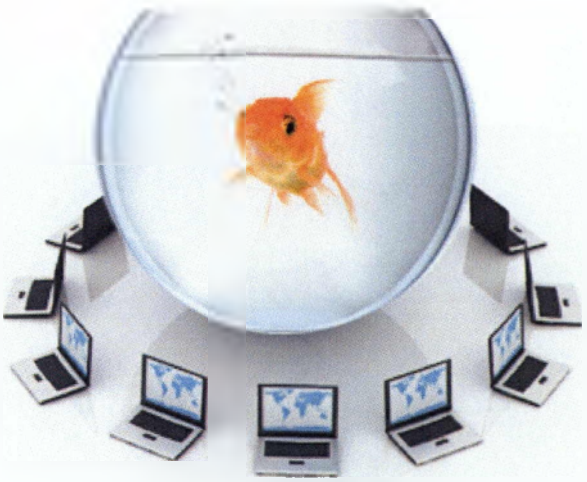
Α.Τ.Ε.Ι Καλαμάτας

Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών

Πτυχιακή Εργασία:

Διαχείριση ασφάλειας σε δίκτυα τοπικών ασύρματων επικοινωνιών για το πρότυπο IEEE 802.11 (Wi-Fi)



Γιαννακοπούλου Αναστασία, ΑΜ:2007114

Επιβλέπων Καθηγητής: Ναστάκος Μιχαήλ

-2012-

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας εργασίας είναι η παρουσίαση της κατάστασης στον τομέα της ασφάλειας των ασύρματων δικτύων. Μελετώνται η αρχιτεκτονική και τα πρωτόκολλα που χρησιμοποιούνται καθώς και οι προδιαγραφές αυτών σε ασφάλεια. Πιο συγκεκριμένα, γίνεται αναφορά σε θέματα ασφάλειας ενός ασύρματου δικτύου που βασίζεται στο πρωτόκολλο IEEE 802.11. Παρουσιάζονται οι απειλές που είναι δυνατό να δεχθεί ένα τέτοιο δίκτυο καθώς και οι τεχνικές άμυνας που χρησιμοποιούνται για να αντιμετωπιστούν οι παραπάνω απειλές.

Πιο αναλυτικά, στο πρώτο κεφάλαιο αναφέρονται κάποια εισαγωγικά θέματα που αφορούν τα δίκτυα και ειδικότερα την ασύρματη επικοινωνία και τα βασικότερα δομικά συστατικά απο τα οποία αποτελείται ένα ασύρματο δίκτυο. Επίσης αναλύεται το πρωτόκολλο IEEE 802.11 και όλα τα πρότυπα αυτής της οικογένειας. Το πρώτο κεφάλαιο κλείνει με τα χαραχτηριστικά, την τοπολογία, και την αρχιτεκτονική του πρωτοκόλλου IEEE 802.11.

Στο δεύτερο κεφάλαιο αναλύονται οι μηχανιμοί ασφαλείας που χρησιμοποιούνται έως και σήμερα, με μια εκτενή αναφορά στον τρόπο λειτουργίας και στα μειονεκτήματα της WEP κρυπτογράφησης. Στο ίδιο κεφάλαιο αναφέρονται και οι λύσεις που δόθηκαν για να καλυφθούν τα κενά που άφηνε η προηγούμενη μέθοδος (TKIP, WPA, WPA2). Στο ίδιο κεφάλαιο γίνεται αναφορά σε ορισμένες από τις πιο γνωστές επίθεσεις σε ασύρματα δίκτυα.

Στο τρίτο κεφάλαιο πραγματοποιούνται πέντε επιτυχημένες επιθέσεις σε ένα ανασφαλές δίκτυο με κρυπτογράφηση WEP. Η πρώτη επίθεση αφορά την αιχμαλώτιση πακέτων και την εξαγωγή χρήσιμων πληροφοριών για το δίκτυο. Στη συνέχεια γίνεται ανάκτηση του μυστικού κωδικού WEP και ακολουθούν ορισμένες επιθέσεις που έχουν ώς στόχο να καταστείλουν την λειτουργία του σταθμού στόχου (DOS attack), την κλοπή κωδικών (Man in the Middle Attcak) και την αλλαγή της Mac Address.

Στο τέταρτο κεφάλαιο παρουσιάζονται κάποιες τεχνικές οι οποίες μπορεί να βοηθήσουν στον περιορισμό των κενών της ασφάλειας που αφήνει το IEEE 802.11 πρωτόκολλο και στην ενίσχυση της ασφάλειας των υπαρχόντων συστημάτων. (SSID Hidding, MAC Filtering, VPNs, RADIUS, IDSs, Firewalls κ.α.)

Τέλος στο πέμπτο κεφάλαιο γίνεται μια ανακεφαλαίωση της εργασίας και καταγράφονται τα αποτελέσματα της μελέτης και οι δυνατότητες για μελλοντική έρευνα.

ABSTRACT

The purpose of this thesis is to present the current state of Wireless Network Security on IEEE 802.11-based networks. This study will examine the architecture, protocols and specifications of wireless networks from a security standpoint. Specifically there will be a presentation of the threats and countermeasures that must be employed on a wireless network based on IEEE 802.11.

In particular, the first chapter is an introduction to wireless networks with a brief history of wireless networks. The basic structure of a wireless network is analyzed and reviewed in detail in the same chapter.

The IEEE 802.11 and all protocols of the same family are also analyzed. The characteristics, topology and the architecture of the protocol are examined in the same chapter. Later on, in the second chapter, there is a reference to the security mechanisms, ways of operation and drawbacks of WEP Cryptography. In the same chapter there is a short description of some new methods that overcome the problems of the WEP Cryptography. (TKIP, WPA, WPA2).

Moreover, the second chapter presents some of the most popular attacks in wireless networks. All attacks are executed in a Linux environment (BackTrack) via command prompt.

The third chapter describes five successful attacks executed on an insecure wireless network with WEP cryptography. In the first attack, a procedure of monitoring the network and trapping some packets is demonstrated. The next attack involves WEP key recovery and the next attacks deactivate the station target (DOS attack), steal codes (Man in the Middle Attack) and change the MAC Address of a station.

Next up is a presentation of the security measures that should be taken for the enhancement of the IEEE 802.11 security on existing systems. (SSID Hiding, MAC Filtering, VPNs, RADIUS, IDSs, Firewalls etc) Finally, in the last chapter, there is a review of the whole study, results and conclusions of this work.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 ΓΕΝΙΚΑ

Ένα από τα χαρακτηριστικά της εποχής μας είναι ο εθισμός στην τεχνολογία της συλλογής, επεξεργασίας και αναδιανομής της πληροφορίας. Όλο και περισσότεροι άνθρωποι γίνονται τόσο παθητικά αλλά και ενεργητικά μέλη στο παγκόσμιο διαδίκτυο. Για αυτούς τους χρήστες που το διαδίκτυο είναι πλέον ζωτικής σημασίας τόσο σε επαγγελματικό αλλά και σε προσωπικό επίπεδο, τα σύστροφα ζεύγη, τα ομοαξονικά καλώδια και οι οπτικές ίνες είναι άχρηστες. Οι χρήστες αυτοί χρειάζονται δεδομένα για το φορητό υπολογιστή, τον υπολογιστή τσέπης ή τον υπολογιστή-ρολόι τους χωρίς να είναι προσδεμένοι στην επίγεια επικοινωνιακή δομή. Για τους χρήστες αυτούς η απάντηση είναι οι ασύρματες επικοινωνίες.

Ένας από τους ορισμούς που έχει επικρατήσει γενικότερα για τα δίκτυα υπολογιστών παρατίθεται πιο κάτω:

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

Θα πρέπει να τονίσουμε ότι σύμφωνα με την λειτουργικότητας τους, τα δίκτυα υπολογιστών χωρίζονται που καθορίζουν και την σημασία τους :

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως Ενσύρματα ή Ασύρματα.
- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως Δημόσια ή Ιδιωτικά δίκτυα.
- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως Τοπικά (LAN και WLAN), Μητροπολιτικά (MAN και WMAN), Ευρείας κάλυψης (WAN και WWAN) και Προσωπικά (PAN και WPAN).(Σιδερίδη, 1998)

Όπως αναφέρεται πιο πάνω, αυτό που μπορεί να διαφοροποιήσει ένα ενσύρματο από ένα ασύρματο δίκτυο είναι το φυσικό μέσο μετάδοσης της πληροφορίας. Τα WLAN αντί για καλώδια και οπτικές ίνες, χρησιμοποιούν υπέρυθρες ακτίνες (IR) ή ραδιοσυχνότητες (RF). Οι ραδιοσυχνότητες είναι πιο διαδεδομένες διότι είναι μεγαλύτερης εμβέλειας, εύρους ζώνης και κάλυψης. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα συνήθως 2,4 GHz και 5 GHz. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου.

Τα ασύρματα δίκτυα υπολογιστών όμως, όπως και τα κλασσικά ενσύρματα δίκτυα, απαιτούν την χρήση αξιόπιστων πρωτοκόλλων μεταφοράς δεδομένων, τα οποία θα εξασφαλίζουν την ασφαλή μετάδοση των δεδομένων μεταξύ των χρηστών, θα παρέχουν
ασφάλεια από οποιαδήποτε ενέργεια παραβίασης, θα δίνουν την δυνατότητα ταχείας πρόσβασης και μεταφοράς δεδομένων και τέλος θα επιτρέπουν την διασύνδεσή των ασύρματων δικτύων με αυτά που κάνουν χρήση ενσύρματων τεχνολογιών.

Ο τομέας των ασύρματων δικτύων, ένας τομέας επανάσταση για το είδος του, είναι ένας από τους ταχύτερα αναπτυσσόμενους κλάδους των τηλεπικοινωνιών.

Με δεδομένη τη αποδοχή του κόσμου για αυτή τη νέα τεχνολογία, τις λύσεις των προμηθευτών και τα βιομηχανικά πρότυπα, η ασύρματη δικτύωση ήρθε και θα μείνει. Όμως πόσο ασφαλής είναι αυτή η τεχνολογία;

1.2 ΣΚΟΠΟΣ

Η χρήση ασύρματων δικτύων (WiFi) είναι πλέον κοινός τόπος σε οικιακούς και εταιρικούς χώρους ενώ έχει ήδη ξεκινήσει και επεκτείνεται η εξάπλωσή τους σε μητροπολιτική κλίμακα.

Η παρούσα πτυχιακή θα ασχοληθεί με την ασφάλεια των ασύρματων δικτύων. Θα μελετηθεί η τυπική αρχιτεκτονική των δικτύων αυτών, τα πρωτόκολλα που χρησιμοποιούνται καθώς και οι προδιαγραφές αυτών σε ασφάλεια. Θα γίνει μελέτη των απειλών που είναι δυνατό να δεχθεί ένα τέτοιο δίκτυο καθώς και των τεχνικών άμυνας που χρησιμοποιούνται για να αντιμετωπιστούν οι παραπάνω απειλές. Θα γίνει επίδειξη ανασφαλούς δικτύου WiFi, των επιθέσεων που μπορούν να γίνουν σε αυτό καθώς και των μεθόδων θωράκισής του.

ΚΕΦΑΛΑΙΟ 2. ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

2.1 ΤΙ ΕΙΝΑΙ ΤΟ WI-FI;

Με την ταχύτητα ανάπτυξη των προτύπων IEEE και την γιγάντωση της βιομηχανίας κατασκευαστών αντίστοιχων συσκευών, κρίθηκε αναγκαία η διασφάλιση της συμβατότητας μεταξύ των διάφορων συσκευών για την προστασία του αγοραστή.

Έτσι το 1999 ιδρύθηκε η WECA (Wireless Ethernet Compatibility Alliance), ένας μη κερδοσκοπικός οργανισμός που σκοπό έχει την πιστοποίηση ασύρματων 802.11 συσκευών. (Wikipedia)

Σε αυτό τον οργανισμό συμμετέχουν κατασκευαστές ολοκληρωμένων κυκλωμάτων, παροχείς υπηρεσιών WLAN, κατασκευαστές υπολογιστών, κατασκευαστές λογισμικού κ.α. Μερικές από τις εταιρίες που μετέχουν είναι οι 3Com, Aironet, Apple, Breezecom, Compaq, Dell, Fujitsu, IBM, Lucent Technologies, Nokia, Samsung, Symbol Technologies, Zoom.

Η ένωση αυτή επινόησε μία σειρά από δοκιμές προκειμένου να πιστοποιηθεί η συμβατότητα των IEEE προϊόντων. Οι συσκευές οι οποίες κατάφερναν να περάσουν με επιτυχία από αυτές τις δοκιμές, 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 λογότυπο. (Εικόνα 1.)

Εικόνα 1. Λογότυπο Wi-Fi

2.2 ΠΕΡΙΓΡΑΦΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Ως ασύρματο τοπικό δίκτυο (WLAN) ορίζεται ένα σύστημα επικοινωνίας μέσω ηλεκτρομαγνητικών κυμάτων ανάμεσα σε σταθερούς ή κινητούς χρήστες επιτρέποντας την μεταξύ τους διασύνδεση και ανταλλαγή δεδομένων.

Η πρώτη γενιά συσκευών WLAN με τη χαμηλή ταχύτητα διάδοσης και την έλλειψη προτύπων δεν ήταν ιδιαίτερα διαδεδομένη. Όμως τα σύγχρονα συστήματα είναι δυνατόν να μεταφέρουν δεδομένα σε αποδεκτές ταχύτητες.

Επίσης, νέες συσκευές και προϊόντα ασύρματης πρόσβασης βασιζόμενα σε τεχνολογίες spread-spectrum ραδιοφωνικά κύματα, υπέρυθρες ακτίνες, κυψελοειδείς και δορυφορικές επικοινωνίες, είναι πια πραγματικότητα.

Σήμερα υπάρχει στην αγορά ένας τεράστιος αριθμός από νέες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέες τεχνολογίες και πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές, οι οποίοι ενσωματώνουν τεχνολογία ασύρματης πρόσβασης, είναι διαθέσιμοι για το ευρύ κοινό, αφού έχουν πλέον χαμηλό κόστος, ικανοποιητική υπολογιστική ισχύ και ποιότητα υπηρεσιών παρόμοια με τους σταθερούς υπολογιστές.

2.2.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Μερικά από τα κυριότερα πλεονεκτήματα των ασύρματων τοπικών δικτύων είναι τα εξής:

Ευκολία (Convenience): Η ασύρματη φύση αυτών των δικτύων επιτρέπει στους χρήστες να έχουν πρόσβαση στους πόρους ενός δικτύου, από σχεδόν οποιαδήποτε τοποθεσία χωρίς να πρέπει να βρίσκονται στο σπίτι ή στο γραφείο. Με την αύξηση της χρήσης φορητών υπολογιστών, αυτό είναι ιδιαίτερα σημαντικό.

Κινητικότητα (mobility): Τα WLAN παρέχουν τη δυνατότητα στους χρήστες για πρόσβαση σε πληροφορίες ενώ βρίσκονται σε κίνηση. Αυτή η ευχέρεια στην κίνηση υποστηρίζει την παραγωγικότητα και τις ευκαιρίες για εξυπηρέτηση οι οποίες δεν είναι δυνατές με ενσύρματα

δίκτυα. Οι εφαρμογές που στηρίζονται στην κινητικότητα κατά τη χρήση συσκευών σε ένα WLAN συμπεριλαμβάνουν και αυτές που στηρίζονται στην πρόσβαση δεδομένων σε πραγματικό χρόνο-τα οποία είναι συνήθως αποθηκευμένα σε βάσεις δεδομένων. Μία τέτοια εφαρμογή συναντάμε στους αγώνες ταχύτητας. Τα αυτοκίνητα έχουν σύνθετα συστήματα επεξεργασίας που παρακολουθούν και ελέγχουν τα διάφορα όργανα που βρίσκονται στο αυτοκίνητο. Όταν το αυτοκίνητο περνάει μπροστά από τη βάση της ομάδας στα pit, οι πληροφορίες αυτές φορτώνονται στον κεντρικό υπολογιστή, καθιστώντας ικανή μια ανάλυση σε πραγματικό χρόνο της επίδοσης του αυτοκινήτου.

Ταχύτητα και ευελιξία εγκατάστασης: Η εγκατάσταση ενός WLAN εξαλείφει την ανάγκη της χρήσης των καλωδίων η οποία απαιτεί συνήθως κόπο και χρόνο, ενώ η ασύρματη τεχνολογία επιτρέπει τη διασύνδεση δικτύων η οποία υπό άλλες συνθήκες θα ήταν αδύνατη. Μακροπρόθεσμα, η εγκατάσταση, η αναβάθμιση και το κόστος συντήρησης των συστημάτων WLAN, τα καθιστούν μια οικονομικότερη λύση.

Υπάρχουν και μερικά περιβάλλοντα στα οποία τα ασύρματα τοπικά δίκτυα αποτελούν καλύτερη λύση από ένα δίκτυο με καλώδιο. Στην κατηγορία αυτή ανήκουν:

- Περιβάλλοντα μεγάλων εκτάσεων, όπως οι χώροι παραγωγής ενός εργοστασίου ή μιας αποθήκης.
- Πολύ παλιά κτίρια, στα οποία είτε απαγορεύεται η οποιαδήποτε τροποποίηση των κτιριακών εγκαταστάσεων, είτε η καλωδίωση είναι ανεπαρκής ή ανύπαρκτη.
- Μικρά γραφεία, όπου η εγκατάσταση και η συντήρηση ενός ενσύρματου δικτύου είναι αντιοικονομική.

Μειωμένο κόστος χρήσης: Παρότι η αρχική επένδυση για ένα εξοπλισμό WLAN μπορεί να είναι υψηλότερη από μια ενσύρματη σύνδεση, το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο, καθώς μακροπρόθεσμα τα κέρδη είναι μεγαλύτερα σε περιβάλλοντα όπου απαιτούνται πολλές μετακινήσεις.

Συμβατότητα: Τα ασύρματα δίκτυα διαφοροποιούνται για να ικανοποιήσουν τις ανάγκες συγκεκριμένων εγκαταστάσεων και εφαρμογών. Οι διαμορφώσεις αλλάζουν εύκολα από μικρά δίκτυα κατάλληλα για έναν μικρό αριθμό χρηστών σε πλήρως ανεπτυγμένα δίκτυα που καλύπτουν εκατοντάδες χρήστες.

Νομαδική πρόσβαση: Η νομαδική πρόσβαση βρίσκει εφαρμογή σε χώρους όπως επιχειρήσεις ή πανεπιστημιουπόλεις, όπου τα κτίρια βρίσκονται συγκεντρωμένα. Σε αυτές τις περιπτώσεις, οι χρήστες μετακινούνται μέσα στο χώρο και μπορούν με τους φορητούς υπολογιστές τους να προσπελαύνουν αρχεία των servers και άλλων κόμβων του δικτύου.

Διασύνδεση: Μια άλλη περίπτωση της διεύρυνσης είναι και η διασύνδεση δυο ή παραπάνω αυτόνομων τοπικών δικτύων που βρίσκονται σε διαφορετικούς χώρους.

Για παράδειγμα αν είναι δύσκολο να χρησιμοποιήσουμε οπτικές ίνες για να ενώσουμε δίκτυα σε διαφορετικά κτίρια (λόγω εδάφους, κόστους, αδειών κ.τ.λ.) συμφέρει να χρησιμοποιήσουμε ασύρματη ζεύξη. Στην περίπτωση αυτή, χρησιμοποιείται μια ασύρματη σύνδεση από σημείο-σε-σημείο (wireless point-to-point link) μεταξύ των δύο κτιρίων. (Tanenbaum, 2000)

2.2.2 ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Η χρήση των ηλεκτρομαγνητικών κυμάτων (ραδιοκυμάτων και υπέρυθρης ακτινοβολίας) για την μεταφορά πληροφορίας κάνουν τα ασύρματα δίκτυα ευπρόσβλητα σε πολλά φαινόμενα παρεμβολής, τα οποία αλλοιώνουν την επικοινωνία των χρηστών. Τα κυριότερα από αυτά τα προβλήματα αναφέρονται στη συνέχεια.

Παρεμβολη λογω πολλαπλων διαδρομων: Σήματα που μεταδίδονται είναι δυνατόν να συνδυαστούν με ανακλώμενα σήματα από επιφάνειες ή εμπόδια που βρίσκονται στην ευθεία μετάδοσης του σήματος.

Path loss: Οι απώλειες που μπορεί να έχουμε σε μια ασύρματη επικοινωνία από το «path loss» εξαρτώνται άμεσα από την ύπαρξη ή μη οπτικής επαφής (LOS: Line Of Sight)

Παρεμβολές ραδιοσημάτων: Οι παρεμβολές από ραδιοσήματα (Radio Signal Interfernece) διαχωρίζονται σε Εσωτερικές (inward) και Εξωτερικές (outward).

Διαχείριση ενέργειας: Θα πρέπει να επιλέγονται προϊόντα για σωστή διαχείριση ενέργειας, ώστε να μεγιστοποιείται η αυτονομία του δικτύου.

Ασυμβατότητα συστημάτων: Για το στήσιμο ενός WLAN θα πρέπει να λάβουμε υπόψη και την ασυμβατότητα μεταξύ προϊόντων διαφορετικών κατασκευαστών.

Προστασία της υγείας των χρηστών: Τα ασύρματα LAN που χρησιμοποιούν την τεχνική μετάδοσης με υπέρυθρες ακτίνες, θα πρέπει να περιορίζουν την ισχύ του εκπεμπόμενου σήματος στο ανώτερο όριο των 2 Watts, για να αποφευχθούν προβλήματα υγείας

Το πρόβλημα του κρυμμένου κόμβου: Το φαινόμενο αυτό παρατηρείται όταν υπάρχει ένας σταθμός που δεν μπορεί να ανιχνεύσει την δραστηριότητα ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται

Ασφάλεια δικτύου: Η συνολική λειτουργία ενός ασύρματου δικτύου εμπεριέχεται στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν ενυπάρχει με άλλες λειτουργίες όπως εγκατάσταση σύνδεσης ή άλλες υπηρεσίες (π.χ. login) που προσφέρουν τα ανώτερα στρώματα. Έτσι το μόνο θέμα που σχετίζεται με την ασφάλεια και τα ασύρματα δίκτυα είναι τα θέματα ασφαλείας των χαμηλότερων στρωμάτων, π.χ. κρυπτογράφηση (encryption) δεδομένων.

Για αυτό το λόγο, έχουν δημιουργηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν δύσκολη την υποκλοπή της πληροφορίας που μεταδίδεται.

Τέτοιες είναι οι τεχνικές εξάπλωσης φάσματος (spread spectrum) ενώ εάν απαιτείται περισσότερη ασφάλεια, καθορίζεται η χρήση της κωδικοποίησης WEP (Wired Equivalent Privacy). (Tanenbaum, 2000)

2.3 ΠΟΙΟΙ ΧΡΕΙΑΖΟΝΤΑΙ ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ;

Μερικοί από τους χώρους στους οποίους μπορούμε να δούμε θετικά αποτελέσματα με τη χρήση των ασύρματων δικτύων είναι οι παρακάτω:

Επιχειρήσεις: Μέσω της ασύρματης πρόσβασης, οι εργαζόμενοι σε μια επιχείρηση μπορούν να χρησιμοποιήσουν το κινητό δίκτυο για πρόσβαση σε e-mail, σε αρχεία και αναζήτηση στο Internet, ανεξάρτητα από την περιοχή που βρίσκεται το γραφείο.

Εκπαίδευση: Σε ακαδημαϊκούς χώρους οι φοιτητές έχουν πρόσβαση μέσω κινητών υπολογιστών σε πανεπιστημιακό δίκτυο ενώ εφαρμόζεται εύκολα και η τηλεκπαίδευση.

Υγεία: Οι εργαζόμενοι σε φορείς υγείας εκμεταλλεύονται τις υπηρεσίες ασύρματης πρόσβασης για την αναβάθμιση της εργασίας τους και την φροντίδα των ασθενών τους, καθώς περιορίζονται προβλήματα που σχετίζονται με τη γραφειοκρατία.

Επενδύσεις: Οι επενδυτές με έναν φορητό υπολογιστή μπορούν να δεχθούν πληροφορίες για τις τιμές σε πραγματικό χρόνο, βελτιώνοντας έτσι την εργασία τους αφού όλα γίνονται πιο άμεσα. (Ε.Μ.Πάλλης, 2000)

2.4 ΑΣΥΡΜΑΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Οι ασύρματες τεχνολογίες μπορούν να χωρισθούν σε διάφορες κατηγορίες, σύμφωνα με κριτήρια όπως:

- Το πρωτόκολλο που χρησιμοποιούν
- Το είδος σύνδεσης
- Το φάσμα συχνοτήτων στο οποίο λειτουργούν

Για την υλοποίηση ενός WLAN επιλέγεται ένα από τα πολλά πρότυπα που έχουν δημιουργήσει διάφοροι οργανισμοί και εταιρείες τα τελευταία χρόνια. Στη συνέχεια αναφέρονται τα κυριότερα.

• IEEE 802.11

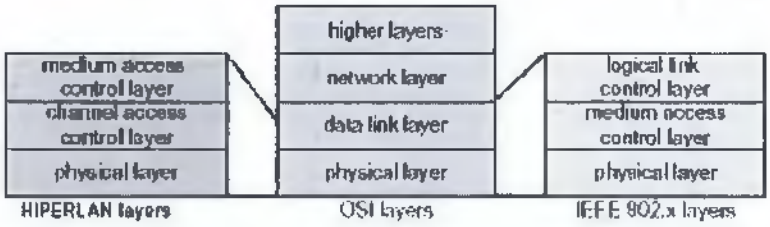
Το 1997 η IEEE κατέληξε στο πρώτο της πρότυπο για WLANs, το οποίο καθορίζει τον έλεγχο πρόσβασης μέσω (MAC) και τα φυσικά στρώματα (PHY) για ένα LAN με ασύρματη σύνδεση. Το 802.11-legacy έχει συχνότητα λειτουργίας στα 2.4 GHz και έχει ρυθμούς μετάδοσης δεδομένων 1 Mbps και 2 Mbps. Για την ασύρματη μεταφορά δεδομένων καθορίζονται οι υπηρεσίες ενός υποστρώματος MAC και τριών διαφορετικών φυσικών στρωμάτων. Το υποστρώμα MAC έχει 2 τρόπους λειτουργίας:

[1] http://en.wikipedia.org/wiki/Carrier_Sense_Multiple_Access_With_Collision_Avoidance

- Μία κατανεμημένη (distributed) λειτουργία (CSMA/CA[1])
- Μια συντονισμένη (coordinated) λειτουργία (polling mode)

- **HiperLAN**

Το HiperLAN εδραιώθηκε το 1996 από την ETSI[2] (European Telecommunications Standards Institute). Η πρώτη έκδοση είναι το HiperLAN I. Το πρότυπο λειτουργεί στην μπάντα από 5.1 έως 5.3 GHz και ο ρυθμός σηματοδοσίας φτάνει τα 24 Mbps. Το πρωτόκολλο χρησιμοποιεί διαφορετική εκδοχή του CSMA/CA, που βασίζεται στο χρόνο ζωής του πακέτου, την προτεραιότητα και τις αναμεταδόσεις στο επίπεδο MAC. Στο επόμενο σχήμα δίνεται η συσχέτιση των διάφορων στρωμάτων στα δυο κυριότερα πρότυπα (HiperLAN και 802.11x) σύμφωνα με την αρχιτεκτονική OSI.



Εικόνα 2. Σχηματική σύγκριση των στρωμάτων των Standards HiperLAN και 802.11 με τα στρώματα της αρχιτεκτονικής OSI.

- **OpenAir**

Η εταιρεία Proxim[3] προώθησε το πρότυπο OpenAir, το οποίο είναι προγενέστερο του 802.11 και χρησιμοποιεί την τεχνική του Frequency Hopping με ρυθμούς δεδομένων 0.8 και 1.6 Mbps (χρησιμοποιώντας τεχνικές διαμόρφωσης 2FSK και 4FSK). Το πρωτόκολλο που χρησιμοποιείται είναι CSMA/CA και προαιρετικά βασίζεται στην ανταλλαγή RTS/CTS πακέτων.

- **HomeRF SWAP**

Η HomeRF, μια ομάδα από εταιρίες που δημιουργήθηκε για την διεύρυνση της χρήσης των WLAN στο σπίτι, έχει αναπτύξει ένα νέο πρωτόκολλο για τον σκοπό αυτό, το οποίο ονομάζεται SWAP (Shared Wireless Access Protocol).

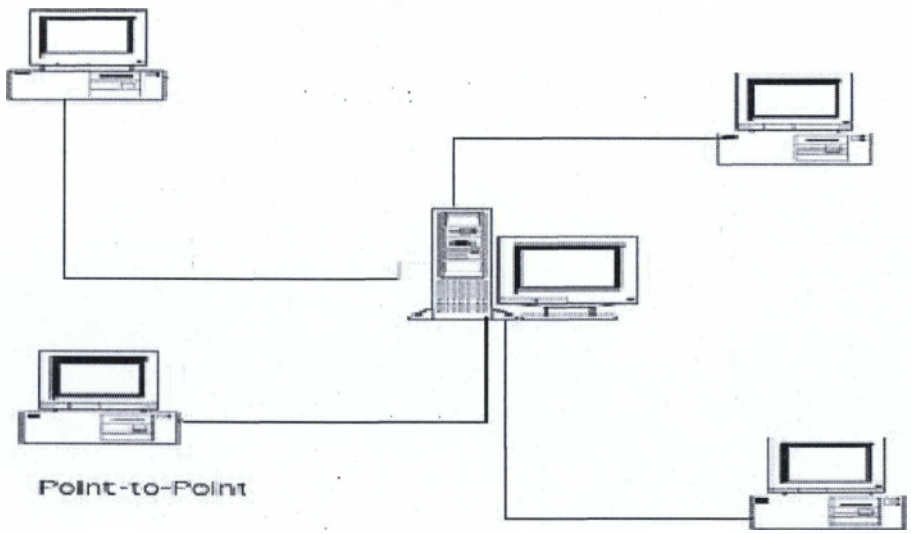
[2] http://en.wikipedia.org/wiki/European_Telecommunications_Standards_Institute

[3] http://www.proxim.com

Το SWAP χρησιμοποιεί ένα νέο πρωτόκολλο στο υποστρώμα MAC, το οποίο συνδυάζει χαρακτηριστικά και λειτουργίες από το DECT (ένα πρότυπο της ETSI για ψηφιακά ασύρματα τηλέφωνα) και το 802.11. Η συχνότητα λειτουργίας είναι τα 2.4 GHz, ενώ χρησιμοποιείται η τεχνική FHSS, υποστηρίζοντας ρυθμούς δεδομένων της τάξης των 1 Mbps και 2 Mbps.

• **Ασύρματα Point-to-Point δίκτυα**

Ο κυριότερος εκπρόσωπος των ασύρματων δικτύων με σύνδεση από σημείο-σε-σημείο (point-to-point) είναι τα ασύρματα μητροπολιτικά δίκτυα WMANs (Wireless Metropolitan Area Networks), τα οποία χρησιμοποιούν τεχνολογίες που ομοιάζουν πολύ με αυτές των WLAN. Η σύνδεση που χρησιμοποιείται συνήθως φαίνεται στο επόμενο σχήμα.



Εικόνα 3. Δίκτυο Point to Point

Χρησιμοποιώντας κατευθυντικές κεραίες και τεχνικές διαμόρφωσης όπως η 'spread spectrum', τα δίκτυα αυτά μπορούν να υποστηρίξουν μετάδοση σε αποστάσεις μέχρι και 30 μίλια, απόσταση πάντως που μειώνεται αισθητά από διάφορους παράγοντες όπως οι καθυστερήσεις μετάδοσης και τα διάφορα εμπόδια και παρεμβολές. Ο ρυθμός μετάδοσης για τα WMAN μπορεί να φτάσει τα 11 Mbps για ζεύξεις των 2-3 μιλίων.

• **Ασύρματα Point-to-Multipoint δίκτυα**

Τα δίκτυα αυτά στηρίζονται στην διασύνδεση ασύρματων (κινητών ή μη) χρηστών με μια σταθερή περιοχή στην οποία βρίσκεται ο παροχέας των υπηρεσιών (Service Provider), τις οποίες μοιράζονται οι ασύρματοι χρήστες. Δύο από τις πλέον αναπτυσσόμενες τεχνολογίες τέτοιου είδους ασύρματων δικτύων είναι και οι:

MMDS (Multichannel Multipoint Distribution Service), η οποία λειτουργεί στην περιοχή συχνοτήτων 2.1-2.7 GHz, ενώ μπορεί να υποστηρίξει ρυθμό δεδομένων έως και 10 Mbps σε ακτίνα 35 μιλίων.

LMDS (Local Multipoint Distribution Service), η οποία λειτουργεί σε διάφορες συχνότητες (από 24 μέχρι 40 GHz), ενώ μπορεί να υποστηρίξει ρυθμούς μέχρι και 155 Mbps σε ακτίνα λειτουργίας των 2 μιλίων.

Η τεχνολογία LMDS (Local Multipoint Distribution System) είναι ένα ασύρματο σύστημα επικοινωνίας ευρείας ζώνης point-to-multipoint και ανήκει σε μία κατηγορία ασύρματων τεχνολογιών που καλείται WLL (Wireless Local Loop) που λειτουργεί σε συχνότητες μεγαλύτερες των 20 GHz. Η τεχνολογία αυτή χρησιμοποιείται για την παροχή ψηφιακών αμφίδρομων υπηρεσιών όπως μετάδοση δεδομένων, φωνής, video και Internet.

Το βασικό δομικό στοιχείο μιας τέτοιας αρχιτεκτονικής είναι το κελί (cell) στο οποίο λαμβάνει χώρα η ασύρματη επικοινωνία. Κάθε κελί στο σύστημα έχει έναν σταθμό βάσης (AP: Access Point) ή hub, ο οποίος αναφέρεται και ως central hub και βρίσκεται στο CMN (Central Main Node). Σε κάθε κελί υπάρχουν από λίγες έως πολλές απομακρυσμένες μονάδες (remote units) οι οποίες αντιπροσωπεύουν ουσιαστικά τους χρήστες.

Η επικοινωνία και η διαχείριση των μονάδων αυτών γίνεται με τη βοήθεια του AP, η σύνδεση με τον οποίο γίνεται με την βοήθεια ενός SA (Station Adapter). Αξίζει να αναφέρουμε πως στο AP μπορεί να συνδεθεί και ένα ενσύρματο δίκτυο μέσω μιας ασύρματης γέφυρας (WB: Wireless Bridge). Καθώς η τεχνολογία LMDS δείχνει να εφαρμόζεται ολοένα και περισσότερο στα ασύρματα δίκτυα ευρείας περιοχής, ενώ μέρος της υποστήριξής της μπορεί να υλοποιηθεί με την χρήση ασύρματων δικτύων που στηρίζονται 802.11, αποφασίσαμε να την μοντελοποιήσουμε και να την προσομοιώσουμε στα πλαίσια της παρούσας εργασίας

Bluetooth

• Το Bluetooth εκδόθηκε από την ομάδα Bluetooth Special Interest Group με την βοήθεια μερικών μεγάλων εταιρειών όπως Ericsson, IBM, Intel κ.α. Το Bluetooth δεν είναι πρωτόκολλο για ασύρματα δίκτυα αλλά βρίσκει εφαρμογές στα ασύρματα προσωπικά δίκτυα WPANs (Wireless Personal Area Networks), που έχουν ακτίνα δράσης έως και 10 μέτρα. Το Bluetooth λειτουργεί στην μπάντα των 2.4 GHz, χρησιμοποιώντας ως τεχνική διαμόρφωσης την FHSS και ο ρυθμός μετάδοσης δεδομένων φτάνει το 1 Mbps.

• Τεχνολογία MIMO

Η τεχνολογία MIMO (Multiple Input Multiple Output) έχει ως στόχο να βελτιώσει την ακτίνα δράσης, την ισχύ του σήματος και στην αξιοπιστία του WLAN. Η MIMO τεχνολογία χρησιμοποιεί πολλαπλές κεραίες εκπομπής και πολλαπλές κεραίες λήψης.

• WIMAX

Η τεχνολογία **WIMAX** ανήκει σε μια νέα οικογένεια προτύπων. Η προηγούμενη πρωτοεμφανίστηκε το 2001, όταν το πρώτο 802.16 πρότυπο εγκρίθηκε και το ακολούθησαν τα πρότυπα 802.16a, 802.16b και 802.16c προκειμένου να βελτιωθούν θέματα που σχετίζονταν με το φάσμα συχνοτήτων, την ποιότητα εξυπηρέτησης και τη διαλειτουργικότητα.

Τον 2003 αναπτύχθηκε το 802.16d για να αντιμετωπίσει ζητήματα του ETSI, ενώ το 2004 δημοσιοποιήθηκε το 802.16-2004, το οποίο και αναίρεσε όλες τις προηγούμενες εκδόσεις του προτύπου. Η τελευταία εξέλιξη είναι το πρότυπο 802.16e το οποίο ενεκρίθη το 2005 και δημοσιεύθηκε το 2006. Αν και θεωρητικά δεν αναιρεί το πρότυπο 802.16-2004, αυτό ισχύει πρακτικά. (Ε.Μ.Πάλλης, 2000)

2.5 ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ

Για την δημιουργία ενός ασύρματου τοπικού δικτύου είναι απαραίτητη κάποια υλικοτεχνική υποδομή, μιλάμε για διάφορα στοιχεία (components) που συντονίζουν την μετάδοση, λήψη και επεξεργασία του σήματος μεταξύ των χρηστών. Η δομή αυτή περιλαμβάνει τόσο το λογισμικό (software) όσο και τον ανάλογο υλικό εξοπλισμού (hardware). Οι κατηγορίες των στοιχείων αυτών αναφέρονται στη συνέχεια.

• **Συσκευές χρηστών (End-user devices)**

Η επικοινωνία των διαφόρων εφαρμογών και υπηρεσιών με τους χρήστες σε ένα ασύρματο δίκτυο γίνεται μέσω συγκεκριμένων συσκευών. Είτε το δίκτυο είναι ασύρματο ή ενσύρματο, οι συσκευές αποτελούν την πηγή επικοινωνίας μεταξύ του χρήστη και του δικτύου. Τέτοιες συσκευές είναι οι επόμενες:

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

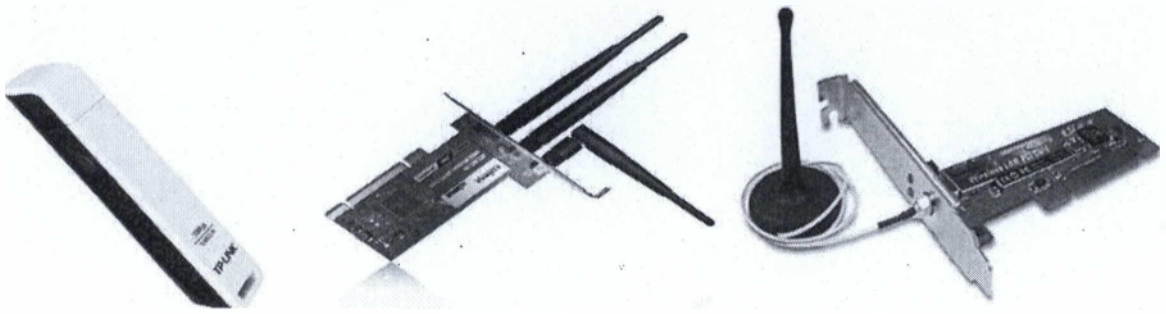
• **Λογισμικό δικτύου (Network Software)**

Ένα ασύρματο δίκτυο είναι δομημένο με το κατάλληλο λογισμικό που βρίσκεται σε διάφορα μέρη του δικτύου. Ένα σύστημα διαχείρισης δικτύου (NOS: Network Operating System), όπως είναι για παράδειγμα το Microsoft NT Server, παρέχει διαφόρων ειδών υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.ά.

Αυτά τα συστήματα στηρίζονται στην ύπαρξη ενός εξυπηρετητή (server), ο οποίος διαθέτει τις τις βάσεις δεδομένων στις οποίες μπορούν να έχουν πρόσβαση οι διάφορες συσκευές τις οποίες ελέγχει ο χρήστης. Οι τελευταίες «τρέχουν» το δικό τους λογισμικό (client software), το οποίο κατευθύνει τις εντολές του χρήστη στον εξυπηρετητή.

• **Ασύρματες κάρτες δικτύου (Wireless NICs)**

Η ασύρματη κάρτα δικτύου (Wireless Network Interface Card) χρησιμοποιείται για την μετάδοση του ψηφιακού σήματος ενός υπολογιστή μέσω του ασύρματου μέσου σε έναν άλλο υπολογιστή. Στην διαδικασία αυτή συμπεριλαμβάνεται η διαμόρφωση και η ενίσχυση του σήματος.



Εικόνα 4. Ασύρματες Κάρτες Δικτύου

Η κάρτα δικτύου μοιάζει με μια τυπική κάρτα δικτύου (είτε σε ISA ή PCI για σταθερούς υπολογιστές, είτε σε PC Card για φορητούς) με μια μικρή κεραία

Μερικές εταιρίες παράγουν κάρτες οι οποίες συνδέονται με τον υπολογιστή μέσω μιας RS-232 σειριακής ή παράλληλης θύρας. Η διασύνδεση της ασύρματης κάρτας με την συσκευή του χρήστη συμπεριλαμβάνει και έναν οδηγό λογισμικού (software driver) που συνδέει το λογισμικό του NOC στην κάρτα.

- **Σημεία πρόσβασης (access points):**

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

Εικόνα 5. Linksys WAP54G 802.11g Wireless Access Point (αριστερά) – Βιομηχανικό σχέδιο Wireless Access Point (δεξιά)

Τα σημεία πρόσβασης περιλαμβάνουν χαρακτηριστικά ασφάλειας όπως επικύρωση και κρυπτογράφηση, έλεγχο πρόσβασης που βασίζεται σε λίστες ή φίλτρα καθώς και πολλά άλλα τα οποία συνήθως απαιτούν τη ρύθμιση τους από τον χρήστη σύμφωνα με τις προτιμήσεις του, συνήθως χρησιμοποιώντας μια διεπαφή βασισμένη στο διαδίκτυο. Πολλά σημεία πρόσβασης περιλαμβάνουν επιπρόσθετα χαρακτηριστικά δικτύωσης όπως πύλες διαδικτύου, κόμβους μεταγωγής, ασύρματες γέφυρες ή επαναλύπτες. Στην εικόνα βλέπουμε μερικά σημεία πρόσβασης. (Held, 2003)

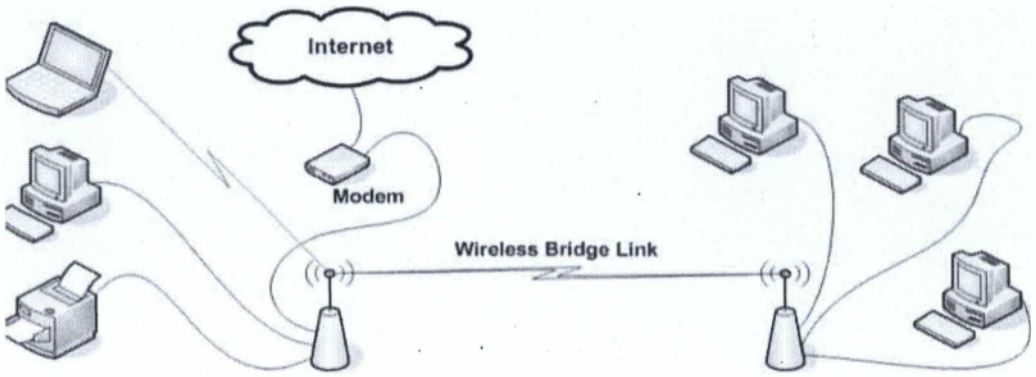
- **Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges)**

Οι ασύρματες τοπικές γέφυρες είναι πολύ σημαντικό κομμάτι της τοπολογίας ενός δικτύου καθώς συνδέουν πολλά τοπικά δίκτυα μεταξύ τους στο επίπεδο του υποστρώματος MAC για την δημιουργία ενός εκτενέστερου και πιο λειτουργικού δικτύου. Οι γέφυρες χωρίζονται σε δύο κατηγορίες:

Local bridges: Δημιουργία σύνδεσης ανάμεσα σε κοντινά τοπικά δίκτυα

Remote bridges: Δημιουργία σύνδεσης ανάμεσα δίκτυα που χωρίζονται από αποστάσεις

μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα των τοπικών δικτύων.



Εικόνα 6. Συνδεσμολογία δικτύου με Ασύρματη Τοπική Γέφυρα

Συνήθως οι γέφυρες, οι οποίες είναι συσκευές που χρησιμεύουν στην διασύνδεση ασύρματου με ενσύρματου δικτύου, αλλά και τη διασύνδεση πολλών WLAN μεταξύ τους, αναφέρονται ως APs (Access Points).

- **Κεραίες (Antennas)**

Οι κεραίες χρησιμεύουν στην εκπομπή του διαμορφωμένου σήματος μέσω του αέρα. Γενικά, οι κεραίες χωρίζονται σε πολλά είδη και μεγέθη και χαρακτηρίζονται από:

- Ισχύς μετάδοσης (Transmit power)
- Εύρος ζώνης (Bandwidth)
- Μοντέλο διάδοσης (propagation pattern)
- Ευαισθησία (Gain)

Ο τρόπος που μεταδίδει το σήμα μια κεραία καθορίζει επίσης και την περιοχή κάλυψης της. Για την μετάδοση του σήματος στα ασύρματα δίκτυα χρησιμοποιούνται κυρίως δύο είδη κεραιών:

Πολυκατευθυντική (omnidirectional) κεραία: Πρόκειται για κεραίες που διοχετεύουν την ισχύ τους προς κάθε κατεύθυνση. Αθροιστικά έχουν την ίδια ενίσχυση προς κάθε κατεύθυνση. Το πρότυπο εκπομπής τους είναι τέτοιο, ώστε να δημιουργούν γύρω τους ένα πεδίο που μοιάζει με «ιπτάμενο δίσκο».

Μονοκατευθυντική (directional) κεραία: συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση. (Ε.Μ.Πάλλης, 2000)

2.6 ΤΟ ΠΡΟΤΥΠΟ IEEE 802.11

Το πρώτο πρότυπο ασύρματων τοπικών δικτύων το IEEE 802.11, το οποίο καθορίζει τον έλεγχο πρόσβασης μέσω (MAC) και τα φυσικά στρώματα (PHY) για ένα LAN με ασύρματη σύνδεση, υιοθετήθηκε το 1997. Σύμφωνα με αυτό το πρότυπο, εξετάζεται η τοπική ασύρματη δικτύωση συσκευών που βρίσκονται κοντά.

Από την αρχική του έκδοση, IEEE 802.11, το πρότυπο έχει επεκταθεί σε πολυάριθμες ομάδες, που καθορίζονται από τα γράμματα a μέχρι το i.

- **Η Οικογένεια**

Στα τέλη του 1999 η IEEE κοινοποίησε δύο νέα συμπληρωματικά πρότυπα για WLANs, τα 802.11a, 802.11b, 802.11g και 802.11y:

- Το 802.11a έχει καθοριστεί έτσι ώστε να υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps (ονομαστικός ρυθμός μετάδοσης), με συνήθη ρθυμό μετάδοσης 23 Mbits/s, εμβέλεια εσωτερικού χώρου έως και 35 m και χρήση της τεχνικής διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) στην μπάντα των 5,7 GHz.

- Το 802.11b είναι ουσιαστικά ο αντικαταστάστης του αρχικού 802.11 καθώς υποστηρίζει ρυθμούς δεδομένων έως και 11 Mbps, εμβέλεια εσωτερικού χώρου έως και 35 m και χρησιμοποιεί ως διαμόρφωση την τεχνική DSSS (direct-sequence spread spectrum) στα 2.4 GHz. (References)

- Επίσης το 2003, η IEEE κοινοποίησε το πρότυπο 802.11g, το οποίο υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps (ονομαστικός ρυθμός μετάδοσης), με συνήθη ρυθμό μετάδοσης 19 Mbits/s, εμβέλεια εσωτερικού χώρου έως και 38 m με την τεχνική OFDM στα 2.4 GHz.

- Για το 2008, προτάθηκε από την IEEE το πρότυπο 802.11y, το οποίο χρησιμοποιεί

την τεχνική MIMO(Multiple – Input Multiple -Output) με συχνότητα 3,7 GHz, ρυθμό μετάδοσης 54Mbits/s και εμβέλεια 5000 m

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

- Οι σπουδαιότερες είναι: 802.11f ή IAPP, το οποίο επιτρέπει άμεση επικοινωνία μεταξύ διαφορετικών AP ώστε να εξαλειφθεί η απώλεια πλαισίων κατά τη μεταγωγή.

- 802.11e ή QoS το οποίο προσπαθεί να διασφαλίσει ποιότητα υπηρεσιών για εφαρμογές πραγματικού χρόνου που εκτελούνται πάνω σε ένα WLAN ελαχιστοποιώντας ή μεγιστοποιώντας ένα από τα παρακάτω κριτήρια: μέση καθυστέρηση από άκρο σε άκρο, μέση μεταβολή της καθυστέρησης ή μέσο ποσοστό επιτυχούς παράδοσης πλαισίων. Αυτό το επιτυγχάνει βελτιώνοντας τους μηχανισμούς DCF και PCF με τους μηχανισμούς EDCF, ο οποίος αναθέτει προτεραιότητες στα πλαίσια δεδομένων ανάλογα με το πόσο χρονικά κρίσιμη είναι η παράδοσή τους και με τα μεγαλύτερης προτεραιότητας πλαίσια να έχουν περισσότερες πιθανότητες να κερδίσουν στον ανταγωνισμό για την πρόσβαση στο κοινό μέσο, και HCF, ο οποίος περιορίζει τον μέγιστο χρόνο δέσμευσης του καναλιού από ένα τερματικό, αντίστοιχα.

- 802.11n, το οποίο με χρήση πολλαπλών κεραιών (μέθοδος γνωστή ως MIMO, εκ του Multiple Inputs Multiple Outputs) παρέχει ονομαστικό ρυθμό μετάδοσης τουλάχιστον 108 Mbps. Το πρότυπο οριστικοποιήθηκε το 2009. (Wikipedia)

Σε γενικές γραμμές, η εξελικτική πορεία των προτύπων φαίνεται στον παρακάτω πίνακα:

802.11	802.11a	802.11b	802.11g	802.11n	802.11y

Μπάντα Modulation	2,4 GHz	5,7 GHz OFDM	2,4 GHz DSSS	2,4 GHz OFDM	2,4 ή 5 GHz MIMO – OFDM	3,7 GHz
Ρυθμός Μετάδοσης	2 Mbps	<54 Mbps	<11 Mbps	<54 Mbps	<248 Mbps	<54 Mbps
Απόσταση	20 m	35 m	35 m	35 m	70 m	5000 m
Χρονιά	1.997	1999	1999	2003	2009	2008

- **Χαρακτηριστικά του IEEE 802.11**

Η ζώνη συχνοτήτων των 2.4 GHz σήμερα είναι ιδιαίτερα δημοφιλής. Αυτό συμβαίνει διότι πρόκειται για ελεύθερη ζώνη που έχει συγκεκριμένα χαρακτηριστικά που χρησιμεύουν για μετάδοση σε μικρές αποστάσεις.

- **Εμβέλεια**

Η εμβέλεια ενός τοπικού ασύρματου δικτύου σε εσωτερικούς χώρους κυμαίνεται από τα 20-38 μέτρα. Τα ραδιοκύματα όμως θα πρέπει να διαπεράσουν τοίχους και οροφές, οπότε έχουμε σημαντικές απώλειες. Επίσης το σήμα ανακλάται από τις προσπίπτουσες επιφάνειες.Σε περιβάλλον όμως με οπτική επαφή (Line Of Sight), σε εξωτερικό χώρο, η εμβέλεια του ασύρματου δικτύου είναι μεγαλύτερη και εξαρτάται από διάφορους παράγοντες που σχετίζονται με τις συσκευές όπως την ευαισθησία του δέκτη, την ποιότητα των κεραιών και την ευθυγράμμιση τους, το επίπεδο παρεμβολών και θορύβου.

- **Ρυθμός μετάδοσης**

Ο ρυθμός μετάδοσης του σήματος εξαρτάται από διάφορους παράγοντες όπως οι παράμετροι ραδιομετάδοσης (εμβέλεια, ανακλάσεις, απορρόφηση και σκέδαση), αλλά και ο αριθμός των χρηστών.

- **Ποιότητα επικοινωνίας**

Μετά από εκατοντάδες εμπορικές και στρατιωτικές εφαρμογές, οι τεχνολογίες ασύρματης μετάδοσης έχουν γίνει πολύ αξιόπιστες. Αυτές μπορούν να παρέχουν στους χρήστες τους αξιόπιστες συνδέσεις και σε καλύτερο επίπεδο από ότι οι αντίστοιχες στην κινητή τηλεφωνία.

- **Συμβατότητα με το υπάρχον δίκτυο**

Τα πιο πολλά ασύρματα δίκτυα έχουν συγκεκριμένο τρόπο διασύνδεσης με τα ενσύρματα δίκτυα.

Έτσι η προσάρτηση ασύρματης δικτύωσης, σε υπάρχουσες δομές δικτύων, μπορεί να γίνει με εύκολο τρόπο.

- **Παρεμβολές**

Το ασύρματο τοπικό δίκτυο μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλες συσκευές που λειτουργούν στα 2.4GHz όπως άλλα ασύρματα δίκτυα, ασύρματα τηλέφωνα, φούρνοι μικροκυμάτων και συσκευές Bluetooth. Σημαντικότερες όμως είναι οι παρεμβολές που προκύπτουν από την κακή σχεδίαση ενός ασύρματου δικτύου. Για τον παραπάνω λόγο χρησιμοποιείται το 802.11a όπου είναι πιο καθαρη μπάντα.

- **Διαλειτουργικότητα**

Οι περιπτώσεις κατά τις οποίες οι συσκευές δε συνεργάζονται μεταξύ του είναι:

- **Διαφορετικές τεχνολογίες**

Μια μετάδοση βασισμένη σε τεχνολογία FHSS δεν μπορεί να συνεργαστεί με κάποια που βασίζεται σε τεχνολογία DSSS

- **Διαφορετικές συχνότητες**

Συσκευές που λειτουργούν σε συχνότητα 5 (5,4 ή 5.7) GHz δεν μπορούν να δουλέψουν μαζί με συσκευές που εργάζονται στα 2.4GHz.

- **Διαφορετικές υλοποιήσεις**

Συσκευές που προέρχονται από διαφορετικούς κατασκευαστές μπορεί να μην συνεργάζονται ή να συνεργάζονται μερικώς μεταξύ τους. Μια προσέγγιση στη λύση του προβλήματος είναι η δημιουργία του πιστοποιητικού Wi-Fi.

Μία λύση που εξετάζεται είναι η πρόταση της IEEE για τη διαπομπή σε ετερογενή δίκτυα. Μια ομάδα της IEEE ασχολείται με την επίτευξη διαπομπής και συμβατότητας μεταξύ δικτύων με διαφορετικό τύπο τεχνολογίας, που μπορεί να ανήκει τόσο στο σύνολο των 802 προτύπων της IEEE όσο και σε άλλα πρότυπα (π.χ. κυψελωτά). Η κατεύθυνση στην οποία κινείται η ομάδα αυτή αναφέρεται ως Διαπομπή Ανεξάρτητη του Μέσου MIH (Media Independent Handover), ενώ το σύνολο των σχετικών προτύπων είναι γνωστά ως IEEE 802.21.

Γενικότερα τα τελευταία χρόνια, ο στόχος διάφορων ερευνητικών σταθμών είναι οι έρευνες με στόχο την άυξηση της ευελιξίας των ασύρματων επικοινωνιών. Η τεχνολογία του Cognitive Radio ή Γνωστικά Συστήματα Ραδιοεπικοινωνιών αποβλέπει στην βελτίωση της επικοινωνίας, επιτρέποντας στα ασύρματα δίκτυα να διαθέτουν ευφυΐα – νοημοσύνη για να προσαρμόζονται κατάλληλα στις συνθήκες λειτουργίας. (Κατσαβριάς, 2009)

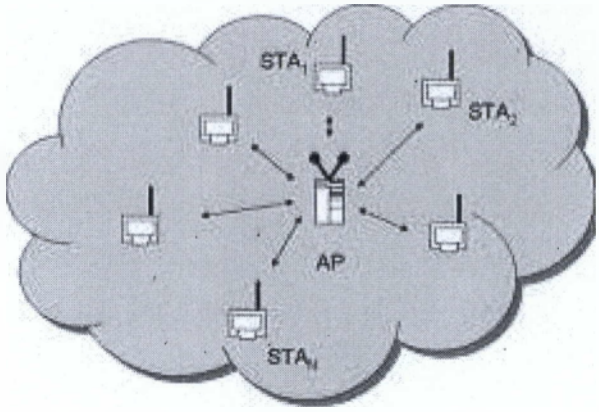
- **Η Τοπολογία του 802.11**

Η τοπολογία του 802.11 αποτελείται από στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο που να παρέχει τη δυνατότητα μετακίνησης των σταθμών η οποία να μην γίνεται αντιληπτή από τα ανώτερα στρώματα, όπως το LLC (Logical Link Control). Ένας σταθμός (station) είναι κάθε συσκευή η οποία εμπεριέχει τις λειτουργίες του 802.11 (δηλαδή το επίπεδο MAC, το φυσικό στρώμα και μια διασύνδεση (interface) με το ασύρματο μέσο).

Οι λειτουργίες του 802.11 ενυπάρχουν (reside) σε μια ασύρματη κάρτα δικτύου NIC (Network Interface Card), το λογισμικό διασύνδεσης που οδηγεί την κάρτα NIC και τον σταθμό βάσης ή AP (Access Point).

- **BSS**

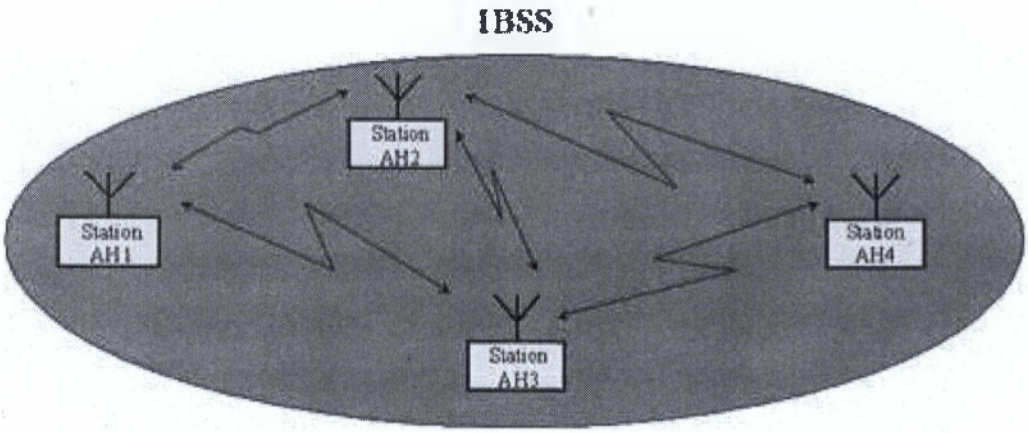
Το βασικό δομικό στοιχείο ενός IEEE 802.11 LAN είναι το BBS (Basic Service Set). Στο παρακάτω σχήμα φαίνεται ένα BSS, το οποίο έχει N σταθμούς (STA) οι οποίοι είναι μέλη του BSS. Αν ένας σταθμός μετακινηθεί έξω από το BSS δεν μπορεί πλέον να επικοινωνεί άμεσα με τα άλλα μέλη του συγκεκριμένου BSS.



Εικόνα 7. Σχηματική αναπαράσταση ενός BSS.

- **IBSS, Independent Basic Service Set ή Peer-to-Peer ή Ad-Hoc**

Πρόκειται μια πολύ απλή τοπολογία για ασύρματα δίκτυα. Οι σταθμοί είναι ίσοι μεταξύ τους και επικοινωνούν ένας προς έναν χωρίς να υπάρχει κεντρικός σταθμός επικοινωνίας.



Εικόνα 8. Σχηματική αναπαράσταση ενός IBSS

Ωστόσο απαραίτητη προϋπόθεση για την σωστή λειτουργία ενός τέτοιου συστήματος είναι ο κάθε σταθμός να βρίσκεται εντός της εμβέλειας του άλλου. Το σύστημα IBSS είναι χρήσιμο σε περιπτώσεις που είτε δεν υπάρχει ασύρματη υποδομή και δεν χρειάζεται είτε οι περιοχές που πρόκειται να καλυφθούν είναι περιορισμένες.

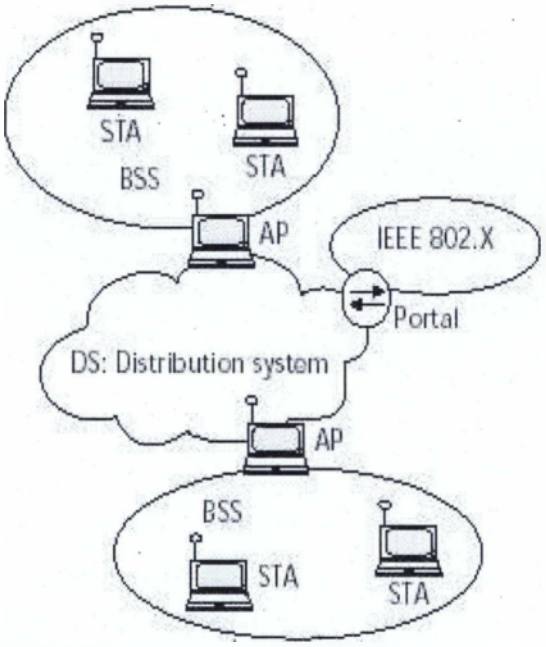
- **DS, Distribution System**

Με τον όρο DS εννοούμε ένα σύστημα διανομής. Πρόκειται για ένα δίκτυο το οποίο συνδέει τους σταθμούς βάσης τόσο μεταξύ τους όσο και με τα υπόλοιπα δίκτυα. Η πολύ μεγάλη ευελιξία στη σχεδίαση είναι ένα από τα βασικά πλεονεκτήματα της συγκεκριμένης τεχνολογίας.

- **ESS, Extended Service Set**

Όταν οι υπηρεσίες ενός συστήματος IBSS δεν είναι αρκετές, τότε στρεφόμαστε σε στην πιο σύνθετη δομή ενός τοπικού δικτύου, που ονομάζεται ESS (Extended Service Set). Με τη βοήθεια αυτού του συστήματος είναι δυνατή η διασύνδεση και η επικοινωνία πολλών BSS μεταξύ τους. Το στοιχείο που χρησιμοποιείται για την διασύνδεση των BSS είναι το σύστημα διανομής DS.

Η πρόσβαση στο σύστημα διανομής γίνεται με την βοήθεια ενός σταθμού AP, ο οποίος παρέχει τη διασύνδεση των σταθμών που βρίσκονται σε διάφορα BSS στο σύστημα διανομής. Η διασύνδεση



αυτή φαίνεται στο επόμενο σχήμα.

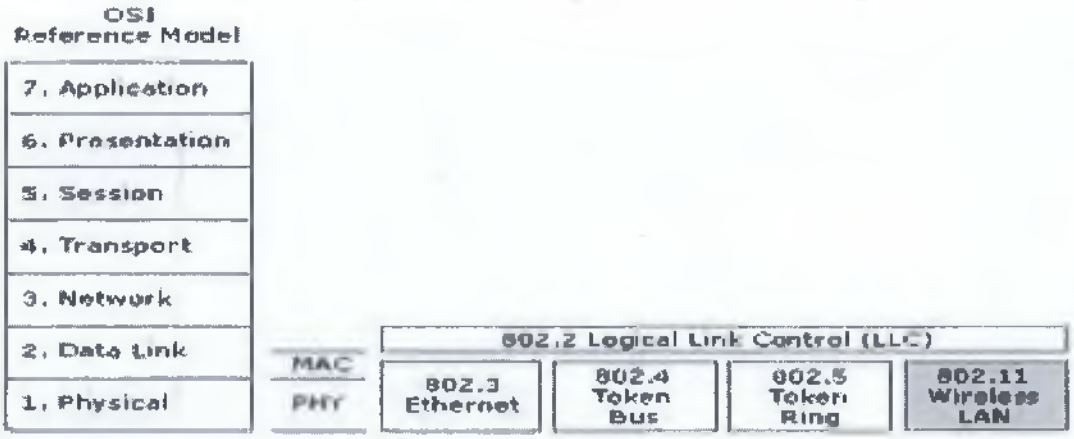
Εικόνα 9. Η σύνδεση των BSSs με το DS

Η πληροφορία μετακινείται από BSS σε BSS μέσω των AP του συστήματος διανομής, ενώ το σύστημα διανομής υποστηρίζει τους τύπους κίνησης του 802.11 παρέχοντας υπηρεσίες ικανές να ελέγχουν την αντιστοίχηση (mapping) της διεύθυνσης στον προορισμό για κάθε σταθμό που

μετακινείται.

- **Η Αρχιτεκτονική του 802.11**

Ενώ η τοπολογία καθορίζει τα αναγκαία μέσα για τη φυσική διασύνδεση του ασύρματου δικτύου, η αρχιτεκτονική καθορίζει τον τρόπο λειτουργίας του δικτύου. Η επιτροπή των IEEE 802.11 προτύπων ορίζει δύο χωριστά στρώματα, το στρώμα Logical Layer Control (LLC) -Έλεγχος Λογικού Συνδέσμου και το Media Access Control (MAC) -Ελέγχου Προσπέλασης Μέσων, αντίστοιχα για το επίπεδο της μετάδοσης δεδομένων (Data Link Layer) του μοντέλου OSI[4]. Το ασύρματο πρότυπο IEEE 802.11 ορίζει τις προδιαγραφές για το φυσικό στρώμα και για το MAC στρώμα που επικοινωνούν μέχρι το στρώμα LLC.



Εικόνα 10. Αντιστοιχία OSI με 802.11

Τα πρωτόκολλα που χρησιμοποιούνται από όλες τις παραλλαγές του 802, συμπεριλαμβανομένου του Ethernet, έχουν κάποια κοινά σημεία στη δομή τους.

- **Φυσικό Επίπεδο (Physical Layer)**

Το πρότυπο 802.11 του 1997 καθορίζει πέντε επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο:

[4] http://en.wikipedia.org/wiki/OSI_model

- Υπέρυθρες

- FHSS (Frequency Hopping Spread Spectrum[5])
- DHSS (Direct Sequence Spread Spectrum[6])
- OFDM (Orthogonal Frequency-Division Multiplexing[7])
- HR-DSSS (High Rate Direct Sequence Spread Spectrum[8])

Όλες αυτές οι τεχνικές λειτουργούν σε 1 ή 2 Mbps και με αρκετά χαμηλή ισχύ, έτσι ώστε να μην παρουσιάζουν πολλές διενέξεις. Το 1999 παρουσιάστηκαν δύο νέες τεχνικές για επίτευξη υψηλότερου εύρους ζώνης. Οι τεχνικές αυτές ονομάζονται OFDM και HR-DSSS. Λειτουργούν μέχρι τα 54 Mbps και τα 11 Mbps, αντίστοιχα.

Το φυσικό επίπεδο είναι όμοιο με το φυσικό επίπεδο του OSI, όμως το επίπεδο συνδέσμου μετάδοσης δεδομένων σε όλα τα πρωτόκολλα 802 χωρίζεται σε δυο ή περισσότερα υποεπίπεδα. Στο 802.11, το υποεπίπεδο MAC ορίζει ποιος θα μεταδίδει κάθε φορά. Πάνω από αυτό βρίσκεται το υποεπίπεδο LLC, δουλειά του οποίου είναι να κρύβει διαφορές ανάμεσα στις παραλλαγές του 802.

• Το επίπεδο σύνδεσης δεδομένων (Data Link Layer)

Το επίπεδο σύνδεσης δεδομένων εφαρμόζεται σε όλους τους 802.11 σταθμούς και επιτρέπει στο σταθμό να εγκαθιδρύει ένα δίκτυο ή να συμμετέχει σε ένα ήδη υπάρχον δίκτυο και να μεταφέρει δεδομένα που περνούν από το επίπεδο λογικής σύνδεσης ελέγχου (LLC).

- Αυτές οι λειτουργίες γίνονται χρησιμοποιώντας δύο μεθόδους υπηρεσιών, τις υπηρεσίες σταθμών (Station Services) και τις υπηρεσίες των συστημάτων διανομής (Distribution System Services). Πριν όμως αρχίσουν να πραγματοποιούνται οι υπηρεσίες του MAC επιπέδου, πρώτα πρέπει να πραγματοποιηθεί η πρόσβαση στο ασύρματο μέσο. Το υπόστρωμα MAC παρέχει τις ακόλουθες βασικές λειτουργίες:Τον έλεγχο της πρόσβασης των σταθμών στο κοινό μέσο μετάδοσης.

[5] http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

[6] http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum

[7] http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing

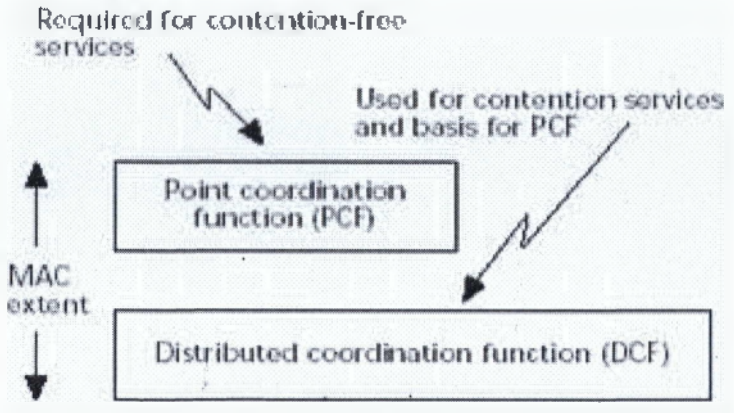
[8] http://www.wireless-center.net/WLANs-WPANs/1472.html

- Τη λειτουργία της αναμετάδοσης του πακέτου.
- Τη λειτουργία της επιβεβαίωσης λήψης.
- Τη λειτουργία του κατακερματισμού και της επανασυναρμολόγησης του πακέτου.

- **Η Πρόσβαση προσβαση στο Ασύρματο Μέσο**

Σε ένα ασύρματο δίκτυο είναι πιο περίπλοκο να μοιράζουμε την πρόσβαση μεταξύ των σταθμών διανομής από ότι σε ένα ενσύρματο. Αυτό συμβαίνει επειδή ένας ασύρματος σταθμός δεν είναι σε θέση να ανιχνεύσει μια σύγκρουση που μπορεί να συμβεί στη μετάδοση του με την μετάδοση ενός άλλου σταθμού. Σε ένα ενσύρματο δίκτυο είναι εύκολο να ανιχνευτούν τυχόν συγκρούσεις με τον μηχανισμό carrier Sense Multiple Access / Collision Detection (CSMA/CD)

Το πρότυπο 802.11 καθορίζει ένα αριθμό από λειτουργίες συντονισμού του MAC επιπέδου για να συντονίσει την πρόσβαση μέσου μεταξύ πολλαπλών σταθμών. Η πρόσβαση στο μέσο μπορεί να γίνει είτε μέσω της λειτουργίας κατανεμημένου συντονισμού (Distributed Coordination Function – DCF), είτε μέσω της λειτουργίας σημείου συντονισμού (Point Coordination Function – PCF). (Comer, 2007)



Εικόνα 11. Η αρχιτεκτονική του επιπέδου MAC του 802.11

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Γενικά

Οι χρήστες ενός ασύρματου δικτύου φυσικά μπορούν να επωφεληθούν από ένα σωρό πλεονεκτήματα όμως σε αυτή την περίπτωση τίθεται ένα πολύ σημαντικό ερώτημα, πόσο ασφαλής είναι η επικοινωνία σε ένα σύστημα όπου το μέσο μετάδοσης της πληροφορίας είναι ο αέρας;

Επιπλέον η ευρεία χρήση του διαδικτύου για την διακίνηση προσωπικών πληροφοριών αναδεικνύει ακόμα πιο πολύ το θέμα της ασφάλειας των δικτύων.

Η λύση έχει ήδη δοθεί (εν μέρει) με τις μεθόδους πιστοποίησης και κρυπτογράφησης των δεδομένων που χρησιμοποιούνται ευρέως σήμερα. Σε ένα ενσύρματο τοπικό δίκτυο οι απειλές αντιμετωπίζονται στο σημείο εξόδου προς τον ISP με πολιτικές ασφάλειας στους δρομολογητές, με firewall κτλ.

Όμως σε ένα ασύρματο δίκτυο όλα τα παραπάνω δεν ισχύουν. Ιδιότητες της ασφαλούς επικοινωνίας αποτελούν τα ακόλουθα:

- **Επικύρωση:** πριν από την μετάδοση δεδομένων, οι κόμβοι αναγνωρίζονται και ανταλλάσουν επικυρωμένα πιστοποιητικά.
- **Κρυπτογράφηση:** πριν την αποστολή ενός ασύρματου πακέτου δεδομένων, ο κάθε υπολογιστής που το στέλνει θα πρέπει να το κρυπτογραφήσει.
- **Ακεραιότητα:** διασφαλίζει ότι το στοιχείο που μεταδίδεται δεν έχει τροποποιηθεί.
- **Μυστικότητα:** είναι ο όρος που χρησιμοποιείται για να περιγράψει τα δεδομένα που προστατεύονται ενάντια στην ανάγνωση από αναρμόδια συμβαλλόμενα μέρη.

3.1 ΕΠΙΚΥΡΩΣΗ ΚΑΙ ΜΥΣΤΙΚΟΤΗΤΑ

Στην ουσία η έννοια της επικύρωσης αφορά τον έλεγχο πρόσβασης. Για να πραγματοποιήσουμε την επικύρωση πρέπει να αποκτήσουμε πρώτα έλεγχο πρόσβασης στο μέσο και στη συγκεκριμένη περίπτωση στο ασύρματο δίκτυο. Αρχικά ελέγχονται τα διαθέσιμα ασύρματα δίκτυα και ακολούθως το δίκτυο επικυρώνει το σταθμό και ο σταθμός επικυρώνει το δίκτυο.

Τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται beacons -πλαίσια διαχείρισης (υπάρχει όμως και η περιπτωση να μην στελνει beacons γιατί έχει κρυφό ssid όπου τότε περίμενει να λάβει αίτηση για να απαντήσει)

Τα beacons είναι αυτά τα οποία ανακοινώνουν την ύπαρξη ενός δικτύου. Το κάθε beacon περιλαμβάνει ένα Service Set Identifier (SSID) ή αλλιώς όνομα δικτύου.
Ένας σταθμός μπορεί να επιλέξει να συνδεθεί σε ένα δίκτυο είτε παθητικά είτε ενεργητικά. Στην παθητική σάρωση ο σταθμός ελέγχει τα κανάλια προσπαθώντας να βρει beacons από τα σημεία πρόσβασης και στην δεύτερη περίπτωση στέλνει αιτήσεις διερεύνησης (είτε σε ένα συγκεκριμένο SSID, είτε με το SSID ρυθμισμένο στο 0), σε όλα τα κανάλια ένα προς ένα. Όλοι οι σταθμοί πρόσβασης που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση.

Ακολούθως ο σταθμός να διαλέγει το δίκτυο που θέλει να συνδεθεί. Την απόφαση μπορεί να λάβει χρήστης ή ένα κατάλληλο λογισμικό που επιλέγει βασιζόμενο στην ισχύ του σήματος ή σε άλλα κριτήρια.

Στο πρότυπο 802.11 έχουμε δύο ειδών τρόπους επικύρωσης, την επικύρωση ανοιχτού κλειδιού (Open System Authentication – OSA) και την επικύρωση μοιρασμένου κλειδιού (Shared Key Authentication – SKA). Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στο μήνυμα της αίτησης επικύρωσης. Το δίκτυο μπορεί να δεχτεί ή να απορρίψει αυτή την πρόταση ανάλογα με τις ρυθμίσεις ασφαλείας. Χρησιμοποιώντας επικύρωση ανοιχτού κλειδιού οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης όμως όχι και να επικοινωνήσει. Η συσκευή μπορεί να επικοινωνεί μόνο αν τα WEP κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης.

Η επικύρωση μοιρασμένου κλειδιού βασίζεται στο σύστημα πρόσκλησης -απάντησης. Για να χρησιμοποιήσουμε αυτή τη μέθοδο επικύρωσης, προϋποθέτει ότι το σημείο πρόσβασης και ο σταθμός είναι συμβατοί με τη λειτουργία WEP (Wired Equivalent Privacy) και ότι έχουν μεταξύ τους ένα προ-μοιρασμένο κλειδί. Αυτό σημαίνει ότι ένα κοινό κλειδί πρέπει να μοιραστεί σε όλους τους σταθμούς που τους έχει επιτραπεί να έχουν πρόσβαση στο δίκτυο, πριν επιχειρήσουν την διαδικασία της επικύρωσης.

3.2 ΚΡΥΠΤΟΓΡΑΦΗΣΗ WEP (WIRED EQUIVALENT PRIVACY)

Κρυπτογράφηση καλείται η διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή – μεταμφιέζονται προκειμένου να επιτευχθεί η ασφαλής μετάδοση πληροφοριών (encryption, συμβολίζεταιμε E). Τα δεδομένα πριν από την κρυπτογράφηση ονομάζονται plaintext

(συμβολίζεται με P) ενώ τα δεδομένα μετά την κρυπτογράφηση αποτελούν το cipher text (συμβολίζεται με C). Η αντίστροφη διαδικασία μετατροπής ονομάζεται αποκρυπτογράφηση (decryption).

Ο αλγόριθμος κρυπτογράφησης ή cipher είναι η μαθηματική ακολουθία που χρησιμοποιείται για την μεταμφίεση και αποκάλυψη των δεδομένων. Συνήθως οι αλγόριθμοι κρυπτογράφησης εμπεριέχουν ακολουθίες κλειδιών για να τροποποιήσουν τα εξαγόμενα τους.

Η πιο γνωστή επιλογή παροχής ασφάλειας για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11 είναι το Wired Equivalent Privacy (WEP). Με την επιλογή του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν επιθυμούμε εμπιστευτικότητα, μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν.

Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία αλλά και την ακεραιότητα των δεδομένων. Με τη βοήθεια ενός συμμετρικού αλγόριθμου κρυπτογράφησης, RC4, επιτυγχάνεται η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω του δικτύου.

- **Επαλήθευση ταυτότητας**

Σε ένα ασύρματο δίκτυο, μια κινητή συσκευή προκειμένου να συνδεθεί στο δίκτυο μέσω ενός σημείου πρόσβασης, θα πρέπει να αποδείξει την ταυτότητας της. Κάτι το οποίο θα έπρεπε να γίνεται και από το σημείο πρόσβασης. Στην επαλήθευση ταυτότητας WEP, η συσκευή θα πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει τον μυστικό κλειδί της κρυπτογράφησης. Αρχικά υποβάλλεται αίτηση επαλήθευσης ταυτότητας από την κινητή συσκευή προς το σημείο πρόσβασης. Το σημείο πρόσβασης ακολούθως στέλνει έναν τυχαίο αριθμό μήκους 128 bit προς κρυπτογράφηση στην ασύρματη συσκευή. Ο αριθμός κρυπτογραφείται από τη συσκευή με το μυστικό κλειδί WEP και αποστέλλεται πίσω. Τέλος το σημείο πρόσβασης ελέγχει εάν η κρυπτογράφηση έγινε με το σωστό κλειδί. Ωστόσο η μέθοδος αυτή αποτελεί πολύ μεγάλο πρόβλημα για την ασφάλεια της κρυπτογράφησης καθώς δίδει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης αλλά και της μη κρυπτογραφημένης πληροφορίας.

- **Κατακερματισμός**

Σε ένα ασύρματο δίκτυο, το πακέτο δεδομένων που καταφθάνει περιέχει τις κατάλληλες πληροφορίες για την αποστολή του. Το συγκεκριμένο πακέτο δεδομένων καλείται MSDU (Mac Service Data Unit).Τα δεδομένα καταφθάνουν στο επίπεδο MAC του προορισμού και σκοπός είναι να περάσουν στο λειτουργικό σύστημα και να μετατεθούν στην κατάλληλη εφαρμογή. Παρόλα αυτά, πριν από αυτή τη διαδικασία τα δεδομένα πρέπει να χωριστούν σε μικρότερα κομμάτια, να υποστεί τη διαδικασία του θραυσματισμού (fragmentation). Ακολούθως κάθε κομμάτι ακολουθεί τη δική του πορεία στην κρυπτογράφηση WEP. Επομένως το αρχικό πακέτο δεδομένων χωρίζεται σε μικρότερα μηνύματα, MPDU (Mac Protocol Data Unit) στα οποία προστίθενται και άλλα bytes.

- **Διάνυσμα Αρχικοποίησης**

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στην κρυπτογράφηση WEP έχουν μήκη 40 ή 104 bits, ωστόσο συχνά ακούμε να μιλάνε για 68 ή 128 bits. Αυτό συμβαίνει επειδή κάποιοι παραλείπουν να αναφέρουν τα επιπλέον 24 bits που χρησιμοποιούνται από το διάνυσμα αρχικοποίησης (Initialization Vector -IV).

Το IV ουσιαστικά αλλάζει για κάθε πακέτο και συνδυάζεται με το μυστικό κλειδί. Το αποτέλεσμα αυτών των δυο κρυπτογραφείται. Έτσι ακόμα και εάν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική.

Το IV δεν είναι μυστικό, ενώ στέλνεται σε μη κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV.

- **Τα κλειδιά που χρησιμοποιούνται στο WEP**

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στο WEP έχουν τα ακόλουθα χαρακτηριστικά:

- *Σταθερό μήκος:* Συνήθως 40 ή 104 bit.
- *Στατικά:* Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.

- *Διαμοιραζόμενα (shared):* Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
- *Συμμετρικά:* Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

Σύμφωνα με το πρότυπο IEEE 802.11, η διάθεση των κλειδιών στα σημεία πρόσβασης και στις ασύρματες συσκευές πρέπει να γίνεται με ασφαλείς μεθόδους ανεξάρτητες του πρωτοκόλλου.

Η επαναχρησιμοποίηση των κλειδιών είναι μια αδυναμία των κρυπτογραφικών πρωτοκόλλων. Γι αυτό το λόγο το WEP, έχει μια δεύτερη κατηγορία κλειδιών που χρησιμοποιούνται για τα ζευγάρια επικοινωνιών. Αυτά τα κλειδιά μοιράζονται μόνο μεταξύ των δύο σταθμών επικοινωνίας. Οι δύο σταθμοί μοιράζονται ένα κλειδί και έχουν έτσι μια σχέση χαρτογράφησης κλειδιού.

Οι πιο κοινές εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά RC4 64 bit. Το μεγαλύτερο μέρος της βιομηχανίας όμως έχει κινηθεί προς ένα 128-bit δημόσιο RC4 κλειδί. Το πρότυπο 64-bit WEP χρησιμοποιεί ένα κλειδί 40 bit (επίσης γνωστό ως WEP-40) το οποίο συνδέεται με την αρχή ενός 24-bit διανύσματος και διαμορφώνει το RC4 κλειδί κυκλοφορίας. Την εποχή που συντασσόταν τα αρχικά πρότυπα WEP, η κυβέρνηση των Η.Π.Α εξέδιδε περιορισμούς στην κρυπτογραφική τεχνολογία για το μέγεθος του κλειδιού. Μόλις εγκαταλείφτηκαν οι περιορισμοί όλοι οι βασικοί κατασκευαστές εφάρμοσαν τελικά το 128-bit WEP πρωτόκολλο χρησιμοποιώντας μέγεθος κλειδιού 104 bit (επίσης γνωστό ως WEP-104).

Ένα 128-bit WEP κλειδί σχεδόν πάντα εισάγεται από τους χρήστες σαν μια ακολουθία 26 δεκαεξαδικών (βάση το 16) χαρακτήρων (0-9 και AF). Κάθε χαρακτήρας αντιπροσωπεύει 4 bit του κλειδιού. 26 ψηφία τεσσάρων bit δίνουν 104 bit και η προσθήκη του 24 bit IV παράγει το τελικό 128-bit κλειδί WEP. Ένα 256-bit σύστημα WEP είναι διαθέσιμο από μερικούς προμηθευτές, και όπως με το 128-bit WEP, τα 24 bit είναι για το IV, αφήνοντας 232 πραγματικά bit για την προστασία. Αυτά τα 232 bit εισάγονται χαρακτηριστικά ως 58 δεκαδικοί χαρακτήρες. (58 * 4 = 232 μπιτ) + 24 IV μπιτ = 256-bit κλειδί WEP.

Ωστόσο το μέγεθος του κλειδιού δεν είναι ο μόνος σημαντικός περιορισμός ασφάλειας σε WEP. Το WEP έχει αρκετά μειονεκτήματα και τα πρόσθετα bit στο κλειδί δεν έχουν ιδιαίτερη σημασία. Η καλύτερη δημόσια επίθεση ενάντια στο WEP μπορεί να ανακτήσει το κλειδί σε μερικά δευτερόλεπτα.

- **Διανομή κλειδιού**

Το βασικότερο μειονέκτημα του WEP είναι πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το 802.11 πρότυπο, δεν μας παρέχει ένα μηχανισμό παραγωγής κλειδιού έτσι ο καθένας μας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή να έχει πρόσβαση σε συσκευές με το χέρι.

Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

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

- **Τιμή Ελέγχου Ακεραιότητας**

Η τιμή ελέγχου ακεραιότητας (Integrity Check Value -ICV) συνεισφέρει στην αποφυγή από την τροποποίηση του μηνύματος κατά τη μετάδοση. Γενικότερα στα κρυπτογραφημένα και μη κρυπτογραφημένα μηνύματα, συνηθίζεται έλεγχος για την αλλαγή των bits κατά τη μετάδοση.

Το σύνολο των Bytes του μηνύματος συνενώνονται στον έλεγχο κυκλικού πλεονασμού (Cyclic Redudancy Check -CRC). Η τιμή αυτή, μήκους τεσσάρων bytes, προστίθεται στο τέλος του πλαισίου πριν από την επεξεργασία για μετάδοση.

Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή CRC από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα. Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη, δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι

σε θέση να υπολογίσει τη νέα τιμή CRC και να αντικαταστήσει την αρχική. Το ICV λειτουργεί όπως το CRC, αλλά υπολογίζεται και εφαρμόζεται πριν τη διαδικασία της κρυπτογράφησης. Το CRC ωστόσο προστίθεται και μετά τη κρυπτογράφηση.

Επομένως ο εισβολέας δε μπορεί να υπολογίσει το μήνυμα εκ νέου. Έτσι το ICV υπολογίζεται ως ένας συνδυασμός όλων των δεδομένων και προκύπτει ως μια τιμή μήκους τεσσάρων bytes, η οποία προστίθεται στο τέλος.

- **Αλγόριθμος κρυπτογράφησης RC4**

Ο αλγόριθμος RC4 χρησιμοποιείται κατά τη διαδικασία της κρυπτογράφησης WEP. Ο RC4, δεδομένου ότι χρησιμοποιείται σωστά, είναι απλός στην υλοποίηση του και ισχυρός. Σημαντικό είναι το γεγονός ότι οι αδυναμίες του WEP δεν οφείλονται στον ίδιο τον RC4 αλλά στον τρόπο χρήσης του μέσα στον WEP.

Βασική ιδέα είναι η δημιουργία μιας τυχαίας ακολουθίας bytes, που ονομάζεται ροή κλειδιού (key stream) και έχει ως στόχο το συνδυασμό της με τα δεδομένα μέσω της λογικής πράξης του αποκλειστικού Η (XOR). Μια σημαντική ιδιότητα της XOR είναι:

A (XOR) B= C, τότε C (XOR) B = A

Ο αλγόριθμος RC4 εκμεταλλεύεται την παραπάνω ιδιότητα ως εξής:

- Κρυπτογράφηση: **plaintext (XOR) keystream = cipher text**
- Αποκρυπτογράφηση: **cipher text (XOR) keystream = plaintext**

Η τυχαία ακολουθία κλειδιού ονομάζεται «ψευδοτυαχαία» διότι θα πρέπει να δείχνει τυχαία σε εισβολέα αλλά τα δυο άκρα της ζεύξης που επικοινωνούν θα πρέπει να παράγουν την ίδια τυχαία τιμή για κάθε byte που επεξεργάζονται.

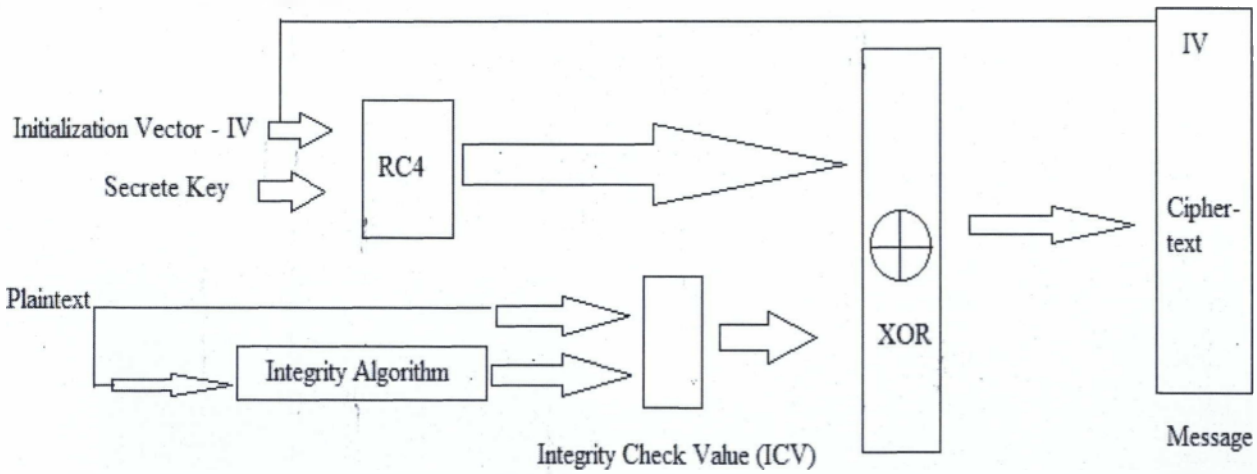
Η πράξη XOR υλοποιείται πολύ εύκολα οπότε, το πιο δύσκολο κομμάτι αποτελεί ο υπολογισμός μιας καλής «ψευδοτυχαίας» ροής bytes. Ουσιαστικά χρειαζόμαστε ένα «ψευδοτυχαίο» byte για κάθε byte του μηνύματος προς κρυπτογράφηση. Ο RC4 παράγει μια ροή αυτής της μορφής..

- **Η κρυπτογράφηση**

Εν ολίγοις η διαδικασία που ακολουθείται αναλύεται παρακάτω:

Πρώτα απ' όλα το μυστικό κλειδί συνδέεται με το διάνυσμα έναρξης (IV) και το αποτέλεσμα τους εισάγεται στον αλγοριθμο RC4. Ο αλγοριθμος RC4 παράγει μια ακολουθία κλειδιού keystream από «ψευδοτυχαία» bits ίσα στο μήκος με τον αριθμό bits δεδομένων που πρέπει να διαβιβαστούν συν 4.

Ακολούθως για προστασία από αναρμόδια τροποποίηση δεδομένων, εφαρμόζεται ο αλγόριθμος ακεραιότητας επάνω στα δεδομένα και παράγεται το ICV. Η κρυπτογράφηση ολοκληρώνεται με τη λογική πράξη του αποκλειστικού Η (XOR) μεταξύ της ακολουθίας κλειδιού και των δεδομένων που μετατράπηκαν σε ICV. Το προϊόν της διαδικασίας είναι ένα μήνυμα που περιέχει το IV και το κρυπτογράφημα.



Εικόνα 12. Η διαδικασία της κρυπτογράφησης WEP

Ο αλγόριθμος RC4 είναι ένας από τους σημαντικότερους παράγοντες της κρυπτογράφησης WEP, αφού μεταμορφώνει ένα σύντομο μυστικό κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού. Αυτή η μέθοδος κάνει απλή τη διαδικασία διανομής κλειδιού, αφού το μόνο που θα πρέπει να μεταδοθεί μεταξύ των σταθμών είναι το μυστικό κλειδί. Το διάνυσμα αρχικοποίησης επεκτείνει την διάρκεια ζωής του μυστικού κλειδιού.

Στη μέθοδο WEP λοιπόν το μόνο που αλλάζει ανά συχνά διαστήματα είναι το διάνυσμα αρχικοποίησης ενώ το μυστικό κλειδί παραμένει πάντα ίδιο. Κάθε νέο IV καταλήγει σε μια νέα ακολουθία κλειδιού. Το IV μπορεί να αλλάξει τόσο συχνά όσο κάθε MPDU και επειδή αυτό έρχεται με το μήνυμα, ο αποδέκτης θα μπορεί πάντα να αποκρυπτογραφήσει οποιοδήποτε μήνυμα. Το IV

δεν είναι μυστικό αφού δεν παρέχει οποιεσδήποτε πληροφορίες για το μυστικό κλειδί.

Για την αποκρυπτογράφηση πρέπει το διάνυσμα αρχικοποίησης να αποσταλεί μαζί με το κρυπτογραφημένο πακέτο. Όταν ο παραλήπτης αποκρυπτογραφήσει το πακέτο υπολογίζει ξανά την τιμή ελέγχου ακεραιότητας και τη συγκρίνει με αυτή που περιείχε το πακέτο που παρέλαβε. Αν οι δύο τιμές ταυτίζονται, τότε θεωρείται ότι το πακέτο είναι έγκυρο.

Σε γενικές γραμμές χρησιμοποιούνται στατικά κλειδιά μήκους 40 bits και ενός IV μήκους 24 bits. Νεότερες εκδόσεις του WEP υποστηρίζουν και μήκος κλειδιού 104 bits και μήκος IV 24 bits. Το κλειδί και το IV ενώνονται για να σχηματίσουν το κλειδί μήκους 64 bits, ή 128 bits αντίστοιχα που χρησιμοποιείται ως είσοδος για τον αλγόριθμο RC4.

Ο αλγόριθμος RC4 είναι πολύ σημαντικός παράγοντας για την αποδοτικότητα του WEP, όσον αφορά την εμπιστευτικότητα των δεδομένων, αφού αυτός είναι στην ουσία η μηχανή κρυπτογράφησης. Θα πρέπει να τονίσουμε ότι το μυστικό κλειδί είναι στατικό, οπότε το IV είναι αυτό που καθορίζει κάθε φορά την ψευδοτυχαία ακολουθία. Επομένως, ο αλγόριθμος RC4 εξαρτάται μόνο από το IV. (Peikari & Fogie, 2002)

3.2.1 ΠΡΟΒΛΗΜΑΤΑ ΤΟΥ WEP

Οι αδυναμίες του WEP είναι πολλές. Μέθοδοι για να ηττηθεί το WEP προκύπτουν από παντού. Μερικά από τα προβλήματα του WEP παρατίθενται παρακάτω:

- Το θέμα της **διανομής των κλειδιών** είναι ένα ιδιαίτερα ευαίσθητο θέμα. Όταν κάποιος αποχωρεί από το σύστημα, θα πρέπει τα κλειδιά να αλλάζουν. Για να επιτύχει μια επίθεση sniffing έχει ανάγκη μόνο τα μυστικά κλειδιά τα οποία αλλάζουν σπάνια. Το WEP χρησιμοποιεί συνήθως ένα δημόσιο μυστικό κλειδί 40 bit. Η καταλληλότητα αυτού του κλειδιού δεν έχει κριθεί ιδιαίτερα καλή, για αυτό το λόγο πολλοί είναι αυτοί που συστήνουν τη **χρήση 128-bit κλειδιών.**

- Η σπάνια **νέα εισαγωγή κλειδιών** επιτρέπει στους επιτιθεμένους να αποκτήσουν αποθέματα κρυπτογραφημένων δεδομένων δηλαδή μεγάλες συλλογές των πλαισίων που κρυπτογραφούνται με τα ίδια κλειδιά.

- Προβληματική φαίνεται να είναι και η διαδικασία της **επαλήθευσης ταυτότητας**. Η επαλήθευση ταυτότητας στηρίζεται σε μια μέθοδο πρόσκλησης – απόκρισης. Αρχικά στέλνεται μια τυχαία ακολουθία bits, η οποία κρυπτογραφείται αποστέλλεται πίσω και τέλος το σημείο πρόσβασης την αποκρυπτογραφεί και τη συγκρίνει με την αρχική ακολουθία. Το κλειδί που χρησιμοποιείται σε αυτή τη διαδικασία είναι το ίδιο με αυτό της κρυπτογράφησης, δίνοντας έτσι την ευκαιρία σε έναν επιτιθέμενο να αποκτήσει στοιχεία. Η όλη διαδικασία δίνει γενικότερα την ευκαιρία σε έναν εισβολέα να επιτεθεί στα κλειδιά κρυπτογράφησης. Αυτό συμβαίνει διότι οποιοσδήποτε παρακολουθεί τη διαδικασία της επαλήθευσης έχει πρόσβαση σε ένα κρυπτογραφημένο και μη κρυπτογραφημένο μήνυμα. Με μια απλή πράξη XOR μεταξύ τους έχουμε την «ψευδοτυχαία» ακολουθία RC4 σε δεδομένη τιμή IV. Εάν η τιμή IV δεν αλλάξει ο επιτιθέμενος μπορεί να κάνει αίτηση για επαλήθευση, να λάβει το μη κρυπτογραφημένο κείμενο και κάνοντας την πράξη XOR με τη ροή κλειδιού που απέκτησε πριν να επιτύχει στην επαλήθευση. Μπορεί ο επιτιθέμενος να μην αποκτάει άμεση πρόσβαση όμως ακόμα και έτσι παρέχει ένα δείγμα 128 bytes της ροής κλειδιού.

- **Ο έλεγχος πρόσβασης** συνίσταται στην απαγόρευση ή όχι της επικοινωνίας μια συσκευής με το δίκτυο. Η πρόσβαση συνήθως ελέγχεται διατηρώντας μια λίστα με επιτρεπόμενες συσκευές ή με κάποιο ηλεκτρονικό πιστοποιητικό. Στο IEEE 802.11 δεν έχουμε κάποιο συγκεκριμένο μηχανισμός υλοποίησης πρόσβασης. Οι συσκευές συνήθως αναγνωρίζονται με τις διευθύνσεις MAC, όμως αυτή δεν είναι μια πολύ καλή προσέγγιση καθώς οι διευθύνσεις αυτές μπορούν εύκολα να αντιγραφούν. Έτσι το μόνο που μένει για το WEP είναι τα κλειδιά κρυπτογράφησης ξανά.

- Ένα άλλο τρωτό σημείο του WEP είναι αδυναμία του να διαχειριστεί **επιθέσεις μέσω αναπαραγωγής μηνυμάτων**. Όταν ένας επιτιθέμενος παρακολουθεί και καταγράφει τα πλαίσια που ανταλλάσσονται σε μια νόμιμη επικοινωνία (sniffing), μπορεί ακολούθως να συνδεθεί στο δίκτυο με τη MAC διεύθυνση της κινητής συσκευής. Στέλνοντας έτσι ένα αντίγραφο ενός παλιού μηνύματος μπορεί να αποκτήσει πρόσβαση στον εξυπηρετητή. Η προστασία από τέτοιου είδους επιθέσεις στο WEP δεν είναι απλά ελλιπής αλλά ανύπαρκτη!

- Το WEP διαθέτει μηχανισμό για την αντιμετώπιση περιπτώσεων τροποποίησης μηνυμάτων, μέσω του **ελέγχου ακεραιότητας -ICV.** Σύμφωνα όμως με τη μέθοδο «bit flipping», μπορούν να μεταβληθούν λίγα bits του κρυπτογραφημένου μηνύματος κάθε φορά χωρίς αυτή η τροποποίηση να γίνει αντιληπτή. Αυτό μπορεί να συμβεί διότι η θέση της κεφαλίδας IP είναι γνωστή μετά την κρυπτογράφηση. Αν αλλαχθούν κάποια bits της κεφαλίδας IP αλλά και του ελέγχου αθροίσματος τότε ο έλεγχος μπορεί να είναι επιτυχής. Για αυτό το λόγο το WEP διαθέτει το πεδίο τιμής ICV, ωστόσο αδυναμίες παρουσιάζει και αυτή η μέθοδος. Η μέθοδος CRC που χρησιμοποιείται είναι γραμμική και έτσι μπορεί να προβλεφθούν τα bits που θα αλλάξουν με την τροποποίηση ενός μηνύματος. Επειδή το WEP χρησιμοποιεί τη λογική πράξη XOR η αντιστροφή των bits δεν επηρεάζει την κρυπτογράφηση. Η αντιστροφή ενός bit στο μη κρυπτογραφημένο αντιστρέφει το ίδιο bit και στο κρυπτογραφημένο κείμενο.

- Ιδιαίτερη βαρύτητα έχει η **επαναχρησιμοποίηση της τιμής του διανύσματος αρχικοποίησης IV.** Εάν συλλεχθούν πολλά δείγματα επαναλαμβανόμενου IV τότε μπορεί κάποιος να υποθέσει τμήματα της ροής κλειδιού και προχωρήσει στην αποκρυπτογράφηση. Άλλωστε όταν κάποιος γνωρίζει το keystream για ένα συγκεκριμένο IV, μπορεί να αποκρυπτογραφήσει κάθε πλαίσιο που χρησιμοποιεί το ίδιο IV. Ωστόσο αυτός ο κίνδυνος δεν είναι και τόσο μεγάλος αφού δεν υπάρχει αυτοματοποιημένο εργαλείο που θα μπορούσε να καταφέρει να διαχειριστεί τον προσδιορισμό ενός κρυπτογραφήματος με αυτή τη μέθοδο.

- **Η τιμή του διανύσματος αρχικοποίησης**, όπως προαναφέραμε, **δεν είναι μυστική**, όμως κάτι τέτοιο δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα σχετικά αδύναμο κλειδί. Τα πρώτα bytes ενός μη κρυπτογραφημένου μηνύματος είναι συνήθως γνωστά διότι αποτελούν μια επικεφαλίδα IEEE 802.11 Με παρακολούθηση της μετάδοσης αναζητείται ένα αδύναμο κλειδί. Ξέρουμε επίσης ότι υπάρχει σχέση ανάμεσα στο κρυπτογραφημένο στο μη κρυπτογραφημένο μήνυμα και το μυστικό κλειδί. Έχοντας καταγράψει έναν σημαντικό αριθμό από τέτοια μηνύματα, ο εισβολέας μπορεί να ανακαλύψει το πρώτο byte του κλειδιού. Η μέθοδος αυτή μπορεί να εφαρμοστεί για κάθε byte και τελικά να αποκαλυφθεί το μυστικό κλειδί. Θα πρέπει να πούμε επίσης ότι η αύξηση του μήκους του κλειδιού δεν επιφέρει εκθετική αύξηση του χρόνου αναζήτησης αλλά απλά γραμμική. (Flickenger, 2003)

3.3 ΠΕΡΑ ΑΠΟ ΤΟ WEP

Τα πρώτα χρόνια της ζωής το IEEE 802.11 για ασύρματα δίκτυα, υποστήριζε μόνο την WEP ως μέθοδο για την ασφάλεια της πληροφορίας που ανταλλάσσονται σε ένα δίκτυο.

Αρκετοί ωστόσο ήταν αυτοί που διαπίστωσαν τις αδυναμίες του συστήματος WEP. Πολύ σύντομα εμφανίστηκαν στο διαδίκτυο εργαλεία που παραβίαζαν το WEP και μάλιστα σε σύντομο χρονικό διάστημα. Παρόλα αυτά το WEP αποτελεί μέχρι και σήμερα για πολλούς, κυρίως οικιακούς χρήστες, τη μοναδική επιλογή για την προστασία των δεδομένων που ανταλλάσσουν μέσω ενός ασύρματου δικτύου.

- **Η λύση του TKIP**

Μετά από τη συνειδητοποίηση της κρισιμότητας της κατάστασης και του κενού ασφαλείας που άφηνε το WEP, αναδύθηκε η λύση του TKIP (Temporal Key Integrity Protocol -TKIP).

Το TKIP προσφέρει μεγαλύτερη ασφάλεια καθώς παρέχει ανάμιξη κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος και μηχανισμό αναπαραγωγής κλειδιών, ο οποίος επιδιορθώνει τα ελαττώματα του WEP. Ενώ το μόνο που απαιτούσε στην αυγή της εμφάνισης του ήταν η αναβάθμιση του firmware και πιθανώς του λογισμικού (driver) της συσκευής.

Αρχικά το TKIP χρησιμοποιήθηκε πάνω στο WEP για να ενισχύσει την ασφάλεια και να μειώσει τον αριθμό των επιθέσεων του WEP. Το πρώτο βήμα στην διαδικασία της κρυπτογράφησης TKIP είναι ο υπολογισμός του κώδικα ακεραιότητας δεδομένων MIC, που γίνεται με τον αλγόριθμο Michael. Με τον αλγόριθμο αυτό προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και παραλήπτη. Αυτά και ένα κλειδί MIC είναι είσοδοι στον αλγόριθμο. Τελικά προκύπτουν 8 bytes, τα οποία προσκολλούνται στο αρχικό μήνυμα το οποίο στη συνέχεια κρυπτογραφείται.

Η TKIP κρυπτογράφηση λειτουργεί σε δύο φάσεις. Η πρώτη φάση χρησιμοποιεί ένα μη γραμμικό πίνακα αντικατάστασης (S-Box) και συνδυάζει το κλειδί συνόδου (TK), τη MAC διεύθυνση του αποστολέα (TA) και τα τέσσερα πιο σημαντικά bytes της τιμής του μετρητή ακολουθίας, (TKIP Sequence Counter), οποίος αυξάνει για κάθε τμήμα δεδομένων που τεμαχίζονται.

Το κλειδί συνόδου αποτελείται από μια τιμή 128 bit, παρόμοια με την τιμή του WEP κλειδιού. Ο TKIP μετρητής ακολουθίας (TSC) είναι φτιαγμένος από την πηγαία διεύθυνση (SA), την διεύθυνση προορισμού (DA), την ιεραρχία και τα δεδομένα.

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

Η δεύτερη φάση «ανακατεύει» την τιμή TTAK με τα δύο λιγότερο σημαντικά bytes της τιμής του μετρητή ακολουθίας (TSC) και το κλειδί συνόδου (TK) για την εξαγωγή του τελικού κλειδιού κρυπτογράφησης. Τέλος κατά τα γνωστά από το WEP, υπολογίζεται το IV και γίνεται η κρυπτογράφηση από τον αλγόριθμο RC4.

Το TKIP χρησιμοποιεί την 802.1X αρχιτεκτονική επικύρωσης, σαν βάση για την ασφαλή ανταλλαγή του κλειδιού.

Το πρότυπο 802.1X παρέχει πρόσφορο έδαφος σε πρωτόκολλα ελέγχου ταυτότητας και διαχείρισης κλειδιού. Ουσιαστικά με το 802.1X, παρέχεται έλεγχος ταυτότητας μεταξύ του πελάτη και ενός διακομιστή RADIUS (Remote Authentication Dial-In User Service) που είναι συνδεδεμένος στο σημείο πρόσβασης. Επιπλέον η χρήση ενός πρωτοκόλλου ελέγχου ταυτότητας, γνωστό ως EAP (Extensible Authentication Protocol) ωφελεί το 802.1X.
Τα αμέσως επόμενα χρόνια η Wi-Fi Alliance όρισε ένα υποσύνολο του νέου προτύπου, το οποίο αποτελεί μια βελτιωμένη έκδοση ασφάλειας που ενδυναμώνει το επίπεδο προστασίας δεδομένων και ελέγχου πρόσβασης σε ασύρματο δίκτυο. Το υποσύνολο αυτό ονομάζεται Wi-Fi Protected Access (WPA). (Barken, 2003)

3.4 WPA (WI-FI PROTECTED ACCESS)

Το 2003, όταν άρχισε να γίνεται εμφανές το κενό ασφαλείας που άφηνε η κρυπτογράφηση WEP, η Wi-Fi Alliance ανέπτυξε το Wi-Fi Protected Access (WPA). Το WPA προέρχεται από το IEEE 802.11 πρότυπο και είναι σαν μια ενδιάμεση λύση ασφάλειας των WLAN και μπορεί να συμπεριληφθεί με αναβαθμίσεις στις ήδη υπάρχουσες WLAN ασύρματες συσκευές.

Το WPA κάνει χρήση της μεθόδου TKIP, που προαναφέρθηκε και αυξάνει σημαντικά το επίπεδο ασφάλειας και ελέγχου πρόσβασης στα ασύρματα συστήματα LAN. Το WPA παρέχει σε κάθε πακέτο το κλειδί, έναν έλεγχο ακεραιότητας μηνύματος (MIC) που ονομάζεται Michael και ένα διάνυσμα ακολουθίας (Initialization Vector-IV). Επίσης για τους οικιακούς χρήστες, το WPA παρέχει ένα μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre-Shared Key).

Για να εκμεταλλευτεί κάποιος την δυνατότητα του PSK θα πρέπει να εισάγει μια λέξη κωδικό και στο σημείο πρόσβασης και στο σταθμό. Αυτή η λέξη κωδικός χρησιμοποιείται για να επικυρώνει οποιονδήποτε σταθμό προσπαθεί να συνδεθεί στο συγκεκριμένο δίκτυο.

Ο κωδικός θα πρέπει να αποτελείται από 8 έως 63 εκτυπώσιμους χαρακτήρες σε ASCII. 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.

Το» preshared» WPA είναι τρωτό στις επιθέσεις ραγίσματος κωδικού πρόσβασης εάν χρησιμοποιείται ένας αδύνατος κωδικός. Για να προστατευτεί από μια επίθεση ένας αληθινά τυχαίος κωδικός 13 χαρακτήρων είναι πιθανώς αρκετός. Τα προϊόντα που γράφουν ότι έχουν "WPA-Personal" σημαίνει ότι υποστηρίζουν τον PSK μηχανισμό επικύρωσης.

Το πρότυπο WPA ορίζει επίσης τη χρήση του προτύπου AES (Advanced Encryption Standard) ως επιπλέον αντικατάσταση για την κρυπτογράφηση WEP. Η υποστήριξη προτύπου AES είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο προμηθευτής όσον αφορά προγράμματα οδήγησης.

3.4.1 AES (ADVANCED ENCRYPTION STANDARD)

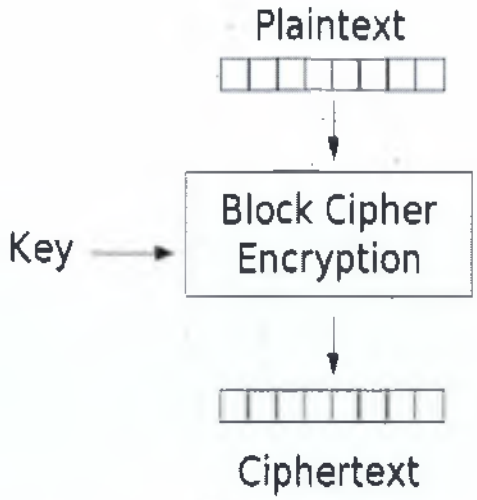
Το WPA παρέχει τη δυνατότητα για κρυπτογράφηση με δυο αλγόριθμους, τον RC4 και τον AES (Advanced Encryption Standard) για την εμπιστευτικότητα των δεδομένων και την ακεραιότητα.

Ο AES αποτελεί την νεότερη μέθοδος κρυπτογράφησης που έχει επιλεγεί από την κυβέρνηση των Η.Π.Α για να αντικαταστήσει τον αλγόριθμο DES το 2001. Ο AES χρησιμοποιεί ένα αλγόριθμο

γνωστό ως Rijndael.

Ο αλγόριθμος Rijndael πήρε το όνομα του από τους δυο Ελβετούς εφευρέτες του, Joan Daemen και Vincent Rijmen. Πρόκειται για έναν αλγόριθμο κρυπτογράφησης ομάδας (block), που σημαίνει ότι λειτουργεί σε μια ομάδα σταθερού μεγέθους bits, η οποία ονομάζεται μπλοκ.

Αρχικά ο Rijndael παίρνει σαν είσοδο ένα μπλοκ συγκεκριμένου μεγέθους, συνήθως 128, και παράγει ένα αντίστοιχο μπλοκ εξόδου του ίδιου μεγέθους. Ο μετασχηματισμός απαιτεί μια δεύτερη είσοδο, η οποία είναι το μυστικό κλειδί. Είναι σημαντικό να γνωρίζουμε ότι το μυστικό κλειδί δεν έχει συγκεκριμένο μέγεθος (ανάλογα με τη χρησιμοποιούμενη κρυπτογράφηση) και ότι ο AES χρησιμοποιεί τρία βασικά μεγέθη: 128, 192 και 256 bytes.



Εικόνα 13. Αλγόριθμος Ομάδας (block)

Στις μέρες μας μπορούμε να βρούμε προϊόντα AES WRAP (Wireless Robust Authentication Protocol), αλλά η τελική προδιαγραφή καθορίζει τον αλγόριθμο AES CCMP (Counter Mode-Cipher Block Chaining Mac Protocol). Οι προδιαγραφές του 802.11i παρέχουν επίπεδο μετάδοσης δεδομένων βασισμένο στο AES. Η χρησιμοποίηση του πρότυπου AES μας προστατεύει από τις ενεργές ασύρματες επιθέσεις. Ωστόσο πρέπει να αναγνωριστεί ότι ένα ασύρματο πρωτόκολλο του επιπέδου μετάδοσης δεδομένων μπορεί να προστατεύσει μόνο το ασύρματο υπόδίκτυο. Στα σημεία που η κίνηση διέρχεται από άλλα τμήματα του δικτύου, είτε σε δίκτυα τοπικής ή ευρείας περιοχής, απαιτείται προστασία υψηλού επιπέδου και κρυπτογράφηση από σημείο σε σημείο. (Barken, 2003)

3.4.2 CCMP (COUNTER MODE WITH CIPHER BLOCK CHAINING

MESSAGE AUTHENTICATION CODE PROTOCOL)

Η προσθήκη στο πρότυπο IEEE 802.11 που ορίζει την ασφάλεια της επόμενης γενιάς για τα ασύρματα δίκτυα ονομάζεται IEEE 802.11i. Το πρότυπο εκδόθηκε τελικά το 2004.

Το πρότυπο αυτό ορίζει μία νέα μέθοδο, για την ασφάλεια των δεδομένων στο MAC επίπεδο. Η μέθοδος αυτή (CCMP) λειτουργεί σύμφωνα με τον αλγόριθμο κρυπτογράφησης AES. Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη πακέτων.

Το CCMP χρησιμοποιεί μέγεθος κλειδιού 128-bit και μέγεθος μπλοκ 128-bit. Μετά από το CCMP το μέγεθος του πακέτου έχει επεκταθεί κατά 16 bytes, 8 bytes για την επικεφαλίδα του CCMP και 8 bytes για την ψηφιακή υπογραφή MIC (Message Integrity Code). Τα δεδομένα του πακέτου και το MIC μεταδίδονται κρυπτογραφημένα, αφού προστεθεί η αρχική επικεφαλίδα του πακέτου και η επικεφαλίδα του CCMP. (Wikipedia)

3.5 WPA2 (WI-FI PROTECTED ACCESS VERSION 2)

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

Μια από τις πρώτες βελτιώσεις του WPA2 είναι ότι με την προσθήκη του AES CCMP, όπως στο 802.11i, παρέχει τη δυνατότητα ισχυρής κρυπτογράφησης. Μια άλλη βελτίωση που περιλαμβάνει το WPA2 είναι τη δυνατότητα για γρήγορη περιαγωγή. Αυτή η ικανότητα είναι σημαντική για τις εφαρμογές ήχου, όπου η μεταφορά τους είναι υψηλής ευαισθησίας. Η γρήγορη περιαγωγή επιτυγχάνεται με την επικύρωση των σταθμών και στα γειτονικά σημεία πρόσβασης αλλά και στο τελικό σημείο πρόσβασης όπου επιτυγχάνεται η επικοινωνία.

Όταν ένας σταθμός θέλει να συνδεθεί σε ένα γειτονικό σημείο πρόσβασης, η επικύρωση 802.1X μπορεί να παραληφθεί αφού έχει ήδη ολοκληρωθεί εκ των πρότερων. Επιπλέον το προσωρινό κλειδί έχει ήδη εγκαθιδρυθεί ανάμεσα στο σταθμό και το σημείο πρόσβασης. Αποκτώντας πρόσβαση στον RADIUS εξυπηρετητή για να ολοκληρώσει την 802.11X επικύρωση καταλαμβάνει

πολύ χρόνο και επιπλέον τα δίκτυα που περιλαμβάνουν γρήγορη περιαγωγή έχει παρατηρηθεί ότι έχουν ομαλότερη λειτουργία και συνεχή συνδεσιμότητα του πελάτη καθώς αυτός μετακινείται στις κυψέλες του WLAN.

Υπάρχουν δύο εκδόσεις του WPA2. Το WPA2-Personal και το WPA2-Enterprise. Το WPA2-Personal προστατεύει την πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες με τη χρήση της εγκατάστασης ενός κωδικού πρόσβασης. Το WPA2Enterprise πιστοποιεί τους χρήστες του δικτύου μέσω ενός εξυπηρετητή. (Wikipedia)

3.6 ROBUST SECURE NETWORK (RSN)

Το πρότυπο IEEE 802.11i ορίζει ένα νέο τύπο ασύρματου δικτύου, το οποίο ονομάζεται Δίκτυο Ανθεκτικής Ασφάλειας (Robust Secure Network -RSN).

Οπωσδήποτε οι ασύρματες συσκευές που θα υποστηρίζουν ένα τέτοιο δίκτυο θα πρέπει να έχουν νέες δυνατότητες. Αυτές είναι η επικύρωση, η διαχείριση κλειδιών σε υψηλό επίπεδο, η κρυπτογράφηση και την επικύρωση των δεδομένων που διακινούνται σε MAC επίπεδο.

Ένα δίκτυο RSN έχει πολύ αυστηρούς περιορισμούς όσον αφορά την προσβασιμότητα και επιβάλλονται αρκετοί περιορισμοί ασφάλειας. Ωστόσο, επειδή χρειάζεται χρόνος για να αναβαθμιστούν οι συσκευές και ο εξοπλισμός, το πρότυπο IEEE 802.11i ορίζει το Δίκτυο Μεταβατικής Ασφάλειας (Transitional Security Network -TSN).

Τα δίκτυα TSN υποστηρίζουν δίκτυα όπως το RSN αλλά και το WEP. Οι χρήστες που εισέρχονται σε ένα δίκτυο TSN, μπορούν να λειτουργήσουν παράλληλα για όλα τα προηγούμενα συστήματα ασφάλειας. (Frankel, Bemard, Les, & Scarfone, 2007)

3.7 ΔΙΑΦΟΡΕΣ ΑΝΑΜΕΣΑ ΣΤΟ RSN ΚΑΙ ΤΟ WPA

Τόσο το RSN αλλά και το WPA είναι μέθοδοι κρυπτογράφησης που ουσιαστικά αντιμετωπίζουν το θέμα της ασφάλειας με παρόμοιο τρόπο. Το WPA διαθέτει μερικές μόνο από τις δυνατότητες του RSN. Το RSN κάνει υποχρεωτική χρήση του πρωτοκόλλου CCMP, με εναλλακτική λύση το TKIP, ενώ το WPA επικεντρώνεται στο TKIP.

Οι παραπάνω μέθοδοι χρησιμοποιούν παρόμοια αρχιτεκτονική με πρωτόκολλα ασφάλειας που βασίζονται στους αλγόριθμους AES και RC4 αντίστοιχα. Μέσω αυτών των μεθόδων καλύπτονται θέματα όπως: α) Επικύρωση σε υψηλό επίπεδο, β) Διανομή του κλειδιού κρυπτογράφησης γ) Ανανέωση του κλειδιού.

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

3.8 ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Η γοητεία της πρόσβασης σε ένα ξένο μέσο και η εξερεύνηση δεδομένων που θεωρούνται μυστικά ή με άλλα λόγια ξένα για εμάς, αποτελούν ένα πολύ σημαντικό κίνητρο για πολλούς από τους επίδοξους επιτιθέμενους. Ωστόσο οι προθέσεις και οι στόχοι κάθε επίθεσης μπορεί να διαφέρουν. Μέσα σε γενικότερα πλαίσια, οι επιθέσεις σε ασύρματα δίκτυα μπορούν να χωριστούν σε παθητικές και ενεργητικές.

Ως *παθητικές* ορίζονται οι επιθέσεις που δε συμπεριλαμβάνουν συμμετοχή του επιτιθέμενου στο δίκτυο. Επίθεση τέτοιου τύπου αποτελεί η Λήψη Πληροφοριών (Snooping/Footprinting)

Οι *ενεργητικές* επιθέσεις προϋποθέτουν ότι ο επιτιθέμενος αναλαμβάνει ενεργή συμμετοχή στο δίκτυο. Οι ενεργητικές επιθέσεις χωρίζονται, σύμφωνα με το σκοπό που έχουν οι επιτιθέμενοι, σε τέσσερις βασικές κατηγορίες:

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

3.8.1 ΠΑΘΗΤΙΚΕΣ: ΛΗΨΗ ΠΛΗΡΟΦΟΡΙΩΝ

(SNOOPING/FOOTPRINTING)

Η λήψη πληροφοριών (snooping) σχετίζεται με την ανάκτηση απόρρητων προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες. Σε αυτή την περίπτωση μια ασφαλής μέθοδος κρυπτογράφησης μπορεί να βοηθήσει να αντιμετωπιστούν τέτοιες επιθέσεις.

Καταρχήν, ο επιτιθέμενος είναι σε θέση να διαβάσει όλες τις πληροφορίες που προέρχονται από τα σημεία πρόσβασης, επομένως ξέρει το όνομα δικτύου (ή SSID). Επίσης είναι πιθανό να μπορεί να προσδιορίσει τον κατασκευαστή κάθε σημείου πρόσβασης με την εξέταση τη διεύθυνση MAC του. Επίσης η παρακολούθηση της πορείας μιας μεγάλης ποσότητας πακέτων προς σημεία πρόσβασης μπορεί να δώσει τον αριθμό των ασύρματων συσκευών που συνδέονται με κάθε σημείο πρόσβασης.

Εάν η κρυπτογράφηση που χρησιμοποιείται στο δίκτυο είναι WEP, τότε μπορεί να εξετάσει εάν ο καθένας χρησιμοποιεί το ίδιο κλειδί (κοινό) ή εάν κάθε συσκευή έχει ένα χωριστό κλειδί με την εξέταση των bit στην IEEE 802.11 επιγραφή. Εκείνες οι πληροφορίες θα μπορούσαν να είναι χρήσιμες αργότερα.

Μια άλλη μέθοδος που χρησιμοποιείται είναι η τεχνική της ανάλυσης κυκλοφορίας. Η ανάλυση κυκλοφορίας είναι η μελέτη των εξωτερικών στοιχείων των μηνυμάτων, παραδείγματος χάριν, της συχνότητας επικοινωνίας και του μεγέθους. Δυστυχώς, είναι δυνατό να μαθευτεί ολόκληρο ή ένα μέρος για τους τύπους των πραγμάτων που συμβαίνουν σε ένα δίκτυο ακριβώς με την προσοχή των μηκών πακέτων και τη σημείωση του συγχρονισμού χωρίς κοίταγμα μέσα στα πακέτα. Παρόλα αυτά δεν υπάρχει άμεση πρόσβαση στο περιεχόμενο μηνυμάτων.

Ένα πολύ χρήσιμο εργαλείο που χρησιμοποιείται στην ανάλυση, παρακολούθηση και στον εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα αλλά και στην εκπαίδευση είναι το Wireshark.

3.8.2 ΕΝΕΡΓΗΤΙΚΕΣ: ΑΝΑΚΤΗΣΗ ΚΩΔΙΚΟΥ WEP (WEP CRACKING -CAFFE LATTE ATTACK)

Όπως αναλύθηκε στο προηγούμενο κεφάλαιο, η μέθοδος κρυπτογράφησης του WEP έχει χάσει την παλιά της αίγλη, εφόσον μέσα σε λίγα λεπτά μπορεί να ανακτηθεί ο μυστικός κωδικός που χρειάζεται για την παραβίαση ενός ασύρματου δικτύου. Οι μέθοδοι που χρησιμοποιούνται σήμερα για το WEP Cracking επικεντρώνονται στην συλλογή μεγάλου ποσοστού IV's πακέτων. Η διαδικασία αυτή πραγματοποιείται μέσω της συλλογής και αναμετάδοσης πακέτων ARP (Address Resolution Protocol) στο σημείο πρόσβασης.

Το Address Resolution Protocol (ARP) (πρωτόκολλο επίλυσης διευθύνσεων) χρησιμοποιείται για να βρεθεί μια διεύθυνση του στρώματος συνδέσμου (link layer) ή διεύθυνση εξοπλισμού (hardware address) ενός host με βάση μια διεύθυνση του επιπέδου επικοινωνίας (network layer). Κάθε host που είναι συδεδεμένος σ'ένα δίκτυο που βασίζεται στο ARP κρατάει έναν κατάλογο (ARP table) ζεύγων του τύπου Διεύθυνση πρωτοκόλλου >
Αντίστοιχη διεύθυνση υλικού. Τα ερωτήματα ARP στέλνονται με broadcast, που σημαίνει πως διάφοροι host τα λαμβάνουν.

Σε γενικές γραμμές η επίθεση σε συστήματα WEP πραγματοποιείται μέσω συλλογής είτε αδύναμων είτε μοναδικών IV's πακέτων. Ωστόσο πάντα απαιτείται η συλλογή μεγάλου ποσοστού κρυπτογραφημένων πακέτων.

Ενδιαφέρουσα περίπτωση αποτελεί και η μέθοδος "Caffe Latte Attack", με τη βοήθεια της οποίας ο επιτιθέμενος μπορεί να ανακαλύψει το WEP κλειδί του δικτύου χωρίς να βρίσκεται στην ίδια περιοχή με το δίκτυο – στόχο απλά στοχεύοντας συγκεκριμένους πελάτες σε δημόσιες περιοχές.

3.8.3 ΕΝΕΡΓΗΤΙΚΕΣ: ΤΡΟΠΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

Οι μέθοδοι τροποποίησης δεδομένων έχουν πολλούς διαφορετικούς στόχους, που κυμαίνονται από την τροποποίηση του ηλεκτρονικού ταχυδρομείου με κακόβουλο περιεχόμενο έως και την αλλαγή αριθμών σε μια ηλεκτρονική τραπεζική μεταφορά.

Ωστόσο παρότι τέτοιες υψηλού επιπέδου τροποποιήσεις έχουν πραγματοποιηθεί, είναι αρκετά περιορισμένες στην πράξη λόγω του βαθμού δυσκολίας που έχουν.

Παράδειγμα μεθόδου τροποποίησης δεδομένων που είναι πιο κοντά στην πραγματικότητα είναι η

αλλαγή της διεύθυνσης προορισμού (διεύθυνση IP) ενός μηνύματος το οποίο διαβιβάζεται σε μια ασύρματη μετάδοση, το οποίο αντί να διαβιβαστεί στον προοριζόμενο παραλήπτη μεταφέρεται στον επιτιθέμενο ή σε κάποιον άλλο επιθυμητό προορισμό μέσω διαδικτύου. Αυτή η μέθοδος χρησιμοποιείται διότι το μήνυμα στην ασύρματη σύνδεση κρυπτογραφείται και δεν μπορεί να διαβαστεί το περιεχόμενο, αλλά εάν μπορεί ο επιτιθέμενος να το πάρει διαβιβασμένο από το Διαδίκτυο, θα λάβει την αποκρυπτογραφημένη έκδοση. Η επιγραφή IP είναι ευκολότερο να δεχτεί επίθεση γιατί είναι μια γνωστή μορφή. Μια επίθεση τροποποίησης είναι η Man-in-the-Middle επίθεση (άτομο στην μέση).

- **Man in the Middle Attack**

Σε αυτό το είδος της επίθεσης, ο επιτιθέμενος βρίσκεται στη μέσης της συνομιλίας δυο συμμετεχόντων στο δίκτυο (Γιώργος και Μαρία). Σε μια πραγματική επικοινωνία Ο Γιώργος θα λάμβανε μηνύματα από τη Μαρία και η προηγούμενη από το Γιώργο. Ο εισβολέας όμως μπορεί να μιμηθεί καθέναν από τους δυο και να στέλνει μηνύματα τα οποία φαίνεται ότι προήλθαν από την πραγματική τους επικοινωνία Συνήθως τέτοιου είδους επιθέσεις χρησιμοποιούνται για την τροποποίηση μηνυμάτων κατά τη μεταφορά χωρίς να υπάρχει περίπτωση να ανιχνευθούν.

Για την εφαρμογή μιας τέτοιας επίθεσης σε ένα ασύρματο δίκτυο υπάρχουν δυο διαφορετικές μέθοδοι, τα πλαίσια διαχείρισης , συγκεκριμένα για την ασύρματη δικτύωση και το ARP Spoofing, το οποίο αποτελεί απειλή ακόμα και για τα ενσύρματα δίκτυα.

3.8.4 ΕΝΕΡΓΗΤΙΚΕΣ: ΜΕΤΑΜΦΙΕΣΗ (SPOOFING)

Κατά τις επιθέσεις της μεταμφίεσης, ο επιτιθέμενος, υποκρίνεται κάποιον νόμιμο χρήστη του δικτύου ώστε να αποκτήσει τα δικαιώματα πρόσβασης σε υπηρεσίες που επιθυμεί. Ουσιαστικά γίνεται χρήση των στοιχείων πρόσβασης ενός νόμιμου χρήστη. Τα στοιχεία πρόσβασης ενός νόμιμου χρήστη ενός δικτύου μπορούν να γίνουν βορά στα χέρια ενός επιτιθέμενου στις εξής περιπτώσεις :

- Όταν δεν χρησιμοποιείται κρυπτογράφηση στο δίκτυο
- Όταν χρησιμοποιούνται εύκολοι κωδικοί
- Όταν δεν ακολουθούνται οι κανόνες προστασίας κωδικών πρόσβασης

Η μέθοδος αυτή είναι ιδανική εάν ένας επιτιθέμενος θέλει να μην αποκαλυφθεί. Εάν η συσκευή καταφέρει να ξεγελάσει το δίκτυο ως εξουσιοδοτημένη συσκευή, τότε ο επιτιθέμενος παίρνει όλα τα δικαιώματα πρόσβασης που επιθυμεί από την εξουσιοδοτημένη. Επιπλέον, δεν θα υπάρξει καμία προειδοποίηση ασφάλειας.

3.8.5 ΕΝΕΡΓΗΤΙΚΕΣ: ΆΡΝΗΣΗ ΥΠΗΡΕΣΙΩΝ (DENIAL OF SERVICE)

Σε αυτή την περίπτωση τόσο ο σκοπός αλλά και η τεχνική της μεθόδου διαφέρουν. Σκοπός μιας τέτοιας επίθεσης είναι η ολική αχρήστευση του ασύρματου δικτύου για ένα χρονικό διάστημα. Ουσιαστικά αφαιρούνται τα δικαιώματα από όλους τους νόμιμους και μη νόμιμους χρήστες του δικτύου και στόχος είναι η διαταραχής της ομαλής λειτουργίας του δικτύου. Μια τέτοια επίθεση μπορεί να πραγματοποιηθεί με δυο τρόπους. Η πρώτη μέθοδος απλά κατακλύζει το στόχο υπολογιστή ή τη συσκευή υλικού με πληροφορίες ώστε να μπλοκάρει. Σύμφωνα με τη δεύτερη μέθοδος στέλνονται καλά διατυπωμένες εντολές ή λάθος δεδομένα με στόχο να κολλήσει το σύστημα. Οι επιθέσεις αυτού του είδους είναι οι πιο επικίνδυνες διότι υπάρχει μικρότερο περιθώριο προστασίας.

Οι πέντε πιο σημαντικοί τύποι επιθέσεων DOS περιγράφονται παρακάτω:

- **Επίθεση πλημμύρας (Flood Attack)**

Αυτές είναι οι πιο γνωστές του είδους των DoS επιθέσεων. Ο μηχανισμός αυτής της επίθεσης είναι απλός. Ο επιτιθέμενος δημιουργεί στον server περισσότερη κίνηση από αυτή που μπορεί να διαχειριστεί. Εάν όμως ο υπολογιστής – θύμα διαθέτει ένα πολύ καλό bandwidth τότε έχει πολύ καλές πιθανότητες να μην επηρεαστεί.

Ωστόσο η αύξηση του bandwidth, δεν είναι από μόνη της μιας επαρκής προστασία ενάντια σε μια τέτοια επίθεση. Παρόλα αυτά, εάν είναι ανεπαρκές, ακόμα και ένας φυσιολογικός όγκος αιτημάτων μπορεί να οδηγήσει σε μια τέτοια δύσκολη κατάσταση.

- **Επίθεση Ping of Death**

Η επίθεση Ping of Death είναι μια άλλη παλιότερη μορφή επίθεσης DoS. Η βασική αρχή της δεν

είναι τόσο έξυπνη όμως καταφέρνει να εκμεταλλευτεί την αδυναμία του TCP/IP πρωτοκόλλου. Η μέθοδος αυτή απλά στέλνει ένα διάγραμμα δεδομένων, το μέγεθος του οποίου ξεπερνάει τα συνηθισμένα.

Όταν ένα τέτοιο διάγραμμα φτάσει στον προορισμό του, το σύστημα που το παραλαμβάνει καταρρέει. Ευτυχώς όμως , τέτοιου είδους επιθέσεις τώρα πια είναι ιστορία επειδή όλοι οι σύγχρονοι εξοπλισμοί διαθέτουν μηχανισμούς άμυνας ενάντια σε τέτοιες επιθέσεις.

- **Επίθεση SYN**

Οι επιθέσεις SYN εκμεταλλεύονται επίσης αδυναμίες του TCP/IP πρωτοκόλλου. Η εγκαθίδρυση μιας σύνδεσης μέσω του TCP/IP, συμπεριλαμβάνει έναν μηχανισμό χειραψίας, στον οποίο έχουμε ανταλλαγή μηνυμάτων συγχρονισμού (Synchronize) και επιβεβαίωσης (Acknowledgment).

Όταν ένας επιτιθέμενος καταφέρει να γεμίσει τον προορισμό με μηνύματα συγχρονισμού (SYN), τότε γεμίζει και ο αποθηκευτικός χώρος τους. Σε αυτή την περίπτωση, δεν είναι δυνατόν να αποσταλούν μηνύματα επιβεβαίωσης (ACK) και κατ' επέκταση δεν είναι δυνατή η δημιουργία TCP/IP συνδέσεων με οποιονδήποτε το επιχειρήσει.

- **Επίθεση Teardrop**

Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει (reassembly) παθαίνει κατάρρευση (crash) ή/και "πάγωμα" (hang) ή/και επανεκκίνηση (reboot). Όπως και η Ping of Death, η επίθεση αυτή είναι τώρα πια ιστορία.

- **Επίθεση Smurf**

Κατά την έναρξη μίας επίθεσης Smurf, ο επιτιθέμενος στέλνει μία πληθώρα πακέτων ping ICMP Echo Request σε διευθύνσεις IP broadcast διαφόρων δικτύων. Τα πακέτα αυτά έχουν τροποποιηθεί κατάλληλα ούτως ώστε στο πεδίο source της κεφαλίδας IP να αναγράφεται η διεύθυνση IP του θύματος και όχι του επιτιθέμενου. Επίσης, δεδομένου ότι στάλθηκαν στην διεύθυνση IP Broadcast των διαφόρων δικτύων, τα λαμβάνουν όλοι οι υπολογιστές που ανήκουν σε αυτά. Αυτό έχει ως συνέπεια όλοι οι υπολογιστές να απαντούν στο ping με πακέτα ICMP Echo Reply, τα οποία έχουν ως διεύθυνση προορισμού την διεύθυνση IP του θύματος. Άρα λοιπόν το θύμα πλημμυρίζει με πακέτα ping και οδηγείται σε κατάρρευση.

Οι επιθέσεις αυτές είναι πιο δύσκολα ανιχνεύσιμες, όμως εάν ένα δίκτυο είναι πολύ καλά οργανωμένο και συντηρείται σωστά, η επίθεση αυτή δε θα είναι καταστροφική. Πριν από αρκετά χρόνια τα περισσότερα δίκτυα υπολογιστών ήταν ευπαθή σε τέτοιου είδους επιθέσεις. Σήμερα όμως έχουν αναπτυχθεί οι κατάλληλες τεχνολογίες ούτως ώστε οι επιθέσεις Smurf να μην αποδίδουν. (Peikari & Fogie, 2002)

ΚΕΦΑΛΑΙΟ 4: ΑΣΥΡΜΑΤΗ ΑΣΦΑΛΕΙΑ

4.1 ΘΩΡΑΚΙΖΟΝΤΑΣ ΤΟ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ

Η αποτυχία των παλιότερων μεθόδων κρυπτογράφησης και η μεγάλη εμβέλεια εκπομπής των ασύρματων δικτύων καθιστούν αναγκαία την ανεύρεση νέων περιοριστικών μεθόδων ασφάλειας που θα ενισχύσουν την προστασία των δεδομένων που μεταφέρονται με μέσο τον αέρα.

Εκτός από την ανεύρεση νέων κρυπτογραφικών μεθόδων, οι προσπάθειες προσανατολίζονται προς την ανεύρεση λύσεων που θα προσφέρουν άμεσα αποτελέσματα μέσω της υπάρχουσας τεχνογνωσίας. Επειδή ο στόχος κάθε επίδοξου εισβολέα είναι το ασύρματο μέσο πρόσβασης (router ή access point), οι παραμετροποιήσεις αυτού του μέσου μπορεί να βοηθήσουν στη διαφύλαξη των δεδομένων.

Στην καθημερινότητα αυτό που συναντάμε είναι ένας ασύρματος δρομολογητής με SSID το όνομα της κατασκευαστικής εταιρείας και εργοστασιακές ρθυμίσεις με ανενεργή οποιαδήποτε μέθοδο κρυπτογράφησης. Σαν προεπιλεγμένη IP address του σημείου πρόσβασης, συναντάμε την 192.168.0.1, 192.168.1.1 ή κάποια άλλη συνηθισμένη διεύθυνση ενώ η ανακάλυψη των προεπιλεγμένων κωδικών πρόσβασης για την διεπαφή από όπου γίνεται η ρύθμιση της συσκευής είναι μια πολυ απλή υπόθεση.

Με προεπιλεγμένη την IP address του σημείου πρόσβασης, username και το password διαχείρισης, το ασύρματο μέσο προσβασης μπορεί πολύ εύκολα να υποκλαπεί ακόμα και από αρχάριους.

Ένας εισβολέας ο οποίος έχει βάλει σκοπό να επιτεθεί στο σύστημα μας, οπωσδήποτε θα έχει κάποια επιτιχυμένη προσπάθεια. Όμως σε ένα οικοιακό περιβάλλον μάλλον κάτι τέτοιο είναι κάπως απίθανο. Για αυτό το λόγο σε αυτό το κεφάλαιο παρουσιάζονται ορισμένα βασικά βήματα που μπορούν να μας βοηθήσουν να κάνουμε ασφαλέστερο ένα οικοιακό δίκτυο. Δυστυχώς αυτές οι ρυθμίσεις μπορούν απλά να καθυστερήσουν και όχι να σταματήσουν έναν έμπειρο επιτιθέμενο.

4.2 ΤΕΧΝΙΚΕΣ ΠΡΟΣΤΑΣΙΑΣ

- **Αλλαγη κωδικου προσβασης στον εξοπλισμο**

Σχεδόν όλα τα ασύρματα σημεία πρόσβασης απαιτούν κωδικούς πρόσβασης για την είσοδο στο διαχειριστικό περιβάλλον τους. Οι πιο πολλές συσκευές έχουν έναν αδύναμο προκαθορισμένο κωδικό, (password / admin) ή και καθόλου. Η αλλαγή των στοιχείων πρόσβασης του διαχειριστή σε ισχυρούς κωδικούς μπορεί να αποτρέψει αυτόν που θα εισβάλει στο δίκτυο να πειράξει τις ρυθμίσεις του εξοπλισμού και να διαχειρίζεται αυτός το ασύρματο δίκτυο.

- **Αλλαγη της προεπιλεγμένης IP διεύθυνσης του εξοπλισμού**

Σίγουρα θα ήταν καλό να αλλάξουμε και την εσωτερική διεύθυνση IP του υπόδικτύου μας αν αυτό μας επιτρέπεται. Το 192.168.x.x εύρος διεύθυνσης προορίζεται μόνο για εσωτερική χρήση. Οι περισσότεροι οι οποίοι χρησιμοποιούν αυτό το εύρος διεύθυνσης, δουλεύουν στο 192.168.0.x για το υπό-δίκτυο τους, το οποίο είναι πολύ εύκολο να μαντέψει κάποιος. Μπορούμε να χρησιμοποιήσουμε οποιοδήποτε αριθμό από το 0 έως το 254 για την Τρίτη οκτάδα, έτσι μπορούμε να χρησιμοποιήσουμε κάτι όπως 192.168.95.x, έτσι ώστε οι τυχών επιτιθέμενοι να χρειαστεί να δουλέψουν περισσότερο. Αυτό μπυρεί να γίνει απενεργοποιώντας τον DHCP server του router και ρυθμίζοντας μόνοι σας τις IP διευθύνσεις του τοπικού δικτύου.

- **Απόκρυψη / Αλλαγη SSID**

Κάθε ασύρματο σημείο πρόσβασης έχει ένα Service Set Identifier (SSID), το οποίο ουσιαστικά είναι το όνομα του δικτύου. Η κύρια λειτουργία του είναι η αναγνώριση του δικτύου. Όταν μια τερματική συσκευή επιθυμεί να συνδεθεί σε ένα δίκτυο χρησιμοποιεί μια ρύθμιση αναγνώρισης η οποία της επιτρέπει να αναγνωρίζει τα διαθέσιμα δίκτυα της περιοχής. Αυτό σημαίνει ότι μπορεί να υπάρχουν περισσότερα από ένα ασύρματα δίκτυα στην ίδια περιοχή. Έτσι οδηγηθήκαμε στη δημιουργία του SSID ώστε να ξεχωρίζουμε τα ασύρματα δίκτυα μεταξύ τους.

Όλα τα ασύρματα σημεία πρόσβασης εκπέμπουν ένα σήμα (beacon) κάθε 1/10 του δευτερολέπτου και το οποίο περιλαμβάνει το SSID μαζί με άλλα δεδομένα. Αυτό το beacon ανιχνεύεται από τις ασύρματες συσκευές και δίνει τις πληροφορίες που χρειάζονται για να συνδεθούν στο δίκτυο. Ωστόσο υπάρχει και η επιλογή να ρυθμίζουμε τις συσκευές στο ασύρματο δίκτυό ώστε να μπορούμε να τις ρυθμίσουμε χειροκίνητα με το επιθυμητό SSID και άλλες συναφής πληροφορίες και να επιτρέπουμε τη σύνδεση στο δίκτυό μας. Η κάθε συσκευή έχει συνήθως ως προεπιλεγμένο SSID το όνομα του κατασκευαστή.

Για να ασφαλίσουμε το οικιακό μας ασύρματο δίκτυο είναι σημαντικό να μην ανακοινώνουμε ότι έχουμε καν SSID, ώστε να να εμποδίσουμε τις ύπουλες ασύρματες συσκευές από το να ανιχνεύσουν και να συνδεθούν στο δίκτυό μας.

Ωστόσο η τακτική αυτή σε δημόσια ή εταιρικά δίκτυα μπορεί να αποβεί μοιραία. Σε αυτές τις περιπτώσεις τα δίκτυα θα πρέπει να εκπέμπουν την ύπαρξή τους, ώστε οι καινούργιες ασύρματες συσκευές να μπορούν να τα ανιχνεύσουν και να συνδεθούν αμέσως σε αυτά. Σε αντίθετη περίπτωση, οι νέες συσκευές θα πρέπει να αναζητούν στην περιοχή το δίκτυο με το συγκεκριμένο SSID και να ρωτούν κάθε τόσο αν είναι το δίκτυο στο οποίο επιθυμούν να συνδεθούν, κεντρίζοντας το ενδιαφέρον των υποψήφιων επιτιθέμενων.

Σε ένα οικοιακό δίκτυο ακόμα και εάν δε θέλουμε να απενεργοποιήσουμε την εμφάνιση του SSID, αυτό που θα πρέπει να κάνουμε είναι να αλλάξουμε το προεπιλεγμένο σε ένα δικό μας μοναδικό, το οποίο μπορεί να είναι μια τυχαία ακολουθία γραμμάτων και αριθμών.

- **Ενεργοποιηση WPA κρυπτογραφησης**

Όπως αποδείχθηκε και στο προηγούμενο κεφάλαιο, η WEP μέθοδος κρυπτογράφησης είναι τόσο αδύναμη ώστε να επιτρέπει σε κάθε επιτιθέμενο με τα κατάλληλα εργαλεία να εισβάλει στο ασύρματο δίκτυο που χρησιμοποιεί αυτή τη μέθοδο. Η WPA (Wi-Fi Protected Access) μέθοδος παρέχει μεγαλύτερη ασφάλεια από την WEP μέθοδο, παρόλα αυτά έχει και αυτή αδυναμίες που μπορεί να εκμεταλλευθεί κάποιος για να προσπεράσει και αυτό το τοίχος προστασίας.

Ειδικότερα, η WPA-PSK (WPA -Pre-Shared Key) είναι ιδιαίτερα ευάλωτη σε επιθέσεις λεξικού (dictionary attacks) αφού όταν ένας σταθμός ζητά να συνδεθεί με σταθμό βάσης (handshake), στέλνει πακέτα στα οποία οπωσδήποτε περιέχεται η μυστική λέξη κλειδί, που έχει οριστεί ως συνθηματικό ταυτοποίησης και εισόδου στο δίκτυο. Έτσι οποιοσδήποτε σταθμός παρακολουθεί την επικοινωνία των δυο μερών μπορεί να συλλέξει πακέτα, που θα χρησιμοποιηθούν σε εφαρμογές που εκτελούν επιθέσεις λεξικού. Είναι γνωστό ότι σε αυτά τα λεξικά υπάρχουν όλοι οι δυνατοί συνδυασμοί 8 χαραχτήρων. Ιδανική θα είναι επίσης η αλλαγή του κλειδιού 2-3 φορές το χρόνο. Η χρήση ενός σωστού κλειδιού είναι πολύ σημαντική αφού η ελάττωση του μήκους του κάτω από τους 20 χαρακτήρες ή/και η χρήση κοινών λέξεων οδηγεί σε μειωμένα επίπεδα ασφαλείας.

Σε συσκευές με WPA2 πιστοποίηση, θα πρέπει να γίνεται χρήση του αλγορίθμου κρυπτογράφησης

CCMP (παραλλαγή του AES) και όχι του συνδυασμού CCMP/TKIP ή AES/TKIP. Σε συσκευές με πιστοποίηση WPA, η χρήση του TKIP είναι προτιμότερη, παρόλα αυτά δε θεωρείται αρκετά ασφαλές αφού ήδη έχουν βρεθεί σοβαρές αδυναμίες του.

- **WEP: Καλυτερο από το τίποτα...**

Εάν η συσκευή που χρησιμοποιείται δεν υποστηρίζει άλλη μέθοδο κρυπτογράφησης παρά την WEP, (συχνό φαινόμενο σε media players, PDAs, and DVRs), αποφύγεται τον πειρασμό να προσπεράσετε τη χρήση της κρυπτογράφησης. Η χρήση της WEP είναι καλύτερη λύση από την απουσία οποιουδήποτε είδους κρυπτογράφησης. Εάν χρησιμοποιήσετε λοιπόν αυτό το είδος κρυπτογράφησης φροντίστε ώστε το μυστικό κλειδί να είναι μεγαλο και δύσκολο για να το μαντέψει κανείς. Επίσης συνίσταται η τακτική αλλαγή του.

- **MAC filtering**

Η διεύθυνση MAC (Media Access Control) είναι η φυσική -μοναδική διεύθυνση για κάθε κάρτα δικτύου. Πρόκειται για έναν 48μπιτο αριθμό καθορισμένο από τον κατασκευαστή. Τα 48 μπιτ του χωρίζονται σε 24 μπιτ και αποτελούν το μοναδικό αναγνωριστικό του κατασκευαστή, εκχωρημένα από την IEEE ενώ τα υπόλοιπα 24 αποτελούν μια μοναδική κάρτα αναγνώρισης. Σε αντίθεση λοιπόν με την IP διεύθυνση, η MAC διεύθυνση είναι μοναδική σε κάθε κάρτα δικτύου, έτσι ενεργοποιώντας το φιλτράρισμα των MAC διευθύνσεων μπορούμε να περιορίσουμε τις συσκευές που θα αποκτήσουν πρόσβασης στο σύστημα μας. Η δυνατότητα αυτή δίνεται μέσα από το διαχειριστικό τμήμα του ασύρματου εξοπλισμού όπου μπορούν να δηλωθούν οι MAC διευθύνσεις των υπολογιστών που μας ενδιαφέρει να έχουν πρόσβαση. Βέβαια αυτή η μέθοδος δεν παρέχει κάποια ουσιαστική ασφάλεια, αφού μια διεύθυνση MAC μπορεί να παραποιηθεί πάρα πολύ εύκολα(όπως δείξαμε στο προηγούμενο κεφάλαιο). Παρ' όλα αυτά, απαγορεύει την σύνδεση στους απλούς χρήστες και καθυστερεί για λίγο μια επίθεση στο ασύρματο σημείο πρόσβασης.

- **Απενεργοποίηση της ασύρματης διαχείρισης του εξοπλισμού**

Το ασύρματο μέσο πρόσβασης θα πρέπει να ρθυμιστεί έτσι ώστε να μην μπορεί κάποιος να έχει πρόσβαση στο διαχειριστικό τμήμα του εξοπλισμού μέσα από την ασύρματη πρόσβαση αλλά μόνο μέσω ενσύρματης. Αυτό θα έχει ώς αποτέλεσμα να αποτρέπει κάθε επιτιθέμενο που θα προσπαθεί να πειράξει το διαχειριστικό σύστημα του σημείου πρόσβασης ασύρματα.

- **Απενεργοποίηση της απομακρυσμένης πρόσβασης**

Οι περισσότεροι ασύρματοι routers προσφέρουν τη δυνατότητα της απομακρυσμένης πρόσβασης

στο διαχριστικό περιβάλλον μέσω internet. Ιδανικά, αυτή η επιλογή θα έπρεπε να υπάρχει μόνο έαν υπήρχε ο τρόπος να καθορίσει ο ίδιος την IP διεύθυνση ή εάν υπήρχε ένα περιορισμένο έυρος σταθμών, οι οποίοι θα μπορούσαν να έχουν πρόσβαση στο ασύρματο μέσο. Κατά κανόνα, εκτός εάν χρειάζεστε αυτή την επιλογή, το καλύτερο είναι να έχετε την έχετε απανεργοποιημένη.

- **Μειωση της ισχύος εκπομπής του ασύρματου μέσου πρόσβασης**

Η δυνατότητα αυτή δεν υπάρχει σε όλους τους ασύρματους routers, αλλά ορισμένοι απο αυτούς επιτρέπουν την μείωση της ισχύος εκπομπής του ασύρματου μέσου. Άν και είναι σχεδόν αδύνατο να ρυθμίσει κάποιος το σήμα τόσο καλά ώστε να περιορίζεται σε ενα χώρο και μόνο, ορισμένες προσπάθειες μπορεί να βοηθήσουν στον περιορισμό της ισχύος εκπομπής και κατ' επέκταση στην μείωση των επικείμενων επιθέσεων. Επίσης θα πρέπει να φροντίσετε για την φυσική θέση του μέσου, η οποία θα πρέπει να είναι όσο το δυνατόν πιο κεντρικά του κτηρίου και μακριά από παράθυρα και εξωτερικούς τοίχους. Τέλος μετακινώντας την κεραία μπορείτε να ελέγξετε την κατεύθυνση του σήματος.

- **Περισσότερες συμβουλές**

Απενεργοποιώντας το UPnP: Μετά την απενεργοποίηση του UPnP μπορείτε να ρυθμίσετε μόνοι σας τις τυχόν πόρτες επικοινωνίας που χρειαζόσαστεγια την λειτουργία των εφαρμογών σας.

Ενεργοποιώντας το firewall: Σε κάθε υπολογιστή που συνδέεται με το τοπικό σας δίκτυο θα πρέπει να υπάρχει ενεργό ένα firewall, είτε αυτό του λειτουργικού σας είτε κάποιο τρίτο.

Απενεργοποιώντας το file και print sharing: Υπάρχει η δυνατότητα απενεργοποίησης του διαμοιρασμού αρχείων και εκτυπωτών ή ακόμα και απεγκατάστασης της υπηρεσίας από την ασύρματη σύνδεση. Για την μεταφορά των αρχείων σας επιλέξτε μια ενσύρματη σύνδεση ή χρησιμοποιήστε κάποιο USB/Flash drive.

Infrastructure mode: Στις ρυθμίσεις σύνδεσης του ασύρματου υπολογιστή επιλέξτε infrastructure τρόπο σύνδεσης και όχι Ad-Hoc. Με αυτό τον τρόπο αποφεύγεται η άμεση επικοινωνία υπολογιστών, χωρίς τη μεσολαβηση του ασύρματου σημείου πρόσβασης.

Περιορίζοντας τον αριθμό των hosts: Μέσω του μηχανισμού διαχείρισης των TCP/IP πρωτοκόλλων είναι δυνατός ο περιορισμός του αποδεκτού αριθμού σταθμών που μπορούν να

συνδεθούν ασύρματα στον εξοπλισμό σας.

Επίσης το ασύρματο δίκτυο θα μπορούσε να απενεργοποιείται και να ανοίγει μόνο τις ώρες που το χρειάζεστε. Ελαχιστοποιώντας έτσι τους κινδύνους επίθεσης αφού δεν θα είναι ανοικτό συνεχώς. (Barken, 2003)

4.3 ΑΛΛΕΣ ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ

Παρότι οι στρατηγικές που αναλύθηκαν παραπάνω μπορεί να προσφέρουν ένα ικανοποιητικό επίπεδο ασφαλειας, σε περιβάλλοντα, όπου η ασφάλεια είναι μείζονος σημασίας (πχ. εργασιακά), απλά δεν αρκούν. Σε αυτές τις περιπτώσεις, θα πρέπει να χρησιμοποιείται επιπλέον hardware ή software, το οποίο θα κάνει το δίκτυο ασφαλέστερο.

4.3.1 FIREWALLS

Ένα ασύρματο δίκτυο θα πρέπει οπωσδήποτε να θεωρείται ανασφαλές και μέρος του διαδικτύου. Σε αυτή την περίπτωση ένα firewall (τοίχος προστασίας) μπορεί να βοηθήσει στην εξάλειψη των κινδύνων ασφαλείας που διατρέχει το δίκτυο. Ανάλογα με την εγκατάσταση και το είδος της πολιτικής που ακολουθείται, ένα firewall μπορεί να αποτρέψει τις μη εξουσιοδοτημένες αιτήσεις. Έτσι δημιουργείται ένα φυσικό εμπόδιο για τους επιτιθέμενους, οι οποίοι μπορεί να έχουν τον έλεγχο του ασύρματου δικτύου και να προσπαθούν να δυεισδύσουν στο εσωτερικό δίκτυο.

Τα firewalls μπορεί να είναι είτε software είτε hardware. Η ιδανική λύση είναι η χρήση και των δυο. Σήμερα όμως οι routers φέρουν ενσωματωμένο firewall και δίνεται η δυνατότητα για ενεργοποίηση / απενεργοποίηση του. Εκτός από την ασφάλεια που παρέχουν τα firewalls όσο αφορά τον περιορισμό της πρόσβασης στο δίκτυο και τον προσωπικό υπολογιστή, επιτρέπει και την ασφαλή απομακρυσμένη πρόσβαση (remote access) μέσα από μηχανισμούς αυθεντικοποίησης.

4.3.2 VPNS

Στη συζήτηση περί firewalls, αξίζει να αναφερθούν και τα VPNs (Virtual Private Network). Το

VPN είναι ένα ιδιωτικό -εικονικό κανάλι, το οποίο βρίσκεται πάνω σε ένα ήδη υπάρχον δίκτυο και υποστηρίζει υπηρεσίες κρυπτογράφησης, πιστοποίησης και διαχείρισης κλειδιών. Το πλεονέκτημα του είναι η ασφαλή μετακίνηση δεδομένων μεταξύ των οντοτήτων.

Ο λόγος όμως για τον οποίο γίνεται αναφορά στα VPNs είναι το γεγονός της συχνής ενσωμάτωσης τους σε εργαλεία ή λογισμικά πακέτα. Έτσι σε ένα firewall μπορούν να δοθούν ρυθμίσεις, οι οποίες θα αποκλείουν εντελώς όλες τις εισερχόμενες αιτήσεις, με εξαίρεση αυτές των πιστοποιημένων VPN σταθμών. Αυτή η μέθοδος δεν δημιουργεί μια δικλίδα ασφαλείας μόνο για το ασύρματο σημείο πρόσβασης αλλά και για τους χρήστες του ασύρματου δικτύου και των δεδομένων τους.

Όπως είδαμε και σε προηγούμενα κεφάλαια, η WEP μέθοδος κρυπτογράφησης είναι ανασφαλής. Ένας επιδέξιος επιτιθέμενος με τα κατάλληλα εργαλεία μπορεί να βρεθεί στην ζώνη εκπομπής του δικτύου σας και να συλλάβει αρκετά πακέτα για να ανακτήσει τον μυστικό κωδικό WEP. Στη συνέχεια με τη βοήθεια αυτού του κωδικού μπορεί να παγιδέψει και όλη την πληροφορία που μετακινείται στον αέρα και να την αποκωδικοποιήσει.

Ωστόσο η χρήση της VPN κρυπτογράφησης σε συνδυασμό με την WEP, αναγκάζει τον επιτιθέμενο να αποκρυπτογραφήσει σε δυο επίπεδα. Στο πρώτο επίπεδο θα πρέπει να βρεθεί ο μυστικός κωδικός της WEP κρυπτογράφησης και στο δεύτερο επίπεδο θα πρέπει να αντιμετωπίσει το ισχυρο τοίχος της VPN κρυπτογράφησης. Επειδή ακριβώς, ακόμα και ένα έμπειρος επιτιθέμενος δε μπορεί με ευκολία να αναπαράγει τον κωδικό της κρυπτογράφησης, να προσπεράσει την πιστοποίηση ή τον έλεγχο πρόσβασης, το ποσοστό επιτυχίας μιας τέτοιας επίθεσης είναι πολύ χαμηλό.

Παρότι η χρήση του VPN και του WEP είναι μια βελτιωμένη πρόταση, υπάρχει ένα τεράστιο μειονέκτημα. Το πρόβλημα προέρχεται από την ανάγκη για διπλάσια επεξεργαστική ισχύ, που προκαλείται από την κρυπτογράφηση και αποκρυπτογράφηση σε δυο επίπεδα. Η χρήση του WEP σε συνδυασμό με το VPN σε ένα σωστά ρυθμισμένο ασύρματο μέσο πρόσβασης μπορεί να ελλαττώσει την ταχύτητα της μετάδοσης κατά 80% . Με άλλα λόγια, θα χρειαστούν περίπου 10 λεπτά για την αποστολή ενός αρχείου με ενεργοποιημένη την WEP κρυπτογράφηση, ενώ χωρίς κρυπτογράφηση θα χρειάζονταν περίπου 2 λεπτά. Αυτό μπορεί να έχει σοβαρές επιπτώσεις στην συνδεσιμότητα και μπορεί να αφανίσει τον ενθουσιασμό μας για την μαγική ασύρματη συνδεσιμότητα.

Επιπλέον, η χρήση ενός VPN δικτύου προυποθέτει την εγκατάσταση λογισμικού σε κάθε σταθμό

που πρόκειται να συνδεθεί στο δίκτυο. Αυτό όμως προσθέτει ακόμα έναν περιορισμό, αφού τα περισσότερα λογισμικά VPN προορίζονται για Windows λειτουργικά. Πράγμα που σημαίνει ότι σταθμοί με λειτουργικά συστήματα όπως MAC OS, linux και υπολογιστές παλάμης (palmtop), μπορεί να μην μπορούν να συνδεθούν στο δίκτυ.

4.3.3 RADIUS

Το πρωτόκολλο Remote Authentication Dial-In User Service (RADIUS) αναπτύχθηκε από την Livingston Enterprises, ως server πρόσβασης, πιστοποίησης και παρακολούθησης. Αν και το πρωτόκολλο αυτό δημιουργήθηκε πριν χρόνια για να εξυπηρετήσει απομακρυσμένους χρήστες ώστε να συνδέονται με ασφάλεια σε εταιρικά δίκτυα, σήμερα χρησιμοποιείται σε VPNs και WLANs για την απόκτηση του ελέγχου κάθε παράμετρου της σύνδεσης.

Το πρωτόκολλο RADIUS βασίζεται στο μοντέλο client/server. Τα σημεία πρόσβασης (NAS-Network Access Servers) θεωρούνται clients του RADIUS. Ο client αναλαμβάνει να προωθήσει την πληροφορία του χρήστη στον αρμόδιο RADIUS server και εκτελεί τις εντολές που θα του σταλούν πίσω από το server.

Ο RADIUS server ή daemon είναι υπεύθυνος για τις υπηρεσίες πιστοποίησης και παρακολούθησης στις συσκευές NAS. Επίσης λαμβάνει τις αιτήσεις σύνδεσης των χρηστών, τις πιστοποιεί και τέλος επιστρέφει όλη τη πληροφορία με τις απαιτούμενες ρυθμίσεις για τους clients ώστε να δοθούν οι αιτούμενες υπηρεσίες στους χρήστες.(Wikipedia)

4.3.4 INTRUSION DETECTION SYSTEMS (IDSS)

Οι ανιχνευτές εισβολέων είναι συσκευές ή λογισμικά παρακολούθησης της κίνησης σε ένα δίκτυο με σκοπό την ανάλυση της για σημάδια κακόβουλων επιθέσεων. Εν συντομία, τα εργαλεία IDSs έχουν ώς σκοπό την ανίχνευση επιθέσεων κατά του υπολογιστή και στη συνέχεια την έκδοση κάποιου είδους προειδοποίησης προς τους ενδιαφερόμενους.

Τα συστήματα αυτά είναι αποτελεσματικά όταν χρησιμοποιούνται σε συνδυασμό με τα ήδη υπάρχοντα μέτρα προστασίας των δικτύων (πολιτική ασφαλείας τρωτών σημείων, κρυπτογράφηση

δεδομένων, ταυτοποίηση του χρήστη, έλεγχο πρόσβασης και τείχη προστασίας).

Τα εν λόγω συστήματα είναι κυρίως απαράιτητα σε μεγάλες ή άλλες επιχειρήσεις με εκτεταμένο δίκτυο. Με αυτό τον τρόπο οι επιχειρήσεις είναι σε θέση να προστατέψουν την επικοινωνίας ανάμεσα στα μέλη της και να εξασφαλίσει, εν μέρει, την προστασία των δεδομένων που ανταλάσσονται ανάμεσα στα μέλη της. Τα IDSs μπορούν να κατηγοριοποιηθούν σε δυο κύριες ομάδες, οι οποίες είναι οι Network IDSs (NIDSs) και Host IDSs (HIDSs).

Τα HIDSs λειτουργούν ψάχνοντας για κάποιο είδος εισβολής σε ένα μόνο σύστημα (host) και το οποίο προστατεύουν. Η λογική εδώ είναι ότι κάθε host προστατεύεται από ένα ξεχωριστό HIDS. Πιο συγκεκριμένα αναλύονται logins, προσβασιμότητα σε αρχεία, μετατροπές δικαιωμάτων κ.α.

Από την άλλη τα NIDSs αναλύουν την κίνηση που υπάρχει σε ολόκληρο το δίκτυο. Συνήθως ένα σύστημα NIDS τοποθετείται στο switch ενός δικτύου και αναλύει κάθε πακέτο που εισέρχεται και εξέρχεται από αυτό.

Εν κατακλείδι, παρότι τα συστήματα αυτά αποτελούν ένα πολύτιμο εργαλείο που μπορεί να εγγυηθεί την αναβάθμισης της ασφάλειας μιας επιχείρησης, σε καμία περίπτωση δε μπορεί να αντικαταστήσει άλλες μεθόδους ασφαλείας. Τα συστήματα αυτά δε μπορούν παρά να χρησιμοποιηθούν σε περιβάλλοντα όπου ισχύουν ήδη τα απαραίτητα μέτρα ασφαλείας. (Wikipedia)

ΚΕΦΑΛΑΙΟ 5. ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 ΑΝΑΚΕΦΑΛΑΙΩΣΗ

Σε αυτό το κεφάλαιο θα γίνει μια σύντομη ανασκόπηση της πτυχιακής εργασίας, των στόχων αλλά και των αποτελεσμάτων αυτής.

Στόχος αυτής της εργασίας ήταν να παρουσιάσει τις αδυναμίες των μεθόδων κρυπτογράφησης – ασφάλειας που εφαρμόζονται σε συστήματα δικτύων ασύρματης επικοινωνίας. Βέβαια αδιαμφισβήτητο γεγονός αποτελεί η πληθώρα των πλεονεκτημάτων που έχει να προσφέρει η ασύρματη επικοινωνία. Η ευελιξία της φορητότητας, η γρήγορη υλοποίηση και το χαμηλό κόστος χρήσης είναι μερικά από τα σημαντικότερα ατού της χρήσης του αέρα ώς μέσο μετάδοσης της πληροφορίας.

Ωστόσο, τα κενά της ασφάλειας σε ένα τέτοιο είδος επικοινωνίας φαίνεται να μεγαλώνουν όλο και πιο πολύ χρόνο με το χρόνο, καθιστώντας αυτού του είδους τις επικοινωνίες εξαιρετικά ανασφαλείς σε περιπτώσεις όπου η προστασία των δεδομένων έχει εξέχοντα ρόλο.

Στην αρχή της παρούσας εργασίας αναφέρθηκαν κάποια εισαγωγικά θέματα που αφορούν τα δίκτυα και ειδικότερα την ασύρματη επικοινωνία. Η ιστορία της ελέλιξης αυτής της τεχνολογίας αποτελεί ένα πολύ σημαντικό κομμάτι για την περαιτέρω εξέλιξη της τεχνολογίας. Κοιτάζωντας πίσω μπορούμε να βρούμε πολλά χαμένα κομμάτια του πάζλ.

Στο επόμενο κεφάλαιο έγινε αναφορά στα δομικά στοιχεία από τα οποία αποτελείται ένα ασύρματο δίκτυο. Η δομή ενός ασύρματου δικτύου επηρεάζει επίσης την ασφάλεια του και τις μεθόδους που μπορούν να εφαρμοστούν για την προστασία των δεδομένων που διακινούνται μέσω αυτού.

Ακολουθώντας μια πορεία προς τα έσω, αναλύθηκε το πρωτόκολλο IEEE 802.11 και όλα τα πρότυπα αυτής της οικογένειας. Τα χαραχτηριστικά, η τοπολογία, και η αρχιτεκτονική του προτύπου προδιαγράφουν την τεχνολογία των ασύρματων δικτύων.

Επίσης αναλύθηκαν οι μηχανιμοί ασφαλείας που χρησιμοποιούνται έως και σήμερα. Γίνεται αναφορά σε μεθόδους κρυπτογράφησης, όπως η περίφημη WEP κρυπτογράφηση και έχουμε μια εκτενή αναφορά στον τρόπο λειτουργίας και στα μειονεκτήματα τα της. Στο ίδιο κεφάλαιο αναφέρονται και οι λύσεις που δόθηκαν για να καλυφθούν τα κενά που άφηνε η προηγούμενη μέθοδος (TKIP, WPA, WPA2).

Στο τρίτο κεφάλαιο αναλύονται ορισμένες από τις πιο κοινές μεθόδους επίθεσης σε ασύρματα δίκτυα. Οι επιθέσεις αυτές χωρίζονται σε δυο κατηγορίες, στις ενεργητικές και στις παθητικές.

Στο τέταρτο κεφάλαιο πραγματοποιούνται πέντε επιτυχημένες επιθέσεις σε ένα ανασφαλές δίκτυο με κρυπτογράφηση WEP.

Τέλος γίνεται μια έκθεση των μεθόδων τις οποίες θα μπορούσε να εφαρμόσει κάποιος για να καθυστερήσει, εάν όχι να εμποδίσει, μια επίθεση σε ένα ανασφαλές ασύρματο δίκτυο.

5.2 ΑΠΟΤΕΛΕΣΜΑΤΑ

Όπως είναι εμφανές, το θέμα της ασφάλειας σε ένα ασύρματο δίκτυο αποτελεί ένα από τα κύρια μειονεκτήματα αυτής της αφοπλιστικά χρήσιμης νέας τεχνολογίας. Σε περιπτώσεις όπου η ασφάλεια των δεδομένων που μεταδίδονται δεν έχουν ιδιαίτερη σημασία τότε θα πρέπει να ληφθούν τα κατάλληλα μέτρα για την περίσταση.

Η μέθοδος κρυπτογράφησης των δεδομένων και της «μεταμφιεσμένης» μεταφοράς τους αποτελεί μια πολύ καλή ιδέα όμως και αυτή έχει τα ελλατώματα της. Έτσι ξεκινώντας από την πρώτη μέθοδο κρυπτογράφησης (WEP), η οποία ενσωματώθηκε στο πρότυπο IEEE 802.11 το 1997, έως και τις πιο συνηθισμένες μεθόδους που χρησιμοποιούνται σήμερα, αποδεικνύεται ότι καμιά από αυτές τις τεχνικές δεν είναι αδιαπέραστες.

Η μέθοδος WEP, ξεκίνησε με τις καλύτερες προυποθέσεις όμως πολύ σύντομα τα κενά της αποδείχθηκαν τεράστια, όπως φάνηκε και στην επίδειξη ανάκτησης του «μυστικού» κλειδιού, στο 4ο κεφάλαιο. Με μια προσπάθεια συλλογής αρκετών IV's πακέτων η επίθεση ήταν απλή υπόθεση. Τα προβλήματα της μεθόδου ξεκινούν από τα IV's, τα οποία είναι αυτά που καθορίζουν κάθε φορά την ψευδοτυχαία ακολουθία που παράγεται από τον αλγόριθμο RC4.

Αμέσως μετά και αφού έγινε έγιναν εμφανή τα κενά που άφηνε στην ασφάλεια η παραπάνω μέθοδος, προτάθηκαν λύσεις όπως η επιμίκυνση κλειδιού και εναλλακτικές μέθοδοι κρυπτογράφησης, όπως WPA/WPA2 και το σύστημα επικύρωσης 802.X.

Παρόλα αυτά, θα πρέπει να αναφερθεί ότι ακόμα και αυτές οι μέθοδοι έχουν αποδειχθεί αρκετά ανασφαλείς με την μέθοδο WPA να σπάει στις αρχές του 2008. Ωστόσο η μέθοδος WPA προσφέρει τη δυνατότητα της χρήσης του αλγόριθμου AES, ο οποίος αποτελεί βελτίωση του RC4, όμως απαιτεί αλλαγή εξοπλισμού που χρησιμοποιείται.

Οπωσδήποτε η αναφορά σε υποστηρικτικές τεχνολογίες, όπως VPNs, IDSs, Firewalls και Radius είναι κάτι παραπάνω από χρήσιμη, όμως πρόκειται για συμπληρωματικό εξοπλισμό που χρησιμοποιείται για να καλύψει τα κενά της υπάρχουσας τεχνολογίας. Σε περιπτώσεις οικιακού περιβάλλοντος δεν συντρέχει κάποιος ιδιαίτερος λόγος για την χρήση του εξοπλισμού, όμως σε επαγγελματικό περιβάλλον είναι συνήθως η μόνη λύση.

5.3 ΤΟ ΜΕΛΛΟΝ ΤΗΣ ΑΣΥΡΜΑΤΗΣ ΑΣΦΑΛΕΙΑΣ

Όπως μπορεί κάποιος εύκολα να συμπεράνει, το μέλλον της ασύρματης ασφάλειας βρίσκεται στα νέα πρότυπα της οικογένειας 802.11, όπως 802.11i και 802.11n.

Το πρότυπο 802.11i, το οποιο εγκρίθηκε για πρώτη φορά την 24η Ιουνίου του 2004, περιλαμβάνει το σύστημα 802.X για επικύρωση (συμπεριλαμβανομένης της χρήσης EAP -Extensible Authentication Protocol), το RSN (Robust Security Network) για την ανίχνευση των συσχετίσεων και τη μέθοδο CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), η οποία βασίζεται στον αλγόριθμο κρυπτογράφησης AES (Advanced Encryption Standard).

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

Το πρότυπο IEEE 802.11 όμως που ορίζει την ασφάλεια της επόμενης γενιάς για τα ασύρματα δίκτυα ονομάζεται IEEE 802.11n. Το πρότυπο ασύρματης δικτύωσης 802.11n παρότι βρισκόταν σε προσχέδιο από τα μέσα του 2006 επικυρώθηκε από την IEEE την 12η Σεπτεμβρίου του 2009.

Οι συσκευές που υποστηρίζουν ασύρματη δικτύωση 802.11n μπορούν να συνδεθούν στα 300Mbps (εξαπλάσια από το πρότυπο 802.11g). Αυτό επιτυγχάνεται με την τεχνολογία MIMO, η οποία κάνει χρήση πολλαπλών κεραιών στο πομπό και το δέκτη, για όσο το δυνατόν μεγαλύτερη ταχύτητα.

Το 802.11n εκπέμπει στα 5GHz όμως διατηρεί την συμβατότητα του με δίκτυα 802.11b/g που εκπέμπουν στα 2.4GHz. Η εμβέλεια του σε εσωτερικούς χώρους υπολογίζεται (θεωρητικά) στα 90 μέτρα ενώ σε εξωτερικούς χώρους στα 182 μέτρα.

Ωστόσο ο τομέας της ασφάλειας στο πρότυπο αυτό παραμένει ένα πρόβλημα προς επεξεργασία, καθώς το νέο αυτό πρότυπο παρότι προσφέρει καινοτόμες δυνατότητες ταχύτητας και εμβέλειας κληρονομεί πολλά από τα αδύναμα σημεία των προηγούμενων προτύπων (802.11a/b/g) σε θέματα ασφάλειας. Όπως συμβαίνει όμως με κάθε νέα τεχνολογία, η έρευνα και η δοκιμή είναι απαρραίτητη διαδικασία για εξέλιξη.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΠΗΓΕΣ

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Barken, L. (2003). *How Secure is Your Wireless Network?* Prentice Hall PTR.
2. Comer, D. (2007). *Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet. Αθήνα: Κλειδάριθμος* .
3. *Flickenger, R. (2003). Wireless Hacks. O'Reilly.*
4. Frankel, S., Bemard, E., Les, O., & Scarfone, K. (2007). *Establishing Wireless Robust Security Networks: A Guide to 802.11i.* Special Publication 800-97.
5. Held, G. (2003). Securing Wireless LANs.
6. Peikari, C., & Fogie, S. (2002). *Wireless Maximum Security.* Sams Publishing.
7. Tanenbaum, A. S. (2000). *Δίκτυα Υπολογιστών.* Αθήνα: Εκδόσεις Παπασωτηρίου.
8. Ε.Μ.Πάλλης. (2000). *Εισαγωγή στα Ασύρματα Δίκτυα.* Ηράκλειο Κρήτης: Τμήμα Εφαρμοσμένης Πληροφορικής.
9. Κατσαβριάς, Κ. (2009). *Μελέτη και Υλοποίηση ανίχνευσης φάσματος για Cognitive Radio σε SIMO συστήματα.*
10. *WireShark. (2010). Retrieved from* http://www.wireshark.ora
11. *Backatrack Penetration Testing Distribution. (2010). Retrieved from* http://www.backtrack-linux.org
12. *Ethercap. (2010). Retrieved from http://ettercap.sourceforge.net*