ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ

Πτυχιακή Εργασία

ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Ονοματεπώνυμο Φοιτητή: Κούτσικος Χρήστος

Επιβλέπων Καθηγητής: Ρίζος Γεώργιος

Τίτλος πτυχιακής εργασίας: ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ

ΚΟΥΤΣΙΚΟΣ ΧΡΗΣΤΟΣ

ΕΞΑΜΗΝΟ: 14

ΑΜ:9921

E-mail: xkoutsikos89@gmail.com

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου, κ. Ρίζο Γεώργιο για την εποικοδομητική συνεργασία και καθοδήγηση κατά τη διάρκεια εκπόνησης της πτυχιακής μου εργασίας.

Περιεχόμενα

Λίστα Εικόνων

Δήλωση Πνευματικής Ιδιοκτησίας

Η παρούσα εργασία αποτελεί προϊόν αποκλειστικά δικής μου προσπάθειας. Όλες οι πηγές που χρησιμοποιήθηκαν περιλαμβάνονται στη βιβλιογραφία και γίνεται ρητή αναφορά σε αυτές μέσα στο κείμενο όπου έχουν χρησιμοποιηθεί.

ΥΠΟΓΡΑΦΕΣ

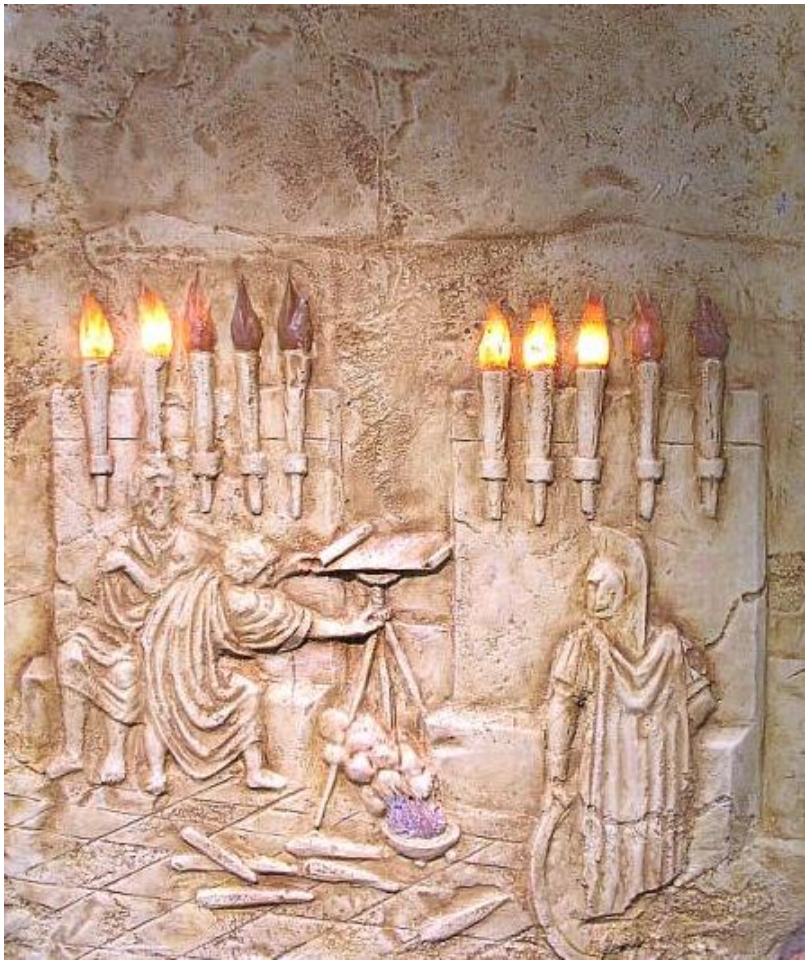
ΠΕΡΙΛΗΨΗ

Στην παρούσα πτυχιακή εργασία γίνεται μία παρουσίαση των μεθόδων που χρησιμοποιούνται για την ασφάλεια των δεδομένων στα ασύρματα δίκτυα και συνεπώς και στις κινητές επικοινωνίες. Αρχικά στο πρώτο κεφάλαιο γίνεται παρουσίαση των χαρακτηριστικών των ασύρματων δικτύων καθώς και κάποια πλεονεκτήματα αλλά και μειονεκτήματα που παρουσιάζουν. Το δεύτερο κεφάλαιο παρουσιάζει κάποιες τεχνικές που αναπτύχθηκαν για την ασφάλεια των δεδομένων στα δίκτυα των υπολογιστών, αφού πάνω σε αυτές τις μεθόδους βασίστηκαν και οι ασύρματες επικοινωνίες. Στο τρίτο και τέταρτο κεφάλαιο αναφερόμαστε στις πιο σημαντικές τεχνικές που χρησιμοποιούνται για να μην είναι δυνατή η παραβίαση των ασύρματων και κινητών δικτύων επικοινωνιών. Τέλος στο τέταρτο κεφάλαιο παρουσιάζουμε κάποια νομικά θέματα που προκύπτουν στα θέματα ασφαλείας, ενώ στο έκτο κεφάλαιο καταλήξουμε στα συμπεράσματα που προκύπτουν έπειτα από την βιβλιογραφική έρευνα που έγινε κατά την εκπόνηση της εργασίας.

ΚΕΦΑΛΑΙΟ 1^{ο} ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

1.1 Εισαγωγή

Οι ασύρματες επικοινωνίες πρωτοεμφανίζονται το 1896 με την εφεύρεση του ασύρματου τηλέγραφου από τον Μαρκόνι. Το 1906 πραγματοποιείται η πρώτη ραδιοφωνική μετάδοση από τον Fessenden. Ο δεύτερος παγκόσμιος πόλεμος επιτάχυνε τις εξελίξεις. Το 1957 εκτοξεύεται από την σοσιαλιστική Σοβιετική Ένωση ο δορυφόρος Sputnik, γεγονός-σταθμός στις ασύρματες επικοινωνίες. Το 1970 εμφανίζονται στις ΗΠΑ τα πρώτα ασύρματα αναλογικά τηλέφωνα. Στις αρχές της δεκαετίας του '80 εμφανίζονται στην Ιαπωνία και την Ευρώπη συστήματα κινητής τηλεφωνίας. Τη δεκαετία του '90 σημειώνεται ραγδαία ανάπτυξη των ασύρματων τεχνολογιών και διαδίδονται τα συστήματα τηλεειδοποίησης. Το 1991 εμφανίζονται τα πρώτα GSM δίκτυα. Το 1992 εμφανίζεται το TCP/IP based δίκτυο – Cellurar Digital Packet Data (CDPD). Το 1995 καταγράφονται οι πρώτες προσπάθειες συνδυασμού της ασύρματης τεχνολογίας με το Διαδίκτυο. Το 1997 εμφανίζονται οι πρώτες προδιαγραφές WAP 1.0. Το 2001 εμφανίστηκαν στην αγορά οι πρώτες συσκευές Bluetooth της ομάδας SIG (Special Interest Group). Οι υπηρεσίες βασισμένες στο WAP δεν γνώρισαν την αναμενόμενη αποδοχή από τους καταναλωτές. Ομοίως και οι τεχνολογίες Bluetooth και WLAN. (Γκρίτζαλης Σ., Λαμπρινουδάκης Κ., Μήτρου Λ., Κάτσικας Σ., 2010)



Εικόνα 1 Πρώτα ασύρματα συστήματα

Οι φρυκτωρίες ήταν ένα σύστημα συνεννόησης στην αρχαία Ελλάδα με σημάδια που μεταβιβάζονταν από περιοχή σε περιοχή με τη χρήση πυρσών στη διάρκεια της νύκτας (φρυκτός=πυρσός και ώρα = φροντίδα). Ο Αισχύλος στο έργο του *Αγαμέμνων* περιγράφει την

είδηση της πτώσης της Τροίας, η οποία μεταδόθηκε ως τις Μυκήνες με τις φρυκτωρίες.[1] Ενδιάμεσοι σταθμοί μεταδόσεως υπήρχαν στην Ίδη της Μυσίας, στο Ακρωτήρι της Λήμνου (σημερινή Πλάκα), στον Άθω, στο βουνό Μάκιστο και στις πλαγιές του Αραχναίου. Το σύστημα χρησιμοποιήθηκε για πολλούς αιώνες μέχρι το 1850 αλλά μπορούσε να μεταφέρει μηνύματα μόνο με ένα κοινό κώδικα. (http://el.wikipedia.org)

Το γεωγραφικό στήσιμο, η κατοχή, η διαχείριση και συντήρηση αυτών των επικοινωνιακών δικτύων από τον αρχαίο ελληνικό πολιτισμό ήταν πρωταρχικής σημασίας για την επικράτηση και την επέκτασή του. Το δίκτυο αυτό χρησιμοποιείτο τόσο κατά την διάρκεια των πολεμικών επιχειρήσεων, όσο και κατά την διάρκεια της ειρήνης, όταν τα νέα και οι διαταγές των αρχόντων έπρεπε να φτάσουν το συντομότερο δυνατό στον προορισμό τους. Κάτι τέτοιο αφορούσε κυρίως τις αυτοκρατορίες, των οποίων οι αχανείς εκτάσεις έκαναν πολύ δύσκολη τη σχετικά γρήγορη ενημέρωση. Χαρακτηριστικά παραδείγματα συνεννόησης με οπτικό σήμα φωτιάς συναντάμε στις περιπτώσεις όπου π.χ. η Μήδεια ύψωσε αναμμένο πυρσό για να ειδοποιήσει τους Αργοναύτες να πάνε στην Κολχίδα [2] ή όταν ειδοποιείται με πυρσό ο Αγαμέμνονας για την είσοδο του Δούρειου Ίππου στην Τροία από τον Σίνωνα και με πυρσό που σήκωσε ο ίδιος προς τον ελληνικό στόλο στην Τένεδο δίνοντάς του το σήμα της επιστροφής και κατάληψης της ανοχύρωτης πολιτείας. (http://el.wikipedia.org)

Πολλά από τα φωτεινά σήματα ανταλλάσσονταν τη νύχτα στη θάλασσα μεταξύ πλοίων, μεταξύ πλοίων και ξηράς και γενικά πρέπει να σημειωθεί ότι τα περισσότερα από αυτά αντιστοιχούσαν σε προσυμφωνημένα μηνύματα. Τα φωτεινά αυτά σήματα οι Έλληνες τα ονόμαζαν «πυρσούς» ή «φρύκτους» και από εδώ γνωρίζουμε και τους «φίλιους φρύκτους» ή τους «πολέμιους φρύκτους». Συγκεκριμένα όπως σημειώνει ο Θουκυδίδης, όταν στο στρατόπεδο έρχονταν φίλοι, οι στρατιώτες ύψωναν απλώς τους αναμμένους πυρσούς (φίλιοι φρύκτοι), ενώ όταν πλησίαζαν εχθροί, οι πυρσοί ανέμιζαν δεξιά-αριστερά (πολέμιοι φρύκτοι). Οι πυρσοί αυτοί στη διάρκεια της ημέρας απλώς έβγαζαν πολύ καπνό, που σήμαινε ότι χρησιμοποιούσαν εύφλεκτα υλικά, στα οποία πολλοί ιστορικοί αποδίδουν τις λέξεις/φράσεις φρύκτους ανίσχειν, πυρσεύειν, φρυκτωρία (γνωστοποιώ είδηση από μεγάλη απόσταση) και φρυκτωρίες. (http://el.wikipedia.org)

Οι φρυκτωρίες εκμεταλλευόμενες τα νησιά του Αιγαίου και την ορεινή μορφολογία του Ελλαδικού χώρου, χρησιμοποιούν την φωτιά και έναν κώδικα αναπαράστασης γραμμάτων (παρόμοιο του κώδικα Μορς) για την μετάδοση αξιόπιστων μηνυμάτων σε πολλά χιλιόμετρα (έως και 130). Στην ουσία μιλάμε για την προϊστορία του τηλέγραφου. Αν ήταν νύχτα, οι υπεύθυνοι στρατιώτες στην φρυκτωρία (φρυκτωρία) άναβαν λαμπρές φωτιές για την μετάδοση σημάτων, ενώ κατά την διάρκεια της ημέρας χρησιμοποιούσαν πυκνό καπνό. (http://el.wikipedia.org)

Σημαντικός σταθμός οπτικών τηλεπικοινωνιών ήταν το «καιροσκοπείο» στην κορυφή του Άθω (κατά τον Αναξίμανδρο) με ιστορία που ξεκινάει από τη Γιγαντομαχία της μυθολογίας. Φρυκτωρία με ξεχωριστή ιστορία είναι και η βουνοκορφή του Μεσσάπιου της Εύβοιας αλλά και του πύργου του Δρακάτου (4ος π.χ. αιώνας) στη Ανατολική Ικαρία, της Ανάφης, της Γιούτας (Κνωσός), του ναού του Ποσειδώνα στο Σούνιο, το Άκτιο, το ακρωτήριο του Σίδερο, κ.ά. Πολλά απ' αυτά τα σημεία είναι και σήμερα φάροι. (http://el.wikipedia.org)

Η μελέτη των Φρυκτωριών εμφανίζει αρκετό ενδιαφέρον αλλά και δυσκολία, τόσο γιατί πολλοί από αυτούς τους αρχαίους πύργους έχουν καταστραφεί εντελώς, όσο και γιατί για όσους διασώζονται δεν μας είναι εύκολο να τεκμηριώσουμε την χρήση τους. Τα πράγματα μπερδεύονται ακόμη περισσότερο όταν αναφέρονται και σοβαρές απόψεις για πυραμίδες ή μικρά φρούρια. Έτσι δεν είναι λίγοι οι ερευνητές (Bits, Poisson, And) που θεωρούν πως τα ερείπια στο χωριό Ελληνικό, έξω από το Κεφαλάρι του Άργους, δεν είναι πυραμίδα αλλά μία φρυκτωρία. Όσον αφορά τα πολλά μικρά αρχαία κτίσματα στην περιοχή της Αργολίδας, οι ερευνητές τα θεωρούν περισσότερο ως μικρά οχυρά στρατηγικών θέσεων, τα μικρά πολυάνδρια όπως τα αποκαλεί και ο Παυσανίας, και όχι ως φρυκτωρίες. (http://el.wikipedia.org)

Τα τελευταία χρόνια παρατηρείται μεγάλη αύξηση στις πωλήσεις των φορητών ηλεκτρονικών υπολογιστών. Άλλωστε και στην καθημερινότητά μας έχει κυριαρχήσει η τάση για φορητότητα, κινητικότητα και συνεχή σμίκρυνση των συσκευών με σκοπό να μεταφέρονται πιο εύκολα και να είναι παντού μαζί μας. Αυτό συνεπάγεται ότι όλες οι παραδοσιακές ενσύρματες τεχνολογίες δικτύωσης είναι ανεπαρκείς σ' αυτόν το νέο τρόπο ζωής. Τη λύση, όμως στο πρόβλημα της

δικτύωσης δίνουν οι τεχνολογίες ασύρματης δικτύωσης οι οποίες καταργούν τα καλώδια και δίνουν σε μεγάλο βαθμό ελευθερία στους χρήστες. (http://el.wikipedia.org)

Ένα ενσύρματο και ένα ασύρματο δίκτυο ξεχωρίζουν από το φυσικό μέσο μετάδοσης της πληροφορίας, όπου τα ασύρματα πλέον δίκτυα χρησιμοποιούν τον αέρα μεταδίδοντας τις πληροφορίες μέσω ηλεκτρομαγνητικών σημάτων ή με χρήση υπερύθρων. Οι ραδιοσυχνότητες όμως είναι ευρέως διαδεδομένες διότι μπορούν να καλύψουν μεγάλες αποστάσεις, χρησιμοποιώντας μεγαλύτερο εύρος ζώνης. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα συνήθως 2,4GHz και 5 GHz. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου. (http://el.wikipedia.org)

Όπως τα κλασικά δίκτυα υπολογιστών έτσι και τα ασύρματα δίκτυα υπολογιστών, για να εξασφαλίσουν την ασφαλή μετάδοση των δεδομένων τους, χρησιμοποιούν αξιόπιστα πρωτόκολλα μεταφοράς δεδομένων, όπου επίσης διασφαλίζουν την ασφάλεια από οποιαδήποτε ενέργεια παραβίασης, δίνουν την δυνατότητα ταχείας πρόσβασης και μεταφοράς δεδομένων και τέλος επιτρέπουν την διασύνδεσή των ασύρματων δικτύων με αυτά που κάνουν χρήση ενσύρματων τεχνολογιών. (http://el.wikipedia.org)

Ο τομέας των ασύρματων δικτύων αποτέλεσε επαναστατική ιδέα όταν κυκλοφόρησαν και αποτελεί έναν από τους ταχύτερα αναπτυσσόμενους κλάδους της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών. Σίγουρα όλοι έχουν αποδεχθεί αυτή τη νέα τεχνολογία, τόσο βιομηχανίες όσο και το ευρύ αγοραστικό κοινό, το ερώτημα όμως που τίθεται είναι κατά πόσο ασφαλές είναι. (http://el.wikipedia.org)

1.2 Ασύρματη ποιότητα

Ο οργανισμός της IEEE αναπτύσσεται ταχύτατα δημιουργώντας διαρκώς νέα πρότυπα οδηγώντας με αυτό τον τρόπο στην γιγάντωση της βιομηχανίας κατασκευαστών αντίστοιχων συσκευών, όπου πλέον κρίνεται αναγκαία η διασφάλιση της συμβατότητας μεταξύ των διάφορων συσκευών για την προστασία του αγοραστή.

Έτσι το 1999 ιδρύθηκε η WECA (Wireless Ethernet Compatibility Alliance), ένας μη κερδοσκοπικός οργανισμός που σκοπό έχει την πιστοποίηση ασύρματων 802.11 συσκευών. Σε αυτό τον οργανισμό συμμετέχουν οι βιομηχανίες που κατασκευάζουν ολοκληρωμένα κυκλώματα, άλλες που παρέχουν υπηρεσίες WLAN, κατασκευαστές υπολογιστών, κατασκευαστές λογισμικού κ.α.. Ονομαστικά κάποιες από αυτές τις εταιρείες είναι, 3Com, Aironet, Apple, Breezecom, Compaq, Dell, Fujitsu, IBM, Lucent Technologies, Nokia, Samsung, Symbol Technologies, Zoom. (Stallings W.)

Αυτή η ένωση εφηύρε μία σειρά από δοκιμές ώστε να είναι δυνατή η πιστοποίηση της συμβατότητας των IEEE προϊόντων. Οι συσκευές οι οποίες κατάφερναν να περάσουν με επιτυχία από αυτές τις δοκιμές, αποκτούσαν το λογότυπο Wi-Fi (Wireless Fidelity). Επομένως αυτό το λογότυπο αποτελεί μία πιστοποίηση για τον υποψήφιο αγοραστή της συσκευής και μία εγγύηση για την επένδυση του. Ο καταναλωτής αγοράζοντας μία συσκευή με το λογότυπο αυτό, έχει την εγγύηση ότι η συσκευή θα συνεργαστεί με οποιαδήποτε άλλη συσκευή φέρει επίσης το λογότυπο. (Stallings W.)

Τι ορίζεται όμως ως ασύρματο τοπικό δίκτυο (WLAN); Ένα σύστημα επικοινωνίας μέσω ηλεκτρομαγνητικών κυμάτων ανάμεσα σε σταθερούς ή κινητούς χρήστες όπου επιτρέπεται η μεταξύ τους διασύνδεση και ανταλλαγή δεδομένων. Η πρώτη γενιά συσκευών WLAN, δεν ήταν ιδιαίτερα διαδεδομένη ίσως λόγω της χαμηλής ταχύτητας διάδοσης ή λόγω της έλλειψης προτύπων. Πλέον τα σύγχρονα ασύρματα συστήματα είναι δυνατόν να μεταφέρουν δεδομένα σε υψηλές ταχύτητες. Επίσης, νέες συσκευές και προϊόντα ασύρματης πρόσβασης βασιζόμενα σε τεχνολογίες spread-spectrum, που θα μελετήσουμε αργότερα σε επόμενο κεφάλαιο, ραδιοφωνικά κύματα, υπέρυθρες ακτίνες, κυψελοειδείς και δορυφορικές επικοινωνίες, είναι πια πραγματικότητα. (Stallings W.)

Πλέον στην αγορά υπάρχει ένας τεράστιος αριθμός από νέες συσκευές και προϊόντα ασύρματης επικοινωνίας τα οποία βασίζονται σε νέες τεχνολογίες και πρότυπα. Τα τελευταία χρόνια οι φορητοί υπολογιστές, οι οποίοι ενσωματώνουν τεχνολογία ασύρματης πρόσβασης, είναι

διαθέσιμοι για το ευρύ κοινό, αφού έχουν πλέον χαμηλό κόστος, ικανοποιητική υπολογιστική ισχύ και ποιότητα υπηρεσιών παρόμοια με τους σταθερούς υπολογιστές. (Stallings W.)

1.3 Πλεονεκτήματα ασύρματων τοπικών δικτύων

Ωστόσο υπάρχουν κάποια περιβάλλοντα στα οποία τα ασύρματα τοπικά δίκτυα αποτελούν καλύτερη λύση από ένα δίκτυο με καλώδιο. Σε αυτή την κατηγορία ανήκουν τα περιβάλλοντα μεγάλων εκτάσεων, όπως είναι οι χώροι παραγωγής ενός εργοστασίου ή μιας αποθήκης, κάποια πολύ παλιά κτίρια, στα οποία είτε απαγορεύεται η οποιαδήποτε τροποποίηση των κτιριακών εγκαταστάσεων, είτε η καλωδίωση είναι ανεπαρκής ή ανύπαρκτη, ή μικρά γραφεία, όπου η εγκατάσταση και η συντήρηση ενός ενσύρματου δικτύου είναι δεν είναι καθόλου οικονομική λύση.

Σε αυτή την ενότητα θα παρουσιάσουμε μερικά από τα κυριότερα πλεονεκτήματα των ασύρματων τοπικών δικτύων ή WLAN: (Tanenbaum, 2000)

- Ευκολία: Η ασύρματη φύση των συγκεκριμένων δικτύων δίνει τη δυνατότητα στους χρήστες να μπορούν να έχουν πρόσβαση στους πόρους ενός δικτύου, σχεδόν από οποιαδήποτε τοποθεσία χωρίς να χρειάζεται να βρίσκονται στο σπίτι ή στο γραφείο τους και αυτό αυξάνεται συνεχώς καθώς αυξάνεται η χρήση των φορητών υπολογιστών.
- Φορητότητα: Το μεγαλύτερο ίσως πλεονέκτημα των WLAN είναι το γεγονός ότι οι χρήστες μπορούν να έχουν πρόσβαση σε δεδομένα ακόμα και όταν βρίσκονται σε κίνηση. Αυτό το πλεονέκτημα ενισχύει την παραγωγικότητα και τις ευκαιρίες για εξυπηρέτηση οι οποίες δεν μπορούν να υποστηριχθούν από τα ενσύρματα δίκτυα. Οι εφαρμογές που στηρίζονται στην κινητικότητα, ενώ οι συσκευές χρησιμοποιούνται σε ένα WLAN, συμπεριλαμβάνουν και αυτές που στηρίζονται στην πρόσβαση δεδομένων σε πραγματικό χρόνο τα οποία είναι συνήθως αποθηκευμένα σε βάσεις δεδομένων.
- Ταχύτητα και ευελιξία εγκατάστασης: Με την εγκατάσταση ενός WLAN μειώνεται η ανάγκη της χρήσης των καλωδίων η οποία συνήθως χρειάζεται αρκετή δουλειά, ενώ η ασύρματη τεχνολογία επιτρέπει τη διασύνδεση δικτύων η οποία υπό άλλες συνθήκες θα ήταν αδύνατη. Μακροπρόθεσμα, η εγκατάσταση, η αναβάθμιση και το κόστος συντήρησης των συστημάτων WLAN, τα καθιστούν μία πιο οικονομική λύση.
- Μειωμένο κόστος χρήσης: Η αρχική επένδυση για ένα εξοπλισμό WLAN είναι υψηλότερη συγκριτικά με μία ενσύρματη σύνδεση, όμως το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο, καθώς μακροπρόθεσμα τα κέρδη είναι μεγαλύτερα σε περιβάλλοντα όπου απαιτούνται πολλές μετακινήσεις.
- Συμβατότητα: Τα ασύρματα δίκτυα διαφοροποιούνται ώστε να είναι δυνατή η κάλυψη των αναγκών συγκεκριμένων εγκαταστάσεων και εφαρμογών. Οι διαμορφώσεις αλλάζουν εύκολα από μικρά δίκτυα κατάλληλα για έναν μικρό αριθμό χρηστών σε πλήρως ανεπτυγμένα δίκτυα που καλύπτουν εκατοντάδες χρήστες.
- Νομαδική πρόσβαση: Η νομαδική πρόσβαση βρίσκει εφαρμογή σε χώρους όπως επιχειρήσεις ή πανεπιστημιουπόλεις, όπου τα κτίρια βρίσκονται συγκεντρωμένα. Σε αυτές τις περιπτώσεις, οι χρήστες μετακινούνται μέσα στο χώρο και μπορούν με τους φορητούς υπολογιστές τους να προσπελαύνουν αρχεία των servers και άλλων κόμβων του δικτύου.
- Διασύνδεση: Μια άλλη περίπτωση της διεύρυνσης είναι και η διασύνδεση δυο ή παραπάνω αυτόνομων τοπικών δικτύων που βρίσκονται σε διαφορετικούς χώρους. Για παράδειγμα μας συμφέρει περισσότερο να εγκαταστήσουμε ασύρματη ζεύξη με σκοπό τη διασύνδεση δικτύων που βρίσκονται σε διαφορετικά κτίρια. Στην περίπτωση αυτή, χρησιμοποιείται μια ασύρματη σύνδεση από σημείο- σε- σημείο (wireless point-to-point link) μεταξύ των δύο κτιρίων.

1.4 Μειονεκτήματα ασύρματων τοπικών δικτύων

Παρόλα τα θετικά που υπάρχουν από τη χρήση των ηλεκτρομαγνητικών κυμάτων, ραδιοκυμάτων και υπέρυθρης ακτινοβολίας, για την μεταφορά πληροφορίας, υπάρχουν και κάποια αρνητικά στοιχεία, όπως για παράδειγμα το γεγονός ότι τα ασύρματα δίκτυα προσβάλλονται πιο εύκολα από φαινόμενα παρεμβολής, τα οποία συχνά αλλοιώνουν την επικοινωνία των χρηστών. Αυτά τα μειονεκτήματα παρουσιάζονται σε αυτή την ενότητα: (Tanenbaum, 2000)

- Παρεμβολή λόγω πολλαπλών διαδρομών: Αυτό το φαινόμενο οφείλεται στην πιθανότητα που υπάρχει τα σήματα που μεταδίδονται να συνδυαστούν με άλλα ανακλώμενα από επιφάνειες ή εμπόδια σήματα, τα οποία βρίσκονται στην ευθεία μετάδοσης του σήματος.
- Path loss: Ονομάζονται οι απώλειες που μπορεί να έχουμε σε μια ασύρματη επικοινωνία και εξαρτώνται άμεσα από την ύπαρξη ή μη οπτικής επαφής (LOS: Line Of Sight)
- Παρεμβολές ραδιοσημάτων: Οι παρεμβολές από ραδιοσήματα (Radio Signal Interference) διαχωρίζονται σε Εσωτερικές (inward) και Εξωτερικές (outward).
- Διαχείριση ενέργειας: Καλό είναι να επιλέγονται προϊόντα για σωστή διαχείριση ενέργειας, ώστε να μεγιστοποιείται η αυτονομία του δικτύου.
- Ασυμβατότητα συστημάτων: Για την εγκατάσταση ενός WLAN θα πρέπει να λάβουμε υπόψη και την ασυμβατότητα μεταξύ προϊόντων διαφορετικών κατασκευαστών.
- Προστασία της υγείας των χρηστών: Τα ασύρματα δίκτυα που χρησιμοποιούν την τεχνική μετάδοσης με υπέρυθρες ακτίνες, θα πρέπει να περιορίζουν την ισχύ του εκπεμπόμενου σήματος στο ανώτερο όριο των 2 Watts, για να αποφευχθούν προβλήματα υγείας.
- Το πρόβλημα του κρυμμένου κόμβου: Το φαινόμενο αυτό παρατηρείται όταν υπάρχει ένας σταθμός ο οποίος δεν μπορεί να ανιχνεύσει την δραστηριότητα ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται.
- Ασφάλεια δικτύου: Η συνολική λειτουργία ενός ασύρματου δικτύου εμπεριέχεται στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν ενυπάρχει με άλλες λειτουργίες όπως εγκατάσταση σύνδεσης ή άλλες υπηρεσίες (π.χ. login) που προσφέρουν τα ανώτερα στρώματα. Έτσι το μόνο θέμα που σχετίζεται με την ασφάλεια και τα ασύρματα δίκτυα είναι τα θέματα ασφαλείας των χαμηλότερων στρωμάτων, π.χ. κρυπτογράφηση (encryption) δεδομένων. Συνεπώς, έχουν δημιουργηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν δύσκολη την υποκλοπή της πληροφορίας που μεταδίδεται. Τέτοιες τεχνικές είναι η εξάπλωση φάσματος (spread spectrum), ενώ εάν απαιτείται μεγαλύτερη ασφάλεια, καθορίζεται η χρήση της κωδικοποίησης WEP (Wired Equivalent Privacy).

1.5 Δίκτυα υπολογιστών

Ένας από τους βασικότερους ορισμούς που χαρακτηρίζει σωστά τα δίκτυα υπολογιστών είναι: «*Ένα δίκτυο υπολογιστών είναι ένα σύνολο από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία(π.χ. εκκίνηση ή τερματισμό) κάποιου άλλου*.» (Tanenbaum, 2000)

Βέβαια τα δίκτυα υπολογιστών μπορούν να χωριστούν σε κατηγορίες σύμφωνα με την λειτουργικότητά τους: (Μαρκομανωλάκη Α., 2010)

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως Ενσύρματα ή Ασύρματα.
- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως Δημόσια ή Ιδιωτικά δίκτυα.
- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως Τοπικά (LAN & WLAN), Μητροπολιτικά (MAN & WMAN), Ευρείας κάλυψης (WAN & WWAN) και Προσωπικά (PAN & WPAN).

1.6 Ασύρματες Τεχνολογίες

Οι ασύρματες τεχνολογίες μπορούν να χωρισθούν σε διάφορες κατηγορίες, σύμφωνα με κριτήρια όπως ποιο είναι το πρωτόκολλο που χρησιμοποιούν, ποιο είναι το είδος σύνδεσης ή ποιο είναι το φάσμα συχνοτήτων λειτουργίας. Για να αναπτυχθεί ένα ασύρματο τοπικό δίκτυο πρέπει να επιλεγεί ένα από τα πολλά πρότυπα που έχουν δημιουργήσει διάφοροι οργανισμοί και εταιρείες τα τελευταία χρόνια. Τα πιο σημαντικά από αυτά είναι: (Πάλλης Μ., 2000)

- IEEE 802.11: Το 1997 η IEEE κατέληξε στο πρώτο της πρότυπο για WLANs, το οποίο καθορίζει τον έλεγχο πρόσβασης μέσω MAC και τα φυσικά στρώματα (PHY) για ένα LAN με ασύρματη σύνδεση. Το 802.11-legacy λειτουργεί στα 2.4 GHz και έχει ρυθμούς μετάδοσης δεδομένων 1 Mbps και 2 Mbps. Υπάρχουν υπηρεσίες οι οποίες καθορίζουν την ασύρματη μεταφορά δεδομένων ενός υποστρώματος MAC και τριών διαφορετικών φυσικών στρωμάτων. Το υπόστρωμα MAC έχει 2 τρόπους λειτουργίας: μία κατανεμημένη (distributed) λειτουργία (CSMA/CA1) και μία συντονισμένη (coordinated) λειτουργία (polling mode).
- HiperLAN: Το HiperLAN εδραιώθηκε το 1996 από την ETSI2 (European Telecommunications Standards Institute). Το πρότυπο λειτουργεί στην μπάντα από 5.1 έως 5.3 GHz και ο ρυθμός σηματοδοσίας φτάνει τα 24 Mbps και χρησιμοποιεί διαφορετική εκδοχή του CSMA/CA, που βασίζεται στο χρόνο ζωής του πακέτου, την προτεραιότητα και τις αναμεταδόσεις στο επίπεδο MAC.
- OpenAir: Η εταιρεία Proxim3 προώθησε το πρότυπο OpenAir, το οποίο είναι προγενέστερο του 802.11 και χρησιμοποιεί την τεχνική του Frequency Hopping με ρυθμούς δεδομένων 0.8 και 1.6 Mbps (χρησιμοποιώντας τεχνικές διαμόρφωσης 2FSK και 4FSK). Το πρωτόκολλο που χρησιμοποιείται είναι CSMA/CA και προαιρετικά βασίζεται στην ανταλλαγή RTS/CTS πακέτων.
- Ασύρματα Point-to-Point δίκτυα: Ο κυριότερος εκπρόσωπος των ασύρματων δικτύων με σύνδεση από σημείο-σε-σημείο (point-to-point) είναι τα ασύρματα μητροπολιτικά δίκτυα WMANs (Wireless Metropolitan Area Networks), τα οποία χρησιμοποιούν τεχνολογίες που ομοιάζουν πολύ με αυτές των WLAN. Τα δίκτυα αυτά στηρίζονται στην διασύνδεση ασύρματων, κινητών ή μη, χρηστών με μια σταθερή περιοχή στην οποία βρίσκεται ο παροχέας των υπηρεσιών (Service Provider), τις οποίες μοιράζονται οι ασύρματοι χρήστες. Δύο από τις πλέον αναπτυσσόμενες τεχνολογίες τέτοιου είδους ασύρματων δικτύων είναι και η MMDS (Multichannel Multipoint Distribution Service), η οποία λειτουργεί στην περιοχή συχνοτήτων 2.1-2.7 GHz, ενώ μπορεί να υποστηρίξει ρυθμό δεδομένων έως και 10 Mbps σε ακτίνα 35 μιλίων και η LMDS (Local Multipoint Distribution Service), η οποία λειτουργεί σε διάφορες συχνότητες (από 24 μέχρι 40 GHz), ενώ μπορεί να υποστηρίξει ρυθμούς μέχρι και 155 Mbps σε ακτίνα λειτουργίας των 2 μιλίων. Η τεχνολογία LMDS (Local Multipoint Distribution System) είναι ένα ασύρματο σύστημα επικοινωνίας ευρείας ζώνης point-to-multipoint και ανήκει σε μία κατηγορία ασύρματων τεχνολογιών που καλείται WLL (Wireless Local Loop) που λειτουργεί σε συχνότητες μεγαλύτερες των 20 GHz. Η τεχνολογία αυτή χρησιμοποιείται για την παροχή ψηφιακών αμφίδρομων υπηρεσιών όπως μετάδοση δεδομένων, φωνής, video και Internet. Το βασικό δομικό στοιχείο μιας τέτοιας αρχιτεκτονικής είναι το κελί (cell) στο οποίο λαμβάνει χώρα η ασύρματη επικοινωνία. Κάθε κελί στο σύστημα έχει έναν σταθμό βάσης (AP: Access Point) ή hub, ο οποίος αναφέρεται και ως central hub και βρίσκεται στο CMN (Central Main Node). Σε κάθε κελί υπάρχουν από λίγες έως πολλές απομακρυσμένες μονάδες (remote units) οι οποίες αντιπροσωπεύουν ουσιαστικά τους χρήστες. Η επικοινωνία και η διαχείριση των μονάδων αυτών γίνεται με τη βοήθεια του AP, η σύνδεση με τον οποίο γίνεται με την βοήθεια ενός SA (Station Adapter). Αξίζει να αναφέρουμε πως στο AP μπορεί να συνδεθεί και ένα ενσύρματο δίκτυο μέσω μιας ασύρματης γέφυρας (WB: Wireless Bridge).
- Bluetooth: Το Bluetooth εκδόθηκε από την ομάδα Bluetooth Special Interest Group με την βοήθεια μερικών μεγάλων εταιρειών όπως Ericsson, IBM, Intel κ.α. Το Bluetooth δεν είναι πρωτόκολλο για ασύρματα δίκτυα αλλά βρίσκει εφαρμογές στα ασύρματα

προσωπικά δίκτυα WPANs (Wireless Personal Area Networks), που έχουν ακτίνα δράσης έως και 10 μέτρα. Το Bluetooth λειτουργεί στην μπάντα των 2.4 GHz, χρησιμοποιώντας ως τεχνική διαμόρφωσης την FHSS και ο ρυθμός μετάδοσης δεδομένων φτάνει το 1 Mbps.

- Τεχνολογία MIMO: Η τεχνολογία MIMO (Multiple Input Multiple Output) έχει ως στόχο να βελτιώσει την ακτίνα δράσης, την ισχύ του σήματος και την αξιοπιστία του WLAN. Η MIMO τεχνολογία χρησιμοποιεί πολλαπλές κεραίες εκπομπής και πολλαπλές κεραίες λήψης.
- WIMAX: Η τεχνολογία WIMAX ανήκει σε μια νέα οικογένεια προτύπων. Η προηγούμενη πρωτοεμφανίστηκε το 2001, όταν το πρώτο 802.16 πρότυπο εγκρίθηκε και το ακολούθησαν τα πρότυπα 802.16a, 802.16b και 802.16c προκειμένου να βελτιωθούν θέματα που σχετίζονταν με το φάσμα συχνοτήτων, την ποιότητα εξυπηρέτησης και τη διαλειτουργικότητα. Τον 2003 αναπτύχθηκε το 802.16d για να αντιμετωπίσει ζητήματα του ETSI, ενώ το 2004 δημοσιοποιήθηκε το 802.16-2004, το οποίο και αναίρεσε όλες τις προηγούμενες εκδόσεις του προτύπου.

1.7 Δομικά στοιχεία ασύρματων δικτυών

Για την ανάπτυξη ενός ασύρματου τοπικού δικτύου είναι απαραίτητη κάποια υλικοτεχνική υποδομή, δηλαδή τα διάφορα στοιχεία (components) τα οποία συντονίζουν την μετάδοση, λήψη και επεξεργασία του σήματος μεταξύ των χρηστών. Η δομή αυτή περιλαμβάνει τόσο το λογισμικό (software) όσο και τον ανάλογο υλικό εξοπλισμό (hardware). (Πάλλης Ε., 2000)

- Συσκευές χρηστών (End-user devices)

Η επικοινωνία μεταξύ των χρηστών σε ένα ασύρματο δίκτυο γίνεται μέσω συγκεκριμένων συσκευών όπως:

- Σταθεροί Υπολογιστές (Desktops)
- Φορητοί Υπολογιστές (Laptops)
- Υπολογιστής παλάμης (Palmtop)
- Υπολογιστής Χειρός και εκτυπωτές (Handheld PCs and printers)
- IP Phones
- IP Cameras
- Projectors
- Printers

- Λογισμικό δικτύου (Network Software)

Ένα ασύρματο δίκτυο είναι σχεδιασμένο σύμφωνα με το κατάλληλο λογισμικό που βρίσκεται σε διάφορα μέρη του δικτύου. Ένα σύστημα διαχείρισης δικτύου (NOS: Network Operating System), όπως είναι για παράδειγμα το Microsoft NT Server, παρέχει διαφόρων ειδών υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.ά. Αυτά τα συστήματα στηρίζονται στην ύπαρξη ενός εξυπηρετητή (server), ο οποίος διαθέτει τις βάσεις δεδομένων στις οποίες μπορούν να έχουν πρόσβαση οι διάφορες συσκευές τις οποίες ελέγχει ο χρήστης. Οι τελευταίες «τρέχουν» το δικό τους λογισμικό (client software), το οποίο κατευθύνει τις εντολές του χρήστη στον server.

- Ασύρματες κάρτες δικτύου (Wireless NICs)

Η ασύρματη κάρτα δικτύου (Wireless Network Interface Card) χρησιμοποιείται για την μετάδοση του σήματος ενός υπολογιστή σε έναν άλλο υπολογιστή. Σε αυτή τη διαδικασία συμπεριλαμβάνεται η διαμόρφωση και η ενίσχυση του σήματος. Αυτή η κάρτα είναι σαν μία τυπική κάρτα δικτύου απλά διαθέτει μία μικρή κεραία. Μερικές εταιρίες παράγουν κάρτες οι οποίες συνδέονται με τον υπολογιστή μέσω μιας RS-232 σειριακής ή παράλληλης θύρας. Η διασύνδεση της ασύρματης κάρτας με την συσκευή του χρήστη συμπεριλαμβάνει και έναν οδηγό λογισμικού (software driver) που συνδέει το λογισμικό του NOC στην κάρτα.

- Σημεία πρόσβασης (access points):

Το σημείο πρόσβασης είναι μια κεντρική συσκευή σε ένα ασύρματο δίκτυο που παρέχει το εύρος για την ασύρματη επικοινωνία με τους άλλους σταθμούς σε ένα δίκτυο. Συνήθως συνδέεται σε ένα ενσύρματο δίκτυο και έτσι παρέχει μια γέφυρα ανάμεσα στο ενσύρματο δίκτυο και τις ασύρματες συσκευές. Τα σημεία πρόσβασης περιλαμβάνουν χαρακτηριστικά ασφάλειας όπως επικύρωση και

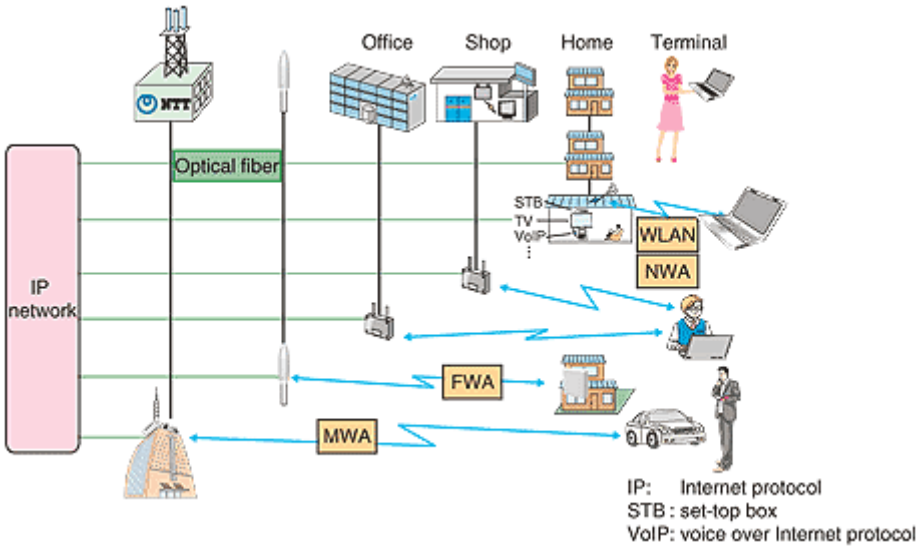
κρυπτογράφηση, έλεγχο πρόσβασης που βασίζεται σε λίστες ή φίλτρα καθώς και πολλά άλλα τα οποία συνήθως απαιτούν τη ρύθμιση τους από τον χρήστη σύμφωνα με τις προτιμήσεις του, συνήθως χρησιμοποιώντας μια διεπαφή βασισμένη στο διαδίκτυο. Πολλά σημεία πρόσβασης περιλαμβάνουν επιπρόσθετα χαρακτηριστικά δικτύωσης όπως πύλες διαδικτύου, κόμβους μεταγωγής, ασύρματες γέφυρες ή επαναλήπτες.

- Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges)

Οι ασύρματες τοπικές γέφυρες είναι βασικό κομμάτι στην τοπολογία ενός δικτύου αφού συνδέουν πολλά τοπικά δίκτυα μεταξύ ώστε να αναπτυχθεί ένα πιο λειτουργικό δίκτυο. Οι γέφυρες χωρίζονται σε δύο κατηγορίες: Local bridges, δημιουργία σύνδεσης ανάμεσα σε κοντινά τοπικά δίκτυα και Remote bridges, δημιουργία σύνδεσης ανάμεσα δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα των τοπικών δικτύων. Συνήθως οι γέφυρες, οι οποίες είναι συσκευές που χρησιμεύουν στην διασύνδεση ασύρματου με ενσύρματου δικτύου, αλλά και τη διασύνδεση πολλών WLAN μεταξύ τους, αναφέρονται ως APs (Access Points).

- Κεραίες (Antennas)

Οι κεραίες είναι υπεύθυνες για την εκπομπή του διαμορφωμένου σήματος στον αέρα και μπορούν να διακριθούν σε πολλές κατηγορίες και βασικά τους χαρακτηριστικά είναι η ισχύς μετάδοσης (Transmit power), το εύρος ζώνης (Bandwidth), το μοντέλο διάδοσης (propagation pattern) που χρησιμοποιούν και το κέρδος (Gain). Ο τρόπος που μεταδίδει το σήμα μια κεραία καθορίζει επίσης και την περιοχή κάλυψης της. Για την μετάδοση του σήματος στα ασύρματα δίκτυα χρησιμοποιούνται κυρίως δύο είδη κεραιών η πολυκατευθυντική (omnidirectional) κεραία, όπου πρόκειται για κεραίες που διοχετεύουν την ισχύ τους προς κάθε κατεύθυνση και αθροιστικά έχουν την ίδια ενίσχυση προς κάθε κατεύθυνση. Το πρότυπο εκπομπής τους είναι τέτοιο, ώστε να δημιουργούν γύρω τους ένα πεδίο που μοιάζει με «ιπτάμενο δίσκο». Η δεύτερη κατηγορία περιλαμβάνει την μονοκατευθυντική (directional) κεραία η οποία συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση.



Εικόνα 2 Ασύρματα δίκτυα

1.8 Πρότυπο IEEE 802.11

Το πρώτο πρότυπο ασύρματων τοπικών δικτύων είναι το IEEE 802.11 και όπως προαναφέραμε είναι υπεύθυνο για τον έλεγχο πρόσβασης στα ασύρματα δίκτυα και υιοθετήθηκε το 1997. (IEEE 802.11 WG)

- Οικογένεια: Στα τέλη του 1999 η IEEE γνωστοποίησε δύο νέα συμπληρωματικά πρότυπα για WLANs, τα 802.11a, 802.11b, 802.11g και 802.11y.
    - Το 802.11a μπορεί να υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps, ονομαστικός ρυθμός μετάδοσης, με συνήθη ρυθμό μετάδοσης 23 Mbits/s, εμβέλεια εσωτερικού χώρου έως και 35 m και χρήση της τεχνικής διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) στην μπάντα των 5,7 GHz.
    - Το 802.11b είναι ουσιαστικά ο αντικαταστάτης του αρχικού 802.11 αφού υποστηρίζει ρυθμούς δεδομένων έως και 11 Mbps, με εμβέλεια εσωτερικού χώρου έως και 35 m ενώ χρησιμοποιεί ως διαμόρφωση την τεχνική DSSS (direct-sequence spread spectrum) στα 2.4 GHz.
    - Το 2003, η IEEE κοινοποίησε το πρότυπο 802.11g, το οποίο υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps, με συνήθη ρυθμό μετάδοσης 19 Mbits/s, εμβέλεια εσωτερικού χώρου έως και 38 m με την τεχνική OFDM στα 2.4 GHz.
    - Για το 2008, προτάθηκε από την IEEE το πρότυπο 802.11y, το οποίο χρησιμοποιεί την τεχνική MIMO (Multiple – Input Multiple - Output) με συχνότητα 3,7 GHz, ρυθμό μετάδοσης 54Mbits/s και εμβέλεια 5000 m.

Εκτός των παραπάνω εκδόσεων έχουν προταθεί και κάποιες άλλες επεκτάσεις τους, οι οποίες όμως δεν έχουν υλοποιηθεί σε εμπορικά προϊόντα και έχουν περισσότερο ακαδημαϊκό ενδιαφέρον. (IEEE 802.11 WG)

- 802.11e ή QoS: προσπαθεί να εξασφαλίζει ικανοποιητική ποιότητα υπηρεσιών για εφαρμογές πραγματικού χρόνου που εκτελούνται πάνω σε ένα WLAN ελαχιστοποιώντας ή μεγιστοποιώντας ένα από τα παρακάτω κριτήρια: μέση καθυστέρηση από άκρο σε άκρο, μέση μεταβολή της καθυστέρησης ή μέσο ποσοστό επιτυχούς παράδοσης πλαισίων.
- 802.11n, το οποίο με χρήση πολλαπλών κεραιών (μέθοδος γνωστή ως MIMO, εκ του Multiple Input Multiple Output) παρέχει ονομαστικό ρυθμό μετάδοσης τουλάχιστον 108 Mbps. Το πρότυπο οριστικοποιήθηκε το 2009.

1.9 Χαρακτηριστικά του IEEE 802.11

Η ζώνη συχνοτήτων των 2.4 GHz σήμερα είναι ιδιαίτερα δημοφιλής, διότι είναι μία ελεύθερη ζώνη με συγκεκριμένα χαρακτηριστικά που επιτυγχάνουν την επικοινωνία σε μεγάλες αποστάσεις. Στη συνέχεια θα παρουσιάσουμε τα πιο σημαντικά: (www.ebusinessforum.gr)

- Εμβέλεια

Η εμβέλεια ενός τοπικού ασύρματου δικτύου σε εσωτερικούς χώρους κυμαίνεται από 20 έως 38 μέτρα. Τα ραδιοκύματα όμως πρέπει να διαπεράσουν τοίχους και οροφές, οπότε έχουμε σημαντικές απώλειες του σήματος. Επιπλέον το σήμα υπόκειται και σε άλλους μηχανισμούς διάδοσης όπως είναι η ανάκλαση σε προσπίπτουσες επιφάνειες ή η διάχυση. Σε περιβάλλον όμως με οπτική επαφή (Line Of Sight) μεταξύ των χρηστών, σε εξωτερικό χώρο, η εμβέλεια του ασύρματου δικτύου είναι μεγαλύτερη και εξαρτάται από διάφορους παράγοντες που σχετίζονται με τις συσκευές όπως την ευαισθησία του δέκτη, την ποιότητα των κεραιών, το επίπεδο παρεμβολών και θορύβου.

- Ρυθμός μετάδοσης

Ο ρυθμός μετάδοσης του σήματος εξαρτάται από διάφορους παράγοντες όπως η απόσταση, οι ανακλάσεις, η απορρόφηση και η σκέδαση, αλλά και ο αριθμός των χρηστών.

- Ποιότητα επικοινωνίας

Ύστερα από την πάροδο ετών χρήσης και εκατοντάδων εμπορικών και στρατιωτικών εφαρμογών, οι τεχνολογίες ασύρματης μετάδοσης έχουν γίνει πολύ αξιόπιστες.

- Συμβατότητα με το υπάρχον δίκτυο

Τα πιο πολλά ασύρματα δίκτυα έχουν συγκεκριμένο τρόπο διασύνδεσης με τα ενσύρματα δίκτυα, επομένως η προσάρτηση ασύρματης δικτύωσης, σε υπάρχουσες δομές δικτύων, μπορεί να γίνει με εύκολο τρόπο.

- Παρεμβολές

Το ασύρματο τοπικό δίκτυο μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλες συσκευές που λειτουργούν στα 2.4GHz όπως άλλα ασύρματα δίκτυα, ασύρματα τηλέφωνα, φούρνοι μικροκυμάτων και συσκευές Bluetooth. Σημαντικότερες όμως είναι οι παρεμβολές που προκύπτουν από την κακή σχεδίαση ενός ασύρματου δικτύου.

- Διαλειτουργικότητα

Οι περιπτώσεις κατά τις οποίες οι συσκευές δε συνεργάζονται μεταξύ τους είναι λόγω διαφορετικής τεχνολογίας, λόγω διαφορετικής συχνότητας, ή λόγω διαφορετικών υλοποιήσεων

- Η Τοπολογία του 802.11

Η τοπολογία του 802.11 αποτελείται από στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο το οποίο παρέχει τη δυνατότητα μετακίνησης των σταθμών χωρίς να γίνεται αντιληπτή στα ανώτερα στρώματα, όπως το LLC (Logical Link Control). Ένας σταθμός (station) είναι κάθε συσκευή η οποία εμπεριέχει τις λειτουργίες του 802.11. Οι λειτουργίες του 802.11 ενυπάρχουν (reside) σε μια ασύρματη κάρτα δικτύου NIC (Network Interface Card), το λογισμικό διασύνδεσης που οδηγεί την κάρτα NIC και τον σταθμό βάσης ή AP (Access Point).

ΚΕΦΑΛΑΙΟ 2^{ο} ΑΣΦΑΛΕΙΑ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΥΠΟΛΟΓΙΣΤΩΝ

2.1 Εισαγωγή

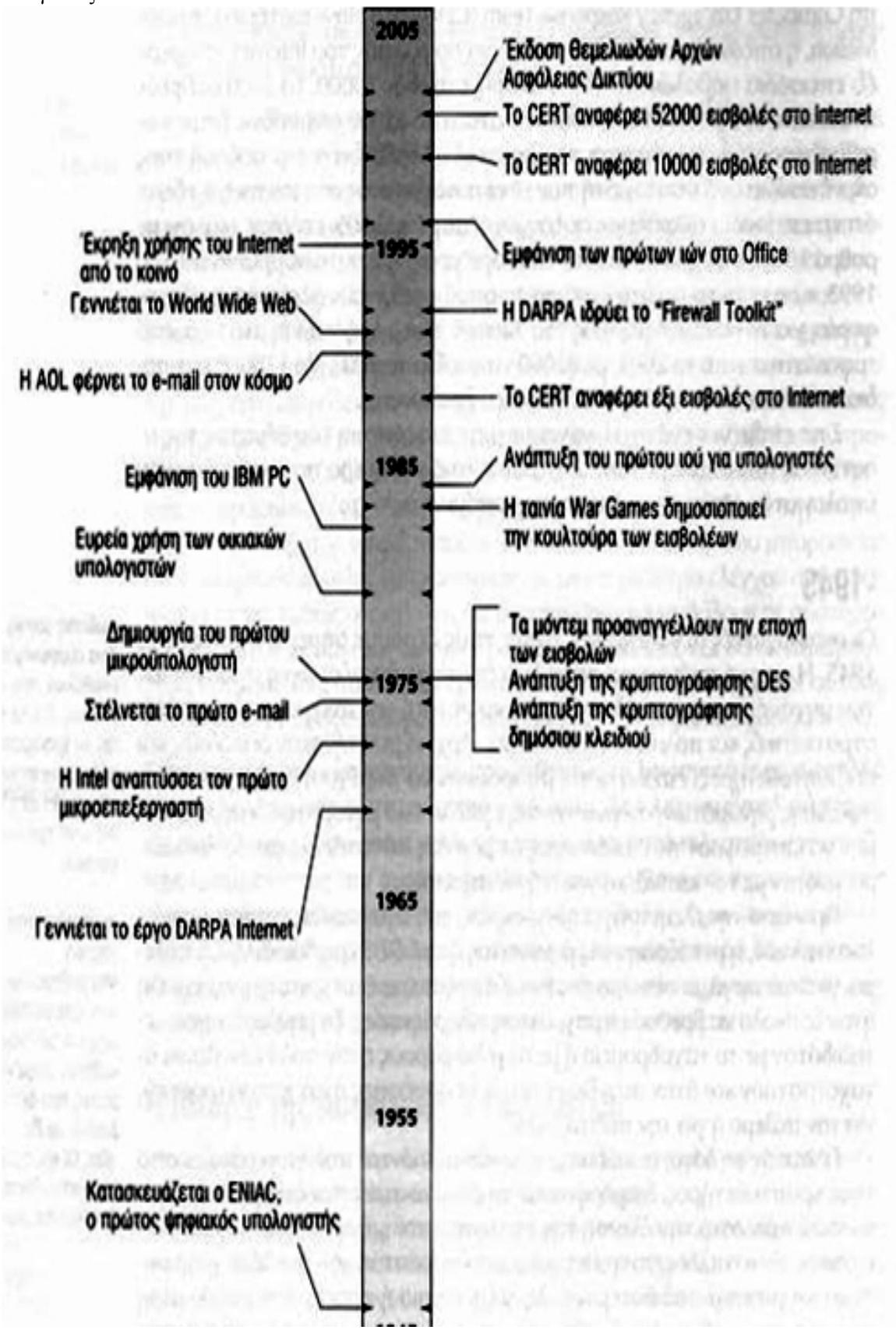
Πιο παλιά, εμφανίζονταν διαρκώς ιστορίες μεγάλων και καταστροφικών εισβολών στους ηλεκτρονικούς υπολογιστές με πιο γνωστή, το 2001 όπου ήταν ένα ιδιαίτερα κακό έτος για την ασφάλεια στο Internet. Τότε ένα «σκουλήκι» με το όνομα Code Red διαχύθηκε χωρίς έλεγχο μέσα στο Internet και αφού διορθώθηκε ο ιός Nimda έκανε ακριβώς το ίδιο πράγμα. Οι ιοί, οι οποίοι είναι υπεύθυνοι για την παραβίαση της ασφάλειας των συστημάτων υπολογιστών, διαχέονται συχνά μέσω e-mail. Όταν η Microsoft εμφάνισε στην αγορά το λειτουργικό σύστημα Windows XP, αποδείχθηκε ότι είχε ένα σφάλμα ασφάλειας, το οποίο ήταν τόσο εμφανές, που οι περισσότεροι εισβολείς θα μπορούσαν να εισβάλουν, σχεδόν, σε κάθε υπολογιστή χωρίς ιδιαίτερη προσπάθεια (http://greg61.gr/blog/)

Οι πρότυπες υπηρεσίες FTP (File Transfer Protocol) και NDS του Unix υπέστησαν εισβολές, δίνοντας μάλιστα στους εισβολείς την δυνατότητα να εισέλθουν σε ιστοσελίδες και να καταστρέψουν τα περιεχόμενά τους. Μέχρι το 2004, παραλλαγές του Nimda συνέχιζαν να υπάρχουν ακόμη στο Internet, πραγματοποιώντας επιθέσεις σε νέες εγκαταστάσεις, ενώ παρόμοιοι ιοί όπως ο Sasser χρησιμοποιούν το διορθωμένο κώδικα για να υλοποιήσουν νέες επιθέσεις. Οι επιχειρήσεις δαπανούν ολοένα και περισσότερα χρήματα ώστε να εξασφαλίσουν την ασφάλεια των πληροφοριακών τους συστημάτων, αλλά οι εισβολείς βελτιώνουν και αυτοί με τη σειρά τους τα εργαλεία που χρησιμοποιούν για τις παραβιάσεις τους. (http://greg61.gr/blog/)

Το έτος που άρχισαν να καταγράφονται τα πρώτα προβλήματα λόγω παραβίασης της ασφάλειας είναι το 1988, από την επιτροπή Computer Emergency Response Team (CERT) στο Πανεπιστήμιο Carnegie Mellon, η οποία παρακολουθεί επεισόδια ασφάλειας του Internet και είχε αναφέρει έξι επεισόδια εισβολών. Η ίδια επιτροπή το 1999, ανέφερε σχεδόν 10000 επιθέσεις, το 2000 ανέφερε πάνω από 22000, ενώ το 2001 ανέφερε πάνω από 52000 επεισόδια Αυτοί οι αριθμοί φαίνονται πολύ μεγάλοι, όμως αν αναλογιστούμε μεμονωμένα τις επιθέσεις που συμβαίνουν σε κάθε υπολογιστή που είναι συνδεδεμένος στο Internet, θα συνειδητοποιήσουμε ότι τα επεισόδια ασφάλειας αυξάνονται με ρυθμό 50% ετησίως και όχι με ρυθμό 100%, που φαίνεται από τους αριθμούς. Ωστόσο από το 2003 και μετά αυτή η αύξηση των επιθέσεων τείνει να μειωθεί. (http://greg61.gr/blog/)

Εικόνα 3 επίθεση από ιό

Στην εικόνα που ακολουθεί φαίνεται συνοπτικά η εξέλιξη των μηχανισμών ασφαλείας στους υπολογιστές.



Εικόνα 4 Εξέλιξη ασφάλειας υπολογιστών (πηγή: (http://greg61.gr/blog/))

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών. (http://greg61.gr/blog/)

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με την ποιότητα και την απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μίας επιχείρησης ή ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό στη σημερινή εποχή όπου πλέον το μεγαλύτερο ποσοστό των παρερχομένων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική. (http://greg61.gr/blog/)

Η έννοια της ασφάλειας ενός δικτύου υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Επίσης έχει να κάνει με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου. (http://greg61.gr/blog/)

Επομένως η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη σχετικών μέτρων. Πιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

- Πρόληψη (prevention) : Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- Ανίχνευση (detection) : Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- Αντίδραση (reaction) : Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών, μπορούν να ορίσουν την ασφάλεια δικτύων και πληροφοριών. (http://greg61.gr/blog/)

Όμως όταν ένα σύστημα βρίσκεται συνδεδεμένο στο δίκτυο, το κάνει πιο επιρρεπές σε απειλές που προέρχονται και από νόμιμους χρήστες του συστήματος αλλά κυρίως από επίδοξους εισβολείς. Κάθε κόμβος του δικτύου είναι ένα υπολογιστικό σύστημα με όλα τα γνωστά προβλήματα ασφάλειας. Σε αυτά, έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας μέσω ενός πολύ εκτεθειμένου μέσου και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανώς μη-έμπιστων υπολογιστικών συστημάτων. Μερικοί λόγοι για τους οποίους αποκτούν ιδιαίτερη σημασία τα θέματα ασφάλειας δικτύων υπολογιστών είναι οι εξής: (http://greg61.gr/blog/)

- Η αυξημένη περιπλοκότητα η οποία περιορίζει το αίσθημα εμπιστοσύνης για την ασφάλεια των δικτύων.
- Αύξηση στον αριθμό των διαύλων επικοινωνίας επομένως και των πιθανών σημείων επίθεσης, τα οποία πρέπει να οχυρωθούν κατάλληλα.
- Τα ασαφή όρια των δικτύων και οι διακρίσεις μεταξύ των τμημάτων μιας επιχείρησης. Κάθε κόμβος οφείλει να είναι ικανός να αντιδράσει σωστά στη παρουσία ενός νέου και μη-έμπιστου κόμβου. Από την άλλη, κάθε κόμβος μπορεί να ανήκει ταυτόχρονα σε περισσότερα από ένα δίκτυα, με αποτέλεσμα να μην είναι ξεκάθαρη η εικόνα των νομίμων χρηστών του κάθε δικτύου.
- Η δυνατότητα ανωνυμίας ενός χρήστη απαιτεί ισχυρούς μηχανισμούς πιστοποίησης μεταξύ των υπολογιστών, που συνήθως είναι διαφορετικοί από αυτούς που πιστοποιούν τους χρήστες στα υπολογιστικά συστήματα.
- Υπάρχει αδυναμία ελέγχου της δρομολόγησης των δεδομένων που διακινούνται μέσω των δικτύων.

Όπως είναι αναμενόμενο, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Μάλιστα πολλές φορές το κόστος της ασφάλειας εμφανίζεται και ως κόστος χρόνου και ως κόστος χρήματος επομένως, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Αυτό όμως δεν είναι σωστό εφόσον η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του. (http://greg61.gr/blog/)

Το συγκεκριμένο κόστος εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας της επιχείρησης. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης. (http://greg61.gr/blog/)

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης. (http://greg61.gr/blog/)

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιομένη επιτηδειότητα των 'επιτιθέμενων', απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο. (http://greg61.gr/blog/)

2.2 Ασφάλεια και προστασία ως απαίτηση

Τα τελευταία χρόνια με την αύξηση της σπουδαιότητας του ρόλου που έχουν τα συστήματα πληροφορικής μέσα στο υπερσύστημα των επιχειρήσεων, αυξήθηκαν και αυτοί που έχουν συμφέρον, άρα και δικαίωμα απαίτησης, το πληροφοριακό σύστημα να ικανοποιεί αρκετούς κανόνες ασφαλείας και προστασίας. Επομένως κάποιοι από αυτούς που έχουν δικαίωμα απαίτησης να υπάρχουν μηχανισμοί και μέτρα ασφαλείας είναι: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

1. ο ιδιοκτήτης του συστήματος.
2. ο σχεδιαστής.
3. ο χρήστης.
4. ο πελάτης.
5. η πολιτεία
6. οι πολίτες, των οποίων οι προσωπικές πληροφορίες είναι αποθηκευμένες ή υφίστανται επεξεργασία από κάποια συστήματα υπολογιστών.

Ο ιδιοκτήτης ενός συστήματος υπολογιστών είναι αυτός ο οποίος εξακολουθεί να έχει υψηλές απαιτήσεις σχετικά με την ασφάλεια και την προστασία, γιατί όλο και περισσότερο εξαρτάται από την απρόσκοπτη λειτουργία του πληροφοριακού συστήματος. Επίσης η δημιουργία ενός πληροφοριακού συστήματος απαιτεί ένα υψηλό κόστος, επομένως είναι λογικό να θέλει να προστατευθεί με τον καλύτερο τρόπο. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Επόμενος στη λίστα των δικαιούχων είναι ο σχεδιαστής του συστήματος ο οποίος προσπαθεί κατά τη δημιουργία του συστήματος, να ικανοποιήσει τις ανάγκες του πελάτη. Ωστόσο ο σχεδιαστής αντιμετωπίζει δυσκολίες διότι τόσο το σύστημα όσο και το περιβάλλον είναι δυναμικό κάτι το οποίο γίνεται αντιληπτό, διότι οι ανάγκες των ανθρώπων μεταβάλλονται όπως ακριβώς

συμβαίνει και με την τεχνολογία. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Ο τρίτος που απαιτεί ασφάλεια είναι ο χρήστης, ο οποίος θέτει απαιτήσεις σε σχέση με την ασφάλεια και την προστασία του συστήματος, σχετικά με τρία θέματα: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

(α) Τα μέτρα και οι διαδικασίες ασφάλειας και προστασίας δεν πρέπει να θέτουν εμπόδια στις λειτουργίες του συστήματος.

(β) Η πρακτική έχει δείξει ότι οι χρήστες συνήθως βρίσκουν τρόπους να παρακάμπτουν συμπλοκές, ως προς τη λειτουργία, μηχανισμούς προφύλαξης.

(γ) Ο χρήστης δυσανασχετεί και υποφέρει από άκαμπτα μέτρα και μηχανισμούς.

Επόμενος δικαιούχος στις απαιτήσεις ασφάλειας έρχεται ο πελάτης, ο οποίος έπεται τον χρηστή, γιατί σε αυτή την κατηγορία τοποθετούμε εκείνον που εξαρτάται από το σύστημα (π.χ. για τη λήψη μιας απόφασης), χωρίς να είναι απαραίτητα άμεσος ο χρήστης, όπως είναι για παράδειγμα, ο πελάτης μιας τράπεζας, ο ασθενής ενός νοσοκομείου, ο πελάτης μιας αεροπορικής εταιρείας, ο επιβάτης ενός αεροπλάνο, κ.λπ.. Ο πελάτης συνήθως απαιτεί την υψηλή διαθεσιμότητα του συστήματος, την ακεραιότητα των δεδομένων και την προστασία της εμπιστευτικότητας των πληροφοριών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Τέλος η πολιτεία καθορίζει σημαντικό ρολό στην διαμόρφωση των μέτρων προφύλαξης, με το να θέτει πλαίσια και κανόνες που πρέπει να τηρούνται. Η βαρύτητα των ποινικών αδικημάτων που μπορούν να διαπραχτούν από την χωρίς περιορισμούς συλλογή, αρχειοθέτηση, χρήση, μετάδοση και επεξεργασία πληροφοριών, αναγκάζει την πολιτεία να καθορίζει αρχές, η παράβαση των όποιων θα συνεπάγεται με ποινικές κυρώσεις. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

2.3 Αναγκαιότητα Ασφαλών Λειτουργικών Συστημάτων

Σύμφωνα με έναν από τους βασικούς ορισμούς που δίνονται «Λειτουργικό σύστημα ενός υπολογιστή ονομάζεται το προϊόν λογισμικού που ελέγχει την εκτέλεση των προγραμμάτων και παρέχει υπηρεσίες χρονοδρομολόγησης (scheduling), σφαλματοθυρίας (debugging), έλεγχου εισόδου-εξόδου (I/O control), μεταγλώττισης (compilation), διαχείρισης μνήμης (memory management) και άλλες σχετικές». (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Συγκεκριμένα, ένα οποιοδήποτε λειτουργικό σύστημα θα πρέπει να διαθέτει τις παρακάτω ιδιότητες: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

- **Ευχρηστία** (usability), δηλαδή το σύστημα θα πρέπει να είναι σχεδιασμένο ώστε να διευκολύνει τον χρήστη.
- **Γενικότητα** (generality), το σύστημα θα πρέπει να μπορεί να εκτελεί ποικίλες διαδικασίες, σύμφωνα με τις ανάγκες του χρηστή.
- **Αποδοτικότητα** (efficiency), το σύστημα πρέπει να λειτούργει γρήγορα και σωστά, χρησιμοποιώντας κατά τον καλύτερο τρόπο τους πόρους (resources) που διατίθενται.
- **Ορατότητα** (visibility), ο χρήστης πρέπει να γνωρίζει όλα όσα απατούνται για την βέλτιστη χρήση του συστήματος.
- **Ευελιξία** (flexibility), το σύστημα πρέπει να μπορεί να προσαρμόζεται διαρκώς σε μεταβαλλόμενες καταστάσεις.
- **Αδιαφάνεια (**opacity), ο χρήστης πρέπει να γνωρίζει μόνο ότι είναι απαραίτητο για να διεκπεραιώσει την εργασία του.
- **Ασφάλεια** (security), το σύστημα πρέπει να διαφυλάσσει τα δεδομένα ενός χρηστή από την μη εξουσιοδοτημένη χρήση αυτών από άλλους.
- **Ακεραιότητα** (integrity), οι χρήστες και τα δεδομένα τους, πρέπει να προφυλάσσονται από απρόβλεπτες μετατροπές από μη εξουσιοδοτημένους χρήστες.

- **Ευκινησία** (capacity), οι χρήστες δεν πρέπει να υφίστανται άσκοπους περιορισμούς στις ενέργειες τους.
- **Αξιοπιστία** (reliability), τα συστήματα πρέπει να λειτουργούν σωστά, για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.
- **Συγκρισιμότητα** (serviceability), πιθανά προβλήματα στη λειτουργία του συστήματος πρέπει να μπορούν να ξεπεραστούν εύκολα και γρήγορα.
- **Επεκτασιμότητα** (extendibility), το σύστημα πρέπει να μπορεί να αναβαθμιστεί εύκολα, με επέκταση των δυνατοτήτων που διαθέτει.
- **Διαθεσιμότητα** (availability), το σύστημα πρέπει να εξυπηρετεί κάποιους χρηστές όσο το δυνατόν πληρεστέρα, για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

Για να ισχύει καθεμία από τις παραπάνω ιδιότητες, θα πρέπει ο σχεδιαστής ενός λειτουργικού συστήματος να προβλέψει την ύπαρξη κατάλληλων τεχνικών και διαδικασιών.

2.4 Θεμελιώδεις αρχές προστασίας

Υπάρχουν δυο βασικοί στόχοι για την προστασία ενός Λειτουργικού Συστήματος, η κατασταλτική προστασία (detection) και η προληπτική προστασία (prevention).

2.4.1 Κατασταλτική Προστασία

Η κατασταλτική προστασία μπορεί και πραγματοποιείται μέσα από μια σειρά μεθόδων, με πιο σημαντική αυτή της επίβλεψης (surveillance). Αυτή η μέθοδος στοχεύει στην καταγραφή κάθε μη εξουσιοδοτημένης απόπειρας εισόδου στο λειτουργικό σύστημα. Επίσης μέσω αυτής της διαδικασίας παρακολουθείται συνεχώς η συνολική λειτουργιά του συστήματος, ώστε να εξασφαλίσει ότι οι μηχανισμοί λειτουργιάς λειτουργούν διαρκώς κανονικά. Η μέθοδος αυτή χρησιμοποίει δυο τεχνικές: την παρακολούθηση των διαρροών (threat monitoring) και την εποπτεία της ασφάλειας (security audit). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Η πρώτη μέθοδος, η παρακολούθηση των διαρροών, σκοπεύει στην άμεση αποκάλυψη κάθε απόπειρας παραβίασης του λειτουργικού συστήματος και στην λήψη απαραίτητων μέτρων για την ακύρωση τους. Με την επόμενη μέθοδο, την εποπτεία της ασφάλειας αποσκοπεί στην καταγραφή των γεγονότων που σχετίζονται με την ασφάλεια του λειτουργικού συστήματος. Μέσω της καταγραφής υπάρχει η δυνατότητα να γίνει αντιληπτή μία παραβίαση εκ των υστέρων αφού μπορεί και εξασφαλίζει τα απαιτούμενα ιστορικά στοιχειά. Αυτή η τεχνική είναι πολύ πρακτική και χρήσιμη, γιατί βοήθα στην αποκάλυψη των μεθόδων που χρησιμοποιήθηκαν για την παραβίαση ενός συστήματος, παρόλο που είναι παθητική. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Η τεχνική αυτή στηρίζεται σε ενέργειες, όπως:

- Παρακολούθηση της λειτουργίας των διαδικασιών ασφάλειας.
- Αναγνώριση των παραβιάσεων και αναφορά αυτών.
- Διάγνωση της φύσης της παραβίασης.

2.4.2 Προληπτική Προστασία

Η προληπτική προστασία σχετίζεται με παραβιάσεις που δεν πρόλαβαν να πραγματοποιηθούν και για αυτό το λόγο είναι ιδιαίτερα σημαντική, αφού το σύστημα δεν έχει υποστεί οποιαδήποτε συνέπεια και υλοποιείται με βάση δύο αρχές: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

- την αρχή της ελεγχόμενης προσπέλασης(controlled access)
- την αρχή του διαχωρισμού (isolation)

2.5 Κρυπτογραφία

Γενικά με τον όρο κρυπτογραφία εννοείται η μελέτη μαθηματικών τεχνικών οι οποίες έχουν σαν στόχο να εξασφαλίσουν θέματα που σχετίζονται άμεσα με την ασφάλεια που απαιτείται για τη μετάδοση των πληροφοριών, όπως είναι η εμπιστευτικότητα, η πιστοποίηση ταυτότητας του αποστολέα και να διασφαλισθεί το αδιάβλητο της πληροφορίας. Η κρυπτογραφία πρέπει να εξασφαλίσει την επίτευξη κάποιων βασικών στόχων όπως να φτάσουν τα μηνύματα στον σωστό προορισμό, να μπορέσει ο παραλήπτης να πιστοποιήσει την ταυτότητα του αποστολέα και η πληροφορία να μην έχει αλλοιωθεί από κάποια μη εξουσιοδοτημένη οντότητα.

Η κρυπτογραφία σύμφωνα με έρευνες που έχουν γίνει από ιστορικούς, ξεκίνησε στην αρχαιότητα και πιο συγκεκριμένα το πρώτο κρυπτογραφημένο κείμενο χρονολογείται το 1500π.Χ. στη Βαβυλώνα. Η κρυπτογραφία ξεκίνησε με την λογική τα κείμενα που μετέφεραν οι αγγελιοφόροι να μην μπορούν να τα διαβάσουν ούτε αυτοί αλλά ούτε και οι μη εγκεκριμένοι παραλήπτες. Επομένως ο Ιούλιος Καίσαρας επειδή δεν εμπιστευόταν τους αγγελιοφόρους του, εφάρμοσε ένα σύστημα κρυπτογράφησης. Πιο συγκεκριμένα, αναφέρεται ότι αντικαθιστούσε κάθε γράμμα του μηνύματος με ένα άλλο που ήταν τρεις θέσεις μπροστά στο ρωμαϊκό αλφάβητο. Την μέθοδο της κρυπτογραφίας την βλέπουμε και στο Β' Παγκόσμιο Πόλεμο όπου οι Γερμανοί ανέπτυξαν το σύστημα enigma για να μεταδίδουν απόρρητες πληροφορίες. Οι Βρετανοί τότε επιστράτευσαν γνωστούς μαθηματικούς οι οποίοι κατάφεραν να σπάσουν τον κώδικα και να διαβάσουν τα μηνύματα. (Κάτος Β. – Στεφανίδης Γ., 2003)

2.5.1 Ορισμοί κρυπτογραφίας

Στην παρούσα ενότητα δίνουμε κάποιος από τους πιο γνωστούς ορισμούς για την κρυπτογραφία: (Κάτος Β. – Στεφανίδης Γ., 2003)

- Κρυπτογραφία: Η επιστήμη, αλλά και η τέχνη, η οποία έχει ως αντικείμενο την εξεύρεση μεθόδων για το μετασχηματισμό των κειμένων έτσι ώστε να είναι αναγνωρίσιμα μόνο από εξουσιοδοτημένα άτομα.
- Κρυπτογράφηση – Encryption: Η διαδικασία μετατροπής ενός κειμένου από την αρχική του μορφή σε μη αναγνωρίσιμη ή μη επεξεργάσιμη μορφή.
- Αποκρυπτογράφηση – Decryption: Η διαδικασία με την οποία το κρυπτογραφημένο κείμενο μετασχηματίζεται στην αρχική του, αναγνωρίσιμη ή/ και επεξεργάσιμη μορφή
- Αρχικό κείμενο, είναι το κείμενο που θέλουμε να κρυπτογραφήσουμε .
- Κρυπτογραφημένο κείμενο ή κρυπτογράφημα ονομάζεται αυτό που προκύπτει μετά την κρυπτογράφηση.
- Αλγόριθμος κρυπτογράφησης ονομάζεται η μέθοδος που χρησιμοποιείται και μετατρέπει το αρχικό κείμενο σε μυστική μορφή.
- Κλειδί κρυπτογράφησης ονομάζεται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης, για παράδειγμα είναι η αντιστοιχία των γραμμάτων του αρχικού κειμένου και του κρυπτογραφήματος.

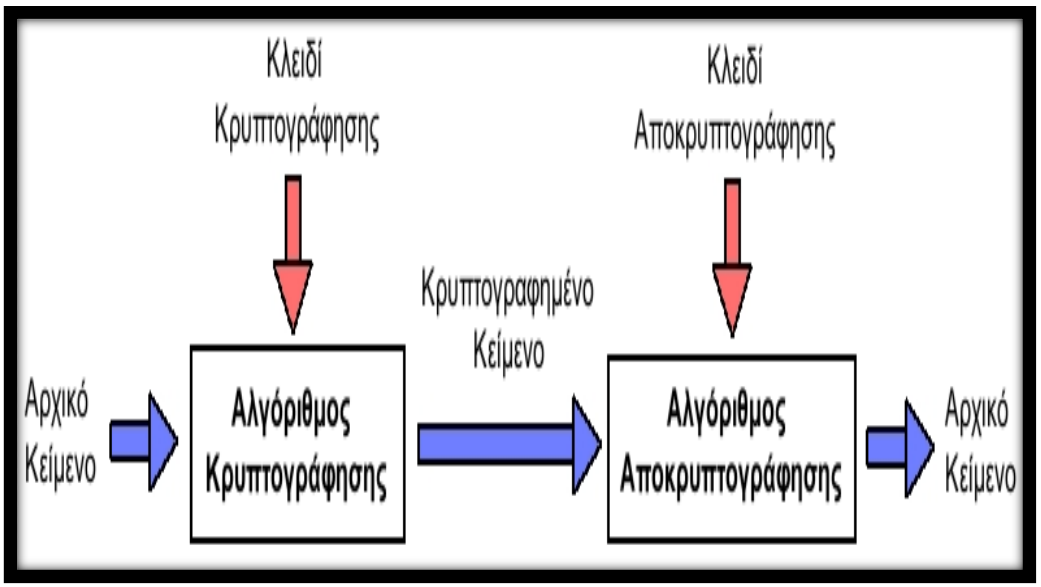
2.5.2 Συστήματα μυστικού κλειδιού

Υπάρχουν διαφόρων ειδών αλγόριθμοι κρυπτογράφησης οι οποίοι είτε χρησιμοποιούν ένα είτε περισσότερα κλειδιά. Η ασφάλεια εξασφαλίζεται με τη μη κοινοποίηση του κλειδιού, ενώ οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι ευρέως γνωστοί. (Κάτος Β. – Στεφανίδης Γ., 2003)

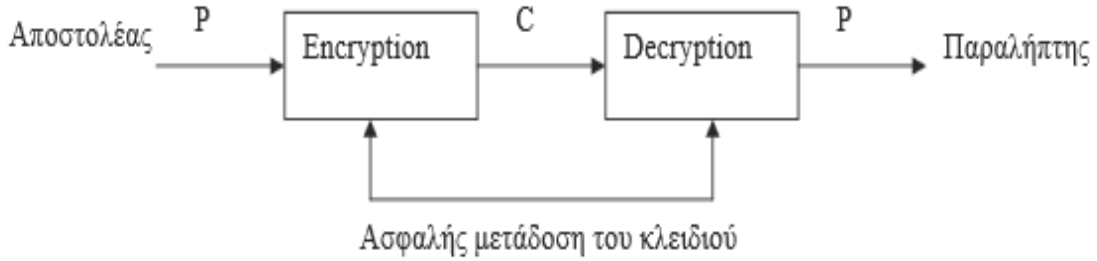
Στα συστήματα μυστικού κλειδιού περιλαμβάνεται η συμμετρική κρυπτογραφία και η ασύμμετρη όπου στην συμμετρική κρυπτογραφία έχουμε το εξής: (Κάτος Β. – Στεφανίδης Γ., 2003)

- Συμμετρική κρυπτογραφία ή διαφορετικά κρυπτογραφία μυστικού κλειδιού είναι η κρυπτογραφία που για να κρυπτογραφηθεί ή να αποκρυπτογραφηθεί κάποια πληροφορία χρησιμοποιείται το ίδιο κλειδί, το οποίο αναφέρεται ως μυστικό ή κρυφό κλειδί (secret key). Αυτό το μυστικό κλειδί είναι γνωστό μόνο μεταξύ αποστολέα και παραλήπτη που

στέλνουν την κρυπτογραφημένη πληροφορία και δεν γνωστοποιείται σε μη εξουσιοδοτημένους χρήστες.



Εικόνα 5 Συμμετρική κρυπτογραφία

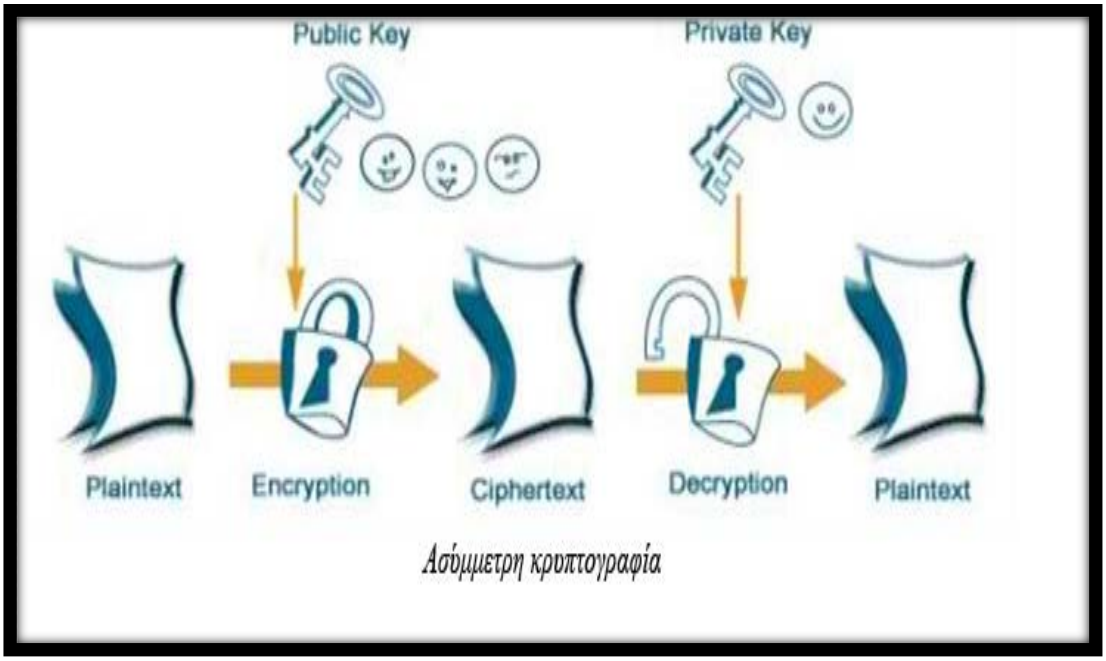


Εικόνα 6 Μυστικό κλειδί

- Η συμμετρική κρυπτογραφία χρησιμοποιείται κυρίως για να προστατεύονται τα μηνύματα από μη εξουσιοδοτημένη αποκάλυψη έτσι ώστε μόνο όσοι χρήστες διαθέτουν το κρυφό κλειδί να έχουν πρόσβαση στο κρυπτογραφημένο αρχείο.
- Σημαντικό πλεονέκτημα της συμμετρικής κρυπτογραφίας είναι ότι υλοποιείται γρήγορα.
- Ο αποστολέας και ο παραλήπτης πρέπει να συμφωνήσουν από την αρχή στη χρήση του κοινού κλειδιού. Για να συμβεί αυτό θα πρέπει να υπάρχει ένα ασφαλές κανάλι για να επικοινωνήσουν μεταξύ τους.
- Όλοι οι χρήστες μπορούν να κατέχουν το ίδιο κλειδί ή ανά δύο να έχουν κοινό κλειδί.
- Εάν ο αριθμός των χρηστών αυξηθεί είναι πολύ δύσκολη η ασφαλής διαχείριση του κλειδιού καθώς αυτό θα πρέπει να μεταφερθεί προς όλους τους εξουσιοδοτημένους χρήστες με ασφαλή τρόπο, οι οποίοι θα πρέπει να πάρουν όλα τα απαραίτητα μέτρα για την προστασία του.

- Ασύμμετρη κρυπτογραφία, σε αυτή τη μέθοδο αλλάζει το μυστικό κλειδί που χρησιμοποιείται στην διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης, δηλαδή δεν μπορεί το κλειδί της μίας διαδικασίας να εξαχθεί από την άλλη. Επίσης μπορεί να χρησιμοποιηθούν δύο ειδών κλειδιά, το δημόσιο και το ιδιωτικό.

- Ασύμμετρη είναι η κρυπτογραφία που χρησιμοποιεί ένα κλειδί για την κρυπτογράφηση και ένα άλλο για την αποκρυπτογράφηση.
- Μηνύματα που κρυπτογραφούνται με το ένα κλειδί, αποκρυπτογραφούνται μόνο με το άλλο κλειδί και αντιστρόφως,
- Το ένα κλειδί ονομάζεται δημόσιο και δημοσιοποιείται στο κοινό ενώ το άλλο ονομάζεται ιδιωτικό κλειδί και είναι απόρρητο.



Εικόνα 7 Ασύμμετρη κρυπτογραφία

- Δημόσιο κλειδί: Όπως αναφέραμε χρησιμοποιείται στην ασύμμετρη κρυπτογραφία και έχει την ιδιότητα ότι μπορεί και γνωστοποιείται στο κοινό μέσω δημοσίων καταλόγων ή δημόσιας βάσης δεδομένων.
- Ιδιωτικό κλειδί. Χρησιμοποιείται και αυτό στην ασύμμετρη κρυπτογραφία, παραμένει απόρρητο στο κοινό και το γνωρίζουν μόνο οι εξουσιοδοτημένοι χρήστες.

Στην ασύμμετρη κρυπτογραφία, κάθε χρήστης εφοδιάζεται τουλάχιστον με ένα ζευγάρι κρυπτογραφικών κλειδιών έτσι ώστε να υπάρχει μονοσήμαντη αντιστοιχία μεταξύ ζευγαριών κλειδιών και χρηστών. Αυτό σημαίνει ότι ένα ζεύγος αντιστοιχεί μόνο σε έναν χρήστη ωστόσο ένας χρήστης μπορεί να έχει πολλά ζεύγη κλειδιών. Το ένα κλειδί του ζεύγους μαζί με τα στοιχεία ταυτοποίησης του κατόχου όπως είναι το ονοματεπώνυμο και η διεύθυνση, ανακοινώνεται μέσω ηλεκτρονικών βάσεων δεδομένων και γι' αυτό το λόγο ονομάζεται δημόσιο κλειδί. (Κάτος Β. – Στεφανίδης Γ., 2003)

Κάθε ενδιαφερόμενος μπορεί να έχει πρόσβαση στη βάση δημόσιων κλειδιών για να πληροφορείται το δημόσιο κλειδί οποιουδήποτε χρήστη μαζί με τα αντίστοιχα στοιχεία ταυτοποίησης του ιδιοκτήτη που το συνοδεύουν. Το άλλο κλειδί του ζευγαριού κρατείται απόρρητο, δεν κυκλοφορεί ποτέ στο διαδίκτυο και το γνωρίζει μόνο ο ιδιοκτήτης του και για αυτό το λόγο ονομάζεται ιδιωτικό κλειδί. Ωστόσο υπάρχει κάποια σύνδεση μεταξύ των δύο κλειδιών και αυτή χρησιμοποιείται για: (Κάτος Β. – Στεφανίδης Γ., 2003)

- Ανταλλαγή εμπιστευτικών μηνυμάτων.
- Επιβεβαίωση ταυτότητας του αποστολέα, που ονομάζεται αυθεντικοποίηση.

Ανακεφαλαιώνοντας, στην ασύμμετρη κρυπτογραφία για την διαδικασία της κρυπτογράφησης ο αποστολέας κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη και ο παραλήπτης αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Στη συνέχεια για την επιβεβαίωση της ταυτότητας του αποστολέα αρχικά ο αποστολέας πρέπει να κρυπτογραφήσει με το ιδιωτικό του κλειδί και

έπειτα ο παραλήπτης αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα. (Κάτος Β. – Στεφανίδης Γ., 2003)

Προτού εμφανιστούν οι υπολογιστές η κρυπτογραφία εφαρμοζόταν σε μηνύματα που αποτελούνταν από τα γράμματα της αλφαβήτου, αλλά και σε αυτή την περίπτωση εφαρμόζονταν κάποιοι αλγόριθμοι. Ο αλγόριθμος της αντικατάστασης, όπου κάθε γράμμα του αρχικού μηνύματος αντικαθιστούνταν από κάποια άλλο διαφορετικό γράμμα ενός αλφάβητου που δημιουργούνταν από το κρυπτόγραμμα. Ο αλγόριθμος μετάθεσης ή αναδιάταξης, όπου το κρυπτόγραμμα αποτελεί τον αναγραμματισμό του αρχικού μηνύματος. Μάλιστα σε αυτόν τον αλγόριθμο τα γράμματα μετατοπίζονταν κάποιες θέσεις προς τα δεξιά, για παράδειγμα αν ήθελε να χρησιμοποιήσει το γράμμα Α, στο κρυπτογραφημένο μήνυμα θα το αντικαθιστούσε με το Γ. Αυτές οι τεχνικές ήταν τεχνικές συμμετρικού κλειδιού.

2.5.3 Εφαρμογές της κρυπτογραφίας

Α) Ασφαλής προσπέλαση

Η σύνδεση ενός χρηστή σε ένα δίκτυο υπολογιστών (WAN ή LAN) επιτυγχάνεται με την τεχνική των συνθημάτων (passwords). Επίσης είναι γνωστό ότι η τεχνική αυτή δεν είναι απόλυτα ασφαλής και παρουσιάζει σημαντικά προβλήματα. Για παράδειγμα έστω ότι επιθυμούμε να εισάγουμε κάποιο κωδικό στον υπολογιστή μας, αυτό μπορεί να γίνει και όταν βρίσκεται ένας παρευρισκόμενος κοντά μας, ή όταν πολλές φορές πραγματοποιούμε σύνδεση σε ένα απομακρυσμένο υπολογιστή εκθέτει τον χρηστή σε υποκλοπές του συνθηματικού, και αυτό συμβαίνει διότι είναι συνήθως περιορισμένη η επιλογή των συνθηματικών, και η εύρεση τους μπορεί να επιτεθεί εύκολα χωρίς ιδιαίτερη παραβίαση του συστήματος. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Όπως γνωρίζουμε όλοι, συχνά για κωδικούς πρόσβασης βάζουμε το όνομα μας τα γενέθλια μας, κάποιο στοιχείο το οποίο είναι γενικά εύκολο να θυμόμαστε, άρα είναι εξίσου εύκολο κάποιος να το μαντέψει χωρίς να πρέπει να χρησιμοποιήσει κάποιο λογισμικό. Γενικότερα, στο πρόβλημα της ασφαλούς σύνδεσης εμπίπτουν οι περιπτώσεις των τραπεζικών μηχανών ATM, της καλωδιακής τηλεόρασης και των καρτών τηλεφώνων. Παρόλο που το πλήθος των ανταλλασσόμενων πληροφοριών στις περιπτώσεις αυτές είναι μικρό, η ζημιά που μπορεί να προκληθεί είναι μεγάλη. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Όμως μία ασφαλής προσπέλαση μπορεί να επιτευχθεί με την χρήση κρυπτογραφικών τεχνικών, όπου μία τέτοια τεχνική βασίζεται σε μια διαδικασία κρίσης-απόκρισης των εμπλεκόμενων μερών και χρησιμοποίει ψηφιακές υπόγραφες. Σε αυτήν ο χρήστης υπογράφει μια τυχαία συμβολοσειρά του συστήματος η όποια επαληθεύεται από το σύστημα. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Μια άλλη τεχνική βασίζεται σε συστήματα μηδενικής γνώσης. Σε αυτήν ο χρήστης εφοδιάζεται με μια υπογραφή της ταυτότητας του από το αρμόδιο κέντρο. Κατά την πραγματοποίηση μιας προσπέλασης χρησιμοποιείται ένα σύστημα μηδενικής γνώσης για να αποδείξει ότι γνωρίζει την υπογραφή χωρίς να την αποκαλύψει. Η υλοποίηση και των δυο αυτών τεχνικών μπορεί να γίνει με την χρήση καρτών (smart cards). Μια έξυπνη κάρτα είναι μια βελτιωμένη έκδοση της συμβατικής πιστωτικής κάρτας, η όποια περιέχει ένα μικροεπεξεργαστή με συνδέσεις εισόδου-εξόδου. Ο μικροεπεξεργαστής αυτός διαθέτει περιορισμένη ασφαλή μνήμη (EPROM και EEPROM) για την καταχώρηση του μυστικού κλειδιού και άλλων στοιχείων, και μπορεί να εκτελεί βασικές πράξεις συμπεριλαμβανόμενων και κρυπτογραφικών αλγορίθμων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Β) Ψηφιακά διαβατήρια

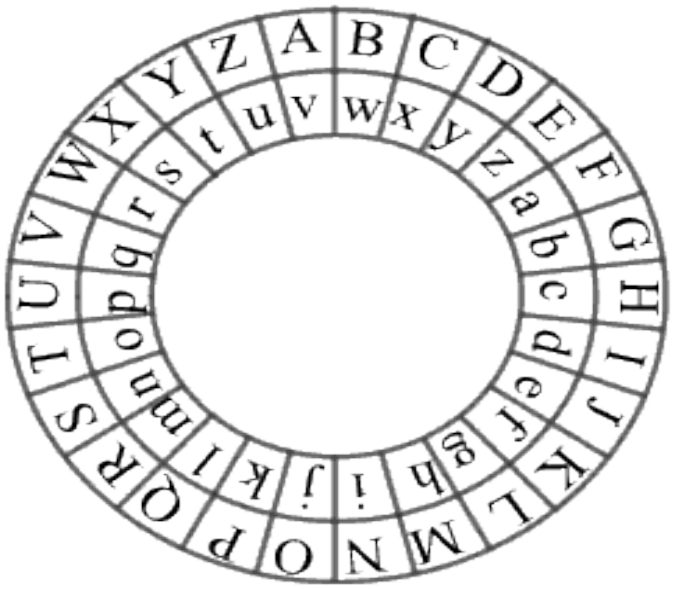
Τα διαβατήρια είναι ένας τρόπος αναγνώρισης ταυτότητας (ταυτοποίησης). Με τη χρήση των ηλεκτρονικών υπολογιστών είναι δυνατόν να δημιουργηθούν ασφαλή ψηφιακά διαβατήρια. Η τεχνική είναι ανάλογη με αυτή της ασφαλούς προσπέλασης. Κάθε τρόπος εκδίδει ένα ψηφιακό

διαβατήριο το οποίο περιλαμβάνει μια υπογραφή της ταυτότητας του χρηστή. Έτσι όταν, ο κάτοχος του διαβατηρίου θέλει να ταχτοποιηθεί αποδεικνύει, χρησιμοποιώντας ένα πρωτόκολλο μηδενικής γνώσης, ότι γνωρίζει την υπογραφή χωρίς να την επιδείξει και αυτό διότι η επίδειξη της αποδείξεως μπορεί να οδηγήσει σε πλαστογράφηση. Είναι απαραίτητο το ψηφιακό διαβατήριο να υλοποιηθεί με tamper-free συσκευές όπως οι έξυπνες κάρτες. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Γ)Ηλεκτρονική μεταβίβαση δεδομένων

Η ηλεκτρονική μεταβίβαση των δεδομένων EDI (Electronic Data Interchange) είναι μια τεχνική ηλεκτρονικής μεταφοράς μηνυμάτων μεταξύ πληροφοριακών συστημάτων σύμφωνα με καθορισμένα πρότυπα δόμησης. Στις ανεπτυγμένες χώρες η τεχνική αυτή αποτελεί καθημερινή πρακτική στο εμπόριο και τη βιομηχανία για τη διεκπεραίωση συναλλαγών, αποφεύγοντας το συμβατικό τρόπο επεξεργασίας και ανταλλαγής εγγράφων. Σύμφωνα με αυτόν οι ανταλλασσόμενες εντολές (πληρωμές, προμήθειες κλπ) μορφοποιούν αυστηρά καθορισμένα πρότυπα, έτσι ώστε να αναγνωρίζονται από τα υπολογιστικά συστήματα εμπλεκόμενων μερών. Η όλη διαδικασία ολοκληρώνεται εντός ελάχιστου χρόνου ηλεκτρονικά με συνέπεια να επιτυγχάνεται ο εμπορικός κύκλος. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Για τη γνησιότητα και ακεραιότητα μιας εντολής, στα πλαίσια του EDI, μπορεί να χρησιμοποιείται η τεχνική ψηφιακής υπογραφής, ενώ η εξασφάλιση της μυστικότητας των ανταλλασσόμενων εντολών επιτυγχάνεται με τη χρήση κρυπτογραφικών τεχνικών. Η παρεχομένη ασφάλεια εξαρτάται από το χρησιμοποιημένο κρυπτογραφικό σύστημα. Η τεχνική SWIFT (Society for Worldwide Interbank Financial Telecommunication), ως μια ειδική μορφή EDI, έχει καθιερωθεί για την ασφαλή διεκπεραίωση τραπεζικών συναλλαγών. Η τελευταία έκδοση της τεχνικής αυτή χρησιμοποιεί το σύστημα DES για την κρυπτογράφηση και την ψηφιακή υπογραφή RSA για την εξασφάλιση της γνησιότητας και ακεραιότητας των εντολών. Τα μυστικά κλειδιά αλλάζονται σε τακτά χρονικά διαστήματα και διανέμονται με ασφαλή τρόπο. Το όλο σύστημα υποστηρίζεται από ένα διεθνή οργανισμό ο όποιος καλύπτει τις συμμετέχουσες τράπεζες από τυχόν ζημίες που μπορεί να προκύψουν από παρεμβάσεις, παρόλο που η πιθανότητα μια επιτύχουν παρέμβασης είναι ελάχιστη. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)



Εικόνα 8 αρχαίο σύστημα κρυπτογραφίας

2.6 Συνήθεις απειλές στα συστήματα υπολογιστών

Ο ιός, που επιτίθεται στους ηλεκτρονικούς υπολογιστές, είναι ένα μικρό πρόγραμμα λογισμικού που εξαπλώνεται από έναν υπολογιστή σε έναν άλλο και παρεμβαίνει στη λειτουργία των υπολογιστών. Ένας ιός υπολογιστή, έχει τέτοια δύναμη, που μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν υπολογιστή, να χρησιμοποιήσει ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου για να μεταδώσει τον ιό σε άλλους υπολογιστές ή ακόμα και να διαγράψει όλα τα δεδομένα στο σκληρό δίσκο. (www.icsd.aegean.gr)

Οι ιοί υπολογιστών διαδίδονται πιο εύκολα, συνήθως από τα συνημμένα αρχεία που βρίσκονται σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μέσω άμεσων μηνυμάτων, μέσω εξωτερικών μέσων αποθήκευσης όπως μνήμη flash USB ή CD. Ωστόσο υπάρχουν προγράμματα που μπορούν να εντοπίσουν και να εξοντώσουν αυτούς τους ιούς. Ορισμένες βασικές ενδείξεις ότι ο υπολογιστής μας έχει προσβληθεί από κάποιο κακόβουλο πρόγραμμα είναι οι εξής: (http://datalabs.edu.gr)

- Ο υπολογιστής λειτουργεί πιο αργά από ότι συνήθως.
- Η λειτουργία του υπολογιστή σταματάει ή κλειδώνει συχνά.
- Ο υπολογιστής παρουσιάζει σφάλματα και μετά κάνει επανεκκίνηση κάθε λίγα λεπτά.
- Ο υπολογιστής κάνει επανεκκίνηση μόνος του και δεν λειτουργεί όπως συνήθως.
- Οι εφαρμογές στον υπολογιστή δεν λειτουργούν σωστά.
- Δεν είναι δυνατή η πρόσβαση στους δίσκους ή στις μονάδες δίσκου.
- Δεν είναι δυνατή η σωστή εκτύπωση.
- Βλέπετε ασυνήθιστα μηνύματα σφάλματος.
- Βλέπετε παραμορφωμένα μενού και παράθυρα διαλόγου.
- Υπάρχει διπλή επέκταση σε ένα συνημμένο που ανοίξατε πρόσφατα, όπως επέκταση .jpg, .vbs, .gif ή .exe.
- Ένα πρόγραμμα προστασίας από ιούς έχει απενεργοποιηθεί χωρίς λόγο. Επιπλέον, δεν είναι δυνατή η επανεκκίνηση του προγράμματος προστασίας από ιούς.
- Δεν μπορεί να εγκατασταθεί ένα πρόγραμμα προστασίας από ιούς στον υπολογιστή ή το πρόγραμμα προστασίας από ιούς δεν θα εκτελεστεί.
- Εμφανίζονται νέα εικονίδια στην επιφάνεια εργασίας, τα οποία δεν τοποθετήσατε εσείς εκεί ή τα εικονίδια δεν σχετίζονται με κανένα από τα προγράμματα που εγκαταστήσατε πρόσφατα.
- Παρατηρείται απροσδόκητη αναπαραγωγή περίεργων ήχων ή μουσικής από τα ηχεία.
- Κάποιο πρόγραμμα εξαφανίζεται από τον υπολογιστή, παρόλο που δεν το καταργήσατε σκόπιμα.

Όμως ποιοι είναι οι επικίνδυνοι για τον υπολογιστή τύποι αρχείων: (http://datalabs.edu.gr)

- File Viruses (Ιοί αρχείων): Πρόκειται για το πιο κοινό είδος ιού. Τα File Viruses κρύβονται στον κώδικα εκτελέσιμων αρχείων και ενεργοποιούνται όταν ο χρήστης ανοίξει κάποιο από αυτά. Κατά το άνοιγμα ενός μολυσμένου αρχείου, ο ιός εκτελείται πρώτος, ενώ στη συνέχεια ακολουθεί το κανονικό πρόγραμμα. Με αυτό τον τρόπο δεν γίνεται αντιληπτή στο χρήστη η ύπαρξη του ιού, αφού το πρόγραμμα φαίνεται να λειτουργεί κανονικά. Με αυτό τον τρόπο και αφού ο ιός έχει ενεργοποιηθεί, του δίνεται η δυνατότητα να αντιγράψει τον εαυτό του στη μνήμη του υπολογιστή, σε άλλα αρχεία του δίσκου, ή ακόμα να ξεκινήσει τη δράση του προκαλώντας παρενέργειες στο σύστημα. Τα File Viruses είναι μία από τις πιο διαδεδομένες μορφές ιών σήμερα, η εξάπλωση των οποίων ενισχύεται ακόμα περισσότερο από την ευκολία που προσφέρουν το Internet και το e-mail για τη μεταφορά αρχείων μεταξύ υπολογιστών.
- Trojan Horse (Δούρειος ίππος): Πρόκειται για μία από τις πιο επικίνδυνες μορφές ιών. Τα Trojan Horses έχουν πάρει την ονομασία τους από το μυθικό ξύλινο άλογο «Δούρειος Ίππος» που αναφέρει ο Όμηρος στην «Ιλιάδα». Τα Trojan Horses είναι πολύ πονηρά προγράμματα, καθώς ξεγελούν το χρήστη ο οποίος νομίζει πως το πρόγραμμα που εκτελούν κάνει κάτι άλλο, ενώ στην ουσία ανοίγει διόδους στον υπολογιστή ώστε να εισέλθουν άλλοι χρήστες. Έτσι, ο προγραμματιστής του ιού μπορεί να αποκτήσει τον

έλεγχο του μολυσμένου υπολογιστή ή να παρακολουθεί τις κινήσεις του χρήστη. Η δομή των Trojan Horses αποτελείται από δύο προγράμματα. Το ένα από αυτά τοποθετείται στον υπολογιστή του θύματος, μετατρέποντάς τον σαν ένα είδος server), ενώ το δεύτερο βρίσκεται στον υπολογιστή του επίδοξου εισβολέα (client). Έπειτα από την ενεργοποίηση του πρώτου προγράμματος από το χρήστη, ο εισβολέας χρησιμοποιεί το client πρόγραμμα για να εισβάλει στο σύστημα. Αν και τα περισσότερα Trojan Horses μπορούν να ανιχνευθούν και να εξοντωθούν με επιτυχία από τα προγράμματα Antivirus, ένα καλό firewall μπορεί να μας προσφέρει ακόμα μεγαλύτερη ασφάλεια από τους απρόσκλητους επισκέπτες.

- Worms (Ιοί Σκουλήκια): Τα γνωστά στους υπολογιστές «σκουλήκια» αποτελούν μια κατηγορία ιών, οι οποίοι έχουν σκοπό να αναπαραχθούν από μόνοι τους. Παρουσιάζουν πιο ανεξάρτητο χαρακτήρα από τους απλούς ιούς και δεν χρειάζεται να «κρυφτούν» σε κάποιο αρχείο για να μεταφερθούν από υπολογιστή σε υπολογιστή. Αντί όμως να μεταδίδονται από αρχείο σε αρχείο, προτιμούν να μεταπηδούν από υπολογιστή σε υπολογιστή. Το «σκουλήκι», από τη στιγμή που θα μολύνει έναν υπολογιστή, αναζητεί τρόπους (είτε μέσω e-mail χρησιμοποιώντας δηλαδή τις contact list του υπολογιστή είτε μέσω του Πρωτοκόλλου TCP/IP) να μεταβεί και σε άλλους υπολογιστές. Λόγω του ότι τα worms χρησιμοποιούν τις δικτυακές συνδέσεις για να εξαπλωθούν, μπορούν να έχουν υπερβολικά γρήγορη εξάπλωση και να δημιουργήσουν μεγάλη δικτυακή κίνηση.
- Virus Hoaxes (Ιός Απάτη): Εάν είστε χρήστης του Internet για κάποιο διάστημα, πιθανόν θα έχετε λάβει hoax virus warnings. Τα hoax virus warnings ξεκινούν από ένα άτομο με κακή πρόθεση (ή ως φάρσα) και κατόπιν διανέμονται σε πολλούς αθώους χρήστες υπολογιστών που λανθασμένα πιστεύουν ότι είναι πραγματικές προειδοποιήσεις και ότι βοηθούν άλλους ανθρώπους με το να διανέμουν αυτά τα μηνύματα. Οι περισσότερες hoax virus ειδοποιήσεις δίνουν οδηγίες στον παραλήπτη να προωθήσει την ειδοποίηση σε «όλους τους γνωστούς του» και γι' αυτόν τον λόγο εξαπλώνονται τόσο γρήγορα. Έχουν ως αποτέλεσμα να σπαταλάται ο χρόνος των χρηστών και μάλιστα ορισμένες hoax virus ειδοποιήσεις προτρέπουν τους χρήστες να σβήσουν αρχεία από τους υπολογιστές τους, για παράδειγμα αρχεία που δεν έχουν μολυνθεί από κάποιο ιό και μπορεί να είναι σημαντικότατα για τη σωστή λειτουργία του υπολογιστή. Σε μία τέτοια περίπτωση το καλύτερο που μπορούμε να κάνουμε είναι να αγνοήσουμε τέτοια μηνύματα.
- Spyware – Addware: Αν και από τη φύση τους δεν είναι πάντα «κακόβουλα», τα κατασκοπευτικά προγράμματα προκαλούν σημαντική βλάβη στα νόμιμα προγράμματα, στην απόδοση του δικτύου και στην παραγωγικότητα των εργαζομένων. Μία «παράπλευρη» συνέπεια της εισβολής των spyware στους υπολογιστές είναι η σώρευση παραπόνων των χρηστών στους διαχειριστές των δικτύων για αναδυόμενα παράθυρα (pop-ups), για δυσλειτουργία εφαρμογών και για χαμηλή απόδοση των υπολογιστών. Στη χειρότερη περίπτωση, η δυνατότητα των κατασκοπευτικών προγραμμάτων να καταγράφουν οτιδήποτε πληκτρολογούμε, να «σαρώνουν» τους σκληρούς δίσκους και να αλλάζουν τις ρυθμίσεις του συστήματος και του μητρώου των υπολογιστών, αποτελεί τεράστια απειλή προσωπικής και επιχειρησιακής ασφάλειας που επιτρέπει την κλοπή στοιχείων ταυτότητας, καταστροφή δεδομένων, ακόμα και κλοπή εμπορικών μυστικών μιας εταιρείας.
- Polymorphic virus (πολυμορφικός ιός): Οι ιοί αυτοί, στην προσπάθειά τους να μη γίνουν αντιληπτοί από τα προγράμματα antivirus, δημιουργούν πολλαπλά ενεργά αντίγραφα του εαυτού τους στο δίσκο ενός μολυσμένου υπολογιστή. Έτσι, είναι δυνατόν ο ίδιος ιός να εμφανίζεται με διαφορετικές μορφές σε διαφορετικά συστήματα ή ακόμα και σε διαφορετικά αρχεία που μολύνει. Οι πιο εξελιγμένοι ιοί του είδους χρησιμοποιούν ειδικές ρουτίνες μετάλλαξης και γεννήτριες τυχαίων αριθμών, ώστε να αλλάξουν τόσο τον κώδικά τους όσο και τον τρόπο κρυπτογράφησής τους.
- Stealth Virus (Αόρατος ιός): Αυτοί οι ιοί είναι ουσιαστικά αυτό που περιγράφει το όνομα τους. Δεν εντοπίζονται καθόλου εύκολα από τα anti-virus, καθώς κρύβονται από αυτά. Μόλις αντιληφθούν ότι ένα πρόγραμμα anti-virus ξεκίνησε το scanning, αποκαθιστούν

προσωρινά το αρχείο που είχαν μολύνει και μόλις τελειώσει το scanning το μολύνουν ξανά (tunneling).

Κάποιοι βασικοί τρόποι ώστε να προστατευτούμε από αυτά τα αρχεία είναι να μην ανοίγουμε επισυναπτόμενα αρχεία από διάφορα email των οποίων δεν γνωρίζουμε τον αποστολέα, να έχουμε στον υπολογιστή μας κάποια antivirus πρόγραμμα και να το ενημερώνουμε συχνά ώστε να έχει διαρκώς την πιο πρόσφατη έκδοση. Τέλος αρκετά σημαντικό είναι να ελέγχουμε συχνά τον υπολογιστή μας για τυχόν κακόβουλο υλικό και να δημιουργούμε τακτικά αντίγραφα ασφαλείας των δεδομένων μας, ώστε ακόμα και αν δεχθούμε «επίθεση» να μην χαθούν και τα δεδομένα μας.

2.7 Προστασία δεδομένων στις τηλεπικοινωνίες

Η τεχνολογική επανάσταση που συνέβη με την σύγκλιση της πληροφορικής και των τηλεπικοινωνιών είχε σαν συνέπεια μία τεράστια αύξηση των διαθέσιμων επικοινωνιακών υποδομών, αλλά και της ποσότητας των προσφερόμενων μέσω αυτών υπηρεσιών.

Παράλληλα η ραγδαία εξέλιξη της τεχνολογίας έδωσε έναυσμα στην ανάπτυξη νέων μορφών ηλεκτρονικής εγκληματικότητας και προσβολών του απορρήτου της επικοινωνίας και της ιδιωτικής ζωής. Για παράδειγμα η εισαγωγή της ψηφιακής τεχνολογίας στις τηλεπικοινωνίες αφενός επιτρέπει την παροχή επιπλέον διευκολύνσεων στους συνδρομητές, όπως κατάσταση αναλυτικής χρέωσης όπου αναγράφονται οι κληθέντες αριθμοί από τη συσκευή του συνδρομητή, η διάρκεια της κλήσης και η χρέωση αυτής.

Η νέα για εκείνη την εποχή, υπηρεσία ήταν επιθυμητή στο μέτρο που επιτρέπει σε μία επιχείρηση την καλύτερη διαχείριση του τηλεπικοινωνιακού κόστους, με τη δυνατότητα ελέγχου και διαχωρισμού των επαγγελματικών και προσωπικών κλήσεων των υπαλλήλων της, ενώ παράλληλα επιτρέπει την άρση πιθανών αμφισβητήσεων από τον πελάτη σχετικά με το ύψος των τελών τα οποία χρεώνονται από τον εκάστοτε τηλεπικοινωνιακό οργανισμό.

Ταυτόχρονα όμως η αναλυτική αποτύπωση όλων ή έστω των τεσσάρων πρώτων ψηφίων των αριθμών που καλούνται από μία συγκεκριμένη συσκευή, καθώς και η διατήρηση των σχετικών στοιχείων στα ηλεκτρονικά αρχεία τιμολόγησης συνδρομητών των τηλεπικοινωνιακών οργανισμών εμπεριέχει το ενδεχόμενο ελέγχου και προσβολής της ιδιωτικής ζωής καλούντων και καλουμένων με όλες τις συναφείς κοινωνικές και πολιτικές προεκτάσεις.

Παράλληλα, εκτός από τον κίνδυνο προσβολής της ιδιωτικής ζωής των ατόμων, η συλλογή δεδομένων προσωπικού χαρακτήρα τα οποία αφορούν τους συνδρομητές είναι δυνατόν να χρησιμοποιηθεί από τους τηλεπικοινωνιακούς παρόδους για καθαρά εμπορικούς σκοπούς ακόμα δε για την επίτευξη αθέμιτου ανταγωνιστικού πλεονεκτήματος σε σχέση με τους υπόλοιπους παρόχους. Για παράδειγμα η συλλογή των προτιμήσεων του καταναλωτικού κοινού στα πλαίσια μιας υπηρεσίας τηλεαγορών ή τηλεηχοπληροφόρησης είναι δυνατόν να μεταπωληθεί σε εταιρείες direct mail με στόχο την εξατομικευμένη προβολή και προώθηση καταναλωτικών προϊόντων.
Εξεταζόμενο σε μια ευρύτερη προοπτική, το πρόβλημα γίνεται ακόμα πιο σύνθετο στον εργασιακό χώρο όπου ειδικές συσκευές επιτρέπουν τον έλεγχο των επαγγελματικών και προσωπικών κλήσεων με στόχο με την θεμιτή μείωση των τηλ/κών δαπανών της επιχείρησης, αλλά με κίνδυνο της αθέμιτης προσβολής της προσωπικής και συνδικαλιστικής ελευθερίας, ιδιαίτερα σε περίπτωση μη εξουσιοδοτημένης πρόσβασης και εκμετάλλευσης των ανωτέρω αναλυτικών στοιχείων κλήσεων του προσωπικού από τον εργοδότη, το λογιστήριο της επιχείρησης, αλλά και από τυχόν τρίτους. Σχετικά με το ζήτημα αυτό, το οποίο αντιμετωπίστηκε στα πλαίσια άλλων έννομων τάξεων, όπως π.χ. στη Γαλλία, η ανεξάρτητη κανονιστική αρχή προστασίας των δεδομένων (CNIL, Commission Nationale Informatique et Libertes) έχει καθορίσει, με μια σειρά μέτρων, τις τεχνικές και κανονιστικές προδιαγραφές που πρέπει να τηρούνται από την France Telecom αλλά και από τους ανταγωνιστές της, για παρόμοιες επεξεργασίες, η παράβαση των οποίων επισείει αυστηρές κυρώσεις για την παραβάτισσα τηλ/κή επιχείρηση. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Πέρα από την συνταγματική διάσταση του, η οποία σχετίζεται με τη διασφάλιση του απορρήτου της επικοινωνίας και των ανταποκρίσεων (η οποία προστατεύεται από το άρθρο 19 του ελληνικού Συντάγματος σε συνδυασμό με το άρθρο 8 της Ευρωπαϊκής Σύμβασης

Δικαιωμάτων του Ανθρώπου και ορισμένες διατάξεις ποινικού κυρίως χαρακτήρα, όπως τα άρθρα 370 Β, Γ και Δ του Ποινικού Κώδικα περί πλαστογραφίας), το θέμα της ασφάλειας δεδομένων παρουσιάζει αναμφίβολα και μια σημαντικότατη οικονομική διάσταση. Αυτή αφορά όχι μόνο τους τηλ/κούς οργανισμούς, δημόσιους και ιδιωτικούς, αλλά και τους διαχειριστές των υποδομών, τους παρόχους υπηρεσιών και τους χρήστες. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Τα τελευταία χρόνια έχει εξελιχθεί σε πραγματική μάστιγα για τους τηλ/κούς οργανισμούς σε παγκόσμιο επίπεδο ή με τη βοήθεια εξειδικευμένου λογισμικού αθέμιτη πρόσβαση τρίτων σε μυστικούς κώδικες ή σειριακούς αριθμούς αναγνώρισης συνδρομητών τους (phone cloning). Η προσπέλαση στα απόρρητα ηλεκτρονικά αρχεία των παρόχων υπηρετών, έχει ως αποτέλεσμα την πραγματοποίηση υπεραστικών συνομιλιών ή τη χρήση τηλεματικών υπηρεσιών (π.χ. διασυνοριακή πρόσβαση σε τηλεπικοινωνιακά δίκτυα και τράπεζες πληροφοριών) με χρέωση του ανυποψίαστου νόμιμου συνδρομητή. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Η αντικειμενική υπόσταση του ανωτέρω εγκλήματος πραγματοποιείται ως εξής: ο αθέμιτος εισβολέας παρεισφρύει σε δίκτυο διαχείρισης πελατών ή στο σύστημα voice - mail του τηλ/κού οργανισμού ή της συν- δρομήτριας εταιρίας και με τη βοήθεια του υπολογιστή του πληκτρολογεί ασταμάτητα διαφορετικούς κώδικες πρόσβασης, μέχρι να ακούσει τον χαρακτηριστικό ήχο που επιτρέπει τις εξωτερικές κλήσεις. Από τούδε και στο εξής η προσπέλαση στις τηλεφωνικές γραμμές του συγκεκριμένου πελάτη είναι ελεύθερη και ο δράστης μπορεί να τηλεφωνεί σε οποιοδήποτε μέρος του κόσμου με έξοδα του νόνιμου δικαιούχου της σύνδεσης. Συχνά μάλιστα η δυνατότητα αθέμιτης πρόσβασης μεταπωλείται περαιτέρω σε ομάδες κακοποιών οι οποίοι πραγματοποιούν τις παράνομες συναλλαγές τους, καθιστώντας πολύ δυσχερή τον εντοπισμό τους, εφόσον διοχετεύουν τις κλήσεις τους (looping) μέσω περισσοτέρων εταιρικών PBXs (private branch exchanges). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Σύμφωνα με στοιχεία του αμερικάνικου περιοδικού "Fortune" οι 100 μεγαλύτερες εταιρίες των ΗΠΑ έχουν καταγγείλει τέτοια φαινόμενα τηλεπικοινωνιακής εγκληματικότητας (αναφερόμενα χαρακτηριστικά ως "PBXs crimes"), των οποίων το κόστος, μέχρι τον εντοπισμό της προσβολής μέσω ειδικού λογισμικού ελέγχου όγκου μηνυμάτων (volume detection software) ξεπέρασε κατά μέσο όρο τις 25.000 δολάρια ανά εταιρία, ποσό το οποίο αντιπροσωπεύει ένα συνολικό ετήσιο κόστος ανώτερο των 100 εκατομμυρίων δολαρίων. Εκτός όμως της άμεσης θετικής ζημίας, οι περιπτώσεις αυτές δίνουν συχνά λαβή και σε περαιτέρω δικαστικές διενέξεις μεταξύ τη- λεπικοινωνιακών οργανισμών και πελατών σχετικά με την ευθύνη που αναλογεί σε κάθε μέρος και τον συνακόλουθο επιμερισμό της ζημίας. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Παρόμοια φαινόμενα παρατηρούνται και στην κινητή τηλεφωνία με την πρόσβαση, χάρη σε ειδικές συσκευές ανάγνωσης, σε κωδικούς αριθμούς αναγνώρισης χρήστη (PIN) με την "σύλληψη" της κίνησης στα ραδιοκύματα και τη μεταγενέστερη χρήση τους, η οποία προσαρμόζεται με προσωπικούς υπολογιστές και ειδικό λογισμικό, σε κλεμμένα ψηφιακά τηλέφωνα, με τα ίδια τα το νόμιμο χρήστη ζημιογόνα αποτελέσματα. Στην ίδια κατηγορία ανήκει ακόμα η παγίδευση γραμμών επικοινωνίας (wiretapping) για εξ αποστάσεως αντιγραφή λογισμικού ηλεκτρονικών υπολογιστών ή για πρόσβαση σε τραπεζικούς λογαριασμούς τρίτων και πραγματοποίηση παράνομων συναλλαγών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Η επέκταση της μηχανοργάνωσης σε δημόσιο και ιδιωτικό τομέα σε συνδυασμό με την αύξηση του αριθμού των διαθέσιμων δικτύων μεταγωγής δεδομένων διευκολύνει τη δημιουργία και εμπορία ηλεκτρονικών αρχείων με "ευαίσθητες" πληροφορίες προσωπικού χαρακτήρα για τα άτομα και τις επιχειρήσεις (π.χ. οικονομική και φορολογική κατάσταση, φυλετική προέλευση, ιατρικά δεδομένα, πιστοληπτική ικανότητα κ.λπ.). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Η διασύνδεση κρατικών αρχείων (υπουργεία, εφορίες, τράπεζες, οργανισμοί κοινωνικής ασφάλισης, αστυνομία κ.λπ.) και η διασταύρωση προσωπικών δεδομένων συντελεί μεν στην πάταξη της γραφειοκρατίας και στον διοικητικό εκσυγχρονισμό, ενέχει όμως παράλληλα το

ενδεχόμενο καταχρήσεων σε βάρος του πολίτη. Τέτοιου είδους παραβάσεις έγιναν ήδη *και* σχεδιάζονται ακόμη περισσότερες και στη χώρα μας, χωρίς δυστυχώς να συναντήσουν ανάλογες αντιδράσεις από τους οικείους κοινωνικούς φορείς. Χαρακτηριστικά παραδείγματα αποτελούν η αυθαίρετη σύνδεση του ύψους των τηλεφωνικών λογαριασμών ελευθέρων επαγγελματιών με τη φορολογική ικανότητά τους, η υποχρεωτική χρήση σχεδιαζόμενης "ηλεκτρονικής ταυτότητας" σε κάθε μορφή συναλλαγής, η διασταύρωση των σχετικών στοιχείων ταυτότητας με τον αριθμό φορολογικού μητρώου από το σύστημα TAXIS με αντικείμενο τη μηχανοργάνωση των Οικονομικών Εφοριών κ.λπ. Στα πλαίσια αυτά λοιπόν, προβάλλει αδήριτη η ανάγκη θέσπισης ενός αποτελεσματικού συστήματος τεχνικών διασφαλίσεων, πρωτίστως, (κρυπτογράφηση δεδομένων, κωδικοποίηση, επίπεδα πρόσβασης ανά κατηγορία υπαλλήλου κ.λπ.), η οποία όμως να συνδυάζεται με τη θέσπιση καταλλήλων νομικών διατάξεων για την προστασία των πληροφοριών προσωπικού χαρακτήρα οι οποίες διακινούνται μέσω τηλ/κών δικτύων και υπηρεσιών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Συνειδητοποιώντας το πρόβλημα αυτό, πρώτοι οι Διεθνείς Οργανισμοί είχαν από νωρίς αναλάβει κάποιες νομοθετικές πρωτοβουλίες είτε υπό μορφή μη δεσμευτικών συστάσεων (Ο.Ο.Σ.Α) είτε υπό μορφή διεθνών συμβάσεων (όπως η Ευρωπαϊκή Σύμβαση αρ. 108 του Συμβουλίου της Ευρώπης "για τη προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα"). Η Σύμβαση αυτή υπογράφηκε το 1981 από όλα τα κράτη-μέλη του Συμβουλίου μεταξύ των οποίων και η Ελλάδα αποτελεί μέχρι στιγμής το σπουδαιότερο διεθνώς νομοθετικό κείμενο περί προστασίας δεδομένων, πρόσφατα δε κυρώθηκε και από τη χώρα μας με το νόμο 2068/1992 (ΦΕΚ 118, 9 Ιουλίου 1992) και έτσι κατέστη εσωτερικό μας δίκαιο. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Περιεχόμενο της Σύμβασης αποτελεί η οριοθέτηση ενός μηχανισμού προστασίας του ατόμου από αυτοματοποιημένες επεξεργασίες προσωπικών πληροφοριών. Ειδικότερα, στο κείμενο της γίνεται, πρώτον, η αποσαφήνιση ορισμένων βασικών όρων όπως "προσωπική πληροφορία", "ηλεκτρονικό αρχείο", "κύριος του αρχείου", "αυτοματοποιημένη επεξεργασία", κ.λπ. Η οριοθέτηση του πεδίου εφαρμογής της ακολουθείται, δεύτερον, από τη θέσπιση ορισμένων αρχών και διαδικασιών προστασίας και ασφάλειας των πληροφοριών (νόμιμη απόκτηση, καταχώρηση για ορισμένους νόμιμους και ειδικά οριζόμενους σκοπούς, ακρίβεια, προσήκουσα και όχι υπέρμετρη έκταση σε σχέση με επιδιωκόμενους σκοπούς, περιορισμένη χρονική διάρκεια διατήρησης). Το σύστημα προστασίας συμπληρώνεται, τρίτον, από την εισαγωγή ορισμένων νέων δικαιωμάτων του ατόμου (δικαίωμα γνώσης των αυτοματοποιημένων επεξεργασιών που το αφορούν μέσω της υποχρέωσης των φορέων επεξεργασίας, δημόσιων και ιδιωτικών, να δημοσιοποιούν το είδος και το περιεχόμενο των κάθε είδους αρχείων που τηρούν, δικαίωμα άρνησης του ατόμου να συναινέσει στη σχεδιαζόμενη επεξεργασία, δικαίωμα πρόσβασης στα χειροκίνητα ή αυτοματοποιημένα αρχεία δημόσιων και ιδιωτικών φορέων, δικαίωμα διόρθωσης τυχόν ανακριβειών ή σφαλμάτων κ.λπ.). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Για την διασφάλιση εφαρμογής των όρων της Σύμβασης και την διενέργεια των προβλεπόμενων ελέγχων οι οποίοι μπορούν να φθάσουν μέχρι την επιβολή, με τη συνδρομή της δικαστικής αρχής, των αναλόγων κυρώσεων και προστίμων κατά των παραβατών, προβλέπεται επίσης η δημιουργία εκ μέρους των κρατών, με την εθνική νομοθεσία, ανεξάρτητων δημόσιων αρχών προστασίας των ατόμων. Οι αρχές αυτές μπορεί να είναι κατά περίπτωση, συλλογικές (όπως π.χ. η προαναφερθείσα γαλλική CNIL - Εθνική Επιτροπή Πληροφορικής και Ελευθεριών, ή η σουηδική Datainspektion) ή μονοπρόσωπες (όπως π.χ. ο Επίτροπος για την προστασία των δεδομένων - Datenshutzbeauftagter - στη Γερμανία), έχουν δε ως αποκλειστική αρμοδιότητα την προστασία των ατόμων από τις ενδεχόμενες παρενέργειες, οι οποίες απορρέουν από καταχρήσεις της νέας τεχνολογίας. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Εκτός από το Συμβούλιο της Ευρώπης σημαντική δραστηριότητα ανέπτυξε στο χώρο αυτό και η Ευρωπαϊκή Ένωση με στόχο να ενθαρρύνει την ελεύθερη ροή πληροφοριών στο εσωτερικό του Ενιαίου Ευρωπαϊκού χώρου με παράλληλη θεσμική και κανονιστική διασφάλιση της προστασίας

της ιδιωτικής σφαίρας του ατόμου. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Στην προοπτική λοιπόν της απελευθέρωσης της αγοράς τηλ/κών υπηρεσιών, το Συμβούλιο δημοσίευσε, εκτός από μια σειρά συστάσεων, δυο προτάσεις Οδηγίας περί προστασίας δεδομένων και ιδιωτικής ζωής. Η πρώτη αναφέρεται στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (COM (90) 314 SYN 287/27-7- 1990). Η δεύτερη τροποποιημένη πρόταση περί προστασίας φυσικών προσώπων έναντι επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ελεύθερης κυκλοφορίας αυτών εκδόθηκε το 1992 (COM (92) 422 - SYN 287 της 27ης Νοεμβρίου 1992, C 311/30). Εκτός όμως από τις γενικές ρυθμίσεις, τα ευρωπαϊκά όργανα ανέλαβαν συγκεκριμένες πρωτοβουλίες για την αντιμετώπιση του εξόχως πρακτικού θέματος της προστασίας προσωπικών δεδομένων στις τηλεπικοινωνίες. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Προς αυτή την κατεύθυνση εκδόθηκε Πρόταση Οδηγίας του Συμβουλίου (ΕΕΚ 1990 C277/12) η οποία αφορά στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής σε δημόσια ψηφιακά δίκτυα τηλ/νιών, καθώς και σε ψηφιακά δίκτυα ενοποιημένων υπηρεσιών (ISDN) (ΕΕΚ 1990 C 277/12). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Βάσει της πρότασης αυτής, η οποία πρόκειται άμεσα να υιοθετηθεί από την Ευρωπαϊκή - Ένωση, οι τηλεπικοινωνιακοί οργανισμοί, ανεξάρτητα από το εάν έχουν εισαγάγει ή όχι υπηρεσίες ISDN, εφόσον το κείμενο εφαρμόζεται και στα αναλογικά δίκτυα (άρθρο 2), θα υπέχουν ορισμένες σημαντικές υποχρεώσεις κατά την ανάπτυξη και προσφορά στο κοινό των νέων υπηρεσιών: μεταξύ αυτών περιλαμβάνεται, εκτός της υποχρέωσης εμπιστευτικότητας και νόμιμης συλλογής και διατήρησης στοιχείων για σκοπούς τιμολόγησης και διαχείρισης πελατολογίου, και η απαγόρευση δημιουργίας "ηλεκτρονικών προφίλ" των συνδρομητών (άρθρο 4). Μετά τη λήξη της σύμβασης οργανισμού-χρήστη τα δεδομένα πρέπει να καταστρέφονται, μετά την περίοδο ορισμένης προθεσμίας αμφισβήτησης των χρεώσεων εκ μέρους των χρηστών (άρθρο 5). Περαιτέρω κοινοποίηση προς τρίτους των στοιχείων αυτών απαιτεί έγγραφη συναίνεση υποκειμένου των επεξεργασιών (άρθρο 7). Οι τηλ/κοί οργανισμοί υποχρεούνται να παρέχουν προς τους πελάτες τους σύγχρονες υπηρεσίες τεχνικές κρυπτογράφησης των δεδομένων και να τους πληροφορούν για ενδεχόμενες προσβολές του δικτύου (άρθρα 15, 16). Παράλληλα, προβλέπονται συγκεκριμένα μέτρα προστασίας του χρήστη από ανεπιθύμητες κλήσεις καθώς και το δικαίωμα του καλούντος να παραμένει ανώνυμος με το να μην απεικονίζεται ο αριθμός στη συσκευή του αποδέκτη της κλήσης. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Η Ευρωπαϊκή πολιτική ανοίγματος των δημόσιων δικτύων στον ανταγωνισμό οφείλει επίσης να γίνεται υπό τον όρο συμμόρφωσης των παροχών υπηρεσιών προς τις "βασικές απαιτήσεις", λόγους δημόσιου συμφέροντος περιοριστικούς της πρόσβασης μεταξύ των οποίων περιλαμβάνεται, εκτός από την ασφάλεια λειτουργίας, την διασφάλιση της ακεραιότητας του δικτύου, την διαλειτουργικότητα των υπηρεσιών, και η προστασία δεδομένων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Ενδεικτικό της σημασίας που αποδίδει η Ευρωπαϊκή Επιτροπή και το Συμβούλιο στο θέμα της προστασίας δεδομένων, αποτελεί το γεγονός ότι η παράμετρος αυτή περιλαμβάνεται τόσο στην Οδηγία-Πλαίσιο για την παροχή ανοικτού δικτύου στις μισθωμένες γραμμές, στη φωνητική τηλεφωνία, στα ψηφιακά δίκτυα ενοποιημένων υπηρεσιών (ISDN), στις κινητές υπηρεσίες κ.λπ. Παρόμοιο είναι το πνεύμα της απόφασης του Συμβουλίου περί ασφαλείας πληροφοριακών συστημάτων (ΕΕΚ 1992 L 123/19, 31-3-1992), καθώς και της -Έκθεσης του Ευρωπαϊκού Ινστιτούτου Τηλεπικοινωνιακών Προτύπων (ETSI Report DTR/NA-70401). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Εικόνα 9 Νομικά θέματα στις τηλεπικοινωνίες

Ύστερα από αρκετές δεκαετίες καθυστέρησης ψηφίστηκε και στην Ελλάδα ο νόμος 2225/1994 (ΦΕΚ 121 Α', 20.7.1994) "για την προστασία της ελευθερίας ανταπόκρισης και επικοινωνίας και άλλες διατάξεις". Με το νόμο αυτό προβλέπεται η δημιουργία και στην Ελλάδα μιας αρχής προστασίας του απορρήτου των επικοινωνιών, αλλά με πολύ πιο περιορισμένες αρμοδιότητες από τις αντίστοιχες ευρωπαϊκές. Στον ανωτέρω νόμο πρόκειται για την "Εθνική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών" (άρθρο 1). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Με το νέο Νόμο, το ζήτημα του απορρήτου των ανταποκρίσεων τίθεται στη θεσμική του διάσταση, υπό την οπτική δηλαδή όχι μόνο της εξισορρόπησης των δύο αντίρροπων συνταγματικών αξιώσεων, του σεβασμού ενός βασικού ατομικού δικαιώματος και της προστασίας της ίδιας της υπόστασης του κράτους, αλλά και της διαδικασίας άρσης του απορρήτου για λόγους εθνικής ασφάλειας (άρθρο 3), για διακρίβωση εγκλημάτων (άρθρο 4) κ.λπ. Καθιερώνονται αφενός πρόσθετες εγγυήσεις για την προστασία του απορρήτου με την ίδρυση ανεξάρτητης Εθνική Επιτροπής και συγκεκριμενοποιείται αφετέρου, τόσο η δικαστική αρχή που μπορεί να διατάξει την άρση του απορρήτου όσο και η διαδικασία που διέπει την άρση αυτή. Ειδικότερα, με το νόμο 2225/1994: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

α) Ιδρύεται "Εθνική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών" (ΕΕΠΑΕ), ως ανεξάρτητη δημόσια αρχή με αποστολή την προστασία του απορρήτου των επιστολών, της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης ή επικοινωνίας καθώς και τον έλεγχο της τήρησης των όρων της άρσης του απορρήτου που έθεσε η δικαστική αρχή.

β) Η ΕΕΠΑΕ συγκροτείται από ένα Σύμβουλο Επικρατείας ή ένα πρώην ανώτατο δικαστικό λειτουργό, ως πρόεδρο, από ένα βουλευτή -εκπρόσωπο κάθε κόμματος, και από μια προσωπικότητα εγνωσμένου κύρους και με ειδικές γνώσεις σε θέματα επικοινωνιών. Η θητεία των μελών, εκτός του προέδρου της, διαρκεί όσο και η βουλευτική περίοδος, στη διάρκεια της οποίας ορίσθηκαν (άρθρο 1).

Η ΕΕΠΑΕ έχει ευρύ φάσμα αρμοδιοτήτων, ως εξής: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

α) Επιθεωρεί χωρίς προειδοποίηση τις σχετικές με το έργο της εγκαταστάσεις, αρχεία και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, του Οργανισμού Τηλεπικοινωνιών Ελλάδας και άλλων δημόσιων επιχειρήσεων που βρίσκονται υπό τον άμεσο ή έμμεσο έλεγχο του Δημοσίου, καθώς και ιδιωτικών επιχειρήσεων που προσφέρουν υπηρεσίες σχετικές με ανταπόκριση ή επικοινωνία, όπως οι επιχειρήσεις κινητής τηλεφωνίας ή οι τράπεζες δεδομένων (άρθρο 2).

β) Ζητεί από τις υπηρεσίες και τις επιχειρήσεις του προηγουμένου εδαφίου, καθώς και από του προϊσταμένου ή εποπτεύοντες Υπουργούς, κάθε πληροφορία χρήσιμη κατά τη κρίση της για την επιτέλεση της αποστολής της (άρθρο 2).

γ) Καλεί σε ακρόαση, με απόφασή της, τον Διοικητή ή τους Υποδιοικητές της ΕΥΠ, τον Πρόεδρο ή τον γενικό διευθυντή του ΟΤΕ, καθώς και κάθε πρόσωπο, το οποίο μπορεί να συμβάλλει στην εκπλήρωση του έργου της (άρθρο 2).

δ) Εφόσον οι παρεχόμενες κατά το προηγούμενο εδάφιο πληροφορίες και εξηγήσεις δεν κριθούν επαρκείς ή ικανοποιητικές, ερευνά αρχεία εγγράφων αναφερόμενων στο προστατευόμενο απόρρητο.

ε) Προβαίνει σε διοικητικές εξετάσεις και σε κατάσχεση των μέσων παραβίασης του απορρήτου που υποπίπτουν στην αντίληψή της, κατ' ανάλογη εφαρμογή των σχετικών άρθρων του Κώδικα Ποινικής Δικονομίας.

Από τα προεκτεθέντα, προκύπτει εναργώς ότι το πρόβλημα της προστασίας του απορρήτου και της ιδιωτικής ζωής, συνδεόμενο παραδοσιακά με το απόρρητο των επιστολών, απομακρύνεται ολοένα και περισσότερο από τις ιστορικές του καταβολές και συνδέεται στενά με τις τεχνολογικές εξελίξεις στο χώρο των τηλεπικοινωνιών.

Η προστασία προσωπικών δεδομένων είναι ένα πολυεπίπεδο και πολυσύνθετο πρόβλημα που τίθεται, όπως αναλύθηκε εκτενώς παραπάνω, όχι μόνο στις σχέσεις κράτους-πολίτη, αλλά και μεταξύ επιχειρήσεων που δραστηριοποιούνται στο χώρο της επικοινωνίας αλλά και μεταξύ παρόχων και χρηστών των παρεχομένων τηλ/κών υπηρεσιών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Ισορροπώντας στο μεταίχμιο πολλών αντίρροπων μεταξύ τους συμφερόντων, όπως η οικονομική πρόοδος, η ανάγκη ελεύθερης ροής της πληροφόρησης, η ανάγκη επιβίωσης των υπηρεσιών του επικοινωνιακού κλάδου υπό καθεστώς ελεύθερης αγοράς, η ανάγκη λήψης συγκεκριμένων μέτρων προστασίας των δεδομένων προβάλλει ως μια επιτακτική ανάγκη, ιδιαίτερα στην παρούσα οικονομικοπολιτική συγκυρία. Χωρίς η προστασία δεδομένων να χρησιμοποιείται ως πρόσχημα αποκλεισμού τρίτων σε πρόσβαση σε υπηρεσίες οι οποίες τελούν υπό καθεστώς ειδικών ή αποκλειστικών δικαιωμάτων, όπως π.χ. ο ΟΤΕ τη φωνητική τηλεφωνία, θα πρέπει οι προεκτεθείσες τεχνικές και κανονιστικές διασφαλίσεις να αποτελέσουν αναπόσπαστο όρο ανάπτυξης νέων υπηρεσιών σε μια ανοιχτή και ανταγωνιστική αγορά. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

Ενόψει των ανωτέρω, αδήριτη προβάλλει η ανάγκη θέσπισης και στην Ελλάδα, κατ' εφαρμογή σχετικών Διεθνών Συνθηκών αλλά και του παραγώγου κοινοτικού δικαίου, ενός ολοκληρωμένου πλέγματος τεχνικών και κανονιστικών διασφαλίσεων περί προστασίας δεδομένων στις τηλεπικοινωνίες, τα οποία μπορούν να συνοψισθούν ως ακολούθως: (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β.. Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, 1995)

- Άμεση εισαγωγή γενικής και τομεακής νομοθεσίας περί προστασίας δεδομένων, κατ' εφαρμογή των σχετικών Διεθνών και Ευρωπαϊκών κειμένων.
- Άμεση θέσπιση συνοπτικών διαδικασιών και ευέλικτων οργάνων ελέγχου, ουσιαστική λειτουργία της νεοσύστατης Επιτροπής Προστασίας του Απορρήτου των Επικοινωνιών.
- Ενσωμάτωση των τεχνικών και κανονιστικών απαιτήσεων προστασίας των προσωπικών δεδομένων στην ανάπτυξη νέων υπηρεσιών.
- Θέσπιση ενός ειδικού πλέγματος κυρώσεων για τους παραβάτες των "ουσιωδών απαιτήσεων" (ασφάλεια λειτουργίας και διατήρηση ακεραιότητας δικτύου, διαλειτουργικότητα υπηρεσιών, προστασία δεδομένων).
- Σύσταση ενός Νομικού Παρατηρητηρίου (Legal Observatory) συμβουλευτικού χαρακτήρα, με τη συμμετοχή εκπροσώπων όλων των συναρμοδίων φορέων (Κυβέρνηση, ΟΤΕ, εταιρίας κινητής τηλεφωνίας, λοιπές τηλ/κές επιχειρήσεις, πάροχοι υπηρεσιών, χρήστες) με δυνατότητες παρέμβασης και εκπροσώπησης της Ελλάδας στην ανταγωνιστική ευρωπαϊκή αγορά τηλ/κών υποδομών και υπηρεσιών.

ΚΕΦΑΛΑΙΟ 3^{ο} ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

3.1 Γενικά

Οι χρήστες ενός ασύρματου δικτύου μπορούν να επωφεληθούν από ένα σωρό πλεονεκτήματα όμως σε αυτή την περίπτωση τίθεται ένα πολύ σημαντικό ερώτημα, πόσο ασφαλής είναι η επικοινωνία σε ένα σύστημα όπου το μέσο μετάδοσης της πληροφορίας είναι ο αέρας; Επίσης η ευρεία χρήση του διαδικτύου για την διακίνηση προσωπικών πληροφοριών αναδεικνύει ακόμα πιο πολύ το θέμα της ασφάλειας των δικτύων. Κάποια λύση προσπαθεί να δοθεί με τις μεθόδους πιστοποίησης και κρυπτογράφησης των δεδομένων που χρησιμοποιούνται ευρέως σήμερα. Σε ένα ενσύρματο τοπικό δίκτυο οι απειλές αντιμετωπίζονται στο σημείο εξόδου προς τον ISP με πολιτικές ασφάλειας στους δρομολογητές, με firewall κτλ. Όμως σε ένα ασύρματο δίκτυο όλα τα παραπάνω δεν ισχύουν.

3.1.1 Επικύρωση και μυστικότητα

Ουσιαστικά με τον όρο επικύρωση αναφερόμαστε στον έλεγχο πρόσβασης. Για να πραγματοποιήσουμε την επικύρωση πρέπει να αρχικά να αποκτήσουμε έλεγχο πρόσβασης στο μέσο και συγκεκριμένα στο ασύρματο δίκτυο. Αρχικά ελέγχονται τα διαθέσιμα ασύρματα δίκτυα και έπειτα το δίκτυο επικυρώνει το σταθμό και ο σταθμός επικυρώνει το δίκτυο. Τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται beacons - πλαίσια διαχείρισης. (Μαρκομανωλάκη Α., 2010)

Τα beacons ανακοινώνουν την ύπαρξη ενός δικτύου. Το κάθε beacon περιλαμβάνει ένα όνομα δικτύου ή αλλιώς Service Set Identifier (SSID). Ένας σταθμός μπορεί να επιλέξει να συνδεθεί σε ένα δίκτυο είτε παθητικά είτε ενεργητικά. Στην περίπτωση της παθητικής σάρωσης ο σταθμός ελέγχει τα κανάλια προσπαθώντας να βρει beacons από τα σημεία πρόσβασης και στην δεύτερη περίπτωση στέλνει αιτήσεις διερεύνησης (είτε σε ένα συγκεκριμένο SSID, είτε με το SSID ρυθμισμένο στο 0), σε όλα τα κανάλια ένα προς ένα. Όλοι οι σταθμοί πρόσβασης που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση, στη συνέχεια ο σταθμός να διαλέξει το δίκτυο που θέλει να συνδεθεί με βάση την ισχύ του σήματος ή σε άλλα κριτήρια. (Μαρκομανωλάκη Α., 2010)

Στο πρότυπο 802.11 υπάρχουν δύο τρόποι επικύρωσης, η επικύρωση ανοιχτού κλειδιού (Open System Authentication – OSA) και η ΚΑΤΑεπικύρωση μοιρασμένου κλειδιού (Shared Key Authentication – SKA). Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στην αίτηση επικύρωσης και το δίκτυο ανάλογα μπορεί να δεχτεί ή να απορρίψει αυτή την πρόταση ανάλογα με τις ρυθμίσεις ασφαλείας. (Μαρκομανωλάκη Α., 2010)

Όταν γίνεται επικύρωση ανοιχτού κλειδιού οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης αλλά όχι να επικοινωνήσει. Η συσκευή μπορεί να επικοινωνεί μόνο αν τα WEP (Wired Equivalent Privacy) κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης. Η επικύρωση μοιρασμένου κλειδιού βασίζεται στο σύστημα πρόσκλησης-απάντησης. Για να γίνει χρήση αυτής της μεθόδου επικύρωσης, απαιτείται το σημείο πρόσβασης και ο σταθμός να είναι συμβατοί με τη λειτουργία WEP και υπάρχει μεταξύ τους ένα κλειδί. Αυτό σημαίνει ότι ένα κοινό κλειδί πρέπει να μοιραστεί σε όλους τους σταθμούς που τους έχει επιτραπεί να έχουν πρόσβαση στο δίκτυο, πριν επιχειρήσουν την διαδικασία της επικύρωσης. (Μαρκομανωλάκη Α., 2010)

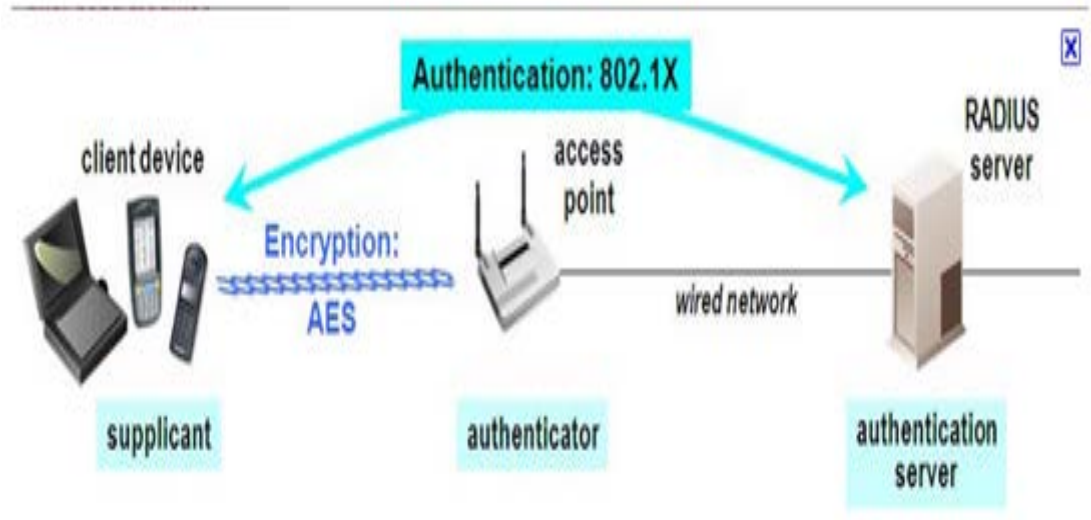
3.2 Κρυπτογράφηση WEP

Με τον όρο Κρυπτογράφηση ονομάζουμε την διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή ώστε να μεταδοθούν με ασφάλεια πληροφορίες (encryption, συμβολίζεται με E). Πριν από την κρυπτογράφηση τα δεδομένα ονομάζονται plaintext (συμβολίζεται με P) και μετά την κρυπτογράφηση αποτελούν το cipher text (συμβολίζεται με C), ενώ η αντίστροφη διαδικασία ονομάζεται αποκρυπτογράφηση (decryption). Ο αλγόριθμος κρυπτογράφησης ή cipher είναι μία μαθηματική ακολουθία που χρησιμοποιείται για την μεταμφίεση και αποκάλυψη των δεδομένων. Συνήθως οι αλγόριθμοι κρυπτογράφησης περιέχουν ακολουθίες κλειδιών για να τροποποιήσουν τα εξαγόμενα τους. (Peikari C. & Fogie S., 2002)

Στα ασύρματα δίκτυα ή πιο γνωστή τεχνική ασφαλείας είναι από το αρχικό πρότυπο 802.11 το Wired Equivalent Privacy (WEP). Με την επιλογή του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν επιθυμούμε εμπιστευτικότητα, μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν. Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία αλλά και την ακεραιότητα των δεδομένων. Με τη βοήθεια ενός συμμετρικού αλγόριθμου κρυπτογράφησης, επιτυγχάνεται η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω του δικτύου. (Peikari C. & Fogie S., 2002)

3.2.1 Επαλήθευση ταυτότητας

Μια κινητή συσκευή προκειμένου να συνδεθεί σε ένα ασύρματο δίκτυο μέσω ενός σημείου πρόσβασης, πρέπει να αποδείξει την ταυτότητας της. Στην επαλήθευση ταυτότητας WEP, η συσκευή πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει το μυστικό κλειδί της κρυπτογράφησης. Στην αρχή πρέπει να «υποβληθεί» αίτηση επαλήθευσης ταυτότητας από την κινητή συσκευή προς το σημείο πρόσβασης. Με τη σειρά του το σημείο πρόσβασης στέλνει ένα τυχαίο αριθμό μήκους 128 bit προς κρυπτογράφηση στην ασύρματη συσκευή, όπου κρυπτογραφείται από τη συσκευή με το μυστικό κλειδί WEP και αποστέλλεται πίσω. Τέλος το σημείο πρόσβασης ελέγχει εάν η κρυπτογράφηση έγινε με το σωστό κλειδί. Αυτή η μέθοδος αποτελεί πολύ μεγάλο πρόβλημα για την ασφάλεια της κρυπτογράφησης καθώς δίνει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης αλλά και της μη κρυπτογραφημένης πληροφορίας. (Peikari C. & Fogie S., 2002)



Εικόνα 10 επαλήθευση ταυτότητας

3.2.2 Κατακερματισμός

Σε ένα ασύρματο δίκτυο, το πακέτο δεδομένων που φθάνει περιέχει τις κατάλληλες πληροφορίες για την αποστολή του και ονομάζεται MSDU (Mac Service Data Unit). Τα δεδομένα φθάνουν στο επίπεδο MAC του προορισμού και σκοπός είναι να περάσουν στο λειτουργικό σύστημα ώστε να μετατεθούν στην κατάλληλη εφαρμογή. Παρόλα αυτά, πριν από αυτή τη διαδικασία τα δεδομένα πρέπει να χωριστούν σε μικρότερα κομμάτια, δηλαδή να υποστούν τη διαδικασία του θρυμματισμού (fragmentation). Ακολούθως κάθε κομμάτι ακολουθεί τη δική του πορεία στην κρυπτογράφηση WEP. Επομένως το αρχικό πακέτο δεδομένων χωρίζεται σε μικρότερα μηνύματα, MPDU στα οποία προστίθενται και άλλα bytes. (Peikari C. & Fogie S., 2002)

3.2.3 Διάνυσμα Αρχικοποίησης

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στην κρυπτογράφηση WEP έχουν μήκος 40 ή 104 bits, ωστόσο συχνά μπορεί να έχουν και μεγαλύτερο όπως 68 ή 128 bits. Αυτό συμβαίνει επειδή κάποιοι παραλείπουν να αναφέρουν τα επιπλέον 24 bits που χρησιμοποιούνται από το διάνυσμα αρχικοποίησης (Initialization Vector - IV). Αυτό το διάνυσμα ουσιαστικά αλλάζει για κάθε πακέτο και συνδυάζεται με το μυστικό κλειδί και έπειτα το αποτέλεσμα αυτών κρυπτογραφείται. Έτσι ακόμα και εάν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική. Το IV δεν είναι μυστικό, στέλνεται σε μη κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV. (Peikari C. & Fogie S., 2002)

Τα κλειδιά που χρησιμοποιούνται στο WEP έχουν τα ακόλουθα χαρακτηριστικά:

- Σταθερό μήκος: Συνήθως 40 ή 104 bit.
- Στατικά: Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.
- Διαμοιραζόμενα (shared): Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
- Συμμετρικά: Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών. Σύμφωνα με το πρότυπο IEEE 802.11, η διάθεση των κλειδιών στα σημεία πρόσβασης και στις ασύρματες συσκευές πρέπει να γίνεται με ασφαλείς μεθόδους ανεξάρτητες του πρωτοκόλλου.

Η επαναχρησιμοποίηση των κλειδιών είναι μια αδυναμία των κρυπτογραφικών πρωτοκόλλων, γι' αυτό το WEP, έχει μια δεύτερη κατηγορία κλειδιών που χρησιμοποιούνται για τα ζευγάρια επικοινωνιών. Αυτά τα κλειδιά μοιράζονται μόνο μεταξύ των δύο σταθμών επικοινωνίας, οι δύο σταθμοί μοιράζονται ένα κλειδί και έχουν έτσι μια σχέση χαρτογράφησης κλειδιού. (Peikari C. & Fogie S., 2002)

Οι πιο κοινές εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά RC4 64 bit. Οι περισσότεροι κατασκευαστές χρησιμοποιούν ένα 128-bit δημόσιο RC4 κλειδί. Το πρότυπο 64-bit WEP χρησιμοποιεί ένα κλειδί 40 bit, το οποίο συνδέεται με την αρχή ενός 24- bit διανύσματος και διαμορφώνει το RC4 κλειδί κυκλοφορίας. Την εποχή που συντασσόταν τα αρχικά πρότυπα WEP, η κυβέρνηση των Η.Π.Α εξέδιδε περιορισμούς στην κρυπτογραφική τεχνολογία για το μέγεθος του κλειδιού. Μόλις εγκαταλείφτηκαν οι περιορισμοί όλοι οι βασικοί κατασκευαστές εφάρμοσαν τελικά το 128- bit WEP πρωτόκολλο χρησιμοποιώντας μέγεθος κλειδιού 104 bit. Ένα 128- bit WEP κλειδί σχεδόν πάντα εισάγεται από τους χρήστες σαν μια ακολουθία 26 δεκαδικών (βάση το 16) χαρακτήρων (0-9 και AF). Κάθε χαρακτήρας αντιπροσωπεύει 4 bit του κλειδιού. 26 ψηφία τεσσάρων bit δίνουν 104 bit και η προσθήκη του 24 bit IV παράγει το τελικό 128- bit κλειδί WEP. Ένα 256-bit σύστημα WEP είναι διαθέσιμο από μερικούς προμηθευτές, και όπως με το 128-bit WEP, τα 24 bit είναι για το IV, αφήνοντας 232 πραγματικά bit για την προστασία. Αυτά τα 232 bit εισάγονται χαρακτηριστικά ως 58 δεκαδικοί χαρακτήρες. (58 × 4 = 232 μπιτ) + 24 IV μπιτ = 256-bit κλειδί WEP. (Peikari C. & Fogie S., 2002)

3.2.4 Διανομή κλειδιού

Το μεγαλύτερο μειονέκτημα του WEP είναι το πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Όμως το 802.11 πρότυπο, δεν παρέχει μηχανισμό παραγωγής κλειδιού επομένως ο καθένας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή να έχει πρόσβαση σε συσκευές με το χέρι. Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι: (Peikari C. & Fogie S., 2002)

- Τα κλειδιά δεν είναι ουσιαστικά μυστικά, αφού εισάγονται στους οδηγούς software ή firmware στην ασύρματη κάρτα. Συνεπώς ένας τοπικός χρήστης μπορεί να έχει πρόσβαση στο «μυστικό» κλειδί.
- Εάν τα κλειδιά είναι προσιτά στους χρήστες, αυτά θα πρέπει να αλλάζουν συχνά. Η γνώση κλειδιών WEP επιτρέπει σε έναν χρήστη να φτιάξει έναν 802.11 σταθμό και να ελέγχει παθητικά και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί.
- Οι επιχειρήσεις με μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύσουν το κλειδί στους πληθυσμούς χρηστών επομένως δεν μιλάμε πια για «μυστικότητα» του κλειδιού.

3.2.5 Τιμή Ελέγχου Ακεραιότητας

Η τιμή ελέγχου ακεραιότητας (Integrity Check Value - ICV) συνεισφέρει στην αποφυγή τροποποίησης του μηνύματος κατά τη μετάδοση. Στα κρυπτογραφημένα και μη μηνύματα, συνήθως γίνεται έλεγχος για την αλλαγή των bits κατά τη μετάδοση. Το σύνολο των Bytes του μηνύματος συνενώνονται στον έλεγχο κυκλικού πλεονασμού (Cyclic Redudancy Check - CRC) και αυτή η τιμή αυτή, μήκους τεσσάρων bytes, προστίθεται στο τέλος του πλαισίου πριν από την επεξεργασία για μετάδοση. Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης υπολογίζει διαφορετική τιμή CRC από αυτή που στέλνει ο πομπός, επομένως θα απορρίψει το μήνυμα. (Peikari C. & Fogie S., 2002)

3.2.6 Κρυπτογράφηση

Η διαδικασία που ακολουθείται περιγράφεται στη συνέχεια: (Peikari C. & Fogie S., 2002)

1. Το μυστικό κλειδί συνδέεται με το διάνυσμα έναρξης και το αποτέλεσμα τους εισάγεται στον αλγόριθμο RC4.
2. Ο αλγόριθμος RC4 παράγει μια ακολουθία κλειδιού keystream από «ψευδοτυχαία» bits ίσα στο μήκος με τον αριθμό bits δεδομένων που πρέπει να διαβιβαστούν προσθέτοντας 4.
3. Για προστασία από αναρμόδια τροποποίηση δεδομένων, εφαρμόζεται ο αλγόριθμος ακεραιότητας πάνω στα δεδομένα και παράγεται το ICV.
4. Η κρυπτογράφηση ολοκληρώνεται με τη λογική πράξη του αποκλειστικού Η (XOR) μεταξύ της ακολουθίας κλειδιού και των δεδομένων που μετατράπηκαν σε ICV. Το προϊόν της διαδικασίας είναι ένα μήνυμα που περιέχει το IV και το κρυπτογράφημα.

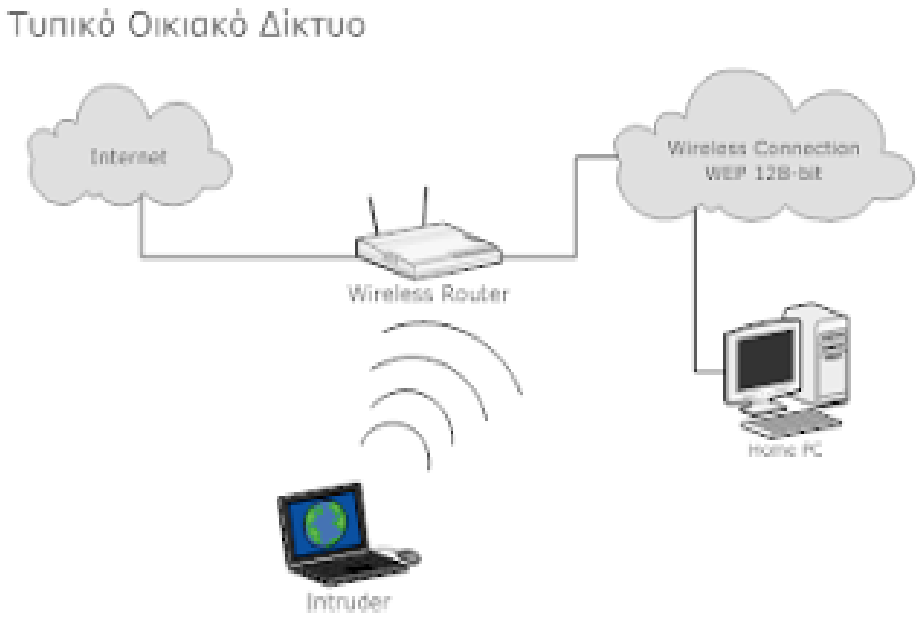
Ο πιο σημαντικός αλγόριθμος WEP κρυπτογράφησης είναι ο αλγόριθμος RC4 ο οποίος μεταμορφώνει ένα σύντομο μυστικό κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού. Αυτή η μέθοδος κάνει απλή τη διαδικασία διανομής κλειδιού, αφού το μόνο που θα πρέπει να μεταδοθεί μεταξύ των σταθμών είναι το μυστικό κλειδί. Το διάνυσμα αρχικοποίησης επεκτείνει την διάρκεια ζωής του μυστικού κλειδιού. Στη μέθοδος WEP λοιπόν το μόνο που αλλάζει ανά συχνά διαστήματα είναι το διάνυσμα αρχικοποίησης ενώ το μυστικό κλειδί παραμένει πάντα ίδιο. Κάθε νέο IV καταλήγει σε μια νέα ακολουθία κλειδιού. (Peikari C. & Fogie S., 2002)

Για την αποκρυπτογράφηση πρέπει το διάνυσμα αρχικοποίησης να αποσταλεί μαζί με το κρυπτογραφημένο πακέτο. Όταν ο παραλήπτης αποκρυπτογραφήσει το πακέτο υπολογίζει ξανά την τιμή ελέγχου ακεραιότητας και τη συγκρίνει με αυτή που περιείχε το πακέτο που παρέλαβε. Αν οι δύο τιμές ταυτίζονται, τότε θεωρείται ότι το πακέτο είναι έγκυρο. Ο αλγόριθμος RC4 είναι πολύ σημαντικός παράγοντας για την αποδοτικότητα του WEP, όσον αφορά την εμπιστευτικότητα των δεδομένων, αφού αυτός είναι στην ουσία η μηχανή κρυπτογράφησης. Θα πρέπει να τονίσουμε

ότι το μυστικό κλειδί είναι στατικό, οπότε το IV είναι αυτό που καθορίζει κάθε φορά την ψευδοτυχαία ακολουθία. Επομένως, ο αλγόριθμος RC4 εξαρτάται μόνο από το IV. (Peikari C. & Fogie S., 2002)

3.2.7 Εύρεση WEP κλειδιού

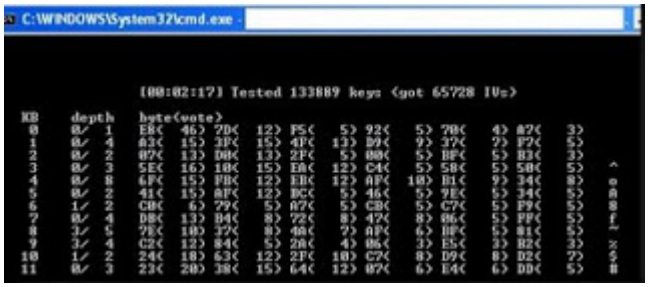
Ωστόσο το μέγεθος του κλειδιού, δεν είναι το μόνο μειονέκτημα ασφάλειας σε WEP. Η καλύτερη δημόσια επίθεση ενάντια στο WEP μπορεί να ανακτήσει το κλειδί σε μερικά δευτερόλεπτα. Πρακτικά για την ανεύρεση ενός κλειδιού WEP δεν χρειάζονται ιδιαίτερα πράγματα, αφού πλέον υπάρχει αρκετό διαθέσιμο λογισμικό, το οποίο είναι προσανατολισμένο σε αυτό τον σκοπό. Επίσης δεν ισχύει πια η άποψη ότι το λογισμικό αυτό υπάρχει μόνο σε Linux και προϋποθέτει γνώσεις προγραμματισμού και πληκτρολόγηση σε γραμμή εντολών κτλ. Όλα αυτά τα προγράμματα υπάρχουν και σε εκδόσεις για Windows και έχουν πλέον ακόμη και παραθυρικό περιβάλλον. (Βιολέττας Γ. 2008)



Εικόνα 11 τυπικό οικιακό δίκτυο

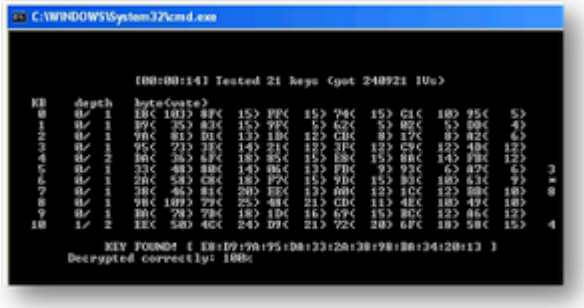
Στην παραπάνω εικόνα φαίνεται ένα τυπικό οικιακό δίκτυο, στο οποίο θεωρούμε ότι χρησιμοποιείται WEP κλειδί των 128-bit. Με την χρήση πολύ απλών εργαλείων, είναι δυνατή η εξαγωγή αυτού του κλειδιού. Η λογική της ανεύρεσης ενός τέτοιου κλειδιού έχει βασικά δύο σκέλη. Στο πρώτο σκέλος καταγράφουμε όλα τα πακέτα που μας ενδιαφέρουν από έναν τέτοιο σταθμό. Στο δεύτερο σκέλος το πρόγραμμα αναλαμβάνει να εξάγει το κλειδί από τους πίνακες αρχικοποίησης που έχουν αποθηκευθεί σε ένα αρχείο από το προηγούμενο πρόγραμμα. Ελέγχονται δηλαδή οι ήδη αποθηκευμένοι πίνακες αρχικοποίησης (IV) για το υπό αναζήτηση

κλειδί. (Βιολέττας Γ. 2008)



Εικόνα 12 αναζήτηση κλειδιού

Όπως φαίνεται στην Εικόνα 7, ένα πλήθος από 240.921 πίνακες αρχικοποίησης (IVs) ήταν αρκετοί για να βρεθεί το 128-bit WEP κλειδί του δικτύου μέσα σε δευτερόλεπτα. Εδώ να σημειώσουμε ότι το υπό «έρευνα» δίκτυο ήταν ένα δίκτυο της τοπολογίας της Εικόνας 6, δηλαδή ένα δίκτυο ενός μοναδικού πελάτη-υπολογιστή άρα θεωρητικά με πολύ περιορισμένη κίνηση. Παρόλα αυτά, ο χρόνος που χρειάστηκε για να συγκεντρωθεί το αναγκαίο πλήθος δεδομένων (οι αναγκαίοι πίνακες δηλαδή), δεν υπερέβη τα 10 λεπτά της ώρας. (Βιολέττας Γ. 2008)



Εικόνα 13 επιτυχής εύρεση κλειδιού

3.2.8 Προβλήματα του WEP

Το WEP έχει αρκετά προβλήματα μερικά από τα οποία είναι τα παρακάτω: (Flickenger, 2003)

- Όταν κάποιος αποχωρεί από το σύστημα, θα πρέπει τα κλειδιά να αλλάζουν. Για να είναι επιτυχημένη μία επίθεση χρειάζεται μόνο τα μυστικά κλειδιά, τα οποία αλλάζουν σπάνια. Αυτή η μέθοδος, όπως αναφέρθηκε, χρησιμοποιεί συνήθως ένα δημόσιο μυστικό κλειδί με μικρό μήκος.
- Η νέα εισαγωγή κλειδιών, είναι σπάνια, κάτι το οποίο επιτρέπει στους επιτιθεμένους να αποκτήσουν αποθέματα κρυπτογραφημένων δεδομένων δηλαδή μεγάλες συλλογές των πλαισίων που κρυπτογραφούνται με τα ίδια κλειδιά.
- Προβληματική είναι και η διαδικασία της επαλήθευσης ταυτότητας, η οποία στηρίζεται στη μέθοδο πρόσκλησης – απόκρισης. Αρχικά στέλνεται μια τυχαία ακολουθία bits, η οποία κρυπτογραφείται και αποστέλλεται πίσω και τέλος το σημείο πρόσβασης την αποκρυπτογραφεί και τη συγκρίνει με την αρχική ακολουθία. Το κλειδί που χρησιμοποιείται σε αυτή τη διαδικασία είναι το ίδιο με αυτό της κρυπτογράφησης, δίνοντας έτσι την ευκαιρία σε έναν επιτιθέμενο να ανακτήσει στοιχεία. Η όλη διαδικασία δίνει γενικότερα την ευκαιρία σε έναν εισβολέα να επιτεθεί στα κλειδιά κρυπτογράφησης.
- Ο έλεγχος πρόσβασης συνίσταται στην απαγόρευση ή όχι της επικοινωνίας μια συσκευής με το δίκτυο. Η πρόσβαση συνήθως ελέγχεται διατηρώντας μια λίστα με επιτρεπόμενες συσκευές ή με κάποιο ηλεκτρονικό πιστοποιητικό. Στο IEEE 802.11 δεν έχουμε κάποιο συγκεκριμένο μηχανισμό υλοποίησης πρόσβασης.

- Ένα άλλο τρωτό σημείο του WEP είναι η αδυναμία του να διαχειριστεί επιθέσεις μέσω αναπαραγωγής μηνυμάτων. Όταν ένας επιτιθέμενος παρακολουθεί και καταγράφει τα πλαίσια που ανταλλάσσονται σε μια νόμιμη επικοινωνία, μπορεί ακολούθως να συνδεθεί στο δίκτυο με τη MAC διεύθυνση της κινητής συσκευής. Στέλνοντας έτσι ένα αντίγραφο ενός παλιού μηνύματος μπορεί να αποκτήσει πρόσβαση στον εξυπηρετητή. Η προστασία από τέτοιου είδους επιθέσεις στο WEP δεν είναι απλά ελλιπής αλλά ανύπαρκτη.
- Η τιμή του διανύσματος αρχικοποίησης, όπως προαναφέραμε, δεν είναι μυστική, όμως κάτι τέτοιο δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα σχετικά αδύναμο κλειδί. Τα πρώτα bytes ενός μη κρυπτογραφημένου μηνύματος είναι συνήθως γνωστά διότι αποτελούν μια επικεφαλίδα IEEE 802.11. Με παρακολούθηση της μετάδοσης αναζητείται ένα αδύναμο κλειδί. Ξέρουμε επίσης ότι υπάρχει σχέση ανάμεσα στο κρυπτογραφημένο και στο μη κρυπτογραφημένο μήνυμα και το μυστικό κλειδί. Έχοντας καταγράψει έναν σημαντικό αριθμό από τέτοια μηνύματα, ο εισβολέας μπορεί να ανακαλύψει το πρώτο byte του κλειδιού. Η μέθοδος αυτή μπορεί να εφαρμοστεί για κάθε byte και τελικά να αποκαλυφθεί το μυστικό κλειδί. Θα πρέπει να πούμε επίσης ότι η αύξηση του μήκους του κλειδιού δεν επιφέρει εκθετική αύξηση του χρόνου αναζήτησης αλλά απλά γραμμική.

3.3 Πέρα από το WEP

Αρχικά το IEEE 802.11 για τα ασύρματα δίκτυα, υποστήριζε μόνο το WEP ως μέθοδο για την ασφάλεια της πληροφορίας που ανταλλάσσονται σε ένα δίκτυο. Αρκετοί ωστόσο ήταν αυτοί που διαπίστωσαν τις αδυναμίες του συστήματος WEP, συνεπώς εμφανίστηκαν στο διαδίκτυο εργαλεία που παραβίαζαν το WEP και μάλιστα σε σύντομο χρονικό διάστημα. Παρόλα αυτά το WEP αποτελεί μέχρι και σήμερα για αρκετούς οικιακούς χρήστες, τη μοναδική επιλογή για την προστασία των δεδομένων που ανταλλάσσουν μέσω ενός ασύρματου δικτύου. (Barmen L., 2003)

Λόγω του κενού ασφαλείας που άφηνε το WEP, αναδύθηκε η λύση του TKIP (Temporal Key Integrity Protocol – TKIP), το οποίο προσφέρει μεγαλύτερη ασφάλεια καθώς παρέχει ανάμιξη κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος και μηχανισμό αναπαραγωγής κλειδιών, ο οποίος επιδιορθώνει τα ελαττώματα του WEP. Το μόνο που απαιτούσε ήταν η αναβάθμιση του Aware και πιθανώς του λογισμικού της συσκευής. Αρχικά το TKIP χρησιμοποιήθηκε πάνω στο WEP για να ενισχύσει την ασφάλεια και να μειώσει τον αριθμό των επιθέσεων του WEP. Σε αυτή την κρυπτογράφηση το πρώτο βήμα είναι ο υπολογισμός του κώδικα ακεραιότητας δεδομένων MIC, που γίνεται με τον αλγόριθμο Bahl. (Barmen L., 2003)

Η TKIP κρυπτογράφηση λειτουργεί σε δύο φάσεις. Η πρώτη φάση χρησιμοποιεί ένα μη γραμμικό πίνακα αντικατάστασης (S-Box) και συνδυάζει το κλειδί συνόδου (TK), τη MAC διεύθυνση του αποστολέα (TA) και τα τέσσερα πιο σημαντικά bytes της τιμής του μετρητή ακολουθίας, (TKIP Sequence Counter), οποίος αυξάνει για κάθε τμήμα δεδομένων που τεμαχίζονται. Το κλειδί συνόδου αποτελείται από μια τιμή 128 bit, παρόμοια με την τιμή του WEP κλειδιού. Ο TKIP μετρητής ακολουθίας (TSC) είναι φτιαγμένος από την πηγαία διεύθυνση (SA), την διεύθυνση προορισμού (DA), την ιεραρχία και τα δεδομένα. (Barken L., 2003)

Στην έξοδο παράγεται μία ενδιάμεση τιμή (TTAK), η οποία μπορεί να αποθηκευτεί προσωρινά και να χρησιμοποιηθεί μέχρι και για 216 πακέτα. Λαμβάνεται υπόψη η διεύθυνση του αποστολέα, η συνάρτηση παράγει διαφορετική ενδιάμεση τιμή για κάθε συσκευή, ακόμα και αν χρησιμοποιείται το ίδιο κλειδί κρυπτογράφησης από όλες τις συσκευές. (Barken L., 2003)

Η δεύτερη φάση συγχωνεύει την τιμή TTAK με τα δύο λιγότερο σημαντικά bytes της τιμής του μετρητή ακολουθίας (TSC) και το κλειδί συνόδου (TK) για την εξαγωγή του τελικού κλειδιού κρυπτογράφησης. Τέλος κατά τα γνωστά από το WEP, υπολογίζεται το IV και γίνεται η κρυπτογράφηση από τον αλγόριθμο RC4. Το TKIP χρησιμοποιεί την 802.1X αρχιτεκτονική επικύρωσης, σαν βάση για την ασφαλή ανταλλαγή του κλειδιού. (Barken L., 2003)

Τα αμέσως επόμενα χρόνια η Wi-Fi Alliance όρισε ένα υποσύνολο του νέου προτύπου, το οποίο αποτελεί μια βελτιωμένη έκδοση ασφάλειας που ενδυναμώνει το επίπεδο προστασίας δεδομένων και ελέγχου πρόσβασης σε ασύρματο δίκτυο. Το υποσύνολο αυτό ονομάζεται Wi-Fi Protected Access (WPA). (Barken L., 2003)

3.4 WPA (WI-FI PROTECTED ACCESS)

Όταν έγινε γνωστό στο ευρύ κοινό το κενό ασφαλείας που άφηνε η κρυπτογράφηση WEP, η Wi-Fi Alliance ανέπτυξε το Wi-Fi Protected Access (WPA), το οποίο προέρχεται από το IEEE 802.11 πρότυπο και αποτελεί μια ενδιάμεση λύση ασφάλειας των WLAN και μπορεί να συμπεριληφθεί με αναβαθμίσεις στις ήδη υπάρχουσες WLAN ασύρματες συσκευές. Το WPA κάνει χρήση της μεθόδου TKIP, που προαναφέρθηκε και αυτό είναι ο λόγος που αυξάνεται σημαντικά το επίπεδο ασφάλειας και ελέγχου πρόσβασης στα ασύρματα συστήματα LAN. (Μαρκομανωλάκη Α., 2010)

Με αυτή την μέθοδο σε κάθε πακέτο παρέχεται το κλειδί, ένας έλεγχος ακεραιότητας μηνύματος και ένα διάνυσμα ακολουθίας. Όσον αφορά τους οικιακούς χρήστες, το WPA παρέχει ένα μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre-Shared Key). Για να χρησιμοποιήσει κάποιος την PSK θα πρέπει να εισάγει μια λέξη κωδικό και στο σημείο πρόσβασης και στο σταθμό, ώστε η λέξη αυτή να αποτελεί τον κωδικό για την επικύρωση οποιοδήποτε σταθμού προσπαθεί να συνδεθεί στο συγκεκριμένο δίκτυο. Ο κωδικός καλό είναι να έχει από 8 έως 63 εκτυπώσιμους χαρακτήρες σε ASCII. Στη συνέχεια παρέχεται από το σημείο πρόσβασης στο σταθμό, ένα προσωρινό κλειδί, το οποίο όμως ανανεώνεται σε τακτά χρονικά διαστήματα. Το 256 bit κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κωδικό ως κλειδί. (Μαρκομανωλάκη Α., 2010)

Το προμοιρασμένο WPA κλειδί είναι τρωτό στις επιθέσεις πρόσβασης εάν χρησιμοποιείται ένας αδύνατος κωδικός και θεωρείται αρκετός ένας πραγματικά τυχαίος κωδικός 13 χαρακτήρων. Τα προϊόντα που γράφουν ότι έχουν "WPA-Personal" σημαίνει ότι υποστηρίζουν τον PSK μηχανισμό επικύρωσης. Το πρότυπο WPA ορίζει επίσης τη χρήση του προτύπου AES (Advanced Encryption Standard) ως επιπλέον αντικατάσταση για την κρυπτογράφηση WEP. Η υποστήριξη προτύπου AES είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο προμηθευτής όσον αφορά προγράμματα οδήγησης. (Μαρκομανωλάκη Α., 2010)

3.4.1 Επίθεση σε δίκτυο WPA

Το WPA είναι απαλλαγμένο από τα μειονεκτήματα του WEP. Όμοια με το WEP, έτσι και στο WPA, χρειάζεται να εισαχθεί από τον χρήστη μία αρχική λέξη-κλειδί, αυτή η λέξη δεν χρησιμοποιείται ποτέ στην αποστολή των κωδικοποιημένων πακέτων. Αντίθετα η λέξη αυτή συνδυάζεται με την MAC Address του κάθε σταθμού-πελάτη και με έναν πίνακα αρχικοποίησης μήκους 48-bit για να πράξει το κλειδί με το οποίο κωδικοποιούνται τα δεδομένα. Επομένως το κωδικό κλειδί στα εκπεμπόμενα πακέτα είναι διαφορετικό ανά συσκευή. Έτσι επειδή το κλειδί κάθε πακέτου είναι διαφορετικό, δεν μπορεί να υπάρξει επίθεση brute force, μία επίθεση δηλαδή που να συγκρίνει στατιστικά τα διάφορα πακέτα προσπαθώντας να βρει ομοιότητες μεταξύ τους, και ως εκ τούτου να βρει το συνθηματικό εισόδου στο δίκτυο. (Βιολέττας Γ. 2008)

Δυστυχώς όμως και το WPA έχει το αδύνατο σημείο του. Αυτό το σημείο είναι το πακέτο που εκπέμπεται όταν ένας σταθμός ζητάει να συνδεθεί με τον σταθμό βάσης (handshake). Το πακέτο με το οποίο θα ζητάει να συνδεθεί ένας σταθμός, θα περιέχει οπωσδήποτε και την μυστική λέξη-κλειδί, που έχει οριστεί ως συνθηματικό ταυτοποίησης και εισόδου στο δίκτυο. Η μέθοδος που ακολουθείται στο WPA έχει ως εξής: Οποιοσδήποτε σταθμός «ακούει» την συναλλαγή των δύο μερών, μπορεί να συλλέξει τα απαραίτητα δεδομένα – πακέτα. Τα πακέτα αυτά μπορούν να χρησιμοποιηθούν για να ελεγχθούν διεξοδικά από υπάρχουσες εφαρμογές που εκτελούν επιθέσεις λεξικού (dictionary attacks). Σχεδόν όλοι οι δυνατοί συνδυασμοί λέξεων 8 χαρακτήρων εμπεριέχονται σε τέτοια λεξικά. Αποδεικνύεται ότι λέξεις μήκους μικρότερου από 20 χαρακτήρες, είναι στατιστικά αδύνατον να αντέξουν σε τέτοιου είδους επίθεση. Αυτού του είδους οι επιθέσεις μάλιστα, θεωρείται πολύ ευκολότερο να υλοποιηθούν από τις επιθέσεις στο WEP. (Βιολέττας Γ. 2008)

Στο WPA δεν έχουμε την δυνατότητα να επιτεθούμε χρησιμοποιώντας brute force μεθόδους, η μέθοδος την οποία επιλέγουμε είναι η επίθεση λεξικού. Μπορούμε λοιπόν να στέλνουμε στον ασύρματο σταθμό συνδυασμούς συμβόλων (γραμμάτων, αριθμών κτλ) προσπαθώντας ουσιαστικά να μαντέψουμε το σωστό μυστικό κλειδί με το οποίο ένα τέτοιο σύστημα θα μας δεχόταν ως «νόμιμο» χρήστη αν το γνωρίζαμε. Γίνεται εύκολα αντιληπτό ότι μία «επίθεση» τέτοιας μορφής χρειάζεται μία μηχανή παραγωγής εκατομμυρίων συνδυασμών ή εναλλακτικά ένα είδος λεξικού που να περιέχει όλους αυτούς τους συνδυασμούς. Ένα από τα αρχικά προβλήματα που έχει να λύσει αυτό το είδος της επίθεσης, είναι ότι βασίζεται στην «σύλληψη» ενός πολύ συγκεκριμένου πακέτου (ή πακέτων). Αφού «συλληφθεί» το (κρυπτογραφημένο) πακέτο «χειραψίας» που περιέχει το μυστικό κλειδί WPA, γίνονται εξαντλητικές δοκιμές διάφορων λέξεων-κλειδιών πάνω του, χωρίς να χρειάζεται η υπόλοιπη ακολουθία σύνδεσης σταθμού στο δίκτυο. (Βιολέττας Γ. 2008)

Για να «συλλάβει» το πακέτο αυτό, ο υποψήφιος εισβολέας έχει δύο επιλογές:

- Είτε να περιμένει πότε κάποιος καινούριος σταθμός θα συνδεθεί επιτυχημένα στο δίκτυο, με την συνεπακόλουθη χρονική αναμονή,
- Είτε να «εξωθήσει» τον ήδη συνδεδεμένο σταθμό-πελάτη σε αποσύνδεση, ώστε αναγκαστικά αυτός να προσπαθήσει να επανασυνδεθεί, οδηγώντας έτσι το εισβολέα, στην «σύλληψη» του πακέτου που τον ενδιαφέρει.

Η χρήση μίας απλής συνηθισμένης λέξης ως μυστικής λέξης-κλειδιού, σε ένα δίκτυο WPA, το κάνει αρκετά ευάλωτο. Όσο πιο συνηθισμένη είναι αυτή η λέξη, τόσο αυξάνονται οι πιθανότητες να υπάρχει σε τουλάχιστον ένα, από τα αρκετά ενημερωμένα και εκτενή «λεξικά» που χρειάζονται για αυτήν την δουλειά, και κυκλοφορούν ευρέως στο διαδίκτυο. Αντιθέτως η χρήση ως λέξης-κλειδιού μίας λέξης που δεν υπάρχει σε λεξικό, δυσχεραίνει πάρα πολύ τον επίδοξο εισβολέα. Αν μάλιστα η όποια λέξη συνδυαστεί με κάποια σημεία στίξης και με κάποια από τα γράμματα της κεφαλαία, τότε καθιστά πρακτικά αδύνατη την ανεύρεση της. (Βιολέττας Γ. 2008)

3.5 AES (ADVANCED ENCRYPTION STANDARD)

Το WPA, που παρέχει μεγαλύτερη ασφάλεια στα ασύρματα δίκτυα, παρέχει τη δυνατότητα για κρυπτογράφηση με δυο αλγόριθμους, τον RC4 και τον AES (Advanced Encryption Standard) για την εμπιστευτικότητα των δεδομένων και την ακεραιότητα. Ο αλγόριθμος AES έχει επιλεγεί από την κυβέρνηση των ΗΠΑ και αποτελεί την νεότερη μέθοδος κρυπτογράφησης. Ο AES χρησιμοποιεί ένα αλγόριθμο με το όνομα Rijndael, ο οποίος πήρε το όνομα του από δυο Ελβετούς εφευρέτες και είναι ένας αλγόριθμος κρυπτογράφησης ομάδας (block), που σημαίνει ότι λειτουργεί σε μια ομάδα σταθερού μεγέθους bits, η οποία ονομάζεται μπλοκ. (Barken L., 2003)

Αυτός ο αλγόριθμος δέχεται ένα μπλοκ συγκεκριμένου μεγέθους, σαν είσοδο και παράγει ένα αντίστοιχο μπλοκ εξόδου του ίδιου μεγέθους. Ο μετασχηματισμός απαιτεί μια δεύτερη είσοδο, η οποία είναι το μυστικό κλειδί. Το μυστικό κλειδί δεν έχει συγκεκριμένο μέγεθος και ο AES χρησιμοποιεί τρία βασικά μεγέθη: 128, 192 και 256 bytes. Πλέον μπορούμε να βρούμε προϊόντα AES WRAP(Wireless Robust Authentication Protocol), αλλά η τελική προδιαγραφή καθορίζει τον αλγόριθμο AES CCMP (Counter Mode-Cipher Block Chaining Mac Protocol). Οι προδιαγραφές του 802.11i παρέχουν επίπεδο μετάδοσης δεδομένων βασισμένο στο AES. Η χρήση του πρότυπου AES μας προστατεύει από τις ενεργές ασύρματες επιθέσεις, αλλά πρέπει να αναγνωριστεί ότι ένα ασύρματο πρωτόκολλο του επιπέδου μετάδοσης δεδομένων μπορεί να προστατεύσει μόνο το ασύρματο υπό-δίκτυο. Στα σημεία που η κίνηση διέρχεται από άλλα τμήματα του δικτύου, είτε σε δίκτυα τοπικής ή ευρείας περιοχής, απαιτείται προστασία υψηλού επιπέδου και κρυπτογράφηση από σημείο σε σημείο. (Barken L., 2003)

3.6 WPA2 (WI-FI PROTECTED ACCESS VERSION 2)

Το WPA2 είναι ο διάδοχος του WPA και στοχεύει να θέσει σε απευθείας σύνδεση το WPA με το IEEE 802.11i πρότυπο. Το WPA2 διαθέτει συμβατότητα προς τα πίσω με το WPA, όπως και με την κρυπτογράφηση TKIP και AES, την 802.1X / EAP επικύρωση και την τεχνολογία PSK, που είναι όλα μέρη του προτύπου. Τα ασύρματα δίκτυα που υποστηρίζουν την μικτή λειτουργία WPA

και WPA2 κάνουν πιο εύκολη την μεταφορά των δεδομένων ανάμεσα στα πρότυπα. Το WPA2 βελτιώθηκε όταν προστέθηκε το AES CCMP, όπως στο 802.11i, το οποίο δίνει τη δυνατότητα ισχυρής κρυπτογράφησης. (http://en.wikipedia.org)

Μια άλλη βελτίωση του WPA2 είναι η δυνατότητα για γρήγορη περιαγωγή, η οποία είναι σημαντική για τις εφαρμογές ήχου, όπου η μεταφορά τους είναι υψηλής ευαισθησίας. Η γρήγορη περιαγωγή επιτυγχάνεται με την επικύρωση των σταθμών και στα γειτονικά σημεία πρόσβασης αλλά και στο τελικό σημείο πρόσβασης όπου επιτυγχάνεται η επικοινωνία. Όταν ένας σταθμός θέλει να συνδεθεί σε ένα γειτονικό σημείο πρόσβασης, η επικύρωση 802.11X μπορεί να παραληφθεί αφού έχει ήδη ολοκληρωθεί εκ των πρότερων. Επιπλέον το προσωρινό κλειδί έχει ήδη εγκαθιδρυθεί ανάμεσα στο σταθμό και το σημείο πρόσβασης, έτσι αποκτώντας πρόσβαση στον εξυπηρετητή για να ολοκληρώσει την επικύρωση, καταλαμβάνει πολύ χρόνο. Έχει παρατηρηθεί ότι τα δίκτυα που περιλαμβάνουν γρήγορη περιαγωγή έχουν ομαλότερη λειτουργία και συνεχή συνδεσιμότητα του πελάτη καθώς αυτός μετακινείται στις κυψέλες του WLAN. Υπάρχουν δύο εκδόσεις του WPA2. Το WPA2-Personal και το WPA2- Enterprise. Το WPA2-Personal προστατεύει την πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες με τη χρήση της εγκατάστασης ενός κωδικού πρόσβασης. Το WPA2- Enterprise πιστοποιεί τους χρήστες του δικτύου μέσω ενός εξυπηρετητή. (http://en.wikipedia.org)

3.7 ROBUST SECURE NETWORK (RSN)

Το πρότυπο IEEE 802.11i ορίζει ένα νέο τύπο ασύρματου δικτύου, το οποίο ονομάζεται Δίκτυο Ανθεκτικής Ασφάλειας (Robust Secure Network - RSN). Οπωσδήποτε οι ασύρματες συσκευές που θα υποστηρίζουν ένα τέτοιο δίκτυο θα πρέπει να έχουν νέες δυνατότητες. Αυτές είναι η επικύρωση, η διαχείριση κλειδιών σε υψηλό επίπεδο, η κρυπτογράφηση και την επικύρωση των δεδομένων που διακινούνται σε MAC επίπεδο. Ένα δίκτυο RSN έχει πολύ αυστηρούς περιορισμούς όσον αφορά την προσβασιμότητα και επιβάλλονται αρκετοί περιορισμοί ασφάλειας. Ωστόσο, επειδή χρειάζεται χρόνος για να αναβαθμιστούν οι συσκευές και ο εξοπλισμός, το πρότυπο IEEE 802.11i ορίζει το Δίκτυο Μεταβατικής Ασφάλειας (Transitional Security Network - TSN). Τα δίκτυα TSN υποστηρίζουν δίκτυα όπως το RSN αλλά και το WEP. Οι χρήστες που εισέρχονται σε ένα δίκτυο TSN, μπορούν να λειτουργήσουν παράλληλα για όλα τα προηγούμενα συστήματα ασφάλειας. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

3.8 Διαφορές RSN και WPA

Τόσο το RSN αλλά και το WPA είναι μέθοδοι κρυπτογράφησης οι οποίες αντιμετωπίζουν το θέμα της ασφάλειας με παρόμοιο τρόπο. Το WPA διαθέτει μερικές μόνο από τις δυνατότητες του RSN. Όμως το RSN κάνει χρήση του πρωτοκόλλου CCMP, υποχρεωτικά, με εναλλακτική λύση το TKIP, ενώ το WPA επικεντρώνεται στο TKIP. Αυτές οι τεχνικές χρησιμοποιούν παρόμοια αρχιτεκτονική με πρωτόκολλα ασφάλειας που βασίζονται στους αλγόριθμους AES και RC4 αντίστοιχα. Μέσω αυτών των μεθόδων καλύπτονται θέματα όπως:

α) Επικύρωση σε υψηλό επίπεδο,
β) Διανομή του κλειδιού κρυπτογράφησης
γ) Ανανέωση του κλειδιού.

Η αρχιτεκτονική του WEP είναι πιο απλή σε σχέση με αυτή του RSN. Για αυτό το RSN είναι μια πολύ σημαντική λύση, η οποία μπορεί να εφαρμοστεί σε μεγάλα δίκτυα. Ένα από τα μεγαλύτερα προβλήματα του WEP είναι η δυσκολία της διανομής των κλειδιών, όταν οι χρήστες ξεπεράσουν τις μερικές δεκάδες. Το πρόβλημα αυτό επιλύεται τόσο στο RSN αλλά και στο WPA. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

3.9 Τύποι επιθέσεων σε ασύρματα δίκτυα

Οι προθέσεις και οι στόχοι κάθε επίθεσης μπορεί να διαφέρουν και γενικά οι επιθέσεις σε ασύρματα δίκτυα μπορούν να χωριστούν σε παθητικές και ενεργητικές. Ως παθητικές ορίζονται οι επιθέσεις που δε συμπεριλαμβάνουν συμμετοχή του επιτιθέμενου στο δίκτυο και τέτοιου τύπου επίθεση αποτελεί η Λήψη Πληροφοριών (Snooping/Footprinting). Οι ενεργητικές επιθέσεις προϋποθέτουν ότι ο επιτιθέμενος αναλαμβάνει ενεργή συμμετοχή στο δίκτυο και χωρίζονται, σύμφωνα με το σκοπό που έχουν οι επιτιθέμενοι, σε τέσσερις βασικές κατηγορίες: (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

- Ανάκτηση κωδικού WEP (WEP Cracking)
- Τροποποίηση Δεδομένων (Man in the Middle Attack)
- Μεταμφίεση (Spoofing)
- Άρνηση Υπηρεσιών (Denial of Service)

3.9.1 Παθητικές επιθέσεις

Η λήψη πληροφοριών (snooping) σχετίζεται με την ανάκτηση απόρρητων προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες. Σε αυτή την περίπτωση για να αντιμετωπισθούν τυχόν επιθέσεις, επιβάλλεται μία ασφαλής μέθοδος κρυπτογράφησης. Ο επιτιθέμενος μπορεί να διαβάσει όλες τις πληροφορίες που προέρχονται από τα σημεία πρόσβασης, επομένως ξέρει το όνομα δικτύου (ή SSID) και είναι πιθανό να προσδιορίσει τον κατασκευαστή κάθε σημείου πρόσβασης με την εξέταση της διεύθυνσης MAC. Η παρακολούθηση της πορείας μιας μεγάλης ποσότητας πακέτων προς σημεία πρόσβασης, μπορεί να δώσει τον αριθμό των ασύρματων συσκευών που συνδέονται με κάθε σημείο πρόσβασης. Εάν στο δίκτυο χρησιμοποιείται κρυπτογράφηση WEP, τότε μπορεί να εξετάσει εάν ο καθένας χρησιμοποιεί το ίδιο κλειδί ή αν κάθε συσκευή έχει ένα ξεχωριστό κλειδί με την εξέταση των bit στην IEEE 802.11 επιγραφή. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

Μπορεί να χρησιμοποιηθεί μία άλλη μέθοδος η τεχνική της ανάλυσης κυκλοφορίας. Η ανάλυση κυκλοφορίας αποτελεί τη μελέτη των εξωτερικών στοιχείων των μηνυμάτων, όπως για παράδειγμα τη συχνότητα επικοινωνίας και το μέγεθος του μηνύματος. Δυστυχώς, είναι δυνατό να μαθευτεί ολόκληρο ή ένα μέρος για τους τύπους των πραγμάτων που συμβαίνουν σε ένα δίκτυο ακριβώς με την προσοχή των μηκών πακέτων και τη σημείωση του συγχρονισμού χωρίς κοίταγμα μέσα στα πακέτα. Παρόλα αυτά δεν υπάρχει άμεση πρόσβαση στο περιεχόμενο μηνυμάτων. Ένα πολύ χρήσιμο εργαλείο που χρησιμοποιείται στην ανάλυση, παρακολούθηση και στον εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα αλλά και στην εκπαίδευση είναι το Wireshark. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

3.9.2 Ενεργητικές επιθέσεις

Όπως αναφέραμε προηγουμένως, η μέθοδος κρυπτογράφησης του WEP έχει χάσει την παλιά της ποιότητα, εφόσον μέσα σε λίγα λεπτά μπορεί να ανακτηθεί ο μυστικός κωδικός που χρειάζεται για την παραβίαση ενός ασύρματου δικτύου. Οι μέθοδοι που χρησιμοποιούνται σήμερα για το WEP Cracking επικεντρώνονται στην συλλογή μεγάλου ποσοστού IV's πακέτων. Η διαδικασία αυτή πραγματοποιείται μέσω της συλλογής και αναμετάδοσης πακέτων ARP (Address Resolution Protocol) στο σημείο πρόσβασης. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

Το Address Resolution Protocol (ARP) (πρωτόκολλο επίλυσης διευθύνσεων) χρησιμοποιείται με σκοπό να βρεθεί μια διεύθυνση του στρώματος συνδέσμου (link layer) ή διεύθυνση εξοπλισμού (hardware address) ενός host με βάση μια διεύθυνση του επιπέδου επικοινωνίας (network layer). Κάθε host που είναι συνδεδεμένος σε ένα δίκτυο που βασίζεται στο ARP κρατάει έναν κατάλογο (ARP table) ζεύγων. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

Τα ερωτήματα ARP στέλνονται με broadcast, που σημαίνει πως διάφοροι host τα λαμβάνουν. Σε γενικές γραμμές η επίθεση σε συστήματα WEP πραγματοποιείται μέσω συλλογής είτε

αδύναμων είτε μοναδικών IV's πακέτων. Ωστόσο πάντα απαιτείται η συλλογή μεγάλου ποσοστού κρυπτογραφημένων πακέτων. Ενδιαφέρουσα περίπτωση αποτελεί και η μέθοδος "Caffe Latte Attack", με τη βοήθεια της οποίας ο επιτιθέμενος μπορεί να ανακαλύψει το WEP κλειδί του δικτύου χωρίς να βρίσκεται στην ίδια περιοχή με το δίκτυο – στόχο απλά στοχεύοντας συγκεκριμένους πελάτες σε δημόσιες περιοχές. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

3.9.3 Ενεργητικές: Τροποποίηση δεδομένων

Αυτές οι μέθοδοι τροποποίησης δεδομένων έχουν πολλούς διαφορετικούς στόχους, που κυμαίνονται από την τροποποίηση του ηλεκτρονικού ταχυδρομείου με κακόβουλο περιεχόμενο, έως και την αλλαγή αριθμών σε μια ηλεκτρονική τραπεζική μεταφορά. Ωστόσο παρότι τέτοιες υψηλού επιπέδου τροποποιήσεις έχουν πραγματοποιηθεί, είναι αρκετά περιορισμένες στην πράξη λόγω του βαθμού δυσκολίας που έχουν. Η επιγραφή IP είναι ευκολότερο να δεχτεί επίθεση γιατί είναι μια γνωστή μορφή. Μια επίθεση τροποποίησης είναι η Man-in-the-Middle επίθεση (άτομο στην μέση).

- Man in the Middle Attack

  Σε αυτό το είδος της επίθεσης, ο επιτιθέμενος βρίσκεται στη μέση της συνομιλίας δυο συμμετεχόντων στο δίκτυο, Π1 και Π2. Σε μια πραγματική επικοινωνία ο Π1 θα λάμβανε μηνύματα από τον Π2 και ο Π2 από τον Π1. Ο εισβολέας όμως μπορεί να μιμηθεί καθέναν από τους δυο και να στέλνει μηνύματα τα οποία φαίνεται ότι προήλθαν από την πραγματική τους επικοινωνία. Συνήθως τέτοιου είδους επιθέσεις χρησιμοποιούνται για την τροποποίηση μηνυμάτων κατά τη μεταφορά χωρίς να υπάρχει περίπτωση να ανιχνευθούν. Για την εφαρμογή μιας τέτοιας επίθεσης σε ένα ασύρματο δίκτυο υπάρχουν δυο διαφορετικές μέθοδοι, τα πλαίσια διαχείρισης, συγκεκριμένα για την ασύρματη δικτύωση και το ARP Spoofing, το οποίο αποτελεί απειλή ακόμα και για τα ενσύρματα δίκτυα. (Frankel, S., Bemard, E., Les, O., & Scarfone, K. 2007)

3.9.4 Ενεργητικές: Μεταμφίεση (SPOOFING)

Σε αυτού του είδους τις επιθέσεις, ο επιτιθέμενος, υποκρίνεται κάποιον νόμιμο χρήστη του δικτύου ώστε να αποκτήσει τα δικαιώματα πρόσβασης σε υπηρεσίες που επιθυμεί. Στην ουσία χρησιμοποιούνται στοιχεία πρόσβασης ενός νόμιμου χρήστη. Αυτά τα στοιχεία μπορούν να γίνουν βορά στα χέρια ενός επιτιθέμενου στις εξής περιπτώσεις :

- Όταν δεν χρησιμοποιείται κρυπτογράφηση στο δίκτυο
- Όταν χρησιμοποιούνται εύκολοι κωδικοί
- Όταν δεν ακολουθούνται οι κανόνες προστασίας κωδικών πρόσβασης. Η μέθοδος αυτή είναι ιδανική εάν ένας επιτιθέμενος θέλει να μην αποκαλυφθεί. Εάν η συσκευή καταφέρει να ξεγελάσει το δίκτυο ως εξουσιοδοτημένη συσκευή, τότε ο επιτιθέμενος παίρνει όλα τα δικαιώματα πρόσβασης που επιθυμεί από την εξουσιοδοτημένη. Επιπλέον, δεν θα υπάρξει καμία προειδοποίηση ασφάλειας.

3.9.5 Ενεργητικές: άρνηση υπηρεσιών (DENIAL OF SERVICE)

Σκοπός μιας τέτοιας επίθεσης είναι η ολική αχρήστευση του ασύρματου δικτύου για ένα χρονικό διάστημα. Ουσιαστικά αφαιρούνται τα δικαιώματα από όλους τους νόμιμους και μη νόμιμους χρήστες του δικτύου και στόχος είναι η διαταραχή της ομαλής λειτουργίας του δικτύου. Μια τέτοια επίθεση μπορεί να πραγματοποιηθεί με δυο τρόπους. Η πρώτη μέθοδος απλά κατακλύζει το στόχο υπολογιστή ή τη συσκευή υλικού με πληροφορίες ώστε να μπλοκάρει. Σύμφωνα με τη δεύτερη μέθοδος στέλνονται καλά διατυπωμένες εντολές ή λάθος δεδομένα με στόχο να κολλήσει το σύστημα. Οι επιθέσεις αυτού του είδους είναι οι πιο επικίνδυνες διότι υπάρχει μικρότερο περιθώριο προστασίας. (Peikari C. & Fogie S., 2002)

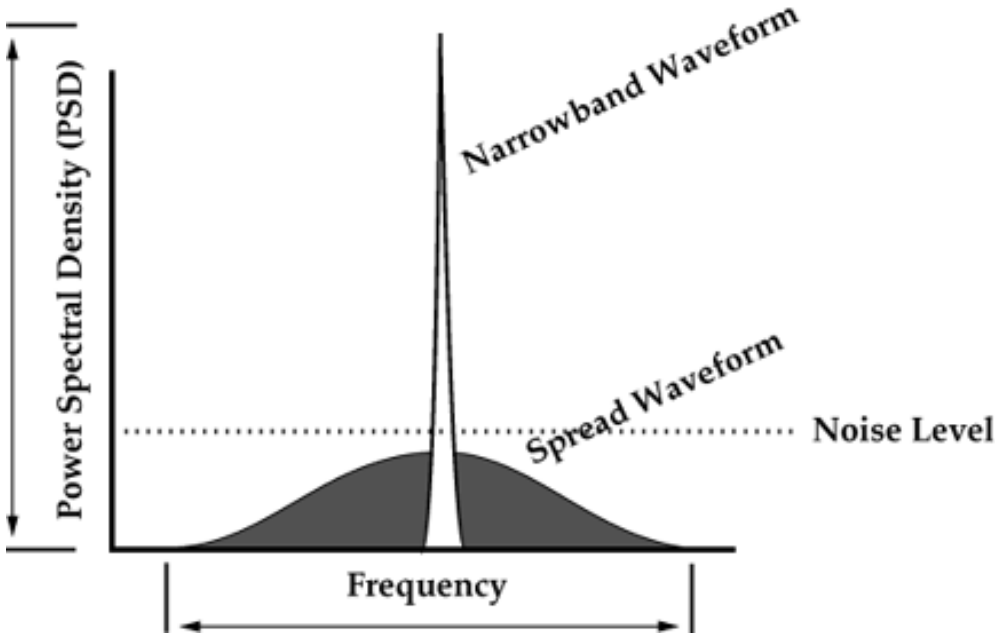
Οι πέντε πιο σημαντικοί τύποι επιθέσεων DOS περιγράφονται παρακάτω: (Peikari C. & Fogie S., 2002)

- Επίθεση πλημμύρας (Flood Attack): Αυτές είναι οι πιο γνωστές του είδους των DoS επιθέσεων. Ο μηχανισμός αυτής της επίθεσης είναι απλός. Ο επιτιθέμενος δημιουργεί στον server περισσότερη κίνηση από αυτή που μπορεί να διαχειριστεί. Εάν όμως ο υπολογιστής – θύμα διαθέτει ένα πολύ καλό bandwidth τότε έχει πολύ καλές πιθανότητες να μην επηρεαστεί. Ωστόσο η αύξηση του bandwidth, δεν είναι από μόνη της μιας επαρκής προστασία ενάντια σε μια τέτοια επίθεση. Παρόλα αυτά, εάν είναι ανεπαρκές, ακόμα και ένας φυσιολογικός όγκος αιτημάτων μπορεί να οδηγήσει σε μια τέτοια δύσκολη κατάσταση.
- Επίθεση Ping of Death: Η επίθεση Ping of Death είναι μια άλλη παλιότερη μορφή επίθεσης DoS. Η βασική αρχή της δεν είναι τόσο έξυπνη όμως καταφέρνει να εκμεταλλευτεί την αδυναμία του TCP/IP πρωτοκόλλου. Η μέθοδος αυτή απλά στέλνει ένα διάγραμμα δεδομένων, το μέγεθος του οποίου ξεπερνάει τα συνηθισμένα. Όταν ένα τέτοιο διάγραμμα φτάσει στον προορισμό του, το σύστημα που το παραλαμβάνει καταρρέει. Ευτυχώς όμως , τέτοιου είδους επιθέσεις τώρα πια είναι ιστορία επειδή όλοι οι σύγχρονοι εξοπλισμοί διαθέτουν μηχανισμούς άμυνας ενάντια σε τέτοιες επιθέσεις.
- Επίθεση SYN: Οι επιθέσεις SYN εκμεταλλεύονται επίσης αδυναμίες του TCP/IP πρωτοκόλλου. Η εγκαθίδρυση μιας σύνδεσης μέσω του TCP/IP, συμπεριλαμβάνει έναν μηχανισμό χειραψίας, στον οποίο έχουμε ανταλλαγή μηνυμάτων συγχρονισμού (Synchronize) και επιβεβαίωσης (Acknowledgment). Όταν ένας επιτιθέμενος καταφέρει να γεμίσει τον προορισμό με μηνύματα συγχρονισμού (SYN), τότε γεμίζει και ο αποθηκευτικός χώρος τους. Σε αυτή την περίπτωση, δεν είναι δυνατόν να αποσταλούν μηνύματα επιβεβαίωσης (ACK) και κατ' επέκταση δεν είναι δυνατή η δημιουργία TCP/IP συνδέσεων με οποιονδήποτε το επιχειρήσει.
- Επίθεση Teardrop: Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει (reassembly) παθαίνει κατάρρευση (crash) ή/και "πάγωμα" (hang) ή/και επανεκκίνηση (reboot). Όπως και η Ping of Death, η επίθεση αυτή είναι τώρα πια ιστορία.
- Επίθεση Smurf: Κατά την έναρξη μίας επίθεσης Smurf, ο επιτιθέμενος στέλνει μία πληθώρα πακέτων ping ICMP Echo Request σε διευθύνσεις IP broadcast διαφόρων δικτύων. Τα πακέτα αυτά έχουν τροποποιηθεί κατάλληλα ούτως ώστε στο πεδίο source της κεφαλίδας IP να αναγράφεται η διεύθυνση IP του θύματος και όχι του επιτιθέμενου. Επίσης, δεδομένου ότι στάλθηκαν στην διεύθυνση IP Broadcast των διαφόρων δικτύων, τα λαμβάνουν όλοι οι υπολογιστές που ανήκουν σε αυτά. Αυτό έχει ως συνέπεια όλοι οι υπολογιστές να απαντούν στο ping με πακέτα ICMP Echo Reply, τα οποία έχουν ως διεύθυνση προορισμού την διεύθυνση IP του θύματος. Άρα λοιπόν το θύμα πλημμυρίζει με πακέτα ping και οδηγείται σε κατάρρευση. Οι επιθέσεις αυτές είναι πιο δύσκολα ανιχνεύσιμες, όμως εάν ένα δίκτυο είναι πολύ καλά οργανωμένο και συντηρείται σωστά, η επίθεση αυτή δε θα είναι καταστροφική. Πριν από αρκετά χρόνια τα περισσότερα δίκτυα υπολογιστών ήταν ευπαθή σε τέτοιου είδους επιθέσεις. Σήμερα όμως έχουν αναπτυχθεί οι κατάλληλες τεχνολογίες ούτως ώστε οι επιθέσεις Smurf να μην αποδίδουν.

ΚΕΦΑΛΑΙΟ 4^{ο} ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΚΙΝΗΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

4.1 Χρήση διάχυτου φάσματος.

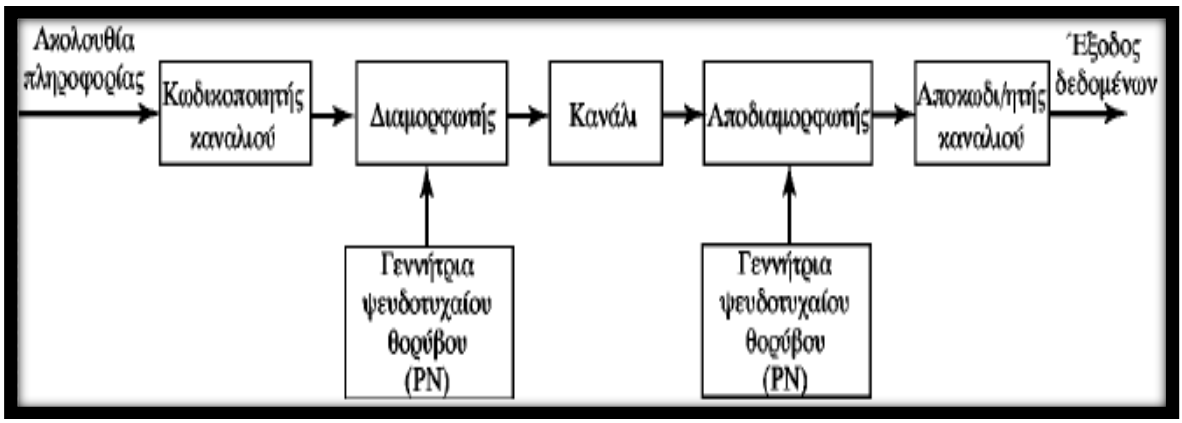
Η χρήση διάχυτου φάσματος για την ασφάλεια ασύρματων επικοινωνιών έχει μια μεγάλη και ενδιαφέρουσα ιστορία. Η αρχική του χρήση έγινε μετά το τέλος του Β' Παγκόσμιου Πολέμου για την βελτίωση των δυνατοτήτων των στρατιωτικών ραντάρ. Στη συνεχεία χρησιμοποιήθηκε, και ακόμα χρησιμοποιείται, στις στρατιωτικές επικοινωνίες για τα δυο βασικά χαρακτηριστικά του που είναι η μικρή πιθανότητα υποκλοπής και η αντίσταση στις παρεμβολές. Στον ιδιωτικό τομέα άρχισε να χρησιμοποιείται από τη στιγμή που η ασφάλεια δεδομένων των δορυφορικών και κινητών επικοινωνιών έγινε σημαντικός οικονομικός και επιχειρηματικός παράγοντας στις συναλλαγές των ανθρώπων. Η θεωρία των πληροφοριών μας δίνει την ανάλυση και τα χαρακτηριστικά του διάχυτου φάσματος.



Εικόνα 14 τεχνική spread spectrum

Τα συστήματα διάχυτου φάσματος διακρίνονται σε:

- **Direct Sequence Spread Spectrum (DS-SS):** αυτά υλοποιούνται συνήθως με PSK και σε συστήματα στα οποία είναι δυνατή η επίτευξη συμφωνίας φάσης μεταξύ εκπεμπόμενου και λαμβανόμενου σήματος, όπου ο ψευδοτυχαίος κώδικας αλλάζει τη φάση του PSK σήματος.
- **Frequency Hopping Spread Spectrum (FH-SS):** υλοποιούνται συνήθως με FSK και σε συστήματα που δεν είναι δυνατή η διατήρηση συμφωνίας φάσης λόγω χρονικών μεταβολών του καναλιού, όπου ο ψευδοτυχαίος κώδικας αλλάζει τη συχνότητα του FSK σήματος.



Εικόνα 15 Διάγραμμα γενικού συστήματος επικοινωνίας διάχυτου φάσματος

4.2 Εφαρμογή στην κινητή τηλεφωνία

Η παγκόσμια ανάγκη της ελεύθερης επικοινωνίας και της αγοράς εγκαινίασε μια νέα αντίληψη σχετικά με την δομή και τις δυνατότητες των σύγχρονων τηλεπικοινωνιακών συστημάτων. Η κινητή τηλεφωνία (mobile telephony) αποτελεί απάντηση στις συνεχώς αυξανόμενες απαιτήσεις για ευέλικτες και αξιόπιστες επικοινωνίες. Στο σύστημα αυτό, κάθε κινητό τηλέφωνο συνδέεται με μια κεραία ραδιοεκπομπής η οποία εκπέμπει στο εύρος 800 έως 900 MHz (στις ΗΠΑ). Η περιοχή που καλύπτεται από το σύστημα ραδιομετάδοσης χωρίζεται σε κυψέλες(cells). Στη θεωρία οι κυψέλες είναι εξάγωνα, στην πράξη όμως είναι λιγότερο κανονικά σχήματα. Το μέγεθος της κυψέλης αντιστοιχεί στην εμβέλεια των κινητών πομπών, έτσι ώστε το σήμα από έναν πομπό να μπορεί να ακουστεί από την δική του κυψέλη, και πιθανόν και από τις διπλανές του, αλλά συνήθως όχι περά από αυτές. Σε κάθε κυψέλη είναι διαθέσιμες για επικοινωνία μερικές ομάδες συχνοτήτων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Όλες οι κυψέλες που συνορεύουν πρέπει να έχουν διαφορετικές ομάδες συχνοτήτων, ώστε να μην υπάρχουν παρεμβολές. Η εκχώρηση των συχνοτήτων είναι μια μορφή προβλήματος χρωματισμού γραφημάτων. Πως μπορεί κάποιος να χρωματίσει τις κυψέλες, έτσι ώστε δυο γειτονικές να μην έχουν το ίδιο χρώμα, όπου με τον όρο χρώμα εννοούμε την συχνότητα της κάθε μίας. Το πρόβλημα γίνεται περισσότερο πολύπλοκο από κυψέλες με ακανόνιστα μεγέθη, από κτίρια από λόφους, και από το γεγονός ότι οι πομποί μπορούν να ακουστούν από δύο κυψέλες πιο μακριά σε μερικές περιπτώσεις. Για κάθε κυψέλη υπάρχει ένας σταθμός βάσης τοποθετημένος στην κορυφή ενός κτηρίου ή λόφου με τέτοιο τρόπο, που μπορεί να επικοινωνεί με όλες τις ραδιοσυσκευές που είναι μέσα στην κυψέλη. Όταν ένα κινητό τηλέφωνο ενεργοποιείται, ψάχνει στις συχνότητες τους σταθμούς βάσης για να βρει το ισχυρότερο σήμα και στέλνει μήνυμα αναγγέλλοντας τον αριθμό του τηλέφωνου του. Τότε ο σταθμός βάσης του λέει σε ποια κυψέλη είναι και ποιες συχνότητες να χρησιμοποιήσει. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Όταν ένα κινητό τηλέφωνο θέλει να καλέσει, στέλνει ένα μήνυμα στο σταθμό βάσης του, ο όποιος τότε κατανέμει σε αυτό μια διαθέσιμη συχνότητα εάν υπάρχει. Όταν τελειώσει το τηλεφώνημα, η συχνότητα απελευθερώνεται και γίνεται διαθέσιμη για άλλη κλήση στην ιδία κυψέλη. Η ίδια η συχνότητα μπορεί να χρησιμοποιείται σε πολλές κυψέλες την ίδια χρονική στιγμή, με την προϋπόθεση ότι αυτές είναι έξω από την εμβέλεια των άλλων πομπών. Στα πλαίσια αυτά γεννήθηκε και εφαρμόζεται κύρια στην Ευρώπη το σύστημα κινητής τηλεφωνίας GSM (Global System for Mobile Communications) που χρησιμοποίει την ζώνη συχνοτήτων των 900MHz, πρωτόκολλο επικοινωνίας πολλαπλής προσπέλασης με διαίρεση χρόνου (Time Division Multiple Access η TDMA), με δυνατότητα εξυπηρέτησης οκτώ συνδρομητών ανά φέρον με εύρος ζώνης συχνοτήτων 200KHz. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Σαν επόμενης γένια σύστημα δημιουργήθηκε και χρησιμοποιείται, στην Αμερική το σύστημα PCN (Personal Communication Network) που λειτούργει στην διπλάσια ζώνη συχνοτήτων των 1800 MHz, με πρωτόκολλο επικοινωνίας CDMA και διαμόρφωση διάχυτου φάσματος. Το

πρωτόκολλο πολλαπλής προσπέλασης με διαίρεση κώδικα (Code Division Multiple Access ή CDMA) είναι ένα σύστημα FH ή DS διάχυτου φάσματος που δύο η περισσότερα σήματα επικοινωνούν το καθένα λειτουργώντας στην ίδια ζώνη συχνοτήτων. Στο πρωτόκολλο CDMA, κάθε χρήστης χαρακτηρίζεται από ένα χωριστό κώδικα. Για παράδειγμα εάν ο χρήστης 1 έχει ένα κώδικα s1 και ο χρήστης 2 έχει ένα κώδικα s2, τότε ο δεκτής που θέλει να λάβει ο χρήστης 1 θα λαμβάνει στην κεραία του όλη την ενεργεία του χρηστή 1 χωρίς να εμποδίζεται από τν εκπομπή των άλλων. Το πρωτόκολλο αυτό χρησιμεύει για στρατιωτικές δορυφορικές επικοινωνίες και για διάφορα εμπορικά δίκτυα δεδομένων που χρησιμοποιούν δορυφορική μετάδοση. Το CDMA έχει ισχυρή αντίσταση στις παρεμβολές και αυξάνει τον αριθμό των χρηστών ίδιου φάσματος συχνοτήτων ανά κυψέλη κινητής τηλεφωνίας χωρίς προβλήματα ποιότητας στην επικοινωνία. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

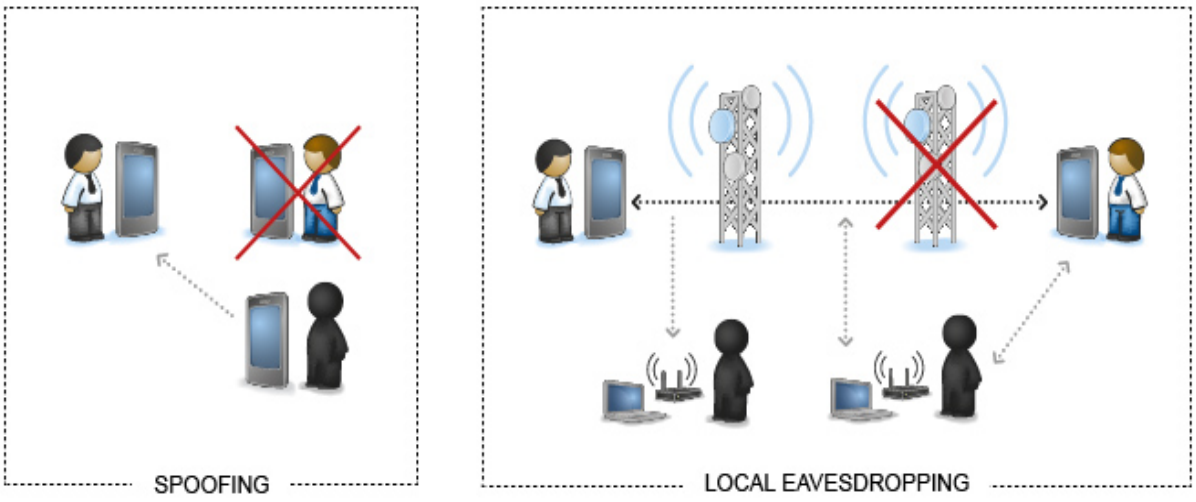
4.3 Ασφάλεια Κινητών Επικοινωνιών

Η επιστημονική έρευνα στο χώρο της ασφάλειας γίνεται πιο έντονη όσο πλησιάζουμε την προοπτική του ενοποιημένου δικτυακού περιβάλλοντος της τέταρτης γενιάς. Οι εμπλεκόμενοι οργανισμοί προτυποποίησης, στην προσπάθειά τους να πετύχουν το μέγιστο βαθμό συμβατότητας με τα προηγούμενων γενεών συστήματα, φαίνεται, τουλάχιστον προς το παρόν, να επιλέγουν για υλοποίηση μεθόδους και διαδικασίες ασφαλείας, που περισσότερο ταιριάζουν σε κλειστά και περιορισμένης εμβέλειας δίκτυα. (www.icsd.aegean.gr)

Το πλήθος των συνδρομητών το οποίο αυξάνεται συνεχώς, οι πολύπλοκες σχέσεις που αναμένεται να αναπτυχθούν μεταξύ των παρόχων, η διασύνδεση των δικτύων αυτών με το διαδίκτυο και το ετερογενές περιβάλλον πρόσβασης, είναι μερικοί από τους λόγους που τα ζητήματα ασφαλείας απαιτείται να αναθεωρηθούν. Οι διαδικασίες εξασφάλισης της επικοινωνίας που διεξάγονται μέσω ενσύρματων δικτύων, έχει το πλεονέκτημα ότι ο ίδιος ο πάροχος (provider) έχει εγκαταστήσει, λειτουργεί και συντηρεί την υπάρχουσα επικοινωνιακή υποδομή (καλωδίωση). Αυτό σημαίνει ότι οποιαδήποτε παρακολούθηση (eavesdropping) ή και υποκλοπή των πληροφοριών που μεταδίδονται τις περισσότερες φορές απαιτεί κάποιου είδους ενεργή (active) παρέμβαση στο δίκτυο του παρόχου (active wiretapping). (www.icsd.aegean.gr)

Το γεγονός αυτό δημιουργεί από την πλευρά των χρηστών αυτών των υπηρεσιών κάποια σιγουριά ότι οι συνομιλίες τους και τα δεδομένα που διακινούνται μέσα από ένα τέτοιο δίκτυο δε μπορούν, εύκολα, να υποκλαπούν. Επιπλέον, αν και πολλές φορές η παγίδευση μιας π.χ. τηλεφωνικής γραμμής δεν απαιτεί ιδιαίτερες τεχνικές γνώσεις, το ανταποδοτικό όφελος για τον επιτιθέμενο στις περισσότερες των περιπτώσεων είναι σχετικά μικρό και οι πιθανότητες να αποκαλυφθεί σχετικά μεγάλες. (www.icsd.aegean.gr)

Αντίθετα, η πιθανότητα επιθέσεων σε ασύρματα περιβάλλοντα επικοινωνιών είναι αρκετά αυξημένη. Οι ραδιο-επικοινωνίες μπορούν να παρακολουθηθούν, ενώ το ρίσκο για τον επιτιθέμενο είναι κατά πολύ μικρότερο. Στην περίπτωση των κινητών επικοινωνιών που βασίζονται σε κυψέλες (Cellular Networks) η υποκλοπή των δεδομένων που διακινούνται μπορεί να συμβεί σε σχετικά μεγάλη απόσταση από την πηγή ή τον προορισμό των δεδομένων, δηλαδή το χρήστη και την κεραία αντίστοιχα. Έτσι, η ασφάλεια (security) των εκπεμπόμενων δεδομένων (data) αλλά και της σηματοδοσίας (signaling) αποτελεί ουσιώδες κεφάλαιο σε ένα σύστημα κινητών επικοινωνιών. Σε ένα ασύρματο δίκτυο η πρόσβαση δεν μπορεί να περιοριστεί σε φυσικά καθορισμένο χώρο (physically). Επιπλέον, τα εκπεμπόμενα δεδομένα των χρηστών αλλά και της σηματοδοσίας μεταξύ δικτύου και των τερματικών κινητών σταθμών μπορούν να ληφθούν από οποιονδήποτε διαθέτει έναν κατάλληλο δέκτη. (www.icsd.aegean.gr)



Εικόνα 16 ασφάλεια κινητών επικοινωνιών

Κατά συνέπεια, είναι απαραίτητο να χρησιμοποιηθούν κατάλληλοι μηχανισμοί προστασίας, όπως κρυπτογραφικές τεχνικές, προκειμένου να προστατέψουν κατάλληλα τα δεδομένα, τη σηματοδοσία αλλά και τους πόρους του δικτύου. Τα θέματα που κρίνεται απαραίτητο να αντιμετωπιστούν είναι: (www.icsd.aegean.gr)

- η εμπιστευτικότητα (confidentiality),
- η ακεραιότητα (integrity),
- η διαθεσιμότητα (availability) των δεδομένων και των υπηρεσιών του δικτύου,
- η ιδιωτικότητα (privacy) των χρηστών.

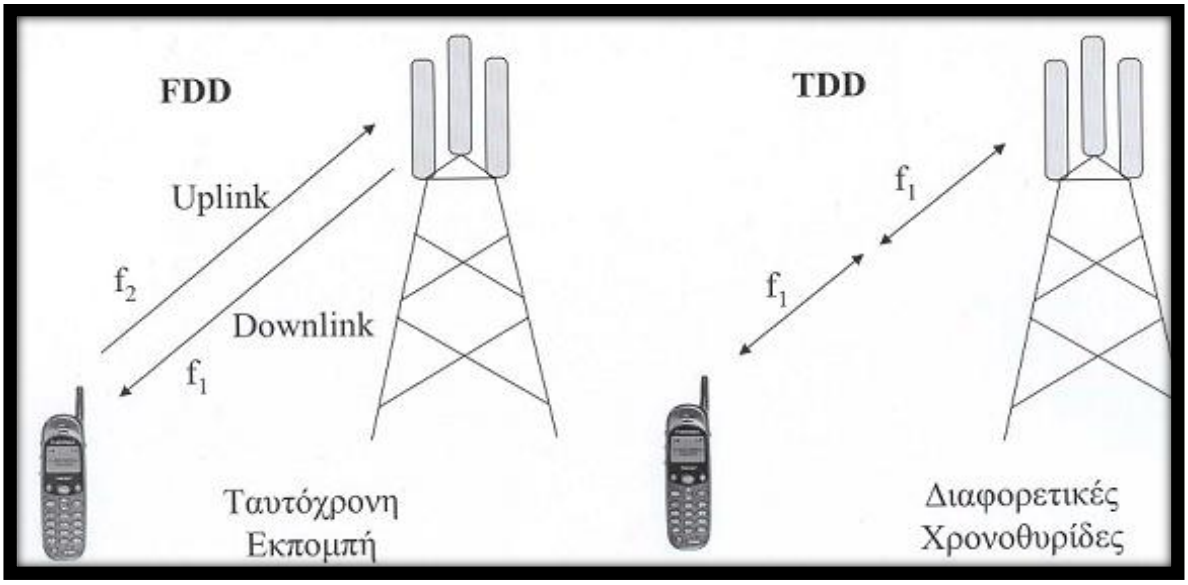
Πολύ σημαντικό είναι επίσης το ζήτημα της αναγνώρισης (identification) και πιστοποίησης της ταυτότητας των χρηστών, του δικτύου και των δεδομένων (authentication). Από την πλευρά της ασφάλειας, η χρησιμοποίηση του πρωτοκόλλου IP δημιουργεί ακόμη περισσότερους κινδύνους. Τα δίκτυα των παρόχων 2G θεωρούνταν κλειστά (closed), εφόσον διέθεταν μικρή διασύνδεση με δίκτυα άλλων παρόχων ή με το Διαδίκτυο (Internet). Παρόλα αυτά, η διασύνδεση των δικτύων 3G με το Διαδίκτυο και με ετερογενή δίκτυα άλλων παρόχων βρίσκεται σε πλήρη εξέλιξη, ενώ το all-IP μοντέλο οδηγεί σε πολύπλοκες σχέσεις εμπιστοσύνης (trust) του τύπου πολλά προς πολλά (many-tomany) μεταξύ των διαφορετικών παρόχων. Κατά συνέπεια, οι τελευταίοι θα κληθούν να αντιμετωπίσουν σοβαρές απειλές για την ασφάλεια των δικτύων τους. Η επιτυχής ή όχι αντιμετώπισή τους θα επηρεάσει και την ποιότητα των προσφερόμενων υπηρεσιών στους τελικούς χρήστες. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η άφιξη των κινητών δικτύων επικοινωνιών δεύτερης γενιάς, όπως είναι για παράδειγμα το σύστημα GSM, τα οποία χρησιμοποιούν ψηφιακή τεχνολογία σε αντίθεση με αυτά της πρώτης γενιάς, αποτέλεσε την απαρχή προκειμένου να αντιμετωπιστούν αποτελεσματικά διάφορα ζητήματα ασφάλειας. Παραδείγματος χάριν, διάφορες κρυπτογραφικές μέθοδοι μπορούν να χρησιμοποιηθούν για να προσφέρουν υπηρεσίες εμπιστευτικότητας (confidentiality) στα δεδομένα που διακινούνται, ενώ παράλληλα μηχανισμοί ακεραιότητας μπορούν να εξασφαλίσουν από άκρο σε άκρο (end-to-end) την ακεραιότητα (integrity) των δεδομένων που εκπέμπονται. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

4.4 Τεχνολογία WCDMA

Το WCDMA (Wideband Code Division Multiple Access), υιοθετήθηκε ως η πιο διαδεδομένη ασύρματη διεπαφή όσον αφορά στα κινητά 3ης γενιάς. Οι προδιαγραφές του δημιουργήθηκαν από τη 3GPP, στην οποία συμμετέχουν τηλεπικοινωνιακοί φορείς από Ευρώπη, Ιαπωνία, Κορέα, Αμερική και Κίνα. Οι βασικές παράμετροι της ασύρματης διεπαφής του WCDMA είναι οι ακόλουθες: (Σιωζοπούλου Θ., 2006)

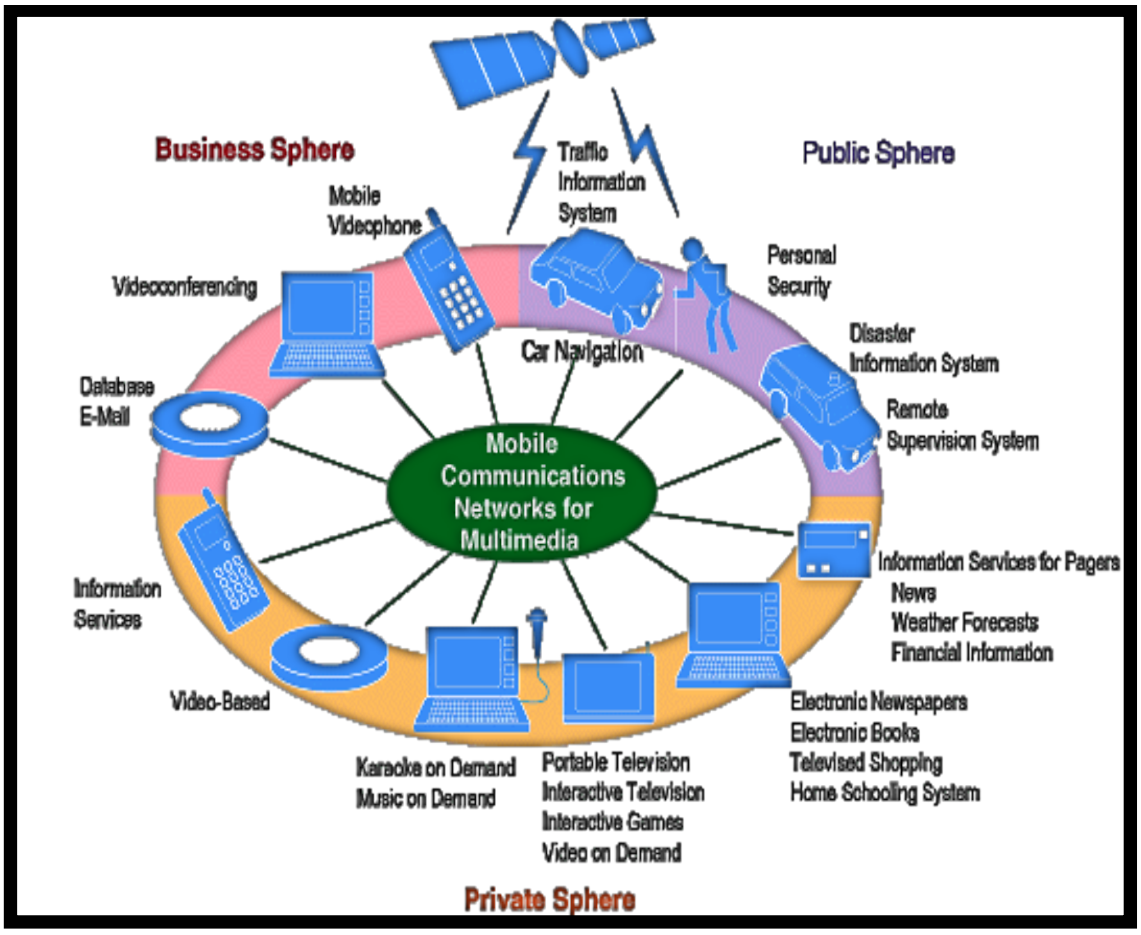
- Το WCDMA είναι ένα ευρείας ζώνης Direct-Sequence Code Division Multiple Access (DS-CDMA) σύστημα. Αυτό σημαίνει ότι τα bits των πληροφοριών του χρήστη απλώνονται σε ένα μεγάλο εύρος συχνοτήτων, έπειτα πολλαπλασιάζονται με ψευδοτυχαία bits (που ονομάζονται chips), τα οποία προέρχονται από τους αντίστοιχους κώδικες του CDMA.
- Ο ρυθμός chip των 3,84 Mcps απαιτεί εύρος ζώνης του φέροντος γύρω στα 5 MHz. Τα DS-CDMA συστήματα με εύρος ζώνης 1MHz, όπως το σύστημα IS-95, συχνά συναντώνται και με τον όρο συστήματα CDMA στενού εύρους ζώνης. Το μεγάλο εύρος του WCDMA υποστηρίζει υψηλούς ρυθμούς δεδομένων χρήστη και μπορεί να προσφέρει συγκεκριμένα προτερήματα απόδοσης, όπως αυξημένη διαφορετικότητα πολλαπλής διαδρομής. Ο διαχειριστής του δικτύου μπορεί να χρησιμοποιήσει πολλαπλά φέροντα των 5 MHz, για να αυξήσει την χωρητικότητα. Η απόσταση των φερόντων μπορεί να επιλεγεί σε 200 kHz μεταξύ 4,4 και 5 MHz, ανάλογα με την παρεμβολή μεταξύ των φερόντων.
- Το WCDMA υποστηρίζει υψηλούς μεταβλητούς ρυθμούς δεδομένων χρήστη, ή διαφορετικά υποστηρίζεται με επάρκεια το εύρος ζώνης κατά απαίτηση (BoD). Κάθε χρήστης χρησιμοποιεί πλαίσια διάρκειας 10 ms, κατά την διάρκεια των οποίων ο ρυθμός δεδομένων διατηρείται σταθερός. Όμως δεν μπορεί να αλλάξει η χωρητικότητα των δεδομένων από πλαίσιο σε πλαίσιο. Η διευθέτηση της χωρητικότητας ρυθμίζεται από το δίκτυο ώστε να επιτευχθεί η μέγιστη απόδοση στις υπηρεσίες με πακέτα δεδομένων.
- Το σύστημα WCDMA υποστηρίζει δύο τρόπους λειτουργίας: Αμφίδρομη διαίρεση συχνότητας (Frequency Division Duplex FDD) και αμφίδρομη διαίρεση χρόνου (Time Division Duplex TDD). Στην τεχνική FDD, χρησιμοποιούνται ξεχωριστά φέροντα συχνοτήτων 5 MHz για τις δύο κατευθύνσεις άνω και κάτω ζεύξης, ενώ στην τεχνική TDD και οι δύο κατευθύνσεις μοιράζονται χρονικά ένα μόνο φέρον 5 MHz. Κατεύθυνση άνω ζεύξης είναι η σύνδεση από το κινητό στο σταθμό βάσης, ενώ κατεύθυνση κάτω ζεύξης από το σταθμό βάσης προς το κινητό. Η τεχνική TDD βασίζεται στις αρχές της FDD και προστέθηκε ώστε να αυξηθεί η απόδοση του βασικού συστήματος WCDMA.



Εικόνα 17 FDD και TDD λειτουργίας

- Το WCDMA υποστηρίζει την λειτουργία ασύγχρονων σταθμών βάσης, έτσι ώστε σε αντίθεση με το IS-95 να μην απαιτείται η ύπαρξη χρονικού σήματος αναφοράς, όπως το GPS.
- Το WCDMA χρησιμοποιεί σύμφωνη ανίχνευση στις δύο κατευθύνσεις άνω και κάτω ζεύξης. Αν και η χρήση σύμφωνης ανίχνευσης στην κάτω ζεύξη έχει ήδη πραγματοποιηθεί στο IS-95, η χρήση και στην κατεύθυνση άνω ζεύξης αναμένεται να αυξήσει την χωρητικότητα και κάλυψη στην κατεύθυνση αυτή.
- Η ασύρματη διεπαφή του WCDMA είναι σχεδιασμένη ώστε να μπορούν να χρησιμοποιηθούν από τον διαχειριστή του δικτύου προχωρημένες μέθοδοι λήψης, όπως έξυπνες, προσαρμοστικές κεραίες, ως μια επιλογή του συστήματος για αύξηση της κάλυψης ή/και της χωρητικότητας. Στα περισσότερα συστήματα δεύτερης γενιάς, δεν υπάρχει πρόνοια, για κάτι τέτοιο με αποτέλεσμα να μην είναι εφαρμόσιμα τέτοια σενάρια ή να χρησιμοποιούνται κάτω από σημαντικούς περιορισμούς με περιορισμένες δυνατότητες αύξησης της απόδοσης.
- Το WCDMA έχει σχεδιαστεί ώστε να λειτουργεί σε συνδυασμό με το GSM. Έτσι, διαπομπές μεταξύ GSM και WCDMA υποστηρίζονται, με σκοπό να αυξηθεί η απόδοση κάλυψης του GSM για την εισαγωγή του WCDMA.

Το παρακάτω σχήμα περιλαμβάνει υπηρεσίες που μπορούν να εξυπηρετηθούν με χρήση του WCDMA συστήματος.



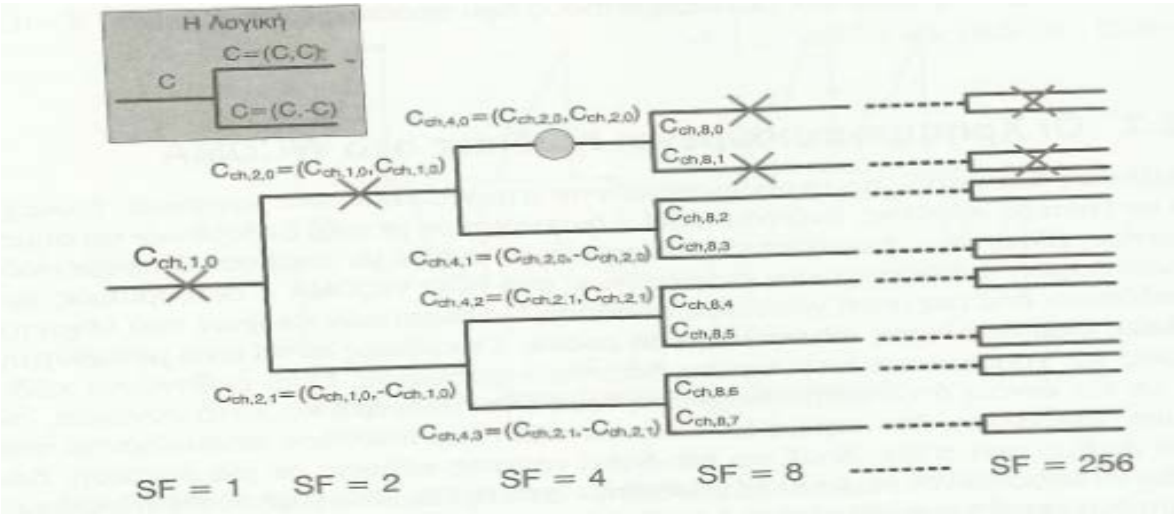
Εικόνα 18 υπηρεσιών που καλύπτει το WCDMA

4.5 Οι Χρησιμοποιούμενοι Κώδικες στο WCDMA

Οι κώδικες διασποράς που χρησιμοποιούνται στο WCDMA είναι μοναδικοί, τουλάχιστο σε επίπεδο κυψέλης. Ενώ στο GSM ο διαχωρισμός μεταξύ δεδομένων και σηματοδοσίας, αλλά και ο διαχωρισμός των χρηστών γίνεται με απόδοση διαφορετικών χρονοσχισμών ή διαφορετικών συχνοτήτων, στο FDD WCDMA ο διαχωρισμός των μεταδόσεων από μια πηγή γίνεται με απόδοση διαφορετικών κωδίκων που λέγονται κώδικες διαυλοποίησης (channelization codes). Οι κώδικες αυτοί είναι μεταβλητού μήκους και χρησιμοποιούνται για τη διασπορά φάσματος. Είναι ορθογώνιοι κώδικες, με την έννοια ότι η ετεροσυσχέτισή τους είναι μηδενική και κατά συνέπεια, σε ιδανικό περιβάλλον, δεν παρεμβάλλονται μεταξύ τους. Επιπλέον, αποτελούνται από άρτιο αριθμό από chips. Άπαξ και αποδοθεί κάποιος κώδικας σε μια σύνδεση, δεν μπορεί να αποδοθεί σε καμία άλλη σύνδεση. Κατά τη διάρκεια μιας σύνδεσης μπορεί να μεταβάλλεται ο ρυθμός μετάδοσης. Το σύστημα στην περίπτωση αυτή αλλάζει το SF και κατά συνέπεια τον κώδικα. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)

Στο FDD έχουμε 512 κώδικες στο DL και 256 στο UL, ενώ στο TDD έχουμε 16 κώδικες τόσο στο DL, όσο και στο UL. Το μήκος κώδικα αντιστοιχεί στον απαραίτητο SF και άρα επιλέγεται σε διακριτά βήματα. Για τον SF ισχύει: SF = 2*, k = 0,...,8. Ο SF δείχνει το μήκος του κώδικα, το οποίο είναι μεταβλητό ανάλογα με το ρυθμό μετάδοσης. Όσο μεγαλύτερος είναι ο ρυθμός, τόσο πιο μικρό είναι το μήκος του κώδικα. Στο FDD, ο SF μπορεί να πάρει τιμές από 4 ως 256 στο uplink (1-66.7μsec) και από 4 ως 512 στο downlink. Στο TDD ο SF μπορεί να πάρει τιμές από 1 ως 16 τόσο στο uplink, όσο και στο downlink. Επειδή οι κώδικες αυτοί έχουν μήκος και συμπεριφορά διασποράς που καθορίζεται από το SF, καλούνται Orthogonal Variable Spreading Factor Codes ή OVSF. Οι OVSF κώδικες οργανώνονται σε δένδρο. Αν ένας κώδικας αποδοθεί σε μια σύνδεση, τότε όλοι οι κώδικες που ακολουθούν, αλλά και οι προηγούμενοι στο δένδρο, δεν μπορούν πλέον να χρησιμοποιηθούν. Ο λόγος είναι βέβαια η διατήρηση της ορθογωνιότητας. Για παράδειγμα, αν χρησιμοποιείται ο κώδικας Cch,4,0 τότε δεν μπορεί να χρησιμοποιηθεί κανένας κώδικας στο δέντρο που πηγάζει από τον Cch,4,0, ούτε και κανείς από τους Cch,2,0, Cch,1,0. Να σημειώσουμε ότι στην πράξη δεν χρησιμοποιείται SF μικρότερος του 4. Χρησιμοποιώντας π.χ. τον κώδικα Cch,8,1, έχουμε χρησιμοποιήσει το 12,5% των κωδικών. Μπορούμε να αποδώσουμε και άλλους κώδικες στην ίδια κυψέλη, μέχρι να φθάσουμε το 100%. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)

Ο επόμενος πίνακας παρουσιάζει τους SF και τους αντίστοιχους ρυθμούς συμβόλων αλλά και bit για τις δύο ζεύξεις, λαμβάνοντας υπόψη ότι σε συστήματα WCDMA FDD, τη μεν άνω ζεύξη έχουμε 1 bit/symbol, ενώ στην κάτω ζεύξη έχουμε 2bits/symbol. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)



Εικόνα 19 δένδρο OVSF κωδικών

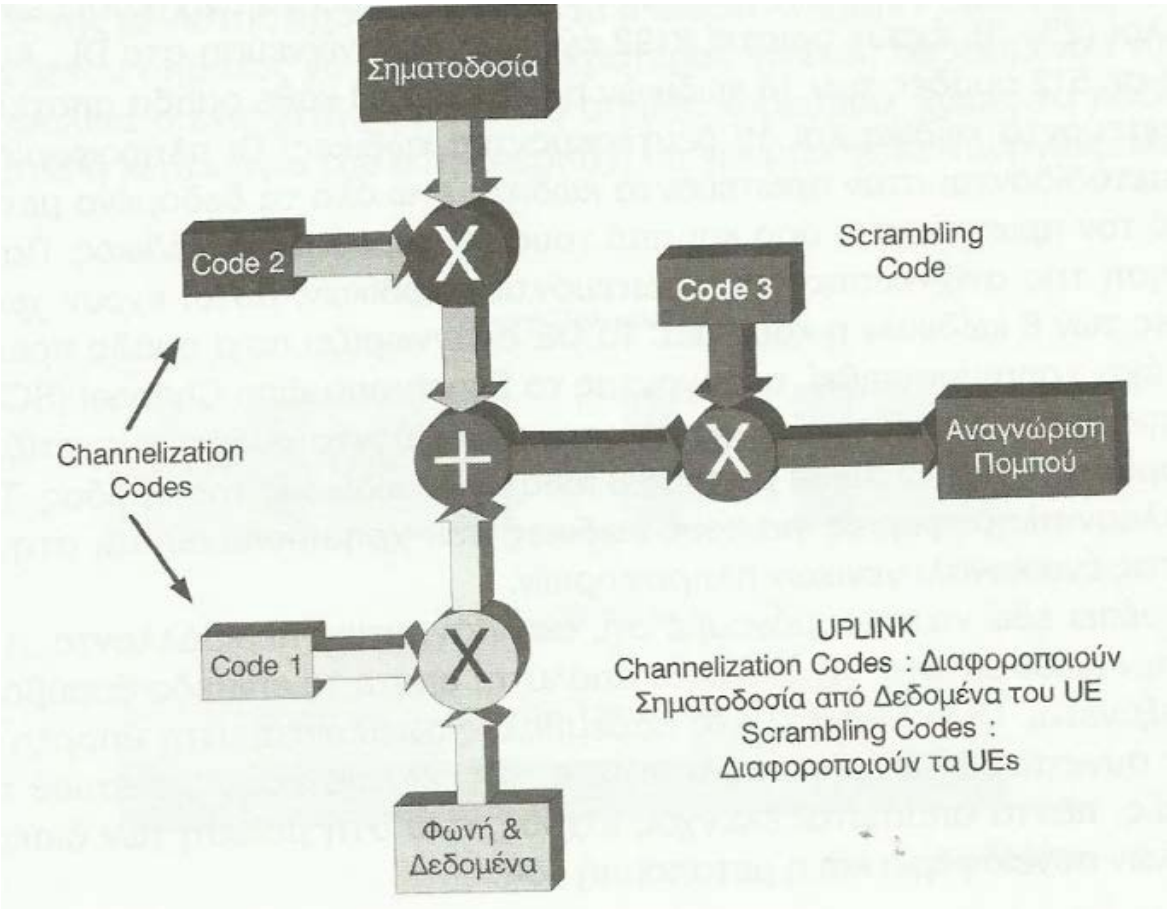
SF	Symbol Rate (Ksps)	Channel bit rate (Kbps) in UL	Channel bit rate (Kbps) in DL
512	7.5	-	15
256	15	15	30
128	30	30	60
64	60	60	120
32	120	120	240
16	240	240	480
8	480	480	960
4	960	960	1920

Εικόνα 20 σχέση κωδικών με ρυθμούς μετάδοσης

Για την αναγνώριση του Node B στο DL και του UE στο UL, εισάγεται ένας επιπλέον κώδικας, ο οποίος καλείται κώδικας περίπλεξης (scrambling code), ο οποίος πολλαπλασιάζει το διεσπαρμένο σήμα προς εκπομπή. Αυτός ο κώδικας δεν προκαλεί κάποια επιπλέον διασπορά, απλά χρησιμοποιείται για το διαχωρισμό των πομπών. Ένα μεγάλο πλεονέκτημα της χρήσης του κώδικα περίπλεξης είναι ότι η διαχείριση του δέντρου των κωδικών σε κάθε πομπό γίνεται πλέον ανεξάρτητα. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)

Ένας ακόμη λόγος για τη χρήση του δεύτερου τύπου κώδικα είναι ότι η πλήρης ορθογωνιότητα είναι δυνατή μόνον αν ο συγχρονισμός στο δέκτη είναι ακριβής. Άρα οι OVSF κώδικες μπορούν να χρησιμοποιηθούν για να διαχωρίσουν διαφορετικούς χρήστες στο DL, σε μια κυψέλη, αλλά όχι και στο UL, όπου η μεταβλητή καθυστέρηση από κάθε UE στο Node B έχει άμεση συνέπεια στην ορθογωνιότητα των μεταδόσεων. Αν βέβαια χρησιμοποιείται τεχνική αμφιδρόμησης TDD με συγχρονισμό στο UL, τότε θα ήταν εφικτός ο διαχωρισμός των χρηστών στο UL. Υπάρχει και ένας ακόμη βασικός λόγος χρησιμοποίησης των κωδικών περίπλεξης, που αφορά στο DL. Συγκεκριμένα, λόγω του μικρού πλήθους των διαθέσιμων OVSF κωδικών, οι κώδικες αυτοί επαναχρησιμοποιούνται σε κάθε κυψέλη. Άρα, δεν είναι δυνατό να διαχωρίσουμε δύο Node B από τον OVSF κώδικα και είναι εξαιρετικά πιθανό ένα UE που βρίσκεται στα άκρα της περιοχής κάλυψης ενός Node B να λαμβάνει δύο σήματα από τα δύο γειτονικά Node B με τον ίδιο κώδικα που προορίζονται όμως, για διαφορετικούς χρήστες. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)

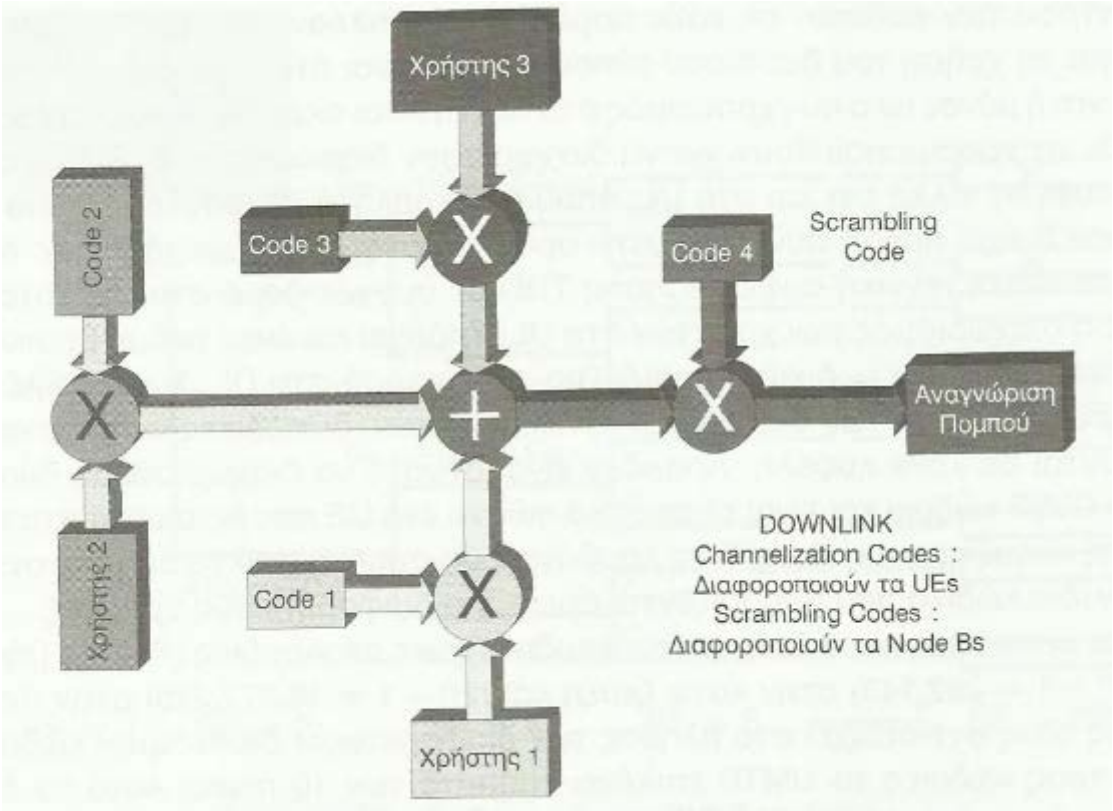
Όλοι οι κώδικες περίπλεξης είναι ψευδοτυχαίες ακολουθίες (PN). Το μήκος τους είναι (2^{18} - 1 = 262,143) στην κάτω ζεύξη και (2^{24} - 1 = 16,777,215) στην άνω ζεύξη. Το μήκος τους αντιστοιχεί στο πλήθος των διαφορετικών διαθέσιμων κωδικών. Από αυτούς τους κώδικες το UMTS επιλέγει τμήματα των 10 msec. Αυτό το διάστημα αντιστοιχεί σε μήκος κώδικα με 38,400 chips ανά πλαίσιο. Παρατηρήστε (Σχήμα 8.18) ότι στο UL οι κώδικες διαυλοποίησης διαχωρίζουν τη σηματοδοσία από τα δεδομένα προς αποστολή. Αντίστοιχα (Σχήμα 8.19), στο DL οι κώδικες διαυλοποίησης χρησιμοποιούνται για να διαχωρίσουν τις εκπομπές προς διαφορετικούς χρήστες (UEs). (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)



Εικόνα 21 Κώδικες στην άνω ζεύξη

Όταν ο UE ενεργοποιείται, προσπαθεί να αναγνωρίσει τους καλύτερους Node B για να συνδεθεί. Επειδή οι κώδικες τους οποίους πρέπει να ανιχνεύσει είναι εξαιρετικά πολλοί (2^{18} - 1), έχουν οριστεί 8192 κώδικες για ανίχνευση στο DL. Αυτοί έχουν χωριστεί σε 512 ομάδες των 16 κωδικών η κάθε μία. Η κάθε ομάδα αποτελείται από έναν πρωτεύοντα κώδικα και 15 δευτερεύοντες κώδικες. Οι πληροφορίες για την κυψέλη μεταδίδονται στον πρωτεύοντα κώδικα, ενώ όλα τα δεδομένα μεταδίδονται τόσο από τον πρωτεύοντα, όσο και από τους δευτερεύοντες κώδικες. Για επιπλέον απλοποίηση της ανίχνευσης των πρωτευόντων κωδίκων, αυτοί έχουν χωριστεί σε 64 ομάδες των 8 κωδικών η κάθε μια. Το UE αναγνωρίζει ποια ομάδα πρωτευόντων κωδίκων έχει χρησιμοποιηθεί, ακούγοντας το Synchronization Channel (SCH). Γνωρίζοντας την ομάδα, το UE μπορεί να βρει τον πρωτεύοντα κωδικό συσχετίζοντας την πληροφορία του Pilot Channel με τους 8 πιθανούς κωδικούς της ομάδας. Το UE βρίσκει επιπλέον πληροφορίες για τους κώδικες που χρησιμοποιούνται στην κυψέλη, ακούγοντας ένα κανάλι γενικών πληροφοριών. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)

Θα πρέπει εδώ να επισημάνουμε ότι, σε πραγματικά περιβάλλοντα, η ορθογωνιότητα των κωδικών στο DL δεν είναι απόλυτη, οπότε το επίπεδο θορύβου-παρεμβολών αυξάνεται. Οι ενδοκυψελικές παρεμβολές οφείλονται στην ύπαρξη πολυδια-δρομικών συνιστωσών, ενώ οι διακυψελικές στην έλλειψη συγχρονισμού των Node B. Συνεπώς, πάντα απαιτείται έλεγχος ισχύος, ενώ στη μείωση των διακυψελικών παρεμβολών συνεισφέρει και η μεταπομπή soft. (Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., 2008)



Εικόνα 22 κώδικες στην κάτω ζεύξη

ΚΕΦΑΛΑΙΟ 5^{ο} ΝΟΜΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

5.1 Εισαγωγή

Είναι γνωστό ότι η άξια του νόμου φαίνεται κυρίως στην εφαρμογή του. Ως προς αυτό το κριτήριο οι νέες τεχνολογίες πληροφορικής βάζουν σε δοκιμασία μεγάλα τμήματα της παραδοσιακής νομοθεσίας. Η ποινική νομοθεσία στα προηγμένα κράτη διευρύνεται ώστε να συμπεριλάβει νέου τύπου αδικήματα, άλλα για την αποτελεσματική εφαρμογή της χρειάζεται ακόμη κατάλληλη εκπαίδευση αστυνομικών και δικαστικών αρχών, των ιδίων των χρηστών και των τεχνολογιών. Παράλληλη εισαγωγή τεχνικών και οργανωτικών μέτρων ασφάλειας και μέτρα για την επιτάχυνση της διεθνούς συνεργασίας. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας εξελίσσεται για να καλύψει τις νέες ηλεκτρονικές μορφές πνευματικών έργων, άλλα για την αποτελεσματική εφαρμογή της χρειάζεται ακόμη εκπαίδευση, διαδικασίες επικοινωνίας των δυο αυτών πλευρών, τεχνικά μέσα για την παρακολούθηση της χρήσης των έργων, νέοι ευέλικτοι τρόποι για την καταβολή και διανομή του αντίτιμου των πνευματικών δικαιωμάτων. Σε όλες τις περιπτώσεις η αποτελεσματικότητα τόσο της νομοθεσίας όσο και των συμπληρωματικών μέτρων θα παραμείνει αμφίβολη όσο τα πεδία εφαρμογής τους είναι μεμονωμένα ανεπτυγμένα κράτη ή και το σύνολο της Ευρωπαϊκής Ένωσης. Οι σύγχρονες τεχνολογικές εξελίξεις απαιτούν μετρά με παγκόσμια εμβέλεια. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Οποιαδήποτε γενική νομοθεσία πρέπει να συνοδεύεται από νομοθετήματα τομεακού χαρακτήρα. Η ραγδαία εξάπλωση των νέων τεχνολογιών σε όλους τους τομείς της κοινωνικής και οικονομικής ζωής, δημιουργεί ειδικές χωριστές ανάγκες για την προστασία των προσωπικών δεδομένων ανάλογα με τις ιδιαιτερότητες του κάθε τομέα. Από το 1981 μέχρι σήμερα το συμβούλιο της Ευρώπης έχει υιοθετήσει μια σειρά από συστάσεις που καλύπτον τις ιατρικές βάσεις δεδομένων, την κοινωνική ασφάλιση, το μάρκετινγκ, τα δεδομένα για τους εργαζόμενους, την εμπορευματοποίηση των δεδομένων του δημόσιου τομέα τα δεδομένα της αστυνομίας, τα δεδομένα της ερευνάς και τις στατιστικής, της τηλεπικοινωνίες. Πρόταση τομεακής οδηγίας για τα ψηφιακά τηλεπικοινωνιακά δίκτυα έχει ήδη υποβληθεί από την ευρωπαϊκή επιτροπή. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Εικόνα 23 νομικά θέματα

Παράλληλα γενικού χαρακτήρα η πρόταση οδηγίας της ευρωπαϊκής ένωσης επιθυμεί από τα κράτη μελή να ενθαρρύνουν τις επαγγελματικές οργανώσεις, ώστε να υιοθετήσουν τομεακούς κώδικες δεοντολογίας, ενώ αφήνει ανοιχτό το ενδεχόμενο νέων τομεακών νομοθετικών προτάσεων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Τα νομοθετήματα και οι κώδικες δεοντολογίας τομεακού χαρακτήρα, έχουν ένα κοινό χαρακτηριστικό, ότι στο βαθμό που εκπονούνται σε στενή συνεργασία με (ή από τους ίδιους τους) ενδιαφερομένους φορείς, συμβάλλουν αποφασιστικά στην ευαισθητοποίηση των χρηστών των προσωπικών δεδομένων κάθε τομέα. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Υπάρχει όμως και μία βασική διάφορα, ότι τα πρώτα έχουν νομική ισχύ δημόσιου δικαίου, κάτι το οποίο αποκτά ιδιαίτερη σημασία εφόσον προβλέπονται αυστηρές κυρώσεις, ενώ οι δεύτεροι αφήνονται ανάλογα στην "νομιμοφροσύνη" των μελών των επαγγελματικών οργανώσεων, δεν είναι βέβαιο ότι δεσμεύουν και τα μη μελή του συγκεκριμένου τομέα και στην αποφασιστικότητα εθελοντικών διαχειριστικών οργάνων όσον αφόρα την επιβολή κυρώσεων. Σε ορισμένα κράτη μελή της Ευρωπαϊκής Ένωσης όπως η Βρετάνια, η Ιρλανδία, και η Ολλανδία, υπάρχει μακρά και σχετικά επιτυχής παράδοση τέτοιων μορφών αυτοδιαχείρισης, η αποτελεσματικότητα του στις χώρες της νότιας Ευρώπης και ειδικά στην Ελλάδα, είναι εξαιρετικά αμφίβολη. Χρειάζεται νομοθετική παρέμβαση με τη μεγαλύτερη συμμέτοχη των ενδιαφερόμενων φορέων, τόσο για την πληρότητα του νομοθετήματος όσο και για την ενημέρωση των χρηστών των προσωπικών δεδομένων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Μεγάλης σημασίας είναι ο ρόλος της υπηρεσίας έλεγχου που προβλέπεται από όλες τις ευρωπαϊκές νομοθεσίες και από την πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης. Η υπηρεσία αυτή ελέγχει κατά κανόνα τόσο το ιδιωτικό όσο και το δημόσιο τομέα, επομένως πρέπει να είναι ουσιαστικά ανεξάρτητη από την Κυβέρνηση. Σε περίπτωση αμφισβητήσεων, τον τελευταίο ρολό έχει η Δικαστική εξουσία και όχι ο υπουργός δικαιοσύνης ή το υπουργικό συμβούλιου. Η υπηρεσία έλεγχου πρέπει να έχει εξουσίες τόσο σε κατασταλτικές (άσκηση έλεγχου, απαγόρευση παράνομης επεξεργασίας δεδομένων, προσφυγή στην δικαιοσύνη), όσο και προληπτικές (έκδοση ερμηνευτικών εγκυκλίων, οργάνωση εκπαιδευτικών σεμιναρίων, θεσμοθετημένο διάλογο με τις ομάδες των χρηστών, συμβολή στην σύνταξη κωδικών δεοντολογίας).Υπάρχουν θαυμάσιες συγκριτικές μελέτες για ορισμένες ευρωπαϊκές χώρες, από τις όποιες μπορούν να αντληθούν χρήσιμα συμπεράσματα. Πρέπει ακόμα να έχει στην διάθεση της επαρκής μέσα έτσι ώστε να ασκεί τα καθήκοντα της. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η περίπτωση του σκανδάλου της εμπορευματοποίησης προσωπικών δεδομένων του δημόσιου στην Νότια Ουαλία της Αυστραλίας, που αποκαλύφθηκε το 1990-1992, από την αρμοδία υπηρεσία έλεγχου, που είχε πενιχρά μέσα (π.χ. συνολικό αριθμό 6 ατόμων), αλλά από την ανεξάρτητη επιτροπή εναντίων της διαφθοράς που είχε ετήσιο προϋπολογισμό άνω των 100 εκατομμυρίων δολαρίων. Πρέπει επίσης η υπηρεσία έλεγχου να έχει πρόσβαση στην δημοσιότητα και κυρίως στα μέσα μαζικής ενημέρωσης και στο Κοινοβούλιο. Σε μια συνειδητοποιημένη κοινωνία όπως ανατάσσεται στην συνεχεία ο φόβος της αρνητικής δημοσιότητας λειτουργίας αποτρεπτικός παράγων για παράνομες πράξεις. Πρέπει τέλος στις αρμοδιότητες (αλλά και στις δυνατότητες) της υπηρεσίας έλεγχου να περιλαμβάνεται και η συνεργασία με τις αντίστοιχες υπηρεσίες άλλων κρατών. Αυτό γίνεται ολοένα περισσότερο αναγκαίο όσο τα τηλεπικοινωνιακά δίκτυα και η πρόοδος της τεχνολογίας διευκολύνουν τη μεταφορά και την επεξεργασία προσωπικών δεδομένων σε οποιαδήποτε χωρά της υδρόγειου. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Στις υπηρεσίες έλεγχου ανήκουν σημαντικές εξουσίες .Τελικός κριτής της σωστής εφαρμογής του νομού και αρμόδιος για την επιβολή κυρώσεων είναι ο δικαστής. Εάν οι υπηρεσίες έλεγχου διαθέτουν στο στελεχιακό τους δυναμικό τόσο νομομαθείς όσο και ειδικούς της πληροφορικής, που εξειδικεύονται στην εφαρμογή του νομού με την πείρα που αποκτούν, οι δικαστές σπάνια διαθέτουν ειδικές γνώσεις είτε του δικαίου της πληροφορικής είτε των εφαρμογών της πληροφορικής σε όλες της πτυχές της κοινωνικής και οικονομικής ζωής. Για τη διαπίστωση νομιμότητας της συγκεκριμένης επεξεργασίας δεδομένων ο νόμος δεν περιέχει πάντοτε ρητές προϋποθέσεις, αλλά παραπέμπει στην συγκριτική εκτίμηση των συμφερόντων τόσο των προσώπων που αφόρα η επεξεργασία, όσο και των χρηστών που προβαίνουν στην επεξεργασία. Είναι βέβαιο ότι από την γενική φύση τους και τουλάχιστον μέχρι να υπάρχουν πολυάριθμα

τομεακά νομοθετήματα για την προστασία των προσωπικών δεδομένων θα αφήσουν μεγάλο πεδίο ερμηνεία και εξειδίκευσης στην νομολογία. Αυτό δεν αφόρα βεβαίως μονό στην προστασία των προσωπικών δεδομένων, αλλά στο σύνολο του δικαίου που επηρεάζεται η δημιουργείται από την πληροφορική. Η συνεχής επιμόρφωση των δικαστών θα ήταν επομένως εξαιρετικά χρήσιμη. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Με την εξάπλωση της χρήσης των νέων τεχνολογιών της πληροφορίας σε παγκόσμιο επίπεδο και των δυνατοτήτων κατάχρησης προσωπικών δεδομένων, ιδιαίτερα σε χώρες οπού η νομοθεσία είναι από ανεπαρκής έως ανύπαρκτη ή ο νομός παραβιάζεται από ισχυρά συμφέροντα(είτε του δημόσιου είτε του ιδιωτικού τομέα), το πλέον αποτελεσματικό όπλο για την προστασία των προσωπικών δεδομένων είναι η συμμέτοχη της κοινωνίας. Ο πολίτης πρέπει να μάθει με σαφήνεια και χωρίς υπερβολές, ποια είναι τα οφέλη καθώς κάποια είναι τα σχετικά δικαιώματα του και ποιοι οι κίνδυνοι από την επεξεργασία των πρωσικών του δεδομένων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Παράλληλα οι χρηστές, πρέπει να ενημερωθούν για της υποχρεώσεις που επιβάλλει η νομοθεσία. το ζητούμενο είναι να βρεθούμε στην πορεία που σήμερα ακόλουθοι, τουλάχιστον στις ανεπτυγμένες χώρες, η προστασία του περιβάλλοντος που περιλαμβάνεται ήδη στο σχεδιασμό της παράγωγης και στην εκστρατεία μάρκετινγκ πολλών προϊόντων. Να φτάσουμε δηλαδή στο σημείο οπού οι συνθήκες ελευθέρου ανταγωνισμού ο πολίτης θα προτίμα εκείνες της υπηρεσίες (τηλεπικοινωνιών, πιστωτικών καρτών, πωλήσεων από απόσταση, ιατρικής περίθαλψης κ.λπ.)που θα σέβονται και θα προστατεύουν τα προσωπικά δεδομένα. Από της ευρωπαϊκές χώρες ο υψηλότερος βαθμός ενδιαφέροντος των πολιτών, παρατηρείτε στην Γερμάνια και αυτό συμβάλει στην θέσπιση αυστηρής, γενικής και τομεακής, νομοθεσίας και σε νομολογία όπως η περίφημη απόφαση του Συνταγματικού Δικαστηρίου της Καρλσρούης που αναγνωρίζει στον πολίτη δικαίωμα "πληροφοριακής αυτοδιάθεσης" Είναι ενδιαφέρουσα η διάφορα ανάμεσα στο πνεύμα της γερμανικής νομοθεσίας που στηρίζει τη νομιμότητα της επεξεργασίας των προσωπικών δεδομένων κυρίως στη συναίνεση του πολίτη και της γαλλικής νομοθεσίας, οπού η νομιμότητα στηρίζεται στην έγκριση της υπηρεσίας έλεγχου. Για να είναι σε θέση να εκτιμήσει τις περιστάσεις και να συναινέσει, ο πολίτης θα πρέπει να είναι ενημερωμένος. Και αυτό είναι φυσικά υποχρέωση του κράτους. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η εξέλιξη των τεχνολογιών πληροφορίας και τηλεπικοινωνιών, καθιστά ολοένα και δυσκολότερο τον έλεγχο της επεξεργασίας των προσωπικών δεδομένων με "παραδοσιακούς τρόπους" καθώς η ποσότητα των δεδομένων που γίνονται αντικείμενο επεξεργασίας, ο συνολικός αριθμός των χρηστών τέτοιων δεδομένων και η ταχύτητα μεταφοράς των δεδομένων μέσω τηλεπικοινωνιών δικτύων αυξάνονται ραγδαίως. Η λύση του προβλήματος αυτού βρίσκεται σε μεγάλο βαθμό στην ίδια την τεχνολογία. Είναι τεχνικά δυνατό στο σχεδιασμό του λογισμικού που χρησιμοποιείτε για την επεξεργασία των προσωπικών δεδομένων, πχ για σκοπούς εργασιακούς, ιατρικής περίθαλψης, κοινωνικών ασφαλίσεων, εμπορικών συναλλαγών, στατιστικής, έρευνας αγοράς, κλπ, να περιλαμβάνονται κανόνες για την αποτελεσματική προστασία των προσωπικών δεδομένων, που θα επιτρέπουν δηλαδή επεξεργασία προσωπικών δεδομένων στο βαθμό που είναι απόλυτος αναγκαίος για τους συγκεκριμένους σκοπούς, που θα σβήσουν η παγώνουν τα δεδομένα όταν δεν απαιτούνται πλέον για τους σκοπούς αυτούς, που θα επιτρέπουν την πρόσβαση μονό σε εξουσιοδοτημένα άτομα, που θα διευκολύνουν την παρακολούθηση της πορείας των δεδομένων προς τους διαφόρους αποδεκτές-χρηστές. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Είναι δυνατό να κατασκευάσει ειδικό λογισμικό για τις ανάγκες των υπηρεσιών έλεγχου, έτσι ώστε να διευκολύνεται και να επιτυγχάνεται ο έλεγχος των δηλώσεων επεξεργασίας που υποβάλλουν οι χρηστές και τις όποιες επιβάλλουν οι περισσότερες ευρωπαϊκές νομοθεσίες και η πρόταση οδηγίας της Ευρωπαϊκής Ένωσης. Είναι προφανές ότι η βιομηχανία λογισμικού θα προχωρήσει προς αυτή την κατεύθυνση όταν υπάρξει σχετική ζήτηση από την αγορά. Και η ζήτηση θα υπάρξει όταν, όπως αναφερθήκαμε η προστασία των προσωπικών δεδομένων θα είναι εμπρός του κοινωνικού προβληματισμού και μέρος τις εμπορικής πολίτικης των επιχειρήσεων. Σε ένα άλλο κλάδο του Δικαίου ,εκείνο της προστασίας της πνευματικής ιδιοκτησίας, οπού τα οικονομικά συμφέροντα για την προστασία των ηλεκτρονικών πνευματικών έργων(βάσεων δεδομένων, υπηρεσιών ψυχαγωγίας,MULTIMEDIA) είναι ήδη ισχυρά, έχουν γίνει σημαντικά

βήματα από την ίδια την τεχνολογία. Χάρη στο υποπρόγραμμα CIED που συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση στα πλαίσια του προγράμματος ESPRIT,οι παραγωγοί τέτοιων έργων έχουν σήμερα την τεχνολογική δυνατότητα να ελέγχουν πλήρως τη χρήση των έργων τους από κάθε κατηγορία χρηστών και να εισπράττουν αυτομάτως το αντίτιμο των δικαιωμάτων τους, ανάλογα με την συγκεκριμένη χρήση και κατηγορία χρηστή. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Για την προστασία των προσωπικών δεδομένων κάποιες μελέτες τεχνολογικού χαρακτήρα έχουν προγραμματίσει στα πλαίσια του προγράμματος της Ε.Ε για την ασφάλεια των πληροφοριών, που έχει ως στόχο την επίτευξη του τρίπτυχου" εμπιστευτικότητα, πληρότητα, διαθεσιμότητα" για τις ηλεκτρονικές πληροφορίες. Μετρά για την ασφάλεια των προσωπικών δεδομένων απαιτούνται βεβαία από κάθε ευρωπαϊκή νομοθεσία και από την πρόταση οδηγίας της Ε.Ε. Αλλά τα μετρά αυτά είναι ένα μικρό μέρος της πιθανής συμβολής της τεχνολογίας στην αποτελεσματική προστασία των προσωπικών δεδομένων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Αν οι νέες τεχνολογίες πληροφοριών αφορούν ένα διαρκώς αυξανόμενο αριθμό ανθρώπινων δραστηριοτήτων και αν η προστασία των προσωπικών δεδομένων είναι ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, τότε οι ανθρωπινές δραστηριότητες που περιλαμβάνουν επεξεργασία δεδομένων η τουλάχιστον ορισμένες από αυτές που θα θεωρηθούν εν δύναμη περισσότερο επιβλαβείς θα πρέπει να συνοδεύονται από έκθεση επιπτώσεων της συγκεκριμένης επεξεργασίας για τα προσωπικά δεδομένα. Αυτό ειδή συμβαίνει με την προστασία του περιβάλλοντος. Συμφώνα με το άρθρο 130 ρ παράγραφος 2 της Ενιαίας πράξης, όπως έχει ενσωματωθεί στην Συνθήκη για την Ευρωπαϊκή Ένωση," οι ανάγκες στο τομέα της προστασίας του περιβάλλοντος πρέπει να λαμβάνονται υπόψη στον καθορισμό και την εφαρμογή των άλλων πολιτικών της Κοινότητας. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Κάτι ανάλογο θα χρειαστεί και για τα προσωπικά δεδομένα και θα συμβάλει θετικά στο έργο των υπηρεσιών έλεγχου, στην άσκηση των δικαιωμάτων τους από τους ιδίους πολίτες και στη συνειδητοποίηση των χρηστών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Όλα όσα αναφέρθηκαν στις προηγούμενες παραγράφους, δηλαδή η θέσπιση τομεακών νομοθετημάτων, η κατάλληλη υποστήριξη των υπηρεσιών έλεγχου, η επιμόρφωση των δικαστικών, η συνειδητοποίηση των πολιτών, η παράγωγη κατάλληλου λογισμικού, η έκθεση για τις επιπτώσεις της επεξεργασίας προσωπικών δεδομένων, θα έχουν μικρή αποτελεσματικότητα αν είναι δυνατή η ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων σε κάποιες τρίτες χώρες. Τεχνικά αυτό είναι εξεταστικά εύκολο, ενώ ο πλήρης προληπτικός έλεγχος της εξαγωγής δεδομένων είναι αδύνατος. Δειγματοληπτικός έλεγχος ή κυρώσεις για παράνομη εξαγωγή που αποκαλύπτεται εκ των υστέρων έχουν βεβαία και κάποια προληπτική επίδραση, αλλά πιθανότητα αφορούν μονό την κορυφή του παγόβουνου. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η Ευρώπη κυρίως η διευρυμένη Ευρωπαϊκή Ένωση με εξαίρεση την Ελλάδα και την Ιταλία προηγείται σημαντικά, σε ότι αφόρα την νομοθεσία προστασίας των προσωπικών δεδομένων, όλων ανεξαιρέτως των τρίτων κρατών, συμπεριλαμβανομένων των κύριων ανταγωνιστών της στο τομέα των νέων τεχνολογιών πληροφόρησης, των ΗΠΑ, της Ιαπωνίας και των ταχέως αναπτυσσόμενων κρατών της Άπω Ανατολής. Αν η κατάσταση αυτή παραμείνει και μεχρί να σημειωθούν οι εξελίξεις που πιθανολογούνται στην παράγραφο 4,τοτε θα κινδυνεύσουν μόνο όχι η ιδιωτική ζωή και τα δικαιώματα των Ευρωπαίων πολιτών αλλά και η ανταγωνιστικότητα των Ευρωπαϊκών εταιριών που επεξεργάζονται προσωπικά δεδομένα και που αφενός υποχρεούνται να λάβουν μέτρα προστασίας που έχουν οικονομικό κόστος και αφετέρου δεν έχουν το δικαίωμα να κάνουν χρήση προσωπικών δεδομένων με την ευχέρεια των ανταγωνιστών τους στις τρίτες χώρες. Θα πρέπει λοιπόν οι διατάξεις των άρθρων 26 και 27 της πρότασης Οδηγίας της Ε.Ε να τηρηθούν με αυστηρότητα, έτσι ώστε να θαμπισθεί επαρκής σχετική νομοθεσία και στης χώρες αυτές. Ήδη παρατηρούνται θετικές εξελίξεις σε ορισμένες Τρεις χώρες, που είναι αποτέλεσμα και της πρότασης οδηγίας. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Ο πολίτης θα πρέπει να έχει ,όταν αυτό είναι δυνατό, δικαίωμα επιλογής ανάμεσα σε λύσεις που περιλαμβάνουν και σε λύσεις που δε περιλαμβάνουν επεξεργασία προσωπικών δεδομένων (π.χ. ανάμεσα σε πληρωμή με πιστωτική κάρτα και τις μετρητοίς).Από την σκοπιά των χρηστών

θα πρέπει να αποφεύγεται η επεξεργασία προσωπικών δεδομένων χωρίς σοβαρό λόγο (και φυσικά να ακολουθούνται οι επιταγές του νομού, εφόσον γίνεται τέτοια επεξεργασία).Οι δυνατότητες των τεχνολογιών δεν αποτελούν επαρκή λόγο για την επεξεργασία προσωπικών δεδομένων, αλλά εργαλείο που θα πρέπει να χρησιμοποιείτε όταν τέτοια επεξεργασία είναι απαραίτητη. Στις περισσότερες χώρες του κώσμου και δυστυχώς στην χωρά μας, η προστασία των προσωπικών δεδομένων δεν έχει βρεθεί μέχρι τώρα, στο επίκεντρο της επικαιρότητας και του δημόσιου ενδιαφέροντος. Η ευκαιρία δίνεται τώρα, στους επομένους μήνες, όταν τα προγράμματα της Ευρωπαϊκής Ένωσης, για την κοινωνία της Πληροφορίας και των ΗΠΑ για την Εθνική Υποδομή Πληροφοριών, θα πάρουν συγκεκριμένη μορφή. Αμφότερα περιλαμβάνουν, στο προκαταρτικό στάδιο, διακηρύξεις υπέρ της προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής. Αν μείνουν στα λόγια μαζί με τις λεωφόρους της πληροφορίας θα ανοίξει ο δρόμος για καταχρήσεις προσωπικών δεδομένων που θα υπομονεύσουν την κοινωνική αποδοχή και την βιωσιμότητα τους. Αν προετοιμαστούν, με σοβαρότητα θα ανοίξουν αναμφίβολα νέους δρόμους για την ανθρωπότητα. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.2 Νέες υπηρεσίες και απόρρητο της επικοινωνίας

Παράλληλα όμως, η ραγδαία εξέλιξη της τεχνολογίας δίνει έναυσμα στην ανάπτυξη νέων φορμών ηλεκτρονικής εγκληματικότητας και προσβολών του απορρήτου της επικοινωνίας και της ιδιωτικής ζωής. Παραδείγματος χάρη, η εισαγωγή της ψηφιακής τεχνολογίας στις τηλεπικοινωνίες επιτρέπει, αφενός, την παροχή στους συνδρομητές επιπλέον διευκολύνσεων, όπως πχ καταστάσεις αναλυτικής χρεώσεις, οπού αναγράφονται οι κληθέντες αριθμοί από την συσκευή του συνδρομητή, ή η διάρκεια κάθε συνομιλίας και η σχετική τιμολόγηση. Η νέα αυτή υπηρεσία είναι καταρχήν επιθυμητή στο μετρό που επιτρέπει σε μια επιχείρηση την καλύτερη διαχείριση του τηλεπικοινωνιακού κόσμου, όπως πχ με την δυνατότητα έλεγχου και διαχωρισμού των επαγγελματικών και προσκοπικών κλήσεων των υπάλληλων της, ενώ παράλληλα επιτρέπει την άρση πιθανών αμφισβητήσεων από τον πελάτη σχετικά με το ύψος των τελών τα όποια χρεώνονται από τον τηλεπικοινωνιακό οργανισμό. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Ταυτόχρονα όμως η αναλυτική αποτύπωση πολλών, ή έστω των τεσσάρων πρώτον ψηφίων των αριθμών που καλούνται από μια συγκεκριμένη συσκευή, καθώς και η διατηρείση των σχετικών στοιχείων στα ηλεκτρονικά αρχεία τιμολόγησης συνδρομητών των τηλεπικοινωνιακών οργανισμών εμπεριέχει το ενδεχόμενο έλεγχου και προσβολής της ιδιωτικής ζωής καλούντων και καλουμένων, με όλες τις συναφείς κοινωνικό-πολιτικές προεκτάσεις. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Παράλληλα, εκτός από τον κίνδυνο προσβολής της ιδιωτικής σφαίρας του ατόμου η συλλογή δεδομένων προσωπικού χαρακτήρα τα οποία αφορούν τους συνδρομητές είναι δυνατόν να χρησιμοποιηθεί άπο τους τηλεπικοινωνιακούς οργανισμούς για καθαρά εμπορικούς σκοπούς ακόμα δε για την επίτευξη αθέμιτου ανταγωνιστικού πλεονεκτήματος σε σχέση με άλλους παρόχους υπηρεσιών. Λογού χάριν, η συλλογή των προτιμήσεων του καταναλωτικού κοινού στα πλαίσια μια υπηρεσίας τηλεαγορών ή Τήλε- ηχοπληροφόρισης είναι δυνατόν να μεταπωληθεί σε εταιρεία direct mail με στόχο την εξατομικευμένη προβολή και προώθηση καταναλωτικών προϊόντων. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Εξεταζόμενο σε μια ευρύτερη προοπτική, το πρόβλημα γίνεται ακόμα πιο σύνθετο στον εργασιακό χώρο οπού ειδικές συσκευές επιτρέπουν τον έλεγχο των επαγγελματικών και των προσωπικών χρήσεων με στόχο με την θεμιτή μείωση των τηλεπικοινωνιακών δαπανών της επιχείρησης, αλλά με κίνδυνο της αθέμιτης της προσωπικής συνδικαλιστικής ελευθερίας, ιδιαίτερα σε περίπτωση μη εξουσιοδοτημένης πρόσβασης και εκμετάλλευσης των ανώτερο αναλυτικών στοιχείων κλήσεων του προσωπικού από τον εργοδότη, το λογιστήριο της επιχείρησης, αλλά και από τυχόν τρίτους. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Σχετικά με το ζήτημα αυτό, το οποίο αντιμετωπίστηκε στα πλαίσια άλλων εννόμων τάξεων, όπως πχ στην Γάλλια, οι ανεξάρτητοι κανονιστική αρχή προστασίας των δεδομένων έχει καθορίσει, με μια σειρά μέτρων, τις τεχνικές και κανονιστικές προδιαγραφές που πρέπει να

τηρούνται από την France Telecom αλλά και από τους ανταγωνιστές της για παρόμοιες επεξεργασίες, η παράβαση των οποίων απαιτεί αυστηρές κυρώσεις για την παραβάτισσα τηλεπικοινωνιακή επιχείρηση. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.3 Ασφάλεια δεδομένων και ηλεκτρονική εγκληματικότητα

Περά από την συνταγματική διάσταση του, η οποία σχετίζεται με την διασφάλιση του απορρήτου της επικοινωνίας και των ανταποκρίσεων το θέμα της ασφάλειας δεδομένων παρουσιάζει αναμφίβολα και μια σημαντικότατη οικονομική διάσταση αυτή αφόρα όχι μονό τους τηλεπικοινωνιακούς οργανισμούς, δημοσίους και ιδιωκτικούς, αλλά και τους διαχειριστές των υποδομών, τους παρόχους υπηρεσιών και τους χρηστές. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Εικόνα 24 ηλεκτρονική εγκληματικότητα

5.3.1 Αθέμιτη πρόσβαση σε τηλεπικοινωνιακές υπηρεσίας

Τα τελευταία χρονιά έχει εξιλεωθεί σε πραγματική μάστιγα για τους τηλεπικοινωνιακούς οργανισμούς σε παγκόσμιο επίπεδο ή με τη βοήθεια εξειδικευμένου λογισμικού αθέμιτη πρόσβαση τρίτων σε μυστικούς κώδικες ή σειριακούς αριθμούς αναγνώρισης συνδρομητών τους. Η προσπέλαση στα απόρρητα ηλεκτρονικά αρχεία των παροχών υπηρεσιών, έχει ως αποτέλεσμα την πραγματοποίηση υπεραστικών συνομιλιών ή την χρήση τηλεματικών υπηρεσιών (πχ διασυνοριακή πρόσβαση σε τηλεπικοινωνιακά δίκτυα και τράπεζες πληροφοριών)με χρέωση του ανυποψίαστου νομικού συνδρομητή. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η αντικειμενική υπόσταση του ανωτέρω εγκλήματος πραγματοποιείται ως εξής: ο αθέμιτος εισβολέας παρεισφρέει δίκτυο διαχείρισης πελατών ή στο σύστημα voice-mail του τηλεπικοινωνιακού οργανισμού ή της συνδρομήτριας εταιρείας και με τη βοήθεια του υπολογιστή του πληκτρολογεί ασταμάτητα διαφορετικούς κώδικες πρόσβασης, μεχρί να ακούσει τον χαρακτηριστικό ήχο που του επιτρέπει τις εξωτερικές κλήσεις. Από τούδε και στο εξής η προσπέλαση στις τηλεφωνικές γραμμές του συγκεκριμένου πελάτη είναι ελεύθερη και ο δράστης πρέπει να τηλεφωνεί σε οποιοδήποτε μέρος του κόσμου με έξοδα του νομίμου δικαιούχου της σύνδεσης. Συχνά μάλιστα η δυνατότητα αθέμιτης πρόσβασης μεταπωλείτε περεταίρω σε ομάδες κακοποιών οι οποίοι πραγματοποιούν τις παράνομες συναλλαγές τους, καθιστώντας πολύ δυσχερή τον εντοπισμό τους, εφόσον διοχετεύσουν τις κλήσεις τους μέσω περισσότερων εταιριών PBXs (private branch exchanges). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.3.2 Το κόστος της αθέμιτης πρόσβασης

Συμφώνα με στοιχειά του Αμερικανικού περιοδικού "Fortune"οι εκατό μεγαλύτερες εταιρίες των ΗΠΑ έχουν καταγγείλει τέτοια φαινόμενα τηλεπικοινωνιακής εγκληματικότητας των οποίων το κόστος,μέχρι των εντοπισμό της προσβολής μέσω ειδικού λογισμικού έλεγχου όγκοι μηνυμάτων ξεπέρασε κατά μέσο όρο τις 25 χιλιάδες δολάρια ανά εταιρία, ποσό το οποίο αντιπροσωπεύει ένα συνολικό ετήσιο κόστος ανωτέρω των 100 εκατομμυρίων δολαρίων. Εκτός όμως της άμεσης της θετικής ζημιάς, οι περιπτώσεις αυτές δίνουν συχνά λαβή και σε περεταίρω δικαστικές διενέξεις μεταξύ τηλεπικοινωνιακών οργανισμών και πελατών σχετικά με την ευθύνη που ανάλογη σε κάθε μέρος και των συνακόλουθων επιμερισμό της ζημιάς. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.4 Η ανάγκη της προστασίας των δεδομένων

Πανόμοια φαινόμενα παρατηρούνται και στην κινητή τηλεφωνία με την πρόσβαση, χάρη σε ειδικές συσκευές ανάγνωσης, σε κωδικούς αριθμούς αναγνώρισης χρηστή (pin)με την "σύλληψη" την κίνηση στα ραδιοκύματα και την μεταγενέστερη χρήση τους, η οποία προσαρμόζεται με προσωπικούς υπολογιστές και ειδικό λογισμικό, σε κλεμμένα ψηφιακά τηλεφωνά, με τον ίδιο το νόμιμο χρηστή ζημιογόνα αποτελέσματα. Στην ίδια κατηγορία ανήκει ακόμα η παγίδευση γραμμών επικοινωνίας για εξ αποστάσεως αντιγραφή λογισμικού ηλεκτρονικών υπολογιστών ή για πρόσβαση σε τραπεζικούς λογαριασμούς τρίτων και πραγματοποίηση παράνομων συναλλαγών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Η επέκταση της μηχανοργάνωσης σε δημόσιο και ιδιωτικό τομέα σε συνδυασμό με την αύξηση του αριθμού των διαθέσιμων δικτύων μεταγωγής δεδομένων διευκολύνει την δημιουργία και εμπόρια ηλεκτρονικών αρχείων με "ευαίσθητες" πληροφορίες προσωπικού χαρακτήρα για τα άτομα και τις επιχειρήσει(πχ οικονομικού και φορολογική κατάσταση, φυλετική προέλευση ,ιατρικά δεδομένα, πιστοληπτική ικανότητα).Η διασύνδεση κρατικών αρχείων (υπουργεία, εφορία, τράπεζες, οργανισμοί κοινωνικής ασφάλισης, αστυνομία κλπ) και η διασταύρωση προσωπικών δεδομένων συντελεί μεν στην πάταξη της γραφειοκρατίες και στον διοικητικό εκσυγχρονισμό, ενέχει όμως παράλληλα το ενδεχόμενο καταχρήσεων σε βάρος του πολίτη. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

Τέτοιου είδους παραβάσεις έγιναν είδη και σχεδιάζονται ακόμα περισσότερες και στην χωρά μας, χωρίς δυστυχώς να συναντήσουν ανάλογες επιδράσεις από τους οικείους κοινωνικούς φορείς. Χαρακτηριστικά παραδείγματα αποτελούν οι αυθαίρετοι σύνδεση του ύψους των ηλεκτρονικών λογαριασμών ελεύθερων επαγγελματιών με την φορολογική ικανότητα τους, η υποχρεωτική χρήση σχεδιαζόμενης "ηλεκτρονικής ταυτότητας" σε κάθε μορφή συναλλαγής, η διασταύρωση των σχετικών στοιχείων ταυτότητας με τον αριθμό φορολογικού μητρώου από το σύστημα TAXIS με αντικείμενο την μηχανοργάνωση των οικονομιών εφοριών κλπ. Στα πλαίσιο αυτό λοιπόν, προβάλλεται αδήριτη η ανάγκη θέσπισης ενός αποτελεσματικού συστήματος τεχνικών διασφαλίσεων, πρώτιστος,(κρυπτογράφηση δεδομένων, κωδικοποίηση ,επίπεδα πρόσβασης, ανά κατηγορία υπάλληλου κλπ)η οποία όμως να συνδυάζεται με την θέσπιση κατάλληλων νομικών διατάξεων με την προστασία των πληροφοριών προσωπικού χαρακτήρα οι όποιες διακινούνται μέσω τηλεπικοινωνιακών δικτύων και υπηρεσιών. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.5 Η νομοθετική δράση των διεθνών οργανισμών

Συνειδητοποιώντας το πρόβλημα αυτό, πρώτοι οι διεθνείς οργανισμοί έχουν από νωρίς αναλάβει κάποιες νομοθετικές πρωτοβουλίες είτε υπό μορφή μη διαζευκτικών συστάσεων(Ο.Ο.Σ.Α) είτε υπό μορφή διεθνών συμβάσεων (όπως η ευρωπαϊκή σύμβαση αρ.108 του συμβούλιου της Ευρώπης "για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα").Η σύμβαση αυτή υπογράφτηκε το 1981 από όλα τα κράτη-μελή του συμβούλιου μεταξύ των οποίων και η Ελλάδα αποτελεί μερί στιγμής το σπουδαιότερο διεθνώς νομοθετικό κείμενο περί προστασίας δεδομένων, πρόσφατα δε κερώθηκε και από την χώρα μας με τον νομό 2068/1992 (ΦΕΚ 118,9 Ιουλίου 1992) και έτσι καταστεί εσωτερικό μας δίκαιο. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.6 Ο μηχανισμός προστασίας

Περιεχόμενο της σύμβασης αποτελεί η οριοθέτηση ενός μηχανισμού προστασίας του ατόμου από αυτοματοποιημένες επεξεργασίες προσωπικών πληροφοριών. Ειδικότερα, στο κείμενο της γίνεται, πρώτον ή αποσαφήνιση ορισμένων βασικών ορών όπως "προσωπική πληροφορία", "ηλεκτρονικό αρχείο" "κύριος του αρχείου", "αυτοματοποιημένη επεξεργασία", κλπ. Η οριοθέτηση του πεδίου εφαρμογής της ακολουθείτε, δεύτερον, από την θέσπιση ορισμένων αρχείων και διαδικασιών προστασίας και ασφάλειας των πληροφοριών (νόμιμη απόκτηση καταχώρηση για ορισμένους νόμιμους και ειδικά ορισμένους σκοπούς, ακρίβεια, προσήκουσα και όχι υπέρμετρη έκταση σε σχέση με επιδιωκόμενους σκοπούς, περιορισμένη χρονική διάρκεια διατήρησης). Το σύστημα προστασίας συμπληρώνεται, τρίτον, από την εισαγωγή ορισμένων νέων δικαιωμάτων του ατόμου (δικαίωμα γνώσης των αυτοματοποιημένων επεξεργασιών που το αφορούν μέσω της υποχρεώσης των φορέων επεξεργασίας, δημοσίων και ιδιωτικών, να δημοσιοποιήσουν το είδος και το περιεχόμενο του κάθε είδους αρχείων που τηρούν, δικαίωμα άρνησης του ατόμου να συναίνεση στη σχεδιασμένη επεξεργασία, δικαίωμα πρόσβασης στα χειροκίνητα ή αυτοματοποιημένα αρχεία δημοσίων και ιδιωτικών φορέων, δικαίωμα διόρθωσης τυχόν ανακριβειών ή σφαλμάτων κλπ). (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

5.7 Η ανεξάρτητη δημοσιά αρχή ελέγχου

Για την διασφάλιση εφαρμογής των ορών της σύμβασης και την διενέργεια των προβλεπόμενων ελέγχων οι όποιοι μπορούν να φτάσουν μεχρί την επιβολή ,με την συνδρομή της δικαστικής αρχής, των αναλόγων κυρώσεων και πρόστιμων κατά των παραβατών, προβλέπεται επίσης η δημιουργία εκ μέρους των κρατών, με την εθνική νομοθεσία, ανεξάρτητων δημοσίων αρχών προστασίας των ατόμων. Οι αρχές αυτές μπορεί να είναι κατά περίπτωση, συλλογικές(όπως πχ η προαναφερθείσα γαλλική CNIL- Εθνική επιτροπή πληροφορικής και ελευθεριών ή η Σουηδική Data inspection)ή μονοπρόσωπες (όπως πχ ο επίτροπος για την προστασία των δεδομένων) έχουν δε ως αποκλειστική αρμοδιότητα των ατόμων από της ενδεχόμενες παρενέργειες ,οι όποιες απορρέουν άπο καταχρήσεις της νέας τεχνολογίας. (Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., 1995)

ΚΕΦΑΛΑΙΟ 6^{ο} ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Σύγχρονες απειλές

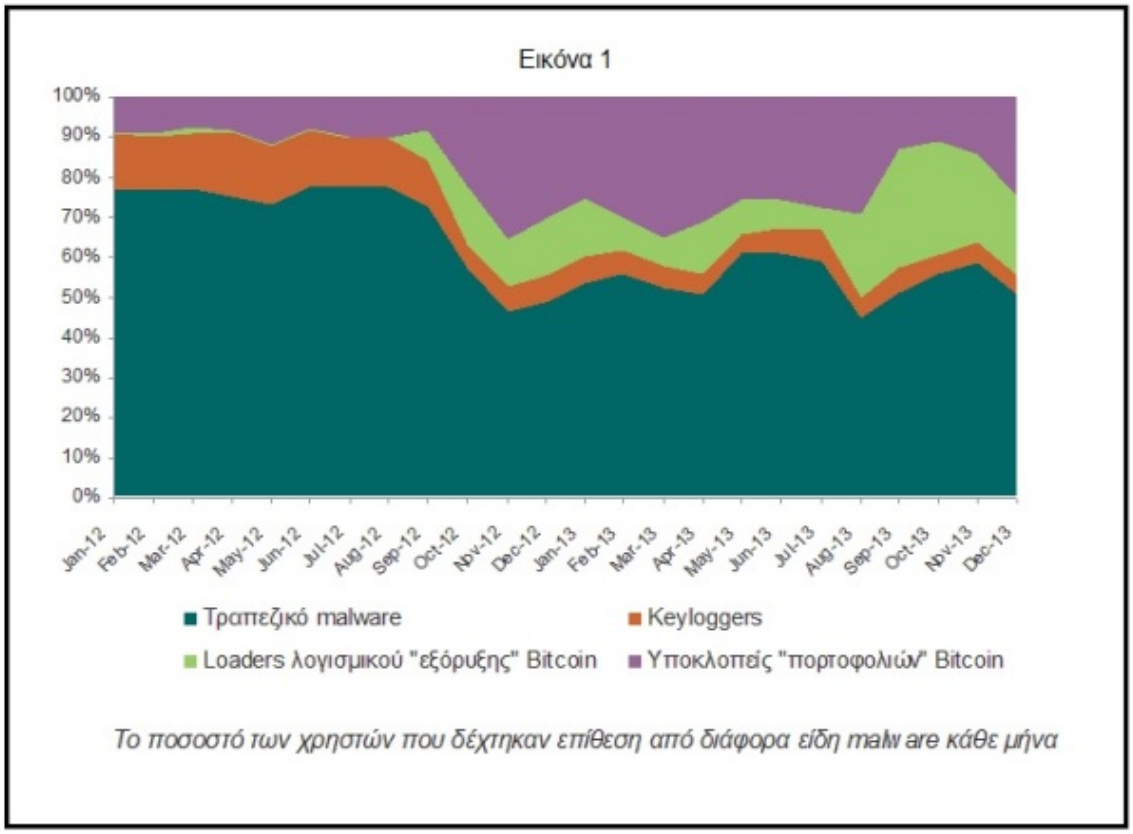
Σύμφωνα με μελέτη της "Financial cyber threats in 2013" της Kaspersky Lab, οι οικονομικές επιθέσεις με κακόβουλα προγράμματα που είχαν ως στόχο το Bitcoin έγιναν εξαιρετικά δημοφιλείς το 2013. Ο αριθμός των επιθέσεων με στόχο το ψηφιακό νόμισμα αυξήθηκε πάνω από 2,5 φορές, αγγίζοντας τα 8,3 εκατομμύρια περιστατικά. (www.infocom.gr)

Εικόνα 25 Kaspersky

Το bitcoin δημιουργήθηκε ειδικά για την πραγματοποίηση ανώνυμων ηλεκτρονικών πληρωμών και έχει γίνει εξαιρετικά δημοφιλές τα τελευταία χρόνια. Στις αρχές του 2013, βάση συναλλαγματικής ισοτιμίας, ένα Bitcoin αντιστοιχούσε σε $13,6. Μέχρι το Δεκέμβριο, έφτασε σε επίπεδα ρεκόρ, ξεπερνώντας τα $1.200. Κατά τη διάρκεια της χρονιάς, σημειώθηκαν αρκετές μεταπτώσεις, αλλά από τον Απρίλιο του 2013 και μετά, η τιμή μονάδας του εικονικού νομίσματος δεν έχει πέσει κάτω από τα $80. Αναπόφευκτα, αυτό προσέλκυσε την προσοχή των απατεώνων. Τα bitcoins αποτελούν συχνά εύκολη λεία για τους ψηφιακούς εγκληματίες. Αν οι χρήστες αποθηκεύουν bitcoins στους υπολογιστές τους σε μη κρυπτογραφημένη μορφή, οι εγκληματίες αρκεί να κλέψουν το αρχείο του «ψηφιακού πορτοφολιού», ώστε να αποσπάσουν πληροφορίες σχετικά με τα «χρήματα» που βρίσκονται σε αυτό και να αποκτήσουν πρόσβαση στο λογαριασμό του θύματος. (www.infocom.gr)

Πάνω από 30 δείγματα malware που σχετίζονταν με οικονομικές επιθέσεις επιλέχθηκαν για την έρευνα της Kaspersky Lab. Εννέα από αυτά αποτελούσαν το πρόγραμμα που είχε σχεδιαστεί για την κλοπή του ψηφιακού νομίσματος. Αυτά τα εννέα κακόβουλα προγράμματα αντιστοίχησαν συνολικά στο 29% του συνόλου των οικονομικών ψηφιακών επιθέσεων που υλοποιήθηκαν με τη χρήση κακόβουλων εφαρμογών. (www.infocom.gr)

Τα εργαλεία που χρησιμοποιούν οι ψηφιακοί εγκληματίες για να κλέβουν bitcoins μπορούν να χωριστούν σε δύο κατηγορίες. Η πρώτη περιλαμβάνει προγράμματα που δημιουργήθηκαν για να κλέβουν αρχεία ψηφιακών πορτοφολιών. Οι εφαρμογές που ανήκουν στη δεύτερη κατηγορία έχουν σχεδιαστεί για να εγκαθιστούν λογισμικό για τη δημιουργία bitcoin (διαδικασία γνωστή ως "mining") από έναν «μολυσμένο» υπολογιστή. Σε απόλυτους αριθμούς, οι κλέφτες «πορτοφολιών» bitcoin πραγματοποίησαν τις διπλάσιες επιθέσεις το 2013. Ωστόσο, η ανάπτυξη των εργαλείων "mining" ήταν πολύ ταχύτερη. (www.infocom.gr)



Εικόνα 26 επιθέσεις από malware

Για την ασφαλή χρήση των ψηφιακών νομισμάτων, οι ειδικοί της Kaspersky Lab προτείνουν την αποθήκευση των αρχείων – «πορτοφολιών» σε κρυπτογραφημένα μέσα. Για μακροχρόνια αποθήκευση, ένας χρήστης μπορεί να μεταφέρει τα αρχεία σε ένα συγκεκριμένο «πορτοφόλι» και να σημειώσει τις λεπτομέρειες σε χαρτί. Είναι επίσης αναγκαίο να προστατεύουν τους υπολογιστές τους ενάντια στα κακόβουλα λογισμικά, με τη χρήση μιας αξιόπιστης, ολοκληρωμένης σουίτας ασφάλειας. (www.infocom.gr)

Οι οικιακοί χρήστες μπορούν να επωφεληθούν από τη χρήση του KasperskyInternetSecurity, μιας πλήρους λύσης ασφαλείας που περιλαμβάνει ολοκληρωμένες τεχνολογίες προστασίας, καθώς και την τεχνολογία SafeMoney, η οποία προστατεύει τα δεδομένα των χρηστών κατά τη διάρκεια τραπεζικών και ηλεκτρονικών πληρωμών. (www.infocom.gr)

Η μελέτη "FinancialCyberThreatsin 2013" αξιοποίησε δεδομένα που παρείχαν οικειοθελώς οι χρήστες του Kaspersky Security Network. Το KasperskySecurityNetwork είναι μια παγκόσμια cloud-based υποδομή, η οποία έχει αναπτυχθεί για την άμεση επεξεργασία αποπροσωποποιημένων δεδομένων σχετικά με τις απειλές που αντιμετωπίζουν οι χρήστες των προϊόντων της KasperskyLab. (www.infocom.gr)

Τον περασμένο Δεκέμβριο, η Kaspersky Lab είχε δημοσιεύσει τις προβλέψεις της σχετικά με το τοπίο των ψηφιακών απειλών το 2014. Μέσα σε μόλις τρεις μήνες, οι ειδικοί της εταιρείας διαπίστωσαν ότι και οι τρεις προβλέψεις τους για τις απειλές εναντίον των τελικών χρηστών είχαν ήδη επιβεβαιωθεί. (www.infocom.gr)

Εικόνα 27 επιθέσεις σε κινητά τηλέφωνα

Συγκεκριμένα, οι ειδικοί της Kaspesky Lab είχαν προβλέψει ότι οι ψηφιακοί εγκληματίες θα στοχοποιούσαν: (www.infocom.gr)

- Την ιδιωτικότητα των χρηστών, με αποτέλεσμα την αύξηση της δημοφιλίας των υπηρεσιών VPN και των Tor-anonymizers. Σήμερα, ο αριθμός των χρηστών που στρέφονται στο Darknet στην προσπάθειά τους να προστατεύσουν τα προσωπικά τους δεδομένα αυξάνεται διαρκώς. Ωστόσο, εκτός από καλοπροαίρετους χρήστες, το Tor εξακολουθεί να γίνεται πόλος έλξης για κακόβουλες δραστηριότητες, καθώς τα ανώνυμα δίκτυα μπορούν να καλύψουν τη δραστηριότητα του malware, τις συναλλαγές σε παράνομες ιστοσελίδες και το ξέπλυμα χρήματος. Για παράδειγμα, τον Φεβρουάριο, η Kaspersky Lab εντόπισε το πρώτο Android Trojan που χρησιμοποιεί ένα domain στην pseudo zone ".onion" ως τοποθεσία Command & Control.
- Τα χρήματά των χρηστών, με τους ειδικούς να εκτιμούν ότι οι ψηφιακοί εγκληματίες θα συνεχίσουν να αναπτύσσουν σχετικά εργαλεία. Η πρόβλεψη επιβεβαιώθηκε τον Μάρτιο, με τον εντοπισμό του Trojan-SMS.AndroidOS.Waller.a. Το συγκεκριμένο Trojan μπορεί να κλέβει χρήματα από ηλεκτρονικά πορτοφόλια QIWI, τα οποία ανήκουν σε κατόχους «μολυσμένων» smartphones. Μέχρι σήμερα, το Trojan αυτό στοχεύει μόνο Ρώσους χρήστες, αλλά μπορεί να διαδοθεί σε κάθε σημείο που τα ηλεκτρονικά πορτοφόλια ελέγχονται μέσω γραπτών μηνυμάτων. Επιπλέον, οι ψηφιακοί εγκληματίες χρησιμοποίησαν και καθιερωμένες μεθόδους, όπως η διάδοση Trojans για φορητές συσκευές που κλέβουν χρήματα με τη βοήθεια κακόβουλων spam. Στην περίπτωση αυτή, το πρόβλημα είναι σαφώς ευρύτερο. Για παράδειγμα, το τραπεζικό mobile Trojan "Faketoken" έχει επηρεάσει χρήστες σε 55 χώρες, συμπεριλαμβανομένης της Γερμανίας, της Σουηδίας, της Γαλλίας, της Ιταλίας, του Ηνωμένου Βασιλείου και των ΗΠΑ. Σημειώνεται ότι ο αριθμός των τραπεζικών mobile Trojans σχεδόν διπλασιάστηκε στο πρώτο τρίμηνο του 2014, φτάνοντας τα 2.503 από 1.321.

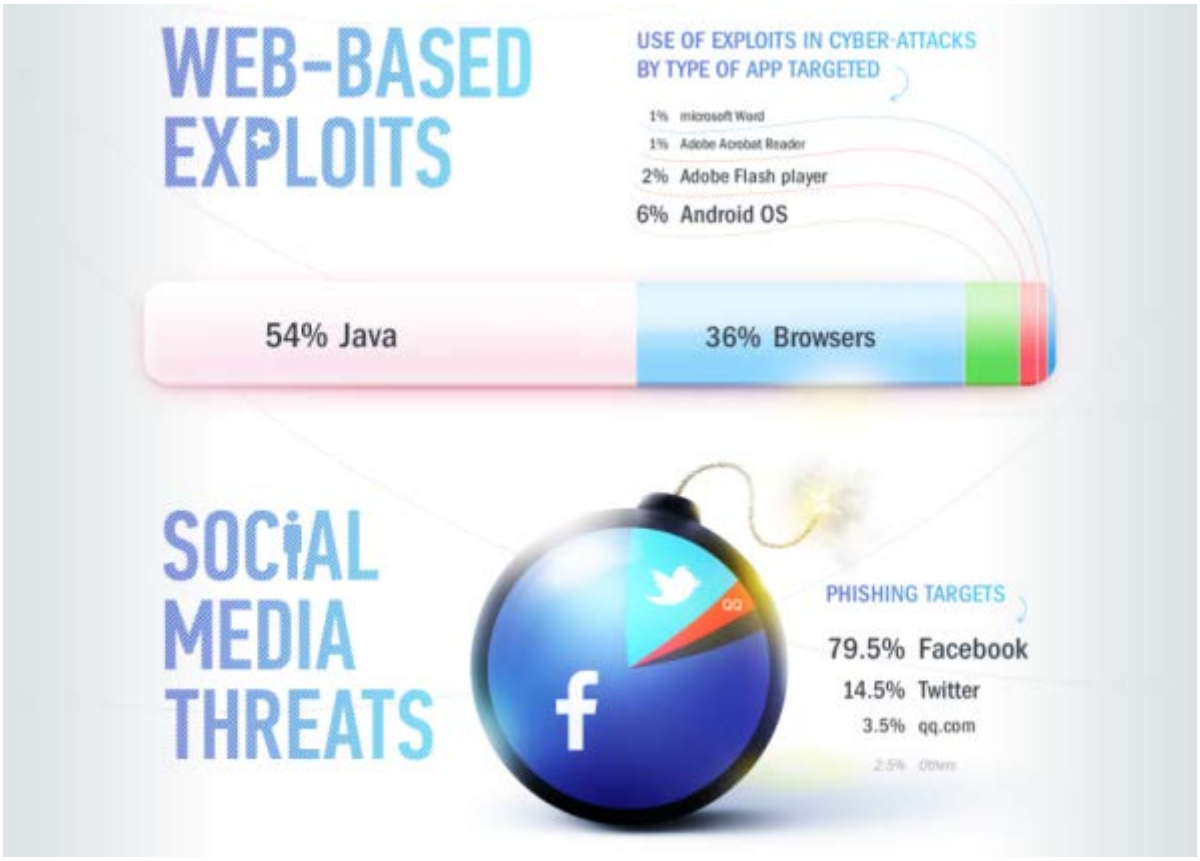
- Τα Bitcoins, με τους ειδικούς να αναμένουν σημαντική αύξηση του αριθμού των επιθέσεων με στόχο τα Bitcoin πορτοφόλια, pools και χρηματιστήρια. Πολλά περιστατικά μέσα στους τρεις πρώτους μήνες του 2014 απέδειξαν ότι η πρόβλεψη ήταν σωστή. Τα πιο σημαντικά από αυτά περιλαμβάνουν τη χρεωκοπία του MtGox, ενός από τα μεγαλύτερα χρηματιστήρια bitcoin, έπειτα από επίθεση χάκερ και την επίθεση στο προσωπικό blog και στο λογαριασμό Reddit του Mark Karpeles, Διευθύνοντος Συμβούλου της MtGox. Με αυτόν τον τρόπο, οι ψηφιακοί εγκληματίες κατάφεραν να δημοσιεύσουν το αρχείο MtGox2014Leak.zip, το οποίο αποδείχτηκε ότι ήταν κακόβουλο λογισμικό με τη δυνατότητα να ψάχνει και να κλέβει Bitcoin πορτοφόλια. Στην προσπάθειά τους να ενισχύσουν τα παράνομα κέρδη τους, οι ψηφιακοί εγκληματίες προσβάλλουν υπολογιστές και χρησιμοποιούν τους πόρους τους για να παράγουν περισσότερα ψηφιακά νομίσματα. Το Trojan.Win32.Agent.aduro, το οποίο κατέλαβε τη δωδέκατη θέση στη λίστα με τα κακόβουλα αντικείμενα που εντοπίστηκαν συχνότερα στο Διαδίκτυο κατά το πρώτο τρίμηνο του 2014, είναι ένα από τα Trojans που χρησιμοποιούνται σε τέτοιου είδους διαδικασίες.

Εικόνα 28 Επιθέσεις σε τράπεζες

Στο πρώτο τρίμηνο του 2014 σημειώθηκε και ένα σημαντικό περιστατικό ψηφιακής κατασκοπείας. Το Φεβρουάριο, η Kaspersky Lab δημοσίευσε την έκθεση της για μια από τις πιο προηγμένες απειλές των ημερών μας, με την ονομασία "The Mask". Βασικός στόχος της ήταν οι εμπιστευτικές πληροφορίες κρατικών υπηρεσιών, πρεσβειών, εταιρειών ενέργειας, ερευνητικών ιδρυμάτων, επενδυτικών εταιρειών και ακτιβιστών από 31 χώρες. Σύμφωνα με τους ερευνητές, η πολυπλοκότητα των εργαλείων που χρησιμοποιήθηκαν από τους εισβολείς και διάφοροι άλλοι παράγοντες υποδεικνύουν ότι η εκστρατεία αυτή θα μπορούσε να είχε κρατική υποστήριξη. (www.infocom.gr)

«Πέρα από την ύπαρξη νέων περιστατικών, παρατηρήσαμε ότι συνεχίστηκαν εκστρατείες που φαίνονταν να έχουν ολοκληρωθεί. Για παράδειγμα, αφού οι ψηφιακοί εγκληματίες είχαν κλείσει όλους τους γνωστούς command servers που εμπλέκονταν στην επιχείρηση Icefog,

εντοπίσαμε μια Java εκδοχή της απειλής. Η προηγούμενη επίθεση είχε στοχοποιήσει κατά κύριο λόγο οργανισμούς στη Νότια Κορέα και την Ιαπωνία, αλλά η νέα εκδοχή ενδιαφερόταν μόνο για οργανισμούς στις ΗΠΑ, αν κρίνουμε από τις διευθύνσεις IP που εντοπίστηκαν», σχολίασε ο Alexander Gostev, Chief Security Expert της Global Research and Analysis Team της Kaspersky Lab. (www.infocom.gr)



Εικόνα 29 επιθέσεις σε browsers

Το πρώτο τρίμηνο σε αριθμούς: (www.infocom.gr)

- Σε ποσοστό 33,2%, οι χρήστες υπολογιστών σε όλο τον κόσμο δέχτηκαν τουλάχιστον μια διαδικτυακή επίθεση κατά τους τελευταίους τρεις μήνες – ποσοστό 5,9% μικρότερο σε σύγκριση την ίδια περίοδο το 2013.
- Το 39% των διαδικτυακών επιθέσεων που εξουδετερώθηκαν πραγματοποιήθηκε μέσω διαδικτυακών πόρων με βάση τις ΗΠΑ και τη Ρωσία. Το συνολικό ποσοστό και για τις δύο αυτές χώρες σημείωσε πτώση 5 ποσοστιαίων μονάδων σε σχέση με το πρώτο τρίμηνο του 2013. Ακολούθησαν η Ολλανδία (10,8%), η Γερμανία (10,5%) και το Ηνωμένο Βασίλειο (6,3%).
- Πάνω από το 99% του mobile malware είχε ως στόχο συσκευές Android. Ο συνολικός αριθμός των mobile κακόβουλων προγραμμάτων σημείωσε αύξηση 1% το τελευταίο τρίμηνο.
- Στο τέλος του 2013, η Kaspersky Lab είχε συγκεντρώσει 189.626 δείγματα mobile malware. Μόνο στο πρώτο τρίμηνο του 2014, προστέθηκαν 110.324 νέα κακόβουλα προγράμματα στη βάση της εταιρείας. Στο τέλος πρώτου τριμήνου, τα δείγματα που έχει συλλέξει η Kaspersky Lab ανέρχονταν σε 299.950.

Η πλήρης έκθεση της Kaspersky Lab για το τοπίο των απειλών στο πρώτο τρίμηνο του 2014 είναι διαθέσιμη στην ηλεκτρονική διεύθυνση securelist.com.

6.2 Συμπεράσματα

Η κρυπτογράφηση των ασύρματων δικτύων έχει φτάσει πλέον σε ικανοποιητικά επίπεδα. Αν χρησιμοποιηθούν οι νέες τεχνικές και τεχνολογίες, τότε ένα τέτοιο δίκτυο μπορούμε να πούμε ότι θα είναι πρακτικά απαραβίαστο. Για να είναι κάτι τέτοιο εφικτό θα πρέπει να συντρέχουν μία σειρά από τις παρακάτω προϋποθέσεις: (Βιολέττας Γ., 2008)

1. Πρέπει οπωσδήποτε να χρησιμοποιείται ως πρωτόκολλο κρυπτογράφησης του δικτύου, τουλάχιστον το WPA, με προτιμητέο το WPA2.
2. Πρέπει να επιλέγεται ως μυστική λέξη-κλειδί του δικτύου μία λέξη που να μην υπάρχει σε λεξικό και να είναι ικανοποιητικού μεγέθους (μπορεί να είναι μήκους 20 χαρακτήρων). Πρέπει επίσης να περιέχονται στην λέξη κάποια γράμματα σε κεφαλαία, και κάποια σύμβολα (8,&,^,% $ κτλ).
3. Η μυστική λέξη-κλειδί θα πρέπει να αλλάζει κατά τακτά χρονικά διαστήματα. Έτσι αποφεύγονται και οι επιθέσεις λεξικού, αλλά και οι πολύ πιθανές διαρροές λόγω του ανθρώπινου παράγοντα.
4. Σε καμία περίπτωση δεν πρέπει να χρησιμοποιείται πλέον το πρωτόκολλο WEP. Είναι τελείως ανασφαλές και η χρήση του ισοδυναμεί με την μη χρήση κρυπτογραφικής μεθόδου.

Επίσης τα δίκτυα τέταρτης γενιάς αναμένεται να προσφέρουν στους χρήστες όλα όσα δεν κατάφεραν να δώσουν τα προηγούμενα δίκτυα. Θα προσφέρουν υπηρεσίες πολυμέσων με αλληλεπίδραση με το χρήστη, ασύρματο Internet, υψηλότερους ρυθμούς μετάδοσης δεδομένων, εξαιρετική ποιότητα παροχής υπηρεσιών (QoS), παγκόσμια κινητικότητα και φορητότητα υπηρεσιών σε χαμηλό κόστος. Τα ασύρματα συστήματα 4G θα εξυπηρετούν στο μέλλον τις ανάγκες για υψηλές ταχύτητες μετάδοσης δεδομένων και ευρεία γεωγραφική κάλυψη, προσεγγίζοντας έτσι τον στόχο για επικοινωνία από οποιοδήποτε σημείο της γης, οποιαδήποτε χρονική στιγμή και κάτω από οποιεσδήποτε συνθήκες. (Βιολέττας Γ., 2008)

Τα δίκτυα που θα χρησιμοποιούνται, πρόκειται να αποτελούνται εξ' ολοκλήρου από κυκλώματα μεταγωγής πακέτου, ενώ όλα τα στοιχεία του δικτύου θα είναι ψηφιακά και θα υποστηρίζουν το πρωτόκολλο IPv6. Ένας από τους πρωταρχικούς στόχους θα είναι η παροχή συμβατότητας και ενδολειτουργίας με τα διαφορετικά κινητά και ασύρματα δίκτυα (νέα και παλαιά). Η τέταρτη γενιά ασύρματων δικτύων πρόκειται να δημιουργήσει ένα ετερογενές δίκτυο, περιλαμβάνοντας πολλά διαφορετικά δίκτυα πρόσβασης και τερματικά τελικών χρηστών. Το ετερογενές δίκτυο θα επιτρέψει την εισαγωγή και παροχή πρόσβασης σε πολυάριθμες και πλούσιες σε χαρακτηριστικά υπηρεσίες, ενσωματώνοντας στο ίδιο περιβάλλον τα δίκτυα 2ης και 3ης γενιάς. Βασικό χαρακτηριστικό των ετερογενών δικτύων θα είναι η χωρίς ασυνέχεια μετάβαση από το ένα σύστημα στο άλλο. (Βιολέττας Γ., 2008)

Η ανάπτυξη των συστημάτων τέταρτης γενιάς θα απαιτήσει τη χρήση νέων τεχνολογιών σε πολλούς τομείς, τις ραδιοσυχνότητες και στη διαχείριση δικτύων. Έχουν ήδη σχεδιαστεί πρωτοποριακές λύσεις που θα αντιμετωπίσουν αυτές τις νέες προκλήσεις για παράδειγμα το Ipv6, OFDM (Orthogonal frequencydivision multiplexing), MIMO (Multiple Input Multiple Output) και οι έξυπνες κεραίες και έχουν αξιολογηθεί σε σύγκριση με συμβατικές προσεγγίσεις επιδεικνύοντας πολύ βελτιωμένα χαρακτηριστικά. Η ευρεία χρησιμοποίηση της θα εξαρτηθεί από το συνδυασμό απόδοσης, κόστους και ολοκλήρωσης με τα ήδη υπάρχοντα τηλεπικοινωνιακά συστήματα. Η σημερινή τεχνολογία αιχμής μπορεί τεχνολογικά να κάνει πραγματικότητα το παραπάνω όραμα των κινητών επικοινωνιών 4G, επιπλέον πρέπει να επιτευχθούν και στόχοι της:

- Δημιουργία νέων, ελκυστικών υπηρεσιών από τους παρόχους υπηρεσιών και περιεχομένου.
- Ελκυστικά μοντέλα χρέωσης από τους δικτυακούς παρόχους πρόσβασης και υπηρεσιών.
- Ενημέρωση και εκπαίδευση των χρηστών και εξοικείωση τους με τη νέα τεχνολογική πραγματικότητα, ώστε να είναι σε θέση να αξιοποιούν στο μέγιστο βαθμό τις νέες υπηρεσίες για βελτίωση του επιπέδου της ζωής τους.

Βιβλιογραφία

Ιστοσελίδες

http://datalabs.edu.gr/Forum/default.aspx?g=posts&t=359
http://www.ebusinessforum.gr/old/content/downloads/Wi-Fi-Guide-final.part1.pdf
http://www.egovplan.gr/?page_id=14
http://www.icsd.aegean.gr/website_files/metaptyxiako/617630519.pdf
http://www.icsd.aegean.gr/website_files/proptyxiako/871591340.pdf
http://www.infocom.gr/2014/04/30/ragdaia-aujhsh-online-epithesewn-me-stoxo-to-bitcoin/15767/
http://www.infocom.gr/2014/04/25/oi-psifiakes-apeiles-sto-prwto-trimhno-tou-2014/15615/
http://greg61.gr/blog/%CE%B7-%CE%B3%CF%89%CE%BD%CE%B9%CE%AC-%CF%84%CE%BF%CF%85-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84/%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD-%CE%BA%CE%B1%CE%B9-%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD/%CE%BA%CE%B5%CF%86%CE%AC%CE%BB%CE%B1%CE%B9%CE%BF-3-%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%83%CF%84%CE%B1-%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%B1-%CF%85%CF%80%CE%BF%CE%BB%CE%BF/
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
http://el.wikipedia.org/wiki/%CE%A6%CF%81%CF%85%CE%BA%CF%84%CF%89%CF%81%CE%AF%CE%B1

Ξένη βιβλιογραφία

Barken, L. (2003). How Secure is Your Wireless Network? Prentice Hall PTR.
Flickenger, R., Wireless Hacks. O'Reilly, 2003
Frankel, S., Bemard, E., Les, O., & Scarfone, K. (2007). Establishing Wireless Robust Security Networks: A Guide to 802.11i. Special Publication 800-97.
IEEE 802.11 WG, IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), International Standard [for] Information Technology - Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 2007
Peikari C. & Fogie S., Maximum Wireless Security, 2002
Stallings William Ασύρματες Επικοινωνίες και Δίκτυα, Εκδ. Τζιόλα
Tanenbaum, A. S. (2000). Δίκτυα Υπολογιστών. Αθήνα: Εκδόσεις Παπασωτηρίου.

Ελληνική βιβλιογραφία

Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζανόγλου Β., Ασφάλεια Πληροφοριών - Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, Εκδόσεις Νέων Τεχνολογιών.
Βιολέττας Γεώργιος, Θεοδώρου Τρύφων, Στεφανίδης Γεώργιος, «Η χρήση κρυπτογραφικών μεθόδων στα σύγχρονα ασύρματα δίκτυα», Πανεπιστήμιο Μακεδονίας, Μεταπτυχιακό Εφαρμοσμένης Πληροφορικής, 2008.
Γκρίτζαλης Σ., Λαμπρινουδάκης Κ., Μήτρου Λ., Κάτσικας Σ., Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, , 2010, Αθήνα, Εκδόσεις Παπασωτηρίου.
Κανάτας Αθ., Κωνσταντίνου Φ., Πάντος Γ., Συστήματα κινητών επικοινωνιών, Παπασωτηρίου 2008

Κάτος Β. – Στεφανίδης Γ. , Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, ΖΥΓΟΣ, 396, 2003
Μαρκομανωλάκη Αικατερίνη, Πτυχιακή εργασία «Ασφάλεια σε ασύρματα δίκτυα 802.11», Ηράκλειο 2010, ΤΕΙ Κρήτης
Πάλλης Ε., Εισαγωγή στα Ασύρματα Δίκτυα. Ηράκλειο Κρήτης: Τμήμα Εφαρμοσμένης Πληροφορικής, 2000
Σιωζοπούλου Θ., Μελέτη και Προσομοίωση Προχωρημένων συστημάτων WCDMA, Αθήνα 2006