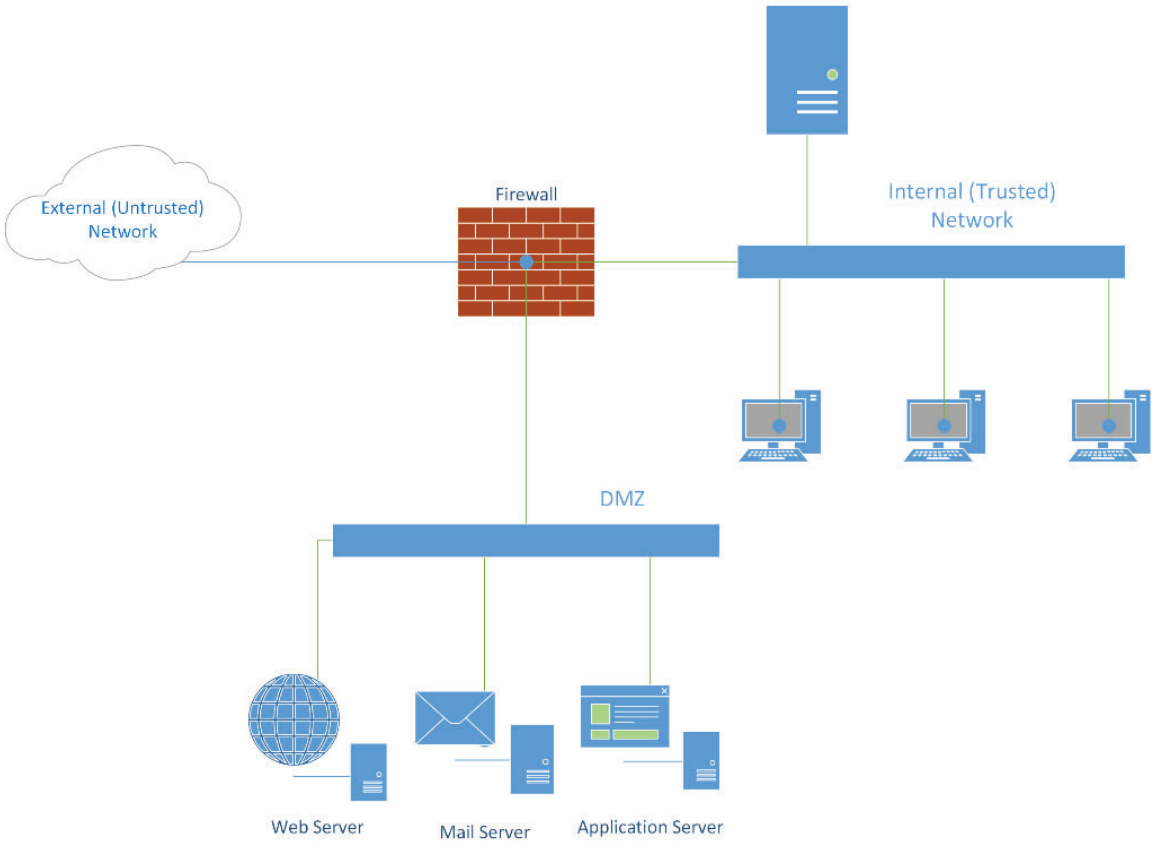


Εικόνα 3. 9 *DMZ.*

3.2.5 Ανίχνευση Εισβολών

Η ανίχνευση εισβολών (intrusion detection) στοχεύει στην ανακάλυψη κακόβουλων ενεργειών μέσω της ανάλυσης καταγραφών (auditing) και του εντοπισμού ύποπτης συμπεριφοράς ενός επιτιθέμενου που έχει καταφέρει να αποκτήσει πρόσβαση στο σύστημα. Η αρχή της λειτουργίας της βασίζεται στην υπόθεση πως ο επιτιθέμενος θα συμπεριφερθεί διαφορετικά σε σχέση με ένα νόμιμο χρήστη του συστήματος. Καθώς η ανάλυση των καταγραφών από το διαχειριστή είναι εργασία επίπονη και χρονοβόρα, έχουν αναπτυχθεί συστήματα τα οποία είναι επιφορτισμένα με την ανάλυση αυτή σε πραγματικό χρόνο, τα οποία είναι γνωστά ως Intrusion Detection Systems (IDS).

3.2.5.1 Κατηγορίες IDS

Η ανίχνευση εισβολών μπορεί να λαμβάνει χώρα σε επίπεδο δικτύου ή σε επίπεδο κόμβου. Έτσι, τα αντίστοιχα συστήματα IDS κατηγοριοποιούνται σε:

- Host-based IDS, που υλοποιούνται με λογισμικό εγκατεστημένο στον κόμβο (host), του οποίου την εισερχόμενη και εξερχόμενη κίνηση ελέγχουν.

- Network-Based IDS, που αποτελούνται από dedicated κόμβους, οι οποίοι περιέχουν δικτυακές διεπαφές που έχουν τεθεί σε κατάσταση ασυδοσίας (promiscuous mode) και καταγράφουν και ελέγχουν το σύνολο της κίνησης του δικτύου. Αποτελούνται από:

- Το Network Tap (π.χ. sniffer), το οποίο συνδέεται με κατάλληλη διεπαφή δικτύου (π.χ. port-mirroring switch port) και μπορεί να καταγράφει το σύνολο της κίνησης του δικτύου.

- Το Detection Engine, το οποίο είναι επιφορτισμένο με την ανάλυση των καταγραφών από την κίνηση του δικτύου.

Τα δύο είδη IDS παρουσιάζουν πλεονεκτήματα και μειονεκτήματα, όπως φαίνεται στον Πίνακα 3.3.

Τύπος	**Πλεονεκτήματα**	**Μειονεκτήματα**
Network-based	Απαιτείται μικρός αριθμός επιλεγμένων σημείων στο δίκτυο που ελέγχεται.	Δεν είναι δυνατή η ανάλυση κρυπτογραφημένων δεδομένων.
	Δεν εμπλέκεται στην κίνηση των πακέτων.	Δε μπορεί να ανιχνεύσει τη συνέπεια της επίθεσης.
	Είναι συσκευές συγκεκριμένου σκοπού, που δύσκολα παραβιάζονται.	Ο μεγάλος όγκος δεδομένων μπορεί να δημιουργήσει προβλήματα ανίχνευσης.
Host-Based	Είναι δυνατή η ανάλυση της κρυπτογραφημένης επικοινωνίας.	Απαιτείται η εγκατάσταση επιπρόσθετου λογισμικού, άρα περισσότεροι πόροι και διαχειριστικός φόρτος.
	Δεν απαιτούν εξειδικευμένο υλικό.	Μπορούν να επηρεαστούν και τα ίδια από τις επιθέσεις.
	Έχουν πρόσβαση σε καταγραφές συστήματος ώστε η ανάλυση να είναι πιο ακριβής.	Δεν μπορούν να εγκατασταθούν σε ειδικού σκοπού συσκευές ή σε μη συμβατά λειτουργικά συστήματα.

Πίνακας 3.3 *Τύποι IDS.*

Δεν υπάρχει χρυσός κανόνας για την επιλογή του τύπου IDS. Η επιλογή γίνεται ανάλογα με το δίκτυο και τις απαιτήσεις προστασίας του. Στην περίπτωση που απαιτούνται και οι δύο περιπτώσεις, υπάρχουν τα υβριδικά συστήματα (Hybrid Detection) τα οποία συνδυάζουν και τους δύο τύπους.

3.2.5.2 Ανίχνευση υπογραφών

Στην περίπτωση της ανίχνευσης υπογραφών (signatures), η καταγεγραμμένη κίνηση ελέγχεται και συγκρίνεται με ένα σύνολο κανόνων που υποδεικνύουν μια μη επιθυμητή κατάσταση. Ένας τέτοιος κανόνας θα μπορούσε να είναι: «Οι χρήστες δεν πρέπει να τοποθετούν αρχεία στο home directory άλλων χρηστών».

Έτσι, αν ένας χρήστης δοκιμάσει να εγγράψει ένα αρχείο στο home directory ενός άλλου χρήστη, το IDS θα θεωρήσει τη συμπεριφορά ύποπτη και θα ενημερώσει το διαχειριστή.

Άλλες υπογραφές, σε επίπεδο δικτύου, μπορούν να αναφέρουν περιπτώσεις που δεν πρέπει να παρατηρούνται σε ένα IP πακέτο, όπως για παράδειγμα η ύπαρξη πακέτων με ίδια διεύθυνση προέλευσης και προορισμού (source & destination address). Η επίθεση αυτού του είδους είναι γνωστή ως Land attack.

3.2.5.3 Ανίχνευση συμπεριφοράς

Στην περίπτωση της ανίχνευσης υπογραφών, μια εισβολή ανιχνεύεται και καταγράφεται εφόσον το IDS είναι ενημερωμένο με την αντίστοιχη υπογραφή. Αν η υπογραφή δεν υπάρχει, τότε η επίθεση δεν θα γίνει αντιληπτή. Αντιθέτως, στην περίπτωση του ελέγχου συμπεριφοράς (behavior), το IDS εντοπίζει συμπεριφορές που δεν ταιριάζουν με τη φυσιολογική χρήση του συστήματος. Η φυσιολογική χρήση «μαθαίνεται» από το IDS κατά

τη διάρκεια της ως τότε λειτουργίας του. Έτσι, αν παρατηρηθεί μια απόκλιση στη συμπεριφορά του συστήματος, όπως αυξημένη δραστηριότητα, ασυνήθιστες αιτήσεις πρόσβασης, αυξημένος αριθμός συνόδων, κ.ά. το IDS θεωρεί πως υπάρχει επίθεση.

Η ανίχνευση συμπεριφοράς λειτουργεί σωστά σε στατικά περιβάλλοντα, όπου υπάρχουν σχετικά επαναλαμβανόμενα μοτίβα λειτουργίας. Αντιθέτως, σε δυναμικά περιβάλλοντα μπορεί να οδηγήσει σε περίπτωση λανθασμένου συναγερμού (false positive), όταν μια συμπεριφορά δεν έχει προηγουμένως καταγραφεί ως νόμιμη.

3.2.5.4 Συστήματα Πρόληψης Εισβολών

Τα συστήματα IDS ανιχνεύουν τις πιθανές εισβολές και ενημερώνουν το διαχειριστή ώστε να προβεί στις απαραίτητες ενέργειες. Η διαδικασία, όμως, αυτή μπορεί να χρειαστεί αρκετό χρόνο, με αποτέλεσμα να προκληθεί ζημιά από μια εισβολή. Σε αντιστοιχία, μπορεί κανείς να σκεφτεί ένα συναγερμό που θα ειδοποιήσει τον κάτοικο ενός σπιτιού, αφού ο διαρρήκτης είναι ήδη μέσα σε αυτό. Για το λόγο αυτό, η δεύτερη γενιά συστημάτων ανίχνευσης εισβολών παρέχει και τη δυνατότητα πρόληψης (Intrusion Prevention Systems – IPS). Η αντίδραση μπορεί να είναι είτε άμεση ή έμμεση. Στην άμεση αντίδραση (inline), το ίδιο το IPS απορρίπτει ή αναδρομολογεί τα πακέτα που ανήκουν στη δικτυακή κίνηση της επίθεσης. Στην περίπτωση της έμμεσης αντίδρασης, το IPS δίνει εντολή σε άλλα συστήματα, με τα οποία συνδέεται (όπως firewalls), να προβούν στις απαραίτητες ενέργειες.

Το μειονέκτημα της χρήσης ενός IPS είναι η περίπτωση ενός false positive, όπου η αντίδραση μπορεί να αποτρέψει μια νόμιμη ενέργεια. Ως αντίστοιχο παράδειγμα, μπορεί κανείς να φανταστεί την ενεργοποίηση της αυτόματης πυρόσβεσης σε ένα γραφείο, χωρίς όμως να υπάρχει φωτιά.

3.2.5.5 Honeypots

Για την αποφυγή ζημίας από επιθέσεις, ή για τη μελέτη πραγματικών επιθέσεων είναι δυνατή η ανάπτυξη ενός κόμβου ή δικτύου δολώματος, γνωστού ως honeypot ή honeynet. Ένα honeypot σκόπιμα περιέχει ευπάθειες με σκοπό να δελεάσει το δυνητικό επιτιθέμενο, ώστε να τον προτρέψει στο να επιτεθεί σε αυτό και να μην ασχοληθεί με τα υπόλοιπα συστήματα, με στόχο:

- Να ανιχνευτεί η επίθεση.
- Να μελετηθεί η επίθεση.
- Να εντοπιστεί ο επιτιθέμενος.
- Η ζημιά να περιοριστεί στο honeypot.

3.3 Ασύρματη Δικτύωση

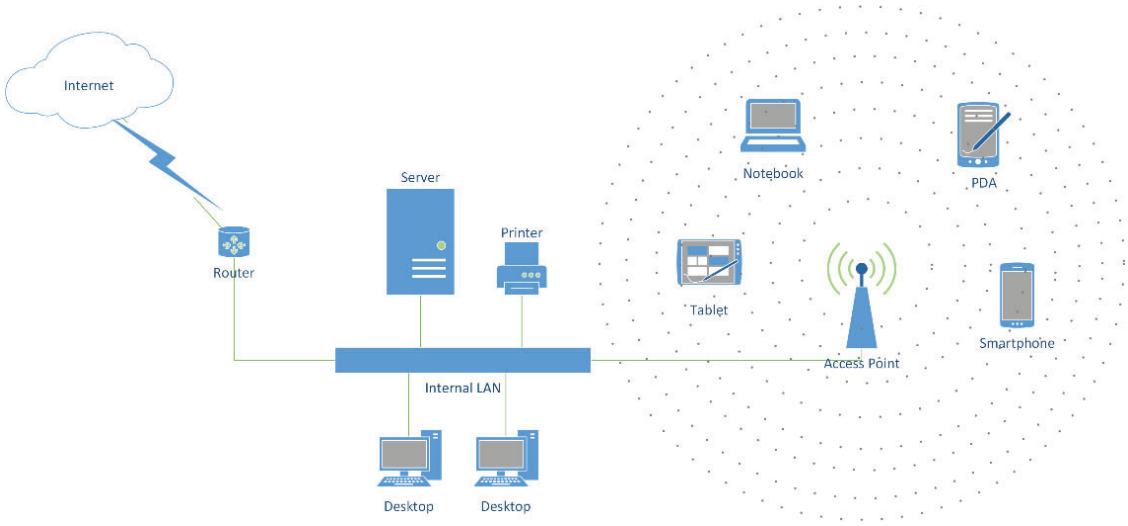
Η ασύρματη δικτύωση παρέχει τη δυνατότητα μεταφοράς δεδομένων χωρίς τη σύνδεση των κόμβων σε φυσικό μέσο (όπως καλώδια χαλκού ή οπτικές ίνες), αλλά με τη χρήση ηλεκτρομαγνητικών κυμάτων που μεταδίδονται στον αέρα. Με τη χρήση τεχνολογιών ασύρματης δικτύωσης, είναι δυνατή η επέκταση του δικτύου και η εξυπηρέτηση κόμβων σε σημεία όπου δεν υπάρχει εγκατάσταση δομημένης καλωδίωσης ή οποιοσδήποτε άλλος τρόπος ενσύρματης σύνδεσης.

Το 1997, η ένωση IEEE παρουσίασε το πρότυπο 802.11 το οποίο περιγράφει ένα σύνολο προδιαγραφών και πρωτοκόλλων που καθορίζουν τον τρόπο επικοινωνίας στο επίπεδο πρόσβασης δικτύου. Κατά την υλοποίηση ασύρματων δικτύων IEEE 802.11, οι λειτουργίες των ανώτερων επιπέδων (δικτύου, μεταφοράς και εφαρμογής) δεν διαφοροποιούνται, επιτρέποντας την απρόσκοπτη λειτουργία των ιδίων πρωτοκόλλων.

Αρχικά, το εύρος ζώνης των ασύρματων συνδέσεων με χρήση του προτύπου IEEE 802.11 ήταν ιδιαίτερα χαμηλό σε σχέση με την ενσύρματη σύνδεση (μόλις 2 Mbps). Με το πέρασμα των χρόνων παρουσιάστηκαν επεκτάσεις του προτύπου οι οποίες επιτρέπουν συνδέσεις με ταχύτητες της τάξεως των Gbps (802.11ac). Η περιγραφή του προτύπου και των επεκτάσεών του είναι εκτός του σκοπού του παρόντος εγχειριδίου.

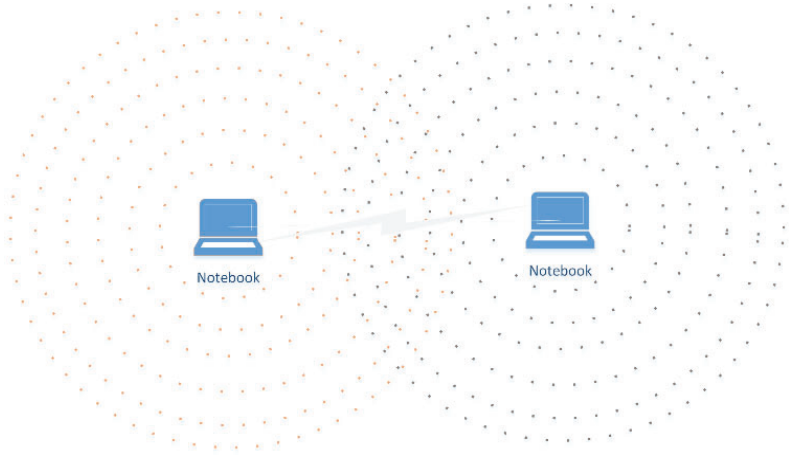
Οι τοπολογίες που συναντώνται συνήθως στα δίκτυα που υλοποιούν το πρότυπο 802.11, είναι οι ακόλουθες:

- Infrastructure Mode, όπου η επικοινωνία μεταξύ των κόμβων γίνεται μέσω ενός κεντρικού σημείου πρόσβασης (access point).



Εικόνα 3.10 *Infrastructure mode.*

- Ad-hoc Mode, όπου εδραιώνονται συνδέσεις απευθείας μεταξύ των τερματικών συσκευών.



Εικόνα 3.11 *Ad-hoc mode.*

3.3.1 Ζητήματα ασφάλειας

Ένα ασύρματο δίκτυο παρουσιάζει το πλεονέκτημα της άμεσης επέκτασης ενός ενσύρματου δικτύου και της ευκολίας διασύνδεσης για κινητούς κυρίως κόμβους (όπως φορητοί υπολογιστές, κινητά τηλέφωνα, tablets κοκ). Καθώς όμως η πληροφορία διακινείται στον αέρα, χωρίς φυσικούς περιορισμούς, μπορεί, πέρα από το νόμιμο αποδέκτη, να αποκτήσει πρόσβαση σε αυτή οποιοσδήποτε άλλος βρίσκεται στην εμβέλεια εκπομπής. Ένας κακόβουλος χρήστης, έχοντας πρόσβαση στο κοινό μέσο, θα μπορούσε να υλοποιήσει επιθέσεις με σκοπό:

- Να υποκλέψει δεδομένα (Sniffing)
  Ο κακόβουλος χρήστης μπορεί να καταγράψει το σύνολο της διακινούμενης πληροφορίας και, στη συνέχεια, να ανακτήσει τα δεδομένα που επιθυμεί να παρακολουθήσει (eavesdropping) ή για να τα χρησιμοποιήσει ώστε να υποκλέψει μια σύνοδο με χρήση επιθέσεων session hijacking, replay attacks ή MAC spoofing.

- Να τροποποιήσει τα μεταδιδόμενα δεδομένα (Man-in-the-Middle)
  Ο κακόβουλος χρήστης μπορεί να υλοποιήσει επίθεση ενδιάμεσου με σκοπό να παρεισφρήσει στην επικοινωνία και να τροποποιήσει τα μεταδιδόμενα δεδομένα.

- Να διακόψει την υπηρεσία (Denial of Service)
  Ο κακόβουλος χρήστης μπορεί να παρεμβάλει μεγάλο όγκο δεδομένων στις χρησιμοποιούμενες συχνότητες, με σκοπό την άρνηση εξυπηρέτησης.

- Να υποκλέψει στοιχεία πρόσβασης (Wireless Phishing)
  Ο κακόβουλος χρήστης μπορεί να τοποθετήσει ένα δικό του access point με ίδιο SSID με αυτό του δικτύου-στόχου. Έτσι, όταν ο πελάτης προσπαθήσει να συνδεθεί σε αυτό, νομίζοντας ότι συνδέεται στο υποτιθέμενο access point, ο επιτιθέμενος θα μπορέσει να καταγράψει τα μεταδιδόμενα στοιχεία αυθεντικοποίησης.

Η αντιμετώπιση των επιθέσεων αυτών απαιτεί την υλοποίηση αντίμετρων που περιλαμβάνουν:

- Μέριμνα κατά τη φυσική σχεδίαση του ασύρματου δικτύου.

- Υλοποίηση τεχνικών και μεθόδων προστασίας των δεδομένων.

3.3.2 Θέματα σχεδίασης

Η αντιμετώπιση των κινδύνων σε ένα ασύρματο δίκτυο, είναι μια διαδικασία που ξεκινά ήδη από το σχεδιασμό του. Για να οργανωθεί όμως το σχέδιο άμυνας ενός δικτύου, θα πρέπει να γίνει πρώτα κατανοητό ποιο είναι το «οχυρό» που πρέπει να προστατευτεί. Έτσι, είναι βασικό να γνωρίζει κανείς πως λειτουργεί η επιμέρους τεχνολογία ασύρματης δικτύωσης, την οποία επιλέγει να χρησιμοποιήσει. Άρα, το πρώτο βήμα είναι η σε βάθος μελέτη των αρχών που διέπουν τη λειτουργία των ασύρματων δικτύων, κάτι που ξεφεύγει από τους σκοπούς του παρόντος εγχειριδίου, αλλά θα αναφερθούν ορισμένοι γενικοί σχεδιαστικοί κανόνες.

3.3.2.1 Ελάχιστη περιοχή κάλυψης

Ένα ασύρματο δίκτυο δεν περιορίζεται εντός των φυσικών ορίων ενός χώρου, όπως οι τοίχοι ενός δωματίου, αλλά είναι διαθέσιμο σε μία περιοχή η έκταση της οποίας εξαρτάται από:

- Την ισχύ εκπομπής.
- Το είδος του δικτύου.
- Τη συχνότητα εκπομπής.
- Τον τύπο και την απολαβή της κεραίας.
- Το φυσικό περιβάλλον.
- Τις παρεμβολές.
- Την απόσταση.

Κατά το σχεδιασμό, θα πρέπει να υπολογιστεί η επιθυμητή απόσταση κάλυψης, να οριστεί κατάλληλα η ισχύς εκπομπής και να επιλεγεί η κατάλληλη για τον τύπο κάλυψης κεραία. Στόχος των παραπάνω είναι η

περιοχή κάλυψης να μην υπερβαίνει την επιθυμητή περιοχή, αλλά επίσης η επιθυμητή περιοχή να καλύπτεται επαρκώς ώστε να μην υπάρχει πρόβλημα διαθεσιμότητας του δικτύου.

Η πρακτική που πολλές φορές ακολουθείται με τη λάθος τοποθέτηση κεραιών (π.χ. εγκατάσταση μιας omnidirectional κεραίας, που παρέχει μια θεωρητικά ομοιόμορφη κάλυψη προς όλες τις κατευθύνσεις, εκτός του κέντρου της επιθυμητής περιοχής κάλυψης ή για περιπτώσεις που επιθυμούμε κάλυψη προς μια μόνο κατεύθυνση) ή η χρήση κεραιών με μεγάλη απολαβή, επιτρέπει στον επιτιθέμενο να εκτελέσει ενέργειες από μεγάλη απόσταση, χωρίς να γίνει αντιληπτή η φυσική του παρουσία.

3.3.2.2 Ορισμός service identifier

Το Service Set Identifier (SSID) χαρακτηρίζει το δίκτυο και το διαφοροποιεί από τα υπόλοιπα. Για το σκοπό αυτό, είναι συνετό το SSID να τροποποιείται, έτσι ώστε να προσδιορίζει με σαφήνεια το δίκτυο. Υπάρχει ακόμη η δυνατότητα της αποφυγής εκπομπής του SSID, σε περίπτωση που δεν είναι επιθυμητή η ανίχνευση του δικτύου ώστε να τραβήξει την προσοχή ενός κακόβουλου χρήστη. Στην περίπτωση επιθυμίας για την αποφυγή εκπομπής του, το SSID θα πρέπει να οριστεί με τέτοιο τρόπο ώστε να μην είναι προβλέψιμο ή να μη διατηρηθεί κάποια προεπιλογή του κατασκευαστή που να διευκολύνει τον επιτιθέμενο στο να το μαντέψει. Ακόμη, η αλλαγή του SSID μπορεί να αποτρέψει μια επίθεση Wireless Phishing, στην οποία ο επιτιθέμενος παρουσιάζει στους clients ένα SSID που τους οδηγεί σε σύνδεση με ένα δικό του δίκτυο, αντί για αυτό που πραγματικά επιθυμούν.

3.3.2.3 Απενεργοποίηση ad-hoc συνδέσεων

Πολλές από τις συσκευές που χρησιμοποιούνται καθημερινά, παρέχουν τη δυνατότητα ασύρματης ad-hoc σύνδεσης με αυτές. Όταν μια τέτοια συσκευή συνδέεται με το υπόλοιπο δίκτυο, θα πρέπει να ληφθεί κατάλληλη μέριμνα ώστε είτε η δυνατότητα αυτή να απενεργοποιηθεί ή να παραμετροποιηθεί με κατάλληλο τρόπο έτσι ώστε να μην είναι δυνατή η χρήση της από έναν κακόβουλου χρήστη για διείσδυση μέσω αυτής στο υπόλοιπο δίκτυο.

3.3.2.4 Έλεγχος ενσύρματων σημείων σύνδεσης

Αν και με την πρώτη ματιά, η συγκεκριμένη προτροπή μοιάζει να μην αφορά το ασύρματο δίκτυο, έχουν καταγραφεί περιπτώσεις όπου νόμιμοι χρήστες του δικτύου συνδέουν σε θύρες δικτύου access points που προμηθεύονται από το εμπόριο για να συνδέσουν τις κινητές τους συσκευές (rogue access points). Η σύνδεση access points χωρίς τις κατάλληλες γνώσεις παραμετροποίησης, μπορεί να αποτελέσει κερκόπορτα για κάποιον επιτιθέμενο. Για την αποφυγή τέτοιων καταστάσεων, πρέπει οι μεταγωγείς (switches) να ρυθμιστούν έτσι ώστε να μην είναι δυνατή η σύνδεση οποιασδήποτε συσκευής σε οποιαδήποτε θύρα (port security).

3.3.2.5 Απομόνωση πελάτη

Σε ένα ασύρματο δίκτυο, κυρίως όταν αυτό αφορά ένα δημόσια διαθέσιμο δίκτυο, συνδέονται αρκετά διαφορετικοί χρήστες. Στο δίκτυο αυτό θα πρέπει να μην επιτρέπεται η ανταλλαγή δεδομένων μεταξύ των τερματικών συσκευών των χρηστών, ώστε να μη μπορεί ένας επιτιθέμενος που είναι συνδεδεμένος, ακόμη και ως νόμιμος χρήστης, να αποκτήσει πρόσβαση στα δεδομένα που είναι αποθηκευμένα στις συσκευές των υπόλοιπων χρηστών (client isolation).

3.3.3 Προστασία δεδομένων

Τα δεδομένα σε ένα ασύρματο δίκτυο, όπως αναφέρθηκε προηγουμένως, μεταδίδονται στον αέρα μέσω ηλεκτρομαγνητικών κυμάτων. Για το λόγο αυτό, θα πρέπει να ληφθεί μέριμνα ώστε να μην είναι διαθέσιμα σε όλους όσοι βρίσκονται στην εμβέλεια κάλυψης του δικτύου. Στο πέρασμα των ετών έχουν προταθεί και υλοποιηθεί διάφορες λύσεις αυθεντικοποίησης και κρυπτογράφησης δεδομένων στο ασύρματο μέσο. Στη συνέχεια θα αναφερθούν οι πιο γνωστές και αυτές που συναντώνται σήμερα.

3.3.3.1 Wired Equivalent Privacy

Στόχος της δημιουργίας του Wired Equivalent Privacy (WEP) δεν ήταν η μέγιστη δυνατή προστασία των ιδιοτήτων της ασφάλειας, αλλά το να παρέχει προστασία αντίστοιχη με αυτή που παρέχεται από ένα ενσύρματο μέσο (όπως εξάλλου δηλώνει και το όνομά του). Έτσι, τα δεδομένα που διακινούνται μεταξύ του access point και των χρηστών κρυπτογραφούνται. Το WEP παρέχει και τη δυνατότητα αυθεντικοποίησης, πέρα από την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

Στο WEP χρησιμοποιείται ένα κοινό κλειδί μεταξύ του access point και του σταθμού (τερματικού). Το κλειδί αυτό διαμοιράζεται από το διαχειριστή του access point με κάθε ασύρματο κόμβο, για την αυθεντικοποίηση και την κρυπτογράφηση της επικοινωνίας.

Υπάρχουν δύο επιλογές αυθεντικοποίησης:

- Open System authentication, όπου ουσιαστικά δεν γίνεται αυθεντικοποίηση και κάθε αίτημα για σύνδεση στο δίκτυο ικανοποιείται από το access point.

- Shared-key authentication, όπου ακολουθείται μια διαδικασία πρόκλησης-απόκρισης (challenge-response), ως εξής:

    - Ο σταθμός αποστέλλει ένα αίτημα στο access point.

    - Το access point δημιουργεί μια τυχαία ακολουθία 128 bits (challenge).

    - Ο σταθμός κρυπτογραφεί την ακολουθία αυτή με χρήση του αλγορίθμου RC4 και του κοινού κλειδιού και αποστέλλει το αποτέλεσμα (κρυπτογράφημα) στο access point.

    - Το access point αποκρυπτογραφεί το κρυπτογράφημα με χρήση του ίδιου αλγόριθμου και του κοινού κλειδιού. Αν το αποτέλεσμα είναι ίδιο με την αρχική ακολουθία, σημαίνει πως το κλειδί μεταξύ των δύο είναι κοινό (το γιατί θα το μελετήσετε αργότερα στο κεφάλαιο 6), άρα ο σταθμός αυθεντικοποιείται.

Η αυθεντικοποίηση στο WEP, βασίζεται στην επαλήθευση της ύπαρξης ενός κοινού κλειδιού μεταξύ του σταθμού και του access point. Ίσως, η αρχική απάντηση στην ερώτηση ποιόν από τους δύο τρόπους αυθεντικοποίησης θα επιλέγατε (Open ή Shared key) θα ήταν πως ο δεύτερος είναι προτιμότερος, καθώς ελέγχεται η πρόσβαση στο δίκτυο και μόνο χρήστες που γνωρίζουν το κοινό κλειδί μπορούν να την αποκτήσουν. Αν το σκεφτούμε όμως καλύτερα, κατά τη διαδικασία της αυθεντικοποίησης ο επιτιθέμενος μπορεί να ανακτήσει (μέσω sniffing) και την αρχική ακολουθία και την κρυπτογραφημένη απάντηση. Έχοντας αυτά τα δύο, εύκολα μπορεί να εξάγει το κλειδί. Άρα, μπορεί με τη σειρά του όχι μόνο να αυθεντικοποιηθεί ώστε να χρησιμοποιήσει το ασύρματο δίκτυο για πρόσβαση στο Διαδίκτυο, αλλά και να υποκλέψει και αποκρυπτογραφήσει το σύνολο της κίνησης που διέρχεται από το access point. Οπότε, η απάντηση είναι ότι, παραδόξως, ασφαλέστερο είναι να επιλεγεί το Open Systems Authentication για την προστασία της εμπιστευτικότητας και ακεραιότητας των δεδομένων (ένας κακόβουλος χρήστης θα μπορέσει να συνδεθεί αλλά όχι να ανταλλάξει δεδομένα).

Η κρυπτογράφηση των frames στο WEP γίνεται ως εξής:

- Ο αποστολέας υπολογίζει το CRC του αρχικού μηνύματος, την τιμή του οποίου συνενώνει (concatenate) με το μήνυμα.

- Στη συνέχεια, δημιουργεί ένα διάνυσμα αρχικοποίησης (initialization vector - IV) 24 bit, το οποίο συνενώνει με το κλειδί μήκους 40 ή 104 bit, ανάλογα. Η συνένωση αυτή τροφοδοτείται σε μια ψευδογεννήτρια τυχαίων αριθμών (Pseudo-random Number Generator – PRNG) που χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης ροής RC4, ώστε να παραχθεί μια κλειδοροή ίση με το μήκος του μηνύματος.

- Το αποτέλεσμα της πράξης XOR μεταξύ του μηνύματος και της κλειδοροής αποτελεί το κρυπτογράφημα (cipher text) το οποίο συνενώνεται με το IV και αποστέλλεται στον παραλήπτη.

Το WEP παρουσιάζει σημαντικές αδυναμίες, όπως:

- Δεν υπάρχει διαχείριση κλειδιών συνόδου, οπότε η διανομή πρέπει να γίνεται «χέρι με χέρι» από το διαχειριστή.

- Το μέγεθος του IV είναι μόλις 24 bit. Άρα, υπάρχουν μόνο 2^{24}, δηλαδή λίγο περισσότερα από 16 εκατομμύρια, διαφορετικά πιθανά IV. Έτσι, σε συνδυασμό με την αυξημένη δικτυακή κίνηση, είναι πιθανή η επανεμφάνιση πακέτων με ίδιο IV σε σύντομο διάστημα. Αν ο επιτιθέμενος καταφέρει να εντοπίσει δύο πακέτα με το ίδιο IV (το οποίο στέλνεται ως ανοικτό κείμενο συνενωμένο με το κρυπτοκείμενο), μπορεί για παράδειγμα να εφαρμόσει μια επίθεση κλειδοροής (keystream attack). Σε μια τέτοια επίθεση, βασιζόμενος στο γεγονός ότι το αποτέλεσμα της XOR σε δύο μηνύματα με κρυπτοκείμενο είναι ίδιο με το αποτέλεσμα της XOR στα δύο μηνύματα με το καθαρού κειμένου από το οποίο προέκυψαν, μπορεί να αποκαλύψει το περιεχόμενο του ενός μηνύματος γνωρίζοντας το περιεχόμενο του άλλου μηνύματος.

- Επειδή ισχύει: $CRC(x \oplus y)=CRC(x) \oplus CRC(y)$, Ο επιτιθέμενος μπορεί να κάνει αλλαγές στο μήνυμα, τέτοιες ώστε η τιμή του CRC να είναι η ίδια.

Οι παραπάνω λόγοι, κατέστησαν σύντομα το WEP ακατάλληλο για χρήση σε ασύρματα δίκτυα και προτάθηκε η αντικατάστασή του από το WPA.

3.3.3.2 Wi-Fi Protected Access

Το Wi-Fi Protected Access (WPA) αποτελεί υποσύνολο του προτύπου 802.11i και παρουσιάστηκε από τη Wi-Fi Alliance με σκοπό να θεραπεύσει προσωρινά τις αδυναμίες του WEP και να μπορεί να εκτελείται στο ίδιο υλικό που εκτελούνταν το τελευταίο. Έπρεπε, ακόμη, να είναι συμβατό με το επερχόμενο 802.11i. Οι βασικές διαφορές του από το WEP είναι:

- Η αυθεντικοποίηση μπορεί να γίνει είτε με χρήση του πρωτοκόλλου 802.1X και χρήση ενός RADIUS Server (Enterprise Mode) είτε βασισμένη στη χρήση ενός συνθηματικού (passphrase) για απλές οικιακές εγκαταστάσεις.

- Εισήχθη το πρωτόκολλο TKIP, που αποτελεί ένα σύνολο αλγορίθμων με σκοπό την αντιμετώπιση των αδυναμιών του WEP, π.χ. όσον αφορά τα IV και τη μη ανανέωση των κλειδιών συνόδου.

Το WPA συνεχίζει να χρησιμοποιεί τον αλγόριθμο RC4, με μεγαλύτερο όμως μήκος κλειδιού (128 bits) και ουσιαστικά αποτελεί μια βελτίωση του WEP.

3.3.3.3 IEEE 802.11i - WPA2

Το πρωτόκολλο WPA2 αποτελεί την υλοποίηση του προτύπου 802.11i. Αντικαθιστά τον αλγόριθμο RC4 με τον AES, ο οποίος χρησιμοποιείται και κατά την αυθεντικοποίηση και κατά την κρυπτογράφηση. Αν και έχει διορθώσει πολλές από τις ευπάθειες των WEP και WPA, είναι ευάλωτο σε επιθέσεις Rollback, RSN IE poisoning και De-Association.