Τ.Ε.Ι. ΠΑΤΡΩΝ

ΣΧΟΛΗ : ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ : ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

΄ΕΤΟΣ : 2007 - 2008

ΘΕΜΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ :

ΑΣΦΑΛΕΙΑ ΜΟΝΤΕΛΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΕΙΣΗΓΗΤΗΣ : ΑΘΑΝΑΣΟΠΟΥΛΟΣ ΣΤΑΥΡΟΣ

ΟΜΑΔΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ :

ΚΑΡΑΝΑΣΤΑΣΗ ΕΛΕΝΗ

ΟΥΛΗ ΜΑΡΙΑ

ΦΙΣΚΑΤΩΡΗ ΠΑΝΙΑΓΙΩΤΑ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Ως σήμερα, γνωρίζαμε ότι οι τυπικές μέθοδοι πληρωμών ήταν, η πληρωμή μέσω χαρτονομισμάτων, επιταγών και πιστωτικών καρτών. Όμως η μεγαλύτερη επανάσταση στον τομέα των συναλλαγών από τότε που χρησιμοποιήθηκε ο χρυσός, είναι το λεγόμενο «Ψηφιακό χρήμα». Το οποίο αποτελείται από τα εξής είδη ηλεκτρονικού χρήματος:

1. **Πιστωτικές κάρτες**
2. **Χρεωστικές Τραπεζικές Κάρτες**
3. **Έξυπνες κάρτες (smart cards)**
4. **Ψηφιακό πορτοφόλι (Digital wallet) και**
5. **Ηλεκτρονικές Επιταγές.**

Όλα αυτά τα είδη λοιπόν εξυπηρετούν να γίνονται οι χρηματικές συναλλαγές σε ένα ψηφιακό περιβάλλον, όπου σχεδιάστηκε να είναι ηλεκτρονικά διαχειρίσιμο. Το e – banking και το ηλεκτρονικό εμπόριο (e – Bay), είναι δείγματα από αυτές τις μορφές, ψηφιακού χώρου συναλλαγών.

Όμως επειδή μιλάμε για ένα ουσιαστικά “ιδεατό” σύστημα συναλλαγών, υπάρχουν και οι αντίστοιχες απειλές όπως είναι το **ηλεκτρονικό έγκλημα**.
Οι εγκληματίες του κυβερνοχώρου είναι γνωστοί ως Hackers και Crackers, οι οποίοι είναι οι δημιουργοί των ηλεκτρονικών απειλών.

Τα είδη των ηλεκτρονικών απειλών είναι:

1. **Spam**
2. **Virus (ιός)**
3. **Trojan horses (δούρειοι ίπποι)**
4. **Worms (σκουλήκια)**
5. **Dialers**
6. **Spoofing**
7. **Keylogger**
8. **Rootkits**
9. **Malware**

10. **Spyware**
11. **Adware**
12. **Scumware καί**
13. **Phishing**

Η αντιμετώπιση αυτών των απειλών είναι τα λεγόμενα **Firewall**, όπου είναι μία μέθοδος για την εφαρμογή ασφάλειας, σχεδιασμένη να διατηρεί ένα δίκτυο ηλεκτρονικών υπολογιστών αδιάβλητο από παράνομες προσβάσεις.

Το ζήτημα λοιπόν της ασφάλειας των δικτύων και συναλλαγών, είναι από τα πιο επίκαιρα και ταυτόχρονα αμφιλεγόμενα ζητήματα, ειδικά σε κάποιες χώρες, όπως η Ελλάδα, όπου υστερεί γενικά σε τεχνολογική ανάπτυξη.

Άρα για να υπάρχει ασφάλεια στις συναλλαγές, απαιτείται η παρουσία ενός ασφαλούς web server, όπου χρησιμοποιείται για την απόκρυψη δεδομένων μεταξύ ενός server, που αντιστοιχεί στην εταιρεία που κάνει την συναλλαγή, και ενός browser, που αντιστοιχεί στον πελάτη. Η απόκρυψη των δεδομένων, γίνεται μέσα από **κρυπτογράφηση** των δεδομένων, πριν φύγουν από την εταιρεία και αποκρυπτογράφηση, όταν φτάσουν στον πελάτη.

Για την επίτευξη μιας κρυπτογράφησης, ούτως ώστε να μπορέσει να γίνει η ηλεκτρονική συναλλαγή, εφευρέθηκαν κάποια κλειδιά, γνωστά ως «Μυστικά Κλειδιά», όπου αποτελούνται από δύο είδη, α) το ιδιωτικό κλειδί και β) το δημόσιο κλειδί (η συμμετρική και ασύμμετρη κρυπτογράφηση δηλαδή). Για την δημιουργία αυτών των κλειδιών, υπήρξαν συγκεκριμένες συναρτήσεις, όπου για είσοδο λαμβάνουν ένα μεγάλο τυχαίο αριθμό και για έξοδο πραγματοποιούν την λειτουργία του ιδιωτικού και δημόσιου κλειδιού.

Για να είναι όμως μια συναλλαγή ασφαλής και επίσημη, χρειάζονται και τα αντίστοιχα πιστοποιητικά ασφαλείας της συναλλαγής, τα οποία χωρίζονται στις εξής κατηγορίες:

1. **Ψηφιακά πιστοποιητικά (Digital Certificates)**
2. **Χρονική σφραγίδα (Time Stamp)**
3. **Ψηφιακός φάκελος (Digital Envelope)**
4. **Ψηφιακή ή Ηλεκτρονική υπογραφή (Digital Signature)**
5. **Υδατογραφήματα (Watermarks)**

Για να εξασφαλιστεί όμως ότι το ψηφιακό περιβάλλον δεν θα μένει χωρίς έλεγχο και κανένας χρήστης ή επισκέπτης, δεν θα μπορεί να παραβεί την ιεραρχία και τα επιτρεπτά επίπεδα πρόσβασης, δημιουργήθηκαν τα Πρωτόκολλα ασφαλείας Συναλλαγών και Δικτύων, όπου είναι τα εξής:

1. **SSH (Secure Shell)**
2. **SSL (Secure Sockets Layer)**
3. **TLS (Transport Layer Security)**
4. **SET (Secure Electronic Transactions)**
5. **S/HTTP (Secure Hyper-text Transfer Protocol)**
6. **Kerberos**
7. **S/MIME (Secure MIME)**
8. **Πρόγραμμα PGP (Pretty Good Privacy)**

Μια ηλεκτρονική συναλλαγή χρειάζεται και την βοήθεια ατόμων εξουσιοδοτημένων από το κράτος και πιστοποιήσεις από το **ISO** (τον οργανισμό για την παραγωγή και καταχώρηση προτύπων) . Γι' αυτό και η κυβέρνηση ασχολήθηκε με το ηλεκτρονικό εμπόριο και ο Υπουργός Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης Καθηγητής κ. Προκόπης Παυλόπουλος υπέγραψε την Εγκύκλιο με θέμα: «Εφαρμογή και χρήση ψηφιακής υπογραφής και κρυπτογράφησης στη Δημόσια Διοίκηση», όπου καλύπτει νομοθετικά και την Ασφάλεια Ηλεκτρονικών Συναλλαγών και Δικτύου.

ΠΡΟΛΟΓΟΣ

Αν ταξιδέψουμε μερικά χρόνια πίσω και αναρωτηθούμε, πώς θα πραγματοποιούσαμε μια χρηματική συναλλαγή, η πρώτη σκέψη στο μυαλό μας θα ήταν μια συναλλαγή, όπου γίνεται χέρι με χέρι και σίγουρα με χαρτονομίσματα.

Η πιστοποίηση αυτής της συναλλαγής θα μπορούσε να ήταν έγκυρη με μια απόδειξη του ατόμου/ εταιρείας, που εισέπραξε το χρηματικό ποσό, είτε χειρόγραφη (με τις ανάλογες υπογραφές), είτε μηχανογραφημένη από το λογιστήριο/ ταμείο.

Η ασφάλεια που παρέχεται σε αυτές τις συναλλαγές (όπως τράπεζες, supermarkets, εμπορικά κέντρα κ.α.), είναι ο συναγερμός, οι κάμερες ασφαλείας, το προσωπικό ασφαλείας (security), η αστυνόμευση του χώρου, ακόμα και οι αυτόπτες

μάρτυρες (π.χ. σε ένα συμβάν ληστείας). Με όλες αυτές τις παροχές, όπως είναι γνωστό, μπορούμε να αποδείξουμε και να αναγνωρίσουμε το κακοποιό στοιχείο μίας παράνομης πράξης.

Όλα αυτά, είναι ενέργειες, τις οποίες εκτελεί ένας άνθρωπος στην καθημερινή του ζωή, στο περιβάλλον το οποίο δρα. Είναι ο χειροπιαστός κόσμος, τον οποίο γνωρίζουμε όλοι μας.

Όταν όμως αυτό το περιβάλλον από πραγματικό και χειροπιαστό, γίνει ιδεατό και άυλο, πόσο ασφαλής θα ένιωθε κάποιος για να μπορεί να ενεργεί και να συναλλάσσεται μέσα από αυτό;

Οι απαντήσεις σε αυτό το ερώτημα θα δοθούν στα παρακάτω κεφάλαια αυτής της εργασίας. Θα παρουσιαστεί μια γενική εικόνα για την ασφάλεια των μοντέλων συναλλαγών ενός δικτύου, με όρους, επεξηγηματικές ενότητες, απεικονίσεις και πίνακες. Θα αναφερθούν όλα τα είδη που εξυπηρετούν να γίνονται οι χρηματικές συναλλαγές σε ένα ψηφιακό περιβάλλον, όπου είναι σχεδιασμένο να είναι ηλεκτρονικά διαχείρισημο, όπως και θα αναλύσουμε όλα τα είδη των ηλεκτρονικών απειλών αλλά και για τα μέτρα ασφαλείας που λαμβάνονται για την αντιμετώπιση τους.

I. ΤΙ ΕΙΝΑΙ ΧΡΗΜΑ

Χρήμα θεωρείται οποιοδήποτε εμπορεύσιμο αγαθό ή υπηρεσία που χρησιμοποιείται από μία κοινωνία ως υποκατάστατο αξίας, μέσο ανταλλαγής και μονάδα υπολογισμού. Είναι το μέσον στο οποίο έχουν εκφραστεί οι τιμές και οι αξίες. Κυκλοφορεί από άτομο σε άτομο και από χώρα σε χώρα, βοηθώντας έτσι το εμπόριο. Είναι το κύριο μέτρο τού πλούτου.

Η έννοια του χρήματος κατέχει κεντρική θέση στην οικονομική θεωρία. Το σχήμα, ο τύπος και το υλικό κατασκευής του χρήματος είναι σχετικά μικρής σημασίας θέμα (αν και η ευχέρεια μεταφοράς και μέτρησης, είναι σημαντικός παράγοντας). Το πλέον κρίσιμο χαρακτηριστικό του είναι η κοινή του αποδοχή στις πληρωμές, για άλλα αγαθά και υπηρεσίες.

Η αξία των χρημάτων προκύπτει κατά ένα μέρος από τη χρησιμότητα του ως μέσο ανταλλαγής εντούτοις η χρησιμότητα του ως μέσον ανταλλαγής εξαρτάται από την αναγνώριση της αγοραστικής του αξίας.

Τα προϊόντα ήταν η πρώτη μορφή χρημάτων που εμφανίστηκαν. Στο πλαίσιο ενός συστήματος χρημάτων – προϊόντων, το αντικείμενο που χρησιμοποιείται ως χρήμα έχει έμφυτη αξία. Υιοθετείται συνήθως για να απλοποιήσει τις συναλλαγές σε μια οικονομία ανταλλαγής, κατά συνέπεια λειτουργεί πρώτα ως μέσο ανταλλαγής. Αρχίζει ως αποθήκη αξίας, δεδομένου ότι οι κάτοχοι φθαρτών αγαθών μπορούν εύκολα να τα μετατρέψουν σε ανθεκτικά χρήματα. Τα στηριγμένα σε χρυσό νομίσματα είναι μια κοινή μορφή χρημάτων, τα οποία έχουν χρησιμοποιηθεί και αυτά ως μονάδα απολογισμού. Τα χαρτονομίσματα που εκδίδονται εις πιστώσιν της οικονομίας και δεν αντιστοιχούν σε κάποιες ποσότητες πολύτιμων μετάλλων συχνά αποκαλούνται χρηματικές εντολές (fiat money).

Έχουν υπάρξει πολλά ιστορικά επιχειρήματα σχετικά με το συνδυασμό λειτουργιών του χρήματος, μερικοί υποστηρίζουν ότι χρειάζονται περισσότερο διαχωρισμό και ότι μια ενιαία μονάδα είναι ανεπαρκής να τους εξετάσει όλους. Αυτά τα επιχειρήματα καλύπτονται στο οικονομικό κεφάλαιο που είναι ένας γενικότερος όρος για όλα τα ρευστά μέσα.

Για τους παραπάνω λόγους έχουν επανειλημμένα υιοθετηθεί σαν χρήμα, εδώ και πολλές χιλιετίες στις περισσότερες κοινωνίες ο χρυσός και ο άργυρος. Αλλά από τα μέσα του 20ού αιώνα , έχει παραμερισθεί ο ιστορικός ρόλος των πολύτιμων μετάλλων σαν χρήμα σε όφελος του fiat money(δηλ. χρησιμοποιούνται σαν χρήμα με κυβερνητική απόφαση όπως π.χ. κέρματα, χαρτονομίσματα, καταθέσεις όψεως).

Γενικά για το χρήμα

Στην οικονομική θεωρία γίνεται δεκτό ότι το χρήμα ζητείται για τέσσερις αλληλεξαρτώμενες λειτουργίες :

i. Ως μέσον ανταλλαγής αγαθών και υπηρεσιών, αλλά και ως μέσον εξόφλησης χρεών και λοιπών υποχρεώσεων. Αυτό το χαρακτηριστικό επιτρέπει στα χρήματα να είναι πρότυπα αναβεβλημένης πληρωμής.

ii. Ως μέσον υπολογισμού της αξίας, αλλά και ως μονάδα μέτρησης, ένα κοινό σημείο αναφοράς που επιτρέπει την λειτουργία του συστήματος των τιμών και παρέχει την βάση τήρησης λογαριασμών, καθώς και υπολογισμού του κόστους, του κέρδους και της απώλειας.

iii. Ως σημείο αναφοράς πληρωμών, ως η μονάδα στην οποία συνάπτονται τα δάνεια και συμφωνούνται οι μελλοντικές συναλλαγές, χωρίς χρήμα δεν θα υπήρχε κοινώς αποδεκτή βάση δανεισμού και η έννοια της τραπεζικής πίστης δεν θα μπορούσε να παίξει σημαντικό ρόλο.

iv. ΩΣ απόθεμα αξίας, ένα βολικό μέσο διατήρησης κάποιου εισοδήματος που δεν είναι αναγκαίο να καταναλωθεί στην παρούσα φάση. Αυτή ειδικά η λειτουργία του χρήματος, επιτρέπει την συσσώρευση αποθεμάτων άμεσης αγοραστικής δύναμης. Το χρήμα είναι το μόνο απολύτως ρευστό περιουσιακό στοιχείο (δηλαδή είναι το μόνο στοιχείο που αμέσως μετατρέπεται σε άλλα αγαθά).

Οι τυπικές μέθοδοι πληρωμών είναι :

- **Ø** Η πληρωμή μέσω χαρτονομισμάτων (δηλ. με τα λεγόμενα μετρητά και τραπεζογραμμάτια σε κυκλοφορία. Πληρώνεις / εισπράττεις οτιδήποτε μπορείς να συναλλαχθείς, η πιο γνωστή και πιο άμεση μέθοδος).
- **Ø** Η πληρωμή μέσω επιταγών (δηλ. σε συνεργασία με κάποια τράπεζα, η οποία σου διαθέτει ένα μπλοκ επιταγών, μπορείς να πληρώνεις και να αγοράζεις καταγράφοντας πάνω τους το αντίστοιχο ποσό που χρειάζεσαι, φυσικά μη παραλείποντας να συμπληρώσεις σε ειδικά πλαίσια που βρίσκονται πάνω στο έντυπο τα προσωπικά σου στοιχεία και την υπογραφή σου, όπως ακόμα το ποσό που θα συμπληρώσεις θα πρέπει να το γράψεις αριθμητικά αλλά και ολογράφως. Ουσιαστικά είναι καταθέσεις όψεως, δηλαδή, τραπεζικοί λογαριασμοί τους οποίους οι καταθέτες χρησιμοποιούν άμεσα για την αγορά αγαθών και υπηρεσιών εκδίδοντας τραπεζικές επιταγές).
- **Ø** Η πληρωμή μέσω πιστωτικών καρτών (δηλ. σε συνεργασία με μία τράπεζα, ο πελάτης διαθέτει μία πιστωτική κάρτα. Όταν ο πελάτης επιθυμεί να αγοράσει ένα αγαθό χρησιμοποιεί την πιστωτική του κάρτα. Ο

πωλητής καταγράφει τα στοιχεία της κάρτας του πελάτη φτιάχνοντας ένα έγγραφο συναλλαγής. Το έγγραφο αυτό υπογράφεται από τον αγοραστή και εν συνεχεία προωθείται στην τράπεζα για διεκπεραίωση. Εν τέλη η τράπεζα χρεοπιστώνει τους εκάστοτε λογαριασμούς, πληροφορώντας τα εμπλεκόμενα μέρη για την συναλλαγή που πραγματοποιήθηκε.

Το χρήμα σήμερα

Η εξέλιξη της κοινωνίας και της τεχνολογίας δεν θα μπορούσε να αφήσει ανέγγιχτο και τον τρόπο των χρηματικών συναλλαγών. Η παγκοσμιοποίηση είναι πλέον γεγονός και το χρήμα πρέπει και αυτό να ακολουθήσει αυτό το πρότυπο, διότι οι γρήγοροι ρυθμοί που απαιτούν οι νέες συνθήκες στον τρόπο ζωής και διαβίωσης των ανθρώπων ζητούν άμεσα αποτελέσματα και σε κάθε ενέργεια που θέλουν να παρέμβουν. Έτσι λοιπόν δημιουργήθηκε και μία άλλη μορφή του χρήματος, η λεγόμενη «ηλεκτρονική» όπου θα αναφερθούμε στις ενότητες που ακολουθούν.

Α) **Ηλεκτρονικές Πληρωμές**

Με βάση το σύγχρονο επιχειρηματικό και καταναλωτικό περιβάλλον και τη συνεχόμενη και αυξανόμενη εμπορευματοποίηση του διαδικτυακού χώρου δημιουργήθηκε το ηλεκτρονικό εμπόριο.

Αυτό όμως έφερε άλλα ζητήματα, όπως τον τρόπο που θα γίνουν οι συναλλαγές με ηλεκτρονική μορφή και κατά πόσο αυτό είναι εφικτό να πραγματοποιηθεί;

Η ανάγκη λοιπόν για την ανάπτυξη νέων μορφών πληρωμών, προσαρμοσμένες για ηλεκτρονικές συναλλαγές, είναι οι λεγόμενες ηλεκτρονικές πληρωμές. Άρα λίγο πολύ μιλάμε για το νέο χρήμα της εποχής μας, την μεγαλύτερη επανάσταση στον τομέα των συναλλαγών από τότε που χρησιμοποιήθηκε ο χρυσός, το λεγόμενο **«Ψηφιακό Χρήμα»**.

Αυτό που διαφέρει στις ηλεκτρονικές πληρωμές σε σχέση με τις παραδοσιακές είναι ότι στην ηλεκτρονική μορφή των πληρωμών, υπάρχει ένα ψηφιακό περιβάλλον όπου είναι σχεδιασμένο ώστε να είναι ηλεκτρονικά διαχειρίσιμο.

i. Ψηφιακό Χρήμα, Μικροπληρωμές και Έξυπνες κάρτες

Το ψηφιακό χρήμα θα μπορούσε να θεωρηθεί το νόμισμα σε ψηφιακή μορφή. Διότι και το ψηφιακό χρήμα έχει ακριβώς την ίδια ιδιότητα με το νόμισμα. Ουσιαστικά μιλάμε για έναν μηχανισμό εξόφλησης μικροσυναλλαγών ή μικροπληρωμών μέσω του διαδικτύου όπου είναι πολύ χρήσιμο για την μεταφορά μικροποσών (small money transfers).

Άρα μιλάμε για συναλλαγές όπου το ύψος των ποσών φτάνουν συνήθως σε μικρή χρηματική αξία και αφορούν τις λεγόμενες μικροϋπηρεσίες πληροφοριών (information mini-services), όπου η πρόσβαση σε ιστοσελίδες στο διαδίκτυο χρεώνονται και είναι κατάλληλες για αγορά άυλων προϊόντων, όμως με τη χρήση μιας πιστωτικής κάρτας μπορούν να αποβούν πολλαπλάσια της καθαρής αξίας του προϊόντος, επομένως η χρήση του ψηφιακού χρήματος συνιστάται ως η καλύτερη λύση όχι μόνο γιατί αποτελούν μία έξυπνη λύση για μικρές αγορές μέσω διαδικτύου αλλά και επειδή χαρακτηρίζεται κατάλληλη από πλευράς ταχύτητας και κόστους επεξεργασίας πληρωμών.

Αρχικά το όριο που καθορίστηκε από το ευρωπαϊκό ινστιτούτο τεχνολογικών σπουδών μαζί με το παρατηρητήριο συστημάτων ηλεκτρονικών πληρωμών ήταν 25 ευρώ. Μετά όμως κατέληξαν να το μειώσουν ακόμα πιο πολύ και να φτάσει στα 5 ευρώ.

Άρα μιλάμε για εφαρμογή μιας ηλεκτρονικής πληρωμής η οποία είναι το νέο κύμα εφαρμογών στην εποχή του ηλεκτρονικού εμπορίου. Η έννοια του ψηφιακού χρήματος είναι στενά συνδεδεμένη με τις κάρτες και τα ηλεκτρονικά κουπόνια και σε ότι υπάρχει σε αυτά τα δύο είδη.

Λειτουργία και χρήση ψηφιακού χρήματος

Όπως αναφέραμε και παραπάνω το ψηφιακό χρήμα είναι το νόμισμα σε ψηφιακή μορφή. Δηλαδή μιλάμε για μία ακολουθία ψηφίων.

Εδώ λοιπόν μπαίνει και ο ρόλος της τράπεζας όπου αυτή την ακολουθία ψηφίων μπορεί να την διανείμει και να χρεώσει τον λογαριασμό του αγοραστή με μια ανάληψη που θα ζητήσει ο χρήστης μεταφέροντας το ποσό αυτό στον ηλεκτρονικό του υπολογιστή.

Για λόγους εξασφάλισης, το ψηφιακό χρήμα που παραχωρείται στη τράπεζα σημαδεύεται με την ψηφιακή της σφραγίδα πριν από την μεταφορά του, στον υπολογιστή του καταναλωτή. Αυτό είναι και το λεγόμενο κουπόνι ή αλλιώς η χρηματική ροή (token). Ο αγοραστής με την σειρά του αποστέλλει τώρα αυτός την αντίτιμη αξία του ψηφιακού χρήματος στον προμηθευτή.

Ο προμηθευτής προωθεί το κουπόνι στην τράπεζα όπου έλαβε από τον αγοραστή για να κάνει έλεγχο εγκυρότητας και πιστοποίησης σε αυτήν την συναλλαγή. Αφού εγκριθεί μπορεί να εξαργυρώσει το κουπόνι.

Για την διασφάλιση ότι κάθε κουπόνι χρησιμοποιείται μόνο μία φορά, η τράπεζα καταγράφει τον σειριακό αριθμό της χρηματικής ροής καθώς ξοδεύεται. Στην περίπτωση που η τράπεζα ανακαλύψει ότι ο σειριακός αριθμός είναι ήδη καταγραμμένος στη βάση δεδομένων, ενημερώνει τον προμηθευτή ότι πρόκειται για εξαπάτηση και του κάνει ακύρωση του κουπονιού διότι αυτή η χρηματική μονάδα είναι άχρηστη.

Τυφλές υπογραφές

Τυφλές υπογραφές (blind signature), είναι ένας μηχανισμός όπου αναπτύχθηκε από την DigiCash και αναφέρεται στους αγοραστές οι οποίοι επιθυμούν να μην γνωστοποιήσουν την ταυτότητα τους και να μπορεί να προμηθευτεί ηλεκτρονικό χρήμα από την τράπεζα χωρίς η τράπεζα να έχει την δυνατότητα να κάνει συσχέτιση του αγοραστή με τα κουπόνια που του διαθέτονται.

Η τράπεζα κάνει κανονικά τον έλεγχο της για την καταλληλότητα του κουπονιού που λαμβάνει από τον προμηθευτή, αλλά δεν έχει την δυνατότητα να γνωρίζει ποιός έκανε την πληρωμή.

Απαιτήσεις ασφάλειας για το ηλεκτρονικό χρήμα

- **Εμπιστευτικότητα (Confidentiality).** Όταν μιλάμε για εμπιστευτικότητα ουσιαστικά εννοούμε την ασφάλεια σε ένα ηλεκτρονικό περιβάλλον όπου θα μας διαβεβαιώνει ότι το περιεχόμενο των μηνυμάτων που συναλλασσόμαστε είναι απόρθητο και προστατευμένο από επιτήδειους εισβολείς.
- **Ακεραιότητα (Integrity)**. Όταν μιλάμε για ακεραιότητα σημαίνει ότι αυτό που επιθυμούμε σε μία ηλεκτρονική συναλλαγή είναι τα δεδομένα που αποστέλλονται ως μέρος της συναλλαγής να μην αλλοιώνονται ή τροποποιούνται κατά τη διάρκεια της μεταφοράς και αποθήκευσής τους στο δίκτυο.
- **΄Ελεγχος Αυθεντικότητας (Authentication).** Ο έλεγχος αυθεντικότητας είναι μία διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα, η πιστοποίηση της ταυτότητας των επιχειρήσεων που συμμετέχουν σε μία συναλλαγή είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να μπορεί να πεισθεί για την ταυτότητα του άλλου.
- **Εξουσιοδότηση (Authorization)**. Η εξουσιοδότηση είναι ότι ο ιδιοκτήτης παραχωρεί στον χρήστη το δικαίωμα να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στον λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.
- **Εξασφάλιση (Assurance).** Λέγοντας εμπιστοσύνη, εννοούμε ότι ο έμπορος ο οποίος συναλλάσσεται με τον εκάστοτε πελάτη έχει την δυνατότητα να τον διαβεβαιώσει ότι είναι νόμιμος και έμπιστος.
- **Μη αποποίηση ευθύνης (Non-repudiation).** Ούτε ο πωλητής αλλά ούτε και ο αγοραστής δεν πρέπει να έχουν τη δυνατότητα να αρνηθούν τη συμμετοχή τους σε μια συναλλαγή.

ii. Είδη Ηλεκτρονικού χρήματος

1) Πιστωτικές κάρτες

Είναι η μορφή του λεγόμενου «πλαστικού χρήματος». Η έκδοση τους γίνεται από πιστωτικούς αποδεκτούς και αναγνωρισμένους οργανισμούς και δίνουν την δυνατότητα στους κατόχους τους, να μπορούν να αγοράζουν αγαθά ή να πληρώνουν υπηρεσίες μέσω αυτών χωρίς να απαιτείται άμεση καταβολή της αξίας τους. Η μορφή της πιστωτικής κάρτας είναι μία πλαστική κάρτα όπου από την μία της πλευρά αναφέρει το ονοματεπώνυμο του κατόχου της, τον αριθμό μητρώου της, την ημερομηνία της λήξης της και το κατάστημα (τράπεζα) όπου την χορήγησε. Και από την άλλη πλευρά παρατηρούμε μία μαγνητική ταινία, ένα πλαίσιο για την υπογραφή του κατόχου της και η επωνυμία του καταστήματος που την εξέδωσε. Επίσης η κάθε πιστωτική κάρτα διαθέτει και ένα προσωπικό αριθμό το λεγόμενο P.I.N. (Personal Identification Number), όπου μιλάμε για έναν αριθμό ο οποίος πρέπει να διατηρηθεί αυστηρά απόρρητος και ο κάτοχος της κάρτας πρέπει να τον φυλάσσει με πολύ μεγάλη προσοχή και να μην υπάρχει κανένα στοιχείο που μπορεί να αποκαλύπτει τον μυστικό κωδικό της κάρτας γιατί είναι απαραίτητος σε συνδυασμό με την κάρτα για την πραγματοποίηση συναλλαγών. Η πιο καλή λύση είναι ή απομνημόνευση του κωδικού.

Όπως αναφέραμε και παραπάνω στις τυπικές μεθόδους πληρωμών : « Σε συνεργασία με μία τράπεζα, ο πελάτης διαθέτει μία πιστωτική κάρτα. Όταν ο πελάτης επιθυμεί να αγοράσει ένα αγαθό χρησιμοποιεί την πιστωτική του κάρτα. Ο πωλητής καταγράφει τα στοιχεία της κάρτας του πελάτη φτιάχνοντας ένα έγγραφο συναλλαγής. Το έγγραφο αυτό υπογράφεται από τον αγοραστή και εν συνεχεία προωθείται στην τράπεζα για διεκπεραίωση. Εν τέλη η τράπεζα χρεοπιστώνει τους εκάστοτε λογαριασμούς, πληροφορώντας τα εμπλεκόμενα μέρη για την συναλλαγή που πραγματοποιήθηκε».

Ακόμα θα μπορούσαμε να χωρίσουμε τις πιστωτικές κάρτες σε τρείς κατηγορίες:

- Πιστωτικές κάρτες όπου λειτουργούν μόνο εντός της χώρας όπου έχει δημιουργηθεί.
- Πιστωτικές κάρτες όπου μπορούν να λειτουργήσουν και έξω από τα σύνορα της χώρας της οποίας ανήκει.
- Οι λεγόμενες Golden Cards ή Prestige Cards, ελληνιστί οι χρυσές κάρτες όπου διαθέτουν υψηλό πιστωτικό όριο και εξασφαλίζουν ισχυρά ασφαλιστικά πακέτα, νομική προστασία όπως και πολλά προνόμια και παροχές.

Τα πλεονεκτήματα τα οποία διαθέτει μία πιστωτική κάρτα είναι :

- Ο κάτοχός δεν χρειάζεται να διαθέτει μετρητά μαζί του διακινδυνεύοντας να τα χάσει, έχει την δυνατότητα να κάνει τις οικονομικές του συναλλαγές με την πιστωτική του κάρτα αυτό του προσφέρει να έχει ασφάλεια στις συναλλαγές που επιθυμεί να κάνει.
- Υπάρχει μία περίοδος χάριτος περίπου 25 ή 40 ημέρες αναλόγως το κατάστημα όπου δεν υπάρχει τόκος για την εξόφληση κάποιας αγοράς από την ημερομηνία έκδοσης του λογαριασμού έως την ημερομηνία πληρωμής.
- Υπάρχει ένα πιστωτικό όριο όπου αυτό βοηθά τον κάτοχο της, να μην υπερβεί το ποσό το οποίο μπορεί να διαθέσει σύμφωνα με την οικονομική του κατάσταση, διότι μιλάμε για ένα άυλο χρήμα, και υπάρχουν μεγάλες πιθανότητες κάποιος να μην έχει την αντίληψη για το τί ξοδεύει.
- Υπάρχει δυνατότητα ανάληψης μετρητών 24 ώρες το 24ωρο σε αντιστοιχία βέβαια με το πιστωτικό όριο του καθενός.

Τα μειονεκτήματα που θα μπορούσε να έχει η πιστωτική κάρτα είναι :

- Ότι όταν κάποιος επιθυμεί να διαθέτει μία πιστωτική κάρτα θα πρέπει να διαβάζει προσεκτικά τους όρους χρήσης των πιστωτικών καρτών, διότι μερικές φορές οι τόκοι που μπορεί να έχουν, υπάρχει περίπτωση να μην συμφέρουν τον ενδιαφερόμενο και συνήθως αυτοί οι όροι είναι τα λεγόμενα «ψιλά γράμματα».
- Η κάρτα επειδή είναι ουσιαστικά μικρή σε μέγεθος, υπάρχει κίνδυνος απώλειας ή κλοπής. Γενικά είναι εύκολο να χαθεί.

- Αν ξεπεράσουν την ημερομηνία λήξης μιας αγοράς που είχαν κάνει για την εξόφληση της, οι τόκοι μπορεί να ανέβουν κατά πολύ.
- Αν έχουν ένα εύκολο PIN, υπάρχει δυνατότητα να είναι εύκολο και να ανακαλυφθεί κυρίως από άτομα που γνωρίζουν τον κάτοχο της.

Επίσης η χρήσεις της πιστωτικής κάρτας είναι :

- Παροχές για ασφάλιση τροχαίου δυστυχήματος, ταξιδιωτική ασφάλιση κ.α.
- Υπάρχει η δυνατότητα λήψης επιπρόσθετου συναλλάγματος για ταξίδια στο εξωτερικό
- Διαθέτει ευνοϊκά τουριστικά πακέτα με εκπτώσεις στις τιμές των ξενοδοχείων
- Χρησιμοποιείται σε ενοικιάσεις αυτοκινήτων
- Ο κάτοχος της μπορεί να ενημερωθεί , μέσω ειδικών περιοδικών που τους αποστέλλονται, για προσφορές καταστημάτων όπου έχουν προγράμματα μεταχρονολογημένων χρεώσεων και προγράμματα άτοκων δόσεων.

Στην χρήση της πιστωτικής κάρτας στο διαδίκτυο οι διαδικασίες που επακολουθούν είναι περίπου οι ίδιες. Απλά αυτό που θέλει περισσότερη προσοχή στις ηλεκτρονικές συναλλαγές είναι ότι έχουν ληφθεί κάποια επιπρόσθετα μέτρα στους μηχανισμούς ασφάλειας που σημαίνει περισσότερες πιστοποιήσεις τόσο για τον αγοραστή όσο και για τον προμηθευτή.

Το γεγονός αυτό έχει οδηγήσει στην ύπαρξη μιας ποικιλίας συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες. Δύο από τα χαρακτηριστικά που προσδιορίζουν και διαφοροποιούν τα συστήματα αυτά, είναι το επίπεδο της ασφάλειας των συναλλαγών, και το λογισμικό που απαιτείται από όλα τα εμπλεκόμενα μέρη (αγοραστής προμηθευτής, τράπεζα).

Όταν γίνεται μία on-line συναλλαγή, ο χειρισμός των πιστωτικών καρτών μπορεί πραγματοποιηθεί με δύο τρόπους :

- Η αποστολή μη κρυπτογραφημένων στοιχείων της ηλεκτρονικής πληρωμής από τον αγοραστή στον προμηθευτή. Βέβαια η μέθοδος αυτή δεν θα

μπορούσε να θεωρηθεί και τόσο ασφαλής, γιατί υπάρχει κίνδυνος υποκλοπής των στοιχείων αυτών από εισβολείς.

- Η αποστολή κρυπτογραφημένων στοιχείων της ηλεκτρονικής πληρωμής από τον αγοραστή στον προμηθευτή. Φυσικά είναι και ο πιο ασφαλής τρόπος και προβλέπει την κρυπτογράφηση όλων πληροφοριών που σχετίζονται με τη πληρωμή πριν την αποστολή τους στον προμηθευτή μέσω του διαδικτύου .

Για την ασφάλεια αυτών των συναλλαγών έχουν δημιουργηθεί και τα αντίστοιχα πρωτόκολλα ασφαλείας που θα αναφέρουμε σε αυτό το κεφάλαιο ονομαστικά αλλά θα τα αναλύσουμε στις επόμενες ενότητες.

- Secure Sockets Layer (SSL)
- Cybercash
- Έμπιστη Τρίτη Οντότητα (ΕΤΟ)
- Secure Electronic Transactions (SET)
- Joint Electronic Payments Initiative (JEPI)

Σύμφωνα με μελέτες που έχουν γίνει, έχει εκτιμηθεί ότι το πλαστικό χρήμα θα αναπτυχθεί με ραγδαίο ρυθμό στα επόμενα χρόνια και θα βγουν πολύ κερδισμένες από αυτό οι τράπεζες και το μάρκετινγκ που χρησιμοποιούν.
Πολλά καταστήματα στο εξωτερικό εκδίδουν πιστωτικές κάρτες και έχουν κερδίσει ένα σημαντικό αριθμό πελατών. Και πλέον και οργανισμοί της Ελλάδας έχουν προβεί σε αυτό όπως ο ΑΝΤ-1VISA, . Παναθηναϊκός FC-Visa, Ολυμπιακός Visa, πολιτιστικοί οργανισμοί όπως η Artion Visa σε συνεργασία με τον Οργανισμό Μεγάρου Μουσικής Αθηνών.

Επίσης σημαντική άνοδο παρουσιάζουν και οι χρεωστικές τραπεζικές κάρτες, οι οποίες έχουν την δυνατότητα να πραγματοποιεί αγορές με απευθείας χρέωση του λογαριασμού του χωρίς κανένα όριο ή επιβάρυνση με τόκους. Ακόμη οι λεγόμενες "έξυπνες κάρτες" (smart cards), που θα αποτελέσουν έναν σημαντικό νέο τρόπο συναλλαγών λειτουργώντας ως ηλεκτρονικά πορτοφόλια..

2) Χρεωστικές Τραπεζικές Κάρτες

Χρεωστικές τραπεζικές κάρτες ή αλλιώς κάρτα αποθηκευμένης αξίας, είναι ουσιαστικά μία προπληρωμένη κάρτα όπου δεν υπάρχει έκδοση χρημάτων αλλά απλά είναι ένας δίαυλος παράδοσης χρηματικού ποσού σε ηλεκτρονική μορφή. Και η κάρτα αυτή έχει την δυνατότητα ο χρήστης της να είναι ανώνυμος ή επώνυμος. Ακόμα όταν ο κάτοχος της επιθυμεί να είναι ανώνυμος μπορεί να την μεταβιβάσει από αυτόν σε ένα άλλο άτομο ενώ η επώνυμη δεν παρέχει αυτή την κίνηση. Η χρεωστική κάρτα μπορεί να εφαρμοστεί και στο διαδίκτυο.

Οι δυνατότητες που έχει η χρεωστική κάρτα είναι :

- Πληρωμές λογαριασμών και συνδρομών (π.χ. ΔΕΗ, ΟΤΕ, ΙΚΑ, ΦΠΑ, εταιρείες κινητής τηλεφωνίας, συνδρομητική τηλεόραση)
- Απευθείας σύνδεση με τον Τρεχούμενο ή Λογαριασμό Ταμιευτηρίου
- Ενημέρωση για τις κινήσεις των εξόδων που γίνονται
- Δεν υπάρχει πληρωμή τόκων ή χρεώσεων.
- Οι συναλλαγές γίνονται χωρίς μετρητά και επιταγές.
- Στη διακίνηση χρημάτων από την χώρα του κατόχου σε οποιαδήποτε άλλη χώρα.
- Τρόπος πληρωμής είναι αρκετά εύκολος και πρακτικός (απλή εντολή, πάγια εντολή, μεταχρονολογημένη εντολή)
- Να γίνουν αγορές και αναλήψεις μετρητών από ATMs και ταμεία τραπεζών.
- Ασφάλεια Αγορών στην χώρα του κατόχου αλλά και στο εξωτερικό, από κλοπή, απώλεια και τυχαία ζημιά.

3) Έξυπνες κάρτες (smart cards)

Οι έξυπνες κάρτες ήταν η αφορμή για την δημιουργία του ηλεκτρονικού χρήματος. Οι κάρτες αυτές είναι πλαστικές με μαγνητικές γραμμές που χρησίμευαν για την αποθήκευση δεδομένων όπως :

- Προσωπικοί αριθμοί αναγνώρισης.
- Αποθήκευση χρηματικής αξίας, όπου αναλόγως με τις κινήσεις που πραγματοποιούνται,μειώνονται τα ποσά.
- Στις μεταφορές.
- Στις βιβλιοθήκες για ανατύπωση αντιγράφων.
- Στις τηλεφωνικές συνδιαλέξεις.

Πλέον η νέα γενιά έξυπνων καρτών διαθέτει προγραμματισμένες λειτουργίες με μικροτσίπς προσωπικής ταυτότητας. Επίσης αποτελούν μια εξέλιξη των φυσικών κουπονιών που χρησιμοποιούνται. Η κάρτα αυτή προπληρώνεται και όταν το ποσό των χρημάτων που διαθέτει εξαντληθεί, υπάρχει η δυνατότητα να ξαναενισχυθεί εκ νέου ανώνυμα ή επώνυμα. Οι κάρτες αυτές επίσης ανατροφοδοτούνται από επιλεκτικά σημεία πώλησης όπως οι τράπεζες και πλέον οι χρήστες τους έχουν ξεχωριστή κάρτα για κάθε ενέργεια τους.

Γενικά οι έξυπνες κάρτες είναι χρήσιμες γιατί :

- Τα δεδομένα τα οποία διαθέτει είναι κρυπτογραφημένα έτσι ώστε, να μην κινδυνεύει από υποκλοπές και τροποποιήσεις. Επίσης η δυνατότητα παραγωγής ψηφιακών πιστοποιητικών καθιστά η κάθε κάρτα να είναι μοναδική. Έτσι αν υπάρχει παραποίηση, ανιχνεύεται αυτόματα όπως επίσης και η μη εξουσιοδοτημένη χρήση είναι αδύνατον να πραγματοποιηθεί, γιατί η χρήση των έξυπνων καρτών είναι αυστηρά προσωπική και για να γίνει χρέωση ενός ποσού στην κάρτα, είναι προσβάσιμη μόνο στον νόμιμο κάτοχο της.
- Το λογισμικό τους διαθέτει πολύ ασφαλή και αξιόπιστα μέτρα προστασίας και αυτό συμβαίνει για την αποτροπή εξωτερικών εισβολών. Τα μέτρα

προστασίας υλικού επίσης έχουν παραβλεφθεί για την ασφάλεια που πρέπει να παρέχουν στο υλικό μέχρι και τα κυκλώματα για επιβεβαίωση της ταυτότητας των χρηστών.

- Έχουν πολύ μικρό κόστος κατασκευής διότι το υλικό που είναι φτιαγμένα, είναι πραγματικά πολύ φθηνό σε αντίθεση με την μεγάλη ανάπτυξη που γνωρίζει η βιομηχανία τεχνολογικών προϊόντων.

Τα μειονεκτήματα που θα μπορούσαν να έχουν οι έξυπνες κάρτες είναι :

- Η πιθανότητα να κλαπούν ή να χαθούν.
- Να καταρριφθεί η ασφάλεια της από την εξέλιξη και της αρνητικής τεχνολογίας, ώστε να είναι μετά θέμα χρόνου να μπορέσουν να «σπάσουν» τους κωδικούς της.
- Λόγω των νέων συνθηκών ζωής που όλα πλέον έχουν ηλεκτρονική μορφή ένα πρόβλημα να υπάρξει σε αυτόν τον μηχανισμό μπορεί να αποφέρει την κατάρρευση όλου του συστήματος.
- Την ανεξέλεγκτη χρήση του χρήματος από τον άνθρωπο όπου επειδή έχει χάσει την επαφή του με το πραγματικό χρήμα δεν αντιλαμβάνεται πόσα λεφτά ξοδεύει.

Στο μέλλον πάντως υπολογίζεται ότι η πληρωμή της κάρτας θα γίνεται μέσω ηλεκτρονικού υπολογιστή, συνδεδεμένο είτε στο δίκτυο της τράπεζας είτε στο διαδίκτυο.

Οι πιο γνωστές κάρτες είναι οι Mondex και Visacash όπου με αυτές υπάρχει η δυνατότητα ενίσχυσης χρημάτων στην κάρτα, πληρωμή διάφορων προϊόντων και υπηρεσιών ακόμα και στο διαδίκτυο και τέλος για ενημέρωση κινήσεων και χρηματικού υπολοίπου.

Οι έξυπνες κάρτες διαθέτουν δύο τύπους συστήματος ηλεκτρονικών πληρωμών :

- Ανοικτά συστήματα όπου η άμεση μεταφορά χρηματικού ποσού μεταξύ καρτών είναι εφικτή.
- Κλειστά συστήματα όπου το ποσό της κάρτας μπορεί να αυξηθεί από ένα τραπεζικό λογαριασμό ο οποίος θα είναι μοναδικός και το χρήμα που έχει κινηθεί θα μεταφερθεί στον τραπεζικό λογαριασμό του αποδέκτη.

4) Ψηφιακό πορτοφόλι (Digital wallet)

Το ψηφιακό πορτοφόλι ουσιαστικά είναι το ψηφιακό χρήμα. Η δυνατότητες του είναι όταν ο χρήστης θέλει να κάνει αγορά μέσω διαδικτύου, δημιουργεί ένα προφίλ on line που τα στοιχεία που εμφανίζει είναι της πιστωτικής κάρτας, την διεύθυνση της χρέωσης και αποστολής. Αυτό το σύστημα βοηθά στην διεκπεραίωση των συναλλαγών γιατί δεν υπάρχει η επανάληψη της συμπλήρωσης των στοιχείων του κατόχου κάθε φορά που επιθυμεί να κάνει αγορές μέσω διαδικτύου. Δηλαδή με λίγα λόγια είναι ένας τρόπος χρήσης της πιστωτικής κάρτας όπου ο κάτοχος δίνει τον αριθμό της κάρτας του, όπου είναι κρυπτογραφημένος, στην εταιρεία που διαθέτει το ψηφιακό πορτοφόλι και έτσι αυτή η μέθοδος δίνει μία ασφαλή και γρήγορη λύση. Επίσης με το ψηφιακό πορτοφόλι ο χρήστης μπορεί να ενημερωθεί για προσφορές που τον ενδιαφέρουν όπως και να αποθηκεύσει τις προτιμήσεις του σε κάποια προϊόντα που τον απασχολούν.

5) Ηλεκτρονικές Επιταγές

Όπως αναφέραμε και παραπάνω στις τυπικές μεθόδους πληρωμών : «Σε συνεργασία με κάποια τράπεζα, η οποία σου διαθέτει ένα μπλοκ επιταγών, μπορείς να πληρώνεις και να αγοράζεις καταγράφοντας πάνω τους το αντίστοιχο ποσό που χρειάζεσαι, φυσικά μη παραλείποντας να συμπληρώσεις σε ειδικά πλαίσια που βρίσκονται πάνω στο έντυπο τα προσωπικά σου στοιχεία και την υπογραφή σου, όπως ακόμα το ποσό που θα συμπληρώσεις θα πρέπει να το γράψεις αριθμητικά

αλλά και ολογράφως. Ουσιαστικά είναι καταθέσεις όψεως όπου είναι τραπεζικοί λογαριασμοί τους οποίους οι καταθέτες χρησιμοποιούν άμεσα για την αγορά αγαθών και υπηρεσιών εκδίδοντας τραπεζικές επιταγές».

Ουσιαστικά μια επιταγή είναι ένα μήνυμα που στέλνεται στην τράπεζα του πελάτη για να μεταφέρει το κεφάλαιο από το λογαριασμό του στον λογαριασμό κάποιου άλλου. Αφού επιτευχθεί η μεταφορά, η εξοφλημένη επιταγή επιστρέφει στον αποστολέα και μπορεί να χρησιμοποιηθεί ως απόδειξη πληρωμής.

Μια ηλεκτρονική επιταγή διαθέτει όλα τα παραπάνω χαρακτηριστικά μόνο που η ηλεκτρονική επιταγή αρχικά αποστέλλεται στον αποδέκτη ο οποίος την υπογράφει και την αποστέλλει στην τράπεζα για να εισπράξει το αντίστοιχο ποσό.

Από θέμα ασφάλειας όσο παράξενο και αν φαίνεται η ηλεκτρονική επιταγή θεωρείται η πιο έμπιστη. Διότι ο αποστολέας έχει την δυνατότητα να κωδικοποιήσει τον αριθμό του λογαριασμού του με το δημόσιο κλειδί της τράπεζας, και έτσι δεν μπορεί να πέσει θύμα απάτης γιατί δεν αποκαλύπτεται ο αριθμός του λογαριασμού του.

Υπάρχουν δύο συστήματα που έχουν αναπτυχθεί για να δίνουν την δυνατότητα στον αγοραστή να χρησιμοποιεί ηλεκτρονικές επιταγές για την άμεση πληρωμή των εμπόρων του δικτύου:

- **Cybercash** Είναι η εξέλιξη των πιστωτικών καρτών και μπορεί να χρησιμοποιηθεί για την συναλλαγή πληρωμών με τους εμπλεκόμενους πωλητές. Δεν είναι διαμεσολαβεί για την εκτίμηση των επιταγών, για αυτό είναι υπεύθυνες οι τράπεζες.
- **Εταιρεία Τεχνολογιών Οικονομικών Υπηρεσιών (Financial Services Technology Corporation – FSTC)** Είναι το αποτέλεσμα μιας συνεργασίας που έγινε μεταξύ τραπεζών και πιστωτικών οργανισμών. Αυτή η συνεργασία δημιούργησε μία ηλεκτρονική επιταγή όπου επιτρέπει την ψηφιακή υπογραφή για πιστοποίηση και εξακρίβωση. Οι ηλεκτρονικές επιταγές μπορούν να παραδοθούν είτε με άμεση παράδοση μέσω ενός δικτύου ή μέσω ηλεκτρονικού ταχυδρομείου.

Έτσι λοιπόν οι ηλεκτρονικές επιταγές προτιμούνται από το καταναλωτικό κοινό γιατί :

- Γιατί το ποσοστό των καταναλωτών που διαθέτει λογαριασμούς με επιταγές είναι μεγαλύτερο από αυτό που διαθέτει πιστωτικές κάρτες .
- Γιατί διαθέτει στους χρήστες διάφορες επιλογές επιταγών ανάλογα με τις ανάγκες τους χρησιμοποιώντας ένα μοναδικό ηλεκτρονικό μπλοκ επιταγών όπου όλες οι συναλλαγές είναι συγκεντρωμένες σε ένα μοναδικό αρχείο λογαριασμών.
- Γιατί ο καταναλωτής έχει δοσοληψίες με την δική του τράπεζα για να χρησιμοποιεί διάφορους τρόπους πληρωμής όπως επιταγές, ΑΤΜ κ.α. αντί να μπλέκει με πλήθος οικονομικών θεσμών.

Η εξέλιξη λοιπόν και η αναβάθμιση της τραπεζικής υποδομής και του διαδικτύου βοηθά πολύ αυτό τον τρόπο πληρωμής.

II. E-BANKING

"Το e-banking (ή Internet banking) υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές. "Μεταφέρει" την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω Διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών, παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών, καθώς και πλήθος άλλων υπηρεσιών.

Οι πελάτες (ιδιώτες και επιχειρήσεις) ωφελούνται σημαντικά από τη χρήση των υπηρεσιών e-banking, καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με την τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για τις εταιρείες, το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα

εξοικονομείται πολύτιμος χρόνος.

Με το e-banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής. Συχνό είναι και το φαινόμενο των προσφορών ή της εφαρμογής ευνοϊκότερων όρων στην παροχή προϊόντων μέσω Internet, γεγονός που από μόνο του είναι ικανό να προσελκύσει σημαντική μερίδα καταναλωτών που αναζητούν προσφορές.

Μορφές e-Banking

- A.T.M.
- EFT/POS
- Phone-banking
- Mobile-banking
- TV-banking
- Online-banking
- Home-banking

Το internet-banking

Κατηγοριοποιείται σε τρία βασικά επίπεδα παροχής υπηρεσιών

- Δικτυακοί τόποι (web sites) βασικού πληροφοριακού περιεχομένου
- Web Sites απλών συναλλαγών
- Web Sites προηγμένων συναλλαγών

Οι βασικότερες υπηρεσίες που παρέχουν μέσω Internet οι ελληνικές τράπεζες είναι οι εξής:

- Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς.
- Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ιδίου νομίσματος.
- Πληροφορίες σχετικά με τις πρόσφατες κινήσεις των τηρούμενων λογαριασμών.
- Δυνατότητα έκδοσης και αποστολής παλαιότερων κινήσεων των τηρούμενων λογαριασμών.
- Παραγγελία μπλοκ επιταγών.

- Παρακολούθηση επιταγών.
- Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκ επιταγών.
- Εντολές αγοραπωλησίας μετοχών.
- Ενημέρωση για την κίνηση των προσωπικών αμοιβαίων κεφαλαίων.
- Δυνατότητα υποβολής αιτήσεων εμβασμάτων.
- Αλλαγή του απορρήτου κωδικού PIN.
- Προσωπικά μηνύματα.
- Αποστολή τακτικών πληρωμών.
- Πληρωμές λογαριασμών επιχειρήσεων κοινής ωφέλειας.
- Διαχείριση διαθεσίμων.
- Πληρωμή μισθοδοσίας.
- Πληρωμή εταιρικών πιστωτικών καρτών.
- Επιλογές ασφαλιστικών πακέτων.
- Λοιπά πληροφοριακά στοιχεία.

Λόγοι περιορισμένης ανάπτυξης του internet banking

- Σχετικός χαμηλός βαθμός διείσδυσης του διαδικτύου
- Περιορισμένη τεχνολογική εξοικείωση και εκπαίδευση των χρηστών
- Έλλειψη εμπιστοσύνης για την ασφάλεια των συναλλαγών

III. ΑΠΕΙΛΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Οι ασφαλείς συναλλαγές είναι σημαντικές διότι καθιερώνουν την εμπιστοσύνη ανάμεσα στο χρήστη και στην εταιρεία / τράπεζα. Όταν ένα πρόσωπο, πράγμα, γεγονός ή ιδέα το οποίο αποτελεί κίνδυνο για κάποιο αγαθό(asset) σε σχέση με την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή/και τη νόμιμη χρήση(legitimate use) του συγκεκριμένου αγαθού τότε απειλείται **(threat).**

Οι απειλές εκφράζονται ως ηλεκτρονικό έγκλημα, ως εξής:

- μη εξουσιοδοτημένη πρόσβαση στα υπολογιστικά συστήματα

κακόβουλα προγράμματα
ιοί, δούρειοι ίπποι, παγίδες , κλπ.
πειρατεία λογισμικού
παράνομη χρήση ηλεκτρονικών ή δικτυακών πόρων,κλπ.

§ απάτη στις ηλεκτρονικές συναλλαγές
ψηφιακή αντιγραφή εντύπων, κλπ.

Α) Ηλεκτρονικές απειλές

i. Spam

Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου, χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Το Spam συχνά έχει την μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο e-γραμματοκιβώτιο μας χωρίς να έχουμε ζητήσει την εν λόγω πληροφόρηση. Η αλληλογραφία αυτή λοιπόν, μπορεί να χαρακτηριστεί ως **ανεπιθύμητη αλληλογραφία,** όρος που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam.

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.

Το spam υποσκάπτει την εμπιστοσύνη των χρηστών ηλεκτρονικών υπηρεσιών και οδηγεί σε απώλεια χρόνου, πόρων και παραγωγικότητας, τόσο για τους ίδιους τους χρήστες, όσο και για τις επιχειρήσεις. Προβλήματα δημιουργεί επίσης και στους Παρόχους Υπηρεσιών Διαδικτύου (ΠΥΔ), καθώς μπορεί να μειώσει την ποιότητα των παρεχόμενων υπηρεσιών και τον χρόνο απόκρισης του δικτύου τους, πλήττοντας έτσι τη διαθεσιμότητα και αξιοπιστία τους. Ενδεικτικά αναφέρεται ότι πάνω από το 70% των μηνυμάτων ηλεκτρονικού ταχυδρομείου σήμερα είναι spam.

Επιπλέον, τα μηνύματα spam, εκτός από ενοχλητικά, μπορεί να είναι προσβλητικά, απατηλά ή ακόμα και επικίνδυνου περιεχομένου. Για παράδειγμα αρκετά μηνύματα spam σήμερα διαφημίζουν πλαστά προϊόντα (π.χ. φαρμακευτικά προϊόντα ή προϊόντα λογισμικού) ως προϊόντα γνωστών εταιρειών, διαδίδουν παραπλανητικές ειδήσεις ή/και προωθούν προϊόντα και υπηρεσίες σεξουαλικού ή/και πορνογραφικού χαρακτήρα. Επίσης, τα μηνύματα spam χρησιμοποιούνται συχνά και ως μέσα μετάδοσης ιών ή άλλων επιβλαβών ή/και κατασκοπευτικών λογισμικών που σκοπεύουν στην "κατάληψη" του υπολογιστή του χρήστη και την μετέπειτα χρήση του ως μέσο αποστολής νέων μηνυμάτων spam. Μεγάλη έκταση επίσης έχει πάρει το spam τύπου ***phising*** που στοχεύει στην παραπλάνηση των χρηστών και στην εκμαίευση προσωπικών τους δεδομένων, συχνά με απώτερο σκοπό την απάτη και την απόσπαση χρηματικών ποσών μέσω τραπεζικών λογαριασμών.

Τι πρέπει να κάνουμε

- Δίνουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου μας μόνο σε πρόσωπα ή οργανισμούς που γνωρίζουμε και εμπιστευόμαστε. Αν πρέπει να δώσουμε τη διεύθυνση μας, π.χ. για εγγραφή σε κάποιο ηλεκτρονικό περιοδικό ή στο πλαίσιο χρήσης ηλεκτρονικών υπηρεσιών, ελέγχουμε αν μας δίνεται η δυνατότητα να δηλώσετε ότι δεν επιθυμείτε την αποστολή διαφημιστικών μηνυμάτων ή άλλων πληροφοριών. Κατά τη χρήση ηλεκτρονικών υπηρεσιών, ελέγχουμε τη πολιτική ιδιωτικότητας (privacy policy) που εφαρμόζει η συγκεκριμένη εταιρεία ή οργανισμός πριν αποκαλύψουμε τα προσωπικά δεδομένα μας μέσω του Διαδικτύου. Βεβαιωθείτε ότι υπάρχει δέσμευση της εταιρείας ή του οργανισμού να μην διαβιβάσουν τα προσωπικά σας δεδομένα σε τρίτους.
- Αποφεύγουμε την δημοσιοποίηση της διεύθυνσης ηλεκτρονικού ταχυδρομείου σε Διαδικτυακούς τόπους, μηχανές αναζήτησης, ηλεκτρονικές λίστες,

καταλόγους ή chat rooms του Διαδικτύου. Οι spammers συνήθως χρησιμοποιούν μηχανισμούς αυτόματης συλλογής διευθύνσεων από τα ανωτέρω σημεία του Διαδικτύου (μια τακτική γνωστή ως "harvesting" - συγκομιδή).

- Αν θέλουμε να αναρτήσουμε τα στοιχεία μας σε κάποιο Διαδικτυακό τόπο, γράφουμε την ηλεκτρονική διεύθυνση με τρόπο που δεν επιτρέπει την αυτόματη συλλογή της από τους spammers. Για παράδειγμα, μπορούμε να παραλείψουμε το σύμβολο "@" που είναι χαρακτηριστικό του ηλεκτρονικού ταχυδρομείου.
- Χρησιμοποιούμε ΠΑΝΤΑ λογισμικό φιλτραρίσματος. Το λογισμικό αυτό μπορεί να εντοπίσει μεταξύ των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου αυτά που είναι SPAM και, ανάλογα με τις ρυθμίσεις που έχουν γίνει από τον χρήστη, είτε να "μπλοκάρει" τα μηνύματα SPAM, είτε να τα τοποθετήσει σε ειδικό φάκελο.

Βέβαια το φιλτράρισμα αυτό είναι χρήσιμο, αλλά δεν είναι πάντα αποτελεσματικό. Μερικές φορές τα φίλτρα αποτυγχάνουν στον εντοπισμό των μηνυμάτων SPAM, ενώ κάποιες άλλες φορές χαρακτηρίζουν ως SPAM μηνύματα που δεν είναι SPAM.

ii. Virus (ιός)

Η διάδοση της χρήσης Η/Υ, αλλά και ειδικότερα του Internet τα τελευταία 25 χρόνια, αποτέλεσε αφορμή για μια ιδιαίτερα μικρή κατηγορία προγραμματιστών να πειραματιστούν πάνω σε κάτι που ίσως φαντάζει σε πολλούς ανόητο ή και τρελό. Στην ανάπτυξη μικρών προγραμμάτων που θα κάνουν τον Η/Υ να «τρελαίνεται» ή και να «αρρωσταίνει» για κάποιο διάστημα. Ή ακόμα, σκεπτόμενοι την χαρά που θα έπαιρναν αν έβλεπαν τον Η/Υ του «εχθρού» τους να χαλάει μια και καλή, δίχως τρόπο επισκευής του! Κάπως έτσι, μάλλον σαν μια κακόγουστη φάρσα, ξεκίνησε η ανάπτυξη και συγγραφή ιών για λειτουργικά συστήματα υπολογιστών. Βέβαια, όσο πέρναγε ο καιρός η όλη «αστεία» πλευρά της υπόθεσης εξανεμίστηκε.

1) Είδη ιών

- **Μεταμορφικός ιός**

Ένας ιός είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό.

Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του.

Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο, την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του.

Κάποιοι άλλοι ιοί δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά

προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash).

Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων.

- **Πολυμορφικοί**

Πολυμορφικοί ονομάζονται οι ιοί, οι οποίοι κρύβουν τον κώδικά τους με διαφορετικό τρόπο, κάθε φορά που μολύνουν ένα εκτελέσιμο αρχείο (συνήθως .exe, .com). Έτσι, όταν ο χρήστης εκτελέσει το μολυσμένο αρχείο, ο ιός «ξεκλειδώνει» τον καταστροφικό κώδικα μέσα από το μολυσμένο εκτελέσιμο αρχείο και τον εκτελεί. Αυτός ο τύπος ιών, αποτελεί ένα ιδιαίτερο «πονοκέφαλο» για τα προγράμματα antivirus, διότι δεν υπάρχει πάντα ένα συγκεκριμένο/παρόμοιο κομμάτι του ιού για να χρησιμοποιηθεί για την αναγνώρισή του.

- **Stealth (αόρατοι) viruses**

Χρησιμοποιούν τους καταχωρητές μνήμης του Η/Υ. Για να εκτελεστεί ένα πρόγραμμα (ιδιαίτερα τα προγράμματα MS-DOS), χρειάζεται να επικαλεστούν μια διεύθυνση στη μνήμη του Η/Υ. Εκεί ακριβώς επεμβαίνει και ο ιός. Όταν το πρόγραμμα καλέσει την συγκεκριμένη διεύθυνση, ενεργοποιείται ο ιός αντί για το πρόγραμμα, με αποτέλεσμα την μόλυνση του συστήματος. Οι stealth ιοί έχουν και μια επιπλέον λειτουργία. Είναι ικανοί να κρύβονται κατά την ανίχνευσή τους από τα προγράμματα antivirus. Συγκεκριμένα, όποτε ανιχνεύουν δράση προγράμματος antivirus, αποκαθιστούν προσωρινά το αρχικό αρχείο στην κανονική του θέση, αφήνοντας το antivirus να το ανιχνεύσει και το ξανά-μολύνουν αργότερα, αφού έχει τελειώσει η λειτουργία του προγράμματος antivirus. Η συγκεκριμένη λειτουργία της απόκρυψης του ιού από το antivirus λέγεται και “tunneling”.

Parasitic a.k.a. Appending viruses

Λέγονται παρασιτικοί ή και επι-προσθετικοί, ακριβώς γιατί προσθέτουν τον καταστροφικό τους κώδικα μέσα στον κώδικα του αρχικού αρχείου (συνήθως στο

τέλος του, για προστασία από ανίχνευση antivirus προγράμματος), χωρίς να το καταστρέψουν. Όμως, αν κάποιος πιστέψει ότι θα εκτελεστεί το αρχικό πρόγραμμα, επειδή ο κώδικας του ιού βρίσκεται στο τέλος του αρχείου, τότε την «πάτησε», μιας και ο ιός φροντίζει να εκτελείται αυτός και όχι το αρχικό πρόγραμμα.

- **Overwriting viruses**

Ο απλούστερος τρόπος για να μολύνεις ένα σύστημα είναι να αντικαταστήσεις το αρχικό αρχείο με τον ιό. Με τον τρόπο αυτό ΔΕΝ υπάρχει δυνατότητα αποκατάστασης (καθαρισμού) του αρχικού αρχείου. Οι ιοί αυτοί μπορούν ακόμα να διατηρούν το αρχικό μέγεθος του αρχείου, αποφεύγοντας έτσι την ανίχνευσή τους από προγράμματα antivirus. Παρά τις δυνατότητές τους, θεωρούνται «αναξιοπρεπείς» για ένα «σοβαρό» συγγραφέα ιών.

- **Companion viruses**

Πρόκειται για ιούς που ενεργούν κυρίως σε λειτουργικό MS-DOS. Όταν ο χρήστης πληκτρολογήσει μια εντολή DOS (π.χ. Program1) και δεν βρεθεί το αρχείο Program1.exe, τότε το λειτουργικό θα εκτελέσει το αρχείο Program1.com, που θα είναι και ο ιός. Προσοχή όμως! Αν ο χρήστης θελήσει να εκτελέσει το αρχείο Program1.exe, ενώ ταυτόχρονα υπάρχει στο δίσκο και ο ιός με το όνομα Program1.com, τότε με την πληκτρολόγηση Program1 θα εκτελεστεί ο ιός!

- **Retro viruses**

Πρόκειται για ιούς που στοχεύουν αποκλειστικά στην καταπολέμηση ενός ή περισσοτέρων προγραμμάτων antivirus.

- **Logic bombs**

Πρόκειται για ιούς που ενεργοποιούνται όταν επέλθει μια συγκεκριμένη χρονική στιγμή, π.χ. στις 12.00 το μεσημέρι στις 12 του Σεπτέμβρη. Συνήθως επιτελούν καταστροφικό έργο, όπως διαγραφή αρχείων κ.ά.

- **Droppers**

Είναι εκτελέσιμα αρχεία, που περιέχουν εντολές για την δημιουργία ιού μέσα στο σύστημα και δεν περιέχουν τον ίδιο τον ιό. Ανιχνεύονται πιο δύσκολα σε σύγκριση με τους απλούς ιούς.

- **Boot sector viruses**

Οι ιοί αυτού του είδους μολύνουν τον τομέα εκκίνησης του Η/Υ, είτε αυτός είναι δίσκος ή δισκέτα. Σε αυτούς οφείλεται το μεγαλύτερο ποσοστό μολύνσεων ανά τον κόσμο. Συνήθως, δεν είναι απαραίτητο να υπάρχει λειτουργικό MS-DOS στον Η/Υ για να ενεργοποιηθεί ένας τέτοιος ιός, μιας και οι συγκεκριμένοι ιοί δεν κάνουν τέτοιου είδους … διακρίσεις. Π.χ. παρ' ότι ο ιός Michelangelo δε μπορεί να επεκταθεί σε λειτουργικό Windows NT, δεν σημαίνει ότι δε θα διαγράψει τα περιεχόμενα του δίσκου στις 6 Μαρτίου!

- **Direct action viruses**

Οι ιοί αυτοί εκτελούν το καταστροφικό τους έργο μόνο όταν εκτελεστούν (μια φορά δηλαδή) και δεν μένουν στην μνήμη του Η/Υ.

- **Macro viruses**

Είναι οι γνωστοί ιοί, που μολύνουν χρησιμοποιώντας μια μακρο-εντολή. Μολύνουν **ΜΟΝΟ** έγγραφα τύπου Word, Excel, Office, PowerPoint, Access. Πρόκειται για ιούς που διαδίδονται πάρα πολύ εύκολα. Χαρακτηριστικό παράδειγμα η ίδια η Microsoft, η οποία όταν πρωτο-κυκλοφόρησε την έκδοση MS Office '97, είχε αφήσει μέσα στο cd ένα κείμενο μολυσμένο με macro-ιό.

- **Multi Platform viruses**

Πρόκειται για ιούς που επιδρούν σε περισσότερα από ένα λειτουργικά συστήματα. Συνήθως όμως, όταν ένας ιός είναι ικανός να ενεργοποιηθεί σε περιβάλλον Windows, δεν θα κάνει απολύτως τίποτα σε περιβάλλον Apple.

2) Τρόποι μετάδοσης ιών

- Εκκίνηση του Η/Υ από μολυσμένη δισκέτα ή μολυσμένο.
- Εκτέλεση/άνοιγμα μολυσμένων αρχείων (.exe, .com, .vbs, .dll, .pif, .scr, .sh, .bat κ.ά) που επισυνάπτονται σε emails.
- Εκτέλεση/άνοιγμα μολυσμένων αρχείων (.exe, .com, .doc, .bat, .hlp, .htm, .ini, .js, .php, .pif, .reg, .ppt, .sh, .shs, .sys, .vbs, .wbt, .xls κ.ά.)
- Άνοιγμα/ανάγνωση emails που συνήθως στέλνουν άγνωστα σε εμάς άτομα, διότι πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του email.
- Άνοιγμα/ανάγνωση μολυσμένων ιστοσελίδων .htm και .html.
- Μέσω πρόσβασης στο internet. Συγκεκριμένα, όλα σχεδόν τα λειτουργικά συστήματα, και κυρίως τα Windows, έχουν "τρύπες" ασφαλείας τις οποίες εκμεταλλεύονται κάποιοι ιοί για να μολύνουν τον Η/Υ, **ΧΩΡΙΣ** να ζητήσουν σε οποιαδήποτε περίπτωση την άδεια του χρήστη για εγκατάσταση κάποιου προγράμματος.

Τρόποι προστασίας από ιούς

- Τήρηση αντιγράφων ασφαλείας σε cd ή δισκέτα.Τακτική ανίχνευση όλου του δίσκου/δισκετών με το αντιβιοτικό πρόγραμμα.
- Συχνή ανανέωση (update) του αντιβιοτικού προγράμματος.
- Ανίχνευση κάθε νέου αρχείου που «κατεβάζουμε» από το Internet.
- Ενεργοποιούμε ΕΝΑ real-time-scan antivirus monitor κατά την λειτουργία του Η/Υ.
- Δεν επισκεπτόμαστε κάθε ιστοσελίδα που μας προτείνει ένας άγνωστος. Μπορεί να περιέχει κώδικα ιού, ο οποίος ΔΕΝ φαίνεται με την απλή ματιά.
- Απενεργοποιούμε το άνοιγμα java ή active x εφαρμογών στον Internet Browser.
- Επιλέγουμε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ .
- Διατηρούμε και ανανεώνουμε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.

- Χρησιμοποιούμε κάποιο πρόγραμμα Firewall
- Χρησιμοποιούμε κάποιο πρόγραμμα anti-spyware .
- Κάνουμε συχνά update στο λειτουργικό σύστημα του Η/Υ (κυρίως στα Windows), ώστε να καλύπτονται τα όποια κενά ασφαλείας έχουν εντοπιστεί.

iii. Trojan horses (δούρειοι ίπποι)

Ονομάζεται έτσι, γιατί (όπως και ο Δούρειος Ίππος της Τροίας) μπορεί να μπει στον υπολογιστή μέσω διαδικασιών που θεωρούνται ακίνδυνες, όπως για παράδειγμα μέσω ενός παιχνιδιού ή μέσω ενός προγράμματος ανίχνευσης ιών και έτσι μπορεί να ξεγελάσει το χρήστη κρύβοντας την παρασκηνιακή του δραστηριότητα.

Στην επιστήμη των υπολογιστών, ο **Δούρειος Ίππος,** είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία, ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Το όνομά του προκύπτει από την *Ιλιάδα* του Ομήρου, όπου αναγράφεται ότι ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου, στην κοιλιά του οποίου κρύβονταν Αχαιοί πολεμιστές.

Η τακτική που χρησιμοποιούν τα προγράμματα Trojans είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας, κρύβουν μέσα τους κακόβουλο κώδικα, ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά, οι Trojans μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας, με αποτέλεσμα ο υπολογιστής να μολυνθεί. Σύνηθες αποτέλεσμα της μόλυνσης από Δούρειο Ίππο, είναι η εγκατάσταση κάποιου προγράμματος, που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς υπολογιστές. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

Υπάρχουν δύο είδη Δούρειων Ίππων:

- κανονικά προγράμματα, τα οποία διάφοροι hackers μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για

παράδειγμα διάφορα προγράμματα διαμοιρασμού αρχείων (peer-to-peer), προγράμματα ανακοίνωσης καιρικών συνθηκών κοκ.

- μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Ένας δούρειος ίππος μπορεί να δράσει και ως κατάσκοπος, δηλ να ξεκινήσει να καταγράφει οτιδήποτε πληκτρολογεί ο χρήστης. Με τον τρόπο αυτό συλλέγει πληροφορίες κωδικών πρόσβασης, λογαριασμών και άλλων προσωπικών δεδομένων.

Αντίθετα με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς κοκ), οι Trojans δεν μπορούν να δράσουν αυτόνομα, αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα. Για το λόγο αυτό είναι αβλαβή προγράμματα, μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Επίσης οι Trojan horses δε μπορούν να πολλαπλασιαστούν όπως οι ιοί, γι’ αυτό και δεν θεωρούνται από πολλούς ως ιοί.

iv. Worms (σκουλήκια)

Είναι ένας ιός που αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του, διαμέσου των δικτύων ηλεκτρονικών υπολογιστών. Χρησιμοποιεί το Internet, ως μέσο διάδοσής του (emails, irc chat κ.ά.). Δρουν αυτόνομα και χρησιμοποιούν τα δίκτυα ηλεκτρονικών υπολογιστών για να πολλαπλασιάζονται και να στέλνουν αντίγραφά τους σε άλλα συστήματα. Ένα σκουλήκι, μπορεί να βλάψει ένα δίκτυο και μπορεί να μειώσει κατά πολύ την ταχύτητα σύνδεσης στο Διαδίκτυο, καταναλώνοντας όλους τους πόρους του υπολογιστή και να οδηγήσει ακόμη και σε κλείσιμο του υπολογιστή. Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές, χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host).

v. Dialers

Ο dialer είναι ένα πρόγραμμα, το οποίο χωρίς να το γνωρίζει ο χρήστης, σταματά τη σύνδεση στο Διαδίκτυο, μέσω του παρόχου και εκτρέπει τη σύνδεση σε μια διεθνή γραμμή, κάτι που έχει ως αποτέλεσμα υπέρογκους λογαριασμούς τηλεφώνου. Αυτό

συμβαίνει συνήθως, όταν ο χρήστης επισκεφθεί μια ιστοσελίδα με ύποπτο ή πορνογραφικό περιεχόμενο, ή αναξιόπιστες ιστοσελίδες. Ένας dialer, μπορεί επίσης να εισέλθει στον υπολογιστή μέσω spam.

Οι dialers μπορούν να δράσουν μόνο στις συνδέσεις μέσω modem. Για το λόγο αυτό, ο χρήστης μπορεί να ζητήσει από τον πάροχό του φραγή διεθνών κλήσεων. Με τον τρόπο αυτό , ο dialer δε θα μπορεί να εκτρέψει τη σύνδεση στο εξωτερικό.

vi. Spoofing

Ο όρος **IP spoofing,** αναφέρεται στην δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης, ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.

Το IP spoofing, χρησιμοποιείται κυρίως σε επιθέσεις άρνησης υπηρεσιών (DOS - Denial of Service). Οι επιθέσεις αυτού του είδους, έχουν ως στόχο να γεμίσουν τον υπολογιστή-θύμα με πολλά πακέτα, ούτως ώστε να τον αναγκάσουν να περιέλθει σε δυσλειτουργία και να μην μπορεί να εξυπηρετήσει σωστά τους νόμιμους χρήστες του. Σε τέτοιες περιπτώσεις ο επιτιθέμενος δεν ενδιαφέρεται να λάβει απάντηση στα πακέτα που στέλνει, οπότε συνήθως χρησιμοποιεί την τεχνική IP spoofing, ούτως ώστε να κατευθύνει τις απαντήσεις του θύματος προς κάποιον άλλο υπολογιστή . Η τεχνική αυτή προσφέρει ακόμα ένα πλεονέκτημα!! Κρύβει την ταυτότητα του επιτιθέμενου.

Ο επιτιθέμενος στις περισσότερες περιπτώσεις διαλέγει μία τυχαία IP διεύθυνση για να τοποθετηθεί στην κεφαλίδα του IP πακέτου, προσέχοντας όμως η διεύθυνση αυτή να μην είναι σε απαγορευμένη περιοχή.

Μια άλλη χρήση του IP spoofing, είναι για το σπάσιμο των μηχανισμών ασφαλείας δικτύων υπολογιστών. Σε πολλά εταιρικά δίκτυα, είναι συνηθισμένο η αναγνώριση των χρηστών να γίνεται μέσω των IP διευθύνσεών τους. Για παράδειγμα, ενδέχεται ένας υπολογιστής να είναι ρυθμισμένος ούτως ώστε να επιτρέπει την πρόσβαση χωρίς username και password, όταν διαπιστώσει ότι η σύνδεση προέρχεται από κάποια συγκεκριμένη IP (πχ. την IP του υπολογιστή που χρησιμοποιεί ο διευθυντής).

Αυτό όμως συνιστά τρύπα ασφαλείας, αφού οποιοσδήποτε εργαζόμενος μπορεί να χρησιμοποιήσει την τεχνική IP spoofing για να κατασκευάσει πακέτα IP με ψεύτικη

διεύθυνση προέλευσης και έτσι να αποκτήσει πρόσβαση στον συγκεκριμένο υπολογιστή.

Ο όρος spoofing, χρησιμοποιείται γενικά για να περιγράψει κάθε μορφής αλλοίωση στην κεφαλίδα ενός πακέτου, η οποία έχει ως στόχο να παραπλανήσει τον παραλήπτη του πακέτου. Η τεχνική αυτή χρησιμοποιείται και από spammers, για την αλλοίωση των κεφαλίδων του ηλεκτρονικού ταχυδρομείου, ούτως ώστε ο παραλήπτης να μην μπορεί να τους εντοπίσει.

vii. Keylogger

Ένα keylogger, είναι ένα επιβλαβές πρόγραμμα που τρέχει σχεδόν αόρατα ως χαμηλή διαδικασία συστημάτων επιπέδων. Αυτό το πρόγραμμα καταγράφει όλα τα κλειδιά, ό,τι δακτυλογραφείται και στέλνει έπειτα τις πληροφορίες στο πρόσωπο που μόλυνε τον υπολογιστή με το keylogger.

Το keylogger, είναι εξαιρετικά επικίνδυνο και μπορεί να χρησιμοποιηθεί για να κλέψει τις προσωπικές πληροφορίες του χρήστη, όπως τον αριθμό πιστωτικών καρτών, κωδικούς πρόσβασης κτλ. Αυτό μπορεί να οδηγήσει στην κλοπή ταυτότητας ή την κλοπή γενικά. Το keylogger, είναι ιδιαίτερα επικίνδυνο σε καθέναν που χρησιμοποιεί το διαδίκτυο για τραπεζικές και άλλες οικονομικές συναλλαγές .

viii. Rootkits

Ο όρος rootkit, χρησιμοποιείται για να περιγράψουμε τους μηχανισμούς και τις τεχνικές όπου κακόβουλα προγράμματα, συμπεριλαμβανομένων ιών, spyware και trojans προσπαθούν να κρυφτούν από προγράμματα προστασίας από ιούς και spyware. Δηλ ένα rootkit, είναι ένα σύνολο εργαλείων λογισμικού που προορίζεται για να κρύψει τις τρέχουσες διαδικασίες, τα αρχεία ή τα στοιχεία συστημάτων από το λειτουργικό σύστημα. Το rootkit, έχει την προέλευσή του, στις σχετικά καλοκάγαθες εφαρμογές, αλλά τα τελευταία χρόνια έχει χρησιμοποιηθεί όλο και περισσότερο από το malware, για να βοηθήσει τους εισβολείς να διατηρήσουν την πρόσβαση στα συστήματα, αποφεύγοντας την ανίχνευση.

Υπάρχουν διάφορες κατηγορίες κατάταξης των rootkits, ανάλογα με το αν το κακόβουλο πρόγραμμα συνεχίζει να υπάρχει μετά από επανεκκίνηση του υπολογιστή και με το αν εκτελείται σε επίπεδο χρήστη ή κελύφους. Τα

Υπάρχουν πολλοί τρόποι, με τους οποίους τα rootkits προσπαθούν να αποφύγουν την ανίχνευση. Για παράδειγμα, ένα rootkit σε επίπεδο χρήστη, μπορεί να ανιχνεύει όλες τις κλήσεις στα APIs των Windows FindFirstFile/FindNextFile, τα οποία χρησιμοποιούνται από λειτουργίες διαχείρισης του αρχείων συστήματος, όπως ο Explorer και η γραμμή εντολών.

Όταν μια εφαρμογή εκτελεί μια καταλογράφηση φακέλου που θα επέστρεφε τα αποτελέσματα που θα περιείχαν αρχεία σχετιζόμενα με το rootkit, το rootkit παρεμβαίνει και τροποποιεί τα αποτελέσματα της καταλογράφησης ώστε να μην φαίνονται τα αρχεία αυτά.

Τα rootkits σε επίπεδο κελύφους, είναι ακόμα πιο ισχυρά καθώς, όχι μόνο παρεμβάλλονται στα native API του επίπεδου κελύφους, αλλά μπορούν απευθείας να χειρίζονται δομές δεδομένων . Μια συνηθισμένη τεχνική για να κρύβεται η παρουσία ενός κακόβουλου προγράμματος/διεργασίας, είναι η αφαίρεση της διεργασίας από τις ενεργές διεργασίες στην λίστα του κελύφους. Αφού τα APIs που χειρίζονται διεργασίες, βασίζονται στα περιεχόμενα αυτής της λίστας, η κακόβουλη διεργασία δεν θα φαίνεται σε εργαλεία διαχείρισης εργασιών, όπως το Task Manager ή το Process Explorer.

Τα προγράμματα αυτά δεν βρίσκονται στο επίπεδο του χρήστη, αλλά ζουν και λειτουργούν στον πυρήνα (kernel) του λειτουργικού συστήματος, όπου δε μπορούν τα προγράμματα antivirus να ψάξουν (λόγω δικαιωμάτων). Ουσιαστικά, πρόκειται για προγράμματα που κρύβουν αρχεία και προγράμματα και δεν αφήνουν ίχνη.

ix. Malware

Ο όρος προέρχεται από τον συνδυασμό των συνθετικών των λέξεων MALicious (βλαβερό) και softWARE (λογισμικό). Πρόκειται δηλ, για λογισμικό που μπορεί να απειλήσει την ασφάλεια του χρήστη και του ηλεκτρονικού υπολογιστή.

x. Spyware

Είναι ένα πρόγραμμα, που μπορεί να προσκολληθεί κρυφά σε αρχεία που κατεβάζουμε από το διαδίκτυο. Μόλις κατέβει, αυτοεγκαθίσταται στον υπολογιστή και ξεκινάει την παρακολούθηση της διαδικτυακής δραστηριότητας του χρήστη.

Οι πληροφορίες που καταγράφει, αποστέλλονται σε τρίτους που τις περισσότερες φορές ενδιαφέρονται να δημιουργήσουν το προφίλ του χρήστη και να ξεκινήσουν την αποστολή διαφημιστικού ή άλλου υλικού προς το χρήστη, ανάλογα με τα ενδιαφέροντα του τελευταίου. Το spyware, μπορεί επίσης να συγκεντρώσει πληροφορίες για τις διευθύνσεις ηλεκτρονικού ταχυδρομείου , για τους κωδικούς πρόσβασης ακόμη και για τους αριθμούς των πιστωτικών καρτών.

Το spyware, μοιάζει με τους δούρειους ίππους, στο γεγονός ότι εισέρχεται στον υπολογιστή κατά τη διάρκεια εγκατάστασης ενός φαινομενικά ακίνδυνου λογισμικού, χωρίς να το αντιλαμβάνεται ο χρήστης. Επιπλέον, στέλνει τις πληροφορίες που συλλέγει στην εγχώρια βάση των spyware, μέσω της σύνδεσης του χρήστη.

Εκτός από τα θέματα της ηθικής και της προστασίας της ιδιωτικής ζωής, το spyware μειώνει την ευρυζωνικότητα του χρήστη και χρησιμοποιεί πόρους της μνήμης του υπολογιστή. Με τον τρόπο αυτό, οι εφαρμογές που τρέχουν στο παρασκήνιο μπορούν να οδηγήσουν σε γενικότερη αστάθεια του συστήματος ή ακόμη και στην κατάρρευσή του.

xi. Adware

Είναι μια μορφή spyware, που συλλέγει πληροφορίες για το προφίλ του χρήστη, με στόχο να προβάλλει αργότερα διαφημίσεις στο φυλλομετρητή του (web browser) , με βάση τις πληροφορίες που έχει συλλέξει, σε σχέση με τις συνήθειες του χρήστη στο σερφάρισμα.

xii. Scumware

Το scumware, αλλάζει τον τρόπο με τον οποίο βλέπει ο χρήστης τους ιστοχώρους που επισκέπτεται. Στην ουσία , αντικαθιστά το πραγματικό τους περιεχόμενο με διαφημίσεις, από τους διαφημιστές scumware και παράγει κίνηση για αυτούς.

xiii. Phishing

Το **phishing,** είναι μία μέθοδος υποκλοπής προσωπικών στοιχείων, αξιοποιήσιμων για μη εξουσιοδοτημένες/παράνομες οικονομικές συναλλαγές στο Διαδίκτυο. Το ιδιότυπο αυτό «ψάρεμα», επιχειρείται όλο και συχνότερα με τη χρήση συνδυασμού **spam mail** και «πλαστών» ιστοσελίδων, που μιμούνται όσο πειστικότερα μπορούν, τα αντίστοιχα των νόμιμων επιχειρήσεων/χρηματοπιστωτικών οργανισμών.

Συνήθως, κάποιο email που έρχεται στο Inbox του χρήστη, φαίνεται ότι προέρχεται από έμπιστη πηγή, ωστόσο, κάποιο περιεχόμενο (ή περισσότερα) link οδηγεί σε παραποιημένη σελίδα κάπου στο δίκτυο, με στόχο την άντληση των στοιχείων των χρηστών-θυμάτων (πχ. αριθμοί πιστωτικών καρτών, e-mails), που οι ίδιοι οι εξαπατημένοι χρήστες δηλώνουν σε ένα είδος φόρμας, θεωρώντας ότι πρόκειται για μια επίσημη και σοβαρή ιστοσελίδα κάποιου οργανισμού, εταιρείας ή υπηρεσίας.

Άλλος τρόπος εξαπάτησης είναι το «φύτεμα» **trojan horse** (δούρειου ίππου), το οποίο εγκαθίσταται στον υπολογιστή του χρήστη - εν αγνοία του φυσικά - το οποίο του έχει σταλεί μέσω ηλεκτρονικού ταχυδρομείου (μέσω θεωρητικά έμπιστης πηγής, π.χ. φίλους κτλ) ή το έχει κατεβάσει πάλι εν αγνοία του από κάποια θεωρητικά ή φαινομενικά «αθώα»ιστοσελίδα.

Επίσης, διάφορα sites που περιέχουν παράνομο λογισμικό ή «ροζ» περιεχόμενο, μπορεί να περιέχουν στις σελίδες τους τέτοιες εφαρμογές, οι οποίες μπορεί να μη γίνουν ποτέ αντιληπτές από το χρήστη και που «επεξεργάζονται» τα προσωπικά του δεδομένα, αποστέλλοντας τις πληροφορίες σε κάποιο άγνωστο email account ή σε κάποιο άλλο προορισμό, που είναι αδύνατο να εντοπίσει ο απλός χρήστης, χωρίς εξειδικευμένες γνώσεις. Ένα τέτοιο παράδειγμα είναι τα **Key Loggers**, που συγκεντρώνουν σε ένα αρχείο, οτιδήποτε πληκτρολογεί ο χρήστης και ενδεχομένως να το αποστέλλουν σε κάποια email accounts ή σε κάποιο άγνωστο server.

Τι μπορούμε να κάνουμε για να αποτρέψουμε το phishing

- Ο χρήστης πρέπει να είναι καχύποπτος σε οποιοδήποτε μήνυμα ηλεκτρονικού ταχυδρομείου ζητά αξιοποιήσιμες προσωπικές πληροφορίες ευαίσθητου οικονομικού χαρακτήρα, εκτός αν είναι ψηφιακά υπογεγραμμένο. Δυστυχώς, το πρωτόκολλο που χρησιμοποιείται σήμερα στην αποστολή e-mail (SMTP), δε διασφαλίζει την πιστοποίηση της ταυτότητας του αποστολέα.
- Τα μηνύματα των phishes, συνήθως περιέχουν πληροφορίες για κάποιο πρόβλημα ή για κάποια «ευκαιρία», στην οποία τα επίδοξα θύματα «πρέπει να απαντήσουν άμεσα», είτε για να αποκατασταθεί το πρόβλημα είτε για να αδράξουν την ευκαιρία. Φυσικά δεν πρόκειται για κάποια ευκαιρία, αλλά για δόλωμα.
- Συνήθως ζητούν πληροφορίες, όπως το όνομα χρήστη και τον κωδικό πρόσβασης για οποιαδήποτε υπηρεσία, αριθμούς πιστωτικών καρτών, αριθμό ταυτότητας, διαβατηρίου κτλ. Τα στοιχεία αυτά, τους διευκολύνουν να προχωρήσουν σε πλαστοπροσωπία και άλλες απάτες. Άρα, ο χρήστης πρέπει να είναι καχύποπτος σε ό,τι πληροφορία του ζητηθεί.
- Θα ήταν καλό, να μη χρησιμοποιεί τους συνδέσμους (links) που βρίσκονται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου για να μεταφερθεί σε μια σελίδα του web, αν υποπτεύεται ότι το μήνυμα αυτό μπορεί να μην είναι αυθεντικό. Υπάρχουν αυτόματα scripts (μικρή εφαρμογή, η οποία λειτουργεί σε συνεργασία με άλλες εφαρμογές, με σκοπό την προσθήκη ειδικών λειτουργιών σε ένα Web Site. Υπάρχουν πολλών ειδών scripts, όπως τα Java Scripts, VB Scripts, CGI Scripts κ.ά.) που συλλέγουν προσωπικά στοιχεία. Επίσης, ο χρήστης πρέπει να αποφεύγει να επισκέπτεται τέτοιες σελίδες χρησιμοποιώντας τον Internet Explorer, καθώς είναι πιο ευάλωτος σε πιθανό URL spoofing
- Να αποφύγει να συμπληρώνει φόρμες με ευαίσθητα οικονομικά στοιχεία και να τις αποστέλλει μέσω ηλεκτρονικού ταχυδρομείου χωρίς να είναι κρυπτογραφημένες. Πέραν του κινδύνου απάτης, λόγω του τρόπου αποστολής των μηνυμάτων ηλεκτρονικού ταχυδρομείου γενικά (αποθηκεύονται σε πολλούς servers στην πορεία), υπάρχει πάντοτε το ρίσκο υποκλοπής των στοιχείων αυτών.

- Να δίνει πληροφορίες, όπως ο αριθμός της πιστωτικής του κάρτας ή στοιχεία λογαριασμών του μέσω ασφαλούς σύνδεσης στο web ή μέσω τηλεφώνου - στην τελευταία περίπτωση, καλύτερα να έχει κάνει αυτός το τηλεφώνημα ή να γνωρίζει με επαληθεύσιμο τρόπο ότι δίνει τις πληροφορίες στο πρόσωπο που πρέπει.
- Να εξακριβώσει και να διασφαλίσει, ότι χρησιμοποιεί ασφαλή σύνδεση web όταν δίνει τέτοιες ευαίσθητες πληροφορίες. Να προσέξει την ηλεκτρονική διεύθυνση στην οποία βρίσκεται: θα πρέπει να αρχίζει με «https://» αντί για το απλό «http://». Στην πρώτη περίπτωση επισημαίνεται ότι χρησιμοποιείτε την ασφαλή έκδοση του πρωτοκόλλου μετάδοσης υπερκειμένου (secure http).
- Υπάρχουν εφαρμογές όπως μπάρες εργαλείων (toolbars), που ενσωματώνονται στους φυλλομετρητές ιστοσελίδων (browsers), ειδικά σχεδιασμένες για την προστασία του, από απόπειρες απάτης.
- Να ελέγχει συχνά τους online λογαριασμούς σας. Να ελέγχει επίσης προσεκτικά την κίνησή τους και κάθε συναλλαγή ξεχωριστά, ώστε να είναι βέβαιος ότι εγκρίνει ό,τι έχει χρεωθεί.

Β) Computer crime (ηλεκτρονικό έγκλημα)

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου, έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο **«Ηλεκτρονικό Έγκλημα»**

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν θεωρούνται οι αξιόποινες εγκληματικές πράξεις, που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές, από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης, διαχωρίζονται σε

εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου

Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

- Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά...
- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.
- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography), να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (news groups) ή μέσα σε chat rooms..
- Οι "εγκληματίες του Κυβερνοχώρου", πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα , αποστέλλουν ηλεκτρονικά μηνύματα(e-mail) με ψευδή στοιχεία.
- Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο, ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες..
- Η έρευνα απαιτεί κατά κανόνα, συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους, είναι σπάνια.
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο, δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του

Κυβερνοχώρου καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», από ότι στον «κοινό» εγκληματικό χώρο.

Τους "εγκληματίες του Κυβερνοχώρου" μπορούμε να τους διακρίνουμε σε δύο κατηγορίες ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα:

i. Hackers

Hacker ονομάζεται το άτομο, που χωρίς εξουσιοδότηση, αποκτά παράνομη πρόσβαση, σε ένα σύστημα υπολογιστών και τα δεδομένα του, χωρίς ωστόσο να έχει πρόθεση να προκαλέσει ζημιά.

Συνήθως οι hackers, αντιμετωπίζουν τη δραστηριότητά τους ως μια πρόκληση και ευχαριστιούνται να μπαίνουν σε υψηλής ασφάλειας συστήματα υπολογιστών, στα οποία δε σκοπεύουν να προκαλέσουν κανένα είδος ζημιάς. Πολλές φορές οι hackers, μπαίνουν σε κάποιο σύστημα (π.χ. τραπεζικό ή κυβερνητικό), για να αποκαλύψουν τα «κενά» στην ασφάλεια του. Αν πετύχουν το σκοπό τους, ενημερώνουν τον ενδιαφερόμενο οργανισμό για την επιτυχία τους, ελπίζοντας σε οικονομικά οφέλη.

ii. Crackers

Cracker, ονομάζεται ένα άτομο, που χωρίς εξουσιοδότηση, αποκτά παράνομη πρόσβαση σε ένα σύστημα υπολογιστών και στα δεδομένα του, με σκοπό την πρόκληση οικονομικής ή άλλου είδους ζημιάς και την κλοπή πληροφοριών. Δηλ , σε αντίθεση με τον hacker, ο χαρακτηρισμός cracker κολλάει περισσότερο σε ανθρώπους που “σπάνε” κωδικούς και εισβάλουν σε συστήματα ή λογισμικά.

Οι crackers, προσπαθούν παράνομα να μπουν σε συστήματα υπολογιστών με σκοπό να υποκλέψουν δεδομένα και να προκαλέσουν ζημιά στις πληροφορίες που βρίσκονται στους φακέλους του συστήματος.

Για παράδειγμα, μόλις αποκτήσουν τον αριθμό μιας πιστωτικής κάρτας, τον χρησιμοποιούν προς όφελός τους.

Οι crackers, βάζουν συνήθως ιούς και άλλου είδους προγράμματα που περιέχουν ειδικό κώδικα στα συστήματα στόχους, με σκοπό να προκαλέσουν σοβαρή ζημιά. Στις περισσότερες περιπτώσεις οι κώδικές αυτοί είναι:

- Δούρειοι ίπποι, κρυμμένοι σε προγράμματα που φαινομενικά δεν είναι βλαβερά.
- Σκουλήκια, τα οποία δεν είναι κρυμμένα σε άλλα αρχεία, αλλά αποστέλλονται εκμεταλλευόμενα τα κενά στην ασφάλεια δικτύων που έχουν εντοπίσει οι crackers.
- Μια λογική βόμβα που υποδηλώνει ανενεργό κώδικα τοποθετημένο μέσα σε ένα πρόγραμμα λογισμικού και ο οποίος ενεργοποιείται σε συγκεκριμένη ημερομηνία ή συμβάν.

Γ) Firewall

Firewall, είναι μία μέθοδος για την εφαρμογή ασφαλείας, σχεδιασμένη να διατηρεί ένα δίκτυο ηλεκτρονικών υπολογιστών αδιάβλητο από παράνομες προσβάσεις.

Τα Firewall μπορούν να εφαρμοστούν στο hardware αλλά και στο software. Μπορεί να είναι μία δικλείδα, η οποία ελέγχει τις προσβάσεις ή να περιλαμβάνει ένα σύνολο δικλείδων, οι οποίες ελέγχουν την πρόσβαση σε διαφορετικά επίπεδα.

Τα Firewall χρησιμοποιούνται για να προσφέρουν στους χρήστες ασφαλή πρόσβαση στο Internet, να διαχωρίζουν τον εσωτερικό server μίας εταιρίας από αυτόν που έχει την κεντρική σελίδα της εταιρίας και να ελέγχουν τα επίπεδα πρόσβασης του προσωπικού στα συστήματα της εταιρίας.

Η κύρια λειτουργία ενός firewall, είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall, παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το δίκτυο ενός σπιτιού διαθέτει τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall, είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά.

Η σωστή πρακτική είναι το firewall να ρυθμίζεται έτσι ώστε να απορρίπτει όλες τις συνδέσεις, εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny).

Για να ρυθμιστεί σωστά ένα firewall, θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα για να ρυθμίσουν το firewall και δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow), έτσι με τη ρύθμιση αυτή το δίκτυο είναι ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

ΙΣΤΟΡΙΚΑ ΣΤΟΙΧΕΙΑ

Ο όρος firewall πρωτοεμφανίστηκε στις αρχές του 20ού αιώνα, όταν οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα για τους εσωτερικούς τοίχους, ούτως ώστε να τα κάνουν πιο ανθεκτικά στην διάδοση της φωτιάς. Σήμερα ο όρος αυτός έφτασε να σημαίνει το λογισμικό ή υλικό που παρεμβάλλεται μεταξύ δικτύων υπολογιστών ούτως ώστε να αποτρέψει την διάδοση ιών, δούρειων ίππων και τις επιθέσεις από κακόβουλους χρήστες.

Η τεχνολογία του firewall εμφανίστηκε στα τέλη της δεκαετίας του 1980, όταν ακόμη το Διαδίκτυο ήταν σε πρώιμα στάδια. Εκείνη την εποχή είχαν παρατηρηθεί αρκετές "τρύπες" ασφαλείας στο Διαδίκτυο οπότε έπρεπε να βρεθεί μία λύση. Η λύση αυτή ήταν η δημιουργία της τεχνολογίας firewall.

Το πρώτο ερευνητικό δημοσίευμα πάνω στην τεχνολογία firewall προέκυψε το 1988 όταν οι μηχανικοί της DEC (Digital Equipment Corporation) ανέπτυξαν **φίλτρα πακέτων** δεδομένων (data packet filters). Τα φίλτρα αυτά θεωρούνται ως η πρώτη γενιά firewall.

Τα **φίλτρα πακέτων** δρουν ως εξής: Διαβάζουν τα πακέτα δεδομένων που διακινούνται από το ένα δίκτυο στο άλλο και αν κάποιο πακέτο ταιριάζει με κάποιο συγκεκριμένο κανόνα, τότε το απορρίπτουν. Ο διαχειριστής του δικτύου είναι σε θέση να ορίσει τους κανόνες βάσει των οποίων θα απορρίπτονται τα πακέτα. Αυτός ο τύπος firewall δεν ενδιαφέρεται για το αν κάποιο πακέτο ανήκει σε μία σύνδεση, δηλαδή δεν αποθηκεύει πληροφορίες σχετικά με την κατάσταση των διαφόρων συνδέσεων από το ένα δίκτυο στο άλλο (stateless packet filtering). Αντιθέτως, φιλτράρει κάθε πακέτο με βάση την πληροφορία που περιέχεται στο ίδιο το πακέτο (π.χ. διεύθυνση IP προέλευσης, διεύθυνση IP προορισμού, πρωτόκολλο, αριθμός θύρας κοκ). Επειδή τα πρωτόκολλα TCP και UDP χρησιμοποιούν τις ευρέως

διαδεδομένες θύρες, ένα firewall πρώτης γενιάς μπορεί να ξεχωρίσει τα πακέτα που αφορούν διάφορες λειτουργίες,

Τα firewall της **δεύτερης γενιάς** δρουν όπως τα firewall πρώτης γενιάς με κάποιες επιπρόσθετες λειτουργίες. Μία από αυτές είναι το γεγονός ότι πλέον εξετάζουν και την κατάσταση (state) του κάθε πακέτου, δηλαδή τη σύνδεση από την οποία προήλθε. Για τον λόγο αυτό και αναφέρονται ως **φίλτρα κατάστασης** (stateful firewalls). Τα φίλτρα αυτά κρατούν ανά πάσα στιγμή πληροφορίες για τον αριθμό και το είδος των συνδέσεων μεταξύ των δύο δικτύων και επιπλέον μπορούν να ξεχωρίσουν εάν ένα πακέτο αποτελεί την αρχή ή το τέλος μιας νέας σύνδεσης ή μέρος μιας ήδη υπάρχουσας. Οι διαχειριστές των firewalls αυτών μπορούν να ορίσουν τους κανόνες, βάσει των οποίων θα επιτρέπεται η δημιουργία συνδέσεων από το εξωτερικό δίκτυο προς το τοπικό δίκτυο. Με τον τρόπο αυτό γίνεται πιο εύκολη η πρόληψη διαφόρων ειδών επιθέσεων.

Η **τρίτη γενιά firewall** βασίζεται πλέον στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI. (Open Systems Interconnection). Το κύριο χαρακτηριστικό αυτής της γενιάς firewall είναι ότι μπορεί να αντιλαμβάνεται ποια προγράμματα και πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση (πχ FTP - File Transfer Protocon, DNS - Domain Name System, περιήγηση στο Διαδίκτυο κοκ). Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μιας υπηρεσίας.

Σήμερα σιγά σιγά εδραιώνονται τα **firewalls 4ης γενιάς**, τα οποία διαθέτουν γραφικό περιβάλλον μέσω του οποίου μπορεί ο χρήστης να κάνει τις επιλογές του, όσον αφορά την ασφάλεια του δικτύου του και να θέσει τους κανόνες, βάσει τον οποίων θα απορρίπτονται κάποια πακέτα ή συνδέσεις. Τα firewalls 4ης γενιάς, μπορούν πλέον να ενσωματωθούν στο λειτουργικό σύστημα και συνεργάζονται στενά με άλλα συστήματα ασφαλείας.

Το firewall, ουσιαστικά είναι κόμβος ελέγχου ασφάλειας, που χωρίζει το εμπιστευόμενο δίκτυο, από ένα μη εμπιστευόμενο δίκτυο και αποφασίζει ποιά κίνηση επιτρέπεται να περάσει και ποιά όχι. Η βασική δουλειά ενός firewall, είναι να διαχωρίζει τα δίκτυα και να εφαρμόζει αρχές ασφάλειας, βάσει ενός συνόλου κανόνων.

Τα χαρακτηριστικά ενός firewall περιλαμβάνουν:

1. εξασφάλιση της πρόσβασης στο δίκτυο
2. έλεγχος όλων των συνδέσεων από και προς το δίκτυο
3. φιλτράρισμα των δεδομένων βάσει προκαθορισμένων κανόνων
4. πιστοποίηση χρηστών και εφαρμογών
5. καταγραφή δραστηριοτήτων
6. δυναμική ειδοποίηση των κατάλληλων ατόμων όταν συμβεί κάποια ύποπτη δραστηριότητα

Η χρήση ενός firewall, προστατεύει το εσωτερικό δίκτυο από το Internet, αλλά γίνεται και υλοποίησή τους για εσωτερικό διαχωρισμό κάποιων τμημάτων του δικτύου από το υπόλοιπο εσωτερικό δίκτυο.

Δράσεις του Firewall

- Συνήθως είναι ένα σύστημα (μερικές εφαρμογές απαιτούν συνδυασμό περισσοτέρων συστημάτων).
- Όλη η κυκλοφορία μεταξύ δύο δικτύων περνά από το firewall. Διαχωρίζει εσωτερικά δίκτυα διαφορετικής κρισιμότητας(Demilitarize Zones).
- Μόνο επιτρεπόμενη κίνηση, όπως δηλώνεται από την security policy,αφήνεται να περάσει.
- Το firewall πρέπει να είναι προστατευόμενο σύστημα(σύνολο συστημάτων).
- Χρησιμοποιείται σαν σημείο συλλογής πληροφοριών(auditing).
- Η νέα τάση τα ορίζει σαν *Security Gateways*. Κεντρικό σημείο υλοποίησης Security Policy. Συνεργασία με πολλά προϊόντα διαφορετικής τεχνολογίας.

Αξιολόγηση των Firewalls

- Η δυνατότητα του firewall να παρέχει ένα ασφαλές περιβάλλον, πρέπει πάντα να είναι το πρωταρχικό κριτήριο στην αξιολόγηση ενός firewall.
- Είναι εξίσου σημαντικό να βρούμε κατασκευαστή με ευέλικτο πλάνο αδειοδότησης (licensing plan), ώστε να επιτρέπει την γρήγορη υλοποίηση νέων firewall χωρίς την περαιτέρω επιβάρυνση σε κόστος.
- Πριν την επιλογή firewall, είναι σημαντικό να αποφασίσουμε ποιο αρχιτεκτονικό μοντέλο θα επιλέξουμε και να ξέρουμε τα υπέρ και τα κατά κάθε διαφορετικής τεχνολογίας.

i. Τύποι firewalls

Τα firewalls διαχωρίζονται σε 4 κύριους τύπους:

- Φιλτραρίσματος πακέτων
- Εξέτασης κατάστασης
- Επιπέδου κυκλώματος
- Επιπέδου εφαρμογής

1) Firewalls φιλτραρίσματος πακέτων

Οι αρχικοί firewalls πήραν τη μορφή απλών «φίλτρων για πακέτα» που εμποδίζουν ή αφήνουν την κίνηση, συγκρίνοντας τις πληροφορίες που βρίσκονται στις επικεφαλίδες κάθε εισερχόμενου ή εξερχόμενου πακέτου με κάποιο πίνακα κανόνων ελεγχόμενης πρόσβασης και λαμβάνοντας υπόψη την IP διεύθυνση, την πόρτα της πηγής και τον προορισμό με βάση συγκεκριμένους κανόνες.

Πρακτικά μπορούμε να αναλογιστούμε έναν φρουρό σε κτιριακό συγκρότημα, που όταν ένα φορτηγό παράδοσης φθάσει με ένα πακέτο,ο φρουρός “packet filter” κοιτάζει γρήγορα για την ισχύουσα διεύθυνση του ιδιοκτήτη, ελέγχει το λογότυπο του φορτηγού για να σιγουρευτεί ότι ισχύει και τότε στέλνει το φορτηγό μέσω της πύλης να παραδώσει το πακέτο.

2) Application Proxy Firewall

Το μοντέλο του application proxy firewall, προσφέρει πολύ ανώτερο έλεγχο ασφάλειας, διότι παρέχει πλήρη ενημερότητα σε επίπεδο εφαρμογών των επιχειρήσεων συνδέσεων, εξετάζοντας τα πάντα στη μέγιστη στρώση του πλήθους των πρωτοκόλλων. Ένας τέτοιος firewall μπορεί, για παράδειγμα, εύκολα να ξεχωρίσει τις σημαντικές εντολές εφαρμογών, εφαρμόζοντας τις κατάλληλες πολιτικές για κάθε μία από αυτές.Οι proxy firewall, παρέχουν επίσης μία ενσωματωμένη proxy λειτουργία, τερματίζοντας τη σύνδεση του πελάτη στο firewall και ξεκινώντας μία νέα σύνδεση στο εσωτερικό προστατευόμενο δίκτυο.
Ο “Προσαρμόσιμος Proxy” αντιπροσωπεύει την τελευταία γενιά του firewall σχεδιασμού.Συνδυάζει τις δυνατότητες των προηγούμενων γενιών, ενώ ελαχιστοποιεί τις αδυναμίες τους.

Αδυναμίες των firewalls

Η τεχνολογία των *firewalls* δεν θα πρέπει να θεωρείται πανάκεια, μιας και ρυθμίζουμε εμείς τι μπορεί να «περάσει» και τι όχι. Τα *firewalls* δεν μπορούν να εμποδίσουν μια σειρά από περιστατικά και ενέργειες, όπως:

- Την πειρατεία συνόδου, όπου ο επιτιθέμενος παίρνει τον έλεγχο από έναν νόμιμο χρήστη.
- Το *network data sniffing* (ή *snooping*).
- Την παραποίηση δικτυακών δεδομένων.
- Την επαναδρομολόγηση δικτυακών δεδομένων.
- Τη μεταμφίεση δικτυακών δεδομένων (*spoofing*).
- Τη διαρροή πληροφοριών, σε τρίτους, από νόμιμα εξουσιοδοτημένους χρήστες.
- Τη σύνδεση *modems* σε συστήματα του εσωτερικού δικτύου για σύνδεση με εξωτερικά δίκτυα (π.χ. το *Internet*).
- Τις επιθέσεις *social engineering.*
- Την αποδοχή «μολυσμένων αρχείων», χωρίς προηγούμενο έλεγχό τους.
- Τις εσωτερικές επιθέσεις.

Τα μοντέρνα συστήματα *firewalls,* είναι -ουσιαστικά- «υβρίδια» όλων των κατηγοριών και υλοποιούνται με συνδυασμό κατάλληλου υλικού και λογισμικού.Η συγκεκριμένη τεχνολογία, δε μετρά περισσότερα από 10 χρόνια ζωής, η εκτεταμένη όμως χρήση τους δείχνει πως στο μέλλον θα αποτελέσουν βασικό -και αναπόσπαστο- κομμάτι κάθε δικτυακής αρχιτεκτονικής.

Η τάση σήμερα πρέπει να εστιάζεται στο συνδυασμό της χρήσης της ισχύος του υλικού (hardware) και της ευφυΐας του λογισμικού (software).

IV. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΜΟΝΤΕΛΩΝ ΣΥΝΑΛΛΑΓΩΝ

Το internet είναι ιδιαίτερα ευπρόσβλητο σε επιθέσεις όπως είδαμε και παραπάνω. Το ζήτημα της ασφάλειας δικτύων και συναλλαγών είναι ένα από τα πιο επίκαιρα και ταυτόχρονα αμφιλεγόμενα ζητήματα σήμερα, ειδικά σε χώρες που υστερούν σε σχετική εκπαίδευση και τεχνολογική ανάπτυξη όπως η Ελλάδα. Το πρόβλημα στην πραγματικότητα είναι ο τρόπος λειτουργίας των ηλεκτρονικών συναλλαγών και η έλλειψη σωστής ενημέρωσης και πρακτικής. Οι on-line αγοραστές όμως υπάρχουν και ένα μεγάλο ποσοστό από αυτούς δηλώνει πως η ασφάλεια δεδομένων αποτελεί από τους σημαντικότερους παράγοντες επιλογής ηλεκτρονικού καταστήματος.

Για να υπάρχει ασφάλεια στις συναλλαγές, απαιτείται η παρουσία ενός ασφαλούς web server. Ο ασφαλής web server χρησιμοποιείται για την απόκρυψη δεδομένων μεταξύ ενός server, που αντιστοιχεί στην εταιρεία που κάνει τη συναλλαγή, και ενός browser, που αντιστοιχεί στον πελάτη. Η απόκρυψη δεδομένων γίνεται μέσα από κρυπτογράφηση των δεδομένων πριν φύγουν από την εταιρεία και αποκρυπτογράφηση όταν φτάσουν στον πελάτη.

Για να κατανοήσουμε τι είναι ασφάλεια συναλλαγών θα δώσουμε ένα γνωστό παράδειγμα :

Υπάρχει ο αποστολέας **A** και ο παραλήπτης **B**.

Ο **A** θέλει να στείλει ένα πακέτο στον **B** μέσω τρίτου προσώπου (π.χ. μέσω ενός ταχυδρόμου) όμως θέλει να εξασφαλίσει ότι μέχρι να φτάσει το δέμα στον προορισμό του, δεν πρόκειται να παραβιαστεί.

Έχει την δυνατότητα να βάλει ένα λουκέτο στο πακέτο του όπου έτσι θα ξέρει ότι δεν θα μπορούν να υποκλέψουν τα στοιχεία του δέματος , το θέμα όμως είναι ότι ούτε ο παραλήπτης δεν θα μπορέσει να ανοίξει το δέμα για τον λόγο ότι δεν έχει το κλειδί. Το σίγουρο πάντως είναι ότι δεν μπορεί να στείλει και το κλειδί μαζί γιατί τότε δεν θα είχε ουσία.

Άρα αφού παραλάβει ο **Β** το πακέτο θα βάλει και αυτός ένα λουκέτο στο δέμα και θα το επιστρέψει πίσω στον **Α**.
Ο **Α** αφού παραλάβει το δέμα πίσω θα βγάλει το δικό του λουκέτο και θα το ξαναστείλει στον **Β**.
Τώρα το δέμα έχει μόνο το λουκέτο του **Β**, που σημαίνει ότι όταν λάβει ο **Β** το πακέτο του θα το ανοίξει με το δικό του κλειδί διότι το πακέτο είναι κλειδωμένο με το δικό του λουκέτο.

Κάπως έτσι συμβαίνει και με τις συναλλαγές μέσω ηλεκτρονικού δικτύου, μόνο που αντί για πακέτα στέλνουμε δεδομένα / μηνύματα και αντί για λουκέτα και κλειδιά έχουμε τα λεγόμενα "μυστικά κλειδιά κρυπτογράφησης" που θα αναφερθούμε παρακάτω.

Κάποια θέματα που συναρτώνται με την ασφάλεια είναι:

- Εξουσιοδότηση (Authorization): Η εξουσιοδότηση αφορά την εκχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη.
- Εξασφάλιση (Assurance): Ο όρος εξασφάλιση αναφέρεται στην αίσθηση εμπιστοσύνης ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνονται.

Σε μια ηλεκτρονική συναλλαγή, υπάρχουν τρεις παράγοντες που συμμετέχουν στην διαδικασία και κατά συνέπεια αντίστοιχα τρία σημεία που χρειαζόμαστε εξασφάλιση:

- **Ασφάλεια στο κανάλι επικοινωνίας**

Όταν αναφερόμαστε στο κανάλι επικοινωνίας συνήθως εννοούμε το Internet, δηλαδή ένα "ανοικτό" μη ελέγξιμο δίκτυο. Επειδή ακριβώς έχουμε να κάνουμε με ανοικτό δίκτυο τα δεδομένα που μεταφέρονται από υπολογιστή σε υπολογιστή, μέχρι να φτάσουν στον προορισμό τους, οποιοσδήποτε υπολογιστής που μεσολαβεί έχει τη δυνατότητα να δει αυτά τα δεδομένα. Η μοναδική λύση για να μην μπορεί κανένας να δει τα δεδομένα είναι η κρυπτογράφηση με ισχυρούς αλγορίθμους τουλάχιστον

128-bit ή 256-bit (SSL certificates), όσο μεγαλύτερη είναι η κλίμακα τόσο πιο δύσκολο είναι να παραβιαστούν τα κωδικοποιημένα δεδομένα. Το SSL είναι ο πλέον αξιόπιστος φορέας για την ασφάλεια συναλλαγών μέσω του internet, σε παγκόσμια κλίμακα. Με αυτή την τεχνολογία, κάθε στοιχείο που καταχωρείτε στο site μας κωδικοποιείται πριν βγει online και σε συνέχεια διερευνάται η αυθεντικότητα του μηνύματος και του server.

Έτσι, ο καθημερινός χρήστης πρέπει να μάθει ότι αν δεν βλέπει το αντίστοιχο "λουκετάκι" στον web browser και απλά δίνει ότι στοιχεία του ζητάνε on-line χωρίς δεύτερη σκέψη, είναι ουσιαστικά το ίδιο με το να βγει στο μπαλκόνι του σπιτιού του και να φωνάξει τα στοιχεία του. Μπορεί να ακούγεται αστείο, αλλά τα πράγματα είναι ακριβώς τόσο απλά. Αυτό είναι συνήθως αρκετό για μια on-line αγορά από κάποιον που θα τύχει να τον ακούει, μια και ο συνδυασμός του αριθμού μιας (ενεργής) πιστωτικής κάρτας και του αντίστοιχου (νόμιμου) κατόχου της είναι τα κύρια στοιχεία που ζητάνε τα περισσότερα on-line καταστήματα.

- **Ασφάλεια στον κόμβο-Η/Υ του πελάτη**

Σχετικά με τον κόμβο-Η/Υ του πελάτη, είναι επίσης πολύ σημαντικό ο καθημερινός χρήστης να μάθει ότι ο Η/Υ δεν είναι ένα κλειστό απαραβίαστο κουτί που "...δεν ξέρω τι έχει μέσα και πως δουλεύει..". Αν δεν χρησιμοποιούν όλοι συνειδητά και συστηματικά τα απαραίτητα εργαλεία (antivirus, anti-spyware, system updates, backups, ...), καλύτερα να μην τον χρησιμοποιούν για καμία σοβαρή δουλειά, γιατί κάποια στιγμή απλά θα πέσουν από τα σύννεφα όταν καταλάβουν πόσο εύκολο είναι να γίνει ανεπανόρθωτη ζημιά.

Επίσης, το ίδιο πρέπει να κατανοήσουν για την φυσική ασφάλεια, ότι π.χ. δεν κάνουμε ποτέ χρηματικές συναλλαγές σε Internet cafe, γιατί απλά δεν έχουμε τον απόλυτο έλεγχο των παραπάνω προϋποθέσεων στον συγκεκριμένο Η/Υ και δεν ανακοινώνουμε τους κωδικούς μας σε τρίτα πρόσωπα και ποτέ δεν επιλέγουμε κωδικούς που μπορεί να προβλεφθούν.

- **Ασφάλεια στον κόμβο-Η/Υ της εταιρίας**

Στον κόμβο-Η/Υ της εταιρίας υπάρχουν δύο σημαντικοί και διακριτοί παράγοντες που καθορίζουν το αντίστοιχο επίπεδο ασφάλειας και προστασίας των πελατών:

Η εταιρική εμπορική πολιτική που αναφέρεται κυρίως στον τρόπο διεκπεραίωσης των συναλλαγών και στον τρόπο διαχείρισης των στοιχείων των πελατών, ώστε να είναι καθ' όλα νόμιμες και έγκυρες. Επίσης συμπεριλαμβάνονται και οι κανόνες χρήσης των πιστωτικών καρτών που θέτουν οι τράπεζες και που σχεδόν ποτέ δεν είναι οι ίδιοι από τράπεζα σε τράπεζα.

Σήμερα, πολλές τράπεζες προσφέρουν πλέον δυνατότητα ηλεκτρονικής χρέωσης πιστωτικών καρτών μέσω Internet, παρόλο που δεν φτιάχτηκαν για αυτό το λόγο, απλά και μόνο γιατί το σύστημα αποδείχτηκε σχετικά ασφαλές. Πάντως οι μοναδικές κάρτες που είναι ακόμη και σήμερα 100% Internet-compatible είναι η VISA (classic) και η MasterCard.

Για λόγους ασφαλείας, τα τελευταία χρόνια έχει προστεθεί η δυνατότητα χρήσης των επιπλέον τετραψήφιων κωδικών στο πίσω μέρος της κάρτας σαν πρόσθετο μέτρο ασφάλειας, αφού αυτά δεν τυπώνονται από τα αυτόματα μηχανήματα αποδείξεων στα καταστήματα (δεν είναι ανάγλυφα). Κατά συνέπεια, δεν μπορεί κάποιος να "αναπαραγάγει" μια τέτοια κάρτα διαβάζοντας απλά μια απόδειξη (π.χ. απώλεια φακέλου με απόδειξη αγοράς στο ταχυδρομείο). Όμως, αυτό δεν σημαίνει ότι ο αριθμός αυτός δεν αποθηκεύεται το ίδιο εύκολα με τα υπόλοιπα στοιχεία της κάρτας, κάθε φορά που ζητείται σε ηλεκτρονικές συναλλαγές. Συνεπώς, το πρόβλημα πιθανής υποκλοπής παραμένει στον κόμβο-Η/Υ της εταιρίας.

Ο άλλος παράγοντας είναι το επίπεδο και η πολιτική ασφάλειας της συγκεκριμένη εταιρίας δηλαδή το “τεχνικό” επίπεδο ασφάλειας που εφαρμόζει η συγκεκριμένη εταιρία στο on-line κατάστημά της, το οποίο κατά τη γνώμη μου είναι το πιο σημαντικό, η εμπιστοσύνη στην συγκεκριμένη εταιρία και η εγγυήσεις ασφάλειας στον κόμβο της είναι αυτά που πρέπει να οδηγούν κάποιον στην τελική αποδοχή ή μη αποδοχή του "ρίσκου" της ηλεκτρονικής συναλλαγής με τη συγκεκριμένη εταιρία. Εφόσον δηλαδή τηρούνται όλα τα παραπάνω, τελικά ο χρήστης-πελάτης πρέπει να αποφασίσει ο ίδιος συνειδητά αν εμπιστεύεται το "άλλο άκρο" της συναλλαγής, που πιθανότατα βρίσκεται χιλιάδες χιλιόμετρα και πολλούς νόμους μακριά, όχι μόνο για την αποστολή-πίστωση χρημάτων αλλά (κυρίως) για την γνωστοποίηση και ασφαλής

αποθήκευση των αντίστοιχων προσωπικών δεδομένων. Μάλιστα, θα πρέπει να γίνεται πάντα η υπόθεση ότι αποθηκεύονται ΟΛΑ τα στοιχεία της συναλλαγής, κάτι που πρακτικά σημαίνει ότι αν δεν εμπιστεύεται κάποιος π.χ. ότι το Amazon δεν μπορεί να προφυλάξει ΟΛΑ τα στοιχεία που ζητούνται (όνομα, διεύθυνση, αριθμοί κάρτας, ...), τότε δεν πρέπει να προχωρήσει στη συναλλαγή (ανεξάρτητα με το τι λέει το Amazon ότι αποθηκεύει στο αρχείο των πελατών του).

Ασφάλεια συναλλαγών σημαίνει τέσσερα πράγματα:

- Εμπιστευτικότητα (Confidentiality): Η εμπιστευτικότητα είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy) καθώς και της προστασίας των ιδιωτικών και απορρήτων πληροφοριών που αφορούν π.χ. τα στοιχεία της πιστωτικής κάρτας και το περιεχόμενο μίας συναλλαγής παραμένει αναλλοίωτο. Είναι η εξασφάλιση πως κανείς πλην του εμπόρου και του πελάτη δεν μπορεί να δει το μήνυμα.
- Ακεραιότητα (Integrity): Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται και παρέχεται μέσω ψηφιακής υπογραφής.
- Έλεγχος αυθεντικότητας (Authentication): Η διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα, αλλά και η βεβαιότητα ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο.
- Μη αποποίηση ευθύνης (Non repudiation): Σύμφωνα με τον όρο αυτό, κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή (επειδή προφανώς άλλαξαν γνώμη).

Από όλα τα παραπάνω βλέπουμε ότι η ασφάλεια των δικτύων και των συναλλαγών εξαρτάται από πάρα πολλούς παράγοντες και το πραγματικό πρόβλημα είναι το εξαιρετικά χαμηλό επίπεδο ενημέρωσης και εκπαίδευσης σε αυτά τα θέματα, τα οποία καλώς ή κακώς αποτελούν πλέον μέρος της καθημερινότητας.

Έτσι αν εξαιρέσουμε την προσωπική ευθύνη του καθενός, που πρέπει να προσέχει αυτό που διαβάζει και ποια σελίδα του web ανοίγει, να αλλάζει συχνά τους κωδικούς ασφαλείας και να ενημερώνεται για το λογισμικό ασφαλείας, η ασφάλεια των παραπάνω επιτυγχάνεται με εργαλεία λογισμικού όπως είναι οι ειδικοί αλγόριθμοι κρυπτογράφησης δεδομένων που παρέχουν ακεραιότητα και εμπιστευτικότητα, οι ηλεκτρονικές υπογραφές που παρέχουν αυθεντικότητα, τα πιστοποιητικά που παρέχουν αυθεντικότητα και μη άρνηση και μια σειρά από πρωτόκολλα ασφάλειας των συναλλαγών, όπως αναλύονται παρακάτω.

Επειδή όταν υπήρχε μία συναλλαγή μηνυμάτων μεταξύ δύο χρηστών, υπήρχε το πρόβλημα ότι εκτός από τον αποστολέα και τον παραλήπτη το μήνυμα θα μπορούσε να το δει και ο :

- Ο εργαζόμενος στον ISP του αποστολέα.
- Ο εργαζόμενος στον ISP του παραλήπτη.
- Ο αρμόδιος ο οποίος λειτουργεί τους routers από τους οποίους τα πακέτα ου μηνύματος που περνάνε είναι πάνω από δέκα.

- Από τους εργαζόμενους της εκάστοτε τηλεφωνικής εταιρίας οι οποίοι έχουν φυσική πρόσβαση στον εξοπλισμό της.
- Όπως και όταν ο κάτοχος έχει ασύρματη συσκευή, μπορεί να δεχθεί ηλεκτρονική επίθεση από άτομα τα οποία έχουν συγκεκριμένες συσκευές για την υποκλοπή τους.

Γι' αυτούς τους λόγους λοιπόν εφαρμόστηκε η λεγόμενη «κρυπτογραφία».

V. ΚΡΥΠΤΟΓΡΑΦΙΑ

Α) Εφαρμογές της κρυπτογραφίας

- Στην ασφάλεια συναλλαγών σε τράπεζες δίκτυα και ATM, τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange -EDI),ηλεκτρονικά τιμολόγια που συντάσσονται σε μορφή άλλη από EDI.
- Υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου (S/MIME)
- Στα συστήματα υπογραφής αυθεντικότητας διακινούμενου λογισμικού (π.χ. Microsoft Authenticode),
- Κλειστές υποδομές PKI για εφαρμογές ασφαλείας μεγάλων οργανισμών (π.χ. ΝΑΤΟ).
- Στις ηλεκτρονικές δημόσιες προμήθειες
- Στην κινητή (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM) και σταθερή τηλεφωνία (cryptophones)
- Στην εξασφάλιση που παρέχουν στις Εταιρικές πληροφορίες.
- Στα στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
- Στα διπλωματικά δίκτυα (Τηλεγραφήματα)
- Στις ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες,ηλεκτρονικές πληρωμές ,EuroPay, MasterCard & VISA μέσω του κοινού πρωτοκόλλου τους EMV)
- Στην ηλεκτρονική ψηφοφορία, δημοπρασία
- Στο ηλεκτρονικό γραμματοκιβώτιο

- Στα συστήματα συναγερμών, συστήματα βιομετρικής αναγνώρισης
- Στα ηλεκτρονικά διαβατήρια και ηλεκτρονικές ταυτότητες (γενικής ή ειδικής χρήσης – π.χ. ναυτικές διεθνείς ταυτότητες) που συνήθως φέρουν ενσωματωμένα και κάποια βιομετρικά στοιχεία (φωτογραφία, δακτυλικά αποτυπώματα κ.τ.λ.) του κατόχου τους
- Στις έξυπνες κάρτες (smart cards)
- Στα ιδιωτικά δίκτυα (VPN)
- Στο διαδίκτυο (Word Wide Web) Πιστοποίηση της ταυτότητας εξυπηρετητών Διαδικτύου (web servers), κ.ά.
- Στις δορυφορικές εφαρμογές (δορυφορική τηλεόραση π.χ. nova)
- Στα ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
- Στα συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
- Στην τηλεδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP) .

Η κρυπτογραφία είναι η επιστήμη που ασχολείται με τα μέσα και τις μεθόδους μετάδοσης και λήψης μυστικών μηνυμάτων. Επίσης η κρυπτογραφία υποδιαιρείται σε δύο κλάδους :

1) Στην ασφάλεια των επικοινωνιών , όπου :

- Καλύπτει όλους τους τρόπους προστασίας των απόρρητων σημάτων,
- Τις μεθόδους μετατροπής των μηνυμάτων σε κώδικα ή αριθμητική μορφή,την ασφάλεια των κωδικών, πινάκων, εγχειριδίων και μηχανισμών μέσω των οποίων γίνεται η κρυπτογράφηση,
- Την αξιοπιστία του χρησιμοποιημένου προσωπικού,
- Όπως και την επιτήρηση των επικοινωνιών.

2) Στην κατασκοπεία των επικοινωνιών , όπου :

Αποβλέπει στη διείσδυση μέσα στο δίκτυο και στην εξουδετέρωση του απορρήτου των επικοινωνιών του εχθρού ή ανταγωνιστών.

Υπάρχουν δύο προϋποθέσεις για την προετοιμασία ενός μυστικού μηνύματος:

Ένα κείμενο που πρέπει να κρυπτογραφηθεί, το ονομαζόμενο σαφές κείμενο (ή απλώς κείμενο), και ένα σύστημα με το οποίο θα γίνει η μετατροπή του σαφούς

κειμένου με παραλλαγμένο κείμενο (ή κρυπτογράφημα). Τα κρυπτογραφικά συστήματα μπορούν να διακριθούν σε κώδικα και αριθμητικά. Η σημαντικότερη διαφορά ανάμεσα στα δύο συστήματα έγκειται (αν και αυτό δεν είναι απόλυτο) στην έκταση του σαφούς κειμένου που πρόκειται να κρυπτογραφηθεί. Γενικά τα αριθμητικά συστήματα θεωρούν ως μονάδες μετατροπής σε παραλλαγμένο κείμενο ομάδες τριών ή περισσοτέρων γραμμάτων. Τα κωδικά συστήματα θεωρούν ως μονάδες μετατροπής ολόκληρες λέξεις, φράσεις , προτάσεις.

Τα συστήματα κρυπτογράφησης είναι τα εξής:

1) Το σύστημα αντικατάστασης, σύμφωνα με το οποίο τα γράμματα του κειμένου αντικαθιστούνται με άλλα γράμματα του αλφαβήτου (ελληνικού ή ξένου) ή με σύμβολα ή με ψηφία αριθμών.
2) Το σύστημα μετάθεσης, όπου τα γράμματα του αλφάβητου αλλάζουν θέση.
3) Το σύστημα του κώδικα ή του λεξικού. Αυτοί που συναλλάσσονται έχουν τον ίδιο κώδικα ή το ίδιο λεξικό. Σε αυτά οι λέξεις παρασταίνονται με αριθμούς.

Η ιστορική αναδρομή της κρυπτογραφίας

Η **σκυτάλη** είναι η αρχαιότερη συσκευή κρυπτογράφησης η οποία χρησιμοποιήθηκε από τους Λακεδαιμονίους. Αποτελούταν από μία κωνική ράβδο όπου γύρω της τυλιγόταν σπειροειδώς ένα συγκεκριμένο υλικό όπου ήταν κατάλληλο για γραφή. Το μήνυμα γραφόταν κατά το μήκος της ράβδου και όταν το υλικό γραφής ξετυλιγόταν, εμφάνιζε την εικόνα μιας ταινίας με γράμματα τα οποία δεν συνδέονταν μεταξύ τους για να σχηματίσουν λέξεις. Όταν η ταινία ξανατυλιγόταν σε μια πανομοιότυπη σκυτάλη, το μήνυμα μπορούσε πάλι να διαβαστεί. Έτσι η ίδια συσκευή κρυπτογράφησης χρησίμευε και για αποκρυπτογράφηση.

Οι Αιγύπτιοι, οι Ρωμαίοι και οι Έλληνες χρησιμοποιούσαν την κρυπτογραφία.

- Τον 13^{ο} αιώνα έκανε την εμφάνιση της η σύγχρονη συστηματική κρυπτογραφία και άρχισε να αναπτύσσεται στην Ιταλία.
- Τον 15^{ο} αιώνα η ιταλική κρυπτογραφία αναπτύχθηκε τόσο πολύ που είχαν καθοριστεί σαφείς κώδικες αλφαβητικών και αριθμητικών συστημάτων κρυπτογράφησης. Οι κώδικες αυτοί χρησίμευσαν ως πρότυπα για πολλά συστήματα απόρρητων επικοινωνιών που παρέμειναν σε χρήση για αρκετούς

αιώνες. Επίσης κατά την διάρκεια αυτού του αιώνα γράφθηκε η πρώτη επιστημονική μελέτη για την *κρυπτογραφία* ή το σπάσιμο των κωδικών.

Τον 19^{ο} αιώνα η κρυπτογραφία η κρυπτογράφηση αναπτύχθηκε με ταχύτατους ρυθμούς. Αυτό οφειλόταν στην εφεύρεση του τηλεγράφου και άλλων νέων μέσων επικοινωνίας, καθώς και στην πρόοδο κατασκευής και ανάλυσης αριθμητικών και αλφαβητικών κωδικών κρυπτογράφησης. Πολλές από τις σύγχρονες μεθόδους κρυπτογραφίας θεωρούνται άκρως απόρρητες. Αυτό έχει ως αποτέλεσμα να μην είναι δυνατό να δημοσιευθούν. Οι μυστικές υπηρεσίες κυβερνητικών επικοινωνιών προσπαθούσαν να αποσιωπήσουν το φαινόμενο της κρυπτογραφίας και πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70.Όπου εκείνη την εποχή ήρθε στο φώς το σχέδιο προτύπου κρυπτογράφησης DES (Data Encryption Standard)στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975.

Β) Αποκρυπτογράφηση

Αποκρυπτογράφηση είναι ουσιαστικά ο αντίστροφος αλγόριθμος της κρυπτογράφησης. Ανακτήει το περιεχόμενο του αρχικού μηνύματος και έτσι καταφέρνει να αποκωδικοποιήσει το μήνυμα. Έτσι με λίγα λόγια μπορεί να σπάσει τον κώδικα.

Γ) Κρυπτανάλυση

Αναφέρεται στην τέχνη της παραβίασης, δηλ. της αποκρυπτογράφησης, των κρυπτοσυστημάτων. Μπορεί να αναφέρεται επίσης και στην εύρεση λαθών ή και ελλείψεων κατά την εφαρμογή ενός αλγορίθμου κρυπτογράφησης.
Μπορεί να αναλύσει και να αποκωδικοποιήσει τις κωδικοποιημένες πληροφορίες χωρίς την χρήση του αντίστροφου αλγορίθμου. Με λίγα λόγια χωρίς την εξουσιοδότηση του αποστολέα.

Άρα καταλήγουμε ότι όσο πιο πολύπλοκος είναι ο αλγόριθμος, τόσο πιο δύσκολο είναι να τον αποκωδικοποιήσει κάποιος.

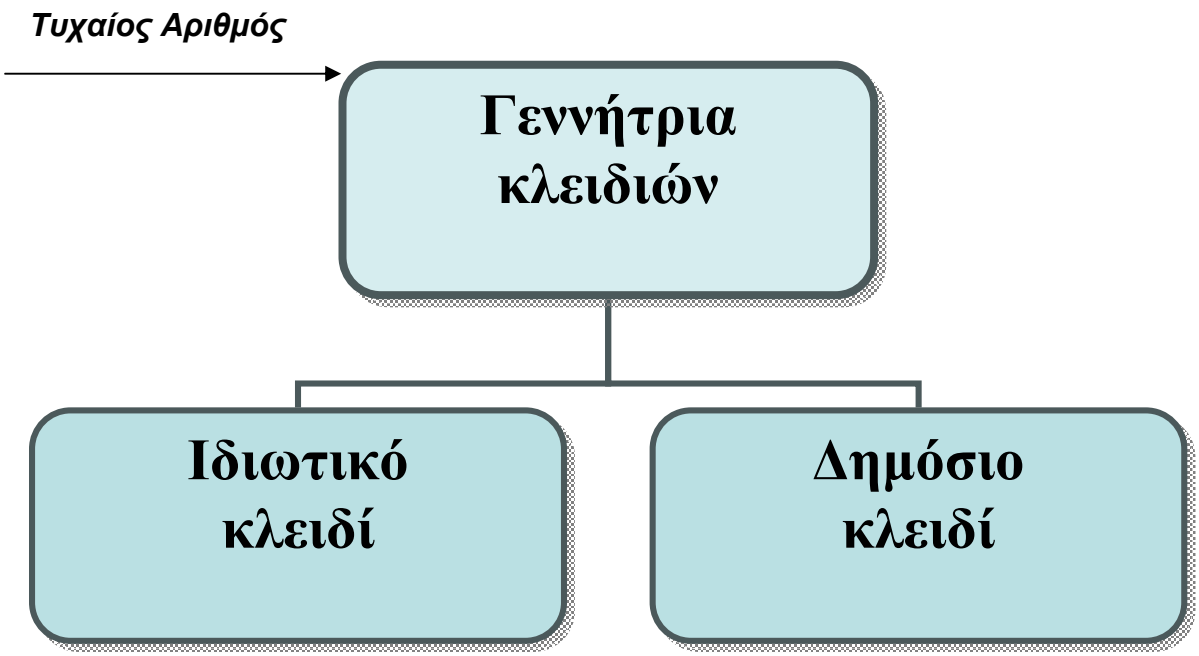
Δ) Συμμετρική και Ασύμμετρη κρυπτογραφία

Γεννήτρια κλειδιών

Για να πραγματοποιηθεί μία κρυπτογράφηση ούτος ώστε να μπορέσει να γίνει η συναλλαγή σε ηλεκτρονική μορφή, θα έπρεπε να υπάρξουν κάποια στοιχεία που θα το εξασφάλιζαν αυτό. Έ τσι λοιπόν όπως θα αναλύσουμε και παρακάτω, δημιουργήθηκαν τα λεγόμενα «μυστικά κλειδιά» (δηλ. Ιδιωτικό και δημόσιο κλειδί).

Για να δημιουργηθούν αυτά τα δύο κλειδιά έπρεπε να υπάρξουν κάποιες συγκεκριμένες συναρτήσεις όπου για είσοδο λαμβάνουν ένα μεγάλο τυχαίο αριθμό και για έξοδο τους πραγματοποιούν την λειτουργία του ιδιωτικού και δημοσίου κλειδιού.

Όσο πιο μεγάλος είναι ο τυχαίος αριθμός τόσο πιο ασφαλή είναι και τα κλειδιά που παράγει η γεννήτρια.



i. Συμμετρική κρυπτογράφηση (Symmetric key encryption)

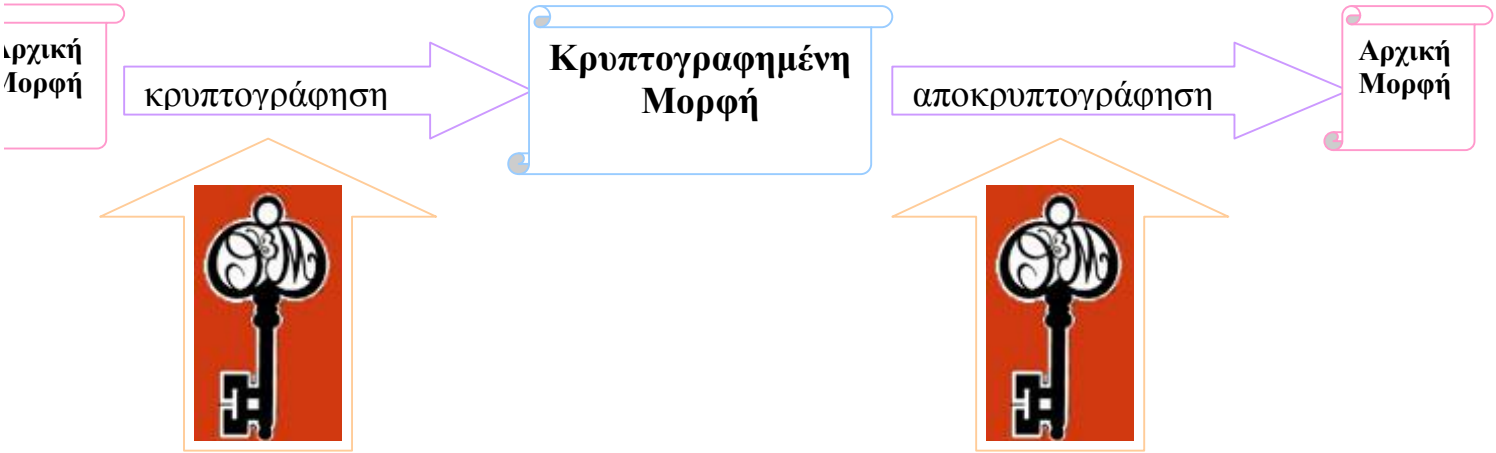
«Το ιδιωτικό κλειδί»

Συμμετρική κρυπτογράφηση η αλλιώς κρυπτογράφηση του ιδιωτικού κλειδιού είναι ένα κοινό κλειδί το οποίο χρησιμοποιείται και από τους δύο χρήστες που συναλλάσσονται μεταξύ τους. Το σύστημα Kerberos και το Data Encryption Standard είναι οι πιο διαδεδομένες τεχνολογίες ιδιωτικού κλειδιού. Το κλειδί αυτό χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των μηνυμάτων. Όπως καταλαβαίνουμε λοιπόν η κρυπτογράφηση και αποκρυπτογράφηση γίνεται με το ίδιο κλειδί, αλλά με αντίστροφες διεργασίες. Αυτό κάνει την συμμετρική κρυπτογραφία έχει γρήγορη διαδικασία και δεν χρειάζεται μεγάλη υπολογιστική ισχύ. Επίσης όταν ο χρήστης θέλει να έχει συναλλαγές και με άλλα άτομα θα πρέπει να μοιράζεται και από ένα ιδιωτικό κλειδί με τον κάθε αποστολέα/ παραλήπτη που συναλλάσσεται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική. Γιατί κατά τη διαδρομή του από τον αποστολέα στον παραλήπτη το μήνυμα είναι ασφαλές, υπάρχει όμως το πρόβλημα στο πώς θα συμφωνήσουν ο αποστολέας και ο παραλήπτης πάνω σε ένα συγκεκριμένο κλειδί και μάλιστα με ασφαλή τρόπο. Επίσης από την στιγμή που δυο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δυο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε το άλλο άτομο. Το πρόβλημα λύθηκε με την επινόηση του σχήματος που ονομάζεται **κρυπτογραφία δημόσιου κλειδιού** (public-key cryptography). Οι αλγόριθμοι συμμετρικής κρυπτογραφίας, είναι οι IDEA, DES, DES3, Blowfish

Απεικόνιση κρυπτογράφησης «Ιδιωτικού κλειδιού»

Αγοραστής

Πωλητής



Ιδιωτικό κλειδί **Ιδιωτικό κλειδί**

ii. Ασύμμετρη Κρυπτογράφηση (Asymmetric Public key Cryptography)

«Το δημόσιο κλειδί»

Ασύμμετρη κρυπτογράφηση ή αλλιώς κρυπτογράφηση του δημοσίου κλειδιού, ουσιαστικά διαθέτει δύο κλειδιά που παράγονται ταυτόχρονα ως μέρος μίας κοινής διαδικασίας παραγωγής. Το ένα κλειδί μπορεί να χρησιμοποιηθεί μόνο για την κρυπτογράφηση του μηνύματος, και το άλλο μπορεί να χρησιμοποιηθεί μόνο για την αποκρυπτογράφηση του μηνύματος. Η διαδικασία βεβαιώνει ότι η κρυπτογραφία και αποκρυπτογράφηση, μπορούν να λειτουργήσουν μόνο με ένα αντίστοιχο ζεύγος κλειδιών.

Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση του μηνύματος μπορεί να διανέμεται ελεύθερα ή να τοποθετηθεί σε μια δημόσια και εύκολα προσβάσιμη υπηρεσία καταλόγου του ιστού, και ο παραλήπτης του μηνύματος κρατάει το κλειδί το οποίο χρησιμοποιείται για την αποκρυπτογράφηση του μηνύματος.

Άρα το κλειδί όπου είναι προσβάσιμο στον οποιοδήποτε χρήστη είναι το λεγόμενο ***δημόσιο κλειδί,*** διότι το δημόσιο κλειδί που χρησιμοποιείται για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα , κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα***,*** ενώ το ***ιδιωτικό κλειδί***, όπως αναφέραμε και παραπάνω, μόνο ο ίδιος ο χρήστης το γνωρίζει, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν, για το λόγω αυτό λοιπόν δεν μπορεί να είναι ένα γνωστό κλειδί, έτσι είναι το λεγόμενο «μυστικό κλειδί».

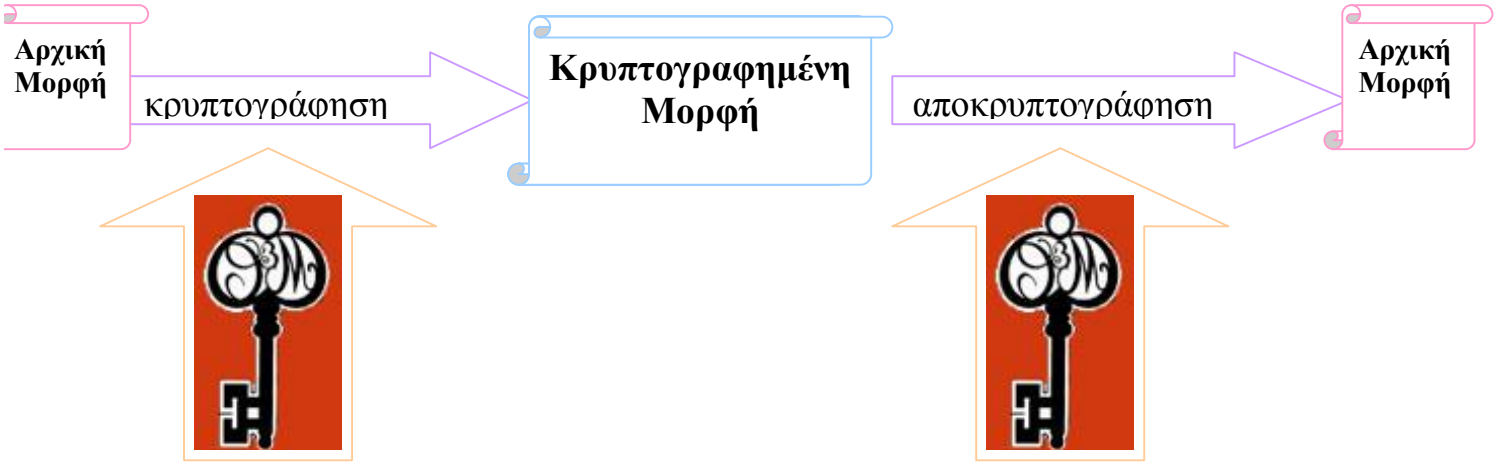
Η ασύμμετρη κρυπτογραφία λοιπόν σε συνδυασμό αυτών των δύο κλειδιών πέτυχε :

- την υπογραφή των δεδομένων με το ιδιωτικό κλειδί, όπου το κάθε ένα ξεχωριστά διαθέτει και ένα αντίστοιχο δημόσιο κλειδί. Επίσης το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.
- Ο παραλήπτης να αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.
- Το μήνυμα που κρυπτογραφήθηκε με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί.
- Το μήνυμα του αποστολέα για να σταλεί στον παραλήπτη θα πρέπει το δημόσιο κλειδί του παραλήπτη να είναι γνωστό στον αποστολέα για να κρυπτογραφήσει το μήνυμα με αυτό.

Απεικόνιση κρυπτογράφησης «Δημόσιου κλειδιού»

Αγοραστής

Πωλητής



Δημόσιο κλειδί

Ιδιωτικό κλειδί

Ε) *Βασικοί αλγόριθμοι Κρυπτογράφησης*

Μετά τον αλγόριθμο DES δημιουργήθηκαν και άλλοι αλγόριθμοι οι οποίοι βοήθησαν στην μετέπειτα εξέλιξη της κρυπτογραφίας. Συνοπτικά αναφέρουμε :

- **Ο αλγόριθμος DES** (Data Encryption Standard) είναι κρυπτογραφικός αλγόριθμος που λειτουργεί με 64 bit μπλοκ. Η βασική ιδέα ήταν η ανάπτυξη ενός αλγόριθμου κρυπτογράφησης που θα μπορούσε να χρησιμοποιηθεί (και να βελτιωθεί) από διάφορες εταιρείες ή οργανισμούς. Το DES ανήκει στην οικογένεια των συμμετρικών αλγόριθμων και κάνει χρήση κλειδιών με μήκος 56bit. Ο «κλασικός» αλγόριθμος DES είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα. Είναι ουσιαστικά αλγόριθμος μιας φοράς, αφού δεν υπάρχει τρόπος

αντιστροφής της διαδικασίας και εξαγωγής του συνθηματικού από την κωδικοποιημένη μορφή, χωρίς να δοκιμαστούν όλοι οι δυνατοί συνδυασμοί. Η πιστοποίηση του DES ανακλήθηκε το 1998 και αντικαταστάθηκε από έναν άλλο αλγόριθμο γνωστό ως 3DEA.

- **Triple – DES** : Κωδικοποιεί το μήνυμα τρείς φορές, με τρία διαφορετικά κλειδιά. Είναι ουσιαστικά η εξέλιξη του DES, διότι πλέον αυτός ο αλγόριθμος μπορεί να παραβιαστεί, κάτι που δεν είναι εύκολο για το Triple – DES.
- **RC2/ RC4/ RC5** : Είναι κατάλληλα για μεγάλου μεγέθους κρυπτογράφηση, διότι διαθέτουν μεγάλη ποικιλία ως προς τον όγκο του κλειδιού κρυπτογράφησης. Ο RC2 διαθέτει μία ομάδα κρυπτογράφησης και μπορεί να αντικαταστήσει το DES. Ο RC4 είναι το λεγόμενο *ρεύμα* ψηφίων κρυπτογράφησης και είναι 10 φορές πιο γρήγορος από τον DES. Όσο πιο μεγάλο είναι το μήκος του κλειδιού τόσο μεγαλύτερη ασφάλεια παρέχουν αυτοί οι αλγόριθμοι καλύτερη από τον DES. Το 1994 δημιουργήθηκε και ο αλγόριθμος RC5, όπου ήταν η εξέλιξη όλης της σειράς. Επίσης σωστό θα ήταν να αναφέρουμε ότι αυτοί οι τρείς αλγόριθμοι κατασκευάστηκαν από τον Ron Rivest.
- **IDEA** : Πρόκειται για μια μέθοδο κρυπτογράφησης που λειτουργεί παρόμοια με την DES ,αλλά με μεγαλύτερο κλειδί μήκους 128 bits για να κάνει μια σειρά από μη γραμμικούς μαθηματικούς μετασχηματισμούς σ' ένα μπλοκ δεδομένων (data block) . Αναπτύχθηκε στην Ελβετία και δημοσιοποιήθηκε το 1990, χρησιμοποιείται στο PGP 2.x ως ο συμμετρικός αλγόριθμος κρυπτογράφησης.
- **RSA :** Είναι ο αλγόριθμος ενός δημόσιου κλειδιού που μπορεί να χρησιμοποιηθεί και για την κρυπτογράφηση μηνυμάτων και για τη δημιουργία ψηφιακών υπογραφών, δηλ. για την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος. Ο αλγόριθμος RSA ανήκει στην οικογένεια των ασύμμετρων. Τα αρχικά του RSA αναφέρονται στους δημιουργούς του αλγορίθμου (Rivest-Shamir-Adleman). Το πλήθος του κειμένου του, πρέπει να είναι μικρότερο από το μήκος του κλειδιού. Έχοντας ένα κλειδί 128 bits, διαθέτει μία πολύ ισχυρή κρυπτογράφηση.
- **Diffie και Hellman** : Είναι το παλαιότερο σύστημα «δημοσίου κλειδιού» όπου επιτρέπει την συναλλαγή μεταξύ δύο ατόμων Α και Β που επικοινωνούν μέσα από ένα δημόσιο κανάλι. Δεν υποστηρίζει την κρυπτογράφηση και την

ψηφιακή υπογραφή αλλά επιτρέπει να υπάρχει ένα κοινό κλειδί για τον αποστολέα και παραλήπτη.

- **Blowfish** : Είναι ένας αλγόριθμος που χρησιμοποιεί κλειδί μήκους 448 bit. Έχει ευρεία χρήση.
- **DSA (Digital Signature Algorithm) :** Έχει να κάνει με την ψηφιακή υπογραφή και είναι η εξέλιξη των παραπάνω αλγορίθμων. Ο πορεία του είναι σταδιακή και ακόμα δεν έχει την ολοκληρωτική εμπιστοσύνη του κοινού, αλλά αναμένεται σε μερικά χρόνια να έχει την ίδια αξία με την υπογραφή δια χειρός. Χρησιμοποιεί τα ίδια κλειδιά με τους *Diffie και Hellman* και είναι πιο γρήγορος από το *RSA*
- **DESX (X-OR):** Είναι ένας αλγόριθμος στο οποίο η είσοδος της κρυπτογράφησης και η έξοδος της αποκρυπτογράφησης περνάει από μια **X-OR** (e**x**clusive **or** – **x-**disjunction) πράξη με ένα επιπλέον κλειδί 64 bit και έτσι αυξάνεται η αντοχή του αλγορίθμου σε επιθέσεις.
- **Οι Stream Ciphers:** είναι εξαιρετικά ταχείς αλγόριθμοι και σε αντίθεση με τους **block ciphers** λειτουργούν με μικρότερες μονάδες κειμένου, συνήθως bits. Επιπλέον αντιθέτως με τους block ciphers όπου η κρυπτογράφηση ενός συγκεκριμένου κειμένου με το ίδιο κλειδί, θα είχε πάντα το ίδιο αποτέλεσμα, εδώ ο μετασχηματισμός των μικρών αυτών μονάδων θα ποικίλει αναλόγως του πότε θα αντιμετωπίζονται. Συνεπώς ως προς τις ιδιότητες τους είναι **One-time Pad** αλγόριθμοι. Για την κρυπτογράφηση παράγουν μια ακολουθία από bits που ονομάζεται key-stream η οποία συνδυάζεται με το κείμενο μέσω μιας **X-OR** πράξης. Ο ευρύτερα χρησιμοποιούμενος μηχανισμός για την παραγωγή του key-stream είναι ο **LFSR (Linear Feedback Shift Register)** του οποίου άλλοι συνδυασμοί μπορεί να είναι ο **Shift Register Cascade** και ο **Shrinking** ή **Self Shrinking Generator.**
- **A5: Stream Cipher** για την προστασία της επικοινωνίας μέσω **GSM** κινητών τηλεφώνων. Έχει διάφορες εκδόσεις οι οποίες όμως όλες ‘έσπασαν’ και χρησιμοποιεί τριπλό μηχανισμό **LFSR.**
- **SEAL (Software–optimized Encryption Algorithm):** Τα δεδομένα κρυπτογραφούνται ένα bit την φορά και χρησιμοποιεί κλείδα 160 *bit.*

ΙΣΤΟΡΙΚΟ ΣΗΜΕΙΩΜΑ

Πρώτοι που διατύπωσαν την βασική αρχή της ασύμμετρης κρυπτογραφίας ήταν οι Diffie και Hellman το 1976. Έπειτα το 1977 βασισμένοι στις προηγούμενες θεωρίες οι Rivest, Shamir και Adleman δημιούργησαν την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού, το λεγόμενο κρυπτοσύστημα RSA.

VI. ΑΣΦΑΛΕΙΑ ΜΟΝΤΕΛΩΝ ΣΥΝΑΛΛΑΓΩΝ

Α)Πιστοποιητικά Ασφαλείας της Συναλλαγής

Ένα πιστοποιητικό συναλλαγής (transaction certificate) αποτελεί ασφάλεια και επιβεβαίωση για την πραγματοποίηση μιας συναλλαγής και με αυτό μπορεί να αποφευχθεί η αποποίηση ευθύνης. Δηλαδή συμβάλλει στη μη άρνηση, όπως είπαμε αρχικά στο κεφάλαιο, γιατί καταγράφουν τη συναλλαγή μεταξύ του πελάτη και του εμπόρου.

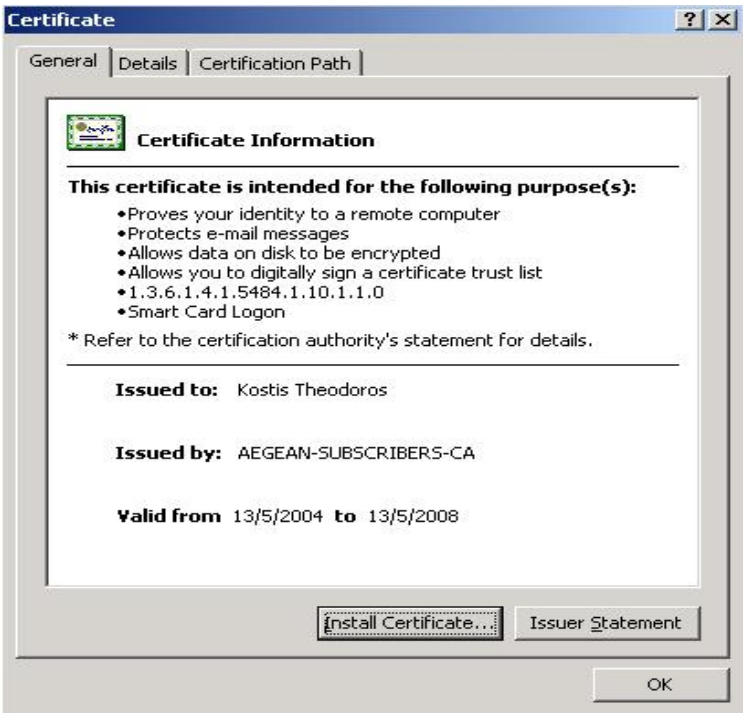
Στην κατηγορία των πιστοποιητικών συναλλαγής εντάσσονται τα:

i. Ψηφιακά πιστοποιητικά (Digital Certificates)
ii. Χρονική σφραγίδα (Time Stamp)
iii. Ψηφιακός φάκελος (Digital Envelope)
iv. Ψηφιακή ή Ηλεκτρονική υπογραφή (Digital Signature)
v. Υδατογραφήματα (Watermarks)

i. Ψηφιακά πιστοποιητικά (Digital Certificates)

Τα ψηφιακά πιστοποιητικά είναι οι αντίστοιχες αστυνομικές ταυτότητες στις ηλεκτρονικές συναλλαγές. Τα ψηφιακά πιστοποιητικά εκδίδονται από ένα τρίτο γνωστό ως αρχή πιστοποίησης έναντι χρεώσεως, που τυγχάνει δημόσιας εμπιστοσύνης (Έμπιστη Τρίτη Οντότητα-ΕΤΟ) (Trusted third party certificate Authority-CA). Εταιρείες όπως η Verisign και η Thawte.

Τα πιστοποιητικά τοποθετούν τις πληροφορίες στον σκληρό δίσκο του χρήστη και χρησιμοποιούν τεχνολογία απόκρυψης για να δημιουργήσουν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη. Τα ψηφιακά πιστοποιητικά είναι αρκετά ασφαλή επειδή χρησιμοποιούν πανίσχυρη τεχνολογία απόκρυψης. Στην πραγματικότητα είναι πιο ασφαλή και από τις υπογραφές. Τα περισσότερα από τα τυποποιημένα πρωτόκολλα, όπως το SSL και το S/MIME, που θα αναφέρουμε παρακάτω, στηρίζονται στα ψηφιακά πιστοποιητικά.



Περιλαμβάνουν στοιχεία της:

- Το όνομα του κατόχου,
- Έναν σειριακό αριθμό,
- Τα δημόσια κλειδιά του κατόχου (ένα για μυστική ανταλλαγή κλειδιού ως αποδοχέας και ένα για ψηφιακά υπογραφή ως αποστολέας),
- Τον αλγόριθμο που χρησιμοποιεί αυτά τα κλειδιά,
- Τον τύπο του πιστοποιητικού,
- Το όνομα της Αρχής Πιστοποίησης,
- Την ημερομηνία λήξης της ισχύος του πιστοποιητικού και
- Την ψηφιακή υπογραφή της Αρχής Πιστοποίησης.

Όπως στα περισσότερα πράγματα στο internet έτσι και εδώ υπάρχει ένα πρότυπο που επικρατεί και είναι γνωστό ως X.509.

Τα ψηφιακά πιστοποιητικά βασίζονται στην αρχή της ασύμμετρης κρυπτογραφίας όπου κάθε χρήστης διαθέτει ένα ιδιωτικό και ένα δημόσιο κλειδί. Το ιδιωτικό κλειδί είναι μυστικό και πρέπει πάντα να προστατεύεται από ένα προσωπικό κωδικό πρόσβασης (PIN) εξασφαλίζοντας την απόδειξη της ταυτότητας του αποστολέα. Το δημόσιο κλειδί είναι διαθέσιμο σε οποιονδήποτε άλλο χρήστη στην αποκρυπτογραφημένη (απλή) μορφή του. Δεν μπορεί να παραχθεί το ιδιωτικό κλειδί από το κοινώς διαδεδομένο αντίστοιχο δημόσιο.

Τα πιστοποιητικά έχουν δύο βασικές λειτουργίες. Η πρώτη πιστοποιεί ότι οι άνθρωποι, ο ιστοχώρος και οι πόροι δικτύων είναι αξιόπιστες πηγές. Ενώ η δεύτερη λειτουργία είναι να παρασχεθεί η προστασία για τα στοιχεία που ανταλλάσσονται.

Υπάρχουν δύο κύριοι τύποι ψηφιακών πιστοποιητικών:

- Τα προσωπικά πιστοποιητικά

  Τα οποία είναι ένα είδος εγγύησης ότι ο χρήστης που θέλει να κάνει τη συναλλαγή είναι αυτός που ισχυρίζεται. Σ' αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη, κωδικός πρόσβασης ακόμα και δακτυλικά αποτυπώματα. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται είτε όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό για να γίνει η συναλλαγή είτε όταν ο χρήστης λαμβάνει κρυπτογραφημένα μηνύματα από τους άλλους χρήστες.
- Τα πιστοποιητικά τοποθεσιών Web

  Τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη τοποθεσία Web είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι καμία άλλη τοποθεσία Web δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά τοποθεσιών χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με την τοποθεσία Web ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν

οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει περάσει η ημερομηνία λήξης, εμφανίζεται προειδοποίηση.

Με λίγα λόγια για να καταλάβουμε ότι ένας δικτυακός τόπος (web site) έχει ψηφιακό πιστοποιητικό κάθε φορά που συνδέομαι με έναν τέτοιο ο πλοηγός (browser) χρησιμοποιεί διαφορετικό πρωτόκολλο επικοινωνίας και εμφανίζεται ως https αντί για http στη διεύθυνση του site.

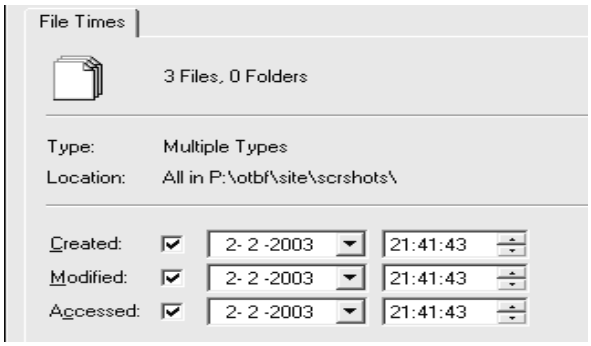
ii. Χρονική σφραγίδα (Time Stamp)

Η χρονική σφραγίδα είναι μια μεταβλητή, μια ψηφιακή πιστοποίηση μη επιδεχόμενη πλαστογράφησης και η οποία πιστοποιεί ότι κάποιο έγγραφο ή συναλλαγή υπήρξε σε συγκεκριμένη χρονική στιγμή.

Μέσω μηχανισμών όπως το Network time protocol ένας υπολογιστής διατηρεί ακριβή τρέχουσα ώρα, σε κλάσματα του δευτερολέπτου, έτσι η χρονική σφραγίδα προσδιορίζει την ακριβή χρονική στιγμή της αρχής της εκτέλεσης μίας συναλλαγής. Ο μηχανισμός χρονικών σφραγίδων δεν χρησιμοποιεί κλειδαριές για την προστασία δεδομένων άρα δεν μπορεί να δημιουργηθεί αδιέξοδο.

Η ακρίβεια καθιστά δυνατό για τους δικτυωμένους υπολογιστές να επικοινωνούν αποτελεσματικά. Η προσπέλαση επιτρέπεται μόνο αν η τελευταία ενημέρωση πραγματοποιήθηκε από παλαιότερη συναλλαγή, αλλιώς πραγματοποιείται τερματισμός και επανεκκίνηση της συναλλαγής (κατά την επανεκκίνηση δημιουργείται νέα χρονική σφραγίδα).

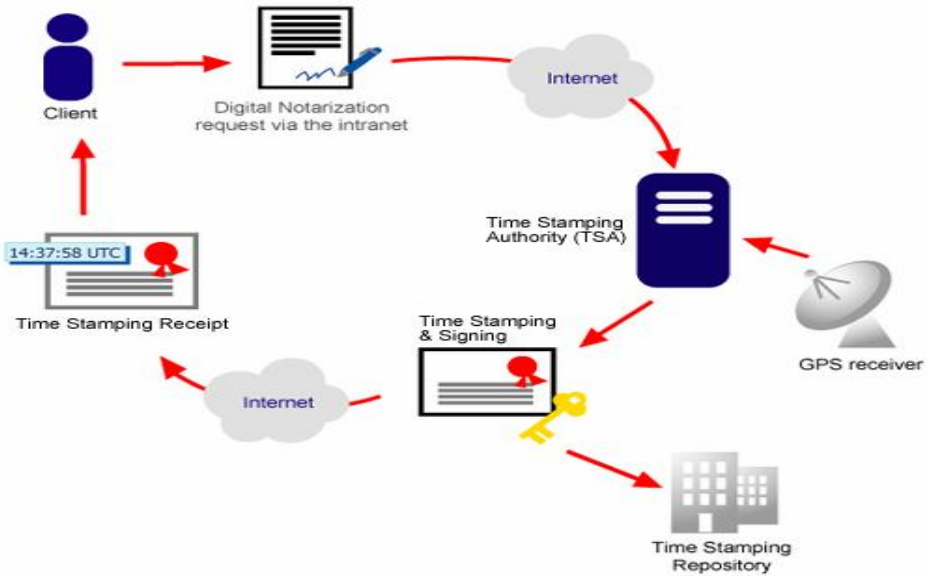
Οι χρονικές σφραγίδες χρησιμοποιούνται και σε δεδομένα (όχι μόνο για τις συναλλαγές).Έτσι έχουμε σε κάθε σελίδα δεδομένων μία χρονική σφραγίδα ανάγνωσης (timestamp-W), όπου είναι η τιμή της χρονικής σφραγίδας της συναλλαγής που πραγματοποίησε τελευταία ανάγνωση στη σελίδα δεδομένων, και μία χρονική σφραγίδα αποθήκευσης (timestamp-R), που είναι η χρονική σφραγίδα της συναλλαγής που πραγματοποίησε τελευταία ενημέρωση στη σελίδα δεδομένων. Κάθε φορά που πραγματοποιείται ανάγνωση ή αποθήκευση της σελίδας δεδομένων ενημερώνονται ανάλογα και οι τιμές timestamp-W και timestamp-R.



Παράδειγμα timestamp W και R

Για την απόκτηση πιστοποιημένης χρονικής σφραγίδας πρέπει να απευθυνθούμε στις Αρχές Χρονικής Σφραγίδας (Time Stamping Authority-TSA) που είναι υπεύθυνη για την έκδοση και επαλήθευση του χρόνου. Αυτή η Αρχή πρέπει να είναι αξιόπιστη, ουδέτερη, ανεξάρτητη και να λειτουργεί 24 ώρες την ημέρα. Πρέπει να παρέχει συμβατικές ρυθμίσεις με τους Προμηθευτές υπηρεσιών χρονικής σφραγίδας (Time Stamping Service Providers-TSSP).

Οι Προμηθευτές υπηρεσιών χρονικής σφραγίδας (Time Stamping Service Providers-TSSP) λειτουργούν ως το μεσαίο στρώμα μεταξύ της Αρχής Χρονικής Σφραγίδας (Time Stamping Authority-TSA) και των τελικών χρηστών και διευκολύνει την επικοινωνία μεταξύ τους. Συνήθως είναι ένας κλάδος ο οποίος αντιλαμβάνεται τις ειδικές ανάγκες των τελικών χρηστών.



Πιστοποίηση χρονικής σφραγίδας

iii. Ψηφιακός φάκελος (Digital Envelope)

Ψηφιακός φάκελος χρησιμοποιείται για την αποστολή εμπιστευτικών δεδομένων, είναι το αποτέλεσμα μίας διαδικασίας κρυπτογράφησης ενός μηνύματος (που μπορεί να είναι τα στοιχεία κάποιου συναλλασσόμενου) που χρησιμοποιεί δύο «στρώσεις» κρυπτογράφησης για την προστασία του.

Πρώτα, το ίδιο το μήνυμα κωδικοποιείται χρησιμοποιώντας συμμετρική κρυπτογράφηση, και στη συνέχεια, το κλειδί για την αποκωδικοποίηση του μηνύματος κρυπτογραφείται με τη χρήση του δημοσίου κλειδιού κρυπτογράφησης.

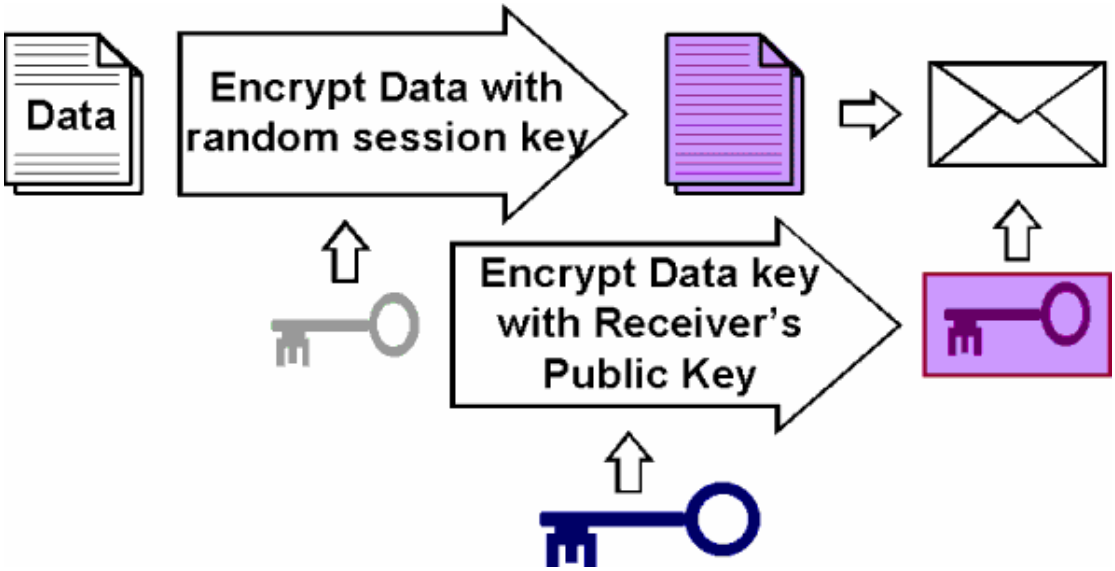
Δηλαδή ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί. Αυτή η τεχνική υπερνικά το σημαντικότερο πρόβλημα του δημόσιου κλειδιού κρυπτογράφησης, το οποίο είναι το ότι είναι πιο αργή από συμμετρική κρυπτογράφηση. Λόγω του ότι μόνο το κλειδί είναι προστατευμένο με κρυπτογράφηση δημόσιου κλειδιού, υπάρχει πολύ μικρή επιβάρυνση.

Για να το κατανοήσουμε θα δώσουμε ένα παράδειγμα:

Ας υποθέσουμε ότι έχουμε δύο χρήστες, τον Α και τον Β.

Ο χρήστης Α θέλει να στείλει μήνυμα στον χρήστη Β. Ο Α διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με την δημόσια κλείδα του Β. Στέλνει στον Β το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί.

Όταν ο Β θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί την ιδιωτική του κλείδα για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ενός παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με την δημόσια κλείδα του κάθε παραλήπτη. Και πάλι μεταδίδεται μόνο ένα κρυπτογραφημένο μήνυμα.



Αναπαράσταση κρυπτογράφησης κλειδιών.

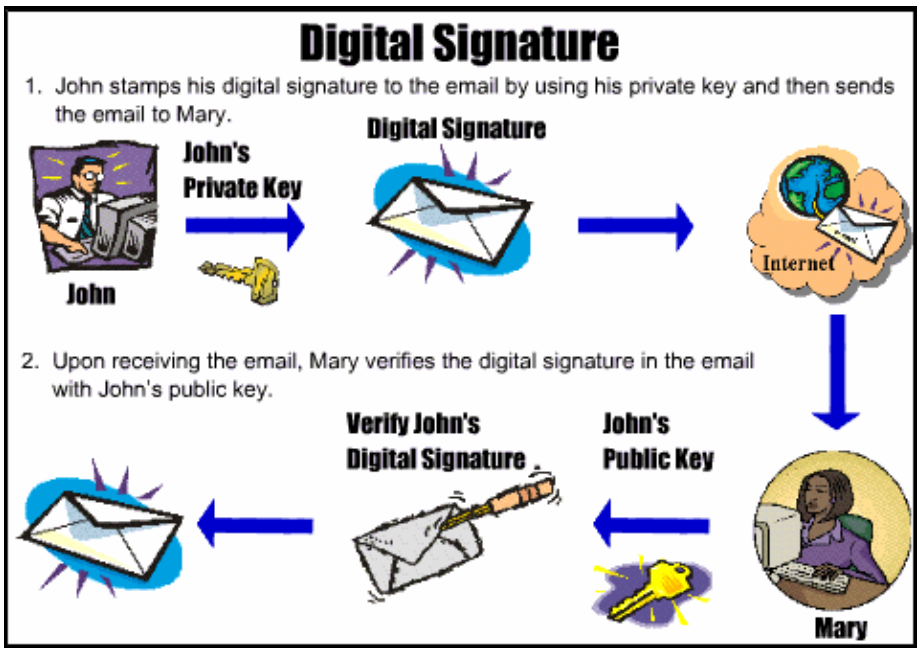
Οι χρήστες έχουν τη δυνατότητα να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι βελτιώνουν την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος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

Το μυστικό κλειδί DES καλείται *ψηφιακός φάκελος* γιατί πρέπει να ανοιχθεί πρώτα για να μπορέσει να αποκωδικοποιηθεί το περιεχόμενο του μηνύματος με αυτό.

iv. Ψηφιακή ή Ηλεκτρονική υπογραφή (Digital Signature)

Η ηλεκτρονική υπογραφή είναι ένα ακόμη μέσο επίτευξης της ασφάλειας σε συστήματα ηλεκτρονικού χρήματος και πολύ χρήσιμη στο ηλεκτρονικό εμπόριο. Η νομιμοποίηση ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε. Καθώς τα ηλεκτρονικά έγγραφα όμως τείνουν να αντικαταστήσουν τα παραδοσιακά χειρόγραφα, αντίστοιχα και η υπογραφή γίνεται «εικονική», ηλεκτρονική.

Οι ψηφιακές υπογραφές χρησιμοποιούν ασύμμετρη κρυπτογραφία. Ο χρήστης διαθέτει ένα ζεύγος κλειδιών (ένα δημόσιο και ένα ιδιωτικό) τα οποία έχουν μαθηματικό συσχετισμό (μέσω αλγορίθμων π.χ. RSA, DSA κ.α.). η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι αδύνατο να υπολογίσει το άλλο. Ουσιαστικά έχουν συμπληρωματική σχέση αφού το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευση της. Ο αποστολέας χρησιμοποιεί το ιδιωτικό κλειδί, που πιστοποιεί την αυθεντικότητά του, για να δημιουργήσει την ηλεκτρονική υπογραφή και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί του αποστολέα. Όλοι όσοι γνωρίζουν ένα δημόσιο κλειδί μπορούν να επαληθεύσουν μια ψηφιακή υπογραφή του κατόχου του αντίστοιχου ιδιωτικού κλειδιού.



Πως λειτουργεί μια ψηφιακή υπογραφή.

Στη διαδικασία δημιουργίας και επαλήθευσης υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού –one way hash). Με την εφαρμογή συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint

ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης. Η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη) είναι διαφορετική για κάθε μήνυμα.

Αυτά τα μηνύματα που αποστέλλονται δεν είναι δυνατό να τροποποιηθούν κατά τη διάρκεια μετάδοσής, αφού οποιαδήποτε αλλοίωσή τα καθιστά αδύνατα να αποκρυπτογραφηθούν, κάτι που θα γίνει αμέσως αντιληπτό από τον παραλήπτη. Για να πλαστογραφηθεί μια ψηφιακή υπογραφή θα πρέπει ο δικαιούχος του ιδιωτικού κλειδιού να όπως έχει τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο είναι αποθηκευμένο το ιδιωτικό κλειδί).

Όπως είχαμε αναφέρει και στην αρχή του κεφαλαίου για να υπάρχει ασφάλεια στις συναλλαγές πρέπει να ισχύουν τέσσερα βασικά πράγματα, η εμπιστευτικότητα, η ακεραιότητα, μη αποποίηση ευθύνης και η πιστοποίηση, όλα αυτά τα παρέχει η ψηφιακή υπογραφή.

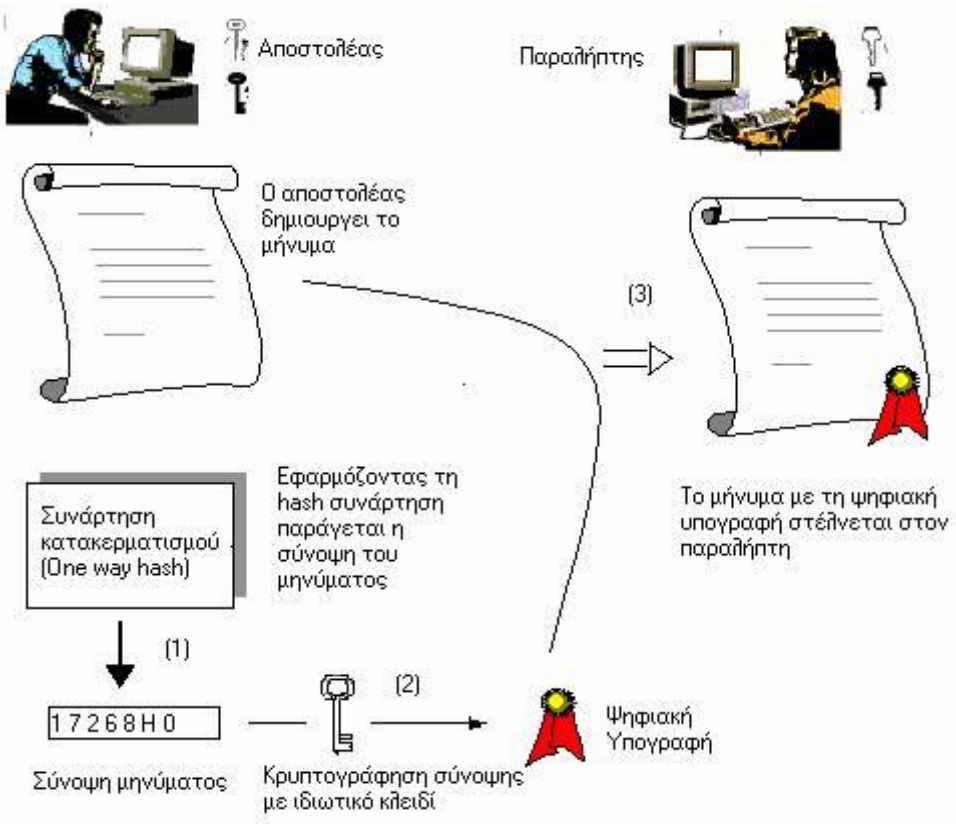
Η ψηφιακή υπογραφή υπηρετεί σκοπούς ύπαρξης ίδιους με της ιδιόχειρης αλλά υπάρχουν κάποιες διαφοροποιήσεις:

Ιδιόχειρη υπογραφή	Ψηφιακή υπογραφή
Ενσωματωμένη στο μήνυμα.	Εξωτερικό «αντικείμενο» το οποίο συνδέεται με το μήνυμα.
Για όλους όπως σκοπούς χρησιμοποιείται η ίδια υπογραφή.	Διαφορετικές υπογραφές για διαφορετικούς σκοπούς.
Δυνατή η πλαστογράφηση.	Σχεδόν αδύνατη η πλαστογράφηση.
Πιστοποιεί την ταυτότητα.	Πιστοποιεί τη γνησιότητα του περιεχομένου όπως πληροφορίας και την ταυτότητα του υπογράφοντος.
Απευθείας ορατή.	Απαιτείται ειδικό λογισμικό για να δημιουργηθεί και κατά συνέπεια για να είναι ορατή.
Ο «μηχανισμός» δημιουργίας παραμένει ο ίδιος και δεν μπορεί να αποσυρθεί.	Ο μηχανισμός δημιουργίας, επαλήθευσής μπορεί να καταστραφεί (αποσυρθεί) και να υποκατασταθεί από κάποιον εντελώς διαφορετικό.

Δημιουργία ψηφιακής υπογραφής

Για να δημιουργηθεί μια ψηφιακή υπογραφή κρυπτογραφείται η «σύνοψη» του μηνύματος, που όπως είπαμε και προηγουμένως είναι μια σειρά από bits με συγκεκριμένο πλήθος. Συγκεκριμένα:

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει.
2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη που έχει δημιουργηθεί. Αυτό που παράγεται είναι η ψηφιακή υπογραφή.
3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου.



Δημιουργία ψηφιακής υπογραφής.

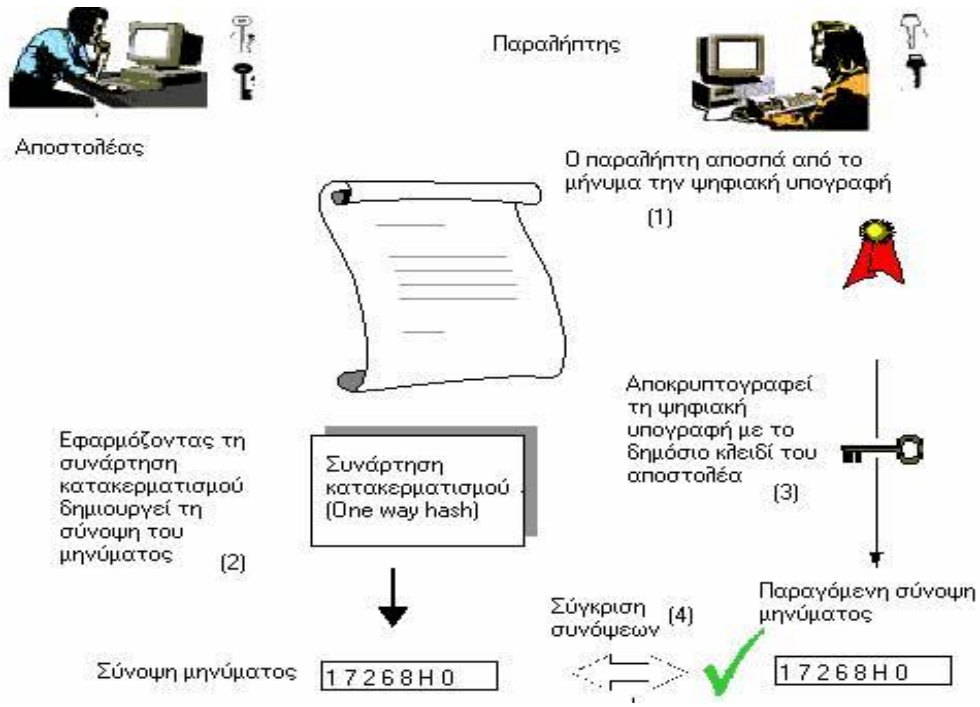
Επαλήθευση ψηφιακής υπογραφής

Κατά τη διαδικασία της επαλήθευσης (verification) μιας ψηφιακής υπογραφής, εφαρμόζεται στο κείμενο ο ίδιος αλγόριθμος κατακερματισμού που χρησιμοποιήθηκε κατά την υπογραφή του και δημιουργείται κατά αυτόν τον τρόπο μια νέα σύνοψη. Έπειτα αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα η κρυπτογραφημένη σύνοψη του μηνύματος. Έτσι, η νέα σύνοψη που παράγεται, συγκρίνεται με την αντίστοιχη σύνοψη που προέρχεται από την αποκρυπτογράφηση της ψηφιακής υπογραφής. Εάν ταυτίζονται οι δύο συνόψεις, τότε η υπογραφή επαληθεύεται και επιβεβαιώνεται αφενός μεν ότι τα δεδομένα υπογράφηκαν από τον

κάτοχο του σχετικού ιδιωτικού κλειδιού, αφετέρου δε ότι τα αρχικά δεδομένα δεν έχουν αλλοιωθεί.

Έτσι έχουμε τα εξής βήματα:

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).
4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.



Επαλήθευση ψηφιακής υπογραφής.

Σε μία συναλλαγή όμως ο παραλήπτης πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Απαιτείται δηλαδή να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Την πιστοποίηση αυτή δίνει ο Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) που είναι ένας «οργανισμός», ο οποίος παρέχει μεταξύ άλλων την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του.

v. Υδατογραφήματα (Watermarks)

Εκτός από τις ψηφιακές υπογραφές και την κρυπτογραφία έννοιες όπως η στεγανογραφία, η υδατογράφηση αναφέρονται ως μέθοδοι προστασίας των πνευματικών δικαιωμάτων στον ψηφιακό κόσμο.

Η στεγανογραφία επιτρέπει την κρυφή επικοινωνία, συνήθως κρύβοντας τις πληροφορίες σε άλλα δεδομένα υπεράνω υποψίας. Βασίζεται στην υπόθεση ότι η ύπαρξη κρυφής επικοινωνίας είναι άγνωστη σε τρίτους και χρησιμοποιείται κυρίως στην κρυφή σημείο-προς-σημείο επικοινωνία ανάμεσα σε έμπιστα μέρη. Ως εκ τούτου, οι κρυφές πληροφορίες δε μπορούν να ανακτηθούν μετά από παραποίηση των δεδομένων.

Σε αντίθεση με την κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει την πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Συμπερασματικά, η στεγανογραφία επιδιώκει την απόκρυψη της πληροφορίας χωρίς να λαμβάνει υπόψη το ενδεχόμενο επίθεσης σε αυτήν, προφυλάσσοντάς την μέσα σε κάποιο "στεγανό". Η κρυπτογραφία εξασφαλίζει ότι η πληροφορία που θα διαβαστεί από μη εξουσιοδοτημένους χρήστες θα είναι άχρηστη και ακατανόητη ή παραπλανητική. Η κρυπτογραφία επίσης, προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο.

Η υδατογράφηση (watermarking) έχει την ιδιότητα προστασίας του περιεχομένου και μετά την αποκρυπτογράφηση του, τοποθετώντας την πληροφορία μέσα στο

περιεχόμενο, απ’ όπου δεν αφαιρείται ποτέ κατά την κανονική χρήση. Ακόμα κι αν η ύπαρξη κρυφών πληροφοριών είναι γνωστή, είναι δύσκολο -ιδανικά αδύνατο- να καταστραφεί το ένθετο υδατογράφημα.

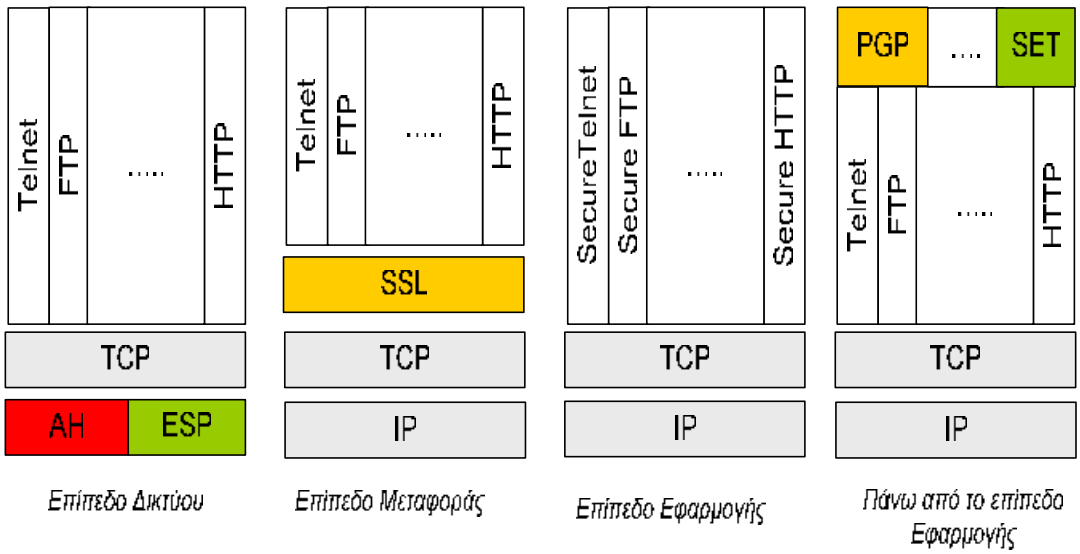
Από όλα όσα αναφέρθηκαν σε αυτό το κομμάτι του κεφαλαίου βλέπουμε ότι όλες οι μορφές πιστοποίησης αποτελούν μεθόδους προστασίας και ασφαλείας στη διακίνηση των ηλεκτρονικών εγγράφων και των ηλεκτρονικών συναλλαγών. Συμπερασματικά, κρίνεται σκόπιμο να αναφερθεί ότι παρέχουν εγγύηση της αυθεντικότητας, της ακεραιότητας, της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Ωστόσο, προστατεύουν ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο. Κατά συνέπεια, προκύπτει πως η ιδανικότερη λύση για την ασφαλή διακίνηση αλλά και χρήση των ψηφιακών αντικειμένων είναι ο συνδυασμός των αναπτυγμένων μεθόδων προστασίας.

VII. ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Πρωτόκολλο είναι ένα σύνολο από κανόνες και πρότυπα που δίνουν τη δυνατότητα στον υπολογιστή να ανταλλάσσει πληροφορίες. Ο αρχικός στόχος στη διατύπωση των πρωτοκόλλων μεταφοράς αρχείων ήταν να κατασταθούν οι μεταφορές αρχείων απλές και να ανακουφιστεί ο χρήστης του φορτίου της εκμάθησης των λεπτομερειών στον τρόπο με τον οποίο η μεταφορά ολοκληρώνεται πραγματικά. Για την πιστοποίηση της ταυτότητας των συναλλασσόμενων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που εγγυώνται την ταυτότητα των συναλλασσομένων ή την ασφάλεια μιας τοποθεσίας Web.

Έχουν αναπτυχθεί διάφορα πρωτόκολλα ασφαλείας ώστε να εξασφαλίζεται το περιβάλλον λειτουργίας και κανένα χαρακτηριστικό να μην αφήνεται στην τύχη, καμία λειτουργία να μην μένει χωρίς έλεγχο και κανένας χρήστης ή επισκέπτης να μην μπορεί να παραβεί την ιεραρχία και τα επιτρεπτά επίπεδα πρόσβασης, όπως το SSL (Secure Sockets Layer), που αναπτύχθηκε από τη Netscape, και το SET (Secure

Electronic Transactions), που αναπτύχθηκε από τη Visa και τη Mastercard, και θα μιλήσουμε παρακάτω για αυτά.



Το σχήμα μας δείχνει τις σχέσεις των πρωτοκόλλων ασφαλείας με το TCP/IP στοίβας, για τα οποία θα μιλήσουμε παρακάτω.

Α) Πρωτόκολλα ασφαλείας

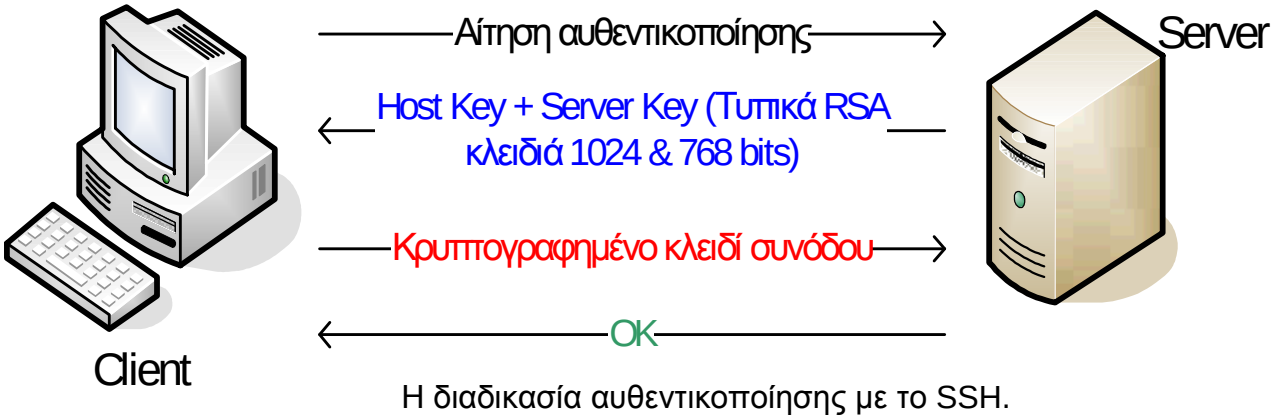
i) SSH (Secure Shell)

Αυτό το πρωτόκολλο (μεταφοράς αρχείων) χρησιμοποιείται για να συνδεθεί κάποιος με ασφάλεια με κάποιον άλλον που βρίσκεται μακριά, επίσης να μπορεί να εκτελεί εντολές σε αυτόν και να μεταφέρει αρχεία.

Είναι ένα σχετικά απλό πρόγραμμα που χρησιμοποιεί ένα γενικό πρωτόκολλο ασφαλείας επιπέδου μεταφοράς (βλέπε 4Γ1) και παρέχει υποστήριξη για αμοιβαία αυθεντικοποίηση, συμπίεση δεδομένων, εμπιστευτικότητα και ακεραιότητα δεδομένων. Δεν μπορούν τρίτοι να πλαστογραφήσουν τα πακέτα που στέλνει ο χρήστης και να υποκλέψουν τους κωδικούς πρόσβασης και άλλα δεδομένα. Με άλλα λόγια το SSH ποτέ δεν εμπιστεύεται το δίκτυο και πάντα προσέχει για την αξιόπιστη ροή των δεδομένων.

Μειονέκτημα αποτελεί το ότι παρ' όλο που χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού για τον έλεγχο της ταυτότητας του απομακρυσμένου υπολογιστή, και μπορεί

να απαιτείται πιστοποίηση της ταυτότητας του χρήστη που αιτείται σύνδεσης, υπάρχει η έλλειψη ολοκληρωμένης διαχείρισης δημόσιων κλειδιών με πιστοποιητικά.



Η διαδικασία αυθεντικοποίησης με το SSH.

Το **SSH** συνήθως χρησιμοποιείται και από άλλα πρωτόκολλα όπως το FTP (File Transfer Protocol).

Το **FTP** είναι κι αυτό ένα πρωτόκολλο, μεταφοράς αρχείων, που σου επιτρέπει τη μεταφορά αρχείων μεταξύ του τοπικού υπολογιστή και ενός διακομιστή στο ιντερνέτ και προς τις δύο κατευθύνσεις.

Ασφάλεια παρέχεται με την υποχρεωτική από τον χρήστη εισαγωγή του username και του password που μπορεί να είναι είτε Επώνυμα FTP, όπου πρόσβαση έχουν χρήστες που διαθέτουν λογαριασμό (user account) και έχουν username και password, είτε Ανώνυμα FTP που επιτρέπουν τη λεγόμενη «ανώνυμη» πρόσβαση (anonymous login) δηλαδή ο κάθε χρήστης βάζει για username τη λέξη «anonymous» και για password τη διεύθυνση e-mail που χρησιμοποιεί.

Όταν αυτά τα δύο πρωτόκολλα χρησιμοποιηθούν μαζί δηλαδή όταν τρέχει το FTP πρωτόκολλο μέσω του SSH τότε έχουμε το **SFTP** ή αλλιώς Secure FTP.

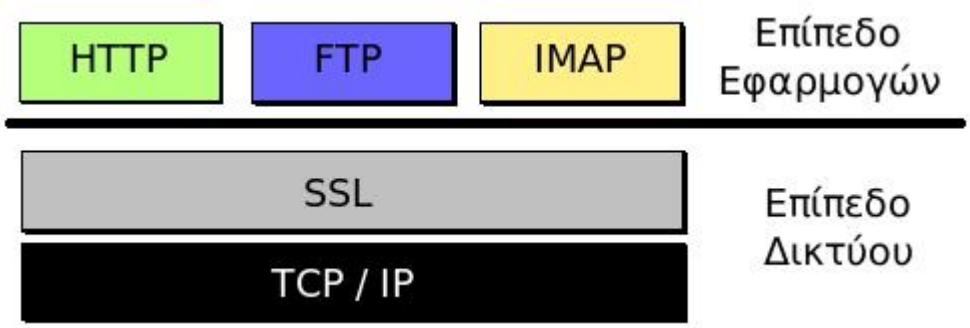
Σε αντίθεση με το απλό FTP το SFTP κρυπτογραφεί και τις εντολές και τα δεδομένα, προστατεύοντας έτσι τους κωδικούς πρόσβασης και τις ευαίσθητες πληροφορίες από τη διαβίβαση στο διαδίκτυο. Παρ' όλο που λειτουργικά μοιάζουν μεταξύ τους ένας FTP client δεν μπορεί να επικοινωνήσει με ένα SFTP server αφού χρησιμοποιούν διαφορετικά πρωτόκολλα.

ii**) SSL (Secure Sockets Layer)**

Το πρωτόκολλο αυτό είναι ένα πρωτόκολλο γενικής χρήσης το οποίο αναπτύχθηκε από την εταιρεία Netscape Communications Corporation και σχεδιάστηκε για να παρέχει ασφάλεια κατά την επικοινωνία του πωλητή (server) με τον αγοραστή (client). Οι ιστοσελίδες που υποστηρίζουν το πρωτόκολλο αυτό έχουν σαν πρόθεμα του ονόματος χώρου το https αντί το http και ένα μικρό χρυσό λουκέτο κάτω δεξιά στην οθόνη του browser.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ του server και του client και χρησιμοποιώντας ένα συνδυασμό δημοσίου και ιδιωτικού κλειδιού μπορεί να προσφέρει υψηλό βαθμό ασφάλειας στη μεταφορά δεδομένων σχετικών με ηλεκτρονικές πληρωμές.

Το πρωτόκολλο αυτό τρέχει πάνω από το TCP/IP και κάτω από την διεπαφή μεταξύ του στρώματος δικτύου (Network Layer) και του στρώματος εφαρμογής (Application Layer).



Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου.

Έτσι το SSL χρησιμοποιεί το TCP/IP για την μεταφορά δεδομένων και είναι σε θέση να παρέχει υπηρεσίες ασφαλείας για αυθαίρετες TCP/IP εφαρμογές, ανεξάρτητα από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Αυτό είναι το σημαντικό

πλεονέκτημα του SSL γιατί μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα HTTP, FTP και άλλα.

Ουσιαστικά το SSL παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, τις κρυπτογραφεί και στη συνέχεια τις μεταδίδει στο internet προς τον υπολογιστή που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Υπό-πρωτόκολλα του SSL και τρόπος λειτουργίας τους

Το πρωτόκολλο SSL αποτελείται βασικά από δύο επιμέρους πρωτόκολλα:
α) Το SSL Record πρωτόκολλο,
β) το SSL Handshake πρωτόκολλο.
Συγκεκριμένα:
α) Το SSL Record πρωτόκολλο καθορίζει τη μορφή με την οποία αναμεταδίδονται τα δεδομένα, παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων. Αυτό το υπό-πρωτόκολλο λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό, τη συμπίεση και την κρυπτογράφηση δεδομένων.
Δέχεται ως είσοδο ένα μπλοκ δεδομένων αυθαίρετου μήκους και παράγει ως έξοδο μια σειρά από SSL εγγραφές με μέγιστο μήκος 16.383 bytes η καθεμία.

Κάθε εγγραφή SSL Record περιέχει τις ακόλουθες πληροφορίες:

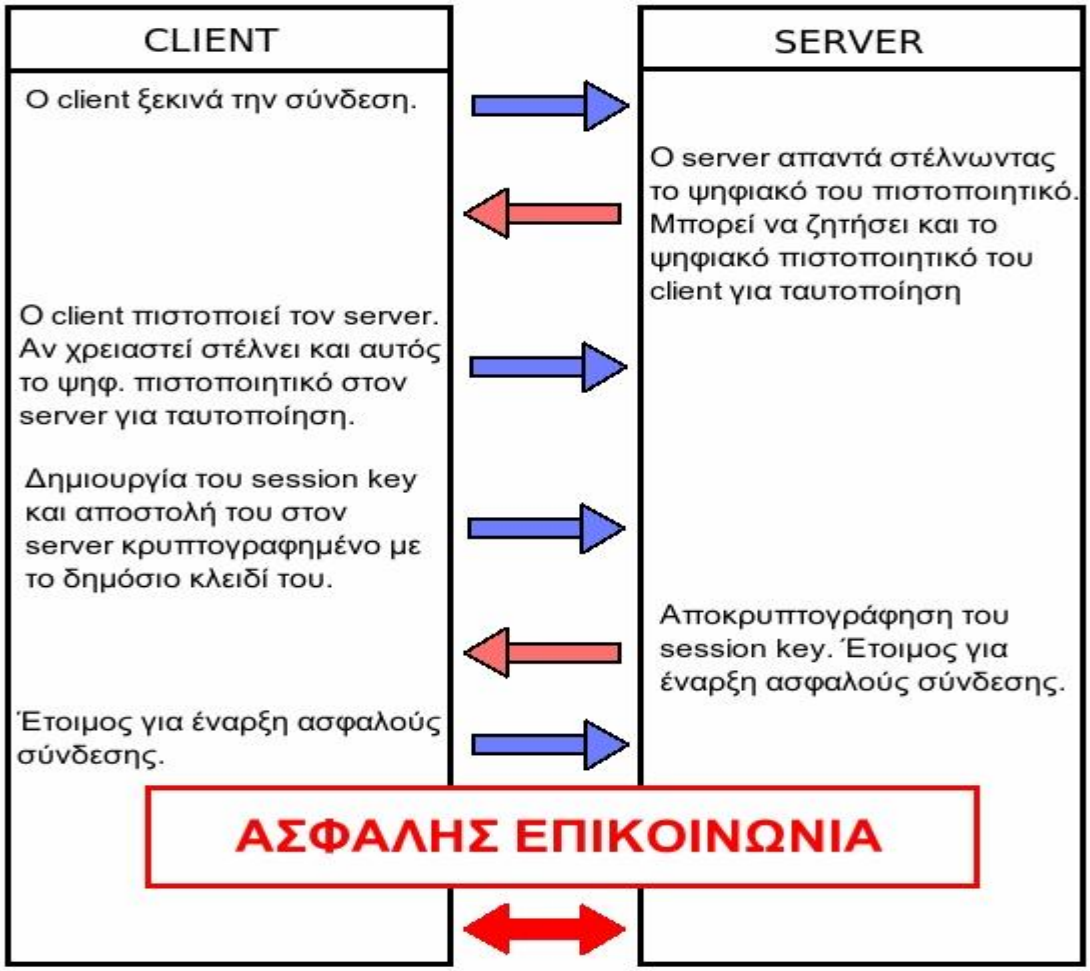
- Τύπο περιεχομένου (Content Type). Καθορίζει το πρωτόκολλο υψηλότερου επιπέδου που θα χρησιμοποιηθεί.
- Αριθμό έκδοσης πρωτοκόλλου (v.2 / v.3).
- Μήκος.
- Ωφέλιμο φορτίο δεδομένων (data payload), το οποίο είναι προαιρετικά συμπιεσμένο και κρυπτογραφημένο, σύμφωνα με αυτά που συμφωνήθηκαν κατά τη φάση Handshake.
- Κώδικα αυθεντικοποίησης μηνυμάτων (MAC), ο οποίος προστίθεται πριν κρυπτογραφηθεί το ωφέλιμο φορτίο δεδομένων

β) Το πρωτόκολλο SSL Handshake χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Κάθε σύνδεση SSL Handshake ξεκινά με ανταλλαγή μηνυμάτων (γι' αυτό χρησιμοποιεί το πρωτόκολλο SSL Record) μεταξύ του SSL Server και του SSL Client έως ότου επιτευχθεί η ασφαλής σύνδεση.

Το Handshake, δηλαδή η χειραψία του Server με τον Client, επιτρέπει στον Server να αποδείξει την ταυτότητα του στον Client και προαιρετικά ο client να αποδείξει την ταυτότητα του στον server. Επίσης γίνεται η επιλογή, από τον Server και τον Client, του κρυπτογραφικού αλγορίθμου που θα χρησιμοποιήσουν, ή του κρυπτογραφήματος (cipher) που υποστηρίζουν και συνεργάζονται για τη δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Έτσι δημιουργείται μια SSL σύνδεση.

Τα Ciphers (κρυπτογραφήματα) που χρησιμοποιούνται από την SSL είναι:

- DES (Data Encryption Standard)
- Triple DES
- DSA (Digital Signature Algorithm)
- KEA (Key Exchange Algorithm)
- MD5 (Message Digest Algorithm)
- RC2 και RC4
- RSA και RSA Key-Exchange
- SHA-1 (Secure Hash Algorithm)
- SKIPJACK (εφαρμόζεται στον FORTEZZA)



Η διαδικασία της χειραψίας των δύο συσκευών σύμφωνα με το πρωτόκολλο SSL.

Το παρακάτω παράδειγμα, που είναι κάτι που σχεδόν όλοι μας έχουμε κάνει, μια αγορά μέσω διαδικτύου, μας βοηθάει ώστε να γίνει πιο κατανοητός ο τρόπος λειτουργίας του SSL Handshake:

Στην περίπτωση της αγοράς ενός προϊόντος μέσω ενός ηλεκτρονικού συστήματος, ο αγοραστής υποβάλλει την αίτηση για την αγορά μέσω διαδικτύου με την αποστολή ενός μηνύματος. Παραλαμβάνει από τον πωλητή ένα δημόσιο κλειδί στον υπολογιστή του, ώστε να κρυπτογραφήσει τα απαραίτητα δεδομένα για την ολοκλήρωση της συναλλαγής (όπως το είδος και ο αριθμός του μέσου πληρωμής ή το ποσό). Τα κρυπτογραφημένα δεδομένα αποστέλλονται με τη χρήση του SSL στον υπολογιστή του πωλητή, όπου αποκρυπτογραφούνται με τη χρήση του ιδιωτικού κλειδιού του τελευταίου. Έτσι ολοκληρώνεται με ασφάλεια η συναλλαγή, χωρίς ο ίδιος να κατέχει ιδιαίτερες τεχνολογικές γνώσεις.

Από την άλλη πλευρά η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Λόγω αυτών των καθυστερήσεων χρησιμοποιείται πλέον μόνο σε περιπτώσεις που πραγματικά χρειάζεται ασφαλής σύνδεση και όχι σε περιπτώσεις απλής επίσκεψης σε μια ιστοσελίδα.

Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε τη βάση για τη μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (που θα μιλήσουμε παρακάτω), το οποίο τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου και αποτελούν τα καλύτερα πρωτόκολλα ασφαλείας.

iii) TLS (Transport Layer Security)

Παρόλο που το SSL είναι το πιο γνωστό κρυπτογραφικό πρωτόκολλο ασφαλείας τείνει να αντικατασταθεί από το TLS. Το SSL 3.0 ήταν η βάση του TLS 1.0, αλλά και τα δύο βρίσκονται στην κορυφή των πρωτοκόλλων μεταφοράς. Υπάρχουν μικρές διαφορές μεταξύ SSL και TLS, αλλά το πρωτόκολλο παραμένει ουσιαστικά το ίδιο.

Το πρωτόκολλο TLS είναι χρήσιμο στις οικονομικές συναλλαγές και στην ανταλλαγή εμπορικών δεδομένων. Επιτρέπει στις εφαρμογές να επικοινωνούν μέσω δικτύου, με δυνατότητα χρήσης κρυπτογράφησης δεδομένων, ούτος ώστε να επιτυγχάνεται πρόληψη της υποκλοπής, της αλλοίωσης καθώς και μηνυμάτων πλαστογραφίας.

Είναι σχεδιασμένο να εγκαθιδρύει μια ασφαλή σύνδεση μεταξύ ενός server και ενός client όπως και SSL, αλλά έχει κάποιες επεκτάσεις ώστε να αποφεύγεται η διαλειτουργικότητα μεταξύ των δύο πρωτοκόλλων. Δεν είναι εξαρτημένο από το TCP/IP και τρέχει κάτω από τα πρωτόκολλα αιτήσεων όπως HTTP, FTP, TELNET.

Οι στόχοι του πρωτοκόλλου TLS είναι οι ίδιοι με του SSL και είναι οι εξής:

- Ασφάλεια κρυπτογράφησης: το TLS πρέπει να χρησιμοποιείται για να δημιουργήσει μία ασφαλής σύνδεση μεταξύ των δυο μερών.

- Διαλειτουργικότητα: ανάπτυξη αιτήσεων και αποστολή κρυπτογραφημένων παραμέτρων από ανεξάρτητους προγραμματιστές.
- Επεκτασιμότητα: δημιουργία προτύπου με βάση το οποίο νέα δημόσια κλειδιά και μέθοδοι κρυπτογράφησης μπορούν να συνεργαστούν όσο το δυνατόν περισσότερο.
- Σχετική αποδοτικότητα: μείωση αριθμού συνδέσεων που απαιτείται να εγκατασταθούν και της δραστηριότητας του δικτύου.

Αποτελείται από τα ίδια υπό-πρωτόκολλα όπως το SSL:

- TLS record πρωτόκολλο,
- TLS handshake πρωτόκολλο.

α) Το TLS record πρωτόκολλο καθορίζει τη μορφή με την οποία αναμεταδίδονται τα δεδομένα, παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων. Πρώτα ορίζει έναν αλγόριθμο συμπίεσης, έναν αλγόριθμο κρυπτογράφησης και έναν MAC αλγόριθμο και μετά κάνει τις εξής εργασίες :

- Οριοθετεί τα δεδομένα σε καθορισμένα blocks,
- Συμπιέζει τα δεδομένα,
- Εφαρμόζει ένα MAC,
- Κρυπτογραφεί,
- Αποστέλλει μηνύματα.

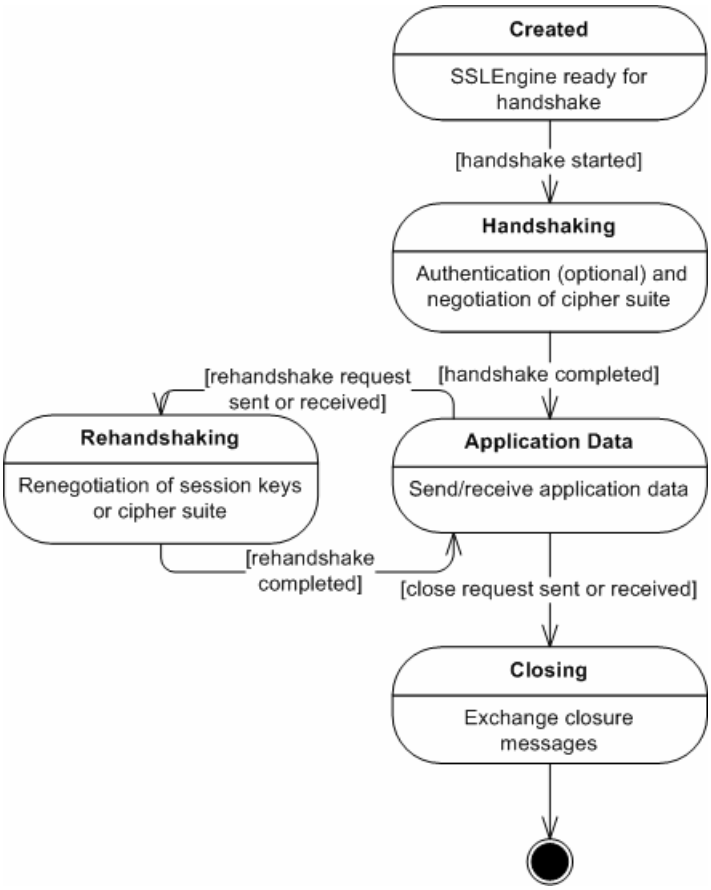
Το πρωτόκολλο TLS Record είναι ένα πρωτόκολλο με στρώματα. Σε κάθε στρώμα, τα μηνύματα μπορεί να περιλαμβάνουν πεδία για το μήκος, την περιγραφή και το περιεχόμενο. Το TLS παίρνει τα μηνύματα που πρέπει να διαβιβασθούν, κάνει διαχειρισμό των δεδομένων σε μπλοκ, προαιρετικά, συμπιέζει τα δεδομένα, εφαρμόζει ένα MAC, κρυπτογραφεί και μεταδίδει το αποτέλεσμα (όπως αναφερθήκαμε πιο πριν).Τα δεδομένων που λαμβάνονται αποκρυπτογραφούνται, επαληθεύονται, αποσυμπιέζονται, ανασυγκροτούνται και, στη συνεχεία, παραδίδονται σε υψηλότερο επίπεδο πελατών.

β) Το TLS handshake πρωτόκολλο χρησιμοποιείται για να συμφωνήσουν ο client και ο server σχετικά με διάφορες παραμέτρους που θα χρησιμοποιήσουν για την ασφαλή σύνδεση μεταξύ τους.

Περιλαμβάνει τα εξής βήματα :

1. Ανταλλαγή μηνυμάτων Hello, μεταξύ του client και του server, ώστε να συμφωνηθούν οι αλγόριθμοι και να γίνει ανταλλαγή τυχαίων τιμών.
2. Ανταλλαγή απαραίτητων παραμέτρων κρυπτογράφησης.
3. Ανταλλαγή πιστοποιητικών και πληροφοριών κρυπτογράφησης.
4. Δημιουργία πρωτεύοντος κλειδιού από το δευτερεύον και ανταλλαγή τυχαίων τιμών.
5. Παροχή στο στρώμα record παραμέτρων ασφαλείας.
6. Πιστοποίηση από τους client και server ότι υπολόγισαν τις ίδιες παραμέτρους ασφαλείας και ότι λειτούργησε το handshaking χωρίς την παρεμβολή κάποιας επίθεσης.

Ο server με τη βοήθεια των hello μηνυμάτων ορίζει αν είναι αναγκαία ή όχι η πιστοποίηση του. Αν ο server δεν έχει στην κατοχή του το αναγκαίο πιστοποιητικό τότε αποστέλλεται το κλειδί του, και μετά την πιστοποίηση του αναμένεται η πιστοποίηση του client του οποίου το κλειδί που αποστέλλεται εξαρτάται σε κάποιο βαθμό από τον αλγόριθμο του δημοσίου κλειδιού.



Λειτουργία handshaking από SSL/TLS.

Το TLS handshake protocol έχει και αυτό δικά του υπό-πρωτόκολλα. Αυτά χρησιμοποιούνται για να επιτρέπουν στα μέλη της σύνδεσης να συμφωνούν όσον αφορά τις παραμέτρους ασφαλείας για το στρώμα εγγραφής, να πιστοποιούν τους ίδιους τους εαυτούς τους και τις υπό διαπραγμάτευση παραμέτρους ασφαλείας και να αναφέρει το ένα μέλος στο άλλο σφάλματα στις συνθήκες.

Συγκεκριμένα:

- Το change cipher spec αποτελεί πρωταρχική παράμετρο κρυπτογράφησης που σχετίζεται με τον τομέα της ασφάλειας και χρησιμοποιείται για τη μετάδοση σημάτων.Αποτελείται από ένα απλό μήνυμα το οποίο είναι κρυπτογραφημένο και συμπιεσμένο στην τρέχουσα κατάσταση σύνδεσης. Το μήνυμα στέλνεται από τον client και τον server κατά την διάρκεια του handshake, αλλά πριν αποσταλεί το ολοκληρωμένο και πιστοποιημένο μήνυμα.

- Το alert protocol υποστηρίζεται από το επίπεδο TLS record. Περιλαμβάνει alert μηνύματα τα οποία είναι συμπιεσμένα και κρυπτογραφημένα και προκαλούν άμεση διακοπή της σύνδεσης.

- Το application data παρέχει προστασία των δεδομένων που πρόκειται να μεταφερθούν και χρησιμοποιεί κρυπτογραφικό αλγόριθμο MAC.

Όπως είπαμε τα πρωτόκολλα SSL-TLS έχουν πολλές διαφορές αλλά είναι, ουσιαστικά, το ίδιο πρωτόκολλο. Οι ομοιότητες και οι διαφορές τους φαίνονται παρακάτω:

ΟΜΟΙΟΤΗΤΕΣ	ΔΙΑΦΟΡΕΣ
1. Έχουν δύο υπο-πρωτόκολλα (record και handshake).	Τα MAC schemes διαφέρουν στις δύο εκδόσεις.
2. Ίδιοι στόχοι.	Στο TLS υπάρχουν επιπλέον κωδικοί (alert codes).
3. Τρέχουν πάνω από το TCP/IP και δεν εξαρτούνται από αυτό.	Το TLS δεν υποστηρίζει την κρυπτογράφηση Fortezza.
4. Τοποθετούνται στην κορυφή των πρωτοκόλλων μεταφοράς.	Το SSL έχει επιπλέον client certificate types.
5. Χρήση MAC αλγορίθμων.	Τα «σπασίματα» (hashes) υπολογίζονται διαφορετικά στην πιστοποίηση του μηνύματος για handshaking.
6. Συγκεκριμένα βήματα handshaking.	Γίνεται διαφορετικός υπολογισμός για το πρωτεύον κλειδί (master secret).

Δύο πρότυπα τα οποία βρίσκονται υπό ανάπτυξη για τα συστήματα ηλεκτρονικών πληρωμών είναι :

Το **Secure Electronic Transactions (SET), το οποίο δημιουργήθηκε από την Visa** και την **MasterCard**. Αυτό το πρότυπο χρησιμοποιεί τα ψηφιακά πιστοποιητικά

για την εγκυρότητα της ταυτότητας των χρηστών που συμμετέχουν σε μια ηλεκτρονική συναλλαγή. Ακόμη, κρυπτογραφεί πριν την μετάδοση τους στο Internet τις πληροφορίες των πιστωτικών καρτών.

Το **Joint Electronic Payments Initiative (JEPI)**, **το οποίο δημιουργήθηκε από την** CommerceNet και το World Wide Web Consortium. Είναι αποτέλεσμα μιας προσπάθειας για προτυποποίηση στους διάφορους μηχανισμούς πληρωμών (πιστωτικές και χρεωστικές κάρτες, ψηφιακό χρήμα και ηλεκτρονικές επιταγές).

Το JEPI παρέχει τη δυνατότητα στον πελάτη να χρησιμοποιήσει μια μόνο εφαρμογή και μια μόνο διεπαφής χρήστη για την διεκπεραίωση των συναλλαγών.

iv) SET (Secure Electronic Transactions)

Secure Electronic Transaction (SET) είναι ένα πρότυπο πρωτόκολλο για την εξασφάλιση συναλλαγών με πιστωτικές κάρτες σε ανασφαλή δίκτυα, συγκεκριμένα, το Internet. Οι περισσότερες μέθοδοι πληρωμής μέσω internet στρέφονται γύρω από την πιστωτική κάρτα και οι καταναλωτές διστάζουν να αποκαλύψουν τα στοιχεία της κάρτας στο Διαδίκτυο. Έτσι για να αντιμετωπιστούν οι ανησυχίες των καταναλωτών για την ασφάλεια αλλά και για να αναπτυχθεί το ηλεκτρονικό εμπόριο, οι δυο κορυφαίες μάρκες πιστωτικών καρτών, η Visa και η MasterCard, συνεργάστηκαν με εταιρείες όπως η GTE, IBM, Microsoft, Netscape και η Verisign το 1996 και δημιούργησαν ένα εγγυημένα ασφαλές πρότυπο συναλλαγών, που ονομάζεται SET.

Ένα σύστημα SET περιλαμβάνει τα εξής μέρη:

- Κάτοχο κάρτας,
- Έμπορος ,
- Εκδότης ,
- Αγοραστής ,
- Πύλη πληρωμών (payment gateway), που ουσιαστικά είναι οι τράπεζες,
- Αρχή πιστοποίησης (μια έμπιστη Τρίτη οντότητα-ΕΤΟ).

Ουσιαστικά το SET εξασφαλίζει ότι οι πληροφορίες της κάρτας είναι αληθινές, διασφαλίζει ότι οι πληροφορίες δεν μπορούν να αλλάξουν ή να αλλοιωθούν και

εξασφαλίζει ότι ο κάτοχος της κάρτας και οι έμποροι είναι πραγματικά αυτοί που ισχυρίζονται ότι είναι. Δηλαδή ισχύει η εμπιστευτικότητα, η ακεραιότητα και η γνησιότητα και των δύο.

Η λειτουργία του SET βασίζεται στην κρυπτογράφηση, στα ψηφιακά πιστοποιητικά και τη χρήση ψηφιακών υπογραφών, με σκοπό τη διασφάλιση ότι ένα μήνυμα λαμβάνεται μόνο από τον επιθυμητό παραλήπτη, χωρίς αλλαγές στο περιεχόμενο, ενώ παράλληλα περιέχει στοιχεία που επιτρέπουν την επαλήθευση του αποστολέα του.

Χρησιμοποιεί συμμετρική, Encryption Standard (DES), αλλά και ασύμμετρη μέθοδο κρυπτογράφησης, με αποτέλεσμα η διαδικασία της συναλλαγής να γίνεται μεν πιο πολύπλοκη, αλλά και περισσότερο ασφαλής. Οι δύο αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται είναι DES 56-bit για την κρυπτογράφηση των συναλλαγών και RSA.

Το SET είναι εξαιρετικά πιο πολύπλοκο από το SSL, το οποίο απλώς διαπραγματεύεται κλειδιά συνόδου μεταξύ της κάρτας και του έμπορου. Ένα πρωτόκολλο όπως το SSL ή το TLS κρατά τα στοιχεία της κάρτας ασφαλή, αλλά δεν κάνει τίποτα για την προστασία από τους ανέντιμους έμπορους ή πελάτες. Το SET απαιτεί από τους κατόχους καρτών και τους έμπορους να εγγράφουν προκείμενου να μπορούν να εμπλακούν σε συναλλαγές, έτσι αντιμετωπίζει το πρόβλημα, παρέχοντας πιστοποιητικά από την αρχή πιστοποίησης και στους δύο (έμπορο-πελάτη). Όλες οι παραγγελιές και επιβεβαιώσεις φέρουν ψηφιακή υπογραφή, η οποία παρέχει πιστοποίηση της ταυτότητας.

Από τα παραπάνω βλέπουμε την πολυπλοκότητα του πρωτοκόλλου λόγω της οποίας χρησιμοποιείται ελάχιστα. Γι’ αυτό και στο ξεκίνημα του απέτυχε να κερδίσει μερίδιο αγοράς.

Αυτό όμως μέχρι το 2000 όπου οι συχνές απάτες και οι καταχρήσεις των πιστωτικών καρτών αναζωπύρωσαν το ενδιαφέρον των εταιρειών και των προμηθευτών της κάρτας, για το πρωτόκολλο SET, που ξεκίνησε την ενσωμάτωση του σε συστήματα συναλλαγών. Ένας παράγοντας που βοήθησε στην επανεμφάνιση του πρότυπου SET ήταν η μετάβαση, από την πλευρά των πελατών, στο ψηφιακό

πορτοφόλι που παρέχει μια μεγαλύτερη ευελιξία στη αγορές τους αλλά και στην αποθήκευση δεδομένων. Και καθώς όλο και περισσότεροι καταναλωτές επιλέγουν να χρησιμοποιούν τις χρεωστικές κάρτες, παρά από τις πιστωτικές κάρτες, για τις ηλεκτρονικές αγορές, η ζήτηση για την ενίσχυση της ασφάλειας κλιμακώνεται.

Διπλή υπογραφή

Μια σημαντική καινοτομία που εισάγει το SET είναι η διπλή υπογραφή. Ο σκοπός της διπλής υπογραφής είναι ο ίδιος με της ηλεκτρονικής υπογραφής: να εγγυηθεί την εξακρίβωση της γνησιότητας και ακεραιότητας των δεδομένων. Συνδέει δυο μηνύματα που προορίζονται για τους δυο διαφορετικούς παραλήπτες. Σε αυτήν την περίπτωση, ο πελάτης θέλει να στείλει τη σειρά πληροφοριών προς τον έμπορο και τα στοιχεία πληρωμής προς την τράπεζα. Ο έμπορος δεν χρειάζεται να ξέρει ο τον αριθμό της πιστωτικής κάρτας του πελάτη και η τράπεζα δεν χρειάζεται να γνωρίζει τις λεπτομέρειες από την παραγγελία του πελάτη. Η σύνδεση είναι απαραίτητη ώστε ο πελάτης να μπορεί να αποδείξει ότι το πόσο προορίζεται για αυτή την παραγγελία.

Οι προϋπόθεσης για το SET είναι:

- Η εκδότρια τράπεζα θα χρειαστεί να ζητήσει από τον κατόχους καρτών να αποκτήσουν ψηφιακά πιστοποιητικά. Συνήθως, διαθέτει ένα χαρτοφυλάκιο λογισμικού, το οποίο θα δημιουργήσει ένα ψηφιακό πιστοποιητικό για τον κάτοχο της κάρτας αυτόματα.
- Θα πρέπει να υπάρχει ένας λογικός αριθμός εμπορικών δικτυακών τόπων που υποστηρίζουν SET. Επί του παρόντος ο αριθμός των SET-enabled web sites- είναι μικρό, ωστόσο, το ποσοστό αυτό αναμένεται να αυξηθεί σημαντικά στο μέλλον. Ο κατάλογος των τόπων SET-enabled είναι διαθέσιμος στις ιστοσελίδες της MasterCard (www.mastercard.com) και της Visa (www.visa.com).

Ένα απλό παράδειγμα για να περιγράψει τον τρόπο που λειτουργεί το SET από την οπτική γωνία του καταναλωτή είναι:

- Ο κάτοχος της κάρτας πάει σε έμπορο του web site και επιλέγει τα στοιχεία που αυτός η αυτή επιθυμεί να αγοράσει. Ο κάτοχος της κάρτας, στη συνεχεία κάνει κλικ στο κουμπί checkout counter. Μια οθόνη ξεπροβάλει παρέχοντας λεπτομερή

στοιχεία, συμπεριλαμβανομένης της δαπάνης του συνόλου των στοιχείων που θέλει να αγοράσει, συν τους φόρους και έξοδα Αποστόλης.

- Αυτό ενεργοποιεί το ηλεκτρονικό πορτοφόλι (digital wallet) και ζητά από τον πελάτη να επιλέξει μια πιστωτική κάρτα από αυτές που διαθέτει. Το ηλεκτρονικό πορτοφόλι λαμβάνει επίσης υπόψη του τα ψηφιακά πιστοποιητικά των δυο οντοτήτων: του έμπορου και της τράπεζας (επίσης ονομάζεται πύλη πληρωμών). Αυτά τα δυο πιστοποιητικά είναι επικυρωμένα.
- Το ηλεκτρονικό πορτοφόλι, στη συνέχεια, δημιουργεί ένα μήνυμα που περιέχει δυο τμήματα: τη σειρά πληροφοριών και τα στοιχεία της πληρωμής. Οι πληροφορίες περιέχουν στοιχεία προκείμενου να επιβεβαιωθεί η παραγγελιά, ενώ η πληρωμή περιέχει στοιχεία όπως ο αριθμός της κάρτας και το πόσο. Τα στοιχεία της πληρωμής κρυπτογραφούνται με ένα τυχαίο κλειδί, συμμετρική κρυπτογράφηση, το οποίο, με τη σειρά του, είναι κωδικοποιημένο με δημόσιο κλειδί, έτσι ώστε μόνο η πύλη πληρωμής να μπορεί να το αποκρυπτογραφήσει. Με αλλά λόγια, ο έμπορος δεν πρόκειται πότε να μάθει τις λεπτομέρειες του αριθμού της κάρτας του πελάτη. Αυτά τα δεδομένα αποστέλλονται αυτόματα από την ιστοσελίδα του έμπορου.
- Ο έμπορος θα επικυρώσει πρώτα το ψηφιακό πιστοποιητικό της κάρτας. Τότε θα στείλουν τα στοιχεία της πληρωμής στην πύλη πληρωμής.
- Η πύλη πληρωμών θα επαληθεύσει τα ψηφιακά πιστοποιητικά και των δυο θα αποκρυπτογραφήσει το μήνυμα και θα έχει πρόσβαση στον αριθμό της κάρτας και το πόσο.
- Τότε η πύλη πληρωμών θα στείλει τη συναλλαγή στην εταιρεία της κάρτας, και στη συνεχεία θα απευθύνει προς την τράπεζα έκδοσης της άδειας.
- Η πιστοποιημένη απάντηση κωδικοποιείται με το συνηθισμένο τρόπο και αποστέλλεται στο έμπορο, ο οποίος, με τη σειρά του, θα επικυρώσει το μήνυμα και να αποθηκεύσει την απάντηση. Στη συνεχεία, ο έμπορος θα μεριμνήσει για την αποστολή του εμπορεύματος.

Όλες αυτές οι συναλλαγές συμβαίνουν στο Διαδίκτυο και είναι αρκετά διαφανής για τον κάτοχο της κάρτας.

Το SET είναι ένα πρωτόκολλο που επιτρέπει εξαιρετικά ασφαλές αγορές στο internet, μέσω πιστωτικών καρτών, αλλά είναι εξαιρετικά πολύπλοκο. Η εκρηκτική αύξηση των συναλλαγών μέσω του Διαδικτύου θα τροφοδοτείται περαιτέρω από το

SET. Το πρωτόκολλο SET συνεχίζει να εξελίσσεται και αυτή τη στιγμή επεκτείνεται για να καλύψει την χρεωστική κάρτα συναλλαγών.

v) S/HTTP (Secure Hyper-text Transfer Protocol)

Το πρωτόκολλο που χρησιμοποιείται ευρέως μεταξύ των διαδικτυακών client και server είναι το HTTP (hyper text transfer protocol). Η ευκολία της χρήσης του www έχει κάνει τους πάντες να το χρησιμοποιούν για πολλές δικτυακές εφαρμογές, οι οποίες όμως απαιτούν αμοιβαία πιστοποίηση της ταυτότητας των δύο (client και server) όπως έχουμε πει πολλές φορές. Αυτή την πιστοποίηση το HTTP δεν μπορεί να την παρέχει αφού δεν υποστηρίζει κρυπτογραφικούς μηχανισμούς.

Έτσι ερχόμαστε στο S-HTTP (Secure HTTP) το οποίο είναι μια επέκταση του HTTP που μπορεί να χρησιμοποιείται για να παρέχει υπηρεσίες ασφαλείας από άκρη σε άκρη για συναλλαγές ιστού. Παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ ενός ζεύγους server-client, ευελιξία επιλογής κλειδιών και χρησιμοποιεί κρυπτογραφικούς αλγορίθμους με σκοπό να επιτρέψει αυθόρμητες εμπορικές συναλλαγές.

Σχεδιάστηκε από τους E. Rescorla και A. Schiffman του EIT. Στόχος τους ήταν να δημιουργηθεί ένα ευέλικτο πρωτόκολλο που θα διαθέτει πολλαπλούς μηχανισμούς και αλγορίθμους και θα υπάρχει η δυνατότητα διαπραγμάτευσης αυτών. Το S-HTTP δεν έγινε δεκτό από την Microsoft και την Netscape, λόγω του δικού τους πρωτοκόλλου SSL.

Χαρακτηριστικά του S/http:

1. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.
2. Αρκετά κρυπτογραφικά στάνταρ ενσωματώνονται στους S/HTTP clients και servers συμπεριλαμβανομένων των PEM, PGP και Kerberos (θα μιλήσουμε αργότερα γι’ αυτό). Είναι συμβατό με το HTTP.

3. Το S/HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλείδων από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί αυθόρμητες ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα.
4. Με το S/HTTP, σε καμία περίπτωση ευαίσθητα δεδομένα δεν θα μεταδοθούν στο δίκτυο απροστάτευτα.
5. Επιτρέπει πλήρη ευελιξία όσον αναφορά τους κρυπτογραφικούς αλγόριθμούς και τις παραμέτρους αυτών. Το είδος της παρεχόμενης προστασίας κρυπτογράφηση, ψηφιακή υπογραφή, και τα δύο), οι αλγόριθμοι και τα πιστοποιητικά μπορούν να διαπραγματευτούν.
6. Οι χρήστες αναμένονται να έχουν (αν και δεν συνιστάται) πολλαπλά πιστοποιητικά.
7. Χρησιμοποιεί το στιλ κεφαλίδων (Headers) του HTTP.

Δημιουργία μηνυμάτων

Υποθέτουμε ότι ένας server δημιουργεί ένα μήνυμα. Αυτό θα γίνει με την εξής διαδικασία:

1. ανακτά από το σκληρό δίσκο το αρχείο (που μπορεί να είναι ένα http μήνυμα ή κάτι άλλο),
2. επεξεργασία των προτιμήσεων του client για κρυπτογράφηση και των πληροφοριών για το κλειδί του,
3. κρυπτογράφηση με βάση τις υποδείξεις του client ή με βάση κάποιο προκαθορισμένο σύνολο επιλογών (default set),
4. αποστολή του μηνύματος στον client.

Στο προστατευμένο HTTP μήνυμα, έπειτα, προστίθενται κατάλληλες S/HTTP επικεφαλίδες και παράγεται το τελικό S/HTTP μήνυμα.

Παραλαβή του μηνύματος

Πριν είδαμε ότι ο server έστειλε ένα μήνυμα. Τώρα για να το πάρει ο client και να ανακτήσει την πληροφορία θα πρέπει:

1. Παίρνει το S-HTTP μήνυμα,
2. διαβάζει τις S-HTTP επικεφαλίδες,

3. συγκρίνει τις αρχικές προτιμήσεις για κρυπτογράφηση του client με αυτά που έστειλε ο server,
4. οι αρχικές προτιμήσεις για κρυπτογράφηση του server κατά την αρχική ανταλλαγή πληροφοριών (handshake),
5. αποκρυπτογράφηση,
6. το μήνυμα στην κανονική του μορφή.

Η προστασία ενός μηνύματος εφαρμόζεται με τρεις διαφορετικούς τρόπους:

- με υπογραφή,
- με κρυπτογράφηση και
- με ελέγχους πιστοποίησης.

Κάθε μήνυμα μπορεί να υπογραφεί, να κρυπτογραφηθεί ή οποιοσδήποτε συνδυασμός αυτών. Υποστηρίζονται αρκετές τεχνικές διαχείρισης κλειδιών όπως συμμετρικά μυστικά κλειδιά, ασύμμετρη διαχείριση και το σύστημα Key Distribution Center (KDC) του Kerberos.

Όταν υπογράφεται ψηφιακά, ένα κατάλληλο πιστοποιητικό μεταφέρεται με το μήνυμα ή ο αποστολέας μπορεί να αφήσει τον παραλήπτη να αποκτήσει το απαιτούμενο πιστοποιητικό από μόνος του.

Μέθοδοι κρυπτογράφησης είναι οι :

- in band κρυπτογράφηση,
- κρυπτογράφηση με ανταλλαγή κλειδιού,
- μέσω εφαρμογής Kerberos.

Το S/HTTP καθορίζει δύο μηχανισμούς ανταλλαγής κλειδιών:
(α) χρήση ασύμμετρης διαχείρισης κλειδιών (οι παράμετροι και το κλειδί του συμμετρικού κρυπτοσυστήματος κρυπτογραφούνται με την δημόσια κλείδα του παραλήπτη) και

(β) χρήση ενός προκαθορισμένου κλειδιού (τα ίδια στοιχεία κρυπτογραφούνται με κλειδί που έχει προαποφασιστεί νωρίτερα).

Οι έλεγχοι πιστοποίησης γίνονταν μέσω Message Authentication Codes (MACs) Χρησιμοποιεί το MAC του μηνύματος, το οποίο υπολογίζεται από hash αλγόριθμο σε συνδυασμό με ένα κοινό μυστικό κλειδί (π.χ. MD5). Αυτή η τεχνική δεν απαιτεί την χρήση ασύμμετρης διαχείρισης ούτε την χρήση κρυπτογράφησης. Η διαχείριση του MAC γίνεται είτε με απευθείας αποστολή είτε μέσω του Kerberos.

Οι Επικεφαλίδες του S/HTTP

Το πρωτόκολλο καθορίζει μία σειρά από επικεφαλίδες που πηγαίνουν στο πεδίο των επικεφαλίδων του S/HTTP μηνύματος. Υποχρεωτικές επικεφαλίδες είναι οι :

"Content-Privacy-Domain" : που υπάρχει για να παρέχει συμβατότητα με τα S/HTTP εφαρμογές που βασίζονται στο PEM (privacy enhanced mail). Όταν χρησιμοποιείται η επικεφαλίδα "Content-Privacy-Domain η προστασία του μηνύματος γίνεται με τους εξής τρόπους: με υπογραφή και με κρυπτογράφηση. Κάθε HTTP μήνυμα μπορεί να κρυπτογραφηθεί, να υπογραφεί ή και τα δύο. Το μήνυμα που υπογράφεται συνήθως συνοδεύεται από πιστοποιητικό ή από αλυσίδα πιστοποιητικών. Οι επικεφαλίδες "Content-Privacy-Domain: PGP" και "Content-Privacy-Domain: PEM" υποδηλώνουν εφαρμογή των κανόνων του PGP ή του PEM, αντίστοιχα.

"Content-Type": Υπό κανονικές συνθήκες, τα ενθυλακωμένα περιεχόμενα μετά την αφαίρεση όλων κρυπτογραφικών μέτρων ασφαλείας, θα είναι ένα HTTP μήνυμα. Σε αυτήν την περίπτωση η επικεφαλίδα θα είναι: Content-Type: application/http.

Υποστηριζόμενοι αλγόριθμοι (S-HTTP Δυνατότητες)

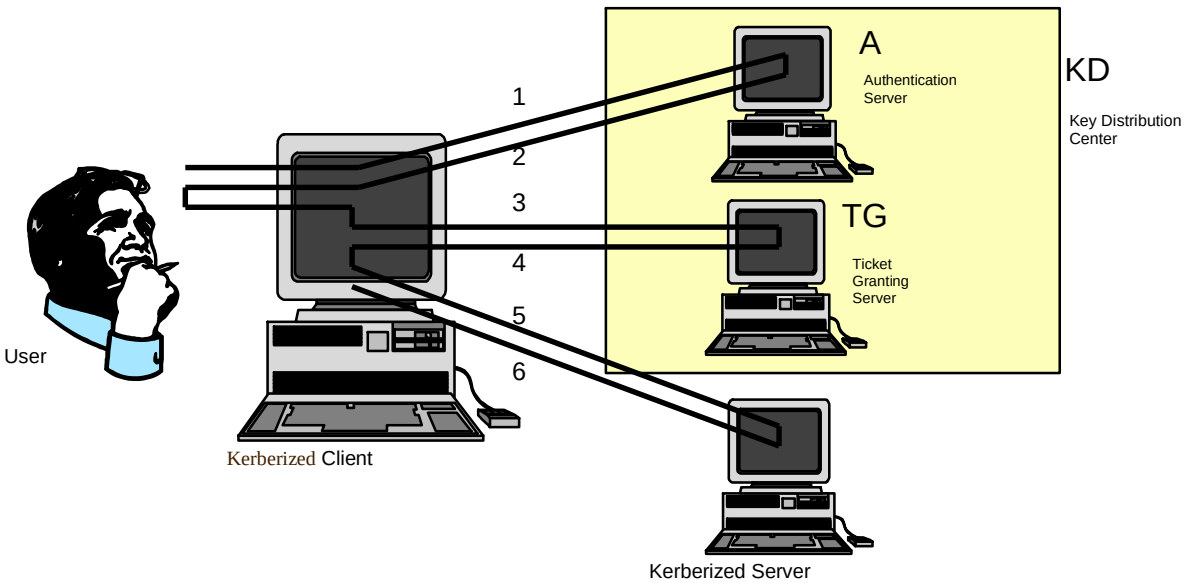
ΚΡΥΠΤΟΓΡΑΦΙΚΗ ΤΕΧΝΙΚΗ	**ΑΛΓΟΡΙΘΜΟΙ**
ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ	RSA DSS
ΠΑΡΑΓΩΓΗ MESSAGE DIGEST	MD2 MD5 SHS
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΠΕΡΙΕΧΟΜΕΝΩΝ	DES-CBC DES-EDE-CBC DES-EDE3-CBC DESX-CBC IDEA-CFB RC2-CBC RC4 CDMF-CBC
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΕΠΙΚΕΦΑΛΙΔΩΝ	DES-ECB DES-EDE-ECB DES-EDE3-ECB DESX-ECB IDEA-ECB RC2-ECB CDMF-ECB

Το s/http είναι μια σταθερή μέθοδος προστασίας, σε σχέση με το SSl, γιατί επιτρέπει την επαναδιαπραγμάτευση των μηχανισμών και των αλγορίθμων. Οι αλγόριθμοι του είναι πιο ανθεκτικοί στις επιθέσεις αλλά η μεταφορά των κλειδιών δεν γίνεται με αρκετή ασφάλεια και μπορούν εύκολα να πέσουν στα χέρια εισβολέων. Δυστυχώς όμως το s/http αδυνατεί στο να κρυπτογραφεί όλα τα μηνύματα που ανταλλάσσονται.

vi) Kerberos

Το Kerberos είναι ένα σύστημα αυθεντικοποίησης, κατά μήκος μη ασφαλών δικτύων, και διανομής κλειδιών για κατανεμημένα δίκτυα. Εάν απαιτηθεί από την εφαρμογή, μπορει επίσης να παρέχει ακεραιότητα (integrity) και κρυπτογράφηση (encryption). Το σύστημα Kerberos αναπτύχθηκε στο MIT (Massachusetts Institute of Technology) στα μέσα της δεκαετίας του 1980. Υπάρχουν σήμερα δύο κύριες εκδόσεις του, η 4 και η 5, οι οποίες για πρακτικούς λόγους είναι ασύμβατες. Οι πρωταρχικοί σχεδιαστές του Kerberos 4 ήταν ο Steve Miller και ο Clifford Neuman ενώ οι συνεχιστές του Kerberos 5 ήταν ο John Kohl και ο Clifford Neuman.

Το Kerberos δεν αντιγράφεται και παρέχει στον κάτοχό του συγκεκριμένα δικαιώματα για ένα αντικείμενο. Βασίζεται σε μία ΒΔ συμμετρικών κλειδιών και χρησιμοποιεί ένα κέντρο διανομής κλειδιών (Key Distribution Center – KDC) το οποίο είναι γνωστό με το όνομα ***Kerberos server***. Χρησιμοποιεί ισχυρή κρυπτογραφία και ο πελάτης μπορεί να αποδείξει την ταυτότητα του σε έναν εξυπηρετητή (και αντιστρόφως) σε μια ανασφαλή σύνδεση δικτύου. Οι περισσότερες σύγχρονες υλοποιήσεις του Kerberos χρησιμοποιούν ως κρυπτοσύστημα μυστικού κλειδιού το DES και ως μονόδρομες συναρτήσεις σύνοψης τις DES-CBC, MD4 και MD5. Το Kerberos είναι ελεύθερα διαθέσιμο από την MIT.



Η λειτουργία του Kerberos

Το σύστημα είναι οργανωμένο σε domains όπου σε κάθε domain υπάρχει ένας κεντρικός εξυπηρετητής αυθεντικοποίησης (Authentication Server - AS) που μοιράζεται ένα μυστικό κλειδί με κάθε συμμετέχοντα. Ο AS αυθεντικοποιεί τους χρήστες κατά τη σύνδεσή τους και τους παρέχει ένα εισιτήριο έκδοσης εισιτηρίων (Ticket Granting Ticket – TGT).

Το σύστημα λειτουργεί παρέχοντας στους συμμετέχοντες τόσο εισιτήρια (tickets) που μπορούν να χρησιμοποιήσουν για να αποδείξουν τη ταυτότητά τους, όσο και μυστικά κλειδιά για ασφαλείς επικοινωνίες μεταξύ τους. Συγκεκριμένα ένας χρήστης ή μια υπηρεσία (“principals”) χρεώνονται με ηλεκτρονικά “tickets” μετά από κατάλληλη επικοινωνία με το KDC. Τα “tickets” αυτά χρησιμοποιούνται για την αυθεντικοποίηση μεταξύ “principals”. Όλα τα “tickets” έχουν ημερομηνία/ώρα που περιορίζει τη χρονική περίοδο για την οποία το ticket είναι έγκυρο. Γι’ αυτό, τόσο οι clients όσο και ο server του Kerberos θα πρέπει να έχουν μία ασφαλή πηγή ημερομηνίας και ώρας και να είναι ικανοί να τηρούν το χρόνο με ακρίβεια. Γι’ αυτό απαιτούνται επίκαιρες συναλλαγές.

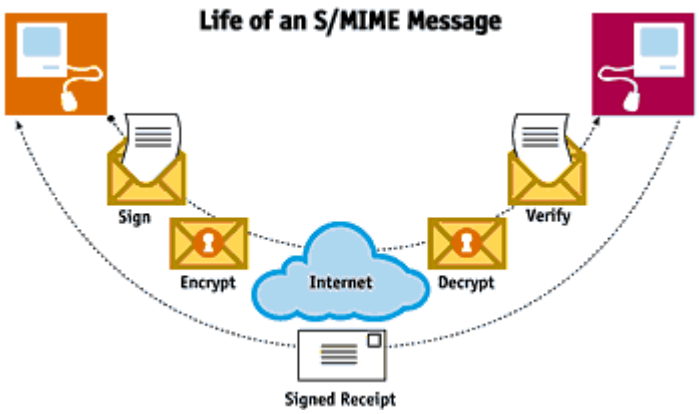
Το πρωτόκολλο Kerberos χρησιμοποιείται από τα Windows 2000 , Windows XP , Windows Vista και τα Apple's Mac OS X. . Συνοπτικά, το Kerberos είναι μια λύση για τα προβλήματα της ασφάλειας του δικτύου. Παρέχει τα εργαλεία της γνησιότητας και ισχυρή κρυπτογραφία πάνω από το δίκτυο για να εξασφαλιστούν τα συστήματα πληροφοριών.

vii) S/MIME (Secure MIME)

Για την προστασία από τυχόν υποκλοπές ηλεκτρονικών μηνυμάτων αλλά και για την καταπολέμηση της πλαστογραφίας δημιουργήθηκε το πρωτόκολλο S/MIME το οποίο είναι και φιλικό προς το χρήστη. Είναι σχεδιασμένο για να μπορέσει να ενώσει τα προϊόντα ηλεκτρονικού ταχυδρομείου. Ουσιαστικά είναι μια πιο εξειδικευμένη μορφή του πρωτοκόλλου MIME το οποίο το επέκτεινε, βασισμένο σε μία ομάδα κρυπτογραφικών τυποποιήσεων, το λεγόμενο Public Key Cryptography Standards (PKCS). Το πρωτόκολλο αυτό χρησιμοποιείται για τα προγράμματα του ηλεκτρονικού ταχυδρομείου όπου εφαρμόζει κρυπτογραφικές υπηρεσίες σε μηνύματα τα οποία έχουν αποσταλεί και επεξεργάζεται αυτά που έχουν ληφθεί.

Η 2η έκδοση του S/MIME προς το παρόν εμπεριέχεται σε αρκετά γνωστά προϊόντα, όπως τα Netscape Communicator, Microsoft Exchange, Lotus Domino και Novell GroupWise. Λογισμικά που έχουν δημιουργηθεί από εταιρείες, με το πρωτόκολλο S/MIME μπορούν να εξελίξουν προγράμματα όπου ένα κρυπτογραφημένο μήνυμα από το Χ πρόγραμμα να έχει την δυνατότητα να αποκρυπτογραφηθεί από το Υ πρόγραμμα.

Η 3η έκδοση του S/MIME που εξειδικεύεται στο Cryptographic Message Syntax (CMS)δηλ . το κρυπτογραφημένο συντακτικά μήνυμα έχει αναπτυχθεί από την ομάδα Internet Engineering Task Force (IETF). Το CMS θέτει μία τυποποιημένη σύνταξη που βοηθά στην ανταλλαγή των κρυπτογραφικών πληροφοριών που είναι συσχετισμένα με προστατευμένα περιεχόμενα. Το CMS παρέχει προστασία σε κάθε τύπο δεδομένων. Επίσης το CMS μπορεί να εφαρμοστεί και σε άλλα πρωτόκολλα όπως SSL, SET, X.400, HTTP και FTP. Η 3η έκδοση είναι συμβατή με την 2η και αυτό γιατί υπήρχαν προαιρετικά και νέα στοιχεία όταν προστέθηκαν, όπου απουσιάζουν οι επικεφαλίδες και έτσι διευκολύνει την συνεργασία των δύο εκδόσεων αλλά και επειδή στην 3η έκδοση επειδή το σύνολο των κρυπτογραφικών αλγορίθμων είναι μικρό, παρέχει την δυνατότητα της συνεργασίας μεταξύ διαφορετικών εφαρμογών.



viii) Πρόγραμμα PGP (Pretty Good Privacy)

Το έτος 1991 ο καθηγητής του MIT Philip Zimmermann δημιούργησε το πρόγραμμα PGP (Pretty Good Privacy), το οποίο είναι ένα από τα πιο διάσημα προγράμματα κρυπτογραφίας του ηλεκτρονικού ταχυδρομείου και αρχείων με γνωστούς και ασφαλείς αλγορίθμους. Επίσης παρέχει και δυνατότητες συμπίεσης όπου αυτό χρειάζεται για να ενισχυθεί η ασφάλεια (λιγότερος πλεονασμός επειδή

κάνει την κρυπτανάλυση πιο δύσκολη). Ο source code (πηγαίος κώδικάς) του είναι ανοικτός ως προς του χρήστες γεγονός που έβαλε σε σκέψεις τους ειδικούς επιστήμονες των κλάδων της πληροφορικής και κρυπτογράφησης να εξετάσουν το θέμα για τυχόν σφάλματα ή "κερκόπορτες" (back doors). Το πρόγραμμα αυτό κάνει χρήση της ασύμμετρης μεθόδου κρυπτογράφησης,όπου διαθέτει το δημόσιο και ιδιωτικό κλειδί για να διασφαλίσει εμπιστευτικότητα.Ακόμη χρησιμοποιεί ψηφιακές υπογραφές για έλεγχο της αυθεντικότητας της ταυτότητας του αποστολέα και για να έχει την εξασφάλιση της ακεραιότητας του μηνύματος όπου παρέχει υπηρεσίες μη-αποποίησης.

Έτσι μιλάμε για ένα πρόγραμμα που θεωρείται αξιόπιστο. Βέβαια για εφαρμογές ηλεκτρονικού εμπορίου (e-commerce) όπως και για εφαρμογές όπου απαιτούν ισχυρή ταυτοποίηση, το πρόγραμμα αυτό θα μπορούσε να θεωρηθεί ακατάλληλο. Αυτό γιατί οι αρχές των ΗΠΑ επικαλέστηκαν ότι με την ελεύθερη διανομή του προγράμματος υπήρχε κίνδυνος εξαγωγής προγραμμάτων κρυπτογράφησης που θα μπορούσε να μετατραπεί σε πανίσχυρο τρομοκρατικό όπλο, όπου οι εκάστοτε τρομοκράτες θα μπορούσαν να κάνουν ανταλλαγή ηλεκτρονικών μηνυμάτων με ύποπτο όπως και επικίνδυνο περιεχόμενο.

Αυτές βέβαια οι αντιρρήσεις της αμερικανικής κυβέρνησης έφεραν ως αποτέλεσμα να εκδιωχθεί ποινικά ο καθηγητής όπου δημιούργησε αυτό το πρωτόκολλο και να αλλάξουν τελικά αυτή την στάση οι αρχές των ΗΠΑ μετά από πίεση της βιομηχανίας πληροφορικής εν έτη 2000, διότι όπως ισχυριζόταν και ο κ. Philip Zimmermann «*είναι καλύτερο για την κοινωνία μας να διαθέτει ένα χρήσιμο εργαλείο προστασίας της ιδιωτικότητας και εκτός από το κυνήγι των τρομοκρατών, οι αρχές έχουν την υποχρέωση να προστατεύουν τις επικοινωνίες και τις συναλλαγές των απλών πολιτών».*

Για την χρησιμοποίηση προγράμματος PGP το πρώτο πράγμα που πρέπει να κάνει ο χρήστης είναι να δημιουργήσει ένα ζευγάρι κλειδιών δηλαδή τα λεγόμενα key pair. Μπορεί να επιλέξει ένα επίπεδο ασφάλειας για τα κλειδιά του από 1.024, 1.536, 2.048, 3.072 ή 4.096 bits. Όσο περισσότερα bits επιλέξει, τόσο πιο ασφαλή θα είναι τα κλειδιά που θα δημιουργήσει, αλλά η δημιουργία τους θα καθυστερήσει και θα είναι πολύ αργά και στη χρήση τους. Οι τιμές από 1.024 έως 2.048 bits είναι οι συνιστώμενες για τις περισσότερες εφαρμογές. Το δημόσιο κλειδί, ο χρήστης, το παρέχει σε όλους τους παραλήπτες με e-mail ή κάνοντας το δημόσιο στο Internet,

ενώ το ιδιωτικό κλειδί πρέπει να είναι ένα αυστηρά προσωπικό κλειδί γιατί όταν το μήνυμα κρυπτογραφηθεί με το δημόσιο κλειδί, ακολουθεί μια μονόδρομη διαδικασία. Έτσι με την κρυπτογράφηση του μηνύματος δεν υπάρχει δυνατότητα αποκρυπτογράφησης παρά μόνο με το ιδιωτικό κλειδί. Το πρόγραμμα PGP αποθηκεύει στο δίσκο, κρυπτογραφημένο το ιδιωτικό κλειδί, επειδή υπάρχει περίπτωση το δημόσιο και ιδιωτικό κλειδί να εμπεριέχουν μεγάλο όγκο αρχείων. Όποτε ο χρήστης που χρησιμοποιεί το πρόγραμμα, πρέπει να εισάγει την "passphrase" δηλαδή την φράση εισόδου, όπου έχει απομνημονεύσει διότι δεν αποθηκεύεται πουθενά.

Το πρόγραμμα PGP δίνει την δυνατότητα στους χρήστες του να διαθέτουν μία λίστα με τα δημόσια κλειδιά των άλλων χρηστών με τους οποίους επικοινωνούν και συναλλάσσονται(keyring). Η λίστα αυτή προστατεύεται από το ιδιωτικό κλειδί του χρήστη όπου γενικά ως πρόγραμμα το PGP διαθέτει μία εξαιρετικά ισχυρή λειτουργία για κρυπτογράφηση στο κείμενο που είναι υπογεγραμμένο από τον χρήστη. Έπειτα το PGP για την δημιουργία της υπογραφής θα χρησιμοποιήσει την αφομοίωση και το ιδιωτικό κλειδί.. Όταν ένα κλειδί προστίθεται στη λίστα, έχει την δυνατότητα να επικαλείται έναν από τους παρακάτω χαρακτηρισμούς:

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

Γενικά το πρόγραμμα PGP είναι χρήσιμο για εφαρμογές απλής και όχι ισχυρής ταυτοποίησης (strong authentication) που εκτελούνται από απλούς χρήστες και αποφεύγεται η χρήση του στο ηλεκτρονικό εμπόριο για ευνόητους λόγους. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Έτσι λοιπόν το PGP μπορεί να δημιουργήσει ηλεκτρονικές υπογραφές που ικανοποιούν την νομοθεσία για «προηγμένες» ηλεκτρονικές υπογραφές αλλά δεν έχει την δυνατότητα να δημιουργήσει αναγνωρισμένες ηλεκτρονικές υπογραφές επειδή δεν διαθέτουν αναγνωρισμένο πιστοποιητικό. Επειδή δεν αναλαμβάνεται ιδιαίτερη ευθύνη από τους πιστοποιούντες δεν μπορεί θεωρηθεί ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη όπως και δεν έχει αποδείξεις ή εγγυήσεις για την αληθινή ταυτότητα συναλλασσομένων.

Β) Εταιρείες που παρέχουν πιστοποιητικά

Για να προστατευθούν οι συναλλαγές μέσω του ιντερνέτ υπάρχουν κάποιες εταιρίες που παρέχουν τα παραπάνω πιστοποιητικά. Αυτές είναι:

- **INSTANTSSL COMODO**: παρέχει το SSL certificate στις παρακάτω εταιρείες HP, IBM, MICROSOFT, ORACLE, FUJITSU, BP, FOUR SEASONS HOTEL, BBC, CONVERSE, SHELL, WARNER BROS, TOSHIBA, GSK (GLAXO SMITH LINE) και πανεπιστήμια όπως UCLA, CAMBRIDGE και MICHIGAN.
- **DIGI-SIGN**: παρέχει SSL και DIGITAL SIGNATURES σε εταιρείες όπως CITIBANK (όχι στην Ελλάδα), VODAFONE και OSRAM (λάμπες).
- **VERISIGN**: παρέχει SSL στις εταιρείες CHANNEL 4, HYATT INTERNATIONAL, LIVE EARTH, MTV EUROPEAN, HOTMAIL και ORACLE.Θυγατρική της είναι και η THAWTE.
- **MILLERSMILES:** παρέχει anti-phising σε εταιρείες όπως η AMAZON.

VIII) ΝΟΜΟΘΕΣΙΑ ΣΤΗΝ ΕΛΛΑΔΑ ΚΑΙ ISO

Α) ΝΟΜΟΘΕΣΙΑ

Όπως αναφέραμε και παραπάνω μια ηλεκτρονική συναλλαγή χρειάζεται και την βοήθεια ατόμων εξουσιοδοτημένων από το κράτος. Γι αυτό και η κυβέρνηση ασχολήθηκε με το ηλεκτρονικό εμπόριο και ο Υπουργός Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης Καθηγητής κ. Προκόπης Παυλόπουλος υπέγραψε την Εγκύκλιο με θέμα: «Εφαρμογή και χρήση ψηφιακής υπογραφής και κρυπτογράφησης στη Δημόσια Διοίκηση».

Η εγκύκλιος εστάλη προς τη Βουλή των Ελλήνων, τις Διευθύνσεις Διοικητικού και τις Μονάδες Πληροφορικής όλων των Υπουργείων, των Αυτ. Γενικών Γραμματειών, των Περιφερειών και των Νομαρχιακών Αυτοδιοικήσεων, καθώς επίσης και σε όλους τους Δήμους της Χώρας, τις Ανεξάρτητες Αρχές και τα Κ.Ε.Π.

Κάποια σημαντικά στοιχεία της εγκυκλίου που πρέπει να αναφερθούν είναι ότι:

«… Για την εφαρμογή και χρήση των ψηφιακών υπογραφών η επικρατέστερη τεχνολογία η οποία παρέχει την απαραίτητη υποδομή φέρει την ονομασία **Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI)** και χρησιμοποιείται από το ΥΠ.ΕΣ.Δ.Δ.Α. μέσα από το έργο «**Εθνικό Δίκτυο Δημόσιας Διοίκησης – ΣΥΖΕΥΞΙΣ**», το οποίο βρίσκεται ήδη σε παραγωγική λειτουργία. Οι υπηρεσίες οι οποίες προσφέρονται από την εν λόγω υποδομή, δίνουν τη δυνατότητα στα στελέχη του Δημοσίου, με τη χρήση έξυπνων καρτών που θα τους διατεθούν, να υπογράφουν ψηφιακά τις μεταξύ τους ηλεκτρονικές επικοινωνίες και συναλλαγές. Η ψηφιακή αυτή υπογραφή, σύμφωνα με το Π.Δ. 150/2001 (ΦΕΚ 125/Α΄/2001), επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

Σημειώνεται, ότι ήδη προωθείται σε επίπεδο Ευρωπαϊκής Ένωσης (Ε.Ε), η υποχρεωτική χρήση ψηφιακής υπογραφής και ασφαλούς ηλεκτρονικής διακίνησης των πληροφοριών – εγγράφων, στις ηλεκτρονικές συναλλαγές των κρατών – μελών με τις υπηρεσίες της Ε.Ε.

Επίσης, με την ανάπτυξη και ολοκλήρωση του έργου **«Εθνική Κεντρική Διαδικτυακή Πύλη – ΕΡΜΗΣ»**, του οποίου η εκτέλεση αρχίζει σύντομα, προβλέπεται αντίστοιχη Υποδομή Δημόσιου Κλειδιού για τις ηλεκτρονικές συναλλαγές των πολιτών και των επιχειρήσεων με τις δημόσιες υπηρεσίες.

Η Υποδομή Δημόσιου Κλειδιού που έχει δημιουργηθεί βασίζεται σε μια ιεραρχικά κατανεμημένη δομή αρμοδιοτήτων. Ειδικότερα, η οργανωτική δομή και διάρθρωση του διοικητικού μηχανισμού για την υποστήριξη της λειτουργίας της Υποδομής Δημόσιου Κλειδιού που έχει δημιουργηθεί από το ΥΠ.ΕΣ.Δ.Δ.Α., έχει ως εξής :

1) Ως **«Αρχή Πιστοποίησης του Ελληνικού Δημοσίου» (ΑΠΕΔ)**, δηλαδή ως **«Πρωτεύουσα Αρχή Πιστοποίησης» (ΠΑΠ)** ορίστηκε, σύμφωνα με το άρθρο 20 του Ν. 3448/2006 (ΦΕΚ 57/Α΄/15-3-2006), έτσι όπως τροποποιήθηκε από το άρθρο

25 του Ν. 3536/2007 (ΦΕΚ 42/Α΄/23-2-2007), η **Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ**) της Γενικής Γραμματείας Δημόσιας Διοίκησης & Ηλεκτρονικής Διακυβέρνησης του ΥΠ.ΕΣ.Δ.Δ.Α..

Η ΑΠΕΔ είναι αρμόδια «…….για την πιστοποίηση, τον καθορισμό των κατευθύνσεων και το συντονισμό των άλλων δημόσιων υπηρεσιών ή φορέων του Δημόσιου Τομέα, οι οποίοι εκδίδουν ψηφιακά πιστοποιητικά για την παροχή υπηρεσιών από φορείς του Δημόσιου Τομέα …» (άρθρο 20 του ν. 3448/2006).

2) Ως **«Υποκείμενη Αρχή Πιστοποίησης» (ΥπΑΠ)** του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης ορίζεται το Τμήμα Επεξεργασίας και Διαρκούς Απογραφής της Διεύθυνσης Προγραμματισμού και Εφαρμογών της Υπηρεσίας Ανάπτυξης Πληροφορικής της Γενικής Γραμματείας Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης του ΥΠ.ΕΣ.Δ.Δ.Α..

Η ΥπΑΠ είναι αρμόδια για την έκδοση και την εν γένει διαχείριση των πιστοποιητικών των τελικών χρηστών, καθώς και για την εποπτεία και τον έλεγχο της ορθής και σύννομης λειτουργίας της υπηρεσίας PKI.

3) Ως **«Αρχή Εγγραφής» (ΑΕ)** του ΥΠ.ΕΣ.Δ.Δ.Α., ορίζεται ο Τομέας Υλοποίησης και Παραγωγικής Λειτουργίας Έργων και Συστημάτων της «Κοινωνίας της Πληροφορίας ΑΕ – ΚτΠ Α.Ε.».

Αποστολή της εν λόγω Αρχής Εγγραφής είναι η υποστήριξη των παρεχόμενων υπηρεσιών πιστοποίησης, όπως αυτές προβλέπονται στο σχετικό Κανονισμό Πιστοποίησης (ΚΠ). Ειδικότερα, η Αρχή Εγγραφής είναι αρμόδια για την ταυτοποίηση, αποδοχή ή απόρριψη Ηλεκτρονικών Εγγραφών για έκδοση πιστοποιητικών, καθώς και για την αποδοχή ή απόρριψη αιτημάτων ανάκλησης, ανάκτησης ή ανανέωσης πιστοποιητικών.

4) Ως «**Εντεταλμένα Γραφεία» (ΕΓ),** ορίζονται τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), σε ολόκληρη τη χώρα.

Τα Εντεταλμένα Γραφεία είναι υπεύθυνα για τη διεκπεραίωση και τις ενέργειες που σχετίζονται κυρίως με την ταυτοποίηση των στοιχείων και την παραλαβή των αιτήσεων των τελικών χρηστών (π.χ. δημοσίων υπαλλήλων) που αφορούν σε θέματα ψηφιακών πιστοποιητικών υπογραφής και κρυπτογράφησης, σύμφωνα και με τα προβλεπόμενα στο σχετικό ΚΠ.

Η υπηρεσία ασφαλούς επικοινωνίας και ηλεκτρονικών συναλλαγών προϋποθέτει ότι οι **Τελικοί Χρήστες** (φυσικό πρόσωπο για το οποίο εκδίδεται ένα ψηφιακό πιστοποιητικό κατόπιν αίτησής του) των εμπλεκόμενων φορέων διαθέτουν από δύο ψηφιακά πιστοποιητικά, ένα για ψηφιακή υπογραφή και ένα για κρυπτογράφηση. Τα ψηφιακά πιστοποιητικά (και τα σχετικά ζεύγη κλειδιών) δημιουργούνται από Ασφαλείς Διατάξεις, εκδίδονται ηλεκτρονικά από την ΥπΑΠ. και αποθηκεύονται με ασφάλεια στις Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής, όπως έξυπνες κάρτες, usb token, οι οποίες διατίθενται στους τελικούς χρήστες. Στο πρώτο στάδιο εφαρμογής της υπηρεσίας PKI χορηγούνται επίσης και οι απαραίτητοι αναγνώστες καρτών (card readers). Το φυσικό πρόσωπο που βασίζεται στα στοιχεία τα οποία περιέχονται σε ένα ψηφιακό πιστοποιητικό, το οποίο εκδίδεται σύμφωνα με τα προβλεπόμενα στον ΚΠ, ονομάζεται **Τρίτος Συμμετέχων (ΤΣ)**. …»

Β) Πρότυπα ISO

Ο ISO (International Organization for Standardization) είναι ο ευρύτερα αποδεκτός οργανισμός για την παραγωγή και καταχώρηση προτύπων. Ανάμεσα στα περίπου 13.000 πρότυπα που έχει παράγει, υπάρχουν αρκετά που σχετίζονται με την ασφάλεια των ΠΣ και κάποια από αυτά εξειδικεύονται στην παροχή υπηρεσιών ΕΤΟ (Έμπιστη Τρίτη Οντότητα).

i) Τεχνολογικά πρότυπα

- **ISO DIS 9735**: EDIFACT – Electronic Document Interchange For Administration, Commerce and Transport: Το πρότυπο EDIFACT ορίζει ένα συντακτικό μεταφοράς ηλεκτρονικών μηνυμάτων που ανταλλάσσονται σε ένα περιβάλλον ηλεκτρονικού εμπορίου. Το μεγαλύτερο τμήμα αυτού του προτύπου αναφέρεται στα θέματα ασφάλειας της ανταλλαγής ηλεκτρονικών μηνυμάτων και προτείνει μηχανισμούς χρήσης πιστοποιητικών και ψηφιακών υπογραφών. Το πρότυπο αυτό θα πρέπει να ληφθεί υπόψη για την υποστήριξη της τεχνολογικής διαλειτουργικότητας των ΕΤΟ που θα πρέπει να

έχουν τη δυνατότητα να διαχειριστούν ψηφιακά πιστοποιητικά διαφορετικών τύπων όπως είναι αυτά του EDIFACT, του προτύπου X.509 και του SPKI.

- **ISO/IEC 9796**: Σχήμα ψηφιακών υπογραφών που παρέχει ανάνηψη του μηνύματος: Το πρότυπο αυτό προσδιορίζει ένα σχήμα για την επιβεβαίωση του αποστολέα και την ακεραιότητα των δεδομένων, χρησιμοποιώντας ένα σύστημα που βασίζεται στη χρήση κρυπτογραφίας δημόσιου κλειδιού.

- **ISO/IEC 9798**: Αυθεντικοποίηση οντοτήτων: Το πρότυπο αυτό περιγράφει μια σειρά από μηχανισμούς που μπορούν να χρησιμοποιηθούν για την αυθεντικοποίηση οντοτήτων. Ορίζονται αλγόριθμοι αυθεντικοποίησης που στηρίζονται στη χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας. Η σημαντικότητα της αυθεντικοποίησης διαπιστώνεται σε κάθε λειτουργική μονάδα της ΕΤΟ.

- **ISO/IEC 11770**: Διαχείριση Κλειδιών: Σκοπός αυτού του προτύπου είναι να προσδιορίσει το πλαίσιο και τις ασφαλείς διαδικασίες που απαιτούνται για τη διαχείριση των κρυπτογραφικών κλειδιών και σχετίζεται με την ΕΤΟ που αναλαμβάνει το ρόλο του Κέντρου Διανομής Κλειδιών.

- **ISO/IEC 14888**: Ψηφιακές υπογραφές με επισύναψη: Ο σκοπός αυτού του προτύπου είναι να ορίσει ένα μηχανισμό για την παροχή ψηφιακών υπογραφών που μπορούν να χρησιμοποιηθούν για την υπογραφή μηνυμάτων αυθαίρετου μεγέθους. Μια ψηφιακή υπογραφή με επισύναψη αποτελείται από το μήνυμα και μια ακολουθία από bits που αποτελούν την υπογραφή του μηνύματος.

ii) Διαχειριστικά πρότυπα

- **ISO/IEC 13335**: Οδηγίες για τη διαχείριση ασφάλειας τεχνολογιών πληροφορικής: Η τεχνική αυτή αναφορά προσδιορίζει όλα τα θέματα εκείνα που σχετίζονται με τη διαχείριση ασφάλειας σε έναν οργανισμό, όπως η ΕΤΟ, η οποία χρησιμοποιεί ή καλείται να προστατέψει ΠΣ που χρήζουν ασφάλειας.

- **ISO-TR 13569**: Τραπεζικές και σχετιζόμενες οικονομικές υπηρεσίες, Οδηγίες για την Ασφάλεια Πληροφοριών: Το κείμενο αυτό, μεταξύ άλλων αναφέρεται στις απαιτήσεις που πρέπει να ικανοποιεί μία ΕΤΟ σε ένα περιβάλλον παροχής οικονομικών υπηρεσιών. Η αναφορά αυτή πραγματεύεται μια σειρά από θέματα που είναι ιδιαίτερα σημαντικά για την τραπεζική οικογένεια όπως η διασφάλιση εμπιστοσύνης, σχετικά νομικά θέματα και απαιτούμενες υπηρεσίες ΕΤΟ.

- **ISO/IEC 14516**: Οδηγίες για τη χρήση και διαχείριση των ΕΤΟ: Η τεχνική αυτή αναφορά παρέχει οδηγίες στους διαχειριστές υπηρεσιών ΕΤΟ σε θέματα διαχείρισης και οργάνωσης. Η αναφορά διερευνά τους ρόλους που αναπτύσσονται και τις σχέσεις μεταξύ τους εντός της ΕΤΟ, τους χρήστες και άλλες οντότητες που εμπλέκονται στην παροχή υπηρεσιών. Επίσης, παρουσιάζονται θέματα που σχετίζονται με την εφαρμογή της πολιτικής ασφάλειας, τις υπευθυνότητες μίας ΕΤΟ και τη διαλειτουργικότητά τους.

- **ISO/IEC 15408**: Κριτήρια αξιολόγησης της ασφάλειας τεχνολογιών πληροφορικής: Ο κύριος στόχος αυτού του προτύπου είναι η παροχή ενός συνόλου κριτηρίων που μπορούν να χρησιμοποιηθούν για την αξιολόγηση της ασφάλειας που προσφέρει ένα προϊόν τεχνολογίας πληροφορικής. Τα κριτήρια αυτά μπορούν να εφαρμοσθούν στις παρεχόμενες από τις ΕΤΟ υπηρεσίες, στα πλαίσια της αξιολόγησής τους. Το πρότυπο αυτό παρουσιάζει τα αποτελέσματα των εναρμονισμένων κριτηρίων αξιολόγησης ασφάλειας τεχνολογιών πληροφορικής (γνωστά και ως Common Criteria) έτσι όπως αυτά

προσδιορίζονται από οργανισμούς προτυποποίησης της Ευρώπης, του Καναδά και των ΗΠΑ.

- **ISO / IEC 27006** μέρος της διευρυνόμενης οικογένειας του ISO / IEC πρότυπα ειδικών μηχανισμών, την «ISO / IEC 27000 σειράς" είναι ένα πρότυπο ασφάλειας που δημοσιεύτηκε από το Διεθνή Οργανισμό Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC). Η έκδοση 2007 έχει τίτλο 'Τεχνολογία πληροφοριών - τεχνικές ασφάλειας - Απαιτήσεις για φορείς που παρέχουν υπηρεσίες ελέγχου και πιστοποίησης των συστημάτων διαχείρισης ασφάλειας πληροφοριών'. Παρέχει κατευθυντήριες γραμμές για τη διαπίστευση των οργανισμών που προσφέρουν την πιστοποίηση και την καταγραφή όσον αφορά κάποιους ειδικούς μηχανισμούς. Ουσιαστικά αντικαθιστά κατευθυντήριες γραμμές για τη διαπίστευση των φορέων πιστοποίησης λειτουργίας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Επομένως η ασφάλεια επιτυγχάνεται όταν ισχύουν όταν υπάρχουν:

- Ακεραιότητα των Περιουσιακών Στοιχείων. Δηλαδή το ηλεκτρονικό χρήμα δεν αλλοιώνεται ούτε ως προς την ποσότητα ούτε ως προς κάποιο άλλο χαρακτηριστικό του.
- Εμπιστευτικότητα των δεδομένων.
- Πιστοποίηση του ηλεκτρονικού χρήματος που μετακινείται μεταξύ των υποσυστημάτων και η πιστοποίηση των υποσυστημάτων που ανταλλάσσουν δεδομένα μεταξύ τους.
- Έλεγχος πρόσβασης στο σύστημα. (χρήση κωδικού)
- Δέσμευση και επιβεβαίωση της αξιοπιστίας των εκτελούμενων συναλλαγών. Κάθε συναλλαγή αφορά συγκεκριμένο ποσό ηλεκτρονικού χρήματος και συγκεκριμένα υποσυστήματα. Αν κάποιο από αυτά δεν μπορεί να καθοριστεί σαφώς, η συναλλαγή πρέπει να καθίσταται αδύνατη.
- Πραγματοποίηση ολοκληρωμένων συναλλαγών. Εφόσον προκύψει κάποιο πρόβλημα πριν την τελική επιβεβαίωση, η συναλλαγή πρέπει να ακυρώνεται εξ ολοκλήρου.

- Ορθή σειρά των συναλλαγών και των διαδικασιών που προβλέπονται για κάθε συναλλαγή. Αλλιώς μπορεί να προκληθούν ανεπιθύμητες επιπλοκές ή απρόβλεπτες συνέπειες.
- Εντοπισμός κάθε μη φυσιολογικής ενέργειας στο σύστημα, όπως η παράνομη πρόσβαση ή η προσπάθεια αλλοίωσης των δεδομένων.
- η χρήση εξελιγμένων πρωτοκόλλων κρυπτογράφησης για προστασία των πληροφοριών.
- Η ενημέρωση του λογισμικού ασφαλείας με τις τελευταίες εκδόσεις για την καταπολέμηση κάθε νέας απειλής.
- Η διαθεσιμότητα του συστήματος, δηλαδή η δυνατότητα χρήσης του ακόμα και σε περιόδους συντήρησης ή βλάβης.

Προκειμένου να επιτευχθούν αυτές οι παράμετροι ασφαλείας είναι απαραίτητη μια σειρά από τεχνικές και εργαλεία όπως οι αλγόριθμοι, τα πιστοποιητικά και τα πρωτόκολλα.

Βλέπουμε πως η ασφάλεια ενός συστήματος ηλεκτρονικών πληρωμών και ειδικότερα ηλεκτρονικού χρήματος δε στηρίζεται σε έναν μόνο τρόπο (δηλαδή ένα μόνο πρωτόκολλο) ούτε είναι κάτι απλό και εύκολα κατανοητό από τους απλούς χρήστες. Χρειάζονται γνώσεις και απαιτείται ο σωστός σχεδιασμός ολόκληρου του συστήματος και η σωστή διαχείριση των διαδικασιών ασφαλείας από εξουσιοδοτημένα άτομα. Χωρίς τη σωστή ασφάλεια τα συμφέροντα του εμπόρου και του καταναλωτή δεν μπορούν να εξυπηρετηθούν. Γι' αυτό πρέπει να είμαστε πάρα πολύ προσεχτικοί πριν κάνουμε οποιαδήποτε συναλλαγή και να ζητάμε την βοήθεια ατόμων εξουσιοδοτημένων από το κράτος.

Υπάρχουν όμως ακόμα ελλείψεις τις οποίες οι τράπεζες θα πρέπει να περιορίσουν για να γίνονται πιο εύκολα οι συναλλαγές. Η ανάπτυξη των ηλεκτρονικών καναλιών διανομής παρουσιάζει σημαντική καθυστέρηση και υπάρχουν τεράστια περιθώρια βελτίωσης της συγκεκριμένης αγοράς. Απαιτείται σημαντική εκπαίδευση του προσωπικού. Μόνο με τον συνδυασμό όλων αυτών θα επιτραπεί στις εν λόγω συναλλαγές να ανθίσουν!

ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

Μελλοντική διερεύνηση της διείσδυσης νέων ηλεκτρονικών μέσων στην σύγχρονη τραπεζική σε συνάρτηση με την εισαγωγή και χρήση νέων τεχνολογιών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Γ. Πάγκαλος & Ι. Μαυρίδης, «Ασφάλεια Πληροφοριακών συστημάτων και Δικτύων», εκδόσεις ΑΝΙΚΟΥΛΑ, σελ.178 – 190

- Εγκυκλοπαίδεια «Πάπυρος Λαρούς Μπριτάνικα», τόμος 61ος, εκδόσεις ΠΑΠΥΡΟΣ, σελ. 256 (Όρος Χρήμα).

- Εγκυκλοπαίδεια «Πάπυρος Λαρούς Μπριτάνικα», τόμος 36ος, εκδόσεις ΠΑΠΥΡΟΣ, σελ. 245 (Όρος Κρυπτολογία).

- Γ. Μπαμπινιώτη, «Λεξικό της Νέας Ελληνικής Γλώσσας», εκδόσεις ΚΕΝΤΡΟ ΛΕΞΙΚΟΛΟΓΙΑΣ, σελ.244 (Όρος Αποκρυπτογράφηση), σελ. 964 (Όρος Κρυπτογράφηση).

- Andrew S. Tanenbaum, «Σύγχρονα Λειτουργικά Συστήματα», εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ, σελ. 688 – 747 (κεφ. ΑΣΦΑΛΕΙΑ).

- «ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ» - Κ. Βλαχόπουλος (ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ)

- «ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ»- Α. ΜΑΛΛΕΡΟΥ (ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ)

- «ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΕΓΛΗΜΑΤΑ»- ΓΡ. ΛΑΖΟΣ (ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ)

- E-bay for dummies

- ΠΡΑΚΤΙΚΑ 3Ο ΚΑΙ 4Ο ΠΑΝΕΛΛΗΝΙΟΥ ΣΥΝΕΔΡΙΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΛΗΜΑΤΟΣ

ΣΕΛΙΔΕΣ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

- http://en.wikipedia.org/wiki/Pretty_Good_Privacy (πρόγραμμα PGP, SSH, ESP, SA, SSL, E-SIGNATURE)

- http://www.go-online.gr/ebusiness/specials (πρόγραμμα PGP)

- http://www.in.gr (Άρθρο «Ασφαλιστικά μέτρα», τεύχος RAM 137, ασφάλεια συναλλαγών, Ramnet A.E.)

- http://www.subject.com/crypto.html (Κρυπτογράφηση)

- http://www.physics4u.gr/news/2004/scnews1344.html (Κβαντική Κρυπτογράφηση)

- http://www.geocities.com/kzerzel/history.htm (Εισαγωγή στην κβαντική κρυπτογραφία, Ιστορική αναδρομή)

- http://en.wikipedia.org/wiki/History_of_cryptography (Η ιστορία της Κρυπτογραφίας)

- http://www.cypher.com.au/crypto_history.html (Η ιστορία της Κρυπτογραφίας)

- http://www.go-online.gr/ebusiness/specials/article.html?article_id=714 (Άρθρο «Η υποδομή δημοσίου κλειδιού και η κρυπτογράφηση στην πράξη», Η-επιχειρείν

- http://www.thelab.gr/forumdisplay (Η κρυπτογράφηση βοηθά στην προστασία των δεδομένων)

- http://www.dmst.aueb.gr/louridas/notes/dais/security/ar01s09.html (Κρυπτογράφηση)

- http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/basikesennoies.htm (Τι είναι S/MIME)

- http://www.digitalnews.gr/modules/mynews (Άρθρα «Ασφάλεια δεδομένων στο διαδίκτυο – μέθοδος DES – RSA»)

- http://www.ypan.gr/index_c_cms.htm (Υποδομή Δημοσίου Κλειδιού HARICA, Συχνές Ερωτήσεις & Απαντήσεις)

- http://www.tech-faq.com/lang/el/symmetric-asymmetric.shtml

(Τι είναι κρυπτογραφικοί αλγόριθμοι;)

- http://nemis.cti.gr/ebusiness/distance_course.htm#49 (Ασφάλεια συναλλαγών. SET)

- http://www.papaki.gr (ασφάλεια συναλλαγών)

- http://www.thezocalo.blogspot.com (ασφάλεια συναλλαγών)

- http://www.kapatel.gr (κρυπτογράφηση, πιστοποιητικά, πρωτόκολλα ασφάλειας)

- http://www.ted.unipi.gr (πρωτόκολλα ασφαλείας)

- http://www.teipir.gr (TCP, FTP, TELNET)

- http://www.noc.auth.gr (SFTP)

- http://www.asxetos.gr (ψηφιακά πιστοποιητικά)

- http://www.epmhs.gr (χρονική σφραγίδα)

- http://www.focusmag.gr (χρονική σφραγίδα)
- http://www.davidreilly.com (SET)
- http://www.isaca.org (SET)
- http://www.web.mit.edu (Kerberos)
- http://www.ftc.gov (e-signature)
- http://www.ypes.gr (νομοθεσία)
- http://www.sch.gr
- http://www.**spam**-uk.com
- http://www.**spam**.com
- http://www.spamlaws.com
- http://www.saferinternet.gr
- http://www.eexi.gr
- www.go-onlin**e**.gr
- https://www.**e**urobank.gr
- www.**e**mporiki.gr/
- www.**e**-**banking**.co.uk
- http://www.winbank.gr
- http://www.ydt.gr
- http://www.dart.gr

ΟΡΙΣΜΟΙ-ΥΠΟΣΗΜΕΙΩΣΕΙΣ

Ciphers: Είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα block μη κρυπτογραφημένου καθορισμένου μήκους κειμένου *(*plaintext*)*, σε block κρυπτογραφημένου του ίδιου μήκους κειμένου *(*ciphertext*)*.

Πιστοποιητικό ΕΤΟ: Είναι ένα ειδικό πιστοποιητικό ταυτότητας του οποίου ιδιοκτήτης είναι μία ΕΤΟ και εκδίδεται είτε από την ίδια την ΕΤΟ (self-signed) είτε από μία άλλη ΕΤΟ. Τυπικές επιτρεπόμενες χρήσεις για αυτό το πιστοποιητικό είναι η υπογραφή πιστοποιητικών, η υπογραφή λιστών ανακληθέντων πιστοποιητικών, η παραγωγή χρονοσφραγίδων και άλλων τεκμηρίων. Μία ΕΤΟ μπορεί να διαθέτει περισσότερα από ένα πιστοποιητικά για χρήση από διαφορετικές υπηρεσίες ή για διαφορετικούς σκοπούς.

Ιδιοκτήτης πιστοποιητικού (subject): Η οντότητα που είναι άρρηκτα συνδεδεμένη με το πιστοποιητικό ταυτότητας και έχει προσδιοριστεί ως κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί που περιέχεται στο πιστοποιητικό. Αναφέρεται και ως το *'υποκείμενο'* του πιστοποιητικού.

Χρήστης πιστοποιητικού (relying party): Η οντότητα που εμπιστεύεται την ακρίβεια της πληροφορίας που περιέχεται στο πιστοποιητικό και τη χρησιμοποιεί. Η τυπική χρήση ενός πιστοποιητικού είναι η επαλήθευση μιας ψηφιακής υπογραφής που προέρχεται από το υποκείμενο του πιστοποιητικού ή η αποστολή κρυπτογραφημένων δεδομένων προς το υποκείμενο.

Αρχή καταχώρησης (registration authority): Λαμβάνει την αίτηση και διαχειρίζεται τα στοιχεία επαλήθευσης της ταυτότητας μιας οντότητας που έχει ζητήσει έκδοση πιστοποιητικού. Αφού ολοκληρώσει αυτή την κρίσιμη διαδικασία, διαβιβάζει το αίτημα στην Αρχή πιστοποίησης για την έκδοση του πιστοποιητικού.

Αρχή πιστοποίησης (certification authority): Διαχειρίζεται τα ψηφιακά πιστοποιητικά, δηλαδή τα εκδίδει, τα αποθηκεύει, τα διανέμει και τα ανακαλεί. Λόγω

της κρισιμότητας των λειτουργιών αυτών, πολλές φορές ο όρος ‘Αρχή Πιστοποίησης’ χρησιμοποιείται στη θέση του όρου ‘Έμπιστη Τρίτη Οντότητα’. Ο βαθμός της φερεγγυότητας της ΕΤΟ και κατά συνέπεια ο βαθμός εμπιστοσύνης που δείχνει ένας χρήστης στα περιεχόμενα ενός πιστοποιητικού εξαρτάται από πλήθος παραγόντων. Μεταξύ άλλων, οι παράγοντες αυτοί περιλαμβάνουν: Την πρακτική που ακολουθείται από την Αρχή καταχώρησης για την αυθεντικοποίηση του αιτούντος. Την πολιτική λειτουργίας, τις διαδικασίες, τις εγκαταστάσεις και τους ελέγχους της Αρχής πιστοποίησης. Τις καταγραμμένες υποχρεώσεις του υποκειμένου (π.χ. προστασία του ιδιωτικού κλειδιού). Τις δημοσιευμένες δεσμεύσεις και νομικές υποχρεώσεις της Αρχής πιστοποίησης, όπως οι εγγυήσεις και οι περιορισμοί ευθυνών.

Μήνυμα (message): Χρησιμοποιείται με την ευρεία έννοια, η οποία μπορεί να περιλαμβάνει τα διακινούμενα δεδομένα στα πλαίσια της διεκπεραίωσης μίας συναλλαγής, την προσωπική αλληλογραφία και τη μεταφορά αρχείων.

Πρότυπο αυθεντικοποίησης Χ.509: Το πρότυπο αυτό δημιουργήθηκε από την ITU-T με σκοπό να ενσωματωθεί στις υπηρεσίες ευρετηρίου Χ.500 ένα πλαίσιο για την παροχή υπηρεσιών αυθεντικοποίησης. Αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων (καταλόγων), η οποία σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

Σύμφωνα με το πρότυπο, το ευρετήριο είναι η τοποθεσία όπου πρέπει να διατηρούνται όλες πληροφορίες που βοηθούν τους χρήστες να επικοινωνούν μεταξύ τους με ασφάλεια. Δύο τύποι αυθεντικοποίησης περιγράφονται στο πρότυπο [ITU01]:

- ˜ Αυθεντικοποίηση βασισμένη στη χρήση συνθηματικών (απλή αυθεντικοποίηση)
- ˜ Αυθεντικοποίηση βασισμένη στη χρήση διαπιστευτηρίων, δηλαδή πιστοποιητικών, που έχουν δημιουργηθεί με χρήση κρυπτογραφικών μεθόδων (ισχυρή αυθεντικοποίηση).

Το Χ.509 ασχολείται με δύο είδη πιστοποιητικών που σχετίζονται άμεσα με τις υπηρεσίες της ΕΤΟ: (1) Τα πιστοποιητικά ταυτότητας (identity certificates) που σχετίζονται με όλες σχεδόν τις υπηρεσίες της ΕΤΟ για αυθεντικοποίηση, ψηφιακές υπογραφές και κρυπτογράφηση και (2) τα πιστοποιητικά ιδιοτήτων (attribute certificates) που χρησιμοποιούνται για τη διαχείριση δικαιωμάτων προσπέλασης.

Αρκετά χρηματοπιστωτικά ιδρύματα χρησιμοποιούν το X.509 για το πρότυπο ασφαλών συναλλαγών SET (Secure Electronic Transactions). Χρησιμοποιείται επίσης σε φυλλομετρητές ιστοσελίδων (browsers), εξυπηρετητές (servers) και προγράμματα λογισμικού, για τη διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server/clients) κτλ., από πολλές γνωστές εταιρίες ανάπτυξης λογισμικού.

Ευρετήρια και Αρχεία (directories and repositories): Για την αποθήκευση και δημοσίευση των πιστοποιητικών και της κατάστασής τους, των ισχυόντων πολιτικών και πρακτικών, καθώς και άλλων τεκμηρίων που παρέχονται από τις υπηρεσίες της ΕΤΟ.

Πιστοποιητικό ταυτότητας (identity certificate): Αναφέρεται απλά ως ‘πιστοποιητικό’. Ο όρος αυτός αναφερόταν αρχικά σε ένα ψηφιακά υπογεγραμμένο κείμενο που περιέχει ένα όνομα και ένα δημόσιο κλειδί. Σήμερα ένα πιστοποιητικό συνδέει ένα δημόσιο κλειδί με ένα σύνολο πληροφοριών που προσδιορίζει πλήρως την ταυτότητα της οντότητας που κατέχει και χρησιμοποιεί το αντίστοιχο ιδιωτικό κλειδί. Ένα πιστοποιητικό μπορεί ακόμα να περιέχει πλήθος άλλων χαρακτηριστικών που σχετίζονται με τη χρήση του, όπως εκδίδουσα αρχή, επιτρεπόμενες χρήσεις, λήξη ισχύος, αλγόριθμους και μέγεθος κλειδιών.

Πιστοποιητικό ιδιοτήτων (attribute certificate): Αυτός ο τύπος πιστοποιητικού αντιστοιχίζει την ταυτότητα του ιδιοκτήτη του ή το πιστοποιητικό ταυτότητάς του σε ένα σύνολο από ιδιότητες, που απαιτείται να αναγνωρίζονται από διάφορες εφαρμογές, όπως η συμμετοχή σε ομάδες ή ρόλους και η παραχώρηση δικαιωμάτων χρήσης.

OSI : Το μοντέλο αναφοράς ανοικτής διασύνδεσης συστημάτων ή μοντέλο αναφοράς OSI είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για σχεδίαση επικοινωνιών και δικτυακών πρωτοκόλλων για υπολογιστές και είναι γνωστό ως μοντέλο των επτά επιπέδων.

TCP/TP: Είναι ένα σύνολο πρωτοκόλλων που αναπτύχθηκε ώστε να επιτρέπει στους υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο να μοιράζονται τα αγαθά του δικτύου.

FTP (file transfer protocol): Είναι το πρωτόκολλο μεταφοράς αρχείων που επιτρέπει στον χρήστη οποιουδήποτε υπολογιστή να πάρει (στείλει) αρχεία από (σε) έναν άλλο υπολογιστή. Ασφάλεια παρέχεται με την υποχρεωτική από τον χρήστη εισαγωγή του username και του password για τον άλλο υπολογιστή.

TELNET: Το πρωτόκολλο τερματικού επιτρέπει στον χρήστη την πρόσβαση σε οποιοδήποτε άλλο υπολογιστή του δικτυού. Το απομακρυσμένο σύστημα θα ζητήσει login name και password. Το telnet περιλαμβάνεται στο πρωτόκολλο TCP/IP.

ESP (encapsulating security payload): χρησιμοποιείται για να παρέχει τήρηση του απορρήτου, τα δεδομένα προέλευσης αυθεντικοποίησης και ακεραιότητα σύνδεσης.

SA (secure association): Θέσπιση κοινών πληροφοριών ασφαλείας μεταξύ δύο οντοτήτων του δικτύου για την υποστήριξη ασφαλούς επικοινωνίας.

ΕΤΟ (έμπιστη Τρίτη οντότητα)