Περί Ηλεκτρονικού Ταχυδρομείου.

Νίκος Μαυρογιαννόπουλος

Δεκεμβριος 2000

Το ηλεκτρονικό ταχυδρομείο (ή πιο απλά e-mail) είναι μία από τις υπηρεσίες του internet που χρησιμοποιούνται περισσότερο. Σίγουρα δεν υπάρχουν πολλοί που να μην ξέρουν, πάνω κάτω, που χρησιμεύει και πως λειτουργεί. Εδώ θα δούμε με κάποια μεγαλύτερη λεπτομέρεια πως λειτουργεί και τι (δεν) μπορεί να μας προσφέρει.

1. Συγγραφή

Η διαδικασία της αποστολής ενός ηλεκτρονικού μηνύματος είναι σχετικά απλή, και μπορούμε να την παρομοιάσουμε με την διαδικασία αποστολής ενός κανονικού γράμματος. Αποστολέας και παραλήπτης έχουν μία μοναδική ηλεκτρονική διεύθυνση που τους χαρακτηρίζει. Όπως θα έχετε δει οι περισσότεροι οι διευθύνσεις είναι της μορφής <**name@provider.gr**>. Το πρώτο μέρος της διεύθυνσης (πριν το @) είναι το όνομα χρήστη σε κάποιον παροχέα Internet, ενώ το δεύτερο μέρος εξαρτάται από το όνομα του παροχέα στο Σύστημα Ονομασίας τομέων (DNS).

Όπως ένα γράμμα έτσι και το ηλεκτρονικό γράμμα πρέπει υποχρεωτικά να έχει τα πεδία του αποστολέα, του παραλήπτη και της ημερομηνίας συμπληρωμένα, σύμφωνα με την πρώτη προσπάθεια τυποποίησης των ηλεκτρονικών γραμμάτων (RFC 822).

Αργότερα με τις **MIME** (ή Multipurpose Internet Mail Extensions, RFC 2045 και 2046) επεκτάσεις, προστέθηκαν και άλλα πεδία που καθορίζουν το character set που χρησιμοποιήθηκε στο περιεχόμενο του μηνύματος κλπ. Αυτές οι πληροφορίες αποθηκεύονται στις επικεφαλίδες του γράμματος (headers), και αντιστοιχούν στις πληροφορίες που γράφουμε στο εξωτερικό ενός ταχυδρομικού φακέλου. Οι επικεφαλίδες συνήθως δημιουργούνται από το πρόγραμμα αποστολής γραμμάτων και δεν είναι ορατές πάντα στους αναγνώστες και τους αποστολείς.

Ας δούμε όμως πως είναι η πλήρης μορφή ενός τυπικού ηλεκτρονικού γράμματος:

```
X-Mailer: XFMail 1.3 [p0] on Linux
X-Priority: 3 (Normal)
Content-Type: text/plain; charset=ISO-8859-7
Content-Transfer-Encoding: 8bit
```

```
MIME-Version: 1.0
Date: Sun, 05 Mar 2000 02:02:08 +0200 (EET)
From: "Mister A" <mistera@hellug.gr>
To: Mister B <misterb@linux.gr>
Subject: hello

... Αυτο ειναι ενα τυπικο γραμμα με ελληνικους χαρακτηρες ...
```

Τα πεδία που αρχίζουν με **X-** είναι προαιρετικά πεδία που εξαρτώνται από τον αποστολέα. Δεν έχουν κάποιο ουσιαστικό ρόλο, μιας και είναι πληροφοριακά. Σε αυτά τα πεδία μπορεί κάποιος να συμπληρώσει το τηλέφωνό του, το λειτουργικό του σύστημα, το όνομα του προγράμματος που χρησιμοποιεί και οτιδήποτε μπορεί να σκεφτεί. Στο συγκεκριμένο γράμμα το πρόγραμμα αποστολής, εκτός των άλλων, έθεσε και την επικεφαλίδα **X-Mailer**, που περιέχει το όνομα και την έκδοσή του. Στις επικεφαλίδες **From** και **To**, δηλώνονται οι αποστολέας και παραλήπτης αντίστοιχα, και είναι υποχρεωτικό να υπάρχουν. Το πεδίο **Date** περιέχει την ημερομηνία και όπως θα έχετε παρατηρήσει περιέχει την ώρα και την ζώνη ώρας του αποστολέα, ώστε να μην δημιουργηθούν σύγχίσεις κατά την αποστολή γραμμάτων σε άλλες περιοχές. Το **Content-Type** περιέχει τα στοιχεία που θα χρειαστεί ο παραλήπτης για να διαβάσει το γράμμα. Στη συγκεκριμένη περίπτωση απλώς αναφέρεται ότι πρόκειται για ένα κείμενο με χαρακτήρες από το *ISO-8859-7* πρότυπο. Αυτήν την πληροφορία την χρησιμοποιεί το πρόγραμμα ανάγνωσης γραμμάτων του παραλήπτη για να διαβάσει σωστά το μήνυμα (θέτει την αντίστοιχη γραμματοσειρά κλπ). Στο **Content-Transfer-Encoding** δηλώνεται η μετατροπή που έχει υποστεί το αρχικό κείμενο για την μεταφορά του. Το δικό μας γράμμα έχει αποσταλεί χρησιμοποιώντας 8βιτ χαρακτήρες. Το "**MIME-Version: 1.0**" δείχνει ότι στο μήνυμα περιέχονται και πεδία από το **MIME** πρότυπο.

Μία σειρά κάτω από τις επικεφαλίδες βρίσκεται το κυρίως σώμα του γράμματος, το οποίο στη συγκεκριμένη περίπτωση αποτελείται από μία μόνο πρόταση στα ελληνικά. Το κυρίως σώμα του γράμματος είναι και το τελευταίο του τμήμα, εκτός αν πρόκειται για κάποιο γράμμα με πολλά μέρη (multipart).

Ένα γράμμα με πολλά μέρη μπορεί να περιέχει πολλές εκδόσεις του ίδιο μηνύματος, για παράδειγμα μία σε απλό κείμενο και μία σε HTML μορφή, ή να περιέχει αρχεία κλπ. Η HTML μορφή για τα μυνήματα έχει προταθεί με το RFC 1896, και συνήθως χρησιμοποιείται παράλληλα με την απλή μορφή κειμένου, αφού δεν την υποστηρίζουν όλα τα προγράμματα ανάγνωσης ηλεκτρονικών γραμμάτων.

Ας δούμε όμως ένα μύνημα το οποίο περιέχει ένα κείμενο σε απλή και HTML μορφή:

```
X-Mailer: XFMail 1.3 [p0] on Linux
Content-Type: multipart/alternative; boundary="a_random_boundary"
MIME-Version: 1.0
Date: Sun, 05 Mar 2000 02:02:08 +0200 (EET)
```

```
From: "Mister A" <mistera@hellug.gr>
To: Mister B <misterb@linux.gr>
Subject: hello

--a_random_boundary
Content-Type: text/plain; charset=ISO-8859-7
Content-Transfer-Encoding: 8bit

  ... Αυτό είναι ένα τυπικό γράμμα με ελληνικούς χαρακτήρες σε απλή μορφή...

--a_random_boundary
Content-Type: text/enriched; charset=ISO-8859-7
Content-Transfer-Encoding: 8bit
<html>
```

... Αυτό είναι ένα τυπικό γράμμα με ελληνικούς χαρακτήρες σε enriched μορφή...

```
</html>
--a_random_boundary
```

2. Αποστολή

Έτσι αφού γράψαμε ένα γράμμα, συμπλήρωσε το πρόγραμμα μας όλα τα απαραίτητα πεδία, είναι καιρός να το στείλουμε. Το που θα το στείλουμε εξαρτάται από το δικτύο που βρισκόμαστε. Ο διακομιστής στον οποίο στέλνουμε το γράμμα εκτελεί μια εφαρμογή MTA[1] (Message Transfer Agent ή Εφαρμογή μεταφοράς ταχυδρομείου). Το προτόκολο που χρησιμοποιεί αυτή η εφαρμογή λέγεται SMTP και γιάυτό πολλές φορές τον συναντάμε σαν SMTP Server. SMTP σημαίνει Simple Mail Transfer Protocol, και μια ελεύθερη μετάφρασή του είναι 'προτόκολο μεταφοράς απλών γραμμάτων'. Ο διακομιστής αυτός είναι μια εφαρμογή όπως το sendmail (το οποίο είναι το πιο διαδεδομένο στο δίκτυο) και είναι υπεύθυνη για την λήψη του γράμματος από τον αποστολέα και αποστολής του στον παραλήπτη. Έτσι στέλνοντας το γράμμα στον SMTP διακομιστή, του φορτώνουμε τη δουλειά της ανεύρεσης του παραλήπτη και αποστολής του γράμματος.

Στη συγκεκριμένη περίπτωση, μόλις ο διακομιστής παραλάβει το γράμμα, ελέγχει τις επικεφαλίδες, κάποιες επιπλέον πληροφορίες που του δίνουμε και καταγράφει τον (ή τους) παραλήπτες. Εδώ είναι ο misterb@linux.gr, οπότε ο SMTP διακομιστής μας θα κάνει επερωτήσεις σε κάποιο κεντρικό σύστημα διαχείρισης ονομασίας τομέων(DNS), για να βρεί ποιος είναι ο υπεύθυνος διακομιστής για την παραλαβή του γράμματος. Έστω ότι είναι ο mail.linux.gr. Τότε ο πρώτος

[1] Ένα νέο προτόκολο, το MSA (Message Submission Agent), έχει δημιουργηθεί για να αντικαταστήσει τον σημερινό τρόπο αποστολής μυνημάτων. Σήμερα είναι σχετικά καινούριο και δεν χρησιμοποιείται ιδιαίτερα.

διακομιστής συνδέεται στον αντίστοιχο SMTP διακομιστή mail.linux.gr και του αποστέλλει το γράμμα.

Σχετικά απλή διαδικασία, και ίσως αναρωτηθείτε γιατί χρειάζεται ο SMTP server αφού μπορεί άνετα κάποιος να αποστείλει το γράμμα απευθείας, χωρίς την μεσολάβηση του. Οι λόγοι είναι αρκετοί, και κυρίως είναι για δική μας διευκόλυνση. Για παράδειγμα, μιας και τα δίκτυα δεν λειτουργούν πάντα σταθερά, η παραπάνω διαδικασία δεν επιτυγχάνεται πάντα σε ένα στάδιο. Έστω ότι υπήρξε διακοπή της επικοινωνίας μεταξύ του mail.linux.gr και του δικού μας διακομιστή. Τότε ο διακομιστής μας, θα αποθηκεύσει το γράμμα και θα ξαναδοκιμάσει αργότερα όταν η επικοινωνία θα είναι εφικτή. Σε περίπτωση που μέσα σε κάποιο χρονικό διάστημα (που συνήθως κυμαίνεται μεταξύ 2 και 5 ημερών) ο διακομιστής δεν καταφέρει να ολοκληρώσει την αποστολή, τότε επιστρέφει κάποιο ειδοποιητήριο γράμμα στον αποστολέα και ακυρώνει την αποστολή. Αν ενεργούσαμε εμείς για λογαριασμό του, θα έπρεπε να συνδεόμαστε συνεχώς στο δίκτυο και να κοιτάμε αν έχει αποκατασταθεί η επικοινωνία.

3. Παραλαβή

Τώρα που ο mail.linux.gr έχει παραλάβει το γράμμα μας, είναι η σειρά του να ενεργήσει. Αφού ελέγξει τις επικεφαλίδες και επιβεβαιώσει ότι ο παραλήπτης υπάρχει, τότε αποθηκεύει το γράμμα ώστε μόλις συνδεθεί ο παραλήπτης, να μπορεί να το παραλάβει. Σε περίπτωση που ο τελικός παραλήπτης δεν υπάρχει ή δεν μπορεί να λάβει άλλα γράμματα (πχ μπορεί να έχει γεμίσει ο δίσκος του διακομιστή), τότε ο διακομιστής διαγράφει το γράμμα και επιστρέφει κάποιο ειδοποιητήριο γράμμα στον αποστολέα που εξηγεί τους λόγους ακύρωσης της αποστολής/παραλαβής.

Η διαδικασία της παραλαβής τώρα συνήθως περνάει στα χέρια κάποιου διακομιστή ανάκτησης ηλ. γραμμάτων. Αυτός συνήθως είναι POP3 ή IMAP διακομιστής. Το POP3 προτόκολο είναι το πιο διαδεδομένο (αλλά όχι και το καλύτερο) σήμερα. Τα αρχικά του σημαίνουν Post Office Protocol 3 ή προτόκολο ταχυδρομείου 3, ενώ ο αριθμός 3 υπάρχει για να δείξει τον αριθμό έκδοσης του προτοκόλου (υπήρξαν εκδόσεις 1 και 2 αλλά σήμερα δεν χρησιμοποιούνται).

Τώρα έρχεται η σειρά του παραλήπτη να ενεργήσει. Για να παραλάβει τα γράμματά του πρέπει αφού συνδεθεί στο δίκτυο, να συνδεθεί με τον POP3 διακομιστή, να δώσει κάποιο όνομα χρήστη και συνθηματικό και να παραλάβει τα μηνύματά του. Κατά την παραλαβή κάποιος μπορεί να παρατηρήσει ότι οι επικεφαλίδες του γράμματος διαφέρουν από τις αρχικές μιας και έχουν προστεθεί μυνήματα από τον κάθε διακομιστή που πέρασε το γράμμα. Για παράδειγμα το παραπάνω γράμμα μπορεί να έχει γίνει:

```
Received: from mail.hellug.gr (mail.hellug.gr[213.215.111.20])
by mail.linux.gr (8.9.3/8.9.3) with ESMTP id BAA22825
for <misterb@linux.gr>; Sun, 5 Mar 2000 01:59:49 +0200
Received: from dynamicip.provider.gr ([193.134.13.116])
by mail.hellug.gr (8.8.7/8.8.7) with ESMTP id BAA30367
for <misterb@linux.gr>; Sun, 5 Mar 2000 01:59:52 +0200
```

```
X-Mailer: XFMail 1.3 [p0] on Linux
X-Priority: 3 (Normal)
Content-Type: text/plain; charset=ISO-8859-7
Content-Transfer-Encoding: 8bit
MIME-Version: 1.0
Date: Sun, 05 Mar 2000 02:02:08 +0200 (EET)
From: "Mister A" <mistera@hellug.gr>
To: "Mister B" <misterb@linux.gr>
Subject: hello

 ... Αυτό είναι ένα τυπικό γράμμα με ελληνικούς χαρακτήρες ...
```

4. Ένα Παράδειγμα

Ας δούμε όμως πώς μπορούμε να στείλουμε απέυθείας ένα γράμμα χωρίς να παρεμβληθεί κάποιο πρόγραμμα αποστολής. Ας υποθέσουμε ότι θέλουμε να στείλουμε στη ηλ. διεύθυνση john@provider.gr. Για να δούμε ποιος διακομιστής είναι υπεύθυνος γιάυτή την διεύθυνση θα συμβουλευτούμε το σύστημα ονομασίας τομέων (DNS) με το πρόγραμμα nslookup.

```
$ nslookup}
Server: 193.94.156.34

Address: a.random.nameserver
> set q=any
> provider.gr
provider.gr preference = 10, mail exchanger = mail.provider.gr
provider.gr nameserver = ns.provider.gr
provider.gr [...]
```

Ανάμεσα στα άλλα υπάρχει ένα πεδίο που αναφέρεται ως "mail exchanger" και περιέχει την διεύθυνση του διακομιστή που χρησιμοποιεί το προιδερ.γρ για το εισερχόμενο ταχυδρομείο. Εδώ έστω ότι είναι το "mail.provider.gr". Έτσι μπορούμε τώρα να συνδεθούμε στον MTA του provider.gr και να στείλουμε το γράμμα. Ας δοκιμάσουμε λοιπόν να στείλουμε το γράμμα σε enriched (HTML) μορφή και να ζητήσουμε από τον SMTP διακομιστή να μας επιστρέψει κάποια απόδειξη παραλαβής. Έστω ότι η δική μας διεύθυνση είναι η george@hello.gr. [Για να ξεχωρίζουν οι δικές μας εντολές προσθέσαμε το '-', το οποίο πρέπει να αφαιρέσετε.]

```
$ telnet mail.provider.gr 25
Trying 193.91.234.2...
Connected to mail.provider.gr.
Escape character is '^]'.
220 mail.provider.gr ESMTP Sendmail 8.10.0/8.10.0; Sat, 27 May 2000 21:44:39 +0300

- HELO hello.gr
```

```
250 mail.provider.gr Hello george@hello.gr [193.95.123.4], pleased to meet you
- MAIL FROM: <georgehello.gr>
250 2.1.0 <george@hello.gr>... Sender ok
- RCPT TO: <john@provider.gr> NOTIFY=SUCCESS,FAILURE
250 2.1.5 <john@provider.gr>... Recipient ok
- DATA
354 Enter mail, end with "." on a line by itself
- From: "George" <george@hello.gr>
- To: "John" <john@provider.gr>
- X-Mailer: HandMade 0.1
- Content-Type: text/enriched: charset=ISO-8859-1
- Content-Transfer-Encoding: 8bit
- MIME-Version: 1.0
- Subject: Can you believe that?
-
- <html>
- <b>Hello</b><br>
- This is my first message with my new HTML compliant mailer.<br>
- </html>
-
- .
250 2.0.0 e4RIix100983 Message accepted for delivery
- quit
```

Οι εντολές "HELO", "MAIL FROM", "RCPT TO" και "DATA" είναι εντολές που καθορίζονται από το SMTP προτόκολο. Στην 'RCPT TO' προσθέσαμε πέρα από τον τοπικό παραλήπτη, και την εντολή NOTIFY=SUCCESS,FAILURE που σημαίνει ότι ο MTA θα μας ειδοποιήσει σε περίπτωση παραλαβής ή μη του γράμματος (η εντολή περιέχεται στις Delivery Status Notification επέκτασεις του SMTP).

5. Αξιοπιστία

Είδαμε παραπάνω, ο αποστολέας θα λάβει ένα ειδοποιητήριο γράμμα στην περίπτωση που ο παραλήπτης δεν μπορεί να λάβει για κάποιο λόγο το γράμμα. Επίσης θα ειδοποιηθεί πάλι ο αποστολέας αν το γράμμα του έχει καθυστερήσει και βρίσκεται αποθηκευμένο στον σκληρό δίσκο ενός διακομιστή. Η ερώτηση είναι πόσο μπορούμε να βασιζόμαστε σε αυτά... Η απάντηση είναι δύσκολο να δωθεί μιας και τα παραπάνω εξαρτώνται κυρίως από την υλοποίηση και συντήρηση των διακομιστών, η οποία δεν είναι ομοιογενής στο διαδίκτυο. Στην ιδεατή περίπτωση που τα συστήματα λειτουργούσαν σωστά και οι διαχειριστές ήταν καλά εκπαιδευμένοι δεν θα υπήρχαν απώλειες σε γράμματα χωρίς να ειδοποιηθεί κάποιος. Λόγω όμως του γεγονότος ότι και οι δύο παραπάνω λόγοι δεν πληρούνται από τους πολλούς συμμετέχοντες στο διαδίκτυο, έχουμε πολλά παραδείγματα χαμμένων γραμμάτων λόγω κάποιας αναβάθμισης του διακομιστή ταχυδρομείου, απροσεξίας του διαχειριστή, ήτε από αδυναμία του λογισμικού. Πολλές φορές η διαχείριση του ηλεκτρονικού ταχυδρομείου αναλαμβάνεται από ανθρώπους που πιστεύουν ότι ένα πρόγραμμα

ή μια εταιρία θα τους λύσει όλα τα προβλήματα, οπότε μέχρι να καταλάβουν ότι το πρόγραμμα που χρησιμοποιούν θέλει κάποια επιπλέον παραμετροποίηση για να λειτουργήσει, ή ότι η εταιρία που εμπιστεύτηκαν δεν ήταν έμπειρη στον χώρο αυτό, αρκετά γράμματα έχουν εξαφανιστεί ενώ μερικοί χρήστες θα περιμένουν κάποια απάντηση για αρκετό καιρό.

Ένα αντίμετρο γιάυτήν την κατάσταση είναι η δυνατότητα απαίτησης από τον παραλήπτη κάποιας απόδειξης παραλαβής. Αυτό μπορεί να επιτευχθεί με το Delivery Status Notification(RFC 1891), και όπως είδαμε στο παραπάνω παράδειγμα, υποχρεώνει τον διακομιστή να μας επιστρέψει μια απόδειξη παραλαβής. Το γεγονός όμως ότι ο διακομιστής έλαβε το γράμμα δεν σημαίνει ότι και ο τελικός παραλήπτης το έλαβε. Γιάυτό το λόγο πολλά προγράμματα θέτουν στην επικεφαλίδα Return-Receipt-To, (μερικά και στην X-Confirm-Reading-To) την διεύθυνση στην οποία θέλουμε να σταλεί η απόδειξη, και έτσι ο το πρόγραμμα ανάγνωσης γραμμάτων του παραλήπτη θα πρέπει να αποστείλει μια απόδειξη παραλαβής. Δυστυχώς η τελευταία μέθοδος δεν είναι αξιόπιστη αφού δεν μπορεί να υποχρεώσει τον παραλήπτη να στείλει απόδειξη παραλαβής, και υποστηρίζεται από μερικά μόνο προγράμματα. Μια άλλη υπηρεσία που μπορεί να μας δώσει πληροφορίες για το αν κάποιος χρήστης έχει διαβάσει το e-mail του είναι η finger. Ας δούμε τις πληροφορίες που μας δίνει αυτή η υπηρεσία:

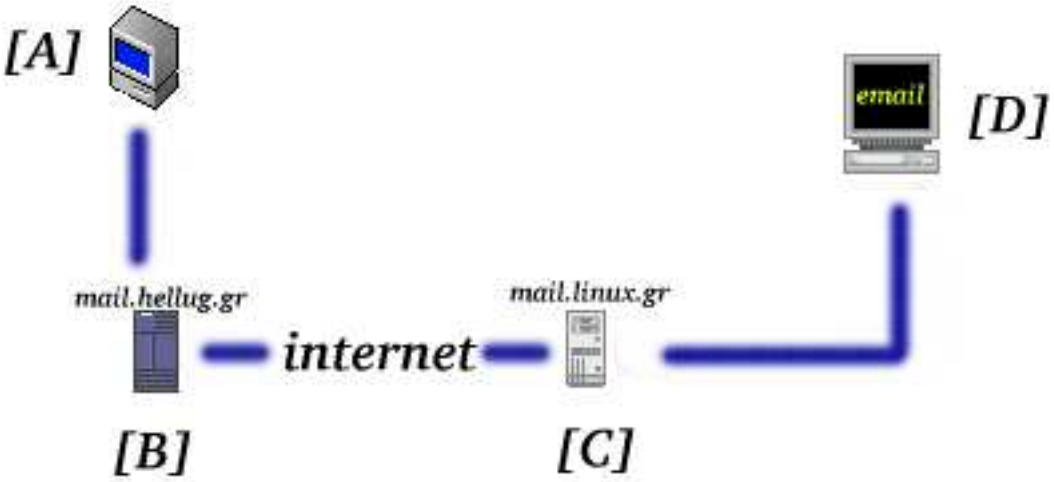
```
$ finger nmav@host.provider.gr
Login: nmav Name: Nikos Mavroyanopoulos
On since Fri May 26 21:43 (EEST) on pts/1
Mail last read Fri May 26 21:16 2000 (EEST)
```

Βλέπουμε ότι μας δίνει κάποιες πληροφορίες, όπως το όνομα του χρήστη, μας αναφέρει ότι αυτή τη στιγμή είναι on-line, ενώ μας δίνει την ημερομηνία που διάβασε τελευταία φορά τα γράμματά του. Αρκετά χρήσιμη υπηρεσία, αλλά χρειάζεται να ξέρουμε τον υπολογιστή από τον οποίο παραλαμβάνει τα γράμματα ο χρήστης (και όχι μόνο το e-mail). Δυστυχώς όμως μερικοί διακομιστές δεν υποστηρίζουν αυτή την υπηρεσία.

6. Ασφάλεια

Όπως βλέπουμε από τα παραπάνω η διαδικασία της αποστολής μέχρι και τις παραλαβής ενός γράμματος είναι πολύ απλή και έχει πολλά κοινά σημεία με την αποστολή ενός γράμματος με το ταχυδρομείο. Δυστυχώς έχει και όλα τα μειονεκτήματα της, αν όχι περισσότερα. Σε κανένα στάδιο δεν υπάρχει ασφάλεια, μεγαλύτερη της ασφάλειας που έχει μια ανοιχτή καρτ-ποστάλ που στέλνουμε από τις διακοπές. Σε οποιοδήποτε στάδιο της μεταφοράς μπορεί ο κάθε διαχειριστής συστήματος να διαβάσει το γράμμα μας, ή να το τροποποιήσει και να περάσει απαρατήρητος. Ακόμα χειρότερα, το μήνυμα μπορεί να υποκλαπεί, κατά την μεταφορά σε κάποιο δορυφόρο, από τα καλώδια του ΟΤΕ, ή και από κάποιο ανασφαλές δίκτυο που διέσχισε το γράμμα (πχ κάποιο LAN σε ethernet). Επίσης η αποστολή του γράμματος είναι ανώνυμη. Δεν υπάρχει κάποιος τρόπος για να καταλάβει κάποιος αν πράγματι ο συγκεκριμένος αποστολέας έστειλε το γράμμα ή καποιος άλλος. Το πεδίο του αποστολέα στο ηλ. γράμμα συμπληρώνεται όπως και στο κανονικό ταχυδρομείο, χωρίς κανένα περιορισμό.

Για την βελτίωση της ασφάλειας στο διαδίκτυο έχουν προταθεί αρκετά πρωτόκολα όπως το IPSec και το TLS. Το πρώτο έχει ως σκοπό την κρυπτογράφηση των δεδομένων μεταξύ διακομιστών στο IP επίπεδο, δηλαδή στα χαμήλώτερου επιπέδου πακέτα που υποστηρίζει το δίκτυο, οπότε και δεν χρειάζεται να αλλάξει η υπάρχουσα βάση των προγραμμάτων. Το TLS (Transport Layer Security) είναι κρυπτογράφηση στο TCP επίπεδο, και άρα χρειάζεται κάποια μετατροπή στην υπάρχουσα βάση προγραμμάτων. Το πλεονέκτημα είναι ότι και στα δύο αυτά προτόκολα η κρυπτογράφηση είναι διαφανής για τον τελικό χρήστη, οπότε και δεν χρειάζεται να αλλάξει τίποτα από αυτά που έκανε μέχρι σήμερα, ούτε να εκπαιδευτεί σε κάτι καινούριο. Το TLS, βασίζεται στο SSL προτόκολο που αναπτύχθηκε από την Netscape για να αυξήσει την ασφάλεια στις συναλλαγές από το Web (ή παγκοσμίου ιστού), έχει βρει εφαρμογές στις περισσότερες δικτυακές υπηρεσίες. Αντίθετα το IPsec δεν χρησιμοποιείται σήμερα ευρέως.



η μεταφορά του γράμματος στο δίκτυο

Μια από τις εφαρμογές του TLS προτοκόλου είναι και η μεταφορά και παραλαβή των ηλεκτρονικών γραμμάτων. Το συγκεκριμένο προτόκολο προστατεύει από την υποκλοπή των μηνύματων κατά την επικοινωνία μεταξύ των διακομιστών. Δηλαδή η κρυπτογραφημένη μεταφορά είναι μεταξύ των AB (SMTP-TLS), BC (SMTP-TLS) και CD (POP3-TLS) σημείων στο σχήμα. Δυστυχώς δεν υπάρχει προστασία από την υποκλοπή των μηνυμάτων μέσα στους διακομιστές (στα σημεία

B,C).

Δηλαδή ακόμα ο διαχειριστής κάποιου ενδιάμεσου συστήματος στην διαδικασία της μεταφοράς, μπορεί να τροποποιήσει και να διαβάσει τα γράμματα κάποιου χρήστη. Ακόμα και στην περίπτωση έμπιστου διαχειριστή, αυτή η κατάσταση δεν είναι αποδεκτή μιας και μπορεί λόγω κάποιων ατελειών στην ασφάλεια του συστήματος (ή και απροσεξίας του διαχειριστή), να καταφέρει κάποιος ξένος προς το σύστημα να αποκτήσει πρόσβαση σαν διαχειριστής.

Η καλύτερες λύσεις σήμερα για ασφαλές ηλεκτρονικό ταχυδρομείο είναι το προτόκολο S/MIME και το προτόκολο OpenPGP (το οποίο βασίζεται στο εμπόρικο πρόγραμμα PGP ή Pretty Good Privacy). Λόγω της μεγάλης επιτυχίας του PGP λίγοι σήμερα υποστηρίζουν το S/MIME. Τα προτόκολα αυτά, λειτουργούν με τρόπο ώστε μόνο ο τελικός παραλήπτης να μπορεί να διαβάσει το μήνυμα (end to end encryption). Δηλαδή η κρυπτογράφηση είναι μεταξύ των σημείων AD στο σχήμα. Έτσι καμία υποκλοπή δεν μπορεί να υπάρξει μεταξύ του αποστολέα και του παραλήπτη. Ένα επίσης πλεονέκτημα των δύο αυτών προτοκόλων είναι ότι υποστηρίζουν και ψηφιακές υπογραφές, έτσι ώστε να μπορεί ο παραλήπτης να καταλάβει αν πράγματι ο αποστολέας έστειλε το γράμμα και όχι καποιος άλλος.

Ας δούμε ένα ηλεκτρονικό γράμμα που είναι υπογεγραμμένο με το OpenPGP προτόκολο:

```
Received: (from nmav@localhost)
by crystal.i-net.gr (8.10.0/8.10.0/CRYSTAL) id e4QA8kY01760
for nmav; Fri, 26 May 2000 13:08:46 +0300
Date: Fri, 26 May 2000 13:08:46 +0300
From: Nikos Mavroyanopoulos <nmav@hellug.gr>
To: Nikos Mavroyanopoulos <nmav@hellug.gr>
Subject: hello
Message-ID: <20000526130846.A1754@i-net.gr>
Mime-Version: 1.0
Content-Type: multipart/signed; micalg=pgp-sha1;
protocol="application/pgp-signature"; boundary="RnlQjJ0d97Da+TV1"
Content-Disposition: inline
User-Agent: Mutt/1.1.9i
X-Operating-System: Debian GNU/Linux
Status: RO
Content-Length: 540
Lines: 26

--RnlQjJ0d97Da+TV1
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
Content-Transfer-Encoding: quoted-printable
hi there!
--=20

Nikos Mavroyanopoulos
```

```
mailto:nmav@hellug.gr
--RnlQjJ0d97Da+TV1
Content-Type: application/pgp-signature
Content-Disposition: inline
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iD8DBQE5Lk0uEcUvRypR0HQRAuY8AKCu25c7UVfR2e4YXPNtxtyJecVyrgCfcqKb
0ZRueYH3iTlJhpgJ1k7a1+o=
=dO7N
-----END PGP SIGNATURE-----
--RnlQjJ0d97Da+TV1--
```

Όπως βλέπουμε είναι ένα γράμμα με δύο μέρη, το οποίο περιέχει το κυρίως μήνυμα, και ένα μέρος με την ηλεκτρονική υπογραφή. Το πρόγραμμα που θα χρησιμοποιηθεί από τον παραλήπτη για να ελέγξει την υπογραφή καθορίζεται στο Content-Type. Η υπογραφή περιέχει εσωτερικά τους αλγόριθμους που χρησιμοποιήθηκαν για την παραγωγή της, ενώ πρέπει να γνωρίζουμε ότι καλύπτει μόνο το κυρίως μύνημα και όχι για τα headers (άρα και το θέμα). Έτσι με αυτόν τον τρόπο μπορεί κάποιος να είναι σίγουρος για την προέλευση του συγκεκριμένου μυνήματος, οπότε μπορεί αργότερα, αν χρειαστεί, να αποδείξει ότι αυτός που τον χαιρέτησε ήταν πράγματι ο nmav@hellug.gr.

Βέβαια σε περίπτωση που χρησιμοποιούμε λογισμικό που χρησιμοποιεί κρυπτογραφία καλό είναι να γνωρίζουμε να το χειριζόμαστε καλά. Ο λόγος είναι ότι στέλνοντας με ένα τέτοιο πρόγραμμα, πιστεύουμε πως τα δεδομένα μας είναι ασφαλή, μα αν δεν το χειριζόμαστε σωστά απλώς έχουμε κάνει μια τρύπα στο νερό. Διαβάστε καλά την τεκμηρίωση τέτοιων προγραμμάτων (που ευτυχώς είναι εκτενής). Το κυριότερο είναι να μην παρασυρθήτε από προγράμματα που υπόσχονται 100% ασφάλεια με τους μυστικούς τους αλγόριθμους, προτιμήστε τα ανοιχτά πρότυπα, είναι δοκιμασμένα.

7. Λογισμικό

Αν δεν θέλετε να στέλνετε ηλ. γράμματα με τον τρόπο που περιγράψαμε στο παράδειγμα, μπορείτε να χρησιμοποιήσετε ένα από τα υπάρχοντα προγράμματα που κάνουν αυτή την εργασία ευκολότερη. Για το Λινυξ, υπάρχουν αρκετά προγράμματα γιάυτό το λόγο. Μερικά (ελεύθερα) είναι:

Διακομιστές ταχυδρομείου (MTA):

- sendmail: http://www.sendmail.org
- exim: http://www.exim.org
- postfix: http://www.postfix.org
- qmail: http://www.qmail.org

Διακομιστές παραλαβής ηλ. γραμμάτων (POP3, IMAP):

- mailutils: http://www.gnu.org/software/mailutils

- qpopper: http://www.eudora.com/qpopper/

Προγράμματα ανάγνωσης ηλ. γραμμάτων (MUA):

- mutt: http://www.mutt.org
- xfmail: http://xfmail.slappy.org/
- kmail: http://devel-home.kde.org/~ kmail/

OpenPGP υλοποιήσεις:

- gnupg: http://www.gnupg.org

TLS υλοποιήσεις:

- openssl: http://www.openssl.org

IPSec υλοποιήσεις:

- freeswan: http://www.freeswan.org