπογεγραμμένα Πιστοποιητικά (Signing Certificates): εξασφαλίζει την αυθεντικότητα των πιστοποιητικών.*

2.3.1 Δημιουργία S/MIME μηνυμάτων

Τα μηνύματα S/MIME είναι συνδυασμός MIME μηνυμάτων και CMS αντικειμένων. Τα CMS αντικείμενα περιγράφουν το είδος της ασφάλειας που θέλουμε να εφαρμόσουμε και μπορεί να είναι Ψηφιακός Φάκελος (Enveloped- Data), Υπογεγραμμένα δεδομένα (Signed- Data) και άλλα. Μπορούν να χρησιμοποιηθούν όλοι οι τύποι δεδομένων του MIME, χωρίς κανένα περιορισμό. Το MIME μήνυμα, μαζί με άλλες πληροφορίες (πιστοποιητικά, αναγνωριστικά αλγόριθμων κ.α.), επεξεργάζονται από τις διαδικασίες του CMS και παράγεται το CMS αντικείμενο. Τέλος, το CMS αντικείμενο τυλίγεται σε εξωτερικό MIME μήνυμα με κατάλληλες επικεφαλίδες.

Προετοιμασία

Η MIME οντότητα που θα ασφαλιστεί από το S/MIME μπορεί να είναι είτε μέρος ενός μηνύματος, είτε ολόκληρο μήνυμα. Σε περίπτωση που η MIME οντότητα ισοδυναμεί με ολόκληρό το μήνυμα, περιλαμβάνονται σ' αυτήν όλες τις MIME

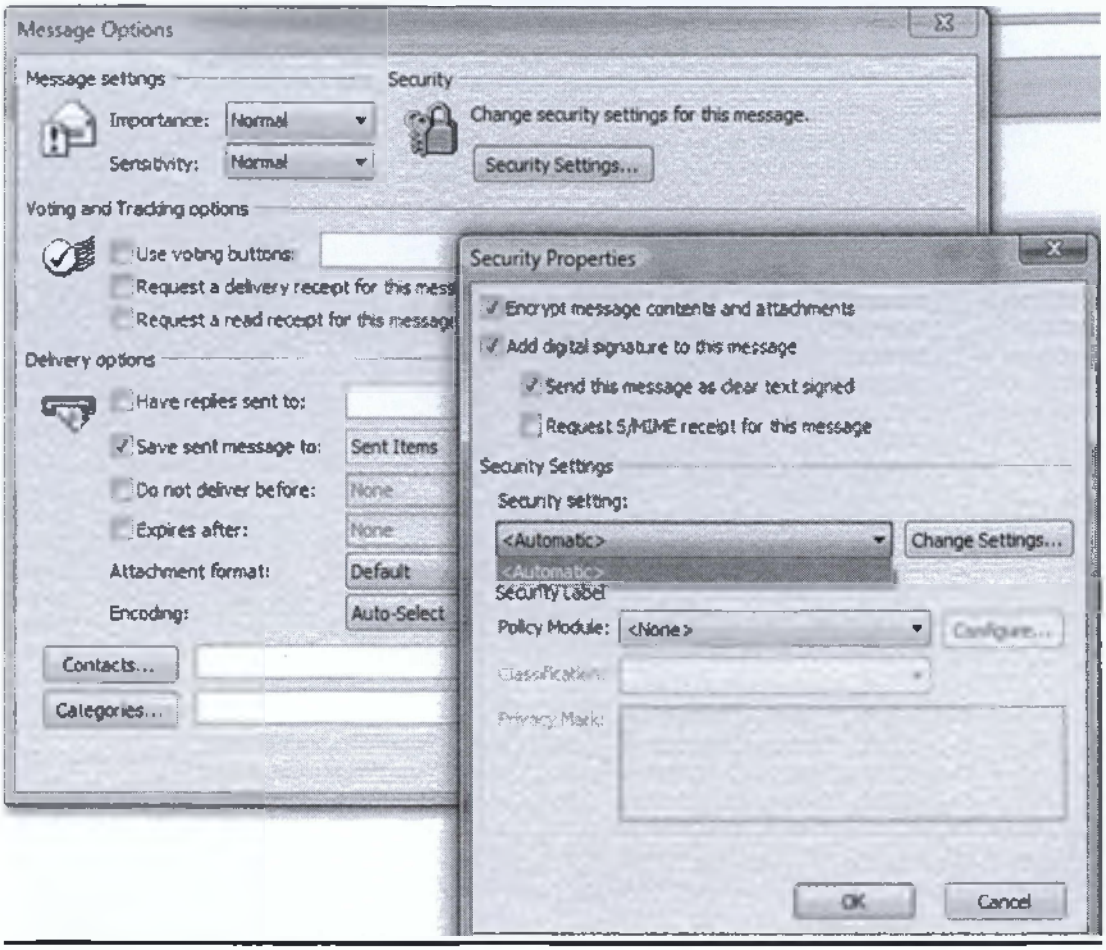
επικεφαλίδες (δεν περιλαμβάνονται οι επικεφαλίδες του RFC822) και φυσικά τα περιεχόμενα.

Η διαδικασία που προετοιμάζει το μήνυμα/οντότητα για επεξεργασία από το CMS αποτελείται από 3 βασικά βήματα:

1. Η MIME οντότητα κατασκευάζεται σύμφωνα με τις υποδείξεις του τοπικού περιβάλλοντος. Το σύνολο χαρακτήρων και οι χαρακτήρες οριοθέτησης γραμμών *(line delimiters)* καθορίζονται από το τοπικό σύστημα.

2. Η MIME οντότητα μετατρέπεται σε κανονική μορφή *(canonical form)*. Η μορφή αυτή είναι διεθνώς αναγνωρίσιμη και παρουσιάσιμη είναι ανεξάρτητη από την πλατφόρμα του εκάστοτε χρήστη. Ανάλογα με τον τύπο δεδομένων, οι ενέργειες που πρέπει να γίνουν ώστε να προκύψει αυτή η μορφή, διαφέρουν. Για παράδειγμα, για περιεχόμενα τύπου κειμένου ο χαρακτήρας οριοθέτησης γραμμών πρέπει να είναι το ζευγάρι <CR>CLF>, και το σύνολο χαρακτήρων πρέπει να είναι ένα από τα τυποποιημένα.

3. Εφαρμόζεται κατάλληλη κωδικοποίηση μεταφοράς (transfer encoding). Απαιτείται όλες οι MIME οντότητες που πρόκειται να ασφαλιστούν με το S/MIME, να είναι σε κωδικοποίηση 7bit, για σίγουρη και σωστή μεταφορά. Αυτό συμβαίνει γιατί δεν είναι βέβαιο κατά πόσο υποστηρίζεται η μεταφορά μηνυμάτων με κωδικοποίηση 8bit ή binary σε όλο το μονοπάτι από τον αποστολέα στον παραλήπτη. Εάν ένα τέτοιο μήνυμα συναντήσει ενδιάμεσο σύστημα που δεν μπορεί να μεταδώσει 8bit ή binary δεδομένα, τότε υπάρχουν τρεις επιλογές: (α) το σύστημα θα μπορούσε να αλλάξει το κωδικοποίηση μεταφοράς, ακυρώνοντας την υπογραφή, (β) το σύστημα θα μπορούσε να προωθήσει το μήνυμα όπως και να' χει, με καταστροφή του 8ου bit και συνεπώς ακύρωσης της υπογραφής και (γ) το σύστημα θα μπορούσε να επιστρέψει το μήνυμα. Και τρεις επιλογές είναι απαράδεκτες. Οι μηχανισμοί, λοιπόν, Quoted - Printable και Base64 είναι απαραίτητοι.



2.4 Secure Socket Layer (SSL)

Το πρωτόκολλο SSL αναπτύχθηκε από την *Netscape Communications Corporation* για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση *(version 1.0)* και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή *RFC (Request For Comments)*. Τον Δεκέμβριο του 1994 εκδίδεται μια αναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του *(version 2.0)*. Η παρούσα έκδοση του SSL, version 3.0, παρουσιάσθηκε στο κοινό στα τέλη του 1995, ενώ από τα μέσα του 1995 είχε αρχίσει να εφαρμόζεται σε προϊόντα της εταιρίας, όπως τον *Netscape Navigator*.

Επειδή η *Netscape* επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου γεγονός που ερχόταν σε σύγκρουση με τους νόμους των Ηνωμένων Πολιτειών περί εξαγωγή κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει την χρήση ασθενών αλγορίθμων στις εξαγόμενες εφαρμογές. Πιο συγκεκριμένα, δημιούργησε παραλλαγές των αλγόριθμων RC4-128 και RC2-128 που στην πραγματικότητα χρησιμοποιούν κλειδιά των 40 bits

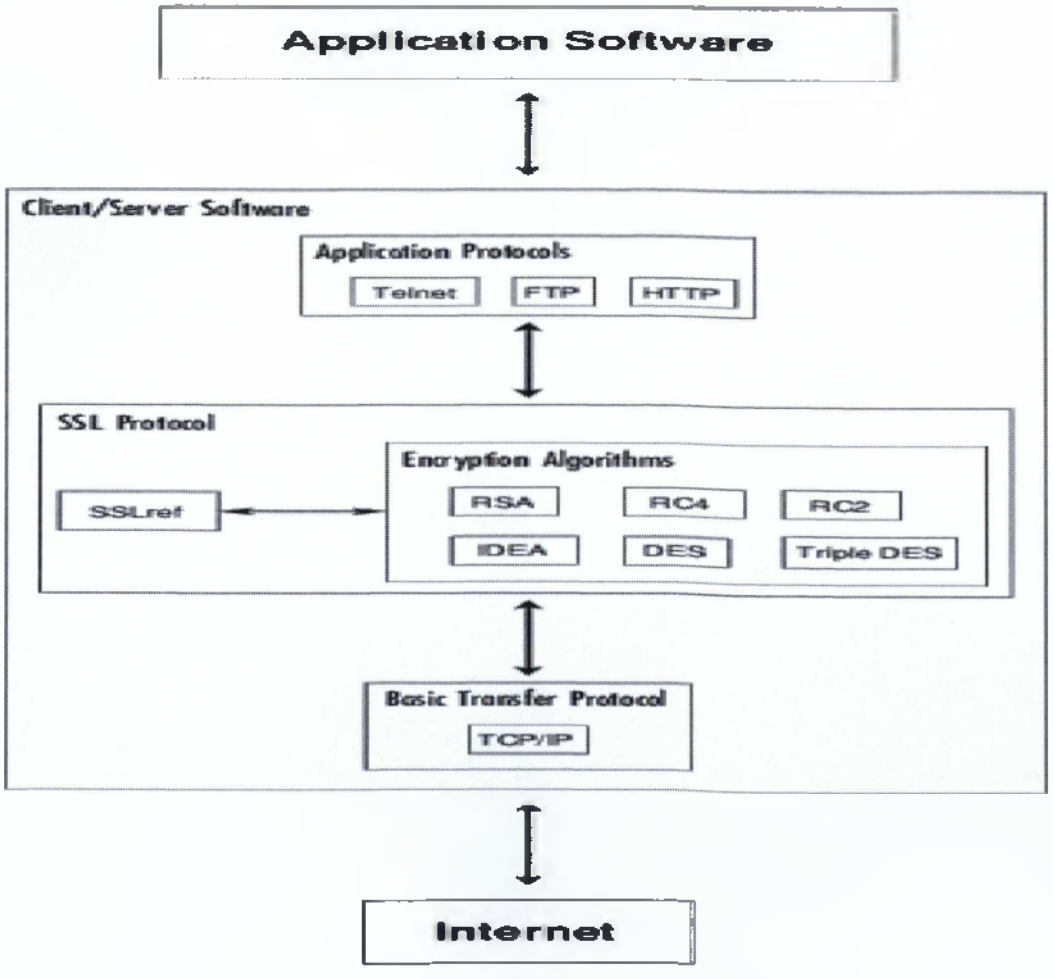
Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates

Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Όλα τα παραπάνω γίνονται με τρόπο διαφανές και απλό.

Η έκδοση 3 του πρωτοκόλλου κάλυψε πολλές αδυναμίες της δεύτερης. Οι σημαντικότερες αλλαγές έχουν να με την μείωση των απαραίτητων μηνυμάτων κατά το *handshake* για την εγκαθίδρυση της σύνδεσης, την επιλογή των αλγόριθμων συμπίεσης και κρυπτογράφησης από τον server και την εκ νέου διαπραγμάτευση του *master-key* και *session- id*. Ακόμα αυξάνονται οι διαθέσιμοι αλγόριθμοι και προστίθενται νέες τεχνικές για την διαχείριση των κλειδιών.

Συμπερασματικά μπορούμε να πούμε πως η έκδοση 3 του SSL είναι πιο ολοκληρωμένη σχεδιαστικά, με μεγαλύτερο εύρος υποστήριξης εφαρμογών και λιγότερες ατέλειες. Παρ' όλο που είναι συμβατή με την δεύτερη έκδοση, η χρήση της τελευταίας δεν πρέπει να προτιμάται.

Το SSL μπορεί να τοποθετηθεί στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς, δεν εξαρτάται από την ύπαρξη του TCP/IP και τρέχει κάτω από πρωτόκολλα εφαρμογών όπως το HTTP, FTP και TELNET. Μια αναπαράσταση του πρωτοκόλλου SSL βλέπουμε παρακάτω.



2.4.1 Λειτουργία του SSL

2.4.1.1 SSL Record Protocol

Ένα πακέτο SSL αποτελείται από δύο μέρη, την επικεφαλίδα και τα δεδομένα. Η επικεφαλίδα μπορεί να είναι είτε 3 bytes είτε 2 bytes, από τις οποίες περιπτώσεις η δεύτερη χρησιμοποιείται όταν τα δεδομένα χρειάζονται συμπλήρωμα (padding). Το πεδίο escape-bit στην περίπτωση των 3 bytes υπάρχει μόνο σε εκδόσεις μετά την δεύτερη του πρωτοκόλλου και προβλέπεται για ρύθμιση πληροφοριών out-of- band. Για την επικεφαλίδα των 2 bytes το μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι 16383 bytes.

Το κομμάτι των δεδομένων αποτελείται από ένα Message Authentication Code (MAC), τα πραγματικά δεδομένα και δεδομένα συμπλήρωσης, εάν χρειάζονται. Αυτό το κομμάτι είναι που κρυπτογραφείται κατά την μετάδοση. Τα συμπληρωματική δεδομένα απαιτούνται όταν οι αλγόριθμοι κρυπτογράφησης εν χρήση είναι τύπου block ciphers και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα ώστε το μέγεθος τους είναι πολλαπλάσιου του μεγέθους που δέχεται σαν είσοδο ο block cipher. Εάν χρησιμοποιούνται stream ciphers τότε δεν απαιτείται συμπλήρωμα και μπορεί αν χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.

Το MAC είναι η digest ή hash value των secret-write key (βλέπε παρακάτω) του αποστολέα του πακέτου, των πραγματικών δεδομένων, των συμπληρωματικών δεδομένων και ενός αριθμού ακολουθίας, στην σειρά που δίνονται.

Προβλέπεται και η συμπίεση των δεδομένων *(data compression)* με κατάλληλους μηχανισμούς που επιλέγονται κατά το handshake, ενώ δεν αποκλείεται να χρειαστεί και τεμαχισμός της πληροφορίας σε πολλά πακέτα *(fragmentation)*

2.4.1.2 SSL Handshake Protocol

Το πρωτόκολλο SSL Handshake διαχωρίζεται σε δύο επιμέρους φάσεις: η πρώτη φάση αφορά την επιλογή των αλγόριθμων, την ανταλλαγή ενός master key και την πιστοποίηση της ταυτότητας του server. Η δεύτερη φάση διαχειρίζεται την πιστοποίηση της ταυτότητας του client (εάν ζητηθεί) και ολοκληρώνει την διαδικασία του handshaking. Όταν το ολοκληρωθούν και οι δύο φάσεις, το στάδιο του handshake τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει. Όλα τα μηνύματα κατά την διάρκεια του handshaking και μετά στέλνονται σύμφωνα με το SSL Record Protocol.

Το πακέτο των αλγορίθμων κρυπτογράφησης *(Cipher Suite)* περιλαμβάνει την μέθοδο για την ανταλλαγή των κλειδιών, τον αλγόριθμο κρυπτογράφησης και τον μηχανισμό για την παραγωγή του MAC.

Παρακάτω θα δούμε τρεις διαφορετικές περιπτώσεις επικοινωνίας.

1. *Πρώτα θα εξετάσουμε την περίπτωση της αρχικής σύνδεσης, χωρίς πιστοποίηση ταυτότητας του client. Χρησιμοποιείται η σύμβαση "{data}key" για να υποδηλώσουμε κρυπτογραφημένα δεδομένα με το κλειδί "key".*

Ας δούμε βήμα προς βήμα την ακολουθία μηνυμάτων.

Τύπος Μηνύματος	*Κατεύθυνση*	*Δεδομένα που μεταφέρονται*
client-hello	C a S	challenge-data, cipher-suite-specs, compressions
server-hello	C ? S	connection-id, server-certificate, cipher-kind, compression-kind
client-master-key	C a S	clear-master-key,{secret-master-key}server-public-key
client-finish	C a S	{connection-id}client-write-key
server-verify	C ? S	{challenge-data}server-write-key
server-finish	C ? S	{session-id}server-write-key

Το μήνυμα **server-hello** επιστρέφει στον client ένα αναγνωριστικό της σύνδεσης (connection-id), την επιλογή του server όσον αναφορά πακέτο των αλγόριθμων κρυπτογράφησης και συμπίεσης (που και οι δύο υποστηρίζουν) και το πιστοποιητικό του server που θα χρησιμοποιηθεί από τον client για την απόκτηση της δημόσιας κλείδας του server. Στην τελευταία έκδοση του

Το **client-master-key** και το master-key, που ανάλογα με το που βρίσκεται κάθε υπολογιστής, μπορεί να έχει δυο διαφορετικές μορφές. Για SSL εφαρμογές έξω από τις Ηνωμένες Πολιτείες, τα 88 bits του master-key μεταδίδονται μη κρυπτογραφημένα και κρυπτογραφούνται τα υπόλοιπα 40 bits με την δημόσια κλείδα του server. Αντίθετα για SSL εφαρμογές εντός των Ηνωμένων Πολιτειών, κρυπτογραφείται όλο το master-key και το clear-master-key είναι άδειο.

Από αυτό το σημείο και μετά όλα τα μηνύματα κρυπτογραφούνται στο επίπεδο του SSL Record Protocol. Το master-key δεν χρησιμοποιείται άμεσα για κρυπτογράφηση, αλλά για την παραγωγή δύο ζευγάρια κλειδιών. Το ένα ζευγάρι ανήκει στον client και αποτελείται από το *client-write-key* που χρησιμοποιεί ο client για να κρυπτογραφήσει τα μηνύματα προς τον server και το *client-read-key* για να αποκρυπτογραφήσει ότι λαμβάνει από αυτόν. Το δεύτερο ζευγάρι ανήκει στον server και αποτελείται από το *server-write-key* για κρυπτογράφηση μηνυμάτων προς τον client και το *server-read-key* για αποκρυπτογράφηση των παραληφθέντων. Για την ακρίβεια, το client-write-key είναι το ίδιο με το server-read-key και το client-read-key είναι το ίδιο με το server-write-key.

Το **client-finish** περιέχει το αναγνωριστικό της σύνδεσης που αρχικά είχε σταλεί από τον server κρυπτογραφημένο με το client-write-key.

Το **server-verify** περιέχει τα challenge-data που είχε στείλει ο client στον server κατά την αρχή της σύνδεσης, κρυπτογραφημένα με το server-write-key. Η παραλαβή και αποκρυπτογράφηση αυτού του μηνύματος είναι το τελικό στάδιο για την επιβεβαίωση της ταυτότητας του server καθ' ότι μόνο ο αληθινός server θα μπορούσε να αποκρυπτογραφήσει με την ιδιωτική του κλείδα το master-key.

Τέλος, το μήνυμα **server-finish** τερματίζει το handshake. Περιέχει το session-id που χρησιμοποιείται σε επόμενες διαδικασίες handshake για την αποφυγή επανάληψης της φάσης επιλογής αλγορίθμων και ανταλλαγής του master-key. Το session-id αποθηκεύεται και από τους δύο και η προτεινόμενη διάρκεια ζωής είναι 100 δευτερόλεπτα. Έπειτα, αχρηστεύεται.

2. *Όταν ένα προηγούμενο session-id από τον client χρησιμοποιείται για να επανεγκαταστήσει την σύνδεση, το handshake γίνεται ως εξής:*

Τύπος Μηνύματος	*Κατεύθυνση*	*Δεδομένα που μεταφέρονται*
client-hello	C a S	challenge-data, session-id, cipher-suite-specs, compressions
server-hello	C? S	connection-id
client-finish	C a S	{connection-id}client-write-key
server-verify	C? S	{challenge-data}server-write-key
server-finish	C? S	{session-id}server-write-key

Αλλάζει το **client-hello** που περιέχει επιπλέον το session-id και χρησιμοποιείται από τον server για να καθορίσει τους αλγόριθμους και το master-key. Η λίστα με τους αλγόριθμους στέλνεται ξανά για την περίπτωση όπου έχει λήξει το session- id. Το **server-hello** στέλνεται μόνο όταν το session-id ισχύει ακόμα.

3. *Όταν ζητείται πιστοποίηση της ταυτότητας του client και έχει προηγουμένως εκδοθεί session-id, η ακολουθία των μηνυμάτων του handshaking γίνεται:*

Τύπος Μηνύματος	*Κατεύθυνση*	*Δεδομένα που μεταφέρονται*
lient-hello	C a S	challenge-data, session-id, cipher-suite-specs
erver-hello	C? S	connection-id, server-certificate, cipher-kind
lient-master-key	C a S	clear-master-key,{secret-master-key}server-public-key
lient-finish	C a S	{connection-id}client-write-key
:rver-verify	C? S	{challenge-data}server-write-key
quest-certificate	C? S	{auth-type, cert-chal-data}server-write-key
ient-certificate	C a S	{cert-type, client-cert, resp-data}client-write-key
rver-finish	C ? S	{session-id}server-write-key

Παρατηρούμε ότι προστίθενται δύο νέα μηνύματα στην προηγούμενη ακολουθία.

Το **request-certificate** στέλνεται από τον server και περιέχει μια δήλωση για την συνάρτηση που θα χρησιμοποιήσει ο client για την παραγωγή της digest value και τον τύπο της συμμετρική κρυπτογράφησης (auth- type). Επίσης, αποστέλλονται και δεδομένα που θα υπογράψει ο client για να αποδείξει την ταυτότητα του (cert- chal-data).

Το **client-certificate** επιστρέφει στον server το πιστοποιητικό του client, μαζί με μια δήλωση του τύπου αυτού (cert- type)και την υπογραφή των δεδομένων cert-chal-data. Ο server θα χρησιμοποιήσει την δημόσια κλείδα που περιέχεται στο πιστοποιητικό του client για να αποκρυπτογραφήσει την υπογραφή. Έπειτα, θα υπολογίσει το message digest των cert-chal-data και θα το συγκρίνει με το message digest που προήλθε από την αποκρυπτογράφηση της υπογραφής.

Κατά την διάρκεια όλων των παραπάνω ανταλλαγών μηνυμάτων, μηνύματα λάθους μπορούν να σταλούν σαν απάντηση σε μηνύματα που δεν βγάζουν νόημα. Η διαδικασία αναγνώρισης λάθους και αποστολή του κατάλληλου μηνύματος αναλαμβάνεται από το πρωτόκολλο SSL Alert Protocol και είναι μέρος του SSL Handshake Protocol. Έτσι, το μήνυμα **no-cipher-error** στέλνεται όταν ο server δεν υποστηρίζει κανένα από τους αλγόριθμους που προτείνει ο client, το μήνυμα **no-certificate-error** όταν δεν είναι διαθέσιμο το ζητηθέν πιστοποιητικό, το μήνυμα **bad-certificate** αν το πιστοποιητικό είναι άκυρο και τέλος το **unsupported-certificate-type- error**, όταν ο τύπος ενός πιστοποιητικού δεν υποστηρίζεται από κανέναν.

2.4.2 Αντοχή του SSL σε γνωστές επιθέσεις

Dictionary Attack

Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του ανέντιμων προσώπων. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί.

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bit κλειδιά και παρ' όλο που τα 88 bit αυτών μεταδίδονται ανασφάλιστα, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών κάνει την επίθεση αδύνατο να επιτύχει.

Brute Force Attack

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι τελείως ανούσια. Μόνο ο DES56 bit cipher είναι ευαίσθητος σε αυτήν την επίθεση, αλλά η χρήση του δεν συνιστάται.

Replay Attack

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

Man-In-The-Middle-Attack

Η επίθεση Man- In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.

Το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατον. Μην ξεχνάμε την δυνατότητα επικοινωνίας των κλειδιών υπογεγραμμένα.

2.4.3 Αδυναμίες του SSL

Brute Force Attack Εναντίον Αδύναμων Αλγορίθμων

Η μεγαλύτερη αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά. Συγκεκριμένα, οι RC4-40, RC2-40 και DES-56 εισάγουν σοβαρά προβλήματα ασφαλείας και θα πρέπει να αποφεύγονται.

Renegotiation of Session Keys (μόνο στην 2 έκδοση)

Από την στιγμή που μία σύνδεση δημιουργηθεί, το ίδιο master key χρησιμοποιείται καθ' όλη την διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνδεση (π.χ. μιας TELNET εφαρμογής), η αδυναμία αλλαγής του master key γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχής Brute Force Attack.

2.4.4 Χρήσεις του SSL

Η πιο κοινή του εφαρμογή είναι για την διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλή έκδοση του HTTP χρησιμοποιεί URLs που ξεκινούν με "https" αντί του κανονικού "http" και διαφορετική πόρτα *(port)* που είναι η προκαθορισμένη στην 443. Ο browser αποθηκεύει τα ιδιωτικά κλειδιά του χρήστη και με κατάλληλο τρόπο υποδεικνύει την διενέργεια ασφαλών συνδέσεων.

Παρ' όλο που μπορεί κανείς να γράψει μια εφαρμογή του SSL ακολουθώντας τα *Internet drafts* και RFCs, είναι προτιμότερο να χρησιμοποιήσει μία από τις υπάρχοντες βιβλιοθήκες εργαλείων του SSL *(SSL toolkit Libraries)*. Τέτοιες βιβλιοθήκες περιέχουν ρουτίνες για κρυπτογράφηση, digestion, και διαχείριση πιστοποιητικών και διακρίνονται στις ακόλουθες:

- SSLRef
- SSLPlus
- SSLava
- SSLeay

2.4.5 E-mail over SSL

Χρησιμοποιώντας την δυνατότητα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου (e- mail) μέσω SSL, η επικοινωνία μας με τους εξυπηρετητές (mail servers) κρυπτογραφείται και επομένως, οι κωδικοί ασφαλείας μας για την πρόσβαση στο ηλεκτρονικό μας ταχυδρομείο (username και password), όπως και η αποστολή και λήψη των ηλεκτρονικών μας μηνυμάτων πραγματοποιείται με ασφάλεια. Η κρυπτογράφηση αυτή είναι ιδιαίτερα σημαντική στις περιπτώσεις που πραγματοποιείτε η πρόσβασή μας μέσω δημόσιων ασύρματων δικτύων (WiFi hotspots) για να αποφευχθεί τυχόν υποκλοπή των στοιχείων πρόσβασής μας (username και password) όπως και υποκλοπή των ηλεκτρονικών μας μηνυμάτων.
Συνίσταται επίσης για την δική μας ασφάλεια να χρησιμοποιείται μόνιμα αυτή η δυνατότητα πρόσβασης μέσω SSL για την υπηρεσία του ηλεκτρονικού μας ταχυδρομείου.
Μέχρι τώρα ο μόνος τρόπος να λαμβάνουμε και να στέλνουμε email μέσω της ηλεκτρονικής μας διεύθυνσης στην Forthnet ήταν η χρήση συγκεκομμένων προγραμμάτων ανάγνωσης e-mail (π.χ. Outlook, Outlook Express, Windows Mail, Windows Live Mail, Firefox, κα) χρησιμοποιώντας τα πρωτόκολλα **POP3** και **IMAP**.
Με τη νέα δυνατότητα μπορείτε να στέλνετε και να λαμβάνετε emails από οποιαδήποτε μέρος του κόσμου και από οποιαδήποτε δίκτυα ενσύρματα ή ασύρματα (WiFi hotspots) **με ασφάλεια με τα ίδια προγράμματα ανάγνωσης ηλεκτρονικών μηνυμάτων**, εφόσον η επικοινωνία κρυπτογραφείται μέσω **SSL (POP3 over SSL, IMAP over SSL)**.
Χρησιμοποιώντας τη δυνατότητα αποστολής και λήψης email μέσω του πρωτόκολλου SSL, ρυθμίζουμε το πρόγραμμα διαχείρισης αλληλογραφίας μας ώστε εκείνο να παρέχει το προσωπικό μας username και κωδικό πρόσβασης στον διακομιστεί αλληλογραφίας (Mail Server) μέσα από μία ασφαλή σύνδεση, απ' οπουδήποτε και αν βρισκόμαστε και με όποιο τρόπο και να έχουμε συνδεθεί στο διαδίκτυο.

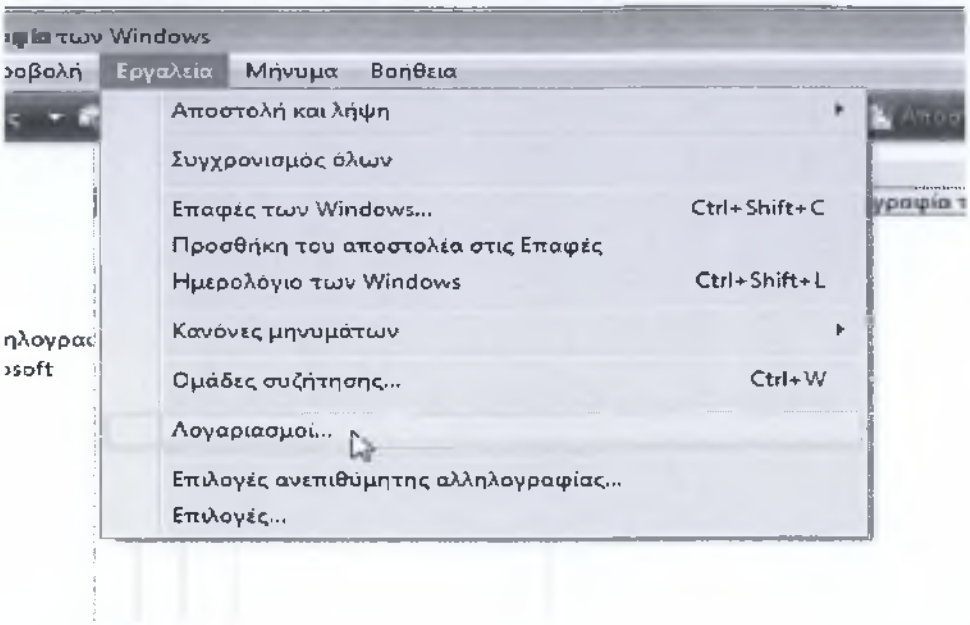
2.4.6 Ρυθμίσει Ασφαλούς Λειτουργίας SSL

Για να χρησιμοποιήσουμε τη δυνατότητα E-mail over SSL θα πρέπει να χρησιμοποιήσουμε τις ακόλουθες ρυθμίσεις (ως παράδειγμα έλαβα την εταιρία Forthnet):

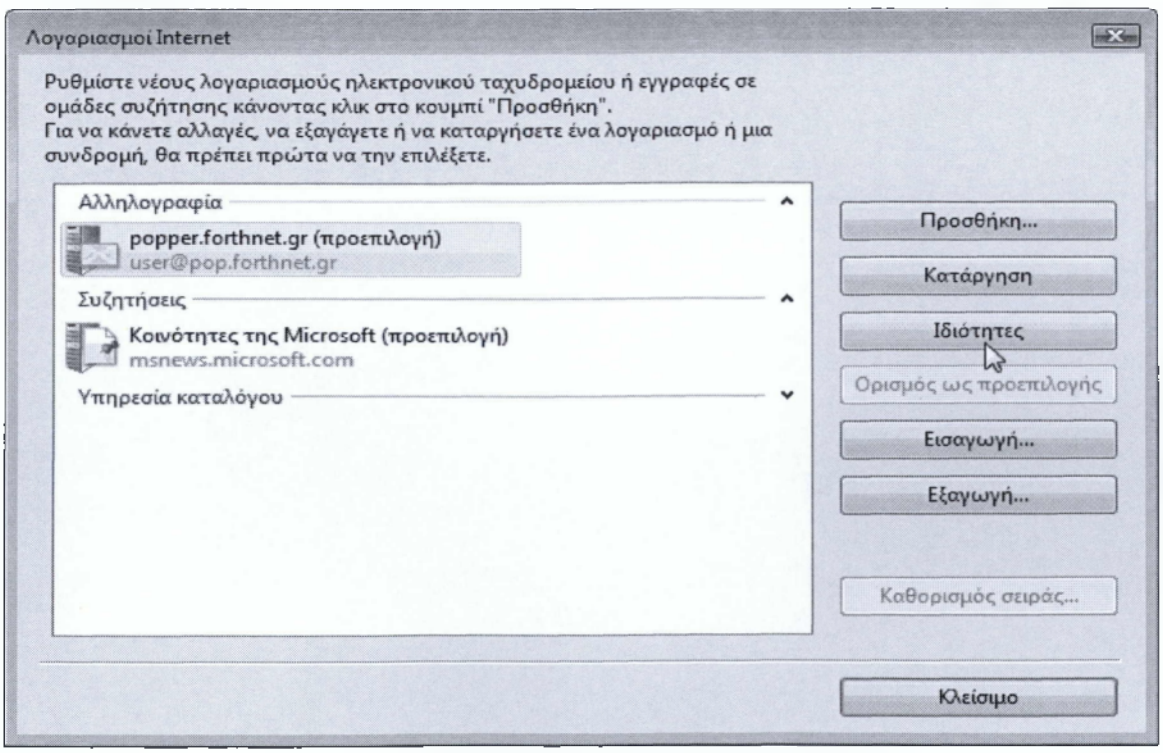
I. Διακομιστείς εισερχόμενης αλληλογραφίας / Incoming Mail (POP3) : **mail.forthnet.gr** πόρτα **995**
II. Διακομιστείς εξερχόμενης αλληλογραφίας / Outgoing Mail (SMTP) :**mail.forthnet.gr** πόρτα **465**
III. Επιλογή **χρήσης SSL** από το αντίστοιχο πρόγραμμα ανάγνωσης ηλεκτρονικών μηνυμάτων.

Για να ρυθμίσουμε τις παραμέτρους του προγράμματος **Αλληλογραφία των Windows (Windows Mail)** ώστε να μπορούμε να στείλουμε και να λάβουμε mail, χρησιμοποιώντας το πρωτόκολλο **SSL**, θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα.

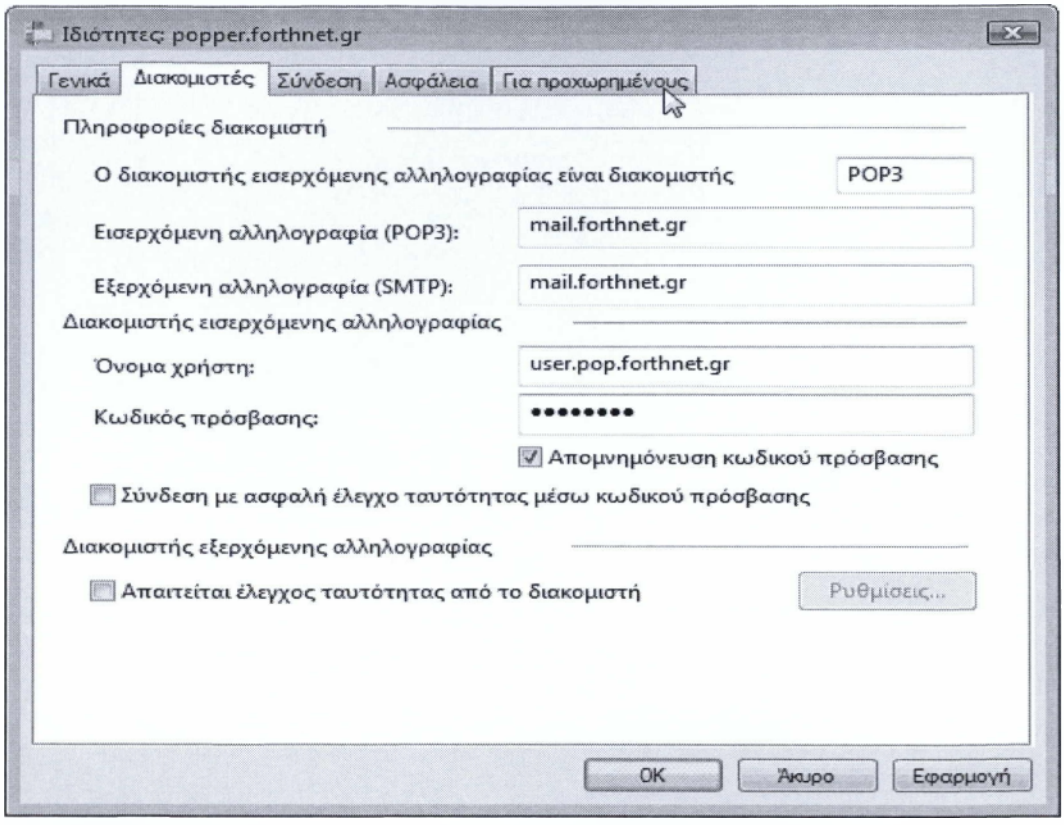
- Ανοίγουμε το πρόγραμμα **Αλληλογραφία των Windows (Windows Mail)**. Επιλέγουμε *Εργαλεία (Tools)* και *Λογαριασμοί (Accounts)*.



- Από τους λογαριασμούς *Αλληλογραφία (Mail)* επιλέγουμε τον λογαριασμό ηλεκτρονικού ταχυδρομείου που έχουμε δημιουργήσει και πατάμε *Ιδιότητες (Properties)*.



- Στην περίπτωση που χρησιμοποιούμε POP



➢ Σε αυτή την καρτέλα πρέπει να έχουμε συμπληρωμένα τα εξής:

I. Το πεδίο *Ο διακομιστείς εισερχόμενης αλληλογραφίας είναι διακομιστείς (My incoming mail server is a ..... server)* θα παραμείνει ως έχει **(POP3).**

II. *Εισερχόμενη αλληλογραφία (Incoming mail):* **mail.mail.forthnet.gr** *Εξερχόμενη αλληλογραφία (Outgoing mail):* **mail.forthnet.gr**

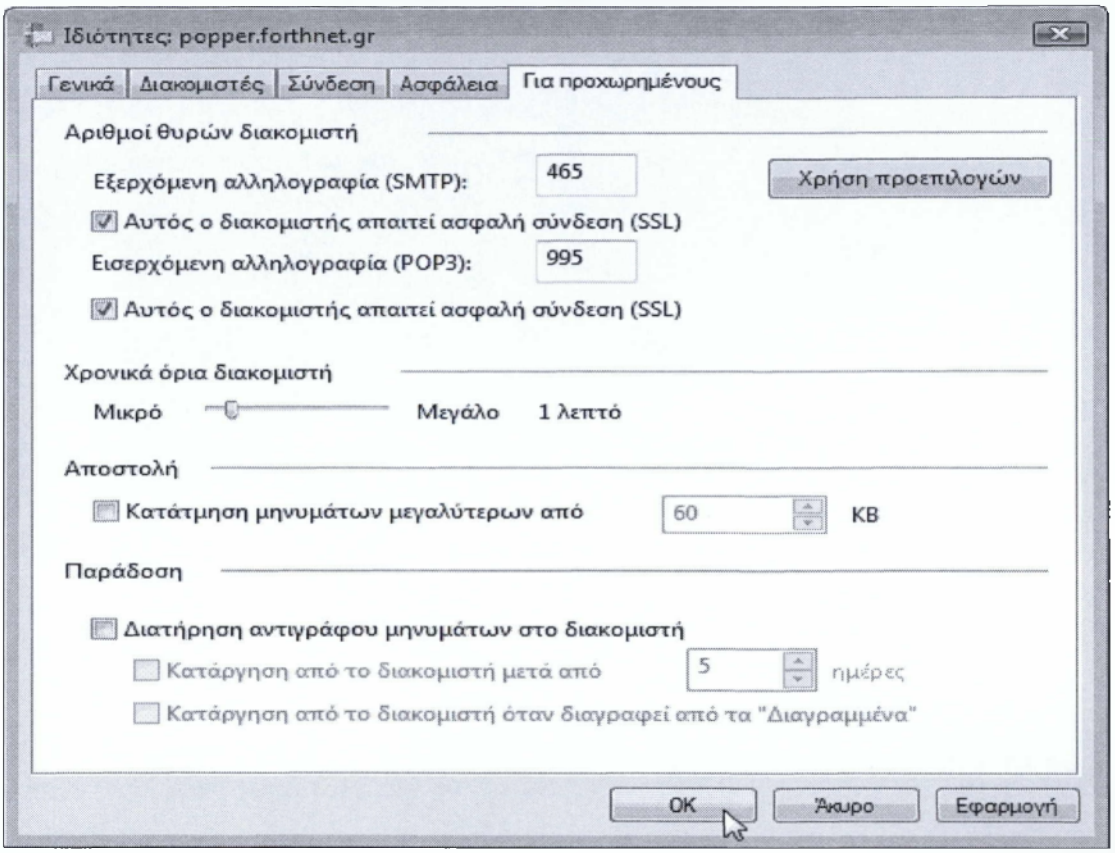
III. Το *Όνομα χρήστη (E-mail username)* θα είναι της μορφής : **user.pop.Forthnet.gr**

IV. Όπου user = Το μέρος του username όπως εμείς το έχουμε επιλέξει (π.χ george, nick κ.λπ.) και pop = Το σημείο παρουσίας (point of presence) π.χ: ATH για Αθήνα, THE για Θεσσαλονίκη κ.λπ.

Στο πεδίο Κωδικός πρόσβασης (password) θα πρέπει να εισάγουμε τον κωδικό πρόσβασης, όπως ακριβώς μας έχει δοθεί από τη Forthnet.
Το password είναι case sensitive, κάτι το οποίο σημαίνει ότι αν αυτό συμπεριλαμβάνει χαρακτήρες με πεζά η κεφαλαία γράμματα, θα πρέπει να εισαχθεί και αντίστοιχα.

✓ Σημείωση: Βεβαιωνόμαστε ότι έχουμε επιλέξει την αγγλική γλώσσα κατά την πληκτρολόγηση των στοιχείων μας. Είναι απαραίτητη η εισαγωγή των στοιχείων με λατινικούς χαρακτήρες.

➢ Επιλέγουμε την καρτέλα, *Για προχωρημένους (Advanced)*



➢ Σε αυτή την καρτέλα συμπληρώνουμε τα παρακάτω:

I. *Αριθμοί θυρών διακομιστεί (Server Port Numbers) Εξερχόμενη αλληλογραφία (Outgoing Mail) (SMTP)* : **465**

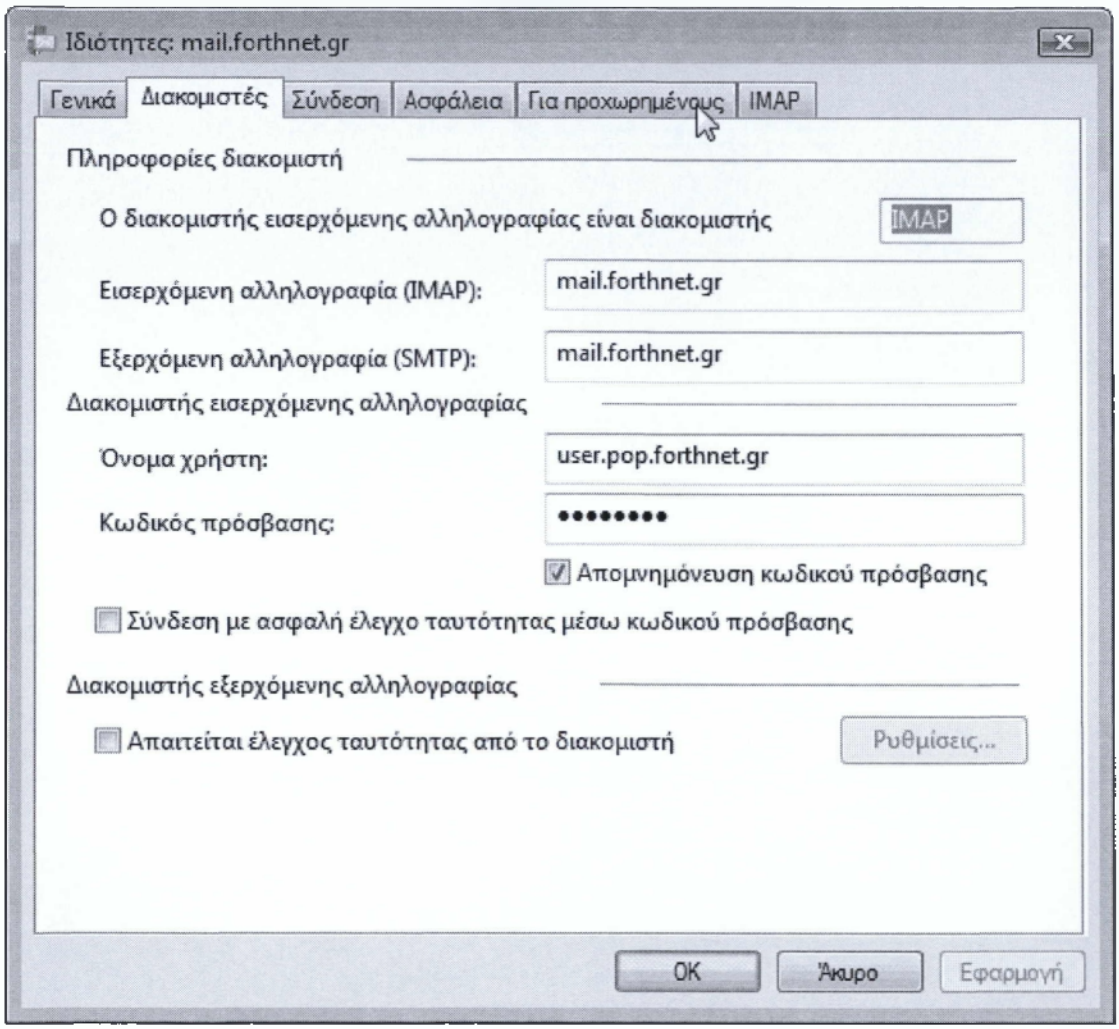
II. Επιλέγουμε *"Αυτός ο διακομιστείς απαιτεί ασφαλή σύνδεση" ("This server requires a secure connection) (SSL).*

III. *Εισερχόμενη αλληλογραφία (Incoming Mail) (POP3)* : **995**

IV. Επιλέγουμε *"Αυτός ο διακομιστείς απαιτεί ασφαλή σύνδεση" ("This server requires a secure connection) (SSL).*

Πατάμε σε όλα τα παράθυρα OK.

- Στην περίπτωση που χρησιμοποιείτε IMAP :



➢ Σε αυτή την καρτέλα πρέπει να έχουμε συμπληρώσει τα εξής.

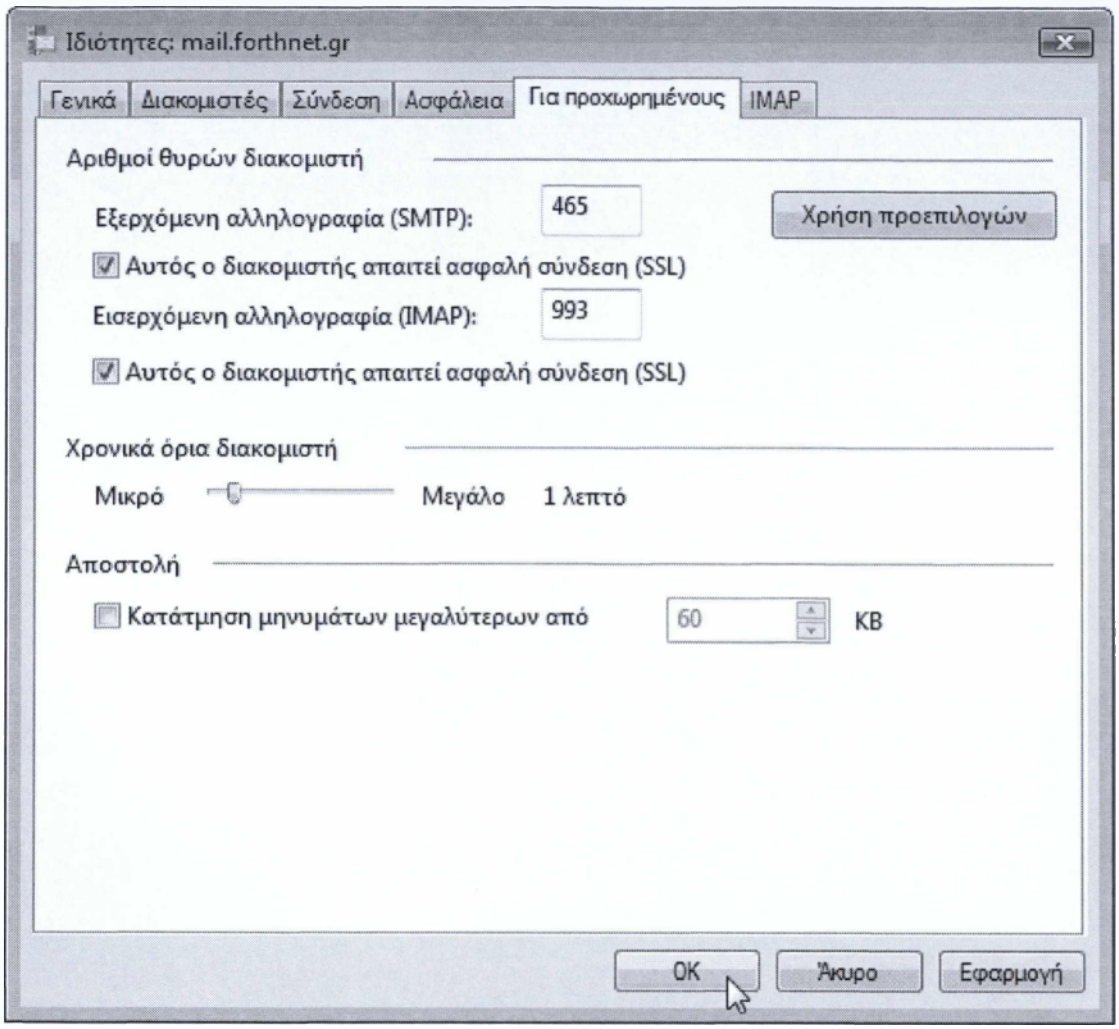
I. Στο πεδίο *"Ο διακομιστείς εισερχόμενης αλληλογραφίας είναι διακομιστείς" (My Incoming mail server is a ... server)* **IMAP**

II. *Εισερχόμενη αλληλογραφία (Incoming mail):* **mail.Forthnet.gr**
Εξερχόμενη αλληλογραφίας (Outgoing mail): **mail.Forthnet.gr**

III. Το *Όνομα χρήστη (username)* μας είναι της μορφής : **user.pop.Forthnet.gr**

IV. όπου user = Το μέρος του username όπως εσείς το έχετε επιλέξει (π.χ George, nick κ.λπ.) και pop = Το σημείο παρουσίας (point of presence) π.χ: ATH για Αθήνα, THE για Θεσσαλονίκη κ.λπ.

- Επιλέγουμε την καρτέλα Για προχωρημένους (Advanced)



- Σε αυτή την καρτέλα συμπληρώνετε τα παρακάτω :

I. *Αριθμοί θυρών διακομιστεί (Server Port Numbers) Εξερχόμενη αλληλογραφία (Outgoing Mail) (SMTP)* : **465**

II. Επιλέγετε *"Αυτός ο διακομιστείς απαιτεί ασφαλή σύνδεση" ("This server requires a secure connection) (SSL).*

III. *Εισερχόμενη αλληλογραφία (Incoming Mail) (POP3)* : **993**

IV. Επιλέγετε *"Αυτός ο διακομιστείς απαιτεί ασφαλή σύνδεση" ("This server requires a secure connection) (SSL).*

Πατήστε σε όλα τα παράθυρα **OK**.

2.5 PEM (Privacy Enhanced Mail)

Το 1985, το Internet Architecture Board (IAB) όρισε μια Privacy Enhanced Mail (PEM) ομάδα εργασίας για να δουλέψει πάνω σε ένα στάνταρ πρωτόκολλο για την ασφάλεια του ηλεκτρονικού ταχυδρομείου. Ένα πρώτο σύνολο μηχανισμών ορίζει πρωτόκολλα που παρέχουν υπηρεσίες ιδιωτικότητας, ακεραιότητας και πιστοποίησης αυθεντικότητας στα μηνύματα ηλεκτρονικού ταχυδρομείου.

Το δεύτερο σύνολο παρέχει μια υπηρεσία πιστοποιητικών με τη βοήθεια της οποίας επιτυγχάνεται η διανομή των κλειδιών στο Διαδίκτυο και παρέχεται υποστήριξη των μηχανισμών του πρώτου συνόλου

Είχε αποφασιστεί ότι ασφαλή μηνύματα θα περιλαμβάνονταν ως μέρη σώματος σε στάνταρ μηνύματα ηλεκτρονικού ταχυδρομείου και θα αποστέλλονταν μέσω ενός βασισμένου στο SMTP πράκτορα μεταφοράς μηνύματος (Message Transfer Agent, MTA). Συνεπώς, τα ασφαλή μηνύματα ηλεκτρονικού ταχυδρομείου δεν είναι απαραιτήτως εμφανή στο σύστημα μεταφοράς μηνυμάτων (Message Transfer System, MTS).

Ο αποστολέας δημιουργεί ένα ηλεκτρονικό μήνυμα και ενεργοποιεί τον Πράκτορα Χρήστη του αποστολέα, ο οποίος υποβάλλει το μήνυμα σε έναν πράκτορα μεταφοράς. Ο πράκτορας αυτός μεταβιβάζει το μήνυμα μέσω ενός άλλου πράκτορα μεταφοράς, ο οποίος βρίσκεται εγκατεστημένος σε διαφορετικό σταθμό. Η διαδικασία επαναλαμβάνεται έως ότου το μήνυμα ανακτηθεί από τον Πράκτορα Μεταφοράς Μηνύματος που βρίσκεται στον σταθμό του παραλήπτη.

Το μήνυμα περνά στον Πράκτορα Χρήστη του παραλήπτη, ο οποίος αναλαμβάνει την αποθήκευσή του. Ο παραλήπτης μπορεί με τον Πράκτορα Χρήστη να διαβάσει ή να αποθηκεύσει το μήνυμα, να απαντήσει σε αυτό ή να εκτελέσει κάποια άλλη λειτουργία.

Τα μηνύματα που ανακτώνται από τον Πράκτορα Μεταφοράς Μηνύματος του αποδέκτη είναι κατάλληλα μορφοποιημένα, ώστε να γίνει η διαχείρισή τους βάσει του πρωτοκόλλου του συστήματος. Είναι αναγκαίο η μορφή των μηνυμάτων να είναι κατανοητή από τους πράκτορες του αποστολέα και του παραλήπτη ή να μπορεί να μεταφραστεί σε κατανοητή και από τους δύο μορφή. Για παράδειγμα, οι Πράκτορες Μεταφοράς Μηνύματος που διαχειρίζονται μηνύματα ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο αναμένουν μηνύματα, τα οποία περιγράφονται από το πρότυπο RFC-822.

Η ύπαρξη πολυάριθμων Πρακτόρων Μεταφοράς Μηνύματος επιβάλλει την ευρεία χρήση ενός μόνο πρωτοκόλλου που θα παρέχει ασφάλεια στα μηνύματα. Βάσει της υπόθεσης αυτής, η παροχή υπηρεσιών ασφάλειας πρέπει να τοποθετηθεί στο επίπεδο Πράκτορα Χρήστη και όχι στο επίπεδο Πράκτορα Μεταφοράς Μηνύματος. Έτσι, οι μεν υπηρεσίες ασφάλειας θα είναι «μη ορατές» από τον πράκτορα μεταφοράς και τα δε συστήματα ηλεκτρονικού ταχυδρομείου θα είναι σε θέση να αποστέλλουν εμπιστευτικά ή μη εμπιστευτικά μηνύματα.

Το PEM δεν έχει διαδοθεί αρκετά γιατί το πρότυπο PEM απαιτεί μια υπάρχουσα και πλήρως χρησιμοποιούμενη ιεραρχική δομή για τα πιστοποιητικά, όπως περιγράφηκε παραπάνω. Υποστηρίζει περιορισμένο αριθμό αλγορίθμων κρυπτογράφησης. Για παράδειγμα, χρησιμοποιείται για κρυπτογράφηση ο αλγόριθμος DES που θεωρείται σχετικά αδύναμος και δεν παρέχει επαρκή ασφάλεια. Τέλος, το πρότυπο PEM είναι περιορισμένο σε ένα βασισμένο σε κείμενο περιβάλλον και δεν παρέχει υποστήριξη για την αποστολή δυαδικών και σύμφωνων με το πρότυπο MIME αρχείων.

2.5.1 Αποστολή μηνύματος στο PEM

Το πρότυπο PEM επιβάλλει την ενθυλάκωση των πεδίων επικεφαλίδας, που σχετίζονται με τη διαχείριση του μηνύματος, στο τμήμα εκείνο του μηνύματος του οποίου η ιδιωτικότητα προστατεύεται, έτσι ώστε τα μηνύματα PEM να αποτελούν το σώμα ενός συνηθισμένου μηνύματος ηλεκτρονικού ταχυδρομείου.

Κάποιοι Πράκτορες Χρήστη (UA) δεν επιτρέπουν στους χρήστες ή σε κάποια άλλη διεργασία να προσθέσει ειδικά πεδία επικεφαλίδων στα οποία θα περιέχεται επιπλέον πληροφορία, για την αποστολή κρυπτογραφημένων μηνυμάτων. Αυτό βέβαια δεν αποτελεί πρόβλημα στην περίπτωση που τα σχετικά πεδία είναι ήδη ενθυλακωμένα στο σώμα του μηνύματος.

Είναι σημαντικό το πρότυπο PEM να παραμείνει συμβατό με την ήδη υπάρχουσα υποδομή για την επεξεργασία του ηλεκτρονικού ταχυδρομείου. Η προσθήκη, όμως, νέων επικεφαλίδων απαιτεί την ύπαρξη Πρακτόρων Μεταφοράς Μηνύματος (Message Transfer Agents, MTA) οι οποίοι θα είναι σε θέση να διαχειρίζονται αυτά τα πεδία. Όμως, αν οι επικεφαλίδες παροχής ιδιωτικότητας είναι απλά ένα τμήμα του σώματος του μηνύματος, τότε οι Πράκτορες Μεταφοράς Μηνύματος δεν είναι απαραίτητο να γνωρίζουν τίποτα σχετικά με τις νέες επικεφαλίδες.

Ένα ενθυλακωμένο σε κάποιο μήνυμα τμήμα, οριοθετείται από χαρακτήρες έναρξης και τερματισμού, ενώ παρεμβάλλονται και ειδικά διαμορφωμένα πεδία. Συγκεκριμένα, αναγνωριστικό έναρξης αποτελεί η γραμμή:

-----BEGIN PRIVACY – ENHANCED MESSAGE BOUNDARY-----

Ακολουθούν ενθυλακωμένα πεδία επικεφαλίδας, μια κενή γραμμή και το ενθυλακωμένο κείμενο. Τέλος, τοποθετείται το αναγνωριστικό τερματισμού του PEM μηνύματος:

-----END PRIVACY – ENHANCED MESSAGE BOUNDARY-----

2.5.2 Μετασχηματισμός του ενθυλακωμένου σώματος

Κατά τη μεταφορά τους, τα μηνύματα PEM πρέπει να βρίσκονται σε μορφή η οποία θα καθιστά εφικτή την αποκρυπτογράφηση του κειμένου και τον έλεγχο της ακεραιότητας του μηνύματος. Μια πρόταση που λαμβάνει υπόψη της τις προδιαγραφές του Διαδικτύου επιβάλλει την αποστολή ενθυλακωμένων μηνυμάτων, των οποίων η μορφή θα είναι κατανοητή από τους πράκτορες μεταφοράς του πρωτοκόλλου SMTP.

Οι χαρακτήρες του μηνύματος πρέπει να ακολουθούν την κωδικοποίηση των 7-bits των χαρακτήρων του κώδικα ASCII, καθώς δεν είναι εγγυημένη η επιτυχής μεταφορά μηνυμάτων στα οποία εφαρμόζεται κωδικοποίηση των 8-bits. Σε κάθε γραμμή του κειμένου δεν πρέπει να περιέχονται περισσότεροι από 1000 χαρακτήρες. Οι γραμμές του κειμένου οριοθετούνται από ένα χαρακτήρα επιστροφής, τον ''<CR>'' (carriage return), ακολουθούμενο από μια γραμμή τροφοδοσίας, την ''<LF>'' (line feed). Η ακολουθία χαρακτήρων ''<CR><LF>.<CR><LF>'', η οποία χρησιμοποιείται από τους πράκτορες μεταφοράς για τον καθορισμό του τέλους του μηνύματος δεν πρέπει να εμφανιστεί στο σώμα του μηνύματος.

Επειδή τα περισσότερα συστήματα υπολογιστών δε χρησιμοποιούν μια αναπαράσταση, που να πληροί τις παραπάνω προδιαγραφές είναι απαραίτητος ο μετασχηματισμός των μηνυμάτων, ώστε να είναι εφικτή η διαχείρισή τους καθώς μεταφέρονται μεταξύ συστημάτων, που έχουν υιοθετήσει διαφορετικούς τρόπους αναπαράστασης.

Το ενθυλακωμένο σώμα μετασχηματίζεται σε τρία στάδια:

1. Τοποθετείται σε μια μορφή, ανεξάρτητη της συγκεκριμένης μηχανής.
2. Πραγματοποιείται έλεγχος της ακεραιότητας και αν είναι απαραίτητο το μήνυμα κρυπτογραφείται,
3. Η παραγόμενη ακολουθία δυαδικών ψηφίων (bits) μετατρέπεται σε ένα σύνολο εκτυπώσιμων χαρακτήρων, κατάλληλο να υποστεί επεξεργασία από κάθε πράκτορα μεταφοράς

2.6 Κλειδιά

Τα Data Encrypting Keys (DEKs) 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) τα DEKs χρησιμοποιούνται στην επιπλέον κρυπτογράφηση των Message Integrity Checks (MICs). «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 αλγόριθμος όταν στην είσοδο εισάγουμε το μήνυμα. Τα κλειδιά DEKs παράγονται εκ νέου για κάθε μήνυμα προς μετάδοση.

Τα 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. 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.

2.7 Πιστοποίηση Αυθεντικότητας και Κρυπτογράφηση

Για να εξασφαλιστεί η ιδιωτικότητα ενός μηνύματος είναι απαραίτητη η κρυπτογράφησή του, Η διαδικασία που απαιτεί τη χρήση κατάλληλου αλγορίθμου κρυπτογράφησης και του κλειδιού συνόδου. Προς το παρόν, ο μόνος ευρέως διαδεδομένος αλγόριθμος κρυπτογράφησης είναι ο DES.

Ένα **MIC-CLEAR** μήνυμα παρέχει υποστήριξη για πιστοποίηση μηνύματος, ακεραιότητα δεδομένων και μη αποκήρυξη υποχρέωσης/οφειλής. Παρόλα αυτά, δεν παρέχει υποστήριξη για υπηρεσίες εμπιστευτικότητας δεδομένων. Ένα MIC-CLEAR μήνυμα μπορεί να ληφθεί και να διαβαστεί από user agents οι οποίοι δεν υποστηρίζουν προς το παρόν PEM. Ένας ικανός user agent PEM επαληθεύει την αυθεντικότητα και την ακεραιότητα ενός MIC-CLEAR μηνύματος, ενώ ένας άσχετος user agent PEM μπορεί να παρουσιάσει αλλά όχι να επαληθεύσει την αυθεντικότητα και την ακεραιότητα του

Το **MIC ONLY** μήνυμα παρέχει την υπηρεσία ασφάλειας του MIC-CLEAR και επιπλέον κωδικοποίηση μετάδοσης. Το βήμα κωδικοποίησης εξασφαλίζει ότι τα PEM μηνύματα μπορούν να περαστούν μέσω ποικίλων MTS και πύλες ηλεκτρονικού ταχυδρομείου χωρίς να μετατραπούν με τέτοιο τρόπο ώστε να ακυρώσουν τα MICs που περιέχουν.

Ένα **ENCRYPTED** μήνυμα παρέχει την υπηρεσία ασφάλειας του MIC ONLY και επιπλέον υπηρεσία εμπιστευτικότητας δεδομένων. Συνεπώς, ένα ENCRYPTED μήνυμα παρέχει υποστήριξη για όλες τις υπηρεσίες που αναφέρθηκαν παραπάνω. Είναι ψηφιακά κρυπτογραφημένο από τον αποστολέα και αποκρυπτογραφείται και επαληθεύεται από τον παραλήπτη.

2.8 Pretty Good Privacy (PGP)

Το PGP διατίθεται δωρεάν για προσωπική χρήση, όμως απαιτείται άδεια για τη χρησιμοποίησή του σε εμπορικές εφαρμογές. Το Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT) λειτουργεί ως κέντρο προώθησης του λογισμικού που προορίζεται για προσωπική χρήση, σε συνεργασία με τον Zimmermann, ο οποίος ίδρυσε και μια ομώνυμη με το λογισμικό, εταιρία (Pretty Good Privacy, Inc.) για να προωθήσει την εμπορική έκδοση του λογισμικού

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.

Το PGP αποτελείται από τέσσερα στοιχεία κρυπτογράφησης και έναν αριθμό συστατικών μερών λογισμικού, συμβατών μεταξύ τους. Ο πυρήνας των μηχανισμών ασφάλειας είναι ο αλγόριθμος κρυπτογράφησης δεδομένων IDEA (International Data Encryption Algorithm), το σύστημα κρυπτογράφησης δημοσίου κλειδιού RSA για τη διαχείριση κλειδιών, η συνάρτηση κατακερματισμού MD5 και μια γεννήτρια τυχαίων αριθμών. Τα άλλα συστατικά του PGP υλοποιούν τυπικές λειτουργίες όπως, για παράδειγμα, αλληλεπίδραση με το χρήστη, διαχείριση αρχείων και συμπίεση δεδομένων.

Το PGP έχει μοναδικές ιδιότητες: Μπορεί να χρησιμοποιηθεί, όχι μόνο για να ασφαλίσει μηνύματα ηλεκτρονικού ταχυδρομείου, αλλά επίσης και για να κρυπτογραφήσει τοπικά αρχεία με το IDEA. Επιτρέπει οι ψηφιακές υπογραφές να διαχωρίζονται και να μεταβιβάζονται ξεχωριστά από τα μηνύματα στα οποία αναφέρονται. Συμπιέζει τα μηνύματα χρησιμοποιώντας το ευρέως διαδεδομένο πρόγραμμα ZIP. Η συμπίεση γενικά ελαττώνει το μέγεθος των μηνυμάτων και συνεπώς απομακρύνει τους πλεονασμούς στο μη κρυπτογραφημένο κείμενο. Σαν αποτέλεσμα, η συμπίεση κάνει την κρυπτοανάλυση πιο δύσκολη

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 μηνύματα e-mail είναι πολύ εύκολο να υποκλέπτουν 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.

Κινούμαστε προς ένα μέλλον όπου οι υπολογιστές διεθνώς θα ενώνονται με δίκτυα οπτικών ινών υψηλής χωρητικότητας. Το e-mail θα είναι κάτι το αυτονόητο για όλους και όχι η καινοτομία που θεωρείται σήμερα. Οι κυβερνήσεις θα προστατεύουν το e-mail των πολιτών με πρωτόκολλα σχεδιασμένα από τις ίδιες. Πιθανότατα οι περισσότεροι άνθρωποι θα συμβιβαστούν με αυτή τη λύση αλλά ίσως μερικοί προτιμήσουν να πάρουν τα δικά τους μέτρα ασφάλειας.

2.8.1 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.

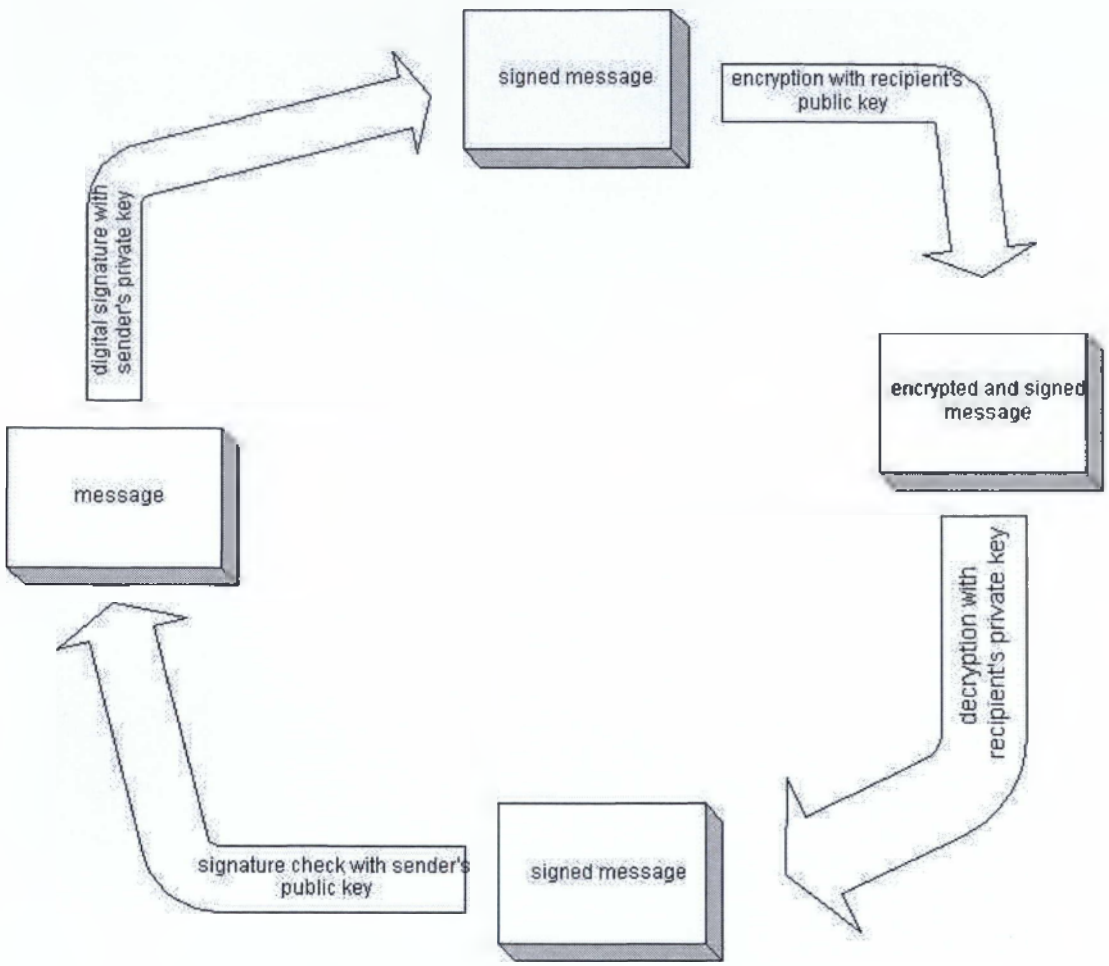
Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη ενός μηνύματος για να κρυπτογραφήσει ένα μήνυμα προς αυτό το άτομο ενώ ο παραλήπτης μπορεί να χρησιμοποιήσει με τη σειρά του το αντίστοιχο μυστικό κλειδί για να αποκρυπτογραφήσει το μήνυμα. Κανένας άλλος εκτός από τον παραλήπτη δεν μπορεί 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 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 κλειδί για να τρέξει τον γρήγορο συμβατικό αλγόριθμο ενός κλειδιού έτσι ώστε να αποκρυπτογραφήσει το κρυπτοκείμενο.

Η όλη διαδικασία φαίνεται στο παρακάτω σχήμα:



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 = συναρτήσεις κατακερματισμού τις λέμε) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολλή 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.

2.8.2 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. Ας εξετάσουμε το λόγο:

Ας υποθέσουμε ότι ο Bob θέλει να στείλει ένα προσωπικό μήνυμα στην Alice. Για να το κάνει αυτό κατεβάζει το πιστοποιητικό δημοσίων κλειδιών από κάποιο σύστημα ηλεκτρονικού πίνακα ανακοινώσεων (BBS). Κατόπιν, κρυπτογραφεί το γράμμα προς την Alice με αυτό δημόσιο κλειδί και το στέλνει σε αυτήν μέσω της λειτουργίας e-mail του BBS.

Ατυχώς, τόσο για τον αποστολέα (Bob) όσο και για την Alice κάποιος τρίτος χρήστης ας υποθέσουμε ο Charlie - έχει δημιουργήσει ένα δημόσιο κλειδί με το user

id της Alice και το έχει βάλει στη θέση του πραγματικού κλειδιού της Alice. Ο Bob χρησιμοποίησε αυτό το πλαστογραφημένο κλειδί για να κρυπτογραφήσει το μήνυμα προς την Alice αντί του αληθινού κλειδιού της Alice. Όπως φαίνεται όλα δείχνουν φυσιολογικά διότι το πλαστογραφημένο κλειδί έχει το user id της Alice. Έτσι ο Charlie μπορεί να αποκρυπτογραφήσει το μήνυμα που προοριζόταν για την Alice μια και έχει το κλειδί που αντιστοιχεί στο πλαστογραφημένο δημόσιο κλειδί της Alice. Όμως το πρόβλημα δεν τελειώνει εδώ. Ο Charlie μπορεί επιπλέον να επανακρυπτογραφήσει το μήνυμα και να το προωθήσει στην Alice οπότε κανείς δεν πρόκειται να υποπτευθεί τίποτα. Εάν θέλει, μπορεί να προχωρήσει στη δημιουργία ψηφιακών υπογραφών της Alice με το πλαστογραφημένο κλειδί μια και όλοι θα το χρησιμοποιούν για να ελέγχουν τις υπογραφές της.

Όπως τελικά φαίνεται ο κίνδυνος είναι πολύ μεγάλος. Ο μόνος τρόπος να αποτραπούν τέτοιες καταστάσεις είναι η αποφυγή της υποκλοπής και του μπερδέματος των δημοσίων κλειδιών. Εάν κάποιος έχει πάρει το δημόσιο κλειδί της Alice κατευθείαν από την ίδια τότε δεν υπάρχει πρόβλημα. Αυτό βέβαια μπορεί να είναι πολύ δύσκολο εάν η Alice είναι χιλιάδες χιλιόμετρα μακριά ή απλά προσωρινά απρόσιτη.

Μία διέξοδος σε αυτό το πρόβλημα είναι η χρήση κάποιου τρίτου κοινά αποδεκτού "φίλου" ο οποίος έχει στη κατοχή του ένα καλό αντίγραφο του δημόσιου κλειδιού της Alice. Για παράδειγμα ας θεωρήσουμε ότι αυτός είναι ο David ο οποίος μπορεί να υπογράψει το δημόσιο κλειδί της Alice με τη δικό του μυστικό κλειδί και να εγγυηθεί με αυτό το τρόπο την αυθεντικότητα του κλειδιού της Alice.

Αυτή η διαδικασία θα παρήγαγε ένα υπογεγραμμένο πιστοποιητικό δημόσιου κλειδιού που θα αποδείκνυε την ακεραιότητα του κλειδιού της Alice. Αυτή η διαδικασία ,βέβαια, προϋποθέτει την δυνατότητα ελέγχου του κλειδιού του David άρα την κατοχή ενός γνήσιου αντίγραφου του δημόσιου κλειδιού του. Ο David θα μπορούσε επιπλέον να στείλει στην Alice ένα υπογεγραμμένο αντίγραφο του δημόσιου κλειδιού του Bob. Με αυτό το τρόπο λειτουργεί σαν μεσάζοντας (introducer) μεταξύ του Bob και της Alice.

Το υπογεγραμμένο κλειδί για την Alice μπορεί να σταλεί από τον David ή την Alice στο BBS και από εκεί να το πάρει αργότερα όποιος το χρειαστεί. Αυτός το μόνο που θα χρειαστεί να κάνει, για να σιγουρευτεί για την ακεραιότητα του δημόσιου κλειδιού της Alice, είναι να την ελέγξει μέσω του δημόσιου κλειδιού του David. Κανένας δεν μπορεί να ξεγελάσει πλέον όποιον έχει το υπογεγραμμένο από τον David δημόσιο κλειδί της Alice διότι κανείς δεν μπορεί να πλαστογραφήσει την υπογραφή του David.

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 η Αχίλλειος φτέρνα 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. Με το να βάλουμε την υπογραφή μας σε ένα δημόσιο κλειδί για το οποίο ήμαστε σίγουροι δεν χάνουμε την αξιοπιστία μας ακόμα και αν αυτό ανήκει σε κάποιον ψυχοπαθή. Αυτό συμβαίνει διότι με την υπογραφή μας δεν λέμε τίποτα παραπάνω από το ότι αυτό το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει το ότι κάποιος μπορεί να εμπιστευθεί το κλειδί δεν έχει καμία σχέση με το αν μπορεί να εμπιστευθεί ή όχι τον ιδιοκτήτη του.

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 κοινή λογική. Ανάλογα εάν εμπιστευόμαστε την υπογραφή της Alice σε ένα δημόσιο κλειδί και η Alice με τη σειρά της εμπιστεύεται την υπογραφή του Charlie σε κάποιο άλλο κλειδί, αυτό δεν σημαίνει ότι και εμείς εμπιστευόμαστε την υπογραφή του Charlie σε εκείνο το κλειδί.

Θα ήταν καλή ιδέα, οι χρήστες να κρατούσαν το δημόσιο κλειδί τους μαζί με ένα σύνολο από πιστοποιητικά για αυτό 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.
Πρέπει να διασφαλίσουμε ότι κανένας δεν πρόκειται να αλλοιώσει το μπρελόκ με τα κλειδιά μας. Ο έλεγχος ενός νέου υπογεγραμμένου δημοσίου κλειδιού πρέπει να εξαρτάται ολοκληρωτικά από την ακεραιότητα των κλειδιών τα οποία ήδη έχουμε στο μπρελόκ μας και τα οποία φυσικά εμπιστευόμαστε. Πρέπει να διατηρούμε συνεχή φυσικό έλεγχο των μπρελόκ δημοσίων κλειδιών μας σε κάποιο PC εκτός δικτύου όπως ακριβώς θα κάναμε και με το μυστικό κλειδί μας. Επιπλέον πρέπει να κρατάμε ένα αντίγραφο του δημόσιου και μυστικού κλειδιού μας σε κάποιο προστατευμένο μέσο όπου αποκλείεται ποτέ να τα σβήσουμε κατά λάθος. Από τη στιγμή κατά την οποία το δημόσιο κλειδί μας χρησιμοποιείται ως ο τελικός κριτής για τη πιστοποίηση ή μη όλων των άλλων κλειδιών του μπρελόκ είναι σημαντική για την ασφάλεια όλου του συστήματος η διασφάλισή του. Το PGP μπορεί αυτόματα να συγκρίνει το δημόσιο κλειδί μας με ένα αντίγραφό του σε κάποιο προστατευμένο φυσικό μέσο.

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.

2.8.3 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:

- Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει(έχει πιστοποιηθεί από κάποιον του οποίου την υπογραφή εμπιστευόμαστε;)
- 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 και ποια όχι να υπογράψει. 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.

2.8.4 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 δισκέτας 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 (ένας Unix dial-in server) διότι μπορεί κάποιος που παρακολουθεί τις επικοινωνίες μέσω modem 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 καλλίτερα 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 επαναχρησιμοποίηση τους. Μπορούμε κατόπιν να

δημιουργήσουμε ένα νέο ζεύγος μυστικού/δημοσίου κλειδιού και να αρχίσουμε πλέον να δουλεύουμε με αυτά.

Βιβλιογραφία

- Email Security : Bruse Schneier
- Ασφάλεια Της Πληροφορικής : Εκδόσης Νέων Τεχνολογιών
- http://en.wikipedia.org/wiki/Spam_(electronic)
- http://www.dpa.gr/portal/page?_pageid=33,20908&_dad=portal&_schema=PORTAL
- http://www.honeyd.org/spam.php
- http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043
- http://en.wikipedia.org/wiki/Phishing
- http://www.hsbc.gr/1/2/el/information/online-security/phishing#top
- www.honeynet.org/papers/phishing
- www.antiphishing.org
- www.antiphishing.org/phishing_archive.html
- http://www.securitymanager.gr/it_security/protection_article.php?id=5&set=11&title=%CF%E9%20%D6%DC%F1%F3%E5%F2%20%C9%FE%ED%20(Virus%20Hoaxes)
- http://hoaxbusters.ciac.org
- http://www.hoaxbuster.com
- http://e-yliko.sch.gr/htmls/pc_use/smail.aspx
- www.tm.teiher.gr
- http://www.eeei.gr
- http://www.symantec.com/business/security_response/threatexplorer/risks/hoaxes.jsp
- http://shop.symantecstore.com/store/symnasmb/en_US/DisplayProductDetailsSmbPage/productID.68498500/ThemeID.106400/pgm.12858700?resid=S-kAHgoHAioAABamr1YAAAAJ&rests=1274609693311
- http://www.fortinet.com/solutions/antispam.html
- http://www.clearswift.com/products/mimesweeper-for-smtp
- http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
- http://www.m86security.com/products/email_security/mailmarshal-smtp.asp
- http://el.wikipedia.org/wiki/SMTP
- http://www.call-centre.cyta.com.cy/techinfo.htm
- http://el.wikipedia.org/wiki/Post_Office_Protocol
- http://www.securitymanager.gr/it_security/protection_article.php?id=3&set=13&title=%D4%EF%20%D0%F1%FC%E3%F1%E1%EC%EC%E1%20PGP%20(Pretty%20Good%20Privacy)
- http://en.wikipedia.org/wiki/Pretty_Good_Privacy
- http://e-pcmag.gr