Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

'Επιθέσεις και τεχνικές προστασίας σε ένα Wireless Network 802.11 '

ΚΑΤΕΡΙΝΑ Π. ΓΑΒΡΙΛΑΚΗ (ΑΜ 1612)
E-mail: gkat85@yahoo.gr

Ηράκλειο – 8/12/2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Υπεύθυνη δήλωση: *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι Κρήτης.*

Ευχαριστίες

Καταρχάς θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον κ. Χαράλαμπο Μανιφάβα, επιβλέποντα αυτής της πτυχιακής εργασίας για την καθοδήγηση, τις συμβουλές, καθώς και για το υλικό που μου πρόσφερε για την εκπόνηση της εργασίας αυτής. Έπειτα ένα μεγάλο ευχαριστώ στην οικογένειά μου για την ηθική και ψυχολογική συμπαράσταση όλα τα χρόνια των σπουδών μου, και στους φίλους μου Σπύρο, Αγγελική, Μαρία για τη βοήθεια τους.

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Συγγραφέας	Λεπτομέρειες
11/2/2009	1.0	Κατερίνα Γαβριλάκη	Εισαγωγικά για τα ασύρματα δίκτυα και μελέτη των μηχανισμών ασφάλειας.
3/3/2009	1.1	Κατερίνα Γαβριλάκη	Μελέτη των ειδών επιθέσεων MAC Spoofing και Sniffing.
14/9/2009	1.2	Κατερίνα Γαβριλάκη	Μελέτη των επιθέσεων wep cracking, Café latte, man-in-the middle και DOS και των μεθόδων ασφαλείας.
15/11/2009	Τελική	Κατερίνα Γαβριλάκη	Συμπλήρωση 802.11 προτύπων, μεγέθυνση εικόνων, διαδικασία ρύθμισης WEP στα Windows, ολοκλήρωση 7 κεφαλαίου.

Περίληψη

Σκοπός αυτής της πτυχιακής εργασίας είναι να εξετάσει τα θέματα ασφάλειας ενός ασύρματου δικτύου που βασίζεται στο πρωτόκολλο IEEE 802.11, να υλοποιηθούν τα πιο γνωστά είδη επιθέσεων και να προταθούν τα αντίστοιχα μέτρα ασφάλειας. Αναλυτικότερα τα είδη των επιθέσεων που θα μελετηθούν είναι: WEP cracking, MAC spoofing, Sniffing, Man-in-the-middle attack, Denial of Service και Cafe Latte attack. Τα είδη άμυνας που θα μελετηθούν είναι Access control, τα Intrusion Detection συστήματα, η χρησιμοποίηση της End-to-End Encryption, η επιλογή MAC Filtering, η υλοποίηση των VPNs και το SSID Hiding.

Το πρώτο κεφάλαιο είναι εισαγωγικό, αναφερόμαστε γενικά στα ασύρματα δίκτυα, στο σκοπό της συγκεκριμένης εργασίας, και παρουσιάζουμε περιληπτικά τα θέματα που θα αναλύσουμε στα επόμενα κεφάλαια, για να έχουμε μια γενική εικόνα της εργασίας. Στο δεύτερο κεφάλαιο υπάρχει μια σύντομη ιστορική αναδρομή των ασύρματων δικτύων. Ακολουθούν σε συντομία τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζουν τα ασύρματα δίκτυα όταν συγκρίνονται με τα ενσύρματα τοπικά δίκτυα, οι εφαρμογές στις οποίες χρησιμοποιούνται ευρέως, καθώς και τα διάφορα προβλήματα που μπορεί να παρουσιαστούν με την χρήση τους. Στο τέλος του κεφαλαίου αυτού μαθαίνουμε για τα βασικά δομικά στοιχεία που είναι απαραίτητα για να υλοποιηθεί ένα ασύρματο δίκτυο.

Στο τρίτο κεφάλαιο γίνεται η παρουσίαση του 802.11 πρωτοκόλλου. Αναφερόμαστε στα πρότυπα που αποτελούν την οικογένεια 802.11 και τα χαρακτηριστικά τους. Αναλύουμε τις τοπολογίες BSS, IBSS και ESS που υποστηρίζει το πρότυπο, και τα βασικά μέρη της αρχιτεκτονικής που καθορίζει τον τρόπο λειτουργίας του δικτύου. Στο επόμενο κεφάλαιο περιγράφονται οι μηχανισμοί ασφαλείας του 802.11. Γίνεται εισαγωγή στις έννοιες επικύρωση και μυστικότητα. Παρατίθεται εκτενής περιγραφή του βασικού μηχανισμού κρυπτογράφησης WEP, καθώς και οι αδυναμίες που παρουσιάζει. Αναφερόμαστε στις βελτιώσεις του WEP που δημιουργήθηκαν, στην 802.1X επικύρωση, στους μηχανισμούς EAP και RADIUS καθώς και στους διάδοχους του WEP, το WPA και το WPA2.

Στο πέμπτο κεφάλαιο παρουσιάζονται τα βασικά είδη επιθέσεων που συναντώνται στις μέρες μας, στα ασύρματα δίκτυα και υλοποιούνται μερικές από αυτές. Βλέπουμε πόσο εύκολο είναι να σπάσει ο αλγόριθμος WEP, με το WEP cracking, που είναι και η πιο γνωστή επίθεση σε ασύρματα δίκτυα. Επίσης βλέπουμε και άλλα είδη επιθέσεων όπως το MAC spoofing και το sniffing, ενώ μελετώνται και πιο σύνθετα είδη επιθέσεων όπως Man-in-the-middle, Denial of Service και Cafe Latte.

Στο προτελευταίο κεφάλαιο περιγράφονται πρακτικά οι βασικές μέθοδοι ασφαλείας που πρέπει να εφαρμοστούν για να αντιμετωπιστούν τα βασικά είδη επιθέσεων που περιγράφτηκαν παραπάνω. Πως εφαρμόζουμε σωστά Access control, τι είναι τα VPNs και πως τα υλοποιούμε, τα Intrusion Detection συστήματα, πως γίνεται το MAC Filtering και διάφορα άλλα ώστε να επιτυγχάνουμε υψηλό βαθμό ασφάλειας. Τέλος παρατίθενται τα συμπεράσματα που προκύπτουν από την παρούσα εργασία.

Abstract

The purpose of this diploma thesis is to examine the security of a wireless network based on IEEE 802.11 protocol, to achieve the best known types of attacks and propose the corresponding security measures. Detail the types of attacks that will be studied are: WEP cracking, MAC spoofing, Sniffing, Man-in-the-middle attack, Denial of Service and Cafe Latte attack. The types of defense that will be studied are Access control, the Intrusion Detection systems, using End-to-End Encryption, how to enable MAC Filtering, the implementation of VPNs and the SSID Hiding.

The first chapter is introduction. We refer generally to wireless networks, the purpose of this work and summarizing the issues to be analyzed in later chapters, to have an overview of the work. The second chapter is a brief history of wireless networks. Here are briefly the advantages and disadvantages of wireless networks when compared with wired LANs, applications which are widely used, and the various problems that may occur with their use. At the end of this chapter we learn about the key components necessary to create a wireless network.

The third chapter is the presentation of the 802.11 protocol. We refer to the standards of the 802.11 family and their characteristics. We analyze the topologies BSS, IBSS and ESS supports by the standard and essential parts of the 802.11 architecture. The next chapter describes the security mechanisms of 802.11. It is import to validate concepts and secrecy. We present a comprehensive description of the basic mechanism for encryption WEP, as well as weaknesses in. We refer to improvements of WEP created in 802.1X ratification mechanisms EAP and RADIUS, and the successor of WEP, the WPA and WPA2.

The fifth chapter presents the main types of attacks which are found, today in wireless networks and implemented some of them. We see how easy it is to break the WEP algorithm, with WEP cracking, which is the best known attack on wireless networks. Also see other types of attacks such as MAC spoofing and sniffing, and studied and more complex types of attacks like Man-in-the-middle, Denial of Service and Cafe Latte.

The penultimate chapter describes the basic methods of practical safety measures to be implemented to address the main types of attacks described above. How to properly apply Access control, what are the VPNs and how to implement, the Intrusion Detection systems, that is the MAC Filtering and several others to achieve a high degree of security. Finally we present the conclusions of this work.

Πίνακας περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Είναι εμφανές ότι η αρχή της τρίτης χιλιετίας μπορεί να χαρακτηριστεί ως δικτυακή εποχή. Η εξάπλωση των δικτύων υπολογιστών συντελείται με τέτοιο ρυθμό, που πλέον έχει γίνει αναπόσπαστο κομμάτι της καθημερινής ζωής του σύγχρονου ανθρώπου. Οι υπολογιστές μετατρέπονται από μεμονωμένες μονάδες σε μέρη ενός ευρύτερου συνόλου. Αιτία αυτής της εξάπλωσης είναι η διαρκής ανάγκη για γρηγορότερη και πιο αποτελεσματική διακίνηση της πληροφορίας.

Ένα δίκτυο υπολογιστών αποτελείται από δύο ή περισσότερους υπολογιστές συνδεδεμένους μεταξύ τους έτσι ώστε να ανταλλάσουν πληροφορίες. Η σύνδεση μπορεί να είναι ενσύρματη ή ασύρματη. Ένα ασύρματο δίκτυο δεν χρησιμοποιεί καλώδια για τις συνδέσεις των υπολογιστών. Αντί του καλωδίου χρησιμοποιείται μετάδοση μέσω ειδικά διαμορφωμένων οπτικών, υπέρυθρων ή ακόμα και ραδιοκυματικών σημάτων. Η έννοια του ασύρματου δικτύου ορίζεται ως εξής:

Ορισμός: Ασύρματο δίκτυο. Ως ασύρματο δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία κάθε φορά εξαρτάται από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο.

Η συνηθισμένη ακτίνα δράσης ενός ασύρματου δικτύου εκτείνεται σε αρκετά μέτρα, η οποία είναι ικανή να διασυνδέσει από τους ορόφους μιας πολυκατοικίας μέχρι τα κτήρια μιας πανεπιστημιούπολης. Η διασύνδεση ενός ασύρματου τοπικού δικτύου με ένα αντίστοιχο ενσύρματο μπορεί να αυξήσει σημαντικά την ακτίνα δράσης του ενσύρματου. Τα ασύρματα δίκτυα τοπικής περιοχής, συχνά αναφέρονται ως WLAN (Wireless Local Area Network) ή Wi-Fi δίκτυα.

Ο τομέας των ασύρματων δικτύων είναι ένας από τους ταχύτερα αναπτυσσόμενους κλάδους των τηλεπικοινωνιών και αποτελεί ένα πεδίο εξαιρετικά πρόσφορο για έρευνα. Η εξέλιξη των ασύρματων δικτύων ακολουθεί αλματώδεις ρυθμούς, καθιστώντας τα διαρκώς πιο αποτελεσματικά και επικερδή. Οι άνθρωποι πλέον τα εγκαθιστούν όλο και περισσότερο στα γραφεία τους, στα ξενοδοχεία, τις καφετέριες και τα σπίτια τους. Τα ασύρματα δίκτυα προσφέρουν εμπιστευτικότητα και κινητικότητα. Πολλές φορές η ασύρματη δικτύωση μπορεί να είναι και λιγότερο δαπανηρή για την εφαρμογή από ότι η ενσύρματη.

Με δεδομένη τη ζήτηση των καταναλωτών, τις λύσεις των προμηθευτών και τα βιομηχανικά πρότυπα, η ασύρματη δικτύωση ήρθε για να μείνει. Αλλά πόσο ασφαλής είναι αυτή η τεχνολογία; Τα ασύρματα δίκτυα βασίζονται στο πρότυπο IEEE 802.11 και παρόλο τις ευκολίες που μας προσφέρουν, μαζί με αυτές υπάρχουν και αρκετοί κίνδυνοι που παρουσιάζονται όσον αφορά θέματα ασφαλείας. Η κατανόηση όμως των διαφόρων απειλών και τρωτών σημείων του 802.11, μας βοηθάει ώστε να προστατευτούμε και να τα κάνουμε περισσότερο ασφαλή.

1.2 Σκοπός

Η εργασία αυτή εστιάζει στον τομέα της ασφάλειας των ασύρματων δικτύων που βασίζονται στο πρωτόκολλο IEEE 802.11. Γι' αυτό το λόγο παρουσιάζονται μερικά από τα ποιο γνωστά είδη επιθέσεων σε ασύρματα δίκτυα, ώστε να μπορούμε να κατανοήσουμε εύκολα τις αδυναμίες τους, καθώς και τα βασικά μέτρα προστασίας που πρέπει να λαμβάνουμε ώστε να προστατεύουμε το δίκτυό μας από τέτοιου είδους επιθέσεις.

Πιο συγκεκριμένα αναλύονται τα παρακάτω θέματα:

1. Πλεονεκτήματα και μειονεκτήματα που παρουσιάζονται με την χρησιμοποίηση των ασύρματων δικτύων σε σχέση με τα τοπικά ενσύρματα.
2. Οι εφαρμογές τους και τα βασικά δομικά στοιχεία που τα αποτελούν.
3. Τα χαρακτηριστικά του IEEE 802.11 προτύπου ασύρματης δικτύωσης.
4. Η τοπολογία και η αρχιτεκτονική του 802.11
5. Οι βασικοί μηχανισμοί ασφαλείας του 802.11 προτύπου, όπως:
    - Επικύρωση ανοιχτού κλειδιού.
    - Επικύρωση δημοσίου κλειδιού.
    - Αλγόριθμος κρυπτογράφησης WEP.
    - 802.1X επικύρωση.
    - Τα πρωτόκολλα EAP και RADIUS.
    - WPA και WPA2.
6. Βασικά είδη επιθέσεων, όπως:
    - WEP cracking
    - MAC spoofing
    - Sniffing
    - Man-in-the-middle
    - Denial-of-service
    - Café latte attack
7. Διάφοροι μέθοδοι ασφάλειας όπως:
    - Access control
    - Intrusion Detection
    - End-to-end encryption
    - MAC filtering
    - VPN
    - SSID Hiding

Θα υλοποιηθούν και θα αναλυθούν οι επιθέσεις WEP cracking, MAC spoofing και Sniffing. Επίσης αναλύονται λεπτομερέστερα ώστε να κατανοηθούν και τα άλλα τρία είδη επιθέσεων, η επίθεση Man-in-the-middle, οι επιθέσεις DOS και η σχετικά πιο καινούρια επίθεση Café Latte. Αντίστοιχα θα υλοποιηθούν και θα αναλυθούν και τα παραπάνω μέτρα ασφαλείας που αναφέραμε, access control, Intrusion Detection, End-to-End encryption, MAC filtering, VPN και SSID Hiding, ώστε να μπορούμε να επιτύχουμε στο ασύρματο δίκτυο μας το μέγιστο δυνατό βαθμό ασφάλειας. Τέλος παρατίθενται τα συμπεράσματα που προκύπτουν από την παρούσα εργασία.

1.3 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος	Σύντομη περιγραφή
1	Εισαγωγή	Γενικά για τα ασύρματα δίκτυα, σύντομη περιγραφή των θεμάτων που εξετάζονται παρακάτω και σχεδιάγραμμα αναφοράς.
2	Γενικά για τα ασύρματα δίκτυα	Ιστορία των ασύρματων δικτύων, πλεονεκτήματα και μειονεκτήματα σε σχέση με τα ενσύρματα, δομικά στοιχεία που τα αποτελούν.
3	Το 802.11 πρότυπο ασύρματης δικτύωσης	Παρουσίαση των 802.11 προτύπων, τα χαρακτηριστικά του 802.11, η τοπολογία και η αρχιτεκτονική που παρουσιάζει.
4	Μηχανισμοί ασφαλείας	Περιγραφή των μηχανισμών ασφαλείας του 802.11 προτύπου. Ανάλυση των μεθόδων επικύρωσης, του αλγόριθμου κρυπτογράφησης WEP καθώς και άλλων μεθόδων κρυπτογράφησης όπως το 802.1X, το EAP, RADIUS, WEP, WPA και WPA2.
5	Σπάζοντας την ασύρματη ασφάλεια	Παρουσίαση των πιο γνωστών επιθέσεων και υλοποίηση μερικών από αυτών, όπως της επίθεσης WEP cracking, MAC Spoofing και Sniffing.
6	Μέθοδοι ασφάλειας	Πρόταση αντίστοιχων μέτρων ασφαλείας για την αντιμετώπιση των παραπάνω επιθέσεων. Πως εφαρμόζουμε access control, τι είναι τα Intrusion Detection συστήματα, end-to-end encryption, MAC filtering, VPN, και SSID hiding.
7	Συμπεράσματα	Παρουσίαση των συμπερασμάτων που προκύπτουν από την παρούσα εργασία.
8	Βιβλιογραφία	Αναφορά των πηγών που χρησιμοποιήθηκαν για την δημιουργία της παρούσας εργασίας.
Παράρτημα Α	Συντομογραφίες	Η σημασία των συντομογραφιών που υπάρχουν σε διάφορα σημεία της εργασίας.

Κεφάλαιο 2 Γενικά για τα ασύρματα δίκτυα

2.1 Η ασύρματη επανάσταση

Το 1970 στο πανεπιστήμιο της Χαβάη υπό την επίβλεψη του Norman Abramson αναπτύχθηκε το πρώτο δίκτυο επικοινωνιών στον κόσμο, με τη χρήση υπολογιστή χαμηλού κόστους και το οποίο ονομάστηκε ALOHAnet[1]. Το σύστημα χρησιμοποιούσε αμφίδρομη τοπολογία αστέρα και περιλάμβανε επτά υπολογιστές, τοποθετημένους σε τέσσερα νησιά, οι οποίοι επικοινωνούσαν με τον κεντρικό υπολογιστή του Oahu Island, με τη βοήθεια ραδιοκυμάτων.

Το 1979 οι FR Gfeller και U Bapst δημοσίευσαν στο IEEE proceedings αναφορά, σχετικά με ένα πειραματικό ασύρματο τοπικό δίκτυο, που έκανε τη χρήση διάχυσης υπέρυθρων επικοινωνιών. Λίγο αργότερα, το 1980, ο P. Ferrert, αναφέρθηκε σε μία πειραματική εφαρμογή ενιαίου κώδικα εκτεταμένου φάσματος ραδιοφώνου για ασύρματες επικοινωνίες σε τερματικό, στην Εθνική Επιτροπή Τηλεπικοινωνιών IEEE Διάσκεψης.

Η πρώτη γενιά ασύρματων modem δεδομένων, αναπτύχθηκε στις αρχές της δεκαετίας του 1980 από ραδιοερασιτέχνες, οι οποίοι συχνά αναφέρονταν σε αυτό το πακέτο, όπως το ραδιόφωνο. Θα προστεθεί μια φωνητική ζώνη επικοινωνίας δεδομένων modem, με ρυθμούς δεδομένων κατώτερους των 9600-bit / s, σε ένα ήδη υπάρχον σύστημα ραδιοπλοήγησης μικρής απόστασης.

Η δεύτερη γενιά ασύρματων modem αναπτύχθηκε αμέσως μετά την αναγγελία στην FCC (Federal Communications Commission)[2], για μη στρατιωτική χρήση του εκτεταμένου φάσματος τεχνολογίας στις πειραματικές ζώνες. Τα modem αυτά παρέχουν ρυθμούς δεδομένων σχετικά με τα ποσοστά της τάξης των εκατοντάδων Kbit / s. Η τρίτη γενιά ασύρματων modem είχε ως στόχο τη συμβατότητα με τα ήδη υπάρχοντα LANs, με ρυθμούς δεδομένων της τάξης του Mbit / s. Πολλές εταιρείες αναπτύσσονται στην τρίτη γενιά προϊόντων με δεδομένα τα ποσοστά άνω του 1 Mbit / s.

Το πρώτο από τα IEEE εργαστήρια πάνω στα WLAN (Wireless Local Area Networks) πραγματοποιήθηκε το 1991. Εκείνη την εποχή μόλις είχαν εμφανιστεί στην αγορά τα ασύρματα προϊόντα και η IEEE 802.11 επιτροπή μόλις είχε ξεκινήσει τις δραστηριότητές της για την ανάπτυξη ενός προτύπου για ασύρματα LANs. Η εστίαση της στο πρώτο εργαστήριο ήταν η αξιολόγηση των εναλλακτικών τεχνολογιών. Το 1997 η IEEE επικύρωσε τα 802.11 ασύρματα πρότυπα, εγκαθιδρύοντας έτσι ένα παγκόσμιο πρότυπο για την εκτέλεση και ανάπτυξη των ασύρματων τεχνολογιών. Ο ρυθμός μετάδοσης για το 802.11 ήταν 2 Mbps.

Ασύρματα δίκτυα είχαν χρησιμοποιηθεί στα νοσοκομεία, τα χρηματιστήρια, στις πανεπιστημιουπόλεις, σε LAN γέφυρες από σημείο σε σημείο, και σε ad-hoc

[1] http://en.wikipedia.org/wiki/ALOHAnet
[2] http://en.wikipedia.org/wiki/Federal_Communications_Commission

δικτύωση. Το πρότυπο IEEE 802.11, καθώς και οι παραλλαγές του, έχουν σημειώσει ταχεία πρόοδο. Αρχικά ο εξοπλισμός των WLAN ήταν τόσο ακριβός και γι αυτό το λόγο χρησιμοποιούταν ως εναλλακτική λύση, σε χώρους όπου η καλωδίωση ήταν δύσκολη ή αδύνατη, στις μέρες μας όμως η χρησιμότητά τους έχει αυξηθεί και χρησιμοποιούνται ευρέως. Στη συνέχεια του κεφαλαίου, αναλύουμε περισσότερο διεξοδικά τα κυριότερα θέματα που σχετίζονται με WLAN.

2.2 Πλεονεκτήματα ασύρματων δικτύων

Τα ασύρματα δίκτυα παρουσιάζουν διάφορα πλεονεκτήματα όταν συγκρίνονται με τα ενσύρματα τοπικά δίκτυα. Σε ένα ασύρματο δίκτυο είναι πιο εύκολο να προσθέσουμε ή να μετακινήσουμε ένα σταθμό ή να εγκαταστήσουμε ένα σημείο πρόσβασης, για να παρέχουμε συνδεσιμότητα σε περιοχές που είναι δύσκολο να καλωδιωθούν. Τα πλεονεκτήματα των ασύρματων δικτύων παρατίθενται παρακάτω:

- Ευκολία (Convenience): Η ασύρματη φύση αυτών των δικτύων επιτρέπει στους χρήστες να έχουν πρόσβαση στους πόρους ενός δικτύου, από σχεδόν οποιαδήποτε τοποθεσία χωρίς να πρέπει να βρίσκονται στο σπίτι ή στο γραφείο. Με την αύξηση της χρησιμοποίησης φορητών υπολογιστών, αυτό είναι ιδιαίτερα σημαντικό.

- Κινητικότητα (mobility): Τα WLAN μπορούν να παρέχουν την δυνατότητα στους χρήστες για πρόσβαση σε πληροφορίες ενώ βρίσκονται εν κίνηση εντός της εμβέλειας τους. Αυτή η ευχέρεια στην κίνηση υποστηρίζει την παραγωγικότητα και τις ευκαιρίες για εξυπηρέτηση, οι οποίες δεν είναι δυνατές με τα ενσύρματα δίκτυα.

- Ταχύτητα και ευελιξία εγκατάστασης**:** Η εγκατάσταση ενός WLAN εξαλείφει την ανάγκη της χρήσης των καλωδίων, η οποία συνήθως απαιτεί κόπο και χρόνο, ενώ η ασύρματη τεχνολογία επιτρέπει τη διασύνδεση δικτύων η οποία υπό άλλες συνθήκες θα ήταν αδύνατη.

- Μειωμένο κόστος κτήσης: Ενώ η αρχική επένδυση που απαιτείται για τον εξοπλισμό σε ένα WLAN μπορεί σε μερικές περιπτώσεις να είναι υψηλότερη από το αντίστοιχο κόστος για μια ενσύρματη σύνδεση, το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο, καθώς τα μακροπρόθεσμα κέρδη είναι πολύ μεγαλύτερα σε δυναμικά περιβάλλοντα όπου απαιτούνται πολύ συχνές μετακινήσεις και αλλαγές.

- Συμβατότητα: Τα WLAN μπορούν να μεταβληθούν σε μια ποικιλία από τύπους για να ικανοποιήσουν τις ανάγκες συγκεκριμένων εγκαταστάσεων και εφαρμογών. Οι διαμορφώσεις αλλάζουν εύκολα και επεκτείνονται από μικρά δίκτυα κατάλληλα για ένα μικρό αριθμό χρηστών μέχρι πλήρως ανεπτυγμένα δίκτυα που καλύπτουν εκατοντάδες χρήστες.

2.3 Εφαρμογές

Ανάλογα με τους χώρους που μπορούμε να δούμε οφέλη από τη χρήση των WLAN, συμπεριλαμβάνονται και οι παρακάτω:

1. Επιχειρήσεις: Με ένα WLAN οι εργαζόμενοι μπορούν να εκμεταλλευθούν το κινητό δίκτυο για e-mail, πρόσβαση σε αρχεία και αναζήτηση στο internet, ανεξάρτητα από την περιοχή που βρίσκεται το γραφείο, αλλά και από το αν βρίσκονται στο γραφείο ή όχι.

2. Εκπαίδευση: Με τη χρήση WLAN από τα ακαδημαϊκά ινστιτούτα οι φοιτητές μπορούν να έχουν πρόσβαση μέσω laptops στο πανεπιστημιακό δίκτυο, ενώ γίνεται και πιο προσιτή η εφαρμόσιμη τηλε-εκπαίδευση.

3. Υγεία: Με την χρήση ασύρματων φορητών υπολογιστών για την επεξεργασία σε πραγματικό χρόνο, οι εργαζόμενοι στον τομέα της υγείας αυξάνουν την παραγωγικότητα τους και την ποιότητα φροντίδας των ασθενών, καθώς εξαλείφονται προβλήματα όπως οι καθυστερήσεις και η γραφειοκρατία.

4. Επενδύσεις: Με ένα φορητό υπολογιστή ο οποίος συνδέεται με ένα ασύρματο τοπικό δίκτυο, οι επενδυτές μπορούν να δεχθούν πληροφορίες για τις τιμές από μια βάση δεδομένων σε πραγματικό χρόνο, βελτιώνοντας έτσι την ταχύτητα και την ποιότητα των συναλλαγών.

2.4 Προβλήματα

Η χρήση των ηλεκτρομαγνητικών κυμάτων για την μετάδοση των σημάτων κάνουν τα WLAN ευπαθή σε πολλά φαινόμενα παρεμβολής τα οποία αλλοιώνουν σε μικρότερο ή μεγαλύτερο βαθμό την επικοινωνία των ασύρματων χρηστών. Τα κυριότερα μειονεκτήματα που παρουσιάζουν είναι:

- Παρεμβολή λόγω πολλαπλών διαδρομών: Τα μεταδιδόμενα σήματα μπορούν να συνδυαστούν με τα ανακλώμενα από διάφορες επιφάνειες ή εμπόδια με αποτέλεσμα την φθορά ή την καταστροφή του σήματος που ανιχνεύεται από τον δέκτη. Το φαινόμενο αυτό είναι γνωστό ως "παρεμβολή λόγω πολλαπλών διαδρομών" ή "πολύοδη διάδοση".

- Path Loss: Το φαινόμενο path loss μεταξύ πομπού και δέκτη είναι ένα από τα σημαντικότερα στοιχεία που πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό ενός WLAN. Τα αναμενόμενα επίπεδα του path loss, τα οποία βασίζονται στην απόσταση μεταξύ του πομπού και του δέκτη, παρέχουν πολύτιμες πληροφορίες για τον καθορισμό των επιπέδων στην ισχύ εκπομπής, στην ευαισθησία του δέκτη και στον λόγο σήματος προς θόρυβο (SNR). Το πραγματικό path loss εξαρτάται από τη συχνότητα μετάδοσης και αυξάνει εκθετικά με την αύξηση της απόστασης μεταξύ του πομπού και του δέκτη.

- Παρεμβολές ραδιοσημάτων: Η διαδικασία της εκπομπής και λήψης ραδιοσημάτων και σημάτων laser μέσω του αέρα καθιστά τα ασύρματα συστήματα ευπαθή από το θόρυβο της ατμόσφαιρας και από τις μεταδόσεις άλλων συστημάτων που λειτουργούν στην ίδια μπάντα συχνοτήτων και λειτουργούν στον ίδιο φυσικό χώρο.

- Διαχείριση ενέργειας: Οι περισσότερες WLAN συσκευές από την πλευρά του χρήστη λειτουργούν με μπαταρίες που έχουν καθορισμένη διάρκεια ζωής. Η χρήση τους σε αυτές τις τηλεπικοινωνιακές εφαρμογές μειώνουν την αυτονομία τους.

- Ασυμβατότητα συστημάτων: Στην κατασκευή ενός WLAN θα πρέπει να ληφθεί υπόψη η ασυμβατότητα μεταξύ προϊόντων διαφορετικών κατασκευαστών, διαφορετικά το δίκτυο δεν θα λειτουργεί σωστά. Λόγοι ασυμβατότητας είναι οι εξής: χρήση διαφορετικής τεχνολογίας, η χρήση διαφορετικού φάσματος συχνοτήτων και η διαφορετική υλοποίηση.

- Ασφάλεια δικτύου: Η λειτουργία ενός ασύρματου δικτύου αντιστοιχεί στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν εμπεριέχει άλλες λειτουργίες όπως εγκατάσταση σύνδεσης από άκρο σε άκρο ή άλλες υπηρεσίες (πχ login), που προσφέρουν τα ανώτερα στρώματα. Για τον λόγο αυτόν το μόνο θέμα που σχετίζεται με την ασφάλεια και απασχολεί τα ασύρματα δίκτυα έχει να κάνει με θέματα ασφαλείας χαμηλότερων στρωμάτων όπως η κρυπτογράφηση των δεδομένων. Έχουν υλοποιηθεί διάφορες τεχνικές κωδικοποίησης, οι οποίες καθιστούν εξαιρετικά δύσκολη τη λήψη της μεταδιδόμενης πληροφορίας από κάποιον χρήστη πέραν του προοριζόμενου.

- Πρόβλημα του κρυμμένου κόμβου: Ένας συνηθισμένος περιορισμός στην απόδοση των WLAN είναι το πρόβλημα που προκύπτει από την περιορισμένη ακτίνα δράσης των ραδιοκυμάτων και είναι γνωστό ως “hidden node problem”. Το φαινόμενο αυτό προκύπτει όταν στο σύστημα υπάρχει ένας σταθμός που δεν μπορεί να ανιχνεύσει την μετάδοση ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται.

2.5 Δομικά στοιχεία ενός WLAN

Ένα ασύρματο δίκτυο αποτελείται από διάφορα στοιχεία που βοηθούν την σωστή μετάδοση, λήψη και επεξεργασία του σήματος από τον χρήστη. Στα στοιχεία αυτά περιλαμβάνονται τόσο το κατάλληλο λογισμικό (software) όσο και το ανάλογο υλικό εξοπλισμού (hardware). Οι κατηγορίες των στοιχείων αυτών αναφέρονται παρακάτω:

1. **Συσκευές χρηστών (End-user devices):** Όπως σε κάθε σύστημα έτσι και στα WLANs πρέπει να υπάρχει τρόπος διασύνδεσης των διαφόρων εφαρμογών με τους χρήστες. Μια συσκευή αποτελεί τη διασύνδεση του χρήστη με το δίκτυο. Συσκευές που χρησιμοποιούνται στα ασύρματα δίκτυα είναι και οι επόμενες:

- Laptop computers
- Palmtop computers
- Handheld PCs and printers
- Personal Digital Assistants (PDAs)
- Handheld printers and scanners

2. **Λογισμικό δικτύου (Network Software):** Ένα ασύρματο δίκτυο είναι δομημένο με το κατάλληλο λογισμικό που βρίσκεται σε διάφορα μέρη του δικτύου. Ένα σύστημα διαχείρισης δικτύου (NOS: Network Operating System), όπως είναι για παράδειγμα το Microsoft NT Server[3], παρέχει διαφόρων ειδών υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση, κ.α. Πολλά τέτοια συστήματα στηρίζονται στην ύπαρξη ενός διακομιστή, στον οποίο βρίσκονται οι βασικές συσκευές λογισμικού και οι βάσεις δεδομένων στις οποίες έχουν πρόσβαση οι διάφορες συσκευές, τις οποίες ελέγχει ο χρήστης.

3. **Ασύρματες κάρτες διασύνδεσης δικτύου (NICs cards):** Η ασύρματη κάρτα διασύνδεσης δικτύου συντονίζει μια συσκευή όπως ένα PDA, ένα laptop ή ένα σταθερό υπολογιστή σε ένα ασύρματο σταθμό και επιτρέπει στη συσκευή να επικοινωνήσει με άλλους σταθμούς σε ένα peer-to-peer δίκτυο ή με το σημείο πρόσβασης. Οι ασύρματες κάρτες δικτύου είναι διαθέσιμές σε μια ποικιλία από διάφορες συνδεσμολογίες και κατασκευαστές (Εικόνα 1). Οι περισσότερες ασύρματες κάρτες έχουν ολοκληρωμένες κεραίες αλλά πολλοί κατασκευαστές παρέχουν ασύρματες κάρτες με εξωτερική σύνδεση κεραίας ή αφαιρούμενη κεραία η οποία μπορεί να χρησιμοποιείται μόνο αν θέλουμε να επιτύχουμε υψηλούς ρυθμούς εύρους ζώνης.

Εικόνα 1 Ασύρματες κάρτες δικτύου με διάφορες συνδεσμολογίες (PCMCIA, PCI και USB από αριστερά προς τα δεξιά)

4. **Σημεία πρόσβασης (access points):** Το σημείο πρόσβασης είναι μια κεντρική συσκευή σε ένα ασύρματο τοπικό δίκτυο που παρέχει το εύρος για την ασύρματη επικοινωνία με τους άλλους σταθμούς σε ένα δίκτυο. Συνήθως συνδέεται σε ένα ενσύρματο δίκτυο και έτσι παρέχει μια γέφυρα ανάμεσα στο ενσύρματο δίκτυο και τις ασύρματες συσκευές. Τα σημεία πρόσβασης περιλαμβάνουν χαρακτηριστικά ασφάλειας όπως επικύρωση και κρυπτογράφηση, έλεγχο πρόσβασης που βασίζεται σε λίστες ή φίλτρα καθώς και πολλά άλλα τα οποία συνήθως απαιτούν τη ρύθμιση τους από τον χρήστη σύμφωνα με τις προτιμήσεις του,

[3] http://www.microsoft.com/ntserver/remove404.mspx

συνήθως χρησιμοποιώντας μια διεπαφή βασισμένη στο διαδίκτυο. Πολλά σημεία πρόσβασης περιλαμβάνουν επιπρόσθετα χαρακτηριστικά δικτύωσης όπως πύλες διαδικτύου, κόμβους μεταγωγής, ασύρματες γέφυρες ή επαναλύπτες. Στην εικόνα 2 βλέπουμε μερικά σημεία πρόσβασης.

Εικόνα 2 Σημεία πρόσβασης διαφόρων κατασκευαστών

5. **Κεραίες:** Η κεραία εκπέμπει το διαμορφωμένο σήμα μέσω του αέρα ώστε αυτό να φτάσει στον προορισμό του. Το μοντέλο διάδοσης μιας κεραίας καθορίζει την περιοχή κάλυψης της κεραίας. Για την μετάδοση του σήματος στα WLANs χρησιμοποιούνται κυρίως δύο είδη κεραιών, είτε πολυκατευθυντικές, είτε μονοκατευθυντικές. Το πιο συνηθισμένο είδος κεραίας που χρησιμοποιείται στις ασύρματες κάρτες και τα σημεία πρόσβασης είναι οι πολυκατευθυντικές των οποίων το όφελος κυμαίνεται από 0 έως 7 dBi και εμβέλεια 360°.

Εικόνα 3 Διάφορα είδη κεραιών

Κεφάλαιο 3 Το 802.11 πρότυπο ασύρματης δικτύωσης

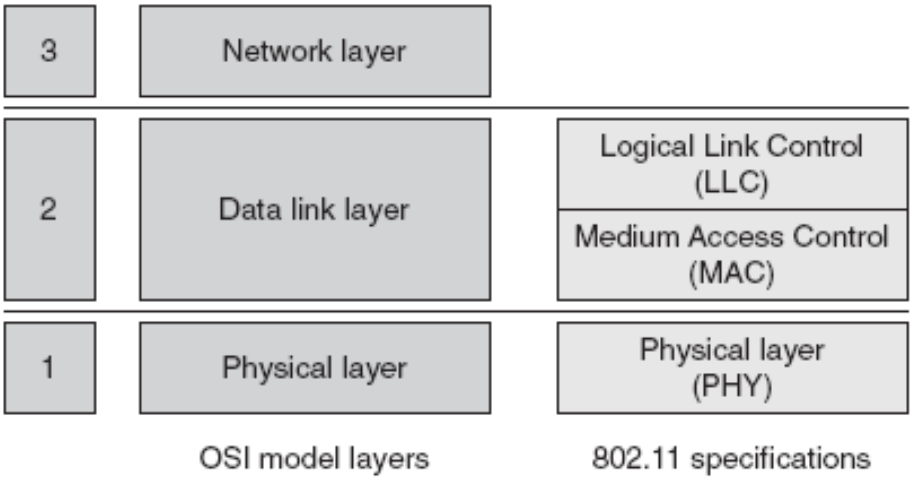
3.1 Το IEEE 802.11 πρωτόκολλο επικοινωνίας

Έχουν αναπτυχθεί διάφορες ασύρματες τεχνολογίες, μερικές από αυτές είναι το Bluetooth[4], το HomeRF[5], το OpenAir[6], το IEEE 802.11, το IEEE 802.16 και το HiperLAN[7] I και II. Κάθε μία από αυτές τις τεχνολογίες έχει διαφορετική εφαρμογή άρα μπορούμε να πούμε ότι είναι πιο πολύ συμπληρωματικές μεταξύ τους παρά ανταγωνιστικές. Το Bluetooth και το HomeRF για παράδειγμα είναι σχεδιασμένα για ζεύξεις μικρών αποστάσεων, για σύνδεση μεταξύ συσκευών και των περιφερειακών τους, το IEEE 802.11 για την υλοποίηση ασύρματων τοπικών δικτύων, ενώ το IEEE 802.16 για την υλοποίηση ευρύτερων ασύρματων μητροπολιτικών δικτύων. Στην παρούσα εργασία θα επικεντρωθούμε στο IEEE 802.11.

Το IEEE 802.11 είναι μια οικογένεια προτύπων της IEEE για τα ασύρματα τοπικά δίκτυα (WLAN), που είχαν σαν σκοπό να επεκτείνουν το 802.3 (Ethernet, το συνηθέστερο πρωτόκολλο ενσύρματης δικτύωσης υπολογιστών), στην ασύρματη περιοχή. Πρωταρχικός στόχος της ομάδας ήταν η κατάργηση των καλωδίων ανάμεσα στους υπολογιστές σε ένα τοπικό δίκτυο. Το 802.11 υποστηρίζει τόσο την επικοινωνία από σημείο σε σημείο (point-to-point) όσο και την επικοινωνία από ένα σημείο προς πολλά (point-to-multipoint). Τα πρότυπα 802.11 είναι ευρύτερα γνωστά ως “Wi-Fi” επειδή η Wi-Fi Alliance, ένας οργανισμός ανεξάρτητος της IEEE, παρέχει την πιστοποίηση για τα προϊόντα που υπακούν στις προδιαγραφές του 802.11. Αυτή η οικογένεια πρωτοκόλλων αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων.

Στα πρότυπα 802.11 περιγράφονται τα δύο πρώτα επίπεδα του μοντέλου OSI, δηλαδή το φυσικό επίπεδο (PHY, Physical Layer) και το επίπεδο σύνδεσης δεδομένων (MAC, Medium Access Control). Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την διαλειτουργικότητα, δηλαδή την ικανότητα συνεργασίας των συσκευών που το ακολουθούν. Η IEEE 802.11 περιγράφει μόνο τα δύο κατώτερα επίπεδα του OSI, επιτρέποντας έτσι σε οποιαδήποτε εφαρμογή να εργάζεται πάνω σε συσκευή 802.11 όπως ακριβώς θα εργαζόταν πάνω από Ethernet. Οι συσκευές 802.11 δηλαδή μεταφέρουν διαφανώς την πληροφορία από τα πιο πάνω επίπεδα του OSI. Όπως φαίνεται στην εικόνα 4, η υπηρεσία για το ανώτερο μέρος του επιπέδου μετάδοσης δεδομένων του μοντέλου OSI, στο 802.11 πρότυπο, παρέχεται από τις υπηρεσίες της λογικής σύνδεσης ελέγχου (LLC Logical Link Control).

[4] http://el.wikipedia.org/wiki/Bluetooth
[5] http://en.wikipedia.org/wiki/HomeRF
[6] http://en.wikipedia.org/wiki/OpenAIR
[7] http://en.wikipedia.org/wiki/HiperLAN



Εικόνα 4 Αρχιτεκτονική του 802.11

3.2 Πρότυπα που ανήκουν στην οικογένεια του 802.11

- **IEEE 802.11**
  Δημοσιεύτηκε το 1997 από την IEEE, μετά από επτά χρόνια μελέτης, είναι το πρώτο πρότυπο για ασύρματη δικτύωση. Προβλέπει ρυθμούς μετάδοσης από 1 έως 2 Mbps. Υποστηρίζει ασύγχρονη υπηρεσία. Στο φυσικό επίπεδο προβλέπει τεχνική FHSS (Frequency Hopping Spread Spectrum)[8] ή DSSS (Direct-Sequence Spread Spectrum)[9] σε ζώνες συχνοτήτων 915 MHz, 2.4 GHz και 5.2 GHz ή υπέρυθρη μετάδοση στα 850 nm έως 900 nm. Υποστηρίζει δυνατότητες όπως κατανομή προτεραιοτήτων της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος της συσκευής. Το πρότυπο γνώρισε περιορισμένη επιτυχία λόγω τον χαμηλών ρυθμών μετάδοσης.

- **IEEE 802.11a**
  Το πρότυπο αυτό εισήλθε στην αγορά αφού το 802.11b είχε ήδη ένα μεγάλο μερίδιο αυτής. Παρόλα αυτά η τεχνολογία που χρησιμοποιεί προσφέρει αρκετά πλεονεκτήματα σε σχέση με αυτή του 802.11b. Χρησιμοποιεί τις μπάντες UNII στα 5GHz, με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας διαμόρφωση OFDM (Orthogonal Frequency Division Multiplexing)[10]. Η επέκταση αυτή αποσκοπούσε να καλύψει την ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Επιλέχθηκε η λειτουργία σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να

[8] http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum
[9] http://en.wikipedia.org/wiki/DSSS
[10] http://en.wikipedia.org/wiki/OFDM

μπορούν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί, αφετέρου ώστε να μην υπάρχει παρεμβολή από τις προηγούμενες συσκευές.

- **IEEE 802.11b**
  Υποστηρίζει επιπλέον μετάδοση σε ρυθμούς 5.5 και 11 Mbps, με κωδικοποίηση CCK (Complementary Code Keying)[11]. Μια δεύτερη κωδικοποίηση PBCC (Packet Binary Convolutional Code), ορίστηκε για προαιρετική υλοποίηση υποστηρίζοντας μετάδοση 5.5 και 11 Mbps και έχοντας ελαφρά καλύτερη ευαισθησία δέκτη, με αντίτιμο την πολυπλοκότητα. Η μετάδοση γίνεται στη ζώνη συχνοτήτων των 2.4 GHz. Είναι το πιο δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, όντας ένα στιβαρό, αποτελεσματικό και δοκιμασμένο πρότυπο. Οι προσθήκες του 802.11b σε σχέση με το 802.11 αφορούν μόνο τον τρόπο μετάδοσης ενώ ο τρόπος πρόσβασης των συσκευών και ο τρόπος λειτουργίας μένουν οι ίδιοι.

- **IEEE 802.11g**
  Αποτελεί επέκταση στο 802.11b, ώστε να υποστηρίζει μεγαλύτερους ρυθμούς μετάδοσης. Έτσι εκτός από τους ρυθμούς μετάδοσης του 802.11b, με CCK διαμόρφωση, υποστηρίζει και ρυθμούς μέχρι και 54 Mbps χρησιμοποιώντας OFDM διαμόρφωση. Οι αντίστοιχες συσκευές εργάζονται στη ζώνη συχνοτήτων των 2.4 GHz, διατηρώντας συμβατότητα προς τα πίσω με το 802.11b.

Έκδοση	**Ημερομηνία**	**Ζώνη Συχνοτήτων**	**Συνήθης ρυθμός μετάδοσης**	**Ονομαστικός ρυθμός μετάδοσης**	**Μέθοδοι μετάδοσης**	**Εμβέλεια εσωτερικών χώρων**
802.11	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s	IR / FHSS / DSSS	~20m
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38m
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35m
802.11g	2003	2.4GHz	19 Mbit/s	54 Mbit/s	OFDM	~38m

Πίνακας 1 Συγκριτικός πίνακας των 802.11 προτύπων

Πέρα των βασικών πρωτοκόλλων η οικογένεια προτύπων 802.11, περιλαμβάνει έναν αριθμό συμπληρωματικών προτύπων, που προσθέτουν επιπλέον λειτουργικότητα στα ασύρματα δίκτυα.

[11] http://en.wikipedia.org/wiki/Complementary_code_keying

- **IEEE 802.11c**
  Παρέχει λειτουργία γεφύρωσης (bringing) 802.11 πλαισίων.

- **IEEE 802.11d**
  Παρέχει επεκτάσεις στο φυσικό επίπεδο, ώστε να λειτουργεί σε επιπλέον ρυθμιστικά πλαίσια (άλλες ζώνες συχνοτήτων).

- **IEEE 802.11e**
  Υποστήριξη QoS στο MAC επίπεδο (EDCF, Enhanced DCF και HCF) και ενίσχυση των μηχανισμών ασφάλειας.

- **IEEE 802.11f**
  Συνιστώμενη πρακτική για το πρωτόκολλο IAPP, Inter Access Point Protocol, που αφορά την επικοινωνία μεταξύ των σημείων πρόσβασης.

- **IEEE 802.11i**
  Επεκτάσεις στο MAC επίπεδο για ενισχυμένη ασφάλεια. Περιγραφή πρωτοκόλλων 802.1X, TKIP, AES.

- **IEEE 802.11j**
  Παρέχει ενίσχυση στο φυσικό επίπεδο του μηχανισμού IEEE 802.11a, ώστε να προσαρμοστεί με τις Ιαπωνικές απαιτήσεις.

- **IEEE 802.11k**
  Βελτιώσεις στην μέτρηση των πόρων του ραδιοφώνου, για την παροχή διασύνδεσης στα υψηλότερα επίπεδα για μετρήσεις δικτύων.

- **IEEE 802.11m**
  Συντήρηση του IEEE 802.11-1999 προτύπου, με τεχνικές και συντακτικές διορθώσεις.

- **IEEE 802.11n**
  Ενίσχυση στο φυσικό επίπεδο και στο επίπεδο MAC για την επίτευξη υψηλότερου ρυθμού μετάδοσης δεδομένων.

- **IEEE 802.11p**
  Στο φυσικό επίπεδο και στο MAC , παροχή ασύρματης πρόσβασης σε περιβάλλοντα που βρίσκονται σε τροχιά μεταξύ τους.

- **IEEE 802.11r**
  Στο φυσικό και στο MAC επίπεδο παρέχει γρήγορη περιαγωγή (γρήγορη μετάβαση BSS).

- **IEEE 802.11s**
  Παρέχει δικτύωση των ESS.

- **IEEE 802.11,2**
  Συνιστώμενη πρακτική για την αξιολόγηση της ασύρματης απόδοσης των 802.11.

- **IEEE 802.11u**
  Βοηθάει στη συνεργασία με διάφορα εξωτερικά δίκτυα.

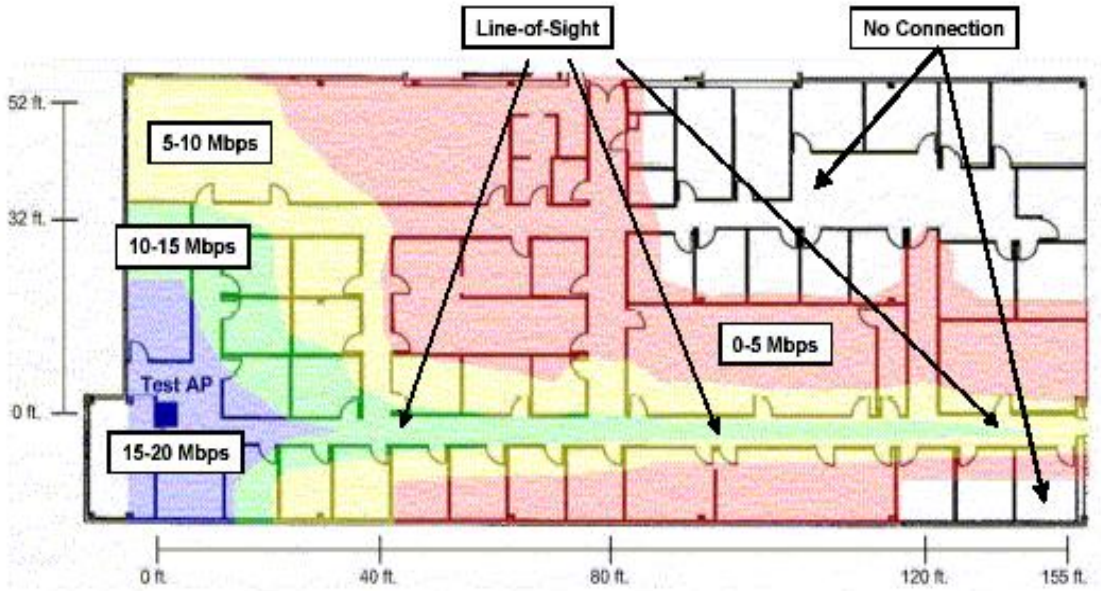
3.3 Χαρακτηριστικά του IEEE 802.11

Η ζώνη των 2.4 GHz γίνεται ολοένα και πιο δημοφιλής σήμερα. Ο λόγος γι' αυτό είναι ότι πρόκειται για ελεύθερη ζώνη και έχει κατάλληλα χαρακτηριστικά για μετάδοση σε μικρές αποστάσεις.

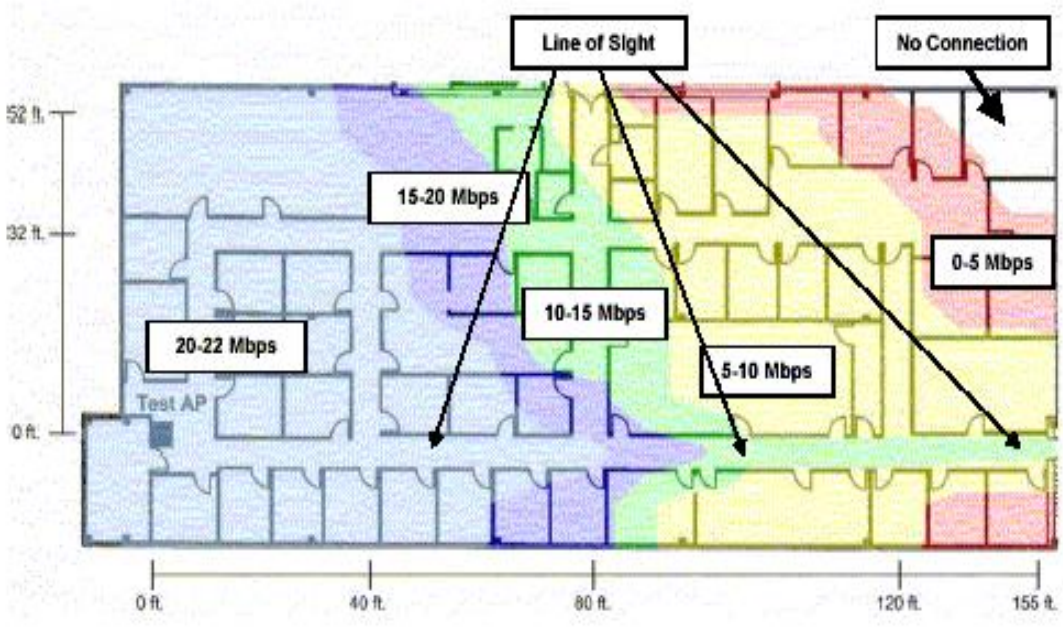
Παρεμβολές
Το ασύρματο LAN μπορεί να δεχτεί και να προκαλέσει παρεμβολές σε άλλα προϊόντα όπως ασύρματα τηλέφωνα ή φούρνους μικροκυμάτων. Μπορεί επίσης να δεχτεί παρεμβολές και από άλλες συσκευές. Το πρόβλημα των παρεμβολών δημιουργείται από την κακή σχεδίαση των δικτύων (κακές και ακατάλληλες κεραίες, λάθος επιλογή συχνοτήτων κ.α.).

Εμβέλεια
Η εμβέλεια ενός ασύρματου δικτύου σε περιβάλλον γραφείου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα σε εσωτερικό χώρο, έχουν να διαπεράσουν τοίχους και οροφές, οπότε υφίστανται σημαντικές απώλειες. Δηλαδή όταν ένα ραδιοκύμα προσπέσει σε ένα τοίχο, ένα μέρος της ισχύος του θα απορροφηθεί από το υλικό του τοίχου και ένα μόνο κομμάτι θα μπορεί να τον προσπελάσει και να διαδοθεί. Επίσης το σήμα ανακλάται από τις προσπίπτουσες επιφάνειες, με αποτέλεσμα στο δέκτη να φτάσουν τελικά ένας αριθμός από αντίγραφα του αρχικού σήματος όλα με διαφορετικά μήκη και πλάτη. Από την άθροισή τους μπορεί να προκύψει αλληλοαναίρεση και το τελικό σήμα να έχει πολύ μικρότερη ισχύ. Σε περιβάλλον όπου υπάρχει οπτική επαφή, σε εξωτερικό χώρο, η εμβέλεια του ασύρματου δικτύου είναι σαφώς μεγαλύτερη και εξαρτάται από την ισχύ εκπομπής, την ευαισθησία του δέκτη, την ποιότητα των κεραιών και την ευθυγράμμιση τους, το επίπεδο παρεμβολών και θορύβου.

Στις παρακάτω εικόνες φαίνεται ενδεικτικά η εμβέλεια του κάθε πρωτοκόλλου συναρτήσει με τον ρυθμό μετάδοσης. Η διαφορετική συμπεριφορά οφείλεται στη διαφορετική συχνότητα λειτουργίας των δύο προτύπων.



Εικόνα 5 Η εμβέλεια στο 802.11a



Εικόνα 6 Η εμβέλεια στο 802.11b

Ρυθμός μετάδοσης
Η πραγματική διαπερατότητα του συστήματος εξαρτάται από ένα πλήθος παραγόντων όπως οι παράμετροι ραδιομετάδοσης (εμβέλεια, ανακλάσεις, απορρόφηση και σκέδαση), όπως και από τον αριθμό των χρηστών. Για τις περισσότερες εφαρμογές το bandwidth είναι επαρκές.

Ποιότητα επικοινωνίας
Έχοντας πίσω τους μισό αιώνα σε εμπορικές και στρατιωτικές εφαρμογές, οι ασύρματες τεχνολογίες έχουν γίνει πολύ στιβαρές και αξιόπιστες. Έτσι μπορούν να παρέχουν στους χρήστες τους αξιόπιστες συνδέσεις και σε καλύτερο επίπεδο από ότι οι αντίστοιχες στην κινητή τηλεφωνία.

Συμβατότητα με το υπάρχον δίκτυο
Τα περισσότερα ασύρματα δίκτυα έχουν προτυποποιημένο τρόπο διασύνδεσης με τα ενσύρματα δίκτυα. Έτσι η προσθήκη ασύρματης δικτύωσης, σε υπάρχουσες δομές δικτύων, μπορεί να γίνει με τον ευκολότερο τρόπο. Συστήματα διαχείρισης επιβλέπουν τους ασύρματους κόμβους όπως και οποιοδήποτε άλλο στοιχείο ελέγχου.

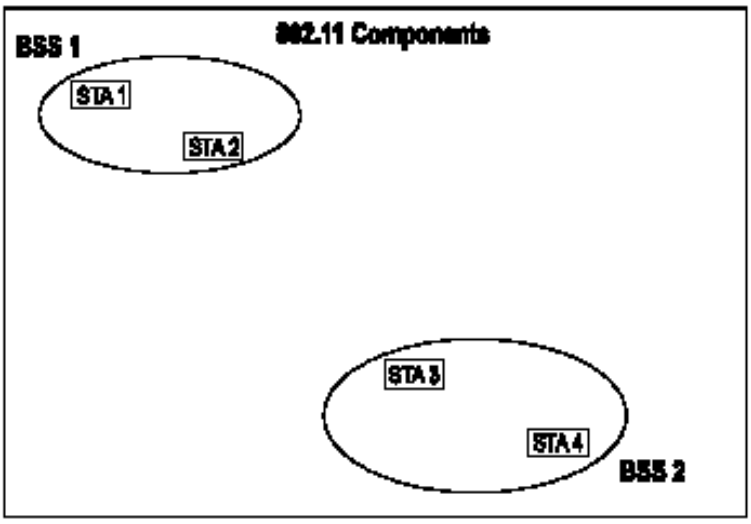
3.4 Η τοπολογία του 802.11

Η τοπολογία του 802.11, αποτελείται από στοιχεία που αλληλεπιδρούν, ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο, που παρέχει τη δυνατότητα μετακίνησης των σταθμών. Ένας σταθμός (station) είναι κάθε συσκευή, η οποία εμπεριέχει τις λειτουργίες του 802.11 (δηλαδή το επίπεδο MAC, το φυσικό στρώμα και μια

διασύνδεση (interface) με το ασύρματο μέσο. Οι λειτουργίες του 802.11 υπάρχουν σε μια ασύρματη κάρτα δικτύου NIC (Network Interface Card)[12]. Το πρότυπο 802.11 ορίζει τρείς τρόπους επικοινωνίας μεταξύ κόμβων ενός δικτύου, τον BSS (Basic Service Set), τον IBSS (Independent Basic Service Set) και τον ESS (Extended Service Set).

3.4.1 BSS (Basic Service Set)

Το βασικό δομικό στοιχείο ενός IEEE 802.11 είναι το BSS (Basic Service Set). Ένα BSS μπορεί να αποτελείται για παράδειγμα από δύο σταθμούς, όπως φαίνεται στην παρακάτω εικόνα, οι οποίοι είναι τα μέλη του. Αν ένας σταθμός μετακινηθεί έξω από το BSS στο οποίο ανήκει, δεν μπορεί πλέον να επικοινωνήσει άμεσα με τα μέλη του συγκεκριμένου BSS.

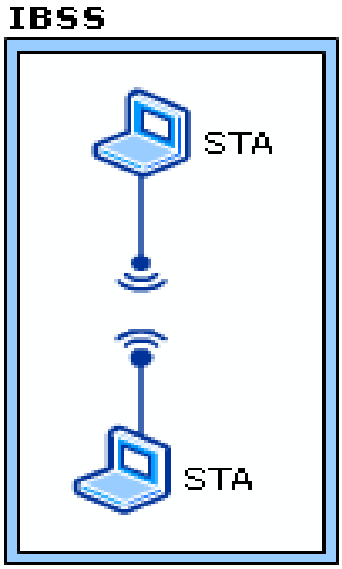


Εικόνα 7 Σχηματική αναπαράσταση δύο BSS

3.4.2 IBSS (Independent Basic Service Set)

Είναι η πιο βασική και η πιο απλή τοπολογία ασύρματης δικτύωσης. Οι ασύρματοι σταθμοί επικοινωνούν κατευθείαν μεταξύ τους ένας προς έναν (peer-to-peer), χωρίς να υπάρχει κεντρικός σταθμός (AP). Όλοι οι σταθμοί είναι ισότιμοι μεταξύ τους. Στο παρακάτω σχήμα φαίνεται ένα δίκτυο IBSS ή όπως αλλιώς ονομάζονται Ad-hoc δίκτυα ή Peer-to-Peer.

[12] http://en.wikipedia.org/wiki/Network_card



Εικόνα 8 IBSS τοπολογία

Βασικός περιορισμός είναι ότι για να γίνει η επικοινωνία μεταξύ δύο σταθμών, θα πρέπει ο ένας σταθμός να είναι εντός της εμβέλειας του άλλου. Έτσι δεν υπάρχει η δυνατότητα μεταγωγής των δεδομένων μέσω ενός σταθμού προς κάποιον τρίτο, ώστε τα δεδομένα να περάσουν με διαφανή τρόπο από κάποιο σταθμό. Έχει βασικό λόγο ύπαρξης την γρήγορη και εύκολη διάρθρωση ενός ασύρματου δικτύου στην περίπτωση που δεν υφίσταται ασύρματη υποδομή ή και δεν χρειάζεται ή για την κάλυψη μικρών περιοχών.

Για παράδειγμα αν θέλουμε να διασυνδέσουμε δύο ή περισσότερους υπολογιστές σε έναν χώρο που δεν υπάρχει κάποια άλλη δομή ασύρματης δικτύωσης, ρυθμίζουμε τις αντίστοιχες ασύρματες κάρτες να εργάζονται σε ad-hoc[13] τρόπο επικοινωνίας. Έτσι αν κάποια συσκευή θέλει να εκπέμψει, ελέγχει να δει αν είναι ελεύθερη η ραδιοσυχνότητα, αν είναι κατειλημμένη περιμένει για κάποιο χρονικό διάστημα μέχρι να ελευθερωθεί. Όταν βρει ευκαιρία δοκιμάζει να στείλει τα προς μετάδοση πακέτα, μαζί με κάποιες άλλες πρόσθετες πληροφορίες, όπως τη διεύθυνση του παραλήπτη. Τα εκπεμπόμενα πακέτα τα ακούνε όλοι οι εκπεμπόμενοι σταθμοί και αυτός που αναγνωρίζει την δική του διεύθυνση σαν διεύθυνση παραλήπτη, τα παραλαμβάνει και τα επεξεργάζεται.

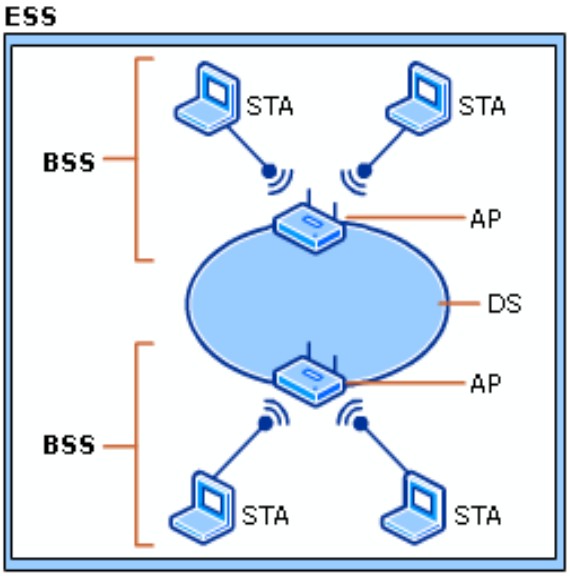
3.4.3 ESS (Extended Service Set)

Όταν οι ανάγκες τις διαδικτύωσης ξεπερνούν τα όρια του IBSS, το 802.11 καθορίζει τη δομή ενός πιο σύνθετου τοπικού δικτύου που ονομάζεται ESS (Extended Service

[13] http://en.wikipedia.org/wiki/Wireless_ad_hoc_network

Set) και στο οποίο είναι δυνατή η διασύνδεση και η επικοινωνία πολλών BSS μεταξύ τους. Το στοιχείο που χρησιμοποιείται για την διασύνδεση των BSS ονομάζεται σύστημα διανομής (Distributed System- DS)[14]. Το 802.11 κάνει διαχωρισμό του ασύρματου μέσου (wireless medium) από το DS.

Η πρόσβαση στο DS γίνεται με τη βοήθεια ενός σταθμού που καλείται AP (Access Point) και ο οποίος παρέχει ουσιαστικά τη διασύνδεση των σταθμών που βρίσκονται σε διάφορα BSS στο DS. Η διασύνδεση αυτή φαίνεται στην εικόνα 9.



Εικόνα 9 Η σύνδεση των BSSs γίνεται με τη βοήθεια τωνAPs

Τα δεδομένα μετακινούνται μεταξύ ενός BSS και του DS μόνο μέσω του AP, ενώ το DS υποστηρίζει τους τύπους κίνησης του 802.11 παρέχοντας υπηρεσίες ικανές να ελέγχουν την αντιστοίχιση της διεύθυνσης στον προορισμό για κάθε σταθμό που μετακινείται. Η κεντρική ιδέα της συγκεκριμένης τοπολογίας, είναι ότι ένα δίκτυο ESS εμφανίζεται το ίδιο σε ένα επίπεδο LLC όπως και ένα δίκτυο IBSS. Οι σταθμοί μέσα στο ίδιο ESS μπορούν να μετακινούνται από ένα BSS σε ένα άλλο διαφανώς ως προς το LLC. Τα ESS δίκτυα αναφέρονται και ως infrastructure δίκτυα, αν και τα τελευταία αποδίδουν συνήθως την τοπολογία όπου ένα BSS συνδέεται μέσω ενός AP σε ένα ενσύρματο δίκτυο.

3.5 Αρχιτεκτονική του 802.11

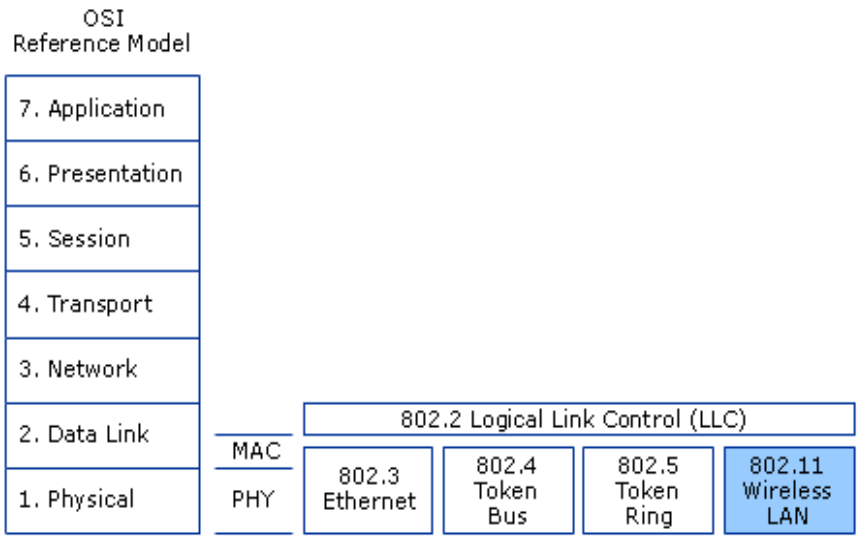
Ένα ασύρματο δίκτυο 802.11 βασίζεται σε μια κυψελοειδή αρχιτεκτονική, σύμφωνα με την οποία ολόκληρο το σύστημα διαιρείται σε περιοχές ή κελιά, με το κάθε κελί να ελέγχεται από ένα σταθμό βάσης (Base Station). Στην ορολογία του 802.11 ένα κελί ονομάζεται Βασικό Σύνολο Υπηρεσιών (Base Service Set-BSS) και ο σταθμός βάσης

[14] http://www.cl.cam.ac.uk/~rja14/Papers/SE-06.pdf

σημείο πρόσβασης (Access Point-AP). Παρόλο που ένα δίκτυο μπορεί να αποτελείται από ένα μόνο κελί, οι περισσότερες δικτυακές εγκαταστάσεις 802.11 συνήθως αποτελούνται από πολλά κελιά, με τα σημεία πρόσβασης να βρίσκονται συνδεδεμένα σε μια ραχοκοκαλιά, η οποία ονομάζεται Σύστημα Διανομής (Distribution System-DS) και η οποία μπορεί να είναι είτε ένα ενσύρματο δίκτυο (Ethernet) ή ένα ασύρματο δίκτυο.

Το σύνολο όλων των δια-συνδεδεμένων ασύρματων δικτύων, μαζί με τα σημεία πρόσβασης και το σύστημα διανομής ονομάζεται Εκτεταμένο Σύνολο Υπηρεσιών (Extended Service Set-ESS). Όσον αφορά τα ανώτερα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, σύμφωνα με το πρότυπο θα πρέπει να θεωρείται ως ένα ενιαίο τοπικό δίκτυο κατηγορίας 802. Το πρότυπο ορίζει επίσης την έννοια της πύλης (Portal). Η πύλη είναι μια συσκευή που χρησιμοποιείται για την διασύνδεση ενός δικτύου 802.11 με ένα άλλο δίκτυο κατηγορίας 802. Η λειτουργιά της μπορεί να παρομοιαστεί με την λειτουργία ενός δρομολογητή (router), ο οποίος είναι ικανός να δια-συνδέει διαφορετικά δίκτυα. Η λειτουργικότητα μιας πύλης μπορεί να βρίσκεται είτε σε ξεχωριστή συσκευή, είτε ενσωματωμένη στο σημείο πρόσβασης.

Ενώ η τοπολογία καθορίζει τα αναγκαία μέσα για τη φυσική διασύνδεση του ασύρματου δικτύου, η αρχιτεκτονική καθορίζει τον τρόπο λειτουργίας του δικτύου. Η επιτροπή των IEEE 802.11 προτύπων ορίζει δύο χωριστά στρώματα, το στρώμα Logical Layer Control (LLC) και το Media Access Control (MAC), αντίστοιχα για το επίπεδο της μετάδοσης δεδομένων (Data Link Layer) του μοντέλου OSI. Το ασύρματο πρότυπο IEEE 802.11 ορίζει τις προδιαγραφές για το φυσικό στρώμα και για το MAC στρώμα που επικοινωνούν μέχρι το στρώμα LLC όπως φαίνεται στην εικόνα 10.



Εικόνα 10 Αντιστοιχία OSI με 802.11

3.5.1 Το επίπεδο σύνδεσης δεδομένων

Το επίπεδο σύνδεσης δεδομένων εφαρμόζεται σε όλους τους 802.11 σταθμούς και επιτρέπει στο σταθμό να εγκαθιδρύει ένα δίκτυο ή να συμμετέχει σε ένα ήδη υπάρχον δίκτυο και να μεταφέρει δεδομένα που περνούν από το επίπεδο λογικής σύνδεσης ελέγχου (LLC). Αυτές οι λειτουργίες γίνονται χρησιμοποιώντας δύο

μεθόδους υπηρεσιών, τις υπηρεσίες σταθμών και τις υπηρεσίες των συστημάτων διανομής. Πριν όμως αρχίσουν να πραγματοποιούνται οι υπηρεσίες του MAC επιπέδου, πρώτα πρέπει να πραγματοποιηθεί η πρόσβαση στο ασύρματο μέσο. Το υπόστρωμα MAC παρέχει τις ακόλουθες βασικές λειτουργίες:

- Τον έλεγχο της πρόσβασης των σταθμών στο κοινό μέσο μετάδοσης.
- Τη λειτουργία του κατακερματισμού και της επανα-συναρμολόγησης του πακέτου.
- Τη λειτουργία της αναμετάδοσης του πακέτου.
- Τη λειτουργία της επιβεβαίωσης λήψης.

Η πρόσβαση στο ασύρματο μέσο

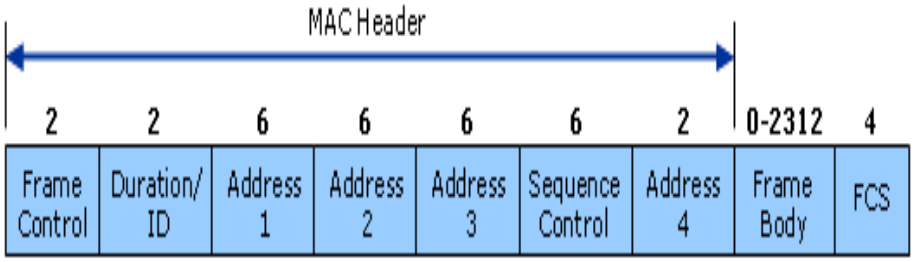
Σε ένα ασύρματο δίκτυο είναι πιο περίπλοκο να μοιράζουμε την πρόσβαση μεταξύ των σταθμών διανομής από ότι σε ένα ενσύρματο. Αυτό συμβαίνει επειδή ένας ασύρματος σταθμός δεν είναι σε θέση να ανιχνεύσει μια σύγκρουση που μπορεί να συμβεί στη μετάδοση του με την μετάδοση ενός άλλου σταθμού. Σε ένα ενσύρματο δίκτυο είναι εύκολο να ανιχνευτούν τυχόν συγκρούσεις με τον μηχανισμό carrier sense multiple access / collision detection (CSMA/CD)[15].

Το πρότυπο 802.11 καθορίζει ένα αριθμό από λειτουργίες συντονισμού του MAC επιπέδου για να συντονίσει την πρόσβαση μέσου μεταξύ πολλαπλών σταθμών. Η πρόσβαση στο μέσο μπορεί να γίνει είτε μέσω της λειτουργίας κατανεμημένου συντονισμού (Distributed Coordination Function – DCF)[16], είτε μέσω της λειτουργίας σημείου συντονισμού (Point Coordination Function – PCF)[17].

Στο DCF το 802.11 καθορίζει τις επόμενες δύο κατηγορίες DCF. Η πρώτη κατηγορία είναι η DCF CSMA/CA, όπου η αρχή της λειτουργίας αυτής βασίζεται στον ανταγωνισμό και για την πρόσβαση στο μέσο χρησιμοποιείται η τεχνική CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance)[18]. Η δεύτερη κατηγορία είναι η DCF RTS/CTS[19]. Η αρχή λειτουργίας της μεθόδου αυτής στηρίζεται στην πρόσβαση στο μέσο με την βοήθεια πακέτων αίτησης (RTS) και άδειας (CTS) χρήσης του μέσου. Το PCF στηρίζεται στην πρόσβαση στο μέσο χωρίς ανταγωνισμό (χρήσιμο για infrastructure δίκτυα), ενώ κύριο λόγο παίζει ένας ελεγκτής ο οποίος καλείται PC (Point Coordinator) και βρίσκεται στα APs.

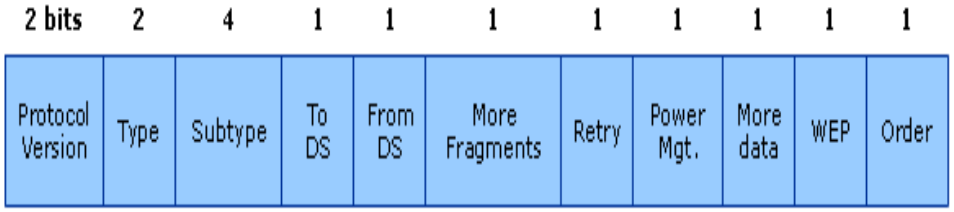
Το υπόστρωμα MAC του 802.11 ορίζει τρεις διαφορετικές κατηγορίες πλαισίων: τα πλαίσια δεδομένων, ελέγχου και διαχείρισης. Κάθε μια από αυτές τις κατηγορίες έχει μια κεφαλίδα με διάφορα πεδία που χρησιμοποιούνται στο υποεπίπεδο MAC. Η μορφή ενός πλαισίου δεδομένων φαίνεται στην εικόνα 11.

[15] http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection
[16] http://en.wikipedia.org/wiki/Distributed_Coordination_Function
[17] http://en.wikipedia.org/wiki/Point_Coordination_Function
[18] http://en.wikipedia.org/wiki/CSMA/CA
[19] http://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS



Εικόνα 11 Γενική δομή ενός MAC πλαισίου

FC (Frame Control): Το πλαίσιο ελέγχου τομέα, που φαίνεται στην εικόνα 12, αποτελείται από 11 υποπεδία. Περιλαμβάνει τον έλεγχο των πληροφοριών που χρησιμοποιήθηκαν για τον καθορισμό του τύπου του 802.11 MAC πλαισίου και για την παροχή υπηρεσιών που απαιτούνται για τα ακόλουθα πεδία για να κατανοήσουν πώς να επεξεργαστούν το πλαίσιο MAC. Οι αριθμοί στο σχήμα αντιπροσωπεύουν τον αριθμό των bit που απαιτούνται για κάθε τομέα. Το πεδίο αυτό περιλαμβάνει πληροφορίες για τον τύπο του πλαισίου, για τον έλεγχο ισχύος, για την κρυπτογράφηση, κ.α.



Εικόνα 12 Η δομή του πλαισίου ελέγχου τομέα

Μια περιγραφή του κάθε υπό-πλαισίου του πλαισίου ελέγχου τομέα ακολουθεί παρακάτω:

- **Protocol Version (Έκδοση πρωτοκόλλου)**: Παρέχει την τρέχουσα έκδοση του 802.11 πρωτοκόλλου που χρησιμοποιείται. Όταν λαμβάνει STAs, χρησιμοποιεί τη λήψη αυτής της τιμής για να διαπιστώσει εάν η έκδοση του πρωτοκόλλου του ληφθέντος πλαισίου υποστηρίζεται.

- **Type and Subtype (Τύπος και δευτερεύον τύπος)**: Τα πεδία αυτά καθορίζουν τη λειτουργία του πλαισίου. Υπάρχουν τρία διαφορετικά πεδία για το κάθε πλαίσιο: έλεγχος, δεδομένα και διαχείριση. Επίσης υπάρχουν πολλαπλά δευτερεύοντος πεδία για κάθε τύπου πλαισίου.

- **To DS and From DS (Από DS και προς DS):** Δείχνει εάν το πλαίσιο πρόκειται να εισέλθει ή να εξέλθει από το DS (Distributed System) και

χρησιμοποιείται μόνο στα πλαίσια του τύπου δεδομένων ενός σταθμού που συνδέεται με ένα AP.

- **More Fragments (Περισσότερα θραύσματα)**: Δείχνει εάν πρόκειται να ακολουθήσουν περισσότερα κομμάτια του πλαισίου, ή τον τύπο διαχείρισης ή τα δεδομένα που ακολουθούν.

- **Retry (Επανάληψη)**: Δείχνει εάν το πλαίσιο ή τα δεδομένα αναμεταδίδονται.

- **Power Mgt (Ισχύς)**: Δηλώνει εάν ο σταθμός αποστολής είναι σε ενεργή λειτουργία.

- **More Data (Περισσότερα δεδομένα)**: Καθορίζουν σε ένα σταθμό που είναι σε κατάσταση εξοικονόμησης ενέργειας ότι το σημείο πρόσβασης έχει να στείλει και άλλα δεδομένα.

- **WEP**: Υποδηλώνει εάν χρησιμοποιείται ή όχι κρυπτογράφηση και επικύρωση στο τρέχων πλαίσιο.

- **Order (Σειρά)**: Αναφέρει ότι έλαβε σε σειρά όλα τα πλαίσια των δεδομένων που θα πρέπει να υποβληθούν σε επεξεργασία.

Duration/ID (Διάρκεια): Η πληροφορία στο πεδίο αυτό δηλώνει για πόσο χρόνο θα καταλάβουν το κανάλι το πλαίσιο και η επιβεβαίωση του.

Address (Διεύθυνση): Η κεφαλίδα του πλαισίου περιέχει τέσσερις διευθύνσεις, όλες με την τυπική μορφή του IEEE 802. Προφανώς χρειάζονται διευθύνσεις προέλευσης και προορισμού. Οι άλλες δύο διευθύνσεις χρησιμοποιούνται για τους σταθμούς βάσης προέλευσης και προορισμού, για την κίνηση μεταξύ των κυψελών.

Sequence Control (Έλεγχος Ακολουθίας): Τα bytes στο πεδίο αυτό υποδεικνύουν τον αριθμό του πλαισίου ενός συγκεκριμένου MSDU[20].

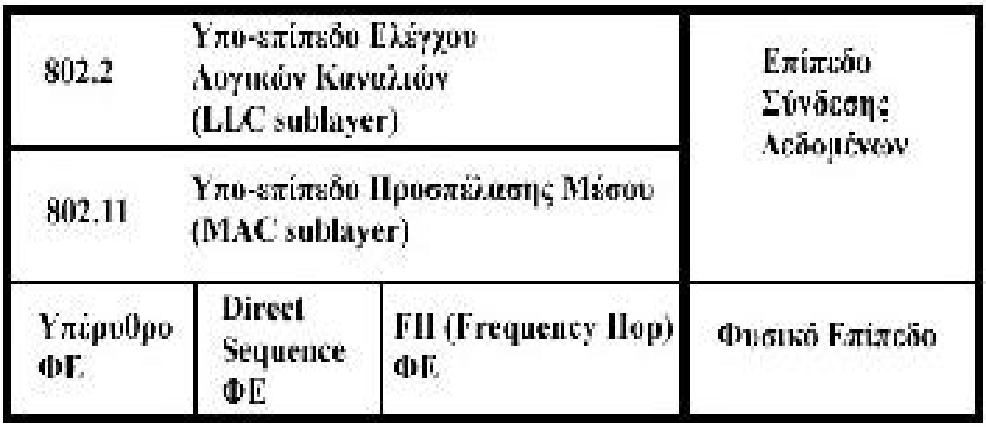
Data (Δεδομένα): Περιέχει το ωφέλιμο φορτίο, δηλαδή τα δεδομένα προς μετάδοση, μήκους μέχρι 2312 bytes, ακολουθούμενο από το συνηθισμένο **άθροισμα ελέγχου**.

3.5.2 Φυσικό επίπεδο

Το αρχικό πρότυπο του 802.11 που δημιουργήθηκε το 1997, υποστήριζε τρείς επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο, όπως φαίνεται στην εικόνα 13. Την μέθοδο υπερύθρων και άλλες δύο μεθόδους, που χρησιμοποιούν ραδιοκύματα μικρής εμβέλειας, χρησιμοποιώντας τεχνικές που ονομάζονται FHSS[21]

[20] http://en.wikipedia.org/wiki/MSDU
[21] http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

και DSSS[22]. Όλες αυτές οι τεχνικές λειτουργούν σε 1 ή 2 Mbps και με αρκετά χαμηλή ισχύ, έτσι ώστε να μην παρουσιάζουν πολλές διενέξεις. Το 1999 παρουσιάστηκαν δύο νέες τεχνικές για την επίτευξη υψηλότερου εύρους ζώνης. Οι τεχνικές αυτές ονομάζονται OFDM[23] και HR-DSSS. Λειτουργούν μέχρι τα 54 Mbps και τα 11 Mbps αντίστοιχα. Το 2001 παρουσιάστηκε μια δεύτερη τεχνική διαμόρφωσης OFDM, αλλά σε διαφορετική ζώνη συχνοτήτων από την πρώτη. Παρακάτω εξετάζουμε σε συντομία την κάθε μια από αυτές τις μεθόδους.



Εικόνα 13 Επίπεδα προτύπου IEEE 802.11

Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη μετάδοση στα 0,85 ή στα 0,95 micron. Επιτρέπονται δύο ταχύτητες: 1 Mbps και 2 Mbps. Στο 1 Mbps χρησιμοποιείται μια μέθοδος κωδικοποίησης, που ονομάζεται κώδικας Gray[24]. Τα υπέρυθρα σήματα δεν μπορούν να διαπεράσουν τους τοίχους, έτσι οι κυψέλες που βρίσκονται σε διαφορετικά δωμάτια είναι καλά απομονωμένες η μια από την άλλη. Ωστόσο λόγω του χαμηλού εύρους ζώνης, η επιλογή αυτή δεν είναι δημοφιλής.

Η Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας ή FHSS (Frequency Hooping Spread Spectrum) χρησιμοποιεί 79 κανάλια, το καθένα με εύρος 1 MHz. Χρησιμοποιείται μια γεννήτρια ψευδοτυχαίων αριθμών για την παραγωγή της ακολουθίας συχνοτήτων στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί. Σε μεγάλες αποστάσεις μπορεί να δημιουργήσει πρόβλημα η εξασθένηση πολλαπλών διαδρομών, η τεχνική FHSS παρέχει όμως αρκετή αντοχή σε αυτό το φαινόμενο. Επίσης είναι σχετικά ανθεκτική στις ραδιοκυματικές παρεμβολές, γεγονός που την κάνει δημοφιλή για συνδέσεις από κτήριο σε κτήριο. Κύριο μειονέκτημα της είναι το χαμηλό της εύρος ζώνης.

[22] http://en.wikipedia.org/wiki/DSSS
[23] http://en.wikipedia.org/wiki/OFDM
[24] http://www.pc-control.co.uk/gray_code.htm

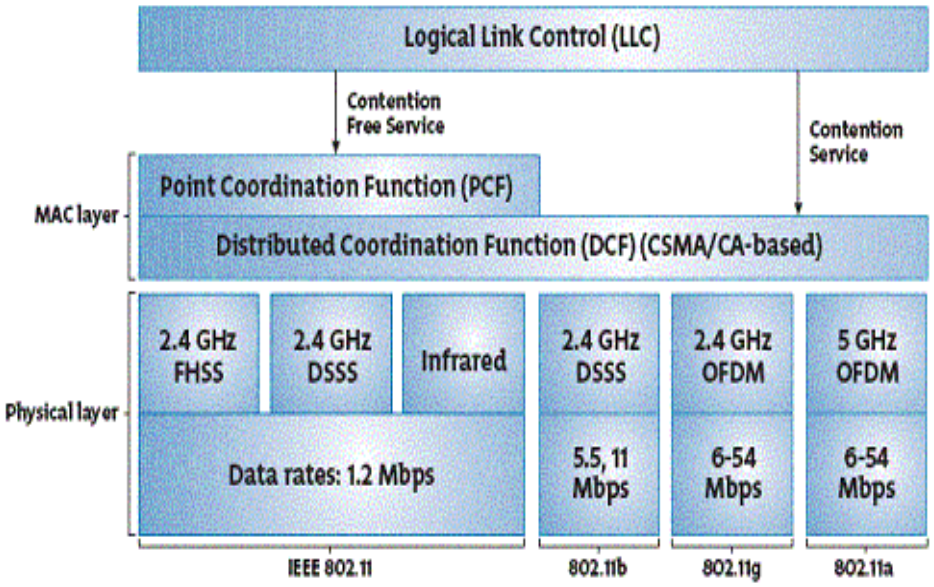
Η Τρίτη τεχνική διαμόρφωσης, η Εξάπλωση Φάσματος Άμεσης Ακολουθίας ή DSSS (Direct Sequence Spread Spectrum), περιορίζεται και αυτή σε 1 ή 2 Mbps. Κάθε bit μεταδίδεται ως 11 θραύσματα χρησιμοποιώντας την λεγόμενη ακολουθία Barker[25]. Χρησιμοποιείται διαμόρφωση μετατόπισης φάσης στο 1 Mbaud[26], με μετάδοση 1 bit ανά baud για λειτουργία στο 1 Mbps και 2 bit ανά baud για λειτουργία στα 2 Mbps.

Το πρώτο από τα ασύρματα LAN υψηλής ταχύτητας, το 802.11a, χρησιμοποιεί Ορθογώνια Πολύπλεξη με Διαίρεση Συχνότητας ή OFDM (Orthogonal Frequency Division Multiplexing) για να πετύχει μέχρι και 54 Mbps στην ευρύτερη ζώνη ISM των 5,4 GHz. Όπως δείχνει ο όρος FDM, χρησιμοποιούνται διαφορετικές συχνότητες, 52 συχνότητες, 48 για δεδομένα και 4 για συγχρονισμό. Μέρος του κινήτρου για χρήση της OFDM είναι η συμβατότητα με το ευρωπαϊκό σύστημα HiperLAN/2. Η τεχνική αυτή έχει καλή αποδοτικότητα φάσματος από πλευράς bit/Hz και καλή αντοχή στην εξασθένηση πολλαπλών διαδρομών.

Στη συνέχεια έχουμε την Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης ή HR-DSSS (High Rate Direct Sequence Spread Spectrum), άλλη μια τεχνική εξάπλωσης φάσματος η οποία χρησιμοποιεί 11 εκατομμύρια θραύσματα/sec για να επιτύχει ταχύτητα 11 Mbps στη ζώνη των 2,4 GHz. Ονομάζεται 802.11b αλλά δεν αποτελεί εξέλιξη του 802.11a. Αν και το 802.11b είναι βραδύτερο από το 802.11a, η εμβέλεια του είναι γύρω στις 7 φορές μεγαλύτερη, γεγονός πολύ σημαντικό σε πολλές περιπτώσεις.

Μια βελτιωμένη παραλλαγή του 802.11b, το 802.11g, εγκρίθηκε από την IEEE το Νοέμβριο του 2001, μετά από πολλές διαφωνίες σχετικά με την πατενταρισμένη τεχνολογία που χρησιμοποιούσε. Χρησιμοποιεί τη μέθοδο διαμόρφωσης OFDM του 802.11a, λειτουργεί όμως στη στενή ζώνη ISM των 2.4 GHz όπως και το 802.11b. Θεωρητικά μπορεί να λειτουργήσει έως τα 54 Mbps. Στην εικόνα 14 βλέπουμε σχηματικά τις τεχνικές μετάδοσης του προτύπου, τις συχνότητες που λειτουργούν και τους ρυθμούς μετάδοσης που υποστηρίζουν.

[25] http://en.wikipedia.org/wiki/Barker_code
[26] http://en.wikipedia.org/wiki/Baud



Εικόνα 14 Τεχνικές μετάδοσης του φυσικού επιπέδου του 802.11

3.6 Η πιστοποίηση Wi-Fi

Με την ανάπτυξη των προτύπων από την IEEE και την εμφάνιση μεγάλου αριθμού κατασκευαστών, αντίστοιχων συσκευών, εμφανίστηκε από νωρίς η ανάγκη διασφάλισης της συμβατότητας μεταξύ των διαφόρων συσκευών και προστασίας του καταναλωτή. Γι' αυτό το σκοπό ιδρύθηκε το 1999 η WECA (Wireless Ethernet Compatibility Alliance), ένας μη κερδοσκοπικός οργανισμός, που σκοπό έχει την πιστοποίηση των 802.11 ασύρματων συσκευών. Αυτός ο οργανισμός στη συνέχεια μετονομάστηκε σε Wi-Fi (Wireless Fidelity) Alliance και δημιούργησε ένα πακέτο από δοκιμές, για να πιστοποιεί τη διαλειτουργικότητα των 802.11b προϊόντων.

Σε αυτό τον οργανισμό μετέχουν κατασκευαστές ολοκληρωμένων κυκλωμάτων, παροχής υπηρεσιών WLAN, κατασκευαστές υπολογιστών και λογισμικού. Μερικές από τις εταιρίες που μετέχουν είναι η 3COM, Aironet, Apple, Breezecom, Cabletron, Compaq, Dell, Fujitsu, IBM, Intersil, Lucent Technologies, No Wires Needed, Nokia, Samsung, Symbol Technologies, Wayport, Zoom.

Εικόνα 15 Λογότυπο πιστοποίησης

Η ένωση αυτή δημιούργησε μια ακολουθία από δοκιμές, προκειμένου να δοκιμαστεί η συμβατότητα των IEEE 802 προϊόντων. Οι συσκευές που περνούσαν με επιτυχία τις δοκιμές, αποκτούσαν το λογότυπο Wi-Fi (Wireless Fidelity) που αποτελεί κατά συνέπεια μια πιστοποίηση, για τον υποψήφιο αγοραστή μιας συσκευής και μια εγγύηση της επένδυσης του. Ο καταναλωτής αγοράζοντας μια συσκευή με το λογότυπο Wi-Fi, έχει την εγγύηση ότι η συσκευή θα συνεργαστεί με οποιαδήποτε άλλη συσκευή που φέρει το ίδιο λογότυπο.

Τέλος να αναφερθεί ότι η πιστοποίηση αφορά τη λειτουργία 802.11b, 802.11g, 802.11a καθώς και τη WPA δυνατότητα. Να σημειωθεί ότι η Wi-Fi πιστοποίηση στο 802.11g απαιτεί την υποστήριξη του ρυθμού 54 Mbps, ενώ το επίσημο πρότυπο θέτει σαν υποχρεωτικούς ρυθμούς 1, 2, 5.5, 11, 6, 12, 24 Mbps, καθώς οι ανώτεροι ρυθμοί των 36, 48, 54 Mbps ορίζονται ως προαιρετικοί. Η διαδικασία πιστοποίησης που έχει αναπτυχθεί για τα 802.11a προϊόντα, ονομάζεται Wi-Fi5.

Κεφάλαιο 4 Μηχανισμοί ασφάλειας

Πριν ξεκινήσουμε την συζήτηση για την ασφάλεια των ασύρματών δικτύων θα πρέπει να ορίσουμε με τον κατάλληλο τρόπο την σημασία της λέξης ασφάλεια. Στην περίπτωση μας την έννοια της λέξης ασφάλεια υπολογιστών την ορίζουμε ως εξής:

Ορισμός: Ασφάλεια υπολογιστών. Είναι η προστασία των προσωπικών ή εμπιστευτικών πληροφοριών και των πόρων του υπολογιστή από άτομα ή οργανισμούς που θα μπορούσαν να τα χρησιμοποιήσουν ή να τα ανακοινώσουν σε άλλους με κακόβουλο τρόπο.

Τα ασύρματα δίκτυα δεδομένων μεταδίδουν τα δεδομένα τους χρησιμοποιώντας ραδιοσήματα. Σε αντίθεση με τις ενσύρματες τεχνολογίες δικτύωσης όπως το Ethernet, είναι δύσκολο να ελέγχουμε την πρόσβαση σε ένα ασύρματο μέσο μετάδοσης. Για παράδειγμα στα ενσύρματα δίκτυα για να έχουμε φυσική πρόσβαση στο δίκτυο θα πρέπει να χρησιμοποιήσουμε καλώδιο. Αν όμως χρησιμοποιούμε ασύρματο τρόπο δικτύωσης δεν χρειάζεται να είμαστε καν στο ίδιο κτήριο που υπάρχει το δίκτυο, μπορούμε να έχουμε πρόσβαση στο δίκτυο από το δρόμο ή ακόμα και από ένα διπλανό κτήριο. Η διαφορά μεταξύ των ασύρματων και των ενσύρματων δικτύων απεικονίζεται στην παρακάτω σχέση:

Στα ενσύρματα δίκτυα το μέσο είναι ιδιωτικό. Δεν χρειάζεται να ανησυχούμε για το ποιος συνδέεται διότι οι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να συνδεθούν στο δίκτυο και να αποκτήσουν πρόσβαση χωρίς να έχουν καλώδιο. Επίσης δεν χρειάζεται να εξασφαλίσουν την μεταφορά της κίνησης κατά μήκος του δικτύου να γίνεται εμπιστευτικά, διότι η κυκλοφορία έχει σταλεί ήδη εμπιστευτικά μέσω της καλωδίωσης που χρησιμοποιείται και δεν είναι προσβάσιμη σε χρήστες χωρίς άδεια. Αντίθετα στα ασύρματα δίκτυα το μέσο είναι κοινό. Καθένας χρησιμοποιώντας την κατάλληλη ασύρματη συσκευή, εντός της εμβέλειας του δικτύου, μπορεί να συνδεθεί. Επίσης η κίνηση στο δίκτυο πρέπει να γίνεται εμπιστευτικά γιατί ένας παράνομος χρήστης μπορεί να λάβει ασύρματα πακέτα και να μην εμφανίζεται στις φυσικές περιοχές ασφάλειας.

Όπως προκύπτει στα ασύρματα LANs, η ασφάλεια είναι ένα απαιτούμενο στοιχείο της τεχνολογίας, που εφαρμόζεται και αναπτύσσεται. Ιδιότητες της ασφαλούς επικοινωνίας αποτελούν τα ακόλουθα:

- ***Επικύρωση****:* πριν επιτραπεί η ανταλλαγή δεδομένων, με το ασύρματο δίκτυο, οι μεταξύ τους κόμβοι αναγνωρίζονται και ανταλλάσουν πιστοποιητικά που πρέπει να είναι επικυρωμένα.

- ***Κρυπτογράφηση:*** πριν την αποστολή ενός ασύρματου πακέτου δεδομένων, ο κάθε υπολογιστής που το στέλνει θα πρέπει να το κρυπτογραφήσει.

- ***Ακεραιότητα:*** διασφαλίζει ότι το στοιχείο που μεταδίδεται δεν έχει τροποποιηθεί.

- ***Μυστικότητα:*** είναι ο όρος που χρησιμοποιείται για να περιγράψει τα δεδομένα που προστατεύονται ενάντια στην επέμβαση από αναρμόδια συμβαλλόμενα μέρη.

4.1 Επικύρωση (Authentication) και μυστικότητα

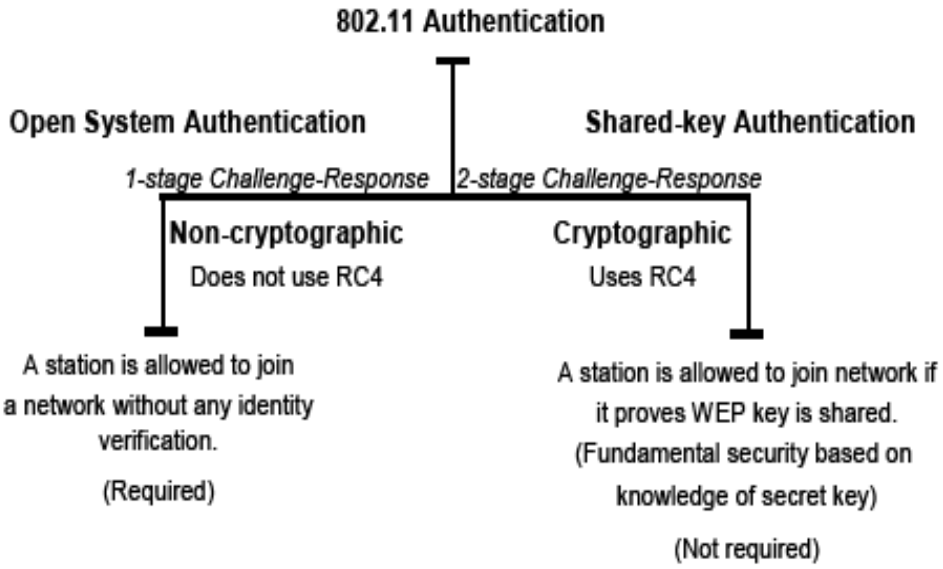
Πριν αρχίσουμε να συζητάμε για την διαδικασία τις επικύρωσης που πραγματοποιείται στο 802.11, υπενθυμίζουμε ότι οι έννοιες της επικύρωσης και του ελέγχου πρόσβασης είναι πολύ στενά συνδεδεμένες μεταξύ τους. Για να πραγματοποιήσουμε την διαδικασία της επικύρωσης πρέπει να αποκτήσουμε πρώτα έλεγχο πρόσβασης στο μέσο. Αν ένας σταθμός θέλει να συνδεθεί με ένα ασύρματο δίκτυο, πρέπει πρώτα να βρει ποια ασύρματα δίκτυα είναι διαθέσιμα. Στη συνέχεια θα πρέπει το δίκτυο να επικυρώσει το σταθμό και ο σταθμός πάλι με τη σειρά του να επικυρώσει το δίκτυο. Μόνο όταν αυτή η διαδικασία πραγματοποιηθεί θα μπορεί ο σταθμός να συνδεθεί με το δίκτυο που θέλει.

Τα σημεία πρόσβασης (AP) σε ένα 802.11 δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται beacons. Τα beacons είναι πλαίσια διαχείρισης, τα οποία ανακοινώνουν την ύπαρξη ενός δικτύου. Αυτά χρησιμοποιούνται από τα σημεία πρόσβασης για να μπορούν να τα ανιχνεύουν οι σταθμοί που θέλουν να συνδεθούν σε αυτά. Το κάθε beacon περιλαμβάνει ένα Service Set Identifier (SSID)[27] ή αλλιώς όνομα δικτύου που ανιχνεύει μοναδικά το ESS.

Όταν ένας σταθμός θέλει να συνδεθεί σε ένα δίκτυο έχει δύο επιλογές: την παθητική σάρωση και την ενεργητική. Στην πρώτη περίπτωση σαρώνει τα κανάλια προσπαθώντας να βρει beacons από τα σημεία πρόσβασης της περιοχής και στην δεύτερη περίπτωση ο σταθμός στέλνει αιτήσεις διερεύνησης (είτε σε ένα συγκεκριμένο SSID, είτε με το SSID ρυθμισμένο στο 0), σε όλα τα κανάλια ένα προς ένα. Αν το SSID είναι 0, αυτό σημαίνει ότι ο σταθμός ψάχνει οποιοδήποτε δίκτυο που μπορεί να έχει πρόσβαση. Όλοι οι σταθμοί πρόσβασης που λαμβάνουν αιτήσεις διερεύνησης, στέλνουν απάντηση.

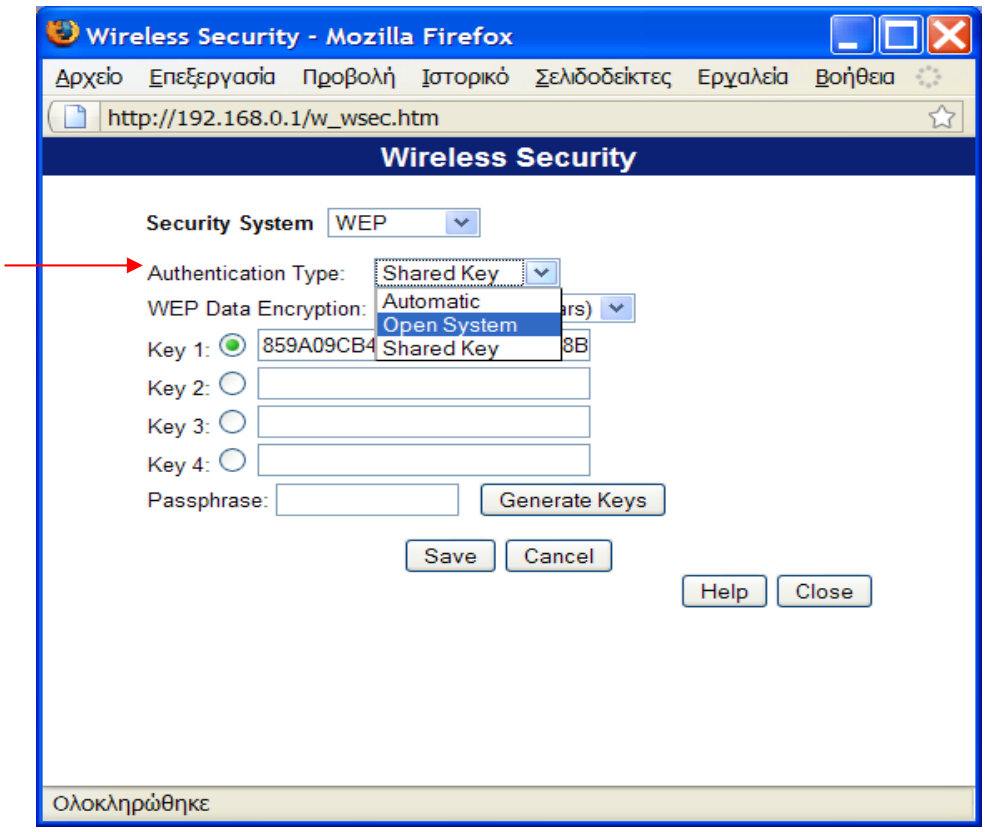
Το επόμενο βήμα είναι ο σταθμός να διαλέξει το δίκτυο που επιθυμεί να συνδεθεί. Η απόφαση αφήνεται στο χρήστη ή στο λογισμικό που μπορεί να επιλέξει βασιζόμενο στην ισχύ του σήματος και σε άλλα κριτήρια. Το 802.11 παρέχει δύο ειδών τρόπους επικύρωσης, την επικύρωση ανοιχτού κλειδιού (Open System Authentication – OSA) και την επικύρωση μοιρασμένου κλειδιού (Shared Key Authentication – SKA), όπως φαίνεται στην εικόνα 16. Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στο μήνυμα της αίτησης επικύρωσης. Τότε το δίκτυο μπορεί να δεχτεί ή να απορρίψει αυτή την πρόταση στο απαντητικό μήνυμα επικύρωσης, ανάλογα με το πώς είναι οι ρυθμίσεις ασφαλείας του δικτύου.

[27] http://en.wikipedia.org/wiki/SSID



Εικόνα 16 Ταξινόμηση των τεχνικών επικύρωσης του 802.11

Καθώς ρυθμίζουμε το σημείο πρόσβασης στο παράθυρο με το μενού επιλογών που μας εμφανίζει (όπως βλέπουμε στην εικόνα 17), παρατηρούμε ότι είτε ο χρήστης μπορεί να επιλέξει το είδος της επικύρωσης που θα χρησιμοποιήσει (Open system ή Shared key), είτε να το αφήσει καθαρά στην επιλογή του συστήματός του (Automatic).

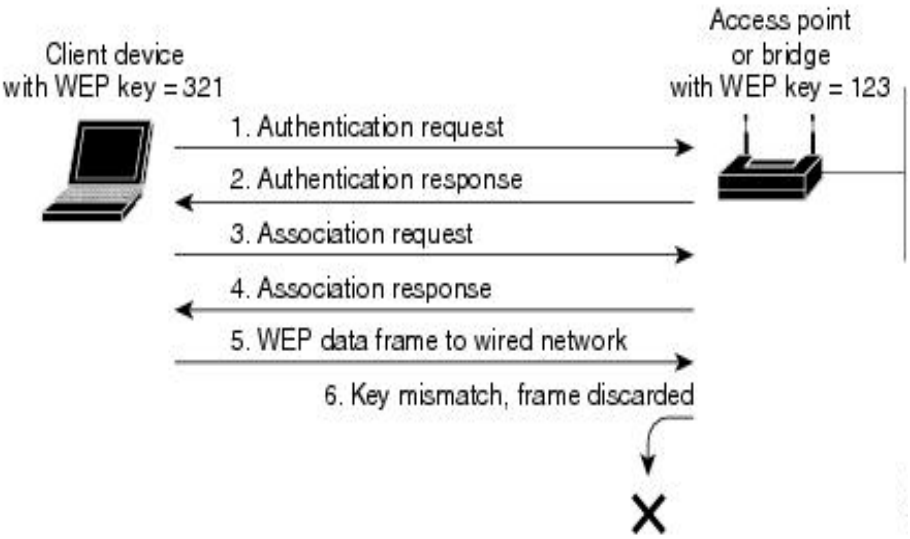


Εικόνα 17 Ρύθμιση του είδους της επικύρωσης

4.1.1 Επικύρωση ανοιχτού κλειδιού (open key authentication)

Είναι ο προεπιλεγμένος αλγόριθμος επικύρωσης που χρησιμοποιείται από το 802.11. Κάθε σταθμός που θέλει να συμμετέχει σε ένα δίκτυο στέλνει μια αίτηση επικύρωσης στο συγκεκριμένο σημείο πρόσβασης. Η αίτηση επικύρωσης περιλαμβάνει και τον αλγόριθμο επικύρωσης που ο σταθμός επιθυμεί (0 στην περίπτωση του ανοιχτού κλειδιού). Το σημείο πρόσβασης απαντάει πίσω με μια απάντηση επικύρωσης, επικυρώνοντας έτσι το σταθμό να συμμετέχει στο δίκτυο, αν αυτό έχει ρυθμιστεί να δέχεται την επικύρωση ανοιχτού κλειδιού, σαν έγκυρο τύπο επικύρωσης. Με λίγα λόγια το σημείο πρόσβασης δεν κάνει κανένα έλεγχο ως προς την ταυτότητα του σταθμού και επιτρέπει σε όλους τους σταθμούς να συμμετέχουν στο δίκτυο.

Δηλαδή η επικύρωση ανοιχτών συστημάτων επιτρέπει σε οποιαδήποτε συσκευή να επικυρώνεται και στη συνέχεια να προσπαθεί να επικοινωνήσει με το σημείο πρόσβασης. Χρησιμοποιώντας επικύρωση ανοιχτού κλειδιού οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης αλλά η συσκευή μπορεί να επικοινωνεί μόνο αν τα WEP[28] κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης. Συσκευές που δεν χρησιμοποιούν WEP, δεν επιχειρούν επικύρωση με κάποιο σημείο πρόσβασης που χρησιμοποιεί WEP. Στην εικόνα 18 φαίνεται η ακολουθία επικύρωσης ανάμεσα σε μια συσκευή που προσπαθεί να επικυρωθεί και σε ένα σημείο πρόσβασης που χρησιμοποιεί επικύρωση ανοιχτού κλειδιού. Στο παράδειγμα αυτό το WEP κλειδί της συσκευής δεν ταιριάζει με το κλειδί του σημείου πρόσβασης και έτσι η συσκευή μπορεί μόνο να επικυρωθεί αλλά όχι να αποκτήσει πρόσβαση στα δεδομένα.



Εικόνα 18 Ακολουθία για επικύρωση ανοιχτού κλειδιού

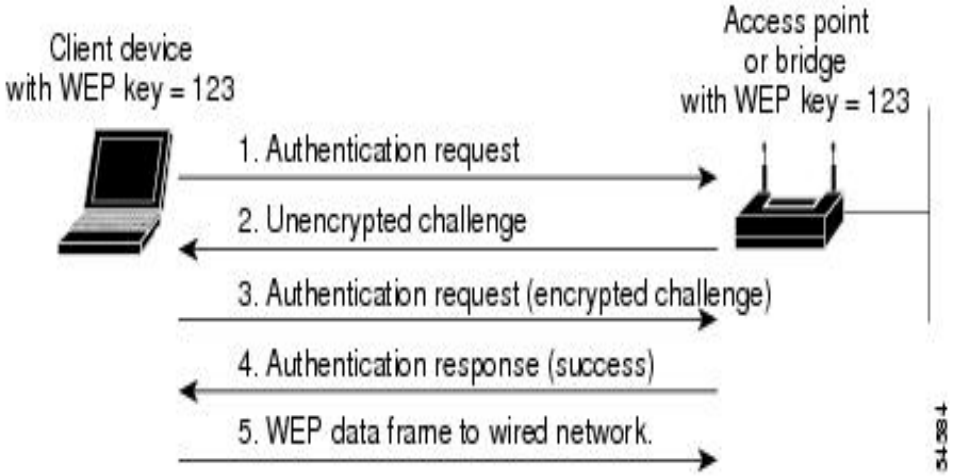
[28] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

4.1.2 Επικύρωση μοιρασμένου κλειδιού (shared key authentication)

Δημιουργήθηκε για να παρέχει την περισσότερη ασφάλεια από τους δύο τύπους. Η επικύρωση μοιρασμένου κλειδιού βασίζεται στο σύστημα πρόκλησης-απάντησης. Η μέθοδος αυτή χωρίζει τους σταθμούς σε δύο ομάδες. Η πρώτη ομάδα περιλαμβάνει τους σταθμούς που τους έχει επιτραπεί η πρόσβαση στο δίκτυο και η δεύτερη ομάδα περιέχει όλους τους άλλους σταθμούς. Για να χρησιμοποιήσουμε αυτή τη μέθοδο επικύρωσης, προϋποθέτει ότι το σημείο πρόσβασης και ο σταθμός είναι συμβατοί με τη λειτουργία WEP και ότι έχουν μεταξύ τους ένα προ-μοιρασμένο κλειδί. Αυτό σημαίνει ότι ένα κοινό κλειδί πρέπει να μοιραστεί σε όλους τους σταθμούς που τους έχει επιτραπεί να έχουν πρόσβαση στο δίκτυο, πριν επιχειρήσουν την διαδικασία της επικύρωσης.

Κατά τη διάρκεια της επικύρωσης του μοιρασμένου κλειδιού το σημείο πρόσβασης στέλνει ένα μη κρυπτογραφημένο κείμενο πρόκληση σε οποιαδήποτε συσκευή προσπαθεί να επικοινωνήσει με το σημείο πρόσβασης. Η συσκευή η οποία έχει κάνει αίτηση για επικύρωση, κρυπτογραφεί το κείμενο πρόκληση και το στέλνει πίσω στο σημείο πρόσβασης. Εάν το κείμενο πρόκληση είναι κρυπτογραφημένο σωστά, το σημείο πρόσβασης επιτρέπει την επικύρωση στη συσκευή που έχει κάνει αίτηση.

Τόσο το μη κρυπτογραφημένο κείμενο πρόκλησης όσο και το κρυπτογραφημένο, μπορούν να παρακολουθηθούν με αποτέλεσμα το σημείο πρόσβασης να γίνεται εύκολος στόχος από έναν εισβολέα, ο οποίος θα υπολογίσει το WEP κλειδί συγκρίνοντας το κρυπτογραφημένο και το μη κρυπτογραφημένο κείμενο. Εξαιτίας αυτής της αδυναμίας, η επικύρωση μοιρασμένου κλειδιού, είναι λιγότερο ασφαλής από την επικύρωση ανοιχτού κλειδιού. Στην εικόνα 19 βλέπουμε την ακολουθία επικύρωσης που πραγματοποιείται ανάμεσα σε μια συσκευή που προσπαθεί να επικυρωθεί και σε ένα σημείο πρόσβασης που χρησιμοποιεί επικύρωση μοιρασμένου κλειδιού. Σε αυτό το παράδειγμα το WEP κλειδί της συσκευής ταιριάζει με το κλειδί του σημείου πρόσβασης και έτσι η συσκευή μπορεί να επικυρωθεί και να επικοινωνήσει.



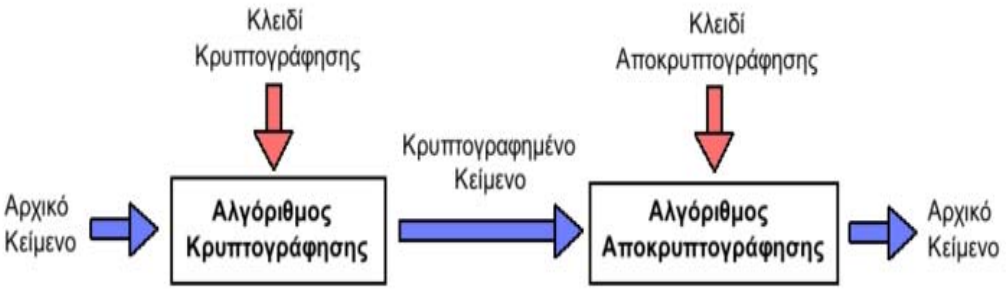
Εικόνα 19 Επικύρωση κοινού κλειδιού

4.2 Κρυπτογράφηση WEP (Wired Equivalent Privacy)

Η διαδικασία μεταμφίεσης (δυαδικών) δεδομένων προκειμένου να κρυφτεί το περιεχόμενο πληροφοριών της καλείται κρυπτογράφηση (encryption, συμβολίζεται με E). Τα δεδομένα που δεν κρυπτογραφούνται αποτελούν το plaintext (συμβολίζεται με P) και τα δεδομένα που κρυπτογραφούνται αποτελούν το cipher text (συμβολίζεται με C). Η διαδικασία μετατροπής του chiphertext σε plaintext καλείται αποκρυπτογράφηση (decryption, συμβολίζεται με D).

Ένας αλγόριθμος κρυπτογράφησης ή cipher είναι μια μαθηματική λειτουργία που χρησιμοποιείται για την κρυπτογράφηση ή αποκρυπτογράφηση δεδομένων. Οι σύγχρονοι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν μια ακολουθία κλειδιού (που συμβολίζεται με k) για να τροποποιήσουν τα εξαγόμενα τους.

Η λειτουργία κρυπτογράφησης E ενεργεί επάνω στο P για να παραγάγει το C.
$E_k(P) = C$
Ενώ στην αντίστροφη διαδικασία η λειτουργία αποκρυπτογράφησης D ενεργεί επάνω στο C για να παραγάγει το P
$D_k(C) = P$
το ίδιο κλειδί μπορεί να χρησιμοποιηθεί στην κρυπτογράφηση και αποκρυπτογράφηση οπότε και θα έχουμε
$D_k(E_k(P)) = P$



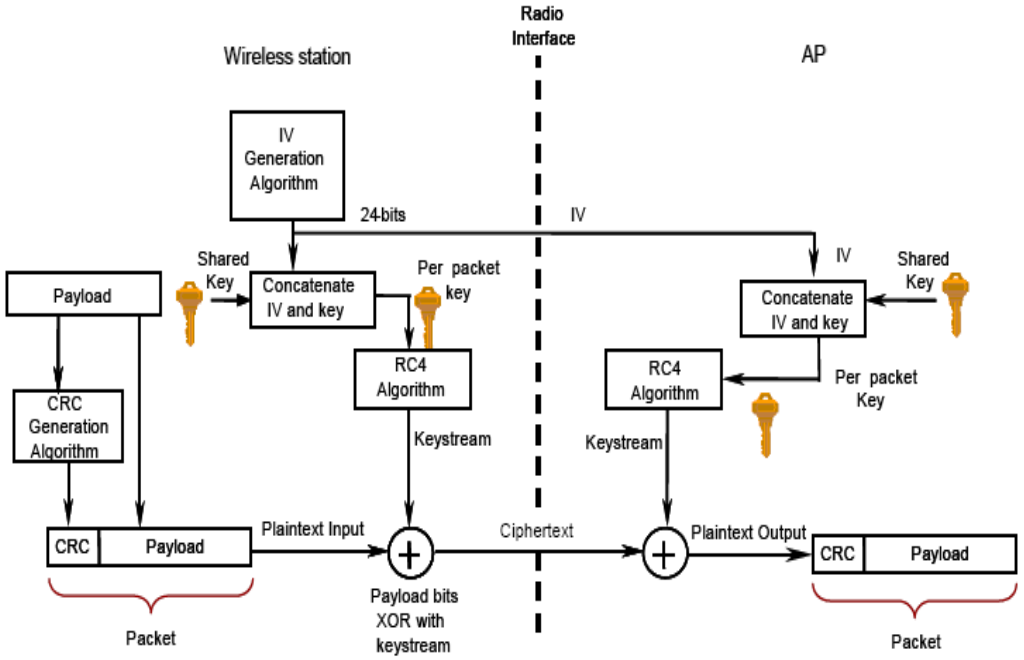
Εικόνα 20 Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Το αρχικό πρότυπο 802.11 για τα ασύρματα δίκτυα, όριζε μια επιλογή για την παροχή ασφάλειας το Wired Equivalent Privacy (WEP). Στο WEP ένα κοινό κλειδί ρυθμίζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Στο 802.11 πρότυπο, τα δεδομένα μεταφέρονται καθαρά από προεπιλογή. Εάν επιθυμούμε εμπιστευτικότητα, με την επιλογή του WEP μπορούμε να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν. Ο αλγόριθμός του WEP χρησιμοποιεί τον συμμετρικό αλγόριθμο κρυπτογράφησης ακολουθίας RC4[29]. Ο αλγόριθμός χρησιμοποιεί ένα μυστικό κλειδί, που μοιράζεται ανάμεσα σε ένα κινητό σταθμό (για παράδειγμα ένα laptop με μια Ethernet κάρτα) και στο σταθμό βάσης του σημείου πρόσβασης, ώστε να προστατευτεί η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω του δικτύου.

4.2.1 Πως λειτουργεί το WEP

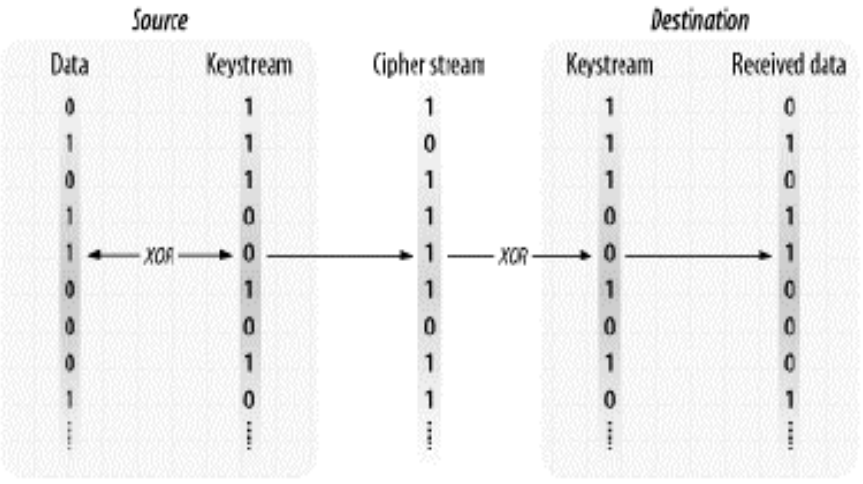
Το WEP για να προστατεύσει τα δεδομένα και να εξασφαλίσει την εμπιστευτικότητα απαιτεί τη χρήση του αλγόριθμου κρυπτογράφησης RC4, ο οποίος είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας (μυστικού κλειδιού) και CRC-32[30] άθροισμα ελέγχου για την ακεραιότητα. Γενικά, ένας αλγόριθμος κρυπτογράφησης ακολουθίας χρησιμοποιεί μια ακολουθία bits, αποκαλούμενη ακολουθία κλειδιού (key stream). Στη συνέχεια το key stream συνδυάζεται με το μήνυμα για να παραγάγει το κρυπτογράφημα (cipher text). Για να ανακτήσει τον αρχικό μήνυμα, ο δέκτης επεξεργάζεται το κρυπτογράφημα με το ίδιο key stream.

[29] http://en.wikipedia.org/wiki/RC4
[30] http://en.wikipedia.org/wiki/CRC-32



Εικόνα 21 Απεικόνιση της διαδικασίας κρυπτογράφησης WEP

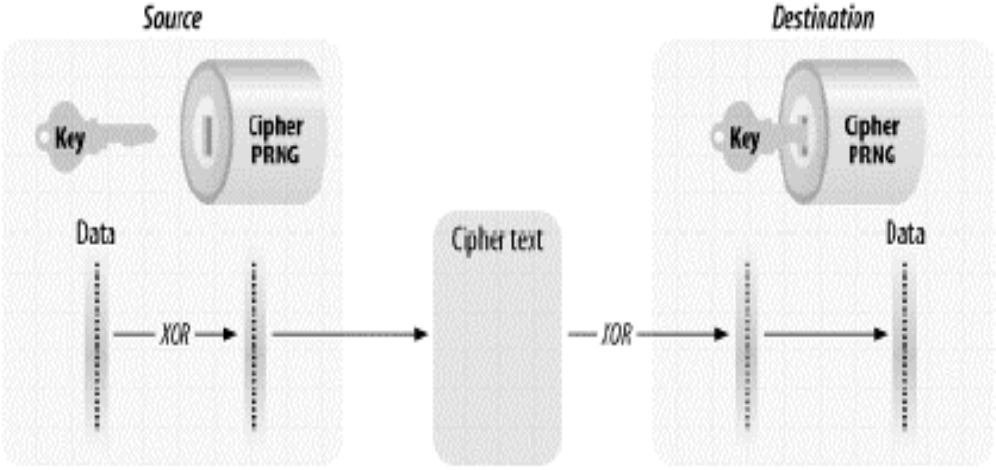
Ο RC4 χρησιμοποιεί αποκλειστικό Η (XOR) για να συνδυάσει το key stream και το κρυπτογράφημα. Στην εικόνα 22 που ακολουθεί βλέπουμε την διαδικασία που πραγματοποιείται:



Εικόνα 22 Διαδικασία κρυπτογράφησης/αποκρυπτογράφησης

Οι περισσότεροι αλγόριθμοι ακολουθίας αποκρυπτογράφησης λειτουργούν παίρνοντας ένα σχετικά μικρό μυστικό κλειδί και το επεκτείνουν στο ψευδοτυχαίο

key stream που έχει το ίδιο μήκος με το μήνυμα. Αυτή η διαδικασία φαίνεται στο παρακάτω σχήμα. Η ψευδοτυχαία γεννήτρια αριθμού (PRNG)[31] είναι ένα σύνολο κανόνων που χρησιμοποιούνται για να επεκταθεί το κλειδί σε key stream. Για να ανακτήσουν τα δεδομένα, και οι δύο πλευρές πρέπει να μοιραστούν το ίδιο μυστικό κλειδί και να χρησιμοποιούν τον ίδιο αλγόριθμο για να επεκτείνουν το κλειδί σε μια ψευδοτυχαία ακολουθία.



Εικόνα 23 Η λειτουργία του αλγόριθμου ακολουθίας

Επειδή η ασφάλεια του αλγόριθμου κρυπτογράφησης ακολουθίας στηρίζεται εξ' ολοκλήρου στην τυχαία ακολουθία του key stream, ο σχεδιασμός της επέκτασης κλειδιού σε key stream είναι ύψιστης σημασίας.

4.2.2 Ασφάλεια της ακολουθίας κρυπτογράφησης

Ένα αποκλειστικά τυχαίο key stream ονομάζεται one-time pad και είναι το μόνο γνωστό σενάριο κρυπτογράφησης που αποδεικνύεται από μαθηματική άποψη ότι παρέχει προστασία από ορισμένους τύπους επιθέσεων. Τα one-time pads δεν χρησιμοποιούνται όμως συνήθως επειδή το key stream πρέπει να είναι εντελώς τυχαίο, να έχει το ίδιο μήκος με τα δεδομένα που θα προστατευθούν και δεν μπορεί ποτέ να επαναχρησιμοποιηθεί. Η κρυπτογράφηση ακολουθίας είναι ένας συμβιβασμός μεταξύ της ασφάλειας και της πρακτικότητας. Η τέλεια τυχαία ακολουθία (και η τέλεια ασφάλεια) ενός one-time pad είναι ελκυστική, αλλά οι πρακτικές δυσκολίες και το κόστος που απαιτούνται για την παραγωγή και τη διανομή του υλικού κλειδιών αξίζει μόνο για τα σύντομα μηνύματα που απαιτούν την ανώτατη ασφάλεια. Οι αλγόριθμοι αποκρυπτογράφησης ακολουθίας χρησιμοποιούν ένα λιγότερο τυχαίο key stream αλλά αρκετά τυχαίο για τις περισσότερες εφαρμογές.

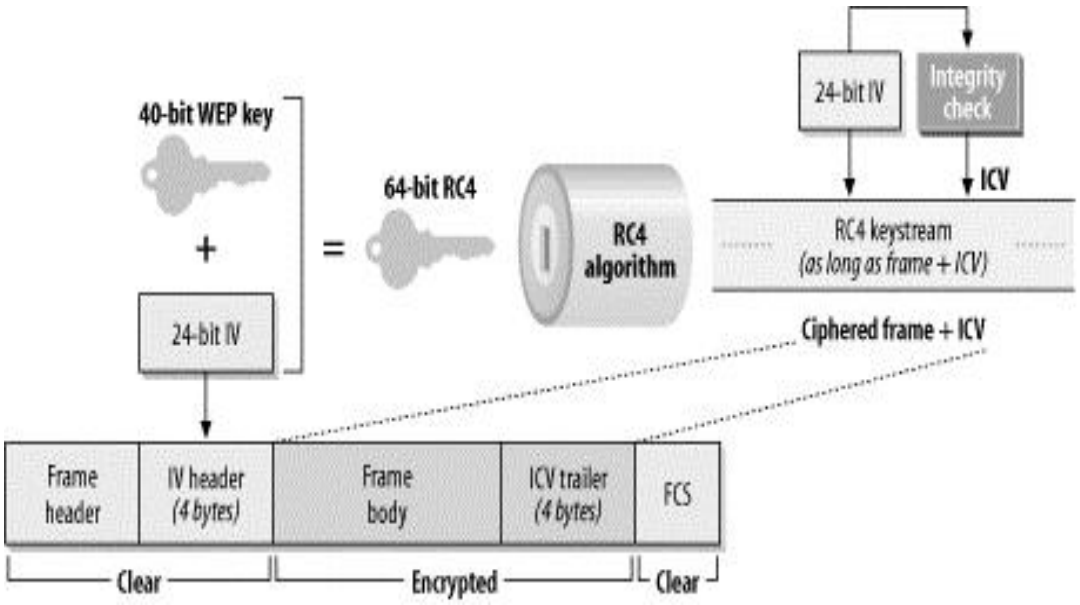
[31] http://en.wikipedia.org/wiki/PRNG

4.2.3 Η διαδικασία κρυπτογράφησης στο WEP

Η ασφάλεια των επικοινωνιών έχει τρεις βασικούς στόχους. Οποιοδήποτε πρωτόκολλο που προσπαθεί να ασφαλίσει δεδομένα καθώς αυτά ταξιδεύουν σε ένα δίκτυο, πρέπει να βοηθήσει τους διαχειριστές του δικτύου για την επίτευξη αυτών των στόχων. Οι στόχοι αυτοί που πρέπει να τηρούνται είναι αξιοπιστία, εμπιστευτικότητα και επικύρωση.

Το WEP παρέχει λειτουργίες που βοηθούν στην επίτευξη αυτών των στόχων. Η κρυπτογράφηση του σώματος ενός πλαισίου, υποστηρίζει την εμπιστευτικότητα. Ο έλεγχος ακολουθίας προστατεύει την ακεραιότητα των δεδομένων κατά την μεταφορά τους και επιτρέπει στους δέκτες να επαληθεύσουν ότι τα δεδομένα που έλαβαν δεν μεταβλήθηκαν κατά τη μεταφορά. Το WEP επίσης επιτρέπει την διαμόρφωση ενός ισχυρότερου κλειδιού αυθεντικοποίησης, των σταθμών για τα σημεία πρόσβασης. Στην πράξη το WEP υστερεί σε όλους αυτούς τους τομείς. Η εμπιστευτικότητα θέτεται σε κίνδυνο από ελλείψεις στο RC4 cipher. Ο έλεγχος ακεραιότητας είναι ελλιπώς σχεδιασμένος.

Το WEP πάσχει επίσης από την προσέγγιση που αυτό λαμβάνει. Κρυπτογραφεί τα πλαίσια που διασχίζουν το ασύρματο μέσο αλλά τίποτα δεν έχει γίνει για την προστασία των πλαισίων καθώς αυτά διασχίζουν έναν ενσύρματο κορμό, όπου εκεί μπορούν να υποβληθούν σε διάφορες επιθέσεις. Επιπλέον το WEP έχει σχεδιαστεί για να διασφαλίζει το δίκτυο από εξωτερικούς εισβολείς.



Εικόνα 24 Οι λειτουργίες του WEP

Η εμπιστευτικότητα και η ακεραιότητα υλοποιούνται ταυτόχρονα όπως βλέπουμε και από την εικόνα 24. Αναλυτικά τα βήματα που ακολουθούνται στη διαδικασία κρυπτογράφησης του WEP είναι τα ακόλουθα:

1. Στο plaintext εφαρμόζεται ένας αλγόριθμος ακεραιότητας ελέγχου (Integrity Check Algorithm). Το πρότυπο 802.11 ορίζει την χρήση του CRC-32 ώστε να παραχθεί μια τιμή ελέγχου ακεραιότητας η ICV (Integrity Check Value). Το ICV προστατεύει το περιεχόμενο από την αλλοίωση και διασφαλίζει ότι το πλαίσιο δεν έχει αλλάξει κατά τη μεταφορά. Τόσο το πλαίσιο όσο και το ICV κρυπτογραφούνται και τα δύο και έτσι το ICV δεν είναι διαθέσιμο στους επιτιθέμενους.

2. Αυτή η τιμή επισυνάπτεται στο τέλος του αρχικού plaintext μηνύματος.

3. Το WEP προσδιορίζει τη χρήση ενός 40-bit μυστικού κλειδιού. Ένα τυχαίο διάνυσμα ακολουθίας 24-bit (IV) δημιουργείται και προστίθεται στην αρχή του μυστικού κλειδιού, για να δημιουργηθεί ένα 64-bit κλειδί RC-4. Τα πρώτα 24 bit του RC-4 κλειδιού είναι το IV και τα υπόλοιπα 40 bit to WEP κλειδί. Στη συνέχεια να εισαχθεί στον RC-4 αλγόριθμο. ώστε να δημιουργηθεί η τιμή WEP από την γεννήτρια ψευδοτυχαίων αριθμών (PRNG)[32].

4. Από την έξοδο WEP της PRNG προκύπτει το κρυπτογραφημένο stream cipher[33].

5. Στη συνέχεια το stream cipher, πολυπλέκεται με XOR μαζί με το plaintext/ ICV μήνυμα, ώστε να παράγουν το WEP chiphertext.

6. Το chiphertext ενσωματώνεται μαζί με το IV του plaintext και μεταφέρεται. Για να μπορέσει ο παραλήπτης να αποκρυπτογραφήσει το πλαίσιο, το IV τοποθετείται στην επικεφαλίδα του πλαισίου.

4.2.4 Τα κλειδιά που χρησιμοποιούνται στο WEP

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

- **Σταθερό μήκος**: Συνήθως 40 ή 104 bit

- **Στατικά:** Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.

- **Μεριζόμενα (shared):** Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.

- **Συμμετρικά:** Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

[32] http://en.wikipedia.org/wiki/Pseudorandom_number_generator
[33] http://en.wikipedia.org/wiki/Stream_cipher

Σύμφωνα με το πρότυπο IEEE 802.11, η διάθεση των κλειδιών στα σημεία πρόσβασης και στις ασύρματες συσκευές πρέπει να γίνεται με ασφαλείς μεθόδους ανεξάρτητες του πρωτοκόλλου. Για να προστατευτούμε από ισχυρές επιθέσεις αποκρυπτογράφησης, το WEP χρησιμοποιεί ένα σύνολο μέχρι τεσσάρων προεπιλεγμένων κλειδιών, και μπορεί επίσης να χρησιμοποιήσει κλειδιά ζευγών (pair wise), αποκαλούμενα χαρτογραφημένα κλειδιά, όταν επιτρέπονται. Τα χαρτογραφημένα κλειδιά μοιράζονται μεταξύ όλων των σταθμών. Μόλις λάβει ένας σταθμός τα κλειδιά προεπιλογής για το σύνολο υπηρεσιών του, αυτός μπορεί να επικοινωνήσει με τη χρησιμοποίηση WEP.

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

Οι τυποποιημένες εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά RC4 64 bit. Το μεγαλύτερο μέρος της βιομηχανίας όμως έχει κινηθεί προς ένα 128-bit δημόσιο RC4 κλειδί (εικόνα 25). Το πρότυπο 64-bit WEP χρησιμοποιεί ένα κλειδί 40 bit (επίσης γνωστό ως WEP-40) το οποίο συνδέεται με την αρχή ενός 24- bit διανύσματος και διαμορφώνει το RC4 κλειδί κυκλοφορίας. Την εποχή που συντασσόταν τα αρχικά πρότυπα WEP, η κυβέρνηση των Η.Π.Α εξέδιδε περιορισμούς στην κρυπτογραφική τεχνολογία για το μέγεθος του κλειδιού. Μόλις εγκαταλείφτηκαν οι περιορισμοί όλοι οι βασικοί κατασκευαστές εφάρμοσαν τελικά το 128- bit WEP πρωτόκολλο χρησιμοποιώντας μέγεθος κλειδιού 104 bit (επίσης γνωστό ως WEP-104).

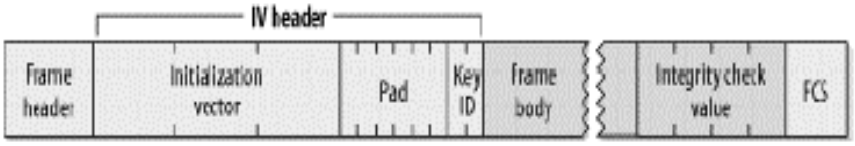
Ένα 128- bit WEP κλειδί σχεδόν πάντα εισάγεται από τους χρήστες σαν μια ακολουθία 26 δεκαεξαδικών (βάση το 16) χαρακτήρων (0-9 και AF). Κάθε χαρακτήρας αντιπροσωπεύει 4 bit του κλειδιού. 26 ψηφία τεσσάρων bit δίνουν 104 bit και η προσθήκη του 24 bit IV παράγει το τελικό 128- bit κλειδί WEP. Ένα 256-bit σύστημα WEP είναι διαθέσιμο από μερικούς προμηθευτές, και όπως με το128-bit WEP, τα 24 bit είναι για το IV, αφήνοντας 232 πραγματικά bit για την προστασία. Αυτά τα 232 bit εισάγονται χαρακτηριστικά ως 58 δεκαδικοί χαρακτήρες. (58 × 4 = 232 μπιτ) + 24 IV μπιτ = 256-bit κλειδί WEP.

Εικόνα 25 Επιλογή των κλειδιών WEP

Το μέγεθος του κλειδιού δεν είναι ο μόνος σημαντικός περιορισμός ασφάλειας σε WEP. Το WEP, δεν είναι ένα καλά σχεδιασμένο κρυπτογραφικό σύστημα, και τα πρόσθετα bit στο κλειδί δεν έχουν ιδιαίτερη σημασία. Η καλύτερη αποκαλυπτόμενη δημόσια επίθεση ενάντια στο WEP μπορεί να ανακτήσει το κλειδί σε μερικά δευτερόλεπτα όπως θα δούμε σε επόμενο κεφάλαιο.

4.2.5 Πλαίσια WEP

Όταν χρησιμοποιείται το WEP το σώμα των πλαισίων επεκτείνεται από οκτώ bytes. Τέσσερα bytes χρησιμοποιούνται για την επικεφαλίδα του σώματος του πλαισίου IV, και τέσσερα χρησιμοποιούνται για το ICV. Αυτά φαίνονται στην εικόνα 26.



Εικόνα 26 Επεκτάσεις πλαισίου WEP

Η επικεφαλίδα IV χρησιμοποιεί 3 bytes για το 24-bit IV, με το τέταρτο byte να χρησιμοποιείται για γέμισμα και προσδιορισμό κλειδιού (key identification). Όταν

ένα προεπιλεγμένο κλειδί χρησιμοποιείται, το υποπόδιο key-ID προσδιορίζει το προεπιλεγμένο κλειδί που χρησιμοποιήθηκε για να κρυπτογραφήσει το πλαίσιο. Εάν χρησιμοποιείται μια σχέση χαρτογράφησης κλειδιού, το υποπόδιο key-ID είναι 0. Τα 6 bit γεμίσματος του τελευταίου byte πρέπει να είναι 0. Ο έλεγχος ακεραιότητας είναι 32-bit, επισυνάπτεται στο σώμα του πλαισίου και προστατεύεται από RC4.

4.2.6 Η διανομή του κλειδιού

Η διαδικασία της διανομής του κλειδιού είναι ένα από τα μέρη στα οποία πάσχει το WEP. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να διανεμηθούν σε όλους τους σταθμούς που συμμετέχουν σε ένα 802.11 σύνολο υπηρεσιών και ασφαλίζονται από WEP. Το 802.11 πρότυπο, εντούτοις, αποτυγχάνει να διευκρινίσει τον μηχανισμό διανομής κλειδιού. Το αποτέλεσμα είναι ότι οι προμηθευτές δεν έχουν κάνει τίποτα. Τα προβλήματα που παρουσιάζονται με την διανομή του κλειδιού είναι τα εξής:

- Τα κλειδιά δεν μπορούν να θεωρηθούν μυστικά γιατί θα πρέπει να εισαχθούν στατικά στους οδηγούς software ή firmware[34] στην ασύρματη κάρτα. Με κάθε τρόπο, το κλειδί δεν μπορεί να προστατευθεί από έναν τοπικό χρήστη που θέλει να το ανακαλύψει.

- Οι οργανισμοί με μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύσουν το κλειδί στους πληθυσμούς χρηστών και έτσι αυτό δεν παραμένει μυστικό.

- Εάν τα κλειδιά είναι προσιτά στους χρήστες, κατόπιν όλα τα κλειδιά πρέπει να αλλάζουν όποτε μέλη του προσωπικού φεύγουν από την επιχείρηση. Η γνώση κλειδιών WEP επιτρέπει σε έναν χρήστη να φτιάξει έναν 802.11 σταθμό και να ελέγχει παθητικά και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί. Το WEP δεν μπορεί να προστατεύσει ενάντια στα εξουσιοδοτημένα μέλη που έχουν επίσης το κλειδί.

4.2.7 Κρυπτογραφικές ιδιότητες WEP

Η επαναχρησιμοποίηση ακολουθίας κλειδιού είναι η σημαντικότερη αδυναμία σε οποιοδήποτε κρυπτογραφικό σύστημα βασισμένο σε αλγόριθμο κρυπτογράφησης ακολουθίας. Όταν τα πλαίσια κρυπτογραφούνται με το ίδιο RC4 key stream, το XOR των δύο κρυπτογραφημένων πακέτων είναι ισοδύναμο με το XOR των δύο πακέτων plaintext. Με την ανάλυση των διαφορών μεταξύ των δύο ακολουθιών από κοινού με τη δομή του σώματος πλαισίων, οι επιτιθέμενοι μπορούν να μάθουν για το περιεχόμενο των πλαισίων plaintext.

[34] http://en.wikipedia.org/wiki/Firmware

Για να αποτρέψει την επαναχρησιμοποίηση key stream, το WEP χρησιμοποιεί το IV για να κρυπτογραφήσει διαφορετικά πακέτα με διαφορετικά RC4 κλειδιά. Εντούτοις, το IV είναι μέρος της επικεφαλίδας πακέτων και δεν κρυπτογραφείται, έτσι οι ωτακουστές έχουν αρκετές πληροφορίες για τα πακέτα που κρυπτογραφούνται με το ίδιο RC4 κλειδί.

Τα προβλήματα εφαρμογής μπορούν να συμβάλουν στην έλλειψη ασφάλειας. Το 802.11 αναγνωρίζει ότι η χρησιμοποίηση του ίδιου IV για έναν μεγάλο αριθμό πλαισίων είναι επισφαλής και πρέπει να αποφευχθεί. Το πρότυπο επιτρέπει τη χρησιμοποίηση ενός διαφορετικού IV για κάθε πλαίσιο, αλλά αυτή δεν απαιτείται. Το WEP ενσωματώνει έναν έλεγχο ακεραιότητας, αλλά ο αλγόριθμος που χρησιμοποιείται είναι ένας κυκλικός έλεγχος πλεονασμού (CRC)[35]. Οι CRCs μπορούν να ανιχνεύσουν τις αλλαγές ενός bit με υψηλή πιθανότητα, αλλά δεν είναι ασφαλείς κρυπτογραφικά.

Κρυπτογραφικά ασφαλείς έλεγχοι ακεραιότητας είναι βασισμένοι σε απρόβλεπτες λειτουργίες. Με τις απρόβλεπτες λειτουργίες, εάν ο επιτιθέμενος αλλάζει ακόμη και ένα bit του πλαισίου, ο έλεγχος ακεραιότητας θα αλλάξει με απρόβλεπτο τρόπο. Η πιθανότητα ενός επιτιθεμένου να βρει ένα αλλαγμένο πλαίσιο με τον ίδιο έλεγχο ακεραιότητας είναι τόσο μικρή που δεν μπορεί να γίνει πραγματικά. Οι CRCs είναι απλά μαθηματικά, και είναι εύκολο να προβλεφθεί πώς η αλλαγή ενός μόνο bit έχει επιπτώσεις στο αποτέλεσμα του υπολογισμού CRC. (Αυτή η ιδιότητα χρησιμοποιείται συχνά από τα συμπιεσμένα δεδομένα για την επανάκτηση! Εάν μερικά συγκεκριμένα bit είναι λάθος, μπορούν μερικές φορές να προσδιοριστούν και να διορθωθούν με βάση μια τιμή CRC).

4.2.8 Προβλήματα που παρουσιάζονται

Οι κρυπτογράφοι έχουν εντοπίσει πολλές αδυναμίες στο WEP. Οι σχεδιαστές καθόρισαν τη χρήση RC4, ο οποίος γίνεται αποδεκτός ευρέως ως ισχυρός κρυπτογραφικός αλγόριθμος κρυπτογράφησης. Οι επιτιθέμενοι, εντούτοις, δεν περιορίζονται σε μια πλήρως μετωπική επίθεση στους κρυπτογραφικούς αλγορίθμους. Μπορούν να επιτεθούν σε οποιοδήποτε αδύνατο σημείο στο κρυπτογραφικό σύστημα. Μέθοδοι για να ηττηθεί το WEP προκύπτουν από παντού. Οι αδυναμίες σχεδιασμού του WEP άρχισαν να φαίνονται όταν η ομάδα Ασφάλειας Εφαρμογών Επικύρωσης και Κρυπτογραφίας (ISAAC) του Πανεπιστημίου του Berkeley δημοσίευσε προκαταρκτικά αποτελέσματα βασισμένα στην ανάλυση του προτύπου WEP. Κανένα από τα προβλήματα που προσδιορίζονται από τους ερευνητές δεν εξαρτάται από το σπάσιμο του RC4. Τα βασικά προβλήματα που βρέθηκαν είναι:

1. Η χειρωνακτική διαχείριση κλειδιών. Μόλις ένας χρήστης λάβει τα κλειδιά WEP, οι επιθέσεις sniffing είναι εύκολες.

[35] http://en.wikipedia.org/wiki/Cyclic_redundancy_check

2. Το τυποποιημένο WEP προσφέρει ένα δημόσιο μυστικό κλειδί από μόνο 40 bit. Οι εμπειρογνώμονες ασφάλειας έχουν εξετάσει από καιρό την επάρκεια του 40-bit ιδιωτικού κλειδιού, και πολλοί συστήνουν τα ευαίσθητα στοιχεία να προστατεύονται από τουλάχιστον 128-bit κλειδιά.

3. Οι αλγόριθμοι κρυπτογράφησης ακολουθίας είναι τρωτοί στην ανάλυση όταν επαναχρησιμοποιείται το key stream. Η χρήση του IV από το WEP πληροφορεί έναν επιτιθέμενο για την επαναχρησιμοποίηση του key stream. Δύο πλαίσια που μοιράζονται το ίδιο IV σχεδόν βέβαια χρησιμοποιούν το ίδιο μυστικό κλειδί και key stream.

4. Η σπάνια νέα εισαγωγή κλειδιών επιτρέπει στους επιτιθεμένους να συγκεντρώσουν ότι η ομάδα του Berkeley καλεί λεξικά αποκρυπτογράφησης, δηλαδή μεγάλες συλλογές των πλαισίων που κρυπτογραφούνται με τα ίδια key streams.

5. Το WEP χρησιμοποιεί ένα CRC για τον έλεγχο ακεραιότητας. Αν και η τιμή του ελέγχου ακεραιότητας κρυπτογραφείται από το RC4 key stream, οι CRCs δεν είναι κρυπτογραφικά ασφαλείς. Η χρήση ενός αδύναμου ελέγχου ακεραιότητας δεν αποτρέπει τους επιτιθεμένους από το να τροποποιούν διαφανώς πλαίσια.

6. Το σημείο πρόσβασης είναι σε προνομιούχα θέση να αποκρυπτογραφεί πλαίσια. Ένας σταθμός μπορεί να δεχθεί επίθεση με την εξαπάτηση του σημείου πρόσβασης στην αναμετάδοση των πλαισίων που κρυπτογραφήθηκαν από WEP.

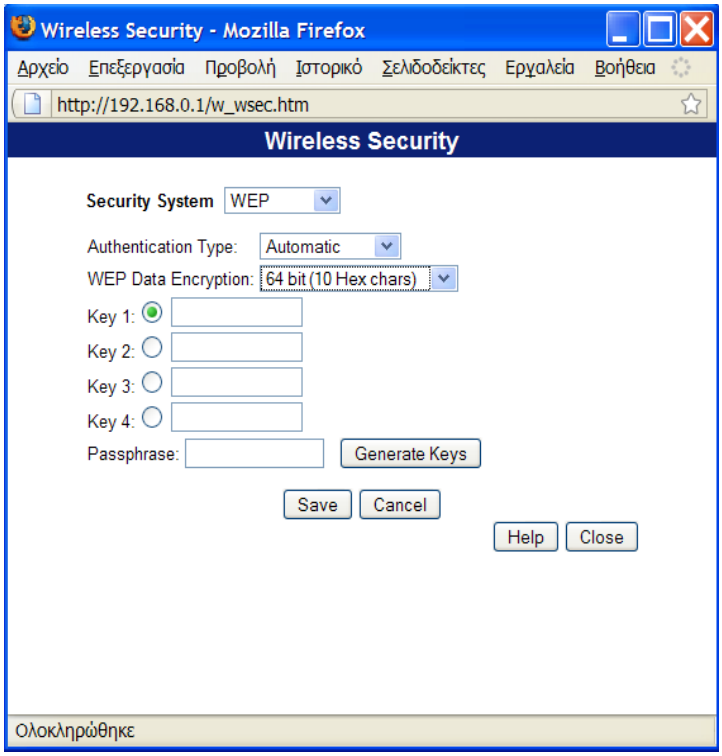
4.2.9 Εφαρμόζοντας τη μέθοδο WEP

Παρόλο που το WEP παρουσιάζει πολλές αδυναμίες, στην πραγματικότητα το σπάσιμο του WEP κλειδιού δεν είναι και τόσο εύκολη υπόθεση για ένα οικιακό δίκτυο για δύο κυρίως λόγους:

- Πρέπει να δημιουργηθεί ένα μεγάλο ποσοστό κίνησης ώστε να επιτύχουμε το σπάσιμο του WEP κλειδιού.

- Οι κατασκευαστές έχουν πάρει μέτρα για την μείωση του αριθμού των αδύναμων διανυσμάτων (Initialization Vectors) που μεταδίδονται.

Δεν παύει όμως να αποτελεί όχι και τόσο δυνατή μέθοδο κρυπτογράφησης αλλά είναι καθαρά στην επιλογή του κάθε χρήστη το να το επιλέγει σαν μέθοδο κρυπτογράφησης ή όχι. Για να ενεργοποιήσουμε το WEP ανοίγουμε την καρτέλα με τις ρυθμίσεις του ασύρματου router μας.



Εικόνα 27 Το παράθυρο των ρυθμίσεων του WEP κλειδιού

Ανοίγουμε το παράθυρο με τις ρυθμίσεις για το WEP κλειδί, όπως φαίνεται στην εικόνα 27, και στην επιλογή WEP Data Encryption αλλάζουμε από 64-bit σε 128-bit όπως φαίνεται στην εικόνα 28. Ο μεγαλύτερος αριθμός bits συνεπάγεται και μεγαλύτερη ασφάλεια για το σπάσιμο του κλειδιού από ότι τα 64-bits.

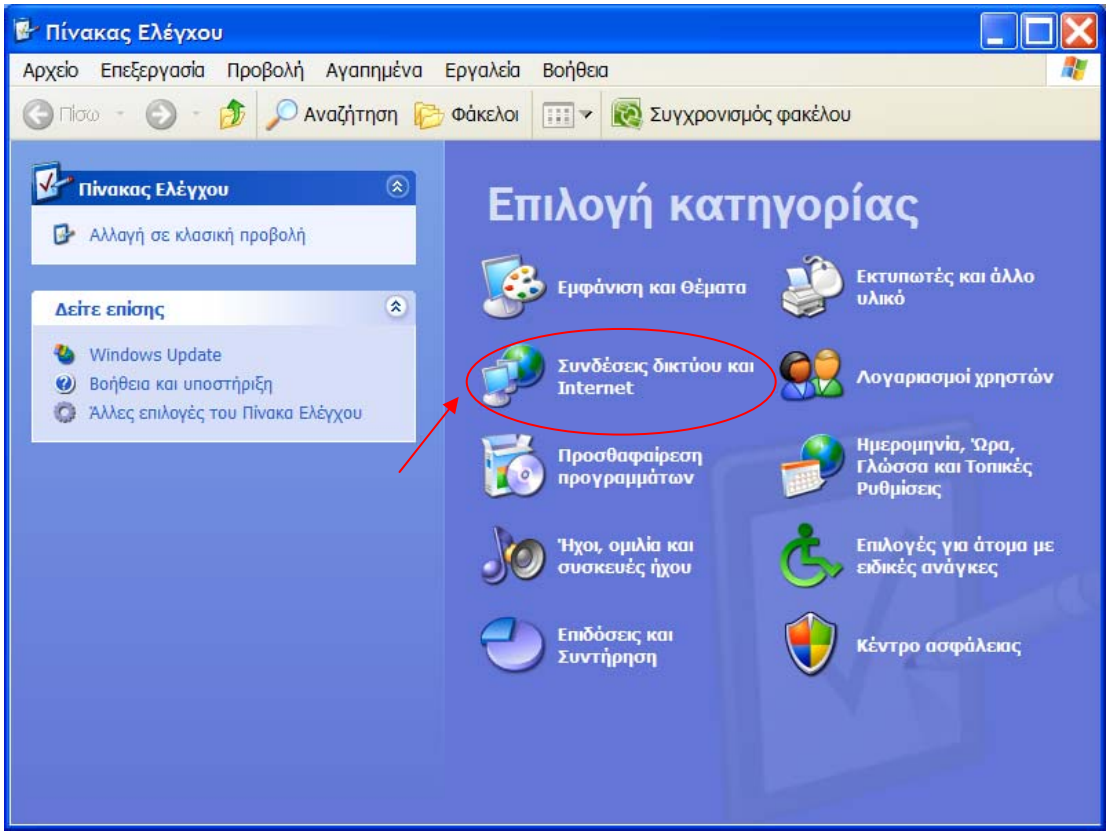
Εικόνα 28 Επιλογή 128-bit WEP κλειδιού

Στη συνέχεια διαλέγουμε μια δυνατή κωδική-λέξη για να δημιουργήσει τα κλειδιά μας. Μια δυνατή κωδική-λέξη αποτελείται από συνδυασμό κεφαλαίων και μικρών γραμμάτων, αριθμών και ειδικών χαρακτήρων. Όταν διαλέξουμε την κωδική-λέξη που θα χρησιμοποιήσουμε την εισάγουμε στο πεδίο **Passphrase** και επιλέγουμε το **Generate Keys**. Αυτό θα μας δημιουργήσει τέσσερα WEP κλειδιά όπως φαίνεται στην εικόνα 29.

Εικόνα 29 Δημιουργία WEP κλειδιών

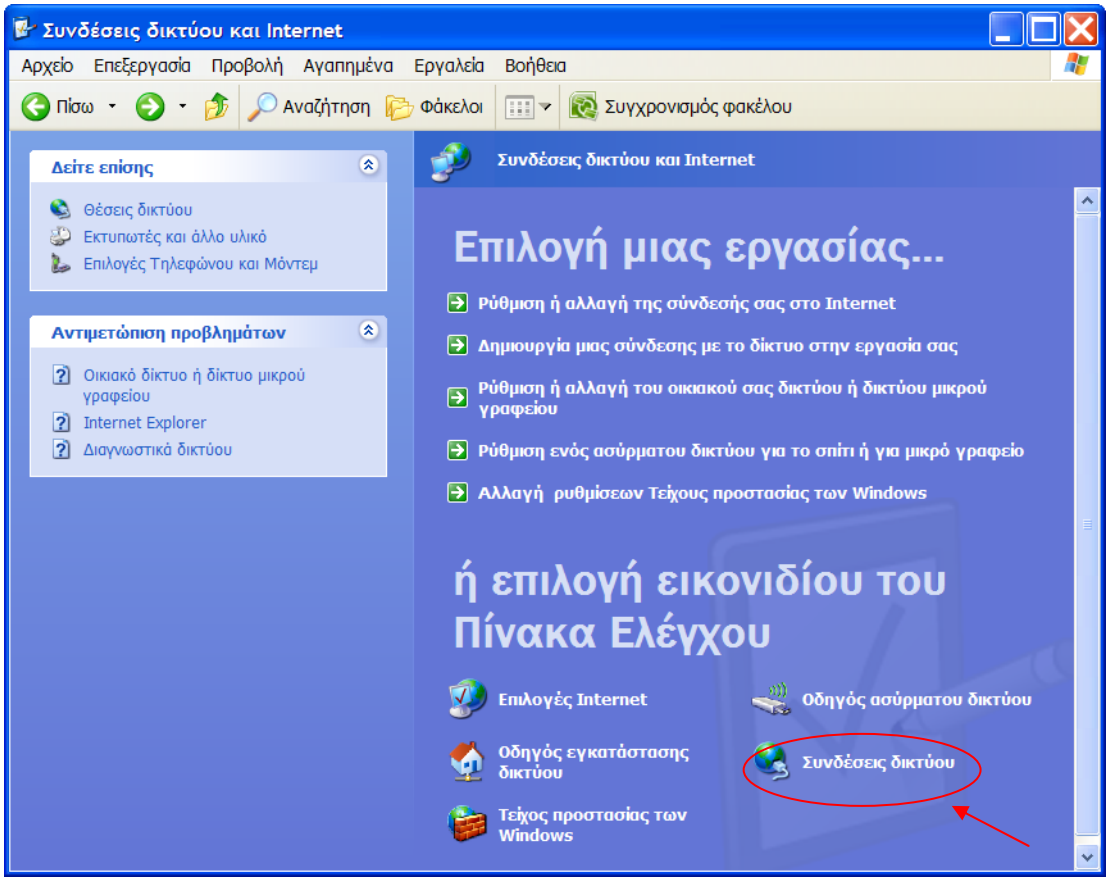
Όταν τα τέσσερα κλειδιά δημιουργηθούν θα πρέπει να επιλέξουμε ποιο από όλα θα χρησιμοποιεί ο πελάτης μας. Τέλος πατάμε save για να σώσουμε τις ρυθμίσεις που κάναμε.

Για να εφαρμόσουμε τις ρυθμίσεις του WEP κλειδιού στα Windows XP πηγαίνουμε **Έναρξη -> Πίνακας Ελέγχου -> Συνδέσεις δικτύου και Internet** και θα μας εμφανιστεί το παράθυρο της εικόνας 30.



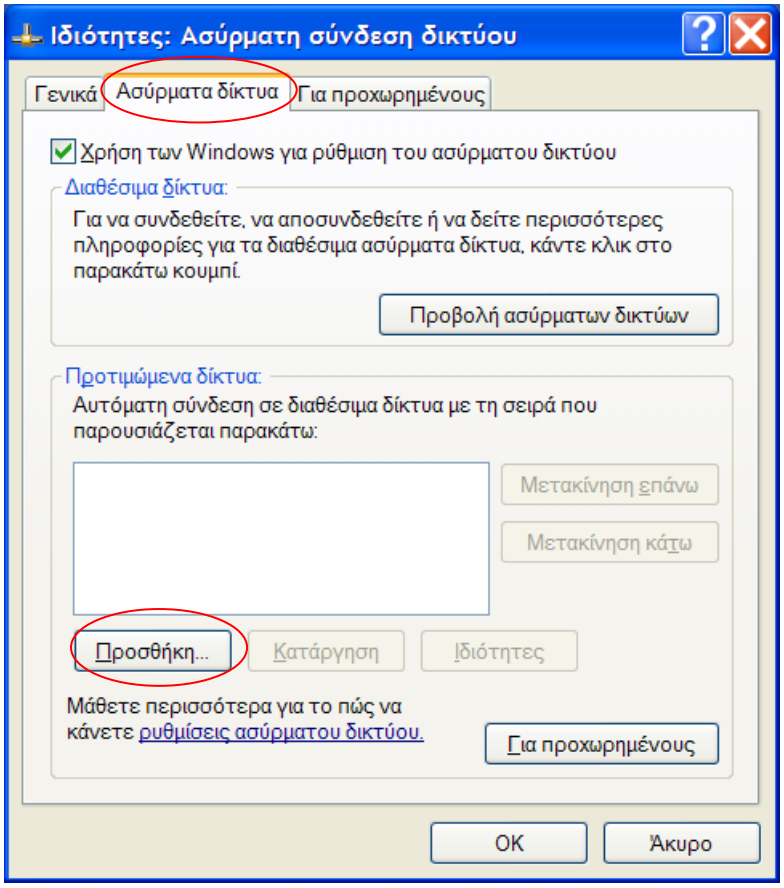
Εικόνα 30 Ρυθμίσεις WEP κλειδιού στα Windows XP

Κάτω από την επικεφαλίδα «*επιλογή εικονιδίου του πίνακα ελέγχου*», επιλέγουμε το εικονίδιο **συνδέσεις δικτύου** όπως φαίνεται στην εικόνα 31.



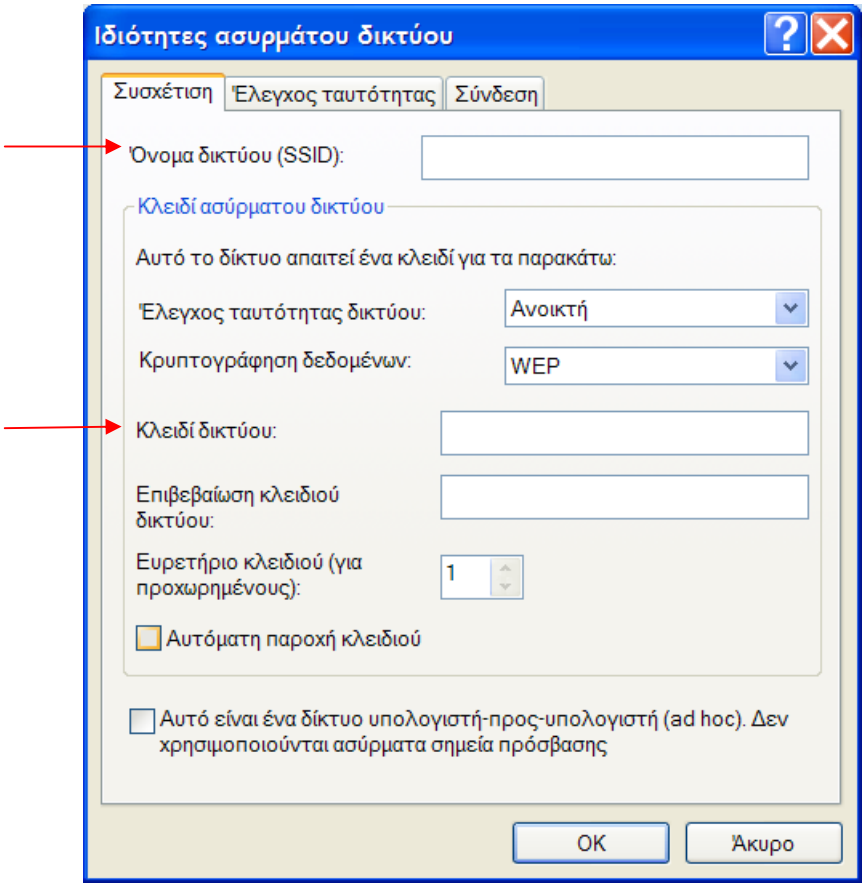
Εικόνα 31 Ρυθμίσεις WEP κλειδιού στα Windows XP

Πατάμε δεξί κλικ στο εικονίδιο της ασύρματης σύνδεσης που ανταποκρίνεται στην ασύρματη συσκευή μας και επιλέγουμε **Ιδιότητες**. Επιλέγουμε την καρτέλα **Ασύρματα δίκτυα** που βρίσκεται στην κορυφή του παραθύρου που εμφανίστηκε (εικόνα 32). Τσεκάρουμε το κουτάκι με την ετικέτα « *Χρήση των Windows για ρύθμιση του ασύρματου δικτύου*» και επιλέγουμε το κουμπί **Προσθήκη** προς το τέλος του παραθύρου.



Εικόνα 32 Ρυθμίσεις WEP κλειδιού στα Windows XP

Στο παράθυρο που εμφανίζεται (εικόνα 33), στο πεδίο **Όνομα δικτύου** πληκτρολογούμε το SSID κλειδί που δώσαμε στο ασύρματο δίκτυο μας. Ξετσεκάρουμε την επιλογή «*Αυτόματη παροχή κλειδιού*». Στο πεδίο **Κλειδί δικτύου** πληκτρολογούμε το WEP κλειδί δικτύου που έχουμε δώσει και στο σημείο πρόσβασης και στο πεδίο **Επιβεβαίωση κλειδιού δικτύου,** πληκτρολογούμε ξανά το WEP κλειδί του δικτύου μας. Τέλος πατάμε OK και είμαστε έτοιμοι να συνδεθούμε στο internet.



Εικόνα 33 Ρυθμίσεις WEP κλειδιού στα Windows XP

4.3 Αναβαθμίσεις της ασφάλειας του WEP.

Η εφαρμογή του WEP αλγόριθμου παρουσιάζει αδυναμίες και στην εμπιστευτικότητα και στην επικύρωση και με διάφορα εργαλεία που παρέχονται στο internet είναι πολύ εύκολο να σπάσει και να αποκαλυφθούν τα μηνύματα. Αυτό έχει ως αποτέλεσμα να αναπτύσσονται ισχυρότερα συστήματα ασφαλείας για το 802.11.

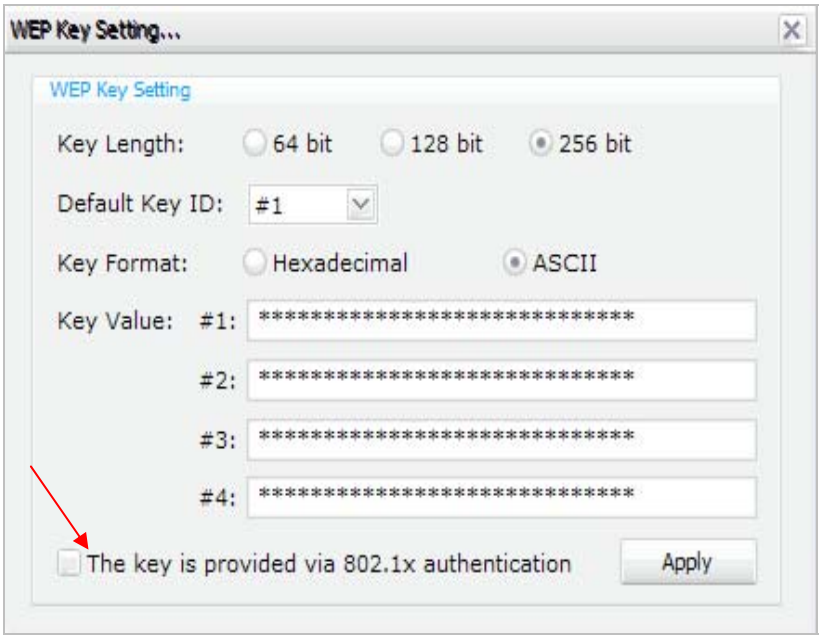
Εξαιτίας των αδυναμιών που παρουσιάζονταν στην ασφάλεια του WEP, η IEEE σχημάτισε μια ομάδα εργασίας την 802.11i, η οποία είχε σαν σκοπό να βελτιώσει την ασφάλεια στα 802.11 δίκτυα. Η ομάδα εργασίας είχε να σκεφτεί βελτιώσεις και περιορισμούς ώστε το WEP πρωτόκολλο να γίνει πιο δυνατό. Μια σκέψη ήταν να ξανασχεδιάσουν την ασφάλεια του 802.11 και να μην συμπεριλάβουν καμία από της λειτουργίες του WEP. Η άλλη σκέψη ήταν να αναβαθμίσουν την ασφάλεια του WEP, διατηρώντας την ίδια αρχιτεκτονική WEP. Και οι δύο σκέψεις επιλέχτηκαν και είχαν ως αποτέλεσμα το καινούργιο ολοκληρωμένο 802.11 πρότυπο και αναβάθμισαν την διαδικασία κρυπτογράφησης του WEP, με την μέθοδο ακεραιότητας που αναβαθμίστηκε και ονομάστηκε Temporal Key Integrity Protocol (TKIP)[36]. Το TKIP χρησιμοποιεί την 802.1X αρχιτεκτονική επικύρωσης, σαν βάση για την ασφαλή ανταλλαγή του κλειδιού, όπου αναλύεται στην επόμενη παράγραφο.

[36] http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

4.3.1 802.1X επικύρωση

Το 802.1X είναι ένας μηχανισμός επικύρωσης βασισμένος στις θύρες, που λειτουργεί κάτω από το Extensible Authentication Protocol (EAP)[37], την λειτουργία του οποίου εξετάζουμε παρακάτω. Ένα πράγμα στο οποίο μπερδεύονται οι άνθρωποι σχετικά με το 802.1X είναι ότι δεν είναι σε καμία περίπτωση είδος κρυπτογράφησης. Όλη η διαδικασία της κρυπτογράφησης λαμβάνει μέρος έξω από το πρότυπο 802.1X. Για παράδειγμα σε ένα ασύρματο δίκτυο το EAP χρησιμοποιεί μια από τις πολλές μεθόδους κρυπτογράφησης για την επικύρωση. Μετά που ο χρήστης επικυρώνεται στο ασύρματο δίκτυο, μπορεί να αρχίσει ο διάλογος χρησιμοποιώντας WEP, TKIP, AES[38] ή πολλά άλλα πρότυπα για ασύρματη κρυπτογράφηση.

Το 802.1X χρησιμοποιείται για την επικύρωση στις θύρες επικοινωνίας. Αυτό σημαίνει ότι το πρότυπο παίρνει την αίτηση επικύρωσης και αποφασίζει εάν πρέπει να της επιτραπεί ή όχι πρόσβαση στο δίκτυο. Στην εικόνα 34, στην ρύθμιση του WEP κλειδιού, βλέπουμε ότι παρέχεται επιλογή στον χρήστη αν θέλει να χρησιμοποιήσει την 802.1X επικύρωση.



Εικόνα 34 Ρύθμιση επιλογής για 802.1X επικύρωση

Το 802.1X είναι απλά ένας μηχανισμός που απορρίπτει όλη την κίνηση που έχει πρόσβαση σε ένα δίκτυο εκτός από τα EAP πακέτα. Εάν το EAP λέει ότι η συσκευή είναι εντάξει και να αποκτήσει πρόσβαση στο ασύρματο δίκτυο, το 802.1X πρωτόκολλο λέει στους διακόπτες ή στα σημεία πρόσβασης να επιτρέψουν την κίνηση που προέρχεται από το χρήστη. Στην εικόνα 35 φαίνονται οι τρείς οντότητες που χωρίζει το πρότυπο, το δίκτυο. Η κάθε μια από αυτές έχει συγκεκριμένες

[37] http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
[38] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

λειτουργίες. Όπως μπορεί κανείς να δει από την εικόνα το πρωτόκολλο χρησιμοποιεί δυο άλλα πρότυπα. Από τον πελάτη στον επικυρωτή το πρότυπο EAP και από τον επικυρωτή στον διακομιστή επικύρωσης το RADIUS. Τα πρωτόκολλα αυτά αναλύονται παρακάτω. Οι τρείς οντότητες που χωρίζει το δίκτυο είναι:

- Τους **Supplicants**, που θέλουν να ενωθούν στο δίκτυο. Είναι η συσκευή που θέλει να ενωθεί στο 802.1X δίκτυο. Αυτή μπορεί να είναι ένα computer, laptop, PDA ή οποιαδήποτε άλλη συσκευή με διεπαφή ασύρματης κάρτας. Όταν συνδέεται στο δίκτυο πάει κατευθείαν στον επικυρωτή. Ο επικυρωτής το μόνο που κάνει είναι να της επιτρέψει να περάσει το EAP αίτημα κυκλοφορίας που προορίζεται για τον διακομιστή επικύρωσης. Αυτό το EAP αίτημα κυκλοφορίας, είναι η πιστοποίηση επικύρωσης του χρήστη ή της συσκευής. Όταν ο εξυπηρετητής επικύρωσης επιτρέψει στο χρήστη ή την συσκευή να συνδεθεί στο δίκτυο, θα σταλεί ένα μήνυμα πιστοποίησης πρόσβασης.

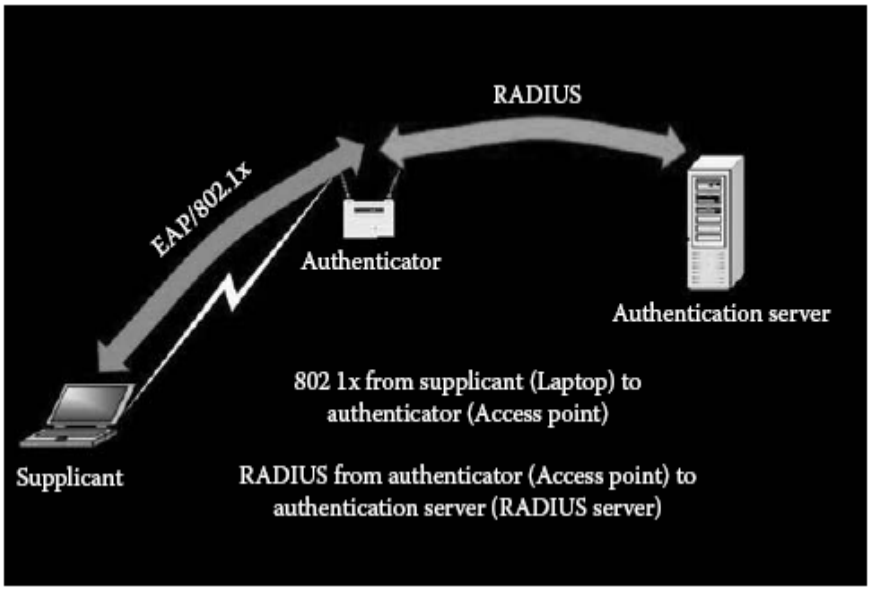
- Τον **Authenticator**, που ελέγχει την πρόσβαση . Είναι το πρώτο ηλεκτρονικό κομμάτι της συσκευής δικτύου του 802.1X που θα προσπαθήσει για σύνδεση. Για παράδειγμα μπορεί να είναι ένα ασύρματο σημείο πρόσβασης, ή οτιδήποτε άλλο που μπορεί να παρέχει πρόσβαση στο δίκτυο. Ο ρόλος της συσκευής είναι να αφήνει μόνο τα EAP πακέτα να περάσουν και μετά να περιμένει μία απάντηση από τον διακομιστή επικύρωσης. Μόνο όταν ο διακομιστής επικύρωσης απαντήσει με ένα μήνυμα αποδοχής ή απόρριψης, η επικύρωση λειτουργεί κατάλληλα.

- Τον **Κεντρικό Υπολογιστή Επικύρωσης** (Authentication Server), ο οποίος λαμβάνει τις αποφάσεις έγκρισης. Ο κεντρικός διακομιστής επικύρωσης, παρέχει ιδιότητες χορήγησης πρόσβασης και χορήγησης απόρριψης. Αυτό το επιτυγχάνει με το να λαμβάνει μία αίτηση πρόσβασης από τον επικυρωτή. Όταν ο διακομιστής επικύρωσης "ακούει" μια αίτηση, θα την επικυρώσει και θα επιστρέψει πίσω στον επικυρωτή ένα μήνυμα που θα χορηγεί ή θα απορρίπτει την πρόσβαση.

Το 802.1X έχει παρόλα αυτά προβλήματα. Μια πρόσφατη ερευνητική έκθεση προσδιόρισε αρκετά προβλήματα με την προδιαγραφή. Το πρώτο σημαντικό πρόβλημα είναι ότι το 802.1X δεν παρέχει ένα τρόπο να εγγυηθεί την αυθεντικότητα και την ακεραιότητα οποιονδήποτε πλαισίων στο ασύρματο δίκτυο. Τα πλαίσια στα ασύρματα δίκτυα μπορούν εύκολα να πειραχτούν ή να καταστραφούν εντελώς, και το πρωτόκολλο δεν παρέχει έναν τρόπο να σταματήσουν εύκολα ή ακόμα και να ανιχνευθούν τέτοιες επιθέσεις.

Το δεύτερο σημαντικό πρόβλημα είναι ότι το 802.1X είχε ως σκοπό να επιτρέψει στο δίκτυο να επικυρώσει το χρήστη. Υπονοείται στο σχέδιο του πρωτοκόλλου ότι οι χρήστες θα συνδεθούν μόνο με το "σωστό" δίκτυο. Στα συνδεδεμένα με καλώδιο δίκτυα, το να συνδεθείς με το σωστό δίκτυο είναι τόσο απλό όσο το να ακολουθήσεις το καλώδιο. Η πρόσβαση στην καλωδίωση βοηθά τους χρήστες να προσδιορίσουν το "σωστό" δίκτυο. Σε ένα ασύρματο δίκτυο, δεν υπάρχουν σαφείς φυσικές συνδέσεις, και έτσι άλλοι μηχανισμοί πρέπει να σχεδιαστούν για να αποδείξουν τα δίκτυα την ταυτότητά τους (ή, ακριβέστερα, την ταυτότητα του ιδιοκτήτη τους) στους χρήστες. Το σημείο στο οποίο ένας χρήστης συνδέεται με το δίκτυο καλείται θύρα (port). Ένα

δίκτυο μπορεί να έχει πολλές θύρες παραδείγματος χάριν, σε ένα switched LAN hub κάθε σύνδεσμος (connector) Ethernet θα ήταν μια θύρα. Υπάρχει μια ένα προς ένα σχέση μεταξύ supplicant και θύρας, και κάθε θύρα έχει ένα σχετικό authenticator για να ελέγξει την κατάστασή της. Υπάρχει μια πολλοί προς ένας σχέση μεταξύ των θυρών και του κεντρικού υπολογιστή επικύρωσης. Με άλλα λόγια, ένας ενιαίος κεντρικός υπολογιστής επικύρωσης είναι συνήθως αρμόδιος για πολλές θύρες, κάθε μια όμως έχει το δικό της authenticator. Η χρησιμοποίηση του 802.1X στα ασύρματα δίκτυα φαίνεται στο παρακάτω σχήμα:

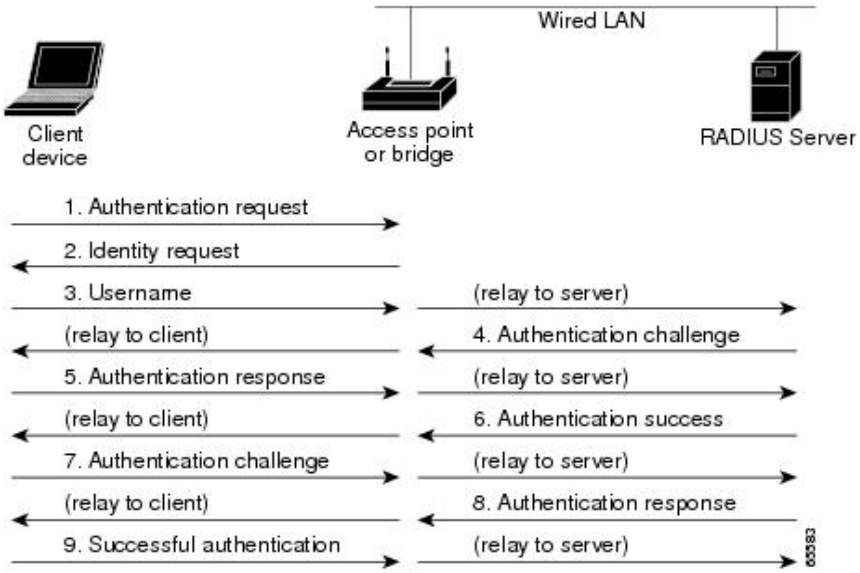


Εικόνα 35 Λειτουργία του 802.1X προτύπου

4.3.2 Extensible Authentication Protocol (EAP)

Το Extensible Authentication Protocol (EAP) είναι μια μέθοδος επικύρωσης για να αποκτήσουμε πρόσβαση σε ένα δίκτυο. Αυτό το είδος επικύρωσης παρέχει το υψηλότερο επίπεδο ασφάλειας για το ασύρματο δίκτυο μας. Χρησιμοποιώντας το Extensible Authentication Protocol (EAP), το σημείο πρόσβασης βοηθάει μια ασύρματη συσκευή πελάτη και ένα διακομιστή RADIUS να εκτελούν αμοιβαία επικύρωση και να αντλούν ένα δυνατό, μοναδικού περιεχομένου WEP κλειδί.

Ο διακομιστής RADIUS στέλνει το WEP κλειδί στο σημείο πρόσβασης, το οποίο το χρησιμοποιεί για όλα τα δεδομένα που στέλνει και λαμβάνει από τον πελάτη. Επίσης το σημείο πρόσβασης κρυπτογραφεί το μεταδιδόμενο WEP κλειδί του μαζί με το μοναδικό κλειδί του πελάτη και το στέλνει στον πελάτη. Όταν ενεργοποιούμε την μέθοδο EAP στο σημείο πρόσβασης και στη συσκευή του πελάτη, η ακολουθία της επικύρωσης που συμβαίνει στο δίκτυο φαίνεται στην εικόνα 36.



Εικόνα 36 Μέθοδος επικύρωσης EAP

Στα βήματα 1 έως 9 στην εικόνα 36, μια ασύρματη συσκευή πελάτη και ένας διακομιστής RADIUS σε ένα ενσύρματο LAN, χρησιμοποιούν 802.1X και EAP για να εκτελέσουν μια αμοιβαία επικύρωση μέσω του σημείου πρόσβασης. Ο διακομιστής RADIUS στέλνει μια πρόκληση επικύρωσης στον πελάτη. Ο πελάτης χρησιμοποιεί κρυπτογράφηση, μέσω του κωδικού πρόσβασης που του έχει δώσει ο χρήστης, για να δημιουργήσει μια απάντηση στην πρόκληση και στέλνει την απάντηση που δημιούργησε στον RADIUS διακομιστή. Χρησιμοποιώντας πληροφορίες από τη βάση δεδομένων του χρήστη του, ο διακομιστής RADIUS δημιουργεί την δική του απάντηση και την συγκρίνει με την απάντηση του χρήστη. Όταν ο διακομιστής RADIUS επικυρώσει τον πελάτη, η διαδικασία επαναλαμβάνεται αντίστροφα και ο πελάτης πιστοποιεί τον διακομιστή RADIUS.

Όταν ολοκληρωθεί ο αμοιβαίος έλεγχος επικύρωσης, ο διακομιστής RADIUS και ο πελάτης καθορίζουν ένα WEP κλειδί, το οποίο είναι μοναδικό για τον πελάτη και του παρέχει εκτός από το κατάλληλο επίπεδο πρόσβασης στο δίκτυο και ένα σημαντικό επίπεδο ασφάλειας. Ένα από τα βασικά πλεονεκτήματα χρησιμοποίησης του EAP είναι ότι έχει την ικανότητα να παρέχει πολλαπλούς τύπους των μηχανισμών επικύρωσης. Η ικανότητα χρησιμοποίησης πολλαπλών τύπων επικύρωσης τοποθετείται στο πεδίο τύπου του EAP πακέτου. Το αρχικό πρότυπο απαριθμούσε τρείς βασικούς τύπους EAP: MD5 Challenge, One Time Password (OTP), και το Generic Token Card (GTC). Στις μέρες μας πλέον μπορούμε να βρούμε ένα μεγάλο αριθμό από διαφορετικούς τύπους EAP όπως το EAP-MD5, EAP-TLS, LEAP, PEAP και διάφορους άλλους.

4.3.3 Υπηρεσία Απομακρυσμένης Πρόσβασης Dial-In Χρηστών (Remote Access Dial-In User Service- RADIUS)

Το RADIUS είναι ένα ακρωνύμιο για την υπηρεσία απομακρυσμένης σύνδεσης dial-up χρηστών. Είναι ένα πρωτόκολλο που βασίζεται στην επικύρωση, την έγκριση, και

τη λογιστική. Μπορεί να τρέξει σε πολλές συσκευές όπως στους δρομολογητές, στους εξυπηρετητές, στα μόντεμ, στους VPN συμπυκνωτές, καθώς και σε οποιαδήποτε άλλη συσκευή, η οποία να είναι συμβατή με το πρότυπο RADIUS.

Η λειτουργία του πρωτοκόλλου βασίζεται στη δημιουργία ενός κρυπτογραφημένου τούνελ, ανάμεσα στη συσκευή δικτύου και στον RADIUS διακομιστή. Αυτό το τούνελ χρησιμοποιείται για να στέλνει όλη την επικυρωμένη και έγκριτη πληροφορία, ανάλογα με το ποιος είναι ο χρήστης, που βρίσκεται, που του επιτρέπεται να πάει και πού στην πραγματικότητα θα πάει. Για να αρχίσει να λειτουργεί αυτό το κρυπτογραφημένο τούνελ θα πρέπει να δημιουργηθεί μία φράση ή ένας κωδικός, που θα είναι κοινό μυστικό. Το κοινό μυστικό θα είναι ανάμεσα στη συσκευή που συμμετέχει στο RADIUS δίκτυο και στον RADIUS εξυπηρετητή. Άμα το κοινό μυστικό εγκατασταθεί σωστά τότε μόνο μπορεί να λάβει μέρος μια ασφαλής συνομιλία.

Ένα από τα πλεονεκτήματα του RADIUS είναι η συνηθισμένη βάση των χρηστών που παρέχουν αξιοπιστία και επικύρωση. Η βάση που οι χρήστες RADIUS χρησιμοποιούν για να αποθηκεύουν usernames και passwords, μπορεί να εγκατασταθεί σε διαφορετικούς τύπους λεξικών. Αυτό σημαίνει ότι το RADIUS μπορεί να χρησιμοποιήσει λεξικά δομών όπως το Microsoft Active Directory (MS-AD), Novel Network Directory System (NDS), Lightweight Directory Access Protocol (LDAP), και πολλούς άλλους συνηθισμένους τύπους λεξικών.

Αυτό το πρωτόκολλο επιτρέπει στους διαχειριστές να τοποθετούν κεντρικά και να διαχειρίζονται την πρόσβαση του κάθε χρήστη, και να λογαριάζουν για όλον τον εξοπλισμό του δικτύου, τόσο καλά όσο για την μετακινούμενη πρόσβαση. Το RADIUS μπορεί να χρησιμοποιηθεί σαν μέθοδος πρόσβασης για την διαχείριση στο σημείο πρόσβασης, όπου αυτό είναι παρόμοιο με το να διαχειρίζεται δρομολογητές.

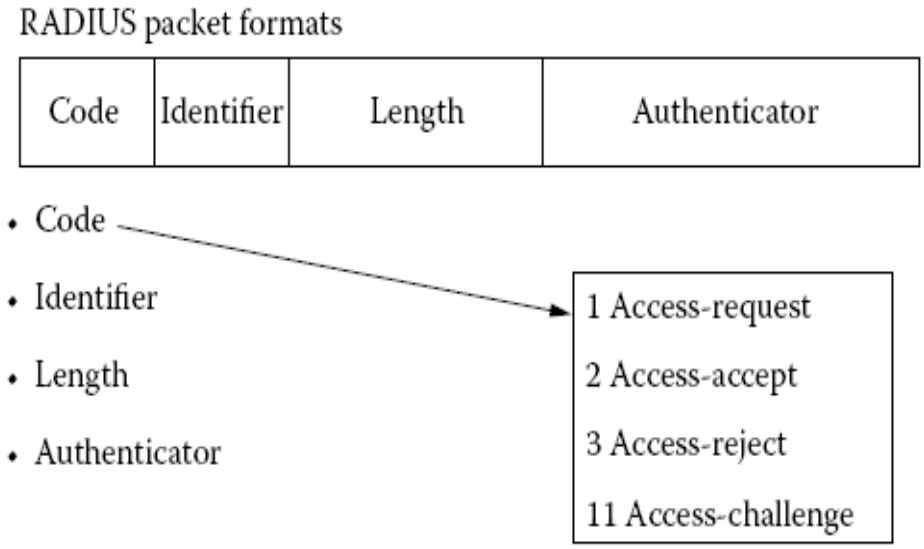
Μία άλλη λύση είναι να χρησιμοποιούμε το RADIUS σαν μία επεξήγηση στο πρότυπο 802.1X, σαν ένα επιπρόσθετο μηχανισμό επικύρωσης. Σε αυτήν την περίπτωση χρειάζεται το σημείο πρόσβασης να εγκατασταθεί σωστά με τον εξυπηρετητή RADIUS, και το σημείο πρόσβασης θα κρατήσει την διαδρομή της απάντησης του χρήστη για να εισέλθει στο δίκτυο. Αυτό σημαίνει ότι ο χρήστης θα διαπραγματευτεί για την επικύρωση μόνο με το σημείο πρόσβασης και όχι με τον εξυπηρετητή RADIUS. Το πρωτόκολλο RADIUS έχει μόνο τέσσερα είδη πακέτων επικύρωσης όπως βλέπουμε και στην εικόνα 37 και αυτά είναι:

1. **Αίτημα πρόσβασης (Access Request):** Αυτό το πακέτο επιτρέπει στην ακολουθία RADIUS, να λάβει χώρο.

2. ***Αίτημα αποδοχής (Access Accept):*** Αυτό το πακέτο πληροφορεί τον πελάτη RADIUS, ότι η επικύρωση που του παραχώθηκε ήταν σωστή.

3. **Αίτημα απόρριψης (Access Reject):** Αυτό το πακέτο πληροφορεί τον πελάτη RADIUS, ότι η επικύρωση που του παραχώθηκε δεν ήταν σωστή.

4. ***Αίτημα πρόκληση (Access-Challenge):*** Αυτό το πακέτο χρησιμοποιείται για να προκαλέσει ένα πελάτη RADIUS για τα επικυρωμένα πιστοποιητικά του.



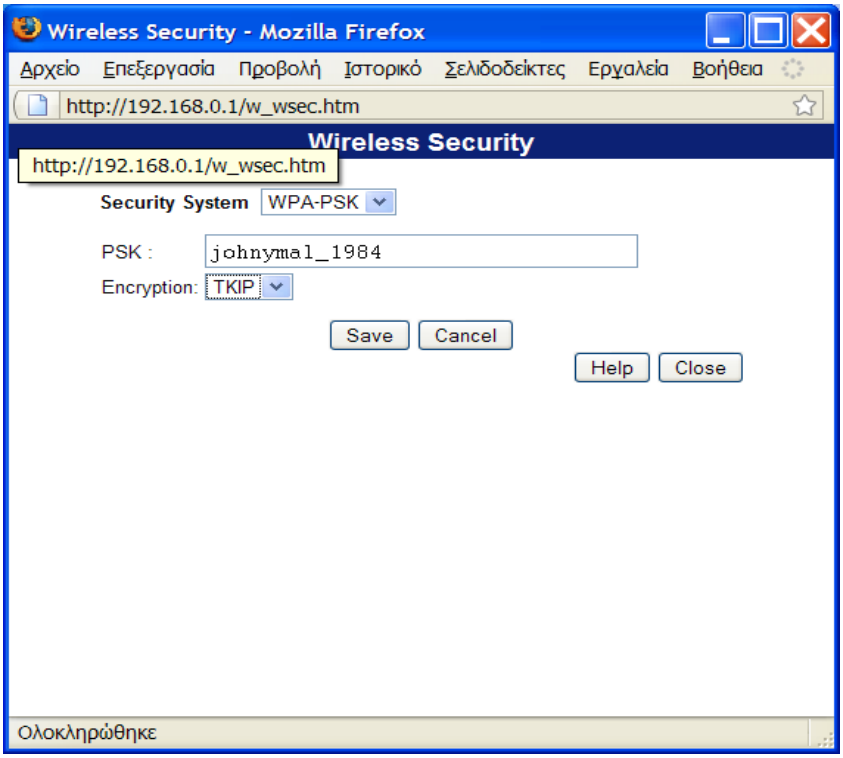
Εικόνα 37 Μορφή του radius πακέτου

4.4 WPA (Wi-Fi Protected Access)

Όταν τα θέματα ασφαλείας των WLAN έγιναν περισσότερο σημαντικά, τα κενά του WEP άρχισαν να εκτίθονταν και οι μηχανισμοί επικύρωσης του 802.11 άρχισαν να ξεπερνιούνται η Wi-Fi Alliance ανέπτυξε το Wi-Fi Protected Access (WPA) το 2003. Το WPA προέρχεται από το IEEE 802.11 πρότυπο και είναι σαν μια ενδιάμεση λύση ασφάλειας των WLAN και μπορεί να συμπεριληφθεί με αναβαθμίσεις στις ήδη υπάρχουσες WLAN ασύρματες συσκευές. Το WPA είναι μια προδιαγραφή, βασισμένη στο πρότυπο, διαλειτουργική βελτίωση ασφάλειας και αυξάνει σημαντικά το επίπεδο ασφάλειας και ελέγχου πρόσβασης στα ασύρματα συστήματα LAN.

Το WPA χρησιμοποιεί Temporal Key Integrity Protocol (TKIP) για να βελτιώσει την κρυπτογράφηση των δεδομένων, το οποίο παρέχει σε κάθε πακέτο ανακάτεμα του κλειδιού, έναν έλεγχο ακεραιότητας μηνύματος (MIC) που ονομάζεται Michael και ένα διάνυσμα ακολουθίας (Initialization Vector-IV). Για τους οικιακούς χρήστες που δεν είναι τυχεροί να χρησιμοποιούν ένα RADIUS εξυπηρετητή για να επικυρώνουν τους σταθμούς τους, το WPA παρέχει ένα μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre-Shared Key)

Για να χρησιμοποιήσει ο χρήστης το PSK θα πρέπει να εισάγει μια λέξη κωδικό και στο σημείο πρόσβασης και στο σταθμό (εικόνα 38). Αυτή η λέξη κωδικός χρησιμοποιείται για να επικυρώνει οποιονδήποτε σταθμό προσπαθεί να συνδεθεί στο συγκεκριμένο δίκτυο. Αποτελείται από 8 έως 63 εκτυπώσιμους χαρακτήρες σε ASCII. Στη συνέχεια το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Εάν χρησιμοποιούνται χαρακτήρες ASCII, το 256 bit κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 , χρησιμοποιώντας το passphrase ως κλειδί.



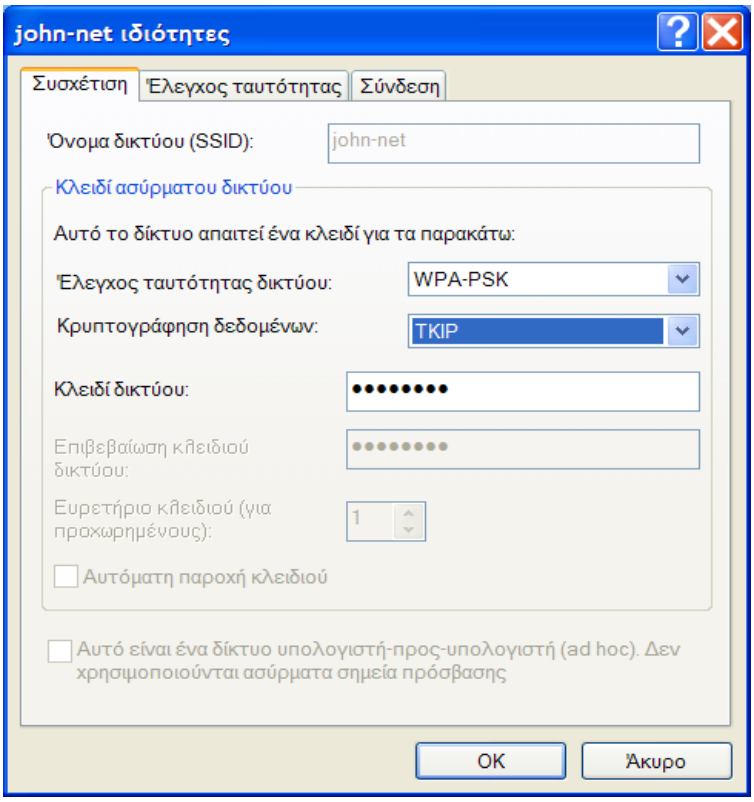
Εικόνα 38 Ρύθμιση του σημείου πρόσβασης για υποστήριξη WPA

Το pre-shared WPA είναι τρωτό στις επιθέσεις ραγίσματος κωδικού πρόσβασης εάν χρησιμοποιείται ένα αδύνατο passphrase. Για να προστατεύσει από μια επίθεση brute-force, ένα αληθινά τυχαίο passphrase 13 χαρακτήρων είναι πιθανώς επαρκές. Τα προϊόντα που γράφουν ότι έχουν "WPA-Personal" σημαίνει ότι υποστηρίζουν τον PSK μηχανισμό επικύρωσης.

Στην ουσία το WPA είναι ένα υποσύνολο του προτύπου 802.11i, το οποίο περιλαμβάνει την διαχείριση κλειδιού και την αρχιτεκτονική της επικύρωσης (802.11X) που διευκρινίζονται στο 802.11i. Η μεγαλύτερη διαφορά ανάμεσα στο WPA και στο 802.11i (το οποίο είναι και γνωστό ως WPA2) είναι ότι το WPA, εκτός από τη χρήση του AES που κάνει για την εμπιστευτικότητα και την ακεραιότητα, χρησιμοποιεί αντίστοιχα και TKIP και MICHAEL.

Ο αλγόριθμος που χρησιμοποιείται από τον MICHAEL, υπολογίζει ένα κωδικό ακεραιότητας μηνύματος 8 byte (MIC). Ο MIC τοποθετείται ανάμεσα στα δεδομένα και στην 4-bit αξία ελέγχου ακεραιότητας (ICV). Ο MICHAEL επίσης βοηθάει στο να αποτρέπει να συμβαίνουν επαναλαμβανόμενες επιθέσεις, με το να παρέχει ένα μετρητή πλαισίων, μέσα στο πλαίσιο 802.11.

Τα βήματα που ακολουθούνται για να ρυθμίσουμε την ασφάλεια WPA στα Windows XP είναι ακριβώς τα ίδια που περιγράψαμε παραπάνω για το WEP, με τη μόνη διαφορά ότι στην καρτέλα με τις ιδιότητες του ασύρματου δικτύου μας επιλέγουμε στην ετικέτα **Έλεγχος ταυτότητας δικτύου** το WPA-PSK. Στην ετικέτα **Κρυπτογράφηση δεδομένων** επιλέγουμε ή την μέθοδο TKIP ή AES και στη συνέχεια πληκτρολογούμε το WPA κλειδί δικτύου που έχουμε επιλέξει (εικόνα 39).



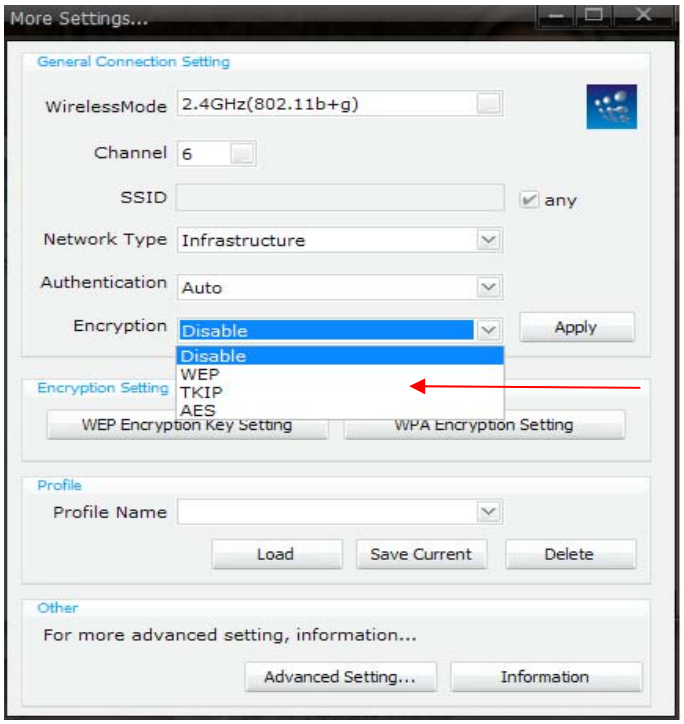
Εικόνα 39 Παράδειγμα ρύθμισης WPA στα Windows XP

4.4.1 TKIP (Temporal Key Integrity Protocol)

Το TKIP περιλαμβάνεται στα 802.11i πρότυπα για συμβατότητα προς τα πίσω. Το TKIP στην αρχή χρησιμοποιούταν πάνω από το WEP για περισσότερη ασφάλεια και για να μειώσει τον αριθμό των επιθέσεων του WEP. Η TKIP κρυπτογράφηση λειτουργεί σε δύο στάδια. Στο πρώτο στάδιο δημιουργεί ένα κλειδί συνόδου από ένα χρονικό κλειδί, τον TKIP μετρητή ακολουθίας (TSC), και την διεύθυνση MAC του πομπού. Το χρονικό κλειδί είναι φτιαγμένο από μια τιμή 128 bit, παρόμοια με την τιμή του WEP κλειδιού. Ο TKIP μετρητής ακολουθίας (TSC) είναι φτιαγμένος από την πηγαία διεύθυνση (SA), την διεύθυνση προορισμού (DA), την ιεραρχία και τα δεδομένα. Όταν ολοκληρωθεί αυτή η φάση μια τιμή που ονομάζεται TKIP μικτή διεύθυνση μεταφοράς και το κλειδί TTAK δημιουργείται. Αυτή η τιμή χρησιμοποιείται σαν κλειδί συνόδου στη δεύτερη φάση.

Στην δεύτερη φάση το TTAK και το διάνυσμα ακολουθίας IV χρησιμοποιούνται για να παράγουν ένα κλειδί που θα κρυπτογραφεί τα δεδομένα. Αυτό είναι παρόμοιο με τον τρόπο λειτουργίας του WEP. Στο WEP τα πρώτα 24 bits του IV προστίθενται μπροστά από το WEP κλειδί και μετά αυτό χρησιμοποιείται για να δημιουργηθεί ένα κλειδί κρυπτογράφησης που εφαρμόζεται στα δεδομένα. Στη συνέχεια το IV ενσωματώνεται στην επικεφαλίδα του πακέτου. Το TKIP παραθέτει χώρο στο IV, επιτρέποντας του ένα κενό πεδίο μέσα του για να συμπεριλάβει 24 bits επιπλέον. Στη

δεύτερη φάση τα πρώτα 24 bits ενώνονται με τα πρώτα 24 bits του TTAK. Τα επόμενα 24 bits γεμίζουν με το αχρησιμοποίητο μέρος του TSC.



Εικόνα 40 Επιλογή του είδους κρυπτογράφησης

4.4.2 AES-CCMP (Advanced Encryption Standard)

Το WPA ακόμα βασίζεται στον αλγόριθμο RC4, αλλά το κύριο συστατικό για ένα ασφαλές περιβάλλον δικτύου είναι η χρησιμοποίηση του Advanced Encryption Standard (AES) για την εμπιστευτικότητα των δεδομένων και την ακεραιότητα. Ο AES είναι η νεότερη μέθοδος κρυπτογράφησης που έχει επιλεγεί από την κυβέρνηση των Η.Π.Α για να αντικαταστήσει το προηγούμενο πρότυπο τους ο DES. Ο AES χρησιμοποιεί ένα αλγόριθμο γνωστό ως Rijndael[39]. Το όνομά του το πήρε από τα ονόματα των δύο βέλγων εφευρετών του Joan Daemen και Vincent Rijmen.

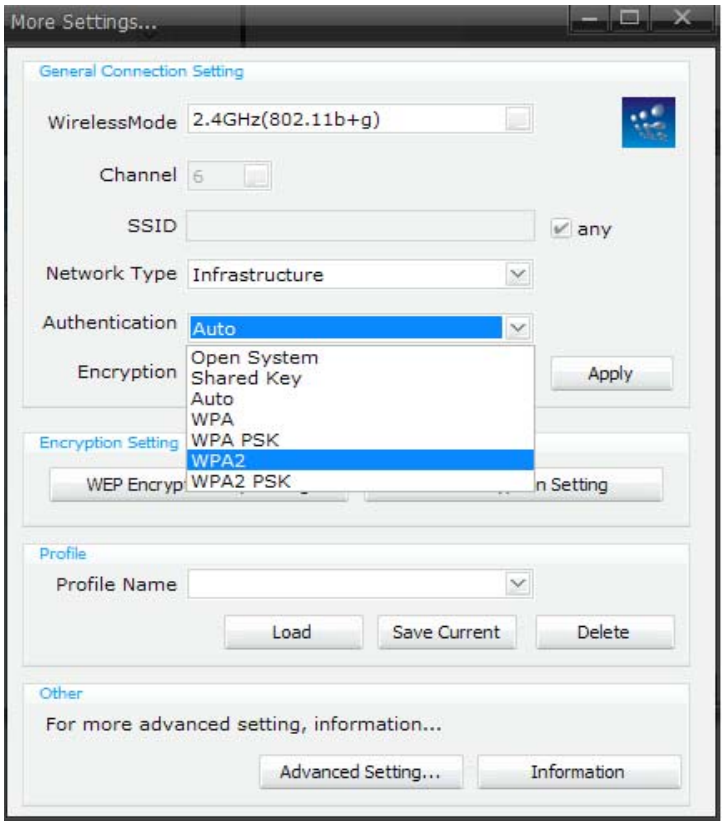
Είναι ένα μπλοκ κρυπτογράφησης, πράγμα που σημαίνει ότι λειτουργεί σε μια ομάδα σταθερού μεγέθους bits, η οποία ονομάζεται μπλοκ. Παίρνει σαν είσοδο ένα μπλοκ συγκεκριμένου μεγέθους, συνήθως 128, και παράγει ένα αντίστοιχο μπλοκ εξόδου του ίδιου μεγέθους. Ο μετασχηματισμός απαιτεί μια δεύτερη είσοδο, η οποία είναι το μυστικό κλειδί. Είναι σημαντικό να γνωρίζουμε ότι το μυστικό κλειδί μπορεί να είναι οποιουδήποτε μεγέθους (ανάλογα με τη χρησιμοποιούμενη κρυπτογράφηση) και ότι ο AES χρησιμοποιεί τρία βασικά μεγέθη: 128, 192 και 256 bytes.

[39] http://en.wikipedia.org/wiki/Rijndael_key_schedule

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

4.5 WPA2 (Wi-Fi Protected Access Version 2)

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



Εικόνα 41 Επιλογή WPA2 ως μέθοδος κρυπτογράφησης

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

Όταν ένας σταθμός θέλει να συνδεθεί σε ένα γειτονικό σημείο πρόσβασης, η επικύρωση 802.1X μπορεί να παραλειφτεί αφού έχει ήδη ολοκληρωθεί εκ των πρότερων. Επιπλέον το προσωρινό κλειδί έχει ήδη εγκαθιδρυθεί ανάμεσα στο σταθμό και το σημείο πρόσβασης. Αποκτώντας πρόσβαση στον RADIUS εξυπηρετητή για να ολοκληρώσει την 802.11X επικύρωση καταλαμβάνει πολύ χρόνο και επιπλέον τα δίκτυα που περιλαμβάνουν γρήγορη περιαγωγή έχει παρατηρηθεί ότι έχουν ομαλότερη λειτουργία και συνεχή συνδεσιμότητα του πελάτη καθώς αυτός μετακινείται στις κυψέλες του WLAN.

Υπάρχουν δύο εκδόσεις του WPA2. Το WPA2-Personal και το WPA2- Enterprise. Το WPA2-Personal προστατεύει την πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες με τη χρήση της εγκατάστασης ενός κωδικού πρόσβασης. Το WPA2-Enterprise πιστοποιεί τους χρήστες του δικτύου μέσω ενός εξυπηρετητή. Το WPA2 διατηρεί συμβατότητα προς τα πίσω με το WPA.

Πρωτόκολλο ασφαλείας	**WEP**	**WPA**	**WPA2**
Εμπιστευτικότητα/ακεραιότητα	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Μήκος κλειδιού	40 ή 104bits	128 bits κρυπτογράφησης και 64 bits της επικύρωσης	128 bits
Διάρκεια ζωής κλειδιού	24bit IV	48 bit IV (Initialization Vector)	
Δημιουργία κλειδιού	Αλληλουχία	Λειτουργία ένωσης δύο φάσεων	Δεν χρειάζεται
Ακεραιότητα δεδομένων	CRC-32	Michael	CBC-MAC
Ακεραιότητα επικεφαλίδας	Καμία	Michael	CBC-MAC
Προστασία επανάληψης	Καμία	Αριθμός του πακέτου	
Διαχείριση κλειδιού	Καμία	Βασισμένο στο EAP	
Επικύρωση	Ανοιχτό ή κοινό κλειδί	IEEE 802.1x ή Pre-Shared Key (PSK)	

Πίνακας 2 Σύνοψη των μεθόδων ασφάλειας των ασύρματων δικτύων

Κεφάλαιο 5 Σπάζοντας την ασύρματη ασφάλεια

Τα ασύρματα δίκτυα είναι ευάλωτα σε επιτιθέμενους. Καθώς αναπτύσσονται και επεκτείνονται διάφοροι μηχανισμοί ασφαλείας για τα ασύρματα δίκτυα, τόσο περισσότεροι τρόποι δημιουργούνται ώστε να μπορούν να επιτεθούν σε αυτά κάποιοι. Η έννοια της επίθεσης ορίζεται ως έξης:

Ορισμός: Επίθεση. Είναι οποιαδήποτε προσπάθεια για παραβίαση της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας ενός συστήματος ή ενός δικτύου. Επίσης είναι οποιαδήποτε μη εξουσιοδοτημένη ενέργεια που έχει σκοπό να εμποδίσει, να παρακάμψει ή να αχρηστεύσει τους μηχανισμούς ασφαλείας και ελέγχου πρόσβασης ενός συστήματος ή ενός δικτύου.

Σε ένα δίκτυο συμβαίνει επίθεση όταν ένας εισβολέας χρησιμοποιεί ορισμένες τεχνικές ή τεχνολογίες κακόβουλα και προσπαθεί να παραβιάσει την ασφάλεια του δικτύου. Οι επιθέσεις πραγματοποιούνται από άτομα που έχουν πρόσβαση στους στόχους τους μέσω του internet, από εξουσιοδοτημένους χρήστες που προσπαθούν να αποκτήσουν περισσότερα δικαιώματα από αυτά που τους έχουν δοθεί και από εξουσιοδοτημένους χρήστες οι οποίοι εκμεταλλεύονται τα δικαιώματα που τους έχουν δοθεί με κακό σκοπό. Συνήθως αυτοί που πραγματοποιούν τις επιθέσεις είναι γνωστοί ως hackers[40] ή crackers.

Οι εισβολείς σε εταιρικά δίκτυα χρησιμοποιούν τα στοιχεία για το οικονομικό κέρδος ή για βιομηχανική κατασκοπία, με το να χρησιμοποιούν παράνομα τους λογαριασμούς χρηστών και προνομίων, για να εκτελέσουν κώδικα και ζημιές σε διεφθαρμένα στοιχεία, να κλέψουν τα δεδομένα και το λογισμικό.

Η ασύρματη ασφάλεια ενός δικτύου έχει συζητηθεί αναλυτικά στο προηγούμενο κεφάλαιο, αλλά προτού εξετάσουμε τους τρόπους για να υπερασπιστούμε το ασύρματο δίκτυό μας πρέπει να κατανοήσουμε από τι κινδυνεύουμε και από τι χρειάζεται να το υπερασπίσουμε. Οι περισσότερες από τις ευπάθειες που συμβαίνουν στα ασύρματα δίκτυα όπως καλά όλοι ξέρουμε σχετίζονται κυρίως με την ασφάλεια του WEP.

Ωστόσο υπάρχουν εργαλεία να αυτοματοποιούν αυτές τις επιθέσεις και να είναι επιτυχημένες σε κάθε δοκιμασία. Είναι σημαντικό να κατανοήσουμε τα εργαλεία που χρησιμοποιούνται για αυτές τις επιθέσεις και το πώς οι επιθέσεις στην πραγματικότητα δουλεύουν και οι διαχειριστές των ασύρματων δικτύων να καταλάβουν τι πρέπει να αντικρούσουν. Παρακάτω αναφερόμαστε στις πιο γνωστές επιθέσεις που μπορούν να πραγματοποιηθούν κατά του 802.11.

[40] http://en.wikipedia.org/wiki/Hacker

5.1 WEP Cracking

Το μεγαλύτερο πρόβλημα με τις επιθέσεις κατά του WEP είναι ότι με την συλλογή μεγάλου ποσοστού IVs πακέτων, μπορούμε να σπαταλήσουμε ένα σημαντικό ποσοστό χρόνου. Δυστυχώς όσο και αν προσπαθήσουμε να επιταχύνουμε την διαδικασία συλλογής αδύναμων ή μοναδικών IVs, σχεδόν πάντα θα ανιχνεύεται κίνηση μέσα στο δίκτυο και θα δημιουργεί επιπλέον πακέτα. Αυτό συχνά ολοκληρώνεται με το να μαζεύουμε ένα ή περισσότερα Address Resolution Protocol (ARP)[41] πακέτα και αναμεταδίδοντας τα στο σημείο πρόσβασης. Τα πακέτα ARP είναι μία καλή επιλογή, γιατί αυτά έχουν ένα προκαθορισμένο μέγεθος (28 byte). Η απάντηση θα δημιουργήσει κίνηση και θα αυξήσει την ταχύτητα συλλογής των πακέτων.

Συλλέγοντας το αρχικό πακέτο ARP μπορεί να παρουσιαστεί πρόβλημα. Εμείς πρέπει να περιμένουμε ένα νομιμοποιημένο ARP πακέτο να δημιουργηθεί στο δίκτυο ή μπορούμε να εμποδίσουμε ένα ARP πακέτο να δημιουργηθεί. Ωστόσο τα ARP πακέτα νομιμοποιούνται και μεταφέρονται κάτω από πολλές διαδικασίες. Μία από τις πολλές συνηθισμένες είναι κατά τη διάρκεια της επικύρωσης. Αντί να περιμένουμε για την επικύρωση, αν ένας πελάτης έχει ήδη επικυρωθεί στο δίκτυο, εμείς μπορούμε να του στείλουμε ένα πλαίσιο μη επικυρωμένο, ώστε ο πελάτης να απαντήσει με ένα πλαίσιο επανεπικύρωσης. Αυτή η διαδικασία σύντομα θα δημιουργήσει ένα ARP πακέτο. Μετά από ένα ή περισσότερα ARP πακέτα που έχουν συλλεχθεί, αυτά μπορούν να αναμεταδοθούν στο δίκτυο, μέχρι να δημιουργηθούν αρκετά πακέτα ώστε να παράγουν τον απαιτούμενο αριθμό μοναδικών IVs.

Υπάρχουν δύο διαφορετικές μέθοδοι επίθεσης σε κρυπτογραφημένα με WEP δίκτυα. Η μία μέθοδος απαιτεί τη συλλογή αδύναμων IVs (Inialization Vectors) και η άλλη μέθοδος απαιτεί τη συλλογή μοναδικών IVs. Δυστυχώς όποια μέθοδος και να χρησιμοποιηθεί, απαιτεί τη συλλογή ενός μεγάλου αριθμού πακέτων κρυπτογραφημένων με WEP.

5.1.1 FMS Attacks

Η επίθεση Fluhrer, Mantin και Shamir (FMS) είναι η πιο συνηθισμένη επίθεση κατά του WEP και έχει γίνει δημοφιλής από εργαλεία όπως το AirSnort[42] και το Kismet[43]. Οι επιθέσεις FMS, είναι οι επιθέσεις κατά του WEP που χρησιμοποιούν τα αδύναμα IVs (Inialization Vectors). Οι επιθέσεις αυτές βασίζονται στην αδυναμία του αλγόριθμου κρυπτογράφησης RC4. Οι Scott Fluhrer, Itsik Mantin και Adi Shamir ανακάλυψαν ότι κατά τη διάρκεια της μεταφοράς, περίπου 9000 από τα 16000000 IVs μπορούν να θεωρηθούν ως αδύναμα. Αν συλλεχθούν αρκετά από αυτά τα αδύναμα IVs, το κλειδί μπορεί να προσδιοριστεί. Για να επιτύχει το σπάσιμο του

[41] http://el.wikipedia.org/wiki/Address_Resolution_Protocol
[42] http://airsnort.shmoo.com/
[43] http://www.kismetwireless.net/

WEP κλειδιού, χρειάζεται να συλλεχθούν τουλάχιστον 5000000 κρυπτογραφημένα πακέτα με σκοπό να συλληφθούν τουλάχιστον 3000 από αυτά αδύναμα IVs.

Μερικές επιθέσεις είναι επιτυχημένες και με 1500 αδύναμα IVs, αλλά πολλές φορές χρειάζεται και πάνω από 5000 για να θεωρηθεί το σπάσιμο του κλειδιού επιτυχημένο. Μετά που θα συλλεχθούν τα αδύναμα IVs, ξανά-εισάγονται στον Key Scheduling Algorithm (KSA) και στην Pseudo Random Number Generator (PRNG) και το πρώτο byte του κλειδιού αποκαλύπτεται. Αυτή η διαδικασία επαναλαμβάνεται και στη συνέχεια για κάθε πρόσθετο byte μέχρι να αποκαλυφθεί το WEP κλειδί.

5.1.2 Chopping Attacks

Η συλλογή αδύναμων IVs δεν είναι ο μόνος τρόπος για το σπάσιμο του WEP κλειδιού. Παρόλο που και οι επιθέσεις τύπου chopping βασίζονται στη συλλογή ενός μεγάλου αριθμού από κρυπτογραφημένα πακέτα, η μέθοδος της κοπής του τελευταίου byte από το πακέτο και η έπειτα επεξεργασία του, επιτρέπει τον προσδιορισμό του κλειδιού, από ότι η συλλογή μοναδικών IVs. Για μια επιτυχημένη επίθεση chopping, το τελευταίο byte του WEP πακέτου μετακινείται και με αυτόν τον τρόπο σπάει αποτελεσματικά τον Cyclic Redundancy Check/Integrity Check Value (CRC/ICV) έλεγχο. Αν το τελευταίο byte που κόψαμε ήταν μηδέν, υλοποιούμε XOR μεταξύ αυτού και μιας σίγουρης τιμής με τα τέσσερα τελευταία bytes του πακέτου και ο CRC θα γίνει έγκυρος ξανά. Αυτό το πακέτο μπορεί μετά να ξανά-μεταφερθεί.

5.1.3 WEP cracking με το KisMAC

Στην αγορά κυκλοφορούν διάφορα εργαλεία για το σπάσιμο των WEP κλειδιών, που μπορούν να τρέξουν στα περισσότερα λειτουργικά συστήματα. Μερικά από αυτά είναι το aircrack[44] για Windows, το kismet για συστήματα Linux, το kisMAC, και το WepOff. Παρακάτω ακολουθεί ένα παράδειγμα σπάσιμο WEP κλειδιού με το KisMAC. Το KisMAC είναι ένα εργαλείο λειτουργικού συστήματος που μοιράζεται το όνομα του με ένα άλλο δημοφιλές εργαλείο παρακολούθησης το kismet. Το KisMAC μπορούμε να το βρούμε και να το κατεβάσουμε δωρεάν στη διεύθυνση (http://www.macupdate.com/info.php/id/10133/kismac). Αυτό είναι πιο προηγμένο εργαλείο στην ανακάλυψη και παρακολούθηση δικτύων από ότι το iStumbler και το MacStumbler.

Το KisMAC είναι παθητικός σαρωτής δικτύου. Αντί να στέλνει αιτήσεις στα ενεργά σημεία πρόσβασης, αναθέτει στην ασύρματη κάρτα να συντονιστεί σε ένα κανάλι, να ακούσει σε αυτό για μικρό χρονικό διάστημα, στη συνέχεια να συντονιστεί στο επόμενο κανάλι να ακούσει κι εκεί για λίγο και πάει λέγοντας. Με αυτό τον τρόπο είναι δυνατόν όχι μόνο να ανιχνεύει δίκτυα χωρίς να ανακοινώνει την παρουσία μας αλλά επίσης να βρίσκει δίκτυα τα οποία δεν ανταποκρίνονται στις αιτήσεις αναζήτησης, τα επονομαζόμενα "κλειστά" δίκτυα (στα access points έχει

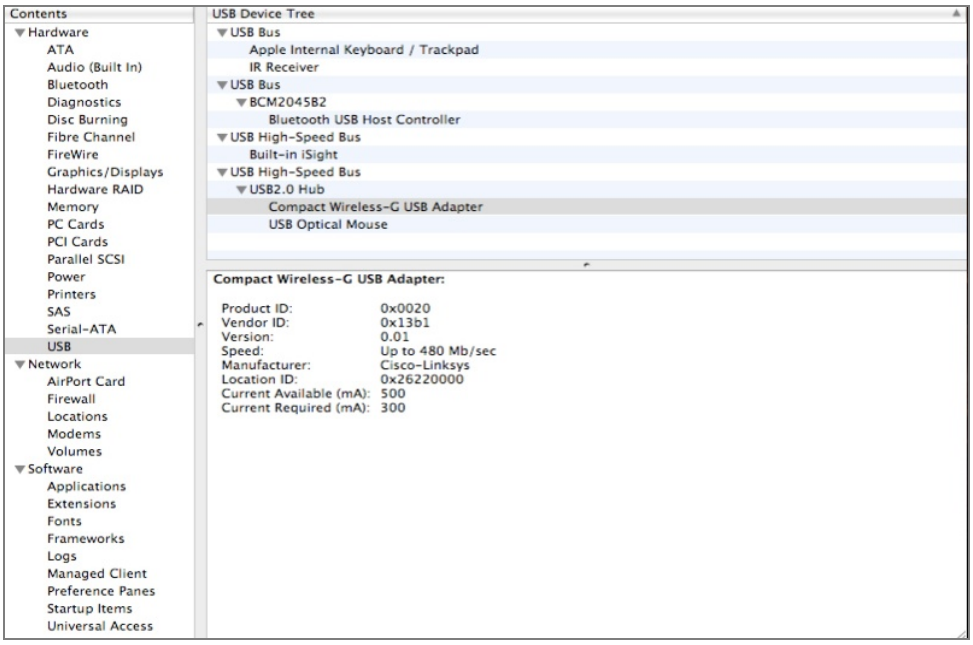
[44] http://www.aircrack-ng.org/

απενεργοποιηθεί το beaconing). Αλλά δεν είναι μόνο αυτό. Οι παθητικοί σαρωτές έχουν πρόσβαση σε κάθε πλαίσιο, που μπορεί να ακούσει το μέσο, όταν συντονίζεται σε ένα συγκεκριμένο κανάλι. Αυτό σημαίνει ότι εμείς μπορούμε να ανιχνεύουμε όχι μόνο τα σημεία πρόσβασης (access points) αλλά και τους ασύρματους πελάτες αυτών των σημείων πρόσβασης.

Ο πρότυπος οδηγός Airport, δεν παρέχει τη δυνατότητα για παθητική παρακολούθηση και έτσι το KisMAC χρησιμοποιεί τον οδηγό ανοιχτού κώδικα Viha AirPort. Αυτό καθορίζει τον κατάλληλο οδηγό Viha για τον δικό μας οδηγό AirPort, όταν αρχίζει το πρόγραμμα και αυτόματα επανεγκαθιστά τον πρότυπο οδηγό κατά την έξοδο. Για να επιτύχει αυτή η μετατροπή του οδηγού, πρέπει να δώσουμε το κλειδί του διαχειριστή (administrator key), όταν ξεκινάμε το KisMAC. Πρέπει να σημειώσουμε ότι όταν τρέχει το KisMAC, η συνηθισμένη μας ασύρματη σύνδεση είναι μη διαθέσιμη. Επίσης το KisMAC παρέχει οδηγούς για κάρτες όπως ORiNOCO, Avaya, Proxim καθώς και για Prism II-based ασύρματες κάρτες.

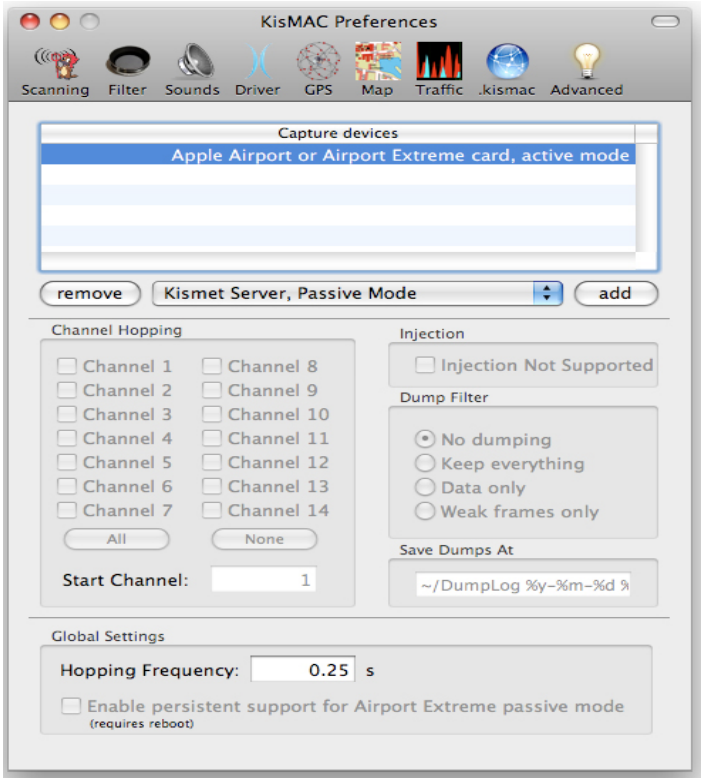
Το KisMAC έχει πολλά χαρακτηριστικά. Σε αυτά συμπεριλαμβάνεται η ενίσχυση με GPS, ενέσεις για τα ακατέργαστα πλαίσια (raw frame injection) για ασύρματες κάρτες όπως οι Prism II-based και οι ORiNOCO και μάλιστα σχετική γραφική παράσταση σε πραγματικό χρόνο. Εάν αυτό εντοπίσει ένα δίκτυο με WEP κλειδί, μπορεί να χρησιμοποιήσει ένα αριθμό από εξελιγμένες τεχνικές για να προσπαθήσει να μαντέψει τον κωδικό πρόσβασης. Επίσης μπορεί να βρει ακόμα και δίκτυα που έχουν κρυμμένο το BSSID.

Παρακάτω ακολουθεί η διαδικασία σπασίματος ενός WEP κλειδιού. Υποθέτουμε ότι έχουμε ένα ασύρματο δίκτυο, το οποίο και έχουμε ονομάσει DWL2000 και για την ασφάλεια του έχουμε χρησιμοποιήσει την κρυπτογράφηση κλειδιού WEP. Για τη σύνδεση μας στο δίκτυο έχουμε χρησιμοποιήσει σαν κλειδί το όνομα του χρήστη (k@t3r!n@).



Εικόνα 42 Αναγνώριση κάρτας δικτύου χωρίς τους drivers

Καταρχάς στην εικόνα 42, βλέπουμε την αναγνώριση της ασύρματης κάρτας που θα χρησιμοποιήσουμε και τα βασικά χαρακτηριστικά της. Στη συνέχεια το πρώτο πράγμα που πρέπει να κάνουμε είναι να ρυθμίσουμε τον οδηγό δικτύου που θα χρησιμοποιήσουμε, γι' αυτό το λόγο μετακινούμε το Apple Airport card που είναι η προεπιλεγμένη μορφή και προσθέτουμε τον ασύρματο οδηγό που εμείς θα χρησιμοποιήσουμε (εικόνα 43). Για να κάνουμε τις παραπάνω ρυθμίσεις επιλέγουμε **KisMAC** -> **preferences** ώστε να εμφανίσει στην οθόνη μας το παρακάτω παράθυρο.

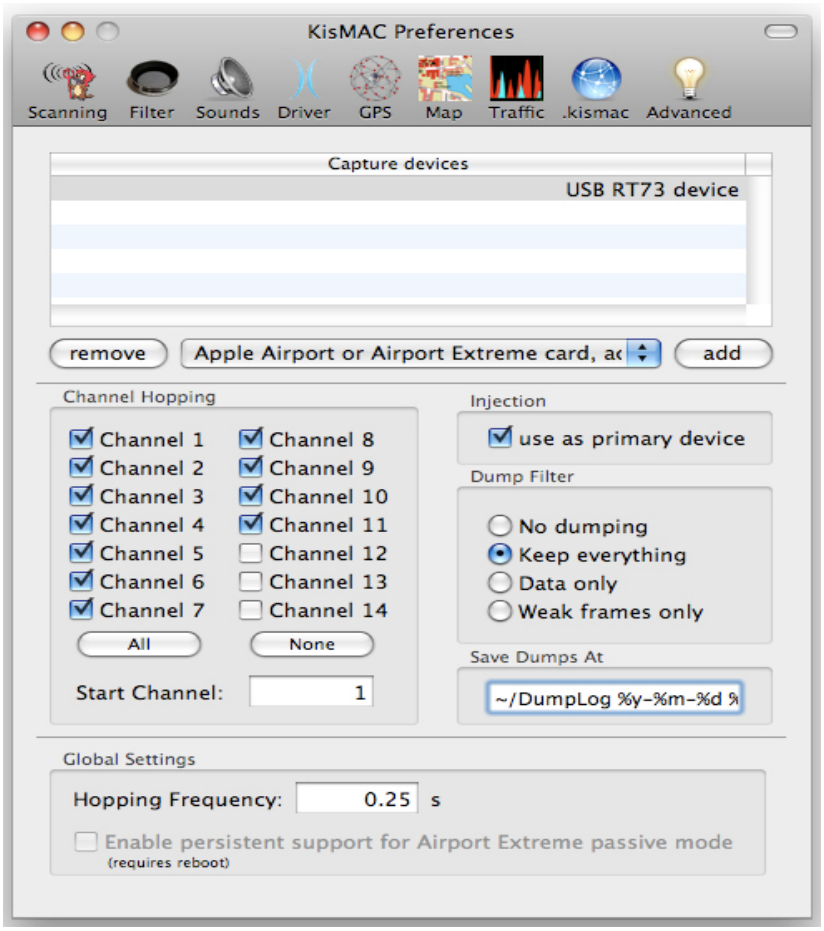


Εικόνα 43 Μετακίνηση του Apple Extreme

Το KisMAC μας δίνει τη δυνατότητα να καθορίσουμε εμείς τα κανάλια που θέλουμε να σαρώσουμε. Αυτό μπορεί να μας βοηθήσει αν προσπαθούμε να βρούμε τα σημεία πρόσβασης που χρησιμοποιούν το ίδιο κανάλι με εμάς. Μια ενδιαφέρουσα παρενέργεια της παθητικής σάρωσης είναι ότι η ανίχνευση καναλιού δεν είναι 100% αξιόπιστη. Από τότε που τα 802.11b κανάλια επικαλύπτονται, μερικές φορές είναι δύσκολο για ένα παθητικό σαρωτή να ξέρει με βεβαιότητα σε ποιο ακριβώς κανάλι είναι συντονισμένο ένα σημείο πρόσβασης, και αυτό διαφέρει από ώρα σε ώρα.

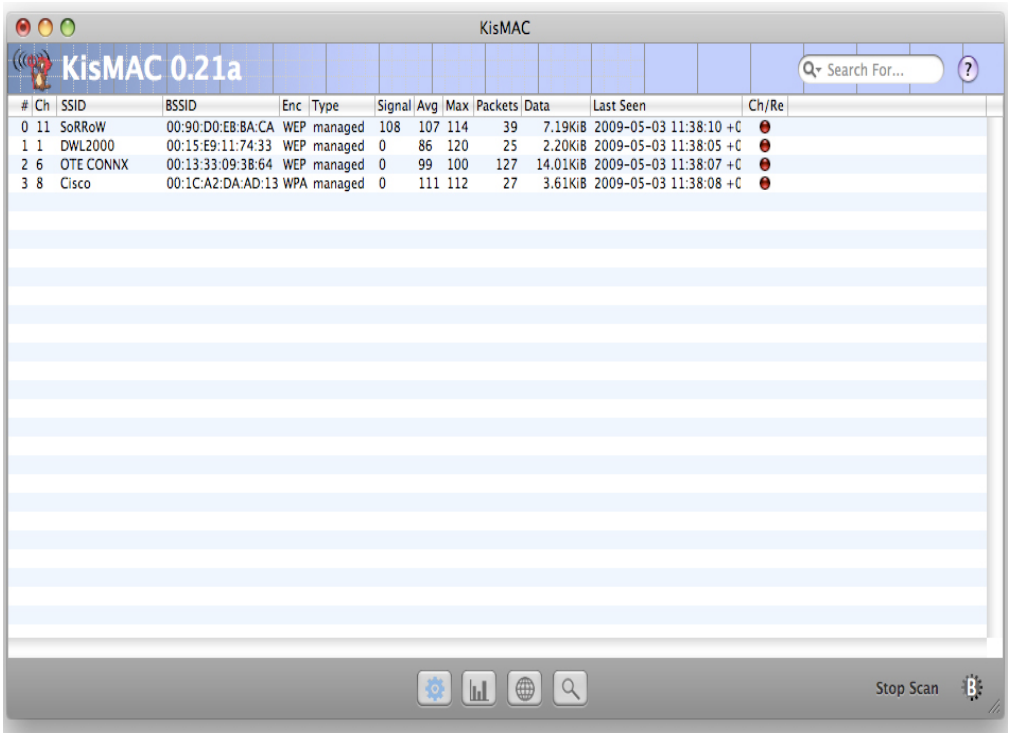
Στο παράδειγμά μας επιλέγουμε σχεδόν όλα τα κανάλια, τσεκάρουμε την επιλογή "**use as primary device**", τσεκάρουμε και την επιλογή "**keep everything**" για να κρατήσουμε όλα τα δεδομένα που μεταφέρονται. Αυτό δεν είναι απαραίτητο άλλα μπορεί να μας φανεί χρήσιμο παρακάτω. Ίσως το πιο ισχυρό χαρακτηριστικό από όλα του KisMAC είναι ότι έχει την ικανότητα να μαζεύει όλη την ακατέργαστη πληροφορία των 802.11 πλαισίων σε μια pcap "χωματερή". Η επιλογή στις προτιμήσεις "διατηρείστε τα πάντα" ή "δεδομένα μόνο" μας δίνει την δυνατότητα να αποθηκεύσουμε αρχεία που μπορεί να διαβάζονται από εργαλεία όπως το Ethereal.

Μετά από αυτό είμαστε έτοιμοι να αρχίσουμε την σάρωση των καναλιών. Αρχίζουμε να σαρώνουμε από το πρώτο κανάλι.



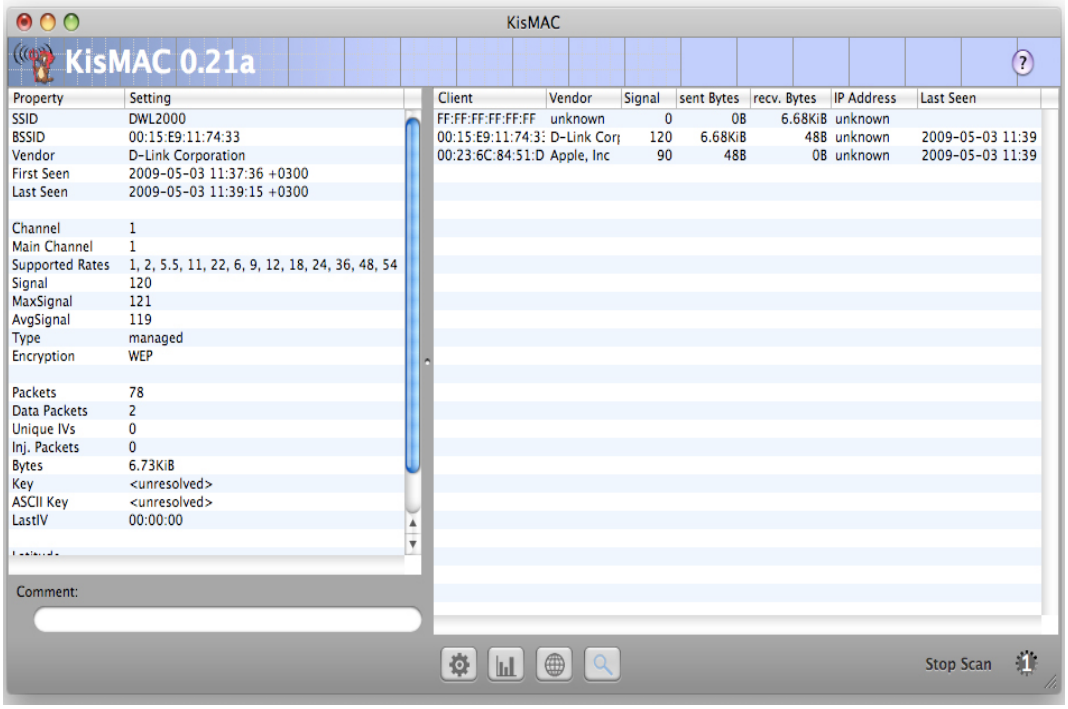
Εικόνα 44 Επιλογή των καναλιών

Η κύρια οθόνη του KisMAC (βλέπε εικόνα 45) είναι πολύ εύκολη και απλή για να την κατανοήσουμε. Παρέχει πολλές ίδιες πληροφορίες όπως το MacStumbler ή το iStumbler. Στο κύριο παράθυρο φαίνονται όλα τα ασύρματα δίκτυα που έχει βρει το KisMAC και ταξινομούνται σύμφωνα με την σειρά που ανιχνεύτηκαν, το SSID, το BSSID, την MAC διεύθυνση, το είδος της κρυπτογράφησης που χρησιμοποιούν, την ισχύ του μέγιστου σήματος, τον αριθμό των πακέτων που μεταφέρονται, κ.α.



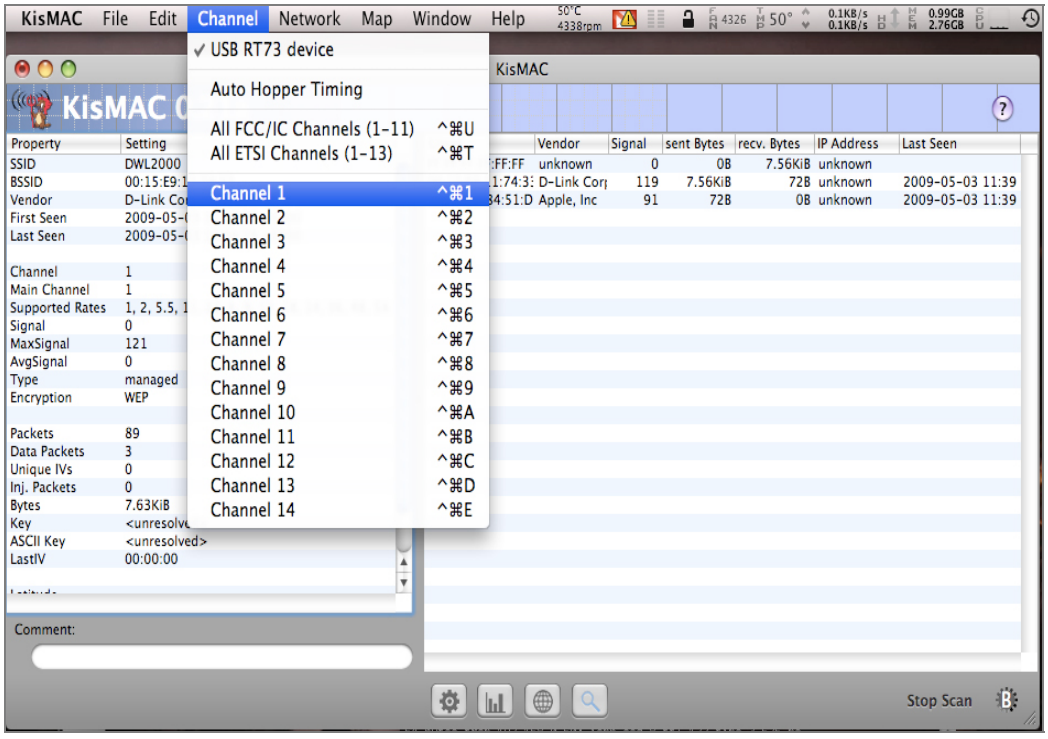
Εικόνα 45 Απεικόνιση της κύριας οθόνης του KisMAC

Με διπλό κλικ σε κάθε διαθέσιμο δίκτυο δείχνει μια πληθώρα καινούργιων πληροφοριών. Μας επιτρέπει να αποκτήσουμε αρκετές και συγκεκριμένες πληροφορίες για το επιθυμητό σημείο πρόσβασης (βλέπε εικόνα 46). Στην περίπτωση μας το επιθυμητό δίκτυο που θέλουμε να σπάσουμε είναι το DWL2000. Στην αριστερή πλευρά της οθόνης απαριθμούνται προεπιλεγμένες πληροφορίες για το συγκεκριμένο ασύρματο δίκτυο, ενώ στη δεξιά πλευρά της οθόνης υπάρχουν πληροφορίες για τους πελάτες που έχουν συνδεθεί στο δίκτυο.



Εικόνα 46 Απεικόνιση λεπτομερειών του κάθε δικτύου

Από τις πληροφορίες που συλλέξαμε για το δίκτυο-στόχο, είδαμε ότι εκπέμπει στο κανάλι 1, οπότε από την επιλογή **channels** του μενού επιλέγουμε επιθυμητό κανάλι.



Εικόνα 47 Συντονιζόμαστε στο κανάλι του στόχου

Αφού προσδιορίσουμε ότι το δίκτυο στόχος χρησιμοποιεί WEP κρυπτογράφηση, πρέπει να αποφασίσουμε πως θα σπάσουμε το WEP κλειδί. Το KisMAC παρέχει την δυνατότητα σπασίματος του WEP κλειδιού με τρείς τρόπους:

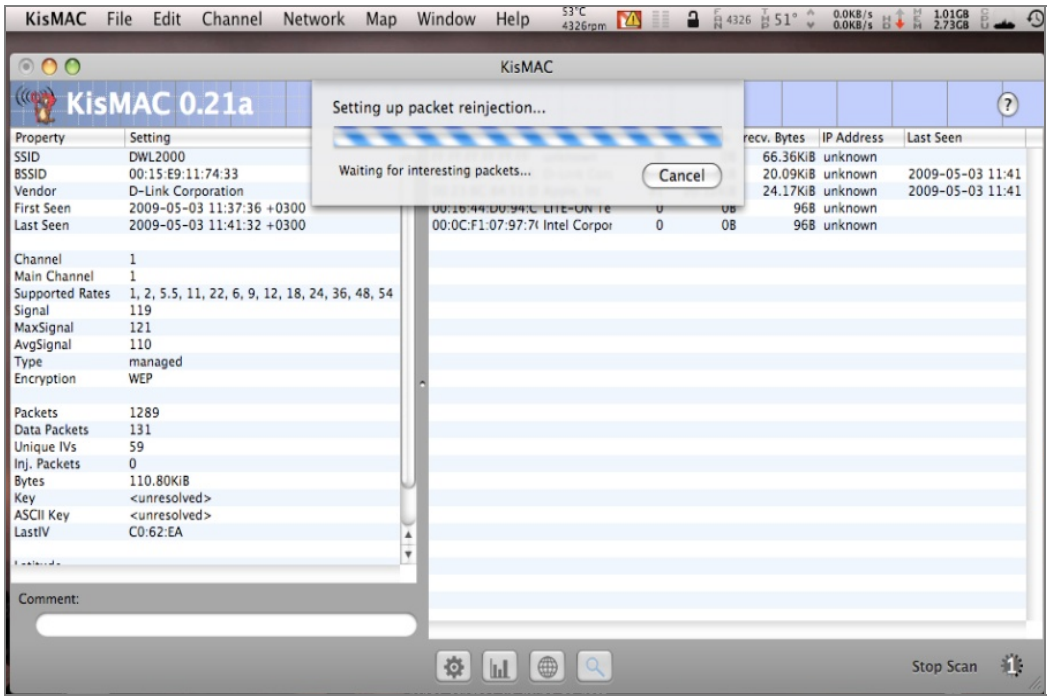
- Επιθέσεις wordlists
- Επιθέσεις weak scheduling
- Επιθέσεις brute force

Για να χρησιμοποιήσουμε οποιαδήποτε από αυτές τις τρεις επιθέσεις, πρέπει να δημιουργήσουμε αρκετά IVs (Inialization Vectors), ώστε να δουλέψει η επίθεση. Ο πιο εύκολος τρόπος για να κάνουμε αυτό είναι με το να πραγματοποιούμε "ενέσεις" στην κίνηση (reinjecting traffic), οι οποίες συνήθως επιτυγχάνονται αν συλλέξουμε ένα Address Resolution Protocol (ARP) πακέτο, εξαπατώντας τον αποστολέα και στέλνοντας το πίσω στο σημείο πρόσβασης. Αυτός ο τρόπος δημιουργεί μεγάλο ποσοστό κίνησης που μπορεί να συλληφθεί και να αποκωδικοποιηθεί.

Δυστυχώς δεν μπορούμε όμως πάντα να συλλαμβάνουμε ένα πακέτο ARP κάτω από φυσιολογικές συνθήκες. Ωστόσο όταν ένας πελάτης πιστοποιεί το σημείο πρόσβασης, συνήθως τότε ένα πακέτο ARP δημιουργείται. Εξ' αιτίας αυτού, για να αποκτήσουμε το ARP πακέτο μας μπορούμε να ξε-επικυρώσουμε όλους τους πελάτες που είναι συνδεδεμένοι στο δίκτυο και να τους κάνουμε να ξανά-προσπαθήσουν να συνδεθούν.

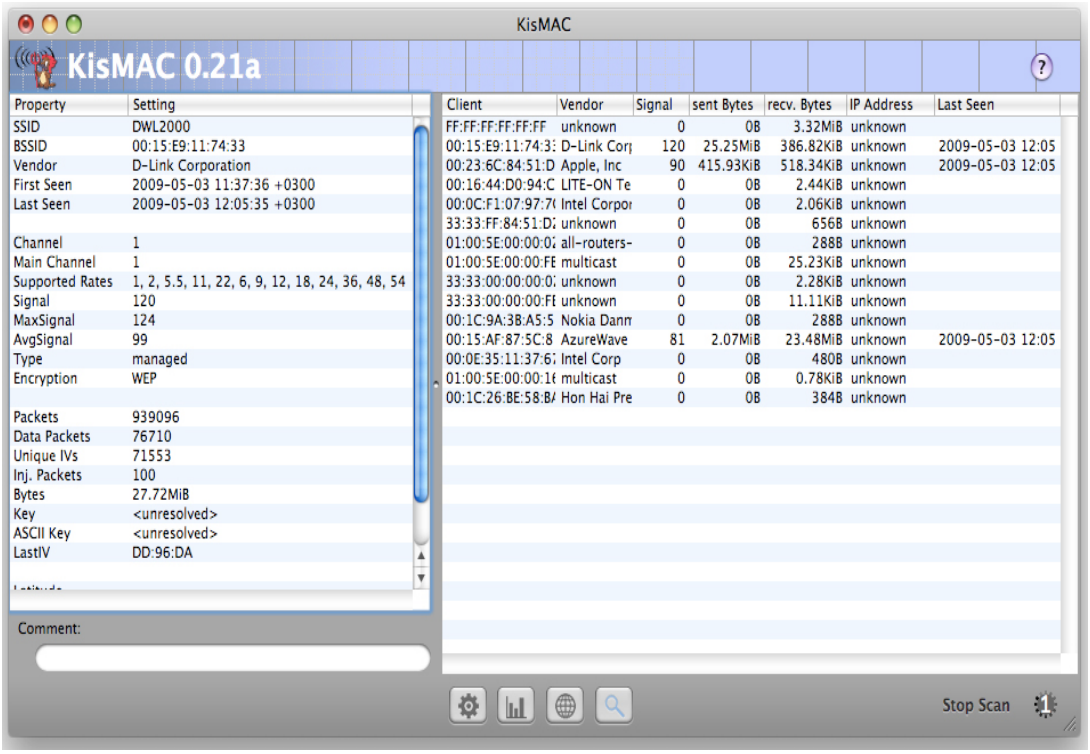
Πηγαίνουμε **Network** -> **Deauthenticate**, ώστε να δημιουργήσουμε μερικά μοναδικά IVs (Inialization Vectors) και να πραγματοποιήσουμε μια επίθεση επικύρωσης.

Αυτό κρατάει συνήθως πολύ ώρα και για να επιταχύνουμε λίγο τα πράγματα πραγματοποιούμε και μια επίθεση packet reinjection (εικόνα 48), με την επιλογή **Network** -> **Reinject packets**.



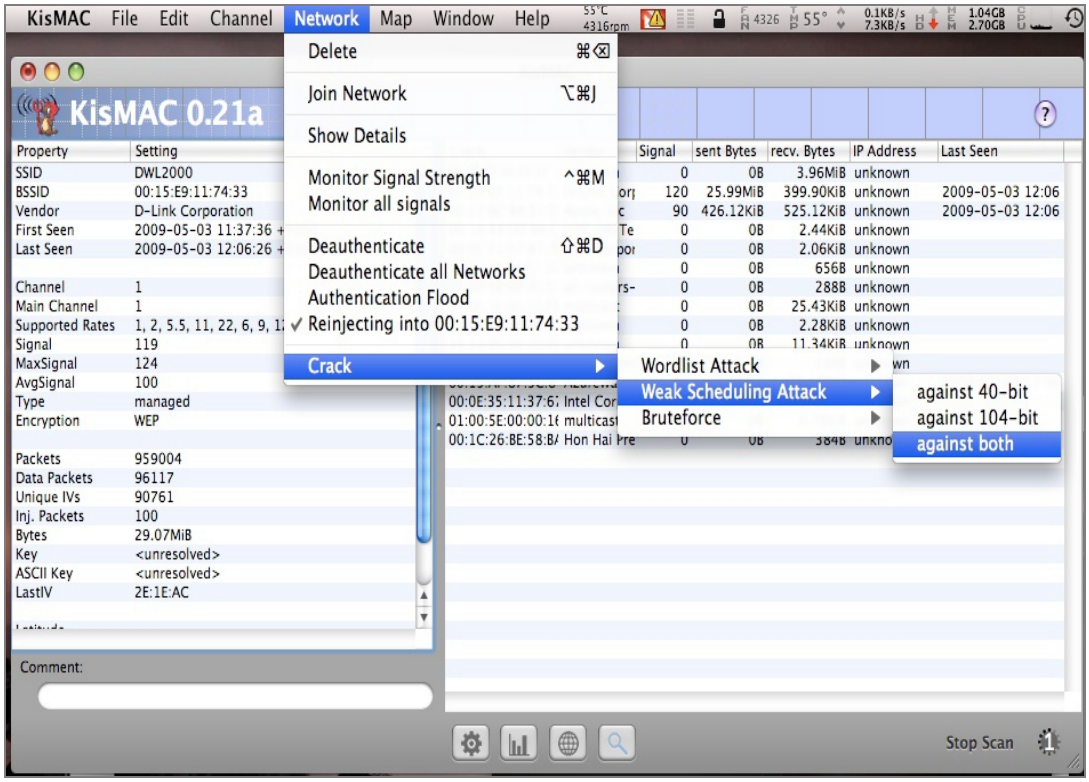
Εικόνα 48 Η διαδικασία reinjection

Κατά τη διάρκεια της διαδικασίας packet reinjection, παρατηρούμε τα μοναδικά IVs που συλλέγονται (εικόνα 49) και διάφορες πληροφορίες γι' αυτά.



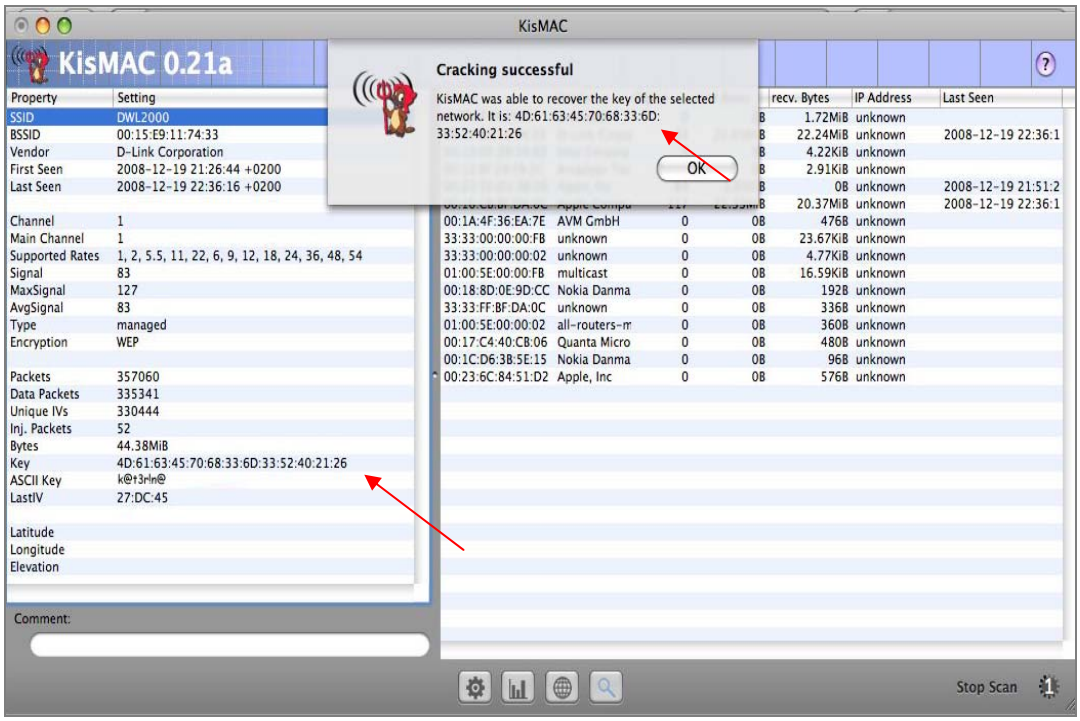
Εικόνα 49 Συλλογή ενέσιμων πακέτων

Μετά από αρκετή ώρα που θα έχουμε μαζέψει αρκετά IVs, έχει φτάσει η στιγμή να σπάσουμε το WEP κλειδί. Επιλέγουμε την μορφή επίθεσης που θα πραγματοποιήσουμε με την επιλογή **Network** -> **Crack**. Όπως βλέπουμε και στην εικόνα 50 υπάρχουν τρία είδη επίθεσης που μπορούμε να χρησιμοποιήσουμε: wordlist attack, weak scheduling attack, bruteforce. Εμείς στο παράδειγμα μας επιλέγουμε το δεύτερο είδος επίθεσης, την weak scheduling attack και επιλέγουμε και τα δύο είδη μήκους κλειδιού, για να είμαστε σίγουροι.



Εικόνα 50 Ξεκινώντας την επίθεση

Τέλος περιμένουμε έως ότου να ολοκληρωθεί με επιτυχία η επίθεσή μας και να εμφανιστεί στην οθόνη του KisMAC το επιθυμητό WEP κλειδί (εικόνα 51).



Εικόνα 51 Αποτελέσματα του KisMAC

5.2 MAC Address Spoofing

Η επίθεση MAC Address Spoofing δεν είναι το ίδιο δημοφιλής όπως την IP spoofing όμως είναι ένα πολύ δυνατό εργαλείο, το οποίο χρησιμοποιείται συχνά για το σπάσιμο ενός δικτύου ή σε δοκιμές διείσδυσης σε κάποιο δίκτυο. Παρακάτω θα εξηγήσουμε τι είναι το MAC Address spoofing, τον λόγο για τον οποίο οι άνθρωποι το χρησιμοποιούν, πως λειτουργεί, τι πλεονεκτήματα μπορεί να μας προσφέρει και πως μπορούμε να το αποφύγουμε.

Κάθε ελεγκτής διασύνδεσης δικτύου (NIC) έχει μία μοναδική Media Access Control διεύθυνση (MAC address) από τον κατασκευαστή. Όταν έχουμε ένα τοπικό δίκτυο, οι υπολογιστές ανταλλάσουν τις διευθύνσεις MAC τους, έτσι ώστε να μπορούν να αναγνωρίζουν ο ένας τον άλλον. Ποιες είναι όμως οι ομοιότητες και οι διαφορές μεταξύ μιας MAC και μιας IP διεύθυνσης; Και οι δύο αναγνωρίζουν από πού προήλθε ένα πλαίσιο και που αυτό διευθυνσιοδοτήται. Ωστόσο μία διεύθυνση IP μπορεί εύκολα να εκχωρηθεί και συχνά υπάρχει και σε άλλες μηχανές. Αντίθετα η διεύθυνση MAC είναι μία διεύθυνση υλικού και υποτίθεται ότι είναι μόνιμη ακολουθώντας τον ελεγκτή διασύνδεσης δικτύου (NIC) όπου κι αν πάει.

Η διεύθυνση MAC είναι σαν την διεύθυνση ενός σπιτιού, όπου λαμβάνουμε το ταχυδρομείο, καθώς και η διεύθυνση IP είναι σαν τον αριθμό του τηλεφώνου μας. Η "οδός" (MAC address) και ο "αριθμός τηλεφώνου" (IP address) δεσμεύονται με το ίδιο το σπίτι (υπολογιστής δικτύου), όμως το τηλέφωνο μπορεί να μεταφερθεί σε ένα άλλο σπίτι αλλά η διεύθυνση πάντα παραμένει η ίδια. Κάθε υπολογιστής που συνδέεται σε ένα δίκτυο χρησιμοποιεί μια NIC κάρτα, η οποία χρησιμοποιείται για τον εντοπισμό του στο δίκτυο.

Το MAC Address Spoofing είναι υποκλοπή ταυτότητας για καλούς ή κακούς λόγους και είναι σχετικά εύκολο. Αναφέρεται στην αλλοίωση της διεύθυνσης MAC σε μία NIC κάρτα. Το MAC Address Spoofing γίνεται τόσο για παράνομους λόγους όπως την υποκλοπή της ταυτότητας ενός άλλου υπολογιστή ή και για νόμιμους λόγους όπως την δημιουργία ασύρματων συνδέσεων. Ένα παράδειγμα της νόμιμης χρήσης του MAC Address Spoofing είναι η αλλαγή της λειτουργίας ενός μόνο υπολογιστή από τον δρομολογητή στον υπολογιστή και πάλι πίσω. Ένα παράδειγμα της παράνομης χρήσης του είναι όταν ένας παρείσακτος αλλάζει την MAC διεύθυνση του υπολογιστή του, για να εισβάλει σε ένα δίκτυο-στόχο, σαν εξουσιοδοτημένος χρήστης.

Η γνώση των παραπάνω μας παροτρύνει να συμμετέχουμε στην πρόληψη των MAC επιθέσεων. Η μία λύση είναι να ανιχνεύουμε το MAC Address Spoofing και η άλλη λύση είναι να μετατρέπουμε το σύστημα σε πιο ανθεκτικό, στα σημεία πρόσβασης ή στα μεμονωμένα μηχανήματα. Ένας γρήγορος τρόπος για να ανιχνεύσουμε κάποια ύποπτη MAC διεύθυνση είναι να τρέξουμε το RARP πρωτόκολλο (Reverse Address Resolution Protocol)[45] εις βάρος της. Το RARP χαρτογραφεί μια διεύθυνση MAC σε σχέση με την IP διεύθυνση. Μια μόνο διεύθυνση MAC θα πρέπει να χαρτογραφείται σε μία μοναδική IP διεύθυνση. Το RARP πρέπει να επιστρέφει μία διεύθυνση IP για

[45] http://en.wikipedia.org/wiki/Reverse_Address_Resolution_Protocol

κάθε συσκευή δικτύου. Έτσι αν επιστρέφονται περισσότερες σημαίνει ότι κάποια από αυτές έχει και στοιχεία που θα πρέπει να οδηγήσουν σε μια περαιτέρω έρευνα.

5.2.1 Πως γίνεται το MAC Address Spoofing;

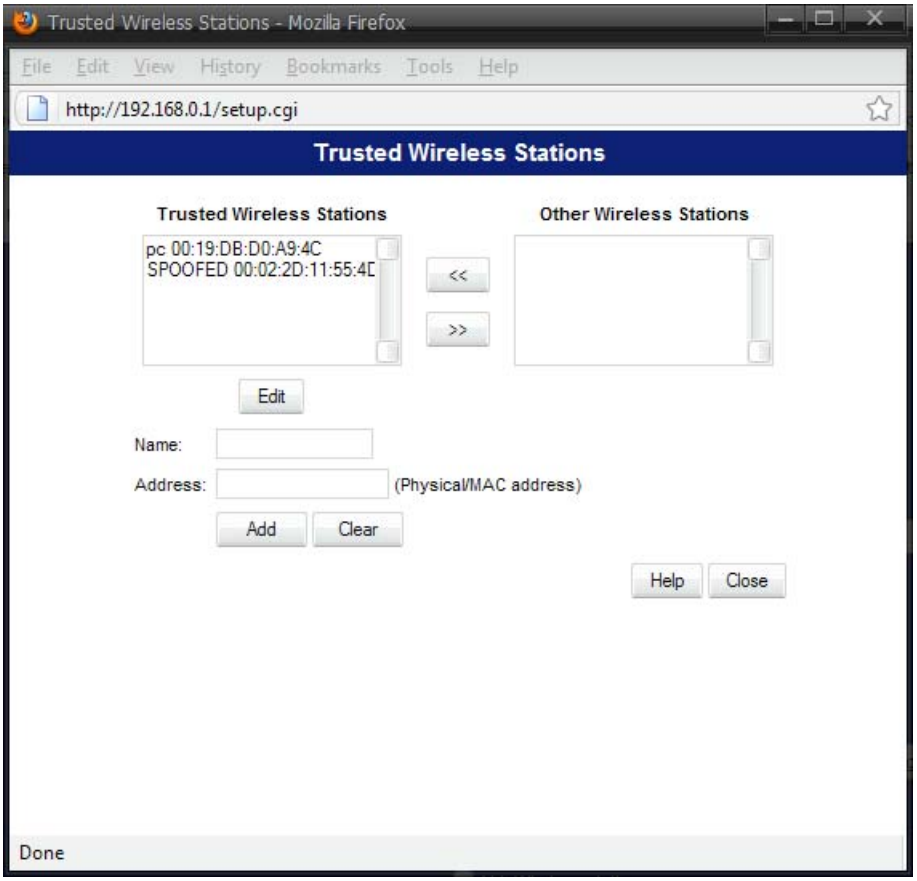
Υπάρχουν MAC Address Spoofing εργαλεία, όπως το SMAC, και διεργασίες όπως το libnet[46], που χρησιμοποιούνται σε συστήματα Windows και Linux αντίστοιχα. Με τα εργαλεία αυτά μπορεί κάποιος να επιλέξει διευθύνσεις οι οποίες δεν εμφανίζονται ήδη στο διαδίκτυο. Υπάρχουν δύο τρόποι για να κάνουμε αυτού του είδους την επίθεση σε υλικό (hardware) ή λογισμικό (software). Η hardware λύση περιλαμβάνει την αλλαγή των EEPROM[47] ρυθμίσεων σε μία κάρτα διασύνδεσης δικτύου. Την στιγμή που κάποιος έχει ως στόχο την MAC διεύθυνση, μπορεί κανείς να ξανά-προγραμματίσει τις EEPROM ρυθμίσεις της κάρτας διασύνδεσης δικτύου. Αυτό όμως περιλαμβάνει περισσότερες τεχνικές γνώσεις από ότι μία λύση λογισμικού.

Τα περισσότερα MAC Address Spoofing εργαλεία περιλαμβάνουν αλλαγές υλικού που γίνονται από εξουσιοδοτημένους χρήστες, για τις ανάγκες του δικτύου και όχι από hackers. Ένα προϊόν για τις λύσεις λογισμικού είναι το SMAC. (είναι δωρεάν διαθέσιμο για προσωπική χρήση στην διεύθυνση http://download.cnet.com/SMAC-MAC-Address-Changer/3000-2085_4-10536535.html). Δουλεύει σε Windows και αναφέρεται ως διεργασία τροποποίησης MAC διεύθυνσης. Επιτρέπει στους χρήστες να αλλάζουν γρήγορα και εύκολα τις MAC διευθύνσεις στις κάρτες διασύνδεσης δικτύου. Περιλαμβάνει οδηγίες αλλά είναι απαραίτητη και λίγη γνώση δικτύων.

Το εργαλείο SMAC δουλεύει σε τοπικό επίπεδο και όχι σε ολόκληρο το δίκτυο. Χρησιμοποιεί μία λειτουργία των Windows, την NdisReadNetworkAddress[48], που κοιτάζει στο τοπικό μητρώο των windows για την τρέχων τοπική MAC διεύθυνση. Στη συνέχεια ο προσαρμογέας δικτύου, αντικαθιστά την εργοστασιακή διεύθυνση MAC, με τις αλλαγές που έγιναν σε αυτήν στους καταχωρητές υλικού. Η διεύθυνση MAC που επιλέγεται πρέπει πάντα να είναι διευθυνσιοδοτημένη σύμφωνα με την ευθυγράμμιση διευθύνσεων IANA[49]. Διευθύνσεις που δεν είναι σύμφωνα με αυτό το πρότυπο όπως 00:00:00:00:00:00 απλά δεν θα λειτουργήσουν.

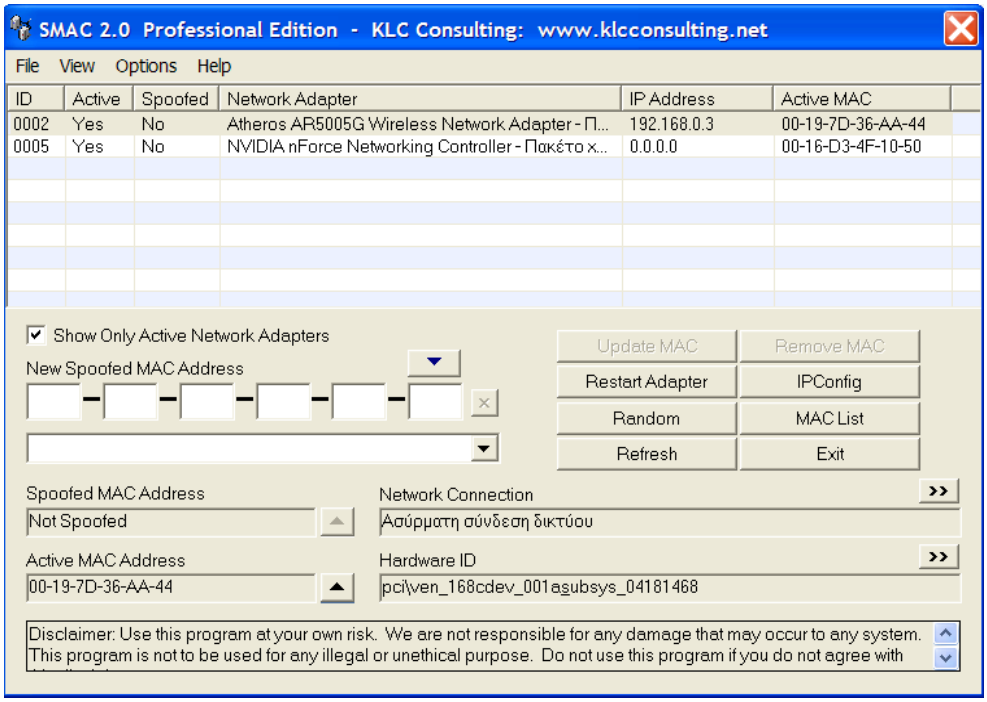
Στις παρακάτω εικόνες φαίνεται πόσο εύκολο είναι να κάνουμε MAC Address Spoofing στο δικό μας σύστημα Windows. Έστω ότι το ασύρματο δίκτυο που έχουμε εγκαταστήσει δέχεται υπολογιστές με συγκεκριμένες MAC διευθύνσεις (εικόνα 52). Οποιοσδήποτε άλλος υπολογιστής όπου η διεύθυνση MAC του δεν είναι στη λίστα με τις επιτρεπόμενες διευθύνσεις, δεν μπορεί να χρησιμοποιήσει την ασύρματη σύνδεση.

[46] http://libnet.sourceforge.net/
[47] http://en.wikipedia.org/wiki/EEPROM
[48] http://msdn.microsoft.com/en-us/library/bb625339.aspx
[49] http://www.iana.org/



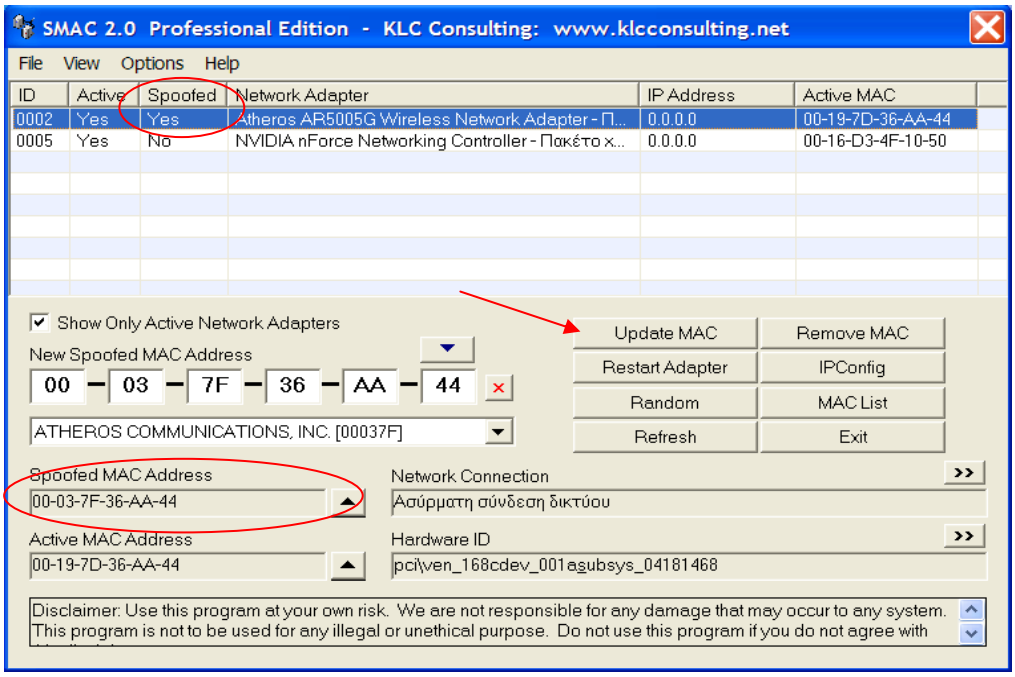
Εικόνα 52 Παράθυρο ρυθμίσεων σημείου πρόσβασης με συγκεκριμένες MAC διευθύνσεις

Από το παραπάνω παράθυρο ρυθμίσεων του σημείου πρόσβασης παρατηρούμε ότι δύο μόνο υπολογιστές με συγκεκριμένες διευθύνσεις MAC, μπορούν να έχουν πρόσβαση στο συγκεκριμένο δίκτυο. Εμείς χρησιμοποιώντας το εργαλείο SMAC, θα τροποποιήσουμε την MAC διεύθυνση του υπολογιστή μας, κάνοντας την όμοια με μια από τις παραπάνω ώστε να μπορούμε να συνδεθούμε με επιτυχία στο συγκεκριμένο ασύρματο δίκτυο. Εγκαθιστούμε λοιπόν το εργαλείο SMAC στον υπολογιστή μας. Όταν ανοίγουμε το πρόγραμμα εμφανίζονται ο network adapter, η MAC address και η IP του υπολογιστή (εικόνα 53).



Εικόνα 53 Περιβάλλον χρήσης του SMAC

- Για να αλλάξουμε την MAC Address του υπολογιστή πληκτρολογούμε την επιθυμητή MAC διεύθυνση στο πεδίο **New Spoofed MAC Address** και πατάμε **Update MAC** (εικόνα 54).



Εικόνα 54 Το εργαλείο SMAC με πλαστογραφημένη MAC διεύθυνση

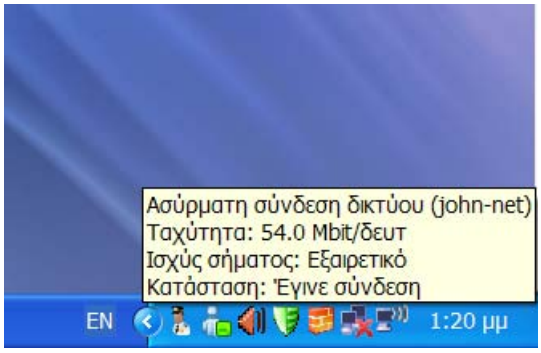
Μέσα σε λίγα δευτερόλεπτα έχουμε καταφέρει με επιτυχία να τροποποιήσουμε την MAC διεύθυνση του υπολογιστή μας. Τώρα αν πληκτρολογήσουμε στην γραμμή

εντολών ipconfig/all (εικόνα 55) βλέπουμε ότι την καινούργια MAC address του υπολογιστή μας.

```
C:\Documents and Settings\katerina>ipconfig/all

Ρύθμιση παραμέτρων IP των Windows

  Όνομα κεντρικού υπολογιστή. . . : acer-a6ec2040ef
  Επίθημα κύριου DNS  . . . . . . :
  Τύπος κόμβου. . . . . . . . . . : Εκπομπής
  Ενεργοποίηση δρομολόγησης IP. . : Όχι
  Ενεργοποίηση μεσολάβησης WINS . : Όχι

Προσαρμογέας Ethernet Τοπική σύνδεση 2:

  Κατάσταση μέσου . . . . . . . . : Έχει αποσυνδεθεί
  Περιγραφή . . . . . . . . . . . : NVIDIA nForce Networking Controller
  Φυσική διεύθυνση. . . . . . . . : 00-16-D3-4F-10-50

Προσαρμογέας Ethernet Ασύρματη σύνδεση δικτύου:

  Κατάσταση μέσου . . . . . . . . : Έχει αποσυνδεθεί
  Περιγραφή . . . . . . . . . . . : Atheros AR5005G Wireless Network Adapter
  Φυσική διεύθυνση. . . . . . . . : 00-03-7F-36-AA-44

C:\Documents and Settings\katerina>_
```

Εικόνα 55 Εύρεση της MAC διεύθυνσης του υπολογιστή μας

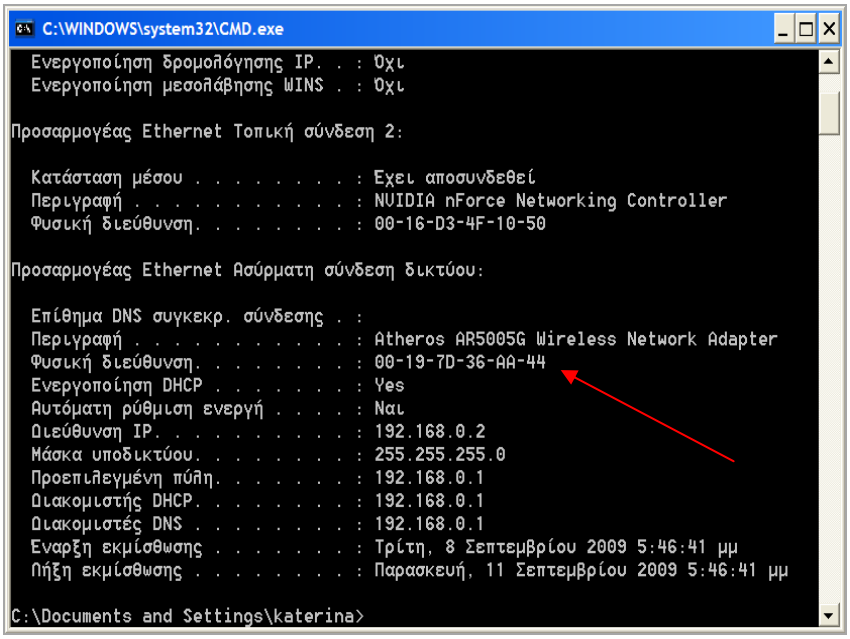
Με αυτόν τον τρόπο, με το να κάνουμε δηλαδή την διεύθυνση MAC του υπολογιστή μας να ανήκει στην λίστα του σημείου πρόσβασης με τις επιθυμητές MAC διευθύνσεις, μπορούμε να συνδεθούμε με επιτυχία στο συγκεκριμένο δίκτυο (εικόνα 56).



Εικόνα 56 Επιτυχία σύνδεσης υπολογιστή με το συγκεκριμένο ασύρματο δίκτυο

Ένας άλλος τρόπος για να επαναπρογραμματίσουμε τις ασύρματες συσκευές δικτύου αν έχουμε βέβαια μια κάρτα δικτύου που να υποστηρίζει κλωνοποίηση της MAC, είναι η παρακάτω διαδικασία:

Στην αρχή πληκτρολογώντας στην γραμμή εντολών ipconfig/all βλέπουμε ότι την MAC διεύθυνση του υπολογιστή μας (εικόνα 57).



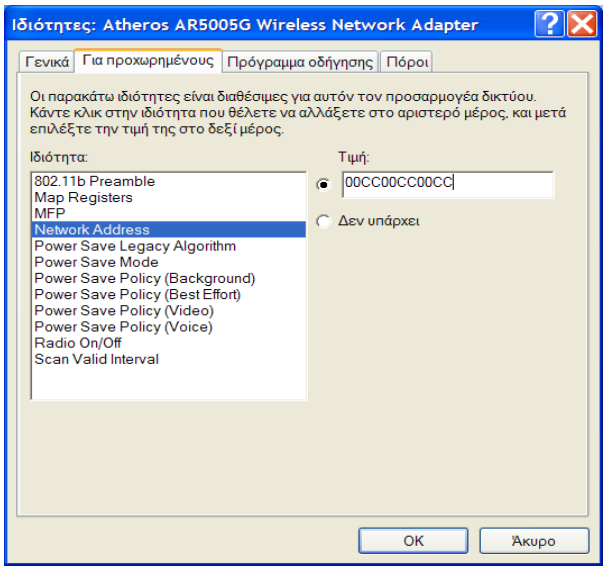
Εικόνα 57 Εύρεση της MAC διεύθυνσης του υπολογιστή μας

1. Πηγαίνουμε **Έναρξη** -> **Ρυθμίσεις** -> **Πίνακας Ελέγχου** -> και διπλό κλικ στις συνδέσεις δικτύου.

2. Πατάμε διπλό κλικ στον τύπο της ασύρματης κάρτας που θέλουμε να τροποποιήσουμε την MAC της διεύθυνση και επιλέγουμε τις ιδιότητες.

3. Στην καρτέλα γενικά πατάμε ρύθμιση παραμέτρων και επιλέγουμε το για προχωρημένους.

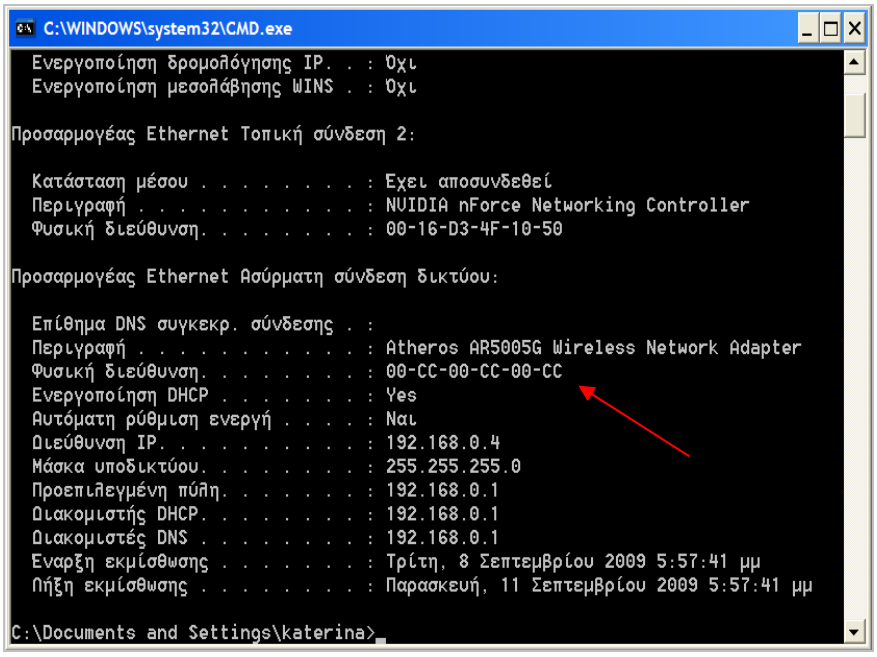
4. Κάτω από την ιδιότητα, επιλέγουμε το **network address**, όπως φαίνεται στην εικόνα 58.



Εικόνα 58 Τροποποίηση της διεύθυνσης MAC

1. Στην δεξιά πλευρά εκεί που λέει τιμή, βάζουμε την καινούρια διεύθυνση MAC που θέλουμε να έχει η ασύρματη κάρτα μας. Οι αριθμοί που εισάγονται δεν έχουν την – ανάμεσα τους.

2. Τέλος πηγαίνουμε στη γραμμή εντολών, πληκτρολογούμε **ipconfig / all** για να επαληθεύσουμε τις αλλαγές (εικόνα 59).



Εικόνα 59 Εμφάνιση τροποποιημένης MAC διεύθυνσης

5.3 Sniffing

Ένας sniffer είναι ένα πρόγραμμα ή μία συσκευή που παρακολουθεί όλες τις πληροφορίες που διαπερνούν ένα δίκτυο υπολογιστών. Κατασκοπεύει τα δεδομένα που διαπερνούν το καλώδιο του δικτύου και μαθαίνει τον προορισμό τους, την προέλευσή τους, και τι ακριβώς είναι αυτά. Εκτός από αυτές τις βασικές λειτουργίες οι sniffers, μπορεί να έχουν πρόσθετα χαρακτηριστικά όπως το να φιλτράρουν ένα συγκεκριμένο είδος δεδομένων, να συλλαμβάνουν passwords και πολλά άλλα. Πολλοί sniffers μπορούν ακόμα και να ξανακατασκευάσουν αρχεία που στέλνονται κατά μήκος του δικτύου όπως ένα email ή μια σελίδα Web.

Ένας sniffer είναι ένα από τα πιο σημαντικά εργαλεία συλλογής πληροφοριών στο οπλοστάσιο ενός hacker. Δίνει στο hacker μία ολοκληρωμένη εικόνα (τοπολογία δικτύου, IP διευθύνσεις) των δεδομένων που στέλνονται και λαμβάνονται από ένα computer ή δίκτυο που παρακολουθείται. Αυτά τα δεδομένα περιλαμβάνουν και όχι μόνο όλα τα μηνύματα ενός email, αλλά και passwords, usernames και αρχεία. Με αυτές τις πληροφορίες ένας hacker μπορεί να έχει μια ολοκληρωμένη εικόνα των δεδομένων που ταξιδεύουν στο δίκτυο και έτσι να αποκτήσει τον πλήρη έλεγχο του δικτύου.

5.3.1 Πως δουλεύει ένας sniffer

Για έναν υπολογιστή που έχει την ικανότητα να κατασκοπεύει ένα δίκτυο, πρέπει να διαθέτει μία κάρτα δικτύου που να μπαίνει σε κατάσταση παρακολούθησης. Αυτό ονομάζεται promiscuous mode, το οποίο σημαίνει ότι θα μπορεί να λαμβάνει όλη την κίνηση που στέλνεται κατά μήκος του δικτύου. Μία κάρτα δικτύου συνήθως δέχεται μόνο τις πληροφορίες που στέλνονται στη δική της συγκεκριμένη διεύθυνση δικτύου. Αυτή η διεύθυνση δικτύου είναι γνωστή ως Media Access Control (MAC) διεύθυνση. Για να βρούμε την δική μας MAC διεύθυνση πάμε στην γραμμή εργασιών των windows και επιλέγουμε **Έναρξη** -> **Εκτέλεση** και πληκτρολογούμε **ipconfig/all**. Αλλιώς η διεύθυνση MAC ενός υπολογιστή ονομάζεται και φυσική διεύθυνση.

Η μόνη διαφορά είναι σε αυτό που ονομάζεται κατάσταση παρακολούθησης. Αυτό το είδος της κάρτας δικτύου εφαρμόζεται σε ασύρματες κάρτες διασύνδεσης δικτύου (NICs). Λόγω των μοναδικών δυνατοτήτων ενός ασύρματου δικτύου, όλα τα δεδομένα που ταξιδεύουν μέσω των ερτζιανών κυμάτων είναι προσιτά σε κάθε συσκευή που έχει ρυθμιστεί για να ακούει. Αν μία κάρτα σε promiscuous κατάσταση, λειτουργήσει σε ασύρματο περιβάλλον, δεν είναι απαραίτητο να είναι οπωσδήποτε μέρος του δικτύου. Αντίθετα οι κάρτες δικτύου WNIC περιορίζονται στο να ακούν τα δεδομένα του δικτύου που προορίζονται μόνο γι' αυτές.

Υπάρχουν διάφορα στρώματα που συμμετέχουν στο δίκτυο επικοινωνιών. Κανονικά το επίπεδο δικτύου είναι υπεύθυνο για την αναζήτηση των πακέτων με τις πληροφορίες για την κάθε διεύθυνση προορισμού. Αυτή η διεύθυνση προορισμού είναι η διεύθυνση MAC του υπολογιστή. Υπάρχει μια μοναδική διεύθυνση MAC για κάθε κάρτα δικτύου στον κόσμο. Αν θέλουμε μπορούμε να αλλάξουμε την διεύθυνση, αλλά η MAC διεύθυνση διασφαλίζει ότι τα δεδομένα θα παραδοθούν στον συγκεκριμένο υπολογιστή. Αν δεν ταιριάζει η διεύθυνση MAC με αυτήν του πακέτου, τότε το πακέτο συνήθως αγνοείται.

Ο λόγος που μία κάρτα δικτύου έχει την δυνατότητα να τρέχει σε promiscuous mode, είναι για λόγους αντιμετώπισης προβλημάτων. Κανονικά ένας υπολογιστής δεν χρειάζεται πληροφορίες που πρέπει να σταλούν σε άλλους υπολογιστές στο δικτύου. Ωστόσο σε περίπτωση που πάει κάτι στραβά με τα καλώδια στο δίκτυο ή στο υλικό είναι σημαντικό για έναν τεχνικό δικτύων να μπορεί να εξετάσει τα δεδομένα που κινούνται μέσα στο δίκτυο και να ανακαλύψει τι είναι αυτό που προκαλεί το πρόβλημα.

Ένας άλλος τρόπος για να καταλάβουμε την σημασία ενός sniffer είναι να υποθέσουμε ότι υπάρχουν δύο άνθρωποι σε ένα party με διαφορετικούς τύπους προσωπικότητας. Ο ένας τύπος ανθρώπου είναι αυτός που ακούει και απαντά στις συνομιλίες στις οποίες συμμετέχει ενεργά. Έτσι είναι και η λειτουργία μιας κάρτας δικτύου που εργάζεται για την τοπική μας μηχανή. Σκοπός της είναι να ακούει και να απαντάει μόνο στις πληροφορίες που στέλνονται απευθείας σε αυτήν.

Από την άλλη πλευρά υπάρχει και ο άλλος τύπος ανθρώπου, που κάθεται σε ένα μέρος ήσυχα και ακούει προσεκτικά διαφορές συζητήσεις. Το πρόσωπο αυτό θα μπορούσε να συγκριθεί με μία κάρτα δικτύου που τρέχει σε promiscuous mode. Αν ο ωτακουστής ασχολείται με το να ακούει ένα συγκεκριμένο θέμα μόνο, θα μπορούσε

να συγκριθεί με ένα sniffer που καταγράφει για παράδειγμα όλα τα δεδομένα που σχετίζονται μόνο με τους κωδικούς πρόσβασης.

5.3.2 Πως οι hackers χρησιμοποιούν τους sniffers

Όπως αναφέρθηκε προηγουμένως, sniffers χρησιμοποιούνται κάθε μέρα για την αντιμετώπιση προβλημάτων του δικτύου και παρακολούθησης της κίνησης. Οι hackers μπορούν να χρησιμοποιήσουν διάφορα εργαλεία για να διεισδύσουν στο κάθε δίκτυο. Ανάλογα με το πρόγραμμα που χρησιμοποιεί ο κάθε hacker, παίρνει κάποιες πληροφορίες σχετικά με την κατάσταση του δικτύου. Μερικά στοιχεία από αυτά που λαμβάνουμε είναι ευανάγνωστα, ενώ ορισμένα στοιχεία δεν είναι. Η διαφορά είναι στο είδος τον δεδομένων που στέλνονται. Οι υπολογιστές μπορούν να στέλνουν πληροφορίες είτε σε μορφή απλού κειμένου (plaintext), είτε σε κρυπτογραφημένη μορφή (chiphertext).

Η επικοινωνία με κείμενο απλής μορφής είναι οι πληροφορίες που αποστέλλονται όπως φαίνονται στο ανθρώπινο μάτι. Για τις περισσότερες εφαρμογές αυτό είναι το πρότυπο μέσο μεταφοράς δεδομένων. Για παράδειγμα το διαδίκτυο χρησιμοποιεί plaintext για τις περισσότερες επικοινωνίες. Αυτός είναι ο γρηγορότερος τρόπος αποστολής δεδομένων. Chat προγράμματα, e-mail, ιστοσελίδες και μια πληθώρα άλλων προγραμμάτων αποστέλλει τις πληροφορίες τους σε plaintext. Αυτό είναι αποδεκτό για τις περισσότερες καταστάσεις. Ωστόσο αυτό αποτελεί πρόβλημα όταν διαβιβάζονται ευαίσθητες πληροφορίες όπως ένας αριθμός τραπεζικού λογαριασμού ή ένας κωδικός πρόσβασης.

Επιπλέον οι πελάτες των email και οι πελάτες των FTP είναι συνήθως αυτοί που δεν κρυπτογραφούν τους κωδικούς πρόσβασης τους. Αυτό τους καθιστά ως τα πιο συνηθισμένα προγράμματα παρακολούθησης σε ένα δίκτυο. Άλλα συνηθισμένα προγράμματα που χρησιμοποιούνται συνήθως και στέλνουν τους κωδικούς τους με μορφή απλού κειμένου είναι οι web browsers, telnet, προγράμματα ειδήσεων. Έτσι αν ένας hacker εγκαταστήσει με επιτυχία ένα sniffer στο δίκτυο μας, θα έχει σύντομα μια λίστα με ονόματα χρηστών και κωδικούς πρόσβασης που θα μπορούσε να εκμεταλλευτεί.

Ακόμα και μερικοί κρυπτογραφημένοι κωδικοί πρόσβασης που χρησιμοποιούνται σε περιβάλλον Windows μπορούν να υποκλεφτούν. Χάρη στο γνωστό σύστημα κρυπτογράφησης ενός κωδικού πρόσβασης σε Windows για παράδειγμα, δεν απαιτείται μεγάλο χρονικό διάστημα σύλληψης και αποκρυπτογράφησης κωδικών πρόσβασης ώστε να σπάσει ένα ασύρματο δίκτυο.

Αν οι sniffers χρησιμοποιούνται στο κλειστό δίκτυο μιας επιχείρησης, μπορούν να χρησιμοποιηθούν και σε όλο το internet. Το FBI έχει ένα πρόγραμμα που συλλαμβάνει όλες τις πληροφορίες που πηγαινοέρχονται σε υπολογιστές online. Αυτό το εργαλείο μέχρι πρόσφατα ονομαζόταν carnivore[50] και το μόνο που απαιτούσε ήταν να συνδεθεί και να ενεργοποιηθεί. Αν και υποτίθεται ότι φίλτραρε οποιαδήποτε

[50] http://en.wikipedia.org/wiki/Carnivore_(software)

πληροφορία δεν ήταν στόχος, το εργαλείο αυτό αιχμαλώτιζε οτιδήποτε ταξίδευε μέσα στο διαδίκτυο και στη συνέχεια φιλτραριζόταν σύμφωνα με τους κανόνες του προγράμματος. Τα sniffers μπορούν να χρησιμοποιηθούν είτε σε ενσύρματα είτε σε ασύρματα δίκτυα.

5.3.3 Πως μπορώ να ανιχνεύσω ένα sniffer?

Υπάρχουν αρκετοί τρόποι που ένας τεχνικός δικτύων μπορεί να ανακαλύψει ένα sniffer. Ένας τρόπος είναι πολύ απλά να τσεκάρει όλα τα τοπικά computer για οτιδήποτε συσκευές sniffing ή προγράμματα. Επίσης υπάρχουν προγράμματα λογισμικού εντοπισμού των sniffers, όπου μπορούν να σαρώσουν τα δίκτυα και να βρουν τέτοιου είδους συσκευές τοποθετημένες. Παράδειγμα τέτοιων εργαλείων είναι το Antisniff[51]. Αυτά τα προγράμματα σάρωσης χρησιμοποιούν διαφορετικές πτυχές του Domain Name Service και TCP/IP χαρακτηριστικά από ένα σύστημα δικτύου για να ανιχνεύουν τυχόν κακόβουλα προγράμματα ή συσκευές υπεύθυνες για την σύλληψη πακέτων και τρέχουν σε promiscuous mode. Ωστόσο για τον μέσο χρήστη που χρησιμοποιεί υπολογιστή στο σπίτι του, πραγματικά δεν υπάρχει τρόπος να εντοπιστεί αν ο υπολογιστής του με τον οποίο συνδέεται στο internet υποκλέπτεται. Γι αυτό το λόγο συνίσταται θέμα κρυπτογράφησης.

5.3.4 Πως μπορώ να μπλοκάρω τους sniffers?

Στην πραγματικότητα υπάρχει μόνο ένας τρόπος για να εμποδίσουμε την υποκλοπή των πληροφοριών μας. Να χρησιμοποιούμε κρυπτογράφηση. Χρησιμοποιώντας το Secure Sockets Layer (SSL)[52] που προστατεύει ιστοσελίδες και άλλα μέσα προστασίας, μπορούμε να κρυπτογραφήσουμε τους κωδικούς πρόσβασης, τα μηνύματα ηλεκτρονικού ταχυδρομείου και συνομιλίες chat. Υπάρχουν πολλά προγράμματα που διατίθενται δωρεάν και είναι εύκολα στη χρήση. Αν δεν έχετε πάντα ανάγκη για την προστασία των πληροφοριών που διαβιβάζονται κατά τη διάρκεια μιας συζήτησης με τους φίλους σας, θα πρέπει τουλάχιστον να έχουν την δυνατότητα, όταν χρειάζεται. Ευτυχώς τα ασύρματα δίκτυα έχουν ενσωματωμένη τη δυνατότητα κρυπτογράφησης στο λογισμικό τους. Πολλοί χρήστες επωφελούνται από αυτή την δυνατότητα όμως είναι πολλοί και οι χρήστες που δεν έχουν επίγνωση του γεγονότος και της επιλογής που υπάρχει.

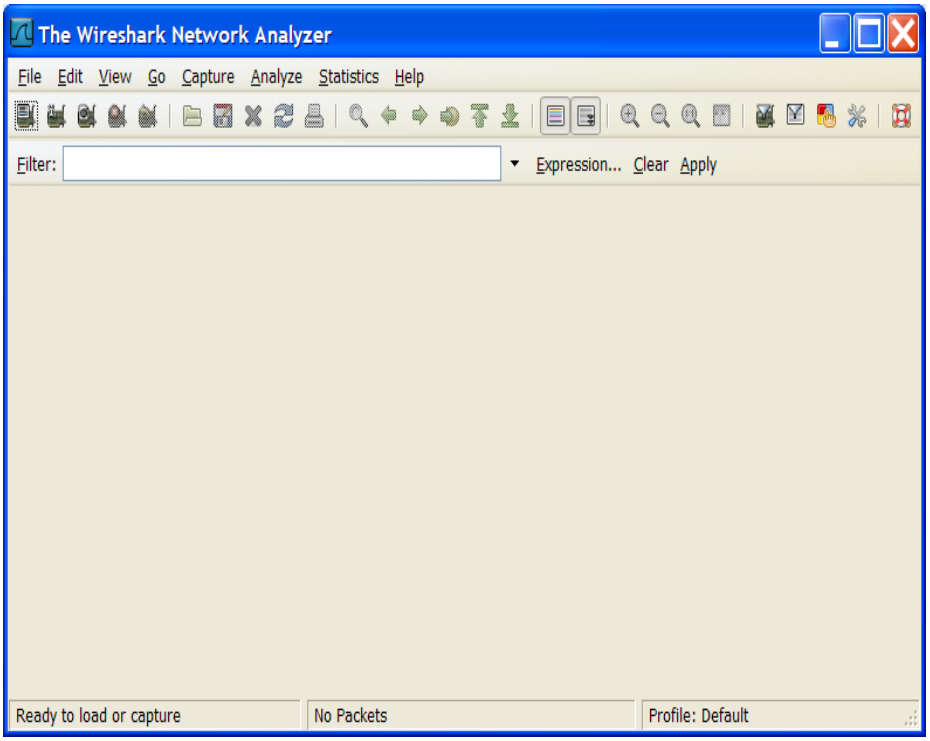
5.3.5 Παράδειγμα χρήσης sniffer

Ένα δημοφιλές sniffing εργαλείο είναι το Wireshark, που στην ουσία είναι μετονομασία του Ethereal project. Το Wireshark δουλεύει με το να συλλαμβάνει όλη την κίνηση των δικτύων σε μια ή περισσότερες διεπαφές δικτύων. Όταν

[51] http://www.linux-sec.net/Sniffer.Detectors/snifferdetection.pdf
[52] http://el.wikipedia.org/wiki/SSL

πραγματοποιούμε sniffing σε μια διεπαφή, πρέπει να έχουμε βάλει την κάρτα δικτύου μας σε promiscuous mode κατάσταση. Σε αυτή την κατάσταση, η διεπαφή μας δέχεται κάθε πακέτο που φτάνει, ακόμα και αν δεν προορίζεται για αυτήν.

Ένα από τα πιο σημαντικά χαρακτηριστικά του Wireshark είναι ότι μπορούμε να δημιουργήσουμε φίλτρα, τα οποία περιορίζουν τον αριθμό των ορατών πακέτων έτσι ώστε να μην μας δημιουργείται πρόβλημα με θόρυβο. Μπορούμε να κατασκευάσουμε ειδικές επεκτάσεις φιλτραρίσματος ή ακόμα και να συνδυάσουμε διάφορα φίλτρα ώστε να δημιουργήσουμε ισχυρές επεκτάσεις. Το Wireshark μπορούμε να το βρούμε στη διεύθυνση http://www.wireshark.org/download.html. Όταν εκτελούμε το πρόγραμμα του Wireshark, εμφανίζεται η παρακάτω εικόνα:



Εικόνα 60 Περιβάλλον χρήσης του Wireshark

Το παράθυρο του Wireshark αποτελείται από πέντε κυρίως μέρη:

- Το μενού εντολών, που είναι πάντα κυλιόμενο και βρίσκεται στην αρχή του παραθύρου. Τα μενού που χρησιμοποιούμε είναι το file και το capture. Το μενού file μας επιτρέπει να αποθηκεύουμε τα πακέτα δεδομένων που συλλαμβάνονται ή να ανοίξουμε ένα αρχείο που περιέχει πακέτα που είχαμε συλλάβει προηγούμενες φορές. Το μενού capture μας επιτρέπει να αρχίσουμε τη σύλληψη των πακέτων.

- Το παράθυρο με τις λίστες πακέτων. Εμφανίζει σε μια γραμμή, μια περίληψη για το κάθε πακέτο, συμπεριλαμβάνει τον αριθμό των πακέτων (όπως αποδίδεται από το Wireshark), την χρονική στιγμή που συνέλαβε το κάθε πακέτο, την πηγή του πακέτου καθώς και τις διευθύνσεις που αυτό

προορίζεται. Ακόμα περιλαμβάνει το τύπο του πρωτοκόλλου και ειδικές πληροφορίες πρωτοκόλλου που περιλαμβάνονται στο πακέτο. Ο κατάλογος των πακέτων μπορεί να ταξινομηθεί σύμφωνα με οποιαδήποτε από αυτές τις κατηγορίες, κάνοντας κλικ στο όνομα της συγκεκριμένης στήλης.

- Το παράθυρο που περιέχει λεπτομέρειες για την επικεφαλίδα του πακέτου. Αυτό το παράθυρο μας δίνει λεπτομέρειες σχετικά με το πακέτο που έχουμε επιλέξει στο παράθυρο με τις λίστες των πακέτων (για να επιλέξουμε ένα πακέτο από το παραπάνω παράθυρο, τοποθετούμε τον κέρσορα πάνω από την γραμμή του πακέτου που θέλουμε και κάνουμε κλικ με το αριστερό κουμπί του ποντικιού). Τα στοιχεία αυτά περιλαμβάνουν πληροφορίες σχετικά με το πλαίσιο του Ethernet και το IP datagram, που περιλαμβάνει το πακέτο.

- Το επόμενο παράθυρο είναι το παράθυρο με το περιεχόμενο των πακέτων. Εμφανίζει το περιεχόμενο των πακέτων που συλλάβαμε σε μορφή ASCII και δεκαεξαδική.

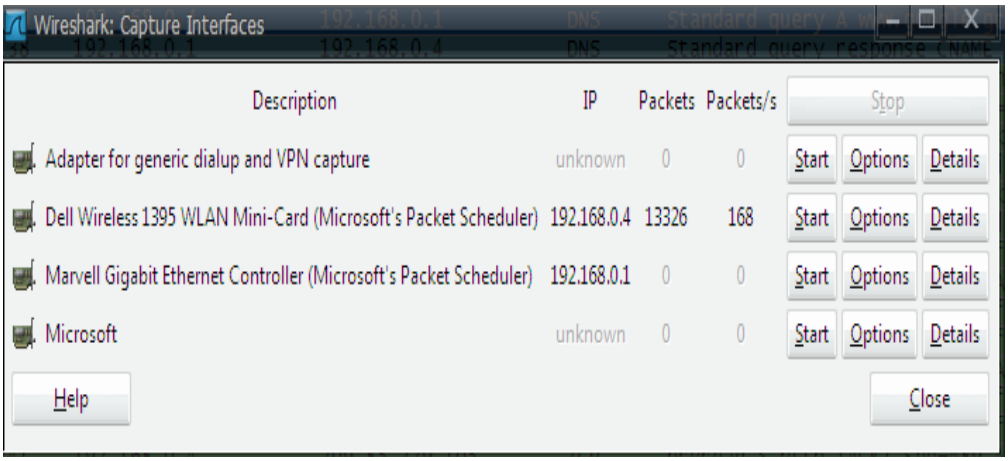
- Στην κορυφή του Wireshark, υπάρχει το πεδίο φίλτρου, όπου μπορούμε να πληκτρολογήσουμε το όνομα ενός πρωτοκόλλου ή άλλες πληροφορίες με σκοπό να φιλτράρουμε τις πληροφορίες που εμφανίζονται στο παράθυρο με τη λίστα των πακέτων.

Για να δούμε πως λειτουργεί το Wireshark ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε λοιπόν τον web browser που χρησιμοποιούμε.

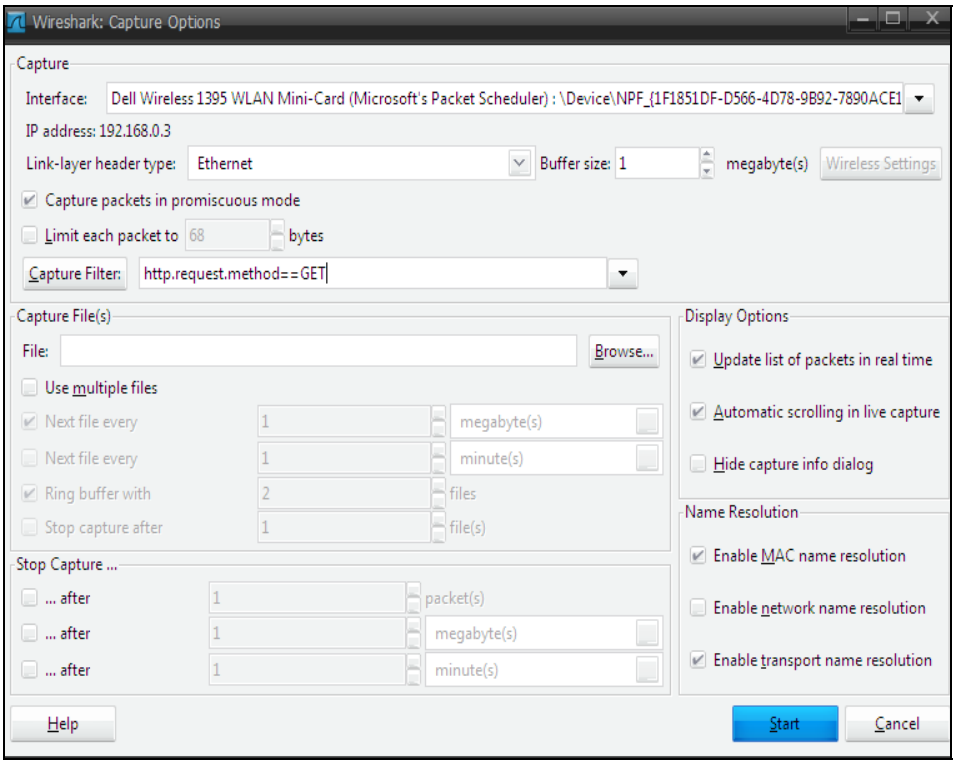
2. Ξεκινάμε το λογισμικό του Wireshark και στην οθόνη μας εμφανίζεται ένα παράθυρο όπως αυτό της εικόνας 60.

3. Για να ξεκινήσουμε την σύλληψη των πακέτων επιλέγουμε το μενού **capture** και στη συνέχεια το υπό-μενού **interfaces**. Έτσι θα εμφανιστεί στην οθόνη μας το παράθυρο Wireshark: Capture Interfaces, όπως φαίνεται στην εικόνα 61, δηλαδή τις διασυνδέσεις δικτύου (δηλαδή οι φυσικές συνδέσεις), που έχει ο υπολογιστής μας στο δίκτυο.



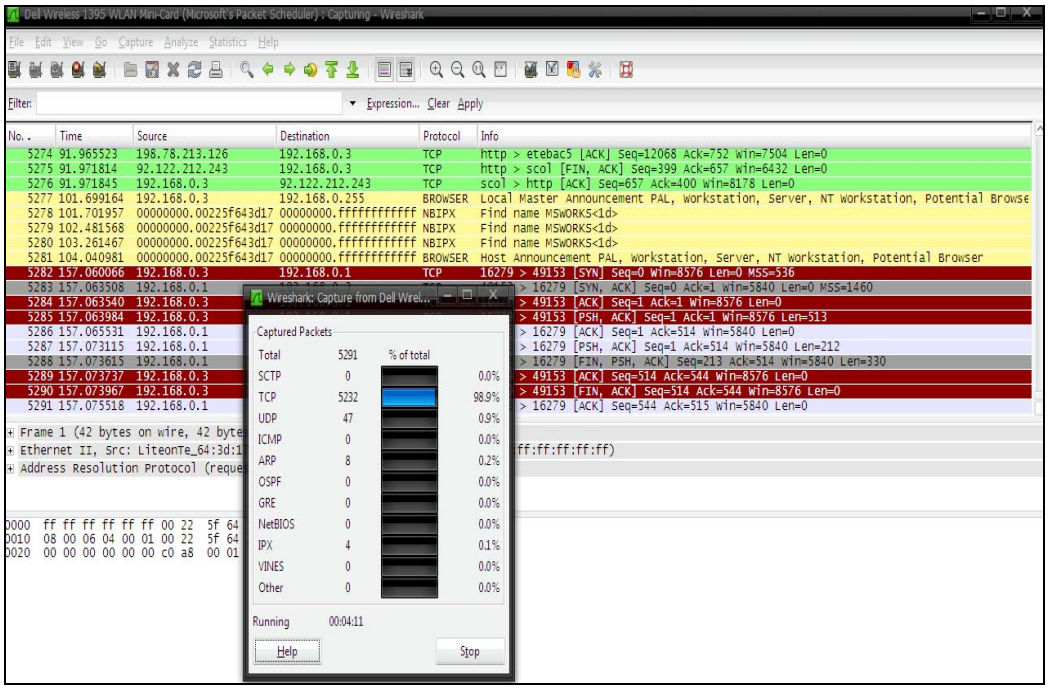
Εικόνα 61 Επιλογή των capture interfaces

4. Επιλέγουμε την κάρτα του υπολογιστή μας και πατάμε **Options**, ώστε να κάνουμε όποιες επιλογές κατά τη γνώμη μας θεωρούμε απαραίτητες (εικόνα 62). Για παράδειγμα μπορούμε να επιλέξουμε το ελάχιστο όριο που θα έχει το συλληφθέν πακέτο, κάποιο φίλτρο, να εμφανίζεται παράθυρο με πληροφορίες κατά τη διάρκεια της σύλληψης και διάφορα άλλα.



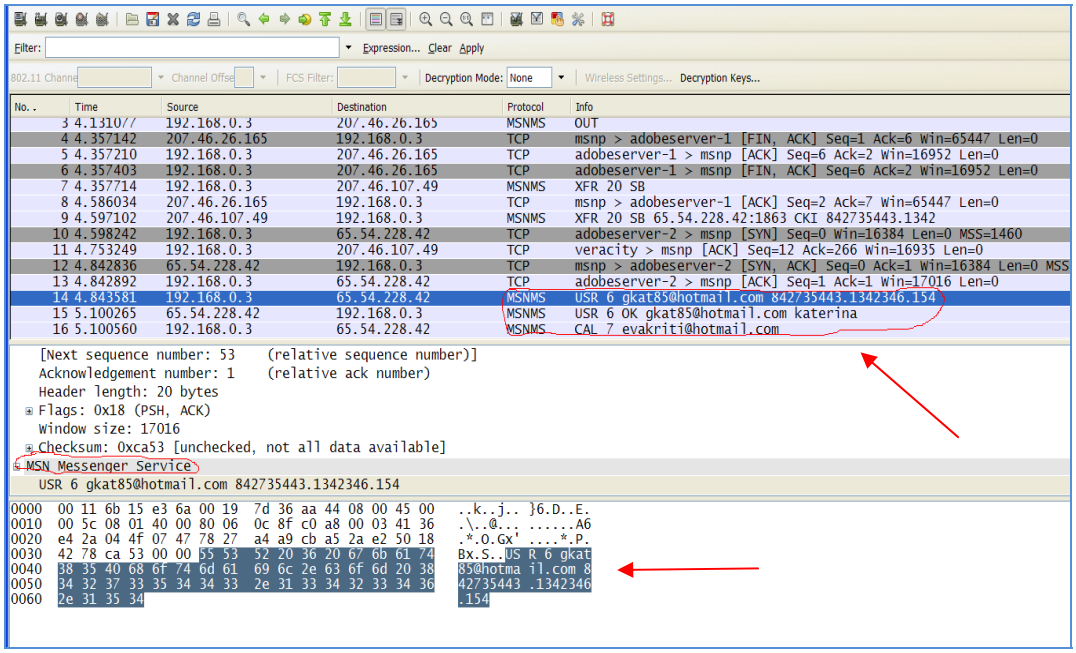
Εικόνα 62 Παράθυρο επιλογών της σύλληψης

5. Πατάμε **start** στη διεπαφή που θέλουμε ώστε να ξεκινήσει η σύλληψη των πακέτων. Όλα τα πακέτα που στέλνονται ή λαμβάνονται από τον υπολογιστή μας μπορούν τώρα να συλληφθούν από το Wireshark. Όταν το Wireshark αρχίζει να συλλαμβάνει πακέτα, γίνονται αμέσως τόσα πολλά και χρειάζεται να χρησιμοποιούμε φίλτρα, ώστε να βλέπουμε μόνο τα σημαντικά πακέτα που μας ενδιαφέρουν. Στην παρακάτω εικόνα (εικόνα 63) φαίνεται πως είναι το παράθυρο του Wireshark κατά τη διάρκεια της σύλληψης των πακέτων.



Εικόνα 63 Διαδικασία σύλληψης των πακέτων

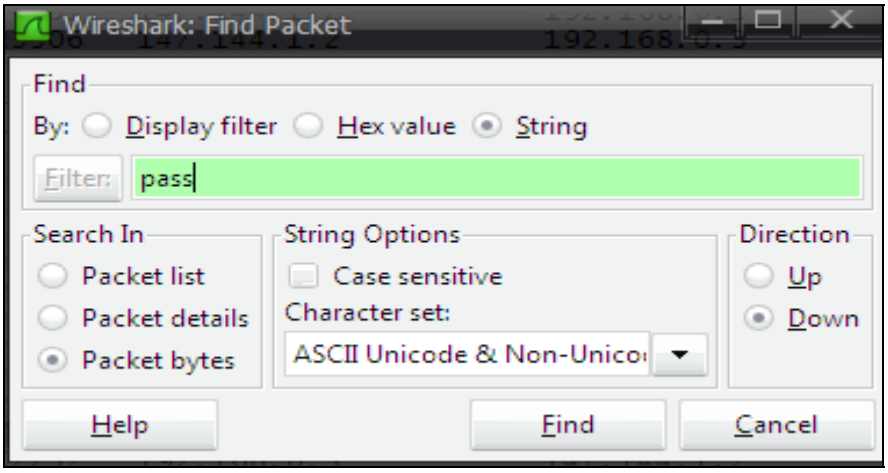
Όπως είπαμε και παραπάνω, το πρώτο παράθυρο δείχνει όλα τα πακέτα που διακινούνται στο δίκτυο, και στο τελευταίο παράθυρο εμφανίζεται τι περιέχουν τα πακέτα αυτά που τις περισσότερες φορές είναι κρυπτογραφημένα με ασύμμετρη κρυπτογραφία. Όταν υπάρχουν πακέτα μη-κρυπτογραφημένα, ο χρήστης βλέπει τα περιεχόμενα τους και όλες τις πληροφορίες στο τελευταίο πλαίσιο.



Εικόνα 64 Πληροφορίες περιεχομένων των συλληφθέντων πακέτων

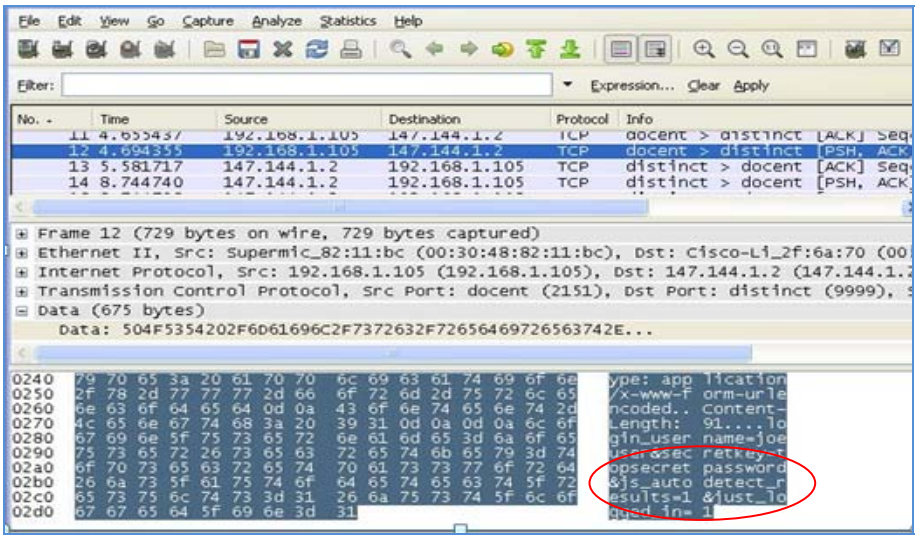
Το πρόγραμμα δίνει επίσης πληροφορίες σχετικά με την IP της πηγής και του παραλήπτη, το πρωτόκολλο που χρησιμοποιείται, και πολλές άλλες. Για να ανοίξουμε κάποιο πακέτο, τοποθετούμε τον κέρσορα πάνω από την γραμμή του πακέτου που θέλουμε και κάνουμε κλικ με το αριστερό κουμπί του ποντικιού. Το συγκεκριμένο πακέτο που επιλέξαμε, παρατηρούμε ότι είναι ένα πακέτο του windows live messenger, παρατηρούμε τη διεύθυνση mail του χρήστη, άλλα και ποιόν χρήστη κάλεσε αν παρατηρήσουμε το επόμενο πακέτο.

Για να βρούμε ένα πακέτο που περιλαμβάνει passwords για παράδειγμα, επιλέγουμε **Edit** -> **Find packet.** Στη γραμμή **By,** επιλέγουμε την επιλογή **string** (όπως φαίνεται στην εικόνα 65). Στο πεδίο του **Filter** πληκτρολογούμε τη λέξη **pass** και στη συνέχει επιλέγουμε το κουμπί **Find.**



Εικόνα 65 Παράθυρο επιλογής πακέτου ανάλογα με το φίλτρο

Με αυτό τον τρόπο το Wireshark εμφανίζει όλα τα πακέτα που περιέχουν την λέξη pass (εικόνα 66). Αν παρατηρήσουμε αναλυτικά ένα-ένα τα πακέτα, σε όποιο δεν είναι κρυπτογραφημένο θα ανακαλύψουμε το password που χρησιμοποιήθηκε.

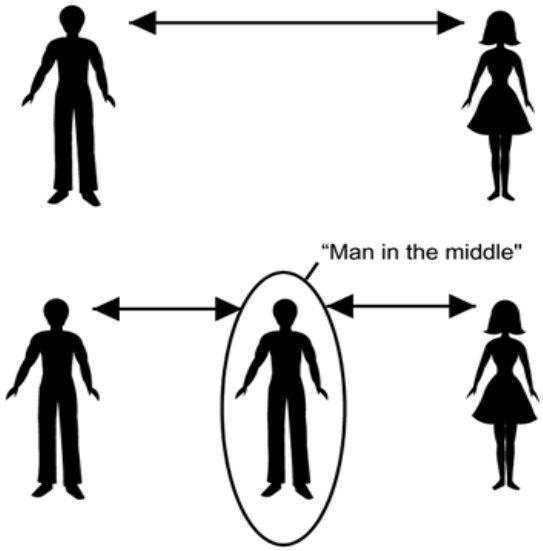


Εικόνα 66 Αποτέλεσμα εύρεσης password

Το Wireshark είναι το πιο δημοφιλής sniffing εργαλείο μέχρι σήμερα. Υπάρχουν όμως και πολλά άλλα εργαλεία που μπορούμε να χρησιμοποιήσουμε όπως το Cain and Abel, Kismet, TCPdump, SmartSniff και διάφορα άλλα.

5.4 Man-in-the-middle Attack

Ας υποθέσουμε ότι δύο άνθρωποι επικοινωνούν, με τον παραδοσιακό τρόπο και ονομάζονται Alice και Bob. Η Alice λαμβάνει μηνύματα από τον Bob και ο Bob λαμβάνει από την Alice. Ας υποθέσουμε ότι υπάρχει ένας εισβολέας, ο οποίος είναι ικανός να παρακολουθεί και να διακόπτει την συνομιλία. Ο εισβολέας μπορεί να μιμηθεί τον Bob στέλνοντας μηνύματα στην Alice ή να μιμηθεί την Alice και να στέλνει μηνύματα στον Bob. Σε αυτή την περίπτωση, λέμε ότι ο Bob και η Alice υπόκεινται σε μια Man-in-the-middle επίθεση όπως φαίνεται στην εικόνα 67. Τέτοιου είδους επιθέσεις μπορούν να χρησιμοποιηθούν για την τροποποίηση μηνυμάτων κατά τη μεταφορά χωρίς να ανιχνευτούν.



Εικόνα 67 Η επίθεση Man-in-the-middle

Υπάρχουν τουλάχιστον δύο τρόποι για να τροποποιηθεί ένα μήνυμα: μπορεί να τροποποιηθεί όταν αυτό βρίσκεται στον αέρα ή να συλληφθεί, να τροποποιηθεί και να ξανασταλθεί το μήνυμα. Η τελευταία τεχνική είναι γνωστή ως αποθήκευση και προώθηση. Η τροποποίηση στον αέρα είναι πραγματικά δύσκολη γιατί χρειάζεται να στείλουμε την μετάδοση των σημάτων ακριβώς την κατάλληλη στιγμή ώστε να επιτύχει το σκοπό του και να ερμηνεύσει λάθος το μήνυμα ο δέκτης. Εξαιτίας της εξελιγμένης διαμόρφωσης που χρησιμοποιείται στα ασύρματα δίκτυα, τα bits που στέλνονται δεν είναι μεμονωμένα, αλλά στέλνονται μαζί κωδικοποιημένα σε ομάδες, γεγονός που καθιστά πολύ δύσκολη την αλλαγή ενός και μόνο λίγο κάθε φορά. Η

τροποποίηση του μηνύματος στον αέρα είναι δυνατή στη θεωρία αλλά εμείς δεν θα καλύψουμε αυτό το θέμα περαιτέρω.

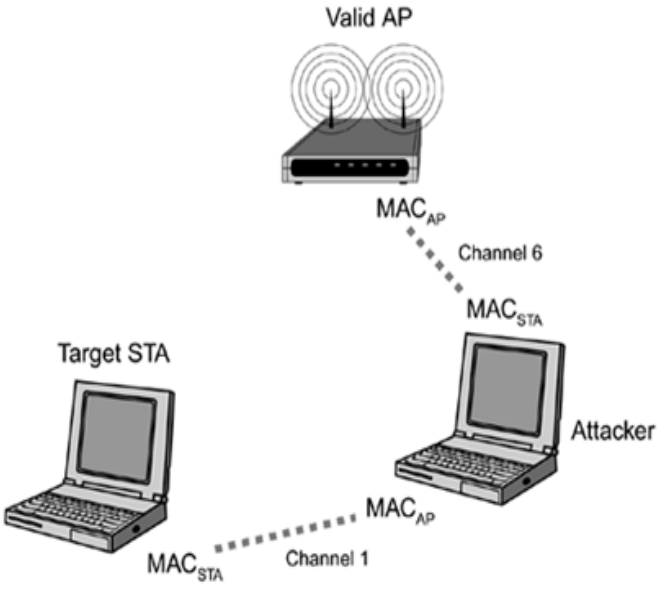
Η βασική ιδέα των man-in-the-middle επιθέσεων εισήχθη στην προηγούμενη παράγραφο. Στις επόμενες παραγράφους θα συζητήσουμε λεπτομερώς για το πώς ακριβώς ένας εισβολέας θα μπορούσε να πραγματοποιήσει μια man-in-the-middle επίθεση στο ασύρματο δίκτυο μας. Υπάρχουν δύο διαφορετικές μέθοδοι για να καθιερωθεί μια Man-in-the-middle επίθεση (MiM) σε ένα ασύρματο δίκτυο. Ο πρώτος χρησιμοποιεί τα πλαίσια διαχείρισης και είναι συγκεκριμένος για την ασύρματη δικτύωση, και ο δεύτερος είναι ARP spoofing, η οποία είναι επίσης ένα πρόβλημα ακόμα και για τα συνδεμένα με καλώδιο δίκτυα.

5.4.1 Πλαίσια διαχείρισης

Επειδή τα πλαίσια διαχείρισης στερούνται οποιαδήποτε προστασία ακεραιότητας, η εγκαθίδρυση μιας επίθεσης man-in-the-middle στα IEEE 802.11 δίκτυα είναι εύκολη. Οι επιθέσεις man-in-the-middle μπορούν να καθιερωθούν ανεξάρτητα από οποιαδήποτε προστασία (WPA, RSN, VPN) χρησιμοποιούμε, αλλά δεν αποτελούν απαραιτήτως μια απειλή εάν το πρωτόκολλο ασφάλειας είναι ισχυρό. Οι επιθέσεις man-in-the-middle συμβαίνουν επειδή δεν παρέχεται καμία εγγύηση ακεραιότητας στο στρώμα συνδέσεων, και οι διευθύνσεις MAC εύκολα πιστοποιούνται.

Η επίθεση αρχίζει (υποθέτοντας ότι ο σταθμός στόχος έχει ήδη συνδεθεί σε ένα AP) από τον επιτιθέμενο που διανέμει ένα μήνυμα τέλους επικύρωσης στο σταθμό-στόχο. Αυτό αναγκάζει το σταθμό να τερματίσει την σύνδεση του με το τρέχον σημείο πρόσβασης του και να φροντίσει να επανασυνδεθεί με ένα άλλο (ενδεχομένως το παλαιό) σημείο πρόσβασης. Ταυτόχρονα, ο επιτιθέμενος εγκαθιστά ένα κακόβουλο AP με το ίδιο ESSID και την ίδια διεύθυνση MAC ως σημείο πρόσβασης, μέσα στο εύρος του επιτιθεμένου αλλά σε ένα διαφορετικό κανάλι από το έγκυρο AP.

Τότε ο σταθμός-στόχος συνδέεται με το πλαστό AP του επιτιθεμένου επειδή το έγκυρο AP του αρνείται την υπηρεσία λόγω των αλλαγμένων μηνυμάτων τέλους επικύρωσης του επιτιθεμένου. Μόλις συνδεθεί ο σταθμός με το ψευδές AP, το ψευδές AP συνδέεται αμέσως με το έγκυρο AP και αρχίζει να προωθεί όλη την κυκλοφορία έτσι ώστε η επικύρωση να ολοκληρωθεί. Αυτή η διαδικασία παρουσιάζεται στην εικόνα 68.



Εικόνα 68 Παράδειγμα επίθεσης man-in-the-middle

Ο επιτιθέμενος έχει τώρα τον πλήρη έλεγχο του ρεύματος κυκλοφορίας μεταξύ του σταθμού και του έγκυρου σημείου πρόσβασης. Εάν δεν χρησιμοποιείται κρυπτογράφηση, ο επιτιθέμενος στη συνέχεια μπορεί να τροποποιήσει τα πακέτα πριν να τα διαβιβάσει. Εάν όμως χρησιμοποιείται κρυπτογράφηση, τα πακέτα μπορούν να αμφισβητηθούν ή να καθυστερήσουν. Μπορούν επίσης να τροποποιηθούν για να βοηθήσουν σε άλλες επιθέσεις.

5.4.2 ARP Spoofing

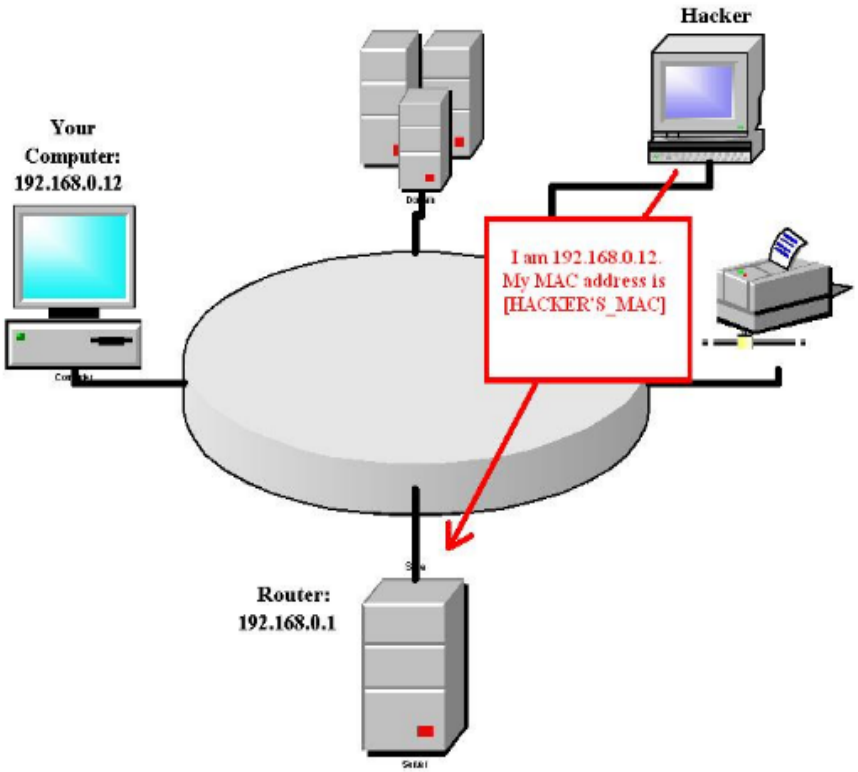
Το ARP spoofing, δηλαδή η πλαστογράφηση των πακέτων ARP (Address Resolution Protocol)[53] ήταν πολύ μεγάλη απειλή κάποτε για τα συνδεμένα με καλώδιο δίκτυα. Ενώ υπάρχουν μερικά εργαλεία διαθέσιμα για να αποτρέψουν και να προσδιορίσουν τις ARP επιθέσεις, μια ARP επίθεση μπορεί να πετύχει τις περισσότερες φορές. Το ARP πακέτο προσδιορίζει τη διεύθυνση MAC για μια δεδομένη διεύθυνση IP.

Ένας πελάτης ή ένας σταθμός που θέλει να επικοινωνήσει με μια συγκεκριμένη διεύθυνση IP εκδίδει ένα ARP-αίτημα ως πακέτο ευρείας μετάδοσης στο LAN ζητώντας να μάθει τη διεύθυνση MAC της δεδομένης διεύθυνσης IP. Επειδή τα πακέτα ARP δεν έχουν καμία προστασία ακεραιότητας, καθένας (ακόμα και οι επιτιθέμενοι που θα αποκτήσουν πρόσβαση στο LAN) μπορεί να αποκριθεί με ανακριβείς ή κακόβουλες πληροφορίες, καταστρέφοντας αποτελεσματικά την ARP μνήμη του αιτούντος. Κατά συνέπεια, από εκείνο το σημείο μέχρι τη στιγμή που μια είσοδος κρυφής μνήμης (cache) λήξει, ο πελάτης χρησιμοποιεί μια λανθασμένη

[53] http://en.wikipedia.org/wiki/Address_Resolution_Protocol

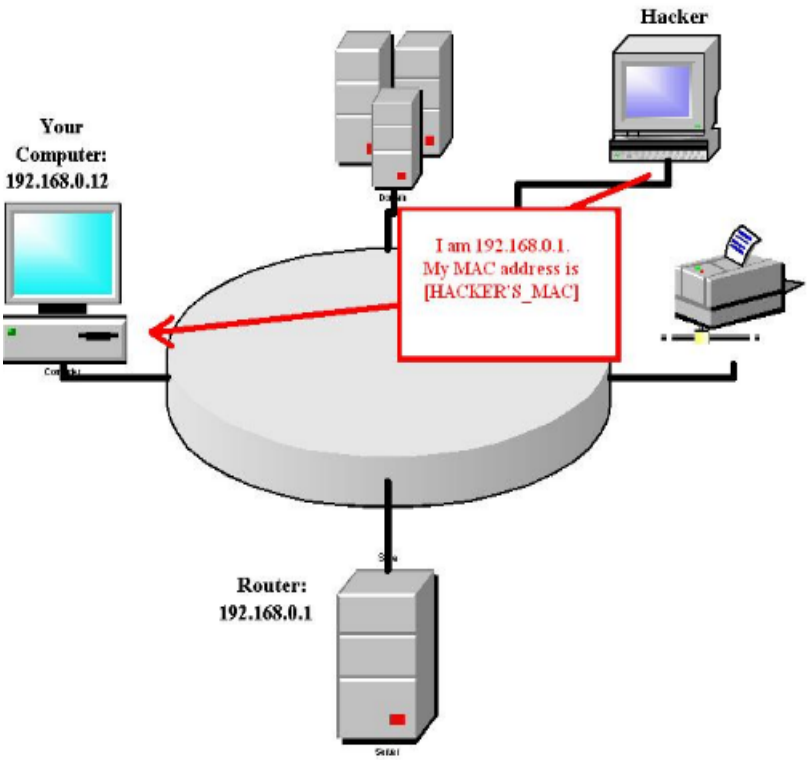
διεύθυνση MAC για τη δεδομένη διεύθυνση IP, με αποτέλεσμα όλη η κυκλοφορία να πηγαίνει στον επιτιθέμενο παρά στον πραγματικό παραλήπτη.

Ένας εισβολέας μπορεί να εκμεταλλευτεί τη κρυφή μνήμη ARP, για να παρακολουθεί την κίνηση μεταξύ δύο συσκευών στο δίκτυο μας. Για παράδειγμα ας πούμε ότι ο εισβολέας θέλει να δει όλη τη κυκλοφορία, μεταξύ του υπολογιστή μας, (με διεύθυνση 192.168.0.12), και του δρομολογητή του δικτύου μας, (με διεύθυνση 192.168.0.1). Ο εισβολέας ξεκινά με την αποστολή μιας κακόβουλης ARP "απάντησης" (για την οποία δεν υπάρχει προηγούμενη αίτηση) στο δρομολογητή μας, συνδέοντας τη MAC διεύθυνση του υπολογιστή του με την δική μας όπως φαίνεται στην εικόνα 69.



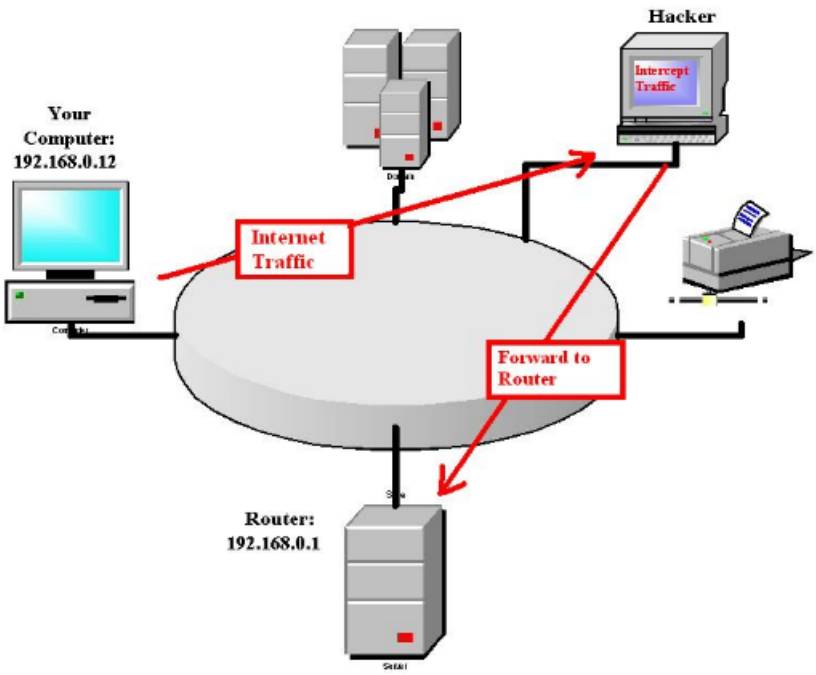
Εικόνα 69 Αλλαγή διεύθυνσης MAC εισβολέα με αυτή του θύματος

Έτσι ο δρομολογητής νομίζει ότι ο υπολογιστής του εισβολέα είναι ο δικός μας υπολογιστής. Στη συνέχεια, ο εισβολέας στέλνει μια κακόβουλη απάντηση ARP στον υπολογιστή μας, έχοντας αλλάξει τη διεύθυνση MAC του με αυτήν του δρομολογητή, δηλαδή με 192.168.0.1 όπως φαίνεται στην εικόνα 70. Έτσι ο υπολογιστής μας νομίζει ότι ο υπολογιστής του εισβολέα είναι ο δρομολογητής μας.



Εικόνα 70 Αλλαγή διεύθυνσης MAC εισβολέα με αυτή του δρομολογητή

Τέλος, ο εισβολέας μετατρέπει ένα χαρακτηριστικό του λειτουργικού συστήματος που ονομάζεται IP forwarding. Το χαρακτηριστικό αυτό επιτρέπει στη μηχανή του εισβολέα να διαβιβάσει την κίνηση του δικτύου, που λαμβάνει από τον υπολογιστή μας στο δρομολογητή (εικόνα 71). Τώρα, κάθε φορά που προσπαθούμε να μπούμε στο διαδίκτυο, ο υπολογιστής μας στέλνει την κίνηση δικτύου στον υπολογιστή του εισβολέα, ο οποίος στη συνέχεια τη διαβιβάζει στον πραγματικό δρομολογητή.



Εικόνα 71 Διαβίβαση κίνησης του δικτύου μέσω του εισβολέα

Υπάρχει μια σημαντική διάκριση μεταξύ της χρησιμοποίησης των πλαισίων διαχείρισης (όπως περιγράφεται στην προηγούμενη ενότητα) και της χρησιμοποίησης ARP spoofing για την καθιέρωση των επιθέσεων MiM. Με το ARP spoofing, ο επιτιθέμενος πρέπει να έχει πρόσβαση στο στρώμα συνδέσεων, ενώ χρησιμοποιώντας τα πλαίσια διαχείρισης δεν υπάρχει αυτή η απαίτηση. Εάν χρησιμοποιείται κρυπτογράφηση, ο επιτιθέμενος πρέπει πρώτα να σπάσει την κρυπτογράφηση (ή να είναι σε θέση να αλλάξει τα πακέτα) προτού να μπορέσει να εκτελέσει μια επιτυχή ARP επίθεση πλαστογράφησης . Με τα δίκτυα που είναι βασισμένα στη WEP κρυπτογράφηση, το σπάσιμο της κρυπτογράφησης όπως έχουμε δει, είναι εύκολο. Αλλά με τα WPA και RSN-βασισμένα δίκτυα, αυτό είναι ένα σημαντικό εμπόδιο.

5.5 Denial-of-Service Attack (DOS)

Οι hackers μπορούν να επιβάλουν το χάος, χωρίς να χρειάζεται να διεισδύσουν στο σύστημα μας. Για παράδειγμα ένας hacker μπορεί να καταφέρει να κλείσει αποτελεσματικά τον υπολογιστή μας με το να μας πλημμυρίζει με ανεπιθύμητα σήματα ή προγράμματα κακόβουλου λογισμικού. Η τεχνική αυτή είναι γνωστή ως επίθεση άρνησης εξυπηρέτησης (Denial-of-Service Attack).

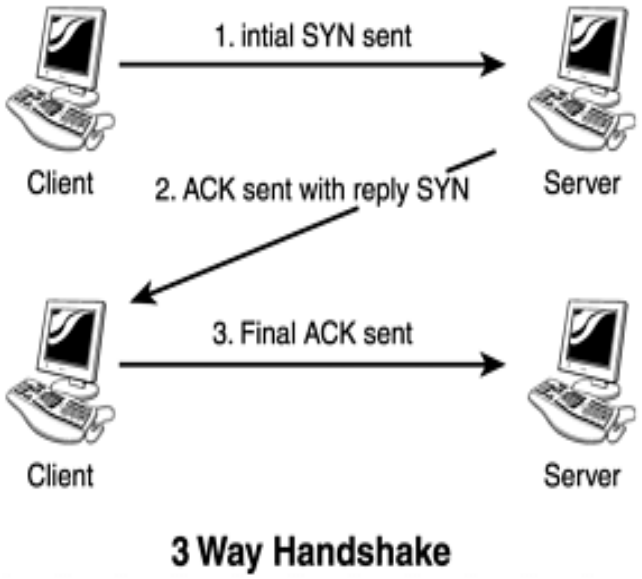
Το είδος αυτής της επίθεσης εκτελείται από τους hackers χρησιμοποιώντας μία από τις παρακάτω δύο μεθόδους. Η πρώτη μέθοδος είναι να κατακλύσουν το στόχο υπολογιστή ή τη συσκευή υλικού με πληροφορίες έτσι ώστε να μπλοκάρει. Η δεύτερη, εναλλακτική μέθοδος είναι να στέλνονται καλά διατυπωμένες εντολές ή κομμάτια από λανθασμένα δεδομένα για να κολλήσουν τον υπολογιστή στόχο. Παρακάτω παρουσιάζονται μερικά είδη επιθέσεων DOS.

5.5.1 SYN Flooding

Ο πρώτος τύπος της DOS επίθεσης που θα συζητήσουμε είναι γνωστός ως πλημμύρες SYN. Αυτού του είδους η επίθεση αιχμαλωτίζει τους πόρους ενός υπολογιστή στόχου, με το να τον κάνει να ανταποκρίνεται σε μια πλημμύρα εντολών. Για να γίνει αυτό κατανοητό μπορούμε να φανταστούμε ότι είμαστε ένας γραμματέας που η δουλεία του είναι να απαντάει και να προωθεί τηλεφωνικές κλήσεις. Έστω ότι μας καλούν 200 άτομα την ίδια χρονική στιγμή, και όταν απαντάμε στις κλήσεις τους αυτοί το κλείνουν. Εμείς είμαστε τόσο απασχολημένοι με το να απαντάμε σε νεκρές γραμμές που ποτέ δε θα φέρουμε εις πέρας οποιαδήποτε εργασία. Αυτό θα έχει ως αποτέλεσμα να απογοητευτούμε που δεν μπορούμε να ανταποκριθούμε και να τα παρατήσουμε. Πρόκειται λοιπόν για την ίδια τεχνική που οι hackers χρησιμοποιούν όταν εκτελούν μία DOS επίθεση.

Για να εκτελεστεί μία DOS επίθεση, το πρώτο πράγμα που χρειάζεται να κάνει ένας hacker είναι να καθορίσει την διεύθυνση IP του στόχου. Χρησιμοποιώντας αυτή την διεύθυνση, ο hacker θα πρέπει να συνδεθεί σε αυτήν χρησιμοποιώντας έναν υπολογιστή-πελάτη. Για να ενισχύσει την ισχύ της επίθεσης, συχνά δημιουργεί πολλούς υπολογιστές-πελάτες ταυτόχρονα προγραμματισμένους για την επίθεση του υπολογιστή στόχου. Αυτό συνήθως επιτυγχάνεται με το να πραγματοποιεί ο hacker κάποιες προκαταρτικές ενέργειες ώστε να αποκτήσει την κυριότητα πολλών υπολογιστών υψηλού εύρου σύνδεσης. Η πιο δημοφιλής πηγή για υπολογιστές-σκλάβους είναι τα πανεπιστημιακά συστήματα ή συστήματα ευρυζωνικών πελατών. Όταν ο hacker έχει εγκαταστήσει τους δικούς του υπολογιστές-σκλάβους, μπορεί να ξεκινήσει την επίθεση από ένα κεντρικό σημείο, που ονομάζεται αφέντης.

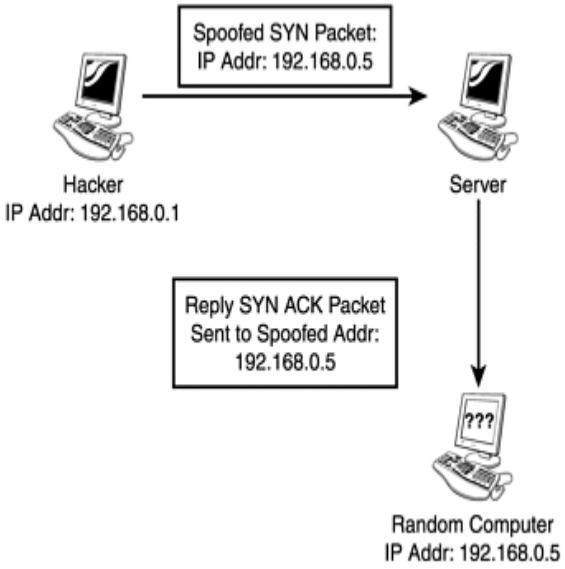
Μια SYN Flooding επίθεση όπως βλέπουμε στην εικόνα 72 χρησιμοποιεί την χειραψία του πρωτοκόλλου TCP/IP, η οποία λαμβάνει χώρα όταν δύο υπολογιστές εγκαθιστούν μια σύνοδο επικοινωνίας. Ο υπολογιστής πελάτης στέλνει πρώτα ένα πακέτο SYN στον υπολογιστή του διακομιστή για να αρχίσει η επικοινωνία. Όταν ο διακομιστής λάβει το πακέτο, που περιέχει δεδομένα, βλέπει την διεύθυνση του αποστολέα και στέλνει πίσω ένα SYN επιβεβαιωτικό πακέτο. Ο διακομιστής τότε περιμένει τον πελάτη να ανταποκριθεί με ένα τελικό πακέτο επιβεβαίωσης, το οποίο συμπληρώνει την διαδικασία σύνδεσης.



Εικόνα 72 Η διαδικασία της χειραψίας του TCP/IP

Ένας διακομιστής έχει ένα περιορισμένο αριθμό πόρων που χρησιμοποιούνται για τις συνδέσεις με τους πελάτες. Όταν ένας διακομιστής λαμβάνει αρχικά ένα πακέτο SYN από έναν πελάτη, ο διακομιστής διαθέτει ορισμένους από τους πόρους του. Ο περιορισμός αυτός έχει ένα ανώτατο όριο σχετικά με το πόσοι πελάτες μπορούν να συνδεθούν ταυτόχρονα. Αν συνδεθούν ταυτόχρονα πολλοί πελάτες με την πρώτη φορά, ο διακομιστής θα υπερφορτωθεί και θα υπερχειλίσει στην τρέχουσα διεργασία.

Η αδυναμία στο σύστημα αυτό συμβαίνει όταν ο hacker προσθέτει μία ψεύτικη διεύθυνση επιστροφής στην αρχική των πακέτων SYN όπως βλέπουμε στην εικόνα 73. Έτσι όταν ο διακομιστής στέλνει πίσω το πακέτο επιβεβαίωσης SYN στο ψεύτικο πελάτη, δεν λαμβάνει ποτέ το τελικό ACK. Αυτό σημαίνει ότι για κάθε ψεύτικο SYN πακέτο, οι περαιτέρω πόροι του διακομιστή είναι δεσμευμένοι μέχρι αυτός να αρνηθεί τις υπόλοιπες συνδέσεις. Μια επιτυχημένη επίθεση απαιτεί χιλιάδες πλαστά πακέτα, αλλά αν ένας hacker έχει πολλούς υπολογιστές-σκλάβους για να αποστέλλει πακέτα, μπορεί γρήγορα να πετύχει την υπερφόρτωση του διακομιστή.



Εικόνα 73 Επίθεση SYN χρησιμοποιώντας πλαστή διεύθυνση επιστροφής

Ένα πολύ γνωστό παράδειγμα αυτής της επίθεσης συνέβη τον Φεβρουάριο του 2000. Αρκετές ιστοσελίδες υψηλού προφίλ, όπως το CNN, Yahoo και το Amazon γονάτισαν από πλημμύρα σημάτων που προέρχονταν από εκατοντάδες διαφορετικούς υπολογιστές ταυτόχρονα. Οι ιστοσελίδες web δεν θα είχαν πρόβλημα να χειριστούν την επίθεση, αν αυτή ήταν από μία πηγή, όμως μέσω της χρήσης προγραμμάτων για εξ αποστάσεως έλεγχο και η χρήση των εκατοντάδων υπολογιστών υπερφόρτωσαν γρήγορα των στόχο.

5.5.2 Smurf Attacks

Μια παραλλαγή των πλημμύρων της DOS επίθεσης είναι οι επιθέσεις smurf. Φανταστείτε μια εταιρία με 50 υπαλλήλους που έχει τη δυνατότητα να ανταποκρίνεται στα ερωτήματα των πελατών της μέσω e mail. Κάθε εργαζόμενος έχει ένα σύστημα αυτόματης απάντησης ότι έστειλε μια ευγενική απάντηση όταν παρέλαβε κάποια ερώτηση. Τι θα συνέβαινε όμως αν ένας θυμωμένος πελάτης έστελνε 100 αντιγραμμένα mail σε κάθε έναν από τους 50 υπαλλήλους και χρησιμοποιώντας μία ψεύτικη διεύθυνση ως διεύθυνση επιστροφής;

Τα 100 εισερχόμενα e mails θα γινόταν ξαφνικά 5000 εξερχόμενα e mail και όλα θα κατευθύνονται σε ένα γραμματοκιβώτιο. Σε αυτόν που θα ανήκει αυτή η ψεύτικη διεύθυνση θα είναι συγκλονισμένος όταν δει όλα αυτά τα mail. Και θα πρέπει να ψάξει σε όλα αυτά για να βεβαιωθεί ότι δεν έχασε κάποιο σπουδαίο mail από φίλο ή το αφεντικό του. Αυτό είναι παρόμοιο με το πώς συμβαίνει μία smurf επίθεση.

Ο επιτιθέμενος στέλνει ένα αίτημα σήματος σε ένα δίκτυο υπολογιστών και κάθε ένας από τους υπολογιστές απαντάει σε μία ψεύτικη διεύθυνση επιστροφής. Ειδικά προγράμματα και άλλες τεχνικές μπορούν να συμπληρώσουν την επίθεση μέχρι να συμβεί μια πλημμύρα πληροφοριών σε έναν ατυχή υπολογιστή. Λόγω τον κανόνων

του πρωτοκόλλου TCP/IP, ένας υπολογιστής αγνοεί όλα τα πακέτα που η διεύθυνσή τους δεν απευθύνεται σε αυτόν. Μία εξαίρεση όμως είναι οι υπολογιστές που έχουν κάρτες δικτύου, οι οποίες τρέχουν σε κατάσταση παρακολούθησης (prosmisius mode), όπως αποδεικνύεται από το παράδειγμα sniffer. Μια άλλη εξαίρεση σε αυτό είναι τα πακέτα εκπομπής.

Τι χρειάζεται να κάνει μια εταιρία όταν θέλει να στείλει ένα σημαντικό μήνυμα σε όλους τους εργαζόμενούς της; μια λύση είναι να στείλει e-mail στο ηλεκτρονικό ταχυδρομείο όλων των εργαζομένων της ή μπορεί να βγάλει ανακοίνωση. Αυτές οι τεχνικές μας βεβαιώνουν ότι όλοι οι εργαζόμενοι θα λάβουν το μήνυμα. Ομοίως σε ένα δίκτυο υπολογιστών υπάρχουν φορές όπου ο διακομιστής χρειάζεται να στείλει πληροφορίες σε οποιονδήποτε συνδέεται στο δίκτυο. Αυτό επιτυγχάνεται με την χρησιμοποίηση εκπεμπόμενων διευθύνσεων.

Εξαιτίας του τρόπου με τον οποίο οι IP διευθύνσεις εγκαθιδρύονται σε ένα δίκτυο, πάντα υπάρχει μια διεύθυνση που μπορεί να απαντάει ο κάθε υπολογιστής. Αυτή η διεύθυνση είναι γνωστή ως διεύθυνση εκπομπής και χρησιμοποιείται για να ενημερώνει τους καταλόγους ονομάτων και άλλα απαραίτητα συστατικά ότι οι υπολογιστές χρειάζεται να διατηρήσουν το δίκτυο σε λειτουργία. Ωστόσο η διεύθυνση εκπομπής είναι απαραίτητη σε μερικές περιπτώσεις γιατί αλλιώς μπορεί να οδηγήσει σε αυτό που λέμε καταιγίδα εκπομπής.

Μια καταιγίδα εκπομπής μοιάζει σαν μια ηχώ που ποτέ δεν σταματάει. Εάν ένας υπολογιστής στέλνει ένα αίτημα σε ένα δίκτυο χρησιμοποιεί τη διεύθυνση μετάδοσης μαζί με τη διεύθυνση επιστροφής της εκπεμπόμενης διεύθυνσης. Κάθε υπολογιστής θα απαντήσει στου άλλου υπολογιστή την απάντηση. Αυτό συνεχίζεται μέχρι το δίκτυο να γεμίσει από ηχώ ώστε να μην μπορεί να περάσει τίποτα άλλο.

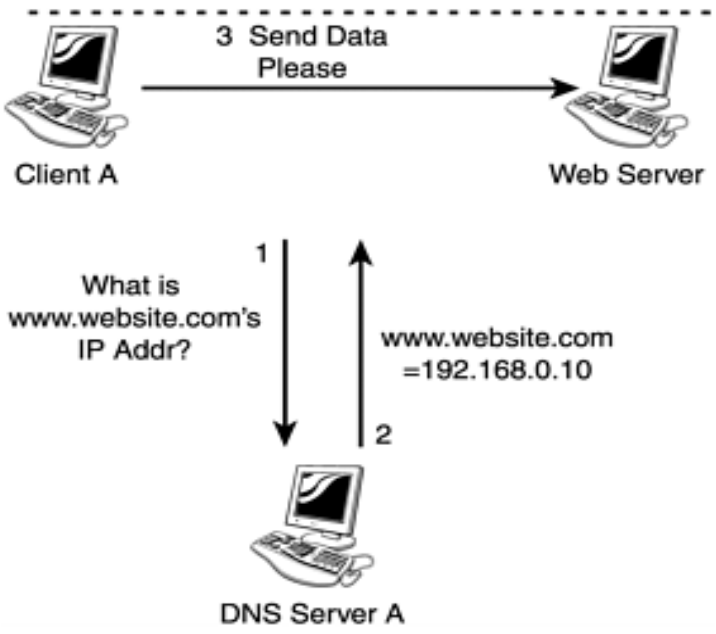
Τώρα που καταλάβαμε πως λειτουργεί μια εκπομπή φανταστείτε τι θα συνέβαινε σε ένα δίκτυο αν ένας hacker μετέδιδε 1000 εκπεμπόμενα πακέτα με μια τροποποιημένη IP διεύθυνση. Το δίκτυο θα γέμιζε από εκατοντάδες πακέτα που θα προορίζονταν σε ένα μόνο υπολογιστή. Αυτού του είδους οι επιθέσεις δεν είναι μόνο γρήγορες και αποτελεσματικές αλλά μπορούν να κρατήσουν τον hacker αόρατο. Λόγω της φύσης της επίθεσης, τα πρότυπα πακέτα που αποστέλλονται από το hacker είναι δύσκολο να εντοπιστούν.

Στην περίπτωση μιας επίθεσης SYN, η διεύθυνση είναι πλαστή. Έτσι, η καταγωγή του πακέτου παραμένει άγνωστη. Στην περίπτωση μιας επίθεσης smurf, ο hacker δεν προσβάλλει άμεσα το στόχο, αλλά, αντίθετα, χρησιμοποιεί ως αποτέλεσμα να στέλνει σήματα που μεταδίδονται σε ένα δίκτυο για να κάνει την εργασία έμμεσα. Ως εκ τούτου, η επίθεση φαίνεται να προέρχεται από άλλο υπολογιστή ή δίκτυο.

5.1.3 DNS Spoofing

Άλλα είδη επιθέσεων DOS λειτουργούν έμμεσα. Αυτά τα είδη των επιθέσεων συνήθως δεν ανακατεύουν τον διακομιστή. Αντίθετα έχουν σαν στόχο τον πελάτη. Για παράδειγμα αν νομίζουμε ότι ο υπολογιστής μας θα επισκεφτεί την διεύθυνση http://www.yahoo.gr και αντί γι' αυτήν επισκέπτεται μια ιστοσελίδα hacker που

μοιάζει με αυτήν του yahoo. Αυτό θα έχει ως αποτέλεσμα να μάθουν οι εισβολείς τους κωδικούς πρόσβασης μας αλλά και άλλες σημαντικές προσωπικές πληροφορίες. Αυτό το είδος της επίθεσης λέγεται Domain Name Service Spoofing και φαίνεται στην εικόνα 74.



Εικόνα 74 Παράδειγμα επίθεσης DNS Spoofing

Συνήθως όταν ένας υπολογιστής πελάτης ρωτάει τον DNS διακομιστή ένα domain name[54] ή τη διεύθυνση μιας ιστοσελίδας, αυτό χρειάζεται να μετατραπεί σε διεύθυνση IP. Αυτό οφείλεται στο γεγονός ότι ο υπολογιστής πελάτης χρειάζεται την διεύθυνση IP, για να εντοπίσει το διακομιστή web ή τον e-mail διακομιστή που χρησιμοποιεί το domain name. Αυτό φαίνεται σε τρία στάδια στην εικόνα 67.

1. Ο πελάτης ζητά από τον DNS διακομιστή, την διεύθυνση IP του domain name.

2. Ο DNS διακομιστής ρωτάει τη βάση δεδομένων του και απαντά με μια διεύθυνση IP που ταιριάζει στο domain name που του ζητήθηκε.

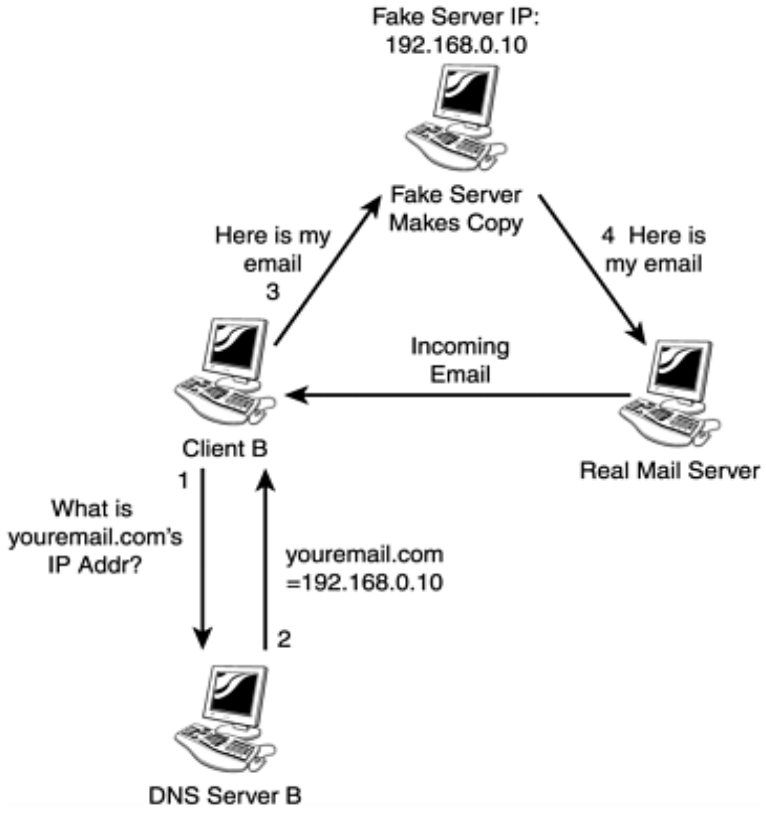
3. Ο πελάτης συνδέεται με το διακομιστή με τη διεύθυνση IP, που του παρείχε ο DNS διακομιστής.

Ωστόσο αυτή η διαδικασία μπορεί εύκολα να παραποιηθεί, με την αποστολή ψευδών ιστοσελίδων σε ανυποψίαστους χρήστες ή τη δρομολόγηση εξερχόμενων e-mail μέσω ενός υπολογιστή χωρίς άδεια (εικόνα 75). Αυτό επιτυγχάνεται με το γράψιμο λάθος

[54] http://en.wikipedia.org/wiki/Domain_name

διεύθυνσης IP στη βάση δεδομένων του διακομιστή DNS. Όταν συμβαίνει αυτό, είναι σχεδόν αδύνατο για τον πελάτη να συνειδητοποιήσει ότι υπάρχει πρόβλημα. Ο μόνος τρόπος είναι να ελεγχθούν ειδικά οι καταχωρήσεις του διακομιστή DNS.

Στην περίπτωση που ένας DNS διακομιστής προσβληθεί από επίθεση, μόνο το εξερχόμενο e-mail στέλνεται στην πλαστογραφημένη τοποθεσία εκτός και αν ο e-mail διακομιστής χρησιμοποιεί τον ίδιο διακομιστή DNS με τον πελάτη. Σε αυτή τη περίπτωση, όλα τα εισερχόμενα και τα εξερχόμενα e-mail δρομολογούνται μέσω ενός μη εξουσιοδοτημένου υπολογιστή. Ωστόσο, στο παράδειγμα μας, θα θεωρήσουμε δεδομένο ότι ο e-mail διακομιστής χρησιμοποιεί έναν ασφαλή διακομιστή DNS για τις αναζητήσεις του.



Εικόνα 75 Επεξήγηση της DNS Spoof επίθεσης

Σε περίπτωση που ο DNS διακομιστής προσβληθεί από επίθεση, όπως φαίνεται στην εικόνα 68 συμβαίνουν τα εξής:

1. Ο πελάτης B κάνει μια αίτηση για διεύθυνση IP για την τοποθεσία youremail.com

2. Ο προσβλημένος DNS διακομιστής απαντά με την πλαστή διεύθυνση 192.168.0.10.

3. Ο πελάτης Β συνδέεται με τον πλαστό e-mail διακομιστή και στέλνει το μήνυμα.

4. Ο πλαστός διακομιστής αντιγράφει το e-mail και το στέλνει στον πραγματικό διακομιστή e-mail.

5. Ο πραγματικός διακομιστής e-mail , χρησιμοποιώντας ένα ασφαλή DNS, στέλνει το μήνυμα ηλεκτρονικού ταχυδρομείου πίσω στον πελάτη.

Αυτό το σενάριο μπορεί να παρέχει στο hacker κάποιες σημαντικές πληροφορίες. Για παράδειγμα, εάν ο πελάτης Β είναι γιατρός ή δικηγόρος, ο hacker θα έχει πρόσβαση σε ευαίσθητες πληροφορίες. Εάν ο πελάτης Β εργάζεται σε ένα άκρως απόρρητο σχέδιο, ο hacker θα μπορούσε να πωλήσει τις πληροφορίες σε μια ανταγωνιστική εταιρεία. Ή, εάν ο πελάτης είναι ένα ηλεκτρονικό κατάστημα στο Web, ο hacker θα μπορούσε να συλλάβει κάθε email επιβεβαίωσης με τις διευθύνσεις των πελατών ή αριθμούς πιστωτικών καρτών. Όπως μπορούμε να δούμε, υπάρχει μια τεράστια δυνατότητα ζημίας από μια επίθεση DNS spoofing. Αν ένας hacker θέλει να μετατρέψει μια τοποθεσία Web σε αόρατη ή να συλλάβει ηλεκτρονικό ταχυδρομείο, αρνείται τις υπηρεσίες σε όσους χρησιμοποιούν το προσβλημένο διακομιστή DNS.

5.6 Café Latte Attack

Οι αδυναμίες που έκαναν το WEP ευάλωτο δημοσιεύτηκαν το 2001 και αυτό είχε ως αποτέλεσμα τη δημιουργία εκατοντάδων εργαλείων που σχετίζονταν με το σπάσιμο του WEP κλειδιού. Μέχρι πρόσφατα αυτού του είδους οι επιθέσεις εστιαζόταν στη σύλληψη της κίνησης από ενεργά δίκτυα, απαιτώντας εγγύτητα στους στόχους των επιχειρήσεων. Αλλά τελευταία, η εστίαση έχει γίνει προς τους ανενεργούς πελάτες, που δεν είναι συνδεδεμένοι σε κανένα δίκτυο. Εκμεταλλευόμενοι τις αδυναμίες του οδηγού, εκτίθενται οι φάκελοι κοινής χρήσης και τα λάθη των χρηστών και έτσι μπορεί κάποιος πολύ εύκολα και αόρατα να επιτεθεί σε ασύρματα laptops και τηλέφωνα σε δημόσιους χώρους, όπως αεροπλάνα, ξενοδοχεία και καφετέριες.

Μια άλλου είδους επίθεση που σχετίζεται με το σπάσιμο του WEP κλειδιού είναι η επονομαζόμενη "Café Latte Attack". Η επίθεση αυτή ανακαλύφθηκε από δύο ερευνητές των Air Tight δικτύων. Με αυτή την επίθεση αποδεικνύεται ότι ο επιτιθέμενος μπορεί να ανακαλύψει το WEP κλειδί, χωρίς να βρίσκεται στην ίδια γειτονία με το συνεργαζόμενο ασύρματο δίκτυο και στοχεύοντας απομονωμένους πελάτες σε δημόσιες περιοχές.

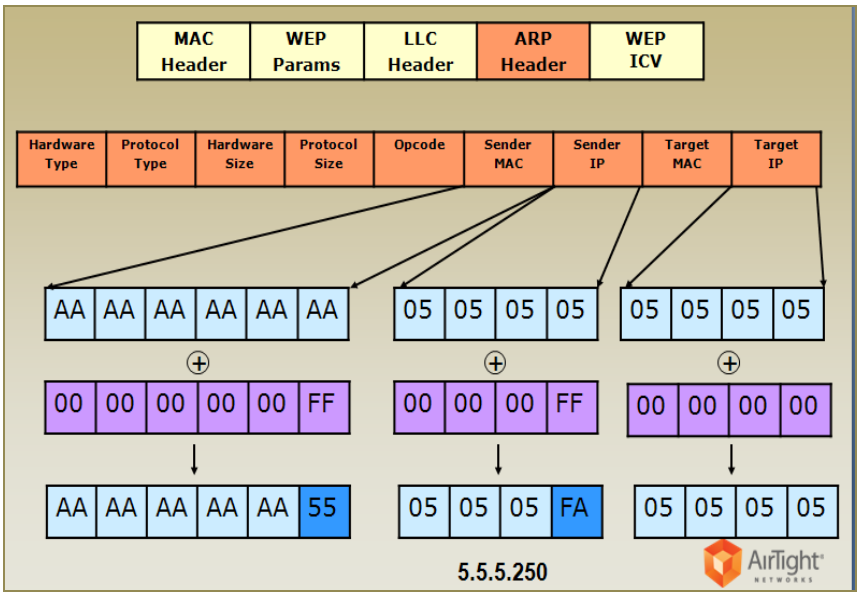
Σύμφωνα με τον Vivek Ramachandran, συγγραφέας της επίθεσης Caffe Latte αποδείχτηκε στο Toorcon, ότι το σπάσιμο του WEP κλειδιού με αυτόν τον τρόπο γίνεται μεταξύ 1, 5 και 6 ημερών, ανάλογα με τη χρήση του πελάτη του DHCP. Αυτό είναι θεωρητικά ενδιαφέρον, αλλά από μικρή πρακτική αξία, δεδομένου ότι μια πραγματική επίθεση hotspot θα πρέπει να ολοκληρωθεί σε μια πολύ μικρότερη χρονική περίοδο, κατά προτίμηση στα λίγα λεπτά που χρειάζεται για να αγοράσει κάποιος ένα εσπρέσο.

5.6.2 Πως λειτουργεί η επίθεση

Ο Ramachandran και ο συνεργάτης του Md Sohail Ahmad αναζήτησαν τρόπους για να κάνουν τον πελάτη πολύ πιο ανθεκτικό. Η δημοσίευση που πραγματοποίησαν στο Toorcon, περιγράφει πολλαπλούς τρόπους για την επιτάχυνση της επίθεσης αυτής. Με την εφαρμογή διαφορετικών τεχνικών WEP cracking (για παράδειγμα FMS, Korek, PTW) και σε διάφορα πλαίσια (όπως DHCP, ARP, 802.11), οι συγγραφείς κατάφεραν να μειώσουν σημαντικά το μέσο όρο του χρόνου που χρειάζεται για να πραγματοποιηθεί η επίθεση. Η χειρότερη περίπτωση διαμόρφωσης (πελάτης με static IP και χωρίς επικύρωση) διήρκεσε περίπου εννέα ώρες, ενώ στην καλύτερη περίπτωση (πελάτης χρησιμοποιεί DHCP και επικύρωση μοιρασμένου κλειδιού) έλαβε μόλις 20 λεπτά. "Αυτό ήταν καλύτερα, αλλά εξακολουθεί να μην είναι αρκετά γρήγορος τρόπος για να είναι μια επίθεση σε καφετέρια", είπε ο Ramachandran.

Στη συνέχεια οι Ramachandran και Ahmad παρατήρησαν ένα θέμα ευπάθειας που θα μπορούσαν να αξιοποιήσουν με μεγαλύτερη συνέπεια για κάθε διαμόρφωση πελάτη. Κάθε σταθμός που λαμβάνει την αίτηση ARP αυτόματα ανταποκρίνεται με μια απάντηση ARP. Οπότε ο εισβολέας θα πρέπει να μπορεί να δημιουργήσει ένα έγκυρο κρυπτογραφημένο αίτημα ARP μην γνωρίζοντας το κλειδί WEP.

Για να το κάνει αυτό ακολουθήται η εξής διαδικασία: Μετά τη σύνδεση, ο πελάτης διαβιβάζει αρκετές κωδικοποιημένες αιτήσεις ARP. Ένας εισβολέας μπορεί να περικόψει μερικά bytes σε ένα από αυτά τα συλλαμβανόμενα πακέτα, η αλλαγή αυτής της άσκοπης ARP σε μια ARP αίτηση, που απευθύνεται προς τον πελάτη. Με την αποστολή αυτής της τροποποιημένης ARP αίτησης, ο πελάτης μπορεί να δεχτεί χιλιάδες απαντήσεις ARP, σωστά κωδικοποιημένων (εικόνα 76).



Εικόνα 76 Τροποποίηση ARP αιτήσεων

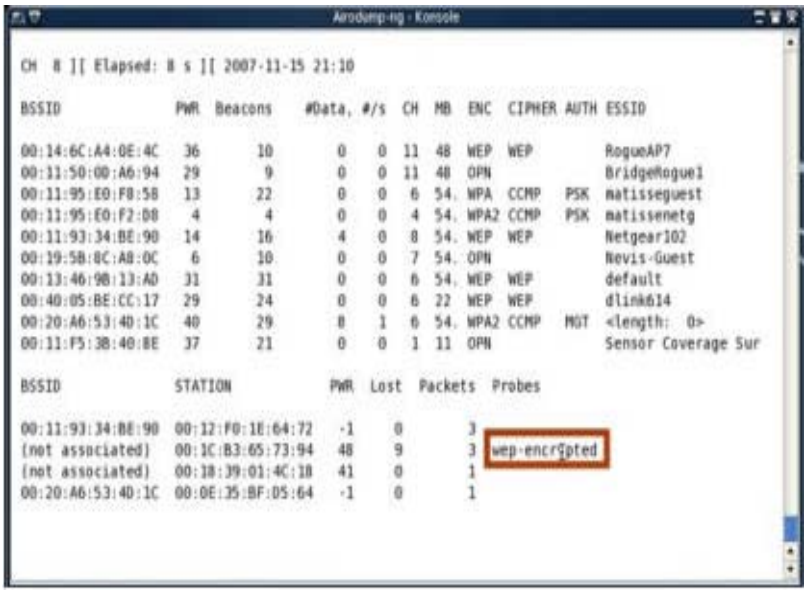
Η τελική έκδοση του εργαλείου Caffe Latte που αναπτύχθηκε από τους Ramachandran και Ahmad, μπορεί να χρησιμοποιήσει αυτήν την σύνθετη

μεθοδολογία για την ανάκτηση της προσωρινής αποθήκευσης 128-bit κλειδιών WEP από κάθε πελάτη σε περίπου έξι λεπτά. Αυτή η επίθεση λειτουργεί, όχι μόνο γιατί το WEP είναι ευάλωτο σε στατιστική ανάλυση, αλλά και γιατί δεν κάνει τίποτα για την προστασία της ακεραιότητας των κρυπτογραφημένων πακέτων. Με άλλα λόγια, οι δικαιούχοι δεν έχουν τρόπο να εντοπίσουν πότε εάν ένα έγκυρο πακέτο έχει συλληφθεί και τροποποιηθεί.

5.6.3 Απόδειξη

Οι Ramachandran και Ahmad απέδειξαν την Café Latte στις 21 Οκτωβρίου 2007, στο Toorcon. Με συνεργάτη το συνάδελφο των Air Tight δικτύων Rick Farina, παρήγαγαν ένα βίντεο πραγματικού χρόνου με το είδος της επίθεσης που ξεκίνησε εναντίον ενός Apple iPhone. Με την άδεια τους έχουν δημοσιευτεί στο διαδίκτυο στιγμιότυπα από αυτού του είδους την επίθεση. Μερικά στιγμιότυπα από την επίθεση παρατίθενται παρακάτω για να μας βοηθήσουν να κατανοήσουμε πως γίνεται αυτού του είδους η επίθεση.

1. Παρακολούθηση της κυκλοφορίας των WLAN hotspot για τον εντοπισμό δυνητικών SSID διαφόρων επιχειρήσεων.

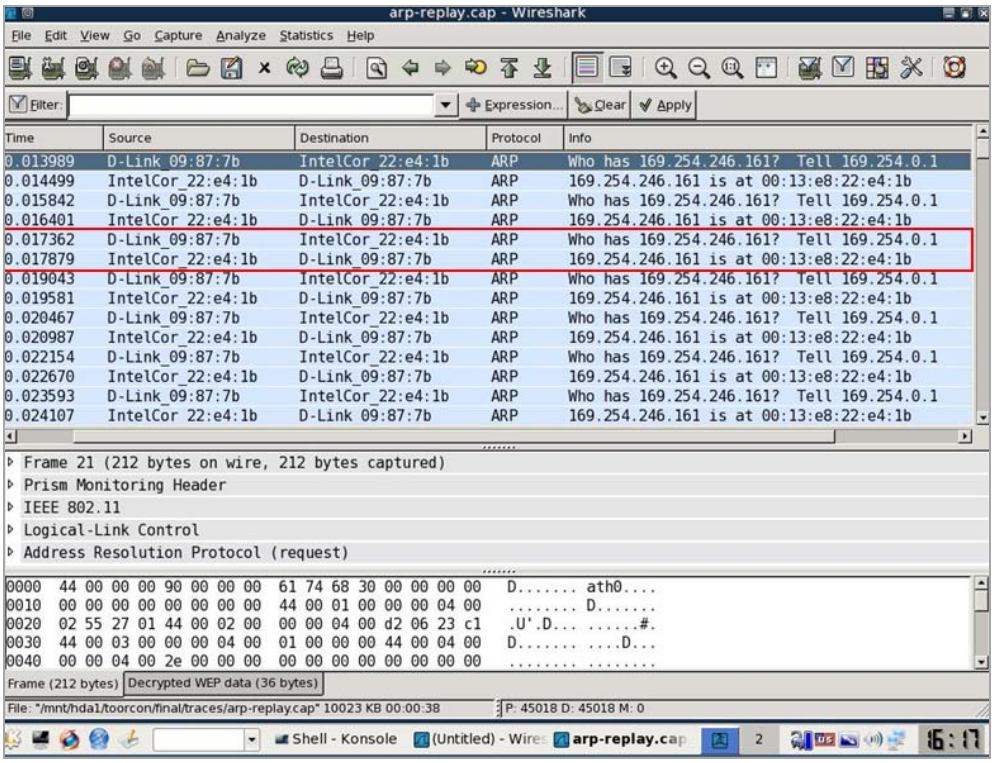


Εικόνα 77 Εντοπισμός των SSID διαφόρων δικτύων

2. Ξεκινάμε τη λήψη της κίνησης που παράγεται από τους πελάτες-στόχους.

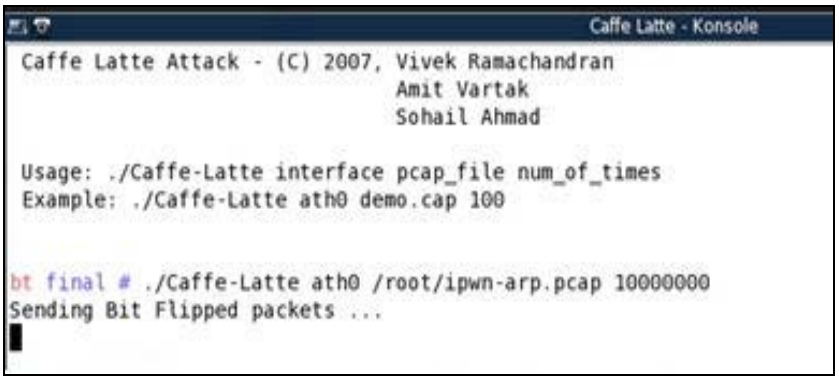
3. Χρησιμοποιούμε ένα ψεύτικο AP με το SSID της εταιρίας που διαλέξαμε και οποιοδήποτε κλειδί WEP για να προσελκύσουμε τους πελάτες-στόχους.

4. Αποσπάμε αιτήματα ARP από το αρχείο καταγραφής (εικόνα 78).



Εικόνα 78 Συλλογή πακέτων ARP

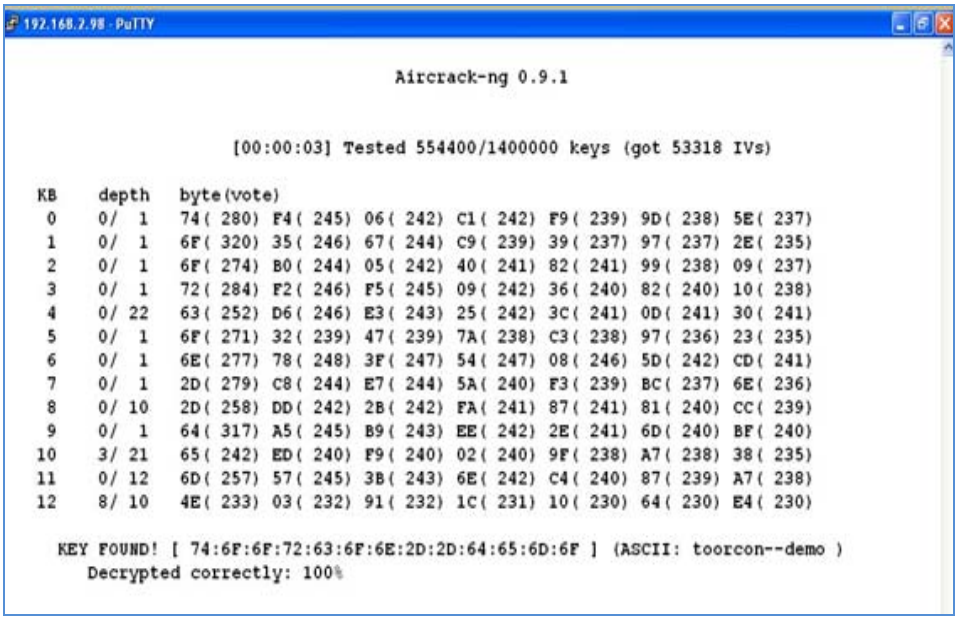
5. Αποστολή ARP αιτήσεων για Caffe-Latte, δημιουργώντας πλημμύρα από bit των ARP αιτήσεων.



Εικόνα 79 Αποστολή τροποποιημένων πακέτων

6. Εκτελούμε το πρόγραμμα aircracker-ng για το συγκεκριμένο SSID και συλλαμβάνουμε το αρχείο.

7. Μετά από την ανάλυση αρκετών ARP απαντήσεων, το πρόγραμμα μας εμφανίζει το 128-bit WEP κλειδί (εικόνα 80).



Εικόνα 80 Αποτελέσματα εύρεσης του WEP κλειδιού

5.6.4 Μέτρα προστασίας

Μετά την παρουσίαση αυτού του είδους της επίθεσης ο Ramachandran δήλωσε " Παρουσιάσαμε αυτού του είδους την επίθεση γιατί θέλαμε να εκπαιδεύσει τους ανθρώπους, αποδεικνύοντας ότι αυτή η απειλή υπάρχει. Όμως δεν θέλαμε να δώσουμε κίνητρο στους hackers. Η καλύτερη άμυνα είναι να σταματήσουμε να χρησιμοποιούμε το WEP".

Αυτή ήταν μια καλή συμβουλή. Για τους εταιρικούς χρήστες, οι αποφάσεις για το κατά πόσον θα χρησιμοποιήσουν WEP γίνονται από τον εργοδότη και όχι τον εργαζόμενο. Οι μεμονωμένοι χρήστες όμως, πρέπει να λαμβάνουν τις ακόλουθες προφυλάξεις για να αποφευχθεί να πέσουν θύματα της Caffe Latte επίθεσης:

- Να απενεργοποιούν τους Wi-Fi προσαρμογείς όταν δεν χρησιμοποιούνται. Πολλοί φορητοί υπολογιστές και άλλες συσκευές έχουν ένα διακόπτη on / off για Wi-Fi, ώστε να ενεργοποιείται και να απενεργοποιείται εύκολα.

- Να επαναρυθμίζουμε τον υπολογιστή μας να αποφεύγει την αυτόματη επανασύνδεση με τα προτεινόμενα δίκτυα. Με αυτόν τον τρόπο, δεν θα παρασυρθεί ο υπολογιστής μας να συνδεθεί σε οποιαδήποτε AP χωρίς τη συγκατάθεσή μας.

- Να εγκαταστήσουμε τις ενημερώσεις για πελάτες ασύρματου δικτύου για εκδόσεις 32-bit των Microsoft Windows XP με Service Pack 2 (KB 917021). Αυτή η ενημερωμένη έκδοση σταματάει τους πελάτες να προσπαθούν να συνδεθούν σε προτεινόμενα δίκτυα που εκπέμπουν το SSIDs τους ακόμα και όταν η επιλογή διαμόρφωσης "Σύνδεση ακόμα και αν το δίκτυο δεν εκπέμπει" είναι απενεργοποιημένη.

Κεφάλαιο 6 Μέθοδοι ασφάλειας

Στα προηγούμενα κεφάλαια είδαμε πως λειτουργούν τα ασύρματα δίκτυα, σε ποια σημεία είναι ευάλωτα, με ποιους τρόπους μπορούν να παραβιαστούν και πως λειτουργεί η διαδικασία της κρυπτογράφησης. Στο κεφάλαιο 5 "Σπάζοντας την ασύρματη ασφάλεια" , εξετάσαμε έγκυρες μεθόδους που ένας εισβολέας μπορεί να χρησιμοποιήσει για να αποκτήσει πρόσβαση σε ασύρματα δίκτυα. Σε αυτό το κεφάλαιο θα συζητήσουμε τρόπους, με τους οποίους τα ασύρματα δίκτυα μπορούν να ρυθμιστούν, ώστε να μειωθεί ο κίνδυνος μιας επιτυχημένης επίθεσης.

Ένας εισβολέας, ο οποίος είναι αποφασισμένος να θέσει το σύστημά μας σε κίνδυνο, σίγουρα θα έχει μια επιτυχημένη προσπάθεια. Σε ένα οικιακό περιβάλλον όμως, είναι σχεδόν απίθανο ότι θα αντιμετωπίσουμε αυτό το είδος του εισβολέα, αλλά για προληπτικά μέτρα, τα βήματα που παρουσιάζονται σε αυτό το κεφάλαιο, έχουν σχεδιαστεί για να μειώσουν τον κίνδυνο να καταστούμε στόχος ευκολίας. Το κεφάλαιο αυτό εξετάζει το πώς να ρυθμίσουμε τις βασικές ρυθμίσεις ασφαλείας στο σημείο πρόσβασης που χρησιμοποιούμε. Υπάρχουν πολύ απλά βήματα που είναι επαρκής για τους χρήστες στο σπίτι, όπως:

- Χρησιμοποίηση μοναδικού SSID (Service Set Identifier)
- Απενεργοποίηση της SSID εκπομπής
- MAC Filtering
- Χρησιμοποίηση End-to-end encryption
- Χρήση VPNs
- Access control
- Intrusion detection systems

Στις επόμενες παραγράφους που ακολουθούν αναλύουμε διεξοδικά κάθε ένα από αυτά τα βήματα, ώστε να μπορούμε να στήσουμε ένα ασφαλές ασύρματο δίκτυο. Δεν μπορούμε να χρησιμοποιήσουμε το υψηλότερο επίπεδο κρυπτογράφησης εκτός και αν το ρυθμίσουμε, οπότε ας το ρυθμίσουμε!

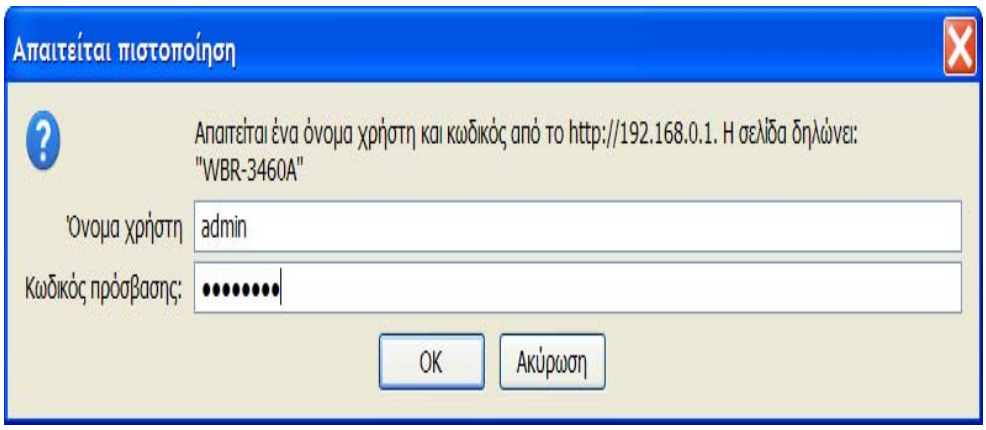
6.1 Access Control

Σύμφωνα με τον όμιλο ασφάλειας πληροφοριακών συστημάτων (ISSA) "έλεγχος πρόσβασης είναι μια συλλογή από μηχανισμούς για περιορισμένη και ελεγχόμενη πρόσβαση συστήματος για να συγκεντρώσουμε πληροφορίες ή χαρακτηρίστηκα που βασίζονται στην αναγνώριση του χρήστη ή των διαφόρων μελών που ανήκουν σε ένα γκρουπ.

Πρώτα από όλα πρέπει να αλλάξουμε το username και password που απαιτείται για να αποκτήσουμε πρόσβαση στην οθόνη με τις ρυθμίσεις διαμόρφωσης του ασύρματου δρομολογητή που χρησιμοποιούμε. Οι περισσότεροι ασύρματοι δρομολογητές που χρησιμοποιούμε για οικιακή χρήση, αποτελούνται από μια διεπαφή διαχείρισης μέσω του web. Η προεπιλεγμένη IP διεύθυνση της συσκευής που χρησιμοποιείται στο εσωτερικό δίκτυο είναι σχεδόν πάντα 192.168.0.1. Το να

ανακαλύψουμε πιο είναι το προεπιλεγμένο username και password για τον κάθε κατασκευαστή δεν είναι πολύ δύσκολο.

Ο εξοπλισμός συνήθως είναι ρυθμισμένος με κάτι σαν "admin" για username και "password" για το password (εικόνα 81). Ακόμα και χωρίς καμιά βασική γνώση για τον κατασκευαστή ή την συσκευή, ένας επιτιθέμενος μπορεί να ανακαλύψει στα τυφλά το username και το password σε λιγότερο από δέκα προσπάθειες. Με την προεπιλεγμένη IP διεύθυνση και τα προεπιλεγμένα username και password διαχείρισης, ο ασύρματος δρομολογητής μας μπορεί να υποκλαπεί ακόμα και από αρχάριους.

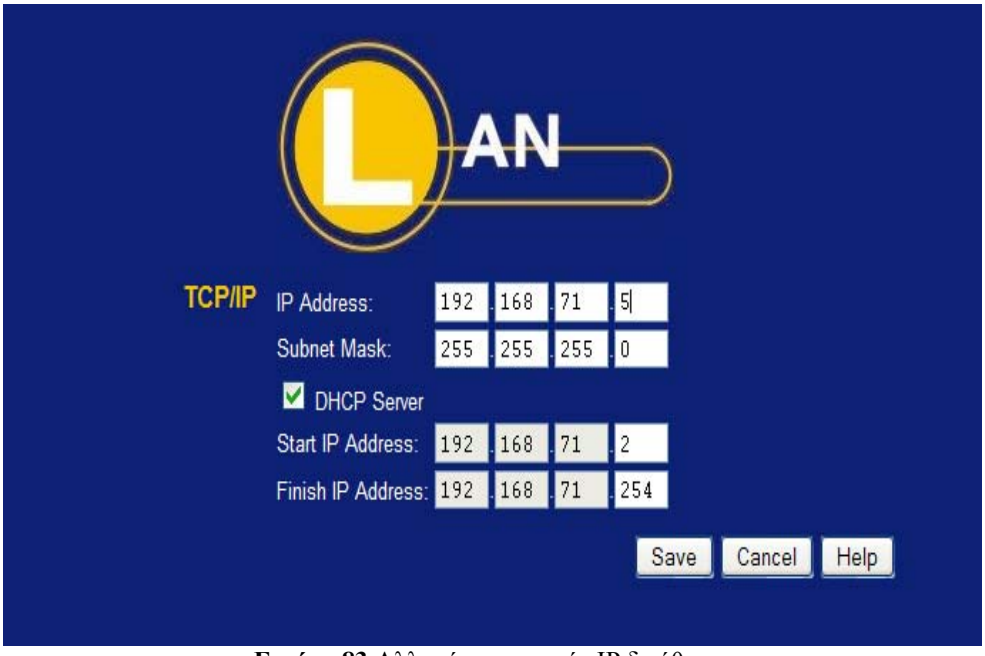


Εικόνα 81 Πρόσβαση στον ασύρματο δρομολογητή

Βεβαιωθείτε ότι αλλάξατε το username σε κάτι που μόνο εσείς θα μπορούσατε να σκεφτείτε. Μετονομάζοντας τον λογαριασμό του διαχειριστή στον υπολογιστή μας, πρέπει να διαλέξουμε ένα username που δεν θα είναι τόσο εύκολο να το μαντέψει κάποιος όπως είναι το "admin" ή οποιοδήποτε άλλο προεπιλεγμένο username ήταν. Στη συνέχεια χρειάζεται να διαλέξουμε ένα ισχυρό password το οποίο δεν θα είναι εύκολο να μαντεύσει κάποιος ή να το σπάσει. Ο δρομολογητής που εμείς χρησιμοποιούμε, μας δίνει την δυνατότητα να αλλάξουμε μόνο το password.

Εικόνα 82 Αλλαγή password του router

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



Εικόνα 83 Αλλαγή εσωτερικής IP διεύθυνσης

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

6.2 Intrusion Detection

Η ανίχνευση εισβολής (ID) αποτελείται από μια ποικιλία κατηγοριών και τεχνικών. Οι βασικές προσεγγίσεις περιλαμβάνουν τον καθορισμό ενός συστήματος, εάν αυτό έχει προσβληθεί από ιούς ή από κακόβουλο κώδικα και εφαρμόζουν μεθόδους ώστε να καθαρίσουν την εισβολή στο δίκτυο από τον επιτιθέμενο. Η σάρωση για ανίχνευση ιών και η πρόληψη εισβολής, χρησιμοποιούνται για να αντιμετωπίζουν τα προβλήματα των ιών και οι μηχανισμοί ανίχνευσης εισβολής και αντιμετώπιση, στοχεύουν τις εισβολές των δικτύων.

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

- Τη δημιουργία και συντήρηση των συστημάτων ανίχνευσης εισβολής (IDSs), διαδικασίες παρακολούθησης των δικτύων και των hosts και επισήμανση των περιστατικών.

- Τη δημιουργία μιας ομάδας για την αντιμετώπιση εισβολών σε υπολογιστή, για την ανάλυση της επισήμανσης ενός περιστατικού, την αντιμετώπιση σε ένα περιστατικό, αν η ανάλυση το επιβάλει και διαδικασίες κλιμακωτών μονοπατιών.

6.2.1 Επισκόπηση των IDSs

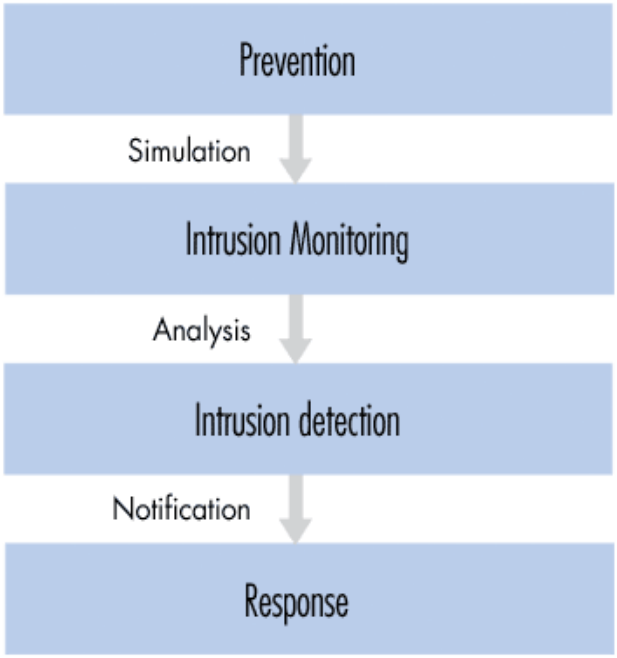
Με λίγα λόγια τα συστήματα ανίχνευσης εισβολής κάνουν αυτό που λέει το όνομά τους: εντοπίζουν πιθανές διεισδύσεις. Πιο συγκεκριμένα τα εργαλεία IDS, αποσκοπούν στην ανίχνευση επιθέσεων κατά του υπολογιστή ή την κακή χρήση του υπολογιστή ή ειδοποιούν τα αρμόδια άτομα όταν ανιχνεύουν κάτι περίεργο. Η εγκατάσταση ενός IDS σε ένα δίκτυο παρέχει το ίδιο αποτέλεσμα με την εγκατάσταση ενός συναγερμού σε ένα σπίτι. Με διάφορες μεθόδους και τα δύο ανιχνεύουν την παρουσία ενός εισβολέα/διαρρήκτη και τα δύο στη συνέχεια εκδίδουν κάποιο είδος προειδοποίησης και συναγερμού.

Παρόλο που τα IDSs μπορούν να συνδυαστούν και να χρησιμοποιηθούν με τα τείχη προστασίας (firewalls), τα οποία αποσκοπούν στη ρύθμιση και τον έλεγχο της ροής των πληροφοριών από και προς ένα δίκτυο, τα δύο αυτά εργαλεία δεν πρέπει να συγχέονται. Χρησιμοποιώντας το προηγούμενο παράδειγμα, τα firewalls μπορούν να θεωρηθούν ως ένας φράχτης ή ένας φύλακας τοποθετημένος μπροστά από ένα σπίτι. Προστατεύουν δηλαδή το δίκτυο και προσπαθούν για την πρόληψη των παρεμβολών, ενώ τα εργαλεία IDS ανιχνεύουν εάν το δίκτυο είναι ή όχι υπό επίθεση ή αν στην πραγματικότητα έχει παραβιαστεί.

Έτσι τα IDS εργαλεία αποτελούν αναπόσπαστο μέρος της λεπτομερούς και πλήρης ασφάλειας του συστήματος. Δεν εγγυάται πλήρως την ασφάλεια αλλά όταν συνδυαστεί με την πολιτική ασφαλείας τρωτών σημείων, την κρυπτογράφηση δεδομένων, την ταυτοποίηση του χρήστη, τον έλεγχο πρόσβασης και τα τείχη προστασίας, μπορούν να ενισχύσουν σημαντικά την ασφάλεια του δικτύου.

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

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



Εικόνα 84 Ενέργειες των Intrusion Detection Systems

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

6.2.2 Host-based IDS

Τα host-based IDSs ψάχνουν για είδη εισβολής στο τοπικό σύστημα του host. Χρησιμοποιούν συχνά το μηχανισμό ελέγχου και καταγραφής τοθ host σαν πηγή πληροφοριών για ανάλυση. Πιο συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα, που περιορίζεται στον τοπικό host όπως logins, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές σε δικαιώματα του συστήματος. Η συγκεκριμένη αρχιτεκτονική χρησιμοποιεί μηχανισμούς βασισμένους σε κανόνες για την ανάλυση της δραστηριότητας. Για παράδειγμα ένας τέτοιος κανόνας μπορεί να είναι ο εξής: δυνατότητα για πρόσβαση στο λογαριασμό του διαχειριστή είναι δυνατή μόνο μέσω της εντολής su. Συνεπώς επιτυχημένες προσπάθειες πρόσβασης στο λογαριασμό του διαχειριστή θα μπορούσαν να θεωρηθούν ως επίθεση.

Πλεονεκτήματα

1. Ένα host-based IDS μπορεί να αποτελέσει πολύ δυνατό εργαλείο ανάλυσης πιθανών επιθέσεων. Για παράδειγμα, είναι σε θέση αρκετές φορές να πει τι ακριβώς έκανε ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιες ρουτίνες του συστήματος κάλεσε αντί για μια αόριστη υπόθεση ότι

προσπάθησε να εκτελέσει μια επικίνδυνη εντολή. Άρα τα host-based IDS συνήθως παρέχουν πολύ πιο λεπτομερής και σχετικές πληροφορίες από ότι τα network-based IDS.

2. Τα host-based IDSs έχουν μικρότερους false positive ρυθμούς από ότι τα network-based. Αυτό συμβαίνει γιατί το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο host είναι πολύ πιο εστιασμένο, παρά τα είδη κίνησης πακέτων που ρέουν σε ένα δίκτυο. Αυτή η ιδιότητα μπορεί να μειώσει την πολυπλοκότητα των host-based μηχανισμών.

3. Μπορούν να χρησιμοποιηθούν σε περιβάλλοντα που δεν χρειάζεται πλήρης ανίχνευση εισβολών ή όταν δεν υπάρχει διαθέσιμο bandwidth για επικοινωνία αισθητήρα-σταθμού ανάλυσης. Τα host-based IDSs είναι πλήρως αυτό-συντηρούμενα, κάτι που τους επιτρέπει σε κάποιες περιπτώσεις να εκτελούνται από read-only μέσα. Έτσι οι εισβολείς μπορούν δύσκολα να εξουδετερώσουν το IDS.

4. Τέλος σε ένα host-based IDS είναι ευκολότερο να σχηματιστεί μια ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή το logging off ενός επιτιθέμενου χρήστη.

Μειονεκτήματα

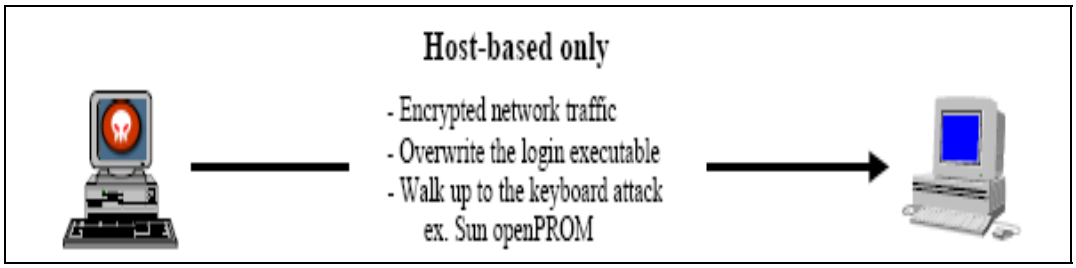
1. Τα host-based IDSs απαιτούν εγκατάσταση στο σύστημα που θέλουμε να προστατεύσουμε. Αν για παράδειγμα έχουμε ένα server που πρέπει να τον προστατεύσουμε, θα πρέπει να εγκαταστήσουμε το IDS στον server αυτόν. Όπως αναφέρθηκε και παραπάνω, αυτό μπορεί να προκαλέσει προβλήματα χωρητικότητας. Σε μερικές περιπτώσεις μπορεί να προκαλέσει και προβλήματα ασφάλειας μιας και το προσωπικό που είναι υπεύθυνο για την ασφάλεια του συστήματος ίσως να μην έχει πρόσβαση στον server όταν χρειαστεί.

2. Ένα άλλο πρόβλημα είναι ότι έχουν την τάση να εξαρτώνται από το υπάρχον σύστημα καταγραφής και ελέγχου του server. Εάν ο server δεν λειτουργεί έτσι ώστε η καταγραφή και ο έλεγχος να είναι σε ικανοποιητικό επίπεδο, θα πρέπει να γίνει αλλαγή στις ρυθμίσεις του. Αυτό αποτελεί τεράστιο πρόβλημα αλλαγής στη διαχείριση του server.

3. Αυτά τα συστήματα είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την δυνατότητα να προστατέψουν ολόκληρα δικτυακά τμήματα με τη χρήση host-based IDSs. Αντίθετα θα πρέπει να επιλέξουν ποια συστήματα θα πρέπει να προστατεύσουν και ποια όχι. Αυτό το γεγονός αφήνει μεγάλα κενά στην κάλυψη της ανίχνευσης εισβολών στο δίκτυο, αφού ένας εισβολέας σε ένα γειτονικό αλλά απροστάτευτο σύστημα μπορεί να υποκλέψει πληροφορίες ή οποιοδήποτε άλλο πολύτιμο υλικό από το δίκτυο.

4. Τέλος τα host-based IDSs είναι πιο ευάλωτα σε μεγαλύτερο βαθμό από τοπικούς περιορισμούς. Αγνοούν εντελώς το περιβάλλον του δικτύου, άρα ο

χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των host που προστατεύονται.

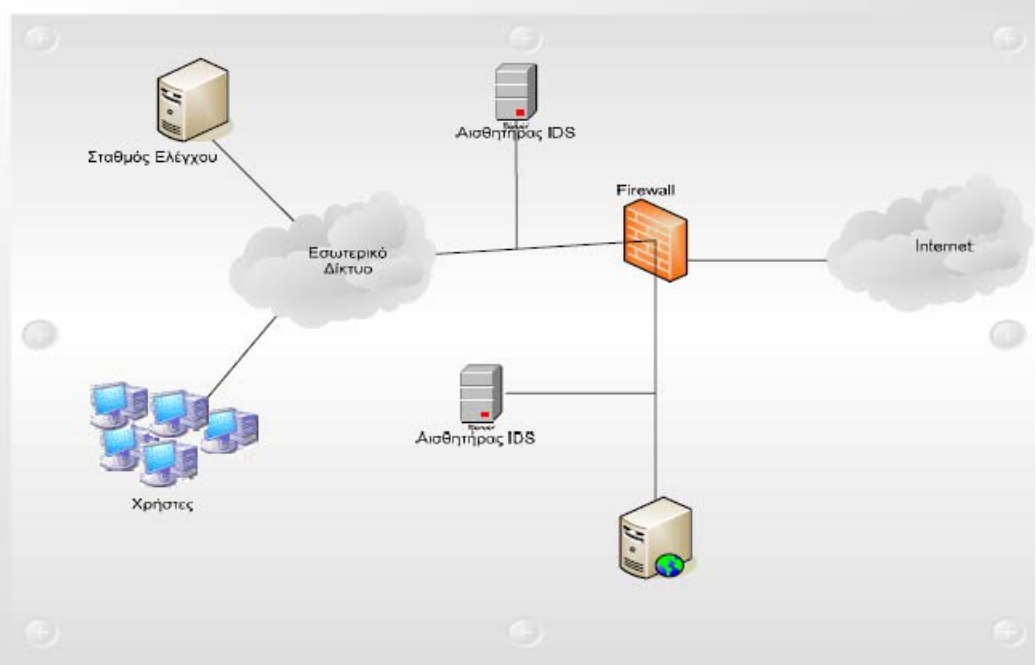


Εικόνα 85 Λειτουργίες των host-based IDS

6.2.3 Network-based IDS

Τα network-based IDSs συλλαμβάνουν την κίνηση του δικτύου (συνήθως ή σε ολόκληρο το δίκτυο ή σε μικρά τμήματα σε αυτό) για τις λειτουργίες ανίχνευσης εισβολής. Το network-based IDS συνήθως αποτελείται από δύο μέρη: τους αισθητήρες και τον σταθμό διαχείρισης /ανάλυσης. Ο αισθητήρας βρίσκεται σε ένα τομέα του δικτύου και παρακολουθεί για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον διαχειριστή του συστήματος δηλαδή στον διαχειριστή ασφάλειας του δικτύου.

Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα. Δηλαδή λαμβάνουν όλη τη δικτυακή κίνηση και όχι μόνο ότι προορίζεται για τη δικιά τους IP διεύθυνση, αλλά και την κίνηση που διέρχεται από αυτούς, με σκοπό την περαιτέρω ανάλυση. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στο σταθμό διαχείρισης/ανάλυσης. Ο σταθμός διαχείρισης/ανάλυσης, μπορεί να δείξει τα σήματα κινδύνου που έλαβε από τους αισθητήρες ή να διεξάγει περαιτέρω ανάλυση.



Εικόνα 86 Διάταξη Network-Based IDS

Πλεονεκτήματα

1. Τα συστήματα ανίχνευσης επιθέσεων μπορούν να ανιχνεύσουν κάποιες από

τις επιθέσεις που χρησιμοποιούν το δίκτυο. Είναι επαρκή για την ανίχνευση πρόσβασης.

2. Τα Network – Based IDSs έχουν την τάση να είναι καλύτερα αυτοσυντηρούμενα από ότι τα host-based. Τρέχουν σε ένα συγκεκριμένο σύστημα και η εγκατάσταση τους είναι απλή και πραγματοποιείται σε μια τοποθεσία στο δίκτυο, που δίνει τη δυνατότητα παρακολούθησης ευαίσθητης κίνησης δεδομένων, χωρίς εξουσιοδότηση.

3. Ένα Network – Based IDSs, δεν απαιτεί μετατροπές στους servers μιας επιχείρησης ή στους hosts για να εγκατασταθεί. Αυτό είναι μεγάλο όφελος γιατί συνήθως οι servers έχουν κλειστές ανοχές όσον αφορά τη CPU, το I/O και τη χωρητικότητα του δίσκου. Η εγκατάσταση επιπλέον λογισμικού ίσως δημιουργήσει προβλήματα λειτουργικότητας.

4. Τα Network – Based IDSs, δεν αποτελούν κρίσιμο παράγοντα για τη λειτουργικότητα του δικτύου και αυτό γιατί δεν λειτουργεί ως δρομολογητής ή ως κάποια άλλη κρίσιμη συσκευή. Άρα τυχόν αποτυχία στο σύστημα του IDS δεν θα έχει σημαντική επίδραση στην επιχείρηση.

Μειονεκτήματα

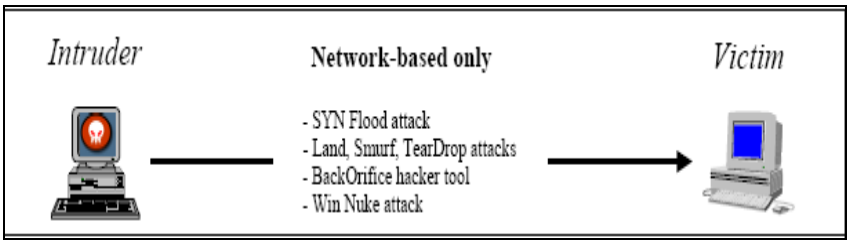
1. Ένα Network – Based IDSs, απλά εξετάζει τη δικτυακή κίνηση στον τομέα που είναι συνδεδεμένο και μόνο. Δεν μπορεί να ανιχνεύσει μια επίθεση που

γίνεται σε διαφορετικό τμήμα του δικτύου. Το πρόβλημα αυτό γίνεται μεγαλύτερο σε ένα περιβάλλον με πολλαπλές δικτυώσεις Ethernet. Για να καλύψει τις ανάγκες του σε δικτυακή κάλυψη ένας μεγάλος οργανισμός θα πρέπει να αγοράσει πολλούς αισθητήρες, κάτι που σημαίνει επιπλέον κόστος.

2. Τα Network – Based IDSs, συνήθως χρησιμοποιούν ανάλυση υπογραφών για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι ανιχνεύονται κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αυτή η μέθοδος δεν είναι επαρκής για τα πιο πολύπλοκα είδη επιθέσεων. Αυτές απαιτούν καλύτερη ικανότητα για ανάλυση του περιβάλλοντος.

3. Ένα τέτοιου είδους σύστημα ανίχνευσης επιθέσεων μπορεί να χρειαστεί να μεταδώσει μεγάλες ποσότητες δεδομένων στο κεντρικό σύστημα ανάλυσης. Κάποιες φορές, οποιοδήποτε αναλυόμενο πακέτο, παράγει μια μεγαλύτερη ποσότητα κίνησης δεδομένων. Πολλά τέτοια συστήματα χρησιμοποιούν επιθετικές μεθόδους ελάττωσης δεδομένων για να μειώσουν την παραγόμενη κίνηση επικοινωνίας.

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



Εικόνα 87 Λειτουργίες των network-based IDS

6.2.4 Signature-based IDS

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

Μια αδυναμία των Signature-based IDSs είναι ότι αποτυγχάνουν να χαρακτηρίζουν τις αργές επιθέσεις και οι οποίες διαρκούν μεγάλο διάστημα. Για να ανιχνευτούν τέτοιου είδους επιθέσεις χρειάζεται να δεσμευτούν μεγάλα ποσοστά πληροφορίας για μεγάλο χρονικό διάστημα. Μια άλλη ευπάθεια των Signature-based IDSs είναι ότι

ανιχνεύονται μόνο οι επιθέσεις των οποίων οι υπογραφές έχουν αποθηκευτεί στη βάση δεδομένων. Επιπλέον μειονέκτημα των Signature-based IDSs είναι ότι η βάση δεδομένων χρειάζεται συχνά συντήρηση και αναβάθμιση σχετικά με τις νέες απειλές που κυκλοφορούν ώστε να παραμένει ενήμερη.

6.2.5 Statistical anomaly based IDS

Τα Statistical anomaly ή Behavior-based IDSs ανιχνεύουν δυναμικά αποκλίσεις από τον κανονικό τρόπο συμπεριφοράς των χρηστών και κρούουν συναγερμό όταν μια λανθασμένη δραστηριότητα συμβαίνει. Τα Behavior-based IDSs μαθαίνουν την κανονική ή την αναμενόμενη συμπεριφορά που πρέπει να έχουν οι χρήστες και αναλαμβάνουν να ανιχνεύσουν οποιαδήποτε διείσδυση συμβεί, παρατηρώντας τις αποκλίσεις του συστήματος από το κανονικό τρόπο.

Με αυτόν τον τρόπο, το IDSs αποκτά τα δεδομένα και ορίζει ένα προφίλ "κανονικής" χρήσης του δικτύου ή του host που παρακολουθείται. Αυτή η κατηγοριοποίηση γίνεται με στατιστικά δείγματα που λαμβάνονται κατά τη διάρκεια μιας συνηθισμένης χρησιμοποίησης του συστήματος. Οι τυπικές πληροφορίες χαρακτηριστικών χρησιμοποιούνται για να εγκαθιδρυθεί ένα κανονικό προφίλ που περιλαμβάνει την χρησιμοποίηση μνήμης, τη χρησιμοποίηση της CPU και τα είδη των πακέτων του δικτύου. Με αυτήν τη προσέγγιση οι νέες επιθέσεις μπορούν να ανιχνευτούν γιατί προκαλούν περίεργα στατιστικά του συστήματος.

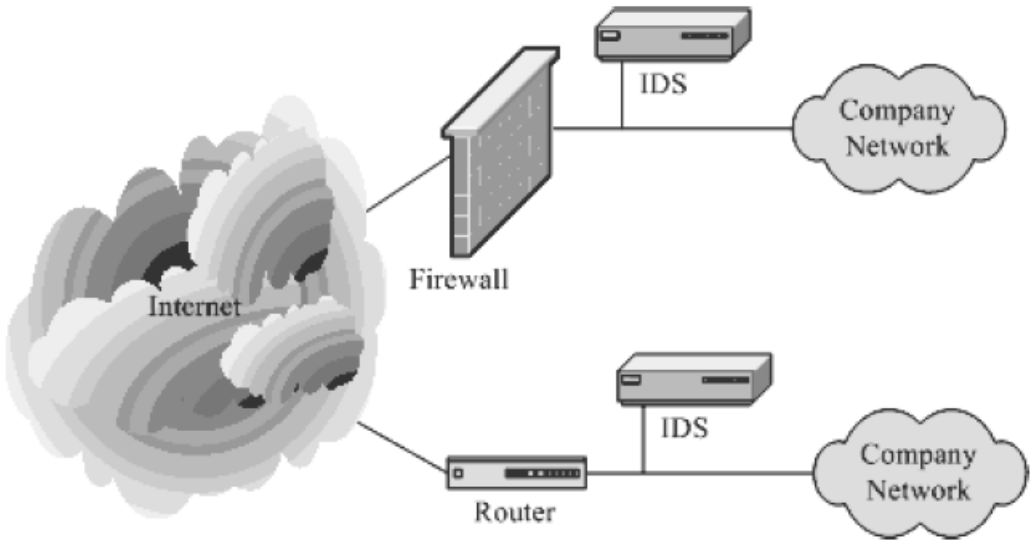
Τα πλεονεκτήματα των Behavior-based IDSs είναι τα επόμενα: το σύστημα μπορεί δυναμικά να προσαρμοστεί σε καινούριες επιθέσεις, δεν εξαρτώνται από συγκεκριμένα λειτουργικά συστήματα όπως τα knowledge-based IDSs και βοηθούν να ανιχνευτούν διάφορα είδη επιθέσεων, τα οποία δεν περιλαμβάνουν μόνο επιθέσεις ασφαλείας. Αντίθετα μερικά μειονεκτήματα των Behavior-based IDSs είναι ότι δεν ανιχνεύουν επιθέσεις που δεν αλλάζουν σημαντικά τα χαρακτηριστικά του συστήματος και μερικές φορές ίσως ανιχνεύουν κατά λάθος περιστατικά που δεν είναι επιθέσεις αλλά προκαλούν στιγμιαία μεταβολή στο σύστημα.

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

Το που θα τοποθετήσουμε ένα IDS στο δίκτυό μας, εξαρτάται από την τοπολογία του δικτύου μας. Μπορεί να θέλουμε να τοποθετήσουμε ένα IDS σε ένα σημείο του δικτύου αλλά μπορούμε να χρησιμοποιήσουμε και περισσότερα σε διάφορα σημεία του δικτύου. Επίσης εξαρτάται από το είδος των δραστηριοτήτων εισβολής που θέλουμε να ανιχνεύσουμε: τις εσωτερικές, εξωτερικές ή και τις δύο. Για παράδειγμα αν θέλουμε να ανιχνεύουμε μόνο τις εξωτερικές εισβολές διείσδυσης στο σύστημά μας, και αν έχουμε μόνο ένα δρομολογητή να συνδέεται στο internet, το καλύτερο μέρος για να τοποθετήσουμε ένα IDS είναι μέσα στο δρομολογητή ή το τοίχος προστασίας που χρησιμοποιούμε. Αν όμως έχουμε πολλαπλά μονοπάτια για τη

σύνδεση μας στο internet, χρειάζεται να τοποθετήσουμε ένα IDS, σε κάθε ένα σημείο εισόδου.

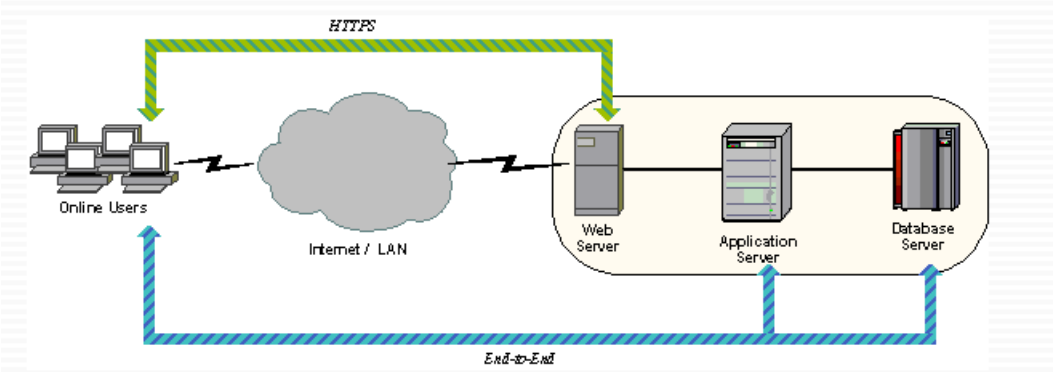
Ωστόσο, αν θέλουμε να ανιχνεύσουμε τις εσωτερικές εισβολές, θα πρέπει να τοποθετήσουμε και από ένα IDS σε κάθε τμήμα του δικτύου. Σε πολλές περιπτώσεις όμως δεν χρειάζεται να έχουμε δραστηριότητα ανίχνευσης εισβολών σε όλα τα τμήματα του δικτύου και θα πρέπει να την περιορίζουμε μόνο στις ευαίσθητες περιοχές. Να θυμόμαστε ότι περισσότερα συστήματα ανίχνευσης εισβολών, απαιτούν περισσότερη δουλεία και περισσότερο κόστος συντήρησης. Η απόφαση μας όμως πραγματικά εξαρτάται από τη γενική πολιτική ασφάλειας που χρησιμοποιούμε για να προστατευτούμε από τους εισβολείς. Στην εικόνα 84, φαίνονται τα τυπικά μέρη που μπορούμε να τοποθετήσουμε ένα σύστημα ανίχνευσης εισβολής.



Εικόνα 88 Τα τυπικά μέρη που μπορούμε να τοποθετήσουμε IDS

6.3 End-to-End Encryption

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



Εικόνα 89 Απεικόνιση της end-to-end encryption

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

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

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

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

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

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

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

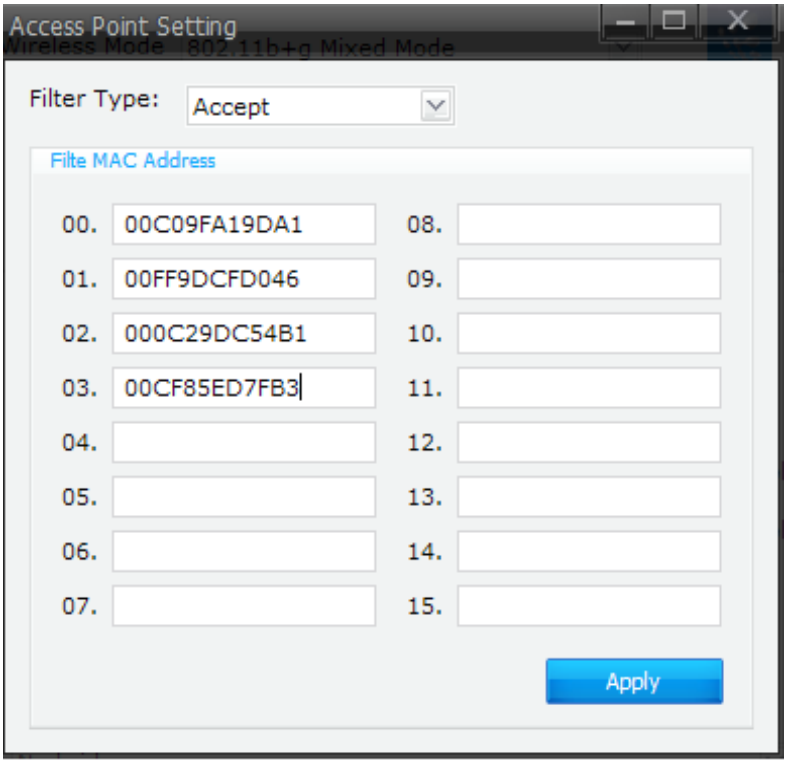
Link encryption	**End-to-end encryption**
Ασφάλεια μεταξύ των ακραίων και των ενδιάμεσων συστημάτων	
Το μήνυμα εκτίθεται στον host που αποστέλλεται	Το μήνυμα κρυπτογραφείται στον host που αποστέλλεται
Το μήνυμα εκτίθεται στους ενδιάμεσους κόμβους	Το μήνυμα κρυπτογραφείται στους ενδιάμεσους κόμβους
Ρόλος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

Πίνακας 3 Χαρακτηριστικά της Link και της end-to-end κρυπτογράφησης

6.4 MAC Filtering

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

Χρησιμοποιούμε την διεύθυνση MAC για να περιορίσουμε την πρόσβαση που βασίζεται στις λίστες ελέγχου πρόσβασης MAC (ACLs), οι οποίες είναι αποθηκευμένες και διανεμημένες σε πολλά σημεία πρόσβασης. Ωστόσο μερικά άλλα σημεία πρόσβασης έχουν την ικανότητα να φιλτράρουν μόνο έμπιστες διευθύνσεις MAC. Το φιλτράρισμα της διεύθυνσης MAC αποδέχεται ή απορρίπτει την πρόσβαση σε ένα υπολογιστή χρησιμοποιώντας τη λίστα από τις επιτρεπτές διευθύνσεις MAC. Όπως βλέπουμε στην εικόνα 90, σε πολλά σημεία πρόσβασης, υπάρχει επιλογή MAC Filtering, την επιλέγουμε, την ενεργοποιούμε τσεκάροντας το κουτάκι enabled και στη συνέχεια προσθέτουμε μόνο τις διευθύνσεις των πελατών που επιτρέπεται να έχουν πρόσβαση στο σύστημά μας.



Εικόνα 90 Ρύθμιση του σημείου πρόσβασης για MAC Filtering

Για να εγκαθιδρύσουμε MAC Address Filtering, σαν διαχειριστές του WLAN μας, θα πρέπει να διαμορφώσουμε μια λίστα από πελάτες, στους οποίους θα επιτρέπεται η

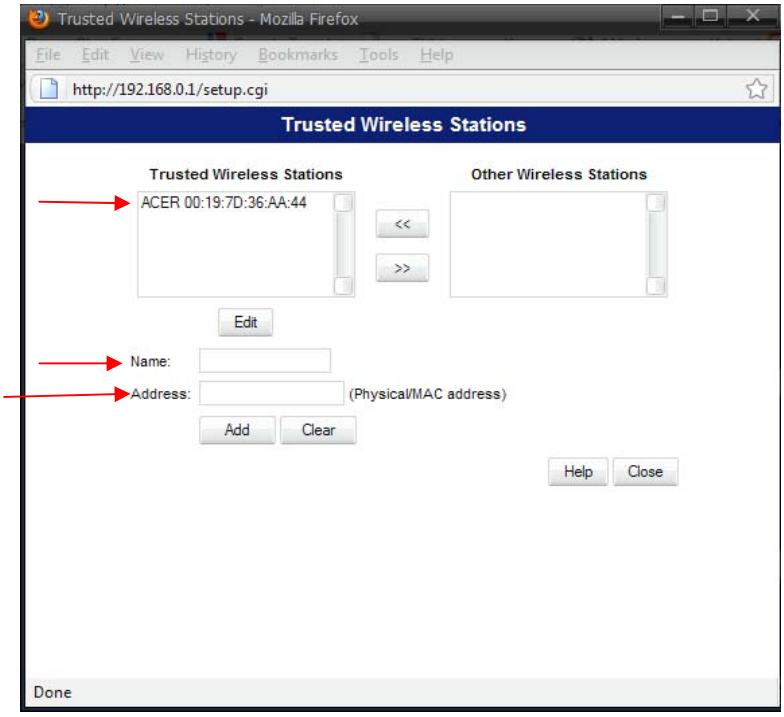
πρόσβαση στο ασύρματο δίκτυο μας. Πρώτα μπαίνουν οι MAC διευθύνσεις των λειτουργικών συστημάτων των πελατών και στη συνέχεια μπαίνουν εκείνες οι διευθύνσεις των ασύρματων σημείων πρόσβασης ή των δρομολογητών που χρησιμοποιούνται για να έχουμε πρόσβαση στην οθόνη με τις ρυθμίσεις τους. Τέλος ενεργοποιούμε την επιλογή του φιλτραρίσματος.

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

Στις παρακάτω εικόνες (εικόνα91 και εικόνα 92) φαίνεται πως ρυθμίζουμε το MAC Filtering στο σημείο πρόσβασης που χρησιμοποιούμε. Η ονομασία που δίνει το συγκεκριμένο σημείο πρόσβασης για το MAC Filtering είναι «*Trusted Wireless Stations*». Στην ετικέτα **Access Point,** τσεκάρουμε την επιλογή **Trusted Wireless stations only** και επιλέγουμε **Set Stations** για να ρυθμίσουμε τους σταθμούς που θέλουμε να έχουν πρόσβαση στο WLAN μας.

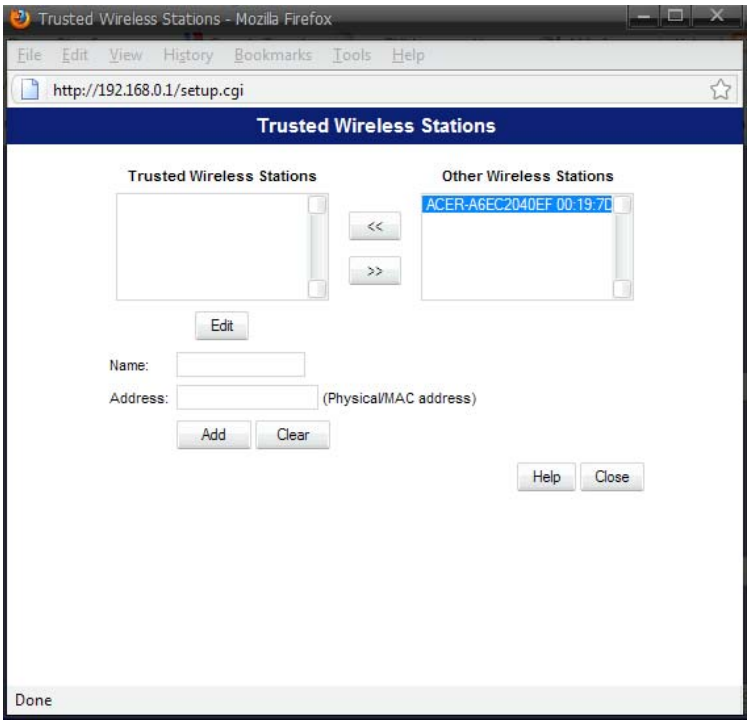
Εικόνα 91 Ρύθμιση σημείου πρόσβασης άλλου κατασκευαστή για MAC Filtering

Επιλέγουμε τους υπολογιστές που θέλουμε να έχουν πρόσβαση στο WLAN μας, γράφοντας το όνομα τους για να τους ξεχωρίζουμε και τη διεύθυνση MAC τους και πατώντας **add** τους προσθέτουμε στη λίστα με τους έμπιστους σταθμούς που θέλουμε να έχουν πρόσβαση στο WLAN μας (εικόνα 92).

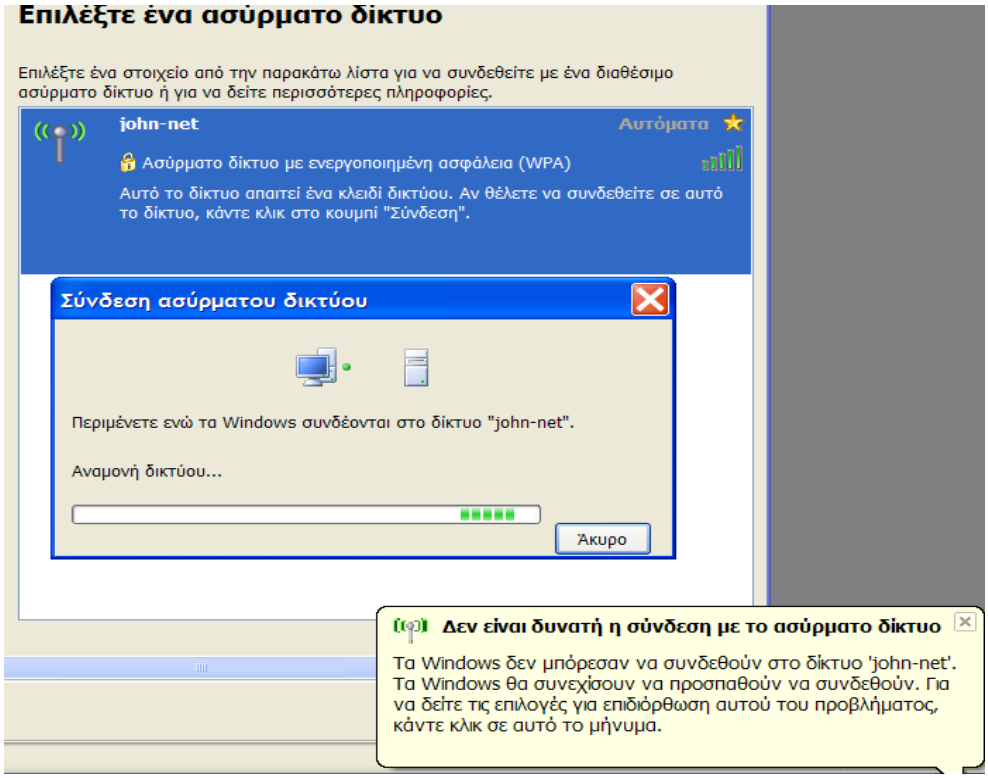


Εικόνα 92 Επιλογή συγκεκριμένων MAC διευθύνσεων

Αν τώρα η MAC διεύθυνση του υπολογιστή μας δεν είναι στην λίστα με τις έμπιστες διευθύνσεις αλλά είναι στη λίστα με τους άλλους σταθμούς (εικόνα 93) ή μπορεί και να μην είναι καθόλου στη λίστα, βλέπουμε ότι το σημείο πρόσβασης δεν επιτρέπει στον υπολογιστή μας να συνδεθεί στο συγκεκριμένο WLAN (εικόνα94).



Εικόνα 93 Μη αξιόπιστες διευθύνσεις MAC



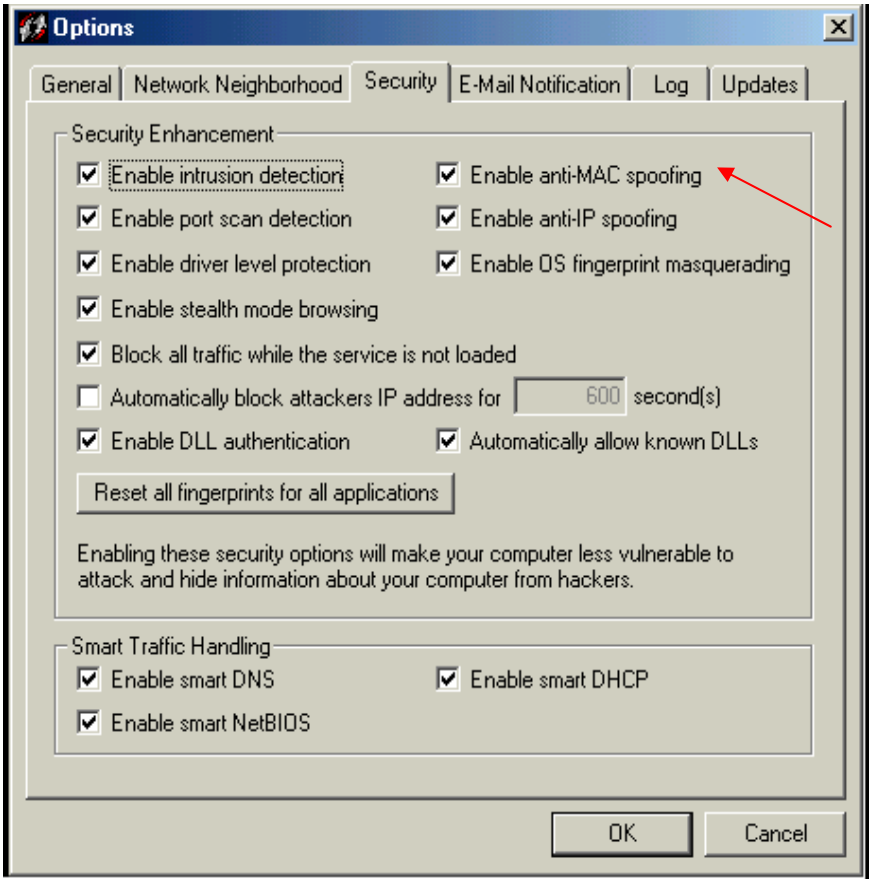
Εικόνα 94 Απόρριψη σύνδεσης στο συγκεκριμένο δίκτυο

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

Εάν χρησιμοποιείται UNIX \ Linux μπορείτε να χρησιμοποιείται το ifconfig() εργαλείο ή ένα μικρό πρόγραμμα C που ονομάζεται macchanger. Για πλατφόρμες MAC OS χρησιμοποιήστε το xnu (www.securemac.com/macosxxnu.php) ή το etherspoof (http://slagheap.net/etherspoof). Ενώ για Windows το SMAC (http://download.cnet.com/SMAC-MAC-Address-Changer/3000-2085_4-10536535.html).

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

Επίσης έχοντας ένα τείχος προστασίας (firewall), όπως το Sygate (βλέπε στο http://bellsouthpwp.net/i/k/ikpe/SygateBasics.html#GUI) ή τρέχοντας μια υπηρεσία όπως το όπως το echolot, το οποίο είναι ρυθμισμένο ειδικά για το MAC Spoofing. Το Sygate είναι φιλικό προς το χρήστη, και δεν χρειάζεται καλές τεχνικές γνώσεις για να θέσει κάποιος σε λειτουργία το anti-spoofing, όπως φαίνεται στην εικόνα παρακάτω. Μπορούμε να επιλέξουμε την ενεργοποίηση του anti-MAC spoofing απλά με το τσεκάρισμα ενός κουτιού (εικόνα 95).



Εικόνα 95 Ρύθμιση ελέγχου Anti-MAC Spoofing

6.5 Virtual Private Networks (VPNs)

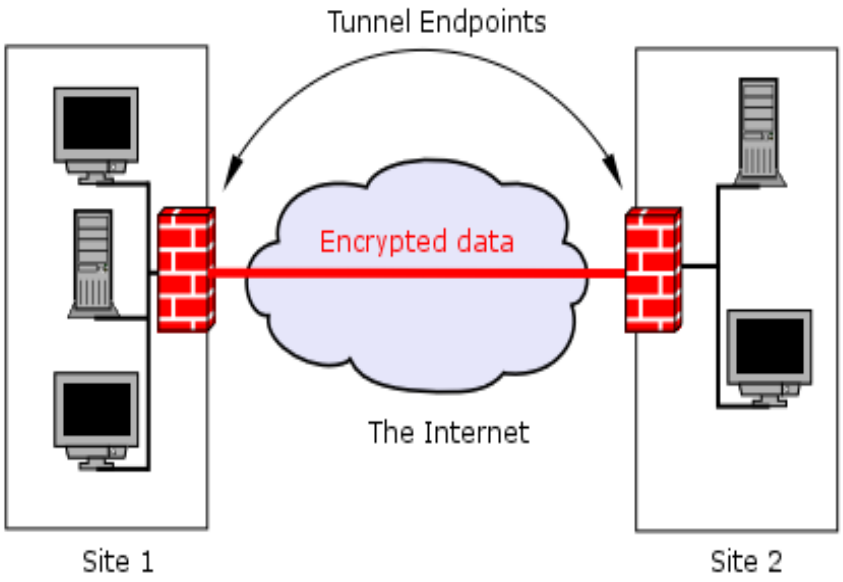
Ένα ιδιωτικό δίκτυο αποτελείται από υπολογιστές που ανήκουν σε ένα μόνο οργανισμό και μοιράζονται πληροφορίες αποκλειστικά μόνο μεταξύ τους. Οι χρήστες του ιδιωτικού δικτύου είναι βέβαιοι ότι αυτοί είναι οι μοναδικοί που χρησιμοποιούν το ιδιωτικό δίκτυο και ότι όλες τις πληροφορίες που στέλνονται μεταξύ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

Ένα ιδιωτικό εικονικό δίκτυο (Virtual Private Network- VPN) είναι κάτι ανάμεσα σε ένα ιδιωτικό και ένα δημόσιο δίκτυο. Το VPN μας επιτρέπει να δημιουργούμε ένα ασφαλές ιδιωτικό δίκτυο βασισμένο πάνω σε ένα δημόσιο δίκτυο όπως είναι το

internet. Μπορούμε να δημιουργήσουμε ένα VPN χρησιμοποιώντας κάποιο λογισμικό ή συσκευές υλικού ή ακόμα και συνδυασμό και των δύο, ώστε να δημιουργηθεί ένας ασφαλής σύνδεσμος ανάμεσα στους κόμβους του δημόσιου δικτύου. Αυτό επιτυγχάνεται με κρυπτογράφηση, επικύρωση, μεταφορά των πακέτων μέσω τούνελ και τοίχων προστασίας.

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

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



Εικόνα 96 Ένα ιδιωτικό εικονικό δίκτυο μέσου του internet

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

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

- **IPSec:** Είναι το πιο ευρέως αναγνωρισμένο, υποστηρίξιμο και ευρέως αναγνωρισμένο όλων των πρωτοκόλλων VPN. Είναι η ιδανική επιλογή για λόγους διαλειτουργικότητας. Το IPSec είναι ένα πλαίσιο ανοιχτών προτύπων, που παράγουν μια ασφαλή σουίτα πρωτοκόλλων, που μπορούν να τρέχουν πάνω από την υπάρχουσα IP συνδεσιμότητα. Παρέχει επικύρωση των

δεδομένων και υπηρεσίες κρυπτογράφησης στο τρίτο επίπεδο του μοντέλου OSI και μπορούν να εφαρμοστούν σε οποιαδήποτε συσκευή επικοινωνεί μέσω IP. Το πρωτόκολλο αυτό περιλαμβάνει τρία κύρια μέρη: την Authentication Header (AH)[55], Encapsulating Security Payload (ESP), και Internet Key Exchange (IKE).

Το AH προστίθεται μετά την IP επικεφαλίδα, παρέχει επικύρωση σε επίπεδο πακέτων και υπηρεσίες ακεραιότητας, διασφαλίζοντας έτσι ότι το πακέτο δεν έχει πειραχτεί από την προέλευση μέχρι τον προορισμό. Το ESP παρέχει εμπιστευτικότητα, επικύρωση των δεδομένων προέλευσης, ακεραιότητα και περιορισμένη εμπιστευτικότητα ροής πληροφορίας. Τέλος το IKE διαπραγματεύεται διάφορες ενώσεις ασφάλειας που περιγράφουν τη χρήση των υπηρεσιών ασφάλειας μεταξύ των συμμετεχόντων φορέων.

- **PPTP:** Το πρωτόκολλο τούνελ από σημείο σε σημείο (Point-to-Point Tunneling Protocol) είναι ένα ιδιόκτητο πρωτόκολλο που αναπτύχθηκε από τη Microsoft και προορίζεται για επικοινωνίες μέσω VPN. Το PPTP προσφέρει ταυτοποίηση χρήστη, χρησιμοποιώντας πρωτόκολλα επικύρωσης όπως MS-CHAP[56], CHAP, SPAP, PAP. Το PPTP προσφέρει την ευελιξία που παρέχουν και οι άλλες λύσεις αλλά δεν διαθέτει το ίδιο επίπεδο διαλειτουργικότητας, όπως τα άλλα πρωτόκολλα VPN, αλλά η χρήση του είναι εύκολη.

- **GRE:** Το Generic Routing Encapsulation (GRE), είναι ένα πρωτόκολλο που αναπτύχθηκε από τη Cisco και χρησιμοποιείται στη δικτύωση μέσω τούνελ, για την κίνηση μεταξύ διαφορετικών ιδιωτικών δικτύων. Το GRE χρησιμοποιείται συχνά σε συνδυασμό με τα πρωτόκολλα κρυπτογράφησης επιπέδου δικτύου, ώστε να παρέχει και ενθυλάκωση των μη-IP πρωτοκόλλων αλλά και κρυπτογράφηση που παρέχονται από άλλα πρωτόκολλα όπως το IPSec.

- **L2TP:** Αναπτύχθηκε από κοινού από τη Cisco, τη Microsoft και τη 3Com. Το L2TP υποσχέθηκε να αντικαταστήσει το PPTP. Ουσιαστικά είναι ένας συνδυασμός του PPTP και του Cisco Layer Two Forwarding (L2F), δηλαδή η συγχώνευση και των δύο σε ένα ενιαίο πρότυπο. Το L2TP χρησιμοποιείται για να δημιουργηθεί ένα τούνελ PPTP πάνω από ένα δημόσιο IP δίκτυο. Βασίζεται στο PPTP, για τη δημιουργία μιας dial-up σύνδεσης, χρησιμοποιώντας PAP ή CHAP επικύρωση. Το πρωτόκολλο δεν χρησιμοποιεί κρυπτογράφηση από μόνο του αλλά μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλα πρωτόκολλα ή με μηχανισμούς κρυπτογράφησης σε επίπεδο εφαρμογών.

Υπάρχουν τέσσερα βασικά βήματα που πρέπει να κάνουμε για να εγκαταστήσουμε ένα VPN τούνελ στον υπολογιστή μας.

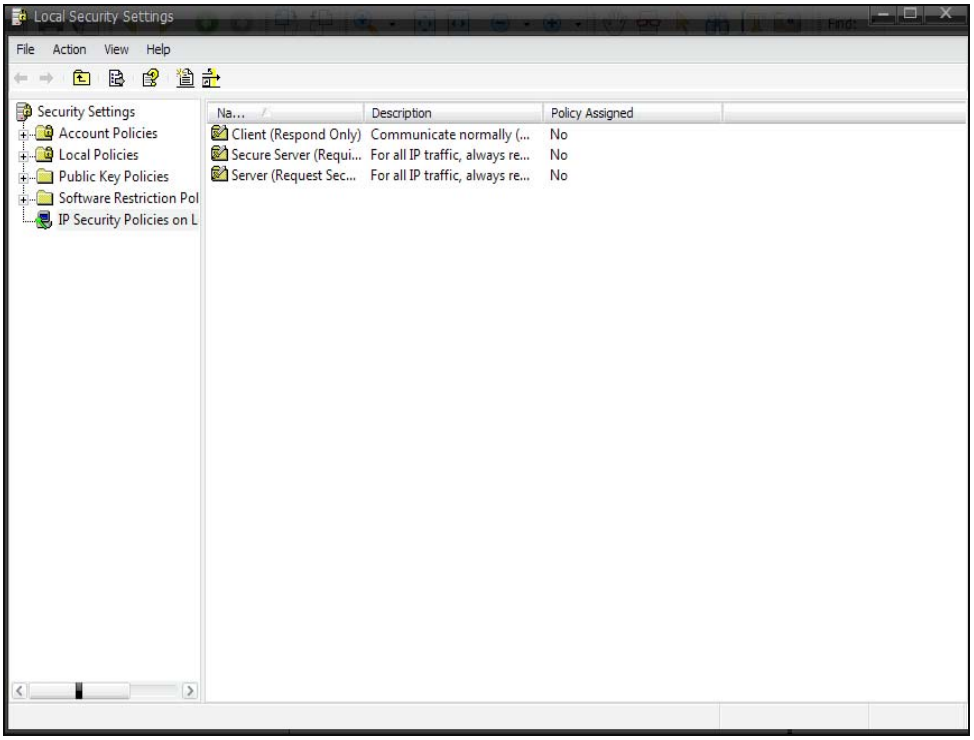
1. Να δημιουργήσουμε μια πολιτική IPSec
2. Να κατασκευάσουμε δύο λίστες φίλτρων

[55] http://en.wikipedia.org/wiki/IPsec
[56] http://en.wikipedia.org/wiki/MS-CHAP

3. Εγκαθιδρύσουμε τους κανόνες του τούνελ
4. Να εφαρμόσουμε την IPSec στον υπολογιστή μας

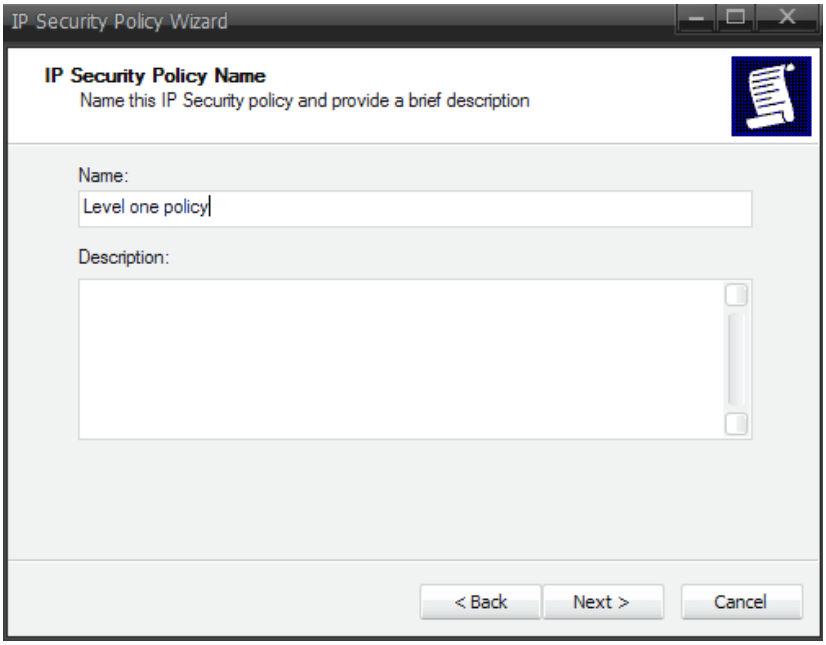
6.5.1 Δημιουργώντας την IPSec πολιτική

Επιλέγουμε **Έναρξη** -> **Εκτέλεση** και πληκτρολογούμε **secpol.msc** στο κουτί που μας ανοίγει, για να μας ανοίξει την οθόνη με τις τοπικές ρυθμίσεις ασφαλείας όπως φαίνεται στην εικόνα 97.



Εικόνα 97 Τοπικές ρυθμίσεις ασφαλείας

Δεξί κλικ στο **IP Security Policies on Local Computer** και επιλέγουμε **Create IP Security Policy.** Εισάγουμε το όνομα που θέλουμε για την πολιτική ασφάλειας (όπως φαίνεται στην εικόνα 98) και πατάμε επόμενο.

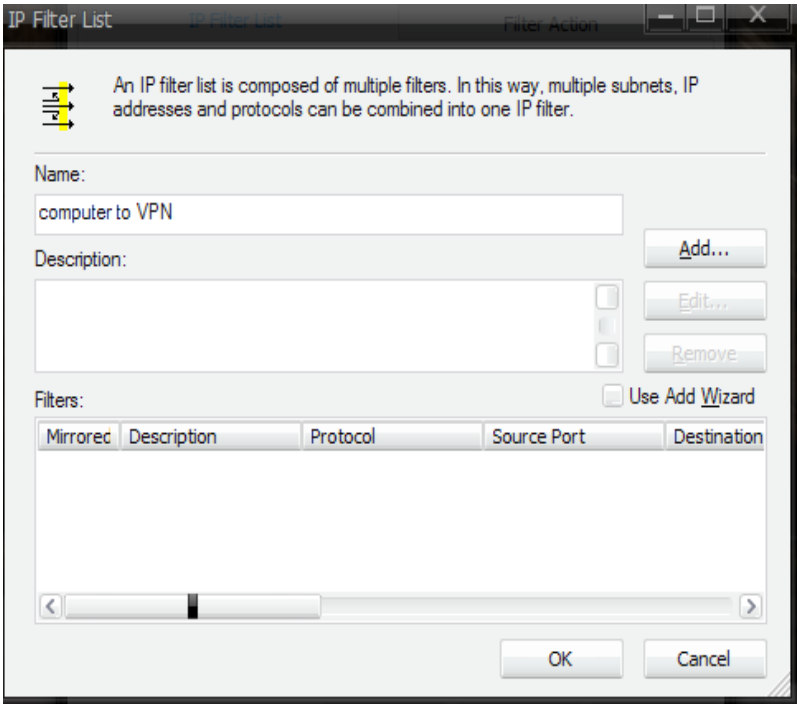


Εικόνα 98 Ονομάζοντας την πολιτική τοπικής ασφάλειας

Ξετσεκάρουμε το κουτάκι του **Activate the default response rule,** πατάμε επόμενο, βεβαιωνόμαστε ότι το κουτάκι του **Edit properties** είναι επιλεγμένο και πατάμε τέλος.

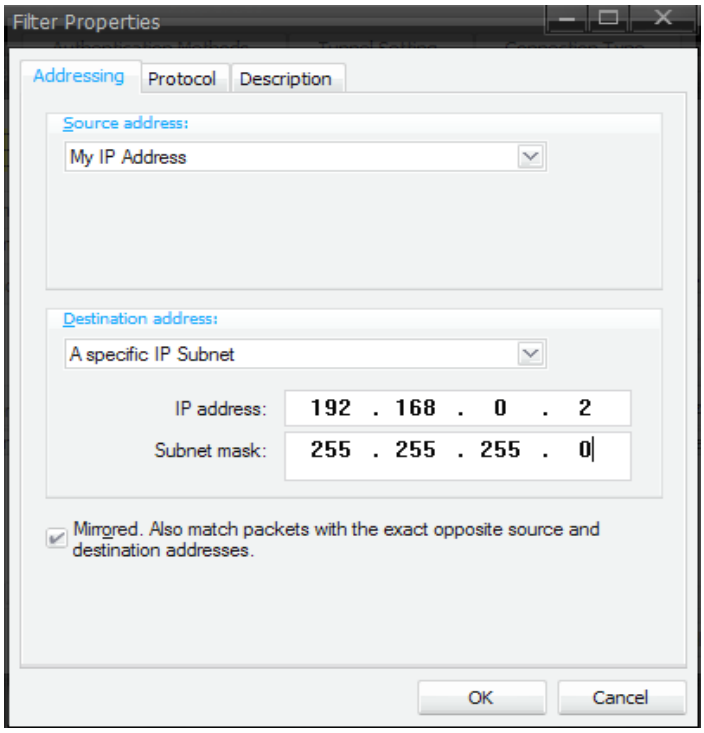
6.5.2 Δημιουργώντας τις λίστες φίλτρων

Επιλέγοντας το κουτάκι **Edit properties** πριν τελειώσουμε το **IP security Policy Wizard,** μας ανοίγει το παράθυρο των καταχωρήσεων για την νέα πολιτική ασφάλειας. Πατάμε **Add** για να μας ανοίξει το παράθυρο του IP Filter List. Εισάγουμε ένα όνομα για το φίλτρο όπως φαίνεται στην εικόνα 99, ξετσεκάρουμε το **Use Add Wizard** και πατάμε **Add.**



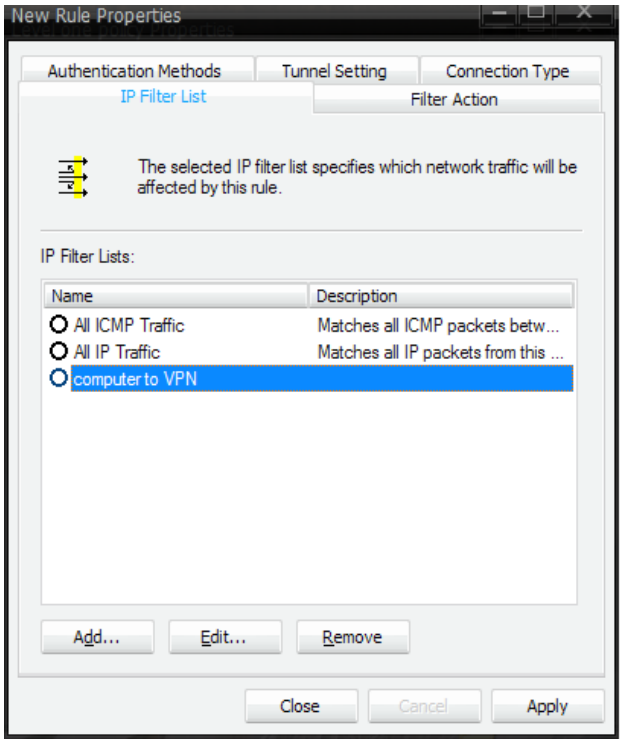
Εικόνα 99 Το IP Filter List παράθυρο

Το παράθυρο με τις ιδιότητες του φίλτρου ανοίγει μια καρτέλα διευθύνσεων. Επιλέγουμε **My IP Address** στο πεδίο **Source Address** και **A Specific IP Subnet** στο πεδίο **Destination Address**. Στο **IP Address** πεδίο εισάγουμε την διεύθυνση IP μας και την μάσκα υποδικτύου στο πεδίο **Subnet Mask** (όπως φαίνεται στην εικόνα 100), η οποία από προεπιλογή είναι 255.255.255.0. Πατάμε OK για να κλείσει το παράθυρο.



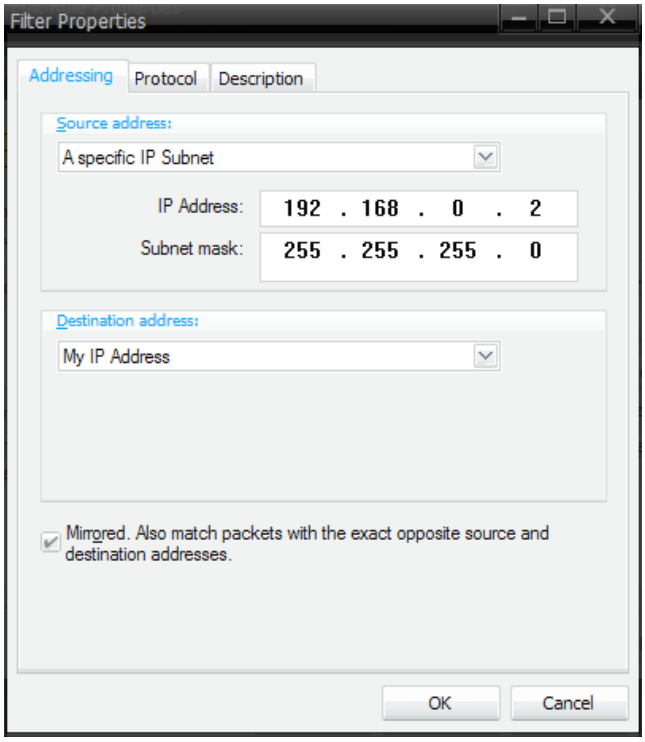
Εικόνα 100 Οι ρυθμίσεις του IP Filter

Αυτό το φίλτρο το χρησιμοποιούμε για την επικοινωνία από τον υπολογιστή μας στον δρομολογητή. Στη συνέχεια χρειάζεται να δημιουργήσουμε ένα φίλτρο για την επικοινωνία από τον δρομολογητή στον υπολογιστή μας. Στο **New Rule Properties** παράθυρο, τονίζουμε τον κανόνα που μόλις δημιουργήσαμε (όπως φαίνεται στην εικόνα 101) και πατάμε **Add**.



Εικόνα 101 Δημιουργώντας το δεύτερο φίλτρο

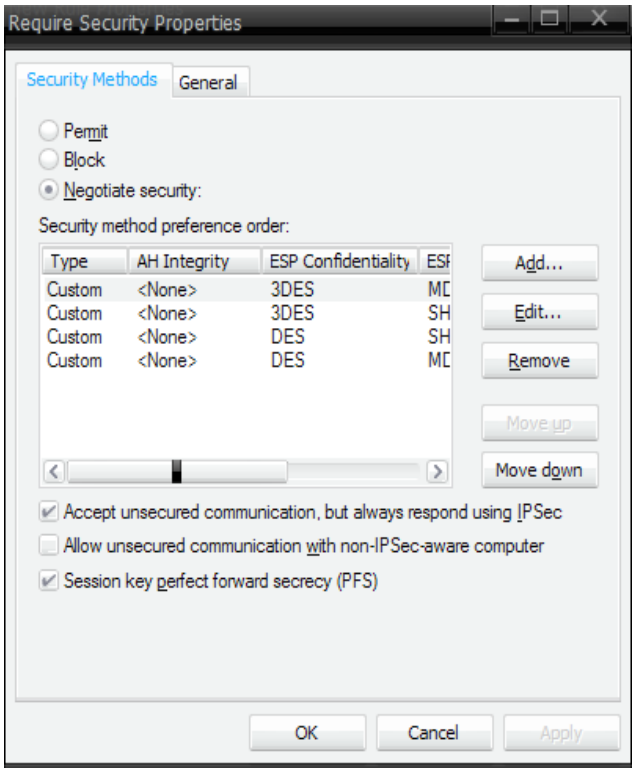
Αυτό ανοίγει το παράθυρο **IP Filter List.** Εισάγουμε ένα όνομα για το καινούριο φίλτρο και πατάμε **Add**. Στην καρτέλα διευθύνσεων επιλέγουμε **A Specific IP Subnet** στο πεδίο **Source Address.** Στο **IP Address** πεδίο εισάγουμε την διεύθυνση IP μας και την μάσκα υποδικτύου στο πεδίο **Subnet Mask** (όπως φαίνεται στην εικόνα 102), η οποία από προεπιλογή είναι 255.255.255.0. Επιλέγουμε **My IP Address** στο πεδίο **Destination Address.** Πατάμε OK για να κλείσει το παράθυρο.



Εικόνα 102 Οι ρυθμίσεις του IP Filter

6.5.3 Εγκαθιδρύοντας τους κανόνες του τούνελ.

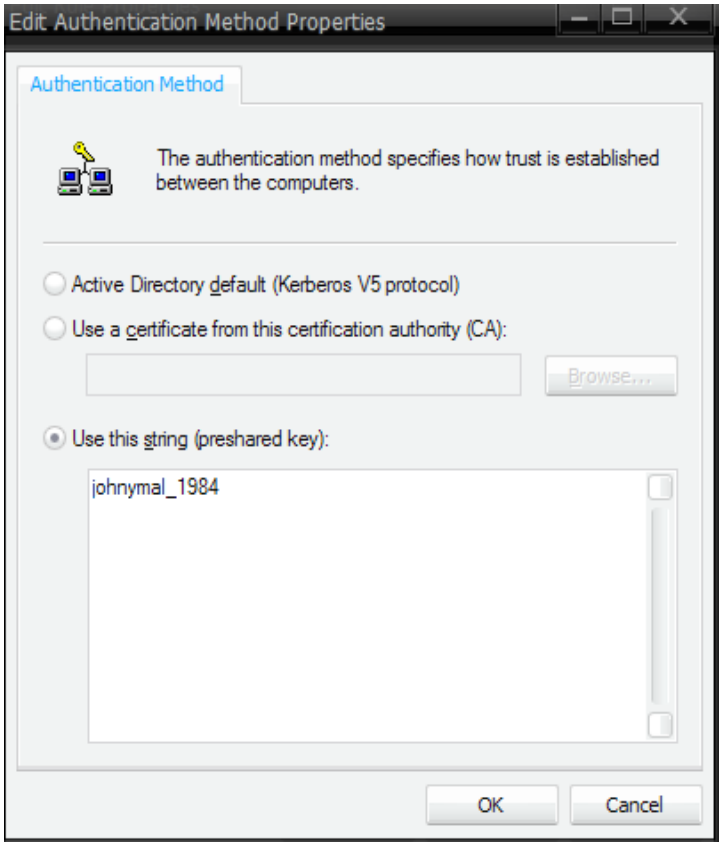
Οι κανόνες των τούνελ πρέπει να δημιουργούνται για να επιτυγχάνεται ομαλά η κίνηση των φίλτρων μέσα στο VPN τούνελ. Πρώτα επιλέγουμε το τούνελ που δημιουργήσαμε για την επικοινωνία από τον υπολογιστή στο δρομολογητή και επιλέγουμε την καρτέλα **Filter Action.** Τσεκάρουμε την επιλογή **Require Security** και πατάμε **Edit** για να μας ανοίξει το Require Security Properties παράθυρο όπως φαίνεται στην εικόνα 103.



Εικόνα 103 Παράθυρο με τις απαιτούμενες ρυθμίσεις ασφαλείας

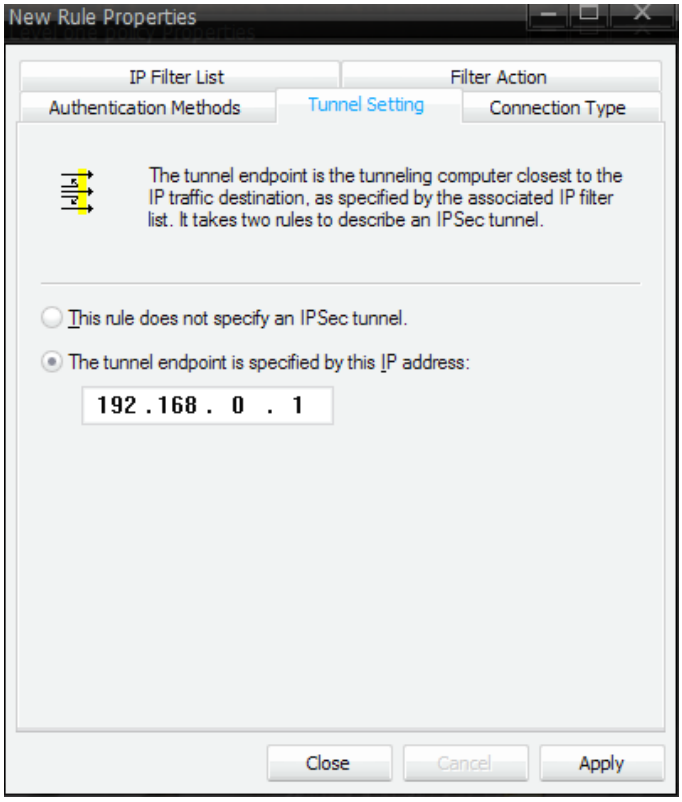
Βεβαιωνόμαστε ότι είναι τσεκαρισμένη η επιλογή **Negotiate security.** Στη συνέχεια ξετσεκάρουμε το **Accept unsecured communication, but always respond using IPSec** και τσεκάρουμε την επιλογή **Session key perfect forward security (PFS),** όπως φαίνεται στην εικόνα 103.

Πατάμε **OK** για να γυρίσουμε πίσω στο **New Rule Properties** παράθυρο**.** Επιλέγουμε την καρτέλα **Authentication Methods** και πατάμε **Edit** για να ανοίξει το **Edit Authentication Method Properties παράθυρο.** Τσεκάρουμε την επιλογή **Use this string (preshared key)** και εισάγουμε το προ-μοιρασμένο κλειδί που θα χρησιμοποιούμε (εικόνα 104). Αυτό μπορεί να είναι ένας συνδυασμός έως 24 γραμμάτων και αριθμών, αλλά οι ειδικοί χαρακτήρες δεν επιτρέπονται. Βεβαιωνόμαστε ότι θα θυμόμαστε εύκολα αυτό το κλειδί, καθώς αυτό θα χρησιμοποιηθεί αργότερα όταν ρυθμιστεί ο δρομολογητής.



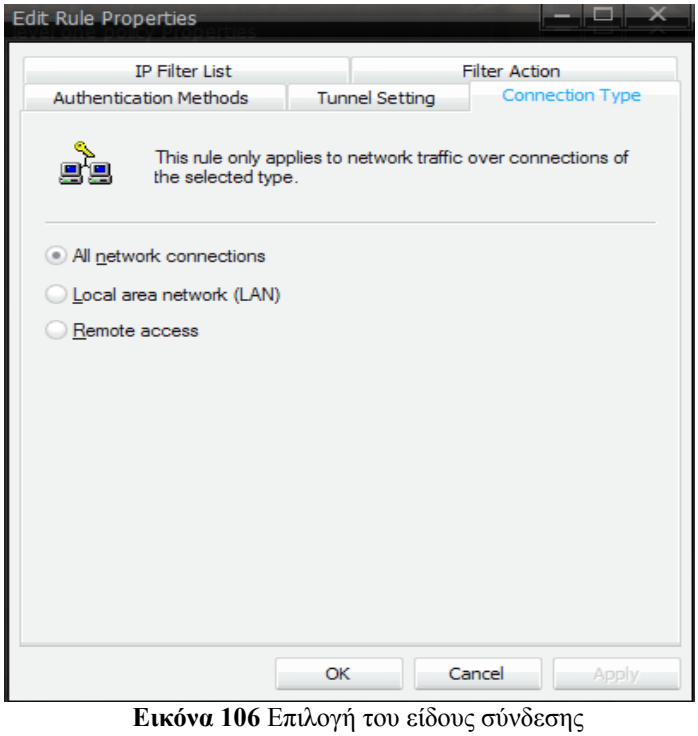
Εικόνα 104 Εισαγωγή προ-μοιρασμένου κλειδιού

Στη συνέχεια πατάμε **OK** για να κλείσει το παράθυρο. Επιλέγουμε την καρτέλα **Tunnel Setting** και έπειτα επιλέγουμε **The tunnel endpoint is specified by this IP address** και εισάγουμε την εξωτερική IP διεύθυνση του δρομολογητή που χρησιμοποιούμε (εικόνα 105). Αυτή είναι η IP διεύθυνση που χρησιμοποιεί ο δρομολογητής για να συνδέεται στο internet.



Εικόνα 105 Η καρτέλα με τις ρυθμίσεις του τούνελ

Έπειτα επιλέγουμε την καρτέλα **Connection Type** (εικόνα 106) και τσεκάρουμε **All network connections** εάν θέλουμε ο κανόνας που δημιουργήσαμε να εφαρμόζεται και στις συνδέσεις internet αλλά και στις τοπικές συνδέσεις, **Local area network (LAN)** εάν θέλουμε το τούνελ να εφαρμόζεται μόνο στις τοπικές συνδέσεις ή **Remote access** για να εφαρμόζεται μόνο στις συνδέσεις που γίνονται από το internet.

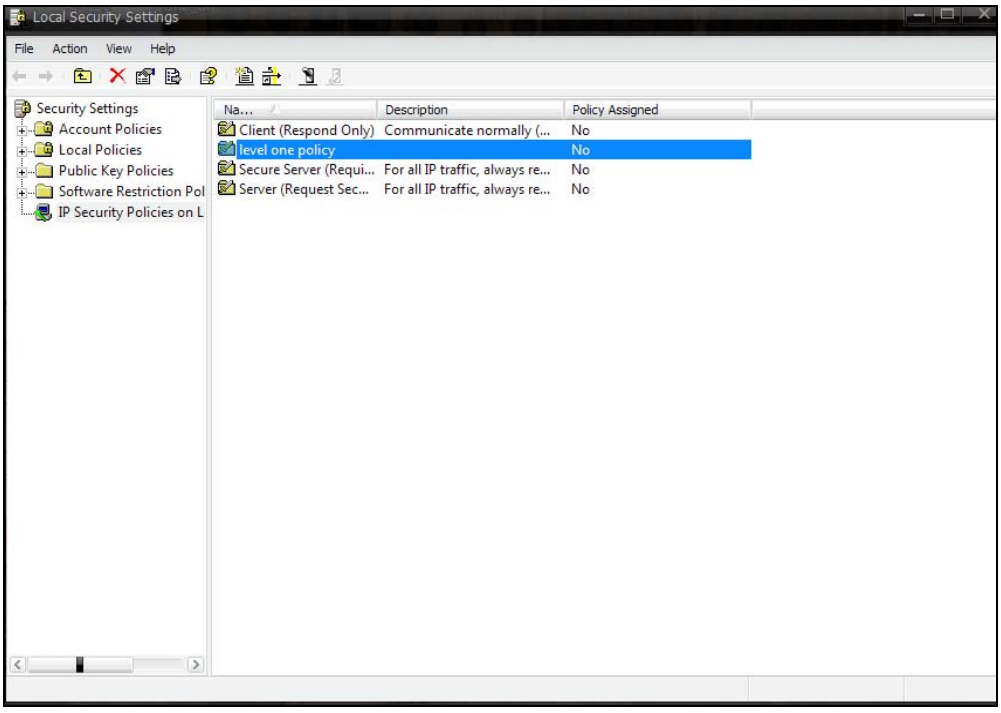


Εικόνα 106 Επιλογή του είδους σύνδεσης

Μετά που έχουμε επιλέξει το είδος της σύνδεσης του δικτύου, πατάμε **Close.** Άλλος ένας κανόνας φίλτρου πρέπει να δημιουργηθεί για να επιτρέπεται η επικοινωνία από το δρομολογητή στον υπολογιστή. Για να δημιουργήσουμε αυτό τον κανόνα επαναλαμβάνουμε τα παραπάνω βήματα και η μόνη διαφορά είναι ότι πληκτρολογούμε την IP διεύθυνση του υπολογιστή μας, ως σημείο τερματισμού του τούνελ.

6.5.4 Εφαρμόζοντας την πολιτική ασφάλειας

Στο τέλος πρέπει να εφαρμόσουμε την πολιτική ασφάλειας που δημιουργήσαμε στον υπολογιστή μας. Στο **Local Security Settings** παράθυρο, πατάμε δεξί κλικ στην πολιτική που έχουμε δημιουργήσει και επιλέγουμε **Assign** (εικόνα 107). Τώρα ο υπολογιστής μας είναι ρυθμισμένος να επικοινωνήσει μέσω ενός VPN τούνελ.

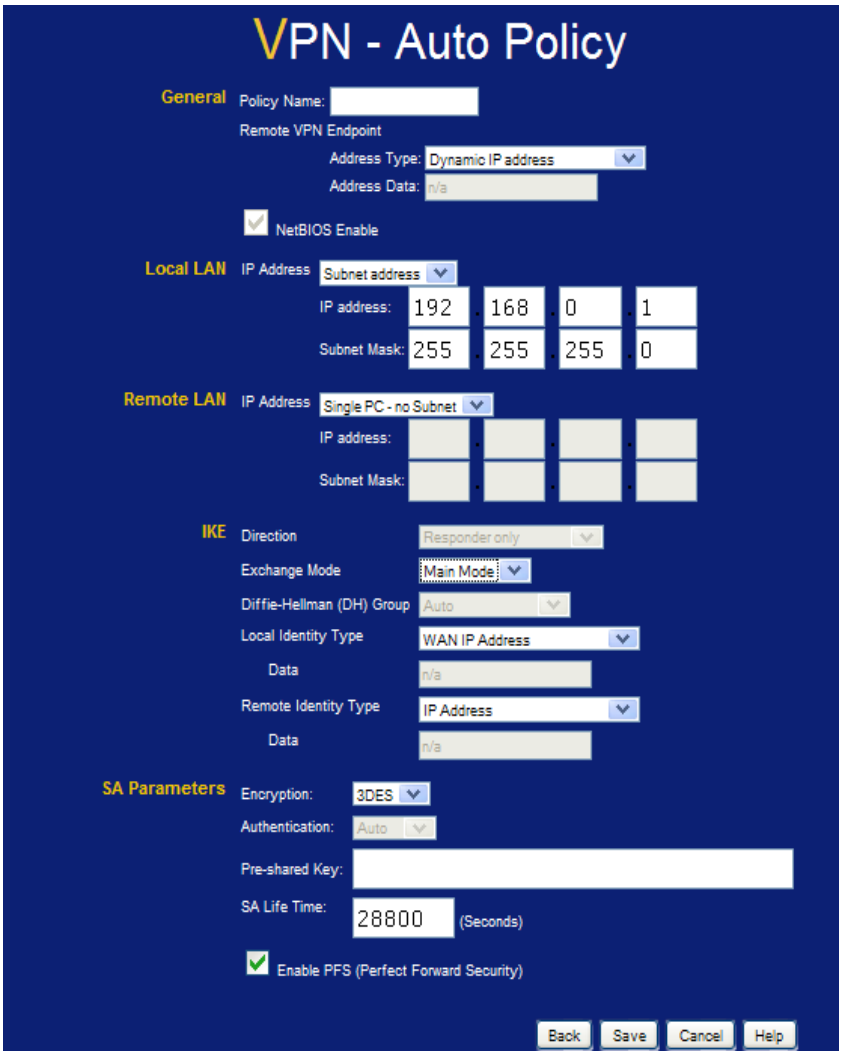


Εικόνα 107 Εφαρμόζοντας την πολιτική ασφάλειας

6.5.5 Εφαρμόζοντας το VPN στο σημείο πρόσβασης

Όταν ο υπολογιστής μας έχει ρυθμιστεί να επικοινωνήσει με ένα IPSec VPN τούνελ, πρέπει να ρυθμίσουμε και το σημείο πρόσβασης ώστε να μπορεί να επικοινωνεί με τον υπολογιστή μας. Χρησιμοποιώντας τον web περιηγητή μας, πληκτρολογούμε τη προεπιλεγμένη IP διεύθυνση του σημείου πρόσβασης που χρησιμοποιούμε στο εσωτερικό μας δίκτυο, 192.168.0.1 στην περίπτωσή μας. Στη συνέχεια πληκτρολογούμε το όνομα χρήστη και τον κωδικό πρόσβασης που έχουμε θέσει, ώστε να ανοίξει η καρτέλα με τις ρυθμίσεις του σημείου πρόσβασης.

Επιλέγουμε **Advanced** -> **VPN** ώστε να μας εμφανιστούν οι ρυθμίσεις του VPN όπως φαίνεται στην εικόνα 108.



Εικόνα 108 Παράθυρο ρυθμίσεων του VPN

Διαλέγουμε ένα όνομα για την πολιτική ασφάλειας και το εισάγουμε στο Policy name κουτί. Στη συνέχεια πληκτρολογούμε την IP διεύθυνση και την μάσκα υποδικτύου, του τοπικού δικτύου, στα πεδία **IP Address** και **Subnet mask** του πεδίου **Local LAN**. Έπειτα εισάγουμε την IP διεύθυνση και την μάσκα υποδικτύου του υπολογιστή που μόλις ρυθμίσαμε στα πεδία **IP Address** και **Subnet mask** του πεδίου **Remote LAN.**

Στο πεδίο **Encryption** επιλέγουμε σαν μέθοδο κρυπτογράφησης το **3DES**. Αυτό απαιτεί τη χρήση του τριπλού προτύπου κωδικοποίησης δεδομένων (Triple Data Encryption Standard). Επιλέγουμε **IKE** ως μέθοδο ανταλλαγής κλειδιού, και τσεκάρουμε την επιλογή **PFS** (Perfect Forward Secrecy). Τέλος, στο πεδίο **Pre-Shared Key** εισάγουμε το ίδιο προ-μοιρασμένο κλειδί που πληκτρολογήσαμε και στον υπολογιστή όταν τον ρυθμίζαμε. Όταν τελειώσουμε με όλες αυτές τις ρυθμίσεις

πατάμε **Save** για να τις σώσουμε και έχει τελειώσει η εγκατάσταση του VPN τούνελ ανάμεσα στο σημείο πρόσβασης και τον υπολογιστή μας.

Εικόνα 109 Οι ολοκληρωμένες ρυθμίσεις του VPN

6.6 SSID Hiding

Όταν κάποιος ενδιαφέρεται για την ασφάλεια των ασύρματων δικτύων, πρέπει να δείξει και σεβασμό στο πεδίο του SSID. Τα περισσότερα ασύρματα δίκτυα από προεπιλογή μπορούν να μεταδώσουν την πληροφορία σε οποιονδήποτε ακούει εκείνη τη στιγμή. Όσοι όμως μελετάμε περισσότερο την ασφάλεια των ασύρματων δικτύων θεωρούμε ότι πρέπει να κρύβουμε το SSID. Παρατηρήθηκε ότι αν δεν εκπέμπεται το SSID, η ύπαρξη του ασύρματου δικτύου μπορεί κάπως να καλυφθεί. Αυτή η κάλυψη θα απαιτούσε από τον πελάτη να στέλνει έλεγχο για οποιαδήποτε ασύρματο δίκτυο είναι διαθέσιμο.

Στα περισσότερα IEEE δίκτυα, η ύπαρξη του SSID προϋποθέτει την ύπαρξη ασύρματου sniffer[57] και αυτό διότι το SSID είναι μέρος της διαδικασίας σύνδεσης σε ένα ασύρματο δίκτυο. Το SSID αναπαρίσταται στην επικεφαλίδα ενός ασύρματου απαντητικού πλαισίου ελέγχου. Αυτή η πληροφορία μπορεί να διαβαστεί από οποιοδήποτε sniffing πρόγραμμα και με το να την κρύψουμε μπορούμε να νικήσουμε οποιεσδήποτε τέτοιου είδους προσπάθειες.

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

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

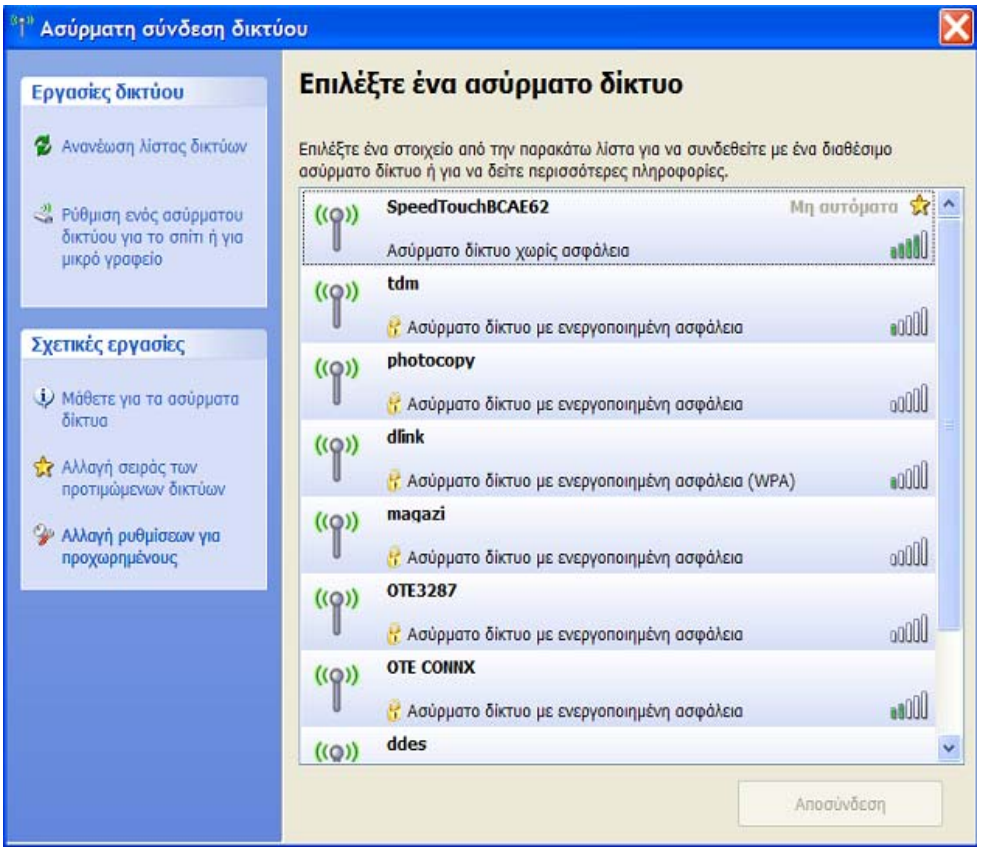
Ένα μεγάλο βήμα που χρειάζεται να κάνουμε για να ασφαλίσουμε το οικιακό μας ασύρματο δίκτυο είναι να μην ανακοινώνουμε ότι έχουμε ένα. Τα δημόσια ή τα εταιρικά δίκτυα ίσως χρειάζεται να εκπέμπουν την ύπαρξή τους, ώστε οι καινούργιες ασύρματες συσκευές να μπορούν να τα ανιχνεύσουν και να συνδεθούν σε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

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

Η κάθε συσκευή έχει συνήθως ως προεπιλεγμένο SSID το όνομα του κατασκευαστή της όπως για παράδειγμα Linksys, Netgear, CONNX και διάφορα άλλα. Στην παρακάτω εικόνα βλέπουμε τα SSID διαφόρων δικτύων που ανιχνεύει η ασύρματη

[57] http://el.wikipedia.org/wiki/Packet_sniffer

κάρτα δικτύου μας. Ακόμα και αν είναι απενεργοποιημένη η εκπομπή του SSID, είναι σημαντικό να μην χρησιμοποιούμε το προεπιλεγμένο SSID. Οι κατασκευαστές του ασύρματου εξοπλισμού είναι μετρημένοι οπότε δεν θα πάρει πολύ χρόνο για να μαντέψει κάποιος το πιθανό SSID.

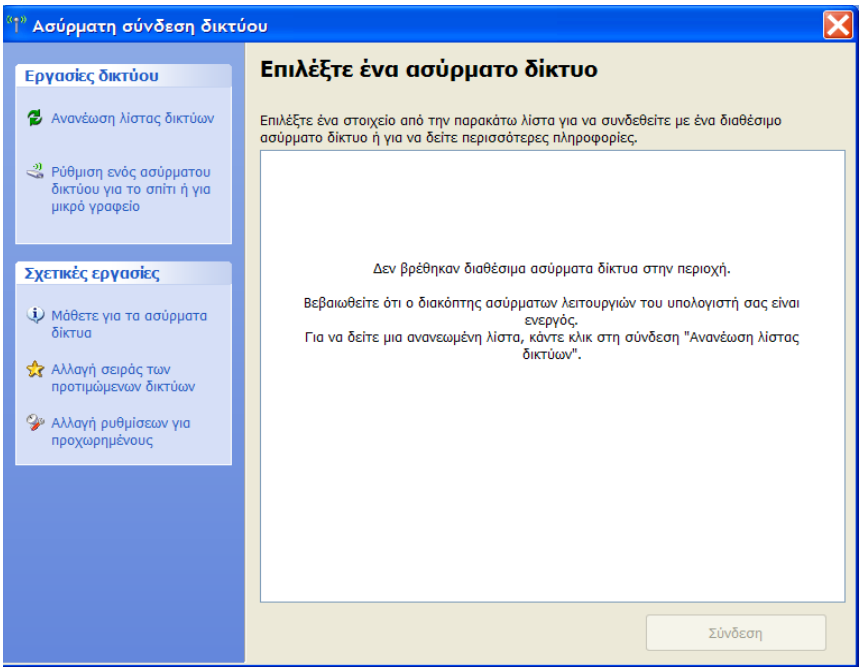


Εικόνα 110 SSID διαφόρων ασύρματων δικτύων που ανιχνεύει η κάρτα δικτύου

Άρα το ένα από τα πρώτα πράγματα που κάνουμε είναι να αλλάξουμε το προεπιλεγμένο SSID και να βάλουμε ένα δικό μας μοναδικό. Όπως φαίνεται στην εικόνα 111 στο κουτί με το SSID βάζουμε ένα μοναδικό δικό μας SSID. Μετά που θα το κάνουμε αυτό, πάμε στην επιλογή broadcast SSID και το ξε-τσεκάρουμε ή πατάμε disable ανάλογα με το τι επιλογή μας δίνει. Τέλος σώνουμε τις ρυθμίσεις που έχουμε κάνει.

Εικόνα 111 Ρύθμιση του access point για μη εκπομπή SSID

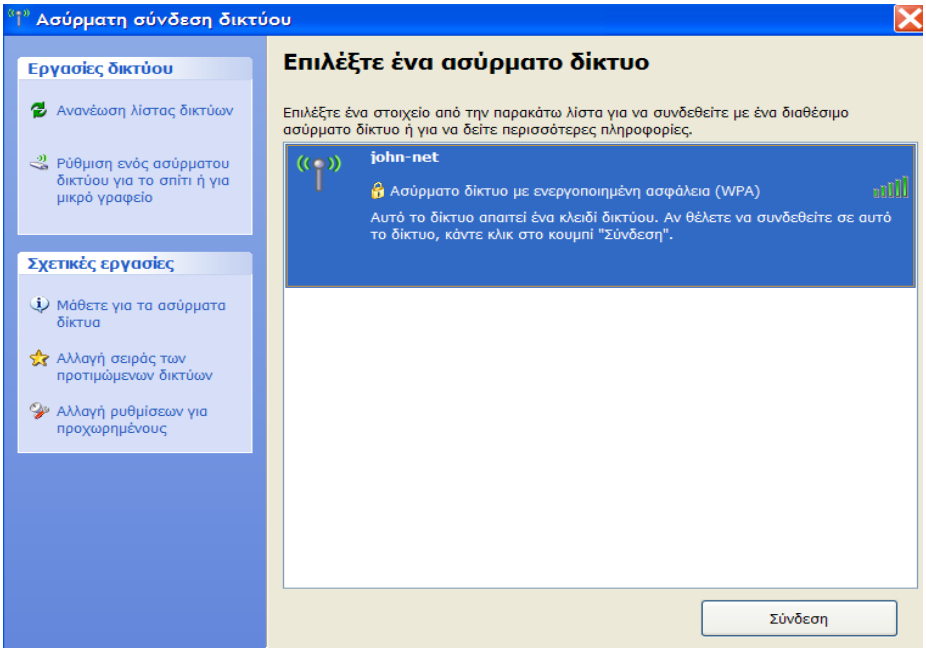
Όπως βλέπουμε και στην εικόνα 112, αν επιλέξουμε να μην εκπέμπεται το SSID του ασύρματου δικτύου μας, οποιαδήποτε ασύρματη κάρτα χρησιμοποιούμε στον υπολογιστή μας, δεν μπορεί να το ανιχνεύσει καθόλου.



Εικόνα 112 Μη ανίχνευση ασύρματου δικτύου από την ασύρματη κάρτα

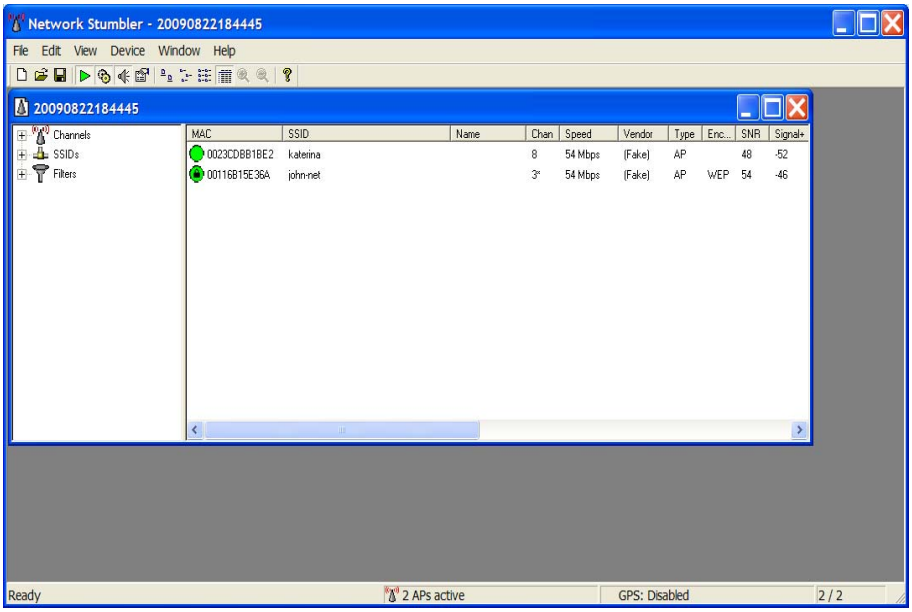
Αντίθετα αν επιλέξουμε να εκπέμπεται το όνομα του SSID μας, το ασύρματο δίκτυο μας θα ανιχνεύεται από οποιαδήποτε ασύρματη κάρτα χρησιμοποιήται εντός της εμβέλειας του συγκεκριμένου δικτύου (εικόνα 113 και εικόνα 114).

Εικόνα 113 Ρύθμιση του access point για εκπομπή SSID



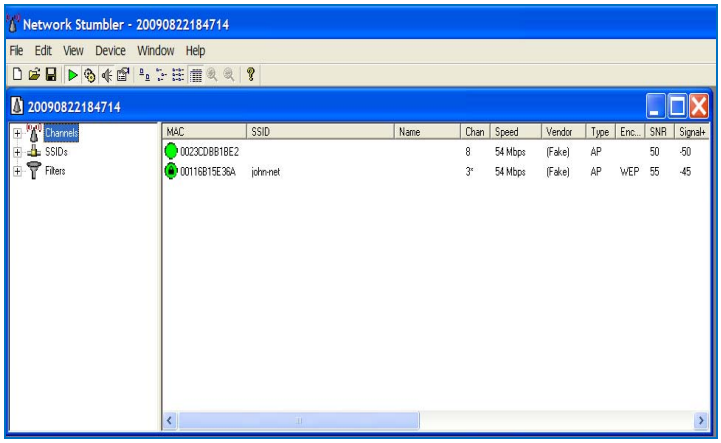
Εικόνα 114 Ανίχνευση ασύρματου δικτύου από την ασύρματη κάρτα

Το NetStumbler είναι μια εφαρμογή ανίχνευσης ενεργών ασύρματων δικτύων. Όταν το NetStumbler ανιχνεύσει ένα ασύρματο δίκτυο, κάνει αίτηση για το όνομα του σημείου πρόσβασης. Επιπλέον οι διασυνδέσεις του NetStumbler παρέχουν εργαλεία φιλτραρίσματος και ανάλυσης. Αυτά τα εργαλεία επιτρέπουν στο χρήστη να φιλτράρει τον αριθμό των σημείων πρόσβασης και τα WLANs βασιζμένος σε διάφορα κρητήρια όπως ποια δίκτυα έχουν ισχυρότερο σήμα, ποία δίκτυα χρημοποιούν κρυπτογράφηση και πολλά άλλα.



Εικόνα 115 Ανίχνευση ασύρματων δικτύων με το NetStumbler

Το NetStumbler μεταδίδει μια αίτηση μετάδοσης για να ανακαλύψει το ασύρματο δίκτυο. Τα περισσότερα σημεία πρόσβασης, από προεπιλογή, ανταποκρίνονται σε αυτή την αίτηση μετάδοσης. Όταν το σημείο πρόσβασης ανταποκριθεί, μεταδίδει το SSID του, τον αριθμό MAC του και διάφορες άλλες πληροφορίες σχετικά με το κανάλι στο οποίο εκπέμπει, την ισχύ του σήματος, το είδος της κρυπτογράφησης και δίαφορα άλλα. Ωστόσο διάφορα μοντέλα σημείων πρόσβασης επιτρέπουν αυτό το χαρακτηριστηκό να απενεργοποιήται. Όταν ένα σημείο πρόσβασης παύει πια να ανταποκρίνεται στην αίτηση το NetStumbler δεν μπορεί πλέον να το ανιχνεύει.



Εικόνα 116 Ανίχνευση ασύρματων δικτύων με απενεργοποιημένο το SSID

Κεφάλαιο 7 Συμπεράσματα

Στο κεφάλαιο αυτό περιγράφονται εν συντομία η πορεία της παρούσας πτυχιακής εργασίας, συνοψίζονται τα αποτελέσματα της και αναφέρονται τα συμπεράσματα που εξήχθησαν. Τέλος γίνεται αναφορά σε επεκτάσεις που θα είχαν ερευνητικό και πρακτικό ενδιαφέρον.

Τα ασύρματα δίκτυα αντιπροσωπεύουν ένα από τα μεγαλύτερα πλεονεκτήματα της δικτύωσης των τελευταίων χρόνων, κυρίως για τους οικιακούς χρήστες που θέλουν να μοιράζονται την σύνδεση τους στο internet χωρίς τη χρήση καλωδίων μεταξύ τοίχων και ορόφων. Δυστυχώς όμως εάν δεν ασφαλίζονται κατάλληλα, τα ασύρματα δίκτυα επίσης παρουσιάζουν ένα από τα μεγαλύτερα μειονεκτήματα ασφάλειας των πρόσφατων χρόνων.

Στην πτυχιακή αυτή εργασία, μελετήθηκε η ασφάλεια του 802.11 προτύπου, που χρησιμοποιείται στα ασύρματα δίκτυα. Μελετήθηκαν τα πιο γνωστά είδη επιθέσεων που συμβαίνουν στα ασύρματα δίκτυα και υλοποιήθηκαν και στην πράξη μερικές από αυτές τις επιθέσεις. Στη συνέχεια προτάθηκαν τα βασικά μέτρα ασφαλείας που πρέπει να εφαρμόζουμε ώστε να αποτρέπουμε το δίκτυο μας από το να πέφτει θύμα σε τέτοιου είδους επιθέσεις.

Πιο συγκεκριμένα αρχικά αναφέρθηκαν κάποιες βασικές πληροφορίες για τα ασύρματα δίκτυα, όπως το πότε άρχισαν να δημιουργούνται, τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζουν σε σχέση με τα ενσύρματα, τις εφαρμογές που τα βρίσκουμε και τα βασικά δομικά στοιχεία που τα αποτελούν. Έπειτα μελετήθηκαν οι αρχές λειτουργίας του IEEE 802.11 πρωτοκόλλου, που προδιαγράφει την τεχνολογία των Ασύρματων Τοπικών δικτύων. Είδαμε τα πρότυπα που αποτελούν την οικογένεια 802.11, τα βασικά χαρακτηριστικά τους, αναφερθήκαμε στις μορφές τοπολογίας που συναντάμε στο 802.11 πρότυπο καθώς και για τη μορφή αρχιτεκτονικής του.

Επιπρόσθετα αναλύθηκαν οι μηχανισμοί ασφάλειας που χρησιμοποιούνται στο 802.11 πρότυπο. Δόθηκε εκτενείς περιγραφή στον αρχικό μηχανισμό ασφάλειας που χρησιμοποιήθηκε, το WEP. Παρουσιάστηκε ο τρόπος λειτουργίας του και δόθηκε ιδιαίτερη έμφαση στις επιδόσεις του όσον αφορά την ασφάλεια. Ακόμα παρουσιάστηκαν οι αναβαθμίσεις που έγιναν για να βελτιωθεί η ασφάλεια του WEP. Παρουσιάστηκαν η 802.1X επικύρωση, το WPA και το WPA2. Επίσης αναλύθηκαν οι έννοιες EAP, RADIUS, TKIP και AES.

Στη συνέχεια παρουσιάστηκαν οι πιο γνωστές επιθέσεις που συμβαίνουν σε Ασύρματα Τοπικά Δίκτυα κυρίως συμβατικής ασφάλειας WEP και υλοποιήθηκαν από αυτές οι επιθέσεις WEP cracking, MAC spoofing και sniffing. Τέλος προτάθηκαν τα βασικά μέτρα ασφάλειας που πρέπει να εφαρμόζουμε κατά την υλοποίηση ενός ασύρματου δικτύου, ώστε να μπορούμε να προστατευτούμε από τέτοιου είδους επιθέσεις.

7.1 Αποτελέσματα της εργασίας

Από τα παραπάνω, γίνεται φανερή η αντικατάσταση του σχήματος ασφάλειας WEP στα Ασύρματα Τοπικά δίκτυα. Παρόλο που το πρότυπο IEEE 802.11 σχεδιάστηκε για να αποτελέσει ένα παγκόσμιο πρότυπο για τη δημιουργία ασύρματων δικτύων, δεν δόθηκε αρκετή προσοχή από την υποεπιτροπή στο σύστημα ασφάλειας. Έτσι φτάσαμε στο σημείο, η αρχική έκδοση του 802.11 να είναι αρκετά ανασφαλής, όπως φαίνεται και από την ανάλυση που προηγήθηκε.

Οι βελτιώσεις που προτάθηκαν έχουν ως κύριο στοιχείο την επιμήκυνση των κλειδιών που χρησιμοποιούνται, κάτι που μπορεί να αυξάνει το κόστος και την πολυπλοκότητα των επιθέσεων αλλά σε καμία περίπτωση δεν τις καθιστά πρακτικά μη πραγματοποιήσιμες. Ακόμα και τα νέα συστήματα ασφάλειας που προτάθηκαν, όπως την επικύρωση 802.1X και το σύστημα της Wi-Fi Προστατευμένης Πρόσβασης (WPA), αν και βελτιώνουν ως ένα βαθμό την κατάσταση δεν αντιμετωπίζουν επαρκώς τα προβλήματα που έχουν δημιουργηθεί. Μάλιστα αρκετοί είναι και αυτοί που θεωρούν ότι και αυτά τα νέα συστήματα αντιμετωπίζουν αρκετά προβλήματα. Αν ψάξουμε στο internet έχουν αρχίσει και κυκλοφορούν πολλά άρθρα με τεχνικές σπασίματος ενός WPA κλειδιού, το οποίο θεωρείται πιο ισχυρό από το WEP.

Το σημαντικότερο πρόβλημα σε όλα τα συστήματα που έχουν προταθεί είναι η χρησιμοποίηση του αλγόριθμου RC4. Ο αλγόριθμος είχε ήδη αρκετά γνωστά προβλήματα και είναι απορίας άξιο γιατί υιοθετήθηκε ως αλγόριθμος κρυπτογράφησης. Υπάρχουν αρκετές προτάσεις για νέους αλγόριθμους κρυπτογράφησης με επικρατέστερη αυτή του Προτύπου Προηγμένης Κρυπτογράφησης (Advanced Encryption Standard, AES), αλλά η υιοθέτηση οποιαδήποτε από αυτούς απαιτεί την αλλαγή εξοπλισμού που χρησιμοποιείται για την υλοποίηση του προτύπου 802.11.

Άρα εύκολα κάποιος θα μπορούσε να καταλήξει στο συμπέρασμα ότι η ασφάλεια ενός δικτύου 802.11 βασίζεται κυρίως σε άλλες βοηθητικές τεχνολογίες που χρησιμοποιούνται, όπως για παράδειγμα τα Εικονικά Ιδιωτικά Δίκτυα (VPN). Ωστόσο και σε αυτή την περίπτωση το επίπεδο ασφαλείας που χρησιμοποιείται δεν είναι το μέγιστο δυνατόν αλλά το συμπέρασμα είναι ότι δεν είναι και ότι καλύτερο η ασφάλεια και η εξέλιξη ενός δημοφιλής και δοκιμασμένου προτύπου να βασίζεται σε ξένες προς σε αυτό τεχνολογίες και να μην παρέχει ολοκληρωμένες λειτουργίες.

Θα πρέπει όμως να σημειώσουμε για να είμαστε ακριβής, ότι το επίπεδο ασφάλειας που παρέχει ένα τοπικό δίκτυο 802.11 είναι ικανοποιητικό για οικιακή χρήση ή για μικρές επιχειρήσεις. Σε καμία περίπτωση πάντως δεν θα πρέπει να μεταδίδονται εμπιστευτικά δεδομένα χρησιμοποιώντας το πρότυπο 802.11, ενώ οι χρήστες θα πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα τα κλειδιά που χρησιμοποιούνται στις διαδικασίες ασφάλειας.

7.2 Μελλοντική έρευνα

Τέλος στην παράγραφο αυτή παρουσιάζονται κάποιες προτάσεις για μελλοντική έρευνα που προέκυψαν μετά από περάτωση αυτής της πτυχιακής εργασίας. Θα μπορούσε να μελετηθεί το πρόσφατα ανεπτυγμένο πρότυπο 802.11i, το οποίο αναπτύχθηκε για να αυξήσει το επίπεδο ασφάλειας. Το πρότυπο ορίζει μία νέα μέθοδο, που εγγυάται την ασφάλεια των δεδομένων στο MAC επίπεδο. Ονομάζεται CCMP και βασίζεται στον αλγόριθμο κρυπτογράφησης AES (Advanced Encryption Standard). Το CCMP παρέχει εμπιστευτικότητα (confidentiality), επικύρωση (authentication), ακεραιότητα (integrity) και προστασία από την επανάληψη πακέτων (replay protection). Βασίζεται στη χρήση του αλγόριθμου κρυπτογράφησης AES σε κατάσταση λειτουργίας CCM. Μια μελέτη του συγκεκριμένου προτύπου, σαν πιο σύγχρονου και εξελιγμένου για την ασφάλεια των ασύρματων δικτύων θα ήταν ενδιαφέρουσα.

Επίσης θα μπορούσαν να μελετηθούν οι επιθέσεις των Wi-Fi σκουληκιών και των επιθέσεων μεγάλης κλίμακας για εξαπάτηση χρηστών. Ακόμα να αναλυθεί η λειτουργία και η χρησιμότητα των honeypots. Ένα «σύστημα honeypot» είναι ουσιαστικά ένας υπολογιστής, ο οποίος δεν έχει ουσιαστικά χρήστες και δεν παρέχει κάποιου είδους υπηρεσία. Τα honeypots σχεδιάζονται, έτσι ώστε να είναι εύκολοι στόχοι και να ελκύουν τους κακόβουλους χρήστες όπως ένα βάζο με μέλι ελκύει τις μέλισσες.

Τα είδη επιθέσεων που μπορούν να εφαρμοστούν για το σπάσιμο ενός κλειδιούWPA και να υλοποιηθούν οι αντίστοιχες επιθέσεις. Ακόμα επιθέσεις που αφορούν το internet και τις ιστοσελίδες όπως Website spoofing, Phishing URLs, e- mail Scams. Επίσης μπορούν να περιγραφτούν πρακτικά κάποιοι μέθοδοι ασφάλειας ασυρμάτων δικτύων δημόσιας πρόσβασης και τα διάφορα είδη επιθέσεων που μπορούν να πραγματοποιηθούν.

Βιβλιογραφία

Εσωτερική Βιβλιογραφία

- Wi-Foo (Vladimirov & συν.,2004)
- How to cheat at Securing a Wireless Network (Brian Baker & συν.,2006)
- Wireless Security handbook (Aaron E. Earle,2006)
- 802.11 Wireless Networks: The Definitive Guide (O' Reilly & Matthew Gast ,2002)
- Real 802.11 Security: Wi-Fi Protected Access and 802.11i (Addison Wesley & William A. Arbaugh,2003)
- Wardriving and Wireless Penetration Testing (Chris Hurley και συν., 2006)
- Network Security Bible (Dr. Eric Cole & συν.,2005)
- Maximum Wireless Security (Cyrus Peikary & Seth Fogie: 2002)
- Wireless Security know it all (Praphul Chandra & συν.,2009)
- Wireless security for dummies (Barry Lewis & Peter T. Davis,2004)
- Cryptography and Network Security (William Stallingw,2006)

Παράρτημα Α Συντομογραφίες

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Packet
BSS	Basic Service Set
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOS	Denial-Of-Service
DS	Distributed System
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialization Vector
KSA	Key Scheduling Algorithm
LLC	Logical Layer Control
MAC	Medium Access Control
MIC	Message Integrity Check
MSDU	MAC Service Data Unit
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
OSA	Open System Authentication
OSI	Open System Interconnection
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
RADIUS	Remote Access Dial-In User Service
RARP	Reverse Address Resolution Protocol
SKA	Shared Key Authentication
SSID	Service Set Identifier
SSL	Secure Socket Layer
STA	Station
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access