Τμήμα Μηχανικών Πληροφορικής Τ.Ε

Σχολή Τεχνολογικών Εφαρμογών (έδρα: Σπάρτη)

Τ.Ε.Ι ΠΕΛΟΠΟΝΝΗΣΟΥ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ : ΕΠΙΔΡΑΣΗ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΑΠΟΔΟΣΗ ΤΩΝ ΑΣΥΡΜΑΤΩΝ LAN/MAN IEEE802.11

ΕΛΕΥΘΕΡΙΟΣ ΣΑΝΤΑΣ

ΑΜ:2008084

Επιβλέπων Καθηγητής: Γεώργιος Μπάρδης

Σπάρτη 2015

ΠΕΡΙΛΗΨΗ

Σε αυτήν την πτυχιακή εργασία εξετάζεται η επίδραση των διαφόρων μηχανισμών ασφαλείας στην απόδοση των ασυρμάτων τοπικών και μητροπολιτικών δικτύων 802.11.

Για να γίνει κατανοητό το θέμα της απόδοσης και της ανάγκης ύπαρξης αυτών των μηχανισμών, εξετάζονται οι παράγοντες του φυσικού στρώματος και του στρώματος ζεύξης δεδομένων που τα επηρεάζουν και αναφέρονται οι τύποι των επιθέσεων, οι οποίοι υπάρχουν.

Επίσης, στα πλαίσια της πτυχιακής, θα προσπαθήσουμε να διαπεράσουμε την ασφάλεια κάποιων δικτύων, με διάφορους "βαθμούς δυσκολίας", χρησιμοποιώντας εργαλεία που μας προσφέρει το λειτουργικό Backtack των linux και θα αξιολογήσουμε τον χρόνο και κόπο που χρειάζεται για το κάθε ένα ξεχωριστά.

ΠΕΡΙΕΧΟΜΕΝΑ

Πίνακας εικόνων

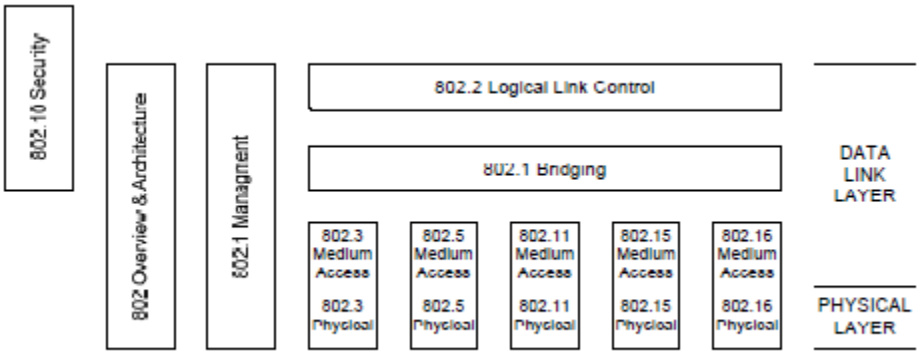
Ασύρματα Δίκτυα IEEE 802.11

1 Εισαγωγή

Τα ασύρματα δίκτυα τύπου έχουν μπει στην καθημερινότητα μας και μπορεί κανείς να τα εντοπίσει σχεδόν παντού. Το WiFi hotspot μπορεί να βρεθεί σε πολλούς χώρους όπως στην εργασία, σε σταθμούς μέσων μαζικής μεταφοράς αλλά ακόμα και σε χώρους διασκέδασης. Ασύρματες κάρτες έχουν εισαχθεί σε κινητά τηλέφωνα, φωτογραφικές μηχανές, κονσόλες παιχνιδιών αλλά ακόμα και σε συσκευές του σπιτιού όπως είναι για παράδειγμα η τηλεόραση. Τα ασύρματα δίκτυα διαδόθηκαν πολύ γρήγορα λόγω της ευκολίας στην υλοποίηση και στην χρήση τους. Παρ' όλα αυτά, η τεχνολογία που βρίσκεται πίσω από την υλοποίηση, αν και άγνωστη για τον τελικό χρήστη, είναι αρκετά απλή.

1.1 Τοπικά και Μητροπολιτικά Δίκτυα 802

Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) είναι υπεύθυνο για την προτοτυποποίηση σχεδόν του συνόλου των τεχνολογιών που αφορούν τα τοπικά και μητροπολιτικά δίκτυα. Σε αυτό το σχήμα φαίνεται η διαστρωμάτωση τους σύμφωνα με το πρότυπο αναφοράς OSI.



Εικόνα 1.1

Το IEEE χωρίζει το στρώμα ζεύξης δεδομένων σε δύο υποστρώματα. Το πάνω υπόστρωμα Logical Link Control είναι κοινό και ανεξάρτητο του φυσικού στρώματος (PHY), το οποίο οδηγεί στην ευκολία της επικοινωνίας μεταξύ των διαφορετικών τεχνολογιών. Ενώ το κάτω υπόστρωμα, Media Access Control (MAC), ορίζει την πρόσβαση αυτών που συμμετέχουν στο δίκτυο στο φυσικό μέσο. Επίσης, τα παραπάνω πρότυπα MAC και PHY,λόγω της στενής σχέσης με το φυσικό στρώμα, δημοσιεύονται ως ένα. Τα κυριότερα από αυτά είναι:

- 802.3 CSMA/CD Access Method and PHY(Ethernet)
- 802.5 Token Ring Access Method and PHY
- 802.11 Wireless LAN MAC and PHY (WiFi)
- 802.15 Wireless MAC and PHY for Personal Area Networks
- 802.16 Air Interface for Fixed Broadband Wireless (WiMax)

1.2 Πρότυπα Ασυρμάτων Δικτύων 802.11

Ο όρος δίκτυα 802.11 περιλαμβάνει μια συλλογή πρωτοτύπων που αφορούν το PHY και το MAC, καθώς και επιμέρους στοιχεία για την αύξηση της απόδοσης και της ασφάλειας των ασυρμάτων δικτύων. Μερικά πρότυπα είναι:

- 802.11-αρχικό MAC και PHY sta 1 και 2 Mpbs
- 802.11a-επέκταση PHY στα 54 Mpbs και 5GHz
- 802.11b-επέκταση PHY στα 11Mpbs και 2.4GHz
- 802.11d-πολλαπλοί ρυθμιστικοί φορείς
- 802.11e-ποιότητα υπηρεσίας (QoS)
- 802.11f-πρωτόκολλο επικοινωνίας μεταξύ Access Points
- 802.11g-επέκταση PHY στα 54Mpbs και 2.4GHz
- 802.11h-έλεγχος ισχύος εκπομπής
- 802.11i-ασφάλεια
- 802.11j-ορισμός καναλιών για την Ιαπωνία στα 5GHz
- 802.11k-μέτρηση
- 802.11m-συντήρηση
- 802.11n[1]-επιπλέον αύξηση της ταχύτητας στα 2.4GHz
- 802.11y-χρησιμοποιεί την τεχνική MIMO με συχνότητα 3.7GHz, PHY στα 54Mpbs και εμβέλεια 5km

1.3 Τοπολογίες Ασυρμάτων Δικτύων

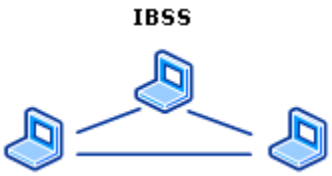
Τα ασύρματα δίκτυα αποτελούνται από τις ασύρματες κάρτες δικτύου (Network Interface Cards, NIC) και τους σταθμούς βάσεις ή τα Access Points(AP) αλλιώς γνωστά ως σημεία πρόσβασης. Η ομαδοποίηση διαφόρων συσκευών για την δημιουργία δικτύου ονομάζεται Service Set.

Η πρόσβαση σε ένα ασύρματο τοπικό δίκτυο επιτυγχάνεται με την εκπομπή σήματος σε συγκεκριμένες συχνότητες. Με μέσο διάδοσης τον αέρα δεν υπάρχει τρόπος χωρικού διαχωρισμού ενός service set από ένα άλλο εντός εμβέλειας και κοινής μπάντας συχνοτήτων. Για να γίνει ο διαχωρισμός των πλαισίων του κάθε service set βοηθάει το Service Set Identifier (SSID). Όσες συσκευές είναι ρυθμισμένες με το ίδιο SSID συμμετέχουν στο ίδιο δίκτυο.

Όταν υπάρχει Access Point στο δίκτυο, αποτελεί το κοινό σημείο επικοινωνίας των συσκευών. Οι κύριες λειτουργίες ενός Access Point είναι η σύνδεση των ασυρμάτων τερματικών με την ενσύρματη υποδομή του τοπικού δικτύου και η υλοποίηση των μηχανισμών ασφαλείας.

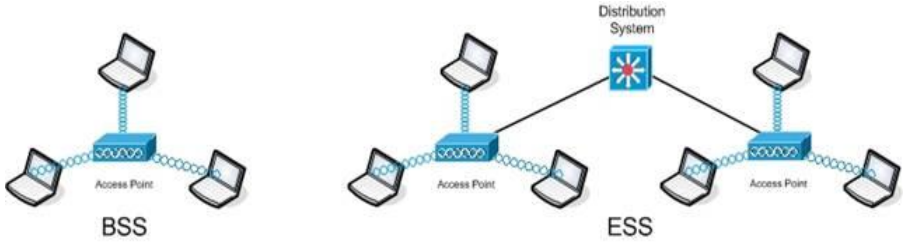
Τα ασύρματα δίκτυα είναι ευέλικτα από τον σχεδιασμό τους και υπάρχουν τρεις τοπολογίες:

- Independent Basic Service Set(IBSS)



Εικόνα 1.2

- Basic Service Set(BSS)
- Extended Service Set(ESS)



Εικόνα 1.3

Η έννοια IBSS δημιουργείται χωρίς την παρουσία AP και είναι στην ουσία ένα απλό peer-to-peer τοπικό δίκτυο. Όλοι οι σταθμοί επικοινωνούν άμεσα ο ένας με τον άλλον. Αυτά τα δίκτυα είναι μικρά και έχουν μικρή διάρκεια ζωής. Τέλος, λόγω ότι δεν υπάρχει AP δεν είναι δυνατή η σύνδεση σε ενσύρματο δίκτυο.

Ένα BSS αποτελείται από σταθμούς που επικοινωνούν μέσω ενός AP.Σε αντίθεση με τα IBSS δεν γίνεται με κατανεμημένο τρόπο αλλά ελέγχεται από το AP. Συνήθως η σύνδεση γίνεται με ενσύρματη υποδομή.

Η σύνδεση πολλών BSS αποτελεί ένα ESS.Η σύνδεση δεν είναι απαραίτητα ενσύρματη αλλά η συνηθέστερη διάταξη είναι πολλά AP να συνδέονται στο σύστημα διανομής του Ethernet για αύξηση της κάλυψης ή του διαθέσιμου εύρους ζώνης του ασύρματου δικτύου.

1.3.1 Επίδραση Λογικής Τοπολογίας

Άσχετα με την φυσική τοπολογία, όλα τα ασύρματα τερματικά ανήκουν στον ίδιο τομέα σύγκρουσης (collision domain) οπότε η λογική τοπολογία είναι δίαυλος. Το μέσο είναι κοινό και συνεχές (αέρας). Το αντίστοιχο στα γνωστά δίκτυα Ethernet είναι τοπολογία αστέρα με κέντρο ένα hub.

Η λογική τοπολογία διαύλου έχει μεγάλο αντίκτυπο στην απόδοση των δικτύων 802.11. Το βασικό αρνητικό είναι ότι το εύρος ζώνης διαμοιράζεται στους συμμετέχοντες.

Για παράδειγμα: Σε ένα δίκτυο 802.11g με ταχύτητα 56Mbps και 10 τερματικά, η ωφέλιμη ταχύτητα του κάθε τερματικού θα είναι 5.6Mpbs.Επίσης, λόγω ότι χρησιμοποιείται το ίδιο μέσο για αποστολή και λήψη δεδομένων αποκλείει την επικοινωνία full duplex.

Τέλος ένας πιο γνωστός τρόπος δικτύωσης είναι το Fast Ethernet (IEEE 802.3u) 100baseT στα 100Mpbs με χρήση switch. Το switch επιτρέπει την λειτουργία full duplex και κάθε τομέας σε κάθε θύρα του αποτελεί διαφορετικό collision domain. Αυτό λοιπόν εξασφαλίζει σε κάθε χρήστη 100Mpbs για αποστολή και 100Mpbs για λήψη. Επιπλέον, κάθε δυνατό ζεύγος χρηστών μπορεί να επικοινωνεί ανεξάρτητα από κάποιο άλλο.

1.4 Μηχανισμοί Πρόσβασης στο Μέσο

Στα ενσύρματα δίκτυα Ethernet ο μηχανισμός που χρησιμοποιείται για πρόσβαση στο μέσο είναι ο CSMA/CD. Δηλαδή, αν κάποιος σταθμός θέλει να στείλει δεδομένα, στην αρχή ελέγχει το καλώδιο και περιμένει μέχρι να μην στέλνει κάποιος άλλος και στην συνέχεια ξεκινάει την αποστολή. Εάν δύο ή περισσότεροι σταθμοί αρχίσουν να στέλνουν ταυτόχρονα υπάρχει collision, την οποία την ανιχνεύουν (Collision Detection). Όλοι οι σταθμοί σταματούν την αποστολή και περιμένουν ένα τυχαίο χρονικό διάστημα και επαναλαμβάνουν την διαδικασία. Μια ταυτόχρονη εκπομπή στα ενσύρματα δίκτυα είναι πολύ εύκολα ανιχνεύσιμη αφού αυξάνεται η τάση στο καλώδιο. Επίσης, το μέσο διάδοσης είναι αρκετά σταθερό και ελεύθερο από παρεμβολές και ο αποστολέας μπορεί να υποθέσει ότι η πληροφορία έχει φτάσει στο παραλήπτη, από την στιγμή που δεν συνέβη κάποια σύγκρουση.

1.4.1 CSMA/CA

Τα παραπάνω δεν μπορούν να εφαρμοστούν ως έχουν σε ένα ασύρματο περιβάλλον. Δεν υπάρχει καμία βεβαιότητα κατά την αποστολή και το κυριότερο, δεν υπάρχει τρόπος ανίχνευσης μιας σύγκρουσης. Αυτό οδήγησε σε ένα πιο πειθαρχημένο σχήμα γνωστό ως Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) που έχει σαν στόχο την αποφυγή των συγκρούσεων από την αρχή. Οι κυριότερες προσθήκες και αλλαγές είναι:

- Πριν την εκκίνηση της εκπομπής, ο αποστολέας ενημερώνει για την διάρκεια της.
- Κανένας άλλος σταθμός δεν μπορεί να εκπέμψει πριν το πέρας του παραπάνω χρονικού διαστήματος.
- Ο αποστολέας δεν έχει την δυνατότητα να ξέρει αν οι πληροφορίες του έχουν φτάσει. Ο παραλήπτης θα πρέπει να στέλνει επιβεβαίωση.
- Αν δύο σταθμοί αρχίσουν να εκπέμπουν ταυτόχρονα, δεν μπορούν να ξέρουν ότι υπάρχει σύγκρουση. Μετά το τέλος της αποστολής καταλαβαίνουν ότι υπήρχε πρόβλημα γιατί δεν λαμβάνουν επιβεβαίωση.
- Σε περίπτωση που δεν ληφθεί επιβεβαίωση, οι συμμετέχοντες στο δίκτυο περιμένουν για ένα τυχαίο χρονικό διάστημα πριν επιχειρήσουν να ξαναστείλουν.

Σύμφωνα με το πρότυπο του IEEE υπάρχουν 4ις συνιστώσες που ολοκληρώνουν το CSMA/CA:

- Ανίχνευση του φέροντος (Carrier Sense)
- Distributed Coordination Function (DCF)
- Πλαίσια επιβεβαίωσης (ACK)
- Κράτηση του μέσου RTS/CTS (Request to Send/Clear to Send)

1.4.2 NAV

Ένας σταθμός που θέλει να εκπέμψει πρέπει πρώτα να βεβαιωθεί ότι το μέσο δεν χρησιμοποιείται, όπως αναφέρθηκε παραπάνω. Στα ασύρματα δίκτυα, υπάρχει περίπτωση το μέσο να είναι σε χρήση από κάποιον σταθμό ακόμη και αν δεν υπάρχει εκπομπή.

Ο τρόπος που χρησιμοποιείται από τους σταθμούς για να ελέγξουν την κατάσταση του φυσικού στρώματος ονομάζεται διάνυσμα Κατανομής Δικτύου (Network Allocation Vector ή NAV). Το NAV είναι ένας μετρητής που συγχρονίζεται από τα πλαίσια που εκπέμπονται στο μέσο. Δηλαδή ουσιαστικά είναι ο χρόνος που χρειάζεται ο αποστολέας για την εκπομπή των δεδομένων του συν τον χρόνο για επιβεβαίωση.

1.4.3 DCF (Distributed Coordination Function)

Το IEEE ονομάζει την κύρια διαδικασία πρόσβασης στο μέσο για τα δίκτυα 802.11 Distributed Coordination Function ή DCF. Σύμφωνα με την λειτουργία του DCF, κάθε σταθμός, ο οποίος έχει δεδομένα για εκπομπή, θα πρέπει να περιμένει κάποιο τυχαίο χρονικό διάστημα πριν αρχίσει την εκπομπή. Χωρίς αυτή την διαδικασία, όλοι οι σταθμοί που περιμένουν τον μετρητή NAV θα άρχιζαν να εκπέμπουν ταυτόχρονα μετά τον μηδενισμό του, όπου θα υπάρξει πρόβλημα λόγω των υπερβολικών αριθμών συγκρούσεων.

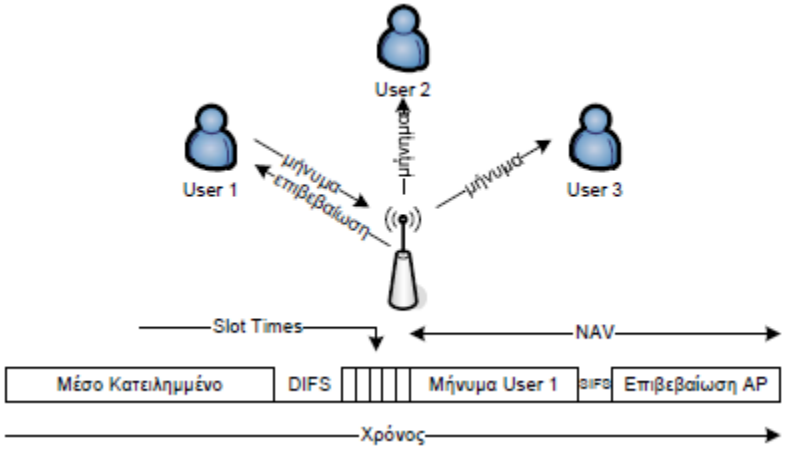
Το χρονικό διάστημα που περιμένει κάθε σταθμός ορίζεται από το DCF Interval (DIFS) και από την τιμή ενός μετρητή που ονομάζεται backoff timer. Η τιμή του backoff timer δημιουργείται από την NIC τοπικά σε κάθε σταθμό και είναι τυχαία με εύρος τιμών από 0 έως την τιμή contention window (CW). Η CW είναι μια σταθερά που εξαρτάται από τους κατασκευαστές.

Η τιμή εκκίνησης του μετρητή backoff δεν είναι ο χρόνος μετά το DIFS αλλά ο αριθμός των χρονοθυρίδων που πρέπει να περιμένει επιπλέον ο κάθε σταθμός. Η διάρκεια της κάθε χρονοθυρίδας ορίζεται από το πρωτότυπο του φυσικού στρώματος.

Ο χρόνος αναμονής του κάθε σταθμού υπολογίζεται ως εξής:

Total=DIFS+(Backoff)*(Timeslots)

Τα παραπάνω σχετικά με τον χρόνο που μεσολαβεί μεταξύ δύο πλαισίων ισχύουν για κάθε τύπο εκτός από τα πλαίσια επιβεβαίωσης. Αν ο σταθμός δεν λάβει έγκαιρα επιβεβαίωση για τα απεσταλμένα δεδομένα τότε θεωρεί ότι έχουν απορριφτεί.



Εικόνα 1.4

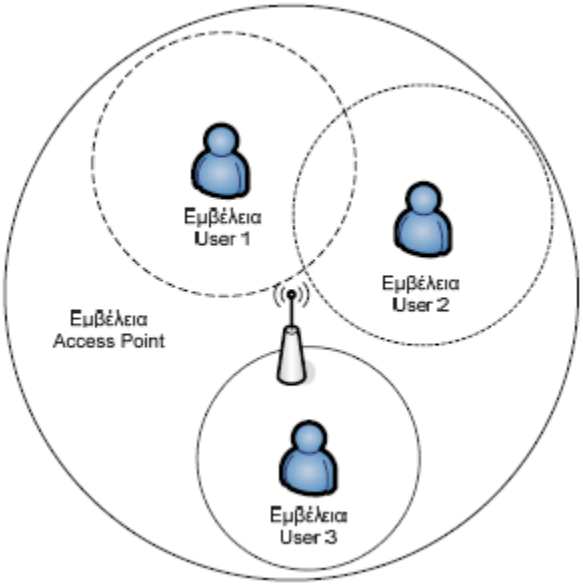
Η προτεραιότητα των πλαισίων επιβεβαίωσης εξασφαλίζεται από το MAC με 2 τρόπους:

Κατά την κράτηση του μέσου μέσω του μετρητή NAV συμπεριλαμβάνεται και ο χρόνος για την επιβεβαίωση. Αλλά σε ένα ασύρματο περιβάλλον, ο χρόνος του NAV είναι μια πρόβλεψη. Αν λοιπόν το NAV δεν τα καταφέρει, το πρότυπο προβλέπει ένα ειδικό χρονικό διάστημα, το short interframe speca (SIFS), που σε κάθε περίπτωση δίνει προτεραιότητα στα πλαίσια επιβεβαίωσης αφού η διάρκεια του είναι κατά δυο χρονοθυρίδες μικρότερη από αυτή του DIFS.(εικ. 1.4)

1.4.4 Κρυμμένος Κόμβος

Κατά την περιγραφή του CSMA/CA αναφέρεται ότι κάθε σταθμός θα πρέπει να ελέγχει το φυσικό μέσο για την διαθεσιμότητα του. Αυτό σημαίνει ότι κάθε σταθμός μπορεί να ακούει τους άλλους.

Παράδειγμα:



Εικόνα 1.5

Όλοι οι χρήστες είναι εντός εμβέλειας του AP, όμως ο χρήστης 3 είναι εκτός εμβέλειας από τους 1 και 2. Με αποτέλεσμα να μην γνωρίζει πότε αυτοί οι δυο εκπέμπουν ή όχι. Αυτό είναι γνωστό ως πρόβλημα του κρυμμένου κόμβου. Το ίδιο πρόβλημα αντιμετωπίζουν και δίκτυα που χρησιμοποιούν δυο τεχνολογίες ταυτόχρονα. Για παράδειγμα όταν συνυπάρχουν τερματικά 802.11g και 802.11b.

Η λύση στο πρόβλημα είναι η διαιτησία του AP και τα πλαίσια RTS/CTS, Ο σταθμός που θέλει να εκπέμψει στέλνει ένα πλαίσιο RTS ως αίτηση εκπομπής στο AP μαζί με τον χρόνο NAV. Το AP αποστέλλει σε όλους τους χρήστες πλαίσια CTS που τους ενημερώνει ποιος σταθμός έχει προτεραιότητα και για πόσο χρονικό διάστημα. Τα CTS είναι μια ακόμη περίπτωση πλαισίων προτεραιότητας και εκπέμπονται από το AP μετά από χρόνο SIFS.

Ουσιαστικά αυτή η διαδικασία RTS/CTS καθυστερεί και μειώνει την απόδοση του δικτύου. Πολλά AP επιτρέπουν από τις ρυθμίσεις την απενεργοποίηση της όλης διαδικασίας αν ο διαχειριστής του δικτύου συμφωνεί ότι δεν υπάρχει πρόβλημα κρυμμένου κόμβου.

1.5 Σύνδεση Σταθμών

Η σύνδεση ενός σταθμού σε ένα ενσύρματο δίκτυο μπορεί να είναι πολύ απλή. Η συσχέτιση ενός ασύρματου τερματικού με το κατάλληλο AP μπορεί να είναι ακόμα πιο απλούστερη, δηλαδή απλώς να βρεθεί εντός εμβέλειας και αυτό είναι ένας από τους λόγους που υπάρχουν τόσα προβλήματα στην ασφάλεια. Αν και γίνεται εύκολα η σύνδεση, υπάρχουν τρεις διακριτές διαδικασίες:

- Διαδικασία βολιδοσκόπησης (probe)
- Διαδικασία πιστοποίησης (authentication)
- Διαδικασία συσχέτισης (association)

Κατά την εκκίνηση μιας ασύρματης κάρτας δικτύου, είναι αδύνατο να γνωρίζει οτιδήποτε για τα διαθέσιμα ασύρματα δίκτυα που βρίσκονται εντός εμβέλειας. Η διαδικασία βολιδοσκόπησης εξυπηρετεί στην ανεύρεση των διαθέσιμων δικτύων και ξεκινάει με τον σταθμό να στέλνει πλαίσια probe request σε όλα τα κανάλια και στην μικρότερη δυνατή ταχύτητα του 1Mbps. Οι κυριότερες πληροφορίες που αποστέλλονται με αυτό τον τρόπο είναι τα SSID με τα οποία είναι ρυθμισμένος ο σταθμός και οι ταχύτητες που υποστηρίζονται από την κάρτα δικτύου.

Όταν ένα AP λάβει ένα probe frame χωρίς σφάλματα απαντάει με ένα probe response που περιέχει τις απαραίτητες πληροφορίες για την συνέχεια της διαδικασίας. Τα κυριότερα τμήματα του πλαισίου probe response είναι:

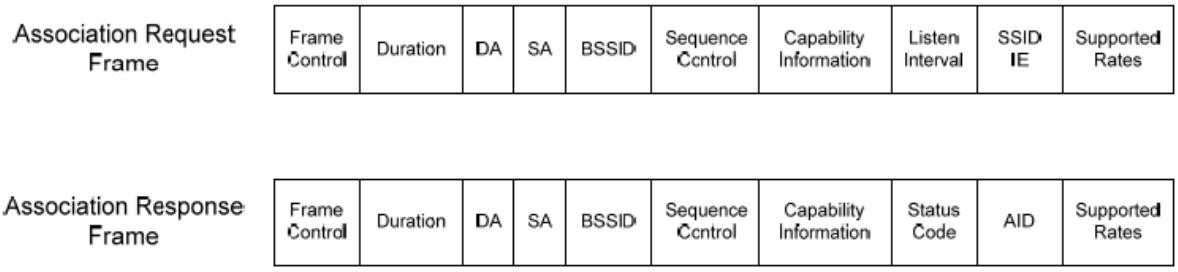
- Timestamp: Χρησιμοποιείται για τον συγχρονισμό των clock του σταθμού και του AP
- Capability Information: Οι δυνατότητες του AP στα PHY και MAC
- SSID Element: Το SSID με το οποίο είναι ρυθμισμένο το AP
- Support Rates Element: Όλες οι υποστηριζόμενες ταχύτητες
- PHY Parameter Set: Αν το AP χρησιμοποιεί αναπήδηση συχνοτήτων ή κάποια από τις άλλες τεχνολογίες φυσικού μέσου

Όταν ένας σταθμός λάβει το probe response frame, εκτός των άλλων πληροφοριών, μπορεί να μετρήσει την ισχύ του σήματος του κάθε AP. Ο μηχανισμός που χρησιμοποιείται από τις ασύρματες κάρτες δικτύου για την επιλογή του καταλληλότερου AP δεν αναφέρεται σε κανένα πρότυπο του IEEE αλλά αφήνεται στους κατασκευαστές. Συνήθως τα κριτήρια είναι το SSID, η ισχύς του σήματος και οι υποστηριζόμενες ταχύτητες.

Με την επιλογή του AP από τον σταθμό τελειώνει η διαδικασία βολιδοσκόπησης και ξεκινάει η διαδικασία πιστοποίησης. Με την διαδικασία πιστοποίησης, το AP ελέγχει αν ο σταθμός και ο

χρήστης έχει δικαίωμα να χρησιμοποιήσει το δίκτυο. Η διαδικασία πιστοποίησης είναι στενά δεμένη με την έννοια της ασφάλειας.

Εάν ο σταθμός πιστοποιηθεί με επιτυχία, ξεκινάει η διαδικασία συσχέτισης του σταθμού με το AP. Η διαδικασία συσχέτισης επιτρέπει στα AP να καθορίσουν μια πύλη εισόδου, μια λογική θύρα στο δίκτυο, για τους σταθμούς. Στην αρχή, ο σταθμός στέλνει ένα πλαίσιο association request με τις δυνατότητες του. Στην συνέχεια, το AP απαντάει με ένα πλαίσιο association response που ενημερώνει τον σταθμό για την αποδοχή του ή όχι στο δίκτυο. Σε περίπτωση αποτυχίας αποστέλλεται και ο κωδικός σφάλματος. Αν όμως είναι επιτυχής το AP χαρτογραφεί τον σταθμό, δίνοντας του ένα αναγνωριστικό κωδικό συσχέτισης association identifier (AID).



Εικόνα 1.6

Τα σημαντικότερα πεδία του πλαισίου association request είναι αυτά που αφορούν το SSID και τις υποστηριζόμενες ταχύτητες. Τα αντίστοιχα στο πλαίσια association response είναι:

- Status Code: Μας δείχνει την επιτυχία ή αποτυχία και τον λόγο αυτής.
- Association ID: Όπως το AID, είναι το αντίστοιχο μιας θύρας ενός hub ή ενός switch στα ασύρματα.

1.6 Πλαισίωση Δεδομένων

Η πλαισίωση δεδομένων είναι η διαδικασία προσθήκης πληροφοριών πριν και μετά τα δεδομένα του χρήστη ώστε να εξασφαλιστεί η σωστή δρομολόγηση τους στο δίκτυο.

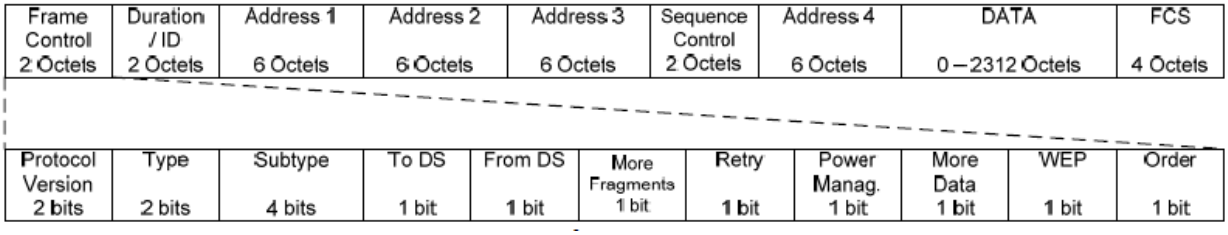
Σε ένα δίκτυο Ethernet οι απαραίτητες πληροφορίες για την σωστή αποστολή και λήψη του πακέτου του στρώματος δικτύου είναι:

- Preamble και Start of Frame Delimiter: Ακολουθία από εναλλασσόμενα 0 και 1 που σηματοδοτούν την έναρξη του πλαισίου.
- Destination Address: Η διεύθυνση MAC του παραλήπτη
- Source Address: Η διεύθυνση MAC του αποστολέα ώστε ο παραλήπτης να μπορεί να απαντήσει.

- Type: Ο τύπος του πρωτοκόλλου που χρησιμοποιείται στο στρώμα δικτύου.
- Frame Check Sequence: Μια τιμή για τον έλεγχο της ακεραιότητας των δεδομένων.

Για ακόμα μια φορά οι απαιτήσεις και οι δυσκολίες της ασύρματης μετάδοσης των δεδομένων στο 802.11 οδήγησαν σε ένα αρκετά πολυπλοκότερο σχήμα. Παρακάτω φαίνεται η γενική μορφή ενός 802.11 MAC πλαισίου και το ανάπτυγμα του πεδίου Frame Control:

- Frame Control: Το κυριότερο πεδίο με 11 πεδία με πληροφορίες που δείχνουν τον τύπο του πλαισίου, την διαχείριση ενέργειας, την κρυπτογράφηση κτλ.
- Duration/ID: Είναι ο χρόνος που θα χρειαστεί για την αποστολή και την επιβεβαίωση
- Address 1,2,3,4: Η χρήση τους εξαρτάται από τα πεδία type και sub-type του frame control.
- Sequence Control: Μας δείχνει αν η πληροφορία στο πλαίσιο είναι συνέχεια από προηγούμενο πλαίσιο ή όχι και την σειρά του.
- Frame Check Sequence: Όμοια με το Ethernet



Εικόνα 1.7

Το 802.11, εκτός από περισσότερα πεδία στο header, προβλέπει 3ις κύριους τύπους πλαισίων στο υπόστρωμα MAC:

- Τα πλαίσια δεδομένων μεταφέρουν τα δεδομένα των χρηστών του δικτύου. Το μέγιστο "ωφέλιμο φορτίο" τους είναι 2312 bytes.
- Τα πλαίσια ελέγχου διευκολύνουν την ανταλλαγή δεδομένων κατά την κανονικά λειτουργία του δικτύου (RTS,CTS κτλ.)
- Τα διαχειριστικά πλαίσια χρησιμοποιούνται κατά την σύνδεση των σταθμών.(probe,authentication,association κτλ)

1.7 Απόδοση του στρώματος ζεύξης δεδομένων

Τρόπος Σύνδεσης	Διαμόρφωση	Μέγιστη Ταχύτητα Σύνδεσης	Θεωρητική Μέγιστη (TCP)	Θεωρητική Μέγιστη (UDP)
802.11b	CCK	11 Mbps	5,9 Mbps	7,1 Mbps
802.11g (με 802.11b)	OFDM / CCK	54 Mbps	11,4 Mbps	19,5 Mbps
802.11g	OFDM / CCK	54 Mbps	24,4 Mbps	30,5 Mbps
802.11a	OFDM	54 Mbps	24,4 Mbps	30,5 Mbps

Εικόνα 1.8

Σε αυτό τον πίνακα φαίνονται οι θεωρητικές μέγιστες αποδόσεις των διαφόρων τεχνολογιών του προτύπου 802.11.

Μια πρώτη παρατήρηση που μπορεί να γίνει είναι ότι η υποβάθμιση της μέγιστης ταχύτητας του link στην θεωρητική μέγιστη είναι ανεξάρτητη της τεχνολογίας φυσικού στρώματος. Η υποβάθμιση της ταχύτητας είναι η ίδια στο 802.11g και στο 802.11a παρόλο που έχουν διαφορετικά PHY με το πρώτο να λειτουργεί στα 2.4GHz και το δεύτερο στα 5GHz. Οπότε το overhead οφείλεται αποκλειστικά σε διεργασίες του στρώματος ζεύξης δεδομένων που είναι κοινές σε όλους τους τρόπους σύνδεσης.

Η πλαισίωση των δεδομένων εισάγει επιπλέον πληροφορία και η λειτουργία του 802.11 προβλέπει και κάποια διαχειριστικά πλαίσια κατά την κανονική χρήση του δικτύου αλλά αυτά δεν είναι ικανά να εξηγήσουν μια πτώση σχεδόν 45%.

Την πραγματικά μεγάλη διαφορά από την ονομαστική ταχύτητα την κάνει η διαδικασία πρόσβασης στο μέσο και η καθυστέρηση που εισάγεται από την επιβεβλημένη επιβεβαίωση των αποσταλμένων δεδομένων.

Τέλος, μια ακόμη παρατήρηση που μπορεί να γίνει είναι ότι η μεγαλύτερη υποβάθμιση παρατηρείται σε περιπτώσεις που στο δίκτυο υπάρχουν τερματικά διαφορετικών αλλά συμβατών τεχνολογιών όπως στην περίπτωση του 802.11b και του 802.11g. Η επιπλέον καθυστέρηση μπορεί να χρεωθεί στο πρόβλημα κρυμμένου κόμβου που δημιουργείται και στην διαδικασία Request to Send/Clear to Send που καλείται να λύσει.

2 Γενικά

Οι χρήστες ενός ασύρματου δικτύου μπορούν να επωφεληθούν από ένα σωρό πλεονεκτήματα, όμως σε αυτή την περίπτωση τίθεται ένα μεγάλο ερώτημα. Πόσο ασφαλής είναι η επικοινωνία σε ένα σύστημα όπου το μέσο μετάδοσης είναι ο αέρας?

Η λύση έχει δοθεί με τις μεθόδους πιστοποίησης και κρυπτογράφησης των δεδομένων που χρησιμοποιούνται ευρέως σήμερα. Σε ένα ενσύρματο τοπικό δίκτυο οι απειλές αντιμετωπίζονται στο σημείο εξόδου ISP με πολιτικές ασφαλείας στους δρομολογητές, με firewall κτλ.

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

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

2.1 Επικύρωση και Μυστικότητα

Ουσιαστικά η έννοια της επικύρωσης αφορά τον έλεγχο πρόσβασης. Για να πραγματοποιήσουμε την επικύρωση πρέπει να αποκτήσουμε πρώτα έλεγχο πρόσβασης στο μέσο και στη συγκεκριμένη περίπτωση στο ασύρματο δίκτυο. Αρχικά ελέγχονται τα διαθέσιμα ασύρματα δίκτυα και στην συνέχεια το δίκτυο επικυρώνει το σταθμό και το ανάποδο.

Τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται beacons-πλαίσια διαχείρισης. Τα beacons είναι αυτά τα οποία ανακοινώνουν την ύπαρξη ενός ασύρματου δικτύου και το κάθε beacon περιλαμβάνει ένα SSID. Ένας σταθμός μπορεί να επιλέξει να συνδεθεί σε ένα δίκτυο είτε παθητικά είτε αρνητικά. Στην παθητική σάρωση ο σταθμός ελέγχει τα κανάλια προσπαθώντας να βρει beacon από τα σημεία πρόσβασης και στην αρνητική στέλνει αιτήσεις διερεύνησης, είτε σε ένα συγκεκριμένο SSID ή με το SSID

ρυθμισμένο στο 0, σε όλα τα κανάλια ένα προς ένα. Όλοι οι σταθμοί πρόσβασης που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση.

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

Στο πρότυπο 802.11 έχουμε δύο ειδών τρόπους επικύρωσης:

- Την επικύρωση ανοιχτού κλειδιού(Open System Authentication-OSA)
- Την επικύρωση μοιρασμένου κλειδιού(Shared Key Authentication_SKA)

Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στο μήνυμα επικύρωσης. Το δίκτυο μπορεί να δεχτεί ή να απορρίψει αναλόγως τις ρυθμίσεις ασφαλείας. Χρησιμοποιώντας την επικύρωση ανοιχτού κλειδιού, οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης όμως όχι και να επικοινωνήσει. Η συσκευή μπορεί να επικοινωνεί μόνο αν τα κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης.

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

2.2 Κρυπτογράφηση WEP

Κρυπτογράφηση ονομάζεται η διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή προκειμένου να επιτευχθεί η ασφαλής μετάδοση πληροφοριών. Τα δεδομένα πριν από την κρυπτογράφηση ονομάζονται plaintext ενώ τα δεδομένα μετά την κρυπτογράφηση αποτελούν το cipher text. Η αντίστροφη διαδικασία μετατροπής ονομάζεται αποκρυπτογράφηση.

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

Η πιο γνωστή επιλογή παροχής ασφάλειας για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11 είναι το WEP. Με την επιλογή του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν επιθυμούμε εμπιστευτικότητα,

μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλθούν.

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

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

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

- **Διάνυσμα Αρχικοποίησης:** Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στην κρυπτογράφηση WEP έχουν μήκη 40 ή 104 bits. Ωστόσο συχνά ακούμε να μιλάνε για 64 ή 128 bits. Αυτό συμβαίνει επειδή κάποιοι παραλείπουν να αναφέρουν τα επιπλέον 24 bits που χρησιμοποιούνται από το διάνυσμα αρχικοποίησης(Initialization Vector-IV)
  Το IV ουσιαστικά αλλάζει για κάθε πακέτο και συνδυάζεται με το μυστικό κλειδί. Το αποτέλεσμα αυτών των δυο κρυπτογραφείται. Έτσι ακόμα και εάν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική.
  Τέλος το IV δεν είναι μυστικό, ενώ στέλνεται σε μη κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV.

- **<u>Τα κλειδιά που χρησιμοποιούνται στο WEP:</u>**

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

- **Σταθερό μήκος**: Συχνά 40 ή 104 bits
- **Στατικά**: Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.
- **Διαμοιραζόμενα**: Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
- **Συμμετρικά**: Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

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

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

Οι πιο κοινές εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά RC4 64bit. Το μεγαλύτερο μέρος της βιομηχανίας όμως έχει κινηθεί προς ένα 128bit δημόσιο RC4 κλειδί. Το πρότυπο 64bit WEP χρησιμοποιεί ένα κλειδί 40bit το οποίο συνδέεται με την αρχή ενός 24bit διανύσματος και διαμορφώνει το RC4 κλειδί κυκλοφορίας.
Ένα 128bit WEP κλειδί σχεδόν πάντα εισάγεται από τους χρήστες σαν μια ακολουθία 26 δεκαεξαδικών χαρακτήρων(0-9 και A-F). Κάθε χαρακτήρας αντιπροσωπεύει 4bit του κλειδιού, 26 ψηφία 4bit δίνουν 104bit και η προσθήκη του 24bit IV παράγει το τελικό 128bit κλειδί WEP. Ένα 256bit σύστημα WEP είναι διαθέσιμο από μερικούς προμηθευτές και όπως με το 128bit WEP, τα 24bit είναι για το IV, αφήνοντας 232 πραγματικά bit για την προστασία.

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

- **<u>Διανομή κλειδιού:</u>** Το βασικότερο μειονέκτημα του WEP είναι το πρόβλημα της διανομής κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να

μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το 802.11 πρότυπο δεν παρέχει ένα μηχανισμό παραγωγής κλειδιού έτσι ο καθένας μας πρέπει να δαχτυλογραφεί το κλειδί στον οδηγό της συσκευής ή να έχει πρόσβαση σε συσκευές με το χέρι.

Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

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

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

  Το σύνολο των bytes του μηνύματος συνενώνονται στον έλεγχο κυκλικού πλεονασμού(Cyclic Redudancy Check-CRC). Η τιμή αυτή, μήκους 4bytes, προστίθεται στο τέλος του πλαισίου πριν από την επεξεργασία για μετάδοση.
  Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή CRC από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα.

  Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη, δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι σε θέση να υπολογίσει τη νέα τιμή CRC και να αντικαταστήσει την αρχική. Το ICV λειτουργεί όπως το CRC, αλλά υπολογίζει και εφαρμόζεται πριν την διαδικασία της κρυπτογράφησης. Το CRC ωστόσο προστίθεται και μετά την κρυπτογράφηση.
  Επομένως ο εισβολέας δεν μπορεί να υπολογίσει το μήνυμα εκ νέου. Έτσι το ICV υπολογίζεται ως ένας συνδυασμός όλων των δεδομένων και προκύπτει ως μια τιμή μήκους 4 bytes, η οποία προστίθεται στο τέλος.

- **<u>Αλγόριθμος κρυπτογράφησης RC4:</u>** Ο αλγόριθμος χρησιμοποιείται κατά την διαδικασία της κρυπτογράφησης WEP. Ο RC4 είναι απλός στην υλοποίηση και ισχυρός. Επίσης σημαντικό είναι το γεγονός ότι οι αδυναμίες του WEP δεν οφείλονται στον ίδιο τον RC4 αλλά στον τρόπο χρήσης του μέσα στον WEP. Βασική ιδέα είναι η δημιουργία μιας τυχαίας ακολουθίας bytes, που ονομάζεται ροή κλειδιού(key stream) και έχει ως στόχο το συνδυασμό της με τα δεδομένα μέσω της λογικής πράξης του αποκλειστικού Η (XOR). ΜΙΑ σημαντική ιδιότητα της XOR είναι:

  A(XOR)B = C, *τότε* C(XOR)B = A

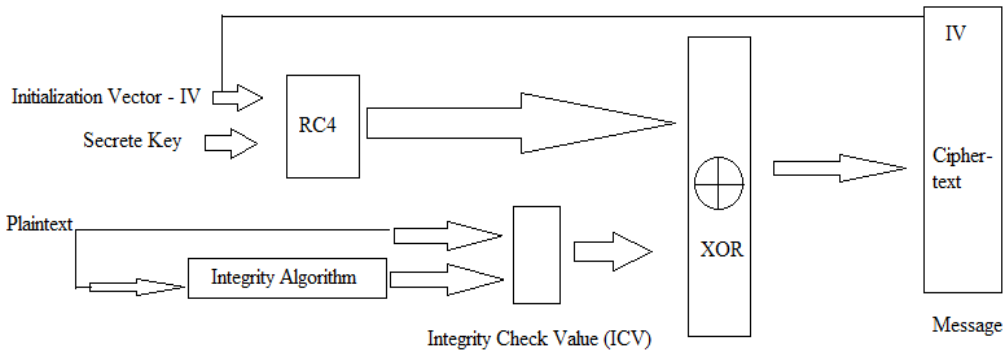
  Ο αλγόριθμος RC4 εκμεταλλεύεται την παραπάνω ιδιότητα ως εξής:
  - Κρυπτογράφηση**: plaintext(XOR)keystream = cipher text**
  - Αποκρυπτογράφηση: **cipher text(XOR)keystream = plaintext**

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

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

- **<u>Η κρυπτογράφηση:</u>** Πρώτα το μυστικό κλειδί συνδέεται με το διάνυσμα έναρξης(IV) και το αποτέλεσμα τους εισάγεται στον αλγόριθμο RC4. Ο αλγόριθμος RC4 παράγει μια ακολουθία κλειδιού keystream από "ψευδοτυχαία" bits ίσα με τον αριθμό bits δεδομένων που πρέπει να διαβιβαστούν συν 4.

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



Εικόνα 2.1

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

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

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

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

Ο αλγόριθμος RC4 είναι πολύ σημαντικός για την αποδοτικότητα του WEP, όσον αφορά την εμπιστευτικότητα των δεδομένων, αφού αυτός είναι στην ουσία η μηχανή κρυπτογράφησης. Θα πρέπει να τονίσουμε ότι το μυστικό κλειδί είναι

στατικό, οπότε το IV είναι αυτό που καθορίζει κάθε φορά την ψευδοτυχαία ακολουθία. Άρα ο αλγόριθμος RC4 εξαρτάται μόνο από το IV.

2.2.1 Προβλήματα του WEP

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

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

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

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

- Ο έλεγχος πρόσβασης συνίσταται στην απαγόρευση ή όχι της επικοινωνίας μια συσκευής με το δίκτυο. Η πρόσβαση συνήθως ελέγχεται διατηρώντας μια λίστα με επιτρεπόμενες συσκευές ή με κάποιο ηλεκτρονικό πιστοποιητικό. Στο IEEE 802.11 δεν έχουμε κάποιο συγκεκριμένο μηχανισμό υλοποίησης πρόσβασης. Οι συσκευές συνήθως αναγνωρίζονται

με τις διευθύνσεις MAC, όμως αυτή δεν είναι μια πολύ καλή προσέγγιση καθώς οι διευθύνσεις αυτές μπορούν εύκολα να αντιγραφούν. Έτσι το μόνο που μένει για το WEP είναι τα κλειδιά κρυπτογράφησης.

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

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

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

- Η τιμή του διανύσματος αρχικοποίησης δεν είναι μυστική, όπως ειπώθηκε παραπάνω, όμως κάτι τέτοιο δίνει την ευκαιρία σε ένα εισβολέα να επιτεθεί σε ένα σχετικά αδύναμο κλειδί. Τα πρώτα bytes ενός μη κρυπτογραφημένου μηνύματος είναι συνήθως γνωστά διότι αποτελούν μια επικεφαλίδα IEEE 802.11. Με παρακολούθηση της μετάδοσης αναζητείται ένα αδύναμο κλειδί. Ξέρουμε επίσης ότι υπάρχει σχέση ανάμεσα στο κρυπτογραφημένο, στο μη κρυπτογραφημένο και το μυστικό κλειδί. Έχοντας

καταγράψει έναν σημαντικό αριθμό από τέτοια μηνύματα, ο εισβολέας μπορεί να ανακαλύψει το πρώτο byte του κλειδιού. Η μέθοδος αυτή μπορεί να εφαρμοστεί για κάθε byte και τελικά να αποκαλυφθεί το μυστικό κλειδί. Τέλος, θα πρέπει να πούμε ότι η αύξηση του μήκους του κλειδιού δεν επιφέρει εκθετική αύξηση του χρόνου αναζήτησης αλλά απλά γραμμική.

2.3 Πέρα από το WEP

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

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

- **Η λύση του TKIP**

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

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

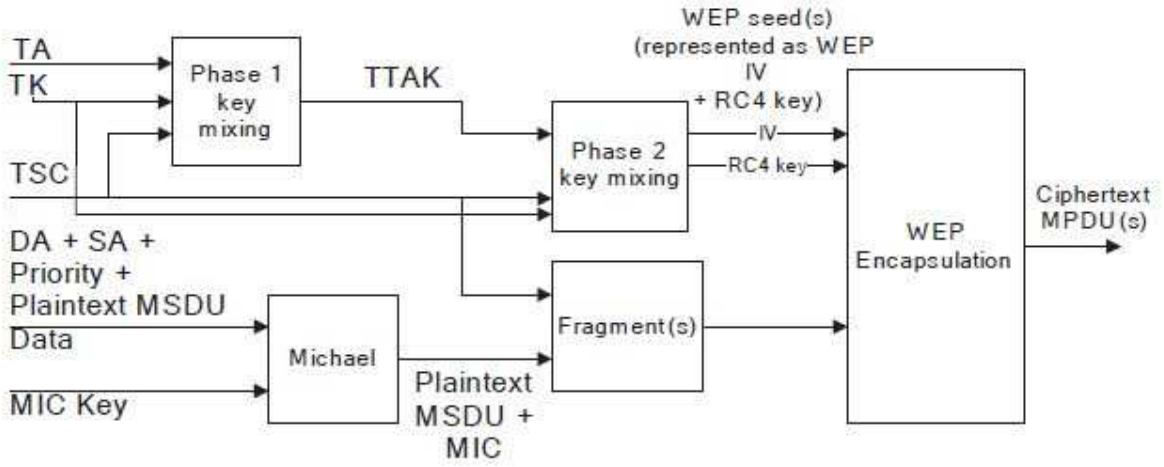
Αρχικά το TKIP χρησιμοποιήθηκε πάνω στο WEP για να ενισχύσει την ασφάλεια και να μειώσει τον αριθμό των επιθέσεων του WEP. Το πρώτο βήμα στην διαδικασία της κρυπτογράφησης TKIP είναι ο υπολογισμός του κώδικα ακεραιότητας δεδομένων MIC, που γίνεται με τον αλγόριθμο Micheal. Με τον αλγόριθμο αυτό προστατεύονται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

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

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

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

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



Εικόνα 2.2

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

Το πρότυπο 802.1x παρέχει πρόσφορο έδαφος σε πρωτόκολλα έλεγχου ταυτότητας και διαχείρισης κλειδιού. Ουσιαστικά με το 802.1x παρέχεται έλεγχος ταυτότητας μεταξύ του πελάτη και ενός διακομιστή RADIUS (Remote Authentication DIal-In User Service) που είναι συνδεδεμένος στο σημείο πρόσβασης. Επιπλέον η χρήση ενός πρωτοκόλλου έλεγχου ταυτότητας, γνωστό ως EAP (Extensible Authentication Protocol) ωφελεί το 802.1x.

Τα επόμενα χρόνια η Wi-Fi Alliance όρισε ένα υποσύνολο του νέου προτύπου, το οποίο αποτελεί μια βελτιωμένη έκδοση ασφάλειας που ενδυναμώνει το επίπεδο προστασίας δεδομένων και έλεγχου πρόσβασης σε ασύρματο δίκτυο. Το υποσύνολο αυτό ονομάζεται Wi-Fi Protected Access(WPA).

2.4 WPA (WI-FI PROTECTED ACCESS)

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

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

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

Ο κωδικός θα πρέπει να αποτελείται από 8-63 εκτυπώσιμους χαρακτήρες σε ASCII. Στην συνέχεια το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το 256bit κλειδί υπολογίζεται χρησιμοποιώντας την hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κώδικα ως κλειδί.

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

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

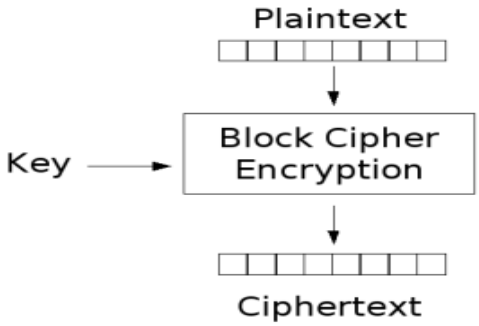
2.4.1 AES (ADVANCED ENCRYPTION STANDARD)

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

Ο AES αποτελεί την νεότερη μέθοδος κρυπτογράφησης μου έχει επιλεγεί από τις Η.Π.Α για να αντικαταστήσει τον αλγόριθμο DES το 2001. Ο AES χρησιμοποιεί ένα αλγόριθμο γνωστό ως Rijndael.

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

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



Εικόνα 2.3

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

2.4.2 CCMP (COUNTER MODE WITH CIPHER BLOCK CHAINING MESSAGE AUTHENTICATION CODE PROTOCOL)

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

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

Το CCMP χρησιμοποιεί μέγεθος κλειδιού 128bit και μέγεθος block 128bit. Μετά από το CCMP το μέγεθος του πακέτου έχει επεκταθεί κατά 16bytes, 8bytes για την επικεφαλίδα του CCMP και 8 bytes για την ψηφιακή υπογραφή MIC αντίστοιχα. Τα δεδομένα του πακέτου και το MIC μεταδίδονται κρυπτογραφημένα, αφού προστεθεί η αρχική επικεφαλίδα του πακέτου και η επικεφαλίδα του CCMP.

2.5 WPA2 (WI-FI PROTECTED ACCESS VERSION 2)

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

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

Όταν ένας σταθμός θέλει να συνδεθεί σε ένα γειτονικό σημείο πρόσβασης, η επικυρώσεις 802.1x μπορεί να παραληφθεί αφού έχει ήδη ολοκληρωθεί εκ των προτέρων. Επιπλέον το προσωρινό κλειδί έχει ήδη εγκαθιδρυθεί ανάμεσα στο σταθμό και στο σημείο πρόσβασης. Αποκτώντας πρόσβαση στο RADIUS εξυπηρετεί για να ολοκληρώσει την 802.1x επικύρωση. Καταλαμβάνει πολύ χρόνο και επιπλέον τα δίκτυα που περιλαμβάνουν γρήγορη περιαγωγή έχει παρατηρηθεί ότι έχουν ομαλότερη λειτουργία και συνεχή συνδεσιμότητα του πελάτη καθώς αυτός μετακινείται στις κυψέλες του WLAN.

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

2.6 ROBUST SECURE NETWORK (RSN)

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

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

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

Τα δίκτυα TSN υποστηρίζουν δίκτυα όπως το RSN, αλλά και κρυπτογράφηση όπως το WEP. Οι χρήστες που εισέρχονται σε ένα δίκτυο TSN, μπορούν να λειτουργήσουν παράλληλα για όλα τα προηγούμενα συστήματα ασφάλειας.

2.7 Διαφορές ανάμεσα στο RSN και το WPA

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

Οι παραπάνω μέθοδοι χρησιμοποιούν παρόμοια αρχιτεκτονική με πρωτόκολλα ασφάλειας που βασίζονται στους αλγόριθμους AES και RC4 αντίστοιχα. Μέσω αυτών των μεθόδων καλύπτονται θέματα όπως:

- Επικύρωση σε υψηλό επίπεδο

- Διανομή του κλειδιού κρυπτογράφησης
- Ανανέωση του κλειδιού

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

2.8 Τύποι επιθέσεων σε ασύρματα δίκτυα

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

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

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

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

2.8.1 Παθητικές: Λήψη πληροφοριών (Snooping/Footprinting)

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

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

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

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

Ένα πολύ χρήσιμο εργαλείο που χρησιμοποιείται για την ανίχνευση, ανάλυση και παρακολούθηση προβλημάτων στα δίκτυα είναι το Wireshark.

2.8.2 Ενεργητικές: Ανάκτηση Κωδικού WEP (WEP Cracking-Caffe Latte Attack)

Η μέθοδος του WEP έχει χάσει την παλιά αίγλη της, εφόσον μέσα σε λίγα λεπτά μπορεί να ανακτηθεί ο μυστικός κωδικός που χρειάζεται για την παραβίαση ενός ασύρματου δικτύου. Οι μέθοδοι που χρησιμοποιούνται σήμερα για το WEP Cracking επικεντρώνονται στην συλλογή και αναμετάδοση πακέτων ARP (Address Resolution Protocol) στο σημείο πρόσβασης.

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

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

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

2.8.3 Ενεργητικές: Τροποποίηση Δεδομένων

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

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

Ένα παράδειγμα μεθόδου τροποποίησης δεδομένων που είναι πιο κοντά στην πραγματικότητα είναι η αλλαγή της διεύθυνσης προορισμού (διεύθυνσης IP) ενός μηνύματος το οποίο διαβιβάζεται σε μια ασύρματη μετάδοση, το οποίο αντί να διαβιβαστεί στον προοριζόμενο παραλήπτη, μεταφέρεται στον επιτιθέμενο ή σε κάποιον άλλο επιθυμητό προορισμό. Αυτή η μέθοδος χρησιμοποιείται διότι το μήνυμα στην ασύρματη σύνδεση κρυπτογραφείται και δεν μπορεί να διαβαστεί το περιεχόμενο, αλλά εάν μπορεί ο επιτιθέμενος να το πάρει διαβιβασμένο από το διαδίκτυο, θα λάβει την αποκρυπτογραφημένη έκδοση. Η επιγραφή IP είναι ευκολότερο να δεχτεί επίθεση διότι είναι μια γνωστή έκδοση. Μια επίθεση τροποποίησης είναι η **Man in the Middle** επίθεση.

- **Man in the Middle Attack:** Σε αυτό το είδος της επίθεσης, ο επιτιθέμενος βρίσκεται στη μέση της συνομιλίας δυο συμμετεχόντων στο δίκτυο (για παράδειγμα user1 και user2). Σε μια πραγματική επικοινωνία ο user1 θα λάμβανε μηνύματα από τον user2 και αντίστροφα. Ο εισβολέας όμως μπορεί να μιμηθεί καθέναν από τους δυο και να στέλνει μηνύματα τα οποία φαίνεται ότι προήλθαν από την πραγματική τους επικοινωνία, Συχνά τέτοιου είδους επιθέσεις χρησιμοποιούνται για την τροποποίηση μηνυμάτων κατά την μεταφορά χωρίς να υπάρχει περίπτωση να ανιχνευθούν.

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

2.8.4 Ενεργητικές: Μεταμφίεση (Spoofing)

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

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

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

2.8.5 Ενεργητικές: Άρνηση υπηρεσιών (Denial of Service)

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

Οι πέντε πιο σημαντικοί τύποι επιθέσεων DDOS περιγράφονται παρακάτω:

- **<u>Επίθεση πλημμύρας (Flood Attack):</u>** Αυτές είναι οι πιο γνωστές DoS επιθέσεις. Ο μηχανισμός αυτής της επίθεσης είναι απλός. Ο επιτιθέμενος δημιουργεί στον server περισσότερη κίνηση από αυτή που μπορεί να διαχειριστεί. Εάν όμως ο υπολογιστής-θύμα διαθέτει ένα πολύ καλό bandwidth τότε έχει πολύ καλές πιθανότητες να μην επηρεαστεί.

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

- **Επίθεση Ping to Death:** Αυτή η επίθεση είναι μια άλλη παλαιότερη μορφή επίθεσης DoS. Η βασική αρχή της δεν είναι τόσο έξυπνη όμως καταφέρνει να εκμεταλλευτεί την αδυναμία του TCP/IP πρωτοκόλλου. Η μέθοδος αυτή απλά στέλνει ένα διάγραμμα δεδομένων, του οποίου το μέγεθος ξεπερνά κατά πολύ τα συνηθισμένα. Όταν ένα τέτοιο διάγραμμα φτάσει στον προορισμό του, το σύστημα που το παραλαμβάνει καταρρέει.

  Ευτυχώς, τέτοιου είδους επιθέσεων τώρα πια δεν υπάρχουν λόγω ότι όλοι οι σύγχρονοι εξοπλισμοί διαθέτουν μηχανισμούς άμυνας ενάντια σε τέτοιες επιθέσεις.

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

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

- **Επίθεση Teardrop:** Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει παθαίνει κατάρρευση (crash), "πάγωμα"(hang/freeze) ή/και επανεκκίνηση (reboot). Αλλά όπως και η Ping to Death δεν υπάρχει πια.

- **Επίθεση Smurf:** Κατά την έναρξη μιας επίθεσης Smurf, ο επιτιθέμενος στέλνει μια πληθώρα πακέτων ping ICMP Echo Request σε διευθύνσεις IP broadcast διαφόρων δικτύων. Τα πακέτα αυτά έχουν τροποποιηθεί κατάλληλα ούτως ώστε στο πεδίο source της κεφαλίδας IP να αναγράφεται η διεύθυνση IP του θύματος και όχι του επιτιθέμενου. Επίσης, δεδομένου ότι στάλθηκαν στην διεύθυνση IP broadcast των διαφόρων δικτύων, τα λαμβάνουν όλοι οι υπολογιστές που ανήκουν σε αυτά. Αυτό έχει ως αποτέλεσμα όλοι οι υπολογιστές να απαντούν στο ping με πακέτα ICMP Echo Reply, τα οποία έχουν ως διεύθυνση προορισμού την διεύθυνση IP του θύματος. Άρα λοιπόν το θύμα πλημμυρίζει με πακέτα ping και οδηγείται σε κατάρρευση.
  Οι επιθέσεις αυτές είναι πιο δύσκολα ανιχνεύσιμες, όμως εάν ένα δίκτυο είναι πολύ καλά οργανωμένο και συντηρείται σωστά, η επίθεση αυτή δεν θα είναι καταστροφική. Πριν από καιρό τα περισσότερα δίκτυα υπολογιστών ήταν ευπαθή σε τέτοιου είδους επιθέσεις, αλλά σήμερα έχουν αναπτυχθεί κατάλληλες τεχνολογίες έτσι ώστε οι επιθέσεις Smurf να μην αποδίδουν.

3 Σπάζοντας την ασύρματη ασφάλεια

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να αναλύσουμε τις μεθόδους που χρησιμοποιούνται για το "σπάσιμο" της ασύρματης ασφάλειας ενός οικιακού δικτύου χρησιμοποιώντας ένα παράδειγμα από την ιστοσελίδα wikiHow.

Για αυτού του είδους επιθέσεις απαραίτητα εργαλεία αποτελούν:

- Το Backtrack σε live μορφή
- Ένα κοντινό ασύρματο δίκτυο που θα χρησιμοποιεί WEP κρυπτογράφηση

Backtack: Το Backtrack αποτελεί μια ελεύθερη διανομή Linux, η οποία διανέμεται σε live CD και USB. Στο Backtrack περιέχει μια ποικιλία εργαλείων τα οποία βοηθούν άτομα τα οποία θέλουν να δοκιμάσουν την ασφάλεια ενός συστήματος αλλά και για εκπαιδευτικούς σκοπούς. Οι διανομές σε live CD και USB κάνουν ακόμα πιο απλή την χρήση του. αφού μπορούν να χρησιμοποιηθούν χωρίς να γίνει εγκατάσταση.

Τα εργαλεία του Backtrack κατατάσσονται σε κατηγορίες, αυτές είναι:

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Web Application Analysis
- Radio Network Analysis
- Penetration
- Voice Over IP
- Privilege Escalation
- Maintaining Access
- Digital Forensics
- Reverse Engineering

Μερικά από τα κύρια εργαλεία του Backtack είναι:

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

Κατά την προσπάθεια επαναφοράς του κλειδιού που χρησιμοποιείται από το Wireless Access Point για να κρυπτογραφήσει τα δεδομένα που διακινούνται στο δίκτυο, χρησιμοποιήθηκε η ποικιλία aircrack-ng.

Αυτή η ποικιλία βοηθάει στον έλεγχο της ασφάλειας του δικτύου μας καθώς μπορούμε να ελέγξουμε κατά πόσο το κλειδί που έχουμε χρησιμοποιήσει στο AP μας μπορεί να σπάσει. Τα βασικά εργαλεία που περιλαμβάνει η ποικιλία aircrack-ng είναι:

- aircrack-ng
- airodump-ng
- aireplay-ng
- airmon-ng
- packetforge-ng

Αλλά πριν προχωρήσουμε στο σημείο της Backtack θα ήταν καλό να γίνει μια αναφορά για τον πρόγραμμα Wireshark, το οποίο αν και ξεχωριστό πρόγραμμα το Backtrack το περιλαμβάνει σαν addon στο λειτουργικό του, όπου μας δίνει την δυνατότητα του Snooping/Footprinting.

3.1 Snooping/Footprinting

Το Wireshark είναι ένα από τα πιο διάσημα εργαλεία αναζήτησης κυκλοφορίας σε παγκόσμια κλίμακα. Το πρόγραμμα αυτό χρησιμοποιείται για την ανάκτηση πληροφοριών για το δίκτυο αλλά και των πρωτοκόλλων ανωτέρου επιπέδου σχετικά πάντα με τα δεδομένα που διακινούνται μέσο στο δίκτυο. Το Wireshark διαθέτει δικτυακή βιβλιοθήκη για την σύλληψη και ανάλυση των πακέτων πληροφορίας.

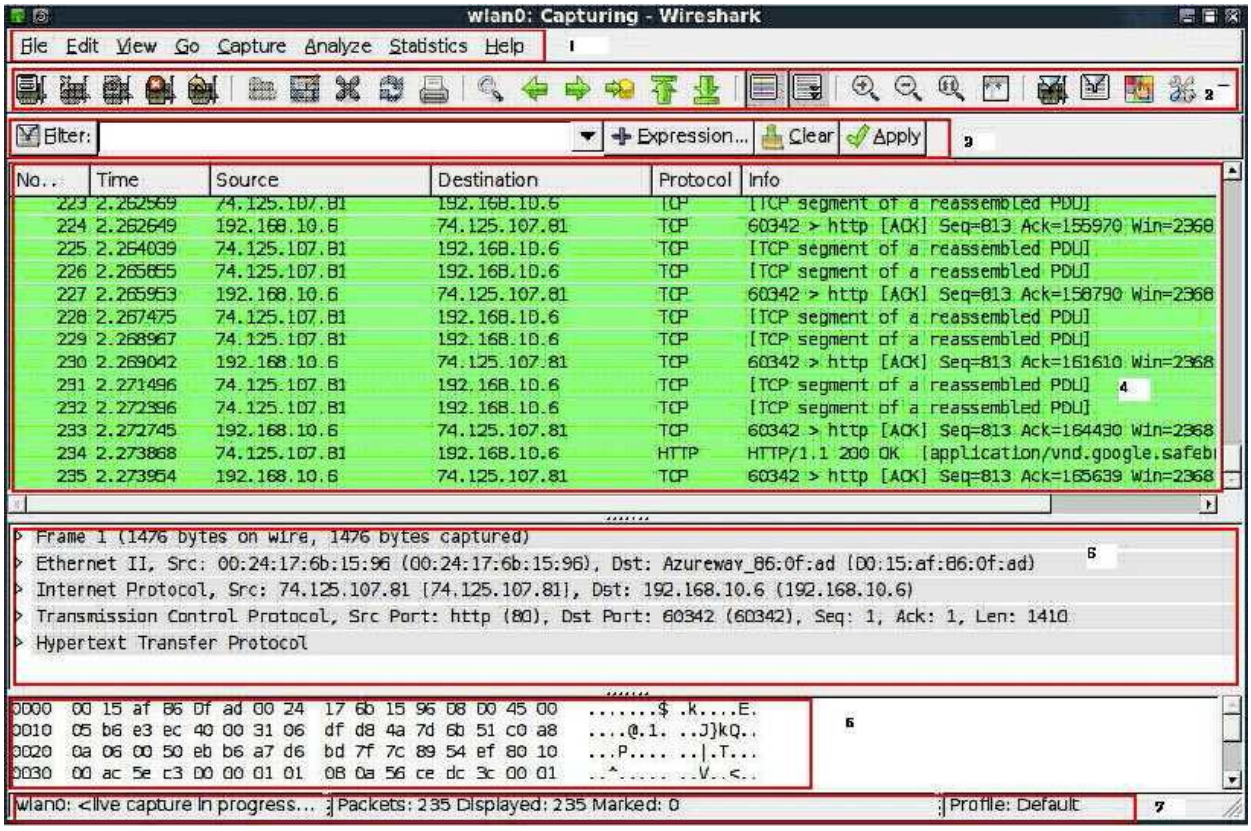
Επίσης το Wireshark είναι ελεύθερο και ανοιχτού κώδικα λογισμικού ανάλυσης πρωτοκόλλων δικτύου υπολογιστών. Το αρχικό όνομα του προγράμματος ήταν Ethereal, αλλά τον Μάιο του 2006 άλλαξε σε Wireshark για λόγους εμπορικών σημάτων.

Το Wireshark είναι παρόμοιο με το πρόγραμμα tcpdump, όμως έχει γραφικό front_end και περισσότερες επιλογές ταξινόμησης και φιλτραρίσματος. Επιτρέπει στο χρήστη να παρακολουθεί όλη την κίνηση που γίνεται στο δίκτυο θέτοντας την κάρτα δικτύου σε λειτουργία promiscuous mode.

Το Interface του Wireshark χωρίζεται σε επτά διαφορετικά τμήματα:

- Μενού

- Συντομεύσεις
- Φίλτρο
- Πίνακας λίστας πακέτων
- Πίνακας λεπτομερειών πακέτων
- Πίνακας ανατομίας
- Διάφορα



Εικόνα 3.1

Φίλτρο: Η γραμμή του φίλτρου χρησιμοποιείται για την αναζήτηση μέσα σε ήδη καταγεγραμμένα αρχεία συλλήψεων. Με την βοήθεια των φίλτρων, τα οποία μπορούν να εφαρμοστούν μετά αλλά και πριν την σύλληψη των πακέτων, περιορίζεται ο αριθμός των ορατών πακέτων, κάτι το οποίο διευκολύνει την μελέτη των πακέτων για τα οποία ενδιαφερόμαστε.

Πίνακας λίστας πακέτων: Ο πίνακας λίστας πακέτων απεικονίζει όλα τα πακέτα που έχουν συλληφθεί. Από τα πακέτα αυτά μπορεί να εξαχθεί χρήσιμη πληροφορία όπως οι διευθύνσεις (MAC/IP) παραλήπτη και αποστολέα, τους αριθμούς θυρών TCP/UDP, το πρωτόκολλο ή ακόμα και τα περιεχόμενα του πακέτου.

Πίνακας λεπτομερειών πακέτων: Ο πίνακας λεπτομερειών πακέτων δίνει αναλυτικές πληροφορίες σχετικά με το επιλεγμένο πακέτο. Οι πληροφορίες αυτές φαίνονται ανά επίπεδο OSL.

Πίνακας ανατομίας: Ο πίνακας ανατομίας ή πίνακας των bytes πακέτων, εμφανίζει τις ίδιες πληροφορίες για τα πακέτα με αυτές του πίνακα λεπτομερειών πακέτων, όμως σε αυτή την περίπτωση έχουμε την δεκαεξαδική μορφή τους.

Λειτουργία: Για να δοκιμάσουμε την λειτουργία του Wireshark πρέπει να ανοίξουμε ένα web browser και να αρχίσουμε να περιηγούμαστε στο διαδίκτυο.

Για να γίνει σύλληψη πακέτων από το Wireshark πρέπει να ανοίξουμε το πρόγραμμα και να επιλέξουμε από το μενού: **Capture→Interfaces** την κάρτα δικτύου που χρησιμοποιούμε και στην συνέχεια την επιλογή **Options** που βρίσκεται στα δεξιά της. Στο παράθυρο που εμφανίζεται μπορούμε να επιλέξουμε κάποιο φίλτρο, το ελάχιστο όριο που θα έχει το πακέτο, αν θα εμφανίζεται παράθυρο με πληροφορίες κατά την σύλληψη και άλλα πολλά. Πατώντας **Start**, ξεκινάει η διαδικασία σύλληψης των πακέτων από το Wireshark.

Όταν αρχίζουμε να συλλαμβάνουμε πακέτα, αυτά είναι τόσα πολλά που η χρήση φίλτρων για την εξέταση τους κρίνεται αναγκαστική. Στο κάτω παράθυρο φαίνονται τα περιεχόμενα των πακέτων, όμως συνήθως είναι κρυπτογραφημένα. Αν σε κάποια περίπτωση δεν υπάρχει κάποιου είδους κρυπτογράφηση τότε ο χρήστης μπορεί να δει και το περιεχόμενο τους.

Τέλος η αναζήτηση κωδικών στο Wireshark γίνεται με την χρήση φίλτρων, είτε εισάγοντας την λέξη password, είτε αναζητώντας το μέσα σε http πακέτα. Αυτή η διαδικασία μπορεί να επαναληφθεί και σε πολλές άλλες περιπτώσεις.

3.2 WEP Cracking

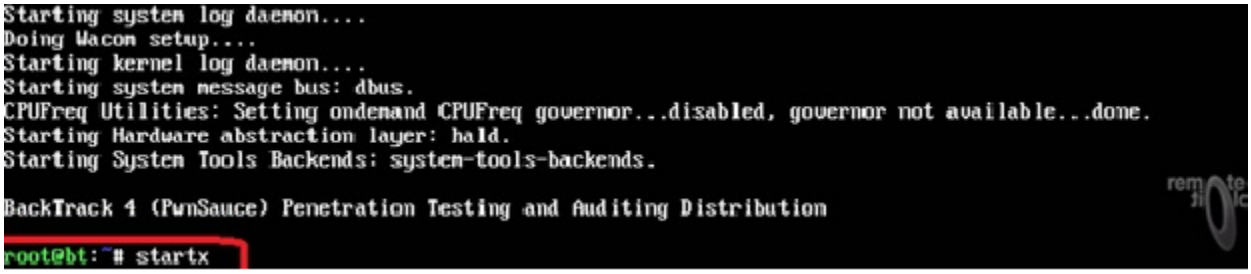
Σε αυτή την παράγραφο θα παρουσιαστεί μια απλή περίπτωση Wep cracking. Αυτό το είδος επίθεσης βασίζεται κυρίως στη δημιουργία μιας απόκρισης σε ένα πακέτο ARP μέσω του aireplay-ng. Στην συνέχεια η αποκρυπτογράφηση ολοκληρώνεται μέσω του aircrack-ng και των μοναδικών πακέτων IV's.

Για την ανάκτηση του WEP κλειδιού είναι απαραίτητη η συλλογή αρκετών IV's πακέτων. Κατά την διάρκεια της φυσιολογικής κίνησης του δικτύου δεν παράγονται τόσα πολλά πακέτα σε σύντομο χρονικό διάστημα. Θεωρητικά εάν κάποιος είναι πολύ υπομονετικός μπορεί να συλλέξει τα πακέτα που χρειάζεται, όμως υπάρχει μέθοδος για την επιτάχυνση αυτής της διαδικασίας. Μέσω της μεθόδου που αποκαλείται "Injection", το ασύρματο σημείο πρόσβασης στέλνει ξανά και ξανά επιλεγμένα πακέτα όλο και με πιο μεγάλο ρυθμό. Αυτή η διαδικασία

επιτρέπει στον επιτιθέμενο να αποκτήσει τα πακέτα που χρειάζεται σε σύντομο χρονικό διάστημα.

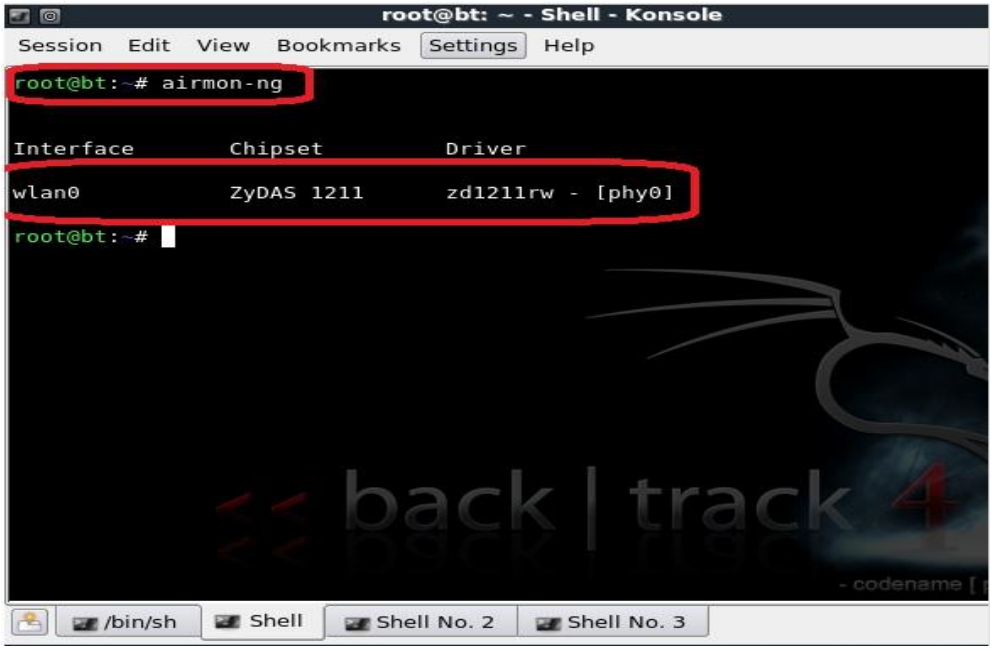
Tutorial για το Backtack: Για να ξεκινήσουμε το "σπάσιμο" σε ένα ασύρματο δίκτυο πρέπει πρώτα να κάνουμε boot την Backtrack από την live συσκευή που την έχουμε (CD/DVD ή USB).

Όταν λοιπόν τρέξει θα μας εμφανίσει μια οθόνη εντολών. Για να μπούμε σε εικονικό περιβάλλον πρέπει να πληκτρολογήσουμε την εντολή **startx**. Και αυτό με την σειρά του θα μας οδηγήσει στο desktop της Backtrack.



Εικόνα 3.2

Χρήση airomon-ng: Ανοίγουμε στην συνέχεια την κονσόλα και πληκτρολογούμε airmon-ng χωρίς κενά. Αυτή η κίνηση γίνεται για να τεθεί η κάρτα δικτύου σε monitor mode και να αλλαχθεί η Mac Adress της αν χρειαστεί.

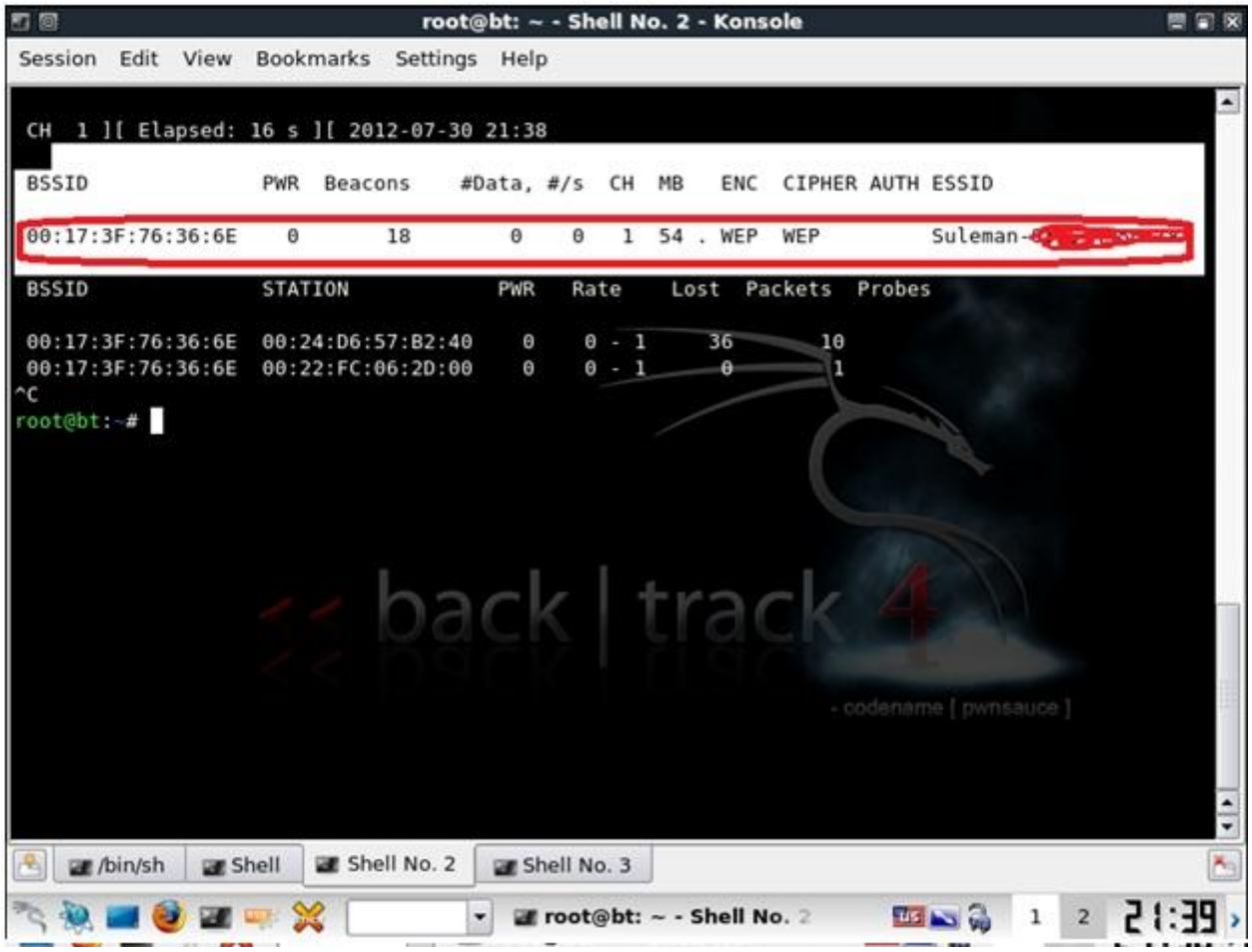


Εικόνα 3.3

Χρήση airodump: Για την καταγραφή πακέτων από 802.11 και την συλλογή των WEP IV's (Initialization vectors) χρησιμοποιούμε την εντολή airodump-ng. Επίσης μπορεί να χρησιμοποιηθεί για τον εντοπισμό των δικτύων 802.11 που βρίσκονται στην εμβέλεια της κάρτα μας.

Αυτή η εντολή μας παρουσιάζει τα εξής:

- BSSID: εμφανίζεται η MAC adress των APs που βρίσκονται κοντά στην κάρτα μας.
- Channel:βλέπουμε την ισχύ, beacon frames, τα πακέτα και άλλα.
- ESSID: βλέπουμε το όνομα του δικτύου (για το παράδειγμα είναι Suleman).

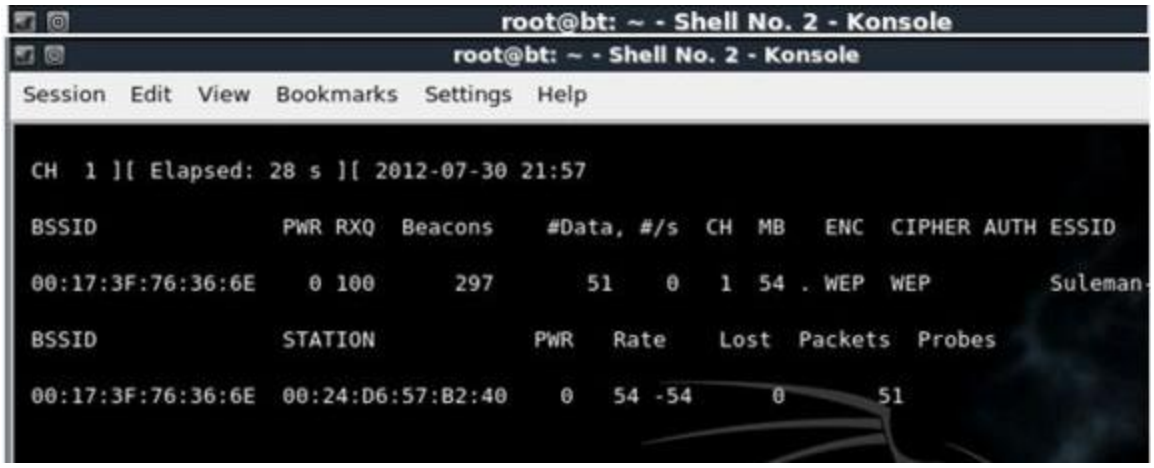


Εικόνα 3.4

Συλλογή IV's: Σε αυτό το βήμα θα πρέπει να συλλεχθούν όσα περισσότερα διανύσματα έναρξης είναι δυνατόν. Σε ένα καινούργιο παράθυρο της κονσόλας πληκτρολογούμε:

airodump-ng -w wep -c 1 -- bssid 00:17:3F:76:36:6E wlan0

Το αφήνουμε να τρέξει και μετά από λίγη ώρα θα πρέπει να έχει ανταποκριθεί.



Εικόνα 3.5

<u>Ψεύτικη ταυτοποίηση:</u> Συνήθως κατά την σύνδεση με ασύρματο δίκτυο λαμβάνει χώρα μια συγκεκριμένη διαδικασία ταυτοποίησης του χρήστη:

- Ζητείται από το AP ταυτοποίηση.
- Το AP αποκρίνεται. Η ταυτοποίηση πραγματοποιήθηκε
- Ζητείται από το AP συσχετισμός.
- Απόκριση του AP. Η σύνδεση πραγματοποιήθηκε.

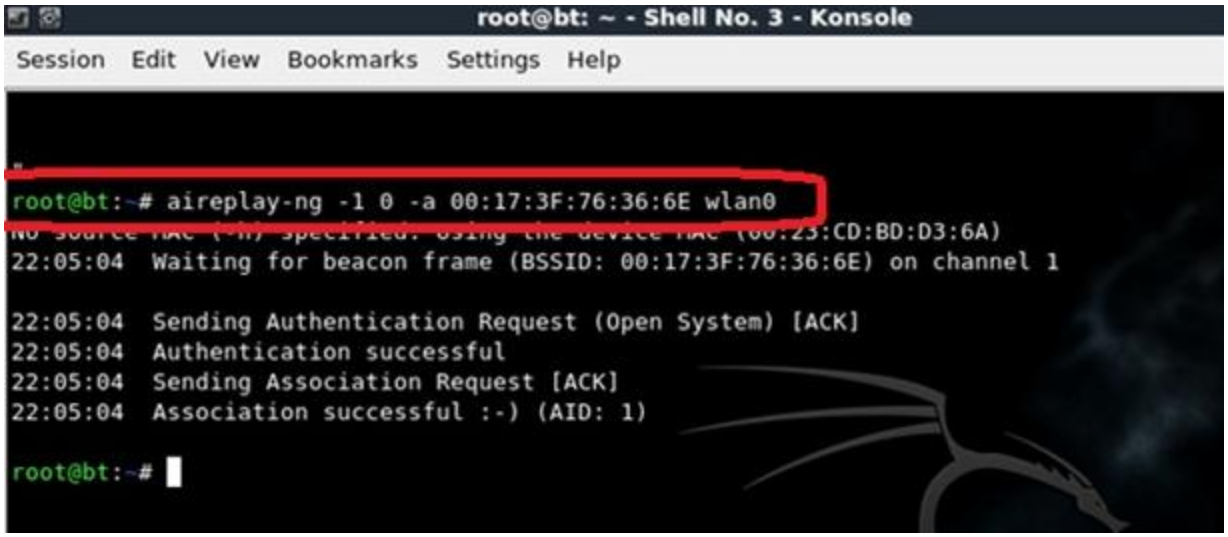
Σε περίπτωση που δεν υπάρχει εξουσιοδότηση υπάρχουν οι εξής περιπτώσεις:

- Αν υφίσταται προστασία δικτύου WPA/WPA2 τότε απαιτείται πιστοποίηση EAPOL.
- Το AP έχει λίστα επιτρεπόμενων clients. Έτσι μόνο οι συσκευές της λίστας μπορούν να συνδεθούν. Αυτό ονομάζεται MAC filtering.
- Το AP χρησιμοποιεί Shared Key Authentication, όπου πρέπει να εισαχθεί το κατάλληλο αναγνωριστικό WEP για να επιτευχθεί η σύνδεση.

Στο παράδειγμα επιχειρείται μια ψεύτικη ταυτοποίηση δίνοντας την εντολή:

aireplay-ng -1 0 –a 00:17:3f:76:36:6E wlan0

Και μετά από λίγη ώρα το σύστημα ανταποκρίνεται:



Εικόνα 3.6

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

Κάποιες επιθέσεις είναι οι εξής:

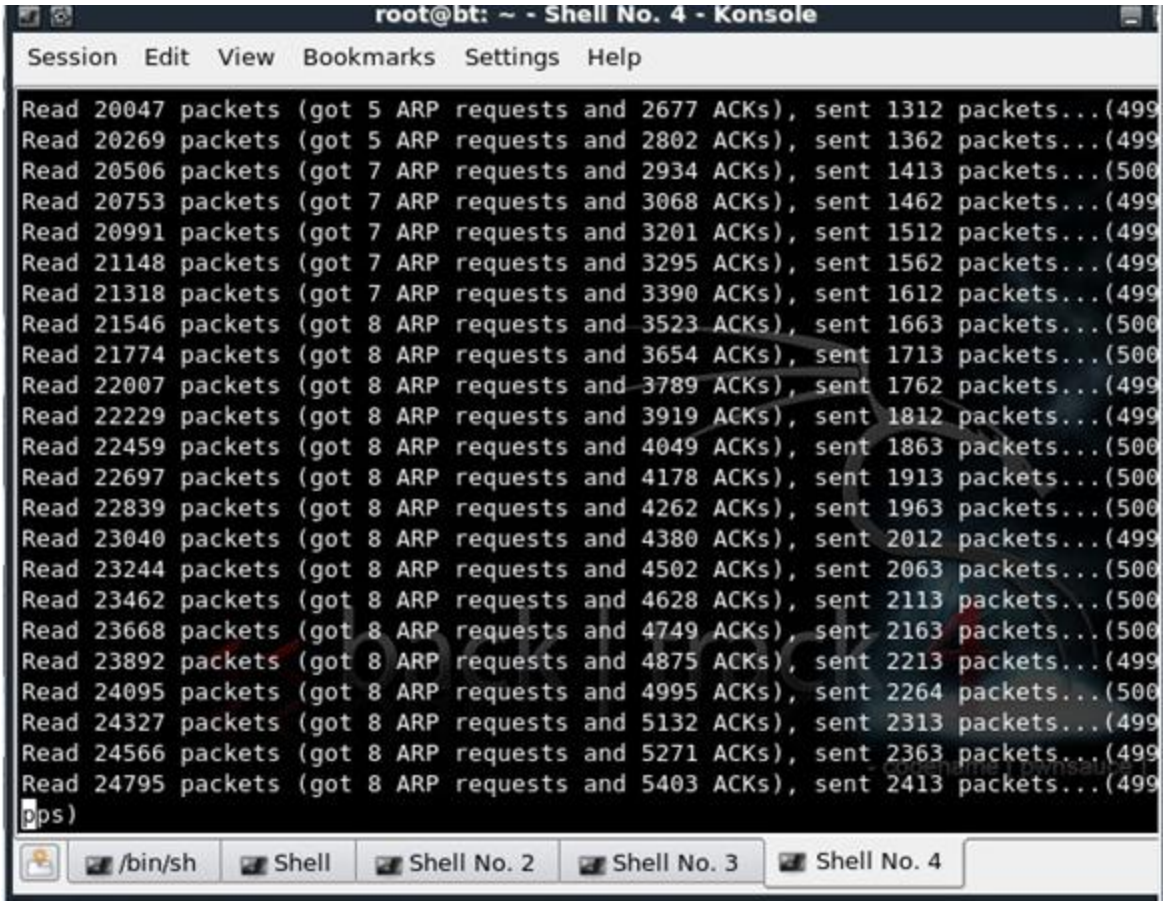
- Attack 0: Deauthentication (-0)
- Attack 1: Fake authentication (-1)
- Attack 2: Interactive packet replay (-2)
- Attack 3: ARP request replay attack (-3)
- Attack 4: KoreK chopchop attack (-4)
- Attack 5: Fragmentation attack (-5)
- Attack 9: Injection test (-9)

Με την βοήθεια του aireplay-ng μπορούν να σταλούν σήματα στο AP ώστε να τον κάνουμε να στέλνει περισσότερα πακέτα δεδομένων στον client. Επίσης είναι δυνατή η δημιουργία ενός εικονικού client, ο οποίος θα αυξήσει σημαντικά την κίνηση των πακέτων δεδομένων στο δίκτυο για την συλλογή περισσοτέρων IV's.

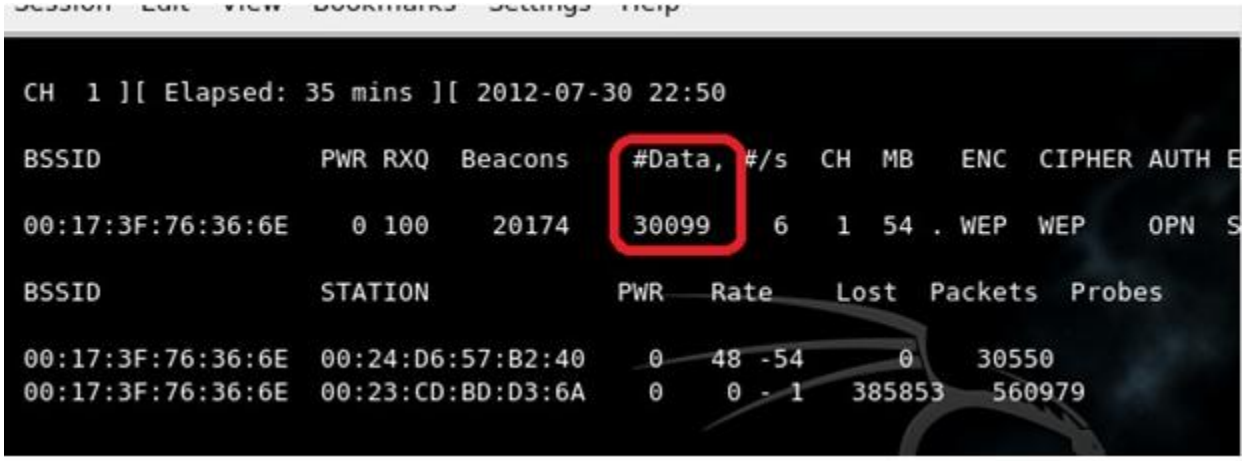
Πληκτρολογώντας:

aireplay-ng -3 –b 00:17:3f:76:36:6e wlan0

ξεκινάει η διαδικασία της ακρόασης των ARP αιτήσεων και της "ένεσης" πακέτων.



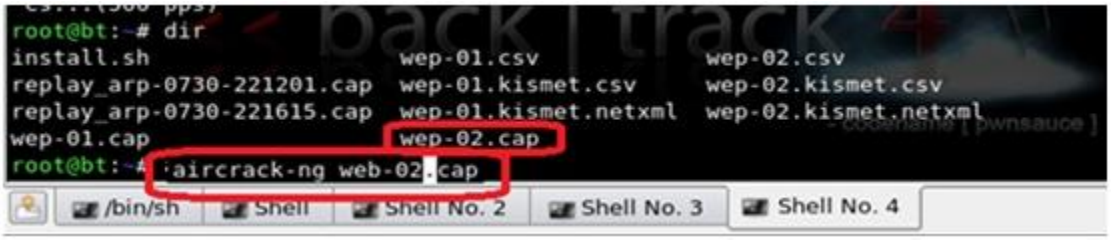
Εικόνα 3.7



Εικόνα 3.8

Περιμένουμε τα δεδομένα να φτάσουν στα 30.000 και άνω. Αυτή η διαδικασία μπορεί να πάρει από 15 έως 60 λεπτά (ή και παραπάνω) αναλόγως το ασύρματο σήμα, το πόσο καλός είναι ο υπολογιστής που χρησιμοποιούμε (hardware) και το φορτίο στο AP.

Απόκτηση του "κλειδιού": Για το τελευταίο βήμα πληκτρολογούμε την εντολή "dir" (χωρίς τα εισαγωγικά). Αυτό θα εμφανίσει τους καταλόγους που είναι αποθηκευμένα κατά την διάρκεια της αποκρυπτογράφησης.

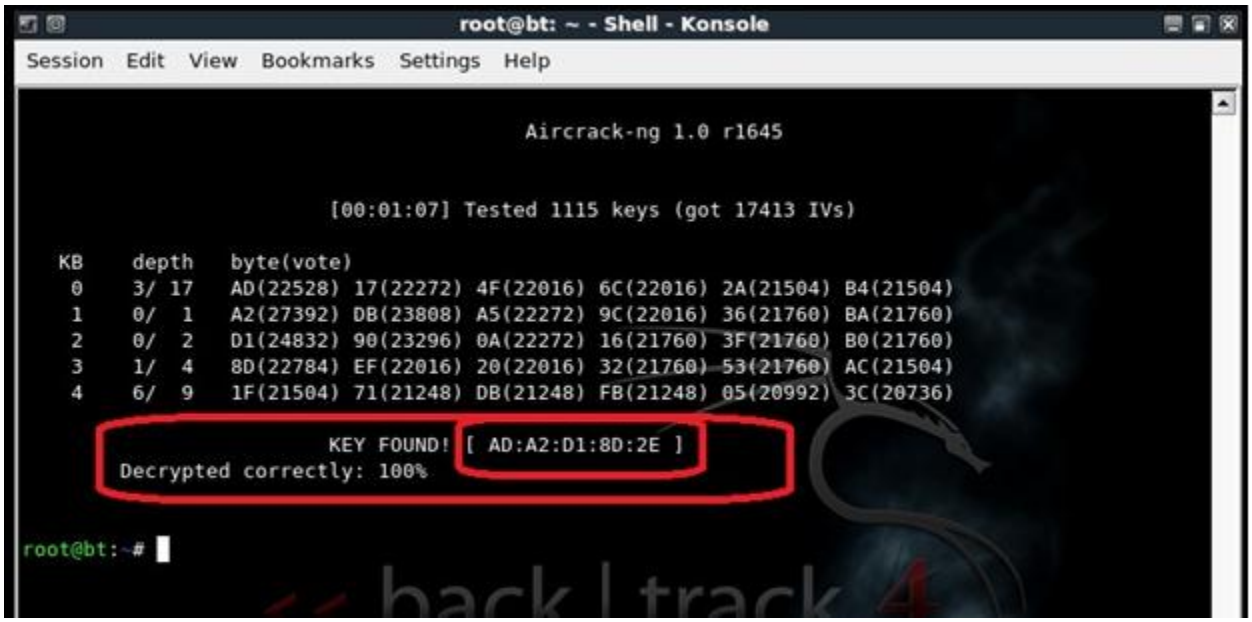


Εικόνα 3.9

Για το παράδειγμα χρησιμοποιούμε το αρχείο wep-02.cap και δίνουμε την εντολή:

aircrack-ng web-02.cap

Η ρύθμιση θα ξεκινήσει και θα μας παράγει το WEP κλειδί που στην συγκεκριμένη περίπτωση είναι το {ADA2D18D2E}.



Εικόνα 3.10

3.3 Θωρακίζοντας το ασύρματο δίκτυο

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

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

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

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

Ένας εισβολέας ο οποίος έχει βάλει σκοπό να επιτεθεί στο σύστημα μας, οπωσδήποτε θα έχει κάποια επιτυχημένη προσπάθεια. Για αυτό τον λόγο υπάρχουν κάποια ορισμένα βασικά βήματα που μπορούν να βοηθήσουν να γίνει ένα οικιακό δίκτυο ασφαλέστερο. Όμως αυτές οι ρυθμίσεις μπορούν απλά να καθυστερήσουν και όχι να σταματήσουν έναν έμπειρο επιτιθέμενο.

3.3.1 Τεχνικές προστασίας

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

- **Αλλαγή της προεπιλεγμένης πύλης του εξοπλισμού:** Σίγουρα θα ήταν καλό να αλλάξουμε και την εσωτερική διεύθυνση IP του υποδικτύου μας αν αυτό μας επιτρέπεται. Το 192.168.x.x εύρος διεύθυνσης προορίζεται μόνο για εσωτερική χρήση. Οι περισσότεροι οι ποίοι χρησιμοποιούν αυτό το εύρος διεύθυνσης, δουλεύουν στο

192.168.0.x για το υποδίκτυο τους, το οποίο είναι πολύ εύκολο να μαντέψει κάποιος. Μπορούμε να χρησιμοποιήσουμε οποιοδήποτε αριθμό από το 0 έως το 254 για την τρίτη οχτάδα, έτσι μπορούμε να χρησιμοποιήσουμε κάτι όπως 192.168.43.x, έτσι ώστε οι τυχών επιτιθέμενοι να χρειαστεί να δουλέψουν περισσότερο. Αυτό μπορεί να γίνει απενεργοποιώντας τον DHCP server του router και ρυθμίζοντας μόνοι μας τις IP διευθύνσεις του τοπικού δικτύου.

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

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

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

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

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

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

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

  Σε συσκευές με WPA2 πιστοποίηση, θα πρέπει να γίνεται χρήση του αλγόριθμου κρυπτογράφησης CCMP και όχι του συνδυασμού CCMP/TKIP ή AES/TKIP. Σε συσκευές με πιστοποίηση WPA, η χρήση του TKIP είναι προτιμότερη, παρόλα αυτά δεν θεωρείται αρκετά ασφαλές αφού ήδη έχουν βρεθεί σοβαρές αδυναμίες του.

- **WEP:** Εάν η συσκευή που χρησιμοποιείτε δεν υποστηρίζει άλλη μέθοδο κρυπτογράφησης παρά την WEP, αποφύγετε τον πειρασμό να προσπεράσετε την χρήση της κρυπτογράφησης. η χρήση της WEP είναι καλύτερη λύση από την απουσία οποιουδήποτε είδους κρυπτογράφησης. Εάν χρησιμοποιήσετε λοιπόν αυτό το είδος κρυπτογράφησης φροντίστε ώστε το μυστικό κλειδί να είναι μεγάλο και δύσκολο για να μαντέψει κανείς. Επίσης συνιστάται η τακτική αλλαγή του.

- **MAC filtering:** Η διεύθυνση MAC (Media Access Control) είναι η φυσική-μοναδική διεύθυνση για κάθε κάρτα δικτύου. Πρόκειται για ένα 48bit αριθμό καθορισμένο από τον κατασκευαστή. Τα 48bit του χωρίζονται σε 24bit και αποτελούν το μοναδικό αναγνωριστικό του κατασκευαστή, εκχωρημένα από την IEEE ενώ τα υπόλοιπα 24bit αποτελούν μια μοναδική κάρτα αναγνώρισης. Σε αντίθεση λοιπόν με την IP διεύθυνση, η MAC διεύθυνση είναι μοναδική σε κάθε κάρτα δικτύου, έτσι ενεργοποιώντας το φιλτράρισμα των MAC διευθύνσεων μπορούμε να περιορίσουμε τις συσκευές που θα αποκτήσουν πρόσβαση στο σύστημα μας. Η δυνατότητα αυτή δίνεται μέσα από το διαχειριστικό τμήμα του ασύρματου εξοπλισμού όπου μπορούν να δηλωθούν οι MAC διευθύνσεις των υπολογιστών που μας ενδιαφέρει να έχουν πρόσβαση. Βέβαια αυτή η

μέθοδος δεν παρέχει κάποια ουσιαστική ασφάλεια, αφού μια διεύθυνση MAC μπορεί να παραποιηθεί πάρα πολύ εύκολα. Παρ' όλα αυτά, απαγορεύει την σύνδεση στους απλούς χρήστες και καθυστερεί για λίγο μια επίθεση στο ασύρματο σημείο πρόσβασης.

- **Απενεργοποίηση της ασύρματης διαχείρισης του εξοπλισμού:** Το ασύρματο μέσο πρόσβασης θα πρέπει να ρυθμιστεί έτσι ώστε να μην μπορεί κάποιος να έχει πρόσβαση στο διαχειριστικό τμήμα του εξοπλισμού μέσα από την ασύρματη πρόσβαση αλλά μόνο μέσω ενσύρματης. Αυτό θα έχει ως αποτέλεσμα να αποτρέπει κάθε επιτιθέμενο που θα προσπαθεί να πειράξει το διαχειριστικό σύστημα του σημείου πρόσβασης ασύρματα.

- **Απενεργοποίηση της απομακρυσμένης πρόσβασης:** Οι περισσότεροι ασύρματοι routers προσφέρουν την δυνατότητα της απομακρυσμένης πρόσβασης στο διαχειριστικό περιβάλλον μέσω Internet. Ιδανικά, αυτή η επιλογή θα έπρεπε να υπάρχει μόνο εάν υπήρχε ο τρόπος να καθορίσει ο ίδιος την IP διεύθυνση ή εάν υπήρχε ένα περιορισμένο εύρος σταθμών, οι οποίοι θα μπορούσαν να έχουν πρόσβαση στο ασύρματο μέσο. κατά κανόνα, εκτός εάν χρειάζεστε αυτή την επιλογή, το καλύτερο είναι να την έχετε απενεργοποιημένη.

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

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

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

- **Απενεργοποιώντας το file και print sharing:** Υπάρχει η δυνατότητα απενεργοποίησης του διαμοιρασμού αρχείων και εκτυπωτών ή ακόμα και απεγκατάστασης της υπηρεσίας από την ασύρματη σύνδεση. Για την μεταφορά των αρχείων σας υπάρχει η επιλογή μιας ενσύρματης σύνδεσης ή η χρήση κάποιου USB/Flash drive.

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

- **Περιορίζοντας τον αριθμό των hosts:** Μέσω του μηχανισμού διαχείρισης των TCP/IP πρωτοκόλλων είναι δυνατός ο περιορισμός του αποδεκτού αριθμού σταθμών που μπορούν να συνδεθούν ασύρματα στον εξοπλισμό μας.

Επίσης το ασύρματο δίκτυο θα μπορούσε να απενεργοποιείται και να ανοίγει μόνο τις ώρες που το χρειάζεστε. Ελαχιστοποιώντας έτσι τους κινδύνους επίθεσης αφού δεν θα είναι ανοιχτό συνεχώς.

3.4 Άλλες μέθοδοι ασφάλειας

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

3.4.1 Firewalls

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

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

3.4.2 VPNS

Αξίζει να αναφερθούν και τα VPNs (Virtual Private Network), εφόσον αναφέραμε τα firewalls. Το VPN είναι ένα ιδιωτικό-εικονικό κανάλι, το οποίο βρίσκεται πάνω σε ένα ήδη υπάρχον δίκτυο και υποστηρίζει υπηρεσίες κρυπτογράφησης, πιστοποίησης και διαχείρισης κλειδιών. Το πλεονέκτημα του είναι η ασφαλή μετακίνηση δεδομένων μεταξύ των οντοτήτων.

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

Όπως αναφέραμε, η WEP μέθοδος κρυπτογράφησης είναι ανασφαλής. Ένας επιτιθέμενος με εμπειρία και με τα κατάλληλα εργαλεία, μπορεί να βρεθεί στην ζώνη εκπομπής του δικτύου και να συλλάβει αρκετά πακέτα ώστε να ανακτήσει τον μυστικό κωδικό WEP. Στην συνέχεια με την βοήθεια αυτού του κωδικού μπορεί να παγιδέψει και όλη την πληροφορία που μετακινείται στον αέρα και να την αποκωδικοποιήσει.

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

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

Τέλος, η χρήση ενός VPN δικτύου προϋποθέτει την εγκατάσταση λογισμικού σε κάθε σταθμό που πρόκειται να συνδεθεί στο δίκτυο. Αυτό όμως προσθέτει ακόμα έναν περιορισμό, αφού τα περισσότερα λογισμικά VPN προορίζονται για Windows λογισμικά. Πράγμα που σημαίνει ότι

σταθμοί με λειτουργικά συστήματα όπως Mac, OS, Linux και tablets, μπορεί να μην μπορούν να συνδεθούν στο δίκτυο.

3.4.3 RADIUS

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

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

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

3.4.4 Intrusion Detection Systems (IDSS)

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

Τα συστήματα αυτά είναι αποτελεσματικά όταν χρησιμοποιούνται σε συνδυασμό με τα ήδη υπάρχοντα μέτρα προστασίας των δικτύων (πολιτική ασφάλειας, τρωτών σημείων, κρυπτογράφηση δεδομένων, ταυτοποίηση του χρήστη, έλεγχο πρόσβασης και firewalls).

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

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

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

Το συμπέρασμα είναι ότι τα συστήματα αυτά αποτελούν ένα πολύτιμο εργαλείο που μπορεί να εγγυηθεί την αναβάθμιση της ασφάλειας μιας επιχείρησης. Όμως σε καμία περίπτωση δεν μπορεί να αντικαταστήσει άλλες μεθόδους ασφάλειας. Τα συστήματα αυτά δεν μπορούν παρά να χρησιμοποιηθούν σε περιβάλλοντα όπου ισχύουν ήδη τα απαραίτητα μέτρα ασφαλείας.

4 Επίλογος

4.1 Αποτελέσματα

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

Η μέθοδος κρυπτογράφησης των δεδομένων και της "μεταμφιεσμένης" μεταφοράς τους αποτελεί μια πολύ καλή ιδέα, όμως και αυτή έχει τα ελαττώματα της. Έτσι ξεκινώντας από την πρώτη μέθοδο κρυπτογράφησης (WEP), η οποία ενσωματώθηκε στο πρότυπο IEEE 802.11 το '97, έως και τις πιο συνηθισμένες μεθόδους που χρησιμοποιούνται σήμερα, αποδεικνύεται ότι καμία από αυτές τις τεχνικές δεν είναι αδιαπέραστες.

Η μέθοδος WEP, ξεκίνησε με τις καλύτερες προϋποθέσεις όμως πολύ σύντομα τα κενά της αποδείχθηκαν τεράστια, όπως είδαμε στο 3ο κεφάλαιο με την ανάκτηση του "κρυφού" κλειδιού. Με μια προσπάθεια συλλογής αρκετών IVs πακέτων η επίθεση είναι μια απλή υπόθεση. Τα προβλήματα της μεθόδου ξεκινούν από τα IVs, τα οποία είναι αυτά που καθορίζουν κάθε φορά την ψευδοτυχαία ακολουθία που παράγεται από τον αλγόριθμο RC4.

Μετά έγιναν εμφανή τα κενά που άφηνε στην ασφάλεια η παραπάνω μέθοδος, δόθηκαν λύσεις όπως η επιμήκυνση κλειδιού και εναλλακτικές μέθοδοι κρυπτογράφησης, όπως WPA/WPA2 και το σύστημα επικύρωσης 802.x.

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

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

4.2 Το μέλλον της ασύρματης ασφάλεια

Το μέλλον της ασύρματης ασφάλειας βρίσκεται στα νέα πρότυπα της οικογένειας 802.11, όπως είναι τα 802.11i και 802.11n.

Το πρότυπο 802.11i, το οποίο εγκρίθηκε για πρώτη φορά στις 24ις Ιουνίου 2004, περιλαμβάνει το σύστημα 802.x για επικύρωση (μαζί με την χρήση του EAP-Extensible Authentication Protocol), το RSN για την ανίχνευση των συσχετίσεων και την μέθοδο CCMP, η οποία βασίζεται στον αλγόριθμο κρυπτογράφησης AES.

Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη πακέτων. Επίσης χρησιμοποιεί μέγεθος κλειδιού 128bit και μέγεθος block 128bit. Τα δεδομένα του πακέτου και το MIC μεταδίδονται κρυπτογραφημένα, αφού προστεθεί η αρχική επικεφαλίδα του πακέτου και η επικεφαλίδα του CCMP.

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

Οι συσκευές που υποστηρίζουν ασύρματη δικτύωση 802.11n μπορούν να συνδεθούν στα 300Mpbs (6 φορές μεγαλύτερο από το πρότυπο 802.11g). Αυτό επιτυγχάνεται με την τεχνολογία MIMO, η οποία κάνει χρήση πολλαπλών κεραιών στο πομπό και το δέκτη, για όσο το δυνατόν μεγαλύτερη ταχύτητα.

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

Ωστόσο ο τομέας της ασφάλειας στο πρότυπο παραμένει ένα πρόβλημα προς επεξεργασία, καθώς το νέο αυτό πρότυπο προσφέρει καινοτομίες δυνατότητες ταχύτητας και εμβέλειας αλλά κληρονομεί πολλά από τα αδύναμα σημεία των προηγούμενων προτύπων σε θέματα ασφάλειας. Όπως δηλαδή συμβαίνει με κάθε νέα τεχνολογία, η έρευνα και η δοκιμή είναι απαραίτητη διαδικασία για εξέλιξη.

Βιβλιογραφία

[1] **ANSI/IEEE Std 802.11,** "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"*

[2] **Nathan J. Muller, 2003.** *"Wireless A to Z"*. **Mc Graw Hill**

[3] **Barken L., 2003.** *"How Secure is Your Wireless Network?"* **Prentice Hall PTR**

[4] **Flickenger R., 2003.** *"Wireless Hacks O'Reilly"*

[5] **Frankel S., Bermard E., Les O., and Scarfone K., 2007.** *"Establishing Wireless Robust Security Networks: A Guide to 802.11i"* **Special Publication 800-97**

[6] **Held G., 2003.** *"Securing Wireless LANs"*

[7] **Peikari C., and Fogie S., 2002.** *"Wireless Maximum Security"* **Sams Publishing**

[8] **Κατσαμβρίας Κ., 2009.** *"Μελέτη και Υλοποίηση ανίχνευσης φάσματος για Cognitive Radio σε SIMO συστήματα"*

Πηγές από διαδίκτυο

[1] https://www.wireshark.org/

[2] http://www.backtrack-linux.org/

[3] http://en.wikipedia.org/wiki/Intrusion_detection_system

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

[5] http://www.wikihow.com/Break-WEP-Encryption

[6] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[7] http://en.wikipedia.org/wiki/CCMP

Ακρώνυμα και Συντομογραφίες

- **AES -** Advanced Encryption Standard
- **AP -** Access Point
- **BSS -** Basic Service Set
- **CCMP -** Counter Mode-Cipher Block Chaining Mac Protocol
- **CRC -** Cyclic Redundancy Check
- **CSMA/CD -** Carrier Sense Multiple Access with Collision Detection
- **DCF -** Distributed Coordination Fuction
- **DOS -** Denial Of Service
- **EAP -** Extensible Authentication Protocol
- **ESS -** Extended Service Set
- **IBSS -** Independent Basic Service Set
- **ICV -**Integrity Check Value
- **IDS -** Intrusion Detection Systems
- **IV -** Initialization Vector
- **LAN -** Local Area Network
- **MAC -** Media Access Control
- **MIMO -** Multiple Input Multiple Output
- **MPDU -** Mac Protocol Data Unit
- **MSDU -**Mac Service Data Unit
- **NAV -** Network Allocation Vector
- **NIC -** Network Interface Card
- **OSA -** Open System Authentication
- **PHY -** Physical Layer
- **RADIUS -** Remote Authentication Dial-In User Service
- **RSN -** Robust Secure Network
- **RTS/CTS -** Request To Send/Clear To Send
- **SKA -** Shared Key Authentication
- **SSID -** Service Set Identifier
- **TKIP -** Temporal Key Integrity Protocol
- **TSN -** Transitional Security Network
- **VPN -** Virtual Private Network
- **WEP -** Wired Equivalent Privacy
- **WLAN -** Wireless Local Area Network
- **WPA -** Wi-Fi Protected Access
- **WPA2 -** Wi-Fi Protected Access Version2
- **WRAP -** Wireless Robust Authentication Protocol