ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Ασφάλεια στα ασύρματα δίκτυα Wi-Fi

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Παπαϊωάννου Χ. Μάρκος (ΑΜ:9261)
Χαρωνάς Θ. Αχιλλέας (ΑΜ:5912)

ΕΠΟΠΤΗΣ ΚΑΘΗΓΗΤΗΣ : ΡΙΖΟΣ ΓΕΩΡΓΙΟΣ

Άρτα, Ιούνιος 2014

Η εργασία αυτή αφιερώνεται στις οικογένειες μας και τους φίλους μας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

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

ΠΑΠΑΪΩΑΝΝΟΥ Χ. ΜΑΡΚΟΣ.
ΧΑΡΩΝΑΣ Θ. ΑΧΙΛΛΕΑΣ

ΠΕΡΙΛΗΨΗ

Σε αυτή την εργασία γίνεται μία ανάλυση των ασυρμάτων δικτύων wi-fi. Παρουσιάζεται ο εξοπλισμός, η αρχιτεκτονική, τα πρωτόκολλα που χρησιμοποιούν και κυρίως τα επίπεδα ασφάλειας που παρέχουν. Αναφέρονται τα προβλήματα ασφάλειας που αντιμετωπίζουν και απειλές που μπορούν να βλάψουν το δίκτυο. Παρουσιάζονται τεχνολογίες ασφάλειας που χρησιμοποιούνται ως άμυνα σε τυχόν επιθέσεις και γίνεται επίδειξη ορισμένων επιθέσεων σε ένα δίκτυο wi-fi.

Στο πρώτο κεφάλαιο αναφέρονται γενικές και ιστορικές πληροφορίες σε σχέση με ταδίκτυα, τον τρόπο μετάδοσης πληροφορίας, τις κατηγορίες με κριτήριο την έκταση που καταλαμβάνουν και τον τρόπο πρόσβασης.

Στο δεύτερο κεφάλαιο γίνεται αναφορά στα δίκτυα wi-fi. Παρουσιάζεται η εξέλιξη τους, τα πλεονεκτήματα ασύρματης δικτύωσης αλλά και τα μειονεκτήματα. Γίνεται μία αναδρομή στο πρότυπο ασυρμάτων δικτύων IEEE 802.11 και οι αλλαγές- βελτιώσεις που προστέθηκαν στην πάροδο του χρόνου. Διαπιστώνεται η ανάγκη για wi-fi δικτύωση και το κοινό που την επιλέγει. Παρουσιάζεται ο εξοπλισμός και η αρχιτεκτονική τους και επισημαίνονται γενικοί τύποι ασύρματης δικτύωσης, πέρα του wi-fi.

Το τρίτο κεφάλαιο επικεντρώνεται στις τεχνολογίες ασφάλειας ενός wi-fi δικτύου. Αναλύονται οι μέθοδοι ασφαλείας που χρησιμοποιούνται με κριτήριο τα πλεονεκτήματα και τα μειονεκτήματα τους. Παρουσιάζονται οι διαδικασίες κρυπτογράφησης κάθε τεχνολογίας και βελτιώσεις αυτών των με την εξέλιξη τους ανάλογα με τις ανάγκες ασφάλειας.

Στο τέταρτο κεφάλαιο επισημαίνονται επιθέσεις που στοχεύουν σε ασύρματα δίκτυα wi-fi και δημιουργούν αμφιβολίες για την ασφάλεια τους. Παρουσιάζονται οι κατηγορίες επιθέσεων και τίτλοι επιθέσεων ανά κατηγορία.

Στο πέμπτο κεφάλαιο γίνεται επίδειξη κάποιων επιθέσεων. Αναλύονται τα βήματα κάθε επίθεσης και παρουσιάζονται τα αποτελέσματα τα της. Για λόγους τις επίδειξης χρησιμοποιείται ένα οικιακό δίκτυο wi-fi και το λειτουργικό BackTracktης Linux

Στο τελευταίο κεφάλαιο γίνεται μια ανακεφαλαίωση της εργασίας, καταγράφονται τα αποτελέσματα της και οι δυνατότητες για εξέλιξη πάνω στον τομέα των ασυρμάτων δικτύων.

ΚΕΦΑΛΑΙΟ 1 - ΓΕΝΙΚΑ

1.1 ΕΙΣΑΓΩΓΗ

Η επικοινωνία είναι ο τρόπος ανταλλαγής πληροφοριών. Οι ηλεκτρονικοί υπολογιστές είχαν σαν σκοπό την επεξεργασία πληροφορίας. Με την εξέλιξη της τεχνολογίας, κατά τον $20^{ο}$ και $21^{ο}$ αιώνα, επιτεύχθηκε η απομακρυσμένη επικοινωνία και έφτασε στα σημερινά επίπεδα. Σιγά, σιγά προέκυψε και η ανάγκη μετάδοσης πληροφορίας, πράγμα που οδήγησε στην δημιουργία δικτύων. Ως δίκτυο ορίζεται η επικοινωνία μεταξύ δύο ή περισσότερων ηλεκτρονικών υπολογιστών που μπορούν να ανταλλάσουν δεδομένα.

Η χρήση της τεχνολογίας είναι πλέον κάτι καθημερινά απαραίτητο. Κάτι που κάποτε αφορούσε μία ομάδα ανθρώπων , τώρα πλέον αφορά όλο το κοινωνικό σύνολο.Ανάλογα με την κατανόηση και την εξοικείωση του χρήστη διαβαθμίζονται και οι απαιτήσεις. Κρίνεται πλέον αναγκαία η αμφίδρομη μετάδοση πληροφοριών, η συλλογή δεδομένων και οι επικοινωνία ανάμεσα στους τελικούς χρήστες. Αυτό είχε σαν αποτέλεσμα την δημιουργία διαφόρων δικτύων που κατέληξαν σε αυτό που ονομάζεται διαδίκτυο. Η ποικιλία των τερματικών όπως σταθεροί Η/Υ, φορητοί Η/Υ , smartphones, tablets , PDAs, διαμόρφωσαν και τις ανάλογες κατηγορίες δικτύων σύμφωνα με τον τρόπο μετάδοσης, τη φυσική τους κάλυψη και την ασφάλεια πρόσβασης.

Παρακάτω φαίνονται πιο αναλυτικά οι κατηγορίες που αναφέρθηκαν.

- Τρόπος μετάδοσης: Τα δίκτυα χωρίζονται σε ενσύρματα και ασύρματα ανάλογα με το μέσο μετάδοσης. Ενσύρματα μέσα: Ομοαξονικά, οπτικές ίνες, καλώδια UTP-STP, Ασύρματα μέσα : ατμόσφαιρα.

- Γεωγραφική κάλυψη: Τα δίκτυα χωρίζονται σε Τοπικά (LocalAreaNet. – LAN), Μητροπολιτικά (MetropolitanAreaNet. –MAN) και Ευρείας περιοχής δίκτυα (WideAreaNet. – WAN). Τα παραπάνω δίκτυα υποστηρίζονται και ασύρματα (WLAN, WMANκαι WWAN).

- Τρόπος πρόσβασης:Τα δίκτυα αυτά χωρίζονται σε ιδιωτικά (Privateaccess) και δημόσια (PublicAccess).

Η διαφοροποίηση στον τρόπο μετάδοσης της πληροφορίας είναι το φυσικό μέσο μετάδοσης Στην ενσύρματη μετάδοση απαιτείται κάποια καλωδίωση, αντίθετα στην ασύρματη επίτευξη της χρησιμοποιούνται ραδιοσυχνότητες ή υπέρυθρες ακτίνες. Λόγω της δυνατότητας που παρέχουν στην κάλυψη μεγαλύτερηςγεωγραφικής έκτασης και της υπεροχής τους, όσον αφορά το εύρος ζώνης (bandwidth), οι ραδιοσυχνότητες (RF) είναι αρκετά ποιό διαδεδομένες. Η μετάδοση γίνεται με ηλεκτρομαγνητικά κύματα σε συχνότητα 2.5GHzή 5GHz.

Τα ασύρματα δίκτυα , για την ορθή τους λειτουργία, απαιτούν ανάλογα πρωτόκολλα με αυτά των ενσύρματων. Πρωτόκολλα για την ασφάλεια μετάδοσης δεδομένων, προστασία σε ενέργειες παραβίασης, και την εξασφάλιση άμεσης επικοινωνίας με ενσύρματα δίκτυα.

Η σύνδεση σε ασύρματο δίκτυο πυροδοτήθηκε και από την εμπορική παραγωγή ασυρμάτων συσκευών. Όλο και περισσότερες τέτοιες συσκευές βρίσκονται καθημερινά σε χρήση από το καταναλωτικό κοινό, με την απαίτηση ασυρμάτου δικτύου πράγμα που οδηγεί σε μια πλήρη εγκατάσταση ασύρματης δικτύωσης στην καθημερινότητα.

Ποιό είναι όμως το επίπεδο ασφάλειας αυτής της τεχνολογίας;

1.2 ΣΤΟΧΟΣ

Τα ασύρματα δίκτυα υπάρχουν πλέον σε κάθε προσωπικό και εργασιακό χώρο. Σε χώρους μαζικής εστίασης, χώρους αναμονής και η εμβέλεια τους έχει αρχίσει να καλύπτει όλο και μεγαλύτερη γεωγραφική κλίμακα.

Σε αυτή την πτυχιακή εργασία θα μελετηθεί η ασφάλεια αυτών των δικτύων, τα πρωτόκολλα που χρησιμοποιούν και η αρχιτεκτονική τους δομή. Θα ερευνηθούν οι αδυναμίες αλλά ακόμα και οι τρόποι προστασία τους, η εξασφάλιση ακεραίας μετάδοσης της πληροφορίας. Θα ερευνηθούν τυχόν απειλές που μπορεί να δεχθεί ένα ασύρματο δίκτυο και τρόποι προστασίας.

ΚΕΦΑΛΑΙΟ 2 – ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ Wi-Fi

2.1 ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Ως ασύρματο δίκτυο ορίζεται η επικοινωνία ,μέσω ηλεκτρομαγνητικών κυμάτων, 2 σταθερών ή κινητών συσκευών επιτρέποντας της αμφίδρομη ανταλλαγή δεδομένων.

Οι πρώτες ασύρματες συσκευές δεν είχαν επαρκή ταχύτητα μετάδοσης δεδομένων έτσι ώστε να χαρακτηριστούν αποδοτικές. Σε αντίθεση, οι σύγχρονες συσκευές μπορούν να στείλουν τη πληροφορία σε επιθυμητές ταχύτητες.

Εικόνα 1-Ασύρματες συσκευές

Πλέον παρατηρούνται ασύρματα δίκτυα που έχουν μεγάλη γεωγραφική κάλυψη και εμβέλεια π.χ. ένα συγκρότημα κτηρίων ή ακόμα και μία πόλη. Έχουν κατακτήσει ένα μεγάλο κομμάτι

της αγοράς δικτύων καθώς πολλές επιχειρήσεις και οργανισμοί έχουν αντιληφθεί την ανάγκη επέκτασης των ενσύρματων δικτύων με ασύρματη τεχνολογία.

Οι ασύρματες συσκευές έχουν πληθύνει λόγω χαμηλού κόστους, της υπολογιστικής τους δύναμης, ανάλογη των σταθερών συσκευών, τη ευκολία στη μεταφορά και τις απαιτήσεις της εποχής για συνεχή μετακίνηση του χρήστη.

2.2 Wi-Fi

Τα ασύρματα δίκτυα έκαναν την εμφάνιση τους τη δεκαετία του 1990.Σκοπός ήταν η επικοινωνία ανάμεσα σε συσκευών χωρίς να είναι απαραίτητη η καλωδίωση. Αυτό είχε σαν αποτέλεσμα την ανάπτυξη διαφόρων προτύπων IEEEκαι πιο συγκεκριμένα την έκδοση 802.11

Το IEEE 802.11, το οποίο δημιουργήθηκε τον Ιούνιο του 1997, είχε ταχύτητα 2Mbps και είναι το αρχικό πρότυπο στο οποίο στηρίχθηκαν μέχρι τώρα τα ασύρματα δίκτυα Ethernet. Είναι το πιο διαδεδομένο πρότυπο για την εγκατάσταση ασυρμάτου δικτύου και αφορά τα δύο τελευταία επίπεδα το OSI: MACκαι φυσικό επίπεδο.

Η έκδοση IEEE 802.11bδημιουργήθηκε τον Ιούλιο του 1998 και έχει ταχύτητα 11Mbpsαυτή και ονομάστηκε Wi-Fi. Το Wi-Fi προέρχεται από τα αρχικά των Wireless Fidelity (Ψηφιακή Πιστότητα) και έχει επικρατήσει σαν όρος για το υψηλής συχνότητας ασύρματο τοπικό δίκτυο (WLAN). Βασικά αποτελεί ένα ασύρματο τρόπο διασύνδεσης, ενώ δίνει την δυνατότητα σύνδεσης και με το Internet.

Όταν επιτεύχθηκε η παραπάνω ταχύτητα μετάδοσης δεδομένων ιδρύθηκε η WirelessEthernetCompatibilityAlliance γνωστή και ως WECA.. Σκοπός της ήταν η πιστοποίηση ασυρμάτων συσκευών που μπορούσαν να υποστηρίξουν το IEEE 802.11b. Επιπλέον πιστοποιούσε την δυνατότητα συνύπαρξης ασυρμάτων συσκευών , διαφόρων κατασκευαστών, με κατασκευή πάνω στο πρότυπο 802.11b.

Μέλη της WECA ήταν εταιρίες λογισμικού, υπολογιστικών συστημάτων , κατασκευαστές η-ημιαγωγών όπως οι :3Com, Aironet, Apple, Breezecom, Cabletron, Compaq, Dell,Fujitsu,IBM, Intersil, LucentTechnologies, Wayportκαι Zoom.

Σαν αποτέλεσμα, η αγορά προμηθεύτηκε με πλήθος ασυρμάτων συσκευών που έφεραν την ένδειξη Wi-Fi. Αυξάνοντας έτσι την επιθυμία για ασύρματα δίκτυα και AccessPoints.

Ένα δίκτυο Wi-Fiέχει όλες τις δυνατότητες ενός ενσύρματου δικτύου, επιπλέον παρέχει ευελιξία, μικρό κόστος και ευκολία πρόσβασης.

Στις μέρες μας, σημεία Wi-Fi βρίσκονται παντού. Όλο και περισσότερες συσκευές είναι πλέον συνδεδεμένες σε ασύρματα δίκτυα, με πρόσβαση στο διαδίκτυο. Στον χρήστη της κάθε ασύρματης συσκευής είναι αυτονόητη η σύνδεση σε στο διαδίκτυο μέσω κάποιου accesspoint, το οποίο είναι και η ερμηνεία ενός απλού χρήστη για το τι είναι το Wi-Fi.

Εικόνα 2-Λογότυπο Wi-fi

2.2.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ

Παρακάτω αναφέρονται κάποια από τα κυριότερα πλεονεκτήματα των ασυρμάτων δικτύων. Ευκολία πρόσβασης, ευελιξία κίνησης, μειωμένο κόστος, συμβατότητα, διασύνδεση, ευκολία εγκατάστασης. Πιο αναλυτικά:

- **Ευκολία πρόσβασης:** Η λογική των ασυρμάτων δικτύων είναι να επιτρέπει στον χρήστη πρόσβαση στο δίκτυο από σχεδόν οποιαδήποτε τοποθεσία ,χωρίς να πρέπει να βρίσκεται στο χώρο εργασίας ή στο σπίτι. Με την ραγδαία αύξηση των φορητών συσκευών αυτό είναι ένα σημαντικό πλεονέκτημα.

- **Ευελιξία κίνησης:** Τα ασύρματα δίκτυα υποστηρίζουν τη λήψη και αποστολή δεδομένων τη στιγμή που η τερματική συσκευή βρίσκεται σε κίνηση και εντός της εμβέλειας του δικτύου. Η ευελιξία αυτή, δίνει ευκαιρίες στις οποίες αδυνατούν τα ενσύρματα δίκτυα.

- **Μειωμένο κόστος:** Η εγκατάσταση ενσύρματης καλωδίωσης είναι, αρχικά, φθηνότερη από την εγκατάσταση αναγκαίουεξοπλισμού για τη δημιουργία ασύρματου δικτύου. Σε βάθος χρόνου όμως παρατηρείται πως η συμφέρουσα λύση είναι η ασύρματη καθώς το συνολικό κόστος είναι χαμηλότερο σε χώρους όπου είναι απαραίτητες οι μετακινήσεις ή υπάρχουν συχνές μετατροπές.

- **Συμβατότητα:** Ένα ασύρματο δίκτυο διαμορφώνεται ανάλογα με τις απαιτήσεις της εγκατάστασης που θα τοποθετηθεί αλλά την εφαρμογή που θα υποστηρίξει. Η εγκατάσταση μπορεί να τροποποιηθεί από ένα μικρό δίκτυο σε ένα πλήρως καταρτισμένο για να υποστηρίξει εκατοντάδες χρήστες.

- **Διασύνδεση:** Ανάμεσα σε δύο ασύρματα δίκτυα είναι πολύ πιο εύκολο να πετύχουμε ζεύξη σε σχέση με δύο ενσύρματα δίκτυα. Για παράδειγμα αν θέλαμε να συνδέσουμε δύο ,σχετικά, απομακρυσμένα κτίρια, όπου το κάθε ένα έχει από ένα δίκτυο, είναι προτιμότερη μία ασύρματη point-to-point.

- **Ευκολία εγκατάστασης:** Η ενσύρματη δικτύωση απαιτεί αρκετό χρόνο και κόπο, λόγω της εγκατάστασης καλωδίων ώστε κάθε συσκευή να ανήκει στο δίκτυο, κάτι που δεν αφορά καθόλου ένα ασύρματο δίκτυο ,όπου το μέσω μεταφοράς είναι η ατμόσφαιρα. Επιτρέπει τη διασύνδεση πολλών δικτύων σε περιπτώσεις που η ενσύρματη εγκατάσταση παρουσιάζει πρόβλημα. Προτείνεται δηλαδή για την κάλυψη μεγάλων εγκαταστάσεων (π.χ. πανεπιστήμια, εταιρείες κ.α.) ή και σε κτήρια που δεν δέχονται τροποποιήσεις

2.2.2 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ

Λόγω της ιδιαίτερης φύσης των ασυρμάτων δικτύων, να χρησιμοποιούν την ατμόσφαιρα ως μέσο επικοινωνίας και οι πληροφορίες να αναμεταδίδονται με την μορφή ραδιοσυχνοτήτων, έχει σαν αποτέλεσμα την ευαισθησία των δικτύων σε διάφορα φαινόμενα παρεμβολής. Ως φαινόμενα παρεμβολής ,ορίζονται οι συνθήκες που αλλοιώνουν την επικοινωνία ανάμεσα στα συνδεδεμένα τερματικά. Παρακάτω αναφέρονται κάποια από αυτά τα προβλήματα.

- **Παρεμβολή λόγω πολλαπλών διαδρομών**:Η πληροφορία στα ασύρματα δίκτυα μεταδίδεται με την μορφή σήματος ,πολλές φορές ,παρατηρείται το φαινόμενο παρεμβολής ανακλώμενων σημάτων από διάφορες επιφάνειες ή σχετικά εμπόδια. Στην μπάντα των 2.4GHz,όπου και λειτουργούν, μπορούν ακόμα και τα ίδια να προκαλέσουν παρεμβολές σε άλλες συσκευές που εκπέμπουν στην ίδια συχνότητα. Συνήθως προβλήματα παρεμβολής δημιουργούνται λόγω λανθασμένων επιλογών ως προς την επιλογή του εξοπλισμού προκειμένου να δημιουργηθεί το δίκτυο.

- **Υγεία**:Τα ασύρματα δίκτυα μεταδίδουν την πληροφορία με την μορφή σημάτων, θα πρέπει να περιορίζουν την ισχύ τουεκπεμπόμενου σήματος στο ανώτερο όριο των 2 Watt, για λόγους υγείας. Ο εξοπλισμός που θα χρησιμοποιηθεί θα πρέπει να πληροί τα κριτήρια και τους περιορισμούς των διεθνών συνθηκών όπως και του Ευρωπαϊκού Ινστιτούτου Τηλεπικοινωνιακών Προτύπων.

- **Υλικό**: Λόγω των διαφόρων κατασκευαστών ασυρμάτων συσκευών θα πρέπει να λαμβάνετε υπ όψιν η συμβατότητα ανάμεσα στις συσκευές που θα δημιουργήσουν το δίκτυο.

- **Ενέργεια**: Οι συσκευές που χρησιμοποιούνται σε ένα wi-fiδίκτυο μπορεί να είναι φορητές και σαν αποτέλεσμα να παρουσιάζουν κάποια κινητικότητα. Λόγω της κινητικότητας σε ένα τέτοιο δίκτυο απαιτείται η χρήση μπαταριών, για να μπορούν να λειτουργήσουν τα ηλεκτρονικά κομμάτια του δικτύου. Η ασύρματη κάρτα δικτύου, καταναλώνει περισσότερη ενέργεια με αποτέλεσμα να εξαντλούνται αρκετά γρήγορα οι μπαταρίες της συσκευής.

- **PathLoss**: Πολλές φορές η μη οπτική επαφή μία ασύρματης επικοινωνίας είναι υπεύθυνη για τις απώλειες που μπορεί να έχουμε κατά τη μετάδοση πληροφορίας.

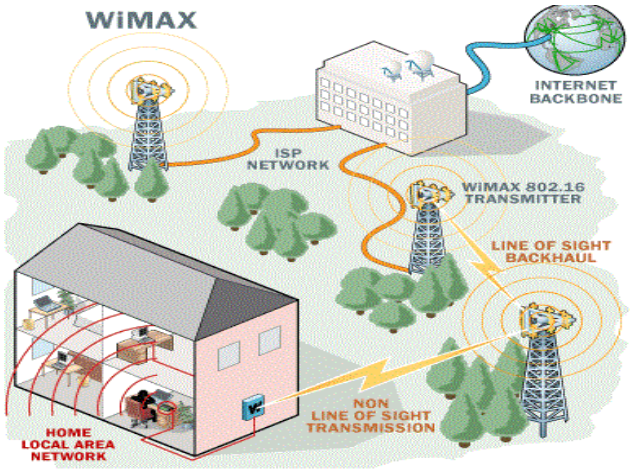
2.3 ΤΥΠΟΙ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ

Η ενότητα αυτή αναφέρεται για ιστορικούς λόγους , καθώς δεν έχει σχέση με τα δίκτυα wi-fi. Σκοπός είναι η επισήμανση και παρουσίαση διαφορετικών τεχνολογιών που προηγήθηκαν του wi-fikαι γενικότερα στην ασύρματη δικτύωση. Πέρα από το wi-fi, με το οποίο κάποιος έρχεται, έμμεσα ή άμεσα, σε καθημερινή επαφή, υπάρχουν αρκετοί άλλοι τρόποι ασύρματης δικτύωσης. Κάθε ένας από αυτούς έχει το δικό του λόγω ύπαρξης και συγκεκριμένες ανάγκες να καλύψει.

Οι πιο γνωστές τεχνολογίες είναι: IEEE 802.11, IEEE 802.16(WiMAX), Hiper LAN, OpenAir, HomeRFSWAP, Point to Point, Point to Multipoint,Bluetooth.
Πιο αναλυτικά:

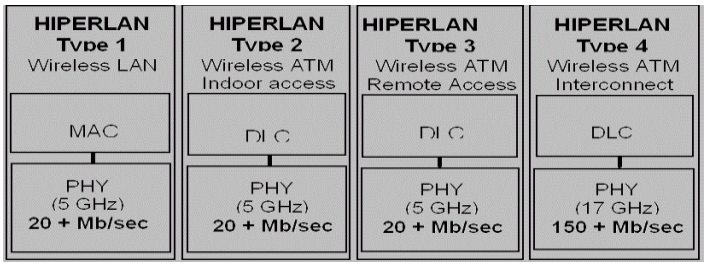
- **IEEE 802.11**:
  Είναι η πρώτη τεχνολογία ασύρματης δικτύωσης και έγινε γνωστή τον Ιούλιο του 1997. Σε ένα τέτοιο δίκτυο ο έλεγχος πρόσβασης γίνεται με τη χρήση των φυσικών διευθύνσεων και των φυσικών στρωμάτων. Χρησιμοποιείται διαμόρφωση FHSSή DSSSμε ρυθμούς μετάδοσης ως 2 Mbpsστην ζώνη των 2.4GHz. Το αρχικό πρότυπο δεν προτιμήθηκε λόγω χαμηλής ταχύτητας μετάδοσης. Θα γίνει αναλυτική περιγραφή του σε παρακάτω κεφάλαιο.

- **IEEE 802.16(WiMAX)**:
  Το IEEE 802.16 αποτελεί μια μεγάλη οικογένεια προτύπων που συμπεριλαμβάνει και το WiMAX. Αρχικά, εμφανίστηκε το 2001 στην πρώτη του μορφή και σκοπό είχε την δημιουργία ασυρμάτων δικτύων με μεγάλη εμβέλεια και υψηλές ταχύτητες μετάδοσης, Το WiMAX υποστηρίζει μετάδοση δεδομένων σε διάφορες συχνότητες σε εύρος από 10 – 66GHzμε ταχύτητα 120Mbps. Με νεότερη του έκδοση, το 2011, έφτασε ταχύτητες μέχρι 1Gbps.



Εικόνα 3-Το WiMAX

- **HiperLAN**:
  ToHiper LAN πιστοποιήθηκε από το ETSI (European Telecommunications Standards Institute) το 1996. Το HiperLAN λειτουργεί στη ζώνη συχνοτήτων 5.1 ως 5.3GHz με ταχύτητα μετάδοσης πληροφορίας ως 2Mbps. Η πρώτη έκδοση ήταν το HiperLAN1 και ακολούθησαν τα HiperLAN2, HiperAccessκαι HiperLink. Η 1η έκδοση σκοπό είχε να πετύχει ταχύτητες μεγαλύτερες του 802.11

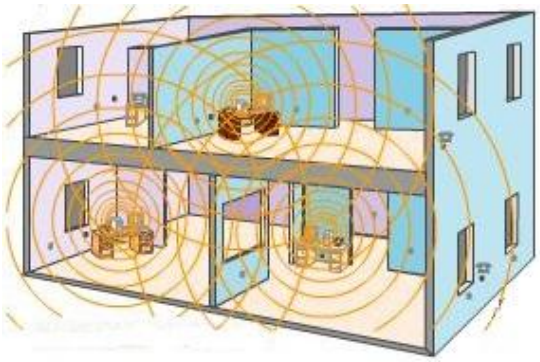


Εικόνα 4-Τύποι HiperLAN

- **OpenAir**:
  Το πρότυπο OpenAir προηγείται χρονικά του 802.11 και προωθήθηκε από την εταιρία Proxim, μία από τις μεγαλύτερες εταιρείες στον τομέα της δικτύωσης. Λειτουργεί με FrequencyHoping με ρυθμό μετάδοσης δεδομένων από 0.8 ως

1.6Mbpsκαι χρησιμοποιεί 2FSKκαι 4FSK τεχνικές διαμόρφωσης. Το πρωτόκολλο που χρησιμοποιεί είναι τοCSMA/CAκαι στηρίζεται στη ανταλλαγή RTS/CTSπακέτων.

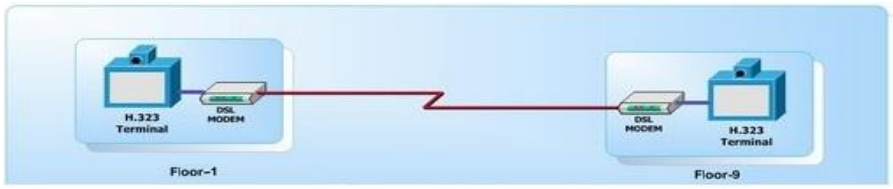
- **HomeRFSWAP**:
  Δημιουργήθηκε το 1998 από την HomeRFworkinggroupμε στόχο τη σύνδεση ασυρμάτων συσκευών οικιακής χρήσης.



Εικόνα 5-HomeRF

Η αρχική του ονομασία ήταν SWAP(SharedWirelessAccessProtocol) και αργότερα μετονομάστηκε σε HomeRF. Λειτουργεί σε επίπεδο MAC χρησιμοποιώντας λειτουργίες του DECT, που αποτελεί ένα πρότυπο για την λειτουργία των ασύρματων τηλεφώνων, και το πρότυπο 802.11. Εκπέμπει στα 2.4GHzμε μετάδοση ως 2Mbps και εμβέλεια 50 μέτρα.

- **Point to Point**:
  Τα point-to-point δίκτυα χρησιμοποιήθηκαν κυρίως από τα WMAN, παρόμοια μετά WLANαλλά με μεγαλύτερη εμβέλεια. Παρακάτω φαίνεται η ασύρματη και ή ενσύρματη δικτύωση ενός point-to-point.



Εικόνα 6-Point-to-Pointδικτύωση

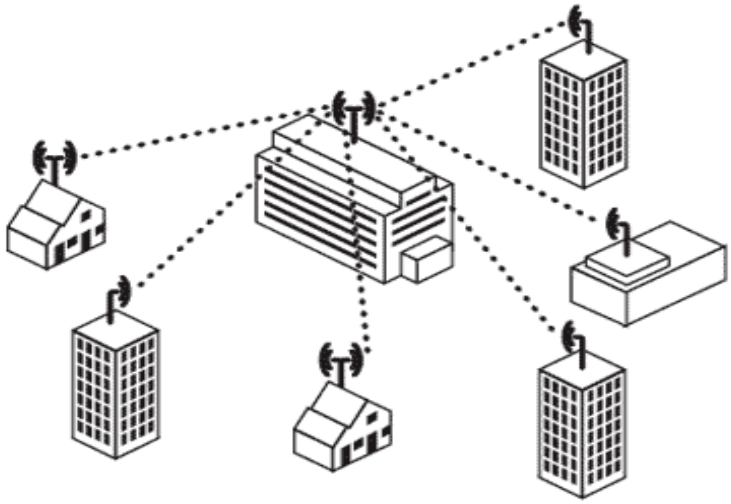
Χρησιμοποιούνται κατευθυντικές κεραίες για τη μετάδοση σήματος και τεχνολογίες όπως η spreadspectrumγια την διαμόρφωση-από διαμόρφωση του σήματος.
Η εμβέλεια του μπορεί να φτάσει τα 50Kmενώ σε απόσταση 3 με 5Kmπετυχαίνει ταχύτητες ως και 11Mbps.

- **Point to Multipoint**:
  Σε αυτού του τύπου τα δίκτυα, όλες οι ασύρματες συσκευές συνδέονται σε μίασταθερή περιοχή όπου βρίσκεται oserver. Οι πλέον διαδεδομένες τεχνολογίες Point-to-Multipointείναι οι MMDSκαι LMDS. Πιο συγκεκριμένα:

  - MMDS(MultichannelMultipointDistributionService):
    Η τεχνολογία αυτή χρησιμοποιεί ζώνη συχνοτήτων από 2.1 ως 2.7GHz με ταχύτητα μετάδοσης ως 10Mbps σε ακτίνα 4Km. Χρησιμοποιείται κυρίως σε περιοχές που η καλωδίωση είναι ασύμφορη.

- LMDS(LocalMultipointDistributionService):
  Αυτή η τεχνολογία χρησιμοποιεί ένα μεγάλο εύρος συχνοτήτων, από 24 ως 40GHz, και ρυθμούς μετάδοσης ως 155Mbps σε ακτίνα 4Km. Είναι ασύρματη τεχνολογία επικοινωνίας και ανήκει στην κατηγορία WLL(WirelessLocalLoop). Χρησιμοποιείται για τη μετάδοση ήχου, video και διαδικτύου

  Ένα παράδειγμα Point-to-Multipointφαίνεται στη παρακάτω εικόνα.



Εικόνα7-ΠαράδειγμαPoint-to-Multipoint

- **Bluetooth**:
  Δημιουργήθηκε το 1994 από την Bluetooth Special Interest Group. Αποτελεί ασύρματη τεχνολογία ραδιοσυχνοτήτων για μετάδοση δεδομένων σε μικρές αποστάσεις. Εκπέμπει στην μπάντα των 2.4GHz με ρυθμό μετάδοσης ως Mbps. Οι πιο σύγχρονες εκδόσεις του έχουν φτάσει ταχύτητες ως και 24Mbps (Bluetooth4). Είναι ένα αρκετά διαδεδομένο πρότυπο και με μεγάλη εμπορική δραστηριότητα καθώς ενσωματώνεται σε διάφορες συσκευές. Η εμβέλεια του φτάνει τα 200m. Βασικό χαρακτηριστικό του Bluetooth αποτελεί η χαμηλή κατανάλωση ενέργειας.

Εικόνα 8-Bluetooth και συσκευές

2.4 ΧΡΗΣΤΕΣ Wi-Fi

Όπως προαναφέρθηκε και σε προηγούμενα κεφάλαιο, είναι εξαιρετικά εύκολο για τον οποιοδήποτε να προμηθευτεί μία ασύρματη συσκευή. Κάθε ιδιοκτήτης μίας ασύρματης wi-fiσυσκευής έχει απαίτηση για κάποιο wi-fiδίκτυο. Άρα ο καθένας θα μπορούσε να είναι χρήστης wi-fiκαθώς απευθύνεται σε όλους. Πιο συγκεκριμένα όμως υπάρχουν συνθήκες όπου η χρήση ασυρμάτου δικτύου wi-fiκρίνεται απαραίτητη για λειτουργικούς λόγους.

Ένα χαρακτηριστικό παράδειγμα, είναι οι εκπαιδευτικές εγκαταστάσεις, όπου η μετακίνηση είναι συχνή και απαραίτητη εξαιτίας του συμπλέγματος των κτιρίων από τα οποία απαρτίζονται. Το προηγούμενο παράδειγμα έχει εφαρμογή και σε χώρους υγείας όπως νοσοκομεία.

Σε προηγούμενο κεφάλαιο αναφέρθηκε το πλεονέκτημα που παρουσιάζουν τα ασύρματα δίκτυα wi-fi σε ιδιωτικές επιχειρήσεις γιατί ανά πάσα στιγμή κάθε εργαζόμενος μπορεί να έχει πρόσβαση στο ασύρματο δίκτυο , βελτιώνοντας σημαντικά την αποδοτικότητα της εταιρίας.

2.5 ΠΑΡΑΜΕΤΡΟΙ ΓΙΑ ΤΗΝ ΥΛΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ Wi-Fi

Για την εγκατάσταση ενός ασυρμάτου δικτύου wi-fiκαι την ορθή λειτουργία του πρέπει να ληφθούν υπόψη κάποιοι παράμετροι.

- Εγκατάσταση

  Για την εγκατάσταση ενός wi-fiδικτύου είναι απαραίτητα access points και τερματικά. Το πιο σημαντικό είναι η σωστή και ασφαλή τοποθέτηση access point . Ηεπιλογή των σημείων που θα εγκατασταθούν τα AP, είναι αυτή που εξασφαλίζει την κάλυψη και την απόδοση, που απαιτούνται από τη σχεδίαση του δικτύου.

- Έρευνα πεδίου

  Για ασύρματα δίκτυα, χρησιμοποιώντας αρχιτεκτονική κυψελών, η κατάλληλη τοποθέτηση των AP διευκολύνεται με την δοκιμαστική εφαρμογή του AP στο χώρο και επιτόπου έρευνα. Πρέπει να ληφθεί υπόψη η ισχύς και η ποιότητα του σήματος που εκπέμπει. Με τη μετακίνηση του APστο χώρο κρίνεται η καταλληλότερη θέση.

- Software

  Κάρτες δικτύου και εργαλεία για την διαμόρφωση των AP ώστε να είναι κατάλληλα για χρήση. Για κάθε υλικό, AP ή κάρτα δικτύου, καθορίζεται η ποιότητα του από το user interfaceπου διαθέτει. Ένα καλό interface διευκολύνει τη διαμόρφωση του δικτύου και βοηθά στη μείωση του χρόνου εγκατάστασης.

- Εργαλεία διαχείρισης

  Ένα ασύρματο δίκτυο 802.11 διαφέρει με ένα ενσύρματο μόνο στα 2 πρώτα επίπεδα του μοντέλου OSI, είναι δηλαδή λογικό να υπάρχει το ίδιο επίπεδο διαχείρισης για τα προϊόντα του δικτύου. Τα προϊόντα αυτά υποστηρίζουν το SNMP2, άρα και μπορούν να διαχειριστούν όπως κάθε ενσύρματη συσκευή, με τις ίδιες εφαρμογές και με τις κατάλληλες MIBs να ελεγχθούν επιμέρους λειτουργίες του ασύρματου εξοπλισμού.

- Εμβέλεια και Throughput

  Τα ασύρματα δίκτυα κάνουν χρήση ραδιοσυχνοτήτων, λόγω της δυνατότητας τους να παρακάμπτουν εμπόδια και να ανακλώνται πάνω στα εμπόδια. Η καλή απόδοση ενός ασυρμάτου δικτύου είναι αποτέλεσμα πολλών παραγόντων όπως ο αριθμός χρηστών, την εμβέλεια μικροκυψελών, παρεμβολές, μετάδοση σε πολλά μονοπάτια, δυνατότητεςhardware και πρότυπο 802.11. Για το εύρος συχνοτήτων δεν ισχύει το όσο μεγαλύτερο τόσο το καλύτερο.

2.6 ΥΛΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΤΑΣΚΕΥΗΣ ΕΝΟΣ ΔΙΚΤΥΟΥ Wi-Fi

Για την κατασκευή και την σωστή λειτουργία ενός δικτύου wi-fi είναι απαραίτητα κάποια υλικά. Οι τεχνολογικές απαιτήσεις είναι τόσο σε επίπεδο λογισμικού όσο και σε επίπεδο υλικού. Ξεκινώντας από τον πάροχο έως τον τελικό χρήστη ,τα υλικά ποικίλουν.
Οι κατηγορίες των βασικών δομικών υλικών ενός ασυρμάτου δικτύου αναφέρονται στη συνέχεια.

- **Τερματικό χρήστη:**Οι συσκευές που διαθέτουν οι χρήστες είναι αυτές που δίνουν τη δυνατότητα επικοινωνίας διαφόρων εφαρμογών και υπηρεσιών. Διασφαλίζουν την ασύρματη μεταφορά δεδομένων από και προς το δίκτυο. Είναι ουσιαστικά το αρχικό στάδιο επικοινωνίας ανάμεσα στο δίκτυο και το χρήστη. Αναφέρονται στη συνέχεια, ενδεικτικά κάποιες από αυτές:
  - Φορητοί Η/Υ
  - Σταθεροί Η/Υ (με ανάλογο προσαρμογέα ασυρμάτου δικτύου)
  - Tablets
  - PDAs
  - Smartphones
  - Και άλλες περιφερειακές ασύρματες συσκευές (π.χ. ipprinter,ipcamera)

- **Ασύρματη κάρτα δικτύου:**Η ασύρματη κάρτα δικτύου είναι αυτή που δίνει τη δυνατότητα μετάδοσης σήματος μέσα σε ένα ασύρματο δίκτυο υπολογιστών και άλλων ασύρματων συσκευών. Η λειτουργία της δεν περιορίζεται μόνο στη λήψη και την αποστολή δεδομένων αλλά διαμορφώνει και ενισχύει το σήμα. Κάθε συσκευή για να συμμετέχει σε ένα wi-fiδίκτυο πρέπει να διαθέτει έναν ασύρματο προσαρμογέα είτε ενσωματωμένο είτε πρόσθετο σαν κάρτα επέκτασης.
  Παρακάτω φαίνονται κάποιες ενδεικτικά.

Εικόνα 9-Ασύρματες κάρτες Δικτύου

- **AccessPoints:**ΤαAccessPoints (Σημεία πρόσβασης) είναι δικτυακές συσκευές που παρέχουν στα ασύρματα τερματικά τη δυνατότητα επικοινωνίας μεταξύ τους

αλλά και με το διαδίκτυο, είναι η μονάδα που παίζει το ρόλο γέφυρας μεταξύ του ενσύρματου και του ασύρματου δικτύου, μετατρέποντας κατάλληλα τα πλαίσια που ανταλλάσσονται μεταξύ αυτών**.** Είναι βασική συσκευή του δικτύου wi-fikαθώς είναι αυτή που καθορίζει το εύρος της ασύρματης επικοινωνίας ανάμεσα στις συσκευές που είναι συνδεδεμένες αλλά και τη γεωγραφική έκταση του δικτύου.

Το σημείο πρόσβασης παρέχει τα πιστοποιητικά ασφάλειας καθώς είναι αυτό που επιλέγει αν έχουμε τα κατάλληλα δικαιώματα για τη σύνδεση στο δίκτυο.

Εικόνα 10-Συσκευές Access Point

- **<u>Μέσο Μετάδοσης:</u>** Τα ασύρματα δίκτυα βασίζονται στις ραδιοσυχνότητες όπου έχουν αποδοθεί για κατασκευαστικούς, επιστημονικούς και ιατρικούς σκοπούς. Για αυτό το λόγω η μετάδοση σημάτων στις συγκεκριμένες συχνότητες δεν απαιτεί άδεια. Το 802.11 παρέχει 13 κανάλια στη συχνότητα των 2.4GHz με σκοπό να μειώνει τις απώλειες και να εξασφαλίζει καλύτερη μετάδοση δεδομένων.

- **<u>Κεραίες Εκπομπής:</u>** Οι κεραίες εκπομπής είναι ένα κρίσιμο στοιχείο για την ασύρματη δικτύωση, λόγω του ρόλου τους στο να μετατρέπουν τα ηλεκτρικά σήματα σε ραδιοσυχνότητες με σκοπό τη μεταφορά του διαμορφωμένου σήματος μέσω της ατμόσφαιρας στην περιοχή κάλυψης.

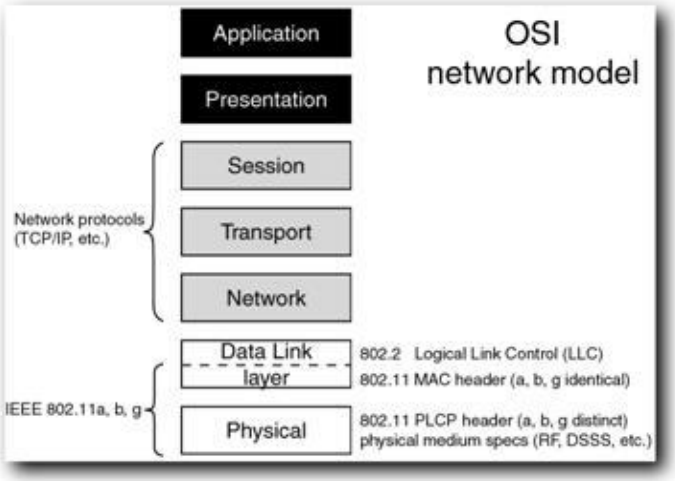
  Ο τρόπος με τον οποίο μία κεραία εκπέμπει το σήμα καθορίζει αυτομάτως και την περιοχή κάλυψης. Υπάρχουν δύο κατηγορίες τέτοιων κεραιών, οι κατευθυντικές και οι πολυκατευθιντικές

  Οι κατευθυντικές στέλνουν όλη την ισχύ της εκπομπής τους σε μία κατεύθυνση. Σε αντίθεση οι πολυκατευθυντικές στέλνουν την ισχύ τους σε κάθε κατεύθυνση, καθώς είναι κατευθυντική και στις τρεις διαστάσεις, με κύριο χαρακτηριστικό πως εκπέμπουν κατά 360^{o} στο οριζόντιο επίπεδο. Συνήθως τα accesspointsέχουν πολυκατευθυντική.

Εικόνα 11-Κεραίες Ασυρμάτου Δικτύου

2.7 IEEE 802.11

Το 1997, μετά από 7 χρόνια εργασιών, η IEEE εξέδωσε το 802.11, ως το πρώτο πρότυπο, διεθνώς εγκεκριμένο για ασύρματα δίκτυα. Όπως όλα τα πρότυπα 802 της IEEE, το 802.11, επικεντρώνεται στα 2 κατώτατα επίπεδα του μοντέλου OSI. Τα επίπεδα αυτά είναι το φυσικό (MAC) και το επίπεδο διασύνδεση δεδομένων (DataLink). Η χαρακτηριστική διαφορά με τα σταθερά TCP/IP δίκτυα είναι ότι οι συσκευές μετακινούνται συνεχώς με αποτέλεσμα να απαιτούνται περίπλοκες στρατηγικές.



Εικόνα 12-Το μοντέλο OSI για το 802.11

Το IEEE 802.11 ορίζει τα χαρακτηριστικά των ασυρμάτων δικτύων, προσθέτοντας βελτιώσεις και διορθώσεις σε κάθε νέα έκδοση του. Μερικά από αυτά είναι τα εξής :

- Αρχιτεκτονική των δικτύων
- Συσχέτιση, αυθεντικοποίηση και μυστικότητα
- Η δομή πλαισίων
- Λειτουργίες Frequency Hopping Spread Spectrum (FHSS)
- ΛειτουργίεςDirect Sequence Spread Spectrum (DSSS)
- Wired Equivalent Privacy (WEP)

Στο IEEE 802.11 έχουμε δύο τύπους φυσικού επιπέδου : την υπέρυθρη ακτινοβολία (IR) και την ελεύθερη ραδιοσυχνότητα των 2,4 GHz. Σε wi-fi δίκτυα χρησιμοποιείται η μπάντα των 2,4 GHz. Πιο κάτω φαίνεται ο πίνακας με κάποιες από τις εκδόσεις του προτύπου IEEE 802.11

Protocol Features	Legacy	802.11a	802.11b	802.11g	802.11n	802.11y
Release Date	July 1997	July 1999	July 1999	June 2003	June 2009	June 2008
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz	2.4 - 5 GHz	3.7 GHz
Throughput	0.9 Mbits	23 Mbits	4.3 Mbits	19 Mbits	74 Mbits	23 Mbits
Max. Data Rate	2 Mbits	54 Mbits	11 Mbits	54 Mbits	248 Mbits	54 Mbits
Modulation		OFDM	DSSS	OFDM	DSSS/CCK /OFDM	
Indoor Range	20 Mts	35 Mtrs	38 Mtrs	38 Mtrs	70 Mtrs	50 Mtrs
Outdoor Range	100 Mtrs	120 Mtrs	140 Mtrs	140 Mtrs	250 Mtrs	5000 Mtrs

Εικόνα 13-Η εξέλιξη του IEEE 802.11

Πιο αναλυτικά :

- IEEE 802.11a: Η δεύτερη έκδοση του προτύπου που έγινε γνωστή στο κοινό τον Ιούλιο του 1999. Βασικότερη τροποποίηση ήταν η λειτουργία ενός ασυρμάτου δικτύου στη συχνότητα των 5GHz. Κάνει χρήση της διαμόρφωσης OFDM (Orthogonalfrequencydivisionmultiplexing), αυξάνοντας τον ρυθμό μετάδοσης στα 54Mbps, αλλά σαν αποτέλεσμα έχει την μείωση της περιοχής κάλυψης. Σημαντικό πλεονέκτημα ήταν η λειτουργία του δικτύου στη μπάντα των 5GHz η οποία έχει λιγότερες παρεμβολές σε σχέση με αυτή των 2.4GHz.

- IEEE 802.11b: Εμφανίστηκε τον Ιούλιο του ίδιου έτους και είναι η $3^{η}$ έκδοση του προτύπου, αυξάνοντας τους ρυθμούς μετάδοσης από 5,5 ως 11 Mbps στην αρχική ζώνη συχνοτήτων(2,4GHz). Στην έκδοση αυτή υποστηρίζεται μόνο η DSSS διαμόρφωση, όπου χρησιμοποιεί τον CCK (ComplementaryCodeKeying) τύπο διαμόρφωσης.

- IEEE 802.11g: Η επόμενη έκδοση που εκδόθηκε τον Ιούνιο του 2003 και αύξησε τους ρυθμούς μετάδοσης στα 54Mbps στη ζώνη των 2.4GHz με διαμόρφωση OFDM – DSSS. Η έκδοση αυτή υποστηρίζει τις ταχύτητες του 802.11a, επιπλέονείναι συμβατή με το με την 802.11b και έτσι συσκευές που υποστηρίζουν 802.11b κ 802.11g αντίστοιχα μπορούν να συνεργαστούν μέσα στο δίκτυο.

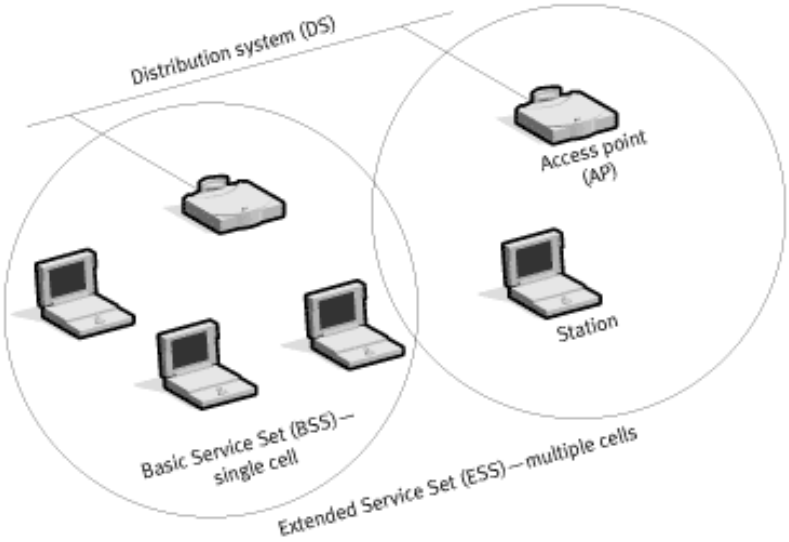
- IEEE 802.11y: Τον Ιούνιο του 2008 παρουσιάστηκε και η $5^{η}$ έκδοση του προτύπου όπου λειτουργούσε στη ζώνη των 3,7GHz, χρησιμοποιώντας την τεχνολογία MIMO (MultipleInputsMultipleOutputs). Υποστήριζε ρυθμούς μετάδοσης ως 54Mbps με εμβέλεια 5000 μέτρων

- IEEE 802.11n: Εκδόθηκε τον Ιούνιο του 2009. Στόχος ήταν ο συνδυασμός όλων των προηγούμενων τεχνολογιών, και με νέες βελτιώσεις, ώστε να αυξηθεί η ταχύτητα του δικτύου.Χρησιμοποιεί για τη μετάδοση κεραίες MIMOπετυχαίνοντας ρυθμούς μετάδοσης από 100 ως 140Mbps αν και σε θεωρητικό επίπεδο μπορεί να φθάσει και τα 400Mbps.

2.7.1 ΤΟΠΟΛΟΓΙΕΣ IEEE 802.11

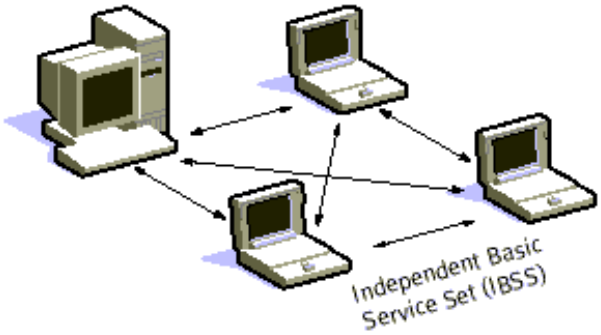
Το IEEE 802.11 ορίζει 2 τρόπους λειτουργίας. ΤηλειτουργίαInfrastructure mode καιτηνAd Hoc mode.

Στην Infrastructuremode,η σύνθεση του δικτύου απαρτίζεται από 1 accesspoint, όπου είναι σε σύνδεση με το ενσύρματο δίκτυο και κάποιο αριθμό από ασύρματα τερματικά. Η τοπολογία αυτή ονομάζεται βασικό σύνολο υπηρεσίας - BSS (BasicServiceSet).Τα όρια του BSS καθορίζονται από την περιοχή ραδιοκάλυψης, που ονομάζεται BasicServiceArea (BSA).Ένας σταθμός σε ένα BSS μπορεί να επικοινωνεί με οποιονδήποτε άλλο σταθμό στο ίδιο BSS.Η σύνδεση παραπάνω από 2 BSS, αποτελεί το ESS(ExtendedServiceSet). Η πλειονότητα των WLANχρησιμοποιεί τον τρόπο της infrastructure, λόγω της απαίτησης πρόσβασης σε ενσύρματο LANγια διαμοιρασμό υπηρεσιών.



Εικόνα 14-InfrastructureMode

Στην AdHocmode, η σύνθεση του δικτύου αποτελείται από ένα σύνολο 802.11 σταθμών που έχουν τη δυνατότητα άμεσης επικοινωνίας μεταξύ τους, χωρίς να είναι απαραίτητα τα accesspoints ή κάποια σύνδεση με ενσύρματο δίκτυο. Αυτός ο τρόπος λειτουργίας χρησιμεύει στην εύκολη και γρήγορη εγκατάσταση ενός ασυρμάτου δικτύου σε περιπτώσεις που δεν υπάρχει καλωδιακή υποδομή ή δεν απαιτείται η χρήση των υπηρεσιών που αναφέρθηκαν για την infrastructure.



Εικόνα 15-AdHocmode

2.7.2 ΗΑΡΧΙΤΕΚΤΟΝΙΚΗΤΟΥΙΕΕΕ 802.11

Ο τρόπος λειτουργίας του IEEE 802.11 χωρίζεται σε 2 στρώματα, το LLC – έλεγχος λογικού συνδέσμου (LogicalLinkControl)και το MAC – έλεγχος προσπέλασης μέσων (MediaAccessControl) για το επίπεδο DataLinkLayer. Το φυσικό επίπεδο με το MACεπικοινωνούν , μέχρι το LLC.

- Physical Layer – Φυσικό επίπεδο

Τοφυσικόεπίπεδοπαρέχειτιςεξήςτεχνικέςμετάδοσης : Υπέρυθρες, FHSS(Frequency Hopping Spread Spectrum), DSSS(Direct Sequence Spread Spectrum), OFDM (Orthogonal Frequency-Division Multiplexing) καιHR-DSSS (High Rate 0 Sequence Spreas Spectrum).

Η μπάντα εκπομπή είναι 2.4GHz, εγκεκριμένη από διεθνείς οργανισμούς χωρίς να χρειάζεται άδεια. Οι τεχνικές SpreadSpectrumπέραν του ότι ικανοποιούν τις απαιτήσεις τυποποίησης, αυξάνουν την αξιοπιστία, προωθούν τον ρυθμό απόδοσης του δικτύου και επιτρέπουν σε διάφορα προϊόντα να μοιράζονται τις ίδιες συχνότητες χωρίς παρεμβολές

Τα FHSSκαι DSSSείναι διαφορετικοίμηχανισμοί για την επεξεργασία σημάτων και δεν είναι δυνατόν να συνεργαστούν ή να συνυπάρξουν.

- DataLinkLayer – Επίπεδο διασύνδεσης δεδομένων

Αποτελείται από τα 2 υποστρώματα που προαναφέρθηκαν, τα LLC καιMAC. Το 802.11 χρησιμοποιεί το ίδιο LLCκαι την διευθυνσιοδότηση 48bitόπως όλα τα υπόλοιπα LAN, διευκολύνοντας τη γεφύρωση μεταξύ ασυρμάτου και ενσύρματουIEEEδικτύου, με διαφορά ότι η MACδιεύθυνση είναι διαφορετική στα WLAN.

Εφαρμόζεται σε όλους τους 802.11 σταθμούς του δικτύου και επιτρέπει την μεταφορά δεδομένων στο επίπεδο LLC.Οι λειτουργίες, του επιπέδου, γίνονται με τις υπηρεσίες σταθμών και τις υπηρεσίες συστημάτων διανομής.

Για τις λειτουργίες του MAC επιπέδου, πρέπει να εξασφαλιστεί η πρόσβαση στο ασύρματο μέσο. Το MACκάνει έλεγχο πρόσβασης των ενδιάμεσων σταθμών στο ίδιο μέσο μετάδοσης.

ΚΕΦΑΛΑΙΟ 3 – ΑΣΦΑΛΕΙΑ ΣΕ ΔΙΚΤΥΟ Wi-fi

Τα wi-fiδίκτυα βασίζονται στη μετάδοση του σήματος χρησιμοποιώντας την ατμόσφαιρα ως μέσο μεταφοράς, με αποτέλεσμα να μπορεί να αμφισβητηθεί η ασφάλεια που παρέχουν.

Επιπλέον η δυνατότητα διασύνδεσης τους με το διαδίκτυο αυξάνει ακόμα περισσότερο την ευαισθησία στο θέμα της ασφάλειας, καθώς παρατηρείται όλο και περισσότερο αύξηση διακίνησης προσωπικών πληροφοριών.

Για να διασφαλιστεί το ζήτημα της ασφάλειας έχουν εφευρεθεί τρόποι πιστοποίησης αλλά και κρυπτογράφησης . Τρόποι διασφάλισης αξιοπιστίας ασυρμάτου δικτύου είναι οι εξής: Επικύρωση, Κρυπτογράφηση, Ακεραιότητα, Μυστικότητα.

Εικόνα 16-Ασφαλές δίκτυο

3.1 ΕΠΙΚΥΡΩΣΗ

Επικύρωση ,είναι η ανταλλαγή πιστοποιητικών ανάμεσα στους κόμβους του δικτύου πριν από τη μετάδοση δεδομένων. Αφορά δηλαδή τον έλεγχο πρόσβασης στο δίκτυο. Τα βήματα της επικύρωσης αναφέρονται παρακάτω.

Αρχικά ανιχνεύονται τα διαθέσιμα ασύρματα δίκτυα, με τη χρήση της ασύρματης κάρτας δικτύου, και το δίκτυο επικυρώνει το σταθμό.
Τα accesspoints εκπέμπουν πακέτα που αποκαλούνται beacons. Τα πακέτα αυτά δείχνουν πως υπάρχει δίκτυο. Κάθε beaconέχει ένα όνομα, όπου είναι και το όνομα του δικτύου. Με την ανίχνευση των διαθέσιμων δικτύων ο χρήστης επιλέγει το σημείο πρόσβασης που θέλει να συνδεθεί.

Υπάρχουν δύο τρόποι επικύρωσης: Ανοιχτού κλειδιού και μοιρασμένου κλειδιού.

Ανοιχτού κλειδιού: Κατά την επικύρωση ανοιχτού κλειδιού ,κάθε τερματικό, επικυρώνετε από το δίκτυο – access point, με την εξαίρεση πως δεν επικοινωνεί με το access point. Το κάθε τερματικό μπορεί να επικοινωνήσει με το access point εάν έχει τα ίδια WEP (Wireless equivalent privacy) κλειδιά με αυτά που περιέχονται στον WEP αλγόριθμο του access point.

Μοιρασμένου κλειδιού:Στην επικύρωση μοιρασμένου κλειδιού ,το κλειδί είναι γνωστό σε όλους τους σταθμούς του δικτύου πριν ακόμα ξεκινήσουν τη διαδικασία της επικύρωσης.

3.2 ΚΡΥΠΤΟΓΡΑΦΗΣΗ WEP

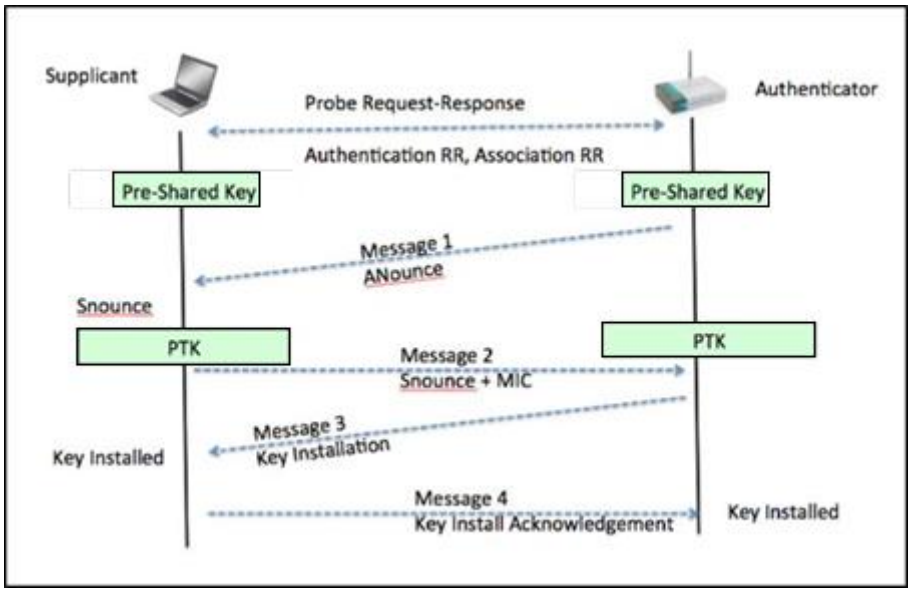
Ως κρυπτογράφηση ορίζεται η διαδικασία κατά την οποία τα πακέτα δεδομένων ,που πρόκειται να σταλθούν από κάθε σταθμό του δικτύου, αλλάζουν μορφή κατά τρόπο τέτοιο που μπορούν να διαβαστούν μόνο από κάποιον χρήστη που διαθέτει το κατάλληλο κλειδί. Στην ουσία αλλάζουν μορφή για ασφαλέστερη μετάδοση των πληροφοριών.

Η πληροφορία, πριν εισέλθει, στη διαδικασία κρυπτογράφησης και αποστολής έχει την ονομασία plaintext (P). Στη συνέχεια , με τη χρήση αλγόριθμου κρυπτογράφησης(cipher) έχει την ονομασία ciphertext(C). Ο αλγόριθμος cipher είναι μία συγκεκριμένη μαθηματική ακολουθία που τροποποιεί, αλλά και επαναφέρει τα δεδομένα, κατά την αποστολή ή τη λήψη αντίστοιχα. Κατά την λήψη της κρυπτογραφημένης πληροφορίας ενεργοποιείται η διαδικασία της αποκρυπτογράφησης.

Το WEP, που αναφέρθηκε και πιο πάνω, είναι η πιο γνωστή ασφάλεια για κάποιο ασύρματο δίκτυο. Με το WEP, το τερματικό και το access point μοιράζονται το κλειδί του δικτύου και επιπλέον παρέχει δυνατότητα κρυπτογράφησης για τα προς αποστολή δεδομένα.
Επιτυγχάνει την κρυπτογράφηση με τη χρήση του αλγορίθμου RC4.

- Επαλήθευση ταυτότητας

  Για τη σύνδεση μιας ασύρματης συσκευής σε ένα δίκτυο wi-fi απαιτείται η επαλήθευση της ταυτότητας της. Με τον αλγόριθμο WEP, η συσκευή πιστοποιεί στο access point το γεγονός ότι διαθέτουν το ίδιο κλειδί. Το τερματικό αποστέλλει αίτημα επαλήθευσης στο access point, που απαντά με ένα αριθμό 128bit προς κρυπτογράφηση. Το τερματικό τότε κρυπτογραφεί αυτόν τον αριθμό και τον επιστέφει στο access point. Το access point χρησιμοποιεί το δικό του κλειδί ώστε να αποκρυπτογραφήσει την πληροφορία και να διασταυρώσει αν είναι ίδια με την αρχική. Σε αυτό το σημείο γίνεται έλεγχος αν έχει χρησιμοποιηθεί το κατάλληλο κλειδί κρυπτογράφησης. Αν το κλειδί είναι το ίδιο τότε επιτρέπετε η πρόσβαση.



Εικόνα 17-Διαδικασία επαλήθευσης κλειδιού

- Κατακερματισμός

  Κατά την αποστολή μίας πληροφορίας σε ένα wi-fi δίκτυο, το πακέτο δεδομένων ονομάζεται MSDU (MacServiceDataUnit). Πρόκειται για πακέτο που περιέχει κάθε πληροφορία για την αποστολή του. Με την άφιξη των δεδομένων στο επίπεδο Macto πακέτο επιβάλλεται στη διαδικασία θρυμματισμού (fragmentation) και χωρίζεται σε μικρότερα τμήματα όπου το κάθε ένα δέχεται τη δικιά του WEP κρυπτογράφηση.

- Διάνυσμα Αρχικοποίησης(Initialization Vector)

  Το διάνυσμα αρχικοποίησης έχει μήκος 24bits, τα οποία περιλαμβάνονται μέσα στα 68 ή 128bits του κρυπτογραφημένου κλειδιού.

  Το διάνυσμα αρχικοποίησης διαφοροποιείται για κάθε πακέτο και κρυπτογραφείτε μαζί με το κλειδί ,με αποτέλεσμα το τελικό πακέτο να είναι πάντα διαφορετικό.

- Κλειδιά WEP

  Τα κλειδιά WEP έχουν μήκος 104bits και οι τιμή τους δεν αλλάζει αν δεν αλλάξουν οι ρυθμίσεις του δικτύου. Για κρυπτογράφηση - αποκρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί από το access point και την ασύρματη συσκευή.

  Υπάρχει και μία άλλη κατηγορία κλειδιών στην οποία το access point και η συσκευή μοιράζονται ένα κλειδί κάνοντας χαρτογράφηση κλειδιού.

  Γενικά, τα κλειδιά WEP δεν παρέχουν μεγάλη ασφάλεια. Μία επίθεση στο δίκτυο μπορεί να το ανακτήσει με ευκολία.

- Η διανομή κλειδιού

  Η διανομή του κλειδιού WEP δημιουργεί ένα από το σημαντικότερα μειονεκτήματα. Όλες οι συσκευές του δικτύου πρέπει να έχουν τα κομμάτια του WEP κλειδιού, βέβαια για το 802.11 πρότυπο δεν υπάρχει αλγόριθμος παραγωγής κλειδιού και αυτό έχει αποτέλεσμα την εισαγωγή κλειδιού στο accesspointχειροκίνητα.

-Μειονεκτήματα διανομής κλειδιού

Α. Ο τελικός χρήστης μπορεί να μάθει το κλειδί λόγω της εισαγωγής του στον προσαρμογέα δικτύου . Δεν υπάρχει μυστικότητα.

Β. Συχνή αλλαγή του κλειδιού για την διασφάλιση της μυστικότητας.

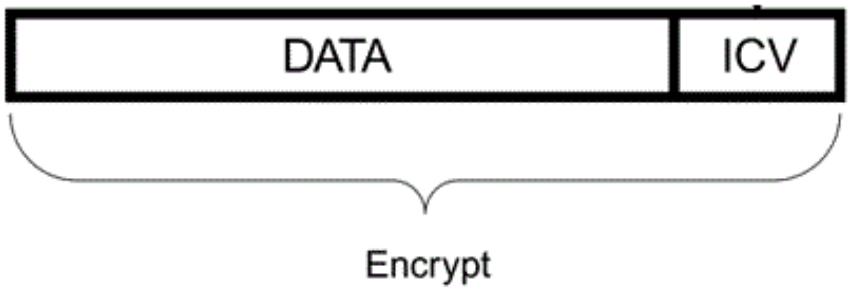
Γ. Σε μεγάλες εγκαταστάσεις ασυρμάτων δικτύων γίνεται γνωστοποίηση του κλειδιού σε όλους τους τελικούς χρήστες. Δεν υπάρχει μυστικότητα.

- ICV

Integrity Check Value (ICV) ή αλλιώς Τιμή Ελέγχου Ακεραιότητας, είναι η διασφάλιση του αρχικού μηνύματος από πιθανή αλλαγή του κατά τη μετάδοση. Σε κάθε ασύρματη μετάδοση πληροφορίας γίνεται έλεγχος για πιθανή αλλαγή των bits λόγω θορύβου.

Στην περίπτωση αλλαγής κάποιου bit πληροφορίας, ο δέκτης θα έχει μια διαφορετική τιμή CRCαπό τον αποστολέα και δεν θα δεχθεί την πληροφορία.

Ως τιμή CRC (Circle Redundancy Check) ορίζουμε τα Byte πληροφορίας που συνδυάζονται στον έλεγχο κυκλικού πλεονασμού. Έχει μήκος 4 Bytes και προστίθεται στο τέλος πριν τη διαδικασία μετάδοσης.



Εικόνα 18-Πληροφορία και ICV

Η τιμή ελέγχου ακεραιότητας εντοπίζει τυχαία λάθη αλλά δεν είναι σε θέση να αναγνωρίσει λάθη πού έχουν σκοπό την εισβολή στο δίκτυο. Ως αποτέλεσμα είναι να υπολογίζεται η τιμή CRC και να αντικατασταθεί η προηγούμενη.

Το ICV έχει αρκετές ομοιότητες με το CRC, με τη διαφορά πως ο υπολογισμός της, προηγείται της κρυπτογράφησης, ενώ CRC έπεται της κρυπτογράφησης.

- Αλγόριθμος RC4 (River Cipher 4)

Ο RC4 εφαρμόζεται κατά τη διαδικασία της κρυπτογράφησης. Είναι ένας απλός αλγόριθμος. Η αδυναμία ασφάλειας του WEPδικτύου δεν είναι ο RC4 αλλά ο τρόπος που εφαρμόζεται.

Ο αλγόριθμος έχει ως σκοπό την παράγωγή μιας ακολουθίας bytes, με την ονομασία key streamκαι συνδυάζεται με την πληροφορία με μια πράξη XOR.

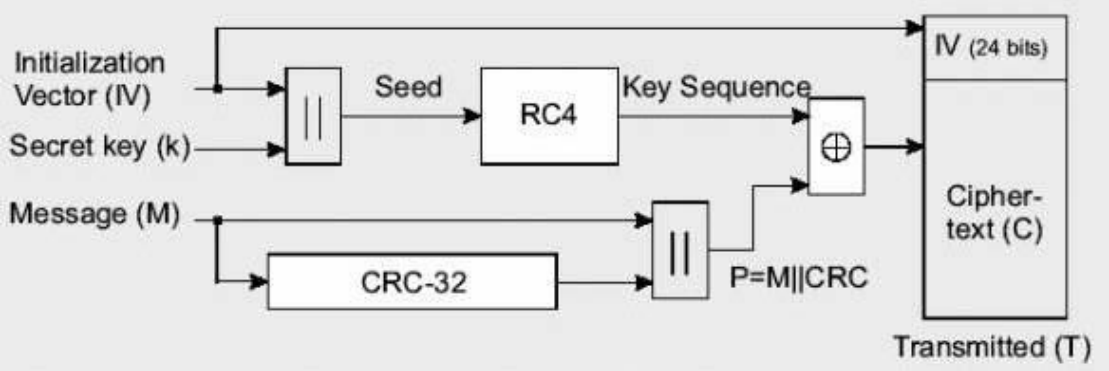
Ο RC4 βάση των ιδιοτήτων της παραπάνω πράξης μπορεί να κάνει κρυπτογράφηση και αποκρυπτογράφηση.

- Κρυπτογράφηση: plain text (XOR) keystream = cipher text
- Αποκρυπτογράφηση: cipher text (XOR) keystream = plain text

Η ακολουθία που παράγει είναι τυχαία για την αποφυγή εισβολής αλλά ο αποστολέας και ο δέκτης της πληροφορίας παράγουν την ίδια τιμή για κάθε ένα byteπου επεξεργάζονται. Ονομάζεται ψευδοτυχαία.

- Διαδικασία Κρυπτογράφησης

Παρακάτω αναφέρονται τα βήματα της διαδικασίας κρυπτογράφησης συνοπτικά.
Βήμα 1ο: Αρχικά το κλειδί του δικτύου συνδυάζεται με το διάνυσμα αρχικοποίησης και το αποτέλεσμα χρησιμοποιείται σαν είσοδο στον RC4.
Βήμα 2ο : Στη συνέχεια στην πληροφορία (plaintext) εφαρμόζεται ο αλγόριθμος ακεραιότητας (IntegrityCheck) και δημιουργείται η τιμή ελέγχου ακεραιότητας (ICV).
Βήμα 3ο : Η είσοδος στο RC4, που αναφέρθηκε στο πρώτο βήμα, παράγει την ακολουθία κλειδιού με bitstόσα όσα και τα δεδομένα προς αποστολή συν 4.
Βήμα 4ο : Σειρά έχει η λογική πράξη XORανάμεσα στην ακολουθία κλειδιού και των δεδομένων της τιμής ελέγχου ακεραιότητας. Το αποτέλεσμα είναι ένα μήνυμα με το διάνυσμα αρχικοποίησης και το κρυπτογράφημα.



Εικόνα 19-Κρυπτογράφηση WEP

Στην κρυπτογράφηση WEP, ο αλγόριθμος RC4 είναι αυτός που δημιουργεί την ακολουθία κλειδιού. Κρίνεται, άρα, απαραίτητος για την διαδικασία κρυπτογράφησης .

3.3 ΜΕΙΟΝΕΚΤΗΜΑΤΑ WEP

Το WEPέχει αρκετά μειονεκτήματα από διάφορες πλευρές. Μερικά από αυτά τα προβλήματα αναφέρονται παρακάτω.

Στο WEPγίνεται σπάνια εισαγωγή νέων κλειδιών που έχει σαν αποτέλεσμα τη συλλογή πληροφοριών για το δίκτυο από κάποιον που θα ήθελε να το βλάψει. Επιπλέον, ένα μειονέκτημα εντοπίζεται στον τρόπο διανομής κλειδιού. Το κλειδί δεν αλλάζει συχνά, όπως προαναφέρθηκε. Κατά την αποχώρηση κάποιου χρήστη από το δίκτυο θα πρέπει το κλειδί να αλλάζει.

Για την διαδικασία της κρυπτογράφησης χρησιμοποιείται πίνακας αρχικοποίησης (IV) 24Bit με κλειδί 40 ή 104bit ενώ προτείνεται η χρήση 48bit IVκαι 148bit κλειδί κρυπτογράφησης. Κρίνετε ακατάλληλο γιατί οι επιθέσεις κατευθύνονται στον πίνακα αρχικοποίησης.

Στις επιθέσεις αποστολής μηνυμάτων τοWEPπαρουσιάζει μεγάλη αδυναμία καθώς κατά την διάρκεια της επίθεσης παρακολουθούνται τα πακέτα που αναμεταδίδονται κατά την διάρκεια της επικοινωνίας. Αυτό έχει σαν αποτέλεσμα, τη δυνατότητα του επιτιθέμενου να συνδεθεί στο δίκτυο με τη φυσική διεύθυνση (MAC) της ασύρματης συσκευής.Έτσι στέλνοντας ένα προηγούμενο μήνυμα συνδέεται, χωρίς ενόχληση, στον server.

Κατά την διαδικασία σύνδεσης σε ένα ασύρματο δίκτυο, πραγματοποιείται ο έλεγχος πρόσβασης. Είναι μια απαραίτητη διαδικασία που ελέγχει το αν έχουμε το δικαίωμα να

συνδεθούμε στο δίκτυο. Το WEP εκτελεί αυτή τη διαδικασία είτε κρατώντας μία λίστα με συσκευές που επιτρέπεται να συνδεθούν ή με κάποιο πιστοποίηση. Συνήθως χρησιμοποιείται η MAC διεύθυνση, που όμως, όπως προαναφέρθηκε, μπορεί εύκολα να αντιγραφεί.

Εκτός του ελέγχου πρόσβασης πραγματοποιείται και η επαλήθευση ταυτότητας. Σε αυτή τη διαδικασία αποστέλλεται, στο το τερματικό που επιθυμεί να συνδεθεί, μία τυχαία ακολουθία bits. Μετά την λήψη η ακολουθία αυτή κρυπτογραφείται, με το κλειδί κρυπτογράφησης που διαθέτει το τερματικό και την ξαναστέλνει, κρυπτογραφημένη πλέον, πίσω στο access point. Το access point την αποκρυπτογραφεί, με το δικό του κλειδί κρυπτογράφησης, και αν είναι ίδια με την αρχική επιτρέπεται η πρόσβαση. Ο επιτιθέμενος με όλη αυτή τη διαδικασία μπορεί να συλλέξει αρκετές πληροφορίες για το δίκτυο, όπως μια κρυπτογραφημένη και μια μη κρυπτογραφημένη ακολουθία. Με μία πράξη XOR ανάμεσα στα δύο μπορεί να βρει το κλειδί κρυπτογράφησης.

ΤοWEP,αρχικά, αποτελούσε μοναδικό τρόπο προστασίας και διασφάλισης ορθής μετάδοσης της πληροφορίας σε ένα ασύρματο δίκτυο. Όπως αναφέρθηκε και πιο πάνω, όμως, είχε πάρα πολλές ατέλειες. Σαν συνέπεια ήταν η γρήγορη δημιουργία τρόπων παραβίασης του.

Στις μέρες μας βλέπουμε συχνά συσκευές που χρησιμοποιούν το WEP, βέβαια αυτό αρχίζει να αλλάζει με την χρήση νεότερων και πιο αξιόπιστων τεχνολογιών κρυπτογράφησης.

3.4 TEMPORAL KEY INTEGRITY (TKIP)

Το TKIP εμφανίστηκε τον Οκτώβριο του 2002 και αποτέλεσε την πρώτη λύση στα αρκετά προβλήματα που παρουσίαζε το WEP. Εφαρμόστηκε, αρχικά, μέσα στο WEPγια να αυξήσει την ασφάλεια του ,ώστε να μειωθούν οι απειλές που δεχόταν.

Εξασφαλίζει καλύτερης ποιότητας ασφάλεια από το WEPλόγω του συνδυασμού κλειδιών με κάθε πακέτο. Παρείχε έλεγχο ακεραιότηταςκαι αλγόριθμο παραγωγής κλειδιών, καλύπτοντας έτσι σημαντικά κενά του WEP.

Κατά την κρυπτογράφηση TKIP, αρχικά, εκτελείται ο αλγόριθμος Michael, υπολογίζοντας τον κώδικα ακεραιότητας δεδομένων MIC. Η χρησιμότητα αυτού του αλγορίθμου είναι στην προστασία των μηνυμάτων και των διευθύνσεων, των δύο άκρων της επικοινωνίας. Το μήνυμα, οι διευθύνσεις επικοινωνίας και το κλειδί MIC χρησιμοποιούνται σαν είσοδοι στον αλγόριθμο. Το αποτέλεσμα είναι 8 bytes, με σκοπό να ενσωματωθούν στο αρχικό μήνυμα, το οποίο πάλι θα περάσει από μια διαδικασία κρυπτογράφησης.

Η κρυπτογράφηση TKIP έχει, γενικά δύο τελικές εισόδους, όπου είναι το αποτέλεσμα της προαναφερμένης διαδικασίας και το αποτέλεσμα της διαδικασίας που περιγράφεται στη συνέχεια. Γίνεται λόγος,για μία μορφή δέντρου μέχρι τις τελικές εισόδους.

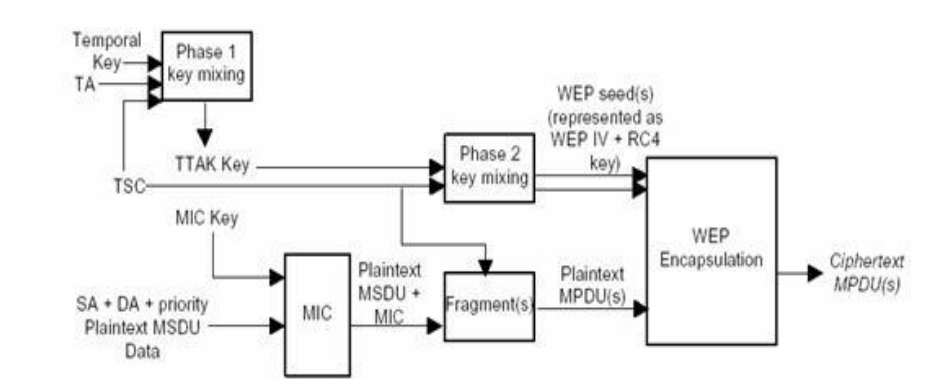
Στη δεύτερη διαδικασία, ο TKIP, έχει σαν εισόδους τα παρακάτω.

- Το Κλειδί Συνόδου (TK), το οποίο έχει τιμή 128bit, όμοια με αυτή του WEP.
- Τη φυσική διεύθυνση του αποστολέα (TA)
- Ένα πίνακα μη γραμμικό
- Τα τέσσερα σημαντικά byte του μετρητή της TKIP ακολουθίας. Ο μετρητής ακολουθίας (TSC) αποτελείται από την διεύθυνση του αποστολέα (SA), τη διεύθυνση παραλήπτη (DA), την ιεραρχία και τα δεδομένα.

Τα στοιχεία αυτά θα περάσουν στη διαδικασία Keymixing και θα παραχθεί η τιμή TTAK (TKIP mixed Transmit Address and Key). Η τιμή TTAK αποθηκεύεται προσωρινά και

χρησιμοποιείται μέχρι και για 216 πακέτα. Λόγω της χρήσης της διεύθυνσης του αποστολέα, η παραπάνω διαδικασία, παράγει διαφορετική τιμή για κάθε συσκευή του δικτύου, παρότι γίνεται χρήση του ίδιου κλειδιού κρυπτογράφησης. Μετά την παραγωγή της, η TTAK, χρησιμοποιείται σαν είσοδος στητρίτη διαδικασία.

Στην 3η διαδικασία η TTAK, τα 2 λιγότερο σημαντικά Bytestou TSC και το κλειδί TK περνούν ξανά από Key Mixing όπου και παράγεται το τελικό κλειδί κρυπτογράφησης. Στη συνέχεια μπαίνει σε λειτουργία η όλη γνωστή διαδικασία της WEP κρυπτογράφησης.



Εικόνα 20-Διαδικασία TKIP κρυπτογράφησης

Τον επόμενο χρόνο η Wi-Fi Alliance δημιούργησε το WPA (Wi-Fi protected access) που αποτέλεσε σημαντική βελτίωση του TKIP καθώς υπερτερούσε σε επίπεδα όπως προστασία δεδομένων και ελέγχου πρόσβασης.

3.5 WPA

Λόγω των προβλημάτων και των αδυναμιών που παρουσίαζε το WEP αναπτύχθηκε το WPA(Wi-Fi Protected Access). Το WPA αύξησε σημαντικά το επίπεδο ασφάλειας στα ασύρματα δίκτυα καθώς παρέχει σε κάθε πακέτο της πληροφορίας κλειδί, έλεγχο ακεραιότητας και διάνυσμα αρχικοποίησης.

Όπως και στο WEP, το WPA κρυπτογραφεί πληροφορίες, ενώ ταυτόχρονα εκτελεί ελέγχους, ώστε να εξασφαλίσει ότι το κλειδί ασφαλείας δικτύου δεν έχει τροποποιηθεί. Επιπλέον, το WPA ελέγχει την ταυτότητα των χρηστών και εξασφαλίζει ότι μόνον εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο. Εάν το υλικό δικτύωσής λειτουργεί τόσο με WEP όσο και με WPA, η συνιστώμενη λύση είναι το WPA.

Το WPA παρέχει δυνατότητα χρήσης προ-μοιρασμένου κλειδιού, έτσι ο διαχειριστής του δικτύου εισάγει μία λέξη-κλειδί (WPA key) στο access point που αποτελεί μέσω έγκρισης για οποιοδήποτε τερματικό επιθυμεί να συνδεθεί στο δίκτυο. Το WPA key αποτελείται από 6 ως 63 αλφαριθμητικούς χαρακτήρες. Σε περίπτωση επίθεσης στο δίκτυο ένα αδύναμο κλειδί θεωρείται τρωτό σημείο, γι' αυτό το λόγω προτείνεται ένας τυχαίος αριθμός 13 ψηφίων και άνω.

Εικόνα 21-AccessPointIinterface, ρυθμίσεις ασυρμάτου δικτύου

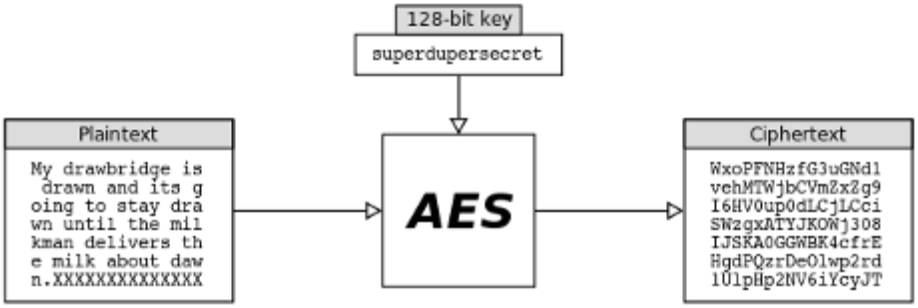
Στη θέση της κρυπτογράφησης WEP, συχνά, χρησιμοποιείται το AES (Advanced Encryption Standard). Το πρότυπο AES δεν παρέχεται σε κάθε συσκευή και αφορά καθαρά και μόνο τον κατασκευαστή του οδηγού της συσκευής.

3.5.1 ΤΙ ΕΙΝΑΙ ΤΟ AES

Για καλύτερη προστασία των δεδομένων και την ασφάλεια του wi-fi δικτύου ,το WPA κάνει χρήση δύο αλγορίθμων κρυπτογράφησης. Χρησιμοποιεί τον RC4 και τον AES. Ο AES διαδέχθηκε τον DES το 2001, κάνοντας χρήση του αλγορίθμου Rijndael.

Ο αλγόριθμος Rijndael δημιουργήθηκε από τους Vincent Rijmen και Joan Daemen. Η κρυπτογράφηση του Rijndael εφαρμόζεται σε μία σταθερού μεγέθους ομάδα από bits, με την ονομασία blocks.

Σε αυτόν τον αλγόριθμο χρησιμοποιούνται 2 είσοδοι, το προαναφερθέν block και το μυστικό κλειδί ώστε να ξεκινήσει η λειτουργία της κρυπτογράφησης. Τα μεγέθη των block που μπορεί να υποστηρίξει ο AES είναι τα εξής 128, 192 ή 256bits. Η δεύτερη είσοδος, μυστικό κλειδί, δεν έχει σταθερό μέγεθος. Ένα απλουστευμένο παράδειγμα με block 128bits φαίνεται στην παρακάτω εικόνα.

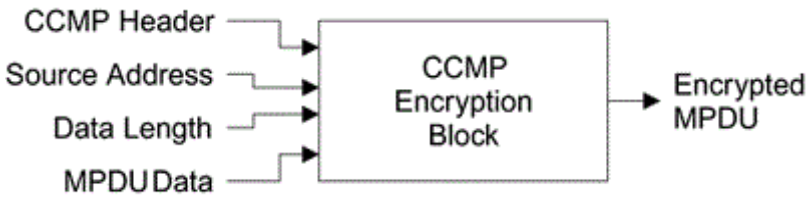


Εικόνα 22-Παράδειγμα AES κρυπτογράφησης

3.5.2AES – CCMP

Στα δίκτυα IEEE 802.11, η νεότερης γενιάς τεχνολογία ασφάλειας, εμφανίστηκε το 2004 με την έκδοση IEEE802.11i . Έχει εφαρμογή στο επίπεδο MAC του δικτύου και ονομάζεται CCMP (Counter mode with Cipher block chaining Message authenticatıon code Protocol). Η μέθοδος αυτή λειτουργεί στα πλαίσια του AES.

Λειτουργεί με κλειδί 128bit και blockμεγέθους 128bit, σύμφωνο με τον AES. Η έξοδος της κρυπτογράφησης του CCMP έχει ως αποτέλεσμα την μεγέθυνση του πακέτου πληροφορίας κατά 16Bytes. Τα 16 Bytes αποδίδονται 8 στην επικεφαλίδα του αλγορίθμου και τα υπόλοιπα 8 στο MIC (Message Integrity Code).



Εικόνα 23- Είσοδοι και αποτέλεσμα CCMP κρυπτογράφησης

Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη πακέτων

3.6 WPA 2

Το WPA 2 αποτελεί την εξέλιξη του WPA και εφαρμόζεται στην έκδοση IEEE 802.11i ασυρμάτων δικτύων. Υποστηρίζει όλες της προηγούμενες τεχνολογίες κρυπτογράφησης και επικύρωσης (TKIP, AES, EAP και τεχνολογία PSK). Τα wi-fi δίκτυα που υποστηρίζουν το WPA και τη νεότερη έκδοση του διευκολύνουν τη μεταφορά δεδομένων.

Εικόνα 24-Access Point Iinterface, ρυθμίσεις ασυρμάτου δικτύου με AES

Σημαντική βελτίωση ήταν η ενσωμάτωση του αλγορίθμου CCMP, που έδινε τη δυνατότητα μιας αρκετά ισχυρής κρυπτογράφησης.Ο νέος αλγόριθμος αντικατέστησε τον RC4. Ο CCMP χρησιμοποιεί πίνακα αρχικοποίησης 48bit και AES κλειδιά μεγέθους 128bit για την ασφαλή μετάδοση του πακέτου. Αυξάνοντας, έτσι την ασφάλεια του δικτύου από επαναλαμβανόμενες επιθέσεις.

Στην παραπάνω εικόνα χρησιμοποιείται το WPA2 Personal. Το WPA 2 έχει δύο υποκατηγορίες την Personalκαι την Enterpsrise. Η διαφορά τους είναι πως, στην κατηγορία personal,το τερματικό προκειμένου να συνδεθεί στο δίκτυο πρέπει να γνωρίζει το WPA Shared key, ενώ στην Enterprise η σύνδεση πιστοποιείται μέσω ενός εξυπηρετητή.

3.7 ROBUST SECURE NETWORK (RSN)

Το Δίκτυο Ανθεκτικής Ασφάλειας (RSN) είναι ένας νέος τύπος δικτύου στο πρότυπο IEEE802.11i.

Λόγω των πολλών περιορισμών στην προσβασιμότητα απαιτούνται συγκεκριμένες συνθήκες ασφάλειας. Προκειμένου να αναβαθμιστεί ο εξοπλισμός του δικτύου (τερματικά και access points) στα νέα δεδομένα, δημιουργήθηκε το TSN (Transitional Security Network) , που σημαίνει Δίκτυο Μεταβατικής Ασφάλειας.

Το TSN δίνει τη δυνατότητα στους συνδεδεμένους χρήστες να συνεργάζονται με όλες τις προηγούμενες τεχνολογίες ασφάλειας δικτύων.

3.8 RSN&WPA

ToRSN αλλά και το WPA δημιουργήθηκαν για λόγους ασφάλειας και αποτελούν τρόπους κρυπτογράφησης σε ένα δίκτυο. Και τα δύο λειτουργούν σχεδόν με τον ίδιο τρόπο. Μία διαφορά τους είναι πως το RSN χρησιμοποιεί ως μέθοδο κρυπτογράφησης τον αλγόριθμο CCMP και σαν εναλλακτικό τον TKIP, ενώ ο WPAχρησιμοποιεί τον TKIP.

Η αρχιτεκτονική του RSN είναι παρόμοια με πρωτοκόλλων που χρησιμοποιούν το AES, σε σχέση με το WPA που τείνει σε αυτών που χρησιμοποιούν το RC4.

Το RSN, αλλά και το WPA, λύνει το πρόβλημα διανομής κλειδιών που έχει το WEP όταν ο αριθμός των χρηστών αυξηθεί πέρα από το προσδοκώμενο.

ΚΕΦΑΛΑΙΟ 4 – ΕΠΙΘΕΣΕΙΣ ΣΕ ΔΙΚΤΥΑ Wi-Fi

Το φυσικό μέσω μετάδοσης σε ένα wi-fi δίκτυο είναι η ατμόσφαιρα, αυτό καθιστά το δίκτυο ευάλωτο σε επιθέσεις. Ως επίθεση ορίζεται η μη εξουσιοδοτημένη παρέμβαση στο δίκτυο, στην ασφάλεια της μεταδιδόμενης πληροφορίας αλλά και διακύβευση υποκλοπής της. Λόγοι επίθεσης σε κάποιο wi-fi δίκτυο μπορεί να είναι απλή περιέργεια για προσπάθεια πρόσβασης σε κάποιο ξένο δίκτυο, κλοπή πληροφοριών, έλεγχο κίνησης ή απλά δωρεάν πρόσβαση, μέσω του υπάρχοντος wi-fi δικτύου, στο διαδίκτυο. Οι τύποι επιθέσεων είναι παθητικές (passive) ή ενεργητικές (active).

4.1 ΠΑΘΗΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Ως παθητικές επιθέσεις σε ένα δίκτυο θεωρούνται αυτές που έχουν σκοπό τη συλλογή πληροφοριών και προσωπικών δεδομένων ή ο έλεγχος κίνησης σε ένα wi-fi δίκτυο. Δεν θεωρούνται, εκ φύσεως επιβλαβείς, καθώς επιθυμούν τη διατήρηση του δικτύου.

Σε τέτοιου τύπου επιθέσεις ο επιτιθέμενος παρακολουθεί συνεχώς την εισερχόμενη και εξερχόμενη κίνηση ενός ασύρματου δικτύου.

Συλλογή πληροφοριών και συλλογή πακέτων είναι οι δύο τύποι παθητικών επιθέσεων.

Στη συλλογή πληροφοριών ο επιτιθέμενος συλλέγει τις πληροφορίες κατευθείαν από το access point. Αυτό έχει σαν αποτέλεσμα να γίνεται γνωστό το SSID του δικτύου, το κανάλι εκπομπής, η διαδικασία κρυπτογράφησης και οι φυσικές (MAC) διευθύνσεις των υπολοίπων συνδεδεμένων συσκευών αλλά και το πλήθος τους.

Στη συλλογή πακέτων ο επιτιθέμενος αντλεί πληροφορίες για το δίκτυο. Μπορεί να διαβάσει το μηνύματα που στέλνονται ανάμεσα στο δίκτυο, μαθαίνει διευθύνσεις των χρηστών και γενικά αντλεί πολλές πληροφορίες για το δίκτυο.

Η φύση αυτών των επιθέσεων είναι σιωπηλή, γι 'αυτό είναι δύσκολο να ανιχνευθούν. Χρησιμοποιώντας αυτήν την επίθεση, ο επιτιθέμενος μπορεί να κάνει μια ενεργή επίθεση στο ασύρματο δίκτυο.

4.2 ΕΝΕΡΓΗΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Ως ενεργητικές ορίζονται οι επιθέσεις κατά τις οποίες ο επιτιθέμενος είναι συνδεδεμένος στο δίκτυο. Διαχωρίζονται ανάλογα με τον λόγο της επίθεσης.

Κατηγορίες ενεργητικών επιθέσεων είναι οι παρακάτω:

- Ανάκτηση WEP κλειδιού (WEP Cracking)
- Τροποποίησης Δεδομένων (Man In The Middle Attack)
- Άρνησης Υπηρεσίας (Denial of Service)

4.2.1 ΑΝΑΚΤΗΣΗWEPΚΛΕΙΔΙΟΥ (WEP Cracking)

Σκοπός της επίθεσης είναι ή πρόσβαση στο δίκτυο και όλες τις δυνατότητες του. Σε αυτού του τύπου επιθέσεις ο χρήστης του δικτύου δεν αποτελεί καν στόχο. Η πρόσβαση γίνεται με την απόκτηση του κλειδιού του δικτύου. Σε προηγούμενη ενότητα αναφέρθηκαν οι αδυναμίες του WEP χάρις τις οποίες μπορεί πολύ εύκολα να βρεθεί το μυστικό κλειδί του δικτύου.

Το WEP cracking βασίζεται στην απόκτηση μεγάλου όγκου IV’s πακέτων. Αυτό γίνεται με την συλλογή και αναμετάδοση πακέτων ARP (Address Resolution Protocol) στο σημείο πρόσβασης.

4.2.2 ΕΠΙΘΕΣΗ ΤΡΟΠΟΠΟΙΗΣΗΣ ΔΕΔΟΜΕΝΩΝ (Maninthemiddle)

Μία τέτοια επίθεση έχει σκοπό να κλέψει δεδομένα, που μοιράζονται σε ένα δίκτυο, εμέσα. Στόχος μπορεί να είναι η τροποποίηση – κλοπή αρχείων, τροποποίηση διεύθυνσης ηλεκτρονικού ταχυδρομείου μέχρι την ακραία περίπτωση της υποκλοπή πληροφοριών τραπεζικής συναλλαγής.

Οι αμυντικοί μηχανισμοί που έχουν αναπτυχθεί, όπως το VPN ή το IPSec, προστατεύουν από μία άμεση επίθεση.

Ο επιτιθέμενος μπορεί να αλλάξει τη διεύθυνση αποστολής της πληροφορίας, στέλνοντας τη στον ίδιο ή σε μία διεύθυνση της επιλογής του. Ουσιαστικά βρίσκεται στη μέση της επικοινωνίας των χρηστών του δικτύου και μπορεί να εμφανίζεται στους, απλούς, χρήστες του δικτύου ως accesspoint.

Η επίθεση αυτή είναι γνωστή ως Man in the Middle Attack.

Κατά την Man in the middle επίθεση, βρισκόμαστε ανάμεσα στη επικοινωνία 2 τερματικών συσκευών. Το Α τερματικό στέλνει πληροφορία στο Β και αντίστροφα. Ο επιτιθέμενος βρίσκεται στη μέση της μετάδοσης προσποιούμενος πότε το Α ή το Β, ακόμα και το accesspoint, στέλνοντας μηνύματα ως ο καθένας εκ των δύο.

4.2.3 ΕΠΙΘΕΣΗ ΜΕ ΜΕΤΑΜΦΙΕΣΗ (Spoofing)

Στην επίθεση με μεταμφίεση, ο επιτιθέμενος παρουσιάζεται σαν έναν υπάρχον χρήστη του δικτύου, με σκοπό να αποκτήσει τις πληροφορίες που χρειάζεται. Όπως είναι λογικό, ο επιτιθέμενος γνωρίζει τον τρόπο πρόσβασης του πραγματικού χρήστη.

Με την μέθοδο spoofingo επιτιθέμενος δεν γίνεται αντιληπτός. Από τη στιγμή που η συσκευή επίθεσης συνδεθεί κανονικά στο δίκτυο, έχει πρόσβαση, με πλήρη δικαιώματα, σε κάθε δεδομένο, πληροφορία ή εφαρμογή που μοιράζεται στο δίκτυο.

4.2.4 ΕΠΙΘΕΣΗ ΑΡΝΗΣΗΣ ΥΠΗΡΕΣΙΑΣ (Denial of service)

Ο συγκεκριμένος τύπος επίθεσης είναι ο πιο δημοφιλής σε περίπτωση που ο επιτιθέμενος επιθυμεί να καταστρέψει το wi-fi δίκτυο. Η μη λειτουργικότητα του δικτύου διαρκεί για κάποιο χρονικό διάστημα και έπειτα επανέρχεται.

Η μέθοδος, αυτής της επίθεσης, είναι ο καταιγισμός του δικτύου με πακέτα που στέλνει ο επιτιθέμενος. Αυτό έχει σαν αποτέλεσμα την κατανάλωση, μεγάλης, υπολογιστικής ισχύς του access point και τέλος την κατάρρευσή του.

Ένας ακόμα τρόπος είναι η παρεμβολή ισχυρών σημάτων στην περιοχή εκπομπής του δικτύου και στην κατάλληλη ζώνη συχνοτήτων. Λόγω αυτών των παρεμβολών οι σταθμοί του δικτύου δεν μπορούν να επικοινωνήσουν μεταξύ τους.

Αναφέρονται οι πιο συχνοί τρόποι επίθεσης Denial of Service (DoS)

- **Ping Of Death**: Η τεχνική αυτή βασίζεται σε αδυναμίες του πρωτοκόλλου TCP/IP. Λειτουργεί αποστέλλοντας ένα διάγραμμα δεδομένων μεγαλύτερο από ότι συνήθως με αποτέλεσμα την κατάρρευση του παραλήπτη.

Αποτελεί παλιά μορφή επίθεσης και πλέον δεν είναι σε θέση να προκαλέσει ζημιά σε ένα wi-fi δίκτυο καθώς τα σύγχρονα συστήματα ασύρματης δικτύωσης έχουν αναπτύξει τεχνολογίες άμυνας απέναντι της.

- **Smurf**: Σε αυτού του είδους την επίθεση στέλνεται μεγάλος αριθμός πακέτων ICMP echo request στις διευθύνσεις broadcast διαφόρων δικτύων. Τα πακέτα αυτά, κατόπιν τροποποίησης, δεν αναγράφουν την IP διεύθυνση του θύτη αλλά του θύματος και με δεδομένη την αποστολή τους σε broadcast διευθύνσεις δικτύων, κάθε τερματικό που ανήκει σε αυτά τα δίκτυα απαντά προς το θύμα με πακέτο ICMP echo reply. Με αυτόν τον τρόπο ο παραλήπτης των ICMP echo reply να οδηγείτε στην κατάρρευση.

  Οι επιθέσεις τύπου Smurf είναι οι πιο δύσκολα αντιληπτές, στην κατηγορία των DoS. Ένα wi-fi δίκτυο, με την κατάλληλη συντήρηση και επίβλεψη, δεν διατρέχει μεγάλο κίνδυνο από μία τέτοια επίθεση. Έχουν πλέον αναπτυχθεί τεχνολογίες τέτοιες ώστε ναμπορούν να τις εμποδίσουν.

- **FloodAttack**: Πρόκειται για την πιο διαδεδομένη DoS επίθεση. Λειτουργεί, στέλνοντας πακέτα, στον Server του δικτύου, περισσότερα από αυτά που μπορεί να επεξεργαστεί. Η λογική της είναι αρκετά απλή και αν ο serverέχει σωστή κατανομή εύρους, στα τερματικά του, τότε δεν θα επηρεαστεί.

- **Syn**: Είναι μια ακόμα επίθεση μου χρησιμοποιεί τις αδυναμίες του πρωτόκολλου TCP/IP καθώς εκμεταλλεύεται την διαδικασία συγχρονισμού και επιβεβαίωσης προκριμένου να δημιουργηθεί η σύνδεση. Ο επιτιθέμενος στέλνει συνεχώς μηνύματα κατά τη διαδικασία συγχρονισμού στο access point με αποτέλεσμα να μην μπορεί να τα επεξεργαστεί ώστε να στείλει μηνύματα επιβεβαίωσης. Όλο αυτό συμβάλλει στη μη δημιουργία σύνδεσης σε όποιον άλλο σταθμό επιθυμεί.

- **Teardrop**: Πρόκειται για μια, ακόμη, παλιάς μορφής επίθεση που πλέον δεν απειλεί ένα wi-fiδίκτυο. Στην επίθεση αυτή στελνόταν από τον επιτιθέμενο αλληλεπικαλυπτόμενα μηνύματα και ο παραλήπτης προσπαθούσε να τα ανακατασκευάσει με αποτέλεσμα να διακόπτεται η λειτουργία του.

ΚΕΦΑΛΑΙΟ 5 – ΕΠΙΘΕΣΗ ΣΕ ΕΝΑ ΔΙΚΤΥΟ WI-FI

Σε αυτό το κεφάλαιο θα γίνει μια σειρά επιδείξεων επιθέσεων σε ένα wi-fi δίκτυο. Το δίκτυο αυτό θα αποτελείται από ένα σταθερό υπολογιστή συνδεδεμένο, με μία ασύρματη κάρτα δικτύου, σε ένα access point. Η επίθεση στο δίκτυο θα γίνει από ένα laptopπου διαθέτει κάρτα ασυρμάτου δικτύου .

5.1 ΕΞΟΠΛΙΣΜΟΣ ΚΑΙ ΕΡΓΑΛΕΙΑ

Αναφέρθηκαν γενικά τι θα χρησιμοποιηθεί κατά την επίθεση. Στη συνέχεια γίνεται μια αναλυτική παρουσίαση όλου του εξοπλισμού.

- **Desktop**: Πρόκειται για σταθερό υπολογιστή στον οποίον θα απευθυνθούν οι επιθέσεις. Συνδέεται στο δίκτυο με μια κάρτα DIGITUS WIRELESS 150NUSB 2.0 Antenna Adapter. Η ασύρματη κεραία έχει ταχύτητα μέχρι 150Mbps, χρησιμοποιεί το πρότυπο IEEE 802.11n στην μπάντα των 2.4GHz, είναι συμβατή με τα 802.11g/d και παρέχει WEP, WPA, WPA2 τρόπους κρυπτογράφησης. Το desktop δουλεύει με γνήσιο λειτουργικό Microsoft Windows 7 Ultimate 32bit. Παρακάτω φαίνονται τα τεχνικά χαρακτηριστικά του.

  - **CPU:** Intel(R) Pentium(R) G3220 @ 3.00GHZ
  - **Μνήμη**: 4Gb DDR3
  - **Μητρική**: Asus H81M-C

  Πρόκειται για ένα αξιόλογο και σύγχρονο υπολογιστή με αρκετά καλή ταχύτητα επεξεργασίας.

- **Laptop**: Είναι η συσκευή με την οποία θα εκτελεστούν οι επιθέσεις στο ασύρματο δίκτυο. Είναι ένα laptop Toshiba Satellite C660 D-1D5 με ενσωματωμένη κάρτα δικτύου Realtek RTL8188CE με υποστήριξη IEEE 802.11b/g/nστη μπάντα των 2.4GHz με μετάδοση δεδομένων έως και 150Mbps. ως λειτουργικό σύστημα, για λόγο των επιθέσεων, χρησιμοποιείται το Backtrack5 R3 από livecd. Πιο αναλυτικά τα χαρακτηριστικά του υπολογιστή.

  - **CPU**: AMD E450 APU with Radeon(tm) HD Graphics 1.65GHz
  - **Μνήμη**: 4GB

  Πρόκειται για laptopπροσωπικής χρήσης με αρκετά καλές δυνατότητες.

- **AccessPoint**: Πρόκειται για ένα router ZXHNH108L και παρέχεται από τον πάροχο υπηρεσιών διαδικτύου Forthnet. Στη συνέχεια είναι η εικόνα του interface του AP για το ασύρματο δίκτυο.

Εικόνα 25-Wirelessinterface

Φαίνεται από την εικόνα πως χρησιμοποιεί το πρότυπο 802.11b και κρυπτογράφηση WEP με κλειδί το kcah2. Το συγκεκριμένο router υποστηρίζει ως και WPA2-PSK κρυπτογράφηση αλλά για χάριν της επίδειξης ρυθμίστηκε για WEP.

- **Backtrack**: Είναι ένα ελεύθερο λειτουργικό σύστημα βασισμένο σε Linuxκαι διατίθεται δωρεάν μέσω διαδικτύου. Λειτουργεί με liveCD ή με bootableusb, παρέχοντας τη δυνατότητα εγκατάστασης στο σκληρό δίσκο ως μόνιμο λειτουργικό. Σκοπός της δημιουργίας του είναι η αξιολόγηση της ασφάλειας ασυρμάτων δικτύων, χρησιμοποιήθηκε βέβαια και για εκπαιδευτικούς λόγους.

Εικόνα 26-BackTrackLogo

Μερικά από τα σημαντικότερα εργαλεία του λειτουργικού είναι τα παρακάτω:

- Metasploit
- Δυνατότητα RFMONγια ασύρματες κάρτες δικτύου
- Kismet
- Nmap
- Ettercap
- Wireshark

Τα εργαλεία που διαθέτει το Backtrack αντιστοιχούν στις παρακάτω κατηγορίες:

- InformationGathering
- NetworkMapping
- VulnerabilityIdentification
- Web ApplicationAnalysis
- Radio Network Analysis (802.11,Bluetooth,Rfid)
- Penetration (Exploit & Social Engineering Toolkit)
- PrivilegeEscalation
- Maintaining Access
- DigitalForensicsReverseEngineering
- VoiceOver IP

Εκτός από τα εξειδικευμένα προγράμματα για την ασφάλεια των δικτύων περιλαμβάνει και απλό softwareόπως Mozilla Firefox, Pidgin, K3bκαι XMMS.

5.2 ΠΡΟΕΤΟΙΜΑΣΙΑ ΓΙΑ ΤΗΝ ΕΠΙΘΕΣΗ

Το εγκατεστημένο λειτουργικό σύστημα, στο laptop από το οποίο θα εκτελεστούν οι επιθέσεις, είναι το Microsoft Windows 7 Home Premium 64-bit. Για λόγους που εξυπηρετούν τις επιθέσεις στο δίκτυο θα χρησιμοποιηθεί το BackTrack5.

Αυτό γίνεται με το να επιλέξουμε, από το BIOS του laptop, ως πρώτη συσκευή εκκίνησης το drive του DVD, που περιέχει το liveCD του Backtrack. Έτσι το ξεκινά πρόγραμμα εκκίνησης. Στην 1η ένδειξη boot χρησιμοποιείται το πλήκτρο enter και στη δεύτερη πρέπει να πληκτρολογηθεί το startx που είναι ο default χρήστης του λειτουργικού.

Με την έναρξη του backtrack εμφανίζεται η αρχική οθόνη. Πρωταρχικός σκοπός είναι η διαμόρφωση του δικτυακού interface. Για να γίνει αυτό, πρέπει να ανοίξει η κονσόλα που βρίσκεται στο κάτω αριστερά μέρος της αρχικής οθόνης και μετά να πληκτρολογηθεί η παρακάτω εντολή.

```
# ifconfig
```

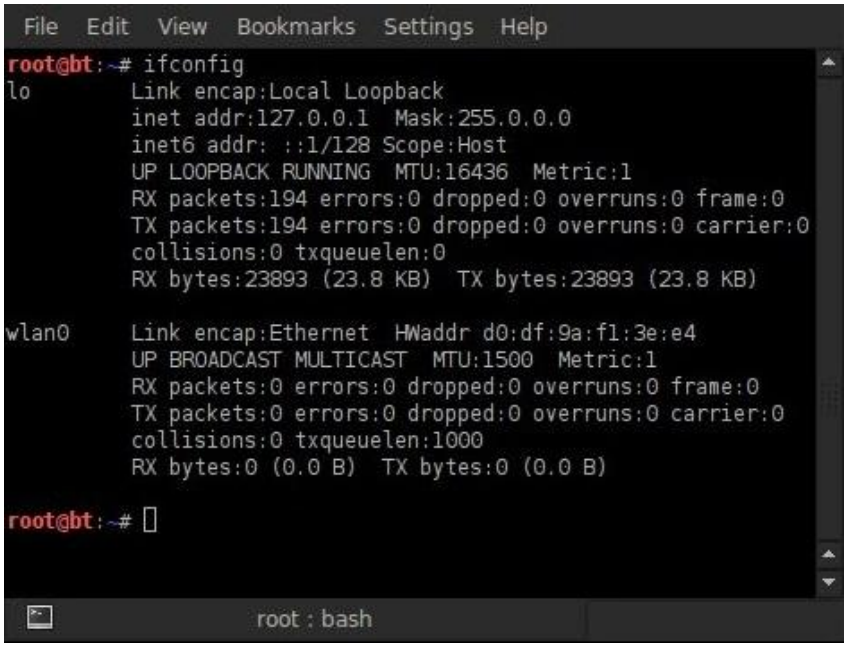
Όπου μας δείχνει το αρχικό δικτυακό interface όπως παρακάτω.

Εικόνα 27-Networkinterface

Για να είναι δυνατή η επίθεση πρέπει να ενεργοποιηθεί το wlan0, γιατί αρχικά είναι προεπιλεγμένη ως απενεργοποιημένη. Θα απενεργοποιηθεί και η θύρα ethernet–eth0. Εισάγουμε τις παρακάτω εντολές.

```
# ifconfig eth0 down
# ifconfig wlan0 up
```

Επαναλαμβάνοντας την αρχική #ifconfig εμφανίζεται μόνο το wlan0 interface όπως παρακάτω.



Εικόνα 28-Network interface μόνο με ασύρματη κάρτα

Με ενεργή, πλέον, μόνο την κάρτα ασυρμάτου δικτύου μπορούν να ξεκινήσουν οι επιθέσεις. Η παραπάνω διαδικασίες θα επαναλαμβάνονται και θα έχουν εκτελεστεί πριν από κάθε επίθεση.

Επόμενο βήμα είναι η αρχή των επιθέσεων στο δίκτυο.

5.3 WEPCRACKING

WEP cracking είναι η πραγματοποίηση μία επίθεσης με σκοπό την ανάκτηση του κλειδιού ώστε να συνδεθεί ο επιτιθέμενος στο δίκτυο. Πριν από κάθε επίθεση κάνουμε μία επανεκκίνηση το σύστημα και διαμορφώνουμε εκ νέου το interface της κάρτας δικτύου του laptop και έχουμε την αρχική μορφή με ενεργοποιημένη μόνο την ασύρματη κάρτα δικτύου.

Η επίθεση WEP cracking λειτουργεί με τη δημιουργία ενός πακέτου ARP στο οποίο αποκρίνεται το Access Point και ακολουθεί η συλλογή IV'σε ένα αρχείο της επιλογής μας ώστε να αποκρυπτογραφηθεί το WEP key.

5.3.1 airmon-ng

Με το πέρας της προετοιμασίας της ασύρματης κάρτας, συνέχεια έχει να τεθεί η ασύρματη κάρτα σε Monitor Mode. Η εντολή #airmon-ng εξυπηρετεί στο να μπει η ασύρματη κάρτα monitor mode-mon0. Στην κατάσταση monitor mode-mon0 η κάρτα είναι σε θέση να αντιλαμβάνεται όλα τα πακέτα που διακινούνται στο ασύρματο δίκτυο. Είναι επίσης απαραίτητη ώστε να επιτευχθεί η διαδικασία injection,των πακέτων, στο δίκτυο, που θα είναι αναγκαία στη συνέχεια.

Η γενική μορφή της #airmon-ngείναι η εξής:

airmon-ng <start/stop><interface><channel>όπου:

Το start ή stop ενεργοποιεί ή απενεργοποιεί, αντίστοιχα, το monitor mode.

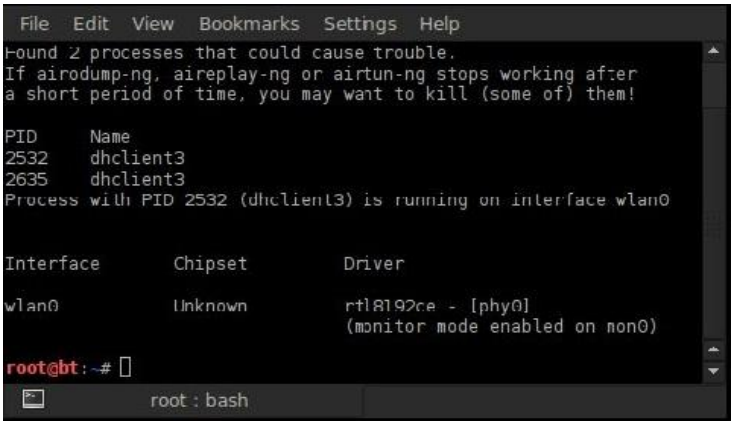
Στη θέση interface βάζουμε την κάρτα η οποία θα μπει σε monitor mode.

Ο αριθμός του καναλιού που εκπέμπει το AP μπαίνει στη θέση channel εφόσον είναι γνωστό.

Για να μπει το wlan0 σε monitor mode, στο παράδειγμα που εκτελείται, εισάγουμε στην κονσόλα την παρακάτω εντολή.

airmon-ng start wlan0

Στην κονσόλα θα εμφανιστεί το παρακάτω αποτέλεσμα.



Εικόνα 29-Εισαγωγή σε Monitore mode

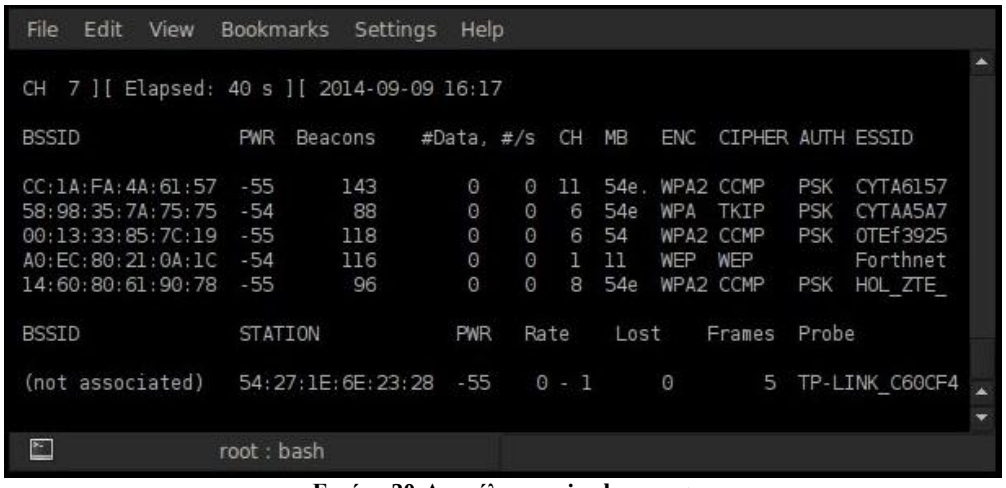
5.3.2 airodump-ng

Επόμενο βήμα είναι να βρεθεί το δίκτυο από το οποίο θέλουμε να αποσπάσουμε το WEP key. Η εντολή για αυτή τη διαδικασία είναι η #airodump-ng και μας εμφανίζει όλα τα δίκτυα στην εμβέλεια μας και παρέχει χρήσιμες πληροφορίες όπως τα BSSID των δικτύων, το κανάλι στο οποίο εκπέμπει το καθένα, το ESSID, η μέθοδος κρυπτογράφησης και άλλα που φαίνονται στην πιο κάτω εικόνα.

Για να εμφανιστούν τα δίκτυα,που υπάρχουν στην εμβέλειά μας εισάγουμε την επόμενη εντολή.

airodump-ng wlan0

Το αποτέλεσμα της εντολής φαίνεται στην παρακάτω εικόνα.



Εικόνα 30-Αποτέλεσμα airodump-ng

Το δίκτυο Forthnet είναι αυτό στο οποίο θα κάνουμε την επίθεση. Από την κονσόλα φαίνεται πως το δίκτυο έχει κρυπτογράφηση WEP και βρίσκεται στο κανάλι 1 με BSSID A0:EC:80:21:0A:1C.

Η εντολή #airodump-ng, με κατάλληλη σύνταξη, χρησιμοποιείται και για την σύλληψη πακέτων και WEP Ivs ώστε να είναι δυνατή η αποκρυπτογράφηση του WEP key.

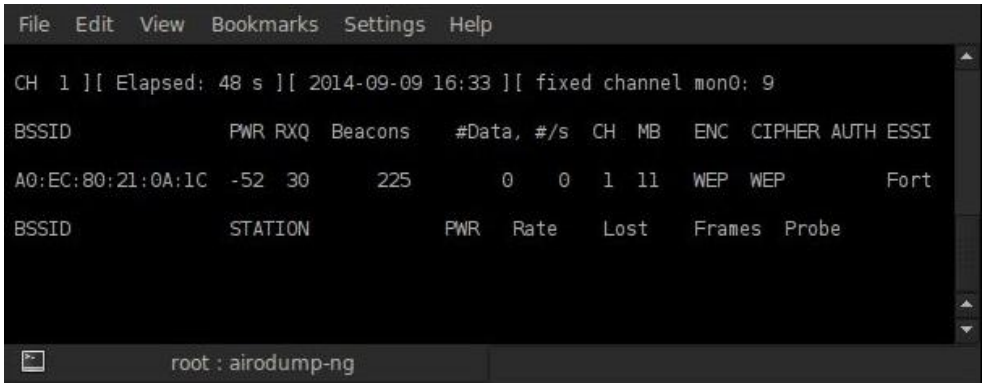
Το επόμενο βήμα είναι η επίθεση στο access point. Για να συμβεί αυτό πρέπει να αποθηκεύσουμε τα δεδομένα που θα λαμβάνουμε σε ένα αρχείο. Το αρχείο θα ονομαστεί capture, και σε αυτό θα αποθηκευτούν τα IV's Για αυτή τη διαδικασία εισάγουμε την παρακάτω εντολή.

airodump-ng--bssid<δικτύου> -c <καν.δικτ.> -w <ονομ.αρχειου>mon0

δηλαδή

airodump-ng --bssidA0:EC:80:21:0A:1C -c 1 -w capture mon0

Το αποτέλεσμα της εντολής είναι το παρακάτω.



Εικόνα 31-2ο αποτέλεσμα airodump-ng

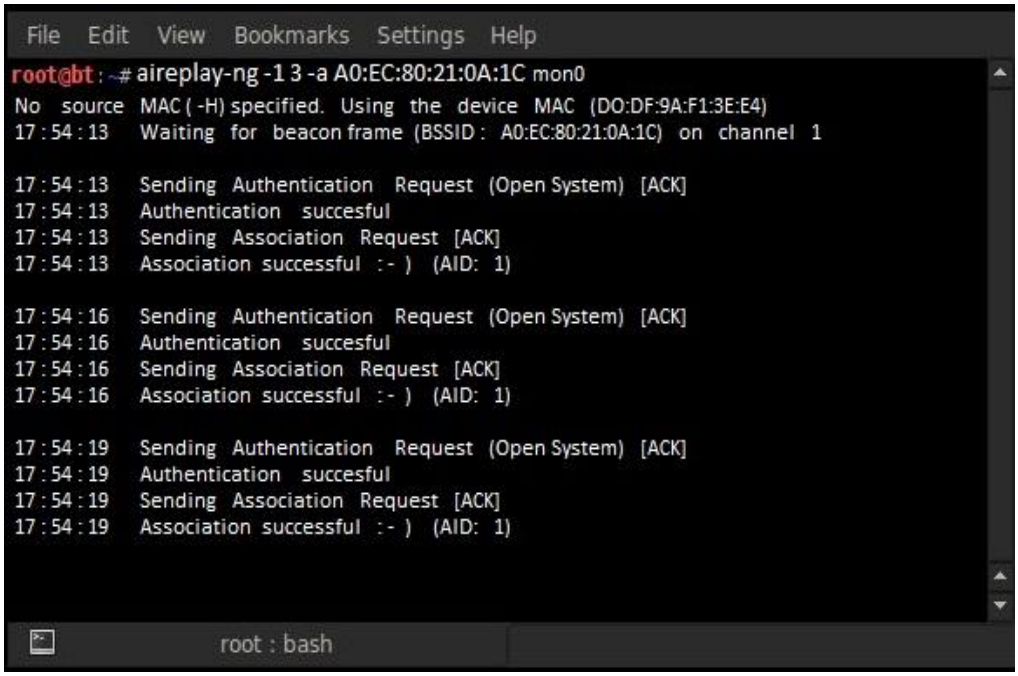
Στην παραπάνω εικόνα είναι φανερό πως τα πακέτα δεδομένων είναι μηδενικά. Για να αποκρυπτογραφηθεί το WEP key χρειάζεται καταγραφή μεγάλου αριθμού πακέτων δεδομένων, τουλάχιστον 20000 Για το λόγο αυτό υπάρχουν εντολές ώστε να αυξήσουν τον αριθμό των δεδομένων, διαφορετικά θα πρέπει να περάσει αρκετό χρονικό διάστημα ώστε να έχουμε τον κατάλληλο αριθμό. Στόχος είναι η αύξηση του αριθμού δεδομένων για την απόκτηση του κλειδιού του access point.

5.3.3 aireplay-ng

Με την εντολή #aireplay-ng δίνεται η δυνατότητα ψεύτικης ταυτοποίησης στο ασύρματο δίκτυο. Για να επιτευχθεί αυτή η ταυτοποίηση πρέπει να εισαχθεί η παρακάτω εντολή.

aireplay-ng -1 3 -a A0:EC:80:21:0A:1C mon0

Το αποτέλεσμα της εντολής φαίνεται παρακάτω.



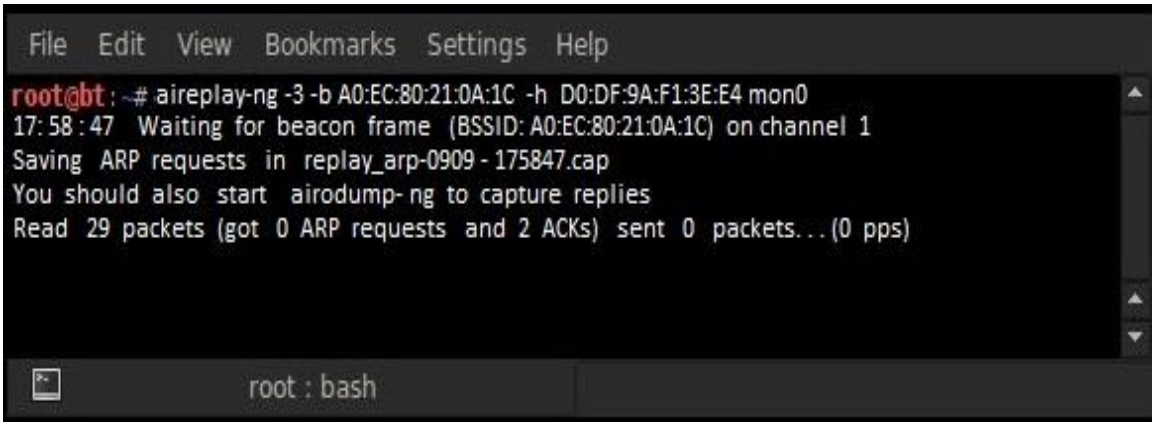
Εικόνα 32-Fake Authentication

Φαίνεται στην εικόνα πως η σύνδεση πραγματοποιήθηκε.

Στη συνέχεια με την #aireplay-ng είναι δυνατό να σταλούν πακέτα στο AP και το laptop να λαμβάνει πιο πολλά πακέτα δεδομένων και αυτό θα οδηγήσει στην συλλογή περισσοτέρων IVs. Για να συμβεί αυτό πρέπει να εισαχθεί η παρακάτω εντολή.

aireplay-ng -3 -b A0:EC:80:21:0A:1C–hD0:DF:9A:F1:3E:E4mon0

Όπου D0:DF:9A:F1:3E:E4 η MAC διεύθυνση του wlan0. Έτσι έχουμε την παρακάτω εικόνα.



Εικόνα 33-Αποστολή πακέτων

Αυτό έχει σαν αποτέλεσμα την ακρόαση ARP αιτήσεων και την είσοδο πακέτων στο δίκτυο.

5.3.4 aircrack-ng

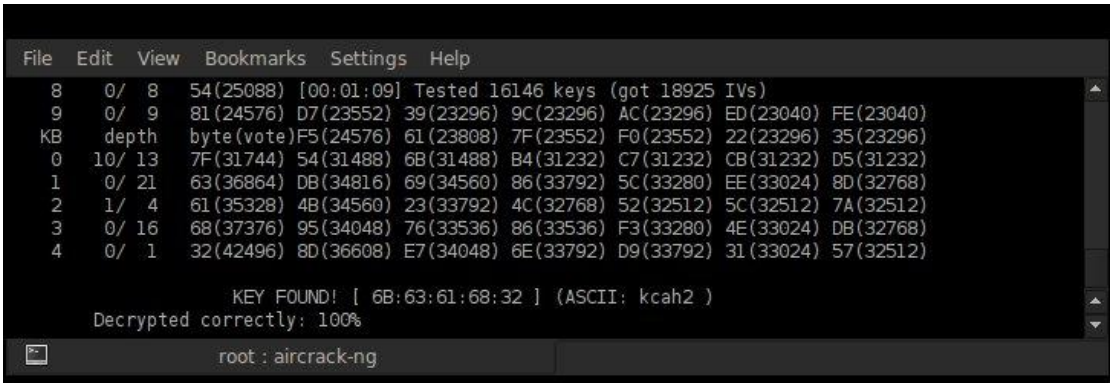
Όταν ο αριθμός πακέτων IVs είναι αρκετά μεγάλος, για παράδειγμα 20000 τότε χρησιμοποιούμε το εργαλείο aircrack και εισάγουμε στην κονσόλα την παρακάτω εντολή.

- aircrack-ng <ονομ.αρχειου>

για το συγκεκριμένο αρχείο που δημιουργήσαμε προηγουμένως πληκτρολογούμε

- aircrack-ng capture-01.cap

και αν τα Ivs είναι αρκετά, τότε εμφανίζεται το παρακάτω αποτέλεσμα.

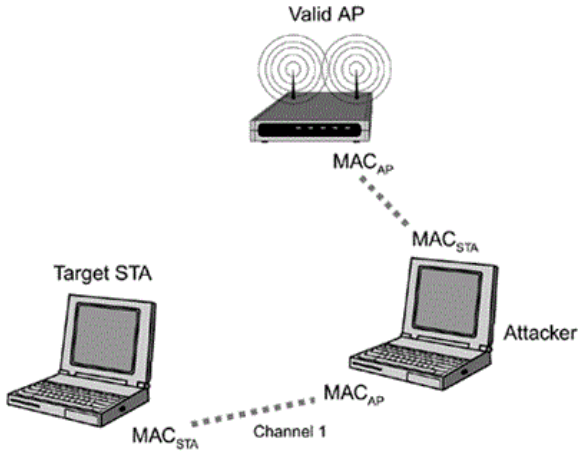


Εικόνα 34-Αποτέλεσμα aircrack-ng

Στην εικόνα φαίνεται το WEP κλειδί του δικτύου, και μπορεί να διασταυρωθεί με το κλειδί στο wireless interface του router.

5.4 MAN IN THE MIDDLE ATTACK

Η Man In The Middle Attack χρησιμοποιεί την διαδικασία ARP poisoning, όπου ο επιτιθέμενος παρουσιάζεται ως AP και μπορεί να βλέπει και να διαμορφώνει τα πακέτα του μοιράζονται από το θύμα στο AP. Παρεμβάλλεται, δηλαδή στο μέσο της επικοινωνίας client – AP.



Εικόνα 35-Man In the Middle

Για αυτή την επίθεση θα χρησιμοποιηθεί το εργαλείο, του BackTrack, Ettercap. Πρόκειται για ένα εργαλείο που παρέχει όλες τις δυνατότητες για μία τέτοια επίθεση. Διαθέτει

δυνατότητα προβολής χρηστών του δικτύου, συνδέσεων και δυνατότητα προβολής των πακέτων που διακινούνται στο δίκτυο.

Η MitMattackπροϋποθέτει την σύνδεση στο δίκτυο όπου βρίσκεται ο χρήστης, για το συγκεκριμένο παράδειγμα, το laptop, από τον οποίο θέλουμε να αποσπάσουμε πληροφορίες. Σε περίπτωση που δεν υπάρχει εξουσιοδοτημένη σύνδεση στο wi-fi δίκτυο πρέπει να επαναληφθεί η διαδικασία WEP cracking ώστε να αποκτηθεί το κλειδί.

Με την απόκτηση της σύνδεσης πρέπει να πληκτρολογηθεί στην κονσόλα του BackTrack η παρακάτω εντολή.

```
# ettercap –G
```

Ως αποτέλεσμα είναι να εμφανίζεται η αρχική οθόνη του ETTERCAP όπως φαίνεται στη εικόνα.

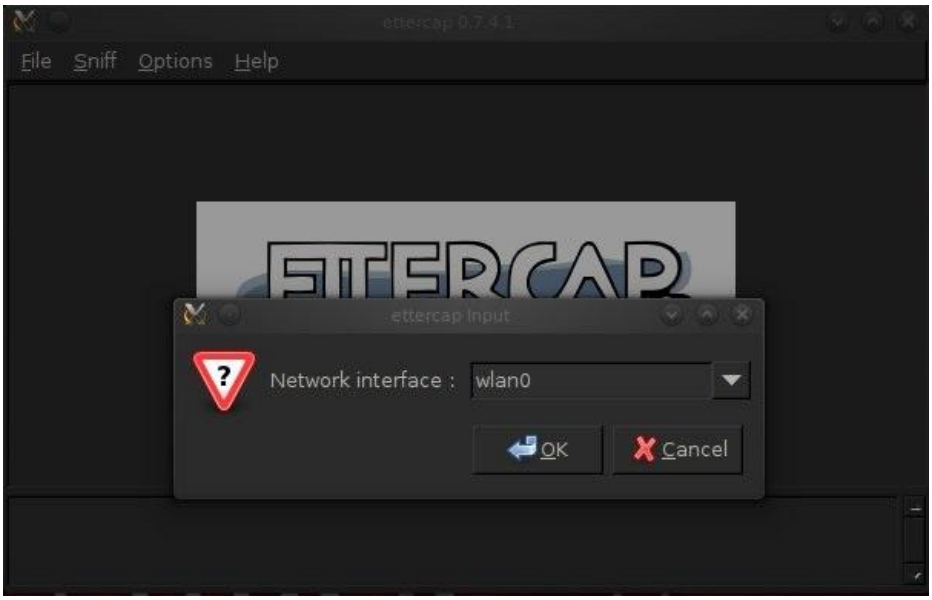
Εικόνα 36-Εκκίνηση ETTERCAP

Με την έναρξη του προγράμματος ορίζεται η μάσκα υποδικτύου που βρίσκεται ο στόχος. Στις επιλογές του προγράμματος υπάρχουν τα File, Sniff, Options, Help. Για να εισαχθεί η subnetmaskθα επιλεχθεί η Options και στη συνέχεια Set netmask, όπου και πληκτρολογείται η 255.255.255.0

Εικόνα 37-Εισαγωγή subnetmask

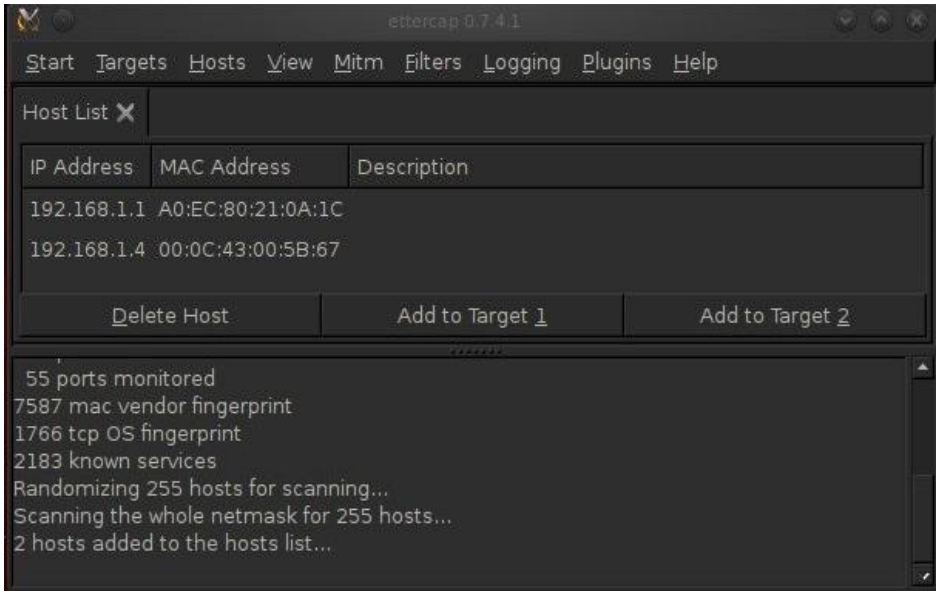
Η διαδικασία της εισαγωγής της netmaskμπορεί να παρακαμφθεί γιατί εισάγεται αυτόματα κατά τη διαδικασία εύρεσης στόχων.

Το επόμενο βήμα είναι η επιλογή του wireless interface. Επιλέγεται το Sniff και στη συνέχεια Unified Sniffing. Από τη λίστα επιλέγεται το interface που θα χρησιμοποιηθεί, στο συγκεκριμένο παράδειγμα το wlan0.



Εικόνα 38-Επιλογή interface για Sniffing

Έχοντας επιλέξει πλέον Interface, γίνεται αναζήτηση χρηστών που είναι συνδεδεμένοι στο δίκτυο. Επιλέγεται Hosts και έπειτα το κουμπί Scan for hosts. Με το πέρας της διαδικασίας, από την ίδια διαδρομή επιλέγεται το κουμπί HostList. Εμφανίζονται με αυτόν τον τρόπο οι χρήστες του δικτύου και είναι πλέον δυνατό να επιλεχθεί ο στόχος, όπως φαίνεται στη συνέχεια.

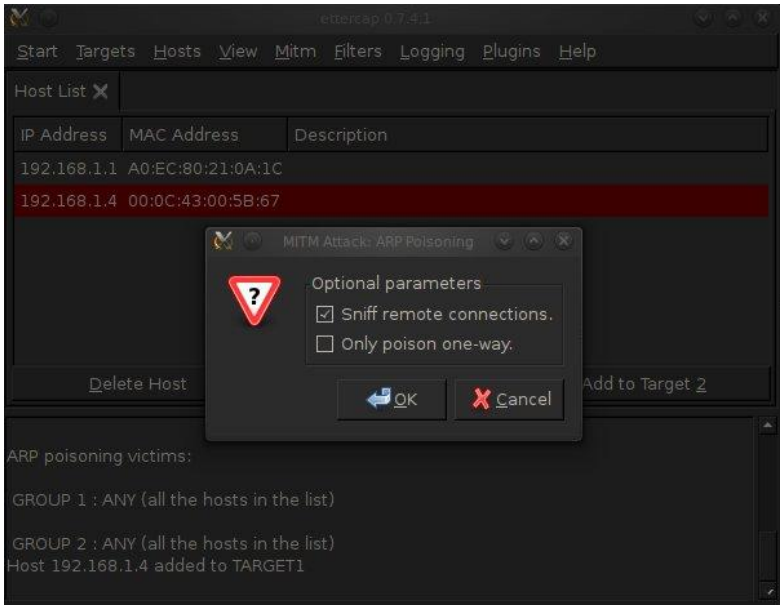


Εικόνα 39-Hosts δικτύου

Στο Host List εμφανίζονται οι χρήστες του δικτύου. Στην συγκεκριμένη περίπτωση είναι μόνο 2 γιατί το δίκτυο είναι μικρό σε μέγεθος. Σε περίπτωση που υπήρχαν παραπάνω

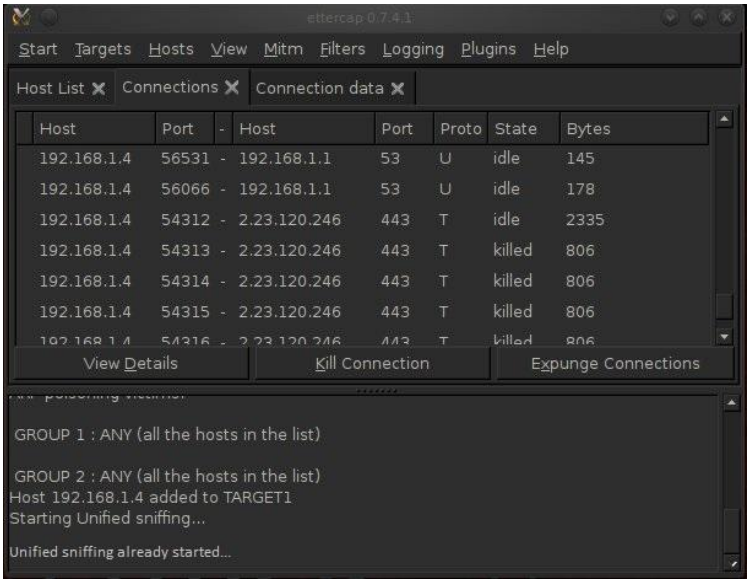
χρήστες θα εμφανιζόταν όλοι στη λίστα. Η πρώτη IP που εμφανίζεται είναι το AP και η δεύτερη ανήκει στο desktop στο οποίο στοχεύουν οι επιθέσεις. Κάνοντας κλικ στην IP του desktop επιλέγεται οστόχος.

Με την επιλογή των στόχων μπορεί να ξεκινήσει η διαδικασία του ARP poisoning. Για να εκκινηθεί η διαδικασία επιλέγεται Mitm και στη συνέχεια το κουμπί Arppoisoning. Στο παράθυρο που εμφανίζεται ,επιλέγεται το Sniff remote connections και τέλος OK.



Εικόνα 40-ARP poisoning

Το τελευταίο βήμα είναι η επιλογή Start και το κουμπί Start sniffing. Μετά από όλα τα παραπάνω βήματα, εάν ο χρήστης-θύμα του υπολογιστή που ορίστηκε σαν στόχος εισάγει κάποιον κωδικό ή όνομα, θα είναι δυνατό να εντοπιστεί και να ανακτηθεί.



Εικόνα 41-Sniffing

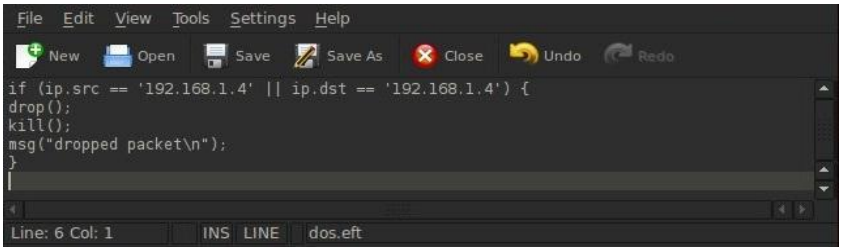
5.5 DoS

Σε αυτή την ενότητα θα εκτελεστεί μία επίθεση DenialOfService.Θα χρησιμοποιηθεί ξανά το εργαλείο Ettercap καθώς παρέχει τη δυνατότητα compilekαι κατασκευή φίλτρων, τα οποία κρίνονται απαραίτητα για μία επίθεση DoS, για να μην είναι δυνατό ο χρήστης να χρησιμοποιήσει το δίκτυο.

Η δημιουργία του φίλτρου προϋποθέτει την σύνταξη κώδικα. Για τη σύνταξη του κώδικα θα χρησιμοποιηθεί ο επεξεργαστής κειμένου του BackTrack, το Kwrite. Στο Kwrite γράφουμε τον παρακάτω κώδικα:

```
if (ip.src == 'TargetIP' || ip.dst == 'TargetIP') {
drop();
kill();
msg("dropped packet\n");
}
```

ΌπουTarget IP εισάγεται η IP του desktop. Για να λειτουργήσει το φίλτρο θα πρέπει να αποθηκευτεί με την κατάληξη *.eft. Τοόνομα είναι καθαρά θέμα επιλογής του συντάκτη. Στην συγκεκριμένη περίπτωση επιλέχθηκε το dos.



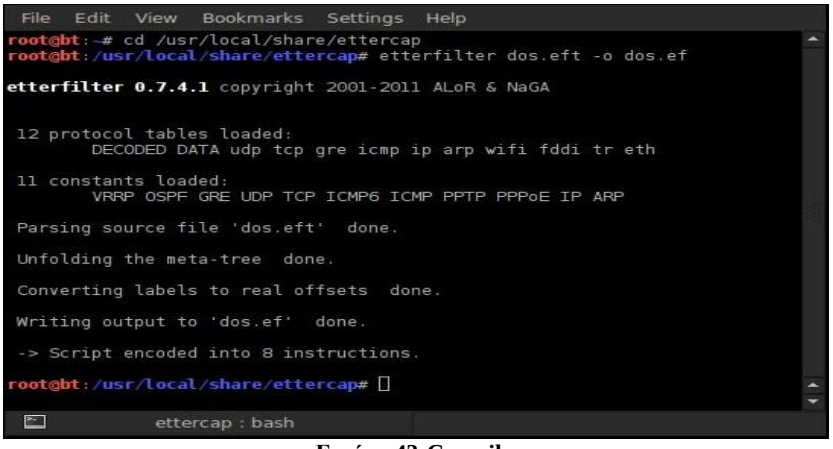
Εικόνα 42-Σύνταξη κώδικα στο KWrite

Σώζουμε ως dos.eftστο ίδιο path που βρίσκεται τοettercap. Το BackTrack τρέχει με liveCD και το ettercap είναι στο φάκελο **/usr/local/share/ettercap**. Στη συνέχεια, είναι απαραίτητο για να λειτουργήσει το φίλτρο, πρέπει να γίνει compile στον κώδικα. Θα χρησιμοποιηθεί η κονσόλα με την παρακάτω εντολή

cd /usr/local/share/ettercap

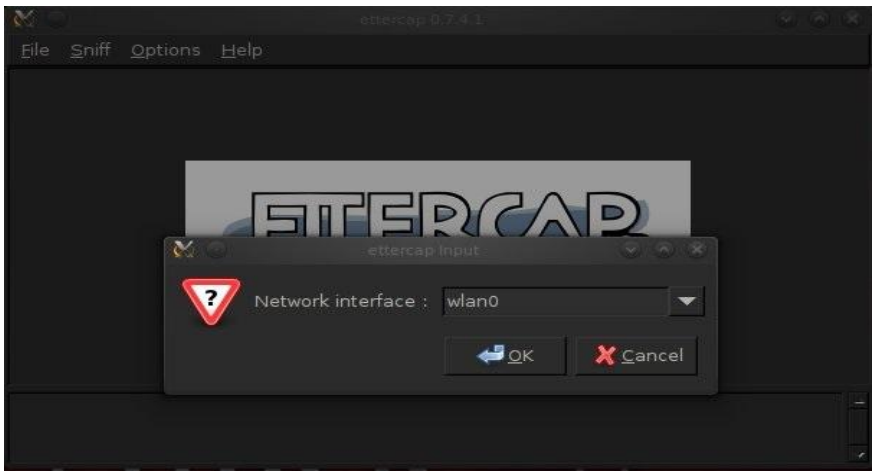
cd /usr/local/share/ettercap # etterfilterdos.eft –o dos.ef

Αν ο κώδικας δεν έχει συντακτικά λάθη θα εμφανιστεί το παρακάτω αποτέλεσμα.



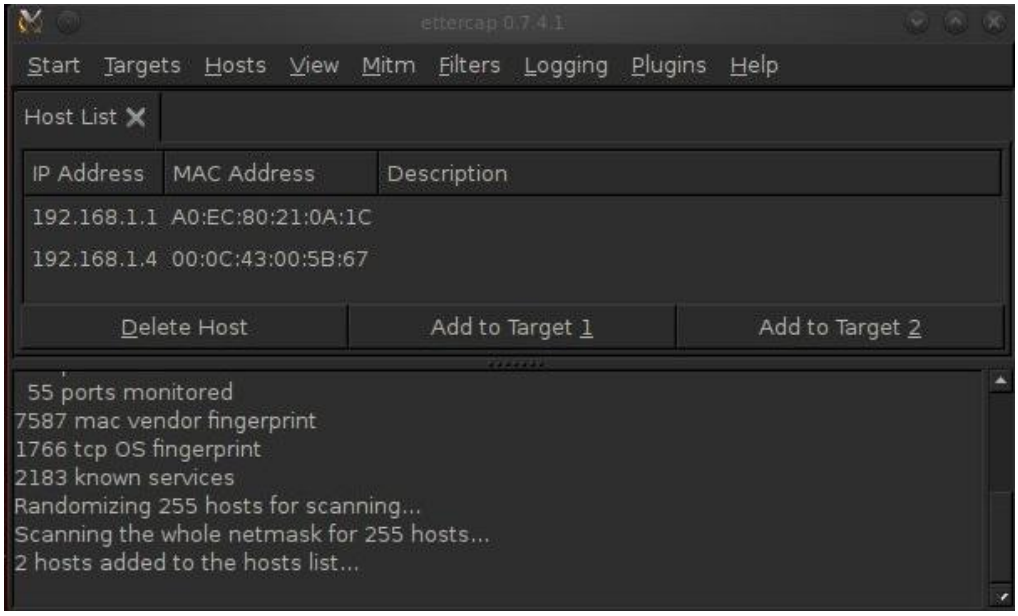
Εικόνα 43-Compile

Έπειτα πρέπει να ξεκινήσει το Ettercap και για αυτό εισάγεται η ανάλογη εντολή στην κονσόλα και εμφανίζεται η αρχική του εικόνα. Πρέπει να επιλεχθεί το ανάλογο interface έτσι επιλέγεται Sniff και Unified Sniffing και το wlan0.



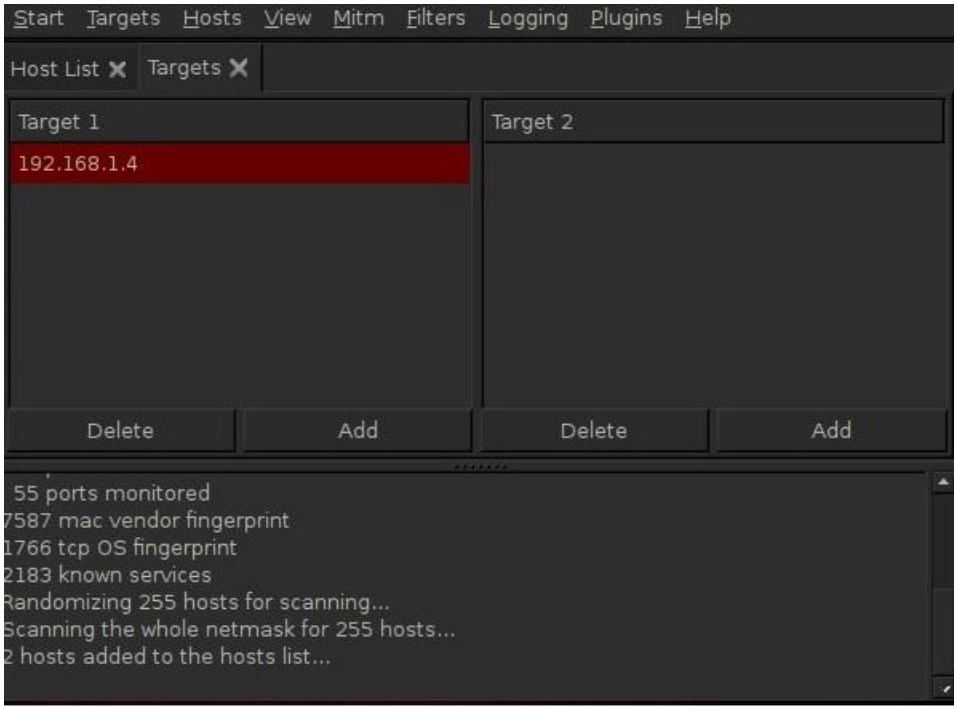
Εικόνα 44- Επιλογή interface για Sniffing

Επόμενο βήμα είναι η επανάληψη αναζήτησης χρηστών στο δίκτυο με την επιλογή Hosts και στη συνέχεια Scan for hosts. Το δίκτυο είναι ίδιο με την προηγούμενη επίθεση έτσι οι χρήστες είναι οι ίδιοι. Η μάσκα υποδικτύου εισάγεται αυτόματα



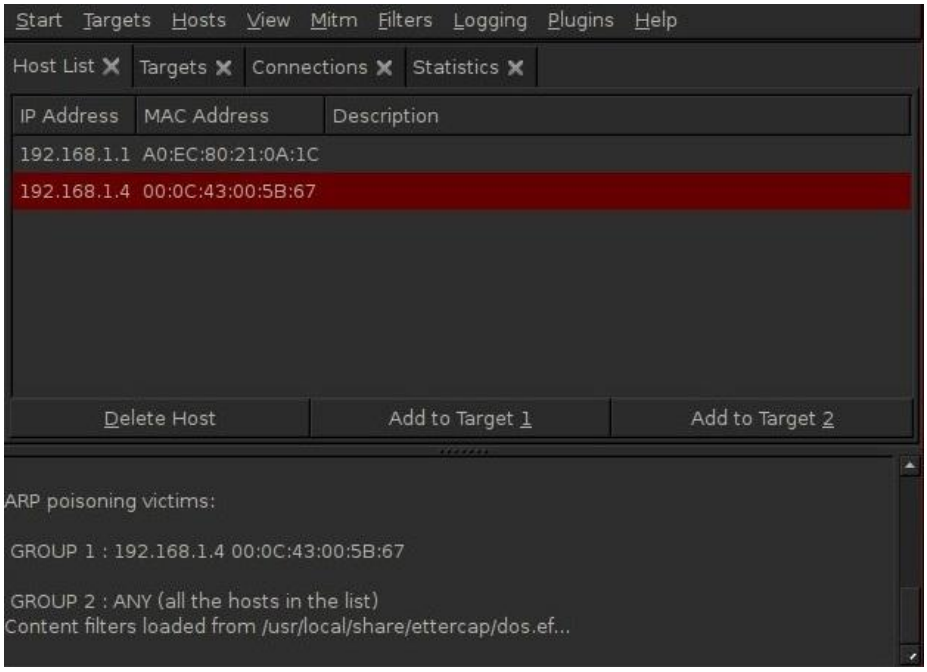
Εικόνα 45-Hosts δικτύου

Σε αυτό το σημείο πρέπει να επιλεχθεί ο χρήστης στον οποίον θα γίνει η επίθεση με ARP πακέτα. Επιλέγεται ο χρήστης, με την IP του desktop, και το επιλέγεται κουμπί του Add to Target 1.



Εικόνα 46-Προσθήκη στόχου

Σειρά έχει η διαδικασία ARP Poisoning. Επιλέγεται το κουμπί Mitm και Sniff remote connections και OK. Τέλος πρέπει να επιλεχθεί το φίλτρο που θα χρησιμοποιηθεί. Επιλέγεται Filters και Load Filter. Πρέπει να επιλεχθεί ο φάκελος του ettercap, στο σωστό path, και επιλέγεται το αρχείο dos.ef, που αποτελεί την compiled μορφή του dos.eft. Με την επιλογή του φίλτρου εμφανίζεται η παρακάτω εικόνα.



Εικόνα 47-Εκκίνηση DoS

Όταν εμφανιστεί η παραπάνω εικόνα, σημαίνει πως η επίθεση έχει ολοκληρωθεί. Αν ο χρήστης του desktop επιχειρήσει να ανοίξει μια σελίδα στον browser του, το αποτέλεσμα θα είναι να καθυστερήσει και τέλος να μην ανοίξει προβάλλοντας κάποιο αίτημα αποτυχίας.

ΚΕΦΑΛΑΙΟ 6 – ΑΣΦΑΛΙΖΟΝΤΑΣ ΤΟ ΔΙΚΤΥΟ Wi-Fi

Από τις παραπάνω επιθέσεις γίνεται κατανοητή η αδυναμία της WEP κρυπτογράφησης να ασφαλίσει ουσιαστικά ένα wi-fi δίκτυο, από κάποιον που πραγματικά θέλει να το προσβάλει. Η ραγδαία εξάπλωση των wi-fi δικτύων και η ευκολία των επιθέσεων έφεραν στο προσκήνιο ανάγκες για νέες και αποτελεσματικότερες τεχνολογίες κρυπτογράφησης.

Μέχρι και σήμερα έχουν αναπτυχθεί νέοι μέθοδοι ασφάλειας και κρυπτογράφησης, όπως το WPA και το WPA2, όπως αναφέρθηκαν σε προηγούμενο κεφάλαιο. Πέρα από τις μεθόδους κρυπτογράφησης υπάρχει και άμεση ανάγκη ασφάλισης του δικτύου. Στις πιο πολλές περιπτώσεις, ο στόχος είναι ένα router, και για αυτό απαιτείται η ανάγκη για ανάλογη διαμόρφωση του routerή access point.

Ένα router ,που παρέχει ένα δίκτυο wi-fi, προσφέρεται από τον πάροχο έχει εφαρμοσμένες τις εργοστασιακές ρυθμίσεις. Συνήθως είναι εμφανές το SSID και λόγω των λίγων παρόχων υπηρεσιών διαδικτύου, ειδικά στη χώρα μας, είναι αρκετά γνωστές οι default gateways. Π.χ. 192.168.2.1, 192.168.1.1, κ.α. οπότε διευκολύνεται η πρόσβαση.

Με το προεπιλεγμένο interface είναι εύκολη η πρόσβαση στο router.

Υπάρχουν τρόποι που ο καθένας θα μπορούσε να ασφαλίσει ένα ιδιωτικό δίκτυο κάνοντας το πιο αξιόπιστο με κάποιες παραμετροποιήσεις. Στην ουσία αυτές οι παραμετροποιήσεις απλά όμως καθυστερούν απλά την παραβίαση του δικτύου.

6.1 ΑΠΛΕΣ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΕΙΣ

Σε αυτή την ενότητα αναφέρονται ενδεικτικά τρόποι παραμετροποίησης του router-access pointγια βελτίωση της ασφάλειας

- **Default Gateway**
  Ένας αρκετά καλός τρόπος ασφάλισης του route-access point είναι η αλλαγή της προεπιλεγμένης πύλης του interface σε κάποια IP πέρα από τις γνωστές. Τα δίκτυα με διευθύνσεις 192.168.x.x παρέχονται για εσωτερική χρήση. Αυτό δίνει τη δυνατότητα επιλογής κάποιας gateway διαφορετικής από τις συνηθισμένες, εάν αυτό είναι δυνατό. Για να πραγματοποιηθεί αυτό πρέπει να απενεργοποιηθεί ο DHCP server και οι IP του δικτύου να ρυθμιστούν χειροκίνητα.

- **Κωδικοί πρόσβασης σε router/access point**
  Συνήθως οι κωδικοί που προαπαιτούνται για τη σύνδεση στο interface είναι αρκετά απλοί και παρόμοιοι, όπως admin ή user. Αυτό είναι μια σημαντική αδυναμία. Αλλάζοντας το username και το password με κάποιους προσωπικούς και σαν αποτέλεσμα πιο ισχυρούς αποτρέπεται ο επιτιθέμενος από το να τροποποιήσει τις ρυθμίσεις της συσκευής.

- **Απόκρυψη / Αλλαγη SSID**
  Όλα τα APs/routers έχουν ένα Service Set Identifier (SSID), όπου και αποτελεί το όνομα του δικτύου. Σκοπός του SSID είναι η δυνατότητα αναγνώρισης του δικτύου από τις συσκευές στη εμβέλεια του. Συνήθως υπάρχουν περισσότερα από ένα ασύρματα δίκτυα στην ίδια περιοχή. Το SSID δημιουργήθηκε ώστε να ξεχωρίζουμε τα ασύρματα δίκτυα μεταξύ τους. Όλα τα routers/APs εκπέμπουν ένα σήμα (beacon) κάθε 1/10 του δευτερολέπτου και το οποίο περιλαμβάνει και το SSID. Το σήμα ανιχνεύεται από τις ασύρματες συσκευές και δίνει τις πληροφορίες που χρειάζονται για να συνδεθούν στο δίκτυο. Η κάθε συσκευή έχει συνήθως ως προεπιλεγμένο SSID το όνομα του κατασκευαστή. Ένας τρόπος ασφάλισης του δικτύου είναι η αλλαγή του SSID με κάποιο της επιλογής του ιδιοκτήτη. Η αλλαγή του SSID θα ήταν καλό να επαναλαμβάνετε συχνά.

- **WPA κρυπτογραφηση**
  Έχουν γίνει γνωστές οι αδυναμίες της WEP κρυπτογράφησης. Αυτό δίνει τη δυνατότητα σε κάποιον με κατάλληλο λογισμικό να παραβιάσει το δίκτυο και να πετύχει πρόσβαση στο μέσο. Η WPA κρυπτογράφηση υπερτερεί τηςWEP μεθόδου, ωστόσο υπάρχουν αδυναμίες που μπορεί να εκμεταλλευθεί κάποιος για να παραβιάσει το δίκτυο.

  Συγκεκριμένα, η WPA-PSK (WPA - Pre-Shared Key) είναι ιδιαίτερα ευάλωτη σε επιθέσεις λεξικού (dictionary attacks) αφού όταν ένας σταθμός ζητά να συνδεθεί με σταθμό βάσης (handshake), στέλνει πακέτα στα οποία οπωσδήποτε περιέχεται η μυστική λέξη κλειδί, που έχει οριστεί ως συνθηματικό ταυτοποίησης και εισόδου στο δίκτυο. Έτσι ο επιτιθέμενος που παρακολουθεί την επικοινωνία δυο σταθμών μπορεί νασυλλέξει πακέτα, ώστε να αξιοποιηθούν σε εφαρμογές που εκτελούν επιθέσεις λεξικού. Σε αυτά τα λεξικά υπάρχουν όλοι οι δυνατοί συνδυασμοί 8χαραχτήρων. Μία καλή λύση είναι η αλλαγή του κλειδιού 2-3 φορές το χρόνο. Το κατάλληλο κλειδί είναι αρκετά σημαντικό καθώς ένα κλειδί με μικρό μήκος, δηλαδή κάτω από 20 χαρακτήρες παρέχει μικρή ασφάλεια. Αν υποστηρίζεται η WPA2 κρυπτογράφηση,καλό θα ήταν να γίνεται χρήση του αλγορίθμου CCMP, εφόσον υποστηρίζεται, και όχι του συνδυασμού CCMP/TKIP ή AES/TKIP. Σε συσκευές με πιστοποίηση WPA, η χρήση του TKIP είναι προτιμότερη, παρόλα αυτά δε θεωρείται αρκετά επαρκής αφού ήδη έχουν βρεθεί σοβαρές αδυναμίες.

- **Απενεργοποιήση remote access**
  Πολλά, σύγχρονά, routers-Aps διαθέτουν δυνατότητα remote access (απομακρυσμένης πρόσβασης) στο interface τους μέσω διαδικτύου. Καλό θα ήταν η επιλογή αυτή να είναι απενεργοποιημένη εκτός και αν παρέχεται δυνατότητα επιλογής, τέτοια ώστε ο διαχειριστής του δικτύου, να καθορίζει ο ίδιος τα τερματικά από τα οποία θα συνδεθεί.

- **No wireless access**
  Κατά τη διάρκεια ασύρματης σύνδεσης σε ένα δίκτυο wi-fi, ο χρήστης, με προϋπόθεση την γνώση των κωδικών πρόσβασης, μπορεί να συνδεθεί στο interface του router/accesspoint. Αυτό κάνει το δίκτυο ευάλωτο. Παρέχεται η δυνατότητα ρύθμισης, τέτοια ώστε να μην είναι δυνατή η πρόσβαση στο interface τηςσυσκευής με ασύρματη πρόσβαση αλλά μόνο με ενσύρματη.

- **Συγκεκριμένες MAC διευθύνσεις**
  Η MAC adress είναι η φυσική διεύθυνση κάθε κάρτας ασυρμάτου ή ενσύρματου δικτύου. Η MAC address αποτελεί μοναδικό χαρακτηριστικό της κάθε συσκευής και είναι ένας αριθμός. Έχει μέγεθος 48bit και αποδίδεται από τον κατασκευαστή της κάρτας. Από τα 48bit, τα 24 αποτελούν το μοναδικό αναγνωριστικό του κατασκευαστή και τα υπόλοιπα 24 έναν αριθμό αναγνώρισης. Λόγω της μοναδικότητας που παρουσιάζει είναι εύκολο, από το διαχειριστή του δικτύου, να καθοριστούν, συγκεκριμένες, MAC διευθύνσεις που να έχουν τη δυνατότητα σύνδεση στο δίκτυο. Η παραπάνω διαδικασία γίνεται μέσω του interface του router/access point.

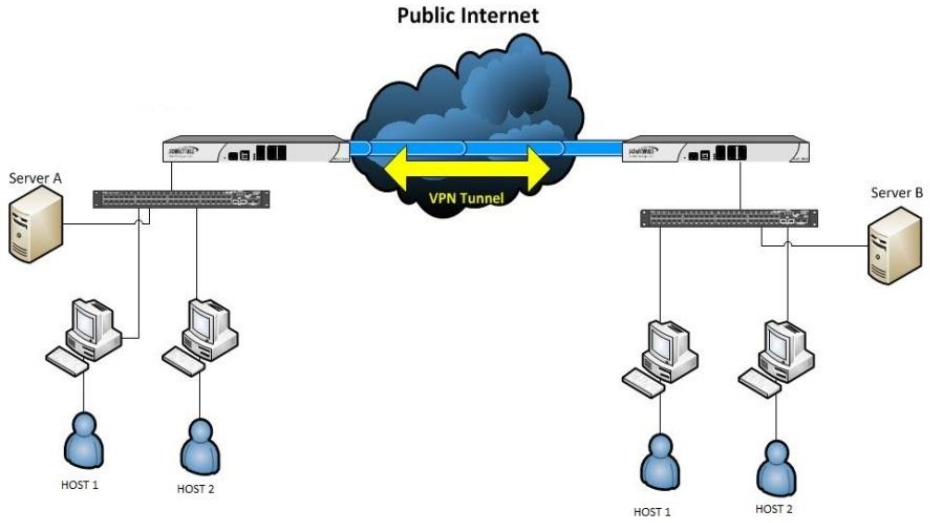
- **Μείωση εμβέλειας**
  Ένα router/access pointέχει σχετικά μεγάλη εμβέλεια. Ένας τρόπος μείωσης των πιθανών επιθέσεων είναι ή μείωση της εμβέλειας εκπομπής του σήματος. Με αυτό τον τρόπο περιορίζεται ο αριθμός των χρηστών που μπορούν να προσβάλουν το δίκτυο. Η δυνατότητα αυτή δεν δίνεται σε όλα τα AP. Σε περίπτωση που υπάρχει αυτή η δυνατότητα, τότε η εμβέλεια μπορεί να περιοριστεί στα όρια ενός δωματίου.

- **Infrastructure mode**
  Σε μια σύνδεση τύπου Infrastracture δεν επιτρέπεται η άμεση επικοινωνία 2 χρηστών του wi-fi δικτύου, χωρίς την παρεμβολή του AP. Η ρύθμιση σε infrastructure mode γίνεται από τις ρυθμίσεις της κάρτας δικτύου.

6.2 ΑΥΞΑΝΟΝΤΑΣ ΤΗΝ ΑΣΦΑΛΕΙΑ ΜΕ HARDWARE-SOFTWARE

Οι λύσεις της προηγούμενης ενότητας απλά καθυστερούσαν την επίθεση στο wi-fi δίκτυο και δυσκόλευαν σχετικά τη διαδικασία, ουσιαστικά όμως το δίκτυο παρέμενε ευάλωτο. Στη συνέχεια προτείνονται λύσεις σε επίπεδο λογισμικού και υλικού.

- **VPN (Virtual Private Network)**
  Το VPN είναι ένα ιδιωτικό κανάλι, το οποίο βρίσκεται πάνω σε ένα ήδη υπάρχον δίκτυο και υποστηρίζει υπηρεσίες κρυπτογράφησης, πιστοποίησης καιδιαχείρισης κλειδιών. Το πλεονέκτημα του είναι η ασφαλή μετακίνηση δεδομένωνανάμεσα στο δίκτυο.



Εικόνα 48-VPN

Όταν κάποιος θέλει να προσβάλει το δίκτυο μπορεί εύκολα να ανακτήσει τοWEP key και να συνδεθεί στο δίκτυο. ΤοVPN, όπως αναφέρθηκε, προσφέρει μέθοδο κρυπτογράφησης. Σε ένα δίκτυο που συμπεριλαμβάνει WEP και VPN κρυπτογράφηση, κατά τη διάρκεια της επίθεσης πρέπει να ανακτηθεί το WEP keyκαι στη συνέχεια το κλειδί της VPN κρυπτογράφησης.

Με την χρήση της VPN κρυπτογράφησης, ο επιτιθέμενος πρέπει να αναπαράγει τον κωδικό κρυπτογράφησης, να προσπεράσει την πιστοποίηση ή τον έλεγχο πρόσβασης. Αυτό έχει σαν αποτέλεσμα τοποσοστό επιτυχίας μιας τέτοιας επίθεσης είναι χαμηλό.

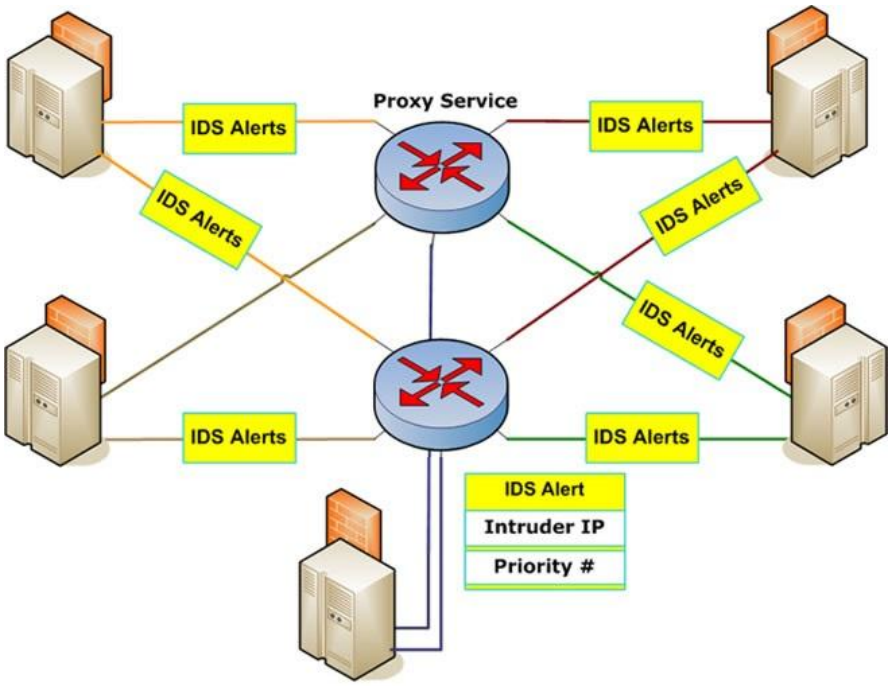
Ο συνδυασμός VPN και WEP είναι αρκετά αποτελεσματική έχει ένα βασικό μειονέκτημα. Για την παράλληλη λειτουργία απαιτείται διπλάσια υπολογιστική ισχύ. Οι 2 αυτές κρυπτογραφήσεις, όταν, εκτελούνται παράλληλα από ένα access point μειώνουν την ταχύτητα της μετάδοσης ως και 80% .

Επιπλέον, η χρήση ενός VPN δικτύου προϋποθέτει την εγκατάσταση λογισμικού σε κάθε τερματικό που επιθυμεί να συμμετάσχει στο δίκτυο.

- **IDS (Intrusion Detection Systems)**

Το IDS έχει στόχο να ανιχνεύσει πιθανές επιθέσεις σε κάποιο τερματικό του δικτύου και να προειδοποιήσει τους υπόλοιπους hosts. Παρέχεται με τη μορφή λογισμικό ή υλικού.

Υπάρχουν δυο κατηγορίες συστημάτων IDS. Το NetworkIDS (NIDS) και το HostIDS (HIDS). Η λειτουργία των HIDSs βασίζεται στην αναζήτηση εισβολής σε ένα μόνο τερματικό. Κάθε τερματικό του δικτύου θα πρέπει να χρησιμοποιεί δικό του HIDS. Τα NIDS αναλύουν την κίνηση που υπάρχει σε ολόκληρο το δίκτυο, για το λόγο αυτό τοποθετούνται σε switch ή hub του δικτύου ώστε να επεξεργάζονται τα πακέτα που αναμεταδίδονται μέσα σε αυτό.



Εικόνα 49-IDS

Το IDS χρησιμοποιείται κυρίως σε μεγάλες εγκαταστάσεις δικτύων με μεγάλο αριθμό χρηστών. Χρησιμοποιώντας, το συγκεκριμένο εργαλείο, τα δίκτυα μπορούν να ασφαλίσουν την επικοινωνία ανάμεσα στουςχρήστες τους και να διασφαλίσουν καλύτερη προστασία στην πληροφορία που κινείται μέσα στο δίκτυο.

Πρόκειται για εργαλεία πουμπορούν να εξασφαλίσουν κάποιο καλύτερο επίπεδο ασφάλειας σε ένα δίκτυο, χωρίς να είναι σε θέση να αντικαταστήσει άλλες μεθόδους ασφαλείας. Κρίνεται, λοιπόν, και σε αυτή την περίπτωση, πως τα συστήματα αυτά είναι καλύτερο να χρησιμοποιούνται σε συνδυασμό με τις ήδη υπάρχουσες προστασίες δικτύων.

ΚΕΦΑΛΑΙΟ 7 – ΣΥΜΠΕΡΑΣΜΑΤΑ

Η εργασία, αυτή είχε σαν στόχο να παρουσιάσει τις αδυναμίες ενός ασυρμάτου δικτύου wi-fi και πιο συγκεκριμένα των μεθόδων κρυπτογράφησης που χρησιμοποιούνται για την διασφάλιση της ασφάλειας.

Πέραν της ασφάλειας των δικτύων, γίνεται κατανοητή η ανάγκη για ασύρματη δικτύωση και τα πλεονεκτήματα της. Το σημερινό επίπεδο διάδοσης δικτύων wi-fi, λόγω της ευελιξίας, της γρήγορης υλοποίησης και φυσικά το χαμηλό κόστος χρήσης, συντήρησης και εγκατάστασης έκανε την ασύρματη δικτύωση αρκετά προσιτή και ευρέως διαδεδομένη.

Με την διάδοση της ασύρματης δικτύωσης εμφανίστηκαν πολλές απειλές και σαν αποτέλεσμα να γίνουν εμφανή τα τρωτά σημεία των δικτύων.

Κατά τη διάρκεια της διεκπεραίωσης της εργασίας παρουσιάστηκαν τα μειονεκτήματα της WEP, συγκεκριμένα, κρυπτογράφησης και τρόποι βελτίωσης τους με νέες τεχνολογίες.
Λύσεις που παρουσιάστηκαν ήταν οι TKIP, WPA καιWPA2

Με τις επιθέσεις που έγιναν διαπιστώνονται στην πραγματικότητα οι αδυναμίες ενός ασυρμάτου δικτύου και η ευκολία παραβίασης του.

Το φυσικό μέσο μετάδοσης ενός δικτύου wi-fi είναι ταυτόχρονα πλεονέκτημα και μειονέκτημα. Λόγω της εύκολης πρόσβασης, είναι αρκετά ελκυστικό σε επιθέσεις. Το θέμα της ασφάλειας σε ένα ασύρματο δίκτυο είναι το πιο σημαντικό μειονεκτήματα που μπορεί να οδηγήσει στην μη επιλογή τέτοιου τύπου δικτύωσης.

Η κρυπτογράφηση WEP, αρχικά θεωρήθηκε επαρκής, αλλά με την εξέλιξη της τεχνολογίας και τη διακίνηση αρκετά σημαντικών και προσωπικών πληροφοριών κρίνεται ακατάλληλη.

Στην επίδειξη WEP cracking διαπιστώνεται πλήρως η αδυναμία της, γιατί με μια απλή προσπάθεια συλλογής αρκετών πακέτων IV's ανακτήθηκε το WEP key μέσα σε λίγα λεπτά.
Η WEP κρυπτογράφηση θα μπορούσε να εφαρμοστεί σε περιπτώσεις που η ασφάλεια της πληροφορίας που κινείται στο δίκτυο δεν έχει ιδιαίτερη σημασία.

Λύσεις που προτάθηκαν ήταν οι παραμετροποιήσεις του router-access point και η χρήση νεότερων τεχνολογιών όπως το WPA και το WPA2.

Ωστόσο, ακόμα και αυτές οι μέθοδοι έχουν δεν έχουν αποδειχθεί αρκετά ανασφαλείς καθώς στις αρχές του 2008 παραβιάστηκε και η WPA. Βέβαια, παρέχει τη δυνατότητα της χρήσης του αλγόριθμου AES που θωρακίζει σημαντικά το δίκτυο.

Το μέλλον της ασύρματης ασφάλειας βρίσκεται στις νεότερες εκδόσεις του προτύπουIEEE 802.11, όπως 802.11i και 802.11n.

Το πρότυπο 802.11i, το οποίο εγκρίθηκε για πρώτη φορά την 24η Ιουνίου του 2004, περιλαμβάνει το σύστημα 802.X για επικύρωση, χρήση του EAP – Extensible Authentication Protocol, το RSNγια την ανίχνευση των συσχετίσεων και τη μέθοδο CCMP, η οποία βασίζεται στον αλγόριθμο κρυπτογράφησης AES

Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη πακέτων. Επίσης χρησιμοποιεί μέγεθος κλειδιού 128-bit και μέγεθος μπλοκ 128-bit. Τα δεδομένα του πακέτου και το MIC (Message Integrity Code - ψηφιακή υπογραφή) μεταδίδονται κρυπτογραφημένα, αφού προστεθεί η αρχική επικεφαλίδα

του πακέτου και η επικεφαλίδα του CCMP.

Το πρότυπο ασύρματης δικτύωσης 802.11n εμφανίστηκε το 2009. Οι συσκευές που υποστηρίζουν το πρότυπο 802.11nέχουν ταχύτητες ως 300Mbps. Οι μεγάλες αυτές ταχύτητες οφείλονται στηντεχνολογία MIMO, η οποία κάνει χρήση πολλαπλών κεραιών στο πομπό και το δέκτη, για όσο το δυνατόν μεγαλύτερη ταχύτητα.

Το IEEE802.11n λειτουργεί στην μπάντα των 5GHz, διατηρώντας την συμβατότητα του με δίκτυα τα προηγούμενα πρότυπα (802.11b/g).

Παρότι οι δυνατότητες μετάδοσης είναι υψηλές, έχει ακόμα προβλήματα ασφάλειας .

Βέβαια αξίζει να αναφερθεί πως όσο εξελίσσονται τα επίπεδα ασφάλειας, τόσο εξελίσσονται και οι μηχανισμοί παραβίασης τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

BingB.(2002)Wireless Local Area Networks:The New Wireless Revolution, New York:Wiley publishing.

Στεργίου Ε.(2003)Ασύρματες Επικοινωνίες-Δίκτυα. Άρτα: Τ.Ε.Ι. Ηπείρου, Τμήμα Τηλεπληροφορικής και Διοίκησης

Αξούργος Γ., Τερζόγλου Α.(2008)Πρωτόκολλα Επικοινωνιών Διαδικτύου. Άρτα:Τ.Ε.Ι. Ηπείρου, Τμήμα Τηλεπληροφορικής και Διοίκησης

TanenbaumA. S. (2000)Δίκτυα Υπολογιστών. Αθήνα: Εκδόσεις Παπασωτηρίου

BarkenL. (2003)Hands-OnWireless LANSecurity. U.S.A: Prentice Hallpublishing.

Backtrack Tutorials (2014) Step by Step Guides on using Backtrack-Linux Διαθέσιμοστοδικτυακότόπο: http://backtracktutorials.com/Ανακτήθηκε 26/3/14

Παπαδόπουλος Μ.(2006)Wardriving, Warchalking& Wireless Hacking. Αθήνα

Gurjar C. (2014)Wireless Attacks Unleashed.Διαθέσιμο στο δικτυακό τόπο: http://resources.infosecinstitute.com/wireless-attacks-unleashed/Ανακτήθηκε 11/8/14