Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**«Ασφάλεια Συστημάτων Ηλεκτρονικού Ταχυδρομείου»**
Ονοματεπώνυμο Φοιτητή	**ΖΑΛΜΑ ΚΩΝΣΤΑΝΤΙΝΑ**
Πατρώνυμο	**ΓΕΩΡΓΙΟΣ**
Αριθμός Μητρώου	**ΜΠΠΛ/09066**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Λέκτορας**

16/10/2014

Οκτώβριος 2014

Τριμελής Εξεταστική Επιτροπή		
(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα
Δρ. Κοτζανικολάου Παναγιώτης **Λέκτορας Τμήματος Πληροφορικής**	**Δουληγέρης Χρήστος** **Καθηγητής Τμήματος Πληροφορικής**	**Παπαδάκης Ιωάννης**

Περίληψη

Τα πρωτόκολλα επικοινωνίας τα οποία παρέχουν την υπηρεσία Ηλεκτρονικού Ταχυδρομείου (email), υποστηρίζουν την από άκρο σε άκρο αποστολή και παράδοση των μηνυμάτων, καθώς επίσης και την προτυποποίηση μίας κοινής μορφής μηνυμάτων. Το Ηλεκτρονικό Ταχυδρομείο αποτελεί ένα πανίσχυρο εργαλείο επικοινωνίας καθώς μπορεί να συμπεριλάβει εκτός από απλό κείμενο ήχο, σύνθετη πληροφορία όπως εικόνα και βίντεο. Η δυνατότητα άμεσης αποστολής μηνυμάτων με ανέξοδο, απλό και μαζικό τρόπο αναπόφευκτα οδηγεί σε εκμετάλλευση των δυνατοτήτων του email για κακόβουλη χρήση, όπως αποστολή μηνυμάτων με διαφημιστικό ή κακόβουλο περιεχόμενο ή μηνύματα που στόχο έχουν την παραπλάνηση του παραλήπτη. Η κρυπτογραφία είναι ένας πολύ αποτελεσματικός μηχανισμός που μπορεί να προστατέψει το Ηλεκτρονικό Ταχυδρομείο από την πλειοψηφία των απειλών που δέχεται. Στην παρούσα Μεταπτυχιακή Διατριβή γίνεται μια μελέτη των δομικών στοιχείων του Ηλεκτρονικού Ταχυδρομείου. Στην συνέχεια αναλύονται οι απειλές που εκμεταλλεύονται τις ευπάθειες των πρωτοκόλλων Ηλεκτρονικού Ταχυδρομείου και παρουσιάζονται μέτρα ασφάλειας, τόσο από πλευράς διακομιστή όσο και από πλευράς χρήστη. Τέλος διεξάγεται μία σειρά δοκιμών με σκοπό την δημιουργία μηχανισμών αποτελεσματικής αναχαίτισης αυτών των απειλών.

Abstract

Electronic mail communication protocols aim to provide email services with guaranteed end-to-end message delivery, as well as common formatting for different implementations. Email it is a powerful tool, since it can be used to exchange not only text messages but other more complex types of information, such as sound, image and video. The capabilities for instant and massive message exchange through an inexpensive communication medium, leads to exploitation of its capabilities by malicious users, for example for sending emails with malicious or unwanted content or messages intending to deceive the recipient. Cryptography is a very effective mechanism that can provide adequate security for the majority of threats targeting email. In this thesis the building blocks of email protocols are studied. Then the threats that exploit vulnerabilities of the email mechanism are analyzed and instructions are given on how to safeguard, both the server side and the end-user side. A series of practical experiments are presented, in order to evaluate the efficiency of the examined security controls against the examined threats.

Περιεχόμενα

1 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

1.1 ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ/ E-MAIL

Ηλεκτρονικό ταχυδρομείο ή ηλεκτρονική αλληλογραφία, ένας όρος που μεταφράζεται στην αγγλική γλώσσα ως: **Electronic mail** ή αλλιώς **e-mail** είναι η μέθοδος ανταλλαγής ψηφιακών μηνυμάτων από ένα συντάκτη-αποστολέα σε ένα ή περισσότερους παραλήπτες.

Η ηλεκτρονική αλληλογραφία έχει σκοπό την προώθηση μηνυμάτων μεταξύ μεγάλων αποστάσεων με στόχο την επικοινωνία των ανθρώπων με ανέξοδο και ασφαλή τρόπο διαμέσου του Διαδικτύου – Internet.

Πιο συγκεκριμένα το ηλεκτρονικό ταχυδρομείο e-mail είναι μια υπηρεσία του διαδικτύου για τη μετάδοση μηνυμάτων μεταξύ ηλεκτρονικών υπολογιστών. Τα μηνύματα μπορούν να παρέχουν πληροφορίες σε διάφορες μορφές. Μια ηλεκτρονική επιστολή έχει τη δυνατότητα να περιλαμβάνει, εκτός από κείμενο, εικόνες, ήχους, κινούμενες εικόνες-video, μια εφαρμογή, μέσα στο μήνυμα ή επισυναπτόμενα αρχεία. (Wikipedia, Email) (Γκρίτζαλης Δημήτρης, 2003)

Το email έχει γίνει μια από τις κινητήριες δυνάμεις πίσω από τη σύνδεση των επιχειρήσεων με το Διαδίκτυο. Τα Πλεονεκτήματα που προσφέρει το Ηλεκτρονικό Ταχυδρομείο είναι η γρήγορη και οικονομική μεταφορά των μηνυμάτων οπουδήποτε στον κόσμο. Όπως οι τοπικές τηλεφωνικές κλήσεις που είναι δωρεάν στις περισσότερες περιοχές των ΗΠΑ, έτσι και τα μηνύματα ηλεκτρονικού ταχυδρομείου που προορίζονται για μεγάλες αποστάσεις. Εκτός των ΗΠΑ, τοπικές κλήσεις τείνουν να είναι δαπανηρές ως εκ τούτου το σύστημα ηλεκτρονικού ταχυδρομείου μπορεί να μειώσει τον λογαριασμό του τηλεφώνου σημαντικά. (Vicomsoft, 2002)

Η σημαντική αυτή μείωση του κόστους έχει ενθαρρύνει πολλές επιχειρήσεις να επενδύσουν σε εφαρμογή των υπηρεσιών e-mail. Επίσης η τεχνολογία του e-mail αντιμετωπίζει με ενιαίο μηχανισμό και για τα μικρά μηνύματα αλλά και για τα πολύ ογκώδη, αυτός είναι και ένας άλλος λόγος που οι περισσότεροι χρήστες προτιμούν την αποστολή αρχείων μέσα από το ηλεκτρονικό ταχυδρομείο παρά με πρωτόκολλα μεταφοράς αρχείων (FTP). (Comer, 2001 4η Αμερικάνικη Έκδοση) (Wikipedia, Email)

Τα Email έχουν σημαντικά οφέλη πέρα από τα παραδοσιακά σημειώματα σε χαρτί και τις υπηρεσίες του κλασσικού ταχυδρομείου:

- Τα μηνύματα μπορούν να αποστέλλονται ανά πάσα στιγμή, σε όλο τον κόσμο τόσο εύκολα σε μια ομάδα ανθρώπων ή ένα μόνο παραλήπτη, χωρίς ο αποστολέας να απομακρυνθεί από το γραφείο του.
- Τα μηνύματα μπορούν να αποθηκεύονται εξασφαλίζοντας έτσι κάποια μορφή καταγραφής-αρχείου , ή αποθηκεύονται στην περίπτωση που ο παραλήπτης απουσιάζει.
- Ο παραλήπτης μπορεί να συλλέξει την αλληλογραφία του, όταν το θελήσει, από όπου κι αν βρίσκεται.
- Αυτό είναι πλέον εφικτό και με την χρήση μίας απλής τηλεφωνικής συσκευής.
- Η αποστολή ενός e-mail είναι άμεση χωρίς την προσπέλαση τρίτων.
- Η αποστολή ενός e-mail είναι φιλική προς το περιβάλλον! Καθώς δεν απαιτείται χαρτί για την αποθήκευση των e-mail παρά λίγος χώρος στο δίσκο του υπολογιστή. (Vicomsoft, 2002)

Μία έρευνα από την Pew Internet & American Life έδειξε ότι η αποστολή/ανάγνωση e-mail παραμένει η πιο δημοφιλής δραστηριότητα των χρηστών με ποσοστό 93%.

Αρχικά το ηλεκτρονικό ταχυδρομείο/e-mail ήταν ιδιόκτητες υπηρεσίες καθώς μπορούσαν να επικοινωνήσουν χρήστες μίας επιχείρησης ή ενός γραφείου που διέθεταν

υπολογιστές που ήταν εξοπλισμένοι με το ίδιο ακριβώς λειτουργικό σύστημα. Με την επικράτηση όμως του Internet στις επιχειρήσεις καθώς και στην καθημερινή ζωή οι κατασκευαστές των ιδιόκτητων αυτών συστημάτων ηλεκτρονικού ταχυδρομείου εισήγαγαν τη δυνατότητα σύνδεσης αυτών των συστημάτων και της μεταφοράς μηνυμάτων και εκτός του τοπικού δικτύου. Αυτό πήρε τη μορφή μίας εφαρμογής λογισμικού που μετέτρεπε τα μηνύματα ενός τοπικού δικτύου σε ένα αναγνωρισμένο πρότυπο κατάλληλο για μεταφορά μέσω του Διαδικτύου.

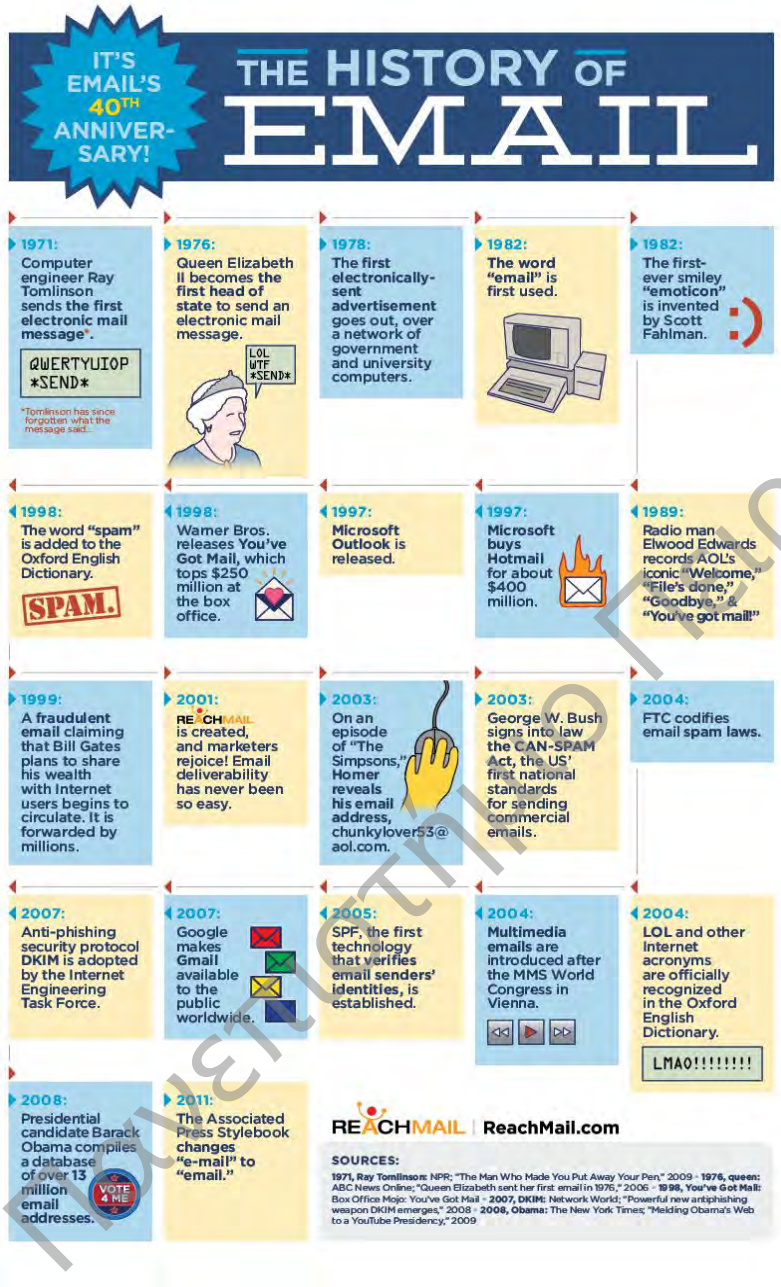
Με την επικράτηση του Internet οι περισσότερες επιχειρήσεις κινούνται πάνω σε διεθνή πρότυπα Διαδικτύου για τοπικές ταχυδρομικές υπηρεσίες δικτύου.

Αυτό έχει τα πλεονεκτήματα ότι συνήθως είναι λιγότερο ακριβά, πιο απλά, δεν συνδέονται πλέον να με ένα συγκεκριμένο προμηθευτή επιτρέποντας ταυτόχρονα σε έναν IT Manager να έχει ευρύτερη επιλογή για εφαρμογές email client ή διαφορετικές πλατφόρμες υλικού. (Vicomsoft, 2002)

Το ηλεκτρονικό ταχυδρομείο/e-mail είναι αρκετά μεταγενέστερο από το ARPAnet ή το Internet. Οι πρώτες μορφές email ήταν απλώς μια παραλλαγή των σύγχρονων file directory-καταλόγου αρχείων. Δηλαδή τοποθετώντας ένα μήνυμα στον κατάλογο κάποιου άλλου χρήστη σε ένα σημείο όπου δεν θα μπορεί να το δει αν δεν είναι συνδεδεμένος μέσα στο σύστημα. Ακριβώς όπως και αφήνοντας ένα σημείωμα στο γραφείο κάποιου.

Πιθανώς τα πρώτα συστήματα ηλεκτρονικού ταχυδρομείου αυτού του τύπου ήταν γραμματοκιβώτια, που χρησιμοποιούσαν στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης το 1965. Ένα άλλο πρόγραμμα που χρησιμοποιούσαν πρωτύτερα για να στείλουν μηνύματα στον ίδιο υπολογιστή ονομαζόταν **SNDMSG**.

Μερικοί από τους κεντρικούς υπολογιστές -mainframe της εποχής είχαν ένα όριο μέχρι εκατό χρήστες και συχνά χρησιμοποιούσαν τα λεγόμενα «κουτά τερματικά" για να έχουν πρόσβαση στο mainframe. Τα κουτά τερματικά συνδέονταν μόνο με το mainframe , δεν είχαν χώρο για αποθήκευση ή μνήμη και εκτελούσαν όλες τις εργασίες στον απομακρυσμένο κεντρικό υπολογιστή.



Εικόνα 1: Η πορεία του email μέχρι σήμερα

πηγή εικόνας: http://en.inmoreau.com/654/infografic-the-history-of-email/

1.2 Δικτυα Μεταγωγης (Switching)

Οι πρώτες υπηρεσίες Ηλεκτρονικού Ταχυδρομείου απαιτούσαν ο αποστολέας και ο παραλήπτης να είναι online ταυτόχρονα για να ανταλλάξουν μηνύματα. Τα σημερινά συστήματα Ηλεκτρονικού Ταχυδρομείου βασίζονται στην τεχνική **store and forward** (αποθήκευση και προώθηση) που είναι βασικό χαρακτηριστικό των Δικτύων Μεταγωγής Μηνυμάτων (Message Switching). Σε αυτό το σημείο είναι απαραίτητο να γίνει αναφορά στα εν λόγω δίκτυα.

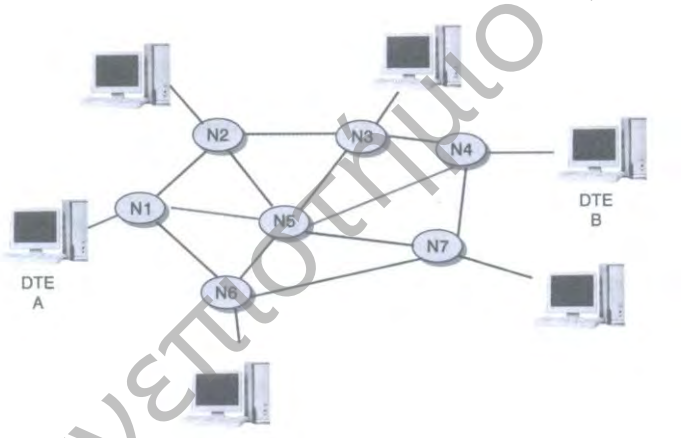
Στα δίκτυα μεταγωγής, η πληροφορία δρομολογείται μέσω των κόμβων που τα αποτελούν. Συνήθως υπάρχουν περισσότεροι του ενός εναλλακτικοί δρόμοι για να φτάσει η πληροφορία στον προορισμό της για λόγους αποτελεσματικότητας και αξιοπιστίας. Η Μεταγωγή σαν τεχνική είναι γνωστή από το τηλεφωνικό δίκτυο και διακρίνεται σε:

- Μεταγωγή Κυκλώματός (Circuit Switching)
- Μεταγωγή Μηνυμάτων (Message Switching)
- Μεταγωγή Πακέτων (Packet Switching)

(Μαργαρίτη, 2007)

1.2.1 Μεταγωγη Κυκλωματος (Circuit Switching)

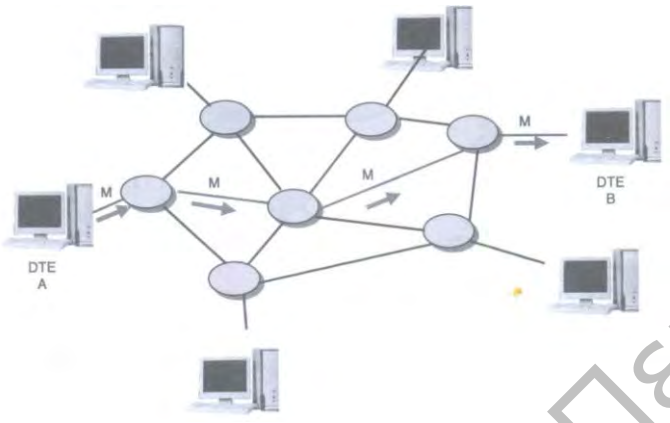
Όπως φανερώνεται και από τον ορισμό στην τεχνική με μεταγωγή κυκλώματος υπάρχουν τερματικά και οι κόμβοι. Για την επικοινωνία ενός τερματικού με ένα άλλο, αφιερώνεται μια φυσική ζεύξη μεταξύ τους – ένας «νοητός δρόμος» από το ένα τερματικό μέχρι το άλλο, καθ' όλη την διάρκεια επικοινωνίας ακόμη και αν υπάρχουν νεκρά διαστήματα. Κλασσικό παράδειγμα αυτής της τεχνικής αποτελεί το τηλεφωνικό δίκτυο. (Μαργαρίτη, 2007)



Εικόνα 2: Circuit Switching πηγή εικόνας: (Μαργαρίτη, 2007)

1.2.2 Μεταγωγη Μηνυματων (Message Switching)

Στην Μεταγωγή Μηνυμάτων, η προς αποστολή πληροφορία οργανώνεται σε μηνύματα (messages), τα οποία παραδίδονται στο δίκτυο για διεκπεραίωση. Το δίκτυο αναλαμβάνει **την προώθηση των μηνυμάτων (messages) από κόμβο σε κόμβο** ως το τελικό παραλήπτη του οποίου η διεύθυνση συμπεριλαμβάνεται στο μήνυμα.



Εικόνα 3: Message Switching πηγή εικόνας: (Μαργαρίτη, 2007)

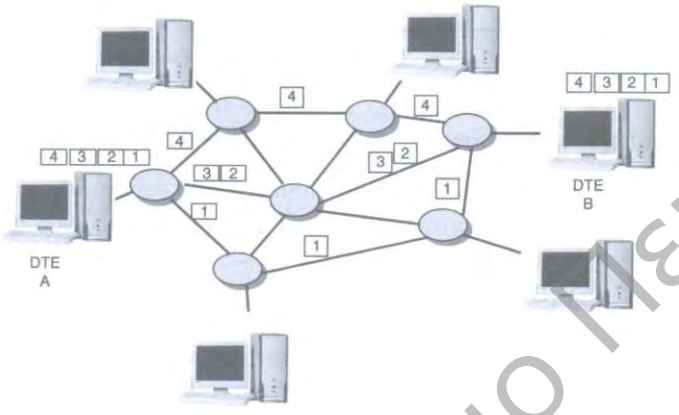
Η τεχνική αυτή είναι γνωστή και ως **store and forward** (αποθήκευση και προώθηση), πλεονεκτεί σε σχέση με την προηγούμενη στο ότι εξαλείφονται τα νεκρά διαστήματα και δεν απαιτείται οι τερματικοί σταθμοί που επικοινωνούν να είναι και οι δύο παρόντες ταυτόχρονα. (Μαργαρίτη, 2007)

Αναλυτικότερα η **store and forward** (αποθήκευση και προώθηση) είναι μία τεχνική στα συστήματα τηλεπικοινωνιών όπου η πληροφορία στέλνεται σε έναν ενδιάμεσο κόμβο όπου αποθηκεύεται εκεί προσωρινά και αργότερα στέλνεται στον τελικό κόμβο-παραλήπτη ή σε κάποιο άλλο ενδιάμεσο κόμβο. Ο ενδιάμεσος σταθμός ή κόμβος που ανήκει σε ένα δίκτυο εξασφαλίζει την ακεραιότητα του μηνύματος πριν το προωθήσει (έλεγχος σφαλμάτων) επίσης τα μηνύματα που ανταλλάσσονται μπορεί να είναι σε διαφορετικό κώδικα ή να έχουν διαφορετική ταχύτητα.

Σε γενικές γραμμές η τεχνική αυτή χρησιμοποιείται για δίκτυα που δεν είναι real time ή που έχουν αυξημένη κινητικότητα. Η εκμετάλλευση των γραμμών είναι καλύτερη και είναι δυνατή η πολλαπλή αποστολή μηνύματος σε πολλούς χρήστες. Μπορεί επίσης να είναι προτιμότερη σε περιπτώσεις όπου υπάρχει μεγάλη καθυστέρηση στη μεταφορά , υψηλά ποσοστά σφαλμάτων ή όταν οι τελικοί κόμβοι δεν είναι διαθέσιμοι. Αυτή η τεχνική ουσιαστικά προέρχεται από δίκτυα ανοχής της καθυστέρησης όπου αυτά τα δίκτυα δεν υποστηρίζουν real-time εφαρμογές. (Wikipedia, Email)' (Μαργαρίτη, 2007)

1.2.3 Μεταγωγη Πακετων (Packet Switching)

Στην μέθοδο αυτή έγινε μια προσπάθεια για να αξιοποιηθούν τα πλεονεκτήματα από τις δύο προηγούμενες τεχνικές. Το κάθε μήνυμα τεμαχίζεται σε πακέτα τα οποία στέλνονται στον προορισμό τους γενικώς μέσω διαφορετικών δρόμων. Η προώθηση των πακέτων γίνεται είτε με την μέθοδο Datagram όπου τα πακέτα στέλνονται με διαφορετική σειρά και από διαφορετικό δρόμο που είναι ο πιο σύντομος κάθε φορά και τοποθετούνται στην σειρά από τον παραλήπτη. Είτε γίνεται με την μέθοδο **Virtual Circuit** όπου πριν την αποστολή γίνεται μια νοητή σταθερή σύνδεση μεταξύ αποστολέα και παραλήπτη και τα πακέτα στέλνονται μέσω αυτής. Οι δύο μέθοδοι παριστάνονται στις επόμενες εικόνες: (Μαργαρίτη, 2007)



Εικόνα 4 : Packet Switching πηγή εικόνας: (Μαργαρίτη, 2007)

1.3 Αρχιτεκτονικη του Ηλεκτρονικου Ταχυδρομειου

Για να περιγραφεί η αρχιτεκτονική των email θα αναλυθούν οι όροι email agent καθώς και 4 σενάρια. Ξεκινώντας από την απλούστερη κατάσταση και θα προστίθενται λειτουργίες στην συνέχεια. Το τέταρτο σενάριο είναι και το πιο συνηθισμένο στην ανταλλαγή email .

1.3.1 E-mail Agent

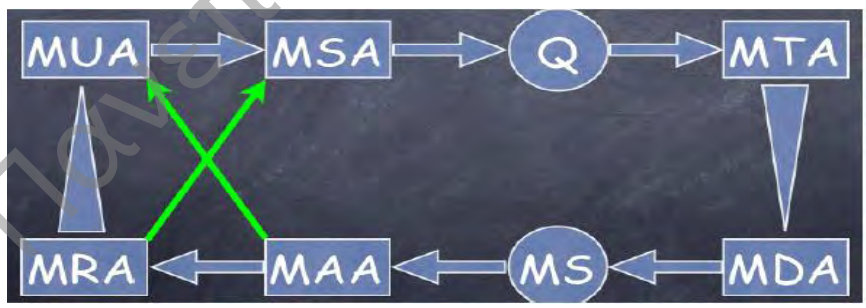
Ένας email agent είναι ένα πρόγραμμα που αποτελεί ένα μέρος της υποδομής του ηλεκτρονικού ταχυδρομείου. Πρόκειται για έναν τεχνικό όρο που περιγράφει τις λειτουργίες που επιτελούνται από διάφορα προγράμματα στην διαδικασία του ηλεκτρονικού ταχυδρομείου. Πιο συγκεκριμένα ένα πρόγραμμα ονομάζεται με βάση τις διάφορες λειτουργίες που εκτελεί π.χ. εάν ένας mail agent είναι υπεύθυνος για την μεταφορά του email αναφέρεται ως **mail transfer agent.**

Αν και μεμονωμένα οι όροι αυτοί χρησιμοποιούνται ευρέως στα πρότυπα του διαδικτύου και των RFC†, παρόλο αυτά δεν υπάρχει ένας γενικός όρος που να περικλείει όλα αυτά τα προγράμματα. Ανεπίσημα έχει δοθεί ο γενικός όρος **mail agents** καθώς και τα ακρωνύμια **MxA**, όπου το «x» παίρνει το όνομα του συγκεκριμένου προγράμματος που αναφέρεται όπως **MUA** και **MTA**.

Οι πιο γνωστοί είναι ο **mail user agent**- **MUA** ή **e-mail client** και οι **mail transfer agent -MTA** προγράμματα που μεταφέρουν email μεταξύ των email clients, αλλά συνολικά υπάρχουν έξι κατηγορίες.

I. Mail user agent (MUA)
II. Mail transfer agent (MTA)
III. Message Access Agent (MAA)
IV. Mail delivery agent (MDA)
V. Mail retrieval agent (MRA)
VI. Mail submission agent (MSA)
(Koymans, 2010)

Η διάκριση που γίνεται σε αυτές τις κατηγορίες είναι από την πλευρά του client (MUA) **και** από την πλευρά του **server** (MTA) (Wikipedia, Message transfer agent). Το παρακάτω διάγραμμα ροής δείχνει την σχέση που έχουν μεταξύ τους **:** (Koymans, 2010)



Εικόνα 5 : «mail user agents» πηγή εικόνας: https://www.os3.nl/_media/2010-2011/courses/cia/week3/email_handout.pdf

†**Requests for Comments (RFC)** είναι μια σειρά κειμένων και σημειώσεων για την τεχνική και την οργάνωση που διέπουν το Internet. Οι σημειώσεις μέσα στις σειρές RFC, αφορούν πολλά θέματα πάνω στη **δικτύωση υπολογιστών, συμπεριλαμβανομένων πρωτοκόλλων**, **διαδικασιών, προγραμμάτων, ιδεών,** και **απόψεων**. Τα επίσημα έγγραφα προδιαγραφών της σουίτας πρωτοκόλλου Διαδικτύου που καθορίζονται από την Internet Engineering Task Force, IETF και την Internet Engineering Steering Group, IESG)καταγράφονται και δημοσιεύονται ως **πρότυπα**

RFCs. **Κατά συνέπεια, η διαδικασία δημοσιεύσεων RFC παίζει έναν σημαντικό ρόλο στη διαδικασία προτύπων Διαδικτύου.** (Wikipedia, Email)

1.3.2 Πρόγραμμα-πελάτης / Email-client- Mail User Agent (MUA)

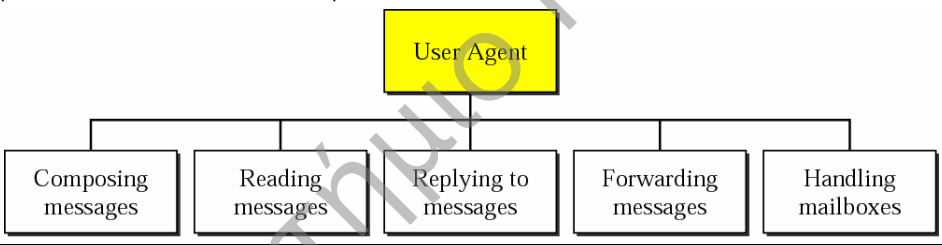
Ένα πρόγραμμα πελάτη-**client** ηλεκτρονικού ταχυδρομείου ή αλλιώς έναν αναγνώστη email είναι γνωστό και ως **mail user agent (MUA)** είναι ένα πρόγραμμα υπολογιστή που χρησιμοποιείται για πρόσβαση και διαχείριση των email του χρήστη. Ο όρος αναφέρεται σε κάθε σύστημα που μπορεί να έχει πρόσβαση σε ένα ηλεκτρονικό γραμματοκιβώτιο –**mailbox** του χρήστη, ανεξάρτητα ένα είναι mail user agent (MUA), ένας διακομιστής αλληλογραφίας, ή ένας χρήστης σε ένα τερματικό.

Δημοφιλέστεροι email clients είναι το **Microsoft Outlook**, το **Lotus Notes** της **IBM**, το **Pegasus Mail**, το **Thunderbird** της **Mozilla** και το **Mail** της **Apple Inc**.

Επίσης, email client μπορεί να θεωρείται μια διαδικτυακή εφαρμογή που παρέχει τη διαχείριση μηνυμάτων, σύνθεση και ανάγνωση νέων μηνυμάτων, που όμως πιο συχνά εμφανίζεται με τον όρο **webmail**.(όρος που θα αναλυθεί παρακάτω) Με απλά λόγια ο όρος email client είναι η διεπαφή συστήματος του χρήστη με τα e-mail. (Vicomsoft, 2002) (Wikipedia, Email client)

Υπηρεσίες που παρέχονται από έναν user agent:

Όπως προαναφέρθηκε ένας user agent είναι ένα πακέτο λογισμικού που δημιουργεί, διαβάζει, απαντά και προωθεί μηνύματα. Η εικόνα 6 παρουσιάζει τις υπηρεσίες ενός τυπικού user agent**.** (Behrouz A. Forouzan, 2005)



Εικόνα 6 : «Οι υπηρεσίες που προσφέρονται από έναν MUA» πηγή εικόνας: Behrouz A. Forouzan, 2005

Για να γίνει πιο κατανοητή η λειτουργία των mail user agent θα περιγραφεί ένα σενάριο:

- **Πρώτο Σενάριο**

Δεδομένα:

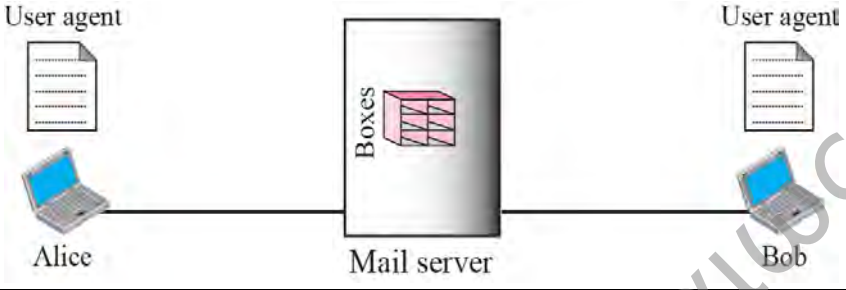
- Ένας αποστολέας,
- ένας παραλήπτης του email
- και οι δύο είναι χρήστες (ή προγράμματα εφαρμογής) στο ίδιο σύστημα και συνδέονται απευθείας με ένα κοινό σύστημα.

Ο διαχειριστής έχει δημιουργήσει ένα γραμματοκιβώτιο για κάθε χρήστη όπου αποθηκεύονται τα ληφθέντα μηνύματα. Ένα γραμματοκιβώτιο αποτελεί μέρος ενός τοπικού σκληρού δίσκου. Είναι ένα ειδικό αρχείο με περιορισμένα δικαιώματα. Μόνο ο χρήστης του γραμματοκιβωτίου έχει πρόσβαση σε αυτό.

Βήματα:

1. Όταν η Alice πρέπει να στείλει ένα μήνυμα στον Bob, εκτελεί ένα πρόγραμμα *user agent* για να προετοιμάσει το μήνυμα και για να το αποθηκεύσει στο γραμματοκιβώτιο του Bob.

2. Το μήνυμα έχει τις διευθύνσεις γραμματοκιβωτίου του αποστολέα και του παραλήπτη.
3. Ο Bob μπορεί να ανακτήσει και να διαβάσει τα περιεχόμενα του γραμματοκιβωτίου του όποτε θέλει, χρησιμοποιώντας και αυτός με την σειρά του έναν *user agent*. Η εικόνα αναπαριστά αυτό το σενάριο.



Εικόνα 7 : «Mail Server» πηγή εικόνας: Behrouz A. Forouzan, 2005

Αυτό μοιάζει με την παραδοσιακή ανταλλαγή σημειωμάτων μεταξύ υπαλλήλων σε ένα γραφείο. Υπάρχει ένα δωμάτιο αλληλογραφίας όπου κάθε υπάλληλος διαθέτει ένα γραμματοκιβώτιο με το όνομα του, όταν η Alice πρέπει να στείλει ένα σημείωμα στον Bob, γράφει το σημείωμα και το τοποθετεί στο γραμματοκιβώτιο του Bob. Όταν ο Bob ελέγχει το γραμματοκιβώτιο του, βρίσκει το σημείωμα της Alice και το διαβάζει. (Behrouz A. Forouzan, 2005)

Όταν ο αποστολέας και ο παραλήπτης ενός email βρίσκονται στο ίδιο σύστημα, χρειαζόμαστε μόνο δύο user agent.

1.3.3 Message Transfer Agent (MTA)

Ο **message transfer agent** (πράκτορες μεταφοράς μηνύματος) ή αλλιώς **mail transfer agent** (**MTA**) ή **mail relay** είναι λογισμικό που μεταφέρει μηνύματα ηλεκτρονικού ταχυδρομείου από έναν υπολογιστή σε έναν άλλο χρησιμοποιώντας το πρότυπο πελάτη-διακομιστή /client-serve. Ένας MTA ενεργοποιεί ταυτόχρονα και την πλευρά τόσο του πελάτη**-client** (για αποστολή email) όσο και την πλευρά του εξυπηρετητή- **server** (για λήψη email) μίας και οι δύο αποτελούν τμήματα του πρωτόκολλου μεταφοράς αλληλογραφίας **SMTP** που θα αναλυθεί σε επόμενο κεφάλαιο.

Οι όροι **mail server** , **mail exchanger** -ανταλλαγή αλληλογραφίας, και **MX host** μπορεί επίσης να αναφέρονται και για έναν υπολογιστή που εκτελεί μία mail transfer agent λειτουργία. Το σύστημα **Domain Name (DNS),** αντιστοιχίζει έναν **mail server** σε έναν τομέα-domain σύμφωνα με τις πληροφορίες/εγγραφές/records που ανακτά από έναν **mail exchanger (MX)** (ανταλλαγή αλληλογραφίας) που περιέχει το domain name ενός host παρέχοντας υπηρεσίες MTA. Οι συγκεκριμένοι όροι αναλύονται στο 2^{ο} κεφάλαιο.

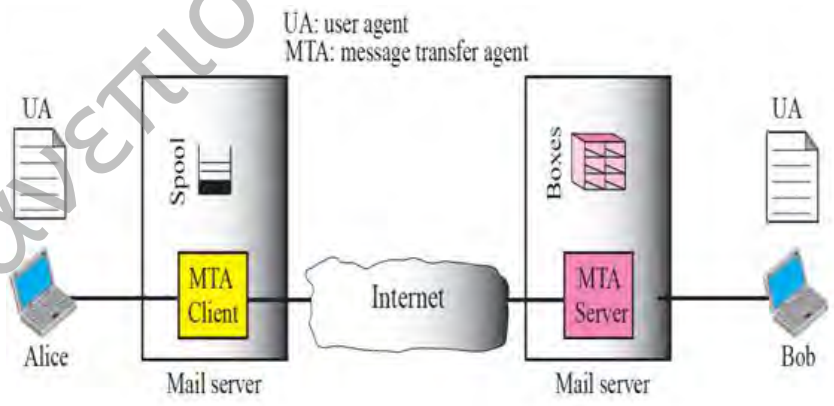
Ο mail server είναι ένας υπολογιστής που λειτουργεί ως ένα ηλεκτρονικό ταχυδρομείο για τα email. Τα Mail διατρέχουν το δίκτυο διαπερνόντας τους mail servers που εκτελούν ένα ειδικά σχεδιασμένο λογισμικό. Αυτό το λογισμικό είναι σχεδιασμένο σύμφωνα με τυποποιημένα πρωτόκολλα που είναι υπεύθυνα για το χειρισμό των μηνυμάτων ηλεκτρονικού ταχυδρομείου. (Wikipedia, Message transfer agent)

Για να γίνει και εδώ πιο κατανοητή η λειτουργία των message transfer agents θα περιγραφεί ένα δεύτερο σενάριο:

- **Δεύτερο Σενάριο**

Δεδομένα:

- Ένας αποστολέας,
- ένας παραλήπτης του email
- οι χρήστες (ή προγράμματα εφαρμογής) είναι σε δύο διαφορετικά συστήματα.
- Άρα το μήνυμα πρέπει να σταλεί μέσω Internet.



Εικόνα 8: «Mail Transfer Agent» πηγή εικόνας: Behrouz A. Forouzan, 2005

Σε αυτή τη περίπτωση χρειάζεται user agents και message transfer agents (MTA) όπως φαίνεται στην εικόνα 8:

Βήματα:

1. Η Alice πρέπει να χρησιμοποιήσει ένα πρόγραμμα user agent για να στείλει το μήνυμα του Bob στο σύστημα στο δικό της site.
2. Το σύστημα (που μερικές φορές λέγεται και mail exchanger) στο δικό της site χρησιμοποιεί μια ουρά για να αποθηκεύσει τα μηνύματα προς αποστολή (store and forward).
3. Ο Bob επίσης χρειάζεται έναν user agent για να ανακτά μηνύματα που έχουν αποθηκευτεί στο γραμματοκιβώτιο του δικού του συστήματος στο δικό του site.
4. Το μήνυμα όμως, πρέπει να σταλεί μέσω Internet από το site της Alice στο site του Bob.Εδώ χρειάζονται δύο message transfer agents: ένας client και ένας server.

Όπως τα περισσότερα προγράμματα client- server στο Internet, ο server πρέπει να εκτελείται συνέχεια επειδή δεν γνωρίζει πότε ένας client θα αιτηθεί σύνδεση. Ο client, από την άλλη , μπορεί να εκτελεστεί από το σύστημα όταν υπάρχει μήνυμα στην ουρά που πρέπει να σταλεί. (Behrouz A. Forouzan, 2005)

Όταν ο αποστολέας και ο παραλήπτης ενός email βρίσκονται σε διαφορετικά συστήματα , χρειαζόμαστε δύο UA και MTA (client και server).

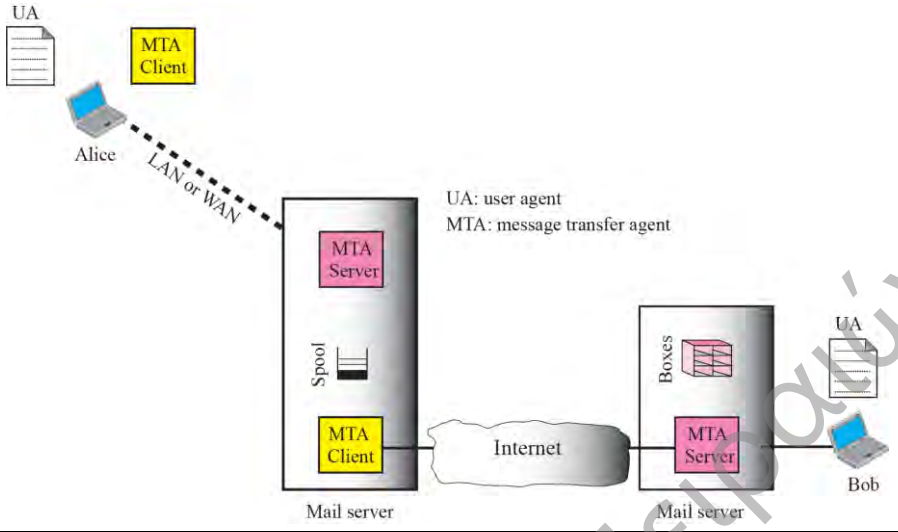
Επίσης θα παραθέσουμε και ένα τρίτο σενάριο που γίνεται πάλι χρήση **των message transfer agents** αλλά αυτή την φορά χρειάζονται δύο transfer agents καθώς ο ένας χρήστης συνδέεται μέσω ενός **LAN ή WAN.**

- **Τρίτο Σενάριο**

Δεδομένα:

- Ένας αποστολέας,
- ένας παραλήπτης του email
- Ο Bob συνδέεται όπως και στο δεύτερο σενάριο απευθείας στο σύστημα του.
- Η Alice όμως έχει διαχωριστεί από το σύστημα της και συνδέεται μέσω point to point WAN- όπως dial-up modem, ένα DSL ή ένα καλωδιακό modem- ή συνδέεται σε ένα LAN σε ένα οργανισμό που χρησιμοποιεί ένα server αλληλογραφίας για χειρισμό των μηνυμάτων.
- Όλοι οι χρήστες πρέπει να στέλνουν τα μηνύματα τους σε αυτόν τον server αλληλογραφίας.
- Η Alice εξακολουθεί να χρειάζεται έναν user agent για να προετοιμάσει το μήνυμα της.
- Για να στείλει η Alice το μήνυμα μέσω LAN ή WAN που αυτό γίνεται με ένα ζεύγος MTA (client και server).

Η εικόνα xx δείχνει τη κατάσταση.



Εικόνα 9: «MTA σε ένα LAN ή WAN» πηγή εικόνας: Behrouz A. Forouzan, 2005

Βήματα:

1. Η Alice για να στείλει ένα μήνυμα καλεί τον user agent, το οποίο με τη σειρά του καλεί το MTA client.
2. Ο MTA client ιδρύει μία σύνδεση με το MTA server στο σύστημα , η οποία εκτελείται συνέχεια.
3. Το σύστημα στο site της Alice τοποθετεί σε ουρά όλα τα μηνύματα που λαμβάνει.
4. Μετά χρησιμοποιεί ένα MTA client για να στείλει τα μηνύματα στο σύστημα στο site του Bob και το σύστημα δέχεται το μήνυμα και το αποθηκεύει στο γραμματοκιβώτιο του Bob.
5. Όποτε ο Bob θέλει χρησιμοποιεί και αυτός με τη σειρά του τον user agent για να ανακτήσει το μήνυμα και να το διαβάσει.

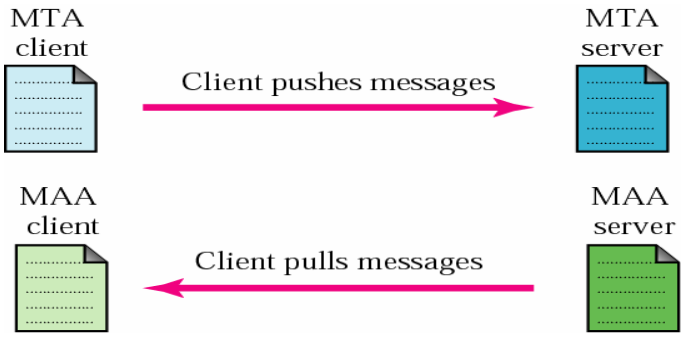
Να σημειωθεί ότι χρειάζονται 2 ζεύγη προγραμμάτων MTA client- server. (Behrouz A. Forouzan, 2005)

1.3.4 Mail Access agent (MAA)

Όταν ο αποστολέας συνδέεται με το server αλληλογραφίας μέσω ενός LAN ή WAN, χρειαζόμαστε δύο UA και δύο ζεύγη MTA (client και server).

Ο **mail access agent** ή αλλιώς **message access agent (MAA)**- πράκτορες πρόσβασης μηνύματος είναι μια και αυτά προγράμματα client- server τα οποία είναι υπεύθυνα για την ανάκτηση του μηνύματος. Ένας **message access agent** προσφέρει υπηρεσίες πρόσβασης ηλεκτρονικού ταχυδρομείου μέσω του MUA (ή του MRA).

Αυτά τα προγράμματα πρόσβασης μηνυμάτων χρειάζονται διότι ένα πρόγραμμα MTA client- server είναι ένα πρόγραμμα ***push (ώθησης)*** δηλαδή ο client ωθεί το μήνυμα στο server. Ο παραλήπτης του μηνύματος χρειάζεται ένα πρόγραμμα ***pull (εξαγωγής)*** δηλαδή ο client πρέπει να εξάγει το μήνυμα από το server. Η εικόνα xx δείχνει τη διαφορά.



Εικόνα 10: «Εξαγωγή εναντίον ώθησης» πηγή εικόνας: Behrouz A. Forouzan, 2005

Σε αυτό το σημείο ένα τέταρτο και τελευταίο σενάριο θα περιγραφεί για την λειτουργία και την χρησιμότητα των **MAA** το οποίο είναι και το πιο σύνηθες σενάριο επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου:

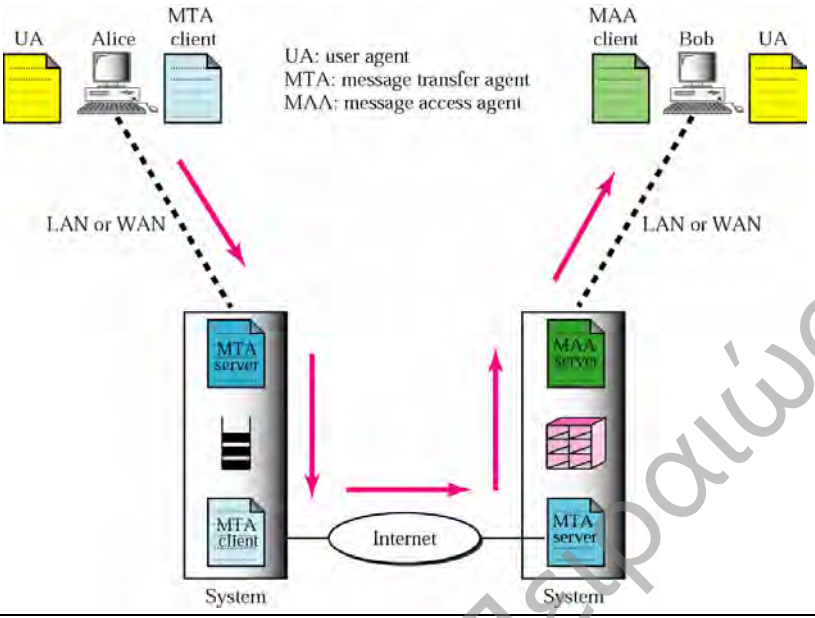
- **Τέταρτο Σενάριο**

Δεδομένα:

- Ο Bob και η Alice συνδέονται όπως με server αλληλογραφίας μέσω LAN ή WAN.

Βήματα:

1. Αφού το μήνυμα φτάσει στο server αλληλογραφίας του Bob , ο Bob πρέπει να το ανακτήσει.
2. Ο Bob χρησιμοποιεί ένα **MAA** client για να ανακτήσει τα μηνύματα του.
3. Ο client στέλνει μια αίτηση στο **MAA** server, ο οποίος εκτελείται συνέχεια και αιτείται τη μεταφορά των μηνυμάτων. Η κατάσταση παρουσιάζεται στην εικόνα xx:



Εικόνα 11: «Mail Agents» πηγή εικόνας: Behrouz A. Forouzan, 2005

- Υπάρχουν δύο σημαντικά σημεία που πρέπει να τονίσουμε:
  a. Ο Bob δεν μπορεί να παρακάμψει το server αλληλογραφίας και να χρησιμοποιήσει το **MTA** server απευθείας θα πρέπει να εκτελεί το **MTA** server συνέχεια επειδή δεν γνωρίζει πότε θα φτάσει ένα μήνυμα. Αυτό σημαίνει ότι ο Bob πρέπει να έχει ανοιχτό τον υπολογιστή του συνέχεια αν είναι συνδεδεμένος μέσω LAN. Αν είναι WAN συνδεδεμένος μέσω πρέπει να κρατάει ανοιχτή τη σύνδεση συνέχεια. Καμία από τις δύο περιπτώσεις δεν είναι εφικτή σήμερα.
  b. Δεύτερον ο Bob χρειάζεται ένα ζεύγος προγραμμάτων client- server : τα προγράμματα πρόσβασης μηνυμάτων **MAA** για να εξάγει – pull τα μηνύματα από τον server. (Behrouz A. Forouzan, 2005)

Όταν ο αποστολέας και ο παραλήπτης συνδέονται στο server αλληλογραφίας μέσω ενός LAN ή WAN, χρειαζόμαστε δύο UA και δύο ζεύγη MTA (client και server) και ένα ζεύγος MAA(client και server). Αυτή είναι η πιο συνηθισμένη σήμερα.

1.3.5 Mail delivery agent (MDA)

Ένας **mail delivery agent** ή **message delivery agent** (πράκτορας παράδοσης ταχυδρομείου) **(MDA)** είναι ένα στοιχείο λογισμικού που είναι υπεύθυνο για την παράδοση των μηνυμάτων ηλεκτρονικού ταχυδρομείου στο γραμματοκιβώτιο/mailbox - στις ηλεκτρονικές θυρίδες του παραλήπτη. Επίσης καλείτε και ως **LDA, ή local delivery agent** (τοπικός πράκτορα παράδοσης). Παραδείγματα MDAs είναι : Procmail, MailDrop.[22]

1.3.6 Mail retrieval agent (MRA)

Ένας mail retrieval agent (MRA) (πράκτορας ανάκτησης ταχυδρομείου), είναι μια εφαρμογή που ανακτά e-mail από απομακρυσμένο mail server και συνεργάζεται με έναν **mail delivery agent** για να παραδώσει e-mail σε ένα τοπικό ή απομακρυσμένο γραμματοκιβώτιο/mailbox. Ο MRA μπορεί να είναι μία external εφαρμογή ή μία εφαρμογή ενσωματωμένη μέσα στον MUA-mail user agent. Παραδείγματα MRAs είναι : fetchmail, getmail και retchmail.

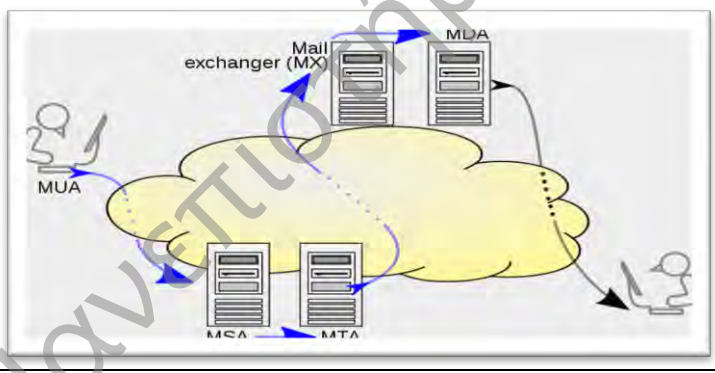
Η έννοια του mail retrieval agent στην ουσία δεν αποτελεί ένα πρότυπο στην αρχιτεκτονική στο e-mail. Παρά το γεγονός ότι λειτουργούν σαν τους mail transfer agents, οι **MRA** είναι τεχνικά client εφαρμογές για την ανάκτηση και να υποβολή μηνυμάτων.[23]

1.3.7 Mail submission agent (MSA)

Ένας **mail submission agent-MSA** (πράκτορας υποβολής ταχυδρομείου) είναι ένα πρόγραμμα ή λογισμικού που λαμβάνει ηλεκτρονικά μηνύματα από έναν user agent (MUA) και συνεργάζεται με ένα mail transfer agent (MTA) για την παράδοση mail. Χρησιμοποιεί μια παραλλαγή του Simple Mail Transfer Protocol (SMTP), όπως ορίζεται στο RFC 6409.[26]

Ένας mail submission agent βρίσκεται μεταξύ του MUA και την MTA σε ένα σύστημα ηλεκτρονικού ταχυδρομείου. Λειτουργεί ως ένα είδος «ρεσεψιονίστ» για τα μηνύματα που εισέρχονται σε ένα σύστημα ηλεκτρονικού ταχυδρομείου από τους MUAs. Κάνει έλεγχο λαθών και επαλήθευση (όπως εξακριβώνεται ότι τα hostnames είναι σωστά, καθορίζει τις κεφαλίδες) πριν περάσει το μήνυμα από τον MTA για την παράδοση. Μπορεί επίσης να αλλάξει η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα από έναν τοπικό λογαριασμό χρήστη σε κάποιο είδος των τυποποιημένων διευθύνσεων e-mail, όπως **lastname.firstname@localdomain.com.**Ο MSA είναι σχετικά νέος agent. Πριν από την ύπαρξή του, όλη αυτή η εργασία γινόταν από τον MTA. Η εικόνα xx δείχνει την θέση ενός MSA στην αρχιτεκτονική του ηλεκτρονικού ταχυδρομείου:

(LinuxQuestions.org, 2009) .



Εικόνα 12: Mail Submission Agent πηγή εικόνας: (Wikipedia, Mail submission agent)

1.4 Αρχιτεκτονικη του Διαδικτυου

Όπως προαναφέρθηκε στην εισαγωγή το ηλεκτρονικό ταχυδρομείο e-mail είναι μια υπηρεσία του διαδικτύου. Σε αυτό το σημείο είναι σκόπιμο να αναλυθεί η αρχιτεκτονική του Internet και πως όλα τα ανομοιογενή συστήματα συνδέονται μεταξύ τους σε ένα απλουστευμένο δίκτυο.

Η ανάγκη για επικοινωνία δεδομένων και διασύνδεσης των διαφόρων δικτύων που ήταν εγκατεστημένα σε όλο τον κόσμο σε ένα ευρύτερο σύνολο που διευκόλυνε και θα επιτάχυνε την επικοινωνία, είναι δύο βασικοί λόγοι που σχεδιάστηκε αυτό που σήμερα γνωρίζουμε σαν *Internet*. Ένα από τα μεγαλύτερα προβλήματα που έπρεπε να λυθούν ώστε το Διαδίκτυο να γίνει πραγματικότητα, ήταν η ύπαρξη πολλών τεχνολογιών δικτύων, καθεμιά από τις οποίες εξυπηρετεί μια συγκεκριμένη ομάδα ανθρώπων μιας και η χρήση μίας και μόνο τεχνολογίας για την δημιουργία ενός παγκόσμιου δικτύου είναι αδύνατη, γιατί δεν υπάρχει τεχνολογία που να ικανοποιεί όλες τις απαιτήσεις.

Το Διαδίκτυο, παρ' όλα αυτά, καταφέρνει να συνενώσει όλες αυτές τις διαφορετικές τεχνολογίες, παρέχοντας ένα σύνολο συμβάσεων επιτρέποντας έτσι σε υπολογιστές από όλο τον κόσμο να βρίσκονται σε επαφή ανεξάρτητα από το δίκτυο στο οποίο συνδέονται. Το Διαδίκτυο βασίζεται σε μια συλλογή από τυποποιήσεις που καλούνται *πρωτόκολλα*. Τα πρωτόκολλα (π.χ. TCP και IP) παρέχουν τους κανόνες για την επικοινωνία. Περιέχουν τις λεπτομέρειες των ανταλλασσόμενων μηνυμάτων, περιγράφουν πως ανταποκρίνεται ο υπολογιστής όταν λαμβάνει κάποιο μήνυμα και ορίζει πως διαχειρίζεται ο υπολογιστής της καταστάσεις λάθους. Με λίγα λόγια ένα πρωτόκολλο επιτρέπει στον χρήστη να καταλάβει τα δεδομένα χωρίς να έχει γνώση του δικτυακού υλικού.

Το Διαδίκτυο αποτελεί παράδειγμα συστήματος τύπου ***open system interconnection***, καλείται ανοιχτό σύστημα *(open system)*, γιατί σε αντίθεση με προηγούμενα επικοινωνιακά συστήματα ανεπτυγμένα από ιδιωτικές εταιρίες, η περιγραφή του είναι δημόσια διαθέσιμη. Έτσι, οποιοσδήποτε μπορεί να γράψει λογισμικό που να συμβαδίζει με τις προδιαγραφές του συστήματος. Σαν τέτοιο σύστημα, το Διαδίκτυο μπορεί να συγκριθεί με το μοντέλο *OSI (Open System Interconnection)*. (Ε.Κ.ΚΦ.Ε.ΔΗΜΟΚΡΙΤΟΣ).

Ο τομέας της δικτύωσης χρησιμοποιεί ένα τυπικό μοντέλο εφτά επιπέδων για την αρχιτεκτονική των πρωτοκόλλων των δικτύων που ονομάζεται *OSI.* Το μοντέλο OSI είναι μια προσπάθεια του ISO, ενός διεθνή οργανισμού προτύπων, να τυποποιηθεί η σχεδίαση των συστημάτων των πρωτοκόλλων των δικτύων, ώστε οι προγραμματιστές λογισμικού να έχουν διασύνδεση και ανοικτή πρόσβαση σε πρότυπα των πρωτοκόλλων.

Το TCP/IP είχε ήδη αρχίσει να εξελίσσεται όταν εμφανίστηκε η αρχιτεκτονική OSI. Ωστόσο, επειδή είχαν παρόμοιούς στόχους και υπήρχε αρκετή αλληλεπίδραση μεταξύ των σχεδιαστών αυτών των προτύπων, έχει σαν αποτέλεσμα τα δύο αυτά μοντέλα να είναι συμβατά. Το μοντέλο OSI έχει επηρεάσει την ανάπτυξη και την εξέλιξη υλοποιήσεων πρωτοκόλλων και είναι πολύ συνηθισμένο να υπάρχει κοινή ορολογία μεταξύ OSI και TCP/IP.

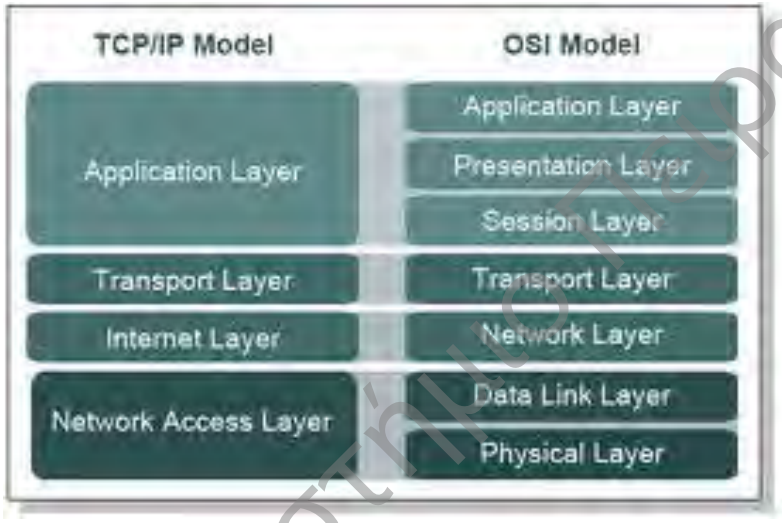
Η παρακάτω εικόνα δείχνει την σχέση μεταξύ του τυπικού TCP/IP τεσσάρων επιπέδων και μοντέλου OSI εφτά επιπέδων. Παρατηρείται ότι το μοντέλο OSI διαιρεί τα καθήκοντα του επιπέδου εφαρμογής σε τρία επίπεδα:

i. Εφαρμογής (Application)
ii. Παρουσίασης (Presentation)
iii. και Συνόδου (Session).

Επίσης χωρίζει τις δραστηριότητες του επιπέδου Διασύνδεσης Δικτύου σε άλλα δύο επίπεδα:

i. Σύνδεσης Δεδομένων (Data Link)
ii. και Φυσικό επίπεδο (Physical).

Αυτή η επιπλέον υποδιαίρεση προσθέτει κάποια πολυπλοκότητα , αλλά επίσης δίνει ευελιξία στους προγραμματιστές να μπορούν να προγραμματίσουν τα επίπεδα πρωτοκόλλων και να προσφέρουν πιο συγκεκριμένες υπηρεσίες. Ιδιαίτερα , η διαίρεση του χαμηλότερου επιπέδου στα επίπεδα Σύνδεσης Δεδομένων και Φυσικό επίπεδο, διαχωρίζει τις λειτουργίες που σχετίζονται με την πρόσβαση στο μέσο επικοινωνίας. Τα τρία ανώτερα επίπεδα OSI προσφέρουν μεγαλύτερη ποικιλία από εναλλακτικές λύσεις για να διασυνδέεται μια εφαρμογή με την στοίβα των πρωτοκόλλων. (Casad, 2009)

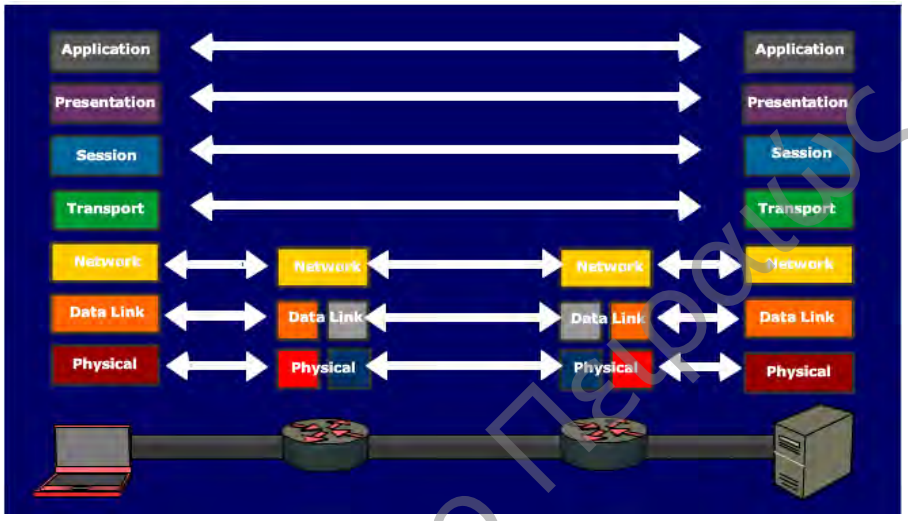


Εικόνα 13: «OSI σε αντίθεση με το TCP/IP» πηγή εικόνας: http://learn-networking.com/tcp-ip/the-tcpip-stack-and-the-osi-model

Έχοντας λοιπόν αναλύσει την αρχιτεκτονική του Internet παρακάτω θα περιγραφεί η διαδικασία του ηλεκτρονικού ταχυδρομείου μέσα από τα 7 επίπεδα του OSI διαμέσου του Internet. Αξιοσημείωτο είναι να αναφερθεί πως το μοντέλο OSI είναι ένα τελείως θεωρητικό μοντέλο καθώς το TCP/IP έχει πρακτική εφαρμογή και έχει καθιερωθεί.

Η Διαδικασία αποστολής και παραλαβής ενός email μέσα από τα επίπεδα του OSI:

- Κάθε επίπεδο του OSI μιλά με το αντίστοιχο στρώμα στον κόμβο προορισμού. Αυτό συμβαίνει επειδή το κάθε στρώμα προσθέτει μία ετικέτα στο αρχικό μήνυμα από το στρώμα που βρίσκεται ακριβώς από πάνω του όπου το διαβάζει το στρώμα του κόμβου προορισμού.



Εικόνα 14: «Επικοινωνία Επιπέδων OSI» πηγή εικόνας: OSI model animation by Khurram Tanvir

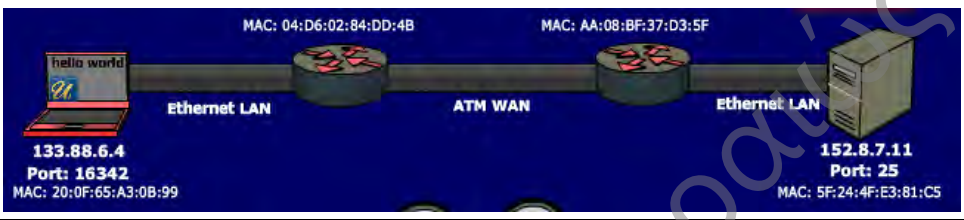
Διαδικασία αποστολής:

1. **Επίπεδο Εφαρμογής (Application):** Παρέχει το σύστημα διεπαφής στα προγράμματα εφαρμογών και χρησιμοποιεί εντολές SMTP για δώσει οδηγίες στο server για τον τρόπο που διαχειριστεί τα δεδομένα.
2. **Επίπεδο Παρουσίασης (Presentation):** Αυτό το επίπεδο μετατρέπει το αρχεία κειμένου σε κώδικα ASCII και καθορίζει το τύπο των εικόνων που πιθανόν να εμπεριέχονται σε ένα email.
3. **Επίπεδο Συνόδου (Session):** Συγχρονίζει τις διάφορες ροές δεδομένων όπως video και ήχο για μια τηλεδιάσκεψη.
4. **Επίπεδο Μεταφοράς (Transport):** Εδώ χρησιμοποιείται το πρωτόκολλο TCP/IP για την συγκεκριμένη διαδικασία (αποστολή email). Κατακερματίζει το μήνυμα σε τμήματα και κάθε τμήμα στέλνεται διαμέσου του δικτύου όπου θα επανασυναρμολογηθούν στο αποστολέα. Επίσης τα ports που παρέχονται για το ηλεκτρονικό ταχυδρομείο έχουν καθοριστεί.
5. **Επίπεδο Δικτύου (Network) :** Παρέχει λογική διευθυνσιοδότηση καθώς και δρομολόγηση. Σε αυτό το επίπεδο χρησιμοποιείται IP address. Τα τμήματα του μηνύματος μετατρέπονται σε πακέτα δεδομένων προσθέτοντας σε κάθε πακέτο μία ετικέτα με την διεύθυνση προορισμού. Στην συνέχεια τα πακέτα στέλνονται στο επίπεδο Σύνδεσης Δεδομένων.
6. **Επίπεδο Σύνδεσης Δεδομένων (Data Link) :** Σε αυτό το επίπεδο τα πακέτα δεδομένων μετατρέπονται σε πλαίσια που δημιουργούνται για συγκεκριμένη τεχνολογία δικτύου (συνήθως τεχνολογία Ethernet). Τα πλαίσια διατηρούν τις

φυσικές διευθύνσεις και του κόμβου αποστολής και του κόμβου λήψης και γίνεται η μεταφορά των δεδομένων διαμέσου του καναλιού.

7. **Φυσικό επίπεδο (Physical) :** Μετατρέπει τα δεδομένα που παρέλαβε από το επίπεδο Σύνδεσης Δεδομένων σε ηλεκτρικό ή αναλογικό σήμα για να περάσουν από το υλικό μετάδοσης και επιβλέπει την μεταφορά των δεδομένων.

Σε αυτό το σημείο γίνεται αποστολή δεδομένων. Εδώ όμως το router πρέπει να στείλει τα πλαίσια δεδομένων διαμέσου ενός διαφορετικού δικτύου που χρησιμοποιεί διαφορετικό πρωτόκολλο Σύνδεσης Δεδομένων. Μόνο το επίπεδο Σύνδεσης Δεδομένων και το φυσικό επίπεδο χρειάζονται τροποποίηση.



Εικόνα 15: «Επικοινωνία routers» πηγή εικόνας: OSI model animation by Khurram Tanvir

Σε μια τέτοια περίπτωση:

- Ο δρομολογητής αφαιρεί την ετικέτα/πληροφορίες του επίπεδου Σύνδεσης Δεδομένων και το στέλνει ένα επίπεδο πάνω δηλαδή στο φυσικό επίπεδο.
- Ο δρομολογητής χρησιμοποιεί την IP προορισμού για να καθορίσει που θα στείλει το πακέτο στην συνέχεια.
- Ο δρομολογητής ενθυλακώνει τα απαραίτητα δεδομένα/πληροφορίες για το επίπεδο Σύνδεσης Δεδομένων του δικτύου ATM.
- Το πακέτο δεδομένων χάνεται λόγω συμφόρησης του δρομολογητή. Το επίπεδο Μεταφοράς του αποστολέα περιμένει ανταπόκριση από το επίπεδο Μεταφοράς του παραλήπτη εάν δεν λάβει απάντηση ότι έλαβε το πακέτο θα αναμεταδώσει τα δεδομένα.
- Ο router του ATM δικτύου αφαιρεί την ετικέτα του επιπέδου Σύνδεσης Δεδομένων και στέλνει το πακέτο στο επίπεδο δικτύου.
- Για ακόμη μία φορά ο router χρησιμοποιεί την IP address από το επίπεδο Δικτύου για να καθορίσει που θα στείλει το πακέτο στην συνέχεια.
- Μόλις καθοριστεί ο παραλήπτης επισυνάπτονται οι κατάλληλες πληροφορίες του επιπέδου Σύνδεσης Δεδομένων για να σταλούν στο δίκτυο.(στην προκειμένη περίπτωση στο δίκτυο Ethernet ξανά). Μερικά πρωτόκολλα Σύνδεσης Δεδομένων παρέχουν αξιόπιστη επικοινωνία μεταξύ δύο κόμβων. Αυτό ακριβώς γίνεται σε αυτό το παράδειγμα στο επίπεδο Σύνδεσης Δεδομένων του δικτύου Ethernet. Όταν το επίπεδο του αποστολέα δεν λάβει ανταπόκριση από το επίπεδο του παραλήπτη αναμεταδίδει το πλαίσιο.

Αφού εν τέλει φτάσει το πακέτο στον τελικό router γίνεται η αντίστροφη διαδικασία που περιγράφτηκε στα πρώτα βήματα δηλαδή κάθε επίπεδο του OSI αφαιρεί την ετικέτα δεδομένων του αντίστοιχου επιπέδου του αποστολέα. Πιο συγκεκριμένα αντίστροφα στην στοίβα κάνει τις εξής ενέργειες :

<u>Διαδικασία παραλαβής:</u>

1. **Φυσικό Επίπεδο :** Διαβάζει τα bits από το φυσικό μέσο τα μετατρέπει σε πλαίσια δεδομένων και τα στέλνει στο επίπεδο Σύνδεσης Δεδομένων.
2. **Επίπεδο Σύνδεσης Δεδομένων:** Αφαιρεί τις επικεφαλίδες του επίπεδου Σύνδεσης Δεδομένων και μετατρέπει τα πλαίσια δεδομένων ξανά σε IP πακέτα.
3. **Επίπεδο Δικτύου:** Αφαιρεί την IP επικεφαλίδα, μετατρέπει ξανά τα IP πακέτα σε τμήματα και τα στέλνει πάνω στο επίπεδο Μεταφοράς.
4. **Επίπεδο Μεταφοράς:** Τα τμήματα του μηνύματος επανασυνδέονται στην αρχική μορφή του μηνύματος. Χρησιμοποιεί το αριθμό του port για να καθορίσει σε ποια εφαρμογή θα στείλει τα δεδομένα.
5. **Επίπεδο Συνόδου:** Χρησιμοποιεί τις πληροφορίες του επιπέδου της Συνόδου για να καθορίσει την ροή επικοινωνίας που τα δεδομένα ανήκουν.
6. **Επίπεδο Παρουσίασης:** Χρησιμοποιεί τις πληροφορίες του επιπέδου της Παρουσίασης για να μπορέσει να παρουσιάσει τα δεδομένα στην μορφή της συγκεκριμένης μηχανής.
7. **Επίπεδο Εφαρμογής:** Η Εφαρμογή διαβάζει τις SMTP εντολές που έστειλε το επίπεδο εφαρμογής του αποστολέα.

Όπως προαναφέρθηκε το μοντέλο OSI είναι ένα θεωρητικό μοντέλο. Το Internet χρησιμοποιεί τη στοίβα πρωτοκόλλων του TCP/IP.

1.5 Συνοπτικη Δομη της Πτυχιακης

Η παρούσα Μεταπτυχιακή Διατριβή χωρίζεται σε 3 θεματικά μέρη όπου:

A. Μέρος Πρώτο:

Στα πρώτα δύο κεφάλαια αναλύεται το θεωρητικό υπόβαθρο της Ηλεκτρονικής Αλληλογραφίας. Συγκεκριμένα τις έννοιες που περικλείονται, η αρχιτεκτονική, τα πρωτόκολλα που καθορίζουν τη μεταφορά και εμφάνιση της Ηλεκτρονικής Αλληλογραφίας.

B. Μέρος Δεύτερο:

Στα επόμενα δύο κεφάλαια δηλαδή στο κεφάλαιο 3^{o} αναλύονται λεπτομερώς οι απειλές που εκμεταλλεύονται τις ευπάθειες του μηχανισμού του email. Ενώ στο κεφάλαιο 4 μελετούνται οι σημερινοί τρόποι αντιμετώπισης και τα μέτρα ασφάλειας που προτείνονται για την διασφάλιση του Ηλεκτρονικού Ταχυδρομείου.

C. Μέρος Τρίτο:

Στο τρίτο και τελευταίο μέρος υλοποιείται η ασφάλεια του Ηλεκτρονικού Ταχυδρομείου και μεταξύ ενός διακομιστή και χρηστών email αλλά και των χρηστών μεταξύ τους. Πιο συγκεκριμένα περιγράφεται η εγκατάσταση ενός e-mail server συγκεκριμένα του Hmailserver 5.4 και υλοποιούνται όλες οι προτεινόμενες ενέργειες για την ασφάλεια του διακομιστή. Στην συνέχεια περιγράφεται η εγκατάσταση του εργαλείου OpenPGP που εξασφαλίζει την ασφάλεια της Αλληλογραφίας μεταξύ χρηστών ανεξάρτητου διακομιστή που ανήκουν.

2 Αναλυτικη Παρουσιαση Πρωτοκολλων Ηλεκτρονικης Αλληλογραφιας

2.1 Εισαγωγη

Υπάρχουν εμπορικές υπηρεσίες που μπορούν να προωθούν ηλεκτρονική αλληλογραφία μεταξύ υπολογιστών χωρίς να χρησιμοποιούν το TCP/IP και χωρίς να έχουν τους υπολογιστές συνδεδεμένους στο παγκόσμιο Internet παρόλο αυτά το σύστημα του ηλεκτρονικού ταχυδρομείου που παρουσιάστηκε έως τώρα είναι προσανατολισμένο σε TCP/IP συνδέσεις . Η τεχνολογία στις ημέρες μας επιτάσσει οι υπηρεσίες του ηλεκτρονικού ταχυδρομείου να είναι σχεδιασμένες πάνω στο σύστημα πρωτοκόλλων TCP/IP διότι εξασφαλίζει:

- **Υπηρεσία Παγκόσμιας Παράδοσης** καθώς προσφέρει παγκόσμια διασύνδεση μεταξύ μηχανημάτων εφόσον όλα τα μηχανήματα σε ένα διαδίκτυο συμπεριφέρονται σαν να είναι συνδεδεμένα σε ένα απλό δίκτυο οποιουδήποτε κατασκευαστή. Με δεδομένες τις βασικές υπηρεσίες δικτύου , η επινόηση ενός τυπικού πρωτοκόλλου ανταλλαγής αλληλογραφίας είναι εύκολη υπόθεση.
- **Αξιοπιστία Παράδοσης** καθώς το TCP/IP προσφέρει συνδεσιμότητα από άκρου εις άκρο (**point to point** connections). Αυτό σημαίνει ότι το λογισμικό ταχυδρομείου στο μηχάνημα του αποστολέα ενεργεί ως πελάτης , επικοινωνώντας με έναν διακομιστή στον τελικό προορισμό. Μόνο αφού ο πελάτης μεταφέρει επιτυχώς ένα μήνυμα αλληλογραφίας στο διακομιστή θα διαγράψει το μήνυμα από το τοπικό μηχάνημα.

  (Comer, 2001 4η Αμερικάνικη Έκδοση)

Συνήθως τα συστήματα ηλεκτρονικού ταχυδρομείου υποστηρίζουν **5 βασικές λειτουργίες**.

a. **Η Σύνθεσή (composition)** αναφέρεται στη διαδικασία της δημιουργίας μηνυμάτων και απαντήσεων. Αν και μπορεί να χρησιμοποιηθεί οποιοσδήποτε κειμενογράφος για τον κορμό του μηνύματος, το ίδιο το σύστημα μπορεί να βοηθήσει στη διευθυνσιοδότηση και στα πολυάριθμα πεδία της επικεφαλίδας που προσκολλώνται σε κάθε μήνυμα. Για παράδειγμα, όταν απαντάμε σ' ένα μήνυμα , το σύστημα ηλεκτρονικού ταχυδρομείου μπορεί να αποσπάσει τη διεύθυνση του δημιουργού από το εισερχόμενο email και αυτόματα να την εισάγει στη σωστή θέση στην απάντηση.
b. **Η Μεταφορά (transfer)** αναφέρεται στη μετακίνηση των μηνυμάτων από τον αποστολέα στον παραλήπτη. Κατά μεγάλο μέρος , αυτό απαιτεί την εγκατάσταση μίας σύνδεσης. Το σύστημα ηλεκτρονικού ταχυδρομείου πρέπει να κάνει αυτό αυτόματα, χωρίς να ενοχλείται ο χρήστης.
c. **Η Αναφορά (reporting)** αφορά την πληροφόρηση του αποστολέα γύρω από την τύχη του μηνύματος. Αν έχει παραδοθεί ; Αν απορρίφθηκε; Αν χάθηκε; Υπάρχουν πολυάριθμες εφαρμογές στις οποίες η επιβεβαίωση της παράδοσης είναι σημαντική και μπορεί ακόμη και να έχει νόμιμη σημασία.
d. **Η Εμφάνιση (displaying)** των εισερχόμενων μηνυμάτων χρειάζεται για να μπορούν οι άνθρωποι να διαβάζουν το ηλεκτρονικό ταχυδρομείο τους. Μερικές φορές

απαιτείται κάποια μετατροπή ή πρέπει να κληθεί μία ειδική διαδικασία εμφάνισης (viewer) , για παράδειγμα , αν το μήνυμα είναι αρχείο postscript ή φωνή σε ψηφιακή μορφή.

e. **Η Διάθεση (disposition)** είναι το τελικό βήμα και αφορά το τι κάνει ο αποδέκτης με το μήνυμα αφού το λάβει. Μπορεί να το πετάξει αφού το διαβάσει, να το αποθηκεύσει , κ.ο.κ. Πρέπει επίσης να είναι σε θέση να βρει και να ξαναδιαβάσει τα αποθηκευμένα μηνύματα, να τα προωθήσει ή να τα επεξεργαστεί μ' άλλους τρόπους. (S.Tanenbaum, 1996)

2.2 Πρότυπα TCP/IP για την υπηρεσία του Ηλεκτρονικού Ταχυδρομείου

Όπως προαναφέρθηκε στόχος των πρωτοκόλλων του TCP/IP είναι να προσφέρει διαλειτουργικότητα σε όσο πιο δυνατόν μεγαλύτερο εύρος υπολογιστικών συστημάτων και δικτύων. Για να επεκταθεί η διαλειτουργικότητα του ηλεκτρονικού ταχυδρομείου , το TCP/IP χωρίζει τα πρότυπα ταχυδρομείου σε δύο σύνολα:

1. Το ένα πρότυπο καθορίζει **τη μορφή** για τα μηνύματα αλληλογραφίας (πρότυπο RFC 822).
2. Και το άλλο καθορίζει **τις λεπτομέρειες για την ανταλλαγή** ηλεκτρονικής αλληλογραφίας μεταξύ δύο υπολογιστών.

Σε αυτό τι κεφάλαιο θα αναλυθούν και τα δύο αυτά πρότυπα.

(Comer, 2001 4η Αμερικάνικη Έκδοση)

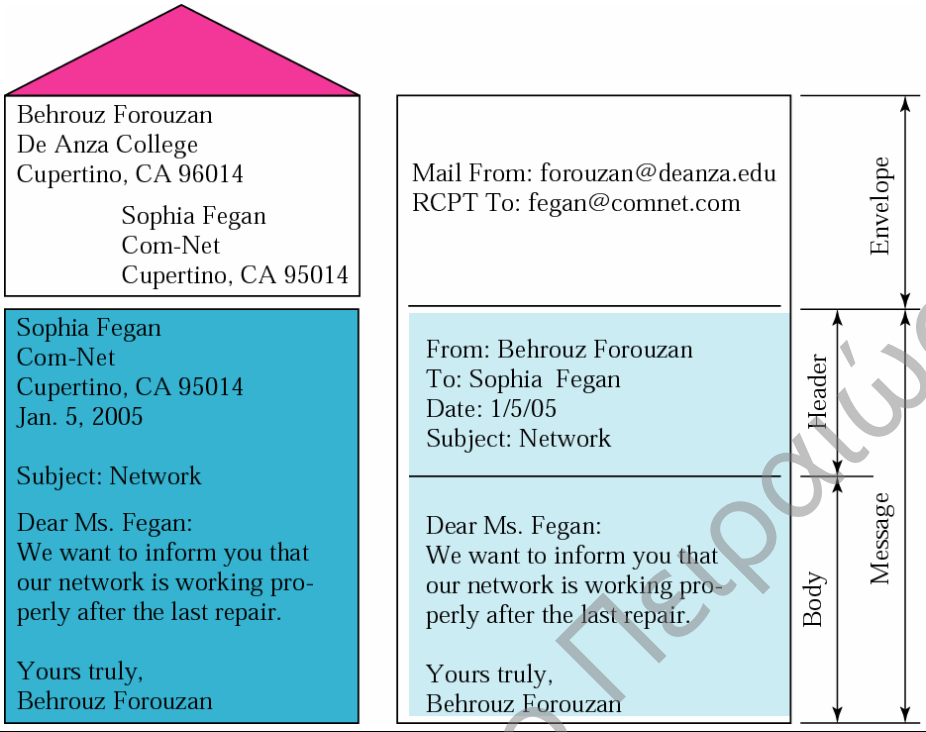
2.3 Η Μορφη του Ηλεκτρονικου Ταχυδρομειου

Το πρότυπο TCP/IP καθορίζει επακριβώς την μορφή για τα μηνύματα ηλεκτρονικού ταχυδρομείου. Ένα ηλεκτρονικό μήνυμα/ e-mail αποτελείται από 3 συστατικά:

i. Το φάκελο του μηνύματος (envelope)
ii. Την επικεφαλίδα του μηνύματος και (header)
iii. Το σώμα του μηνύματος (body)

(Wikipedia, Email)

Μία ιδέα κλειδί σε όλα τα μοντέρνα συστήματα ηλεκτρονικού ταχυδρομείου είναι η διάκριση μεταξύ **φακέλου (envelope)** και των περιεχομένων του. Ο φάκελος ενθυλακώνει το μήνυμα. Περιέχει όλες τις πληροφορίες που χρειάζονται για τη μεταφορά του μηνύματος, όπως τη διεύθυνση προορισμού, την προτεραιότητα, το επίπεδο ασφάλειας, που είναι όλα ξεχωριστά από το ίδιο το μήνυμα. Οι πράκτορες μεταφοράς μηνυμάτων χρησιμοποιούν το φάκελο για τη δρομολόγηση , όπως ακριβώς κάνει και ένα ταχυδρομικό γραφείο. (S.Tanenbaum, 1996)



Εικόνα 16: «Μορφή ενός email» πηγή εικόνας: Behrouz A. Forouzan, 2005

Το μήνυμα μέσα στον φάκελο περιέχει δύο μέρη: Το σώμα και την επικεφαλίδα. Όπου μεταδίδονται ως κείμενο σε κώδικα ASCII (*Αμερικανικός Πρότυπος Κώδικας για Ανταλλαγή Πληροφοριών*). Η επικεφαλίδα αποτελείται από μία σειρά από λέξεις κλειδιά, που ακολουθούνται από μία ή περισσότερες τιμές χωρισμένες σε κόμματα. Τα περισσότερα από αυτά τα πεδία κεφαλίδας είναι γνωστά σε όποιον έχει δουλέψει με ηλεκτρονικό ταχυδρομείο. Στο Πίνακα 1 αναλύονται τα σημαντικότερα πεδία της κεφαλίδας:

Πίνακας 1 «Τα βασικότερα headers ενός μηνύματος»

Πεδίο Επικεφαλίδας	Περιγραφή
To:	Διεύθυνση (ή διευθύνσεις) ηλεκτρονικού ταχυδρομείου του παραλήπτη (ή των παραληπτών).
From:	Διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα.
Date:	Ημερομηνία και ώρα που στάλθηκε το μήνυμα.
Subject:	Σύντομη περιγραφή του θέματος του μηνύματος.
Cc:	Διευθύνσεις ηλεκτρονικού ταχυδρομείου άλλων χρηστών οι οποίοι θα λάβουν ένα αντίγραφο του μηνύματος.
Bcc:	Διευθύνσεις ηλεκτρονικού ταχυδρομείου άλλων χρηστών οι οποίοι θα λάβουν ένα **κρυφό** αντίγραφο του μηνύματος. Το Bcc (blind copy - κοινοποίηση) είναι ένα αντίγραφο του οποίου δεν ξέρουν την ύπαρξη οι παραλήπτες. Η διεύθυνση ηλεκτρονικού ταχυδρομείου που εμφανίζεται στο πεδίο κοινοποίησης δεν θα εμφανιστεί στην κεφαλίδα που λαμβάνεται από τους άλλους παραλήπτες.
Reply-To:	Η διεύθυνση ηλεκτρονικού ταχυδρομείου που θα λαμβάνει απαντήσεις σε αυτό μήνυμα. Αν δεν δοθεί αυτό το πεδίο , οι απαντήσεις θα πάνε στην διεύθυνση που αναφέρεται στο πεδίο From:
Attachment	Αρχεία που **επισυνάπτονται** στο μήνυμα.

Η επικεφαλίδα περιέχει πληροφορίες ελέγχου για τους πράκτορες χρήστη ενώ το σώμα του μηνύματος προορίζεται καθαρά για τον ανθρώπινο αποδέκτη.

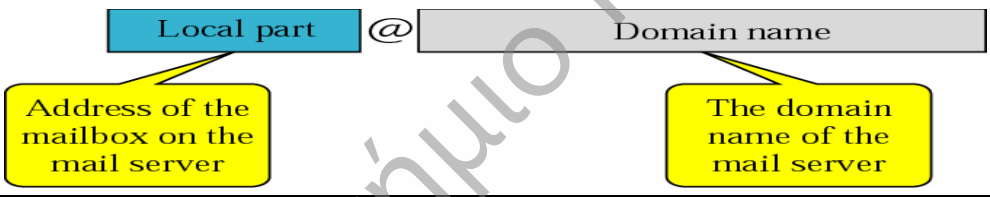
(Casad, 2009), (Παν.Θεσσαλίας)

2.3.1 Ηλεκτρονικη Διευθυνση Αλληλογραφιας (e-mail address)

Όπως προκύπτει από τα παραπάνω για να μπορέσει κάποιος να χρησιμοποιήσει την υπηρεσία της ηλεκτρονικής αλληλογραφίας, χρειάζεται μια ηλεκτρονική διεύθυνση αλληλογραφίας (e-mail address) καθώς αυτή είναι που καθορίζει τον αποστολέα και τον παραλήπτη και επίσης είναι η μόνη «μορφή» δεδομένων που μπορεί να συμπληρώσει τα πεδία της επικεφαλίδας του μηνύματος : To, From, Cc, Bcc, Reply- To έτσι όπως αναλύθηκαν πρωτύτερα. Σε αυτήν λοιπόν την ενότητα θα περιγραφεί η μορφή μίας ηλεκτρονικής διεύθυνσης αλληλογραφίας και το τι συμβολίζουν τα αποτελούμενα μέρη της.

Κάθε χρήστης του Internet έχει τη δική του μοναδική **διεύθυνση ηλεκτρονικού ταχυδρομείου** (**E-mail address**). Μια διεύθυνση ηλεκτρονικού ταχυδρομείου εντοπίζει τη θυρίδα/ το γραμματοκιβώτιο του ηλεκτρονικού ταχυδρομείου ενός χρήστη. Αν και τα παλιότερα συστήματα ηλεκτρονικού ταχυδρομείου υποστήριζαν διαφορετικούς τύπους διευθύνσεων η μορφή της διεύθυνσης που έχει επικρατήσει αποτελείται από δύο μέρη:

a. Το μέρος πριν το σύμβολο **@** είναι το **local-τοπικό μέρος** της διεύθυνσης και
b. Το τμήμα μετά το σύμβολο **@** όπου είναι το **όνομα τομέα-domain** στον οποίο το μήνυμα ηλεκτρονικού ταχυδρομείου θα αποσταλεί (example.org), όπως φαίνεται και στην εικόνα xx. Το τμήμα του τομέα δεν είναι case-sensitive , αλλά το τοπικό μέρος συνήθως είναι. (Wikipedia, Email address)



Εικόνα 17: Ηλεκτρονική Διεύθυνση Ταχυδρομείου πηγή εικόνας: Behrouz A. Forouzan, 2005

- **Τοπικό μέρος**

Το **τοπικό μέρος** ορίζει το όνομα ενός ειδικού αρχείου που ονομάζεται γραμματοκιβώτιο χρήστη όπου αποθηκεύονται όλα τα μηνύματα που λαμβάνονται για έναν χρήστη. (Behrouz A. Forouzan, 2005) Πολύ συχνά το τοπικό μέρος της διεύθυνσης καταδεικνύει το όνομα του παραλήπτη (π.χ. JSmith). (Wikipedia, Email address)

- **Όνομα τομέα**

Το δεύτερο μέρος της διεύθυνσης είναι το **όνομα τομέα**. Ένας οργανισμός συνήθως επιλέγει έναν ή περισσότερους κεντρικούς υπολογιστές για να λάβει και να στείλει αλληλογραφία και αυτοί μερικές φορές ονομάζονται **servers** ή ανταλλακτήρια αλληλογραφίας. Το όνομα τομέα που αποδίδεται σε κάθε ανταλλακτήριο αλληλογραφίας προέρχεται από τη DNS βάση δεδομένων ή είναι ένα λογικό όνομα (π.χ. ο τίτλος του οργανισμού). (Behrouz A. Forouzan, 2005)

Δεν είναι σαφές από το όνομα τομέα της διεύθυνση ηλεκτρονικού ταχυδρομείου ποιος είναι ο πραγματικός προορισμός (ο χρήστης της θυρίδας) του e-mail. Ένας διακομιστής αλληλογραφίας θα χρησιμοποιήσει το Domain Name System (DNS), το οποίο είναι μια κατανεμημένη βάση δεδομένων, για να βρει τη διεύθυνση IP του κεντρικού υπολογιστή του τομέα. Ο διακομιστής ρωτάει το DNS για οποιεσδήποτε εγγραφές ανταλλαγής αλληλογραφίας (MX records) για να βρείτε τη διεύθυνση IP ενός ορισμένου Mail Transfer Agent (MTA) για την εν λόγω διεύθυνση. (Wikipedia, Email address)

2.3.2 Σύνταξη Διεύθυνσης Ηλεκτρονικής Αλληλογραφίας

Η μορφή των διευθύνσεων ηλεκτρονικού ταχυδρομείου είναι **τοπικό τμήμα @ domain** όπου:

- το τοπικό τμήμα μπορεί να είναι έως και 64 χαρακτήρες και
- το όνομα τομέα μπορεί να έχει ένα μέγιστο 255 χαρακτήρες.

Πιο συγκεκριμένα:

Τοπικό τμήμα- local part:

- Το τοπικό τμήμα-local part μπορεί να χρησιμοποιήσει οποιοδήποτε από αυτούς τους χαρακτήρες ASCII (στο RFC 6531 επιτρέπονται και χαρακτήρες συστήματος Unicode):
- Κεφαλαία και πεζά λατινικά γράμματα (a–z, A–Z) (ASCII: 65–90, 97–122)
- Ψηφία από το 0 έως το 9 (ASCII: 48–57)
- Ειδικοί χαρακτήρες όπως: ! # $ % & ' * + - / = ? ^ _ ` { | } ~
- Χαρακτήρες όπως τελεία, διάστημα, τελεία και παύλα (ASCII: 46) υπό την προϋπόθεση ότι δεν θα βρίσκονται στη θέση του πρώτου ή του τελευταίου χαρακτήρα, και ότι δεν εμφανίζονται δύο ή περισσότερες φορές διαδοχικά (π.χ η διεύθυνση **John .. Doe@example.com** - δεν επιτρέπεται).
- Οι ειδικοί χαρακτήρες επιτρέπεται με κάποιους περιορισμούς. Αυτοί είναι:
- Το κενό και `" () , : ; <> @ [ \]` (ASCII: 32, 34, 40, 41, 44, 58, 59, 60, 62, 64, 91–93)
- Οι περιορισμοί για ειδικούς χαρακτήρες είναι ότι πρέπει να χρησιμοποιούνται μόνο όταν περιέχονται ανάμεσα σε εισαγωγικά, και ότι 2 από αυτά (το backslash \ και εισαγωγικά "(ASCII: 92, 34)), πρέπει να προηγείται μια ανάστροφη κάθετο-backslash \ (π.χ." \ \ \ "").
- Τα σχόλια επιτρέπονται με παρενθέσεις σε κάθε άκρο του τοπικού τμήματος? Π.χ. "john.smith(comment)@example.com" ή "(comment)john.smith@example.com" ισοδυναμεί με : "john.smith@example.com".
- Τα τμήματα του τοπικού τμήματος είναι case-sensitive και ως εκ τούτου οι διευθύνσεις jsmith@example.com και JSmith@example.com καθορίζουν διαφορετικές γραμματοκιβώτια. Ωστόσο , πολλές άλλες υπηρεσίες αντιμετωπίζουν τα κεφαλαία και τα πεζά γράμματα ως ισοδύναμα. Οι περισσότερες υπηρεσίες δεν επιτρέπουν τη χρήση πολλών από τα τεχνικά έγκυρους ειδικούς χαρακτήρες. Οι υπηρεσίες είναι ελεύθερες στο να διαμορφώσουν τις δικές του μορφές για τις

διευθύνσεις ηλεκτρονικού ταχυδρομείου, για παράδειγμα , το Windows Live Hotmail , επιτρέπει μόνο τη δημιουργία των διευθύνσεων ηλεκτρονικού ταχυδρομείου που χρησιμοποιούν αλφαριθμητικά , τελεία , κάτω παύλα (_) και παύλα (-).

- Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου που στέλνουν μηνύματα πρέπει να είναι σε θέση να χειρίζονται εξερχόμενη αλληλογραφία για όλες τις έγκυρες διευθύνσεις . Σε αντίθεση με τα σχετικά πρότυπα , ορισμένα συστήματα αλληλογραφία αντιμετωπίζουν ορισμένες διευθύνσεις ως μη-έγκυρες και δεν παραδίδουν τα μηνύματα .Το Hotmail , για παράδειγμα , αποτυγχάνει να στείλει email σε οποιαδήποτε διεύθυνση που περιέχει οποιαδήποτε από τους ακόλουθους χαρακτήρες: ! . # $ % * / ^ ` { | } ~ [

Όνομα τομέα- Domain part:

Το όνομα τομέα της διεύθυνσης ηλεκτρονικού ταχυδρομείου θα πρέπει να είναι συμβατό με τα εκάστοτε πρότυπα: θα πρέπει να ταιριάζει με τις απαιτήσεις για ένα hostname, αποτελούμενο από γράμματα, ψηφία, παύλες και τελείες. Επίσης, το τμήμα του τομέα μπορεί να είναι και μια διεύθυνση IP η οποία θα περιβάλλεται από αγκύλες, όπως **jsmith@[192.168.2.1]** , αν και αυτό είναι σπάνια γίνεται , εκτός και αν πρόκειται για spam. (Wikipedia, Email address)

2.3.3 Συστημα Ονομασιας Περιοχων - DNS (Domain Name System)

Το **Σύστημα Ονομασίας Περιοχών DNS** είναι ένας πολύ σημαντικός και σύνθετος μηχανισμός του Διαδικτύου γι' αυτό θα περιγραφεί συνοπτικά και στη συνέχεια θα αναλυθούν οι περιπτώσεις που αφορούν τη μεταφορά του ηλεκτρονικού ταχυδρομείου.

Τα προγράμματα σπανία απευθύνονται σε host, ταχυδρομικά κουτιά και σε άλλους πόρους με τη δυαδική τους διεύθυνση δικτύου. Αντί για δυαδικούς αριθμούς, χρησιμοποιούν συρμούς ASCII χαρακτήρων, όπως tana@art.ucsb.edu .Όμως , το δίκτυο και γενικά οι υπολογιστές καταλαβαίνουν μόνο δυαδικές διευθύνσεις και γι αυτό χρειαζόταν κάποιος μηχανισμός που να μετατρέπει τους ASCII χαρακτήρες σε διευθύνσεις δικτύου. Η αντιστοίχιση αυτή στο Internet έγινε τη χρήση του **Συστήματος Ονομασίας Περιοχών DNS (Domain Name System)**. Η ουσία του DNS είναι η επινόηση μιας ιεραρχικής μεθόδου ονοματοδότησης βασισμένης σε περιοχές και μίας κατανεμημένης βάσης δεδομένων που να υλοποιεί αυτήν τη μέθοδο. Χρησιμοποιείται πρωταρχικά για αντιστοιχίσει τα ονόματα host και τους προορισμούς του ηλεκτρονικού ταχυδρομείου με τις IP διευθύνσεις, αλλά μπορεί να χρησιμοποιηθεί και για άλλους σκοπούς. Το **DNS** περιγράφεται στα RFC 1034 και 1035. (S.Tanenbaum, 1996)

Οι εξυπηρετητητές ονομάτων είναι συχνά υπολογιστές UNIX που εκτελούν το λογισμικό Berkeley Internet Name Domain (BIND). Το πρωτόκολλο DNS εκτελείται επάνω σε UDP και χρησιμοποιεί τη θύρα 53. Το DNS χρησιμοποιείται συνήθως από άλλα πρωτόκολλα επιπέδου εφαρμογής περιλαμβανομένων των HTTP, SMTP και FTP για μετάφραση ονομάτων υπολογιστών υπηρεσίας που παρέχονται από τον χρήστη σε διευθύνσεις IP.

Πιο συγκεκριμένα όταν ένα πρόγραμμα περιήγησης (δηλαδή ένας πελάτης HTTP), που εκτελείται στον υπολογιστή υπηρεσίας ενός χρήστη, ζητήσει το URL www.someschool.edu/index.html για να μπορέσει ο υπολογιστής υπηρεσίας του χρήστη να στείλει ένα μήνυμα αίτησης HTTP στον εξυπηρετητή Web www.someschool.edu , ο υπολογιστής υπηρεσίας του χρήστη πρέπει να πάρει τη διεύθυνση IP του www.someschool.edu. Αυτό γίνεται ως εξής:

- Ο ίδιος υπολογιστής χρήστη εκτελείται στην πλευρά πελάτη της εφαρμογής DNS. Το πρόγραμμα περιήγησης εξάγει το όνομα υπολογιστή υπηρεσίας, www.someschool.edu από το URL και περνά το όνομα υπολογιστή υπηρεσίας στην πλευρά πελάτη της εφαρμογής DNS. Σαν τμήμα ενός μηνύματος ερωτήματος DNS,
- ο πελάτης DNS στέλνει ένα ερώτημα που περιέχει το όνομα υπολογιστή υπηρεσίας προς ένα DNS εξυπηρετητή.
- Ο πελάτης DNS δέχεται τελικά μια απάντηση, η οποία περιλαμβάνει τη διεύθυνση IP του ονόματος υπολογιστή υπηρεσίας.
- Το πρόγραμμα περιήγησης κατόπιν ανοίγει μια σύνδεση TCP προς τη διεργασία HTTP εξυπηρετητή που βρίσκεται σε αυτή τη διεύθυνση IP. (Kurose&Ross, 2008)

Όλη αυτή η διαδικασία παριστάνεται στην παρακάτω εικόνα:

Εικόνα 18: «Διαδικασία Επίλυσης Διευθύνσεων με DNS» πηγή εικόνας: (Barb, 2013)

Το DNS παρέχει μερικές σημαντικές υπηρεσίες εκτός του ότι μεταφράζει ονόματα υπολογιστών υπηρεσίας σε διευθύνσεις IP:

- **Ψευδώνυμα υπολογιστών υπηρεσίας**. Ένας υπολογιστής υπηρεσίας με ένα περίπλοκο όνομα υπολογιστή υπηρεσίας μπορεί να έχει ένα ή περισσότερα ψευδώνυμα. Για παράδειγμα, ένα όνομα υπολογιστή υπηρεσίας σαν το relay1.west-coast.enterprise.com, μπορεί να έχει δύο ψευδώνυμα, π.χ. enterpnise.com και www.enterprise.com. Το DNS μπορεί να κληθεί από μια εφαρμογή για να βρει το όνομα υπολογιστή υπηρεσίας για ένα παρεχόμενο ψευδώνυμο υπολογιστή υπηρεσίας, καθώς και τη διεύθυνση IP του υπολογιστή υπηρεσίας.

- **Ψευδώνυμα εξυπηρετητή ταχυδρομείου**. Για προφανείς λόγους, είναι άκρως επιθυμητό μια διεύθυνση e-mail να είναι ευκολομνημόνευτη. Για παράδειγμα, αν ο Bob έχει ένα λογαριασμό στο Hotmail, η διεύθυνση e-mail του Bob μπορεί να είναι bob@hotmail.com . Αλλά όμως, το όνομα υπολογιστή υπηρεσίας του εξυπηρετητή ταχυδρομείου Hotmail είναι πιο περίπλοκο και λιγότερο ευκολομνημόνευτο από το απλό hotmail.com (για παράδειγμα, το κανονικοποιημένο όνομα υπολογιστή υπηρεσίας μπορεί να είναι κάτι σαν relay1.west-coast.hotmail.com). Το DNS μπορεί να κληθεί από μια εφαρμογή ταχυδρομείου για να πάρουμε το κανονικοποιημένο όνομα υπολογιστή υπηρεσίας για ένα ψευδώνυμο υπολογιστή υπηρεσίας, καθώς και τη διεύθυνση IP του υπολογιστή υπηρεσίας. Στην πραγματικότητα, η εγγραφή MX (που θα αναλυθεί παρακάτω) επιτρέπει στον εξυπηρετητή ταχυδρομείου μιας εταιρείας και στον Εξυπηρετητή Web να έχουν πανομοιότυπα (ψευδώνυμα) ονόματα υπολογιστών υπηρεσίας. Για παράδειγμα, ο Εξυπηρετητής Web και ο εξυπηρετητής ταχυδρομείου μιας εταιρείας μπορούν να καλούνται και οι δύο enterprise.com.

- **Κατανομή φορτίου**. Είναι αρκετά ενδιαφέρον ότι το DNS χρησιμοποιείται επίσης για να κάνει κατανομή φορτίου, ανάμεσα σε αντίγραφα εξυπηρετητών, π.χ., σε αντίγραφα Εξυπηρετητών WEB. Απασχολημένοι servers, όπως ο cnn.com αντιγράφονται σε πολλαπλούς εξυπηρετητές, όπου ο καθένας εξυπηρετεί ένα διαφορετικό τερματικό σύστημα, και ο καθένας έχει μια διαφορετική διεύθυνση IP. Για τα αντίγραφα εξυπηρετητών WEB λοιπόν ένα σύνολο διευθύνσεων IP σχετίζεται με ένα **κανονικοποιημένο όνομα υπολογιστή υπηρεσίας**. Η βάση δεδομένων DNS περιέχει αυτό το σύνολο διευθύνσεων IP. Όταν οι πελάτες κάνουν ένα ερώτημα DNS για ένα όνομα που αντιστοιχίζεται σε ένα σύνολο διευθύνσεων, ο εξυπηρετητής αποκρίνεται με όλο το σύνολο διευθύνσεων IP, αλλά κάνει περιστροφή της σειράς των διευθύνσεων σε κάθε απάντηση. Επειδή ο πελάτης συνήθως στέλνει το μήνυμα αίτησης HTTP στη διεύθυνση IP που αναφέρεται πρώτη μέσα στο σύνολο, η

περιστροφή DNS κατανέμει την κίνηση ανάμεσα σε όλες τα αντίγραφα εξυπηρετητών.

Η περιστροφή DNS χρησιμοποιείται επίσης για **e-mail**, οπότε πολλαπλοί εξυπηρετητητές ταχυδρομείου μπορούν να έχουν το ίδιο ψευδώνυμο. (Kurose&Ross, 2008)

2.3.4 Εγγραφες ανταλλαγης αλληλογραφιας –MX-mail exchanger records

Οι εξυπηρετητές ονομάτων που υλοποιούν όλοι μαζί την κατανεμημένη βάση δεδομένων DNS αποθηκεύουν εγγραφές πόρων (Resource records, RR) για τις αντιστοιχίσεις ονόματος υπολογιστή υπηρεσίας-διεύθυνσης IP. Κάθε μήνυμα απόκρισης DNS μεταφέρει μια ή περισσότερες εγγραφές πόρων. Μια εγγραφή πόρου είναι μια τετράδα, που περιέχει τα παρακάτω πεδία:

(Όνομα, Τιμή, Τύπος, TTL)

Όπου:

- **TTL:** (Time-To-Live) είναι ο χρόνος που θα ζει μια εγγραφή πόρου.

Η σημασία των **Όνομα** και **Τιμή** εξαρτάται από τον τύπο:

- **Αν τύπος = A,** τότε το Όνομα είναι **ένα όνομα υπολογιστή υπηρεσίας και η τιμή είναι η διεύθυνση IP** για το όνομα υπολογιστή υπηρεσίας. Έτσι, μια εγγραφή Τύπου A παρέχει την πρότυπη αντιστοίχιση ονόματος υπολογιστή υπηρεσίας προς διεύθυνση IP. Π.χ. (relayl.bar.fo.com, 145.37.93.126, A) είναι μια εγγραφή Τύπου A.
- **Αν τύπος = NS**, τότε **το Όνομα είναι ένας τομέας** (π.χ. foo.com) και **η τιμή είναι το όνομα υπολογιστή υπηρεσίας** ενός αυθεντικού εξυπηρετητή ονομάτων. Αυτή η εγγραφή χρησιμοποιείται για να δρομολογήσει ερωτήματα DNS μέσα στην αλυσίδα ερωτημάτων. Π.χ. (foo.com., dns.foo.com., N) είναι μια εγγραφή Τύπου NS.
- **Αν Τύπος = CNAME** (συντόμευση του "Canonical Name"), τότε **η Τιμή είναι ένα κανονικοποιημένο όνομα υπολογιστή** υπηρεσίας για το ψευδώνυμο (alias) υπολογιστή υπηρεσίας Όνομα. Αυτή η εγγραφή θα παρέχει στους ερωτώντες υπολογιστές υπηρεσίας το κανονικοποιημένο όνομα για ένα όνομα υπολογιστή υπηρεσίας. Σαν ένα παράδειγμα, (foo.com, relayl.bar.foo.com, cNAMe) είναι μια εγγραφή CNAME.
- **Αν τύπος = MX** , τότε η τιμή είναι το κανονικοποιημένο όνομα ενός εξυπηρετητή ταχυδρομείου που έχει ψευδώνυμο υπολογιστή υπηρεσίας Όνομα. Π.χ. (foo.com, mail.bar.foo.com, MX) είναι μια εγγραφή MX. Οι εγγραφές MX επιτρέπουν σε ονόματα υπολογιστών υπηρεσίας εξυπηρετών ταχυδρομείων να έχουν απλά ψευδώνυμα. Έτσι χρησιμοποιώντας την εγγραφή MX, μια εταιρεία μπορεί να έχει το ίδιο ψευδώνυμο για τον εξυπηρετητή ταχυδρομείου της και για έναν από τους άλλους εξυπηρετητές της (π.χ., τον Εξυπηρετητή Web). Για να πάρει το κανονικοποιημένο όνομα για τον εξυπηρετητή ταχυδρομείου, ένας πελάτης DNS Θα κάνει ερώτημα για μια εγγραφή MX. Για να πάρει το κανονικοποιημένο όνομα για τον άλλο εξυπηρετητή, ο πελάτης DNS θα κάνει ερώτημα για την εγγραφή CNAME. (Kurose&Ross, 2008)

Μια εγγραφή ανταλλαγής αλληλογραφίας γνωστό ως (**MX) mail exchanger record** λοιπόν είναι ένα είδος καταγραφής πόρου στο **Σύστημα Ονομάτων Τομέα-DNS** που καθορίζει έναν mail server που είναι υπεύθυνος για την παραλαβή των μηνυμάτων ηλεκτρονικού ταχυδρομείου για τον παραλήπτη που διαθέτει λογαριασμό στο συγκεκριμένο domain. Επίσης μία **εγγραφή MX** διαθέτει και μία τιμή σειράς κατάταξης που χρησιμοποιείται για την παράδοση αλληλογραφίας με σειρά προτεραιότητας , στην περίπτωση που είναι διαθέσιμοι πολλοί διακομιστές αλληλογραφίας. Το σύνολο των εγγραφών MX ενός domain name καθορίζει τον τρόπο με τον οποίο ένα e-mail δρομολογείται με το Simple Mail Transfer Protocol (SMTP).

Όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται μέσω του Internet:

- Ο πράκτορας μεταφοράς ταχυδρομείου (mail transfer agent -MTA) από την πλευρά του αποστολέα ρωτά το Domain Name System για MX εγγραφές του domain name του κάθε παραλήπτη.
- Αυτό το ερώτημα επιστρέφει μια λίστα με τα διαθέσιμα host names των servers ανταλλαγής αλληλογραφίας που μπορούν να δεχθούν μηνύματα εισερχόμενης αλληλογραφίας για αυτόν τον τομέα.
- Αφού λοιπόν ολοκληρωθούν όλα αυτά τα βήματα ο πράκτορας αποστολής αλληλογραφίας από την μεριά του αποστολέα θα προσπαθήσει να εγκαθιδρύσει μια σύνδεση SMTP με τον εξυπηρετητή του παραλήπτη.

(Wikipedia, MX record)

2.4 Η ανταλλαγη του Ηλεκτρονικου Ταχυδρομειου

Εκτός από τις μορφές μηνυμάτων, το πακέτο πρωτοκόλλων TCP/IP καθορίζει και ένα πρότυπο για την ανταλλαγή αλληλογραφίας μεταξύ μηχανημάτων. Το σύστημα μεταφοράς μηνυμάτων ασχολείται με την αναμετάδοση των μηνυμάτων από τον δημιουργό τους στον αποδέκτη. Ο απλούστερος τρόπος για να γίνει αυτό είναι η εγκατάσταση μίας σύνδεσης μεταφοράς από τη μηχανή αφετηρίας στη μηχανή προορισμού και μετά απλώς η μεταβίβαση του μηνύματος. (S.Tanenbaum, 1996) (Comer, 2001 4η Αμερικάνικη Έκδοση)

Εντός του Internet, το ηλεκτρονικό ταχυδρομείο παραδίνεται με τη μηχανή αφετηρίας να εγκαθιστά μία σύνδεση TCP στη θύρα 25 της μηχανής προορισμού. Σε αυτήν τη θύρα ακούει ένας daemon ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί το **Πρωτόκολλο Απλής Ταχυδρομικής Μεταφοράς SMTP (Simple Mail Transfer Protocol)**. Αυτός ο daemon δέχεται τις εισερχόμενες συνδέσεις και αντιγράφει τα μηνύματα από αυτές στα κατάλληλα γραμματοκιβώτια. (S.Tanenbaum, 1996)

Το SMTP είναι ένα απλό ASCII πρωτόκολλο και χρησιμοποιείται δύο φορές, μεταξύ του αποστολέα του server αλληλογραφίας και μεταξύ των δύο servers αλληλογραφίας. Όπως Θα δούμε σε λίγο, χρειάζεται ακόμα ένα πρωτόκολλο μεταξύ του server αλληλογραφίας και του παραλήπτη. Το SMTP απλώς ορίζει πώς πρέπει να αποστέλλονται οι εντολές και οι απαντήσεις. Κάθε δίκτυο είναι ελεύθερο να επιλέξει ένα λογισμικό για υλοποίηση. (Behrouz A. Forouzan, 2005)

Το πρωτόκολλο SMTP λοιπόν εστιάζει ειδικά στον τρόπο με τον οποίο το υποκείμενο σύστημα παράδοσης ταχυδρομείου μεταβιβάζει μηνύματα διαμέσου ενός διαδικτύου, από το ένα μηχάνημα σε κάποιο άλλο. Δεν καθορίζει τον τρόπο με τον οποίο το σύστημα ταχυδρομείου θα δέχεται αλληλογραφία από ένα χρήστη, ή τον τρόπο με τον οποίο η διασύνδεση χρήστη θα παρουσιάζει στο χρήστη το εισερχόμενο ταχυδρομείο. Επιπλέον, το SMTP δεν καθορίζει πώς θα αποθηκεύεται η αλληλογραφία ή πόσο συχνά θα προσπαθεί το σύστημα ταχυδρομείου να στείλει τα μηνύματα. (Comer, 2001 4η Αμερικάνικη Έκδοση)

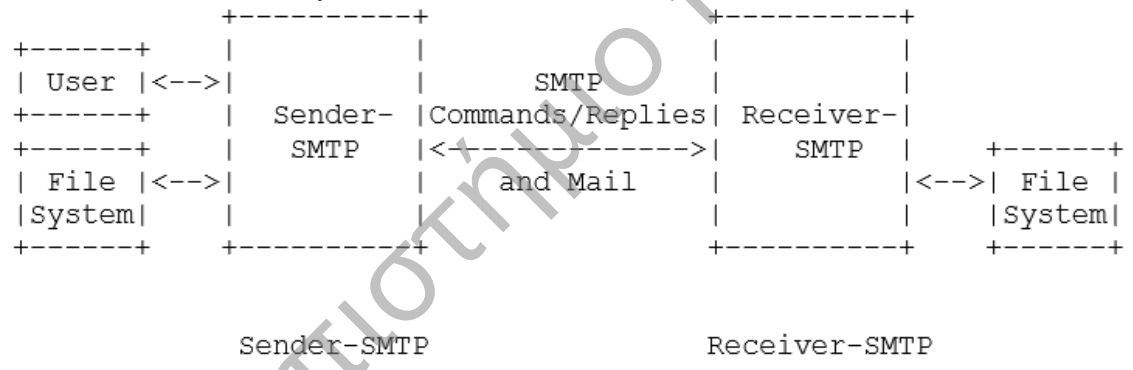
2.4.1 Simple Mail Transfer Protocol (SMTP)

Το Simple Mail Transfer Protocol είναι γνωστό με τα αρχικά SMTP. Οι πρώτες λέξεις του συνοψίζουν το σκοπό αυτού του πρωτοκόλλου αρκετά λακωνικά : «Ο στόχος για το απλό πρωτόκολλο μεταφοράς αλληλογραφίας (SMTP) είναι να μεταφέρει mail αξιόπιστα και αποτελεσματικά»

Το SMTP λοιπόν είναι ένα πρότυπο για το ηλεκτρονικό ταχυδρομείο (e-mail) για μετάδοση σε δίκτυα βασισμένα στο πρωτόκολλο Internet (IP). Το SMTP στην αρχή προτάθηκε από το RFC 821 (το 1982), και ενημερώθηκε τελευταία από το RFC 5321 (το 2008) που περιέχει το Extended SMTP (ESMTP) και είναι το πρωτόκολλο που χρησιμοποιείται ευρέως σήμερα. Το SMTP χρησιμοποιεί τη θύρα TCP 25. Οι συνδέσεις SMTP προστατεύονται από το πρωτόκολλο SSL και είναι γνωστό ως SMTPS . (Wikipedia, Simple Mail Transfer Protocol, 2008)

❖ **Βασική Ιδέα**

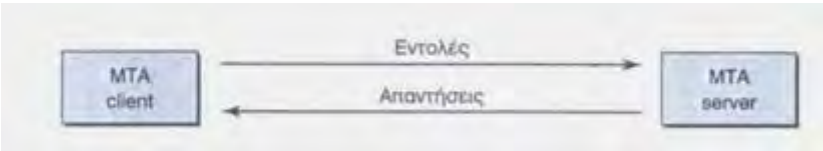
Ο σχεδιασμός του SMTP βασίζεται στο ακόλουθο μοντέλο επικοινωνίας: ο χρήστης κάνει ένα αίτημα για mail, ο αποστολέας δημιουργεί ένα αμφίδρομο κανάλι μετάδοσης με το δέκτη. Ο δέκτης μπορεί να είναι είτε ο τελικός προορισμός (user account) ή ενδιάμεσος (mail server). Στη συνέχεια ο αποστολέας παράγει SMTP-εντολές που αποστέλλονται στον παραλήπτη. Ενώ ο παραλήπτης από την άλλη απαντά. (Jonathan B. Postel-Information Sciences Institute University of Southern California, 1982)



Εικόνα 19: Το Μοντέλο SMTP πηγή εικόνας: (Jonathan B. Postel-Information Sciences Institute University of Southern California, 1982)

❖ **Εντολές και απαντήσεις**

Το SMTP χρησιμοποιεί εντολές και απαντήσεις για να μεταφέρει μηνύματα μεταξύ MTA client και MTA server (δείτε την παρακάτω Εικόνα). Κάθε εντολή ή απάντηση τελειώνει σε μία ένδειξη δύο χαρακτήρων για το τέλος της γραμμής (χαρακτήρας επιστροφής και αλλαγή γραμμής). (Behrouz A. Forouzan, 2005)



Εικόνα 20: «Εντολές και απαντήσεις του SMTP» πηγή εικόνας: Behrouz A. Forouzan, 2005

❖ **Εντολές**

Οι εντολές αποστέλλονται από τον client στο server. Η μορφή μίας εντολής φαίνεται στην στον Πίνακα 2. Αποτελείται από μία λέξη που ακολουθείται από κανένα ή περισσότερα ορίσματα. Το SMTP ορίζει 14 εντολές. Οι πρώτες πέντε είναι υποχρεωτικές και κάθε υλοποίηση πρέπει να τις υποστηρίζει. Οι επόμενες τρεις συχνά χρησιμοποιούνται και συστήνονται ανεπιφύλακτα. Οι τελευταίες έξι χρησιμοποιούνται σπάνια. Οι εντολές καταγράφονται στον Πίνακα 2 και περιγράφονται πιο αναλυτικά παρακάτω. (Behrouz A. Forouzan, 2005)

Όνομα	Μορφή εντολής	Περιγραφή
HELO	HELO <SP> <domain> <CRLF>	Αποστολή ταυτότητας
MAIL	MAIL <SP> FROM:<reverse-path> <CRLF>	Αναγνώριση παραλήπτη μηνύματος
RCPT	RCPT <SP> TO:<forward-path> <CRLF>	Αναγνώριση δημιουργού μηνύματος
DATA	DATA <CRLF>	Μεταφορά κειμένου μηνύματος
RSET	RSET <CRLF>	Ματαίωση τρέχουσας συναλλαγής αλληλογραφίας
NOOP	NOOP <CRLF>	Καμία λειτουργία
QUIT	QUIT <CRLF>	Τερματισμός σύνδεσης TCP
SEND	SEND <SP> FROM:<reverse-path> <CRLF>	Αποστολή μηνύματος στο τερματικό
SOML	SOML <SP> FROM:<reverse-path> <CRLF>	Αποστολή μηνύματος στο τερματικό, αν είναι εφικτό, αλλιώς στη θυρίδα ηλεκτρονικής αλληλογραφίας
SAML	SAML <SP> FROM:<reverse-path> <CRLF>	Αποστολή μηνύματος στο τερματικό και στη θυρίδα ηλεκτρονικής αλληλογραφίας
VRFY	VRFY <SP> <string> <CRLF>	Επιβεβαίωση ονόματος χρήστη
EXPN	EXPN <SP> <string> <CRLF>	Επιστροφή ιδιότητας μέλους της λίστας αλληλογραφίας
HELP	HELP [<SP> <string>] <CRLF>	Αποστολή τεκμηρίωσης σχετικά με το σύστημα
TURN	TURN <CRLF>	Αντιστροφή των ρόλων αποστολέα και δέκτη

Πίνακας 2: «Εντολές SMTP» πηγή εικόνας: Behrouz A. Forouzan, 2005

- **HELO**. Αυτή η εντολή χρησιμοποιείται από τον client για να πιστοποιηθεί. Το όρισμα είναι το όνομα τομέα του κεντρικού υπολογιστή client. Η μορφή είναι:

HEIO: challenger.atc.fhda.edu

- **MAIL FROM**. Αυτή η εντολή χρησιμοποιείται από τον client για να αναγνωρίσει τον αποστολέα του μηνύματος. Το όρισμα είναι η διεύθυνση email του αποστολέα (τοπικό μέρος συν όνομα τομέα). Η μορφή είναι :

MAIL FROM: forouzan@challenger.atc.fhda.edu

- **RCPT TO**. Αυτή η εντολή χρησιμοποιείται από τον client για να αναγνωρίσει τον παραλήπτη του μηνύματος. Το όρισμα είναι η διεύθυνση email του παραλήπτη. Αν υπάρχουν πολλοί παραλήπτες, η εντολή επαναλαμβάνεται. Η μορφή είναι :

RCPT TO: betsy@mcgraw-hil.com

- **DATA**. Αυτή η εντολή χρησιμοποιείται για να σταλεί το μήνυμα. Όλες οι γραμμές που ακολουθούν την εντολή DATA αντιμετωπίζονται ως μήνυμα. Το μήνυμα τελειώνει με μία γραμμή που περιέχει μόνο μία τελεία. Η μορφή είναι :

```
DATA
This is the message
to be sent to the McGraw-Hill
Company
.
```

- **QUIT**. Αυτή η εντολή τελειώνει το μήνυμα. Η μορφή είναι :

```
QUIT
```

- **RSET**. Αυτή η εντολή αναστέλλει την τρέχουσα συναλλαγή αλληλογραφίας. Οι αποθηκευμένες πληροφορίες για τον αποστολέα και τον παραλήπτη διαγράφονται. Η σύνδεση θα μηδενιστεί.

```
RSET
```

- **VRFY**. Αυτή η εντολή χρησιμοποιείται για να επικυρωθεί η διεύθυνση του παραλήπτη, η οποία αποστέλλεται ως όρισμα. Ο αποστολέας μπορεί να ζητήσει από τον παραλήπτη να επιβεβαιώσει ότι ένα όνομα ανήκει σε έναν έγκυρο παραλήπτη. Η μορφή του είναι :

```
VRFY: betsy@mcgraw-hill.com
```

- **NOOP**. Αυτή η εντολή χρησιμοποιείται από τον client για να ελέγξει την κατάσταση του παραλήπτη. Απαιτεί μία απάντηση από τον παραλήπτη. Η μορφή του είναι :

```
NOOP
```

- **TURN**. Αυτή η εντολή επιτρέπει στον αποστολέα και τον παραλήπτη να αλλάξουν Θέσεις, δηλαδή ο αποστολέας να γίνει παραλήπτης και αντιστρόφως. Οι περισσότερες όμως SMTP υλοποιήσεις σήμερα δεν υποστηρίζουν αυτήν την ιδιότητα. Η μορφή είναι :

```
TURN
```

- **EXPN**. Αυτή η εντολή ζητά από τον παραλήπτη κεντρικό υπολογιστή να επεκτείνει τη λίστα αλληλογραφίας που αποστέλλεται ως όρισμα και να επιστρέψει τις διευθύνσεις γραμματοκιβωτίου του παραλήπτη που περιέχονται στη λίστα. Η μορφή είναι :

```
EXPN: x y z
```

- **HEIP**. Αυτή η εντολή ζητά από το παραλήπτη να στείλει πληροφορίες για την εντολή που αποστέλλεται ως όρισμα. Η μορφή είναι:

```
HEIP: mail
```

- **SEND FROM.** Αυτή η εντολή ορίζει ότι το μήνυμα πρέπει να παραδοθεί στο τερματικό του παραλήπτη και όχι στο γραμματοκιβώτιο. Αν ο παραλήπτης δεν είναι συνδεδεμένος, το μήνυμα επιστρέφεται. Το όρισμα είναι η διεύθυνση του αποστολέα. Η μορφή είναι :

```
SEND FROM: forouzan@fhda.atc.edu
```

- **SMOL FROM**. Αυτή η εντολή ορίζει ότι το μήνυμα πρέπει να παραδοθεί στο τερματικό ή το γραμματοκιβώτιο του παραλήπτη. Αυτό σημαίνει ότι αν ο παραλήπτης

είναι συνδεδεμένος, το μήνυμα παραδίδεται μόνο στο τερματικό. Αν ο παραλήπτης δεν είναι συνδεδεμένος, το μήνυμα παραδίδεται στο γραμματοκιβώτιο. Το όρισμα είναι η διεύθυνση του αποστολέα. Η μορφή είναι :

SMOL FROM: forouzan@fhda.atc.edu

- **SMAL FROM**. Αυτή η εντολή ορίζει ότι το μήνυμα πρέπει να παραδοθεί στο τερματικό και το γραμματοκιβώτιο του παραλήπτη. Αυτό σημαίνει ότι αν ο παραλήπτης είναι συνδεδεμένος, το μήνυμα παραδίδεται στο τερματικό και το γραμματοκιβώτιο. Αν ο παραλήπτης δεν είναι συνδεδεμένος, το μήνυμα παραδίδεται μόνο στο γραμματοκιβώτιο. Το όρισμα είναι η διεύθυνση του αποστολέα. Η μορφή είναι :

SMAL FROM: forouzan@fhda.atc.edu

Αποκρίσεις :

Οι αποκρίσεις αποστέλλονται από το server στον client. Μία απάντηση είναι ένας κωδικός τριών ψηφίων και πιθανόν να ακολουθείται από περαιτέρω πληροφορίες σε κείμενο. Το αρχικό ψηφίο δείχνει την κατηγορία της απόκρισης:

- **y z-Θετική Απόκριση Ολοκλήρωσης :** Αν το πρώτο ψηφίο είναι **2** (το ψηφίο 1 δεν χρησιμοποιείται σήμερα), αυτό σημαίνει ότι η αιτούμενη ενέργεια έχει ολοκληρωθεί επιτυχώς. Είναι δυνατή η εκκίνηση μιας νέας αίτησης.
- **3 y z-Θετική Ενδιάμεση Απόκριση:** Αν το πρώτο ψηφίο είναι **3**, σημαίνει ότι η εντολή έχει γίνει αποδεκτή, αλλά η αιτούμενη ενέργεια βρίσκεται σε εκκρεμότητα. αναμένοντας τη λήψη περαιτέρω πληροφοριών. Ο αποστολέας SMTP πρέπει να στείλει μία άλλη εντολή με την οποία προσδιορίζει αυτές τις πληροφορίες. Αυτή η απόκριση χρησιμοποιείται οε ομάδες ακολουθίας εντολών.
- **4 y z-Μεταβατική Αρνητική Απόκριση Ολοκλήρωσης:** Αν το πρώτο ψηφίο είναι 4, σημαίνει ότι η εντολή δεν έγινε αποδεκτή και η αιτούμενη ενέργεια δεν έχει εκτελεστεί. Ωστόσο, η συνθήκη σφάλματος είναι προσωρινή και η αιτούμενη ενέργεια είναι δυνατόν να ζητηθεί εκ νέου.
- **5 y z- Μόνιμη Αρνητική Απόκριση Ολοκλήρωσης:** Αν το πρώτο ψηφίο είναι 5, σημαίνει ότι η εντολή δεν έγινε αποδεκτή και η αιτούμενη ενέργεια δεν έχει εκτελεστεί.

Το δεύτερο και το τρίτο ψηφίο παρέχουν επιπλέον λεπτομέρειες για τις απαντήσεις.

Ο Πίνακας 2 παρουσιάζει τις SMTP αποκρίσεις.

(Stallings, 2011), (Behrouz A. Forouzan, 2005)

Πίνακας 3: «SMTP αποκρίσεις»

ΚΩΔΙΚΟΣ	ΠΕΡΙΓΡΑΦΗ
211	Κατάσταση συστήματος ή απάντηση βοήθειας συστήματος
214	Μηνύματα βοήθειας
220	<domain> Υπηρεσία έτοιμη
221	<domain> Η υπηρεσία κλείνει το κανάλι μετάδοσης
250	Εντολή αίτησης ολοκληρώθηκε
251	Ο χρήστης δεν είναι τοπικός και το μήνυμα θα προωθηθεί (<forward-path>)
354	Εκκίνηση εισόδου μηνυμάτων. Τερματισμός με τους χαρακτήρες <CRLF><CRLF>
421	<domain> Η Υπηρεσία δεν είναι διαθέσιμη, Απώλεια καναλιού μετάδοσης
450	Το γραμματοκιβώτιο-θυρίδα δεν είναι διαθέσιμο
451	Αναστολή εντολής, τοπικό σφάλμα επεξεργασίας
452	Αναστολή εντολής, ανεπαρκής χώρος αποθήκευσης
500	Συντακτικό λάθος, μη αναγνωρισμένη εντολή
501	Συντακτικό λάθος, σε παραμέτρους ή ορίσματα
502	Εντολή μη υλοποιημένη
503	Κακή ακολουθία εντολών
504	Η εντολή προσωρινά δεν είναι υλοποιημένη
550	Η εντολή δεν εκτελείται, το γραμματοκιβώτιο δεν είναι διαθέσιμο
551	Ο χρήστης δεν είναι τοπικός
552	Αναστολή αιτούμενης ενέργειας , υπέρβαση μνήμης
553	Η αιτηθείσα ενέργεια δεν εκτελέστηκε, το όνομα του γραμματοκιβωτίου δεν επιτρέπεται
554	Η συναλλαγή απέτυχε- αποτυχία μετάδοσης

(Behrouz A. Forouzan, 2005) (Stallings, 2011)

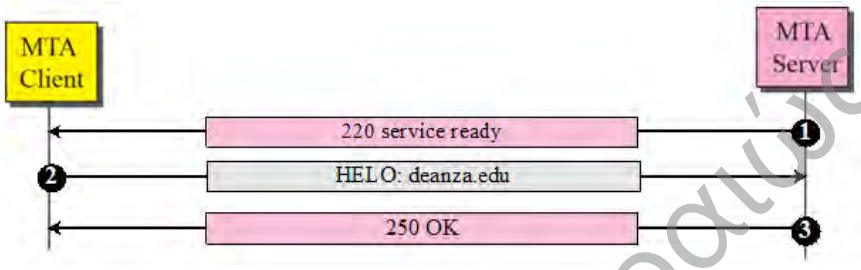
Η βασική λειτουργία του πρωτοκόλλου SMTP υλοποιείται σε τρεις φάσεις: αποκατάσταση σύνδεσης. ανταλλαγή ενός ή περισσότερων ζευγών εντολών-αποκρίσεων, και τερματισμός σύνδεσης. Εξετάζουμε κατά σειρά κάθε φάση. (Stallings, 2011)

Φάσεις μεταφοράς αλληλογραφίας:

Η διαδικασία μεταφοράς ενός μηνύματος αλληλογραφίας γίνεται σε τρεις φάσεις: έναρξη σύνδεσης, μεταφορά αλληλογραφίας και τερματισμό σύνδεσης.

1. **Έναρξη σύνδεσης**

Αφού ένας client έχει πραγματοποιήσει μία TCP σύνδεση στη γνωστή Θύρα 25, ο SMTP server ξεκινά τη φάση σύνδεσης. Αυτή η φάση γίνεται με τα επόμενα τρία βήματα, τα οποία βλέπετε στην Εικόνα 21.



Εικόνα 21: «Έναρξη Σύνδεσης» πηγή εικόνας: Behrouz A. Forouzan, 2005

- Ο server στέλνει τον κωδικό **220** (υπηρεσία έτοιμη) για να ενημερώσει τον client ότι είναι έτοιμος να δεχθεί αλληλογραφία. Αν ο server δεν είναι έτοιμος, στέλνει τον κωδικό **421** (η υπηρεσία δεν είναι διαθέσιμη) και η διαδικασία τερματίζεται εδώ .
- Ο client στέλνει το μήνυμα **HELO** για να αναγνωριστεί με τη διεύθυνση του ονόματος τομέα του. Αυτό το βήμα είναι απαραίτητο για να ενημερωθεί ο server για το όνομα τομέα του client. Θυμηθείτε ότι κατά την έναρξη της TCP σύνδεσης, ο αποστολέας και ο παραλήπτης γνωρίζουν ο ένας τον άλλον μέσω των διευθύνσεων IP τους.
- Ο server απαντά με τον κωδικό 250 (η αιτηθείσα εντολή ολοκληρώθηκε) ή κάποιον άλλο κωδικό, ανάλογα με την κατάσταση.

2. **Μεταφορά μηνύματος**

Αφού ιδρυθεί η σύνδεση μεταξύ των SMTP client και server, μπορεί να γίνει ανταλλαγή ενός μηνύματος μεταξύ ενός αποστολέα και ενός ή περισσότερων παραληπτών. Αυτή η φάση γίνεται σε οκτώ βήματα. Τα βήματα 3 και 4 επαναλαμβάνονται αν υπάρχουν περισσότεροι από έναν παραλήπτες .

- Ο client στέλνει το μήνυμα **MAIL FROM** για να γνωστοποιήσει τον αποστολέα του μηνύματος. Συμπεριλαμβάνει τη διεύθυνση του αποστολέα (γραμματοκιβώτιο και όνομα τομέα). Αυτό το βήμα είναι απαραίτητο για να δώσει ο server τη διεύθυνση επιστροφής για επιστροφή μηνυμάτων λάθους και αναφοράς.
- Ο server απαντά με τον κωδικό **250** αν είναι προετοιμασμένος να δεχθεί μηνύματα διαφορετικά θα επιστρέψει μία απόκριση ένδειξης αποτυχίας εκτέλεσης εντολής (κωδικοί 451. 452. 552) ή σφάλματος της εντολής (κωδικοί 421.500.501).
- Ο client στέλνει το μήνυμα **RCPT TO** (παραλήπτης), το οποίο συμπεριλαμβάνει τη διεύθυνση του παραλήπτη.

Η εντολή **RCPT** αναγνωρίζει ένα μεμονωμένο δέκτη των δεδομένων του μηνύματος. Πολλαπλοί παραλήπτες προσδιορίζονται με πολλαπλή χρήση αυτής της εντολής. Μία ξεχωριστή απόκριση επιστρέφεται για κάθε εντολή **RCPT**, με μία από τις ακόλουθες πιθανότητες:

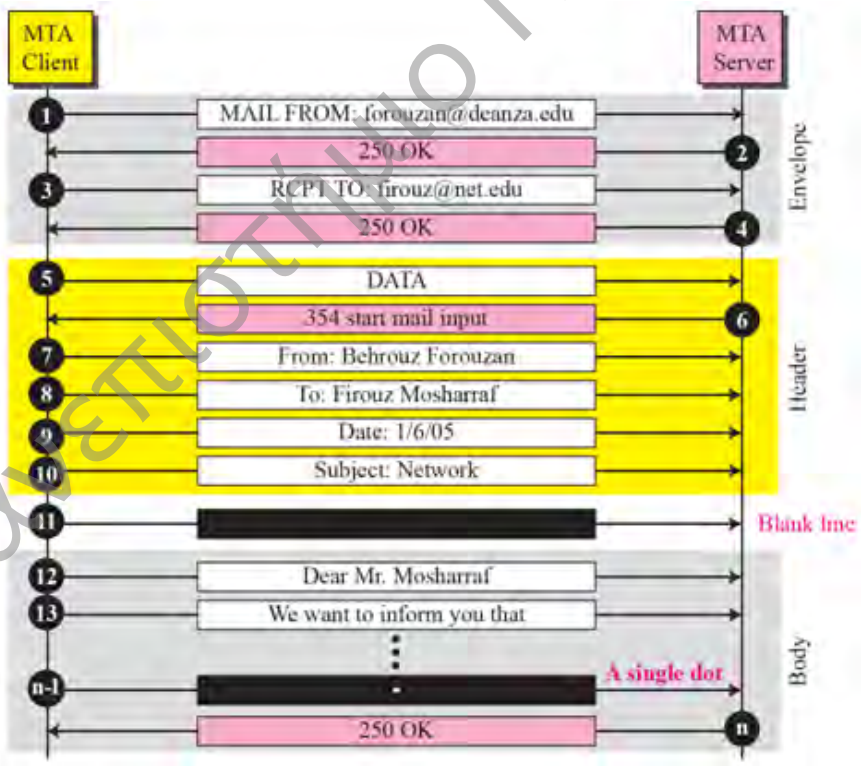
- Ο δέκτης αποδέχεται τον προορισμό με απόκριση 250. Αυτό δείχνει ότι η καθορισμένη θυρίδα ηλεκτρονικής αλληλογραφίας βρίσκεται στο σύστημα του δέκτη.

- Ο προορισμός θα απαιτεί προώθηση και ο δέκτης θα προωθήσει (251).
- Ο προορισμός απαιτεί προώθηση αλλά ο δέκτης δεν προωθεί. Ο αποστολέας πρέπει να στείλει το μήνυμα εκ νέου στη διεύθυνση προώθησης (551).
- Δεν υπάρχει θυρίδα ηλεκτρονικής αλληλογραφίας για το συγκεκριμένο προορισμό σε αυτόν τον κεντρικό υπολογιστή (550).
- Ο προορισμός απορρίπτεται λόγω κάποιας αποτυχίας στην εκτέλεση (κωδικοί 450. 451. 452. 552.553) ή λόγω ενός σφάλματος της εντολής (κωδικοί 421.500.501.503).

Το πλεονέκτημα από τη χρήση μιας ξεχωριστής φάσης RCPT είναι ότι ο αποστολέας δεν θα στείλει το μήνυμα έως ότου βεβαιωθεί ότι ο δέκτης είναι προετοιμασμένος να λάβει το μήνυμα **για έναν τουλάχιστον παραλήπτη**, αποφεύγοντας επομένως την επιβάρυνση αποστολής ολόκληρου του μηνύματος μόνο για να μάθει ότι ο προορισμός είναι άγνωστος. Από τη στιγμή που ο δέκτης SMTP έχει συμφωνήσει να λάβει ένα μήνυμα ταχυδρομείου για τουλάχιστον έναν παραλήπτη.

Προσοχή: *Όταν το ίδιο μήνυμα προορίζετε σε πολλούς παραλήπτες το SMTP ορίζει τη μετάδοση μόνο για ένα αντίγραφο των δεδομένων για όλους τους παραλήπτες στο ίδιο κεντρικό υπολογιστή προορισμού*.

- Ο server απαντά με τον κωδικό 250 ή κάποιον άλλο κατάλληλο κωδικό.
- Ο client στέλνει το μήνυμα DATA για να αρχικοποιήσει τη μεταφορά μηνύματος.



Εικόνα 22: «Μεταφορά μηνύματος» πηγή εικόνας: Behrouz A. Forouzan, 2005

- Ο server απαντά με τον κωδικό **354** (εκκίνηση εισόδου αλληλογραφίας) σε διαφορετική περίπτωση ο δέκτης επιστρέφει μία απόκριση με την οποία δείχνει ότι

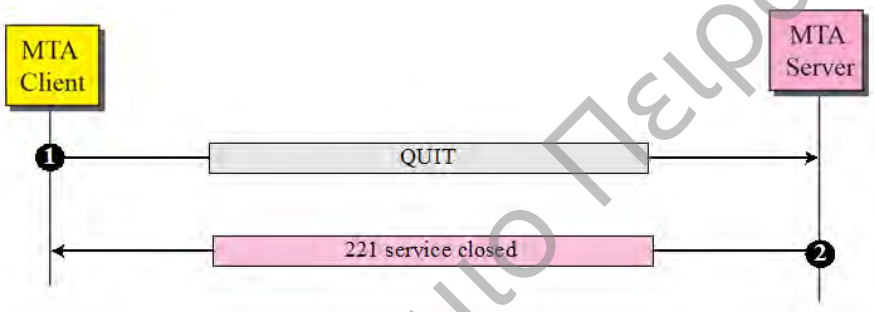
υπάρχει αδυναμία εκτέλεσης της εντολής (κωδικοί 451,554) ή ότι υπάρχει σφάλμα εντολής (κωδικοί 421, 500, 501, 503).

- Ο client στέλνει τα περιεχόμενα του μηνύματος σε συνεχείς γραμμές. Κάθε γραμμή τερματίζεται από δύο χαρακτήρες που δείχνουν το τέλος της γραμμής (χαρακτήρας επιστροφής και αλλαγή γραμμής). Το μήνυμα τελειώνει με μία γραμμή που περιέχει μόνο μία τελεία.
- Ο server απαντά με τον κωδικό **250** (**OK**) ή με τον κατάλληλο κωδικό σφάλματος (451,452,552,554).

3. Τερματισμός σύνδεσης

Αφού το μήνυμα μεταφερθεί επιτυχώς, ο client τερματίζει τη σύνδεση. Αυτή η φάση γίνεται σε δύο βήματα (δείτε την Εικόνα 20.18).

- Ο client στέλνει την εντολή **QUIT**.
- Ο server απαντά με τον κωδικό **221** ή κάποιον άλλο κατάλληλο κωδικό. Μετά τη φάση τερματισμού σύνδεσης, η TCP σύνδεση πρέπει να κλείσει.



Εικόνα 23: «Τερματισμός σύνδεσης» πηγή εικόνας: Behrouz A. Forouzan, 2005

Ακολουθεί ένα παράδειγμα εντολών SMTP που δείχνουν ένα mail που στέλνεται από τον χρήστη Smith από τον server mail Alpha.ARPA, στους χρήστες Jones, Green και Brown στον server mail Beta.ARPA. Υποθέτοντας ότι οι servers mail Alpha και Beta επικοινωνούν άμεσα χωρίς ενδιάμεσο server.

S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

Ο αποστολέας SMTP μεταδίδει ένα μήνυμα που προέρχεται από το χρήστη Smith@Alpha.ARPA. Το μήνυμα προορίζεται για τρεις χρήστες στο server Beta.ARPA. και ειδικότερα στους **Jones , Green και Brown**. Ο δέκτης SMTP δείχνει ότι διαθέτει θυρίδες ηλεκτρονικής αλληλογραφίας για τους δύο πρώτους χρήστες (Jones. Green). αλλά δεν διαθέτει καμία πληροφορία για το χρήστη Brown. Επειδή τουλάχιστον ένας από τους επιθυμητούς παραλήπτες έχει επαληθευτεί ,ο αποστολέας προχωρά στην αποστολή του μηνύματος κειμένου. (Jonathan B. Postel-Information Sciences Institute University of Southern California, 1982)

Το SMTP είναι πιο περίπλοκο από αυτό που περιγράφτηκε. Για παράδειγμα , αν ένας χρήστης έχει μετακινηθεί, ο διακομιστής μπορεί να γνωρίζει τη νέα διεύθυνση της θυρίδας του. Το SMTP επιτρέπει στο διακομιστή να πληροφορήσει τον πελάτη για τη νέα διεύθυνση , ο διακομιστής μπορεί να επιλέξει να προωθήσει την αλληλογραφία που ενεργοποίησε το μήνυμα μήνυμα αυτό, ή μπορεί να ζητήσει από τον πελάτη να αναλάβει την ευθύνη της προώθησης. (Comer, 2001 4η Αμερικάνικη Έκδοση)

Ενώ οι mail servers και άλλοι mail transfer agents χρησιμοποιούν το SMTP για αποστολή και λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου, σε επίπεδο εφαρμογής χρήστη-πελάτη ηλεκτρονικού ταχυδρομείου συνήθως χρησιμοποιούν μόνο SMTP για την αποστολή μηνυμάτων σε ένα διακομιστή αλληλογραφίας για μετεγκατάσταση. Για τη λήψη μηνυμάτων, εφαρμογές client συνήθως χρησιμοποιούν είτε το **Post Office Protocol (POP**) ή το **Internet**

Message Access Protocol (IMAP) ή ένα ιδιόκτητο σύστημα (όπως το Microsoft Exchange ή Lotus Notes / Domino) να αποκτήσουν πρόσβαση στα mail boxes του διακομιστή αλληλογραφίας. (Wikipedia, Simple Mail Transfer Protocol, 2008)

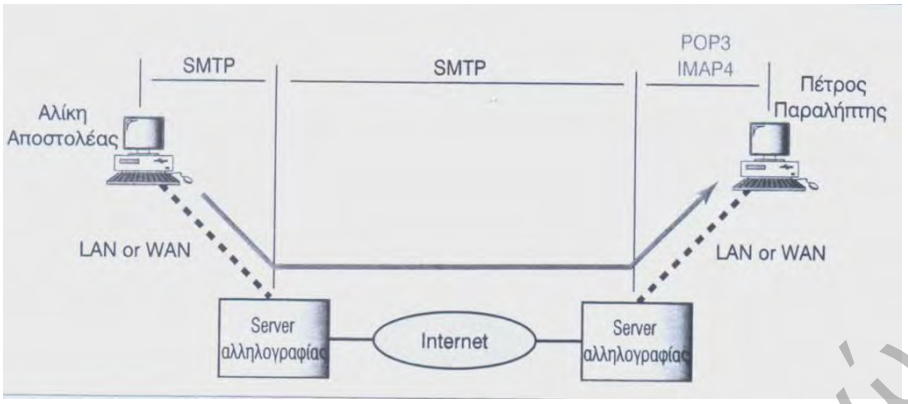
2.5 ΑΝΑΚΤΗΣΗ ΑΛΛΗΛΟΓΡΑΦΙΑΣ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΧΕΙΡΙΣΜΟΥ ΓΡΑΜΜΑΤΟΚΙΒΩΤΙΩΝ

Η μέθοδος μεταφοράς SMTP που περιγράφτηκε προηγουμένως συνεπάγεται ότι ο διακομιστής πρέπει να παραμένει πάντα έτοιμος για να δέχεται ηλεκτρονικό ταχυδρομείο. Ο πελάτης προσπαθεί να στείλει το μήνυμα μόλις ένας χρήστης το πληκτρολογήσει. Το σενάριο αυτό δουλεύει καλά όταν ο διακομιστής λειτουργεί σε έναν υπολογιστή που έχει σύνδεση μόνο κατά περιόδους. Για παράδειγμα αν σε ένα χρήστη που έχει πρόσβαση στο Internet μόνο μέσω τηλεφώνου δεν θα έχει κανένα νόημα να λειτουργήσει ένας συμβατικός διακομιστής ηλεκτρονικού ταχυδρομείου , επειδή ο διακομιστής θα είναι διαθέσιμος μόνον όταν ο χρήστης θα συνδεθεί με το Internet. Με αποτέλεσμα όλες οι άλλες προσπάθειες για επικοινωνία με το διακομιστή θα αποτυγχάνουν και η ηλεκτρονική αλληλογραφία που στέλνεται στο χρήστη θα παραμένει ανεπίδοτη. Προκύπτει λοιπόν το ερώτημα «Πώς μπορεί ένας χρήστης που δεν έχει μόνιμη σύνδεση να λαμβάνει ηλεκτρονικό ταχυδρομείο;»

Η απάντηση του ερωτήματος αυτού βρίσκεται σε μία διαδικασία παράδοσης με δύο στάδια. Στο πρώτο στάδιο, σε κάθε χρήστη εκχωρείται ένα γραμματοκιβώτιο σε κάποιον υπολογιστή που έχει μόνιμη σύνδεση με το Internet. Ο υπολογιστής αυτός λειτουργεί ένα συμβατικό διακομιστή SMTP, ο οποίος παραμένει πάντα έτοιμος για να δεχτεί ηλεκτρονική αλληλογραφία. Στο δεύτερο στάδιο, ο χρήστης πραγματοποιεί μία σύνδεση μέσω τηλεφώνου και στη συνέχεια , λειτουργεί ένα πρωτόκολλο το οποίο ανακτά μηνύματα στον υπολογιστή του χρήστη, όπου είναι δυνατή η ανάγνωση τους. Πιο συγκεκριμένα το SMTP είναι ένα πρωτόκολλο γνωστό ως «πρωτόκολλο ώθησης», ωθεί δηλαδή το μήνυμα από τον client στον server από την άλλη όμως χρειάζεται και ένα «πρωτόκολλο εξαγωγής», για να μπορέσει ο client να εξάγει τα μηνύματα από τον server.

Υπάρχουν δύο πρωτόκολλα τα οποία επιτρέπουν σε έναν απομακρυσμένο χρήστη να ανακτήσει την αλληλογραφία από ένα μόνιμο γραμματοκιβώτιο αυτά είναι το **Post Office Protocol, έκδοση 3 (POP3)** και το **Internet Message Access Protocol** έκδοση 4 (**IMAP4)**. Τα πρωτόκολλα έχουν παρόμοιες λειτουργίες: εκτός από την παροχή πρόσβασης, το καθένα από τα πρωτόκολλα αυτά επιτρέπει στο χρήστη να χειρίζεται το περιεχόμενο του γραμματοκιβώτιου (π.χ. να διαγράφει μόνιμα ένα μήνυμα). Η εικόνα 24 παρουσιάζει τη θέση αυτών των δύο πρωτοκόλλων στη πιο συνηθισμένη περίπτωση. Οι δύο επόμενες ενότητες περιγράφουν τα δύο αυτά πρωτόκολλα.

(Comer, 2001 4η Αμερικάνικη Έκδοση) (Behrouz A. Forouzan, 2005)



Εικόνα 24: «Χρήση Πρωτοκόλλων» πηγή εικόνας: Behrouz A. Forouzan, 2005

2.5.1 Πρωτοκολλο Ταχυδρομειου POP3

Το πιο γνωστό πρωτόκολλο που χρησιμοποιείται για μεταφορά μηνυμάτων από ένα μόνιμο γραμματοκιβώτιο σε έναν τοπικό υπολογιστή είναι η **έκδοση 3** του **Πρωτοκόλλου Ταχυδρομείου (Post Office Protocol, POP3)** χρησιμοποιώντας σύνδεση TCP/IP.

Αξίζει να σημειωθεί ότι ο υπολογιστής με το σταθερό γραμματοκιβώτιο πρέπει να εκτελεί δύο διακομιστές:

- έναν διακομιστή SMTP, ο οποίος δέχεται την αλληλογραφία που στάλθηκε στο χρήστη και προσθέτει κάθε εισερχόμενο μήνυμα στο μόνιμο γραμματοκιβώτιο του χρήστη και,
- έναν διακομιστή POP3, ο οποίος επιτρέπει σε έναν χρήστη να εξάγει και να διαγράφει μηνύματα από το γραμματοκιβώτιο.

Για να εξασφαλιστεί η σωστή λειτουργία , οι δύο διακομιστές θα πρέπει να συντονίζουν τη χρήση του γραμματοκιβώτιου, έτσι ώστε αν φτάσει μέσω SMTP ένα μήνυμα όσο ο χρήστης εξάγει μηνύματα μέσω του POP3, το γραμματοκιβώτιο να μένει σε μία έγκυρη κατάσταση. (Comer, 2001 4η Αμερικάνικη Έκδοση)

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. (Wikipedia, Post Office Protocol)

Η λειτουργικότητά του πρωτοκόλλου είναι απλή. Το POP3 εκκινεί όταν ο πράκτορας χρήστη (ο πελάτης) ανοίγει μια σύνδεση TCP προς το ταχυδρομείο στη θύρα 110. Με καθορισμένη τη σύνδεση TCP, το POP3 εργάζεται σε τρεις φάσεις:

- εξουσιοδότηση,
- συναλλαγή και
- ενημέρωση.

a. Κατά τη διάρκεια της πρώτης φάσης, εξουσιοδότησης, ο πράκτορας χρήστη στέλνει ένα όνομα χρήστη και έναν κωδικό πρόσβασης για να εξουσιοδοτήσει τον χρήστη που φορτώνει το ταχυδρομείο.
b. Κατά τη διάρκεια της δεύτερης φάσης, συναλλαγής, ο πράκτορας χρήστη επαναφέρει μηνύματα. Τα μηνύματα αποθηκεύονται και μεταφέρονται ως αρχεία κειμένου στην τυπική μορφή RFC 822.Στη φάση συναλλαγής, ο πράκτορας χρήστη μπορεί επίσης να σημάνει μηνύματα για διαγραφή, να αφαιρέσει σημάνσεις διαγραφής και να πάρει στατιστικά στοιχεία ταχυδρομείου.
c. Η τρίτη φάση, ενημέρωσης, γίνεται μετά την έκδοση από τον πελάτη της εντολής quit, η οποία τερματίζει τη σύνδεση POP3. Εκείνη την ώρα, ο εξυπηρετητής ταχυδρομείου διαγράφει τα μηνύματα που έχουν σημανθεί για διαγραφή.

Σε μια συναλλαγή POP3, ο πράκτορας χρήστη εκδίδει εντολές, και ο εξυπηρετητής αποκρίνεται σε κάθε εντολή με μια απόκριση. Υπάρχουν δύο πιθανές αποκρίσεις:

- **+ok** , η οποία χρησιμοποιείται από τον εξυπηρετητή για να δηλώσει ότι η προηγούμενη εντολή πήγε καλά, και
- **-ERR** , που χρησιμοποιείται από τον εξυπηρετητή για να δηλώσει ότι κάτι πήγε λάθος με την προηγούμενή εντολή.

Η φάση εξουσιοδότησης έχει δύο κύριες εντολές:

i. user <user name> και
ii. pass <pass-word>

Αν εκτελεστεί η εντολή: `Telnet` απευθείας σε ένα POP3 εξυπηρετητή, χρησιμοποιώντας τη Θύρα 110, δίνοντας τις παρακάτω εντολές, υποθέτοντας ότι `mailserver` είναι το όνομα ενός εξυπηρετητή ταχυδρομείου.

Έχουμε το εξής αποτέλεσμα:

telnet mailServer 110
+OK POP3 server ready
user bob
+OK
pass hungry
+OK user successfully logged on

Αν γραφτεί λανθασμένα η εντολή, ο POP3 εξυπηρετητής θα απαντήσει με ένα μήνυμα ERR.

Στη φάση συναλλαγής όμως ένας πράκτορας χρήστη που χρησιμοποιεί POP3 μπορεί συχνά να παραμετροποιηθεί (από τον χρήστη), ώστε να "φορτώνει και να διαγράφει" ή να "φορτώνει και να κρατά". Η αλληλουχία εντολών που εκδίδονται από έναν πράκτορα χρήστη POP3 εξαρτάται από το με ποιον από τους δύο αυτούς τρόπους λειτουργίας λειτουργεί ο πράκτορας χρήστη. Στον τρόπο λειτουργίας φόρτωσης και διαγραφής, ο πράκτορας χρήστη Θα εκδώσει τις εντολές: **`list, retr και dele.`**

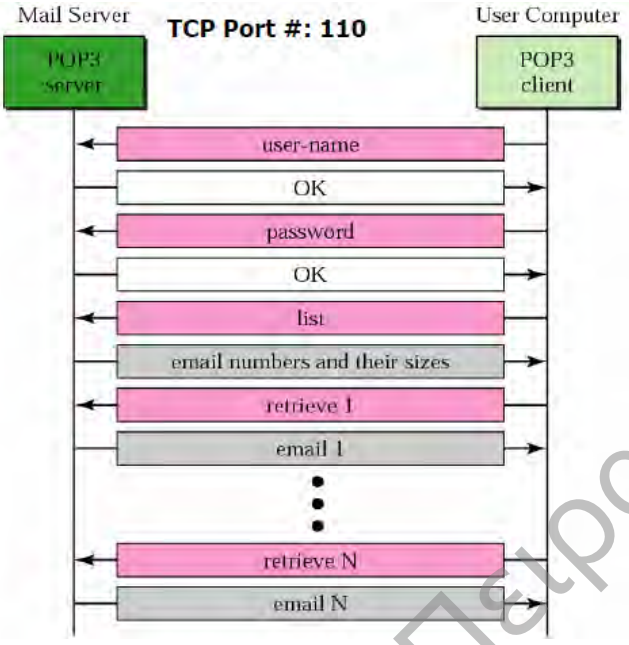
Σαν παράδειγμα, υποθέστε ότι ο χρήστης έχει δύο μηνύματα στην ταχυδρομική του Θυρίδα. Στον διάλογο που φαίνεται παρακάτω όπου:

C: (πελάτης) είναι ο πράκτορας χρήστη και
S: (εξυπηρετητής) είναι ο εξυπηρετητής ταχυδρομείου.

Η συναλλαγή Θα είναι κάπως έτσι:

```
C: list        # Ο πράκτορας χρήστη ζητά από τον εξυπηρετητή ταχυδρομείου να αναφέρει το μέγεθος κάθε αποθηκευμένου μηνύματος.
S: 1 498
S: 2 912
S: .
C: retr 1                  # επαναφέρει το 1ο μήνυμα από τον εξυπηρετητή
S: (blah blah .....
S: ....
S: ..... blah)
S: .
C: dele 1                  # διαγράφει το 1ο μήνυμα
C: retr 2                  # επαναφέρει το 2ο μήνυμα από τον εξυπηρετητή
S: (blah blah ...
S: .....
S: .... blah)
S: .
C: dele 2                  # διαγράφει το 2ο μήνυμα
C: quit                    #τερματίζει τη σύνδεση
S: +OK POP3 server signing off
```

Σημειώστε ότι μετά τη φάση εξουσιοδότησης, ο πράκτορας χρήστη χρησιμοποίησε μόνο τέσσερεις εντολές: `list`, `retr`, `dele` και `quit`. Η σύνταξη αυτών των εντολών ορίζεται στο RFC 1939. Μετά την επεξεργασία της εντολής `quit`, ο εξυπηρετητής POP3 εισέρχεται στη φάση ενημέρωσης και αφαιρεί τα μηνύματα 1 και 2 από την ταχυδρομική θυρίδα. (Kurose&Ross, 2008)



Εικόνα 25: «Σύνδεση POP3» πηγή εικόνας: Behrouz A. Forouzan, 2005

Το POP3 επιτρέπει την ανάγνωση των email μονάχα από τον υπολογιστή στον οποίο έχουν κατέβει. Για να αποδεχθεί ο mail server την σύνδεση, θα πρέπει ο χρήστης να δώσει το όνομα χρήστη και τον κωδικό πρόσβασής του. Όπως προαναφέρθηκε χρησιμοποιεί την πόρτα 110 για να εγκαθιδρύσει μία σύνδεση με τον mail server, πολλά προγράμματα όμως ηλεκτρονικού ταχυδρομείου χρησιμοποιούν κρυπτογράφηση ούτως ώστε τα δεδομένα που διακινούνται στην σύνδεση αυτή να μην είναι αναγνώσιμα από άλλους. Κρυπτογραφημένη επικοινωνία στο POP3 επιτυγχάνεται είτε χρησιμοποιώντας την εντολή **STLS** ή με την υπηρεσία **POP3S**, η οποία συνδέεται με το διακομιστή χρησιμοποιώντας το **Transport Layer Security (TLS) ή Secure Sockets Layer (SSL)**, στη γνωστή θύρα του TCP 995.

(Wikipedia, Post Office Protocol)

2.5.2 ΔΙΑΔΙΚΤΥΑΚΟ ΠΡΩΤΟΚΟΛΛΟ ΤΑΧΥΔΡΟΜΕΙΟΥ- IMAP4

Το **Internet Message Access Protocol** ή **IMAP** είναι ένα Διαδικτυακό πρωτόκολλο για ανάκτηση των e-mail, το οποίο συνδυάζει μερικές από τις δυνατότητες που προσφέρουν το πρωτόκολλο POP3 (Post Office Protocol) και το SMTP μέσω Παγκόσμιου Ιστού (webmail). Η έκδοση IMAP που έχει καθιερωθεί σήμερα είναι η έκδοση 4, η οποία ορίζεται από το RFC 3501. Ένας διακομιστής IMAP ανοίγει μια σύνδεση TCP στη θύρα 143. Το **IMAP** έχει περισσότερα χαρακτηριστικά από το **POP3** που το κάνουν πιο ισχυρό και πιο σύνθετο καθώς επιτρέπει σε έναν χρήστη να δημιουργεί δυναμικά, να διαγράφει ή να μετονομάζει γραμματοκιβώτια.

Η πρόσβαση σε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου πραγματοποιείται μέσω ενός ειδικού προγράμματος αλληλογραφίας (προγράμματος-πελάτη όπως π.χ. το Mozilla Thunderbird). Συνήθως τα προγράμματα που υποστηρίζουν το POP3 υποστηρίζουν και το IMAP. Σε οποιονδήποτε υπολογιστή και αν βρίσκεται ο χρήστης και οποιοδήποτε πρόγραμμα ηλεκτρονικής αλληλογραφίας και αν χρησιμοποιεί για να έχει πρόσβαση στο λογαριασμό του, το IMAP τα **"βλέπει" όλα με την ίδια δομή**. Το IMAP λειτουργεί και με σύνδεση και χωρίς σύνδεση. Τα προγράμματα-πελάτες τα οποία χρησιμοποιούν το IMAP συνήθως αφήνουν τα

μηνύματα να υπάρχουν και στον διακομιστή, εκτός εάν ο χρήστης επιλέξει την διαγραφή τους. Αυτό είναι ένα από τα χαρακτηριστικά της λειτουργίας IMAP το οποίο επιτρέπει περισσότερους από ένα χρήστες να διαχειρίζονται το ίδιο λογαριασμό ηλεκτρονικού ταχυδρομείου.

Ένας IMAP εξυπηρετητής θα συσχετίσει κάθε μήνυμα με ένα φάκελο. Όταν ένα μήνυμα φτάνει για πρώτη φορά στον εξυπηρετητή συσχετίζεται με τον φάκελο **INBOX** του παραλήπτη. Ο παραλήπτης μπορεί κατόπιν να μεταφέρει το μήνυμα σε ένα νέο φάκελο, που δημιουργείται από τον χρήστη, να διαβάσει το μήνυμα, να το διαγράψει κλπ.

Το πρωτόκολλο IMAP παρέχει εντολές που επιτρέπουν σε χρήστες να δημιουργούν φακέλους και να μεταφέρουν μηνύματα από ένα φάκελο σε ένα άλλο. Το IMAP επίσης παρέχει εντολές, που επιτρέπουν σε χρήστες να κάνουν αναζήτηση σε απομακρυσμένους φακέλους για μηνύματα που ταιριάζουν με συγκεκριμένα κριτήρια. Επίσης μέσω του IMAP ένας χρήστης μπορεί να δημιουργήσει μια ιεραρχία γραμματοκιβώτιων σε ένα κατάλογο με σκοπό την καλύτερη αποθήκευση της αλληλογραφίας.

Ένα άλλο σημαντικό χαρακτηριστικό του IMAP είναι ότι έχει εντολές που επιτρέπουν σε έναν πράκτορα χρήστη να λαμβάνει πληροφορίες σχετικά με ένα μήνυμα. Για παράδειγμα, ένας πράκτορας χρήστη μπορεί να πάρει μόνο την επικεφαλίδα ενός μηνύματος ή απλώς ένα κομμάτι από ένα μήνυμα χωρίς να χρειάζεται να ανακτήσει όλο το μήνυμα. Η μερική ανάκτηση είναι εξαιρετικά χρήσιμη στις χαμηλής ταχύτητας συνδέσεις, επειδή ο χρήστης δεν θα χρειάζεται να κατεβάσει άχρηστες πληροφορίες.

Η λειτουργία του IMAP εκτελείται μέσω TCP όπου:

- ο πελάτης από τη μεριά του μηχανήματος του χρήστη δίνει εντολές με τη μορφή γραμμών ASCII οι οποίες τερματίζονται με <CLRF> και
- ο διακομιστής ταχυδρομείου από τη μεριά που διατηρείται το γραμματοκιβώτιο αποκρίνεται αντίστοιχα.
- Η ανταλλαγή ξεκινά με τον πελάτη να πιστοποιεί την ταυτότητα του και να προσδιορίζει το γραμματοκιβώτιο που θέλει να προσπελάσει.

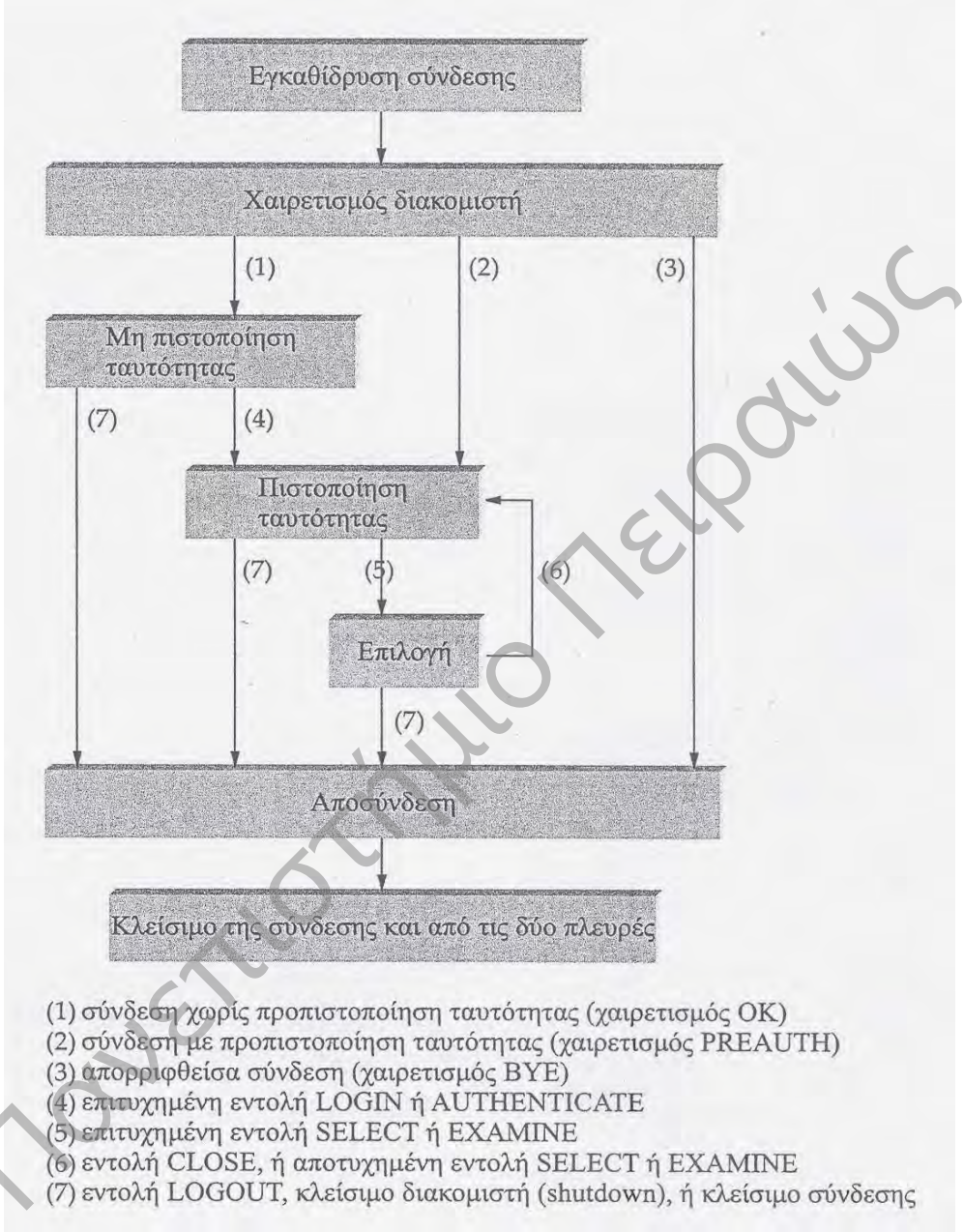
Αυτή η λειτουργία παριστάνεται στο παρακάτω διάγραμμα μεταβολής κατάστασης όπου οι εντολές:

- LOGIN (ΣΥΝΔΕΣΗ),
- AUTHENTICATE (ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ),
- SELECT (ΕΠΙΛΟΓΗ),
- EXAMINE (ΕΞΕΤΑΣΗ),
- CLOSE (ΚΛΕΙΣΙΜΟ) και
- LOGOUT (ΑΠΟΣΥΝΔΕΣΗ) αποτελούν παραδείγματα εντολών που μπορεί να δώσει ο πελάτης, ενώ η απάντηση OK είναι μία από τις δυνατές απαντήσεις του διακομιστή.

Άλλες συνηθισμένες εντολές είναι:

- FETCH (ΠΡΟΣΚΟΜΙΣΗ),
- STORE (ΑΠΟΘΗΚΕΥΣΗ),
- DELETE (ΔΙΑΓΡΑΦΗ) και
- EXPUNGE (ΠΛΗΡΗΣ ΔΙΑΓΡΑΦΗ) με προφανείς σημασίες.
- Πρόσθετες απαντήσεις διακομιστή είναι:
- NO (ΟΧΙ, ο πελάτης δεν έχει άδεια να εκτελέσει τη συγκεκριμένη ενέργεια) και
- BAD (ΜΗ ΑΠΟΔΕΚΤΗ , η εντολή είναι κακοδιατυπωμένη).

(Wikipedia, Internet Message Access Protocol) (Comer, 2001 4η Αμερικάνικη Έκδοση) (Behrouz A. Forouzan, 2005) (Kurose&Ross, 2008) (Peterson&Davie, 2008)



Εικόνα 26 : «Λειτουργία του IMAP» πηγή εικόνας: (Peterson&Davie, 2008)

2.5.3 Συγκριση Πρωτοκολλων POP3 με IMAP

POP3	IMAP4
✓ Είναι ένα απλό πρωτόκολλο, καθιστώντας ευκολότερη την εφαρμογή.	✓ Το **IMAP** έχει περισσότερα χαρακτηριστικά από το **POP3** που το κάνουν πιο σύνθετο.
✓ Μετακινεί τα μηνύματα από το διακομιστή e-mail στο τοπικό υπολογιστή, αλλά υπάρχει και η επιλογή να τα αφήσει και στον server. .	✓ Το IMAP διατηρεί το μήνυμα στο διακομιστή e-mail και κατεβάζει απλά ένα τοπικό αντίγραφο.
✓ Το POP αντιμετωπίζει το γραμματοκιβώτιο ως ένα ενιαίο χώρο αποθήκευσης χωρίς την ύπαρξη φακέλων.	✓ Ένα πρόγραμμα-πελάτη IMAP εκτελεί περίπλοκες ερωτήσεις, ζητώντας από τον server επικεφαλίδες μηνυμάτων ή το σώμα συγκεκριμένων μηνυμάτων, ή να αναζητήσει μηνύματα που πληρούν ορισμένα κριτήρια. Τα μηνύματα μπορούν να σημανθούν με διάφορες σημαίες κατάστασης (π.χ. "διαγραμμένα" ή "απεσταλμένα") και μπορούν να μείνουν στον server μέχρι να αφαιρεθούν εντελώς από το χρήστη. Εν ολίγης : Το IMAP έχει σχεδιαστεί για να χειρίζεται τα απομακρυσμένα γραμματοκιβώτια σαν να ήταν τοπικά.
✓ Το πρωτόκολλο POP απαιτεί ο τρέχων χρήστης που είναι συνδεδεμένος εκείνη τη στιγμή να είναι ο **μόνος** πελάτης συνδέεται με το γραμματοκιβώτιο	✓ **<u>Πολλαπλοί clients στο ίδιο mailbox</u>** Το IMAP επιτρέπει ρητά την ταυτόχρονη πρόσβαση πολλών χρηστών και παρέχει μηχανισμούς για να αποθηκεύονται τυχών τροποποιήσεις που γίνονται στο γραμματοκιβώτιο.
✓ Όταν POP ανακτά ένα μήνυμα, λαμβάνει όλα τα τμήματά του,	✓ Το ενώ IMAP4 επιτρέπει στους χρήστες να ανακτήσουν κάποια από τα επιμέρους τμήματα MIME ξεχωριστά – π.χ., την ανάκτηση του απλού κειμένου χωρίς την ανάκτηση συνημμένων αρχείων.
✓ Το POP3 δεν υποστηρίζει κανενός είδους σήμανση μηνυμάτων.	✓ Το IMAP υποστηρίζει τη σήμανση στο διακομιστή για την κατάσταση μηνύματος: για παράδειγμα, αν ή όχι το μήνυμα έχει διαβαστεί, αν έχει απαντηθεί, ή έχει διαγραφεί. ✓
Λειτουργίες σύνδεσης και αποσύνδεσης	
✓ Με τη χρήση του POP, οι clients	✓ Με τη χρήση του IMAP4, οι clients

συνήθως συνδέονται με το διακομιστή e-mail για λίγο, μόνο για όσο χρόνο χρειάζεται για να κάνουν λήψη νέων μηνυμάτων.	παραμένουν συνδεδεμένοι για όσο διάστημα ο χρήστης είναι ενεργός.

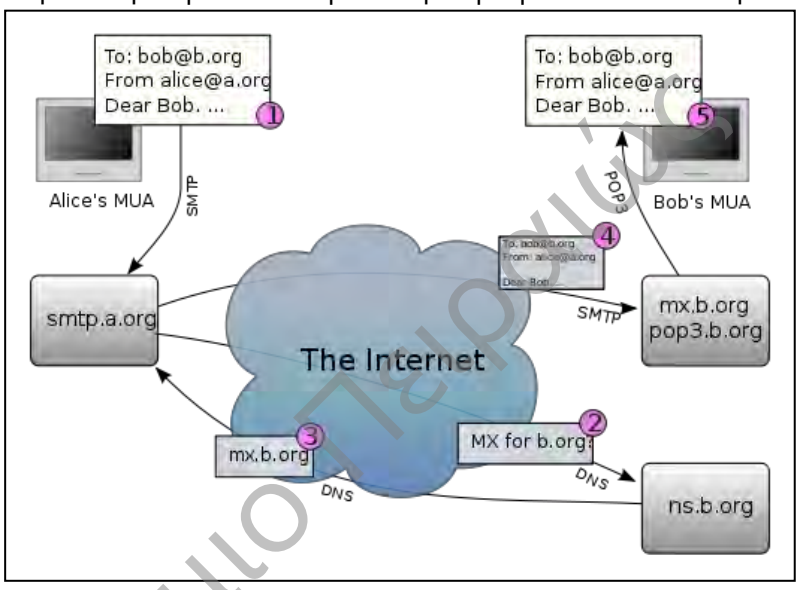
Πίνακας 4: «Πλεονεκτήματα και Μειονεκτήματα POP3 και IMAP4»

(Wikipedia, Post Office Protocol) (Wikipedia, Internet Message Access Protocol)

2.6 Επισκοπηση Λειτουργιας του Ηλεκτρονικου Ταχυδρομειου

Αφού αναλύσαμε όλους τους όρους που περικλείουν την διαδικασία του Ηλεκτρονικού Ταχυδρομείου σε αυτό το σημείο θα αναφερθούν όλα τα βήματα της σύνθεσης-αποστολής-και παράδοσης ενός mail σε μία τυπική επικοινωνία μεταξύ δύο χρηστών : της Alice και του Bob.

1. Η Alice θέλοντας να στείλει ένα email χρησιμοποιεί το δικό της mail user agent (MUA) για να συνθέσει το μήνυμα, ύστερα εισάγει την διεύθυνση του παραλήπτη και πατάει το κουμπί **“send”**.
2. Ο **MUA** της Alice μετατρέπει το μήνυμα σε μορφή που επιβάλλεται από το πρωτόκολλο **SMTP** για να στείλει το μήνυμα στον **mail submission agent (MSA)**, σε αυτή την περίπτωση το **smtp.a .org** εκτελείται από το ISP της Alice.
3. Ο MSA εξετάζει τη διεύθυνση προορισμού που προβλέπεται από το πρωτόκολλο SMTP (όχι από την κεφαλίδα του μηνύματος), στην περίπτωση αυτή είναι το **bob@b.org**.
4. Ο MSA αντιστοιχίζει ένα domain name με την ακριβή διεύθυνση του όνομα τομέα του διακομιστή ανταλλαγής αλληλογραφίας από το Domain Name System (DNS).
5. Ο DNS server απαντά για τον τομέα **b.org, ns.b.org**, με κάθε MX εγγραφές που έχει στην λίστα του που αφορούν τους διακομιστές ανταλλαγής μηνυμάτων (mail exchange servers) για αυτόν τον τομέα, σε αυτή την περίπτωση ο **mx.b.org**, ο message transfer agent (MTA) εκτελείται από τον ISP του Bob .
6. Ο **smtp.a.org** στέλνει ένα μήνυμα στον **mx.b.org** χρησιμοποιώντας το πρωτόκολλο **SMTP.**
7. Αυτός ο διακομιστής μπορεί να χρειαστεί να διαβιβάσει το μήνυμα σε ενδιάμεσους MTA πριν το μήνυμα φτάσει στον τελικό **message delivery agent (MDA).**
8. Ο MDA παραδίδει το μήνυμα στο **mailbox** του Bob.
9. Ο Bob πατάει το κουμπί **"get Mail"** στο MUA του, που παίρνει το μήνυμα χρησιμοποιώντας το πρωτόκολλα **Post Office Protocol (POP3)** ή **Internet Message Access Protocol (IMAP4).** (Wikipedia, Email)



Εικόνα 27: «Λειτουργία Ηλεκτρονικού Ταχυδρομείου» πηγή: (Wikipedia, Email)

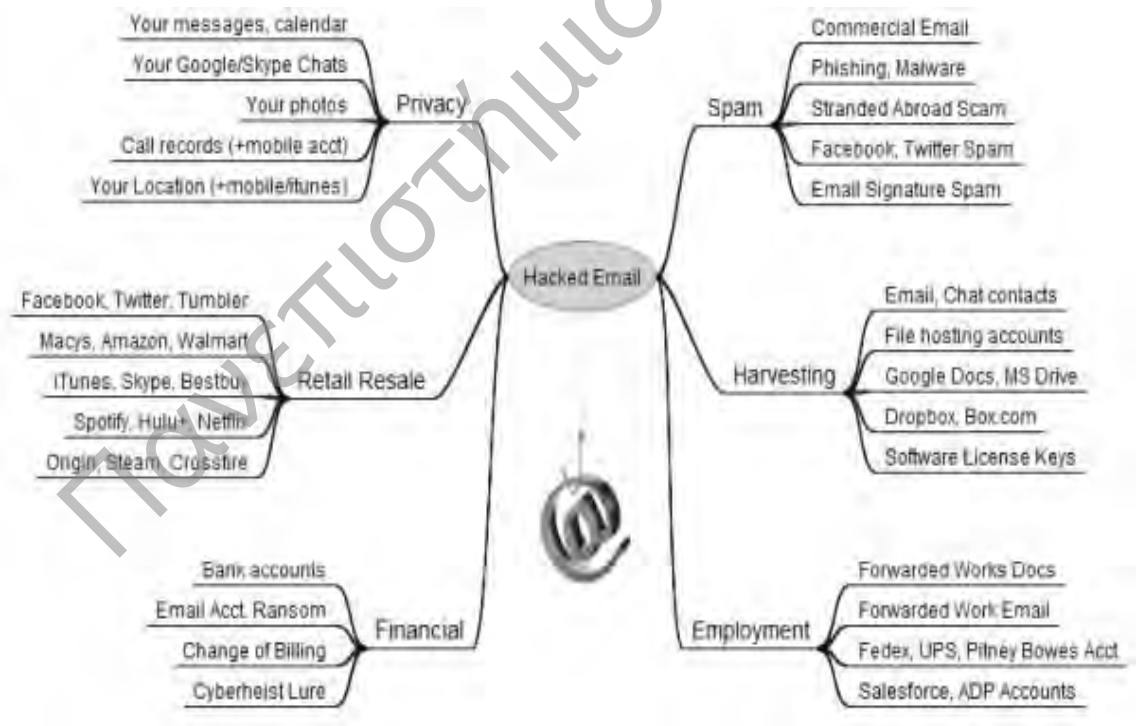
3 ΑΠΕΙΛΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

3.1 EMAIL HACKING

Το Email είναι αδιαμφισβήτητα ένα πανίσχυρο εργαλείο στο χώρο των υπολογιστών και του Διαδικτύου. Όταν πλέον ενσωματώνει δυναμικές τεχνολογίες όπως ActiveX και JavaScript καθώς και με τις δικές του ισχυρές δυνατότητες, όπως τα συνημμένα αρχεία, ένα απλό μήνυμα email μπορεί να γίνει μία από τις πιο αποτελεσματικότερες μορφές επίθεσης. Οι ευπάθειες που έχουν εντοπιστεί μέχρι σήμερα, έχουν άμεση σχέση τα προϊόντα της Microsoft που λόγω της δημοτικότητας τους τα κάνει ταυτόχρονα και ελκυστικούς στόχους.

Ένα από τα πιο ισχυρά και ταυτόχρονα βολικά από πλευράς επίθεσης, χαρακτηριστικά του email είναι η δυνατότητα επισύναψης αρχείου στα μηνύματα διότι παρέχει την ευκολία με την οποία ένα εκτελέσιμο κακόβουλο αρχείο να μπορεί να παραδοθεί κατευθείαν στο σκληρό δίσκο των τελικών χρηστών και να εκτελεστεί.

Email hacking είναι παράνομη πρόσβαση σε λογαριασμό email ή αλληλογραφία. Υπάρχουν διάφοροι τρόποι με τους οποίους επίδοξοι χάκερ μπορούν να αποκτήσουν παράνομα πρόσβαση σε έναν λογαριασμό e-mail και η πλειοψηφία από αυτούς βασίζονται στην συμπεριφορά των χρηστών. Η παράνομη πρόσβαση σε έναν email λογαριασμό χωρίζεται κατά βάση σε 3 κατηγορίες επιθέσεων: **Spam, Virus** και **Phishing** όπου αυτές οι επιθέσεις εκμεταλλεύονται τις αδυναμίες/κενά ασφάλειας του μηχανισμού Ηλεκτρονικού Ταχυδρομείου. (Wikipedia, Email hacking) (MCCLURE, 2009)



Εικόνα 28: «Κατηγοριοποίηση Απειλών» πηγή εικόνας: https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

3.2 SPAMMING

Με τον όρο spam εννοούμε την "ανεπιθύμητη ηλεκτρονική αλληλογραφία". Πρόκειται δηλαδή για οποιοδήποτε μήνυμα ανεξάρτητα από το περιεχόμενό του, το οποίο αποστέλλεται σε πολλούς παραλήπτες χωρίς αυτοί να το έχουν ζητήσει. Άλλοι όροι που χρησιμοποιούνται στο Internet για το αντί του spam είναι η "Αυτόκλητη Εμπορική Ηλεκτρονική Αλληλογραφία" (Unsolicited Commercial E-mail - UCE) και η "Αυτόκλητη Μαζική Ηλεκτρονική Αλληλογραφία" (Unsolicited Bulk E-mail - UBE).

Οι υπεύθυνοι για την αποστολή των spams ονομάζονται spammers και συνήθως αγοράζουν, αποκτούν παρανόμως ή συλλέγουν διευθύνσεις e-mails από chatrooms, ιστοσελίδες, καταλόγους πελατών, newsgroups, και οι ιοί που παραβιάζουν κάποιο λογαριασμό ηλεκτρονικού ταχυδρομείου και συλλέγουν τις διευθύνσεις των χρηστών, οι οποίες στη συνέχεια πωλούνται σε άλλους spammers. Ακόμα και με ένα απλό search σε μία σελίδα που φιλοξενεί αρχεία torrents μπορεί ο οποιοσδήποτε να κατεβάσει ένα αρχείο στο υπολογιστή του με εκατομμύρια έγκυρες διευθύνσεις που έχουν συλλεχθεί από προηγούμενες ενέργειες spammers.

Εικόνα 29: «Δείγματα Spam διευθύνσεων» πηγή εικόνας: http://thepiratebay.se/

Χρησιμοποιούν ποικίλες πρακτικές για να αναζητήσουν τη διεύθυνση ηλεκτρονικού ταχυδρομείου του στόχου-θύμα.

Έχοντας αποκτήσει τη διεύθυνση στη συνέχεια, στέλνουν τα μηνύματα τους χωρίς την έγκριση του παραλήπτη σε αντίθεση με τις τεχνικές e-mail marketing όπου ο πελάτης επιλέγει την λήψη διαφημιστικών/ενημερωτικών μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου. Η «εκούσια» αυτή αλληλογραφία είναι ένα υποσύνολο της UBE το UCE (εκούσιο εμπορικό ηλεκτρονικό ταχυδρομείο). Το αντίθετο του «spam», e-mail που κάποιος θέλει, ονομάζεται "ham".

Με τον όρο "αυτόκλητη" εννοείται η αλληλογραφία η οποία δεν έχει προηγηθεί η συγκατάβαση του παραλήπτη για την αποστολή της, σε αντίθεση για παράδειγμα με τα ηλεκτρονικά ενημερωτικά μηνήματα (e-newsletters).

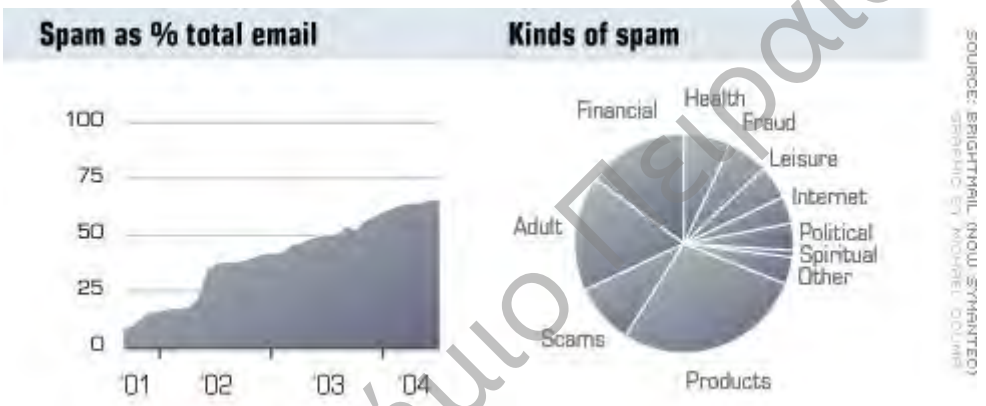
Τα κυριότερα χαρακτηριστικά του Spam μπορούν να συνοψιστούν στα ακόλουθα σημεία:

- **Απρόκλητο**: Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.
- **Εμπορικό**: Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.

- **Μαζικό**: Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σε ένα μεγάλο πλήθος παραληπτών. (Ανεπιθύμητη Αλληλογραφία)

Το spam ξεκινά να λαμβάνει "τρομακτικές" διαστάσεις από το 2002 και έπειτα όπου μέχρι τότε αποτελούσε μόνο το 8% της συνολικής ηλεκτρονικής αλληλογραφίας και το 2009 έφτασε να καλύπτει το 90% των συνολικών μηνυμάτων.

Η αύξηση αυτή των spam αντιστοιχεί με τη μετατροπή του Internet από μια μη εμπορική ακαδημαϊκή και ερευνητική κοινότητα σε ένα παγκόσμιο εμπορικό δίκτυο. Το ακόλουθο γράφημα δείχνει την δραματική αύξηση των spams και την τυπική θεματολογία τους. (Anti-Spamming) (Quinn, 2012) (Wikipedia, Email spam)



Εικόνα 30: «Εξέλιξη και θεματολογία των spams» πηγή εικόνας: http://wiki.apache.org/spamassassin/Spam

3.2.1 Είδη Spam

Το Spam χωρίζεται σε 2 μεγάλες κατηγορίες και διαφοροποιείται με βάση την πηγή που προέρχεται, αυτές είναι:

- ***Unsolicited bulk email* (UBE):** ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, που αποστέλλονται σε μεγάλες ποσότητες.
- ***Unsolicited commercial email* (UCE):** αυτός ο ορισμός είναι πιο αυστηρός και χρησιμοποιείται από τις ρυθμιστικές αρχές των οποίων η αποστολή είναι να ρυθμίζουν το εμπόριο, όπως η U.S. Federal Trade Commission (αμερικανική Ομοσπονδιακή Επιτροπή Εμπορίου).

Ο λόγος για τον οποίο η spam αλληλογραφία είναι τόσο αποτελεσματική είναι το κόστος αρκετά αρκετά χαμηλό σε σχέση με άλλες μορφές διαφήμισης. Για την ακρίβεια είναι 100 φορές φθηνότερο από το κόστος της παραδοσιακής αλληλογραφίας. Αξιοσημείωτο είναι ότι το κόστος είναι τόσο χαμηλό που η εκάστοτε εταιρεία αποφέρει κέρδος στην περίπτωση που μόνο ένας στους 100.000 παραλήπτες αγοράσει το προϊόν ή υπηρεσία. (Quinn, 2012)

Τα είδη spam που διακινούνται καθημερινά μέσω του ηλεκτρονικού ταχυδρομείου χωρίζονται στις εξής κατηγορίες:

1. **Adult content spam-** Επιθέσεις με Email για Ενήλικες. Αυτή η κατηγορία των spam συμπεριλαμβάνει περιεχόμενο ή αναφορές σε προϊόντα ή υπηρεσίες που απευθύνονται σε άτομα άνω των 18, συχνά προσβλητικά ή ακατάλληλα. Παραδείγματα: πορνογραφικές ιστοσελίδες, προσωπικές αγγελίες, συμβουλές για σχέσεις και υπηρεσίες γνωριμιών. Κατά τη διάρκεια των τελευταίων ετών η επικράτηση αυτής της κατηγορίας spam έχει υποχωρήσει, και έχει αντικατασταθεί από άλλες αποστολές. Πριν από τρία χρόνια ξεκίνησε η προσφορά/διαφήμιση πρόσβασης σε τόπους με πορνογραφικό υλικό και σήμερα αυτό το είδος των spam έχει μειωθεί σημαντικά.

Εικόνα 31: «Adult Spam»

2. **Health and Medicine -** Επιθέσεις με Email με θέματα Υγείας: Μηνύματα που προσφέρουν ή διαφημίζουν προϊόντα και υπηρεσίες σχετικά με την υγεία. Περιλαμβάνουν διαφημίσεις για την απώλεια βάρους, την περιποίηση του δέρματος, τη βελτίωση της στάσης του σώματος, θεραπείες για την τριχόπτωση, συμπληρώματα διατροφής, φάρμακα, θεραπείες, συνταγές με βότανα και μη-παραδοσιακά φάρμακα κ.λπ., τα οποία μπορούν όλα να αγοραστούν on-line.

Εικόνα 32: «Health Spam»

3. **Personal finance-** Επιθέσεις με Email με Οικονομικά Στοιχεία με αναφορές ή προσφορές σχετικά με χρήματα, μετοχές ή άλλες οικονομικές 'ευκαιρίες'. Παραδείγματα: επενδύσεις, αναφορές πιστώσεων, ακίνητα, δάνεια.
4. **Fraud**-Επιθέσεις με απατηλά Email τα οποία φαίνεται να προέρχονται από μια γνωστή εταιρεία, χωρίς να είναι. Επίσης γνωστά και με τους όρους "brand spoofing" ή "phishing," τα μηνύματα αυτά χρησιμοποιούνται συχνά για να ξεγελάσουν τους χρήστες να αποκαλύψουν προσωπικές πληροφορίες όπως διεύθυνση email, οικονομικά δεδομένα και κωδικούς. Παραδείγματα: πληροφορίες λογαριασμών, επαλήθευση πιστωτικών καρτών, ενημερώσεις λογαριασμών
5. **Leisure**-Επιθέσεις με Email με θέματα Αναψυχής που προσφέρουν ή διαφημίζουν βραβεία, δώρα ή εκπτώσεις σε δραστηριότητες αναψυχής. Παραδείγματα: προσφορές διακοπών, online καζίνο, παιχνίδια
6. **Political**-Πολιτικά Μηνύματα που διαφημίζουν την πολιτική καμπάνια ενός υποψηφίου, προσφορές για χρηματική δωρεά σε ένα πολιτικό κόμμα ή για ένα πολιτικό σκοπό, προσφορές προϊόντων σχετικών με έναν πολιτικό ή μια καμπάνια κλπ.Παραδείγματα: πολιτικό κόμμα, εκλογές, δωρεές**.**
7. **Scams**-Επιθέσεις με Πλαστά Email τα οποία αναγνωρίζονται ως ψεύτικα, διεθνώς παραπλανητικά, ή με εγνωσμένο αποτέλεσμα την απάτη από την πλευρά του αποστολέα.Παραδείγματα: Νιγηριανές επενδύσεις, πυραμίδες, αλυσιδωτές επιστολές (chain letters)
8. **Spiritual**-Επιθέσεις με Email Πνευματικού περιεχομένου με πληροφορίες σχετικές με θρησκευτικό ή πνευματικό προσηλυτισμό ή/και υπηρεσίες. Παραδείγματα: μέντιουμ, αστρολογία, οργανωμένη θρησκεία, ψυχικά φαινόμενα
9. **Education – Εκπαίδευσης:** σε αυτήν τη κατηγορία περιλαμβάνονται emails που διαφημίζουν/ προσφέρουν σεμινάρια, μαθήματα, πιστοποιήσεις ή ακόμα και πτυχία online.
10. **Προϊόντα υπολογιστών και Internet** σε αυτήν τη κατηγορία προσφέρονται ηλεκτρονικές συσκευές, προγράμματα λογισμικού ή ακόμα και υπηρεσίες hosting, εγγραφές domain, βελτιώσεις websites σε χαμηλές τιμές. (SecureList) (Techblog.gr, 2007) (Symantec) (Anti-Spamming)

3.2.2 Τεχνικες Spam

I. Appending

Email appending, επίσης γνωστό ως e-appending, είναι μια πρακτική μάρκετινγκ στην οποία οι spammers έχοντας στην διάθεση τους στοιχεία πελατών όπως: όνομα, επώνυμο και ταχυδρομική διεύθυνση συγκρίνουν αυτά τα στοιχεία με τη βάση δεδομένων μίας εταιρείας με σκοπό να αποκτήσουν και τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των πελατών. Ο σκοπός είναι να αυξηθεί λίστα email κάποιου συνδρομητή με την πρόθεση της αποστολής πληροφοριών των πελατών μέσω του ηλεκτρονικού ταχυδρομείου αντί μέσω του παραδοσιακού ταχυδρομείου .

Εικόνα 33: «Email appending» πηγή: http://www.mylist.fr/email-appending.html

Μια διαδικασία email appending περιλαμβάνει μια βάση δεδομένων μίας εμπορικής επιχείρησης που αποτελείται από επαφές με το όνομα , τη διεύθυνση και το όνομα της εταιρείας (για επιχειρηματικές επαφές) . Εάν η εταιρεία θέλει να επεκταθεί σε επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, μπορούν να συμπεριλάβουν έναν φορέα παροχής υπηρεσιών που έχει μια βάση δεδομένων με έγκυρες διευθύνσεις, προκειμένου να συγχωνευθούν τα στοιχεία και να προσαρτήσει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των καταναλωτών ή ακόμα και επιχειρήσεων με το υπάρχον αρχείο τους . Με αυτόν τον τρόπο μπορούν να έχουν μια ενημερωμένη βάση δεδομένων με την τρέχουσα διεύθυνση ηλεκτρονικού ταχυδρομείου των ατόμων που περιλαμβάνονται στον κατάλογο . Η επιτυχία αυτής της διαδικασίας εξαρτάται από την ποιότητα και των δύο βάσεων δεδομένων που συγχωνεύονται. (Wikipedia, Email appending)

(Πηγή εικόνας: http://www.towerdata.com/email-append/email-appending/)

II. **Image spam**

Το spam εικόνας ή το spam με βάση την εικόνα, είναι μια μέθοδος παραπλάνησης με σκοπό την αποφυγή των spam φίλτρων στην οποία το κείμενο του μηνύματος αποθηκεύεται ως εικόνα τύπου .gif ή .jpeg και εμφανίζεται στο ηλεκτρονικό ταχυδρομείο. Με αυτό τον τρόπο αποτρέπει τα text φίλτρα spam από την ανίχνευση και τελικά το μπλοκάρισμα των μηνυμάτων. Φαινόμενο που εμφανίστηκε στα μέσα της δεκαετίας του 2000 για διαφημιστικούς σκοπούς.

Συχνά, τα spam εικόνας περιέχουν κείμενο computer-generated που δύσκολο να σαρωθεί. Ωστόσο, η νέα τεχνολογία σε ορισμένα προγράμματα έχει καταφέρει να διαβάσει εικόνες προσπαθώντας να εντοπίσει κάποιο κείμενο σε αυτές. Δεν έχουν αποδειχτεί πολύ ακριβή και αποτελεσματικά καθώς μερικές φορές μπλοκάρουν και «αθώα» μηνύματα.

Νεώτερες τεχνικές έχουν χρησιμοποιηθεί για να αποφύγουν τον εντοπισμό από τα εργαλεία αναγνώρισης χαρακτήρων (OCR) όπως είναι η κινούμενη εικόνα τύπου .gif που δεν περιέχει σαφή κείμενο στο αρχικό του πλαίσιου, ή η παραμόρφωση των γραμμάτων στην εικόνα να φαίνονται σαν σχήματα (όπως με το εργαλείο CAPTCHA).

Εικόνα 34: «Spam εικόνας» πηγή εικόνας: (Wikipedia, Email spam)

III. **Blank spam**

Τα Blank spam είναι αυτά που στο εσωτερικό τους λείπει η διαφήμιση δηλαδή είναι κενά. Συχνά το σώμα του μηνύματος λείπει εντελώς , καθώς η γραμμή θέματος . Παρόλα αυτά , συγκαταλέγονται και αυτά στην κατηγορία των spam λόγω της φύσης του ως ανεπιθύμητα e-mail. Τα Blank το spam μπορεί να προέρχεται είτε εκ προθέσεως είτε χωρίς πρόθεση:

1. Blank spam μπορεί να έχουν αποσταλεί από μια μαζική επίθεση λεγόμενη ως **directory harvest attack** όπου είναι μια μορφή επίθεσης που αποσκοπεί στη συλλογή έγκυρων διευθύνσεων. Δεδομένου ότι ο στόχος σε μια τέτοια επίθεση είναι να χρησιμοποιήσουν τα μηνύματα αποτυχίας παράδοσης για να διαχωριστούν οι έγκυρες διευθύνσεις, οι spammers παραλείπουν τα περισσότερα στοιχεία της κεφαλίδας και ολόκληρο το σώμα του μηνύματος , και στο τέλος πάλι καταφέρνουν να ολοκληρώσουν το στόχο τους. Η εικόνα 35 δείχνει ένα παράδειγμα Directory Harvest Attack συναλλαγής.

```
220 esa02.cisco.com ESMTP
HELO external-sender.com
250 esa02.cisco.com
MAIL FROM: <sender@external-sender.com>
250 sender <sender@external-sender.com> ok
RCPT TO: chris@cisco.com
550 #5.1.0 Address rejected.
RCPT TO: cporter@cisco.com
550 #5.1.0 Address rejected.
RCPT TO: chrisporter@cisco.com
550 #5.1.0 Address rejected.
RCPT TO: chriport@cisco.com
250 recipient <chriport@cisco.com> ok
RCPT TO: chrisp@cisco.com
550 #5.1.0 Address rejected.
```

Εικόνα 35: « Παράδειγμα Directory Harvest Attack»πηγή εικόνας: (Porter, 2012)

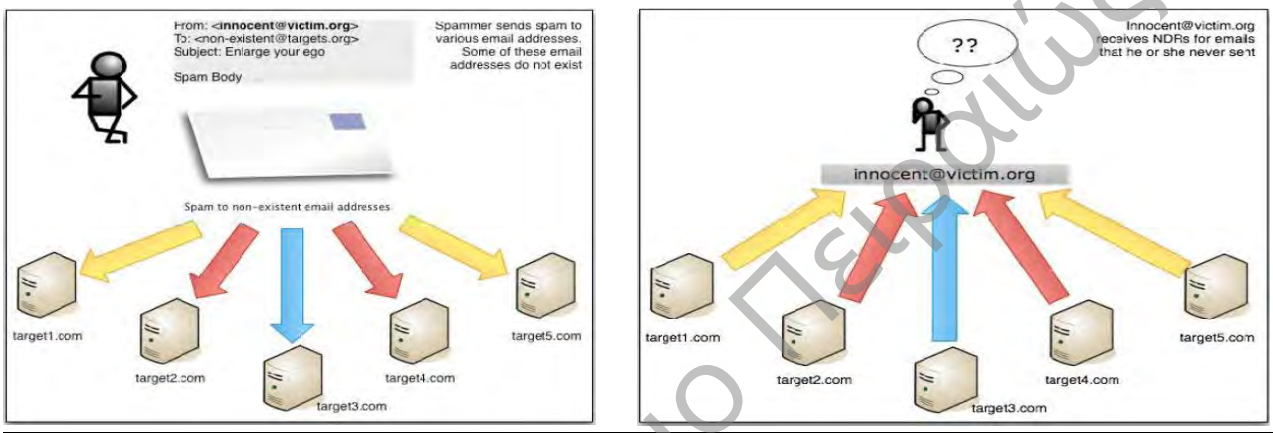
2. Blank spam μπορεί επίσης να προκύψει σε περίπτωση που ο spammer ξεχάσει ή παραλείπει να προσθέσει το μήνυμα διαφήμισης , κατά τη δημιουργία του spam.
3. Συχνά κενές κεφαλίδες εμφανίζονται σε spam που προέρχονται λόγω χαμηλής ποιότητας λογισμικού δημιουργίας spam ή κακής αναμετάδοσης servers.
4. Μερικά spam μπορεί να φαίνονται να είναι κενά αλλά στην πραγματικότητα να μην είναι όπως στη περίπτωση του worm **VBS.Davinia.B** το οποίο διαδίδεται μέσω μηνυμάτων που έχουν κενό θέμα ενώ στην πραγματικότητα χρησιμοποιεί κώδικα HTML για να κατεβάσει άλλα αρχεία.

IV. Backscatter spam

Το Backscatter spam γνωστό και ως **outscatter**, **misdirected bounces**, **blowback** ή **collateral spam,** είναι μια άλλη μορφή spam email, ιού ή worm, όπου εμφανίζονται σαν ασφαλές μήνυμα. Μπορεί να είναι ένα μήνυμα αποτυχίας παράδοσης που παράγεται από ένα

junk email υποδεικνύοντας ότι προέρχεται από έναν «νόμιμο και αθώο» αποστολέα. Worms και άλλου είδους κακόβουλο λογισμικό στέλνουν μηνύματα από μια διεύθυνση χωρίς τη γνώση του ιδιοκτήτη που απρόσμενα μπορεί να οδηγήσει σε αποτυχία παράδοσης.

Οι πιθανοί spammers μπορούν να υποδυθούν κάποιο αθώο αποστολέα και να στείλουν κάποιο spam μήνυμα αν αυτό αποτύχει θα γυρίσει σαν μήνυμα αποτυχίας στη διεύθυνση του αποστολέα και όχι στο spammer, αναπαράγοντας επιπλέον και το αρχικό μήνυμα αποφεύγοντας ταυτόχρονα και τα φίλτρα junk και spam μηνυμάτων με την «μεταμφίεση» ενός μηνύματος αποτυχίας παράδοσης. (Wikipedia, Email hacking) (Protogenist)



Εικόνα 36: «Παράδειγμα Backscatter spam» πηγή: (Protogenist)

3.3 PHISHING

Μια από τις πιο συνήθεις πρακτικές εξαπάτησης των χρηστών του internet είναι το λεγόμενο phishing. Η λέξη παραπέμπει στο αγγλικό fishing, ψάρεμα δηλαδή και ουσιαστικά αντανακλά αυτό ακριβώς που κάνουν ρίχνουν «δόλωμα» για να πιάσουν τους ανυποψίαστους.

Το Phishing είναι μία παράνομη πράξη στην οποία προσπαθούν να αποκτήσουν ευαίσθητες πληροφορίες όπως ονόματα χρηστών , κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών (και φυσικά εμμέσως χρήματα) μεταμφιεσμένο με τη μορφή ενός αξιόπιστου πρόσωπου στο πλαίσιο μιας ηλεκτρονικής επικοινωνίας. Ισχυριζόμενοι ότι είναι ένα δημοφιλές κοινωνικό web site, ιστοσελίδες δημοπρασιών , ή τράπεζες με απευθείας σύνδεση επεξεργασίας πληρωμής ή IT διαχειριστές με αυτό τον τρόπο οι επιτήδειοι δελεάζουν ανυποψίαστους πολίτες.

Η πιο διαδεδομένη αιτιολογία με την οποία παρουσιάζεται ένα μήνυμα phishing είναι η ανάγκη επιβεβαίωσης των δεδομένων για την ενημέρωση του συστήματος. Πολλές φορές επίσης οι σελίδες αυτές παραπέμπουν σε site όπου μεταφορτώνεται εν αγνοία των χρηστών κακόβουλο λογισμικό όπως ιοί, malware κλπ.

. Ο όρος phishing συγκαταλέγεται στην κατηγορία **email spoofing** ή instant messaging και συχνά οδηγεί τους χρήστες να εισάγουν τα στοιχεία σε μια πλαστή ιστοσελίδα του οποίου η εμφάνιση και αίσθηση είναι σχεδόν πανομοιότυπη με τη νόμιμη. Το phishing είναι ένα παράδειγμα τεχνικών social engineering που χρησιμοποιούνται για να εξαπατήσουν τους χρήστες και να εκμεταλλεύονται την κακή χρηστικότητα των σημερινών τεχνολογιών ηλεκτρονικής ασφαλείας. (Wikipedia, Email hacking) (Wikipedia, Phishing)

3.3.1 ΤΕΧΝΙΚΕΣ PHISHING

I. Clone phishing

Μία από τις πιο γνωστές τεχνικές phishing μέσω ηλεκτρονικής αλληλογραφίας είναι: το **Clone phishing** όπου είναι ένας τύπος επίθεσης phishing στην οποία ένα φαινομενικά νόμιμο email που περιέχει ένα συνημμένο ή ένα σύνδεσμο όπου το περιεχόμενό του και η διεύθυνση του παραλήπτη χρησιμοποιήθηκαν για να δημιουργήσουν ένα αντίγραφο email. Το συνημμένο αρχείο ή το link στο e-mail αντικαθίσταται με ένα κακόβουλο λογισμικό και στη συνέχεια αποστέλλονται από μια διεύθυνση ηλεκτρονικού ταχυδρομείου πλαστογραφημένες έτσι ώστε να φαίνονται ότι προέρχονται από τον αρχικό αποστολέα. Παρουσιάζεται ως επαναποστολή του αρχικού μηνύματος ή μια ενημερωμένη έκδοση του πρωτότυπου. Οι περισσότερες μέθοδοι phishing χρησιμοποιούν κάποια μορφή τεχνικής εξαπάτησης σχεδιασμένη έτσι ώστε να δημιουργείται η αίσθηση ότι ο σύνδεσμος που περιέχεται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου (που οδηγεί σε πλαστή ιστοσελίδα) είναι ασφαλής.

II. Link manipulation

Ανορθόγραφα URLs ή η χρήση των subdomains είναι μερικά από τα τεχνάσματα που χρησιμοποιούν οι phishers. Για παράδειγμα το URL , **http://www.yourbank.example.com/** , φαίνεται σαν μία ασφαλής διεύθυνση όπου επισυνάπτεται σε ένα email, όπου θα μεταφέρει το χρήστη στη επίσημη ιστοσελίδα της Τράπεζας του όμως στην πραγματικότητα αυτό το URL οδηγεί σε μία σελίδα phishing. Ένα άλλο τέχνασμα όταν συνδέουν το κείμενο ή την ετικέτα να εμφανίζει ότι οδηγεί σε μια ασφαλή σύνδεση προτείνει αλλά στην πραγματικότητα οδηγεί σε sites με περιεχόμενο phishing, όπου σε αυτές τις περιπτώσεις προτείνεται το πέρασμα του κέρσορα του ποντικιού για λίγα δευτερόλεπτα μέχρι να εμφανιστεί το πραγματικό link.

From: Citibank Service
[mailto:security@citibank.com]
Sent: Thursday, January 29, 2004 10:22 PM
To: **********
Subject: Security Update

Dear Citibank Customer,

At Citibank, we value the trust you have placed in us by using our service to conduct your transactions. Because our relationship with you is financial in nature, the protection of your privacy is particularly important to us.

We are sending this verification notice to provide you with information about how Citibank safeguards your privacy, as well as to comply with U.S. federal privacy guidelines that apply to financial institutions such as Citibank. The full terms of Citibank's privacy policy are available on the Citibank web site, which you are welcome to review at any time.

Please verify your account information by clicking on the link below.

Verify your accounts here

Εικόνα 37: «Παράδειγμα Link manipulation» πηγή εικόνας: (MCCLURE, 2009)

III. IDN spoofing

Μία άλλη ευπάθεια που έχει εντοπιστεί με τα URLs είναι στο χειρισμό των Διεθνών Ονομάτων Τομέα (Internationalized domain names- IDN) σε προγράμματα περιήγησης Ιστού, που υπάρχει πιθανότητα να επιτρέψει σε οπτικά πανομοιότυπες διευθύνσεις ιστοσελίδων να οδηγήσουν σε διαφορετικές, ενδεχομένως κακόβουλες, ιστοσελίδες, π.χ το domain name citibank.com μπορεί αντί να έχει γραφτεί με λατινικό **C** να αντικατασταθεί με **Cyrillic C.**

Παρά τον εντοπισμό του προβλήματος, γνωστό και ως **IDN spoofing**, **homograph attack** ή **script spoofing**, οι phishers έχουν επωφεληθεί από αυτή τη τεχνική, χρησιμοποιώντας URL ανακατεύθυνσης ανοικτού κώδικα στις ιστοσελίδες των αξιόπιστων οργανισμών για να συγκαλύψουν κακόβουλα URLs κάτω από την «ομπρέλα» ενός αξιόπιστου ονόματος τομέα. Ακόμη και **τα ψηφιακά πιστοποιητικά** δεν έχουν καταφέρει να λύσουν αυτό το πρόβλημα, διότι είναι πολύ πιθανό για ένας phisher να αγοράσει ένα έγκυρο πιστοποιητικό και στη συνέχεια να αλλάξει το περιεχόμενο για να εξαπατήσει δυνητικούς χρήστες ότι πρόκειται για μια γνήσια ιστοσελίδα.

Εικόνα 38: Ένα παράδειγμα phishing e-mail προορισμένο για τους πελάτες της Wells Fargo Τράπεζας πηγή εικόνας: (MCCLURE, 2009)

IV. Filter evasion

Οι Phishers έχουν τη δυνατότητα να χρησιμοποιούν εικόνες αντί για κείμενο για να μην εντοπίζεται εύκολα από τα anti-phishing φίλτρα των emails που ανιχνεύουν κείμενο. Παρόλο αυτά έχουν σχεδιαστεί anti-phishing φίλτρα που με τη χρήση OCR φίλτρων (optical character recognition) σαρώνουν την εικόνα και εντοπίζουν το κρυφό κείμενο.

Μερικά αντι-phishing φίλτρα χρησιμοποιούν ακόμα και IWR (intelligent word recognition), όπου μπορούν να ανιχνεύσουν καλλιγραφικούς ή χειρόγραφούς χαρακτήρες, ανάποδο ,κυματιστό, κάθετο, πλαγίως ή σε διαφορετικές κατευθύνσεις τοποθετημένο κείμενο, καθώς και κείμενο σε έγχρωμο φόντο. (Wikipedia, Email hacking) (Wikipedia, Phishing)

3.4 VIRUS

Ο Ιός (Virus) είναι ένα πρόγραμμα υπολογιστή, συνήθως μικρό σε χωρητικότητα, αλλά πολύ αποτελεσματικό σε δράση, που έχει την ικανότητα να μεταδίδεται μεταξύ υπολογιστών και δικτύων και να δημιουργηθεί αντίγραφα του εαυτού του χωρίς φυσικά να το γνωρίζει ή να το εγκρίνει ο τελικός χρήστης.

Ο σκοπός ενός ιού υπολογιστή αποσκοπεί σε επιθέσεις κατά της Εμπιστευτικότητας, της Ακεραιότητας ή/και της Διαθεσιμότητας των συστημάτων.

Για την εγκατάσταση ενός κακόβουλου λογισμικού σε έναν Η/Υ, συνήθως απαιτείται η ανθρώπινη συμμετοχή: άμεση (π.χ. ανταλλαγή αρχείων, άνοιγμα συνημμένων ή προεπισκόπηση μηνυμάτων αλληλογραφίας αμφιβόλου προέλευσης) είτε έμμεση (ανεπαρκής προστασία του υπολογιστή, μη λήψη ενημερωμένων εκδόσεων - updates του λογισμικού ασφαλείας και των προγραμμάτων). Το τμήμα του κώδικα που είναι υπεύθυνο για τις παρενέργειες του λογισμικού ονομάζεται **φορτίο** (payload). Εκτός από τις παρενέργειες, το κακόβουλο λογισμικό περιλαμβάνει επιπλέον κώδικα με σκοπό την:

- **Αναπαραγωγή του:** Εξάπλωση του στο σύστημα που προσβάλλει («μόλυνση» από πρόγραμμα σε πρόγραμμα).
- **Μετάδοση του:** Εξάπλωση του από το σύστημα που μολύνθηκε σε άλλο/άλλα συστήματα (π.χ. από Η/Υ σε Η/Υ)

Ο υπολογιστής μπορεί να μολυνθεί από έναν ιό είτε από ένα CD ή από μία συσκευή αποθήκευσης USB , που αποτελούν παλιές και όχι τόσο αποτελεσματικές τεχνικές σήμερα, ο συνηθέστερος και πιο δημοφιλής τρόπος είναι από ένα συνημμένο αρχείο σ' ένα μήνυμα ηλεκτρονικού ταχυδρομείου με το πρόγραμμα του ιού, να εκτελείται αυτόματα και μολύνει τον υπολογιστή του χρήστη που θα κάνει το λάθος να ανοίξει το ύποπτο μήνυμα. Υπάρχει και η περίπτωση της μόλυνσης από ένα αρχείο που έχει κατέβει (download) από το Internet ή ακόμα και από μια ιστοσελίδα που έχουμε επισκεφθεί.

Για να τεθεί σε λειτουργία ένας ιός, θα πρέπει να εκτελεσθεί ως πρόγραμμα στο υπολογιστή που εγκαθίσταται. Επίσης μπορεί να είναι προσκολλημένος σ' ένα άλλο κανονικό πρόγραμμα που ο χρήστης εκτελεί χωρίς να είναι σε θέση να υποψιασθεί κάτι ή μπορεί να είναι κρυμμένος σε κώδικα ο οποίος εκτελείται αυτόματα κατά την έναρξη συγκεκριμένων τύπων αρχείων.

Οι επιθέσεις αυτές εκμεταλλεύονται τις αδυναμίες του λειτουργικού συστήματος και της ασφάλειας ενός υπολογιστή που είναι συνδεδεμένος στο Internet καθώς και τις αδυναμίες των πρωτοκόλλων επικοινωνίας που χρησιμοποιούν οι υπολογιστές. Συνολικά έχουν εμφανισθεί περί τους 90.000 ιοί τα τελευταία 15 χρόνια και ενώ οι περισσότεροι έχουν εξαφανισθεί, περίπου 400 παραμένουν ενεργοί και μπορούν να μολύνουν ανά πάσα στιγμή όποιους υπολογιστές συναντήσουν στην πορεία τους.

Υπάρχουν αρκετές μορφές ιών οι οποίες αναλύονται στην συνέχεια της ενότητας:

I. **Ιός (virus).** Κακόβουλο λογισμικό το οποίο αφού μολύνει έναν Η/Υ έχει την ικανότητα να αναπαράγεται και να μολύνει άλλα προγράμματα όπως είναι για παράδειγμα ένα πρόγραμμα λογιστικών φύλλων και έτσι κάθε φορά που εκτελείται το πρόγραμμα αυτό,

εκτελείται και το πρόγραμμα του ιού και έχει επίσης τη δυνατότητα να αναπαράγεται προσκολλούμενο σ' άλλα προγράμματα ή να προκαλεί καταστροφή στον Η/Υ-ξενιστή. Η μετάδοση του σε άλλους Η/Υ μπορεί να γίνεται αυτόματα (να έχει δηλαδή τα χαρακτηριστικά ενός Σκουληκιού – Worm) ή να απαιτεί ανθρώπινη παρέμβαση (π.χ. αντιγραφή ενός αρχείου σε USB flash disk και άνοιγμα του αρχείου σε κάποιον Η/Υ).

II. **Ιοί των e-mail (e-mail viruses)**. Ένας ιός e-mail μεταφέρεται μέσω μηνυμάτων e-mail και συνήθως αναπαράγει αυτόματα τον εαυτό του χρησιμοποιώντας το βιβλίο διευθύνσεων (address book) του χρήστη που έχει προσβληθεί ώστε να μπορέσει σταλεί αυτόματα στους παραλήπτες που βρίσκονται καταχωρημένοι εκεί.

III. **Σκουλήκι (Worm).** Μικρό κομμάτι προγράμματος το οποίο, αφού μολύνει έναν Η/Υ, έχει την ικανότητα να μεταδίδεται αυτόματα. Κάνοντας χρήση της υπάρχουσας δικτυακής υποδομής (π.χ. Τοπικά Δίκτυα - Δίκτυα WAN) ή/και των υπηρεσιών του Internet (chat, e-mail, newsgroups, κ.λ.π).σαρώνει το δίκτυο με σκοπό να εντοπίσει ένα άλλο μηχάνημα που να έχει μια συγκεκριμένη τρύπα ασφαλείας (security hole). Αντιγράφει τον εαυτό του στο καινούργιο μηχάνημα χρησιμοποιώντας αυτήν την τρύπα ασφαλείας και μετά ξεκινάει την αναπαραγωγή του από εκεί κ.ο.κ.

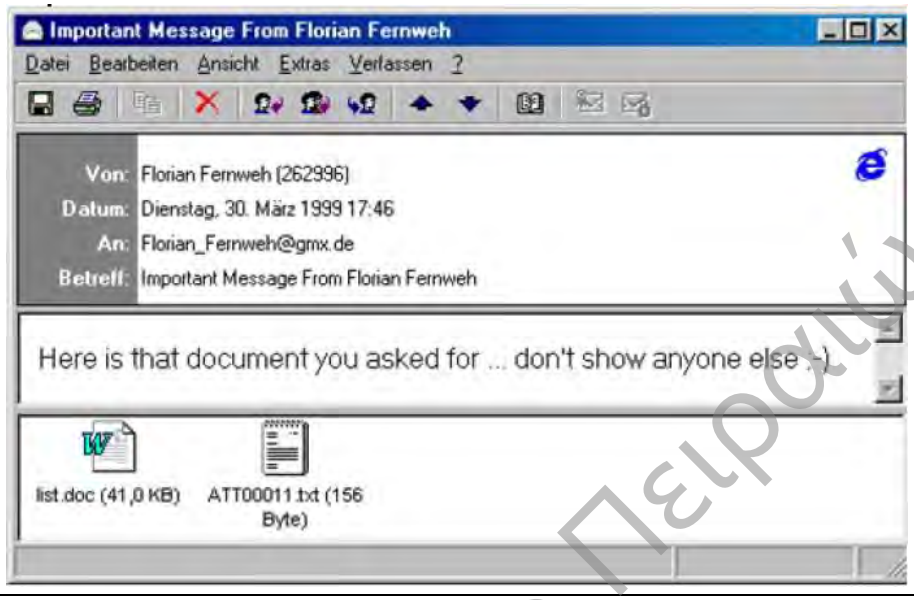
IV. **Δούρειοι Ίπποι (Trojan Horses).** Κακόβουλο λογισμικό στο οποίο είναι χαρακτηριστικό το στοιχείο της παραπλάνησης, καθώς συνήθως μεταμφιέζεται σε μια χρήσιμη εφαρμογή, όπως για παράδειγμα ένα παιχνίδι, αλλά στην πραγματικότητα κάνει κάποια ζημιά ή κάποια μη νόμιμη ενέργεια όταν εκτελεστεί. Στην πιο κλασσική των περιπτώσεων, ένα Trojan δημιουργεί μια κερκόπορτα (backdoor) στο σύστημα, στην οποία ο επιτιθέμενος θα μπορέσει αργότερα να συνδεθεί ώστε να διαχειριστεί εξ' αποστάσεως το σύστημα. Τις περισσότερες φορές τα trojans δεν έχουν μολυσματικό χαρακτήρα, δηλαδή δεν αναπαράγονται αυτόματα και για αυτό το λόγο δεν χαρακτηρίζονται επισήμως ως ιοί.

V. **Spyware – Adware.** Κακόβουλο λογισμικό με χαρακτηριστικά που εντάσσονται στις λειτουργίες ενός Δούρειου Ίππου (κυρίως ως προς τον τρόπο μόλυνσης), με σκοπό τη παρακολούθηση - υποκλοπή ευαίσθητων δεδομένων (spyware), ή την αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων (adware). Αναφέρονται ως μέλη της ίδιας κατηγορίας, καθώς συνήθως συνεργάζονται για να πετύχουν τον σκοπό τους (π.χ παρακολούθηση της αγοραστικής συμπεριφοράς κατά την περιήγηση στο Web και στη συνέχεια αποστολή-εμφάνιση διαφημιστικών μηνυμάτων).

VI. **Rootkits**. Όπως φαίνεται από την ονομασία τους, ένα rootkit είναι κακόβουλο λογισμικό το οποίο λειτουργεί σε πολύ χαμηλό επίπεδο στο λειτουργικό σύστημα, και συνήθως ενσωματώνει λειτουργίες απόκρυψης - stealth ώστε να παρακάμπτει τους μηχανισμούς πρόληψης και ανίχνευσης, όπως firewalls και antivirus. Ένα λογισμικό rootkit μπορεί να ανήκει σε οποιαδήποτε από τις ως άνω κατηγορίες, ωστόσο συνήθως ανοίγει κερκόπορτες (backdoors) που μ' αυτόν τον τρόπο οι επίδοξοι hackers θα εκτελέσουν από απόσταση ότι εντολές θέλουν για να αποσπάσει πληροφορίες.

VII. **Bots – zombies.** Κακόβουλο λογισμικό που προσβάλλει Η/Υ καθιστώντας τους μέλη ενός δικτύου Η/Υ (botnet) που ελέγχεται εξ' αποστάσεως από τρίτους, με σκοπό την πραγματοποίηση Κατανεμημένων Επιθέσεων Άρνησης Εξυπηρετητήσης (DDOS attacks), δηλαδή επιθέσεων κατά τις οποίες ένας (συνήθως μεγάλος) αριθμός μολυσμένων υπολογιστών προσπαθεί να συνδεθεί στον Η/Υ-στόχο μέσω δικτύου. Ο όρος «bot» προέρχεται από την (Τσεχικής προέλευσης) λέξη «robota» και χρησιμοποιείται για να περιγράψει κάθε είδους αυτοματοποιημένη διαδικασία (π.χ. τα γνωστά IRC bots).Ένας Η/Υ που έχει μολυνθεί από ένα bot συχνά αναφέρεται ως «zombie». Οι Η/Υ zombies μπορεί να χρησιμοποιηθούν για επιθέσεις DOS σε εξυπηρετητές Web, για την αποστολή μηνυμάτων spam, για την πραγματοποίηση

επιθέσεων παραπλάνησης (phishing) κ.λ.π. (Wikipedia, Email hacking) (Wikipedia, Computer virus) (ΠΛΗΝΕΤΝ) (Μάγκος, 2007)



Εικόνα 39: «Ο ιός Melissa (1999)» πηγή εικόνας:http://www.heise.de/artikel archiv/ct/1999/08/017_Buechse-der-Pandora

3.4.1 Αποτελεσματα ενος ιου

Οι παρενέργειες του φορτίου (payload) ενός κακόβουλου λογισμικού ποικίλλουν:

- Ενοχλητικά μηνύματα, διαφημίσεις κ.λ.π (σχετική κατηγορία: adware)
- Επιθέσεις υποκλοπής δεδομένων και πληροφοριών, ή κλήσης (dialers) με υπεραστική χρέωση (σχετική κατηγορία: trojans, spyware)
- Επιθέσεις Διακοπής, Αλλοίωσης, Εισαγωγής (σχετικές κατηγορίες: Ιοί, worms)
  - Διαγραφή ή αλλοίωση δεδομένων, εφαρμογών και αρχείων συστήματος
  - Αντιγραφή αρχείων στο τοπικό δίκτυο (μετάδοση μέσω κοινής χρήσης
  - αρχείων) ή στο Internet (για μετάδοση μέσω των προγραμμάτων P2P)
  - Αναστολή λειτουργίας ή δυσλειτουργία του Λ.Σ.
  - Καταστροφή των τομέων εκκίνησης (boot sectors), πινάκων καταχώρησης αρχείων (FAT), και πινάκων κατατμήσεων (partition tables).
- Δημιουργία «κερκόπορτας» (back door) με σκοπό την (μετέπειτα) παραβίαση της ασφάλειας του συστήματος (σχετικές κατηγορίες: trojans, rootikits, zombies)
- Επιθέσεις εναντίον της διαθεσιμότητας συστημάτων (σχετικές κατηγορίες: worms, bots-zombies)
  - Κατανάλωση υπολογιστικών πόρων (κύρια μνήμη, αποθηκευτικός χώρος)
  - Κατανάλωση της χωρητικότητας (bandwidth) του δικτύου
  - Χρήση των ξενιστών για συγχρονισμένη επίθεση σε κάποιον τρίτο, στα πλαίσια μιας επίθεσης DDOS (Μάγκος, 2007)

```
beginvirus:
   if spread-condition then begin
       for some set of target files do begin
           if target is not infected then begin
               determine where to place virus instructions
               copy instructions from beginvirus to endvirus
                   into target
               alter target to execute added instructions
           end;
       end;
   end;
   perform some action(s)
   goto beginning of infected program
endvirus:
```

Εικόνα 40: «Ιός–Ψευδοκώδικας» πηγή εικόνας: http://oncampus.richmond.edu/~dszajda/classes/cs395_computer_security/Fall_2004/slides/MaliciousLogic.ppt

3.5 Ισχυον θεσμικο πλαισιο στην Ελλαδα για την απατη μεσω ηλεκτρονικου ταχυδρομειου

❖ ***SPAM***

*Στην Ελλάδα το spam ρυθμίζεται από το αρ. 11 του **Νόμου 3471/2006**, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.*

Σύμφωνα με τις παρ. 1 και 2 του αρ. 11 "Μη ζητηθείσα επικοινωνία": "

1. *Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.*
2. *Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών με ανθρώπινη παρέμβαση (κλήσεων) για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής της διαθέσιμης στο κοινό υπηρεσίας, ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις. Ο φορέας υποχρεούται να καταχωρίζει δωρεάν τις δηλώσεις αυτές σε ειδικό κατάλογο συνδρομητών, ο οποίος είναι στη διάθεση κάθε ενδιαφερομένου. "*

Με άλλα λόγια, κάθε ηλεκτρονικό μήνυμα που σας αποστέλλεται χωρίς την πρότερη ρητή συγκατάθεση σας, δηλαδή κάθε μήνυμα spam, είναι παράνομο. Το σύστημα αυτό είναι γνωστό στη διεθνή ορολογία ως σύστημα «opt-in».

*Ειδικά για τα μηνύματα ηλεκτρονικού ταχυδρομείου, εξαίρεση αποτελεί, σύμφωνα με την **παρ. 3 του αρ. 11,** η περίπτωση στην οποία η ηλεκτρονική διεύθυνση του χρήστη αποκτήθηκε από τον αποστολέα νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής. Στην περίπτωση αυτή μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να αποστέλλονται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρετηθήση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση (σύστημα "opt-out").*

Επίσης, ως προς την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, ορίζεται ότι θα πρέπει να αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητά τον τερματισμό της επικοινωνίας.

Η εφαρμογή των παραπάνω ρυθμίσεων επεκτείνεται, πέρα από τα φυσικά, και στα νομικά πρόσωπα.

(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

❖ ***Phishing***

Επειδή η μέθοδος "phishing" βασίζεται στην πλάνη του θύματος με σκοπό την περιουσιακή του ζημία, είναι προφανές ότι οι Phishers μέσω αυτής προσπορίζουν στον εαυτό τους ή/και σε τρίτους παράνομο περιουσιακό όφελος. Επειδή δε οι δράστες έχουν γνώση και θέληση σχετικά με την παράνομη δραστηριότητά τους, συμπεραίνεται ότι το "phishing" συνιστά

*απάτη, κατά το **άρθρο 386 του Ποινικού Κώδικα**, σύμφωνα με το οποίο «όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών».* (Wikipedia, Διαδίκτυο-Νομικά και ηθικά ζητήματα)

- ***Ηλεκτρονική Απάτη***

*Ο **Ν. 1805/88**, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) και στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.*

Στην ελληνική νομοθεσία όμως, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τελεία αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Αρθρο 370Β

1. *Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.*
2. *Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.*
3. *Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.*
4. *Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.*

Άρθρο 370Γ

1. *Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.*
2. *Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις*

μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. *Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.*
4. *Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.*

Αρθρο 386Α - Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα. (Αστυνομία)

4 Μηχανισμοι ασφαλειας για το Ηλεκτρονικο Ταχυδρομειο

4.1 Εισαγωγη

Αφού περιγράψαμε λεπτομερώς όλους τους κινδύνους του ηλεκτρονικού ταχυδρομείου που θέτουν σε κίνδυνο την ασφάλεια του, σε αυτό το κεφάλαιο θα καθορίσουμε το πλαίσιο της ασφάλειας. Ανακεφαλαιώνοντας, έγινε σαφές από το προηγούμενο κεφάλαιο ότι οι επιθέσεις για το e-mail έχουν σαν στόχο:

- την υποκλοπή ενός μηνύματος.
- την παραποίηση ενός μηνύματος.
- την μεταμφίεση του αποστολέα.

Οι απειλές για την ασφάλεια λοιπόν μπορούν να χαρακτηριστούν ως : **παθητικές απειλές** οι οποίες αναφέρονται ως υποκλοπές και εμπεριέχουν τις απόπειρες από την πλευρά του επιτιθέμενου να αποκτήσει πληροφορίες και **ενεργητικές απειλές** που εμπεριέχουν κάποια μορφή τροποποίησης των μεταδιδόμενων δεδομένων ή τη δημιουργία εσφαλμένων μεταδόσεων. Εύλογα λοιπόν γεννιέται η ανάγκη για έναν μηχανισμό που θα έχει σαν στόχο:

- Την μετατροπή ενός μηνύματος σε μία μορφή κατανοητή μόνο από τα συμβαλλόμενα μέρη,
- Την βεβαίωση του αποστολέα για την ταυτότητα του και
- Την βεβαίωση για την αυθεντικότητα του μηνύματος και μη παραποίηση του.

Με μεγάλη διαφορά το μόνο αυτοματοποιημένο εργαλείο που μπορεί να παρέχει μία τέτοια ασφάλεια στην ηλεκτρονική αλληλογραφία είναι η **κρυπτογράφηση**. (Kurose&Ross, 2008) (Stallings, 2011) (S.Tanenbaum, 1996)

4.1.1 Σκοπος της κρυπτογραφιας

Στόχος της κρυπτογραφίας είναι η ασφαλέστερη ανταλλαγή δεδομένων και μηνυμάτων ανάμεσα σε 2 ανθρώπους χωρίς την παραβίαση του περιεχομένου του μηνύματος από τρίτους. Η κρυπτογραφία είναι κλάδος της επιστήμης της «κρυπτολογίας» (από τα συνθετικά «κρυπτός» και «λόγος») η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Η κρυπτολογία λοιπόν χωρίζεται σε δυο κλάδους:

a) την «κρυπτογραφία» που είναι η επιστήμη της απόκρυψης και στόχος της είναι να παρέχει μηχανισμούς ώστε δυο η περισσότερα μέλη να μπορούν να ανταλλάξουν μηνύματα μεταξύ τους, χωρίς να έχει πρόσβαση στην πληροφορία κάποιος άλλος.
b) Ο δεύτερος κλάδος της κρυπτολογίας είναι η «κρυπτανάλυση» που σαν στόχο έχει την αποκάλυψη του περιεχομένου κωδικοποιημένων μηνυμάτων ή δεδομένων. (Wikipedia, Cryptography) (Ζαρκάδης)

4.1.2 Αναγκαιοτητα της κρυπτογραφιας

Τα συστήματα υπολογιστών εκτίθενται καθημερινά σε πολλούς κινδύνους. Οι απειλές αυτές θέτουν σε κίνδυνο την ασφάλεια των υπολογιστών και των πληροφοριακών συστημάτων. Οι απόπειρες αυτές παραβίασης της ασφάλειας είναι ακούσιες η εκ προθέσεως. Οι επιπτώσεις όμως και στις δυο περιπτώσεις είναι ίδιες και διακρίνονται στις εξής κατηγορίες:

- Διακοπής ή άρνησης υπηρεσίας
- Υποκλοπής

- Παραποίησης
- Πειρατείας
- Αμφισβήτησης

Εδώ λοιπόν παίρνει ενεργό ρόλο στον τομέα της ασφάλειας η κρυπτογραφία. Για πολλούς ειδικούς , ασφάλεια χωρίς κρυπτογραφία είναι ……. Μισή ασφάλεια!!!!! Όσο και αν κάποιος θωρακίσει τον υπολογιστή του ώστε να μην μπαίνει τίποτα το ανεπιθύμητο χωρίς την έγκριση του, δεν αποκλείει ποτέ την περίπτωση της υποκλοπής. Όσο κάποιος θα έχει την δυνατότητα να παραβιάσει τα δεδομένα ποτέ δεν υπάρχει ασφάλεια. Την λύση σε αυτό το πρόβλημα έρχεται να δώσει η κρυπτογραφία. Εφόσον κρυπτογραφούνται τα δεδομένα που διακινούνται, ακόμα και αν κάποιος «βλέπει» τα πακέτα που ταξιδεύουν από και προς το μηχάνημά μας, αδυνατεί να εξάγει χρήσιμη πληροφορία από αυτά.

4.1.3 Στοχοι της κρυπτογραφιας

Σύμφωνα με όσα έχουν αναφερθεί καταλήγουμε στους βασικούς στόχους της κρυπτογραφίας οι οποίοι είναι:

a. Εμπιστευτικότητα ή μυστικότητα : είναι η δυνατότητα του να διατηρείται η πληροφορία κρυφή από όλους τους άλλους εκτός από αυτούς που είναι εξουσιοδοτημένοι να την δουν. Έτσι στην περίπτωση που στην ανταλλαγή αλληλογραφίας παρεμβάλλεται κάποιος τρίτος , το μήνυμα που θα υποκλαπεί δεν θα είναι δυνατόν να γίνει κατανοητό από τον υποκλοπέα. Αύτό το στοιχείο της εμπιστευτικότητας είναι πιθανώς η συνηθέστερα αντιληπτή σημασία του όρου «ασφαλής επικοινωνία».
b. Ακεραιότητα των δεδομένων: η δυνατότητα της διασφάλισης ότι η πληροφορία δεν έχει παραποιηθεί από τρίτους κατά την διάρκεια της μεταφοράς της.
c. Πιστοποίηση ταυτότητας: η επιβεβαίωση της ταυτότητας του χρήστη.
d. Πιστοποίηση μηνύματος: η επιβεβαίωση της πηγής από την οποία προέρχεται η πληροφορία.
e. Υπογραφή : η οποία είναι ένα μέσο προσάρτησης της πληροφορίας ενός χρήστη στα δεδομένα που μεταδίδονται που σαν στόχο έχουν πιστοποίηση της ταυτότητας.
f. Εξουσιοδότηση : η δυνατότητα της έγκρισης σε μια οντότητα να κάνει κάτι.
g. Επικύρωση : είναι το μέσο για να αποδώσει κάποιος έγκριση σε μια οντότητα να έχει το δικαίωμα πρόσβασης σε μια πληροφορία ή σε άλλα μέσα.
h. Μη αποκύρηξη ευθύνης: όπου είναι μια υπηρεσία στην οποία αποτρέπει μια οντότητα από την άρνηση πραγματοποίησης προηγούμενων δεσμεύσεων ή ενέργειων. Όταν προκύπτουν διαφορές οφείλονται σε μια οντότητα που αρνείται ότι έχουν γίνει κάποιες πράξεις ,τότε είναι απαραίτητο ένα μέσο για την επίλυση της κατάστασης π.χ. στην περίπτωση μιας πράξης αγοροπωλησίας. Μια διαδικασία που εμπλέκει , μία έμπιστη τρίτη αρχή είναι αναγκαία για την επίλυση της διαφοράς.

Ο θεμελιώδης στόχος της κρυπτογραφίας είναι να συνδυάσει επαρκώς όλους αυτούς τους τομείς και από πλευράς θεωρίας και πρακτικής , προλαμβάνοντας και ανιχνεύοντας ταυτόχρονα την πιθανή εξαπάτηση και άλλες κακόβουλες δραστηριότητες. (Kurose&Ross, 2008) (Λιμνιώτης) (A. Menezes, August 2001)

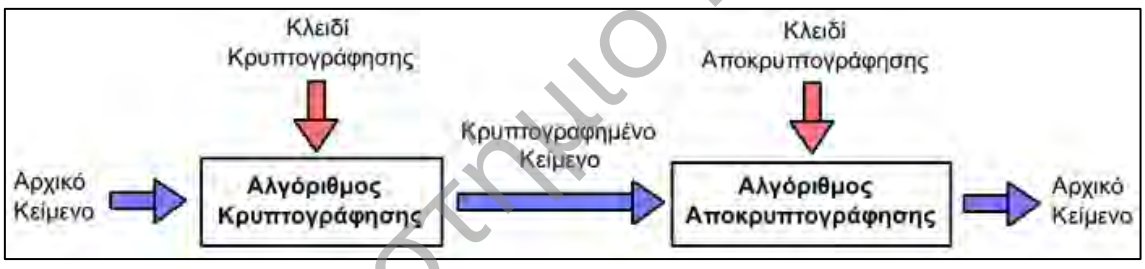
4.1.4 Ορισμος της Κρυπτογραφιας & Δομικα Στοιχεια της Κρυπτογραφιας

Αρχικά ο όρος «**κρυπτογραφία**» προέρχεται από τα συνθετικά «κρυπτός» και το ρήμα «γράφω». Κρυπτογραφία είναι η τέχνη και η επιστήμη του κρυφού γραψίματος. Όταν χρησιμοποιείται η τέχνη της κρυπτογραφίας στην ουσία συμπεριλαμβάνει τις εξής έννοιες:

- «**plain text**» όπου είναι το αρχικό μήνυμα απλού κείμενου το οποίο συντάσσεται.

- «**encryption function-συνάρτηση κρυπτογράφησης**» ο αποστολέας του μηνύματος εφαρμόζει τη συνάρτηση αυτή στο αρχικό μήνυμα απλού κειμένου για να παράγει το κρυπτογραφημένο μήνυμα.
- «**κλειδί-key**» η συνάρτηση κρυπτογράφησης παίρνει σαν παράμετρο ένα κλειδί όπου είναι μία συμβολοσειρά πεπερασμένου μήκους το οποίο παραμένει απόρρητο για την δημιουργία της συνάρτησης ενώ οι συναρτήσεις θεωρούνται δημόσια γνώση.
- «**αλγόριθμος κρυπτογράφησης E**» Η διαδικασία της κρυπτογράφησης επιτυγχάνεται με την εφαρμογή ενός αλγόριθμου που λαμβάνεται σαν παράμετρος για την συνάρτηση. Αυτός ο αλγόριθμος κρυπτογράφησης και είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον διαβάλλει κάποιος . Μαθηματικά ο αλγόριθμος κρυπτογράφησης **E** δέχεται ως είσοδο ένα μήνυμα **M**(plaintext) και ένα κλειδί $\mathbf{K_A}$, και δίνει στην έξοδο ένα κρυπτογραφημένο μήνυμα **C** (ciphertext) : $\mathbf{C=E_{KA}\ (M)}$
- «**cipher text**» το κείμενο που μετατρέπεται σε κάτι δυσανάγνωστο το οποίο ονομάζεται κρυπτογράφημα.
- «**decryption function-συνάρτηση αποκρυπτογράφησης**» ο παραλήπτης εφαρμόζει μία απόρρητη συνάρτηση αποκρυπτογράφησης –την αντίστροφή της συνάρτησης κρυπτογράφησης ,εφαρμογή του αντίστροφου αλγόριθμου —για να ανακτήσει το αρχικό απλό κείμενο.

Η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα.

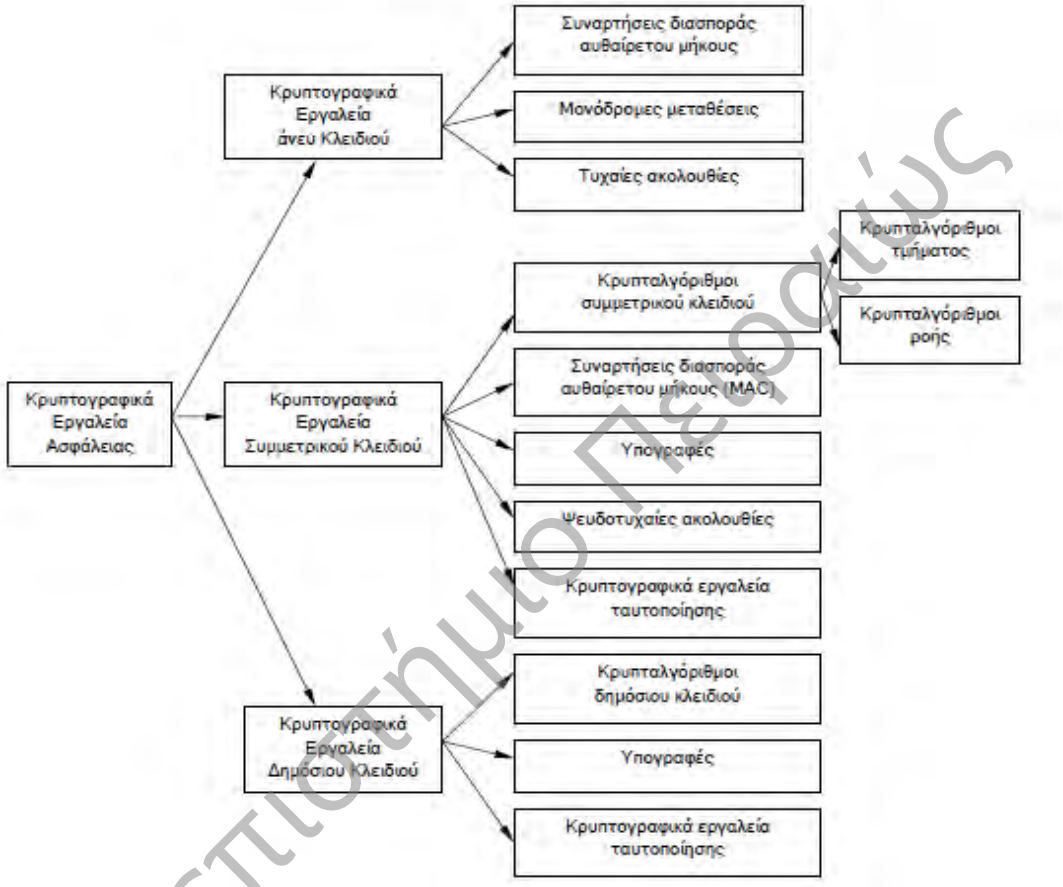


Εικόνα 41: «Τυπικό σύστημα κρυπτογράφησης – αποκρυπτογράφησης» πηγή εικόνας: http://en.wikipedia.org/wiki/Cryptography)

(Ζαρκάδης) (Wikipedia, Cryptography) (Κοτζανικολάου, 2012)

4.2 Κρυπτογραφικα Συστηματα

Σε αυτό το κεφάλαιο θα αναλύσουμε κάποιες από τις κατηγορίες των κρυπτογραφικών συστημάτων που χρησιμοποιούνται για την ασφαλή αλληλογραφία. Στην παρακάτω εικόνα παρουσιάζεται η γενική δομή των κρυπτογραφικών εργαλείων.



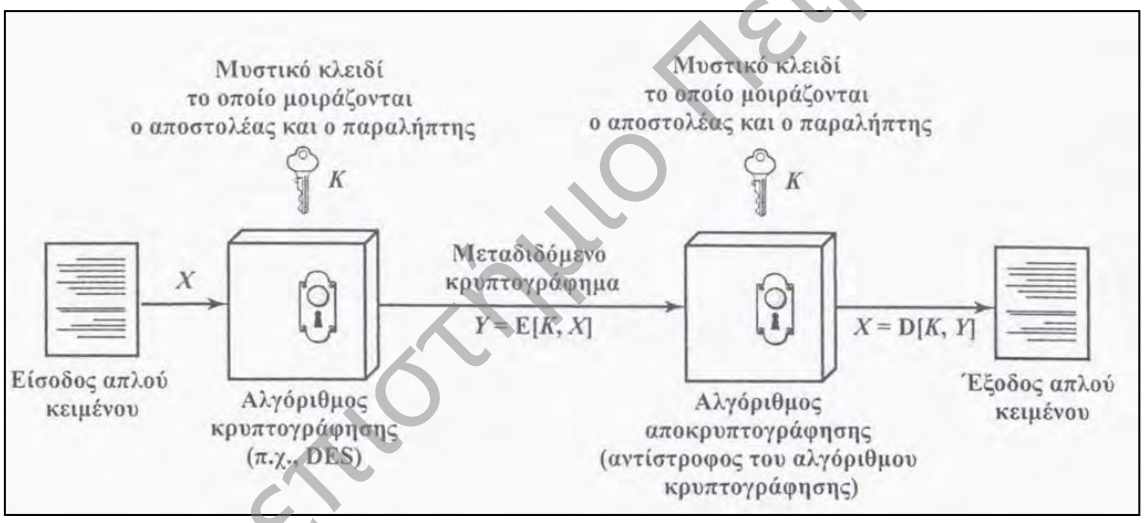
Εικόνα 42: «Ταξινόμηση των κρυπτογραφικών εργαλείων» πηγή εικόνας: (Πληροφορική_Online) (Κοτζανικολάου, 2012)

4.2.1 Συμμετρικη Κρυπτογραφια η Κρυπτογραφια Συμμετρικου Μυστικου Κλειδιου

Στην συμμετρική κρυπτογραφία χρησιμοποιείται ένα κλειδί για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Ο Data Encryption Standard (DES), είναι ο γνωστός αλγόριθμος συμμετρικής κρυπτογράφησης ο οποίος υιοθετήθηκε από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Άρα στην συμμετρική κρυπτογραφία θα πρέπει να γνωρίζουν και να χρησιμοποιούν μόνο τα εξουσιοδοτημένα μέλη το ίδιο μυστικό κλειδί, δηλαδή ο αποστολέας και ο παραλήπτης. Επομένως απαιτείται ασφαλές μέσο για τη μετάδοσή του όπου τα μέλη θα συμφωνήσουν για το κλειδί που θα χρησιμοποιείται.

Κατά τη συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού, ο αποστολέας με την χρήση του μυστικού κλειδιού κρυπτογραφεί το μήνυμα ενώ ο παραλήπτης με το ίδιο κλειδί το αποκρυπτογραφεί. Δηλαδή χρησιμοποιείται το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση $K_A = K_B = K$. Οι κρυπτογραφίες συμμετρικού κλειδιού είναι γνωστές και ως **κρυπτογραφίες απόρρητου κλειδιού (secret-key ciphers).** Η διαδικασία συμμετρικής κρυπτογραφίας φαίνεται αναλυτικότερα στη παρακάτω εικόνα.

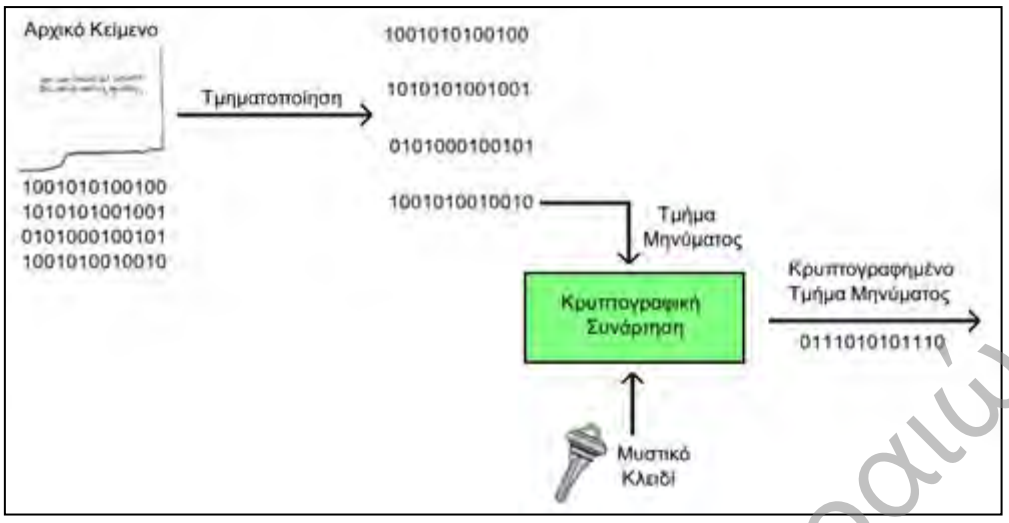


Εικόνα 43: «Συμμετρική Κρυπτογραφία» πηγή εικόνας: (Stallings, 2011)

Η συμμετρική κρυπτογράφηση χρησιμοποιεί δυο κατηγορίες αλγορίθμων:

i. Αλγόριθμους κρυπτογράφησης τμήματος (block ciphers)

Οι Αλγόριθμοι κρυπτογράφησης τμήματος (block ciphers) μετατρέπουν ένα τμήμα μη κρυπτογραφημένου κειμένου, καθορισμένου μεγέθους (plaintext), σε ίδιου μεγέθους τμήμα κρυπτογραφημένου κειμένου (ciphertext).Το καθορισμένο μήκος καλείται μέγεθος τμήματος (block size) όπου συνήθως το block size είναι ίσο με το μέγεθος του κλειδιού (key size). Οι αλγόριθμοι τμημάτων λειτουργούν επαναληπτικά, κρυπτογραφώντας δηλαδή ένα τμήμα διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπό-κλειδί. Το σύνολο των υπό-κλειδιών προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Μια απεικόνιση τέτοιας κρυπτογράφησης με αλγόριθμο τμήματος (block ciphers) παριστάνεται στην παρακάτω εικόνα:

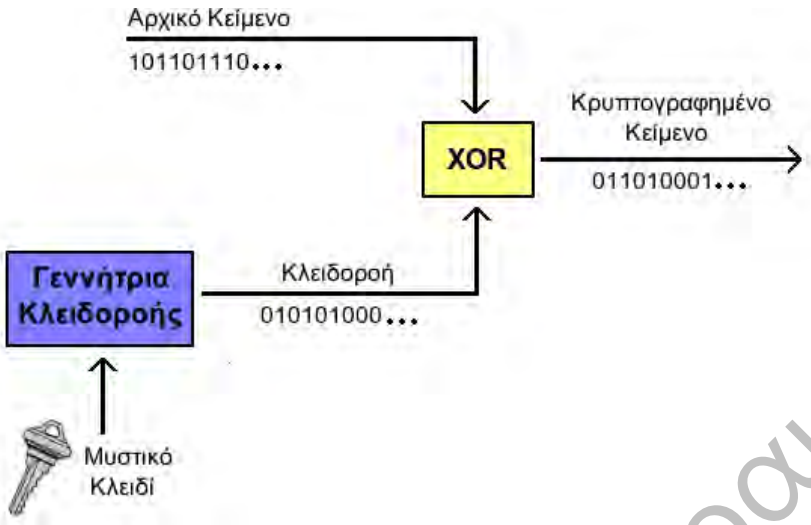


Εικόνα 44: «Αλγόριθμος κρυπτογράφησης τμήματος (block ciphers)» πηγή εικόνας: http://el.wikipedia.org

Συνηθισμένα μεγέθη ενός τμήματος δεδομένων είναι τα 64 ή 128 bits που χρησιμοποιούν ο DES και 3DES αντίστοιχα. Επίσης ο AES τμηματοποιεί από 128, 256 έως 512 bits.

ii. Αλγόριθμοι κρυπτογράφησης ροής (stream ciphers)

Οι αλγόριθμοι ροής (stream ciphers) χρησιμοποιούνται για την κρυπτογράφηση μίας συνεχούς ροής δεδομένων (data stream). Για την κρυπτογράφηση επιλέγεται αρχικά μία *γεννήτρια κλειδοροής (keystream generator)*, η οποία δέχεται ως είσοδο το μυστικό κλειδί και παράγει στην έξοδό της μία ψευδοτυχαία ακολουθία bits, η οποία ονομάζεται κλειδοροή (keystream). Στην συνέχεια εφαρμόζεται η συνάρτηση **XOR** ανάμεσα στο αρχικό κείμενο και στην κλειδοροή και το αποτέλεσμα της συνάρτησης είναι η τελική κρυπτογραφημένη ροή δεδομένων. Η διαδικασία που μόλις περιγράφηκε φαίνεται πιο καθαρά στο σχήμα που παρατίθεται. Η αποκρυπτογράφηση γίνεται με την ακριβώς αντίστροφη διαδικασία. Εάν χρησιμοποιηθεί το ίδιο κλειδί ως είσοδο στην γεννήτρια κλειδοροής, τότε η δεύτερη θα παράγει ακριβώς την ίδια ακολουθία bits (κλειδοροή) όπως και προηγουμένως κατά την διαδικασία της κρυπτογράφησης. Εφαρμόζοντας την συνάρτηση XOR ανάμεσα στην κρυπτογραφημένη ακολουθία δεδομένων και την κλειδοροή παράγεται τελικά το αρχικό κείμενο. Στην παρακάτω εικόνα φαίνεται η λειτουργία αυτού του αλγορίθμου:



Εικόνα 45: «Αλγόριθμος κρυπτογράφησης ροής (stream ciphers)» πηγή εικόνας: (Wikipedia, Κρυπτογραφικοί Αλγόριθμοι Ροής)

Για την ασφαλέστερη μετάδοση όμως του συμμετρικού κλειδιού απαιτείται μια προσωπική συνάντηση, κάτι που στις περισσότερες περιπτώσεις καθίσταται αδύνατο και αυτό είναι που κάνει την συμμετρική κρυπτογραφία πολλές φορές αναποτελεσματική. Παρόλα αυτά όμως η συμμετρική κρυπτογραφία δεν χρησιμοποιείται μόνο για κρυπτογράφηση αλλά και για πιστοποίηση ταυτότητας. (Wikipedia, Κρυπτογραφικοί Αλγόριθμοι Ροής)

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
○ Μεγάλη απόδοση (efficiency): μέχρι 100-αδες MB/sec για h/w implementations	○ Η δύσκολη συνεννόηση και ανταλλαγή κλειδιού και η ευκολία παραβίασης μίας τέτοιας συνεννόησης.
○ Μικρό μήκος κλειδιού	○ Στην περίπτωση παραβίασης του μυστικού κλειδιού η τροποποίηση των μηνυμάτων μπορεί να περάσει απαρατήρητη σε 2 ανυποψίαστους χρήστες.
	○ Αριθμός κλειδιών: για n χρήστες, (n-1) κλειδιά ανά χρήστη, συνολικά n(n-1)/2 κλειδιά

Πίνακας 5: «Πλεονεκτήματα / Μειονεκτήματα Συμμετρικής Κρυπτογραφίας» πηγή: (Κοτζανικολάου, 2012)

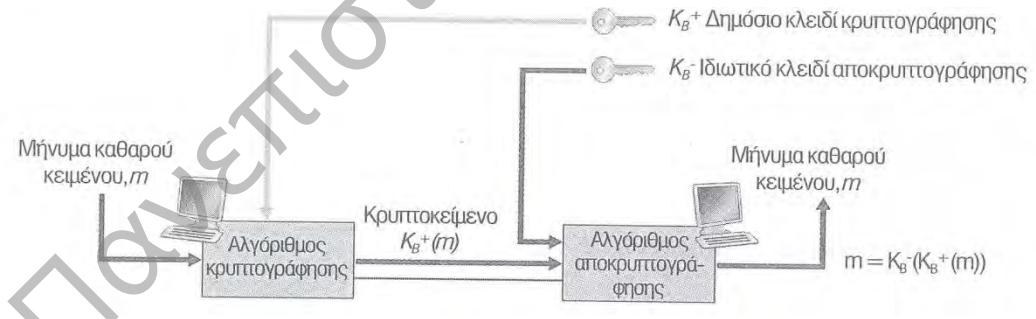
4.2.2 Ασυμμετρη κρυπτογραφηση η Κρυπτογραφια δημοσιου κλειδιου

Λόγω της δυσκολίας ανταλλαγής κλειδιού στην συμμετρική κρυπτογραφία προτάθηκε ένας άλλος αλγόριθμος κρυπτογράφησης γνωστή ως ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού. Στην ασύμμετρη κρυπτογραφία χρησιμοποιούνται δυο διαφορετικά κλειδιά για τις διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης. Η βασική αρχή κρυπτογραφίας δημοσίου κλειδιού διατυπώθηκε από τους Diffie και Hellman το 1976 ενώ το 1977 παρατηρούμε την πρώτη εμφάνιση του κρυπτοσυστήματος RSA που θεωρείται η πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού από τους Rivest, Shamir και Adleman οι οποίοι βασιστήκαν σε αρχές θεωρίες των πεπερασμένων πεδίων. Κάθε εξουσιοδοτημένος χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών:

a) το ένα είναι το δημόσιο κλειδί το οποίο δημοσιοποιείται γι΄αυτό και ονομάζεται έτσι και πάνω σε αυτό βασίζονται όλες οι επικοινωνίες και
b) το δεύτερο κλειδί ονομάζεται ιδιωτικό κλειδί και διατηρείται μυστικό και δεν μεταδίδεται στο δίκτυο.

Η βασική ιδέα της ασύμμετρης κρυπτογραφίας είναι η εμπιστοσύνη, η γνησιότητα και η επιβεβαίωση της συσχέτισης μεταξύ κλειδιών και κατοχών έτσι ώστε να μην είναι δυνατή η πλαστοπροσωπία. Αυτό για να επιτευχθεί εμπλέκονται και άλλοι μηχανισμοί που θα αναλυθούν παρακάτω αλλά οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης γίνονται με τον εξής τρόπο:

- Έστω ότι ο χρήστης Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα ***m*** στον χρήστη Β. Αφού γράψει το αρχικό μήνυμα στην συνέχεια χρησιμοποιεί το δημόσιο κλειδί του χρήστη Β K_B^+ που είναι γνωστό και διαθέσιμο προς όλους που επιθυμούν να συνομιλήσουν με το συγκεκριμένο χρήστη και μαζί με έναν γνωστό αλγόριθμο κρυπτογράφησης κρυπτογραφεί το μήνυμα { $K_B^+(m)$ }.
- Ο χρήστης Β λαμβάνει το κρυπτογραφημένο μήνυμα του Α και με το ιδιωτικό του κλειδί K_B^- σε συνδυασμό με έναν γνωστό αλγόριθμο κρυπτογράφησης, αποκρυπτογραφεί το μήνυμα δηλαδή υπολογίζει το ($K_B^-(K_B^+(m))$).
- Σε περίπτωση που ο χρήστης Β θέλει να απαντήσει στον χρήστη Α γίνεται η ανάστροφή διαδικασία.Η διαδικασία παρατηρείται στην παρακάτω εικόνα:



Εικόνα 46: «η κρυπτογραφία δημοσίου κλειδιού» πηγή εικόνας: (Kurose&Ross, 2008)

Η χρήση της ασύμμετρης κρυπτογραφίας αν και φαίνεται θεωρητικά απλή, παρόλο αυτά παρουσιάζει κάποια τρωτά σημεία στην ασφάλεια του μηνύματος.

I. Ένα πρώτο θέμα είναι ότι στην περίπτωση που κάποιος εισβολέας υποκλέψει το μήνυμα του χρήστη Α προς τον χρήστη Β παρόλο που το μήνυμα θα είναι σε μία ακατανόητη μορφή , το δημόσιο κλειδί καθώς και ο προτυποποιημένος αλγόριθμος είναι γνωστά, έτσι μπορεί αν τα εφαρμόσει σε κάποιο αρχικό μήνυμα που υποθέτει ότι μπορεί να έχει γράψει ο χρήστης Α και το αποτέλεσμα είναι ίδιο έχει ανακτήσει το κρυπτογραφημένο μήνυμα ή ακόμα χειρότερα να συμπεριλάβει τμήματα κειμένου

μέσα στο αρχικό μήνυμα του χρήστη Α με την ίδια κρυπτογράφηση χωρίς να δώσει την παραμικρό στοιχείο να υποψιαστεί ο χρήστης Β ότι το μήνυμα έχει παραποιηθεί.

II. Μία δεύτερη και πολύ σημαντική ευπάθεια του ασύμμετρου μηχανισμού κρυπτογραφίας είναι η αβεβαιότητα της ταυτότητας του αποστολέα καθώς στην συμμετρική κρυπτογραφία το γεγονός ότι ο αποστολέας γνωρίζει το μυστικό κλειδί ταυτοποιεί άρρητα τον αποστολέα στον παραλήπτη.

Αυτές τις αδυναμίες έρχονται να λύσουν δύο ακόμα μηχανισμοί που λειτουργούν συμπληρωματικά στης κρυπτογραφία δημοσίου κλειδιού και είναι γνωστοί ως **συνάρτηση κατακερματισμού ή σύνοψη μηνύματος (hash function)** και **η ψηφιακή υπογραφή (digital signature)** που λύνουν τα προβλήματα της ακεραιότητας του μηνύματος και την ταυτοποίηση του αποστολέα αντίστοιχα. Πριν αναλύσουμε αυτές τις έννοιες. Θα αναφερθούμε στον αλγόριθμο RSA που έχει γίνει σχεδόν συνώνυμος με την κρυπτογραφία δημοσίου κλειδιού καθώς είναι αυτός που δημιουργεί την σύνοψη μηνύματος και την ψηφιακή υπογραφή.

Τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας παρουσιάζονται στον παρακάτω πίνακα:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
➢ Αποδεικνύεται εύκολα από που ξεκίνησε το κάθε κρυπτογραφημένο μήνυμα.	○ Πολύπλοκοι Υπολογισμοί : Αυξημένο Υπολογιστικό Κόστος (1000 φορές πιο αργή από την συμμετρική)
➢ Δεν χρειάζεται ασφαλές κανάλι επικοινωνίας για την ανταλλαγή των δημοσίων κλειδιών.	○ Κρυπτογράφηση Περιορισμένου Μεγέθους Πληροφορίας.
➢ Μπορεί να εφαρμοστεί ευκολότερα σε μεγάλα frameworks.	○ Ανάγκη ισχυρής προστασίας του ιδιωτικού κλειδιού

Πίνακας 6: «Πλεονεκτήματα / Μειονεκτήματα Συμμετρικής Κρυπτογραφίας» πηγή: (Κοτζανικολάου, 2012)

4.2.3 Αλγοριθμος RSA

Ο RSA είναι ένας κρυπταλγόριθμος ασύμμετρου κλειδιού που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακής υπογραφής.

Η Λειτουργία του RSA βασίζεται στην δυσκολία παραγοντοποίησης μεγάλων αριθμών έως και 2048 bits. Χρησιμοποιούνται δυο κλειδιά, ένα δημόσιο κατά την διάρκεια της κρυπτογράφησης και ένα κρυφό για την αποκρυπτογράφηση.

i. Για την Δημιουργία των κλειδιών:

- Επιλέγονται δυο τυχαίοι (μεγάλοι) πρώτοι αριθμοί **p** και **q**
- έτσι ώστε **p ≠ q**
- Προκύπτει μια σχέση **p * q**
- Υπολογίζεται η συνάρτηση του Όιλερ όπου είναι μια αριθμοθεωρητική συνάρτηση η οποία ορίζεται στους θετικούς ακέραιους αριθμούς η οποία συμβολίζεται με φ ελληνικό και είναι:**φ(n)= (p-1) (q-1)**.
- Επιλογή ενός αριθμού e >1 έτσι ώστε ο **ΜΚΔ(e, φ) =1.**
- Στην συνέχεια υπολογίζεται ο αριθμός d έτσι ώστε **e d = 1 mod φ(n).**

Για την εύρεση πρώτων αριθμών χρησιμοποιούνται πιθανολογικοί αλγόριθμοι. Συνηθισμένες επιλογές για το **e** είναι το 3, 7 και 216 + 1. Μικροί αριθμοί οδηγούν σε ταχύτερους υπολογισμούς αλλά και σε πιο αδύνατη ασφάλεια. Έχοντας κάνει αυτούς τους υπολογισμούς τα κλειδιά που δημιουργούνται είναι:

a) Δημόσιο: $\mathbf{PK_A = e}$
b) Κρυφό: $\mathbf{SK_A = d}$

Στην συνέχεια το πρώτο κλειδί μπορεί να δημοσιευτεί, δίνοντας έτσι την δυνατότητα σε οποιονδήποτε χρήστη να στείλει κρυπτογραφημένα μηνύματα που μόνο εμείς (χάρη στο κρυφό κλειδί) μπορούμε να αποκρυπτογραφήσουμε.

ii. Κρυπτογράφηση:

Το μήνυμα μπορεί να αντιπροσωπευθεί από έναν αριθμό **m** όπου **m < n** (π.χ. "RSA" → 0x525341, όπου 0x52 είναι ο δεκαεξαδικός κωδικός ASCII του χαρακτήρα R, 0x53 του S και τέλος 0x41 του A). Το κρυπτογραφημένο μήνυμα **c** υπολογίζεται με τον εξής τρόπο**:** $\mathbf{c = m^e \bmod n}$.

iii. Αποκρυπτογράφηση:

Αφού ληφθεί ένα κρυπτογραφημένο μήνυμα **c**, για να διαβαστεί το αρχικό μήνυμα γίνεται ο ακόλουθος υπολογισμός: $\mathbf{m = c^d \bmod n \equiv (m^e)^d \bmod n \equiv m^{ed} \bmod n}$. Ξέρουμε πως $\mathbf{e.d \equiv 1 \pmod{p-1}}$ **και** $\mathbf{e.d \equiv 1 \pmod{q-1}}$**,** όποτε χρησιμοποιώντας το μικρό θεώρημα του Φερμά, έχουμε:

$\mathbf{m^{ed} \equiv m^1 \equiv m \bmod p-1}$ και $\mathbf{m^{ed} \equiv m^1 \equiv m \bmod q-1}$

Οι αριθμοί p και q είναι πρώτοι μεταξύ τους δηλαδή έχουν **ΜΚΔ=1**, χρησιμοποιώντας λοιπόν το Κινέζικο Θεώρημα Υπολοίπων, έχουμε: $\mathbf{m^{ed} \equiv m \bmod n}$.

(Κοτζανικολάου, 2012) (Wikipedia, RSA (cryptosystem))

4.2.4 Ψηφιακη υπογραφη

Το πρόβλημα της ταυτοποίησης έρχεται να λύσει ο μηχανισμός της Ψηφιακής Υπογραφής. Ο RSA επιτρέπει την ψηφιακή υπογραφή μηνυμάτων. Σαν άνθρωποι στην καθημερινή μας ζωή πιστοποιούμε κάποιον με πολλούς τρόπους όπως π.χ. αναγνώριση προσώπου, φωνής, φωτογραφία σε κάποιο δημόσιο έγγραφο, στην επικοινωνία μας όμως με άλλους πάνω στο δίκτυο δεν μπορούμε να βασιστούμε σε τέτοιες βιομετρικές πληροφορίες. Έτσι στην ηλεκτρονική επικοινωνία για την επίτευξη της βεβαίωσης του αποστολέα κάποιου μηνύματος χρησιμοποιείται μια τεχνική κρυπτογράφησης **η ψηφιακή υπογραφή (digital signature)**.

Όπως με τις κανονικές υπογραφές έτσι και η ψηφιακή υπογραφή πρέπει να γίνεται κατά τέτοιο τρόπο ώστε να μπορεί να είναι επαληθεύσιμη , με δυσκολία πλαστογράφησης αλλά και με δυνατότητα αποκήρυξης ευθύνης.

Έτσι στο παράδειγμα μας , της επικοινωνίας του χρήστη Α με τον χρήστη Β όταν ο χρήστης Α θέλει να υπογράψει ψηφιακά το μήνυμα **(m)** που έχει συντάξει θα χρησιμοποιήσει απλώς το ιδιωτικό του κλειδί $\boldsymbol{K_B^-}$, για να υπολογίσει το $\boldsymbol{K_B^-}$**(m)**, στόχος του είναι όχι να περιπλέξει ή να κρύψει τα περιεχόμενα του εγγράφου, αλλά να υπογράψει το έγγραφο. Έτσι όταν ο χρήστης Β παραλάβει το μήνυμα εάν θέλει να πιστοποιήσει ότι ο χρήστης Α έχει πράγματι υπογράψει το έγγραφο θα πάρει το δημόσιο κλειδί του Β, $\boldsymbol{K_B^+}$ και θα το εφαρμόζει στην ψηφιακή υπογραφή $\boldsymbol{K_B^-}$**(m),** συσχετίζοντάς το με το έγγραφο, m. Δηλαδή, υπολογίζει το $\boldsymbol{K_B^+}$**(**$\boldsymbol{K_B^-}$**(m))** και παράγει το αρχικό **m**, το οποίο ταιριάζει ακριβώς με το πρωτότυπο έγγραφο! Ο παραλήπτης προβαίνει στη ίδια μέθοδο. Έτσι η ταυτοποίηση επιτυγχάνεται ως εξής:

- Όποιος υπογραφεί ένα μήνυμα πρέπει να είχε χρησιμοποιήσει το ιδιωτικό του κλειδί K_B^-, για να υπολογίσει την υπογραφή $K_B^-(m)$, έτσι ώστε $K_B^+(K_B^-(m)) = m$.
- Το μόνο άτομο που γνωρίζει το ιδιωτικό κλειδί K_B^- είναι ο χρήστης Α, διότι όπως έχει προαναφερθεί η γνώση του δημόσιου κλειδιού K_B^+, δεν βοηθά στη διάδοση του ιδιωτικού, K_B^-. Έτσι, το μόνο άτομο που μπορεί να γνωρίζει το K_B^- είναι το άτομο που παρήγαγε το ζεύγος κλειδιών, (, K_B^-, , K_B^+).
- Αξιοσημείωτο επίσης είναι ότι αν το πρωτότυπο έγγραφο, m, τροποποιηθεί ποτέ σε κάποια εναλλακτική μορφή, m', η υπογραφή που έχει δημιουργήσει ο χρήστης Α για το m δεν Θα είναι έγκυρη για το m', εφόσον $K_B^+(K_B^-(m))$ δεν ισούται με m'. (S.Tanenbaum, 1996) (Κοτζανικολάου, 2012) (Kurose&Ross, 2008)

4.2.5 Συναρτηση Κατακερματισμου (Hash function)

Όπως προείπαμε στην περίπτωση υποκλοπής ενός μηνύματος από έναν μη εξουσιοδοτημένο χρήστη στην ασύμμετρη κρυπτογράφηση μπορεί να έχει σαν αποτέλεσμα ή την παραποίηση του μηνύματος εφόσον το δημόσιο κλειδί του παραλήπτη και ο αλγόριθμος κρυπτογράφησης είναι γνωστά αλλά ακόμα και η ανάκτηση ολόκληρου του μηνύματος. Την ευπάθεια της ακεραιότητας του μηνύματος έρχεται να λύσει ο μηχανισμός της σύνοψης του μηνύματος (message digest) που είναι το αποτέλεσμα μίας συνάρτησης κατακερματισμού (hash function).

Είναι σκόπιμο επίσης να ειπωθεί ότι οι συνόψεις μηνυμάτων δεν βεβαιώνουν μόνο την ακεραιότητα του μηνύματος αλλά βοηθάνε και τις ψηφιακές υπογραφές. Αυτό γίνεται ως εξής: πολλές συσκευές και διεργασίες δικτύου (π.χ., δρομολογητές που ανταλλάσσουν πληροφορίες πίνακα δρομολόγησης και πράκτορες email χρήστη, που ανταλλάσσουν e-mail) ανταλλάσσουν δεδομένα σε τακτά χρονικά διαστήματα, τα οποία ίσως να μην χρειάζεται να κρυπτογραφηθούν. Παρά ταύτα, απαιτείται η βεβαίωση ότι:

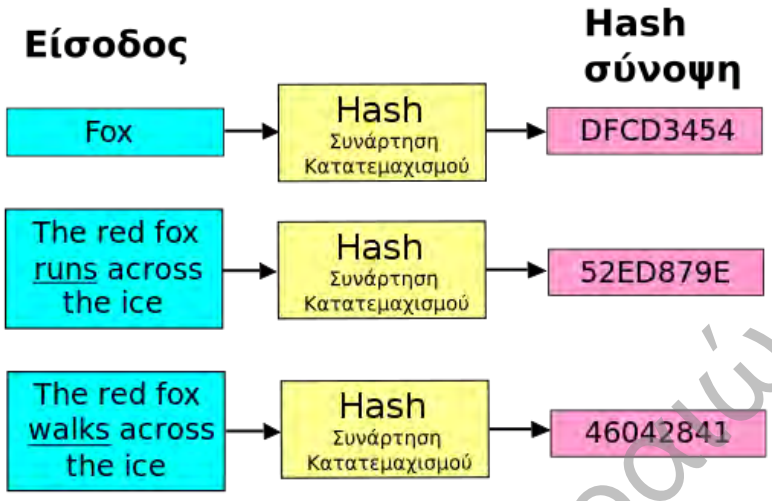
- ✓ Ο αποστολέας των δεδομένων είναι αυτός που ισχυρίζεται, δηλαδή, ότι ο αποστολέας έχει υπογράψει τα δεδομένα και ότι η υπογραφή αυτή μπορεί να ελεγχθεί.
- ✓ Τα μεταδιδόμενα δεδομένα δεν έχουν τροποποιηθεί από την ώρα που ο αποστολέας τα δημιούργησε και τα υπέγραψε.

Δεδομένων των επιπρόσθετων βαρών της κρυπτογράφησης και της αποκρυπτογράφησης, η υπογραφή δεδομένων μέσω πλήρους κρυπτογράφησης/ αποκρυπτογράφησης μπορεί να θεωρηθεί υπερβολή. Μια πιο αποδοτική προσέγγιση είναι η χρήση συνόψεων μηνυμάτων, μπορεί να επιτύχει αυτούς τους δύο στόχους χωρίς πλήρη κρυπτογράφηση μηνύματος.

Η συνάρτηση κατατεμαχισμού λοιπόν είναι μια μαθηματική συνάρτηση που έχοντας ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων m δίνει έξοδο μια καθορισμένου μεγέθους στοιχειοσειρά (string). Η έξοδος δεν μπορεί με κανένα τρόπο αντιστρέφοντας την να παράγει την αρχική είσοδο).Μια ιδανική κρυπτογραφική συνάρτηση κατατεμαχισμού έχει τις παρακάτω ιδιότητες:

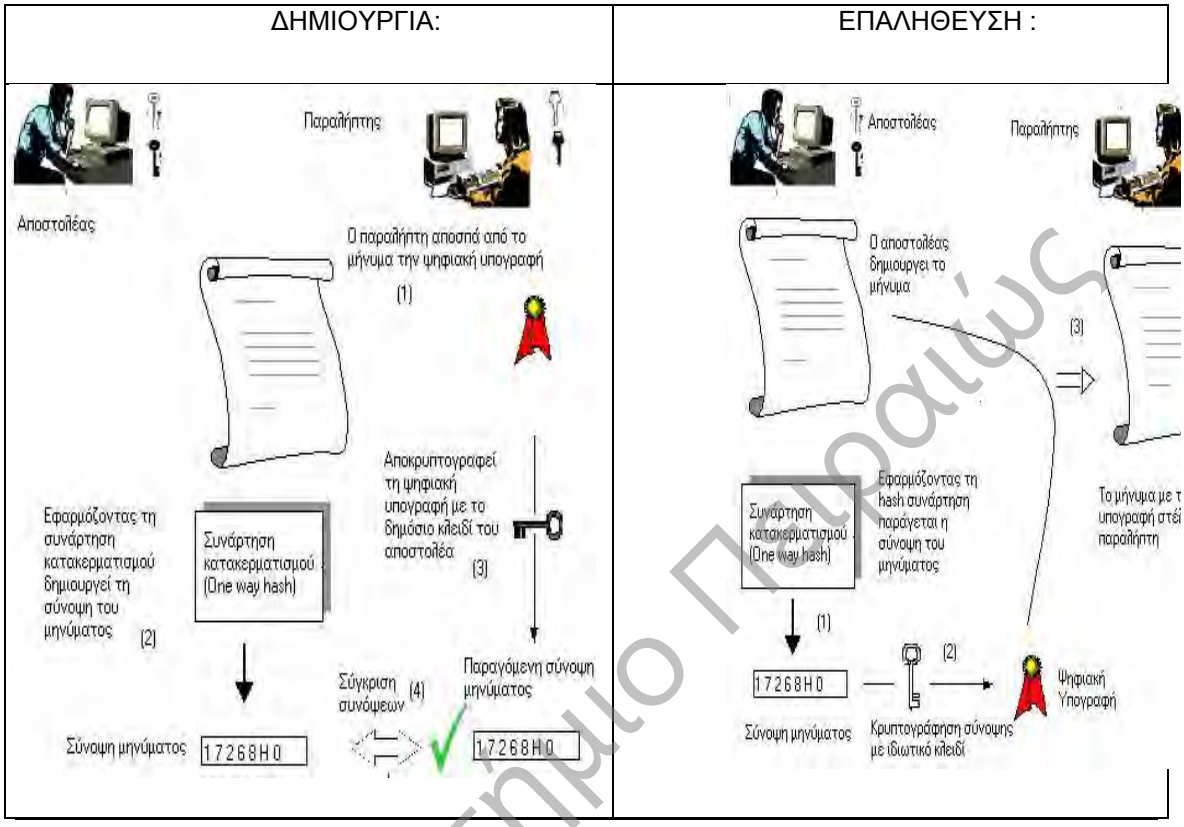
- Είναι εύκολο να υπολογιστεί η σύνοψη για οποιαδήποτε είσοδο.
- Δεν είναι εφικτό να βρεις την είσοδο από την σύνοψη.
- Δεν είναι εφικτό να τροποποιήσεις την είσοδο χωρίς να τροποποιηθεί η σύνοψη.
- Δεν είναι εφικτό να βρεθούν δύο διαφορετικές είσοδοι που δίνουν την ίδια σύνοψη.

Διάσημες συναρτήσεις κατατεμαχισμού είναι η **MD5** και η **SHA-1**. Η σύνοψη ενός μηνύματος **H(m)** είναι το αποτέλεσμα (έξοδος) της συνάρτησης κατατεμαχισμού. Η σύνοψη είναι συνήθως μικρότερη από το αρχικό μήνυμα και δεν μπορούμε να ξαναγυρίσουμε στο αρχικό μήνυμα από αυτή. Οι κρυπτογραφικοί αλγόριθμοι κατατεμαχισμού είναι φτιαγμένοι με τέτοιο τρόπο ώστε μια μικρή μεταβολή στα δεδομένα εισόδου (π.χ. Ένα μόνο γράμμα ή ακόμα και ένα μόνο bit) να προκαλεί ολοκληρωτική αλλαγή στην έξοδο (πλήρης αλλαγή της σύνοψης). Πιο αναλυτικά αν το **m** αλλάξει σε **m'** (είτε κακόβουλα, είτε κατά λάθος), τότε το **H(m)**, που υπολογίζεται για τα πρωτότυπα δεδομένα και μεταδίδεται μαζί με τα δεδομένα δεν θα ταιριάζει με το **H(m')**, που υπολογίζεται από τα τροποποιημένα δεδομένα **m'**. (Kurose&Ross, 2008) (wikipedia)



Εικόνα 47: «Παράδειγμα σύνοψης με την κρυπτογραφική συνάρτηση κατατεμαχισμού SHA-1» πηγή εικόνας: (wikipedia)

Οι διαδικασίες Δημιουργίας και Επαλήθευσης Ψηφιακής Υπογραφής- Σύνοψης Μηνύματος παριστάνονται στις παρακάτω εικόνες:



Εικόνα 48: «Δημιουργίας και Επαλήθευσης Ψηφιακής Υπογραφής»

4.3 PGP

Ένα από τα εργαλεία που υλοποιούν με το καλύτερο τρόπο τους σκοπούς της κρυπτογραφίας είναι το σχήμα κρυπτογράφησης e-mail **Pretty Good Privacy (PGP)** που δημιουργήθηκε από τον Phil Zimmermann το 1991, το οποίο χρησιμοποιείται για την ασφάλεια, πιστοποίηση και αυθεντικότητα ενός μηνύματος από την πλευρά του χρήστη, δηλαδή ο κάθε χρήστης που επιθυμεί ασφαλή επικοινωνία με άλλους χρήστες , μπορούν να εγκαταστήσουν το λογισμικό στον υπολογιστή τους να δημιουργήσουν το ιδιωτικό του κλειδί και να δημοσιεύσει το δημόσιο κλειδί του σε κάποιο ιστοχώρο του ή να το τοποθετήσει σε έναν εξυπηρετητή δημοσίων κλειδιών. Το PGP και όποιο παρόμοιο λογισμικό ακολουθούν το πρότυπο OpenPGP (RFC 4880) για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Επίσης παρέχει την πιστοποίηση ενός δημόσιου κλειδιού που είναι βέβαια διαφορετικός από την συμβατική αρχή πιστοποίησης. Τα δημόσια κλειδιά PGP πιστοποιούνται από έναν ιστό εμπιστοσύνης καθώς μπορούν να πιστοποιήσουν την εγκυρότητα και αυθεντικότητα του χρήστη. Η κρυπτογραφία PGP προσφέρει ασφάλεια από πλευράς πελάτη-χρήστη ηλεκτρονικού ταχυδρομείου και στο επίπεδο εφαρμογής στο TCP/IP.

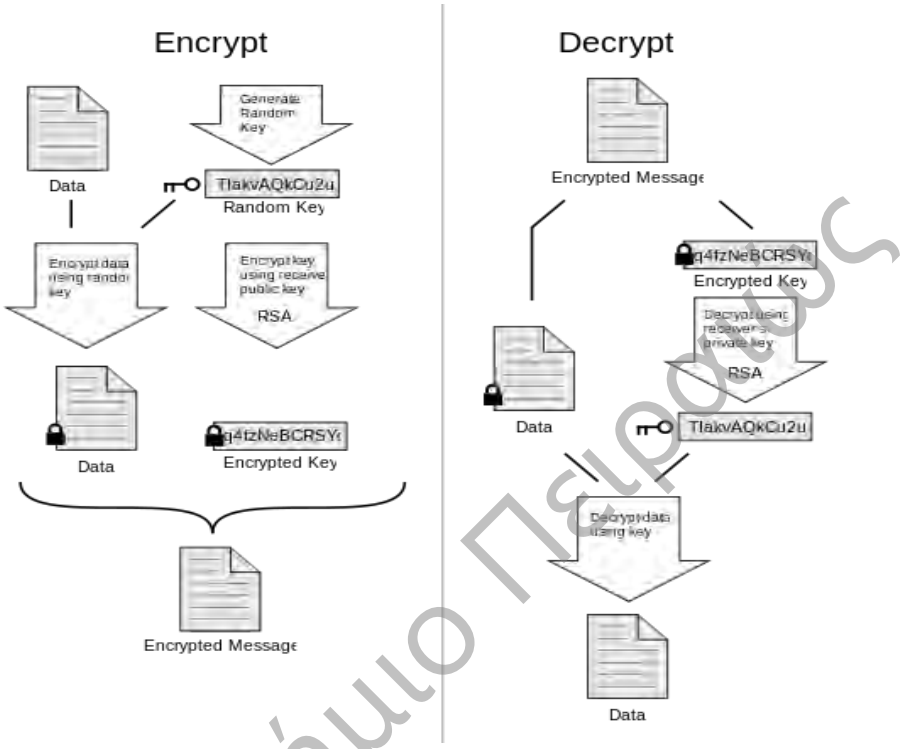
Πιο συγκεκριμένα η λειτουργία του PGP είναι ως εξής:

- Κάθε χρήστης που επιθυμεί να επικοινωνήσει με έναν άλλο χρήστη ανεξαρτήτως προγράμματος πελάτη ταχυδρομείου που έχει εγκατεστημένο στον υπολογιστή του και ανεξαρτήτως domain στο οποίο ανήκει η ταχυδρομική του θυρίδα , εγκαθιστά το λογισμικό PGP το οποίο με τη σειρά του δημιουργεί ένα ζεύγος κλειδιών που είναι δεσμευμένα με το όνομα κάθε χρήστη και την διεύθυνση email του.
- Στην συνέχεια ο εκάστοτε χρήστης μπορεί να δημοσιεύσει το δημόσιο κλειδί του έτσι ώστε όποιος επιθυμεί να επικοινωνήσει κρυπτογραφημένα μαζί του να χρησιμοποιήσει το κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Έτσι επιτυγχάνεται η ασφάλεια του μηνύματος και η αποτροπή ανάγνωσης από μη-εξουσιοδοτημένους χρήστες.
- Κατά την διάρκεια κρυπτογράφησης επίσης ο αποστολέας του μηνύματος χρησιμοποιεί αντίστοιχα το ιδιωτικό του κλειδί –που προστατεύεται από έναν κωδικό πρόσβασης και που κάθε φορά που προσπελαύνεται θα πρέπει να εισάγεται - για να υπογράψει ψηφιακά το μήνυμα. Έτσι επιτυγχάνεται η πιστοποίηση του χρήστη.

```
-----BEGIN PGP SIGNED MESSAGE-----

this is a test message,
signed with pgp using Test User's public key

adios.

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

iQEVAwUBPT4oB+C7envFYmALAQG9swgAo1+IKwaObHsPHd43ekD6wZYEJ8xl6qfR
AZp86aRCj3Pg49mS1BU2Yiq6QJPM0QTn7yCh2dWdr/1SvBvXavBvQfSmJTN4VU+j
IcNoHsZqmpnWhuLnoeQ9/HqCOWw50NcY1wU/1CTZYKT/D0ZqgP9eyonn9kf0JOGz
9PT/AK7MM+BFuO6CzTl0lXc0To3VPzRA87WU8IjTfEf/UGNWn3iysl6z/TQSKo1w
zq5EP7endZIPy6aal8B6buB6ql24s0bcklFALj6Ux4HIjjh6IEfd5kiJjtJPiArd
/xeY0fw0G39RpI5SrlhZNUCRR4m1wmQZX1d2L9Y9yoVjb2dq5xCDMA==
=oBys
-----END PGP SIGNATURE-----
```

Εικόνα 49: «Ένα υπογεγραμμένο μήνυμα PGP» πηγή εικόνας: http://peculiarplace.com/pgpex1.shtml)

- Μαζί με το κρυπτογραφημένο μήνυμα και την ψηφιακή υπογραφή το PGP υπολογίζει και στέλνει μαζί και την σύνοψη του μηνύματος έτσι ώστε να εξασφαλίζεται και η ακεραιότητα του μηνύματος. Στην εικόνα ___ φαίνεται η λειτουργία του PGP.



Εικόνα 50: «Λειτουργία PGP» πηγή εικόνας: http://en.wikipedia.org/wiki/Pretty_Good_Privacy

Στην προκειμένη περίπτωση που εγκαθιστούμε ένα διακομιστή αλληλογραφίας είναι χρήσιμο να παρέχουμε και ασφάλεια από πλευράς διακομιστή έτσι ώστε να πιστοποιείται η εγκυρότητα του κάθε διακομιστή που επιθυμεί επικοινωνία με κάποιο άλλο και όταν γίνεται αυτό να εγκαθιδρύεται ένα ασφαλές κανάλι μετά την πιστοποίηση.

Αυτό υλοποιείται σε ένα επίπεδο πιο κάτω, δηλαδή στο επίπεδο Μεταφοράς με τα γνωστά πρωτόκολλα SSL-Secure Sockets Layer και το μεταγενέστερο TLS-Transport Layer Security.

(Kurose&Ross, 2008) (Wikipedia, Pretty Good Privacy) (Alliance)

4.4 SSL

Μία από τις ευρύτατα χρησιμοποιούμενες υπηρεσίες ασφάλειας είναι το Επίπεδο Ασφαλούς Υποδοχής- SSL (Secure Sockets Layer) και το μεταγενέστερο πρότυπο γνωστό ως Ασφάλεια Επιπέδου Μεταφοράς - TLS (Transport Layer Security) είναι πρωτόκολλα που εγγυώνται την ασφαλή επικοινωνία εξυπηρετητή - πελάτη (server -client) μέσω του Διαδικτύου χωρίς την παρέμβαση τρίτων που θα "υποκλέψουν" το περιεχόμενο της επικοινωνίας. Χρησιμοποιούνται ως ενδιάμεσα πρωτόκολλα μεταξύ του επιπέδου εφαρμογών και του επιπέδου μεταφοράς.

Το SSL είναι σχεδιασμένο ώστε να χρησιμοποιεί το TCP/IP για να παρέχει αξιόπιστη υπηρεσία ασφάλειας από άκρο σε άκρο. Με την εμφάνιση και επικράτηση του Internet άρχισαν ταυτόχρονα να δείχνουν ενδιαφέρον οι εμπορικές επιχειρήσεις , έγινε λοιπόν προφανές ότι θα ήταν απαραίτητο ένα επίπεδο ασφάλειας για τις συναλλαγές στον Ιστό π.χ. όταν ένας χρήστης στέλνει τα στοιχεία της πιστωτικής του με σκοπό κάποια αγορά σε μία ιστοσελίδα αυτή η κίνηση πάντα προκαλεί μία ανησυχία για την ασφάλεια των δεδομένων του. Επομένως η ανάγκη για ακεραιότητα , εμπιστευτικότητα και πιστοποίηση ταυτότητας ήταν ζωτικής σημασίας για την διάδοση του Internet.

Η πρώτη και ευρέως χρησιμοποιούμενη λύση σε αυτό το πρόβλημα ήταν το SSL σχεδιασμένο από την εταιρεία Netscape. Στην συνέχεια οι σχεδιαστές του SSL και του μετέπειτα TLS αναγνώρισαν ότι τα προβλήματα δεν περιοριζόντουσαν μόνο στις συναλλαγές στο Διαδίκτυο και έτσι δημιούργησαν ένα πρωτόκολλο γενικής χρήσης το οποίο βρίσκεται μεταξύ Επιπέδου Εφαρμογών π.χ. HTTP ή SMTP και ενός πρωτοκόλλου Μεταφοράς TCP. Ο λόγος για το οποίο το πρωτόκολλο αποκαλείται **«ασφάλεια επιπέδου μεταφοράς»** είναι ότι από την οπτική γωνία της εφαρμογής, αυτό το επίπεδο πρωτόκολλων μοιάζει με κανονικό πρωτόκολλο μεταφοράς , με την εξαίρεση ότι είναι ασφαλές. Πιο συγκεκριμένα ο αποστολέας μπορεί να ανοίξει συνδέσεις , να παραδώσει byte προς μετάδοση και το ασφαλές πρωτόκολλο μεταφοράς θα τα διαβιβάσει στον παραλήπτη με την απαραίτητη εμπιστευτικότητα, ακεραιότητα και πιστοποίηση ταυτότητας. Έτσι με την υπηρεσία του SSL πάνω από το επίπεδο του TCP επιτυγχάνεται η χρήση όλων των χαρακτηριστικών του TCP όπως: αξιοπιστία , έλεγχος ροής, έλεγχος συμφόρησης και παρέχονται επίσης και στην εκάστοτε εφαρμογή.

Εναλλακτικά λοιπόν η υπηρεσία SSL μπορεί να χρησιμοποιηθεί είτε γενικά είτε σε συγκεκριμένα πακέτα λόγου χάριν εάν η υπηρεσία HTTP χρησιμοποιεί SSL είναι γνωστό ως HTTPS (ασφαλές HTTP, Secure HTTP) και το SMTP γνωστό ως SMTPS στην περίπτωση που χρησιμοποιεί SSL. Για λόγους ευκολίας εάν χρησιμοποιείται το SSL για διάφορες υπηρεσίες γίνεται χρήση και διαφορετικών θυρών στο TCP έτσι το συμβατικό HTTP χρησιμοποιεί την πόρτα 80 ενώ το HTTPS την πόρτα 443 αντίστοιχα το SMTP από την πόρτα 25 αλλάζει στην πόρτα 465 για SMTPS. Η παρακάτω εικόνα απεικονίζει τη θέση που βρίσκεται το ασφαλές επίπεδο μεταφοράς ανάμεσα στα επίπεδα εφαρμογών και TCP:

Εφαρμογή (π.χ. HTTP, SMTP)
Ασφαλές επίπεδο μεταφοράς
TCP
IP
Υποδίκτυο

Πίνακας 7: Ασφαλές Επίπεδο Μταφοράς στο TCP/IP

(Stallings, 2011) (Peterson&Davie, 2008)

4.4.1 Λειτουργια SSL

Το επίπεδο Ασφαλών Sockets, Secure Sockets layer (SSL) είναι ένα πρωτόκολλο σχεδιασμένο ώστε να παρέχει κρυπτογράφηση και πιστοποίηση δεδομένων ανάμεσα σε ένα πελάτη και ένα εξυπηρετητή WEB. Αρχικά ξεκινάει με μία φάση χειραψίας που διαπραγματεύεται έναν αλγόριθμο κρυπτογράφησης (π.χ. DES ή IDEA) και κλειδιά και πιστοποιεί τον εξυπηρετητή στον πελάτη. Προαιρετικά, ο πελάτης μπορεί επίσης να πιστοποιηθεί από τον εξυπηρετητή. Όταν ολοκληρωθεί η χειραψία και αρχίσει η μετάδοση των δεδομένων της εφαρμογής, όλα τα δεδομένα κρυπτογραφούνται χρησιμοποιώντας κλειδιά συνόδου, για τα οποία έχει προηγηθεί διαπραγμάτευση κατά τη φάση χειραψίας.

Τα SSL και TLS δεν περιορίζονται στην εφαρμογή Web, μπορούν να χρησιμοποιηθούν παρόμοια για πιστοποίηση και για κρυπτογράφηση δεδομένων για προσπέλαση ταχυδρομείου IMAP .

- **Από την πλευρά αποστολής**, το SSL δέχεται δεδομένα (όπως ένα μήνυμα HTTP ή IMAP από μια εφαρμογή), κρυπτογραφεί τα δεδομένα και κατευθύνει τα κρυπτογραφημένα δεδομένα σε μια ορισμένη TCP socket.
- **Από την πλευρά λήψης**, το SSL διαβάζει από την TCP socket, αποκρυπτογραφεί τα δεδομένα και τα κατευθύνει στην εφαρμογή.

Το SSL γενικά παρέχει τα εξής χαρακτηριστικά:

1. **Πιστοποίηση εξυπηρετητή SSL**, που επιτρέπει σε ένα χρήστη να επιβεβαιώσει την ταυτότητα ενός εξυπηρετητή. Ένα πρόγραμμα περιήγησης με δυνατότητες SSL διατηρεί μια λίστα έμπιστων αρχών πιστοποίησης (CA) μαζί με τα δημόσια κλειδιά των CA. Όταν το πρόγραμμα περιήγησης Θέλει να συνεργαστεί με έναν εξυπηρετητή Web με δυνατότητες SSL, το πρόγραμμα περιήγησης παίρνει ένα πιστοποιητικό από τον εξυπηρετητή, που περιέχει το δημόσιο κλειδί του. Το πιστοποιητικό εκδίδεται (δηλαδή, υπογράφεται ψηφιακά) από μια CA, που αναφέρεται στη λίστα των έμπιστων CA του πελάτη. Αυτό το χαρακτηριστικό επιτρέπει στο πρόγραμμα περιήγησης να πιστοποιήσει τον εξυπηρετητή πριν ο χρήστης υποβάλει έναν αριθμό κάρτας πληρωμών.
2. **Πιστοποίηση πελάτη SSL**, που επιτρέπει σε έναν εξυπηρετητή να επιβεβαιώσει την ταυτότητα ενός χρήστη. Ανάλογα με την πιστοποίηση εξυπηρετητή, η πιστοποίηση πελάτη χρησιμοποιεί πιστοποιητικά πελατών, τα οποία έχουν εκδοθεί επίσης από CA. Αυτή η πιστοποίηση είναι σημαντική αν οι εξυπηρετητές για παράδειγμα, είναι μια τράπεζα που στέλνει εμπιστευτικές οικονομικές πληροφορίες σε έναν πελάτη και θέλει να ελέγξει την ταυτότητα του παραλήπτη.
3. **Μια κρυπτογραφημένη σύνοδο SSL**, στην οποία όλες οι πληροφορίες που στέλνονται ανάμεσα στο πρόγραμμα περιήγησης και στον εξυπηρετητή κρυπτογραφούνται από το λογισμικό αποστολής (πρόγραμμα περιήγησης ή εξυπηρετητή Web) και αποκρυπτογραφούνται από το λογισμικό λήψης. Αυτή η εμπιστευτικότητα μπορεί να είναι σημαντική τόσο για τον πελάτη, όσο και για τον έμπορο. Επίσης, το SSL παρέχει ένα μηχανισμό για ανίχνευση της επέμβασης στις πληροφορίες από έναν εισβολέα.

Λειτουργία του SSL

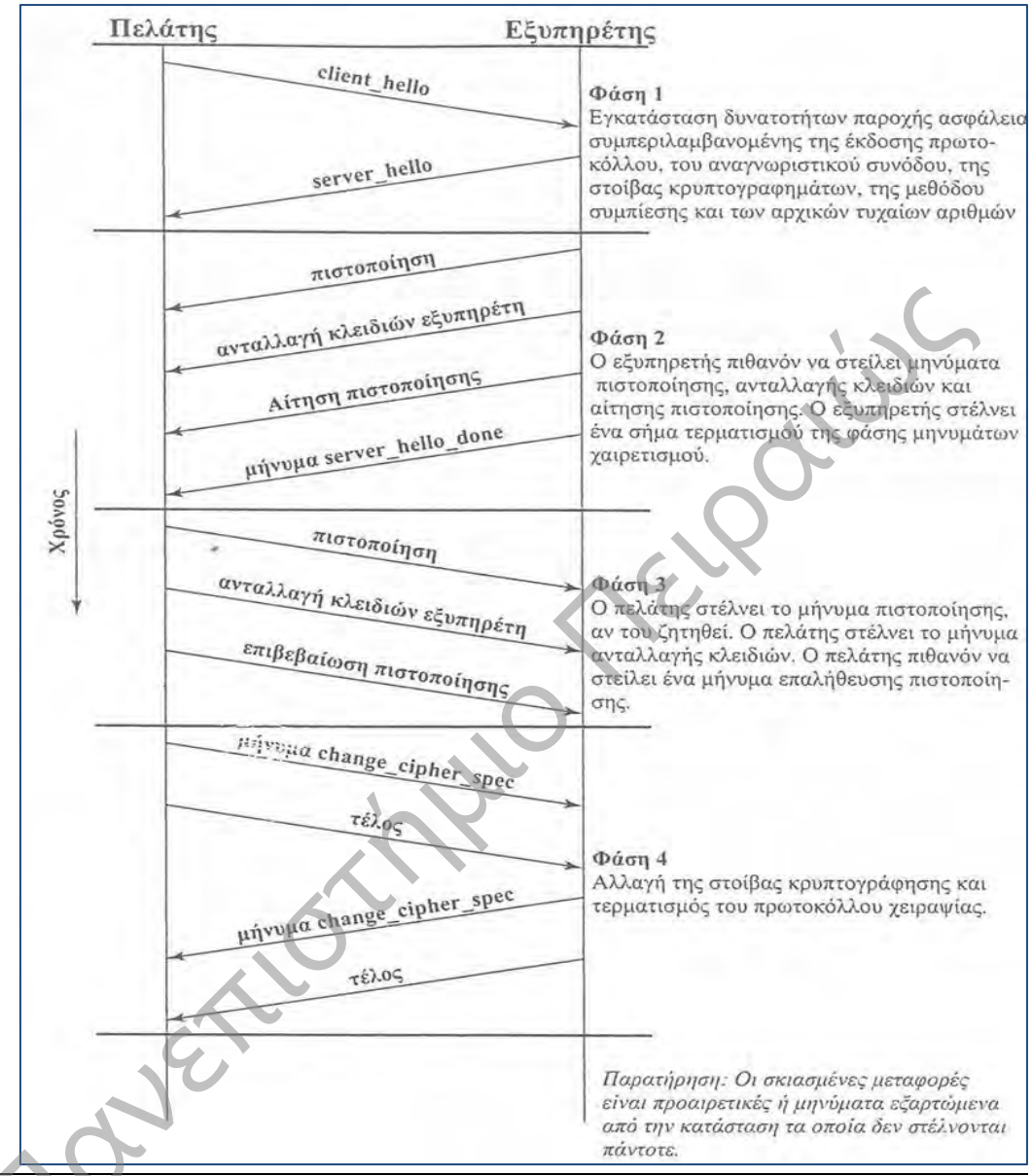
Για γίνει πιο κατανοητή η λειτουργία του πρωτοκόλλου SSL θα περιγραφεί ένα παράδειγμα επικοινωνίας του χρήστη **A** και ενός εξυπηρετητή **B**.

- Ο χρήστης **A** κάνει μια περιήγηση στο Web και κάνει κλικ σε μια σύνδεση, που τον μεταφέρει σε μια ασφαλή σελίδα, η οποία βρίσκεται μέσα στον εξυπηρετητή με δυνατότητες SSL του B.
- Το τμήμα πρωτοκόλλου του URL για αυτή τη σελίδα είναι "https" και όχι το γνωστό "http".
- Το πρόγραμμα περιήγησης και ο εξυπηρετητής εκτελούν κατόπιν το πρωτόκολλο χειραψίας SSL, το οποίο α) πιστοποιεί τον εξυπηρετητή και β) παράγει ένα διαμοιρασμένο συμμετρικό κλειδί. Και οι δύο αυτές εργασίες χρησιμοποιούν την τεχνολογία δημόσιου κλειδιού RSA. Κατά την διάρκεια αυτής της φάσης, ο **B** στέλνει στον **A** το πιστοποιητικό του, από το οποίο ο **A** παίρνει το δημόσιο κλειδί του B. Ο A κατόπιν δημιουργεί ένα τυχαίο συμμετρικό κλειδί, το κρυπτογραφεί με το δημόσιο κλειδί του **B** και του στέλνει το κρυπτογραφημένο κλειδί του. Ο **A** και ο **B** μοιράζονται τώρα ένα συμμετρικό κλειδί συνόδου.
- Όταν ολοκληρωθεί το πρωτόκολλο χειραψίας, όλα τα δεδομένα που στέλνονται ανάμεσα στο πρόγραμμα περιήγησης και στον εξυπηρετητή (επάνω σε συνδέσεις TCP) κρυπτογραφούνται χρησιμοποιώντας το συμμετρικό κλειδί συνόδου.

Άρα λοιπόν η χειραψία SSL εκτελεί τα παρακάτω βήματα:

1. Το πρόγραμμα περιήγησης στέλνει στον εξυπηρετητή τον αριθμό έκδοσης SSL και τις προτιμήσεις κρυπτογράφησης του προγράμματος περιήγησης επειδή αυτό και ο εξυπηρετητής διαπραγματεύονται τον αλγόριθμο συμμετρικού κλειδιού που πρόκειται να χρησιμοποιήσουν.
2. Ο εξυπηρετητής από την δική του την πλευρά στέλνει στο πρόγραμμα περιήγησης τον αριθμό έκδοσης SSL, τις προτιμήσεις κρυπτογράφησης και το πιστοποιητικό του.
3. Το πρόγραμμα περιήγησης έχει μια λίστα έμπιστων CA και ένα δημόσιο κλειδί για κάθε CA μέσα στη λίστα. Όταν το πρόγραμμα περιήγησης δεχθεί το πιστοποιητικό από τον εξυπηρετητή, ελέγχει για να δει αν η CA βρίσκεται μέσα στη λίστα.
   - Αν όχι, ο χρήστης προειδοποιείται για το πρόβλημα και πληροφορείται ότι δεν μπορεί να καθορισθεί μια κρυπτογραφημένη και πιστοποιημένη σύνδεση.
   - Αν η CA βρίσκεται στην λίστα, το πρόγραμμα περιήγησης χρησιμοποιεί το δημόσιο κλειδί της CA για να επαληθεύσει το πιστοποιητικό και να πάρει το δημόσιο κλειδί του εξυπηρετητή.
4. Το πρόγραμμα περιήγησης παράγει ένα συμμετρικό κλειδί συνόδου, το κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρετητή και στέλνει το κρυπτογραφημένο κλειδί συνόδου στον εξυπηρετητή.
5. Το πρόγραμμα περιήγησης και ο εξυπηρετητής στέλνουν μήνυμα αντίστοιχα, πληροφορώντας, ότι μελλοντικά μηνύματα μεταξύ τους θα κρυπτογραφούνται με το κλειδί συνόδου. Κατόπιν στέλνει ένα ξεχωριστό (κρυπτογραφημένο) μήνυμα, που δηλώνει ότι το τμήμα της χειραψίας έχει τελειώσει.
6. Η χειραψία SSL τώρα ολοκληρώθηκε και άρχισε η σύνοδος SSL. Το πρόγραμμα περιήγησης και ο εξυπηρετητής χρησιμοποιούν τα κλειδιά συνόδου για να κρυπτογραφήσουν και να αποκρυπτογραφήσουν τα δεδομένα που στέλνουν μεταξύ τους και για να επιβεβαιώσουν την ακεραιότητά τους. (Stallings, 2011) (Kurose&Ross, 2008)

Η παρακάτω εικόνα δείχνει την λειτουργία της χειραψίας του πρωτοκόλλου SSL.



Εικόνα 51: «Λειτουργία της χειραψίας SSL» πηγή εικόνας: (Stallings, 2011)

5 ΥΛΟΠΟΙΗΣΗ

Στην παρούσα εργασία επιλέχθηκε να χρησιμοποιηθεί εγκατάσταση και παραμετροποίηση του hMailServer e-mail server συμβατός με τα Microsoft Windows.

5.1 Επισκοπηση

Ο hMailServer είναι ένας e-mail server για τα Microsoft Windows. Σας επιτρέπει να χειριστείτε μόνοι σας όλα τα email σας χωρίς να χρειάζεται να βασίζεστε στην υπηρεσία παροχής Internet (ISP) για τη διαχείριση. Ο hMailServer προσφέρει ευελιξία και ασφάλεια και σας δίνει πλήρη έλεγχο για προστασία από τα spam.

5.1.1 Ιστορια

Το έργο του hMailServer ξεκίνησε στα τέλη του 2002 από τον Martin Knafve. Από τότε, έχει γίνει ένας από τους πιο δημοφιλής διακομιστές e-mail για τα Windows. Ο στόχος ήταν από την αρχή, να δημιουργήσουν ένα εύκολο στη χρήση σύστημα ηλεκτρονικού ταχυδρομείου που περιλαμβάνει όλα τα βασικά χαρακτηριστικά. Το έργο ξεκίνησε στην SourceForge.net, αλλά αργότερα μεταφέρθηκε σε ιστοσελίδα. Ο hMailServer είναι δωρεάν, και ο καθένας μπορεί να έχει πρόσβαση στον πηγαίο κώδικα μέσω της NovellForge της Novell και συγκεκριμένα στην ιστοσελίδα: https://www.novell.com/developer/redirect.html.

5.1.2 Πρωτοκολλα που χρησιμοποιει

Τα πρωτόκολλα που χρησιμοποιεί ο **hMailServer** για την παράδοση της αλληλογραφίας είναι τα γνωστά από το **TCP / IP** και συγκεκριμένα τα **SMTP, POP**3 και **IMAP**.

5.1.3 Επισκοπηση Λειτουργιας hMailServer

Ας υποθέσουμε ότι χρησιμοποιείτε τον hMailServer ως διακομιστή email σας για να στείλετε ένα email στη διεύθυνση: ***bill@microsoft.com***.

- Κάντε κλικ στο κουμπί **Αποστολή** στο πρόγραμμα-πελάτη ηλεκτρονικού ταχυδρομείου σας, για παράδειγμα, το Outlook Express.
- Το Outlook Express παραδίδει το μήνυμα στον hMailServer χρησιμοποιώντας το πρωτόκολλο **SMTP**.
- Ο hMailServer παραδίδει το μήνυμα ηλεκτρονικού ταχυδρομείου στο διακομιστή ηλεκτρονικού ταχυδρομείου της Microsoft, **mail.microsoft.com**, χρησιμοποιώντας **SMTP**.
- Το Mozilla Mail client του Bill κάνει λήψη του e-mail από το mail.microsoft.com στο φορητό υπολογιστή του χρησιμοποιώντας το πρωτόκολλο POP3 (ή IMAP).

5.1.4 Απαιτησεις Συστηματος

Ο hMailServer μπορεί να εγκατασταθεί στα παρακάτω λειτουργικά συστήματα. Το τελευταίο διαθέσιμο service pack των Windows θα πρέπει να έχει εγκατασταθεί. Ο hMailServer έχει δοκιμαστεί μόνο για τα ακόλουθα λειτουργικά συστήματα. Ο hMailServer μπορεί να

λειτουργήσει και σε άλλες εκδόσεις του λειτουργικού συστήματος, αλλά μόνο στις παρακάτω εκδόσεις έχουν επίσημα και επιτυχώς δοκιμαστεί. Εδώ θα αναφερθούν μόνο για την έκδοση hMailServer 5 διότι αυτή και θα γίνει εγκατάσταση:

Για την έκδοση hMailServer 5.4:

- Microsoft Windows 2008 (όλες οι εκδόσεις, εκτός από την Core)
- Microsoft Windows Vista
- Microsoft Windows 2003 (όλες οι εκδόσεις)
- Microsoft Windows XP Professional
- Microsoft Windows 2000 (όλες οι εκδόσεις)

5.1.5 Επιλεγοντας Βαση Δεδομενων

Ο hMailServer υποστηρίζει τις παρακάτω εκδόσεις βάσεων δεδομένων:

- Microsoft SQL Server 2000 and later
- Microsoft SQL Server Compact Edition (CE)
- MySQL 4 και μεταγενέστερη έκδοση
- PostgreSQL

Εάν πρόκειται να εγκαταστήσετε μια εμπορικού περιεχομένου υπηρεσία, θα πρέπει να επιλέξετε έναν από τους παρακάτω servers:

- Microsoft SQL Server 2000 ή και μεταγενέστερη έκδοση
- MySQL

Η Microsoft SQL Server Compact Edition δεν μπορεί να συνδυαστεί με υπηρεσίες διαφημιστικού τύπου. Το μεγαλύτερο όφελος με τον SQL Server Compact Edition είναι η μικρή μνήμη και χώρο στο δίσκο και το γεγονός ότι δεν απαιτεί κάποιο εξωτερικό λογισμικό για να τρέξει στον υπολογιστή. Ο μηχανισμός διαχείρισης βάσεων δεδομένων που λειτουργεί στο εσωτερικό του hMailServer σημαίνει ότι η λειτουργία του hMailServer δεν εξαρτάται από εξωτερικούς μηχανισμούς βάσεων δεδομένων. Οι προηγούμενες εκδόσεις του hMailServer (4 και άνω) περιλαμβάνουν την MySQL, αλλά αυτό άλλαξε σε MSSQL CE στην έκδοση 5.

Τα μειονεκτήματα με την προεπιλεγμένη βάση δεδομένων όμως είναι ότι μπορεί να χρησιμοποιηθεί μόνο για ιδιωτική χρήση και όχι για εμπορικά περιβάλλοντα. Η Microsoft SQL Server Compact Edition που εμπεριέχεται με τον hMailServer περιορίζεται σε 4GB. Αν επιθυμείτε ότι η εγκατάσταση του hMailServer να εξυπηρετήσει εκατοντάδες ή χιλιάδες μηνύματα ηλεκτρονικού ταχυδρομείου ή πολλούς λογαριασμούς συνιστάται να επιλέξετε το Microsoft SQL Server ή την MySQL. Μια MSSQL CE βάση δεδομένων των 4GB μπορεί να κρατήσει αναφορές σε περίπου 10 εκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου. Δοκιμές έδειξαν ότι η MSSQL CE είναι πιο αργή από άλλες βάσεις δεδομένων. Επίσης, υπάρχουν μερικά εργαλεία διαθέσιμα εάν η βάση δεδομένων SQL CE καταστραφεί, για παράδειγμα, σε μία αστοχία υλικού ή μια κατάρρευση του συστήματος.

Για την συγκεκριμένη εγκατάσταση δεν θα χρησιμοποιήσουμε κάποια εξωτερική βάση αλλά θα γίνει χρήση της βάσης που εμπεριέχεται ήδη στον hMailServer.

5.2 ΕΓΚΑΤΑΣΤΑΣΗ HMAILSERVER

5.2.1 Οδηγος Εγκαταστασης

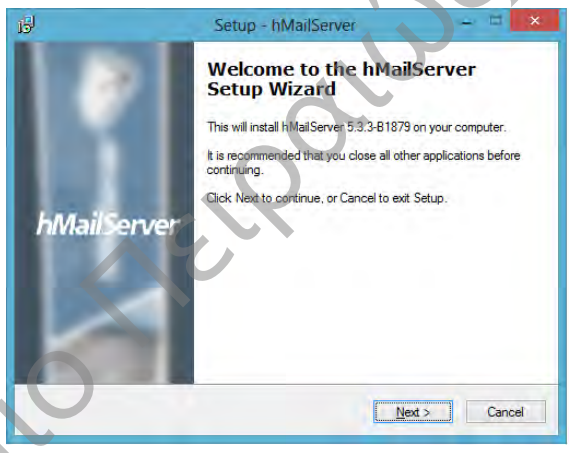
Σε αυτό το σημείο θα περιγράφει η διαδικασία για την εγκατάσταση του **hMailServer5**. Πριν από την εγκατάσταση του hMailServer, θα πρέπει να βεβαιωθείτε ότι ο υπολογιστής σας πληροί τις απαιτήσεις συστήματος που προαναφέρθηκαν.

- **1ο Βήμα: Λήψη**

Το πρώτο βήμα είναι να κατεβάσετε hMailServer. Το πρόγραμμα εγκατάστασης είναι διαθέσιμο για download στην επίσημη σελίδα του hMailServer: http://www.hmailserver.com/index.php?page=download. Συνιστάται να κατεβάσετε την τελευταία σταθερή έκδοση. Το αρχείο που κατεβάζετε έχει ένα όνομα της μορφής **hMailServer έκδοση-build.exe.**

- **2ο Βήμα: Εγκατάσταση**

a) Κάντε διπλό κλικ στο αρχείο για να ξεκινήσει η εγκατάσταση. Το πρώτο παράθυρο διαλόγου που εμφανίζεται στην χχχχ εικόνα και σε αυτό απλά κάντε κλικ στο κουμπί Next.



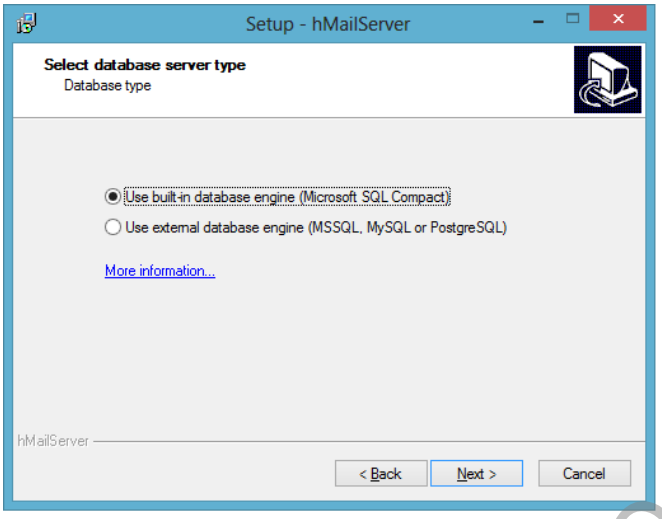
Εικόνα 52: «Οδηγός Εγκατάστασης hMailServer»

b) Το επόμενο βήμα είναι να διαβάσετε την άδεια χρήσης. Αν δεν αποδέχεστε την άδεια χρήσης, ακυρώστε την εγκατάσταση. Εάν συμφωνείτε, επιλέξτε "**Αποδέχομαι**" και κάντε κλικ στο επόμενο.

c) Επιλέξτε το φάκελο προορισμού και κάντε κλικ στο κουμπί **Next**. Θα πρέπει να επιλέξετε μια τοπική μονάδα δίσκου και όχι ένα φάκελο δικτύου. Είναι δυνατόν να εγκαταστήσετε hMailServer σε αφαιρούμενες συσκευές, αλλά δεν θα είναι σε θέση να τρέξει hMailServer από τη συσκευή σε έναν άλλον υπολογιστή.

d) Επιλέξτε ποια στοιχεία θέλετε να εγκαταστήσετε και κάντε κλικ στο **Next**. Επάνω στο server, θα πρέπει να εγκαταστήσετε όλα τα διαθέσιμα στοιχεία. Εάν έχετε ήδη εγκαταστήσει το hMailServer σε έναν άλλο υπολογιστή, το μόνο που χρειάζεται να εγκαταστήσετε είναι τα Administrative tools.

e) Επιλέξτε τύπο Βάσης Δεδομένων που θα εγκαταστήσετε μαζί με το hMailServer σύμφωνα με τις απαιτήσεις που έχετε από έναν mail server π.χ. εξυπηρέτηση εκατοντάδων χρηστών κ.τ.λ. όπως αυτές που έχουν αναφερθεί στην ενότητα «Επιλογή Βάσης Δεδομένων». Στην συγκεκριμένη περίπτωση επιλέγουμε τον Microsoft SQL Compact που εμπεριέχεται με τον hMailServer καθώς η εγκατάσταση προορίζεται για μόνο για ιδιωτική χρήση και όχι για εμπορικά περιβάλλοντα και δεν απαιτεί ιδιαίτερα μεγάλη μνήμη παρά μόνο 4GB.



Εικόνα 53: «Επιλογή Βάσης»

f) Επιλέξτε το φάκελο εκκίνησης που θέλετε να τοποθετηθούν τα εικονίδια του hMailServer και κάντε κλικ στο Next.

g) Επιβεβαιώστε ότι οι ρυθμίσεις είναι σωστές και στη συνέχεια κάντε κλικ στο κουμπί **Εγκατάσταση** για να κάνει την εγκατάσταση.

h) Περιμένετε ...
Η εγκατάσταση θα διαρκέσει περίπου 10-20 δευτερόλεπτα.

i) Όταν τα αρχεία εγκατασταθούν, θα πρέπει να δώσετε στο πρόγραμμα εγκατάστασης έναν **κύριο κωδικό πρόσβασης** για τον hMailServer. Από την έκδοση 4.3 και μετά, ο κωδικός πρόσβασης χρησιμοποιείται για την αύξηση της ασφάλειας. Ο κωδικός πρόσβασης μπορεί να είναι οτιδήποτε, αρκεί να είναι μεγαλύτερο από 5 χαρακτήρες. Θα χρειαστείτε τον κωδικό πρόσβασης αργότερα στην διαχείριση του server. Θα πρέπει να καθορίσετε κωδικό πρόσβασης την πρώτη φορά που γίνεται εγκατάσταση του hMailServer.

j) Μόλις ολοκληρωθεί η διαδικασία θα εμφανιστεί το παράθυρου επιτυχούς εγκατάστασης.

➢ **3ο Βήμα: Ρύθμιση DNS υπηρεσίας**

Μετά την εγκατάσταση hMailServer, θα πρέπει να ρυθμιστή ο διακομιστής DNS . Για να λειτουργήσει ο SMTP, θα πρέπει να οριστούν οι εγγραφές MX για τον τομέα.

5.2.2 Σενάρια εγκατάστασης

Υπάρχουν 2 περιπτώσεις ρύθμισης του hMailServer για να επικοινωνεί με τους άλλους server και για να μπορέσει να επικοινωνήσει αποτελεσματικά με το δίκτυο:

a. Με δυναμική IP και
b. Με στατική IP

Στην συγκεκριμένη διατριβή ο email server θα ρυθμιστεί να λειτουργεί σε ένα τοπικό δίκτυο όποτε δεν θα χρειαστεί ούτε MX records ούτε ρυθμίσεις για IP.

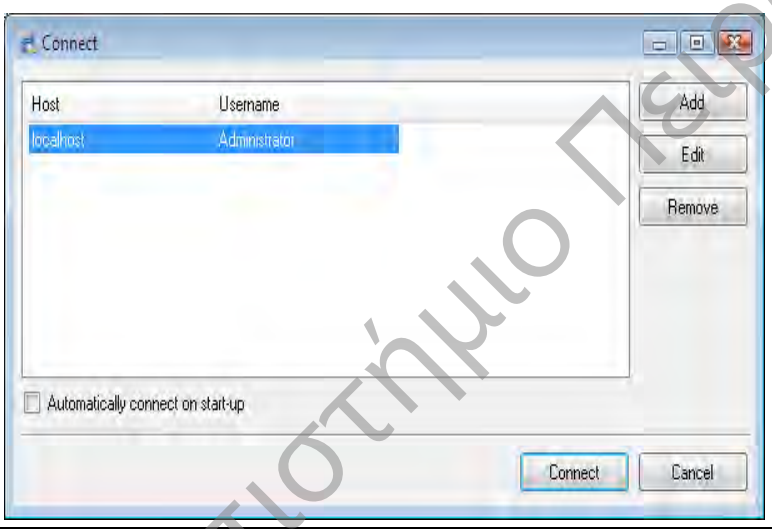
(hMailServer)

5.2.3 Ρυθμιση Τοπικου Email Server

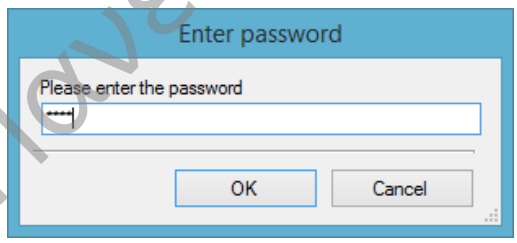
Αφού ολοκληρωθεί η εγκατάσταση, στην συνέχεια γίνεται εκκίνηση του hMailServer διαχειριστή. Το πρώτο πράγμα που φαίνεται είναι το παράθυρο σύνδεσης. Αυτό το παράθυρο διαλόγου επιτρέπει στον χρήστη να συνδεθεί με διαφορετικές εγκαταστάσεις hMailServer στο δίκτυό.

I. **Δημιουργία Domain Name**

a) Επιλέγουμε την προεγκατεστημένη σύνδεση **localhost**, και πατάμε **Connect**. Στο παράθυρο διαλόγου πρέπει να εισαχθεί ο κωδικός πρόσβασης που χρησιμοποιήθηκε κατά την εγκατάσταση του hMailServer

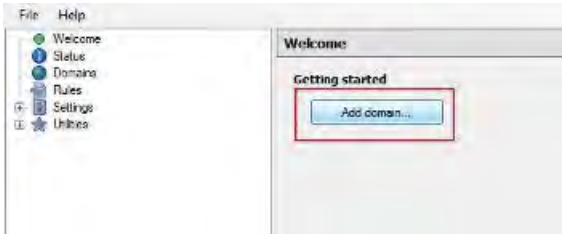


Εικόνα 54: «Σύνδεση με τον localhost»



Εικόνα 55: «Εισαγωγή password»

b) Αφού υποβάλετε τον κωδικό πρόσβασής, ο hMailServer διαχειριστής θα ανοίξει. Επιλέγουμε το κουμπί " **Add Domain** " για να προσθέσουμε και να δώσουμε όνομα domain .



Εικόνα 56: «Add Domain»

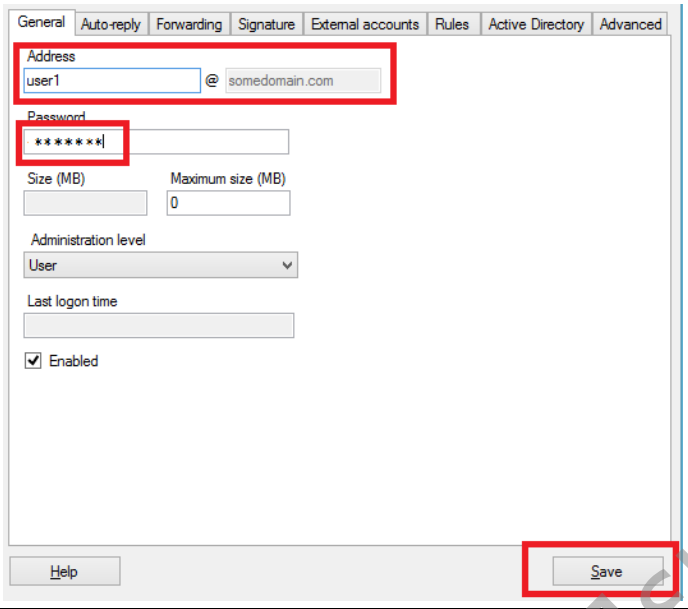
c) Πληκτρολογούμε το όνομα τομέα, συγκεκριμένα θα χρησιμοποιήσουμε το όνομα: "**somedomain.com**" στο πλαίσιο κειμένου τομέα και επιλέγουμε " **Save** ".

Εικόνα 57: «Δημιουργία Domain»

II. Δημιουργία Λογαριασμών Χρηστών

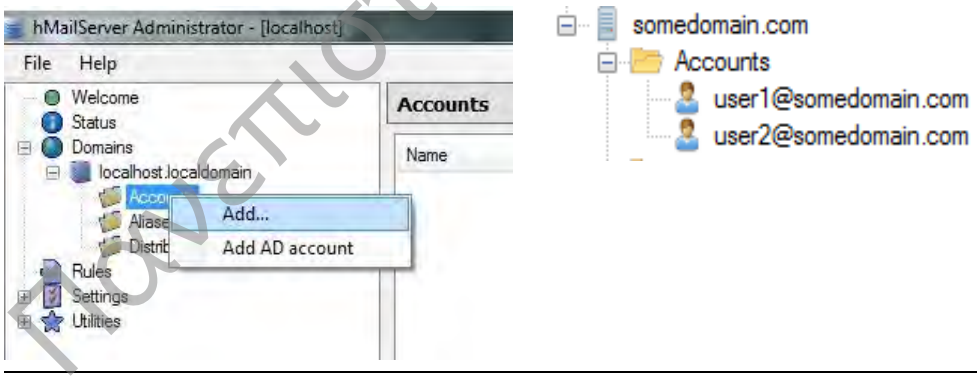
Αφού δημιουργήσουμε το domain name του email server, κάτω από την περιοχή Domains εμφανίζεται το νέο τομέα. Στην συνέχεια θα προσθέσουμε λογαριασμούς χρηστών.

a) Κάνοντας δεξί κλικ στο εικονίδιο "**Accounts**" στο υπομενού του domain μας και επιλέγοντας " **Add**...".



Εικόνα 58: «Καρτέλα Χρήστη»

b) Εμφανίζεται η καρτέλα με τα στοιχεία του λογαριασμού, όπου πληκτρολογούμε το όνομα για το λογαριασμό email και έναν κωδικό πρόσβασης για αυτό το χρήστη και πατάμε "**Save**". Ο νέος λογαριασμός θα φανεί στο υπομενού του εικονιδίου "**Accounts**".Με αυτό το τρόπο δημιουργούμε 2 λογαριασμούς user1@somedomain.com και user2@somedomain.com όπως απεικονίζονται παρακάτω:



Εικόνα 59: «Λογαριασμοί Χρηστών»

III. Ρύθμιση DNS υπηρεσίας για το email server

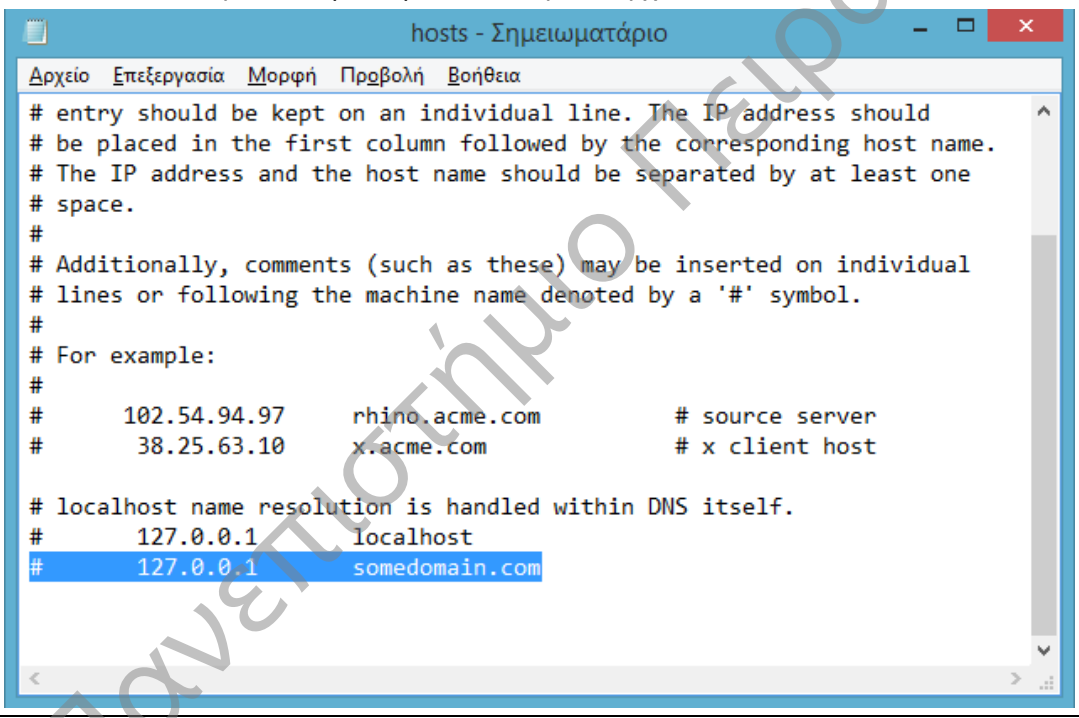
Εκ των προτέρων ο υπολογιστής όταν στο brower του εισάγεται κάπιο url π.χ. Gmail.com ελέγχει το αρχείο **host** που βρίσκεται στην διεύθυνση: **C:\Windows\System32\drivers\etc** μέσα στον υπολογιστή, το οποίο είναι υπεύθυνο για την αντιστοίχιση των IP με τα hostname.

Στην περίπτωση εγκατάστασης ενός τοπικού email server θα πρέπει να προστεθεί η IP με το hostname που έχουμε δώσει στον email server. Αυτό γίνεται ως εξής:

Μεταβαίνουμε στην παραπάνω τοποθεσία μέσα στον υπολογιστή και επιλέγουμε «**Επεξεργασία**» του αρχείου host και στο τέλος του κειμένου προσθέτουμε την παρακάτω γραμμή κώδικα:

```
#      127.0.0.1       somedomain.com
```

Πατάμε Αποθήκευση και κλείνουμε το αρχείο.



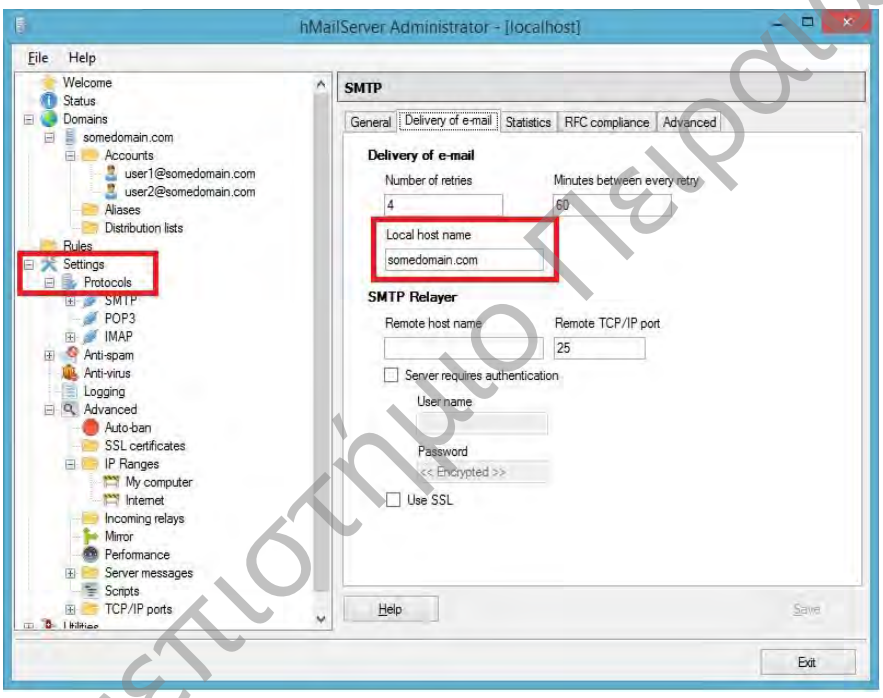
Εικόνα 60: «Αρχείο host»

Αυτό θα μας χρειαστεί αργότερα στη ρύθμιση των email clients για να «βλέπουν» το διακομιστή εξερχόμενων μηνυμάτων που θα παραδώσουν την αλληλογραφία.

IV. Ρύθμιση Επιλογών Παράδοσης SMTP του email

Στην συνέχεια αφού οι νέοι λογαριασμοί έχουν αποθηκευτεί θα ρυθμίσουμε τις επιλογές παράδοσης του **SMTP**. Όπως προείπαμε πρόκειται για ένα τοπικό email server οπότε αφού συμπληρώσουμε το όνομα του domain, στο πεδίο των IP θα υπάρχει η IP του υπολογιστή που θα στηθεί ο server και η Internet IP. Αυτό γίνεται ως εξής:

- Στην περιοχή "**Settings"** επιλέγουμε **"Protocols"** και στο υπομενού **SMTP**. Στο παράθυρο του **SMTP** επιλέγουμε την καρτέλα "**Delivery of email"**. Εισάγουμε το όνομα " **somedomain.com** " στην περιοχή ***Local host name*** και πατάμε **save**.



Εικόνα 61: «Καρτέλα SMTP»

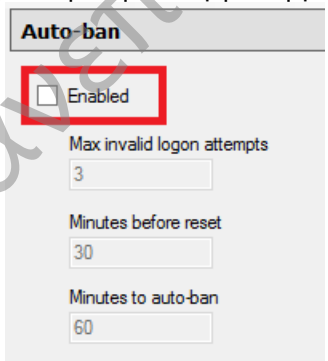
IV. Προαιρετικές ρυθμίσεις

Εδώ θα παραθέσουμε κάποιες πρόσθετες ρυθμίσεις που είναι προαιρετικές και στην περίπτωση που δεν πραγματοποιηθούν η εγκατάσταση θα είναι και πάλι επιτυχής.

- **Welcome μήνυμα:** Στην καρτέλα "**General**" της περιοχής **Settings > Protocols** εάν επιθυμούμε μπορούμε να προσθέσουμε κάποιο Welcome μήνυμα. Συγκεκριμένα θα εισάγουμε το μήνυμα: **«Welcome to Dina's email server :-)»** το οποίο θα μας βοηθήσει στη συνέχεια στο τεστάρισμα της θύρας 25 του SMTP.

Εικόνα 62: «Welcome message»

a) **Κλείδωμα εισαγωγής λογαριασμού μετά από αποτυχημένες προσπάθειες:** Μπορείτε να ρυθμίσετε κλείδωμα κάποιου λογαριασμού για λόγους ασφαλείας εάν ο χρήστης αποτύχει μετά από ένα συγκεκριμένο αριθμό προσπαθειών που μπορεί να τροποποιηθεί στο πεδίο **"Max invalid logon attempts"** ή να απενεργοποιηθεί τελείως αυτή η λειτουργία εάν αποεπιλεχθεί η επιλογή "**Enabled**".Στην παρούσα εργασία έχει απενεργοποιηθεί η επιλογή αυτή για ευκολία.



Εικόνα 63: «Auto-Ban»

5.2.4 Εγκατασταση Mail User Agent

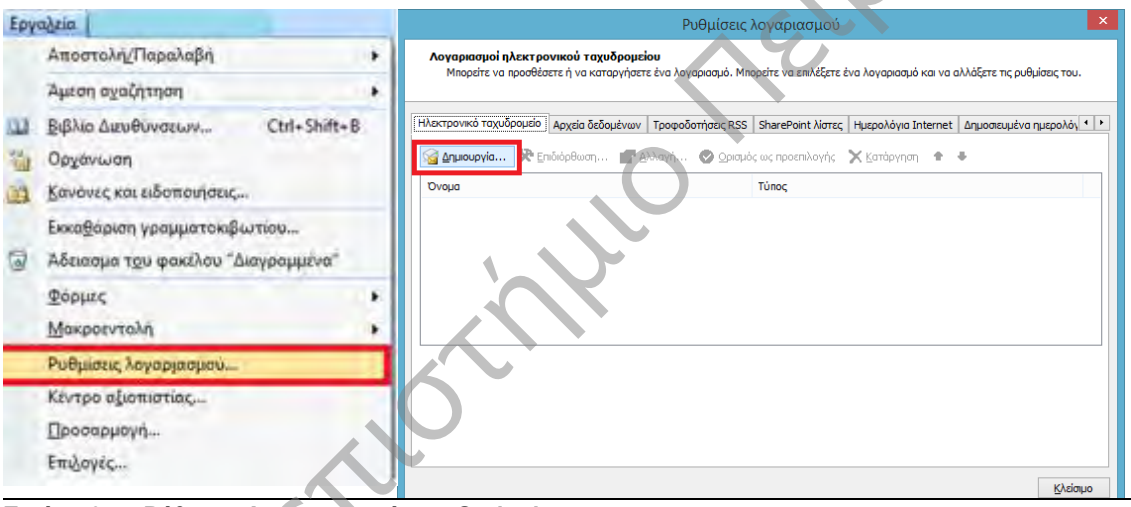
Αφού έχουμε κατεβάσει, εγκαταστήσει και ρυθμίσει τον hMailServer στην συνέχεια θα πρέπει να ρυθμίσουμε κάποιο MUA-Mail User Agent/ Email Client έτσι ώστε να επικοινωνεί με τον email server για παράδοση και αποστολή emails αλλά και να μας προσφέρει όλα τα εργαλεία γραφικού περιβάλλοντος για την σύνταξη ενός email. Ο συγκεκριμένος server έχει δοκιμαστεί σε όλους τους γνωστούς Email User Agents όπως: Mozilla Thunderbird, Outlook Express, Opera Mail και Microsoft Outlook και δουλεύει κανονικά.

Για να ελέγξουμε την ασφαλή επικοινωνία μεταξύ δύο χρηστών, στην συγκεκριμένη εργασία θα εγκαταστήσουμε και θα ρυθμίσουμε δύο Email Clients: τον Opera Mail και το Microsoft Outlook 2007 λόγω μικρής απαίτησης μνήμης και απλότητας στην χρήση τους.

Microsoft Outlook 2007

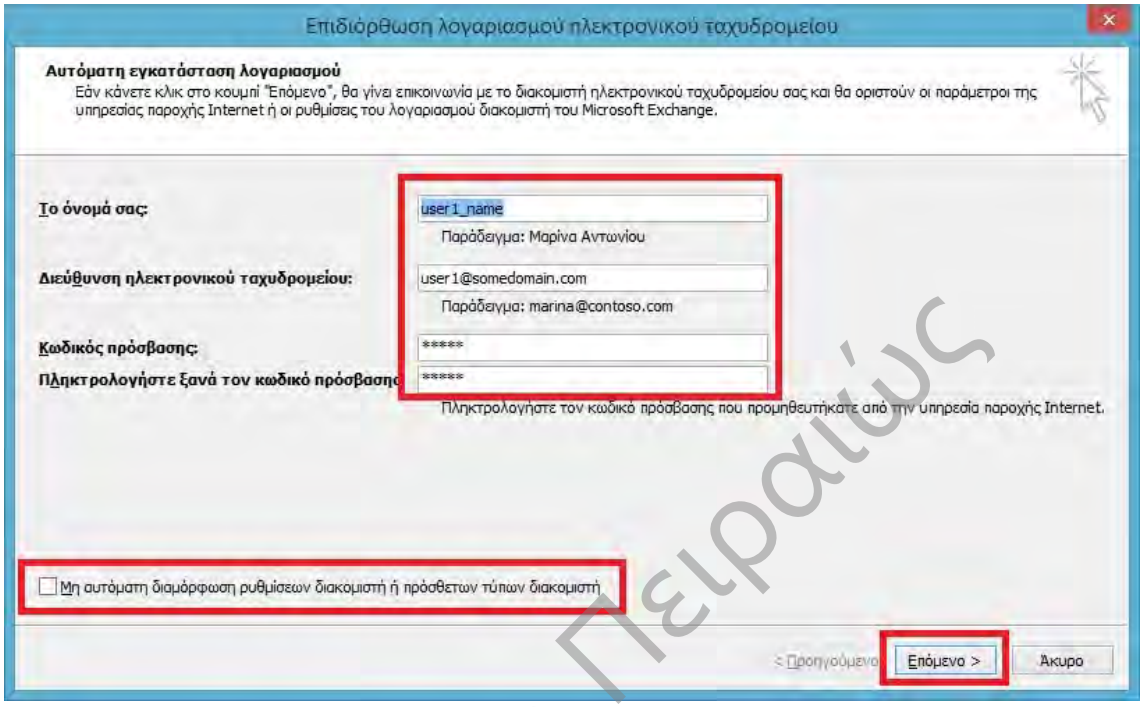
Στις περισσότερες περιπτώσεις έχοντας εγκαταστήσει κάποια version του Office Professional υπάρχει και ο Client της Microsoft για ηλεκτρονικό ταχυδρομείο, οπότε θα τον ρυθμίσουμε για το 1^{ο} λογαριασμό email που έχουμε δημιουργήσει ως εξής:

a) Έχοντας ανοίξει την εφαρμογή πάμε **Εργαλεία-tools > Account settings-Ρυθμίσεις Λογαριασμού.** Στο παράθυρο **Account settings** επιλέγουμε **Create-Δημιουργία**.



Εικόνα 64: «Ρύθμιση Λογαριασμού στο Outlook»

b) Στο παράθυρο “Add new Account- Δημιουργία Νέου Λογαριασμού”



Εικόνα 65: «Στοιχεία Λογαριασμού Outlook»

Opera Mail

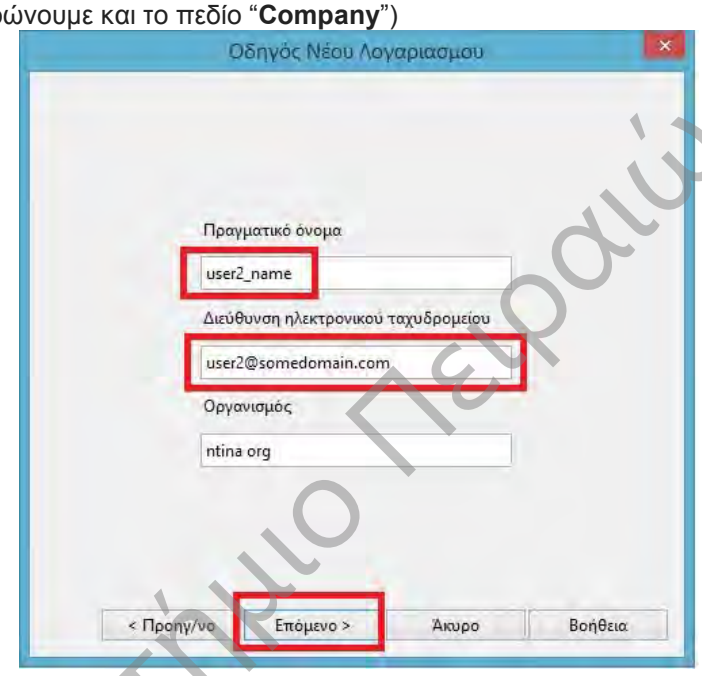
Έχοντας λοιπόν εγκαταστήσει τον Opera Mail όπου διατίθεται δωρεάν από την ιστοσελίδα της εταιρείας Opera Software πραγματοποιούμε τις εξής κινήσεις;

a) Εκκινώντας τον Opera σαν διαχειριστής επιλέγουμε **"Mail and Chat Accounts..."** από το μενού του Opera:

Εικόνα 66: «Opera Mail»

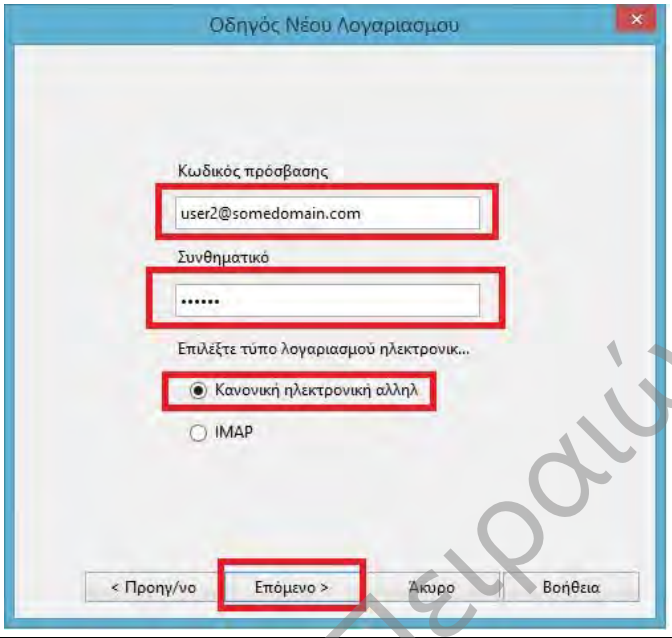
b) Επιλέγουμε “Email” από τη λίστα των επιλογών των λογαριασμών (account).

c) Εισάγουμε τα στοιχεία στα κατάλληλα πεδία. Δίνουμε ένα όνομα με το οποίο θέλουμε να φαίνεται ο λογαριασμός στο πεδίο **“Real Name-Πραγματικό όνομα”** εδώ δίνουμε **“user2_name”** και τη διεύθυνση email στο πεδίο **“Email address”**. Προσοχή θα πρέπει να ταιριάζει με αυτή που προστέθηκε στο hMailServer και πατάμε **Next**. (εάν θέλουμε συμπληρώνουμε και το πεδίο “**Company**”)



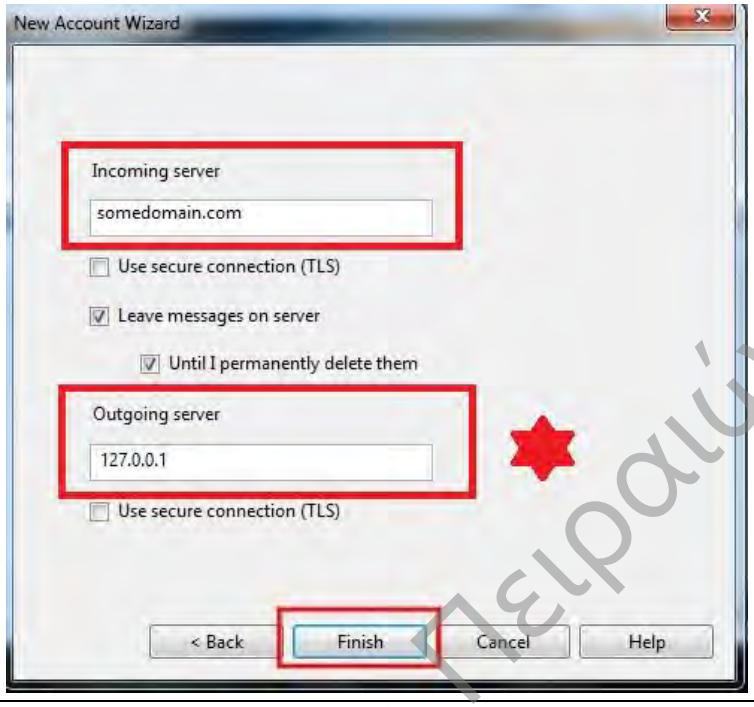
Εικόνα 67: «Ρύθμιση Λογαριασμού στο Opera 1»

d) Στην επόμενη καρτέλα που μας εμφανίζεται πληκτρολογούμε την πλήρη διεύθυνση ηλεκτρονικού ταχυδρομείου για το πεδίο **“login name”** και δίνουμε τον κωδικό πρόσβασης στο πεδίο “**password**” αυτόν που χρησιμοποιήσαμε κατά τη δημιουργία του λογαριασμού στον **hMailServer Administrator**, επιλέγουμε **‘”POP3 email-Κανονική ηλεκτρονική αλληλογραφία”** και πατάμε **Next**..



Εικόνα 68: «Ρύθμιση Λογαριασμού στο Opera 2»

e) Αυτό το βήμα είναι πολύ σημαντικό στη ρύθμιση και των δύο clients…..!!!!! Στην καρτέλα με τα στοιχεία για **incoming/outgoing server** θα πρέπει να εισάγουμε τα στοιχεία του διακομιστή που έχουμε δημιουργήσει . Οπότε στο πεδίο **incoming server** βάζουμε το όνομα του server δηλαδή **"somedomain.com"** και στο πεδίο **outgoing server** θα πρέπει να εισάγουμε την εξωτερική IP που χρησιμοποιεί ο τοπικός διακομιστής αλληλογραφίας διότι ο δρομολογητής δεν μπορεί να μεταφράσει το domain name για την κίνηση εντός του δικτύου, δηλαδή προσθέτουμε **127.0.0.1** και πατάτε "**Finish**".



Εικόνα 69: «Ρυθμίσεις Διακομιστή Εισερχομένων-Εξερχομένων»

Με το ίδιο τρόπο δημιουργούμε και τον άλλο λογαριασμό που δημιουργήσαμε στην αρχή.

5.3 Έλεγχος Σωστης Λειτουργιας Email Server

Σε αυτήν την ενότητα θα πραγματοποιηθούν κάποια test cases για να ελέξουμε τη σωστή λειτουργία του email server και τη ανταλλαγή μηνυμάτων. Τα test αυτά πραγματοποιούνται με το γραφικό περιβάλλον των Mail User Agents αλλά και με εντολές σε Command Prompt.

5.3.1 Test case 1: blocked Port 25

Test εάν ο ISP έχει μπλοκαρισμένη την πόρτα 25:

Ένας από τους πιο συνηθισμένους λόγους για τους οποίους δεν είναι σε θέση ο server να στείλει μηνύματα είναι ότι η **υπηρεσία παροχής Internet (ISP)** μπλοκάρει τη θύρα 25 την οποία χρησιμοποιεί το πρωτόκολλο **SMTP**. Πριν προχωρήσουμε λοιπόν παρακάτω θα πρέπει να τεστάρουμε εάν έχουμε ανοιχτή την πόρτα αυτή. Με βάση το Λειτουργικό Σύστημα που έχουμε στον υπολογιστή μας προχωρούμε στις παρακάτω ενέργειες:

Στην συγκεκριμένη περίπτωση διαθέτουμε τα **Windows 8**, άρα ανοίγουμε ένα **command prompt** και πληκτρολογούμε την εντολή ακριβώς:

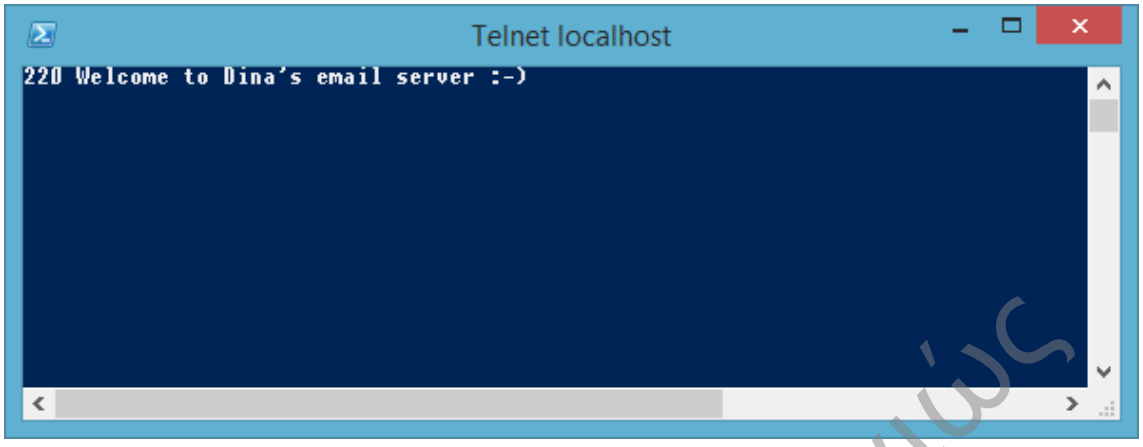
telnet localhost 25

Αξίζει εδώ να σημειωθεί ότι από την έκδοσή Windows Vista και μετά η υπηρεσία **telnet client** είναι απενεργοποιημένη λόγω ασφάλειας, οπότε από τον Πίνακα Ελέγχου θα πρέπει να την ενεργοποιήσουμε για να τρέξει η εντολή. Πληκτρολογώντας την εντολή και πατώντας Enter εάν συνδεθούμε η λάβουμε κάποιο μήνυμα παρόμοιο με τα παρακάτω δηλαδή μία απάντηση τύπου **220**:

220-serv01.siteground XXX.com ESMTP Exim 4.63 #1 Wed, 18 Apr 2008 07:17:30 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

Τότε σημαίνει ότι η πόρτα 25 δεν είναι μπλοκαρισμένη. Από την άλλη εάν πάρουμε μήνυμα σφάλμα σύνδεσης (connection error) ή καμία απάντηση τότε θα πρέπει να ακολουθήσουμε μια διαδικασία που θα ανοίξουμε η θα παρακάμψουμε την πόρτα 25.

Η απάντηση που λαμβάνουμε είναι η εξής:



Εικόνα 70: «Απάντηση server»

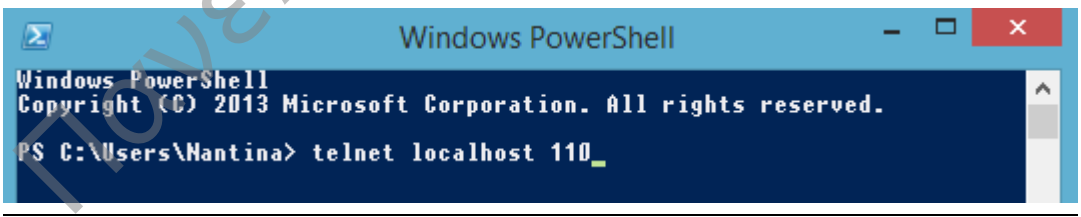
Όπου είναι απάντηση της μορφής 220 και μας εμφανίζεται και το μήνυμα που προσθέσαμε κατά τη ρύθμιση του hMailServer άρα η πόρτα 25 δεν είναι μπλοκαρισμένη.

(SMTP Port – How to Check if SMTP Port 25 is Blocked) (Dinesh, Install and Enable Telnet in Windows 8 & 8.1 – Use The Telnet Client Utility) (Checking your outgoing mail server (Is Port 25 blocked?))

5.3.2 Test case 2: Έλεγχος POP3

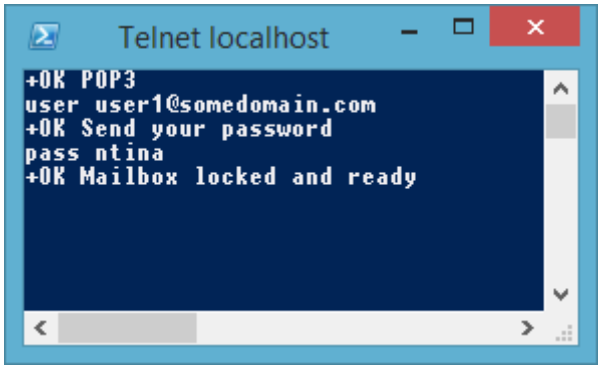
Σε αυτό το σημείο με τις εντολές του POP3 πρωτοκόλλου ανάκτησης email θα συνδεθούμε με το username και το password ενός από τους λογαριασμούς που δημιουργήσαμε. Για να γίνει η σύνδεση με το POP3 στο server θα πρέπει να συνδεθούμε με telnet στο όνομα του τοπικού server και στη συνέχεια στην προκαθορισμένη θύρα που ακούει στο TCP/IP το πρωτόκολλο POP3 δηλαδή την 110. Η σύνταξη της εντολής είναι:

```
Telnet < όνομα server > 110
```



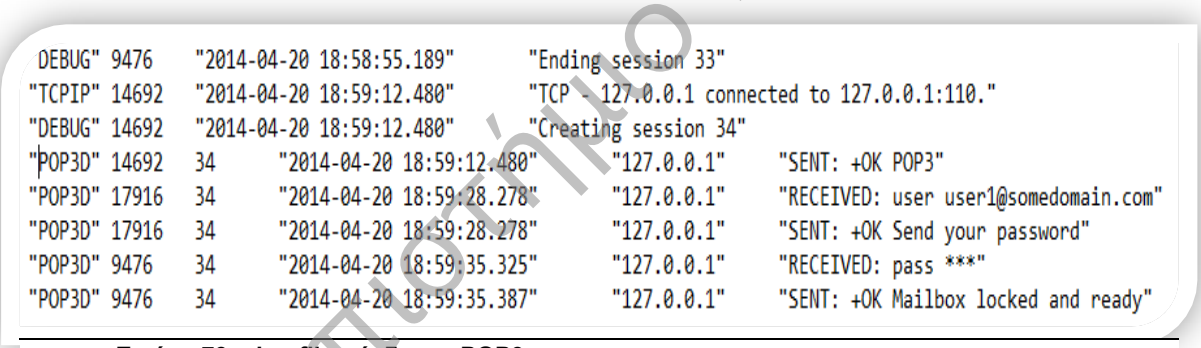
Εικόνα 71: «Telnet στην 110»

Μόλις πληκτρολογήσουμε την εντολή και πατήσουμε <Enter> μετά από μερικά δευτερόλεπτα μας απαντάει ο POP3 ότι είναι έτοιμός και ζητάει username και το password του χρήστη με το οποίο θέλουμε να συνδεθούμε για να φορτώσουμε στον υπολογιστή τα emails. Η σύνδεση όπως παρατηρούμε και από την παρακάτω εικόνα είναι επιτυχής:



Εικόνα 72: «Απάντηση POP3»

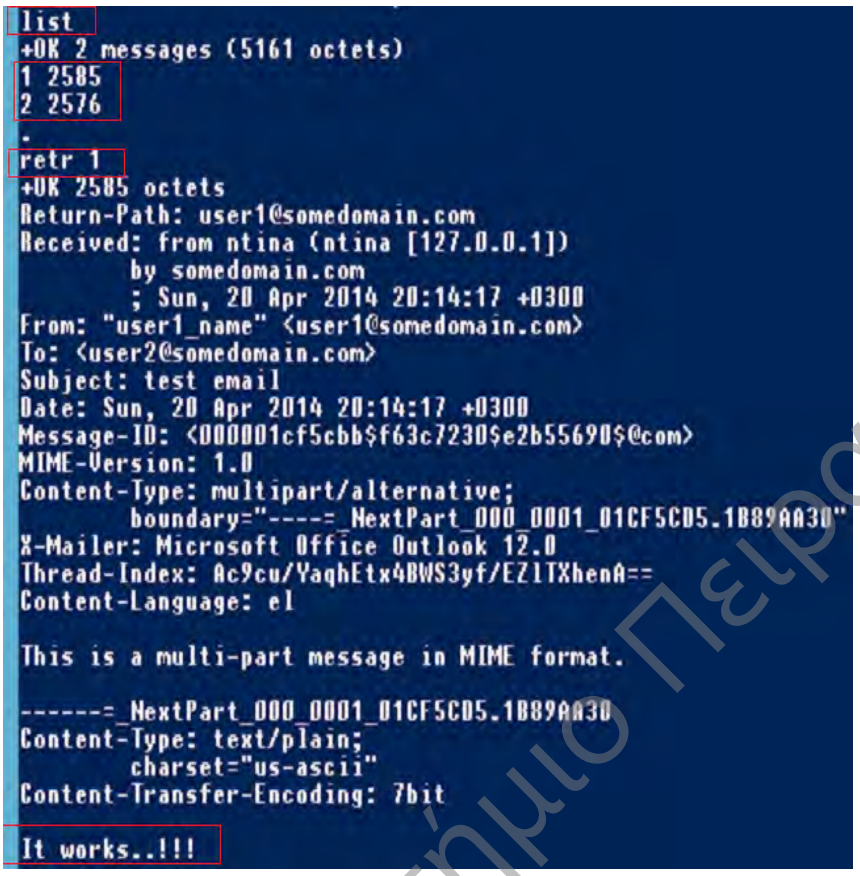
Ένας αλλός τρόπος με τον οποίο μπορούμε να τεστάρουμε τις επιτυχείς ή και αποτυχημένες συνδέσεις με τον server αλλά και να παίρνουμε όλες τις πληροφορίες για όλα τα προβλήματα που μπορεί να μας τύχουν είναι ο φάκελος των log που δημιουργείται κατά την εγκατάσταση του Hmailserver. Έτσι πηγαίνοντας στην διαδρομή C:\Program Files (x86)\hMailServer\Logs βρίσκουμε το log αρχείο που μας πληροφορεί για την επιτυχή σύνδεση μας στο λογαριασμό του χρήστη: user1@somedomain.com



```
DEBUG" 9476    "2014-04-20 18:58:55.189"      "Ending session 33"
"TCPIP" 14692  "2014-04-20 18:59:12.480"      "TCP - 127.0.0.1 connected to 127.0.0.1:110."
"DEBUG" 14692  "2014-04-20 18:59:12.480"      "Creating session 34"
"POP3D" 14692  34     "2014-04-20 18:59:12.480"     "127.0.0.1"     "SENT: +OK POP3"
"POP3D" 17916  34     "2014-04-20 18:59:28.278"     "127.0.0.1"     "RECEIVED: user user1@somedomain.com"
"POP3D" 17916  34     "2014-04-20 18:59:28.278"     "127.0.0.1"     "SENT: +OK Send your password"
"POP3D" 9476   34     "2014-04-20 18:59:35.325"     "127.0.0.1"     "RECEIVED: pass ***"
"POP3D" 9476   34     "2014-04-20 18:59:35.387"     "127.0.0.1"     "SENT: +OK Mailbox locked and ready"
```

Εικόνα 73: «log file σύνδεσης POP3»

Τέλος χρησιμοποιούμε τις εντολές **list** για να δούμε σε λίστα τα email που έχει ο χρήστης και την εντολή **retr** που ακολουθεί ένας αριθμός με το οποίο ανακτά ο χρήστης το email που με τη σειρά εμφανίζεται στη λίστα έτσι αν επιλέξουμε **retr 1** εμφανίζεται το πρώτο email κ.ο.κ. Στην παρακάτω εικόνα εμφανίζονται οι εντολές καθώς και ολόκληρο το μήνυμα.



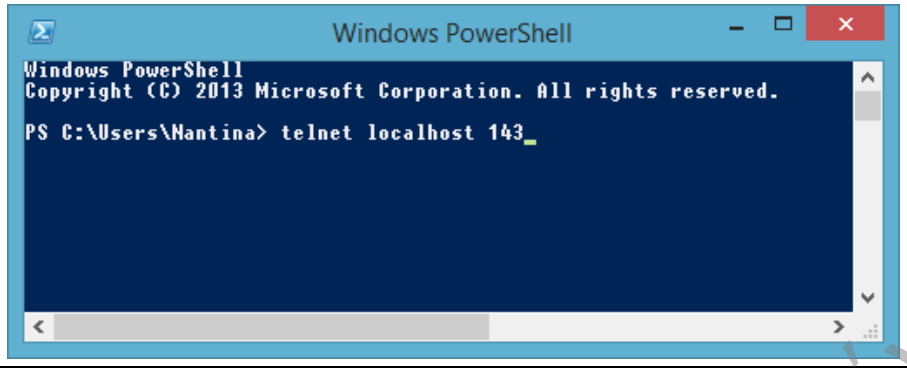
Εικόνα 74: «Εντολές list & retr »

5.3.3 Test case 3: Έλεγχος IMAP4

Την ίδια διαδικασία θα ακολουθήσουμε για να τεστάρουμε την σύνδεση και μέσω IMAP αλλά με διαφορετικές εντολές.

Πρώτα συνδεόμαστε με telenet στην θύρα που ακούει στο TCP/IP το πρωτόκολλο IMAP4 δηλαδή την 143. Η σύνταξη της εντολής είναι:

```
Telnet < όνομα server > 143
```



Εικόνα 75: «Telnet στην 143»

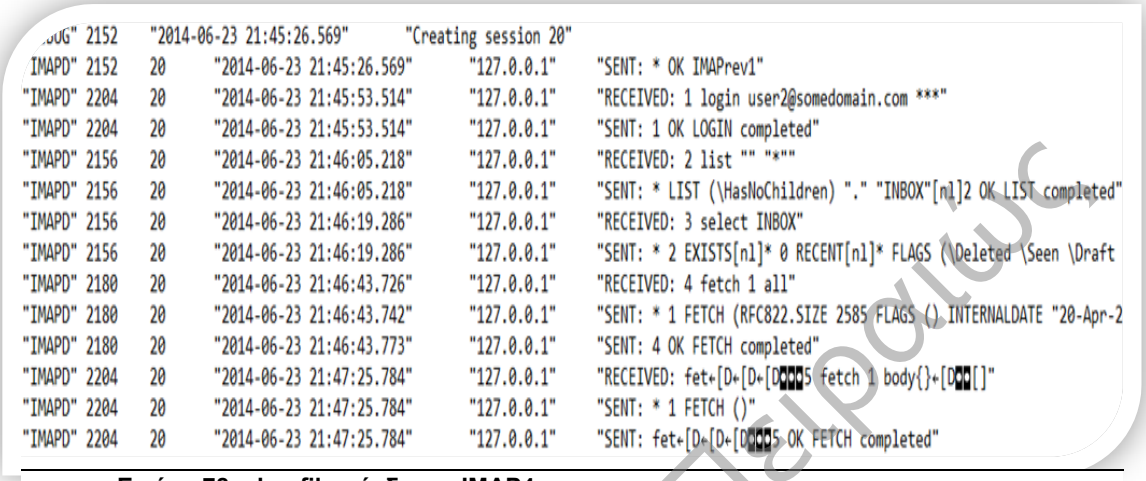
Στην συνέχεια θα δώσουμε τις εντολές του IMAP για να συνδεθούμε στο λογαριασμό του χρήστη. Αξιοσημείωτο είναι ότι οι εντολές του πρωτοκόλλου IMAP θα πρέπει να ξεκινάνε με έναν αύξων αριθμό και το IMAP απαντάει με το ίδιο αριθμό της εντολής. Παρατηρούμε ότι αφού γίνει η ταυτοποίηση του χρήστη με την εντολή :list μας δίνεται η δυνατότητα να δούμε τη δομή των φακέλων με την οποία ταξινομούνται τα μηνύματα μέσα στο server καθώς και τμήματα του μηνύματος π.χ. θέμα μηνύματος, δυνατότητες που δεν διαθέτει το POP3.

Εικόνα 76: «Απάντηση IMAP4»

Για να μπορέσουμε να ανακτήσουμε την αλληλογραφία του χρήστη πληκτρολογούμε την εντολή: **fetch** και από ποιο φάκελο να ανακτήσει το μήνυμα και όπως φαίνεται στην εικόνα XXXXX εμφανίζεται ολόκληρο το μήνυμα καθώς και όλες οι πληροφορίες. Τέλος αν θέλουμε να τερματίσουμε τη σύνδεση πληκτρολογούμε τον αύξοντα αριθμό και την εντολή: **LOGOUT**.

Εικόνα 77: «Φόρτωση μηνυμάτων με fetch»

Το log αρχείο μας πληροφορεί για την επιτυχή σύνδεση μας στο λογαριασμό του χρήστη: user2@somedomain.com



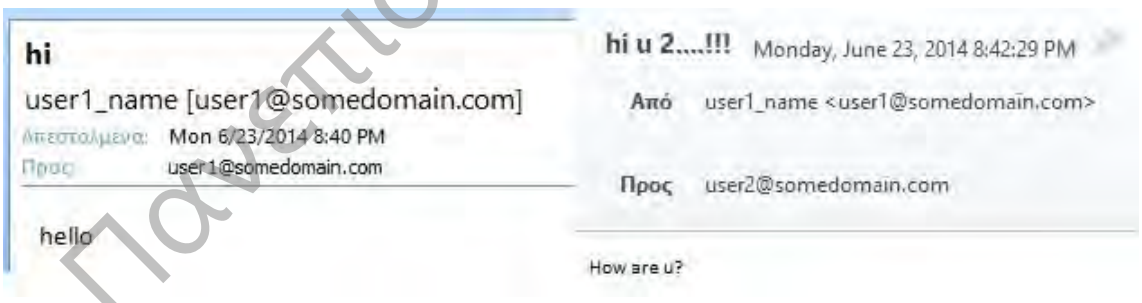
"IMAPD"	2152	20	"2014-06-23 21:45:26.569"	"127.0.0.1"	"SENT: * OK IMAPrev1"
"IMAPD"	2204	20	"2014-06-23 21:45:53.514"	"127.0.0.1"	"RECEIVED: 1 login user2@somedomain.com ***"
"IMAPD"	2204	20	"2014-06-23 21:45:53.514"	"127.0.0.1"	"SENT: 1 OK LOGIN completed"
"IMAPD"	2156	20	"2014-06-23 21:46:05.218"	"127.0.0.1"	"RECEIVED: 2 list "" "*""
"IMAPD"	2156	20	"2014-06-23 21:46:05.218"	"127.0.0.1"	"SENT: * LIST (\HasNoChildren) "." "INBOX"[nl]2 OK LIST completed"
"IMAPD"	2156	20	"2014-06-23 21:46:19.286"	"127.0.0.1"	"RECEIVED: 3 select INBOX"
"IMAPD"	2156	20	"2014-06-23 21:46:19.286"	"127.0.0.1"	"SENT: * 2 EXISTS[nl]* 0 RECENT[nl]* FLAGS (\Deleted \Seen \Draft
"IMAPD"	2180	20	"2014-06-23 21:46:43.726"	"127.0.0.1"	"RECEIVED: 4 fetch 1 all"
"IMAPD"	2180	20	"2014-06-23 21:46:43.742"	"127.0.0.1"	"SENT: * 1 FETCH (RFC822.SIZE 2585 FLAGS () INTERNALDATE "20-Apr-2
"IMAPD"	2180	20	"2014-06-23 21:46:43.773"	"127.0.0.1"	"SENT: 4 OK FETCH completed"
"IMAPD"	2204	20	"2014-06-23 21:47:25.784"	"127.0.0.1"	"RECEIVED: fet←[D←[D←[D[]5 fetch 1 body{}←[D[]"
"IMAPD"	2204	20	"2014-06-23 21:47:25.784"	"127.0.0.1"	"SENT: * 1 FETCH ()"
"IMAPD"	2204	20	"2014-06-23 21:47:25.784"	"127.0.0.1"	"SENT: fet←[D←[D←[D[]5 OK FETCH completed"

Εικόνα 78: «log file σύνδεσης IMAP4»

(Workaround.org)

5.3.4 Test case 4: Έλεγχος επικοινωνιας μεταξυ χρηστων

Σε αυτό το test θα επιχειρήσουμε κάτι πού απλό μέσω των δύο client να επικοινωνήσουν οι δύο χρήστες μεταξύ τους για να τεστάρουμε εάν οι ρυθμίσεις έχουν γίνει σωστα. Απλά θα εκκινήσουμε τα δύο διαφορετικά προγράμματα και θα συνθέσουμε ένα μήνυμα θα το στείλουμε στον άλλο χρήστη και από το άλλο πρόγραμμα θα απαντήσουμε στο μήνυμα. Όπως φαίνεται και στην παρακάτω εικόνα η επικοινωνία μέσω client λειτουργεί σωστά:

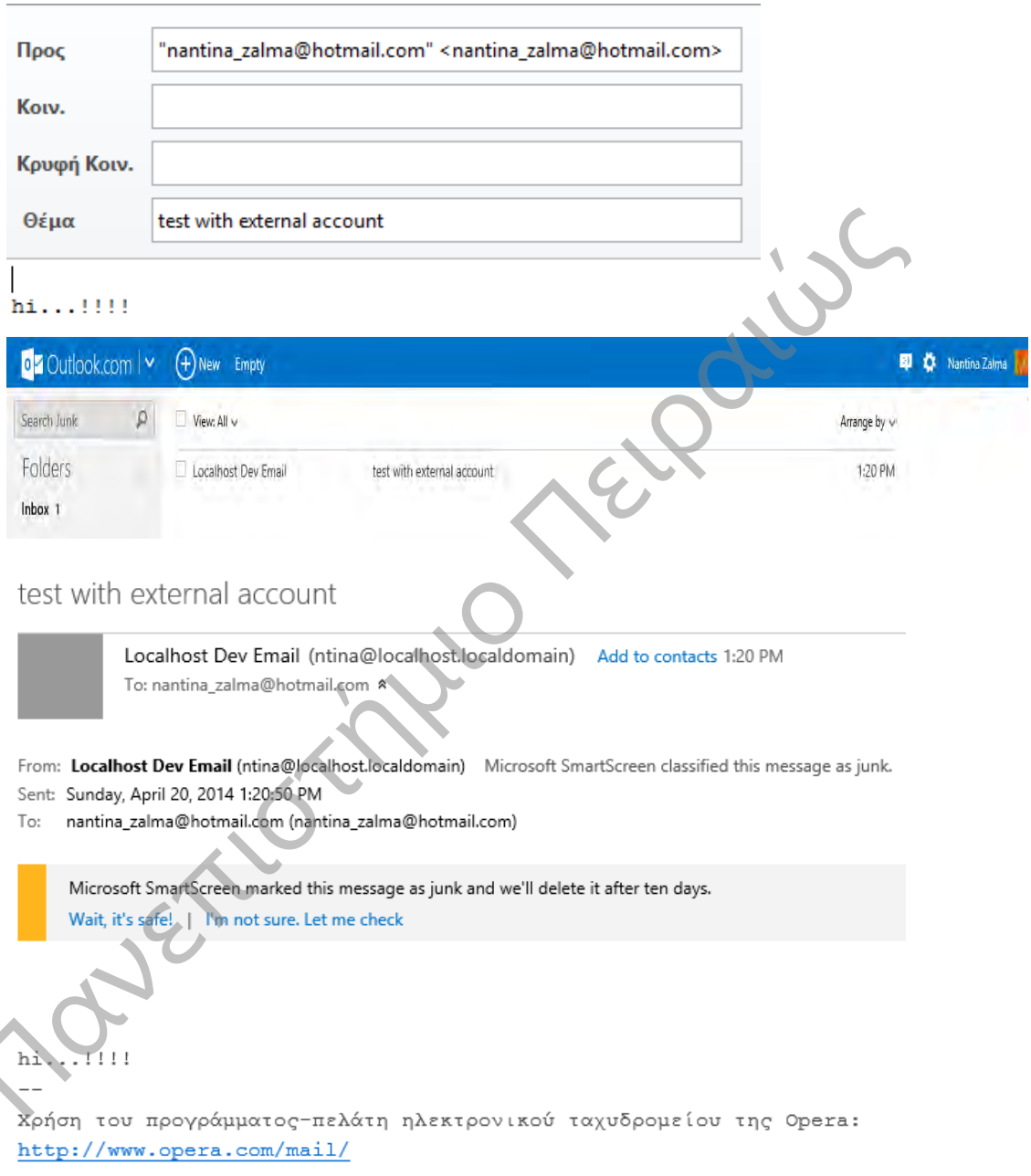


Εικόνα 79: «Επιτυχής Επικοινωνία Χρηστών»

5.3.5 Test case 5: Έλεγχος επικοινωνιας με εξωτερικους λογαριασμους χρηστων

Τέλος για να δούμε εάν ο SMTP λειτουργεί κανονικά δοκιμάζουμε να στείλουμε ένα μήνυμα σε ένα εξωτερικό λογαριασμό ηλεκτρονικού ταχυδρομείου. Αξίζει να σημειωθεί σε αυτό το σημείο ότι η αποστολή έγινε στον υπολογιστή που είναι εγκατεστημένος ο server και έχει προστεθεί στο αρχείο **host** η IP του email server επειδή πρόκειται για τοπικό διακομιστή δεν

έχουν ρυθμιστεί MX Records. Στις παρακάτω εικόνες φαίνεται η επιτυχής αποστολή και παράδοση αλληλογραφίας σε εξωτερικό λογαριασμό χρήστη.

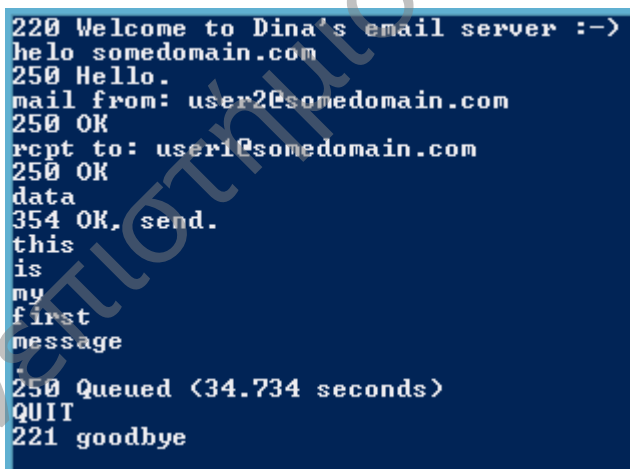


Εικόνα 80: «Επιτυχής Επικοινωνία με Εξωτερικούς Χρήστες»

5.3.6 Αποστολη email με εντολες SMTP

Έχοντας αναλύσει τις εντολες του SMTP μπορούμε να συντάξουμε και να αποστείλουμε μηνύματα μέσω command line χωρίς την χρήση προγραμμάτων σύνταξης email. Ένα τυπικό ηλεκτρονικό μήνυμα με απευθείας εντολές στον διακομιστή αλληλογραφίας θα ήταν ως εξής:

- Telnet localhost 25
- 220 Welcome to Dina's email server :-)
- helo somedomain.com
- 250 Hello.
- mail from: user1@somedomain.com
- 250 OK
- rcpt to: user2@somedomain.com
- 250 OK
- data
- 354 OK, send.
- this
- is
- my
- first
- time
- .
- 250 Queued (21.750 seconds)
- QUIT.



Εικόνα 81: «Αποστολή email με εντολές SMTP»

5.4 Μετρα Ασφαλειας απο πλευρας Διακομιστη

Ο hMailServer παρέχει ασφάλεια απέναντι σε όλους του κινδύνους στο ηλεκτρονικό ταχυδρομείο είτε έχοντας ενσωματωμένες λειτουργίες ασφάλειας είτε δίνοντας τη δυνατότητα στο χρήστη να προσθέσει εργαλεία ασφάλειας της επιλογής του. Θα εξετάσουμε λεπτομερώς κάθε μία τεχνική απέναντι στους κινδύνους του ηλεκτρονικού ταχυδρομείου και πως μπορούμε να ενσωματώσουμε τα μέτρα ασφάλειας στον server.

5.4.1 Τεχνικες Anti-spam

Ο hMailServer διαθέτει μια σειρά από ενσωματωμένες μεθόδους για προστασία από ανεπιθύμητη αλληλογραφία. Αυτές λειτουργούν ελέγχοντας τα εξής:

a) τον αποστολέα των μηνυμάτων
b) το περιεχόμενο του μηνύματος και
c) τον τρόπο που το μήνυμα έχει παραδοθεί στον hMailServer.

Για παράδειγμα, εάν το μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει συνδέσμους προς ιστοσελίδες spammer, ή αποστέλλεται από μια διεύθυνση η οποία είναι γνωστή για την αποστολή spam, το μήνυμα μπορεί να χαρακτηριστεί ως **spam**. Όλα τα αντι-spam εργαλεία του hMailServer, βρίσκονται στην ενότητα **Settings - Anti-spam.** Πιο συγκεκριμένα η προστασία απέναντι στην ανεπιθύμητη αλληλογραφία ενεργοποιείται σε τρεις άξονες: σκορ, στο χρόνο και στο είδος των μηνυμάτων.

- **Spam scoring- Spam βαθμολόγηση**

Κάθε ένα από τα spam τεστ που πραγματοποιούνται από τον hMailServer δημιουργεί ένα Spam σκορ-αριθμό. Εάν ο hMailServer εντοπίσει -με ένα συγκεκριμένο spam τεστ- ότι το μήνυμα είναι spam, υπολογίζεται ένα spam σκορ και προστίθεται στο μήνυμα. Όταν όλα τα spam τεστ τρέξουν, ο hMailServer συγκρίνει τη συνολική βαθμολογία του spam μηνύματος σε δύο διαφορετικά **κατώτατα όρια** που είναι ενσωματωμένα στον hMailServer.

Το πρώτο όριο είναι το **Mark όριο** όπως ονομάζεται. Αν το συνολικό spam σκορ για το μήνυμα φτάσει το Mark όριο, τότε το θέμα του μηνύματος τροποποιείται για να φαίνεται ότι το μήνυμα περιέχει spam. Χρησιμοποιώντας τη σήμανση των μηνυμάτων, οι χρήστες μπορούν ευκολότερα να εντοπίσουν και να διαγράψουν τα spam μηνύματα, ή ο διαχειριστής του διακομιστή μπορεί να δημιουργήσει κανόνες για τη μετακίνηση των μηνυμάτων σε ένα συγκεκριμένο IMAP φάκελο, ή την προώθηση τους σε ένα συγκεκριμένο φάκελο.

Το δεύτερο όριο spam είναι το **όριο Διαγραφής**. Αν το μήνυμα φτάσει σε αυτό το όριο, το μήνυμα διαγράφεται.

- **Χρόνος απόκρισης προστασίας απέναντι στα spam;**

Το ερώτημα που εύλογα γεννιέται είναι πότε υπάρχει προστασία απέναντι στα spam. Ο hMailServer προσπαθεί να προσδιορίσει αν το μήνυμα είναι spam όσο το δυνατόν νωρίτερα στην επικοινωνία με τον παραλήπτη. Όσο νωρίτερα γίνεται ο εντοπισμός, τόσο λιγότεροι πόροι θα χρησιμοποιηθούν από τον server για να διαχειριστούν τα μηνύματα. Ένα άλλο πλεονέκτημα με την έγκαιρη διάγνωση είναι ότι ο hMailServer μπορεί πιο εύκολα να πει στον αποστολέα ότι το μήνυμα απορρίπτεται και ο αποστολέας μπορεί να κοινοποιηθεί.

Αν ένα μήνυμα ηλεκτρονικού ταχυδρομείου παραδίδεται στον hMailServer χρησιμοποιώντας πρωτόκολλο SMTP, τότε ο hMailServer ενεργοποιεί την προστασία από τα spam στα ακόλουθα στάδια:

- Μετά την **RCPT TO** εντολή. Όταν ο παραλήπτης του μηνύματος έχει προσδιοριστεί, ο hMailServer εκτελεί προστασία από spam.
- Μετά την εντολή **DATA**. Όταν ολόκληρο το μήνυμα έχει μεταφερθεί στον hMailServer, τότε εκτελεί spam προστασία για το περιεχόμενο του μηνύματος.
- Αν ο hMailServer παραλάβει ένα μήνυμα από έναν εξωτερικό λογαριασμό, η προστασία ενάντια στα spam εκτελείται πριν το μήνυμα αποθηκευτεί στο φάκελο του λογαριασμού του χρήστη.

- **Είδος των μηνυμάτων που σαρώνονται**

Ο hMailServer σαρώνει όλα τα μηνύματα που παραδίδονται και χρησιμοποιούν τους λογαριασμούς, υποθέτοντας ότι έχουν τις εξής προϋποθέσεις:

- Το μήνυμα παραδίδεται στον hMailServer χρησιμοποιώντας πρωτόκολλο SMTP, η από έναν εξωτερικό λογαριασμό χρησιμοποιώντας πρωτόκολλο POP3.
- Όταν τουλάχιστον μία μέθοδος προστασίας κατά της ανεπιθύμητης αλληλογραφίας είναι ενεργοποιημένη στις Anti-spam ρυθμίσεις.
- Η διεύθυνση IP του αποστολέα ή του τομέα δεν συμπεριλαμβάνεται στην white list.
- Οι διευθύνσεις IP των αποστολέων ταιριάζουν με ένα εύρος διευθύνσεων IP, όπου η επιλογή του Anti-spam είναι ενεργοποιημένη.

Ρυθμίσεις

Οι ρυθμίσεις που πρέπει να γίνουν στην πλευρά του server ώστε να υπάρχει προστασία απέναντι στην ανεπιθύμητη αλληλογραφία είναι:

- **Κατώτατο Mark όριο**

Όταν στον hMailServer είναι ενεργοποιημένη η προστασία απέναντι στα spam, ο κάθε μηχανισμός προστασίας δίνει μια βαθμολογία-έναν σκορ. Αν το συνολικό σκορ του μηνύματος φτάσει αυτή την τιμή - αλλά παραμένει κάτω από Spam όριο Διαγραφής, το μήνυμα θα χαρακτηρίζεται μόνο ως spam. Στην περιοχή Anti-spam-στην καρτέλα General ενεργοποιήστε τα εξής:

- **Add X-hMailServer-Spam :** προσθέτει μια X-hMailServer-Spam MIME κεφαλίδα στο μήνυμα του ηλεκτρονικού ταχυδρομείου.
- **Add X-hMailServer- Reason :** Όταν είναι ενεργοποιημένη αυτή η επιλογή ο hMailServer θα προσθέσει μια κεφαλίδα στο μήνυμα το οποίο περιέχει πληροφορίες σχετικά με την αιτία που ο hMailServer χαρακτηρίζει το συγκεκριμένο email ως spam.
- **Add to message subject:** Με αυτή τη ρύθμιση, μπορείτε να καθορίσετε ένα κείμενο που ο hMailServer θα προσθέτει πριν από το θέμα του μηνύματος. Σε συνδυασμό με τους κανόνες, τα spam μηνύματα θα μετακινούνται σε συγκεκριμένους IMAP φακέλους.

- **Όριο Διαγραφής**

Όταν στον hMailServer είναι ενεργοποιημένη η προστασία απέναντι στα spam, κάθε μηχανισμός προστασίας δίνει έναν σκορ. Αν η συνολική βαθμολογία του μηνύματος φτάσει την τιμή αυτή, το μήνυμα θα πρέπει να διαγραφεί και να μην παραδοθεί στους παραλήπτες του.

- **Μέγιστο όριο μηνύματος που θα σαρωθεί (σε KB)**

Εάν ένα μήνυμα ξεπεράσει το όριο μεγέθους δεν θα σαρωθεί από τον hMailServer σαν spam. Στις περισσότερες περιπτώσεις οι spammers στέλνουν μικρά σε μέγεθος μηνύματα για να μην μειώσουν το εύρος ζώνης οπότε η σάρωση μεγάλων μηνυμάτων είναι περιττή στις περισσότερες περιπτώσεις.

Οι τεχνικές που χρησιμοποιούνται από το hMailServer για μια ολοκληρωμένη λύση απέναντι στα spam είναι:

- **SPF**

SPF σημαίνει Sender Policy Framework -Πλαίσιο Πολιτικής Αποστολέα. Οι ιδιοκτήτες domain μπορούν, μέσω μιας εγγραφής στο DNS τους, να αναγνωρίσουν τους email servers που τους έχει επιτραπεί η αποστολή e-mail από το δικό τους domain. Εάν ενεργοποιήσετε την επιλογή SPF, τότε ο hMailServer θα ελέγξει εάν η διεύθυνση IP του αποστολέα ταιριάζει με τη διεύθυνση IP με την εγγραφή DNS. Αν όχι, τότε το μήνυμα αντιμετωπίζεται ως spam. Περισσότερες πληροφορίες σχετικά με το SPF μπορούν να βρεθούν στη σελίδα ***http://spf.pobox.com/***.

- **Έλεγχος ονόματος κεντρικού υπολογιστή στην εντολή HELO**

Όταν ένας άλλος e-mail server παραδίδει ένα email στον hMailServer, θα πρέπει να προσδιορίσει την ταυτότητα του, στέλνοντας ταυτόχρονα το δικό του όνομα κεντρικού υπολογιστή- host name.

Αν έχετε ρυθμίσει ο hMailServer να ελέγχει το όνομα κεντρικού υπολογιστή στην εντολή HELO, τότε θα γίνει **μια αναζήτηση DNS (DNS lookup)** και να επιβεβαιωθεί ότι ο αποστολέας διακομιστής έχει δώσει το σωστό όνομα κεντρικού υπολογιστή.

Εδώ αξίζει να σημειωθεί ότι μια **αναζήτηση DNS** είναι όταν μια συσκευή που υποστηρίζει το πρωτόκολλο IP ζητά από το διακομιστή DNS τη διεύθυνση IP που σχετίζεται με ένα όνομα τομέα. Ο διακομιστής DNS πρέπει να **"εξετάσει (look-up)"** την IP που συνδέεται με αυτό το όνομα τομέα.(πηγή εικόνας: http://wiki.answers.com/Q/What_is_DNS_Lookup)

Το μειονέκτημα αυτής της μεθόδου είναι το ρίσκο των εσφαλμένων αποτελεσμάτων. Διότι ενώ αυτή η μέθοδος μπορεί να χρησιμοποιηθεί για να ανιχνεύσει τα spam, πολλοί από τους νόμιμους ιδιοκτήτες τομέα δεν έχουν ρυθμίσει τον server τους σωστά.

- **Έλεγχος ότι αποστολέας έχει DNS MX εγγραφές**

Εάν ενεργοποιήσετε αυτήν την επιλογή, ο hMailServer θα ελέγξει αν το όνομα τομέα στη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα αν έχει DNS-MX εγγραφές. Για παράδειγμα, εάν ο χρήστης με διεύθυνση: **bill@microsoft.com** σας στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ο hMailServer θα ελέγξει αν το domain, **microsoft.com**, έχει DNS-MX εγγραφή. Αν έχει, τότε το μήνυμα γίνεται αποδεκτό, αν δεν έχει, τότε το μήνυμα απορρίπτεται (αν το spam σκορ φτάσει το όριο Διαγραφής). Αυτό το χαρακτηριστικό υπάρχει στον hMailServer για να εμποδίσει την αποδοχή των email στην περίπτωση που μερικοί spammers στείλουν email από ψεύτικά domain που δεν υπάρχουν.

Το μειονέκτημα αυτής της επιλογής είναι ότι ο διακομιστής μπορεί να απορρίψει νόμιμά email. Για παράδειγμα, εάν ένα email δημιουργηθεί αυτόματα από την διεύθυνση: **cgi.domain.com** και ο **cgi.domain.com** δεν διαθέτει έγκυρη MX-εγγραφή, τότε το μήνυμα θα διαγραφεί (υποθέτοντας ότι τα spam σκορ φτάσουν το όριο Διαγραφής).

- **SpamAssassin**

Το SpamAssassin είναι ένα δημοφιλές, εξωτερικό σύστημα, ανίχνευσής spam. Είναι ένα e-mail φίλτρο ανοιχτού κώδικα για τον εντοπισμό spam. Είναι ένα έξυπνο email φίλτρο που χρησιμοποιεί ένα ευρύ φάσμα δοκιμών για να διαπιστωθεί αν το e-mail είναι spam.

Οι δοκιμές αυτές εφαρμόζονται στους τίτλους των email και στο περιεχόμενο για να ταξινομήσει email με τη χρήση προηγμένων στατιστικών μεθόδων. Επιπλέον, το SpamAssassin έχει σχεδιαστεί για εύκολη ενσωμάτωση σε οποιοδήποτε σύστημα ηλεκτρονικού ταχυδρομείου.

Για να χρησιμοποιήσετε SpamAssassin με hMailServer, θα πρέπει να εγκαταστήσετε το SpamAssassin ξεχωριστά. (πηγή εικόνας: http://wiki.apache.org/spamassassin/SpamAssassin)

- **Tarpitting**

Το Tarpitting μπορεί να χρησιμοποιηθεί για να επιβραδύνει την επικοινωνία του hMailServer με τους spammers. Μερικοί spammers μπορεί να σταματήσουν την αποστολή e-mail στο διακομιστή σας, αν ανταποκρίνεται πολύ αργά στα αιτήματά τους. Υποθέτοντας ότι ο spammer στέλνει ένα e-mail σε πολλούς παραλήπτες στον server σας κατά τη διάρκεια μιας SMTP σύνδεσης. Εάν ο αριθμός των παραληπτών υπερβαίνει τον Tarpitting μετρητή, ο hMailServer θα καθυστερήσει την απάντηση του κάθε παραλήπτη ξεχωριστά, για κάποιο συγκεκριμένο αριθμό δευτερολέπτων.

Ενώ αυτή η μέθοδος αποτρέπει σε κάποιο βαθμό τους spammers, μπορεί όμως να προκαλέσει προβλήματα στους νόμιμους αποστολείς email. Ως εκ τούτου, η χρήση αυτής της μεθόδου για προστασία από spam δεν προτείνεται.

- **DNS blacklists**

Οι DNS Blacklists είναι λίστες e-mail servers που είναι γνωστές για την αποστολή spam. Αυτές οι λίστες δημιουργούνται και ενημερώνονται από διαφορετικούς οργανισμούς ή και από ιδιώτες. Εάν ενεργοποιήσετε την επιλογή DNS blacklists, όποτε ο hMailServer λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου θα ελέγξει τη διεύθυνση IP του αποστολέα σε σχέση με τις λίστες που έχετε επιλέξει να χρησιμοποιήσετε. Αν η διεύθυνση IP έχει βρεθεί να είναι σε οποιαδήποτε από αυτές τις λίστες, τότε ο hMailServer δεν θα δεχθεί το μήνυμα.

Σύμφωνα με γνωστές στατιστικές, είναι γνωστό ότι οι DNS Blacklists μπορούν να μειώσουν το φαινόμενο της ανεπιθύμητης αλληλογραφίας περίπου κατά 15-25%, απλώς και μόνο βάσει της διεύθυνσης IP του αποστολέα. Θα πρέπει όμως να γνωρίζετε ότι η λίστα μπορεί να εμποδίσει και νόμιμα μηνύματα. Για παράδειγμα, εάν ο αποστολέας χρησιμοποιεί έναν λογαριασμό email από κάποιο διακομιστή που έχει χαρακτηριστεί ως διακομιστής spam τότε και το μήνυμα του θα αποκλειστεί.

- **SURBL**

Τα SURBLs διαφέρουν από τις DNS blacklists στο ότι για τον εντοπισμό των spam βασίζονται στο σώμα του μηνύματος ή URL (συνήθως για web sites). Τα SURBLs δεν προορίζονται στο να εντοπίζουν αποστολείς spam μηνυμάτων από τις κεφαλίδες των μηνυμάτων τους ή τις διευθύνσεις IP. Αντίθετα σας επιτρέπουν να εντοπίσετε τα μηνύματα από τα spam sites που μπορεί να περιέχονται στο σώμα ενός μηνύματος. Αυτό σημαίνει ότι όταν είναι ενεργοποιημένο το SURBL, ο hMailServer αναζητά μέσα στο μήνυμα ηλεκτρονικού ταχυδρομείου για links. Αν βρεθεί οποιοδήποτε link, ο hMailServer με το SURBL διακομιστή, ελέγχουν εάν αυτά τα links υπάρχουν συνήθως σε μηνύματα spam.

- **Grey listing**

Η δημιουργία μίας «Γκρι λίστας» σας επιτρέπει να αποτρέψετε την ανεπιθύμητη αλληλογραφία με την προσωρινή απόρριψη του e-mail από το διακομιστή σας. Το **Grey listing** λειτουργεί ως εξής οι σωστοί διακομιστές e-mail θα προσπαθήσει να ξαναστείλουν το μήνυμα αργότερα, ενώ οι spammers συνήθως θα εγκαταλείψουν αμέσως αν ο διακομιστής σας απορρίψει ένα email.

Όταν ο αποστολέας προσπαθήσει να στείλει ένα μήνυμα, για πρώτη φορά στον server σας, ο hMailServer θα σώσει:

1. τη διεύθυνση IP του αποστολέα,
2. τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα και
3. τη διεύθυνση email του παραλήπτη.

Αυτή η πληροφορία ονομάζεται **triplet**. Ο hMailServer θα απορρίψει το μήνυμα και θα ζητήσει από το διακομιστή αποστολής να ξαναδοκιμάσει αργότερα. Την επόμενη φορά που ο αποστολέας θα στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που ταιριάζει με το **triplet**, τότε ο hMailServer θα δεχτεί το μήνυμα.

1. **DKIM**

Τα DKIM-Domain Keys Identified Mail, είναι μια μέθοδος για να υπογράφεται το περιεχόμενο των μηνυμάτων. Ο παραλήπτης μπορεί να επαληθεύσει ότι το μήνυμα έχει σταλεί από έναν έγκυρο αποστολέα, και ότι το περιεχόμενο του μηνύματος δεν έχει τροποποιηθεί κατά τη μεταφορά.

Αν η επιλογή της DKIM-επαλήθευσης είναι ενεργοποιημένη, τότε ο hMailServer θα ψάξει για μια DKIM-υπογραφή σε κάθε μήνυμα. Εάν η επικεφαλίδα βρεθεί, τότε ο hMailServer θα επιβεβαιώσει ότι το περιεχόμενο του μηνύματος ταιριάζει με την υπογραφή. Εάν δεν περιλαμβάνεται DKIM-Υπογραφή, δεν θα γίνει επαλήθευση του μηνύματος. Αυτή η τεχνική στοχεύει να εντοπίσει ένα μικρό ποσοστό spam μηνυμάτων μίας και οι επίδοξοι spamers θα παραλείψουν να υπογράψουν τα μηνύματα τους.

❖ **Εξωτερικά εργαλεία**

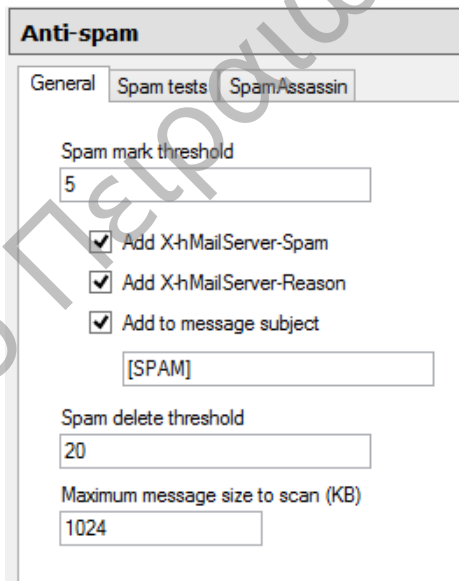
Εξωτερικά εργαλεία, όπως το ASSP ή το SpamAssassin, μπορεί να χρησιμοποιηθούν παράλληλα με τον hMailServer για την πρόληψη των spam. Τόσο το ASSP και το SpamAssassin είναι ειδικά λογισμικά με μοναδικό σκοπό την ανίχνευση ενός email αν είναι spam. Προσφέρουν συνεπώς πολύ πιο πλούσια προστασία spam από εκείνα που περιλαμβάνονται στον hMailServer.

Ρυθμίσεις στον hMailServer για την παρούσα μελέτη:

Για την συγκεκριμένη υλοποίηση επιλέξαμε τις παρακάτω ρυθμίσεις για την περιοχή anti-spam:

Στην καρτέλα **General**:

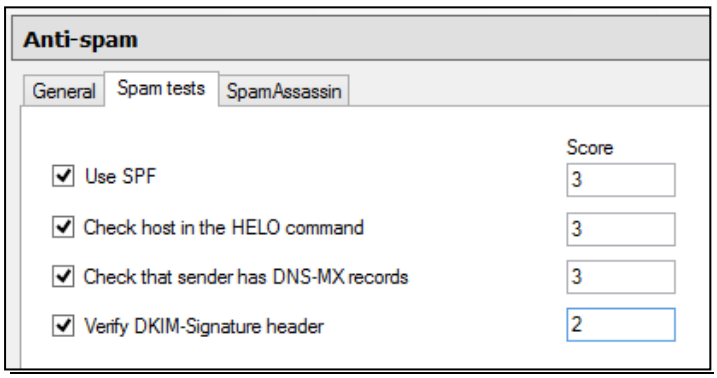
- ❖ **Spam mark threshold** (κατώτατο όριο σκορ) = **5** δηλαδή εάν το μήνυμα ξεπεράσει το σκορ 5 μετά τα Spam test που θα γίνονται θα χαρακτηρίζεται ως **Spam**.
- ❖ Επιπρόσθετα ενεργοποιούμε και τις επιλογές:
  - **Add X-hMailServer-Spam:** θα προσθέτει μια κεφαλίδα στο μήνυμα αν είναι spam,
  - **Add X-hMailServer-Reason:** θα προσθέσει άλλη μία σχετικά με τις πληροφορίες για την οποία χαρακτηρίζει το συγκεκριμένο email ως spam και
  - **Add to message subject:** τέλος θα προσθέτει πριν από το θέμα του μηνύματος το όνομα **[SPAM]**.
- ❖ **Spam delete threshold** (όριο διαγραφής) **=20** αν η συνολική βαθμολογία του μηνύματος ξεπεράσει την τιμή αυτή, το μήνυμα διαγράφεται και δεν παραδίδεται στους παραλήπτες.
- ❖ **Maximum message size to scan (KB)= 1024**



Εικόνα 82: «Ρυθμίσεις Anti-spam/ General»

Στην καρτέλα **Spam tests**:

- ❖ Σε αυτήν την καρτέλα ενεργοποιούμε όλα τα spam test που μπορούν να γίνουν από τον hmailserver δίνοντας τους ένα σκορ, το άθροισμα αυτών μαζί με τα σκορ στην καρτέλα **DNS Blacklist** ξεπερνά το σκορ διαγραφής που έχουμε βάλει στην καρτέλα **General** δηλαδή το **Spam delete threshold.** (Alter Procedure)

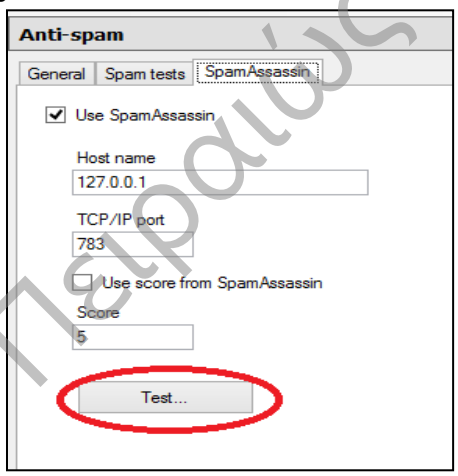


Εικόνα 83: «Ρυθμίσεις Anti-spam/ Spam tests»

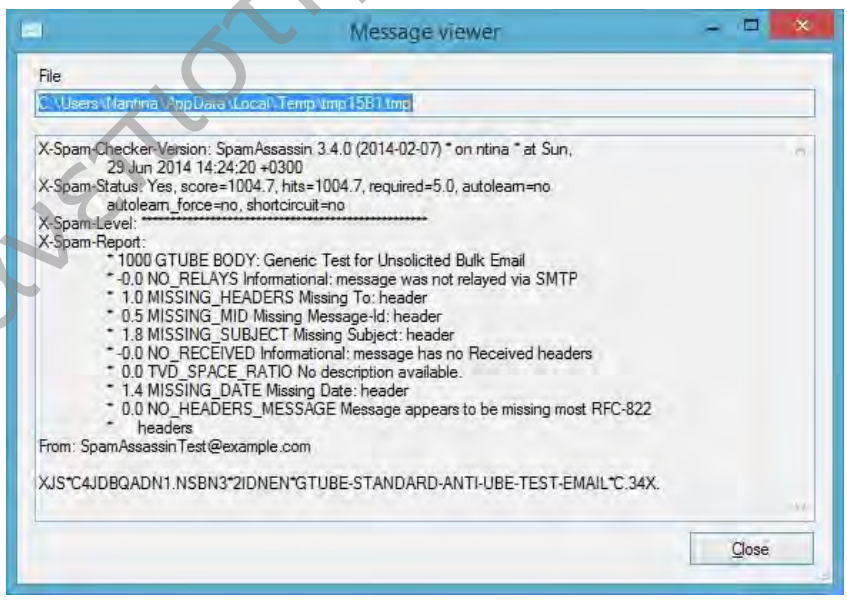
Στην καρτέλα **SpamAssassin**:

Θέλοντας να χρησιμοποιήσουμε και την πρόσθετη τεχνική για προστασία κατά των Spam, την ενσωμάτωση εξωτερικού σαρωτή επιλέξαμε το εργαλείο **SpamAssissin** και ακολουθούμε τα εξής βήματα:

- Στην επίσημη ιστοσελίδα http://www.jam-software.com/spamassassin/ επιλέγουμε να κατεβάσουμε το λογισμικό στον υπολογιστή ή server που βρίσκεται εγκατεστημένος ο hmailserver. Για να είναι δυνατόν η εφαρμογή να χρησιμοποιηθεί σαν φλιτάρισμα αλληλογραφίας σε server ταχυδρομείου προτείνεται να επιλέξετε την εφαρμογή «**SpamAssassin in a Box**».
- Αφού επιλέξουμε την συγκεκριμένη εκδοχή και Δωρεάν Δοκιμή (30 Days Trial) , τρέχουμε τον οδηγό εγκατάστασης του προϊόντος.
- Στην καρτέλα **SpamAssissin** ενεργοποιούμε την επιλογή «**Use SpamAssissin**» με **Hostname**: την IP του server και πόρτα TCP/IP: **783** (ως προεπιλεγμένη) και πατάμε το κουμπί «**Test**» για να ελέγξουμε ότι υπάρχει επικοινωνία με τον server. Στην περίπτωση επιτυχούς επικοινωνίας μας εμφανίζεται το παράθυρο «**Message Viewer**» που μας πληροφορεί για το path που είναι εγκατεστημένη η εφαρμογή καθώς ένα κομμάτι κώδικα για να ελέγξουμε την προστασία απέναντι στα **Spam**.



Εικόνα 84: «Ρυθμίσεις Anti-spam/ SpamAssassin»

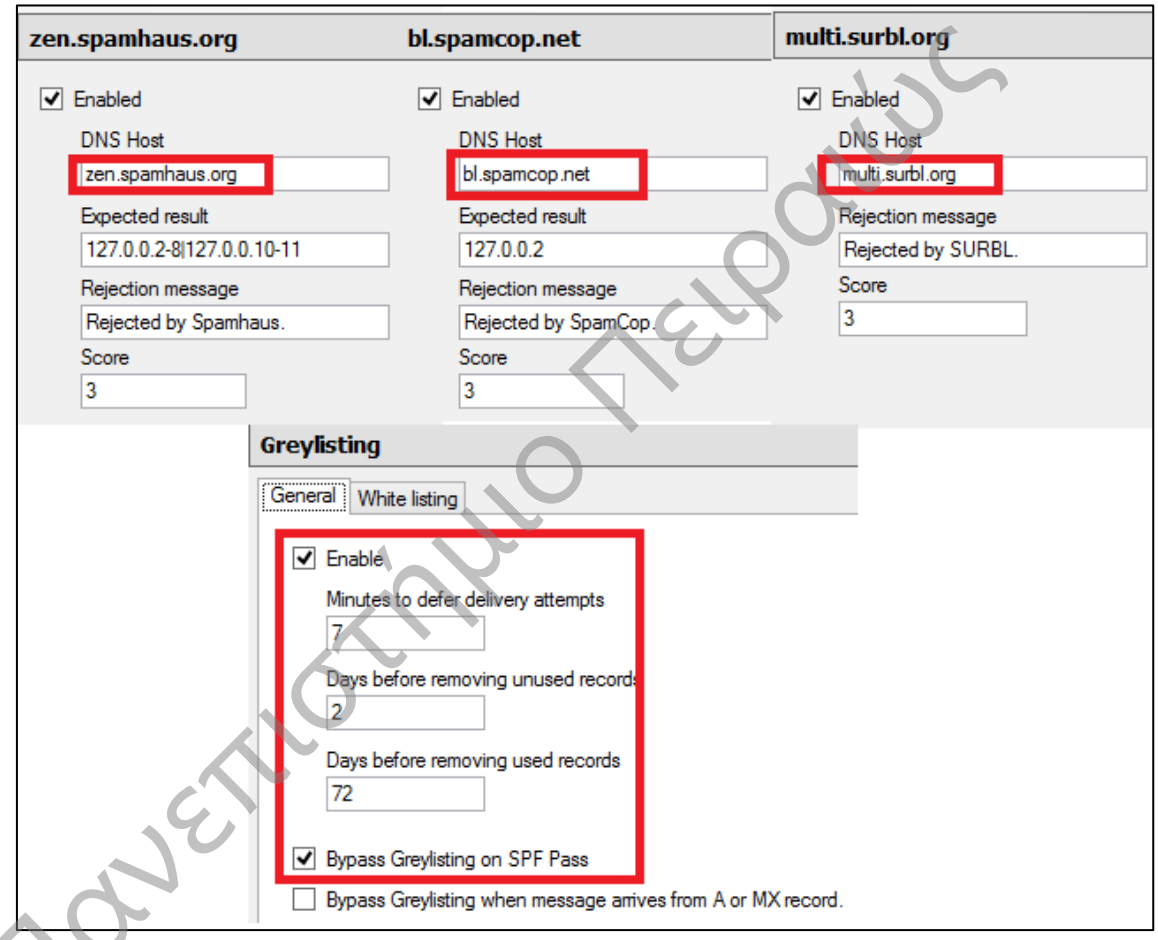


Εικόνα 85: «Μήνυμα Επιτυχούς Σύνδεσης με SpamAssassin»

(Alter Procedure) (Youtube)

Στις περιοχές **DNS Blacklists, SURBL Servers, Greylisting, Whitelisting**:

- Είναι δυνατόν να ορίσουμε IP server αλληλογραφίας που χαρακτηρίζονται ως αποστολείς Spam ωστόσο δεν έγινε κάποια αλλαγή εδώ, ενεργοποιηθήκαν οι default επιλογές ασφάλειας του hmailserver δηλαδή οι προτεινόμενες IP των Spam server **zen.spamhaus.org** , **bl.spamcop.net** , **multi.surbl.org** με τα αντίστοιχα σκορ και στην περιοχή **Greylisting** ενεργοποιήσαμε την επιλογή απόρριψης του μηνύματος και επαναποστολής με σκοπό την σύγκριση του **triplet** .



Εικόνα 86: «Ρυθμίσεις DNS Blacklists, SURBL Servers, Greylisting, Whitelisting»

5.4.2 Antivirus

Ο hMailServer έχει ενσωματωμένη υποστήριξη απέναντι στην ανίχνευση ιών που αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου με το open source λογισμικό προστασίας από ιούς, το **ClamWin.**

Μπορεί επίσης να υποστηρίξει διαφορετικά προγράμματα ανίχνευσης ιών. Ενεργοποιώντας την επιλογή **Χρήση εξωτερικού σαρωτή – Use external scanner** στην καρτέλα **External virus scanner** δίνεται η δυνατότητα επιλογής εξωτερικού scanner ανίχνευσης ιών. Σας επιτρέπει να εκτελέσετε οποιοδήποτε anti virus πρόγραμμα που υποστηρίζει λειτουργία σάρωσης σε επίπεδο γραμμής εντολών- **command line scanning.** Χρησιμοποιώντας την μακροεντολή **%FILE%** στην γραμμή εντολών, ο hMailServer θα αντικαταστήσει την εντολή %FILE% με το path που χρειάζεται να σαρωθεί.

Στον πεδίο **Scanner executable**, μπορείτε να καθορίσετε τη γραμμή εντολών που θα πρέπει να χρησιμοποιείται κατά τη σάρωση. Στο πεδίο **Return value**, μπορείτε να ορίσετε την τιμή που θα επιστρέφει το πρόγραμμα όταν ένας ιός ανιχνεύεται. Αυτή η τιμή ποικίλει ανάλογα με τον σαρωτή ιού. Για αυτήν την υλοποίηση επιλέξαμε να χρησιμοποιήσουμε την ενσωματωμένη υποστήριξη του hmailserver το **ClamWin**.

Test case: Ανίχνευση ιού

Για να μπορέσουμε να δοκιμάσουμε την προστασία απέναντι σε ιούς θα χρησιμοποιήσουμε ένα εικονικό αρχείο με όνομα EICAR το οποίο αντιμετωπίζεται σαν ιός από σαρωτές anti-virus, αλλά είναι ασφαλές για χρήση, δεδομένου ότι δεν πρόκειται για πραγματικός ιό μίας και οι δοκιμές με πραγματικούς ιούς είναι ριψοκίνδυνο. Οι παρακάτω σελίδες περιέχουν το κώδικα του αρχείου EICAR που προορίζεται για δοκιμές anti-virus:

- Alpha-tec.
- Webmail.us.

Ρυθμίσεις:

- Περίπτωση εντοπισμού ιού

Μπορείτε να επιλέξετε **Delete e-mail** εάν επιθυμείτε το μήνυμα που ανιχνεύτηκε να περιέχει ιό να σβήνεται άμεσα. Μπορείτε να επιλέξετε Delete attachments εάν επιθυμείτε το μηνύματα που ανιχνεύτηκαν να περιέχουν ιό να παραδίδονται στον παραλήπτη αλλά τα συνημμένα αρχεία να διαγράφονται από το περιεχόμενο του μηνύματος. Στην περίπτωση που ένα μήνυμα διαγράφεται υπάρχει και η επιλογή να πληροφορείται ο αποστολέας και / ή ο παραλήπτης ότι το μήνυμα διαγράφεται επειδή περιέχει ιό.

- Μέγιστο Μέγεθος μηνύματος που θα σαρωθεί (σε KB)

Στις περισσότερες περιπτώσεις που ένα μήνυμα περιέχει ιό είναι μικρά σε μέγεθος. Χρησιμοποιώντας αυτό το πεδίο μπορείτε να παραλείψετε μηνύματα από κάποιο μέγεθος και πάνω να σαρώνονται.

ClamWin:

Όπως προείπαμε σε αυτήν τη μελέτη θα ρυθμίσουμε τον διακομιστή να χρησιμοποιεί το εργαλείο ClamWin αυτόματα. Για να ρυθμιστεί αυτόματα ο hMailServer να χρησιμοποιεί το ClamWin, θα πρέπει να ενεργοποιηθεί η επιλογή **Autodetect**.

Block attachments:

Αυτή η επιλογή επιτρέπει να μπλοκάρονται συνημμένα αρχεία με βάση την επέκταση. Εάν ενεργοποιηθεί αυτή η επιλογή ο hMailServer θα αφαιρέσει τα συνημμένα αρχεία με συγκεκριμένη επέκταση αρχείου και θα τα αντικαταστήσει με νέο με όνομα: **<αρχικό_όνομα_αρχείου >.txt** που θα περιέχει ένα σύντομο μήνυμα ότι το συνημμένο έχει αφαιρεθεί.

Ρυθμίσεις στον hMailServer για την παρούσα μελέτη:

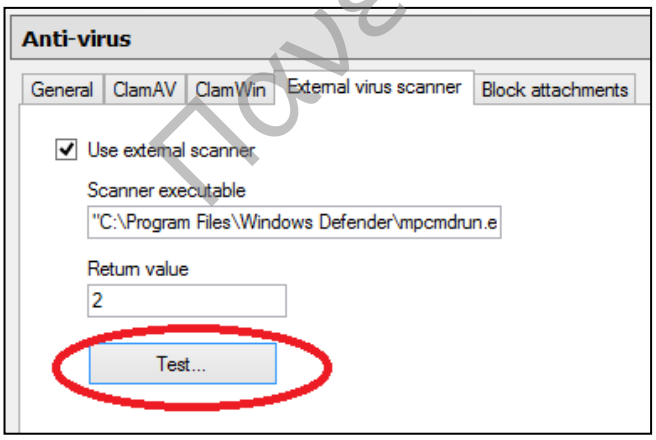
Για την παρούσα μελέτη στόχος μας ήταν η παροχή ασφάλειας απέναντι στους ιούς που στέλνονται μέσω ηλεκτρονικού ταχυδρομείου και όχι η αποτελεσματικότητα των διαφόρων antivirus εργαλείων, όποτε χρησιμοποιήσαμε ένα προεγκατεστημένο εργαλείο των Windows και αρκετα δημοφιλές για την ασφάλεια που παρέχει το **Windows Defender**.

Οπότε στην καρτέλα **General**:

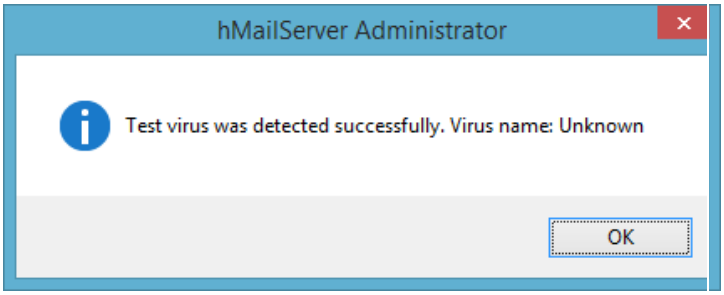
Ενεργοποιήσμε όλες τις επιλογές στην περίπτωση που εντοπιστεί ιός σε κάποιο email **Delete email ή Delete attachment** , που στην ενότητα του Penetration Test θα δούμε αναλυτικότερα πως συμπεριφέρεται σε κάθε μία από τις δύο αυτές επιλογές και δώσαμε **1KB** όριο μηνύματος σάρωσης.

Στην καρτέλα **External virus scanner**:

Ενεργοποιήσαμε την επιλογή **Use External scanner** και στο πεδίο Scanner executable προσθέσαμε την περιοχή που βρίσκεται εγκατεστημένο το εκτελέσιμο αρχείο του προγράμματος Windows Defender και στο τέλος την μακροεντολή **-scan -scantype 3 -file "%FILE%" –disableremediation** μέσα σε εισαγωγικά και **Return value = 2** όπως ορίζεται στο Specification του Hmailserver για την ενεργοποίηση του συγκεκριμένου εργαλείου (https://www.hmailserver.com/forum/viewtopic.php?f=12&t=23906) δηλαδή όλη η εντολή είναι: **"C:\Program Files\Windows Defender\mpcmdrun.exe" -scan -scantype 3 -file "%FILE%" –disableremediation.** Πατώντας το κουμπί «Test» παίρνουμε και το μήνυμα επιτυχούς σύνδεσης.



Εικόνα 87: «Ρυθμίσεις Anti-virus/ External virus scanner»



Εικόνα 88: «Μήνυμα Επιτυχούς Σύνδεσης με virus scanner »

5.4.3 SSL CERTIFICATE

Εισαγωγή

Ο hMailServer έχει ενσωματωμένη υποστήριξη για SSL και TLS. Αυτό σημαίνει ότι αφού αποκτήσετε ένα πιστοποιητικό SSL, μπορείτε να κρυπτογραφήσετε τα email ανάμεσα στον διακομιστή και τους χρήστες. Συνήθως η αλληλογραφία στο Internet αποστέλλεται χωρίς κρυπτογράφηση, πράγμα που σημαίνει ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου συχνά μπορούν να διαβαστούν από μη-εξουσιοδοτημένους χρήστες. Για παράδειγμα, αν ένας χρήστης σε ένα μη κρυπτογραφημένο ασύρματο δίκτυο στέλνει ένα e-mail, άλλα μέρη μπορούν να υποκλέψουν την ασύρματη κίνηση και να διαβάσουν το μήνυμα. Άλλα παραδείγματα περιλαμβάνουν Πάροχους Υπηρεσιών Διαδικτύου που αναλύουν την επικοινωνία των χρηστών ηλεκτρονικού ταχυδρομείου τους.

Ο hMailServer υποστηρίζει SSL έκδοση 2, έκδοση 3 και TLS έκδοση 1.

Η απόκτηση ενός πιστοποιητικού SSL

Υπάρχουν δύο μέθοδοι για την απόκτηση πιστοποιητικού SSL. Μπορείτε να αγοράσετε ένα πιστοποιητικό SSL από μια αρχή έκδοσης πιστοποιητικών, ή μπορείτε να δημιουργήσετε το δικό σας υπογεγραμμένο πιστοποιητικό. Αγοράζοντας ένα πιστοποιητικό από μια αξιόπιστη αρχή έκδοσης πιστοποιητικών κατά κανόνα οδηγεί σε υψηλότερη ασφάλεια από τη δημιουργία ενός ιδιωτικού πιστοποιητικού.

Οι email clients δεν έχουν ρυθμιστεί ώστε να εμπιστεύονται ιδιωτικά πιστοποιητικά. Αυτό σημαίνει ότι αν χρησιμοποιείτε ένα τέτοιο πιστοποιητικό, ένα παράθυρο διαλόγου θα πρέπει να εμφανίζεται όταν συνδέεστε στο διακομιστή. Σε πολλά προγράμματα ηλεκτρονικού ταχυδρομείου, μπορείτε να επιλέξετε να αγνοήσετε την προειδοποίηση και να συνδεθείτε στον server. Αυτός είναι ένας ακόμα λόγος που είναι καλύτερα να αγοράσετε ένα πιστοποιητικό από μια αξιόπιστη αρχή.

Υπάρχει ένας μεγάλος αριθμός οργανώσεων που πωλεί τα πιστοποιητικά SSL. Αν προτιμάτε τη δημιουργία του δικού σας πιστοποιητικού SSL, ο ευκολότερος τρόπος να γίνει αυτό είναι να χρησιμοποιήσετε **OpenSSL**.

I. Η αγορά ενός πιστοποιητικού SSL περιλαμβάνει τα εξής βήματα:

1. Δημιουργία ιδιωτικού κλειδιού, με τη χρήση OpenSSL.
2. Δημιουργία αιτήματος υπογραφής πιστοποιητικού, χρησιμοποιώντας OpenSSL.
3. Να αφαιρέστε το κωδικό πρόσβασης από ένα ιδιωτικό κλειδί.
4. Να παραγγείλετε ένα πιστοποιητικό από την αρχή έκδοσης πιστοποιητικών
5. Η έκδοσης πιστοποιητικών να σας στείλει το πιστοποιητικό.
6. Να ρυθμίσετε τον hMailServer να χρησιμοποιεί το ιδιωτικό κλειδί και το πιστοποιητικό SSL.

Για τις ανάγκες της παρούσας μελέτης επιλέξαμε να δημιουργήσουμε ένα αυτό-υπογεγραμμένο πιστοποιητικό με την χρήση του προγράμματος **OpenSSL** όπου μπορείτε να κατεβάσετε το εργαλείο ανάλογα με την έκδοση του λειτουργικού που διαθέτετε από την επίσημη ιστοσελίδα: http://slproweb.com/products/Win32OpenSSL.html**.** Εγκαθιστώντας το εργαλείο του OpenSSL μπορείτε ανοίγοντας το παράθυρο γραμμής εντολών στην διαδρομή **C:\OpenSSL-Win64\bin** το αρχείο **openssl.exe**, να δημιουργήσετε το δικό σας πιστοποιητικό.

II. Η Δημιουργία αυτό-υπογεγραμμένου πιστοποιητικού περιλαμβάνει τα εξής βήματα:

1. Δημιουργία ιδιωτικού κλειδιού, με τη χρήση OpenSSL.

Πληκτρολογώντας την εντολή : **genrsa -des3 -out my_key.key 1024**

Όπου δημιουργείτε ένα ιδιωτικό κλειδί 1024 bit με RSA αλγόριθμο που είναι κρυπτογραφημένο με Triple-DES και αποθηκεύεται σε μορφή PEM, έτσι ώστε να είναι αναγνώσιμη μορφή κειμένου ASCII. Στην συνέχεια σας εμφανίζει κάποιες πληροφορίες ότι δημιουργεί το κλειδί και σας ζητάει συνθηματικό-password για το κλειδί.

2. Δημιουργία αιτήματος υπογραφής πιστοποιητικού, χρησιμοποιώντας OpenSSL.

Πληκτρολογώντας την εντολή : **req -new -key my_key.key -out my_req.csr**

Όταν δημιουργείται ένα ιδιωτικό κλειδί στην συνέχεια μπορεί να δημιουργηθεί ένα Αίτημα Υπογραφής Πιστοποιητικού. Επίσης κατά την διάρκεια δημιουργίας αιτήματος υπογραφής μας ζητάει και κάποιες άλλες πληροφορίες που παρατίθενται παρακάτω:

```
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Athens
Locality Name (eg, city) []:Marousi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Diplwmatikh Zalma
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:somedomain.com
Email Address []:user1 at somedomain dot com
```

3. Αφαίρεση κωδικού πρόσβασης από το ιδιωτικό κλειδί.

Μία ατυχής παρενέργεια κατά την δημιουργία του ιδιωτικού κλειδιού είναι ότι κρυπτογραφείται με 3DES όπου ζητάει τον κωδικό που εισάγαμε στο βήμα 1 για να μπορέσουμε να το χρησιμοποιήσουμε. Επειδή είναι αδύνατον να ενσωματώσουμε το ιδιωτικό κλειδί μέσα στον server με το κωδικό διότι σε κάθε συναλλαγή με τους clients θα πρέπει να εισάγεται ο κωδικός κρίνεται αναγκαίο να αφαιρέσουμε το κωδικό πρόσβασης από το ιδιωτικό κλειδί, αυτό γίνεται ως εξής:

- Αντιγράφοντας το αρχείο με την εντολή: **cp my_key.key my_key.key.org**
- Και στην συνέχεια εκτελώντας την εντολή: **rsa -in my_key.key.org -out my_key.key**

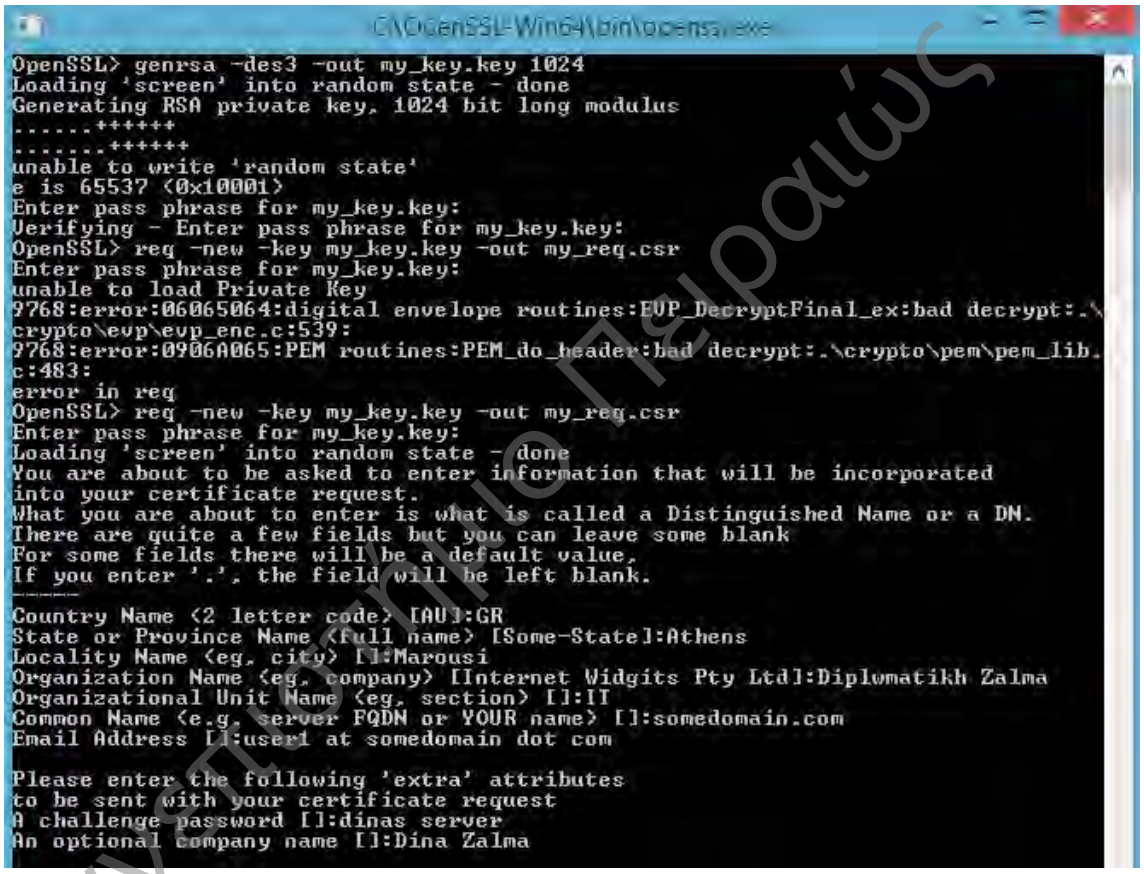
Το νέο κλειδί που έχει δημιουργηθεί δεν έχει πλέον username και password.

4. Χρησιμοποιώντας το OpenSSL να δημιουργήσετε ένα αυτό-υπογεγραμμένο πιστοποιητικό.

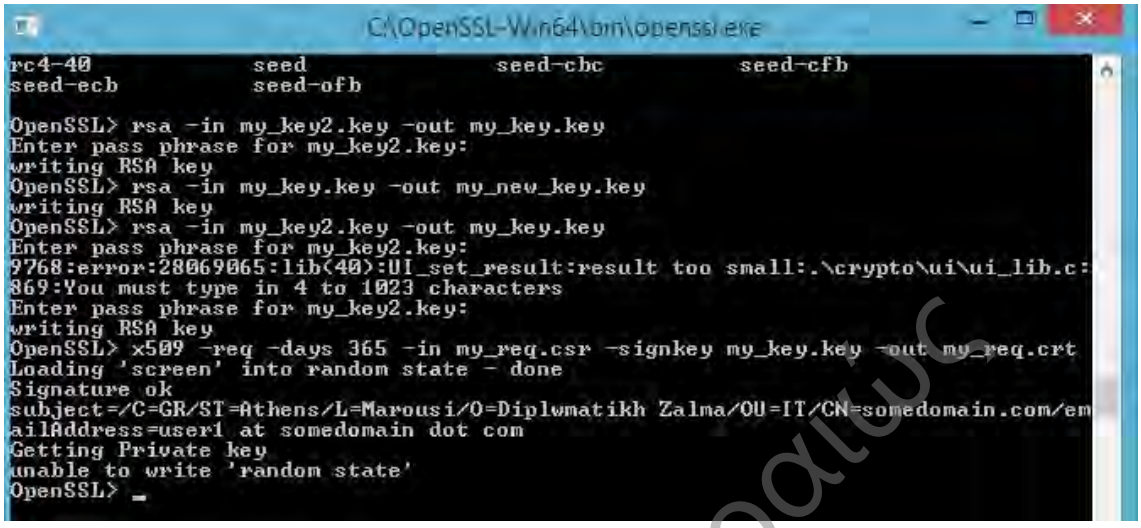
Σε αυτό το σημείο θα δημιουργήσουμε ένα αυτο-υπογεγραμμένο πιστοποιητικό, για να δοκιμάσουμε την εφαρμογή SSL και ταυτόχρονα η αρμόδια αρχή υπογράφει το πιστοποιητικό μας. Για να δημιουργήσετε ένα προσωρινό πιστοποιητικό το οποίο είναι καλό για 365 ημέρες, δώστε την ακόλουθη εντολή:

-req -days 365 -in my_req.csr -signkey my_key.key -out my_req.csr

Παρακάτω εμφανίζονται τα screenshots της εκτέλεσης των εντολών.



Εικόνα 89: «Δημιουργία κλειδιού - Αφαίρεση κωδικού- Δημιουργία request-Δημιουργία Πιστοποιητικού»



Εικόνα 90: «Δημιουργία αυτό-υπογεγραμμένου Πιστοποιητικού»

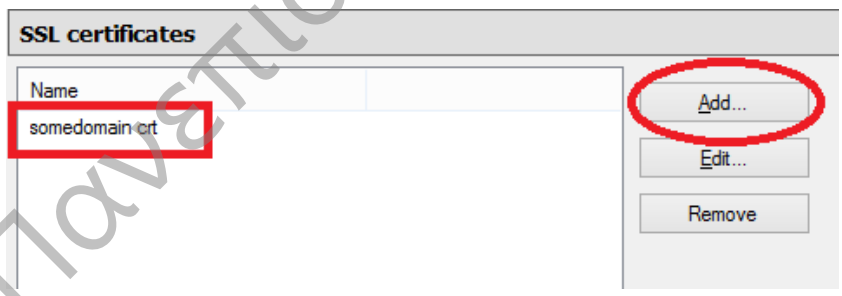
5. **Να ρυθμίσετε τον hMailServer να χρησιμοποιεί το ιδιωτικό κλειδί και το πιστοποιητικό SSL.**

(www.akadia.com)

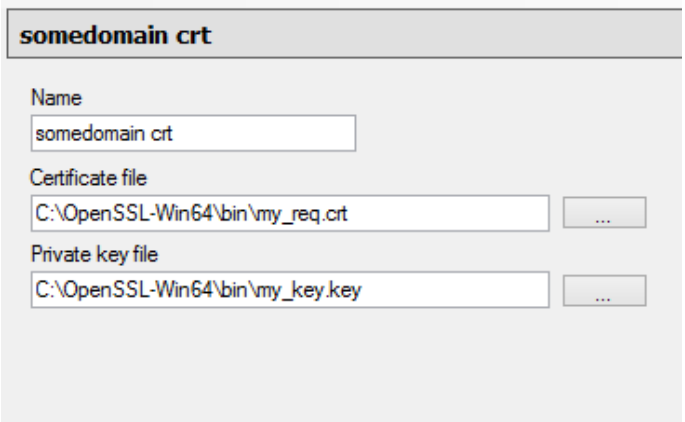
Ρύθμιση του hMailServer να χρησιμοποιεί το OpenSSL

Η ρύθμιση αυτή μπορεί να γίνει σε δύο βασικά σημεία:

a. Ενσωμάτωση του SSL πιστοποιητικού στο hMailServer:
b. Εκκινώντας τον Administrator του hMailServer .
c. Επιλέξτε Add στο πεδίο Settings->Advanced->SSL certificate.
d. Πληκτρολογήστε ένα όνομα για το SSL πιστοποιητικό.
e. Επιλέξτε το αρχείο του πιστοποιητικού και το αρχείο του ιδιωτικού κλειδιού.
f. Αποθηκεύστε τις αλλαγές.



Εικόνα 91: «Ρυθμίσεις Καρτέλας SSl certificates»



Εικόνα 92: «Πρόσθεση Πιστοποιητικού στον hMailServer»

Αφού ολοκληρώσετε αυτές τις ρυθμίσεις πλέον ο hMailServer γνωρίζει για το SSL πιστοποιητικό, αλλά δεν γνωρίζει πότε θα πρέπει να το χρησιμοποιεί. Αυτό θα γίνει ως εξής:

a. Ρύθμιση του hMailServer να χρησιμοποιεί το SSL πιστοποιητικό:

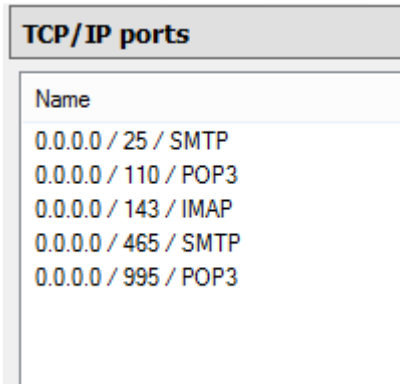
1. Εκκινώντας τον Administrator του hMailServer .
2. Μεταβείτε στο πεδίο **Settings->Advanced->TCP/IP ports.**
3. Επιλέξτε port .
4. Επιλέξτε **"Use SSL"** και το πιστοποιητικό.
5. Αποθηκεύστε τις αλλαγές.
6. Επανεκκινήστε τον t hMailServer.

Αυτό θα έχει ως αποτέλεσμα ότι όλη η κίνηση που αποστέλλονται σε αυτή τη θύρα θα κρυπτογραφούνται με τη χρήση του συγκεκριμένου πιστοποιητικού. Σε αυτό το σημείο θα πρέπει να ρυθμιστούν και όλοι οι πελάτες που συνδέονται σε αυτή τη θύρα θα πρέπει να χρησιμοποιούν το SSL.

Στην περίπτωση μας επιλέξαμε διαφορετικές θύρες για τα πρωτόκολλα ηλεκτρονικού ταχυδρομείου που θα επικοινωνούν με ασφαλή σύνδεση με τον διακομιστή.

Συγκεκριμένα :

i. Θύρα 465 για SMTP
ii. Θύρα 995 για POP3



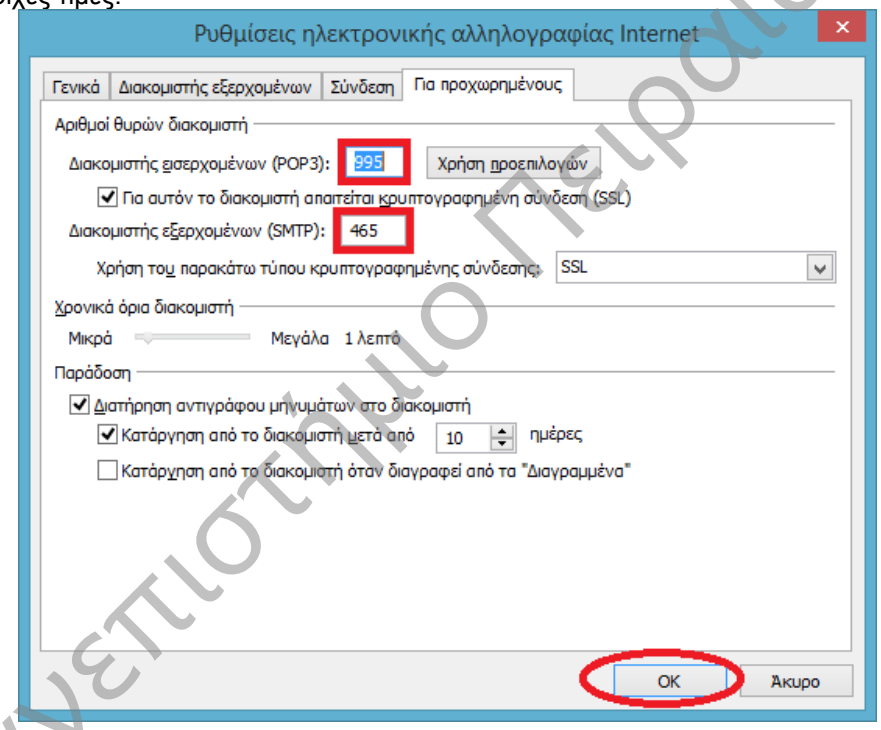
Εικόνα 93: «Ρυθμίσεις Καρτέλας TCP/IP ports»

Ρύθμιση clients

Μετά τη ρύθμιση του hMailServer να χρησιμοποιεί τα SSL πιστοποιητικά, θα πρέπει να ρυθμίσετε και τους clients επίσης. Αυτό για να υλοποιηθεί θα πρέπει να ενεργοποιηθεί αυτή η επιλογή στις ρυθμίσεις λογαριασμών σε κάθε client ξεχωριστά. Εάν επιθυμείτε η SMTP επικοινωνία σας μεταξύ του διακομιστή και των users να είναι κρυπτογραφημένη θα πρέπει να ρυθμιστεί η θύρα TCP/IP για το SMTP να χρησιμοποιεί το SSL.

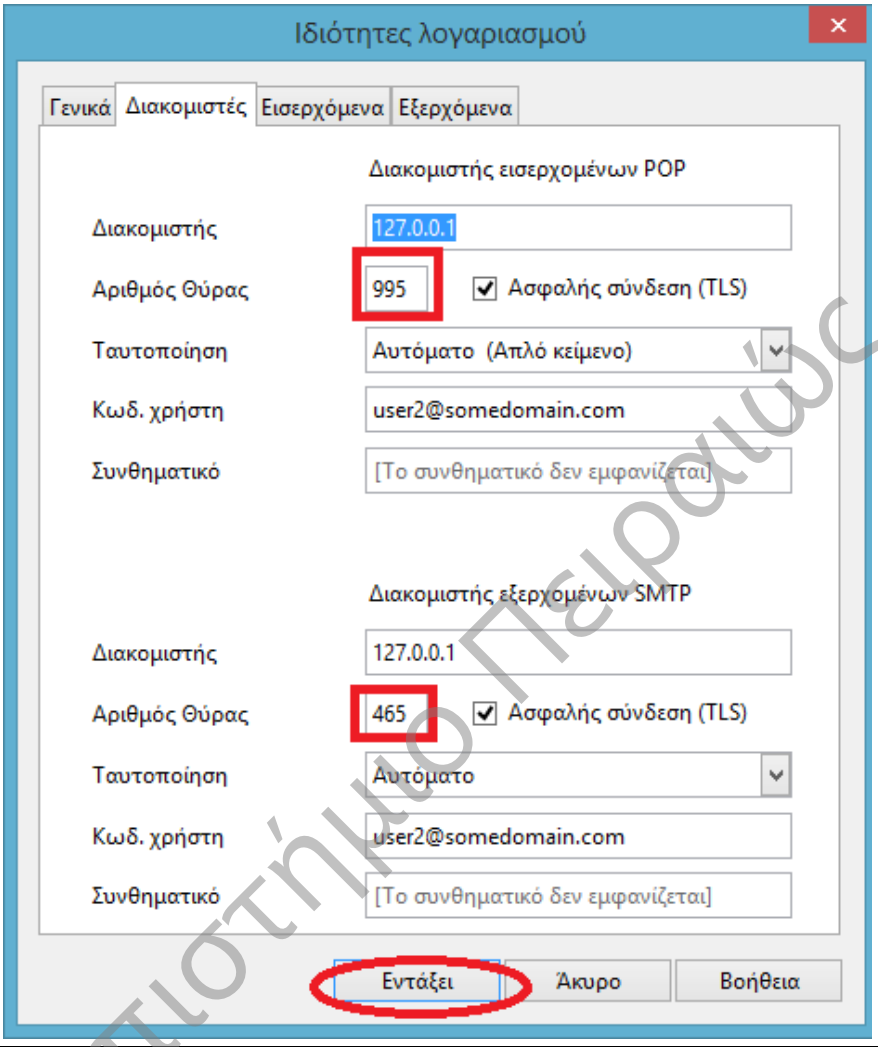
Στην περίπτωση μας ξανά ορίσαμε θύρες επικοινωνίας στους Clients με το διακομιστή και συγκεκριμένα:

i. Για το outlook: Στην διαδρομή Εργαλεία – Ρυθμίσεις Λογαριασμού- (Επιλογή Λογαριασμού) Αλλαγή – Περισσότερες Ρυθμίσεις- και καρτέλα «Για Προχωρημένους» , αλλάζουμε τα πεδία Διακομιστής εισερχόμενων και Διακομιστής εξερχόμενων με τις αντίστοιχες τιμές.



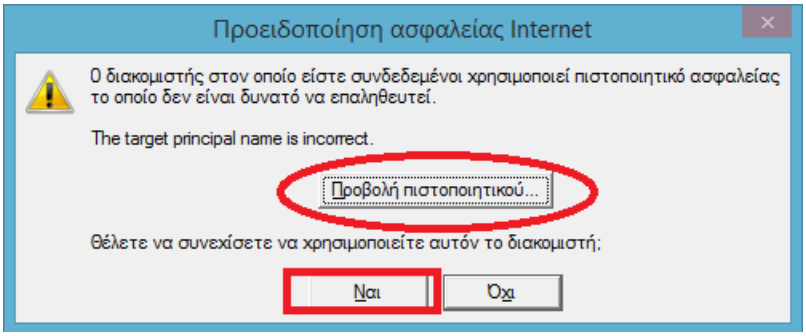
Εικόνα 94: «Ρυθμίσεις διαφορετικών ports στο Outlook»

ii. Για το Opera: Στην διαδρομή Εργαλεία – Λογαριασμοί Αλληλογραφίας - (Επιλογή Λογαριασμού) Επεξεργασία- και καρτέλα «Διακομιστές» και εδώ αλλάζουμε τα πεδία Διακομιστής εισερχόμενων και Διακομιστής εξερχόμενων με τις αντίστοιχες τιμές.

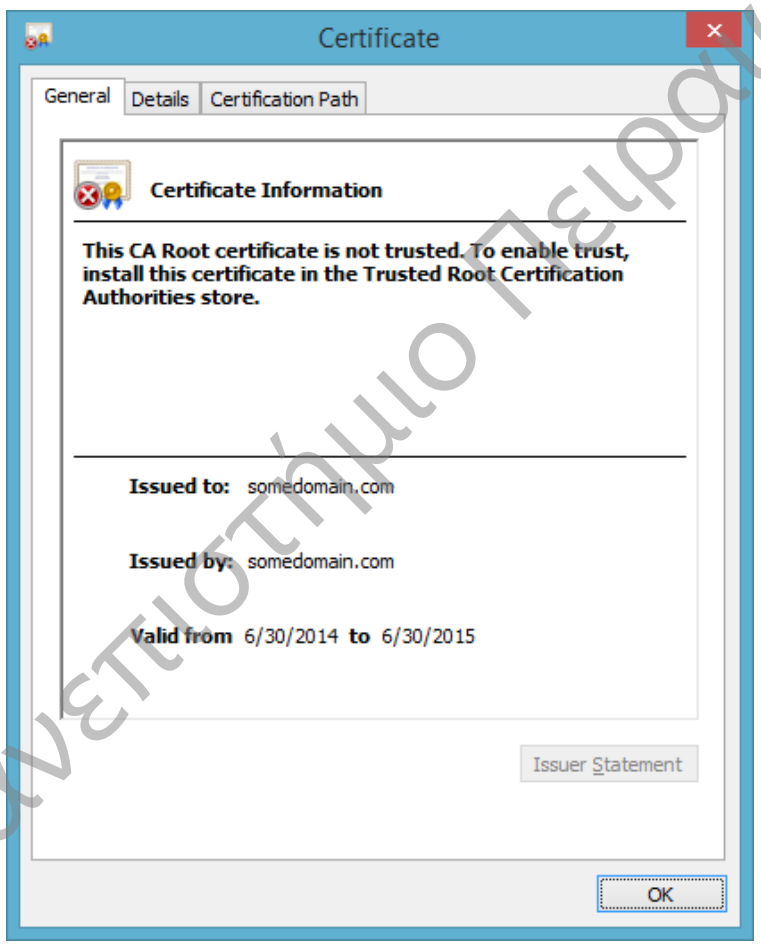


Εικόνα 95: «Ρυθμίσεις διαφορετικών ports στο Opera»

Υλοποιώντας τις παραπάνω ενέργειες από εδώ και πέρα όλοι οι clients πιστοποιούνται στον server και το ανάποδο για μία ασφαλή μετακίνηση δεδομένων. Επειδή πρόκειται για αυτό-υπογεγραμμένο πιστοποιητικό κάθε φορά που θα εκκινείτε ένας client ηλεκτρονικού ταχυδρομείου θα προβάλλεται το μήνυμα ότι ο συγκεκριμένος διακομιστής χρησιμοποιεί πιστοποιητικό και οι χρήστες θα πρέπει να επιλέγουν την προβολή πιστοποιητικού για περισσότερες πληροφορίες και για την συνέχεια επικοινωνίας με τον διακομιστή.



Εικόνα 96: «Προειδοποίηση Ασφάλειας»



Εικόνα 97: «Πιστοποιητικό»

Συστάσεις

Προτείνεται από την επίσημη ιστοσελίδα του hMailServer να χρησιμοποιήσετε κλειδί κρυπτογράφησης RSA.

Εκτιμήσεις Ασφάλειας

Όταν ο hMailServer συνδέεται με έναν άλλο χρησιμοποιώντας SSL (κατά την διάρκεια μιας SMTP παράδοσης ή λήψη emails από εξωτερικό λογαριασμό), δεν ελέγχει τους servers πιστοποιητικών SSL. Αυτό σημαίνει ότι η επικοινωνία μεταξύ του διακομιστή και των client είναι κρυπτογραφημένη και λιγότερο ευπαθής στην υποκλοπή. Αλλά εξακολουθεί να παραμένει ευάλωτη σε μη-εξουσιοδοτημένους χρήστες καθώς δεν επαληθεύεται ότι η επικοινωνία γίνεται με τον σωστό server.

Για να εξασφαλίσετε ότι ο hMailServer θα ελέγξει το πιστοποιητικό των servers θα πρέπει να υλοποιηθούν τα παρακάτω βήματα:

1. Προσδιορίζοντας την αρχή προστασίας που εξέδωσε το πιστοποιητικό του server που είστε συνδεδεμένοι. Αυτό μπορεί να γίνει εκτελώντας την εντολή:
   `openssl s_client -connect ${URL}:${PORT}`
   Π.χ.:
   `openssl s_client -connect pop.gmail.com:995`
   Η Αρχή θα πρέπει να περιλαμβάνεται στο τέλος του πιστοποιητικού.
2. Ανακτώντας το πιστοποιητικό από την ίδια την Αρχή είτε επικοινωνώντας με την Αρχή είτε εξάγοντας το από κάποιο πρόγραμμα περιήγησης Ιστού π.χ. ο Firefox περιλαμβάνει όλα τα πιστοποιητικά το πιο γνωστών Αρχών. Το αρχείο του πιστοποιητικού είναι της μορφής PEM.
3. Υπολογίζοντας την συνάρτηση κατακερματισμού για το συγκεκριμένο πιστοποιητικό. Αυτό μπορεί να γίνει εκτελώντας την εντολή:
   `openssl x509 -in "C:\path\to\ca.pem" -hash`
   Η πρώτη γραμμή θα εμφανίσει την τιμή κατακερματισμού του αρχείου. Π.χ. Η τιμή κατακερματισμού του **Equifax Secure CA** είναι **594f1775**.
4. Μετονομάζοντας το όνομα αρχείου PEM σε <hash>.0 (το όνομα αρχείου θα πρέπει τότε να πάρει την τιμή κατακερματισμού και η επέκταση να είναι 0 (μηδέν). Ξανά στο παράδειγμα του Equifax , το αρχείο θα πρεπεί να έχει το όνομα **594f1775.0.**
5. Τοποθετώντας το αρχείο στο φάκελο C:\Program Files\hMailServer\Externals\CA.
6. Επανεκκινώντας την υπηρεσία του hMailServer.

Μετά από τα παραπάνω βήματα ο hMailServer πάντα θα προσπαθεί να επαληθεύσει τα πιστοποιητικά των server certificate όταν θα συνδέεται στη θύρα SSL. Εάν η επαλήθευση αποτυγχάνει ο hMailServer αυτόματα θα διακόπτει τη σύνδεση.

Ρυθμίσεις

- Όνομα:

  Το όνομα του πιστοποιητικού SSL. Το όνομα χρησιμοποιείται μόνο για την εμφάνιση του πιστοποιητικού και καμία σχέση δεν έχει με το περιεχόμενο καθαυτό.

- Αρχείο Πιστοποιητικού:

  Καθορισμός αρχείου πιστοποιητικού που θα χρησιμοποιεί..

- Ιδιωτικό κλειδί:

  Καθορισμός αρχείου ιδιωτικού κλειδιού που θα χρησιμοποιεί.

Προσοχή….!!! Ο hMailServer δεν θα μπορέσει να διαβάσει το ιδιωτικό κλειδί ένα περιέχει κωδικό πρόσβασης. Βεβαιωθείτε ότι θα έχετε αφαιρέσει το password πρίν ρυθμίσετε τον hMailServer να χρησιμοποιεί αυτό το αρχείο.

5.5 E-MAIL SERVER PENETRATION TESTING

Στα πλαίσια της παρούσας Διπλωματικής θα προσπαθήσουμε να ελέγξουμέ την συμπεριφορά του διακομιστή απέναντι στις απειλές. Παρακάτω αναλύονται δύο διαφορετικά τεστ απέναντι στις πιο δημοφιλείς κατηγορίες απειλών ηλεκτρονικού ταχυδρομείου.

5.5.1 TEST CASE 1 : SPAM PROTECTION- ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΩΝ SPAM

Δοκιμάζουμε να στείλουμε ένα Spam μήνυμα από τον ένα mail user client στον αλλό. Το μήνυμα περνώντας μέσω του διακομιστή μας φιλτραρεται από τους ελέγχους που έχουμε ορίσει και τελικά στέλνεται στον παραλήπτη με την σήμανση SPAM που έχουμε ρυθμίσει στην περιοχή Anti-Spam. Επειδή πρόκειται για τοπικό email server θα χρησιμοποιήσουμε έναν ψευδοκώδικα που αντιμετωπίζεται από τα φίλτρα Ανεπιθυμιτής Αλληλογραφίας ως Spam μήνυμα.

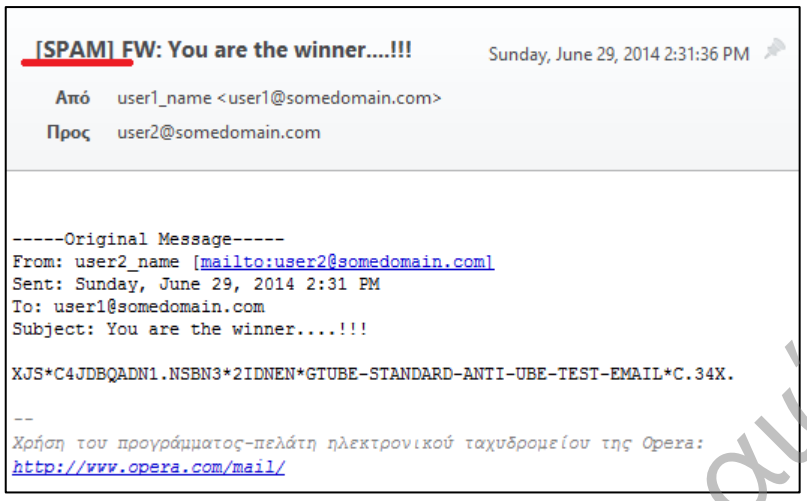
1. Δημιουργούμε ένα νέο email.
2. Αντιγράφουμε το παρακάτω κείμενο στο σώμα του μηνύματος:

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

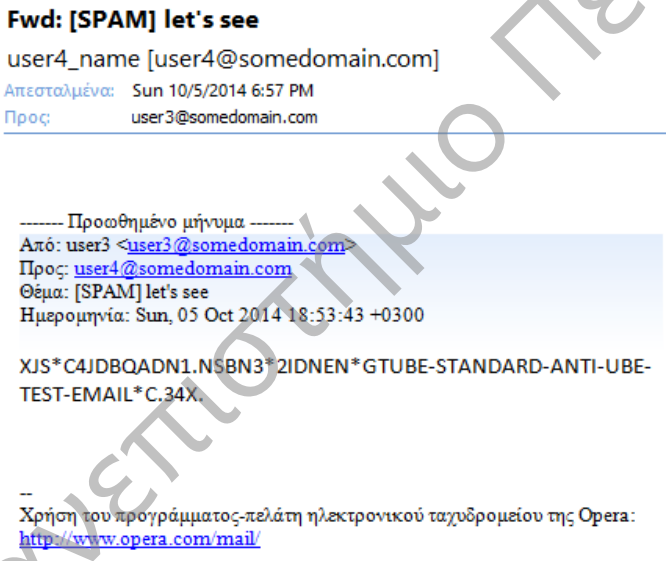
Σημείωση: Βεβαιωθείτε ότι θα το αντιγράψετε με χωρίς επιπλέον κενά ή αλλαγές γραμμής.

3. Από μια διεύθυνση ηλεκτρονικού ταχυδρομείου , στέλνουμε το νέο μήνυμα ηλεκτρονικού ταχυδρομείου σε μια άλλη ηλεκτρονική διεύθυνση στο διακομιστή στον οποίο έχουμε εγκαταστήσει το λογισμικό antispam. Το λογισμικό σαρώνει το μήνυμα, αναγνωρίζει ως μήνυμα ανεπιθύμητης αλληλογραφίας, και να αναλαμβάνει δράση (όπως ορίζεται στις ρυθμίσεις μας).Η δοκιμή GTUBE παρακάμπτει τις μαύρες λίστες και λευκές λίστες.

Όντως συντάσσοντας το μήνυμα στο outlook που είναι ρυθμιζμένος με τον λογαριασμο του user1 και στέλνοντας το στον user2 δηλαδή στο opera mail το μήνυμα χαρακτηρίζεται ως Spam και στέλνεται στον παραλήπτη αυτούσιο προσθέτωντας μόνο μια ταμπελα στο θέμα του μηνύματος που έχουμε ορίσει εμείς και σε αυτήν την περίπτωση προσθέσαμε [**SPAM**] .



Εικόνα 98: «SPAM στο Opera»



Εικόνα 99: «SPAM στο Outlook»

5.5.2 Test case 2 : Virus Protection – Προστασια κατα των Ιων

Σε αυτήν την περίπτωση επειδή είναι ριψοκίνδυνο να ελέγξουμέ την συμπεριφορά του διακομιστή απέναντι σε πραγματικούς ιούς και π]άλι θα χρησιμοποιήσουμε έναν ψευδοκώδικα που αντιμετωπίζεται ως ιος.

1. Δημιουργούμε ένα νέο email.
2. Αντιγράφουμε το παρακάτω κείμενο σε ένα notepad ή οποιοδήποτε επεξεργαστή κειμένου και το σώζουμε με όνομα **EICAR.COM**:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

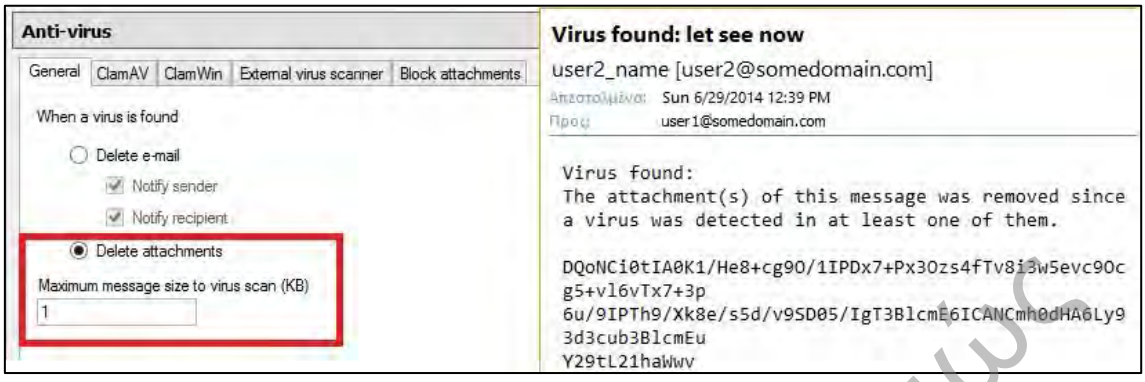
Προσοχή: Θα πρέπει να απενεργοποιήσετε οποιαδήποτε είδους firewall διότι αντιμετωπίζεται ως ιός και αμέσως διαγράφεται. Επίσης δεν θα πρέπει να ξεπερνά το αρχείο τα 68 με 70 bytes.

3. Από μια διεύθυνση ηλεκτρονικού ταχυδρομείου , στέλνουμε το νέο μήνυμα ηλεκτρονικού ταχυδρομείου με συννημένο αρχείο το αρχείο **EICAR.COM** που δημιουργήσαμε. Μόλις το μήνυμα σαρωθεί από το antivirus πρόγραμμα που έχουμε επιλέξει θα πραγματοποιήσει μία εκ των ενεργειών που έχουμε επιλέξει, αυτές είναι:
   - Είτε **θα διαγράψει ολόκληρο το μήνυμα** και θα ενημερώσει ο αποστολέα και παραλήπτη για αυτήν την κίνηση καθώς και το λόγο για το οποίο το μήνυμα έχει διαγραφεί.
   - Είτε **θα διαγράψει μόνο το συννημένο αρχείο** που θεωρεί μολυσμένο , προσθέτοντας και την αιτία αφού ενημερώσει και πάλι τον παραλήπτη.

a. Delete e-mail

Εικόνα 100: «Delete e-mail σε περίπτωση ιού»

b. Delete attachments



Εικόνα 101: «Delete attachments σε περίπτωση ιού»

Παρατηρούμε ότι ο διακομιστής και στις δύο περιπτώσεις αλλά και στους δύο clients επιτυχώς εντοπίζει τον ιό.

(Intoolbox, 2010)

5.6 Μετρα Ασφαλειας απο Πλευρας Χρηστη

Έχοντας εγκαταστήσει το OpenSSl στον διακομιστή μας καταφέραμε να κρυπτογραφήσουμε την συνομιλία μεταξύ χρηστών και διακομιστή καθώς και να πιστοποιήσουμε στους χρήστες ότι συνδέονται με διακομιστή ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί πιστοποιητικό. Άλλα δεν έχουμε λάβει μέτρα ασφάλειας στην περίπτωση επικοινωνίας με χρήστες που ανήκουν σε άλλους διακομίστες. Για να διασφαλιστεί η ακεραιότητα, η εμπιστευτικότητα ενός μηνύματος και πιστοποίηση αποστολέα θα χρησιμοποιήσουμε ένα εργαλείο τεχνολογίας OpenPGP το **gpg4win** έκδοση 0.9.4 για Windows.

5.6.1 Εγκαταστση OpenPGP

Το **Gpg4win** επιτρέπει στους χρήστες να μεταφέρουν με ασφάλεια μηνύματα και αρχεία με τη βοήθεια της κρυπτογράφησης και ψηφιακών υπογραφών. Προσφέρει ασφάλεια και ακεραιότητα περιεχομένου και ταυτοποίηση αποστολέα. Υποστηρίζει τόσο τα σχετικά πρότυπα κρυπτογράφησης, OpenPGP και S / MIME (X.509), αλλά είναι και η επίσημη διανομή GnuPG για τα Windows. Συντηρείται από το GnuPG και το λογισμικό που περιλαμβάνεται είναι ελεύθερο και

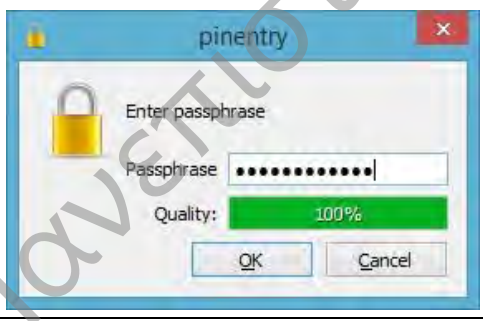
Εικόνα 102: «gpg4win»

υποστηρίζεται από τη Γερμανική Ομοσπονδιακή Υπηρεσία Ασφάλειας Πληροφοριών (BSI).
Η έκδοση Gpg4win για τα Windows και περιέχει και άλλα εργαλεία όπως:

- **GnuPG**: που είναι ο πυρήνας-το πραγματικό εργαλείο κρυπτογράφησης.
- **Kleopatra** : ένας διαχειριστής πιστοποιητικών OpenPGP και X.509 (S / MIME).
- **GPA** : ένα εναλλακτικό εργαλείο διαχείρισης πιστοποιητικών OpenPGP και X.509 (S / MIME).
- **GpgOL**: ένα plugin για το Microsoft Outlook 2003/2007/2010/2013 (κρυπτογράφηση ηλεκτρονικού ταχυδρομείου).
- **GpgEX**: ένα plugin για το Microsoft Explorer (κρυπτογράφηση αρχείων).
- **Claws Mail**: μια ολοκληρωμένη εφαρμογή ηλεκτρονικού ταχυδρομείου με υποστήριξη κρυπτογραφίας.
- **Gpg4win Compendium**: μία τεκμηρίωση (για αρχάριους και προχωρημένους χρήστες), διατίθεται στα αγγλικά και τα γερμανικά.

Έχοντας ολοκληρώσει την εγκαταστάση του λογισμικού **gpg4win** από την επίσημη ιστοσελίδα του: http://www.gpg4win.org/ αυτό δημιουργεί μια επιπλέον δυνατότητα στα Windows με την οποία οι χρήστες μπορούν να κάνουν **Sign and Encrypt** σε κάθε αρχείο μέσα στον υπολογιστή τους από το υπομενού του δεξιού. Αυτό προϋποθέτει φυσικά την δημιουργία ζεύγους κλειδιών και την εισαγωγή του δημοσίου κλειδιού του παραλήπτη στο **Key Manager** του λογισμικού , αυτό γίνεται ως εξής:

- Δημιουργούμε ένα ζεύγος κλειδιών (ιδιωτικό για αποκρυπτογράφηση- δημόσιο για δημοσίευση και κρυπτογράφηση) ακολουθώντας τα βήματα του οδηγού κατά την πρώτη φορά εκκίνησης του προγράμματος ή από την γραμμή μενού επιλέγουμε **Keys- New Key**.
- Κατά την δημιουργία του ζεύγους κλειδιών μας ζητάει ένα όνομα και την διεύθυνση email για την οποία θα δημιουργηθούν τα κλειδιά.
- Όταν ολοκληρωθεί η διαδικασία δημιουργίας κλειδιών μας ζητείται ένας κωδικός για το ιδιωτικό κλειδί που θα πρέπει να συμπληρώνουμε κατά την διαδικασία αποκρυπτογράφησης του μηνύματος μας.



Εικόνα 103: Εισαγωγή κωδικού για το ιδιωτικό κλειδί

- Τέλος μπορούμε να αποθηκεύσουμε το κλειδί σε όποιο σημείο επιθυμούμε μέσα στον υπολογιστή μας και να το στείλουμε στον παραλήπτη που θέλουμε να επικοινωνούμε με κρυπτογρφημένα μηνύματα ή με την μορφή επισυνναπτόμενου αρχείου ή ανοίγοντας το με ένα πρόγραμμα κειμένου και αντιγράφοντας το περιεχόμενο στο σώμα ενός μηνύματος.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFQ7+88BCACjXLj8aWGMKmFuf8myqOenpoFF1OSXaEvDdclzrTLDWQDxs9Nr
01OcdcvSgZTGgrFZeAjuXz93jTfNngycjNaPnM6YfoyOpK09cLpKhXFeE8L1FYjf
IT4Uq3ggkl9evZIHLyMhY5EdUoOAH3QNq9p1p8ZAK47HQtRd7JrA94z83qRcT73j
sSmpSh/ZzTEy+JbZi720S3KJddd7jH/ixdPKD4NFdnw3pVSzQ1I2dkVQRe8a/YK5
rR4Lp8ukLKYna3k7+mpe+HvvzSJRNHZAngAVEbBASjGB2tsXBGdJ3DhHfvwzRw5v
3rmoQ3gKfkK1cLSZvUce4iVygTbSvrcDv813ABEBAAG0HFVzZXIxIDx1c2VyMUBz
b211ZG9tYWluLmNvbT6JATkEEwECACMFAlQ7+88CGwMHCwkIBwMCAQYVCAIJCgsE
FgIDAQIeAQIXgAAKCRAmaeitr+8ejTxDB/kBompV/hzv4ygP98EmJJQyR/Gol8dH
thLjDHwIjiF3+dDQO3NAxa1zaODHurD6drtAFmeLMGZas0syn9kLHKTTBjcA+w8b
gVZwfr8LRs/pgTPBJ64YLa1Nhqbzwn9YpZDvT+hdU+ZTYMEzoo8kilDjhuFHwlqd
X4gE8m48WsSNXE8fAoGA/P2US6aiiLSr5j7ISeEI7ewk9wHHD0WZYEHTX6KLawRV
GaGnE2SQBqr3O1DXcsWIr0iXOGreGgJQDoxWEyEApzPnNt/p/Mmd3amf4UweRwVg
rSjp9ZTRd8nPqPjcF6Qk881d8XUgsVWZ//wQquy5KU5/qlKVqNKO50ZvuQENBFQ7
+88BCADZw0Nv6KhwgqnmHgq21fplHmlL1OlpUj7xIbL4XOz70tqOAo3c/W0jxw/y
DZCdqmJ8BafoFRPAcYinLRKPcUp7JVv0ApQgfUCYoxZWbKhpJwhdIOEm4E8rkomM
UYZTZR7SGnRazubF1YuXLAVPbrVMWsUdE03Ar1f8fqTxrRc+Uhc2HiOuKsgnsewY
GckM240kyGGdnDzH+EX0w3a13wtQOcl700h2xEPFPevA+Sfu9Xcmb69P24nzaC+8
vdRL1p4efEQig68Iy18EErrRsqlqzkk0slmes1ja0sIjaSR2/xkb9xr6O7MGFRnt
WLVF/8bvXCkvjvPat89MBv9h8oObABEBEBAAGJAR8EGAECAAkFAlQ7+88CGwwACgkQ
Jmnora/vHo1nIQf/cKjdppQ+JJz5+Tf81C4D/1Yrcmiz4/3bZRZgGqTUC9evkYQj
l6dVuij//c125J6lEDhj+d4t1bb+5Dw0fHK+5+KVnC1Tjbe5/Qk0WeGQ+TdFVm6L
08R5fjs+dc4rw/3xMktZZfgpjs4Roy2xdrBqfRmSrC1MZw2Znf5L6AjLWkIhVoCX
Ld3oZpPku8TDGRAVCLId3R+UWhXBwxl+OYz4hVvL1ptHsmu6VEtau+bc30KSrgod
rGp5Z7nu9u5+GvHG9inp6CwbAzckVutpIVfR31N86baeNiaAul5vMDONpvMT8qWI
MHgejIgRRRnfFtk0kcnhIi1etSktfGI9kY1J0A==
=Dein
-----END PGP PUBLIC KEY BLOCK-----
```

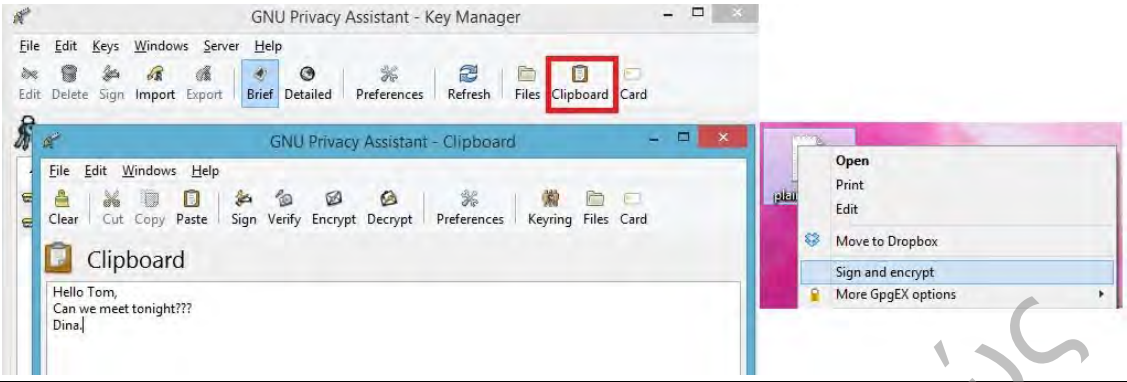
Εικόνα 104: «Μορφή του δημόσιου κλειδιού»

5.6.2 Κρυπτογραφηση με gpg4win και αποστολη μεσω Hmailserver

Στην περίπτωση του hmailserver δεν χρειάζεται κάποια ειδική ρύθμιση καθώς πρόκειται απλά για ένα κρυπτογραφημένο μήνυμα που θα μεταφερθεί μέσω του διακομιστή που έχουμε εγκαταστήσει σαν ένα απλό μήνυμα.

Για να γίνει μια αποστολή και παραλαβή μηνύματος με ασύμμετρη κρυπτογραφία θα πρέπει να έχουμε εισάγει το δημόσιο κλειδί του παραλήπτη στον Key Manager, το οποίο μπορούμε να το βρούμε είτε από κάποια σελίδα που το έχει αναρτήσει είτε το εχουμε αποκτήσει μέσω email από τον ίδιο. Η περίπτωση υποκλοπής της συνομιλίας δεν διακινδυνεύει την κρυπτογραφία διότι πρόκειται για το δημοσίο κλειδί. Οπότε τα βήματα μιας επιτυχημένης συνομιλίας είναι:

- Αφού έχουμε αποκτήσει το αρχείο με το κλειδί του παραλήπτη ,επιλέγουμε στον Key Manager **Keys- Import Keys** και επιλέγουμε το αρχείο.
- Στην συνέχεια έχουμε δύο τρόπους να κρυπτογραφήσουμε ένα μήνυμα είτε γράφωντας σε ένα αρχείο και αποθηκεύοντας το και επιλέγοντας **Sign and Encrypt** είτε από την επιλογή Clipboard μέσα από τον Key Manager που μπορούμε απευθείας να γράψουμε, όπως φαίνεται στην επόμενη φωτογραφία.



Εικόνα 105: Encrypt & Sign

- Με την επιλογή **Sign and Encrypt,** ανοίγει το επιπλεόν λογισμικό Cleopatra στο οποίο επιλέγουμε το Δημόσιο κλειδί που θα κρυπτογραφήσουμε και κάνουμε Add και εκτελούμε την εντολή.
- Αποστέλουμε το μήνυμα που στην περίπτωση του αρχείου θα μας έχει φέρει σαν αποτέλεσμα ένα αρχείο με το ίδιο όνομα αλλά επέκταση .pgp ενώ στην περίπτωση του Clipboard μας εμφανίζει απευθείας το κρυπτογραφημένο κείμενο, όπου το αντιγράφουμε στο μήνυμα ηλεκτρονικού τα χυδρομείου.
- Στην περίπτωσή της αποκρυπτογράφησης απλά επιλέγουμε **Decrypt & Verify** και εισάγουμε το κωδικό για το ιδιωτικό κλειδί εκτελώντας τα ίδια βήματα.

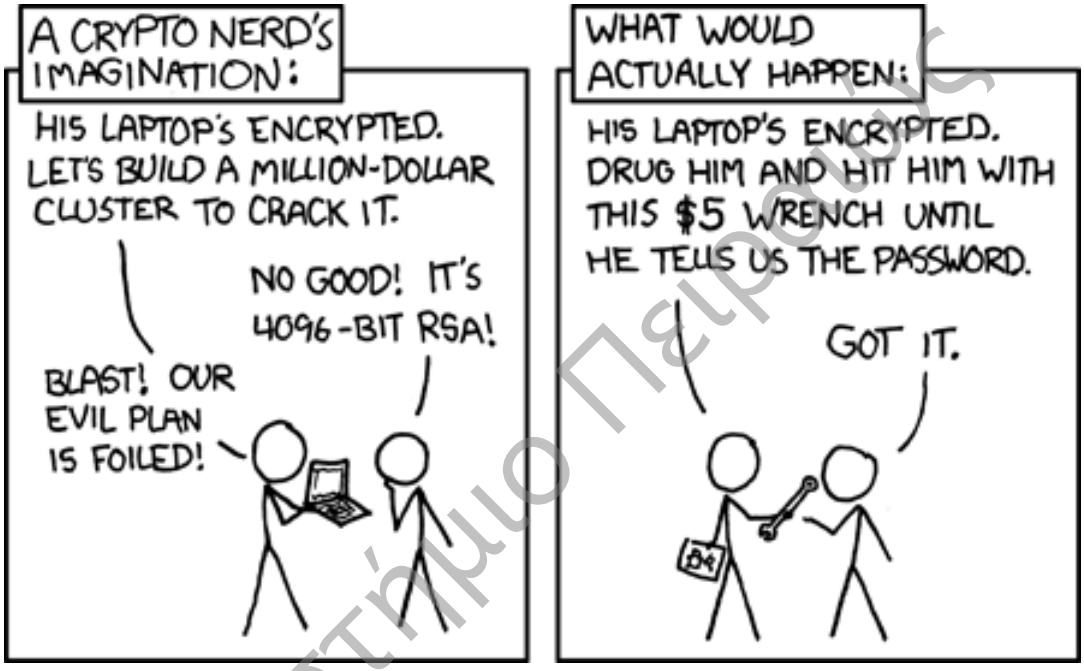
6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα Διατριβή έγινε διεξοδική μελέτη όλων των εννοιών που περιλαμβάνονται στον μηχανισμό του Ηλεκτρονικού Ταχυδρομείου. Στην συνέχεια αναλύθηκε η αρχιτεκτονική του Email σε δύο άξονες, στον πρώτο έγινε ανάλυση των ανεξάρτητών πρακτόρων – agent και των ρόλων τους κατά την διάρκεια της μεταφοράς ενός μηνύματος και στον δεύτερο αναλύθηκε το ίδιο το μήνυμα πως διασπάται και περνά από τα επίπεδα OSI και επανασυναρμολογείται στην πλευρά του τελικού χρήστη.

Στην συνέχεια παρουσιάστηκαν τα πρωτόκολλα που ορίζονται από το TCP/IP για την μορφή και μεταφορά ηλεκτρονικής αλληλογραφίας.

Στα επόμενα κεφάλαια εντοπίστηκαν οι ευπάθειες του Ηλεκτρονικού Ταχυδρομείου και πως αυτές εκμεταλλεύονται από τους παράνομους χρήστες. Υλοποιώντας όλα τα εργαλεία που ορίζονται από την Ασφάλεια Πληροφοριακών Συστημάτων και τον τομέα της Κρυπτογραφίας καταλήγουμε στον συμπέρασμα ότι κατά αρχήν το Ηλεκτρονικό Ταχυδρομείο είναι ένας πανίσχυρος μηχανισμός ο οποίος μπορεί να αποτελέσει και πολύ αποτελεσματικός μηχανισμός στην περίπτωση που χρησιμοποιείται για δόλιους σκοπούς. Λόγω της απλότητας και αποτελεσματικότητας του είναι πολύ πιθανόν να συνεχιστεί η κακή χρήση του όποτε είναι απαραίτητη και η συνεχής εξέλιξη μηχανισμών και φίλτρων για την ανίχνευση ιών και spam. Εν συνεχεία συμπεραίνουμε ότι η Κρυπτογραφία είναι ό πιο αποτελεσματικός τρόπος προστασίας του χρήστη στην ανταλλαγή μηνυμάτων.

Αυτό που αντιμετωπίζεται στην πλειοψηφία των μηνυμάτων αλλά δεν μπορεί να αντιμετωπιστεί πλήρως είναι η προστασία του χρήστη από τα spam καθώς αυτός ο χαρακτηρισμός σε κάποιες περιπτώσεις είναι και υποκειμενικός. Το οικειοθελές αίτημα του χρήστη για ενημέρωση προϊόντων ή υπηρεσιών μέσω newsletters ή εγγραφή του σε λίστες email δεν μπορεί εύκολα να το διακρίνει ένας σαρωτής. Με λίγα λόγια δεν υπάρχει αυστηρός διαχωρισμός μεταξύ επιθυμητής και ανεπιθύμητης αλληλογραφίας.



(Πηγή εικόνας: http://www.makeuseof.com/tag/3-secure-encrypted-email-providers-online/)

7 Βιβλιογραφια

A. Menezes, P. v. (August 2001). *Applied Cryptography .* CRC Press.

Alliance, O. (n.d.). *OpenPGP Alliance*. Ανάκτηση από OpenPGP Alliance: http://www.openpgp.org/

Alter Procedure. (n.d.). Ανάκτηση από How To Configure SpamAssassin for HMailserver in Windows Server 2003: http://www.alterprocedure.net/articles/alterprocedure/how-to-configure-spamassassin-for-hmailserver-in-windows-server-2003.aspx

Alter Procedure. (n.d.). Ανάκτηση από The best SPAM settings for hMailServer: http://www.alterprocedure.net/articles/alterprocedure/the-best-spam-settings-for-hmailserver.aspx

Anti-Spamming. (n.d.). Ανάκτηση από Anti-Spamming: http://www.no-spam.gr/index.php

Barb. (2013, July 06). *DNS Propagation Life Cycle – The Process.* Ανάκτηση από webhosting.uk.com: http://blog./web-hosting/dns-propagation-life-cycle-the-process/

Behrouz A. Forouzan, S. C. (2005). *Πρωτόκολλο TCP/IP.* Γκιούρδας Μ.

Casad, J. (2009). *Μάθετε το TCP/IP σε 24 ώρες.* Indianapolis: Γκιούρδας Μ.

Checking your outgoing mail server (Is Port 25 blocked?). (n.d.). Ανάκτηση από https://kb.mediatemple.net/questions/888/Checking+your+outgoing+mail+server+%28Is+Port+25+blocked%3F%29

Comer, D. E. (2001 4η Αμερικάνικη Έκδοση). *Διαδίκτυα με TCP/IP Αρχές, πρωτόκολλα, και αρχιτεκτονικές.* Κλειδάριθμος .

Cyprus, U. o. (n.d.). *Cryptography*. Ανάκτηση από Cryptography: http://www.cs.ucy.ac.cy/courses/EPL698/lecture1_Introduction.pdf

Dinesh. (n.d.). *Install and Enable Telnet in Windows 8 & 8.1 – Use The Telnet Client Utility*. Ανάκτηση από http://www.sysprobs.com/install-and-enable-telnet-in-windows-8-use-as-telnet-client

Dinesh. (n.d.). *Install and Enable Telnet in Windows 8 & 8.1 – Use The Telnet Client Utility*. Ανάκτηση από http://www.sysprobs.com/install-and-enable-telnet-in-windows-8-use-as-telnet-client

hMailServer. (n.d.). *hMailServer Documentation*. Ανάκτηση από hMailServer.

How to Set up a Free Local Email Server. (2011, Οκτώβριος). Ανάκτηση από CyberStream.US: http://www.cyberstream.us/post/2011/10/how-to-set-up-an-email-server-locally

Jonathan B. Postel-Information Sciences Institute University of Southern California. (1982, August). *ietf.org.* Ανάκτηση από RFC 821-SIMPLE MAIL TRANSFER PROTOCOL: http://tools.ietf.org/html/rfc821#page-1

Koymans, K. (2010, September 30). *Informatics Institute University of Amsterdam.* Ανάκτηση από Informatics Institute University of Amsterdam: https://www.os3.nl/_media/2010-2011/courses/cia/week3/email_handout.pdf

Kurose&Ross. (2008). *Δικτύωση Υπολογιστών.* USA: Μ. Γκιούρδας.

LinuxQuestions.org. (2009, 10 14). *Mail submission agent*. Ανάκτηση από Mail submission agent: http://wiki.linuxquestions.org/wiki/Mail_submission_agent

Intoolbox. (2010, August Wednesday). *HowTo: Test AntiSpam & Antivirus*. Ανάκτηση από HowTo: Test AntiSpam & Antivirus: http://www.Intoolbox.com/en/categories/other/214-howto-test-antispam-a-antivirus.html

MCCLURE, S. (2009). *Hacking Exposed 6: Network Security Secrets & Solutions.* McGraw-Hill Companies.

Peterson&Davie. (2008). Δίκτυα Υπολογιστών. Κλειδάριθμος.

Porter, C. (2012). *Email Security with Cisco IronPort.* Indianapolis,USA: Cisco Press.

Protogenist. (n.d.). *How does NDR Spam work*. Ανάκτηση από How does NDR Spam work: http://protogenist.wordpress.com/2012/09/11/how-does-ndr-spam-work/

Quinn, M. J. (2012). *Ethics for Information Age.* New Jersey: Addison-Wesley.

S.Tanenbaum, A. (1996). *ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ 3η ΕΚΔΟΣΗ.*

SecureList. (n.d.). *Types of spam.* Ανάκτηση από Types of spam: http://www.securelist.com/en/threats/spam?chapter=88

SMTP Port – How to Check if SMTP Port 25 is Blocked. (n.d.). Ανάκτηση από http://kb.siteground.com/smtp_port_25_blocked/

Stallings, W. (2011). *ΕΠΙΚΟΙΝΩΝΙΕΣ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ.* Τζιόλα.

Symantec. (n.d.). *Spam Categories*. Ανάκτηση από Spam Categories: http://www.symantec.com/popup.jsp?popupid=sr_spam_categories

Techblog.gr. (2007, Μαϊος 16). *Κατηγορίες spam σε παγκόσμιο επίπεδο.* Ανάκτηση από Κατηγορίες spam σε παγκόσμιο επίπεδο: http://techblog.gr/internet/symantec-spam-categories/

Vicomsoft. (2002). *Vicomsoft Ltd.* Ανάκτηση από Vicomsoft Ltd: http://www.vicomsoft.com/learning-center/email-and-email-servers/

Wikipedia. (2008). *Simple Mail Transfer Protocol.* Ανάκτηση από Simple Mail Transfer Protocol: http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Wikipedia. (n.d.). *Computer virus*. Ανάκτηση από Computer virus: http://en.wikipedia.org/wiki/Computer_virus

Wikipedia. (n.d.). *Cryptography*. Ανάκτηση από Cryptography: http://en.wikipedia.org/wiki/Cryptography

Wikipedia. (n.d.). *Cryptography*. Ανάκτηση από Cryptography: http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

Wikipedia. (n.d.). *Email*. Ανάκτηση από Email: http://en.wikipedia.org/wiki/Email

Wikipedia. (n.d.). *Email address*. Ανάκτηση από Email address: http://en.wikipedia.org/wiki/Email_address

Wikipedia. (n.d.). *Email appending*. Ανάκτηση από Email appending: http://en.wikipedia.org/wiki/Email_appending

Wikipedia. (n.d.). *Email client*. Ανάκτηση από Email client: http://en.wikipedia.org/wiki/Mail_user_agent

Wikipedia. (n.d.). *Email hacking*. Ανάκτηση από Email hacking: http://en.wikipedia.org/wiki/Email_hacking

Wikipedia. (n.d.). *Email spam*. Ανάκτηση από Email spam: http://en.wikipedia.org/wiki/Email_spam

Wikipedia. (n.d.). *Internet Message Access Protocol*. Ανάκτηση από Internet Message Access Protocol: http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

Wikipedia. (n.d.). *Mail submission agent*. Ανάκτηση από Mail submission agent: http://en.wikipedia.org/wiki/Mail_submission_agent

Wikipedia. (n.d.). *Message transfer agent*. Ανάκτηση από Message transfer agent: http://en.wikipedia.org/wiki/Mail_Transfer_Agent

Wikipedia. (n.d.). *MX record*. Ανάκτηση από MX record: http://en.wikipedia.org/wiki/MX_records

Wikipedia. (n.d.). *Phishing*. Ανάκτηση από Phishing: http://en.wikipedia.org/wiki/Phishing

Wikipedia. (n.d.). *Phishing*. Ανάκτηση από Phishing: http://en.wikipedia.org/wiki/Phishing

Wikipedia. (n.d.). *Post Office Protocol*. Ανάκτηση από Post Office Protocol: http://en.wikipedia.org/wiki/Post_Office_Protocol

Wikipedia. (n.d.). *Pretty Good Privacy*. Ανάκτηση από Pretty Good Privacy: http://en.wikipedia.org/wiki/Pretty_Good_Privacy

Wikipedia. (n.d.). *RSA (cryptosystem)*. Ανάκτηση από RSA (cryptosystem): http://en.wikipedia.org/wiki/RSA_(cryptosystem)

Wikipedia. (n.d.). *Διαδίκτυο-Νομικά και ηθικά ζητήματα*. Ανάκτηση από http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

wikipedia. (n.d.). *Κρυπτογραφική Συνάρτηση Κατατεμαχισμού*. Ανάκτηση από Κρυπτογραφική Συνάρτηση Κατατεμαχισμού: http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%B9%CE%BA%CE%AE_%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%9A%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D

Wikipedia. (n.d.). *Κρυπτογραφικοί Αλγόριθμοι Ροής*. Ανάκτηση από Κρυπτογραφικοί Αλγόριθμοι Ροής: http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%B9%CE%BA%CE%BF%CE%AF_%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CE%B9_%CE%A1%CE%BF%CE%AE%CF%82

Workaround.org. (n.d.). *Test fetching emails with IMAP and POP3* . Ανάκτηση από Test fetching emails with IMAP and POP3 : https://workaround.org/ispmail/lenny/test-fetching-with-imap-and-pop3

www.akadia.com. (n.d.). *www.akadia.com*. Ανάκτηση από : http://www.akadia.com/services/ssh_test_certificate.html

Youtube . (n.d.). Ανάκτηση από instalando spamassasin como servicio antispam en hmailserver: https://www.youtube.com/watch?v=eYtA8wMaf9w

Ανεπιθύμητη Αλληλογραφία . (n.d.). Ανάκτηση από Ανεπιθύμητη Αλληλογραφία : http://www.sch.gr/sch-portlets/static/manual/aboutSpam/index.php?_list=whatis

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. (n.d.). Ανάκτηση από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL

Αστυνομία, Ε. (n.d.). *Ηλεκτρονικό Έγκλημα* . Ανάκτηση από Ηλεκτρονικό Έγκλημα : http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN

Γκρίτζαλης Δημήτρης, Γ. Σ. (2003). *Ασφάλεια δικτύων υπολογιστών.* Αθήνα: Παπασωτηρίου.

Ε.Κ.ΚΦ.Ε.ΔΗΜΟΚΡΙΤΟΣ. (n.d.). *Internet Systematics*. Ανάκτηση από Internet Systematics: http://www.islab.demokritos.gr/gr/html/

Ζαρκάδης, Β. (n.d.). Κρυπτογραφία Διδακτορική Διατριβή. Πανεπιστήμιο Αιγαίου.

Κοτζανικολάου, Π. (2012). *Ασφάλεια Πληροφοριών.* Πειραιά: Παν.Πειραιώς.

Λιμνιώτης, Δ. Κ. (n.d.). *Κυπτογραφία.* Ανάκτηση από http://cgi.di.uoa.gr/~klimn/cryptography/chapter_1-General_Overview.pdf

Μάγκος, Δ. Ε. (2007). *Ασφάλεια Υπολογιστών και Προστασία Δεδομένων Σημειώσεις Μαθήματος Δ' Εξαμήνου.* Κέρκυρα: Τμήμα Πληροφορικής Ιόνιο Πανεπιστήμιο.

Μαργαρίτη, Σ. (2007). *Τοπικά & Αστικά Δίκτυα (LAN-MAN).* Αθήνα: ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ.

Παν.Θεσσαλίας. (n.d.). *Ηλεκτρονικό Ταχυδρομείο (E-mail)*. Ανάκτηση από Ηλεκτρονικό Ταχυδρομείο (E-mail): http://www2.uth.gr/main/help/help-desk/email/e-mail2.html

ΠΛΗΝΕΤΝ, Κ. (n.d.). *Οι Ιοί (Viruses) των Υπολογιστών*. Ανάκτηση από Οι Ιοί (Viruses) των Υπολογιστών: http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html

Πληροφορική_Online. (n.d.). *Ταξινόμηση κρυπτογραφικών εργαλείων*. Ανάκτηση από Ταξινόμηση κρυπτογραφικών εργαλείων: http://pliroforiki-online.blogspot.gr/2013/05/taxinomisi-kriptografikon-ergaleion.html