ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

Κατεύθυνση Ψηφιακές Επικοινωνίες & Δίκτυα

ΑΣΦΑΛΕΙΑ ΣΤΑ ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ (DNS Tunneling)

Διπλωματική Εργασία

Γαδανάκης Αντώνιος , ΜΕ 09076

Επιβλέπων :Δρ. Ξενάκης Χρήστος , Επίκουρος Καθηγητής

Πειραιάς , Οκτώβριος 2013

Περίληψη

Σκοπός αυτής της διπλωματικής εργασίας είναι η περιγραφή του τρόπου λειτουργίας των ασυρμάτων τοπικών δικτύων ,των DNS Tunnels και η παραβίαση της ασφάλειας. Θα αναφερθούν γνωστές υλοποιήσεις για DNS Tunneling. Θα χρησιμοποιηθεί η εφαρμογή Iodine για να παρακάμψει ένα Captive Portal και να αποκτήσει ένας χρήστης μη πληρωμένη πρόσβαση στο Διαδίκτυο. Στη συνέχεια θα αναλυθούν οι τεχνικές ανίχνευσης DNS Tunneling και η εφαρμογή τους.

Πιο αναλυτικά, το κεφάλαιο ένα περιγράφει την ανάγκη του σύγχρονου ανθρώπου για επικοινωνία και δικτύωση, τον ορισμό, την αρχιτεκτονική και τις κατηγορίες που διαχωρίζονται τα δίκτυα δεδομένων.

Το κεφάλαιο δύο εξηγεί τι είναι το ασύρματο τοπικό δίκτυο και γιατί προτιμάται σε αντίθεση με το ενσύρματο δίκτυο. Περιγράφει την εξέλιξη, τα δομικά στοιχεία, τα πρότυπα, τις τοπολογίες του προτύπου 802.11 και τον τρόπο λειτουργίας του.

Το κεφάλαιο τρία περιγράφει την ασφάλεια στα ασύρματα δίκτυα, τα πρωτόκολλα, την επικύρωση και την κρυπτογράφηση. Αναλύει γνωστές απειλές και τον τρόπο που πρέπει να εφαρμόζεται η ασφάλεια σε ένα ασύρματο τοπικό δίκτυο.

Στο τέταρτο κεφάλαιο πραγματοποιείται η παραβίαση της ασύρματης ασφάλειας. Γίνεται επισκόπηση του DNS και του DNS tunneling. Παρουσιάζονται γνωστές υλοποιήσεις DNS Tunneling και επιλέγεται μία από αυτές το Iodine για την πραγματοποίηση της επίθεσης στο Hotspot των Starbucks.

Τέλος, το πέμπτο κεφάλαιο περιγράφει γενικές τεχνικές μετριασμού επιθέσεων, αναλύει τις δύο τεχνικές ανίχνευσης DNS Tunneling και παρουσιάζει την εφαρμογή ορισμένων τεχνικών ανίχνευσης.

Abstract

The purpose of this thesis is to describe the way wireless networks as well DNS Tunnels works and security violation with use of DNS Tunneling. Known DNS Tunneling utilities will be reported. The Iodine utility will be used to bypass a captive portal (or Hotspot's access control lists) and a host will gain access to Internet without to pay money. Afterwards, detection techniques and their implementation will be analyzed.

More specifically, chapter one describes the human need for communication and networking, the definition ,the architecture and the categories that wireless networks are divided into.

Chapter two explains what is the wireless local network and the reasons that it is preferred contrary to the wired network. It describes the evolution, the components, the standards, the topologies of 802.11 standard and way it works.

Chapter three describes the security in the wireless networks, the protocols, the authentication and the encryption. It analyzes known threats and the way that security should be implemented in a wireless local network.

Chapter four describes the violation of wireless security. Overview of DNS and of DNS Tunneling. Known DNS Tunneling utilities are presented and one of them "Iodine" is selected to perform an attack in Starbuck's Hotspot.

In conclusion, chapter five describes general techniques of attacks mitigation, analyze the two techniques of DNS Tunneling detection and presents the implementation of certain techniques of detection.

Ευχαριστίες

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Διδακτική της τεχνολογίας και Ψηφιακά Συστήματα» στην κατεύθυνση «Ψηφιακές Επικοινωνίες και Δίκτυα» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Θα ήθελα να ευχαριστήσω τους καθηγητές μου και πιο συγκεκριμένα τον Επίκουρο Καθηγητή κ. Χρήστο Ξενάκη για την εμπιστοσύνη που μου έδειξε προκειμένου να αναλάβω την παρούσα διπλωματική εργασία που είναι πάνω στον τομέα των ενδιαφερόντων μου. Τον διδάκτορα Χριστόφορο Νταντογιάν για την καθοδήγηση και την επίβλεψη που μου παρείχε για την ολοκλήρωση της διπλωματικής μου εργασίας.

Τέλος εκφράζω την ευγνωμοσύνη μου στους γονείς μου για υποστήριξη και την βοήθεια τους σε όλη την διάρκεια των σπουδών μου.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Γλωσσάρι

Access Point: (AP), μια συσκευή ενός ασύρματου δικτύου η οποία συνδέει τις ασύρματες τελικές συσκευές του δικτύου αυτού μεταξύ τους και με τα ενσύρματα δίκτυα.

Ad Hoc:Η λειτουργία κατά την οποία μία τελική συσκευή μπορεί να συνδεθεί με μια άλλη απευθείας σχηματίζοντας δίκτυο , χωρίς την μεσολάβηση ενός AP.

Address Resolution Protocol: (ARP) , πρωτόκολλο μετάφρασης διευθύνσεων IP σε διευθύνσεις MAC.

Association Identifier: (AID) , ο μοναδικός αριθμός που σχετίζεται με μια συγκεκριμένη σύνδεση ενός Access Point με έναν ασύρματο χρήστη.

Authentication: η διαδικασία πιστοποίησης της ταυτότητας μιας συσκευής.

Beacon: το σήμα που στέλνει ένα AP για διαφημίσει την παρουσία του και μπορεί να περιέχει και άλλες πληροφορίες όπως essid, mac address κ.α.

Basic Service Set Identifier : (BSSID), η MAC διεύθυνση του access point.

Captive Portal: η τεχνική με την οποία ένας χρήστης παραπέμπεται σε μία ειδική ιστοσελίδα (συνήθως για επικύρωση) για να αποκτήσει σύνδεση στο Διαδίκτυο.

Covert Channel: δίνει την δυνατότητα για την μεταφορά δεδομένων και την επικοινωνία μεταξύ διαδικασιών που δεν επιτρέπονται από την πολιτική ασφαλείας.

Domain Name: (DN) ,είναι ένας τομέας, μια καταχώρηση γραμματοσειρά του DNS ο οποίος εκχωρείται για αποκλειστική χρήση σε ένα φυσικό ή νομικό πρόσωπο.

DNS Records: χρησιμοποιούνται για να αντιστοιχίσουν URLs σε διευθύνσεις IP. Διαφορετικοί τύποι χρησιμοποιούνται για διαφορετικό σκοπό.

Domain Name System: (DNS), είναι ένα ιεραρχικό σύστημα ονοματοδοσίας, αντιστοιχίζει ονόματα με διευθύνσεις IP ή άλλα ονόματα στο Διαδίκτυο.

Endianness: ο τρόπος αποθήκευσης των σειρών bytes στην μνήμη ενός ηλεκτρονικού υπολογιστή. Υπάρχουν δύο τρόποι αναπαράστασης των bytes που αναπαριστάται ένας αριθμός μέσα στην εσωτερική μνήμη του υπολογιστή: η αναπαράσταση *big-endian* και η αναπαράσταση *little-endian*

Extended Service Set Identifier: (ESSID), το όνομα του δικτύου.

Fragmentation: η διαδικασία κατά την οποία ένα πακέτο δεδομένων σπάει σε μικρότερα πακέτα για να αποσταλεί και τα οποία επανασυνδέονται στον προορισμό.

Frame: μπορούμε να θεωρήσουμε πως το frame είναι το ίδιο με ένα packet.Η διαφορά είναι ότι στο layer 2 του OSI ορίζεται ως frame ενώ στο layer 3 ως packet.

Fully Qualified Domain Name: είναι ένα Domain Name που διευκρινίζει την ακριβή θέση του στην τριπλή ιεραρχία του DNS. Διακρίνεται για την έλλειψη ασάφειάς του. Μπορεί να ερμηνευθεί με έναν μόνο τρόπο.

Hub: Είναι μια συσκευή μορφή αναμεταδότη πολλαπλών θυρών. Λειτουργεί στο φυσικό επίπεδο (στρώμα 1) του μοντέλου OSI.

Infrastructure: ο τρόπος λειτουργίας κατά τον οποίο μία τελική συσκευή συνδέεται πρώτα με ένα AP και μετά με το δίκτυο.

Interface: είναι το σημείο αλληλεπίδρασης με λογισμικό ή με φυσικό υλικό.

Local Area Network: (LAN), τοπικό δίκτυο.

Media Access Control Address: (Mac Address), ένας 48μπιτ αριθμός που δίνεται σε κάθε κάρτα δικτύου από τον κατασκευαστή της.

Message Integrity Code: (MIC), ένα πεδίο που προσαρτάται για τον έλεγχο της ακεραιότητας των δεδομένων.(αλγόριθμος Michael)

Payload: είναι εκείνο το κομμάτι των μεταδιδόμενων δεδομένων το οποίο είναι ο κύριος σκοπός της μετάδοσης ,εξαιρώντας τα δεδομένα των headers.

Pre-Shared Key: (PSK),κλειδί που παράγεται από έναν κωδικό (passphrase) και χρησιμοποιείται στην διαδικασία της κρυπτογράφησης προκειμένου να ασφαλίσει την κυκλοφορία των δεδομένων μεταξύ των συστημάτων.

Probes: πλαίσια που χρησιμοποιούνται από τους χρήστες ασύρματων συσκευών για να ανακαλύψουν ασύρματα δίκτυα.

Radio Frequency: (RF) ,ραδιοσυχνότητα , ραδιοκύματα.

Regular Expression: (regex) , είναι μια ακολουθία χαρακτήρων που διαμορφώνει ένα σχέδιο αναζήτησης.

Secure Shell: (SSH), είναι ένα ασφαλές δικτυακό πρωτόκολλο το οποίο επιτρέπει τη μεταφορά δεδομένων μεταξύ δύο υπολογιστών

Service Set Identifier: (SSID), αναγνωριστικό όνομα των ασύρματων δικτύων , διαφορετικό από το ESSID.

Session: μια διαρκής σύνδεση δυο συσκευών που χρησιμοποιεί το *επίπεδο συνόδου* ενός πρωτοκόλλου δικτύωσης ή μια διαρκής σύνδεση μεταξύ ενός χρήστη και ενός ομολόγου του, που συνήθως είναι ένας εξυπηρετητής.

Temporary Key Integrity Protocol: (TKIP), πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο WPA και βασίζεται στον αλγόριθμο RC4.

TUN/TAP Interface: εικονικό interface.Υλοποιείται σε λογισμικό. Το TAP χρησιμοποιείται για επικοινωνία σε layer 2 ενώ το TUN για layer 3.

User Datagram Protocol: (UDP), από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Δεν εγγυάται αξιόπιστη επικοινωνία.

Virtual Local Area Network: (VLAN), ένα εικονικό δίκτυο που αποτελείται από εικονικές συνδέσεις. Η εικονική σύνδεση χρησιμοποιεί μεθόδους εικονικής δικτύωσης.

Virtual Private Network: (VPN), δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο. Απαιτεί πιστοποίηση, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης.

Wired Equivalent Privacy: (WEP), το προεπιλεγμένο πρωτόκολλο ασφαλείας για τα δίκτυα 802.11.

Wireless Local Area Network: (WLAN), ένα ασύρματο τοπικό δίκτυο.

Wireless Protected Access: (WPA), πρωτόκολλο ασφαλείας βασίζεται στο TKIP, πολλές φορές αναφέρεται και ως πρώιμη έκδοση του προτύπου IEEE 802.11i. Έγινε διαθέσιμο το 2003.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

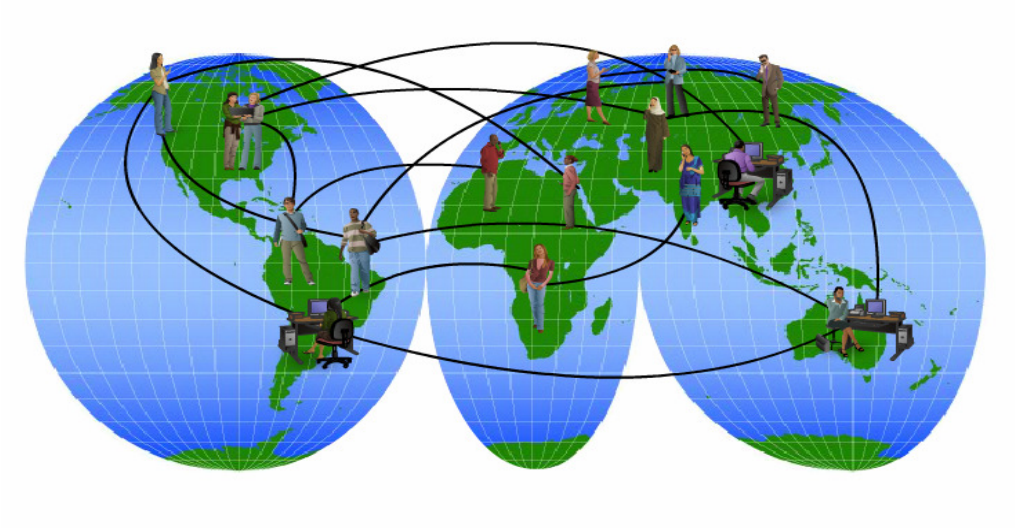
1.1 Γενικά

Μεταξύ όλων των πρώτων αναγκών για την ανθρώπινη ύπαρξη, η ανάγκη για αλληλεπίδραση των ανθρώπων ταξινομείται στις πρώτες θέσεις . Η επικοινωνία είναι τόσο σημαντική για τους ανθρώπους όσο σχεδόν η ανάγκη για νερό, αέρα, τροφή, και στέγη.
Οι μέθοδοι που χρησιμοποιούμε για να μοιραστούμε τις ιδέες και τις πληροφορίες αλλάζουν συνεχώς και εξελίσσονται. Ενώ στο παρελθόν η ανθρώπινη επικοινωνία περιοριζόταν μόνο στις πρόσωπο με πρόσωπο συνομιλίες, οι σημαντικές ανακαλύψεις και εξελίξεις των μέσων επέκτειναν τις επικοινωνίες μας. Από την εφημερίδα στην τηλεόραση και στον ηλεκτρονικό Τύπο, κάθε νέα ανάπτυξη έχει βελτιώσει και έχει ενισχύσει τις επικοινωνίες μας.

Σημαντική επίδραση στην πρόοδο της τεχνολογίας των επικοινωνιών έχει η δημιουργία και η διασύνδεση των **δικτύων δεδομένων**.

Τα πρόωρα δίκτυα δεδομένων περιορίστηκαν στην ανταλλαγή απλών χαρακτήρων μεταξύ των συνδεδεμένων ηλεκτρονικών υπολογιστών. Τα τρέχοντα δίκτυα έχουν εξελιχθεί και μπορούν να μεταφέρουν φωνή, βίντεο, κείμενα, και εικόνες μεταξύ πολλών διαφορετικών τύπων συσκευών. Παρέχουν πρόσβαση σε ένα ευρύ φάσμα εναλλακτικών και νέων μεθόδων επικοινωνίας που επιτρέπουν στους ανθρώπους να αλληλεπιδρούν άμεσα ο ένας με τον άλλον σχεδόν στιγμιαία.
.
Η άμεση φύση των επικοινωνιών μέσω του Διαδικτύου ενθαρρύνει το σχηματισμό παγκόσμιων κοινοτήτων. Αυτές οι κοινότητες ενθαρρύνουν την κοινωνική αλληλεπίδραση που είναι ανεξάρτητη από τη θέση ή τη διαφορά ώρας.

Τα δίκτυα δεδομένων υποστηρίζουν τον τρόπο που ζούμε, μαθαίνουμε, εργαζόμαστε, και παίζουμε. Παρέχουν την πλατφόρμα στις υπηρεσίες που μας επιτρέπουν να συνδεθούμε - και τοπικά και παγκόσμια - με τις οικογένειες, τους φίλους, την εργασία, και τα ενδιαφέροντά μας.



Εικόνα 1. Η παγκοσμιοποίηση των επικοινωνιών.

1.2 Τι είναι δίκτυο δεδομένων

Ένα δίκτυο δεδομένων είναι ένα σύστημα επικοινωνίας που συνδέει δύο ή περισσότερες αυτόνομες και ανεξάρτητες τελικές συσκευές που μπορούν να ανταλλάζουν μεταξύ τους πληροφορίες.

Η εικόνα 2 παρουσιάζει τα στοιχεία ενός χαρακτηριστικού δικτύου.

Εικόνα 2. Ένα χαρακτηριστικό δίκτυο και τα στοιχεία του.

Σ ένα δίκτυο δεδομένων συμπεριλαμβάνονται :

- Οι συσκευές
- Το μέσο
- Οι κανόνες
- Τα δεδομένα

Οι συσκευές δικτύων με τις οποίες οι περισσότεροι άνθρωποι είναι εξοικειωμένοι καλούνται τερματικές συσκευές . Αυτές οι συσκευές διαμορφώνουν τη διεπαφή μεταξύ του ανθρώπινου δικτύου και του δικτύου επικοινωνίας.
Μερικά παραδείγματα τερματικών συσκευών είναι:

- Υπολογιστές (σταθμοί εργασίας, laptops, διακομιστές αρχείων, κεντρικοί υπολογιστές δικτύου-web servers)
- Εκτυπωτές δικτύων
- Τηλέφωνα VoIP

- Κάμερες ασφαλείας
- Κινητές και φορητές συσκευές (όπως οι ασύρματοι ανιχνευτές barcode, PDAs)

Εκτός από τις τερματικές συσκευές με τις οποίες οι περισσότεροι άνθρωποι είναι εξοικειωμένοι , τα δίκτυα στηρίζονται στις ενδιάμεσες συσκευές για να παρέχουν συνδεσιμότητα και για να εξασφαλίσουν τις ροές των δεδομένων στο δίκτυο. Αυτές οι συσκευές συνδέουν μεμονωμένες τερματικές συσκευές με το δίκτυο αλλά μπορούν και να συνδέσουν πολλαπλά μεμονωμένα δίκτυα για να διαμορφώσουν ένα υπερδίκτυο.

Παραδείγματα των ενδιάμεσων συσκευών δικτύων είναι:

- Οι συσκευές πρόσβασης στο δίκτυο (hubs, switches και ασύρματα σημεία πρόσβασης).
- Οι συσκευές σύνδεσης δικτύων (δρομολογητές-routers).
- Τα modems.
- Οι συσκευές ασφάλειας (firewalls).

Η επικοινωνία σ ένα δίκτυο μεταξύ των συσκευών του γίνεται μ ένα μέσο. Το μέσο αυτό παρέχει το κανάλι μέσα από το οποίο το μήνυμα ταξιδεύει από την πηγή στον προορισμό.

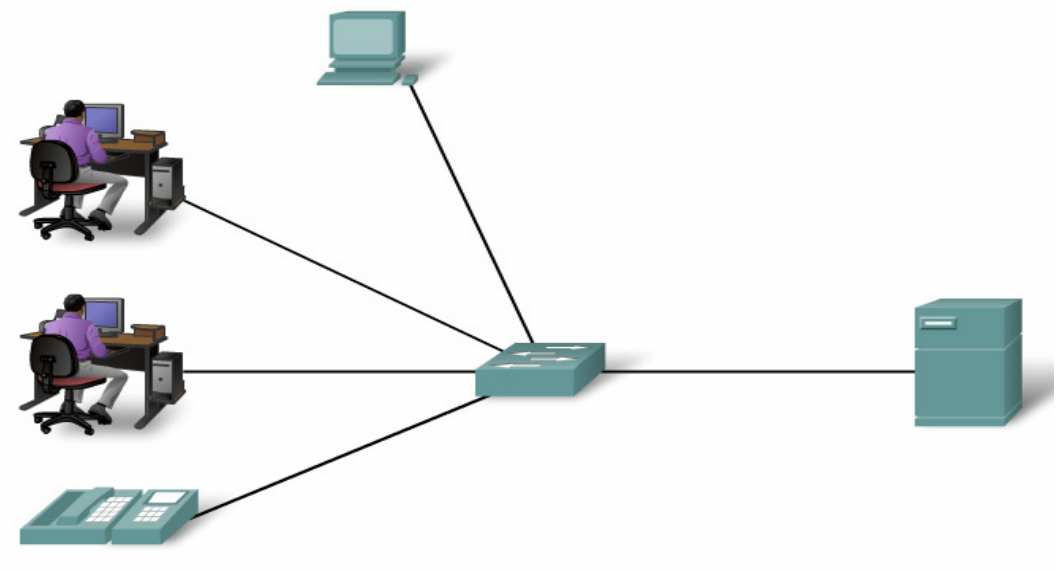
Τα σύγχρονα δίκτυα χρησιμοποιούν κυρίως τρεις τύπους μέσων για να διασυνδέσουν τις συσκευές και για να παρέχουν το κανάλι μέσα από το οποίο τα δεδομένα μπορούν να διαβιβαστούν. Αυτά τα μέσα είναι:

1. Μεταλλικά καλώδια.
2. Γυαλί ή πλαστικές ίνες (καλώδιο οπτικών ινών).
3. Ηλεκτρομαγνητικά κύματα.

Οι υποδομές των δικτύων μπορούν να ποικίλουν ανάλογα:

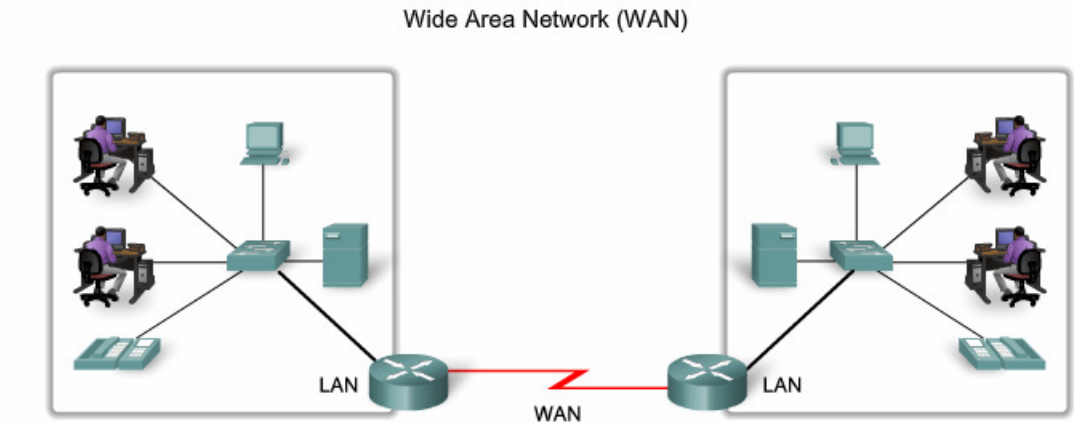
- Το μέγεθος της περιοχής που καλύπτουν.
- Τον τηλεπικοινωνιακό φορέα εξυπηρέτησης.
- Το φυσικό μέσο μετάδοσης.

Ένα μεμονωμένο δίκτυο που εκτείνεται συνήθως σε μια ενιαία γεωγραφική περιοχή, παρέχοντας υπηρεσίες και εφαρμογές σε ανθρώπους μέσα σε μια κοινή οργανωτική δομή, όπως μια επιχείρηση, μια πανεπιστημιούπολη ή μια περιοχή καλείται δίκτυο τοπικής περιοχής (LAN). Το LAN ελέγχεται συνήθως από μια ενιαία οργάνωση.



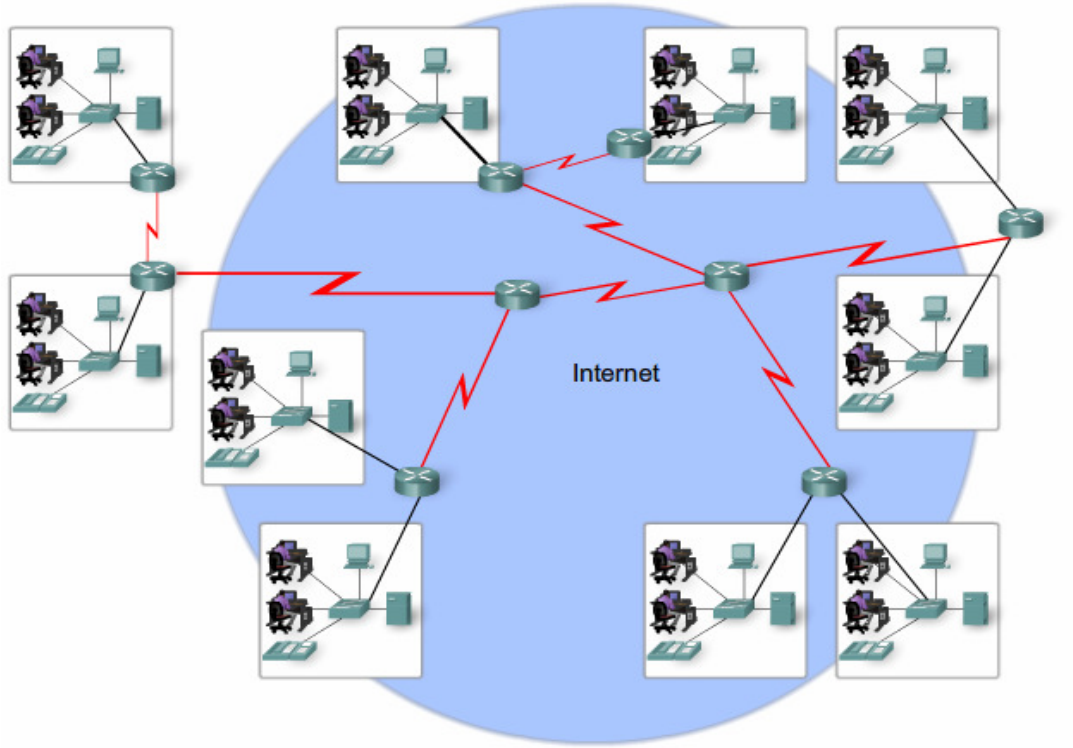
Εικόνα 3. Ένα δίκτυο τοπικής περιοχής (LAN).

Μεγάλοι οργανισμοί και επιχειρήσεις μισθώνουν συνήθως συνδέσεις μέσω ενός δικτύου προμηθευτών τηλεπικοινωνιακών υπηρεσιών προκειμένου να ενώσουν τα τοπικά δίκτυα τους που βρίσκονται σε διαφορετική γεωγραφική περιοχή. Αυτά τα δίκτυα που συνδέουν LANs σε γεωγραφικά χωρισμένες θέσεις αναφέρονται ως δίκτυα ευρείας περιοχής (WANs).



Εικόνα 4.Ένα δίκτυο ευρείας περιοχής (WAN).

Ένα σφαιρικό πλέγμα διασυνδεμένων δικτύων (internetworks) ικανοποιεί τις ανθρώπινες ανάγκες επικοινωνίας. Μερικά από αυτά τα διασυνδεμένα δίκτυα ανήκουν σε μεγάλες δημόσιες και ιδιωτικές οργανώσεις, ή βιομηχανικές επιχειρήσεις, και προορίζονται για την αποκλειστική ιδιωτική χρήση τους. Το πιο γνωστό και ευρέως χρησιμοποιημένο δημόσια-προσιτό internetwork είναι το Διαδίκτυο (Internet).



Εικόνα 5.Τα LANs και τα WANs όταν διασυνδεθούν αποτελούν ένα Internetwork.

Ανάλογα τον τηλεπικοινωνιακό φορέα εξυπηρέτησης διακρίνονται σε ιδιωτικά ή δημόσια.

Ανάλογα το φυσικό μέσο μετάδοσης χωρίζονται σε ενσύρματα και ασύρματα. Τα ενσύρματα δίκτυα χρησιμοποιούν ως φυσικό μέσο μετάδοσης τα καλώδια τα οποία περιέχουν είτε κάποιο μέταλλο, είτε γυαλί, είτε πλαστικό. Τα ασύρματα δίκτυα σε αντίθεση χρησιμοποιούν τα ηλεκτρομαγνητικά κύματα για την μετάδοση των δεδομένων. Οι συχνότητες στις οποίες συνήθως λειτουργούν τα ασύρματα δίκτυα είναι τα 2,4 και 5 GHz.Στην πραγματικότητα τις περισσότερες φορές τα δίκτυα που συναντάμε είναι μεικτά. Ενσύρματα και ασύρματα επικοινωνούν μεταξύ τους με συγκεκριμένους κανόνες και πρότυπα.

Ωστόσο τα τελευταία χρόνια οι ασύρματες επικοινωνίες ολοένα και αναπτύσσονται καταλαμβάνοντας περισσότερο έδαφος στον τομέα των τηλεπικοινωνιών.

Τόσο η αλλαγή του τρόπου ζωής του σύγχρονου ανθρώπου όσο και η εξέλιξη των νέων τηλεπικοινωνιακών τεχνολογιών έκαναν την ανάγκη για ασύρματη επικοινωνία επιτακτικότερη!

ΚΕΦΑΛΑΙΟ 2

2.1 Τι είναι το ασύρματο τοπικό δίκτυο (WLAN)

Το ασύρματο τοπικό δίκτυο (WLAN) είναι ότι ακριβώς υπονοεί και το όνομά του. Παρέχει όλα τα χαρακτηριστικά γνωρίσματα και τα οφέλη των παραδοσιακών τεχνολογιών του τοπικού δικτύου Ethernet , αλλά χωρίς τους περιορισμούς των καλωδίων .Κατά συνέπεια, τα ασύρματα τοπικά δίκτυα (WLANs) επαναπροσδιορίζουν τον τρόπο με τον οποίο έβλεπαν μέχρι σήμερα οι βιομηχανίες τα δίκτυα. Η συνδεσιμότητα δεν υπονοεί πλέον τη σύνδεση σε κάτι στατικό.
Οι περιοχές του δικτύου δεν μετριούνται πια με μέτρα, αλλά με χιλιόμετρα.
Η υποδομή του δικτύου δεν χρειάζεται να θαφτεί στο έδαφος ή να κρυφτεί πίσω από τοίχους. Η υποδομή είναι δυναμική και όχι στατική. Μπορεί να μετακινηθεί και να παραμετροποιηθεί ανάλογα με τις ανάγκες κάθε φορά.

Ένα ασύρματο τοπικό δίκτυο WLAN, όπως ακριβώς και ένα τοπικό δίκτυο LAN, απαιτεί ένα φυσικό μέσο μέσω του οποίου μεταφέρονται τα δεδομένα. Αντί για τη χρήση διαφόρων τύπων καλωδίων, τα WLAN χρησιμοποιούν την υπέρυθρη ακτινοβολία (IR) ή τα ηλεκτρομαγνητικών κύματα με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο.
Τα WLAN χρησιμοποιούν τις ζώνες συχνοτήτων (RF) των 2,4 GHz και 5 GHz . Αυτά τα τμήματα του φάσματος ραδιοσυχνοτήτων είναι δεσμευμένα στο μεγαλύτερο μέρος του κόσμου για συσκευές χωρίς άδεια. Η ασύρματη δικτύωση παρέχει την ελευθερία και την ευελιξία να λειτουργεί εντός των κτιρίων και μεταξύ διαφορετικών κτιρίων.

Τα ασύρματα συστήματα δεν είναι εντελώς ασύρματα. Οι ασύρματες συσκευές είναι μόνο ένα μέρος του παραδοσιακού ενσύρματου δικτύου. Αυτά τα ασύρματα συστήματα, έχουν σχεδιαστεί και κατασκευαστεί με συγκεκριμένα πρότυπα μικροεπεξεργαστών και ψηφιακών κυκλωμάτων, ώστε να συνδέονται στα παραδοσιακά ενσύρματα συστήματα. Επιπλέον, οι ασύρματες συσκευές πρέπει με κάποιο τρόπο να τροφοδοτούνται με ρεύμα για να μπορούν να λειτουργήσουν.

Η πρώτη γενιά συσκευών WLAN, με τις χαμηλές ταχύτητες και την έλλειψη προτύπων ,δεν ήταν δημοφιλής. Μοντέρνα τυποποιημένα συστήματα έχουν πλέον την δυνατότητα να μεταφέρουν δεδομένα σε αποδεκτές ταχύτητες.

Η ασύρματη τεχνολογία, υποστηρίζει πλεον τα μεγέθη, την ταχύτητα των δεδομένων και την διαλειτουργικότητα που είναι απαραίτητα για την συνεργασία με τα ενσύρματα δίκτυα. Επίσης, το κόστος των νέων ασύρματων συσκευών έχει μειωθεί σημαντικά. Η ασύρματη επικοινωνία είναι πλέον προσιτή επιλογή. Στις περισσότερες χώρες για την χρήση των ασύρματων συσκευών δεν απαιτείται ειδική άδεια.

2.2 Γιατί ασύρματη επικοινωνία;

Τα τρέχοντα ενσύρματα τοπικά δίκτυα LAN λειτουργούν σε ταχύτητες γύρω στα 100 Mbps στο επίπεδο "πρόσβασης" και έως και 10 Gbps στο επίπεδο του "κορμού". Τα περισσότερα ασύρματα δίκτυα WLANs λειτουργούν στα 11 Mbps και 54 Mbps στο επίπεδο πρόσβασης και δεν προορίζονται να λειτουργούν στο επίπεδο του κορμού.Το κόστος της εφαρμογής των WLAN είναι ανταγωνιστικό με αυτό των ενσύρματων LAN.

Γιατί όμως να εγκαταστήσουμε ένα σύστημα το οποίο έχει χαμηλότερες δυνατότητες μεταφοράς δεδομένων;

Ένας λόγος είναι ότι σε πολλά μικρά περιβάλλοντα τοπικών δικτύων, ακόμα και οι πιο αργές ταχύτητες των ασύρματων δικτύων είναι κατάλληλες να υποστηρίξουν τις ανάγκες των χρηστών. Με πολλά γραφεία τώρα συνδεδεμένα στο Διαδίκτυο μέσω ευρυζωνικών υπηρεσιών DSL, τα WLAN μπορούν να χειριστούν τις απαιτήσεις εύρους ζώνης.
Ένας άλλος λόγος είναι ότι τα WLANs επιτρέπουν στους χρήστες να κινούνται σε μια καθορισμένη περιοχή και να εξακολουθούν να παραμένουν συνδεδεμένοι.
Επίσης σε μια πιθανή αναδιάρθρωση των γραφείων ,τα WLAN δεν απαιτούν επανεγκατάσταση και μεταφορά των καλωδιώσεων αποφεύγοντας τα συναφή έξοδα.

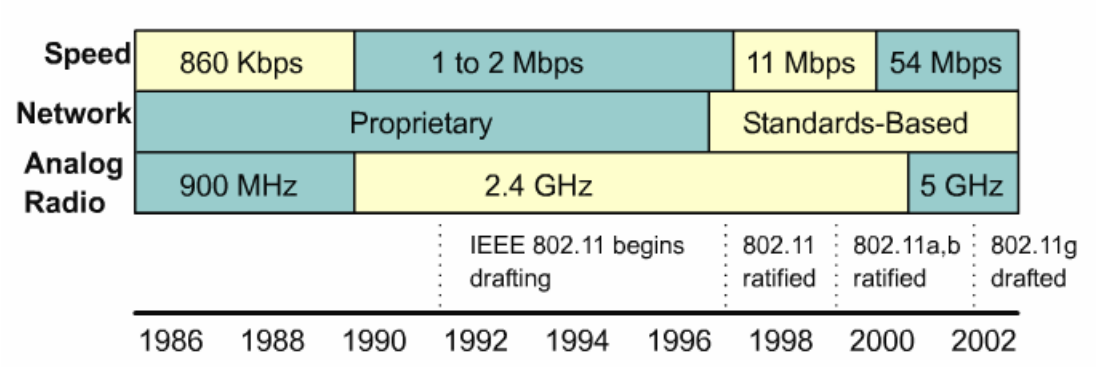
Τα WLANs έχουν πολλά πλεονεκτήματα για το σπίτι, τις μικρές επιχειρήσεις, τις μικρομεσαίες επιχειρήσεις και τις μεγαλύτερες εταιρείες.
Τα περιβάλλοντα που είναι πιθανό να επωφεληθούν από ένα WLAN έχουν τα ακόλουθα χαρακτηριστικά:

- Απαιτούν συγκεκριμένες ταχύτητες Ethernet
- Επωφελούνται από την περιαγωγή των χρηστών
- Αλλάζουν τη φυσική διάταξη των γραφείων συχνά
- Επεκτείνονται ταχέως
- Χρησιμοποιούν μια ευρυζωνική σύνδεση Internet
- Αντιμετωπίζουν σημαντικές δυσκολίες στην εγκατάσταση ενσύρματου LAN
- Χρειάζονται συνδέσεις μεταξύ δύο ή περισσότερων LANs σε μια μητροπολιτική περιοχή
- Απαιτούν χρήση προσωρινών γραφείων και δικτύων

Μολονότι τα WLANs είχαν πρωτίστως σχεδιασθεί ως συσκευές τοπικού δικτύου, μπορούν να χρησιμοποιηθούν για σύνδεση site-to-site σε αποστάσεις μέχρι 40 χιλιομέτρων. Η χρήση των WLAN συσκευών είναι πολύ καλύτερη από άποψη κόστους απ' ότι η χρήση WAN ή την εγκατάσταση ή την ενοικίαση μια γραμμής. Για παράδειγμα, το κόστος για την εγκατάσταση ενός WLAN ανάμεσα σε δύο κτίρια θα κοστίσει για μία φορά αρκετές χιλιάδες ευρώ. Η αποκλειστική μίσθωση μιας γραμμής T1, που παρέχει λιγότερες δυνατότητες από ένα WLAN, μπορεί εύκολα να κοστίσει εκατοντάδες ευρώ ανά μήνα ή και περισσότερο. Η εγκατάσταση οπτικών ινών σε απόσταση μεγαλύτερη από 1,6 km είναι πολλή δύσκολη και θα κοστίσει πολύ περισσότερο από μια ασύρματη λύση.

2.3 Η εξέλιξη των ασύρματων δικτύων.

Οι πρώτες ασύρματες τεχνολογίες τοπικών δικτύων καθορίστηκαν από το πρότυπο 802.11 και ήταν χαμηλής ταχύτητας από 1 έως 2 Mbps.
Παρά τις μικρές δυνατότητες, η ελευθερία και η ευελιξία της ασύρματης τεχνολογίας επέτρεψαν μια θέση στις αγορές της τεχνολογίας. Οι εργαζόμενοι στο λιανικό εμπόριο και σε μεγάλες αποθήκες που έπρεπε συνέχεια να κινούνται χρησιμοποίησαν πρώτοι φορητές συσκευές για τη διαχείριση, την καταγραφή και τη συλλογή δεδομένων.
Αργότερα, τα νοσοκομεία εφάρμοσαν τη ασύρματη τεχνολογία για να συγκεντρώνουν και να παραδίδουν πληροφορίες για τους ασθενείς. Όταν οι ηλεκτρονικοί υπολογιστές άρχισαν να μπαίνουν στις τάξεις, τα σχολεία και τα πανεπιστήμια κατασκεύασαν ασύρματα δίκτυα για να αποφύγουν τις δαπάνες καλωδιακών εγκαταστάσεων και προσέφεραν ταυτόχρονα κοινή ασύρματη πρόσβαση στο Διαδίκτυο.
Αναγνωρίζοντας την ανάγκη για ένα ενιαίο πρότυπο, οι κατασκευαστές και προμηθευτές ασυρμάτων συσκευών ενώθηκαν το 1991 και διαμόρφωσαν την "ασύρματη συμμαχία συμβατότητας Ethernet" (WECA).Η WECA πρότεινε και έχτισε πρότυπα βασισμένα στις ασύρματες τεχνολογίες. Η WECA αργότερα άλλαξε το όνομά της σε WI-Fi. Τον Ιούνιο του 1997,η IEEE δημοσίευσε τα πρότυπα 802.11 για την ασύρματη τοπική δικτύωση.
Η εικόνα 6 επεξηγεί την εξέλιξη των ασύρματων τοπικών δικτύων.



Εικόνα 6. Η εξέλιξη των ασύρματων τοπικών δικτύων στο χρόνο.

Οι τρέχουσες τεχνολογίες WLAN προσφέρουν αυξανόμενα μεγέθη και ταχύτητες μεταφοράς δεδομένων, καλύτερη αξιοπιστία και αυτονομία και μειωμένες δαπάνες. Οι δυνατότητες μεταφοράς δεδομένων έχουν αυξηθεί από 1 Mbps σε 54 Mbps, η διαλειτουργικότητα έχει γίνει πραγματικότητα με την εισαγωγή των προτύπων της IEEE 802.11 και οι τιμές έχουν μειωθεί εντυπωσιακά.
Δεδομένου ότι τα WLANs γίνονται δημοφιλέστερα με τα χρόνια, οι κατασκευαστές μπορούν όλο και περισσότερο να προσφέρουν οικονομικότερες λύσεις. Θα υπάρξουν πολλές βελτιώσεις στο μέλλον. Παραδείγματος χάριν, πολλές αδυναμίες έχουν βρεθεί στις ρυθμίσεις ασφάλειας των ασυρμάτων δικτύων και η ισχυρότερη ασφάλεια σε όλα τα μελλοντικά προϊόντα είναι στις προτεραιότητες των κατασκευαστών.

2.4 Ασύρματα πρότυπα δικτύωσης

Η προτυποποίηση των λειτουργιών των δικτύων έχει συμβάλει πολύ στην ανάπτυξη προσιτών και διαλειτουργικών προϊόντων. Αυτό ισχύει και για τα ασύρματα προϊόντα επίσης. Πριν από την ανάπτυξη των προτύπων, τα ασύρματα συστήματα "έπασχαν" με χαμηλούς ρυθμούς μεταφοράς δεδομένων, ασυμβατότητα και υψηλά κόστη.

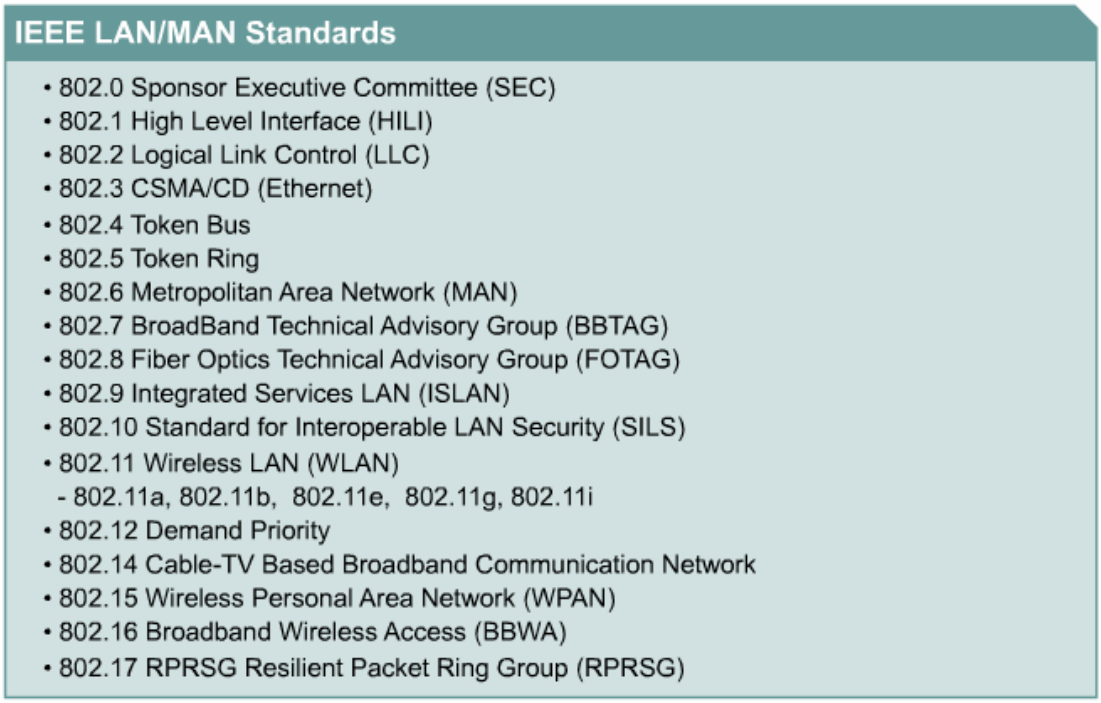
Η προτυποποίηση παρέχει όλα τα ακόλουθα οφέλη:

- Διαλειτουργικότητα μεταξύ των προϊόντων διαφορετικών προμηθευτών
- Γρηγορότερη ανάπτυξη και εξέλιξη προϊόντων
- Σταθερότητα
- Δυνατότητα αναβαθμίσεων
- Μειώσεις στο κόστος

Μερικοί σημαντικοί οργανισμοί προτύπων παρουσιάζονται στην εικόνα 7.

Εικόνα 7. Οργανισμοί προτύπων.

Η IEEE, ιδρύθηκε το 1884, είναι ένας μη κερδοσκοπικός επαγγελματικός οργανισμός που αποτελείται από πάνω από 377.000 μέλη παγκοσμίως. Η IEEE αποτελείται από πολλές μεμονωμένες κοινωνίες και ομάδες εργασίας. Διαδραματίζει έναν κρίσιμο ρόλο στην ανάπτυξη των προτύπων, την έκδοση των τεχνικών εργασιών, υποστηρίζει διασκέψεις και παρέχει πιστοποιήσεις στον τομέα των ηλεκτρικών και ηλεκτρονικών τεχνολογιών. Στον τομέα των δικτύων, η IEEE έχει παραγάγει πολλά ευρέως χρησιμοποιημένα πρότυπα όπως το σύνολο των 802.x προτύπων δικτύων τοπικής και μητροπολιτικής περιοχής, τα οποία παρατίθενται στην παρακάτω εικόνα.



Εικόνα 8. Λίστα προτύπων της ομάδας 802.x .

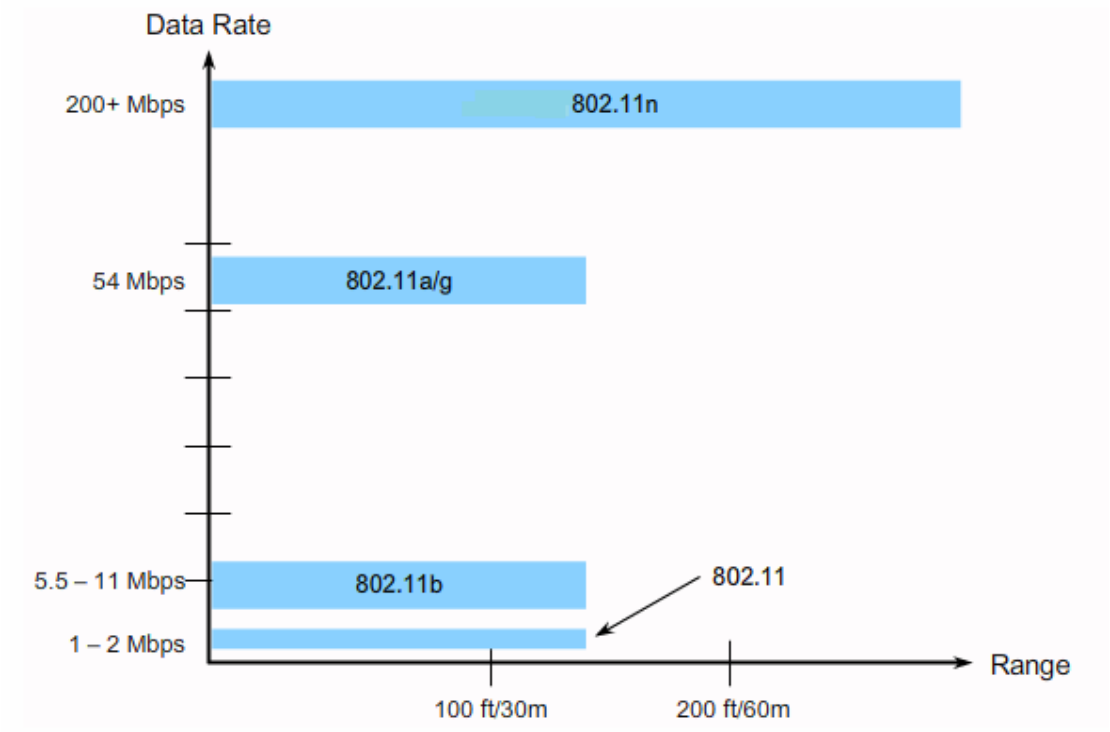
IEEE 802.11

Ο όρος 802.11 στην πραγματικότητα αναφέρεται σε μια οικογένεια πρωτοκόλλων, συμπεριλαμβανομένων των αρχικών προδιαγραφών των 802.11 , 802.11 b,802.11 a, 802.11 g και άλλων, όπως παρουσιάζονται στην εικόνα.

Το πρότυπο 802.11 είναι ένα ασύρματο πρότυπο που καθορίζει τη συνδεσιμότητα για σταθερές, φορητές και κινούμενες συσκευές σε μια τοπική περιοχή. Σκοπός του προτύπου είναι να παρέχει ασύρματη συνδεσιμότητα σε αυτοματοποιημένα μηχανήματα και εξοπλισμούς που απαιτούν ταχεία επέκταση.

Όταν το πρότυπο 802.11 πρωτοδημοσιεύθηκε, όριζε ρυθμούς μεταφοράς δεδομένων 1-2 Mb/s στα 2.4 Ghz. Εκείνη την εποχή ,τα ενσύρματα τοπικά δίκτυα λειτουργούσαν στα 10 Mb/s και έτσι η νέα ασύρματη τεχνολογία δεν υιοθετήθηκε ενθουσιωδώς. Από τότε, τα ασύρματα πρότυπα βελτιώνονται συνεχώς με την δημοσίευση νέων προτύπων όπως είναι το IEEE 802.11a,το IEEE 802.11b,το IEEE 802.11g και το 802.11n.

Συνήθως, η επιλογή του πρότυπου του WLAN που θα χρησιμοποιηθεί βασίζεται στον ρυθμό μεταφοράς δεδομένων. Για παράδειγμα, τα πρότυπα 802.11 a και g μπορούν να υποστηρίξουν έως και 54 Mb/s, ενώ το 802.11 b υποστηρίζει έως 11 Mb/s, καθιστώντας το 802.11 b ένα "αργό" πρότυπο .



Εικόνα 9. Τα πρότυπα των ασύρματων τοπικών δικτύων.

Οι ρυθμοί δεδομένων στα διάφορα ασύρματα πρότυπα, επηρεάζονται από την τεχνική διαμόρφωσης που θα επιλεγεί για το κάθε πρότυπο.
Δύο τεχνικές διαμόρφωσης είναι η διασπορά φάσματος άμεσης ακολουθίας (DSSS) και η ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM).
Όταν ένα πρότυπο χρησιμοποιεί OFDM, έχει ταχύτερους ρυθμούς δεδομένων.
Επίσης, η διαμόρφωση DSSS είναι απλούστερη από ότι η OFDM και έτσι είναι λιγότερο δαπανηρή να εφαρμοστεί.

802.11 a

Το πρότυπο IEEE 802.11 a υιοθέτησε την τεχνική διαμόρφωσης OFDM και χρησιμοποιεί την συχνότητα των 5 GHz . Οι συσκευές που λειτουργούν στη ζώνη των 5 GHz είναι λιγότερο πιθανό να αντιμετωπίσουν κάποιο πρόβλημα από παρεμβολές σε αντίθεση με τις συσκευές που λειτουργούν στη ζώνη 2,4 GHz γιατί υπάρχουν λιγότερες συσκευές που χρησιμοποιούν την ζώνη των 5 GHz.
Επίσης, οι υψηλότερες συχνότητες επιτρέπουν τη χρήση μικρότερων κεραιών.

Υπάρχουν όμως και ορισμένα σημαντικά μειονεκτήματα στη χρήση της συχνότητας των 5 GHz. Το πρώτο είναι ότι τα κύματα υψηλότερων ραδιοσυχνοτήτων είναι πιο εύκολο να απορροφηθούν από εμπόδια όπως είναι οι τοίχοι, καθιστώντας το πρότυπο 802.11 a επιρρεπές σε κακή απόδοση εξαιτίας εμπόδιων. Το δεύτερο είναι ότι αυτή η ανώτερη ζώνη συχνότητας έχει ελαφρώς μικρότερη ακτίνα δράσης από τα 802,11 b και g. Επίσης, σε ορισμένες χώρες, συμπεριλαμβανομένης της Ρωσίας, δεν επιτρέπεται η χρήση των 5 GHz, κάτι το οποίο είναι ανασταλτικό για την ανάπτυξη του προτύπου

802.11 b και 802.11 g

Στο πρότυπο 802,11b ορίζονται ρυθμοί δεδομένων 1, 2, 5.5 και 11 Mb/s στην ζώνη συχνοτήτων 2,4 GHz με την χρήση της τεχνικής διαμόρφωσης DSSS. Το πρότυπο 802,11 g επιτυγχάνει υψηλότερους ρυθμούς δεδομένων στην ίδια συχνότητα, χρησιμοποιώντας όμως τεχνική διαμόρφωσης OFDM . Το IEEE 802.11 g προσδιορίζει επίσης τη χρήση της διαμόρφωσης DSSS για συμβατότητα με τα συστήματα 802.11 b.
Στο πρότυπο 802.11 g υποστηρίζονται με τεχνική διαμόρφωσης DSSS ρυθμοί δεδομένων 1, 2, 5.5 και 11 Mb/s, όπως και ρυθμοί δεδομένων 6, 9, 12, 18, 24, 48, και 54 Mb/s με την χρήση OFDM διαμόρφωσης.

Υπάρχουν πλεονεκτήματα με τη χρησιμοποίηση της συχνότητας των 2,4 GHz. Οι συσκευές στη ζώνη 2,4 GHz έχουν μεγαλύτερη ακτίνα από αυτές στην ζώνη των 5GHz. Επίσης, η μετάδοση σε αυτή την ζώνη συχνοτήτων δεν αντιμετωπίζει τόσο έντονο πρόβλημα εμποδίων όσο το πρότυπο 802.11 a.

Υπάρχει και ένα σημαντικό μειονέκτημα στη χρήση των 2,4 GHz. Πολλές συσκευές άλλων χρήσεων χρησιμοποιούν επίσης τα 2,4 GHz με αποτέλεσμα οι συσκευές των 802.11 b και g να είναι επιρρεπείς σε παρεμβολές.

802.11 n

Το πρότυπο IEEE 802.11 n αποσκοπεί στην βελτίωση των ρυθμών μεταφοράς δεδομένων και της ακτίνας δράσης στα ασύρματα τοπικά δίκτυα, χωρίς να απαιτείται πρόσθετη ισχύς η αλλαγή ζώνης ραδιοσυχνοτήτων.
Το 802,11 n δημιουργεί πολλαπλές ροές δεδομένων στην ίδια συχνότητα. Η τεχνολογία πολλαπλής εισόδου/πολλαπλής εξόδου (MIMO) διαχωρίζει μία υψηλού ρυθμού δεδομένων ροή σε πολλαπλές ροές χαμηλότερου ρυθμού και
τις εκπέμπει ταυτόχρονα από τις διαθέσιμες κεραίες. Αυτή η χρήση των πολλαπλών ροών επιτρέπει μια μέγιστη θεωρητική ταχύτητα μεταφοράς δεδομένων της τάξεως των 600 Mb/s. Το πρότυπο επικυρώθηκε στις 29 Οκτωβρίου 2009.

Wireless LAN Standards

	802.11a	802.11b	802.11g		802.11n
Band	5.7 GHz	2.4 GHz	2.4 GHz		Unconfirmed Possibly 2.4 and 5 GHz bands
Channels*	Up to 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Data Rates	Up to 54 Mbps	Up to 11 Mbps	Up to 11 Mbps	Up to 54 Mbps	Speculated to be 248 Mbps for two MIMO streams
Range	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters		~230 feet or 70 meters
Release Date	October 1999	October 1999	June 2003		October 2009
Pros	Fast, less prone to interference	Low cost, good range	Fast, good range, not easily obstructed		Very good data rates, improved range
Cons	Higher cost, shorter range	Slow, prone to interference	Prone to interference from appliances operating on 2.4 GHz band		

Πίνακας 1. Τα πρότυπα των ασύρματων τοπικών δικτύων και τα χαρακτηριστικά τους.

2.5 Η πιστοποίηση Wi-Fi

Η πιστοποίηση Wi-Fi παρέχεται από την Wi-Fi Alliance (http://www.wi-fi.org), μια παγκόσμια, μη κερδοσκοπική, ένωση που αφιερώνεται στην προώθηση της ανάπτυξης και της αποδοχής των ασύρματων τοπικών δικτύων.
Η ένωση αυτή διαδραμάτισε σημαντικό ρόλο στο πλαίσιο των πρότυπων στα ασύρματα τοπικά δίκτυα.

Τα πρότυπα εξασφαλίζουν διαλειτουργικότητα μεταξύ συσκευών που είναι από διαφορετικούς κατασκευαστές. Διεθνώς, οι τρεις κυριότερες οργανώσεις που επηρεάζουν τα WLAN πρότυπα είναι:

- ITU-R
- IEEE
- Wi-Fi Alliance

Η ITU-R ρυθμίζει την κατανομή του φάσματος ραδιοσυχνοτήτων και τις δορυφορικές τροχιές. Αυτά περιγράφονται ως πεπερασμένοι φυσικοί πόροι που είναι σε ζήτηση από καταναλωτές των σταθερών ασυρμάτων δικτύων, των κινητών ασυρμάτων δικτύων και των συστημάτων παγκόσμιας πλοήγησης.

Η IEEE ανέπτυξε και διατηρεί τα πρότυπα για τα τοπικά και μητροπολιτικά δίκτυα με την IEEE 802 LAN/MAN οικογένεια προτύπων. Η IEEE 802 ρυθμίζεται από τη IEEE 802 LAN/MAN Επιτροπή προτύπων (LMSC), η οποία επιτηρεί πολλές ομάδες εργασίας. Τα κυρίαρχα πρότυπα στην IEEE 802 οικογένεια είναι το 802.3 Ethernet, το 802.5 και το ασύρματο τοπικό δίκτυο 802.11.

Αν και η IEEE έχει διευκρινίσει πρότυπα για τις συσκευές διαμόρφωσης RF, δεν έχει διευκρινίσει πρότυπα κατασκευής, έτσι οι ερμηνείες των 802.11 προτύπων από διαφορετικούς προμηθευτές μπορούν να προκαλέσουν προβλήματα διαλειτουργικότητας μεταξύ των συσκευών τους.

Η WI-Fi Alliance είναι μια ένωση προμηθευτών των οποίων στόχος είναι να βελτιωθεί η διαλειτουργικότητα των προϊόντων που βασίζονται στα πρότυπα 802.11. Αυτό γίνεται με την πιστοποίηση των προμηθευτών για την προσαρμογή τους στα πρότυπα και στους κανόνες της βιομηχανίας. Η πιστοποίηση περιλαμβάνει και τις τρεις IEEE 802.11 RF τεχνολογίες.

Οι ρόλοι αυτών των τριών οργανώσεων μπορούν να συνοψιστούν ως εξής:

- Η ITU-R ρυθμίζει την κατανομή των ζωνών ραδιοσυχνοτήτων.
- Η IEEE διευκρινίζει πώς οι ραδιοσυχνότητες είναι διαμορφωμένες για να φέρουν τις πληροφορίες.
- Η πιστοποίηση wi-Fi εξασφαλίζει ότι οι προμηθευτές κατασκευάζουν συσκευές που είναι διαλειτουργικές.

Η πιστοποίηση Wi Fi αποτελεί και για τον αγοραστή μία εγγύηση ότι το προϊόν που αγόρασε μπορεί να λειτουργήσει χωρίς κανένα πρόβλημα με άλλες συσκευές στα πλαίσια ενός ασύρματου τοπικού δικτύου.

Εικόνα 10. Η πιστοποίηση Wi-Fi.

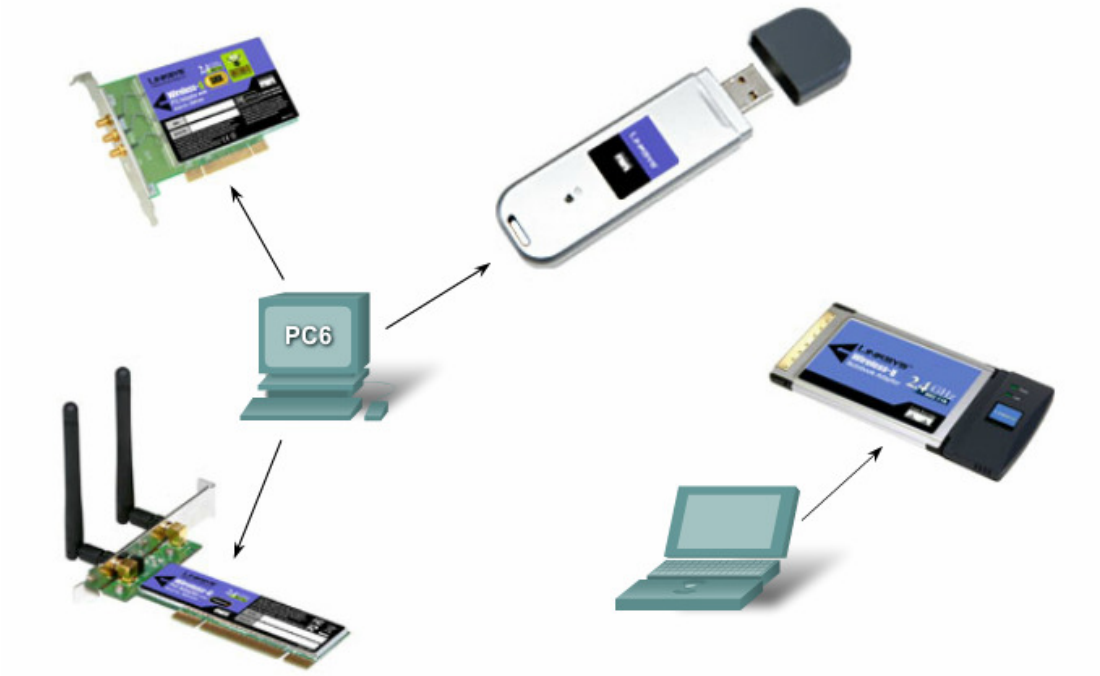
2.6 Δομικά στοιχεία ασύρματων τοπικών δικτύων

Ασύρματη κάρτα δικτύου

Από τα κυριότερα δομικά στοιχεία ενός WLAN είναι οι σταθμοί χρηστών που συνδέονται με τα σημεία πρόσβασης που, με τη σειρά τους, συνδέονται με τη υποδομή του δικτύου. Η συσκευή που καθιστά έναν σταθμό χρήστη ικανό να στέλνει και να λαμβάνει σήματα ραδιοσυχνοτήτων (RF) είναι η ασύρματη κάρτα δικτύου.

Όπως μία κάρτα δικτύου Ethernet, έτσι και η ασύρματη κάρτα δικτύου, χρησιμοποιώντας την τεχνική διαμόρφωσης που έχει επιλεγεί να χρησιμοποιήσει, κωδικοποιεί μία ροή δεδομένων σε ένα σήμα ραδιοσυχνοτήτων (RF). Οι ασύρματες κάρτες δικτύου συχνότερα χρησιμοποιούνται σε κινητές συσκευές, όπως οι φορητοί προσωπικοί υπολογιστές. Στη δεκαετία του '90, οι ασύρματες κάρτες για φορητούς υπολογιστές ήταν κάρτες που τοποθετούνταν στην υποδοχή PCMCIA. Οι PCMCIA ασύρματες κάρτες δικτύου έχουν καταργηθεί με τα χρόνια και οι κατασκευαστές πλέον τοποθετούν τις ασύρματες κάρτες εντός τον φορητών υπολογιστών. Αντίθετα από τις ενσύρματες κάρτες δικτύου που έχουν κάποια διεπαφή σύνδεσης 802.3 Ethernet για να συνδεθεί το καλώδιο, οι ασύρματες κάρτες είναι αόρατες.

Άλλες ανάγκες έχουν προκύψει κατά τη διάρκεια των ετών. Οι υπολογιστές γραφείου που θέλουν να συνδεθούν ασύρματα μπορούν να το κάνουν εύκολα εγκαθιστώντας μία ασύρματη κάρτα δικτύου.
Στις μέρες μας για να συνδεθεί ένας υπολογιστής ασύρματα, φορητός ή υπολογιστής γραφείου, υπάρχουν πολλές επιλογές διαθέσιμες USB ασύρματων καρτών.



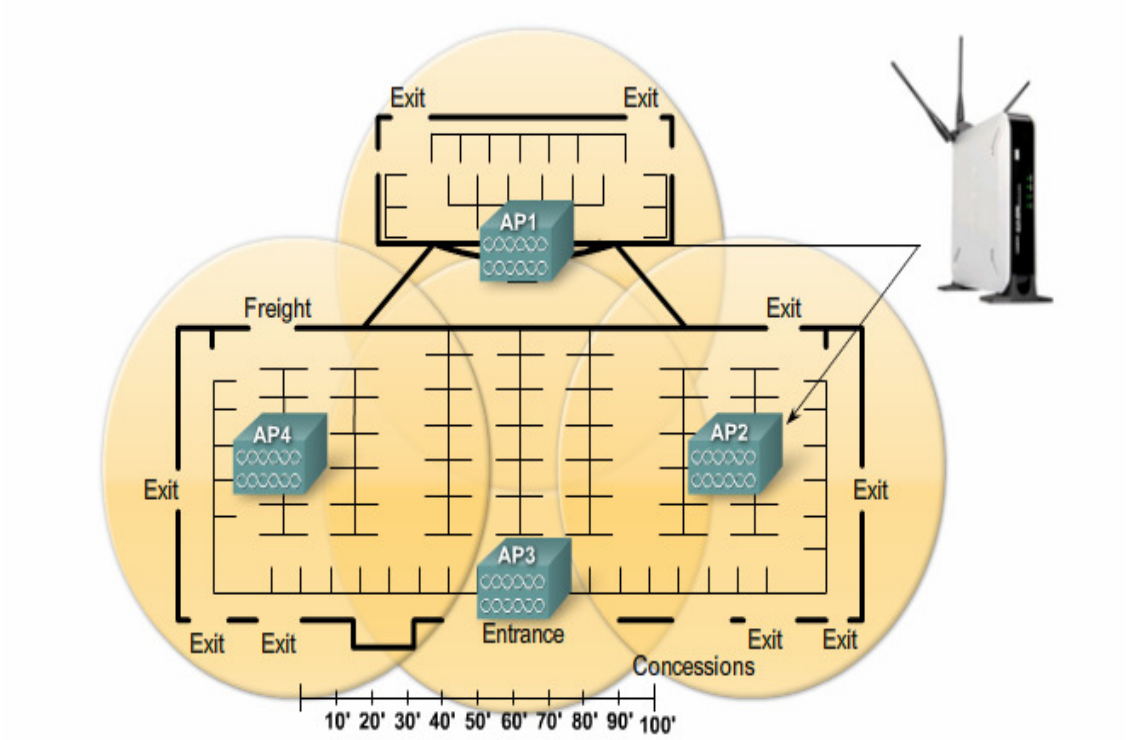
Εικόνα 11. Ασύρματες κάρτες δικτύου.

Ασύρματα σημεία πρόσβασης (Access Points)

Ένα σημείο πρόσβασης συνδέει τους ασύρματους χρήστες (ή σταθμούς) με το ενσύρματο τοπικό δίκτυο. Οι συσκευές των χρηστών δεν επικοινωνούν άμεσα η μια με την άλλη, επικοινωνούν με το access point (AP).
Στην ουσία, ένα σημείο πρόσβασης μετατρέπει τα πακέτα δεδομένων TCP/IP από τη μορφή 802.11 που έχουν τα πλαίσια τους στον αέρα στη μορφή πλαισίων 802.3 Ethernet στο ενσύρματο τοπικό δίκτυο.

Σε ένα δίκτυο υποδομής, οι χρήστες πρέπει να συνδεθούν με ένα σημείο πρόσβασης για να λάβουν τις υπηρεσίες του δικτύου. Η ένωση είναι η διαδικασία με την οποία ένας χρήστης ενώνεται σ ένα δίκτυο 802.11. Είναι παρόμοιο με τη σύνδεση με ένα ενσύρματο τοπικό δίκτυο. Η διαδικασία περιγράφεται αναλυτικότερα στην παρακάτω ενότητα 2.8.

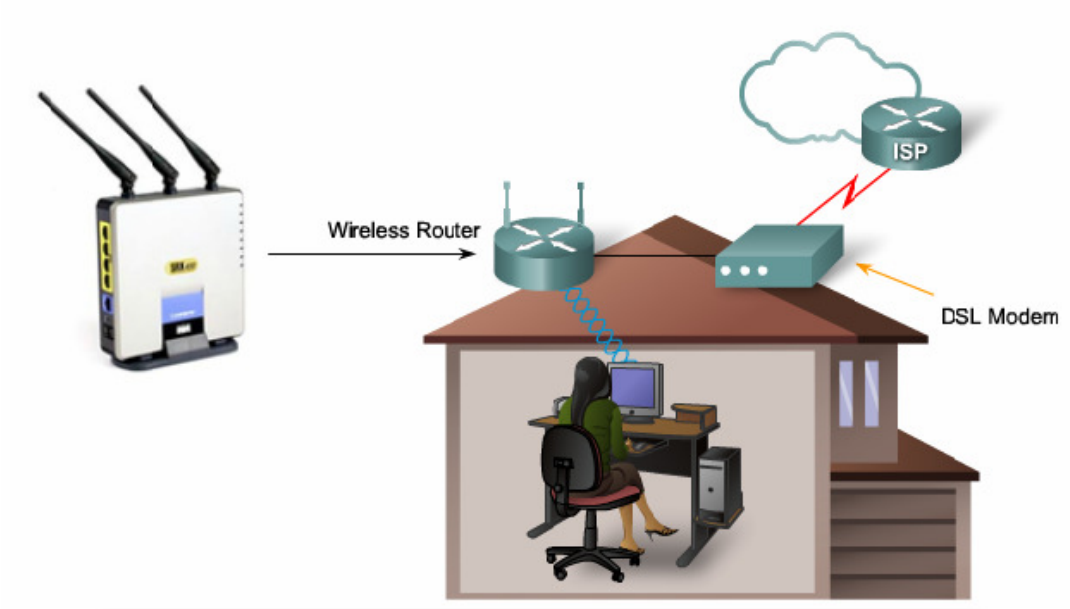
Ένα σημείο πρόσβασης (access point) είναι μία συσκευή " layer 2" που λειτουργεί όπως μια συσκευή hub 802.3 Ethernet. Οι ραδιοσυχνότητες (RF) είναι ένα κοινό μέσο και τα σημεία πρόσβασης ακούνε όλη τη ραδιο κυκλοφορία. Ακριβώς όπως στο 802.3 Ethernet, οι συσκευές που θέλουν να χρησιμοποιήσουν το μέσο το ζητούν. Αντίθετα από τις ενσύρματες κάρτες δικτύου, είναι δαπανηρό να κατασκευαστούν ασύρματες κάρτες δικτύου που να μπορούν να μεταδίδουν και να λαμβάνουν συγχρόνως, ώστε οι ασύρματες συσκευές να μην συγκρούονται κατά την μετάδοση των πακέτων τους.



Εικόνα 12. Ασύρματα σημεία πρόσβασης- Access Points.

Ασύρματοι δρομολογητές (Wireless Routers)

Οι ασύρματοι δρομολογητές εκτελούν το ρόλο του σημείου πρόσβασης, του Ethernet switch, και του δρομολογητή.
Συνήθως οι ασύρματοι δρομολογητές είναι τρεις συσκευές σε μία. Κατ' αρχάς, υπάρχει το ασύρματο σημείο πρόσβασης, το οποίο εκτελεί τις χαρακτηριστικές λειτουργίες ενός σημείου πρόσβασης. Έχει ενσωματωμένες θύρες ethernet για να παρέχει συνδεσιμότητα στις ενσύρματες συσκευές. Τέλος, η λειτουργία του δρομολογητή παρέχει μια πύλη για τη σύνδεση με άλλες υποδομές δικτύου. Για παράδειγμα με ένα φορέα παροχής υπηρεσιών Διαδικτύου (ISP).

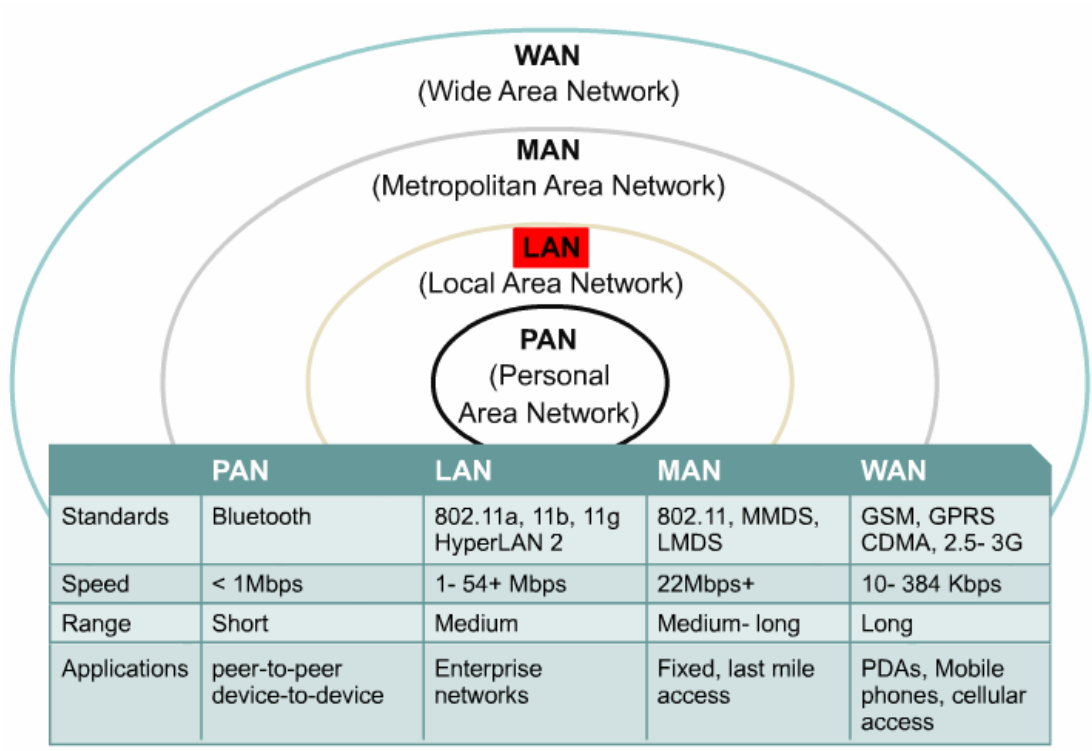


Εικόνα 13. Ασύρματοι δρομολογητές -Wireless Routers.

Ατμόσφαιρα: το μέσο για την ασύρματη τεχνολογία

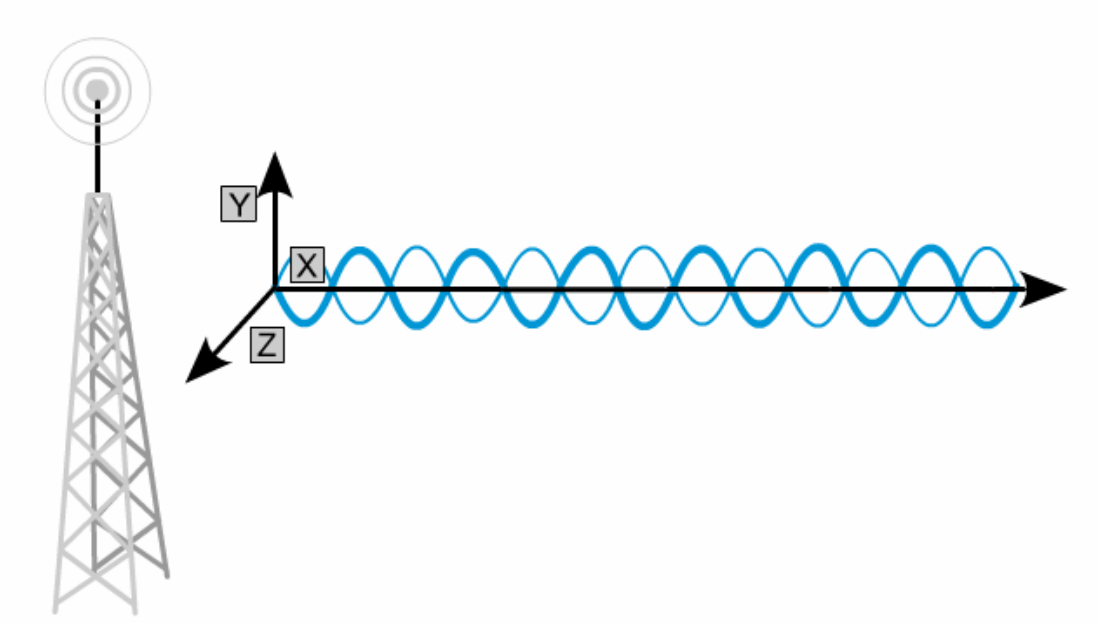
Τα ασύρματα σήματα είναι ηλεκτρομαγνητικά κύματα, τα οποία μπορούν να ταξιδέψουν μέσω της ατμόσφαιρας. Κανένα φυσικό μέσο δεν είναι απαραίτητο για τα ασύρματα σήματα, τα οποία ταξιδεύουν τόσο στο κενό του διαστήματος όσο και μέσω του αέρα σε ένα κτίριο γραφείων. Η δυνατότητα των ράδιο κυμάτων να περνούν μέσω των τοίχων και να καλύπτουν μεγάλες αποστάσεις καθιστά τα ασύρματα δίκτυα ευπροσάρμοστα στην κατασκευή ενός δικτύου. Το πρότυπο IEEE 802.11 ορίζει 13 κανάλια στη συχνότητα των 2.4GHz προκειμένου να αυξήσει την ακεραιότητα των δεδομένων και να μειώσει τις παρεμβολές.

Η εικόνα 14 παρουσιάζει τις ασύρματες τεχνολογίες και χαρακτηριστικά τους γνωρίσματα. Η εικόνα 15 αναπαριστά ένα ηλεκτρομαγνητικό κύμα.



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HyperLAN 2	802.11, MMDS, LMDS	GSM, GPRS CDMA, 2.5- 3G
Speed	< 1Mbps	1- 54+ Mbps	22Mbps+	10- 384 Kbps
Range	Short	Medium	Medium- long	Long
Applications	peer-to-peer device-to-device	Enterprise networks	Fixed, last mile access	PDAs, Mobile phones, cellular access

Εικόνα 14. Οι ασύρματες τεχνολογίες και χαρακτηριστικά τους.



Εικόνα 15. Το ηλεκτρομαγνητικό κύμα.

Κεραίες

Ποικίλες επιλογές 2.4 Ghz και 5 Ghz κεραιών είναι διαθέσιμες για τις ασύρματες συσκευές των δικτύων. Οι κεραίες πρέπει να επιλεχτούν προσεκτικά για να εξασφαλίσουν τη βέλτιστη ακτίνα δράσης και κάλυψη.

Κάθε κεραία έχει διαφορετικές ικανότητες κέρδους , πλάτους ακτίνας, κάλυψης και τύπου κατασκευής. Υπάρχουν δύο είδη κεραιών ανάλογα με τον τρόπο που εκπέμπουν, οι πολυκατευθυντικές (omnidirectonal) και οι κατευθυντικές (directional). Οι πολυκατευθυντικές κεραίες εκπέμπουν προς όλες τις κατευθύνσεις με μεγάλο εύρος δέσμης και γι αυτό προτιμώνται σε συνδέσεις μικρών αποστάσεων. Στις κατευθυντικές κεραίες η ακτινοβολία τους είναι ενισχυμένη έντονα προς μία κατεύθυνση και γι αυτό προτιμώνται σε συνδέσεις μεγάλων αποστάσεων.
Η ένωση της σωστής κεραίας με το σωστό access point (AP) επιτρέπει αποδοτικότερη κάλυψη σε κάθε περίσταση, καθώς επίσης και καλύτερη αξιοπιστία στους υψηλούς ρυθμούς δεδομένων.

Εικόνα 16. Διάφορα είδη κεραιών.

Συσκευές χρηστών

Οι ασύρματες συσκευές για τα τοπικά δίκτυα έχουν αυξηθεί παρά πολύ. Οι παραδοσιακές ενσύρματες συσκευές όπως οι σταθεροί υπολογιστές, τα τηλέφωνα IP και οι εκτυπωτές έχουν ενσωματώσει ασύρματες επιλογές. Σήμερα, οι διαθέσιμες ασύρματες συσκευές περιλαμβάνουν

- PDAs
- Τηλέφωνα IP

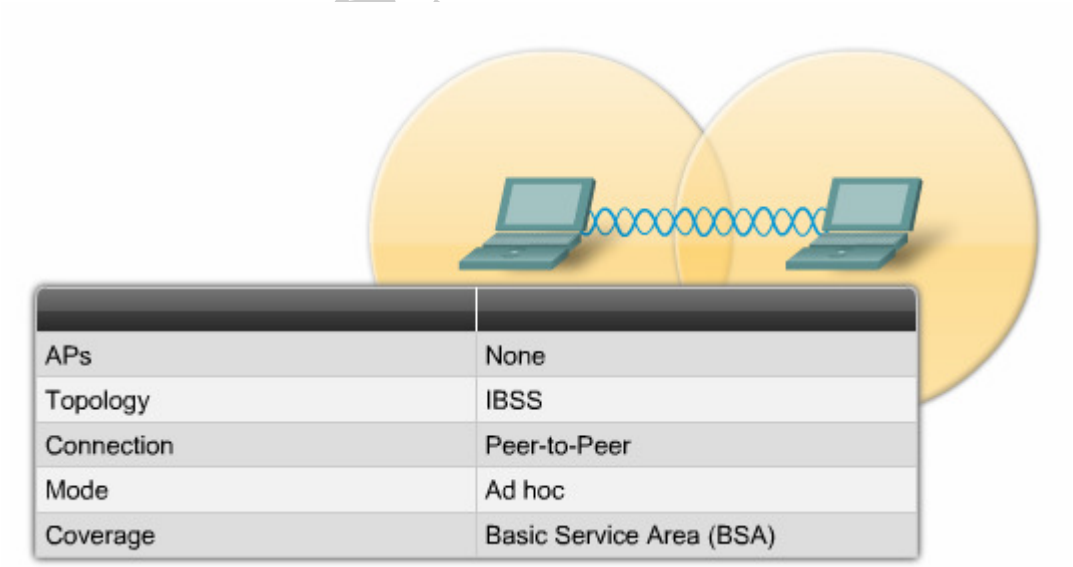
- Εκτυπωτές
- Προτζέκτορες
- Tablet PCs
- Κάμερες ασφαλείας
- Ανιχνευτές Barcode
- Ειδικές συσκευές για τις αγορές:
  - ❖ Υγειονομικής περίθαλψης
  - ❖ Κατασκευών
  - ❖ Λιανικό Εμπόριο
  - ❖ Εστιατόρια

2.7 Οι τοπολογίες του IEEE 802.11

Τα ασύρματα τοπικά δίκτυα μπορούν να φιλοξενήσουν διάφορες τοπολογίες δικτύων. Όταν περιγράφουμε αυτές τις τοπολογίες, θεμελιώδης δομική μονάδα της αρχιτεκτονικής IEEE 802.11 , είναι το Basic Service Set (BSS). Τα πρότυπα καθορίζουν ένα BSS ως μία ομάδα σταθμών που επικοινωνούν ο ένας με τον άλλον.

Δίκτυα Ad Hoc

Το ασύρματο δίκτυο που μπορεί να λειτουργήσει χωρίς κανένα σημείο πρόσβασης καλείται τοπολογία Ad hoc.
Οι συσκευές των χρηστών που διαμορφώνονται για να λειτουργήσουν σε τοπολογία Ad hoc καθορίζουν τις ασύρματες παραμέτρους μεταξύ τους. Το πρότυπο IEEE 802.11 αναφέρει την ad hoc τοπολογία ως Independent BSS (IBSS), ως δηλαδή μια ανεξάρτητη ομάδα σταθμών που μπορούν να επικοινωνήσουν μεταξύ τους.

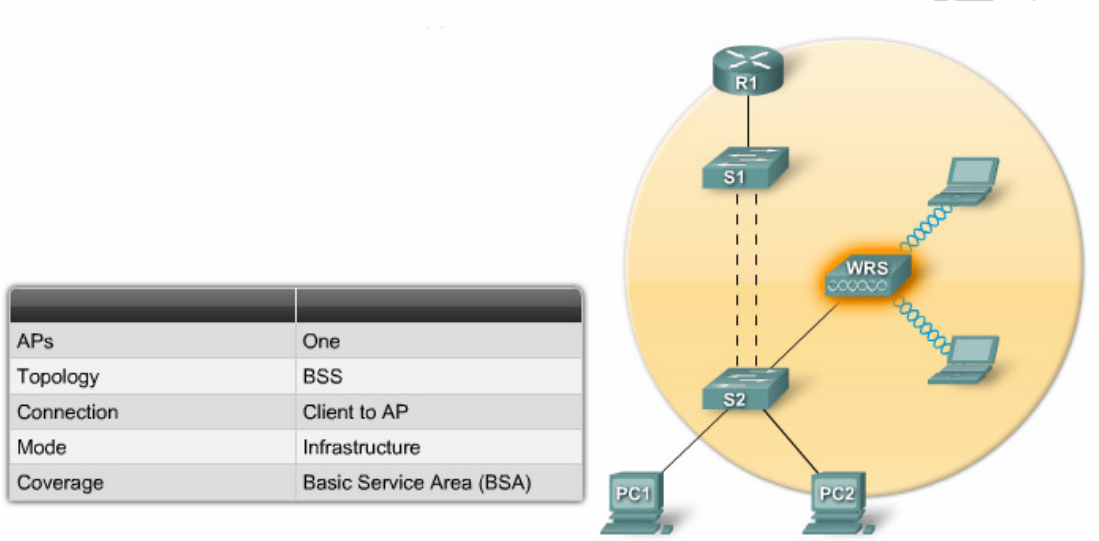


APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

Εικόνα 17. Το δίκτυο Ad-Hoc.

Basic Service Sets

Ένα μόνο σημείο πρόσβασης υπάρχει στην υποδομή αυτού του δικτύου το οποίο διαχειρίζεται τις ασύρματες παραμέτρους. Τα σημεία πρόσβασης παρέχουν μια υποδομή που προσθέτει υπηρεσίες και βελτιώνουν την ακτίνα κάλυψης των χρηστών. Η περιοχή κάλυψης ενός IBSS και BSS ονομάζεται *βασική περιοχή υπηρεσίας* (Basic Service Area,BSA).

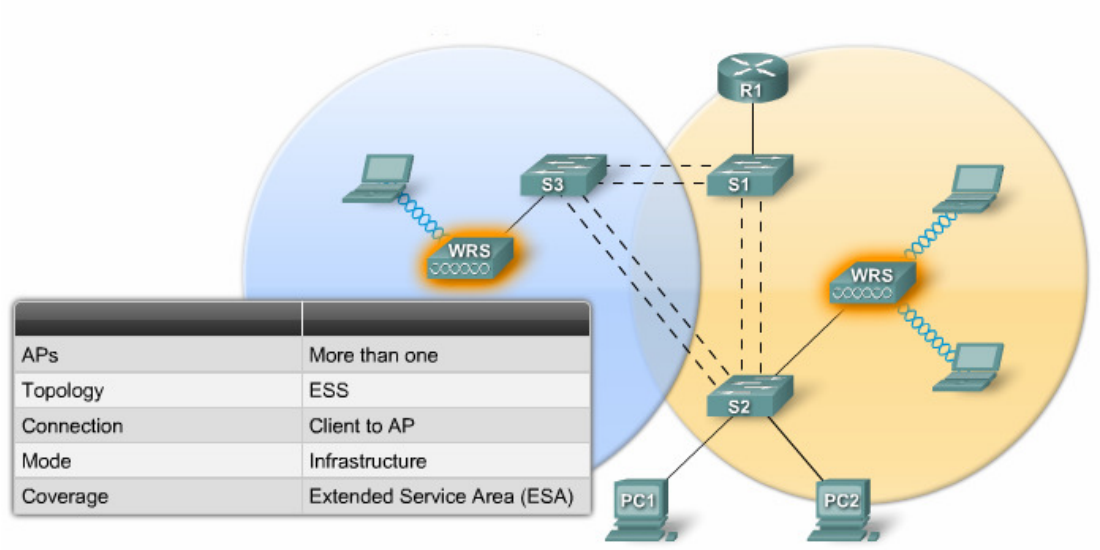


APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)

Εικόνα 18. Basic Service Area (BSA).

Extended Service Sets

Όταν ένα BSS δεν παρέχει επαρκή κάλυψη για όλους του επιθυμητούς σταθμούς των χρηστών ,τότε ένα ή περισσότερα BSS μπορούν να ενωθούν με την προσθήκη επιπλέον σημείων πρόσβασης μέσω ενός κοινού συστήματος διανομής δημιουργώντας έτσι ένα extended service set (ESS). Σε ένα ESS, ένα BSS διαφοροποιείται από τα άλλα με ένα προσδιοριστικό, το BSSID, το οποίο είναι η διεύθυνση MAC του σημείου πρόσβασης που εξυπηρετεί το BSS. Η περιοχή κάλυψης σε ένα ESS ονομάζεται *εκτεταμένη περιοχή υπηρεσίας* extended service area (ESA).



Εικόνα 19. Extended Service Set (ESS).

Το σύνηθες σύστημα διανομής

Στο κοινό σύστημα διανομής συνήθως πολλά σημεία πρόσβασης υπάρχουν σε ένα ESS αλλά μοιάζει να φαίνεται σαν ένα απλό BSS. Ένα ESS περιλαμβάνει ένα κοινό SSID και επιτρέπει σε έναν χρήστη να μετακινείται από σημείο πρόσβασης σε σημείο πρόσβασης.

Οι κυψέλες αντιπροσωπεύουν την περιοχή κάλυψης που παρέχεται από ένα κανάλι. Ένα ESS πρέπει να έχει επικάλυψη 10 έως 15 τοις εκατό μεταξύ των κυψελών του σε μια εκτεταμένη περιοχή υπηρεσίας (ESA). Με μια επικάλυψη 15 τοις εκατό μεταξύ των κυψελών, ένα κοινό SSID και με μη επικαλυπτόμενα κανάλια (μία κυψέλη στο κανάλι 1 και άλλη στο κανάλι 6), η ικανότητα περιαγωγής επιτυγχάνεται.

Wireless Devices	Topology Mode	Topology Building Block	Coverage Area
No access points	Ad Hoc	Independent Basic Service Set (IBSS	Basic Service Area (BSA)
One access point	Infrastructure	Basic Service Set (BSS)	Basic Service Area (BSA)
More than one access point	Infrastructure	Extended Service Set (ESS)	Extended Service Area (ESA)

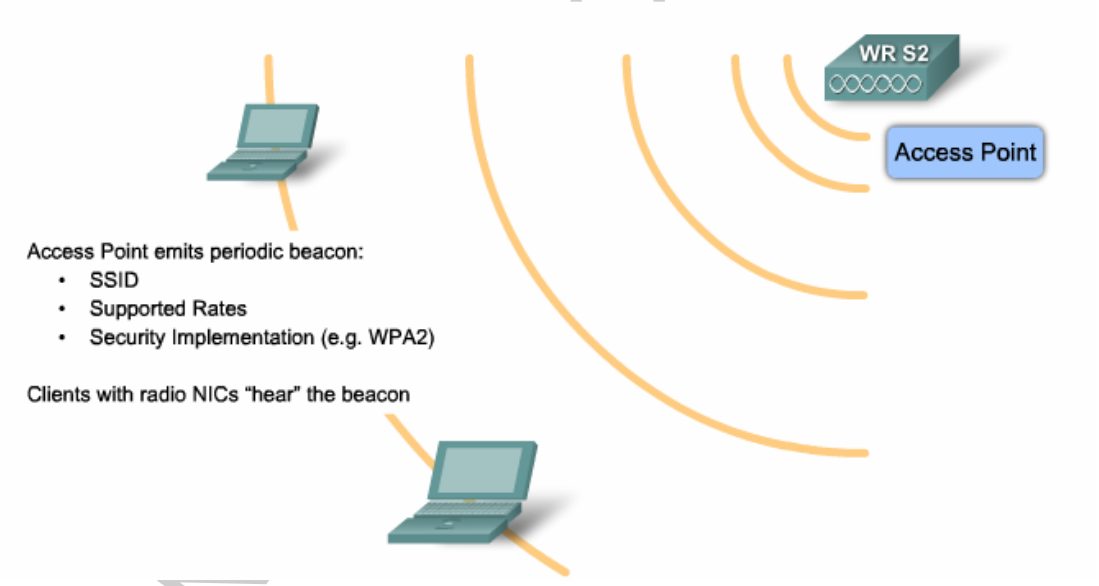
Πίνακας 2. Σύγκριση των τοπολογιών των WLAN.

2.8 Η ασύρματη λειτουργία

Ένα σημαντικό κομμάτι της διαδικασίας 802.11 είναι η ανακάλυψη ενός WLAN και η σύνδεση του με αυτό. Τα κυρία συστατικά αυτής της διαδικασίας είναι τα ακόλουθα:

- Αναγνωριστικά σήματα (Beacons) - πλαίσια που χρησιμοποιούνται από το ασύρματο δίκτυο για να διαφημίσει την παρουσία του.
- Probes - πλαίσια που χρησιμοποιούνται από τους WLAN χρήστες για να βρουν δίκτυα.
- Επικύρωση (Authentication) - μια διαδικασία στην οποία γίνεται επαλήθευση της ταυτότητας των χρηστών
- Ένωση (Association) - η διαδικασία για την δημιουργία σύνδεσης μεταξύ ενός σημείου πρόσβασης και ενός χρήστη WLAN.

Ο αρχικός σκοπός του αναγνωριστικού σήματος (beacon) είναι να επιτραπεί στους χρήστες των ασυρμάτων δικτύων να μάθουν ποια δίκτυα και ποια σημεία πρόσβασης είναι διαθέσιμα στην συγκεκριμένη περιοχή , ώστε να επιλέξουν ποιο δίκτυο και ποιο σημείο πρόσβασης θέλουν να χρησιμοποιήσουν. Τα σημεία πρόσβασης μπορούν να μεταδίδουν τα αναγνωριστικά σήματα (beacons) περιοδικά.



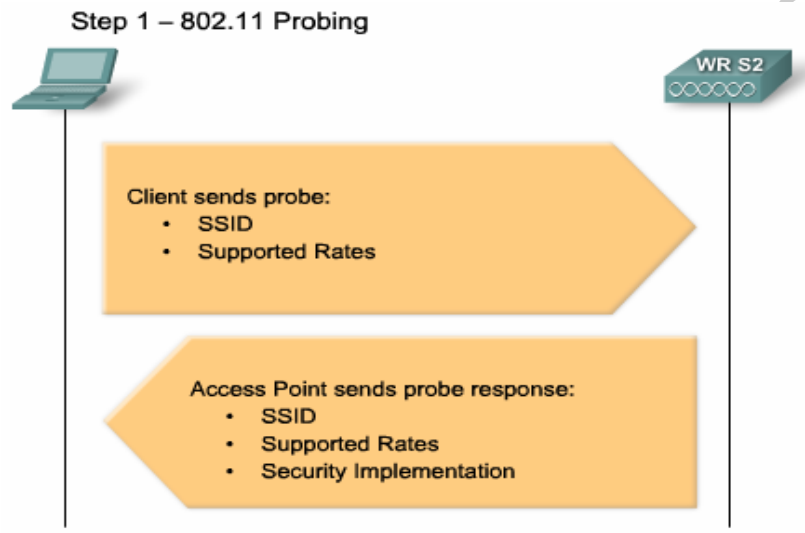
Εικόνα 20. Η μετάδοση των Beacons.

Προτού να μπορέσει να στείλει ένας χρήστης δεδομένα σ ένα ασύρματο δίκτυο, περνά από την ακόλουθη διαδικασία τριών σταδίων:

Στάδιο 1 - 802.11 probing

Οι χρήστες ψάχνουν για ένα συγκεκριμένο δίκτυο στέλνοντας ένα αίτημα probe. Το αίτημα probe διευκρινίζει το όνομα του δικτύου (SSID) και τον ρυθμό των bits. Όταν ένας χρήστης WLAN έχει προεπιλεγμένο ένα επιθυμητό συγκεκριμένο SSID, τα αιτήματα probe από τον χρήστη περιέχουν το SSID του επιθυμητού ασύρματου δικτύου.

Εάν ο χρήστης προσπαθεί απλά να ανακαλύψει τα διαθέσιμα ασύρματα δίκτυα, μπορεί να στείλει ένα αίτημα probe χωρίς SSID και όλα τα σημεία πρόσβασης (access points) να αποκριθούν. Το σημεία πρόσβασης που έχουν απενεργοποιήσει την επιλογή να διαφημίζουν σε όλους το όνομα τους (SSID) δεν θα αποκριθούν.



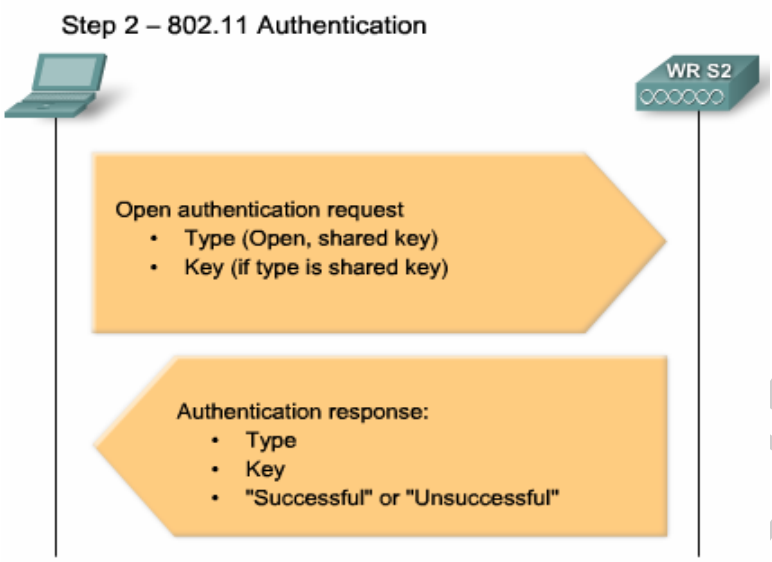
Εικόνα 21. Probing

Στάδιο 2 - 802.11 authentication

Το πρότυπο 802.11 αναπτύχθηκε αρχικά με δύο μηχανισμούς επικύρωσης. Ο πρώτος, αποκαλούμενος μηχανισμός ανοιχτής επικύρωσης (open authentication), είναι μια ΜΗΔΕΝΙΚΗ επικύρωση όπου ο πελάτης λέει «επικύρωσε με», και το σημείο πρόσβασης αποκρίνεται με «ναι.» Αυτός ο μηχανισμός χρησιμοποιείται σχεδόν σε όλες τις 802.11 διαμορφώσεις.

Ένας δεύτερος μηχανισμός επικύρωσης αναφέρεται ως επικύρωση διαμοιρασμένου κλειδιού. Αυτή η τεχνική είναι βασισμένη σε ένα κλειδί προστασίας Wired Equivalency Protection (WEP) που μοιράζεται μεταξύ του χρήστη και του σημείου πρόσβασης. Σε αυτήν την τεχνική, ο χρήστης στέλνει ένα αίτημα επικύρωσης (authentication) στο σημείο πρόσβασης. Το σημείο πρόσβασης στέλνει έπειτα ένα κείμενο στον χρήστη, που κρυπτογραφεί το μήνυμα χρησιμοποιώντας το κοινό κλειδί του, και επιστρέφει το κρυπτογραφημένο κείμενο πίσω στο σημείο πρόσβασης.
Το σημείο πρόσβασης αποκρυπτογραφεί έπειτα το κρυπτογραφημένο κείμενο χρησιμοποιώντας το κλειδί του και εάν το αποκρυπτογραφημένο κείμενο ταιριάζει με το αρχικό κείμενο , ο χρήστης και το σημείου πρόσβασης έχουν το ίδιο κλειδί

κρυπτογράφησης και το σημείο πρόσβασης επικυρώνει το χρήστη/σταθμό. Εάν τα μηνύματα δεν ταιριάζουν, ο χρήστης δεν επικυρώνεται.

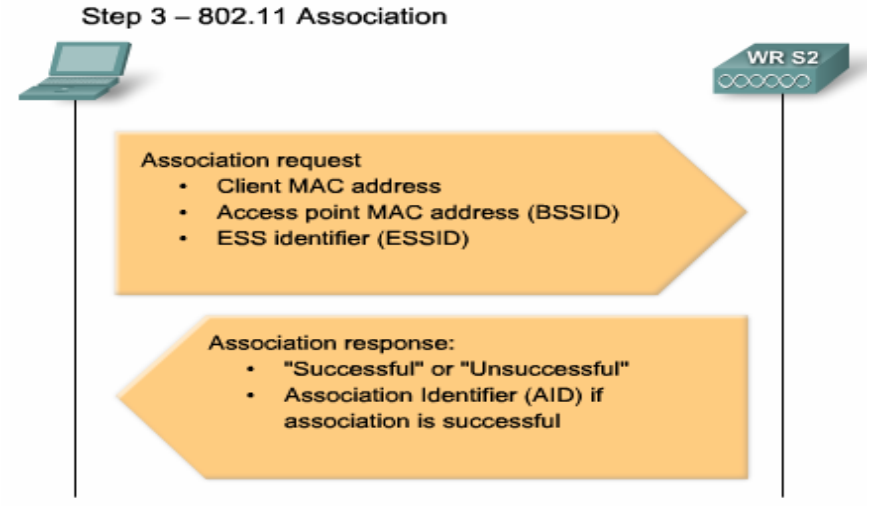


Εικόνα 22. Authentication.

Στάδιο 3 - 802.11 association

Αυτό το στάδιο οριστικοποιεί τις επιλογές ασφάλειας και του ρυθμού των δεδομένων και καθιερώνει την σύνδεση μεταξύ του WLAN χρήστη και του σημείου πρόσβασης. Ως τμήμα αυτού του σταδίου, ο χρήστης μαθαίνει το BSSID, το οποίο είναι η διεύθυνση MAC του σημείου πρόσβασης και το σημείο πρόσβασης προσδίδει μία "λογική" πόρτα γνωστή ως προσδιοριστικό ένωσης (association identifier, AID) στον χρήστη. Είναι κάτι αντίστοιχο με την φυσική πόρτα ενός switch.

Μόλις ένας ασύρματος χρήστης έχει συνδεθεί με ένα σημείο πρόσβασης, η κυκλοφορία είναι πλέον ικανή να ταξιδέψει μεταξύ των δύο συσκευών.



Εικόνα 23. Association.

ΚΕΦΑΛΑΙΟ 3

Ασφάλεια στα ασύρματα τοπικά δίκτυα

3.1 Τι είναι ασφάλεια ?

Ο κύριος σκοπός της ασφάλειας είναι να κρατηθούν οι εισβολείς έξω από ένα κλειστό σύστημα. Στην ιστορία, αυτό σήμαινε ισχυρούς τοίχους και μικρές, καλά φρουρημένες πόρτες για να μπορούν να ελέγχουν την πρόσβαση. Μόνο όσοι είχαν άδεια μπορούσαν να εισέρχονται.
Αυτή η στρατηγική λειτουργεί καλύτερα στα ενσύρματα τοπικά δίκτυα σε σχέση με τα ασύρματα. Η άνοδος του κινητού εμπορίου και των ασύρματων δικτύων κάνουν το παλαιό πρότυπο ακατάλληλο. Νέες λύσεις ασφάλειας απαιτούνται περισσότερο ευέλικτες και εύχρηστες.

Η ασφάλεια εξασφαλίζει ότι οι χρήστες μπορούν να εκτελέσουν μόνο τις λειτουργίες και μπορούν να λάβουν μόνο τις πληροφορίες για τις οποίες είναι εξουσιοδοτημένοι. Η ασφάλεια πρέπει να εξασφαλίζει ότι οι χρήστες δεν μπορούν να προκαλέσουν ζημία στα δεδομένα, στις εφαρμογές, ή το λειτουργικό περιβάλλον ενός συστήματος. Η λέξη ασφάλεια περιλαμβάνει την προστασία ενάντια στις κακόβουλες επιθέσεις. Η ασφάλεια περιλαμβάνει επίσης τον έλεγχο των αποτελεσμάτων των λαθών και των αποτυχιών του εξοπλισμού. Οτιδήποτε μπορεί να προστατεύσει από μια ασύρματη επίθεση θα αποτρέψει επίσης πιθανώς άλλους τύπους προβλημάτων.

3.2 Απειλές στην ασύρματη ασφάλεια.

Η ασφάλεια πρέπει να είναι προτεραιότητα για τον καθένα που χρησιμοποιεί ή διαχειρίζεται τα δίκτυα. Πόσο μάλλον για ένα ασύρματο δίκτυο όπου οι δυσκολίες στην διατήρηση της ασφάλειας πολλαπλασιάζονται σε σχέση με το ενσύρματο. Ένα WLAN είναι ανοικτό στον καθένα εντός της ακτίνας εκπομπής του σημείου πρόσβασης του. Με μία ασύρματη κάρτα δικτύου και την γνώση τεχνικών παραβίασης, ένας επιτιθέμενος μπορεί να πραγματοποιήσει μια επίθεση. Πολλές φορές μάλιστα δεν χρειάζεται να βρίσκεται φυσικά στον χώρο όπου επιχειρείται η επίθεση αφού μπορεί να βρίσκεται εκτός του κτιρίου εντός όμως της ακτινας κάλυψης του WLAN.

Αυτά τα προβλήματα ασφαλείας είναι ακόμα σημαντικότερα όταν έχουν να κάνουν με επιχειρησιακά δίκτυα, αφού οι οικονομικοί πόροι της επιχείρησης στηρίζονται στην προστασία των πληροφοριών της. Οι παραβιάσεις της ασφαλείας για μια επιχείρηση μπορούν να έχουν σημαντικό αντίκτυπο, ειδικά εάν η επιχείρηση διατηρεί οικονομικές πληροφορίες των πελατών της.

3.2.1 Μη εξουσιοδοτημένη πρόσβαση

Υπάρχουν τρεις σημαντικές κατηγορίες απειλών που οδηγούν στην μη εξουσιοδοτημένη πρόσβαση:

- War drivers
- Χάκερς (Crackers)
- Υπάλληλοι

Το «war driving» αρχικά αναφερόταν στη χρησιμοποίηση μιας συσκευής ανίχνευσης αριθμών κινητών τηλεφώνων για να εκμεταλλευτεί. Το war driving τώρα σημαίνει την περιπλάνηση γύρω από μια γειτονιά με ένα lap-top και μια ασύρματη κάρτα 802.11b/g ψάχνοντας ένα ακάλυπτο σύστημα 802.11b/g που στην πορεία θα εκμεταλλευτεί.

Ο όρος χάκερ σήμαινε αρχικά κάποιον που ερευνά βαθειά τους ηλεκτρονικούς υπολογιστές για να καταλάβει και ίσως να εκμεταλλευθεί για δημιουργικούς λόγους, τη δομή και την πολυπλοκότητα ενός συστήματος. Σήμερα, ο όρος χάκερ και (cracker) σημαίνουν τους κακόβουλους εισβολείς που εισέρχονται στα συστήματα ως εγκληματίες και κλέβουν στοιχεία ή σκόπιμα προκαλούν ζημιά στα συστήματα. Οι χάκερ που θέλουν να κάνουν ζημιά είναι σε θέση να εκμεταλλευτούν τα αδύνατα μέτρα ασφάλειας.

Οι περισσότερες ασύρματες συσκευές που πωλούνται σήμερα είναι σχεδόν έτοιμες για χρήση WLAN. Με άλλα λόγια, οι συσκευές έχουν προεπιλεγμένες ρυθμίσεις και μπορούν να εγκατασταθούν και να χρησιμοποιηθούν με ελάχιστη ή καμία διαμόρφωση από τους χρήστες. Συχνά, οι χρήστες δεν αλλάζουν τις προεπιλεγμένες ρυθμίσεις, αφήνοντας την επικύρωση χρηστών ανοικτή (open authentication), ή εφαρμόζουν την τυποποιημένη ασφάλεια WEP. Δυστυχώς, τα κοινά κλειδιά WEP είναι εύκολο να επιτεθούν.

Τα εργαλεία με νόμιμο σκοπό, όπως τα ασύρματα sniffers, επιτρέπουν στους μηχανικούς δικτύων να συλλάβουν πακέτα δεδομένων για τη διόρθωση των συστημάτων(debugging). Αυτά τα ίδια εργαλεία μπορούν να χρησιμοποιηθούν από τους εισβολείς για να εκμεταλλευτούν τις αδυναμίες ασφαλείας.

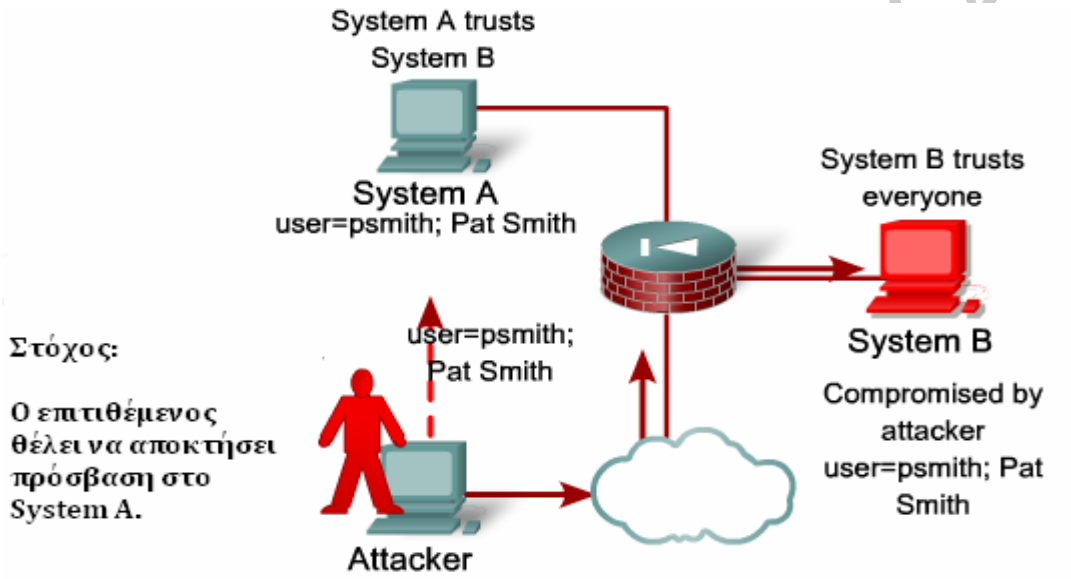
"War Drivers"	Hackers	Employees
Find "Open" networks; use them to gain free Internet access	Exploit weak privacy measures to view sensitive WLAN information and even break into WLANs	Plug consumer-grade APs/gateways into company Ethernet ports to create their own WLANs

Πίνακας 3. Μη εξουσιοδοτημένη πρόσβαση.

Μια άλλη επίθεση μη εξουσιοδοτημένης πρόσβασης ονομάζεται επίθεση trust exploitation . Ο στόχος μιας επίθεσης trust exploitation είναι να χρησιμοποιηθεί ένας χρήστης με εξουσιοδότηση ώστε να στηθούν επιθέσεις σε άλλους hosts σε ένα δίκτυο. Εάν ένας host σε ένα δίκτυο μιας επιχείρησης προστατεύεται από ένα firewall (εσωτερικός host), αλλά είναι προσιτός σε έναν host που «εμπιστεύεται» έξω από το

firewall (εξωτερικός host), ο εσωτερικός host μπορεί δεχθεί επίθεση μέσω του «έμπιστου» εξωτερικού host.

Για παράδειγμα στην εικόνα 24 ο επιτιθέμενος στο κάτω μέρος της εικόνας έχει πρόσβαση στον εξωτερικό host, System B και όχι στον εσωτερικό host, System A. Μόλις ο επιτιθέμενος κερδίσει πρόσβαση στο System B που το System A εμπιστεύεται, μπορεί να τον χρησιμοποιήσει ώστε να αποκτήσει πρόσβαση στον εσωτερικό host, System A.



Εικόνα 24. Επίθεση Trust Exploitation.

Οι επιθέσεις trust exploitation μπορούν να μετριαστούν μέσω των σφιχτών περιορισμών στα επίπεδα εμπιστοσύνης μέσα σε ένα δίκτυο. Παραδείγματος χάριν, ιδιωτικά VLANs (PVLANs) μπορούν να υλοποιηθούν στα τμήματα όπου πολλοί δημόσιοι κεντρικοί υπολογιστές (servers) είναι διαθέσιμοι. Τα συστήματα έξω από το firewall δεν πρέπει ποτέ να είναι απολύτως εμπιστευμένα από τα συστήματα στη εσωτερική ζώνη του firewall. Η εμπιστοσύνη πρέπει να περιοριστεί σε συγκεκριμένα πρωτόκολλα και πρέπει να γίνεται authentication με κάτι άλλο εκτός από μια διεύθυνση IP, όπου είναι δυνατόν.

3.2.2 Κακόβουλα σημεία πρόσβασης (Rogue Access Points)

Ένα κακόβουλο σημείο πρόσβασης είναι ένα σημείο πρόσβασης που τοποθετείται σε ένα WLAN και χρησιμοποιείται για να παρεμποδίσει την κανονική του λειτουργία. Εάν το κακόβουλο σημείο πρόσβασης έχει παραμετροποιηθεί με τις σωστές ρυθμίσεις ασφάλειας, τα δεδομένα των χρηστών μπορούν να υποκλαπούν. Ένα κακόβουλο σημείο πρόσβασης θα μπορούσε επίσης να διαμορφωθεί ώστε να παρέχει στους μη εξουσιοδοτημένους χρήστες πληροφορίες όπως τις MAC διευθύνσεις των χρηστών (ασύρματων και ενσύρματων),ή να συλλέξει και να μεταλλάξει πακέτα δεδομένων ή, στη χειρότερη περίπτωση, να αποκτήσει πρόσβαση στους κεντρικούς υπολογιστές (servers) και τα αρχεία.

Ένα συνηθισμένο τέτοιο παράδειγμα είναι ένα σημείο πρόσβασης που εγκαθίσταται από τους υπαλλήλους μία εταιρίας χωρίς έγκριση. Οι υπάλληλοι εγκαθιστούν σημεία πρόσβασης που προορίζονται για οικιακή χρήση στα δίκτυα επιχειρήσεων. Αυτά τα σημεία πρόσβασης δεν έχουν την απαραίτητη διαμόρφωση ασφαλείας, έτσι δημιουργείται στο δίκτυο μια τρύπα ασφαλείας.

3.2.3 Επιθέσεις Man-in-the-Middle

Μια από τις περιπλοκότερες επιθέσεις που ένας μη εξουσιοδοτημένος χρήστης μπορεί να κάνει καλείται επίθεση Man-in-the-Middle (MITM). Οι επιτιθέμενοι επιλέγουν έναν χρήστη του δικτύου ως στόχο και τοποθετούνται "λογικά" μεταξύ του στόχου και του δρομολογητή ή της gateway του στόχου. Σε ένα ενσύρματο περιβάλλον τοπικού δικτύου, ο επιτιθέμενος πρέπει να είναι σε θέση να έχει φυσική πρόσβαση για να παρεμβάλει μια συσκευή στην τοπολογία. Σε ένα WLAN, τα ραδιοκύματα που εκπέμπονται από τα σημεία πρόσβασης δίνουν την ευκαιρία για αυτήν την ενδιάμεση παρεμβολή.

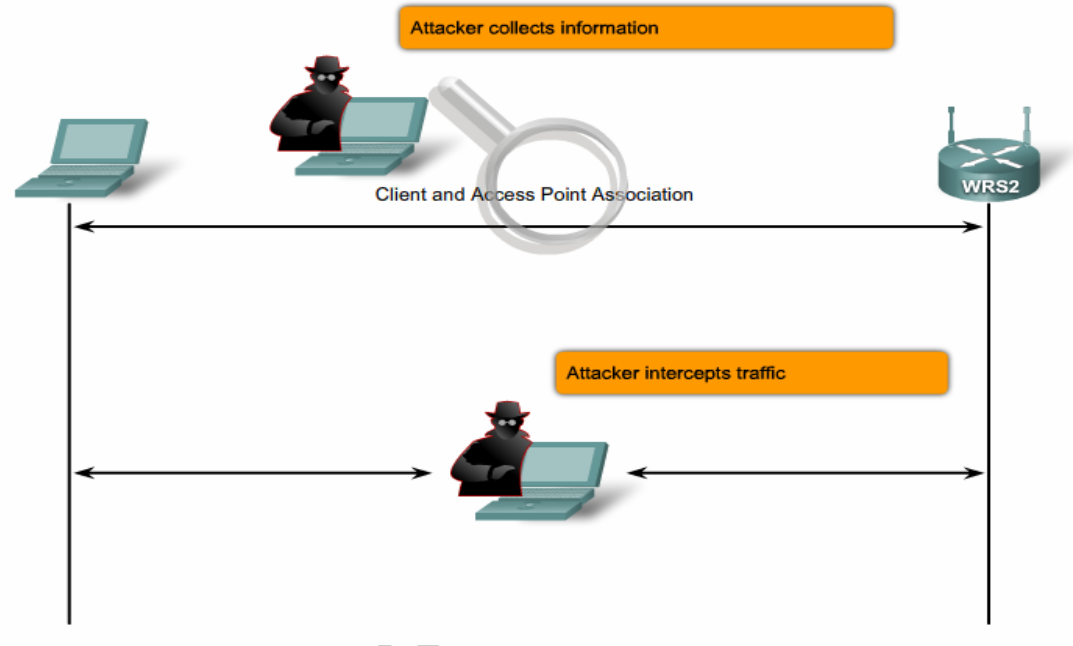
Τα ραδιοσήματα από τους σταθμούς και τα σημεία πρόσβασης μπορούν να ληφθούν από τον καθένα σε ένα BSS με τον κατάλληλο εξοπλισμό, όπως ένα laptop με μία ασύρματη κάρτα δικτύου.
Επειδή τα σημεία πρόσβασης ενεργούν όπως τα Ethernet hubs, κάθε κάρτα δικτύου σε ένα BSS "ακούει" όλη την κυκλοφορία. Η συσκευή απορρίπτει την κυκλοφορία που δεν απευθύνεται σε αυτήν. Οι επιτιθέμενοι μπορούν να τροποποιήσουν την ασύρματη κάρτα δικτύου του laptop τους με ειδικό λογισμικό έτσι ώστε να δέχεται όλη την κυκλοφορία. Με αυτήν την τροποποίηση, ο επιτιθέμενος μπορεί να πραγματοποιήσει τις ασύρματες επιθέσεις MITM, χρησιμοποιώντας την κάρτα δικτύου του laptop του που θα λειτουργεί ως σημείο πρόσβασης.

Για να πραγματοποιήσει αυτήν την επίθεση, ένας χάκερ επιλέγει έναν σταθμό ως στόχο και χρησιμοποιεί λογισμικό packet sniffing, όπως το Wireshark, για να παρατηρήσει την σύνδεση του σταθμού του χρήστη με ένα σημείο πρόσβασης. Ο χάκερ μπορεί να είναι σε θέση να διαβάσει και να αντιγράψει το όνομα χρήστη του στόχου, το όνομα των κεντρικών υπολογιστών, τη διεύθυνση IP του κεντρικού υπολογιστή (server) και του χρήστη , την ταυτότητα AID που χρησιμοποιήθηκε για να γίνει η σύνδεση με το σημείο πρόσβασης κατά το στάδιο της ένωσης (association) και της απάντησης η οποία περνάει σε μη κρυπτογραφημένο κείμενο μεταξύ του σταθμού και του σημείου πρόσβασης.

Εάν ένας επιτιθέμενος είναι σε θέση να επηρεάσει ένα σημείο πρόσβασης, ο επιτιθέμενος μπορεί ενδεχομένως να επηρεάσει όλους τους χρήστες στο BSS. Ο επιτιθέμενος μπορεί να ελέγξει ένα ολόκληρο ασύρματο δίκτυο και να καταστρέψει οποιονδήποτε χρήστη είναι συνδεδεμένος με αυτό.

Για να αντιμετωπιστεί μια επίθεση όπως είναι η επίθεση MITM, σημαντικό ρόλο παίζουν το πόσο "έξυπνη" είναι η υποδομή του ασύρματου τοπικού δικτύου και η συνεχής επαγρύπνησή στη διαδικασία ελέγχου του δικτύου. Η διαδικασία αρχίζει με τον προσδιορισμό των νόμιμων συσκευών στο ασύρματο δίκτυο. Για να γίνει αυτό, πρέπει να επικυρωθούν (authentication) οι χρήστες του δικτύου.

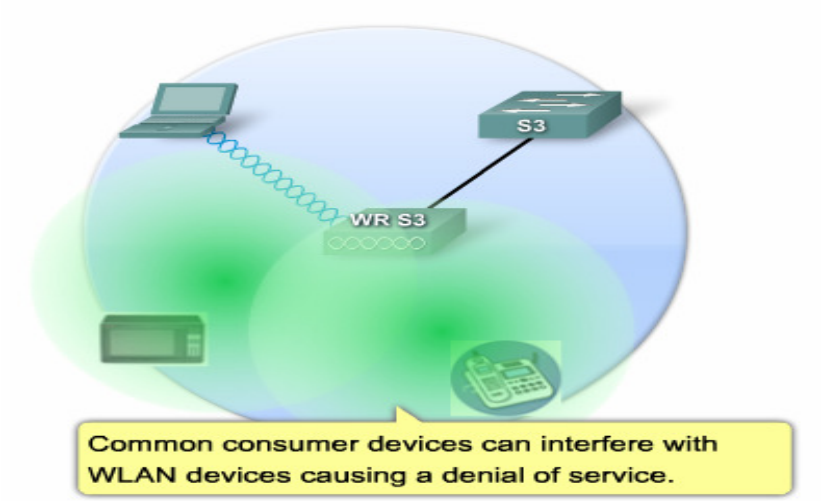
Όταν όλοι οι νόμιμοι χρήστες είναι γνωστοί, το δίκτυο μπορεί να ελέγχει ευκολότερα τις συσκευές και την κυκλοφορία που δεν θα έπρεπε να είναι εκεί. Τα WLANs των επιχειρήσεων που χρησιμοποιούν συσκευές κατάστασης προόδου παρέχουν στους διαχειριστές εργαλεία που λειτουργούν ως ασύρματο intrusion prevention system (IPS). Αυτά τα εργαλεία περιλαμβάνουν ανιχνευτές που εντοπίζουν τα κακόβουλα σημεία πρόσβασης και τα δίκτυα ad hoc καθώς και τη ραδιο διαχείριση των πόρων ,radio resource management (RRM), που ελέγχει τη ζώνη των ραδιοσυχνοτήτων (RF) για το φορτίο του σημείου πρόσβασης. Ένα σημείο πρόσβασης που είναι απασχολημένο περισσότερο από το κανονικό, προειδοποιεί τον διαχειριστή για την πιθανή ύπαρξη μη εξουσιοδοτημένης κυκλοφορίας.



Εικόνα 25. Επίθεση Man-in-the-Middle.

3.2.4 Επιθέσεις Denial of Service (DoS)

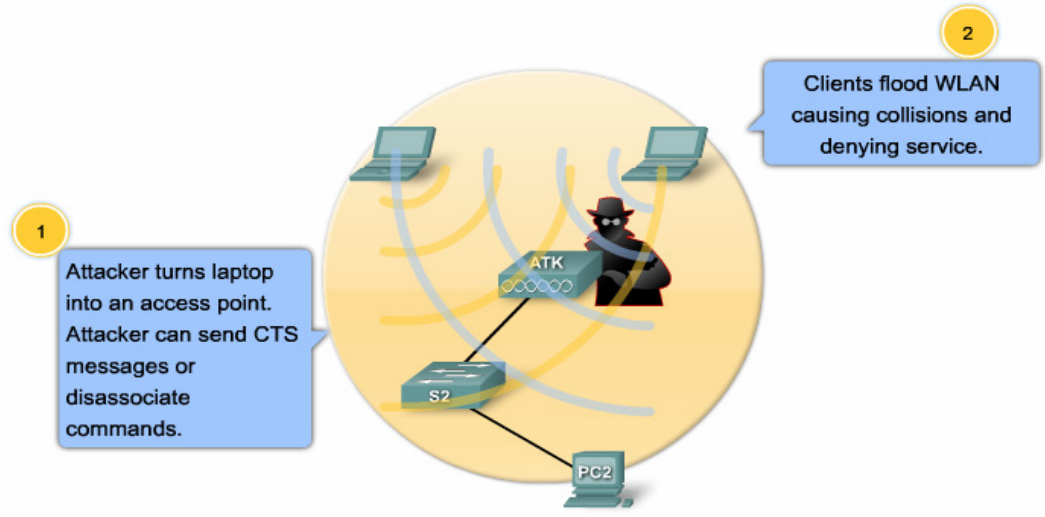
Τα ασύρματα δίκτυα 802.11b και g χρησιμοποιούν τη χωρίς άδεια ζώνη των 2.4 Ghz. Αυτή η ζώνη που χρησιμοποιείται και από τα περισσότερα ασύρματα καταναλωτικά προϊόντα, συμπεριλαμβανομένων των ασύρματων τηλέφωνων και των φούρνων μικροκυμάτων. Με αυτές τις συσκευές που εκπέμπουν όλες στην ίδια ζώνη RF, οι επιτιθέμενοι μπορούν να δημιουργήσουν "θόρυβο" σε όλα της τα κανάλια.



Εικόνα 26. Άρνηση υπηρεσίας εξαιτίας παρεμβολών από άλλες συσκευές.

Ο επιτιθέμενος, που χρησιμοποιεί ένα PC ως σημείο πρόσβασης (με ειδικό λογισμικό στην ασύρματη κάρτα δικτύου), μπορεί να πλημμυρίσει ένα BSS με μηνύματα clear to send (CTS), τα οποία νικούν τη λειτουργία CSMA/CA που χρησιμοποιείται από τους σταθμούς. Τα σημεία πρόσβασης, με τη σειρά τους, πλημμυρίζουν το BSS με ταυτόχρονη κυκλοφορία, προκαλώντας συγκρούσεις στα πακέτα (collisions).

Μια άλλη επίθεση DOS που μπορεί να πραγματοποιηθεί σε ένα BSS είναι όταν ένας επιτιθέμενος στέλνει μια σειρά εντολών αποσυσχέτισης που αναγκάζουν όλους τους σταθμούς στο BSS να αποσυνδεθούν. Όταν οι σταθμοί αποσυνδεθούν, ξεκινούν αμέσως την διαδικασία association από την αρχή, κάτι το οποίο δημιουργεί μια έκρηξη κυκλοφορίας. Ο επιτιθέμενος στέλνει άλλη μια εντολή αποσυσχέτισης και ο κύκλος επαναλαμβάνεται.



Εικόνα 27. Επίθεση άρνησης υπηρεσίας (DoS).

3.3 Πρωτόκολλα ασύρματης ασφάλειας

Σε αυτήν την ενότητα, θα παρουσιαστούν τα χαρακτηριστικά γνωρίσματα των κοινών πρωτοκόλλων και το επίπεδο ασφάλειας που το κάθε ένα παρέχει.

Δύο τύποι επικυρώσεων (authentication) εισήχθησαν στα τα αρχικά πρότυπα 802.11: η ανοικτή και η διαμοιραζόμενου κλειδιού WEP. Η ανοικτή επικύρωση είναι στην πραγματικότητα «καμία επικύρωση». Ένας σταθμός ζητά επικύρωση και το σημείο πρόσβασης την χορηγεί. Η επικύρωση WEP παρέχει ασφάλεια σε μια σύνδεση, όπως ένα καλώδιο που συνδέει ένα PC με μία θύρα Ethernet. Τα κοινά διαμοιραζόμενα κλειδιά WEP αποδειχτήκαν αδύναμα και κάτι καλύτερο χρειαζόταν. Η πρώτη αντίδραση των εταιριών στην αδυναμία του διαμοιραζόμενου κλειδιού WEP, ήταν να δοκιμαστούν τεχνικές όπως η απόκρυψη των SSIDs και το φιλτράρισμα των MAC διευθύνσεων. Αυτές οι τεχνικές ήταν επίσης πάρα πολύ αδύνατες.

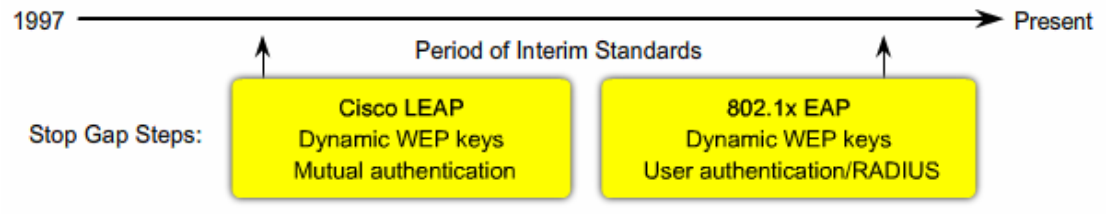
Οι αδυναμίες με την κρυπτογράφηση διαμοιραζόμενου κλειδιού WEP ήταν δύο. Πρώτον, ο αλγόριθμος που χρησιμοποιήθηκε για να κρυπτογραφήσει τα δεδομένα δεν ήταν ισχυρός. Δεύτερον, τα συστήματα δεν ήταν ευέλικτα . Τα κλειδιά WEP των 32 bit εισάγονταν με το χέρι από τους χρήστες, συχνά ανακριβώς, δημιουργώντας συνεχώς την ανάγκη για τεχνική υποστήριξη.

Μετά από την αδυναμία της WEP ασφάλειας, υπήρξε μια περίοδος προσωρινών μέτρων ασφαλείας. Οι προμηθευτές όπως η Cisco, που ήθελαν να ικανοποιήσουν τις απαιτήσεις για καλύτερη ασφάλεια, ανέπτυξαν δικά τους συστήματά και ταυτόχρονα βοήθησαν να εξελιχτούν τα πρότυπα 802.11i. Κατά τη διαδρομή στο πρότυπο 802.11i, ο αλγόριθμος κρυπτογράφησης TKIP δημιουργήθηκε, ο οποίος συνδέθηκε με την μέθοδο ασφάλειας (WPA) WiFI Protected Access εγκεκριμένη από την Wi-Fi Alliance.

Σήμερα, τα πρότυπα που πρέπει να ακολουθηθούν στα περισσότερα δίκτυα επιχειρήσεων είναι τα πρότυπα 802.11i.
Για τις επιχειρήσεις το WPA2 περιλαμβάνει μια σύνδεση σε μια βάση δεδομένων ενός server Remote Authentication Dial In User Service (RADIUS).

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i

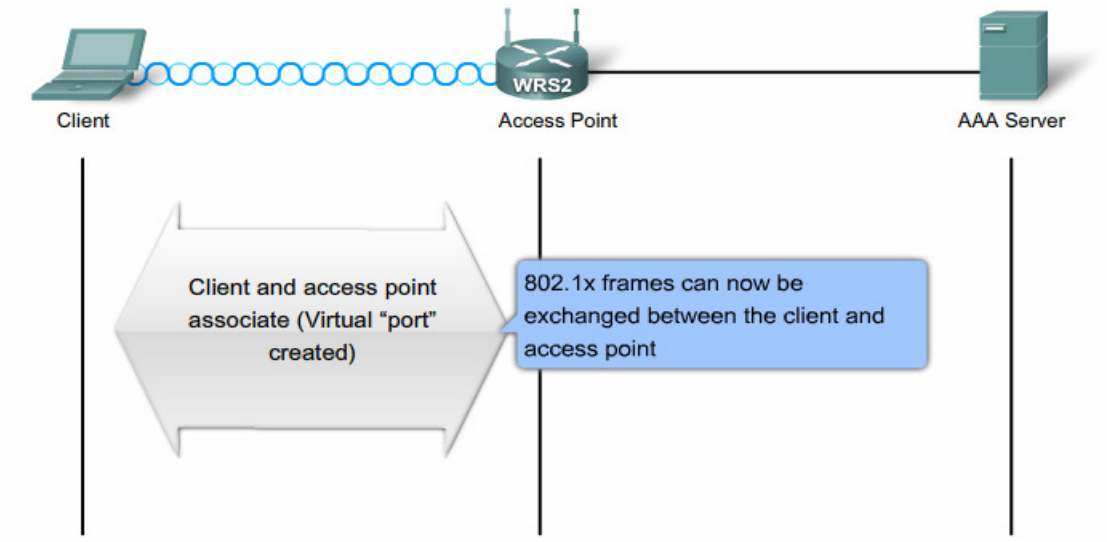
Πίνακας 4. Τα πρωτόκολλα ασύρματης ασφάλειας.



Εικόνα 28. Τα πρωτόκολλα ασύρματης ασφάλειας στο χρόνο.

3.4 Επικύρωση (Authentication)

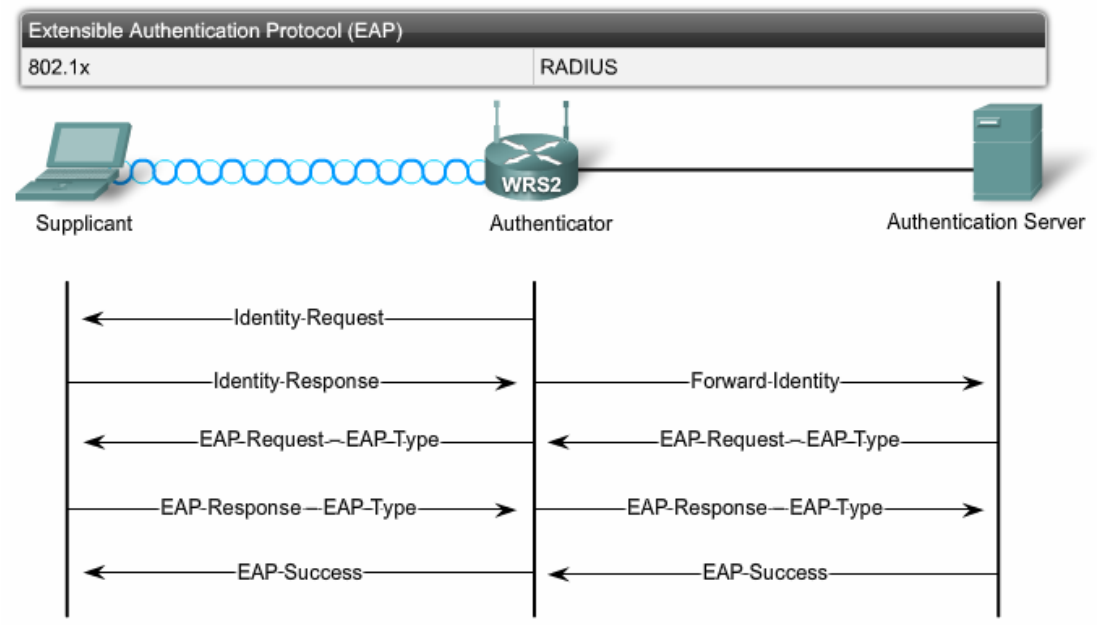
Σε ένα ανοικτό δίκτυο, όπως ένα οικιακό δίκτυο, η ένωση (association) μπορεί να είναι αρκετή για να αποκτήσει ο χρήστης πρόσβαση στις συσκευές και τις υπηρεσίες του ασύρματου δικτύου. Στα δίκτυα που έχουν αυστηρότερες απαιτήσεις ασφάλειας, απαιτείται επικύρωση (authentication) ή σύνδεση με τη χρήση κάποιου κωδικού, για να αποκτήσει ο χρήστης πρόσβαση. Αυτή η διαδικασία σύνδεσης με τη χρήση κωδικού ρυθμίζεται από το πρωτόκολλο EAP (Extensible Authentication Protocol). Το EAP είναι ένα πλαίσιο για την επικύρωση (authentication) στο δίκτυο. Η IEEE βελτίωσε το πρότυπο 802.11i για την επικύρωση και την έγκριση στα WLAN με το πρωτόκολλο IEEE 802.1x.



Εικόνα 29. Association μεταξύ χρήστη και σημείου πρόσβασης.

Η διαδικασία επικύρωσης (authentication) WLAN συνοψίζεται ως εξής:

- Η διαδικασία ένωσης (association) 802.11 δημιουργεί μία εικονική πόρτα για κάθε χρήστη στο σημείο πρόσβασης.
- Το σημείο πρόσβασης εμποδίζει όλα τα πλαίσια δεδομένων, εκτός από την κυκλοφορία 802.1x.
- Τα πλαίσια 802.1x μεταφέρουν τα πακέτα επικύρωσης EAP μέσω του σημείου πρόσβασης σε έναν κεντρικό υπολογιστή που διατηρεί τα πιστοποιητικά επικύρωσης. Αυτός ο κεντρικός υπολογιστής είναι ένας AAA server (Authentication, Authorization,Accounting), που τρέχει ένα πρωτόκολλο RADIUS .
- Εάν η επικύρωση EAP είναι επιτυχής, ο AAA Server στέλνει ένα μήνυμα επιτυχίας EAP στο σημείο πρόσβασης, το οποίο επιτρέπει έπειτα την κυκλοφορία των δεδομένων μέσω της εικονικής πόρτα.
- Πρίν ανοίξει η εικονική πόρτα, δημιουργείται μια κρυπτογραφημένη σύνδεση μεταξύ του χρήστη και του access point για να εξασφαλίσει ότι κανένας άλλος χρήστης του δικτύου δεν μπορεί να έχει πρόσβαση στην πόρτα που έχει καθιερωθεί για τον συγκεκριμένο επικυρωμένο πελάτη.



Εικόνα 30. Η διαδικασία επικύρωσης-authentication.

Προτού αρχίσει να χρησιμοποιείται το 802.11i (WPA2) ή ακόμα και το WPA, μερικές επιχειρήσεις προσπάθησαν να ασφαλίσουν τα WLANs τους με φιλτράρισμα των MAC διευθύνσεων και την μη εκπομπή των SSID των σημείων πρόσβασης. Σήμερα, είναι εύκολο να χρησιμοποιηθεί λογισμικό για να τροποποιήσει την MAC διεύθυνση , έτσι το φιλτράρισμα διευθύνσεων MAC είναι αναποτελεσματικό. Δεν σημαίνει ότι δεν πρέπει γίνεται, αλλά πρέπει να συνοδεύεται με πρόσθετη ασφάλεια, όπως WPA2.

Ακόμα κι αν ένα SSID δεν εκπέμπεται από ένα σημείο πρόσβασης, η κυκλοφορία που περνά μπρος πίσω μεταξύ του χρήστη και του σημείου πρόσβασης αποκαλύπτει

τελικά το SSID. Εάν ένας επιτιθέμενος παρακολουθεί τη ζώνη των ραδιοσυχνοτήτων RF, το SSID μπορεί συλλεχθεί μαζί με άλλες πληροφορίες σε μια από αυτές τις συναλλαγές, επειδή στέλνεται χωρίς κρυπτογράφηση. Η ευκολία ανακάλυψης των SSIDs έχει οδηγήσει μερικούς ανθρώπους να επιτρέπουν την αναμετάδοση των SSIDs στα σημεία πρόσβασης.

Η ιδέα να ασφαλιστεί ένα WLAN με τίποτα περισσότερο από το φιλτράρισμα των MAC και την απενεργοποίηση της μετάδοσης SSID μπορεί να οδηγήσει σε ένα απολύτως επισφαλές WLAN. Ο καλύτερος τρόπος για να διασφαλιστούν οι χρήστες στο WLAN είναι να χρησιμοποιηθεί μια μέθοδος ασφάλειας που ενσωματώνει έλεγχο προσπέλασης δικτύων βασισμένο σε πόρτες, όπως το WPA2.

3.5 Κρυπτογράφηση (Encryption)

Δύο μηχανισμοί κρυπτογράφησης που προσδιορίζονται στο 802.11i έχουν πιστοποιηθεί ως WPA και WPA2 από τη WI-Fi Alliance: ο μηχανισμός Temporal Key Integrity Protocol (TKIP) και Advanced Encryption Standard (AES).

TKIP είναι η μέθοδος κρυπτογράφησης που πιστοποιείται ως WPA. Παρέχει υποστήριξη στον εξοπλισμό WLAN με την επανεξέταση των αρχικών αδυναμιών που συνδέονται με τη μέθοδο κρυπτογράφησης 802.11 WEP. Χρησιμοποιεί τον αρχικό αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε από το WEP.

Ο μηχανισμός TKIP έχει δύο βασικές λειτουργίες:

- Κρυπτογραφεί τα πακέτα "επιπέδου 2" (Layer2).
- Πραγματοποιεί έλεγχο ακεραιότητας μηνυμάτων (message integrity check - MIC) στο κρυπτογραφημένο πακέτο.

Αυτό εξασφαλίζει ότι το μήνυμα δεν θα αλλάξει από το αρχικό, δηλαδή από τον αποστολέα στον παραλήπτη κατά την διαδικασία της μετάδοσης.

Αν και ο μηχανισμός TKIP επανεξετάζει όλες τις γνωστές αδυναμίες του WEP, η κρυπτογράφηση AES WPA2 είναι η προτιμώμενη μέθοδος, αφού είναι η μέθοδος που προσεγγίζει καλύτερα τις απαιτήσεις των περισσοτέρων επιχειρήσεων, γνωστή και ως IEEE 802.11i.

Ο μηχανισμός AES έχει τις ίδιες λειτουργίες με τον TKIP, αλλά χρησιμοποιεί πρόσθετα στοιχεία από τον header της MAC που επιτρέπει στους σταθμούς προορισμού να αναγνωρίσουν εάν τα μη κρυπτογραφημένα κομμάτια του μηνύματος έχουν πειραχτεί. Προσθέτει επίσης έναν αριθμό ακολουθίας (sequence number) στον header των κρυπτογραφημένων δεδομένων.

Μερικές φορές κατά την παραμετροποίηση των ρυθμίσεων ασφαλείας σε ένα σημείο πρόσβασης ή έναν ασύρματο δρομολογητή στις επιλογές των ρυθμίσεων μπορεί να μην εμφανίζονται οι επιλογές WPA ή WPA2 αντί γι αυτών να υπάρχει κάτι που ονομάζεται pre-shared key (PSK). Διάφοροι τύποι PSKs φαίνονται παρακάτω:

- ❖ Το PSK ή το PSK2 με TKIP είναι το ίδιο με το WPA
- ❖ Το PSK ή το PSK2 με AES είναι το ίδιο με το WPA2
- ❖ Το PSK2, χωρίς να προσδιορίζεται κάποια μέθοδος κρυπτογράφησης, είναι το ίδιο με το WPA2

TKIP – Temporal Key Integrity Key	AES – Advanced Encryption Standard
• Encrypts by adding increasingly complex bit coding to each packet • Based on same cipher (RC4) as WEP	• New cipher used in 802.11i • Based on TKIP with additional features that enhances the level of provided security

Πίνακας 5. Μηχανισμοί κρυπτογράφησης TKIP και AES.

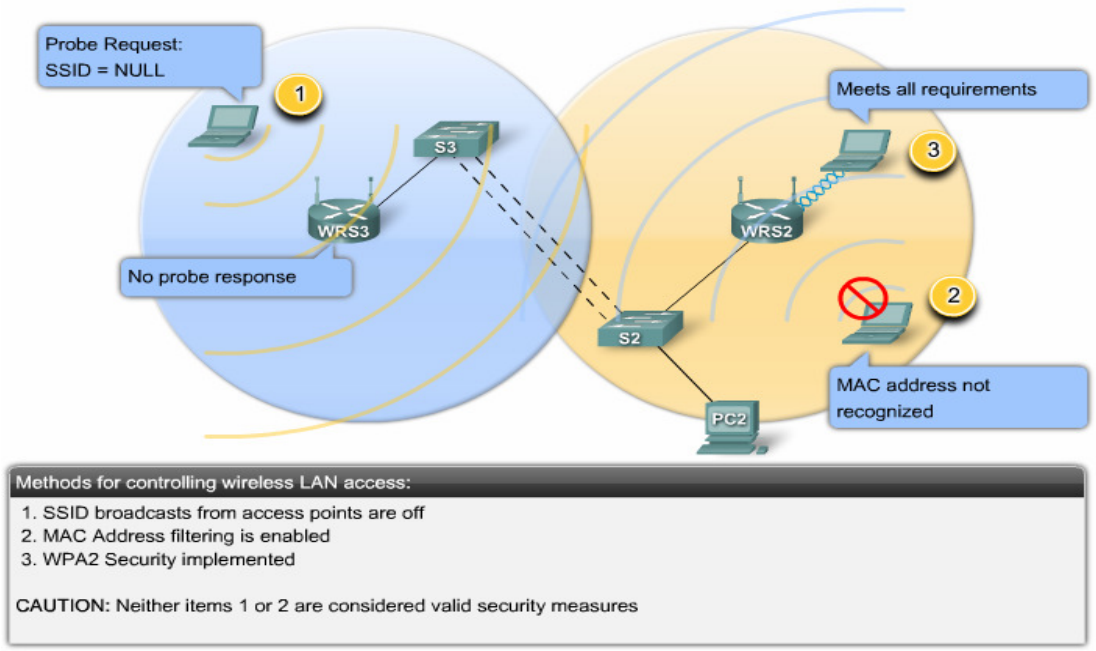
3.6 Ασφαλίζοντας ένα ασύρματο δίκτυο

Η ασφάλεια σ ένα ασύρματο τοπικό δίκτυο και ειδικά σ εκείνα των επιχειρήσεων πρέπει να γίνεται σε βάθος. Η έννοια του βάθους σημαίνει ότι ο διαχειριστής έχει πολλές λύσεις διαθέσιμες. Είναι όπως η κατοχή ενός συστήματος ασφαλείας στο σπίτι, που ενώ έχει τοποθετηθεί ο συναγερμός, όλες οι πόρτες και τα παράθυρα έχουν κλειδωθεί και επιπλέον ζητάμε από τους γείτονες μας να το προσέχουν όταν απουσιάζουμε.

Οι μέθοδοι ασφάλειας , ειδικά το WPA2, είναι όπως η κατοχή ενός συστήματος ασφαλείας. Εάν όμως απαιτείται κάτι για να ασφαλίσει επιπλέον την πρόσβαση στο WLAN, τότε μπορεί να εφαρμοστεί η παρακάτω προσέγγισης τριών σταδίων:

1. Απενεργοποίηση της επιλογής της μετάδοσης SSID από τα σημεία πρόσβασης.
2. Φιλτράρισμα των MAC διευθύνσεων - Πίνακες βασισμένοι στις MAC διευθύνσεις κατασκευάζονται με το χέρι από τον διαχειριστή στο σημείο πρόσβασης για να επιτρέψουν ή να απαγορεύσουν στους χρήστες την πρόσβαση.
3. Εφαρμογή ασφάλειας στο WLAN - WPA ή WPA2.

Μια πρόσθετη ενέργεια για έναν άγρυπνο διαχειριστή δικτύων είναι να διαμορφώσει τα σημεία πρόσβασης που είναι κοντά στους εξωτερικούς τοίχους των κτηρίων να εκπέμπουν σε χαμηλότερη ένταση από τα άλλα σημεία πρόσβασης που είναι τοποθετημένα στη μέση του κτηρίου. Αυτό πρόκειται να μειώσει την εκπομπή ραδιοκυμάτων εκτός του κτηρίου όπου καθένας μπορεί να τρέξει μια εφαρμογή όπως Netstumbler (http://www.netstumbler.com), το Wireshark και άλλα και να χαρτογραφήσει το WLAN.



Εικόνα 31. Ασφαλίζοντας ένα ασύρματο δίκτυο.

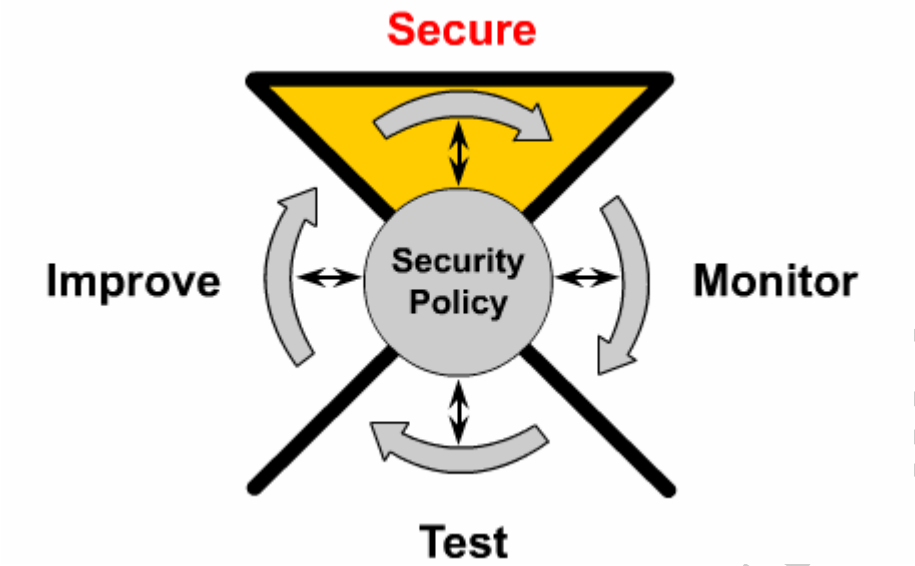
3.7 Ο τροχός ασφαλείας (Security Wheel)

Τα περισσότερα γεγονότα στην ασύρματη ασφάλεια εμφανίζονται επειδή οι διαχειριστές των συστημάτων δεν εφαρμόζουν τα διαθέσιμα αντίμετρα. Επομένως, το ζήτημα δεν είναι μόνο η επιβεβαίωση ότι μια τεχνική ευπάθεια υπάρχει και η εύρεση ενός αντίμετρου που λειτουργεί. Είναι επίσης κρίσιμο να ελεγχτεί ότι το αντίμετρο είναι σωστά τοποθετημένο και λειτουργεί κατάλληλα.

Σε αυτό ακριβώς, ο τροχός ασφαλείας (security wheel), που είναι μια συνεχής διαδικασία ασφάλειας, είναι αποτελεσματικός. Ο τροχός ασφαλείας WLAN όχι μόνο προωθεί την εφαρμογή των μέτρων ασφάλειας στο δίκτυο, αλλά το πιο σημαντικό, προωθεί τον επανέλεγχο και την εφαρμογή ενημερωμένων μέτρων ασφάλειας σε συνεχή βάση. Ο τροχός ασφάλειας WLAN φαίνεται στις παρακάτω εικόνες.

Σταδιο1.
Ασφαλίζοντας το δίκτυο με την εφαρμογή πολιτικής ασφαλείας και την εφαρμογή των ακόλουθων λύσεων :

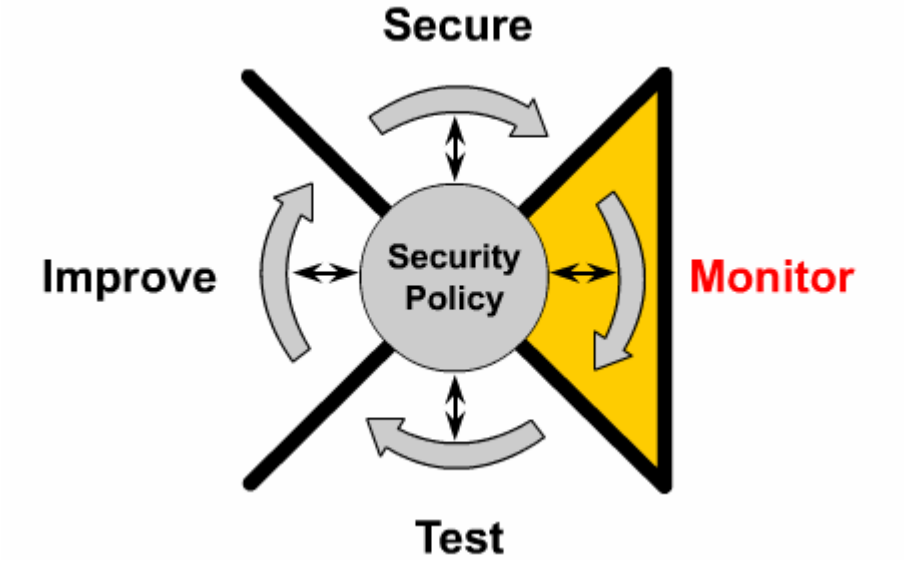
- Authentication, authorization and accounting
- Firewalls
- Virtual Private Networks (VPNs)
- Vulnerability patching
- Intrusion Detection



Εικόνα 32. Security Wheel – Secure.

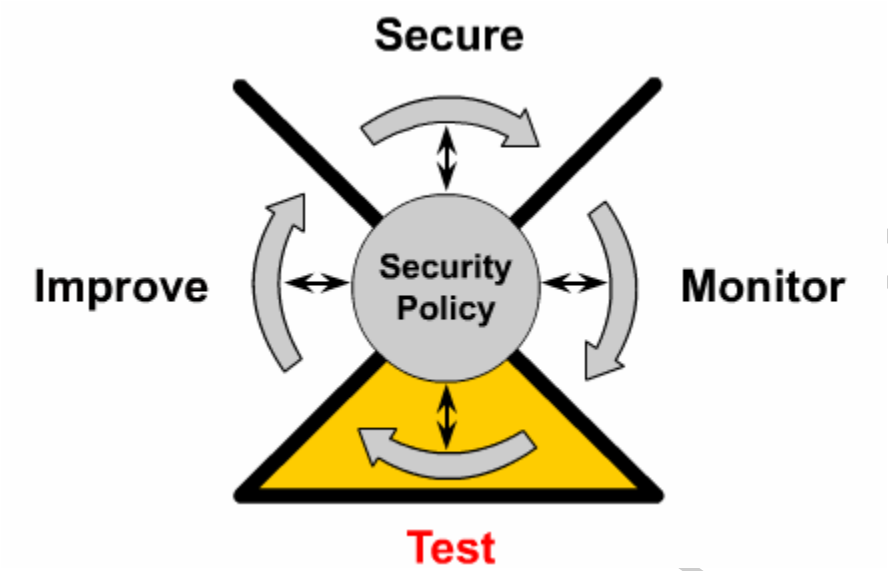
Στάδιο 2.
Έλεγχος του δικτύου.
Επικυρώνονται οι εφαρμογές ασφαλείας που έγιναν στο στάδιο 1.
Εντοπισμός παραβιάσεων στην πολιτική ασφαλείας:

- System Auditing
- Real-time Intrusion Detection



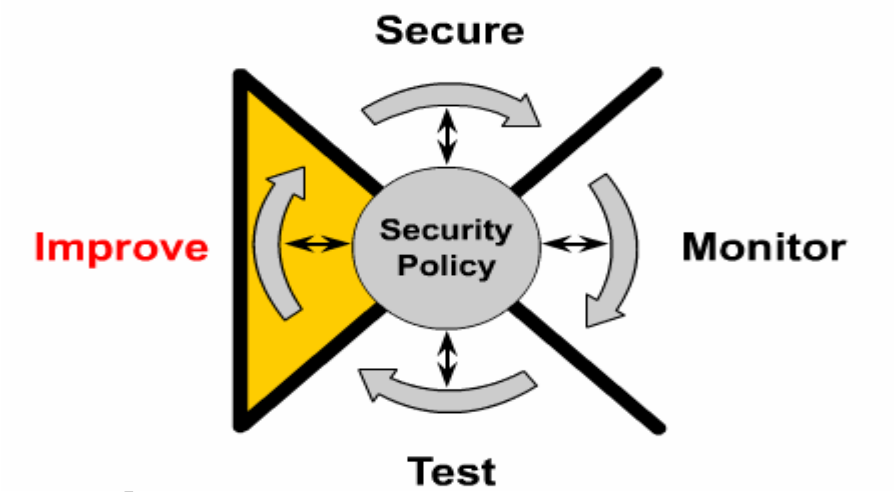
Εικόνα 33. Security Wheel – Monitor.

Στάδιο 3.
Επικυρώνεται η αποτελεσματικότητα της εφαρμογής της πολιτικής ασφαλείας μέσω του ελέγχου του συστήματος και την ανίχνευση ευπαθειών.



Εικόνα 34. Security Wheel – Test.

Στάδιο 4.
Χρησιμοποιούνται οι πληροφορίες από τα προηγούμενα στάδια 2 και 3 του ελέγχου και των δοκίμων προκειμένου να γίνουν βελτιώσεις στην εφαρμογή της ασφάλειας. Επίσης η πολιτική ασφαλείας αναπροσαρμόζεται σύμφωνα με τις αδυναμίες και τους κινδύνους που εντοπίστηκαν προηγουμένως.



Εικόνα 35. Security Wheel – Improve.

Για να αρχίσει η διαδικασία του τροχού ασφαλείας, πρώτα πρέπει να αναπτυχθεί μια πολιτική ασφαλείας WLAN που επιτρέπει την εφαρμογή των μέτρων ασφαλείας. Μια πολιτική ασφαλείας πρέπει να πληροί τα ακόλουθα:

- Να προσδιορίζει τους στόχους της ασύρματης ασφάλειας.
- Να καταγράφει τους πόρους που πρέπει να προστατευτούν.
- Να προσδιορίζει την υποδομή του δικτύου με χάρτες και καταλόγους-πίνακες.

Οι ασύρματες πολιτικές ασφαλείας αξίζουν το χρόνο και την προσπάθεια να αναπτυχθούν επειδή παρέχουν πολλά οφέλη. Η ανάπτυξη μιας καλής πολιτικής ασφαλείας ολοκληρώνει τα εξής:

- Παρέχει μια διαδικασία που ελέγχει την υπάρχουσα ασύρματη ασφάλεια.
- Παρέχει ένα γενικό πλαίσιο για την εφαρμογή της ασφάλειας.
- Καθορίζει τη συμπεριφορά που επιτρέπεται και που δεν επιτρέπεται.
- Βοηθάει να καθοριστούν ποια εργαλεία και ποιές διαδικασίες απαιτούνται για την οργάνωση.
- Βοηθάει την επικοινωνία και την συναίνεση μεταξύ μιας ομάδας ατόμων που παίρνουν τις αποφάσεις κλειδιά και καθορίζουν τις ευθύνες των χρηστών και των διαχειριστών.
- Καθορίζει μια διαδικασία για τις ασύρματες παραβιάσεις.
- Δημιουργεί μια βάση για νομική δράση, εάν είναι απαραίτητο.

Μια αποτελεσματική πολιτική ασύρματης ασφαλείας λειτουργεί για να εξασφαλίσει ότι το δίκτυο και οι πληροφορίες του οργανισμού προστατεύονται από τη δολιοφθορά και από την ακατάλληλη πρόσβαση, η οποία περιλαμβάνει και τη σκόπιμη και τυχαία πρόσβαση. Όλες οι ασύρματες ιδιότητες ασφαλείας πρέπει να διαμορφωθούν σύμφωνα με τη πολιτική ασφαλείας του οργανισμού. Εάν μια πολιτική ασφαλείας δεν είναι επίκαιρη, ή είναι ξεπερασμένη, μια νέα πολιτική πρέπει να δημιουργηθεί πριν αποφασιστεί κάποια αλλαγή στην παραμετροποίηση ή την επέκταση ασύρματων συσκευών.

ΚΕΦΑΛΑΙΟ 4

Αποκτώντας μη εξουσιοδοτημένη πρόσβαση - DNS Tunneling

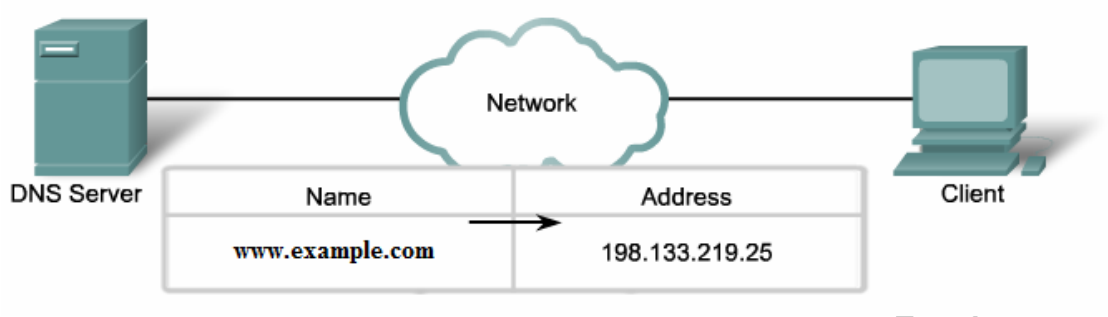
4.1 Εισαγωγή

Η περιήγηση στο Διαδίκτυο και το ηλεκτρονικό ταχυδρομείο βασίζονται στη χρήση ενός σημαντικού πρωτοκόλλου, του Domain Name System (DNS), που επιτρέπει στις εφαρμογές να λειτουργούν με την χρησιμοποίηση ονομάτων, όπως το example.com, αντί των διευθύνσεων IP που είναι πολύ δύσκολο να τις θυμάται κάποιος. Επειδή το πρωτόκολλο DNS δεν προορίζεται για τη μεταφορά δεδομένων, οι άνθρωποι μπορούν να το αγνοήσουν ως απειλή για κακόβουλες επικοινωνίες ή για υποκλοπή στοιχείων. Σύμφωνα με τον Rasmussen, για τις απειλές DNS, οι περισσότερες επιχειρήσεις είναι τελείως ανοιχτές στις πραγματικές επιθέσεις μέσω αυτού του όχι και τόσο διαδεδομένου παράγοντα (Rasmussen, 2012). Πολλές οργανώσεις έχουν ελάχιστο ή κανέναν έλεγχο για το DNS. Αντ' αυτού, στρέφουν την προσοχή τους στην κυκλοφορία της κίνησης από το Διαδίκτυο ή του ηλεκτρονικού ταχυδρομείου όπου συχνά πραγματοποιούνται επιθέσεις .

Υπάρχουν διάφορα εργαλεία διαθέσιμα για DNS tunneling που θα παρουσιαστούν παρακάτω. Ένα κοινό κίνητρο για αυτά τα εργαλεία είναι να αποκτηθεί η ελεύθερη πρόσβαση WI-Fi για τις περιοχές όπου απαιτείται πληρωμή , αλλά υπάρχει δυνατότητα ελεύθερης ροής DNS. Αυτά τα εργαλεία μπορούν επίσης να χρησιμοποιηθούν για περισσότερες κακόβουλες δραστηριότητες. Ένα DNS tunnel μπορεί να χρησιμοποιηθεί ως ένα πλήρες κανάλι απομακρυσμένου χειρισμού για έναν εσωτερικό χρήστη. Οι ικανότητες χειρισμού περιλαμβάνουν εντολές για τα λειτουργικά συστήματα (OS) και μεταφορές αρχείων. Παραδείγματος χάριν, η υποκλοπή στοιχείων μέσω DNS είναι μια μέθοδος που ενσωματώνεται μέσα στο εργαλείο δοκιμής διείσδυσης (penetration testing) squeeza (Haroon, 2007). Αυτά τα εργαλεία μπορούν επίσης να χρησιμοποιηθούν ως συγκεκαλυμμένο κανάλι για ένα malware. Παραδείγματος χάριν, το Feederbot (Dietrich, 2011) και το Moto (Mullaney, 2011) χρησιμοποιούν το DNS ως μέθοδο επικοινωνίας.

4.2 Επισκόπηση του DNS

Το Domain Name System (DNS) είναι ένα σημαντικό πρωτόκολλο και μια υπηρεσία που χρησιμοποιείται στο Διαδίκτυο. Η πιο κοινή χρήση του DNS είναι να αντιστοιχεί ονόματα με διευθύνσεις IP. Οι χρήστες μπορούν να εισάγουν ένα όνομα (π.χ. το example.com) στον περιηγητή (browser) τους. Το DNS χρησιμοποιείται για να βρει μια ή περισσότερες διευθύνσεις IP για εκείνο το όνομα. Αυτό είναι γνωστός ως "A' record". Οι χρήστες μπορούν μετά να στείλουν την κυκλοφορία HTTP στην διεύθυνση IP προορισμού. Το DNS ενισχύεται συνεχώς για να παρέχει νέες δυνατότητες. Αν και υπάρχουν προηγούμενα RFCs, η κυρίως DNS λειτουργία καθορίζεται στα RFCs 1034 και 1035 (Kozierok, 2005). Υπάρχουν πάνω από 20 άλλα RFCs που περιγράφουν πρόσθετες DNS λειτουργίες.

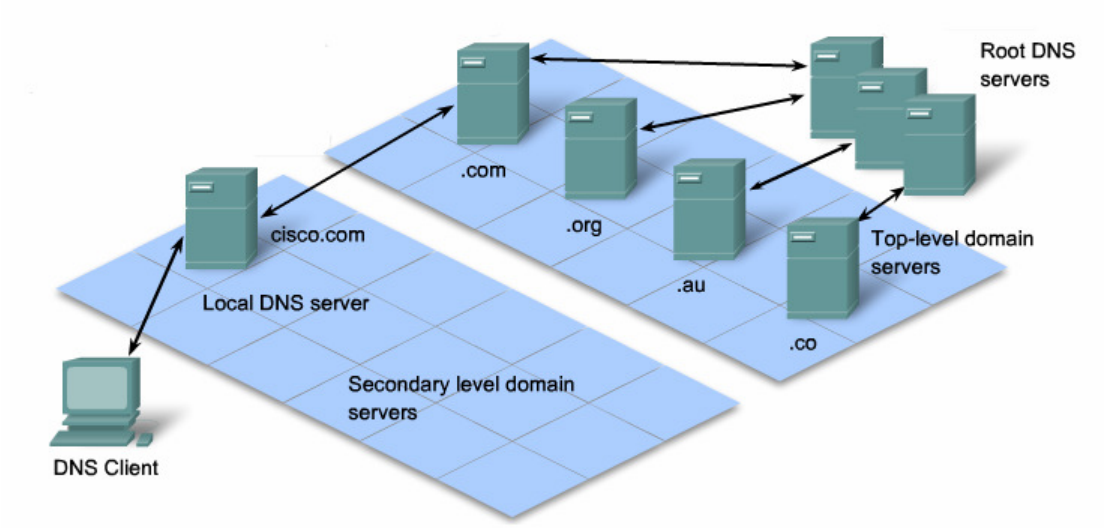


Εικόνα 36. Η λειτουργία του Domain Name System (DNS).

Το DNS έχει πάνω από 30 τύπους εγγραφών. Πολλοί είναι κρίσιμοι για βασικές υπηρεσίες του Διαδικτύου. Όπως αναφέρεται νωρίτερα, ο τύπος "A' record" αντιστοιχεί ένα όνομα με μια διεύθυνση ipv4. Ο τύπος "AAAA' record" χρησιμοποιείται για να αντιστοιχίσει ένα όνομα με μια ipv6 διεύθυνση. Ο τύπος "CNAME` record" χρησιμοποιείται για να αντιστοιχίσει ένα domain name στο κανονικό όνομα. Ο τύπος "MX` record" χρησιμοποιείται για να καθορίσει τους κεντρικούς υπολογιστές ταχυδρομείου (mail servers) για ένα domain. Ο τύπος "NS` record" χρησιμοποιείται για να καθορίσει τους servers που εγκρίνουν τα ονόματα για ένα domain. Ο τύπος "PTR` ή pointer record" συνήθως χρησιμοποιείται για να αντιστοιχίσει μια διεύθυνση IP στο domain name. Αυτό αναφέρεται συνήθως σαν αντίστροφη αναζήτηση. Ο τύπος "TXT` record" χρησιμοποιείται για να επιστρέψει στοιχεία κειμένων. Αυτός ο τύπος ήταν για συγκεκριμένους λόγους, όπως το Sender Policy Framework (SPF) για αντι-spam (Wong, 2006).

Το DNS χρησιμοποιεί την πόρτα 53 UDP και TCP για τις επικοινωνίες. Συνήθως το UDP χρησιμοποιείται, αλλά το TCP θα χρησιμοποιηθεί για φορτία (payloads) άνω των 512 bytes. Υπάρχει επίσης ο μηχανισμός επέκτασης DNS (EDNS) (Vixie, 1999). Εάν ο EDNS υποστηρίζεται και από τις δυο πλευρές σε μια DNS επικοινωνία, τότε φορτία UDP μεγαλύτερα από 512 bytes μπορούν να χρησιμοποιηθούν. Ο μηχανισμός EDNS είναι ένα χαρακτηριστικό που μπορεί να βελτιώσει το ρυθμό μεταφοράς δεδομένων σε ένα DNS tunnel.

Το DNS είναι ένα ιεραρχικό σύστημα, κάθε επίπεδο στην ιεραρχία μπορεί να παρασχεθεί από ένα κεντρικό υπολογιστή με διαφορετική ιδιοκτησία. Για το Διαδίκτυο, υπάρχουν 13 κύριοι dns servers. Αυτοί αντιπροσωπεύονται από πολύ περισσότερους από 13 φυσικούς servers. Η ιεραρχική φύση του DNS μπορεί να εξηγηθεί χρησιμοποιώντας ένα παράδειγμα . Πάρτε ένα παράδειγμα αιτήματος για τη διεύθυνση IP ενός domain που ονομάζεται my.test.example.com. Ένα νέο αίτημα θα πάει αρχικά στους κεντρικούς υπολογιστές να βρει ποιος κεντρικός υπολογιστής ελέγχει το κορυφαίοο domain .com. ο κεντρικός υπολογιστής που ελέγχει το .com θα παράσχει τον κεντρικό υπολογιστή που ελέγχει το domain example.com. Έπειτα ο DNS κεντρικός υπολογιστής example.com θα παράσχει τον κεντρικό υπολογιστή που ελέγχει το domain test.example.com. Τέλος, ο DNS κεντρικός υπολογιστής του test.example.com θα παράσχει τη διεύθυνση IP για το my.test.example.com.



Εικόνα 37. Η ιεραρχική φύση του DNS.

Σε μια επιχείρηση, οι τελικές συσκευές των χρηστών δεν κάνουν DNS αιτήματα άμεσα στο Διαδίκτυο. Έχουν τους εσωτερικούς DNS servers που παρέχουν DNS υπηρεσίες στις τελικές συσκευές. Εντούτοις, δεδομένου ότι ο εσωτερικός DNS server θα διαβιβάσει τα αιτήματά τους μέχρι να επικοινωνήσει με τον DNS server που είναι υπεύθυνος για τα κορυφαία domain , ένας επιτιθέμενος με πρόσβαση σε μια εσωτερική τελική συσκευή μπορεί να παρέμβει με την υποδομή ενός DNS tunnel σε ένα domain που αυτοί ελέγχουν.

Το DNS αποθηκεύει για κάποιο χρονικό διάστημα τις εγγραφές του. Όταν οι DNS απαντήσεις δίνονται, ένα time to live (TTL) συμπεριλαμβάνεται. Ο λαμβάνων ενδιάμεσος DNS server μπορεί να χρησιμοποιήσει εκείνη την εγγραφή και να αποθηκεύσει για το χρονικό διάστημα TTL το αποτέλεσμα. Κατόπιν εάν ένα ίδιο αίτημα του ζητηθεί, το αποθηκευμένο αποτέλεσμα μπορεί να παρασχεθεί άμεσα αντί της εκτέλεσης μιας νέας αναζήτησης.

4.3 DNS tunneling

Το DNS είναι μια υπηρεσία που χρησιμοποιείται σε κάθε σύστημα με πρόσβαση στο Διαδίκτυο. Είναι επομένως ένας κατάλληλος στόχος για κακόβουλη χρήση. Η κακόβουλη χρήση υπό εξέταση εδώ είναι το DNS tunneling. Με το DNS tunneling, ένα άλλο πρωτόκολλο μπορεί να περάσει μέσω του πρωτοκόλλου DNS.
Ένα DNS tunnel μπορεί να χρησιμοποιηθεί για εντολές και έλεγχο, υποκλοπή στοιχείων ή να περάσει οποιαδήποτε IP κυκλοφορία. Σε μια παρουσίαση του 2012 στη διάσκεψη RSA,προσδιορίστηκε το “DNS command and control of malware” ως μια από τις έξι πιο επικίνδυνες νέες επιθέσεις. Οι επιτιθέμενοι έχουν χρησιμοποιήσει πρόσφατα αυτήν την τεχνική σε περιπτώσεις που περιλαμβάνουν την κλοπή εκατομμυρίων λογαριασμών των χρηστών (Skoudis, 2012). Έχει παρουσιαστεί ότι το DNS tunneling μπορεί να επιτύχει ρυθμό μεταφοράς δεδομένων 110 KB/s με latency 150ms (Van Leijenhorst, 2008).

4.3.1 Βασικά στοιχεία των Dns tunnels

Πολλά από τα εργαλεία για DNS tunneling δημιουργήθηκαν με την πρόθεση να παρακάμψουν τα captive portals για την πληρωμένη υπηρεσία Wi-Fi. Εάν ένα από αυτά τα συστήματα επιτρέπει όλη την DNS κυκλοφορία, ένα DNS tunnel μπορεί να στηθεί για να ανοίξει την κυκλοφορία IP χωρίς πληρωμή για την υπηρεσία. Μερικές από τις εφαρμογές DNS tunneling δημιουργούν μια διεπαφή tun ή tap τοπικά στο σύστημα της τελικής συσκευής. Θα υπάρξει επίσης μια συσκευή tun ή tap στον DNS server που φιλοξενεί το εργαλείο για το DNS tunneling. Αυτό θα επιτρέψει στο χρήστη να περάσει την κυκλοφορία IP στο Διαδίκτυο. Αυτή η τεχνική είναι παρόμοια με την λειτουργία του λογισμικού του VPN , το OpenVPN. Υπάρχουν ακόμη και εμπορικοί φορείς παροχής υπηρεσιών που παρέχουν το tunnel από την πλευρά του server ως υπηρεσία. Αυτές οι υπηρεσίες μπορούν να πωληθούν ως VPN over DNS. Ο χρήστης εγκαθιστά το λογισμικό και συνδέεται με τον DNS server του παρόχου της υπηρεσίας που τρέχει το λογισμικό για το tunneling.Αυτές οι υπηρεσίες έχουν λογισμικό πελατών για διάφορα λειτουργικά συστήματα συμπεριλαμβανομένου των Android. Τέλος σε ορισμένες περιπτώσεις υπάρχουν δυναμικά λογισμικά για DNS tunneling όπως το Iodine.

4.3.2 Τα συστατικά των Dns tunnels

Η πρώτη γνωστή συζήτηση για το DNS tunneling ήταν από τον Oskar Pearson τον Απρίλιο του 1998 (pearson, 1998). Από την εποχή εκείνη διάφορες εφαρμογές DNS tunneling έχουν αναπτυχθεί. Όλες οι εφαρμογές χρησιμοποιούν παρόμοιες τεχνικές στον βασικό τους κορμό αλλά διαφέρουν στην κωδικοποίηση και σε άλλες λεπτομέρειες υλοποίησης. Οι βασικές τεχνικές που χρησιμοποιούνται από όλες τις εφαρμογές περιλαμβάνουν ένα ελεγχόμενο domain ή subdomain, κάποιο κομμάτι από την πλευρά του server και της τελικής συσκευής και μία τεχνική κωδικοποίησης του DNS payload.

4.3.3 Κωδικοποίηση και Τεχνικές

Μια από τις βασικές διαδικασίες είναι να κωδικοποιηθούν τα δεδομένα στο DNS payload. Είναι μια περιοχή όπου οι διάφορες εφαρμογές που υπάρχουν ποικίλλουν ευρέως. Με πολύ απλά λόγια, ένας χρήστης θέλει να στείλει δεδομένα στο server. Θα κωδικοποιήσει τα δεδομένα στο payload. Για παράδειγμα, ο χρήστης θα μπορούσε να στείλει ένα αίτημα τύπου A record όπου τα δεδομένα κωδικοποιούνται:

MRZGS3TLEBWW64TFEBXXMYLMORUW4ZI.t.example.com.

Ο κεντρικός υπολογιστής θα μπορούσε να αποκριθεί με μια απάντηση ως απάντηση CNAME:

NVWW2IDPOZQWY5DJNZSQ.t.example.com.

Κατά αυτόν τον τρόπο οποιαδήποτε δεδομένα μπορούν να κωδικοποιηθούν και να σταλούν στον server. Ο server μπορεί επίσης να αποκριθεί με οποιαδήποτε δεδομένα.

Ο server δεν μπορεί να αρχίσει άμεσα μια επικοινωνία. Οι τελικές συσκευές δεν έχουν κάποια υπηρεσία που να μπορεί να "ακούσει" τα αιτήματα DNS και είναι συνήθως πίσω από ένα firewall.

Οι εφαρμογές DNS tunneling διαφέρουν σε κάποιες λεπτομέρειες υλοποίησης. Ποικίλλουν στη γλώσσα υλοποίησης με τα εργαλεία να υλοποιούνται σε C, Java, Perl και Python. Μερικές υλοποιήσεις χρησιμοποιούν ένα tun ή tap interface που έχει δημιουργηθεί τοπικά και δύο διευθύνσεις IP για το tunnel. Άλλες μεταφέρουν μέσω του tunnel μόνο τα δυαδικά στοιχεία.

Η μέθοδος κωδικοποίησης συμπεριλαμβανομένου των διαφόρων τύπων DNS records είναι μια περιοχή όπου υπάρχουν διαφοροποιήσεις στην υλοποίηση των εργαλείων. Μερικές εφαρμογές χρησιμοποιούν τους κοινούς τύπους record όπως A record. Άλλες χρησιμοποιούν τους πειραματικούς τύπους όπως το Null record και το EDNS για να βελτιώσουν την απόδοση τους (Revelli, 2009).

Κωδικοποίηση Base32
Η κωδικοποίηση Base32 ή 5-bit χρησιμοποιείται συνήθως στα αιτήματα από τον client. Ενώ τα ονόματα DNS μπορούν να έχουν κεφαλαία και πεζά γράμματα, η κωδικοποίηση αυτή τα αγνοεί και έτσι μένουν26 γράμματα. Επιπλέον, οι αριθμοί και ο χαρακτήρας "-" επιτρέπονται. Αυτό παρέχει ένα σύνολο από 37 μοναδικούς χαρακτήρες. Επομένως, μπορούμε να πάρουμε τα δεδομένα σε 5 μπιτ τη φορά που μας δίνει 32 πιθανές τιμές. Αυτές οι 32 τιμές μπορούν να ταιριάξουν μέσα στους 37 διαθέσιμους χαρακτήρες μας. Το DNS επιτρέπει μέχρι 255 χαρακτήρες συνολικά σε κάθε subdomain.

Κωδικοποίηση Base64
Η κωδικοποίηση Base64 ή 6-bit μπορεί να χρησιμοποιηθεί για τις απαντήσεις TXT records. Ένα TXT record μπορεί να έχει κεφαλαία και πεζά που παρέχουν 52 χαρακτήρες. Οι αριθμοί προσθέτουν άλλους 10. Εάν προσθέσουμε άλλους δύο χαρακτήρες όπως "-" και "+", έχουμε έπειτα 64 μοναδικές τιμές που μπορούν να χρησιμοποιηθούν για την κωδικοποίηση Base-64. Παρόμοια με το Base32 κωδικοποιημένο αίτημα, η απάντηση μπορεί να κωδικοποιηθεί 6 μπιτ τη φορά χρησιμοποιώντας μια TXT απάντηση και να σταλεί πίσω στον client.

Κωδικοποίηση Binary (8 bit)
Η δυαδική οκτάμπιτη κωδικοποίηση μπορεί να χρησιμοποιηθεί αν και δεν δουλεύει με κάθε DNS server. Σε κάποιες περιπτώσεις λοιπόν, μπορεί επιτυχώς να χρησιμοποιηθούν 8 μπιτ ανά χαρακτήρα για κωδικοποίηση. Αυτή η κωδικοποίηση υποστηρίζει μεγαλύτερο ρυθμό μεταφοράς δεδομένων στο tunnel (Revelli, 2009). Το Iodine χρησιμοποιεί τον τύπο NUll record για τις απαντήσεις στον client και χρησιμοποιεί την οκτάμπιτη κωδικοποίηση.

Κωδικοποίηση NetBIOS
Η κωδικοποίηση NetBIOS είναι μια άλλη μέθοδος που έχει χρησιμοποιηθεί για την κωδικοποίηση των δεδομένων. Για την κωδικοποίηση NetBIOS, κάθε ψηφιολέξη (byte) είναι χωρισμένη σε 4 μπιτ. Το δεκαδικό 65 προστίθεται σε κάθε ένα τέτοιο μπιτ. Κάθε ψηφιολέξη (byte) έπειτα κωδικοποιείται σε δύο χαρακτήρες σε μια ετικέτα DNS . Αυτή η μέθοδος χρησιμοποιείται μόνο από το DNScat-B.

Κωδικοποίηση δεκαεξαδικού
Η κωδικοποίηση δεκαεξαδικού είναι μια άλλη μέθοδος κωδικοποίησης. Για την κωδικοποίηση δεκαεξαδικού, οι δύο τιμές του δεκαεξαδικού χαρακτήρα χρησιμοποιούνται για να αντιπροσωπεύσουν κάθε ψηφιολέξη(byte). Αυτή η μέθοδος χρησιμοποιείται μόνο από το DNScat-B.

Τεχνικές
Οι διάφορες υλοποιήσεις DNS tunneling που υπάρχουν χρησιμοποιούν διαφορετικούς τύπους DNS record και μεθόδους κωδικοποίησης. Πολλές φορές κάποιες επιπλέον τεχνικές υλοποίησης χρησιμοποιούνται που αξίζουν την αναφορά. Σε ορισμένες περιπτώσεις όπως το Iodine, η υλοποίηση θα εντοπίσει αυτόματα την καλύτερη δυνατή κωδικοποίηση.
Άλλες υλοποιήσεις DNS tunneling χρησιμοποιούν το EDNS που τους επιτρέπει να έχουν payloads μεγαλύτερα από 512 bytes και με αυτόν τον τρόπο να βελτιώσουν την απόδοση τους. Μια υλοποίηση DNS tunneling,το Heyoka κλέβει και χρησιμοποιεί τις διευθύνσεις IP των αποστολέων για τα DNS αιτήματα στον server (upstream) ώστε να κάνει τον client αόρατο.

4.4 Γνωστές υλοποιήσεις DNS tunneling

Υπάρχουν πολλές διαφορετικές υλοποιήσεις DNS tunneling. Συνοψίζονται εδώ.

4.4.1 DeNiSe

Το DeNiSe είναι μια απόδειξη της υλοποίησης tunnel του πρωτοκόλλου TCP μέσω του DNS σε Python. Έχει έξι python scripts μεταξύ του 2002 και του 2006 (mdornseif, 2002).

4.4.2 dns2tcp

Το dns2tcp γράφτηκε από τον Olivier Dembour και το Nicolas Collignon. Γράφτηκε σε Cand και τρέχει σε Linux. Ο client μπορεί να τρέξει σε Windows. Υποστηρίζει τους τύπους αιτημάτων KEY και TXT (Dembour, 2008).

4.4.3 DNScapy

Το DNScapy αναπτύχθηκε από τον Pierre Bienaime. Χρησιμοποιεί Scapy για την δημιουργία των πακέτων του. Το DNScapy υποστηρίζει το SSH tunneling μέσω του DNS συμπεριλαμβανομένου ενός πληρεξούσιου server Socks. Μπορεί να διαμορφωθεί ώστε να χρησιμοποιήσει τους τύπους CNAME ή TXT record ή και τους δύο τυχαία (Bienaime, 2011)

4.4.4 DNScat (DNScat-P)

Το DNScat (DNScat-P) κυκλοφόρησε αρχικά το 2004 και η πιο πρόσφατη έκδοση του το 2005. Γράφτηκε από τον Tadeusz Pietraszek. Το DNScat παρουσιάστηκε ως εργαλείο με πολλές χρήσεις που περιλαμβάνουν και την αμφίδρομη επικοινωνία μέσω του DNS. Το DNScat βασίζεται στην Java και τρέχει σε συστήματα παρόμοια με τα Unix. Το DNScat υποστηρίζει αιτήματα τύπου A και CNAME record (Pietraszek, 2004). Δεδομένου ότι υπάρχουν δύο εφαρμογές που ονομάζονται DNScat, αυτή εδώ θα αναφέρεται ως DNScat-P για να διακρίνεται από την άλλη.

4.4.5 DNScat (DNScat-B)

Το DNScat (DNScat-β) γράφτηκε από τον Ron Bowes. Η παλαιότερη γνωστή κυκλοφορία ήταν το 2010. Τρέχει σε Linux, σε Mac OS X και σε Windows.
Το DNScat θα κωδικοποιήσει τα αιτήματα είτε σε NetBIOS κωδικοποίηση είτε σε δεκαεξαδική κωδικοποίηση . Το DNScat μπορεί να χρησιμοποιήσει τους τύπους A, AAAA, CNAME, NS, TXT και του MX record. Παρέχει δύο τύπους λειτουργίας, datagram και stream. Υπάρχει επίσης ένα DNScat-B βασισμένο στο Metasploit payload (Bowes, 2010).

4.4.6 Heyoka

Το Heyoka είναι μια έμπρακτη απόδειξη της δημιουργίας ενός αμφίδρομου tunnel για την υποκλοπή στοιχείων. Αυτό το εργαλείο έχει γραφτεί σε C και έχει δοκιμαστεί σε Windows. Το Heyoka αναπτύχθηκε από τον Alberto Revelli και το Nico Leidecker. Χρησιμοποιεί δυαδικά στοιχεία αντί των 32 ή των εξηντατετράμπιτων κωδικοποιημένων στοιχείων για να αυξήσει το ρυθμό μεταφοράς δεδομένων. Χρησιμοποιεί επίσης EDNS για να επιτρέψει τα μηνύματα μεγαλύτερα από 512 bytes. Το Heyoka χρησιμοποιεί επίσης παραλλαγή της πηγής των πακέτων για να την κάνει μη ορατή και να φαίνεται ότι τα αιτήματα έχουν προέλθει από πολλές διευθύνσεις IP. (Revelli, 2009).

4.4.7 Iodine

Το Iodine είναι ένα πρόγραμμα DNS tunneling που κυκλοφόρησε πρώτα το 2006 με αναπροσαρμογές μέχρι πρόσφατα ως το 2010. Αναπτύχθηκε από τον Bjorn Andersson και τον Erik Ekman. Το Iodine γράφτηκε σε Cand και τρέχει σε Linux, σε Mac OS X, σε Windows και άλλα. Το Iodine είναι προσανατολισμένο και σε Android. Χρησιμοποιεί μια tun ή tap διεπαφή στην τελική συσκευή (Andersson, 2010).

4.4.8 NSTX

Το NSTX (Nameserver Transfer Protocol) από τον Florian Heinz και τον Julien Oster κυκλοφόρησε το 2000. Τρέχει μόνο σε Linux.Το NSTX καθιστά δυνατή την δημιουργία IP tunnels χρησιμοποιώντας το DNS (NSTX, 2002).
Περνάει την κυκλοφορία χρησιμοποιώντας είτε tun είτε tap διεπαφή στην τελική συσκευή.

4.4.9 OzymanDNS

Το OzymanDNS γράφτηκε σε Perl από τον Dan Kaminsky το 2004. Χρησιμοποιείται για να στηθεί ένα SSH tunnel μέσω DNS ή για τη μεταφορά αρχείων. Τα αιτήματα είναι base32 κωδικοποιημένα και οι απαντήσεις είναι κωδικοποιημένες base64 τύπου TXT record.

4.4.10 Psudp

Το psudp αναπτύχθηκε από τον Kenton Born. Εγχέει τα δεδομένα στα υπάρχοντα DNS αιτήματα με την τροποποίηση του μήκους του πακέτου IP/UDP. Απαιτεί ότι όλοι οι χρήστες που συμμετέχουν στο συγκεκαλυμμένο δίκτυο στέλνουν τα DNS αιτήματα τους σε μια "ενδιάμεση" υπηρεσία που μπορεί να κρατήσει τα μηνύματα για ένα συγκεκριμένο χρήστη έως ότου ένα DNS αίτημα να ζητηθεί από εκείνον τον χρήστη. Το μήνυμα μπορεί έπειτα να σταλεί μέσα στην DNS απάντηση (Born, 2010a).

4.4.11 Squeeza

Το Squeeza είναι ένα εργαλείο SQL injection. Χωρίζεται στο κανάλι εντολών και στο κανάλι υποκλοπής δεδομένων. Το κανάλι εντολών μπορεί να χρησιμοποιηθεί για να δημιουργήσει μια βάση δεδομένων για τα δεδομένα και να εκτελεί άλλες εντολές. Υποστηρίζει τρία κανάλια υποκλοπής δεομένων: HTTP λαθών, συγχρονισμού και DNS. (Haroon, 2007).

4.4.12 tcp-over-dns

Το TCP-overdns κυκλοφόρησε το 2008. Έχει ένα server στημένο σε Java και ένα client επίσης σε Java. Τρέχει στα Windows,τα Linux και Solaris. Υποστηρίζει τη συμπίεση LZMA και την κυκλοφορία TCP και UDP (Analogbit, 2008).

4.4.13 TUNS

Το TUNS αναπτύχθηκε από τον Lucas Nussbaum. Το TUNS έχει γραφτεί σε Ruby. Δεν χρησιμοποιεί πειραματικούς ή σπάνια χρησιμοποιημένους τύπους record. Χρησιμοποιεί μόνο records CNAME. Αυτό ρυθμίζει το MTU που χρησιμοποιείται σε 140 χαρακτήρες για να ταιριάξει με τα δεδομένα σε ένα DNS αίτημα. Το TUNS ίσως είναι πιο δύσκολο να ανιχνευτεί, αλλά χάνει σε κόστος απόδοσης (Nussbaum, 2009).

4.4.14 Malware μέσω DNS

Το DNS έχει χρησιμοποιηθεί ως μέθοδος επικοινωνίας από τα κακόβουλα λογισμικά (malware). Γνωστά κακόβουλα λογισμικά που χρησιμοποιούν το DNS είναι: το Feederbot (Dietrich, 2011) και το Moto (Mullaney, 2011). Και τα δύο από τα παραπάνω χρησιμοποιούν τον τύπο DNS TXT record για εντολές και έλεγχο.

4.5 Παρακάμπτοντας την πληρωμένη υπηρεσία Wi-Fi.

Όπως αναφέρθηκε και παραπάνω πολλά από τα εργαλεία για DNS tunneling δημιουργήθηκαν με την πρόθεση να παρακάμψουν τα captive portals για την πληρωμένη υπηρεσία Wi-Fi. Εάν ένα από αυτά τα συστήματα επιτρέπει την DNS κυκλοφορία, ένα DNS tunnel μπορεί να στηθεί για να ανοίξει την κυκλοφορία IP χωρίς πληρωμή για την υπηρεσία.

4.5.1 Captive Portals

Η τεχνική captive portal αναγκάζει έναν πελάτη HTTP σε ένα δίκτυο να δει μια ειδική ιστοσελίδα (συνήθως για λόγους επικύρωσης) πριν αποκτήσει πρόσβαση στο Διαδίκτυο. Το captive portal μετατρέπει τον εξυπηρετητή Ιστού (Web Browser) σε συσκευή επικύρωσης (authentication). Αυτό γίνεται με την παρεμπόδιση όλων των πακέτων, ανεξάρτητα από την διεύθυνση IP ή από την πόρτα, έως ότου ο χρήστης ανοίξει έναν εξυπηρετητή και προσπαθήσει να αποκτήσει πρόσβαση στο Διαδίκτυο. Εκείνη τη στιγμή ο εξυπηρετητής εμφανίζει μια ιστοσελίδα που μπορεί να απαιτήσει επικύρωση ή και την πληρωμή, ή να επιδείξει απλά μια αποδεκτή πολιτική χρήσης και να απαιτήσει από το χρήστη να συμφωνήσει. Τα captive portals χρησιμοποιούνται χαρακτηριστικά από εμπορικά κέντρα, αερολιμένες, λόμπι ξενοδοχείων, καφετερίες και άλλους τόπους συναντήσεως που προσφέρουν ελεύθερα σημεία Wi-Fi για τους χρήστες του Ίντερνετ.

Υπάρχουν περισσότεροι από έναν τρόποι να εφαρμοστεί ένα captive portal.

- HTTP redirection: Εάν ένας μη επικυρωμένος χρήστης ζητήσει έναν ιστοχώρο, το DNS ρωτιέται από τον εξυπηρετητή του χρήστη και η αρμόδια IP λαμβάνεται για εκείνον τον ιστοχώρο. Ο εξυπηρετητής στέλνει έπειτα ένα αίτημα HTTP σε εκείνη την διεύθυνση IP. Αυτό το αίτημα, εντούτοις, παρεμποδίζεται από το firewall και διαβιβάζεται σε έναν redirect server. Αυτός ο server αποκρίνεται με μια κανονική απάντηση HTTP που περιέχει τον κώδικα θέσης HTTP 302 για να παραπέμψει τον χρήστη στο captive portal. Αυτή η διαδικασία δεν γίνεται αντιληπτή από τον χρήστη.

- IP redirection: Το αίτημα παραπέμπεται στο επίπεδο layer 3 (IP) από το firewall.

- DNS redirection: Όλα τα αιτήματα DNS απαντώνται από τον τοπικό DNS server στο ασύρματο δίκτυο και η απάντηση είναι πάντα η διεύθυνση IP του captive portal.

Υπάρχουν ωστόσο πολλοί τρόποι να παρακαμφθεί ένα captive portal. Για παράδειγμα πολλά captive portals επικυρώνουν τους χρήστες βασιζόμενα στην IP/MAC διεύθυνση τους. Είναι όμως εύκολο για έναν επιτιθέμενο να υποδυθεί έναν επικυρωμένο χρήστη κλέβοντας την IP/MAC διεύθυνση του.

Ένας άλλος τρόπος είναι το DNS tunneling! Όμως δεν μπορούν όλες οι υλοποιήσεις captive portal να παρακαμφθούν. Εάν ένα captive portal χρησιμοποιεί DNS redirection το Dns tunneling δεν μπορεί να χρησιμοποιηθεί.

4.5.2 Iodine

Το Iodine επιτρέπει να περάσει κίνηση IPv4 μέσω ενός DNS server. Αυτό μπορεί να είναι χρήσιμο σε διάφορες καταστάσεις όπου η πρόσβαση στο Διαδίκτυο παρεμποδίζεται από ένα firewall, αλλά τα αιτήματα DNS επιτρέπονται. Το όνομα Iodine επιλέχτηκε δεδομένου ότι αρχίζει με "IOD" (IP over DNS) και δεδομένου ότι το ιώδιο έχει τον ατομικό αριθμό 53, ο οποίος τυχαίνει να είναι ο ίδιος με τον αριθμό της πόρτας για το DNS. Τρέχει σε λειτουργικά Linux, Mac OS X, FreeBSD, NetBSD, OpenBSD και Windows και χρειάζεται μια TUN/TAP συσκευή . Ο ρυθμός μεταφοράς δεδομένων είναι ασύμμετρος με περιορισμένη ροή προς τα πάνω και μέχρι 1 Mbit/s προς τα κάτω.

Σε σύγκριση με τις άλλες εφαρμογές DNS tunneling, το Iodine προσφέρει:

- ✓ Υψηλότερη απόδοση

Το Iodine χρησιμοποιεί τον τύπο NULL record που επιτρέπει στα δεδομένα, στη ροή downstream ,να σταλούν χωρίς κωδικοποίηση. Κάθε DNS απάντηση μπορεί να περιέχει πάνω από ένα kilobyte συμπιεσμένων στοιχείων.

- ✓ Φορητότητα

Το Iodine μπορεί να λειτουργήσει σε πολλά διαφορετικά συστήματα τύπου Unix καθώς επίσης και σε Win32. Το tunnel μπορεί να στηθεί μεταξύ δύο χρηστών ανεξάρτητα από το endianness ή το λειτουργικό τους σύστημα.

- ✓ Ασφάλεια

Το Iodine χρησιμοποιεί login που εξασφαλίζεται από MD5 hash. Επίσης φιλτράρει οποιαδήποτε πακέτα δεν προέρχονται από την IP που χρησιμοποιήθηκε κατά το Login.

- ✓ Ευκολία κατά το στήσιμο

Το Iodine χειρίζεται αυτόματα την ανάθεση των διευθύνσεων IP στα interfaces και μέχρι 16 χρήστες μπορούν να μοιραστούν έναν server συγχρόνως. Στο downstream το μέγεθος των πακέτων εξετάζεται αυτόματα για τη μέγιστη απόδοση.

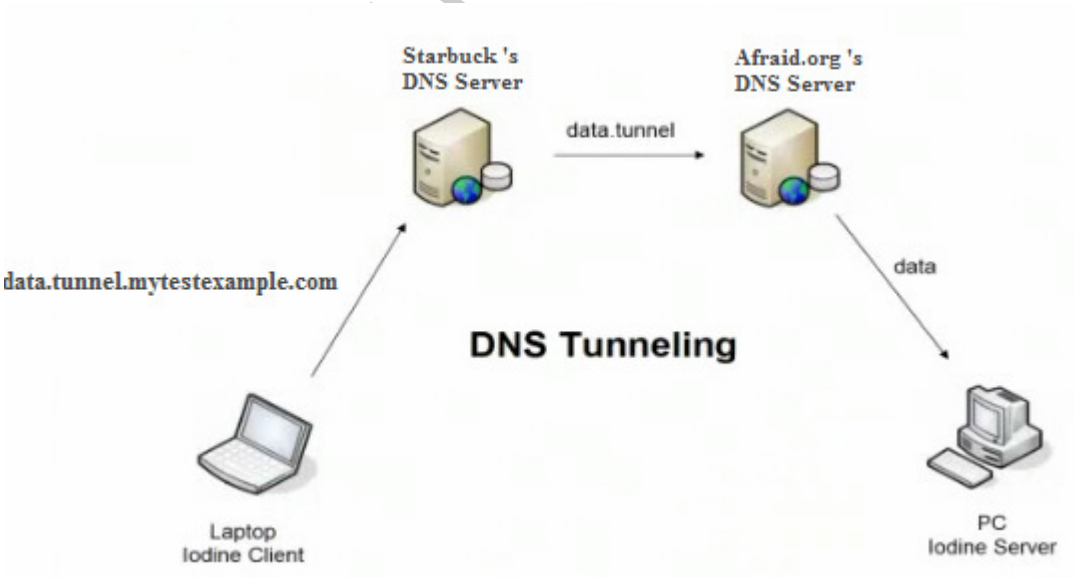
Το Iodine θα αποτελέσει το εργαλείο με το οποίο θα στηθεί το DNS tunnel προκειμένου να παρακαμφθεί η πληρωμένη υπηρεσία παρακάτω.

4.5.3 Η Επίθεση

Για την πραγματοποίηση της επίθεσης χρησιμοποιήθηκαν τα παρακάτω:

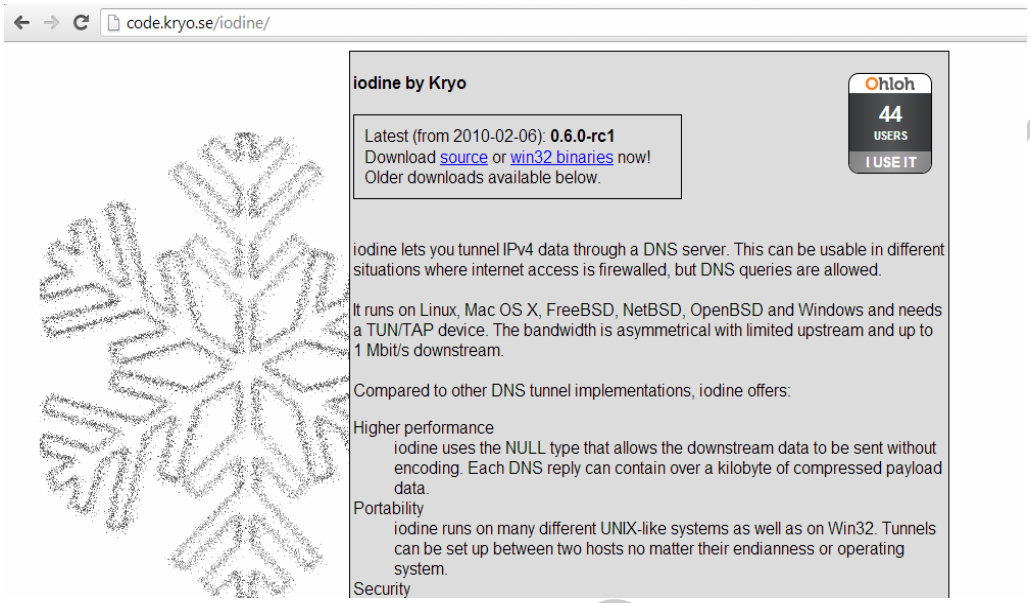
- ένας φορητός υπολογιστής με λειτουργικό σύστημα windows (iodine client)
- ένας σταθερός υπολογιστής με λειτουργικό σύστημα windows και με πρόσβαση στο Διαδίκτυο (iodine server)
- η κατοχή και ο έλεγχος ενός domain name
- το πρόγραμμα για DNS tunneling, iodine και πιο συγκεκριμένα η έκδοση iodine-0.6.0-rc1-win32 για το λειτουργικό σύστημα windows
- το πρόγραμμα MinGW 5.1.4 για συμβατότητα
- το πρόγραμμα OpenVPN 2.0.9 για την δημιουργία του TAP/TUN interface
- ένα Captive Portal !

Τα περισσότερα Hotspots δεν εμποδίζουν την κυκλοφορία μεταξύ του DNS server τους και των υπολογιστών που έχουν εισέλθει στο δίκτυο τους. Έτσι υπάρχει η δυνατότητα για πρόσβαση στο Διαδίκτυο μέσω της DNS κυκλοφορίας επηρεάζοντας τον DNS server να παρακάμψει τις λίστες ελέγχου πρόσβασης.
Ο DNS server που θα χρησιμοποιηθεί είναι ο Iodine σε έναν κεντρικό υπολογιστή. Ο υπολογιστής αυτός θα πρέπει να βρίσκεται σε ένα δίκτυο εκτός του ασύρματου Hotspot που πραγματοποιείται η επίθεση και να είναι προσπελάσιμος από το Διαδίκτυο.

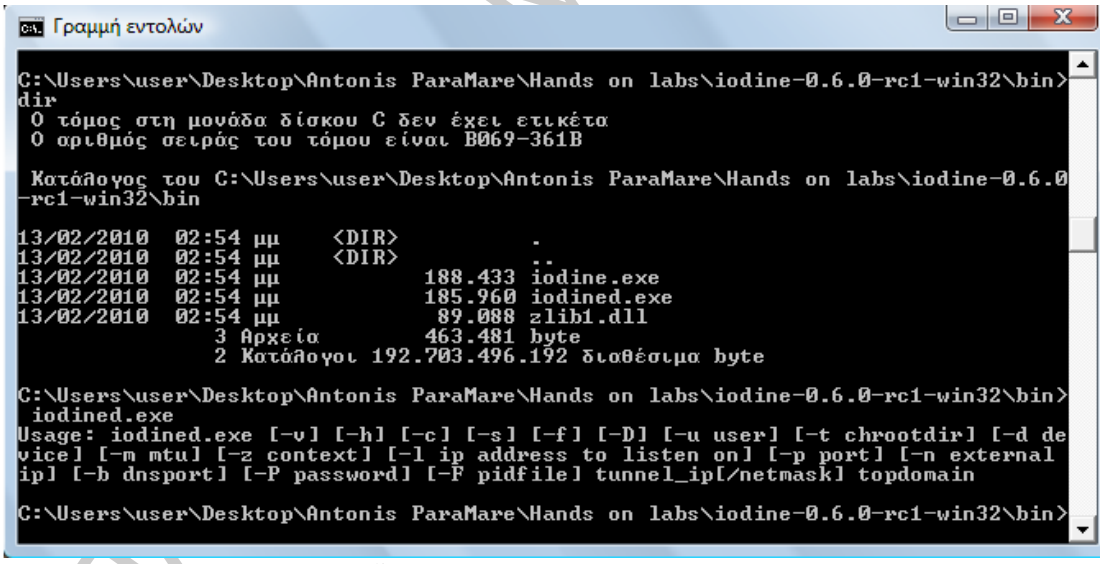


Εικόνα 38. DNS Tunneling

Στον υπολογιστή αυτό που θα έχει τον ρόλο του server γίνεται εγκατάσταση του λογισμικού Iodine Server.



Εικόνα 39. Η εφαρμογή Iodine για DNS tunneling.

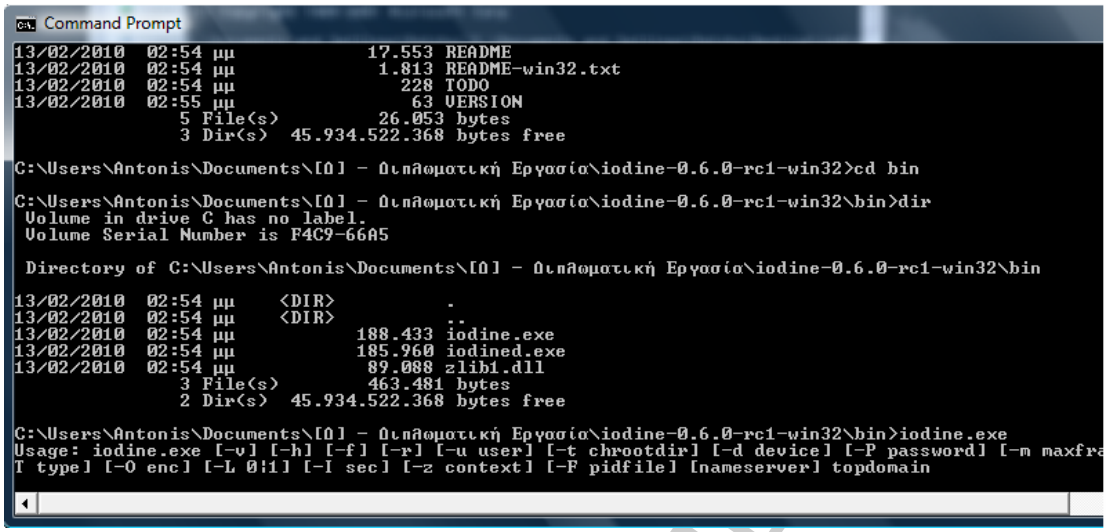


Εικόνα 40. Η εγκατάσταση του Iodine Server.

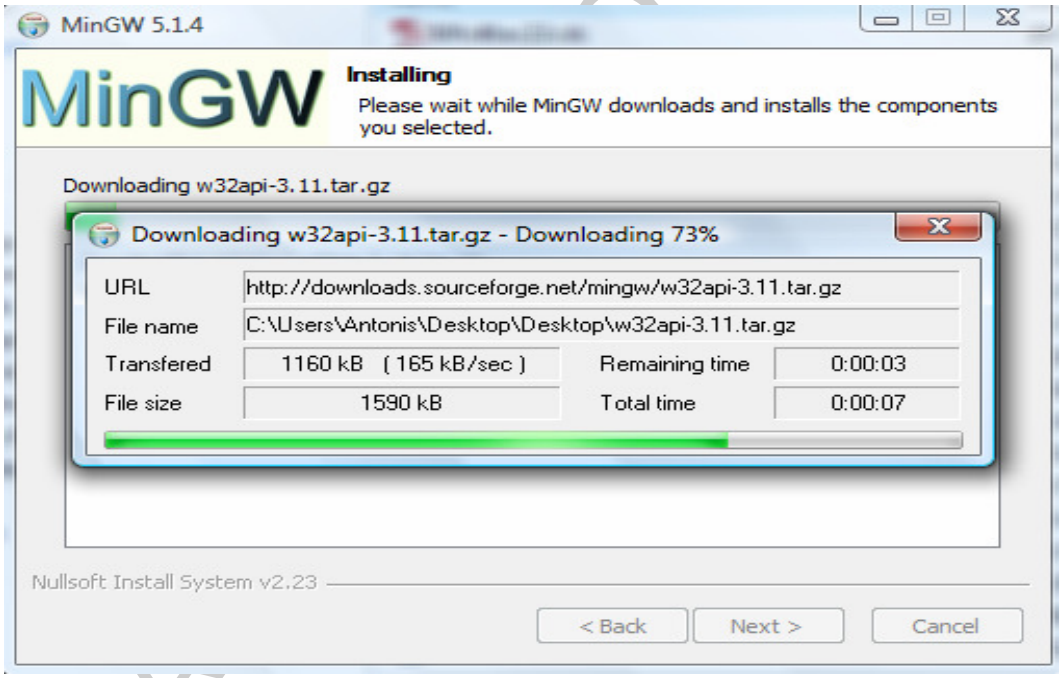
Ο υπολογιστής αυτός χαρακτηρίζεται ως "iodined" από το iodine deamon που θα τρέχει προκειμένου να δημιουργηθεί το DNS tunnel.

Στον υπολογιστή που βρίσκεται στο Hotspot και προσπαθεί να αποκτήσει παράνομη πρόσβαση στο Διαδίκτυο παρακάμπτοντας την πληρωμένη υπηρεσία και που έχει το

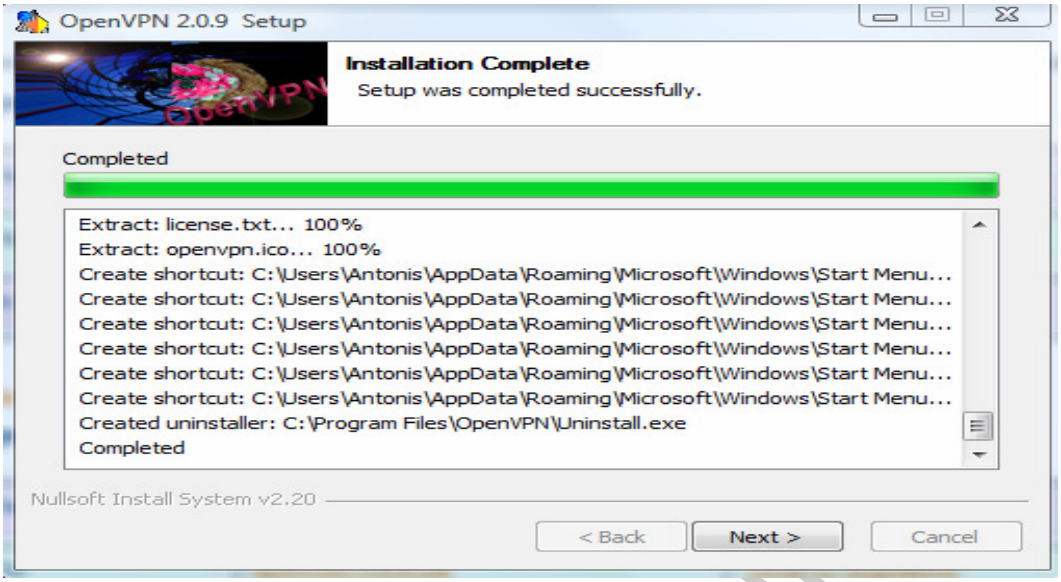
ρόλο του Iodine Client θα πρέπει να εγκατασταθούν τα παρακάτω προγράμματα. Ο υπολογιστής αυτός χρησιμοποιεί λειτουργικό σύστημα Windows.



Εικόνα 41. Εγκατάσταση του Iodine Client.

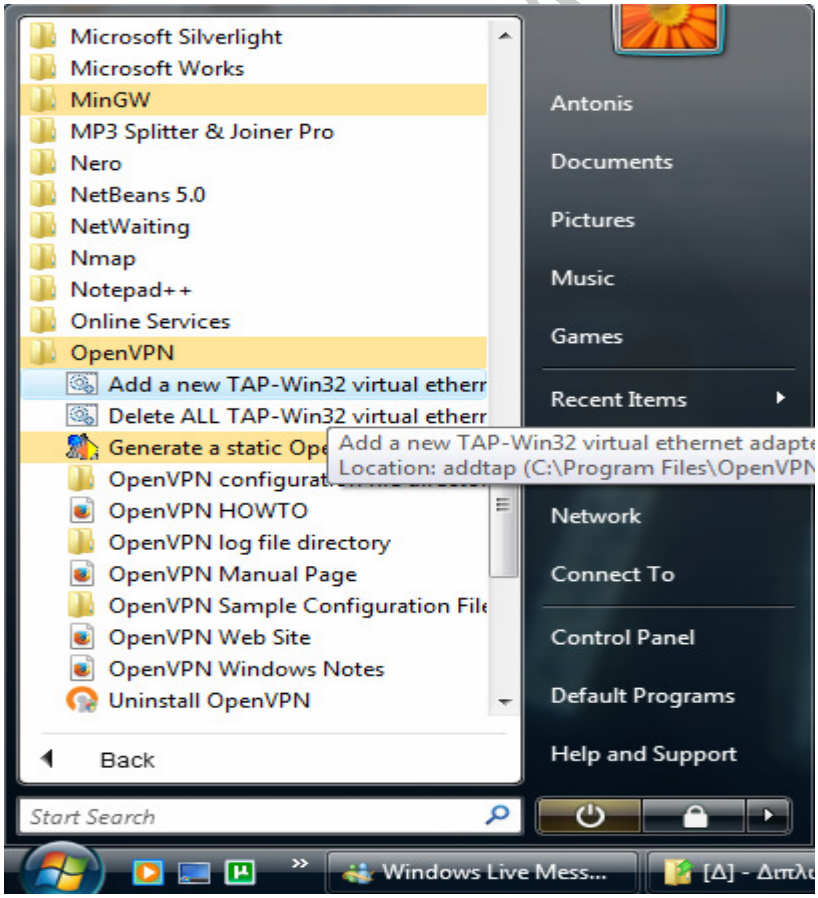


Εικόνα 42. Εγκατάσταση του προγράμματος MinGW.

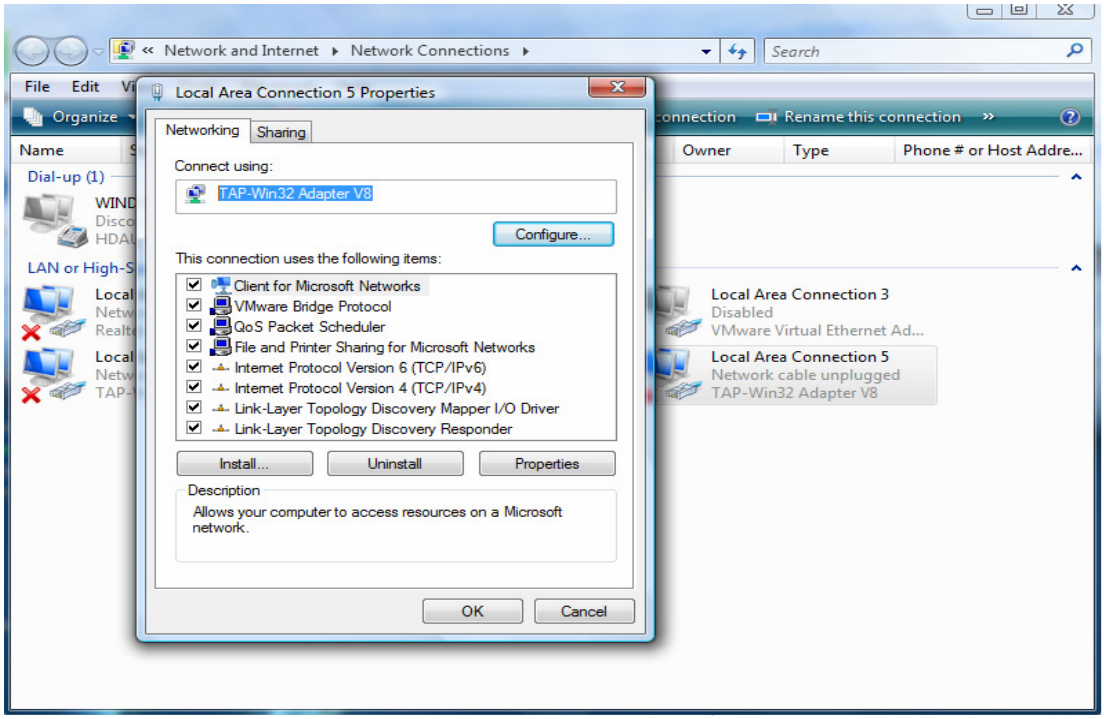


Εικόνα 43. Εγκατάσταση του προγράμματος OpenVpn.

Το πρόγραμμα OpenVpn θα χρησιμοποιηθεί για την δημιουργία ενός Tap Interface απαραίτητο για την λειτουργία του Iodine. Όπως παρουσιάστηκε παραπάνω σε προηγούμενη ενότητα το Iodine για να λειτουργήσει χρειάζεται μία TAP/TUN συσκευή.

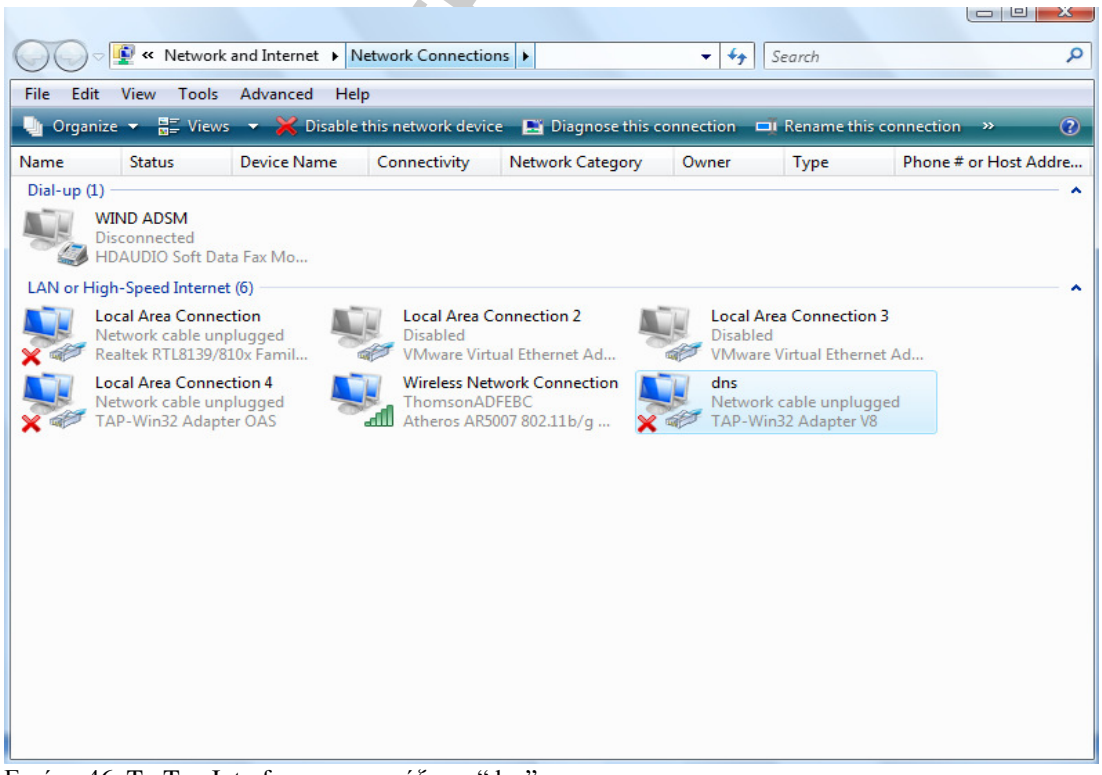


Εικόνα 44. Δημιουργία ενός TAP-Win32 interface με το OpenVpn.



Εικόνα 45. Το TAP Interface έχει δημιουργηθεί.

Αφού το Tap Interface έχει δημιουργηθεί το μετονομάζουμε “dns” έτσι ώστε το Iodine να γνωρίζει ποιο interface να χρησιμοποιήσει.

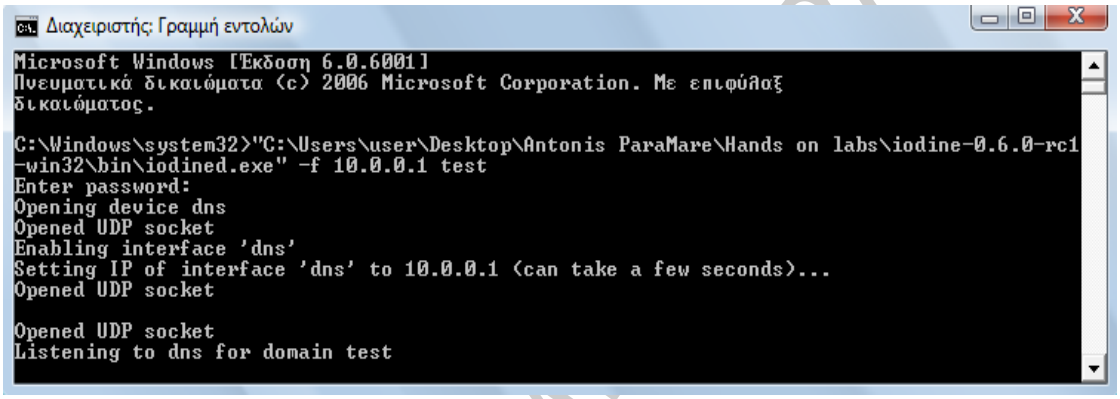


Εικόνα 46. Το Tap Interface μετονομάζεται “dns”.

Αφού έχει γίνει η εγκατάσταση των απαραίτητων προγραμμάτων τόσο στον client όσο και στον server θα πρέπει να γίνει μία δοκιμή στο τοπικό δίκτυο ώστε να επιβεβαιωθεί η ορθή λειτουργία.
Στον υπολογιστή που έχει το ρόλο του Iodine Server εκτελείται η εντολή:

./ iodined -f 10.0.0.1 test

Με την εντολή αυτή ξεκινάει να τρέχει ο iodine deamon. Το δίκτυο 10.0.0.0 που έχει επιλεχθεί για το tunnel μπορεί να είναι οποιοδήποτε δίκτυο αρκεί να μην χρησιμοποιείται από κάποιο άλλο interface του υπολογιστή.Το domain που χρησιμοποιείται είναι το "test".Όλη η κυκλοφορία που αφορά το domain αυτό θα περάσει μέσα από το tunnel που θα δημιουργηθεί με την μορφή DNS.Μόλις εκτελεστεί η εντολή ένας κωδικός θα ζητηθεί, που θα χρησιμοποιηθεί και στον client.

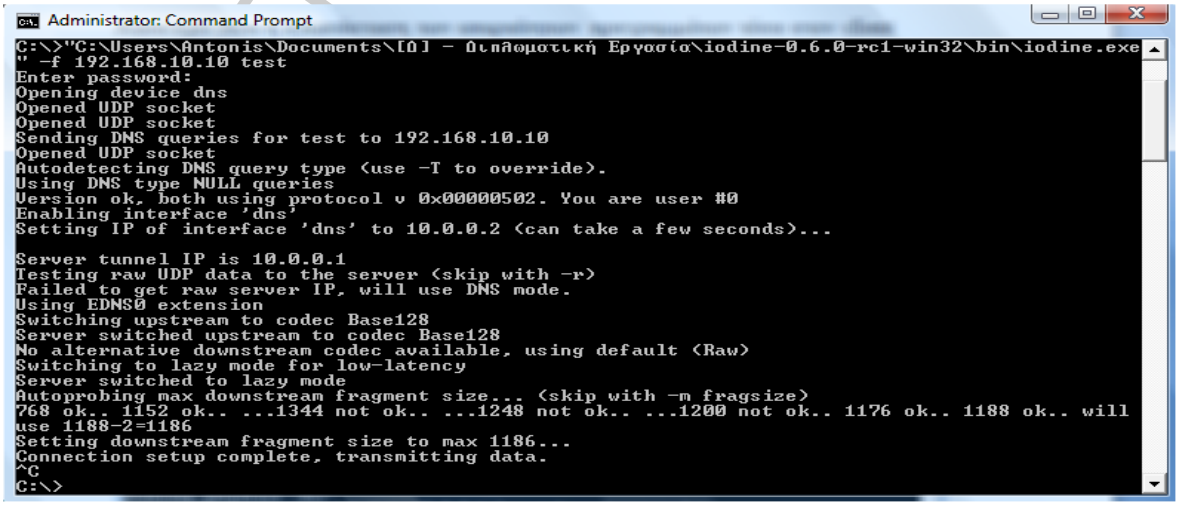


Εικόνα 47. Εκκίνηση του Iodine Server για δοκιμή στο τοπικό δίκτυο.

Στη συνέχεια στον client εκτελείται η εντολή :

./iodine -f 192.168.10.10 test

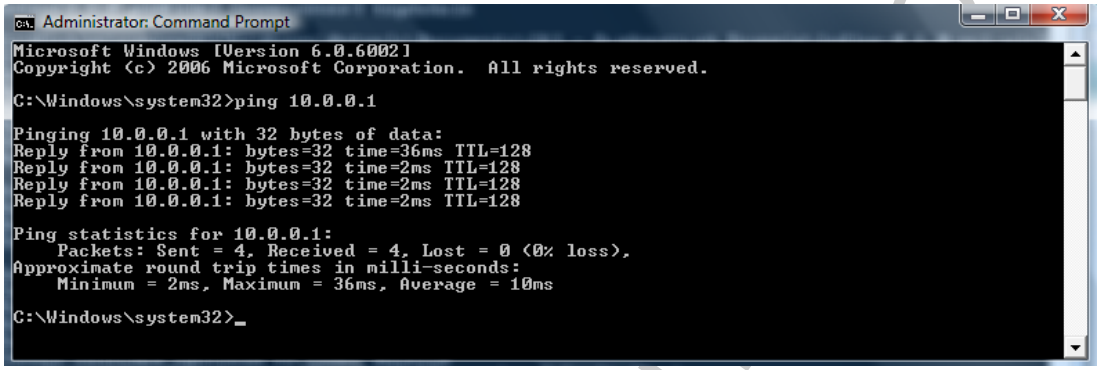
Με την εντολή αυτή ξεκινάει το iodine στον client.Η παραπάνω διεύθυνση IP στην εντολή είναι η πραγματική διεύθυνση IP του iodine server.Ο κωδικός που θα ζητηθεί θα πρέπει να είναι ο ίδιος με τον κωδικό που εισήχθη στον server.



Εικόνα 48. Εκκίνηση του Iodine Client για δοκιμή στο τοπικό δίκτυο.

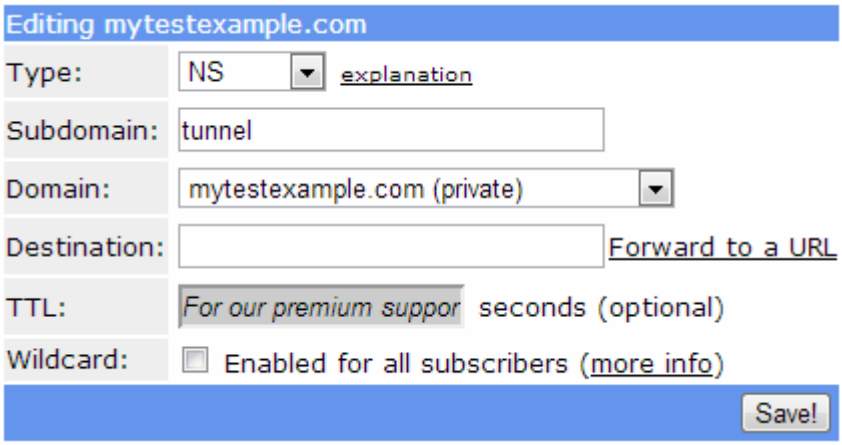
Όπως φαίνεται στην παραπάνω εικόνα 48 το dns tunnel στήνεται δίνοντας στον iodine client τη διεύθυνση IP 10.0.0.2 για το interface “dns”. Ο server θα έχει την διεύθυνση 10.0.0.1 και έτσι το tunnel έχει στηθεί. Στη συνέχεια ορίζεται ο τύπος του DNS record που θα χρησιμοποιηθεί όπου θα είναι “NULL”, η κωδικοποίηση “Base128” και το μέγεθος των πακέτων 1186k.

Για να εξακριβωθεί ότι το tunnel έχει στηθεί και όλα δουλεύουν σωστά μια εντολή ping θα δοθεί στον client με την διεύθυνση tunnel IP του server.

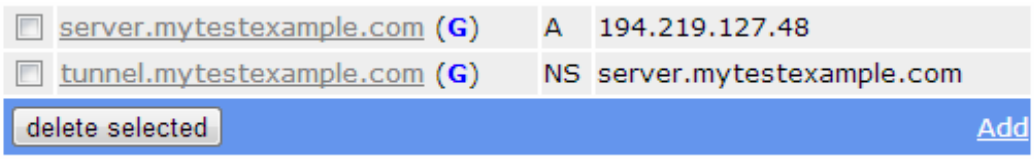


Εικόνα 49. Επικοινωνία Iodine server - Iodine Client.

Αφού όλα λειτουργούν σωστά μπορεί να συνεχιστεί η υλοποίηση της επίθεσης. Για να γίνει όμως αυτό θα χρειαστεί πρόσβαση σε ένα αληθινό domain. Αυτό που χρειάζεται είναι πρόσβαση σ ένα αληθινό domain,στο οποίο μπορούν να δημιουργηθούν νέες εγγραφές Dns ,για τα subdomains ,τύπου NameServer (NS). Επίσης αν ο server δεν έχει στατική διεύθυνση IP , λύση δίνουν οι πάροχοι δυναμικού DNS όπως είναι dyndns.com, freedns.afraid.org κ.α.



Εικόνα 50. Δημιουργία Subdomain tunnel.example.com.



Εικόνα 51. Σύνδεση του Subdomain με την διεύθυνση IP του Iodine server.

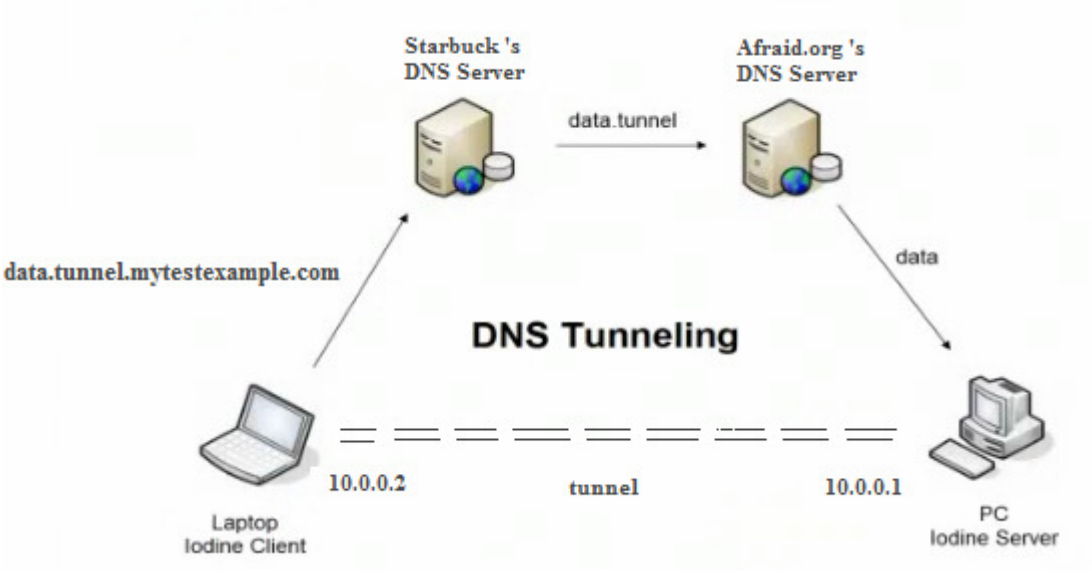
Στις παραπάνω εικόνες 50 και 51 φαίνεται η δημιουργία του subdomain "tunnel.mytestexample.com" στο domain mytestexample.com. Το subdomain "tunnel.mytestexample.com" που είναι τύπου NameServer παραπέμπει στο server.mytestexample.com που είναι τύπου A record και έχει την διεύθυνση IP του υπολογιστή που τρέχει ο Iodine server.

Αυτό σημαίνει ότι οποιοδήποτε αίτημα DNS για το subdomain tunnel.mytestexample.com θα επερωτά για το subdomain server.mytestexample.com. Με αυτόν τον τρόπο μπορούμε να στείλουμε DNS πακέτα από τον ασύρματο υπολογιστή που βρίσκεται στο Hotspot , στο Dns Server του Hotspot και από εκεί στον DNS server του Afraid.org που ελέγχει το domain mytestexample.com και τέλος στον κεντρικό υπολογιστή που τρέχει το Iodine.

Ο Iodine client που τρέχει στον φορητό υπολογιστή και προσπαθεί να αποκτήσει πρόσβαση στο Διαδίκτυο, θα ενθυλακώσει την κίνηση για το Διαδίκτυο μέσα σε DNS αιτήματα. Έτσι τα πακέτα DNS θα έχουν μια δέσμη από κωδικοποιημένα δεδομένα τα data.tunnel.mytestexample.com τα οποία θα σταλούν στον προεπιλεγμένο από το δίκτυο DNS server που στην προκειμένη περίπτωση είναι ο DNS server των Starbucks.Αυτός ο DNS server έχει πληροφορίες για το "mytestexample.com" όμως θα χρειαστεί να πάρει πληροφορίες από τον DNS server του Afraid.org για το subdomain.

Ο DNS server του Afraid.org επερωτά τα αιτήματα στον υπολογιστή που τρέχει ο Iodine Server. Ο Iodine Server θα αποκωδικοποιήσει αυτήν την κίνηση για το Διαδίκτυο θα κάνει αυτό που χρειάζεται να κάνει και θα την στείλει πίσω στον φορητό υπολογιστή!

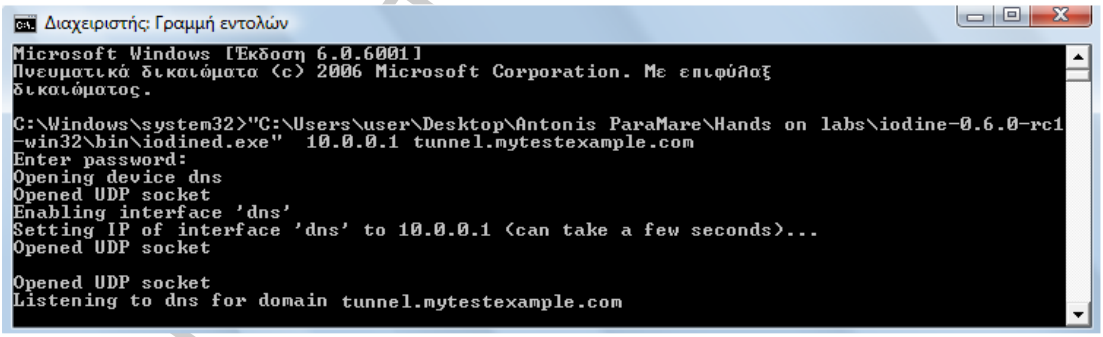
Αυτή είναι η βασική ιδέα για το πώς δουλεύει το DNS tunneling.



Εικόνα 52. DNS Tunneling – Λειτουργία.

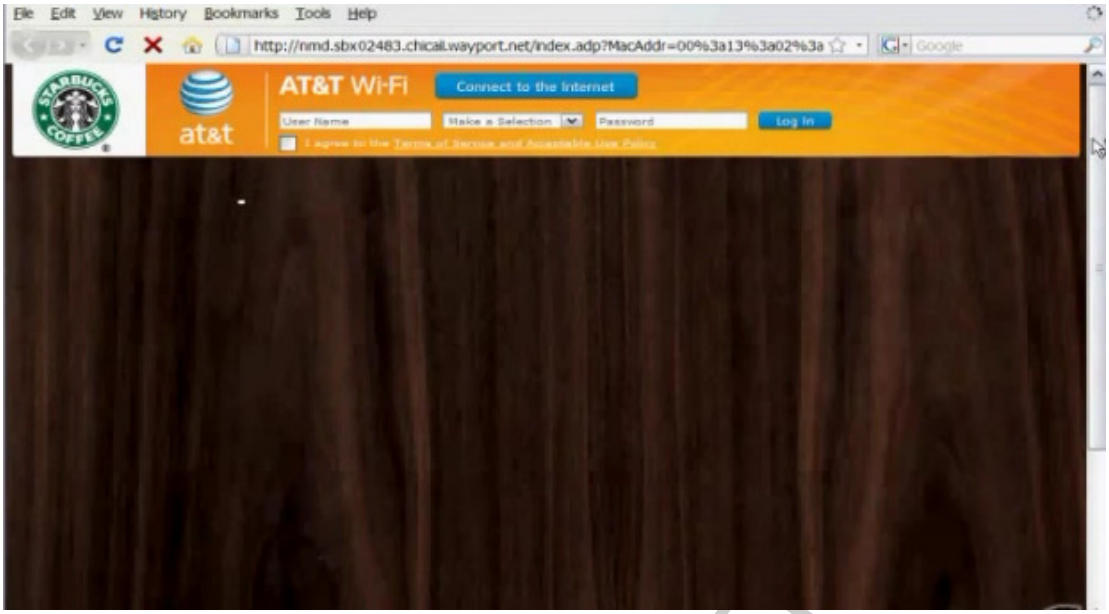
Επαναλαμβάνεται η διαδικασία της δοκιμής που περιγράφηκε παραπάνω για το στήσιμο του DNS tunneling αλλά αυτή την φορά το domain στις εντολές που θα εκτελεστούν θα είναι αληθινό. Για τον iodine server η εντολή που θα εκτελεστεί θα είναι :

./ iodined 10.0.0.1 tunnel.mytestexample.com



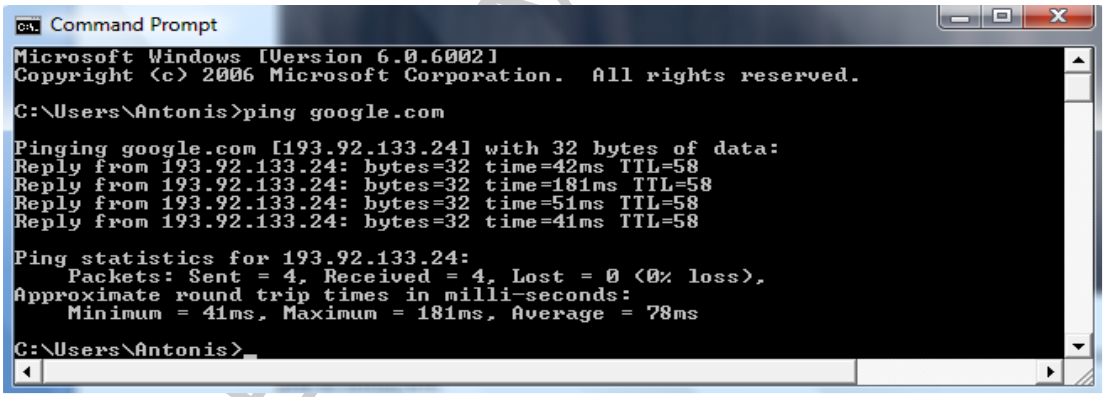
Εικόνα 53. Εκκίνηση του Iodine Server.

Ο Iodine Server έχει τώρα στηθεί και παραμετροποιηθεί και βρίσκεται σε αναμονή. Έπειτα από τον φορητό υπολογιστή που βρίσκεται στο Hotspot ανοίγεται ένας περιηγητής Διαδικτύου και επιχειρείται επίσκεψη σε μια ιστοσελίδα. Το αποτέλεσμα θα είναι το captive portal του Starbucks όπου ζητείται πληρωμή για την πρόσβαση όπως φαίνεται και στην εικόνα 54.



Εικόνα 54. Starbuck' s captive portal.

Τώρα θα πρέπει να εξεταστεί εάν η DNS κίνηση επιτρέπεται. Γι αυτό θα γίνει ping σε μία ιστοσελίδα.

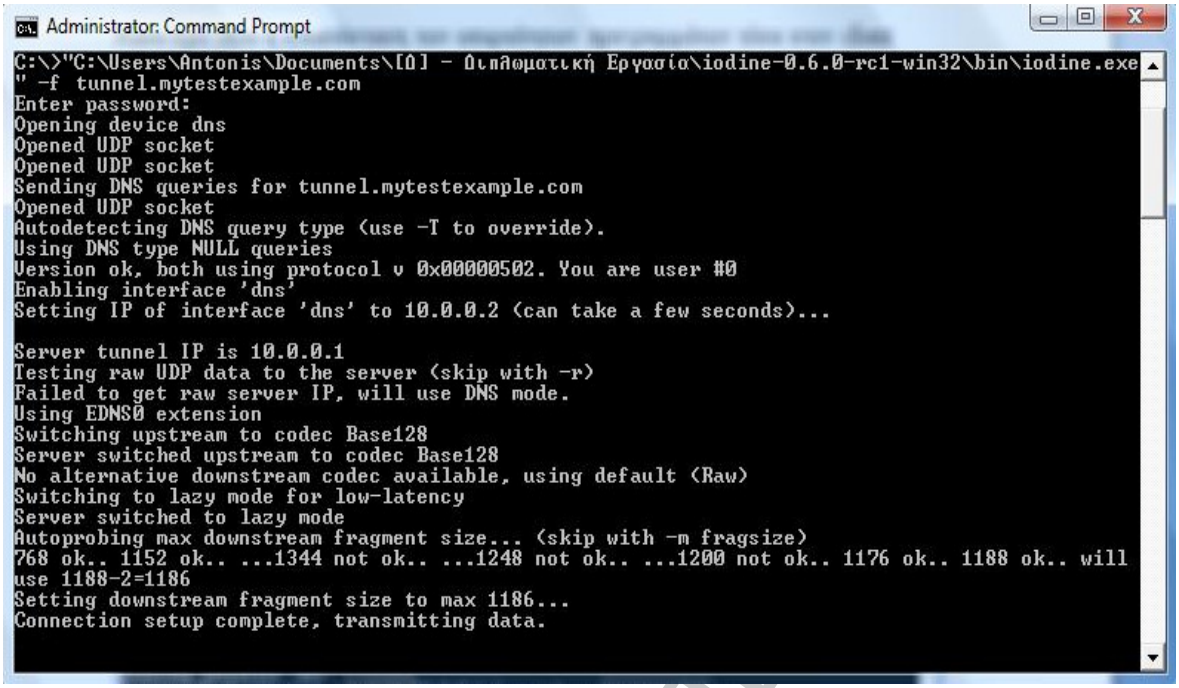


Εικόνα 55. Η DNS κίνηση επιτρέπεται.

Στην εικόνα 55 φαίνεται στην πρώτη γραμμή του αποτελέσματος η ιστοσελίδα που ζητήθηκε και δίπλα η διεύθυνση IP της. Αυτό σημαίνει ότι με τη βοήθεια του DNS server ανακτήθηκε η διεύθυνση IP για την ιστοσελίδα www.google.com και συνεπώς τα DNS αιτήματα επιτρέπονται.

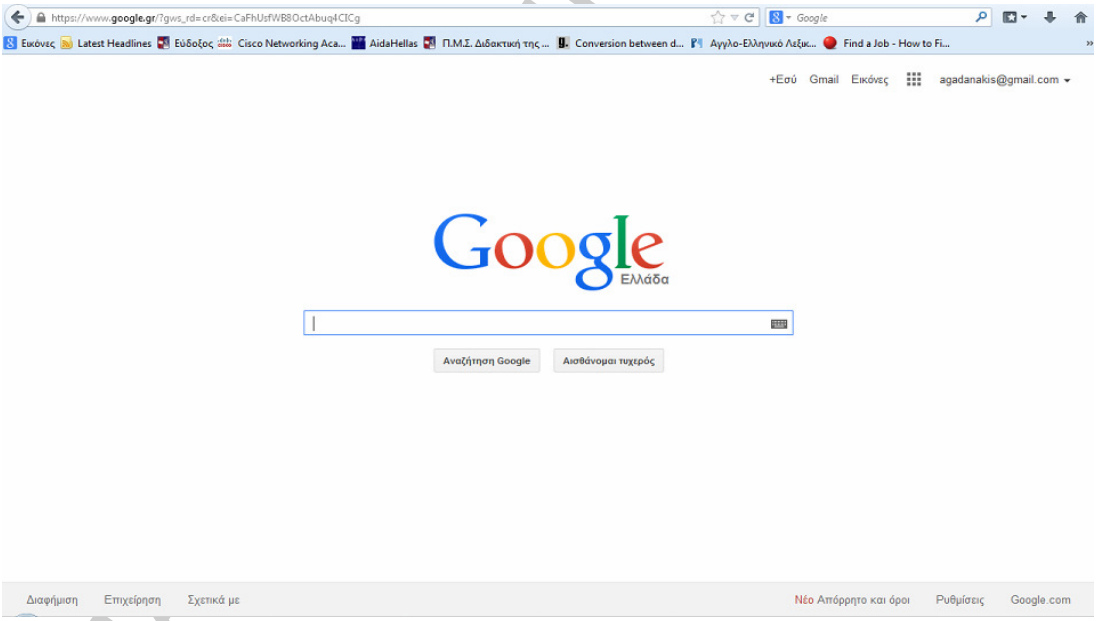
Τώρα μπορεί να χρησιμοποιηθεί ο iodine client για να συνδεθεί στο dns tunnel. Η εντολή που θα εκτελεστεί θα είναι :

./ Iodine –f tunnel.mytestexample.com



Εικόνα 56. Σύνδεση του Iodine client με τον Iodine server.

Το DNS tunnel έχει στηθεί και είναι έτοιμο για την μεταφορά δεδομένων. Ο φορητός υπολογιστής μπορεί πλέον να έχει πρόσβαση στο Διαδίκτυο παρακάμπτοντας το Captive portal του Starbucks.

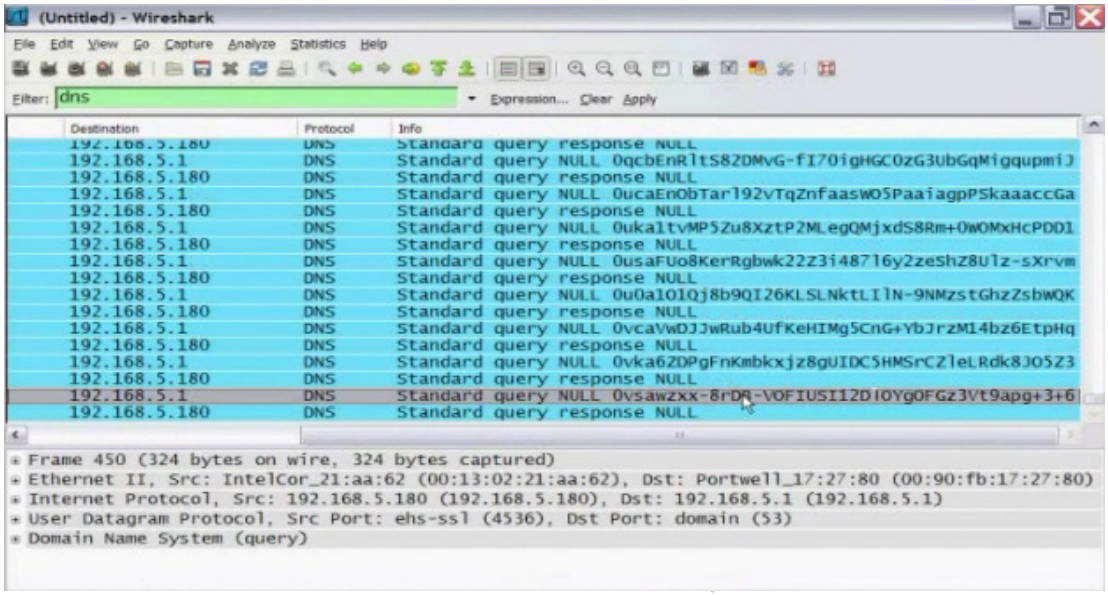


Εικόνα 57. Επιτυχής παράκαμψη του Captive Portal και σύνδεση στο Internet.

Η σύνδεση δεν είναι πολύ γρήγορη, υπάρχει καθυστέρηση. Αυτό οφείλεται στο tunneling και είναι αναμενόμενο. Είναι όμως αρκετή και ικανή για κάποιον που θέλει να κάνει ένα απλό σερφάρισμα στο Διαδίκτυο ή και να ελέγξει τα email του.

Τρέχοντας το Wireshark ένα εργαλείο παρακολούθησης της κίνησης, σε κάθε interface του υπολογιστή και επιλέγοντας το ασύρματο interface θα παρατηρήσουμε

ότι στην κίνηση συμπεριλαμβάνεται μεγάλος όγκος DNS queries-responses αποτέλεσμα του Dns Tunnel που δημιουργήθηκε. Όλη πλέον η κίνηση από τον φορητό υπολογιστή προς το Διαδίκτυο περνάει με την μορφή των DNS queries-responses.



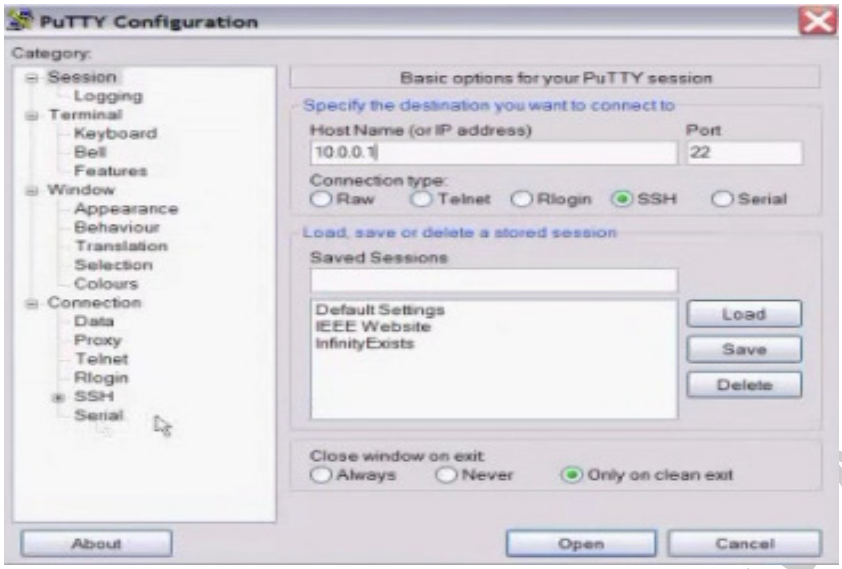
Εικόνα 58. Wireshark-Παρακολούθηση της DNS κίνησης.

Εάν ανοίξουμε ένα τέτοιο DNS πακέτο και δούμε το περιεχόμενο του θα είναι της μορφής:

adnmkjhwsokvcH78jlkjjhjLnuOnnhjL09876KJBhhialkjnjKhhjHfytdmRWaggfghj0k
NU7554ouygt87riupuih;908976675e4werghiuy7&GGkiuy7rdyfUygk756rfJBikuyrdE
uygfuwpo8jlJHJhgfjghJlkjuguygJLutyuh.tunnel.mytestexample.com..

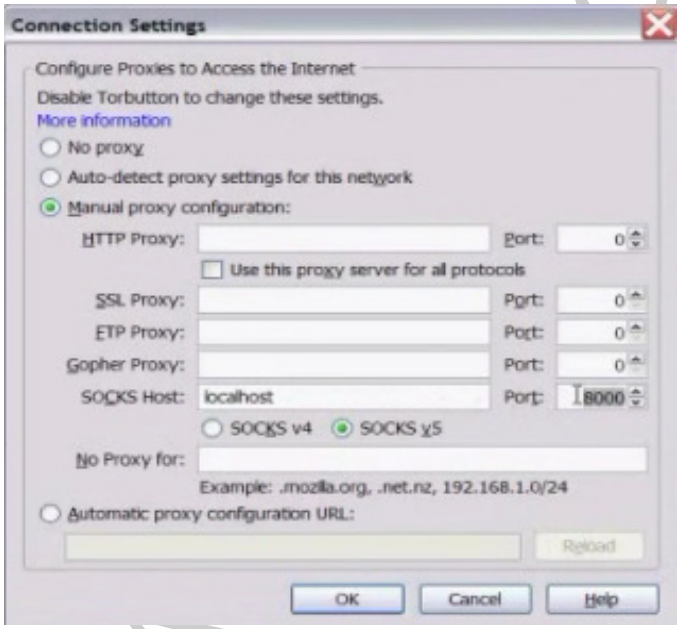
Αξίζει να αναφερθεί ότι η κωδικοποιημένη κίνηση των δεδομένων που διέρχεται από το tunnel δεν κρυπτογραφείται καθόλου και μπορεί να διαβαστεί και να αλλάξει από κάποιον τρίτο σχετικά εύκολα.
Για μεγαλύτερη ασφάλεια μπορεί να χρησιμοποιηθεί η πρόσβαση Secure Shell (SSH) να έχουμε δηλαδή άλλο ένα tunnel μέσα στο DNS tunnel (double tunneling).
Για να γίνει αυτό θα πρέπει να έχει στηθεί στον υπολογιστή που τρέχει ο Iodine server ένας SSH Server .

Στη συνέχεια στον client η εφαρμογή PuTTY αφού εγκατασταθεί και παραμετροποιηθεί σωστά θα επιτρέψει την πρόσβαση με τον SSH Server.
Στις ρυθμίσεις της εφαρμογής PuTTY εισάγουμε την IP 10.0.0.1 του server και την πόρτα 8000.



Εικόνα 59. Ρύθμιση της εφαρμογής PuTTy για SSH.

Τέλος θα πρέπει να ρυθμιστεί ο περιηγητής (browser) για την λειτουργία του SSH. Επιλέγεται η ρύθμιση “Manual proxy” και εισάγεται η πόρτα 8000 η οποία ορίστηκε πριν στις ρυθμίσεις της εφαρμογής PuTTy.



Εικόνα 60. Ρυθμιση του περιηγητή για SSH.

Έτσι μπορεί να λειτουργήσει το DNS tunneling με περισσότερη ασφάλεια χωρίς απειλή των δεδομένων για υποκλοπή και αλλοίωση.

ΚΕΦΑΛΑΙΟ 5

Μετρίαση των κινδύνων

5.1 Γενικές τεχνικές μετριασμού επιθέσεων

Virtual Private Network (VPN)
Ένα δίκτυο (VPN) είναι ένα ιδιωτικό δίκτυο πάνω από μια δημόσια υποδομή δικτύου διατηρώντας την εμπιστευτικότητα και την ασφάλεια. Τα δίκτυα VPNs χρησιμοποιούν πρωτόκολλα κρυπτογράφησης μέσα σε τούνελ για να παρέχουν επικύρωση αποστολέων, ακεραιότητα μηνυμάτων, και εμπιστευτικότητα προστατεύοντας τα δίκτυα από την υποκλοπή των πακέτων. Το VPN μπορεί να εφαρμοστεί στα στρώματα 2, 3, και 4 του Open Systems Interconnection (OSI).

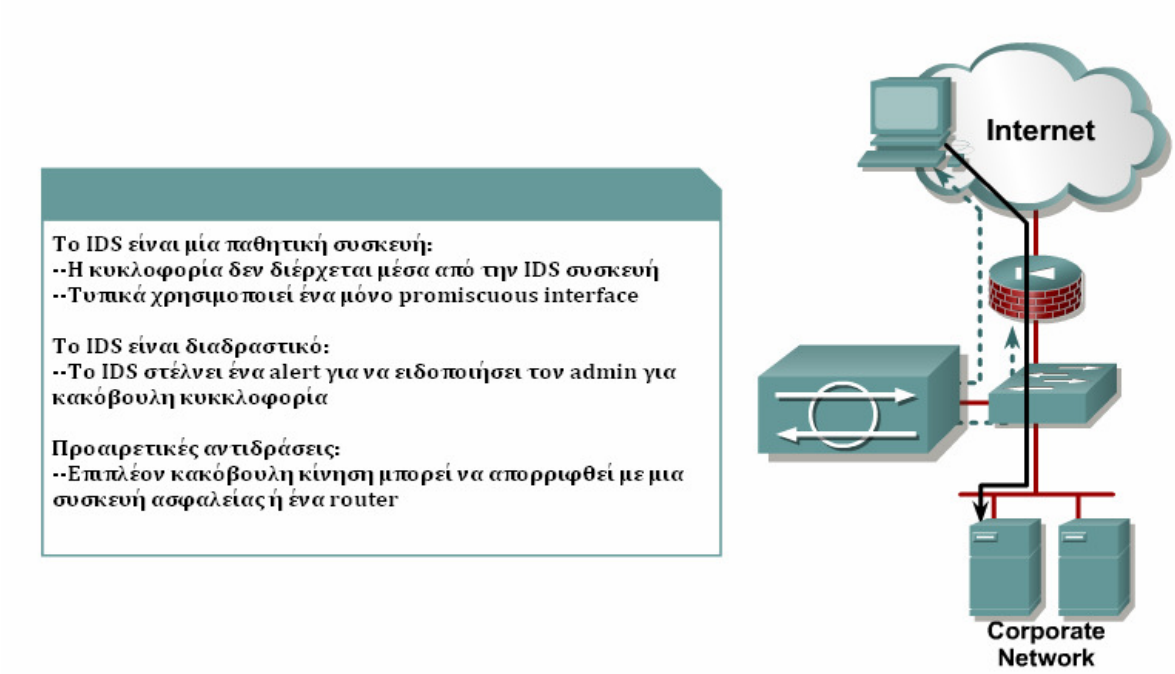
Το κλειδί για την τεχνολογία VPN είναι η ασφάλεια. Τα VPNs παρέχουν ασφάλεια με την τοποθέτηση των δεδομένων μέσα σε άλλης μορφής πακέτα (encapsulating), με την κρυπτογράφηση των δεδομένων ή και με τα δυο παραπάνω ταυτόχρονα:

- Η **ενθυλάκωση** (encapsulation) αναφέρεται επίσης ως tunneling επειδή η διαβιβάζει τα στοιχεία χωρίς να φαίνονται από δίκτυο σε δίκτυο μέσω μιας κοινής υποδομής δικτύου.
- Η **κρυπτογράφηση** κωδικοποιεί τα δεδομένα σε ένα διαφορετικό τύπο. Η αποκρυπτογράφηση αποκωδικοποιεί τα κρυπτογραφημένα στοιχεία στον αρχικό τους τύπο.

Το VPN εξασφαλίζει:
- Την **εμπιστευτικότητα** των δεδομένων.
- Την **ακεραιότητ**α των δεδομένων

Σύστημα ανίχνευσης παρείσφρησης - Intrusion Detection System (IDS)
Το Σύστημα ανίχνευσης παρείσφρησης (IDS) είναι μια λύση λογισμικού ή hardware που ακούει παθητικά την κυκλοφορία των δικτύων. Το IDS δεν είναι στην πορεία της κυκλοφορίας, αλλά ακούει όλη την κυκλοφορία του δίκτυου. Όταν το IDS ανιχνεύσει κακόβουλη κυκλοφορία, στέλνει μία προειδοποίηση στον διαχωριστή του δικτύου .

Το IDS έχει περιορισμένες ικανότητες ενεργών αντιδράσεων. Μπορεί να ρυθμιστεί έτσι ώστε να εμποδίσει την περαιτέρω κακόβουλη κυκλοφορία με την βοήθεια κάποιων συσκευών δικτύου (παραδείγματος χάριν, συσκευές ασφάλειας ή routers) σε απάντηση του εντοπισμού της κακόβουλη κυκλοφορίας. Εντούτοις, η αρχική κακόβουλη κυκλοφορία έχει περάσει ήδη μέσω του δικτύου στον προορισμό και δεν μπορεί να εμποδιστεί. Μόνο η επόμενη κυκλοφορία θα εμποδιστεί.

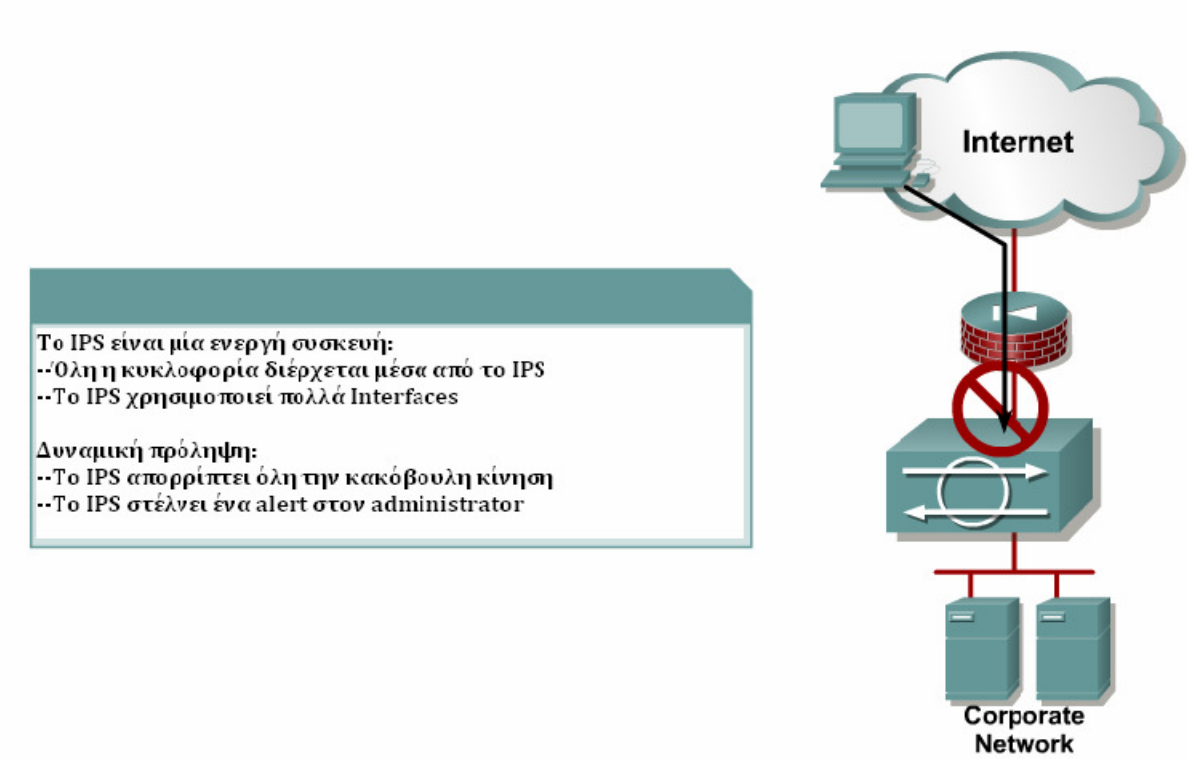


Εικόνα 61. Σύστημα ανίχνευσης παρείσφρησης - Intrusion Detection System (IDS)

Σύστημα πρόληψης παρείσφρησης- Intrusion Prevention System (IPS)

Ένα Σύστημα πρόληψης παρείσφρησης (IPS) είναι μια ενεργός συσκευή στην πορεία της κυκλοφορίας που «ακούει» την κυκλοφορία και επιτρέπει ή αρνείται τις ροές των πακέτων στο δίκτυο. Όλη η κυκλοφορία περνά μέσω του IPS για επιθεώρηση. Όταν το IPS ανιχνεύσει κακόβουλη κυκλοφορία, στέλνει μια προειδοποίηση στον διαχειριστή του δικτύου και μπορεί να διαμορφωθεί ώστε να εμποδίσει αυτή την κακόβουλη κυκλοφορία αμέσως. Το IPS αποτρέπει τις επιθέσεις με το μπλοκάρισμα τόσο της αρχικής κακόβουλης κυκλοφορίας που θα εντοπίσει όσο και της επόμενης .

Επειδή οι μηχανισμοί επίθεσης στα δίκτυα των επιχειρήσεων και των οργανισμών γίνονται ολοένα και πιο περίπλοκοι, αυτή η δυναμική προσέγγιση του IPS απαιτείται για να προστατευθούν από τους ιούς , τα worms, τις κακόβουλες εφαρμογές και την εκμετάλλευση των ευπαθειών των πρωτοκόλλων.



Εικόνα 62. Σύστημα πρόληψης παρείσφρησης- Intrusion Prevention System (IPS)

Συνδυασμός IDS και IPS

Το IDS και το IPS τοποθετούνται συχνά παράλληλα στα δίκτυα των επιχειρήσεων. Το IPS εμποδίζει ενεργά την εισερχόμενη κυκλοφορία και μπορεί να θεωρηθεί μια άλλη εφαρμογή ενός συστήματος firewall. Το IPS πρέπει να συντονιστεί να εμποδίσει μόνο τη γνωστή κακόβουλη κυκλοφορία προκειμένου να αποφευχθούν οι διασπάσεις συνδεσιμότητας. Ένα IDS μπορεί να ελέγξει ότι το IPS εμποδίζει πραγματικά την κακόβουλη κυκλοφορία και δεν εισέρχεται στο δίκτυο. Επιπλέον, το IDS μπορεί να διαμορφωθεί να στέλνει alerts για την κυκλοφορία «γκρίζας περιοχής» - τα δεδομένα που δεν είναι ούτε σαφώς κακόβουλα ούτε σαφώς νόμιμα. Τέτοια κυκλοφορία δεν πρέπει να εμποδιστεί από το IPS επειδή ίσως προκαλέσει διακοπή της συνδεσιμότητας, αλλά τα alerts που θα λαμβάνονται για αυτήν την κυκλοφορία μπορούν να παρέχουν πολύτιμη διορατικότητα για πιθανά προβλήματα ή τεχνικές επίθεσης.

Λογισμικό Antivirus

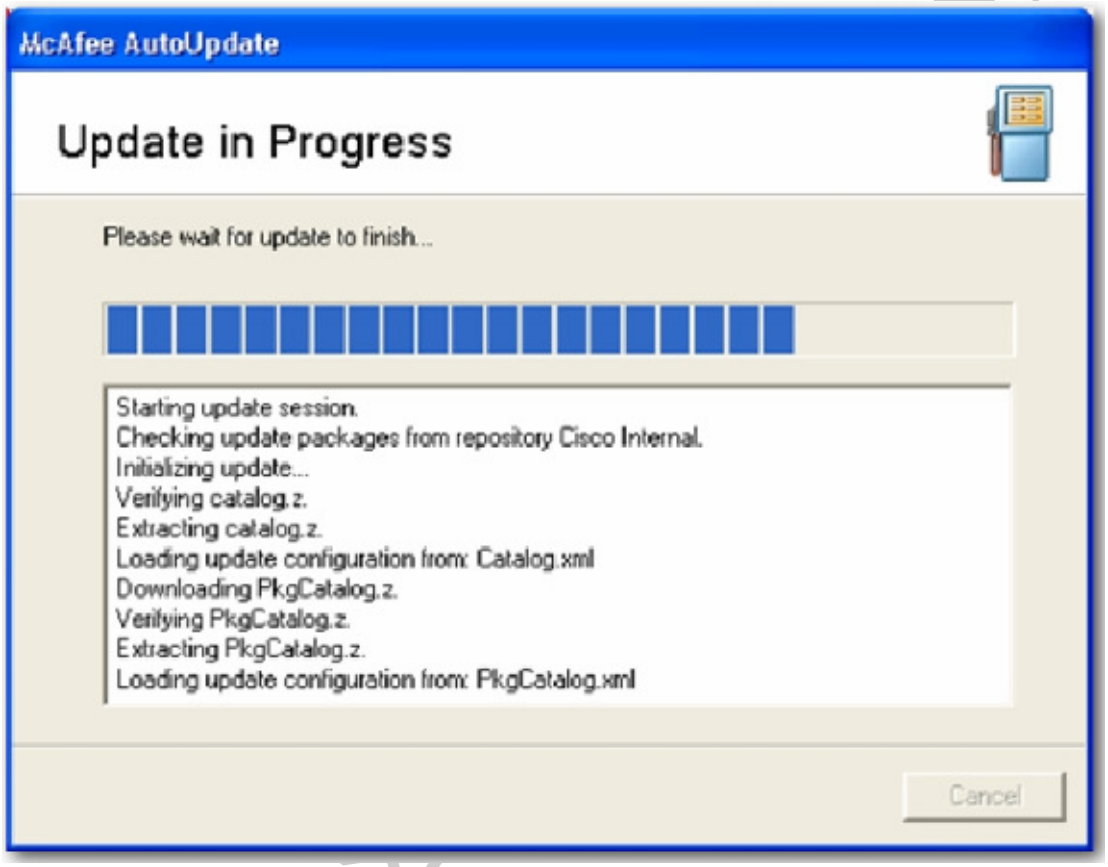
Η εγκατάσταση λογισμικών antivirus προστατεύουν από τους γνωστούς ιούς που μπορεί να μολύνουν τα λειτουργικά συστήματα των τελικών συσκευών. Το λογισμικό antivirus μπορεί να ανιχνεύσει τους περισσότερους ιούς και πολλές εφαρμογές, Trojan Horse και να τις αποτρέψει από τη διάδοση τους στο δίκτυο.

Το λογισμικό antivirus το κάνει αυτό με δύο τρόπους:

- Ανιχνεύει τα αρχεία, συγκρίνοντας το περιεχόμενό τους με τους γνωστούς ιούς σε ένα λεξικό ιών. Οι αντιστοιχίες επισημαίνονται με έναν τρόπο που καθορίζεται από τον τελικό χρήστη.

- Ελέγχει τις ύποπτες διαδικασίες που τρέχουν σε έναν host . Αυτός ο έλεγχος μπορεί να περιλαμβάνει τις συλλογές δεδομένων ,τον έλεγχο των πορτών και άλλες μεθόδους.

Τα περισσότερα εμπορικά λογισμικά antivirus χρησιμοποιούν και τις δύο προσεγγίσεις.



Εικόνα 63. Συνεχής ενημέρωση και αναβάθμιση του antivirus.

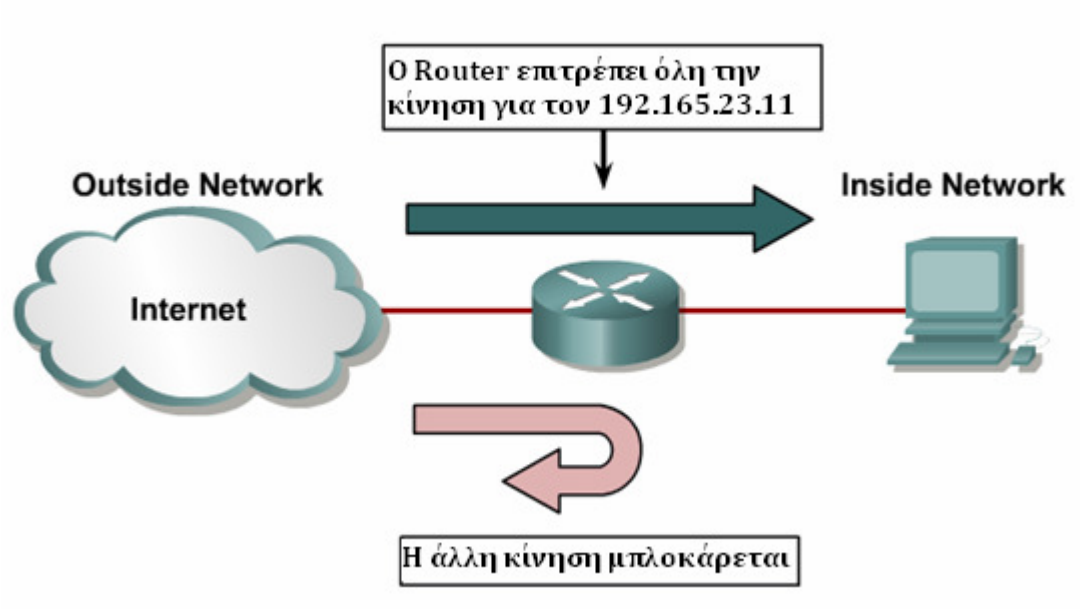
Firewalls

Οι προκλήσεις ασφάλειας που αντιμετωπίζουν οι σημερινοί διαχειριστές δικτύων δεν μπορούν να αντιμετωπιστούν επιτυχώς από μία μόνο εφαρμογή. Εντούτοις, το λογισμικό Firewall προσφέρει ένα πλήρες σύνολο ιδιοτήτων ασφαλείας που μπορεί να εφαρμοστούν για να παρέχουν την ασφάλεια σε ένα δίκτυο.

Τα firewalls επιβάλλουν το έλεγχο προσπέλασης μεταξύ δικτύων, τα οποία μπορούν να είναι διαφορετικών τύπων και επιπέδων εμπιστοσύνης. Ένα κοινό όνομα για μια ομάδα δικτύων που μπορεί να επιτευχθεί πέρα από ένα firewall είναι μια ζώνη ασφάλειας. Μια ζώνη ασφάλειας είναι μια διοικητικά χωριστή περιοχή στην οποία ή από την οποία ένα firewall μπορεί να φιλτράρει την εισερχόμενη ή την εξερχόμενη κυκλοφορία. Οι πιο ξεχωριστές ζώνες ασφάλειας είναι τα εσωτερικά(inside) και τα εξωτερικά(outside)δίκτυα που συνδέονται με τα firewalls στα εσωτερικά και εξωτερικά Interfaces αντίστοιχα.

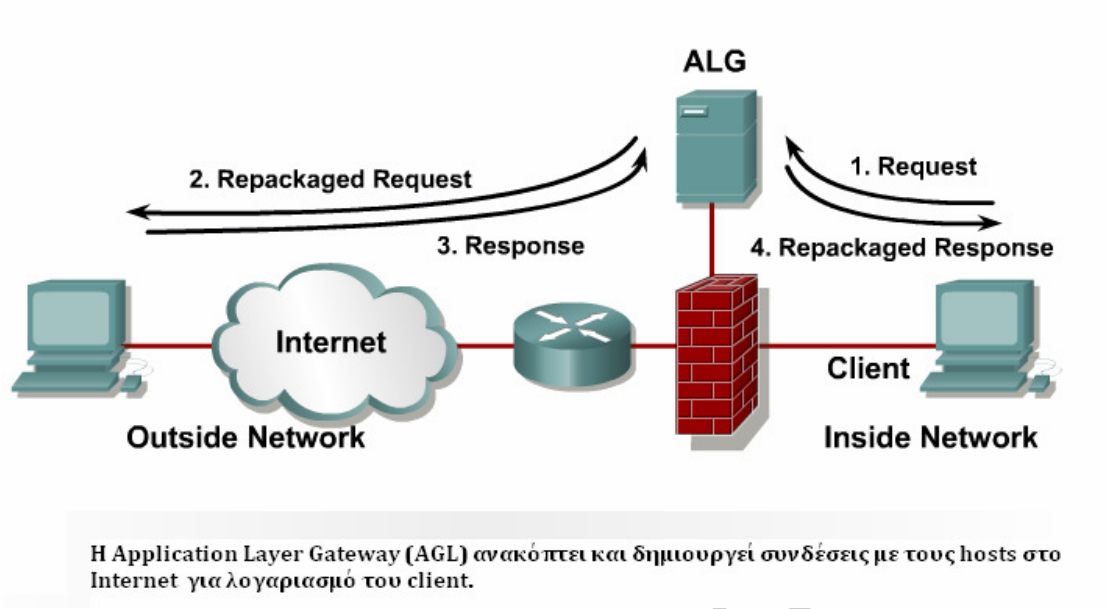
Οι λειτουργίες των firewall είναι βασισμένες σε μια από τις παρακάτω τεχνολογίες:

- Packet filtering: Το φιλτράρισμα πακέτων περιορίζει τις πληροφορίες που εισέρχονται σε ένα δίκτυο βασισμένο στις στατικές πληροφορίες των header των πακέτων. Οι συσκευές Layer 3 χρησιμοποιούν συνήθως το φιλτράρισμα πακέτων για να προσδιορίσουν τις access-lists (ACLs) που αποφασίζουν ποια κυκλοφορία να επιτρέψουν ή να απορρίψουν. Το φιλτράρισμα πακέτων μπορεί να εξετάσει τις πληροφορίες των header του πρωτοκόλλου μέχρι το transport layer (Layer 4) για να επιτρέψει ή να αρνηθεί ορισμένη κυκλοφορία. Το φιλτράρισμα πακέτων στέλνει τα επιτρεπόμενα πακέτα στο αιτούμενο σύστημα και απορρίπτει όλα τα άλλα πακέτα.



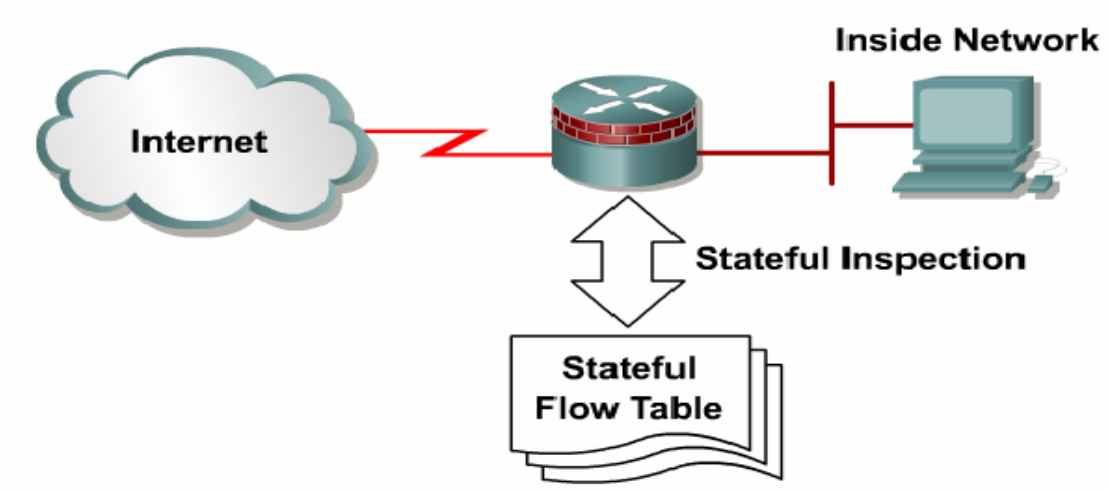
Εικόνα 64. Firewall-Φιλτράρισμα πακέτων.

- Application Layer Gateways: Οι ALGs εργάζονται στο application layer. Μία ALG είναι ένα πρόσθετο κομμάτι του λογισμικού που έχει σχεδιαστεί να προωθεί τα αιτήματα και τις απαντήσεις του application layer μεταξύ των τελικών σημείων. Μια ALG ενεργεί ως μεσάζων μεταξύ ενός application client για τον οποίο η ALG ενεργεί ως εικονικός server, και ενός server για τον οποίο η ALG ενεργεί ως εικονικός client. Ο client συνδέεται με τον proxy server και υποβάλλει ένα application layer αίτημα . Το application layer αίτημα περιλαμβάνει τον αληθινό προορισμό της κυκλοφορίας και τα δεδομένα . Ο proxy server αναλύει το αίτημα και μπορεί να φιλτράρει ή να αλλάξει το περιεχόμενο του αιτήματος και μετά να ανοίξει ένα session με τον server προορισμού. Ο server προορισμού απαντά στον proxy server. Ο proxy server περνά την απάντηση, που μπορεί να φιλτράρει και να αλλάξει, πίσω στον client.



Εικόνα 65. Firewall-Application Layer Gateway (AGL)

- Stateful packet filtering: Το φιλτράρισμα πακέτων Stateful είναι η ευρύτατα χρησιμοποιημένη τεχνολογία firewall. Το Stateful φιλτράρισμα πακέτων είναι μια μέθοδος –σε επίπεδο εφαρμογής- φιλτραρίσματος πακέτου που δουλεύει στη σύνδεση, ή στο επίπεδο ροής. Το Stateful φιλτράρισμα πακέτων διατηρεί έναν πίνακα καταστάσεων (state table) για να παρακολουθεί όλες τις ενεργές συνόδους που διασχίζουν το firewall. Ο πίνακας αυτός, που είναι μέρος της εσωτερικής δομής του firewall, παρακολουθεί όλα τα sessions και επιθεωρεί όλα τα πακέτα που περνούν μέσω του firewall. Εάν τα πακέτα έχουν τις αναμενόμενες ιδιότητες που ο πίνακας καταστάσεων προβλέπει, τα πακέτα διαβιβάζονται.



Εικόνα 66. Firewall - Φιλτράρισμα πακέτων Stateful.

5.2 Τεχνικές ανίχνευσης DNS tunneling

Το DNS tunneling θέτει μια σημαντική απειλή αλλά υπάρχουν μέθοδοι για να την ανιχνεύσουν. Πολλές από τις εφαρμογές DNS tunneling δεν προσπαθούν καν να είναι μη ανιχνεύσιμες. Στηρίζονται στο γεγονός ότι η DNS κίνηση συχνά δεν ελέγχεται. Διάφορες τεχνικές ανίχνευσης DNS tunneling έχουν προταθεί. Οι τεχνικές ανίχνευσης χωρίζονται σε δύο κατηγορίες, ανάλυση του φορτίου των πακέτων (payload) και ανάλυση της κυκλοφορίας. Για την ανάλυση του φορτίου των πακέτων το DNS φορτίο για ένα ή περισσότερα ζεύγη αιτήματος - απάντησης θα αναλυθεί .Για την ανάλυση της κυκλοφορίας η κυκλοφορία θα αναλυθεί σε συνάρτηση με το χρόνο. Ο αριθμός, η συχνότητα και άλλα χαρακτηριστικά των DNS αιτημάτων θα εξεταστούν.

5.2.1 Ανάλυση φορτίου (payload)

Η ανάλυση του payload χρησιμοποιείται για να ανιχνεύσει κακόβουλη δραστηριότητα βασισμένη σε ένα μόνο DNS αίτημα. Ιδιότητες ενός αιτήματος όπως το μήκος του domain ,ο αριθμός των bytes και το περιεχόμενο μπορούν να χρησιμοποιηθούν για να δημιουργήσουν τους κανόνες της ανίχνευσης. Η ανίχνευση ασυνήθιστου περιεχομένου ,όπως TXT , μπορεί να χρησιμοποιηθεί επίσης.

5.2.1.1 Μέγεθος του αιτήματος και της απάντησης

Μια τεχνική περιλαμβάνει την ανάλυση του μεγέθους του αιτήματος και της απάντησης. Σε ένα blog (Bianco, 2006) ο συντάκτης καθορίζει μεθόδους για να προσδιορίσει την ύποπτη κυκλοφορία DNS tunneling βασισμένες στην αναλογία των bytes της πηγής και του προορισμού. Τα DNS δεδομένα αποθηκεύονται σε μια βάση δεδομένων MySQL ,ως τμήμα ενός Snort/Squil συστήματος ανίχνευσης παρείσφρυσης (intrusion detection). Η αναλογία των bytes της πηγής και του προορισμού συγκρίνεται έπειτα με ένα κατώτατο όριο.

Άλλοι (Pietraszek, 2004), (Skoudis, 2012) έχουν προτείνει την εξέταση του μήκους της DNS ερώτησης και απάντησης για να ανιχνευτεί το tunneling. Οι εφαρμογές DNS tunneling προσπαθούν συνήθως να βάλουν όσο πιο πολλά δεδομένα μπορούν μέσα στα αιτήματα και τις απαντήσεις. Κατά συνέπεια, είναι πιθανό τα αιτήματα να έχουν ετικέτες μέχρι 63 χαρακτήρες και μεγάλα γενικά ονόματα μέχρι 255χαρακτήρες. Μια άλλη πρόταση είναι να εξεταστούν όλα τα DNS αιτήματα που είναι μεγαλύτερα από 52 χαρακτήρες (Guy, 2009).

5.2.1.2 Εντροπία των hostnames

Τα DNS tunnels μπορούν να ανιχνευθούν βάση της εντροπίας των αιτούμενων hostnames (Van Horenbeeck, 2006), (Butler, 2011). Τα νόμιμα DNS ονόματα έχουν συχνά λέξεις λεξικών ή λέξεις που φαίνεται να σημαίνουν κάτι. Τα κωδικοποιημένα ονόματα έχουν μια υψηλότερη εντροπία και μια μεγαλύτερη χρήση του συνόλου των

χαρακτήρων. Η αναζήτηση των DNS ονομάτων που έχουν υψηλή εντροπία μπορεί να είναι δείκτης tunneling αν και υπάρχουν και εξαιρέσεις.

5.2.1.3 Στατιστική ανάλυση

Η εξέταση συγκεκριμένων χαρακτήρων που έχει φτιαχτεί ένα DNS όνομα είναι μια άλλη μέθοδος που μπορεί χρησιμοποιηθεί για να ανιχνεύσει tunneling. Τα νόμιμα DNS ονόματα τείνουν να έχουν λίγους αριθμούς ενώ τα κωδικοποιημένα ονόματα μπορούν να έχουν πολλούς αριθμούς. Η εξέταση του ποσοστού των αριθμητικών χαρακτήρων στα ονόματα έχει προταθεί (Bilge, 2011). Η εξέταση του ποσοστού του μήκους του Longest Meaningful Substring (LMS) είναι μια άλλη μέθοδος βασισμένη στην εξέταση συγκεκριμένου χαρακτήρα (Bilge, 2011). Η εξέταση του αριθμού μοναδικών χαρακτήρων είναι μια άλλη δυνατότητα. Μια σύσταση για συναγερμό σε οτιδήποτε με πάνω από 27 μοναδικούς χαρακτήρες έχει προταθεί. (Guy, 2009)

Δεδομένου ότι τα νόμιμα ονόματα αντανακλούν κοινές λέξεις της γλώσσες σε κάποιο βαθμό, η χρήση της ανάλυσης συχνότητας χαρακτήρα (Born, 2010b) θα μπορούσε επίσης να χρησιμοποιηθεί για να ανιχνεύσει ονόματα που έχουν παραχθεί από το DNS tunneling.

Τα επαναλαμβανόμενα σύμφωνα μπορούν να εξεταστούν για να ανιχνεύσουν ένα DNS tunneling, ή τα επαναλαμβανόμενα σύμφωνα μαζί με αριθμούς (Lockington, 2012). Μια εφαρμογή DNS tunneling θα δημιουργήσει ενδεχομένως ονόματα με διαδοχικά σύμφωνα και αριθμούς κάτι που είναι απίθανο σε νόμιμα ονόματα.

5.2.1.4 Ασυνήθιστοι τύποι "record"

Ψάχνοντας τους τύπους των record που δεν χρησιμοποιούνται συνήθως, όπως για παράδειγμα TXT records (Pietraszek, 2004) είναι μια άλλη πιθανή μέθοδος ανίχνευσης.

5.2.1.5 Παραβίαση Πολιτικής

Εάν μια πολιτική απαιτεί όλες τις αναζητήσεις DNS να περάσουν από έναν εσωτερικό DNS server, οι παραβιάσεις αυτής της πολιτικής θα μπορούσαν να χρησιμοποιηθούν ως μέθοδος ανίχνευσης.
Η κυκλοφορία θα μπορούσε να ελεγχθεί για τα DNS αιτήματα απευθείας στο Διαδίκτυο (Fry, 2009).

5.2.1.6 Συγκεκριμένες υπογραφές

Σε ορισμένες περιπτώσεις, οι ερευνητές έχουν παράσχει υπογραφές για συγκεκριμένες εφαρμογές DNS tunneling. Μια υπογραφή μπορεί να χρησιμοποιηθεί για να ελέγξει συγκεκριμένες ιδιότητες σε ένα DNS header και για να ελέγξει συγκεκριμένο περιεχόμενο στο φορτίο. Παραδείγματος χάριν, η υπογραφή Snort αναπτύχθηκε για την ανίχνευση του NSTX DNS tunneling (Van Horenbeeck, 2006).

alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"Potential NSTX DNS Tunneling"; content:"\|01 00\|"; offset:2; within:4; content:"cT"; offset:12; depth:3; content:"\|00 10 00 01\|"; within:255; classtype:badunknown; sid:1000 2;)

Στο ανωτέρω παράδειγμα τα βασικά μέρη αυτού του κανόνα είναι τα ακόλουθα. Αυτή η υπογραφή έχει τρεις αντιστοιχίες. Το "offset 2" θα πηδήσει το μέρος ID του DNS header που αντιπροσωπεύουν τα πρώτα δύο bytes. Τα επόμενα δύο bytes αντιπροσωπεύουν τα διάφορα χαρακτηριστικά του header. Με το δεκαεξαδικό "01", τα bits 0 μέχρι 6 είναι 0 και το bit 7 είναι 1. Αυτό αντιστοιχεί σε μια DNS ερώτηση και όχι σε μια απάντηση και τα 4 bits είναι 0 που σημαίνει ότι είναι μια τυποποιημένη ερώτηση. Η επόμενη ικανοποιημένη αντιστοιχία αρχίζει ένα "offset 12". Αυτό είναι η έναρξη του τμήματος της ερώτησης και συγκεκριμένα το πεδίο QNAME. Επομένως, αυτή η ικανοποιημένη αντιστοιχία ψάχνει για το "cT" ως τμήμα των πρώτων 3 bytes του domain name. Η τελευταία ικανοποιημένη αντιστοιχία ψάχνει τις δεκαεξαδικές τιμές "00 10 00 01" μέσα στα πρώτα 255 bytes του φορτίου (payload). Αυτό θα ταιριάξει τα δύο QTYPE και QLASS τμήματα της ερώτησης όταν το QTYPE είναι δεκαεξαδικό 10 (δεκαδικό 16) και το QCLASS είναι 1 το όποιο αντιστοιχεί στο "IN"για το Διαδίκτυο. Το "IN" είναι το μόνο QCLASS που χρησιμοποιείται συνήθως και έτσι πάντα θα ταιριάζει με το "00 01". Ένα QTYPE του δεκαδικού 16 αντιστοιχεί στον τύπο TXT resource record (Aitchison, 2011). Συνοψίζοντας, αυτή η υπογραφή ψάχνει για τυποποιημένες DNS ερωτήσεις με τύπο TXT resource record με τη γραμματοσειρά "cT" κοντά στην αρχή του ονόματος.

5.2.2 Ανάλυση κυκλοφορίας

Η ανάλυση κυκλοφορίας περιλαμβάνει την εξέταση πολλών ζευγαριών αιτήματος/απάντησης. Η ποσότητα και η συχνότητα των αιτημάτων μπορούν να χρησιμοποιηθούν ως ένδειξη για tunneling. Οι τεχνικές ανίχνευσης ανάλυσης κυκλοφορίας παρουσιάζονται παρακάτω.

5.2.2.1 Ο όγκος της DNS κυκλοφορίας ανά διεύθυνση IP

Μια βασική και απλή μέθοδος είναι να εξεταστεί το ποσό της DNS κυκλοφορίας που προέρχεται από μια συγκεκριμένη διεύθυνση IP (Pietraszek, 2004), (Van Horenbeeck, 2006). Επειδή τα δεδομένα που θα περάσουν μέσω του tunnel έχουν όριο 512 bytes ανά αίτημα, ένας μεγάλος αριθμός αιτημάτων απαιτείται για την επικοινωνία και τη μεταφορά της πληροφορίας.

5.2.2.2 Ο όγκος της DNS κυκλοφορίας ανά domain

Μια άλλη βασική μέθοδος είναι να εξεταστούν τα μεγάλα ποσά κυκλοφορίας για ένα συγκεκριμένο domain name (Butler, 2011). 'Ολες οι εφαρμογές DNS tunneling χρησιμοποιούν ένα συγκεκριμένο όνομα (domain name) στο οποίο προωθούν τα κωδικοποιημένα δεδομένα έτσι, όλη η DNS κυκλοφορία θα απευθύνεται σε εκείνο το όνομα. Πρέπει να εξετάσουμε την πιθανότητα ότι θα μπορούσε να διαμορφωθεί DNS

tunneling με πολλά domain names και κατά συνέπεια την μείωση του ποσού της κυκλοφορίας ανά domain!

5.2.2.3 Ο αριθμός hostnames ανά domain

Ο αριθμός των hostnames για ένα συγκεκριμένο domain μπορεί να αποτελέσει δείκτη tunneling (Guy, 2009).Οι εφαρμογές DNS tunneling ζητούν ένα μοναδικό hostname σε κάθε αίτημα. Αυτό μπορεί να οδηγήσει σε ένα πολύ μεγαλύτερο αριθμό από ένα χαρακτηριστικό νόμιμο domain name.

5.2.2.4 Η γεωγραφική θέση του DNS server

Οι γεωγραφικές εκτιμήσεις είναι ένας άλλος παράγοντας που θα μπορούσε να χρησιμοποιηθεί. (Skoudis, 2012). Για τις επιχειρήσεις που περιορίζονται σε τοπικό επίπεδο και δεν δραστηριοποιούνται διεθνώς, αυτή η μέθοδος θα μπορούσε να είναι χρήσιμη.

5.2.2.5 Το ιστορικό των domain

Το ιστορικό των domain μπορεί επίσης να χρησιμοποιηθεί για να αυξήσει την υποψία για κακόβουλη κυκλοφορία DNS. Έλεγχος όταν ένα αρχείο τύπου NS record ή A record προστίθεται (Zrdnja, 2007). Αυτή η μέθοδος χρησιμοποιήθηκε για τον εντοπισμό των domain names που εμπλέκονται σε κακόβουλη δραστηριότητα. Είναι επίσης σχετικό με την ανίχνευση DNS tunneling. Ένα domain θα μπορούσε να έχει αποκτηθεί πρόσφατα με σκοπό το DNS tunneling και οι εγγραφές NS του θα μπορούσαν να έχουν προστεθεί πρόσφατα.

5.2.2.6 Ο όγκος των απαντήσεων NXDomain

Η έρευνα των υπερβολικών απαντήσεων NXDomain προτάθηκε για την ανίχνευση των DGA δημιουργημένων ονομάτων. (Antonakakis, 2012). Αυτή η μέθοδος θα μπορούσε να είναι χρήσιμη για τον εντοπισμό του Heyoka που παραγάγει μεγάλα ποσά απαντήσεων NXDomain.

5.2.2.7 Απεικόνιση

Έχει αποδειχθεί ότι η απεικόνιση μπορεί να χρησιμοποιηθεί για την ανίχνευση των DNS tunneling (Guy,2009). Αυτή η μέθοδος απαιτεί διαδραστική εργασία από έναν αναλυτή, αλλά μπορεί να ξεχωρίσει την κακόβουλη κυκλοφορία εντυπωσιακά.

5.2.2.8 Ορφανά αιτήματα DNS

Ενώ οι περισσότερες μέθοδοι ανίχνευσης εξετάζουν αυτό που μπορούμε να δούμε, μια άλλη προσέγγιση είναι να εξεταστεί το τι αναμένουμε να δούμε, αλλά λείπει.

Γενικά ένα DNS αίτημα υποβάλλεται μόνο πριν από ένα άλλο αίτημα, παραδείγματος χάριν για ένα αίτημα ιστοσελίδας μέσω HTTP. Έχοντας αυτό υπόψη μια άλλη μέθοδος ανίχνευσης είναι να ψαχτούν τα αιτήματα DNS που δεν έχουν ένα αντίστοιχο αίτημα από μια άλλη εφαρμογή όπως το HTTP. Σίγουρα θα υπάρξουν εξαιρέσεις που θα μπορούσαν όμως εύκολα να φιλτραριστούν. Οι συσκευές ασφάλειας μπορούν να κάνουν τις αντίστροφες αναζητήσεις στις διευθύνσεις IP. Οι αντι-spam λύσεις χρησιμοποιούν DNS ερωτήσεις που ελέγχουν εάν μια δεδομένη διεύθυνση IP είναι σε μαύρη λίστα.

5.2.2.9 Γενική ανίχνευση συγκεκαλυμμένων καναλιών (covert channel)

Μερικές τεχνικές για την ανίχνευσης των συγκεκαλυμμένων καναλιών ανεξάρτητα από το πρωτόκολλο έχουν παρουσιαστεί σε έρευνες στο παρελθόν (Couture, 2010). Οι εφαρμογές που έχουν σχεδιαστεί για την ανίχνευση των tunnels μπορούν να εξετάσουν πράγματα όπως την ώρα της ημέρας του αιτήματος ή να συγκρίνουν την κυκλοφορία με ένα στατιστικό δακτυλικό αποτύπωμα.

5.3 Εφαρμογή των μεθόδων ανίχνευσης

Ένας μεγάλος αριθμός πιθανών μεθόδων ανιχνεύσεων παρουσιάστηκε παραπάνω. Στην πραγματική εφαρμογή, οι μέθοδοι πρέπει να ζυγιστούν για το κόστος και την αποτελεσματικότητα τους. Το κόστος περιλαμβάνει δαπάνες όπως η απόκτηση των συστημάτων ανίχνευσης, ο χρόνος που χρειάζεται για να εξελιχθούν και οι υπολογιστικοί πόροι που καταναλώνονται.
Η "άμυνα σε βάθος" είναι μια στρατηγική ασφάλειας όπου υπάρχουν πολλά στρώματα ασφάλειας. Εάν ένα στρώμα αποτύχει να ανιχνεύσει την κακόβουλη δραστηριότητα, ένα άλλο στρώμα θα τα καταφέρει. Έτσι εφαρμόζοντας παράλληλα την ανάλυση φορτίου (payload) και την ανάλυση της κυκλοφορίας επιτυγχάνεται σε κάποιο βαθμό η "άμυνα σε βάθος".

Για τα παραδείγματα των υλοποιήσεων ανίχνευσης που παρουσιάζονται παρακάτω ένα σύστημα από αυτά που κυκλοφορούν στο εμπόριο απαιτείται για να συλλέγει και να αναλύει την κυκλοφορία. Αυτό το σύστημα θα αναφέρεται γενικά ως CAP (Capture and Parse).Το σύστημα συγκεντρώνει την κυκλοφορία του δικτύου μέσω μιας πόρτας TAP.Η κυκλοφορία που έχει συλλεχθεί περιλαμβάνει διάφορα πρωτόκολλα συμπεριλαμβανομένου του DNS.Η κίνηση στην συνέχεια μπορεί να φιλτραριστεί με μια απλή γλώσσα κανόνα συμπεριλαμβανομένου της περιορισμένης χρήσης κανονικών εκφράσεων (regex).Μια άλλη εφαρμογή αναφορών χρησιμοποιείται στην συνέχεια η οποία κρατάει αναφορά κάθε φορά που η κίνηση ταιριάζει με συγκεκριμένους κανόνες.

5.3.1 Εφαρμογή ανίχνευσης ανάλυσης φορτίου DNScat-B πρόθεμα FQDN

Ο ιστοχώρος για την εφαρμογή DNScat-B περιγράφει τα στοιχεία που αποτελούν το FQDN που αυτή παράγει (Bowes, 2010). Υπάρχουν παραλλαγές στην παραγωγή του

FQDN ανάλογα με τον τύπο (datagram ή stream) και εάν χρησιμοποιείται ή όχι session. Η παραγωγή ενός FQDN τύπου datagram χωρίς session φαίνεται παρακάτω :
<signature>.<flags>.<count>.<data>.<garbage>.<domain>
Στον κανόνα αυτό, θα γίνει εστίαση στο στοιχείο "signature". Αυτό το στοιχείο υπάρχει σε όλα τα FQDNs που παράγονται από την εφαρμογή DNScat-B. Από προεπιλογή έχει οριστεί ως "dnscat" αν και μπορεί εύκολα να αλλαχτεί. Για να γίνει ταυτοποίηση των FQDNs που αρχίζουν με το "dnscat" ως signature, ο ακόλουθος κανόνας θα χρησιμοποιηθεί:

alias.host begins'dnscat'

Η λέξη κλειδί "alias.host" είναι το όνομα που το σύστημα CAP (Capture and Parse) χρησιμοποιεί για το FQDN. Η λέξη κλειδί "begins" σημαίνει την αναζήτηση οποιουδήποτε alias.host που αρχίζει με την ακόλουθη γραμματοσειρά. Το μέρος του κανόνα "dnscat" δείχνει ότι ο alias.host πρέπει να αρχίζει με τη γραμματοσειρά "dnscat".

5.3.2 Εφαρμογή ανίχνευσης ανάλυσης φορτίου DNScat-B κωδικοποιημένης κυκλοφορίας NetBIOS

Η εφαρμογή DNScat-B χρησιμοποιεί από προεπιλογή NetBIOS κωδικοποίηση. Με αυτόν τον τύπο κωδικοποίησης, κάθε χαρακτήρας θα είναι μεταξύ του "A" και του "O" (Bowes, 2010). Όταν η υλοποίηση DNScat-B μεταφέρει δεδομένα, υπάρχουν από προεπιλογή ετικέτες domain μήκους 63 που μπορούν να αλλάξουν και 3 ετικέτες για τα δεδομένα που μπορούν πάλι να αλλάξουν. Για να ανιχνευτεί η NetBIOS κωδικοποιημένη κυκλοφορία που αφορά το μέρος "των δεδομένων" του FQDN ο ακόλουθος κανόνας θα χρησιμοποιηθεί:

alias.host regex '[[.period.]][a-o]{50,63}[[.period.]][a-o]{50,63}[[.period.]]'

Η λέξη κλειδί "alias.host" είναι το όνομα που το σύστημα CAP χρησιμοποιεί για το FQDN. Το "[[.period.]]" αντιστοιχεί στον χαρακτήρας "." . Το "[a-o]{50.63}" ψάχνει μια γραμματοσειρά που αποτελείται από 50 έως 63 χαρακτήρες από το "a" ως το "o".

Μερικοί από τους κανόνες ανάλυσης φορτίου θα μπορούσαν να παρακαμφθούν από έναν πεπειραμένο χάκερ. Ένας επιτιθέμενος με εμπειρία μπορεί να πειράξει τις ετικέτες που χρησιμοποιούνται μικραίνοντας τις και να μειώσει τον αριθμό των ετικετών σε ένα FQDN. Για το FQDN “www.mydomain.test.com” το root domain (top & second level domain) είναι το “test.com”. Το σύστημα CAP δεν παρέχει τη δυνατότητα για αναφορές σχετικά με τον αριθμό των FQDNs ανά root domain που αποτελεί μια ασφαλή μέθοδο ανίχνευσης tunneling. Εντούτοις αυτό μπορεί να παρασχεθεί από το API (Application Program Interface) που μπορεί να χρησιμοποιηθεί για επέμβει στα αποθηκευμένα δεδομένα και να δημιουργήσει τον επιθυμητό κανόνα. Μέσω του API τα αποθηκευμένα δεδομένα μπορούν να ζητηθούν και να παραληφθούν σε μορφή TXT, HTML, XML ή json. Ένα πρωτότυπο αναπτύχθηκε χρησιμοποιώντας Python και τη βιβλιοθήκη nwmodule από nwmaltego (Bressler, 2012).

5.3.3 Εφαρμογή ανίχνευσης ανάλυσης κυκλοφορίας

Για τα δεδομένα της δοκιμής, η κυκλοφορία ελέγχθηκε για μια ημέρα κατά τη διάρκεια των κανονικών ωρών ενός γραφείου.
Πάνω από 380.000 εξωτερικά αιτήματα DNS εμφανίστηκαν κατά τη διάρκεια μιας εργάσιμης ημέρας. Το περιβάλλον είχε πάνω από 1.000 χρήστες. Ένα DNS tunneling δημιουργήθηκε χρησιμοποιώντας την εφαρμογή DNScat-B σε ένα σημείο κατά τη διάρκεια της ημέρας και χρησιμοποιήθηκε για να μεταφέρει ένα αρχείο κειμένου μεγέθους 122K (το κείμενο του RFC 1035). Η μεταφορά του αρχείου διήρκησε περίπου 2 λεπτά και το tunnel παρέμεινε ενεργό για λίγα λεπτά μετά από αυτήν.
Η τεχνική ανίχνευσης "μοναδικού αριθμού FQDN ανά root domain" υλοποιήθηκε για να παρθούν δείγματα με παράθυρο δέκα λεπτών το κάθε ένα.

Το σχήμα 5-1 παρουσιάζει την κυκλοφορία DNS από τη δραστηριότητα του tunneling. Ο κάθετος άξονας είναι ο αριθμός των sessions .

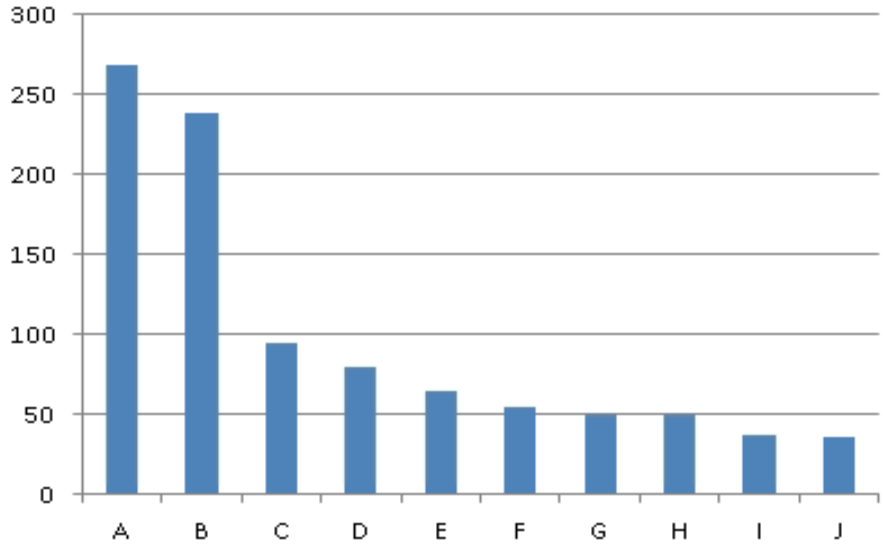
Σχήμα 5-1. Χρονική διάρκεια κίνησης DNS tunneling

Η ευθεία γραμμή στο τέλος της γραφικής παράστασης εμφανίζεται επειδή η μεταφορά του αρχείου ολοκληρώθηκε και το tunnel πέρασε στην κατάσταση "ενεργό" όπου ένας σταθερός αριθμός αιτημάτων στέλνεται στον DNS tunnel server.

Στις γραφικές παραστάσεις παρακάτω, τα κανονικά ονόματα root domain αντικαταστάθηκαν με απλά γράμματα για απλούστευση της διαδικασίας. Το root domain που χρησιμοποιήθηκε για το tunneling αντικαταστάθηκε με την ετικέτα "TUN".

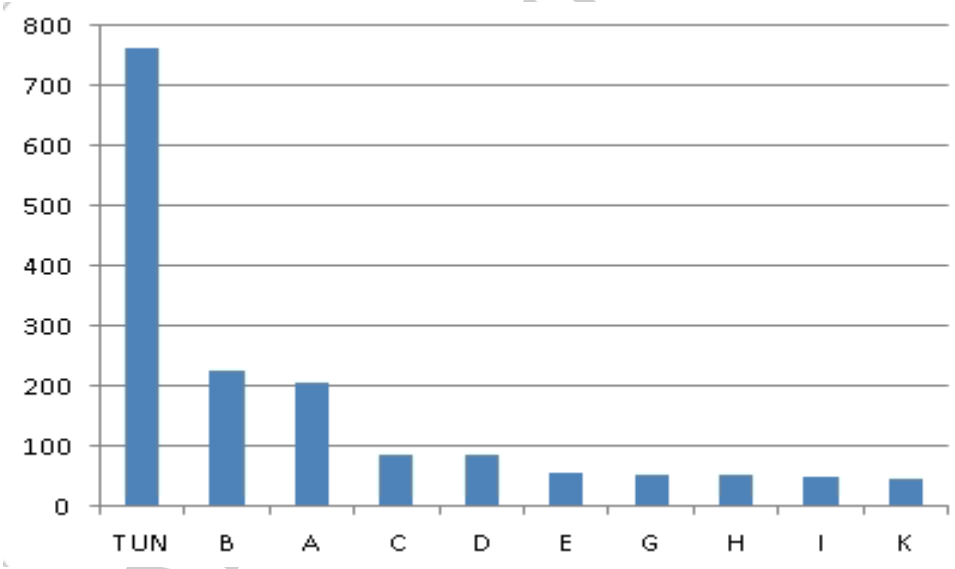
Στο σχήμα 5-2 παρουσιάζεται το παράθυρο 10 λεπτών της κυκλοφορίας αμέσως προτού να εμφανιστεί οποιαδήποτε κίνηση tunneling.Ο κάθετος άξονας είναι ο αριθμός των μοναδικών FQDNs. Τα domains που έχουν μεγάλο αριθμό μοναδικών FQDNs χωρίζονται σε μερικές διαφορετικές κατηγορίες. Τα domains που χρησιμοποιούνται για διαφήμιση, υπηρεσίες παράδοσης περιεχομένου (content delivery) και υπηρεσιών clouding χρησιμοποιούν συχνά έναν μεγάλο αριθμό μοναδικών FQDNs. Τα domains που παρέχουν ποικιλία υπηρεσιών μπορεί να έχοουν μεγάλο αριθμό FQDNs.

Ένα ενδιαφέρον παράδειγμα είναι η ετικέτα "A". Αυτό το domain είναι μια υπηρεσία ασφάλειας που χρησιμοποιεί κωδικοποιημένα αρχεία ως μέρος ενός FQDN για τον έλεγχο των αρχείων. Αυτό το domain έχει έναν μεγάλο αριθμό μοναδικών FQDNs. Ένα άλλο παράδειγμα είναι ένα domain δευτέρου επιπέδου που χρησιμοποιείται για να παρέχει domain για άλλους οργανισμούς, όπως το "co.uk". Τα domains στις παρακάτω εικόνες ανήκουν όλα σε μια από τις ανωτέρω κατηγορίες ή στην πραγματική κυκλοφορία tunneling.



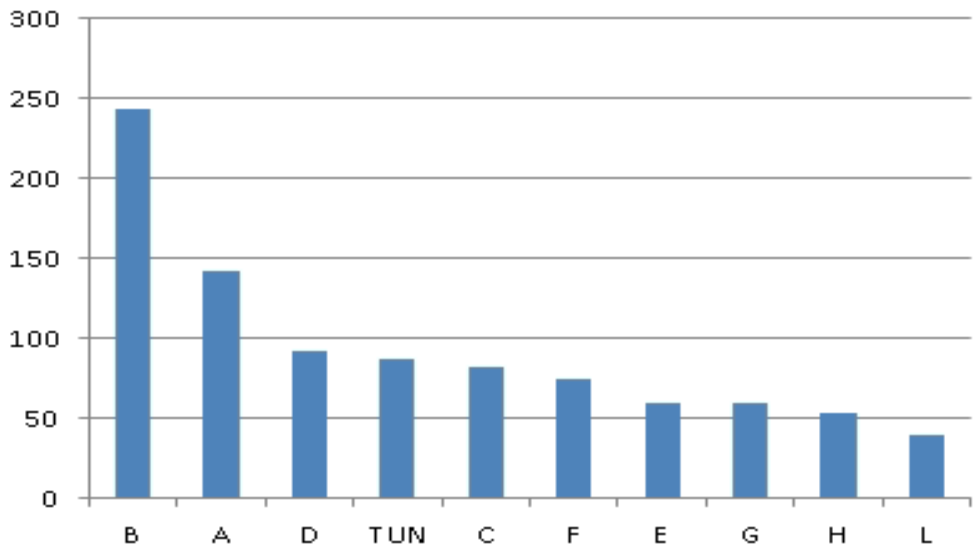
Σχήμα 5-2.Ο αριθμός των FQDNs με παράθυρο δείγματος 10 λεπτών, πριν το DNS tunneling.

Χαρακτηριστικά όπως φαίνεται στο σχήμα 5-2, όλα τα domain έχουν λιγότερα από 300 μοναδικά FQDNs για ένα παράθυρο δείγματος δέκα λεπτών. Ένα κατώτατο όριο 300 θα μπορούσε να χρησιμοποιηθεί για να αποτελέσει προειδοποίηση για πιθανό DNS tunneling domain.



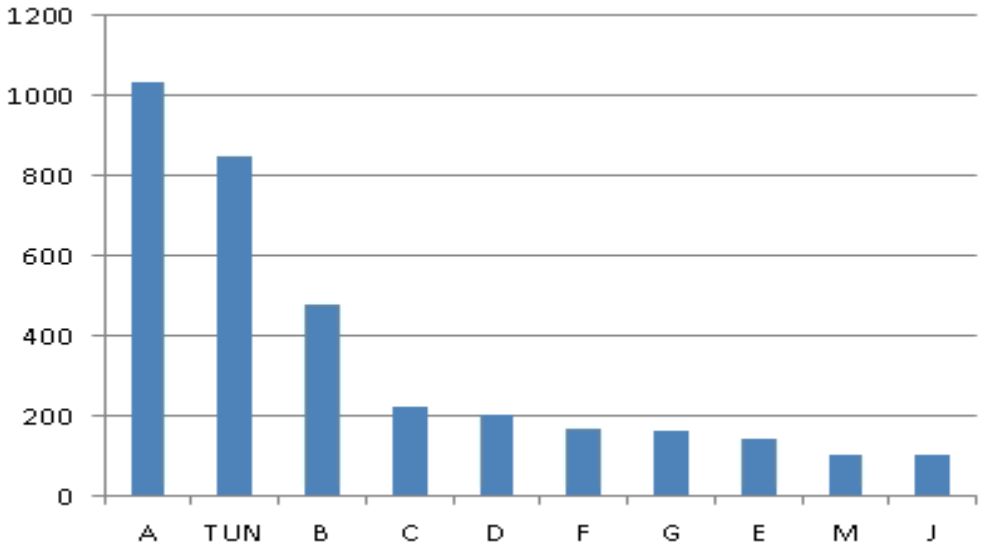
Σχήμα 5-3. Ο αριθμός των FQDNs με παράθυρο δείγματος 10 λεπτών, κατά την διάρκεια του DNS tunneling

Το σχήμα 5-3 είναι ένα παράθυρο δέκα λεπτών στο οποίο ένα αρχείο 122K μεταφέρθηκε με τη χρήση του DNS tunneling. Όπως φαίνεται η στήλη "TUN" είναι σημαντικά μεγαλύτερη από όλες τις άλλες. Το domain με την ετικέτα "TUN" είναι εκείνο που χρησιμοποιήθηκε για το DNS tunneling. Αυτό δείχνει ότι το DNS tunneling μπορεί να ανιχνευθεί με τη χρησιμοποίηση της αρίθμησης των μοναδικών FQDNs ανά root domain.



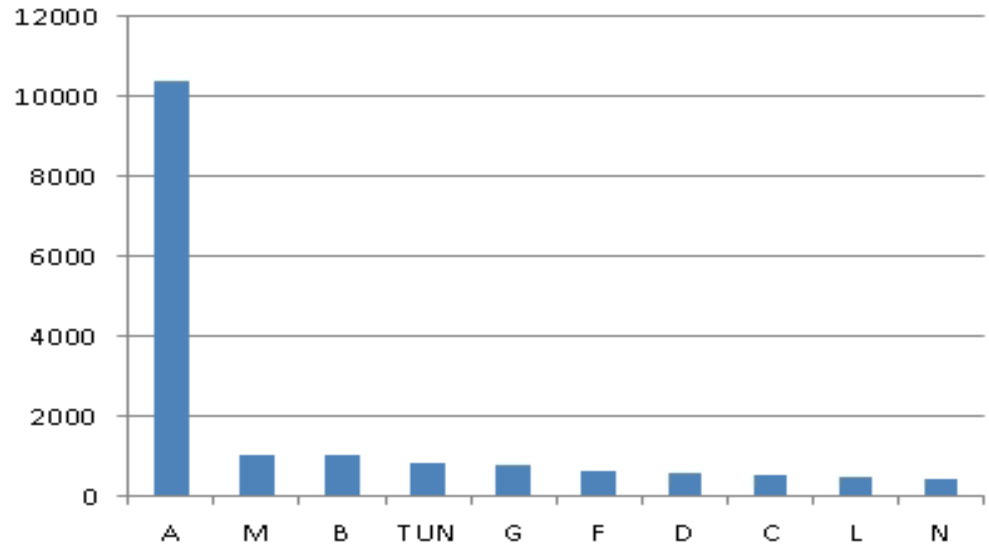
Σχήμα 5-4. Ο αριθμός των FQDNs με παράθυρο δείγματος 10 λεπτών, μετά την μεταφορά του αρχείου με DNS tunneling.

Το σχήμα 5-4 παρουσιάζει το παράθυρο των δέκα λεπτών μετά από τη μεταφορά του αρχείου των 122K. Υπάρχει ακόμα DNS κυκλοφορία του domain "TUN". Αυτή είναι από τη δραστηριότητα της εφαρμογής DNScat-B που χρησιμοποιήθηκε και την προσπάθεια της να κρατήσει ενεργό το tunnel. Στο παράθυρο αυτής της χρονικής περιόδου, το επίπεδο δραστηριότητας του tunnel είναι αρκετά χαμηλότερο σε σχέση με το σχήμα 5-3 δεδομένου ότι δεν γίνεται μεταφορά κάποιου αρχείου. Ακόμη όμως και με αυτό το χαμηλό επίπεδο δραστηριότητας, το "TUN" root domain βρίσκεται στις τέσσερις πρώτες θέσεις των μοναδικών FQDNs.



Σχήμα 5-5. Ο αριθμός των FQDNs με παράθυρο δείγματος 1 ώρας , συμπεριλαμβανομένου του DNS tunneling

Το σχήμα 5-5 παρουσιάζει τον αριθμό των μοναδικών FQDNs με παράθυρο δειγματοληψίας 1 ώρας. Όπως φαίνεται μόνο η στήλη με ετικέτα "A" που είναι μια υπηρεσία ασφάλειας αρχείων υπερτερεί της στήλης "TUN".



Σχήμα 5-6. Ο αριθμός των FQDNs με παράθυρο δείγματος 9 ωρών , συμπεριλαμβανομένου του DNS tunneling

Το σχήμα 5-6 παρουσιάζει τον αριθμό των μοναδικών FQDNs σε μια ολόκληρη ημέρα εργασίας (8πμ-5μμ τοπική ώρα). Η στήλη Α είναι σημαντικά υψηλότερη από τις υπόλοιπες. Αυτό είναι αναμενόμενο αφού για αυτήν την υπηρεσία ασφάλειας σε κάθε αίτημα για ένα μοναδικό αρχείο θα παράγει ένα μοναδικό FQDN. Η στήλη με το domain που χρησιμοποιήθηκε για το tunneling είναι η τέταρτη υψηλότερη ακόμα κι αν ήταν για μερικά λεπτά σε σύγκριση με την δραστηριότητα για ενεά ώρες των άλλων domain.
Συνεπώς ακόμη και λίγα λεπτά εφαρμογής DNS tunneling είναι αρκετά για να μπορεί κάποιος να την ανιχνεύσει , εξετάζοντας ακόμα και τα αποτελέσματα των δεδομένων από μια πλήρη ημέρα.

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα

Η ανάγκη για ασύρματη δικτύωση γίνεται ολοένα και επιτακτικότερη. Η τεχνολογία αυτή κερδίζει καθημερινά νέους χρήστες. Ενώ ξεκίνησε διστακτικά μόλις πριν λίγα χρόνια, κατάφερε σε μικρό χρονικό διάστημα να εξελιχθεί και να πετύχει μεγάλες ταχύτητες μεταφοράς των δεδομένων και ευρεία κάλυψη.

Εξαιτίας της γρήγορης εξάπλωσης της τεχνολογίας της μικρής της ηλικίας και της φύσης του μέσου που χρησιμοποιεί πολλά ζητήματα ασφαλείας προέκυψαν. Σημαντική βοήθεια στην ασφάλεια προσφέρουν τα πρωτόκολλα ασύρματης ασφάλειας WEP , WAP, WPA2, η επικύρωση των χρηστών και οι μηχανισμοί κρυπτογράφησης TKIP και AES.

Παρά τους μηχανισμούς ασφαλείας ένας διαχειριστής ενός ασύρματου δικτύου πρέπει να είναι πάντα σε επιφυλακή και να ακολουθεί τον «τροχό ασφαλείας». Οι επιθέσεις και απειλές για ασύρματα δίκτυα μπορεί να είναι καθημερινό φαινόμενο. Μια τέτοια νέα απειλή για τα ασύρματα δίκτυα είναι και το DNS tunneling.

Ένας μεγάλος αριθμός εφαρμογών DNS tunneling υπάρχει με ένα ευρύ φάσμα δυνατοτήτων. Παρέχουν ένα συγκεκαλυμμένο κανάλι για κακόβουλες δραστηριότητες που αποτελεί μια σημαντική απειλή για τους οργανισμούς. Αυτές οι απειλές μπορούν να μετριαστούν χρησιμοποιώντας τις τεχνικές ανίχνευσης ανάλυσης της κυκλοφορίας και ανάλυσης φορτίου (payload).

Παρουσιάστηκαν παραπάνω, πάνω από δώδεκα διαφορετικές υλοποιήσεις DNS tunneling. Ενώ ορισμένες υλοποιήσεις είναι διαθέσιμες εδώ και αρκετά έτη, άλλες έχουν αναπτυχθεί πρόσφατα με τη βελτιωμένες ικανότητες. Παραδείγματος χάριν, το Heyoka χρησιμοποιεί επιπλέον μια τεχνική εξαπάτησης ώστε να κάνει την τελική συσκευή που το χρησιμοποιεί , αόρατη. Επιπλέον, η ικανότητα για DNS tunneling έγινε διαθέσιμη ως τμήμα των εργαλείων "δοκιμής διείσδυσης" του Metasploit και του squeeza.

Παρουσιάστηκε αναλυτικά η δημιουργία ενός DNS tunneling με την χρήση της εφαρμογής Iodine προκειμένου να παρακαμφθεί η πληρωμένη για το Διαδίκτυο πρόσβαση σ ένα Hotspot.Η υλοποίηση της επίθεσης έγινε με σχετικά μικρή τεχνική υποδομή , με την χρήση δύο υπολογιστών και μερικών μόνο προγραμμάτων. Διαπιστώνουμε λοιπόν πόσο εύκολα κάμπτεται η ασφάλεια ενός ασύρματου δικτύου.

Το DNS tunneling αποτελεί μια σημαντική απειλή για τους οργανισμούς. Οι δύο κύριες απειλές του DNS tunneling είναι ο έλεγχος των συμβιβασμένων τελικών συσκευών και η υποκλοπή δεδομένων από αυτούς. Ο έλεγχος μπορεί να επιτευχθεί με DNS tunnelling και την χρήση των κακόβουλων λογισμικών όπως το Feederbot και το Moto. Ο έλεγχος επίσης μπορεί να περιλαμβάνει την πλήρη απομακρυσμένη πρόσβαση σε μια τελική συσκευή. Η άλλη απειλή είναι η υποκλοπή και εξαγωγή δεδομένων. Το DNS tunneling παρέχει ένα συγκεκαλυμμένο κανάλι για παράνομη

εξαγωγή δεδομένων. Αν και είναι ανεπαρκές για τη μεταφορά δεδομένων το DNS tunneling μπορεί να χρησιμοποιηθεί για να υποκλαπούν εύκολα μεγάλης αξίας στοιχεία όπως κωδικοί πρόσβασης ή ευαίσθητα έγγραφα. Εάν η κίνηση δεν παρακολουθείται από έναν υπεύθυνο διαχειριστή και το DNS tunneling μπορεί να χρησιμοποιηθεί για αρκετή ώρα τότε μεγάλα ποσά δεδομένων μπορούν να εξαχθούν.

Η απειλή DNS tunneling μπορεί να μετριαστεί χρησιμοποιώντας τις τεχνικές ανίχνευσης ανάλυσης της κυκλοφορίας και ανάλυσης φορτίου (payload).
Η ανάλυση φορτίου μπορεί να χρησιμοποιηθεί για να ανιχνεύσει το DNS tunneling χρησιμοποιώντας "υπογραφές" βασισμένες στις ιδιότητες των ξεχωριστών DNS φορτίων όπως τα περιεχόμενα του FQDN. Η ανάλυση φορτίου είναι αποτελεσματικότερη για τον εντοπισμό γνωστών υλοποιήσεων DNS tunneling .Η ανάλυση κυκλοφορίας είναι η άλλη τεχνική ανίχνευσης. Η ανάλυση κυκλοφορίας μπορεί να χρησιμοποιηθεί για να ανιχνεύσει DNS tunneling βασιζόμενη στα χαρακτηριστικά της γενικής κυκλοφορίας. Χρησιμοποιώντας την ανάλυσης της κυκλοφορίας, ένας καθολικός ανιχνευτής DNS tunneling μπορεί να εφαρμοστεί. Αυτό επιτυγχάνεται με τον έλεγχο του αριθμού των μοναδικών FQDNs για ένα root domain. Αυτή η τεχνική είναι ανεξάρτητη από τον τύπο record, την κωδικοποίηση μήκος των DNS ετικετών και το μήκος του FQDN. Αυτή η τεχνική λειτουργεί με επιτυχία ωστόσο, υπάρχει χώρος για βελτίωση. Η μέθοδος «αρίθμησης μοναδικών FQDNS» θα μπορούσε να βελτιωθεί με τη βελτιστοποίηση των συστατικών και των αλγόριθμων της για να μειωθούν οι απαιτήσεις σε υπολογιστικούς πόρους.
Οι πρακτικές μέθοδοι ανίχνευσης που παρουσιάστηκαν μπορούν να χρησιμοποιηθούν για τον επιτυχή εντοπισμό του DNS tunneling.

Εάν οι οργανισμοί και οι επιχειρήσεις εφαρμόσουν αυτές τις μεθόδους μπορούν να μειώσουν τον κίνδυνο που συνδέεται με το DNS tunneling!

Βιβλιογραφικές Αναφορές

Andersson, B. (2010). *iodine by kryo*. Retrieved from http://code.kryo.se/iodine/

Antonakakis, M. (2012). *Dgas and cyber-criminals: A case study*. Retrieved from https://www.damballa.com/downloads/r_pubs/RN_DGAs-and-Cyber-Criminals-A-Case-Study.pdf

Bianco, D. (2006, May 3). A traffic-analysis approach to detecting dns tunnels. Retrieved from http://blog.vorant.com/2006/05/traffic-analysis-approach-to-detecting.html

Bienaime, P. (2011). *dnscapy, dns tunneling with scapy*. Retrieved from http://code.google.com/p/dnscapy/

Bilge, L. (2011). *Exposure: Finding malicious domains using passive dns analysis*. Retrieved from http://www.syssec-project.eu/media/page-media/3/bilgendss11. Pdf

Born, K. (2010a). *Psudp: A passive approach to network-wide covert communication*. Retrieved from http://www.kentonborn.com/sites/default/files/psudp_born_slides_bh_2010.pdf

Born, K. (2010b). *Dns tunnel detection using character frequency analysis*. Retrieved from http://www.kentonborn.com/sites/default/files/dns_cfa.pdf

Bressler, D. (2012, December). *nwmaltego*. Retrieved from https://github.com/bostonlink/nwmaltego

Buetler, I. (2009). Covert Channel Attacks – Inside-out Attacks, Compass Security Retrieved from: www.csnc.ch/misc/files/publications/covert_channel_csnc_v1.0.pdf

Chamberland, M. (2009). Snort rules for Iodine Covert DNS Tunnel Detection. Retrievedvfrom: http://blog.securitywire.com/2009/07/26/snort-rules-for-iodine-covert-dnstunnel-detection

Cisco Networking Academy , https://www.netacad.com
Curriculums CCNA CCNP

Couture, E. (2010, August 19). *Covert channels*. Retrieved from http://www.sans.org/reading_room/whitepapers/detection/covert-channels_33413

Dembour, O. (2008, November 3). Dns2tcp. Retrieved from http://www.hsc.fr/ressources/outils/dns2tcp/index.html.en

Dietrich, C. (2011, September 2). *Feederbot - a bot using dns as carrier for its c&c*. Retrieved from http://blog.cj2s.de/archives/28-Feederbot-a-bot-using-DNS-ascarrier-for-its-CC.html

Dusi, M., Crotti, M., F. Gringoli, Salgarelli, L. (2008). Detection of Encrypted Tunnels across Network Boundaries, Proceedings of the 43rd IEEE International Conference on Communications.

Dusi, M., Crotti, M., Gingili, F., Salgarelli, L. (2009). Tunnel Hunter: Detecting Application-Layer Tunnels with Statistical Fingerprinting. Elsevier "Computer Networks" (COMNET) Vol 53.

Fry, C. (2009). *Security monitoring, proven methods for incident detection on enterprise networks*. (1st ed., p. 28). Sebastopol, CA, USA: O'Reilly Media.

Guy, J. (2009, February 13). *dns part ii: visualization*. Retrieved from http://armatum.com/blog/2009/dns-part-ii/

Gregg, M. (2007). Hack the Stack: Using Snort and Ethereal to Master The 8 Layers of An Insecure Network, Syngress Publishing.

Hassinen Timo, Overview of WLAN Security, Helsinki University of Technology

IEEE Standards Association, http://standards.ieee.org

Kunwar, N. (2006). DNS Amplification Attack. Retrieved from: www.nirlog.com/2006/03/28/ dns-amplification-attack.

Maniscalchi, J. (2009). Threat vs Vulnerability vs Risk. Retrieved from: www.digitalthreat.net/2009 /06/threat-vs-vulnerability-vs-risk.

Mullaney, C. (2011, August 31). *Morto worm sets a (dns) record*. Retrieved from http://www.symantec.com/connect/blogs/morto-worm-sets-dns-record

Nussbaum, L. (2009). *On robust covert channels inside dns*. Retrieved from http://hal.inria.fr/docs/00/42/56/16/PDF/tuns-sec09-article.pdf

NSTX. (2002, September 22). NSTX -- tunneling network-packets over dns - summary.Retrieved from http://savannah.nongnu.org/projects/nstx/

Pearson, O. (1998, April 13). *Dns tunnel - through bastion hosts*. Retrieved from http://archives.neohapsis.com/archives/bugtraq/1998_2/0079.html

Pietraszek, T. (2004, October 31). Dnscat. Retrieved from http://tadek.pietraszek.org/projects/DNScat/

Rasmussen, R. (2012, April 03). *Do you know what your dns resolver is doing right now?*. Retrieved from http://www.securityweek.com/do-you-know-whatyour-dns-resolver-doing-right-now

Revelli, A. (2009). *Playing with heyoka*. Retrieved from http://heyoka.sourceforge.net/heyoka-shakacon2009.pdf

Skoudis, E. (2012, February 29). The six most dangerous new attack techniques and what's coming next?. Retrieved from https://blogs.sans.org/pentesting/files/2012/03/RSA-2012-EXP-108-Skoudis-Ullrich.pdf

Smith, J.C. (2001). Covert Channels. Retrieved from: www.sans.org/infosecFAQ/covertchannels /covert_shells.htm .

Stallings William (2007) Wireless Communications & Networks

Van Leijenhorst, T. (2008). *On the viability and performance of dns tunneling*. Retrieved from http://www.uow.edu.au/~kwanwu/DNSTunnel.pdf

Van Horenbeeck, M. (2006). Dns tunneling. Retrieved from http://web.archive.org/web/20060613210141/http://www.daemon.be/maarten/dnstunnel.html

Van Horenbeeck, M. (2010). DNS Tunneling. Retrieved from: http://www.daemon.be/maarten/ dnstunnel.html

Vixie, P. (1999, August). *Extension mechanisms for dns (edns0)*. Retrieved from http://www.ietf.org/rfc/rfc2671.txt

Wong, M. (2006, April). *Sender policy framework (spf) for authorizing use of domains in e-mail, version 1*. Retrieved from http://tools.ietf.org/html/rfc4408

Zander, S., Armitage, G., Branch, P. (2007). A Survey of Covert Channels and Countermeasures in Computer Network Protocols, IEEE Communications Surveys and Tutorials, Vol. 9, No. 3.

Zander, S., Armitage, G., Branch, P. (2007). Covert Channels and Countermeasures in Computer Network Protocols, IEEE Communications Magazine, Vol. 45, No. 12.

Zdrnja, B. (2007). *Passive monitoring of dns anomolies*. Retrieved from http://www.caida.org/publications/papers/2007/dns_anomalies/dns_anomalies.pdf

Βικιπαίδεια, http://el.wikipedia.org