ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ FIREWALL

Επιμέλεια Εργασίας: Κώστας Αθανάσιος

E- mail: mis105@uom.gr

Μάθημα: Δίκτυα υπολογιστών

Επιβλέπων καθηγητής: Αναστάσιος Α. Οικονομίδης

Τμήμα: Δ.Π.Μ.Σ Πληροφοριακά Συστήματα

Ακαδημαϊκό έτος 2010-2011

Περίληψη

Οι επιθέσεις με ιούς (viruses) και σκουλήκια (worms), βρίσκονται σε μεγάλη άνοδο, παράλληλα με την εκμετάλλευση των ευπαθειών του εξοπλισμού και τη χρήση της κοινωνικής μηχανικής, για την επίθεση στα εταιρικά δίκτυα. Οι προκύπτουσες παραβιάσεις δεδομένων επιτρέπουν την κλοπή και κακή χρήση προσωπικών και εταιρικών δεδομένων, με κόστος εκατομμυρίων ευρώ. Επίσης, η κίνηση του δικτύου αυξάνεται, λόγω της αύξησης των δικτύων υψηλής ταχύτητας, της υπολογιστικής πελάτη- διακομιστή, της απομακρυσμένης αποθήκευσης αλλά και τη συνεχή αύξηση των συσκευών των πελατών. Αυτή η αύξηση της κίνησης, σε συνδυασμό με την αυξημένη ζήτηση για πρόσβαση σε δεδομένα, δημιουργεί μεγαλύτερη έμφαση ώστε να βελτιωθεί η ασφάλεια δικτύων και πρωτοκόλλων. Ο στόχος της παρούσας εργασίας είναι να ωθήσει τον μη-ειδικό αναγνώστη στο να γνωρίσει τα προβλήματα και τις απειλές των δικτύων.

Abstract

Virus and worm attacks are on the rise, along with the exploitation of equipment vulnerabilities and the use of social engineering to attack corporate networks. The resulting data breaches allow the theft and misuse of personal and corporate data at a cost of millions of dollars. In addition, network traffic is increasing due to factors such as high-speed networks, service-orientated cloud computing, remote storage, and ever-increasing numbers of client devices. This increase in traffic, combined with the increased demand for data accessibility, places a greater emphasis on the need for network and protocol security. The goal of this paper is to make the non-specialist reader aware of the disadvantages and threats of networks.

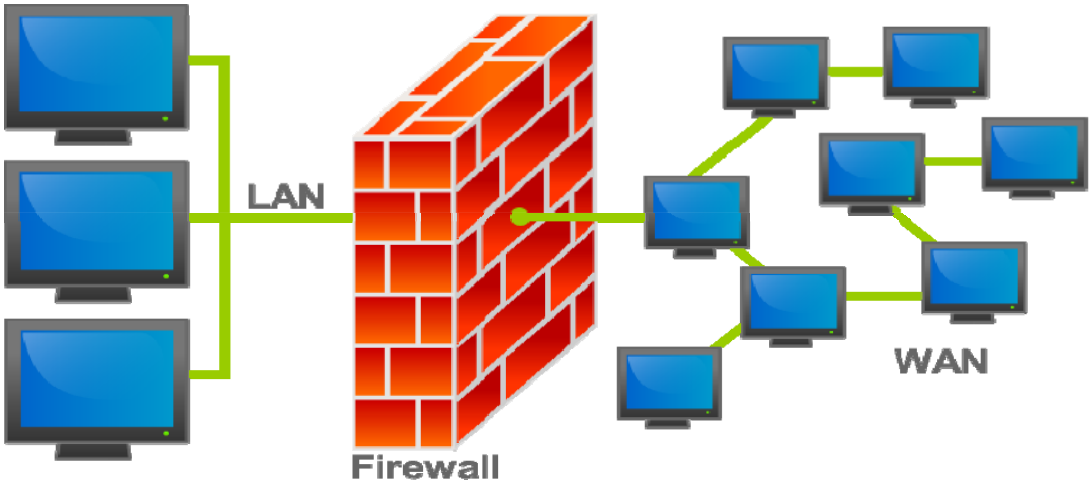
1. Εισαγωγή

Η ασφάλεια δικτύων έχει γίνει πολύ σημαντική παρά ποτέ στις ζωές μας, μιας και όλο και περισσότερα από τα προσωπικά και ευαίσθητα δεδομένα μας, κινούνται σε διάφορα δίκτυα. Αυτά τα δεδομένα δεν περιλαμβάνουν μόνο οικονομικές πληροφορίες, όπως ας πούμε μια on- line κράτηση που περιλαμβάνει τον αριθμό πιστωτικής κάρτας, αλλά επίσης, περιλαμβάνουν ιατρικές πληροφορίες που ταξιδεύουν σε γιατρούς, νοσοκομεία και ασφαλιστικούς οργανισμούς. Είναι ξεκάθαρο ότι σε απροστάτευτα δίκτυα μπορούν να διαρρεύσουν πληροφορίες, τόσο εκτός των δικτύων αυτών αλλά επίσης και μέσα σε αυτά. Οπότε, δεν είναι πλέον αρκετό το να προστατεύονται τα δεδομένα που βρίσκονται μόνο στους υπολογιστές και στις αποθηκευτικές συσκευές. Πρέπει να προστατεύονται τα δεδομένα και κατά τη μεταφορά τους. Η ασφάλεια δικτύων είναι ένα μια αυξανόμενη ανησυχία στην τεχνολογία πληροφοριών. Με τον όρο ασφάλεια εννοούμε την απαγόρευση της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα χωρίς επέμβαση. Με τον ορό υποδομή τεχνολογίας πληροφοριών (IT Infrastructure) εννοούμε την τεχνολογία ασφαλείας εντός του τοίχους ασφαλείας (firewall). Η γενική κατάσταση φαίνεται άκαμπτη. Αυτό που πριν από 10 χρόνια ξεκίνησε σαν μη εξουσιοδοτημένη πρόσβαση σε δίκτυα για προσφιλή ενασχόληση (hobby), τώρα εξελίσσεται σε κλοπή δεδομένων από οργανισμούς, κυβερνήσεις και πολίτες για την δημιουργία κέρδους, οι οποίοι απειλούν την αξιοπιστία του διαδικτύου (Internet) και όλων των υπολοίπων δικτύων που είναι συνδεδεμένα με αυτό.

2. Firewalls και Ασφάλεια Δικτύου

Ως firewall (τείχος προστασίας), ορίζεται το λογισμικό ή το υλικό (hardware) που επιτρέπει σε ορισμένους εξωτερικούς χρήστες με συγκεκριμένα χαρακτηριστικά να έχουν πρόσβαση σε ένα προστατευμένο δίκτυο ή δικτυακό τόπο (site). Στην τυπική του μορφή, ένα τέτοιο προστατευτικό τείχος επιτρέπει στους έσω να έχουν πλήρη και χωρίς περιορισμούς πρόσβαση σε υπηρεσίες έξω από το συγκεκριμένο δίκτυο, ενώ παραχωρεί την άδεια πρόσβασης εκ των έξω επιλεκτικά, με βάση κωδικούς πρόσβασης, ονόματα χρηστών, διευθύνσεις του διαδικτύου (Internet IP address) ή ονομασίες περιοχών (domain name).
(Πανεπιστήμιο Πειραιώς, Εφαρμογές Ηλεκτρονικών Υπολογιστών)

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο (Internet) και το τοπικό/ εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) διαθέτει μεσαίο επίπεδο εμπιστοσύνης.



Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική, είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default- allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες. (Bellovin,S, n.d), (Ingham K., & Forrest S., 2009).

3. Γενικά στοιχεία ασφαλείας

Πριν την έλευση των μεταγωγέων (switches), τα δίκτυα μπορούσαν να παραβιαστούν με την παρακολούθηση της κίνησης του δικτύου μέσα από ένα διανομέα (hub). Με την έλευση των switches, οι υποκλοπές έχουν γίνει πιο δύσκολες. Πολλά switches

επιτρέπουν την παρακολούθηση της κίνησης του δικτύου, με την τοποθέτηση μιας από τις πόρτες του switch σε κατάσταση παρακολούθησης. Η κατάσταση παρακολούθησης, είναι ένα νόμιμο μέσο επίλυσης προβλημάτων του δικτύου, αλλά ταυτόχρονα κάνει ευάλωτο το δίκτυο σε οποιονδήποτε έχει πρόσβαση στο switch. Είναι επίσης πιθανή η υποκλοπή σε δίκτυα οπτικών ινών, με τη δημιουργία μιας εκτροπής στην κίνηση πολλαπλής λειτουργίας του δικτύου. Η εκτροπή επιτρέπει σε αρκετό φως να φεύγει από την οπτική ίνα, με αποτέλεσμα να είναι πιθανές οι υποκλοπές στο δίκτυο. Τα ασύρματα δίκτυο έχουν γίνει υπέρ- κυρίαρχα στην πρόσβαση στο διαδίκτυο, χρησιμοποιώντας το ασύρματο μέσο σαν πρώτο κρίκο. Ιστορικά, τα ασύρματα δίκτυα άντεχαν μικρότερη ασφάλεια και μπορούσαν εύκολα να παρακολουθηθούν από κάποιον μέσα στην εμβέλεια του ασύρματου σημείου πρόσβασης. Τα τελευταία χρόνια, μια ολόκληρη σουίτα από ασύρματα πρότυπα ασφαλείας έχουν εισαχθεί και καθιερωθεί ευρέως. Προσφέρουν πιστοποίηση και εμπιστευτικότητα δεδομένων σε ασύρματες επικοινωνίες, από μια δοσμένη συσκευή στο άμεσο Επίπεδο 2 (Layer 2) των γειτόνων. Αυτά τα πρότυπα, καθιερώθηκαν από την IEEE. Ένα από τα κυρίαρχα πρότυπα ασφαλείας, είναι το 802.11i με πολλά παρελκόμενα παράγωγα πρότυπα που έχουν ήδη οριστεί. Αυτά τα πρότυπα προσφέρουν επιπρόσθετες υπηρεσίες ασφαλείας στα ασύρματα δίκτυα. Όλοι οι τρόποι ασύρματης ασφάλειας, αναλύονται σε επόμενα κεφάλαια. (Cornett, L., & Grewal, K., & Long, M., & Millier, M., & Williams, 2009).

Το λογισμικό το οποίο υποστηρίζει την επικοινωνία δεδομένων σε κάθε μια από τις διάφορες συσκευές σε οποιαδήποτε διαδρομή δεδομένων στο Internet, οργανώνεται σε στρώματα. Κάθε στρώμα εκτελεί μια διαφορετική λειτουργία, ή μεταβάλλει τα δεδομένα καθώς περνούν μέσα από τις στοίβες των επιπέδων. Αν κάποιος εισβολέας, μπορεί να πάρει κάποιο κομμάτι από αυτό το κακόβουλο λογισμικό που έχει εισαχθεί

ανάμεσα σε αυτά τα στρώματα, ο εισβολέας μπορεί παρακολουθεί ή ακόμα να εισάγει κακόβουλα προγράμματα σε άλλα συστήματα, κατά μήκος του καναλιού επικοινωνίας. (Cornet, et al, 2009)

3.1 Άμυνα δικτύου

Η άμυνα ενάντια σε αυτές τις απειλές ρυθμίζεται σήμερα με την εγκατάσταση πολυάριθμων τεχνολογιών ασφαλείας, όπως τον έλεγχο πρόσβασης δικτύου (NAC) και τα αντί-υιικά προγράμματα σε πλατφόρμες αλλά και εντός του δικτύου. Στο δίκτυο, οι επιχειρήσεις σήμερα εγκαθιστούν συσκευές σε κάποιο σημείο της υπάρχουσας υποδομής, έτσι ώστε να διαχωρίσουν την εξωτερική μη αξιόπιστη περιοχή του δικτύου, μέσα σε αυτήν και το διαδίκτυο (Internet), από την αξιόπιστη εσωτερική, που προφυλάσσεται φυσικά σαν τμήμα του δικτύου. Αυτές οι συσκευές, ανιχνεύουν και εμποδίζουν επιθέσεις από το διαδίκτυο, σαρώνουν εισερχόμενα πακέτα για ιούς και άλλο κακόβουλο λογισμικό και αμύνονται ενάντια στις επιθέσεις άρνησης υπηρεσίας. Αυτή η άμυνα με συσκευές λειτουργεί λιγότερο αποτελεσματικά για πολλούς λόγους. Αρχικά, πολλές επιθέσεις έρχονται εσωτερικά από την αμυντική περίμετρο, από πηγές που θεωρητικά θα έπρεπε να είναι έμπιστες, συμπεριλαμβανομένων των υπαλλήλων και των εργολάβων για παράδειγμα. Στη συνέχεια, είναι όλο και πιο κοινό να ανοιχτούν πόρτες μέσα από την περίμετρο ασφαλείας, ώστε να παρέχεται πρόσβαση σε συγκεκριμένους τύπους ρευμάτων κίνησης, όπως το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), πρωτόκολλο μεταφοράς αρχείων (FTP) κλπ. Έτσι σχεδιάζονται οι επιθέσεις, με στόχο να διαπερνούν αυτά τα κενά στα συστήματα. (Kent, S. 2005).

Σαν αποτέλεσμα αυτών, η προστατευμένη περίμετρος κινείται πιο κοντά στα συστήματα που έχει σχεδιαστεί για να προστατεύει, όπως οι εξυπηρετητές (servers)

και οι αποθηκευτικές συσκευές (storage media). Η αυξανόμενη πρόσβαση, ακόμα και μέσα από τον οργανισμό, δρομολογείται μέσα από συσκευές έλεγχου εισβολής, ανίχνευσης και απαγόρευσης. Έτσι, το στρώμα ασφαλείας ανάμεσα στην περίμετρο ασφαλείας και τα συστήματα, γίνεται λεπτότερο. Η λογική επέκταση ασφαλείας, είναι ο ορισμός της περιμέτρου ακριβώς δίπλα στους ίδιους τους εξυπηρετητές. Αυτό όμως θα σήμαινε ότι δημιουργήθηκε μια άμυνα σε βάθος για κάθε εξυπηρετητή. Μια τέτοια λύση, δεν είναι πρακτική στη σημερινή υπολογιστική, δεδομένου του υπάρχοντος οικονομικού βάρους στους οργανισμούς. Οι πόροι οι οποίοι μεταφέρονται από την παραγωγική εργασία στα συστήματα ασφαλείας, είναι ακόμα περισσότερο αντιοικονομικοί από οτιδήποτε άλλο. (Kent, S. 2005).

Μια εναλλακτική λύση για να μειωθεί το κόστος αμυντικής λειτουργίας σε κάθε εξυπηρετητή, είναι να δημιουργηθεί το ίδιο επίπεδο προστασίας στα πρωτοκόλλα επικοινωνίας, επιτρέποντας στα δεδομένα να προστατεύονται καθώς κινούνται εντός του οργανισμού αλλά και κατά μήκος του διαδικτύου. Κατά μια έννοια, η μερική προστασία αυτού του τύπου χρησιμοποιείται σε μεγάλο βαθμό σήμερα. Τα Ιδιωτικά Εικονικά Δίκτυα (VPN) δημιουργούν ένα προστατευτικό τούνελ στο οποίο, τα δεδομένα κρυπτογραφούνται καθώς κινούνται μεταξύ οργανισμών και των απομακρυσμένων υπολογιστών που λειτουργούν στο διαδίκτυο. Τα VPN's χρησιμοποιούνται με μεγάλο αποτέλεσμα τα τελευταία χρόνια , αλλά ακόμα δεν προστατεύουν από υπερχειλίσεις απροστάτευτων δεδομένων μέσα στην αμυντική περίμετρο που υπάρχει, και συχνά είναι ακατάλληλα για χρήση από χρήστες σε απομακρυσμένους υπολογιστές. (Cornet, et al, 2009)

4. Ασφάλεια πρωτοκόλλων

Η ασφάλεια πρωτοκόλλων είναι ένας γενικός όρος, που χρησιμοποιείται για να περιγράψει τις υπηρεσίες κρυπτογράφησης που παρέχονται στα πακέτα δεδομένων του δικτύου. Η ροη δεδομένων μέσα σε ένα δίκτυο μπορεί να πάρει πολλές μορφές και μπορεί να διαφοροποιηθεί από τις παρεχόμενες υπηρεσίες εντός του δικτύου. Αυτές μπορεί να ποικίλουν, από πρωτόκολλα επικοινωνίας που διαχειρίζονται υπηρεσίες δικτύων, άμεση ανταλλαγή μηνυμάτων ανάμεσα σε διαφορετικούς κόμβους του δικτύου, εγκατάσταση απομακρυσμένων συνεδριών και ροών ανάμεσα σε δυο ή περισσότερους κόμβους του δικτύου για το σκοπό της επικοινωνίας δεδομένων ανάμεσα σε αυτούς τους κόμβους, καθώς επίσης και για έναν μεγάλο αριθμό από άλλες εργασίες του δικτύου. Πολλές από αυτές τις υπηρεσίες μπορούν να χαρτογραφηθούν σε διαφορετικά στρώματα του μοντέλου OSI. (Cornet, et al, 2009)

Το μοντέλο OSI, ξεχωρίζει την αρχιτεκτονική του δικτύου σε πολλαπλά επίπεδα, όπου το κάθε επίπεδο πραγματοποιεί μια λογική λειτουργία και αλληλεπιδρά με τα επίπεδα που βρίσκονται πάνω και κάτω. Τα ανώτερα επίπεδα σε αυτό το μοντέλο βασίζονται σε υπηρεσίες που παρέχονται από τα κατώτερα επίπεδα, με μια εγγύηση του τι είδους είναι αυτές οι υπηρεσίες, χωρίς να χρειάζεται να κατανοήσουν με ποιον τρόπο μπορεί να παρέχονται αυτές οι υπηρεσίες. Ένα παράδειγμα αυτού του μοντέλου φαίνεται στο πως το πρωτόκολλο μεταφοράς (TCP) παρέχει υπηρεσίες προσανατολισμένης σύνδεσης σε ανώτερα επίπεδα, ενώ βασίζεται σε υπηρεσίες δικτύου από το πρωτόκολλο IP που βρίσκεται σε επίπεδο κατώτερο. Το επίπεδο πρωτοκόλλου διαδικτύου (IP), βασίζεται στο επίπεδο συνδέσμου δεδομένων και στα φυσικά επίπεδα πιο κάτω για να παρέχει επιπλέον υπηρεσίες. Αυτές οι υπηρεσίες μπορεί να είναι εξαρτημένες από υποκείμενα μέσα επικοινωνίας, χωρίς να χρειάζονται επιπλέον πληροφορίες σε αυτό το υποκείμενο μέσο. (Canavan, J.E, 2001).

4.1 Υπηρεσίες ασφαλείας OSI

Υπάρχουν 8 υπηρεσίες ασφαλείας σχετικές με το μοντέλο OSI:

a. Αναγνώριση: ομότιμες οντότητες πρέπει να αναγνωρίζονται.
b. Πιστοποίηση: παρέχει πιστοποίηση για την ταυτότητα των οντοτήτων που επικοινωνούν ή της προέλευσης των δεδομένων.
c. Έλεγχος πρόσβασης: υπάρχουν κανόνες για την προστασία ενάντια στην μη εξουσιοδοτημένη πρόσβαση και χρήση πηγών στο OSI. Για να προστατεύουν πολύτιμα δεδομένα, αυτοί οι κανόνες καθορίζουν υποχρεωτικούς ελέγχους πρόσβασης.
d. Εμπιστευτικότητα δεδομένων: παρέχει προστασία ενάντια στη μη εξουσιοδοτημένη γνωστοποίηση.
e. Ακεραιότητα επικοινωνίας: επιτυγχάνει ακριβή μετάδοση δεδομένων από την πηγή στον προορισμό.
f. Διαθεσιμότητα υπηρεσίας: επιτυγχάνει τη μικρότερη αποδεκτή, συνεχόμενη και παρεχόμενη υπηρεσία.
g. Ευθύνη: ανιχνεύει δραστηριότητες που επηρεάζουν την υπεύθυνη οντότητα.
h. Μη αποκήρυξη: στόχος της είναι να προστατεύσει τον αποστολέα και/ ή τον παραλήπτη ενάντια σε χρηστή που λαθεμένα αρνείται την αποδοχή ή μετάδοση των δεδομένων.

(Brenton, & Hunt, 2003)

Πίνακας 1: Σχέση υπηρεσιών και επιπέδων

	Επίπεδα						
	1	2	3	4	5	6	7
Πιστοποίηση							
a. Δεδομένα Προέλευσης			X	X			X
b. Ομότιμη Οντότητα			X	X			X
Έλεγχος πρόσβασης							
a. Πιστοποίηση χρήστη							X

b. Πιστοποίηση ομότιμης οντότητας			X	X		X
Ακεραιότητα							
a. Με σύνδεση			X	X		X
b. Χωρίς σύνδεση			X	X		X
Εμπιστευτικότητα							
a. Με σύνδεση	X	X	X	X		X
b. Χωρίς Σύνδεση		X	X	X		X
c. Επιλεκτικό πεδίο						X
d. Ροή κυκλοφορίας	X		X			X
Άρνηση							
a. Δημιουργού						X
b. Παραλήπτη						X

(Pozzo, M., & Gray, T., 1987)

4.2 Μηχανισμοί ασφαλείας OSI

a. Μηχανισμοί ελέγχου δρομολόγησης: διαλέγει τα πιο ασφαλή υπό-δίκτυα και συνδέσμους.
b. Μηχανισμοί ακεραιότητας δεδομένων: αποτελούνται από κώδικες μπλοκαρίσματος και κρυπτογραφικό έλεγχο λειτουργιών.
c. Κρυπτογράφηση: μπορεί να παρέχει εμπιστευτικότητα δεδομένων και δεδομένα ροής της κυκλοφορίας.
d. Μηχανισμοί ψηφιακής υπογραφής: μέρος κρυπτογραφίας ως διαδικασία υπογραφής.
e. Μηχανισμοί πιστοποίησης συναλλαγών: κωδικοί και κρυπτογραφικές μέθοδοι.
f. Μηχανισμοί κίνησης: προστασία ενάντια στην ανάλυση κίνησης.

(Brenton, & Hunt, 2003)

Πίνακας 2: Σχέση υπηρεσιών και μηχανισμών

	Επίπεδα						
	1	2	3	4	5	6	7
Έλεγχος δρομολόγησης			X				

Ακεραιότητα δεδομένων			X	X	X	
Κρυπτογράφηση	X	X	X	X	X	
Ψηφιακή υπογραφή	X	X		X	X	
Ανταλλαγή πιστοποίησης			X	X		
Συνθήκες κίνησης			X			X
Πιστοποίηση συμβολαίου					X	X
Έλεγχος πρόσβασης			X	X		X

(Pozzo, M., & Gray, T., 1987)

5. Ασύρματα δίκτυα

Η κυριότερη διαφορά μεταξύ ενσύρματων και ασύρματων δικτύων είναι ο τρόπος με τον οποίο μεταδίδονται τα δεδομένα. Όσο αφορά τα προβλήματα ασφαλείας, η κύρια διαφορά ανάμεσα σε αυτά τα δυο είδη δικτύων είναι ο τρόπος με τον οποίο γίνεται η πρόσβαση στα μεταδιδόμενα δεδομένα. Στα ενσύρματα δίκτυα, αυτό γίνεται με υποκλοπή του μέσου (καλώδιο) που χρησιμοποιείται για την επικοινωνία του δικτύου. Στα ασύρματα δίκτυα, το μέσο επικοινωνίας είναι ο αέρας. Η μεταδιδόμενη πληροφορία, μέσα από τη συχνότητα μετάδοσης, μπορεί να γίνει διαθέσιμη από διάφορους εξοπλισμούς, οι οποίοι βρίσκονται εύκολα, γρήγορα και φθηνά στην αγορά. Από τα πρώτα στάδια ανάπτυξης των ασύρματων δικτύων, η ασφάλειά τους θα έπαιζε μεγάλο ρόλο, σύμφωνα με τους ειδικούς. Τα ασύρματα δίκτυα είναι παραδοσιακά λιγότερο ασφαλή σε σχέση με τα ενσύρματα, από τη στιγμή που η μετάδοση της πληροφορίας γίνεται μέσω του αέρα και ο καθένας μπορεί να έχει πρόσβαση σε αυτήν. (Bulbul, H. & Batmaz, I. & Ozel, M, 2008)

5.1 Ασφάλεια στα ασύρματα δίκτυα

Υπάρχουν τρία είδη ασύρματης ασφάλειας, κάθε ένα από τα οποία χρησιμοποιεί τον ομώνυμο αλγόριθμο, που παρέχει την απαιτούμενη κρυπτογράφηση της μεταδιδόμενης πληροφορίας. Αυτά είναι: η Ισοδύναμη ενσύρματη ασφάλεια (Wired Equivalent Privacy ή WEP), η Ασύρματη προστατευόμενη πρόσβαση (Wi-fi Protected Access ή WPA) και το Δίκτυο αυτοδύναμης ασφάλειας (Robust Security Network ή RSN). (Mishra, A., & Petroni, & N.L., & Arbaugh, W.A., & Fraser, T, 2004)

5.2 Ο μηχανισμός ασφαλείας WEP

Ο WEP αρχικά προοριζόταν στο να δώσει στους χρήστες την αίσθηση ότι βρίσκονται σε ενσύρματα δίκτυα με την αντίστοιχη ασφάλεια. Ο κύριος προορισμός του WEP δεν ήταν να παρέχει ένα επίπεδο ασφαλείας υψηλότερο από αυτό που υπήρχε στα ενσύρματα δίκτυα, αλλά ένα επίπεδο ασφαλείας ιδίου μεγέθους. Παρόλα αυτά, η πρακτική του χρήση έδειξε ότι ο WEP ήταν αρκετά υποδεέστερος από την ασφάλεια των ενσύρματων δικτύων. (Wong, S, 2003)

Όταν ο WEP είναι ενεργός, κάθε 802.11 πακέτο κρυπτογραφείται ξεχωριστά με ένα Rivest Cipher 4 (RC4) κύμα και παράγεται ένα κλειδί των 64-bit. Αυτό το κλειδί αποτελείται από 24-bit διάνυσμα αρχικοποίησης (Initialization Vector ή IV) και ένα κλειδί WEP των 40-bit. Το κρυπτογραφημένο πακέτο παράγεται με αποκλειστική διάζευξη του αρχικού πακέτου και του κύματος RC4. Το IV επιλέγεται από τον αποστολέα και μπορεί να αλλαχθεί περιοδικά, έτσι ώστε κάθε πακέτο να μην κρυπτογραφείται με το ίδιο κύμα RC4. Όπως αναφέρθηκε πριν, ο WEP χρησιμοποιεί το RC4 κύμα κρυπτογράφησης με ένα διάνυσμα αρχικοποίησης των 24-bit για κρυπτογράφηση. Η σχεδίαση του WEP αφήνει το σύστημα ευάλωτο σε πολλές

περιοχές, και ένα από τα πιο ευάλωτα μέρη είναι το διάνυσμα αρχικοποίησης των 24-bit, το οποίο μπορεί να οδηγήσει σε επαναχρησιμοποίηση του κλειδιού κρυπτογράφησης. (Wong, S, 2003)

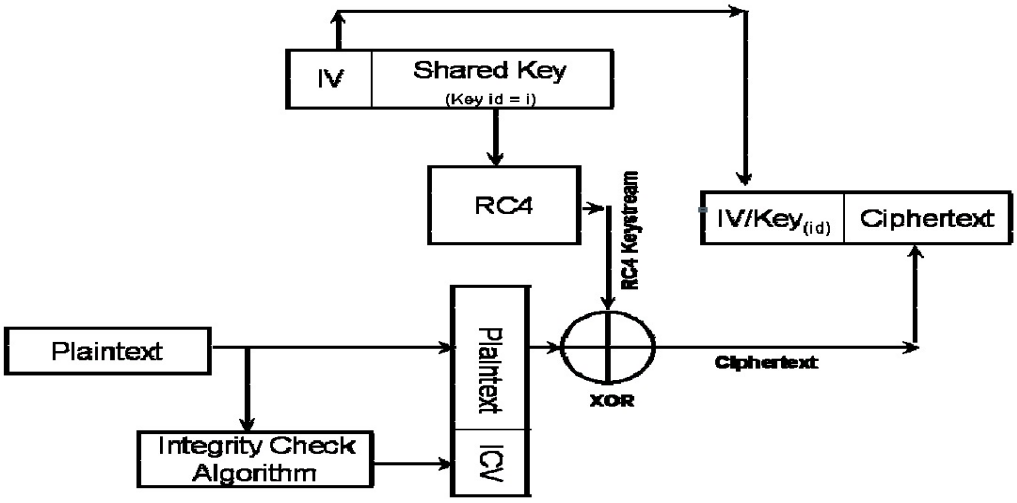


Figure -1 WEP Encryption

(Kerry, S, 2001).

5.3 Οι αδυναμίες του WEP

Η χρήση κύριων κλειδιών άμεσα: Από την κρυπτογραφική άποψη, η χρήση κύριων κλειδιών κρυπτογράφησης άμεσα δεν συνίσταται. Τα κύρια κλειδιά πρέπει μόνο να χρησιμοποιούνται για την παραγωγή προσωρινών κλειδιών. (Boland, H., & Mousavi, H, 2004)

Μικρό μέγεθος κλειδιού: Το μέγεθος κλειδιού για τον WEP είναι 40-bit, το οποίο έχει καταταγεί σα μια από τις μεγαλύτερες αδυναμίες του. Την προηγούμενη 10ετία, τα κλειδιά των 40-bit, θεωρούνταν αξιόπιστα για μερικές εφαρμογές, όπως την προστασία από απλή παρακολούθηση των δεδομένων. Το πρότυπο 802.11 δεν καθορίζει κάποια αλλά κλειδιά διαφορετικού μεγέθους, παρά μόνο τα υπάρχοντα των 40-bit. Οι περισσότεροι πωλητές χρησιμοποιούν κλειδιά με μέγεθος που κυμαίνεται

στα 104-232 bit, τα όποια είναι πιο ανθεκτικά σε επιθέσεις. . (Boland, H., & Mousavi, H, 2004)

Έλλειψη διαχείρισης κλειδιού: Η διαχείριση κλειδιού δεν καθορίζεται συγκεκριμένα στο WEP. Από τη στιγμή λοιπόν που δεν καθορίζονται, τότε τα κλειδιά δεν θα ανανεώνονται, θα είναι μεγάλης διάρκειας ζωής και χαμηλής ποιότητας. Τα περισσότερα ασύρματα δίκτυα τα οποία χρησιμοποιούν ασφάλεια WEP, μοιράζονται το ίδιο κλειδί για κάθε κόμβο του δικτύου. Τα σημεία πρόσβασης και οι σταθμοί των πελατών πρέπει να προγραμματίζονται με το ίδιο κλειδί. Από τη στιγμή που η αλλαγή κλειδιών είναι μια δύσκολη διαδικασία, τα κλειδιά παραμένουν τα ιδία για μεγάλο χρονικό διάστημα και δεν ανανεώνονται από τους διαχειριστές των δικτύων. (Gast M, 2002)

Η χρήση του RC4: Η εφαρμογή του RC4 θωρείται ότι έχει αδύναμα κλειδιά, που σημαίνει ότι υπάρχει μεγαλύτερη συσχέτιση μεταξύ του κλειδιού και του τελικού αποτελέσματος, σε αντίθεση με αυτό που πρέπει να γίνεται. Είναι εύκολο να προσδιοριστεί, ποια πακέτα έχουν κρυπτογραφηθεί με το αδύναμο κλειδί. Από τη στιγμή που τα τρία πρώτα bit λαμβάνονται από το IV, το οποίο στέλνεται χωρίς κρυπτογράφηση στο κάθε πακέτο, αυτή η αδυναμία μπορεί να «αξιοποιηθεί» από διάφορες παθητικές επιθέσεις. . (Boland, H., & Mousavi, H, 2004)

Επαναχρησιμοποιούμενα και μικρού μεγέθους IV: Ανεξάρτητα από το μέγεθος του κλειδιού, το μέγεθος του IV το οποίο είναι 24-bit, μπορεί να παράγει 16.777.216 διαφορετικά RC4 κύματα κρυπτογράφησης για ένα δοσμένο κλειδί. Σε ένα σχετικά απασχολημένο δίκτυο, αυτός ο αριθμός μπορεί εύκολα να ξεπεραστεί μέσα σε μερικές ώρες και η επαναχρησιμοποίηση τους γίνεται αναπόφευκτη. Αν με κάποιο

τρόπο ,μπορεί να βρεθεί το κύμα κρυπτογράφησης RC4, κάποιος εισβολές μπορεί να αποκρυπτογραφήσει μεταγενέστερα πακέτα, που είχαν κρυπτογραφηθεί με το ίδιο IV. Από τη στιγμή που υπάρχουν το πολύ 16.777.216 τιμές, ο τρόπος με τον οποίο επιλέγεται το IV κάνει τη διαφορά. Δυστυχώς, ο WEP δεν προκαθορίζει τον τρόπο επιλογής, δηλαδή το πόσο συχνά πρέπει να αλλάζουν τα IV. Μερικές εγκαταστάσεις ξεκινούν το IV από το μηδέν και το αυξάνουν σταδιακά για κάθε πακέτο, μέχρις ότου περάσουν οι 16.777.216 τιμές και ξαναφτάσουμε στο 0. Με μια τυχαία επιλογή του IV, υπάρχει 50% μικρότερη πιθανότητα επαναχρησιμοποίησης μετά από περίπου 5000 πακέτα.. (Boland, H., & Mousavi, H, 2004)

Η αδυναμία του αλγορίθμου: Ο WEP ICV βασίζεται στον κυκλικό έλεγχο πλεονασμού CRC-32, έναν αλγόριθμο που μπορεί να ανιχνεύει το θόρυβο και τα κοινά λάθη στη μετάδοση. Ο CRC-32 είναι πολύ καλός για τον έλεγχο της ακεραιότητας και για την εύρεση λαθών, αλλά δεν είναι καλή επιλογή από κρυπτογραφική σκοπιά. Ο CRC-32 ICV, είναι μια γραμμική λειτουργία του μηνύματος που σημαίνει ότι ένας εισβολέας μπορεί εύκολα να μεταβάλει ένα κρυπτογραφημένο μήνυμα ώστε το ICV να δείχνει αυθεντικό, μετά από αυτή την αλλαγή. Οποίος είναι ικανός να μεταβάλει κρυπτογραφημένα πακέτα, μπορεί να προκαλέσει μια σειρά από επιθέσεις. Αυτός που κάνει την επίθεση, μπορεί να κάνει το ασύρματο σημείο πρόσβασης του θύματος, να κρυπτογραφεί τα πακέτα για αυτόν. Αυτό γίνεται πολύ εύκολα, με την κυρίευση ενός κρυπτογραφημένου πακέτου, αλλάζοντας τη διεύθυνση προορισμού του κάθε πακέτου, ώστε να είναι η IP διεύθυνση του εισβολέα.. (Gast M, 2002)

Εύκολη σφυρηλάτηση των μηνυμάτων πιστοποίησης: Το 802.11 στάνταρ, καθορίζει 2 τύπους πιστοποίησης , την πιστοποίηση ανοιχτού συστήματος (Open System) και την πιστοποίηση κοινόχρηστου κλειδιού (Shared Key). Η πιστοποίηση

μαζί με τη WEP ασφάλεια, στην πραγματικότητα μειώνει την συνολική ασφάλεια του δικτύου, αφού κάνει πιο εύκολο σε εισβολείς , να μαντεύουν το WEP κλειδί. Η πιστοποίηση κοινόχρηστου κλειδιού περιλαμβάνει τη κρυπτογράφηση του δημοσίου κλειδιού με την κρυπτογράφηση μιας πρόκλησης. Το πρόβλημα εδώ είναι, ότι κάποιος μπορεί να παρακολουθεί την κρυπτογραφημένη απάντηση. Αυτοί λοιπόν, μπορούν να προσδιορίσουν το κύμα RC4 που χρησιμοποιείται στην κρυπτογράφηση της απάντησης, και χρησιμοποιούν αυτό το κύμα ώστε να κρυπτογραφήσουν οποιοδήποτε πρόκληση λάβουν στο μέλλον. Έτσι, παρακολουθώντας μια επιτυχημένη πιστοποίηση, αυτός που κάνει την επίθεση μπορεί να πλαστογραφήσει μια πιστοποίηση. Το μόνο πλεονέκτημα της πιστοποίησης κοινόχρηστου κλειδιού είναι ότι μειώνει την ικανότητα του επιτιθέμενου να δημιουργεί επιθέσεις άρνησης υπηρεσίας, με την αποστολή πακέτων σκουπιδιών. (Gast M, 2002)

5.4 Ο μηχανισμός προστασίας ασύρματης πρόσβασης WPA

Ο WPA σχεδιάστηκε ώστε να βελτιώνει τα προβλήματα ασφαλείας που παρουσιάστηκαν στο WEP. Η τεχνολογία σχεδιάστηκε ώστε να δουλεύει με τα υπάρχοντα προϊόντα ασύρματης πρόσβασης που έχουν λειτουργήσει με WEP ασφάλεια. Οι κύριες βελτιώσεις της νέας ασφάλειας είναι οι εξής:

- **Βελτιωμένη κωδικοποίηση δεδομένων μέσα από το πρωτόκολλο ακεραιότητας προσωρινού κλειδιού (TKIP).** Αυτό το πρωτόκολλο ανακατεύει τα κλειδιά, χρησιμοποιώντας έναν αλγόριθμο κατακερματισμού, προσθέτοντας ένα στοιχείο ελέγχου ακεραιότητας και βεβαιώνοντας ότι τα κλειδιά δεν έχουν μετριαστεί. Το TKIP είναι μια λειτουργιά κατακερματισμού προσωρινού κλειδιού, η οποία είναι εναλλακτική του WEP, ώστε να διορθώνει όλα τα προβλήματα ασφαλείας και δεν χρειάζεται αλλαγή

υλικού (hardware). Το TKIP χρησιμοποιείται το ίδιο RC4 κύμα κρυπτογράφησης με το WEP. Το κλειδί σε αυτή την περίπτωση είναι 128- bit και ονομάζεται προσωρινό κλειδί. Το TKIP χρησιμοποιεί ένα διάνυσμα αρχικοποίησης των 48- bit, το οποίο χρησιμοποιείται σα μετρητής. Ακόμα και αν το προσωρινό κλειδί μοιράζεται, όλες οι σχετικές οντότητες παράγουν ένα διαφορετικό κλειδί RC4. Από τη στιγμή που οι επικοινωνούντες οντότητες εκτελούν παραγωγή κλειδιού δύο φάσεων, ενός μοναδικού πακέτου που ονομάζεται «Κλειδί πακέτου», αυτό είναι το κλειδί που χρησιμοποιείται για το ρεύμα RC4. (Fluhrer, S., Mantin, I., Shamir, A, n.d)

- Πιστοποίηση χρήστη, η οποία λείπει από τον WEP μηχανισμό, μέσα από το πρωτόκολλο εκτεταμένης πιστοποίησης (EAP). Ο WEP μεθοδεύει την πρόσβαση σε ένα ασύρματο δίκτυο, σε μια συγκεκριμένη διεύθυνση ελέγχου της πρόσβασης των μέσων (MAC Address) του υλικού του δικτύου, που είναι σχετικά απλό να κλαπεί. Το EAP δημιουργείται πάνω σε μια κωδικοποίηση πιο ασφαλούς δημόσιου κλειδιού, για να μπορέσει να επιβεβαιώσει ότι μόνο τα πιστοποιημένα δίκτυα μπορούν να προσπελάσουν το υπάρχων δίκτυο.
- Ακεραιότητα, ένας νέος μηχανισμός, χρησιμοποιείται για την ακεραιότητα, ο οποίος ονομάζεται κώδικας ακεραιότητας μηνυμάτων (MIC). Ο κώδικας ακεραιότητας μηνυμάτων χρησιμοποιείται στο να ανακαλύπτει λάθη σε περιεχόμενα δεδομένων, είτε λόγω λαθών μετάδοσης είτε πιθανών αλλαγών από εισβολείς. (Potter, B, 2003)

5.5 Ο μηχανισμός αυτοδύναμης ασφάλειας δικτύων RSN

Η αυτοδύναμη ασφάλεια δικτύων χρησιμοποιεί δυναμική διαπραγμάτευση της πιστοποίησης και αλγόριθμους κρυπτογράφησης ανάμεσα στα σημεία πρόσβασης και στις φορητές συσκευές. Τα σχήματα πιστοποίησης που βρίσκονται στο σχέδιο αυτό βασίζονται στο 802.1X και στο πρωτόκολλο επεκτάσιμης πιστοποίησης (EAP). Ο αλγόριθμος κρυπτογράφησης είναι ο AES (Advanced Encryption Standard). Η δυναμική διαπραγμάτευση της πιστοποίησης και οι αλγόριθμοι κρυπτογράφησης, επιτρέπουν στην RSN να εξελιχθεί. Η χρήση δυναμικής διαπραγμάτευσης καθώς και των EAP- AES δίνει στην RSN τα πρωτεία ασφαλείας σε σχέση με τα WEP- WPA. Ωστόσο, ο RSN δε λειτουργεί σωστά σε κληροδοτημένες συσκευές. Δυστυχώς, μόνο οι τελευταίες συσκευές έχουν την απαιτούμενη δυνατότητα να επιταχύνουν τους αλγόριθμους σε πελάτες και σημεία πρόσβασης, παρέχοντας την αναμενόμενη απόδοση των σημερινών προϊόντων ασύρματων δικτύων. (Gueron, S, (2008)

Πίνακας 3	**Σύγκριση μηχανισμών**		
Χαρακτηριστικά μηχανισμών	*WEP*	*WPA*	*RSN*
Μηχανισμός κρυπτογράφησης	RC4	RC4/TKIP	AES/CCMP,CCMP/TKIP
Μέγεθος κλειδιού	40 bit	128 bit	128 bit
Κλειδί κρυπτογράφησης ανά πακέτο	Συνεχόμενη	Μικτή	Όχι απαραίτητη
Διαχείριση κλειδιού	Καμία	802.1X	802.1X
Αλλαγή κλειδιού	Καμία	Για κάθε πακέτο	Όχι απαραίτητη
Μέγεθος IV	24 bit	48 bit	48 bit
Πιστοποίηση	Αδύναμη	802.1X- EAP	802.1X- EAP
Ακεραιότητα δεδομένων	CRC 32- ICV	MIC	CCM

Ακεραιότητα κεφαλίδας	Καμία	MIC	CCM
Αποτροπή επαναλαμβανόμενης επίθεσης	Καμία	Ακολουθία IV	Ακολουθία IV

(Bulbul, H. & Batmaz, I. & Ozel, M, 2008)

6. Συμπεράσματα

Όπως παρατηρούμε, η ασφάλεια δικτύων αποκτά όλο και μεγαλύτερη σημασία, εν όψει των διάφορων επιθέσεων, που καθιστούν την περίμετρο ασφαλείας λιγότερο αποτελεσματική αλλά και ταυτόχρονα πολύ ευάλωτη. Αναφέραμε ένα μεγάλο είδος απειλών σε συστήματα, οι οποίες μπορούν να αντιμετωπιστούν με την χρήση του τοίχους προστασίας (firewall) αλλά και της ασφάλειας που παρέχουν τα πρωτόκολλα επικοινωνίας. Παρ' όλα αυτά, λόγω της ραγδαίας εξέλιξης των επικοινωνιών, αλλά κυρίως των ασύρματων δικτύων, η ανάγκη για συνεχόμενη ασφάλεια στα νέα δίκτυα είναι επιβεβλημένη. Οι υπάρχοντες μηχανισμοί ασύρματης ασφαλείας, ξεκινώντας από τον παλαιότερο WEP έως τον πιο πρόσφατο RSN, παρέχουν ένα είδος ασφαλείας που σε πολλές περιπτώσεις απωθεί τις επιθέσεις από εισβολείς, οι οποίες περιλαμβάνουν από την πιο απλή περίπτωση την παρακολούθηση της κίνησης του δικτύου, έως τις πιο περίπλοκες όπως την μεταβολή και υποκλοπή δεδομένων της ασύρματης επικοινωνίας. Το προσωπικό ασφαλείας που διαχειρίζεται τα ασύρματα δίκτυα, πρέπει να μπορεί να είναι σε θέση να κατανοεί και να αντιλαμβάνεται τέτοιες επιθέσεις. Παρόλα αυτά, τα ευάλωτα σημεία των μηχανισμών αυτών είναι γνωστά και πρέπει να μπορούν να αντιμετωπιστούν μέσα από την υπάρχουσα υποδομή και τεχνολογία. Η καλή εφαρμογή των αλγορίθμων ασφαλείας πρέπει να ληφθεί πολύ σοβαρά υπ' όψιν, γιατί το κόστος υποκλοπής δεδομένων υπολογίζεται ότι θα είναι πολύ μεγάλο. Για το λόγο αυτό, η προσαρμογή και συνεχόμενη εξέλιξη των ήδη

υπαρχόντων μηχανισμών θεωρείται επιβεβλημένη, ώστε να μπορεί να λειτουργεί σωστά, αποδοτικά και αξιόπιστα το δίκτυο.

Βιβλιογραφία- Αναφορές

1. Bellovin, S. (n.d). Retrieved from http://el.wikipedia.org/wiki/Firewall (assessed 04-01-2011)
2. Boland, H., & Mousavi, H. (2004). Security issues of the IEEE 802.11b wireless LAN, Electrical and Computer Engineering. Canadian Conference on, Volume 1, Page(s):333-336 Vol.1.
3. Brenton, & Hunt. (2003). Mastering Network Security, Sybex Comp. Books.
4. Bulbul, H. & Batmaz, I. & Ozel, M. (2008). Comparison of WEP Mechanism, WPA and RSN Security Protocols. Retrieved from http://portal.acm.org/citation.cfm?id=1363229&dl=ACM&coll=DL&CFID=5748762&CFTOKEN=83595681 (assessed 15-11-2010).
5. Canavan, J.E. (2001). Fundamentals of Network Security, Artech House/Horizon.
6. Cornett, L., & Grewal, K., & Long, M., & Millier, M., & Williams, S. (2009). Intel Technology Journal ,Volume 13 Issue 2. Retrieved from ftp://download.intel.co.jp/technology/itj/2009/v13i2/pdfs/ITJ9.2.8-Network-Security.pdf (assessed 25-11-2010)
7. Fluhrer, S., Mantin, I., Shamir, A. (n.d). Weaknesses in the Key Scheduling Algorithm of RC4. Retrieved from http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (assessed 26-11-2010).
8. Gast M. (2002). Seven Security Problems of 802.11 Wireless. Retrieved from http://www.oreillynet.com/lpt/a/2404 (assessed 04-12-2010).
9. Gueron, S. (2008). Advanced Encryption Standard AES Instructions Set. Retrieved from http://www.intel.com (assessed 07-12-2010).
10. IEEE Systems. (2003). Man and Cybernetics Society, NY 18, Page(s):76- 83.
11. Ingham K., & Forrest S. (2009). A History and Survey of Network Firewalls, Retrieved from http://www.cs.unm.edu (assessed 13-12-2010).

12. Kent, S. (2005). IP Encapsulating Security Payload (ESP), *RFC* 4303
13. Kent, S. (2005). IP Authentication Header, *RFC* 4302.
14. Kerry, S. (2001). Response from the IEEE 802.11 Chair on WEP Security, IEEE 802.11 Working Group. Retrieved from http://slashdot.org/it/01/02/15/1745204.shtml (assessed 17-12-2010).
15. Manley, M.E., & McEntee, C.A., & Molet, A.M., & Park, J.S. (2005). Wireless Security Policy Development for Sensitive Organizations, Systems, Man and Cybernetics (SMC) Information Assurance Workshop. Proceedings from the Sixth Annual IEEE, 15-17 June 2005 Page(s):150-157
16. Mishra, A., & Petroni, & N.L., & Arbaugh, W.A., & Fraser, T. (2004). Security Issues in IEEE 802.11 Wireless Local- Area Networks: A Survey, Wireless Communications and Mobile Computing Journal, Vol. 4, No. 8, Page(s):821-833.
17. Pozzo, M., & Gray, T. (1987). An Approach to Containing Computer Viruses, Computer & Security 6, Page(s):321-331.
18. Potter, B. (2003). Wireless security's future, Security & Privacy Magazine, IEEE, Volume 1, Issue 4, July- Aug. Page(s):68 . 72. Retrieved from http://ieeexplore.ieee.org/iel5/8013/27399/01219074.pdf?tp=&arnumber=1219074&isnumber=27399 (assessed 18-12-2010)
19. Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11standards. Retrieved from http://www.sans.org/rr/whitepapers/wireless/1109.php (assessed 04-01-2010).
20. Πανεπιστήμιο Πειραιώς. (n.d). Εφαρμογές Ηλεκτρονικών Υπολογιστών. Retrieved from http://www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf (assessed 03-01-2011)