Τ.Ε.Ι ΠΑΤΡΩΝ

Σχολή Διοίκησης και Οικονομίας

Τμήμα Επιχειρηματικού Σχεδιασμού και Πληροφοριακών Συστημάτων

ΘΕΜΑ:ΑΣΦΑΛΕΙΑ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΣΩΤΗΡΟΠΟΥΛΟΥ ΒΑΣΙΛΙΚΗ

ΜΥΛΩΝΑΣ ΜΙΧΑΗΛ

ΜΥΛΩΝΑΣ ΑΠΟΣΤΟΛΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πάτρα, Ιούνιος 2013

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε θερμά τον επιβλέποντα καθηγητή μας κ. Λουκά Μάνδαλο για την εμπιστοσύνη που μας έδειξε, καθώς επίσης και για την άριστη συνεργασία και κατανόηση του. Ακόμη, τον ευχαριστούμε για πολύτιμη βοήθεια του και καθοδήγηση για την εκπόνηση της παρούσας εργασίας.

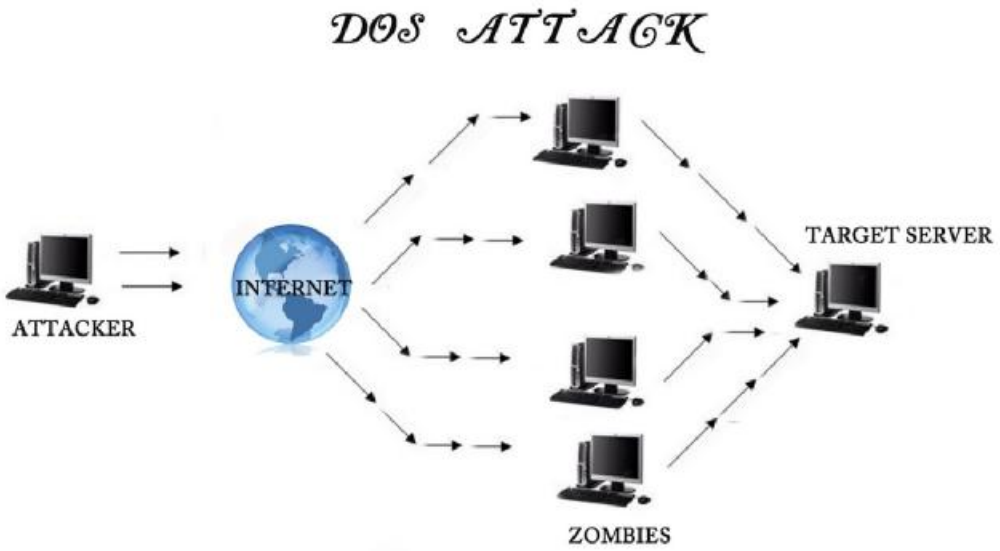
Σωτηροπούλου Βασιλική

Μυλωνάς Μιχαήλ

Μυλωνάς Απόστολος

Πάτρα, Ιούνιος 2013

Πίνακας περιεχομένων



ΚΕΦΑΛΑΙΟ 1ο:ΕΙΣΑΓΩΓΗ ΔΙΚΤΥΩΝ

1.1 Γενικά για τα δίκτυα

Τις τελευταίες δεκαετίες η **ανάπτυξη** της τεχνολογίας είχε σαν αποτέλεσμα την ραγδαία **ανάπτυξη** των δικτύων υπολογιστών. Εάν το τέλος του 20ου αιώνα χαρακτηρίστηκε ως η περίοδος της ψηφιακής επανάστασης, η αρχή της τρίτης χιλιετίας δίκαια μπορεί να χαρακτηριστεί ως η δικτυακή εποχή. Η εξάπλωση των δικτύων υπολογιστών και των υπολογιστικών μηχανών συντελείται με τέτοιο ρυθμό, που πλέον έχουν γίνει αναπόσπαστο κομμάτι της καθημερινής ζωής του σύγχρονου ανθρώπου. Ένα από τα κυρίαρχα χαρακτηριστικά στην σημερινή εποχή είναι η ανάγκη των ανθρώπων για πρόσβαση στο διαδίκτυο. Με τον όρο ανάγκη εννοούμε ότι ο κυβερνοχώρος έχει εισέλθει δυναμικά στην καθημερινότητα των ανθρώπων τόσο παθητικά όσο και ενεργητικά είτε για επαγγελματικό σκοπό είτε για ψυχαγωγία είτε για την επικοινωνία τους. Οι χρήστες αυτοί χρειάζονται πρόσβαση στο διαδίκτυο μέσα από ένα σύνολο τεχνολογικών μέσων όπως φορητοί υπολογιστές,tablets,imac και smartphones χωρίς να είναι προσδεμένοι στην επίγεια επικοινωνιακή δομή. Για τους χρήστες αυτούς η απάντηση είναι οι ασύρματες επικοινωνίες.

Σε ένα δίκτυο ο κάθε υπολογιστής πρέπει να είναι ικανός να επικοινωνεί με τους υπόλοιπους και μάλιστα αμφίδρομα, δηλαδή να έχει την δυνατότητα να διοχετεύσει

πληροφορίες αλλά και να λάβει. Για να γίνει τώρα αυτό θα πρέπει να οριστούν αρχικά ο τρόπος επικοινωνίας του με το υπόλοιπο δίκτυο. Θα πρέπει δηλαδή να οριστούν κάποιοι κανόνες για την ασφαλή και απρόσκοπτη μεταφορά των δεδομένων.
Οι συσκευές σε ένα δίκτυο δεν είναι απαραίτητο (αλλά ούτε και εφικτό πολλές φορές) να ακολουθούν τα ίδια πρότυπα ως μεμονωμένοι σταθμοί εργασίας (workstations), δηλαδή δεν είναι απαραίτητο να εκτελούν τις εντολές κάτω από το ίδιο λειτουργικό σύστημα ή να χρησιμοποιούν το ίδιο Hardware.

1.2 Τι είναι δίκτυο υπολογιστών

Δίκτυο είναι το σύνολο από υπολογιστές και συσκευές που ομοιάζουν με υπολογιστή, τα οποία επικοινωνούν μεταξύ τους μέσω ενός μέσου μεταφοράς των δεδομένων. Αυτό το μέσο μεταφοράς μπορεί να είναι καλώδιο, η τηλεφωνική μας γραμμή ή κάποιο άλλο π.χ. κάποιος ασύρματος μεταδότης.

Ένας από τους ορισμούς που έχει επικρατήσει γενικότερα για τα δίκτυα υπολογιστών είναι ο παρακάτω:

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

Η δημιουργία των δικτύων είναι απόρροια της εξάπλωσης της χρήσης των Η/Υ για την εξυπηρέτηση των αναγκών των χρηστών. Η ύπαρξη των δικτύων έχει ως σκοπό τον διαχωρισμό των πόρων του συστήματος καθώς και την ανταλλαγή κάθε είδους πληροφορίας όπως προγράμματα, αρχεία και δεδομένα. Λέγοντας πόροι του συστήματος αναφερόμαστε τόσο στο υλικό (hardware) όπως είναι οι Η/Υ, εκτυπωτές, σκληροί δίσκοι όσο και στο λογισμικό (software) όπως δεδομένα και υπηρεσίες. Κάθε ένας που έχει πρόσβαση στο δίκτυο, ανεξαρτήτως της φυσικής του θέσης, έχει

διαθέσιμα προγράμματα, δεδομένα και συσκευές. Με τον τρόπο αυτό, επιτυγχάνεται η εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα. Επίσης μέσω ενός δικτύου υπάρχει ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων και αποστολής μηνυμάτων e-mail. Επιπρόσθετα ένα δίκτυο προσφέρει έναν πανίσχυρο τρόπο επικοινωνίας των ανθρώπων ανεξαρτήτου τοποθεσίας και τεχνολογίας.

Τα δίκτυα φέρουν τους εξής χαρακτηρισμούς, που καθορίζουν και την κατηγορία τους :

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως ενσύρματα ή ασύρματα.

- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως δημόσια ή ιδιωτικά δίκτυα.

- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως

    1. Τοπικά (LAN και WLAN)
    2. Μητροπολιτικά (MAN και WMAN)
    3. Ευρείας κάλυψης (WAN και WWAN)
    4. Προσωπικά (PAN και WPAN)

Ø *Οι χαρακτηρισμοί με το πρόσθετο W ανταποκρίνονται στον ασύρματο (Wireless) τρόπο σύνδεσης*

Ο σκοπός ενός δικτύου υπολογιστών είναι να συνδέει έναν αριθμό υπολογιστών και άλλων ψηφιακών συσκευών μεταξύ τους και να επιτρέπει στους χρήστες να μεταδίδουν δεδομένα αλλά και να έχουν πρόσβαση στις υπηρεσίες και στους πόρους απομακρυσμένων υπολογιστών ή συστημάτων. Η **επικοινωνία** δηλαδή η μετάδοση και λήψη πληροφοριών σε μικρή ή μεγάλη κλίμακα και απόσταση ήτανε πάντα μείζονος σημασίας και οδήγησε τους ανθρώπους από πολύ παλιά σε προσπάθειες μετάδοσης πληροφοριών με τα διαθέσιμα τεχνολογικά μέσα της κάθε εποχής.

1.3 Οφέλη των δικτύων

Είναι σαφές ότι ένα δίκτυο υπολογιστών, μπορεί να αποφέρει πολλά οφέλη στον όποιο επαγγελματικό χώρο, αυξάνοντας την παραγωγικότητα και την αποτελεσματικότητα, σε μεγάλο βαθμό.

Τα σημαντικότερα πλεονεκτήματα των δικτύων υπολογιστών :

 **Έλεγχος των δεδομένων :** Ένα δίκτυο δίνει τη δυνατότητα στον υπεύθυνο εγκατάστασης να ελέγξει, ποιος χρήστης πρέπει να έχει ή να μην έχει πρόσβαση και ακριβώς σε ποιες πληροφορίες.

 **Ανταλλαγή αρχείων :** Είναι δυνατό να οριστούν συγκεκριμένες περιοχές στον σκληρό δίσκο ενός υπολογιστή, σαν κοινόχρηστες ή και σε όλο τον δίσκο δίνοντας δικαίωμα σε άλλους χρήστες του εσωτερικού δικτύου, να διαβάζουν ή και να γράφουν πληροφορίες.

 **Κοινή χρήση του διαθεσίμου εξοπλισμού :** Ένα δίκτυο επιτρέπει το μοίρασμα του διαθέσιμου εξοπλισμού (π.χ. των εκτυπωτών, scanner, NAS).

 **Ασφάλεια :** Ένα δίκτυο κάνει ευκολότερη τη διαχείριση των αντιγράφων ασφαλείας (backup) σημαντικών δεδομένων.

 **Κοινή χρήση Internet :** Μπορούμε να μοιράσουμε την σύνδεση του **Internet** στους υπολογιστές του δικτύου προσφέροντας πρόσβαση σε όλους.

 **Παράλληλη εκτέλεση διαχειριστικών εφαρμογών:** Εκτέλεση διαχειριστικών εφαρμογών οι οποίες είναι σχεδιασμένες για παραπάνω από έναν χρήστη (π.χ. διαχείριση πελατών, διαχείριση προμηθευτών, τιμολόγηση, λογιστική και άλλα), είναι δυνατό να χρησιμοποιούνται παράλληλα από όλους.

 **Επεκτασιμότητα :** Η προσθήκη ενός νέου σταθμού στο δίκτυο γίνεται εύκολα και γρήγορα και πέρα από όλα τα άλλα δημιουργεί τις προϋποθέσεις για την δημιουργία αλυσίδας δικτύων επικοινωνιών.

Εμείς στην παρούσα εργασία θα εστιάσουμε στην ασφάλεια των ασυρμάτων δικτύων υπολογιστών αναλύοντας τις τεχνολογίες, τα προβλήματα, τα είδη των επιθέσεων και των τεχνικών τους.

1.4 Ασύρματα δίκτυα

Οι ασύρματοι υπολογιστές αποτελούν έναν από τους γρηγορότερα εξελισσόμενους τομείς της βιομηχανίας των υπολογιστών. Παραδείγματα αποτελούν οι φορητοί υπολογιστές, όπως είναι τα notebooks και τα laptops και οι προσωπικοί ψηφιακοί βοηθοί *(Personal Digital Assistants - PDAs)*. Πολλοί από τους κατόχους ασύρματων υπολογιστών έχουν παράλληλα και προσωπικούς υπολογιστές γραφείου συνδεδεμένους σε κάποιο τοπικό δίκτυο, το οποίο μπορεί να βρίσκεται είτε στο σπίτι τους, είτε στο χώρο εργασίας τους. Αποτελεί πολύ συνηθισμένη περίπτωση αυτοί οι χρήστες να θέλουν να βρίσκονται συνδεδεμένοι με το δίκτυο αυτό, είτε όταν βρίσκονται σε κάποια άλλη τοποθεσία, είτε καθοδόν. Από τη στιγμή που δεν είναι καθόλου πρακτική η χρήση καλωδίων σε αεροπλάνα, πλοία, ή τραίνα, η έννοια της ασύρματης δικτύωσης αποτελεί μια πολύ ευέλικτη και πρακτική λύση.

Οι χρήσεις των ασύρματων δικτύων είναι πολλές. Η πιο κοινή είναι εκείνη του *φορητού γραφείου*. Οι χρήστες που βρίσκονται στη μέση ενός ταξιδιού πολύ συχνά θέλουν να χρησιμοποιούν τους φορητούς τους υπολογιστές, για να στέλνουν και να λαμβάνουν μηνύματα, τηλεφωνήματα, fax, να συνδέονται με το δίκτυο της εταιρείας

τους, κλπ και θέλουν να μπορούν να το κάνουν αυτό, είτε όταν βρίσκονται στην ξηρά, είτε στη θάλασσα, είτε στον αέρα.

1.4.1 Τι είναι ασύρματο δίκτυο

Ως **ασύρματο δίκτυο** χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί, ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου. Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά, αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και, επομένως, κατά μία έννοια, είναι ουσιαστικώς δίκτυα υπολογιστών.

Το ασύρματο δίκτυο αναφέρεται σε οποιοδήποτε τύπο δικτύου υπολογιστή που είναι ασύρματο και συνήθως συνδέεται με ένα δίκτυο τηλεπικοινωνίας του οποίου οι διασυνδέσεις ανάμεσα σε κόμβους χρησιμοποιείται χωρίς την χρήση καλωδίων όπως ένα δίκτυο υπολογιστών. Γενικά τα ασύρματα δίκτυα τηλεπικοινωνίας χρησιμοποιούνται με κάποιο είδος συστήματος εκπομπής πληροφοριών από απόσταση που χρησιμοποιεί ηλεκτρομαγνητικά κύματα, όπως ραδιοκύματα, για την μεταφορά. Αυτή η χρήση συνήθως γίνεται σε φυσικό επίπεδο η στο επίπεδο του δικτύου. Παλαιότερα τα τηλεφωνικά δίκτυα ήταν αναλογικά αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και ουσιαστικά είναι δίκτυα υπολογιστών. Στα ασύρματα δίκτυα ανήκουν τα δίκτυα κινητής τηλεφωνίας, οι δορυφορικές επικοινωνίες, τα ασύρματα δίκτυα ευρείας περιοχής (WWAN), τα ασύρματα μητροπολιτικά δίκτυα (WMAN), τα ασύρματα τοπικά δίκτυα (WLAN) και τα ασύρματα προσωπικά δίκτυα (WPAN). Η τηλεόραση και το ραδιόφωνο αν και είναι ασύρματα ως τηλεπικοινωνιακά μέσα, στις περισσότερες περιπτώσεις, δεν συμπεριλαμβάνονται στα ασύρματα δίκτυα, καθώς η μετάδοση γίνεται προς

οποιαδήποτε κατεύθυνση χωρίς να υπάρχει κάποιο δομημένο «δίκτυο» τηλεπικοινωνιακών συσκευών. Τα μεταφερόμενα δε δεδομένα συνήθως είναι αναλογικά και γι' αυτό δεν μπορούν να θεωρηθούν δίκτυα υπολογιστών.

1.4.2 Οφέλη των ασύρματων δικτύων

Τα πλεονεκτήματα ασύρματων δικτύων είναι βραχυπρόθεσμα και μακροπρόθεσμα. Ενδεικτικά αναφέρονται τα ακόλουθα:

- **Ευκολία χρήσης:** Σήμερα, όλοι οι φορητοί υπολογιστές και πολλά κινητά τηλέφωνα είναι εξοπλισμένα με τεχνολογία WiFi που απαιτείται για απευθείας σύνδεση σε ένα ασύρματο δίκτυο LAN. Οι χρήστες μπορούν να συνδέονται με ασφάλεια στους πόρους του δικτύου από οπουδήποτε εντός της εμβέλειας κάλυψης του δικτύου. Η περιοχή κάλυψης είναι κατά κανόνα οι εγκαταστάσεις του χώρου όπου βρίσκονται, ωστόσο μπορεί να επεκτείνεται και σε περισσότερα κτήρια.
- **Φορητότητα:** Οι χρήστες μπορούν να παραμένουν συνδεδεμένοι στο δίκτυο, ακόμα και όταν δεν βρίσκονται στο χώρο τους. Οι συμμετέχοντες σε συσκέψεις μπορούν να έχουν πρόσβαση σε έγγραφα και εφαρμογές. Οι πωλητές μπορούν να εντοπίζουν στο δίκτυο σημαντικές λεπτομέρειες από οποιαδήποτε τοποθεσία.
- **Παραγωγικότητα:** Η πρόσβαση στις πληροφορίες και στις βασικές εφαρμογές της εταιρείας υποστηρίζει το προσωπικό κατά τη διεκπεραίωση των εργασιών και ενθαρρύνει τη συνεργασία. Οι επισκέπτες (όπως πελάτες, συνεργάτες ή προμηθευτές) μπορούν να έχουν πρόσβαση υψηλής ασφαλείας στο Internet και στα επιχειρηματικά δεδομένα τους.
- **Εύκολη ρύθμιση:** Εφόσον δεν απαιτείται η τοποθέτηση καλωδίων σε ένα χώρο, η εγκατάσταση μπορεί να ολοκληρωθεί γρήγορα και οικονομικά. Τα ασύρματα δίκτυα LAN διευκολύνουν επίσης τη συνδεσιμότητα δικτύου σε δυσπρόσιτους χώρους, όπως οι αποθήκες ή οι εγκαταστάσεις εργοστασιακής παραγωγής.
- **Δυνατότητα κλιμάκωσης:** Καθώς οι επιχειρηματικές δραστηριότητές αναπτύσσονται, ενδεχομένως να απαιτείται άμεση επέκταση του δικτύου. Τα ασύρματα δίκτυα μπορούν κατά κανόνα να επεκταθούν με τον υπάρχοντα

εξοπλισμό, ενώ ένα ενσύρματο δίκτυο ενδέχεται να απαιτεί επιπλέον καλωδίωση.

- **Κόστος:** Μπορεί να αποδειχθεί οικονομικότερη η λειτουργία ενός ασύρματου δικτύου LAN, το οποίο εξαλείφει ή μειώνει το κόστος καλωδίωσης σε περιπτώσεις μετακόμισης, αναδιάταξης ή επέκτασης γραφείων.

1.4.3 Μειονεκτήματα των ασύρματων δικτύων

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

- **Παρεμβολή λόγω πολλαπλών διαδρομών:** Σήματα που μεταδίδονται είναι δυνατόν να συνδυαστούν με ανακλώμενα σήματα από επιφάνειες ή εμπόδια που βρίσκονται στην ευθεία μετάδοσης του σήματος.
- **Pathloss:** Οι απώλειες που μπορεί να έχουμε σε μια ασύρματη επικοινωνία από το pathloss εξαρτώνται άμεσα από την ύπαρξη ή μη οπτικής επαφής (LOS: Line Of Sight)
- **Παρεμβολές ραδιοσημάτων:** Οι παρεμβολές από ραδιοσήματα (Radio Signal Interfernece) διαχωρίζονται σε Εσωτερικές (inward) και Εξωτερικές (outward).
- **Διαχείριση ενέργειας:** Θα πρέπει να επιλέγονται προϊόντα για σωστή διαχείριση ενέργειας, ώστε να μεγιστοποιείται η αυτονομία του δικτύου.
- **Ασυμβατότητα συστημάτων:** Για το στήσιμο ενός WLAN θα πρέπει να λάβουμε υπόψη και την ασυμβατότητα μεταξύ προϊόντων διαφορετικών κατασκευαστών.
- **Προστασία της υγείας των χρηστών:** Τα ασύρματα LAN που χρησιμοποιούν την τεχνική μετάδοσης με υπέρυθρες ακτίνες, θα πρέπει να περιορίζουν την ισχύ του εκπεμπόμενου σήματος στο ανώτερο όριο των 2 Watts, για να αποφευχθούν προβλήματα υγείας

- **Το πρόβλημα του κρυμμένου κόμβου:** Το φαινόμενο αυτό παρατηρείται όταν υπάρχει ένας σταθμός που δεν μπορεί να ανιχνεύσει την δραστηριότητα ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται.
- **Ασφάλεια δικτύου:** Η συνολική λειτουργία ενός ασύρματου δικτύου εμπεριέχεται στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν ενυπάρχει με άλλες λειτουργίες όπως εγκατάσταση σύνδεσης ή άλλες υπηρεσίες (π.χ. login) που προσφέρουν τα ανώτερα στρώματα. Έτσι το μόνο θέμα που σχετίζεται με την ασφάλεια και τα ασύρματα δίκτυα είναι τα θέματα ασφαλείας των χαμηλότερων στρωμάτων, π.χ. κρυπτογράφηση (encryption) δεδομένων. Για αυτό το λόγο, έχουν δημιουργηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν δύσκολη την υποκλοπή της πληροφορίας που μεταδίδεται. Τέτοιες είναι οι τεχνικές εξάπλωσης φάσματος (spreadspectrum) ενώ εάν απαιτείται περισσότερη ασφάλεια, καθορίζεται η χρήση της κωδικοποίησης WEP (Wired Equivalent Privacy). (*Tanenbaum, 2000*)

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο των παρερχομένων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας).

Η έννοια της ασφάλειας ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε

φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων. Πιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

- Πρόληψη (prevention) :Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- Ανίχνευση (detection) :Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- Αντίδραση (reaction) :Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Η προστασία ενός δικτύου το οποίο συνδέεται και με το Internet είναι ένα θέμα που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις και οργανισμοί. Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες:

- Διαθεσιμότητα (Availability)
- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)

ΚΕΦΑΛΑΙΟ 2^{ο} :ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

2.1 Εισαγωγή

Τα τελευταία χρόνια η ανάγκη για συνεχή χρήση κάποιας μορφής ηλεκτρονικών υπολογιστών ασχέτως του σημείου που βρίσκεται κάποιος είναι διαρκώς αυξανόμενη. Κάθε άτομο που χειρίζεται ηλεκτρονικό υπολογιστή στην καθημερινότητα του έχει την ανάγκη να τον χρησιμοποιεί παντού και με εύκολο τρόπο, χωρίς να περιορίζεται στα πλαίσια ενός χώρου. Η χρήση των υπολογιστών ταυτίζεται με την ταυτόχρονη χρήση των δικτύων στα οποία διασυνδέονται οι ηλεκτρονικοί υπολογιστές. Για αυτό τον λόγο δεν μπορεί να θεωρηθεί ως ισχυρό πλεονέκτημα το να χρησιμοποιεί κάποιος έναν υπολογιστή χωρίς να συνδέεται σε κάποιο είδος δικτύου πληροφοριών.

Με την δημιουργία των φορητών υπολογιστών (laptop) λύθηκε το πρόβλημα της φορητότητας. Επίσης η διαρκώς αναπτυσσόμενες τεχνολογίες των ασυρμάτων δικτύων έλυσαν το πρόβλημα της διασύνδεσης των υπολογιστών αυτών. Ο συνδυασμός ενός φορητού υπολογιστή με μια ασύρματη σύνδεση σε κάποιο τοπικό δίκτυο και κατ' επέκταση με το διαδίκτυο είναι πλέον μια συνηθισμένη υπόθεση. Δημόσιοι χώροι, κοινόχρηστοι χώροι, αεροδρόμια, πανεπιστήμια, ΤΕΙ έχουν εγκαταστάσεις ασύρματων δικτύων, έτσι λοιπόν, δόθηκαν λύσεις στις συνδέσεις απομακρυσμένων δικτύων καταργώντας τα καλώδια. Τέλος οι ασύρματες συνδέσεις χρησιμοποιούνται δυναμικά και από τη κινητή τηλεφωνία.

2.2 Βασικές τεχνολογίες ασύρματων δικτύων

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

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

Για την υλοποίηση ενός WLAN επιλέγεται ένα από τα πολλά πρότυπα που έχουν

δημιουργήσει διάφοροι οργανισμοί και εταιρείες τα τελευταία χρόνια. Στη συνέχεια αναφέρονται τα κυριότερα.

- IEEE 802.11

  Καθορίζει τον έλεγχο πρόσβασης μέσω (MAC) και τα φυσικά στρώματα (PHY) για ένα LAN ασύρματη σύνδεση.
- HiperLAN

  Βασίζεται στο χρόνο ζωής του πακέτου, την προτεραιότητα και τις αναμεταδόσεις στο επίπεδο MAC
- Open Air

  Χρησιμοποιεί την τεχνική του Frequency Hopping με ρυθμούς δεδομένων 0.8 και 1.6 Mbps.
- HomeRF SWAP

  Οικονομικό πρότυπο για μεταφορά ήχου και δεδομένων με ταχύτητα μέχρι 2 Mbps.
- Ασύρματα Point-to-Point δίκτυα

  Εκπροσωπούνται από τα ασύρματα μητροπολιτικά δίκτυα WMAN χρησιμοποιώντας τεχνολογίες όμοιες με αυτές των WLAN.
- Ασύρματα Point-to-Multipoint δίκτυα
- Bluetooth

  Άμεση επικοινωνία μεταξύ 2 ή και περισσότερων συσκευών.
- Τεχνολογία MIMO(Multiple Input Multiple Output)

  Στοχεύει στην βελτίωση της ακτίνας δράσης, της ισχύς του σήματος και της αξιοπιστίας WLAN.
- IEEE 802.16 (WIMAX)

  Δημιουργήθηκε προκειμένου να βελτιωθούν θέματα που σχετίζονταν με το φάσμα συχνοτήτων, την ποιότητα εξυπηρέτησης και τη δια λειτουργικότητα.

Στη συγκεκριμένη εργασία έμφαση θα δοθεί στα δίκτυα της οικογένειας IEEE 802.11 και IEEE 802.16

2.3 Εισαγωγή στο πρότυποIEEE 802.11

Το 1997 δημοσιεύθηκε από ομάδες εργασίας του ινστιτούτου ηλεκτρολόγων και ηλεκτρονικών μηχανικών, το γνωστό Institute of Electrical and Electronics Engineers (IEEE), ύστερα από 7 χρόνια ανάπτυξης, το πρώτο πρότυπο ασύρματων τοπικών δικτύων (WLAN), το IEEE 802.11. Το πρότυπο IEEE 802.11 περιγράφει τις τεχνολογίες που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα και εξετάζει την τοπική δικτύωση όπου οι συνδεδεμένες συσκευές επικοινωνούν μέσω του αέρα με άλλες συσκευές που βρίσκονται κοντά η μια στην άλλη.

Το πρότυπο IEEE 802.11 είναι μια οικογένεια πρωτοκόλλων που περιγράφουν τη λειτουργία ασύρματων τοπικών δικτύων, WLAN. Περιγράφονται τα δύο πρώτα επίπεδα του μοντέλου OSI, δηλαδή το φυσικό επίπεδο (PHY, Physical Layer) και το επίπεδο σύνδεσης δεδομένων (MAC, Medium Access Control). Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την λειτουργικότητα των συσκευών που το ακολουθούν.

Περιγράφοντας μόνο τα δύο κατώτερα επίπεδα, επιτρέπει σε οποιαδήποτε εφαρμογή να εργάζεται πάνω σε συσκευή 802.11 όπως ακριβώς θα εργαζόταν πάνω από Ethernet. Δηλαδή τα πιο πάνω επίπεδα δεν γνωρίζουν και δεν απασχολούνται από το τι βρίσκεται πιο κάτω.

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

2.3.1 Τι είναιWi-Fi

Με την ταχύτατη ανάπτυξη των προτύπων IEEEκαι την εμφάνιση μεγάλου αριθμού κατασκευαστών της βιομηχανίας των ασύρματων συσκευών, κρίθηκε αναγκαία η διασφάλιση της συμβατότητας μεταξύ των διαφόρων συσκευών και της προστασίας του καταναλωτή.

Έτσι ιδρύθηκε το 1999 ηWEKA (Wireless Ethernet Compatibility Alliance). Είναι ένας μη κερδοσκοπικός οργανισμός που έχει ως σκοπό την πιστοποίηση ασύρματων συσκευών 802.11. Στο συγκεκριμένο οργανισμό λαμβάνουν μέρος κατασκευαστές

ολοκληρωμένων κυκλωμάτων, παροχής υπηρεσιών WLAN, κατασκευαστές λογισμικού, κατασκευαστές υπολογιστών και άλλοι. Κάποιες από τις εταιρείες που συμμετέχουν είναι οι IBM, Apple, Nokia, Samsung, 3Com, Dell, Compaq, Symbol Technologies και πολλές άλλες.

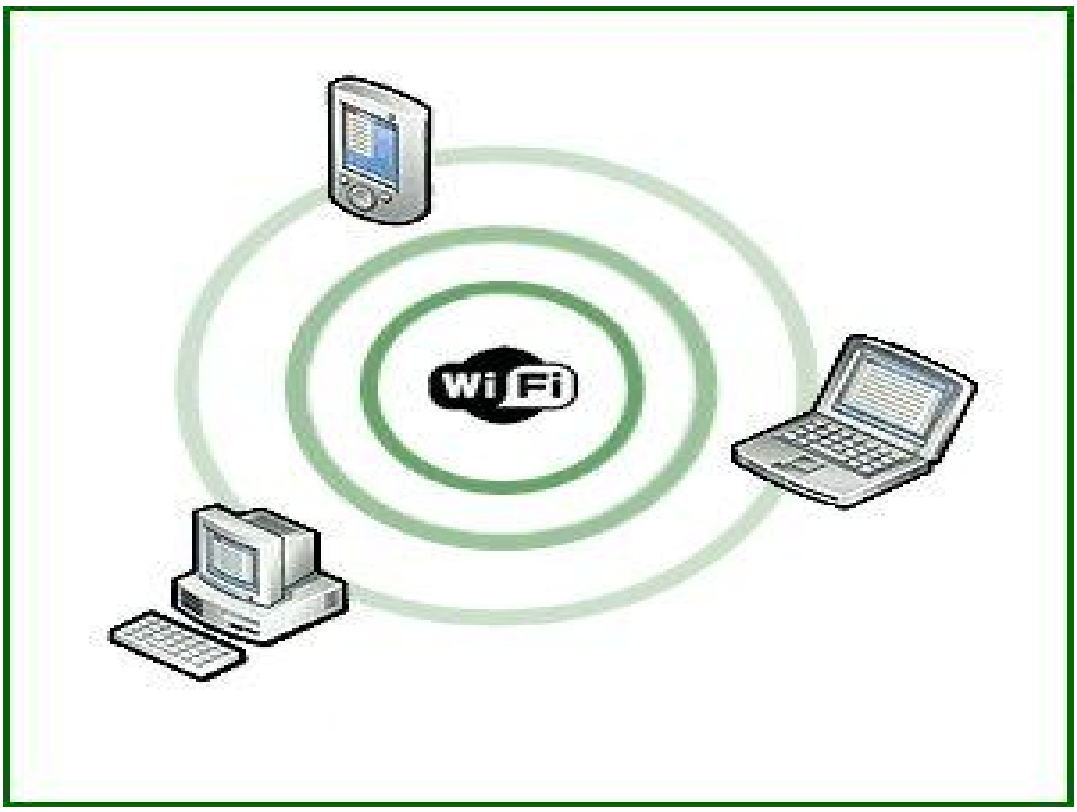
Η ένωση αυτή δημιούργησε μια σειρά από δοκιμές προκειμένου να πιστοποιηθεί η συμβατότητα τωνIEEE προϊόντων. Οι συσκευές που θα περνούσαν με επιτυχία αυτές τις δοκιμές, θα αποκτούσαν το λογότυπο Wi-Fi (Wireless Fidelity). Έτσι το συγκεκριμένο λογότυπο θα αποτελούσε πιστοποίηση για τον υποψήφιο αγοραστή μιας συσκευής καθώς επίσης και εγγύηση για την επένδυσή του. Όταν ο πελάτης αγοράζει μια συσκευή με το λογότυπο Wi-Fi, η συσκευή εγγυάται ότι θα συνεργαστεί και με οποιαδήποτε άλλη συσκευή αναγράφει το λογότυπο αυτό.

Εικόνα 1: Λογότυπο Wi-Fi

Το Wi-Fi αποτελεί έναν ασύρματο τρόπο διασύνδεσης μεταξύ των ηλεκτρονικών συσκευών όπως είναι ο φορητός ή σταθερός υπολογιστής, ενώ ταυτόχρονα υπάρχει η δυνατότητα σύνδεσης με το Διαδίκτυο. Μοναδική προϋπόθεση σύνδεσης συσκευών στο Wi-Fi είναι να μπορούν να συνδεθούν σε ασύρματο δίκτυο Wi-Fiείτε μέσω μιας κάρτας ασύρματου δικτύου ήδη εγκατεστημένης είτε με την προσθήκη μιας τέτοιας κάρτας, και επιπρόσθετα πρέπει να βρίσκεται σε περιοχή κάλυψης του σήματος.

Το ασύρματο δίκτυο μπορεί να εγκατασταθεί είτε από τον εργασιακό σας χώρο, το σπίτι σας είτε ακόμη και από χώρους ψυχαγωγίας ή κοινόχρηστους έχοντας την

δυνατότητα να συνδεθείτε με έναν ή περισσότερους υπολογιστές τοπικά ή ευρυζωνικά με το Διαδίκτυο.



Εικόνα 2:Μέσα σύνδεσης στο Wi-Fi

2.4 Βασικά χαρακτηριστικά για το 802.11

Το 802.11 επιτρέπει την εναλλαγή και την κινητικότητα των συσκευών που υποστηρίζουν και δίνει την δυνατότητα στον πελάτη να κινείται και να επιλέγει μεταξύ πολλών 802.11 σταθμών βάσης που λειτουργούν στις ίδιες ή διαφορετικές συχνότητες (κανάλια).Αυτό επιτυγχάνεται μέσω της χρήσης πλαισίων αναγνωριστικών σημάτων, τα οποία χρησιμοποιούνται για να συγχρονίσουν τις συσκευές 802.11 και της υποδομής που συνδέει τις συσκευές με κάθε σταθμό βάσης.

Για να ανιχνευτούν τα υπάρχοντα 802.11 δίκτυα υπάρχουν 2 τρόποι: . Στον ενεργητικό τρόπο ανίχνευσης, η 802.11 συσκευή στέλνει “probe” πλαίσια, που ζητάνε απαντήσεις που να δηλώνουν την ύπαρξη άλλων υπάρχουσων συσκευών

802.11. Στον παθητικό τρόπο, οι συσκευές απλά περιμένουν για αναγνωριστικά πλαίσια, τα οποία μεταδίδονται περιοδικά από τις ενεργές συσκευές.

Η ασφάλεια του IEEE 802.11 δεν είναι ισάξια με τις υπόλοιπες συσκευές του προτύπου παρόλο που θεωρείται επιτυχές. Οι σχεδιαστές του IEEE 802.11 γνώριζαν την ανάγκη της ύπαρξης διαδικασιών ταυτοποίησης και μυστικότητας, στην εφαρμογή το σχέδιο δεν λειτούργησε και τόσο καλά. Το πρόβλημα εντοπίζεται στον αλγόριθμο WEP που χρησιμοποιήθηκε για τον σκοπό αυτό.

2.4.1 Ανάλυση του προτύπου 802.11b

Την χρονιά 1999 το IEEE 802.11b παρουσιάστηκε ως η βελτιωμένη εκδοχή του αρχικού πρωτοκόλλου 802.11 και σκοπός του ήταν η αύξηση της απόδοσης των ασύρματων δικτύων με ταχύτητα έως 54 Mbps. Το 802.11b λειτουργεί σε συχνότητα 2.4 GHZ για συσκευές όπως φούρνοι μικροκυμάτων, Bluetooth , ασύρματα τηλέφωνα και monitor μωρών. Χρησιμοποιεί σύστημα μετάδοσης το DSSS (τεχνική ευρέως φάσματος άμεσης ακολουθίας) και περιέχει ρυθμούς μετάδοσης 5.5 και 11 Mbps. Η τεχνική αυτή χρησιμοποιεί την Συμπληρωματική Διαμόρφωση Κώδικα (CCK) καθιστώντας έτσι δυνατή την επίτευξη ταχυτήτων έως 11 Mbps. Επιπλέον το φυσικό επίπεδο του 802.11b χρησιμοποιεί ακριβώς τα ίδια πλαίσια με του αρχικού με αποτέλεσμα την συνύπαρξη των δύο φυσικών επιπέδων στο ίδιο βασικό σύνολο εξυπηρέτησης καθώς και την ανταλλαγή δεδομένων.

Είναι το δημοφιλέστερο από όλα τα πρότυπα καθώς θεωρείται αυτό με την μεγαλύτερη δια λειτουργικότητα όντας στιβαρό, αποτελεσματικό και δοκιμασμένο .

Μια συσκευή που λειτουργεί με το 802.11b υλοποιεί και τους τρόπους μετάδοσης του 802.11 με αποτέλεσμα να είναι συμβατή με αυτό. Η ιδιότητα αυτή ονομάζεται συμβατότητα προς τα πίσω, μπορούν δηλαδή καινούργιες συσκευές να συνεργαστούν και με παλιότερες έτσι ώστε ο καταναλωτής να μην υποχρεωθεί να αλλάξει τον εξοπλισμό του ολοκληρωτικά.

2.4.2 Ανάλυση του προτύπου 802.11g

Το IEEE 802.11g-2003 ή 802.11g είναι μια τροποποίηση του IEEE 802.11 που η παρατεταμένη διεκπεραίωση φτάνει ως 54 Mbit/s χρησιμοποιώντας την ίδια συχνότητα των 2.4 GHZ όπως το 802.11b. αυτή η ιδιαιτερότητα υπό την εμπορική ονομασία ως WI-FI, έχει εφαρμοστεί σε όλον τον κόσμο. Το 802.11 είναι ένα σύνολο των επιπέδων της IEEE που διέπουν ασύρματες μεθόδους μετάδοσης δικτύωσης. Κοινώς σήμερα χρησιμοποιούνται στις 802.11 a/b/g/n εκδόσεις που παρέχουν ασύρματη συνδεσιμότητα στο σπίτι, το γραφείο και ορισμένες εμπορικές επιχειρήσεις.

Είναι το τρίτο πρότυπο διαμόρφωσης για ασύρματα δίκτυα LAN . Το υλικό του 802.11g είναι πλήρως συμβατό με τα πρότυπα του 802.11b υλικού. Λεπτομέρειες των αποφάσεων b και g λειτουργούν μαζί και καταλαμβάνουν μεγάλο μέρος της τεχνικής διαδικασίας. Σε ένα δίκτυο 802.11g, ωστόσο, η παρουσία ενός συμμετέχοντος 802.11b θα μειώσει σημαντικά την ταχύτητα του 802.11g δικτύου. Το σχήμα διαμόρφωσης που χρησιμοποιείται στο 802.11g είναι ορθογώνια συχνότητα πολλαπλής διαίρεσης(OFDM).

2.4.3 Ανάλυση του 802.11 n

Το IEEE 802.11 n είναι μια τροποποίηση του IEEE 802.11 – 2007 επιπέδου ασύρματης δικτύωσης για την βελτίωση της δικτύωσης μέσω των δύο προηγούμενων μοντέλων 802.11 a και 802.11g με σημαντική αύξηση της καθαρής σε ρυθμό μετάδοσης δεδομένων από Mbit/s σε 600 Mbit/s. Ένα επιπλέον χαρακτηριστικό που ενσωματώνεται στο 802.11n είναι ότι τα κανάλια λειτουργούν σε ένα πλάτος καναλιών 40 MHZ. Το 802.11 n υποστηρίζει πολλαπλές εισόδους-πολλαπλές εξόδους (MIMO) και αθροιστικά πλαίσια καθώς και οι βελτιώσεις ασφάλειας μεταξύ άλλων χαρακτηριστικών. Το πρότυπο 802.11n χρησιμοποιεί νέες τεχνολογίες για να δώσει στο Wi-Fi μεγαλύτερη ταχύτητα και εύρος.

Η πιο αξιοσημείωτη τεχνολογία ονομάζεται multiple-input, multiple-output (MIMO). Η τεχνολογία MIMO χρησιμοποιεί αρκετές κεραίες για να μεταδώσει πολλαπλές ροές δεδομένων από το ένα μέρος στο άλλο. Αντί για την αποστολή και λήψη μιας ενιαίας ροής δεδομένων, η MIMO μπορεί να μεταδώσει ταυτόχρονα τρεις ροές δεδομένων

και να λαμβάνει δύο. Αυτό επιτρέπει περισσότερα δεδομένα να μεταδοθούν στην ίδια χρονική περίοδο. Αυτή η τεχνική μπορεί επίσης να αυξήσει την περιοχή ή την απόσταση κατά την οποία τα δεδομένα μπορούν να μεταδοθούν.

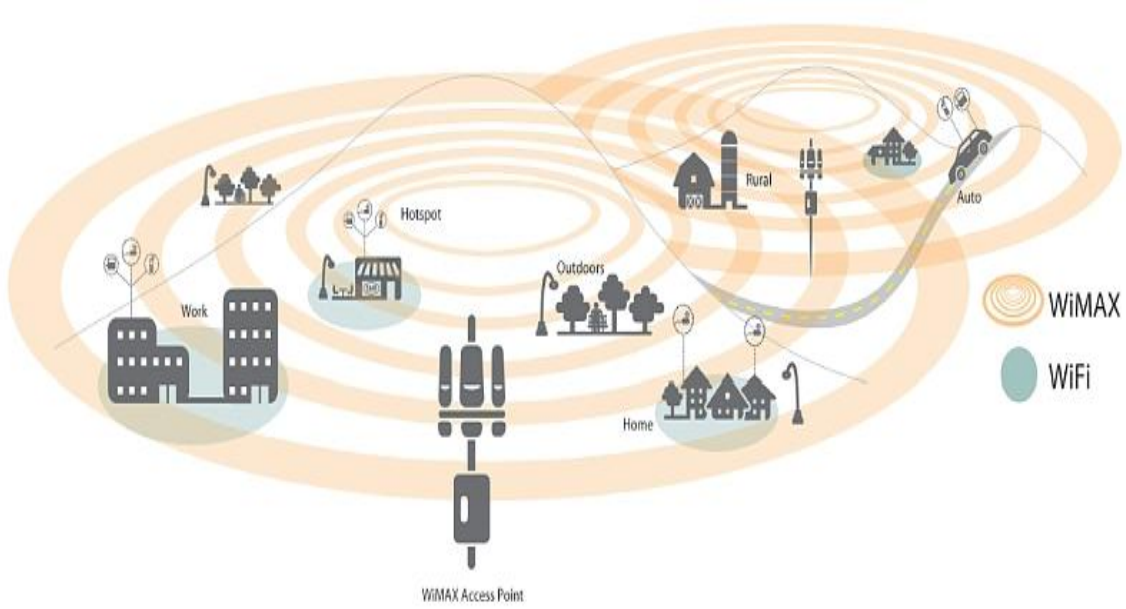
2.5 Εισαγωγή στο πρότυπο 802.16

Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16 γνωστό και σαν WiMax, ώστε να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση (με σταθερούς ρυθμούς) ευρείας ζώνης. Όπως συμβαίνει με τα πρότυπα της σειράς 802 για ασύρματα τοπικά δίκτυα, έτσι και το 802.16 καθορίζει μια οικογένεια προτύπων με επιλογές για συγκεκριμένες ρυθμίσεις. Το WiMax είναι μια νέα τεχνολογία, ένα βήμα μπροστά από το Wi-Fi, που παρέχει ασύρματη ευρυζωνική πρόσβαση υψηλών ταχυτήτων σε μεγάλες αποστάσεις. Είναι σαφώς καλύτερο από το Wi-Fi και μπορεί να καλύψει μεγαλύτερες αποστάσεις μετάδοσης. Πλέον ένας φορητός υπολογιστής μπορεί να συνδυάζει τις ιδιότητες κινητού τηλεφώνου και ραδιοφωνικού πομπού: θα πιάνει «παντού» και θα εξασφαλίζει επικοινωνία με και από κάθε γωνιά του πλανήτη.

Τα αρχικά της λέξης WiMax προκύπτουν από τις λέξεις World Interoperability for Microwave Access και είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος ταυτοποιεί συγκεκριμένο εξοπλισμό υποστηριζόμενος από εταιρίες (Intel) προσπαθώντας να προωθήσει το πρότυπο 802.16 σε κάθε ευρυζωνικής ασύρματης πρόσβασης σύστημα. Για να γίνουμε λίγο πιο σαφής το WiMax δεν είναι ένα πρότυπο αλλά ένα εμπορικό όνομα που αναφέρεται σε κάθε σύστημα και εφαρμογή που χρησιμοποιεί το πρότυπο 802.16.Το να ταυτοποιείται λοιπόν ένα προϊόν με το όνομα WiMax σημαίνει ότι έχει κατασκευαστεί με βάση το πρότυπο 802.16 και έτσι εξασφαλίζεται η συμβατότητα και η δια λειτουργικότητα (interoperability) στον BWA(broadband wireless access) εξοπλισμό.

Αντίθετα με άλλα ασύρματα δίκτυα, τα οποία επιτρέπουν μεταδόσεις μόνο με ένα φάσμα συχνότητας, το WiMax επιτρέπει τη μεταφορά δεδομένων με πολλαπλά, ευρέα φάσματα συχνότητας. Αυτό βοηθάει πάρα πολύ, γιατί το να υπάρχουν πολλά

φάσματα, μεγιστοποιεί τη δυνατότητα της τεχνολογίας να μεταδώσει πέρα από τις συχνότητες άλλων ασύρματων εφαρμογών.



Εικόνα 3: WiMax vs Wi-Fi

Το WiMax αναμένεται να επιτρέψει αληθινές ευρυζωνικές ταχύτητες πέρα από τα ασύρματα δίκτυα με κόστος που θα καταστήσει ενεργή την υιοθέτηση μαζικής αγοράς. Το WiMax είναι το μόνο ασύρματο πρότυπο που σήμερα έχει τη δυνατότητα να παραδώσει τις αληθινές ευρυζωνικές ταχύτητες και βοηθάει στο να γίνει το όραμα της κυρίαρχης συνδεσιμότητας μια πραγματικότητα.

2.5.1 Πλεονεκτήματα προτύπου 802.16

Τα *βασικά πλεονεκτήματα* των συστημάτων που βασίζονται στο πρότυπο 802.16 είναι τα εξής:

- Η ικανότητα γρήγορης παροχής υπηρεσιών ακόμα και σε περιοχές πολύ απομακρυσμένες όπου η εγκατάσταση ενσύρματων δικτύων θα ήταν εξαιρετικά δύσκολη.
- Αποφυγή μεγάλου κόστους εγκατάστασης.

- Η ικανότητα υπέρβασης των φυσικών περιορισμών που υπάρχουν στην ενσύρματη δικτύωση

Συνοψίζοντας τα παραπάνω θα μπορούσαμε να πούμε ότι το 802.16 συνιστά ένα πολύ ευέλικτο και οικονομικό πρότυπο το οποίο μπορεί να καλύψει τις αδυναμίες της ενσύρματης δικτύωσης και επιπλέον να παρέχει νέες υπηρεσίες και προϊόντα.

2.6 Τι είναι το WiMax

WiMaxκαλείται η τεχνολογία ασύρματης δικτύωσης, η οποία λειτουργεί με παραπλήσιο τρόπο με την Wi-Fiαλλά με μεγαλύτερη εμβέλεια. Πιο συγκεκριμένα , το Wi-Fi εξασφαλίζει εμβέλεια επικοινωνίας μέχρι 100 μέτρα σε αντίθεση με το WiMaxπου φτάνει τα 35 χιλιόμετρα –μπορεί και παραπάνω.

Το WiMax θα χρησιμοποιείται για την παροχή υπηρεσιών ευρυζωνικής πρόσβασης στο Διαδίκτυο σε τελικούς χρήστες, με εξοπλισμό ιδιαίτερα εύκολο στην εγκατάσταση. Με τον ίδιο τρόπο που σήμερα εγκαθιστά κανείς στον υπολογιστή του μια κάρτα δικτύωσης Wi-Fi, στο μέλλον θα εγκαθιστά μια κάρτα WiMaxη οποία θα του επιτρέπει να χρησιμοποιήσει από τον οικιακό του χώρο (και όχι μόνο) τις ασύρματες υπηρεσίες που παρέχουν οι ISP.

Το WiMax έχει σημαντικά πλεονεκτήματα έναντι των σημερινών ασύρματων και ενσύρματων συνδέσεων:

- Ιδιωτικές εταιρείες θα έχουν τη δυνατότητα να αναπτύξουν ανεξάρτητα ασύρματα δίκτυα τηλεπικοινωνιών και υπηρεσιών Internet, με πολύ μεγάλη ευκολία, καθώς δεν απαιτείται η εγκατάσταση καλωδίων σε κάθε σημείο της χώρας, αυξάνοντας τον ανταγωνισμό.

- Ο συνδρομητής θα μπορεί να χρησιμοποιήσει τη σύνδεσή του από οπουδήποτε ακόμη και εν κινήσει μέσα στην πόλη ή και ολόκληρη τη χώρα. Κάτι που δεν είναι εφικτό με τις σημερινές συνδέσεις ADSL, ούτε και με την τεχνολογία Wi-Fi, λόγω της περιορισμένης της εμβέλειας.

- Ένα δίκτυο WiMax που θα καλύπτει μια μεγαλούπολη μπορεί να εγκατασταθεί σε λίγες μέρες, σε αντίθεση με ένα αντίστοιχο ενσύρματο δίκτυο που θα χρειαζόταν πολλούς μήνες ή και χρόνια.

- Μετακομίζοντας σε άλλη περιοχή, ο συνδρομητής δεν θα χρειαστεί να κάνει ενεργοποίηση ευρυζωνικής σύνδεσης στον νέο του χώρο, όπως ισχύει για τις ADSLγραμμές. Αφού θα καλύπτεται από το ασύρματο σήμα του πάροχου υπηρεσιών WiMax, μπορεί να αρχίσει άμεσα να χρησιμοποιεί τη σύνδεσή του.

Το WiMax θα επιτρέπει επίσης την πραγματοποίηση τηλεφωνικών κλήσεων ή ακόμη και βιντεοκλήσεων, λόγω των υψηλών ταχυτήτων μετάδοσης δεδομένων.

ΚΕΦΑΛΑΙΟ3^{0}:ΠΡΟΒΛΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

3.1 Προβλήματα ασφάλειας

Είναι γνωστό από παλιά ότι η διακίνηση των πληροφοριών αντιμετωπίζει κάποιες αδυναμίες όσο αφορά την ασφάλεια. Τα δεδομένα διακινούνται ανά πάσα στιγμή στο δίκτυο και διοχετεύονται ελεύθερα επιτρέποντας στον οποιοδήποτε επισκέπτη να τα χρησιμοποιήσει είτε για καλό σκοπό είτε για να εξαπολύσει μια οποιαδήποτε επίθεση. Οι επιθέσεις που μπορεί να δεχτεί ένα ασύρματο δίκτυο χωρίζονται σε δυο βασικούς τύπους. Ο πρώτος έχει ως βασικό σκοπό την υποκλοπή των διακινούμενων πληροφοριών. Στόχος αυτών των επιθέσεων, κατά κύριο λόγο, είναι τα εταιρικά δίκτυα στα οποία ανταλλάσσονται αρκετά ευαίσθητες πληροφορίες τόσο για την ίδια την εταιρεία όσο και για τους ανταγωνιστές της. Ο δεύτερος τύπος περιλαμβάνει επιθέσεις, με τις οποίες ένας «κακόβουλος» χρήστης προσπαθεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει ένα ασύρματο δίκτυο προσωρινά. Σκοπός ενός «εισβολέα» στο δίκτυο είναι η γνωστοποίηση των πληροφοριών, η μεταβολή και καταστροφή αυτών καθώς και η εισαγωγή προγραμμάτων ιών στο σύστημα.

3.2 Τύποι επιθέσεων στα ασύρματα δίκτυα

Η σκέψη της πρόσβασης σε ένα άγνωστο μέσο και η εξερεύνηση δεδομένων που θεωρούνται κρυφά (μυστικά) ή ξένα για εμάς, αποτελούν ένα από τα σημαντικότερα κίνητρα για πολλούς από τους επίδοξους επιτιθέμενους χρήστες. Ωστόσο οι στόχοι των επιθέσεων και οι προθέσεις σίγουρα διαφέρουν.

Η έννοια της επίθεσης ορίζεται ως:

Ορισμός: Ως επίθεση ορίζεται οποιαδήποτε προσπάθεια για παραβίαση της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας ενός συστήματος ή ενός δικτύου. Ακόμη είναι μια οποιαδήποτε μη εξουσιοδοτημένη ενέργεια που έχει ως σκοπό να

εμποδίσει ή να αχρηστεύσει τους μηχανισμούς ασφάλειας και ελέγχου πρόσβασης ενός συστήματος ή ενός δικτύου.

Γενικότερα, οι επιθέσεις σε ασύρματα δίκτυα χωρίζονται σε ενεργητικές και παθητικές.

3.2.1 Παθητικές επιθέσεις

Ως παθητικές ορίζονται οι επιθέσεις στις οποίες ο χρήστης δεν παρεμβαίνει καθόλου στη ροή των πληροφοριών μέσα στο δίκτυο. Τέτοιου τύπου επίθεση θεωρείται η Λήψη Πληροφοριών (Snooping/Footprinting). Η παθητική εισβολή διακρίνεται σε δυο υποκατηγορίες:

1. Η πρώτη, αφορά την παρατήρηση περιεχομένων των μηνυμάτων στην οποία ο επιτιθέμενος υποκλέπτει μέρος αυτής ή και ολόκληρη την διακινούμενη πληροφορία.
2. Ενώ στη δεύτερη υποκατηγορία ο επιτιθέμενος χρήστης καταγράφει και αναλύει τα μηνύματα που διέρχονται μέσα στο δίκτυο με σκοπό να συγκεντρώσει άμεσες πληροφορίες. Οι πληροφορίες αυτές αφορούν την δομή του συστήματος, τα πρωτόκολλα που χρησιμοποιούνται , τους ενεργούς χρήστες και κόμβους καθώς και τις εκτελούμενες υπηρεσίες και εφαρμογές του συστήματος.

3.2.1.1 Παθητικές: Λήψη Πληροφοριών (Snooping/Footprinting)

Η λήψη πληροφοριών (snooping) έχει σχέση με την ανάκτηση μη εμφανών προσωπικών δεδομένων από μη εξουσιοδοτημένους χρήστες. Σε αυτή την περίπτωση, θα βοηθούσε μια ασφαλής μέθοδος κρυπτογράφησης για να αντιμετωπιστούν τέτοιες επιθέσεις.

Αρχικά, ο επιτιθέμενος είναι σε θέση να διαβάσει όλες τις πληροφορίες που προέρχονται από τα σημεία πρόσβασης, συνεπώς γνωρίζει το όνομα του δικτύου(ή αλλιώς SSID). Ακόμη, με την εξέταση της διεύθυνσης MACτου, είναι πιθανό να

μπορεί να προσδιορίσει τον κατασκευαστή κάθε σημείου πρόσβασης. Επίσης η παρακολούθηση της πορείας μιας μεγάλης ποσότητας πακέτων προς τα σημεία πρόσβασης, μπορεί να δώσει τον αριθμό των ασύρματων συσκευών που συνδέονται με κάθε σημείο πρόσβασης. Αν η κρυπτογράφηση που χρησιμοποιείται στο δίκτυο είναι WEP, τότε μπορεί να τσεκάρει εάν ο καθένας χρησιμοποιεί κοινό κλειδί ή εάν κάθε συσκευή έχει διαφορετικό κλειδί με την εξέταση των bit στην IEEE 802.11 επιγραφή. Οι πληροφορίες αυτές θα μπορούσαν να είναι χρήσιμες αργότερα.

Άλλη μια μέθοδος που χρησιμοποιείται είναι η τεχνική της ανάλυσης κυκλοφορίας. Η ανάλυση αυτή είναι η μελέτη των εξωτερικών στοιχείων των μηνυμάτων όπως είναι για παράδειγμα η συχνότητα επικοινωνίας και το μέγεθος. Δυστυχώς, είναι δυνατό να μαθευτεί ολόκληρο ή ένα μέρος για τους τύπους των πραγμάτων που συμβαίνουν σε ένα δίκτυο ακριβώς με την προσοχή των μηκών πακέτων και τη σημείωση του συγχρονισμού χωρίς κοίταγμα μέσα στα πακέτα. Παρόλα αυτά όμως δεν υπάρχει άμεση πρόσβαση στο περιεχόμενο μηνυμάτων.

Ένα από σημαντικότερα και διασημότερα εργαλεία ανάλυσης και παρακολούθησης κυκλοφορίας αλλά και στο εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα σε παγκόσμια κλίμακα είναι το Wireshark.

3.2.2 Ενεργητικές επιθέσεις

Ως ενεργητικές ορίζονται οι επιθέσεις στις οποίες ο εισβολέας παρεμβαίνει στο σύστημα επομένως και στην διακίνηση της πληροφορίας. Οι ενεργητικές επιθέσεις, ανάλογα με τον σκοπό του κάθε επιτιθέμενου , διακρίνονται σε τέσσερις βασικές κατηγορίες:

- WEP cracking – Ανάκτηση κωδικού WEP
- Man in the Middle Attack – Τροποποίηση δεδομένων
- Spoofing – Μεταμφίεση
- Denial of Service (DOS) – Άρνηση υπηρεσιών

3.3 Σπάζοντας την ασύρματη ασφάλεια

Είναι γνωστό ότι τα ασύρματα δίκτυα είναι ευάλωτα στους εισβολείς. Η ανάπτυξη και η επέκταση διαφόρων μηχανισμών ασφάλειας για τα ασύρματα δίκτυα δημιουργούν ολοένα και περισσότερους τρόπους με τους οποίους κάποιοι μπορούν να επιτεθούν σε αυτά.

Σε ένα δίκτυο γίνεται επίθεση όταν ένας επιτιθέμενος χρησιμοποιεί κάποιες τεχνικές ή τεχνολογίες κακόβουλα και προσπαθεί να παραβιάσει την ασφάλεια του δικτύου. Οι επιθέσεις αυτές πραγματοποιούνται από άτομα που έχουν πρόσβαση στους στόχους τους μέσω διαδικτύου, από εξουσιοδοτημένους χρήστες που προσπαθούν να αποκτήσουν περισσότερα δικαιώματα από αυτά που τους έχουν δοθεί και από χρήστες που είναι εξουσιοδοτημένοι, οι οποίοι εκμεταλλεύονται τα δοθέντα δικαιώματα με κακό σκοπό.

Οι επιθέσεις αυτές πραγματοποιούνται κατά κύριο λόγο από άτομα γνωστά ως «hackers».

Οι επιτιθέμενοι στα εταιρικά δίκτυα χρησιμοποιούν τα δεδομένα για οικονομικό κέρδος ή για βιομηχανική κατασκοπία, με το να χρησιμοποιούν παράνομα λογαριασμούς χρηστών για να δημιουργήσουν ζημιές σε παραποιημένα στοιχεία, να κλέψουν τα δεδομένα και το λογισμικό.

Η ασύρματη ασφάλεια ενός δικτύου έχει αναλυθεί πιο πάνω, αλλά πρέπει να κατανοήσουμε από τι κινδυνεύουμε και πως θα προστατεύσουμε το δίκτυο μας, προτού εξετάσουμε τους τρόπους για να υπερασπίσουμε το ασύρματο δίκτυο.

3.4 WEP Cracking

Ένα από τα μεγαλύτερα προβλήματα των επιθέσεων κατά του WEP είναι ότι με την συλλογή μεγάλου ποσοστού πακέτων IVs, μπορούμε να καταναλώσουμε σημαντικά μεγάλο μέρος του χρόνου. Παρά το γεγονός της προσπάθειας για επιτάχυνση της διαδικασίας συλλογής αδύναμων ή μοναδικών IVs(Inialization Vectors), δυστυχώς θα ανιχνεύεται κίνηση μέσα στο δίκτυο δημιουργώντας επιπλέον πακέτα. Συχνά αυτό

ολοκληρώνεται με την συλλογή ενός ή περισσοτέρων Address Resolution Protocol (ARP) πακέτων και την αναμετάδοσή τους στο σημείο πρόσβασης. Τα πακέτα ARP είναι μια καλή επιλογή καθώς έχουν ένα προκαθορισμένο μέγεθος (28 bytes). Η απάντηση θα δημιουργήσει κίνηση και θα αυξήσει την ταχύτητα συλλογής των πακέτων.

Πρόβλημα μπορεί να παρουσιαστεί συλλέγοντας το αρχικό πακέτο ARP. Πρέπει να περιμένουμε να δημιουργηθεί ένα νομιμοποιημένο ARP πακέτο στο δίκτυο ή μπορούμε να εμποδίσουμε την δημιουργία ενός ARPπακέτου. Ωστόσο τα ARP πακέτα νομιμοποιούνται και μεταφέρονται κάτω από πολλές διαδικασίες. Μια από τις πιο συνηθισμένες είναι κατά την διάρκεια της επικύρωσης. Αντί να περιμένουμε για την επικύρωση, αν ένας πελάτης έχει ήδη επικυρωθεί στο δίκτυο, εμείς μπορούμε να του στείλουμε ένα μη επικυρωμένο πλαίσιο έτσι ώστε ο πελάτης να απαντήσει με ένα πλαίσιο επανεπικύρωσης. Σύντομα η διαδικασία αυτή θα δημιουργήσει ένα πακέτο ARP. Μετά από την συλλογή ένα ή περισσότερων ARP πακέτων, μπορούν να μεταδοθούν στο δίκτυο, έως ότου δημιουργηθούν αρκετά πακέτα ώστε να παράγουν τον απαιτούμενο αριθμό μοναδικών IVs.

Οι μέθοδοι επίθεσης σε κρυπτογραφημένα με WEP δίκτυα είναι δυο ειδών. Η μια μέθοδος απαιτεί την συλλογή αδύναμωνIVs, ενώ η άλλη μέθοδος απαιτεί την συλλογή μοναδικών IVs. Δυστυχώς όποια μέθοδο και να χρησιμοποιήσουμε, απαιτείται η συλλογή ενός μεγάλου αριθμού κρυπτογραφημένων πακέτων με WEP.

3.5 MAC Address Spoofing

Η επίθεση MAC Address Spoofing είναι ένα πολύ δυνατό εργαλείο το οποίο χρησιμοποιείται αρκετά συχνά για το σπάσιμο ενός δικτύου ή ακόμη και σε δοκιμές διείσδυσης σε κάποιο δίκτυο. Παρακάτω θα αναφερθούμε τι είναι το Mac Address Spoofing, για ποιο λόγο το χρησιμοποιούν οι άνθρωποι, πως λειτουργεί, τι οφέλη μπορεί να μας προσφέρει και πώς να το αποφύγουμε.

Κάθε ελεγκτής δικτύου (NIC) έχει μια μοναδική MACδιεύθυνση (Media Access Control) από τον κατασκευαστή. Όταν έχουμε ένα τοπικό δίκτυο, οι υπολογιστές ανταλλάσσουν τις MACδιευθύνσεις τους για να μπορούν να αναγνωρίζουν ο ένας τον άλλον. Ποιες είναι οι ομοιότητες και οι διαφορές μεταξύ μιας MACκαι μιας

IPδιεύθυνσης; Και οι δυο διευθύνσεις αναγνωρίζουν από που προέρχεται και από πού κατευθύνεται ένα πλαίσιο. Μια IP διεύθυνση ωστόσο μπορεί εύκολα να εκχωρηθεί και σε πολλές περιπτώσεις υπάρχει και σε άλλες μηχανές. Ενώ η διεύθυνση MAC είναι μια διεύθυνση υλικού και είναι μόνιμη υποθετικά ακολουθώντας τον ελεγκτή διασύνδεσης δικτύου όπου και αν πάει.

Το MAC address Spoofing είναι υποκλοπή ταυτότητας είτε για καλούς είτε για κακούς σκοπούς και είναι εύκολο σχετικά. Αναφέρεται στην αλλοίωση της MACδιεύθυνσης σε μια NIC κάρτα. Το συγκεκριμένο είδος επίθεσης αποσκοπεί όχι μόνο για μη νόμιμους λόγους όπως είναι η υποκλοπή της ταυτότητας ενός υπολογιστή αλλά και για νόμιμους σκοπούς όπως την δημιουργία ασύρματων συνδέσεων. Ένα παράδειγμα παράνομης χρήσης του MAC Address Spoofing είναι όταν ένας «κακόβουλος» χρήστης αλλάζει την διεύθυνση MACτου υπολογιστή του για να μπορέσει να εισβάλει σε ένα οποιοδήποτε δίκτυο που έχει βάλει στόχο ως εξουσιοδοτημένος χρήστης. Από την άλλη, ένα παράδειγμα νόμιμης χρήσης αυτού είναι η αλλαγή της λειτουργίας ενός υπολογιστή μόνο από τον δρομολογητή στον υπολογιστή και πάλι πίσω.

Έχοντας υπόψη όλα τα παραπάνω, καλό θα ήταν να συμμετέχουμε στην πρόληψη των επιθέσεων MAC. Μία λύση είναι να εντοπίζουμε το MAC Address Spoofing και μια άλλη είναι να μετατρέπουμε το σύστημα σε πιο ανθεκτικό, στα περιορισμένα μηχανήματα ή στα σημεία πρόσβασης. Ένας ταχύς τρόπος για να εντοπίσουμε κάποια ύποπτη διεύθυνση MACείναι να τρέξουμε εις βάρος του το πρωτόκολλο RARP (Reverse Address Resolution Protocol). Το πρωτόκολλο αυτό χαρτογραφεί μια MACδιεύθυνση σε σχέση με την IP διεύθυνση. Μόνο μια διεύθυνση MAC θα πρέπει να χαρτογραφείται σε μια μοναδική διεύθυνσηIP. Το πρωτόκολλο RARP πρέπει να επιστρέφει μια IP διεύθυνση για κάθε συσκευή δικτύου. Εάν επιστρέφονται όλο και πιο πολλές ερμηνεύεται ότι μια από αυτές περιέχει και στοιχεία που θα πρέπει μας κατευθύνουν σε μια «βαθύτερη» έρευνα.

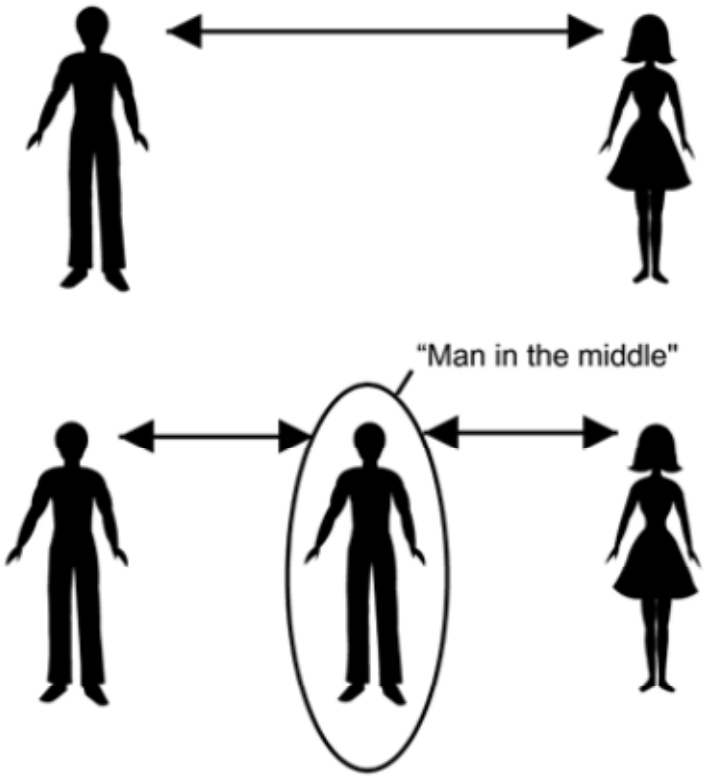
3.6 Sniffing

Ένας sniffer είναι ένα πρόγραμμα ή μια συσκευή που παρακολουθεί όλες τις πληροφορίες που περνούν μέσα από ένα δίκτυο υπολογιστών. Δίνει στον «εισβολέα» μια ολοκληρωμένη εικόνα(IP διευθύνσεις, τοπολογία δικτύου) των δεδομένων που στέλνονται και λαμβάνονται από έναν υπολογιστή ή ένα δίκτυο που παρακολουθείται. Δηλαδή ελέγχει τα δεδομένα που διαπερνούν το καλώδιο ενός δικτύου και μαθαίνει τον προορισμό τους, από πού προέρχονται αυτά τα δεδομένα και τι ακριβώς είναι. Εκτός από τις βασικές λειτουργίες, οι sniffers πιθανότατα να έχουν επιπρόσθετα χαρακτηριστικά όπως το να φιλτράρουν ένα συγκεκριμένο είδος δεδομένων, να συλλαμβάνουν κωδικούς (passwords), usernamesκαι άλλα. Αρκετοί sniffers μπορούν να φτιάξουν από την αρχή αρχεία που στέλνονται κατά μήκος του δικτύου όπως για παράδειγμα μια σελίδα Webή ένα e-mail. Με βάση τις πληροφορίες αυτές, ένας «εισβολέας» μπορεί να έχει μια πλήρη εικόνα των δεδομένων που κυκλοφορούν στο δίκτυο και έτσι να αποκτήσει τον πλήρη έλεγχο του δικτύου.

3.7 Man in the middle Attack

Η επίθεσηMan in the middle attack είναι μια κοινή παραβίαση ασφάλειας σε τοπικά ασύρματα δίκτυα. Ο hackerπαρεμποδίζει μια νόμιμη επικοινωνία μεταξύ δυο πλευρών, τα οποία ενδέχεται να είναι φιλικά μεταξύ τους. Στη συνέχεια, ο «εισβολέας» ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να παραποιήσει πληροφορίες που στέλνονται από τον ένα χρήστη στον άλλο.

Για παράδειγμα, ας υποθέσουμε ότι δυο άτομα επικοινωνούν και ονομάζονται BobκαιAlice. Ο Bob λαμβάνει μηνύματα από την Alice και αυτή αντίστοιχα από τονBob. Ας θεωρήσουμε, ότι υπάρχει ένας επιτιθέμενος χρήστης ο οποίος μπορεί να παρακολουθεί και να διακόπτει την συνομιλία. Ο εισβολέας μπορεί να στέλνει μηνύματα στην Alice μιμούμενος τον Bob, είτε να στέλνει στον Bob μιμούμενος την Alice. Έτσι μπορούμε να πούμε ότι η Alice και οBob έπεσαν θύματα της Man in the middle attack επίθεσης όπως δείχνει το παρακάτω σχήμα.



Εικόνα 4: Παράδειγμα της επίθεσης Man in the middle attack

Για να παραποιηθεί ένα μήνυμα, υπάρχουν τουλάχιστον δυο τρόποι: είτε τροποποίηση του μηνύματος όταν αυτό βρίσκεται στον αέρα είτε το μήνυμα να ληφθεί, να παραποιηθεί και να σταλεί ξανά(γνωστή ως αποθήκευση και προώθηση). Η αλλαγή του μηνύματος στον αέρα είναι αρκετά δύσκολη διότι χρειάζεται η μετάδοση των σημάτων να σταλεί ακριβώς την κατάλληλη στιγμή ώστε να πετύχει τον σκοπό του και να ερμηνευτεί από τον δέκτη λάθος το μήνυμα. Σύμφωνα με την εξελιγμένη διαμόρφωση που χρησιμοποιείται στα ασύρματα δίκτυα, τα bitsπου στέλνονται δεν είναι μεμονωμένα αλλά στέλνονται μαζί κωδικοποιημένα σε ομάδες, γεγονός που κάνει την αλλαγή αρκετά δύσκολη.

Παρακάτω θα αναλύσουμε πως ένας κακόβουλος χρήστης θα μπορούσε να πραγματοποιήσει μια επίθεση Man in the middle attack στο ασύρματο δίκτυο μας. Υπάρχουν δυο διαφορετικές μέθοδοι για να γίνει μια επίθεση Man in the middle σε ένα ασύρματο δίκτυο. Η πρώτη μέθοδος αναφέρεται στην χρησιμοποίηση πλαισίων

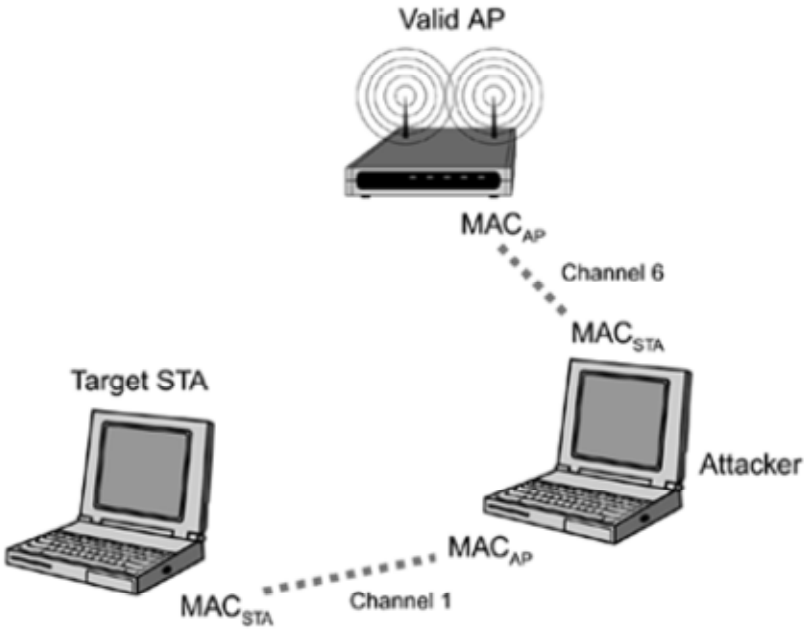
διαχείρισης και είναι συγκεκριμένος για την ασύρματη δικτύωση και η δεύτερη μέθοδος είναι ARP spoofing, η οποία είναι ένα ακόμη πρόβλημα για δίκτυα με συνδεδεμένο καλώδιο

3.7.1 Πλαίσια διαχείρισης

Αφού τα πλαίσια διαχείρισης στερούνται οποιαδήποτε προστασία ακεραιότητας, η εγκαθίδρυση μιας man in the middle επίθεσης στα δίκτυα IEEE 802.11 δεν είναι δύσκολη. Οι συγκεκριμένες επιθέσεις μπορούν να καθιερωθούν ανεξαρτήτως οποιασδήποτε προστασίας (WAP, VPN) και αν χρησιμοποιούμε, αλλά δεν αποτελούν απαραίτητα απειλή εφόσον το πρωτόκολλο ασφαλείας έχει ισχύ. Οι man in the middle attack γίνονται επειδή δεν υπάρχει καμία εγγύηση ακεραιότητας στο στρώμα των συνδέσεων και οι MACδιευθύνσεις πιστοποιούνται εύκολα.

Η επίθεση ξεκινά από τον επιτιθέμενο που μοιράζει ένα μήνυμα τέλους επικύρωσης στο σταθμό-στόχο (υποθέτουμε ότι ο σταθμός-στόχος έχει συνδεθεί ήδη σε ένα AP). Αυτό αναγκάζει το σταθμό να φτάσει στο τέρμα την σύνδεσή του με το τρέχον σημείο πρόσβασης του και να μπορέσει να επανασυνδεθεί με ένα άλλο σημείο πρόσβασης (πιθανότατα παλαιό). Επιπρόσθετα, ο εισβολέας τοποθετεί ένα κακόβουλο AP με το ίδιο ESSID και την ίδια MAC διεύθυνση ως σημείο πρόσβασης, μέσα στο εύρος του εισβολέα αλλά σε ένα διαφορετικό κανάλι από το σωστό AP.

Εκείνη τη στιγμή ο σταθμός-στόχος συνδέεται με το ψευδές AP του εισβολέα καθώς το έγκυρο AP του δεν συνδέεται με την υπηρεσία εξαιτίας των αλλοιωμένων μηνυμάτων τέλους επικύρωσης του εισβολέα. Όταν ο σταθμός συνδεθεί με το ψευδές AP, το συγκεκριμένο AP συνδέεται αμέσως με το έγκυρο AP και αρχίζει να μεταδίδει όλη την κυκλοφορία μέχρι να ολοκληρωθεί η επικύρωση, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 5: Επίθεση man in the middle attack

Ο εισβολέας έχει πλέον τον πλήρη έλεγχο του ρεύματος κυκλοφορίας μεταξύ του έγκυρου σημείου πρόσβασης και του σταθμού. Εφόσον δεν χρησιμοποιείται κρυπτογράφηση, τα πακέτα μπορούν να καθυστερήσουν ή να αμφισβητηθούν. Ακόμη μπορούν να αλλαχθούν για να βοηθήσουν και σε άλλες επιθέσεις.

3.7.2 ARP Spoofing

Η πλαστογράφηση των πακέτων ARP (Address Resolution Protocol) ή αλλιώς ARP Spoofing ήταν κάποτε μια αρκετά μεγάλη απειλή για τα συνδεδεμένα δίκτυα με καλώδιο. Ενώ υπάρχουν κάποια διαθέσιμα εργαλεία για να εμποδίσουν και να προσδιορίσουν τις επιθέσεις ARP, μια επίθεση ARP μπορεί να είναι επιτυχής σε πολλές των περιπτώσεων. Για μια δεδομένη IPδιεύθυνση, το πακέτο ARP προσδιορίζει τη MAC διεύθυνση.

Όταν ένας πελάτης ή ένας σταθμός που θέλει να έρθει σε επαφή με μια συγκεκριμένη IP διεύθυνση εκδίδει ένα ARP αίτημα ως πακέτο ευρείας μετάδοσης στο LAN ζητώντας να μάθει την MACδιεύθυνση της συγκεκριμένης IP διεύθυνσης. Ο οποιοσδήποτε, ακόμη και εισβολείς που θα μπορέσουν να αποκτήσουν πρόσβαση στο

LAN, μπορεί να γεμίσουν με κακόβουλες και μη ακριβείς πληροφορίες, καταστρέφοντας αποτελεσματικά την ARP μνήμη του αιτούντος, διότι τα ARPπακέτα δεν έχουν καμία προστασία ακεραιότητας. Συνεπώς, από εκείνο το σημείο μέχρι τη στιγμή που μια είσοδος κρυφής μνήμης τελειώσει, ο πελάτης χρησιμοποιεί μια λαθεμένη MACδιεύθυνση για τη δεδομένη IP διεύθυνση, που έχει ως αποτέλεσμα ολόκληρη η κυκλοφορία να καταλήγει στον κακόβουλο χρήστη παρά στον πραγματικό λήπτη.

3.7.3 Μορφές επιθέσεων

Οι συγκεκριμένες επιθέσεις έχουν δυο κοινές μορφές:

- ο κακόβουλος χρήστης είτε κρυφακούει
- είτε παραποιεί τα μηνύματα

Σύμφωνα με την πρώτη μορφή επίθεσης, ο hacker ακούει ένα σύνολο μεταδόσεων από και σε διαφορετικά επίπεδα ακόμη και αν ο υπολογιστής του επιτιθέμενου χρήστη δεν λαμβάνει μέρος στη συνδιάλεξη. Αρκετοί ταυτίζουν τον συγκεκριμένο τύπο επίθεσης με διαρροή, σύμφωνα με την οποία ευαίσθητες πληροφορίες μπορούν να αποκαλυφθούν σε έναν τρίτο, χωρίς να το γνωρίζουν οι νόμιμοι χρήστες.

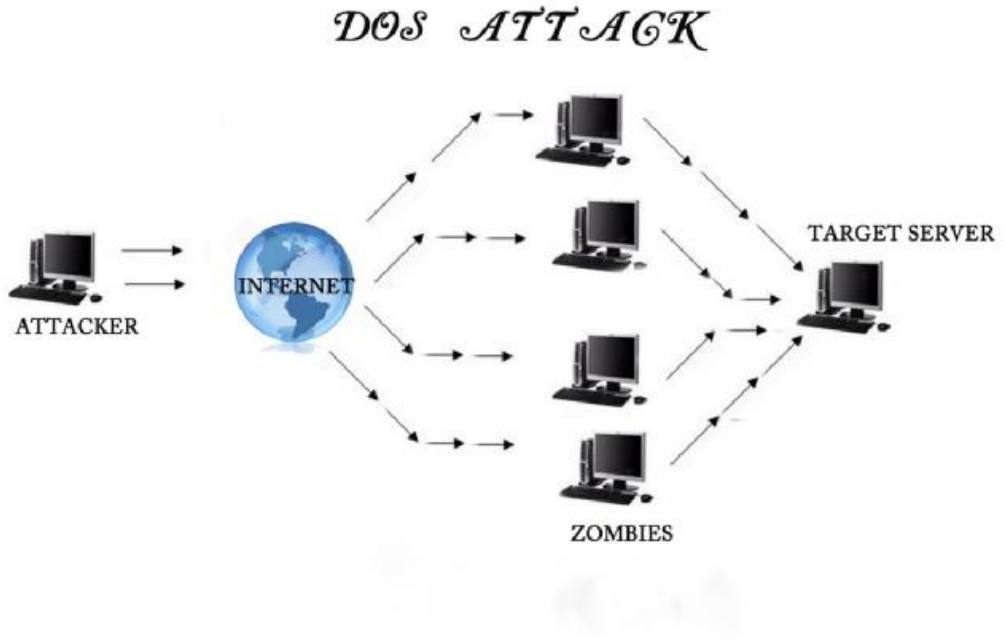
Οι επιθέσεις κατά τις οποίες γίνεται παραποίηση του μηνύματος βασίζονται στην ικανότητα του εισβολέα να κρυφακούει. Ο εισβολέας παίρνει αυτή την μη εξουσιοδοτημένη απόκριση, ένα ρεύμα δεδομένων (data stream), τροποποιώντας τα περιεχόμενα έτσι ώστε να ικανοποιούν ένα συγκεκριμένο σκοπό, πιθανότατα χρησιμοποιώντας ψεύτικη IP διεύθυνση, μετατρέποντας την MAC διεύθυνση ή με το να κάνει κάποιες άλλες τροποποιήσεις.

3.8 Denial of Services

Οι επιθέσεις denial of service είναι ο γνωστότερος τύπος επιθέσεων ακόμη και στα ενσύρματα δίκτυα και αρκετά δύσκολος για να αντιμετωπιστεί. Ο όρος denial of

service δηλώνει την άρνηση μιας υπηρεσίας ή ενός υπολογιστικού πόρου να εξυπηρετεί τους πελάτες του. Πρόκειται για μια επίθεση η οποία είναι ικανή να αναστείλει οριστικά την λειτουργία ακόμη και ενός ολόκληρου δικτύου ή να την σταματήσει εντελώς λόγω υπερφόρτωσης του έναντι των πελατών του.

Αυτό μπορεί να συμβεί για πολλούς λόγους. Ο πιο συνήθης λόγος είναι για να μπορέσει η μη καλή λειτουργία του δικτύου να αποτελέσει μέσο για μια από τις επιθέσεις που προαναφέρθηκαν, αλλά σε κάποιες περιπτώσεις μπορεί να αποτέλεσμα της προσπάθειας ενός κακόβουλου χρήστη, ο οποίος μετά από πολλές προσπάθειες δεν κατάφερε να αποκτήσει πρόσβαση σε αυτό. Πέρα από αυτό όμως, υπάρχει πάντα μια πιθανότητα πολιτικοί λόγοι ή θέματα επαγγελματικού ανταγωνισμού να είναι η αιτία για να εξαπολύσει κάποιος μια denial of service επίθεση. Αυτό που πρέπει να σημειωθεί, είναι ότι οι επιθέσεις αυτές στα ασύρματα δίκτυα δεν μπορούν για κανένα λόγο να αντιμετωπιστούν, λόγω της φύσης των δικτύων. Ο σοβαρότερος τρόπος αντιμετώπισής τους είναι με εφαρμογή Intruction Detection Systems (IDS) τα οποία μπορούν να αρκεστούν στην άμεση ειδοποίηση του διαχειριστή του δικτύου. Το σχήμα παρακάτω μας δείχνει πως είναι μια επίθεση denial of service.



Εικόνα 6: Απεικόνιση της DOS επίθεσης

3.8.1 Κατηγορίες Dos επιθέσεων

Οι denial of service επιθέσεις που εφαρμόζονται στα ασύρματα δίκτυα διακρίνονται σε τέσσερις κατηγορίες.

Η πρώτη κατηγορία είναι εκείνη της επίθεσης στο φυσικό επίπεδο, το ***jamming***. Η τεχνική αυτή βασίζεται στο θόρυβο και στις παρεμβολές που δημιουργούν ορισμένες συσκευές όπως είναι για παράδειγμα οι φούρνοι μικροκυμάτων, τα κινητά τηλέφωνα, οι συσκευές Bluetooth και γενικά οι ηλεκτρικές συσκευές που μπορούν να λειτουργήσουν στο φάσμα των 2,4 GHz. Το αποτέλεσμα από αυτές τις επιθέσεις δεν είναι απαραίτητα κακό γιατί κατά κύριο λόγο δεν γίνεται με πρόθεση αλλά παραμένει σοβαρό διότι είναι ικανό να οδηγήσει το δίκτυο σε δυσλειτουργία και σε προβληματική χρήση αυτού με αρκετές διακοπές και αποτυχίες.

Η δεύτερη κατηγορία έχει να κάνει με την μαζική εκπομπή deassociation και deauthentication frames. Έτσι δημιουργείται το φαινόμενο της πλημμύρας. Στη διάρκεια αυτής της επίθεσης, ο εισβολέας αποστέλλει όσα περισσότερα πακέτα deassociation και deauthentication προς το εκάστοτε AP έχοντας ως αποτέλεσμα κάνει αυτό αποσύνδεση τους χρήστες που «υποτίθεται» πως έχουν κάνει αυτές τις αιτήσεις για να αποσυνδεθούν. Αυτό το μέτρο είναι καλό, για να καταφέρει ο εισβολέας να εφαρμόσει τεχνικές spoofing και να παριστάνει την ταυτότητα του χρήστη που αποσυνδέθηκε.

Η τρίτη κατηγορία είναι μια παρόμοια τεχνική με αυτή του authentication frame attack. Στην συγκεκριμένη περίπτωση ο εισβολέας στέλνει authentication πακέτα στο AP με τροποποιημένο περιεχόμενο έτσι ώστε να θεωρήσει την προσπάθεια του υποτιθέμενου χρήστη που έστειλε το αίτημα αποτυχημένη και απαντήσει αρνητικά μη επιτρέποντας τον χρήστη να μπει στο δίκτυο, χωρίς να καταλάβει ο νόμιμος χρήστης το γιατί. Έπειτα ο επιτιθέμενος μπορεί να πλαστογραφήσει την διεύθυνση MAC του και να συνδεθεί στο δίκτυο.

Τελευταία κατηγορία που πρέπει να αναφερθεί είναι η τεχνική buffer over flow. Οι επιθέσεις denial of service συχνά παρομοιάζονται με την τεχνική αυτή. Με την αποστολή πολλών πακέτων προς τα AP, οι buffers του κάθε AP ξεπερνούν αρκετά το όριο με αποτέλεσμα το AP να οδηγείται σε κατάρρευση. Αυτό προσπαθούν και πολλοί εισβολείς που εξαπολύουν τέτοιου είδους επιθέσεις, για να μπορέσουν στη συνέχεια να εφαρμόσουν τις man in the middle πρακτικές τους.

ΚΕΦΑΛΑΙΟ 4^{ο} : ΑΝΑΛΥΣΗ ΚΑΙ ΑΠΟΤΥΠΩΣΗ ΤΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ WEP, WPA, WPA2, 802.11i, 802.11x

4.1 Βασικές αρχές ασφάλειας

Όπως αναφέραμε και πιο πάνω στις μέρες μας βασική αρχή στις ασύρματες επικοινωνίες βασισμένες στο 802.11 είναι η ασφάλεια. Πριν λοιπόν αναλύσουμε τις τεχνολογίες για την ασφάλεια των ασυρμάτων δικτύων αποφασίσαμε πως ορθό θα ήταν να αναλύσουμε σύντομα κάποιες έννοιες που ισχύουν και εφαρμόζονται παντού και πάντα όταν αναφερόμαστε στο θέμα της ασφάλειας υπολογιστικών συστημάτων.

Αναλυτικότερα, παρακάτω θα δοθεί μια σύντομη περιγραφή των εννοιών του **confidentiality**, του **integrity**, του **availability**, του **privacy**, του **authentication** και του **authorization**. Οι έννοιες αυτές είναι γενικές και εφαρμόζονται σε όλα τα δίκτυα υπολογιστών ανεξαρτήτως αρχιτεκτονικής και πρωτοκόλλων.

4.2 Confidentiality

Η αρχή του **confidentiality** (εμπιστευτικότητας), άπτεται στην αποτροπή της μη εξουσιοδοτημένης επικοινωνίας χρηστών που επιχειρούν να προσπελάσουν πόρους ενός υπολογιστικού συστήματος, είτε ηθελημένα είτε όχι. Κυρίως η εμπιστευτικότητα αναφέρεται στο φυσικό επίπεδο, όπου στόχος είναι να μην είναι εφικτή η φυσική πρόσβαση στους πόρους ενός συστήματος. Επιδιώκουμε δηλαδή να αποτρέψουμε πιθανές κλοπές εξοπλισμού ή μη εξουσιοδοτημένης χρήσης αυτού, από χρήστες που είτε δεν τους γνωρίζουμε είτε απλά δε μπορούμε να τους εμπιστευτούμε. Εμπιστευτικότητα όμως πρέπει να υπάρχει και σε επίπεδο δικτύου, όπου τα ηλεκτρικά σήματα δεν πρέπει να είναι εφικτό να αναγνωστούν και να επεξεργαστούν από οποιονδήποτε κακόβουλο χρήστη. Βέβαια κάτι τέτοιο είναι σχεδόν αδύνατο στις μέρες μας όπου λιγότερο πολύπλοκοι μηχανισμοί και εργαλεία αναπτύσσονται με αποτέλεσμα ο οποιοσδήποτε θέλει να μπορεί να έχει κάποιου είδους και μέχρι

κάποιου βαθμού εποπτεία του τι γίνεται σε ένα δίκτυο και χωρίς μάλιστα αναγκαστικά να έχει όλες τις τεχνικές γνώσεις.

Αυτή η αρχή βέβαια είναι επόμενο, από την ίδια την φύση των ασύρματων δικτύων, ότι δε μπορεί με κανένα τρόπο να διατηρείται. Το φυσικό μέρος της επικοινωνίας σε τέτοια δίκτυα δεν είναι κάποιο καλώδιο, αλλά ο αέρας και κανένας δε μπορεί να απαγορέψει από τον οποιοδήποτε να τον χρησιμοποιεί με όποιον τρόπο αυτός θέλει. Σε αντίθεση με τα ενσύρματα δίκτυα, δεν είναι απαραίτητο ένα καλώδιο δικτύου, ένα σημείο πρόσβασης στο INTEPNET ή ακόμα ακόμα και το ίδιο το ηλεκτρικό ρεύμα, για να μπορέσει ένας χρήστης να αποκτήσει τη δυνατότητα για πρόσβαση σε κάποιο δίκτυο. Τα πράγματα στον ασύρματο κόσμο είναι πιο απλά και δυστυχώς επικίνδυνα. Οι λύσεις που συχνά προτείνονται σε αυτό το επίπεδο και καλούνται οι διαχειριστές τέτοιων δικτύων να υλοποιήσουν έχουν να κάνουν κυρίως με τη διασπορά του σήματος στο χώρο και τον περιορισμό του με τη χρήση κατευθυντικών συνδέσεων. Το μέτρο βέβαια αυτό δεν μπορεί να θεωρηθεί επαρκές αφού ποτέ δε θα μπορέσει το σήμα να περιοριστεί τόσο ώστε μόνο ένας συγκεκριμένος ή κάποιοι συγκεκριμένοι να μπορούν να το λαμβάνουν, άλλωστε κάτι τέτοιο θα ήταν και ενάντια στα χαρακτηριστικά της ασύρματης επικοινωνίας, αφού αυτή έγκειται στην μη στατικότητα των χρηστών. Ένα επιπλέον μέτρο και ίσως πιο ουσιώδες, που συχνά χρησιμοποιείται είναι η κρυπτογράφηση των δεδομένων. Οι προσπάθειες που έχουν γίνει προς αυτή την κατεύθυνση έχουν να κάνουν κυρίως με τον RC4 αλγόριθμο και το WEP πρωτόκολλο που αρχικά προτάθηκε ως μια λύση κρυπτογράφησης αλλά και την χρήση ασφαλών καναλιών επικοινωνίας μέσω του πρωτοκόλλου SSL.

4.3 Integrity

Η αρχή του **integrity** (ακεραιότητα) έχει να κάνει με την προσπάθεια να παραμένουν τα ανταλλασσόμενα δεδομένα ακέραια και αξιόπιστα. Σκοπός δηλαδή είναι η αποφυγή λαθών κατά τη μετάδοση κάποιων πακέτων δεδομένων και η πιθανή διόρθωση τέτοιων λαθών. Για να επιτευχθεί αυτό, έχει κατά καιρούς χρησιμοποιηθεί η ιδέα του checksum. Το checksum δεν είναι τίποτα παραπάνω από την εφαρμογή κάποιων προσθετικών ή modulo-n συναρτήσεων στο εκπεμπόμενο και λαμβανόμενο μήνυμα ενός χρήστη προς κάποιον άλλο. Ο έλεγχος αυτός είναι κυκλικός (δηλαδή

στον παραλήπτη εφαρμόζεται η συμπληρωματική συνάρτηση αυτής που εφαρμόζεται στον πομπό) και για αυτό τέτοιοι αλγόριθμοι ονομάζονται CRC (Cyclic Redundancy Checks). Αυτοί οι μέθοδοι ανίχνευσης λαθών είναι γνωστοί από πολύ παλιά, γι' αυτό πλέον δε μπορούν να θεωρούνται αρκετά ασφαλείς και παρακάτω εξηγείται το γιατί.

Αν κάποιος γνωρίζει εκ των προτέρων ένα συγκεκριμένο σύνολο από χαρακτήρες προς αποστολή, μπορεί να αλλάξει τα περιεχόμενα της πληροφορίας αυτής και να ολοκληρώσει την αποστολή κάνοντας μάλιστα χρήση ενός έγκυρου checksum. Ο παραλήπτης δε θα γνωρίζει ότι υπήρξε αυτού του είδους διαμεσολάβηση και επομένως θα έχει παραβιαστεί η αρχή της ακεραιότητας.

Η λύση σε τέτοιου είδους προβλήματα είναι και πάλι η ισχυρότερη κρυπτογράφηση κάνοντας χρήση μερικών από τους πιο γνωστούς αλγορίθμους όπως ο **MD5** και ο **RC4**.

4.4 Availability

Η αρχή του **availability** (διαθεσιμότητα) έχει να κάνει με την ανάγκη για αξιόπιστη και πάντα διαθέσιμη προς χρήση πληροφορία. Η ίδια ανάγκη βέβαια αφορά και τους υπολογιστικούς πόρους ενός συστήματος. Το σημαντικό στην παραπάνω αρχή είναι η απρόσκοπτη και σε συνεχή μήκος χρόνου διαθεσιμότητα της πληροφορίας. Η ανάγκη αυτή υπήρξε πάντα ένα ζητούμενο και αυτή η ανάγκη ακριβώς ήταν τελικά που οδήγησε στη του INTEPNET.

Το ζήτημα της διαθεσιμότητας τίθεται στα ασύρματα δίκτυα με τη μορφή της συμβατότητας των διαφορετικών συσκευών και της δυνατότητας επικοινωνίας μεταξύ τους. Αρχικά και μέχρι την προτυποποίηση του Wi-Fi, οι διάφοροι κατασκευαστές δικτυακού εξοπλισμού καθόριζαν διαφορετικά πρότυπα επικοινωνίας με αποτέλεσμα να μην μπορούν να επιτύχουν επικοινωνία με συσκευές διαφορετικού κατασκευαστή. Ευτυχώς αυτό το ζήτημα πλέον δεν τίθεται. Το ζητούμενο που μένει ακόμα να λυθεί στα 802.11 βασισμένα δίκτυα, είναι το πρόβλημα του κρυμμένου κόμβου, που δημιουργεί προβλήματα ασταθούς πρόσβασης και επικοινωνίας μεταξύ των χρηστών.

Ο τρόπος που σχετίζεται το availability με την ασφάλεια έχει να κάνει με το κατά πόσο ένας χρήστης του δικτύου μπορεί να διακόψει τη σωστή και απρόσκοπτη

λειτουργία μιας υπηρεσίας ή και ολόκληρου του δικτύου. Μια επίθεση από τη μεριά ενός κακόβουλου χρήστη – όπως για παράδειγμα μια Denial of Service επίθεση – μπορεί να αποτελέσει πλήγμα για την διαθεσιμότητα του δικτύου. Στο αρχικό **ARPANET** μια τέτοια επίθεση ήταν αδιανόητη αφού όλοι οι χρήστες θεωρούνταν νόμιμοι και «καλοπροαίρετοι» χρήστες του δικτύου. Η σύγχρονη όμως πραγματικότητα άλλαξε αυτά τα δεδομένα και σε ένα χώρο όπως το INTERNET, κανένας χρήστης δε μπορεί να θεωρηθεί καλοπροαίρετος. Η ίδια εσφαλμένη λογική επικράτησε αρχικά και στα ασύρματα δίκτυα. Γρήγορα όμως φάνηκε ότι «ο αέρας ανήκει σε όλους» και οποιοσδήποτε το επιθυμούσε θα μπορούσε να βλάψει την διαθεσιμότητα ενός ασύρματου δικτύου.

4.5 Privacy

Η αρχή του **privacy** (ιδιωτικότητας) είναι ίσως το συνώνυμο της ασφάλειας, τουλάχιστον ως προς το πώς αντιλαμβάνεται ο περισσότερος κόσμος την ασφάλεια. Η αρχή αυτή έχει να κάνει με την εξασφάλιση του απορρήτου της επικοινωνίας μεταξύ των χρηστών. Η πληροφορία κατά τη μετάδοση της είναι κρίσιμο να μένει ασφαλής και προστατευμένη από οποιεσδήποτε αλλαγές αλλά και από κακόβουλα «βλέμματα». Δεν είναι αρκετό να μην είναι μπορεί κάποιος να αλλάξει το περιεχόμενο της πληροφορίας – μιας πληροφορίας που μπορεί να περιέχει και ευαίσθητα προσωπικά δεδομένα – πρέπει να μην μπορεί και να «διαβάσει» αυτή την ίδια πληροφορία.

Η λύση και σε αυτό το ζήτημα έγκειται και πάλι στην αυξημένη κωδικοποίηση των μεταδιδόμενων σημάτων. Ίσως μάλιστα σε αυτή την περίπτωση να είναι και πιο σημαντική και ουσιαστική αυτή η ανάγκη για προηγμένες μεθόδους κρυπτογράφησης των δεδομένων.

4.6 Authentication

Το **authentication** (πιστοποίηση) είναι η διαδικασία εκείνη που εξασφαλίζει τόσο στον πομπό όσο και στον παραλήπτη ότι ο ένας για τον άλλον είναι ο κατάλληλος για να επιτευχθεί μια επιτυχής και ασφαλής επικοινωνία. Με χρήση ορισμένων τεχνικών,

πιστοποιούνται οι χρήστες και μετά από τη σχετική διαδικασία, είναι γνωστή πλέον η πραγματική ταυτότητα του καθενός. Το κατά πόσο αυτή η ταυτότητα που δηλώνεται, είναι και η αληθινή είναι το ζήτημα που χρήζει εξέτασης υπό το πρίσμα της ασφάλειας των δεδομένων και της εν γένει επικοινωνίας. Στην όλη διαδικασία, η εμπιστοσύνη που δείχνουν οι χρήστες απέναντι στις χρησιμοποιούμενες τεχνικές, είναι το σημείο κλειδί ώστε να θεωρηθεί αξιόπιστη και επιτυχημένη η όποια τεχνική πιστοποίησης.
Τέτοιες τεχνικές υπάρχουν πολλές και στο πέρασμα των χρόνων έχουν αποτελέσει τον ακρογωνιαίο λίθο στα ζητήματα ασφάλειας και στην εμπιστοσύνη που δείχνουν οι χρήστες σε ένα σύστημα ή ένα δίκτυο. Η πιο γνωστή και πάντα αξεπέραστη τεχνική είναι εκείνη του διαμοιραζόμενου password ή κλειδιού (shared password or key). Ένας μυστικός κωδικός είναι απαραίτητος σε κάθε χρήστη ώστε να πιστοποιεί έναντι του συστήματος την ταυτότητα του. Βέβαια η τεχνική αυτή από μόνη της, δε μπορεί να αποτελέσει πανάκεια ασφάλειας. Είναι ολόκληρος ο μηχανισμός διαχείρισης τέτοιων password ή και κλειδιών που κάνει μια φόρμα πιστοποίησης, αξιόπιστη ή όχι.

Τα ζητήματα ασφάλειας που καλείται να αντιμετωπίσει συνήθως ένας διαχειριστής στο επίπεδο του authentication έχουν να κάνουν όχι μόνο με το μηχανισμό και τον αλγόριθμο πιστοποίησης, αλλά και με το ίδιο το κανάλι επικοινωνίας πάνω από το οποίο γίνεται η όλη διαδικασία ανταλλαγής passwords, κλειδιών και γενικότερα πληροφορίας.

Στο πεδίο των ασύρματων δικτύων, η διαδικασία του authentication είναι εκεί που επικεντρώνουν οι διάφορες εταιρείες και προμηθευτές την προσοχή τους, ώστε να αντιμετωπίσουν τις τεχνικές ατέλειες του πρωτοκόλλου 802.11b ως προς την ασφάλεια του. Το κύριο λάθος όμως που κάνουν όλες οι γνωστές τεχνικές authentication που έχουν χρησιμοποιηθεί στο 802.11b, είναι ότι κάθε φορά γίνεται πιστοποίηση μεταξύ των συσκευών (πελάτη και server) που αναλαμβάνουν το association και όχι μεταξύ των χρηστών ή των σταθμών εργασίας. Κάποια από τα **EAP** πρωτόκολλα που δημιουργήθηκαν σε αυτή την κατεύθυνση κινήθηκαν όπως και κάποια καινούρια πρότυπα που αναμένονται σύντομα. Πιο σοβαρή λύση authentication φαντάζει ακόμα και στα ασύρματα δίκτυα ο γνωστός και από τα ενσύρματα δίκτυα, RADIUS μηχανισμός πιστοποίησης.

4.7 Authorization

Η αρχή του **authorization** (εξουσιοδότηση) αν και τελευταία στην αναφορά μας, σίγουρα δεν μπορεί και δεν πρέπει να θεωρηθεί λιγότερο σημαντική. Αυτό το λάθος συχνά γίνεται από πολλούς διαχειριστές με αποτέλεσμα να αναιρούν οποιαδήποτε μέτρα ασφαλείας έχουν λάβει σε ανώτερα επίπεδα.

Στην φάση αυτή, αφού ο χρήστης ολοκληρώσει τη διαδικασία πιστοποίησης του, ανατίθενται σε αυτόν τα δικαιώματα που του αναλογούν και του παρέχεται πρόσβαση σε υπηρεσίες και πόρους που του έχουν εκχωρηθεί σύμφωνα με τη συμφωνία/σύμβαση που έχει συνάψει με το σύστημα και τους διαχειριστές του. Στα πρώτα στάδια εξέλιξης των υπολογιστών η λογική του authorization ήταν σχεδόν ανύπαρκτη. Με το πέρασμα των χρόνων όμως και κυρίως με την ανάπτυξη της πλατφόρμας του Unix η λογική αυτή άρχισε να υιοθετείται όλο και συχνότερα, μέχρι που φτάσαμε στη σημερινή κατάσταση, όπου τα επίπεδα ελέγχου πρόσβασης σχεδόν σε κάθε υπολογιστική υπηρεσία είναι αρκετά και άμεσα συσχετισμένα με το περιεχόμενο και τους πόρους.

Στα σύρματα δίκτυα και πάλι, κάτι τέτοιο αρχικά δεν ήταν απαραίτητο, όμως όπως και σε όλα τα παραπάνω στάδια, εξελίχθηκε αργότερα σε αναγκαιότητα που έπρεπε να καλυφθεί και να ιδωθεί κάτω από το πρίσμα της γενικότερης πολιτικής για βελτίωση της ασφάλειας των συστημάτων και των δικτύων. Το πρόβλημα που υπήρχε – και ακόμα υπάρχει – είναι ότι το authorization και πάλι αφορά τις συσκευές και όχι τους χρήστες. Διάφορες τεχνικές που χρησιμοποιούνται, όπως το MAC Filtering, σίγουρα δε μπορούν να θεωρηθούν ούτε αξιόπιστες αλλά και ούτε ικανές να καλύψουν τις ανάγκες για βελτίωση της παρεχόμενης ασφάλειας. Η λύση που φαντάζει η πιο σωστή είναι και πάλι η χρήση **RADIUS**.

4.8 Τεχνολογίες ασύρματων δικτύων υπολογιστών

Όταν σχεδιάστηκε το πρωτόκολλο 802.11 προτεραιότητα του δεν ήταν η ασφάλεια των δεδομένων όσων την χρησιμοποιούσαν αλλά η ανάγκη τους για διασύνδεση. Το ζήτημα της ασφάλειας δεν είχε τεθεί καν αρχικά στον σχεδιασμό του πρωτοκόλλου

αλλά και αργότερα που θεωρήθηκε αναγκαίο και απαραίτητο από τους σχεδιαστές, δεν του δόθηκε η προσοχή που θα έπρεπε.

Η ασφάλεια στα ασύρματα δίκτυα είναι ένα πολύ σοβαρό ζήτημα αφού είναι δύσκολο να περιοριστεί ένας οποιοδήποτε κακόβουλος χρήστης από το να εξαπολύσει ενός οποιουδήποτε είδους επίθεση. Τα είδη των επιθέσεων είναι πολλά και διαφέρουν μεταξύ τους, υπάρχουν δηλαδή ποικίλα είδη που συνήθως δεν μπορούν να αποτελέσουν από μονά τους μια «δυναμική» έτσι ώστε να επιτρέψουν την πρόσβαση σε κάποιον κακόβουλο χρήστη. Έτσι λοιπόν ο επιτιθέμενος, όπως πλέον είναι συνηθισμένο, είναι να χρησιμοποιεί 2 ή και περισσότερες από αυτές τις τεχνικές έτσι ώστε να πετύχει το σκοπό του. Επίσης σε πολλές περιπτώσεις δεν είναι καν αναγκαίο ο εισβολέας να έχει ούτε ιδιαίτερα πολύπλοκες τεχνικές δεξιότητες ούτε καν ιδιαίτερες γνώσεις κάποιας γλώσσας προγραμματισμού για να πετύχει το περιβόητοcrack του δικτύου που έχει στοχεύσει. Η μη γνώση και η απροσεξία, των χρηστών ή των διαχειριστών του ασύρματου δικτύου μπορεί να προκαλέσει από κάποιον τρίτο μεγάλη ζημιά στο δίκτυο τους ή ακόμη και στους ίδιους. Για να σας δώσουμε να καταλάβετε την σημαντικότητα της κατάστασης θα σας αναφέρουμε ένα παράδειγμα για το ποσό εύκολα μπορεί κάποιος να παραβιάσει ένα ασύρματο δίκτυο και μάλιστα να προκαλέσει και τεράστιους μπελάδες στους ιδιοκτήτες.

4.8.1 Παράδειγμα

Ένα από τα πρώτα καταγεγραμμένα περιστατικά παραβίασης ασφάλειας ασύρματων δικτύων, ήταν εκείνο που δημοσιεύτηκε σε μία από τις mailing lists του γνωστού web site **http://www.securityfocus.com** όπου κάποιος χρήστης περιέγραφε την εξής εμπειρία που είχε καθώς καθόταν στο αμάξι στο parking γνωστού καταστήματος εμπορίας υπολογιστών στην Αμερική.

Μόλις είχε βγει από το κατάστημα έχοντας αγοράσει μια καινούρια ασύρματη κάρτα και αφού εγκατέστησε τους οδηγούς της κάρτας (drivers) παρατήρησε ότι τα λαμπάκια που είχε η κάρτα αναβόσβηναν καταδεικνύοντας την ύπαρξη κίνησης κάποιου ασύρματου δικτύου.

Αμέσως μετά, έσπευσε να εκτελέσει το γνωστό network scanner/sniffer πρόγραμμα **KISMET**, και παρατήρησε συνεχή και έντονη κίνηση πακέτων. Αφού κατέγραψε

αρκετά από αυτά, με κάποιο άλλο επίσης γνωστό network analyzer πρόγραμμα όπως το **ETHEREAL**, ανέτρεξε στο να αναλύσει τι είδους πακέτα ήταν αυτά. Προς έκπληξη του διαπίστωσε πως σε clear text μορφή εμφανίζονταν πολλά SQL queries καταδεικνύοντας από το όνομα των πεδίων τους, ότι επρόκειτο για queries που εφαρμόζονταν στη βάση δεδομένων του εν λόγω καταστήματος. Με λίγο περισσότερο ψάξιμο μάλιστα μπόρεσε να βρει και αριθμούς πιστωτικών καρτών και για το λόγο αυτό ενημέρωσε το κατάστημα.
Το θέμα έλαβε μεγάλη έκταση σε εφημερίδες, περιοδικά και σε web sites στο INTERNET, με αποτέλεσμα το εν λόγω κατάστημα να αναγκαστεί να αναστείλει τη λειτουργία των ασύρματων δικτύων που είχε εγκαταστήσει σε περισσότερα από 500 καταστήματα του, προκαλώντας μεγάλη αναταραχή στους πελάτες του, μεγάλη οικονομική ζημιά στο ίδιο και φυσικά ένα τεράστιο πλήγμα στην αξιοπιστία του.

Το παρακάτω παράδειγμα δόθηκε για να γίνει σαφές το πόσο σημαντικό είναι το ζήτημα της ασφάλειας γενικότερα και τι επιπτώσεις μπορεί να έχει. Βέβαια ο κίνδυνος αυτός δεν αφορά μόνο τις εταιρείες που σκέφτονται ή και έχουν ήδη αναπτύξει ασύρματες λύσεις δικτύωσης, αλλά και όλες εκείνες τις **SOHO** (Small Office – Home Office [Μικρό Γραφείο – Μικρό Σπίτι]) εγκαταστάσεις που μπορούν να αφορούν τον καθένα μας.

Στη συνέχεια εξετάζονται οι διάφορες τεχνικές παραβίασης της ασφάλειας ενός 802.11 δικτύου. Πρέπει να επισημάνουμε και πάλι ότι οι περισσότερες από τις τεχνικές αυτές δεν αποτελούν σοβαρό κίνδυνο από μόνες τους αλλά χρειάζεται συνήθως να συνδυαστούν κάποιες από αυτές έτσι ώστε να υπάρξει παραβίαση.

4.9 Ανάλυση της τεχνολογίας WEP

Προβλέποντας τα προβλήματα που θα δημιουργούνταν από τη χρήση ασύρματων δικτύων στον τομέα της ασφάλειας δεδομένων του χρήστη ή της υπηρεσίας, η IEEE αποφάσισε να δημιουργήσει ένα πρωτόκολλο που θα αναλάμβανε το authentication των συσκευών που θα ήθελαν να χρησιμοποιήσουν κάποιο δίκτυο. Η αρχική αυτή λύση ήταν το **WEP** (**Wireless Equivalent Privacy**) πρωτόκολλο που από το όνομα του φαίνεται ότι επιδιώχθηκε να ισοσταθμιστεί η ασφάλεια στα ασύρματα δίκτυα με

εκείνη των ενσύρματων. Φυσικά κάτι τέτοιο ήταν αδύνατο λόγω της φύσης του Wi-Fi. Όμως πολλές φορές ένα όνομα και μόνο είναι αρκετό ώστε να δώσει μια αίσθηση ασφάλειας στους χρήστες για αυτό και τελικά δημιουργήθηκε αυτό το πρωτόκολλο στις προδιαγραφές του Wi-Fi.

Όπως αποδείχθηκε τελικά, στη συνέχεια το WEPήταν μια πρόχειρη και προσωρινή λύση που εφαρμόστηκε για να προσφέρει ένα υποτυπώδες επίπεδο ασφάλειας στους χρήστες έχοντας ως σκοπό να αποτρέψει πολλούς εισβολείς ασχέτους ή μη να εκμεταλλευτούν ένα δίκτυο το οποίο δεν έχει καμία ασφάλεια, ένα ανοιχτό δίκτυο όπως αλλιώς κοινά ονομάζεται. Περνώντας όμως ο καιρός και σχετικά γρήγορα θα μπορούσε να πει κανείς, διαπιστώθηκε πως το WEP απέτυχε να εξασφαλίσει έστω και μια από τις αρχές ασφάλειας.

4.9.1 Εισαγωγή

Ξεκινώντας λοιπόν την πορεία του το 802.11 πρότυπο και για τα 4-5 πρώτα χρόνια της ζωής του είχε μια μόνο ορισμένη μέθοδο για την ασφάλεια του και αυτή ήταν το WEP. Τη χρονιά του 2000 τα WLANS είχαν αυξημένη δημοτικότητα και για αυτό το λόγο η προσοχή των ειδικών στην κρυπτογραφία στράφηκε πάνω τους. Ύστερα από μελέτες ανακαλυφθήκαν αδυναμίες στην προσέγγιση του WEP. Η χρονιά του 2000 τελείωνε και ήδη υπήρχαν στο διαδίκτυο εργαλεία διαθέσιμα με τα οποία κάποιος χρησιμοποιώντας τα μπορούσε αρκετά εύκολα να σπάσει την ασφάλεια του WEP. Οι σχεδιαστές του αρχικούstandard του 802.11 δέχθηκαν σκληρές κρητικές για το WEPκαι τις αδυναμίες του. Πριν όμως βιαστούμε να κριτικάρουμε τους σχεδιαστές ας λάβουμε υπόψιν μας κάποια πράγματα.

Το πρώτο είναι ότι το WEP την περίοδο που σχεδιάστηκε, δεν σκόπευε να παρέχει πολύ υψηλά επίπεδα ασφάλειας. Όπως λέει και το όνομά του, σκόπευε να κάνει τόσο δύσκολη την εισβολή όσο δύσκολο είναι να εισβάλεις σε ένα κτίριο και να συνδεθείς με ένα ενσύρματο δίκτυο, το οποίο δεν είναι αδύνατο.

Πιο συγκεκριμένα στο standard του 1999 περιλαμβάνονται τα εξής σχόλια για το WEP :

I. Παρέχει λογικό επίπεδο ασφάλειας: Η ασφάλεια που παρέχεται από τον αλγόριθμο έγκειται στην δυσκολία να ανακαλύψεις το κρυφό κλειδί με brute-

force επίθεση. Αυτό έχει άμεση σχέση με το μέγεθος του κλειδιού και τη συχνότητα αλλαγής των κλειδιών. Το WEP επιτρέπει την αλλαγή των κλειδιών και τη συχνή αλλαγή του IV (Initialization Vector).

II. Συγχρονίζεται μόνος του: Το WEP είναι αυτοσυγχρονιζόμενο για κάθε μήνυμα, ιδιότητα που είναι ιδιαίτερα σημαντική για έναν αλγόριθμο που χρησιμοποιείται στο data-link υποεπίπεδο, όπου υποτίθεται ότι πρέπει να παρέχεται η καλύτερη δυνατή προσπάθεια παράδοσης και όπου ο ρυθμός απώλειας πακέτων μπορεί να είναι μεγάλος.

III. Είναι εύκολος στην υλοποίηση: Ο αλγόριθμος του WEP μπορεί να υλοποιηθεί είτε σε λογισμικό είτε σε υλικό.

IV. Είναι προαιρετικό: Η υλοποίηση και χρήση του WEP στο 802.11 είναι προαιρετική.

V. Υπάρχει η δυνατότητα για εξαγωγή: Έγινε προσπάθεια κατά το σχεδιασμό του WEP ώστε να μεγιστοποιηθούν οι πιθανότητες έγκρισης από Τμήμα Εμπορίου των Ηνωμένων Πολιτειών για εξαγωγή προϊόντων που θα υποστήριζαν WEP.

Βλέπουμε δηλαδή ότι οι απαιτήσεις προσπαθούσαν να ισορροπήσουν ανάμεσα στην ανάγκη για μια σε λογικά επίπεδα δυνατή λύση και την ανάγκη για έναν απλό στην υλοποίηση αλγόριθμο. Πάντως, πρέπει να πούμε ότι η λογική της «περίπου ασφάλειας» ήταν λάθος. Πολλοί υποστηρίζουν ότι υπάρχουν δυο επίπεδα ασφάλειας, δυνατή ασφάλεια και καθόλου ασφάλεια.

Την πρώτη περίοδο χρήσης των ασύρματων τοπικών δικτύων και αφού οι περιορισμοί για εξαγωγή κρυπτογραφικών προϊόντων είχαν γίνει πιο ελαστικοί, πολλοί κατασκευαστές μπήκαν στη διαδικασία να υλοποιήσουν προϊόντα που αντί για 40 bits κλειδί χρησιμοποιούσαν 104 bits κλειδί παρά το γεγονός ότι δεν προβλεπόταν κάτι τέτοιο από το αρχικό standard. Με την υιοθέτηση αυτής της επέκτασης οι κατασκευαστές άρχισαν να μιλούν για ολοκληρωμένη λύση ασφάλειας στα ασύρματα τοπικά δίκτυα, που από ότι θα δούμε πιο κάτω ήταν μια πολύ βιαστική τοποθέτηση.

4.9.2 Πως λειτουργεί το WEP

Ας δούμε όμως πως ακριβώς λειτουργεί το WEP. Στο standard 802.11 του 1999 έχουν οριστεί δυο επίπεδα ασφάλειας που αντίστοιχα υιοθετούν τη μέθοδο ανοιχτού (open) και κοινού (shared) κλειδιού. Η μέθοδος ανοιχτού κλειδιού σημαίνει επί της ουσίας καθόλου ασφάλεια, ενώ η μέθοδος κοινού κλειδιού σημαίνει ότι τα δύο άκρα που επικοινωνούν γνωρίζουν και τα δύο την τιμή του κλειδιού, το οποίο προφανώς έχει νόημα μόνο όταν αυτό το κλειδί είναι κοινό μόνο για αυτούς που έχουν δικαίωμα σύνδεσης στο δίκτυο και όχι γενικώς κοινό σε όλους.
Στο σημείο αυτό, είναι απαραίτητο να περιγράψουμε λίγο τη δομή και αρχιτεκτονική του πρωτοκόλλου, ώστε να μπορέσουμε αργότερα να κατανοήσουμε καλύτερα τις αδυναμίες που εμφανίζει. Μάλιστα ίσως μια τέτοια ανάλυση να βοηθήσει και στην κατανόηση και κάποιων από τις υπόλοιπες επιθέσεις που μπορούν να συμβούν στο 802.11b πρωτόκολλο.

4.9.3 Πιστοποίηση

Το WEP παρότι είναι κυρίως γνωστό για την δυνατότητα κρυπτογράφησης που προσφέρει σε ένα ασύρματο δίκτυο, έχει επίσης και την αρμοδιότητα να πιστοποιεί και χρήστες - συσκευές με το εκάστοτε Access Point. Αναλαμβάνει δηλαδή η κάθε client συσκευή να αποδείξει την ταυτότητα της στο εκάστοτε AP. Το σωστό βέβαια θα ήταν το ίδιο ακριβώς να γίνεται και για το AP ως προς τη συσκευή. Κι αυτό άλλωστε είναι και το πρώτο πρόβλημα του πρωτοκόλλου.
Ο τρόπος που έχει επιλεχθεί για να γίνει αυτή η πιστοποίηση ταυτότητας του χρήστη (συσκευής) είναι μέσω της MAC address του, η οποία είναι μοναδική για κάθε δικτυακή συσκευή που υπάρχει στον κόσμο .
Το AP και ο χρήστης συμφωνούν σε ένα κρυφό κλειδί με το οποίο θα γίνει όλη η διαδικασία της πιστοποίησης και της κρυπτογράφησης και αφού επιβεβαιωθεί ότι και οι 2 πλευρές έχουν το ίδιο κλειδί τότε επιτρέπεται από μεριάς του AP η σύνδεση του χρήστη σε αυτό.

Εικόνα 7: Εικόνα πιστοποίησης αυθεντικότητας

Στη φάση πιστοποίησης αυθεντικότητας χρησιμοποιούνται management frames όπου ανταλλάσσονται τέσσερα τέτοια μηνύματα.

1. Ο χρήστης στέλνει την αίτηση πιστοποίησης αυθεντικότητας
2. Το AP απαντά με ένα μήνυμα δοκιμασίας (challenge message).
3. Ο χρήστης απαντά στο παραπάνω μήνυμα για να αποδείξει ότι γνωρίζει το κρυφό κλειδί
4. Αν η απόδειξη είναι αποδεκτή, το AP απαντά με μήνυμα επιτυχίας και αποδοχής του χρήστη

4.9.4 Κωδικοποίηση

Μετά τη φάση της πιστοποίησης, ακολουθεί η φάση της κωδικοποίησης. Βέβαια κωδικοποίηση υπάρχει και στην πρώτη φάση και συγκεκριμένα κατά τη διάρκεια αποστολής των μηνυμάτων δοκιμασίας (challenge messages).

Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ο γνωστός και από άλλες εφαρμογές **RC4**. Πρόκειται για έναν ιδιαίτερα ισχυρό αλγόριθμο κωδικοποίησης ο οποίος είναι απλός και παράλληλα ευέλικτος στην υλοποίηση αφού μπορεί να υλοποιηθεί τόσο σε software όσο και σε hardware. Η κρυπτογράφηση των δεδομένων γίνεται ως μια συνεχή ροή (stream cipher) χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση αλλά και για την αποκρυπτογράφηση (symmetric algorithm).

Ο RC4 έχει δυο φάσεις:

1. την φάση αρχικοποίησης, όπου δημιουργούνται κάποιοι πίνακες με βάση την τιμή του κλειδιού.
2. η δεύτερη φάση όπου γίνεται η κρυπτογράφηση των δεδομένων

Στην περίπτωση του WEP τόσο η φάση αρχικοποίησης όσο και κρυπτογράφησης πραγματοποιούνται για κάθε πακέτο. Επεξεργάζονται δηλαδή τα πακέτα σαν να ήταν διακριτά διαφορετικά κομμάτια πληροφορίας. Αυτό εξασφαλίζει ότι αν κάποιο πακέτο χαθεί μπορεί και πάλι να συνεχίσει η αποκρυπτογράφηση των πακέτων. Όμως αυτό το σημείο εκτός από θετικό είναι επίσης και αρνητικό.

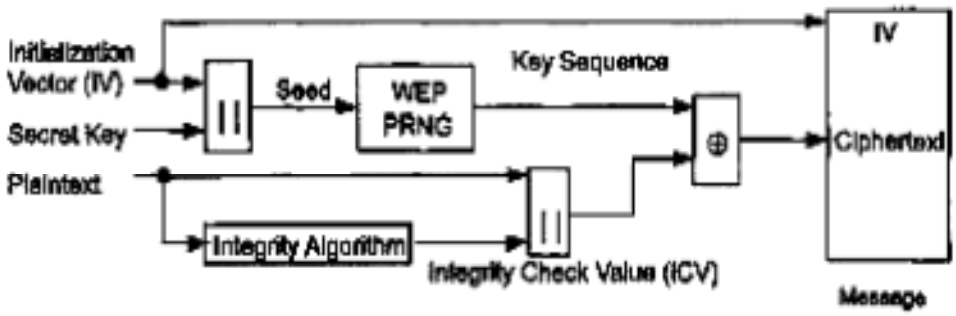
Το «μέγεθος» της κωδικοποίησης για το WEP, είναι συνήθως της τάξης των 128 bits. Από αυτά τα 104 είναι το διαμοιραζόμενο κλειδί και τα άλλα 24 είναι μια τυχαία σειρά αριθμών που χρησιμοποιείται για να συνδυαστεί με το κλειδί, έτσι ώστε να παράγεται πάντα μια ψευδό-τυχαία συμβολοσειρά χαρακτήρων και να επιτευχθεί η κωδικοποίηση με το γνωστό1ο τρόπο που αυτό επιτυγχάνεται από τον RC4 αλγόριθμο. Η συμβολοσειρά αυτή ονομάζεται διάνυσμα αρχικοποίησης (**initialization vector - IV**) και για πολλούς αποτέλεσε την αφορμή ώστε να αρχίσει όλη η ερευνητική κοινότητα να ασχολείται σοβαρότερα με το θέμα της ασφάλειας στα ασύρματα δίκτυα.

Καταλήγοντας λοιπόν, επισημαίνουμε ότι τα κλειδιά που χρησιμοποιούνται στον αλγόριθμο αυτό είναι 104 bits (παλιότερα ήταν 40 και αργότερα έχουν επιλεγεί για λόγους ασφάλειας ακόμα και κλειδιά 232 bits), όμως το IV παραμένει πάντα ίδιο. Τα κλειδιά αυτά είναι στατικά, κοινά μεταξύ χρήστη και AP και συμμετρικά, χρησιμοποιούνται δηλαδή τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Να επισημάνουμε εδώ ότι για λόγους ασφαλείας (αφού τα

κλειδιά είναι στατικά), έχουν επιλεγεί 2 εναλλακτικοί τρόποι χρήσης τέτοιων κλειδιών.

1. Η πρώτη είναι αυτή των **default keys** όπου μια τετράδα από στατικά κλειδιά εισάγεται ώστε να αλλάζονται μετά από κάποιο ορισμένο χρόνο τα κλειδιά και να αποφεύγεται η πολύ συνεχόμενη και μη εναλλασσόμενη χρήση του ίδιου κλειδιού. Αυτός ο τρόπος βέβαια απαιτεί και την ίδια διαδικασία (της πληκτρολόγησης τεσσάρων διαφορετικών κλειδιών) και σε όλους τους χρήστες του δικτύου που εφαρμόζεται αυτή η πολιτική. Επίσης απαιτεί και την προσθήκη 1 byte στο πακέτο που αποστέλλεται, αφού πρέπει να μεταδοθεί και ένας αριθμός με το όνομα **key ID**, ο οποίος θα διευκρινίζει ποιο από τα 4 αυτά κλειδιά είναι στην συγκεκριμένη στιγμή σε χρήση.

2. Ο εναλλακτικός αυτού του τρόπου είναι η χρήση διαφορετικού κλειδιού ανά συσκευή και έτσι 2 διαφορετικοί χρήστες μπορούν να έχουν και διαφορετικά κλειδιά γνωστός και ως **key mapping**. Ο τρόπος αυτός, αν και πιο ασφαλής, δυστυχώς δεν υποστηρίζεται από τους κατασκευαστές δικτυακών ασύρματων συσκευών λόγω της πολυπλοκότητας του.



Εικόνα 8: Γραφική απεικόνιση του αλγορίθμου.

4.9.5 Γιατί δεν είναι ασφαλές το WEP;

Οι έρευνες των επιστημόνων είχαν να κάνουν κυρίως με προβλήματα υλοποίησης του RC4 αλγορίθμου στο WEP πρωτόκολλο και με προβλήματα στη διαχείριση των κλειδιών του.

Το WEP διαθέτει όλους τους μηχανισμούς που χρειάζονται στην ασφάλεια. Πιο συγκεκριμένα αυτοί οι μηχανισμοί έχουν να κάνουν με:

- Πιστοποίηση αυθεντικότητας
- Έλεγχος πρόσβασης
- Αποφυγή επαναλήψεων
- Ανίχνευση αλλοίωσης του μηνύματος
- Ανίχνευση αλλοίωσης του μηνύματος
- Προστασία του κλειδιού

Όμως κανένας από αυτούς τους μηχανισμούς δεν είναι αξιόπιστος με αποτέλεσμα να αποτυγχάνει παντελώς, καθιστώντας το WEP όχι απλά άχρηστο αλλά και επικίνδυνο για χρήση σε δίκτυα που χρειάζονται ασφάλεια. Πολύ συχνά αυτά τα προβλήματα που παρουσιάζει κάνουν πολλούς να υποστηρίζουν ότι ίσως είναι καλύτερο να μην ενεργοποιείται καν γιατί είναι σχετικά εύκολο να σπάσει η ασφάλεια που παρέχει. Παρόλα τα προβλήματα του, το WEP μπορεί ακόμα και σήμερα να αποτελέσει μια πρώτη ασπίδα προστασίας εναντίον όλων εκείνων που θα επιχειρήσουν να εκμεταλλευτούν τα πλεονεκτήματα ενός ασύρματου δικτύου χωρίς την εξουσιοδότηση του παρόχου του δικτύου αυτού. Αυτό βέβαια μόνο σε περιπτώσεις όπου κανένας άλλος από τους γνωστούς τρόπους προστασίας δεν είναι διαθέσιμος. Ο αντίλογος σε αυτή την άποψη είναι, ότι όποιος είναι αποφασισμένος να χρησιμοποιήσει τους πόρους ενός WLAN, δε θα τον εμποδίσει μια τέτοιου είδους προστασία από το να πετύχει το σκοπό του και μάλιστα πολύ συχνά μπορεί μια τέτοια κίνηση να του εξάψει περισσότερο την περιέργεια για το τι μπορεί να επιχειρείται να κρυφτεί πίσω από ένα τέτοιο, οποιασδήποτε ποιότητας, επίπεδο ασφαλείας.

4.10 Έλεγχος ταυτότητας 802.1x

Το πρωτόκολλο 802.1x είναι ένα standard της IEEE το οποίο ορίστηκε για τον έλεγχο πρόσβασης σε δίκτυα, βασισμένα σε ports. Αρχικά σχεδιάστηκε για τοπικά δίκτυα Ethernet, μπόρεσε όμως και βρήκε εφαρμογή στα ασύρματα δίκτυα που βασίζονται στο 802.11. Το 802.11x δεν επιβάλλει την χρήση των ίδιων WEP κλειδιών από όλες

τις δικτυακές συσκευές και επιτρέπει σε μια συσκευή να διατηρεί δύο σύνολα διαμοιραζόμενων κλειδιών. Ένα ανά σταθμό unicast κλειδί συνόδου και ένα multicast κλειδί. Γι αυτό και πολύ συχνά χρησιμοποιείται κι ο όρος Dynamic WEP για να το περιγράψει, αν και ο συσχετισμός αυτός είναι μάλλον άδικος. Οι σημερινές υλοποιήσεις του 802.11 υποστηρίζουν κυρίως multicast κλειδιά. Η διαχείριση και η ανανέωση αυτών των κλειδιών χειροκίνητα είναι μια περίπλοκη και χρονοβόρα διαδικασία, η οποία γίνεται απαγορευτική στην περίπτωση μεγάλων δικτυακών υποδομών ή σε ad-hoc δίκτυα.

Ο έλεγχος ταυτότητας 802.1x είναι ανεξάρτητος από τη διαδικασία ελέγχου ταυτότητας 802.11, παρέχει ένα πλαίσιο εργασίας για διάφορα πρωτόκολλα ελέγχου ταυτότητας και διαχείρισης κλειδιού. Υπάρχουν διαφορετικοί έλεγχοι ταυτότητας 802.1xκαι καθένας τους παρέχει μια διαφορετική προσέγγιση, αλλά όλοι χρησιμοποιούν το ίδιο πρωτόκολλο και πλαίσιο εργασίας 802.1x για επικοινωνία μεταξύ πελάτη και σημείου πρόσβασης. Στα περισσότερα πρωτόκολλα, αμέσως μετά την ολοκλήρωση της διαδικασίας ελέγχου 802.1x, το σύστημα υποδοχής (supplicant) λαμβάνει ένα κλειδί που το χρησιμοποιεί για κρυπτογράφηση δεδομένων. Με τον έλεγχο ταυτότητας 802.1x, μια μέθοδος ελέγχου ταυτότητας χρησιμοποιείται μεταξύ του πελάτη και ενός διακομιστή RADIUS (Remote Authentication Dial-In User Service) που είναι συνδεδεμένος στο σημείο πρόσβασης. Η διαδικασία ελέγχου ταυτότητας χρησιμοποιεί διαπιστευτήρια, όπως ένα συνθηματικό χρήστη που δεν μεταφέρεται μέσω ασύρματου δικτύου. Οι περισσότεροι τύποι 802.1x υποστηρίζουν δυναμικά κλειδιά ανά χρήστη και ανά συνεδρία για να ενδυναμώσουν την ασφάλεια του στατικού κλειδιού. Η χρήση ενός υπάρχοντος πρωτοκόλλου ελέγχου ταυτότητας, γνωστό ως EAP (Extensible Authentication Protocol) ωφελεί το 802.1x.

Ο έλεγχος ταυτότητας 802.1x για ασύρματα δίκτυα αποτελείται από τρία κύρια συστατικά:

- Τον ελεγκτή ταυτότητας (το σημείο πρόσβασης)
- Το σύστημα υποδοχής (το λογισμικό του πελάτη)
- Το διακομιστή ελέγχου ταυτότητας (RADIUS)

Η ασφάλεια ελέγχου ταυτότητας 802.1x εκκινεί μια αίτηση ελέγχου ταυτότητας από τον ασύρματο πελάτη στο σημείο πρόσβασης, το οποίο ελέγχει την ταυτότητα του πελάτη σε ένα διακομιστή RADIUS συμβατό με το πρωτόκολλο EAP (Extensible Authentication Protocol). Αυτός ο διακομιστής RADIUS μπορεί να ελέγχει την ταυτότητα είτε του χρήστη (μέσω κωδικών πρόσβασης ή πιστοποιητικών) είτε του συστήματος (από τη διεύθυνση MAC). Θεωρητικά, δεν επιτρέπεται στον ασύρματο πελάτη να συνδεθεί με τα δίκτυα έως ότου ολοκληρωθεί η συναλλαγή.

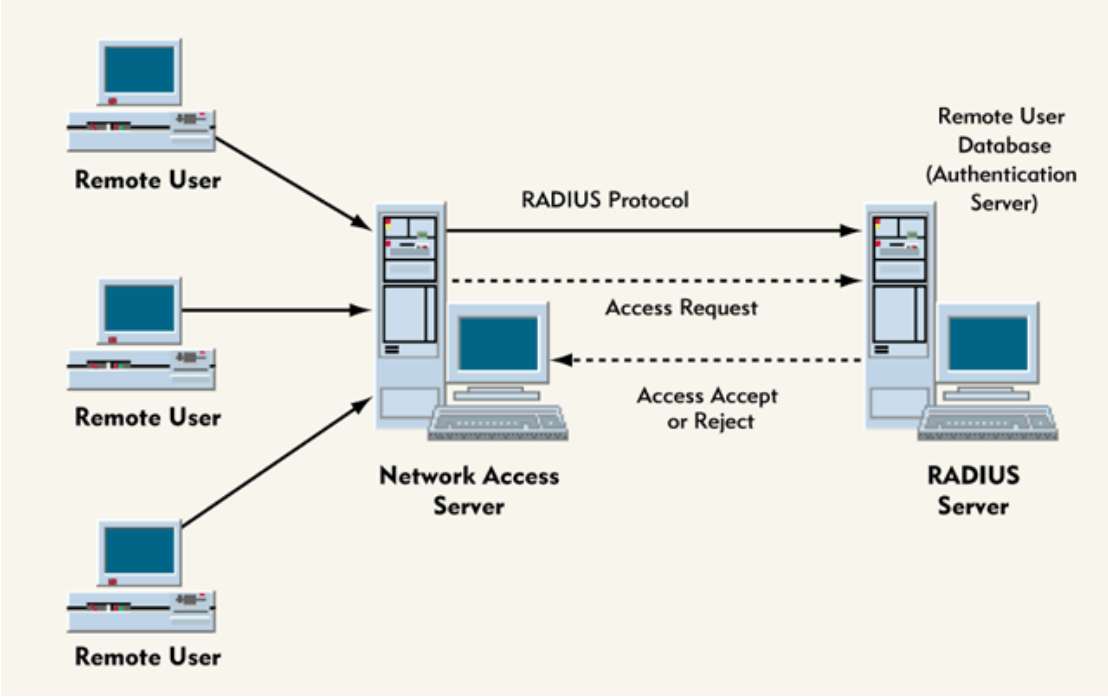
Χρησιμοποιούνται αρκετοί αλγόριθμοι ελέγχου ταυτότητας για το 802.1x. Μερικά παραδείγματα είναι: EAP-TLS, EAP-TTLS και Protected EAP (PEAP). Αυτές είναι όλες μέθοδοι αναγνώρισης του ασύρματου πελάτη στο διακομιστή RADIUS. Με τον έλεγχο ταυτότητας RADIUS, οι ταυτότητες χρήστη ελέγχονται έναντι των βάσεων δεδομένων. Αποτελεί ένα σύνολο προτύπων που αντιμετωπίζουν τον έλεγχο ταυτότητας, την εξουσιοδότηση και τη λογιστική Authentication, Authorization, Accounting (AAA). Περιλαμβάνει μια διαδικασία μεσολάβησης για την επικύρωση πελατών σε περιβάλλον πολλαπλών διακομιστών. Το πρότυπο IEEE 802.1x προορίζεται για τον έλεγχο και την πρόσβαση ελέγχου ταυτότητας σε ασύρματα 802.11 βάσει θύρας και καλωδιακά δίκτυα Ethernet. Ο έλεγχος πρόσβασης δικτύου βάσει θύρας είναι παρόμοιος με μια υποδομή τοπικού δικτύου (LAN) μεταγωγής που ελέγχει την ταυτότητα συσκευών που συνδέονται σε θύρα LAN και αποτρέπουν την πρόσβαση στη θύρα αυτή, εάν αποτύχει η διαδικασία ελέγχου ταυτότητας.

4.10.1 Τι είναι το radius;

Το RADIUS (Remote Authentication Dial-In User Service) είναι ένα πρωτόκολλο πελάτη-διακομιστή για έλεγχο ταυτότητας, εξουσιοδότηση και λογιστική (Authentication, Authorization, Accounting (AAA)), που χρησιμοποιείται όταν ο πελάτης με σύνδεση μέσω τηλεφώνου (dial-up) AAA συνδέεται ή τερματίζει τη σύνδεση του από ένα διακομιστή πρόσβασης δικτύου. Συνήθως, ο διακομιστής RADIUS χρησιμοποιείται από τις υπηρεσίες παροχής Διαδικτύου (ISP) για την εκτέλεση εργασιών AAA. Οι φάσεις AAA περιγράφονται ως ακολούθως:

- Φάση ελέγχου ταυτότητας: Επαληθεύει ένα όνομα χρήστη και κωδικό πρόσβασης έναντι μιας τοπικής βάσης δεδομένων. Μετά την επικύρωση των διαπιστευτηρίων, αρχίζει η διαδικασία ελέγχου ταυτότητας.

- Φάση εξουσιοδότησης: Καθορίζει εάν επιτρέπεται πρόσβαση μιας αίτησης σε ένα πόρο. Μια διεύθυνση IP εκχωρείται για έναν πελάτη dial-up.
- Φάση λογιστικής: Συλλέγει πληροφορίες για τη χρήση πόρων με σκοπό την ανάλυση τάσεων, το λογιστικό έλεγχο, την τιμολόγηση χρόνου συνεδρίας ή την κατανομή εξόδων.



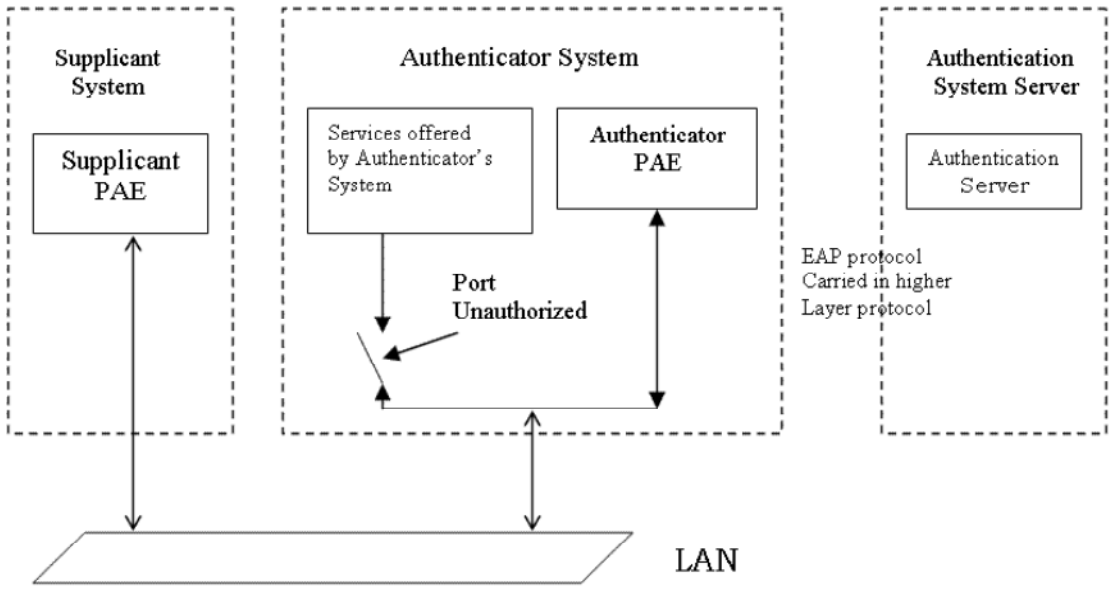
Εικόνα 9: Απεικόνιση του Radius

4.11 Βασική λειτουργία του 802.11x

Για να καταλάβουμε την βασική λειτουργία του πρωτοκόλλου, ας ορίσουμε μερικές από τις οντότητες που παίρνουν μέρος στο 802.1x. Οι οντότητες αυτές είναι ο **authenticator**, ο **supplicant**και ο **authentication server**.

Ο authenticator είναι μια οντότητα που απαιτεί πιστοποίηση πριν να επιτρέψει πρόσβαση στις υπηρεσίες του δικτύου. Ο supplicant είναι η οντότητα που θέλει να αποκτήσει πρόσβαση στις υπηρεσίες μέσω του authenticator. Ο authentication server εκτελεί την εξής λειτουργία: ελέγχει την εγκυρότητα των διαπιστευτηρίων του supplicant για λογαριασμό του authenticator. Έπειτα απαντά στον authenticator υποδεικνύοντας του αν πρέπει ή όχι να δώσει πρόσβαση στον αιτούντα supplicant. Ο

server αυτός μπορεί να είναι μια ξεχωριστή οντότητα ή οι λειτουργίες του να εκτελούνται από τον ίδιο τον authenticator.



Μια LAN port μπορεί να παίξει δύο ρόλους στην διαδικασία ελέγχου πρόσβασης στο δίκτυο: authenticator και supplicant. Ο έλεγχος πρόσβασης του authenticator που βασίζεται σε ports ορίζει δύο λογικά σημεία πρόσβασης προς το LAN μέσω μιας απλής LAN σύνδεσης. Το πρώτο λογικό σημείο πρόσβασης ονομάζεται «Uncontrolled Port» και επιτρέπει την μη ελεγχόμενη ανταλλαγή μεταξύ του authenticator και των υπολοίπων συστημάτων του LAN, ανεξάρτητα από την δικαιοδοσία των συστημάτων αυτών. Το δεύτερο λογικό σημείο πρόσβασης είναι η «Controlled Port» η οποία επιτρέπει πρόσβαση στις υπηρεσίες που προσφέρει ο authenticator, μόνο όταν το σύστημα που τις ζητά είναι πιστοποιημένο.

Μια χρήση της Uncontrolled Port είναι η ανταλλαγή στοιχείων μεταξύ του supplicant και του authenticator. Η κατάσταση πιστοποίησης ορίζει αν η Controlled Port επιτρέπει την ροή δεδομένων από τον supplicant προς το LAN μέσω αυτής της port. Αρχικά αυτή η Port είναι κλειστή και μόλις ο supplicant πιστοποιηθεί ανοίγει.

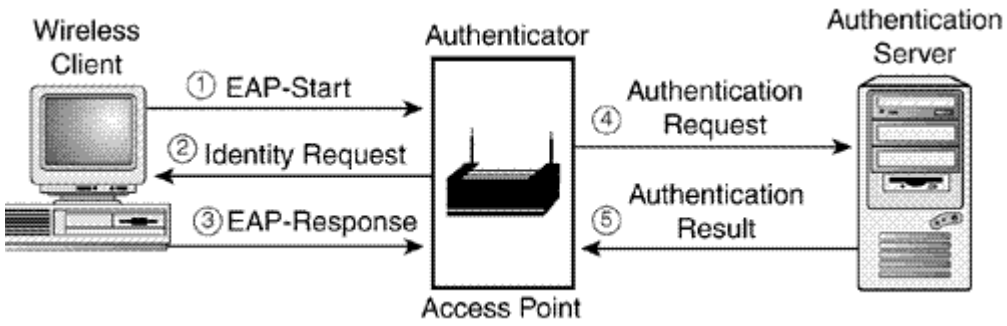
Το 802.1x χρησιμοποιεί το Extensible Authentication Protocol(EAP) για να ανταλλάξει πληροφορίες πιστοποίησης μεταξύ του supplicant και του authentication server. Το EAP είναι η ραχοκοκαλιά του πρωτοκόλλου 802.1x και με το πέρασμα των

χρόνων έχουν εμφανιστεί πολλές παραλλαγές αυτού που καλύπτουν κάθε φορά διαφορετικές ανάγκες.

4.11.1 Διαδικασία πιστοποίησης

Στην διαδικασία που θα παρουσιάσουμε θεωρούμε ότι γίνεται χρήση EAP για την πιστοποίηση και RADIUS για authentication server. Υπάρχουν και άλλες πιθανές ροές μηνυμάτων, ανάλογα με τον μηχανισμό που χρησιμοποιούμε. Συνοπτικά η συνολική διαδικασία των πρωτοκόλλων που χρησιμοποιούνται σε κάθε φάση φαίνεται πιο κάτω:

1. Ο authenticator στέλνει ένα μήνυμα EAP-Request/Identity στον supplicant
2. Supplicant στέλνει μήνυμα EAP-Response/Identity με την ταυτότητά του στον authenticator. Ο authenticator προωθεί αυτήν την πληροφορία στον RADIUS
3. Ο RADIUS απαντά με ένα πακέτο EAP-Request μήνυμα που περιέχει έναν κωδικό επαλήθευσης (challenge password) στον supplicant μέσω του authenticator.
4. Ο Supplicant στέλνει την απάντηση σε αυτόν τον κωδικό στον RADIUS μέσω του authenticator
5. Αν η πιστοποίηση είναι επιτυχής, αποστέλλεται ένα πακέτο EAP-Success από τον RADIUS στον supplicant Μέσω του authenticator. Ο authenticator μόλις δει αυτό το πακέτο ενεργοποιεί την Controlled Port και επιτρέπει στον supplicant να έχει πρόσβαση στις υπηρεσίες



Εικόνα 10:Διαδικασία πιστοποίησης

3.11.2 Τι προβλήματα επιλύει;

Το βασικό 802.1x πρωτόκολλο πρέπει να επεκταθεί για να επιλύει τα προβλήματα του 802.11. Αυτό γίνεται με την παροχή ενός κλειδιού πιστοποίησης στον πελάτη και στο AP, σαν μέρος της διαδικασίας πιστοποίησης. Το 802.1x βοηθά στην επίλυση αυτού του προβλήματος προβλέποντας κλειδιά ανά σταθμό ή ανά σύνοδο ώστε να μειώσει την πιθανότητα χρήσης ίδιου κλειδιού από περισσότερα πακέτα καθώς και την ανανέωση κλειδιών κάθε 5 με 10 λεπτά ή κάθε 4 εκατομμύρια πακέτα, μειώνοντας έτσι την επαναχρησιμοποίηση διαμοιραζόμενων κλειδιών, την κύρια αδυναμία του WEP.

Με το 802.1x αυτό γίνεται αυτόματα.

Μετά την πιστοποίηση, το 802.1x πρέπει να παραμετροποιείται ώστε να απαιτεί από τον σταθμό να επαναπιστοποιείται περιοδικά, σε συγκεκριμένα χρονικά διαστήματα. Επίσης το 802.1x επιτρέπει ταυτοποίηση χρήστη και πιστοποίηση καθώς και κεντρικοποιημένη πιστοποίηση, πολιτική επιτρεπτών ενεργειών χρήστη και μηχανισμούς accounting. Αυτό επιτρέπει επίσης την μελλοντική χρήση εκτενών μηχανισμών πιστοποίησης.
Είναι σημαντικό να θυμόμαστε ότι όλη η κίνηση των πακέτων πιστοποίησης γίνεται από την Uncontrolled Port, ενώ όλες οι επιτρεπόμενες μετά την πιστοποίηση μεταφορές δεδομένων λαμβάνουν χώρα στην Controlled Port. Η πιστοποίηση ενός ασύρματου χρήστη μέσω του 802.1x περιλαμβάνει τα πιο κάτω βήματα:

1. Χωρίς κάποιο έγκυρο κλειδί πιστοποίησης, το AP απαγορεύει την κίνηση μέσω αυτού.
2. Όταν η συσκευή βρεθεί στο πεδίο του AP, το AP στέλνει μια πρόκληση στον STA.
3. Ο STA απαντά με την ταυτότητά του στο AP.
4. Το AP στέλνει την ταυτότητα στον RADIUS ο οποίος ζητά τα διαπιστευτήρια του STA και ορίζει τον τύπο που απαιτείται για να γίνει η πιστοποίηση.
5. Ο STA στέλνει τα απαραίτητα διαπιστευτήρια στον RADIUS.

6. Όταν εξακριβωθεί η εγκυρότητα των στοιχείων του STA ο RADIUS στέλνει ένα κλειδί πιστοποίησης στο AP σε κρυπτογραφημένη μορφή ώστε μόνο το AP να μπορεί να το δει.
7. Το AP χρησιμοποιεί αυτό το κλειδί για να εκπέμψει για κάθε σταθμό ξεχωριστά τα unicast κλειδιά συνόδου και τα multicast κλειδιά πιστοποίησης στον STA.

4.12 Πώς λειτουργεί (με απλά λόγια) ο έλεγχος ταυτότητας 802.1x

Μια απλουστευμένη περιγραφή του ελέγχου ταυτότητας 802.1x είναι η ακόλουθη:

- Ένας πελάτης στέλνει μήνυμα "αίτησης για πρόσβαση" σε σημείο πρόσβασης. Το σημείο πρόσβασης ζητά την ταυτότητα του πελάτη.
- Ο πελάτης απαντά με το πακέτο ταυτότητάς του το οποίο περνά στο διακομιστή ελέγχου ταυτότητας.
- Ο διακομιστής ελέγχου ταυτότητας στέλνει ένα πακέτο "αποδοχής" στο σημείο πρόσβασης.
- Το σημείο πρόσβασης τοποθετεί τη θύρα πελάτη στην εξουσιοδοτημένη κατάσταση και επιτρέπεται στην κίνηση δεδομένων να συνεχιστεί.

4.13 Ανάλυση της τεχνολογίας WPA

Το Wi-Fi Protected Access (WPA ή WPA2) είναι μια βελτιωμένη έκδοση ασφάλειας που ενδυναμώνει το επίπεδο προστασίας δεδομένων και ελέγχου πρόσβασης σε ασύρματο δίκτυο. Το WPA επιβάλλει έλεγχο ταυτότητας 802.1x και ανταλλαγή κλειδιών και λειτουργεί μόνο με κλειδιά δυναμικής κρυπτογράφησης. Για την ενίσχυση της κρυπτογράφησης δεδομένων, το WPA χρησιμοποιεί Temporal Key Integrity Protocol (TKIP). Το TKIP παρέχει σημαντικές βελτιώσεις κρυπτογράφησης δεδομένων που περιλαμβάνουν μια λειτουργία ανάμιξης κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος (MIC) με το όνομα Michael, διάνυσμα εκτεταμένης προετοιμασίας (IV) με κανόνες ακολουθίας και μηχανισμό αναπαραγωγής κλειδιών. Με τις βελτιώσεις αυτές, το TKIP προστατεύει κατά των γνωστών αδυναμιών του WEP.

Η δεύτερη γενιά των WPA που συμμορφώνεται με τις προδιαγραφές IEEE TGi είναι γνωστή ως WPA2.

Εικόνα 11: Σήμα WPA/WPA2

4.12.1 Εισαγωγή

Μια ομάδα της IEEE εργάζεται για την προτυποποίηση του πρωτοκόλλου 802.11i. Το πρωτόκολλο αυτό αναμένεται να διασυνδέει όλες τις γνωστές μεθόδους ασφάλειας που αναφέραμε παραπάνω και να θέτει αυστηρότερους κανόνες ως προς την ασφάλεια των ασύρματων δικτύων. Οι εργασίες αυτού του task group έχουν ξεκινήσει εδώ και κάποια χρόνια και ολοκληρώθηκαν στα μέσα του 2004. Επειδή όμως τα κενά ασφαλείας που είχαν εμφανιστεί εδώ και καιρό δε μπορούσαν να αντιμετωπίζονται με υπομονή και καρτερικότητα από τη μεριά των εταιρειών που δραστηριοποιούνται στη συγκεκριμένη αγορά, καθώς έχαναν την εμπιστοσύνη των

πελατών τους, αποφάσισαν να συνασπιστούν κάτω από την «ομπρέλα» μιας συμμαχίας με το όνομα **Wi-Fi Alliance**.

Τα τελευταία χρόνια η Wi-Fi Alliance, μια μη κερδοσκοπική οργάνωση που ασχολείται με την ασφάλεια σε ασύρματα δίκτυα, ξεκίνησε την προσπάθεια της να φέρει στην αγορά μία σύμβαση ασφάλειας βασισμένη σε κάποια standards που θα αύξανε σημαντικά το επίπεδο προστασίας των δεδομένων και τον έλεγχο πρόσβασης στα 802.11 Ασύρματα Τοπικά Δίκτυα. Φυσικά για να συμβεί με τρόπο που μια τέτοια επένδυση σε χρόνο και χρήμα να μην πάει χαμένη, η οργάνωση αυτή φρόντισε να συμβουλευτεί μέλη της ομάδας 802.11i σχετικά με τις σκέψεις που κάνουν πάνω στο πρότυπο που θα εφαρμόσουν στο μέλλον. Επεδίωξαν δηλαδή να αντλήσουν πληροφορίες ώστε αυτό που θα καθόριζαν ως μη επίσημο πρότυπο, να μην απέχει πολύ από το πρότυπο που θα ανακοινώσει στο εγγύς μέλλον η IEEE και αναγκαστούν αργότερα να επανασχεδιάσουν το hardware τους. Αυτή η σύμβαση είναι η **Wireless Protected Access** ή **WPA**.

Σχεδιάστηκε για να προσφέρει ασφάλεια σε όλες τις 802.11 συσκευές, 802.11b, 802.11a και 802.11g. Το WPA είναι ένα υποσύνολο του επερχόμενου 802.11i standard, το οποίο είναι το τελευταίο που έχει εκδοθεί για ασύρματη ασφαλή δικτύωση. Έτσι είναι συμβατό και το WPA συμβατό με το 802.11i αλλά και το 802.11i με το WPA και τις συσκευές που το υποστηρίζουν.

Κάνει χρήση του Temporal Key Integrity Protocol (TKIP) για την κρυπτογράφηση και του πρωτοκόλλου 802.1x για την πιστοποίηση σε συνεργασία με κάποιον από τους τύπους του Extensible Authentication Protocol που υπάρχουν σήμερα. Στην ουσία δηλαδή, το WPA ενσωματώνει κάτω από ένα κοινά αποδεκτό πλαίσιο όλους εκείνους τους μηχανισμούς που προσφέρουν αυξημένα επίπεδα ασφάλειας στα ασύρματα δίκτυα.

Εικόνα 12: Εικονίδιο επιλογής μεθόδου κρυπτογράφησης

Υλοποιεί ένα μεγάλο μέρος του προτύπου IEEE 802.11i. Συγκεκριμένα, το Temporal Key Integrity Πρωτόκολλο (TKIP), εγκρίθηκε για το WPA. Το WEP χρησιμοποιεί ένα 40-bit ή 104-bit κλειδί κρυπτογράφησης που πρέπει να εισαχθεί χειροκίνητα σε σημεία ασύρματης πρόσβασης και δεν αλλάζει. Το TKIP χρησιμοποιεί μια σειρά κλειδιών ανά πακέτο, που σημαίνει ότι δημιουργεί δυναμικά ένα νέο 128-bit κλειδί για κάθε πακέτο και έτσι εμποδίζει τους τύπους των επιθέσεων που διακυβεύεται το WEP.

Περιλαμβάνει επίσης ένα έλεγχο ακεραιότητας μηνύματος. Αυτό έχει σχεδιαστεί για να αποτρέψει έναν εισβολέα από τη σύλληψη, την τροποποίηση ή και την εκ νέου αποστολή πακέτων δεδομένων. Αυτό αντικαθιστά τον κυκλικό έλεγχο πλεονασμού (CRC), ο οποίος χρησιμοποιείται από το πρότυπο WEP. Το κύριο ελάττωμα CRC ήταν ότι δεν παρέχουν μια αρκετά ισχυρή εγγύηση της ακεραιότητας των δεδομένων για τα πακέτα που διακινούνται.

Το Wi-Fi Protected Access (WPA ή WPA2) είναι μια βελτιωμένη έκδοση ασφάλειας που ενδυναμώνει το επίπεδο προστασίας δεδομένων και ελέγχου πρόσβασης σε ασύρματο δίκτυο, επιβάλλει έλεγχο ταυτότητας 802.1x και ανταλλαγή κλειδιών και λειτουργεί μόνο με κλειδιά δυναμικής κρυπτογράφησης. Για την ενίσχυση της κρυπτογράφησης δεδομένων, το WPA χρησιμοποιεί Temporal Key Integrity Protocol (TKIP). Το TKIP παρέχει σημαντικές βελτιώσεις κρυπτογράφησης δεδομένων που

περιλαμβάνουν μια λειτουργία ανάμιξης κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος (MIC) με το όνομα Michael, διάνυσμα εκτεταμένης προετοιμασίας (IV) με κανόνες ακολουθίας και μηχανισμό αναπαραγωγής κλειδιών. Με τις βελτιώσεις αυτές, το TKIP προστατεύει κατά των γνωστών αδυναμιών του WEP.

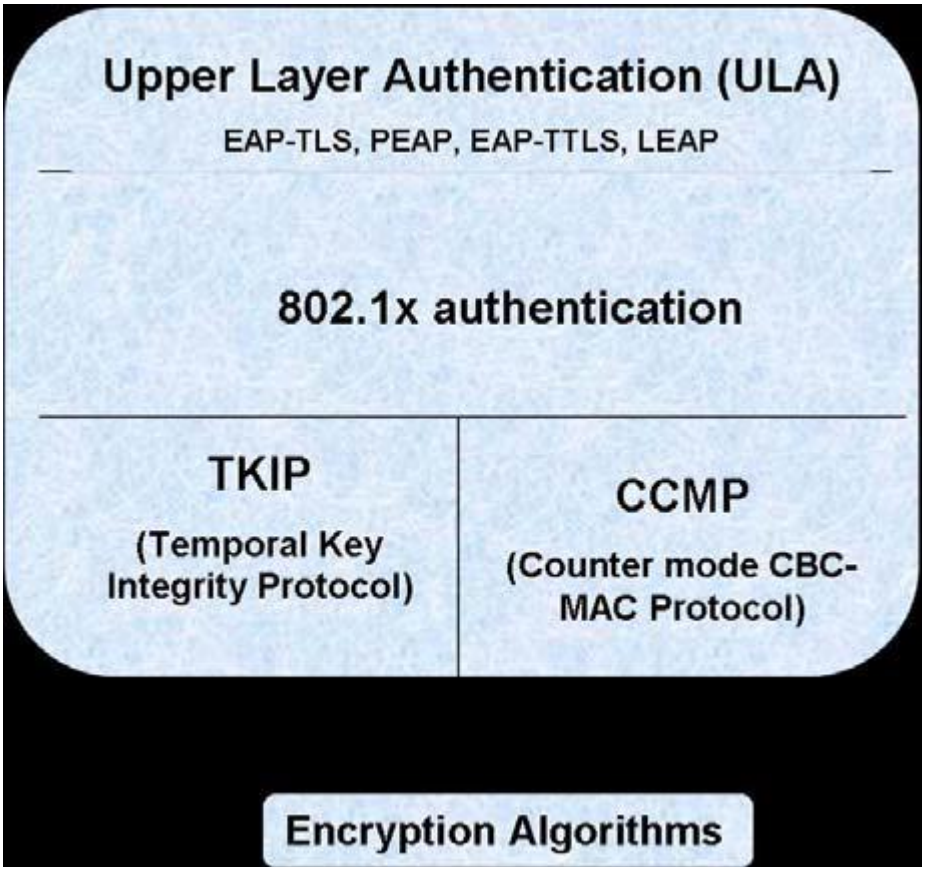
Εικόνα 13: Πως ξεκινά το cracking

4.13 802.11i

Το πολυαναμενόμενο πρότυπο ασφάλειας 802.11i κυκλοφόρησε στα μέσα του 2004. Ως πρότυπο βασίζεται στην εμπειρία που αποκτήθηκε από την χρήση των προηγούμενων πρωτοκόλλων και γίνεται προσπάθεια να μάθει από τις αδυναμίες των προηγούμενων προτύπων ώστε να δώσει ισχυρές λύσεις σε αυτές. Επίσης συνδυάζει τα καλύτερα υπάρχοντα πρωτόκολλα και αλγόριθμους για να δοθεί ένα πρωτόκολλο που υπόσχεται μεγάλη ασφάλεια.

4.13.1 Αρχιτεκτονική του 802.11i

Ο ορισμός του 802.11i μπορεί να ιδωθεί σαν να είναι οργανωμένο σε δύο επίπεδα, όπως φαίνεται και στην παρακάτω εικόνα. Στο χαμηλότερο επίπεδο χρησιμοποιούνται ισχυροί αλγόριθμοι κρυπτογράφησης για να παρέχουν απόρρητη επικοινωνία και στο επόμενο επίπεδο ορίζεται η μέθοδος πιστοποίησης με χρήση του 802.1x.

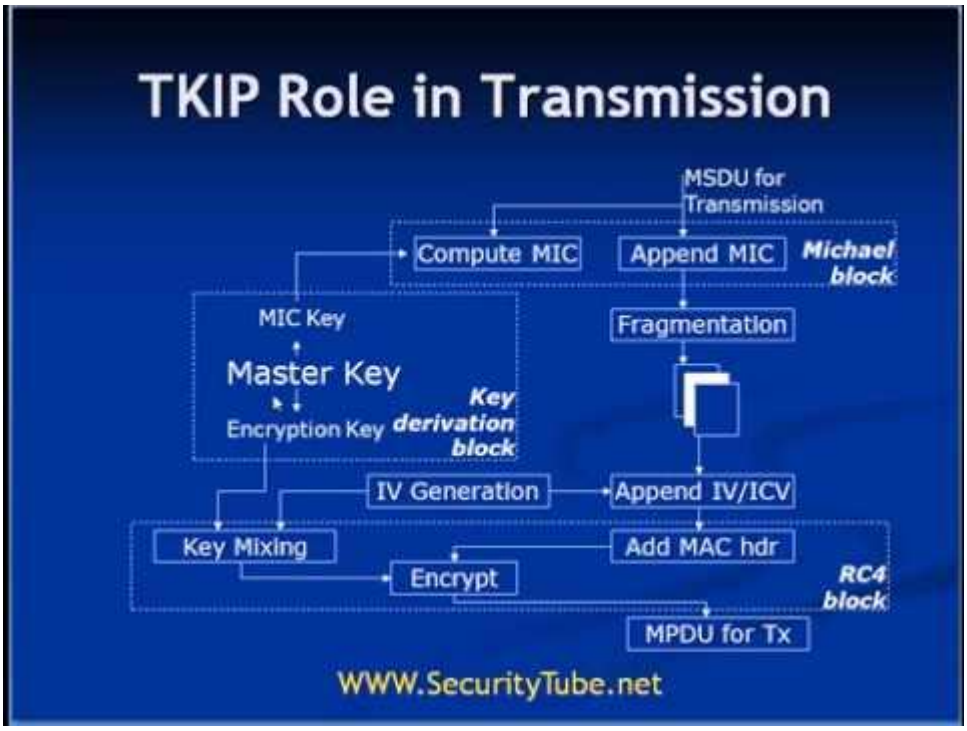


Εικόνα 14: Αρχιτεκτονική του 802.11i

Το 802.11i προτείνει την χρήση τουTemporal Key Integrity Protocol (TKIP) και του Counter mode Cipher Block Chaining Message Authentication and Control Protocol (Counter mode CBC-MAC Protocol - CCMP).

Το TKIP αποτελεί βασικά ένα μονοπάτι για την αναβάθμιση παλαιότερων συστημάτων που χρησιμοποιούσαν το WEP. Είναι προς τα πίσω συμβατό και επιλύει τα προβλήματα της διαχείρισης κλειδιών στο WEP. Όπως φαίνεται και από το όνομά του τα κλειδιά που χρησιμοποιούνται σε αυτόν εξαρτώνται από τον χρόνο. Στο TKIP οι δύο άκρες της σύνδεσης ξεκινούν με ένα κοινό κλειδί μήκους 128 bit που είναι το προσωρινό κλειδί (temporal key–TK).Η διεύθυνση MAC του αποστολέα αναμιγνύεται με το TK για να παράγει το κλειδί της Φάσης 1. Αυτό το κλειδί της Φάσης 1 αναμιγνύεται με την σειρά του ένα διάνυσμα αρχικοποίησης (IV) για να παράγει κλειδιά ανά πακέτο. Κάθε κλειδί χρησιμοποιείται με RC4 για να κρυπτογραφήσει ένα και μόνον ένα πακέτο δεδομένων. Για να αποφευχθεί η επαναχρησιμοποίηση κλειδιού, τα προσωρινά κλειδιά πρέπει να αλλάζουν συχνά. Το

πρωτόκολλο βεβαιώνει την χρήση διαφορετικών streams κλειδιών για την κρυπτογράφηση των δεδομένων.



Εικόνα 15: Η TKIP μέθοδος αναβάθμισης του WEP

Το TKIP χρησιμοποιεί ένα εκτεταμένο 48 bit διάνυσμα αρχικοποίησης (IV) που ονομάζεται TKIP sequence counter (TSC). Η χρήση του αυξάνει την ζωή του προσωρινού κλειδιού σε μια απλή συσχέτιση. Μιας και ο TSC

4.13.2 Συμπέρασμα

Το 802.11i έχει αυστηρές απαιτήσεις για την μεταφορά δεδομένων. Αυτές είναι:

1. Σε κανένα σημείο δεν στέλνονται δεδομένα στο δίκτυο χωρίς προστασία
2. Απαιτείται πιστοποίηση αποστολέα
3. Απαιτείται αρίθμηση των πακέτων για ανίχνευση επιθέσεων επανάληψης
4. Απαιτεί προστασία των διευθύνσεων MAC των συσκευών του δικτύου για προστασία από πλαστογραφήσεις

Υπάρχουν δύο ζητήματα τα οποία πρέπει να λαμβάνονται υπόψιν.

Πρώτον η απαίτηση για χρήση του CCMP να υποστηρίζεται από όλους τους κατασκευαστές. .

Το δεύτερο ζήτημα είναι ότι το 802.11i παίρνει πολλά διαφορετικά πρωτόκολλα και τα βάζει μαζί σε ένα. Πρέπει να διασφαλιστεί η δια λειτουργικότητα των πρωτοκόλλων αυτών και να υλοποιηθούν από τους κατασκευαστές με έναν τρόπο που να σέβεται το πρότυπο και παράλληλα οι συσκευές από διαφορετικούς κατασκευαστές να διατηρούν την απαραίτητη συμβατότητα μεταξύ τους.

Ο CCMP είναι ένας νέος και εξαιρετικά δυνατός αλγόριθμος κρυπτογράφησης που βασίζεται στην μηχανή του Advanced Encryption Standard (AES). Η κρυπτογράφηση που βασίζεται στον AES μπορεί να χρησιμοποιηθεί σε διάφορες καταστάσεις ή αλγόριθμους.

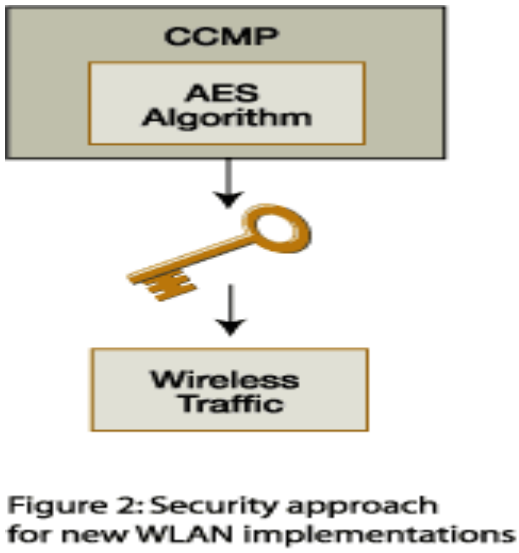


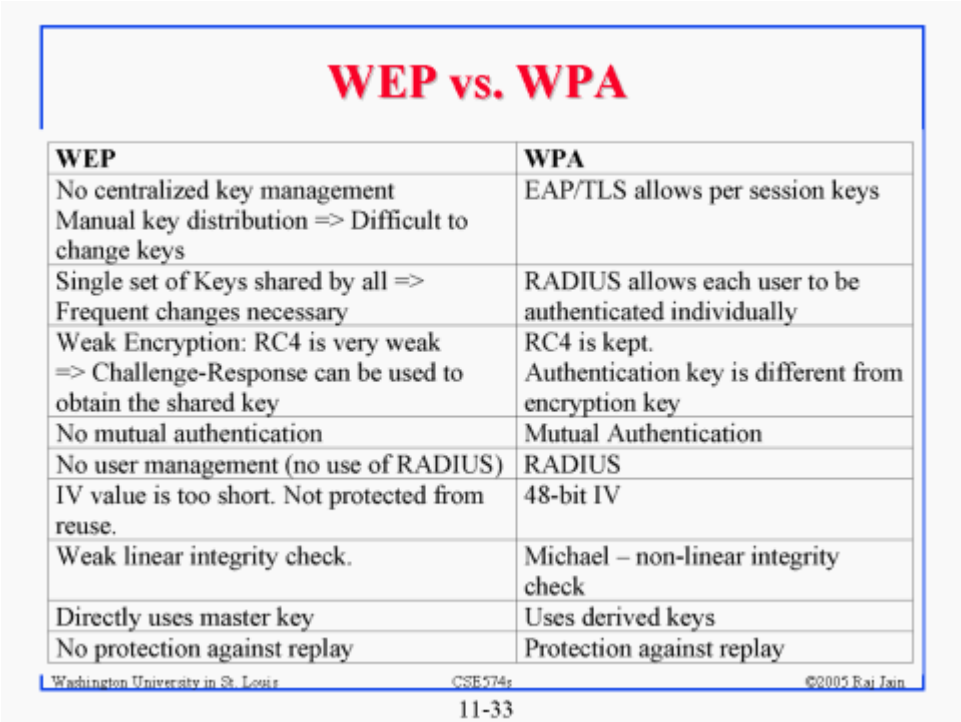
Figure 2: Security approach
for new WLAN implementations

Εικόνα 16: Ασφαλής προσέγγιση για την εκτέλεση νέου WLAN

Η κατάσταση που έχει επιλεγεί για το 802.11 είναι η κατάσταση μετρητή (Counter Mode) με CBC-MAC (CCM). Η κατάσταση μετρητή προσδίδει μυστικότητα δεδομένων ενώ το CBC-MAC προσδίδει ακεραιότητα δεδομένων και πιστοποίηση. Ο AES είναι ένας συμμετρικός επαναληπτικός αλγόριθμος κρυπτογράφησης κατά μπλοκ, που σημαίνει την χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση, πολλαπλά περάσματα γίνονται στα δεδομένα για να κρυπτογραφηθούν και το αρχικό κείμενο κρυπτογραφείται σε διακριτά σταθερού

μήκους μπλοκ. Το standard του AES χρησιμοποιεί μπλοκ 128 bit και το κλειδί για το 802.11 είναι επίσης ορισμένο στα 128 bit.

Αντίθετα με το TKIP, το CCMP είναι υποχρεωτικό για την υλοποίηση του 802.11i. Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης στο CCMP είναι γνωστό ότι είναι πολύ απαιτητική σε υπολογισμούς. Αυτό μπορεί να είναι ένα μεγάλο εμπόδιο για την ανάπτυξη συστημάτων συμβατών με το 802.11i εκτός αν κάποιος επεξεργαστής ειδικού σκοπού ή παρόμοια κυκλώματα αναπτυχθούν σε υλικό για την διαδικασία αυτή.
Οι δύο πιο πάνω αλγόριθμοι θεωρούνται τα θεμέλια της κρυπτογράφησης στα οποία βασίζεται η κρυπτογράφηση του 802.11i. Πάνω από αυτό το επίπεδο βρίσκεται ο μηχανισμός πιστοποίησης που κληρονομεί τα χαρακτηριστικά του από την αρχιτεκτονική του 802.1x .



Εικόνα 17: Σύγκριση WEP vs WPA

ΚΕΦΑΛΑΙΟ 5^{ο} : ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ

Στα κεφάλαια που αναλύσαμε παραπάνω είδαμε πως λειτουργούν τα ασύρματα δίκτυα, ποια σημεία τους είναι ευάλωτα και με ποιους τρόπους μπορούν να παραβιαστούν. Στο κεφάλαιο 3 εξετάσαμε έγκυρες μεθόδους που ένας κακόβουλος χρήστης μπορεί να χρησιμοποιήσει για να αποκτήσει πρόσβαση σε ασύρματα δίκτυα. Στο κεφάλαιο αυτό, θα αναλύσουμε τρόπους με τους οποίους τα ασύρματα δίκτυα μπορούν να ρυθμιστούν, ώστε να ελαττωθεί ο κίνδυνος για μια επιτυχημένη επίθεση.

Ένας εισβολέας ο οποίος έχει βάλει στόχο να θέσει το σύστημα μας σε κίνδυνο, σίγουρα θα έχει μια επιτυχημένη προσπάθεια. Σε ένα οικιακό περιβάλλον όμως, είναι σχεδόν απίθανο ότι θα έρθουμε αντιμέτωποι με αυτού του είδους των εισβολέων, αλλά για προληπτικούς λόγους, οι τεχνικές που παρουσιάζονται σε αυτό το κεφάλαιο, έχουν σχεδιαστεί για να ελαττώσουν τον κίνδυνο να γίνουμε στόχος ευκολίας. Το συγκεκριμένο κεφάλαιο εξετάζει το πώς να ρυθμίσουμε τις βασικές ρυθμίσεις ασφάλειας στο σημείο πρόσβασης που χρησιμοποιούμε. Υπάρχουν εύκολα και απλά βήματα τα οποία είναι επαρκή για τους χρήστες στο σπίτι, όπως είναι:

- Access Control
- Mac Filtering
- End-to-end encryption
- Intrusion Detection systems
- Χρήση VPNs
- ΧρήσηSSID (Service Set Identifier)
- Firewalls

Στις παραγράφους που ακολουθούν πιο κάτω, αναλύουμε λεπτομερώς καθένα από αυτά τα βήματα, έτσι ώστε να έχουμε την δυνατότητα να στήσουμε ένα ασφαλές ασύρματο δίκτυο. Για να μπορέσουμε να χρησιμοποιήσουμε το πιο υψηλό επίπεδο κρυπτογράφησης θα πρέπει να το ρυθμίσουμε.

5.1 Intrusion Detection system

Η ανίχνευση εισβολής (ID) αποτελείται από μια ποικιλία κατηγοριών και τεχνικών. Οι κύριες προσεγγίσεις περιλαμβάνουν τον καθορισμό ενός συστήματος, εάν αυτές έχουν προσβληθεί από ιούς ή από κακόβουλο κώδικα και εφαρμόζουν μεθόδους ώστε να καθαρίσουν την εισβολή του επιτιθέμενου στο δίκτυο. Η σάρωση για ανίχνευση ιών και η παρεμπόδιση εισβολής, χρησιμοποιούνται για να αντιμετωπίζουν τα προβλήματα των ιών και οι μηχανισμοί ανίχνευσης εισβολής και αντιμετώπιση, έχουν ως στόχο τις εισβολές των δικτύων.

Η ανίχνευση εισβολής και η αντιμετώπισή της, έχουν σαν καθήκον να παρακολουθούν τα συστήματα και να διαπιστώνουν εισβολές ή την μη κατάλληλη χρήση των συστημάτων και να ανταποκρίνονται σε αυτές. Η ανταπόκριση περιλαμβάνει την επισήμανση των κατάλληλων τμημάτων, ώστε να ληφθεί δράση, τον καθορισμό της σοβαρότητας επέκτασης ενός περιστατικού και να αποκαταστήσει τις επιδράσεις του περιστατικού. Επιπλέον ID είναι η ανίχνευση ανακριβών, ακατάλληλων και περίεργων δραστηριοτήτων. Η ανίχνευση εισβολής και η αντιμετώπισή της έχουν δυο βασικές ικανότητες:

- Τη δημιουργία και συντήρηση των συστημάτων ανίχνευσης εισβολής (IDSs), διαδικασίες παρακολούθησης των δικτύων και επισήμανση των περιστατικών.
- Τη δημιουργία μιας ομάδας για την αντιμετώπιση εισβολών σε ηλεκτρονικό υπολογιστή, για την ανάλυση της επισήμανσης ενός περιστατικού, την αντιμετώπιση σε ένα περιστατικό, αν η ανάλυση το επιβάλει και διαδικασίες κλιμακωτών μονοπατιών.

5.1.1 Αναφορά των IDSs

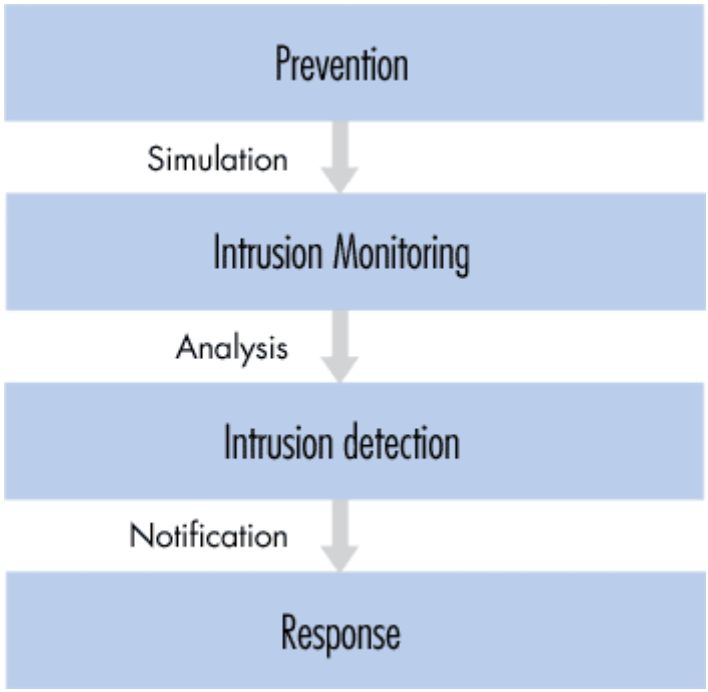
Συνοπτικά τα συστήματα ανίχνευσης εισβολής κάνουν αυτό που λέει το όνομά τους: εντοπίζουν πιθανές διεισδύσεις. Πιο ειδικά τα IDSsεργαλεία, έχουν ως στόχο στην ανίχνευση επιθέσεων κατά του υπολογιστή ή την μη καλή χρήση του υπολογιστή ή ειδοποιούν τα άτομα τα οποία είναι αρμόδια όταν ανιχνεύσουν κάτι περίεργο. Η εγκατάσταση ενός IDS σε ένα δίκτυο εξασφαλίζει το ίδιο αποτέλεσμα με την εγκατάσταση ενός συναγερμού σε ένα σπίτι. Με διάφορες μεθόδους το κάθε ένα από αυτά ανιχνεύουν την παρουσία ενός εισβολέα-διαρρήκτη και τα δυο στη συνέχεια εκδίδουν κάποιο είδος προειδοποίησης και συναγερμού.

Μολονότι που τα IDSsμπορούν να συνδυαστούν και να χρησιμοποιηθούν με τα firewalls (τείχη προστασίας), τα οποία αποβλέπουν στη ρύθμιση και τον έλεγχο της ροής των πληροφοριών από ένα δίκτυο και προς ένα δίκτυο, τα δυο αυτά εργαλεία δεν πρέπει να μπερδεύονται καθώς δεν είναι όμοια. Με βάση το προηγούμενο παράδειγμα, τα τείχη προστασίας (firewalls) μπορούν να θεωρηθούν ως ένας φύλακας ή ένας φράχτης μπροστά από ένα σπίτι. Προστατεύουν το δίκτυο και κάνουν προσπάθεια για την πρόληψη των παρεμβολών, αντιθέτως ταIDS εργαλεία ανιχνεύουν αν το δίκτυο είναι ή όχι υπό επίθεση ή εάν στην πραγματικότητα έχει παραβιαστεί.

Έτσι τα εργαλεία IDS αποτελούν άρρηκτα συνδεδεμένο μέρος της λεπτομερούς και πλήρης ασφάλειας του συστήματος. Δεν εγγυάται ολοκληρωτικά την ασφάλεια αλλά όταν συνδυαστεί με την πολιτική ασφαλείας δυνατών σημείων, την κρυπτογράφηση δεδομένων, την ταυτοποίηση του χρήστη, τον έλεγχο πρόσβασης και τα firewalls, μπορούν να ενδυναμώσουν σημαντικά την ασφάλεια του δικτύου.

Τα συστήματα ανίχνευσης εισβολής εξυπηρετούν τρεις βασικές λειτουργίες ασφάλειας: να παρακολουθούν, να ανιχνεύουν και να ανταποκρίνονται σε παράνομη δραστηριότητα. Μερικά συστήματα ανίχνευσης εισβολής μπορούν να στέλνουν ειδοποιήσεις έτσι ώστε ο διαχειριστής να λαμβάνει μια ειδοποίηση σχετικά με το συμβάν της επίθεσης, είτε με τη μορφή σελίδας, είτε με e-mail. Αρκετά IDSs δεν αναγνωρίζουν μόνο ένα συγκεκριμένο περιστατικό και εκδίδουν σήμα αλλά έχουν την ικανότητα να ανταποκρίνονται και αυτόματα με την εκδήλωση. Μια τέτοια αντίδραση μπορεί να περιλαμβάνει την αποσύνδεση του χρήστη, την απενεργοποίηση του λογαριασμού του ή την εκκίνηση διαφόρων σεναρίων. Κάποια από τα πιο γνωστά IDSs είναι τα παρακάτω:

- Sguil
- Snort
- Dragon Sensor
- OSSEC HIDS
- E-trust IDS
- Audit-Guard
- Cisco Secure IDS
- Symantec



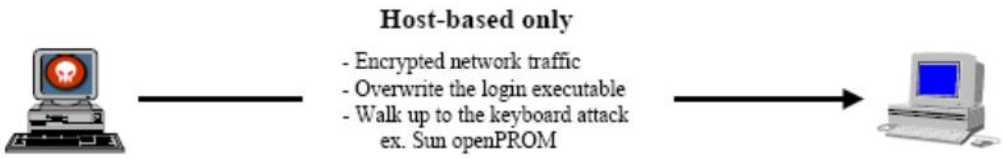
Εικόνα 18:Ενέργειες των Intrusion Detection Systems

Υπάρχουν διάφοροι τύποι IDSs. Οι πιο συνηθισμένοι τύποι IDSs είναι statistical anomaly detection, signature-based, host-based IDSs και τα network-based IDSs. Επειδή το καθένα από αυτά έχει τα συν και τα πλην του, καλό θα είναι να χρησιμοποιείται ένας συνδυασμός των host-based IDSs και των network-based IDSs.

5.1.2 Host-based IDS

Τα host-based IDSs ψάχνουν για είδη εισβολής στο τοπικό σύστημα του host. Συχνά χρησιμοποιούν τον μηχανισμό ελέγχου και καταγραφής του host ως πηγή πληροφοριών για ανάλυση. Συγκεκριμένα ψάχνουν για μη συνηθισμένη δραστηριότητα, που περιορίζεται στον τοπικό hostόπως login, περίεργη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές σε δικαιώματα του συστήματος. Η αρχιτεκτονική αυτή χρησιμοποιεί μηχανισμούς βασισμένους σε κανόνες για την ανάλυση της δραστηριότητας. Παραδείγματος χάρη, ένας τέτοιος κανόνας μπορεί να είναι ο εξής: δυνατότητα για πρόσβαση στο λογαριασμό του διαχειριστή είναι ισχυρή μόνο μέσω της εντολής του. Άρα, επιτυχημένες προσπάθειες

πρόσβασης στο λογαριασμό του διαχειριστή θα μπορούσαν να θεωρηθούν ως επίθεση.



Εικόνα 19: Λειτουργίες των host-based IDS

5.1.2.1 Πλεονεκτήματα

1. Ένα host-based IDS μπορεί να αποτελέσει πολύ ισχυρό εργαλείο ανάλυσης πιθανών επιθέσεων. Για παράδειγμα, πολλές φορές είναι σε θέση να πει τι ακριβώς έκανε ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιες ρουτίνες του συστήματος κάλεσε αντί για μια αόριστη υπόθεση ότι συνήθως παρέχουν πολύ πιο λεπτομερείς και σχετικές πληροφορίες από ότι τα network-based IDS
2. Τα host-based IDSs έχουν μικρότερους false positive ρυθμούς από ότι τα network-based. Αυτό συμβαίνει διότι το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο hosteίναι πολύ πιο εστιασμένο, παρά τα είδη κίνησης πακέτων που κυκλοφορούν σε ένα δίκτυο. Η ιδιότητα αυτή μπορεί να μειώσει την πολυπλοκότητα των μηχανισμών host-based.
3. Μπορούν να χρησιμοποιηθούν σε περιβάλλοντα που δεν χρειάζεται πλήρη ανίχνευση εισβολών ή όταν δεν υπάρχει διαθέσιμο εύρος ζώνης για επικοινωνία αισθητήρα-σταθμού ανάλυσης. Τα host-based IDSsείναι πλήρως αυτοσυντηρούμενα, κάτι που τους επιτρέπει σε ορισμένες περιπτώσεις να εκτελούνται από read-only (μόνο για ανάγνωση) μέσα. Έτσι οι εισβολείς μπορούν δύσκολα να εξουδετερώσουν το IDS.
4. Τέλος σε ένα host-based IDSsείναι πιο εύκολο να σχηματιστεί μια ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή την αίτηση αποσύνδεσης ενός επιτιθέμενου χρήστη.

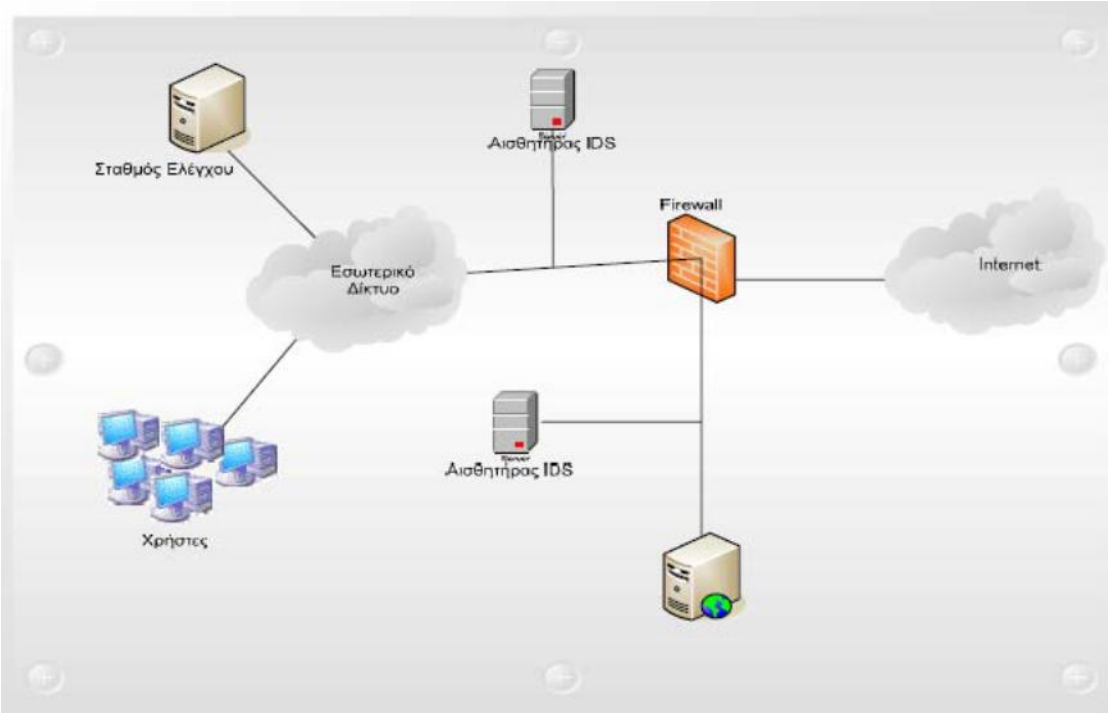
5.1.2.2 Μειονεκτήματα

1. Τα host-based IDSs απαιτούν εγκατάσταση στο σύστημα που θέλουμε να προστατεύσουμε. Αν έχουμε έναν server για παράδειγμα που πρέπει να τον προστατεύσουμε, θα πρέπει να εγκαταστήσουμε το IDSστο συγκεκριμένο server. Όπως προαναφέραμε, αυτό μπορεί να προκαλέσει και προβλήματα ασφάλειας μιας και το προσωπικό που είναι υπεύθυνο για την ασφάλεια του συστήματος ίσως να μην έχει πρόσβαση στο server όταν χρειαστεί.
2. Ένα άλλο πρόβλημα είναι ότι έχουν την τάση να εξαρτώνται από το υπάρχον σύστημα καταγραφής και ελέγχου του server. Εάν ο server δεν λειτουργεί έτσι ώστε η καταγραφή και ο έλεγχος να είναι σε ικανοποιητικό επίπεδο, θα πρέπει να γίνουν αλλαγές στις ρυθμίσεις του. Αυτό αποτελεί αρκετά μεγάλο πρόβλημα αλλαγής στη διαχείριση του server.
3. Τα συστήματα αυτά είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την δυνατότητα να προστατεύσουν ολόκληρα δικτυακά τμήματα με την χρήση host-based IDSs. Αντιθέτως θα πρέπει να επιλέξουν ποια συστήματα θα πρέπει να επιλέξουν και ποια όχι. Το γεγονός αυτό αφήνει μεγάλα κενά στην κάλυψη της ανίχνευσης εισβολών στο δίκτυο, αφού ένας κακόβουλος χρήστης σε ένα γειτονικό αλλά απροστάτευτο σύστημα μπορεί να υποκλέψει πληροφορίες ή οποιοδήποτε άλλο πολύτιμο υλικό από το δίκτυο.
4. Τέλος, ταhost-based IDSs είναι πιο ευάλωτα σε μεγαλύτερο βαθμό από τοπικούς περιορισμούς. Αγνοούν πλήρως το περιβάλλον του δικτύου, επομένως ο χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των hostπου προστατεύονται.

5.1.3 Network-based IDS

Τανetwork-based IDSs συλλαμβάνουν την κίνηση του δικτύου (πιο συχνά ή σε ολόκληρο το δίκτυο ή σε μικρά τμήματα σε αυτό) για τις λειτουργίες ανίχνευσης εισβολής. Το network-based IDS αποτελείται συνήθως από δυο μέρη: τους

αισθητήρες και τον σταθμό διαχείρισης/ανάλυσης. Ο αισθητήρας βρίσκεται σε ένα μέρος του δικτύου και παρακολουθεί για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον διαχειριστή του συστήματος δηλαδή στον διαχειριστή ασφάλειας του δικτύου. Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα. Δηλαδή λαμβάνουν όλη τη δικτυακή κίνηση και όχι μόνο ότι προορίζεται για τη δικιά τους IP διεύθυνση, αλλά και την κίνηση που διέρχεται από αυτούς, με σκοπό την περαιτέρω ανάλυση. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στο σταθμό διαχείρισης/ανάλυσης. Ο σταθμός διαχείρισης/ανάλυσης, μπορεί να δείξει τα σήματα κινδύνου που έλαβε από τους αισθητήρες ή να διεξάγει περαιτέρω ανάλυση.



Εικόνα 20: Διάταξη Network-Based IDS

5.1.3.2 Πλεονεκτήματα

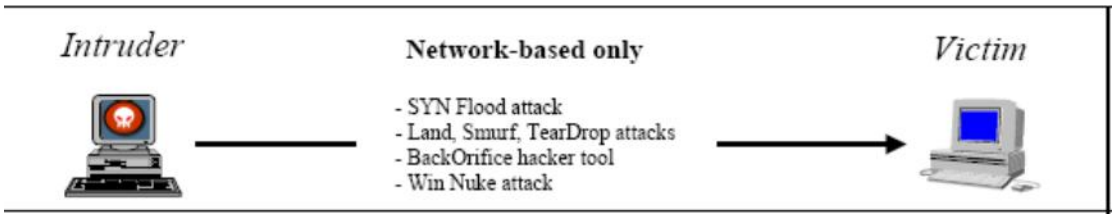
1. Τα συστήματα ανίχνευσης επιθέσεων έχουν την δυνατότητα να ανιχνεύσουν κάποιες από τις επιθέσεις που χρησιμοποιούν το δίκτυο. Είναι επαρκή για την ανίχνευση πρόσβασης.

2. Τα network-based IDSs τείνουν να είναι καλύτερα αυτοσυντηρούμενα από ότι τα host-based. Τρέχουν σε ένα συγκεκριμένο σύστημα και η εγκατάσταση τους είναι απλή και πραγματοποιείται σε μια τοποθεσία στο δίκτυο, που δίνει τη δυνατότητα παρακολούθησης ευαίσθητης κίνησης δεδομένων, χωρίς εξουσιοδότηση.
3. Ένα network–based IDSs, δεν απαιτεί μετατροπές στους server μιας επιχείρησης ή στους φιλοξενιτές (hosts) για να εγκατασταθεί. Αυτό είναι μεγάλο πλεονέκτημα γιατί συνήθως οι server έχουν κλειστές ανοχές όσον αφορά τη CPU, το I/O και τη χωρητικότητα του δίσκου. Επιπλέον, η εγκατάσταση λογισμικού ίσως δημιουργήσει προβλήματα λειτουργικότητας.
4. Τα network-based IDSs, δεν αποτελούν κρίσιμο παράγοντα για τη λειτουργικότητα του δικτύου και αυτό γιατί δεν λειτουργεί ως δρομολογητής ή ως κάποια άλλη κρίσιμη συσκευή. Άρα τυχόν αποτυχία στο σύστημα του IDS δεν θα έχει σημαντική επίδραση στην επιχείρηση.

5.1.3.2 Μειονεκτήματα

1. Έναnetwork-based IDSs, εξετάζει απλά τη δικτυακή κίνηση στον τομέα που είναι συνδεδεμένο και μόνο. Δεν μπορεί να ανιχνεύσει μια επίθεση που γίνεται σε διαφορετικό τμήμα του δικτύου. Το πρόβλημα αυτό γίνεται μεγαλύτερο σε ένα περιβάλλον με πολλαπλές δικτυώσεις Ethernet. Για να καλύψει τις ανάγκες του σε δικτυακή κάλυψη ένας μεγάλος οργανισμός θα πρέπει να αγοράσει πολλούς αισθητήρες, κάτι που σημαίνει επιπλέον κόστος.
2. Τανetwork-based IDSs, κατά κύριο λόγο χρησιμοποιούν ανάλυση υπογραφών για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι ανιχνεύονται κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά η μέθοδος αυτή δεν επαρκεί για τα πιο πολύπλοκα είδη επιθέσεων. Αυτές απαιτούν καλύτερη ικανότητα για ανάλυση του περιβάλλοντος.
3. Ένα τέτοιου είδους σύστημα ανίχνευσης επιθέσεων μπορεί να χρειαστεί να μεταδώσει μεγάλες ποσότητες δεδομένων στο κεντρικό σύστημα ανάλυσης. Κάποιες φορές, οποιοδήποτε αναλυόμενο πακέτο, παράγει μια μεγαλύτερη ποσότητα κίνησης δεδομένων. Πολλά τέτοια συστήματα χρησιμοποιούν επιθετικές μεθόδους ελάττωσης δεδομένων για να μειώσουν την παραγόμενη κίνηση επικοινωνίας.

4. Πολλές φορές είναι πιθανόν να αντιμετωπίσει δυσκολίες στο χειρισμό επιθέσεων, στη διάρκεια κρυπτογραφημένων συνόδων. Ευτυχώς είναι πολύ λίγες οι επιθέσεις που χρησιμοποιούνται κατά τη διάρκεια μιας κρυπτογραφημένης συνόδου.



Εικόνα 21: Λειτουργίες των network-based IDS

5.1.4 Signature-based IDS

Τα Signature-based IDSs ή αλλιώς knowledge based IDSs είναι χαρακτηριστικά ή υπογραφές που χαρακτηρίζουν μια επίθεση και αποθηκεύονται στο σύστημα μας για τυχόν ξανά αναφορά. Τα δεδομένα των περιστατικών που έχουν αποθηκευτεί από τον host και έχουν καταγραφεί στα μητρώα περιστατικών ή από την παρακολούθηση πακέτων του δικτύου, τα δεδομένα αυτά συγκρίνονται με τη βάση των υπογραφών των επιθέσεων και το σύστημα μας ενημερώνει αν υπάρχει ταυτοποίηση.

Μια αδυναμία των Signature-based IDSs είναι ότι δεν επιτυγχάνουν να χαρακτηρίζουν τις αργές επιθέσεις και οι οποίες διαρκούν μεγάλο διάστημα. Για να ανιχνευτούν τέτοιου είδους επιθέσεις χρειάζεται να δεσμευτούν μεγάλα ποσοστά πληροφορίας για αρκετό χρονικό διάστημα. Μια άλλη ευαισθησία των Signature-based IDSs είναι ότι ανιχνεύονται μόνο οι επιθέσεις των οποίων οι υπογραφές έχουν αποθηκευτεί στο βάση δεδομένων. Επιπρόσθετα, ένα αρνητικό των Signature-based IDSs είναι ότι η βάση δεδομένων χρειάζεται συχνά συντήρηση και αναβάθμιση σχετικά με τις νέες απειλές που κυκλοφορούν έτσι ώστε να παραμένει ενήμερη.

5.1.5 Statistical anomaly based IDS

Το Statistical anomaly based IDS ή αλλιώς Behavior-based IDSs ανιχνεύουν δυναμικά αποκλίσεις από τον σύνηθες τρόπο συμπεριφοράς των χρηστών και κρούουν τον κώδωνα του κινδύνου όταν μια λανθασμένη δραστηριότητα συμβαίνει.. Τα Statistical anomaly based IDS μαθαίνουν την κανονική ή την αναμενόμενη

συμπεριφορά που πρέπει να έχουν οι χρήστες και να αναλαμβάνουν να εντοπίσουν οποιαδήποτε διείσδυση συμβεί, παρατηρώντας τις αποκλίσεις του συστήματος από τον κανονικό τρόπο.

Με τον τρόπο αυτό, το IDSs αποκτά τα δεδομένα και ορίζει ένα προφίλ «κανονικής» χρήσης του δικτύου ή του hostπου παρακολουθείται. Η κατηγοριοποίηση αυτή γίνεται με στατιστικά δείγματα που λαμβάνονται κατά την διάρκεια μιας συνηθισμένης χρησιμοποίησης του συστήματος. Οι πληροφορίες χαρακτηριστικών χρησιμοποιούνται για να δημιουργήσει ένα κανονικό προφίλ που περιλαμβάνει την χρησιμοποίηση μνήμης, την χρησιμοποίηση της CPU και τα είδη των πακέτων του δικτύου. Με την προσέγγιση αυτή, οι νέες επιθέσεις μπορούν να ανιχνευτούν διότι προκαλούν περίεργα στατιστικά του συστήματος.

Τα υπέρ τωνBehavior-based IDSs είναι τα εξής:

- το σύστημα μπορεί δυναμικά να προσαρμοστεί σε καινούργιες επιθέσεις,
- δεν εξαρτώνται από συγκεκριμένα λειτουργικά συστήματα όπως τα Signature-based IDSs
- και βοηθούν να ανιχνευτούν διάφορα είδη επιθέσεων, τα οποία δεν περιλαμβάνουν μόνο επιθέσεις ασφάλειας

Αντίθετα μερικά μειονεκτήματα των Behavior-based IDSs είναι ότι:

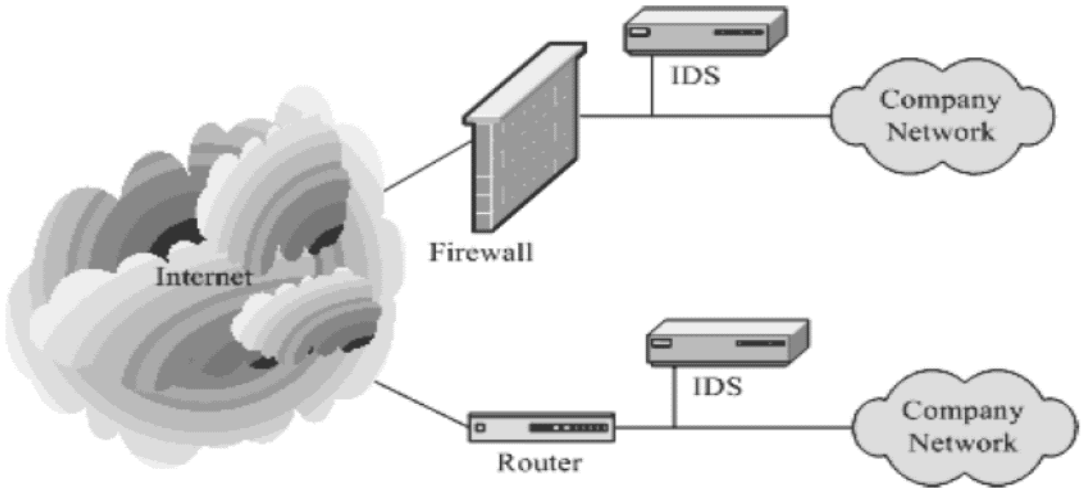
- δεν ανιχνεύουν επιθέσεις που δεν αλλάζουν σημαντικά τα χαρακτηριστικά του συστήματος
- και μερικές φορές ίσως ανιχνεύουν κατά λάθος περιστατικά που δεν είναι επιθέσεις αλλά προκαλούν στιγμιαία μεταβολή στο σύστημα.

5.1.6 Σε ποια σημεία της τοπολογίας του δικτύου πρέπει να τοποθετούνται τα IDS

Το που θα τοποθετήσουμε ένα IDS στο δίκτυό μας, εξαρτάται από την τοπολογία του δικτύου μας. Μπορεί να θέλουμε να τοποθετήσουμε ένα IDS σε ένα σημείο του δικτύου αλλά μπορούμε να χρησιμοποιήσουμε και περισσότερα σε διάφορα σημεία του δικτύου. Επίσης εξαρτάται από το είδος των δραστηριοτήτων εισβολής που θέλουμε να ανιχνεύσουμε: τις εσωτερικές, εξωτερικές ή και τις δύο. Για παράδειγμα

αν θέλουμε να ανιχνεύουμε μόνο τις εξωτερικές εισβολές διείσδυσης στο σύστημά μας, και αν έχουμε μόνο ένα δρομολογητή να συνδέεται στο internet, το καλύτερο μέρος για να τοποθετήσουμε ένα IDS είναι μέσα στο δρομολογητή ή το τοίχος προστασίας που χρησιμοποιούμε. Αν όμως έχουμε πολλαπλά μονοπάτια για τη σύνδεση μας στο διαδίκτυο, χρειάζεται να τοποθετήσουμε ένα IDS, σε κάθε ένα σημείο εισόδου.

Ωστόσο, αν θέλουμε να ανιχνεύσουμε τις εσωτερικές εισβολές, θα πρέπει να τοποθετήσουμε και από ένα IDS σε κάθε τμήμα του δικτύου. Σε πολλές περιπτώσεις όμως δεν χρειάζεται να έχουμε δραστηριότητα ανίχνευσης εισβολών σε όλα τα τμήματα του δικτύου και θα πρέπει να την περιορίζουμε μόνο στις ευαίσθητες περιοχές. Να θυμόμαστε ότι περισσότερα συστήματα ανίχνευσης εισβολών, απαιτούν περισσότερη δουλεία και περισσότερο κόστος συντήρησης. Η απόφαση μας όμως πραγματικά εξαρτάται από τη γενική πολιτική ασφάλειας που χρησιμοποιούμε για να προστατευτούμε από τους εισβολείς.



Εικόνα 22:Τα πιο συνηθισμένα μέρη όπου μπορούμε να τοποθετήσουμε IDS

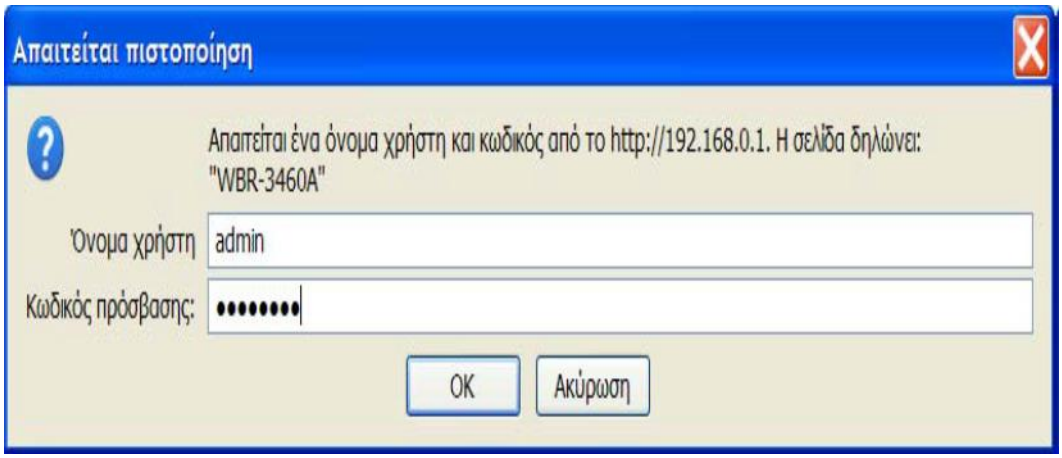
5.2 Access Control

Σύμφωνα με τον όμιλο ασφάλειας πληροφοριακών συστημάτων (ISSA) «έλεγχος πρόσβασης" είναι μια συλλογή από μηχανισμούς για περιορισμένη και ελεγχόμενη πρόσβαση συστήματος για να συγκεντρώσουμε πληροφορίες ή χαρακτηριστικά που

βασίζονται στην αναγνώριση του χρήστη ή των διαφόρων μελών που ανήκουν σε μια ομάδα.

Αρχικά πρέπει να αλλάξουμε το όνομα χρήστη (username) και τον κωδικό(password) που απαιτείται για να αποκτήσουμε πρόσβαση στην οθόνη με τις ρυθμίσεις διαμόρφωσης του ασύρματου δρομολογητή που χρησιμοποιούμε. Οι περισσότεροι ασύρματοι δρομολογητές που χρησιμοποιούμε για οικιακή χρήση, αποτελούνται από μια διεπαφή διαχείρισης μέσω του web. Η προεπιλεγμένη IP διεύθυνση της συσκευής που χρησιμοποιείται στο εσωτερικό δίκτυο είναι σχεδόν πάντα 192.168.0.1. Το να ανακαλύψουμε πιο είναι το προεπιλεγμένο username και password για τον κάθε κατασκευαστή δεν είναι πολύ δύσκολο.

Ο εξοπλισμός συνήθως είναι ρυθμισμένος με κάτι σαν «admin» για username και password για το password. Ακόμα και χωρίς καμιά βασική γνώση για τον κατασκευαστή ή την συσκευή, ένας επιτιθέμενος μπορεί να ανακαλύψει στα τυφλά το username και το password σε λιγότερο από δέκα προσπάθειες. Με την προεπιλεγμένη IP διεύθυνση και τα προεπιλεγμένα username και password διαχείρισης, ο ασύρματος δρομολογητής μας μπορεί να υποκλαπεί ακόμα και από αρχάριους.



Εικόνα 23: Πρόσβαση στον ασύρματο δρομολογητή

Σιγουρευτείτε ότι αλλάξατε το username σε κάτι που μόνο εσείς θα μπορούσατε να γνωρίζετε, κάτι μοναδικό. Μετονομάζοντας τον λογαριασμό του διαχειριστή στον υπολογιστή μας, πρέπει να διαλέξουμε ένα username που δεν θα είναι τόσο εύκολο να το μαντέψει κάποιος όπως είναι το «admin» ή οποιοδήποτε άλλο προεπιλεγμένο username ήταν. Στη συνέχεια χρειάζεται να διαλέξουμε ένα ισχυρό password το οποίο δεν θα είναι εύκολο να μαντεύσει κάποιος ή να το σπάσει. Ο δρομολογητής

που εμείς χρησιμοποιούμε, μας δίνει την δυνατότητα να αλλάξουμε μόνο το password.

Τέλος καλό θα ήταν να αλλάξουμε και την εσωτερική διεύθυνση IP του υπό-δικτύου μας αν αυτό μας επιτρέπεται. Το 192.168.x.x εύρος διεύθυνσης είναι μόνο για εσωτερική χρήση. Ένα μεγάλο ποσοστό αυτών που χρησιμοποιούν αυτό το εύρος διεύθυνσης, χρησιμοποιούν το 192.168.0.x για το υπό-δίκτυο τους, το οποίο είναι πολύ εύκολο να μαντέψει ένας επιτιθέμενος. Μπορούμε να χρησιμοποιήσουμε οποιοδήποτε αριθμό από το 0 έως το 254 για την Τρίτη οκτάδα , έτσι διαλέξτε κάτι όπως 192.168.71.x, έτσι ώστε οι τυχών επιτιθέμενοι να χρειαστεί να «κουραστούν» περισσότερο.

Στόχος είναι να δυσκολέψουμε τους επιτιθέμενους ή το κακόβουλο λογισμικό στο να διεισδύσουν στο σύστημά μας. Τίποτα δεν κάνει το δίκτυο μας 100% ανθεκτικό σε έναν εισβολέα. Αλλά με το να θέτουμε πολλαπλά επίπεδα άμυνας, όπως σύνθετα password, προσωπικά firewalls, λογισμικό antivirus και άλλα μέτρα ασφάλειας, μπορούμε να το μετατρέψουμε σε αρκετά σκληρότερο ώστε να μην μας ενοχλούν διάφοροι κακόβουλοι χρήστες.

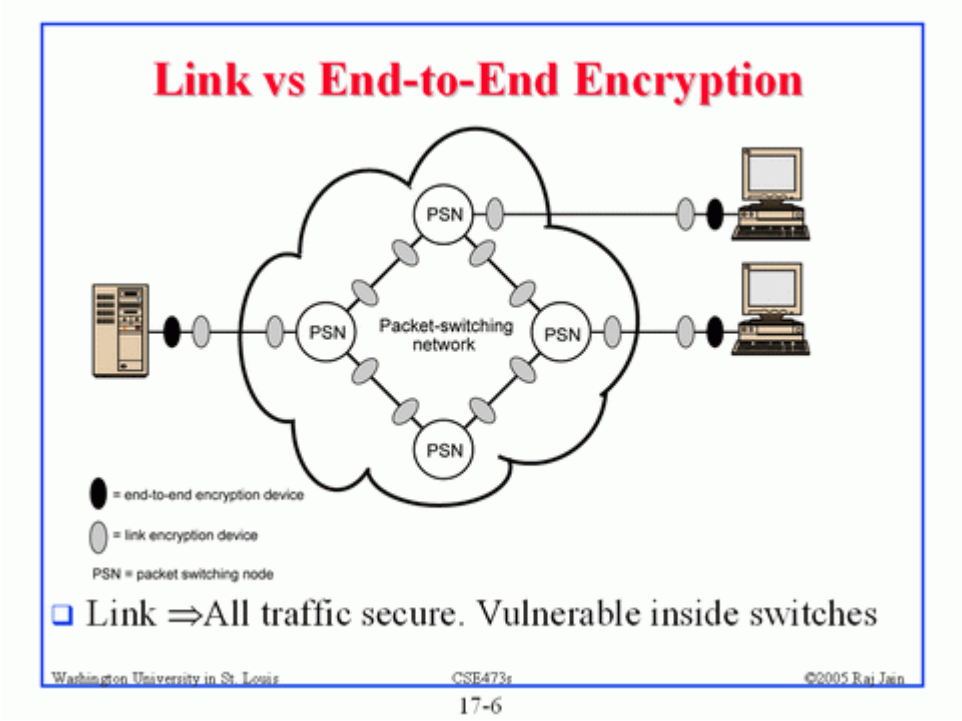
5.3 End-to-end Encryption

Τα «ευάλωτα» δεδομένα που ταξιδεύουν σε ένα δίκτυο, κρυπτογραφούνται με ασφάλεια από το σημείο που θα γίνει η εισαγωγή τους μέχρι το σημείο που θα γίνει η επεξεργασία τους. Ως ευαίσθητα δεδομένα χαρακτηρίζονται κυρίως το όνομα χρήστη, ο κωδικός πρόσβασης, αριθμός πιστωτικής κάρτας και διάφορα άλλα. Ο αρχικός σταθμός κρυπτογραφεί τα δεδομένα και στη συνέχεια τα δεδομένα, σε κρυπτογραφημένη μορφή, διαβιβάζονται αμετάβλητα μέσα από το δίκτυο προς το σταθμό προορισμού. Ο σταθμός προορισμού διαμοιράζεται ένα κλειδί με το σταθμό αποστολής και είναι σε θέση να αποκρυπτογραφήσει τα δεδομένα.

Τα κρυπτογραφικά πρωτόκολλα που υλοποιούνται και στην πηγή και στον προορισμό ονομάζονται πρωτόκολλα από άκρο-σε-άκρο (end-to-end protocols). Αν η διαδικασία της κρυπτογράφησης υλοποιείται σε κάθε κόμβο ξεχωριστά, κατά μήκος του μονοπατιού από την προέλευση στον προορισμό, τότε το πρωτόκολλο ονομάζεται πρωτόκολλο συνδέσμου (link protocol).

Για παράδειγμα το πρωτόκολλο Telnet είναι ένα πρωτόκολλο του επιπέδου εφαρμογών που επιτρέπει στους χρήστες να αποκτούν ένα εικονικό τερματικό με ένα απομακρυσμένο host. Αυτό είναι ένα end-to-end πρωτόκολλο. Ενώ το IP είναι ένα πρωτόκολλο επιπέδου δικτύου, όπου οδηγεί τα μηνύματα από τον host σε οποιονδήποτε από τους γείτονες του.

Τα πρωτόκολλα αυτά μπορεί να είναι κρυπτογραφικά πρωτόκολλα. Αν η διαδικασία της κρυπτογράφησης γίνεται μόνο στην πηγή και τον προορισμό, τότε το πρωτόκολλο είναι end-to-end πρωτόκολλο και η κρυπτογράφηση που χρησιμοποιείται είναι end-to-end κρυπτογράφηση. Εάν η διαδικασία της κρυπτογράφησης συμβαίνει σε κάθε ένα host ξεχωριστά κατά μήκος του μονοπατιού από την πηγή στον προορισμό, τότε το πρωτόκολλο ονομάζεται link και η κρυπτογράφηση που χρησιμοποιείται ονομάζεται link κρυπτογράφηση.



Εικόνα 24: Link vs End-to-end κρυπτογράφηση

Στην κρυπτογράφηση end-to-end, ο φιλοξενιτής (host) ή το τερματικό της πηγής κρυπτογραφεί τα δεδομένα. Τα δεδομένα με την κρυπτογραφημένη τους μορφή μεταφέρονται κατά μήκος του δικτύου στον host ή το τερματικό του προορισμού. Ο προορισμός μοιράζεται ένα κλειδί με την πηγή, ώστε να μπορεί να αποκρυπτογραφεί τα δεδομένα. Αυτή η προσέγγιση φαίνεται ότι διασφαλίζει τη μεταφορά των δεδομένων εναντίων των επιθέσεων που συμβαίνουν στο επίπεδο δικτύου.

Με την end-to-end κρυπτογράφηση, τα δεδομένα του χρήστη είναι ασφαλή, όμως το σχέδιο της κίνησης δεν είναι, επειδή οι επικεφαλίδες των πακέτων μεταφέρονται «καθαρές». Από την άλλη πλευρά η end-to-end κρυπτογράφηση παρέχει ένα σημαντικό βαθμό επικύρωσης. Αν δύο τερματικά συστήματα μοιράζονται ένα κρυπτογραφημένο κλειδί, ο παραλήπτης είναι σίγουρος ότι οποιοδήποτε μήνυμα λαμβάνει από ένα εικαζόμενο αποστολέα είναι σωστό, γιατί μόνο με τον αποστολέα μοιράζεται το αξιόπιστο κλειδί.

Για να επιτύχουμε υψηλό βαθμό ασφάλειας χρειάζεται ο συνδυασμός και της end-to-end κρυπτογράφησης αλλά και της link κρυπτογράφησης. Όταν χρησιμοποιούνται και τα δύο αυτά είδη κρυπτογράφησης, ο host κρυπτογραφεί το μέρος του πακέτου με τα δεδομένα του χρήστη, χρησιμοποιώντας το κλειδί της end-to-end κρυπτογράφησης. Στη συνέχεια όλο το πακέτο κρυπτογραφείται χρησιμοποιώντας το κλειδί της link κρυπτογράφησης.

Καθώς το πακέτο ταξιδεύει μέσα στο δίκτυο, κάθε κόμβος που το λαμβάνει, το αποκρυπτογραφεί με το κλειδί της link κρυπτογράφησης, για να διαβάσει την επικεφαλίδα και στη συνέχεια κρυπτογραφεί ξανά ολόκληρο το πακέτο για να το στείλει στην επόμενη σύνδεση. Έτσι, ολόκληρο το πακέτο είναι ασφαλές εκτός από τη χρονική περίοδο που αυτό βρίσκεται στην μνήμη πακέτων του κάθε κόμβου, όπου η επικεφαλίδα του πακέτου είναι «καθαρή». Ο παρακάτω πίνακας συνοψίζει τα χαρακτηριστικά των κλειδιών των δύο στρατηγικών κρυπτογράφησης.

Link Encryption	End-to-end encryption
Ασφάλεια μεταξύ των ακραίων και των ενδιάμεσων συστημάτων	
Το μήνυμα εκτίθεται στον hostπου αποστέλλεται.	Το μήνυμα κρυπτογραφείται στο hostπου αποστέλλεται.
Το μήνυμα εκτίθεται στους ενδιάμεσους κόμβους.	Το μήνυμα κρυπτογραφείται στους ενδιάμεσους κόμβους.
Ρόλος του χρήστη	
Εφαρμόζεται από τον αποστολέα.	Εφαρμόζεται από την διαδικασία αποστολής.
Διάφανες για τον χρήστη.	Ο χρήστης εφαρμόζει την κρυπτογράφηση.
Ο host συντηρεί τη διαδικασία κρυπτογράφησης.	Ο χρήστης πρέπει να ερμηνεύσει τον αλγόριθμο.
Μια διαδικασία για όλους τους χρήστες.	Ο χρήστης επιλέγει το σύστημα κρυπτογράφησης.
Μπορεί να γίνει στις συσκευές υλικού (hardware).	Ανάμειξη λογισμικού
Η όλα ή κανένα από τα μηνύματα κρυπτογραφούνται.	Ο χρήστης επιλέγει σε κάθε μήνυμα τι θα κρυπτογραφήσει και τι όχι.
Όσον αφορά την εφαρμογή	
Απαιτεί ένα κλειδί ανά ζεύγος (host-ενδιάμεσου κόμβου, ενδιάμεσου κόμβου-ενδιάμεσου κόμβου).	Απαιτείται ένα ζεύγος κλειδιών για κάθε χρήστη
Παρέχει επικύρωση του host	Παρέχει επικύρωση χρήστη

5.4 SSID Απόκρυψη

Τα περισσότερα ασύρματα δίκτυα από προεπιλογή μπορούν να μεταδώσουν την πληροφορία σε οποιονδήποτε ακούει εκείνη τη στιγμή. Όσοι όμως μελετάμε περισσότερο την ασφάλεια των ασύρματων δικτύων θεωρούμε ότι πρέπει να κρύβουμε το SSID. Παρατηρήθηκε ότι αν δεν εκπέμπεται το SSID, η ύπαρξη του

ασύρματου δικτύου μπορεί κάπως να καλυφθεί. Αυτή η κάλυψη θα απαιτούσε από τον πελάτη να στέλνει έλεγχο για οποιοδήποτε ασύρματο δίκτυο είναι διαθέσιμο.

Στα περισσότερα IEEE δίκτυα, η ύπαρξη του SSID προϋποθέτει την ύπαρξη ασύρματου sniffer57 και αυτό διότι το SSID είναι μέρος της διαδικασίας σύνδεσης σε ένα ασύρματο δίκτυο. Το SSID αναπαρίσταται στην επικεφαλίδα ενός ασύρματου απαντητικού πλαισίου ελέγχου. Αυτή η πληροφορία μπορεί να διαβαστεί από οποιοδήποτε sniffing πρόγραμμα και με το να την κρύψουμε μπορούμε να νικήσουμε οποιεσδήποτε τέτοιου είδους προσπάθειες.

Ακόμα και αν το SSID είναι καλυμμένο, κάθε φορά που ένας πελάτης θέλει να συνδεθεί σε ένα δίκτυο, θα στέλνει όλες τις ρυθμίσεις σύνδεσης, συμπεριλαμβανομένου και του SSID έξω στην περιοχή σαν μέρος της διαδικασίας ελέγχου. Πολλοί προμηθευτές έχουν το προεπιλεγμένο SSID στον εξοπλισμό τους. Αυτό είναι ένα από τα πρώτα βήματα που ακολουθούν οι «hackers» για να εκμεταλλευτούν ένα ασύρματο δίκτυο. Μερικές εταιρίες χρησιμοποιούν πολύ απλά SSID ονόματα όπως Wireless, WLAN.

Η κύρια λειτουργία του Service Set Identifier (SSID) είναι η αναγνώριση του δικτύου, όπως αναφέρει το όνομα του. Όταν η τερματική συσκευή ενός πελάτη θέλει να συνδεθεί σε ένα δίκτυο, πρέπει να έχει μια ρύθμιση αναγνώρισης ώστε να της επιτρέπει να γνωρίζει ποια δίκτυα είναι διαθέσιμα για να συνδεθεί και πως αυτά λειτουργούν. Όταν τα ασύρματα πρότυπα δημιουργήθηκαν η IEEE είχε προβλέψει ότι μπορεί να υπάρχουν περισσότερα από ένα ασύρματα δίκτυα στην ίδια εμβέλεια. Αυτό οδήγησε στη δημιουργία του SSID ώστε να ξεχωρίζουμε τα ασύρματα δίκτυα μεταξύ τους. Στις μέρες μας με την πληθώρα των ασύρματων δικτύων που υπάρχουν αυτό έχει γίνει αναγκαιότητα. Αυτός είναι λοιπόν ο σκοπός του SSID: αναγνώριση δικτύων.

Ένα μεγάλο βήμα που χρειάζεται να κάνουμε για να ασφαλίσουμε το οικιακό μας ασύρματο δίκτυο είναι να μην ανακοινώνουμε ότι έχουμε ένα. Τα δημόσια ή τα εταιρικά δίκτυα ίσως χρειάζεται να εκπέμπουν την ύπαρξή τους, ώστε οι καινούργιες ασύρματες συσκευές να μπορούν να τα ανιχνεύσουν και να συνδεθούν σε αυτά. Ωστόσο στο σπίτι μας θα πρέπει να προσπαθήσουμε να εμποδίσουμε τις ύπουλες ασύρματες συσκευές από το να ανιχνεύσουν και να συνδεθούν στο δίκτυό μας.

Κάθε ασύρματος δρομολογητής ή σημείο πρόσβασης έχει ένα Service Set Identifier (SSID). Βασικά το SSID είναι το όνομα του ασύρματου δικτύου. Από προεπιλογή οι ασύρματοι δρομολογητές και σημεία πρόσβασης εκπέμπουν ένα σήμα που λέγεται beacon κάθε 1/10 του δευτερολέπτου και το οποίο περιλαμβάνει το SSID μαζί με άλλες πληροφορίες. Αυτό είναι το beacon που οι ασύρματες συσκευές ανιχνεύουν και το οποίο τους παρέχει πληροφορίες που χρειάζονται για να συνδεθούν στο δίκτυο. Για να ρυθμίσουμε τις συσκευές στο ασύρματο δίκτυό μας αντί να βασιζόμαστε στην εκπομπή του σήματος beacon, μπορούμε να τις ρυθμίσουμε χειροκίνητα με το επιθυμητό SSID και άλλες συναφής πληροφορίες σε κάθε πελάτη ώστε να τους επιτρέψουμε τη σύνδεση στο δίκτυό μας.

Η κάθε συσκευή έχει συνήθως ως προεπιλεγμένο SSID το όνομα του κατασκευαστή της όπως για παράδειγμα Linksys, Netgear, CONNX και διάφορα άλλα. Στην παρακάτω εικόνα βλέπουμε τα SSID διαφόρων δικτύων που ανιχνεύει η ασύρματη κάρτα δικτύου μας. Ακόμα και αν είναι απενεργοποιημένη η εκπομπή του SSID, είναι σημαντικό να μην χρησιμοποιούμε το προεπιλεγμένο SSID. Οι κατασκευαστές του ασύρματου εξοπλισμού είναι μετρημένοι οπότε δεν θα πάρει πολύ χρόνο για να μαντέψει κάποιος το πιθανό SSID.

5.5 Firewalls

Ένα ασύρματο δίκτυο θα πρέπει οπωσδήποτε να θεωρείται μη ασφαλές και μέρος του Internet. Στην περίπτωση αυτή ένα τείχος προστασίας είναι ικανό να βοηθήσει στην εξάλειψη των κινδύνων ασφαλείας που το δίκτυο διατρέχει. Ανάλογα με την εγκατάσταση και το είδος της πολιτικής που ακολουθείται, ένα τείχος προστασίας (firewall) να εμποδίσει τις μη εξουσιοδοτημένες αιτήσεις. Με αυτό τον τρόπο δημιουργείται ένα φυσικό εμπόδιο για τους εισβολείς, οι οποίοι μπορεί να ελέγχουν το ασύρματο δίκτυο και να προσπαθούν να εισχωρήσουν στον εσωτερικό δίσκο.

Τα τείχη προστασίας μπορεί να είναι ή softwareή hardware. Η χρήση και των δυο θα ήταν το ιδανικό. Τώρα όμως τα router έχουν ενσωματωμένο firewallκαι παρέχεται η δυνατότητα για ενεργοποίηση / απενεργοποίηση του. Πέρα από την ασφάλεια που παρέχουν τα τείχη προστασίας όσο αφορά την μείωση πρόσβασης στο δίκτυο και τον

προσωπικό υπολογιστή, εγκρίνει και την ασφαλή απομακρυσμένη πρόσβαση μέσα από μηχανισμούς αυθεντικοποίησης.

5.6 MAC Filtering

Το φιλτράρισμα της διεύθυνσης MAC (είτε αυτό γίνεται με φυσικό τρόπο είτε με τη βοήθεια κάποιου είδους λογισμικού) παρέχει ένα βασικό έλεγχο σχετικά με τους σταθμούς που θέλουν να συνδεθούν στο σημείο πρόσβασης μας. Μια διεύθυνση MAC (Media Access Control) είναι η φυσική διεύθυνση, μοναδικό αναγνωριστικό για κάθε υπολογιστή. Είναι ένας 48μπιτος αριθμός καθορισμένος από τον κατασκευαστή. Τα 48 μπιτ διασπώνται σε 24 μπιτ που αποτελούν το μοναδικό αναγνωριστικό του κατασκευαστή, εκχωρημένα από την IEEE και τα υπόλοιπα 24 αποτελούν μια μοναδική κάρτα αναγνώρισης.

Χρησιμοποιούμε την διεύθυνση MAC για να περιορίσουμε την πρόσβαση που βασίζεται στις λίστες ελέγχου πρόσβασης MAC (ACLs), οι οποίες είναι αποθηκευμένες και διανεμημένες σε πολλά σημεία πρόσβασης. Ωστόσο μερικά άλλα σημεία πρόσβασης έχουν την ικανότητα να φιλτράρουν μόνο έμπιστες διευθύνσεις MAC. Το φιλτράρισμα της διεύθυνσης MAC αποδέχεται ή απορρίπτει την πρόσβαση σε ένα υπολογιστή χρησιμοποιώντας τη λίστα από τις επιτρεπτές διευθύνσεις MAC.

Για να εγκαθιδρύσουμε MAC Address Filtering, σαν διαχειριστές του ασύρματου τοπικού δικτύου μας, θα πρέπει να διαμορφώσουμε μια λίστα από πελάτες, στους οποίους θα επιτρέπεται η πρόσβαση στο ασύρματο δίκτυο μας. Αρχικά μπαίνουν οι MAC διευθύνσεις των λειτουργικών συστημάτων των πελατών και στη συνέχεια μπαίνουν εκείνες οι διευθύνσεις των ασύρματων σημείων πρόσβασης ή των δρομολογητών που χρησιμοποιούνται για να έχουμε πρόσβαση στην οθόνη με τις ρυθμίσεις τους. Τέλος ενεργοποιούμε την επιλογή του φιλτραρίσματος.

Από τη στιγμή που έχει ενεργοποιηθεί το MAC Filtering, όταν το ασύρματο σημείο πρόσβασης ή ο δρομολογητής λάβει αίτηση από κάποιον υπολογιστή για να ενταχθεί στο WLAN, συγκρίνει την διεύθυνση MAC του πελάτη με τον κατάλογο διευθύνσεων MAC του διαχειριστή. Οι πελάτες των οποίων οι διευθύνσεις MAC

είναι στον κατάλογο επικυρώνονται κανονικά, ενώ οι πελάτες που δεν είναι στη λίστα αρνούνται οποιαδήποτε πρόσβαση στο WLAN.

Το φιλτράρισμα μιας Ethernet MAC διεύθυνσης από μόνο του δεν αποτελεί ισχυρό μηχανισμό άμυνας, επειδή παρόλο που ένας πελάτης μπορεί να μεταφέρει την δική του διεύθυνση MAC «καθαρή», κάποιος επιτιθέμενος μπορεί πολύ εύκολα να την "συλλάβει" και να την τροποποιήσει ώστε να αποκτήσει πρόσβαση σε κάποιο ασύρματο δίκτυο. Μπορούμε να προσθέσουμε στη μνήμη μια διεύθυνση δικτύου (πριν κάνουμε οποιαδήποτε αλλαγή στη μνήμη θα πρέπει να έχουμε κάνει ένα back-up) ή εναλλακτικά μπορούμε να χρησιμοποιήσουμε λογισμικό για αλλαγή διεύθυνσης MAC.

Για την προστασία του συστήματος μας από MAC Spoofing επίθεση, δύο είναι οι λύσεις που μπορούμε να εφαρμόσουμε. Η μία λύση είναι να ανιχνεύσουμε το MAC Spoofing, και η άλλη λύση είναι να κάνουμε το σύστημα μας ανθεκτικότερο όσον αφορά τα σημεία πρόσβασης και τις ξεχωριστές μηχανές. Ένας γρήγορος τρόπος να το ανακαλύψουμε, αν αυτό συμβαίνει είναι να τρέξουμε RARP εναντίον της ύποπτης MAC. Αν μας επιστραφούν περισσότερες από μια IP διευθύνσεις, τότε κάποια από αυτές θα θέλει περισσότερη ανάλυση.

5.7 Virtual Private Networks (VPNs)

Ένα ιδιωτικό δίκτυο αποτελείται από υπολογιστές που ανήκουν σε ένα μόνο οργανισμό και μοιράζονται πληροφορίες αποκλειστικά μόνο μεταξύ τους. Οι χρήστες του ιδιωτικού δικτύου είναι βέβαιοι ότι αυτοί είναι οι μοναδικοί που χρησιμοποιούν το ιδιωτικό δίκτυο και ότι όλες τις πληροφορίες που στέλνονται μεταξύ τους, μπορούν να τις δουν μόνο όσοι ανήκουν στο ιδιωτικό δίκτυο.

Ένα ιδιωτικό εικονικό δίκτυο (Virtual Private Network- VPN) είναι κάτι ανάμεσα σε ένα ιδιωτικό και ένα δημόσιο δίκτυο. Το VPN μας επιτρέπει να δημιουργούμε ένα ασφαλές ιδιωτικό δίκτυο βασισμένο πάνω σε ένα δημόσιο δίκτυο όπως είναι το Internet. Μπορούμε να δημιουργήσουμε ένα VPN χρησιμοποιώντας κάποιο λογισμικό ή συσκευές υλικού ή ακόμα και συνδυασμό και των δύο, ώστε να δημιουργηθεί ένας ασφαλής σύνδεσμος ανάμεσα στους κόμβους του δημόσιου

δικτύου. Αυτό επιτυγχάνεται με κρυπτογράφηση, επικύρωση, μεταφορά των πακέτων μέσω τούνελ και τοίχων προστασίας.

Το VPN ονομάζεται “εικονικό” διότι εξαρτάται από την χρησιμοποίηση εικονικών συνδέσεων, οι οποίες είναι προσωρινές συνδέσεις που στην πραγματικότητα δεν υπάρχει φυσική παρουσία, αλλά βασίζονται σε πακέτα που δρομολογούνται μέσω διαφόρων μηχανών στο διαδίκτυο σε ad hoc δίκτυα. Υπάρχουν πολλοί τρόποι για να ταξινομήσει κάποιος τα VPNs, αλλά οι τρείς είναι οι βασικοί τύποι. Ασφαλής εικονικές συνδέσεις δημιουργούνται μεταξύ:

- δυο μηχανών
- μεταξύ δυο δικτύων
- μιας μηχανής και του δικτύου

Επίσης υπάρχουν διάφορες τεχνολογίες που χρησιμοποιούν τα VPNs για να προστατεύουν τα δεδομένα μας καθώς αυτά ταξιδεύουν διάμεσο του Internet. Οι πιο σημαντικές από αυτές τις τεχνολογίες είναι τα τείχη προστασίας, η επικύρωση, η κρυπτογράφηση και τα τούνελ.

Τα πιο κοινά και ευρέως χρησιμοποιούμενα πρωτόκολλα για τα VPN τούνελ είναι:

- ***IPSec***: Είναι το πιο ευρέως αναγνωρισμένο, υποστηρίξιμο και ευρέως αναγνωρισμένο όλων των πρωτοκόλλων VPN. Είναι η ιδανική επιλογή για λόγους δια λειτουργικότητας. Το IPSec είναι ένα πλαίσιο ανοιχτών προτύπων, που παράγουν μια ασφαλή σουίτα πρωτοκόλλων, που μπορούν να τρέχουν πάνω από την υπάρχουσα IP συνδεσιμότητα. Παρέχει επικύρωση των δεδομένων και υπηρεσίες κρυπτογράφησης στο τρίτο επίπεδο του μοντέλου OSI και μπορούν να εφαρμοστούν σε οποιαδήποτε συσκευή επικοινωνεί μέσω IP. Το πρωτόκολλο αυτό περιλαμβάνει τρία κύρια μέρη: την Authentication Header (AH), Encapsulating Security Payload (ESP), και Internet Key Exchange (IKE).

  Το AH προστίθεται μετά την IP επικεφαλίδα, παρέχει επικύρωση σε επίπεδο πακέτων και υπηρεσίες ακεραιότητας, διασφαλίζοντας έτσι ότι το πακέτο δεν έχει πειραχτεί από την προέλευση μέχρι τον προορισμό. Το ESP παρέχει εμπιστευτικότητα, επικύρωση των δεδομένων προέλευσης, ακεραιότητα και περιορισμένη εμπιστευτικότητα ροής πληροφορίας. Τέλος το IKE

διαπραγματεύεται διάφορες ενώσεις ασφάλειας που περιγράφουν τη χρήση των υπηρεσιών ασφάλειας μεταξύ των συμμετεχόντων φορέων.

- ***GRE***: Το Generic Routing Encapsulation (GRE), είναι ένα πρωτόκολλο που αναπτύχθηκε από τη Cisco και χρησιμοποιείται στη δικτύωση μέσω τούνελ, για την κίνηση μεταξύ διαφορετικών ιδιωτικών δικτύων. Το GRE χρησιμοποιείται συχνά σε συνδυασμό με τα πρωτόκολλα κρυπτογράφησης επιπέδου δικτύου, ώστε να παρέχει και ενθυλάκωση των μη-IP πρωτοκόλλων αλλά και κρυπτογράφηση που παρέχονται από άλλα πρωτόκολλα όπως το IPSec.
- ***PPTP***: Το πρωτόκολλο τούνελ από σημείο σε σημείο (Point-to-Point Tunneling Protocol) είναι ένα ιδιόκτητο πρωτόκολλο που αναπτύχθηκε από τη Microsoft και προορίζεται για επικοινωνίες μέσω VPN. Το PPTP προσφέρει ταυτοποίηση χρήστη, χρησιμοποιώντας πρωτόκολλα επικύρωσης όπως MS-CHAP, CHAP, SPAP, PAP. Το PPTP προσφέρει την ευελιξία που παρέχουν και οι άλλες λύσεις αλλά δεν διαθέτει το ίδιο επίπεδο δια λειτουργικότητας, όπως τα άλλα πρωτόκολλα VPN, αλλά η χρήση του είναι εύκολη.
- ***L2TP***: Αναπτύχθηκε από κοινού από τη Cisco, τη Microsoft και τη 3Com. Το L2TP υποσχέθηκε να αντικαταστήσει το PPTP. Ουσιαστικά είναι ένας συνδυασμός του PPTP και του Cisco Layer Two Forwarding (L2F), δηλαδή η συγχώνευση και των δύο σε ένα ενιαίο πρότυπο. Το L2TP χρησιμοποιείται για να δημιουργηθεί ένα τούνελ PPTP πάνω από ένα δημόσιο IP δίκτυο. Βασίζεται στο PPTP, για τη δημιουργία μιας dial-up σύνδεσης, χρησιμοποιώντας PAP ή CHAP επικύρωση. Το πρωτόκολλο δεν χρησιμοποιεί κρυπτογράφηση από μόνο του αλλά μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλα πρωτόκολλα ή με μηχανισμούς κρυπτογράφησης σε επίπεδο εφαρμογών.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην συγκεκριμένη πτυχιακή εργασία, μελετήθηκε η ασφάλεια του 802.11 και 802.16 προτύπου, που χρησιμοποιείται στα ασύρματα δίκτυα. Μελετήθηκαν τα πιο γνωστά είδη επιθέσεων που συμβαίνουν στα ασύρματα δίκτυα. Στη συνέχεια προτάθηκαν τα

βασικά μέτρα ασφαλείας που πρέπει να εφαρμόζουμε ώστε να αποτρέπουμε το δίκτυο μας από το να πέφτει θύμα σε τέτοιου είδους επιθέσεις.

Στα κεφάλαια που αναλύσαμε παραπάνω είδαμε πως λειτουργούν τα ασύρματα δίκτυα, ποια σημεία τους είναι ευάλωτα και με ποιους τρόπους μπορούν να παραβιαστούν. Στο κεφάλαιο 3ο εξετάσαμε έγκυρες μεθόδους που ένας κακόβουλος χρήστης μπορεί να χρησιμοποιήσει για να αποκτήσει πρόσβαση σε ασύρματα δίκτυα. Στο 5ο κεφάλαιο, αναλύθηκαν τρόποι με τους οποίους τα ασύρματα δίκτυα μπορούν να ρυθμιστούν, ώστε να ελαττωθεί ο κίνδυνος για μια επιτυχημένη επίθεση

Λόγω των θετικών στοιχείων που παρέχουν, τα ασύρματα δίκτυα έχουν γίνει αποδεκτά από τους καταναλωτές και η εξάπλωσή τους συνεχίζει να είναι ραγδαία. Αντιπροσωπεύουν ένα από τα μεγαλύτερα πλεονεκτήματα της δικτύωσης των τελευταίων χρόνων, ειδικά για τους οικιακούς χρήστες που θέλουν να μοιράζονται την σύνδεσή τους στο Διαδίκτυο χωρίς την χρήση καλωδίων μεταξύ ορόφων και τοίχων.

Τα τελευταία χρόνια η ανάγκη για συνεχή χρήση κάποιας μορφής ηλεκτρονικών υπολογιστών ασχέτως του σημείου που βρίσκεται κάποιος είναι διαρκώς αυξανόμενη. Κάθε άτομο που χειρίζεται ηλεκτρονικό υπολογιστή στην καθημερινότητα του έχει την ανάγκη να τον χρησιμοποιεί παντού και με εύκολο τρόπο, χωρίς να περιορίζεται στα πλαίσια ενός χώρου. Η χρήση των υπολογιστών ταυτίζεται με την ταυτόχρονη χρήση των δικτύων στα οποία διασυνδέονται οι ηλεκτρονικοί υπολογιστές. Για αυτό τον λόγο δεν μπορεί να θεωρηθεί ως ισχυρό πλεονέκτημα το να χρησιμοποιεί κάποιος έναν υπολογιστή χωρίς να συνδέεται σε κάποιο είδος δικτύου πληροφοριών.

Με την δημιουργία των φορητών υπολογιστών (laptop) λύθηκε το πρόβλημα της φορητότητας. Επίσης η διαρκώς αναπτυσσόμενες τεχνολογίες των ασυρμάτων δικτύων έλυσαν το πρόβλημα της διασύνδεσης των υπολογιστών αυτών. Ο συνδυασμός ενός φορητού υπολογιστή με μια ασύρματη σύνδεση σε κάποιο τοπικό δίκτυο και κατ’ επέκταση με το διαδίκτυο είναι πλέον μια συνηθισμένη υπόθεση. Δημόσιοι χώροι, κοινόχρηστοι χώροι, αεροδρόμια, πανεπιστήμια, ΤΕΙ έχουν εγκαταστάσεις ασύρματων δικτύων, έτσι λοιπόν, δόθηκαν λύσεις στις συνδέσεις απομακρυσμένων δικτύων καταργώντας τα καλώδια. Τέλος οι ασύρματες συνδέσεις χρησιμοποιούνται δυναμικά και από τη κινητή τηλεφωνία.

Πίνακας εικόνων

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) http://el.wikipedia.org/wiki/IEEE_802.11

2) http://en.wikipedia.org/wiki/WiMAX

3) http://broadband.cti.gr/el/evrizonikotita/wimax.php

4) http://windows.microsoft.com/el-GR/windows7/Wireless-networking-frequently-asked-questions

5) http://windows.microsoft.com/el-gr/windows-vista/What-are-the-different-wireless-network-security-methods

6) http://en.wikipedia.org/wiki/IEEE_802.1X

7) http://www.brighthub.com/computing/smb-security/articles/53262.aspx

8) http://www.wimax.com/wimax/five-essential-elements-of-wimax-security

9) Μαρκομανωλάκη Αικ, Νοέμβριος 2010, Ασφάλεια σε Ασύρματα Δίκτυα, Πτυχιακή Εργασία.

10) Σπανού Χ, Σεπτέμβριος 2008, Σχεδιασμός Ασύρματου Συστήματος Ευρείας Ζώνης σύμφωνα με το Πρότυπο της IEEE 802.16, Διπλωματική Εργασία.

11) Κεφαλάς Γ, Οκτώβριος 2011, Ασφάλεια στα Ασύρματα Τοπικά Δίκτυα (WRA/WPA2), Διπλωματική Εργασία.

12) Tanenbaum, A. S. (2000). Δίκτυα Υπολογιστών. Αθήνα: Εκδόσεις Παπασωτηρίου.

13) Ε.Μ.Πάλλης. (2000). Εισαγωγή στα Ασύρματα Δίκτυα. Ηράκλειο Κρήτης: Τμήμα Εφαρμοσμένης Πληροφορικής.

14) Comer, D. (2007). Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet. Αθήνα: Κλειδάριθμος .

15) Κρυπάρος Γ, Μάρτιος 2005, Θέματα Ασφάλειας σε 802.11b Ασύρματα Δίκτυα, Διπλωματική Εργασία.

16) Γαβριλάκη Κ, Δεκέμβριος 2009, Επιθέσεις και Τεχνικές Προστασίας σε ένα WirelessNetwork 802.11, Πτυχιακή Εργασία.