ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

Κατεύθυνση: Ψηφιακές Επικοινωνίες & Δίκτυα

ΑΣΦΑΛΕΙΑ ΣΤΑ ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ (WPA/WPA2)

Διπλωματική εργασία

Κεφαλάς Γρηγόριος, Α.Μ. ΜΕ09082

Επιβλέπων: Δρ. Ξενάκης Χρήστος, Επίκουρος Καθηγητής

Πειραιάς, Οκτώβριος 2011

Αφιερώνεται στους γονείς μου

Περίληψη

Σκοπός αυτής της διπλωματικής εργασίας είναι η περιγραφή του τρόπου λειτουργίας, των πρωτοκόλλων κρυπτογράφησης και η παραβίαση της ασφάλειας των ασύρματων δικτύων. Με τη χρήση εξειδικευμένων λειτουργικών και εφαρμογών, θα πραγματοποιηθεί αναζήτηση και η καταγραφή όλων των ενεργών ασύρματων δικτύων σε συνοικίες της πόλης των Αθηνών. Με τη δημιουργία ενός xml parser θα γίνει η επεξεργασία των δεδομένων, θα δημιουργηθεί λεξικό επίθεσης και τέλος θα παραβιαστεί η ασφάλεια σε ένα ασύρματο δίκτυο κρυπτογράφησης WPA/WPA2.

Πιο αναλυτικά, το κεφάλαιο ένα περιγράφει την ανάγκη του ανθρώπου για απομακρυσμένη επικοινωνία, τον ορισμό, την αρχιτεκτονική, τις κατηγορίες που διαχωρίζονται τα ασύρματα δίκτυα και τις διαφορές μεταξύ ασύρματης και ενσύρματης δικτύωσης.

Το κεφάλαιο δύο περιγράφει τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης ασύρματων δικτύων, παρουσιάζονται οι συσκευές που χρησιμοποιούνται και γίνεται η περιγραφή των ασύρματων προτύπων δικτύωσης. Επιπλέον αναλύονται οι εκδόσεις και η αρχιτεκτονική του πρότυπου 802.11.

Στο κεφάλαιο τρία γίνεται αναφορά στα είδη των αλγορίθμων κρυπτογράφησης, περιγράφονται και συγκρίνονται αναλυτικά τα πρωτόκολλα κρυπτογράφησης WEP και WPA/WPA2 και αναλύονται τα δύο είδη επιθέσεων.

Το τέταρτο κεφάλαιο περιγράφει την παραβίαση της ασύρματης ασφάλειας. Παρουσιάζονται αναλυτικά τα εργαλεία που χρησιμοποιήθηκαν για την αναζήτηση, την καταγραφή και την παραβίαση των ασύρματων δικτύων. Από την ανάλυση του xml αρχείου παρουσιάζονται ποσοτικές πληροφορίες σχετικά με τις κρυπτογραφικές μεθόδους και τα κανάλια εκπομπής που χρησιμοποιούνται. Επιπλέον εντοπίζεται βάση των στατιστικών η πλέον κοινή ονομασία ασύρματου δικτύου, και οι κρυπτογραφικές μέθοδοι που χρησιμοποιούνται. Τέλος γίνεται σύγκριση των αποτελεσμάτων των επιθέσεων και αναλύονται λεπτομερώς τα αποτελέσματά τους.

Abstract

The purpose of this thesis is to describe the way wireless networks work, as well as their encryption protocols and security violation. More precisely, all active wireless networks within regions of Athens will be searched for and registered through the use of specific functions and applications. By creating an xml parser data will be processed, a dictionary attack will be created and finally the security of an encrypted WPA/WPA2 wireless network will be violated.

More specifically, chapter one describes the human need for remote communication, the definition, the architecture, the categories that wireless networks are divided into and the differences between wireless and wired networking.

Chapter two describes the advantages and disadvantages in using wireless networks, analyzes wireless devices being used and describes wireless networking standards. Moreover, it gives the analysis of publications and architecture of the standard 802.11.

Chapter three refers to the types of encryption algorithms, describes and compares in detail the encryption protocols WEP and WPA/WPA2 and analyzes two types of attacks.

Chapter four describes the violation of wireless security. It presents in detail the tools used for searching, registrating and violating wireless networks. The analysis of the xml file presents statistical information about cryptographic methods and the channels in use. Additionally, based on the statistics, the most common wireless network ssid and cryptographic methods primarily used are found. Finally, the effects of the attacks will be compared and the results will be analyzed in detail.

Ευχαριστίες

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Διδακτική της Τεχνολογίας & Ψηφιακά Συστήματα» στην κατεύθυνση «Ψηφιακές Επικοινωνίες και Δίκτυα» του τμήματος Ψηφιακών Συστημάτων.

Κατ΄αρχάς θα ήθελα να εκφράσω τις θερμές ευχαριστίες μου στους καθηγητές μου και πιο συγκεκριμένα στον Επίκουρο Καθηγητή κ. Χρήστο Ξενάκη για την εμπιστοσύνη που μου έδειξε προκειμένου να αναλάβω την παρούσα διπλωματική εργασία που αποτελεί ένα από τα κεφάλαια που με ενδιαφέρουν. Τον διδάκτορα Χριστόφορο Νταντογιάν για την καθοδήγηση και την επίβλεψη που μου παρείχε για την ολοκλήρωση της διπλωματικής εργασίας.

Τέλος εκφράζω την ευγνωμοσύνη μου στους γονείς μου για την υποστήριξη και βοήθειά τους σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

AP: (Access Point), μια συσκευή ενός Wi-Fi δικτύου η οποία συνδέει πελάτες του δικτύου αυτού μεταξύ τους και με ενσύρματα δίκτυα.

Ad hoc: Η λειτουργία κατά την οποία ένας υπολογιστής μπορεί να συνδεθεί με έναν άλλο απευθείας σχηματίζοντας δίκτυο, χωρίς την παρεμβολή ενός AP.

ARP: (Address Resolution Protocol), πρωτόκολλο μετάφρασης διευθύνσεων ip σε διευθύνσεις mac.

Authentication: Η διαδικασίας πιστοποίησης της ταυτότητας ενός σταθμού.

Authenticator: Η συσκευή η οποία δρομολογεί τη σύνδεση ενός σταθμού με έναν άλλο ή με ένα δίκτυο (συνήθως είναι ένα AP).

Beacon: Το σήμα που στέλνει ένα AP για να ανακοινώσει την ύπαρξή του και μπορεί να περιλαμβάνει διάφορα στοιχεία πχ essid, mac address.

BSSID: (Basic Service Set Identifier), διεύθυνση mac του access point.

CCMP: (Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol), πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο WPA2, βασισμένο στον AES block cipher.

Dictionary: ένα σύνολο λέξεων που θα χρησιμοποιηθεί σε μια επίθεση.

EAP: (Extensible Authentication Protocol), βασικό πρωτόκολλο στο οποίο πατάνε διάφορες μέθοδοι authentication.

EAPOL: (EAP Over LAN), εφαρμογή του πρωτοκόλλου EAP στα δίκτυα.

ESSID: (Extended Service Set Identifier), το όνομα του δικτύου.

Fragmentation: η διαδικασία κατά την οποία ένα πακέτο πληροφορίας σπάει σε μικρότερα πακέτα για να αποσταλεί και τα οποία θα χρειαστεί να «επανακολληθούν» στον προορισμό τους.

Frame: μπορούμε να θεωρήσουμε πως frame είναι το ίδιο με ένα packet. Ο «ορισμός» είναι πως όταν υπάρχει ανταλλαγή μηνυμάτων στο layer 2 του OSI model αναφερόμαστε σε frames, ενώ όταν η ανταλλαγή γίνεται στο 3 layer για packets.

Handshake: διαδικασία μιας σειράς ερωτήσεων-απαντήσεων με σκοπό την πιστοποίηση του supplicant.

ICV: (Integrity Check Value), data field που προσαρτάται στην plaintext για έλεγχο της ακεραιότητάς της (βασισμένο στον αδύναμο CRC32 αλγόριθμο).

Infrastructure: Ο τρόπος λειτουργίας κατά τον οποίο ένας υπολογιστής συνδέεται πρώτα με ένα AP και μετά με το δίκτυο.

IV: (Initialization Vector), δεδομένα που συνδυάζονται με το encryption key ώστε να παραχθεί μια μοναδική keystream.

KCK: (Key Confirmation Key), κλειδί ελέγχου ακεραιότητας που προστατεύει τα μηνύματα handshake.

KEK: (Key Encryption Key), «εμπιστευτικό» κλειδί που προστατεύει τα handshake μηνύματα.

MAC Address: (Media Access Control Address), ένας 48-bit αριθμός που δίνεται σε κάθε κάρτα δικτύου από τον κατασκευαστή της.

MIC: (Message Integrity Code), data field που προσαρτάται στην plaintext για έλεγχο της ακεραιότητάς της (παράγεται από τον αλγόριθμο Michael).

MK: (Master Key), το κύριο κλειδί που γνωρίζει ο supplicant και ο authenticator μετά τη διαδικασία authentication του 802.1x.

Monitor Mode: Η κατάσταση λειτουργίας μιας Wi-Fi συσκευής κατά την οποία λαμβάνει τα πακέτα που κυκλοφορούν στο Wi-Fi δίκτυο. Είναι γνωστή και ως raw mode.

MPDU: (Mac Protocol Data Unit), πακέτο δεδομένων πριν το fragmentation.

MSDU: (Mac Service Data Unit), πακέτο δεδομένων μετά το fragmentation.

NACK: (Negative Acknowledgement), σε πολλά πρωτόκολλα δικτύου, σε περίπτωση μη παραλαβής ενός εκ των πακέτων δεδομένων ο δέκτης εκπέμπει ένα NACK, αναγκάζοντας τον αποστολέα να αποστείλει είτε το πακέτο είτε ολόκληρη τη σειρά των πακέτων που ανήκε το απολεσθέν.

Packet: Η ελάχιστη μονάδα συμπύκνωσης των δεδομένων κατά τη διάρκεια οποιασδήποτε μεταφοράς και επικοινωνίας μεταξύ δύο υπολογιστών. Σε κάθε είδος δικτύου, υπάρχει συνεχής ροή "πακέτων" από και προς κάθε σταθμό του δικτύου.

PMK: (Pairwise Master Key), κύριο κλειδί στην ιεραρχία pairwise key.

PRGA: (Pseudo Random Generation Algorithm) η διαδικασία παραγωγής της keystream στον RC4.

PSK: (Pre-Shared Key), κλειδί που παράγεται από έναν κωδικό (passphrase) αντικαθιστώντας το PMK σεWPA-PSK mode.

PTK: (Pairwise Transient Key), κλειδί που παράγεται από το PMK.

Rainbow Tables: έτοιμα hashes λέξεων για χρήση σε brute force ή dictionary attacks.

SSID: (Service Set Identifier), wireless network identifier (όχι το ίδιο με το ESSID).

TK: (Temporary Key), κλειδί για κρυπτογράφηση δεδομένων σε unicast traffic (χρησιμοποιείται και για έλεγχο ακεραιότητας -integrity checking- στο CCMP).

TKIP: (Temporal Key Integrity Protocol), πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο WPA και βασίζεται στον RC4 αλγόριθμο (ο οποίος χρησιμοποιείται και στο WEP).

TMK: (Temporary MIC Key), κλειδί για data integrity σε unicast traffic (TKIP).

WEP: (Wired Equivalent Privacy), default πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στα 802.11 δίκτυα.

Wi-Fi: (Wireless Fidelity), η γνωστή σε όλους μας τεχνολογία ασύρματης δικτύωσης.

WPA: (Wireless Protected Access), εφαρμογή μιας πρώιμης έκδοσης του 802.11i στάνταρ, βασισμένη στο TKIP.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Γενικά

Ο άνθρωπος χρησιμοποιεί πολλούς αιώνες την επικοινωνία ως μέσο για ανταλλαγή πληροφοριών. Ωστόσο μόλις τον $20^{ο}$ αιώνα κατάφερε να εξασφαλίσει την απομακρυσμένη επικοινωνία και τη μετάδοση της πληροφορίας μέσω του τηλεφωνικού, του τηλεοπτικού, του ραδιοφωνικού σήματος, καθώς και των υπολογιστικών δικτύων, τα οποία δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Οι ηλεκτρονικοί υπολογιστές κατασκευάστηκαν για να επεξεργάζονται και να διαχειρίζονται την πληροφορία. Αργότερα προέκυψε η ανάγκη διακίνησης της πληροφορίας σε μεγάλες αποστάσεις με αποτέλεσμα να δημιουργηθούν τα δίκτυα υπολογιστών που διαχειρίζονταν και επεξεργάζονταν τις πληροφορίες μεταξύ τους.

1.2 Τι είναι δίκτυο υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο ή περισσότερους αυτόνομους και ανεξάρτητους υπολογιστές και περιφερειακές συσκευές. Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες.

Η αρχιτεκτονική των δικτύων καθορίζει τον τρόπο με τον οποίο οι υπολογιστές και οι λοιπές συσκευές συνδέονται μεταξύ τους για να σχηματίσουν ένα σύστημα επικοινωνίας που θα επιτρέπει στους χρήστες να διαμοιράζονται πληροφορίες και συσκευές του δικτύου. Σε ένα δίκτυο δεδομένων περιλαμβάνονται:

- Τερματικοί Κόμβοι: Ελέγχουν τους πόρους του δικτύου (λογισμικό και υλικό).

- Υποδίκτυα: Φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τοπολογία, τερματικοί κόμβοι, πόροι που μπορούν να διαφέρουν πολύ ανά υποδίκτυο.
- Συσκευές διασύνδεσης: Συνδέουν τα ετερογενή υποδίκτυα έτσι ώστε να εξασφαλίζεται η επικοινωνία τερματικών κόμβων που βρίσκονται σε διαφορετικά υποδίκτυα.

Τα δίκτυα διακρίνονται στις ακόλουθες κατηγορίες:

- Με βάση το φυσικό μέσο διασύνδεσής τους διακρίνονται σε ενσύρματα ή ασύρματα.
- Με βάση τον τηλεπικοινωνιακό φορέα εξυπηρέτησης διακρίνονται σε ιδιωτικά ή δημόσια δίκτυα.
- Με βάση την γεωγραφική ανάπτυξη διακρίνονται σε δίκτυα ευρείας περιοχής (WAN), δίκτυα μικρών αποστάσεων ή τοπικά δίκτυα (LAN), αστικά Δίκτυα (MAN) και προσωπικά (PAN).
- Με βάση την τεχνική προώθησης της πληροφορίας διακρίνονται σε δίκτυα μεταγωγής και δίκτυα ακρόασης.

Η διαφορά μεταξύ της ενσύρματης και της ασύρματης μετάδοσης εντοπίζεται στο φυσικό μέσο μετάδοσης της πληροφορίας. Τα ασύρματα δίκτυα δεν χρησιμοποιούν ως μέσο μετάδοσης κάποιον τύπο καλωδίου για τη μεταφορά των δεδομένων, αλλά ηλεκτρομαγνητικά κύματα, με συχνότητα συνήθως 2,4 και 5 GHz. Για την ομαλή επικοινωνία μεταξύ των ασύρματων και ενσύρματων δικτύων, απαιτείται η χρήση συγκεκριμένων προτύπων.

Οι ασύρματες επικοινωνίες αποτελούν τον ταχύτερα αναπτυσσόμενο τομέα των τηλεπικοινωνιών τα τελευταία χρόνια. Τα ασύρματα δίκτυα δεδομένων, όπως η κινητή τηλεφωνία και οι δορυφορικές επικοινωνίες είναι χαρακτηριστικές ασύρματες εφαρμογές με υψηλό ρυθμό εξάπλωσης παγκοσμίως και αποτελούν βασικό εργαλείο ανάπτυξης των προηγμένων χωρών, ενώ δημιουργούν τις προϋποθέσεις τηλεπικοινωνιακής ενδυνάμωσης και αναβάθμισης των λιγότερο αναπτυγμένων χωρών.

Η αποδοχή του κόσμου, οι λύσεις των κατασκευαστών και τα βιομηχανικά πρότυπα, είναι σημαντικοί λόγοι για την αποδοχή της ασύρματης δικτύωση.

Είναι όμως ασφαλής αυτή η τεχνολογία;

ΚΕΦΑΛΑΙΟ 2

Ασύρματα δίκτυα

2.1 Τι είναι το Wi-Fi

Με την ανάπτυξη των προτύπων από την IEEE (Institute of Electrical and Electronics Engineers - μη κερδοσκοπικού χαρακτήρα οργανισμός) και την εμφάνιση μεγάλου αριθμού κατασκευαστών ασύρματων συσκευών, φάνηκε από νωρίς η ανάγκη διασφάλισης της συμβατότητας μεταξύ των διαφόρων συσκευών και προστασίας του αγοραστή.

Για το σκοπό αυτό ιδρύθηκε το 1999 η WECA (Wireless Ethernet Compatibility Alliance). Πρόκειται για έναν μη κερδοσκοπικό οργανισμό που σκοπό έχει τη πιστοποίηση ασύρματων συσκευών με βάση το πρότυπο 802.11. Σ' αυτόν τον οργανισμό μετέχουν κατασκευαστές ολοκληρωμένων κυκλωμάτων, παροχείς υπηρεσιών WLAN, κατασκευαστές υπολογιστών και κατασκευαστές λογισμικού. Μερικές από τις εταιρίες που μετέχουν είναι οι 3Com, Aironet, Apple, Breezecom, Cabletron, Compaq, Dell, Fujitsu, IBM, Intersil, Lucent Technologies, No Wires Needed, Nokia, Samsung, Symbol Technologies, Wayport, Zoom, κ.α.

Η ένωση αυτή δημιούργησε μία ακολουθία από δοκιμές προκειμένου να ελεγχθεί η συμβατότητα των IEEE προϊόντων. Οι συσκευές οι οποίες περνούσαν με επιτυχία τις δοκιμές αυτές, αποκτούσαν το λογότυπο Wi-Fi (Wireless Fidelity). Το λογότυπο αυτό αποτελεί κατά συνέπεια μία πιστοποίηση για τον υποψήφιο αγοραστή μιας συσκευής και μία εγγύηση για την επένδυση του. Ο καταναλωτής αγοράζοντας μία συσκευή με το λογότυπο αυτό, έχει την εγγύηση ότι η συσκευή θα συνεργαστεί με οποιαδήποτε άλλη συσκευή φέρει επίσης το ίδιο λογότυπο.

Εικόνα 1: Το λογότυπο Wi-Fi

2.2 Περιγραφή ασύρματων δικτύων

Ασύρματο δίκτυο είναι ένα σύστημα επικοινωνίας μέσω ηλεκτρομαγνητικών κυμάτων ανάμεσα σε σταθερούς ή κινητούς χρήστες επιτρέποντας την μεταξύ τους διασύνδεση και ανταλλαγή δεδομένων.

Μόλις τα τελευταία χρόνια, τα ασύρματα δίκτυα, άρχισαν να καταλαμβάνουν ένα σημαντικό τμήμα της αγοράς δικτύων. Ολοένα και περισσότερο, οι οργανισμοί και οι επιχειρήσεις διαπιστώνουν ότι τα ασύρματα τοπικά δίκτυα αποτελούν απαραίτητο συμπλήρωμα των παραδοσιακών ενσύρματων δικτύων, για την ικανοποίηση των απαιτήσεων της φορητότητας, της μετεγκατάστασης, της ad hoc δικτύωσης και της κάλυψης τοποθεσιών για τις οποίες είναι δύσκολη η εγκατάσταση καλωδίων.

Στα αρχικά στάδια της τεχνολογίας του, το ασύρματο δίκτυο λόγω των αρκετών μειονεκτημάτων και της έλλειψης προτύπων δεν ήταν ιδιαίτερα διαδεδομένο. Με την τεχνολογική εξέλιξη τα σύγχρονα ασύρματα δίκτυα είναι ιδιαίτερα διαδεδομένα αφού έχουν πλέον χαμηλό κόστος και ποιότητα υπηρεσιών παρόμοια με τα ενσύρματα δίκτυα.

2.2.1 Πλεονεκτήματα ασύρματων δικτύων

Η χρήση της ασύρματης μετάδοσης έχει μία σειρά από πλεονεκτήματα:

- Κινητικότητα χρήστη: Οι χρήστες μπορούν να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου, δηλαδή σε χώρο που θα έχουν επαρκές σήμα, διατηρώντας την συνδεσιμότητα τους.

- Ευκολία, ευελιξία και απλότητα εγκατάστασης: Μπορεί να γίνει η δικτύωση σε μέρη όπου η καλωδίωση θα ήταν αδύνατη ή μη επιθυμητή.
- Κλιμάκωση, δυνατότητα επέκτασης: Τα ασύρματα δίκτυα μπορούν να διαρθρωθούν σε ένα πλήθος από τοπολογίες, ώστε να ταιριάξουν στις απαιτήσεις των εφαρμογών. Οι τοπολογίες αλλάζουν εύκολα και επεκτείνονται από απλά δίκτυα με μικρό αριθμό χρηστών, έως μεγάλες δομές δικτύων με εκατοντάδες χρήστες.
- Κόστος: Παρόλο που το αρχικό κόστος εγκατάστασης είναι υψηλότερο σε σχέση με λύσεις της ενσύρματης δικτύωσης, το τελικό όμως κόστος για όλη τη διάρκεια ζωής της επένδυσης μπορεί να είναι μικρότερο, ιδιαίτερα σε δυναμικό περιβάλλον που απαιτεί συχνές αλλαγές, αναδιαρθρώσεις και μετακινήσεις. Με την εμφάνιση περισσότερων κατασκευαστών και τον έντονο ανταγωνισμό μεταξύ τους το κόστος έχει πέσει αισθητά, ενώ παράλληλα οι συσκευές έχουν αποκτήσει περισσότερα ποιοτικά χαρακτηριστικά.
- Ταχύτητες μετάδοσης: Όσο αναπτύσσεται η τεχνολογία γίνεται δυνατή η μετάδοση μεγαλύτερων ρυθμών δεδομένων. Ήδη ο μέγιστος ρυθμός μετάδοσης δεδομένων, από τα 2 Mbps που μπορούσαν να επιτευχθούν αρχικά, έφτασε σήμερα σε ταχύτητες πάνω από 400 Mbps ενώ ήδη έχουν εξαγγελθεί ακόμα μεγαλύτερες ταχύτητες.
- Αξιοπιστία-ανεξαρτησία: Ένα ασύρματο δίκτυο κατάλληλα διαμορφωμένο μπορεί να έχει μεγάλη αξιοπιστία. Μπορεί να σχεδιαστεί ώστε να λειτουργεί όταν συμβαίνουν διακοπές ρεύματος και να περιλαμβάνει πολλές εναλλακτικές διαδρομές.
- Εμβέλεια: Η εμβέλεια ενός ασύρματου δικτύου μπορεί να είναι μερικές δεκάδες μέτρα σε κλειστό χώρο, ενώ σε ανοιχτό χώρο οι αποστάσεις που μπορεί να καλυφθούν είναι μεγαλύτερες.
- Συμβατότητα με το υπάρχον δίκτυο: Τα περισσότερα ασύρματα δίκτυα συνδέονται με τα ενσύρματα δίκτυα βάσει προτύπων. Έτσι, η προσθήκη ασύρματης δικτύωσης σε υπάρχουσες δομές δικτύων μπορεί να γίνει με ευκολότερο τρόπο. Πολλές φορές δε, αποτελούν επέκταση ενός ενσύρματου δικτύου.

2.2.2 Μειονεκτήματα ασύρματων δικτύων

Η χρήση των ασύρματων δικτύων για την μεταφορά πληροφορίας τα κάνουν ευπρόσβλητα σε πολλά φαινόμενα παρεμβολών, τα οποία αλλοιώνουν την επικοινωνία των χρηστών. Τα μειονεκτήματα των ασύρματων δικτύων μπορούν να συνοψιστούν ως εξής:

- Ασφάλεια: Είναι γνωστό ότι τα δίκτυα υστερούν στον τομέα της ασφάλειας, καθώς υπάρχουν πολλοί τρόποι επίθεσης από επίδοξους εισβολείς. Επιθέσεις παρεμπόδισης των επικοινωνιών (jamming) και καταγραφής δεδομένων που κινούνται στο δίκτυο (sniffing), είναι ιδιαίτερα διαδεδομένες.
- Παρεμβολές: Τα ασύρματα τοπικά δίκτυα, κυρίως όσα βρίσκονται σε ζώνες χαμηλής συχνότητας, είναι ευάλωτα στις παρεμβολές. Μπορεί να δεχτούν και να προκαλέσουν παρεμβολές σε άλλα 2.4 GHz προϊόντα, όπως τα ασύρματα τηλέφωνα ή να δεχθούν παρεμβολές από αρμονικές συχνότητες από συσκευές που εκπέμπουν σε υποπολλαπλάσια της συχνότητας λειτουργίας. Όμως το σημαντικότερο πρόβλημα παρεμβολών προκύπτει από την κακή σχεδίαση ενός ασύρματου δικτύου, όπως μεγαλύτερη ισχύς εκπομπής από το αναγκαίο, ακατάλληλες κεραίες, συσκευές με μικρή ευαισθησία, λάθος επιλογή συχνότητας και τοποθεσίας.
- Προστασία της υγείας των χρηστών: Ο εξοπλισμός που χρησιμοποιείται πρέπει να είναι απολύτως συμβατός με τις διεθνείς και ευρωπαϊκές οδηγίες και να είναι αποδεκτός από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI).

2.3 Ποιοι χρειάζονται ασύρματη πρόσβαση

Οι εφαρμογές ενός ασύρματου δικτύου είναι πολλές και περιορίζονται μόνο από την φαντασία του χρήστη. Τα τελευταία χρόνια χρησιμοποιούνται σε εφαρμογές, συμπεριλαμβανομένων αυτών της υγείας, της παιδείας, των ακαδημαϊκών ιδρυμάτων, καθώς και της επαγγελματικής και οικιακής χρήσης. Στη συνέχεια

παρατίθενται ορισμένες εφαρμογές των ασύρματων δικτύων, οπού φαίνεται τόσο η ευελιξία όσο και η ισχύς που προσφέρουν:

- Με ένα ασύρματο δίκτυο είναι πολύ εύκολο να γίνει κοινή χρήση της σύνδεσης στο διαδίκτυο από όλες τις Wi-Fi συσκευές.
- Αν μία επιχείρηση καταλαμβάνει περισσότερα του ενός κτίρια, είναι θεμιτή η επικοινωνία μεταξύ των δικτύων τους. Η χρήση ασύρματης ζεύξης είναι η πιο απλή και οικονομική λύση, με μόνο μειονέκτημα την ενδεχόμενη παραβίαση της ασφάλειας.
- Σε αίθουσες συνεδρίων (meeting rooms) για πρόσβαση στις πληροφορίες του εταιρικού δικτύου.
- Hot spots: Εκτός του εσωτερικού δικτύου, μία εταιρεία μπορεί να επεκτείνει την πελατεία της, κατά συνέπεια τα κέρδη της, προσφέροντας διάφορες υπηρεσίες σε επιλεγμένα σημεία των εγκαταστάσεών της. Ήδη τέτοια σημεία εντοπίζονται σε εστιατόρια, καφέ, ξενοδοχεία, αεροδρόμια, νοσοκομεία, σιδηροδρομικούς σταθμούς, κ.α.
- Γιατροί και νοσηλευτικό προσωπικό χρησιμοποιούν ασύρματες φορητές συσκευές για να έχουν άμεση πρόσβαση στα προσωπικά αρχεία των ασθενών και σε ιατρικές βιβλιοθήκες.
- Υλοποίηση δικτύων σε παλιά ή διατηρητέα κτίρια, όπου η καλωδίωση είναι ασύμφορη ή απαγορευτική.
- Υλοποίηση ασύρματων δικτύων ως backup συστημάτων των ενσύρματων εγκαταστάσεων.

2.4 Δομικά στοιχεία

Συσκευές χρηστών (End users devices): Οι συσκευές αποτελούν την πηγή επικοινωνίας μεταξύ του χρήστη και του δικτύου. Η επικοινωνία σε ένα ασύρματο δίκτυο γίνεται μέσω συσκευών που υποστηρίζουν την ασύρματη μετάδοση. Τέτοιες συσκευές είναι οι παρακάτω:

- Σταθεροί/φορητοί υπολογιστές
- Υπολογιστές παλάμης, χειρός και εκτυπωτές (palmtop, handheld PCs and printers)

- Smartphones
- IP κάμερες

Κάρτες δικτύου: Η κάρτα δικτύου επιτρέπει την επικοινωνία μεταξύ των υπολογιστών μέσω του δικτύου. Αποτελεί συσκευή του φυσικού επιπέδου και του επιπέδου ζεύξης δεδομένων του προτύπου OSI, αφού παρέχει πρόσβαση στο φυσικό μέσο δικτύωσης αλλά και ένα σύστημα διευθυνσιοδότησης χαμηλού επιπέδου μέσω της χρήσης των διευθύνσεων MAC.

Σημεία πρόσβασης (access points): Στα δίκτυα υπολογιστών καλούμε ασύρματο σημείο πρόσβασης ή σταθμό βάσης (access point) μια συσκευή που συνδέει μεταξύ τους ασύρματες συσκευές επικοινωνίας για τον σχηματισμό ενός ασύρματου δικτύου. Ο σταθμός βάσης συνήθως συνδέεται με ένα ενσύρματο δίκτυο και μπορεί να μεταφέρει δεδομένα ανάμεσα στις ασύρματες και τις ενσύρματες συσκευές. Πολλοί σταθμοί βάσης μπορούν να συνδεθούν μεταξύ τους για να σχηματίσουν ένα μεγαλύτερο δίκτυο που επιτρέπει περιαγωγή. Αντίθετα με το μοντέλο αυτό, ένα δίκτυο στο οποίο συσκευές-πελάτες επικοινωνούν από μόνες τους, χωρίς να χρειάζονται κάποιο σημείο πρόσβασης που πρέπει να γνωρίζουν εκ των προτέρων, λέγεται ad hoc δίκτυο.

Μέσο μετάδοσης: Οι τεχνολογίες ασύρματης δικτύωσης χρησιμοποιούν ραδιοσυχνότητες που έχουν δοθεί για βιομηχανικούς, επιστημονικούς και ιατρικούς σκοπούς. Αντιθέτως με όλα τα άλλα μέρη του ραδιοφωνικού φάσματος, η χρήση πομπού σε αυτές τις συχνότητες δεν χρειάζεται άδεια. Το πρότυπο IEEE 802.11 ορίζει 13 κανάλια μέσα στη συχνότητα των 2.4 GHz. Το ασύρματο τοπικό δίκτυο εκπέμπει σε αυτά τα κανάλια με τρόπο ώστε να μειώνει τις παρεμβολές και να αυξάνει την ακεραιότητα των δεδομένων.

Κεραίες (Antennas): Η κεραία είναι μια διάταξη με αγωγούς που επιτρέπει την αποτελεσματική εκπομπή και λήψη ραδιοκυμάτων, βάση του φαινομένου της ηλεκτρομαγνητικής επαγωγής. Όταν λειτουργεί ως δέκτης λαμβάνει ραδιοκύματα και τα μετατρέπει σε εναλλασσόμενο ρεύμα, και όταν λειτουργεί ως πομπός λαμβάνει εναλλασσόμενο ρεύμα και το μετατρέπει αντίστοιχα σε ραδιοκύματα. Υπάρχουν δύο ειδών κεραιών όσον αφορά τον τρόπο εκπομπής, οι

πολυκατευθυντικές (omnidirectional) και οι κατευθυντικές (directional). Στις κατευθυντικές κεραίες το χαρακτηριστικό διάγραμμα ακτινοβολίας τους είναι έντονα ενισχυμένο προς μια κατεύθυνση και υποβαθμισμένο ή ανύπαρκτο προς άλλες κατευθύνσεις. Αντίθετα οι πολυκατευθυντικές κεραίες εκπέμπουν προς όλες τις κατευθύνσεις στο οριζόντιο διάγραμμα ακτινοβολίας και με μεγάλο εύρος δέσμης στο κάθετο διάγραμμα ακτινοβολίας και για αυτό το λόγο περιορίζονται για συνδέσεις μικρών σχετικά αποστάσεων.

2.5 Ασύρματα πρότυπα δικτύωσης

Με την συνεχή τεχνολογική εξέλιξη έχουν αναπτυχθεί διάφορα ασύρματα πρότυπα. Τα πιο διαδεδομένα είναι: IEEE 802.11, IEEE 802.16, HiperLan, Openair, HomeRF, Bluetooth.

Κάθε ένα πρότυπο έχει διαφορετική εφαρμογή, άρα μπορούμε να πούμε ότι είναι συμπληρωματικά μεταξύ τους παρά ανταγωνιστικά. Το Bluetooth και το HomeRF είναι σχεδιασμένα για ζεύξεις μικρών αποστάσεων, για την σύνδεση μεταξύ συσκευών και των περιφερειακών τους, το IEEE 802.11 για την υλοποίηση ασύρματων τοπικών δικτύων, ενώ το IEEE 802.16 για την υλοποίηση ευρύτερων ασύρματων μητροπολιτικών δικτύων.

IEEE 802.11: Το 1997, μετά από επτά χρόνια μελέτης, δημοσιεύτηκε το πρώτο πρότυπο για ασύρματη δικτύωση. Η μετάδοση γίνεται ασύρματα με χρήση διαμόρφωσης FHSS ή DSSS. Το πρότυπο αυτό προβλέπει ρυθμούς μετάδοσης 1-2 Mbps. Υποστηρίζει δυνατότητες όπως προτεραιότητα εκπομπής, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής. Το πρότυπο γνώρισε περιορισμένη επιτυχία λόγω των πολύ χαμηλών ρυθμών μετάδοσης.

Το 802.11 υποστηρίζει δύο τρόπους λειτουργίας:

- Όταν δεν υπάρχει κάποιος κεντρικός σταθμός βάσης, οι κόμβοι είναι ισότιμοι και η πρόσβαση ρυθμίζεται από τα πρωτόκολλα επικοινωνίας.
- Η ύπαρξη ενός κεντρικού κόμβου τοπικού δικτύου, ο οποίος αναλαμβάνει τον έλεγχο πρόσβασης στο ασύρματο κανάλι.

Από την αρχική του έκδοση, το πρότυπο έχει επεκταθεί σε πολυάριθμες εκδόσεις, που καθορίζονται από το γράμμα a μέχρι το u.

IEEE 802.16: Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16, γνωστό και ως WiMax. Αναπτύχθηκε για να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση ευρείας ζώνης και υψηλών ταχυτήτων σε μεγάλη απόσταση. Αντίθετα με άλλα ασύρματα δίκτυα τα οποία επιτρέπουν μεταδόσεις μόνο με ένα φάσμα συχνότητας, το WiMax επιτρέπει τη μεταφορά δεδομένων κάνοντας χρήση πολλαπλών συχνοτήτων. Λειτουργεί στο συχνοτικό φάσμα των 10 - 66 GHz και έχει ρυθμό μετάδοσης δεδομένων 120 Mbps.

HiperLan: Το HiperLan είναι και αυτό ένα πρότυπο για ασύρματη δικτύωση στη ζώνη συχνοτήτων 5,1 - 5,3 GHz και εγκρίθηκε το 1996 από την ETSI (European Telecommunications Standards Institute). Υπάρχουν οι ακόλουθες τέσσερις εκδόσεις: HiperLan/1, HiperLan/2, HiperAccess και HiperLink. Ο στόχος της πρώτης έκδοσης ήταν η επίτευξη υψηλού ρυθμού μετάδοσης σε σχέση με του 802.11. Η επόμενη έκδοση του ήταν το HiperLan/2, η οποία εγκρίθηκε το 2000 και σχεδιάστηκε ως μία γρήγορη ασύρματη σύνδεση για πολλά δίκτυα, όπως Ip, ATM, UMTS.

Openair: Η Proxim είναι μία από τις μεγαλύτερες κατασκευαστικές εταιρείες ασύρματων δικτύων η οποία δημιούργησε το πρωτόκολλο Openair. Χρησιμοποιεί Frequency Hopping με ρυθμό μετάδοσης 0,8 και 1,6 Mbps και με τεχνικές διαμόρφωσης 2 και 4 FSK. Το πρωτόκολλο που χρησιμοποιείται είναι CSMA/CA και βασίζεται στην ανταλλαγή RTS/CTS πακέτων.

HomeRF SWAP: Το πρότυπο SWAP σχεδιάστηκε για να συνδέει τις ασύρματες συσκευές οικιακής χρήσης. Αναπτύχθηκε το 1998 από το HomeRF Working Group, μία κοινοπραξία των μεγαλύτερων εταιριών κινητής και ασύρματης τεχνολογίας. Το πρότυπο SWAP έχει συχνότητα λειτουργίας στα 2,4 GHz, χρησιμοποιεί την τεχνική FHSS, με ρυθμούς μετάδοσης 1 και 2 Mbps.

Bluetooth: Είναι ένα πρωτόκολλο το οποίο βρίσκει εφαρμογή στα ασύρματα προσωπικά δίκτυα υπολογιστών (WPAN). Ιδρύθηκε από το Bluetooth Special Interest Group, μία κοινοπραξία μεγάλων εταιριών όπως είναι η Ericsson, η IBM,

η Intel, κ.α. Χρησιμοποιεί την τεχνική FHSS, με συχνότητα λειτουργίας τα 2,4 GHz, με εμβέλεια που φτάνει τα 200 m και με ρυθμό μετάδοσης δεδομένων που φτάνει τα 3 Mbps.

2.6 Το πρότυπο 802.11

Η μελέτη για τα ασύρματα δίκτυα του προτύπου 802.11 άρχισε το 1987 από την ομάδα εργασίας IEEE 802.4. Στόχος της ομάδας ήταν η ανάπτυξη ενός ασύρματου δικτύου το οποίο θα βασίζονταν σε ένα πρωτόκολλο MAC ισοδύναμο με αυτό του διαύλου «token bus». Όμως μετά από έρευνες αποφασίστηκε ότι ο δίαυλος «token bus» δεν ήταν κατάλληλος για τον έλεγχο ενός ραδιομέσου χωρίς την αναπόφευκτη ανεπαρκή χρήση του φάσματος ραδιοσυχνοτήτων. Έτσι το 1990 η επιτροπή του IEEE 802 αποφάσισε να σχηματίσει μία νέα ομάδα εργασίας, την IEEE 802.11, αφιερωμένη ειδικά στα ασύρματα δίκτυα με σκοπό την ανάπτυξη ενός πρωτοκόλλου MAC και τον σχεδιασμό προδιαγραφών για το φυσικό μέσο.

2.7 Οι εκδόσεις του 802.11

Η πρώτη έκδοση του Wi-Fi ονομάζεται 802.11, ανακοινώθηκε το 1997 και στο φυσικό επίπεδο περιελάμβανε δύο μεθόδους διασποράς φάσματος για τη μετάδοση στη ζώνη συχνοτήτων 2,4 GHz. Η πρώτη μέθοδος λειτουργούσε με Frequency Hopping (FHSS) και υποστήριζε ρυθμό μετάδοσης 1 Mbps, ενώ η δεύτερη λειτουργούσε με Direct Sequence (DSSS) και υποστήριζε ρυθμό μετάδοσης 1-2 Mbps. Από την αρχική του έκδοση, το πρότυπο έχει υλοποιηθεί σε διάφορες εκδόσεις, που καθορίζονται από το γράμμα a έως το u.

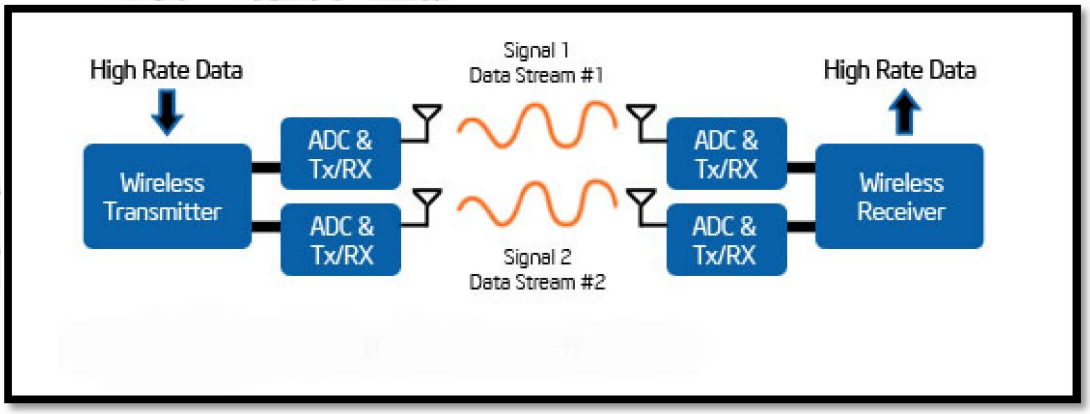
802.11b: Το 1999 ανακοινώθηκε το νέο πρότυπο το 802.11b, που είναι ο αντικαταστάτης του αρχικού 802.11 και υποστηρίζει ρυθμούς μετάδοσης δεδομένων έως 11 Mbps χρησιμοποιώντας τη μέθοδο διασποράς φάσματος (DSSS) για τη μετάδοση στη ζώνη συχνοτήτων 2,4 GHz. Ο ρυθμός μετάδοσης μεταβάλλεται, διότι όταν οι συσκευές δεν έχουν ισχυρό σήμα πρέπει να προσαρμοστεί η ταχύτητα για την εξασφάλιση της σύνδεσης. Με την έκδοση

αυτή, ο όρος Wi-Fi άρχισε να χρησιμοποιείται και να εξαπλώνεται η χρήση των ασύρματων δικτύων.

802.11a: Η προδιαγραφή 802.11a χρησιμοποιεί τη ζώνη συχνοτήτων των 5 GHz. Σε αντίθεση με τις άλλες προδιαγραφές, χρησιμοποιεί την ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM) με αποτέλεσμα να υποστηρίζει ρυθμούς μετάδοσης δεδομένων έως 54 Mbps. Μειονέκτημα της συγκεκριμένης προδιαγραφής είναι η ασυμβατότητα με τις ασύρματες κάρτες δικτύου οι οποίες υποστηρίζουν 802.11b.

802.11g: Το 2003 ανακοινώθηκε το πρότυπο 802.11g, το οποίο διορθώνει το πρόβλημα συμβατότητας μεταξύ των προτύπων 802.11a και 802.11b. Όπως και το πρότυπο 802.11a, χρησιμοποιεί και αυτό την ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM), υποστηρίζει ρυθμούς μετάδοσης δεδομένων έως 54 Mbps, με τη διαφορά να εντοπίζεται στα 2,4 GHz της ζώνης συχνοτήτων. Το πρότυπο 802.11g είναι συμβατό με το 802.11b, καθιστώντας εφικτή την επικοινωνία συσκευών εξοπλισμένων με κάρτες 802.11b και 802.11g.

802.11n: Το 2009 παρουσιάστηκε το πρότυπο 802.11n το οποίο ενσωματώνει τεχνολογικά στοιχεία των προηγούμενων προτύπων αλλά και καινούρια τεχνικά χαρακτηριστικά για την επίτευξη μεγαλύτερων ταχυτήτων. Κάνει χρήση πολλαπλών «έξυπνων» κεραιών (MIMO), έχει ρυθμό μετάδοσης από 100 έως 140 Mbps, ενώ θεωρητικά μπορεί να πετύχει ρυθμό μετάδοσης ακόμη και 400 Mbps.



Εικόνα 2: Χρήση πολλαπλών «έξυπνων» κεραιών (MIMO)

Είναι σημαντικό να τονίσουμε ότι η MIMO τεχνολογία απαιτεί ξεχωριστές ραδιοσυχνότητες (RF) και διαφορετικούς analog to digital μετατροπείς (ADC) για κάθε MIMO κεραία.

Εκτός των ανωτέρω εκδόσεων υπάρχουν και άλλες εκδόσεις, οι οποίες όμως δεν έχουν υλοποιηθεί σε εμπορικά προϊόντα και έχουν περισσότερο ακαδημαϊκό ενδιαφέρον. Οι σπουδαιότερες είναι:

802.11f: Το πρότυπο αυτό ανακοινώθηκε το 2003 και επιτρέπει την άμεση επικοινωνία μεταξύ διαφορετικών access point ώστε να εξαλειφθεί η απώλεια πλαισίων κατά τη μετάδοση.

802.11e: Το MAC πρωτόκολλο του IEEE 802.11 δεν παρέχει καμιά προτεραιότητα στους σταθμούς που μεταδίδουν. Όλοι οι σταθμοί έχουν την ίδια προτεραιότητα, με αποτέλεσμα να μη μπορούν να υποστηριχθούν εφαρμογές που απαιτούν ποιότητα υπηρεσίας. Για τον παραπάνω λόγο ανακοινώθηκε το 2005 το πρότυπο 802.11e, που παρέχει μηχανισμούς και διασφαλίζει τις διαδικασίες εκείνες που περιλαμβάνουν τη μεταφορά φωνής, ήχου και βίντεο στα ασύρματα τοπικά δίκτυα.

	802.11	**a**	**b**	**g**	**n**
Release	1997	1999	1999	2003	2009
Frequency (GHz)	2.4	5	2.4	2.4	2,4 ή 5
Data rate (Mbps)	2	54	11	54	100-140
Modulation	FHSS/DSSS	OFDM	DSSS	OFDM	MIMO
Indoor range (m)	~20	~35	~38	~38	~70

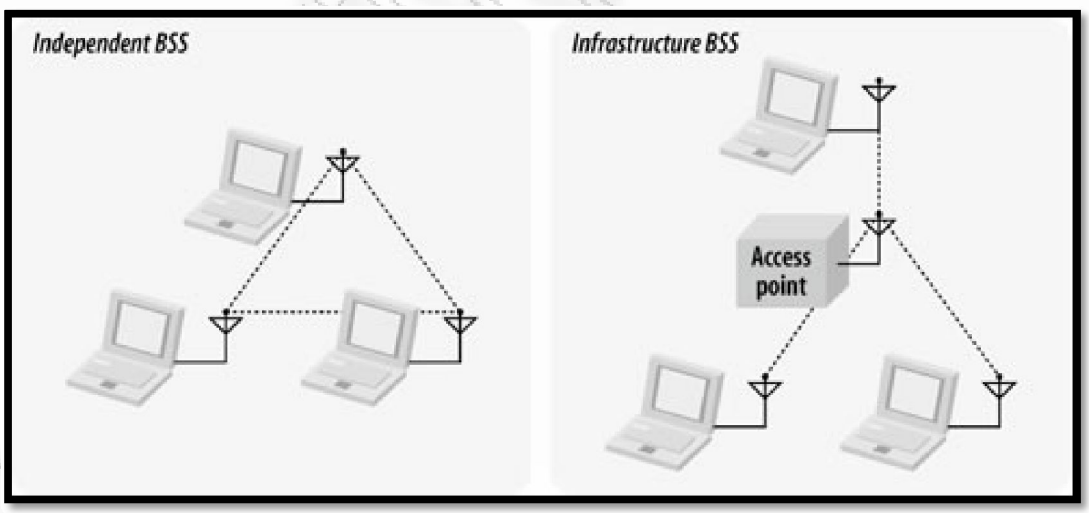
Πίνακας 1: Η εξελικτική πορεία των προτύπων 802.11

2.8 Αρχιτεκτονική του IEEE 802.11

Το μικρότερο τμήμα ενός ασύρματου δικτύου είναι μία βασική ομάδα υπηρεσιών Basic Service Set (BSS), η οποία αποτελείται από έναν αριθμό σταθμών που εκτελούν το ίδιο πρωτόκολλο MAC και ανταγωνίζονται για την πρόσβαση στο ίδιο κοινόχρηστο ασύρματο μέσο. Κάθε BSS έχει μια περιοχή κάλυψης που ονομάζεται Basic Service Area και καθορίζεται από τα τεχνικά χαρακτηριστικά των συσκευών και των κεραιών. Κάθε σταθμός ανήκει σε μία μόνο BSS, δηλαδή

βρίσκεται μέσα στην ασύρματη εμβέλεια μόνο όσων σταθμών βρίσκονται στην ίδια BSS και διακρίνεται σε δύο τύπους λειτουργίας:

- Independent BSS ή Ad-hoc mode: Είναι η πιο απλή περίπτωση δημιουργίας ενός ασύρματου δικτύου, όπου κάθε ασύρματος σταθμός επικοινωνεί απευθείας με όλους τους άλλους σταθμούς. Η δημιουργία ενός ad-hoc δικτύου είναι πολύ εύκολη και γρήγορη, γι' αυτό χρησιμοποιείται συνήθως σε περιπτώσεις που απαιτείται η δημιουργία ενός δικτύου ανταλλαγής δεδομένων για περιορισμένο χρονικό διάστημα. Οι δυνατότητες αυτού του τύπου δικτύου όσον αφορά την ασφάλεια είναι αρκετά περιορισμένες σε σχέση με το Infrastructure BSS.
- Infrastructure BSS: Τα Infrastructure ασύρματα δίκτυα διαφοροποιούνται από τα ad-hoc, λόγω της χρήσης των access points. Ένα Infrastructure BSS αποτελείται από ένα access point και ένα αριθμό από ασύρματους σταθμούς. Το access point αποτελεί το κεντρικό κομβικό σημείο του Infrastructure BSS, καθώς όλη η δικτυακή κίνηση μεταξύ των σταθμών περνάει αναγκαστικά από το access point.



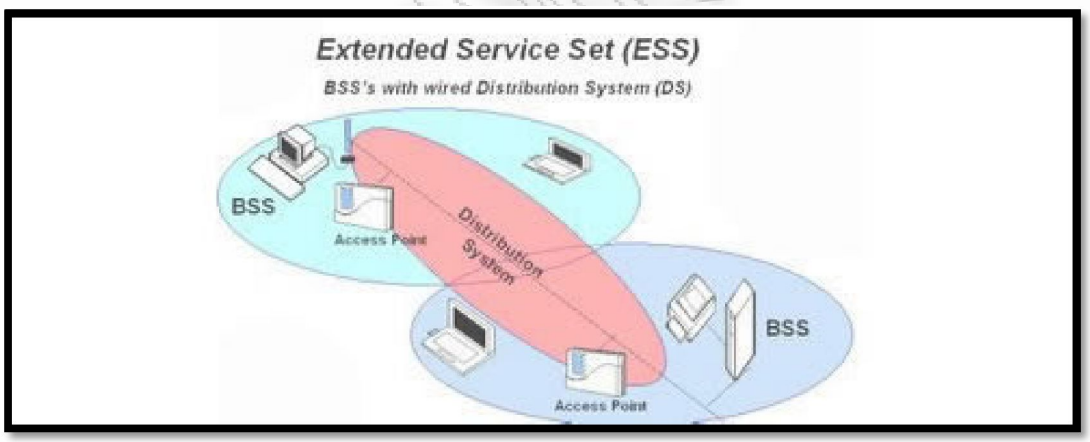
Εικόνα 3: Τύποι ασύρματων δικτύων

Η χρήση των access point παρέχει δύο σημαντικά πλεονεκτήματα:

- Η ακτίνα της περιοχής κάλυψης του BSS καθορίζεται με βάση την απόσταση από το access point. Αυτό σημαίνει ότι κάθε σταθμός αρκεί να βρίσκεται στην εμβέλεια του access point.

- Η δομή του Infrastructure BSS επιτρέπει την διαχείριση του δικτύου από ένα κεντρικό κόμβο και παρέχει μεγάλη ευελιξία όσον αφορά την ασφάλεια. Αυτό οφείλεται στην ύπαρξη ενός κεντρικού κόμβου στο δίκτυο και στον τρόπο με τον οποίο ένας ασύρματος σταθμός συνδέεται στο access point για να επικοινωνήσει με το υπόλοιπο δίκτυο.

Extended Service Set (ESS): Μία εκτεταμένη ομάδα υπηρεσιών αποτελείται από δύο ή περισσότερα BSS που συνδέονται μεταξύ τους. Το Distribution System (DS) είναι το συστατικό της αρχιτεκτονικής που διασυνδέει τα BSS. Η σύνδεση γίνεται συνδέοντας τα access points των BSS μεταξύ τους μέσω του δικτύου κορμού. Αυτή η λύση, επιτρέπει την επικοινωνία των ασύρματων σταθμών που βρίσκονται σε διαφορετικά BSS, καθώς και την μετακίνηση από ένα BSS σε ένα άλλο χωρίς να διακοπεί η επικοινωνία. Φυσικά, αυτό μπορεί να γίνει μόνο με την προϋπόθεση ότι μεταξύ των BSS δεν υπάρχουν κενά στην κάλυψη.



Εικόνα 4: Extended Service Set

2.8.1 Υπηρεσίες του IEEE 802.11

Το ασύρματο δίκτυο 802.11 ορίζει εννέα υπηρεσίες που το υποστηρίζουν ώστε να παρέχει λειτουργικότητα ισοδύναμη με αυτή των ενσύρματων δικτύων.

Διανομή (Distribution): Είναι η κύρια υπηρεσία που χρησιμοποιείται από τους σταθμούς για την ανταλλαγή πλαισίων MAC όταν το πλαίσιο πρέπει να παραδοθεί από το AP στον τελικό προορισμό του.

Ενοποίηση (Integration): Η υπηρεσία ενοποίησης δίνει τη δυνατότητα μεταφοράς δεδομένων μεταξύ ενός σταθμού 802.11 LAN και ενός σταθμού ενοποιημένου

802.x LAN. Ο όρος ενοποιημένο αναφέρεται σε ένα ενσύρματο τοπικό δίκτυο το οποίο είναι φυσικά συνδεδεμένο στο DS και του οποίου οι σταθμοί μπορεί να είναι λογικά συνδεδεμένοι με ένα ασύρματο τοπικό δίκτυο μέσω της υπηρεσίας ενοποίησης. Αναλαμβάνει ουσιαστικά τη μετάφραση της όποιας διεύθυνσης και της όποιας μετατροπής μέσου απαιτούνται για την ανταλλαγή των δεδομένων.

Παράδοση MSDU: Η παράδοση των πλαισίων MAC (MAC Service Data Unit) στον τελικό προορισμό τους.

Συσχέτιση (Association): Αποκαθιστά μία αρχική συσχέτιση μεταξύ ενός σταθμού και ενός σημείου πρόσβασης, προκειμένου ένας σταθμός να εκπέμψει ή να κάνει λήψη πλαισίων σε ένα ασύρματο δίκτυο. Η συσχέτιση δίνει τη δυνατότητα στο δίκτυο διανομής (DS) να γνωρίζει τη θέση κάθε σταθμού και κατά συνέπεια το Access Point προωθεί τα πλαίσια για να τα λάβει ο σταθμός.

Επανασυσχέτιση (Reassociation): Δίνει τη δυνατότητα σε μία συσχέτιση που είναι ήδη αποκατεστημένη να μεταφερθεί από ένα σημείο πρόσβασης σε ένα άλλο, επιτρέποντας σε ένα κινητό σταθμό να μετακινηθεί από μία BSS σε μία άλλη, διατηρώντας την σύνδεσή του στο δίκτυο.

Αποσυσχέτιση (Disassociation): Είναι μία ειδοποίηση είτε από ένα σταθμό είτε από ένα σημείο πρόσβασης ότι μία υπάρχουσα συσχέτιση τερματίζεται.

Πιστοποίηση (authentication): Χρησιμοποιείται για την επαλήθευση της ταυτότητας των σταθμών μεταξύ τους. Σε ένα ενσύρματο δίκτυο, γενικά θεωρείται ότι η πρόσβαση στη φυσική σύνδεση μεταβιβάζει και το δικαίωμα της σύνδεσης στο δίκτυο. Στα ασύρματα δίκτυα η φυσική σύνδεση επιτυγχάνεται απλά έχοντας μία κεραία κατάλληλα συντονισμένη, για αυτό τον λόγο η υπηρεσία πιστοποίησης χρησιμοποιεί τους σταθμούς για την επαλήθευσης της ταυτότητάς τους.

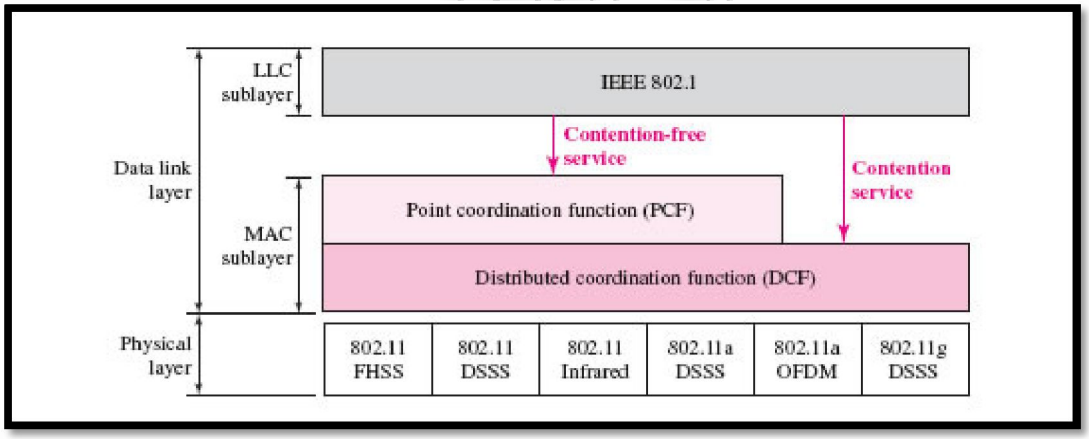
Αποπιστοποίηση (deauthentication): Αυτή η υπηρεσία χρησιμοποιείται όταν μία υπάρχουσα πιστοποίηση πρόκειται να τερματιστεί.

Ιδιωτικότητα (privacy): Χρησιμοποιείται για να αποτρέψει την ανάγνωση των περιεχομένων των μηνυμάτων από σταθμούς άλλους, εκτός από τον

προοριζόμενο αποδέκτη. Το πρότυπο επιτρέπει την προαιρετική χρήση κρυπτογράφησης για την εξασφάλιση προστασίας.

2.9 Αρχιτεκτονική πρωτοκόλλου IEEE 802.11

Το πρότυπο 802.11 ορίζει κάποια επίπεδα κατά αντιστοιχία με τα επίπεδα του προτύπου OSI. Το φυσικό επίπεδο (physical layer) ορίζει τον τρόπο μετάδοσης και λήψης σημάτων. Το Data link layer του OSI μοντέλου είναι υποδιαιρεμένο σε δυο υποεπίπεδα, το Medium Access Control (MAC) και το Logical Link Control (LLC). Το υποεπίπεδο MAC ορίζει τον τρόπο πρόσβασης στο μέσο μετάδοσης καθώς και την αξιοπιστία της μετάδοση των δεδομένων. Τέλος, το υποεπίπεδο LLC είναι ένα επίπεδο σύνδεσης, που χρησιμοποιείται από κοινού σε όλα τα πρότυπα LAN του IEEE.



Εικόνα 5: Αρχιτεκτονική πρωτοκόλλου IEEE 802.11

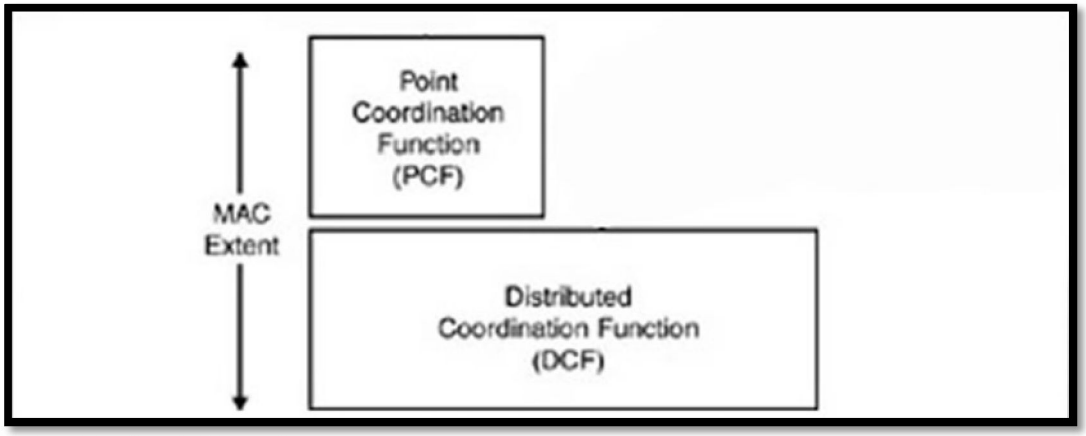
Το υποεπίπεδο MAC είναι υπεύθυνο για τον έλεγχο των παρακάτω λειτουργιών:

- Τον έλεγχο της πρόσβασης των σταθμών στο μέσο μετάδοσης.
- Τη λειτουργία του κατακερματισμού και της επανασυναρμολόγησης (fragmentation and reassembly).
- Τη λειτουργία της αναμετάδοσης πακέτου (packet retransmission).
- Τη λειτουργία της επιβεβαίωσης λήψης (acknowledge).

Στην αρχιτεκτονική του MAC υποεπιπέδου ορίζονται δύο μέθοδοι πρόσβασης:

- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)

Παρατηρούμε πως η DCF λειτουργία είναι η βασική μέθοδος, διότι λειτουργεί σαν βάση για την PCF, επιτρέποντας της να υλοποιεί έναν polling αλγόριθμο προσπαθώντας να εξασφαλίσει καλύτερο QoS.



Εικόνα 6: Δομή του MAC επιπέδου

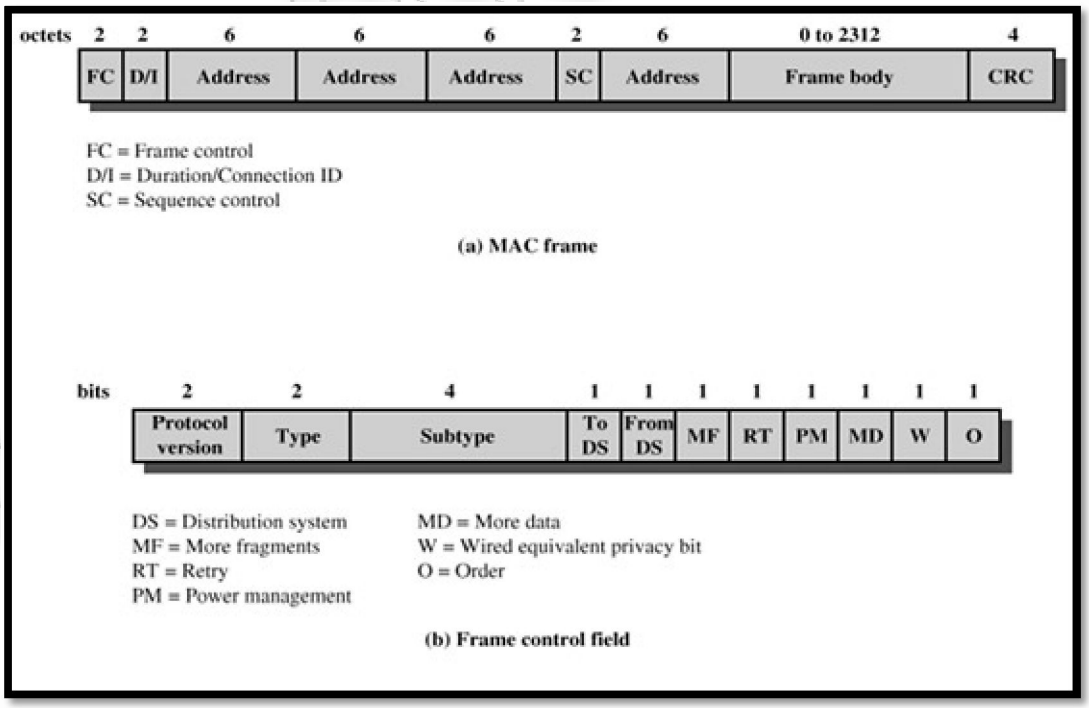
DCF: Η μέθοδος DCF είναι η βασική μέθοδος που χρησιμοποιείται για την υποστήριξη της ασύγχρονης μεταφοράς δεδομένων. Όπως ορίζεται στο πρότυπο, όλοι οι σταθμοί πρέπει να υποστηρίζουν την DCF μέθοδο. Η λειτουργία της βασίζεται στο πρωτόκολλο Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Η μέθοδος DCF δεν υποστηρίζει κάποιον μηχανισμό ανίχνευσης των συγκρούσεων, όπως το CSMA/CD, διότι η ανίχνευση των συγκρούσεων δεν είναι πρακτική σε ένα ασύρματο δίκτυο. Για την μετάδοση πρέπει ο σταθμός να παρακολουθεί το φυσικό μέσο ώστε να εξακριβώσει αν κάποιος άλλος σταθμός εκπέμπει. Στα ενσύρματα δίκτυα η παρακολούθηση του καναλιού είναι πολύ εύκολο να γίνει, διότι όλοι οι κόμβοι είναι συνδεδεμένοι με ένα κοινό καλώδιο και μπορούν να επικοινωνήσουν μεταξύ τους. Αντίθετα στα ασύρματα δίκτυα ο πομποδέκτης κάθε σταθμού έχει περιορισμένη εμβέλεια και μπορεί να επικοινωνήσει άμεσα μόνο με τους γειτονικούς σταθμούς. Η επικοινωνία με πιο απομακρυσμένους σταθμούς πραγματοποιείται χρησιμοποιώντας άλλους ενδιάμεσους που είναι σε θέση να προωθήσουν το πακέτο στον τελικό προορισμό. Για να γίνει εφικτή η παρακολούθηση του καναλιού ανταλλάσσονται ειδικά πλαίσια ελέγχου Request to Send (RTS) και Clear to Send (CTS) μεταξύ αποστολέα και παραλήπτη. Ο μηχανισμός αυτός ελέγχει το φυσικό μέσο με σκοπό την μείωση της πιθανότητας να συμβεί σύγκρουση πακέτων. Η ανταλλαγή γίνεται μετά τον έλεγχο διαθεσιμότητας του

μέσου και ακριβώς πριν την αποστολή των δεδομένων. Βελτιώνει την αξιοπιστία σε δίκτυα με πολλούς σταθμούς, όπου η πιθανότητα συγκρούσεων είναι αυξημένη.

PCF: Η μέθοδος PCF αποτελεί μία εναλλακτική μέθοδο και λειτουργεί ένα επίπεδο πιο πάνω από την μέθοδο DCF, γιατί η μέθοδος πρόσβασης εναλλάσσεται, για κάποιο χρονικό διάστημα χρησιμοποιείται η PCF και για το υπόλοιπο χρησιμοποιείται η DCF. Απαιτεί την ύπαρξη ενός κεντρικού σταθμού (Point Coordinator) που αναλαμβάνει την κεντρική διαχείριση των εκπομπών των υπολοίπων σταθμών. Ο Point Coordinator ρωτάει κυκλικά όλους τους σταθμούς αν έχουν δεδομένα προς αποστολή και μπορούν να εκπέμψουν μόνο αν τους το επιτρέψει.

2.9.1 Πλαίσιο MAC

Οι συσκευές που χρησιμοποιούνται στα ασύρματα δίκτυα επικοινωνούν μεταξύ τους ανταλλάσσοντας πλαίσια στο υποεπίπεδο MAC. Η μορφοποίηση του πλαισίου του 802.11 φαίνεται στην παρακάτω εικόνα.



Εικόνα 7: Μορφοποίηση πλαισίου MAC του 802.11

Το MAC πλαίσιο αποτελείται από το header μήκους 30 bytes, από πλαίσια μεταβλητού μήκους και το πλαίσιο FCS μήκους 4 bytes.

Έλεγχος πλαισίου (Frame control): Το πεδίο αυτό είναι σημαντικό διότι δηλώνει τον τύπο του πλαισίου και παρέχει πληροφορίες ελέγχου. Αποτελείται από 11 υποπεδία, τα οποία είναι σημαντικά για τους μηχανισμούς ασφαλείας του προτύπου 802.11 και αναλύονται παρακάτω.

- Έκδοση πρωτοκόλλου (Protocol version): Δηλώνει την έκδοση του 802.11 MAC που περιέχεται στο πλαίσιο.
- Τύπος (Type): Προσδιορίζει τους τρεις τύπους πλαισίων. Είναι τα πλαίσια ελέγχου (control frames), τα πλαίσια δεδομένων (data frames) και τα πλαίσια διαχείρισης (management frames).
- Υποτύπος (Subtype): Υποδιαιρεί κάθε ένα από τους βασικούς τύπους πλαισίου, σε κάποιους υποτύπους.
- Προς DS (To DS): Το bit έχει την τιμή 1 όταν ένα πλαίσιο δεδομένων προορίζεται για το σύστημα διανομής.
- Από DS (From DS): Το bit έχει την τιμή 1 όταν ένα πλαίσιο δεδομένων φεύγει από το σύστημα διανομής.
- Επιπλέον τμήματα (More fragments): Το πεδίο έχει τιμή 1 όταν μετά από αυτό ακολουθούν και άλλα τμήματα.
- Επανάληψη (Retry): Εάν έχει τιμή 1 το πλαίσιο έχει επανεκπεμφθεί.
- Διαχείριση ενέργειας (Power management): Προσδιορίζει την κατάσταση διαχείρισης ενέργειας του σταθμού. Εάν η τιμή είναι 1 ο σταθμός που εκπέμπει είναι σε κατάσταση ύπνου (sleep mode).
- Επιπλέον δεδομένα (More Data): Δηλώνει ότι ένας σταθμός έχει αποθηκευμένα και άλλα δεδομένα που πρόκειται να σταλούν. Το κάθε μπλοκ δεδομένων μπορεί να εκπεμφθεί σαν ένα πλαίσιο ή σαν μία ομάδα τμημάτων σε πολλαπλά πλαίσια.
- Protected frame: Το πλαίσιο αυτό ονομαζόταν WEP στο αρχικό πρότυπο 802.11. Με την έκδοση 802.11i άλλαξε ονομασία και δηλώνει με την τιμή 1 ότι το σώμα του πλαισίου είναι κρυπτογραφημένο με κάποιο πρωτόκολλο ασφαλείας.

- Σειρά (Order): Αν έχει την τιμή 1 δηλώνει ότι χρησιμοποιείται η υπηρεσία Τήρησης Σειράς (strictly ordered).

Ταυτότητα διάρκειας (Duration ID): Ο ρόλος του πεδίου αυτού είναι διπλός και εξαρτάται από τον τύπο του πλαισίου. Αν χρησιμοποιείται ως πεδίο διάρκειας υποδηλώνει το χρονικό διάστημα (σε μs) που θα διαρκέσει η εκπομπή του πλαισίου, δηλαδή το χρονικό διάστημα για το οποίο το μέσο μετάδοσης θα είναι απασχολημένο. Όταν είναι πλαίσιο ελέγχου, περιέχει μία ταυτότητα συσχέτισης ή σύνδεσης.

Διευθύνσεις (Addresses): Υπάρχουν τέσσερα πεδία διευθύνσεων. Το κάθε πεδίο χρησιμοποιείται για διαφορετικό σκοπό ανάλογα με το είδος του πλαισίου. Ο τύπος διεύθυνσης μπορεί να είναι διεύθυνση προορισμού, πηγής, εκπέμποντος σταθμού και λαμβάνοντος σταθμού.

Έλεγχος σειράς (Sequence Control): Το πεδίο αυτό περιέχει δύο υποπεδία. Τον αριθμό τμήματος (fragment number) 4 bit που χρησιμοποιείται για την κατάτμηση και την ανασύνθεση, και ένα αριθμό σειράς πλαισίου (sequence number) 12 bit που χρησιμοποιείται για την αρίθμηση των πλαισίων που στέλνονται μεταξύ ενός πομπού και ενός δέκτη.

Frame Check Sequence (FCS): Το πεδίο περιέχει ένα 4 byte Cyclical Redundancy Check (CRC) το οποίο χρησιμοποιείται για τον έλεγχο ακεραιότητας των πλαισίων που λαμβάνονται.

ΚΕΦΑΛΑΙΟ 3

Ασφάλεια σε ασύρματα δίκτυα

3.1 Γενικά

Τα πλεονεκτήματα της χρήσης των ασύρματων δικτύων είναι αναμφίβολα πολλά, με σημαντικότερο την ευελιξία που παρέχουν. Όμως, λόγω του ότι τα δεδομένα που διακινούνται στο δίκτυο μεταδίδονται χρησιμοποιώντας ραδιοσυχνότητες, επιτρέπεται στον οποιονδήποτε να συνδεθεί στο δίκτυο. Αμέσως δημιουργήθηκε η ανάγκη της ασφάλειας του δικτύου, την οποία ήρθαν να καλύψουν οι τεχνικές κρυπτογράφησης. Η εμπιστοσύνη, η ακεραιότητα, η πιστοποίηση και η διαθεσιμότητα της ανταλλασσόμενης πληροφορίας, πλέον οριοθετούνται από τα πρωτόκολλα κρυπτογράφησης, τα οποία βασίζονται σε ήδη γνωστές κρυπτογραφικές μεθόδους, κληρονομώντας έτσι τα όποια μειονεκτήματα και πλεονεκτήματα από άλλες υλοποιήσεις της σύγχρονης επιστήμης της κρυπτογραφίας.

3.2 Κρυπτογράφηση

Κρυπτογράφηση (encryption) είναι ο μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανέναν παρά μόνο από αυτόν που διαθέτει το κατάλληλο κλειδί.

Υπάρχουν δύο οικογένειες αλγόριθμων κρυπτογράφησης:

- Οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι μυστικού κλειδιού)
- Οι ασύμμετροι αλγόριθμοι (ή αλγόριθμοι δημόσιου κλειδιού)

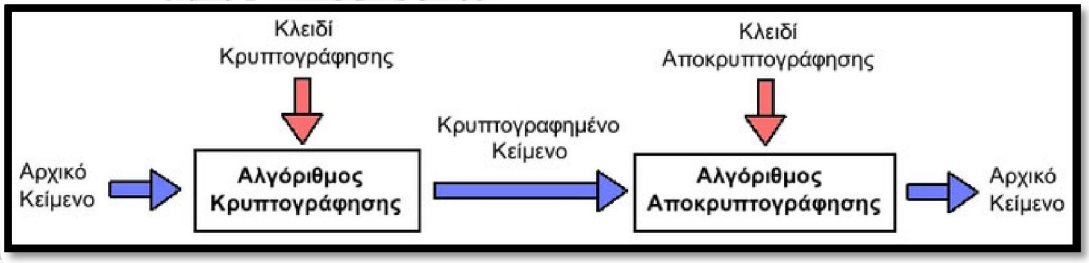
Ο κύριος στόχος της κρυπτογράφησης είναι να παρέχει μηχανισμούς ώστε δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να έχει την ικανότητα να διαβάσει την πληροφορία.

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες:

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη.
- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- Πιστοποίηση: Οι αποστολείς και οι παραλήπτες μπορούν να εξακριβώνουν τις ταυτότητές τους, καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Βασική ορολογία κρυπτογράφησης:

- Αρχικό κείμενο (plaintext): είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- Κλειδί (key): είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.
- Κρυπτογραφημένο κείμενο (ciphertext): είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.



Εικόνα 8: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου και ενός κλειδιού κρυπτογράφησης. Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης.

3.2.1 Κρυπτογράφηση συμμετρικού κλειδιού

Η κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography) προϋποθέτει την ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση του μηνύματος. Το πρόβλημα που εντοπίζεται στην κρυπτογράφηση συμμετρικού κλειδιού είναι η αδυναμία ανταλλαγής του κλειδιού με ασφαλή τρόπο. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες:

- Αλγόριθμοι ροής: (stream ciphers), οι οποίοι λειτουργούν bit προς bit.
- Μπλοκ αλγόριθμοι: (block ciphers), οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit).

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

3.2.2 Κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρου κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970. Η κρυπτογράφηση των κλειδιών γίνεται με τελείως διαφορετικό τρόπο. Είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Ο αποστολέας και ο παραλήπτης διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες, το ιδιωτικό (private) και το δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να ανακοινώνεται στους παραλήπτες. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το

άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού.

3.3 Πρωτόκολλα κρυπτογράφησης ασύρματων δικτύων

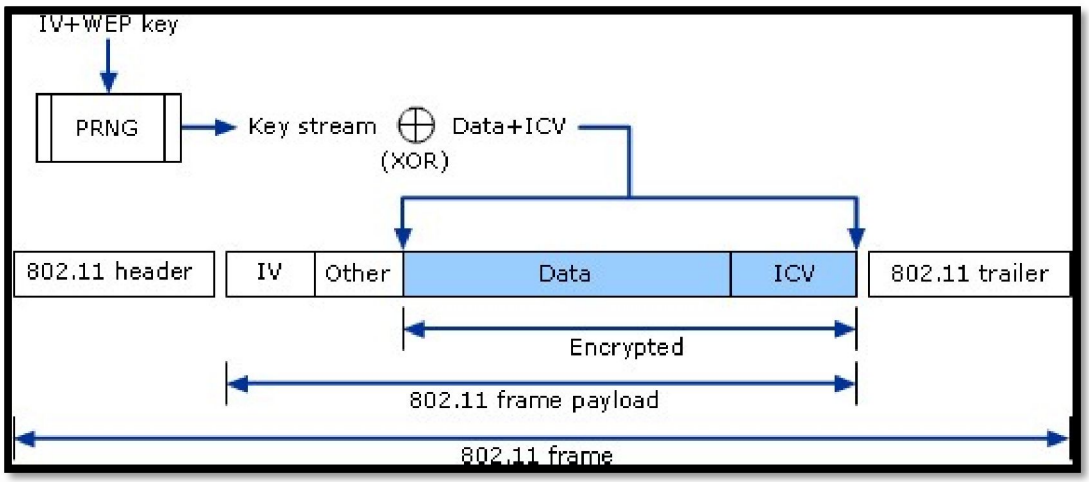
Από την έρευνα που πραγματοποιήθηκε σε κεντρικές περιοχές της πόλης των Αθηνών, ακόμη και σήμερα, παρατηρήθηκε ότι είναι αρκετά τα δίκτυα που δεν χρησιμοποιούν κανενός είδους κρυπτογράφηση. Σε αυτά τα ανασφάλιστα δίκτυα είναι προφανές ότι δεν μπορεί να υπάρξει καμία προστασία στους χρήστες που είναι συνδεδεμένοι, στην πληροφορία που ανταλλάσουν, καθώς και στα αποθηκευμένα δεδομένα στο εσωτερικό του δικτύου. Η κρυπτογράφηση των ασύρματων δικτύων μπορεί να χωριστεί σε δύο βασικές κατηγορίες:

- WEP: Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4, για τον οποίο πλέον υπάρχουν διαδεδομένες τεχνικές εύρεσης του μυστικού κλειδιού.
- Στην οικογένεια WPA/WPA2: Θεωρείται το πιο ασφαλές πρωτόκολλο κρυπτογράφησης. Αντικατέστησε το ανασφαλές WEP και χρησιμοποιεί τον αλγόριθμο CCMP, ο οποίος βασίζεται στον AES.

3.4 Κρυπτογράφηση WEP

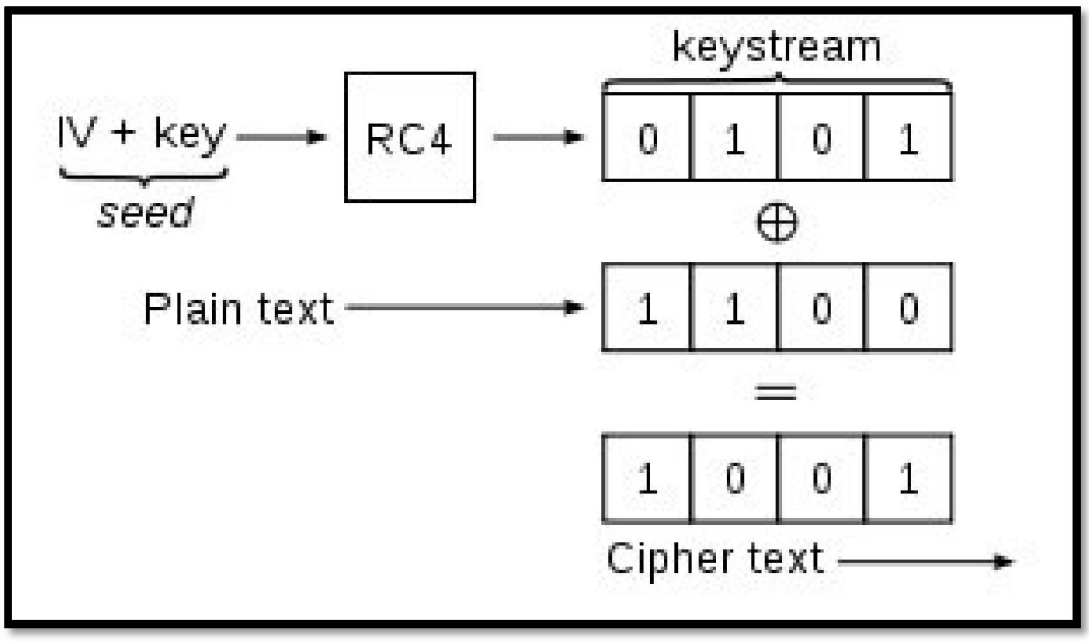
Ο τομέας της ασφάλειας των επικοινωνιών θέτει τους ακόλουθους τρεις σημαντικούς στόχους:

- Εμπιστευτικότητα: με τον όρο αυτό περιγράφεται η προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών.
- Ακεραιότητα: η διασφάλιση ότι το στοιχείο δεν έχει τροποποιηθεί.
- Επικύρωση: η υποστήριξη οπουδήποτε μηχανισμού ασφάλειας της αξιοπιστίας των δεδομένων.



Εικόνα 9: Υλοποίηση WEP

Το πρωτόκολλο κρυπτογράφησης WEP παρέχει τις διαδικασίες που βοηθούν στην επιτυχία αυτών των στόχων. Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων στο πρωτόκολλο αυτό εξασφαλίζεται συγχρόνως, χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης RC4 (River Cipher 4), μήκους 64 ή 128 bit. Είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας, ο οποίος δημιουργεί μία ψευδοτυχαία ακολουθία από bit, που συνδυάζεται με το υπό κρυπτογράφηση κείμενο (cipher text) με τη γνωστή συνάρτηση XOR για να παράξει το κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο κείμενο παράγεται χρησιμοποιώντας τα 24 bit του πίνακα αρχικοποίησης (Initialization Vector) και το κλειδί κρυπτογράφησης (pre-shared key) που εισήγαγε ο χρήστης, μήκους 40 ή 104 bit. Το αποτέλεσμα εισάγεται σε μία πύλη XOR μαζί με το αρχικό κείμενο (plain text) ώστε να δημιουργηθεί το τελικό κρυπτογραφημένο κείμενο.



Εικόνα 10: Basic WEP encryption: RC4 keystream XORed with plaintext

Το πρωτόκολλο WEP χρησιμοποιεί ένα κλειδί μήκους μόνο 40 bit, λόγω περιορισμών που έθεσε η Αμερικάνικη κυβέρνηση, το οποίο ευνοεί τις brute force επιθέσεις. Οι συγκεκριμένες επιθέσεις χρησιμοποιούν όλους τους πιθανούς συνδυασμούς κλειδιών μέχρι να βρεθεί το σωστό, με αποτέλεσμα υπολογιστές με μεγάλη υπολογιστική ισχύ να το σπάσουν πολύ γρήγορα. Όταν οι περιορισμοί κάμφθηκαν, όλοι οι κατασκευαστές προσπάθησαν να το διορθώσουν. Επέκτειναν το μήκος του κλειδιού στα 128 bit χρησιμοποιώντας κλειδί κρυπτογράφησης μήκους 104 bit. Αυτό δεν άλλαξε τον τρόπο επίθεσης, αλλά λόγω της μεγάλης υπολογιστικής ισχύς που χρειάζονταν, καθιστά τις brute force επιθέσεις δυσκολότερες.

Η επικύρωση εξασφαλίζεται μέσω του ελέγχου των πακέτων. Ο αλγόριθμος CRC32 αναπτύχθηκε για να εντοπίζει, να επισημαίνει και πολλές φορές να διορθώνει τα λάθη κατά τη μετάδοση των πακέτων.

3.4.1 Ασφάλεια στο WEP

Η κρυπτογράφηση του πρωτοκόλλου WEP έχει μειωμένα επίπεδα ασφαλείας, γεγονός που το κάνει ιδιαίτερα ευάλωτο σε επιθέσεις. Το μήκος του IV είναι μόλις 24 bit, τα οποία θεωρούνται λίγα για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων. Η τιμή ελέγχου ακεραιότητας (ICV) δεν παρέχει την

απαιτούμενη ασφάλεια και δεν αποτρέπει την τροποποίηση των μηνυμάτων από κάποιον εισβολέα. Επιπλέον, το WEP συνδυάζει το κλειδί της κρυπτογράφησης με το IV, με τέτοιο τρόπο ώστε ο οποιοσδήποτε μπορεί να αποκτήσει το κλειδί της κρυπτογράφησης χρησιμοποιώντας μερικά εκατομμύρια κρυπτογραφημένα πακέτα. Επιπλέον δεν παρέχεται προστασία της ακεραιότητας των διευθύνσεων του αποστολέα και του παραλήπτη.

Οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης (IV), ο οποίος εκπέμπεται συνεχώς μαζί με τα πακέτα. Τη στιγμή που θα επανεκπεμφθεί ο ίδιος πίνακας σε δύο διαφορετικά πακέτα, μπορούμε μέσω της XOR να βρούμε κομμάτια του αρχικού κειμένου. Τμηματικά θα αποκαλυφθεί όλο το μη-κωδικοποιημένο κομμάτι του μηνύματος. Επειδή ο χρόνος εκπομπής του πίνακα αρχικοποίησης δεν είναι ίδιος, έχουν αναπτυχθεί διάφορες τεχνικές για την επιτάχυνση της. Η πιο συνηθισμένη τεχνική είναι ο εξαναγκασμός του σταθμού να εκπέμψει πάλι το πακέτο είτε λόγω απώλειας, είτε απόρριψης, είτε στέλνοντας πακέτα NACK. Με αυτή τη τεχνική, ο σταθμός αναγκάζεται να εκπέμπει συνεχώς, μειώνοντας έτσι ταχύτατα το διαθέσιμο εύρος τιμών του, με αποτέλεσμα σε σύντομο χρονικό διάστημα να επανεκπεμφθεί ο ίδιος πίνακας.

Η ακεραιότητα των δεδομένων δεν είναι καλά προστατευμένη στο WEP, διότι ο αλγόριθμος CRC προστατεύει μόνο από τυχαία λάθη που συμβαίνουν κατά τη μετάδοση. Γι’ αυτό το λόγο τα κρυπτογραφημένα πακέτα μπορούν να αλλοιωθούν ή να υποκλαπούν. Οι εταιρείες αναγκάστηκαν να προβούν σε διορθώσεις του πρωτοκόλλου. Νέες εκδόσεις αναπτύχθηκαν για να εξαλειφθούν τα ελαττώματα του. Η πρώτη αναβάθμιση έγινε με την έκδοση WEP2 η οποία αύξησε το μέγεθος του πίνακα αρχικοποίηση στα 128 bit. Ως αποτέλεσμα, αυξήθηκε ο χρόνος επανεκπομπής του ίδιου πίνακα αρχικοποίησης. Στη συνέχεια ακολούθησαν ακόμα δύο αναβαθμίσεις, το WEPplus (WEP+) και το Dynamic WEP.

3.5 WPA (Wi-Fi Protected Access)

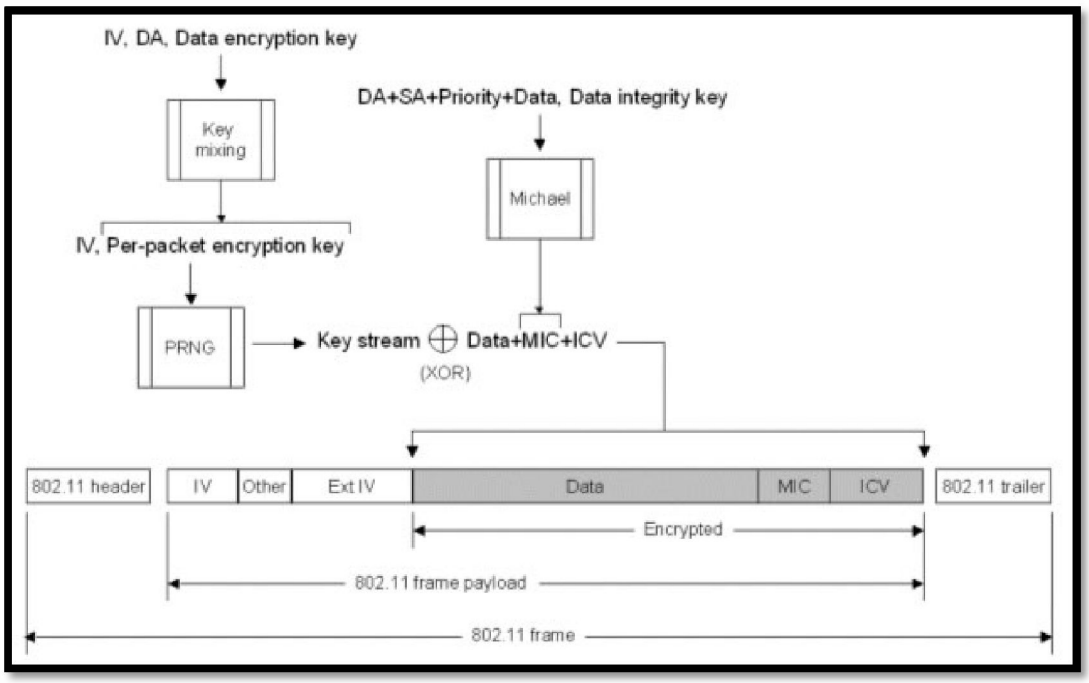
Το 2004 το πρότυπο IEEE με την έκδοση 802.11i ανέπτυξε ένα καινούργιο πρωτόκολλο ασφάλειας για ασύρματη προστατευμένη πρόσβαση, το WPA (Wi-Fi

Protected Access). Ουσιαστικά είναι ο αντικαταστάτης του WEP, διότι υπήρχε η ανάγκη στις ασύρματες μεταδόσεις για περισσότερη ασφάλεια. Αποτέλεσε μία ενδιάμεση λύση έως την πλήρη ανάπτυξη της έκδοσης 802.11i με το πρωτόκολλο WPA2. Η WPA κρυπτογράφηση βελτιώνει την WEP και προσθέτει έναν ισχυρό μηχανισμό αυθεντικοποίησης. Η αυθεντικοποίηση των χρηστών γίνεται με δύο τρόπους λειτουργίας:

- Μέσω της WPA-Personal ή WPA-PSK ο χρήστης συνδέεται σε ένα Access Point και η αυθεντικοποίηση γίνεται μέσω προ-μοιρασμένων κλειδιών (Pre-Shared keys). Επακόλουθο είναι ότι για την καλύτερη ασφάλεια των συνδέσεων παίζει ρόλο το μήκος και η πολυπλοκότητα του κλειδιού.
- Η ασφαλέστερη λειτουργία εκτελείται με την υλοποίηση WPA-Enterprise, η οποία προϋποθέτει την ύπαρξη ενός 802.1x server, μέσω του οποίου ανά τακτά χρονικά διαστήματα, γίνεται ο διαμοιρασμός διαφορετικών κλειδιών για κάθε υπολογιστή, με αποτέλεσμα το σύστημα να είναι πιο ασφαλές, πιο πολύπλοκο και με μεγαλύτερο κόστος.

3.5.1 Ασφάλεια στο WPA

Το WPA χρησιμοποιεί τον RC4 αλγόριθμο, ο οποίος αποτελείται από τον πίνακα αρχικοποίησης μήκους 48 bit και ένα κλειδί χρονικής κρυπτογράφησης μήκους 128 bit. Η ύπαρξη του RC4 και στην καινούργια έκδοση εξασφαλίζει συμβατότητα με τις προηγούμενες εκδόσεις προϊόντων ασύρματης δικτύωσης. Επιπλέον, το WPA εισάγει ένα νέο πρωτόκολλο χρονικής ακεραιότητας κλειδιού, το TKIP (Temporal Key Integrity Protocol), το οποίο αναλαμβάνει δυναμικά την ανανέωση των κλειδιών κατά τη διάρκεια της σύνδεσης. Για να μειωθεί το ποσοστό επανάληψης του ίδιου κλειδιού, χρησιμοποιείται ανά εκπεμπόμενο πακέτο μία ακολουθία αριθμών, το pre-shared key και η εκπεμπόμενη MAC address.



Εικόνα 11: Υλοποίηση WPA

Στο νέο κλειδί που δημιουργείται προστίθεται ο πίνακας αρχικοποίησης και παράγεται μία νέα ακολουθία κλειδιού (keystream). Για την ενίσχυση της ακεραιότητας των πακέτων έχει προστεθεί ένα πεδίο ελέγχου της ακεραιότητας των δεδομένων, το MIC (Message Integration Check). Η τιμή του MIC υπολογίζεται από τον κρυπτογραφικό αλγόριθμο Michael και προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και παραλήπτη. Ένα επιπλέον χαρακτηριστικό είναι ότι υποστηρίζει έναν ειδικό μηχανισμό, ο οποίος ανιχνεύει οποιαδήποτε προσπάθεια παραβίασης του TKIP, με αποτέλεσμα το μπλοκάρισμα της επικοινωνίας.

3.5.2 Αυθεντικοποίηση στο WPA

Η αυθεντικοποίηση στο πρωτόκολλο κρυπτογράφησης WPA-Personal ή WPA-PSK έχει σχεδιαστεί για επαγγελματική και οικιακή χρήση. Με αυτή τη μέθοδο η αυθεντικοποίηση των χρηστών γίνεται μέσω του Access Point χρησιμοποιώντας μία φράση 8 έως 63 ASCII χαρακτήρες. Όταν επιλεγούν οι ASCII χαρακτήρες, μία hash function αναλαμβάνει τη μείωση από τα 504 bit (63characters * 8bit) στα 256 bit. Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το 256 bit

κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κωδικό ως κλειδί.

3.6 WPA vs WEP

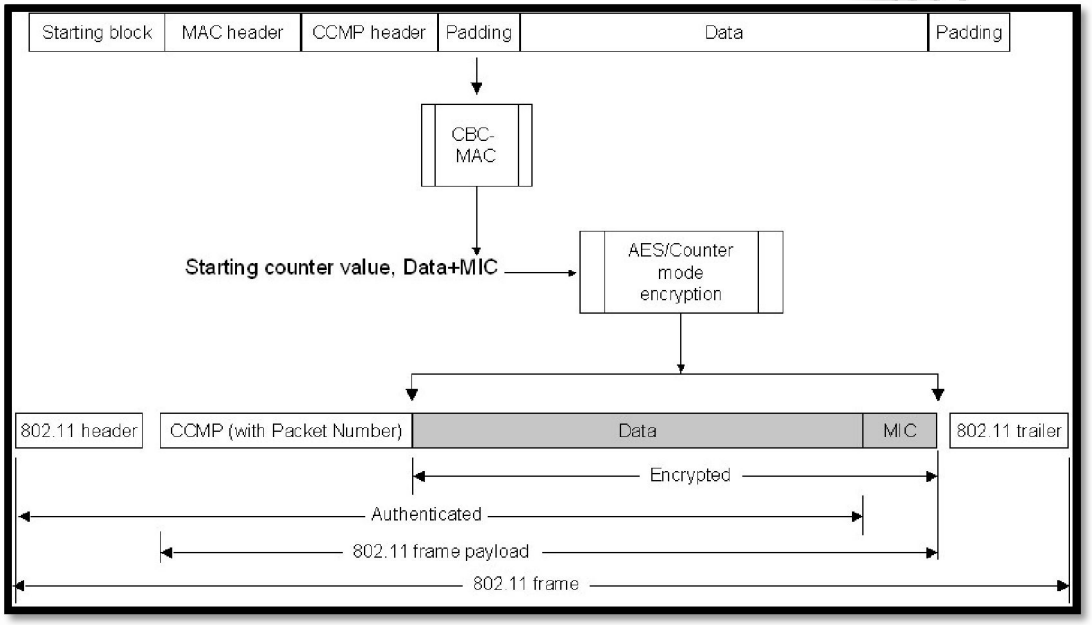
Τα πρωτόκολλα κρυπτογράφησης WPA και WEP χρησιμοποιούν τον αλγόριθμο RC4 για κρυπτογράφηση. Ωστόσο, το WEP χρησιμοποιεί πίνακα αρχικοποίησης μήκους 24 bit με κλειδί κρυπτογράφησης μήκους 40 ή 104 bit, σε αντίθεση με το WPA που χρησιμοποιεί 48 bit IV με 128 bit κλειδί κρυπτογράφησης. Το WEP είναι ανεπαρκές για ασφάλεια, διότι οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης και στις αλλοιώσεις των πακέτων. Στο WPA έχουν ελαχιστοποιηθεί τέτοιου είδους επιθέσεις εξαιτίας του συνδυασμού του πρωτοκόλλου TKIP, του MIC και του μεγαλύτερου μήκους πίνακα αρχικοποίησης. Το κλειδί TKIP χρησιμοποιεί περίπου 300 τρισεκατομμύρια πιθανά κλειδιά για την κρυπτογράφηση του πακέτου. Συνδυάζοντας το με τον 48 bit πίνακα αρχικοποίησης, το TKIP συμβάλλει στην αποτελεσματική ασφάλεια του δικτύου στις επιθέσεις ανάκτησης κλειδιού. Επίσης, το MIC βάζει ένα τέλος στην υποκλοπή πακέτων.

Το WPA-Enterprise και η WPA-PSK κρυπτογράφηση παρέχουν έναν ισχυρό μηχανισμό ασφάλειας, ο οποίος έλειπε από το WEP. Στο WEP η αυθεντικοποίηση του χρήστη γινόταν με τον διαμοιρασμό ενός κοινού κλειδιού. Στο WPA η αυθεντικοποίηση και η κρυπτογράφηση είναι ξεχωριστές λειτουργίες. Η αυθεντικοποίηση στον 802.1x server γίνεται με credentials, και τα κλειδιά διανέμονται αυτόματα.

3.7 WPA2 (Wi-Fi Protected Access Version 2)

Το πρωτόκολλο κρυπτογράφησης WPA2 είναι ο διάδοχος του WPA. Αποτελεί μέρος του προτύπου 802.11i. Η κρυπτογράφηση γίνεται με τον αλγόριθμο CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), ο οποίος για την ανάπτυξή του βασίστηκε στο CCM (Counter Mode

with CBC-MAC) του αλγορίθμου AES (Advanced Encryption Standard), για την προστασία της ιδιωτικότητας.



Εικόνα 12: Υλοποίηση WPA2

Με την είσοδο του νέου αλγορίθμου αντικαταστάθηκε ο RC4. Όπως το TKIP, έτσι και ο CCMP χρησιμοποιεί πίνακα αρχικοποίησης 48 bit, αλλά αντί για την ακολουθία αριθμών ανά πακέτο χρησιμοποιεί AES κλειδιά για την προστασία της εμπιστευτικότητας και ακεραιότητας του πακέτου. Χρησιμοποιεί πίνακα αρχικοποίησης 48 bit με 128 bit κλειδί κρυπτογράφησης το οποίο ελαχιστοποιεί την ευπάθεια του συστήματος σε επαναλαμβανόμενες επιθέσεις. Η ενισχυμένη προστασία που παρέχει το CCMP σε σύγκριση με το TKIP απαιτεί μεγαλύτερη επεξεργαστική ισχύ, και συχνά χρειάζεται νέο ή αναβαθμισμένο hardware.

3.8 Τύποι επιθέσεων σε ασύρματα δίκτυα

Τα ασύρματα δίκτυα λόγω του μέσου μετάδοσης είναι ευπαθή σε επιθέσεις. Οι επιθέσεις διενεργούνται για διαφορετικούς σκοπούς, για παράδειγμα, ένας εισβολέας μπορεί απλά να θέλει να ελέγξει την κίνηση ή να αποκτήσει πρόσβαση σε ένα δίκτυο. Επίθεση θεωρείται οποιαδήποτε ενέργεια που εκθέτει την ασφάλεια της πληροφορίας. Υπάρχουν δύο είδη επιθέσεων, οι παθητικές (passive) και οι ενεργητικές (active).

3.8.1 Παθητικές επιθέσεις

Οι παθητικές επιθέσεις είναι εκείνες στις οποίες ο επιτιθέμενος αποκτά πληροφορίες οι οποίες εκπέμπονται από κάποιο access point. Υπάρχουν δύο τύποι παθητικών επιθέσεων:

- Συλλογή πληροφοριών (traffic analysis)
- Συλλογή πακέτων (packet sniffing)

Οι επιθέσεις traffic analysis είναι εκείνες στις οποίες ο επιτιθέμενος αποκτά πληροφορίες οι οποίες προέρχονται από τα access points, επομένως γνωρίζει το όνομα του δικτύου, το κανάλι εκπομπής, την μέθοδο κρυπτογράφησης, και τις MAC διευθύνσεις των συμμετεχόντων.

Οι επιθέσεις συλλογής πακέτων λειτουργούν πανομοιότυπα με τις επιθέσεις traffic analysis, καθώς και εδώ αποκαλύπτονται πληροφορίες του δικτύου. Επιπλέον, ο επιτιθέμενος έχει πρόσβαση και διαβάζει το περιεχόμενο των μηνυμάτων. Αν το μήνυμα είναι κρυπτογραφημένο, ο επιτιθέμενος πρέπει να το αποκρυπτογραφήσει πρώτα. Εκτός από το διάβασμα της πληροφορίας, γίνονται γνωστά περισσότερα χαρακτηριστικά του πακέτου.

3.8.2 Ενεργητικές επιθέσεις

Οι ενεργητικές επιθέσεις συνεπάγονται τη συμμετοχή του επιτιθέμενου στο δίκτυο και διακρίνονται στις ακόλουθες κατηγορίες:

- Επιθέσεις μη εξουσιοδοτημένης πρόσβασης (Unauthorized Access)
- Επιθέσεις τροποποίησης μηνυμάτων (Man in the Middle Attack)
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service)

Οι επιθέσεις μη εξουσιοδοτημένης πρόσβασης δεν έχουν ως στόχο κάποιον συγκεκριμένο χρήστη, αλλά την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο. Σε κάποιες αρχιτεκτονικές δικτύων όταν ο επιτιθέμενος εισβάλλει σε ένα ασύρματο δίκτυο, αποκτά όλα τα δικαιώματα, ενώ σε άλλες για να έχεις πρόσβαση σε όλες τις δυνατότητες του δικτύου πρέπει να είσαι εξουσιοδοτημένος χρήστης, συνήθως

με την εφαρμογή λιστών πρόσβασης ACL (Access Control Lists). Ωστόσο και ο έλεγχος πρόσβασης μπορεί να παραβιαστεί με την τεχνική της μεταμφίεσης (spoofing). Με την τεχνική αυτή ο επιτιθέμενος αντιγράφει το όνομα του δικτύου και δημιουργεί ένα άλλο με δυνατότερο σήμα, με αποτέλεσμα οι υπολογιστές να συνδέονται στο ψεύτικο δίκτυο μεταδίδοντας όλα τα δεδομένα τους μέσα απ' αυτό.

Οι επιθέσεις τροποποίησης μηνυμάτων έχουν έναν έμμεσο τρόπο για να υποκλέπτουν δεδομένα. Οι οργανισμοί παρόλο που έχουν αναπτύξει μηχανισμούς ασφαλείας όπως το VPN και το IPSec, τα οποία όμως προστατεύουν από άμεσες επιθέσεις. Στην επίθεση Man in the Middle, ο επιτιθέμενος βρίσκεται στη μέση της συνομιλίας και εμφανίζεται στο access point ως χρήστης και στον χρήστη ως το access point. Ως αποτέλεσμα τα δεδομένα περνάνε πρώτα από τον επιτιθέμενο.

Οι επιθέσεις άρνησης υπηρεσίας είναι η πιο διαδεδομένη επίθεση για να αχρηστευτεί το ασύρματο δίκτυο για κάποιο χρονικό διάστημα. Αυτό μπορεί να επιτευχθεί αποστέλλοντας πολλά πακέτα στο δίκτυο, ώστε όλη η επεξεργαστική ισχύς του access point να καταναλώνεται στην επεξεργασία τους. Μία άλλη μέθοδος για την πραγματοποίηση DoS επιθέσεων είναι να καταληφθεί το φυσικό μέσο με ισχυρά σήματα στο κανάλι λειτουργίας του ώστε να είναι αδύνατη η επικοινωνία μεταξύ των σταθμών. Οι πέντε πιο σημαντικοί τύποι DoS επιθέσεων είναι η επίθεση πλημμύρας (Flood Attack), η επίθεση Ping of Death, η επίθεση SYN, η επίθεση Teardrop και η επίθεση Smurf.

ΚΕΦΑΛΑΙΟ 4

Παραβιάζοντας την ασύρματη ασφάλεια

4.1 Εισαγωγή στο Linux

Η ονομασία Linux, είναι ένας γενικός όρος αναφοράς σε λειτουργικά συστήματα που βασίζονται στον πυρήνα Linux. Η αρχιτεκτονική του Linux είναι παρόμοια με αυτή του λειτουργικού Unix αλλά έχει αναπτυχθεί εκ του μηδενός και δεν περιλαμβάνει κώδικα από το Unix. Η ανάπτυξη του είναι χαρακτηριστικό παράδειγμα εθελοντικής συνεργασίας από διαδικτυακές κοινότητες, ενώ όλο το έργο είναι ανοικτού κώδικα και ελεύθερα προσβάσιμο από όλους για αντιγραφή, τροποποίηση ή αναδιανομή χωρίς περιορισμό. Μπορεί να εγκατασταθεί και να λειτουργήσει σε μεγάλη ποικιλία υπολογιστικών συστημάτων, από μικρές συσκευές όπως κινητά τηλέφωνα μέχρι μεγάλα υπολογιστικά συστήματα και υπερυπολογιστές. Κυκλοφορεί σε διανομές Linux, δηλαδή ο πυρήνας σε συνδυασμό με συνοδευτικά προγράμματα, όπως βιβλιοθήκες, εργαλεία συστήματος, παραθυρικό περιβάλλον εργασίας και πολλές άλλες εφαρμογές που απαιτούνται για την εύρυθμη λειτουργία ενός υπολογιστή. Χαρακτηριστικό των διανομών είναι η μεγάλη δυνατότητα παραμετροποίησης και επιλογής που προσφέρουν καθώς κάθε μια απευθύνεται σε διαφορετικό τύπο χρηστών.

4.2 Η διανομή BackTrack

Η διανομή BackTrack προήλθε από διάφορες παραλλαγές. Το WHAX, μια διανομή σχεδιασμένη για εργασίες ασφάλειας, παράχθηκε από το Whoppix, το οποίο ήταν βασισμένο στο Knoppix. Όταν το Whoppix έφτασε στην έκδοση 3.0 το όνομα του άλλαξε σε WHAX. Το Auditor Security Collection ήταν ένα Live CD βασισμένο στο Knoppix και είχε διάφορα εργαλεία για την ασφάλεια συστημάτων. Μετά τη συγχώνευση των δύο προήλθε το BackTrack. Απευθύνεται κυρίως στα άτομα που θέλουν να δοκιμάσουν την ασφάλεια ενός συστήματος. Η διανομή του σε Live CD και Live USB δίνει την άμεση δυνατότητα εκκίνησης

του BackTrack χωρίς να χρειάζεται εγκατάσταση. Υπάρχει και η δυνατότητα εγκατάστασης σε σκληρό δίσκο.

Μερικά από τα κύρια εργαλεία του BackTrack είναι:

- Kismet
- Δυνατότητα RFMON στις ασύρματες κάρτες δικτύου 802.11
- Metasploit
- Nmap
- Ettercap
- Wireshark

Τα εργαλεία του BackTrack κατατάσσονται στις ακόλουθες κατηγορίες:

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Web Application Analysis
- Radio Network Analysis (802.11, Bluetooth, Rfid)
- Penetration (Exploit & Social Engineering Toolkit)
- Privilege Escalation
- Maintaining Access
- Digital Forensics
- Reverse Engineering
- Voice Over IP

4.3 Kismet

Το Kismet είναι ένα πρόγραμμα ηλεκτρονικού υπολογιστή, προεγκατεστημένο στην διανομή BackTrack. Μπορεί να εντοπίζει δίκτυα (network detector), να υποκλέπτει πακέτα (packet sniffer) και επίσης μπορεί να εντοπίζει επιθέσεις σε 802.11 WLAN δίκτυα. Το Kismet δουλεύει με όλες τις ασύρματες κάρτες που υποστηρίζουν monitor mode, και μπορεί να ανιχνεύσει δίκτυα 802.11a, 802.11b,

802.11g. Εργάζεται στο στρώμα ζεύξης δεδομένων (Data lank layer) του μοντέλου OSI.

4.4 Wardriving

Ο όρος «Wardriving» περιγράφει την πρακτική εκείνη κατά την οποία ένας χρήστης περιπλανιέται στους δρόμους συνοικιών, εφοδιασμένος με συσκευή που έχει δυνατότητα ασύρματης πρόσβασης με σκοπό να εντοπίσει ασύρματα δίκτυα πρόσβασης και να χαρτογραφήσει την ύπαρξή τους για στατιστικούς ή άλλους λόγους. Πήρε την ονομασία του κατά παράφραση μίας συνήθους πρακτικής στη δεκαετία του 1980 γνωστής ως «Wardialing» κατά την οποία οι δράστες καλούσαν τηλεφωνικούς αριθμούς με σκοπό να εντοπίσουν dial-up modems σε λειτουργία και στη συνέχεια να επιχειρήσουν την παράνομη χρήση αυτών των modems για την παράνομη πρόσβαση των δραστών σε τηλεφωνικά δίκτυα, αλλά αργότερα και στο διαδίκτυο.

Το Wardriving αναφέρθηκε για πρώτη φορά στις ΗΠΑ το 2000, σε μία έρευνα για τα ασύρματα δίκτυα στην πόλη Berkeley της California. Η συγκεκριμένη έρευνα αποσκοπούσε να δείξει τα κενά ασφαλείας των ασύρματων δικτύων που αναπτύσσονταν ραγδαία στο Berkeley, και να προκαλέσει την προσοχή των καθ' ύλη αρμοδίων φορέων για την βελτίωση της ασύρματης τεχνολογίας δικτύων αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων. Η έρευνα απέδειξε ότι είναι δυνατή η πρόσβαση σε ασύρματο δίκτυο, κάνοντας χρήση απλών εργαλείων, ακόμη και σε μεγάλη απόσταση μακριά από το σημείο που είναι τοποθετημένος ο πομπός ασύρματης δικτύωσης. Το Wardriving δεν απαιτεί τη χρήση ακριβού ή δυσεύρετου εξοπλισμού για την διενέργειά του. Μπορεί να γίνει με χρήση είτε φορητού ηλεκτρονικού υπολογιστή είτε κινητού τηλεφώνου (smartphone).

4.5 Εξοπλισμός

Για τέτοιου είδους επιθέσεις χρησιμοποιούνται συγκεκριμένα εργαλεία όπως μία συμβατή κάρτα δικτύου, η οποία θα υποστηρίζει τις μεθόδους που θα χρησιμοποιηθούν, το BackTrack, μία εξωτερική κεραία, gps receiver για να

λαμβάνει την ακριβή γεωγραφική θέση του πομπού και ένα ασύρματο δίκτυο που θα χρησιμοποιεί WPA/WPA2 κρυπτογράφηση. Πιο συγκεκριμένα, για την επίθεση χρησιμοποιήθηκαν:

- Υπολογιστές

Χρησιμοποιήθηκαν δύο φορητοί υπολογιστές για την προσομοίωση της επίθεσης. Ο πρώτος είναι μάρκας Dell, Latitude D820, ο οποίος με τη χρήση εξωτερικής κεραίας και του gps receiver κατάφερε να σαρώσει τα ασύρματα δίκτυα από συνοικίες της πόλης των Αθηνών και να καταγράψει την γεωγραφική θέση του κάθε πομπού. Χρησιμοποιώντας την ενσωματωμένη ασύρματη κάρτα δικτύου που διαθέτει πραγματοποιήθηκαν οι επιθέσεις.

Ο δεύτερος φορητός υπολογιστής δέχτηκε τις επιθέσεις. Είναι μάρκας HP, Compaq 6530b. Διαθέτει ενσωματωμένη ασύρματη κάρτα δικτύου η οποία υποστηρίζει τα πρότυπα IEEE 802.11b, IEEE 802.11g, IEEE 802.11n και τις μεθόδους κρυπτογράφησης WEP/WPA/WPA2.

- Ασύρματο μέσο πρόσβασης

Το ασύρματο μέσο πρόσβασης που δέχτηκε τις επιθέσεις είναι το μοντέλο Netgear DG834Gv4. Διαθέτει 4 θύρες Ethernet και υποστηρίζει τα πρότυπα IEEE 802.11b και IEEE 802.11g. Για την πραγματοποίηση των επιθέσεων ορίστηκε WPA2 encoding με όνομα ssid «NetFasteR IAD 2 (PSTN)» και κωδικός πρόσβασης «dictionary».

- Gps receiver

Η καταγραφή της γεωγραφικής θέσης γίνεται μέσω ενός δέκτη gps της εταιρείας UniTraQ UD-731, ο οποίος είναι συνδεδεμένος σε μια θύρα USB του φορητού υπολογιστή.

- Εξωτερική κεραία

Τέλος, χρησιμοποιήθηκε η εξωτερική κεραία της Kinamax η οποία έχει πιο ευαίσθητο δέκτη σε σχέση με την ενσωματωμένη ασύρματη κάρτα δικτύου του laptop, με αποτέλεσμα να μπορεί να εντοπίσει περισσότερα δίκτυα.

4.6 Εντοπισμός και καταγραφή ssid

Για τις ανάγκες της συγκεκριμένης διπλωματικής αποφασίσαμε να χαρτογραφήσουμε πυκνοκατοικημένες συνοικίες της πόλης των Αθηνών, αποτυπώνοντας στον χάρτη την διαδρομή και το είδος των ασύρματων δικτύων που εντοπίστηκαν. Η έρευνα πραγματοποιήθηκε στις 26 Ιουλίου 2011, καλύφθηκε μία απόσταση περίπου 30 km και κατεγράφησαν 13693 ασύρματα δίκτυα. Για να εντοπίσουμε και να καταγράψουμε τα ssid των ασύρματων δικτύων πρέπει να επιλέξουμε εκκίνηση του υπολογιστή χρησιμοποιώντας το λειτουργικό σύστημα BackTrack. Πριν την εκτέλεση της εφαρμογής kismet πρέπει να θέσουμε την κάρτα δικτύου σε κατάσταση monitor και να ενεργοποιήσουμε την θύρα usb που έχει τοποθετηθεί το gps receiver. Ανοίγουμε την κονσόλα (terminal) για να εκτελέσουμε το script airmon-ng, το οποίο το χρησιμοποιούμε πριν από τα υπόλοιπα εργαλεία, ώστε να θέσουμε την ασύρματη κάρτα δικτύου σε κατάσταση monitor.

- airmon-ng start wlan0

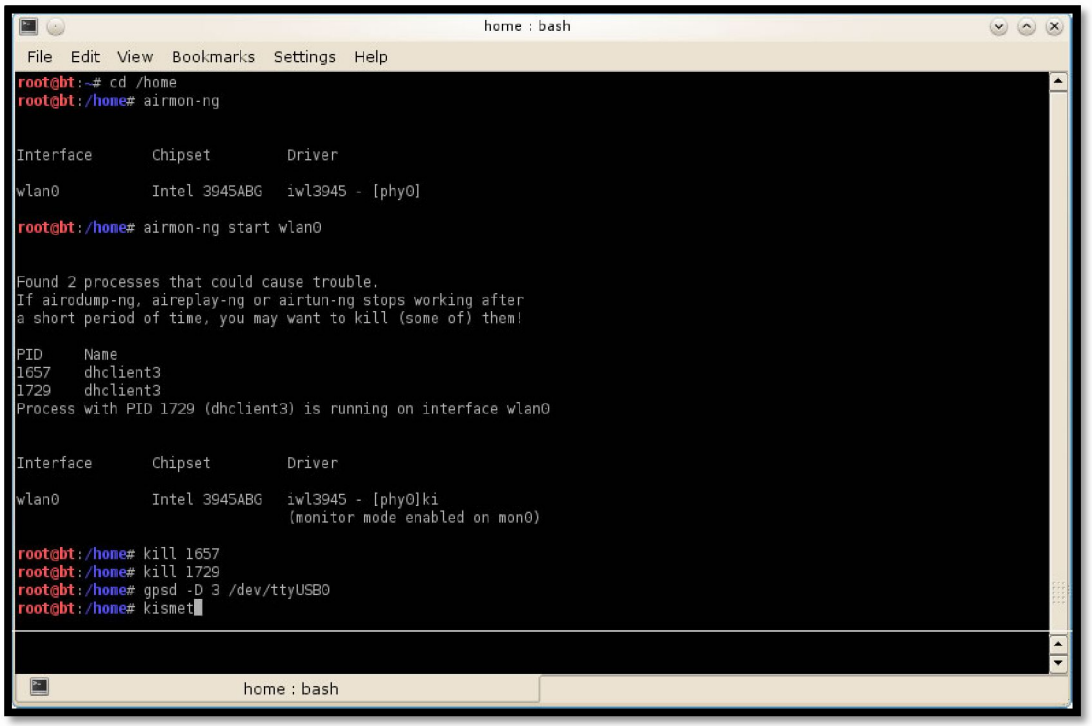
Παράλληλα παρατηρούμε ότι υπάρχουν κάποιες διεργασίες οι οποίες πρέπει να τερματιστούν, διότι μπορεί να προκαλέσουν προβλήματα στην σωστή λειτουργία της εφαρμογής kismet. Με χρήση των παρακάτω εντολών τερματίζονται οι συγκεκριμένες διεργασίες:

- kill 1657
- kill 1729
- ή killall dhclient3

Επιπλέον πρέπει να ενεργοποιήσουμε την θύρα usb που έχει τοποθετηθεί το gps receiver. Η επικοινωνία με αυτή τη συσκευή γίνεται με τη χρήση του gpsd, ο οποίος είναι ένας ανοιχτού κώδικα daemon που συλλέγει πληροφορίες από gps δέκτες. Η ανάγνωση της εξόδου του gpsd πραγματοποιείται με τη χρήση μιας TCP σύνδεσης στη θύρα 2947.

- gpsd –D 3 /dev/tty/USB0

Στη συνέχεια τρέχουμε την εφαρμογή kismet.



Εικόνα 13: Διαδικασία ενεργοποίησης της εφαρμογής kismet

Για τη σωστή λειτουργία του kismet πρέπει να ρυθμιστεί κατάλληλα. Επιλέγουμε ο kismet server να ξεκινήσει αυτόματα και στην επιλογή «Add source» ορίζουμε τα ακόλουθα:

- Intf: wlan0
- Name: localhost
- Opts: -

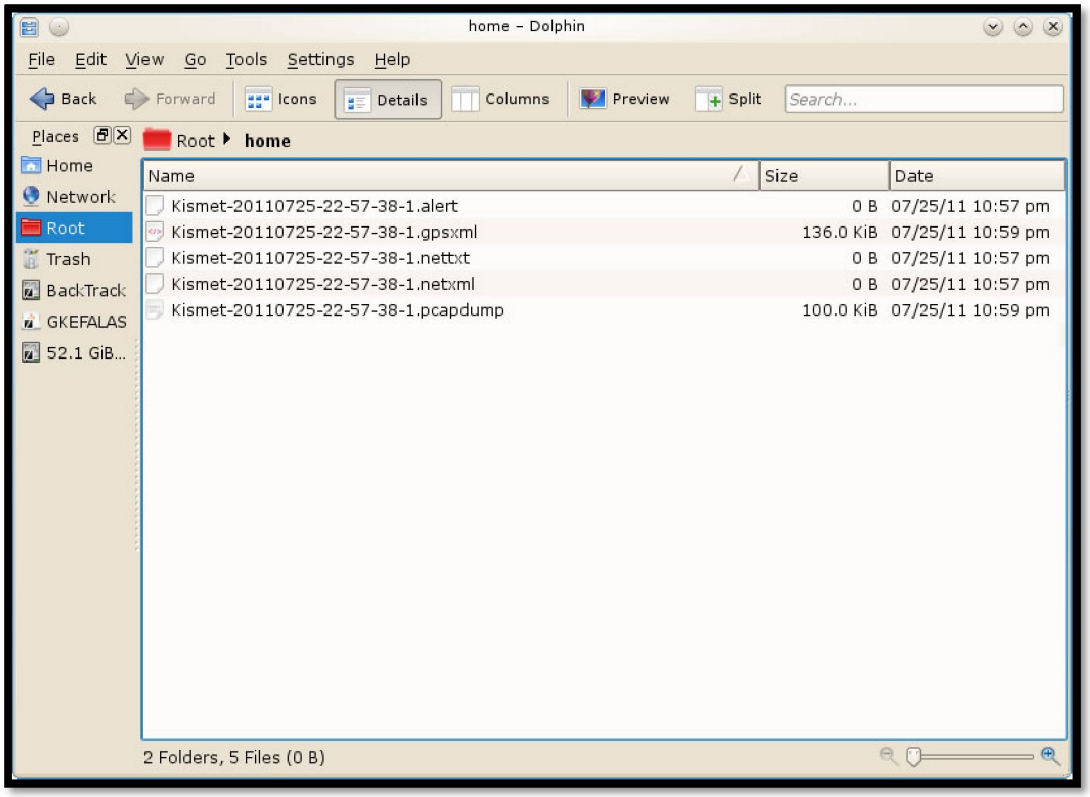
Μόλις δηλωθούν τα παραπάνω στοιχεία το kismet αρχίζει να εντοπίζει και να καταγράφει το essid, το κανάλι που εκπέμπει και την γεωγραφική θέση του κάθε πομπού.

Εικόνα 14: Εντοπισμός και καταγραφή των essid χρησιμοποιώντας το kismet

Κατά τη διάρκεια της σάρωσης δημιουργούνται τα αρχεία που αποθηκεύονται τα δεδομένα. Το βασικό αρχείο αποθήκευσης έχει την κατάληξη netxml. Το συγκεκριμένο αρχείο μπορούμε να το μετατρέψουμε σε kml εκτελώντας τις παρακάτω εντολές:

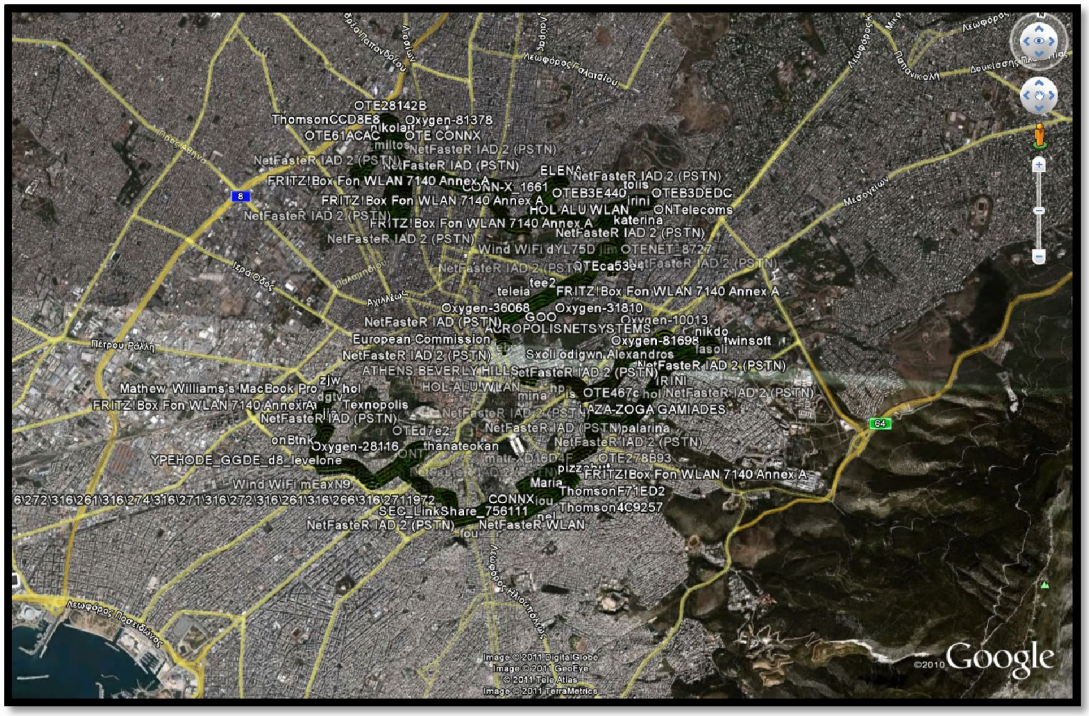
- giakismet –x wardriving.netxml
- giskismet –q ‘select*from wireless’ –o output.kml wardriving.netxml

ώστε να αναπαραστήσουμε χρησιμοποιώντας το google earth τη διαδρομή με όλα τα Access Points που κατεγράφησαν. Επιπλέον μετονομάζοντας το αρχείο από netxml σε xml δημιουργείται το αρχείο που θα χρησιμοποιηθεί στο xml parser.



Εικόνα 15: Τα αποτελέσματα του kismet

Εικόνα 16: Η διαδρομή που ακολουθήθηκε



Εικόνα 17: Η διαδρομή που ακολουθήθηκε με εμφάνιση των ssid

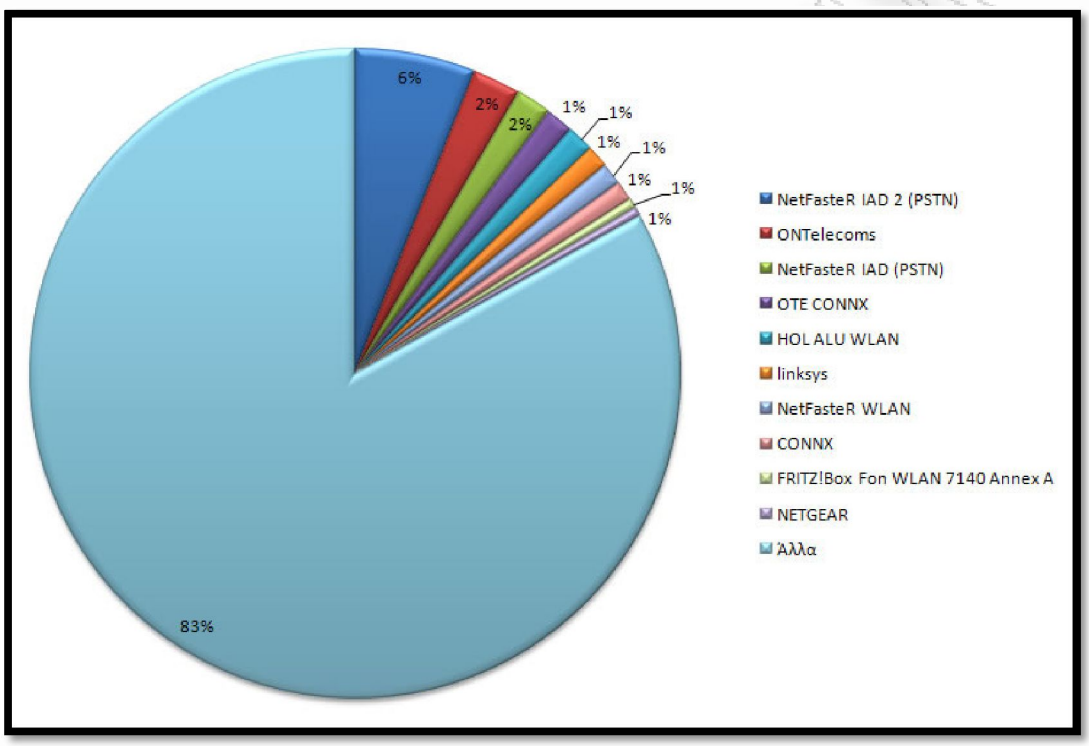
4.7 Xml parser

Για να μπορέσουμε να κάνουμε την ανάλυση των δεδομένων που κατεγράφησαν από το xml αρχείο χρειάστηκε να γραφτεί ένα xml parser σε γλώσσα προγραμματισμού java. Με τη χρήση κατάλληλων java βιβλιοθηκών το xml parser διαβάζει τα tags που χρειάζονται από το αρχείο, τα επεξεργάζεται και εξάγει τα αποτελέσματα σε txt αρχεία. Ο παρακάτω πίνακας περιέχει τα αποτελέσματα για τα δέκα πιο συχνά χρησιμοποιούμενα ssid που προέκυψαν από την ανάλυση του xml.

A/A	ssid	Σύνολο
1	NetFasteR IAD 2 (PSTN)	856
2	ONTelecoms	337
3	NetFasteR IAD (PSTN)	246
4	OTE CONNX	195
5	HOL ALU WLAN	194
6	linksys	158
7	NetFasteR WLAN	154
8	CONNX	138

9	FRITZ!Box Fon WLAN 7140 Annex A	70
10	NETGEAR	62

Πίνακας 2: Αποτελέσματα των 10 δημοφιλέστερων ssid

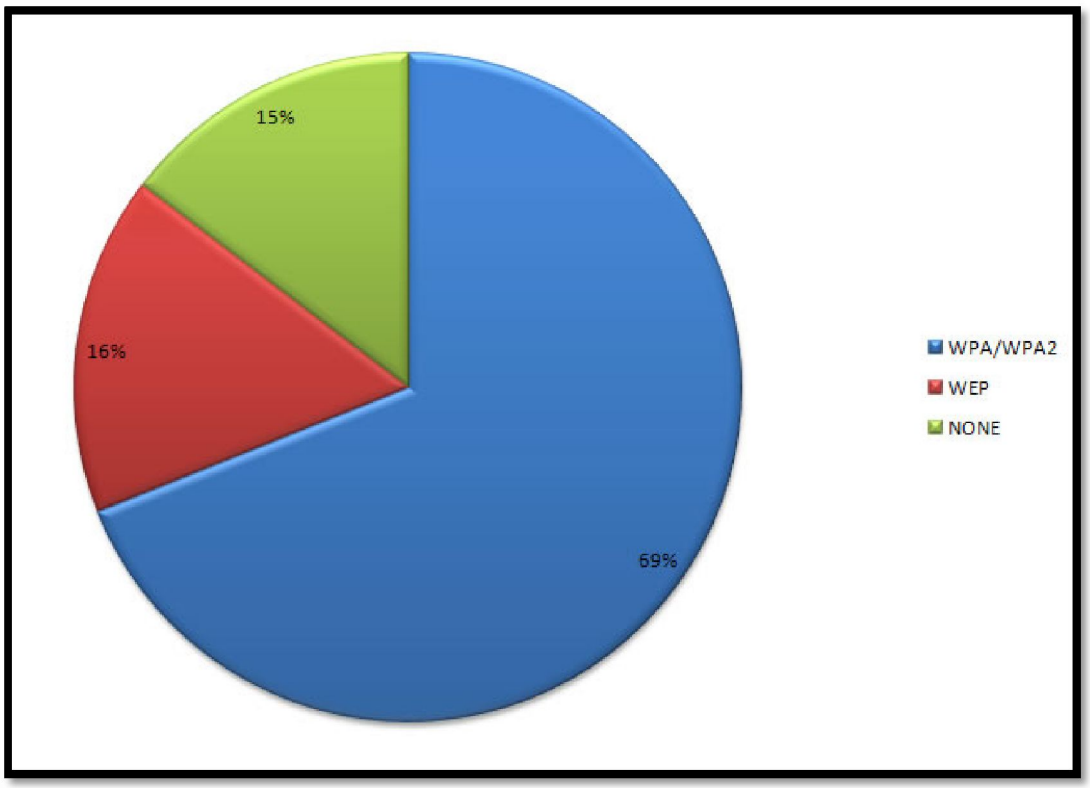


Εικόνα 18: Ποσοστιαία κατανομή των δημοφιλέστερων ssid

Ένα ακόμη ενδιαφέρον στατιστικό στοιχείο είναι το είδος της κωδικοποίησης που χρησιμοποιούν οι χρήστες. Αναλύοντας τα δεδομένα του xml παρατηρούμε ότι 7 στους 10 χρήστες ασύρματων δικτύων χρησιμοποιούν κρυπτογράφηση WPA ή WPA2, το 16% χρησιμοποιεί το τελείως ανασφαλές WEP, ενώ το 15% των χρηστών δεν χρησιμοποιεί κανενός είδους κωδικοποίηση. Στον ακόλουθο πίνακα εμφανίζονται τα αποτελέσματα της συνολικής κατανομής των πρωτοκόλλων ασφαλείας, ενώ στην παρακάτω εικόνα παρουσιάζεται σε γράφημα το ποσοστό κατανομής των πρωτοκόλλων ασφαλείας.

Πρωτόκολλο ασφαλείας	**Σύνολο**
WPA/WPA2	9441
WEP	2246
None	2006

Πίνακας 3: Αποτελέσματα συνολικής κατανομής των πρωτοκόλλων ασφαλείας

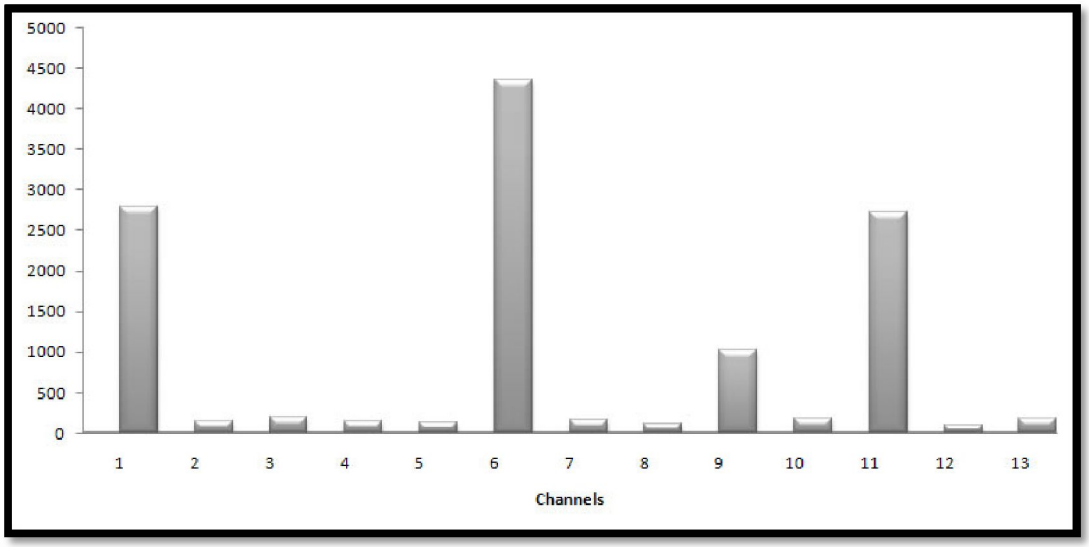


Εικόνα 19: Ποσοστιαία κατανομή των πρωτοκόλλων ασφαλείας

Τα ασύρματα δίκτυα στη ζώνη συχνοτήτων 2.4 GHz υλοποιούν 13 διαφορετικά κανάλια με πλάτος 22 MHz το καθένα. Όπως φαίνεται από την ανάλυση του xml, τα 13 κανάλια επικοινωνίας είναι μερικώς επικαλυπτόμενα ανά 3, δηλαδή το κάθε κανάλι επικαλύπτεται από τα δύο γειτονικά του. Επομένως, ένα ακόμα σημαντικό πρόβλημα είναι η επιλογή του καναλιού του ασύρματου δικτύου. Η ανάλυση των καναλιών έδειξε ότι η συντριπτική πλειοψηφία των δικτύων χρησιμοποιούν συγκεκριμένα κανάλια. Αυτά είναι το κανάλι 1, το κανάλι 6 και το κανάλι 11. Τα υπόλοιπα κανάλια παραμένουν ουσιαστικά αχρησιμοποίητα. Αυτό συνεπάγεται πτώση αποδοτικότητας του δικτύου, αύξηση λαθών και επανεκπομπών, ακόμη και απώλεια αξιοπιστίας δεδομένων.

Channel	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Σύνολο	2798	147	193	144	132	4362	176	116	1025	176	2733	100	181

Πίνακας 4: Κατανομή συχνοτήτων ασύρματων δικτύων

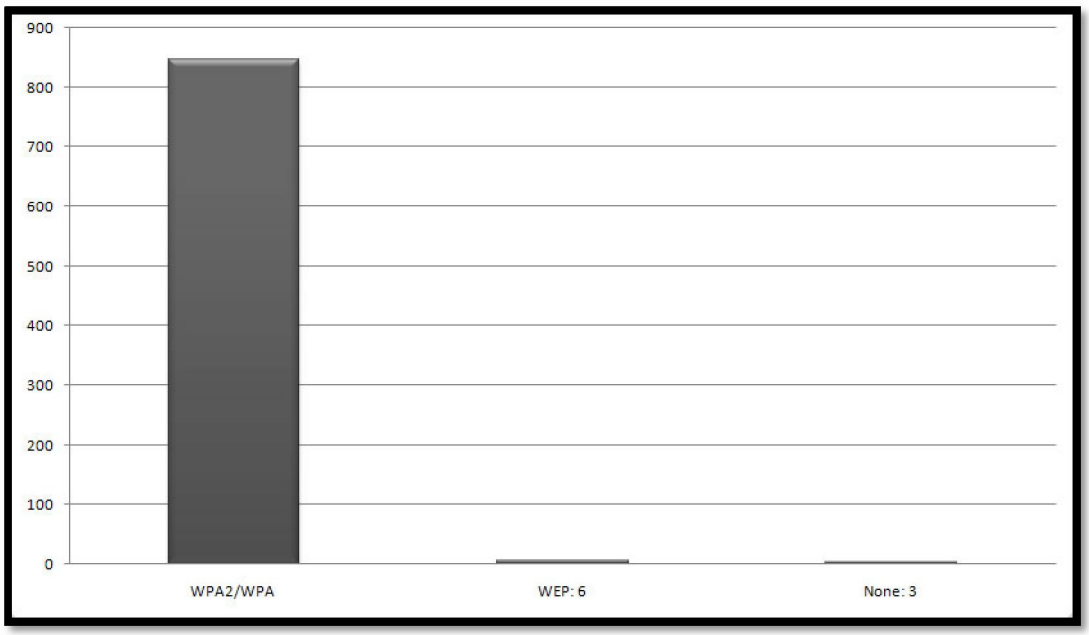


Εικόνα 20: Κατανομή συχνοτήτων ασύρματων δικτύων

Τα τελευταία χρόνια όλοι οι πάροχοι και οι κατασκευαστές ασύρματων συσκευών παρέχουν ασύρματες συσκευές με προρυθμισμένο το πρωτόκολλο WPA/WPA2. Οι συσκευές στέλνονται στον τελικό χρήστη με εργοστασιακές ρυθμίσεις και το κυριότερο εξατομικευμένες. Αυτό σημαίνει ότι η κάθε συσκευή έχει υλοποιημένο το πρωτόκολλο WPA/WPA2 με δικό του διαφορετικό κωδικό εισόδου. Επιλέγοντας το πιο συχνά χρησιμοποιούμενο ssid, το NetFasteR IAD 2 (PSTN), και αναλύοντας την κωδικοποίηση που χρησιμοποιεί η ασύρματη συσκευή, παρατηρούμε ότι οι περισσότεροι χρήστες επιλέγουν WPA/WPA2 κωδικοποίηση.

Πρωτόκολλο ασφαλείας	**Σύνολο**
WPA/WPA2	847
WEP	6
None	3

Πίνακας 5: Κατανομή των πρωτοκόλλων ασφαλείας ανά ssid



Εικόνα 21: Κατανομή των πρωτοκόλλων ασφαλείας ανά ssid

4.8 Προετοιμασία επίθεσης

Στις WPA/WPA2 επιθέσεις ο χρήστης εισάγει μία λέξη-κλειδί, η οποία όμως δεν χρησιμοποιείται στην αποστολή των κωδικοποιημένων πακέτων, αλλά συνδυάζεται με την MAC Address του κάθε σταθμού-πελάτη και με βάση τον πίνακα αρχικοποίησης μήκους 48-bit, παράγει το κλειδί με το οποίο πραγματοποιείται η κωδικοποίηση των δεδομένων. Επομένως, το κωδικό κλειδί στα εκπεμπόμενα πακέτα είναι διαφορετικό ανά συσκευή. Ο επιτιθέμενος θα προσπαθήσει να παραβιάσει το ασύρματο δίκτυο όταν ένας σταθμός ζητήσει να συνδεθεί με τον σταθμό βάσης (handshake), διότι τα συγκεκριμένα πακέτα περιέχουν οπωσδήποτε την μυστική λέξη-κλειδί, που έχει οριστεί ως συνθηματικό ταυτοποίησης και εισόδου στο δίκτυο.

Ο επιτιθέμενος κάνοντας χρήση εξειδικευμένων εφαρμογών θα προσπαθήσει να εντοπίσει τους χρήστες που είναι συνδεδεμένοι σε ένα ασύρματο δίκτυο, συλλέγοντας τα απαραίτητα πακέτα. Για τη λήψη του πακέτου αυτό, ο επιτιθέμενος έχει δύο επιλογές:

- Είτε περιμένοντας κάποιον χρήστη να συνδεθεί επιτυχημένα σε κάποιο access point.

- Είτε να προκαλέσει αποσύνδεση στον ήδη συνδεδεμένο χρήστη, ώστε αναγκαστικά να προσπαθήσει να επανασυνδεθεί, δημιουργώντας νέα πακέτα «handshake».

Αφού ληφθεί το πακέτο «handshake» (που περιέχει το μυστικό κλειδί), θα αναλυθεί από εφαρμογές που εκτελούν επιθέσεις λεξικού (dictionary attacks). Θα πραγματοποιηθούν εξαντλητικές δοκιμές διάφορων λέξεων-κλειδιών, με συνδυασμούς γραμμάτων, αριθμών και συμβόλων, προσπαθώντας ουσιαστικά να ανακαλύψουμε το σωστό μυστικό κλειδί. Είναι προφανές ότι η επιτυχής έκβαση της συγκεκριμένης τεχνικής εξαρτάται αποκλειστικά από την «ποιότητα» του «λεξικού» που χρησιμοποιείται.

4.9 Dictionary attack

Η επίθεση λεξικού είναι μια μέθοδος για να παραβιαστεί ένα ασύρματο δίκτυο. Είναι πολύ αποτελεσματική και γρήγορη διότι πολλοί χρήστες ηλεκτρονικών υπολογιστών και επιχειρήσεις επιμένουν στη χρησιμοποίηση κοινών λέξεων για κωδικούς πρόσβασης. Συνήθως όλοι οι δυνατοί συνδυασμοί λέξεων 8 χαρακτήρων εμπεριέχονται σε τέτοια λεξικά. Αποδεικνύεται ότι λέξεις μήκους μικρότερου από 20 χαρακτήρες, είναι στατιστικά αδύνατον να αντέξουν σε τέτοιου είδους επίθεση. Οι επιθέσεις λεξικού είναι σπανίως επιτυχημένες κατά των συστημάτων που χρησιμοποιούν πολλές λέξεις-φράσεις, και ανεπιτυχή κατά των συστημάτων που χρησιμοποιούν τυχαίους συνδυασμούς κεφαλαίων και πεζών γραμμάτων και περιέχουν αριθμούς και σύμβολα. Σε αυτά τα συστήματα, η μέθοδος επίθεσης brute-force, μπορεί μερικές φορές να είναι πιο αποτελεσματική, αν και είναι περισσότερο χρονοβόρα.

4.10 Pre-computed hashes

Τα pre-computed hashes είναι αρχεία (αρκετά μεγάλου μεγέθους) τα οποία περιέχουν προϋπολογισμένα hashes, για μια σειρά κωδικών. Η ουσία είναι πως με αυτά τα αρχεία μειώνεται πολύ ο χρόνος του dictionary attack αφού ο υπολογισμός του hash για κάθε κωδικό έχει γίνει, και μένει να συγκριθεί με αυτό που έχει γίνει capture.

Στο WPA, το hash προκύπτει από τον κωδικό που έχει επιλεχθεί σε συνδυασμό με το ssid. Οπότε τα hashes που έχουν υπολογισθεί στα αρχεία αυτά ισχύουν για συγκεκριμένα ssid, τα οποία είναι αυτά που χρησιμοποιούνται συνήθως από προεπιλογή (π.χ. linksys, netgear).

4.11 Εισαγωγή στη σουίτα aircrack-ng

Το aircrack-ng είναι μια σουίτα η οποία περιλαμβάνει εργαλεία που μας βοηθούν να επαναφέρουμε το κλειδί που χρησιμοποιείται από ένα ασύρματο Access Point ώστε να κρυπτογραφήσει τα δεδομένα που διακινούνται στο δίκτυο. Επίσης, μας βοηθάει στον έλεγχο της ασφάλειας του δικτύου μας καθώς μπορούμε να ελέγξουμε κατά πόσο το κλειδί που έχουμε χρησιμοποιήσει μας μπορεί να εντοπιστεί. Τα βασικά εργαλεία που περιλαμβάνει η σουίτα aircrack-ng είναι:

- airmon-ng
- airodump-ng
- aireplay-ng
- aircrack-ng
- airolib-ng

4.11.1 airmon-ng

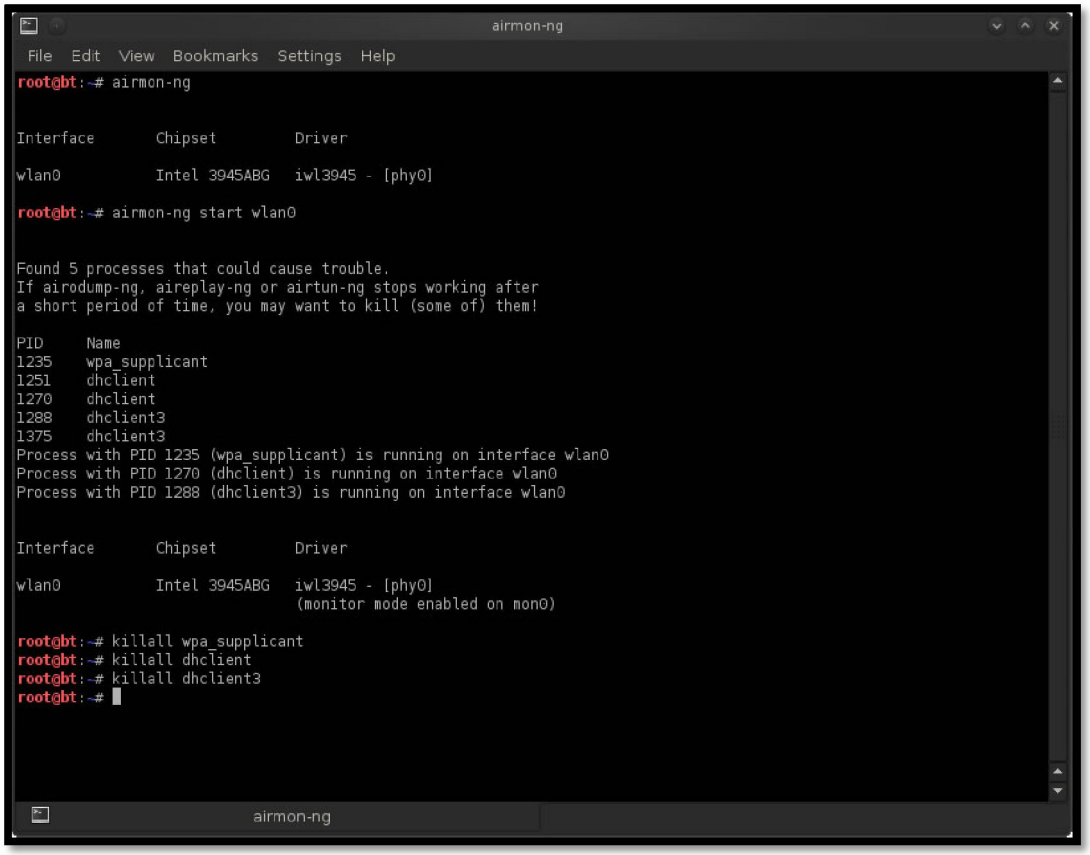
Όπως αναφέρθηκε το airmon-ng το χρησιμοποιούμε για να θέσουμε την κάρτα δικτύου μας σε monitor mode.

Χρήση

- airmon-ng {start|stop} {interface}

Το start|stop προσδιορίζει αν θα ενεργοποιήσουμε ή αν θα απενεργοποιήσουμε την κατάσταση monitor της ασύρματης κάρτας μας.

Το interface προσδιορίζει την κάρτα δικτύου για την οποία θέλουμε να ενεργοποιήσουμε/ απενεργοποιήσουμε την κατάσταση monitor.



Εικόνα 22: Η ασύρματη κάρτα σε κατάσταση monitor

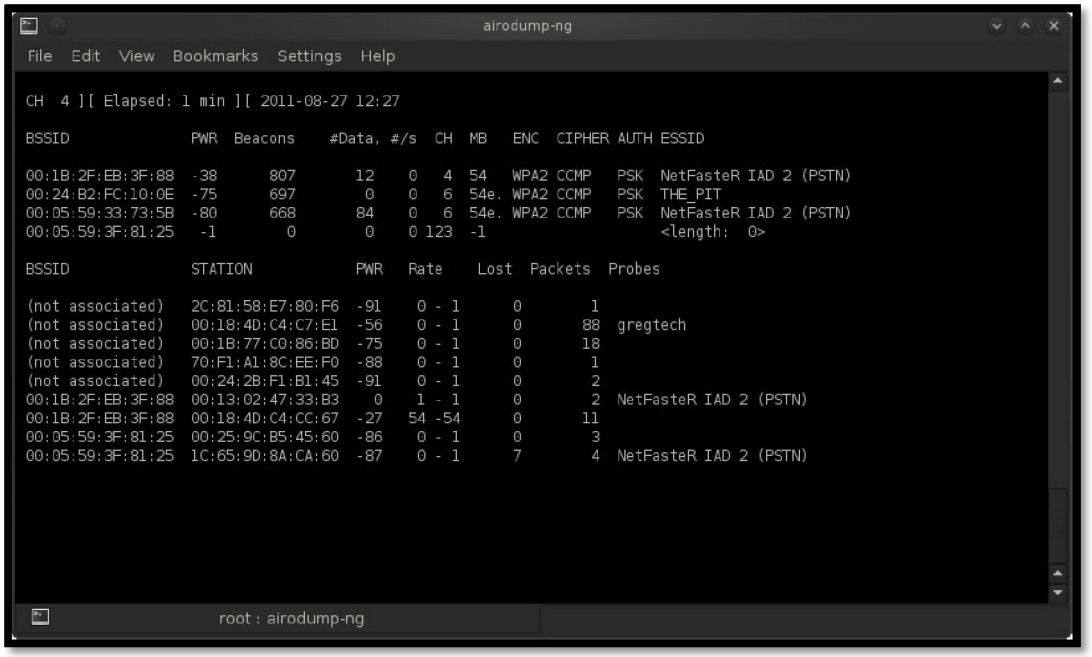
4.11.2 airodump-ng

Το airodump-ng χρησιμοποιείται για την καταγραφή πακέτων από 802.11 δίκτυα και για τη συλλογή των IVs (Initialization Vectors). Επίσης, μπορεί να χρησιμοποιηθεί για τον εντοπισμό των δικτύων 802.11 που βρίσκονται εντός της κάλυψης της κάρτας μας.

Χρήση

- airodump-ng {interface}

Το interface προσδιορίζει την κάρτα δικτύου που θα χρησιμοποιείται ώστε να καταγράφουμε πακέτα.



Εικόνα 23: Συλλογή των IV's

Ας αναλύσουμε λίγο το αποτέλεσμα:

- Στην καρτέλα BSSID εμφανίζεται η MAC address των APs που βρίσκονται εντός της εμβέλειας της κάρτας μας.
- Στην καρτέλα PWR βλέπουμε την ισχύ του σήματος.
- Στην καρτέλα Beacon βλέπουμε τα beacon frames που έχει έχουμε λάβει από κάθε AP.
- Στην καρτέλα #Data βλέπουμε τα πακέτα που έχουμε λάβει από κάθε AP.
- Στην καρτέλα #/s βλέπουμε το ρυθμό με τον οποίο εμείς στέλνουμε πακέτα στο AP.
- Στην καρτέλα CH βλέπουμε το κανάλι στο οποίο λειτουργεί το AP.
- Στην καρτέλα ENC βλέπουμε το είδος της κρυπτογράφησης που χρησιμοποιείται.
- Στην καρτέλα ESSID βλέπουμε το όνομα του δικτύου.

Όταν υπάρχουν συνδεδεμένοι πελάτες στα AP εμφανίζονται κάτω από αυτά τα στοιχεία των πελατών.

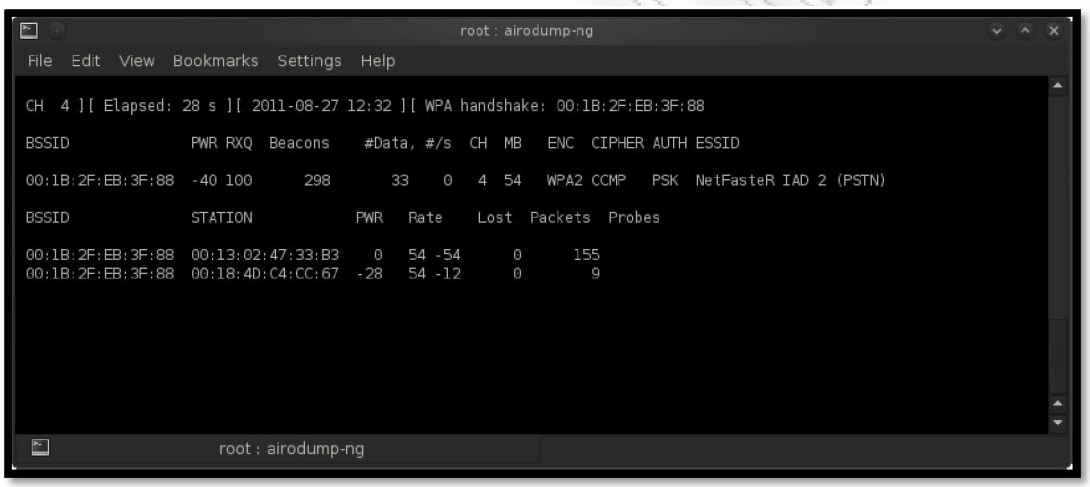
- Κάτω από το BSSID φαίνεται η διεύθυνση του AP στο οποίο είναι συνδεδεμένος ο πελάτης.
- Κάτω από το Station φαίνεται η διεύθυνση MAC του πελάτη.

- Κάτω από το Packets φαίνεται ο αριθμός των πακέτων που έχουν καταγραφεί και προορίζονται για τον συγκεκριμένο πελάτη.

Για να λάβουμε γρηγορότερα τα πακέτα που στέλνει ο AP που μας ενδιαφέρει, και να καταγράψουμε τα πακέτα που θα κάνουμε inject πρέπει να επικεντρωθούμε στον συγκεκριμένο AP.

Χρήση

- airodump-ng --channel 4 --write netfaster --bssid 00:1B:2F:EB:3F:88 mon0



Εικόνα 24: «Σύλληψη» του πακέτου handshake

Ας δούμε τις επιλογές που χρησιμοποιούμε:

- -channel: καθορίζει το κανάλι.
- --bssid: καθορίζει τη διεύθυνση MAC του AP στόχου.

4.11.3 aireplay-ng

Το aireplay-ng χρησιμοποιείται για να κάνουμε inject πακέτα σε κάποιο ασύρματο δίκτυο στόχο. Η κύρια λειτουργία του είναι να δημιουργήσουμε κυκλοφορία πακέτων ώστε να καταγράφουμε πολύ περισσότερα πακέτα από αυτά που ανταλλάσσονται πραγματικά στο δίκτυο. Ωστόσο, μπορεί να χρησιμοποιηθεί ώστε να αναγκάσει κάποιον ασύρματο client να συνδεθεί ή να αποσυνδεθεί από το AP και να εκτελέσει ψεύτικες πιστοποιήσεις ώστε να συνδεθούμε εμείς με το AP στόχο.

Επιθέσεις που υποστηρίζονται:

- Attack 0: Deauthentication (-0)
- Attack 1: Fake authentication (-1)
- Attack 2: Interactive packet replay (-2)
- Attack 3: ARP request replay attack (-3)
- Attack 4: KoreK chopchop attack (-4)
- Attack 5: Fragmentation attack (-5)
- Attack 9: injection test (-9)

Χρήση

- aireplay-ng -0 –death 1 –a *macAddressAP* –c *macAddressClient* mon0

Για deauthentication attack όπου η MAC address του AP είναι: 00:1B:2F:EB:3F:88, και η MAC address του client είναι: 00:13:02:47:33:B3 εκτελούμε:

- aireplay-ng --death 1 -a 00:1B:2F:EB:3F:88 -c 00:13:02:47:33:B3 mon0

Ας δούμε τις επιλογές:

- -deauth στέλνει 1 πακέτο deauthentication.
- -a η MAC address του AP.
- -c η MAC address του client.

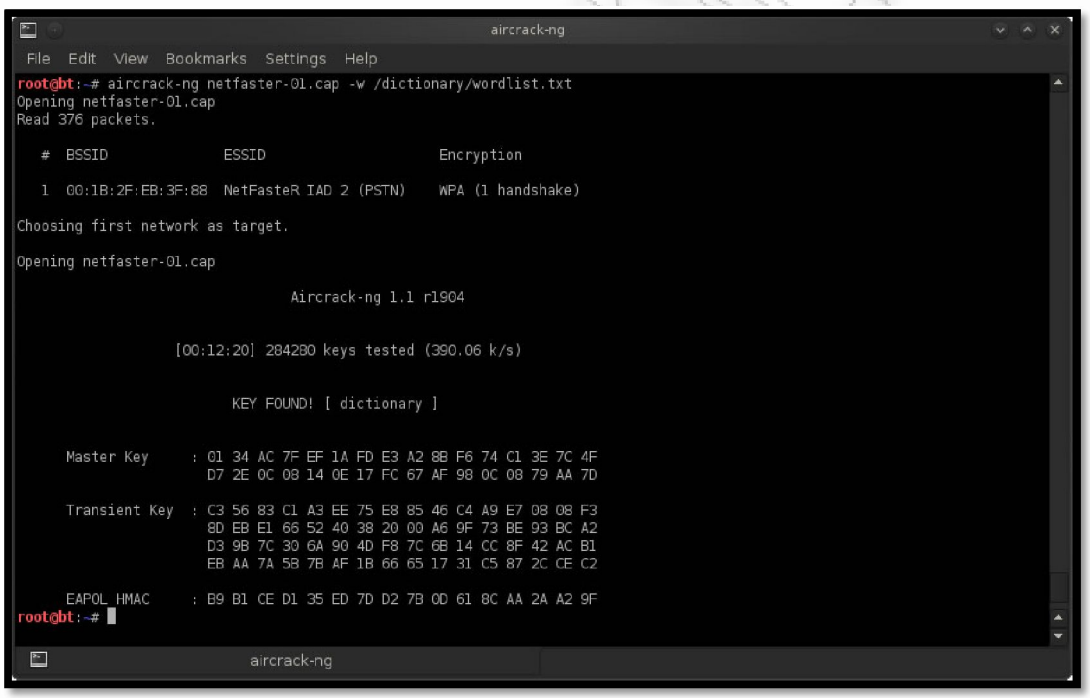
Εικόνα 25: Η εντολή aireplay-ng

4.11.4 aircrack-ng

Το aircrack-ng είναι το εργαλείο που χρησιμοποιούμε για να σπάσουμε το κλειδί κρυπτογράφησης ενός AP. Όπως και τα περισσότερα εργαλεία επιθέσεων χρησιμοποιούν το αρχείο καταγραφής των IV's και ένα λεξικό επιθέσεων.

Χρήση

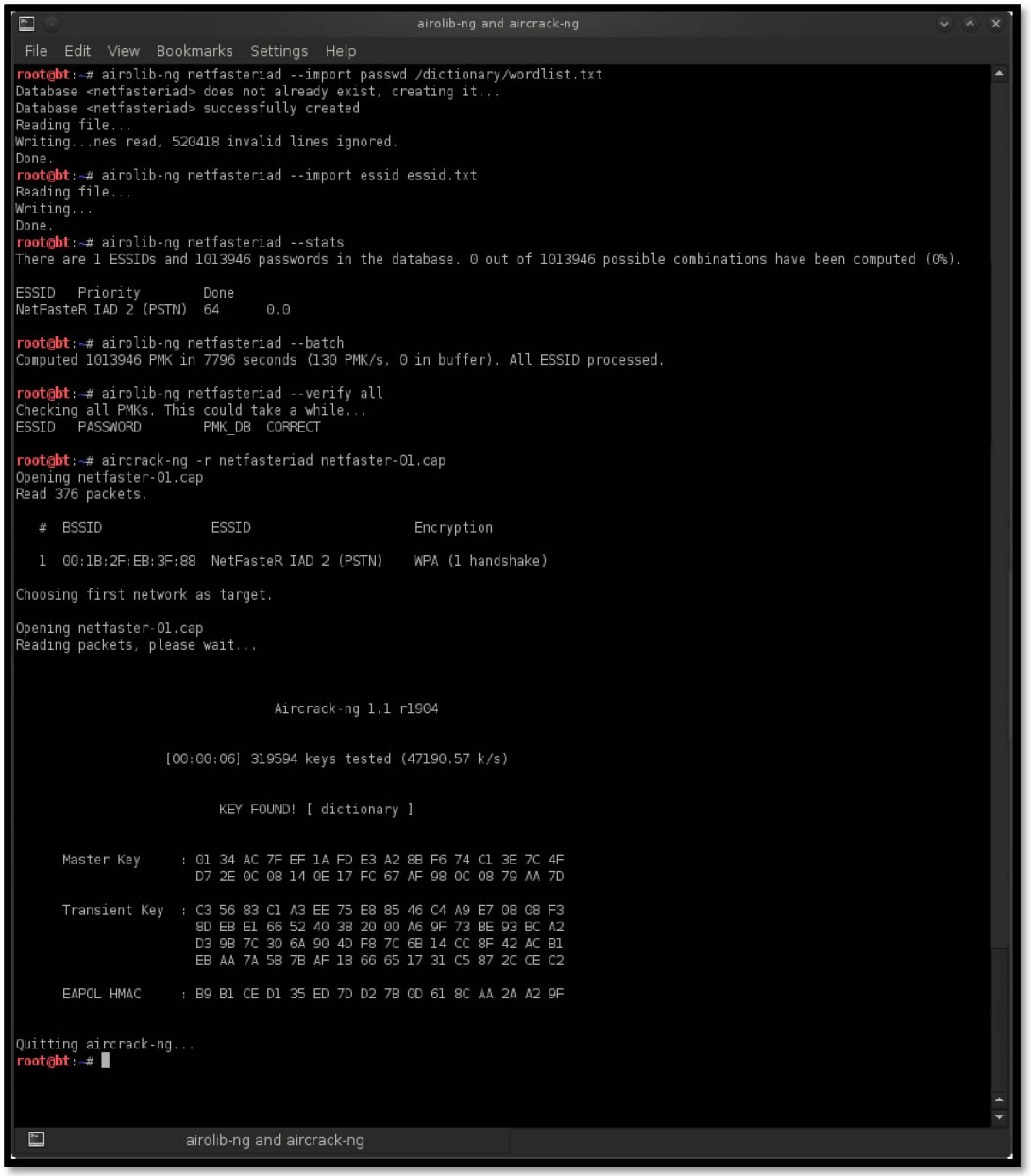
- aircrack-ng [input] {capture file(s)}
- aircrack-ng netfaster-01.cap –w /dictionary/wordlist.txt



Εικόνα 26: Η παραβίαση της κρυπτογράφησης

4.12 airolib-ng και aircrack-ng

Το airolib-ng το χρησιμοποιούμε για να αποθηκεύουμε και να διαχειριζόμαστε τις λίστες των essid, των password και να υπολογίζουμε τα Pairwise Master Keys (PMKs). Το πρόγραμμα χρησιμοποιεί την βάση δεδομένων SQLite3 η οποία διατίθεται για πολλές πλατφόρμες και κάνει καλύτερη διαχείριση μνήμης και χώρου στο δίσκο. Μας δίνει τη δυνατότητα να προϋπολογίσουμε τα PMK για να τα χρησιμοποιήσουμε κάποια στιγμή στο μέλλον.



Εικόνα 27: Επίθεση στο δίκτυο χρησιμοποιώντας βάση δεδομένων

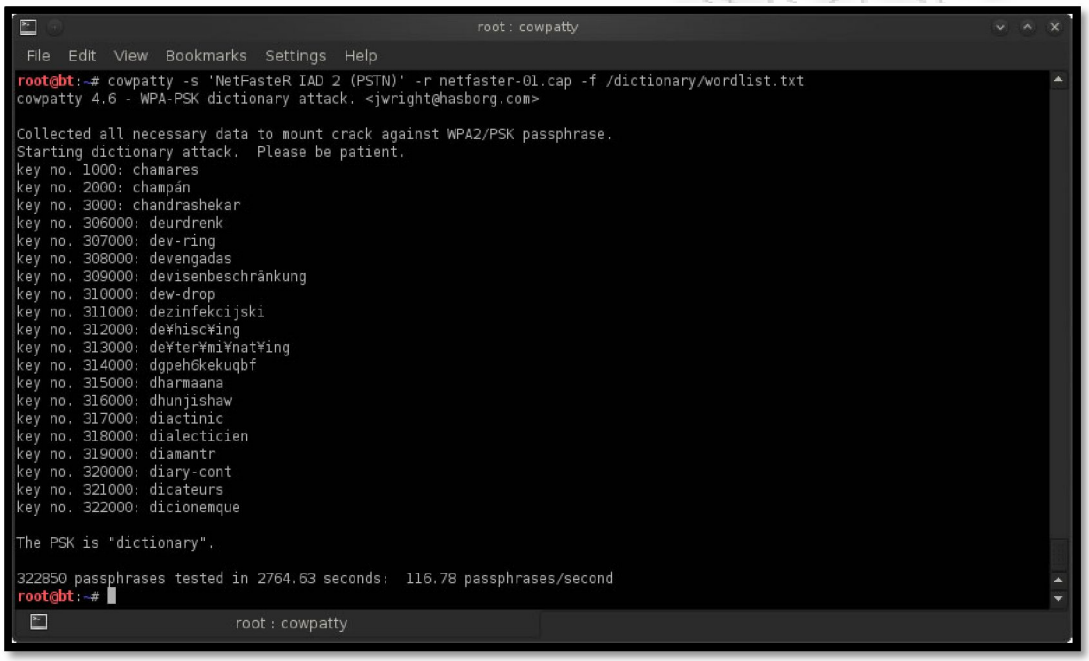
4.13 coWPAtty

Το aircrack-ng είναι ένα ισχυρό εργαλείο, ωστόσο έχει κάποιους περιορισμούς. Ένα πιο ισχυρό εργαλείο επιθέσεων είναι το coWPAtty. Δημιουργήθηκε από τον Joshua Wright και έχει όλα τα χαρακτηριστικά που κάποιος μπορεί να ζητήσει από ένα καλό εργαλείο, καθώς μπορεί να συνδυαστεί με δημοφιλή password cracking εργαλεία, όπως το «John the ripper». Είναι ένα εργαλείο dictionary attack, το οποίο απαιτεί τουλάχιστον τη λήψη τουλάχιστον 2 frames από ένα 4-

way handshake. Για την πραγματοποίηση της επίθεσης του καθορίζουμε το λεξικό της επίθεσης, το ssid του δικτύου και το αρχείο καταγραφής των IV's.

Χρήση

- cowpatty –s 'NetFasteR IAD 2 (PSTN)' –r netfaster-01.cap –f /dictionary/wordlist.txt



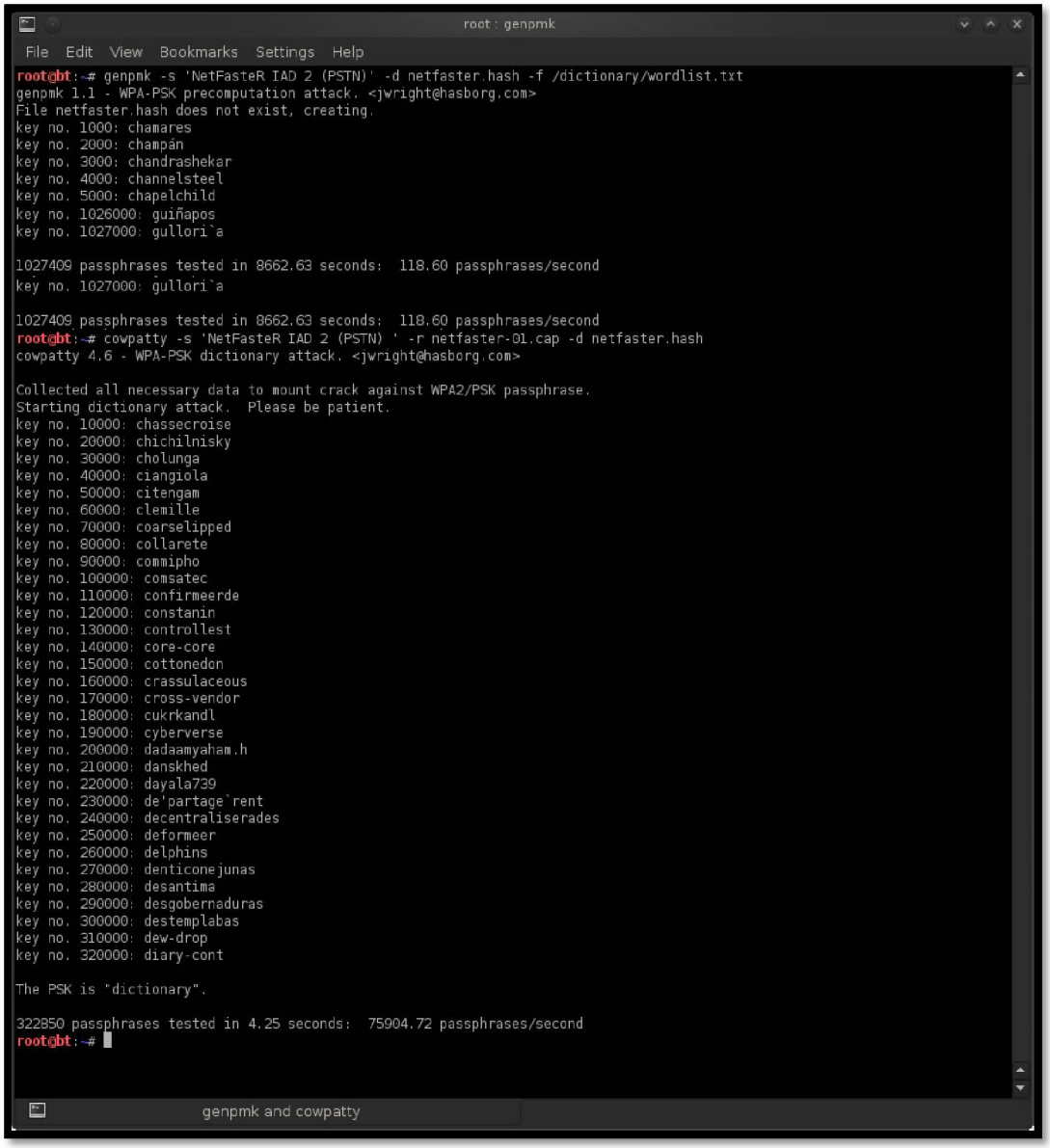
Εικόνα 28: Το εργαλείο coWPAtty

4.14 genpmk και coWPAtty

Η εντολή genpmk χρησιμοποιείται για να δημιουργήσει pre-compute hashes αρχεία. Υπάρχει όμως αλληλεξάρτηση από το ssid του Access Point. Αυτό σημαίνει ότι χρειαζόμαστε διαφορετικά σύνολα hash για κάθε μοναδικό ssid.

Χρήση

- genpmk -s 'NetFasteR IAD 2 (PSTN)' –d netfaster.hash -f /dictionary/wordlist.txt
- cowpatty –s 'NetFasteR IAD 2 (PSTN)' –r netfaster-01.cap -d netfaster.hash



Εικόνα 29: Η Επίθεση στο δίκτυο χρησιμοποιώντας pre-computed hashes

4.15 John the ripper

Πρόκειται για ένα δημοφιλές password cracking εργαλείο το οποίο υποστηρίζει 15 διαφορετικές πλατφόρμες. Μπορεί να σπάσει κρυπτογραφημένες πληροφορίες με DES, MD5, Blowfish, Kerberos AFS, WinNT/2000/XP. Με plugins μπορεί να σπάσει και MD4, LDAP passwords, MySQL. Ανιχνεύει αυτόματα το είδος κρυπτογράφησης απέναντι στο οποίο μπορεί να εφαρμόσει dictionary και brute force attacks.

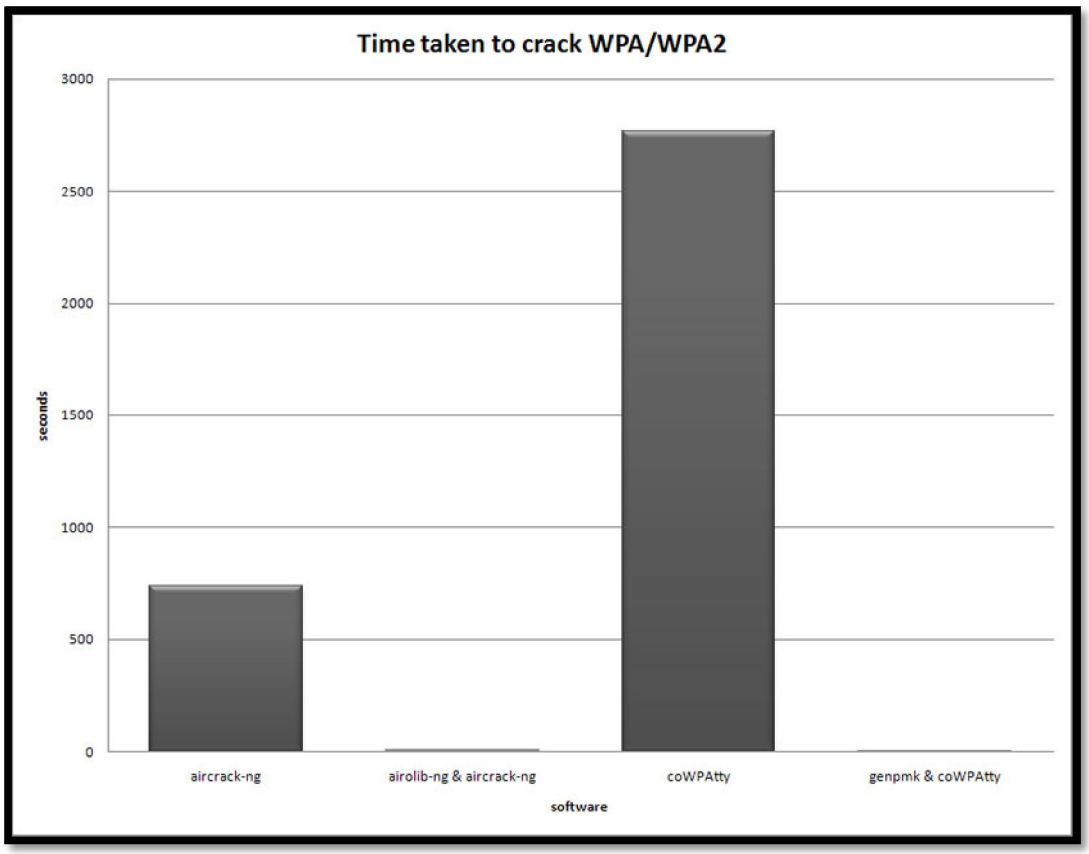
Μια πολύ ενδιαφέρουσα δυνατότητα είναι τα rules του, με τα οποία μπορούμε να αντικαταστήσουμε για παράδειγμα το ο με το 0, το 1 με το ! ή το a με το @. Έτσι θα μπορούσαμε να δώσουμε στο coWPAtty το output ενός dictionary από τον JtR, τα rules του οποίου θα μετατρέψουν τις λέξεις του dictionary.

4.16 Σύγκριση επιθέσεων

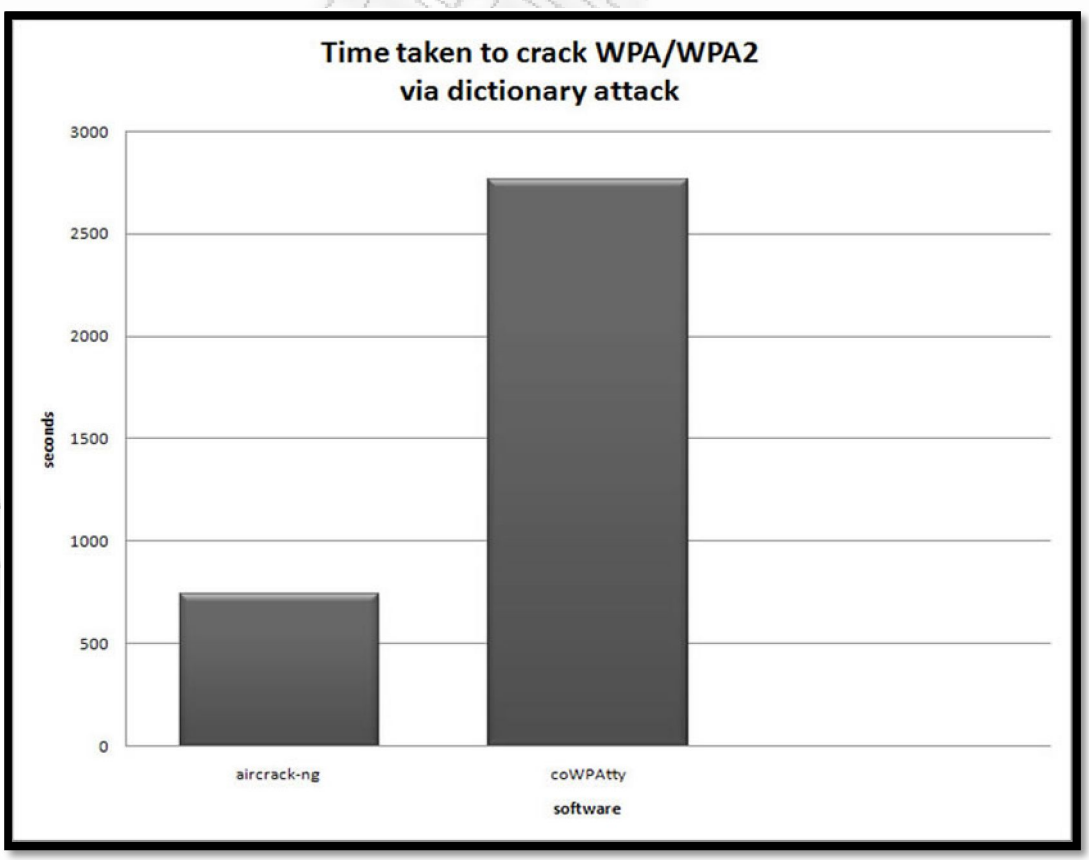
Για την επίθεση στο ασύρματο δίκτυο «NetFasteR IAD 2 (PSTN)» χρησιμοποιήθηκε ένα λεξικό 1534724 λέξεων, μεγέθους 15 MB. Η φράση κλειδί βρίσκεται στην 466600 γραμμή, επομένως το πρόγραμμα για τον υπολογισμό του κλειδιού επεξεργάστηκε το 30% του λεξικού. Στον παρακάτω πίνακα παρατηρούμε τα αποτελέσματα των επιθέσεων. Η εφαρμογή που χρησιμοποιήθηκε για την κάθε επίθεση βρίσκεται στην στήλη software, η στήλη time δείχνει σε δευτερόλεπτα την χρονική διάρκεια την κάθε επίθεσης, η στήλη keys/sec δείχνει τον ρυθμό προσπέλασης του λεξικού και η στήλη pre-calculate time δείχνει σε δευτερόλεπτα την χρονική διάρκεια που χρειάστηκαν τα εργαλεία airolib-ng και genpmk για να δημιουργήσουν τα hash αρχεία.

software	**time (sec)**	**keys/sec**	**pre-calculate time (sec)**
aircrack-ng (dictionary)	740	390,06	-
airolib-ng & aircrack-ng (pre-computed hashes)	6	47190,57	7796
coWPAtty (dictionary)	2764,63	116,78	-
genpmk & coWPAtty (pre-computed hashes)	4,25	75904,72	8662,63

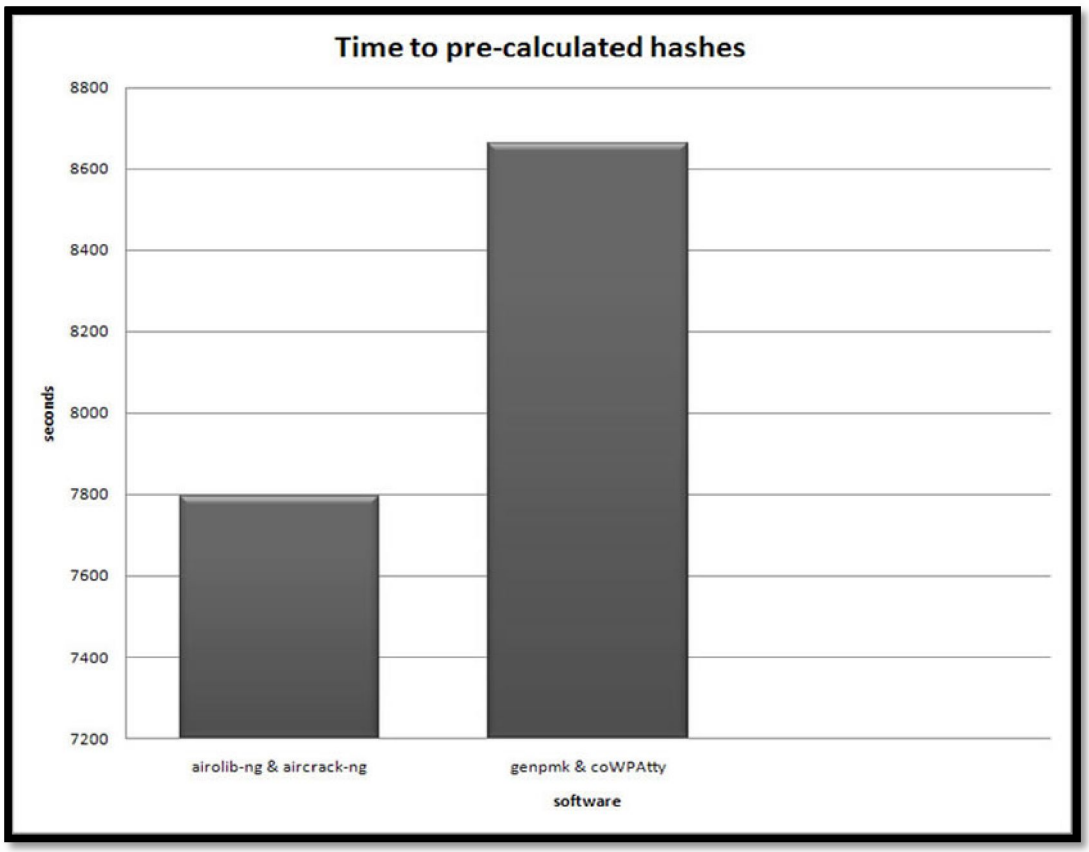
Πίνακας 6: Συγκριτικός πίνακας των αποτελεσμάτων των επιθέσεων



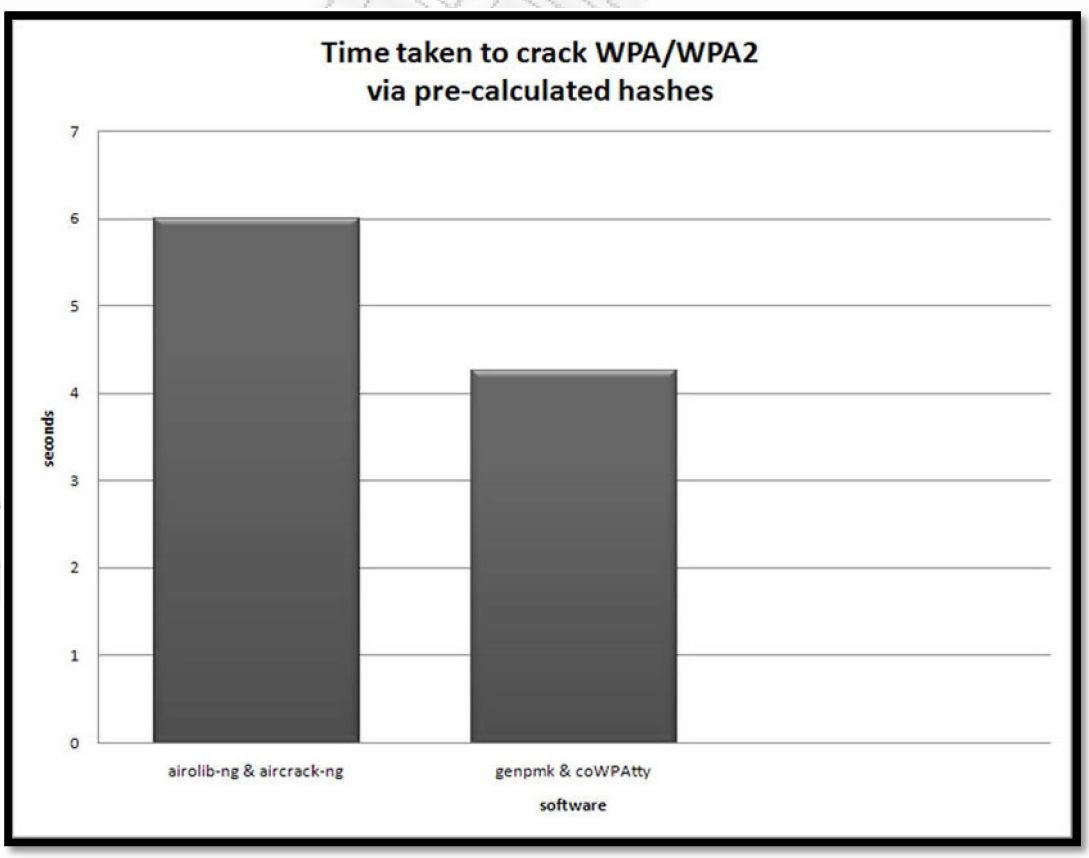
Εικόνα 30: Time taken to crack WPA/WPA2



Εικόνα 31: Time taken to crack WPA/WPA2 via dictionary attack



Εικόνα 32: Time to pre-calculated hashes



Εικόνα 33: Time taken to crack WPA/WPA2 via pre-calculated hashes

Συγκρίνοντας τους χρόνους που χρειάστηκε η κάθε επίθεση για να ολοκληρωθεί παρατηρούμε ότι τον περισσότερο χρόνο χρειάστηκε η εντολή coWPAtty και είναι 2764,63 sec, δηλαδή περίπου 45 min, ενώ η μικρότερη διάρκεια πραγματοποιήθηκε με χρήση hash αρχείου στα μόλις 4,25 sec. Συγκρίνοντας τις επιθέσεις λεξικού παρατηρούμε ότι για την εντολή aircrack-ng ο χρόνος ολοκλήρωσης της επίθεσης είναι 740 sec, περίπου 12 min, σε αντίθεση με την coWPAtty η οποία όπως προαναφέρθηκε χρειάστηκε περίπου 45 min. Οι pre-calculated hash επιθέσεις είναι πιο γρήγορες στην εκτέλεση τους, όμως χρειάζονται περισσότερο χρόνο προετοιμασίας. Η εντολή genpmk χρειάστηκε για να δημιουργήσει το hash αρχείο 8662,63 sec, περίπου 2½ hr, ενώ η εντολή airolib-ng χρειάστηκε 7796 sec, περίπου 2 hr και 15 min. Οι εντολές που χρησιμοποιούν τα hash αρχεία μπορεί να χρειάζονται περισσότερο χρόνο προετοιμασίας, όμως είναι πολύ πιο γρήγορες στην επίθεσή τους καθώς η aircrack-ng που συνδυάζεται με την airolib-ng χρειάζεται 6 sec, ενώ η coWPAtty που συνδυάζεται με την genpmk χρειάζεται μόλις 4,25 sec. Τέλος διαπιστώνουμε ότι η aircrack-ng είναι καλύτερη με dictionary attack, ενώ η genpmk & coWPAtty είναι καλύτερη με pre-computed hashes.

Συμπεράσματα

Στην παρούσα διπλωματική εργασία παρουσιάστηκε μία γενική ανασκόπηση στο παρελθόν, στο παρόν και στις επιθέσεις που παραβιάζουν την ασφάλεια των ασύρματων δικτύων.

Τα ασύρματα τοπικά δίκτυα, λόγω των πλεονεκτημάτων που προσφέρουν, γνωρίζουν μεγάλη αποδοχή από τους καταναλωτές και εξαπλώνονται ταχύτατα. Όμως το βασικό ζήτημα που απασχολεί όλους τους φορείς που ασχολούνται με την ανάπτυξή τους είναι το θέμα της ασφάλειας.

Για την βελτίωση της ασφάλειας των ασύρματων δικτύων χρησιμοποιήθηκαν οι αλγόριθμοι κρυπτογράφησης, οι οποίοι όμως έχουν και αυτοί αδύνατα σημεία. Το πρωτόκολλο κρυπτογράφησης WEP εμφανίστηκε πρώτο και αποκάλυψε πολλά κενά στον τομέα της ασφάλειας. Παρ όλες όμως τις βελτιώσεις του δεν κατάφερε να χαρακτηριστεί ως ένα ασφαλές πρωτόκολλο. Μία νέα, αποτελεσματικότερη λύση προτάθηκε με το πρότυπο 802.11i, το πρωτόκολλο κρυπτογράφησης WPA και η τελική του έκδοση το WPA2, με σκοπό την επίτευξη ακόμα μεγαλύτερης ασφάλειας. Αναπτύχθηκε για να αντιμετωπίσει και να διορθώσει τα ελαττώματα του WEP. Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης CCMP ο οποίος παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη πακέτων. Οι επιθέσεις στα δίκτυα με πρωτόκολλο κρυπτογράφησης WEP και WPA/WPA2 αυτοματοποιήθηκαν με τη χρήση εφαρμογών, όπως η σουίτα εργαλείων AirCrack, με αποτέλεσμα ο καθένας που διαθέτει έναν σύγχρονο υπολογιστή και την κατανόηση της τεχνολογίας των υπολογιστών να μπορεί να εφαρμόσει επιθέσεις. Ωστόσο, και ένα ολοκληρωμένο σύστημα ασφάλειας καθίσταται αδύναμο εάν κανείς δεν γνωρίζει τον τρόπο χρησιμοποίησής του.

Βιβλιογραφικές Αναφορές

Wireless Communications & Networks, (William Stallings, 2007)

Hacking exposed wireless: Wireless security & solutions, Second edition, (Johnny Cache, Joshua Wright, Vincent Liu, 2010)

Wireless Communications & Networking, (Vijay K. Garg, 2007)

Surveying Wi-Fi security, Dept. of Applied Informatics, University of Macedonia, (George E. Violettas, Tryfon L. Theodorou, Konstantinos Chalkias1 & George C. Stephanides)

HiperLan/2, Department of Computer Science and Engineering, Helsinki University of Technology (Janne Korhonen)

802.11 Security - Cracking 802.11, Security with aircrack, (Giorgos Kappes)

Investigation of the IEEE 802.11 Medium Access Control (MAC) Sublayer Functions, (B.P. Crow, I. Widjaja, J. G. Kim, and P. Sakai)

Overview of WLAN security, Helsinki University of Technology, (Timo Hassinen)

Wardriving, Warchalking & Wireless Hacking, (Marinos Papadopoulos)

Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2), (Paul Arana, 2006)

Security Improvement of WPA 2, (Nazmus Sakib, 2011)

A Survey on Wireless Security protocols, (Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, Behrang Samadi, 2009)

Βικιπαίδεια, http://el.wikipedia.org

IEEE Standards Association, http://standards.ieee.org

Standards & Initiatives, http://www.intel.com

Ένωση Μηχανικών Πληροφορικής & Επικοινωνιών Ελλάδος, http://www.computer-engineers.gr

Παιδαγωγικό ινστιτούτο, http://www.pi-schools.gr

Πανεπιστήμιο Μακεδονίας, http://www.cnc.uom.gr

Κοινωνία της πληροφορίας, http://www.ebusinessforum.gr

Athens Wireless Metropolitan Network, http://www.awmn.net

Εισαγωγή στη σουίτα aircrack-ng, http://geekay.freehostingcloud.com

Security & hacking tools, http://tools.securitytube.net

Aircrack-ng, http://www.aircrack-ng.org

Main.java

```
package changexml;
import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.DataInputStream;
import java.io.FileInputStream;
import java.io.FileWriter;
import java.io.InputStreamReader;
public class Main {
public static void main(String[] args) {
try{
FileWriter tostream = new FileWriter("C:/KismetXMLParser/GregStats/CleanKismetResults.txt");
BufferedWriter out = new BufferedWriter(tostream);
FileInputStream fstream = new FileInputStream("C:/KismetXMLParser/Files/Kismet_results.xml");
DataInputStream in = new DataInputStream(fstream);
BufferedReader br = new BufferedReader(new InputStreamReader(in));
String startElement = "<wireless-client";
String endElement = "</wireless-client";
String strLine;
boolean inClient=false;
while ((strLine = br.readLine()) != null){
if (strLine.trim().startsWith(startElement))
inClient=true;
if (strLine.trim().startsWith(endElement))
inClient=false;
```

```
if (!inClient){
out.write(strLine+"\n");
//    System.out.println(strLine);
}
}
in.close();
out.close();
}
catch (Exception ex){}
}
}
```

Wireless_Network.java

```
package kismetstats;

public class Wireless_Network {

protected int number;

protected String essid;

protected int channel;

protected String encryption;

public Wireless_Network(int number){

this.number=number;

 }

public Wireless_Network(int number, String essid, int channel, String encryption){

this.number=number;

this.essid=essid;

this.channel=channel;

this.encryption=encryption;

}

public void setEssid(String essid){

this.essid=essid;

}

public void setChannel(int channel){

this.channel=channel;

}

public void setEncryption(String encryption){

this.encryption=encryption;

}

public int getNumber(){

return number;
```

```
}
public String getEssid(){
return essid;
}
public int getChannel(){
return channel;
}
public String getEncryption(){
return encryption;
}
}
```

Main.java

```
package kismetstats;
import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.DataInputStream;
import java.io.FileInputStream;
import java.io.FileWriter;
import java.io.InputStreamReader;
import java.util.LinkedList;
import java.util.Vector;
public class Main {
protected static LinkedList networksList;
public static void main(String[] args) {
networksList = new LinkedList();
initNetworksList();
createNetworksFile();
createEssidFile();
createChannelFile();
createEncryptionFile();
createPopularEncryptionFile();
}
private static void initNetworksList(){
try{
FileInputStream fstream = new FileInputStream("C:/KismetXMLParser/GregStats/CleanKismetResults.txt");
DataInputStream in = new DataInputStream(fstream);
BufferedReader br = new BufferedReader(new InputStreamReader(in));
```

```
String strLine;
int networkNo=0;
String networkEssid="null";
int networkChannel=0;
String networkEncryption="null";
String networkNoTag="<wireless-network number=\"";
String essidFalseTag="<essid cloaked=\"false\">";
String essidTrueTag="<essid cloaked=\"true\">";
String channelTag="<channel>";
String encryptionTag="<encryption>";
while ((strLine = br.readLine()) != null){
// System.out.println(strLine);

if (strLine.trim().startsWith(networkNoTag)){
String temp="";
for (int i=networkNoTag.length();i<strLine.trim().length();i++){
if (strLine.trim().charAt(i)!="\"".charAt(0))
temp+=strLine.trim().charAt(i);
else
break;
}
networkNo=new Integer(temp);
//    System.out.println("Number: "+networkNo);
networkEssid="null";
networkChannel=-1;
networkEncryption="null";
}
if (strLine.trim().startsWith(essidFalseTag)){
```

```
String temp="";
for (int i=essidFalseTag.length();i<strLine.trim().length();i++){
if (strLine.trim().charAt(i)!="<".charAt(0))
temp+=strLine.trim().charAt(i);
else
break;
}
networkEssid=temp;
//  System.out.println("Essid: "+networkEssid);
}
if (strLine.trim().startsWith(essidTrueTag)){
String temp="";
for (int i=essidTrueTag.length();i<strLine.trim().length();i++){
if (strLine.trim().charAt(i)!="<".charAt(0))
temp+=strLine.trim().charAt(i);
else
break;
}
networkEssid=temp;
//    System.out.println("Essid: "+networkEssid);
}
if (strLine.trim().startsWith(channelTag)){
String temp="";
for (int i=channelTag.length();i<strLine.trim().length();i++){
if (strLine.trim().charAt(i)!="<".charAt(0))
temp+=strLine.trim().charAt(i);
else
break;
```

```
}
networkChannel=new Integer(temp);
//   System.out.println("Channel: "+networkChannel);
if (networkEncryption.equals("null"))
networkEncryption=findClientEncryption(networkNo);
networksList.add(new Wireless_Network(networkNo, networkEssid, networkChannel, networkEncryption));
}
if (strLine.trim().startsWith(encryptionTag)){
String temp="";
for (int i=encryptionTag.length();i<strLine.trim().length();i++){
if (strLine.trim().charAt(i)!="<".charAt(0))
temp+=strLine.trim().charAt(i);
else
break;
}
networkEncryption=temp;
// System.out.println("Encryption: "+networkEncryption);
}
}
in.close();
}
catch(Exception ex){System.out.println(ex.getMessage());}
}
private static void createNetworksFile() {
try{
FileWriter tostream = new FileWriter("C:/KismetXMLParser/GregStats/networksInclClients.txt");
BufferedWriter out = new BufferedWriter(tostream);
```

```
for (int i=0;i<networksList.size();i++){
Wireless_Network temp=(Wireless_Network)networksList.get(i);
out.write("Number: " + temp.getNumber()+"\n");
out.write("Essid: " + temp.getEssid()+"\n");
out.write("Channel: " + temp.getChannel()+"\n");
out.write("Encryption: " + temp.getEncryption()+"\n");
out.write("\n");
}
out.close();
}
catch (Exception ex){System.out.println(ex.getMessage());}
}
private static void createEssidFile() {
try{
FileWriter tostream = new FileWriter("C:/KismetXMLParser/GregStats/essids.txt");
BufferedWriter out = new BufferedWriter(tostream);
LinkedList essids=new LinkedList();
LinkedList essidsPopulation=new LinkedList();
for (int i=0;i<networksList.size();i++){
Wireless_Network temp=(Wireless_Network)networksList.get(i);
System.out.println("Network number: "+temp.getNumber());
boolean found=false;
for (int j=0;j<essids.size();j++){
if (((String)essids.get(j)).equals(temp.getEssid())){
found=true;
int pop=((Integer)essidsPopulation.get(j)).intValue();
essidsPopulation.set(j, new Integer(pop+1));
}
```

```
}
if (!found){
essids.add(temp.getEssid());
essidsPopulation.add(new Integer(1));
}
}
for (int pass=1; pass < essidsPopulation.size(); pass++) {
for (int i=0; i < essidsPopulation.size()-pass; i++) {
if ((Integer)essidsPopulation.get(i) < (Integer)essidsPopulation.get(i+1)) {
Integer temp = (Integer)essidsPopulation.get(i);
String essidTemp=(String)essids.get(i);
essidsPopulation.set(i, (Integer)essidsPopulation.get(i+1));
essids.set(i, (String)essids.get(i+1));
essidsPopulation.set(i+1, temp);
essids.set(i+1, essidTemp);
}
}
}
for (int i=0;i<essids.size();i++){
System.out.println(essids.get(i)+ ": " + essidsPopulation.get(i)+"\n");
out.write(essids.get(i)+ ": " + essidsPopulation.get(i)+"\n");
}
out.close();
}
catch (Exception ex){System.out.println(ex.getMessage());}
}
private static void createChannelFile() {
try{
```

```
FileWriter tostream = new FileWriter("C:/KismetXMLParser/GregStats/channels.txt");
BufferedWriter out = new BufferedWriter(tostream);
LinkedList channels=new LinkedList();
LinkedList channelsPopulation=new LinkedList();
for (int i=0;i<networksList.size();i++){
Wireless_Network temp=(Wireless_Network)networksList.get(i);
System.out.println("Network number: "+temp.getNumber());
boolean found=false;
for (int j=0;j<channels.size();j++){
if (((Integer)channels.get(j)).intValue()==temp.getChannel()){
found=true;
int pop=((Integer)channelsPopulation.get(j)).intValue();
channelsPopulation.set(j, new Integer(pop+1));
}
}
if (!found){
channels.add(new Integer(temp.getChannel()));
channelsPopulation.add(new Integer(1));
}
}
for (int pass=1; pass < channelsPopulation.size(); pass++) {
System.out.println("Sorting number: "+ pass);
for (int i=0; i < channelsPopulation.size()-pass; i++) {
if ((Integer)channelsPopulation.get(i) < (Integer)channelsPopulation.get(i+1)) {
Integer temp = (Integer)channelsPopulation.get(i);
Integer channelTemp=(Integer)channels.get(i);
channelsPopulation.set(i, (Integer)channelsPopulation.get(i+1));
channels.set(i, (Integer)channels.get(i+1));
```

```
channelsPopulation.set(i+1, temp);
channels.set(i+1, channelTemp);
}
}
}
for (int i=0;i<channels.size();i++){
System.out.println(channels.get(i)+ ": " + channelsPopulation.get(i)+"\n");
out.write(channels.get(i)+ ": " + channelsPopulation.get(i)+"\n");
}
out.close();
}
catch (Exception ex){System.out.println(ex.getMessage());}
}
private static void createEncryptionFile() {
try{
FileWriter tostream = new FileWriter("C:/KismetXMLParser/GregStats/encryptionsInclClients.txt");
BufferedWriter out = new BufferedWriter(tostream);
LinkedList encryptions=new LinkedList();
LinkedList encryptionsPopulation=new LinkedList();
for (int i=0;i<networksList.size();i++){
Wireless_Network temp=(Wireless_Network)networksList.get(i);
System.out.println("Network number: "+temp.getNumber());
boolean found=false;
for (int j=0;j<encryptions.size();j++){
if (((String)encryptions.get(j)).equals(temp.getEncryption())){
found=true;
int pop=((Integer)encryptionsPopulation.get(j)).intValue();
encryptionsPopulation.set(j, new Integer(pop+1));
```

```
}
}
if (!found){
encryptions.add(temp.getEncryption());
encryptionsPopulation.add(new Integer(1));
}
}
for (int pass=1; pass < encryptionsPopulation.size(); pass++) {
System.out.println("Sorting number: "+ pass);
for (int i=0; i < encryptionsPopulation.size()-pass; i++) {
if ((Integer)encryptionsPopulation.get(i) < (Integer)encryptionsPopulation.get(i+1)) {
Integer temp = (Integer)encryptionsPopulation.get(i);
String encryptionTemp=(String)encryptions.get(i);
encryptionsPopulation.set(i, (Integer)encryptionsPopulation.get(i+1));
encryptions.set(i, (String)encryptions.get(i+1));
encryptionsPopulation.set(i+1, temp);
encryptions.set(i+1, encryptionTemp);
}
}
}
for (int i=0;i<encryptions.size();i++){
System.out.println(encryptions.get(i)+ ": " + encryptionsPopulation.get(i)+"\n");
out.write(encryptions.get(i)+ ": " + encryptionsPopulation.get(i)+"\n");
}
out.close();
}
catch (Exception ex){System.out.println(ex.getMessage());}
```

```
}
private static void createPopularEncryptionFile() {
try{
FileWriter tostream = new FileWriter("C:/KismetXMLParser/GregStats/popularEncryptions.txt");
BufferedWriter out = new BufferedWriter(tostream);
LinkedList encryptions=new LinkedList();
LinkedList encryptionsPopulation=new LinkedList();
for (int i=0;i<networksList.size();i++){
if (((Wireless_Network)networksList.get(i)).getEssid().equals("NetFasteR IAD 2 (PSTN)")){
Wireless_Network temp=(Wireless_Network)networksList.get(i);
System.out.println("Network number: "+temp.getNumber());
boolean found=false;
for (int j=0;j<encryptions.size();j++){
if (((String)encryptions.get(j)).equals(temp.getEncryption())){
found=true;
int pop=((Integer)encryptionsPopulation.get(j)).intValue();
encryptionsPopulation.set(j, new Integer(pop+1));
}
}
if (!found){
encryptions.add(temp.getEncryption());
encryptionsPopulation.add(new Integer(1));
}
}
}
for (int pass=1; pass < encryptionsPopulation.size(); pass++) {
System.out.println("Sorting number: "+ pass);
```

```
for (int i=0; i < encryptionsPopulation.size()-pass; i++) {
if ((Integer)encryptionsPopulation.get(i) < (Integer)encryptionsPopulation.get(i+1)) {
Integer temp = (Integer)encryptionsPopulation.get(i);
String encryptionTemp=(String)encryptions.get(i);
encryptionsPopulation.set(i, (Integer)encryptionsPopulation.get(i+1));
encryptions.set(i, (String)encryptions.get(i+1));
encryptionsPopulation.set(i+1, temp);
encryptions.set(i+1, encryptionTemp);
}
}
}
for (int i=0;i<encryptions.size();i++){
System.out.println(encryptions.get(i)+ ": " + encryptionsPopulation.get(i)+"\n");
out.write(encryptions.get(i)+ ": " + encryptionsPopulation.get(i)+"\n");
}
out.close();
}
catch (Exception ex){System.out.println(ex.getMessage());}
}
private static String findClientEncryption(int networkNo) {
String tempEncryption="null";
try{
FileInputStream fstream = new FileInputStream("C:/KismetXMLParser/Files/Kismet_results.xml");
DataInputStream in = new DataInputStream(fstream);
BufferedReader br = new BufferedReader(new InputStreamReader(in));
String strLine;
String networkTag="<wireless-network number=\"" + networkNo + "\"";
```

```
boolean inNetwork=false;
while ((strLine = br.readLine()) != null){
if (strLine.trim().startsWith(networkTag)){
inNetwork=true;
}
if (inNetwork){
if (strLine.trim().startsWith("<encryption>")){
String temp="null";
for (int i="<encryption>".length();i<strLine.trim().length();i++){
if (strLine.trim().charAt(i)!="<".charAt(0))
temp+=strLine.trim().charAt(i);
else{
inNetwork=false;
break;
}
}
if (strLine.trim().startsWith("</wireless-network>")){
inNetwork=false;
}
tempEncryption=temp;
// System.out.println("Encryption: "+networkEncryption);
}
}
}
in.close();
}
catch (Exception ex){System.out.println(ex.getMessage());}
```

```
return tempEncryption;
}
}
```