Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ο ΡΟΛΟΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.**
Ονοματεπώνυμο Φοιτητή	**ΚΑΣΙΩΝΗ ΒΑΣΙΛΙΚΗ**
Πατρώνυμο	**ΠΑΝΑΓΙΩΤΗΣ**
Αριθμός Μητρώου	**ΜΠΠΛ / 07050**
Επιβλέπων	**ΣΙΝΑΝΙΩΤΗ ΑΡΙΣΤΕΑ / ΚΑΘΗΓΗΤΡΙΑ**

Ημερομηνία Παράδοσης: 26/4/2010 **Μήνας: ΑΠΡΙΛΙΟΣ** **Έτος: 2010**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο	Όνομα Επώνυμο	Όνομα Επώνυμο
Χρήστος Δουλιγέρης	Δημήτριος Βέργαδος	Αριστέα Σινανιώτη
Βαθμίδα	Βαθμίδα	Βαθμίδα
Καθηγητής	Λέκτωρ	Καθηγήτρια

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η ανάγκη για την προστασία των προσωπικών δεδομένων στη σημερινή εποχή από το διαδίκτυο είναι μεγάλη. Όπως διαπιστώνουμε η προστασία βασίζεται σε κανονισμούς που διέπουν την καλύτερη ασφάλεια. Η δομή του διαδικτύου στηρίζεται στο μοντέλο αρχιτεκτονικής του OSI το οποίο έχει 7 επίπεδα τα εξής: το επίπεδο μεταφοράς, το επίπεδο δικτύου, το επίπεδο εφαρμογών, το επίπεδο φυσικής σύνδεσης δεδομένων , το επίπεδο παρουσίασης και το φυσικό επίπεδο. Μέσω αυτού του μοντέλου στηρίζεται η δομή και η λειτουργία του διαδικτύου. Οι απειλές του υπολογιστικού συστήματος είναι πάρα πολλές όπως οι ιοί, η συνομιλία στο διαδίκτυο, το ηλεκτρονικό εμπόριο , οι έξυπνες κάρτες, είναι μερικές από τις αιτίες οι οποίες μπορούν να βλάψουν το υπολογιστικό σύστημα. Οι κανόνες οι οποίοι προστατεύουν τον υπολογιστή βασίζονται σε νομοθετικές διατάξεις για την προστασία των πνευματικών δικαιωμάτων. Η αρχή προστασίας προσωπικών δεδομένων στηρίζεται στο δικαίωμα των ανθρώπων να διαφυλάξουν τα προσωπικά τους δεδομένα στο διαδίκτυο.

Οι απειλές του διαδικτύου μπορούν να αποφευχθούν μέσω χρήση κάποιων μέτρων ασφαλείας όπως είναι η χρησιμοποίηση κάποιων firewall. Αυτά μπορεί να είναι είτε υλικό είτε κάποιο λογισμικό. Μέσω κάποιας συσκευής μπορεί να έχουμε πολύ καλή προστασία του υπολογιστή μας και η χρησιμοποίηση κάποιου λογισμικού προγράμματος μπορεί να καλύψει πλήρως την ασφάλεια του υπολογιστή όπως π.χ είναι το antivirus κ.α προγράμματα λογισμικού. Με αυτό τον τρόπο εξασφαλίζεται κάθε κίνδυνος υποκλοπής ή ελεύθερης διακίνησης των προσωπικών δεδομένων στο διαδίκτυο.

Σημαντική είναι και η χρήση κάποιων δρομολογητών και διαμορφωτών για την σωστή δρομολόγηση των δεδομένων μεταξύ των ηλεκτρονικών υπολογιστών στο διαδίκτυο. Η χρησιμοποίηση αυτών βοηθούν στη σωστή αποστολή των πακέτων (δεδομένων) μέσω του διαδικτύου.

Η χρήση των ψηφιακών υπογραφών μπορούν να διασφαλίσουν την γνησιότητα , την ακρίβεια και τη μη αλλοίωση του περιεχομένου ενός εγγράφου. Τα ψηφιακά πιστοποιητικά αποτελούνται από πανίσχυρα συστήματα απόκρυψης των προσωπικών δεδομένων όσων τα κατέχουν. Χρησιμοποιούνται επιπλέον κάποια πρωτόκολλα για να παρέχουν εμπιστευτικότητα και κάποιοι αλγόριθμοι όπως είναι ο αλγόριθμος DES.

ΕΙΣΑΓΩΓΗ

Το Internet εισβάλει με γρήγορους ρυθμούς στη ζωή μας και αλλάζει καθημερινά της συνήθειας μας ,τον τρόπο διασκέδασης, τον τρόπο επικοινωνίας και τον τρόπο εργασίας. Έχει γίνει πλέον απαραίτητο στοιχείο της καθημερινότητας μας. Το Internet δημιουργήθηκε για να κάνει τη ζωή μας πιο εύκολη, δηλαδή στο να μας βοηθά να μεταφέρουμε, να εντοπίζουμε, να αποθηκεύουμε πληροφορίες πιο γρήγορα και πιο ασφαλή. Ζούμε στην εποχή του Ιντερνέτ, στην εποχή των γρήγορων ταχυτήτων. Ξεχάστε όσα ξέρατε. Ο υπολογιστής που έχετε απέναντί σας δεν είναι πια ένα μαύρο κουτί, κατάλληλο μόνο για γραφή κειμένων, άντε και για αποστολή ηλεκτρονικών μηνυμάτων. Νέες δυνατότητες δημιουργούνται διαρκώς σε συνδυασμό με την επέκταση του Διαδικτύου. Φθηνές τηλεφωνικές κλήσεις, oline ενημέρωση, τεράστιες αγορές προϊόντων και ένα τεράστιο αριθμό επισκεπτών(πελατών).

Η εκρηκτική επέκταση του διαδικτύου, με τις 600 δισεκατομμύρια ιστοσελίδες (περίπου 100 για κάθε άνθρωπο!), δεν αποτελεί πια μια παρωνυχίδα των εξελίξεων, καθώς σε μεγάλο βαθμό τροποποιεί μια σειρά λειτουργίες και δραστηριότητές μας. Η χρήση του Ιντερνέτ θα ξεπεράσει τη χρήση τηλεόρασης και τον Ιούνιο του 2010 θα αποτελεί το πιο διαδεδομένο μέσο για πρώτη φορά στην Ευρώπη σύμφωνα με μελέτες, που έχουν γίνει.

Οι χρήστες παραβιασμένων συστημάτων αντιμετωπίζουν πολύ σοβαρούς κινδύνους, χωρίς να το γνωρίζουν τις περισσότερες φορές. Ένας επιτιθέμενος μπορεί να παρακολουθεί ότι πληκτρολογείτε στον υπολογιστή για να μάθει αριθμούς πιστωτικών καρτών και κωδικούς, να χρησιμοποιήσει το σύστημα για τη διακίνηση πορνογραφικού υλικού, να αποσπάσει ευαίσθητα δεδομένα, ακόμα και να πραγματοποιήσει επιθέσεις σε άλλα συστήματα μέσω αυτού, ώστε να σβήσουν τα ίχνη του.

Οι επιθέσεις στο διαδίκτυο αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων. Καθημερινά ανακοινώνονται καινούργιες αδυναμίες στο λογισμικό και νέοι τρόποι επίθεσης. Με δεδομένη την εξέλιξη αυτή, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που αυτά περιέχουν και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Όλες αυτές οι απειλές είναι σημαντικοί λόγοι για να αυξηθεί η ασφάλεια στο διαδίκτυο και μεταξύ των χρηστών του. Αυτό περιλαμβάνει τη βελτίωση της ασφάλειας των συστημάτων που συνδέονται με το διαδίκτυο και την ενημέρωση και εκπαίδευση των χρηστών για τις απειλές.

ΚΕΦΑΛΑΙΟ 1ο

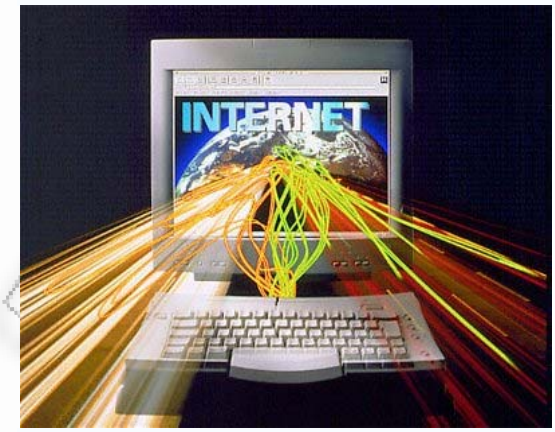
ΤΟ ΔΙΑΔΙΚΤΥΟ

Το καθημερινό όμως δίκτυο το οποίο μοιάζει περισσότερο με το Internet είναι... ο δρόμος. Έχετε μια διεύθυνση σ' αυτόν τον δρόμο. Και αυτός, και οι άλλοι δρόμοι στη γειτονιά σας ή στην πόλη σας, συνδέονται και τελικά οδηγούν σ' ένα μεγαλύτερο δρόμο ή σε λεωφόρο. Αυτή η λεωφόρος διατρέχει άλλες γειτονιές. Και αυτές οι λεωφόροι τελικά οδηγούν σε μεγαλύτερες λεωφόρους οι οποίες με τη σειρά τους οδηγούν σε πύλες: αεροδρόμια και λιμάνια τα οποία συνδέουν μεταξύ τους. Σκεφτείτε την κάθε γειτονιά ή πόλη σαν ένα δίκτυο από δρόμους. Εάν γνωρίζετε την διεύθυνση που θέλετε, μπορείτε να βρείτε έναν δρόμο που οδηγεί σε ένα άλλο κτίριο στον κόσμο. Σκεφτείτε, έπειτα, το σύνολο των δικτύων σαν ένα "δίκτυο των δικτύων". Αυτό είναι το Internet. Το Web, ο παγκόσμιος ιστός, είναι λοιπόν ένα τεράστιο δίκτυο μεταφοράς ενός απίστευτου όγκου αρχείων, κειμένων, δεδομένων, φωτογραφιών κτλ. Απλά φανταστείτε την εποχή όπου ο μοναδικός τρόπος αποστολής δεδομένων ήταν το ταχυδρομείο και ύστερα το φαξ. Όπως και σε ότι αφορά τη σύλληψη του Internet, η ιδιωτική επιχείρηση δεν έπαιξε μεγάλο ρόλο στη φάση της δημιουργίας του παγκόσμιου ιστού. Η ανάπτυξη του Web προήλθε μετά από έρευνα και ξεκίνησε το 1980 στο CERN (European Particle Physics Laboratory) από τον Tim Berners-Lee.

1.1 Η ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ

Σχετικά με τη χρήση του Διαδικτύου στην Ελλάδα, παρατηρείται σημαντική αύξηση του αριθμού των χρηστών (από 13% το 2001 σε 31% το 2007) ηλικίας 15 έως 65 ετών που κατέχουν προσωπικό Η/Υ. Αντίστοιχα, παρατηρείται αύξηση των ωρών χρήσης του Διαδικτύου που φτάνουν κατά μέσω όρο τις 8,6 ανά εβδομάδα. Η υπηρεσία που χρησιμοποιείται περισσότερο είναι το ηλεκτρονικό ταχυδρομείο (e-mail) αλλά και η ενημέρωση (νέα, καιρός, αθλητικά) αποτελεί από τους κυριότερους λόγους χρήσης του Διαδικτύου.

Αντίθετα, η αναζήτηση για προϊόντα και υπηρεσίες ακολουθεί πτωτική πορεία από το 2002. Ιδιαίτερα χαμηλή παραμένει η χρήση του Διαδικτύου για αγορά προϊόντων και υπηρεσιών. Περίπου 18% των χρηστών προχώρησε σε κάποια αγορά κατά το 2006 ωστόσο το ποσοστό αυτό ανέρχεται μόλις στο 4,5% του γενικού πληθυσμού. Παρόλα αυτά, οι αγορές πραγματοποιήθηκαν κυρίως από ελληνικούς ιστοχώρους (sites) (41%) έναντι των ξένων (35%). Οι χρήστες που αγοράζουν μέσω του Διαδικτύου συνήθως δεν επισκέπτονται τα αντίστοιχα καταστήματα, ενώ οι κυριότεροι λόγοι αγοράς είναι η προσιτή τιμή και η καλή εξυπηρέτηση. Τέλος, αξιοσημείωτο είναι το γεγονός ότι σε ποσοστό πάνω από 60% οι χρήστες θεωρούν ότι ο κίνδυνος διαρροής προσωπικών δεδομένων κατά τη χρήση πιστωτικής κάρτας στις ηλεκτρονικές αγορές είναι μεγάλος ή πολύ μεγάλος.



1.2 ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ Η ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

Το δικαίωμα των Ευρωπαίων πολιτών για ελεύθερη πρόσβαση στο Διαδίκτυο κατοχυρώνεται στο άρθρο 11 του Χάρτη των Θεμελίων Δικαιωμάτων της Ευρωπαϊκής Ένωσης περί ελευθερίας της έκφρασης και της ενημέρωσης. Πρόσφατα στο Ευρωπαϊκό Κοινοβούλιο ψηφίστηκε τροπολογία σύμφωνα με την οποία «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς να προηγηθεί δικαστική απόφαση... εκτός από περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών και στις οποίες η απόφαση δύναται να είναι αντίστοιχη». Ακόμη όμως και με την εν λόγω τροπολογία η πρόσβαση στο Διαδίκτυο θα μπορεί να απαγορευτεί με σχετικές δικαστικές αποφάσεις που θα επιβάλλει η εκάστοτε εθνική νομοθεσία στο όνομα της απειλής της ασφάλειας. Συγκεκριμένα, η τροπολογία αναφέρει επίσης «…η πρόσβαση στο Διαδίκτυο δεν μπορεί να περιοριστεί χωρίς να προηγηθεί δικαστική απόφαση. Εξαιρούνται οι περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών.» Χαρακτηριστικό παράδειγμα αποτελεί η Βρετανία, στην οποία οι πάροχοι απαγόρευσαν την πρόσβαση σε μια λίστα ιστοσελίδων στην οποία μέχρι τώρα βρίσκονταν σελίδες παιδικής πορνογραφίας, όμως πρόσφατα προστέθηκαν και άλλες, όπως αυτή που αφορά το χάκινγκ (hacking). Στους χρήστες που θα επιχειρούν να εισέλθουν σε κάποια από αυτές τις σελίδες θα απαγορεύεται η είσοδος, ενώ τα ηλεκτρονικά τους ίχνη θα καταγράφονται. Έτσι, παρά την εν λόγω τροπολογία, εξακολουθεί να μην λαμβάνεται υπ' όψη ότι το αδιάσειστο δικαίωμα της πρόσβασης των πολιτών στο Διαδίκτυο αποτελεί προαπαιτούμενο για την προάσπιση και άλλων θεμελιωδών δικαιωμάτων όπως η γνώση, η παιδεία η ελευθερία έκφρασης και πολιτικής δράσης.

Είναι σημαντικό, επίσης, να κατανοηθεί πως οι χρήστες του Διαδικτύου δεν είναι πελάτες αλλά πολίτες και ως τέτοιοι θα πρέπει να λογίζονται σε θέματα που αφορούν αφενός την υποδομή του διαδικτύου και αφετέρου το δικαίωμα πρόσβασης σε αυτό. Σχετικά με την υποδομή οφείλει η εκάστοτε εθνική αρχή να μεριμνά για την επέκταση του δικτύου, ακόμα και σε περιοχές που η ιδιωτική πρωτοβουλία αρνείται να προβεί στην απαιτούμενη επένδυση, όταν τη θεωρεί οικονομικά ασύμφορη. Έτσι θα διασφαλιστεί το δικαίωμα των πολιτών για ενημέρωση και ελευθερία έκφρασης. Όσον αφορά την πρόσβαση πρέπει να κατοχυρώνεται το δικαίωμα των πολιτών για ελεύθερη και ισότιμη πρόσβαση όπως αναφέρθηκε και με τα παραπάνω.

1.3 Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το Internet υιοθετεί το μοντέλο client/server (πελάτη/διακομιστή) όσον αφορά στην παράδοση των πληροφοριών. Βάσει του μοντέλου αυτού ένας client υπολογιστής συνδέεται σε έναν server υπολογιστή στον οποίο υπάρχουν οι πληροφορίες και φυσικά ο client εξαρτάται από τον server για να παραλάβει τις πληροφορίες.

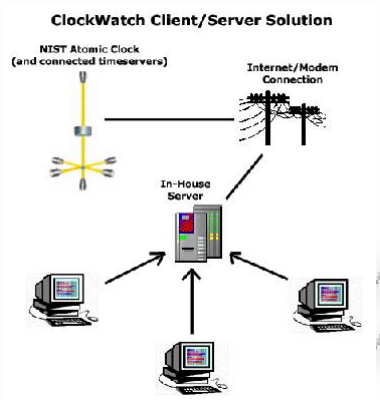
Πρακτικά ο client ζητά τις υπηρεσίες του μεγαλύτερου υπολογιστή. Οι υπηρεσίες αυτές μπορούν να αφορούν στην εύρεση πληροφοριών και την αποστολή τους στον client, όπως γίνεται στην περίπτωση ερωτήσεων σε μία βάση δεδομένων του Web. Αλλα παραδείγματα τέτοιων υπηρεσιών είναι η παράδοση Web σελίδων και η διαχείριση του εισερχόμενου και εξερχόμενου ταχυδρομείου. Οποτε χρησιμοποιείτε το Internet, είστε συνδεδεμένος σε έναν server και ζητάτε τη χρήση των υπολογιστικών του πόρων..

Στη συνηθισμένη περίπτωση ο client είναι ο τοπικός προσωπικός υπολογιστής και ο server (γνωστός επίσης και ως host) είναι ένας πολύ ισχυρότερος υπολογιστής που φιλοξενεί τα δεδομένα. Οι υπολογιστές αυτοί μπορεί να είναι διαφόρων ειδών: πανίσχυρα PCs με Windows, Macintoshes καθώς και ένα ευρύ φάσμα συστημάτων με λειτουργικό σύστημα Unix. Η σύνδεση στον server πραγματοποιείται μέσω ενός LAN, μίας τηλεφωνικής γραμμής ή ενός δικτύου ευρείας περιοχής (WAN) το οποίο βασίζεται στο TCP/IP. Ενας βασικός λόγος υιοθέτησης ενός δικτύου client/server είναι η δυνατότητα που παρέχει σε πολλούς χρήστες να χρησιμοποιούν ταυτόχρονα την ίδια εφαρμογή και τα αρχεία που βρίσκονται αποθηκευμένα στον server.

Στην περίπτωση του World Wide Web, client είναι ουσιαστικά ο browser του προσωπικού υπολογιστή σας και server είναι ο host υπολογιστής που βρίσκεται κάπου στο Internet. Τυπικά, ο browser στέλνει στον server μία αίτηση για μια καθορισμένη Web σελίδα.

Ο server επεξεργάζεται την αίτηση και στέλνει μία απάντηση στον browser (επίσης, πιο συχνά με τη μορφή μιας Web σελίδας). Η σύνδεση μεταξύ του client και του server διατηρείται μόνο κατά τη διάρκεια της πραγματικής ανταλλαγής πληροφοριών. Συνεπώς, αφού ολοκληρωθεί η μεταφορά της Web σελίδας από τον host υπολογιστή, διακόπτεται η HTTP σύνδεση μεταξύ του συστήματος και του client (HTTP αντιστοιχεί στο Hypertext Transfer Protocol, δηλαδή στο πρωτόκολλο που χρησιμοποιείται στον World Wide Web).

Ακόμη και όταν κλείσει η HTTP σύνδεση, ο ISP διατηρεί την TCP/IP σύνδεση στο Internet. Το μοντέλο client/server επιτρέπει στο επιτραπέζιο PC να τρέχει τον browser και να αναζητά πληροφορίες στο Internet αλλά και να έχει πρόσβαση στους host servers του Internet για την εκτέλεση λειτουργιών αναζήτησης και ανάκλησης πληροφοριών. Ουσιαστικά αυτή η αρχιτεκτονική επιτρέπει στον Web να θεωρείται ως ένα αποθηκευτικό μέσο και βάση δεδομένων απεριόριστης χωρητικότητας κατανεμημένα μεταξύ χιλιάδων υπολογιστών, οι οποίοι είναι προσβάσιμοι από οποιοδήποτε ανεξάρτητο PC.



Στο επίπεδο της φυσικής πρόσβασης (network access) ανήκουν τα πρωτόκολλα LAN όπως Ethernet, Token Ring, FDDI και πρωτόκολλα WAN όπως X.25, Frame Relay, SLIP, PPP που επιτρέπουν την φυσική διασύνδεση, την πρόσβαση στο μέσο και τον έλεγχο της ζεύξης.

- Στο επίπεδο δικτύου (network) χρησιμοποιείται το πρωτόκολλο IP, του οποίου τα πακέτα δρομολογούνται με ειδικές συσκευές, τους δρομολογητές (routers).
- Στο επίπεδο μεταφορά (transport) χρησιμοποιείται το πρωτόκολλο TCP και δευτερευόντως το UDP.
- Στο επίπεδο εφαρμογών (application) ανήκουν μεταξύ άλλων και τα πρωτόκολλα FTP, Telnet, SMTP, HTTP για την παροχή διάφορων υπηρεσιών όπως την μεταφορά αρχείων, την πρόσβαση σε υπολογιστές, ηλεκτρονικό ταχυδρομείο και το Web.

1.4 Η ΤΕΧΝΟΛΟΓΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το Διαδίκτυο ή Ίντερνετ (Internet) είναι ένα επικοινωνιακό δίκτυο ηλεκτρονικών υπολογιστών, που επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου υπολογιστή. Η τεχνολογία του είναι κυρίως βασισμένη στην διασύνδεση επιμέρους δικτύων ανά τον κόσμο και

πολυάριθμα τεχνολογικά πρωτόκολλα, με κύριο το TCP/IP. Ο αντίστοιχος αγγλικός όρος internet προκύπτει από τη σύνθεση λέξεων inter-network. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη μορφή του, με τους όρους Διαδίκτυο, Ιντερνέτ ή Ίντερνετ (με κεφαλαίο το αρχικό γράμμα) περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του. Το Διαδίκτυο χρησιμοποιεί μεταγωγή πακέτων (packet switching) και τη στοίβα πρωτοκόλλων TCP/IP.

Σήμερα, ο όρος Διαδίκτυο κατέληξε να αναφέρεται στο παγκόσμιο αυτό δίκτυο. Για να ξεχωρίζει, το παγκόσμιο αυτό δίκτυο γράφεται με κεφαλαίο το αρχικό "Δ". Η τεχνική της διασύνδεσης δικτύων μέσω μεταγωγής πακέτων και της στοίβας πρωτοκόλλων TCP/IP ονομάζεται Διαδικτύωση.

ΚΕΦΑΛΑΙΟ 2ο

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Η πιο γνωστή αρχιτεκτονική τα τελευταία είκοσι χρόνια – κυρίως σε εφαρμογές βάσεων δεδομένων – είναι αυτή του πελάτη-εξυπηρετητή (client-server). Σε αυτή την αρχιτεκτονική, ο πελάτης στέλνει ένα αίτημα (request) για δεδομένα στον εξυπηρετητή και αυτός επιστρέφει την απάντηση (response), την οποία επεξεργάζεται ο πελάτης και εμφανίζει στο χρήστη τα αποτελέσματα. Το πρόβλημα με αυτή την προσέγγιση είναι ότι η εμφάνιση των δεδομένων και η επεξεργασία τους γίνεται από το ίδιο πρόγραμμα, τον πελάτη. Αν υπάρχουν πολλαπλά κανάλια διάχυσης της πληροφορίας ή συχνή αλλαγή στη μορφή παρουσίασης, τοτε θα πρέπει να αλλάζει κάθε φορά η client εφαρμογή. Τα τελευταία χρόνια με την εμφάνιση του διαδικτύου, έχει επικρατήσει σε εφαρμογές web η αρχιτεκτονική τριών επιπέδων (3-tier architecture) η οποία τοποθετεί σε διαφορετικά εννοιολογικά επίπεδα τη λογική του προγράμματος που επεξεργάζεται τα δεδομένα (application logic) από τον τρόπο και μέσο που γίνεται η παρουσίαση (presentation).

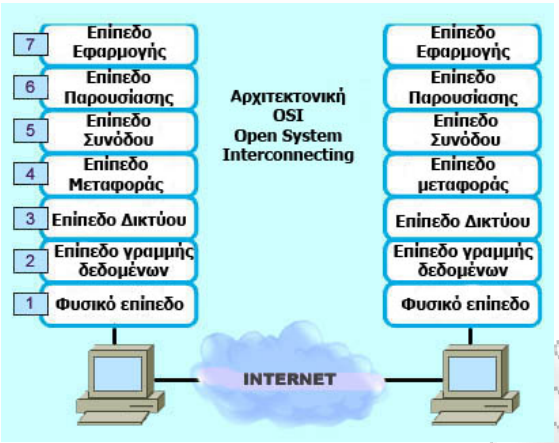
2.1 ΤΟ ΜΟΝΤΕΛΟ OSI

Το μοντέλο OSI υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατώτερού του στη στοίβα επιπέδου, ενω στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδό του. Μία συγκεκριμένη υλοποίηση του μοντέλου, με καθορισμένα πρωτόκολλα για κάθε επίπεδο, ονομάζεται στοίβα πρωτοκόλλων ή απλά στοίβα. Το κάθε πρωτόκολλο υλοποιείται είτε σε υλικό είτε σε λογισμικό. Συνήθως τα κατώτερα επίπεδα υλοποιούνται στο υλικό ενώ τα ανώτερα σε λογισμικό.

Το μοντέλο OSI είναι στενά συσχετισμένο με τον κλάδο της επιστήμης υπολογιστών και τη δικτύωση υπολογιστών. Το βασικό χαρακτηριστικό του είναι η διασύνδεση μεταξύ των επιπέδων, η οποία υπαγορεύει τις προδιαγραφές της αλληλεπίδρασής τους. Αυτό σημαίνει ότι ένα επίπεδο υλοποιημένο με κάποιο συγκεκριμένο πρωτόκολλο μπορεί να συνεργαστεί με το γειτονικό του στη στοίβα επίπεδο, το οποίο υλοποιείται με κάποιο άλλο πρωτόκολλο, υπό την προϋπόθεση ότι οι προδιαγραφές του καθενός έχουν δημοσιευθεί και έχουν γίνει αντιληπτές σωστά. Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (Requests for Comments) και αποτελούν πρότυπα του Διεθνούς Οργανισμού Τυποποίησης ISO.

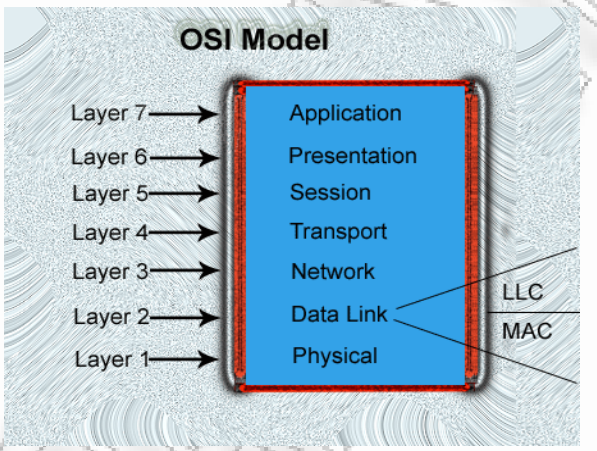
Συνήθως τα επίπεδα είναι αυστηρά διαχωρισμένα μεταξύ τους: αξιοποιούν τις υπηρεσίες του κατώτερου επιπέδου τους και προσφέρουν υπηρεσίες στο ανώτερό τους, αλλά

το καθένα δεν παρεμβαίνει στις λειτουργίες του άλλου· πιθανόν να μη γνωρίζει καν γι' αυτές. Αυτός ο λογικός διαχωρισμός των επιπέδων διευκολύνει πολύ τη μελέτη της συμπεριφοράς των πρωτοκόλλων και επιτρέπει τη σχεδίαση πολύπλοκων και αξιόπιστων στοιβών πρωτοκόλλων. Ορισμένες φορές όμως αυτή η αρχή ανεξαρτησίας των επιπέδων παραβιάζεται, για λόγους βελτιστοποίησης της απόδοσης ή αύξησης της λειτουργικότητας, με πρωτόκολλα διαφορετικών επιπέδων να συγχωνεύονται ή να παρεμβαίνουν το ένα στη λειτουργία του άλλου.



Σχήμα 1

Στο 1 σχήμα φαίνεται η διασύνδεση των δυο ηλεκτρονικών υπολογιστών μέσω της αρχιτεκτονικής osi και στο 2 σχήμα μας δείχνει τα 7 επίπεδα του osi.



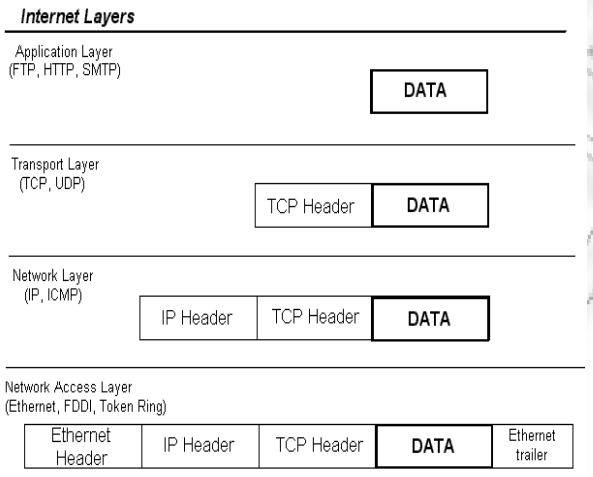
Σχήμα 2

2.2 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΠΡΟΣΒΑΣΗΣ

Το φυσικό επίπεδο ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές της επικοινωνίας. Σ' αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. Συσκευές φυσικού επιπέδου είναι οι διανεμητές (αγγλ. hub), οι επαναλήπτες (αγγλ. repeater), οι κάρτες δικτύου (αγγλ. card), οι προσαρμοστές (αγγλ. adaptor) διαύλου (αγγλ. bus). Οι κυριότερες λειτουργίες και υπηρεσίες του φυσικού επιπέδου είναι:

- Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας επικοινωνιακής συσκευής.
- Συμμετοχή σε διαδικασίες όπου οι επικοινωνιακές συσκευές εξυπηρετούν αποτελεσματικά πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σε οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να φθάσουν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.

Οι παράλληλοι δίαυλοι SCSI λειτουργούν στο επίπεδο αυτό. Επίσης τα επίπεδα 1 και 2 αφορούν οι προδιαγραφές των πρωτοκόλλων Ethernet, Token Ring, FDDI (αγγλ. Fiber Distributed Data Interface, Διασύνδεση Κατανεμημένων Δεδομένων με Οπτικές Ίνες) και IEEE 802.11.



2.3 ΤΑ ΕΠΙΠΕΔΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

1) Το επίπεδο φυσικής πρόσβασης.

Σε αυτό το επίπεδο ανήκουν οι εκάστοτε δικτυακές τεχνολογίες όπως Ethernet, FDDI και Token Ring. Το επίπεδο ασχολείται με την μετάδοση των bit μέσω διάφορων μέσων και αναλυτικότερα με τα ηλεκτρικά, μηχανικά και λειτουργικά χαρακτηριστικά των διασυνδέσεων. Επίσης ασχολείται με τον τρόπο που γίνεται η πρόσβαση στο φυσικό μέσον και καθορίζει τους κανόνες επικοινωνίας στο τοπικό δίκτυο.

2) Το επίπεδο δικτύου (IP PROTOCOL)

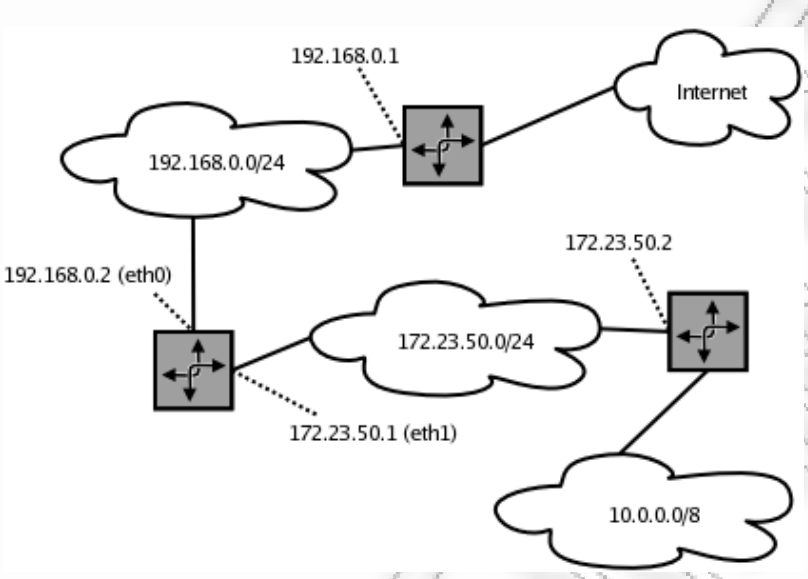
Η μετάδοση στο IP (Internet Protocol) γίνεται με την τεχνική των datagrams. Το κάθε datagram (πακέτο) φθάνει στον παραλήπτη διασχίζοντας ένα η περισσότερα διασυνδεόμενα IP δίκτυα, χωρίς να εξαρτάται από άλλα προηγούμενα ή επόμενα πακέτα.

Το IP, σαν πρωτόκολλο του τρίτου επιπέδου, δεν ασχολείται με τις φυσικές συνδέσεις ή τον έλεγχο των ενδιάμεσων ζεύξεων μεταξύ των κόμβων του δικτύου. Αυτά είναι αρμοδιότητα των χαμηλότερων επιπέδων. Στην ουσία ασχολείται με την διευθυνσιοδότητη, τον τεμαχισμό και την επανασυγκόληση των πακέτων. Το πρωτόκολλο IP δεν είναι αξιόπιστης μεταφοράς (reliable transfer) καθώς δεν εξασφαλίζει την σίγουρη παράδοση των πακέτων με τεχνικές επανεκπομπής και έλεγχο ροής. Επιπλέον είναι connectionless γιατί δεν απαιτεί την αποκατάσταση σύνδεσης μεταξύ των δύο σημείων πριν την ανταλλαγή δεδομένων. Τα IP πακέτα μπορεί να ακολουθήσουν διαφορετικές διαδρομές και να φθάσουν με λανθασμένη σειρά στον αποδέκτη. Προβλήματα σαν αυτό αναλαμβάνουν να διορθώσουν το πρωτόκολλο TCP του ανωτέρου επιπέδου.

Δρομολόγηση

Τα IP πακέτα διασχίζουν το Διαδίκτυο από δρομολογητή σε δρομολογητή με κατεύθυνση τον τελικό αποδέκτη. Κάθε δρομολογητής διατηρεί πίνακες δρομολόγησης βάσει των οποίων το κάθε πακέτο αποστέλλεται στον επόμενο δρομολογητή που θα αναλάβει να το προωθήσει προς τον αποδέκτη του. Ο καθορισμός του επόμενου δρομολογητή γίνεται με την ανάγνωση της IP διευθύνσεως του παραλήπτη. Ανάλογα με το δίκτυο στο οποίο βρίσκεται ο παραλήπτης, επιλέγεται από τον πίνακα δρομολόγησης διαδεχόμενος router.

Όταν ένα πακέτο φθάσει σε ένα δρομολογητή αποθηκεύεται προσωρινά σε μία ουρά (queue). Τα IP πακέτα επεξεργάζονται με την σειρά άφιξης τους. Κατά την επεξεργασίας τους, διαβάζεται η διεύθυνση του τελικού παραλήπτη. Εάν υπάρχει μποτιλιάρισμα στο δίκτυο, τότε η ουρά των πακέτων μέσα στον δρομολογητή μπορεί να γίνει μεγάλη, αυξάνοντας έτσι τις καθυστερήσεις μετάδοσης. Σε περίπτωση που η ουρά γίνει τόσο μεγάλη που να ξεπερνά τις χωρητικές δυνατότητες του δρομολογητή, τα πακέτα απορρίπτονται και χάνονται.



Διευθυνσιοδότηση

Καθ' ότι το Διαδίκτυο είναι μια εικονική κατασκευή που εφαρμόζεται λογισμικά, οι σχεδιαστές του είναι ελεύθεροι να διαλέξουν σχήμα διευθυνσιοδότησης που να μην σχετίζεται με κανένα υπάρχον δικτυακό υλικό. Το IP λειτουργεί με βάσει ένα νέο σετ διευθύνσεων που είναι ανεξάρτητο από τις υποκείμενες δικτυακές διευθύνσεις των υπολογιστών. Οι νέες αυτές διευθύνσεις καλούνται Internet Addresses ή IP διευθύνσεις.

Οι IP διευθύνσεις είναι φτιαγμένες έτσι ώστε να διευκολύνουν την δρομολόγηση. Κάθε IP πακέτο περιέχει την διεύθυνση του αποστολέα και του παραλήπτη, κάθε μια από τις οποίες έχει μήκος 32 bits. Μια IP διεύθυνση αποτελείται από δύο μέρη: το netid και το hostid. Το netid προσδιορίζει το δίκτυο στο οποίο βρίσκεται ο υπολογιστής, ενώ το hostid προσδιορίζει τον υπολογιστή. Ανάλογα με το μήκος της διευθύνσεως που αφιερώνεται σε κάθε τμήμα αυτής, οι διευθύνσεις διακρίνονται σε τρεις κλάσεις δικτύων:

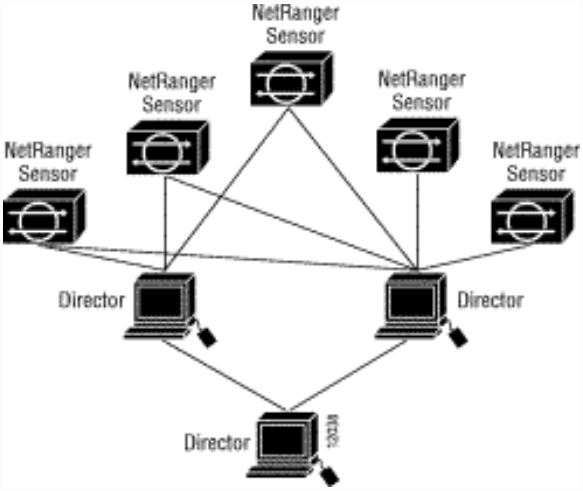
Κλάση Α: 8 bit διεύθυνση δικτύου / 24 bit διεύθυνση υπολογιστή

Κλάση Β: 16 bit διεύθυνση δικτύου / 16 bit διεύθυνση υπολογιστή

Κλάση Γ: 24 bit διεύθυνση δικτύου / 8 bit διεύθυνση υπολογιστή

Επειδή οι IP διευθύνσεις κωδικοποιούν ένα δίκτυο αλλά και έναν υπολογιστή σε αυτό το δίκτυο, δεν καθορίζουν έναν συγκεκριμένο υπολογιστή, αλλά μία σύνδεση σε ένα δίκτυο.

Στην πράξη η απομνημόνευση των 32 bits είναι εξαιρετικά δύσκολη. Γι' αυτό έχει επινοηθεί η αναπαράσταση της διεύθυνσης με την χρήση δεκαδικών αριθμών. Η διεύθυνση διαχωρίζεται με τελείες σε τέσσερα πεδία των οκτώ bit. Κάθε πεδίο μετατρέπεται στο ισοδύναμο δεκαδικό αριθμό, όπως φαίνεται στο παρακάτω σχήμα.



Internet Control Message Protocol (ICMP)

Ένα άλλο πρωτόκολλο αυτού του επιπέδου είναι το Internet Control Message Protocol (ICMP). Το ICMP δρα βοηθητικά, παράγοντας και διαχειρίζοντας μηνύματα λάθους για το πακέτο πρωτοκόλλων TCP/IP. Επιτρέπει στους δρομολογητές να επιστρέφουν μηνύματα λάθους σε άλλους δρομολογητές ή υπολογιστές. Για παράδειγμα, εάν ζητηθεί η σύνδεση με υπολογιστή που δεν υπάρχει ή δεν είναι διαθέσιμος προς το παρών, το ICMP σε κάποιον router θα επιστρέψει στον αποστολέα του αρχικού μηνύματος ένα μήνυμα με περιεχόμενο "host unreachable". Επιπλέον, το ICMP μπορεί να χρησιμοποιηθεί για την συλλογή πληροφοριών για ένα δίκτυο και για σκοπούς debugging. Περαιτέρω και πιο αναλυτικές λεπτομέρειες για το ICMP υπάρχουν στο RFC 792.

2.4 ΤΟ ΕΠΙΠΕΔΟ ΜΕΤΑΦΟΡΑΣ

Το επίπεδο μεταφοράς διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν αξιόπιστη και μεταφορά ο ένα άκρο της επικοινωνίας στο άλλο. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (αγγλ. flow control), κατάτμηση και τμηματοποίηση (αγγλ. segmentation / desegmentation), καθώς και έλεγχο σφαλμάτων (αγγλ. error control). Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά. Τα διάφορα πρωτόκολλα μορφοποιούν διαφορετικά τα εκπεμπόμενα πακέτα πληροφοριών, αλλά τα προς αποστολή δεδομένα παραλαμβάνονται αρχικά από τα ανώτερα επίπεδα.

Το συνηθέστερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP(αγγλ. Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης). Άλλα πρωτόκολλα μεταφοράς είναι τα UDP (αγγλ. User Datagram Protocol, πρωτόκολλο για ασυνδεσμική αποστολή δεδομένων, SCTP (αγγλ. Stream Control Transmission Protocol, πρωτόκολλο ελέγχου της ροής μετάδοσης), κλπ.

Το TCP (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς) είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το IP protocol (πρωτόκολλο IP). Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP (port 25), το παλαιότερο (και μη-ασφαλές) Telnet (port 23), το FTP και πιο σημαντικό το

HTTP (port 80), γνωστό ως υπηρεσίες World Wide Web (WWW - Παγκόσμιος Ιστός). Το TCP χρησιμοποιείται σχεδόν παντού, για αμφίδρομη επικοινωνία μέσω δικτύου.

Το πρωτόκολλο User Datagram Protocol (UDP) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι Universal Datagram Protocol. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών. Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Αντιθέτως, το πρωτόκολλο TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία.

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές. Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα παιχνίδια που παίζονται ζωντανά μέσω του Διαδικτύου.

2.5 ΤΟ ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΩΝ

Το επίπεδο εφαρμογών παρέχει στον χρήστη έναν τρόπο να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου κλπ. Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν τα Telnet, FTP, SMTP και http.

Το ηλεκτρονικό ταχυδρομείο (αγγλικά e-mail, email ή mail προφέρεται "ιμέιλ" ή "μέιλ" αντίστοιχα) είναι μια μέθοδος συγγραφής, αποστολής, λήψης και αποθήκευσης μηνυμάτων με χρήση ηλεκτρονικών συστημάτων τηλεπικοινωνιών. Γενικά ο όρος "ηλεκτρονικό ταχυδρομείο" αναφέρεται στο σύστημα ηλεκτρονικού ταχυδρομείου του Διαδικτύου που χρησιμοποιεί το Simple Mail Transfer Protocol πρωτόκολλο, σε δικτυακά συστήματα που βασίζονται σε άλλα πρωτόκολλα μεταφοράς μηνυμάτων, αλλά και σε διάφορα συστήματα μηνυμάτων σε μικρά δίκτυα, υπερυπολογιστές, κλπ που επιτρέπουν στους χρήστες τους να στέλνουν μηνύματα μεταξύ τους για την υποστήριξη ομαδικής συνεργασίας. Τα συστήματα σε τοπικά δίκτυα ή σε δίκτυα intranet είναι πιθανόν να βασίζονται σε ιδιωτικά πρωτόκολλα, που υποστηρίζονται από το συγκεκριμένο σύστημα, ή να είναι τα ίδια πρωτόκολλα που χρησιμοποιούνται στα δημόσια δίκτυα. Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται συχνά για τη μεταφορά ανεπιθύμητων μηνυμάτων σε μεγάλο όγκο (σπάμ (spam)), αλλά υπάρχουν προγράμματα που μπορούν να "φιλτράρουν" και να σταματήσουν ή να σβήσουν αυτόματα τα περισσότερα από αυτά.

Ο User Agent (UA) είναι το πρόγραμμα client στον υπολογιστή του χρήστη που αναλαμβάνει την διαχείριση και ανάκτηση του ταχυδρομείου. Με την βοήθεια αυτού του προγράμματος ο χρήστης γράφει τα μηνύματα του, τα στέλνει, παραλαμβάνει άλλα μηνύματα και τα διαβάζει. Ο Mail Transfer Agent (MTA) παραλαμβάνει τα μηνύματα από τον UA και τα προωθεί στον επόμενο MTA μέχρι να βρεθεί ο MTA που έχει άμεση σύνδεση με τον υπολογιστή του χρήστη. Ο τελευταίος MTA επικοινωνεί με τον UA του παραλήπτη για την παράδοση των μηνυμάτων. Το σύνολο των MTA καλείται Message Transfer System (MTS).

Η επικοινωνία από MTA σε MTA γίνεται με χρήση του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol, ενώ η επικοινωνία του UA με τον MTA γίνεται με χρήση των πρωτοκόλλων POP (Post Office Protocol) και IMAP (Internet Message Access Protocol). Τα ίδια τα μηνύματα συντάσσονται με βάσει το πρωτόκολλο MIME (Multipurpose Internet Mail Extensions) ή με το RFC822.Το παραπάνω σύστημα παράδοσης του ηλεκτρονικού ταχυδρομείου επιτρέπει το ηλεκτρονικό ταχυδρομικό του χρήστη να βρίσκεται σε κάποιον server και έτσι δεν είναι απαραίτητο να είναι εν λειτουργία ο υπολογιστή του αποδέκτη κατά την αποστολή του μηνύματος. Ο αποδέκτης θα παραλάβει τα μηνύματα του όταν ανοίξει τον υπολογιστή του και συνδεθεί με τον server (MTA).

Το File Transfer Protocol (FTP), (ελληνικά: Πρωτόκολλο Μεταφοράς Αρχείων) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet). Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.ο.κ. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα.

Το Simple Mail Transfer Protocol (SMTP) έχει καθιερωθεί για την μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο. Επίσημα περιγράφεται στα έγγραφα RFC821 και RFC1123. Το πρωτόκολλο που χρησιμοποιείται σήμερα αποτελεί επέκταση του αρχικού προτύπου και περιγράφεται στο έγγραφο RFC 2821.

Το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, HTTP) είναι η κύρια μέθοδος που χρησιμοποιούν τα πρωτόκολλα του Παγκοσμίου Ιστού για να μεταφέρουν δεδομένα ανάμεσα σε έναν διακομιστή (server) και ένα πελάτη (client).Η ανάπτυξη του HTTP έγινε υπό την εποπτεία του World Wide Web Consortium και του Internet Engineering Task Force (IETF).Το HTTP είναι ο συνήθης για τη διεκπαιρέωση αιτήσεων/απαντήσεων μεταξύ ενός υπολογιστή πελάτη (client) και ενός εξυπηρέτη (server). Πελάτης ονομάζεται ο τελικός χρήστης, και ο εξυπηρέτης είναι η εκάστοτε ιστοσελίδα.

ΚΕΦΑΛΑΙΟ 3ο

ΟΙ ΚΑΝΟΝΕΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η ραγδαία ανάπτυξη της τεχνολογίας της πληροφορικής δεν άφησε ανεπηρέαστο κανέναν τομέα της οικονομίας και της κοινωνίας , στη σύγχρονη εποχή αντιθέτως δε, έχει επιφέρει πλήθος αλλαγές στην εργασία, στις συναλλαγές, την εκπαίδευση και σε πλήθος άλλους τομείς. Παράλληλα όμως οι αυξημένες χάρη στην τεχνολογία δυνατότητες συλλογής, επεξεργασίας και ποικίλης χρήσης πληροφοριών που αφορούν το άτομο συνεπάγονται κινδύνους για επεμβάσεις στην ιδιωτική ζωή του ατόμου. Αυτή ακριβώς , η ανησυχία από τους κινδύνους που διατρέχει η ιδιωτική ζωή του σύγχρονου ανθρώπου ενόψει των αυξημένων δυνατοτήτων της τεχνολογίας της πληροφορικής γέννησε και την προβληματική για την προστασία των προσωπικών δεδομένων. Για την αντιμετώπιση των προβλημάτων που ανακύπτουν από τη χρήση της πληροφορικής θεσπίστηκαν ειδικές νομικές ρυθμίσεις, καθώς συνειδητοποιήθηκε ότι οι γενικές διατάξεις για την προστασία της προσωπικότητας, όπως είναι η διάταξη του άρθρου 57 στο ελληνικό δίκαιο δεν επαρκούν. Στην Ελλάδα, νομοθεσία για την προστασία προσωπικών δεδομένων θεσπίστηκε με αφορμή την ανάγκη της εναρμόνισης με την κοινοτική οδηγία 95/46/ΕΟΚ. Ειδικότερα, ψηφίστηκε ο νόμος 2472/1997, με τον οποίο ρυθμίζονται οι προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι οποίες αποτείνουν στην προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ο νόμος αυτός ο οποίος τροποποιήθηκε , αποτελεί τη γενική νομοθεσία για την προστασία των προσωπικών δεδομένων, ενώ ειδική νομοθεσία υφίσταται στον τομέα των τηλεπικοινωνιών νόμος 3471/2006.

3.1ΟΡΙΣΜΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ως "δεδομένα προσωπικού χαρακτήρα" προσδιορίζονται "όλες οι πληροφορίες που αφορούν ένα φυσικό πρόσωπο, του οποίου ή ταυτότητα είναι γνωστή ή μπορεί να προσδιοριστεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική." (Οδηγία 95/46, άρθρο 2 α). Τα είδη των προσωπικών δεδομένων είναι τα εξής: Δεδομένα που χρησιμοποιούνται για τον προσδιορισμό της ταυτότητας του προσώπου: όνομα, αριθμός της κοινωνικής ασφάλισης, αριθμός του δελτίου ταυτότητας, αριθμός πελάτη. Ως στοιχεία δηλωτικά της ταυτότητας γίνονται αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (κωδικός αναγνώρισης ή πρόσβασης, PIN κ.α.)._Οι προσωπικές πληροφορίες μπορεί να αφορούν τις σχέσεις ενός προσώπου προς πρόσωπα ή τις σχέσεις προς πράγματα: περιουσιακή κατάσταση, επαγγελματική και οικονομική δραστηριότητα, οικογενειακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις (συνήθειες του ελεύθερου χρόνου, συμμετοχή και δραστηριοποίηση σε ενώσεις, καταναλωτική συμπεριφορά) καθώς και τις σχέσεις και καταστάσεις ιδιωτικού και δημοσίου δικαίου (ιδιοκτησία, συμβατικές σχέσεις, διοικητικές άδειες κλπ.). Ως δικαίωμα προστασίας προσωπικών δεδομένων νοείται το δικαίωμα κάθε ανθρώπου να μην καθίσταται πληροφοριακό αντικείμενο και να (συν)προσδιορίζει ο ίδιος, ποιες πληροφορίες που τον αφορούν θα καταστούν γνωστές στο περιβάλλον. Το δικαίωμα της προστασίας προσωπικών δεδομένων, όπως τείνει να παγιωθεί στον ευρωπαϊκό τουλάχιστον νομικό πολιτισμό, έχει μία πολύπλοκη δομή: Αποτελείται από ένα σύνολο κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων αλλά και από ρυθμίσεις σχετικές με διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων των προσώπων.

3.2 Η ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Σύσταση - αποστολή - νομική φύση

1. Συνιστάται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Αρχή), με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.
2. Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή, και εξυπηρετείται από δική της γραμματεία. Η Αρχή δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής απολαύουν προσωπικής και λειτουργικής ανεξαρτησίας. Η Αρχή υπάγεται στον Υπουργό Δικαιοσύνης και εδρεύει στην Αθήνα.
3. Οι απαιτούμενες πιστώσεις για τη λειτουργία της Αρχής εγγράφονται σε ειδικό φορέα, που ενσωματώνεται στον ετήσιο Προϋπολογισμό του Υπουργείου Δικαιοσύνης. Διατάκτης της δαπάνης είναι ο Πρόεδρος ή ο αναπληρωτής του.

Συγκρότηση της Αρχής

1. Η Αρχή συγκροτείται από έναν δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω, ως Πρόεδρο, και έξι μέλη ως εξής:
   (Α) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο του δικαίου.
   (Β) Έναν καθηγητή ή αναπληρωτή καθηγητή ΑΕΙ σε γνωστικό αντικείμενο της πληροφορικής.
   (Γ) Έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι.
   (Δ) Τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα.

   Ο δικαστικός λειτουργός - Πρόεδρος και οι καθηγητές - μέλη μπορεί να είναι εν ενεργεία ή μη.

"Στα μέλη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επιτρέπεται η άσκηση καθηκόντων μέλους διδακτικού προσωπικού Α.Ε.Ι. με καθεστώς πλήρους ή μερικής απασχόλησης.»

2. Ο Πρόεδρος της Αρχής είναι πλήρους και αποκλειστικής απασχόλησης και διορίζεται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργικού Συμβουλίου, ύστερα από εισήγηση του Υπουργού Δικαιοσύνης. Εάν για τη θέση του Προέδρου επιλεγεί εν ενεργεία δικαστικός λειτουργός, απαιτείται απόφαση του οικείου Ανώτατου Δικαστικού Συμβουλίου. Με την ίδια διαδικασία επιλέγεται και διορίζεται ο αναπληρωτής του Προέδρου.

3. Τα μέλη της Αρχής διορίζονται με την εξής διαδικασία: ο Υπουργός Δικαιοσύνης υποβάλλει στον Πρόεδρο της Βουλής πρόταση για το διορισμό των έξι τακτικών μελών της Αρχής και των ισάριθμων αναπληρωτών τους. Η πρόταση περιλαμβάνει διπλάσιο αριθμό υποψηφίων. Ο Πρόεδρος της Βουλής διαβιβάζει την πρόταση στην Επιτροπή Θεσμών και Διαφάνειας, η οποία διατυπώνει γνώμη. Τα τακτικά μέλη της Αρχής και οι αντίστοιχοι αναπληρωτές τους επιλέγονται από τη Διάσκεψη των Προέδρων. Οι επιλεγέντες διορίζονται με προεδρικό διάταγμα, που εκδίδεται με πρόταση του Υπουργού Δικαιοσύνης και δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως.

(Οι παράγραφοι 2 και 3 καταργήθηκαν σύμφωνα με την παρ. 9 του άρθρου 5 του ν. 3051/2002 και ισχύουν οι γενικές διατάξεις του ως άνω νόμου)

4. Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με θητεία. Η θητεία τους είναι τετραετής και μπορεί να ανανεωθεί μία μόνο φορά. Κανείς δεν μπορεί να υπηρετήσει συνολικά περισσότερο από οκτώ (8) χρόνια. Η σύνθεση των έξι μελών της Αρχής ανανεώνεται κατά το ήμισυ ανά διετία.

Κατά την πρώτη εφαρμογή του παρόντος η θητεία των έξι (6) μελών της Αρχής είναι τετραετής. Μετά τη δεύτερη συγκρότηση της Αρχής γίνεται κλήρωση μεταξύ των έξι τακτικών μελών της, ώστε τρία να έχουν τετραετή θητεία και τρία διετή.

5. Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με ισάριθμους αναπληρωτές, οι οποίοι πρέπει να διαθέτουν τις αυτές ιδιότητες και προσόντα. Οι αναπληρωτές του Προέδρου και των μελών μετέχουν στις συνεδριάσεις της Αρχής μόνο σε περίπτωση προσωρινής απουσίας ή κωλύματος του αντίστοιχου τακτικού. Με απόφασή του ο Πρόεδρος της Αρχής αναθέτει ειδικά καθήκοντα στους αναπληρωτές. «Οπότε οι τελευταίοι μετέχουν στη συνεδρίαση με ψήφο ανεξάρτητα από την παράλληλη παρουσία του τακτικού μέλους». Η θητεία του κάθε αναπληρωτή είναι ίση με τη θητεία του αντίστοιχου τακτικού.

3.3 Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

"Κάθε πολίτης πρέπει να είναι σε θέση να γνωρίζει κάθε στιγμή ποιος, πού, πότε, πώς και γιατί επεξεργάζεται τα προσωπικά του στοιχεία".

Στην Ελλάδα έχει ιδρυθεί και λειτουργεί από το Νοέμβριο του 1997 ως ανεξάρτητη διοικητική υπηρεσία η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με βάση το Νόμο 2472/97. Αποστολή της Αρχής Προστασίας Δεδομένων είναι η εποπτεία της εφαρμογής των νόμων και άλλων ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Τα δεδομένα που συλλέγουν οι οργανισμοί ηλεκτρονικού εμπορίου για τους πελάτες τους, στα πλαίσια πραγματοποίησης ηλεκτρονικών συναλλαγών, αποτελούν προσωπικά δεδομένα και συνεπώς προστατεύονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Συγκεκριμένα κάθε οργανισμός ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την εν λόγω Αρχή.

Η Αρχή αυτή έχει τις εξής αρμοδιότητες:

- Να εκδίδει οδηγίες και κανονιστικές πράξεις για την εφαρμογή των διατάξεων που αφορούν στην προστασία προσωπικών δεδομένων και να γνωμοδοτεί για σχετικά θέματα.
- Να απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και να επιβάλλει/βοηθάει όσους διατηρούν αρχεία να καταρτίζουν κώδικες δεοντολογίας.
- Να καταγγέλλει τις παραβάσεις στις αρμόδιες διοικητικές και δικαστικές αρχές αλλά και να επιβάλλει κυρώσεις.
- Να ενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, ελέγχους σε κάθε αρχείο.

Στη χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97), ενώ ο Νόμος 2774/1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα καταργήθηκε στις 29 Ιουλίου 2006.

Ο Νόμος 2472/97 ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ και αναφέρεται στην "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Με λίγα λόγια καθορίζει τις υποχρεώσεις των φορέων και των υπηρεσιών που "εκτελούν την επεξεργασία" και θέτει τα δικαιώματα προστασίας των ατόμων, όσον αφορά την προστασία και διαφύλαξη των προσωπικών τους δεδομένων.

Με βάση το νόμο 2472/97:

- Η επεξεργασία προσωπικών πληροφοριών είναι επιτρεπτή μόνο στις περιπτώσεις που ο νόμος προσδιορίζει περιοριστικά και δεσμευτικά.
- Η επεξεργασία επιτρέπεται μόνο για νόμιμους, θεμιτούς και εξειδικευμένους σκοπούς που είναι γνωστοί στον πολίτη.
- Αναγνωρίζονται και κατοχυρώνονται νέα δικαιώματα των πολιτών για να αμύνονται έναντι των προσβολών της ιδιωτικής ζωής και της προσωπικότητας τους (δικαίωμα προηγούμενης πληροφόρησης, διόρθωσης, αποζημίωσης).

Οι ρυθμίσεις του νόμου 2472/97 συμπληρώθηκαν από το Νόμο 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών). Ο νόμος αυτός κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών.

3.4 ΚΑΝΟΝΙΣΜΟΙ ΑΔΑΕ

<<Η αρχή διασφάλισης του απορρήτου των επικοινωνιών>>

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) προβλέπεται από το Ν.3115/2003. Είναι ανεξάρτητη αρχή με διοικητική αυτοτέλεια και έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης και επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στο πλαίσιο αυτό, η Α.Δ.Α.Ε. είναι η αρμόδια αρχή για τον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. Η δράση της διέπεται πάντοτε από τις αρχές της διαφάνειας, της αντικειμενικότητας και της αμεροληψίας. Η Α.Δ.Α.Ε. αποτελείται από 7 μέλη και ισάριθμα αναπληρωματικά, τα οποία απολαμβάνουν κατά την άσκηση των καθηκόντων τους πλήρη προσωπική και λειτουργική ανεξαρτησία. Ωστόσο, έχουν καθήκον εχεμύθειας, το οποίο υφίσταται και μετά την αποχώρησή τους. Τα πρόσωπα που θα γίνουν μέλη της Α.Δ.Α.Ε. επιλέγονται από τη Βουλή και πρέπει να τυγχάνουν ευρείας κοινωνικής αποδοχής και να διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στο νομικό τομέα ή στον τεχνικό τομέα των επικοινωνιών.

Η Α.Δ.Α.Ε. στο πλαίσιο εκπλήρωσης του σκοπού της, μπορεί:

- Να διενεργεί αυτεπαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.
- Να καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.
- Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.
- Να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

Τα μέλη και το προσωπικό της Α.Δ.Α.Ε., για να διαπιστώσουν παράβαση της νομοθεσίας για την προστασία του απορρήτου, μπορούν να ελέγχουν τα βιβλία και στοιχεία των ελεγχόμενων υπηρεσιών, οργανισμών και επιχειρήσεων, καθώς και πάσης φύσεως αρχεία, βιβλία, στοιχεία και λοιπά έγγραφα των προσώπων που ελέγχουν. Επιπλέον, έχουν δικαίωμα να ενεργούν έρευνες στα γραφεία και τις λοιπές εγκαταστάσεις των ελεγχομένων και να διενεργούν ένορκες και μη καταθέσεις, με την επιφύλαξη του επαγγελματικού απορρήτου των εξεταζόμενων προσώπων.

Σε περίπτωση που κατά τον έλεγχο διαπιστωθεί παραβίαση του απορρήτου, τα μέλη της Α.Δ.Α.Ε. μπορούν να κατασχέσουν τα μέσα με τα οποία πραγματοποιείται η παραβίαση αυτή, ενώ παράλληλα καταστρέφουν τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών. Για τα μέσα που κατάσχονται, ορίζεται μεσεγγυούχος ωσότου αποφανθούν τα αρμόδια δικαστήρια.

Η Α.Δ.Α.Ε. αποφασίζει με απόλυτη πλειοψηφία των παρόντων μελών της με φανερή ψηφοφορία. Για να είναι όμως νόμιμη η συνεδρίαση, θα πρέπει να μετέχουν τουλάχιστον 3 μέλη. Οι αποφάσεις της πρέπει να είναι αιτιολογημένες, καταχωρούνται σε ειδικό βιβλίο και μπορούν να δημοσιεύονται, εφόσον δεν αφορούν στην εθνική άμυνα ή τη δημόσια ασφάλεια. Σε κάθε περίπτωση, η Α.Δ.Α.Ε. οφείλει να μην αποκαλύπτει πληροφορίες και δεδομένα για φυσικά ή νομικά πρόσωπα, τα οποία ενδέχεται να προσβάλλουν την προσωπικότητά τους ή να επηρεάσουν δυσμενώς την επαγγελματική ή την κοινωνική τους θέση, εκτός εάν προκύπτει τέτοια υποχρέωση από το νόμο.

Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή από 15.000 έως 60.000 ευρώ. Σε περίπτωση που ο παραβάτης ανήκει στο προσωπικό υπηρεσίας, οργανισμού, νομικού προσώπου ή επιχείρησης που ασχολείται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση ή την επικοινωνία, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον 2 ετών και η χρηματική ποινή τουλάχιστον 30.000 ευρώ.

ΚΕΦΑΛΑΙΟ 4ο

ΟΙ ΑΠΕΙΛΕΣ ΕΝΟΣ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανύποπτου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο αρχείο, φαινομενικά αθώο, όπως ένα κείμενο ή μια φωτογραφία και, όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα και μπορεί να καταστρέψει αρχεία ή και ολόκληρο το σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστιοτόπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη (φυλλομετρητή ή Λειτουργικό σύστημα). Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται worm (κατά λέξη μετάφραση σκουλήκι). Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την "προσκόλλησή" του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης, επειδή καταναλώνει σημαντικό εύρος ζώνης (bandwidth).Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

4.1 ΙΟΥΣ

Ένας ιός υπολογιστών 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 USB. 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. Αλλοι 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.

Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι που προαναφέρθηκαν, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό όχι μόνον είναι δυνατό να υφαρπαγούν προσωπικά δεδομένα κάποιου χρήστη, όπως ο αριθμός ταυτότητάς του ή το ΑΦΜ του, όσο και, πιο σημαντικό, αριθμοί πιστωτικών καρτών, λογαριασμών Τραπέζης κτλ. Ανάλογη μέθοδος ακολουθείται και από ορισμένους ιστιοτόπους, στους οποίους ο ανύποπτος χρήστης καταχωρεί παρόμοια στοιχεία παραγγέλοντας ένα προϊόν, το οποίο όχι μόνο δε θα λάβει ποτέ, αλλά τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους δημιουργούς του ιστοτόπου για να πραγματοποιήσουν οι ίδιοι αγορές, χρεώνοντας τον "πελάτη" τους. Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείται "Phishing"

(παραφθορά της λέξης fishing = ψάρεμα). Αρκετά προγράμματα περιήγησης (browsers) αναγνωρίζουν τους ιστοτόπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα, ωστόσο αυτό δεν συμβαίνει σε ποσοστό 100%. Οι χρήστες είναι καλό να γνωρίζουν ότι κανείς χρηματοπιστωτικός φορέας δεν χρησιμοποιεί το Διαδίκτυο για να ανανεώσει προσωπικές πληροφορίες, ενώ ένας προστατευμένος ιστοτόπος αρχίζει πάντα με το πρόθεμα https (secure, ασφαλής).

Το ηλεκτρονικό ταχυδρομείο (αγγλικά e-mail, email ή mail προφέρεται "ιμέιλ" ή "μέιλ" αντίστοιχα) είναι μια μέθοδος συγγραφής, αποστολής, λήψης και αποθήκευσης μηνυμάτων με χρήση ηλεκτρονικών συστημάτων τηλεπικοινωνιών. Γενικά ο όρος "ηλεκτρονικό ταχυδρομείο" αναφέρεται στο σύστημα ηλεκτρονικού ταχυδρομείου του Διαδικτύου που χρησιμοποιεί το Simple Mail Transfer Protocol πρωτόκολλο, σε δικτυακά συστήματα που βασίζονται σε άλλα πρωτόκολλα μεταφοράς μηνυμάτων, αλλά και σε διάφορα συστήματα μηνυμάτων σε μικρά δίκτυα, υπερυπολογιστές, κλπ που επιτρέπου στους χρήστες τους να στέλνουν μηνύματα μεταξύ τους για την υποστήριξη ομαδικής συνεργασίας. Τα συστήματα σε τοπικά δίκτυα ή σε δίκτυα intranet είναι πιθανόν να βασίζονται σε ιδιωτικά πρωτόκολλα, που υποστηρίζονται από το συγκεκριμένο σύστημα, ή να είναι τα ίδια πρωτόκολλα που χρησιμοποιούνται στα δημόσια δίκτυα. Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται συχνά για τη μεταφορά ανεπιθύμητων μηνυμάτων σε μεγάλο όγκο (σπάμ (spam)), αλλά υπάρχουν προγράμματα που μπορούν να "φιλτράρουν" και να σταματήσουν ή να σβήσουν αυτόματα τα περισσότερα από αυτά.

Κατηγορίες ιών

1. ΔΟΥΡΕΙΟΣ ΙΠΟΣ

Υπάρχουν δύο είδη δούρειων ίππων:

- Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία διάφοροι χάκερς μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για παράδειγμα διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων (peer-to-peer), προγράμματα ανακοίνωσης καιρικών συνθηκών κοκ.
- Το δεύτερο είδος περιλαμβάνει 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.

Σε αντίθεση με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς κοκ), οι δούρειοι ίπποι δεν μπορούν να δράσουν αυτόνομα αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα. Τέλος, στην επιστήμη της αρχιτεκτονικής υπολογιστών, η λέξη "δούρειος ίππος" μπορεί επίσης να αναφέρεται και σε κενά ασφαλείας που επιτρέπουν σε διάφορα προγράμματα να διαβάσουν αρχεία χωρίς εξουσιοδότηση.

Οι τύποι δούρειων ίππων μπορούν να διαχωριστούν περαιτέρω στις εξής κατηγορίες ανάλογα με τις συνέπειες που έχουν στον μολυσμένο υπολογιστή:

- Απομακρυσμένη πρόσβαση.

- Αποστολή e-mail.
- Καταστροφή αρχείων.
- Κατέβασμα αρχείων.
- Proxy Trojan.
- FTP Trojan (προσθήκη, διαγραφή ή μεταφορά αρχείων από τον μολυσμένο υπολογιστή).
- Απενεργοποίηση λογισμικού ασφαλείας (firewall, αντιϊκά κλπ).
- Denial of Service (DoS).
- URL Trojan (επιτρέπει στον υπολογιστή να συνδεθεί στο διαδίκτυο μόνο μέσω μίας πολύ ακριβής σύνδεσης).

Μερικές από τις επιπτώσεις εκτέλεσης ενός δούρειου ίππου είναι για παράδειγμα η διαγραφή αρχείων στον μολυσμένο υπολογιστή, η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές, το ανοιγόκλεισμα του οδηγού CD-ROM, η παρακολούθηση των κινήσεων του χρήστη για την απόκτηση των κωδικών του σε τράπεζες, απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, επανεκκίνηση του υπολογιστή, απενεργοποίηση προγραμμάτων firewall ή αντιϊκών και πολλά άλλα.

2. ΠΡΟΓΡΑΜΜΑ ΥΠΟΛΟΓΙΣΤΗ

Στην επιστήμη υπολογιστών με τον όρο πρόγραμμα αναφερόμαστε σε μια συγκεκριμένη ακολουθία εντολών τις οποίες πρέπει να εκτελέσει ένας υπολογιστής για να παραγάγει το επιθυμητό για το χρήστη αποτέλεσμα. Σύμφωνα με τον γενικό ορισμό που έδωσε ο Τζον φον Νόιμαν το 1945, το πρόγραμμα αποτελείται από μια συνεχή αλληλουχία εντολών τις οποίες ο υπολογιστής καλείται να εκτελέσει μία προς μία για να παραχθεί το επιθυμητό αποτέλεσμα.

Στους σύγχρονους υπολογιστές το πρόγραμμα εγγράφεται σε κάποιο αποθηκευτικό μέσο προσβάσιμο από τον υπολογιστή. Ο υπολογιστής "διαβάζει" από εκεί μια εντολή, την εκτελεί και επανέρχεται διαβάζοντας την επόμενη κ.ο.κ. Η περιοχή αποθήκευσης μπορεί, επίσης, να περιέχει τα δεδομένα, τα οποία κάποια ή κάποιες από τις εντολές οφείλει να επεξεργαστεί. Η εκτέλεση ενός προγράμματος από τον υπολογιστή συνηθίζεται να ονομάζεται "τρέξιμο" (run).

Ένα πρόγραμμα μπορεί να χαρακτηριστεί ως δέσμης (batch) ή αλληλεπιδραστικό (interactive), από την άποψη του ποιος το καθοδηγεί και του πώς εκτελείται (τρέχει). Το αλληλεπιδραστικό (με το χρήστη) πρόγραμμα λαμβάνει δεδομένα είτε από το χρήστη είτε από κάποιο άλλο πρόγραμμα που προσομοιώνει το χρήστη. Αντίθετα, ένα πρόγραμμα δέσμης τρέχει και εκτελεί την αποστολή του αυτοτελώς, χωρίς να δεχθεί δεδομένα ή εντολές από κάποιο χρήστη και σταματά να εκτελείται μόνον όταν ολοκληρώσει την ομάδα εντολών από την οποία αποτελείται. Χαρακτηριστικά παραδείγματα αλληλεπιδραστικών προγραμμάτων είναι οι πλοηγοί του World Wide Web (web browser), ενώ ένα πρόγραμμα το οποίο υπολογίζει και εκτυπώνει τις αμοιβές του προσωπικού μιας εταιρείας είναι πρόγραμμα δέσμης.

Όπως είναι αναμενόμενο ένα πρόγραμμα δεν μπορεί να εκτελεί πολλαπλές διαφορετικές εργασίες. Έτσι, για να είναι χρήσιμος ένας υπολογιστής, συνήθως πρέπει να συνδυαστούν περισσότερα του ενός προγράμματα. Π.χ. τα προγράμματα που αναφέρθηκαν πιο πάνω περιέχουν και ένα επιπλέον πρόγραμμα, αυτό που αναλαμβάνει την εκτύπωση των αποτελεσμάτων. Αλληλεπιδραστικά και προγράμματα δέσμης μπορούν να συνυπάρχουν και να συνεργάζονται: το πρόγραμμα εκτύπωσης ενός πλοηγού Web, για παράδειγμα, είναι πρόγραμμα δέσμης.

Το πρόγραμμα δημιουργείται από ειδικευμένα άτομα, τους προγραμματιστές. Για την κατασκευή ενός προγράμματος χρησιμοποιείται μια κατάλληλη γλώσσα που επιτρέπει την επικοινωνία προγραμματιστή και υπολογιστή. Η γλώσσα αυτή, που στις περισσότερες περιπτώσεις είναι η ίδια ένα πρόγραμμα, ονομάζεται γλώσσα προγραμματισμού. Η διαδικασία δημιουργίας ενός προγράμματος ονομάζεται προγραμματισμός. Οι εντολές που γράφει ο προγραμματιστής αποτελούν τον πηγαίο κώδικα (source code). Συνήθως, οι εντολές του προγράμματος χρειάζεται να "μεταφραστούν" στη γλώσσα που αντιλαμβάνεται ο υπολογιστής και αυτό γίνεται δυνατό με τη χρήση ενός άλλου προγράμματος που ονομάζεται, ανάλογα με τον τρόπο λειτουργίας του, μεταγλωττιστής (compiler) ή διερμηνέας (interpreter). Το παραγόμενο αποτέλεσμα λέγεται ότι αποτελεί τον αντικειμενικό κώδικα. Αυτός αποτελείται από μια μακροσκελή σειρά από δυαδικά ψηφία, 0 και 1, η οποία αποτελεί τη γλώσσα μηχανής (machine code), τη μόνη που αντιλαμβάνεται ο επεξεργαστής ενός υπολογιστή.

Τα προγράμματα, το σύνολο των οποίων λέγεται και λογισμικό (software) κατ' αντιδιαστολή με το υλικό του υπολογιστή (hardware), ταξινομούνται ανάλογα με τη χρήση τους σε κατηγορίες όπως για παράδειγμα, μεταξύ άλλων, λογισμικό εφαρμογών, λειτουργικά συστήματα, βιντεοπαιχνίδια και μεταγλωττιστές. Προγράμματα που είναι ενσωματωμένα σε συσκευές υλικού λέγονται firmware.

3. ΥΠΟΛΟΓΙΣΤΗΣ ZOMBIE

Ένας ηλεκτρονικός υπολογιστής θεωρείται ότι είναι υπολογιστής zombie όταν είναι συνδεδεμένος στο Διαδίκτυο και ελέγχεται από κάποιον εξωτερικό χρήστη. Αυτός ο εξωτερικός χρήστης είναι στην πλειοψηφία των περιπτώσεων κάποιος χάκερ που εξαπέλυσε επιτυχημένη επίθεση ενάντια στον υπολογιστή και κατάφερε να τον μετατρέψει σε υπολογιστή zombie. Η επίθεση αυτή περιλαμβάνει μεταξύ άλλων την μόλυνση του υπολογιστή-θύμα από κάποιον ιό ή δούρειο ίππο.

4. ΑΡΧΕΙΟ ΥΠΟΛΟΓΙΣΤΗ

Ένα αρχείο υπολογιστή είναι ένα σύνολο από πληροφορίες, δεδομένα ή και ένας πόρος, που χρησιμεύει ως "δοχείο" για την αποθήκευση πληροφορίας και είναι διαθέσιμο σε ένα πρόγραμμα υπολογιστή. Συνήθως βρίσκεται σε διατηρητέο αποθηκευτικό μέσο υπολογιστή. Ένα αρχείο είναι διατηρητέο με την έννοια ότι ακόμα και όταν τερματίσουν να εκτελούνται τα προγράμματα που το δημιούργησαν ή το χρησιμοποιούν αυτό θα συνεχίσει να υπάρχει.

Ένα αρχείο υπολογιστή μπορεί να θεωρηθεί σαν το σύγχρονο ισοδύναμο ενός εγγράφου το οποία παραδοσιακά βρίσκονταν σε φοριαμούς - αρχειοθήκες γραφείων και βιβλιοθηκών. Αυτή είναι και η προέλευση της έννοιας.

Σε κάθε αρχείο υπολογιστή ενός υπολογιστή δίνεται ένα όνομα ώστε να ξεχωρίζει από όλα τα άλλα αρχεία.

5. ΧΑΚΕΡ

Αρχικά ο όρος "χάκερ" σήμαινε στα αγγλικά το δημιουργό ενός επίπλου ή γενικότερα ξύλινου αντικειμένου με τη βοήθεια πελέκεως (τσεκουριού).Χάκερ ονομάζεται κάποιος που αντλεί ευχαρίστηση από τη βαθειά κατανόηση της εσωτερικής λειτουργίας ενός συστήματος, ειδικότερα ενός υπολογιστή ή δικτύου υπολογιστών, στον οποίο, όμως, δεν έχει δικαίωμα πρόσβασης. Ο όρος (ειδικά στην ελληνική γλώσσα) συγχέεται πολύ συχνά με τον όρο κράκερ (cracker), κάτι που αποτελεί σφάλμα. Σε αντίθεση με τον χάκερ, ο κράκερ είναι άτομο (ή ομάδα ατόμων) που αποπειράται να αποκτήσει πρόσβαση σε βλάψει με οποιοδήποτε τρόπο. Οι κράκερ είναι εξ ορισμού κακόβουλοι, αντίθετα προς τους χάκερ, ενώ διαθέτουν και πολλά εργαλεία για τις κακόβουλες ενέργειές τους. Η διεθνής κοινότητα των χάκερ πιστεύει υπολογιστικό σύστημα για την οποία όχι μόνο δε διαθέτει εξουσιοδότηση, αλλά με στόχο να το ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητές τους τόσο δημιουργώντας λογισμικό ανοικτού κώδικα, όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό. Έχουν, επίσης, την αμφιλεγόμενη πεποίθηση ότι το "σπάσιμο" και η "εξερεύνηση" ενός υπολογιστικού συστήματος, τόσο σε επίπεδο υλικού όσο και (κυρίως) λογισμικού είναι ηθικά αποδεκτή, εφόσον ο χάκερ δεν διαπράττει κλοπή, βανδαλισμό ή παραβίαση εμπιστευτικότητας. Για τους χάκερς, όποιος "αξίζει αυτόν τον τίτλο, είναι στην πραγματικότητα ένας έξυπνος προγραμματιστής ή άτομο με ιδιαίτερες ικανότητες στην κατανόηση και το χειρισμό υπολογιστικών συστημάτων". Σε καμία, όμως, περίπτωση, δεν αποδέχονται ότι οι πράξεις ενός χάκερ έχουν κακόβουλους στόχους και αυτή η διαφορά είναι που τους διακρίνει από τους κράκερς.

4.2 ΠΑΡΑΠΛΑΝΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Αρκετές φορές οι χρήστες του Διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν κάποιες πληροφορίες που χρειάζονται. Μερικοί ιστότοποι εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές. Το κίνητρο για τέτοιες πράξεις μπορεί να είναι είτε η αποκομιδή ιδίου οφέλους είτε, απλά, η χαρά της παραπλάνησης των (αγνώστων) χρηστών. Ο όρος που περιγράφει αυτού του τύπου την παραπλάνηση είναι "Hoax". Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know").

Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

"Pharming" σημαίνει όταν εγκληματίες χάκερ ανακατευθύνουν την κίνηση του Διαδικτύου από μία τοποθεσία Web σε μια άλλη, πανομοιότυπη έτσι ώστε να σας ξεγελάσουν και να καταχωρίσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής τοποθεσίας. Τοποθεσίες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να βρουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Το Pharming (παραπλάνηση), η χρήση δηλαδή ψεύτικων τοποθεσιών Web πιθανόν να θυμίζει τις απάτες ψαρέματος από ηλεκτρονικά μηνύματα, όμως η παραπλάνηση είναι πιο ύπουλη, αφού μπορεί να κατευθυνθείτε σε μία ψεύτικη τοποθεσία χωρίς τη συμμετοχή σας ή χωρίς να το γνωρίζετε.

Εώς σήμερα έγιναν μερικές τεκμηριωμένες επιθέσεις, και η διατήρηση της ακεραιότητας του Διαδικτύου είναι πολύ ψηλά στον κατάλογο των προτεραιοτήτων των κυβερνήσεων και των επιχειρήσεων. Είναι επίσης σημαντικό να θυμάστε πως το Διαδίκτυο είναι μια δωρεάν και ανεξάρτητη πηγή, όπως μία βιβλιοθήκη ή άλλες δημόσιες υπηρεσίες, στον τόπο όπου ζείτε. Για τους περισσότερους ανθρώπους, τα πλεονεκτήματα του να πηγαίνουν για ψώνια, να γυρνούν στα μαγαζιά, να κάνουν έρευνα, να συναντούν κόσμο, αντισταθμίζει τον κίνδυνο και τον απρόβλεπτο παράγοντα να είσαι σε έναν δημόσιο χώρο.

Εάν παρατηρήσετε κάτι ύποπτο σχετικά με μία τοποθεσία Web που εμπιστεύεστε, αναφέρετέ το —τηλεφωνικά εάν είναι δυνατόν—στην επιχείρηση ή στον ιδιοκτήτη της τοποθεσίας. Μπορεί να είναι κάτι συνηθισμένο ή μια νέα ενημερωμένη έκδοση ή μπορεί να είναι ένα λάθος που έκανε ο εγκληματίας προσπαθώντας να αντιγράψει την τοποθεσία Web. Αυτό το άρθρο για τις απάτες ψαρέματος παρέχει μερικές συμβουλές για το πώς να καταλάβετε εάν μία τοποθεσία Web είναι αυθεντική ή όχι.

ΣΗΜΑΝΤΙΚΕΣ ΕΡΩΤΗΣΕΙΣ –ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΤΗΝ ΠΑΡΑΠΛΑΝΗΣΗ

1. Πώς μπορεί κάποιος απατεώνας που θέλει να με παραπλανήσει, να κατευθύνει το πρόγραμμα περιήγησης μου σε κάποια άλλη τοποθεσία;

Α: Με τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS" κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών Διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση και μπορεί να κάνει τροποποιήσεις σε κάποιο σημείο έτσι ώστε να εκτρέπεστε στην ψεύτικη τοποθεσία πριν αποκτήσετε πρόσβαση σε αυτή που τελικά επιθυμούσατε.

2. Κάποιες εταιρίες υποστηρίζουν πως το λογισμικό του τείχους προστασίας που χρησιμοποιούν προστατεύει και από την παραπλάνηση. Είναι αλήθεια αυτό;

Α: Κάποιοι πάροχοι υπηρεσιών διαδικτυακής ασφάλειας πιστεύουν πως οι πελάτες τους που καθοδηγούν όλη τους την διαδικτυακή κίνηση μέσω των δικών τους, ασφαλών, διακομιστών είναι και προστατευμένοι από επιθέσεις παραπλανήσεις. Η φύση της παραπλάνησης υποδεικνύει το αντίθετο αλλά, ανεξάρτητα από το τι υποστηρίζει η κάθε εταιρεία, είναι καλή ιδέα να αναζητάτε προσεκτικά τα προϊόντα ασφαλείας πριν επενδύσετε και εμπιστευτείτε κάποιες λύσεις λογισμικού, διαβάζοντας τις κριτικές των προϊόντων από αξιόπιστες πηγές, όπως το CNET Reviews.

3. Δεν μπορώ να αναγνωρίσω εάν μία τοποθεσία Web είναι ψεύτικη απλά μετακινώντας το δείκτη πάνω από τους συνδέσμους και παρατηρώντας εάν ο κώδικας με οδηγεί σε κάποιο εμφανώς άσχετο σημείο εκτός τοποθεσίας;

Α: Όχι απαραίτητα. Οι ψεύτικες τοποθεσίες Web που χρησιμοποιούνται στις απάτες παραπλάνησης συνήθως "πλαστογραφούν" τους συνδέσμους τους έτσι ώστε να μοιάζουν ακριβώς με αυτούς που αναμένετε να δείτε, ακόμη και στον κώδικα που εμφανίζεται όταν το ποντίκι περάσει πάνω από αυτούς. Επίσης, οι τοποθεσίες Web πιθανόν να αλλάζουν τον κώδικα των δικών τους συνδέσμων αρκετά συχνά και για διάφορους λόγους, όπως όταν αναβαθμίζουν το λογισμικό τους, την πλατφόρμα του διακομιστή τους και τις μεθόδους ανάλυσης της κίνησης της τοποθεσίας.

4. Γιατί το pharming γράφεται με "ph" αντί για "f";

Α: Ανήκει σε μια ανεξάρτητη αργκό, η οποία ξεκίνησε με την έκφραση "phone phreaking": η χρήση ηλεκτρονικών μέσων για την παραβίαση τηλεφωνικών γραμμών με σκοπό την επίτευξη δωρεάν κλήσεων. Σήμερα, υπάρχει μια ολόκληρη υποκουλτούρα ηλεκτρονικής γλώσσας που αλλάζει συνεχώς, μέρος της οποίας παρουσιάζεται στην ενότητα Εισαγωγή των γονέων στην αργκό των υπολογιστών.

4.3 ΗΛΕΚΤΡΟΝΙΚΕΣ ΚΑΡΤΕΣ

Οι ηλεκτρονικές κάρτες δημιουργούνται με τον ίδιο τρόπο που δημιουργούνται οι τοποθεσίες Web: κατασκευάζονται στο Internet, όπως ακριβώς αυτή η σελίδα. Έτσι, όταν στέλνετε σε κάποιον μια ηλεκτρονική κάρτα, στην πραγματικότητα τους παρέχετε μια σύνδεση. Όταν οι παραλήπτες κάνουν κλικ επάνω της, τους οδηγεί στην ευχετήρια ηλεκτρονική κάρτα που δημιουργήσατε για αυτούς.

Πρέπει πάντα να είστε προσεκτικοί με τις συνδέσεις σε μηνύματα ηλεκτρονικού ταχυδρομείου. Η Sally Babcock, Γενική διευθύντρια και Αντιπρόεδρος της American Greetings Interactive, που είναι ένας δημοφιλής προορισμός για την αποστολή ευχετήριων καρτών εντός και εκτός Internet, συμφωνεί και λέει:

> "Οι επιθέσεις ηλεκτρονικού "ψαρέματος" με χρήση ηλεκτρονικών καρτών μοιάζουν με όλους τους υπόλοιπους τύπους επιθέσεων ηλεκτρονικού "ψαρέματος" στο ότι εκμεταλλεύονται την άγνοια ή την αμέλεια του χρήστη". Επιπλέον παρέχουν ακεραιότητα δεδομένων, ασφάλεια και ιδιωτικότητα. Όπως είναι γνωστό, για να γίνει μια ηλεκτρονική συναλλαγή απαιτείται η ανταλλαγή ευαίσθητων προσωπικών δεδομένων μεταξύ των συναλλασσόμενων πλευρών. Οι έξυπνες κάρτες αποτελούν ένα άριστο μέσο για τη μεταφορά ευαίσθητων προσωπικών δεδομένων όπως για παράδειγμα αριθμούς πιστωτικών καρτών, κλειδιά κρυπτογράφησης και αποκρυπτογράφησης κλπ. Οι έξυπνες κάρτες μπορούν επιπλέον να αντικαταστήσουν κάρτες όπως οι τηλεκάρτες, οι πιστωτικές κάρτες, οι κάρτες ανάληψης μετρητών και άλλες παρόμοιες κάρτες. Μπορούν επίσης να χρησιμοποιηθούν ως προπληρωμένες κάρτες για την αποθήκευση ψηφιακών νομισμάτων. Μία τέτοια κάρτα είναι η κάρτα javacard.

Όλοι μας έχουμε ακούσει να μιλούν για τους κινδύνους της χρήσης πιστωτικών καρτών στο Internet. Η λαϊκή φαντασία, τροφοδοτούμενη από αμαθείς δημοσιογράφους, υποστηρίζει ότι κάθε φορά που πραγματοποιούμε μια συναλλαγή online και δίνουμε τα στοιχεία της κάρτας μας σε έναν έμπορο, αυτά αποθηκεύονται στη βάση δεδομένων του και βρίσκονται πλέον στο έλεος κάθε αδίστακτού εισβολέα ο οποίος μπορεί να τα αποκτήσει, παραβιάζοντας τα συστήματα ασφαλείας, και στη συνέχεια να σπαταλήσει τεράστια ποσά τα οποία φυσικά θα χρεώσει στη δική μας κάρτα.

Ευτυχώς για τους καταναλωτές όμως τα πράγματα δεν είναι ακριβώς έτσι. Είναι αλήθεια βέβαια ότι, αν κάνω χρήση της πιστωτικής μου κάρτας στο δίκτυο, τα στοιχεία της μπορεί να πέσουν στα χέρια αδίστακτων ανθρώπων. Ωστόσο, για να προστατευτούν οι καταναλωτές από αυτό τον κίνδυνο, υπάρχει ειδική νομοθεσία, τόσο στην Ευρωπαϊκή Ένωση όσο και στις ΗΠΑ, η οποία ορίζει ότι ο κάτοχος της κάρτας μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσίαση του φυσικού σώματος της κάρτας.

Με τον τρόπο αυτό η ευθύνη για την κάρτα μου περιορίζεται μόνο στο υλικό μέρος της και μόνο αν χάσω την ίδια την κάρτα αναλαμβάνω την ευθύνη της ακύρωσής της και βαρύνομαι με όποιες δαπάνες έγιναν πριν

δηλώσω την απώλειά της. Επειδή όμως η διακίνηση των στοιχείων της κάρτας δεν ελέγχεται και μπορεί να τα αποκτήσει χωρίς δική μου γνώση ή υπαιτιότητα ο οποιοσδήποτε (π.χ. ο πωλητής του πολυκαταστήματος από το οποίο αγόρασα ένα ζευγάρι κάλτσες), δεν με υποχρεώνει κανείς να αναγνωρίσω όποια συναλλαγή πραγματοποιείται χωρίς την ίδια την κάρτα.

Έτσι, σε περίπτωση online συναλλαγών με κλεμμένα στοιχεία καρτών, ο κάτοχος όταν δει τη χρέωση στο αντίγραφο του λογαριασμού του μπορεί να αρνηθεί την καταβολή του αντιτίμου και η τράπεζα όχι μόνο δεν θα καταβάλει το ποσό αυτό στον πωλητή, αλλά θα χρεώσει και το κατάστημα με τα έξοδα ακύρωσης της συναλλαγής. Φυσικά, για τον κάτοχο της κάρτας η διαδικασία άρνησης χρέωσης και στη συνέχεια αλλαγής της κάρτας του (προκειμένου να μην επαναληφθεί το ίδιο φαινόμενο) δεν είναι απλή υπόθεση. Ωστόσο, ο "μπελάς" είναι μικρός συγκρινόμενος με τις δυσκολίες που έχει να αντιμετωπίσει όποιο ηλεκτρονικό κατάστημα εμπιστεύθηκε αυτή την κάρτα και παρέδωσε προϊόντα ή προσέφερε υπηρεσίες στον ψεύτικο κάτοχό της.

Κάθε ηλεκτρονικός επιχειρηματίας έχει φυσικά το δικαίωμα να διώξει δικαστικά τον παραλήπτη των προϊόντων τα οποία ζητήθηκαν με κλεμμένα στοιχεία πιστωτικής κάρτας, ζητώντας αποζημίωση. Δυστυχώς όμως, το δύσκολο έργο της ανακάλυψης του ενόχου και της τιμωρίας του σπάνια έχει αίσιο τέλος. Στην πλειοψηφία των περιπτώσεων μάλιστα αυτό είναι πρακτικώς αδύνατον (π.χ. τα έξοδα δίωξης κατοίκου άλλης χώρας είναι τόσο υψηλά που δεν αξίζει τον κόπο να ασχοληθεί κανείς με το θέμα). Γι' αυτό και τα ηλεκτρονικά καταστήματα προτιμούν την πρόληψη από τη θεραπεία.

Η πρώτη γραμμή άμυνάς τους είναι ο έλεγχος της αξιοπιστίας των πιστωτικών καρτών. Πολλές φορές μια κάρτα μπορεί να είναι έγκυρη (να μην έχει ακυρωθεί ακόμη από την Τράπεζα), αλλά τα στοιχεία της να έχουν κλαπεί και να έχει ήδη χρησιμοποιηθεί στο παρελθόν για αγορές τις οποίες αρνήθηκε να αναγνωρίσει ο κάτοχός της.

Γι' αυτό και τα ηλεκτρονικά καταστήματα μισθώνουν τις υπηρεσίες ειδικών εταιρειών, όπως η Cybersource (http://www.cybersource.com), οι οποίες παρακολουθούν τα περιστατικά αυτά και ενημερώνουν το ηλεκτρονικό κατάστημα αν παρουσιάστηκαν προβλήματα με τη συγκεκριμένη κάρτα στο παρελθόν. Οι υπηρεσίες αυτές βέβαια δεν παρέχονται δωρεάν. Ωστόσο, η χρήση τους είναι υποχρεωτική για όλα τα καταστήματα, καθώς περιορίζουν τις απώλειες από το 20% στο 1% των παραγγελιών. (Δηλαδή χωρίς έλεγχο των καρτών το 20% των παραγγελιών αποδεικνύονται πλαστές και η αξία των προϊόντων δεν εισπράττεται ποτέ!).

Η δεύτερη, και τελευταία, γραμμή άμυνας για κάθε ηλεκτρονικό κατάστημα είναι ο έλεγχος των παραγγελιών για την ανακάλυψη "ύποπτων" αιτημάτων. Ενδεικτικά αναφέρουμε μερικά παραδείγματα παραγγελιών οι οποίες πρέπει να ελέγχονται εξονυχιστικά:

- Μεγάλες παραγγελίες από πελάτες οι οποίοι δεν έχουν αγοράσει τίποτε στο παρελθόν
- Παραγγελία η οποία πρέπει να παραδοθεί σε ανεξέλεγκτη διεύθυνση όπως κάποια γραμματοθυρίδα ή το post restant
- Πολλαπλές παραγγελίες για καταναλωτικά είδη τα οποία συνήθως αγοράζονται μια φορά (π.χ. παραγγελία 30 ρακετών του τένις από ένα άτομο)
- Παραγγελία ειδών με περίεργη ακολουθία (π.χ. παραγγελία 2 πουκαμίσων μεγέθους small, συν 2 ίδιου χρώματος και σχεδίασης μεγέθους medium, συν άλλα δύο large, συν άλλα δύο extra large)
- Υποβολή πολλών παραγγελιών με την ίδια κάρτα σε μικρό χρονικό διάστημα
- Υποβολή πολλών παραγγελιών με την ίδια κάρτα και παράδοση σε διαφορετικές διευθύνσεις
- Υποβολή πολλών παραγγελιών με διαφορετικές κάρτες και παράδοση στην ίδια διεύθυνση

4.4 ΣΥΝΟΜΙΛΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται

«δωμάτιο επικοινωνίας» (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Το chat αποτελεί μια κοινωνική δραστηριότητα ιδιαίτερα δημοφιλή ανάμεσα στους νέους, διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο γνωριμίας με ανθρώπους απ' όλον τον κόσμο.

Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό

(όπως στην περίπτωση του δημοφιλούς IRC). Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όταν κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο

«δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους.

Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές, επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός internet-cafe, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδόφιλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι και η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς, όσο και από τους εκπαιδευτικούς.

4.5 ΜΗΝΥΜΑΤΑ ΕΝΟΧΛΗΤΙΚΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

Το λεγόμενο spam ή junk mail είναι μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ.ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet.
Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.
Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express).
Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

ΚΕΦΑΛΑΙΟ 5ο

Η ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΙΣ ΑΠΕΙΛΕΣ ΜΕ ΤΗΝ ΧΡΗΣΙΜΟΠΟΙΗΣΗ ΤΩΝ ΜΕΣΩΝ ΑΣΦΑΛΕΙΑΣ

Ο Παγκόσμιος Ιστός (World Wide Web) είναι μια από τις σημαντικότερες υπηρεσίες του Internet και προσφέρει στους χρήστες του τη δυνατότητα πρόσβασης στη μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο. Πρόκειται για μια τεράστια συλλογή εγγράφων, τα οποία είναι αποθηκευμένα σε εκατομμύρια υπολογιστές στον κόσμο και η οποία εμπλουτίζεται συνεχώς από όλους τους χρήστες οι οποίοι αποφασίζουν να ανεβάσουν στο χώρο του τις σελίδες τους. Η πλοήγηση στις σελίδες του παγκοσμίου ιστού πραγματοποιείται μέσω ειδικών προγραμμάτων πλοήγησης -browsers- (συνηθέστεροι ο Internet Explorer και ο Netscape Navigator) και απαιτεί ιδιαίτερη προσοχή από τον χρήστη, διότι εγκυμονεί πολλαπλούς κινδύνους, τόσο για την ασφάλεια του υπολογιστή του, όσο και για την ασφάλεια των προσωπικών του δεδομένων.Τα μέτρα τα οποία μπορεί να ληφθούν για να εξασφαλίσουν κατά το δυνατόν ασφαλή πλοήγηση στις σελίδες του παγκοσμίου ιστού εξαρτώνται α) από τις υπηρεσίες που μπορεί να προσφέρει ο παροχέας σύνδεσης (internet provider) και β) από τις ενέργειες που κάνει ο ίδιος ο χρήστης.

5.1 Η ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ FIREWALL

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 ούτως 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 και ρυθμίσουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

5.2 ΙΣΤΟΡΙΚΑ ΣΤΟΙΧΕΙΑ

Ο όρος firewall είναι αρκετά παλιός. 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.

1η γενιά - Φίλτρα πακέτων

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, εάν 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 εάν 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 (Well known ports), ένα firewall πρώτης γενιάς μπορεί να ξεχωρίσει τα πακέτα που αφορούν διάφορες λειτουργίες, όπως για παράδειγμα το email, την μεταφορά αρχείων, την περιήγηση στο Διαδίκτυο κοκ.

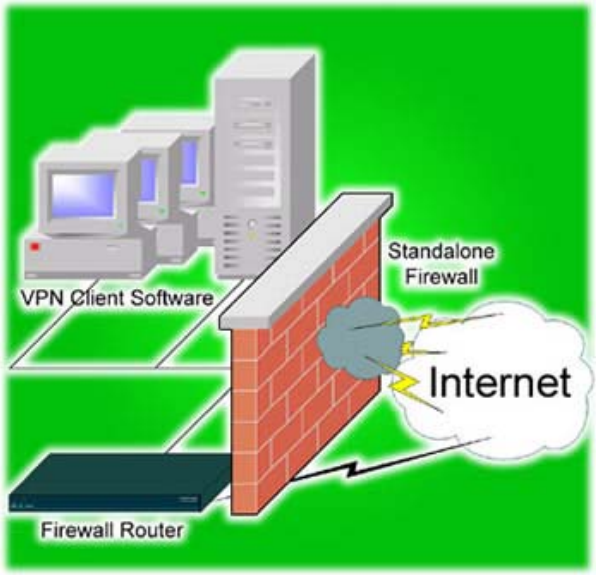
2η γενιά - Φίλτρα κατάστασης

Η δεύτερη γενιά firewall αναπτύχθηκε από τρεις ερευνητές στα εργαστήρια της AT&T Bell: Dave Presetto, Howard Trickey και Kshitij Nigam.

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 την 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 μία νέας σύνδεσης ή μέρος μίας ήδη υπάρχουσας.Οι διαχειριστές τέτοιων firewalls μπορούν να ορίσουν τους κανόνες βάσει των οποίων θα επιτρέπεται η δημιουργία συνδέσεων από το εξωτερικό δίκτυο (Διαδίκτυο) προς το τοπικό/εταιρικό δίκτυο. Με τον τρόπο αυτό γίνεται πιο εύκολη η πρόληψη διαφόρων ειδών επιθέσεων, όπως για παράδειγμα ή επίθεση SYN flood.

3η γενιά - Επίπεδο εφαρμογών

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 μίας υπηρεσίας.

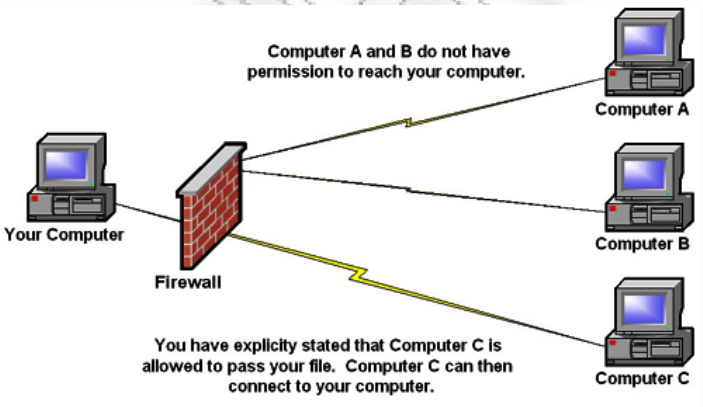


5.3 ΟΡΙΣΜΟΣ ΤΩΝ FIREWALL

Είναι ένας συνδυασμός υλικού και λογισμικού που απομονώνει το εσωτερικό δίκτυο ενός υπολογιστή από το υπόλοιπο διαδίκτυο, επιτρέποντας σε ορισμένα πακέτα να περνούν και μπλοκάροντας άλλα πακέτα. Ένα firewall επιτρέπει σε ένα διαχειριστή δικτύου να ελέγχει την προσπέλαση ανάμεσα στον έξω κόσμο και στους πόρους μέσα στο διαχειριζόμενο δίκτυο, διαχειριζόμενο την κίνηση προς και από αυτούς τους πόρους Υπάρχουν δύο τύποι firewalls: firewalls φιλτραρίσματος πακέτων (τα οποία λειτουργούν στο επίπεδο δικτύου) και firewalls επιπέδου εφαρμογής (τα οποία λειτουργούν στο επίπεδο εφαρμογής). Τα firewalls ελέγχουν τα εισερχόμενα και εξερχόμενα πακέτα δεδομένων και σύμφωνα με τους κανόνες που έχουν οριστεί από τον διαχειριστή του δικτύου επιτρέπουν να συνεχίσουν την πορεία τους ή διαφορετικά την φράζουν.

Τα firewalls επιτρέπουν την πρόσβαση σε εξουσιοδοτημένους χρήστες ενώαποκλείουν εκείνους οι οποίοι δεν έχουν δικαιώματα πρόσβασης. Γενικά αποτελεί ένα σύστημα το οποίο προστατεύει από την μη εξουσιοδοτημένη πρόσβαση προς ή από σε ένα ιδιωτικό δίκτυο.Firewalls μπορούν να υλοποιηθούν είτε με hardware είτε με software ή μεμσυνδυασμό αυτών των δύο. Σήμερα firewalls χρησιμοποιούνται συχνά για να

εμποδίζουν χρήστες του Internet να προσπελάσουν ιδιωτικά δίκτυα που συνδέονται με το Internet και ειδικότερα τα intranets. Όλα τα μηνύματα τα οποία εισέρχονται ήφεύγουν από το intranet περνούν διαμέσου του firewall, το οποίο εξετάζει κάθε μήνυμα και εμποδίζει να συνεχίσουν εκείνα τα οποία δεν ικανοποιούν δοθέντα κριτήρια. Μπορούμε να φανταστούμε ως firewall την πρώτη γραμμή της άμυνας στηνπροστασία ιδιωτικής πληροφορίας. Στην συνέχεια για μεγαλή ασφάλεια η πληροφορία θα πρέπει να κρυπτογραφηθεί.



5.4 ΣΧΕΔΙΑΣΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΕΝΟΣ FIREWALL

Κατά την σχεδίαση ενός firewall υπάρχουν ορισμένα στοιχεία τα οποία θα πρέπει να ληφθούν υπόψη. Τα στοιχεία αυτά αφορούν περισσότερο την πολιτική που θέλει να ακολουθήσει ένας οργανισμός για την πρόσβαση του στο Internet και όχι τόση στο καθαρά τεχνικό κομμάτι. Έτσι θα πρέπει να οριστούν αρχικά οι υπηρεσίες οι οποίες θέλουμε να περνούμε διαμέσου του firewall και ποιοί θα έχουν πρόσβαση σε αυτές.

Θα πρέπει να διευκρινιστεί αν το επιδιωκόμενο είναι μία λεπτομερής και αναλυτική πρόσβαση ή το απλό φιλτράρισμα.

Αφού οριστεί η πολιτική που θα ακολουθηθεί στο firewall στο επόμενο στάδιο δημιουργείται μια λίστα από το τι θα πρέπει να παρακολουθείται και να ελέγχεται και από το τι θα επιτρέπεται ή θα απορρίπτεται.

Στο τρίτο μέρος θα πρέπει να ληφθούν υπόψη τα οικονομικά στοιχεία της υλοποίησης ενός firewall. Στο σημείο αυτό υπάρχει αρκετή ασάφεια σχετικά με το κόστος της αγοράς ή το κόστος της κατασκευής. Έτσι υπάρχουν λύσεις οι οποίες περιλαμβάνουν την αγορά ενός router ή τον προγραμματισμό ενός Unix συστήματος. Η κατασκευή ενός firewall εξειδικευμένου στις ανάγκες ενός Οργανισμού μπορεί να απασχολήσει προσωπικό για αρκετούς μήνες και πάλι να μην υπάρχει η δυνατότητα να ελεγχθεί σε όλα του τα σημεία. Είναι φανερό όμως ότι θα λάβει υπόψη της η λύση αυτή καλύτερα όλες τις ειδικές ανάγκες Οργανισμού και το αποτέλεσμα αναμένεται καλύτερα προσαρμοσμένο σε αυτόν.

5.5 ΟΙ ΑΔΥΝΑΜΙΕΣ ΤΩΝ FIREWALL

Ένα firewall δεν αποτελεί ολοκληρωμένη λύση ασφαλείας. Για την κάλυψη κάποιων απειλών απαιτούνται άλλες συμπληρωματικές ενέργειες, όπως:

1. Μηχανισμοί φυσικής προστασίας
2. Ενσωμάτωση ασφάλειας σε επίπεδο εξυπηρετητή
3. Εκπαίδευση των χρηστών στο πλαίσιο του συνολικού πλάνου ασφάλειας.

Οι αδυναμίες των firewall είναι οι εξής:

1. Δεν μπορεί να προστατέψει από συνδέσεις που δεν διέρχονται από αυτό: παρέχει πλήρη προστασία μόνο αν ελέγχει όλη την περίμετρο του περιβάλλοντος. Για παράδειγμα να επιτρέπεται σε εσωτερικούς χρήστες συνδέονται με απευθείας PPP συνδέσεις με το Internet. Άλλο παράδειγμα αποτελεί ένα site που επιτρέπει ελεύθερα την πρόσβαση στους εσωτερικούς υπολογιστές και ελέγχει μόνο τα εξωτερικά αιτήματα.

2. Δεν μπορεί να προστατεύσει από προγράμματα-ιούς: τα firewalls δεν ασκούν σε βάθος έλεγχο των δεδομένων που εισέρχονται στο δίκτυο. Ο έλεγχος αφορά στις διευθύνσεις και στις θύρες πηγής και προορισμού και όχι στις λεπτομέρειες των δεδομένων. Έτσι απαιτείται σε κάθε υπολογιστή και ιδιαίτερα στους servers η χρήση antivirus λογισμικού.

3. Δεν μπορεί να προστατεύσει από επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού: Οι εσωτερικές απειλές απαιτούν εσωτερικά μέτρα ασφάλειας, όπως ασφάλεια σε επίπεδο ξενιστή (host)και εκπαίδευση των χρηστών. Οι χρήστες πρέπει να ενημερωθούν σχετικά με τις διάφορες απειλές, τη σημασία της μυστικότητας του συνθηματικού τους και περιοδικής αλλαγής του.

4. Δεν μπορεί να προστατέψει τον οργανισμό από επιθέσεις σχετιζόμενες με δεδομένα: συμβαίνουν όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρετητές του οργανισμού, είτε μέσω e-mail,είτε διαμέσου της αντιγραφής από δισκέτα και εκτελούνται με σκοπό να εξαπολύσουν επίθεση εναντίον του συστήματος. Π. χ. μια επίθεση θα μπορούσε να οδηγήσει σε μεταβολή των αρχείων προνομίων.

5. Δεν μπορεί να προστατεύσει από απειλές άγνωστου τύπου: δεν μπορεί να αμυνθεί αυτομάτως σε νέες απειλές που προκύπτουν κατά καιρούς.

6. Η αυστηρή ρύθμιση ασφάλειας διαμέσου του firewall: είναι δυνατό ένα firewall να ρυθμιστεί με πολύ αυστηρό τρόπο με αποτέλεσμα να μην επιτρέπει τη δικτύωσης ή να προκαλεί δυσαρέσκεια στους χρήστες εξαιτίας των πολλών ελέγχων, των πολλαπλών επιπέδων ασφαλείας και κατά συνέπεια της συνολικής ελαττωμένης φιλικότητας και μειωμένης ευχρηστίας .

5.6 ΖΗΤΗΜΑΤΑ ΣΧΕΔΙΑΣΗΣ ΤΩΝ FIREWALL

Η υλοποίηση ενός firewall δεν αποτελεί τετριμμένο θέμα και δεν παρέχεται ενσωματωμένη σε κανένα λειτουργικό σύστημα. Ο λόγος είναι ότι ένα firewall αποτελεί περισσότερο φιλοσοφία προστασίας και λιγότερο υλικό και λογισμικό που παρέχει πλήρη προστασία από κάθε εξωτερική απειλή. Υπάρχει μια αντίληψη ότι το firewall εξασφαλίζει την πλήρη προστασία ενός δικτύου απέναντι σε κάθε είδους απειλή η οποία είναι τελείως λανθασμένη και μπορεί να οδηγήσει το διαχειριστή ασφάλειας ενός οργανισμού στην καταστροφική άποψη ότι με την εγκατάσταση ενός firewall είναι εγγυημένη η ασφάλεια του εσωτερικού δικτύου του οργανισμού την οποία διαχειρίζεται.

Η εγκατάσταση ενός firewall αποτελεί σημαντική σχεδιαστική απόφαση για τους παρακάτω λόγους:

1) Η εγκατάσταση ενός firewall επιφέρει καθυστέρηση στο χρόνο απόκρισης των προγραμμάτων που υλοποιούν τις υπηρεσίες που παρέχει η ιστοθέση.

5.7 ΕΓΚΑΤΑΣΤΑΣΗ ΕΝΟΣ FIREWALL

Η εγκατάσταση ενός firewall περιλαμβάνει μια σειρά διαδοχικά εκτελούμενων φάσεων.
Αυτές είναι:

Σχεδιασμός Πολιτικής.

Ο σχεδιασμός ενός firewall προϋποθέτει τον ακριβή προσδιορισμό των ορίων των διακριτών περιοχών ασφάλειας του δικτύου, καθεμιά από τις οποίες λειτουργεί με βάση συγκεκριμένη πολιτική ασφάλειας. Στη συνέχεια επιλέγονται:

- Η βασική αρχιτεκτονική (αριθμός υπολογιστών, μέθοδοι συνδέσεων, λειτουργίες που εκτελούνται).
- Οι λειτουργίες που θα υλοποιηθούν (επίπεδο δικτύου, επίπεδο εφαρμογής, υβριδικός συνδυασμός).
- Το αρχιτεκτονικό σχέδιο του firewall (διπλοσυνδεδεμένο, με υπολογιστή διαλογής, με υποδίκτυο διαλογής).

Απόκτηση υλικού και λογισμικού για firewalls.

Στη φάση αυτή εξασφαλίζεται η ύπαρξη του κατάλληλου εξοπλισμού (υλικό και λογισμικό), για να είναι δυνατή η εγκατάσταση, ο δοκιμαστικός έλεγχος, η λειτουργία και η επίβλεψη του firewall. Συγκεκριμένα εκτελείται:

- Προσδιορισμός των απαραίτητων τμημάτων υλικού (υπολογιστές, δρομολογητές, επεξεργαστές, μνήμη, δίσκος, κάρτες, καλώδια κλπ).

- Προσδιορισμός των απαραίτητων τμημάτων λογισμικού (λειτουργικά συστήματα, patches, device drivers, λογισμικό firewall, λογισμικό παρακολούθησης δικτύου).

Απόκτηση τεκμηρίωσης, εκπαίδευσης και υποστήριξης.

Ανάλογα με τον επιλεγέντα αρχιτεκτονικό σχεδιασμό, πιθανότατα απαιτείται επιπρόσθετη εκπαίδευση και υποστήριξη από την προμηθεύτρια εταιρεία. Εάν ο οργανισμός δε διαθέτει εμπειρία στις τεχνολογίες που πρόκειται να υλοποιήσει, υπάρχει σοβαρό ενδεχόμενο να οδηγηθεί σε σφάλματα που θα μπορούσαν να προκαλέσουν καθυστέρηση στην εγκατάσταση, στη ρύθμιση και στη λειτουργία του firewall. Επιπλέον η συντήρηση του υλικού και του λογισμικού μπορεί να είναι τόσο περίπλοκη ώστε να απαιτείται εκπαίδευση και συνεχής υποστήριξη. Όλα αυτά πρέπει να μελετηθούν λεπτομερώς στη φάση αυτή.

Εγκατάσταση υλικού και λογισμικού.

Στη φάση αυτή εγκαθίσταται και ρυθμίζεται το λειτουργικό σύστημα που θα υποστηρίξει το λογισμικό του firewall. Το λειτουργικό σύστημα περιλαμβάνει μόνο τις υπηρεσίες που είναι απαραίτητες για τη λειτουργία του firewall, ενώ όλες οι υπόλοιπες υπηρεσίες πρέπει να είναι απενεργοποιημένες. Στη συνέχεια το λογισμικό του firewall εγκαθίσταται στο επιλεγμένο υλικό για δοκιμαστικό έλεγχο.

Ρύθμιση της δρομολόγησης.

Όταν ένα πακέτο φτάνει σε ένα δρομολογητή, ο δρομολογητής πρέπει να αποφασίσει για τη διάθεση του. Στόχοι του μηχανισμού δρομολόγησης είναι η απόδοση και η αξιοπιστία, όχι η υλοποίηση πολιτικής ασφάλειας.

Ρύθμιση των κανόνων φιλτραρίσματος πακέτων.

Ο μηχανισμός φιλτραρίσματος ελέγχει το περιεχόμενο του πακέτου και με βάση ορισμένα κριτήρια και κανόνες υλοποιεί την πολιτική ασφάλειας αποφασίζοντας για την προώθηση ή απόρριψη του πακέτου. Εάν στην αρχιτεκτονική σχεδίαση περιλαμβάνονται και proxy servers, τότε πρέπει στη φάση αυτή να εγκατασταθεί το λογισμικό για κάθε υποστηριζόμενη υπηρεσία.

Ρύθμιση μηχανισμών καταγραφής και έγκυρης προειδοποίησης.

Στη φάση αυτή πρέπει να γίνει επιλογή των περιπτώσεων φιλτραρίσματος πακέτων που θα καταγράφονται. Επιπλέον θα πρέπει να οριστούν εκείνα τα συμβάντα για τα οποία πρέπει να σημάνει συναγερμός.

Έλεγχος στο σύστημα firewall.

Το σύστημα ελέγχεται στο περιβάλλον δοκιμών για τυχόν λάθη και ελλείψεις με χρήση συστημάτων ανίχνευσης εισβολής, σαρωτών θυρών (ports scanners), εργαλείων ανίχνευσης αδυναμιών, εργαλείων παραγωγής κίνησης στο δίκτυο και εργαλείων παρακολούθησης δικτύων. Επιπλέον εκτελούνται πιθανά σενάρια για επιβεβαίωση της ορθής λειτουργίας του firewall.

Εγκατάσταση του firewall.

Αν το firewall πρόκειται να συνδέσει δύο ασύνδετα δίκτυα, τότε εγκαθίσταται σταδιακά. Αν το firewall πρόκειται να αντικαταστήσει ένα υπάρχον σύστημα, τότε το firewall εγκαθίσταται παράλληλα με τη λειτουργία του υπάρχοντος συστήματος, προσέχοντας πάντοτε να μην επηρεαστεί το παραγωγικό περιβάλλον λειτουργίας.

ΚΕΦΑΛΑΙΟ 6^{ο}

Η ΧΡΗΣΙΜΟΤΗΤΑ ΤΩΝ ΔΡΟΜΟΛΟΓΗΤΩΝ ΚΑΙ ΤΩΝ ΔΙΑΜΟΡΦΩΤΩΝ

6.1 ΟΡΙΣΜΟΣ ΔΡΟΜΟΛΟΓΗΤΗ

Ο Router είναι συσκευή στην οποία συνδέονται περισσότεροι του ενός ηλεκτρονικοί υπολογιστές ενός τοπικού δικτύου. Ο δρομολογητής αναλαμβάνει τη μεταβίβαση των δεδομένων από και προς τον κατάλληλο υπολογιστή του δικτύου, με βάση συγκεκριμένα κριτήρια που θέτει ο διαχειριστής του, όπως διεύθυνση IP, κανόνες NAT. Ένας δρομολογητής (router) αναλαμβάνει τη διασύνδεση μεταξύ δύο δικτύων, συνήθως ενός τοπικού ασύρματου (WLAN) και ενός τοπικού ενσύρματου (LAN), οπότε έχουμε λόγο για έναν Wireless Router, είτε ενός τοπικού ενσύρματου (LAN) και ενός ευρέους δικτύου (WAN), όπως είναι το Internet για συνδέσεις μέσω xDSL (2), οπότε έχουμε xDSL Router.

Ένας router δρομολογεί κατάλληλα τα δεδομένα από ένα δίκτυο σε συγκεκριμένο τερματικό άλλου δικτύου. Συνήθως έχει δύο IP διευθύνσεις, και έχει τη δυνατότητα να συνδεθεί με παραπάνω από έναν υπολογιστές. Στο παράδειγμα του xDSL Router, η πρώτη IP διεύθυνση ανήκει στο Range του εσωτερικού δικτύου και χρησιμεύει στη σύνδεση υπολογιστών μέσω τοπικού δικτύου στον router. Η δεύτερη IP διεύθυνση αντιστοιχεί στη διεύθυνση που έχει αποκτηθεί είτε δυναμικά είτε στατικά από τον πάροχο Internet (ISP) και είναι η "εξωτερική" διεύθυνση του δρομολογητή, στην οποία πρέπει να απευθυνθεί οποιοσδήποτε θέλει να επικοινωνήσει με κάποιον υπολογιστή του Τοπικού Δικτύου.

Ο router, με κατάλληλες διαδικασίες, αναλαμβάνει να δρομολογήσει τα εισερχόμενα πακέτα, στον κατάλληλο υπολογιστή. Οι περισσότεροι routers της αγοράς, έχουν την δυνατότητα NAT και μπορούν να κάνουν Port Forwarding, δηλαδή αντιστοίχιση συγκεκριμένης πόρτας σε συγκεκριμένη διεύθυνση IP του Τοπικού Δικτύου. Παράδειγμα: έστω η διεύθυνση του router στο Ίντερνετ xx.xx.xx.xx, προσπάθεια επικοινωνίας σε συγκεκριμένη πόρτα, (στο παράδειγμα μας 1234) η οποία γίνεται χρησιμοποιώντας τη διεύθυνση xx.xx.xx.xx:1234, θα κάνει τον router να αντιληφθεί ότι κάποιος υπολογιστής προσπαθεί να επικοινωνήσει μέσω της θύρας 1234 μαζί του. Ο router, όντας ρυθμισμένος να προωθεί σε μια στατική διεύθυνση του Τοπικού Δικτύου (πχ 10.0.0.2) όλα τα εισερχόμενα πακέτα που καταφθάνουν μέσω της θύρας 1234 σε αυτό, θα προωθήσει τα πακέτα στη διεύθυνση 10.0.0.2. Έτσι, κάποιος που προσπαθεί να επικοινωνήσει με τη διεύθυνση xx.xx.xx.xx:1234, στην ουσία επικοινωνεί με τον υπολογιστή του Τοπικού Δικτύου που βρίσκεται συνδεδεμένο "πίσω" από το router, με διεύθυνση IP 10.0.0.2.

6.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΔΡΟΜΟΛΟΓΗΤΩΝ

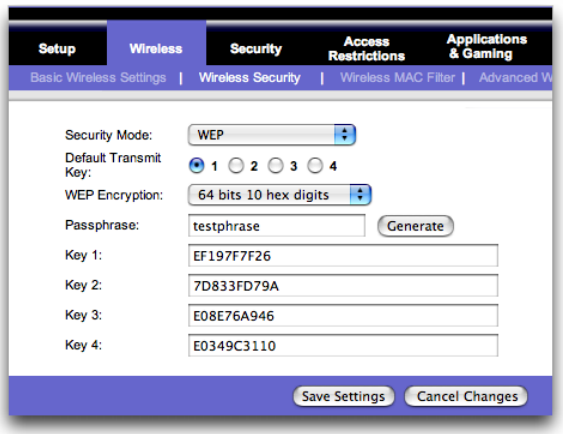
Τα χαρακτηριστικά των δρομολογητών είναι τα εξής:

1. Any IP: το χαρακτηριστικό αυτό επιτρέπει την επικοινωνία Η/Υ με το Internet ακόμη και αν ο Η/Υ έχει IP που ανήκει σε διαφορετικό υποδίκτυο (subnet) από ότι η IP του δρομολογητή.
2. Content Filtering (Έλεγχος Πρόσβασης): η λειτουργία Ελέγχου Πρόσβασης επιτρέπει την φραγή συγκεκριμένων ιστοσελίδων.
3. Media Bandwidth: η λειτουργία διαχείρισης του εύρους ζώνης (Bandwidth Management) επιτρέπει την κατανομή του ανά εφαρμογή ή υποδίκτυο.
4. NAT: το NAT επιτρέπει τη μετάφραση μίας εσωτερικής IP του δικτύου σε μία άλλη γνωστή στο Internet.
5. DHCP: σημαίνει ότι ο δρομολογητής διαθέτει ενσωματωμένο DHCP server. Με βάση αυτό οι Η/Υ μπορούν να λάβουν TCP/IP παραμετροποίηση από τον δρομολογητή, κατά την εκκίνησή τους.

6.3WPA/WEP

WPA
Το Wi-Fi Protected Access (WPA) είναι ένα στοιχείο του πρότυπου ασφαλείας IEEE 802.11i. Εξέλιξη του WPA είναι το WPA2 το οποίο είναι ισχυρότερο πρότυπο ασφαλείας όσο αφορά την κρυπτογράφηση, την πιστοποίηση και τη διαχείριση των κλειδιών κρυπτογράφησης.
Τόσο το WPA όσο και το WPA2 βελτιώνουν την κρυπτογράφηση των δεδομένων με χρήση Temporal Key Integrity (TKIP), Message Integrity Check (MIC) και IEEE 802.1x. επιπροσθέτως, εκτός από TKIP, το WPA2 χρησιμοποιεί το Adnanced Encryption Standard (AES) επιτυγχάνοντας ισχυρότερη κρυπτογράφηση.

WEP
Το Wired Equivalent Privacy κρυπτογραφεί τα δεδομένα πριν μεταδοθούν μέσω του ασύρματου δικτύου, διατηρώντας την ιδιωτικότητα των επικοινωνιών μέσω του ασύρματου δικτύου.



Οι βασικές διαφορές μεταξύ WPA και WEP είναι η πιστοποίηση και ο βελτιωμένος τρόπος κρυπτογράφησης. Συγκεκριμένα:

1. NAT: Ένα πρότυπο που βρίσκει εφαρμογή σε τοπικά δίκτυα των οποίων οι υπολογιστές μοιράζονται μια κοινή σύνδεση Internet. Το NAT, ορίζει σε κάθε ηλεκτρονικό υπολογιστή του τοπικού δικτύου μια διαφορετική εσωτερική διεύθυνση IP, της μορφής 192.168.x.x ή 10.1.x.x και μια κοινή εξωτερική IP με την οποία αναγνωρίζονται από άλλα συστήματα συνδεδεμένα στο Internet.

   Το NAT βρίσκει εφαρμογή σε ιδιωτικά και εταιρικά δίκτυα που συνδέονται στο Internet μέσω routers και συνδέσεων ADSL ή μισθωμένων γραμμών. Πολλές φορές ο διαχειριστής των δικτύων αυτών θα πρέπει να ρυθμίσει κατάλληλα τους κανόνες NAT, ώστε να είναι εφικτή η πρόσβαση από το Internet σε υπηρεσίες και εφαρμογές που εκτελούνται σε συγκεκριμένο υπολογιστή του εσωτερικού δικτύου. Η ρύθμιση αυτή ονομάζεται και port forwarding. Επειδή όλοι οι ηλεκτρονικοί υπολογιστές εμφανίζονται στο διαδίκτυο με την ίδια διεύθυνση IP, ένας κανόνας NAT ή port forwarding καθορίζει σε ποιον από όλους θα πρέπει να αναζητηθεί μια συγκεκριμένη υπηρεσία. Αυτό γίνεται με την αντιστοίχιση του port της εν λόγω υπηρεσίας (π.χ. port 80 για HTTP server) στην εσωτερική διεύθυνση του υπολογιστή του τοπικού δικτύου όπου αυτή εκτελείται.

   Η υπηρεσία UPnP (Universal Plug and Play) που υποστηρίζεται σήμερα από πολλές εφαρμογές, λειτουργικά συστήματα και routers έχει περιορίσει σημαντικά την ανάγκη καθορισμού κανόνων NAT,.

2. xDSL: Οικογένεια πρωτοκόλλων τηλεφωνικών συνδέσεων υψηλής ταχύτητας, που περιλαμβάνει τα πρωτόκολλα ADSL, HDSL,DSL Lite, SDSL, RADSL, VDSL.

3. Το IRC (Internet Relay Chat) είναι ένας τρόπος συνομιλίας ανάμεσα σε ανθρώπους σε ολόκληρη τη γη, οι οποίοι απλά χρησιμοποιούν το πληκτρολόγιο του υπολογιστή τους. Οι λέξεις που τυπώνουν αναμεταδίδονται αμέσως σε οποιονδήποτε υπολογιστή σε όλο τον κόσμο και οι αποδέκτες τους μπορούν να τις διαβάσουν. Αυτή η διαδικασία πραγματοποιείται σε πραγματικό χρόνο (real time) που σημαίνει ότι ο καθένας μπορεί να δει τις λέξεις όπως και αυτός που τις γράφει.

   Το IRC τρέχει πάνω στο μοντέλο client/server, οπότε για να το χρησιμοποιήσετε θα πρέπει να τρέχετε κάποιο πρόγραμμα client στον υπολογιστή σας. Υπάρχουν πολλά τέτοια προγράμματα διαθέσιμα για υπολογιστές που τρέχουν Windows, για Macintoshes, για Unix και γενικά για κάθε τύπο υπολογιστή. Όταν λοιπόν θέλετε να συνομιλήσετε, αφού πρώτα μπείτε στο Internet θα πρέπει να ξεκινήσετε το client πρόγραμμά σας. Μετά, θα χρειαστεί να συνδεθείτε σε έναν IRC server που βρίσκεται τοποθετημένος στο Internet. Ο αριθμός αυτών των servers είναι πολύ μεγάλος, οπότε δεν θα δυσκολευτείτε να κάνετε την σύνδεση. Όλοι αυτοί οι servers είναι συνδεδεμένοι σε ένα δίκτυο ώστε να μπορούν να στέλνουν μηνύματα ο ένας στον άλλο.

   Η μορφή της σύνδεσης είναι όπως ενός δένδρου με τα κλαδιά του, δηλαδή ο κάθε server μπορεί να επικοινωνεί με τους άλλους, αλλά κανένας δεν συνδέεται κατευθείαν με τον άλλο. Αφού λοιπόν συνδεθείτε σε έναν server, διαλέγετε ένα συγκεκριμένο κανάλι που σας ενδιαφέρει και επιλέγετε ένα όνομα με το οποίο θα σας αναγνωρίζουν κάθε φορά που θα συνδέεστε.Υπάρχουν πολλά κανάλια

διαθέσιμα, το καθένα με διαφορετικό θέμα. Μόλις μπείτε στο κανάλι, θα μπορέσετε να δείτε τις συνομιλίες που γίνονται εκείνη την στιγμή. Για να πάρετε μέρος στην συζήτηση πληκτρολογείστε το μήνυμα σας και στείλτε το. Το πρόγραμμα IRC που τρέχετε θα στείλει το μήνυμα σας στον IRC server που είστε συνδεδεμένοι.

Σύμφωνα τώρα με την μορφή του δέντρου, που αναφέραμε πιο πριν, το μήνυμα θα σταλεί από τον server σας στους άλλους επιλέγοντας την πιο σύντομη διαδρομή ώστε τελικά να φτάσει στους servers που είναι συνδεδεμένα τα άτομα που βρίσκονται μέσα στο κανάλι. Τελικά ο κάθε server θα στείλει το μήνυμα σας στο client πρόγραμμα το οποίο θα το εμφανίσει στην οθόνη του υπολογιστή που βρίσκεται στην άλλη άκρη της γραμμής ώστε να μπορεί να το διαβάσει κάποιος και να ανταποκριθεί στέλνοντας το δικό του μήνυμα από τον υπολογιστή του.

4. ADSL : Σε κάθε γραμμή υπάρχουν 2 ADSL modems, ένα από την πλευρά του συνδρομητή και ένα από την πλευρά της τηλεφωνικής εταιρείας. Οι ταχύτητες μετάδοσης δεδομένων που επιτυγχάνει το ADSL είναι 1,5 έως 9 Mbps για download και έως 800 Kbps για upload δεδομένων. Χρησιμοποιεί τα κοινά (χάλκινα) τηλεφωνικά καλώδια που υπάρχουν ήδη στις τηλεφωνικές γραμμές. Όπως και το ISDN, περιλαμβάνει κανάλια φωνής και δεδομένων. Στην Ελλάδα θα αρχίσει να παρέχεται σε λίγο καιρό από τον ΟΤΕ (λειτουργεί ήδη σε πειραματικό στάδιο). Προέρχεται από τα αρχικά Asymmetric Digital Subscriber Line. Συνήθως απαιτείται από την πλευρά του συνδρομητή η εγκατάσταση DSL modem που θα κάνει διαχωρισμό των καναλιών φωνής και δεδομένων. DSL Lite: Παραλλαγή του ADSL υπό εξέλιξη. Ο διαχωρισμός καναλιών φωνής και δεδομένων γίνεται από την τηλεφωνική εταιρεία. Έχει μικρότερο κόστος και πολυπλοκότητα από το ADSL, αλλά η ταχύτητα περιορίζεται στα 1,544 Mbps.

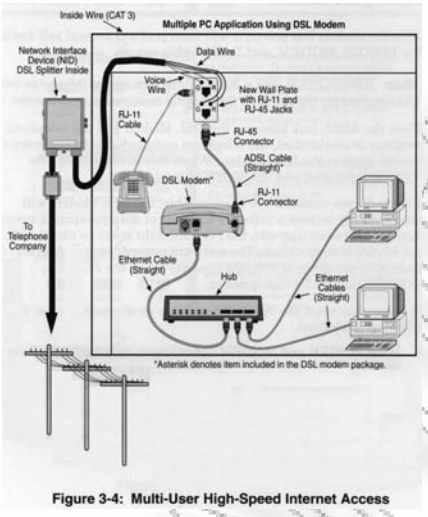
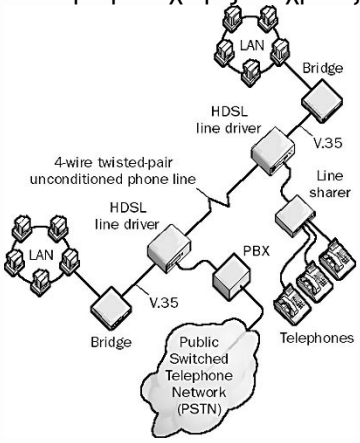


Figure 3-4: Multi-User High-Speed Internet Access

5. HDSL: διαφέρει από το ASDL στο ότι είναι συμμετρικό, δηλαδή έχει τις ίδιες ταχύτητες για upload και download. Δίνει ίδια ταχύτητα μετάδοσης με το T1, 1,544 Mbps. Από τα αρχικά High bit-rate Digital Subscriber Line. Χρησιμοποιεί δύο ζεύγη καλωδίων και μπορεί να μεταδόσει δεδομένα σε ακτίνα

4500 μέτρων χωρίς να χρειάζεται επαναλήπτης για να ενισχύει το σήμα και να το επανακατευθύνει.



6. SDSL - Single line Digital Subscriber Line: το ίδιο με το HDSL, μόνο που χρησιμοποιεί ένα ζεύγος καλωδίων αντί για δύο και η ακτίνα μετάδοσης δεδομένων χωρίς χρήση repeater είναι 3000 μέτρα αντί για 4500.
7. RADSL - Rate Adaptive Digital Subscriber Line: παρόμοιο με το ADSL, αλλά κατάλληλο πρόγραμμα, ρυθμίζει αυτόματα την ταχύτητα μετάδοσης ανάλογα με διάφορους παράγοντες, όπως η ποιότητα της τηλεφωνικής γραμμής και η απόσταση που πρέπει να διανύσει η μετάδοση των πληροφοριών. Στις συνδέσεις RADSL, οι μεταδόσεις μπορούν να φτάσουν τα 2,2 Mbps για κατέβασμα και 1,088 Mbps γιαανέβασμα.

8. VDSL - Very High rate Digital Subscriber Line: μορφή του DSL που βρίσκεται υπό εξέλιξη και δίνει τη μεγαλύτερη, μέχρι αυτή τη στιγμή, ταχύτητα μετάδοσης δεδομένων: 52 Mbps για download και 2,3 Mbps για upload. Σημαντικό μειονέκτημά της όμως είναι ότι λειτουργεί μόνο σε αποστάσεις μικρότερες από 1300 μέτρα.

   ADSL: Τεχνολογία για τη διαβίβαση ψηφιακών πληροφοριών σε υψηλό εύρος ζώνης πάνω από τις υπάρχουσες τηλεφωνικές γραμμές. Αντίθετα από την κανονική τηλεφωνική υπηρεσία dial-up, το ADSL παρέχει συνεχή σύνδεση.

9. Το ADSL χρησιμοποιεί ασύμμετρη ροή δεδομένων, δεδομένου ότι χρησιμοποιεί το μεγαλύτερο μέρος γι α αν
   Μεταφέρει ταυτόχρονα τις αναλογικές πληροφορίες (φωνής) στην ίδια γραμμή. Προσφέρεται γενικά για μεταφορά δεδομένων με ταχύτητες που κυμαίνονται από 256 Kbps μέχρι 6 Mbps. Μια μορφή ADSL, γνωστή ως universal ADSL ή G.lite, έχει εγκριθεί ως πρότυπο από το ITU-TS.

Χρησιμοποιήστε αυτό το διαγνωστικό εργαλείο της Microsoft (Internet Connectivity Evaluation Tool) για να δείτε τι διαδικτυακές τεχνολογίες ο δρομολογητής σας υποστηρίζει. Απαραίτητη προϋπόθεση λειτουργικό σύστημα Windows Vista ή Windows XP. Η χρήση του με λειτουργικά συστήματα διαφορετικών από τα αναφερόμενα θα δώσει ανακριβή αποτελέσματα.

6.4 ΔΙΑΜΟΡΦΩΤΕΣ

Οι Η/Υ μπορούν να συνδεθούν μεταξύ τους με ειδικά καλώδια και software. Σ΄αυτή την περίπτωση υπάγονται τα τοπικά δίκτυα. Στα τοπικά δίκτυα οι Η/Υ που είναι συνδεδεμένοι μεταξύ τους δεν μπορούν να έχουν απεριόριστες αποστάσεις. Μια εταιρεία για παράδειγμα που διαθέτει γραφεία σε κάποια πολυόροφη πολυκατοικία ή ακόμα και σε διπλανές, μπορεί να δημιουργήσει και να χρησιμοποιεί ένα τοπικό δίκτυο. Αν όμως η ίδια εταιρεία έχει και διάφορα παραρτήματα σε διαφορετικές συνοικίες της πόλης ή ακόμα σε

διαφορετικές πόλεις και χώρες τότε ο μοναδικός τρόπος για να συνδέσει μεταξύ τους Η/Υ είναι τα καλώδια των τηλεπικοινωνιακών δικτύων, και συγκεκριμένα για τους Έλληνες τα καλώδια του ΟΤΕ. Εδώ θα ανοίξουμε μια μικρή παρένθεση για να τονίσουμε ότι τα τοπικά δίκτυα χρησιμοποιούν ένα ειδικό ομοαξονικό καλώδιο μέσα από το οποίο η ταχύτητα μεταφοράς των δεδομένων είναι μέχρι 10 Mbit το δευτερόλεπτο. Το καλώδιο αυτό χρησιμοποιείται και από την καλωδιακή τηλεόραση. Αντίθετα με αυτό το καλώδιο υπάρχει σήμερα και το καλώδιο οπτικών ινών το οποίο τελευταία χρησιμοποιεί και ο ΟΤΕ. Το καλώδιο αυτό αποτελείται από ίνες γυαλιού. Η μεταφορά των δεδομένων σήμερα μέσα απ΄αυτό, είναι της τάξης των 100Mbit ανά δευτερόλεπτο, η θεωρητική του ταχύτητα είναι φοβερά μεγάλη. Για να γίνει χειροπιαστά κατανοητό αναφέρουμε ότι ένας παλμός φωτός μπορεί να διανύσει 40.000 περίπου χιλιάδες χιλιόμετρα (τον γύρο της γης) σε 1/8 του δευτερολέπτου. Ο τρόπος λειτουργίας του είναι ότι μεταφέρει δεδομένα εκπέμποντας παλλόμενες δέσμες φωτός αντί ηλεκτρικών συχνοτήτων. Το μεγαλύτερο πλεονέκτημα του καλωδίου οπτικών ινών, πέρα από την μεγάλη ταχύτητα είναι ότι δεν επηρεάζεται από ηλεκτρομαγνητικές παρεμβολές, οι οποίες προκαλούν σφάλματα κατά τη μετάδοση.

Τα modem είναι συσκευές οι οποίες συνδέουν μεταξύ τους Η/Υ. Επειδή το Internet είναι ένα παγκόσμιο δίκτυο που συνδέει χιλιάδες Η/Υ μεταξύ τους, το modem είναι η απαραίτητη συσκευή γι΄αυτή τη σύνδεση. Το modem παρεμβάλλεται συνήθως μεταξύ του Η/Υ και της τηλεφωνικής μας συσκευής. Χρησιμοποιώ τη λέξη συνήθως επειδή οι περισσότεροι χρήστες χρησιμοποιούν την βασική τηλεφωνική γραμμή τους. Αυτό βέβαια σημαίνει ότι όταν χρησιμοποιούμε το modem θα είναι κατελλειμένη η τηλεφωνική μας γραμμή σαν να μιλούσαμε στο τηλέφωνο με κάποιον άλλον. Το ίδιο βέβαια συμβαίνει και με το Fax. Μερικές εταιρείες διαθέτουν κάποια τηλεφωνική γραμμή αποκλειστικά για το Fax ή για το modem.

Πριν από την μεγάλη εξάπλωση του Internet, όταν επιθυμούσαμε να συνδεθούμε με τον Η/Υ κάποιου φίλου μας, μιας εταιρείας, κάποιου συνεργάτη μας κλπ, προμηθευόμασταν από ένα modem ο καθένας και έτσι επιτυγχάναμε τον σκοπό μας. Με την σύνδεση αυτή έχουμε τη δυνατότητα να αποστέλλουμε και να λαμβάνουμε αρχεία από τον απομακρυσμένο Η/Υ με τον οποίο είμαστε συνδεδεμένοι, μπορούμε επίσης να χειριζόμαστε τα αρχεία του απομακρυσμένου Η/Υ και γενικότερα να εργαζόμαστε σ΄αυτόν σαν να τον έχουμε στο γραφείο μας.

Ο τρόπος της παραπάνω σύνδεσης έλυνε και λύνει αρκετά προβλήματα αλλά υπάρχει το μεγάλο μειονέκτημα της χρέωσης. Όταν είμαστε συνδεδεμένοι με κάποιο Η/Υ μέσω modem, ο οποίος βρίσκεται σε άλλη πόλη ή ακόμα χειρότερα σε άλλη χώρα η δαπάνη της τηλεφωνικής χρέωσης είναι πολύ μεγάλη λόγω υπεραστικής χρέωσης. Αυτός είναι και ο λόγος που παρόλο τα modem είναι φθηνές συσκευές, δεν χρησιμοποιήθηκαν ποτέ άσκοπα από τους χρήστες.

Σήμερα, με την θυελλώδη είσοδο του Internet έχουν αυξηθεί κατακόρυφα οι πωλήσεις των modems επειδή η χρέωση σ΄αυτό είναι αστική και όχι υπεραστική άσχετα αν εμείς βρισκόμαστε σε Η/Υ της Αμερικής της Ευρώπης ή της Ελλάδας.

Επομένως, για να συνδέσουμε τον Η/Υ μας με κάποιον άλλο είτε μέσω του Internet είτε έξω από αυτό, πρέπει οι Η/Υ που θα συνδεθούν πρέπει να είναι εφοδιασμένοι και οι δυο με ένα modem.

Ο λόγος που καθιστά απαραίτητη τη χρήση του modem για την σύνδεση δυο Η/Υ είναι τα σήματα της μετάδοσης. Οι Η/Υ λειτουργούν ψηφιακά, δηλαδή μεταδίδουν τα δεδομένα σε ψηφιακή μορφή ενώ τα καλώδια στην τηλεπικοινωνία μεταδίδουν τη φωνή μας σαν αναλογικό σήμα. Επομένως πρέπει να παρεμβάλουμε μια συσκευή ανάμεσα στους Η/Υ η οποία θα μετατρέπει το ψηφιακό σε αναλογικό σήμα για να μπορέσει να διοχετευθεί μέσα από τα καλώδια του ΟΤΕ. Οι συσκευές που κάνουν αυτές τις μετατροπές είναι τα Modem.

Το modem λοιπόν είναι μια συσκευή που έχει τη δυνατότητα να δέχεται αναλογικά σήματα και να τα μετατρέπει σε ψηφιακά, αλλά και το αντίθετο. Το όνομά του βγαίνει από τις λέξεις Modulation (διαμόρφωση ψηφιακού σε αναλογικό σήμα) και Demodulation (αποδιαμόρφωση του σήματος από αναλογικό σε ψηφιακό). Τα αρχικά προθέματα Mo από το Modulation και το Dem από το Demodulation έδωσαν το όνομα στο Modem.

Εδώ θα πρέπει να σημειώσουμε ότι η ψηφιακή τεχνολογία που χρησιμοποιεί το τηλεπικοινωνιακό δίκτυο είναι διαφορετική από αυτή των Η/Υ, επομένως, για να μη γίνεται σύγχυση με τα λεγόμενα αναλογικά και ψηφιακά τηλέφωνα που παρέχει ο ΟΤΕ, εμείς πρέπει να έχουμε στο νου μας ότι είτε από τα μεν είτε από τα δε, το σήμα της φωνής μεταδίδεται μέσα από τα καλώδιά του σαν αναλογικό.

6.5 ΕΙΔΗ ΤΩΝ ΔΙΑΜΟΡΦΩΤΩΝ

Τα modem που κυκλοφορούν σήμερα στην αγορά, όσον αφορά την κατασκευή τους και τον τρόπο σύνδεσής τους είναι δυο ειδών, τα Εσωτερικά και τα Εξωτερικά.

Τα εσωτερικά είναι όπως μια οποιαδήποτε ηλεκτρονική κάρτα η οποία τοποθετείται σε κάποιο slot του Η/Υ, ενώ τα εξωτερικά τοποθετούνται έξω από την κεντρική μονάδα και συνδέονται με αυτόν με κάποιο καλώδιο. Η σύνδεση των modem με τον Η/Υ γίνεται μέσω της σειριακής θύρας, αν και υπάρχουν και σπάνιες περιπτώσεις όπου συνδέονται σε παράλληλες θύρες του εκτυπωτή επειδή αυτές είναι ταχύτερες. Τα εξωτερικά modem δεν απασχολούν slots του Η/Υ, διαθέτουν ενδείξεις με λαμπάκια led τα οποία μας εμφανίζουν συνεχώς το είδος της λειτουργίας τους. Άλλο πλεονέκτημα είναι το γεγονός ότι αν "κολλήσει" ή κάτι και δεν πάει καλά μπορούμε να σβήσουμε το modem χωρίς να είμαστε υποχρεωμένοι να θέσουμε εκτός λειτουργίας τον Η/Υ μας.

Τα εξωτερικά λοιπόν modem συνδέονται σε κάποια από τις σειριακές θύρες του Η/Υ ή σε μια RS232 ενώ τα εσωτερικά διαθέτουν δική τους ενσωματωμένη σειριακή θύρα. Αυτό αποτελεί ένα πλεονέκτημα των εσωτερικών Modem επειδή δεν απασχολούν καμιά σειριακή θύρα του Η/Υ επομένως μπορούμε να συνδέσουμε εκεί κάποια άλλη συσκευή. Μεταξύ των άλλων συσκευών που χρησιμοποιούν σειριακή θύρα είναι το ποντίκι.

Τα εσωτερικά modem είναι φθηνότερα από τα εξωτερικά επειδή δεν διαθέτουν το κουτί, το τροφοδοτικό και τα καλώδια. Τα εσωτερικά είναι πολύ δύσκολα στην τοποθέτηση και στην ρύθμιση από αρχάριους γιατί συνήθως συγκρούονται με άλλες υπάρχουσες συσκευές του Η/Υ.

Ένας άλλος διαχωρισμός που γίνεται στα modem είναι το αν διαθέτουν συγχρόνως Fax, Voice ή αυτόματο τηλεφωνητή. Σήμερα όλα σχεδόν τα modem που είναι 28.800 bps είναι συγχρόνως Fax και Voice. Αυτό σημαίνει ότι έχουν την δυνατότητα να χρησιμοποιούνται και σαν συσκευές Fax με ειδικά software όπως είναι το Exchange της Microfoft (Η Microsoft κατά τη γνώμη μου θα πρέπει να το τροποποιήσει ή να το καταργήσει γιατί είναι φοβερά πολύπλοκο και δυσκίνητο). Με την αγορά κάθε modem οι εταιρείες μας εφοδιάζουν με μερικές δισκέτες οι οποίες περιέχουν κάποια εφαρμογή για Fax. Μερικοί παροχείς του Internet όπως για παράδειγμα η FORTHnet παρέχουν στους συνδρομητές τους ειδική υπηρεσία Fax μέσα από την οποία μπορούμε να στείλουμε Fax με απλές διαδικασίες χωρίς να χρειαστεί να προβούμε σε καμιά απολύτως ρύθμιση. Η ταχύτητα με την οποία μεταδίδει το modem σαν Fax είναι ασφαλώς πολύ μικρότερη από την ονομαστική του ταχύτητα.

6.6 ΣΥΝΔΕΣΗ ΤΩΝ ΔΙΑΜΟΡΦΩΤΩΝ

Έχουμε ήδη τονίσει ότι η σύνδεση του modem με τον Η/Υ γίνεται στη σειριακή θύρα. Συνήθως οι Η/Υ διαθέτουν δυο σειριακές θύρες όπου στη μια τοποθετείται το ποντίκι και στην άλλη το modem ή κάποια άλλη συσκευή. Σχεδόν σε όλους τους Η/Υ το ποντίκι καταλαμβάνει τη σειριακή θύρα COM1. Οι σειριακές θύρες συμβολίζονται με τον όρο COM ενώ οι παράλληλες με LPT. Με την ευκαιρία σημειώνουμε ότι παράλληλη θύρα χρησιμοποιούν οι εκτυπωτές και είναι πολύ ταχύτερες από τις σειριακές. Ο λόγος βέβαια που οι εκτυπωτές χρησιμοποιούν την παράλληλη είναι ότι ο Η/Υ έχει τη δυνατότητα της ταχείας μετάδοσης προς τον εκτυπωτή γιατί αποτελεί δικό του περιφερειακό εξάρτημα, ενώ τα δεδομένα από το modem που έρχονται από αρκετά απομακρυσμένες περιοχές δεν έχουν την δυνατότητα να ταξιδεύουν με μεγάλες ταχύτητες. Ο κάθε Η/Υ διαθέτει τουλάχιστον μια παράλληλη θύρα.

Οι θύρες του υπολογιστή διαφέρουν μεταξύ τους και μπορεί να τις ξεχωρίσει και ο πλέον αρχάριος χρήστης. Οι σειριακές θύρες που είναι πίσω από τον υπολογιστή καταλήγουν σε καρφάκια, ενώ οι παράλληλες αντί για καρφιά έχουν τις αντίστοιχες μικρές τρύπες.

Όταν λοιπόν διαθέτουμε εξωτερικό modem θα πρέπει να προμηθευτούμε και το ανάλογο σειριακό καλώδιο (μερικές εταιρείες το διαθέτουν μαζί με το modem άλλες εταιρείες όχι) για να το συνδέσουμε στην σειριακή του Η/Υ μας. Η θύρα που συνδέουμε το modem είναι συνήθως η COM2 εκτός και αν έχουμε τοποθετήσει σ΄αυτήν το ποντίκι. Είναι αυτονόητο ότι δεν μπορούμε να συνδέσουμε ή να δηλώσουμε δυο συσκευές στην ίδια θύρα.

Ένας άλλος διαχωρισμός που γίνεται μεταξύ modem είναι η ταχύτητα μετάδοσης. Θυμάμαι ότι στην δεκαετία του 1980 ότι το πρώτο modem που αγόρασα ήταν 2400. Τότε κυκλοφορούσαν μόνο τα 1200 και 2400. Σήμερα έχουν καταργηθεί τελείως γιατί έχουν αντικατασταθεί από τα 14400 που και αυτά τείνουν να καταργηθούν δίνοντας τη θέση τους στα 28800 και τελευταία στα 33600. Υπάρχουν βέβαια και τα 57600 αλλά για τους Έλληνες μάλλον μόνο στα χαρτιά. Τα modem που αγοράζει σήμερα η πλειοψηφία των χρηστών είναι τα 28800. Η μονάδα μέτρησης της ταχύτητας ονομάζεται bps και βγαίνει από τα αρχικά Bits Per Second που σημαίνει πόσα bit μεταδίδονται σε κάθε δευτερόλεπτο.

Οι αριθμοί αυτοί που χαρακτηρίζουν τα modem υποδηλώνουν την ταχύτητα ή της μετάδοσης των δεδομένων. Η μονάδα μέτρησης ταχύτητας ή ρυθμού μεταφοράς δεδομένων κανονικά είναι το Baud (που δηλώνει ταχύτητα μεταφοράς δεδομένων) αλλά η επεξήγηση της μονάδας αυτής είναι ακατανόητη για τους περισσότερους χρήστες. Γι΄αυτόν το λόγο χρησιμοποιείται σαν μονάδα μέτρησης το bps.

Ένα modem 28800 bps σημαίνει ότι έχει δυνατότητα μετάδοσης 28800 χιλιάδων bit στο δευτερόλεπτο (Bits Per Second).

Bit & Byte

Στο σημείο αυτό πρέπει να κάνουμε μια μικρή αναφορά στις μονάδες μέτρησης χωρητικότητας και μετάδοσης για να κατανοήσουν τη σημασία τους οι εντελώς αρχάριοι χρήστες. Η αναφορά μας θα είναι τελείως επιγραμματική και απλή χωρίς να αναλύει ειδική τεχνογνωσία ηλεκτρονικής.

Στους Η/Υ χρησιμοποιούμε για μονάδα μέτρησης το byte. Το byte είναι μια μονάδα η οποία αποτελείται από 8 μικρότερες υπομονάδες που στην ουσία αποτελούν τη βασική μονάδα χωρητικότητας και ονομάζονται bit. 8

λοιπόν bit αποτελούν 1 byte. Η λέξη byte δεν υπάρχει στο λεξικό, έχει επινοηθεί σαν σύντμηση από την φράση by eight που σημαίνει "από οκτώ" επειδή αποτελείται από 8 bit.

Το bit είναι καθαρά μια μονάδα που χρησιμοποιείται στην ηλεκτρονική και στόχος αυτού του βιβλίου δεν είναι να διδάξει τέτοιες θεωρίες. Θα προσπαθήσουμε τελείως απλά να εξηγήσουμε τι σημαίνει το bit και τι το byte.

Έχουμε πει πολλές φορές ότι τα δεδομένα αποθηκεύονται ή μεταδίδονται στον Η/Υ σαν ψηφιακό σήμα. Αυτό σημαίνει ότι οι πύλες από τις οποίες περνά το σήμα είναι κλειστά ή ανοιχτά κυκλώματα. Όταν το κύκλωμα είναι κλειστό σημαίνει ότι διαπερνάται από ηλεκτρικό ρεύμα (5 volt) και αυτό συμβολίζεται με τον αριθμό 1. Όταν το κύκλωμα είναι ανοιχτό δεν υπάρχει τάση ρεύματος επομένως η τιμή εδώ είναι μηδέν 0. Αυτή λοιπόν είναι η λογική πάνω στην οποία βασίζεται η λειτουργία των Η/Υ και αυτό επειδή σε ένα κύκλωμα το ηλεκτρικό ρεύμα μπορεί να βρίσκεται μόνο σε δυο καταστάσεις, υπάρχει ρεύμα ή δεν υπάρχει. Σίγουρα έχουμε ακούσει πολλές φορές ότι οι Η/Υ είναι κατασκευασμένοι έτσι ώστε να λειτουργούν και να καταλαβαίνουν απόλυτα το δυαδικό σύστημα αρίθμησης. Το δυαδικό σύστημα είναι αυτό που χρησιμοποιεί μόνο δυο αριθμούς, που είναι το μηδέν 0 και το 1 και εξηγήσαμε το γιατί.

Αυτό λοιπόν το 1 ή το 0 ονομάζεται bit και αποτελεί την μικρότερη μονάδα. 8 bit συνθέτουν 1 byte.

Για να απλοποιήσω πάρα πολύ τα πράγματα για τους χρήστες που δεν έχουν καμιά σχέση με τα ηλεκτρονικά θα τους συμβουλέψω να φανταστούν την μονάδα byte σαν το χώρο μέσα στον οποίο χωρά ένας χαρακτήρας. Για παράδειγμα η λέξη Μαρία αποτελείται από 5 byte. Πολλαπλάσια αυτής της μονάδας είναι το KB (KiloByte), το MB (MegaByte), το GB (GigaByte) κλπ.Το 1 KB είναι 1000 byte (για την ακρίβεια είναι 1024), το ένα MB είναι περίπου 1.000.000 byte κλπ. Όταν λέμε επομένως ότι ένας σκληρός δίσκος έχει χωρητικότητα 800 MB σημαίνει ότι χωράνε πάνω σ΄αυτόν 800 εκατομμύρια χαρακτήρες. Με την μονάδα λοιπόν byte μετράμε την χωρητικότητα της μνήμης, των δίσκων, τη μετάδοση δεδομένων κλπ.

Επανερχόμενοι τώρα στη μεταφορά των δεδομένων μέσα από τα καλώδια των τηλεπικοινωνιακών δικτύων θυμίζουμε ότι για να ταξιδέψουν μέσα σ΄αυτά θα πρέπει ψηφιοποιηθούν δηλαδή να πάρουν τη μορφή του 1 ή 0 δηλαδή να μετατραπούν σε bit. Αυτός είναι λοιπόν και ο λόγος που η ταχύτητα μεταφοράς μετριέται σε bit ανά second που σημαίνει πόσα bit μεταδίδονται σε κάθε δευτερόλεπτο.

Τώρα πιστεύω ότι μπορούμε να κάνουμε τα πράγματα περισσότερο χειροπιαστά. Ένα modem με ταχύτητα 28800 bps σημαίνει ότι μεταδίδει 28800 bit το δευτερόλεπτο. Αν κάνουμε μια διαίρεση το 28800 δια το 8 (8 Bit=1byte) θα βρούμε ότι το modem αυτό μπορεί να μετάδοση 3600 byte ή 3,6 Kb στο δευτερόλεπτο. Για να γίνει ακόμα πιο κατανοητό, σας γνωρίζω ότι αυτά αντιστοιχούν με περίπου δυο σελίδες οθόνης κείμενο. Άρα σε ένα δευτερόλεπτο μπορεί να μετάδοσει χονδρικά, ένα κείμενο δυο σελίδων.

Αν κάποιος χρήστης μου έθετε το ερώτημα τι ταχύτητα πρέπει να έχει το modem που θα αγοράσει, θα απαντούσα αμέσως 33600 παρόλο που γνωρίζω ότι οι περισσότεροι παροχείς χρησιμοποιούν modem των 28800. Πιστεύω όμως ότι σε λίγο καιρό θα τα αντικαταστήσουν όλοι με 33600. Εδώ πρέπει να με την ευκαιρία να τονίσουμε ότι αν ο παροχέας μας χρησιμοποιεί modem 28800 και εμείς διαθέτουμε 33600 θα λαμβάνουμε αυτά που μας αποστέλλει ο παροχέας και όχι αυτά της πραγματικής δυνατότητας του modem που διαθέτουμε.

Το μέγιστο όριο ταχύτητας σήμερα θεωρείται το 33600.

6.7 ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΓΙΑ MODEM

Γνωρίζουμε όλοι ότι οι Η/Υ έχουν τη δυνατότητα να μεταφέρουν δεδομένα με πολύ μεγαλύτερες ταχύτητες έναντι των modem, επειδή χρησιμοποιούν ψηφιακά σήματα. Όταν αποστέλλουμε ένα μήνυμα μέσα από το δίκτυο τηλεπικοινωνιών πρέπει να υπάρχει μια συμβατότητα στην σύνδεση και ταχύτητα ώστε να υπάρχει ασφάλεια και σιγουριά ότι τα δεδομένα μεταδόθηκαν κανονικά. Τον ρόλο αυτής της επικοινωνίας τον αναλαμβάνουν τα πρωτόκολλα επικοινωνίας.

Κατά καιρούς και ανάλογα με τις ταχύτητες των modem εμφανίζονται διάφορα πρωτόκολλα. Όταν έχουμε κακές γραμμές στις επικοινωνίες, τα πρωτόκολλα επεμβαίνουν και χαμηλώνουν την ταχύτητα ώστε να μπορέσουν να προχωρήσουν τα δεδομένα. Τα modem χρησιμοποιούν αρκετά πρωτόκολλα επικοινωνίας όπως Kermit, Xmodem, Zmodem κλπ. Το πρωτόκολλο που χρησιμοποιείται στο Internet είναι το γνωστό TCP/IP.

Τα πρωτόκολλα είναι απαραίτητα για τη μεταφορά των δεδομένων μεταξύ modem. Για να επικοινωνήσουν δυο modem πρέπει πρώτα να συνεννοηθούν ποιο πρωτόκολλο θα χρησιμοποιήσουν σαν να πρόκειται να επιλέξουν μια κοινή γλώσσα, διαφορετικά δεν μπορούν να συνεννοηθούν. Η επικοινωνία μεταξύ δυο modem είναι αμφίδρομη, αυτό σημαίνει ότι όταν το ένα από τα δυο λαμβάνει λανθασμένα δεδομένα

ειδοποιεί να αποσταλλούν ξανά από την αρχή. Αυτό βέβαια είναι πολύ σημαντικό γιατί έτσι υπάρχει η βεβαιότητα ότι ελήφθη ακριβώς αυτό που έχει αποσταλλεί.

Τα πρωτόκολλα, εκτός από τον ασφαλή τρόπο μετάδοσης, παίζουν πολύ σημαντικό ρόλο στην αύξηση της ταχύτητας μετάδοσης των δεδομένων επειδή έχουν τη δυνατότητα να συμπιέζουν τα δεδομένα πριν από την αποστολή και να τα αποσυμπιέζουν όταν φθάσουν στον προορισμό τους. Είναι αυτά που τοποθετούν τα δεδομένα στη σειρά με την οποία θα μεταδοθούν και χρησιμοποιούν μια ειδική τεχνική για να αποφεύγονται τα λάθη. Σύμφωνα με την τεχνική αυτή τοποθετούνται τα start και stop bit στην αρχή και τέλος κάθε ψηφιολέξης καθώς και το bit ισοτιμίας το οποία είναι για την ανίχνευση λαθών. Σ΄αυτό το τελευταίο αναφερόμαστε αποκλειστικά και μόνο επειδή θα το συναντήσουμε στη ρύθμιση του modem.

Ο λόγος συμπίεσης που ισχύει σήμερα είναι 4:1. Αυτό σημαίνει ότι όταν στέλνουμε 1000 byte ταξιδεύουν σαν δεδομένα των 250 επομένως τετραπλασιάζεται η ταχύτητα μετάδοσης. Άρα ένα modem 28800 λειτουργεί σαν να είναι 28.800x4 = 115.000 bps. Αυτή είναι και η πραγματική ταχύτητα που ισχύει μεταξύ του Η/Υ μας και του modem, γι'αυτό πρέπει, όπως επεξηγούμε και στην παράγραφο ρυθμίσεις Modem, να έχουμε ρυθμισμένο το modem στην ταχύτητα αυτή. Για ένα modem ονομαστικής ταχύτητας 33600 η πραγματική είναι 134.400.

Μέχρις εδώ όλα καλά, αλλά πρέπει να γνωρίζουμε ότι για να μπορέσει μια σειριακή θύρα να μεταδώσει τέτοιες μεγάλες ταχύτητες θα πρέπει να είναι εφοδιασμένη με ένα ειδικό chip UART (Universal asynchronous receiver-transmitter) που είναι το 16650 και χρησιμοποιείται εκτός των άλλων και για τις μετατροπές δεδομένων από παράλληλες σε σειριακές και από σειριακές σε παράλληλες. Σήμερα το microchip αυτό το διαθέτουν προκαθορισμένα όλοι οι μοντέρνοι Η/Υ. Υπενθυμίζουμε ότι τα εσωτερικά modem, επειδή δεν συνδέονται σε σειριακές θύρες, διαθέτουν ενσωματωμένη σειριακή θύρα και UART.

6.8 ΠΡΟΤΥΠΑ ΤΑΧΥΤΗΤΑΣ ΜΕΤΑΔΟΣΗΣ

ITU-T: Πρόκειται για έναν παγκόσμιο οργανισμό που ορίζει τα πρότυπα τηλεπικοινωνιακού εξοπλισμού. Παλαιότερα ονομάζονταν CCITT.

V.32: Πρόκειται για πρότυπο, standard της ITU-U επικοινωνίας για ταχύτητες 9600 bps.

V.32bis: Πρόκειται για πρότυπο, standard της ITU-T επικοινωνίας για ταχύτητες 14.400 bps.

V.34: Πρόκειται για πρότυπο, standard της ITU-T επικοινωνίας για ταχύτητες 28.800bps.

Πρότυπα διόρθωσης σφαλμάτων.

Οι εταιρίες που ανέπτυξαν πρότυπα για τη διόρθωση σφαλμάτων είναι η Microcom με το MNP το οποίο είναι για modem μικρών ταχυτήτων και η ITU-T με το V.42 για modem μεγαλύτερων ταχυτήτων.

V.42: Πρόκειται για πρότυπο της ITU-T για διόρθωση σφαλμάτων.

MNP2 έως 4: Πρόκειται για το πρότυπο διόρθωσης λαθών της Microcom και αφορά modem μικρότερων ταχυτήτων.

Πρότυπα συμπίεσης δεδομένων

Τα modem χρησιμοποιούν ειδικούς αλγόριθμους οι οποίοι συμπιέζουν τα δεδομένα πριν από την από την αποστολή τους. Αυτό σημαίνει απλά αύξηση της ταχύτητας μετάδοσης.

V.42bis: Πρόκειται για δημοφιλέστερο πρότυπο συμπίεσης δεδομένων το οποίο μπορεί να τετραπλασιάσει της ταχύτητες μετάδοσης. Είναι της ITU-T και είναι καλύτερο από το MNP.

MNP5: Πρόκειται για το πρότυπο συμπίεσης δεδομένων της Microcom.

Τελειώνοντας αναφέρουμε ότι ο όρος Hayes AT δηλώνει ότι το modem είναι συμβατό με την ομάδα εντολών της εταιρείας Hayes η οποία επινόησε πρώτη τις διάφορες εντολές που δίνονται στα modem.

Επίσης, μπορεί να αναφέρεται στο modem και ο όρος V.FC. Πρόκειται για ένα πρότυπο επικοινωνίας που ανέπτυξε η εταιρεία Rockwell για ταχύτητες μέχρι και 28800 πριν από την εμφάνιση του πρωτότυπου V.34.

ΚΕΦΑΛΑΙΟ 7°

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Για την εξασφάλιση της γνησιότητας της ηλεκτρονικής υπογραφής τα μέρη δημιουργούν το ηλεκτρονικό μέσο αναγνωρίσεως της ταυτότητας τους με τη βοήθεια κρυπτογραφικών κωδικών. Μια μέθοδος κρυπτογραφήσεως ηλεκτρονικών δεδομένων για την παράγωγη ηλεκτρονικής υπογραφής στηρίζεται στη χρήση ασύμμετρου κρυπτογραφικού συστήματος. Η ιδιαίτερη αυτή μέθοδος αναγνωρίσεως του εκδότη εγγράφου, που παράγεται μέσω ηλεκτρονικών υπογραφών, ονομάζεται ψηφιακή υπογραφή. Την ορολογία αυτή χρησιμοποιούν ο νόμος περί ψηφιακής υπογραφής του 1995 της πολιτείας Γιούτα, ο νόμος περί ηλεκτρονικής υπογραφής της Φλόριντα (Florida electronic signature act του 1996) καθώς και ο γερμανικός νόμος του 1997, ο οποίος ορίζει ρητά ότι ψηφιακή υπογραφή είναι η μέθοδος αναγνώρισης του εκδότη ηλεκτρονικού εγγράφου, όταν προς το σκοπό αυτό χρησιμοποιείται η ασύμμετρη κρυπτογράφηση. Με άλλα λόγια ο όρος <<ψηφιακή υπογραφή>> είναι η έννοια είδους σε σχέση με τον όρο << ηλεκτρονική υπογραφή>> , για την οποία χρησιμοποιούνται και σύμμετρα κρυπτογραφικά συστήματα.

7.1 ΟΡΙΣΜΟΣ

Μια ψηφιακή υπογραφή ή ψηφιακή υπογραφή σύστημα είναι ένα μαθηματικό σύστημα για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή έγγραφο. Μια έγκυρη ψηφιακή υπογραφή δίνει αποδέκτη λόγο να πιστεύει ότι το μήνυμα δημιουργήθηκε από ένα γνωστό αποστολέα, και ότι δεν αλλοιώθηκε κατά τη μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούνται συνήθως για τη διανομή λογισμικού, οικονομικές συναλλαγές, καθώς και σε άλλες περιπτώσεις όπου είναι σημαντικό για τον εντοπισμό πλαστογραφία και παραποίηση.

Οι ψηφιακές υπογραφές που χρησιμοποιούνται συχνά για την υλοποίηση ηλεκτρονικών υπογραφών, ένας ευρύτερος όρος που αναφέρεται σε όλα τα ηλεκτρονικά δεδομένα που φέρει την πρόθεση της υπογραφής, αλλά δεν είναι όλες οι ηλεκτρονικές υπογραφές χρήση ψηφιακών υπογραφών. Σε ορισμένες χώρες, συμπεριλαμβανομένων των Ηνωμένων Πολιτειών, καθώς και τα μέλη της Ευρωπαϊκής Ένωσης, οι ηλεκτρονικές υπογραφές έχουν νομική σημασία. Ωστόσο, οι νόμοι σχετικά με τις ηλεκτρονικές υπογραφές, δεν διευκρινίζουν πάντοτε σαφές εάν οι ψηφιακές υπογραφές κρυπτογράφησης, με την έννοια που χρησιμοποιείται εδώ, αφήνοντας ο νομικός ορισμός, και έτσι η σημασία τους, κάπως συγκεχυμένη.

Τα έγγραφα που αποθηκεύονται στη μνήμη του η/υ και διακινούνται ηλεκτρονικά , δηλ τα ηλεκτρονικά έγγραφα παρουσιάζουν μια σειρά από μειονεκτήματα , όπως ότι στερούνται της σταθερότητας κατά την ενσωμάτωση τους και μπορεί να υποστούν μετατροπές, αλλοιώσεις ή διαγραφές που είναι αδύνατον να εντοπιστούν, αλλά και ότι δεν διαθέτουν την ιδιόχειρη υπογραφή που είναι απαραίτητη στα έγγραφα όπου ο τύπος είναι συστατικός. Επιπλέον, όταν διακινούνται μέσω ανοικτών δικτύων , όπως το διαδίκτυο , υπάρχει κίνδυνος να υποκλαπούν αυτά από τρίτους και να αλλοιωθεί ή τροποποιηθεί το περιεχόμενο τους.

Ειδικά δε όσον αφορά τα έγγραφα που διακινούνται ηλεκτρονικά, παρατηρείται ότι είναι δυσχερής η ακριβής εξακρίβωση της ταυτότητας του αποστολέα των εγγράφων, όπως και της αυθεντικότητας και της μη αλλοίωσης τους. Για την πλήρη αξιοποίηση των δυνατοτήτων που προσφέρει η σύγχρονη τεχνολογία απαιτείται, συνεπώς , η ενίσχυση της ασφάλειας των ηλεκτρονικών συναλλαγών και προς τούτο χρησιμοποιούνται μέθοδοι κρυπτογράφησης που εξασφαλίζουν την ασφαλή μεταφορά δεδομένων η/υ μέσω ανοιχτών δικτύων. Για την εξασφάλιση της γνησιότητας των εγγράφων που διακινούνται ηλεκτρονικά χρησιμοποιείται Ειδικότερα, η τεχνολογία της ηλεκτρονικής υπογραφής. Δυο είναι δε οι κυριότεροι τύποι συστημάτων κρυπτογράφησης που χρησιμοποιούνται για την παραγωγή της ηλεκτρονικής υπογραφής, το συμμετρικό κρυπτογραφικό σύστημα και το ασύμμετρο κρυπτογραφικό σύστημα. Τα συμμετρικά συστήματα, τα συστήματα δηλ που χρησιμοποιούν συμμετρικούς αλγορίθμους , όπως είναι λ.χ το σύστημα DES , έχουν ένα κοινό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, το οποίο είναι γνωστό στον αποστολέα και στον παραλήπτη του μηνύματος μόνο και πρέπει να μείνει μυστικό. Η τεχνολογία αυτή είναι κατάλληλη

επομένως μόνο για κλειστές ομάδες χρηστών και όχι για συναλλαγές, στις οποίες μετέχει ένας μεγάλος αριθμός συναλλασσομένων.

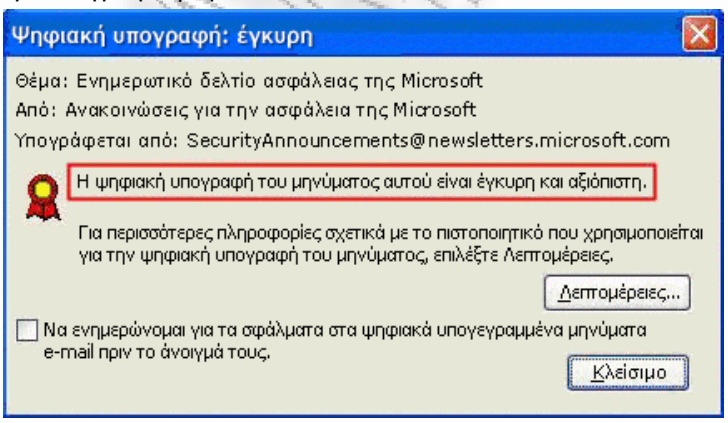
Τα συστήματα που χρησιμοποιούν ασύμμετρους αλγόριθμους ή συστήματα δημοσίου κλειδιού RSA για τη θέση της ηλεκτρονικής υπογραφής εφαρμόζουν ένα συνδυασμό δημόσιου και μυστικού κλειδιού. Ο αποστολέας ενός μηνύματος χρησιμοποιεί το μυστικό, ιδιωτικό κλειδί για την κρυπτογράφηση του. Ο συνδυασμός αυτός του μηνύματος με το μυστικό κλειδί αποτελεί την ηλεκτρονική ή ψηφιακή υπογραφή του αποστολέα. Ο αποδέκτης του μηνύματος αποκρυπτογραφεί στη συνέχεια το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί ή κλειδί αποκρυπτογράφησης. Η διαδικασία αυτή είναι πιο πρόσφορη για ανοιχτά δίκτυα, όπως είναι το διαδίκτυο, αλλά δεν είναι κατάλληλη για την μεταβίβαση εκτενών μηνυμάτων λόγω του ότι είναι χρονοβόρα (τα συστήματα DES χρησιμοποιούν κλειδιά με μήκος 56 bit, ενώ τα συστήματα RES χρησιμοποιούν κλειδιά με μήκος 1024 bits.

Πιο πρόσφατα για την αποστολή εκτενών μηνυμάτων είναι η διαδικασία (επίσης δημοσίου κλειδιού ή ασύμμετρη) , κατά την οποία δημιουργείται το <<δακτυλικό αποτύπωμα >> του εγγράφου, δηλ εξάγεται το άθροισμα των bits , από τα οποία αποτελείται το κείμενο με μια διαδικασία hashing και στη συνέχεια κρυπτογραφείται με τη μέθοδο RSA. Ο αποστολέας κρυπτογραφεί , έτσι, την περίληψη αυτή του εγγράφου , μαζί με άλλα πρόσθετα δεδομένα, όπως είναι π.χ ο τόπος και η ημερομηνία της υπογραφής, χρησιμοποιώντας το ιδιωτικό κλειδί. Ο αποδέκτης χρησιμοποιεί το δημόσιο κλειδί για την αποκρυπτογράφηση του δακτυλικού αποτυπώματος, το οποίο και εξάγει με τη βοήθεια κατάλληλου λογισμικού, ώστε να διαπιστώσει εάν το περιεχόμενο του έχει παραμείνει αναλλοίωτο (επαλήθευση υπογραφής).

Επίσης πρέπει να αναφερθεί και το σύστημα του <<ψηφιακού φακέλου>>, το οποίο συνδυάζει τα συστήματα συμμετρικών και ασύμμετρων αλγορίθμων. Κατά τη μέθοδο αυτή, το έγγραφο κρυπτογραφείται από τον αποστολέα με ένα συμμετρικό αλγόριθμο και με τη χρήση ενός συντόμου, αλλά ασφαλούς κλειδιού, 128 bits , το οποίο καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και για αυτό ονομάζεται κλειδί συνεδρίας. Το κλειδί αυτό για ασφάλεια κρυπτογραφείται με έναν ασύμμετρο αλγόριθμο. Έτσι, ο παραλήπτης του εγγράφου θα πρέπει πρώτα να αποκρυπτογραφήσει το κλειδί με το δημόσιο κλειδί και στη συνέχεια και το μήνυμα.

ΟΙ Ψηφιακές υπογραφές χρησιμοποιούν ένα είδος ασύμμετρη κρυπτογράφηση. Για τα μηνύματα που αποστέλλονται μέσω ενός αβέβαιου κανάλι, ένα σωστά υλοποιούνται ψηφιακή υπογραφή δίνει το λόγο δέκτη να πιστεύουν ότι το μήνυμα που εστάλη από την ισχυρίστηκε αποστολέα. Ψηφιακές υπογραφές είναι ισοδύναμες με τις παραδοσιακές χειρόγραφες υπογραφές, από πολλές απόψεις. Εφαρμοστεί σωστά ψηφιακές υπογραφές είναι πιο δύσκολο να σφυρηλατήσει από τη χειρόγραφη τύπου. Συστήματα ψηφιακής υπογραφής, με την έννοια που χρησιμοποιείται εδώ βασίζονται cryptographically, και πρέπει να εφαρμοστεί σωστά να είναι αποτελεσματική. Ψηφιακές υπογραφές μπορούν επίσης να παρέχουν μη άρνηση, την έννοια ότι ο υπογράφων δεν μπορεί με επιτυχία ισχυρίζονται ότι δεν είχαν υπογράψει ένα μήνυμα, ενώ ισχυρίζεται επίσης ιδιωτικό κλειδί τους παραμένει μυστική. Περαιτέρω, κάποιες μη-άρνηση συστήματα προσφέρουν μια χρονική σήμανση για την ψηφιακή υπογραφή, έτσι ώστε να ακόμη και αν το ιδιωτικό κλειδί είναι εκτεθειμένη, η υπογραφή είναι έγκυρη, ωστόσο.

Ψηφιακή υπογραφή μηνύματα μπορεί να είναι οτιδήποτε αντιπρόσωπος ςως bitstring: παραδείγματα περιλαμβάνουν ηλεκτρονικό ταχυδρομείο, τις συμβάσεις, ή ένα μήνυμα που αποστέλλεται μέσω άλλου κρυπτογραφική πρωτόκολλο.



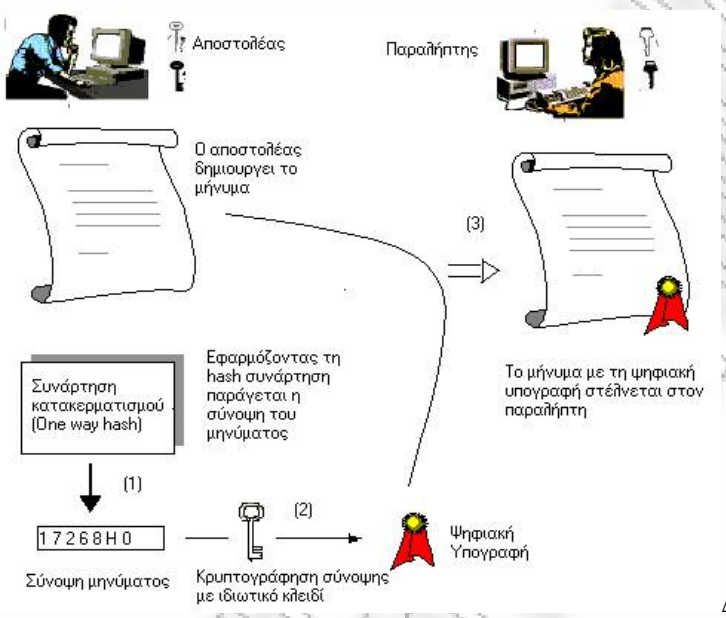
Μια ψηφιακή υπογραφή σύστημα αποτελείται συνήθως από τρία αλγορίθμων:

1. Α κλειδί αλγόριθμος γενιά που επιλέγει ένα ιδιωτικό κλειδί ομοιόμορφα τυχαία από ένα σύνολο πιθανών ιδιωτικών κλειδιών. The algorithm outputs the private key and a corresponding public key . Ο αλγόριθμος εξόδους το ιδιωτικό κλειδί και ένα αντίστοιχο δημόσιο κλειδί.
2. Ένας αλγόριθμος υπογραφής που, δεδομένης ένα μήνυμα και ένα ιδιωτικό κλειδί, παράγει μια υπογραφή.
3. Υπογραφή επαλήθευση αλγόριθμος που δοθεί ένα μήνυμα, το δημόσιο κλειδί και μια υπογραφή, είτε αποδέχεται ή απορρίπτει τον ισχυρισμό της μήνυμα για την αυθεντικότητα.

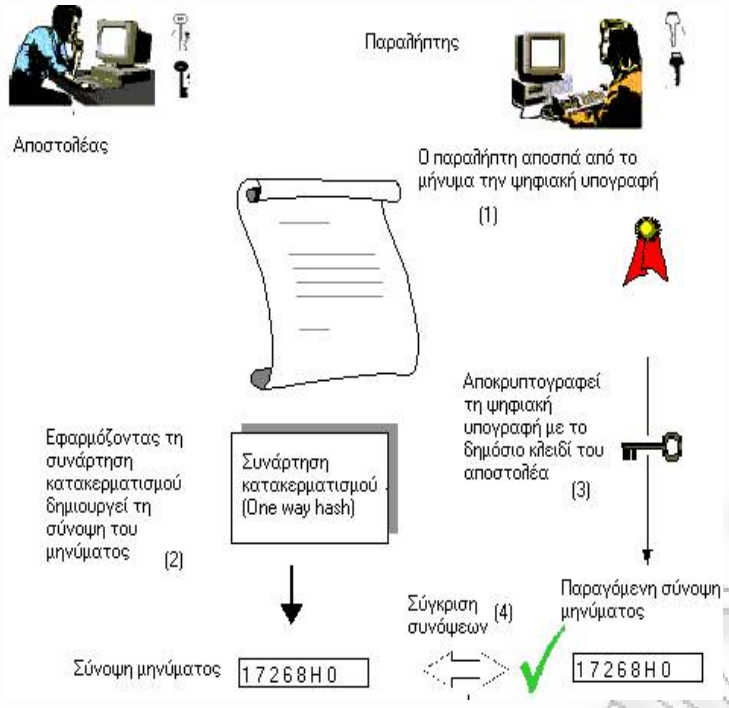
Απαιτούνται δύο βασικές ιδιότητες:

Πρώτον, μια υπογραφή που παράγεται από ένα σταθερό μήνυμα και σταθερό ιδιωτικό κλειδί πρέπει να επαληθεύει την αυθεντικότητα του μηνύματος, χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί.

Δεύτερον, θα πρέπει να είναι υπολογιστικά ανέφικτη να δημιουργήσει μια έγκυρη υπογραφή για ένα κόμμα που δεν διαθέτει το ιδιωτικό κλειδί.



ΔΗΜΙΟΥΡΓΙΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ



ΕΠΑΛΗΘΕΥΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

7.2 ΠΡΟΣΘΕΤΕΣ ΠΡΟΦΥΛΑΞΕΙΣ ΑΣΦΑΛΕΙΑΣ

Όλα δημόσιου κλειδιού / ιδιωτικού κλειδιού Κρυπτοσυσκευών εξαρτηθεί εξ ολοκλήρου από τη διατήρηση του ιδιωτικού κλειδιού μυστικό. Ένα ιδιωτικό κλειδί μπορεί να αποθηκευτεί στον υπολογιστή ενός χρήστη, και προστατεύονται από έναν κωδικό πρόσβασης του τοπικού, αλλά αυτό έχει δύο μειονεκτήματα:

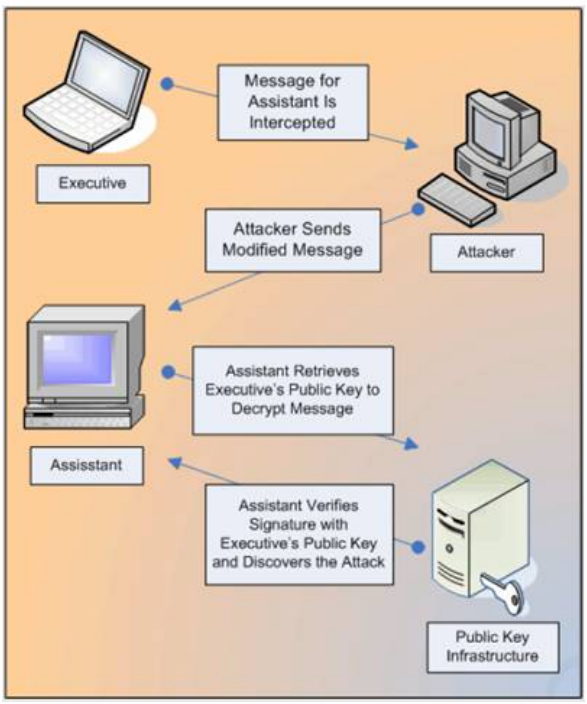
1. ο χρήστης μπορεί να υπογράψει μόνο έγγραφα για το συγκεκριμένο υπολογιστή
2. την ασφάλεια του ιδιωτικού κλειδιού εξαρτάται πλήρως από την ασφάλεια του υπολογιστή

Μια πιο ασφαλής εναλλακτική λύση είναι η αποθήκευση του ιδιωτικού κλειδιού σε μια έξυπνη κάρτα. Πολλές έξυπνες κάρτες σχεδιαστεί για να προστασίας έναντι της παραποίησης (αν και έχουν σπασμένα μερικά σχέδια, ιδίως από τον Ross Anderson και τους μαθητές του). Σε μια τυπική εφαρμογή ψηφιακή υπογραφή, το κλειδί κατακερματισμού που υπολογίζεται από το έγγραφο αυτό αποστέλλεται στην έξυπνη κάρτα, CPU οποίων κρυπτογραφεί το κλειδί κατακερματισμού χρησιμοποιώντας τις αποθηκευμένες ιδιωτικό κλειδί του χρήστη, και στη συνέχεια επιστρέφει το κρυπτογραφημένο hash.

Συνήθως, ο χρήστης πρέπει να ενεργοποιήσει έξυπνη κάρτα του από την είσοδο έναν προσωπικό αριθμό αναγνώρισης ή τον κωδικό PIN (και προσφέροντας έτσι δύο παράγοντα ελέγχου ταυτότητας).

Μπορεί να οργανωθούν ότι ποτέ δεν το ιδιωτικό κλειδί αφήνει την έξυπνη κάρτα, αν και αυτό δεν εφαρμόζεται πάντα. Εάν η έξυπνη κάρτα είναι κλαπεί, ο κλέφτης θα εξακολουθεί να χρειάζεται τον κωδικό PIN για να δημιουργήσετε μια ψηφιακή υπογραφή. Αυτό μειώνει την ασφάλεια του συστήματος με εκείνο του συστήματος PIN, αν και εξακολουθεί να απαιτεί έναν εισβολέα να κατέχει την κάρτα.

Ελαφρυντικό στοιχείο είναι ότι τα ιδιωτικά κλειδιά, εάν παράγονται και αποθηκεύονται σε έξυπνες κάρτες, θεωρείται συνήθως ως δύσκολη την αντιγραφή, και υποτίθεται ότι υπάρχει ακριβώς σε ένα αντίγραφο. Έτσι, η απώλεια της έξυπνης κάρτας μπορεί να εντοπιστεί από τον ιδιοκτήτη και το αντίστοιχο πιστοποιητικό μπορεί να ανακληθεί αμέσως. Ιδιωτικά κλειδιά που προστατεύονται από το λογισμικό μόνο μπορεί να είναι πιο εύκολο να αντιγράψετε, και όπως συμβιβασμοί είναι πολύ πιο δύσκολο να ανιχνευθούν.



ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

7.3 ΠΡΩΤΟΚΟΛΛΑ ΔΙΚΤΥΟΥ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΝΑ ΠΑΡΕΧΟΥΝ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Ο μηχανισμός ελέγχου αξιοπιστίας επιλέγεται σε σχέση με την εφαρμογή και τη σημασία της, το περιβάλλον λειτουργίας (είδη λαθών, συχνότητα σφαλμάτων κ.ά.) και την εγκατάσταση της επικοινωνίας (για παράδειγμα ο αριθμός των παραληπτών).Εδώ θα μας απασχολήσουν θέματα που αφορούν το είδος (για παράδειγμα έχουμε περισσότερη επιπρόσθετη πληροφορία ανά πακέτο ή περισσότερα πακέτα;), το ποσοστό και τις χρονικές στιγμές (συμβαίνουν συνεχώς ή μόνο σε περίπτωση σφάλματος;) της επιβάρυνσης που προκύπτει, τις πληροφορίες που πρέπει να ξέρει ο αποστολέας για τον παραλήπτη, το είδος και τον αριθμό των παραληπτών και τέλος τις παραμέτρους που επηρεάζουν την μέγιστη δυνατή απόδοση. Θα καταφύγουμε και πάλι σε μία εγνωσμένη μέθοδο για να γίνουν πιο κατανοητά όλα αυτά και δεν είναι άλλη από αυτή της παράθεσης παραδείγματος! Παρακάτω παρατίθεται ένα σχήμα που απεικονίζει την TCP επικοινωνία και πάνω σε αυτή θα μελετήσουμε συγκεκριμένους τρόπους με τους οποίους εμφανίζονται τα προβλήματα που προαναφέρθηκαν και βέβαια μεθόδους αντιμετώπισης.

Το θέμα της υπερφόρτωσης (overload) και της ‘παραγγελίας’ (ordering).Ο όρος ordering αναφέρεται στους αριθμούς ακολουθίας (sequence numbers SN) που μετράνε μηνύματα, πακέτα ή bytes και σαν στόχο έχουν την αποφυγή αναδιπλώσεων (wrap around) σε γρήγορα δίκτυα. Ο όρος overload έχει να κάνει τόσο με τον παραλήπτη όσο και με το δίκτυο. Στην περίπτωση του παραλήπτη έχουμε έλεγχο ροής (τυπικά μηνύματα παραθύρων με χρήση SN και με τον παραλήπτη να δηλώνει το διαθέσιμο μέγεθος buffer) με στόχο την ανανέωση της συχνότητας και της ικανότητας να είναι γεμάτος ο αγωγός και έλεγχο συχνότητας ο οποίος είναι προσυμφωνημένος μεταξύ του αποστολέα και του παραλήπτη και μπορεί να αλλάζει.

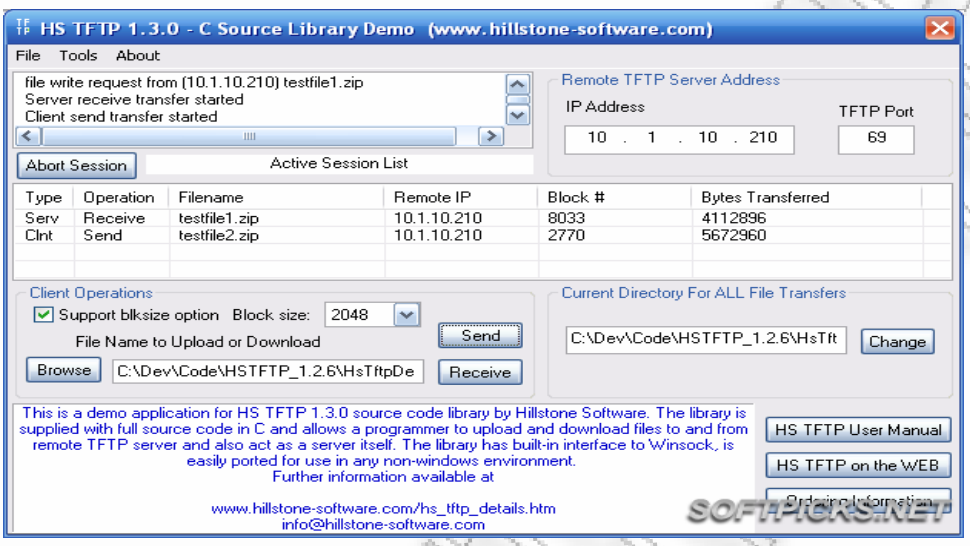
Μηχανισμοί εύρεσης λαθών (error detection)

Υπάρχουν διάφοροι τρόποι για να αντιμετωπίσουμε τα προβλήματα που μπορεί να δημιουργηθούν στην προσπάθειά μας να επιτύχουμε όσο το δυνατό μεγαλύτερη αξιοπιστία τόσο σε επίπεδο bit όσο και σε επίπεδο πακέτων. Μπορούμε να

χρησιμοποιήσουμε Checksums, CRCs (Cyclic Redundancy Check Code) και MACs (Medium Access Control) για να βρούμε λάθη σε επίπεδο bit ή σε επίπεδο πλαισίου (frame) σε ένα πακέτο και Sequence numbers (SN) για να βρούμε πακέτα που έχουν χαθεί (με τον όρο χαθεί περιλαμβάνουμε και τις αποτυχημένες αποστολές).

Μηχανισμοί διόρθωσης λαθών (error correction):

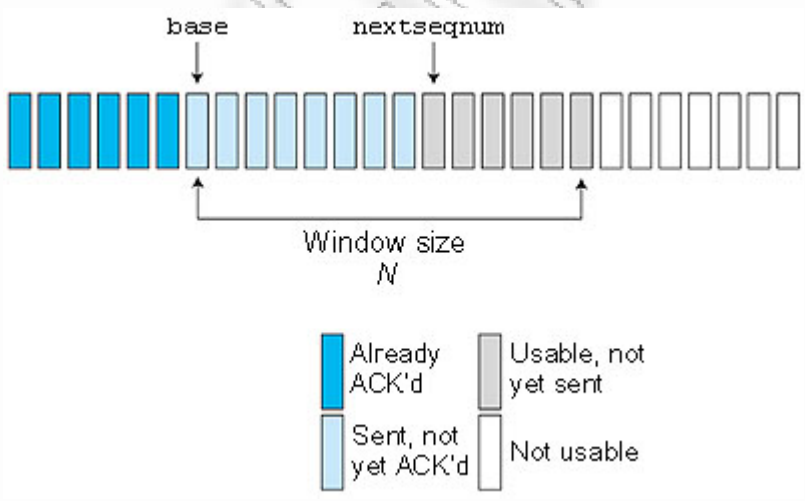
1. Απλό Lock-Step Πρωτόκολλο (simple Lock-Step protocol)
   Τα δεδομένα αποστέλλονται και περιμένουμε για επιβεβαίωση (acknowledgement (ACK))
   Timeout στη μετάδοση trigger (trigger retransmission)
   Ασήμαντο αλλά και πολύ περιορισμένο
   Παράδειγμα: Trivial File Transfer Protocol (TFTP)



2. Αθροιστικό ACK με Go-back-N (Cumulative ACK with Go-back-N)

Μηχανισμός βασισμένος σε παράθυρα που επιτρέπει πολλαπλά σημαντικά πακέτα (με αυστηρό SN εύρος και μέγεθος buffer)

Timeouts ή trigger αναμεταδώσεις (trigger retransmissions) των εκτός αίτησης ληφθέντων πακέτων Παραλλαγές: HDLC (LAPB/D/F), X.25 layer 3, plain old TCP

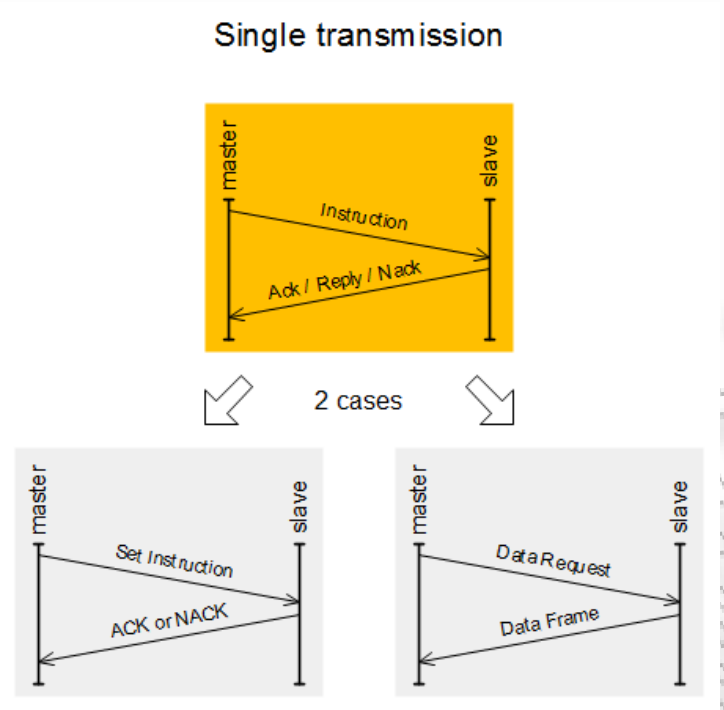


Απλό NACK Πρωτόκολλο (Simple NACK (Negative ACK) Protocol)

Αισιόδοξη υπόθεση :τα πακέτα θα φθάσουν ,άρα αναφέρουμε μόνο τις αποτυχίες (Negative ACK)

Ειδικοί μηχανισμοί απαραίτητοι για το τελευταίο πακέτο

Ειδικοί μηχανισμοί απαραίτητοι για έλεγχο ροής



Simple NACK Protocol

Forward Error Correction (FEC)

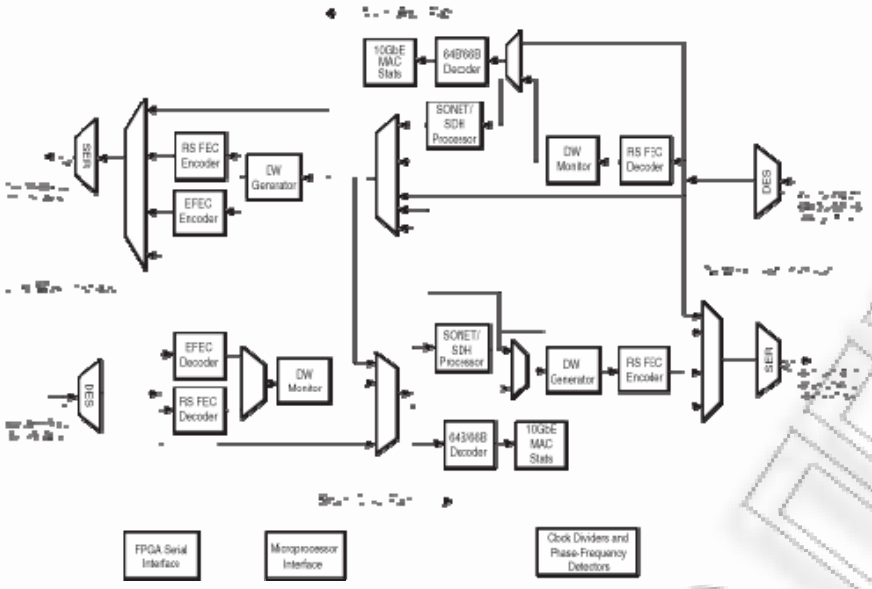
Βασική υπόθεση :θα συμβούν λάθη (αυξάνουμε την πιθανότητα σωστής λήψης στέλνοντας πακέτα μαζί με πακέτα ισοτιμίας (parity packets))

Απλό XOR-based FEC (P_fec=P1 XOR P2 XOR P3… XOR Pn)

Αυξάνονται οι απαιτήσεις σε bandwidth

Αυξάνεται το overhead μειώνεται όμως η καθυστέρηση (δε χρειάζεται να περιμένουμε για NACK ή timeout)

Υπάρχουν και πιο περίπλοκα FEC



Forward Error Correction

Συνοψίζοντας υπάρχουν κάποια προβλήματα όσο αφορά στην αξιοπιστία. Κάποια στοιχεία πρέπει να είναι γνωστά μεταξύ αποστολέα και παραλήπτη όπως το μέγεθος του παραθύρου του παραλήπτη, τα SN και το τελευταίο ACK, ωστόσο η αρχικοποίηση είναι πιθανό να προκαλέσει Denial-of-Service (DoS) προβλήματα οπότε το ιδανικό είναι όλα αυτά να προσαρμόζονται δυναμικά στο περιβάλλον που πιθανότατα να είναι συχνά μεταβαλλόμενο. Αυτά όμως δεν ισχύουν στην περίπτωση που έχουμε επικοινωνία μεταξύ ομάδων κόμβων. Ενδεικτικά να αναφέρουμε ότι ακόμα κ ο ορισμός της σημασίας της σύνδεσης αλλάζει εδώ.

Χαλάρωση των απαιτήσεων για αξιοπιστία

Όπως είδαμε υπάρχουν πολλά ζητήματα που πρέπει να ικανοποιηθούν προκειμένου να έχουμε αξιοπιστία σε ικανοποιητικά επίπεδα. Το θέμα που θα σχολιάσουμε εδώ είναι τα περιθώρια που έχουμε ώστε να μειωθούν αυτές οι απαιτήσεις και έτσι με το μικρότερο δυνατό κόστος σε απώλειες να έχουμε αύξηση του επιπέδου της αξιοπιστίας. Αρχικά ας σχολιάσουμε για τους κόμβους. Δεν είναι απαραίτητο για όλους τους κόμβους να παίρνουν όλες τις πληροφορίες, όμως υπάρχουν κόμβοι που οι λειτουργίες που εκτελούν απαιτούν όλες το μέγεθος της πληροφορίας και κάποιοι άλλοι που είναι πιθανό να καταρεύσουν αν δεν λάβουν όλες τις πληροφορίες. Συνεχίζοντας να αναφερθούμε στην πληροφορία και τη σημασία της. Πιθανότατα όλο το εύρος της πληροφορίας δεν είναι εξίσου σημαντικό, επομένως η ορθότητα και τα χρονικά περιθώρια για την αποστολή τους δεν είναι το ίδιο σημαντικά για όλα τα δεδομένα κάτι που ευνοεί την καλύτερη κάλυψη κάποιων τμημάτων της πληροφορίας έναντι άλλων. Για παράδειγμα μπορούμε να μειώσουμε τις απώλειες ανά πλαίσιο αν παρέχουμε CRC και/ή FEC μόνο σε τμήματα του πακέτου αφήνοντας τα λιγότερο σημαντικά τμήματα να περιέχουν σφάλματα, αλλά προστατεύοντας τα τμήματα που είναι απαραίτητα για την ανακατασκευή. Επίσης μπορούμε να έχουμε χαλάρωση σε θέματα που αφορούν την ακολουθιακή μετάδοση των δεδομένων (αξιόπιστη, αλλά όχι σειριακή μετάδοση όλων των δεδομένων διαχωρίζοντας πολλαπλά και ανεξάρτητα σειριακά ρεύματα μετάδοσης) και στις συγκρούσεις.

7.4 ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΙΣ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

ΤΟ ΥΠΟΔΕΙΓΜΑ ΤΗΣ ΠΟΛΙΤΕΙΑΣ ΓΙΟΥΤΑ.

Το πρώτο νομοθετικό κείμενο που ρύθμισε την ψηφιακή υπογραφή βασισμένη στη μέθοδο των ασύμμετρων αλγορίθμων είναι ο νόμος περί ψηφιακής υπογραφής της πολιτείας Γιούτα των ΗΠΑ που ισχύει από τις 9 Μαρτίου 1995. ο νόμος αυτός επιτρέπει τη συγκρότηση οργανισμών, δημοσίου ή ιδιωτικού δικαίου, οι οποίοι κατόπιν Άδειας του Υπουργείου Εμπορίου, μπορούν να εκδίδουν πιστοποιητικά σχετικά με τη ταυτότητα συγκεκριμένου συνδρομητή τους. Τα πιστοποιητικά βεβαιώνουν ότι συγκεκριμένη δημόσια κλειδιά ανήκει σε ορισμένο πρόσωπο και παρέχει όλα τα αναγκαία στοιχεία για τη χρησιμοποίηση της στην αποκρυπτογράφηση της ψηφιακής υπογραφής του αποστολέα εγγράφου. Οι οργανισμοί αυτοί υποχρεούνται να τηρούν στοιχεία τουλάχιστον για 40 χρόνια. Η μυστική κλείδα ανήκει στην ιδιοκτησία του συνδρομητή, ο οποίος είναι υπεύθυνος για την ασφαλή τήρησή της. Ο νόμος καθιερώνει επίσης νομικό τεκμήριο, σύμφωνα με το οποίο η αποκρυπτογράφηση ενός μηνύματος με τη χρησιμοποίηση της δημόσιας κλείδας , όπως είναι αυτή καταχωρημένη στο πιστοποιητικό που βεβαιώνει την αντιστοιχία της συγκεκριμένης δημόσιας κλείδας και του συνδρομητή και συγχρόνως αποστολέα μηνύματος, θεωρείται ως αναγνώριση της γνησιότητας της υπογραφής. Το τεκμήριο ανατρέπεται, αν αποδειχθεί ότι η ψηφιακή υπογραφή δεν μπορεί να αποκρυπτογραφηθεί με τη δημόσια κλείδα ή αν ο δικαιούχος μυστικής κλείδας έχει απωλέσει τον αποκλειστικό έλεγχο της κατά το χρόνο θέσεως της υπογραφής. Αν δεν επιτρέπει το τεκμήριο, τότε το ηλεκτρονικό έγγραφο ισχύει όπως το χάρτινο.

Η ΟΔΗΓΙΑ 1999/93/ΕΚ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ

Η οδηγία 1999/93/εκ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου <<σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές>> εκδόθηκε στις 13 Δεκεμβρίου 1999.στόχος της οδηγίας είναι να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώριση τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίζει την ομαλή λειτουργία της εσωτερικής αγοράς. Δεν καλύπτει πτυχές που αφορούν τη σύναψη και την ισχύ συμβάσεων ή άλλων υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου και δεν θίγει κανόνες και περιορισμούς σχετικά με τη χρήση εγγράφων, οι οποίοι περιέχονται στο εθνικό ή κοινοτικό δίκαιο (άρθρο 1). Κατά την οδηγία ηλεκτρονική υπογραφή είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Σύμφωνα με το άρθρο 5 τα κράτη μέλη οφείλουν να εξισώσουν την ηλεκτρονική υπογραφή με την ιδιόχειρη και να την κάνουν δεκτή ως αποδεικτικό στοιχείο σε νομικές διαδικασίες. Αυτό ισχύει μόνο για τις προηγμένες ηλεκτρονικές υπογραφές, που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής. Προηγμένη είναι η ηλεκτρονική υπογραφή που συνδέεται μονοσήμαντα με τον υπογράφοντα., είναι ικανή να τον <<τακτοποιήσει>>, δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και συνδέεται με τα δεδομένα, στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων (άρθρο 2 παραγ 2).

Τα κράτη μέλη δεν πρέπει να απορρίπτουν τη νομική ισχύ και το παραδεκτό μιας ηλεκτρονικής υπογραφής, ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι υπό μορφή ηλεκτρονικών δεδομένων ή ότι δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο παροχέα υπηρεσιών πιστοποίησης ή δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Η οδηγία αυτή περιέχει σημαντικές διατάξεις για τους παροχείς υπηρεσιών πιστοποίησης των ηλεκτρονικών υπογραφών. Καμία έγκριση δεν χρειάζεται για την παροχή υπηρεσιών πιστοποίησης. Κάθε κράτος μέλος όμως οφείλει να εξασφαλίζει την καθιέρωση κατάλληλου συστήματος που καθιστά δυνατή την επιτήρηση των εγκατεστημένων στο έδαφος τους παροχέων υπηρεσιών πιστοποίησης, οι οποίοι εκδίδουν για το κοινό αναγνωρισμένα πιστοποιητικά (άρθρα 3 και 4).

ΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΓΡΑΦΑ

Α ΙΔΙΩΤΙΚΟ ΔΙΚΑΙΟ

Στην Ελλάδα, πριν από τη ρύθμιση σχετικά με την αναγνώριση της ψηφιακής υπογραφής ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων, ετίθετο το ζήτημα, αν μπορεί να εξομοιωθεί με την ιδιόχειρη υπογραφή. Το πρόβλημα παρίστατο δυσεπίλυτο, και η απάντηση, που έπρεπε να δοθεί, εξαρτάτο από την εξέλιξη της τεχνολογίας. Η αλήθεια είναι ότι μέχρι σήμερα το ηλεκτρονικό έγγραφο δεν παρέχει την απαραίτητη εγγύηση σταθερότητας της καταγραφής των δηλώσεων βουλήσεως. Πολύ εύκολα μπορούν να επιχειρηθούν αλλοιώσεις του καταγαραφόμενου κειμένου. Το αντίθετο συμβαίνει με τα έντυπα έγγραφα που περιέχουν ιδιόχειρη υπογραφή. Ακριβώς για΄ αυτόν τον λόγο δεν ήταν δυνατό πριν το π.δ 150/2001 να εξομοιωθούν οι ιδιόχειρες με τις ηλεκτρονικές υπογραφές. Συνεπώς το ηλεκτρονικό έγγραφο, αν χρησιμοποιείτο ως συστατικός τύπος δικαιοπραξίας, οδηγούσε στη σύναψη άκυρων δικαιοπραξιών κατά το άρθρο 443 κΠολΔ. Αντιθέτως παραδεκτά χρησιμοποιείτο το έγγραφο αυτό ως αποδεικτικό, διότι το άρθρο 444 αριθμ3 ΚΠολΔ, το οποίο αποτελεί και το νομικό θεμέλιο του ηλεκτρονικού εγγράφου, δέχεται ως έγγραφα μηχανικές απεικονίσεις, στις οποίες η θέση ιδιόχειρης υπογραφής είναι τεχνικά αδύνατη. Γι ’αυτό και είναι δυνατό να υπάρξει έμμεση απόδειξη σχετικά με τον εκδότη του κειμένου, σύμφωνα με το άρθρο 457 παρ 4 ΚΠολΔ, που επιβάλλει την απόδειξη της γνησιότητας των μηχανικών απεικονίσεων από το πρόσωπο που τις επικαλείται.

Σύμφωνα με το άρθρο 14 παρ 2 νοείται ως <<ψηφιακή υπογραφή, η ψηφιακής μορφής υπογραφή σε δεδομένα ή συννημένη σε δεδομένα ή λογικά συσχετιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη αποδοχής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή

1. συνδέεται μονοσήμαντα με τον υπογράφοντα
2. ταυτοποιεί τον υπογράφοντα
3. δημιουργείται με μέσα, τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχο του και
4. συνδέεται με τα δεδομένα, στα οποία αναφέρεται κατά κάποιο τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων. >>

Το άρθρο 14 παράγ. 19 και 20 παρέχει εξουσιοδότηση σχετικά με τον τρόπο θέσης και τη λειτουργία της ψηφιακής υπογραφής: <<Με προεδρικό διάταγμα, που εκδίδεται με πρόταση των Υπουργών Εσωτερικών, Δημοσίας Διοίκησης και Αποκέντρωσης, Οικονομικών, Ανάπτυξης και Μεταφορών και Επικοινωνιών καθορίζονται οι προϋποθέσεις και η διαδικασία έκδοσης, διακίνησης, διαχείρισης της ψηφιακής υπογραφής, οι προϋποθέσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης, οι τεχνικοί άξονες για την κατάρτιση, την αποστολή, τη διατήρηση, την αντιγραφή και την αναπαραγωγή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εγγύηση της ακεραιότητας, διάθεσης και διατήρησης των πληροφοριών που περιέχονται στο μήνυμα, καθώς και κάθε άλλη αναγκαία λεπτομέρεια. Με το ίδιο π.δ μπορεί να καθορίζονται και οι κατηγορίες μηνυμάτων, τα οποία έχουν ισχύ και χωρίς να φέρουν ψηφιακή υπογραφή. Με το ανώτερο προεδρικό διάταγμα , μπορεί να επεκτείνεται η διακίνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου μεταξύ δημοσίων υπηρεσιών , Ν.Π.Δ.Δ και ΟΤΑ ή μεταξύ αυτών και των φυσικών και νομικών προσώπων ιδιωτικού δικαίου σε όλες ή ορισμένες από τις αναφερόμενες στην παράγ. 3 του άρθρου 14 κατηγορίες εγγράφων.

Η ψηφιακή υπογραφή επιφέρει τα αποτελέσματα της ιδιόχειρης υπογραφής, κατά την κείμενη νομοθεσία. Το μήνυμα ηλεκτρονικού ταχυδρομείου που φέρει ψηφιακή υπογραφή σύμφωνα με το προεδρικό διάταγμα της παραγράφου 19 έχει την αποδεικτική ισχύ εγγράφου κατά τους ορισμούς του Κώδικα Πολιτικής Δικονομίας και κάθε άλλη σχετικής διάταξης.

Το προεδρικό διάταγμα 150/2001 για τις ηλεκτρονικές υπογραφές που ενσωματώνει την οδηγία 1999/93/ΕΚ περιλαμβάνει αντίστοιχες προβλέψεις αναφορικά με τα αναγνωριζόμενα είδη ηλεκτρονικών υπογραφών, τις έννομες συνέπειες, τη διεθνή αναγνώριση τους καθώς και τη λειτουργία, ευθύνη και εποπτεία των Παροχών Υπηρεσιών Πιστοποίησης.

Το προεδρικό διάταγμα υιοθετώντας τον ορισμό της οδηγίας προσδιορίζει την <<ηλεκτρονική υπογραφή>> ως δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Με την ευρεία αυτή διατύπωση το π.δ δεν απαιτεί πρόσθετες διακριτικές ιδιότητες για την αναγνώριση της ηλεκτρονικής υπογραφής. Ταυτόχρονα όμως εισάγει την έννοια της προηγμένης ηλεκτρονικής υπογραφής, η οποία και κατά την οδηγία υπό τον όρο τήρησης των πρόσθετων προϋποθέσεων που διατυπώνονται έχει αυξημένη νομική ισχύ στις συναλλαγές του ηλεκτρονικού εμπορίου. Οι αυστηρές αυτές προϋποθέσεις είναι:

1. να συνδέεται η υπογραφή αυτή μονοσήμαντα με τον υπογράφοντα
2. να είναι ικανή να προσδιορίσει ειδικά και αποκλειστικώς την ταυτότητα του υπογράφοντα
3. να δημιουργείται με μέσα του αποκλειστικού ελέγχου του υπογράφοντα
4. να συνδέεται με τέτοιο τρόπο με τα δεδομένα στα οποία αναφέρεται ώστε να είναι εύκολο να διαπιστωθεί οποιαδήποτε στιγμή τυχόν αλλοίωση σε αυτά και τέλος η μέθοδος δημιουργίας της να κρίνεται ασφαλής, εννοώντας ότι το υλικό/λογισμικό δημιουργίας της πρώτης πρέπει να ανταποκρίνεται στις προδιαγραφές του παραρτήματος ΙΙΙ του π.δ.

Οι προδιαγραφές είναι αντίστοιχες με αυτές της οδηγίας, όπου ορίζεται ότι τα χρησιμοποιούμενα δεδομένα πρέπει να είναι μονοσήμαντα, να μην μπορούν με εύλογη βεβαιότητα να αντληθούν από άλλες πηγές και να

προστατεύονται αποτελεσματικά κατά του κινδύνου πλαστογραφίας ή χρησιμοποίησης από τρίτους. Πέρα από την τήρηση των ως άνω ουσιαστικών προϋποθέσεων για την απόκτηση της αυξημένης νομικής ισχύος θα πρέπει η ‘’η προηγμένη ηλεκτρονική υπογραφή’’ να περιβάλλεται με την οριζόμενη πιστοποίηση από ένα τρίτο ανεξάρτητο πρόσωπο αποκαλούμενο ‘’Πάροχο Υπηρεσιών Πιστοποίησης ‘’. Ο όρος ‘’πιστοποιητικό’’ αναφέρεται στης ηλεκτρονικής μορφής βεβαίωση η οποία συνδέει τα δεδομένα επαλήθευσης ηλεκτρονικής υπογραφής με ένα άτομο και βεβαιώνει την ταυτότητα του για τις ανάγκες των ηλεκτρονικών συναλλαγών.

Ωστόσο δίνεται στον Πάροχο η δυνατότητα να ορίζει περιορισμούς χρήσης του πιστοποιητικού και όρια ύψους των συναλλαγών, υπό τον όρο ότι οι απαλλαγές αυτές του παροχέα καθίστανται σαφείς στους τρίτους και δεν θίγουν τα δικαιώματα του καταναλωτή. Με αυτόν τον τρόπο θεμελιώνεται η ευθύνη των Παροχών ως νόθος αντικειμενική και επιρρίπτεται το βάρος απόδειξης στον Πάροχο που επικαλείται να αποδείξει έλλειψης ευθύνης του κατά το χρόνο έκδοσης του πιστοποιητικού.

Υπό το πρίσμα της κοινοτικής ενοποίησης ορίζεται στο π.δ ότι τα πιστοποιητικά παροχών υπηρεσιών που προέρχονται από άλλα κράτη μέλη , εφόσον συνάδουν με τις προβλέψεις της οδηγίας, γεννούν τις ίδιες συνέπειες όπως και τα εκδιδόμενα στην Ελλάδα. Για τους παρόχους τους εγκατεστημένους εκτός Ευρωπαϊκής Ένωσης ορίζει ρητώς το άρθρο 5 παράγ. 4 του π.δ ότι αυτά καθίστανται νομικώς ισοδύναμα προς τα εκδιδόμενα εντός της ένωσης εφόσον:

1. ο πάροχος πληροί τις προϋποθέσεις της ελληνικής νομοθεσίας και έχει διαπιστευτεί εθελοντικώς σε οποιοδήποτε κράτος της ένωσης ή
2. για το συγκεκριμένο πιστοποιητικό έχει εγγυηθεί πάροχος εγκατεστημένος εντός της Ευρωπαϊκής Ένωσης ή
3. το συγκεκριμένο πιστοποιητικό έχει εκδοθεί με βάση διμερή ή πολυμερή σύμβαση.

Β ΠΟΙΝΙΚΗ ΠΡΟΣΤΑΣΙΑ

Τα ηλεκτρονικά έγγραφα απολαμβάνουν και ποινική προστασία. Συγκεκριμένα <<έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό , μαγνητικό ή άλλο τρόπο, για εγγραφή , αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα , σύμβολο ή ήχος αυτοτελώς ή σε συνδυασμό, εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία>>.

Είναι γενικά παραδεκτό ότι για να θεωρηθεί ένα έγγραφο <<γραπτό>> ή <<σημείο>> κατά την έννοια του π.δ απαιτείται να έχει τρείς βασικές ιδιότητες: διάρκεια, εγγύηση, απόδειξη. Διάρκεια υπάρχει, όταν υπάρχει σταθερή ενσωμάτωση σε μια ύλη ενός διανοητικού περιεχομένου. Εγγύηση υπάρχει όταν από τη σταθερή ενσωμάτωση υπάρχει, ποιά είναι η πηγή της προέλευσης του δηλ ο εκδότης. Απόδειξη τέλος υπάρχει, όταν το διανοητικό αυτό περιεχόμενο προορίζεται ή είναι απλώς πρόσφορο να αποδείξει γεγονότα σημαντικά για το δίκαιο. Το πρόβλημα των εγγράφων στο διαδίκτυο παρουσιάζει ιδιαιτερότητες. Οι ηλεκτρονικές επιστολές, οι ιστοσελίδες, το IRC (internet relay chat), τα αρχεία δεδομένων, τα προγράμματα έχουν διαφορετική λειτουργία και γι’ αυτό θεωρούνται όλα έγγραφα.

Οι ηλεκτρονικές επιστολές αποθηκεύονται στον υπολογιστή του παραλήπτη και στον υπολογιστή του αποστολέα. Ενσωματώνονται σταθερά σε υλικό φορέα (δηλ στο σκληρό δίσκο) και συνεπώς επιτελούν διαιωνιστική λειτουργία. Ως προς την εγγυητική λειτουργία υπάρχει έγγραφο από τη στιγμή που αποστέλλονται και κυκλοφορούν στο διαδίκτυο. Με αυτόν τον τρόπο αποκτούν σύνδεση με την ηλεκτρονική διεύθυνση του αποστολέα. Η ύπαρξη ονόματος αποστολέα αποτελεί επαρκές στοιχείο σύνδεσης με τον εκδότη και συνεπώς είναι αδιάφορο για το χαρακτηρισμό της επιστολής ως εγγράφου. Αντιθέτως, η ύπαρξη ενός συνδυασμού υπαρκτού ονόματος, υπαρκτής ψηφιακής διευθύνσεως, ψηφιακής υπογραφής, αλλά και η ύπαρξη στοιχείων σχετικά με τη διαδρομή του μηνύματος που επιτρέπει στον παραλήπτη να ελέγξει κατά μεγάλο ποσοστό την αυθεντικότητα της προέλευσης του μηνύματος., είναι στοιχεία αρκετά για να προσδώσουν στις ηλεκτρονικές επιστολές τον χαρακτήρα εγγράφων.

Τα ίδια ισχύουν και για το περιεχόμενο των ηλεκτρονικών επιστολών. Η αλλοίωση τους είναι μεν εφικτή, αλλά προϋποθέτει παρεμβάσεις που αφήνουν ίχνη. Όλα αυτά ισχύουν και για τους ταχυδρομικούς καταλόγους. Οι ιστοσελίδες περιέχουν δεδομένα που αποθηκεύονται τόσο στον υπολογιστή του δημιουργού τους όσο και και στον υπολογιστή του παροχέα, που φιλοξενεί τα δεδομένα. Πληρούνται κατ΄ αυτόν τον τρόπο οι προϋποθέσεις σταθερής ενσωμάτωσης των δεδομένων σε υλικό φορέα και επιτελείται συνεπώς η διαιωνιστική λειτουργία. Οι ιστοσελίδες επιτελούν και την εγγυητική λειτουργία και θεωρούνται έγγραφα από τη στιγμή που αποθηκεύονται στον υπολογιστή του παροχέα. Με αυτόν τον τρόπο αποκτούν σύνδεση με την

ηλεκτρονική διεύθυνση του διαθέτοντος την ιστοσελίδα, και στο βαθμό που η ηλεκτρονική διεύθυνση μπορεί να δηλώσει το πρόσωπο που είναι εκφραστής του διανοητικού περιεχομένου των δεδομένων, τα δεδομένα να συνδέονται με συγκεκριμένο πρόσωπο-εκδότη, οπότε διασφαλίζεται η εγγυητική λειτουργία. Αν όμως η διεύθυνση περιέχει ψευδώνυμα, φανταστικά ονόματα, περιγραφές κτ.λ , τότε δεν υπάρχει σύνδεση με κανένα εκδότη και συνεπώς δεν υφίσταται έγγραφο.

Η επικοινωνία μέσω IRC, δηλαδή μέσω αποστολής γραπτών προτάσεων διακομιστή- server που φιλοξενεί το δίαυλο συζητήσεως, δεν μπορεί να θεωρηθεί ότι συνιστά έγγραφο. Αφενός δεν επιτελείται η διαιωνιστική λειτουργία, αφού τα μηνύματα εμφανίζονται στις οθόνες μόνο για λίγα λεπτά, αφετέρου οι συμμετέχοντες χρησιμοποιούν ψευδώνυμα, γεγονός που αποτρέπει τη σύνδεση του διανοήματος με κάποιον εκδότη. Αυτό ισχύει και για τις ομάδες συζητήσεων, την τηλεφωνία, την τηλεδιάσκεψη και τη ραδιοφωνική αναμετάδοση προγραμμάτων.

Το αποθηκευμένο σε σκληρό δίσκο έχει διαιωνιστική λειτουργία καθώς είναι σταθερά ενσωματωμένο σε υλικό φορέα. Για να επιτελεί όμως και την εγγυητική λειτουργία και να θεωρηθεί έγγραφο πρέπει να υπάρχουν και πρόσθετα στοιχεία που να θεμελιώνουν τη σύνδεση προγράμματος- εκδότη. Όσον αφορά τα αρχεία που είναι αποθηκευμένα σε σκληρό δίσκο υπολογιστή, δεν αποτελούν έγγραφα γιατί δεν συνδέονται άμεσα και ουσιαστικά με τον εκδότη και επιπλέον συχνά δεν έχουν αποδεικτική σημασία. Η κυριότητα ή η φυσική κατοχή του μηχανήματος δεν σημαίνουν τίποτε για τον δημιουργό των δεδομένων. Αυτά δεν ισχύουν για τα FTP sites, δηλαδή τα πρωτόκολλα μεταφοράς αρχείων που, εφόσον είναι επώνυμα, βάσει της ψηφιακής διευθύνσεως τους μπορούν να συνδεθούν με τον εκδότη τους και ενδεχομένως να θεωρηθούν έγγραφα.

Εφόσον γίνει δεκτό ότι υφίσταται διαδικτυακό έγγραφο κατά την έννοια του άρθρου 13 του π.δ τότε είναι δυνατό να εφαρμοστούν οι διατάξεις των άρθρων. Η καθιέρωση της ψηφιακής υπογραφής θα διευρύνει κι άλλο την έννοια των εγγράφων κατά το άρθρο 13 και παράλληλα το πεδίο προστασίας τους. Και σε αυτή την περίπτωση , η αυξανόμενη χρήση του διαδικτύου και η εξέλιξη της τεχνολογίας θα δημιουργήσουν μια νέα κοινωνική πραγματικότητα, την οποία ο νομοθέτης οφείλει να παρακολουθεί λαμβάνοντας τις ορθές αποφάσεις.

ΟΙ ΡΥΘΜΙΣΕΙΣ ΤΟΥ Π.Δ 150/2001

Με το π.δ. 150/2001 , το οποίο εκδόθηκε σε συμμόρφωση προς την κοινοτική οδηγία 1999/93, αναγνωρίζονται οι τεχνολογίες ηλεκτρονικής υπογραφής, καθορίζονται οι έννομες συνέπειές τους και ρυθμίζεται η παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών. Ως ηλεκτρονική υπογραφή νοούνται τα <<δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτό και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας>>(αρθρο 2 αριθμ1 π.δ 150/2001).
Από τον ορισμό αυτό γίνεται σαφές ότι στην έννοια της ηλεκτρονικής υπογραφής εμπίπτουν οι τεχνικές κρυπτογράφησης, με τις οποίες κρυπτογραφείται όλο ή τμήμα του ηλεκτρονικού εγγράφου. Για το σκοπό χρησιμοποιείται μια διάταξη δημιουργίας υπογραφής (άρθρο 2 αριθμ.5) , δηλ κατάλληλο λογισμικό, και κλειδιά κρυπτογραφίας που ορίζονται ως δεδομένα επαλήθευσης υπογραφής(άρθρο 2 αριθμ. 7).

Η προηγούμενη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή, σύμφωνα με την ορολογία του π.δ 150/2001, εξομοιώνεται με την ιδιόχειρη υπογραφή. Ειδικότερα, σύμφωνα με το άρθρο 3 παράγραφος 1, η προηγούμενη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο ουσιαστικό όσο και στο δικονομικό δίκαιο. Ως <<προηγμένη ηλεκτρονική υπογραφή>> ορίζεται η ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:

1. συνδέεται μονοσήμαντα με τον υπογράφοντα
2. είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος
3. δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο
4. συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων (άρθρο 2 αριθμ. 2). Επιπρόσθετα, πρέπει η προηγμένη ηλεκτρονική υπογραφή να βασίζεται σε αναγνωρισμένο πιστοποιητικό και να δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Από τα παραπάνω γίνεται σαφές ότι μόνο τεχνολογίες ηλεκτρονικής υπογραφής που βασίζονται στο ασύμμετρο σύστημα κρυπτογράφησης πληρούν τις προϋποθέσεις για να θεωρούν ως προηγμένες υπογραφές, ενώ σαφώς δεν τις πληρούν τα συμμετρικά συστήματα που χρησιμοποιούν ένα μόνο κλειδί, το οποίο δεν μπορεί να παραμείνει μυστικό.
Η εξομοίωση της προηγμένης ηλεκτρονικής με την ιδιόχειρη υπογραφή σημαίνει ότι όπου προβλέπεται έγγραφος τύπος από το νόμο ή από τη συμφωνία των μερών, το ηλεκτρονικό έγγραφο με την ηλεκτρονική υπογραφή επέχει θέση ιδιωτικού εγγράφου με την έννοια του άρθρου 160 ΑΚ και θεωρείται, κατά πλάσμα δικαίου, ως ιδιωτικό έγγραφο κατά το άρθρο 443 ΚΠολΔ.

Παραπέρα, σύμφωνα με το άρθρο 3 παράγραφος 2 π.δ 150/2001, σε περίπτωση όπου η ηλεκτρονική υπογραφή δεν είναι προηγμένη ή δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό ή δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, η ισχύς της ηλεκτρονικής υπογραφής ή το παραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο τον λόγο αυτό. Η διάταξη αυτή έχει έχει ερμηνευτικό χαρακτήρα και δεν καθορίζει τις έννομες συνέπειες της απλής ηλεκτρονικής υπογραφής, με συνέπεια να εξακολουθεί να παραμείνει ζητούμενο η εξακρίβωση της νομικής ισχύος της απλής ηλεκτρονικής υπογραφής.

Κατά την άποψή μας, η <<απλή>> ηλεκτρονική υπογραφή μπορεί να παρέχει τα εχέγγυα για την εγκυρότητα των συμβάσεων, για την εγκυρότητα των συμβάσεων, για τις οποίες δεν προβλέπεται έγγραφος τύπος και δύναται, συνεπώς να έχει αποδεικτική αξία. Συγκεκριμένα, το έγγραφο που φέρει απλή ηλεκτρονική υπογραφή μπορεί να χρησιμοποιηθεί ως αποδεικτικό έγγραφο κατά το άρθρο 444 αριθμ.3 ΚΠολΔ, καθ' όσον εμπίπτει ευχερώς στην έννοια της μηχανικής απεικόνισης. Ασφαλώς, όμως, δεν δύναται να εξομοιωθεί με την ιδιόχειρη υπογραφή, αφού κάτι τέτοιο θα αντέβαινε στο νόμο και πιο συγκεκριμένα, στο ρθρο 3 παράγραφος 1 του π.δ 150/2001, και συνεπώς , δεν δύναται να χρησιμοποιηθεί ως υποκατάστατο της ηλεκτρονικής υπογραφής σε δικαιοπραξίες όπου ο έγγραφος τύπος είναι συστατικός.

Όσον αφορά τα ηλεκτρονικά έγγραφα που δεν φέρουν καθενός είδους ηλεκτρονική υπογραφή, η απόδειξη της γνησιότητας τους καθίσταται δυνατή, καταρχήν, με τη βοήθεια των διδαγμάτων των κοινής πείρα κατά την εφαρμογή της μεθόδου της έμμεσης δια τεκμηρίων απόδειξης, χωρίς να αποκλείεται και η θεώρηση τους ως μηχανικών απεικονίσεων. Αξίζει να σημειωθεί ότι στην ελληνική νομολογία αναγνωρίζεται η αποδεικτική αξία των ηλεκτρονικών εγγράφων που περιέχονται σε μηνύματα ηλεκτρονικής αλληλογραφίας. Πιο συγκεκριμένα, έγινε δεκτό ότι η εκτύπωση των ηλεκτρονικών εγγράφων και των ηλεκτρονικών επιστολών μπορεί να θεωρηθεί ως μηχανική απεικόνιση, η οποία εμπίπτει στην έννοια του ιδιωτικού εγγράφου με αποδεικτική δύναμη. Το π.δ 150/2001 ρυθμίζει περαιτέρω, την παροχή υπηρεσιών πιστοποίησης. Αυτές παρέχονται από <<παροχής υπηρεσιών πιστοποίησης>> οι οποίοι μπορεί να είναι φορείς, φυσικά ή νομικά πρόσωπα, με αρμοδιότητα να εκδίδουν πιστοποιητικά ή να παρέχουν άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές. Τα πιστοποιητικά που εκδίδουν οι παροχής υπηρεσιών πιστοποίησης είναι ηλεκτρονικές βεβαιώσεις που συνδέουν τα δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνουν έτσι την ταυτότητα του (άρθρο 2 αριθμ 9). Οι παροχείς υπηρεσιών πιστοποίησης τελούν υπό την εποπτεία της εθνικής επιτροπής τηλεπικοινωνιών και ταχυδρομείων και πρέπει να συμμορφώνονται με τους όρους που προβλέπονται στην υπ' αριθμό 248/71 Απόφαση της ΕΕΤΤ (<<Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής>>).

Σύμφωνα με το παράρτημα ιι του π.δ 150/2001, μεταξύ άλλων, οι παροχείς υπηρεσιών πιστοποίησης πρέπει να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης, σύμφωνα με τα εκάστοτε ισχύοντα κριτήρια, να καταγράφουν τις αναγκαίες πληροφορίες, ώστε να ελέγχουν τη γνησιότητα των πιστοποιητικών και το χρόνο έκδοσης ή ανάκλησης τους και να προβαίνουν σε επαλήθευση της ταυτότητας του κατόχου του πιστοποιητικού. Οι παροχείς που εκδίδουν αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυώνται για την ακρίβεια ενός τέτοιου πιστοποιητικού, ευθύνονται έναντι τρίτου για τη ζημιά που προκλήθηκε σε βάρος του και η ευθύνη αυτή καθορίζεται στο νόμο ως νόθος αντικειμενική, καθ' όσον προβλέπεται ότι ο παροχέας δεν ευθύνεται , αν αποδείξει ότι δεν τον βαρύνει πταίσμα (άρθρο 6 παράγραφος 3 π.δ 150/2001).

Η συλλογή των προσωπικών δεδομένων κατά την έκδοση πιστοποιητικού πρέπει να περιορίζεται στο απολύτως απαραίτητο μέτρο. Συγκεκριμένα, ορίζεται ότι οι παροχείς υπηρεσιών πιστοποίησης συγκεντρώνουν προσωπικά δεδομένα μόνο απευθείας από το ενδιαφερόμενο πρόσωπο ή με ρητή συγκατάθεση του και μόνο εφόσον είναι απαραίτητο για την έκδοση και διατήρηση πιστοποιητικού, ενώ η συλλογή ή επεξεργασία δεδομένων για άλλους σκοπούς απαγορεύεται, χωρίς τη συγκατάθεση του ενδιαφερόμενου προσώπου (άρθρο 7).

Το άρθρο 14 του νόμου 2672/1998, όπως ισχύει σήμερα μετά τις τροποποιήσεις του άρθρου 10 του Ν. 3230/2004, αναφέρεται στην διακίνηση εγγράφων με ηλεκτρονικά μέσα (τηλεομοιοτυπία – ηλεκτρονικό

ταχυδρομείο) και προβλέπει την έκδοση Προεδρικού Διατάγματος που θα καθορίζει τις προϋποθέσεις και την διαδικασία έκδοσης, διακίνησης, διαχείρισης και εξασφάλισης της ψηφιακής υπογραφής.

Στη συνέχεια, το Προεδρικό Διάταγμα 150/2001 αποτελεί προσαρμογή στη σχετική Ευρωπαϊκή Οδηγία (1999/93ΕΚ) και έτσι αποδέχεται ότι μετά από ορισμένες διαδικασίες έκδοσης ψηφιακών υπογραφών και εφόσον συντρέχουν ορισμένες προϋποθέσεις, οι ψηφιακές υπογραφές έχουν την αυτή νομική ισχύ με αυτήν την οποία έχει η ιδιόχειρη υπογραφή.

Τέλος, το Προεδρικό Διάταγμα 342/2002 ρυθμίζει την διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων σε ορισμένες περιπτώσεις με υποχρεωτική ψηφιακή υπογραφή (π.χ. αποφάσεις, πιστοποιητικά κλπ.) και σε άλλες χωρίς ψηφιακή υπογραφή (εγκύκλιοι, οδηγίες κλπ.)

Το Προεδρικό Διάταγμα 150 του 2001 έχει σκοπό να εναρμονίσει την ελληνική νομοθεσία με την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις ηλεκτρονικές υπογραφές. Οι διατάξεις του παρόντος διατάγματος δεν θίγουν διατάξεις που επιβάλλουν τη χρήση ορισμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα.

Περιέχει ορισμούς των εννοιών ηλεκτρονική υπογραφή, προηγμένη ηλεκτρονική υπογραφή, ψηφιακή υπογραφή, υπογράφων, δεδομένα δημιουργίας υπογραφής, διάταξη δημιουργίας υπογραφής και άλλων. Ορίζει τις έννομες συνέπειες των ηλεκτρονικών υπογραφών δηλαδή ότι η ηλεκτρονική υπογραφή επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

Αναφέρει ποια νομοθεσία δεσμεύει τα φυσικά ή νομικά πρόσωπα που εκδίδουν πιστοποιητικά ηλεκτρονικών υπογραφών στην Ελλάδα και στο εξωτερικό αλλά και τις ευθύνες με τις οποίες βαρύνονται οι πάροχοι υπηρεσιών πιστοποίησης. Περιέχει διατάξεις για την προστασία των προσωπικών δεδομένων στην διαδικασία έκδοσης πιστοποιητικών. Τέλος στα παραρτήματα αναφέρονται ποια στοιχεία πρέπει απαραίτητα να περιλαμβάνονται στα αναγνωρισμένα πιστοποιητικά και τι πρέπει να διασφαλίζουν οι διαδικασίες δημιουργίας ηλεκτρονικής υπογραφής.

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 150.2001

ΠΡΟΣΑΡΜΟΓΗ ΣΤΗΝ ΟΔΗΓΙΑ 99/93/ΕΚ ΤΟΥ ΕΥΡΩΠΑΙΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΣΧΕΤΙΚΑ μΕ ΤΟ ΚΟΙΝΟΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ.

Συγκεκριμένα το παράρτημα ΙΙ του ΠΔ έχει τα εξής:

Διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής:

1.Οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον ότι:

α) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ' ουσία, μόνο μία φορά και ότι το απόρρητο είναι διασφαλισμένο.

.β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή

προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας.

γ) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους.

2. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν μμεταβάλλουν τα προς υπογραφή δεδομένα ούτε ποδίζουν την υποβολή των δεδομένων αυτών στο υπογράφοντα πριν
από τη διαδικασία υπογραφής.

Συγκεκριμένα το παράρτημα IV έχει τα εξής:

Συστάσεις για την ασφαλή επαλήθευση της υπογραφής κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται με εύλογη βεβαιότητα ότι:
α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση
της υπογραφής αντιστοιχούν στα δεδομένα που αφανίζονται στον επαληθεύοντα.

β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με ορθό τρόπο

γ) ο επαληθεύων μπορεί ενδεχομένως να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται,

δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία,

ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο,

στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς,

ζ) μορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.

Απόφαση ΕΕΤΤ 295/63/2003 Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης.

ΠΑΡΑΡΤΗΜΑ Ι

ΚΡΙΤΗΡΙΑ ΟΡΙΣΜΟΥ ΦΟΡΕΩΝ

το Προεδρικό Διάταγμα 150/2001 "Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαικού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές" (ΦΕΚ 125/Α/2001), και ιδίως το άρθρο 4, παράγραφοι 2, 5 και 8, το άρθρο 5 και το άρθρο 7 παράγραφος 1 αυτού,

Αρθρο 4 παράγραφοι:

2. Η ΕΕΤΤ υποχρεούται, εντός δέκα (10) εργάσιμων ημερών από την κατάθεση της αίτησης, να επιβεβαιώσει ότι η αίτηση αυτή περιλαμβάνει το σύνολο των εγγράφων τα οποία αναφέρονται στο Παράρτημα Ι του

παρόντος Κανονισμού και την παράγραφο 1 του παρόντος ή ειδικώς να προσδιορίσει ποιο έγγραφο υπολείπεται και να το ζητήσει εγγράφως από τον αιτούντα τον Ορισμό. Ο αιτών οφείλει να προσκομίσει το ως άνω έγγραφο εντός δεκαπέντε (15) ημερών από την κοινοποίηση του σχετικού εγγράφου της ΕΕΤΤ. Σε περίπτωση μη έγκαιρης υποβολής των στοιχείων από τον αιτούντα η αίτηση απορρίπτεται.

5. Με το πέρας του ελέγχου, η Επιτροπή Ελέγχου συντάσσει Έκθεση Αξιολόγησης του αιτούντος και την υποβάλλει στην ΕΕΤΤ η οποία με αιτιολογημένη απόφασή της αποφασίζει εντός προθεσμίας τεσσάρων (4) εβδομάδων από τη διενέργεια του επιτόπιου ελέγχου για τον Ορισμό του αιτούντος.

8. Πριν την έκδοση της ατομικής διοικητικής πράξης Ορισμού του Φορέα απαγορεύεται η έναρξη οποιωνδήποτε εργασιών που εμπίπτουν στα καθήκοντα του εκάστοτε οριζόμενου Φορέα Ελέγχου.

Απόφαση ΕΕΤΤ 295/64/2003 - Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων.

Ασφαλής κρυπτογραφική Μονάδα είναι προϊόν Ηλεκτρονικής Υπογραφής που προστατεύεται έναντι τροποποίησης και διασφαλίζει τεχνική και Κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης.

Φορέας για Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής και Ασφαλείς Κρυπτογραφικές Μονάδες ή Φορέας για Προϊόντα είναι ο αρμόδιος φορέας για τη διαπίστωση της συμμόρφωσης των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής .

Οι Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής οφείλουν να πληρούν τουλάχιστον τις απαιτήσεις του Παραρτήματος ΙΙΙ του ΠΔ 150/2001.

Οι Ασφαλείς κρυπτογραφικές Μονάδες οφείλουν να πληρούν τουλάχιστον τις εξής απαιτήσεις:

α) Η μυστικότητα και ακεραιότητα των παραγόμενων, αποθηκευόμενων και χρησιμοποιούμενων Δεδομένων Δημιουργίας Υπογραφής εξασφαλίζεται καθ' όλη τη διάρκεια ζωής τους,
β) Τα Δεδομένα Δημιουργίας Υπογραφής που χρησιμοποιούνται για την παραγωγή της υπογραφής δεν πρέπει να μπορούν, με εύλογη βεβαιότητα, να αντληθούν και η υπογραφή πρέπει να προστατεύεται από πλαστογραφία, με τα μέσα της σύγχρονης τεχνολογίας,
γ) Ο νόμιμος υπογράφων πρέπει να έχει τη δυνατότητα να προστατεύει αποτελεσματικά τα Δεδομένα Δημιουργίας Υπογραφής που χρησιμοποιούνται για την παραγωγή της υπογραφής έναντι της χρησιμοποίησής τους από τρίτους.

Άρθρο 1

Σκοπός - Πεδίο Εφαρμογής

Σκοπός της παρούσας Απόφασης είναι ο προσδιορισμός των κριτηρίων και της διαδικασίας ελέγχου συμμόρφωσης των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και των Ασφαλών κρυπτογραφικών Μονάδων προς τα Παραρτήματα ΙΙΙ και ΙΙ στ) του Π.Δ. 150/2001, αντιστοίχως.

Άρθρο 2

Ορισμοί

1. Ασφαλής κρυπτογραφική Μονάδα: Το χρησιμοποιούμενο, από τους Παρόχους Υπηρεσιών Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά, Προϊόν ΗλεκτρονικήςΥπογραφής που προστατεύεται έναντι τροποποίησης και διασφαλίζει τεχνική και Κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης, σύμφωνα με το Παράρτημα ΙΙ στ' του ΠΔ 150/2001 και πληροί τις απαιτήσεις της παραγράφου 2 του άρθρου 3 του παρόντος Κανονισμού.

2. Φορέας για Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής και Ασφαλείς Κρυπτογραφικές Μονάδες ή Φορέας για Προϊόντα: Ο αρμόδιος φορέας για τη διαπίστωση της συμμόρφωσης των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής με το Παράρτημα ΙΙΙ του Π.Δ. 150/2001 και των Ασφαλών κρυπτογραφικών Μονάδων, που ορίστηκε σύμφωνα με την προβλεπόμενη στην Απόφαση της ΕΕΤΤ ΑΠ 295/63/2003 "Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης" διαδικασία.

7. Εκθεση Αξιολόγησης: Το έγγραφο που περιέχει το σύνολο των αποτελεσμάτων της αξιολόγησης μιας Ασφαλούς Διάταξης Δημιουργίας Υπογραφής ή μιας Ασφαλούς κρυπτογραφικής Μονάδας σύμφωνα με τις απαιτήσεις του άρθρου 3του παρόντος Κανονισμού.

8. Λέξεις ή φράσεις, οι οποίες χρησιμοποιούνται στον παρόντα Κανονισμό, έχουν την έννοια η οποία τους αποδίδεται στο Προεδρικό Διάταγμα 150/2001, στην Απόφαση της ΕΕΤΤ 248/71/2002, στην Απόφαση της ΕΕΤΤ 295/63/2003 "Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης" ή σε περίπτωση που δεν αναφέρονται σε αυτά, την έννοια η οποία τους αποδίδεται στο Ν. 2867/2000 ή σε περίπτωση που δεν αναφέρονται σε αυτόν, στο σχετικό δευτερογενές δίκαιο της Ευρωπαϊκής Κοινότητας.

Άρθρο 3

Απαιτήσεις και Κριτήρια Αξιολόγησης

1. Οι Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής οφείλουν να πληρούν τουλάχιστον τις απαιτήσεις του Παραρτήματος ΙΙΙ του ΠΔ 150/2001.

α) Η μυστικότητα και ακεραιότητα των παραγόμενων, αποθηκευόμενων και χρησιμοποιούμενων Δεδομένων Δημιουργίας Υπογραφής εξασφαλίζεται καθ' όλη τη διαρκεια ζωης τους,

β) Τα Δεδομένα Δημιουργίας Υπογραφής που χρησιμοποιούνται για την παραγωγή της υπογραφής δεν πρέπει να μπορούν, με εύλογη βεβαιότητα, να αντληθούν και η υπογραφή πρέπει να προστατεύεται από πλαστογραφία, με τα μέσα της σύγχρονης τεχνολογίας,

γ) Ο νόμιμος υπογράφων πρέπει να έχει τη δυνατότητα να προστατεύει αποτελεσματικά τα Δεδομένα Δημιουργίας Υπογραφής που χρησιμοποιούνται για την παραγωγή της υπογραφής έναντι της χρησιμοποίησής τους από τρίτους.

3. Η αξιολόγηση της συμμόρφωσης ή μη προς τις απαιτήσεις των παρ, 1 και 2 του παρόντος άρθρου για τις Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής και τις Ασφαλείς κρυπτογραφικές Μονάδες, αντίστοιχα, διενεργείται με βάση τα κριτήρια, τα οποία προσδιορίζονται στο Παράρτημα του παρόντος Κανονισμού,

4. Η αξιολόγηση των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και των Ασφαλών Κρυπτογραφικών Μονάδων, η οποία διενεργείται σύμφωνα με την διαδικασία του άρθρου 4 του παρόντος Κανονισμού, θα πρέπει να αναφέρεται στις ακόλουθες λειτουργίες, στο μέτρο που αυτές παρέχονται:

α) Παραγωγή Δεδομένων Δημιουργίας Υπογραφής,

β) Μεταφορά Δεδομένων Δημιουργίας Υπογραφής σε αποθηκευτικό μέσο,

γ) Αποθήκευση Δεδομένων Δημιουργίας Υπογραφής,

δ) Δημιουργία υπογραφής

Άρθρο 4

Διαδικασία Διαπίστωσης Συμμόρφωσης

1. Η Διαπίστωση Συμμόρφωσης των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και των Ασφαλών κρτυπτογραφικών Μονάδων διενεργείται από τον Φορέα για Προϊόντα.

β) Βεβαίωση ότι το προϊόν πληροί τουλάχιστον τις απαιτήσεις του Παραρτήματος ΙΙΙ του ΠΔ 150/2001 και του άρθρου 3 παράγραφος 1 και 3 του παρόντος Κανονισμού, εάν πρόκειται για Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής, ή του Παραρτήματος ΙΙ στ) του ΠΔ 150/2001 και του άρθρου 3 παράγραφος 2 και 3 του παρόντος, εάν πρόκειται για Ασφαλείς Κρυπτογραφικές Μονάδες,

6. Η ισχύς του Πιστοποιητικού Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής ή Ασφαλών Κρυπτογραφικών Μονάδων άρχεται από της δημοσίευσής του στο Μητρώο που τηρεί η ΕΕΤΤ βάσει του άρθρου 8 του παρόντος Κανονισμού.

Άρθρο 8

Δημοσιότητα πιστοποιητικών

1. Η ΕΕΤΤ τηρεί Μητρώο των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και αντίστοιχα Μητρώο των Ασφαλών Κρυπτογραφικών Μονάδων για τα οποία χορηγήθηκε

Πιστοποιητικό Συμμόρφωσης από αρμόδιο Φορέα για Προϊόντα. Στο Μητρώο αναγράφονται τα στοιχεία του προϊόντος (όνομα, τύπος, έκδοση), τα στοιχεία του κατασκευαστή και όπου υπάρχει τα στοιχεία του εξουσιοδοτημένου αντιπροσώπου του (επωνυμία, διακριτικός τίτλος, έδρα, ΑΦΜ, νόμιμοι εκπρόσωποι) και τηρείται, επίσης, επικυρωμένο αντίγραφο του Πιστοποιητικού Συμμόρφωσης. Στο ίδιο Μητρώο αναγράφεται κάθε τροποποίηση των

προαναφερόμενων στοιχείων και όποια ανάκληση των Πιστοποιητικών Συμμόρφωσης.

Άρθρο 9

Καταγγελίες-Κυρώσεις

Καταγγελίες κατά των Φορέων ή των κατόχων Πιστοποιητικών Συμμόρφωσης πρέπει

να κατατίθενται στην ΕΕΤΤ, η οποία τις εξετάζει και δύναται να επιβάλει τις

διοικητικές κυρώσεις του άρθρου 12 παράγραφος 1 του Ν. 2867/2000 σε

συνδυασμό με το άρθρο 9 της Απόφασης της ΕΕΤΤ 295/63/2003 "Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και

Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης".

ΠΑΡΑΡΤΗΜΑ

Α. Κριτήρια Αξιολόγησης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής

Η αξιολόγηση διενεργείται με βάση τα εξής κριτήρια:

α) Κριτήρια Ασφάλειας Αξιολόγησης Πληροφοριακών Συστημάτων (Information

Technology Security Evaluation Criteria ITSEC), έκδοση 1.2 (Γραφείο Επίσημων

Δημοσιεύσεων των Ευρωπαϊκών Κοινοτήτων, 28 Ιουνίου 1991) ή της εκάστοτε

ισχύουσας έκδοσης με ελάχιστο επίπεδο αξιολόγησης Ε3 και βαθμολογία "υψηλή"

για την ελάχιστη ισχύ των μηχανισμών ασφάλειας ή

β) Κοινά Κριτήρια για την Αξιολόγηση Ασφάλειας Πληροφοριακών Συστημάτων

(Common Criteria for Information Technology Security Evaluation CC), όπως

αυτά διατυπώνονται στο Πρότυπο ISO/IEC 15408:1999, έκδοση 2.1 ή της εκάστοτε

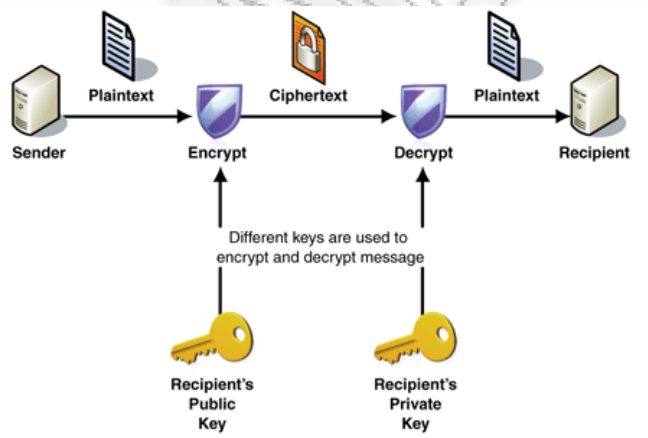
ισχύουσας έκδοσης με ελάχιστο επίπεδο αξιολόγησης Διασφάλισης "4", Επαυξημένο (Evaluation Assurance Level Augmented "EAL4+").

7.5 ΔΗΜΙΟΥΡΓΙΑ ΑΙΤΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ (CSR)

Η υποδομή δημόσιου κλειδιού

- Το ιδιωτικό κλειδί (private key), το οποίο πρέπει να το φτιάξει ο χρήστης και να το διαφυλάσσει προστατευμένο κατάλληλα. Η ασφάλεια της υποδομής δημοσίου κλειδιού εξαρτάται από την ασφάλεια του ιδιωτικού κλειδιού. Το ιδιωτικό κλειδί πρέπει να δημιουργηθεί επιτόπου, στον εξυπηρετητή στον οποίο πρόκειται να χρησιμοποιηθεί το πιστοποιητικό και να προστατευθεί με κατάλληλα δικαιώματα πρόσβασης.
- Το αίτημα υπογραφής πιστοποιητικού (certificate signing request - CSR), το οποίο θα αποσταλεί προς υπογραφή μέσω της υπηρεσίας PKI του ΕΔΕΤ. Η Αρχή Πιστοποίησης θα επιτρέψει ένα υπογεγραμμένο ψηφιακό πιστοποιητικό το οποίο μπορεί να χρησιμοποιήσει ο χρήστης στις υπηρεσίες που επιθυμεί.
- Την αλυσίδα εμπιστοσύνης (certificate trust chain) που συνοδεύει το πιστοποιητικό. Η αλυσίδα αυτή περιλαμβάνει όλες τις ενδιάμεσες αρχές πιστοποίησης που οδηγούν στη Μητρική Αρχή (Root Certification Authority).

Δημιουργία ιδιωτικού κλειδιού και αιτήματος υπογραφής πιστοποιητικού



Χρήση του λογισμικού OpenSSL

Συνδεθείτε στον εξυπηρετητή για τον οποίο θέλετε το πιστοποιητικό και ακολουθήστε τα παρακάτω βήματα

Δημιουργία ιδιωτικού κλειδιού

```
$ touch key.pem
$ chmod 640 key.pem
$ openssl genrsa 2048 > key.pem
Generating RSA private key, 2048 bit long modulus
..+++
.....+++
e is 65537 (0x10001)
```

Προσοχή! Το ιδιωτικό κλειδί πρέπει να προστατεύεται με κατάλληλα δικαιώματα πρόσβασης (permissions). Οποιοσδήποτε αποκτήσει πρόσβαση στο ιδιωτικό κλειδί μπορεί να προσποιηθεί την ταυτότητα του εξυπηρετητή και να υποκλέψει τα δεδομένα που διακινούνται μέσα από το κανάλι ασφαλούς επικοινωνίας.

Προσοχή! Αν το ιδιωτικό κλειδί χαθεί ή σβηστεί, τότε το πιστοποιητικό είναι άχρηστο. Γι' αυτό προτείνεται η τήρηση ενός αντιγράφου ασφαλείας του ιδωτικού κλειδιού σε ασφαλή τοποθεσία.

Δημιουργία αιτήματος υπογραφής πιστοποιητικού

```
$ openssl req -new -key key.pem -nodes
```

Θα ερωτηθείτε σχετικά με τα στοιχεία που θέλετε να περιλαμβάνει το πιστοποιητικό. Πρέπει υποχρεωτικά να συμπληρώσετε το «Common Name», το οποίο πρέπει να συμπίπτει με το πλήρες όνομα (fully-qualified domain name - FQDN) του εξυπηρετητή για τον οποίο ζητάτε το πιστοποιητικό. Αν ο εξυπηρετητής έχει περισσότερα του ενός ονόματα (π.χ. www.example.com και mail.example.com) δώστε εδώ το κύριο και η εφαρμογή του ΕΔΕΤ θα σας δώσει τη δυνατότητα να προσθέσετε τα επιπλέον ονόματα κατά τη διάρκεια της διαδικασίας έκδοσης του πιστοποιητικού.

Τα υπόλοιπα στοιχεία είναι προαιρετικά. Το όνομα χώρας, το όνομα του οργανισμού και η τοποθεσία δε λαμβάνονται υπ' όψιν και συμπληρώνονται αυτόματα με τα αντίστοιχα στοιχεία του φορέα στον οποίο υποβάλλεται το αίτημα.

Τέλος, μην ορίσετε συνθηματικό για το αίτημα.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Lakonia
Locality Name (eg, city) []:Sparti
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Some organization
Organizational Unit Name (eg, section) []:Some unit
```

```
Common Name (eg, YOUR name) []:www.example.com
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
-----BEGIN CERTIFICATE REQUEST-----
MIICvzCCAacCAQAwejELMAkGA1UEBhMCR1IxEDAOBgNVBAgTB0xha29uaWExDzAN
BgNVBAcTBlNwYXJ0aTEaMBgGA1UEChMRU29tZSBvcmdhbml6YXRpb24xEjAQBgNV
BAsTCVNvbWUgdW5pdDEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtAR3RZavJpfC/hAdzb+/O2fgdSEPlVJw
nAS6IYnEKLGp7qmaPGQZK06tl6FAIAepU8i9bXfcnX4k9JvIzsEBAm454SyTVcGo
jxQ4buadLQyLSNiK9nEMbMexkwYZkYkOHGb7OmBcw1FT3Jhr1sqCRMPhUjE4UttS
dhc5bNo2IZK34c9GipnOQ6dz3IVa/21JGgPbm6b0wuv4i9R8YQs6d0ElUlIya2VS
6Kd3gB+3U87URqneYUdL6gYqzVGV/Fc1R+HsoBl8P3VWybKDHaLXXxnIC84av4nM
c+20C8gUuUAwXdd2/uhNnU4lVTc8HwjB9LxL0RJvGSMno/H8vy9VUwIDAQABoAAw
DQYJKoZIhvcNAQEFBQADggEBAEyke2DL8Pay015JLeC6elzC8uBuPtO5gYHdlmIQ
lE2MnFzjWWvWF8Y5eCUtJv+ccmL3Yj6YvtjoEN5VyWLUdVABrrnv+F+yXRTRPD+3
sm9Rd/XWSrv+Gu5KPZ2RtuligTwljMZ7MLGkH8HvZzhNnb0rKzILVVybbVns5kTp
sjqYBdS0CSAzsrMyYItUjLg/alhnFA/c3rG9B+nrQrbfr8+K+JgV+I2z3cTuXLiw
dSdgj9+KosvH8K+gwtAcB1FQ3lamYr1hcGWzOg9seF122JfpWxmXqW8D5lPntrDs
TXwM9KO+aSDtF4ei4Y52wniB9spK5K+3bbWr3MBL6WqZ1KE=
-----END CERTIFICATE REQUEST-----
```

Στη συνέχεια, το κείμενο που βρίσκεται ανάμεσα στις γραμμές «BEGIN CERTIFICATE REQUEST» και «END CERTIFICATE REQUEST», συμπεριλαμβανομένων των γραμμών αυτών, δηλαδή το:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvzCCAacCAQAwejELMAkGA1UEBhMCR1IxEDAOBgNVBAgTB0xha29uaWExDzAN
BgNVBAcTBlNwYXJ0aTEaMBgGA1UEChMRU29tZSBvcmdhbml6YXRpb24xEjAQBgNV
BAsTCVNvbWUgdW5pdDEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtAR3RZavJpfC/hAdzb+/O2fgdSEPlVJw
nAS6IYnEKLGp7qmaPGQZK06tl6FAIAepU8i9bXfcnX4k9JvIzsEBAm454SyTVcGo
jxQ4buadLQyLSNiK9nEMbMexkwYZkYkOHGb7OmBcw1FT3Jhr1sqCRMPhUjE4UttS
dhc5bNo2IZK34c9GipnOQ6dz3IVa/21JGgPbm6b0wuv4i9R8YQs6d0ElUlIya2VS
6Kd3gB+3U87URqneYUdL6gYqzVGV/Fc1R+HsoBl8P3VWybKDHaLXXxnIC84av4nM
c+20C8gUuUAwXdd2/uhNnU4lVTc8HwjB9LxL0RJvGSMno/H8vy9VUwIDAQABoAAw
DQYJKoZIhvcNAQEFBQADggEBAEyke2DL8Pay015JLeC6elzC8uBuPtO5gYHdlmIQ
lE2MnFzjWWvWF8Y5eCUtJv+ccmL3Yj6YvtjoEN5VyWLUdVABrrnv+F+yXRTRPD+3
sm9Rd/XWSrv+Gu5KPZ2RtuligTwljMZ7MLGkH8HvZzhNnb0rKzILVVybbVns5kTp
sjqYBdS0CSAzsrMyYItUjLg/alhnFA/c3rG9B+nrQrbfr8+K+JgV+I2z3cTuXLiw
dSdgj9+KosvH8K+gwtAcB1FQ3lamYr1hcGWzOg9seF122JfpWxmXqW8D5lPntrDs
TXwM9KO+aSDtF4ei4Y52wniB9spK5K+3bbWr3MBL6WqZ1KE=
-----END CERTIFICATE REQUEST-----
```

πρέπει να αντιγραφεί και να επικολληθεί στην εφαρμογή έκδοσης ψηφιακών πιστοποιητικών του ΕΔΕΤ, στο πεδίο «CSR (PEM format)».

Χρήση του λογισμικού GnuTLS

Δημιουργία ιδιωτικού κλειδιού

```
$ certtool -p --outfile key.pem
Generating a 2048 bit RSA private key...
```

Προσοχή! Το ιδιωτικό κλειδί πρέπει να προστατεύεται με κατάλληλα δικαιώματα πρόσβασης (permissions). Οποιοσδήποτε αποκτήσει πρόσβαση στο ιδιωτικό κλειδί μπορεί να προσποιηθεί την ταυτότητα του εξυπηρετητή και να υποκλέψει τα δεδομένα που διακινούνται μέσα από το κανάλι ασφαλούς επικοινωνίας.

Προσοχή! Αν το ιδιωτικό κλειδί χαθεί ή σβηστεί, τότε το πιστοποιητικό είναι άχρηστο. Γι' αυτό προτείνεται η τήρηση ενός αντιγράφου ασφαλείας του ιδωτικού κλειδιού σε ασφαλή τοποθεσία.

Δημιουργία αιτήματος υπογραφής πιστοποιητικού

```
$ certtool -q --load-privkey key.pem
```

Θα ερωτηθείτε σχετικά με τα στοιχεία που θέλετε να περιλαμβάνει το πιστοποιητικό. Πρέπει υποχρεωτικά να συμπληρώσετε το «Common Name», το οποίο πρέπει να συμπίπτει με το πλήρες όνομα (fully-qualified domain name - FQDN) του εξυπηρετητή για τον οποίο ζητάτε το πιστοποιητικό. Αν ο εξυπηρετητής έχει περισσότερα του ενός ονόματα (π.χ. www.example.com και mail.example.com) δώστε εδώ το κύριο και η εφαρμογή του ΕΔΕΤ θα σας δώσει τη δυνατότητα να προσθέσετε τα επιπλέον ονόματα κατά τη διάρκεια της διαδικασίας έκδοσης του πιστοποιητικού.

Τα υπόλοιπα στοιχεία είναι προαιρετικά. Το όνομα χώρας, το όνομα του οργανισμού και η τοποθεσία δε λαμβάνονται υπ' όψιν και συμπληρώνονται αυτόματα με τα αντίστοιχα στοιχεία του φορέα στον οποίο υποβάλλεται το αίτημα.

Τέλος, μην ορίσετε συνθηματικό για το αίτημα.

```
Generating a PKCS #10 certificate request...
Country name (2 chars): GR
Organization name: Sample Organization
Organizational unit name: Some unit name
Locality name: Sparti
State or province name: Lakonia
Common name: www.example.com
UID:
Enter a challenge password:
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC0zCCAb0CAQAwgYExCzAJBgNVBAYTAkdSMRwwGgYDVQQKExNTYW1wbGUgT3Jn
YW5pemF0aW9uMRcwFQYDVQQLEw5Tb21lIHVuaXQgbmFtZTEQMA4GA1UEBxMHTGFr
b25pYTEPMA0GA1UECBMGU3BhcnRpMRgwFgYDVQQDEw93d3cuZXhhbXBsZS5jb20w
ggEfMAsGCSqGSIb3DQEBAQOCAQ4AMIIBCQKCAQDX3rBMNN9CfjcEPBWnX6zp4fyq
3WFJYVKeKmAnYTbAKR4WsnLJ7j428tRZ72+U0IjXizeo6ZwUZW2BRhSwNL+AdH/u
olLyCSPUkXDPtO7SN3mLlTytanyQyAPIYxqRHR8IsDPzAysEylqQH8DHqw9/bwGM
RyYWTFVMfLjxMmqbJutm3KxpOtvfmCP30srYTdJw6bC8viOyg8Ai93I+nT9Ozhn0
/+xzKIdGkMhulzcP/FaltEoZsyPjijyz8tOVPS6f7H3B5OPFYid9kWTM6iUA2UYc
ofg+33b25SkM0tnfF1mjJzyO6giq+qoIVfZjN+j+zYLZdA31M+M1GuOQlLuNAgMB
AAGgETAPBgkqhkiG9w0BCQcxAhMAMAsGCSqGSIb3DQEBBQOCAQEAIj1sQNeTDeTa
ZMvITxho2IljkRbiYSMRBlvGyOWioqbHe9xWbqTCO+eh2xh5SCqfQdFAuM3oXTJ0
hvv5A0GCwysJxMs//l8GwIusiR9CaDrxkrziacAy2G2pY5KfltOFPF1/SK2jJlEC
```

```
fKWyqsZ9l5zFgNCxjo5Dz9pxBFBgZ8fp2zjJCaW3f1a8IVAxf6YaNlLBS8YlvLq0
YlhAtlZV98rQ2FRzNPLzdV0ZUukkpGfholEeLyRf81iPIL3bWF9lMRF3JopJUV3S
Q/zhkKvtzX3KQgsIea43PGkcVXCj1inxi7ODa8W4LPhGN15vn0n5GDqltLlGPsNR
awSlJVVjkw==
-----END NEW CERTIFICATE REQUEST-----
```

Στη συνέχεια, το κείμενο που βρίσκεται ανάμεσα στις γραμμές «BEGIN CERTIFICATE REQUEST» και «END CERTIFICATE REQUEST», συμπεριλαμβανομένων των γραμμών αυτών, δηλαδή το:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0zCCAb0CAQAwgYExCzAJBgNVBAYTAkdSMRwwGgYDVQQKExNTYW1wbGUgT3Jn
YW5pemF0aW9uMRcwFQYDVQQLEw5Tb21lIHVuaXQgbmFtZTEQMA4GA1UEBxMHTGFr
b25pYTEPMA0GA1UECBMGU3BhcnRpMRgwFgYDVQQDEw93d3cuZXhhbXBsZS5jb20w
ggEfMAsGCSqGSIb3DQEBAQOCAQ4AMIIBCQKCAQDX3rBMNN9CfjcEPBWnX6zp4fyq
3WFJYVKeKmAnYTbAKR4WsnLJ7j428tRZ72+U0IjXizeo6ZwUZW2BRhSwNL+AdH/u
olLyCSPUkXDPtO7SN3mLlTytanyQyAPIYxqRHR8IsDPzAysEylqQH8DHqw9/bwGM
RyYWTFVMfLjxMmqbJutm3KxpOtvfmCP30srYTdJw6bC8viOyg8Ai93I+nT9Ozhn0
/+xzKIdGkMhulzcP/FaltEoZsyPjijyz8tOVPS6f7H3B5OPFYid9kWTM6iUA2UYc
ofg+33b25SkM0tnfF1mjJzyO6giq+qoIVfZjN+j+zYLZdA31M+M1GuOQlLuNAgMB
AAGgETAPBgkqhkiG9w0BCQcxAhMAMAsGCSqGSIb3DQEBBQOCAQEAIj1sQNeTDeTa
ZMvITxho2IljkRbiYSMRBlvGyOWioqbHe9xWbqTCO+eh2xh5SCqfQdFAuM3oXTJ0
hvv5A0GCwysJxMs//l8GwIusiR9CaDrxkrziacAy2G2pY5KfltOFPF1/SK2jJlEC
fKWyqsZ9l5zFgNCxjo5Dz9pxBFBgZ8fp2zjJCaW3f1a8IVAxf6YaNlLBS8YlvLq0
YlhAtlZV98rQ2FRzNPLzdV0ZUukkpGfholEeLyRf81iPIL3bWF9lMRF3JopJUV3S
Q/zhkKvtzX3KQgsIea43PGkcVXCj1inxi7ODa8W4LPhGN15vn0n5GDqltLlGPsNR
awSlJVVjkw==
-----END CERTIFICATE REQUEST-----
```

πρέπει να αντιγραφεί και να επικολληθεί στην εφαρμογή έκδοσης ψηφιακών πιστοποιητικών του ΕΔΕΤ, στο πεδίο «CSR (PEM format)».

7.6 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ API

«Υπογραφή API μόνο ενεργοποιηθεί με Aloaha 25 + άδειες

Αντικείμενο aloaha Δημ. pdf '

Λόγο υπογραφή Δημ. λόγο »

Υπογραφή Δημ. τοποθεσία «φυσική θέση

Inputpdf Δημ. infile '

Outputpdf Δημ. outfile »- μπορεί να είναι το ίδιο με inputpdf

Image Δημ. εικόνας »που πρέπει να χρησιμοποιούνται για την υπογραφή - κενό string επιτρέπεται

Πιστοποιητικό Δημ. cert »που πρέπει να χρησιμοποιούνται. Μπορεί να είναι είτε UniqueContainerName ή Serialnumber

Δημ. x Mediabox x1 'αρχίσει

Δημ. y Mediabox έναρξη y1 »
Δημ. x Mediabox x2 "τέλος
Δημ. y Mediabox τέλος y2 »
PageHeight Δημ. ph '- 0 για την αυτόματη
Pagewidth Δημ. PW '- 0 για την αυτόματη
Δημ. XOFF «x-offset αν η σελίδα δεν ξεκινούν από το 0
Υ Δημ. yoff «αντιστάθμιση αν η σελίδα δεν ξεκινούν από το 0
String Mediabox Δημ. Mediabox »
Σελίδα Δημ. σελίδα »που πρέπει να χρησιμοποιούνται
Δημ. px1 «x1 συντονίζουν ως ποσοστό της πλήρους σελίδας (επάνω αριστερά)
Δημ. py1 «y1 coordinage ως ποσοστό της πλήρους σελίδας (επάνω αριστερά)
Δημ. px2 «x2 coordinage ως ποσοστό της πλήρους σελίδας (κάτω δεξιά)
Δημ. py2 «y2 coordinage ως ποσοστό της πλήρους σελίδας (κάτω δεξιά)

px1 = 84
py1 = 8

px2 = 99
py2 = 2

XOFF = 0
yoff = 0

λόγος = "Δημιούργησα αυτό το έγγραφο"
location = "είμαι στο γραφείο"

»που μοναδικό όνομα δοχείο του πιστοποιητικού. serialnumber μπορεί να χρησιμοποιηθεί επίσης
cert = "9e82c38e348ddcf70d58e0a21f56d6f6_dc4ff486-0fc3-4b64-B582-b94a2eba4ba5"

»που υπογραφή σελίδα όπου θα εμφανίζονται
page = 1

που ονομάτων αρχείων »
infile = "c: \ pdf \ input.pdf"
outfile = "c: \ pdf \ output.pdf"

«δημιουργία αντικείμενο
Set pdf = CreateObject ("aloahapdf.edit")

pdf.currentpage = CLng (σελίδα)

»που ImagePath υπογραφή. Πρέπει να είναι ένα χρώμα jpg αρχείο. empty string επίσης δυνατό
image = pdf.aloahapath + "jpg \ george1.jpg"

«κτλ Mediabox μόνο εάν χρειάζεται PageSize είναι άγνωστη εντοπίσει αυτόματα και δεν θα πρέπει να χρησιμοποιούνται.
Mediabox = pdf.get_pagesize_s (CStr (infile), CLng (σελίδα))
Αν Mediabox <> "" Then
x1 = Trim (split (Mediabox) (0))

```
y1 = Trim (split (Mediabox) (1))
x2 = Trim (split (Mediabox) (2))
y2 = Trim (split (Mediabox) (3))
pH = Abs (y2-y1)
pw = Abs (x2-x1)
Άλλος
ph = 0
pw = 0
End If

»που PageHeight pagewidth και 0 για να εντοπίσει αυτόματα
'ph = 0
«pw = 0

Εάν pH> 0 Then
yoff = ((y1/ph) * 100) \ 1
Άλλος
yoff = 0
End If
Αν pw> 0 Then
XOFF = ((x1/pw) * 100) \ 1
Άλλος
XOFF = 0
End if
```

Καλέστε pdf.sign_pdf_file (CStr (infile), CStr (outfile), CLng (PW), CLng (ph), CLng (px1 + XOFF), CLng (py1 + yoff), CLng (px2 + XOFF), CLng (py2 + yoff), CStr (λόγος), CStr (τοποθεσία), CStr (CERT), CStr (image))

Set pdf = δεν

Τέλος κώδικα.

7.7 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ DSS

Το Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard, DSS), δημοσιεύθηκε από το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (NIST) το οποίο καθορίζει ένα σύστημα ψηφιακών υπογραφών, για γενική χρήση. Το DSS περι-γράφει έναν αλγόριθμο ψηφιακής υπογραφής, τον DSA (Digital Signature Algorithm), οποίος βασίζεται σε ασύμμετρη κρυπτογραφία. Σε αντίθεση με τα συστήματα ψηφιακών υπογραφών που περιγράψαμε, ο DSA αναφέρεται αποκλειστικά σε σύστημα ψηφιακών υπογραφών και δεν μπορεί να χρησιμοποιηθεί ως κρυπτοσύστημα.Ο DSA είναι μια τροποποίηση του συστήματος ψηφιακής υπογραφής ElGamal. Επομένως, η ασφάλειά του βασίζεται στο πρόβλημα του υπολογισμού του διακριτού λογάριθμου.

Όπως όλα τα συστήματα ψηφιακών υπογραφών , έτσι και ο DSA αποτελείται από τον καθορισμό των ασύμμετρων παραμέτρων (των κλειδιών), το πρωτόκολλο ψηφιακής υπογραφής και το πρωτόκολλο επαλήθευσης της υπογραφής.

Κατά τη δημιουργία των κλειδιών, το κάθε μέλος θα πρέπει να εκτελέσει τα ακόλουθα βήματα. Αρχικά, επιλέγεται ένας πρώτος αριθμός q τέτοιος ώστε $2^{159} < q < 2^{160}$. Από τα όρια αυτά φαίνεται ότι το μέγεθος του

αριθμού q θα είναι ίσο με 160 bits. Στη συνέχεια επιλέγεται πρώτος αριθμός p τέτοιος ώστε $2^{t-1} < p < 2^{t}$, με 512 ≤ t ≤ 1024, και ο t να είναι ακέραιο πολλαπλάσιο του 64. Επίσης ο q θα πρέπει να διαιρεί τον (p–1).
Με βάση τους πρώτους αριθμούς p και q, επιλέγεται γεννήτορας a μιας κυκλικής υποομάδας τάξης q της ομάδας $\mathbf{Z}_p^*$. Αυτό επιτυγχάνεται επιλέγοντας $g \in \mathbf{Z}_p^*$ τέτοιο ώστε:
και θέτουμε
.
Στη συνέχεια, επιλέγεται τυχαίος ακέραιος τέτοιος ώστε 0 < b < q, και υπολογίζεται ο:
.
Η τετράδα (p, q, a, y) αποτελεί το δημόσιο κλειδί, ενώ ο b αποτελεί το ιδιωτικό κλειδί.
Το πρωτόκολλο υπογραφής ενός μηνύματος m αποτελείται από τα ακόλουθα βήματα:

1. Επιλογή τυχαίου μυστικού ακέραιου k τέτοιου ώστε 0 < k <q.

2. Υπολογισμός του $r \equiv (a^{k} \bmod p) \pmod q$.

3. Υπολογισμός του $k^{-1} \bmod q$.

4. Υπολογισμός του $s \equiv k^{-1} (h(m) + br) \pmod q$.

Η ψηφιακή υπογραφή του μηνύματος m είναι το ζεύγος (s, r). Κατά την επαλήθευση της ψηφιακής υπογραφής εκτελείται το ακόλουθο πρωτόκολλο:

1. Έλεγχος ότι 0<r,s<q. Σε περίπτωση που κάποιο από τα r,s δεν είναι εντός των καθορισμένων ορίων, η υπογραφή απορρίπτεται.

2. Υπολογισμός του $w=s^{-1} \bmod q$.

3. Υπολογισμός των:

. qbr)(mod))□+

4. Υπολογισμός του .

5. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν r = r΄.
() qyaruumod 2 1 ≡ ′ q p y a q p a q b u u k qb u u k ws q wbr m wh wks q br m h ks m h k s u u k mod) mod (mod) mod ( ) (mod) (mod) ( ) (mod) ( ) (mod) (((2 1 2 1 2 1 1 = □ + ≡ □+ ≡ □ □ + ≡ □ + ≡ ≡ −
Το παράδοξο της επαλήθευσης της υπογραφής του τελευταίου βήματος είναι ότι η ποσότητα r δεν εξαρτάται από το μήνυμα, οπότε δεν είναι ευθέως φανερό πως μπορεί να πραγματοποιηθεί η επαλήθευση χωρίς την άμεση συμβολή του μη-νύματος που υπογράφηκε. Ωστόσο, μπορούμε να επαληθεύσουμε την εγκυρότητα της υπογραφής με την ισοδυναμία του τελευταίου βήματος του πρωτοκόλλου επαλήθευσης ως εξής:
ή ισοδύναμα, r΄ = r. ( ) .

7.8 ΑΛΓΟΡΙΘΜΟΣ RSA

Ο αλγόριθμος RSA

1. Η Alice επιλέγει τυχαία δύο
πρώτους αριθμούς p, q ϵ ZN*
2. Η Alice υπολογίζει N = p * q
3. Η Alice διαλέγει αριθμό e
4. Η Alice υπολογίζει αριθμό d ϵ ZN*,
ώστε

Κρυπτογραφία Δημόσιου Κλειδιού
Ο αλγόριθμος RSA

Κρυπτογράφηση:
Αποκρυπτογράφηση:
H. Mel, D. Baker.
Cryptography Decrypted.
Addison-Wesley, 2001
$e * d = 1 \bmod \varphi(N)$

Δημόσιο Κλειδί : (e, N)
Ιδιωτικό Κλειδί : d
(Υπολογιστική) Ασφάλεια
RSA problem. Ανάγεται στο:
Factoring problem: Πρόβλημα εύρεσης πρώτων παραγόντων μεγάλων αριθμών
Για μεγάλο N, (>= 1024 bit), «δύσκολο» να βρεθούν οι πρώτοι παράγοντες p και q
Υπολογιστικά Αδύνατο

ΠΑΡΑΔΕΙΓΜΑ

Example 10.16

Say $p = 11$, $q = 23$, and $e = 3$. Then $N = 253$, $\phi(N) = 220$, and $d = 147$.

To encrypt the binary message $m = 0111001$ with textbook RSA and the public key $pk = \langle N = 253, e = 3 \rangle$, simply interpret m as the number 57 (and hence an element of $\mathbb{Z}^*_{253}$) in the natural way. Then compute

$$250 := [57^3 \bmod 253].$$

To decrypt, compute $57 := [250^{147} \bmod 253]$. Alternatively, using the Chinese remainder theorem the receiver could compute

$$250^{[147 \bmod 10]} \bmod 11 = 8^7 \bmod 11 = 2$$

and

$$250^{[147 \bmod 22]} \bmod 23 = 20^{15} \bmod 23 = 11.$$

Indeed, $57 \leftrightarrow (2, 11)$ and so decryption succeeds. (The desired answer can be recovered from the representation $(2, 11)$ as described in Section 7.1.5.) ◊

7.9 ΑΛΓΟΡΙΘΜΟΣ DES

Του DES (Data Encryption Standard) Ο αλγόριθμος είναι το πιο ευρέως χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης στον κόσμο. Για πολλά χρόνια, και μεταξύ πολλών ανθρώπων, "καθιστώντας μυστικό κωδικό" και DES έχουν συνώνυμα. Και παρά το πρόσφατο πραξικόπημα από το Electronic Frontier Foundation για τη δημιουργία μιας μηχανής 220.000 δολάρια για να σπάσουμε DES-κρυπτογραφημένα μηνύματα, DES θα ζουν με το κυβέρνησης και τραπεζών για τα επόμενα χρόνια μέσα από τη ζωή την επέκταση έκδοση ονομάζεται "Triple-DES."

DES λειτουργεί σε bits, ή δυαδικούς αριθμούς - τα 0s και 1s κοινές ψηφιακών υπολογιστών. Κάθε ομάδα τεσσάρων bits κάνει ένα δεκαεξαδικό, ή βάση 16, αριθμός. Binary "0001" είναι ίσο με το δεκαεξαδικό αριθμό

"1", binary "1000" είναι ίσο με το δεκαεξαδικό αριθμό "8", "1001" είναι ίσο με το δεκαεξαδικό αριθμό "9", "1010" είναι ίσο με το δεκαεξαδικό αριθμό "A", και "1111" είναι ίσο με το δεκαεξαδικό αριθμό "F".

DES έργα κρυπτογράφηση ομάδες των 64 bits μήνυμα, το οποίο είναι το ίδιο με 16 δεκαεξαδικούς αριθμούς. Για να γίνει η κρυπτογράφηση, DES χρησιμοποιεί "κλειδιά", όπου είναι επίσης προφανώς 16 δεκαεξαδικό αριθμούς, προφανώς ή 64 bits καιρό. Ωστόσο, κάθε 8ης βασικό κομμάτι αγνοείται στον αλγόριθμο DES, έτσι ώστε η αποτελεσματική βασικό μέγεθος είναι 56 bits. Αλλά, εν πάση περιπτώσει, 64 bits (16 δεκαεξαδικά ψηφία) ο αριθμός γύρω από το οποίο είναι DES οργανωμένη.

Για παράδειγμα, αν πάρουμε το plaintext μήνυμα "8787878787878787", και να κρυπτογραφήσετε το με το DES κλειδί "0E329232EA6D0D73", θα καταλήξουμε με το ciphertext "0000000000000000". Αν η ciphertext είναι αποκρυπτογραφούνται με το ίδιο μυστικό DES κλειδί "0E329232EA6D0D73", το αποτέλεσμα είναι το αρχικό plaintext "8787878787878787".

Το παράδειγμα αυτό είναι πετυχημένος και ομαλή επειδή plaintext μας ήταν ακριβώς 64 bits καιρό. Το ίδιο θα ίσχυε αν η plaintext έτυχε να είναι πολλαπλάσιο των 64 bits. Αλλά τα περισσότερα μηνύματα που δεν θα εμπίπτουν στην κατηγορία αυτή. Δεν θα αποτελέσει ακριβές πολλαπλάσιο των 64 bits (δηλαδή, ένα ακριβές πολλαπλάσιο των 16 δεκαεξαδικούς αριθμούς).

Για παράδειγμα, λαμβάνει το μήνυμα "Τα χείλη σου είναι ομαλότερη από βαζελίνη". Αυτό το μήνυμα plaintext είναι 38 bytes (76 δεκαεξαδικά ψηφία) καιρό. Έτσι, αυτό το μήνυμα πρέπει να είναι παραγεμισμένο με κάποια επιπλέον bytes στην ουρά τέλος για την κρυπτογράφηση. Όταν το κωδικοποιημένο μήνυμα έχει αποκρυπτογραφηθούν, είναι αυτά τα επιπλέον bytes πετιούνται. Υπάρχουν, φυσικά, διάφορα συστήματα padding - διαφορετικούς τρόπους να προσθέσετε επιπλέον bytes. Εδώ θα προσθέσω μόνο 0s στο τέλος, έτσι ώστε το συνολικό μήνυμα είναι πολλαπλάσιο των 8 bytes (ή 16 δεκαεξαδικό ψηφίο, ή 64 μπιτ).

ΣΥΜΠΕΡΑΣΜΑ

Οι επιθέσεις στο διαδίκτυο αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων. Καθημερινά ανακοινώνονται καινούργιες αδυναμίες στο λογισμικό και νέοι τρόποι επίθεσης. Με δεδομένη την εξέλιξη αυτή, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που αυτά περιέχουν και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Η ηλεκτρονική υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των ηλεκτρονικών εγγράφων. Έχει δηλαδή μία επιβεβαιωτική λειτουργία, βοηθώντας τον παραλήπτη να βεβαιωθεί ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις.

ΠΑΡΑΡΤΗΜΑ –ΝΟΜΟΙ-ΟΔΗΓΙΕΣ

1. ΝΟΜΟΣ 2472/1997

Σκοπός του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.

Για τους σκοπούς του παρόντος νόμου νοούνται ως:

α) "Δεδομένα προσωπικού χαρακτήρα", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

β) "Ευαίσθητα δεδομένα", τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Ειδικά για τα σχετικά με ποινικές διώξεις ή καταδίκες δύναται να επιτραπεί η δημοσιοποίηση μόνον από την εισαγγελική αρχή για τα αδικήματα που αναφέρονται στο εδάφιο β' της παραγράφου 2 του άρθρου 3 με διάταξη του αρμόδιου Εισαγγελέα Πρωτοδικών ή του Εισαγγελέα Εφετών, εάν η υπόθεση εκκρεμεί στο Εφετείο. Η δημοσιοποίηση αυτή αποσκοπεί στην προστασία του κοινωνικού συνόλου, των ανηλίκων, των ευάλωτων ή ανίσχυρων πληθυσμιακών ομάδων και προς ευχερέστερη πραγμάτωση της αξίωσης της Πολιτείας για τον κολασμό των παραπάνω αδικημάτων.

γ) "Υποκείμενο των δεδομένων", το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

δ) "Επεξεργασία δεδομένων προσωπικού χαρακτήρα" ("επεξεργασία"), κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.

ε) "Αρχείο δεδομένων προσωπικού χαρακτήρα" ("αρχείο"), κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια.

στ) "Διασύνδεση", μορφή επεξεργασίας που συνίσταται στην δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας ή που τηρούνται από τον ίδιο υπεύθυνο επεξεργασίας για άλλο σκοπό.

ζ) "Υπεύθυνος επεξεργασίας", οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.

η) "Εκτελών την επεξεργασία", οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

θ) "Τρίτος", κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.

ι) "Αποδέκτης", το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι.

ια) “Συγκατάθεση” του υποκειμένου των δεδομένων, κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για τον σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

ιβ) “Αρχή”, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που θεσπίζεται στο κεφάλαιο Δ΄ του παρόντος νόμου.

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

1. Οι διατάξεις του παρόντος νόμου εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.
2. Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών.
3. Ο παρών νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:
   α) Από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο.
   β) Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους- Μέλους της Ευρωπαϊκής Ένωσης ή κράτους του Ευρωπαϊκού Οικονομικού Χώρου, αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινική δίωξη.

Η ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

1. Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει :
   α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.
   β) Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.
   γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
   δ) Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.

2. Η τήρηση των διατάξεων της προηγούμενης παραγράφου βαρύνει τον υπεύθυνο επεξεργασίας. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή,

εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει την διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλέγει ή τύχει επεξεργασίας.

Προϋποθέσεις επεξεργασίας

1. Επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.
2. Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν:

   α) Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο.

   β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

   γ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

   δ) Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

   ε) Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

   3. Η Αρχή μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης.

2. ΝΟΜΟΣ 3471/2006

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002)

Σκοπός των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

Ορισμοί

Πέραν των ορισμών που περιλαμβάνονται στο άρθρο 2 του ν. 2472/1997 (ΦΕΚ 50 Α'), όπως ισχύει, λαμβανομένων δε υπόψη των ορισμών του ν. 3431/2006 (ΦΕΚ 13 Α') νοούνται, για τους σκοπούς του νόμου αυτού, ως:

1. «συνδρομητής»: κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής

διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.

2. «χρήστης»: κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

3. «δεδομένα κίνησης»: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.

4. «δεδομένα θέσης»: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

5. «επικοινωνία»: κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Δεν περιλαμβάνονται πληροφορίες που διαβιβάζονται ως τμήμα ραδιοτηλεοπτικών υπηρεσιών στο κοινό μέσω δικτύου ηλεκτρονικών επικοινωνιών, εκτός από τις περιπτώσεις κατά τις οποίες οι πληροφορίες μπορούν να αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει.

6. «κλήση»: σύνδεση που πραγματοποιείται μέσω μίας διαθέσιμης στο κοινό τηλεφωνικής υπηρεσίας που επιτρέπει αμφίδρομη επικοινωνία σε πραγματικό χρόνο.

7. «Υπηρεσία προστιθέμενης αξίας»: κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή δεδομένων θέσης πέραν εκείνων που απαιτούνται για τη μετάδοση μίας επικοινωνίας και τη χρέωση της.

8. «Ηλεκτρονικό ταχυδρομείο»: κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη.

9. «Υπηρεσίες ηλεκτρονικών επικοινωνιών»: οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και υπηρεσίες της Κοινωνίας της Πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του π.δ. 39/2001 (ΦΕΚ 28 Α'), και που δεν αφορούν, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών.

10. «Δημόσιο δίκτυο επικοινωνιών»: το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

11. «Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών»: οι υπηρεσίες ηλεκτρονικών επικοινωνιών που παρέχονται στο κοινό.

Αρθρο 3

Πεδίο εφαρμογής

1. Οι διατάξεις των άρθρων 1 έως 17 του παρόντος νόμου έχουν εφαρμογή κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, εφαρμόζεται ο ν. 2472/1997 (ΦΕΚ 50 Α'), όπως ισχύει.

2. Ο ν. 2472/1997, όπως ισχύει, και οι εκτελεστικοί του άρθρου 19 του Συντάγματος νόμοι, όπως ισχύουν, εφαρμόζονται για κάθε ζήτημα σχετικό με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, που δεν ρυθμίζεται ειδικότερα από τον παρόντα νόμο.

3. Οι διατάξεις των άρθρων 8 και 9 εφαρμόζονται στις γραμμές συνδρομητών που συνδέονται με

ψηφιακά κέντρα και, όταν αυτό είναι τεχνικώς εφικτό, σε γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα, εφόσον τούτο δεν συνεπάγεται δυσανάλογη οικονομική επιβάρυνση. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) διαπιστώνει τις περιπτώσεις όπου η σύνδεση με αναλογικά κέντρα είναι τεχνικώς αδύνατη ή απαιτεί δυσανάλογη επένδυση, και ενημερώνει σχετικώς την Ευρωπαϊκή Επιτροπή.

Αρθρο 4

Απόρρητο

1. Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, όπως ορίζονται στις διατάξεις του άρθρου 2 του παρόντος νόμου, προστατεύεται από το απόρρητο των επικοινωνιών.

Η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος.

2. Απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο.

3. Επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, υπό την προϋπόθεση ότι και τα δύο μέρη, μετά από προηγούμενη ενημέρωση σχετικά με το σκοπό της καταγραφής, παρέχουν τη συγκατάθεση τους. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθορίζεται ο τρόπος ενημέρωσης των μερών και παροχής της συγκατάθεσης, καθώς και ο τρόπος και ο χρόνος διατήρησης των καταγεγραμμένων συνδιαλέξεων και των συναφών δεδομένων κίνησης.

4. Με την επιφύλαξη της τήρησης των υποχρεώσεων που απορρέουν από την προστασία του απορρήτου, σύμφωνα με τον παρόντα νόμο, επιτρέπεται η τεχνικής φύσεως αποθήκευση, η οποία είναι αναγκαία για τη διαβίβαση της επικοινωνίας.

5. Απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων. Κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες, σύμφωνα με το άρθρο 11 του ν. 2472/1997, όπως ισχύει, και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στον συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών, παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης.

Αρθρο 5

Κανόνες επεξεργασίας

1. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων και των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των

σκοπών της.

2. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον εφόσον:

α) ο συνδρομητής ή ο χρήστης μετά από ενημέρωση για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών έχει συγκατατεθεί, ή

β) η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία ο συνδρομητής ή ο χρήστης είναι συμβαλλόμενο μέρος, ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, μετά από αίτηση του συνδρομητή.

3. Όπου ο παρών νόμος απαιτεί τη συγκατάθεση του συνδρομητή ή χρήστη, η σχετική δήλωση δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Στην τελευταία περίπτωση, ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωση του η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στον χρήστη ή συνδρομητή και μπορεί οποτεδήποτε να ανακληθεί.

4. Ο φορέας παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα και τα δεδομένα κίνησης και θέσης ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός εάν ο συνδρομητής ή ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεση του. Εξαιρούνται οι σκοποί που συνδέονται με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών ή την παροχή υπηρεσιών προστιθέμενης αξίας που έχει ζητήσει ο συνδρομητής ή χρήστης, όπως η διαφήμιση ή η εμπορική έρευνα αγοράς προϊόντων και υπηρεσιών.

5. Για τα δεδομένα κίνησης, ο φορέας παροχής των υπηρεσιών οφείλει να ενημερώσει τον συνδρομητή ή τον χρήστη πριν από τη χορήγηση της συγκατάθεσης του σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασίας αυτής.

Όταν τα δεδομένα διαβιβάζονται σε τρίτους, η συγκατάθεση απαιτείται να είναι έγγραφη. Δεν θεωρούνται ως τρίτοι οι φορείς παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, όσον αφορά στη διαβίβαση σε αυτούς από αντίστοιχο φορέα δεδομένων κίνησης, με αποκλειστικό σκοπό τη χρέωση των παρεχομένων υπηρεσιών, υπό τον όρο ότι ο συνδρομητής ή ο χρήστης έχει ενημερωθεί κατά την κατάρτιση της σύμβασης εγγράφως. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Αν ανακληθεί και εφόσον τα δεδομένα έχουν εν τω μεταξύ ανακοινωθεί σε τρίτους, η ανάκληση ανακοινώνεται σε αυτούς με φροντίδα του υπεύθυνου επεξεργασίας. Ο φορέας παροχής δημοσίου δικτύου ή/ και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών απαγορεύεται να εξαρτά την παροχή των υπηρεσιών αυτών προς τον συνδρομητή ή τον χρήστη από τη συγκατάθεση του στην επεξεργασία των δεδομένων αυτών για σκοπούς άλλους από εκείνους που εξυπηρετούν άμεσα την παροχή των υπηρεσιών στις οποίες αφορούν τα άρθρα 1 έως 17.

6. Ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα.

7. Ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει, στο βαθμό που αυτό είναι τεχνικώς εφικτό, να καθιστά δυνατή τη χρήση και πληρωμή των υπηρεσιών αυτών ανωνύμως ή με ψευδώνυμο. Σε περίπτωση αμφισβήτησης της τεχνικής δυνατότητας της ανώνυμης και ψευδώνυμης χρήσης και πληρωμής των υπηρεσιών αυτών, γνωμοδοτεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).

3. ΚΟΙΝΟΤΙΚΗ ΟΔΗΓΙΑ 95/46/ΕΕ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών έχει διπλό στόχο: την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής του ατόμου και την εξασφάλιση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, για την επίτευξη οικονομικής και κοινωνικής προόδου και συνεργασίας, καθώς και τεχνικής και επιστημονικής συνεργασίας στην ολοένα αναπτυσσόμενη κοινωνία της πληροφορικής και των τηλεπικοινωνιών.Η Οδηγία 95/46/ΕΚ αποτελεί το κείμενο αναφοράς, σε ευρωπαϊκό επίπεδο, στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα. Θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση. Η εν λόγω Οδηγία ορίζει ως «δεδομένα προσωπικού χαρακτήρα» κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί το πρόσωπο στο οποίο αναφέρονται τα δεδομένα.Οι διατάξεις της παρούσας οδηγίας εφαρμόζονται στην αυτοματοποιημένη, εν όλο ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. πληροφοριακή βάση δεδομένων πελατών).

Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει δυνάμει της παρούσας οδηγίας σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον η επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Συνεπώς η Ελλάδα είναι υπεύθυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται οι οργανισμοί ηλεκτρονικού εμπορίου που είναι εγκατεστημένοι στα γεωγραφικά όρια της Ελλάδας. Στη συνέχεια ακολουθούν κάποιες γενικές προϋποθέσεις, που ορίζει η Οδηγία 95/46/ΕΚ, σχετικά με τη θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα:

Αρχές που Πρέπει να Τηρούνται ως Προς την Ποιότητα των Δεδομένων

Τα κράτη μέλη καθορίζουν τις προϋποθέσεις υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη. Προβλέπεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται σύννομη και θεμιτή επεξεργασία και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Θα πρέπει εξάλλου τα δεδομένα αυτά να είναι ακριβή και, αν χρειάζεται, να ενημερώνονται.

Βασικές Αρχές της Νόμιμης Επεξεργασίας Δεδομένων

Τα κράτη μέλη προβλέπουν ότι επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται μόνον εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή αν η επεξεργασία είναι απαραίτητη:

1. Για την εκτέλεση σύμβασης της οποίας το υπόψη πρόσωπο αποτελεί συμβαλλόμενο μέρος.
2. Για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας.
3. Για τη διαφύλαξη ζωτικού συμφέροντος του υπόψη προσώπου.
4. Για την εκτέλεση αποστολής δημόσιου συμφέροντος.
5. Για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.

- Ειδικές Κατηγορίες Επεξεργασίας

Τα κράτη μέλη απαγορεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Η διάταξη αυτή συνοδεύεται από επιφυλάξεις που αφορούν π.χ. την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του υπόψη προσώπου ή για σκοπούς προληπτικής ιατρικής και ιατρικής διάγνωσης.

- Ενημέρωση του Ενδιαφερόμενου Προσώπου

Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας ή ο εκπρόσωπός του πρέπει να παρέχει στο πρόσωπο από το οποίο συλλέγονται δεδομένα που το αφορούν πληροφορίες για την ταυτότητα του υπευθύνου της επεξεργασίας, για τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα καθώς και άλλες πληροφορίες, όπως για παράδειγμα τους αποδέκτες των δεδομένων κλπ.

- Εξαιρέσεις και Περιορισμοί

Τα κράτη μέλη μπορούν να περιορίζουν με νομοθετικά μέτρα την εμβέλεια των υποχρεώσεων και δικαιωμάτων που προβλέπονται στην παρούσα οδηγία όταν ο περιορισμός αυτός απαιτείται για τη διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημόσιας ασφάλειας και της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης παραβάσεων του ποινικού νόμου ή της δεοντολογίας των νομοθετικά κατοχυρωμένων επαγγελμάτων.

- Απόρρητο και Ασφάλεια της Επεξεργασίας

Κάθε πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου της επεξεργασίας δεν δύναται να επεξεργαστεί τα προσωπικά δεδομένα παρά κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο υπεύθυνος της επεξεργασίας θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα έναντι τυχαίας ή παράνομης καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια.

Τα κράτη μέλη προβλέπουν ότι κάθε πρόσωπο θα πρέπει να έχει τη δυνατότητα νομικής προσφυγής στην περίπτωση παραβίασης των δικαιωμάτων που εγγυώνται οι εθνικές διατάξεις οι οποίες ισχύουν για τη σχετική επεξεργασία δεδομένων. Εξάλλου, τα άτομα που έχουν υποστεί βλάβη λόγω μιας παράνομης επεξεργασίας των προσωπικών τους δεδομένων έχουν το δικαίωμα να επιτύχουν αποκατάσταση της ζημίας που υπέστησαν.

Επιτρέπονται οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι η εν λόγω τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Αντίθετα, οι εν λόγω μεταβιβάσεις δεν μπορούν να πραγματοποιηθούν προς τρίτες χώρες οι οποίες δεν διαθέτουν το κατάλληλο επίπεδο προστασίας, εκτός από συγκεκριμένες περιπτώσεις παρέκκλισης οι οποίες απαριθμούνται περιοριστικά.

Κάθε κράτος μέλος προβλέπει τη δημιουργίας μίας ή περισσότερων ανεξάρτητων κρατικών αρχών οι οποίες επιφορτίζονται με την εποπτεία της εφαρμογής, στο εθνικό έδαφος, των εθνικών διατάξεων που έχουν θεσπιστεί από τα κράτη μέλη, κατ' εφαρμογή της παρούσας οδηγίας.

4. ΚΟΙΝΟΤΙΚΗ ΟΔΗΓΙΑ 2002/58/Ε.Ε ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η Οδηγία 2002/58/ΕΚ αναθεωρεί και αναπροσαρμόζει την προηγούμενη Οδηγία 97/96/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, προκειμένου να ληφθούν υπόψη οι νέες υπηρεσίες και τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ αποτελεί βασικό στοιχείο του κανονιστικού πλαισίου που επιδιώκει να εξασφαλίσει τη συνέχιση της ανάπτυξης του τομέα ηλεκτρονικών επικοινωνιών, με οφέλη για το σύνολο των εταιρειών και των ιδιωτών που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικών επικοινωνιών..

Η εν λόγω Οδηγία επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία 2002/58/ΕΚ εναρμονίζονται οι διατάξεις των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση.

ΚΟΙΝΟΤΙΚΗ ΟΔΗΓΙΑ 2002/58/Ε.Ε..

(Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών)

Η Οδηγία 2002/58/ΕΚ αναθεωρεί και αναπροσαρμόζει την προηγούμενη Οδηγία 97/96/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, προκειμένου να ληφθούν υπόψη οι νέες υπηρεσίες και τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ αποτελεί βασικό στοιχείο του κανονιστικού πλαισίου που επιδιώκει να εξασφαλίσει τη συνέχιση της ανάπτυξης του τομέα ηλεκτρονικών επικοινωνιών, με οφέλη για το σύνολο των εταιρειών και των ιδιωτών που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικών επικοινωνιών..

Η εν λόγω Οδηγία επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία 2002/58/ΕΚ εναρμονίζονται οι διατάξεις των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση.

Η Οδηγία λοιπόν για την προστασία προσωπικών δεδομένων στηρίζεται στις εξής βασικές

Η επεξεργασία προσωπικών δεδομένων πρέπει να είναι πάντοτε θεμιτή και νόμιμη.

- Τα προσωπικά δεδομένα πρέπει πάντα να συλλέγοντας για ρητώς καθορισμένους και νόμιμους σκοπούς και να χρησιμοποιούνται ανάλογα.
- Τα προσωπικά δεδομένα πρέπει να είναι κατάλληλα και να μην υπερβαίνουν τα απολύτως αναγκαία

για τους σκοπούς της επεξεργασίας τους

- Τα δεδομένα που αποκαλύπτουν την ταυτότητα των προσώπων δεν πρέπει να φυλάσσονται για περισσότερο χρόνο απ' όσο είναι απαραίτητο
- Τα δεδομένα πρέπει να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται
- Οι κάτοχοι δεδομένων οφείλουν να παρέχουν στα πρόσωπα που αφορούν τα δεδομένα αυτά εύλογα μέσα για τη διόρθωση, τη διαγραφή ή τη δέσμευση ανακριβών δεδομένων
- Πρέπει να λαμβάνονται τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα για την αποτροπή της παράνομης ή χωρίς άδεια επεξεργασίας προσωπικών δεδομένων
- Τα προσωπικά δεδομένα δεν πρέπει να μεταφέρονται σε χώρες ή επικράτειες εκτός του Ευρωπαϊκού Οικονομικού Χώρου, εκτός εάν αυτές εγγυώνται "επαρκές επίπεδο προστασίας" για τα πρόσωπα που αφορούν τα δεδομένα

Η οδηγία επιβάλλει επίσης στα κράτη μέλη την υποχρέωση να συστήσουν μία η περισσότερες ανεξάρτητες εποπτικές Αρχές για να παρακολουθούν την εφαρμογή της. Ένα από τα καθήκοντα αυτών των Αρχών είναι να τηρούν ενημερωμένο δημόσιο μητρώο, ώστε το κοινό να μπορεί να γνωρίζει τα ονόματα όλων των κατόχων προσωπικών δεδομένων και το είδος της επεξεργασίας στην οποία τα υποβάλλουν. Επίσης ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οφείλει να λαμβάνει από κοινού με τους φορείς παροχής δημόσιων δικτύων επικοινωνιών, καθόσον αφορά την ασφάλεια του δικτύου, τα ενδεδειγμένα τεχνικά και οργανωτικά μέσα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Οι εν λόγω φορείς υποχρεώνονται να ενημερώνουν τους συνδρομητές σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος για την ασφάλεια του δικτύου.

Απόρρητο των Επικοινωνιών

Το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, αποτελεί βασικό δικαίωμα του πολίτη και ως τέτοιο κατοχυρώνεται από την εκάστοτε ισχύουσα εθνική νομοθεσία.

Γενικά, στο πλαίσιο της διασφάλισης του απορρήτου απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερόμενων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια (π.χ. για περιπτώσεις της δημόσιας ασφάλειας).

Η πιο πάνω απαγόρευση δεν επηρεάζει οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ΑΡΙΣΤΕΑ ΣΙΝΑΝΙΩΤΗ-ΜΑΡΟΥΔΗ ΙΩΑΝΝΗΣ Δ. ΦΑΡΣΑΡΩΤΑΣ ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ

   ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑ

2. ΙΙΓΓΛΕΖΑΚΗΣ Ι. ΕΙΣΑΓΩΓΗ ΣΤΟ ΔΙΚΑΙΟ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑ

3. ΚΑΡΑΚΩΣΤΑΣ Ι. ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΑ ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑΣ

4. ΑΔΑΕ (2006) ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗ ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΣΤΙΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΤΙΣ ΣΥΝΑΦΕΙΣ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ.

5. ΑΔΑΕ (2006) ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗ ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΔΙΑΔΙΚΤΥΑΚΩΝ ΥΠΟΔΟΜΩΝ.

6. ΒΑΡΕΛΑΣ Χ. ΑΦΙΕΡΩΜΑ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΠΕΡΙΟΔΙΚΟ RAM.

7. ΚΑΤΣΙΚΑΣ << Ο ΡΟΛΟΣ ΤΟΥ ΔΗΜΟΣΙΟΥ ΚΑΙ ΤΟΥ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ>> ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ.

8. ΣΤΕΡΓΙΟΣ ΔΕΛΛΑΣ, ΜΕΤΑΔΟΣΗ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΚΤΥΑ Η/Υ

9. ΑΝΑΣΤΑΣΙΟΣ ΠΑΠΑΔΟΠΟΥΛΟΣ ΣΧΟΛΙΚΟ ΒΙΒΛΙΟ ΓΙΑ ΤΕΕ/ΕΠΑΛ ΣΤΟ ΜΑΘΗΜΑ ΔΙΚΤΥΑ Η/Υ ΙΙ

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ELGAMAL T., “CRYPTOGRAPHY AND LOGARITHMS OVER FINITE FIELDS”, PHD THESIS, STANFORD UNIVERSITY, 1984

2. LAI X., “ON THE DESIGN AND SECURITY OF BLOCK CIPHERS”, DISSERTATION ETH NO.9752, SWISS FEDERAL INSTITUTE OF TECHNOLOGY, SWITZERLAND, 1992

3. FIREWALL- HENING MARKEL ,3/2009

4. ALEXANDER, MICHAEL TO UNDERGROUND ΟΔΗΓΟΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ 1996

5. AKDENIZ, YAMAN (ΚΑΙ NICHOLAS BOHM & ΚΑΘΗΓΗΤΉΣ ΚΛΆΙΒ WALKER) ΣΤΟ INTERNET ΠΡΟΣΤΑΣΊΑ ΠΡΟΣΩΠΙΚΏΝ ΔΕΔΟΜΈΝΩΝ: CYBER-ΕΓΚΛΉΜΑΤΑ ΚΑΤΆ CYBER-ΔΙΚΑΙΏΜΑΤΑ (1999) ΥΠΟΛΟΓΙΣΤΈΣ ΚΑΙ VOL ΝΌΜΟΥ. 11034JISSUE 1 3410 ΤΕΎΧΟΣ 1 34

6. DIFFIE W., HELLMANN M., "NEW DIRECTIONS IN CRYPTOGRAPHY", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL.IT-22, NO.6, PP.644-654, 1976

7. GRINGRAS, CLIVE ΟΙ ΝΌΜΟΙ ΤΟΥ ΔΙΑΔΙΚΤΎΟΥ 1997

8. GUNKEL DAVID J ΚΥΒΕΡΝΟΧΩΡΟ HACKING 2001

9. HILL, SHELLEY ΟΔΗΓΗΣΗ ΔΟΥΡΕΙΟΣ ΊΠΠΟΣ ΚΑΙ ΑΓΟΡΩΝ ΜΕΣΩ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΚΑΤΑΧΡΗΣΗ ΠΡΑΞΗ (2003/JANUARY ΔΕΚΕΜΒΡΙΟΥ 2004) ΠΛΗΡΟΦΟΡΙΚΗ & VOL ΝΟΜΟΥ. 14 ΈΚΔΟΣΗ 530

10. HIRST, MICHAEL CYBEROBSCENITY ΚΑΙ ΤΟ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΑΓΓΛΙΚΗΣ ΠΟΙΝΙΚΟΥ ΔΙΚΑΙΟΥ (2002) ΠΛΗΡΟΦΟΡΙΚΗ & VOL ΝΟΜΟΥ. 13 ΈΚΔΟΣΗ

11. AALBERTS BP & VAN DER HOF S ΨΗΦΙΑΚΗ BLINDNESS ΑΝΑΛΥΣΗ ΥΠΟΓΡΑΦΗ ΝΟΜΟΘΕΤΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ AUTHENTICATION 2000

ΔΙΑΔΙΚΤΥΟ

1. http://www.go online.gr/files/legislation/Hlektroniko_Emporio/Update/295.64.2003.pdf
2. http://www.go-online.gr/ebusiness/specials/article.html?article_id=1075
3. http://www.google.com
4. http://www.dpa.gr
5. http://pnt.wikipedia.org/
6. http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL