ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Π.Μ.Σ "ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ"

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Ποιότητα υπηρεσιών και ασφάλεια σε τοπικά δίκτυα υπολογιστών (Local Access Networks)

Ο φοιτητής:

Αρβανιτάκης Ιωάννης

Διδάσκουσα Καθηγήτρια: Αρίστη Γαλάνη

Πειραιάς 2016-2017

Περιεχόμενα

ΠΡΟΛΟΓΟΣ

Στο πρώτο μέρος της παρούσας διπλωματική εργασίας θα μελετήσουμε τις τρέχουσες εξελίξεις που επικρατούν στον τομέα της ασφάλειας και της ποιότητας υπηρεσιών (QoS) αναφορικά με τα τοπικά δίκτυα υπολογιστών (LANs). Θα παρουσιαστούν οι απειλές που δέχονται τα δίκτυα αυτά καθώς και οι τεχνικές άμυνας που χρησιμοποιούνται για την αντιμετώπισή τους. Επιπλέον θα πραγματοποιηθεί αναφορά στα θέματα ασφαλείας που αφορούν στα ασύρματα τοπικά δίκτυα (WLANs), η οποία θα είναι βασισμένη στο πρωτόκολλο IEEE802.11 και τις μεταγενέστερες εκδόσεις του.

Στο δεύτερο μέρος θα πραγματοποιηθεί τεχνοοικονομική ανάλυση, η οποία θα αφορά στα τοπικά δίκτυα υπολογιστών και στην οποία θα θεωρηθεί ως ενιαία η διαχείριση των προσφερόμενων υπηρεσιών. Η ανάλυση αυτή θα στηριχθεί στην κατηγοριοποίηση των υπηρεσιών συναρτήσει του QoS και σύμφωνα με το 3GPP, το οποίο καθορίζει τέσσερα διαφορετικά επίπεδα υπηρεσιών τα οποία διαφέρουν μεταξύ τους αναφορικά με την ευαισθησία στην καθυστέρηση της μετάδοσης των δεδομένων. Θα πραγματοποιηθούν δύο επιμέρους αναλύσεις. Στη πρώτη θα απαιτείται υψηλή ποιότητα και πολύ χαμηλές καθυστερήσεις μετάδοσης ενώ στη δεύτερη οι απαιτήσεις θα είναι χαμηλότερες.

Τα τοπικά δίκτυα αναφέρονται σε ένα σύνολο συνδεδεμένων υπολογιστών που εκτείνονται σε περιορισμένη γεωγραφική περιοχή. Οι υπολογιστές αυτοί αποτελούν τους κόμβους μέσω των οποίων μεταδίδονται τα πακέτα επικοινωνίας. Σε ένα τέτοιο δίκτυο όμως, οποιοσδήποτε κόμβος έχει τη δυνατότητα να λάβει πακέτα δεδομένων, επομένως κάποιος μη εξουσιοδοτημένος χρήστης που θα έχει πρόσβαση σε έναν κόμβο του δικτύου, θα μπορεί πιθανώς να παρακολουθήσει, να αποσυμπιέσει όλα τα πακέτα και να κλέψει κρίσιμες πληροφορίες.

Κατά την τελευταία δεκαετία, η εφαρμογή της τεχνολογίας Wireless LAN (WLAN) έχει εξελιχθεί σε έναν από πιο περιορισμένους τομείς, όπως οι αποθήκες, στις επιχειρήσεις και τα σπίτια, λόγω της ευκολίας, της κινητικότητας και των προσιτών τιμών για τις ασύρματες συσκευές. Η ασύρματη τεχνολογία επιτρέπει στους κινητούς σταθμούς να κυκλοφορούν ελεύθερα εντός της εμβέλειας των σημείων πρόσβασης, χωρίς να είναι φυσικά συνδεδεμένοι με το ενσύρματο δίκτυο. Ωστόσο, τα WLANs παρουσιάζουν σοβαρά προβλήματα ασφαλείας, επειδή το ασύρματο σήμα μεταδίδεται μέσω του αέρα προς όλες τις κατευθύνσεις ταυτόχρονα. Ένας μη εξουσιοδοτημένος χρήστης μπορεί εύκολα να συλλάβει αυτό το σήμα χρησιμοποιώντας δωρεάν εργαλεία λογισμικού και να εκμεταλλευτεί την ευπάθεια του WLAN.

Το Quality of Service (QoS) αφορά στη μέτρηση της συνολικής απόδοσης μίας υπηρεσίας όπως η τηλεφωνία ή ένα δίκτυο υπολογιστών και θεωρείται σήμερα αναγκαία συνάρτηση της ποιότητας που θα προσφερθεί. Σε ένα τοπικό δίκτυο και με

την επιλογή του κατάλληλου εξοπλισμού, ο διαχειριστής του δικτύου οφείλει να συμπεριλάβει την εφαρμογή του QoS ώστε να αποδοθεί η βέλτιστη ποιότητα υπηρεσιών.

1. Ασφάλεια Δικτύων- Επισκόπηση

Στην σύγχρονη εποχή, οι οργανισμοί βασίζονται πολύ στα δίκτυα υπολογιστών για να διαμοιράζονται πληροφορίες με αποτελεσματικό και παραγωγικό τρόπο. Τα δίκτυα υπολογιστών γίνονται πλέον πολύ μεγάλα και βρίσκονται στους περισσότερους οργανισμούς. Υποθέτοντας ότι κάθε μέλος του προσωπικού έχει μια ειδική θέση εργασίας, μια μεγάλης κλίμακας εταιρεία θα έχει κάποιες χιλιάδες θέσεις εργασίας καθώς και αρκετούς εξυπηρετητές στο δίκτυο της.

Είναι πολύ πιθανόν ότι αυτές οι θέσεις εργασίας να μην διαχειρίζονται από κάποιο κεντρικό σύστημα, ούτε να έχουν κάποια προστασία. Μπορεί να έχουν ποικιλία από λειτουργικά συστήματα, υλικό, λογισμικό καθώς και πρωτόκολλα , καθώς και να υπάρχει διαφορετικό γνωστικό υπόβαθρο της χρήσης υπολογιστών ανάμεσα στους χρήστες. Αν υποθέσουμε ότι αυτές οι θέσεις εργασίας της εταιρείας συνδέονται άμεσα στο διαδίκτυο, τότε το δίκτυο μπορεί να γίνει στόχος για μια επίθεση που μπορεί να αποκαλύψει πληροφορίες οι οποίες θα φανερωθούν εξαιτίας των ευπαθειών του δικτύου.

1.1 Φυσικό Δίκτυο

Ένα δίκτυο ορίζεται όταν δύο η περισσότερες υπολογιστικές συσκευές είναι συνδεδεμένες μεταξύ τους ώστε να μοιράζονται οι πόροι του συστήματος αποτελεσματικά. Επίσης, η σύνδεση δύο η περισσότερων δικτύων μεταξύ τους είναι γνωστό ως διαδικτύωση. Έτσι και το διαδίκτυο είναι ένα σύνολο πολλών διασυνδεδεμένων δικτύων.

Για την δημιουργία ενός δικτύου, ένας οργανισμός έχει διάφορες επιλογές. Μπορεί να χρησιμοποιήσει ενσύρματο δίκτυο ή ασύρματο δίκτυο για να ενώσει όλους τους σταθμούς εργασίας. Πλέον οι οργανισμοί χρησιμοποιούν πιο πολύ συνδυασμό από ενσύρματα και ασύρματα δίκτυα.

1.2 Ενσύρματα και Ασύρματα Δίκτυα

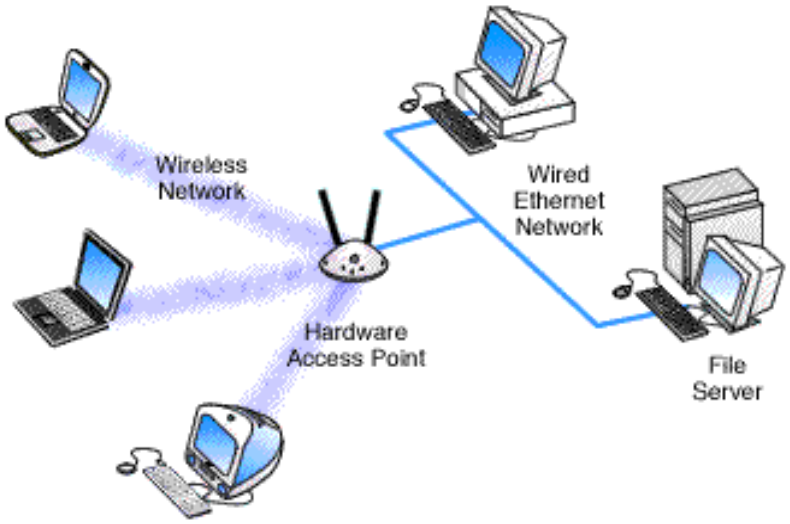
Σε ένα ενσύρματο δίκτυο, οι συσκευές συνδέονται μεταξύ τους χρησιμοποιώντας καλώδια. Τα ενσύρματα δίκτυα βασίζονται στο πρωτόκολλο Ethernet όπου οι συσκευές συνδέονται με την χρήση καλωδίων συνεστραμμένων ζευγών(UTP) σε διαφορετικούς μεταγωγείς. Οι μεταγωγείς αυτοί είναι συνδεδεμένοι με τον δρομολογητή του δικτύου που επιτρέπει την πρόσβαση στο διαδίκτυο.

Σε ένα ασύρματο δίκτυο, οι συσκευές είναι συνδεδεμένες με ένα σημείο πρόσβασης μέσω σημάτων. Τα σημεία πρόσβασης είναι συνδεδεμένα μέσω καλωδίων στους μεταγωγείς και τους δρομολογητές και μπορούν να μεταφέρουν δεδομένα ανάμεσα στις ενσύρματες και ασύρματες συσκευές.

Τα ασύρματα δίκτυα είναι πολύ δημοφιλή λόγω της ευελιξίας που παρέχουν. Οι συσκευές δεν χρειάζεται να είναι συνδεδεμένες με καλώδια και μπορούν να

μετακινούνται ελευθέρα μέσα στο εύρος του ασύρματου δικτύου. Αυτό διασφαλίζει τον αποτελεσματικό διαμοιρασμό της πληροφορίας και ενισχύει την παραγωγικότητα.

Ένα παράδειγμα δικτύου το οποίο έχει ταυτόχρονα ασύρματη και ενσύρματη σύνδεση, παρουσιάζεται στην παρακάτω εικόνα.



Εικόνα 1 – Υποδομή ενός δικτύου

1.3 Ευπάθειες του δικτύου και Επιθέσεις

Οι πιο κοινή ευπάθεια που υπάρχει στα ενσύρματα και ασύρματα δίκτυα είναι η μη εξουσιοδοτημένη πρόσβαση στο δίκτυο. Ο επιτιθέμενος μπορεί να συνδέσει την συσκευή του μέσω ενός απροστάτευτου κόμβου ή μεταγωγέα. Σε αυτό το πλαίσιο τα ασύρματα δίκτυα θεωρούνται λιγότερο ασφαλή από τα ενσύρματα καθώς μπορεί να υπάρχει πρόσβαση σε αυτά χωρίς την χρήση κάποιας φυσικής σύνδεσης.

Μετά την πρόσβαση, ο μη εξουσιοδοτημένος χρήστης να πραγματοποιήσει ενέργειες όπως :

Παρακολούθηση πακέτων δεδομένων του δικτύου (packet sniffing) για να υποκλέψει χρήσιμες πληροφορίες

Επίθεση άρνησης υπηρεσιών (DoS), το δίκτυο «πλημμυρίζει» με ψεύτικα πακέτα με αποτέλεσμα το δίκτυο να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.

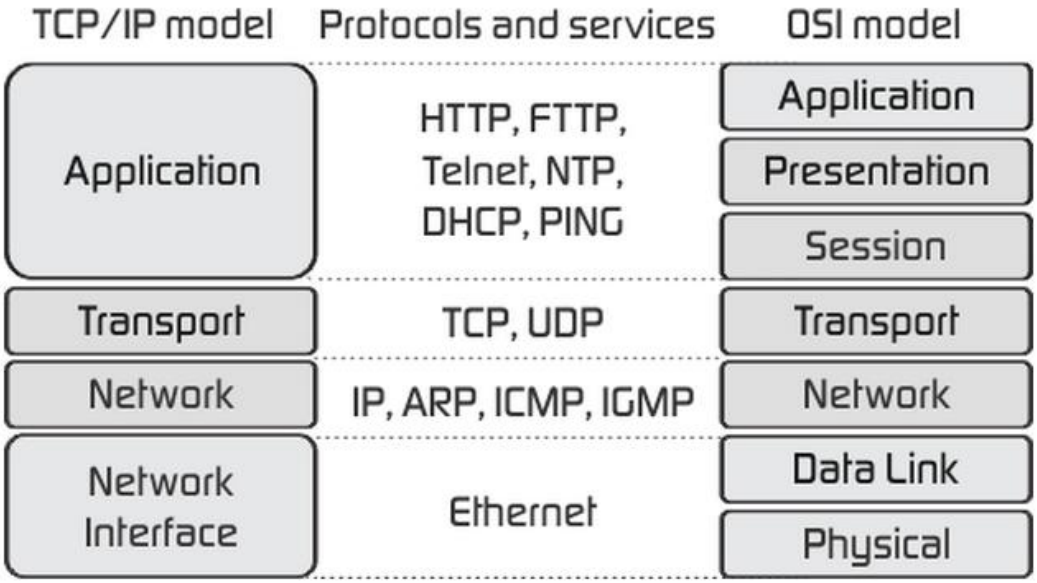
Πλαστογράφηση (Spoofing), δηλαδή δημιουργία πακέτων TCP/IP χρησιμοποιώντας τα στοιχεία και την διεύθυνση κάποιου αξιόπιστου χρήστη ώστε να αποκτήσει ο μη εξουσιοδοτημένος χρήστης πρόσβαση σε υπολογιστές. (1)

1.4 Πρωτόκολλο Δικτύου

Το πρωτόκολλο δικτύου είναι ένα σύνολο από κανόνες που χρησιμοποιούνται μεταξύ των συσκευών που είναι συνδεδεμένες σε ένα δίκτυο ώστε να υπάρχει επικοινωνία μεταξύ τους καθώς και ανταλλαγή πληροφοριών. Οι κανόνες περιέχουν τους μηχανισμούς για την δημιουργία συνδέσεων καθώς και για πακέτα δεδομένων που λαμβάνονται και αποστέλλονται.

Αρκετά πρωτόκολλα δικτύου έχουν αναπτυχθεί με το καθένα να έχει συγκεκριμένο σκοπό. Ωστόσο το πρωτόκολλο που χρησιμοποιείται πιο πολύ είναι τοTCP/IP που σχετίζεται με τα υψηλότερου και χαμηλότερου επιπέδου πρωτόκολλα.

Στην παρακάτω εικόνα παρουσιάζονται οι διαφορές αυτού του μοντέλου (TCP/IP) με το μοντέλο OSI στα πρωτόκολλα και τις υπηρεσίες που περιλαμβάνουν, ανάλογα με το επίπεδο.



Εικόνα 2 - Διαφορές μεταξύ του TCP/IP μοντέλου και OSI

1.5 Αρχιτεκτονική TCP/IP

Το Transmission Control Protocol (TCP) και το Internet Protocol (IP) είναι δύο ξεχωριστά πρωτόκολλα δικτύου τα οποία συνήθως χρησιμοποιούνται μαζί. Συγκεκριμένα το TCP χρησιμοποιείται για την μετάδοση των δεδομένων μέσω των IP δικτύων Λόγω της δημοτικότητας τους καθώς και της ευρείας υιοθέτησης τους, εφαρμόζονται σε όλα τα λειτουργικά συστήματα των συσκευών του δικτύου.

Το πρωτόκολλο TCP/IP δημιουργήθηκε το 1980 ως μια λύση διαδικτύωσης , χωρίς όμως να υπάρχει ιδιαίτερη μέριμνα όσον αφορά σε θέματα ασφαλείας. Σχεδιάστηκε

με σκοπό την επικοινωνία σε ένα περιορισμένο ασφαλές δίκτυο, ωστόσο με τον καιρό το πρωτόκολλο αυτό καθιερώθηκε για τις επικοινωνίες στο διαδίκτυο.

Το TCP/IP είναι χτισμένο με τεχνολογία "χωρίς σύνδεση" (connectionless). Η πληροφορία μεταφέρεται σαν μια ακολουθία datagrams. Το datagram είναι μια ομάδα δεδομένων που στέλνεται σαν ξεχωριστό μήνυμα. Κάθε ένα από τα datagrams, στέλνεται ατομικά μέσω του δικτύου. Αφού επιτευχθεί εγκατάσταση σύνδεσης, η πληροφορία διασπάται σε datagrams, τα οποία αντιμετωπίζονται από το δίκτυο απολύτως ξεχωριστά. (2)

Μερικές από τις κοινές ευπάθειες που υπάρχουν στην ασφάλεια του TCP/IP πρωτοκόλλου είναι:

Το HTTP είναι ένα πρωτόκολλο που βρίσκεται στο Application layer και χρησιμοποιείται για την μεταφορά αρχείων που συνθέτουν τις ιστοσελίδες από τους web servers. Αυτές οι μεταφορές γίνονται με απλά κείμενα (cookies), και έτσι ένας μη εξουσιοδοτημένος χρήστης θα μπορούσε να διαβάσει τα πακέτα δεδομένων που ανταλλάσσονται μεταξύ του server και του client και να υποκλέψει ευαίσθητες πληροφορίες.

Μια ακόμα ευπάθεια του HTTP είναι η αδύναμη αυθεντικοποίηση μεταξύ του client και του web server κατά την προετοιμασία μιας συνόδου (session). Αυτή η ευπάθεια μπορεί να οδηγήσει σε μια επίθεση κλοπής συνόδου (session hijack attack) όπου ο επιτιθέμενος υποκλέπτει μια σύνοδο από ένα εξουσιοδοτημένο χρήστη.

Η ευπάθεια του TCP πρωτοκόλλου είναι το three-way handshake που γίνεται για την δημιουργία της σύνδεσης. Ο κακόβουλος χρήστης μπορεί να χρησιμοποιήσει επιθέσεις άρνησης υπηρεσιών (SYN-Flood) και με αυτόν τον τρόπο να δημιουργήσει πολλές συνόδους(sessions) χωρίς όμως να ολοκληρώνει το handshake (αυτοματοποιημένη διαδικασία επικύρωσης της δημιουργίας καναλιού επικοινωνίας μεταξύ 2 οντοτήτων). Αυτό οδηγεί σε υπερφόρτωση του server με τελικό αποτέλεσμα την διακοπή των υπηρεσιών του.

Το IP layer είναι ευαίσθητο σε πολλές ευπάθειες. Μέσω της μετατροπής του header, ο επιτιθέμενος μπορεί να χρησιμοποιήσει IP Spoofing ώστε να παραποιηθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή

Εκτός από τα παραπάνω που αναφέρθηκαν, υπάρχουν αρκετές ακόμα ευπάθειες στην σχεδίαση και την εφαρμογή του πρωτόκολλου TCP/IP.

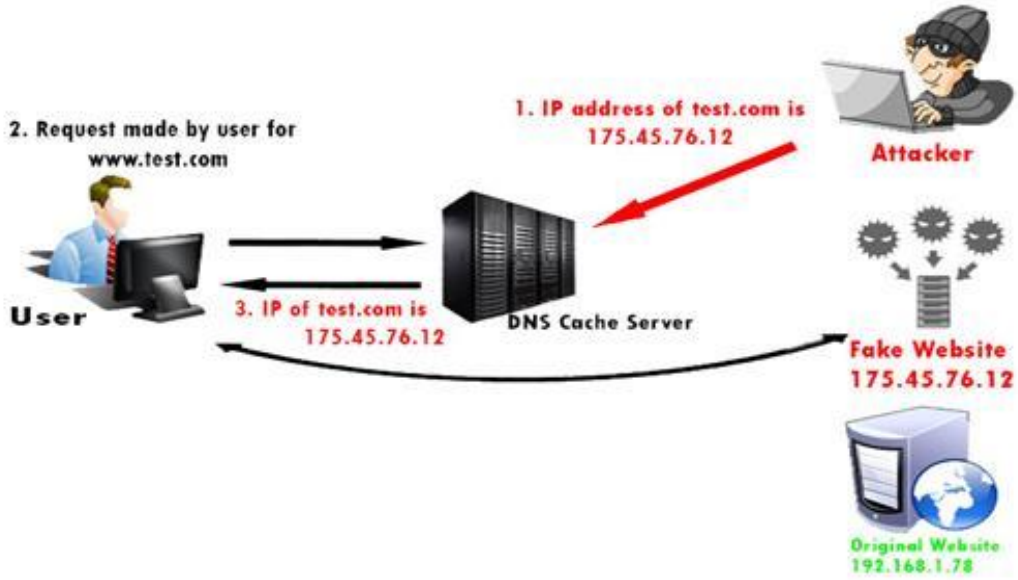
Παρεμπιπτόντως, στα δίκτυα που βασίζονται στο TCP/IP, αν το ένα επίπεδο (layer) παραβιαστεί, τότε τα υπόλοιπα επίπεδα δεν αντιλαμβάνονται την παραβίαση και το σύνολο της επικοινωνίας τίθεται σε κίνδυνο. Ως εκ τούτου, υπάρχει ανάγκη για εφαρμογή τεχνικών ασφαλείας σε κάθε επίπεδο ώστε να διασφαλιστεί η μέγιστη ασφάλεια. (3)

1.6 Πρωτόκολλο DNS

Το Domain Name System χρησιμοποιείται για να δίνει σε κόμβους του δικτύου IP διευθύνσεις. Οι χρήστες του δικτύου εξαρτώνται από την λειτουργικότητα του DNS για να μπορούν να περιηγηθούν στο διαδίκτυο χρησιμοποιώντας τους φυλλομετρητές(browsers).

Σε μια επίθεση στον DNS, ο στόχος του επιτιθέμενου είναι να τροποποιήσει μια εξουσιοδοτημένη DNS εγγραφή (record) ώστε να δοθεί σε μια λανθασμένη IP διεύθυνση. Έτσι θα κατευθύνει όλη την κίνηση του δικτύου για αυτήν την IP στον μη εξουσιοδοτημένο υπολογιστή.

Το DNS cache poisoning είναι μια ευπάθεια στην ασφάλεια των υπολογιστών στην οποία τα παραποιημένα στοιχεία του DNS εισάγονται στην προσωρινή μνήμη του DNS, υποχρεώνοντας τον διακομιστή που δίνει το όνομα του ιστότοπου (webpage) να το επιστρέψει αλλά με λανθασμένη διεύθυνση IP. Αυτό οδηγεί στην εκτροπή της κίνησης του δικτύου στον υπολογιστή του κακόβουλου χρήστη. Στη ακόλουθη εικόνα παρουσιάζεται η διαδικασία αυτής της επίθεσης.



Εικόνα 3 - DNS Poisoning

1.7 Πρωτόκολλο ICMP

Το Internet Control Management Protocol (ICMP) είναι ένα βασικό πρωτόκολλο διαχείρισης των TCP/IP δικτύων. Χρησιμοποιείται για να στέλνει μηνύματα σφαλμάτων και ελέγχου σχετικά με την κατάσταση των δικτυακών συσκευών. Το ICMP έχει τις δικές του ευπάθειες και μπορεί να χρησιμοποιηθεί για γίνουν επιθέσεις στο δίκτυο.

Οι πιο κοινές επιθέσεις που μπορεί να προκύψουν σε ένα δίκτυο λόγω των ευπαθειών του ICMP είναι:

Το ICMP επιτρέπει στον επιτιθέμενο να ερευνά το δίκτυο με σκοπό την εξεύρεση της τοπολογίας και τα μονοπάτια που χρησιμοποιούνται στο δίκτυο. Η σάρωση του ICMP περιλαμβάνει την ανακάλυψη όλων των IP διευθύνσεων των χρηστών που χρησιμοποιούνται σε ολόκληρο το δίκτυο.

Το Trace Route είναι μια δημοφιλής υπηρεσία του ICMP που χρησιμοποιείται για την χαρτογράφηση της δικτύωσης περιγράφοντας την διαδρομή των πακέτων σε πραγματικό χρόνο από τον client στον απομακρυσμένο υπολογιστή.

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει επίθεση άρνησης υπηρεσιών (DoS) χρησιμοποιώντας την ευπάθεια του πρωτόκολλου ICMP. Αυτή η επίθεση περιλαμβάνει την αποστολή IPMP ping πακέτων που ξεπερνούν το μέγεθος των 65kb στην συσκευή προορισμού. Συγκεκριμένα, πραγματοποιείται συνδυασμός δύο ή περισσότερων φυσικών διεπαφών του δικτύου σε μια ομάδα ICMP. Σε κάθε μία από αυτές τις διεπαφές διατίθεται μια διεύθυνση IP με σκοπό να πραγματοποιεί δοκιμές (failure testing). Η κάθε διεύθυνση στέλνει περιοδικά ένα αίτημα ICMP στο σύστημα που έχει στοχοποιήσει και περιμένει για απάντηση. Εάν δεν λάβει την απάντηση μετά από συγκεκριμένο αριθμό προσπαθειών, θα θεωρήσει το σύνδεσμο νεκρό και αμέσως μετά θα προκαλέσει την αποτυχία όλων των εφαρμογών που έχουν συνδεθεί στο σύνδεσμο τη δεδομένη στιγμή. Επομένως ο υπολογιστής πιθανώς να αποτύχει να διαχειριστεί κατάλληλα αυτό το πακέτο και αυτό το γεγονός μπορεί να έχει ως συνέπεια την διακοπή λειτουργίας του λειτουργικού συστήματος. (4)

1.8 Στόχοι της ασφάλειας δικτύων

Ένα δίκτυο, ειδικά κατά την μετάδοση των δεδομένων είναι ευπαθές σε διάφορες επιθέσεις. Ο επιτιθέμενος μπορεί να στοχεύσει στο κανάλι επικοινωνίας, με σκοπό να λάβει τα δεδομένα, να τα διαβάσει, ή ακόμα και να εισάγει κάποιο ψεύτικο μήνυμα για να επιτύχει τον σκοπό του.

Η ασφάλεια δικτύων δεν αφορά μόνο στην ασφάλεια των υπολογιστών που είναι εκτεθειμένοι σε εξωτερικές παρεμβάσεις, αλλά και στο σύνολο του δικτύου. Συγκεκριμένα εστιάζει στη προστασία της ακεραιότητας, της ευχρηστίας, της αξιοπιστίας καθώς και των δεδομένων του δικτύου.

Ο κύριος στόχος της ασφάλειας των δικτύων είναι η Ακεραιότητα, η Διαθεσιμότητα καθώς και η Εμπιστευτικότητα. Αυτές οι 3 έννοιες είναι ο ακρογωνιαίος λίθος που περιβάλει την ασφάλεια των δικτύων.

Διαθεσιμότητα: Η λειτουργία της διαθεσιμότητας στην ασφάλεια δικτύων είναι η βεβαίωση και σιγουριά ότι τα δεδομένα, οι πόροι καθώς και οι υπηρεσίες του δικτύου θα συνεχίσουν να λειτουργούν απρόσκοπτα και να είναι στην διάθεση των νόμιμων χρηστών, κάθε φορά που το απαιτούν.

Ακεραιότητα: Ο στόχος αυτός σημαίνει την διατήρηση και διασφάλιση της ακρίβειας και της συνέπειας των δεδομένων. Η σημαντικότερη λειτουργία της είναι η βεβαίωση ότι τα δεδομένα είναι αξιόπιστα και δεν έχουν αλλάξει από μη εξουσιοδοτημένα άτομα.

Εμπιστευτικότητα: Η λειτουργία της είναι να προστατεύσει τα πολύτιμα δεδομένα από μη εξουσιοδοτημένα πρόσωπα. Η εμπιστευτικότητα είναι μέρος της ασφάλειας του δικτύου όσο αναφορά την διασφάλιση των δεδομένων που είναι διαθέσιμα για τα προβλεπόμενα και εξουσιοδοτημένα πρόσωπα. (5)

1.9 Επίτευξη ασφάλειας δικτύων

Η διασφάλιση της ασφάλειας του δικτύου , όπως και η επίτευξη των στόχων μπορεί να φαίνονται εύκολες έννοιες αλλά στην πραγματικότητα οι μηχανισμοί που χρησιμοποιούνται για την επίτευξη των στόχων αυτών είναι εξαιρετικά πολύπλοκοι και για την υλοποίησή τους χρειάζεται κάποιος πολύ εξειδικευμένος.

Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), στην πρόταση της για την αρχιτεκτονική ασφάλειας X.800, έχει καθορίσει ορισμένους μηχανισμούς για την τυποποίηση μεθόδων ώστε να επιτευχθεί η ασφάλεια του δικτύου. Μερικοί από αυτούς τους μηχανισμούς είναι:

Κρυπτογράφηση: Ο μηχανισμός αυτός παρέχει εμπιστευτικότητα των δεδομένων, με την μετατροπή τους σε μη αναγνώσιμη μορφή για άτομα που δεν είναι εξουσιοδοτημένα χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης-αποκρυπτογράφησης με μυστικά κλειδιά.

Ψηφιακές υπογραφές: Αυτός ο μηχανισμός είναι ισοδύναμος των απλών υπογραφών σε ηλεκτρονικά δεδομένα. Παρέχει αυθεντικότητα των δεδομένων καθώς ο παραλήπτης λαμβάνει την πιστοποίηση ότι το μήνυμα που έλαβε ανήκει στον αποστολέα που το υπέγραψε καθώς και ότι δεν αλλοιώθηκε κατά την μεταφορά.

Έλεγχος της πρόσβασης: Ο μηχανισμός αυτός χρησιμοποιείται για να παρέχει υπηρεσίες ελέγχου πρόσβασης στο σύστημα επιτρέποντας την ταυτοποίηση και αυθεντικοποίηση ενός χρήστη ώστε να καθορίζει και να επιβάλλει τα δικαιώματα πρόσβασης του.

Έχοντας αναπτύξει και αναγνωρίσει διάφορους μηχανισμούς ασφαλείας για την επίτευξή της ασφάλειας των δικτύων, είναι σημαντικό να γνωρίζουμε που θα εφαρμοστούν, και σε φυσικό επίπεδο αλλά και σε λογικό (π.χ. TCP/IP).

1.10 Μηχανισμοί ασφαλείας

Αρκετοί μηχανισμοί ασφαλείας έχουν αναπτυχθεί με τέτοιο τρόπο ώστε να μπορούν να εφαρμοστούν σε ένα συγκεκριμένο επίπεδο του μοντέλου OSI.

Ασφάλεια στο επίπεδο Εφαρμογής (Application layer): Τα μέτρα ασφαλείας που χρησιμοποιούνται σε αυτό το επίπεδο είναι συγκεκριμένες εφαρμογές. Οι διαφορετικοί τύποι εφαρμογών χρειάζονται και ξεχωριστά μέτρα ασφαλείας. Για αυτόν τον λόγο για να διασφαλιστεί η ασφάλεια στο application layer, αυτές οι εφαρμογές θα πρέπει να τροποποιηθούν κατάλληλα ανάλογα με τις ανάγκες που υπάρχουν.

Θεωρείται ότι ο σχεδιασμός και η εφαρμογή ενός κρυπτογραφημένου πρωτόκολλου εφαρμογής είναι πολύ δύσκολος. Ως εκ τούτου οι μηχανισμοί ασφαλείας του application layer για την προστασία των επικοινωνιών του δικτύου προτιμούνται να είναι λύσεις που έχουν δοκιμαστεί και υπάρχουν ήδη. Ένα παράδειγμα αυτού είναι το Secure Multipurpose Internet Mail Extensions (S/MIME), το οποίο χρησιμοποιείται συνήθως για την κρυπτογράφηση των e-mail μηνυμάτων. Το DNSSEC είναι ένα άλλο πρωτόκολλο που εφαρμόζεται σε αυτό το επίπεδο και χρησιμοποιείται για την ασφαλή ανταλλαγή DNS ερωτημάτων.

Ασφάλεια στο επίπεδο μετάδοσης (Transport layer): Τα μέτρα ασφαλείας σε αυτό το επίπεδο μπορούν να χρησιμοποιηθούν για την προστασία των δεδομένων σε μια συνεδρία μεταξύ δύο χρηστών. Η πιο κοινή χρήση του για τα πρωτόκολλα ασφαλείας του επιπέδου μεταφοράς είναι για την προστασία των επικοινωνιών του HTTP και FTP. Το Transport Layer Security(TLS) και το Secure Socket Layer(SSL) είναι τα πιο κοινά πρωτόκολλα που χρησιμοποιούνται για τον σκοπό αυτό.

Ασφάλεια στο Επίπεδο Δικτύου (Network Layer): Τα μέτρα ασφαλείας σε αυτό το επίπεδο μπορούν να εφαρμοστούν σε όλες τις εφαρμογές. Όλες οι επικοινωνίες μεταξύ χρηστών ή δικτύων μπορούν να προστατευτούν σε αυτό το επίπεδο χωρίς να χρειάζεται η τροποποίηση κάποιας εφαρμογής. Σε ορισμένα περιβάλλοντα, τα πρωτόκολλα του επιπέδου δικτύου όπως το Internet Protocol Security (IPSec) παρέχουν μια πολύ καλύτερη λύση από αυτά του επιπέδου μετάδοσης (transport) ή εφαρμογών (application) λόγω των δυσκολιών που υπάρχουν στην προσθήκη ελέγχου σε ξεχωριστές εφαρμογές. Ωστόσο τα πρωτόκολλα ασφαλείας σε αυτό το επίπεδο παρέχουν λιγότερη ευελιξία στην επικοινωνία που μπορεί να απαιτείται από ορισμένες εφαρμογές.

Παρεμπιπτόντως , ένας μηχανισμός ασφαλείας που έχει σχεδιαστεί για να λειτουργεί σε υψηλότερο επίπεδο, δεν μπορεί να παρέχει προστασία για τα δεδομένα σε χαμηλότερα επίπεδα διότι τα χαμηλότερα επίπεδα εκτελούν λειτουργίες τις οποίες τα υψηλότερα δεν γνωρίζουν. Ως εκ τούτου θεωρείται ότι είναι απαραίτητη η ανάπτυξη πολλαπλών μηχανισμών ασφαλείας σε όλα τα επίπεδα για την ενίσχυση της ασφάλειας των δικτύων.

2. Ασφάλεια στο επίπεδο εφαρμογών

Υπάρχουν πολλές επιχειρηματικές υπηρεσίες που προσφέρονται σε απευθείας σύνδεση μέσω εφαρμογών στο μοντέλο "πελάτη-διακομιστή (client-server)". Οι πιο δημοφιλείς μορφές είναι η διαδικτυακή εφαρμογή (web app) και η αλληλογραφία. Και στις δύο αυτές εφαρμογές, ο χρήστης επικοινωνεί με τον καθορισμένο εξυπηρετητή και αποκτά υπηρεσίες.

Κατά την χρήση μιας υπηρεσίας από οποιοδήποτε application server , ο χρήστης και ο διακομιστής ανταλλάσουν πολλές πληροφορίες οι οποίες είναι ευάλωτες σε διάφορες επιθέσεις. Η ασφάλεια του δικτύου συνεπάγεται με την προστασία των δεδομένων από επιθέσεις όσο αυτά μεταφέρονται μέσα στο δίκτυο. Για να υπάρχει η επίτευξη αυτού του στόχου, έχουν σχεδιαστεί πολλά πρωτόκολλα τα οποία λειτουργούν σε πραγματικό χρόνο. Αυτά τα πρωτόκολλα πρέπει να παρέχουν τους εξής στόχους:

- Θα πρέπει να γίνεται αυθεντικοποίηση μεταξύ των συνδέσεων
- Καθιέρωση ενός μυστικού κλειδιού συνεδρίας πριν από την ανταλλαγή πληροφοριών στο δίκτυο
- Ανταλλαγή πληροφοριών σε κρυπτογραφημένη μορφή

Είναι ενδιαφέρον ότι αυτά τα πρωτόκολλα λειτουργούν σε διαφορετικά επίπεδα του μοντέλου δικτύωσης. Όπως π.χ. το πρωτόκολλο S/MIME που λειτουργεί στο επίπεδο εφαρμογών ή το IPSec πρωτόκολλο που λειτουργεί στο επίπεδο δικτύου.

2.1 Ασφάλεια του e-mail

Ο απλούστερος τρόπος για την αποστολή ενός e-mail είναι η αποστολή του μηνύματος απευθείας από την συσκευή του αποστολέα σε αυτήν του παραλήπτη. Σε αυτήν την περίπτωση είναι σημαντικό και για τις δύο συσκευές να λειτουργούν στο δίκτυο ταυτόχρονα. Ωστόσο αυτή η λειτουργία δεν είναι πρακτική καθώς οι χρήστες συνδέονται περιστασιακά στο δίκτυο. Για αυτό γεννήθηκε η ιδέα για την δημιουργία διακομιστών για το e-mail. Με αυτόν τον τρόπο το mail στέλνεται σε ένα διακομιστή ο οποίος είναι μόνιμα διαθέσιμος στο δίκτυο, και όταν ο παραλήπτης συνδέεται στο δίκτυο μπορεί να διαβάσει το mail από τον διακομιστή. Σε γενικές γραμμές, η αρχιτεκτονική του e-mail αποτελείται από ένα πλέγμα εξυπηρετητών που αναφέρονται και ως Message transfer agents(MTA) , καθώς και συσκευές οι οποίες έχουν ένα πρόγραμμα που περιλαμβάνει έναν user agent και ένα τοπικό MTA. Συνήθως, ένα μήνυμα ηλεκτρονικού ταχυδρομείου προωθείται από έναν user agent, περνάει μέσα από το πλέγμα των Message transfer agents και στο τέλος καταλήγει στον user agent του παραλήπτη. Τα πρωτόκολλα που χρησιμοποιούνται για το e-mail είναι:

- Το πρωτόκολλο Simple mail Transfer Protocol (SMTP) το οποίο χρησιμοποιείται για την προώθηση μηνυμάτων.

- Τα πρωτόκολλα POP και IMAP τα οποία χρησιμοποιούνται για την ανάκτηση των μηνυμάτων του παραλήπτη από τον διακομιστή.

Η αυξανόμενη χρήση της αλληλογραφίας για σημαντικές και κρίσιμες συναλλαγές απαιτεί την παροχή ορισμένων θεμελιωδών υπηρεσιών ασφαλείας ως εξής:

- Εμπιστευτικότητα, το mail δεν πρέπει να αναγνωστεί από κανένα, παρά μόνο από τον αποδέκτη
- Αυθεντικότητα, ο παραλήπτης θα πρέπει να είναι σίγουρος για την ταυτότητα του αποστολέα
- Ακεραιότητα, η διαβεβαίωση στον παραλήπτη ότι τα μηνύματα δεν έχουν τροποποιηθεί από την στιγμή που μεταδόθηκαν από τον αποστολέα.
- Ο παραλήπτης του μηνύματος να μπορεί να αποδείξει σε τρίτους ότι ο αποστολέας πραγματικά έστειλε το μήνυμα
- Απόδειξη της υποβολής, ο αποστολέας παίρνει την επιβεβαίωση ότι το μήνυμα έχει παραδοθεί στο σύστημα παράδοσης της αλληλογραφίας
- Απόδειξη παράδοσης, ο αποστολέας παίρνει μια επιβεβαίωση ότι ο παραλήπτης έχει λάβει το μήνυμα.

Οι υπηρεσίες ασφαλείας όπως η ιδιωτικότητα, αυθεντικότητα και ακεραιότητα παρέχονται με την χρήση ενός κρυπτογραφημένου δημόσιου κλειδιού.

2.2 Pretty Good Privacy (PGP)

Το PGP είναι ένα πρόγραμμα κρυπτογράφησης το οποίο χρησιμοποιείται για την παροχή υπηρεσιών ασφαλείας στην επικοινωνία της αλληλογραφίας. Χρησιμοποιεί την κρυπτογραφία δημόσιου κλειδιού, συναρτήσεις κατακερματισμού, κρυπτογράφηση συμμετρικού κλειδιού καθώς και ψηφιακές υπογραφές και παρέχει:

- Ιδιωτικότητα
- Αυθεντικοποίηση του αποστολέα
- Ακεραιότητα του μηνύματος

Το PGP χρησιμοποιεί υπάρχοντες αλγόριθμους κρυπτογράφησης όπως το RSA,MD5 αντί να εφεύρει νέους.

2.3 Secure Multipurpose Internet Mail Extension

Το S/MIME είναι παρόμοιο με το PGP. Παρέχει και αυτό τις ίδιες υπηρεσίες για την επικοινωνία του e-mail όπως κρυπτογράφηση δημόσιου/συμμετρικού κλειδιού κτλ. Οι πιο κοινοί συμμετρικοί αλγόριθμου που χρησιμοποιεί το S/MIME είναι το RC2

και το TripleDes. Η συνήθης μέθοδος δημόσιου κλειδιού είναι το RSA και της συνάρτησης κατακερματισμού το MD5 ή το SHA-1.

3. Ασφάλεια στο επίπεδο μετάδοσης

Η ασφάλεια του δικτύου περιλαμβάνει την διασφάλιση των δεδομένων από επιθέσεις την στιγμή της μετάδοσης τους στο δίκτυο. Για την επίτευξη αυτού του στόχου έχουν σχεδιαστεί πολλά πρωτόκολλα ασφαλείας που λειτουργούν σε πραγματικό χρόνο. Για το TCP/IP πρωτόκολλο, το φυσικό και το επίπεδο δεδομένων εμπεριέχονται στο τερματικό του χρήστη καθώς και στην κάρτα δικτύου. Τα επίπεδα TCP και IP εμπεριέχονται στο λειτουργικό σύστημα, και οτιδήποτε υπάρχει σε επίπεδο πάνω από αυτά είναι διεργασίες του χρήστη.

3.1 Transport Layer Security

Το TLS είναι ένα πρωτόκολλο κρυπτογράφησης το οποίο λειτουργεί πάνω από το TCP επίπεδο το οποίο προσφέρει ασφάλεια στις επικοινωνίες μέσα σε ένα δίκτυο. Χρησιμοποιείται από φυλλομετρητές καθώς και άλλες εφαρμογές οι οποίες θέλουν τα δεδομένα τους να μεταδίδονται με ασφάλεια στο δίκτυο π.χ. με την μεταφορά αρχείων, τις συνδέσεις VPN κτλ. Το TLS Χρησιμοποιεί δημοφιλείς διεπαφές προγραμματισμού εφαρμογών (API's) οι οποίες ονομάζονται sockets με σκοπό την διασύνδεση με το επίπεδο TCP.

Το TLS έχει μια ποικιλία από μέτρα ασφαλείας όπως:

- Προστασία από την υποβάθμιση του πρωτοκόλλου σε προηγούμενη έκδοση του η οποία ήταν λιγότερο ασφαλής.
- Αρίθμηση μεταγενέστερων αιτήσεων με έναν αριθμό ακολουθίας ο οποίος θα χρησιμοποιείται μέσα στον κωδικό ταυτότητας του μηνύματος (MAC)
- Το μήνυμα που τελειώνει το handshake στέλνει ένα hash όλων των μηνυμάτων που ανταλλάχτηκαν το οποίο το βλέπουν και οι δύο πλευρές.

3.2 HTTPS

Το http είναι το πρωτόκολλο το οποίο χρησιμοποιείται για την πλοήγηση στο δίκτυο. Η λειτουργία του https είναι παρόμοια με αυτή του http, με την διαφορά ότι η πρώτη προσφέρει ασφαλή πλοήγηση με την χρήση του SSL. Αυτό το πρωτόκολλο χρησιμοποιείται για να προσφέρει κρυπτογραφημένη και επικυρωμένη σύνδεση μεταξύ του χρήστη και του διακομιστή της ιστοσελίδας. Η ασφαλής πλοήγηση μέσω του https διασφαλίζει ότι τα παρακάτω δεδομένα είναι κρυπτογραφημένα:

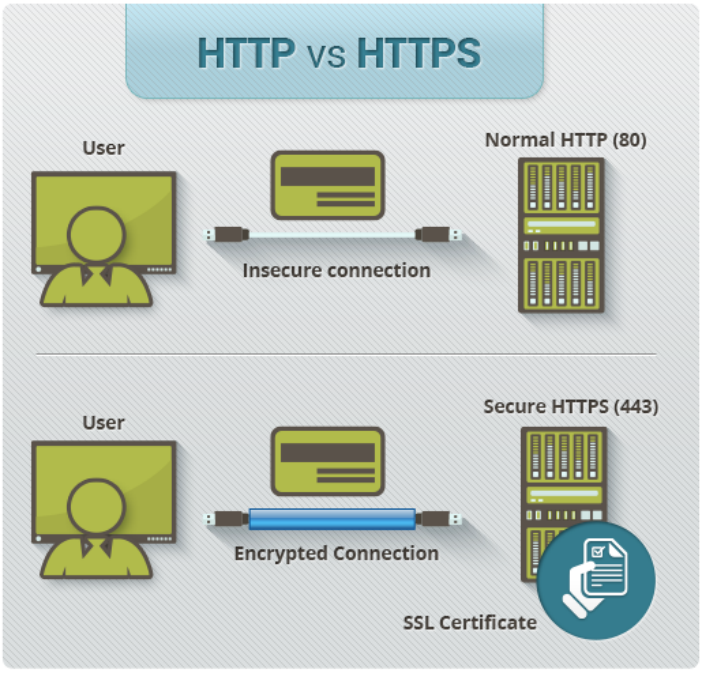
- Ο υπερσύνδεσμος της σελίδας
- Τα περιεχόμενα της σελίδας που παρέχονται από τον διακομιστή της σελίδας στον χρήστη.
- Τα περιεχόμενα διάφορων φορμών που συμπληρώνει ο χρήστης

- Τα αρχεία κειμένου (cookies) και στις δύο κατευθύνσεις.

Το πρωτόκολλο εφαρμογής του https συνήθως χρησιμοποιεί ένα από τα δύο πρωτόκολλα TLS ή SSL. Η διαδικασία για την ασφαλή πλοήγηση περιγράφεται ως εξής:

- Καλούμε μια https σύνδεση σε μια ιστοσελίδα βάζοντας https και τον υπερσύνδεσμο σε μια γραμμή διευθύνσεων
- Ο φυλλομετρητής ξεκινάει μια σύνδεση με τον web διακομιστή. Η χρήση του https καλεί το SSL πρωτόκολλο
- Ο φυλλομετρητής χρησιμοποιεί την πόρτα (port) 443 του συστήματος αντί για την 80 που χρησιμοποιεί το http
- Το πρωτόκολλο SSL χρησιμοποιεί ένα handshake πρωτόκολλο για την δημιουργία μιας ασφαλούς συνεδρίας
- Η ιστοσελίδα αρχικά στέλνει την ψηφιακή υπογραφή της στον φυλλομετρητή. Κατά την επαλήθευση η διαδικασία του handshake προχωράει στην ανταλλαγή των πληροφοριών για την συνεδρία.

Η χρησιμότητα του https είναι ότι προσφέρει εμπιστευτικότητα, αυθεντικοποίηση και ακεραιότητα των μηνυμάτων στον χρήστη. Με αυτόν τον τρόπο μπορούν και γίνονται ασφαλείς συναλλαγές στο διαδίκτυο χωρίς να υπάρχει ανησυχία για τυχόν υποκλοπή των δεδομένων. Στην παρακάτω εικόνα παρουσιάζεται η διαφορά του http με το https που έγκειται στο γεγονός ότι στη σύνδεση https χρησιμοποιείται κρυπτογράφηση μέσω ενός SSL πιστοποιητικού. (6)



Εικόνα 4 - Difference Between http:// and https://

3.3 Secure Shell (SSH)

Το Secure Shell είναι ένα πρωτόκολλο κρυπτογράφησης το οποίο παρέχει υπηρεσίες λειτουργίας του δικτύου με ασφάλεια πάνω σε ένα μη ασφαλές δίκτυο. Το SSH παρέχει ένα ασφαλές κανάλι μέσω ενός μη ασφαλούς δικτύου, συνδέοντας μια SSH εφαρμογή του χρήστη με έναν SSH διακομιστή.

Τα κυριότερα χαρακτηριστικά του είναι τα εξής:

- Το SSH είναι ένα πρωτόκολλο δικτύου πού λειτουργεί πάνω από το επίπεδο του TCP/IP. Έχει σχεδιαστεί να αντικαταστήσει το TELNET το οποίο δεν παρείχε ασφάλεια για την δημιουργία μιας απομακρυσμένης σύνδεσης

- Το SSH παρέχει μια ασφαλή επικοινωνίας μεταξύ χρήστη και διακομιστή και μπορεί να χρησιμοποιηθεί για εργασίες όπως η μεταφορά αρχείων και η αλληλογραφία.

- Το SSH είναι ένα διαδεδομένο πρωτόκολλο το οποίο παρέχει βελτιωμένη ασφάλεια επικοινωνίας στο δίκτυο σε σύγκριση με την παλαιότερη έκδοση του SSH1.

Το SSH χωρίζεται σε 3 πρωτόκολλα

- Πρωτόκολλο επίπεδου μετάδοσης: Αυτό το μέρος του SSH πρωτοκόλλου παρέχει εμπιστευτικότητα και ακεραιότητα στα δεδομένα και αυθεντικοποίηση από τον διακομιστή. Μπορεί επίσης να παρέχει συμπίεση των δεδομένων.

    - Αυθεντικοποίηση του διακομιστή: Τα κλειδιά των χρηστών είναι ασύμμετρα, όπως τα δημόσια και τα ιδιωτικά κλειδιά. Ένας διακομιστής χρησιμοποιεί ένα δημόσιο κλειδί για να αποδείξει την ταυτότητά του στον χρήστη. Ο χρήστης επιβεβαιώνει ότι διακομιστής που επικοινώνησε είναι γνωστός στον χρήστη από την βάση δεδομένων που διατηρεί. Μόλις γίνει η αυθεντικοποίηση του διακομιστή, δημιουργούνται τα κλειδιά για την συνεδρία (session).

    - Εγκατάσταση κλειδιών για συνεδρίες: Μετά την αυθεντικοποίηση, ο διακομιστής και ο χρήστης συμφωνούν για το ποια κρυπτογράφηση θα χρησιμοποιηθεί, και έπειτα κλειδιά για την συνεδρία παράγονται και από τους δύο. Τα κλειδιά αυτά παράγονται πριν την αυθεντικοποίηση του χρήστη ώστε το όνομα του χρήστη (username) και ο κωδικός να αποστέλλονται κρυπτογραφημένα. Αυτά τα κλειδιά αντικαθίστανται σε τακτά χρονικά διαστήματα κατά την διάρκεια της συνεδρίας και καταστρέφονται έπειτα από την λήξη της σύνδεσης.

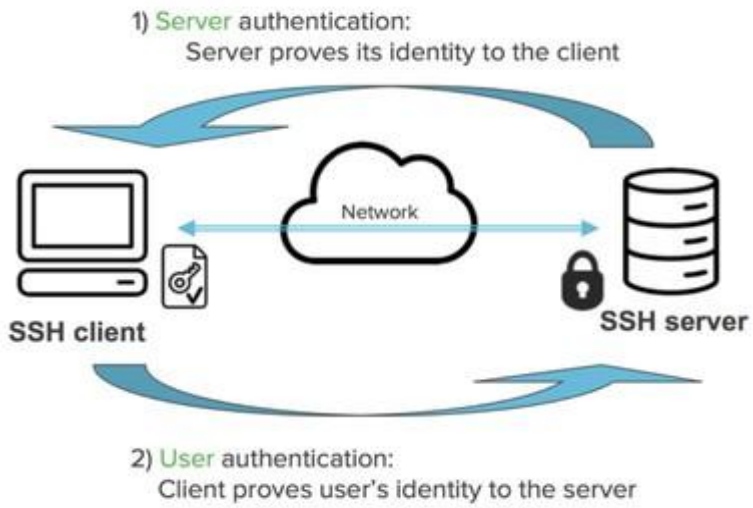
    - Ακεραιότητα των δεδομένων: Το SSH χρησιμοποιεί τον αλγόριθμο MAC για τον έλεγχο της ακεραιότητας των δεδομένων. Το MAC

δέχεται ως είσοδο ένα μυστικό κλειδί και ένα μήνυμα που χρειάζεται να πιστοποιηθεί και εξάγει μια τιμή MAC η οποία προστατεύει την ακεραιότητα και αυθεντικότητα των δεδομένων, επιτρέποντας τον έλεγχο για τον εντοπισμό τυχόν αλλαγών στο περιεχόμενο του μηνύματος.

- Πρωτόκολλο ελέγχου ταυτότητας: Αυτό το μέρος του SSH επεξεργάζεται την αυθεντικοποίηση του χρήστη στον διακομιστή. Με την σειρά ο διακομιστής επαληθεύει ότι η πρόσβαση δίνεται μόνο στους εξουσιοδοτημένους χρήστες. Υπάρχουν αρκετές μέθοδοι αυθεντικοποίησης όπως με τους κωδικούς πρόσβασης, το Kerberos κτλ.

- Πρωτόκολλο σύνδεσης: Προσφέρει πολλαπλά λογικά κανάλια πάνω σε μια SSH σύνδεση.

Στην ακόλουθη εικόνα παρουσιάζεται η διαδικασία της αυθεντικοποίησης μέσω ενός SSH κλειδιού.



Εικόνα 5 – SSH Key

3.4 KERBEROS

Το πρωτόκολλο ελέγχου ταυτότητας Kerberos εφευρέθηκε στο τέλος της δεκαετίας του 1980 στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT) στην Βοστώνη ως μέρος του προγράμματος Αθηνά. Ωστόσο βρίσκεται ακόμα υπό ενεργή ανάπτυξη και με τη δημοσιοποίηση του Kerberos 5 υπήρξε μια σημαντική αναθεώρηση το 2005. Το σύστημα λειτουργεί ως κέντρο ελέγχου ταυτότητας και πρόσβασης για ομάδες σταθμών εργασίας. Οι κύριοι στόχοι στον σχεδιασμό του Kerberos ήταν:

- Ασφάλεια: Ούτε οι παθητικοί ούτε οι ενεργητικοί επιτιθέμενοι δεν θα έπρεπε να είναι σε θέση να προσποιηθούν κάποιον άλλον κατά τη πρόσβαση σε μια

υπηρεσία ή να είναι σε θέση να κρυφακούσουν τις απαραίτητες πληροφορίες που θα τους βοηθήσουν να το πετύχουν.

- Αξιοπιστία: Επειδή κάθε χρήση της υπηρεσίας απαιτεί από πριν ταυτοποίηση, η ίδια η υπηρεσία Kerberos πρέπει να σχεδιαστεί ώστε να είναι ιδιαίτερα αξιόπιστη και πάντα διαθέσιμη.

- Διαφάνεια: Πέρα από την απαίτηση εισαγωγής κωδικού πρόσβασης κατά την έναρξη μιας συνόδου, η διαδικασίας επαλήθευσης ταυτότητας θα πρέπει να είναι σε μεγάλο βαθμό διαφανής για τον χρήστη.

- Επεκτασιμότητα: Το Kerberos πρέπει να έχει τη δυνατότητα να υποστηρίξει έναν μεγάλο αριθμό χρηστών, σταθμών εργασίας, υπηρεσιών και διακομιστών.

4. Ασφάλεια στο επίπεδο δικτύου

4.1 Πρωτόκολλο IPSec

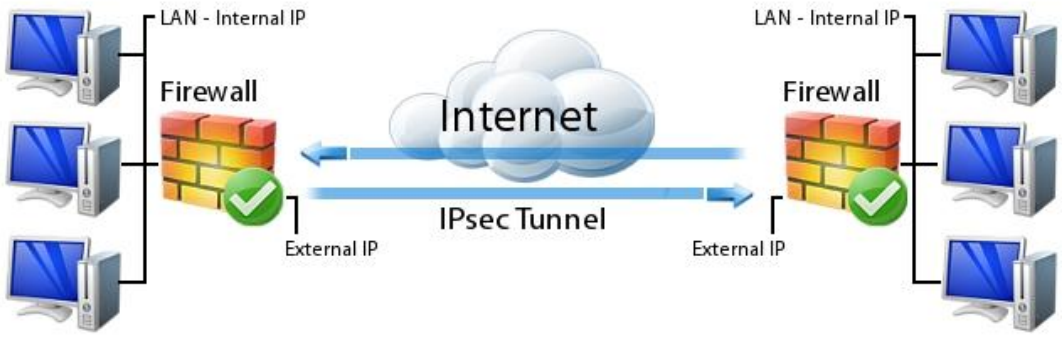
Το δημοφιλές πλαίσιο που αναπτύχθηκε για την διασφάλιση της ασφάλειας στο επίπεδου δικτύου είναι το Internet Protocol Security (IPSec).

Τα πρωτόκολλα TCP/IP δεν παρέχουν μηχανισμούς κρυπτογράφησης. Συνεπώς, για την ασφαλή μετάδοση πάνω σε δίκτυο IP υπήρξε η ανάγκη νέου πρωτοκόλλου με μηχανισμούς κρυπτογράφησης, το οποίο θα είναι εφαρμόσιμο σε IP δίκτυα. Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την ασφαλή μετάδοση και ανταλλαγή δεδομένων (packets) μέσω του στρώματος IP. Το IPSec σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN. (7)

Το IPSec λειτουργεί κάνοντας έλεγχο της ταυτότητας καθώς και κρυπτογραφώντας κάθε ένα IP πακέτο μιας σύνδεσης. Περιλαμβάνει πρωτόκολλα για την εγκατάσταση μιας κοινής αυθεντικοποίησης ανάμεσα στους agents κατά την έναρξη μιας συνεδρίας και διαπραγματεύεται για το ποια κρυπτογραφικά κλειδιά θα χρησιμοποιηθούν κατά την διάρκεια της συνεδρίας. Το IPSec μπορεί να προστατεύσει την ροή δεδομένων μεταξύ ενός ζεύγους χρηστών, μεταξύ 2 πυλών ασφαλείας (gateways), και μεταξύ μιας πύλης και ενός χρήστη. Επίσης χρησιμοποιεί υπηρεσίες κρυπτογράφησης ώστε να προστατεύσει τις επικοινωνίες στα IP δίκτυα. Το IPSec υποστηρίζει σε επίπεδο δικτύου τον έλεγχο ταυτότητας καθώς και τα στοιχεία της προέλευσης της ταυτότητας, την ακεραιότητα και εμπιστευτικότητα των δεδομένων (με την χρήση της κρυπτογράφησης). Οι σημαντικές λειτουργίες ασφαλείας που παρέχονται από το IPSec είναι οι εξής:

- Εμπιστευτικότητα: Επιτρέπει στους κόμβους που επικοινωνούν να κρυπτογραφούν τα μηνύματα τους και αποτρέπει τις υποκλοπές από τρίτους.
- Αυθεντικοποίηση και ακεραιότητα των δεδομένων: Παρέχει την διαβεβαίωση ότι ένα πακέτο που λήφθηκε μεταδόθηκε από τον πραγματικό χρήστη, και επιβεβαιώνει ότι το πακέτο δεν έχει αλλοιωθεί.
- Διαχείριση των κλειδιών: Επιτρέπει την ασφαλή ανταλλαγή των κλειδιών και παρέχει προστασία από ορισμένους τύπους επιθέσεων.

Στην παρακάτω εικόνα παρουσιάζεται η διαδικασία με την οποία λειτουργεί το πρωτόκολλο IPSec στην επικοινωνία 2 τοπικών δικτύων μέσω του διαδικτύου.



Εικόνα 6 – IPSec Tunnel

4.2 Ασφάλεια Δρομολόγησης

Ο αυτόματος προσδιορισμός των διαδρομών των πακέτων δεδομένων είναι μια βασική υπηρεσία στα δίκτυα υπολογιστών. Αυτή η δρομολόγηση πραγματοποιείται συνήθως σε δίκτυα IP μέσω κατανεμημένων αλγορίθμων. Ουσιαστικά υπάρχει διάκριση μεταξύ των πρωτοκόλλων απόστασης-φορέα και των πρωτοκόλλων σύνδεσης-κατάστασης, αφού στα πρώτα οι δρομολογητές ενημερώνουν ο ένας τον άλλον για τους προορισμούς που μπορούν να φτάσουν και τα αντίστοιχα έξοδα. Επίσης αν είναι απαραίτητο οι δρομολογητές ενημερώνουν τους άλλους γειτονικούς για αλλαγές δρομολογίων και μετά στέλνουν τα πακέτα τους στον προορισμό μέσω των γειτόνων με τα χαμηλότερα κόστη διαδρομής. Παραδείγματα τέτοιων πρωτοκόλλων (απόστασης-φορέα) είναι το "πρωτόκολλο πληροφοριών δρομολόγησης" (Routing Information Protocol) RIP και το «πρωτόκολλο ιδιόκτητης εσωτερικής πύλης δρομολόγησης» (Interior Gateway Routing Protocol) IGRP.

Στην δεύτερη κατηγορία πρωτοκόλλων(σύνδεσης-κατάστασης) οι δρομολογητές διανέμουν τις περιγραφές των κόστων σύνδεσης σε ολόκληρο το δίκτυο με τη βοήθεια του flooding. Με αυτό τον τρόπο, κάθε δρομολογητής ξέρει ολόκληρο το δίκτυο και μπορεί να υπολογίσει τα συντομότερα μονοπάτια μέσω του αλγορίθμου Dijkstra. Το πιο χαρακτηριστικό πρωτόκολλο από αυτή την κατηγορία είναι το "πρώτο πρωτόκολλο ανοιχτής συντομότερης διαδρομής" (Open Shortest Path First Protocol) OSPF.

Όλα τα πρωτόκολλα δρομολόγησης που αναφέρθηκαν μέχρι τώρα έχουν ένα κοινό στοιχείο: είναι πρωτόκολλα εσωτερικής πύλης (Interior Gateway Protocols) δηλαδή χρησιμοποιούνται μόνο στο εσωτερικό ενός αυτόνομου συστήματος του παρόχου υπηρεσίας.

Μεταξύ των δικτύων IP που υπόκεινται σε διαφορετικές διοικητικές αρχές, το πρωτόκολλο πύλης συνόρου (Border Gateway Protocol) BGP είναι το ουσιαστικό πρότυπο πρωτόκολλο δρομολόγησης. Το BGP είναι πρωτόκολλο μονοπατιού-φορέα, δηλαδή ουσιαστικά συμπεριφέρεται σαν πρωτόκολλο απόστασης-φορέα αλλά

ανταλλάσσονται με τους γείτονες και τα ολοκληρωμένα μονοπάτια στις ατομικές διαδρομές και όχι μόνο τα κόστη των διαδρομών. Αυτό επιτρέπει την πρόληψη βρόχων δρομολόγησης.

Για λόγους ασφαλείας οι δρομολογητές βρίσκονται συνήθως σε φυσικά προστατευμένες τοποθεσίες και λειτουργούν μόνο από εκπαιδευμένο προσωπικό. Οι καταστάσεις απειλών για επίθεση σε πρωτόκολλα δρομολόγησης στο εσωτερικό οργανισμών είναι πολύ σπάνιες. Τέτοιες καταστάσεις στο ιντερνέτ είναι πιο δύσκολες αφού χιλιάδες διαφορετικοί οργανισμοί ανταλλάσσουν πληροφορίες ο ένας με τον άλλον με τη βοήθεια του BGP. Οι απειλές μπορούν να διαφοροποιηθούν ως ακολούθως:

- **Πηγή μιας επίθεσης:** Μια επίθεση σε πρωτόκολλο δρομολόγησης μπορεί να πραγματοποιηθεί στη σύνδεση μεταξύ 2 δρομολογητών, για παράδειγμα με την τροποποίηση των ανταλλασσόμενων πακέτων. Εναλλακτικά, ο επιτιθέμενος μπορεί να θέσει σε κίνδυνο έναν ή και περισσότερους δρομολογητές ή να αυξήσει τον αριθμό τους στο σύστημα χωρίς άδεια.

- **Έκταση μιας επίθεσης:** Ανάλογα με τη δομή του δικτύου και τη θέση και τη διαδικασία του επιτιθέμενου, ίσως επηρεαστούν μόνο μεμονωμένοι δρομολογητές, συγκεκριμένες περιοχές του δικτύου ή και ολόκληρο το διαδίκτυο.

- **Συνέπεια μιας επίθεσης:** Οι λεπτομερείς πληροφορίες σχετικά με το πώς κατασκευάζονται τα δίκτυα είναι συνήθως εμπιστευτικές, επομένως ακόμα και η ανακάλυψη πληροφοριών δρομολόγησης ίσως αποτελέσει πρόβλημα. Επιπλέον, οι δρομολογητές μπορούν να εξαπατηθούν από μηνύματα που δεν είναι αυθεντικά με αποτέλεσμα είτε να διαταράσσονται οι κανονικές εργασίες δρομολόγησης, είτε να είναι σε θέση ο επιτιθέμενος να ελέγξει την κυκλοφορία.

- **Διάρκεια των συνεπειών μιας επίθεσης:** Οι συνέπειες μπορεί να υπάρξουν μόνο τη στιγμή της επίθεσης ή μπορεί να διαρκέσουν μέχρι να σταθεροποιηθεί το δίκτυο. Με το BGP-λόγω των σύνθετων πολιτικών με τις οποίες προωθούνται ή καθυστερούν οι διαδρομές-είναι θεωρητικώς πιθανό ότι μια μη-αυτόματη παρέμβαση θα είναι αναγκαία για τη σύγκλιση.

Από την άποψη ενός δικτύου, οι ακόλουθες βασικές απειλές υπάρχουν λεπτομερώς σε σχέση με τη διαθεσιμότητα:

- **Συμφόρηση:** Εξαιτίας της επαναδρομολόγησης της κυκλοφορίας, μπορούν να προκύψουν καταστάσεις συμφόρησης σε τμήματα του δικτύου με αποτέλεσμα μερικές φορές να χάνονται πακέτα.

- **Επιθέσεις μαύρης τρύπας (Black hole attacks):** Αν ένας επιτιθέμενος προκαλέσει την προώθηση πακέτων σε έναν δρομολογητή που δεν έχει έγκυρη διαδρομή προορισμού, τα πακέτα θα ακυρωθούν.

- **Βρόχοι δρομολόγησης:** Αν ένας επιτιθέμενος μπορεί να κανονίσει ώστε 2 ή περισσότεροι δρομολογητές θα διαβιβάσουν την κυκλοφορία σε έναν προορισμό, κυκλικά πάνω στον καθένα, τότε από τη μία πλευρά θα προκύψει κατάσταση συμφόρησης για άλλα πακέτα που έχουν ίδια τμήματα διαδρομής και από την άλλη πλευρά τα πακέτα στον προορισμό θα πέφτουν αφού φτάσουν τον μέγιστο αριθμό κόμβων.

- **Λογικός διαχωρισμός δικτύου:** Ένας επιτιθέμενος μπορεί, υπό συγκεκριμένες περιστάσεις, να χειριστεί τμήματα του δικτύου με τέτοιο τρόπο που φαίνεται ότι δεν υπάρχει καμία έγκυρη διαδρομή στο υπόλοιπο δίκτυο. Σε αυτή την περίπτωση, τα πακέτα δεν μπορούν να φτάσουν στο σχετικό υποδίκτυο.

- **Συχνές αλλαγές δρομολόγησης:** Οι διαδρομές μέσα από το δίκτυο μπορούν να αλλάζουν συνεχώς μέσω των συχνών αλλαγών δρομολόγησης και επομένως προκαλούνται διακυμάνσεις στα πακέτα καθυστέρησης και ενημέρωσης για τον τελικό χρήστη.

- **Αστάθειες κατά τη σύγκλιση της δρομολόγησης:** Εξαιτίας των χειρισμών του επιτιθέμενου, το πρωτόκολλο δρομολόγησης μπορεί, υπό ορισμένες συνθήκες, να αποκλειστεί από τη σύγκλιση και να προληφθεί η προσαρμογή των σχετικών διαδρομών.

- **Υπερφόρτωση λόγω του πρωτοκόλλου δρομολόγησης:** Εξαιτίας των αλλαγών στη δρομολόγηση, αφενός ένα σημαντικό εύρος ζώνης μπορεί να χρειαστεί για το ίδιο το πρωτόκολλο δρομολόγησης, και από την άλλη πλευρά οι δρομολογητές μπορούν να φορτωθούν σε τέτοιο βαθμό ώστε να μπορούν να ανταποκριθούν πολύ αργά στις νόμιμες αλλαγές. Στο πλαίσιο αυτό χρησιμοποιείται ο όρος "BGP update storm"

Παράλληλα με αυτό, οι επιτιθέμενοι μπορούν παράλληλα να χειραγωγήσουν τη δρομολόγηση και να ανακατευθύνουν τις επιθέσεις BGP που στοχεύουν την κυκλοφορία, στον εαυτό τους. Με αυτό τον τρόπο η κυκλοφορία που σε άλλη περίπτωση θα υπήρχε η δυνατότητα επαναδρομολόγησής της θα είναι απροσπέλαστη και μπορεί να παρακολουθηθεί ή χειραγωγηθεί από τους επιτιθέμενους.

Οι ακόλουθες 2 απειλές αναφέρονται συχνά σε αυτό το πλαίσιο:

- **Sinkhole attack:** Αν οι επιτιθέμενοι δίνουν ψεύτικές διευθύνσεις ή μετρήσεις και έτσι παίρνουν περισσότερη κυκλοφορία για αυτούς από ότι θα ήταν το φυσιολογικό, αυτή η περίπτωση αναφέρεται ως Sinkhole attack.

- **Wormhole attack:** Μπορεί να είναι πιθανό υπό ορισμένες συνθήκες για τους επιτιθέμενους να προσομοιώσουν μια σύνδεση μεταξύ δρομολογητών σε απόσταση που δεν υπάρχει στην πραγματικότητα, για παράδειγμα με την προώθηση της κυκλοφορίας μέσω σηράγγων. Έτσι, διαβιβάζεται περισσότερη πληροφορία μέσω των δρομολογητών, καθώς η σύνδεση γίνεται αντιληπτή ως μια συντόμευση μεταξύ των διαφόρων περιοχών του δικτύου.

Από την άποψη των τελικών συστημάτων, οι επιπτώσεις αυτών των παγκόσμιων απειλών εμφανίζονται κάπως διαφορετικές:

- **Καθυστέρηση και παραμόρφωση:** Η καθυστέρηση και η παραμόρφωση των μεταδιδόμενων πακέτων αυξάνεται αν η κυκλοφορία διαρκεί περισσότερο ή αν υπερφορτώνονται τα μονοπάτια σε ορισμένους προορισμούς. Ο επιτιθέμενος μπορεί επίσης να διαβιβάσει τα πακέτα σε παραβιασμένα συστήματα και να τα κρατήσει εκεί με τεχνικό τρόπο. Αυτό το είδος επίθεσης μερικές φορές αναφέρεται με το όνομα Jellyfish, είναι πολύ δύσκολο να ανιχνευτεί και μειώνει σημαντικά το ποσοστό απόδοσης σε ορισμένες περιπτώσεις.

- **Μη-διαθεσιμότητα:** Τα πακέτα μπορούν να χαθούν υπό ορισμένες συνθήκες επειδή τμήματα του δικτύου πιστεύουν ότι δεν μπορούν να φτάσουν στον προορισμό ή επειδή υπάρχει δρομολόγηση βρόχου.

- **Παρακολούθηση της κίνησης:** Η κυκλοφορία μεταξύ 2 μερών μπορεί ενδεχομένως να παρακολουθείται ακόμα και αν ο επιτιθέμενος δεν είναι στο πιο σύντομο μονοπάτι μεταξύ των 2 εταίρων επικοινωνίας. Ακόμα και αν χρησιμοποιούνται μέθοδοι κρυπτογράφησης, είναι συνήθως πιθανό για τον επιτιθέμενο να προβεί σε ανάλυση της ροής της κυκλοφορίας και να αποφασίσει ποιά μέρη επικοινωνούν, πότε επικοινωνούν και με πόση ένταση. Μπορεί ακόμα και να είναι δυνατή η επανασύσταση της εφαρμογής, με βάση το μέγεθος του πακέτου και τα μοτίβα επικοινωνίας.

- **Ελεγχόμενη παράδοση:** Οι επιτιθέμενοι μπορεί να είναι σε θέση να απορρίψουν κάποια συγκεκριμένα μεμονωμένα πακέτα. Επιπλέον, ακόμα και αν λαμβάνει χώρα η προστασία κρυπτογράφησης, είναι συχνά επίσης δυνατό να πραγματοποιηθεί ταυτοποίηση και στοχεύμενη καταστολή, με βάση για παράδειγμα την εφαρμογή και ανάλογα με το μοτίβο της επικοινωνίας. Αυτή η μορφή επίθεσης περιγράφεται στη βιβλιογραφία ως grey hole attack.

Ο μεγάλος αριθμός των απειλών και η πολυπλοκότητά τους απεικονίζουν τις προκλήσεις που προκύπτουν κατά την προστασία μιας υποδομής δρομολόγησης. Σε σύγκριση με τη διασφάλιση της μετάδοσης, για παράδειγμα με τη βοήθεια του IPSec, το βασικό πρόβλημα είναι ότι δεν είναι μόνο αναγκαίο να ασχοληθούμε με τους επιτιθέμενους μεταξύ των τερματικών συστημάτων, αλλά να πετύχουμε και μία συναίνεση μεταξύ των δρομολογητών, όπου κάποιοι από τους οποίους θα έχουν πιθανώς παραβιαστεί. Η ανάπτυξη των μέτρων ασφαλείας, εστιάζεται ιδιαίτερα στο

BGP, επειδή το πρωτόκολλο έχει παγκόσμια επιρροή και, λόγω του μεγάλου αριθμού των οργανώσεων που συμμετέχουν, είναι λογικό να αναμένουμε την πλειονότητα των επιθέσεων για αυτό.

Οι επιθέσεις στο BGP σπάνια τεκμηριώνονται ως τέτοιες και οι περισσότερες από αυτές συχνά θεωρούνται απλά ως "εσφαλμένες ρυθμίσεις παραμέτρων". Ωστόσο, το 2013 ήταν δυνατόν να ανακατασκευαστεί μια επίθεση man-in-the-middle με λεπτομερή τρόπο. Σε αυτή την περίπτωση, για μια περίοδο αρκετών μηνών ο Ρώσικος πάροχος GlobalOneBel χρησιμοποίησε κατ'επανάληψη το BGP για να ανακοινώσει 1500 μπλοκ διεύθυνσης σε διάφορα χρονικά διαστήματα, για τα οποία δεν είχε στην πραγματικότητα καμία άδεια. Ως αποτέλεσμα, η αντίστοιχη κυκλοφορία προσελκύστηκε από τον πάροχο GlobalOneBel στη Μόσχα και δρομολογήθηκε σε αυτόν.

Μετά την «επιθεώρηση», η κυκλοφορία του GlobalOneBel προωθήθηκε σε διαφορετικούς παρόχους στη Φρανκφούρτη και στο Μέιν που δεν είχαν αναλάβει τις ψεύτικες διαδρομές και είχαν παραδώσει την κυκλοφορία στον αρχικό προορισμό. Καθώς οι αλλαγές είναι συνήθως μόνο προσωρινές και είναι δύσκολο να ανακατασκευαστούν, ακόμα και με τη χρήση των διαδρομών ανίχνευσης (trace routes), τέτοιες επιθέσεις είναι πολύ δύσκολο να ανιχνευτούν και να προληφθούν.

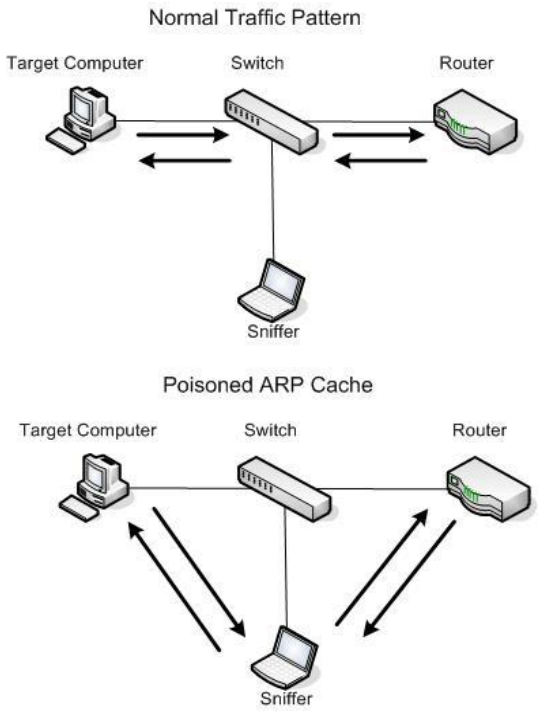
5. Ασφάλεια στο επίπεδο ζεύξης δεδομένων

Το επίπεδο ζεύξης δεδομένων στα Ethernet δίκτυα είναι ιδιαίτερα επιρρεπές σε διάφορες επιθέσεις. Οι πιο συχνές από αυτές είναι:

5.1 ARP Spoofing

Το ARP είναι ένα πρωτόκολλο που χρησιμοποιείται για να χαρτογραφήσει μια διεύθυνση IP σε μια φυσική διεύθυνση την οποία γνωρίζει το τοπικό Ethernet. Όταν ένα μηχάνημα πρέπει να βρει μια MAC διεύθυνση για μια διεύθυνση IP, μεταδίδει ένα αίτημα ARP. Ο άλλος χρήστης στον οποίο ανήκει η IP διεύθυνση στέλνει ένα απαντητικό μήνυμα ARP με την φυσική διεύθυνση. Το κάθε ένα μηχάνημα στο δίκτυο διατηρεί έναν πίνακα ο οποίος ονομάζεται μνήμη ARP. Ο πίνακας περιέχει τις διευθύνσεις IP καθώς και τις MAC διευθύνσεις όλων των χρηστών στο δίκτυο. Το ARP είναι ένα stateless πρωτόκολλο, δηλαδή κάθε φορά που ένας χρήστης λαμβάνει μια απάντηση από έναν άλλο χρήστη, ακόμα και αν ο ίδιος δεν έχει κάνει ένα ARP αίτημα, δέχεται την απάντηση και ενημερώνει την ARP μνήμη του.

Η διαδικασία της τροποποίησης της μνήμης ARP με μία πλαστή καταχώρηση είναι γνωστή ως ARP poisoning ή spoofing. Η πλαστογράφηση (spoofing) ARP μπορεί να επιτρέψει σε έναν επιτιθέμενο να "μεταμφιεστεί" ως ένας νόμιμος χρήστης και μετά να παρακολουθεί τα πακέτα δεδομένων σε ένα δίκτυο, να μπορεί να τα τροποποιήσει ή και να τα σταματήσει. Συχνά αυτή η επίθεση χρησιμοποιείται για να ξεκινήσουν άλλων ειδών επιθέσεις, όπως DOS, man-in-the-middle κτλ. Στην παρακάτω εικόνα φαίνεται η διαφορά στη κανονική ροή κυκλοφορίας στο δίκτυο, σε σύγκριση με τη ροή κυκλοφορίας όταν έχει πραγματοποιηθεί ARP poisoning. (8)



Εικόνα 7 – Παρακολούθηση της επικοινωνίας με ARP Cache Poisoning

5.1.1 Αποτροπή της πλαστοπροσωπίας (spoofing) ARP

Η μέθοδος της ασφάλειας στις θύρες μπορεί να αποτρέψει τις επιθέσεις MAC flooding και cloning. Ωστόσο αυτό δεν εμποδίζει το ARP spoofing. Η ασφάλεια στις θύρες επιβεβαιώνει την πηγή της MAC διεύθυνσης στην κεφαλίδα του πλαισίου, αλλά τα ARP πλαίσια εμπεριέχουν ένα επιπλέον MAC πεδίο στα δεδομένα, και ο χρήστης χρησιμοποιεί αυτό το πεδίο για να συμπληρώσει την μνήμη ARP. Παρακάτω δίνονται κάποιες από τις μεθόδους για την αποτροπή του ARP spoofing.

- Στατικό ARP: Μια από τις συνιστώμενες ενέργειες είναι η χρήση των στατικών ARP καταχωρήσεων στον ARP πίνακα. Οι στατικές καταχωρήσεις του ARP είναι μόνιμες καταχωρήσεις στην μνήμη. Ωστόσο αυτή η μέθοδος δεν είναι πρακτική, και δεν επιτρέπει την χρήση κάποιων DHCP διευθύνσεων καθώς οι στατική IP πρέπει να χρησιμοποιείται από όλους τους χρήστες στο επίπεδο ζεύξης δεδομένων (data link)

- Σύστημα ανίχνευσης εισβολής: Η μέθοδος της άμυνας για την αξιοποίηση αυτού του συστήματος είναι διαμόρφωση του έτσι ώστε να ανιχνεύει όταν υπάρχει μεγάλος φόρτος σε αιτήματα ARP. Ωστόσο το μειονέκτημα του είναι πως είναι επιρρεπές σε ψευδείς αναφορές.

Δυναμικό ARP: Αυτή η μέθοδος αποτροπής του ARP spoofing είναι παρόμοια με αυτή του DHCP Snooping. Χρησιμοποιεί τις αξιόπιστες και μη αξιόπιστες θύρες. Οι απαντήσεις του ARP επιτρέπονται μόνο στις αξιόπιστες θύρες. Αν μια απάντηση ARP έρθει στην μη αξιόπιστη θύρα, τότε τα περιεχόμενα της απάντηση συγκρίνονται με τον πίνακα DHCP για να ελεγχθεί η ακρίβεια του. Αν η απάντηση δεν είναι έγκυρη τότε απορρίπτεται και η θύρα απενεργοποιείται.

5.2 MAC flooding

Ο κάθε μεταγωγέας που υπάρχει στο Ethernet έχει ένα πίνακα (CAM) ο οποίος αποθηκεύει τις MAC διευθύνσεις, τους αριθμούς των port των μεταγωγέων καθώς και άλλες πληροφορίες. Ο πίνακας έχει συγκεκριμένο μέγεθος με αποτέλεσμα, όταν γίνεται μια επίθεση MAC flooding, ο επιτιθέμενος “γεμίζει” τον μεταγωγέα με MAC διευθύνσεις χρησιμοποιώντας πλαστογραφημένα ARP πακέτα μέχρι να γεμίσει ο πίνακας. Μόλις ο πίνακας γεμίσει, ο μεταγωγέας ξεκινάει την μετάδοση των δεδομένων σε όσους δεν είναι καταχωρημένοι στον CAM πίνακα. Ο επιτιθέμενος ο οποίος είναι στο ίδιο δίκτυο λαμβάνει όλα τα πακέτα τα οποία προορίζονταν για ένα συγκεκριμένο χρήστη.

5.3 Port Stealing

Οι μεταγωγείς του Ethernet έχουν την δυνατότητα να μαθαίνουν και να δεσμεύουν τις MAC διευθύνσεις σε ports. Όταν ένας μεταγωγέας λαμβάνει δεδομένα από μια port με μια διεύθυνση MAC, δεσμεύει τον αριθμό της port και την MAC διεύθυνση. Η επίθεση port stealing εκμεταλλεύεται αυτήν την ιδιότητα των μεταγωγών. Ο επιτιθέμενος γεμίζει τον μεταγωγέα με πλαστά ARP πλαίσια δεδομένων με την MAC διεύθυνση του χρήστη ως την διεύθυνση πηγής. Ο μεγαγωγέας μπερδεύεται και πιστεύει ότι ο χρήστης είναι στην port, αλλά στην πραγματικότητα είναι ο επιτιθέμενος. Και όλα τα πλαίσια δεδομένων που προορίζονταν για έναν συγκεκριμένο χρήστη καταλήγουν στην port που έχει συνδεθεί ο επιτιθέμενος και όχι στον νόμιμο χρήστη. (9)

5.4 Επιθέσεις DHCP

Το Dynamic Host Configuration Protocol (DHCP) δεν είναι ένα πρωτόκολλο για την ζεύξη δεδομένων αλλά χρησιμεύει γιατί παρέχει λύσεις ώστε να ματαιώσει επιθέσεις που γίνονται στο επίπεδο ζεύξης δεδομένων (layer 2). Το DHCP χρησιμοποιείται για να κατανέμει δυναμικά τις διευθύνσεις στους υπολογιστές για ένα συγκεκριμένο χρονικό διάστημα. Είναι πιθανόν να γίνει επίθεση σε διακομιστές DHCP με την χρήση άρνησης υπηρεσιών στο δίκτυο. Σε μια επίθεση DHCP starvation, ο επιτιθέμενος ζητάει όλες τις διαθέσιμες DHCP διευθύνσεις, με αποτέλεσμα το σύστημα να μην μπορεί να εξυπηρετήσει τον νόμιμο χρήστη του δικτύου. Σε μια επίθεση πλαστογράφησης (spoofing) του DHCP, ο επιτιθέμενος μπορεί να αναπτύξει έναν πλαστό DHCP διακομιστή που θα παρέχει τις διευθύνσεις στους χρήστες. Με αυτόν τον τρόπο παρέχει στους χρήστες μια πλαστή πύλη (gateway) με τα DHCP αιτήματα. Τα πλαίσια δεδομένων από τους χρήστες καθοδηγούνται μέσω της πλαστής πύλης όπου ο επιτιθέμενος μπορεί να υποκλέψει όλα τα πακέτα και να απαντήσει στην πραγματική πύλη ή και να τα αποβάλει.

5.5 Ασφάλεια σε τοπικά δίκτυα

Ασφάλεια στις θύρες (ports)

Οι ασφάλεια στις θύρες βοηθάει στην προστασία του δικτύου με την αποτροπή άγνωστων συσκευών από το να προωθούν πακέτα. Οι ασφάλεια στις θύρες έχει τα εξής πλεονεκτήματα:

- Μπορείς να περιορίσεις των αριθμό των MAC διευθύνσεων σε μια συγκεκριμένη θύρα. Τα πακέτα που αντιστοιχούν σε μια διεύθυνση MAC προωθούνται ενώ όλα τα υπόλοιπα πακέτα περιορίζονται.

- Μπορείς να ενεργοποιήσεις την ασφάλεια για τις θύρες ανά θύρα.

Η ασφάλεια υλοποιεί δύο μεθόδους για τον έλεγχο της κυκλοφορίας, το στατικό και το δυναμικό κλείδωμα. Αυτές οι μέθοδοι μπορούν να χρησιμοποιηθούν και ταυτόχρονα.

- Δυναμικό κλείδωμα: Μπορούμε να ορίσουμε τον μέγιστο αριθμό ων MAC διευθύνσεων που μπορεί να γνωρίζει μια θύρα (port). Ο μέγιστος αριθμός των MAC διευθύνσεων εξαρτάται από την πλατφόρμα και δίνεται στις σημειώσεις έκδοσης του λογισμικού. Όταν φτάσει στο όριο, επιπλέον MAC διευθύνσεις δεν μπορούν να εξυπηρετηθούν. Μόνο τα πλαίσια τα οποία είναι από γνωστή πηγή προωθούνται.

  Οι δυναμικά κλειδωμένες διευθύνσεις μπορούν να μετατραπούν σε στατικά κλειδωμένες διευθύνσεις. Οι δυναμικές διευθύνσεις απορρίπτονται αν το πακέτο που έχουν στείλει αργήσει να ληφθεί από τον χρήστη μέσα στο επιτρεπτό χρονικό όριο. Το χρονικό όριο μπορεί να οριστεί, και οι δυναμικά κλειδωμένες MAC διευθύνσεις μπορούν να εξυπηρετηθούν από μια άλλη θύρα.

- Στατικό κλείδωμα: Μπορούμε να καθορίσουμε μια λίστα με στατικές MAC διευθύνσεις σε μια θύρα. Επίσης οι δυναμικά κλειδωμένες διευθύνσεις μπορούν να μετατραπούν σε στατικά κλειδωμένες.

Για να εξασφαλιστεί η ασφάλεια, η αντίδραση στην μεταβολή των καθορισμένων MAC διευθύνσεων σε μια θύρα μπορεί να ελεγχθεί με αρκετούς τρόπους. Η θύρα μπορεί να τροποποιηθεί ώστε να κλείσει η να εμποδίσει MAC διευθύνσεις οι οποίες υπερβαίνουν ένα συγκεκριμένο όριο. Συνήθως η καλύτερη πρακτική είναι να κλείσουμε την θύρα. Η ασφάλεια στις θύρες αποτρέπει επιθέσεις όπως το MAC Flooding και τις επιθέσεις cloning. (10)

5.6 DHCP Snooping

Η υποκλοπή (spoofing) του DHCP είναι μια επίθεση όπου ο επιτιθέμενος παρακολουθεί τα αιτήματα DHCP από τον χρήστη στο δίκτυο και τους απαντάει με πλαστές απαντήσεις πριν φτάσει η εγκεκριμένη απάντηση στον χρήστη. Το DHCP Snooping είναι μια ρύθμιση στους μεταγωγείς και μπορεί να αποτρέψει τέτοιες επιθέσεις. Ο μεταγωγέας μπορεί να τροποποιηθεί ώστε να καθορίσει ποιες θύρες του μεταγωγέα μπορούν να ανταποκρίνονται στα αιτήματα DHCP. Οι θύρες του μεταγωγέα μπορούν να προσδιοριστούν ως αξιόπιστες ή μη αξιόπιστες. Μόνο οι θύρες που συνδέονται σε έναν εξουσιοδοτημένο DHCP διακομιστή ρυθμίζονται ως αξιόπιστες, και επιτρέπουν την αποστολή όλων ων μηνυμάτων DHCP. Όλες οι άλλες θύρες του μεταγωγέα είναι μη αξιόπιστες και μπορούν να στέλνουν μόνο DHCP αιτήματα. Αν όμως υπάρξει μια DHCP απάντηση σε μια μη αξιόπιστη θύρα, τότε η θύρα σταματάει την λειτουργία της.

5.7 Ασφάλεια στο πρωτόκολλο Spanning Tree (STP)

Το πρωτόκολλο Spanning Tree είναι ένα πρωτόκολλο διαχείρισης που βρίσκεται στο επίπεδο ζεύξης δεδομένων (data link). Ο κύριος στόχος του είναι να εξασφαλιστεί ότι δεν υπάρχουν βρόγχοι στις ροές δεδομένων όταν το δίκτυο έχει πλεονάζοντα μονοπάτια. Γενικά τα πλεονάζοντα μονοπάτια δημιουργούνται ώστε να παρέχουν

αξιοπιστία στο δίκτυο, ωστόσο μπορούν να σχηματίσουν επικίνδυνους βρόγχους που μπορούν να οδηγήσουν σε μια επίθεση DoS στο δίκτυο.

5.7.1 Επίθεση στο πρωτόκολλο Spanning Tree

Η επίθεση αυτή χρησιμοποιεί το πρωτόκολλο Spanning Tree και ο επιτιθέμενος συνδέεται απευθείας σε μια θύρα στον μεταγωγέα ή μέσω ενός άλλου μεταγωγέα. Οι παράμετροι του STP μπορούν να παραποιηθούν προκειμένου να επιτευχθεί η κατάσταση root bridge η οποία βοηθάει τον εισβολέα να δει διάφορα πλαίσια τα οποία δεν θα μπορούσε να τα δει αλλιώς. Ο μεταγωγέας στέλνει ένα BPDU (bridge protocol data unit) κάθε 2 δευτερόλεπτα με την ίδια προτεραιότητα με αυτήν της τωρινής root bridge, αλλά με μια λίγο χαμηλότερη σε αριθμό MAC διεύθυνση, η οποία εξασφαλίζει την επιλογή της συγκεκριμένης root bridge. Ο μεταγωγέας που χειρίζεται ο εισβολέας μπορεί να ξεκινήσει DoS επίθεση, με το να μην αναγνωρίζει κατάλληλα τους άλλους μεταγωγείς προκαλώντας BPDU flooding. Επίσης μια άλλη επίθεση είναι ότι ο μεταγωγέας δεν επιχειρεί να αναλάβει ως root, και αντί για αυτό παράγει μεγάλους αριθμούς σε BPDU ανά δευτερόλεπτο που οδηγεί σε πολύ υψηλή χρήση του επεξεργαστή των μεταγωγέων.

5.7.2 Αποτροπή επιθέσεων στο πρωτόκολλο Spanning Tree

Υπάρχουν δύο επιλογές που βοηθούν στην αποτροπή της ανάληψης του root bridge:

Root Guard: Το Root guard περιορίζει τις θύρες του μεταγωγέα από τα οποίες μπορεί να υπάρξει ανάληψη της Root Bridge. Αν μια θύρα λάβει BPDU τα οποία είναι ανώτερα από αυτά που στέλνει η τωρινή root bridge, τότε η θύρα μπαίνει σε μια κατάσταση αδράνειας και δεν προωθούνται καθόλου δεδομένα προς αυτήν.

BPDU-Guard: Το BPDU-Guard χρησιμοποιείται για να προστατέψει το δίκτυο από προβλήματα που μπορεί να προκληθούν από την παραλαβή των BPDU στις θύρες πρόσβασης. Αυτές είναι οι θύρες οι οποίες δεν πρέπει να τα λαμβάνουν. Το BPDU-Guard αποτρέπει την πρόσβαση στις θύρες πρόσβασης από ένα επιτιθέμενο που χρησιμοποιεί ένα switch για αυτόν τον σκοπό.

5.8 Ασφάλεια σε εικονικά τοπικά δίκτυα (VLAN)

Στα τοπικά δίκτυα, τα εικονικά τοπικά δίκτυα χρησιμοποιούνται ως ένα μέτρο ασφαλείας για τον περιορισμό τον χρηστών που είναι ευπαθείς σε επιθέσεις μέσω του επιπέδου ζεύξης δεδομένων. Τα VLAN δημιουργούν όρια στο δίκτυο, μέσω των οποίων η μετάδοση δεδομένων (DHCP,ARP) είναι αδύνατη. Ένα δίκτυο το οποίο χρησιμοποιεί μεταγωγείς οι οποίοι υποστηρίζουν τις δυνατότητας ενός VLAN, μπορεί να τροποποιηθεί ώστε να καθορίσει πολλαπλά VLAN πάνω σε ένα ενιαίο τοπικό δίκτυο. Οι θύρες του μεταγωγέα ομαδοποιούνται σε VLANs μέσω του λογισμικού διαχείρισης του μεταγωγέα, οπότε ένας απλός μεταγωγέας μπορεί να λειτουργήσει πολλαπλά VLANs. Η χρήση των VLAN παρέχει απομόνωση στην κυκλοφορία των δεδομένων. Χωρίζει την μετάδοση στο επίπεδο ζεύξης δεδομένων (data link) σε μικρότερα λογικά επίπεδα και έτσι μειώνει το εύρος των επιθέσεων

(ARP και DHCP Spoofing). Τα πλαίσια (frames) δεδομένων ενός VLAN μπορούν να κινηθούν μόνο από και προς τις θύρες η οποίες ανήκουν μόνο στο ίδιο VLAN. Η προώθηση των πλαισίων μεταξύ δύο VLAN γίνεται μέσω της δρομολόγησης. (11)

5.8.1 Επιθέσεις στο VLAN

Σε μια επίθεση VLAN hopping, ο επιτιθέμενος σε ένα VLAN μπορεί να αποκτήσει πρόσβαση στην μετάδοση των δεδομένων άλλων VLAN που κανονικά δεν θα ήταν προσβάσιμα. Θα παράκαμπτε τον δρομολογητή κατά την επικοινωνία μεταξύ δύο VLAN, αχρηστεύοντας έτσι τον σκοπό της δημιουργίας των VLAN. Η επίθεση αυτή μπορεί να πραγματοποιηθεί με δύο τρόπους, με το switch spoofing και το double tagging.

5.8.1.1 Switch spoofing

Μπορεί να συμβεί όταν η θύρα του μεταγωγέα στην οποία είναι συνδεδεμένος ο επιτιθέμενος είναι σε κατάσταση trunking ή auto-negotiation. Ο επιτιθέμενος λειτουργεί ως μεταγωγέας και προσθέτει 802.1Q κεφαλίδες με ετικέτες VLAN και στέλνει τα πλαίσια σε απομακρυσμένα VLAN. Ο μεταγωγέας που λαμβάνει τα πλαίσια ερμηνεύει αυτά τα πλαίσια ότι προέρχονται από ένα άλλον 802.1 μεταγωγέα, και τα προωθεί σε συγκεκριμένο VLAN. Τα δύο προληπτικά μέτρα κατά των επιθέσεων spoofing είναι η ρύθμιση των θυρών σε στατικές και η απενεργοποίηση του auto-negotiation σε όλες τις θύρες.

5.8.1.2 Double tagging

Σε αυτήν την επίθεση ο εισβολέας που είναι συνδεδεμένος στην native VLAN θύρα του μεταγωγέα τοποθετεί δύο VLAN ετικέτες στην κεφαλίδα του πλαισίου. Η πρώτη ετικέτα είναι του native VLAN και η δεύτερη είναι για το προοριζόμενο VLAN. Όταν το πρώτο frame λαμβάνει τα πλαίσια του εισβολέα, αφαιρεί την πρώτη ετικέτα δεδομένου ότι τα πλαίσια του native VLAN προωθούνται χωρίς ετικέτα στην trunk θύρα. Δεδομένου ότι η δεύτερη ετικέτα δεν αφαιρέθηκε ποτέ από τον πρώτο μεταγωγέα, ο μεταγωγέας που λαμβάνει το πλαίσιο αναγνωρίζει την ετικέτα ως τον προορισμό του VLAN και προωθεί τα πλαίσια στον στόχο του VLAN. Το double tagging εκμεταλλεύεται τις ιδιότητες του native VLAN.

Το πρώτο μέτρο πρόληψης είναι η αφαίρεση όλων των θυρών πρόσβασης από το προεπιλεγμένο VLAN1 από την στιγμή που η θύρα του εισβολέα πρέπει να ταιριάζει με αυτή του native VLAN. Επίσης όλα οι μεταγωγείς θα πρέπει να παραμετροποιηθούν ώστε να μεταφέρουν συγκεκριμένες ετικέτες από τα native VLAN πλαίσια στις trunk θύρες.

6. Έλεγχος της πρόσβασης στο δίκτυο

Ο έλεγχος της πρόσβασης στο δίκτυο είναι μια μέθοδος για την ενίσχυση της ασφάλειας ενός ιδιωτικού δικτύου, περιορίζοντας την διαθεσιμότητα των πόρων του δικτύου σε συσκευές που ακολουθούν την πολιτική ασφαλείας του οργανισμού. Ένα τυπικό σύστημα ελέγχου της πρόσβασης στο δίκτυο αποτελείται από δύο βασικά μέρη, την περιορισμένη πρόσβαση και την προστασία των συνόρων του δικτύου. Η περιορισμένη πρόσβαση στις συσκευές του δικτύου επιτυγχάνεται με την ταυτοποίηση του χρήστη επιτυγχάνεται με την ταυτοποίηση του χρήστη καθώς και με τον έλεγχο της άδειας ο οποίος είναι υπεύθυνος για την αναγνώριση και την ταυτοποίηση διαφορετικών χρηστών στο δίκτυο. Η εξουσιοδότηση είναι η διαδικασία για την χορήγηση ή την άρνηση συγκεκριμένων δικαιωμάτων πρόσβασης σε ένα προστατευμένο πόρο. Η προστασία των συνόρων του δικτύου ελέγχει την λογική συνδεσιμότητα μέσα και έξω από τα δίκτυα. Πολλαπλά τείχη ασφαλείας μπορούν να αναπτυχθούν για να αποτραπεί μια μη εξουσιοδοτημένη πρόσβαση στα συστήματα του δικτύου. Επίσης η ανίχνευση εισβολής καθώς και οι τεχνολογίες αποτροπής μπορούν να αναπτυχθούν ώστε να παρέχουν ασφάλεια ενάντια σε επιθέσεις που γίνονται από το διαδίκτυο.

Ο περιορισμός της πρόσβασης στις συσκευές του δικτύου είναι ένα πολύ σημαντικό βήμα για την προστασία ενός δικτύου. Ένας σημαντικός τομέας για την προστασία μιας συσκευής του δικτύου είναι ο έλεγχος της πρόσβασης και η εξουσιοδότηση. Πολλά πρωτόκολλα έχουν αναπτυχθεί για την αντιμετώπιση αυτών των απαιτήσεων και για την ενίσχυση της ασφάλειας σε υψηλότερα επίπεδα.

6.1 Ταυτοποίηση και εξουσιοδότηση του χρήστη

Η ταυτοποίηση του χρήστη είναι απαραίτητη για τον έλεγχο της πρόσβασης στα συστήματα του δικτύου. Η ταυτοποίηση έχει δύο μέρη, τον γενικό έλεγχο της πρόσβασης και την αδειοδότηση. Ο γενικός έλεγχος της πρόσβασης είναι η μέθοδος για τον έλεγχο αν ο συγκεκριμένος χρήστης έχει συγκεκριμένα δικαιώματα στο σύστημα που προσπαθεί να συνδεθεί. Συνήθως αυτή η μέθοδος είναι συνδεδεμένη με τον χρήστη να έχει κάποιον “λογαριασμό” στο σύστημα. Η εξουσιοδότηση ασχολείται με τα δικαιώματα που έχει ένας χρήστης αφού έχει ταυτοποιηθεί π.χ. ο χρήστης μπορεί μόνο να δει τα δεδομένα.

Η αυθεντικοποίηση του χρήστη εξαρτάται από παράγοντες που ο ίδιος ο χρήστης γνωρίζει (π.χ. ο κωδικός πρόσβασης). Κατ’ ελάχιστο, όλες οι συσκευές του δικτύου θα πρέπει να έχουν ταυτοποίηση του χρήστη με username και password. Ο κωδικός θα πρέπει να είναι περίπλοκος (με αρκετούς χαρακτήρες, αριθμούς και σύμβολα), και θα πρέπει να αλλάζει ανά τακτά χρονικά διαστήματα. Στην περίπτωση απομακρυσμένης σύνδεσης από ένα χρήστη, θα πρέπει να χρησιμοποιηθεί μια μέθοδος κρυπτογράφησης για την προστασία των κωδικών.

6.2 Λίστες ελέγχου πρόσβασης (access control lists)

Πολλές δικτυακές συσκευές μπορούν να διαμορφωθούν με λίστες πρόσβασης. Οι λίστες αυτές καθορίζουν τα hostnames ή τις IP διευθύνσεις που έχουν λάβει άδεια για να έχουν πρόσβαση στην συσκευή. Για παράδειγμα, είναι τυπικός ο περιορισμός της πρόσβασης σε δικτυακό εξοπλισμό από IPs, εκτός από τον διαχειριστή του δικτύου. Αυτός ο περιορισμός θα προστατεύει όλες τις προσπάθειες εισόδου που μπορεί να μην είναι εξουσιοδοτημένες. Αυτοί οι τύποι των λιστών πρόσβασης χρησιμεύουν ως μια πολύ σημαντική προστασία και μπορεί να είναι πολύ αποτελεσματικοί σε ορισμένες συσκευές που έχουν διαφορετικούς κανόνες και διαφορετικά πρωτόκολλα πρόσβασης.

6.3 Προστασία των Επικοινωνιών στα Δίκτυα

6.3.1 Ασφάλεια των τερματικών συστημάτων

Οι υποδομές για τις επικοινωνίες αποτελούνται κυρίως από συνδέσεις του δικτύου καθώς και την σύνδεση συσκευών, όπως οι μεταγωγείς (switches), οι δρομολογητές ή οι πύλες. Επιπλέον υπάρχουν συστήματα που παρέχουν υπηρεσίες υποστήριξης όπως το Domain Name System. Ωστόσο η ασφάλεια των επικοινωνιών εξαρτάται όχι μόνο στα πρωτόκολλα του δικτύου και τα συστήματα, αλλά και στα συνδεδεμένα τερματικά συστήματα δηλαδή τους εξυπηρετητές και τις συσκευές που είναι συνδεδεμένες μέσω του δικτύου.

Η πρόκληση σε αυτήν την περίπτωση είναι ότι , λόγο της πολυπλοκότητας του υλικού και του λογισμικού, ακόμα και η ασφάλεια ενός μεμονωμένου συστήματος είναι δύσκολο να αναλυθεί και εξασφαλιστεί. Ένα βασικό πρόβλημα κυρίως κατά την διάρκεια της ανάπτυξης λογισμικού είναι το υψηλό κόστος και η πίεση για την γρήγορη ολοκλήρωση του έχουν ως αποτέλεσμα να μην δίνεται ιδιαίτερη βάση στην ασφάλεια της εφαρμογής. Αυτό επιβεβαιώνεται περαιτέρω από την ευρεία χρήση γλωσσών προγραμματισμού που έχουν όμως συγκεκριμένα προβλήματα ασφαλείας. Για παράδειγμα η έλλειψη ελέγχου της μνήμης σε προγράμματα C και C++ οδηγούν συχνά σε προβλήματα. Εξαιτίας αυτός των παραγόντων, οι τελικοί χρήστες καθώς και οι διαχειριστές των συστημάτων έρχονται αντιμέτωποι με ένα μεγάλο αριθμό από ευπάθειες καθώς και με updates πάνω σε αυτό. Ο αριθμός των κενών ασφαλείας που έχει καταγραφτεί τα τελευταία χρόνια είναι μεγάλος. Κάθε χρόνο αναφέρονται περίπου 5000 κενά ασφαλείας, με αποτέλεσμα ένα τεράστιο φόρτο εργασίας για τους διαχειριστές και για τους τελικούς χρήστες που θέλουν να προστατευτούν από όλες τις γνωστές απειλές. Εκτός από τις δημοσιευμένες απειλές, μπορεί να υπάρχουν και άλλα αδύνατα σημεία που να είναι γνωστά μόνο σε λίγους ανθρώπους και που ο κατασκευαστής να μην γνωρίζει καθόλου την ύπαρξη τους. Η προστασία ενάντια σε αυτά είναι σχεδόν αδύνατη για τον μέσο χρήστη ή διαχειριστή. Εξίσου σημαντικό εκτός από τον αριθμό των ευπαθειών, είναι και ο αριθμός των επηρεαζόμενων συστημάτων ώστε να γίνει αξιολόγηση της απειλής. Λόγω της επικράτησης της πλατφόρμας των Windows στους υπολογιστές, το λειτουργικό σύστημα του Unix

στον τομέα των εξυπηρετητών και της Cisco στους δρομολογητές, μπορούν να βρεθούν μεμονωμένα αδύνατα σημεία που μπορούν να αξιοποιηθούν ιδιαίτερα καλά όταν επηρεάζουν ένα από αυτά τα συστήματα. Παρακάτω θα δούμε τις πιο κοινές ευπάθειες που μπορούν να οδηγήσουν έναν εισβολέα να αναλάβει τον έλεγχο των συστημάτων. Συνήθως αυτές οι ευπάθειες αφορούν τα τελικά συστήματα, αλλά η έκθεση τους αποτελεί ένα σημαντικό κίνδυνο για τις επικοινωνίες των συστημάτων. Επιπροσθέτως οι δρομολογητές και οι μεταγωγείς μπορούν να επηρεαστούν και αυτοί από τα ζητήματα ασφαλείας.

6.3.2 Επίθεση Buffer Overflow

Επειδή οι υπηρεσίες του δικτύου καθώς και όλα τα μέρη του είναι συνήθως προγραμματισμένα σε C ή C++ , οι ¨υπερχειλίσεις¨ της μνήμης που υπάρχουν από αυτές τις γλώσσες προγραμματισμού είναι από τους πιο συνηθισμένους και από τους πιο γνωστούς τύπους επιθέσεων σε συστήματα που εκτείνονται μέσα στο δίκτυο. Ο κύριος λόγος είναι ότι και στις 2 γλώσσες προγραμματισμού η μέθοδος array access δεν ελέγχεται αυτόματα για το μήκος της. Αν ο επιτιθέμενος καταφέρει και περάσει σε ένα πρόγραμμα μια συμβολοσειρά (string) η οποία να είναι μεγαλύτερη από αυτήν που έχει η μνήμη, και η υπόθεση αυτή δεν εξεταστεί από τον προγραμματιστή, τότε τα μέρη της μνήμης στα οποία είναι αποθηκευμένα άλλα δεδομένα θα αντικατασταθούν. Και αυτό εξαρτάται από την περιοχή της μνήμης που επηρεάζεται και διακρίνεται μεταξύ του overflow(υπερχείλιση) της στοίβας και της ουράς.

Η αντικατάσταση της μνήμης μπορεί να έχει διαφορετικά αποτελέσματα ανάλογα με την δομή του προγράμματος και τα περιεχόμενα της μνήμης:

- Στο καλύτερο σενάριο, η μνήμη που αντικαταστάθηκε δεν χρησιμοποιείται πια και η εκτέλεση του προγράμματος δεν διαταράσσεται.

- Οι ανεξέλεγκτες αλλαγές συνήθως καταλήγουν στην διακοπή της λειτουργίας του προγράμματος.

- Αν ο εισβολέας μπορεί να ελέγξει τις αλλαγές στην μνήμη, υπάρχει πιθανότητα να μπορεί να αλλάξει τις παραμέτρους, με αποτέλεσμα να μεταβάλλεται η εκτέλεση του προγράμματος πχ ο επιτιθέμενος θα μπορούσε να αλλάξει τις παραμέτρους που ελέγχουν τα δικαιώματα μέσα στο σύστημα.

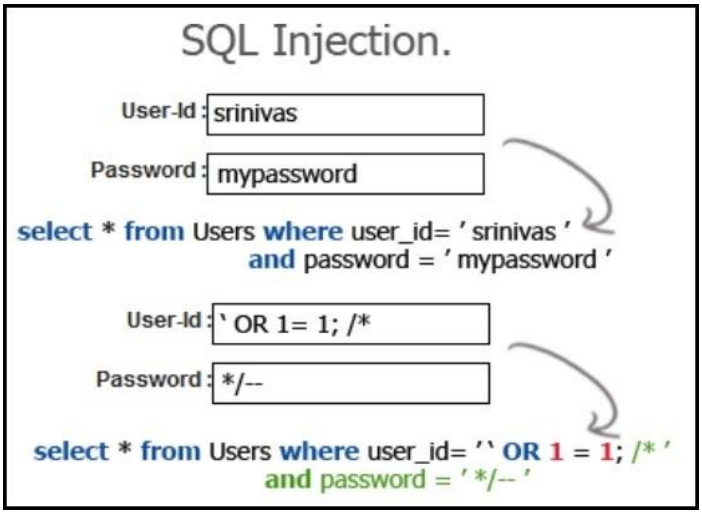
- Ειδικά με τα overflows της στοίβας, είναι συχνά εφικτό για τον επιτιθέμενο να αλλάξει τα περιεχόμενα των δεικτών(pointers) στον κώδικα. Αν αυτοί οι δείκτες χρησιμοποιηθούν για ¨άλματα¨ στην επόμενη εκτέλεση του προγράμματος, τότε κάτω από συγκεκριμένες συνθήκες οι εισβολείς μπορούν να εκτελέσουν τον δικό τους κώδικα με αποτέλεσμα να πάρουν τον έλεγχο του προγράμματος. Με τα overflow της στοίβας, η διεύθυνση που επιστρέφεται από την λειτουργία της εκτέλεσης συνήθως αντικαταστείτε, έτσι ώστε όταν τελειώσει η λειτουργία το πρόγραμμα να συνεχίσει με τον κώδικα του επιτιθέμενου.

Στις περισσότερες επιθέσεις που χρησιμοποιούν την υπερχείλιση της μνήμης, ο στόχος είναι ο επιτιθέμενος να αναπτύξει τον δικό του κώδικα(exploit) και να τον εκτελέσει. (12)

6.3.3 SQL Injections και Cross-site Scripting

Σε πολλά περιστατικά που έχουν να κάνουν με την ασφάλεια, οι εισβολείς δεν έχουν σχεδόν καμία πρόσβαση στα συστήματα που κάνουν επίθεση. Παίρνοντας τα παραδείγματα των αιτημάτων(web requests), οι εισβολείς ενσωματώνουν εντολές σε SQL ή σε JavaScript στο HTTP αίτημα που στέλνεται στον εξυπηρετητή. Αν ο εξυπηρετητής χρησιμοποιήσει τις μεταβλητές που έλαβε χωρίς να τις εξετάσει περαιτέρω μπορεί να δημιουργήσει ερωτήματα(queries) ή προσαρμοσμένες ιστοσελίδες, που στην συνέχεια ο κώδικας αυτός ενδεχομένως να μπορεί να εκτελεστεί. Στην τεχνική που είναι γνωστή ως SQL injection, ο επιδέξιος σχεδιασμός των ερωτημάτων SQL μπορεί να επιτρέψει την αντιγραφή, τροποποίηση η ακόμα και την διαγραφή των βάσεων δεδομένων. Αν ο επιτιθέμενος ενσωματώσει JavaScript σε άλλες ιστοσελίδες, τότε μιλάμε για cross site scripting (XSS). Μια επίθεση για να είναι επιτυχής, τότε τα θύματα θα πρέπει να ανοίξουν έναν ειδικά διαμορφωμένο υπερσύνδεσμο για να οδηγηθούν σε μια ιστοσελίδα η οποία ελέγχεται εξολοκλήρου από τον επιτιθέμενο, χωρίς όμως αυτό να είναι εμφανές στον υπερσύνδεσμο. Παρόμοια είδη επιθέσεων υπάρχουν και σε άλλες γλώσσες. Για παράδειγμα υπάρχουν τα LDAP injections (Lightweight Directory Access Protocol) στα οποία οι χαρακτήρες των συνθηματικών καθώς και το όνομα του χρήστη (username) αντικαθίστανται με χαρακτήρες του LDAP. Ο στόχος σε αυτήν την περίπτωση είναι η τροποποίηση των αιτήσεων για εξουσιοδότηση με τέτοιο τρόπο ώστε ο επιτιθέμενος που δεν έχει άδεια, να λαμβάνει πρόσβαση στο σύστημα.

Στη παρακάτω εικόνα παρουσιάζεται ένα SQL Query που έχει ως στόχο τη μη εξουσιοδοτημένη πρόσβαση στον λογαριασμό



Εικόνα 7 - SQL Injection

6.3.4 Κακόβουλο Λογισμικό

Ένας τρόπος για την διείσδυση σε υπολογιστικά συστήματα που συνεχώς αυξάνεται είναι η στοχευμένη τοποθέτηση κακόβουλων προγραμμάτων. Ο τρόπος που μπορούν αυτά τα προγράμματα να διανεμηθούν ποικίλει:

- Αποστολή ψεύτικων e-mail που περιέχουν κακόβουλο λογισμικό
- Μολυσμένα Usb αφήνονται με την ελπίδα ότι οι χρήστες θα τα συνδέσουν στις θέσεις εργασίας τους
- Ιστοσελίδες έχουν τροποποιηθεί έτσι ώστε να έχουν κακόβουλα προγράμματα.

Ανάλογα με τον τρόπο της διανομής καθώς και της προσπάθειας για την απόκρυψη του κακόβουλου κώδικα, μπορούν να διακριθούν τα ακόλουθα βασικά είδη κακόβουλου λογισμικού:

- Backdoor: Στην πιο απλή περίπτωση το κακόβουλο λογισμικό δεν έχει καμία λειτουργία για την διανομή, είναι "αχαρτογράφητο" και υπάρχει μέσα σε ένα πρόγραμμα το οποίο λειτουργεί όπως θα έπρεπε. Μόνο όταν έχει περάσει κάποιο χρονικό διάστημα ή ενεργοποιείται από ένα εξωτερικό συμβάν όπως πακέτα που στέλνονται στο δίκτυο από τον επιτιθέμενο για να ενεργοποιήσουν το λογισμικό.
- Δούρειος Ίππος (Trojan): Είναι ένα εξειδικευμένο λογισμικό που έχει ως κύριο στόχο την παραγωγή κακόβουλων λειτουργιών. Σε αντίθεση με το backdoor ο δούρειος ίππος εγκαθίσταται μόνος του σαν μια διεργασία που βρίσκεται στο παρασκήνιο του περιβάλλοντος ενός λειτουργικού συστήματος, ώστε να μην χρειάζεται να ενεργοποιηθεί ειδικά από τον χρήστη. Κάποιες κοινές κακόβουλες λειτουργίες του είναι η αποστολή αρχείων ή spam μηνυμάτων, η παρακολούθηση του χρήστη που μπορεί να χρησιμοποιεί το μικρόφωνο ή την κάμερα, ή ακόμα και η υποκλοπή στοιχείων από πιστωτικές κάρτες.
- Rootkits: Σε ορισμένες περιπτώσεις οι δούρειοι ίπποι μπορούν να ανιχνευτούν και να αφαιρεθούν πολύ εύκολα. Το λογισμικό το οποίο μπορεί να κρυφτεί με ένα καλύτερο τρόπο συνήθως αναφέρεται ως rootkit. Υπάρχει ένα ευρύ φάσμα των χρήσεων του rootkit. Στις πιο απλές περιπτώσεις εντολές όπως το ls ανταλλάσσονται με σκοπό να κρυφτούν τα αρχεία του rootkit. Πιο σύνθετα rootkits προσπαθούν να ¨καμουφλάρουν¨ τον εαυτό τους μεταβάλλοντας τις κλήσεις του λειτουργικού συστήματος. Αυτό έχει ως αποτέλεσμα το λογισμικό το οποίο χρησιμοποιεί αυτές της κλήσεις να μην μπορεί να ανιχνεύσει το rootkit.
- Ιοί: Αν ο κακόβουλος κώδικας έχει την δυνατότητα να φτιάχνει αντίγραφα του εαυτού του μέσω usb συσκευών ή άλλων μέσων, τότε αναφέρεται ως ιός.

- Worms: Κάποια προγράμματα έχουν την ικανότητα να μολύνουν και άλλους υπολογιστές μέσα στο δίκτυο. Όταν ένα σύνολο αυτών των υπολογιστών ελέγχονται απομακρυσμένα με σκοπό να επιτεθούν σε άλλους υπολογιστές στο δίκτυο τότε ονομάζονται bots.

Ο κακόβουλος κώδικας μπορεί να αντιμετωπιστεί μόνο από διάφορα μέτρα πρόληψης και ελέγχου. Οι κύριες προσεγγίσεις σε αυτό είναι:

- Με την χρήση σαρωτών για ιούς καθώς και εργαλείων για την παρακολούθηση του δικτύου. Με αυτόν τον τρόπο κακόβουλα λογισμικά τα οποία είναι γνωστά καθώς και ύποπτα κομμάτια με κώδικες μπορούν πιθανώς να ανιχνευτούν.

- Η προμήθεια λογισμικού που προέρχεται από αξιόπιστες πηγές καθώς και η εκτέλεση μόνο υπογεγραμμένου κώδικα βοηθάει να μειωθεί και άλλο η απειλή από backdoors και δούρειους ίππους. Συγκεκριμένα, θα πρέπει να γίνονται αναβαθμίσεις στο λογισμικό ώστε να θωρακίζεται το σύστημα από τις γνωστές ευπάθειες. Η υπογραφή του κώδικα είναι πολύ σημαντικό προαπαιτούμενο, έτσι ώστε οι εισβολείς να μην μπορούν εύκολα να αντικαταστήσουν το νόμιμο λογισμικό με ένα κακόβουλο.

- Τελικώς, το backdoor μπορεί να βρεθεί μόνο από τακτικούς ελέγχους του λογισμικού, καθώς και ανιχνεύοντας τις λειτουργίες του λειτουργικού συστήματος που χρησιμοποιούνται.

- Για την αποτροπή μιας τυχαίας εκτέλεσης ενός προγράμματος μέσα σε ένα e-mail ή σε κάποια ενδεχομένως κακόβουλη ιστοσελίδα, ένα σημαντικό μέτρο αντιμετώπισης είναι η κατάλληλη εκπαίδευση των χρηστών με σκοπό να αυξηθεί η επίγνωση της κατάστασης και να μειωθεί ο κίνδυνος μιας ασυνείδητης εκτέλεσης κάποιου κακόβουλου κώδικα.

Εκτός από τους κλασικούς στόχους της ασφάλειας δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας, τα τελευταία χρόνια η επίγνωση του επικεντρώνεται όλο και περισσότερο στην διαθεσιμότητα των μέσων επικοινωνίας. Ο λόγος για αυτό είναι η δυνατότητα των κακόβουλων χρηστών να διακόπτουν τις επικοινωνίες των συστημάτων αρκετά εύκολα χρησιμοποιώντας επιθέσεις άρνησης υπηρεσιών (Dos attack) χωρίς να μπορούν να εντοπιστούν αλλά πάραυτα να μπορούν να προκαλέσουν σημαντικές βλάβες. (13)

6.3.5 Επιθέσεις άρνησης υπηρεσιών

Ακόμα και αν αυτές οι επιθέσεις συχνά δεν επιτρέπουν στον εισβολέα να έχει άμεση πρόσβαση σε ευαίσθητα δεδομένα, εξακολουθούν και υπάρχουν κίνητρα για την δημιουργία DoS επιθέσεων.

- Πολλές φορές οι επιθέσεις άρνησης υπηρεσιών είναι αρκετά εύκολες στο να εκτελεσθούν, συχνά από άτομα που μπορεί να μην έχουν σοβαρό γνωστικό

υπόβαθρο του αντικειμένου και χωρίς να γνωρίζουν την πραγματική ζημιά που προκαλούν. Τα άτομα αυτά συνήθως χρησιμοποιούν λογισμικό το οποίο υπάρχει στο internet (π.χ. LOIC) το οποίο αναπαράγει τα κατάλληλα πακέτα για αποστολή.

- Εμπορικά πλεονεκτήματα: Οι επιθέσεις άρνησης υπηρεσιών μπορεί να οδηγήσουν σε χρηματικά οφέλη, όπως η αποτροπή των ανταγωνιστών από την απόκτηση πληροφοριών.

- Δυσφήμιση: Μη διαθέσιμο e-mail ή web servers μπορούν να πλήξουν την αξιοπιστία των διαχειριστών.

Τα πολλά διαφορετικά κίνητρα για τις επιθέσεις DoS είναι μόνο μια πτυχή του προβλήματος. Η μορφή της επίθεσης γίνεται όλο και πιο σημαντική με την αύξηση της χρήσης των δικτύων και τον βαθμό στον οποίο η κοινωνία μας βασίζεται σε αποτελεσματικά δίκτυα επικοινωνίας. Σε κάποιο βαθμό τα εργαλεία για να κάνει κάποιος μια τέτοια επίθεση είναι πολύ εύκολο να τα αποκτήσει και είναι σε πολύ μεγάλο βαθμό αυτοματοποιημένα. Επιπροσθέτως, η προστασία ενάντια σε επιθέσεις άρνησης υπηρεσιών είναι συχνά πολύ δύσκολο να εφαρμοστεί και επομένως είναι και ακριβή.

Η καλύτερη περίπτωση για τον επιτιθέμενο είναι να μπορεί να καθιστά τους εξυπηρετητές, τους δρομολογητές και όποια άλλη σημαντική δικτυακή συσκευή μονίμως εκτός λειτουργίας για οποιονδήποτε άλλο χρήστη. Αυτό είναι εφικτό με την χρήση δυο ειδών επιθέσεων. Την ¨καταστροφή¨ των συσκευών ή την κράτηση όλων των πόρων του συστήματος από τον επιτιθέμενο.

Σε σχέση με την καταστροφή μόνο υπάρχει πλήθος δυνατοτήτων. Εκτός από την φυσική καταστροφή, η καταστροφή μέσω των εντολών λογισμικού είναι πιθανή σε πολλές περιπτώσεις. Στην πιο απλή περίπτωση ο σκληρός δίσκος θα διαγράψει τα δεδομένα του έπειτα από μια επιτυχημένη εισβολή στο σύστημα του υπολογιστή. Ωστόσο διάφορα σφάλματα στο λειτουργικό σύστημα ή στις εφαρμογές του εξυπηρετητή μπορούν επίσης συχνά να χρησιμοποιηθούν ώστε να βγάλουν εκτός λειτουργίας το σύστημα. Οι πιο γνωστές επιθέσεις αυτού του είδους που έχουν συμβεί στο παρελθόν περιλαμβάνουν:

- Το ping του θανάτου (ping of death): Το μέγιστο μέγεθος των IP πακέτων είναι 65.535 bytes. Ωστόσο κάτω από συγκεκριμένες συνθήκες όταν τα κομμάτια των IP πακέτων ενωθούν μπορούν να παράγουν πολύ μεγαλύτερα πακέτα τα οποία στα τέλη του 1990 διαχειρίστηκαν εσφαλμένα από πολλές εφαρμογές. Αντικαθιστώντας τις περιοχές της μνήμης, τα λειτουργικά συστήματα βγήκαν εκτός λειτουργίας και οι επιτιθέμενοι μπορούσαν συνέχεια να διαταράσσουν τις λειτουργίες με την χρήση κάποιων ειδικά διαμορφωμένων IP πακέτων.

- Teardrop Attack: Η επίθεση αυτή επίσης στοχεύει σε ευπάθειες που ήταν κοινές στην λειτουργία του IP στα λειτουργικά συστήματα. Σε αυτήν την επίθεση ο επιτιθέμενος δημιουργούσε 2 κομμάτια IP πακέτων τα οποία δεν περιείχαν συνεχόμενα πακέτα. Αντ' αυτού το ένα κομμάτι εμπεριεχόταν τελείως μέσα στο άλλο κομμάτι και ένας αρνητικός αριθμός λαμβάνονταν κατά τον υπολογισμό μιας μετατόπισης κατά την διάρκεια της συναρμολόγησης του πακέτου. Ωστόσο, καθώς το σύστημα προσπαθήσει να συναρμολογήσει αυτά τα τμήματα, γίνεται overflow στην μνήμη και το αποτέλεσμα μεταφράζεται ως ένας πολύ μεγάλος αριθμός, ο οποίος οδηγεί στην παύση λειτουργίας του συστήματος.

- Επίθεση land: Το πρόβλημα πού αξιοποιείται με την λεγόμενη επίθεση land σε παλιά συστήματα είναι παρόμοια με την επίθεση teardrop. Σε αυτήν την περίπτωση ο επιτιθέμενος ξεκινάει την δημιουργία μια σύνδεσης TCP με τον χρήστη. Ωστόσο το αντίστοιχο πακέτο SYN εφοδιάζεται με μια πλαστή διεύθυνση, που σε αυτήν την περίπτωση είναι ή διεύθυνση του ίδιου του χρήστη. Λόγω των σφαλμάτων εφαρμογής της στοίβας IP των επηρεαζόμενων συστημάτων, το σύστημα απαντάει συνεχώς στον εαυτό του με αποτέλεσμα την δημιουργία ενός ατελείωτου βρόχου. Αυτό οδηγεί στην αποτυχία του συστήματος. (14)

6.3.6 Επιθέσεις εξάντλησης της μνήμης

Στις επιθέσεις εξάντλησης της μνήμης, μια διεργασία του θύματος αναγκάζεται να χρησιμοποιεί πολύ μνήμη ή χώρο στον δίσκο. Ανάλογα με την εφαρμογή, η επεξεργασία των αιτήσεων επιβραδύνει τόσο πολύ που η υπηρεσία δεν είναι πλέον διαθέσιμη στους άλλους χρήστες. Σε επιθέσεις που στοχεύουν στην εξάντληση της μνήμης, οι επιδράσεις αυτές μερικές φορές είναι πιο δραστικές όσο αυξάνεται το φορτίο. Τα συστήματα αντιδρούν ακόμα πιο αργά όταν τα δεδομένα επεξεργάζονται από τον σκληρό δίσκο λόγω έλλειψης μνήμης.

Μερικές από τις επιθέσεις εξάντλησης της μνήμης στο επίπεδο δικτύου και μεταφοράς:

- SYN Flood: Η μνήμη που προορίζεται για τις συνδέσεις δικτύου μπορεί εύκολα να εξαντληθεί σε πολλά συστήματα με την αποστολή SYN πακέτων στο θύμα. Οι συνδέσεις TCP δημιουργούνται μέσω της διαδικασίας που είναι γνωστή ως three-way handshake. Κατά την διάρκεια αυτής της διαδικασία, ο επιτιθέμενος στέλνει TCP-SYN πακέτα που υποδεικνύουν ότι ζητάει να συνδεθεί. Αυτό παίρνει την απάντηση με ένα SYN-ACK (acknowledge) που αναγνωρίζει το αίτημα για συγχρονισμό και διαθέτει ένα μέρος του χώρου στο πλαίσιο της προετοιμασίας για την σύνδεση που επρόκειτο να γίνει. Μετά από αυτό ο στόχος περιμένει την τελευταία βεβαίωση (ACK) για να οριστικοποιήσει την σύνδεση. Με αυτόν τον τρόπο μπορεί να γίνει κατάχρηση

αυτής της διαδικασίας ώστε να γίνονται συνέχεια αιτήματα για νέες συνδέσεις χωρίς ποτέ όμως να ολοκληρώνεται η σύνδεση.

- Επίθεση IP fragment: Μια παρόμοια αρχή ακολουθείται με την αποστολή ενός μεγάλου αριθμού από τυχαία IP fragments (τεμάχια). Σε αυτήν την περίπτωση, το σύστημα του θύματος πρέπει να διατηρεί πόρους για να ανασχηματίσει τα διαγράμματα από τα fragments. Ωστόσο αν ο επιτιθέμενος δεν στείλει κανένα πλήρες διάγραμμα (datagram), τότε το σύστημα θα πρέπει να περιμένει για ένα συγκεκριμένο χρονικό διάστημα. (15)

7. Τείχος Προστασίας (Firewall)

Σχεδόν όλοι οι οργανισμοί που έχουν παρουσία στο διαδίκτυο έχουν ένα δίκτυο συνδεδεμένο σε αυτό. Ο διαχωρισμός μεταξύ του διαδικτύου και του εσωτερικού δικτύου είναι απαραίτητος για την ασφάλεια του δικτύου. Μερικές φορές το εσωτερικό δίκτυο αναφέρεται ως η αξιόπιστη πλευρά, και το διαδίκτυο η αναξιόπιστη.

7.1 Τύποι των τειχών προστασίας

Το τείχος προστασίας είναι μια δικτυακή υπηρεσία η οποία απομονώνει το εσωτερικό δίκτυο από ένα εξωτερικό δίκτυο ή το διαδίκτυο. Μπορεί να είναι υλικό ή λογισμικό, ή ένα συνδυασμένο σύστημα το οποίο να αποτρέπει μη εξουσιοδοτημένη πρόσβαση προς ή από το εσωτερικό δίκτυο.

Όλα τα πακέτα δεδομένων που εισέρχονται η εξέρχονται από το εσωτερικό δίκτυο διέρχονται μέσα από το τείχος προστασίας, το οποίο εξετάζει κάθε πακέτο και μπλοκ για την περίπτωση που δεν πληρούν τα καθορισμένα κριτήρια ασφαλείας. Η ανάπτυξη του τείχους προστασίας στα όρια του δικτύου είναι σαν να συγκεντρώνεις την ασφάλεια σε ένα μοναδικό σημείο. Θεωρείται βασικό στοιχείο για την επίτευξη της ασφάλειας του δικτύου για τους εξής λόγους:

- Το εσωτερικό δίκτυο και οι χρήστες είναι πολύ πιθανόν να μην έχουν την κατάλληλη ασφάλεια.
- Για την αποτροπή ενός εισβολέα στο να ξεκινήσει μια επίθεση άρνησης υπηρεσιών στους πόρους του δικτύου
- Το διαδίκτυο είναι ένα επικίνδυνο μέρος με εγκληματίες, χρήστες από ανταγωνίστριες εταιρείες, δυσαρεστημένους πρώην υπαλλήλους και κατασκόπους από άλλες χώρες.
- Για την αποτροπή της παράνομης πρόσβασης και τροποποίησης δεδομένων από έναν εισβολέα.

Το τείχος προστασίας κατηγοριοποιείται σε τρείς βασικούς τύπους:

- Φίλτρα πακέτων
- Φίλτρα κατάστασης
- Επίπεδο εφαρμογών

Αυτές οι τρείς κατηγορίες δεν είναι αμοιβαία αποκλειστικές. Τα σύγχρονα τείχη προστασίας έχουν μια ποικιλία από ικανότητες που μπορούν να τα κατατάσσουν σε περισσότερες από μια κατηγορίες. (16,17)

7.1.1 Stateless και Stateful τείχος προστασίας

Σε αυτόν τον τύπο του τείχους προστασίας, το εσωτερικό δίκτυο είναι συνδεδεμένο στο εξωτερικό δίκτυο/διαδίκτυο μέσω ενός δρομολογητή ο οποίος λειτουργεί ως τείχος προστασίας. Το τείχος προστασίας επιθεωρεί και φιλτράρει τα πακέτα δεδομένων ένα προς ένα. Το τείχος προστασίας λειτουργεί με το φιλτράρισμα των πακέτων μπορεί να επιτρέψει η να αποκλείσει πακέτα ως επί το πλείστον με βάση κριτήρια όπως η πηγή ή ο προορισμός μιας διεύθυνσης IP, ενός πρωτοκόλλου, τον αριθμό μιας θύρας (port) καθώς και διάφορες άλλες παραμέτρους μέσα στην κεφαλίδα IP. Η απόφαση μπορεί να βασίζεται και σε άλλους παράγοντες εκτός από τα πεδία της κεφαλίδας IP, όπως τα μηνύματα ICMP, τα TCP SYN και ACK bits. Ο κανόνας για το φιλτράρισμα των πακέτων έχει δύο μέρη:

- Τα κριτήρια επιλογής που χρησιμοποιούνται για να παρθεί μια απόφαση
- Το πεδίο δράσης, που καθορίζει τι ενέργειες θα πρέπει να γίνουν αν ένα πακέτο IP πληροί τα κριτήρια. Η απόφαση για το πακέτο θα ήταν είτε η φραγή του είτε αποδοχή του μέσω του τοίχους προστασίας.

Το φιλτράρισμα των πακέτων επιτυγχάνεται με την ρύθμιση των παραμέτρων της λίστας ελέγχου πρόσβασης (ACL) σε δρομολογητές και μεταγωγείς. Η λίστα ελέγχου πρόσβασης είναι ένας πίνακας με κανόνες για το φιλτράρισμα των πακέτων. Καθώς τα δεδομένα εισέρχονται και εξέρχονται από μια διεπαφή (interface), το τείχος προστασίας εφαρμόζει τις λίστες ελέγχου από την κορυφή μέχρι το τέλος σε κάθε ένα εισερχόμενο πακέτο, βρίσκει αν πληροί τις προϋποθέσεις και είτε επιτρέπει είτε αρνείται την είσοδο στα πακέτα.

Το stateless τείχος προστασίας εξετάζει το πακέτο και επιτρέπει την μετάδοση του αν πληροί τα κριτήρια ακόμα και αν δεν είναι μέρος μιας εγκατεστημένης συνεχής επικοινωνίας. Για αυτό, αυτά τα τείχη προστασίας αντικαταστάθηκαν από stateful τείχη προστασίας σε όλα τα σύγχρονα δίκτυα. Αυτός ο τύπος προσφέρει μια πιο εμπεριστατωμένη μέθοδο ελέγχου πάνω στις λίστες ελέγχου πρόσβασης σε σύγκριση με του stateless.

Τα stateful τείχη προστασίας ελέγχουν την σύνδεση και παρακολουθούν όλες τις συνδέσεις που γίνονται στο TCP/IP επίπεδο. Αυτό τους επιτρέπει να παρακολουθούν των καταστάσεων στις οποίες βρίσκονται οι συνδέσεις και να προσδιορίζουν ποιοι χρήστες έχουν ανοιχτές εξουσιοδοτημένες συνδέσεις σε κάθε δεδομένη στιγμή

Επικαλούνται τον κανόνα μόνο όταν υπάρχει μια καινούργια αίτηση για σύνδεση. Τα πακέτα που ανήκουν σε μια υπάρχουσα σύνδεση συγκρίνονται με τον πίνακα των συνδέσεων του τείχους προστασίας, και αποφασίζουν αν θα επιτραπεί η πρόσβαση ή όχι. Αυτή η διαδικασία εξοικονομεί χρόνο και προσφέρει αυξημένη ασφάλεια. Σε κανένα πακέτο δεν επιτρέπετε η πρόσβαση αν δεν υπάρχει ήδη υπάρχουσα σύνδεση. Μπορεί να λήγει ανενεργές συνδέσεις στο τείχος προστασίας και μετά να μην δέχεται καινούργια πακέτα για αυτήν την σύνδεση.

7.2 Πύλες Εφαρμογών

Μία πύλη στο επίπεδο Εφαρμογών λειτουργεί ως ένας κόμβος αναμετάδοσης για την κυκλοφορία στο επίπεδο μετάδοσης. Παρακολουθεί εισερχόμενα και εξερχόμενα πακέτα, στέλνει πληρεξούσια (proxies) τα οποία αντιγράφουν και προωθούν τις πληροφορίες σε όλη την πύλη, και λειτουργεί ως πληρεξούσιος (proxy) διακομιστής ο οποίος αποτρέπει οποιαδήποτε άμεση σύνδεση μεταξύ ενός αξιόπιστου διακομιστή με μια μη αξιόπιστη πηγή.

Τα πληρεξούσια είναι συγκεκριμένες εφαρμογές που μπορούν να φιλτράρουν τα πακέτα στο επίπεδο εφαρμογής του μοντέλου OSI. Δέχονται πακέτα που παράγονται μόνο από συγκεκριμένη εφαρμογή για την οποία έχουν σχεδιαστεί να αντιγράφουν, να προωθούν και να φιλτράρουν. Για παράδειγμα μόνο ένα πληρεξούσιο Telnet μπορεί να αντιγράψει να προωθήσει και να φιλτράρει δεδομένα που προορίζονται για αυτό. Αν ένα δίκτυο βασίζεται μόνο σε μια πύλη εφαρμογών, τα εισερχόμενα-εξερχόμενα πακέτα δεν θα μπορούν να έχουν πρόσβαση στις υπηρεσίες όπου τα πληρεξούσια δεν έχουν ρυθμιστεί. Αν π.χ. μια πύλη έχει FTP πληρεξούσιο, μόνο τα πακέτα που δημιουργούνται από αυτήν την υπηρεσία θα μπορούν να περάσουν το τείχος προστασίας. Στις υπόλοιπες υπηρεσίες θα απαγορεύεται η πρόσβαση.

7.2.1 Φιλτράρισμα στο επίπεδο εφαρμογών

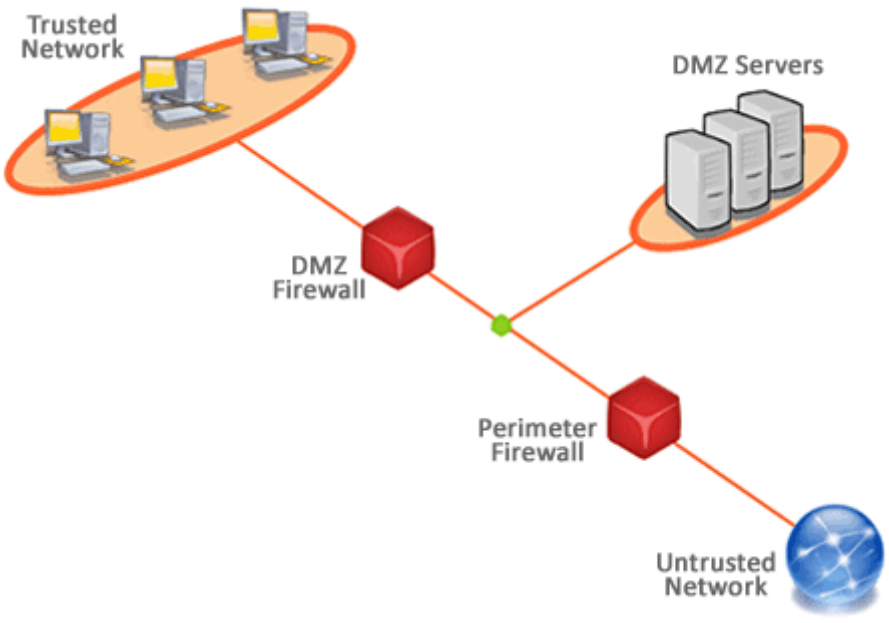
Μια πύλη μεσολάβησης (proxy gateway) που λειτουργεί στο επίπεδο εφαρμογών, εξετάζει και φιλτράρει ξεχωριστά πακέτα, και όχι απλώς αντιγράφοντας και στέλνοντας τα στην πύλη. Τα πληρεξούσια μπορούν να ελέγχουν κάθε πακέτο που περνάει από την πύλη, επιβεβαιώνοντας τα περιεχόμενα του πακέτου μέσω του επιπέδου εφαρμογής. Μπορούν επίσης να φιλτράρουν συγκεκριμένα είδη εντολών και πληροφοριών στα πρωτόκολλα εφαρμογής. Οι πύλες μπορούν να περιορίσουν συγκεκριμένες ενέργειας από το να εκτελούνται. Για παράδειγμα, μια πύλη μπορεί να έχει παραμετροποιηθεί ώστε να αποτρέπει χρήστες από το να χρησιμοποιούν μια εντολή FTP. Αυτό μπορεί να αποτρέψει έναν εισβολέα να τροποποιήσει πληροφορίες που είναι αποθηκευμένες σε ένα διακομιστή.

Πολλές από τις διεργασίες στις πύλες εφαρμογών απαιτούν τον έλεγχο της ταυτότητας του χρήστη, πριν ο χρήστης μπορεί να έχει πρόσβαση σε ένα μη αξιόπιστο δίκτυο. Η αυθεντικοποίηση μπορεί να είναι διαφορετική αν ο χρήστης προέρχεται από το εσωτερικό δίκτυο ή από το διαδίκτυο. Για το εσωτερικό δίκτυο, μια απλή λίστα των IP διευθύνσεων μπορεί να επιτρέψει στον χρήστη να συνδεθεί σε εξωτερικές εφαρμογές. Αλλά από την μεριά του διαδικτύου πρέπει να εφαρμόζεται η αυθεντικοποίηση. Η πύλη αναμεταδίδει τμήματα μεταξύ των δύο TCP συνδέσεων και προς στις δύο κατευθύνσεις. Για τα εξερχόμενα πακέτα, η πύλη μπορεί να αντικαταστήσει την IP με την οποία προήλθε με μια δικιά της IP διεύθυνση. Αυτή η διαδικασία αναφέρεται ως NAT και εγγυάται ότι η εσωτερική IP διεύθυνση δεν είναι εκτεθειμένη στο διαδίκτυο.

7.3 Τείχος προστασίας με DMZ

Το τείχος προστασίας είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγξει την κίνηση που εισέρχεται και εξέρχεται σε ένα εσωτερικό δίκτυο. Στις περισσότερες περιπτώσεις αυτά τα συστήματα έχουν 2 διεπαφές για το δίκτυο, η μια είναι για το εξωτερικό δίκτυο όπως το διαδίκτυο και η άλλη για το εσωτερικό. Το τείχος προστασίας μπορεί και ελέγχει αυστηρά στο τι επιτρέπεται να μεταφερθεί από την μια μεριά μέχρι την άλλη. Ένας οργανισμός που επιθυμεί να δώσει εξωτερική πρόσβαση στον web διακομιστή μπορεί να περιορίσει την κίνηση (traffic) που φτάνει στο τείχος εκτός από την port 80 που είναι η βασική πόρτα για το πρωτόκολλο http. Η υπόλοιπη κίνηση όπως για την αλληλογραφία, το FTP κτλ, δεν επιτρέπεται νε περάσει από το firewall στο εσωτερικό δίκτυο.

Το πρόβλημα που οι περισσότεροι οργανισμοί αντιμετωπίζουν, είναι πώς να ενεργοποιήσουν την νόμιμη πρόσβαση σε δημόσιες υπηρεσίες όπως το web ή την αλληλογραφία διατηρώντας όμως παράλληλα την ασφάλεια του εσωτερικού δικτύου σε υψηλά επίπεδα. Η προσέγγιση που χρησιμοποιείται είναι της ανάπτυξης δύο τειχών ασφαλείας ώστε να παρέχεται μια dmz ζώνη για το δίκτυο. Στην παρακάτω εικόνα υπάρχουν 2 τείχη ασφαλείας, ένα ανάμεσα στο εξωτερικό δίκτυο και το dmz, και ένα ανάμεσα στο dmz και το εσωτερικό. Όλοι οι κοινόχρηστοι διακομιστές βρίσκονται μέσα στην dmz ζώνη. Με αυτόν τον τρόπο είναι δυνατόν να υπάρχουν κανόνες οι οποίοι επιτρέπουν την πρόσβαση του κοινού στους κοινόχρηστους διακομιστές αλλά παράλληλα το εσωτερικό τείχος προστασίας να περιορίζει όλες τις εισερχόμενες συνδέσεις. Με την dmz ζώνη, οι κοινόχρηστοι διακομιστές έχουν επαρκή προστασία σε σχέση με το να τους τοποθετούσαμε απευθείας στο εξωτερικό δίκτυο. Στην ακόλουθη εικόνα παρουσιάζεται ο τρόπος με τον οποίο λειτουργεί το τείχος προστασίας με dmz.



Εικόνα 8 – Τείχος προστασίας με DMZ

Η τοποθέτηση των δικτυακών κόμβων στη ζώνη DMZ τους καθιστά πιο ευάλωτους σε επιθέσεις ασφάλειας. Για αυτό το λόγο ρυθμίζονται συνήθως με κατάλληλη διαμόρφωση ενίσχυσης της ασφάλειάς τους. Οι εξυπηρετητές οι οποίοι βρίσκονται στην ζώνη DMZ αναφέρονται επίσης και ως εξυπηρετητές έπαλξης (bastion hosts). Οι bastion hosts, είναι κατάλληλα διαμορφωμένοι υπολογιστές οι οποίοι έχουν ρυθμιστεί να εκτελούν μόνο τις οριζόμενες υπηρεσίες και τίποτα περισσότερο. (18)

7.4 Σύστημα ανίχνευσης εισβολής (Intrusion Detection)

Τα τείχη προστασίας φιλτράρουν τα πακέτα και λειτουργούν με βάση τους κανόνες που αφορούν τις κεφαλίδες του TCP/IP/UDP, και δεν προσπαθούν να δημιουργήσουν έλεγχους συσχέτισης μεταξύ των διαφόρων συνεδριών. Το σύστημα ανίχνευσης εισβολής διενεργεί έλεγχο των πακέτων δεδομένων (deep packet inspection) εξετάζοντας τα περιεχόμενα του πακέτου.

Οι πύλες στο επίπεδο εφαρμογής βλέπουν τα περιεχόμενα των πακέτων αλλά μόνο για συγκεκριμένες εφαρμογές. Δεν κάνουν έλεγχο για ύποπτα δεδομένα μέσα στο πακέτο. Το σύστημα ανίχνευσης/αποτροπής ελέγχει για ύποπτα δεδομένα που εμπεριέχονται μέσα στα πακέτα και προσπαθεί να εξετάσει τους συσχετισμούς μεταξύ πολλαπλών πακέτων ώστε να αναγνωρίσει επιθέσεις όπως το port scanning, της άρνησης υπηρεσιών κτλ.

7.4.1 Διαφορές μεταξύ ενός συστήματος ανίχνευσης και ενός συστήματος αποτροπής

Και τα 2 αυτά συστήματα είναι παρόμοια όσο αναφορά την ανίχνευση απειλών στο δίκτυο. Το σύστημα ανίχνευσης θεωρείται ως ένα εργαλείο ¨προβολής¨ ενώ το σύστημα αποτροπής ως ένα εργαλείο ελέγχου. Το σύστημα ανίχνευσης ανιχνεύει την κίνηση στο δίκτυο σε πολλά διαφορετικά σημεία και παρέχει σημαντικό έλεγχο σχετικά με την κατάσταση της ασφάλειας του δικτύου. Σε περίπτωση κάποιας αναφοράς μια πιθανής απειλής από το σύστημα ανίχνευσης, οι διορθωτικές ενέργειες ξεκινούν από τον διαχειριστή ή από κάποια άλλη συσκευή στο δίκτυο. Το σύστημα αποτροπής είναι σαν ένα τείχος ασφαλείας που υπάρχει ανάμεσα σε δύο δίκτυα και ελέγχει την δικτυακή κίνηση που το διαπερνάει. Επιβάλλει μια συγκεκριμένη πολιτική για την ανίχνευση απειλών στην κίνηση του δικτύου. Συνήθως απορρίπτει όλα τα πακέτα σταματάει ολόκληρη την δικτυακή κίνηση σε περίπτωση που εντοπίσει μια απειλή μέχρι και την στιγμή που θα αντιμετωπιστεί από τον διαχειριστή.

Υπάρχουν δύο είδη συστημάτων ανίχνευσης:

Με βάση την υπογραφή (signature based)

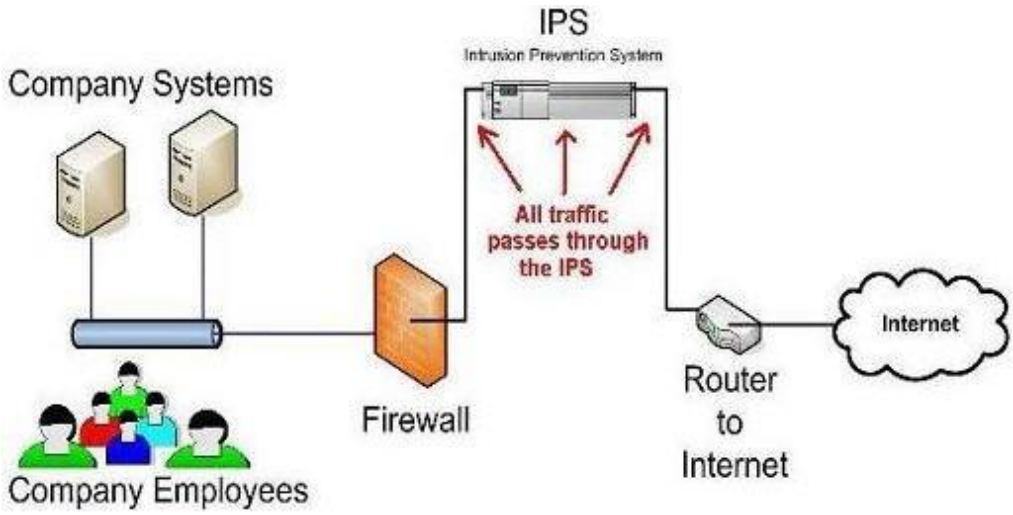
- Χρειάζεται μια βάση δεδομένων από γνωστές επιθέσεις καθώς και τις υπογραφές τους.
- Οι υπογραφές ορίζονται από τους τύπους και την σειρά των πακέτων που χαρακτηρίζουν μια συγκεκριμένη επίθεση.

- Ο περιορισμός αυτού του τύπου συστήματος ανίχνευσης είναι ότι μόνο οι γνωστές επιθέσεις μπορούν να ανιχνευτούν. Επίσης μπορεί να σημάνει λάθος συναγερμό. Ο συναγερμός αυτός μπορεί να προκύψει όταν μια κανονική ροή πακέτων ταιριάζει με την υπογραφή μιας επίθεσης.

Anomaly-based

- Αυτός ο τύπος δημιουργεί ένα μοτίβο από την κανονική λειτουργία του δικτύου.
- Κατά την διάρκεια της ανίχνευσης, κοιτάει τα μοτίβα στην δικτυακή κίνηση που είναι ασυνήθιστα.
- Ο εντοπισμός της οποιαδήποτε ασυνήθιστης κίνησης ενεργοποιεί τον συναγερμό.
- Η κύρια πρόκληση που αντιμετωπίζει αυτό το είδος είναι η δυσκολία στην διάκριση μεταξύ της κανονικής και της ασυνήθιστης κίνησης στο δίκτυο.

Στη παρακάτω εικόνα παρουσιάζεται ο τρόπος λειτουργίας ενός συστήματος αποτροπής μη εξουσιοδοτημένης πρόσβασης.



Εικόνα 9 - Network intrusion prevention system (IPS)

8. Ασφάλεια Ασύρματων Δικτύων

8.1 Πρότυπα IEEE 802.11a, b, g, n και ac

Το πρότυπο IEEE802.11 κυκλοφόρησε από την επιτροπή του προτύπου IEEE (LAN / MAN) τον Ιούνιο του 1997. Από τότε έχουν κυκλοφορήσει πολλές αναβαθμίσεις για να καλύψουν τη διαφορά με τις εξελίξεις στις τεχνολογίες επικοινωνίας που αναφέρθηκαν νωρίτερα. Σε αυτή τη ενότητα θα παρουσιαστεί μια συγκριτική μελέτη των προτύπων IEEE802.11a, b, g, n, και ac όπου κάθε βασικό χαρακτηριστικό θα συζητηθεί ξεχωριστά. Η μελέτη αυτή θα έχει ένα τελικό τμήμα που θα συγκρίνει αυτά τα πρότυπα και θα απαριθμήσει τα οφέλη και τους περιορισμούς για καθένα από αυτά.

Το IEEE802.11 έχει κυκλοφορήσει πολλά σύνολα προτύπων για διάφορες λειτουργικές συχνότητες και με κυμαινόμενες προδιαγραφές. Η πρώτη έκδοση ήταν το αρχικό πρότυπο IEEE802.11 που ορίστηκε το 1997 και αποσαφηνίστηκε το 1999. Κάποια από αυτά τα παλιά πρότυπα είναι πλέον παρωχημένα και κάποια είναι ακόμα ενεργά. Κάποιος θα έπρεπε να μελετήσει τις λεπτομέρειες των διαθέσιμων προτύπων για να διαλέξει το κατάλληλο πρότυπο για την προβλεπόμενη εφαρμογή του δικτύου WLAN.

- IEEE802.11a

  Το πρότυπο IEEE802.11a κυκλοφόρησε τον Σεπτέμβρη του 1999. Τα δίκτυα χρησιμοποιούσαν το 802.11a για να λειτουργούν σε ραδιοσυχνότητες των 5GHz και των 3,7GHz με εύρος ζώνης στα 20MHz. Η προδιαγραφή χρησιμοποιεί ένα σύστημα διαμόρφωσης γνωστό ως "ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM)" που είναι ιδιαίτερα κατάλληλο για την χρήση σε γραφεία. Στο 802.11a, οι ταχύτητες των δεδομένων είναι τόσο υψηλές που φτάνουν τα 54 Mbps. Αυτό το πρότυπο χρησιμοποιεί τεχνολογίες SISO(single input single output) και η εμβέλεια για εσωτερικό-εξωτερικό χώρο κυμαίνεται από τα 35 στα 125 μέτρα για συχνότητα λειτουργίας των 5GHz. Η εμβέλεια του εξωτερικού χώρου φτάνει μέχρι 5 χιλιόμετρα για συχνότητα λειτουργίας στα 3,7GHz. Το IEEE802.11a είναι λιγότερο επιρρεπές σε παρεμβολές σε σχέση με το 802.11b λόγω της υψηλής συχνότητας λειτουργίας των 5GHz.

- IEEE 802.11b

  Το πρότυπο 802.11b κυκλοφόρησε επίσης τον Σεπτέμβρη του 1999. Αυτό το πρότυπο παρέχει μετάδοση στα 11 Mbps(με επαναφορά στα 5.5 , 2 και 1 Mbps) με συχνότητα λειτουργίας 2,4MHz και εύρος ζώνης στα 22MHz. Το 802.11b χρησιμοποιεί μόνο την τεχνική διαμόρφωσης DSSS (Direct Sequence Spread Spectrum). Αυτό το πρότυπο χρησιμοποιεί επίσης τεχνολογία κεραίας SISO όπως και το πρότυπο 802.11a. Το πρότυπο 802.11b επικυρώθηκε το 1999 από το αρχικό πρότυπο IEEE802.11 που επέτρεψε ασύρματη

λειτουργικότητα συγκρίσιμη με το Ethernet. Το πρότυπο 802.11b είναι ευάλωτο σε υψηλότερες παρεμβολές λόγω του γεγονότος ότι το εύρος συχνότητας των 2,4GHz είναι γεμάτο με φέροντα(carriers) και επομένως υπάρχει αυξημένος κίνδυνος παρεμβολών. Η εμβέλεια εσωτερικού και εξωτερικού χώρου κυμαίνεται από τα 35 στα 140 μέτρα.

- IEEE 802.11g

  Το πρότυπο 802.11g επικυρώθηκε το 2003 ως πρότυπο IEEE για ασύρματη δικτύωση WiFi και υποστηρίζει μέγιστο εύρος ζώνης δικτύου στα 54 Mbps συγκριτικά με τα 11 Mbps του 802.11b. Αυτό το πρότυπο λειτουργεί σε συχνότητα των 2,4GHz και με εύρος ζώνης των 20 MHz. Αυτό το πρότυπο χρησιμοποιεί τα συστήματα διαμόρφωσης OFDM ή DSSS. Επίσης χρησιμοποιεί τις τεχνολογίες κεραίας SISO και η εμβέλεια του εσωτερικού-εξωτερικού του χώρου είναι από τα 38 στα 140 μέτρα αντίστοιχα.

- IEEE 802.11n

  Το πρότυπο 802.11n επικυρώθηκε το 2009 και χρησιμοποιεί σε συνδυασμό πολλές ασύρματες κεραίες για τη μετάδοση και τη λήψη των δεδομένων. Το πρότυπο αυτό χρησιμοποιεί τεχνική διαμόρφωσης OFDM. Η τεχνολογία κεραίας που χρησιμοποιήθηκε στο 802.11n είναι γνωστή ως MIMO(multiple input,multiple output). Αυτή η τεχνολογία αναφέρεται στην ικανότητα του 802.11n αλλά και άλλων τεχνολογιών να συντονίσουν ταυτόχρονα πολλαπλά ραδιοσήματα. Το MIMO αυξάνει τόσο το εύρος όσο και την απόδοση ενός ασύρματου δικτύου. Μία πρόσθετη τεχνική εφαρμοσμένη από το 802.11n περιλαμβάνει την αύξηση του εύρους ζώνης του καναλιού από τα 20 MHz στα 40MHz. Το πρότυπο 802.11n υποστηρίζει θεωρητικό μέγιστο εύρος ζώνης στα 300Mbps. Η εμβέλεια αυτού του προτύπου σε εσωτερικούς και εξωτερικούς χώρους είναι τα 75 και 250 μέτρα αντίστοιχα.

- IEEE 802.11ac

  Το IEEE 802.11ac είναι η πέμπτη γενιά των προτύπων δικτύων WiFi και κυκλοφόρησε τον Δεκέμβρη του 2013. Η συχνότητα λειτουργίας αυτού του προτύπου είναι στα 5 GHz και έχει τομείς εύρους ζώνης στα 20,40,80 και 160 MHz. Τα ποσοστά ροής δεδομένων κυμαίνονται για αυτούς τους τομείς εύρους ζώνης σε 7,2-96.3Mbps για τα 20MHz, σε 15 – 200Mbps για τα 40MHz,σε 32.5 - 433.3Mbps για τα 80Mhz και σε 65 - 866.7Mbps για τα 160MHz. Αυτό το πρότυπο παρουσιάζει καλύτερη επίδοση και καλύτερη κάλυψη σε σχέση με τα πρότυπα IEEE 802.11a,b,g και n. Το πρότυπο 802.11ac χρησιμοποιεί ένα ευρύτερο κανάλι και ένα βελτιωμένο σύστημα διαμόρφωσης που επίσης υποστηρίζει περισσότερους χρήστες. Το πρότυπο IEEE 802.11ac χρησιμοποιεί τη τεχνική διαμόρφωσης γνωστή ως multi-user MIMO. Αυτή η τεχνική επιτρέπει σε ένα σύνολο χρηστών ή ασύρματων τερματικών ο καθένας/το καθένα από τους οποίους/τα οποία μπορεί να έχει

παραπάνω από 1 κεραίες, να επικοινωνούν ο ένας/το ένα με τον άλλον/το άλλο. Η εμβέλεια του εσωτερικού χώρου είναι στα 35 μέτρα ενώ δεν υπάρχει καταγεγραμμένο μέγιστο για την εμβέλεια στον εξωτερικό χώρο. (19,20,21)

8.1.1 Σύγκριση των προτύπων IEEE 802.11a, b, g, n, ac και ad

Ο παρακάτω πίνακας παρέχει μια ποιοτική σύγκριση μεταξύ των προτύπων 802.11a,b,g,n,ac και ad σχετικά με τις πτυχές της μορφοποίησης δέσμης σήματος, του μέγιστου ρυθμού μετάδοσης, του εύρους ζώνης καθώς και ποια σε ζώνη λειτουργούν. Σε αυτή την ενότητα θα παρουσιαστούν περισσότερες λεπτομέρειες σχετικά με τα πρότυπα.

ΠΡΟΤΥΠΑ IEEE 802.11						
Ημερομηνία κυκλοφορίας	ΠΡΟΤΥΠΑ	Band (GHz)	Εύρος (MHz)	Διαμόρφωση	Προηγμένες τεχνολογίες των κεραιών	Μέγιστος ρυθμός μετάδοσης
1997	802.11	2.4	20	DSSS,FHSS	-	2 Mbits/s
1999	802.11b	2.4	20	DSSS	-	11 Mbits/s
1999	802.11a	5	20	OFDM	-	54 Mbits/s
2003	802.11g	2.4	20	DSSS,OFDM	-	54 Mbits/s
2009	802.11n	2.4 , 5	20,40	OFDM	MIMO	600 Mbits/s
2012	802.11ad	60	2160	SC,OFDM	Beam forming	6.76 Gbits/s
2013	802.11ac	5	40,80,160	OFDM	MIMO,MU-MIMO	6.93 Gbits/s

- Μορφοποίηση δέσμης ακτινοβολίας

  Η μορφοποίηση δέσμης σήματος (beam forming) είναι μια τεχνική επεξεργασίας σήματος που μετρά την ικανότητα λήψης και μετάδοσης δεδομένων σε μια κατευθυντική δέσμη σήματος. Τα πρότυπα IEEE802.11n, ac και ad έχουν αυτή τη δυνατότητα, αλλά τα υπόλοιπα πρότυπα όχι.

- Κάλυψη και χωρητικότητα

  Όπως συζητήθηκε νωρίτερα, το πρότυπο IEEE802.11ac παρουσιάζει ευρεία κάλυψη περιοχής συγκριτικά με τα άλλα πρότυπα. Το IEEE802.11ac εξοπλισμένο με το multi-user MIMO και τις πολλαπλές χωρικές ροές επιτρέπει πολύ υψηλότερα ποσοστά ροών δεδομένων.

- Παρεμβολή και ποιότητα

  Το πρότυπο IEEE802.11ac χρησιμοποιεί τη συχνότητα λειτουργίας των 5 GHz που είναι λιγότερο ευάλωτη σε παρεμβολές συγκριτικά με τα πρότυπα IEEE802.11b και g που λειτουργούν σε συχνότητα των 2,4 GHz. Σχετικά με το πρότυπο IEEE802.11a, όταν λειτουργεί με συχνότητα 2,4 GHz είναι πιο ευάλωτο σε παρεμβολές ενώ όταν λειτουργεί σε συχνότητα των 5 GHz παρουσιάζει λιγότερες παρεμβολές παρόμοια με το πρότυπο IEEE802.11ac. (22)

8.2 IEEE 802.11ad

Το πρότυπο 802.11ad αποτελεί μια βελτιωμένη έκδοση του προτύπου 802.11 που επιτρέπει ασύρματες επικοινωνίες πολλών gigabit στη ζώνη των 60 GHz. Η προδιαγραφή WiGig σύμβαλλε στη διαδικασία προτυποποίησης του 802.11ad και επιβεβαιώθηκε τον Μάιο του 2010 ως η βάση για το σχέδιο του προτύπου 802.11ad. Τα πρώτα δημοφιλή πρότυπα για το ασύρματο LAN(τα 802.11a και b) σχεδιάστηκαν κυρίως για να εξυπηρετήσουν τις ανάγκες ενός υπολογιστή laptop στο σπίτι ή στο γραφείο και αργότερα για να επιτρέψουν συνδεσιμότητα «στον δρόμο»-σε αεροδρόμια, ξενοδοχεία, internet cafes και εμπορικά κέντρα. Η κύρια λειτουργία τους ήταν να παρέχουν συνδεσιμότητα σε μια ενσύρματη ευρυζωνική σύνδεση για την περιήγηση στο web και το ηλεκτρονικό ταχυδρομείο. Δεδομένου ότι η ταχύτητα της ευρυζωνικής σύνδεσης ήταν ο περιοριστικός παράγοντας, μία σχετικά χαμηλής ταχύτητας ασύρματη σύνδεση ήταν επαρκής-το 802.11a παρείχε μέχρι 54 Mb/s στα 5 GHz και το 802.11b μέχρι 11 Mb/s στα 2.4 GHz, και τα 2 σε μη αδειοδοτημένες ζώνες φάσματος. Για την ελαχιστοποίηση των παρεμβολών από άλλες συσκευές, και τα 2 πρότυπα χρησιμοποίησαν μορφές μετάδοσης εύρους φάσματος και κωδικοποιήθηκαν σε μεγάλο βαθμό. Μία μεταγενέστερη αναθεώρηση αυτού του προτύπου, το 802.11g, το 2003 ενοποιήθηκε στη ζώνη των 2,4 GHz αλλά διατήρησε το μέγιστο ρυθμό δεδομένων στα 54Mb/s.

Ωστόσο, την ίδια στιγμή νέα μοντέλα χρήσης που χρειάζονταν υψηλότερη απόδοση είχαν αναγνωριστεί: η ανταλλαγή δεδομένων μεταξύ των συνδεδεμένων συσκευών στο σπίτι ή σε ένα μικρό γραφείο και η ασύρματη εκτύπωση αποτελούν τέτοια παραδείγματα.

Ο πρωταρχικός στόχος του 802.11ad είναι να επιτρέπει γρηγορότερες ταχύτητες δικτύου σε πυκνά περιβάλλοντα ανάπτυξης και υπερταχείες ταχύτητες στο σπίτι, το οποίο εν μέρει επιτυγχάνεται επειδή τα 60 GHz έχουν μικρότερη εμβέλεια και επιπλέον τα άλλα δίκτυα είναι λιγότερο πιθανό να παρακολουθήσουν και να παρέμβουν στη σύνδεσή (πιο ασφαλές).

Η προδιαγραφή WiGig ορίζει τα στρώματα PHY(φυσικό) και MAC(medium access control) και είναι βασισμένη στο πρότυπο IEEE 802.11. Αυτό παρέχει τη δυνατότητα ενσωματωμένης υποστήριξης για δικτύωση IP πάνω από τα 60 GHz.

Το IEEE 802.11ad PHY υποστηρίζει 3 διαφορετικές μεθόδους διαμόρφωσης:

- Διαμόρφωση εύρους φάσματος-το Control PHY
- Διαμόρφωση μονού φέροντος(SC)- το Single Carrier PHY και το Low Power Single Carrier PHY
- Διαμόρφωση ορθογώνιας διαίρεσης συχνότητας(OFDM)-το OFDM PHY

Κάθε τύπος PHY έχει ξεχωριστό σκοπό και διαφορετική δομή πακέτων.

- Φυσικό Επίπεδο

  Το πρότυπο IEEE 802.11ad καθορίζει 2 τρόπους λειτουργίας που λειτουργούν στο εύρος ζώνης καναλιού 2,16 GHz. Η λειτουργία OFDM σχεδιάστηκε για εφαρμογές υψηλής απόδοσης ή για επιλεκτικά κανάλια συχνότητας. Η λειτουργία SC χρησιμοποιείται για πομποδέκτες χαμηλής ισχύος και πολυπλοκότητας. Επίσης χρησιμοποιείται για τον έλεγχο σηματοδότησης. Τα κωδικοποιημένα δεδομένα πρώτα κωδικοποιούνται με έναν κωδικοποιητή LDPC.Οι ακανόνιστοι κώδικες LDPC (672,336), LDPC (672, 420), LDPC (672, 504) και LDPC(672, 546) χρησιμοποιούνται για τα αντίστοιχα ποσοστά κωδικοποίησης των 1/2, 5/8, 3/4, και 13/16. Η ζώνη των 60 GHz έχει πολύ περισσότερο φάσμα διαθέσιμο από τις ζώνες των 2,4 και 5 GHz-συνήθως έχουμε 7 GHz φάσματος συγκριτικά με τα 83.5 MHz στην ζώνη συχνότητας των 2.4 GHz. Αυτό το φάσμα διαιρείται σε πολλαπλά κανάλια όπως και στις ζώνες των 2,4 και 5 GHz. Επειδή η ζώνη των 60 GHz έχει πολύ περισσότερο διαθέσιμο φάσμα, τα κανάλια είναι πολύ πιο ευρεία επιτρέποντας ταχύτητες μεταφοράς δεδομένων πολλών gigabit. Η προδιαγραφή WiGig ορίζει 4 κανάλια, το καθένα εύρους 2,16 GHz-50 φορές μεγαλύτερο από τα κανάλια που είναι διαθέσιμα στο 802.11n.

- MAC (έλεγχος πρόσβασης στο μέσο)

  Στο IEEE 802.11ad χρησιμοποιείται ένα υβρίδιο πολλαπλής πρόσβασης με βάση το contention-based CSMA-CA (carrier sense multiple access with collision avoidance) και το contention-free TDMA (time division multiple access). Το CSMA-CA χρησιμοποιείται για εφαρμογές όπως είναι η περιήγηση στο web εξαιτίας της χαμηλότερης μέσης καθυστέρησης, ενώ το TDMA είναι πιο επιθυμητό για μετάδοση βίντεο λόγω της καλύτερης ποιότητας της υπηρεσίας και της αποτελεσματικότητας. Η αίτηση μετάδοσης χρησιμοποιείται στην κορυφή των περιόδων πρόσβασης ώστε να κατανέμει δυναμικά τον χρόνο του καναλιού.

  Η απόδοση του στρώματος MAC προσδιορίζεται από την ποσότητα των πληροφοριών bits που ανταλλάσσονται μεταξύ των πομποδεκτών MAC και από τη διάρκεια που απαιτείται για την επιτυχή παράδοση της πληροφορίας.

- Συστήματα κωδικοποίησης και διαμόρφωσης στο πρότυπο IEE 802.11ad

  Η προδιαγραφή υποστηρίζει 2 τύπους συστημάτων κωδικοποίησης και διαμόρφωσης που παρέχουν διαφορετικά οφέλη:

  - Η OFDM υποστηρίζει επικοινωνίες σε μεγαλύτερες αποστάσεις με μεγαλύτερα ανοίγματα καθυστέρησης, παρέχοντας μεγαλύτερη ευελιξία στον χειρισμό εμποδίων και αντανακλώμενων σημάτων. Επιπλέον, επιτρέπει μεγαλύτερες ταχύτητες μετάδοσης μέχρι και τα 7 Gbps.

  - Η SC έχει χαμηλότερη κατανάλωση ενέργειας, έτσι συχνά είναι καλύτερη επιλογή για μικρές, χαμηλής ισχύος συσκευές χειρός .Η SC υποστηρίζει ταχύτητες μετάδοσης στα 4,6 Gbps. (23)

8.2.1 Ιδιότητες του καναλιού στα 60 GHz

Η ζώνη των 60 GHz έρχεται με έναν μεγάλο ελεύθερο χώρο απώλειας διάδοσης(περίπου 20 db περισσότερα από την ζώνη των 5 GHz) που πρέπει να αντισταθμιστεί με κατευθυντικές κεραίες υψηλού κέρδους ώστε να φτάσει σε μια αξιοπρεπή εμβέλεια περισσότερο από 1 μέτρο. Ευτυχώς οι κατευθυντικές κεραίες υψηλού κέρδους είναι εφικτό να εφαρμοστούν ακόμα και για μικρές συσκευές εξαιτίας των σχετικά βραχέων μήκων των κυμάτων των 5mm. Τέτοιες κατευθυντικές κεραίες μπορούν να υλοποιηθούν είτε με μια κεραία που μπορεί να ενεργοποιηθεί από τομέα σε τομέα είτε με μια προσαρμοστική συστοιχία κεραιών που μπορεί να διαμορφωθεί σε διαφορετικά πρότυπα ακτινοβολίας.

Δεύτερον, το κανάλι των 60 GHz γενικά παρουσιάζει σχεδόν οπτικές ιδιότητες που σημαίνει ότι τα ισχυρότερα εξαρτήματά του τείνουν να είναι Line of Sight (LOS).Τα εξαρτήματα Non Line of Sight (NLOS) υπάρχουν, αλλά ως επί το πλείστον με τη μορφή ανάκλασης. Παρόλα αυτά, τα μικρά μήκη κύματος σε αυτή τη ζώνη επιβάλλουν μερικές σοβαρές προκλήσεις όπως είναι η μεγαλύτερη διάδοση του σήματος και η δυσκολία περίθλασης γύρω από τα εμπόδια. Οι μετρήσεις της ζώνης των 60 GHz δείχνουν ότι γενικά τα ισχυρότερα αντανακλώμενα εξαρτήματα είναι τουλάχιστον 10 db κάτω από το εξάρτημα LOS. Ακόμα πιο δύσκολα είναι τα προβλήματα που δημιουργούνται από τα εμπόδια. Ένα ανθρώπινο σώμα που διασχίζει το μονοπάτι ανάμεσα στον πομπό και τον δέκτη μπορεί να εξασθενήσει το σήμα κατά 15 db ή και περισσότερα και εύκολα να σπάσει τη σύνδεση. Τα κοινά αντικείμενα όπως τα έπιπλα, οι τοίχοι, οι πόρτες και τα πατώματα που βρίσκονται σε εσωτερικούς χώρους μπορούν εξίσου να δημιουργήσουν πρόβλημα. Σαν αποτέλεσμα, το πρακτικό εύρος λειτουργίας για εσωτερικούς χώρους στα 60 GHz πιθανώς να περιοριστεί από την απώλεια διείσδυσης αντί από την απώλεια διάδοσης στον ελεύθερο χώρο και επομένως συνήθως περιορίζεται σε ένα μονό δωμάτιο. Συγκριτικά, τα χαρακτηριστικά σύνδεσης είναι πολύ διαφορετικά σε χαμηλότερες ζώνες συχνοτήτων όπως τα 2,4 και τα 5 GHz όπου η απώλεια διείσδυσης είναι μικρότερη, ενώ υπάρχει η δυνατότητα πάρα πολλών διαφορετικών διαδρομών που

παρέχει ποικιλομορφία, και η εμβέλεια μπορεί να φτάσει μέχρι και εκατοντάδες μέτρα.

Απορρόφηση από το οξυγόνο και τη βροχή

Τα συστήματα που λειτουργούν στα 60 GHz έχουν χρησιμοποιηθεί για πολλά χρόνια από την κοινωνία της πληροφορίας για επικοινωνίες υψηλής ασφάλειας και από τον στρατό για επικοινωνίες από δορυφόρο σε δορυφόρο. Το ενδιαφέρον τους σε αυτή τη ζώνη συχνοτήτων πηγάζει από το φαινόμενο της φύσης: το μόριο του οξυγόνου(O2) απορροφά ηλεκτρομαγνητική ενέργεια στα 60 GHz. Αυτή η απορρόφηση λαμβάνει μέρος σε πολύ μεγαλύτερο βαθμό στα 60 GHz απ'ότι σε χαμηλότερες συχνότητες που συνήθως χρησιμοποιούνται για τις ασύρματες επικοινωνίες. Αυτή η απορρόφηση αποδυναμώνει(εξασθενεί) τα σήματα των 60 GHz με την απόσταση. έτσι τα σήματα δεν μπορούν να ταξιδέψουν πέρα από τον αποδέκτη τους.

Μια άλλη συνέπεια της απορρόφησης του O2 είναι ότι η ακτινοβολία από μια συγκεκριμένη ραδιοζεύξη των 60 GHz γρήγορα μειώνεται σε ένα επίπεδο που δεν θα παρεμβαίνει σε άλλες συνδέσεις των 60 GHz που λειτουργούν στην ίδια γεωγραφική περιοχή. Αυτή η μείωση επιτρέπει μεγαλύτερη «επαναχρησιμοποίηση συχνοτήτων»-η ικανότητα για περισσότερες συνδέσεις των 60 GHz που λειτουργούν στην ίδια γεωγραφική περιοχή από ότι για συνδέσεις με μεγαλύτερη εμβέλεια. Οι αποστάσεις των συνδέσεων των millimeter ραδιοκυμάτων που λειτουργούν στον πραγματικό κόσμο, περιορίζονται κατά κύριο λόγο από τη βροχή. Οι χρήστες αυτών των προϊόντων συνήθως θέλουν τις συνδέσεις να παρέχουν ισχυρή δυνατότητα επικοινωνίας. Σε αυτή την εφαρμογή, τα ποσοστά βροχοπτώσεων όπου το προϊόν χρησιμοποιείται, συνήθως αποτελούν τον πιο περιοριστικό παράγοντα σε σχέση με την απορρόφηση του O2.

Σε περιοχές με μέτρια βροχή, η εξασθένιση της βροχής είναι περίπου διπλάσια από την εξασθένιση του οξυγόνου και σε περιοχές με δυνατή βροχή η εξασθένιση της βροχής είναι τριπλάσια από την εξασθένιση του οξυγόνου. Επομένως, στον σχεδιασμό μιας σύνδεσης των 60 GHz που θα παρέχει ισχυρή ικανότητα επικοινωνίας στον πραγματικό κόσμο, η εξασθένηση της βροχής αποτελεί μεγαλύτερο παράγοντα από την απορρόφηση του οξυγόνου.

Το πρότυπο IEEE 802.11ad είναι ιδανική επιλογή για δεδομένα υψηλής ταχύτητας και επικοινωνίες φωνής στο διαδίκτυο, και προσφέρει τα ακόλουθα πλεονεκτήματα:

- Μη αδειοδοτημένη ζώνη - δεν απαιτείται η απόκτηση άδειας από το FCC.
- Εξαιρετικά ασφαλής διαδικασία-που προκύπτει από τις σύντομες αποστάσεις μεταφοράς λόγω της απορρόφησης οξυγόνου και του στενού πλάτους της δέσμης της κεραίας.
- Λειτουργία ουσιαστικά χωρίς παρεμβολές- που προκύπτει από τις σύντομες αποστάσεις μεταφοράς λόγω της απορρόφησης οξυγόνου, του στενού πλάτους

της δέσμης της κεραίας και την περιορισμένη χρήση του φάσματος των 60 GHz.

- Ενεργοποιημένη η επαναχρησιμοποίηση υψηλού επιπέδου συχνότητας-οι επικοινωνιακές ανάγκες πολλών πελατών σε μια μικρή γεωγραφική περιοχή μπορούν να ικανοποιηθούν.

- Πιθανές οι ταχύτητες μετάδοσης δεδομένων οπτικών ινών-είναι διαθέσιμα 7 GHz συνεχούς διαθέσιμου εύρους ζώνης σε σχέση με τα λιγότερα από 0,3 GHz διαθέσιμα στις άλλες μη αδειοδοτημένες ζώνες.

- Ώριμη επικοινωνία-η μακρά ιστορία αυτού του φάσματος χρησιμοποιείται για ασφαλείς επικοινωνίες.

Παρόλο που το πρότυπο αυτό είναι ακόμα υπό ανάπτυξη, περιμένουμε σύντομα να είναι το πλέον χρησιμοποιούμενο δίκτυο για τη μετάδοση δεδομένων. Το πρότυπο IEEE 802.11ad τυποποιεί την τεχνολογία των 60 GHz στη διευκόλυνση των επικοινωνιών πολλαπλών gigabit ανά δευτερόλεπτο μέσω μικρότερων αποστάσεων. Το πρότυπο αυτό έχει πολλά νέα χαρακτηριστικά να βελτιώσει και να διατηρήσει τις επικοινωνίες υψηλής ταχύτητας με συστήματα TDMA ενός φέροντος και OFDM. Η μελλοντική εξέλιξη του 802.11ad προς την πλήρη υποστήριξη MIMO μπορεί να αυξήσει περαιτέρω τον ρυθμό δεδομένων του. Με την έλευση των νέων τεχνολογιών που θα καταστήσουν αυτά τα πρότυπα πρακτικά και με την τυποποίηση από φορείς όπως το WiGig και το IEEE, θα επιτευχθεί η πραγματική ασύρματη ευρυζωνική επικοινωνία με τα 60 GHz, και όλα τα καλώδια στα προσωπικά δίκτυα θα εξαλειφθούν. (24)

8.3 Επιθέσεις στο WLAN

Αυτό το κεφάλαιο επιθυμεί να περιγράψει την προοπτική των θεμάτων ασφαλείας κατά τη μεταφορά δεδομένων μεταξύ χρηστών στο WLAN. Η παρούσα μελέτη προβλέπεται να προσδιορίσει τον αντίκτυπο των προβλημάτων ασφαλείας στο WLAN. Επί του παρόντος, το WLAN αντιμετωπίζει αρκετές απειλές και επιθέσεις λόγω της φύσης του, επειδή η πληροφορία μεταδίδεται μέσω της ατμόσφαιρας όπου κάποιος μπορεί να "σπάσει" την ασφάλεια των WLANs έχοντας μόνο πολύ βασικές γνώσεις του δικτύου.

8.3.1 Διαφορετικά Είδη Επιθέσεων στο WLAN

Οι διαφορετικοί τύποι επιθέσεων και απειλών κατηγοριοποιούνται σε 2 κύρια μέρη. Αυτοί οι τύποι επιθέσεων θεωρούνται γενικοί για κάθε WLAN και θα περιγραφούν παρακάτω λεπτομερώς με τα μειονεκτήματα και τις λύσεις τους.

1. Λογική επίθεση

2. Φυσική επίθεση

Μια λογική επίθεση σχετίζεται πάντα με το λογισμικό, το σύστημα και τα ευαίσθητα δεδομένα που μεταφέρονται στο δίκτυο. Σε αυτό το είδος επίθεσης ο στόχος του εισβολέα είναι να βρει τον κωδικό και το λογισμικό ή οποιοδήποτε μειονέκτημα του δικτύου που θα τον βοηθήσει να αποκτήσει πρόσβαση στο δίκτυο και να αλλάξει εύκολα τα ευαίσθητα δεδομένα. Ο κύριος στόχος της επίθεσης είναι να εντοπιστούν τα ευαίσθητα δεδομένα που μεταδίδονται στο δίκτυο. Αν η επίθεση είναι επιτυχής, τότε θα προκαλέσει πολλά προβλήματα για το δίκτυο καθώς και για τα άλλα δίκτυα με τα οποία είναι συνδεδεμένο. Παρακάτω ορίζονται μερικές λογικές επιθέσεις και οι τεχνικές μετριασμού τους. (25,26)

- Πλαστογράφηση της διεύθυνσης MAC
- Επίθεση άρνησης παροχής υπηρεσιών (DOS)
- Επίθεση “Man in the middle”
- Διαμόρφωση προεπιλεγμένου σημείου πρόσβασης
- Επιθέσεις αναγνωρίσεων
- Υποκλοπή συνομιλιών
- Επίθεση DHCP

8.3.1.1 Πλαστογράφηση της διεύθυνσης MAC

Οι διευθύνσεις MAC στέλνονται από το μέσο όταν έχει ξεκινήσει η επικοινωνία μεταξύ του κόμβου και του σημείου πρόσβασης. Όταν ο οποιοσδήποτε κόμβος προσπαθεί να δημιουργήσει μια σύνδεση με το σημείο πρόσβασης, τότε πρέπει να γίνεται έλεγχος ταυτότητας μέσω της διεύθυνσης MAC ή των ασύρματων καρτών δικτύου ώστε η σύνδεση να είναι πιο ασφαλής. Στην κανονική διαδικασία ελέγχου ταυτότητας, οι διευθύνσεις MAC προωθούνται με σαφή μορφή κειμένου και κάθε εισβολέας μπορεί να διαλέξει τη διεύθυνση οποιουδήποτε πιστοποιημένου χρήστη χρησιμοποιώντας διαφορετικά εργαλεία όπως το kismet. Έτσι θα δημιουργηθεί μια βάση δεδομένων νόμιμων ασύρματων κόμβων καθώς και των MAC διευθύνσεών τους. Ο εισβολέας μπορεί απλά να “κοροϊδέψει” τη διεύθυνση MAC οποιουδήποτε κόμβου και να τη χρησιμοποιήσει για να αποκτήσει πρόσβαση στο WLAN. Η κλοπή των κόμβων μέσω των MAC διευθύνσεών τους που επικυρώνονται από τα ασύρματα σημεία πρόσβασης είναι επίσης πιθανή. Για την εξάλειψη αυτής της κατάστασης, ο διαχειριστής του δικτύου πρέπει να ενημερώνεται για κάθε χαμένο χρήστη ή κόμβο ώστε να αφαιρεί τις αντίστοιχες διευθύνσεις MAC από τον κατάλογο που επέτρεπαν την πρόσβαση των σημείων πρόσβασης στο WLAN.

8.3.1.2 Άρνηση υπηρεσιών (DOS) ή διανεμημένη άρνηση υπηρεσιών (DDOS)

Η διαθεσιμότητα του δικτύου είναι πολύ σημαντική για τις σημαντικές υπηρεσίες. Στο δίκτυο WLAN, η μεταφορά των δεδομένων πρέπει να είναι εξασφαλισμένη με

υψηλό ποσοστό επιτυχίας, ενώ παράλληλα να παρέχεται άμεση εξυπηρέτηση σε υπηρεσίες που απαιτούν άμεση απόκριση. Οι επιθέσεις DOS και DDOS χρησιμοποιούνται για να χαθεί η διαθεσιμότητα των διαφόρων υπηρεσιών ενός δικτύου.

Οι επιθέσεις DOS θεωρούνται ως ο πιο κοινός τύπος επιθέσεων, με μεγάλη πολυπλοκότητα από τη φύση τους και μεγάλη δυσκολία να μετριαστούν πλήρως, αλλά μπορούν να ελεγχθούν μέχρι κάποιο βαθμό. Ο στόχος των επιθέσεων αυτών είναι να περιορίσουν τον νόμιμο χρήστη σχετικά με τη πρόσβασή του στο δίκτυο. Οι επιθέσεις αυτές καθιστούν τις υπηρεσίες αναποτελεσματικές για τους νόμιμους χρήστες και μπορούν να υλοποιηθούν με τη χρήση των επιθέσεων Flood SYN και Ping of Death.

Υπάρχουν όμως και κάποιοι περιορισμοί που εμποδίζουν τους επιτιθέμενους να προβούν σε επιθέσεις DoS:

- Περιορισμένοι Πόροι

  Μεγάλος αριθμός πόρων απαιτείται ώστε να υπάρξει υψηλός ρυθμός πακέτων ώστε να δημιουργηθούν μαζικές επιθέσεις DoS.

- Δυσκολία ανίχνευσης λόγω της φύσης των DoS επιθέσεων

  Οι επιτιθέμενοι χρησιμοποιούν παραποιημένες διευθύνσεις πηγής IP προκειμένου να κρύψουν την ταυτότητα τους πίσω από άλλες μηχανές που έχουν θέσει υπό τον έλεγχο τους.

- Αυτοματοποιημένα εργαλεία

  Οι επιτιθέμενοι συνεχώς προσπαθούν να αναπτύξουν πιο αποτελεσματικά εργαλεία προκειμένου να ξεπεράσουν τα συστήματα ασφαλείας που αναπτύσσονται από τους ερευνητές. (27)

Οι επιθέσεις DDOS θεωρούνται ως η πιο κοινή κατηγορία των επιθέσεων DOS. Ο στόχος τους είναι να επιτεθούν στον διακομιστή στέλνοντας πολλά άσχετα αιτήματα στον διακομιστή του δικτύου, ο οποίος μετά από κάποιο χρονικό διάστημα γίνεται αργός και δεν μπορεί να παρέχει υπηρεσίες στους νόμιμους χρήστες.

Ο πιο σημαντικός τρόπος για να προστατευτούμε από τέτοιες επιθέσεις είναι να εντοπιστεί η πηγή της επίθεσης και μετά να εμποδιστεί η κυκλοφορία από αυτή την πηγή. Υπάρχουν 3 κοινές τεχνικές μετριασμού για τις επιθέσεις DOS και DDOS.

- Λειτουργία Anti-spoof
- Λειτουργία Anti-DoS
- Περιορισμός ποσοστού κυκλοφορίας

Οι επιθέσεις DDOS είναι μια σειρά επιθέσεων DOS που είναι πιο επιβλαβείς για το δίκτυο από τις DOS. Το WLAN επιτρέπει σε αυτούς τους εισβολείς να ξεκινήσουν εύκολα μέσα στο εσωτερικό του. Επομένως το δίκτυο αυτό έχει να αντιμετωπίσει πολλές προκλήσεις και οφείλει να ανακαλύψει διάφορα είδη εργαλείων προκειμένου να προστατευτεί από αυτές τις επιθέσεις. Αυτό το είδος των επιθέσεων μπορεί να αποκλειστεί μέσω της πιστοποίησης και την εξουσιοδότησης. (28)

8.3.1.3 Επίθεση "Man in the middle"

Μια τέτοια επίθεση χρησιμοποιείται για να πάρει μυστικές πληροφορίες ή για να τροποποιήσει τα πακέτα δεδομένων, επομένως παραβιάζει την αξιοπιστία μιας συνόδου. Αυτή είναι μια μορφή ενεργών υποκλοπών όπου ο επιτιθέμενος κάνει ανεξάρτητες συνδέσεις με διαφορετικούς χρήστες.

Οι χρήστες αυτοί στέλνουν και λαμβάνουν δεδομένα ο ένας με τον άλλον, κάνοντάς τους να πιστέψουν ότι είναι συνδεδεμένοι μεταξύ τους σε μια ιδιωτική σύνδεση ενώ στην πραγματικότητα ολόκληρη η μετάδοση ελέγχεται από τον εισβολέα. Ο κύριος στόχος αυτού του είδους επιθέσεων είναι να διαβάσουν και να αλλάξουν τα δεδομένα όποτε θέλει ο εισβολέας κατά τη διάρκεια της συνόδου επικοινωνίας χωρίς να το γνωρίζουν οι συσκευές. Αυτό το είδος επίθεσης είναι επίσης γνωστή ως επίθεση κακόβουλων χρηστών. Υπάρχουν διάφορα θέματα που δημιουργούνται από την επίθεση "man in the middle" στο WLAN.

- Να συλλέξει τις πληροφορίες
- Να εισάγει νέες πληροφορίες στις συνόδους του δικτύου
- Να θέσει σε κίνδυνο την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα
- Να τροποποιήσουν τα μεταδιδόμενα δεδομένα
- Το θέμα του rogue proxy μπορεί να οδηγήσει τόσο τον αρχικό όσο και τον τελικό χρήστη να εξαπατηθούν κατά τη μεταφορά δεδομένων
- Μπορεί να συλλέξει πάρα πολύ απόρρητες πληροφορίες (για παράδειγμα αριθμούς pin πιστωτικών καρτών, τον κωδικό του λειτουργικού συστήματος και άλλους τύπους προσωπικών πληροφοριών).

Ένα τυπικό παράδειγμα αυτής της επίθεσης είναι η εναλλακτική Diffie Helman Key φάση ανταλλαγής σε μια TLS handshake διαδικασία οργάνωσης κλήσης. Αυτή η διαδικασία είναι τρωτή σε αυτήν την επίθεση καθιστώντας ενδεικνυόμενη τη χρησιμοποίηση της δημόσιας κρυπτογράφησης κλειδιών όπως η RSA έναντι της ανταλλαγής κλειδιών. Η RSA παρέχει αρκετές βάσεις για την μείωση της επίθεσης αυτής με την χρήση των ψηφιακών υπογραφών και των πιστοποιητικών για την ενισχυμένη αυθεντικοποίηση. (29)

Αυτό το είδος των επιθέσεων μπορεί να μειωθεί μέσω της χρήσης κρυπτογραφημένης κρυπτογράφησης και πιστοποίησης, γνωστής ως ασφαλές στρώμα υποδοχών secure socket layer (SSL).

8.3.1.4 Διαμόρφωση προεπιλεγμένου σημείου πρόσβασης

Όλα τα καινούργια σημεία πρόσβασης δεν έχουν ρυθμιστεί με ασφάλεια. Κάποιες φορές αυτό είναι καλύτερο για τους απλούς χρήστες διότι αν τα σημεία πρόσβασης έχουν ρυθμιστεί με ασφάλεια, είναι δύσκολο για τους νέους χρήστες να τα λειτουργήσουν. Σήμερα, η φιλοδοξία των κατασκευαστών είναι να παραδώσουν δεδομένα με σχετικά υψηλό ρυθμό μετάδοσης και επίσης να παρέχουν κάποιο είδος ασφάλειας για τη συσκευή. Οι μηχανικοί του δικτύου πρέπει να ρυθμίσουν τα σημεία πρόσβασης σύμφωνα με την ασφάλεια που απαιτείται από την εταιρεία, επειδή λίγες εταιρείες απαιτούν περισσότερη ασφάλεια όπως οι τράπεζες. Σε καινούργια σημεία πρόσβασης δεν υπάρχει ρυθμισμένη ασφάλεια, γεγονός που δεν είναι καλό για καμιά εταιρεία με ευαίσθητα δεδομένα.

Το SSID είναι ένας έλεγχος ασφαλείας που έχει ανατεθεί σε WLAN και ανακοινώνεται από τα σημεία πρόσβασης. Για σκοπούς ασφαλείας το SSID είναι σημαντικό και λειτουργεί σαν αρχικός έλεγχος ασφαλείας σε οποιοδήποτε WLAN. Καμιά φορά σε πολλά σημεία πρόσβασης το SSID είναι απενεργοποιημένο από προεπιλογή και οι χρήστες μπορούν να έχουν πρόσβαση στα σημεία πρόσβασης χωρίς κανένα έλεγχο ταυτότητας από το SSID. Σε πολλές περιπτώσεις τα σημεία πρόσβασης δεν απενεργοποιούν το αίτημα SSID, είναι ενεργό αλλά το πραγματικό όνομά του μεταδίδεται στον αέρα γεγονός που καθιστά το δίκτυο ευάλωτο. Σε ένα ασφαλές δίκτυο το SSID πρέπει να είναι ενεργό και το όνομά του δεν πρέπει να μεταδίδεται στο δίκτυο έτσι ώστε οι χρήστες να πρέπει να αποδείξουν ότι το γνωρίζουν και μετά να μπορούν να αποκτήσουν πρόσβαση μέσω των σημείων πρόσβασης. Το άλλο πρόβλημα είναι ότι μέσω του διακομιστή DHCP κάθε χρήστης θα λάβει αυτόματα διεύθυνση IP και θα μπορεί να εκτελέσει οποιαδήποτε εφαρμογή. Για αυτό το λόγο είναι ευθύνη του μηχανικού του δικτύου να απενεργοποιήσει το DHCP και να θέσει την τιμή του με ασφαλή τρόπο έτσι ώστε μόνο οι εξουσιοδοτημένοι χρήστες να μπορούν να έχουν πρόσβαση στο δίκτυο.

Αν το σημείο πρόσβασης είναι κοντά στον εισβολέα τότε απλά ο εισβολέας μπορεί να κάνει επαναφορά στο σημείο πρόσβασης το οποίο θα έρθει στις προεπιλεγμένες ρυθμίσεις από τις οποίες ο εισβολέας θα επωφεληθεί. Έτσι είναι καθήκον του διαχειριστή ασφαλείας του δικτύου να αλλάξει τις προεπιλεγμένες ρυθμίσεις του δικτύου έτσι ώστε να ενισχυθεί η ασφάλεια των σημείων πρόσβασης.

8.3.1.5 Επιθέσεις αναγνωρίσεων

Αυτή η επίθεση χρησιμοποιείται για τη συλλογή πληροφοριών και την παροχή βάσης για επιθέσεις DOS. Στην αρχή, οι επιθέσεις αναγνώρισης προσπαθούν να πάρουν τις πληροφορίες από ενεργές διευθύνσεις χρησιμοποιώντας την σάρωση ping. Από αυτή ο εισβολέας λαμβάνει πληροφορίες σχετικά με τις ενεργές θύρες στις ενεργές

διευθύνσεις. Ενώ χρησιμοποιεί αυτή την πληροφορία, στέλνει το ερώτημα για το λειτουργικό σύστημα και τις εφαρμογές που τρέχουν στον επιθυμητό κόμβο. Η επίθεση αναγνώρισης αποτελείται από τις 4 παρακάτω διαδικασίες:

- Σάρωση ping
- Σάρωση θύρας
- Ανίχνευση πακέτου
- Ερωτήματα για πληροφορίες του διαδικτύου

Η σάρωση ping είναι μια μέθοδος σάρωσης δικτύου που καθορίζει το εύρος των διευθύνσεων IP που έχουν εκχωρηθεί σε ενεργούς υπολογιστές. Η σάρωση ping είναι μια συλλογή echo αιτημάτων που αποστέλλονται σε πολλαπλούς κόμβους. Αν οποιαδήποτε διεύθυνση στη λίστα είναι ενεργή τότε θα απαντήσει πίσω. Αυτή η μέθοδος είναι παλιά και αργεί να σαρώσει το δίκτυο. Πολλά αιτήματα στέλνονται σε μια σειρά διευθύνσεων για να ανακαλυφθεί πόσοι υπολογιστές με ευπαθή σημεία μπορούν να εντοπιστούν.

Ο σκοπός της σάρωσης θύρας είναι να μπει μέσα στο σύστημα και να αποκτήσει πρόσβαση στο ποιές υπηρεσίες τρέχουν στο δίκτυο. Κάθε υπηρεσία συνδέεται με έναν διακριτό αριθμό θύρας. Επίσης μπορεί μια αυτοματοποιημένη σάρωση των θυρών TCP ή UDP σε έναν υπολογιστή να αποκτήσει τον έλεγχο σε υπηρεσίες που τρέχουν. Η σάρωση θύρας είναι η προτιμώμενη μέθοδος επίθεσης σε ένα δίκτυο και κάνει φανερά τα αδύνατα σημεία του. Στη σάρωση αυτή το μήνυμα αποστέλλεται σε όλες τις θύρες αλλά σε μία κάθε φορά. Εάν οποιαδήποτε θύρα απαντήσει σημαίνει ότι είναι ενεργή και μπορεί να χρησιμοποιηθεί ως τρωτό σημείο.

Ο αναλυτής πακέτων δικτυακής πληροφορίας (packet sniffer) είναι μια εφαρμογή λογισμικού που χρησιμοποιεί μια κάρτα δικτύου σε μια ειδική κατάσταση γνωστή ως promiscuous για να λάβει τα πακέτα δικτύου που στέλνονται μέσω του δικτύου. Ο αναλυτής πακέτων δικτυακής πληροφορίας λειτουργεί πάντα στην ίδια περιοχή όταν το δίκτυο δέχεται επίθεση. Η κατάσταση αυτή είναι ένας τύπος λειτουργίας στην οποία η κάρτα προσαρμογέα δικτύου στέλνει όλα τα δεδομένα και τα πακέτα φωνής σε μια εφαρμογή λογισμικού που αναλαμβάνει την επεξεργασία. Τα δεδομένα που είναι σε μορφή απλού κειμένου δεν είναι κωδικοποιημένα, αν και πολύ λίγες εφαρμογές δικτύου διανέμουν τα πακέτα σε μορφή απλού κειμένου .Όταν τα πακέτα δεν είναι σε κρυπτογραφημένη μορφή, μπορούν να υποβληθούν σε επεξεργασία και να γίνουν κατανοητά από οποιαδήποτε εφαρμογή.

Το να θέτεις κάποια ερώτηση στο διαδίκτυο για τη συλλογή χρήσιμων πληροφοριών σχετικά με την ιστοσελίδα οποιουδήποτε οργανισμού, είναι γνωστό ως DNS ερώτημα. Για τη συλλογή πληροφοριών χρησιμοποιούνται οι αιτήσεις DNS όπως το ποιές διευθύνσεις έχουν ανατεθεί και σε ποιόν τομέα καθώς και ποιός κατέχει τον τομέα. Οι αιτήσεις DNS βοηθούν τις σαρώσεις ping να εντοπίσουν ενεργούς

υπολογιστές σε μια συγκεκριμένη περιοχή. Μετά τη δημιουργία μιας τέτοιας λίστας, τα εργαλεία σάρωσης θύρας μπορούν να αναπτυχθούν ώστε να γνωρίζουν όλες τις υπηρεσίες που εκτελούνται σε υπολογιστές που εντοπίστηκε η σάρωση ping. Οι εισβολείς πάντα παίρνουν ειδοποίηση των ιδιοτήτων όλων των εφαρμογών που εκτελούνται στους υπολογιστές. Για την εξάλειψη των επιθέσεων αναγνώρισης χρησιμοποιούνται τα IPS και IDS.

8.3.1.6 Conversation Sniffing

Το conversation sniffing είναι μια διαδικασία λήψης και κατανόησης των πληροφοριών του δικτύου που ρέουν στο μέσο. Σε δικτυωμένο περιβάλλον όλες οι πληροφορίες περνούν από τις κάρτες δικτύου σε ένα μέσο επικοινωνίας, και μια κεντρική συσκευή είναι υπεύθυνη για τη μετάδοση των πληροφοριών στους πελάτες. Όποτε ο επιτιθέμενος θέλει να εκτελέσει conversation sniffing απλά ξαναρυθμίζει τη κάρτα δικτύου σε promiscuous λειτουργία, δηλαδή τη ίδια λειτουργία μέσω της οποίας η κεντρική συσκευή μεταδίδει τα δεδομένα στο δίκτυο. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν το conversation sniffing με τη βοήθεια των sniffers που διατίθενται ελεύθερα στο διαδίκτυο για να κλέψουν τα μυστικά δεδομένα και να υποκλέψουν τα δεδομένα του δικτύου όπως τη συλλογή των πιστοποιήσεων σύνδεσης των χρηστών, τη διεύθυνση IP του πελάτη, τη διεύθυνση MAC των καρτών δικτύου τα emails και γενικά ότι κινείται στο μέσο.

Η εμπιστευτικότητα είναι ένας σημαντικός παράγοντας για τη μετάδοση δεδομένων και φωνής. Η κίνηση WLAN μπορεί να γίνει αντιληπτή αν η μετάδοση και η κυκλοφορία των μέσων ενημέρωσης δεν έχουν ασφαλιστεί κατάλληλα. Η εμπιστευτικότητα και η ακεραιότητα είναι 2 σημεία κλειδιά στο WLAN. Εμπιστευτικότητα σημαίνει να διασφαλιστεί το απόρρητο των πληροφοριών που ανταλλάσσονται μεταξύ όλων των χρηστών. Η ακεραιότητα αναφέρεται στην πληροφορία που ανταλλάσσεται και δεν πρέπει να παραβιαστεί κατά τη διάρκεια της μετάδοσης. Υπάρχουν πολλές τεχνικές που μπορούν να χρησιμοποιηθούν για να εγγυηθούν την εμπιστευτικότητα και την ακεραιότητα ενός δικτύου WLAN. Το IPSec μπορεί να χρησιμοποιηθεί σε λειτουργία μεταφοράς ή σε tunnel mode για τον έλεγχο ταυτότητας.

8.3.1.7 Επίθεση DHCP

Πολλά αιτήματα στέλνονται στον διακομιστή DHCP κατά τη διάρκεια μιας επίθεσης DHCP. Αυτή η επίθεση αναγκάζει τον διακομιστή να εκδώσει διεύθυνση προς κάθε αίτημα. Ο σκοπός αυτής της επίθεσης είναι να πλαστογραφήσει τις απαντήσεις DHCP. Αφού ληφθούν οι διευθύνσεις από τον διακομιστή DHCP, οι εισβολείς έχουν περισσότερα σημεία να του επιτεθούν και τότε ο διακομιστής δεν θα μπορεί να ανταποκριθεί στα αιτήματα των χρηστών. Αυτός ο τύπος επίθεσης δημιουργείται όπως η DOS και ο « man on the middle». Για την αποφυγή τέτοιου είδους επίθεσης, συνίσταται η χρήση στατικών διευθύνσεων IP σε δίκτυο WLAN.

8.3.2 Φυσικές επιθέσεις και τεχνικές μετριασμού τους

Μια φυσική επίθεση πάντα σχετίζεται με το λογισμικό και τη διαμόρφωση του δικτύου. Σε αυτό το είδος επίθεσης ο στόχος του εισβολέα είναι να διακόψει ή να μειώσει την απόδοση του δικτύου παρά να ψάξει σε ευαίσθητα δεδομένα και να κάνει κάποιες αλλαγές σε αυτά. Αυτό το είδος επίθεσης μπορεί να δημιουργήσει λιγότερα προβλήματα για οποιοδήποτε οργανισμό, για το hardware και όχι για την μυστική πληροφορία που υποκλέπτεται. Πρέπει να σημειωθεί ότι αυτό το είδος επίθεσης πάντα θα ανοίγει τον δρόμο για μια λογική επίθεση. Κάποιες φυσικές επιθέσεις ορίζονται παρακάτω με τις τεχνικές μετριασμού τους.

- Πλαστά (rogue) σημεία πρόσβασης
- Φυσική τοποθέτηση των σημείων πρόσβασης
- Κάλυψη των σημείων πρόσβασης
- Επίθεση ανεπιθύμητης αλληλογραφίας(spam attack)

8.3.2.1 Πλαστά σημεία πρόσβασης

Ο κύριος σκοπός αυτού του τύπου επίθεσης είναι να αποκτήσει πρόσβαση στους πόρους άλλων χρηστών. Μόλις ο εισβολέας πετύχει να αποκτήσει πρόσβαση στους πόρους, τότε μπορεί εύκολα να προσθέσει οποιεσδήποτε εφαρμογές που θα κάνουν το ρυθμό δεδομένων επιτυχή. Για την απαλλαγή αυτού του είδους επίθεσης, οι διαχειριστές του δικτύου χρησιμοποιούν μια απλή τεχνική γνωστή ως “μηχανισμό κλειδώματος”. Με την εγκατάσταση αυτής της εφαρμογής ο διαχειριστής του δικτύου θα λάβει τα αρχεία καταγραφής όποτε ο εισβολέας προσπαθήσει να προσθέσει κάποια εφαρμογή. Η μεταφορά των δεδομένων θα απορριφθεί όταν οποιοσδήποτε χρήστης αποκτήσει παράνομη πρόσβαση στο δίκτυο. Ο εισβολέας μπλοκάρεται αυτόματα όταν πραγματοποιηθούν παραπάνω από 3 απόπειρες.

8.3.2.2 Φυσική τοποθέτηση των σημείων πρόσβασης

Ο τόπος εγκατάστασης ενός σημείου πρόσβασης είναι σημαντικός παράγοντας, εάν τοποθετηθεί το σημείο πρόσβασης εσφαλμένα θα οδηγήσει σε φυσικές επιθέσεις. Το σημείο πρόσβασης μπορεί εύκολα να κλείσει από τους επιτιθέμενους και μετά από αυτή την ενέργεια όλη η διαμόρφωση θα χαθεί και το σημείο θα τεθεί σε προεπιλεγμένη ρύθμιση κάτι το οποίο δεν είναι ασφαλές. Έτσι είναι σημαντικό για τον μηχανικό ασφάλειας δικτύου να διαλέξει προσεκτικά την τοποθεσία των σημείων πρόσβασης.

8.3.2.3 Κάλυψη των σημείων πρόσβασης

Η κύρια διαφορά μεταξύ ενός ενσύρματου και ασύρματου LAN είναι ότι το δεύτερο εξαρτάται από τα σήματα RF. Τα σήματα αποστέλλονται από τα σημεία πρόσβασης στο εξωτερικό του κτιρίου όπου είναι τοποθετημένα, επιτρέποντας στους χρήστες που δεν είναι στο κτίριο με τη φυσική τους παρουσία να αποκτήσου πρόσβαση στο

δίκτυο. Για να εντοπίσουν ένα WLAN, οι επιτιθέμενοι χρησιμοποιούν διαφορετικά εργαλεία και μπορούν να επικοινωνήσουν ακόμα και ενώ οδηγούν. Στο RF δεν υπάρχει κανένα καθορισμένο όριο για το σήμα που εκπέμπεται. Οι επιτιθέμενοι που βρίσκονται έξω μπορούν να εξαπολύσουν επιθέσεις στο WLAN. Αυτό το είδος επίθεσης είναι γνωστό ως war driving. Οι κακόβουλοι χρήστες επίσης ερευνούν κτίρια για να δείξουν ότι τα σήματα που μεταδίδονται από το σημείο πρόσβασης και το WLAN μέσα σε αυτό μπορούν να προσεγγιστούν εύκολα. Κάποιες φορές προτιμάται η πρόσβαση σε κάποιο δημόσιο WLAN που καλείται hot spot. Είναι σημαντικό να γνωρίζουμε ότι η παραβίαση της ασφάλειας ενός hot spot σημαίνει ότι είναι εύκολο να παραβιαστεί η ασφάλεια ενός ενσύρματου WLAN που είναι συνδεδεμένο με το hot spot.

8.3.2.4 Επίθεση ανεπιθύμητης αλληλογραφίας(spam attack)

Τα μηνύματα spam δημιουργούν προβλήματα στο WLAN, όπως τα spam emails που καταναλώνουν εύρος ζώνης. Αν υπάρχει spam στο δίκτυο WLAN, αυξάνεται η καθυστέρηση κατά τη διάρκεια ταυτοποίησης των χρηστών καθώς και στη μετάδοση δεδομένων. Ο σκοπός του spam είναι να κατακλύσουν με μηνύματα όλο το δίκτυο όπως τα παραδοσιακά emails. Η επίθεση αυτή καταναλώνει εύρος ζώνης και για την αποφυγή της συνίσταται να χρησιμοποιείται λογισμικό anti-spam.

8.4 Ασφάλεια στο Ασύρματο Δίκτυο

Αυτό το κεφάλαιο περιγράφει τις διάφορες λύσεις ασφαλείας για το πρότυπο IEEE 802.11 όπως τα WEP, WPA και WPA2 χρησιμοποιώντας 802.1X και διακομιστή RADIUS με την αρχιτεκτονική τους, τα μειονεκτήματα και την εξήγηση των διαφορετικών επιθέσεων σε αυτές τις λύσεις ασφαλείας με λεπτομέρειες, καθώς και ποιές ξεπερνάνε η μία την άλλη και ποιά θεωρείται καλύτερη σε κάθε περιβάλλον

8.4.1 WEP

Το WEP είναι μια πρώτη τεχνική ασφαλείας που χρησιμοποιείται στα πρότυπα IEEE 802.11. Ο κύριος σκοπός της χρήσης της είναι να παρέχει ασφάλεια στο WLAN καθώς και στο ενσύρματο LAN. Συμβάλλει στο να καταστεί ασφαλής η επικοινωνία και παρέχει μυστικό σύστημα ελέγχου ταυτότητας μεταξύ του σημείου πρόσβασης και του τελικού χρήστη που θα αποκτήσει πρόσβαση στο WLAN. Βασικά το WEP εφαρμόζεται σε αρχικά δίκτυα WiFi έτσι ώστε ο χρήστης να μην μπορεί να αποκτήσει πρόσβαση χωρίς το σωστό κλειδί. Το WEP χρησιμοποιεί κρυπτογράφηση συμμετρικού κλειδιού, όπου το μήκος του κλειδιού κρυπτογράφησης κυμαίνεται από τα 64 στα 128 bit. Συνήθως το ίδιο κρυπτογραφημένο κλειδί χρησιμοποιείται για όλους τους κόμβους του δικτύου και προωθείται χειροκίνητα σε κάθε κόμβο, δηλαδή το WEP δεν μπορεί να παράσχει λειτουργία διαχείρισης κλειδιού. Το WEP χρησιμοποιεί την κοινή μέθοδο ελέγχου ταυτότητας κλειδιού όπου κάθε χρήστης χρειάζεται 2 πράγματα για να αποκτήσει πρόσβαση στο WLAN, το ένα είναι το SSID και το δεύτερο είναι το κλειδί WEP που παράγεται από το σημείο πρόσβασης. Το πρότυπο IEEE 802.11 καθορίζει 3 διαφορετικές παραμέτρους για το WEP όπως τον

έλεγχο πρόσβασης, το απόρρητο των δεδομένων και την ακεραιότητα των δεδομένων.

8.4.1.1 Αρχιτεκτονική WEP

Το πρότυπο IEEE 802.11 χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4 για το WEP έτσι ώστε να παρέχει ιδιωτικότητα για το WiFi δίκτυο επειδή είναι εύκολο να εφαρμοστεί στο λογισμικό και πολύ φθηνό σε σχέση με οποιοδήποτε άλλο αλγόριθμο κρυπτογράφησης. Το RC4 θεωρείται ένας λογικός αλγόριθμος αλλά σήμερα δεν χρησιμοποιείται. Ο ασφαλής και πρότυπος τρόπος για να είναι ασφαλής η ακεραιότητα είναι να προστεθεί κάποιος κώδικας ελέγχου γνησιότητας μηνύματος σε κάθε τμήμα των δεδομένων προτού μεταδοθεί προς το ασύρματο μέσο. Το WEP χρησιμοποιεί 32 bit κυκλικού κώδικα (CRC-32) ως αλγόριθμο ακεραιότητας που παράγεται από την πλευρά της εκπομπής. Παράγεται για κάθε πλαίσιο δεδομένων που πρόκειται να μεταδοθεί εκτελώντας κάποιους πολυωνυμικούς υπολογισμούς και έπειτα το άθροισμα ελέγχου προστίθεται σε κάθε πλαίσιο δεδομένων. Στην πλευρά του δέκτη πραγματοποιούνται παρόμοιοι πολυωνυμικοί υπολογισμοί, και αν το άθροισμα ελέγχου που υπολογίζεται στις 2 πλευρές είναι το ίδιο, τότε θεωρείται ότι τα δεδομένα είναι ασφαλή, αλλιώς θεωρείται ότι είναι αλλοιωμένα. Το CRC-32 θεωρείται ότι είναι θεμελιώδης προσέγγιση και πολύ εύκολο να υλοποιηθεί. Το WEP κρυπτογραφούσε την πληροφορία στη πλευρά της μετάδοσης και αποκρυπτογραφούσε τα δεδομένα στη πλευρά της λήψης.

Η κρυπτογράφηση πληροφοριών στη πλευρά της αποστολής

Υπάρχουν 4 βήματα που βοηθούν να καθοριστεί πώς λειτουργεί το WEP για να κρυπτογραφήσει την πληροφορία πριν τη μεταδώσει στο μέσο επικοινωνίας που είναι ο αέρας.

1. Το μυστικό PSK που έχει μήκος 40 bit κατακερματίζεται με ένα αρχικοποιημένο διάνυσμα μήκους 24 bit.

2. Δημιουργείται ένα PRNG ως αποτέλεσμα των ανάμικτων IV και ένα προμοιρασμένο κλειδί για να δημιουργήσει ένα νέο διαδοχικό κλειδί.

3. Το απλό κείμενο και το ICV κατακερματίζονται στον μίκτη όπου ένα αντίγραφο του απλού κειμένου μεταφέρεται στον αλγόριθμο ακεραιότητας που δημιούργησε το ICV.

4. Το διαδοχικό κλειδί και το αποτέλεσμα του κατακερματισμένου απλού κειμένου και του ICV μεταφέρονται στον αλγόριθμο RC4 ο οποίος εκτελεί τη λειτουργία XOR για να δώσει το κρυπτογραφημένο αποτέλεσμα.

Στο τέλος το κρυπτογραφημένο μήνυμα λαμβάνεται, πρώτα προσθέτοντας το IV στην αρχή του κρυπτογραφημένου κειμένου. Έτσι, το κρυπτογραφημένο μήνυμα είναι έτοιμο να σταλθεί μέσω του αέρα.

Η αποκρυπτογράφηση των πληροφοριών στη πλευρά της λήψης

Υπάρχουν 5 βήματα για να καθοριστεί πώς λειτούργει το WEP για να αποκρυπτογραφήσει τις πληροφορίες ή να διαχωρίσει το IV και το κρυπτογραφημένο κείμενο το ένα από το άλλο στη πλευρά της λήψης.

1. Το κοινόχρηστο κλειδί μήκους 40 bit κατακερματίζεται με το IV που έχει μήκος 24 bit και διατίθεται σε κρυπτογραφημένη πληροφορία για να δημιουργήσει ένα PRNG που θα σχηματίσει ένα διαδοχικό κλειδί.

2. Το κρυπτογραφημένο κείμενο που διατίθεται σε κρυπτογραφημένο μήνυμα και το διαδοχικό κλειδί που έχει ήδη δημιουργηθεί, μεταφέρονται στον αλγόριθμο RC4 που εκτελεί τη λειτουργία XOR και στα 2 για να δημιουργήσουν ένα απλό κείμενο.

3. Το ICV διαχωρίζεται από το απλό κείμενο.

4. Το απλό κείμενο μεταφέρεται στον αλγόριθμο ακεραιότητας για να δημιουργήσει ένα νέο ICV.

5. Το νέο ICV συγκρίνεται με το αρχικό και αν και τα 2 ταιριάζουν τότε τα δεδομένα είναι ασφαλή, αλλιώς μεταβάλλονται.

Με αυτό τον τρόπο το μήνυμα αποκρυπτογραφείται επιτυχώς και το πρωτότυπο μήνυμα είναι διαθέσιμο στην πλευρά του παραλήπτη.

8.4.1.2 Οι ευπάθειες στο WEP

Το WEP θεωρείται ασθενής τεχνική ασφαλείας για το WLAN σήμερα. Παρακάτω είναι μερικοί κύριοι λόγοι για τους οποίους το WEP δεν μπορεί να παράσχει ασφάλεια στο WLAN και έτσι κάθε στοιχείο του WEP είναι πολύ αδύναμο.

- Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4 για έλεγχο ταυτότητας και ιδιωτικότητα. Το πρόβλημα δεν είναι με τον αλγόριθμο RC4 αν και είναι καλός αλγόριθμος κρυπτογράφησης αλλά ότι δεν εφαρμόστηκε σωστά για τη τεχνική WEP. Σε κάθε στάδιο της RC4 ορίζεται ξεκάθαρα να μη χρησιμοποιείται το ίδιο κλειδί παραπάνω από μια φορά ανεξάρτητα από το ποιό είναι το ωφέλιμο φορτίο. Το RC4 απλά εκτελεί την λειτουργία XOR για τα δεδομένα.

- Χρησιμοποιεί αρχικοποιημένο διάνυσμα (IV) μήκους 24 bit που προστίθεται με το πακέτο που είναι έτοιμο να μεταδοθεί στον αέρα. Υπάρχουν 2 λύσεις διαθέσιμες για να απαλλαγούμε από αυτό το μειονέκτημα όπως είναι η χρήση μεγαλύτερων IVs και κάποιος ασφαλής ανάμικτος αλγόριθμος στη θέση του CRC-32 για ακεραιότητα.

- Άλλο πρόβλημα με τον αλγόριθμο RC4 είναι η προσθήκη του IV με το προμοιρασμένο κλειδί. Αν υπάρχει πολλή κίνηση διαθέσιμη στα ασύρματα δίκτυα, υπάρχει η πιθανότητα για πολλά πακέτα να χαθούν κατά τη διάρκεια της επικοινωνίας και να πρέπει να αναμεταδοθούν. Έτσι, στο WEP, για κάθε

επαναποστολή του πακέτου αλλάζει το IV το οποίο έχει μόνο 224 θέσεις για κλειδιά.

- Επομένως η προσθήκη του IV με το κλειδί WEP είναι το κύριο μειονέκτημα στο σχεδιασμό. Αν το WEP χρησιμοποιεί κλειδί μήκους 40 bit τότε θα χρειαστεί μεγαλύτερη προστασία από επιθέσεις σε σχέση με ένα κλειδί WEP μήκους 128 bit. Έτσι και τα 2 είναι πολύ αδύναμα και ανίκανα να προσφέρουν προστασία σε δίκτυα WiFi.
- Χρησιμοποιεί αδύναμο αλγόριθμο ελέγχου ταυτότητας.
- Χρησιμοποιεί αδύναμη μέθοδο ενθυλάκωσης δεδομένων.
- Το μέγεθος του IV είναι πολύ μικρό(24 bit).
- Η χρήση ακατάλληλου αλγορίθμου ακεραιότητας(πχ CRC-32).
- Αδυναμία αποτροπής από την επανάληψη προστασίας.
- Έλλειψη αμοιβαίας επαλήθευσης ταυτότητας και διαχείρισης κλειδιού.

Από τις προηγούμενες μελέτες και την τωρινή έρευνα είναι αποδεδειγμένο ότι το WEP απέτυχε να παρέχει προστασία στο WLAN.

8.4.1.3 Επίθεση στο WEP

Το WEP είναι ένα είδος πρωτοκόλλου ασφαλείας που βασίζεται στον κρυπτογραφημένο αλγόριθμο RC4. Ο σκοπός του είναι να παρέχει προστασία στο WLAN παρόμοια με την προστασία που παρέχεται στο ενσύρματο LAN. Υπάρχουν κάποια μειονεκτήματα στο WEP όπως το μικρό κλειδί κρυπτογράφησης RC4 και η αξιοποίηση μικρού IV. Άλλο μειονέκτημα είναι η χρήση της διαδικασίας XOR για το κλειδί κρυπτογράφησης με απλό κείμενο έτσι ώστε να δημιουργηθεί το κρυπτογραφημένο κείμενο. Τόσο η διεύθυνση MAC όσο και το IV στέλνονται με σαφή μορφή απλού κειμένου. Τα μυστικά κλειδιά μοιράζονται μεταξύ των κόμβων που είναι οι κύρια ανησυχία ασφαλείας. Τα δεδομένα που κρυπτογραφούνται μέσω του WEP μπορούν εύκολα να γίνουν προσβάσιμα στον εισβολέα μέσω διαφορετικών εργαλείων όπως τα AirSnort και WEPCrack.

Υπάρχουν τόσα πολλά προβλήματα με τις λύσεις ασφαλείας WEP, που επίσης επηρεάζονται από τη κακή διαχείριση κλειδιών στο δίκτυο με αποτέλεσμα τα κλειδιά που αποθηκεύονται στη συσκευή να παραμένουν αμετάβλητα καθ' όλη τη σύνοδο της επικοινωνίας. Κατά τη διάρκεια αυτής της περιόδου, αν κάποιος από τον εξοπλισμό κλαπεί ή χαθεί, ο εισβολέας μπορεί να χρησιμοποιήσει τα αποθηκευμένα κλειδιά στον χαμένο εξοπλισμό, όχι μόνο να επηρεάσει αυτό τον εξοπλισμό αλλά και αυτόν που μοιράζεται κοινά κλειδιά. Για να μετριαστεί αυτό το πρόβλημα, η λύση "δυναμικής διαχείρισης κλειδιού" θα βοηθήσει πολύ κάνοντας αυτά τα κλειδιά WEP να μην

πέσουν σε λάθος χέρια αλλά αυτή η διαδικασία θα αυξήσει την πολυπλοκότητα του δικτύου.

Το WEP υποφέρει από τρωτά σημεία από όταν αναπτύχθηκε και αντιμετώπισε πολλές επιθέσεις από την αρχή αλλά όλες έμοιαζαν αρκετά ανέφικτες επομένως οι προμηθευτές αποφάσισαν να μην επενδύσουν σε νέα λύση ασφαλείας. Σχεδίασαν να δώσουν λύσεις μετριασμού του προβλήματος αλλά λόγω της παρόδου του χρόνου οι επιθέσεις σταδιακά αναπτύχθηκαν και έγιναν όλο και πιο σοβαρές για το WEP. Αυτή η ενότητα περιγράφει κάποιες επιθέσεις στο WEP και ποια λύση παρέχουν οι προμηθευτές.

1. Επίθεση brute force

Μία επίθεση brute force περιλαμβάνει την αποστολή ενός τεράστιου αριθμού αλφαριθμητικών συνδυασμών και εξαντλητική χρήση της μεθόδου δοκιμής και λάθους, με σκοπό την εύρεση νόμιμα πιστοποιητικά αυθεντικοποίησης. Ο αντικειμενικός στόχος αυτής της χρονοβόρου διαδικασίας είναι η απόκτηση πρόσβασης στο σύστημα στόχο. Οι επιθέσεις αυτού του τύπου μπορούν να υπερφορτώσουν ένα σύστημα και να το αναγκάσουν να μην ανταποκρίνεται σε αιτήματα. Επιπλέον, αν εφαρμόζεται κλείδωμα λογαριασμών, οι επιθέσεις brute force μπορούν να κλείσουν τους λογαριασμούς εξουσιοδοτημένων χρηστών. (30)

Η επίθεση brute force θεωρείται η πιο "ανόητη" επίθεση που δοκιμάζει όλα τα πιθανά κλειδιά με χειροκίνητο τρόπο έτσι ώστε να βρει το σωστό. Ένα ενιαίο σύγχρονο μηχάνημα θα βοηθήσει να βρεθεί το κλειδί σε χρονικό διάστημα μικρότερο του μήνα με συνεχή έρευνα, ειδικά όταν η εργασία είναι μοιρασμένη(η εύρεση του κλειδιού δεν είναι απίθανη μέσω επίθεσης brute force σε κλειδί WEP μήκους 40 bit). Κάποια από τα εργαλεία έχουν τη δυνατότητα να αλλάξουν την ανθρώπινη αναγνώσιμη συνθηματική φράση σε κλειδιά WEP. Νέα εργαλεία έχουν την επιλογή να αλλάξουν τη συνθηματική φράση σε δεκαεξαδικά κλειδιά με τη βοήθεια των κωδικών ASCII των αλφαριθμητικών χαρακτήρων. Αυτό το είδος μη-πρότυπων μεθόδων ελαχιστοποίησε τις δυσκολίες για πολλές από τις επιθέσεις brute force. Προφανώς ένας τυποποιημένος αλγόριθμος θα βοηθούσε να απαλλαγούμε από την εύκολη επίθεση brute force αναμιγνύοντας την συνθηματική φράση σε ένα κλειδί WEP. Διαφορετικοί προμηθευτές παρουσίασαν ένα κλειδί WEP μήκους 104 bit που θεωρείται ότι είναι το πιο εντυπωσιακό για τις επιθέσεις brute force.

2. Επίθεση εναντίον της επαναχρησιμοποίησης κλειδιού

Η ασφάλεια στους αλγορίθμους είναι τελείως ανεξάρτητη από το κλειδί του, που ορίζεται από την Κρυπτανάλυση στην εντροπία WEP. Τον πρώτο καιρό φαινόταν αχρείαστο να επεκταθεί το μέγεθος του κλειδιού για επιπλέον προστασία στο WEP. Αν ο επιτιθέμενος ανακτήσει επιτυχώς το key stream τότε σίγουρα μπορεί να αποκρυπτογραφήσει τα δεδομένα που συνδέονται με αυτό. Ο πιο λογικός μηχανισμός ανακαλύφθηκε, ο οποίος είναι βασισμένος στην ενεργοποίηση του ελέγχου ταυτότητας προμοιρασμένου κλειδιού. Ο κύριος σκοπός αυτού του μηχανισμού είναι

να περιορίσει τη μη εξουσιοδοτημένη πρόσβαση στο δίκτυο. Σε αυτή τη διαδικασία, ο πρώτος πιστοποιημένος χρήστης(authenticator) στέλνει ένα σαφές κείμενο πρόκλησης (clear text challenge) στον αιτούντα (supplicant), γνωστό ως ομότιμη πιστοποίηση (authentication peer). Ο αιτώντας επικυρώνεται και απαντάει με το κρυπτογραφημένο μήνυμα της πρόκλησης. Αν ο επιτιθέμενος κατασκοπεύσει με επιτυχία αυτή την επικοινωνία, τότε απλά μπορεί να κάνει XOR του κρυπτογραφημένου κειμένου και ταίριασμα του απλού κειμένου ώστε να λάβει το key stream.

Αυτή η επίθεση είναι αναγνωρισμένη από το πρότυπο IEEE 802.11 και αποθαρρύνει τους πελάτες από το να επαναλαμβάνουν τα ίδια IVs στη διαδικασία επικοινωνίας. Μετά από αυτή την επίθεση τα συστήματα πιστοποίησης αποθαρρύνονται και μας παρουσιάζεται η απόκρυψη SSID και οι μηχανισμοί φιλτραρίσματος των διευθύνσεων MAC. Έτσι, το αίτημα συνεργασίας και οι μηχανισμοί της διεύθυνσης MAC έχουν και τα 2 μειονεκτήματα αλλά εμπεριέχουν λίγη σημασία στο σύστημα ελέγχου ταυτότητας.

3. Επιθέσεις IV

Οι τωρινές μελέτες απέδειξαν ότι το κλειδί μπορεί να επαναϋπολογιστεί από τον επιτιθέμενο. Αυτό το είδος επίθεσης απαιτεί τη συλλογή περίπου 1000000 στην οποία κάποια από τα πακέτα χρησιμοποίησαν IVs. Στην πραγματικότητα, αυτές οι ιδιότητες έχουν ήδη καθοριστεί στον αλγόριθμο RC4 4 χρόνια πριν γνωρίσουμε το WEP. Οι απλοί ανειδίκευτοι επιτιθέμενοι μπορούν να δώσουν και να λάβουν πληροφορίες σε ένα δίκτυο, και συλλέγοντας ένα τεράστιο αριθμό IVs κάποιος μπορεί να υπολογίσει εύκολο το ακριβές κλειδί. Μόνο ένα IV θα βοηθήσει να βρεθεί το σωστό κλειδί σε ποσοστό 5% κάθε φορά. Έτσι αποδεικνύεται ότι τα IVs θεωρούνται ως η πιο σημαντική απειλή στα WEP. Εκτός από αυτό, αυτή η επίθεση μπορεί αν μετριαστεί μόνο σε συγκεκριμένες περιπτώσεις μετά τη συλλογή μεγαλύτερου αριθμού IVs, το οποίο θα μπορούσε να χρειαστεί αρκετές μέρες για να βρεθεί το σωστό κλειδί WEP.

4. Σύγχρονες Επιθέσεις

Οι παραπάνω επιθέσεις αντιμετώπισαν 2 σημαντικά προβλήματα στο παρελθόν. Πρώτον το πώς θα μειωθεί ο χρόνος για να εντοπιστεί το ακριβές κλειδί στις επιθέσεις IV και δεύτερον πώς να επιτευχθεί αξιόπιστα το key stream στις επιθέσεις εναντίον της επαναχρησιμοποίησης κλειδιού. Και τα 2 προβλήματα λύθηκαν τώρα. Για το πρώτο πρόβλημα αποδείχτηκε από τις τωρινές μελέτες ότι κάποιος μπορεί εύκολα να ανακτήσει ένα byte ενός key stream πιάνοντας το μέγιστο των 256 πακέτων. Για το δεύτερο πρόβλημα επίσης αποδείχτηκε ότι για τη μείωση της χρονικής περιόδου σε μια ασθενή επίθεση IV, αν οποιοδήποτε πακέτο αποκτήσει μια απάντηση που επαναλαμβάνεται, μετά η κυκλοφορία παράγεται αυτόματα στο δίκτυο και ο επιτιθέμενος δεν θα περιμένει να πιάσει χειροκίνητα τα δεδομένα αλλά μπορεί να εντοπίσει ενεργά τη κίνηση των δεδομένων που χρησιμοποιούν IVs. Σε αυτό το στάδιο αποδεικνύεται ότι το WEP απέτυχε πλήρως να εξασφαλίσει προστασία. Ένας

επιτιθέμενος μπορεί να σπάσει την ασφάλεια του δικτύου μέσα σε λίγα λεπτά χρησιμοποιώντας αυτά τα τρωτά σημεία.

8.4.2 WPA

Η συμμαχία WiFi (WFA) παρέχει μια νέα τεχνική το έτος 2002 για την ασύρματη ασφάλεια που είναι WPA ώστε να λυθούν τα προβλήματα που ήταν ορατά κατά τα αρχικά στάδια της λύσης ασφαλείας WEP. Το WPA έχει πολλά πλεονεκτήματα σε σχέση με το WEP που περιγράφονται παρακάτω:

- Δυνατή και διαλειτουργική με αντικατάσταση των κενών ασφαλείας του WEP.
- Βελτιωμένη κρυπτογράφηση δεδομένων, επειδή το WEP έχει πολύ αδύναμη μέθοδο κρυπτογράφησης δεδομένων.
- Δυνατή ταυτότητα χρήστη που δεν είναι διαθέσιμη στο WEP.
- Υπάρχουν πολλές επιθέσεις που σχετίζονται με το στατικό κλειδί, για αυτό το WPA ελαχιστοποιεί το διαμοιρασμένο μυστικό κλειδί ανάλογα με τη μετάδοση του πλαισίου.
- Το WPA χρησιμοποιεί μια ασφαλή και σύνθετη συνάρτηση κατακερματισμού κρυπτογράφησης που λειτουργεί μοιράζονται το διαμοιρασμένο κλειδί ανάμεσα στο χρήστη και το σημείο πρόσβασης.
- Η χρήση του αλγορίθμου RC4 με σωστό τρόπο και η παροχή γρήγορης μεταφοράς δεδομένων προτού κάποιος μπορέσει να τα αποκρυπτογραφήσει.
- Το WPA αποφεύγει τις επαναλήψεις με τη χρήση μεγαλύτερων IVs.

Το WPA είναι μια έξυπνη λύση ασφαλείας σε σχέση με το WEP και λειτουργεί έτσι ώστε να μεταφέρει το κλειδί WEP χρησιμοποιώντας μηχανισμό κρυπτογράφησης TKIP όσο το δυνατόν γρηγορότερα πριν κάποιος αποκρυπτογραφήσει το κλειδί. Όταν αυτή η τεχνική έχει ρυθμιστεί σωστά τότε αυτομάτως όλα τα εμπιστευτικά δεδομένα είναι διαθέσιμα σε όλους τους εξουσιοδοτημένους χρήστες που είναι συνδεδεμένοι στο δίκτυο WiFi. Από την άλλη πλευρά, όλα τα μέρη που χρησιμοποιούνται στην WPA θεωρούνται υποσύνολο της επέκτασης 802.11i και όλα τα μέρη του WPA είναι συμβατά με συσκευές 802.11i. Δύο φάσεις του WPA είναι:

- Επιχειρηματικές/εμπορικές WPA
- Προσωπικές/WPA-PSK(προμοιρασμένο κλειδί) WPA

Στην επιχειρηματική WPA,η κεντρική συνιστώσα του είναι γνωστή ως διακομιστής RADIUS, ο οποίος είναι υπεύθυνος για τον έλεγχο ταυτότητας, την αδειοδότηση και την ευθύνη των χρηστών με το σημείο πρόσβασης.

Στο προσωπικό δίκτυο WPA δεν υπάρχουν έννοιες του RADIUS. Λειτουργεί με προμοιρασμένο κλειδί και οι χρήστες χρειάζονται 2 πράγματα για να αποκτήσουν πρόσβαση στο δίκτυο τα οποία είναι το SSID του δικτύου και το κλειδί WPA που παράγεται από το σημείο πρόσβασης.

8.4.2.1 Πρωτόκολλο ακεραιότητας προσωρινού κλειδιού

Νέες μέθοδοι κρυπτογράφησης δεδομένων και ακεραιότητας αναπτύχθηκαν από το 802.11i όπως το TKIP και το CCMP,επειδή το WEP έχει πολλά ελαττώματα. Το TKIP έχει 2 βασικούς στόχους, πρώτα να ξεφορτωθεί τα προβλήματα που είναι διαθέσιμα με το WEP και δεύτερον να λειτουργεί ως κληρονομικό hardware, διότι σχεδόν όλος ο αλγόριθμος κρυπτογράφησης του WEP υλοποιείται στο hardware. Έτσι από αυτή την άποψη παρατηρείται ότι το TKIP θα συνδεθεί με τη βασική δομή του WEP, γνωρίζοντας το αρχικοποιημένο διάνυσμα, την κρυπτογράφηση RC4 και το διάνυσμα ελέγχου της ακεραιότητας. Επίσης στην TKIP περιλαμβάνονται κάποια ισχυρότερα συστήματα κρυπτογράφησης έτσι ώστε ο τεράστιος αριθμός των παλιών καρτών διασύνδεσης δικτύου και των σημείων πρόσβασης που χρησιμοποιούνται στο δίκτυο δεν θα είναι απόλυτος.

Βασικά η TKIP είναι κρυπταλγοριθμική σουίτα γνωστή ως ένας ασφαλής αλγόριθμος κρυπτογράφησης σε σχέση με τον αλγόριθμο κρυπτογράφησης WEP. Συνδυάζει τον αλγόριθμο ανάμιξης και ένα μετρητή πακέτων και εκτελεί τη λειτουργία με τέτοιο τρόπο ώστε να παρέχει προστασία στα κλειδιά κρυπτογράφησης. Το TKIP χρησιμοποιεί το Michael ως αλγόριθμο ακεραιότητας, γνωστό αλγόριθμο ελέγχου ακεραιότητας μηνύματος (MIC). Το TKIR θα δουλέψει μαζί με το MIC και τον μετρητή πακέτων ώστε να εμποδίσει την καθυστέρηση πακέτων και την αλλοίωση των μηνυμάτων μεταξύ του μέσου. Το TKIP και ο Michael θα δουλέψουν μαζί σε οποιοδήποτε τύπο δικτύου χωρίς να απαιτούν αλλαγές στα εξαρτήματα του hardware. Το TKIP παρέχει τη καλύτερη λύση και προτείνει τη χρήση διαφορετικών βασικών κλειδιών WEP για κάθε πακέτο ώστε να λύσει το πρόβλημα στην κρυπτογράφηση WEP (πχ η επαναχρησιμοποίηση του κλειδιού RC4 περισσότερες από 1 φορά και η χρήση κάποιων αδύναμων κλειδιών RC4).

Το TKIP κυρίως εστιάζει σε 3 βασικά πρωτόκολλα:

- Έναν αλγόριθμο ελέγχου ακεραιότητας μηνύματος(MIC) όπως πχ ο Michael
- Έναν αλγόριθμο ανάμιξης κλειδιών
- Επέκταση του διανύσματος αρχικοποίησης ανάλογα με το μέγεθος

Ο αλγόριθμος κρυπτογράφησης TKIP αποφεύγει το πρόβλημα που συναντάται στο WEP (πχ δημιουργεί ξεχωριστό κλειδί για κάθε πακέτο παρά μόνο ένα κλειδί για όλα τα πακέτα όπως ισχύει στην τεχνική WEP. Ο αλγόριθμος κατακερματισμού αποφεύγει την αλλοίωση των πακέτων στο μέσο. Επίσης το TKIP λύνει το μειονέκτημα στα IVs, αυξάνοντας το μέγεθος του IV που θα βοηθήσει να λυθούν τα

προβλήματα χρησιμοποιώντας μεγαλύτερο μετρητή πακέτου και αποφεύγοντας την προστασία της επανάληψης. Ο σκοπός της χρήσης του μετρητή πακέτου είναι να μην χρησιμοποιούνται αδύναμα κλειδιά RC4. Με όλη αυτή τη μέθοδο το TKIP μπορεί να λύσει τα προβλήματα του WEP σε κάποιο βαθμό.

8.4.2.2 Αρχιτεκτονική του WPA

Η νέα τεχνική ασφαλείας που αναπτύχθηκε μετά το WEP είναι η WPA. Ο κύριος στόχος της WPA είναι να παρέχει μια πιο σύνθετη μέθοδο κρυπτογράφησης και ελέγχου ταυτότητας χρησιμοποιώντας το TKIP με τη βοήθεια του MIC. Ο σκοπός του MIC είναι να εμποδίσει τις επιθέσεις από την «αναδίπλωση bit» γνωστή και ως αλλοίωση του μηνύματος που μπορεί αν επιτευχθεί εύκολα με την τεχνική κατακερματισμού του WEP.

Υπάρχουν 5 βασικά βήματα για να καθοριστεί πως λειτουργεί το WPA ώστε να κρυπτογραφήσει τα δεδομένα χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης TKIP με τη βοήθεια της μεθόδου ακεραιότητας MIC.

1. Τρια πράγματα συνδυάζονται στην πρώτη φάση για να δημιουργηθεί το TKTA στη πλευρά του πομπού του TKIP που είναι το IV, προσωρινό κλειδί και διεύθυνση MAC του NIC. Για να ξεφορτωθούμε τις επιθέσεις επανάληψης, ο πρώτος πομπός TKIP χρησιμοποιεί TSC που έχει μήκος 48 bits και επίσης χρησιμεύει ως IV. Το TSC είναι συνδυασμός 2 πεδίων δηλαδή του TH και του TL. Τα TSC0 και TSC1 ανήκουν στο TL ενώ τα TSC2, TSC3, TSC4 και TSC5 ανήκουν στο TH. Δεύτερον, ο TKIP χρησιμοποιεί ένα προσωρινό κλειδί μήκους 128 bits που κατανέμεται μεταξύ του χρήστη και του σημείου πρόσβασης. Τρίτον, το TKIP χρησιμοποιεί τη διεύθυνση μεταφραστή της κάρτας διασύνδεσης δικτύου που έχει μήκος 48 bit.

2. Το παραγόμενο προσωρινό κλειδί για τη διεύθυνση μεταφραστή (TKTA) έχει μήκος 80 bit και το TL μεταφέρεται στη φάση 2 ώστε να παράγει ένα ξεχωριστό κλειδί πακέτου για κάθε πακέτο μήκους 128 bits. Ο σκοπός χρήσης του TL εδώ είναι η αποφυγή χρήσης αδύναμων κλειδιών.

3. Η λειτουργία XOR πραγματοποιείται σε κάθε πακέτο ανά κλειδί και πλήρης TSC από τον αλγόριθμο RC4 για να δημιουργηθεί το κλειδί WEP.

4. Ο αλγόριθμος ελέγχου ακεραιότητας μηνύματος(MIC) που έχει μήκος 64 bit συνδυάζεται με το απλό κείμενο. Το TKIP εισάγει έναν νέο αλγόριθμο ελέγχου ακεραιότητας μηνύματος (MIC) . Ο πομπός TKIP πάντα προσθέτει αυτό το MIC πριν το ICV. Ο πομπός και ο δέκτης αναγνωρίζουν μόνο αυτόν το MIC. Στη πλευρά της λήψης ο δέκτης ελέγχει τον MIC αφού αποκρυπτογραφήσει τα δεδομένα.

5. Κατά τη διαδικασία ενθυλάκωσης WEP, η λειτουργία XOR πραγματοποιείται στο κλειδί WEP που δημιουργήθηκε νωρίτερα και το συνδυαζόμενο

αποτέλεσμα του MIC και του απλού κειμένου δημιουργεί το κρυπτογραφημένο μήνυμα.

8.4.2.3 Οι ατέλειες στο WPA

Το WPA έχει το μειονέκτημα με τη χρήση των προ-μοιρασμένων κλειδιών (PSKs) που θεωρείται ότι είναι μια συσκευή ελέγχου ταυτότητας για μικρές επιχειρήσεις και οικιακούς πελάτες που δεν χρειάζονται να χρησιμοποιούν ατομικό διακομιστή ελέγχου ταυτότητας και ολόκληρη την αρχιτεκτονική κλειδιού 802.11x. Οποιοσδήποτε έχει λίγη αντίληψη του PSK μπορεί αν συμπεράνει κάποια PTK στο ESS κατά τη διάρκεια παθητικού sniffing του ασύρματου δικτύου, κρυφακούγοντας όλα τα απαραίτητα κλειδιά που ανταλλάσσουν πλαίσια δεδομένων.

Τα εργαλεία WPA χρησιμοποιούν διαδικασία του handshake για την εναλλαγή των κλειδιών κρυπτογράφησης δεδομένων για το ασύρματο μέσο ανάμεσα στο σημείο πρόσβασης και τον τελικό χρήστη. Ο επιτιθέμενος που δεν γνωρίζει το PSK μπορεί να κάνει μια μαντεψιά γνωστή ως επίθεση dictionary ή επίθεση brute force. Αν χρησιμοποιηθεί μια μικρή ή αδύναμη συνθηματική φράση, χρησιμοποιώντας μια εκτός-σύνδεσης επίθεση dictionary, κάποιος μπορεί εύκολα να μαντέψει το PSK διαθέτοντας λεξικό μεγέθους των 3 gigabyte και πάνω. Δεδομένου ότι η συνήθης πρακτική θα είναι ένα μόνο PSK για το ESS, μόλις αυτό προσδιοριστεί από τον εισβολέα, ο εισβολέας θα θεωρείται μέλος του ESS και επομένως όλο το ESS θα είναι προσβάσιμο από τον ίδιο.

Το PSK παρέχεται στο πρότυπο για να κάνει απλούστερες αναπτύξεις σε μικρά και λιγότερο επικίνδυνα δίκτυα. Ο κίνδυνος από τη χρήση του PSK εναντίον εσωτερικών επιθέσεων είναι συγκριτικά χειρότερος καθώς το WEP και η επικινδυνότητα της συνθηματικής φράσης βασισμένης στα PSKs εναντίον εξωτερικών επιθέσεων είναι μεγαλύτερος από το WEP.

8.4.2.4 Επίθεση στο WPA

Είναι απαραίτητο για κάθε επιτιθέμενο να συλλάβει αρχικά τη κυκλοφορία δεδομένων στο δίκτυο εκτός και αν ο επιτιθέμενος βρει το κρυπτογραφημένο αίτημα ARP ή κάποια απάντηση. Σε ορισμένες περιπτώσεις αυτά τα είδη πακέτων μπορούν να αναγνωριστούν εύκολα από τον επιτιθέμενο, ανάλογα με το μήκος του χαρακτηριστικού. Από την άλλη πλευρά το WEP και το TKIP δεν μπορούν να προστατεύσουν τις διευθύνσεις πηγής και προορισμού και πάντα τις στέλνουν να μεταδοθούν στη διεύθυνση του δικτύου. Σε αυτή την περίπτωση ο επιτιθέμενος γνωρίζει το συνολικό απλό κείμενο εκτός από τα τελευταία 8 bit των διευθύνσεων προορισμού και πηγής, 64 bits από τον κώδικα MIC και 32 bits από το ICV. Το τελευταίο τμήμα του απλού κειμένου είναι συνδυασμός του MIC και του ICV και έχει μήκος 12 bytes. Τώρα ο επιτιθέμενος εισαγάγει μια βελτιωμένη έκδοση της επίθεσης CHOPCHOP προκειμένου να αποκρυπτογραφήσει το άγνωστο απλό κείμενο που κινείται στο μέσο επικοινωνίας. Βασικά το WPA προτείνει 2 λύσεις για να προστατεύσει το δίκτυο από την επίθεση CHOPCHOP.

- Πρώτον, αν ο χρήστης έλαβε το πακέτο έχοντας άκυρο ICV, το δίκτυο θεωρεί το λάθος ως σφάλμα μετάδοσης και σαν αποτέλεσμα το πακέτο απορρίπτεται. Δεύτερον, αν ο κώδικας MIC είναι λάθος το δίκτυο νομίζει ότι γίνεται επίθεση, ανεξάρτητα από το αν η τιμή του ICV είναι σωστή και το σημείο πρόσβασης είναι ενημερωμένο από την ανταλλαγή αναφοράς αποτυχημένων πλαισίων MIC από τη πλευρά του πελάτη. Η επικοινωνία κλείνει αυτόματα αν το δίκτυο λάβει περισσότερες από 2 αναφορές αποτυχίας MIC σε διάστημα 60 δευτερολέπτων. Μετά από 60 δευτερόλεπτα τα κλειδιά επανεγκαθίστανται εκ νέου και η επικοινωνία ξαναρχίζει.

- Αν ένα πακέτο έχει επιτυχώς ληφθεί από την πλευρά του τελικού χρήστη, ένας προσωρινός μετρητής ακολουθίας (TSC) ελέγχεται και αν ο αριθμός του TSC είναι από τον τωρινό μετρητή που λήφθηκε, γίνεται η υπόθεση ότι βρίσκεται εκτός λειτουργίας και απορρίπτεται.

  Παρόλα αυτά η επίθεση CHOPCHOP εξακολουθεί να είναι εφικτή. Απλά ο επιτιθέμενος προσπαθεί να εστιάσει σε ειδικά κανάλια QoS στα οποία λαμβάνεται το πακέτο αρχικά. Συχνά το δίκτυο αποτελείται από πολλά κανάλια στα οποία τρέχουν καθόλου ή πολύ λίγα δεδομένα και όπου ο αριθμός TSC είναι ακόμα χαμηλότερος από τον τρέχοντα μετρητή. Δύο πιθανότητες υπάρχουν εδώ: Αν ο επιτιθέμενος αποτύχει να μαντέψει το τελευταίο bit κατά τη διάρκεια της επίθεσης CHOPCHOP, αυτά τα πακέτα απορρίπτονται. Αν όμως μαντέψει το τελευταίο bit με επιτυχία, οι τελικοί χρήστες στέλνουν απλά μία αναφορά αποτυχημένου πλαισίου MIC αλλά σε αυτή την περίπτωση ο αριθμός TSC δεν ενημερώνεται. Ως μέτρο ασφαλείας, ο επιτιθέμενος θα πρέπει να περιμένει για τουλάχιστον 60 δευτερόλεπτα αλλιώς ο τελικός χρήστης θα αρχίσει να δουλεύει πάνω σε αντίμετρα και θα μπλοκάρει την επικοινωνία. Εντός του χρονικού διαστήματος των 12 λεπτών maximum, ο επιτιθέμενος μπορεί να αναγνωρίσει τα τελευταία 12 bytes του απλού κειμένου που περιέχουν κώδικα MIC και ICV.

  Για τα υπόλοιπα bytes όπως τις διευθύνσεις πηγής και προορισμού, ο επιτιθέμενος μπορεί απλά να τα μαντέψει βασιζόμενος στον αποκρυπτογραφημένο ICV. Μόλις ο κώδικας MIC και το απλό κείμενο προσδιοριστούν, το επόμενο βήμα είναι να βρεθεί το κλειδί MIC που χρησιμοποιείται για να προστατέψει τα πακέτα στην πλευρά αποστολής (το σημείο πρόσβασης του τελικού χρήστη), απλά αντιστρέφοντας τον αλγόριθμο MICHAEL. Αφού εντοπιστεί το MIC και το key stream στην πλευρά αποστολής του πελάτη, ο επιτιθέμενος είναι σε θέση να στείλει τα πακέτα προς τον τελικό χρήστη, σε εκείνα τα κανάλια QoS όπου ο αριθμός TSC είναι χαμηλότερος από τον μετρητή των καταγραμμένων δεδομένων.

  Όταν η επίθεση εφαρμοστεί πλήρως, ο επιτιθέμενος μπορεί απλά να προσδιορίσει το περαιτέρω key stream μέσα στο χρονικό διάστημα των 6-7 λεπτών επειδή αρκεί να γνωρίζει μόνο τα 4 byte του ICV χρησιμοποιώντας

CHOPCHOP. Οι άλλες πληροφορίες όπως οι διευθύνσεις πηγής και προορισμού μπορεί εύκολα να τα μαντέψει κάποιος και εξίσου εύκολα μπορεί να προσδιορίσει το κλειδί MIC. Για να μετριαστεί αυτό το είδος της επίθεσης, οι προμηθευτές προτείνουν τη χρήση πολύ σύντομης αναπαραγωγής κλειδιών στο διάστημα των 130 δευτερολέπτων περίπου. Η πρακτική πρόταση για να απαλλαγούμε από αυτή την επίθεση είναι απλά να αντικαταστήσουμε το TKIP με το CCMP (AES).

8.4.3 WPA2

Το IEEE 802.11i είναι ένα πρόσθετο πρότυπο που οριστικοποιήθηκε το φθινόπωρο του 2004 ώστε να βελτιώσει τον έλεγχο ταυτότητας και την κρυπτογράφηση. Το WPA2 εισήγαγε μια νέα έννοια του RSN χρησιμοποιώντας έναν μεγάλο αριθμό πρωτοκόλλων στοιβάδας IEEE 802.11 MAC που παρέχει επιπλέον διαχείριση κλειδιών και ελέγχου ταυτότητας στα δίκτυα. Το IEEE 802.11i βελτίωσε τις 3 βασικές περιοχές ώστε να παρέχει ασφάλεια στο IEEE 802.11b εκεί όπου το WEP δεν είναι σε θέση να παρέχει προστασία.

- Έλεγχος ταυτότητας
- Διαχείριση κλειδιού
- Μεταφορά δεδομένων

Η αρχιτεκτονική του WPA2 είναι τελείως διαφορετική από αυτή των WEP και WPA επειδή χρησιμοποιεί ένα μόνο στοιχείο για τη διαχείριση κλειδιού και την ακεραιότητα του μηνύματος που είναι το CCMP βασισμένο στη προηγμένη ασφάλεια κρυπτογράφησης AES. Υπάρχουν 2 σκοποί του CCMP:

- Η λειτουργία μετρητή χρησιμοποιείται για να παρέχει προστασία δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
- Το CBC-MAC χρησιμοποιείται για να παρέχει την ακεραιότητα του μηνύματος στο δίκτυο.

Το 802.1X και το EAP θεωρούνται τα συστήματα πιστοποίησης του δικτύου στο πρότυπο IEEE 802.11i. Υπάρχουν βελτιωμένα χαρακτηριστικά ασφαλείας στο WPA2 που είναι η χρήση δυναμικής διανομής κλειδιού και ένα νέο σύστημα κρυπτογράφησης σε σχέση με το WEP και το WPA. Στο WPA2, το RADIUS είναι γνωστό ως πρωτόκολλο AAA που λειτουργεί ως έλεγχος ταυτότητας χρήστη στον μηχανισμό μεταφοράς EAP. Ο κύριος σκοπός της χρήσης των EAP και RADIUS είναι για τις νέες μεθόδους ασφάλειας πακέτων της διανομής κλειδιών κάτι το οποίο δεν είναι διαθέσιμο στον αλγόριθμο WEP.

Στο WPA2 το νέο κλειδί δημιουργείται για όλα τα κρυπτογραφημένα πακέτα δεδομένων που είναι που είναι έτοιμα να σταλθούν μέσω του αέρα, με το δικό του κλειδί κρυπτογράφησης. Χρησιμοποιώντας αυτή την τεχνική η πολυπλοκότητα της

αποκωδικοποίησης του πακέτου στο δίκτυο αυξάνει και είναι πολύ δύσκολη η αποκρυπτογράφηση του κλειδιού για έναν μη εξουσιοδοτημένο χρήστη. Αυτές οι νέες τεχνικές είναι πιο επεκτάσιμες και ασφαλείς ειδικά για τα μεγαλύτερα δίκτυα, αλλά πολύ πιο πολύπλοκες σε σχέση με τους τρέχοντες μηχανισμούς ασύρματης ασφάλειας. Το WPA2 παρέχει κάποια πλεονεκτήματα σε σχέση με τις τεχνικές WPA και WEP.

- Παροχή περισσότερης ασφάλειας με τη χρήση προηγμένης ασφάλειας κρυπτογράφησης (AES).
- Χρήση ισχυρότερης διαχείρισης κλειδιών.
- Προστασία ενάντια σε επιθέσεις man in the middle με τη χρήση 2 τρόπων της διαδικασίας ελέγχου ταυτότητας.
- Παροχή βελτιωμένης απόδοσης ακεραιότητας μηνύματος με τη χρήση του CBC-MAC.

8.4.3.1 CCMP

Το CCMP είναι ένας αλγόριθμος κρυπτογράφησης του IEEE 802.11i. Το CCMP λειτουργεί με ένα συγκεκριμένο τρόπο λειτουργίας που είναι AES. Με λίγα λόγια ο τρόπος λειτουργίας είναι γνωστός ως ο αλγόριθμος του οποίου ο σκοπός είναι να αλλάξει το κρυπτογραφημένο κείμενο σε απλό και το αντίστροφο. Ο κύριος σκοπός χρήσης της τεχνικής κρυπτογράφησης είναι να παρέχει το απόρρητο των δεδομένων και έτσι αποδεικνύεται ότι η προηγούμενη τεχνική κρυπτογράφησης απέτυχε να παρέχει ακεραιότητα των δεδομένων. Για την παροχή της ακεραιότητας δεδομένων ένας νέος κώδικας επαλήθευσης ταυτότητας μηνύματος επισυνάπτεται με το αρχικό μήνυμα. Ο κώδικας επαλήθευσης ταυτότητας μηνύματος είναι χρήσιμος για κλειδωμένες κρυπτογραφικές λειτουργίες ώστε να δημιουργήσει την τιμή ακεραιότητας (ICV).

Στο πρότυπο IEEE 802.11i το CCMP διαιρείται σε 2 μέρη:

- Λειτουργία μετρητή (CTR MODE): Η λειτουργία αυτή χρησιμοποιείται στο AES για την κρυπτογράφηση των δεδομένων.
- Αλυσιδωτή σύνδεση κρυπτογράφησης (CBC-MAC MODE): Η λειτουργία αυτή χρησιμοποιείται για να δημιουργήσει έναν κώδικα MIC που παρέχει την ακεραιότητα των δεδομένων.

Το ίδιο προσωρινό κλειδί χρησιμοποιείται και στις 2 λειτουργίες, το οποίο είναι μήκους 128 bit ή 16 byte και παράγεται κατά τη διάρκεια ελέγχου ταυτότητας του 802.11x για την κρυπτογράφηση και τον υπολογισμό MIC. Το CCMP χρησιμοποιεί το νεοαποκτηθέν προσωρινό κλειδί για κάθε σύνοδο. Επίσης χρησιμοποιεί την ειδική τιμή αποστολής για ξεχωριστά πλαίσια και παρέχει προστασία με τη χρήση του προσωρινού κλειδιού και έτσι το CCMP περιλαμβάνει αριθμό πακέτου(PN) μήκους 48 bit.

8.4.3.2 Αρχιτεκτονική WPA2

Το φορτίο του πρωτοκόλλου μονάδας δεδομένων μηνύματος απλού κειμένου (plaintext message protocol data unit) κρυπτογραφείται από το CCMP και εκτελεί την λειτουργία της ενθυλάκωσης στο κρυπτογραφημένο κείμενο. Η διαδικασία κρυπτογράφησης του CCMP στο 802.11i περιγράφεται περαιτέρω στα ακόλουθα σημεία:

- Για κάθε MPDU απαιτείται ένα νέο PN που μπορεί να αποκτηθεί με την επαύξηση του προηγούμενου PN. Επειδή το ίδιο προσωρινό κλειδί χρησιμοποιεί διαφορετικό PN, αυτό σημαίνει ότι το PN ίσως δεν χρησιμοποιείται παραπάνω από 1 φορά με το ίδιο προσωρινό κλειδί.

- Το AAD για το CCM κατασκευάζεται από τους τομείς που είναι διαθέσιμοι στην κεφαλίδα MPDU. Επίσης τα πεδία που είναι διαθέσιμα στο AAD εφοδιάζονται με ακεραιότητα από τον αλγόριθμο CCM.

- Η αποστολή CCMP κατασκευάζεται από 3 πράγματα που είναι ο αριθμός πακέτου PN, ο τομέας προτεραιότητας του MPDU και το A2 που θεωρείται η διεύθυνση του MPDU. Το 0 έχει οριστεί ως η τιμή διατήρησης για το πεδίο προτεραιότητας.

- Η κεφαλίδα CCMP κατασκευάζεται από το συνδυασμό του αναγνωριστικού κλειδιού και του νέου αριθμού πακέτου. Το μέγεθος της κεφαλίδας CCMP είναι 64 bit.

- Το κρυπτογραφημένο κείμενο και το MIC παράγονται από το συνδυασμό του προσωρινού κλειδιού, του AAD, της αποστολής και των δεδομένων MPDU. Αυτό το βήμα του συνδυασμού είναι επίσης γνωστό ως επεξεργασία εντολέα CCM.

- Τα κρυπτογραφημένα δεδομένα και το MIC συνενώνονται με την αρχική κεφαλίδα CCMP και την κεφαλίδα MPDU που έχουν ήδη κατασκευαστεί, ώστε να σχηματίσουν το κρυπτογραφημένο MPDU.

Η διαδικασία ξε-ενθυλάκωσης του απλού κειμένου MPDU και η αποκρυπτογράφηση του κρυπτογραφημένου κειμένου MPDU με τη χρήση του CCMP στο 802.11i περιγράφεται από κάτω:

- Το AAD και η τιμή αποστολής ανακατασκευάζονται από το κρυπτογραφημένο MPDU.

- Το AAD ανακατασκευάζεται από την κεφαλίδα MPDU του κρυπτογραφημένου MPDU.

- Η τιμή αποστολής ανακατασκευάζεται από 3 πράγματα, το A2 που είναι γνωστό ως η διεύθυνση του MPDU, τον αριθμό πακέτου PN και το πεδίο προτεραιότητας του PDU.

- Με τη χρήση του ελέγχου ακεραιότητας CCM, το MIC αποκτάται από το PN, το απλό κείμενο και το προσωρινό κλειδί.

- Το απλό κείμενο MPDU σχηματίζεται από το συνδυασμό των AAD, της αποστολής, του προσωρινού κλειδιού, του MIC και του κρυπτογραφημένου κειμένου MPDU στη πλευρά αποκρυπτογράφησης του CCM. Σε αυτή τη διαδικασία, ελέγχεται η ακεραιότητα του απλού κειμένου και του AAD.

- Το αποκρυπτογραφημένο απλό κείμενο MPDU και η αρχική κεφαλίδα MAC του MPDU συνδυάζονται για να δημιουργήσουν ένα απλό κείμενο MPDU.

- Τα MPDUs εμποδίζονται από την επανάληψη, συγκρίνοντας αν το PN στο MPDU είναι υψηλότερο από τον πραγματικό μετρητή που έχει ήδη εκχωρηθεί πριν τη διαδικασία αποκρυπτογράφησης. (31)

8.4.3.3 Οι ατέλειες στο WPA2

Το WPA2 έχει περιορισμένα μειονεκτήματα σε σχέση με την αρχική λύση ασφαλείας WEP και την υποκατάστατη λύση ασφαλείας WPA:

- Η τεχνική WPA2 είναι πάρα πολύ δαπανηρή για τα ήδη αναπτυγμένα δίκτυα λόγω των νέων κρυπτογραφήσεων CCMP και AES και χρειάζεται να αλλάξει το συνολικό hardware του δικτύου.

- Μερικές φορές το δίκτυο είναι ευάλωτο σε κινδύνους ασφαλείας επειδή το WPA2 έχει απόλυτη πρόσβαση στη απόρρητες συνόδους κλειδιών.

- Το WPA2 απαιτεί περισσότερο hardware λόγω του αμφίδρομου ελέγχου ταυτότητας μεταξύ του τελικού χρήστη και του σημείου πρόσβασης.

- Είναι πιο δύσκολο και περίπλοκο να κατανοηθεί σε σχέση με τα τωρινά δίκτυα.

- Η προσωπική έκδοση του WPA2 αντιμετωπίζει πολλές απειλές όπως τη πλαστογράφηση MAC, τη σύνδεση ad hoc, τη λανθασμένη διαμόρφωση κτλ.

8.4.3.4 Επίθεση στο WPA2

Αυτή η επίθεση είναι πιθανή μόνο αν η αρχική τιμή του μετρητή του AES CCMP είναι σημαντικά αναγνωρίσιμη, αλλιώς αυτή η επίθεση δεν έχει σημασία. Οι τωρινές μελέτες δείχνουν ότι αν ο επιτιθέμενος έχει επαρκείς γνώσεις μπορεί εύκολα να μαντέψει την αρχική τιμή του μετρητή που χρησιμοποιείται στο AES CCMP του 802.11. Τα WLANs και η τιμή αποστολής μπορούν εύκολα να επαναϋπολογιστούν. Η τιμή αποστολής είναι ο συνδυασμός 3 πραγμάτων, του πεδίου προτεραιότητας, της

διεύθυνσης του MAC(κεφαλίδας) και του τομέα αριθμού πακέτων. Ο εισβολέας θέλει μόνο να μάθει την αρχική τιμή του μετρητή και το μέγεθος του φορτίου. Το μέγεθος του φορτίου μπορεί να προσδιοριστεί εύκολα από τις πληροφορίες προτεραιότητας. Οι τωρινές έρευνες έδειξαν ότι οι ασύρματες επικοινωνίες είναι ευαίσθητες στη φύση, αν ο εισβολέας έχει συμβατές συσκευές μπορεί εύκολα να υποκλέψει τα MPDUs. Αν ο εισβολέας θέλει να επαληθεύσει την ήδη υπολογισμένη τιμή αποστολής, τότε μπορεί να το κάνει εξάγοντας το A2 και την προτεραιότητα από την κεφαλίδα MAC και το πεδίο PN από την κεφαλίδα CCMP. Για να βρει την τιμή του μετρητή block (counter block value) είναι απαραίτητο να βρει το μέγεθος του ωφέλιμου φορτίου και το μέγεθος των IEEE 802.11 MPDUs που έχουν ήδη καθοριστεί και είναι 2312 bytes εκ των οποίων τα 2296 bytes είναι για δεδομένα, τα 8 bytes για τον κώδικα MIC και τα 8 bytes για την κεφαλίδα CCMP. Μόλις ο εισβολέας βρει το μέγεθος του ωφέλιμου φορτίου μπορεί εύκολα να υπολογίσει την αρχική τιμή του μετρητή (μήκους 128 bits), απλά συνδυάζοντας το πεδίο Flags, το πεδίο αποστολής και το μέγεθος του φορτίου. Αυτή η αρχική τιμή του μετρητή παρέχει βάση για τις επιθέσεις εξισορρόπησης (trade-off) και χρόνου-μνήμης(time memory).

Οι επιθέσεις προ-υπολογισμού TMTO χρησιμοποιούνται μόνο για να βρουν το ολοκληρωμένο κλειδί αναζήτησης και πάντα εργάζονται πάνω στην κρυπτογράφηση των δεδομένων. Αυτό το είδος επίθεσης είναι πιθανό μόνο αν ο επιτιθέμενος διαθέτει μια τεράστια βάση δεδομένων ώστε να επιτεθεί σε οποιοδήποτε μυστικό κλειδί. Κατά τη διάρκεια της επίθεσης, ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτή την τεράστια βάση δεδομένων και έχει τη δυνατότητα να επιτεθεί σε πολλά διαφορετικά κλειδιά κάθε φορά. Το πλεονέκτημα αυτού του είδους επίθεσης είναι ότι κατά τη διάρκεια της επίθεσης δεν χρειάζεται το απλό κείμενο. Αυτή η επίθεση είναι διάσημη όταν υπάρχει αναξιοπιστία στο απλό κείμενο και το δίκτυο χρησιμοποιεί πολλά μυστικά κλειδιά. Ο μεγάλος αριθμός των δεδομένων που είναι διαθέσιμα στο δίκτυο παίζει μεγάλο ρόλο στην επιτυχία της επίθεσης TMTO και το σχέδιο του επιτιθέμενου σχετικά με το πώς ακριβώς θα επιτεθεί, διαδραματίζει έναν εξίσου σημαντικό ρόλο. Ο αρχικός μετρητής και η κρυπτογραφική λειτουργία του μετρητή επαυξάνονται διαρκώς στην πανομοιότυπη σύνοδο.

Σημειώνεται ότι το μέγεθος του MPDU στο CCMP είναι 2296 bytes και δεν υπάρχει κάποιο ανώτερο καθορισμένο όριο για τα MPDUs σε μια σύνοδο. Έτσι αυτή η ποσότητα των δεδομένων είναι εφικτή προκειμένου να γίνει επίθεση TMTO σε οποιοδήποτε δίκτυο. Είναι σαφώς ορισμένο ότι η λειτουργία του μετρητή αντιμετωπίζει απειλή από την επίθεση προ-υπολογισμού TMTO μέχρι και εκτός αν την μαντέψει ο επιτιθέμενος. Αν ο αρχικός μετρητής και ο μετρητής ενημέρωσης είναι προσβάσιμοι από τον επιτιθέμενο τότε μια επίθεση TMTO είναι εφικτή. Η επίθεση αυτή χρησιμοποιεί μια φόρμουλα 2n/3 που βοηθάει να υπολογιστεί το αποτελεσματικό μέγεθος κλειδιού του δικτύου, όπου n είναι το μέγεθος του κλειδιού κρυπτογράφησης που είναι μήκους 128 bits στη λειτουργία μετρητή AES. Επομένως, το αποτελεσματικό μέγεθος κλειδιού TMTO μπορεί να δοθεί ως 2 x 128/ 3 = περίπου

85 bits. Για να μετριαστεί η επίθεση προ-υπολογισμού TMTO υπάρχουν 3 βασικές προτάσεις να ακολουθηθούν:

- Το μέγεθος του κλειδιού να είναι μεγαλύτερο από τα 128 bits.
- Η χρήση τουλάχιστον 64 bit στον αρχικό μετρητή που είναι άγνωστα από τον επιτιθέμενο και περιλαμβάνονται ως μέρος της λειτουργίας μετρητή κλειδιού AES.
- Η χρήση κάποιων απροσδιόριστων αλλά πανομοιότυπα κατανεμημένων στοιχείων στον αρχικό μετρητή.

9. Ποιότητα υπηρεσιών (QoS)

Το QoS αντιπροσωπεύει την ποιότητα υπηρεσιών (Quality of service). Στο QoS, το εύρος ζώνης, τα ποσοστά σφάλματος και η καθυστέρηση μπορούν να παρακολουθούνται, να γίνεται δειγματοληψία και πιθανώς να βελτιώνονται. Επίσης το QoS παραδίδει το σύνολο των εργαλείων που βοηθούν στην αποτελεσματική παροχή δεδομένων μειώνοντας τον αντίκτυπο της καθυστέρησης κατά τη διάρκεια των ωρών αιχμής που τα δίκτυα πλησιάζουν στην πλήρη χωρητικότητα. Το QoS δεν προσθέτει χωρητικότητα ούτε πολυπλέκει τα σήματα όπως το WDM. Απλά προσπαθεί να διαχειριστεί την κίνηση των δεδομένων καλύτερα έτσι ώστε να μην κινδυνεύσει η κίνηση των δεδομένων που βρίσκονται σε ύψιστη προτεραιότητα. Το QoS βοηθάει στη διαχείριση της χρήσης του εύρους ζώνης εφαρμόζοντας μια σειρά εργαλείων όπως το σύστημα προτεραιότητας έτσι ώστε ορισμένα πακέτα (αυτά που είναι υψηλής σημαντικότητας και πρέπει να σταλθούν οπωσδήποτε) θα διαβιβαστούν πρώτα.

9.1 Η ανάγκη για Ποιότητα Υπηρεσιών

Πολλοί χρήστες πιστεύουν ότι περισσότερο εύρος ζώνης θα επιλύσει το πρόβλημα αλλά αυτή η μέθοδος ίσως δεν λειτουργεί πλέον. Η τηλεφωνία Voice over IP και άλλες νέες τεχνολογίες όπως τα δικτυωμένα βίντεο ασφαλείας, η απομακρυσμένη παρακολούθηση και η καταγραφή μέσω δικτύων IP γίνονται όλο κ πιο δημοφιλείς. Έχουν αρχίσει να διεισδύουν σε δίκτυα που διαχειρίζονται πολλά δεδομένα, αναγκάζοντας τους διαχειριστές δικτύων και τους διευθυντές να χρησιμοποιούν μέτρα όπως το QoS για να φιλοξενήσουν αυτές τις τεχνολογίες αποτελεσματικά και χωρίς καμία αλλαγή στην απόδοση του υπάρχοντος δικτύου.

Η κυκλοφορία πολλαπλών υπηρεσιών είναι δύσκολο να χειριστεί αποτελεσματικά διότι κάθε είδος κυκλοφορίας απαιτεί διαφορετική ταχύτητα μεταφοράς και έχει διαφορετική ανοχή στην καθυστέρηση ή στην αλληλουχία πακέτων. Η αρχική καλύτερη προσπάθεια σχεδιασμού πρωτοκόλλων LAN έγινε για υπηρεσίες όπως η βασική συνδεσιμότητα μεταξύ των σταθμών, η μεταφορά αρχείων, τα emails, τα MRPs και αργότερα στο διαδίκτυο.

Αυτές οι εφαρμογές δεν κινδυνεύουν από καθυστέρηση πακέτων για όσο καθιερώθηκε η επικοινωνία και η μεταφορά των δεδομένων δεν δημιούργησε πρόβλημα, επομένως το δίκτυο εξυπηρέτησε τον σκοπό του. Επίσης η κυκλοφορία πολλαπλών υπηρεσιών πρέπει να συνυπάρχει αρμονικά με την υποδομή. Σε πολλές περιπτώσεις το VOIP πρέπει να δρομολογείται πίσω στο PSTN ώστε να μεταδοθεί η απαραίτητη κλήση ή να μεταδοθεί το IP βίντεο μέσω του CCTV.

Το εύρος ζώνης του δικτύου εξακολουθεί να είναι σημαντικό αλλά δεν είναι ο μόνος παράγοντας εξέτασης για την εφαρμογή μελλοντικών τεχνολογιών. Τα νέα ειδικά χαρακτηριστικά αυτής της κυκλοφορίας (καθυστέρηση, παραμόρφωση κτλ) πρέπει να διαβαστούν, να κατανοηθούν και να εφαρμοστούν. Ένα από τα κλειδιά στην παροχή

φωνής ή βίντεο σε οποιοδήποτε μέσο είναι η διατήρηση ενός επιπέδου ποιότητας. Η ποιότητα της φωνής ή του βίντεο μπορεί να επιδεινωθεί εξαιτίας 3 παραγόντων:

- Υπερσυμπίεση

  Οι αναλογίες συμπίεσης είναι αντιστρόφως ανάλογες με την ποιότητα του σήματος της φωνής που μεταδίδεται μέσω του δικτύου, και είναι κατώτερη από αυτή που είχε συνηθίσει ο χρήστης με το POTS (απλό παλιό τηλέφωνο). Όσο πιο χαμηλή είναι η συμπίεση τόσο πιο υψηλή είναι η απαραίτητη απόδοση για τη μετάδοση πακέτων φωνής, αυξάνοντας έτσι την πιθανότητα συμφόρησης του δικτύου και άρα της απώλειας ποιότητας. Η συμπίεση μπορεί να ελεγχθεί εύκολα από τους χρήστες.

- Απώλεια πακέτων στο δίκτυο

  Τα πακέτα χάνονται στο δίκτυο, το οποίο δεν είναι πρόβλημα για τις παραδοσιακές εφαρμογές. Η ποιότητα των παραδοσιακών εφαρμογών όπως η μεταφορά αρχείων έχει ανοσία στην απώλεια πακέτων επειδή αυτές οι ζημιές αναγνωρίζονται από το δίκτυο και τα αρχεία αναμεταδίδονται. Τα προϊόντα VOIP ανακατασκευάζουν τα πακέτα αν ο αριθμός είναι ελάχιστος. Ο γενικός κανόνας είναι να μην χάνεται πάνω από το 10% των πακέτων στα δίκτυα VOIP διαφορετικά η ποιότητα φωνής θα τεθεί σε κίνδυνο.

- Καθυστέρηση

  Η καθυστέρηση στα δίκτυα δεδομένων δεν είναι τόσο σημαντική. Η αναμονή για τη φόρτωση μιας σελίδας δεν είναι τόσο εκνευριστική όσο η σιωπή από τη πλευρά του αποδέκτη όταν είσαι στη μέση μιας σημαντικής συζήτησης. Μια μέγιστη καθυστέρηση των 150 ms είναι ο κανόνας για μονόδρομη καθυστέρηση για την επίτευξη παρόμοιας ποιότητας με τη φωνή POTS.

  Οι διαχειριστές του δικτύου αντιμετωπίζουν μια νέα πρόκληση με τις εφαρμογές φωνής και ασφάλειας. Τα παραδοσιακά POTS είναι αρκετά αξιόπιστα σε όρους μεταφοράς και επικοινωνίας. Ενώ ήταν αποδεκτό να περιμένεις 5 δευτερόλεπτα για να φορτώσει μια σελίδα είναι απαράδεκτο να ανεχτείς τέτοια καθυστέρηση κατά τη διάρκεια συνδιάσκεψης με έναν πελάτη.

Αυτές οι προσδοκίες στα δίκτυα δημιούργησαν την ανάγκη για το QoS. Μια σημαντική προϋπόθεση ώστε να είναι επιτυχές το QoS είναι ότι πρέπει να χρησιμοποιηθεί και διαχειριστεί από άκρη σε άκρη σε διάφορα LANs και WANs. Αυτό θα αποτελεί τη εγγύηση ότι όλα τα σημεία συμφόρησης θα αντιμετωπιστούν και η φωνή/το βίντεο δεν θα παραμορφωθεί. Αν το QoS λειτουργεί μόνο σε ένα τμήμα του δικτύου, οτιδήποτε πρέπει να βγει έξω από το δίκτυο μέσω της συμφόρησης πρέπει να αντιμετωπιστεί και προωθηθεί στη σειρά που λήφθηκε, στη διαθέσιμη ταχύτητα και με μια πιθανή καθυστέρηση.

Επομένως, απαιτείται η προσφορά των ελάχιστων έστω εγγυήσεων στον πελάτη (QoS) ώστε να είναι βέβαιος ότι θα μπορεί να χρησιμοποιήσει τις υπηρεσίες που θέλει και με τον καλύτερο δυνατό τρόπο.

Με βάση τα προαναφερθέντα προκύπτει ότι υπήρχε ανάγκη για τον διαχωρισμό μεταξύ των υπηρεσιών που χρησιμοποιούνται, έτσι ώστε η καθεμία να υπόκειται σε διαφορετική μεταχείριση ώστε να είναι ομαλή η χρήση τους. Εμφανίστηκαν διάφορες λύσεις για το θέμα αυτό, με τις τρεις κυρίαρχες να είναι η «αρχιτεκτονική βέλτιστης προσπάθειας» (Best Effort), η «αρχιτεκτονική ενοποιημένων υπηρεσιών» (Integrated Services – IntServ) και η «αρχιτεκτονική διαφοροποιημένων υπηρεσιών» (Differentiated Services – DiffServ). (32,33,34)

9.2 Αρχιτεκτονική Βέλτιστης Προσπάθειας (Best Effort)

Η μέθοδος αυτή δεν χρησιμοποιεί QoS και αφορά στις περιπτώσεις όπου δεν είναι σημαντικό το πότε και με ποιό τρόπο θα φτάσουν τα πακέτα στον προορισμό τους.

Η βέλτιστη προσπάθεια είναι ένα μοντέλο απλής υπηρεσίας, στο οποίο μια εφαρμογή στέλνει οποιαδήποτε ποσότητα δεδομένων, οποτεδήποτε πρέπει και χωρίς να ζητάει άδεια ή να ενημερώνει πρώτα το δίκτυο. Για την υπηρεσία βέλτιστης προσπάθειας το δίκτυο μεταδίδει τα δεδομένα εφόσον μπορεί, χωρίς καμία εξασφάλιση για την αξιοπιστία, τα όρια της καθυστέρησης ή την ικανότητα μετάδοσης. Η υπηρεσία βέλτιστης προσπάθειας είναι κατάλληλη για μια ευρεία γκάμα δικτυακών εφαρμογών, όπως η μεταφορά αρχείων (FTP) και το ηλεκτρονικό ταχυδρομείο (E-mail). Μια από τις τεχνικές που προσφέρουν την υπηρεσία αυτή είναι οι ουρές FIFO (First In First Out). (35)

Συγκεκριμένα, στο μοντέλο αυτό το βέλτιστο μονοπάτι αποφασίζεται εκ των προτέρων από κάθε δρομολογητή για όλους τους προορισμούς ανάλογα με τις αλλαγές στην τοπολογία. Επίσης τα πακέτα προωθούνται στη βάση της καλύτερης δυνατής προσπάθειας και ίσως απορριφθούν ή παραδοθούν εκτός προγραμματισμένου χρόνου σε περίπτωση συμφόρησης ή αλλαγών δρομολόγησης. Η προώθηση των πακέτων εφαρμόζεται στη βάση του hop by hop χρησιμοποιώντας κατάσταση προορισμού-διεύθυνσης τα οποία είναι ήδη υπολογισμένα από τη διαδικασία δρομολόγησης.

Αυτό το μοντέλο έχει αποδειχτεί εξαιρετικά ισχυρό και πράγματι η επιτυχία της αρχιτεκτονικής του διαδικτύου στηρίζεται πολύ στο μοντέλο δρομολόγησής του. Παρόλα αυτά, οι περιορισμοί αυτού του μοντέλου είναι πολύ μεγάλοι όταν μιλάμε για πιο απαιτητικές αρχιτεκτονικές.

Ένας σημαντικός περιορισμός είναι ότι υποστηρίζει μόνο μία διαδρομή για κάθε προορισμό. Συγκεκριμένα, η κατάσταση διαβίβασης στο διαδίκτυο αποτελείται από μία μόνο καταχώρηση για κάθε προορισμό δίνοντάς την κάθε φορά στον επόμενο δρομολογητή από την πηγή στον προορισμό. Ως αποτέλεσμα υποστηρίζεται μόνο μία διαδρομή για κάθε προορισμό, και αυτή η διαδρομή υπολογίζεται για να

βελτιστοποιήσει μία απλή μετρική. Επομένως, ο περιορισμός της μονής διαδρομής μεταφράζεται σε ανικανότητα άμεσης υποστήριξης εφαρμογών με ποικίλες απαιτήσεις QoS. Είναι επομένως σαφές ότι αυτό το μοντέλο δεν είναι το κατάλληλο για τις ολοένα και πιο απαιτητικές εφαρμογές που συναντώνται σήμερα. (36)

9.3 Differential Services

Μία άλλη πολύ δημοφιλής μέθοδος του QOS στις επιχειρήσεις είναι οι διαφοροποιημένες υπηρεσίες. Είναι μια αποτελεσματική μέθοδος διαχείρισης της κυκλοφορίας βασισμένη στην κλάση του. Το Diffserv θέτει σε προτεραιότητα συγκεκριμένους τύπους κυκλοφορίας όπως η κίνηση φωνής σε σχέση με άλλους τύπους επικοινωνιών. Λειτουργεί με την κατηγοριοποίηση των πακέτων IP σε κλάσεις. Τα 6 bits σε αυτό το είδος της υπηρεσίας που βρίσκονται στην κεφαλίδα IP του κάθε πακέτου, καθορίζουν ένα συγκεκριμένο τύπο συμπεριφοράς που καθορίζει το σύστημα και την προτεραιότητα της προώθησης των πακέτων.

Οι διαφοροποιημένες υπηρεσίες μπορούν να προσφέρουν τα ακόλουθα:

- Ταχεία προώθηση (EF) που ορίζει την ελάχιστη καθυστέρηση και παραμόρφωση. Η κλάση αυτή προσφέρει υπηρεσίες με χαμηλά delay, delay jitter και loss probability. Το αρνητικό στοιχείο της όμως είναι ότι ακριβώς επειδή προσφέρει τόσο καλή ποιότητα υπηρεσιών χρησιμοποιεί πολύ λίγους πόρους του δικτύου και για αυτό χρησιμοποιείται κυρίως για συγκεκριμένα είδη υπηρεσιών όπως είναι η υπηρεσία VoIP.

- Εγγυημένη προώθηση (AF) που εισάγει 3 επιλεγόμενα ποσοστά πτώσης προτεραιότητας πακέτων. Κατά τη διάρκεια της συμφόρησης τα πακέτα με μεγάλη πτώση προτεραιότητας απορρίπτονται. Επιτρέπεται στη πιο σημαντική κυκλοφορία με χαμηλό ποσοστό πτώσης προτεραιότητας να περάσει. Η κλάση αυτή λειτουργεί παρόμοια με τη λειτουργία ελεγχόμενου φορτίου της IntServ. Συγκεκριμένα, υπάρχουν 12 κωδικοί DSCP οι οποίοι χωρίζονται σε διαφορετικές κλάσεις που για κάθε μία από αυτές υπάρχουν διαφορετικές προτεραιότητες απόρριψης. Τα πακέτα που έχουν τις μεγαλύτερες προτεραιότητες απόρριψης έχουν προφανώς μεγαλύτερη πιθανότητα να απορριφθούν. Επίσης αυτή η κλάση προσφέρει τη δυνατότητα στις ροές να δανείζονται εύρος ζώνης όποτε χρειάζεται από τις κλάσεις χαμηλότερης προτεραιότητας συνήθως. Η κλάση AF λοιπόν θεωρείται ιδανική για εφαρμογές μη πραγματικού χρόνου όπως είναι το browsing.

Οι δρομολογητές DiffServ εκτελούν γενικά τις ακόλουθες λειτουργίες:

- Μετρητής: Ο μετρητής συλλέγει τα στατιστικά της κίνησης και ελέγχει αν τηρεί τα συμφωνηθέντα βάσει το SLA. Επίσης προωθεί τις μετρήσεις που πραγματοποιεί στη μονάδα σήμανσης και στο ρυθμιστή.

- Ταξινομητής: Επιλέγει τα πακέτα βάσει κάποιου χαρακτηριστικού τους όπως είναι η τιμή DHCP.
- Μονάδα σήμανσης: Προσθέτει ή αλλάζει την τιμή DHCP όπου χρειάζεται.
- Ρυθμιστής: Εφαρμόζει τις PHB's και προσπαθεί να ταιριάξει την κίνηση βάσει των προδιαγραφών του SLA. Αυτό επιτυγχάνεται είτε μέσω της απόρριψης πακέτων είτε μέσω της μορφοποίησης της κίνησης με την καθυστέρηση των πακέτων.

Οι DiffServ μπορούν να χρησιμοποιηθούν ως μηχανισμός QoS στα επιχειρηματικά δίκτυα. Σχεδόν όλοι οι νέοι δρομολογητές αλλά και τα τελικά προϊόντα όπως τα τηλέφωνα VOIP υποστηρίζουν τις DiffServ και βάζουν ετικέτες στα πακέτα ανάλογα με τη συμπεριφορά τους. Οι σημάνσεις των DiffServ διαβάζονται και κατανοούνται πλήρως και τα πακέτα προωθούνται με βάση τα προαναφερθέντα συστήματα προτεραιότητας. Ο μετατροπέας MAC περνάει αυτά τα πακέτα με διαφάνεια.

Τέτοιες υπηρεσίες QoS δεν είναι μέρος καμίας διαπραγμάτευσης ή σηματοδότησης αναμεταξύ των συσκευών. Αυτοί οι κανόνες έχουν ανατεθεί στους διαχειριστές των τοπικών δικτύων που αντιλαμβάνονται τους παραπάνω λόγους για συμφόρηση και προσαρμόζουν ανάλογα τις προτεραιότητες για τους χρήστες, τις υπηρεσίες και τις εφαρμογές. Αυτές οι ανατιθέμενες ετικέτες περνούν στα πακέτα και δεν γίνονται αντικείμενα αλλαγής κατά τη διαδικασία της αυτόματης διαπραγμάτευσης των άλλων μορφών σηματοδότησης. Η προσέγγιση αυτή λέγεται SOFT QoS. 802.1P.H προτεραιότητα IP και οι διαφοροποιημένες υπηρεσίες είναι παραδείγματα των τεχνικών SOFT QoS. (37,38)

9.4 Hard QoS

Το Hard QoS περιγράφει τη διαδικασία κατά την οποία οι συσκευές στο δίκτυο μέσω σηματοδότησης μπορούν να διαπραγματευτούν, να ζητήσουν και να προσαρμόσουν τα επίπεδα προτεραιότητας για διαφορετικούς τύπους κυκλοφορίας, βασισμένες σε προηγούμενα συμφωνηθείσες τιμές. Το Hard QoS περιλαμβάνει πρωτόκολλα όπως το Integrated Services/Resource Reservation Protocol.

9.5 Integrated Services/ Resource Reservation Protocol (RSVP)

Η αρχιτεκτονική ενοποιημένων υπηρεσιών έχει ως λογική το γεγονός ότι η κάθε ροή έχει απόλυτες εγγυήσεις ποιότητας υπηρεσιών, ορίζοντας μηδενική loss probability και συγκεκριμένο ανώτατο όριο για το delay, με την προϋπόθεση πάντα ότι η ροή θα υπακούει σε προκαθορισμένες παραμέτρους.

Το RSVP είναι απλά ένα μονόδρομο (simplex) πρωτόκολλο σηματοδοσίας (signalling) που μεταφέρει αιτήσεις δέσμευσης πόρων για ροές μίας κατεύθυνσης και επιστρέφει μια ένδειξη για την επιτυχή ή αποτυχημένη περάτωση της διαδικασίας στην πλευρά που πραγματοποιεί την αίτηση. Δεν είναι το ίδιο πρωτόκολλο

δρομολόγησης αλλά χρησιμοποιεί τους πίνακες δρομολόγησης όπως έχουν διαμορφωθεί από άλλους μηχανισμούς. (39)

Στο IPV4 η ροή καθορίζεται από τις IP διευθύνσεις πηγής και προορισμού, τα πρωτόκολλα μεταφοράς και τους αριθμούς sockets, ενώ στο IPV6 υπάρχει ειδικό πεδίο για αυτό το σκοπό. Οι ροές αναφέρονται πάντα σε μία κατεύθυνση αλλά σε μια σύνδεση TCP αναφέρονται σε 2 κατευθύνσεις-είναι η ίδια δικατευθυντική. Επομένως κάθε ροή σχετίζεται με μία τιμή TOS (Type Of Service) που σχετίζεται με την ποιότητα υπηρεσίας που απαιτεί.

Η διαδικασία έχει ως εξής: Η εφαρμογή στέλνει αίτημα στο δίκτυο αποστέλλοντας το προφίλ της κίνησής της και τις απαιτήσεις της σε delay και bandwidth, και αν το δίκτυο έχει τους απαραίτητους πόρους για να την προωθήσει απαντά θετικά στο αίτημα αλλιώς το αρνείται. Μόνο αν απαντήσει θετικά όμως στο αίτημα η εφαρμογή θα αρχίσει να στέλνει δεδομένα.

Το πρωτόκολλο που χρησιμοποιείται για τους πόρους είναι το RSVP (Resource Reservation Protocol) που σχεδιάστηκε ειδικά για αυτό το σκοπό. Τα 2 πιο σημαντικά χαρακτηριστικά του είναι ότι υποστηρίζει τη δυναμική μεταβολή ποιότητας των υπηρεσιών μιας συγκεκριμένης ροής πακέτων χωρίς να απαιτείται επανεκκίνηση ή κατάργησή της και ότι η δέσμευση των πόρων δεν γίνεται από την πλευρά του πομπού αλλά από την πλευρά του δέκτη, γεγονός που διευκολύνει την υποστήριξη διαφορετικής ποιότητας υπηρεσιών για τους διάφορους δέκτες αλλά και την ταυτόχρονη συνύπαρξη μεγάλου αριθμού χρηστών. Το πρωτόκολλο αυτό παρόλο που σχεδιάστηκε ειδικά για τις ενοποιημένες υπηρεσίες IntServ, μπορεί να χρησιμοποιηθεί και σε άλλες αρχιτεκτονικές. (40,41,42)

Το πρωτόκολλο αυτό προσφέρει 2 διαφορετικούς τύπους λειτουργίας:

- Εγγυημένο (Guaranteed)

  Παρέχει αυστηρά όρια για το delay και είναι ο πιο κατάλληλο για τις υπηρεσίες πολυμέσων (μεταφορά εικόνας και ήχου) όπου τα πακέτα που καθυστερούν απορρίπτονται.

- Ελεγχόμενου Φορτίου (Controlled Load)

  Είναι αντίστοιχος με τον best effort αλλά αναφέρεται σε μη-φορτωμένο δίκτυο και αφορά εφαρμογές που είναι σχετικά ανεκτό το delay ή το packet loss. Τέτοιες υπηρεσίες είναι οι προσαρμοσμένες υπηρεσίες πραγματικού χρόνου (adaptive-real time apps).

Επομένως, η αρχιτεκτονική αυτή προσφέρει πολύ καλές εγγυήσεις ποιότητας υπηρεσίας αλλά έχει και κάποια σημαντικά μειονεκτήματα:

- Οι μηχανισμοί δέσμευσης πόρων όπως το πρωτόκολλο RSVP εισάγουν επιπλέον φορτίο στο δίκτυο.

- Η αρχιτεκτονική αυτή προσθέτει πολυπλοκότητα στο δίκτυο λόγω του γεγονότος ότι όλοι οι ενδιάμεσοι δρομολογητές πρέπει να αποθηκεύουν πληροφορίες για κάθε ροή ξεχωριστά.

- Στην περίπτωση ροών που είναι μικρής διάρκειας και απαιτούν υψηλή ποιότητα υπηρεσίας είναι ασύμφορη η επιλογή IntServ.

- Το πρωτόκολλο RSVP μπορεί μεν να διασχίζει και δρομολογητές που δεν είναι RSVP αλλά κάτι τέτοιο οδηγεί συνήθως σε υπηρεσία βέλτιστης προσπάθειας.

Το RSVP επιτρέπει στις συσκευές το δικτύου όπως οι δρομολογητές και οι μεταγωγείς να ζητήσουν το απαραίτητο/εγγυημένο εύρος ζώνης από άλλες συσκευές στο δίκτυο για συγκεκριμένο είδος κίνησης (πχ VOIP). Οι επιθυμητές τιμές στην καθυστέρηση μπορούν επίσης να οριστούν σε αυτή την προσέγγιση. Το RSVP στέλνει αίτημα για να κρατήσει συγκεκριμένο εύρος ζώνης ή να κάνει αλλαγή ή προώθηση της δυνατότητας από άλλες συσκευές στο δίκτυο. Αυτή η απαίτηση που αποστέλλεται μέσω του δικτύου καλείται ροή προσδιορισμού. Οι απαιτήσεις μπορούν να οδηγήσουν σε 3 επιθυμητούς τύπους μεταφοράς:

- Ευαίσθητο σε ποσοστό-Το VOIP απαιτεί ένα εγγυημένου bit-rate εύρος ζώνης για εφαρμογές video streaming.

- Ευαίσθητο σε καθυστέρηση-Το VOIP απαιτεί η μέγιστη καθυστέρηση να προσδιοριστεί και να μην επιτρέπεται να ξεπεραστεί το μέγιστό της.

Διαφορές Αρχιτεκτονικών IntServ-DiffServ

IntServ	**DiffServ**
Απόλυτες εγγυήσεις ανά ροή	Μη απόλυτες εγγυήσεις για ομάδες ροών
Πολύπλοκες λειτουργίες σε κάθε δρομολογητή	Σχετική πολυπλοκότητα στους ακραίους δρομολογητές και πιο απλή λειτουργία στους ενδιάμεσους δρομολογητές
Σηματοδοσία από δρομολογητή σε δρομολογητή	Δεν απαιτείται σηματοδοσία, αλλά ρυθμίσεις
Μειωμένη δυνατότητα κλιμάκωσης	Εύκολη κλιμάκωση
Connection Oriented QoS (προσανατολισμένη σε σύνδεση)	Packet Oriented QoS (προσανατολισμένη σε πακέτα)

9.6 QoS vs. CoS

Το QoS χρησιμοποιείται συχνά με το CoS.

Ο διαχωρισμός της κίνησης σε κατηγορίες (traffic classification), κάνει δύο πράγματα δυνατά. Μπορεί να δοθεί προτεραιότητα στα πακέτα ανάλογα με τις ανάγκες μιας συγκεκριμένης εφαρμογής, και συγκεκριμένοι τύποι κίνησης με παρόμοιες απαιτήσεις υπηρεσίας μπορούν να καταταχθούν στο ίδιο σύνολο, έτσι ώστε ο χειρισμός τους να είναι δίκαιος και αποδοτικός. Η δημιουργία του CoS (Class of Service) στην δικτύωση επιβεβαιώνει ότι η κίνηση υψηλής προτεραιότητας, που είναι ευαίσθητη στην καθυστέρηση και στο jitter θα εξυπηρετείται πάντα πριν από την κίνηση χαμηλής προτεραιότητας. (43)

Το CoS ορίζει ομάδες κυκλοφορίας με ένα συγκεκριμένο είδος υπηρεσίας και το QoS διαχειρίζεται αυτόν τον τύπο υπηρεσίας και διαβεβαιώνεται ότι παραδόθηκε. Παρόμοιοι τύποι δεδομένων όπως η φωνή, το live βίντεο ή η ροή βίντεο και η μεταφορά μεγάλων αρχείων μπορούν να ομαδοποιηθούν σε μία κλάση εξυπηρέτησης και να επεξεργαστούν με το ίδιο επίπεδο ποιότητας εξυπηρέτησης.

9.7 Ιεράρχηση QoS IEEE 802.1P στα LANs

Το IEEE 802.1p είναι μια τεχνική σηματοδότησης για την ιεράρχηση της κυκλοφορίας του δικτύου στο data-link/MAC sublayer (OSI Reference Model Layer 2). Η κεφαλίδα IEEE 802.1p περιλαμβάνει ένα πεδίο 3 bit για τον καθορισμό προτεραιοτήτων που επιτρέπει στα πακέτα να ομαδοποιηθούν σε διάφορες κατηγορίες κυκλοφορίας. Οι συμβατοί μεταγωγείς IEEE 802.1p παίρνουν αυτή την ετικέτα (το πακέτο περιλαμβάνει μια κεφαλίδα ετικέτα 32 bit που βρίσκεται μετά τη διεύθυνση επικεφαλίδας πηγής και προορισμού)τη διαβάζουν και βάζουν το πακέτο στη κατάλληλη ουρά προτεραιότητας. Δεν δεσμεύεται εύρος ζώνης για αυτή την τεχνική.

Υπάρχουν 8 επίπεδα προτεραιότητας(0-7) και επομένως μπορούν να δημιουργηθούν 8 ουρές. Το επίπεδο 7 αντιπροσωπεύει την υψηλότερη προτεραιότητα και θα ανατεθεί για κρίσιμες εφαρμογές. Τα επίπεδα 6 και 5 σχεδιάστηκαν για εφαρμογές ευαίσθητες στην καθυστέρηση όπως τα διαδραστικά βίντεο και η φωνή. Τα επίπεδα από 4 και κάτω είναι κατάλληλα για τη μεταφορά των τακτικών δεδομένων των επιχειρήσεων όπως τα βίντεο συνεχούς ροής. Το επίπεδο 0 έχει αναλάβει τη κυκλοφορία που μπορεί να ανταπεξέλθει σε όλα τα μειονεκτήματα ενός πρωτοκόλλου βέλτιστης προσπάθειας.

Το switch θα αναλύσει το πακέτο βασισμένο στην ετικέτα “P” και θα το τοποθετήσει στη κατάλληλη ουρά προτεραιότητας για αποστολή. Ο χρήστης μπορεί να έχει μέχρι 8 ουρές προτεραιότητας. Ένας ρυθμιζόμενος αλγόριθμος χρησιμοποιείται για να επιλέξει πόσα πακέτα θα σταλθούν από κάθε ουρά προτού σταλθούν τα πακέτα με χαμηλή σειρά προτεραιότητας.

Το MAC είναι ένας μετατροπέας που επιτρέπει την απομακρυσμένη διαχείριση του δικτύου. Ένα από τα πολλά χαρακτηριστικά του MAC περιλαμβάνει την υποστήριξη πακέτων 802.1P. Το MAC διαβάζει την ετικέτα 802.1P και τοποθετεί τα εισερχόμενα πακέτα είτε σε χαμηλή είτε σε υψηλή ουρά προτεραιότητας. Ο διαχειριστής δικτύου ορίζει το κατώφλι του επιπέδου προτεραιότητας(0-7) που αποφασίζει πού τοποθετείται το πακέτο. Ο μετατροπέας MAC εφαρμόζει επίσης ένα ρυθμιζόμενο αλγόριθμο για το χρήστη για την επιλογή της ουράς που θα πάει το πακέτο.

Επίσης ο χρήστης μπορεί να ορίσει υψηλή προτεραιότητα σε μια συγκεκριμένη θύρα (για τηλέφωνα IP,κτλ) και αυτό αυτόματα θα τοποθετήσει όλα τα πακέτα σε ουρά υψηλής προτεραιότητας. Εκτός από τις ουρές, ο μετατροπέας MAC επιτρέπει στους χρήστες να ενεργοποιούν, απενεργοποιούν, παύουν εφαρμογές υψηλής προτεραιότητας έτσι ώστε η κυκλοφορία πραγματικού χρόνου να μην σταματά σε περιόδους συμφόρησης.

Όλη η διαχείριση του μετατροπέα γίνεται από ένα λογισμικό SNMP πλήρως συμβατό με τη γραφική διεπαφή χρήστη (GUI) ή μπορεί να γίνει διαδικτυακή διαχείριση χρησιμοποιώντας οποιοδήποτε browser.

Το QoS 802.1P είναι ένα αποτελεσματικό εργαλείο για τον καθορισμό προτεραιοτήτων μέσα σε ένα LAN. Επίσης το QoS μπορεί να συνοδεύεται από προτεραιότητα σε IP ή διαφοροποιημένες υπηρεσίες-οι μηχανισμοί του QoS στο Layer 3 χρησιμοποιούνται για την επίτευξη ιεράρχησης μέσα στο LAN.

Προτεραιότητα IP

Το πρωτόκολλο IP περιλαμβάνει το TOS, ένα πεδίο 8 bit που χρησιμοποιείται για ιεράρχηση πακέτων. Διαθέτει 3 από τα bits του TOS για να δημιουργήσει έως και 8 επίπεδα προτεραιότητας και άλλα 3 bits για να περιγράψει την ευαισθησία της καθυστέρησης και την απώλεια των πακέτων. Ο μετατροπέας MAC είναι διαφανής σε αυτά τα πακέτα. (44)

10. Τεχνοοικονομική Ανάλυση

10.1 OPEX-CAPEX και QoS

Μια επιχείρηση χρειάζεται να λάβει υπόψιν της δύο είδη δαπανών με στόχο να υπολογίσει αθροιστικά όλα τα οικονομικά κόστη και να μπορέσει να καθορίσει τον μελλοντικό σχεδιασμό της βάση των στρατηγικών της. Αυτές οι δαπάνες συμπεριλαμβάνουν το κόστος για την κατασκευή του δικτύου (CAPEX) και το κόστος για τη λειτουργία και τη συντήρηση του δικτύου (OPEX).

Ως CAPEX, ορίζονται οι δαπάνες/ κόστη που σχετίζονται με την κατασκευή ή την επέκταση του πάγιου ενεργητικού (δηλαδή των σταθερών πόρων, όπως για παράδειγμα η υποδομή του δικτύου), οι οποίες υπόκεινται σε μείωση κατά τη διάρκεια της οικονομικής ζωής ενός προγράμματος/ έργου.

Ως OPEX, ορίζονται οι δαπάνες που είναι απαραίτητες για τη διεύθυνση της επιχείρησης ή του εξοπλισμού και αναγκαίες για να διατηρήσουν τις προσφερόμενες υπηρεσίες αδιάλειπτα ενεργές. Αυτές οι δαπάνες δεν προορίζονται για να επεκτείνουν το πάγιο ενεργητικό και δεν υπόκεινται σε μείωση. Μόλις γίνουν, αυτές οι δαπάνες δεν έχουν καμία υπόλοιπη αξία (residual value). (45)

Συγκεκριμένα, το CAPEX αναφέρεται στις κεφαλαιακές δαπάνες της επιχείρησης αναφορικά με τη δικτυακή λειτουργία, οι οποίες περιλαμβάνουν τα αρχικά έξοδα για την αγορά του αναγκαίου εξοπλισμού και την αρχική εγκατάσταση και παραμετροποίηση του δικτύου. Το CAPEX είναι αναγκαίο σε μια επιχείρηση διότι συμβάλλει στη δημιουργία ή και τη βελτίωση των υπηρεσιών που παρέχει μέσω της αγοράς των απαραίτητων συσκευών για την επίτευξη του στόχου τους. Αφορά τον βασικό εξοπλισμό που θα εγκατασταθεί, δηλαδή στην τοποθέτηση μεταγωγών, δρομολογητών, καλωδίωσης κ.τ.λ. Επιπλέον συμπεριλαμβάνει τις εργασίες που πρόκειται να πραγματοποιηθούν για την εγκατάσταση των ανωτέρω εξοπλισμών, δηλαδή τη πληρωμή των εργατών που θα σκάψουν, θα μεταφέρουν τον εξοπλισμό, θα πραγματοποιήσουν τις συγκολλήσεις κτλ.

Η βελτιστοποίηση των κεφαλαιακών δαπανών CAPEX μιας επιχείρησης, επιτυγχάνεται βρίσκοντας τη κατάλληλη μεθοδολογία επιλογής και αγοράς του εξοπλισμού που απαιτείται (μηχανισμών και υπηρεσιών). Με την κατάλληλη ανάλυση ρίσκου και κρισιμότητας, είναι δυνατόν για μια επιχείρηση να υπολογίσει αλλά και να προβλέψει τις δαπάνες που απαιτούνται για τη δημιουργία και εγκατάστασή της, με πολύ υψηλά ποσοστά επιτυχίας.

Το OPEX είναι οι λειτουργικές δαπάνες που αφορούν στη λειτουργία, τη διαχείριση, τη συντήρηση και την ανάπτυξη του δικτύου. Αφορά όλα τα κόστη που δεν συμπεριλαμβάνονται στο CAPEX. Οι δαπάνες αυτές αφορούν αρχικά στο ανθρώπινο δυναμικό όπως την εκπαίδευση των εργαζομένων και τεχνικών της εταιρείας. Επιπλέον, σχετίζονται με την απρόσκοπτη λειτουργία των μηχανημάτων και τη

συντήρηση τους, καθώς και με την άμεση αποκατάσταση των εξαρτημάτων που ίσως υποστούν φθορές.

Η βελτιστοποίηση των λειτουργικών δαπανών OPEX μπορεί να επιτευχθεί με τη σωστή εξισορρόπηση μεταξύ του ανθρώπινου δυναμικού που απαιτείται, και των λειτουργιών της επιχείρησης έτσι ώστε η τελευταία να μειώσει αυτά τα είδη δαπανών στο ελάχιστο. Κάτι τέτοιο μπορεί να πραγματοποιηθεί με καθημερινό έλεγχο των αναγκών της επιχείρησης και με την απομάκρυνση των υπηρεσιών και ατόμων που δεν κρίνονται πλέον απαραίτητα για τη λειτουργία της. Παράλληλα πρέπει να προσδιοριστούν οι συνθήκες κάτω από της οποίες είναι δυνατόν να μειωθούν ή καταργηθούν δεδομένες δαπάνες. Ένα χαρακτηριστικό παράδειγμα είναι η μείωση της κατανάλωσης ενέργειας τις ημέρες όπου αυτό είναι δυνατό, με αποτέλεσμα τη μεγάλη μείωση μη αναγκαίων δαπανών για την εκάστοτε επιχείρηση.

Σημαντικό ρόλο στα δύο παραπάνω είδη δαπανών διαδραματίζει και η ποιότητα των υπηρεσιών QoS που θέλει να προσφέρει μια επιχείρηση. Αυτή θα εξαρτηθεί όχι μόνο από το ποσό που διατίθεται να διαθέσει μια επιχείρηση για τη δημιουργία, τη συντήρηση και την ανάπτυξή της, αλλά και από τα σημεία στα οποία θέλει να εστιάσει και στα οποία θέλει να προσφέρει υψηλότερη ποιότητα. Για παράδειγμα κάποια εταιρεία ίσως θελήσει να εστιάσει περισσότερο στην μείωση της κατανάλωσης ενέργειας με στόχο να μειώσει τα κόστη, ενώ κάποια άλλη μπορεί να θέλει να αυξήσει την ασφάλεια του δικτύου διατηρώντας παράλληλα backup για έκτακτα έξοδα συντήρησης που είναι πιθανόν να προκύψουν. (46,47,48)

10.2 QoS Κλάσεις

Στην εργασία αυτή θεωρούμε τα τοπικά δίκτυα πρόσβασης (ενσύρματα και ασύρματα) ως τμήματα των δικτύων επόμενης γενιάς, στα οποία θα έχουμε ενιαία διαχείριση των προσφερόμενων υπηρεσιών ανεξάρτητα από την τεχνολογία του υποκείμενου δικτύου. Στο πλαίσιο αυτό υιοθετούμε μία γενικευμένη κατηγοριοποίηση των υπηρεσιών σε σχέση με το προσφερόμενο QoS σύμφωνα με το 3GPP TS 23.107 V14.0.0 (2017-03) (Quality of Service (QoS) concept and architecture (Release 14)). Στο specification καθορίζονται τέσσερα (4) διαφορετικά επίπεδα παροχής υπηρεσιών τα οποία διαφοροποιούνται μεταξύ τους ανάλογα με το πόσο ευαίσθητη (delay sensitive) είναι η μετάδοση των δεδομένων στην καθυστέρηση. Η κατηγοριοποίηση αυτή είναι η ακόλουθη:

1. Conversational Class

   Η conversational class είναι η πιο delay sensitive κλάση και αφορά ροές δεδομένων πραγματικού χρόνου. Χαρακτηριστικά της είναι ο χαμηλός χρόνος μεταφοράς, η χαμηλή καθυστέρηση καθώς και η διατήρηση της χρονικής αλληλουχίας. Απαιτεί πολύ περιορισμένο χρονικό περιθώριο για την καθυστέρηση (delay) και τη διακύμανση της καθυστέρησης (jitter). Οι υπηρεσίες σε αυτή την κλάση απαιτούν εγγυημένο ρυθμό μετάδοσης διότι

πρόκειται ουσιαστικά για υπηρεσίες πραγματικού χρόνου όπως είναι οι conference video και VoIP.

2. Streaming Class

   Η streaming class είναι η δεύτερη delay sensitive κλάση για τις ροές δεδομένων και αφορά επίσης ροές δεδομένων πραγματικού χρόνου. Η κύρια διαφορά της από την conversational class έγκειται στο γεγονός ότι οι απαιτήσεις που υπάρχουν για real-time μεταδόσεις είναι μικρότερες. Συγκεκριμένα, το μέγεθος της καθυστέρησης (delay) διαδραματίζει ρόλο μόνο κατά τη διάρκεια της αλληλεπίδρασης με τον διακομιστή, δηλαδή για παράδειγμα όταν ξεκινάει ή σταματάει μια υπηρεσία. Παρόλα αυτά, οι υπηρεσίες σε αυτή την κλάση επίσης απαιτούν εγγυημένο ρυθμό μετάδοσης. Τέτοιες υπηρεσίες είναι οι video και audio streaming.

3. Interactive Class

   Η interactive class είναι η τρίτη delay sensitive κλάση. Οι υπηρεσίες που προσφέρει δεν είναι πραγματικού χρόνου και δεν απαιτούν εγγυημένο ρυθμό μετάδοσης. Τέτοιες υπηρεσίες είναι οι web browsing και το remote control.

4. Background Class

   Η background class είναι η λιγότερο ευαίσθητη κλάση σχετικά με τις ροές δεδομένων. Η διαφορά της με την interactive class έγκειται στο γεγονός ότι η interactive κλάση χρησιμοποιείται για διαδραστικές υπηρεσίες ενώ η background κλάση για background υπηρεσίες όπως για παράδειγμα η λήψη αρχείων. Η background κλάση συνήθως δεν εγγυάται καμία ποιότητα υπηρεσιών (QoS) και προφανώς δεν απαιτεί εγγυημένο ρυθμό μετάδοσης. Παραδείγματα υπηρεσιών είναι οι ηλεκτρονικές διευθύνσεις, η μεταφορά αρχείων και το telemetry-monitoring. (49,50,51)

Πίνακας Χαρακτηριστικών των Κλάσεων

Traffic class	**Conversational class** Conversational RT	**Streaming class** Streaming RT	**Interactive class** Interactive best effort	**Background** Background best effort
Βασικά χαρακτηριστικά	Διατήρηση των διακυμάνσεων του χρόνου βάσει των πληροφοριών που λαμβάνονται από τη ροή Απαιτήσεις χαμηλής καθυστέρησης	Διατήρηση των διακυμάνσεων του χρόνου βάσει των πληροφοριών που λαμβάνονται από τη ροή	Αίτημα απόκρισης Διατήρηση ωφέλιμου περιεχομένου	Δεν υπάρχει απαίτηση άφιξης των δεδομένων σε συγκεκριμένο χρονικό διάστημα Διατήρηση ωφέλιμου περιεχομένου

Εφαρμογές	Εφαρμογές φωνής	Βίντεο συνεχούς ροής	Περιήγηση στο διαδίκτυο	Λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου στο παρασκήνιο

Στην παρακάτω ανάλυση, θα χρησιμοποιήσουμε κάποια παραδείγματα εφαρμογών ανάλογα με το σε ποιά από τις 4 κλάσεις που αναφέρθηκαν παραπάνω αντιστοιχούν. Οι εφαρμογές αυτές είναι οι ακόλουθες:

Ανάλυση Εφαρμογών κλάσεων

- VoIP

  Το VoIP (Voice over IP) περιλαμβάνεται στην conversational class διότι έχει υψηλές απαιτήσεις QoS και συγκεκριμένα πολύ μικρή ανοχή στην καθυστέρηση και στον χρόνο μεταφοράς δεδομένων. Συγκεκριμένα, τίθεται ως περιορισμός ότι η μέγιστη μεταφορά καθυστέρησης θα είναι μικρότερη από 100ms.

- Video Conferecing

  Αντίστοιχα με το VoIP, οι τηλεδιασκέψεις είναι υπηρεσίες πραγματικού χρόνου που απαιτούν ελάχιστη καθυστέρηση στη μεταφορά δεδομένων ώστε να πραγματοποιούνται απρόσκοπτα και χωρίς διακοπές ή απώλειες.

- Streaming Video

  Το streaming video είναι υπηρεσία υψηλής ποιότητας αν και σίγουρα δεν έχει τόσες απαιτήσεις όσο το video τηλεδιασκέψεων λόγω του γεγονότος ότι η καθυστέρηση υπολογίζεται μόνο στην έναρξη ή τη διακοπή της μετάδοσής του. Παρόλα αυτά έχει εξίσου υψηλές απαιτήσεις και απαιτεί εγγυημένο ρυθμό μετάδοσης δεδομένων.

- Streaming Audio

  Παρόμοια με το streaming video, το streaming audio απαιτεί εγγυημένο ρυθμό μετάδοσης δεδομένων και η καθυστέρηση υπολογίζεται στην έναρξη και τη διακοπή της μετάδοσής του.

- Web browsing

  Το web browsing θεωρείται μια διαδραστική υπηρεσία τύπου request-response και επομένως συγκαταλέγεται στην κατηγορία της interactive κλάσης. Η υπηρεσία αυτή δεν είναι real-time και δεν εγγυάται συγκεκριμένο ρυθμό μετάδοσης.

- Remote Control

Η εφαρμογή αυτή χρησιμοποιείται για απομακρυσμένη σύνδεση και δεν έχει ιδιαίτερες απαιτήσεις εφόσον δεν είναι πραγματικού χρόνου.

- File Transfer

  Η μεταφορά αρχείων συγκαταλέγεται στην κλάση background εφόσον πρόκειται για υπηρεσία μη-πραγματικού χρόνου η οποία όμως δεν είναι διαδραστική. Παρουσιάζει ελάχιστα ποσοστά σφάλματος λόγω της αναμετάδοσης σε περιπτώσεις που χαθεί κάποιο αρχείο ή σταλεί σε λάθος προορισμό.

- Email

  Όμοια με τη μεταφορά αρχείων, τα emails είναι μια υπηρεσία ανταλλαγής ψηφιακών μηνυμάτων που παρουσιάζει επίσης ελάχιστα ποσοστά σφάλματος και λειτουργεί με αντίστοιχη λογική.

- Telemetry-Monitoring

  Η υπηρεσία αυτή αφορά στην παρακολούθηση του δικτύου και συγκαταλέγεται επίσης στην background κλάση.

10.2.1 Ανάλυση παραδείγματος

Στην παρακάτω ανάλυση θα εξετάσουμε την προσέγγιση στο θέμα των υπηρεσιών συναρτήσει του κόστους τους. Η ανάλυση θα πραγματοποιηθεί για αναλογία χρηστών 50, 100 και 500 αντίστοιχα με 30% επιπλέον πιθανούς χρήστες συνδεδεμένους στο ασύρματο δίκτυο, δηλαδή 15, 30 και 150 αντίστοιχα.

Η ανάλυση θα πραγματοποιηθεί για 2 περιπτώσεις, στα οποία θα εξεταστεί η τάξη μεγέθους κόστους των υπηρεσιών ανάλογα και με τις 3 κατηγορίες αριθμού χρηστών που αναφέρθηκαν παραπάνω.

Στην πρώτη περίπτωση, θα γίνει ανάλυση χρησιμοποιώντας και τις 4 κατηγορίες κλάσεων (conversational, streaming, interactive και background). Σε αυτό το μέρος, λόγω της conversational κλάσης που προσφέρει υπηρεσίες πραγματικού χρόνου, προσφέρεται υψηλή ποιότητα υπηρεσιών (QoS) και απαιτείται υψηλή ασφάλεια του δικτύου.

Στην δεύτερη περίπτωση, η ανάλυση θα περιοριστεί στις 3 κατηγορίες κλάσεων (streaming, interactive και background). Οι υπηρεσίες αυτές, ελλείψει των υπηρεσιών που περιέχονται στην conversational κλάση, έχουν χαμηλότερες απαιτήσεις και επομένως δεν απαιτούν τόσο υψηλή ποιότητα υπηρεσιών που μπορεί να συνδυαστεί με χαμηλότερες απαιτήσεις ασφάλειας στο σύστημα.

1η περίπτωση

Στο πρώτο μέρος της ανάλυσης θα χρησιμοποιήσω και τις 4 κλάσεις QoS. Με την χρήση της conversational κλάσης, οι οποία είναι η πιο ευαίσθητη από την άποψη της καθυστέρησης μεταφοράς δεδομένων λόγω της χρήσης υπηρεσιών πραγματικού χρόνου, θα απαιτήσουμε υψηλή ποιότητα υπηρεσιών (QoS) καθώς και υψηλή ασφάλεια στο δίκτυο. Οι εφαρμογές που θα χρησιμοποιηθούν και συγκαταλέγονται και στις 4 κλάσεις θα πρέπει να βρίσκονται σε ένα δίκτυο με την κατάλληλη διαμόρφωση ώστε να προσφέρει ταχύτητα, ασφάλεια και δυνατότητα να πραγματοποιούνται υψηλής ποιότητας τηλεδιασκέψεις και κλήσεις VoIP.

Πίνακας Εφαρμογών Κλάσεων

Conversational class	**Streaming class**	**Interactive class**	**Background class**
VoIP, video conferencing	Video streaming, audio streaming	Web browsing, remote control	File transfer, email, telemetry-monitoring

Ανάλογα με τον αριθμό των χρηστών, εξετάστηκε ο εξοπλισμός και οι υπηρεσίες που χρησιμοποιήθηκαν, αναλύθηκαν τα επιμέρους κόστη και εξήχθη το συνολικό τελικό κόστος.

Οι εφαρμογές που επιλέχθηκαν ήταν οι ακόλουθες:

- Σύνδεση παρόχου: Περιλαμβάνει γραμμές μεγάλης ευρυζωνικότητας ανάλογα με τον αριθμό των χρηστών. Επιλέχθηκε η τεχνολογία VDSL η οποία προσφέρει γρηγορότερους ρυθμούς μετάδοσης δεδομένων σε σχέση με το ADSL. Οι μέγιστες ταχύτητες είναι τα 26 Mbps συμμετρικά ή τα 52/12 mbps ασύμμετρα και επιτυγχάνονται σε απόσταση έως 300 μέτρα. Μία άλλη εναλλακτική θα ήταν η μισθωμένη γραμμή η οποία αποτελεί τη βέλτιστη επιλογή από άποψη ταχύτητας, αλλά απορρίφθηκε λόγω του υψηλού κόστους της.

- Antivirus: Επιλέχθηκε ανάλογα με τον αριθμό των συσκευών που καλύπτει και έχει ετήσιο κόστος. Το κόστος αυτό ήταν σχετικά υψηλό με στόχο την καλύτερη προστασία του δικτύου λόγω των παροχών που προσφέρει. Συγκεκριμένα, μπορεί να ελέγχει τη δραστηριότητα των εφαρμογών στο δίκτυο συναρτήσει με τις ρυθμίσεις που έχουν εφαρμοστεί στο firewall. Επιπλέον, προσφέρει μεγαλύτερες ταχύτητες λόγω βελτιστοποιημένης απόδοσης του λογισμικού και της κατανάλωσης των πόρων των υπολογιστών. Επομένως πραγματοποιείται πιο αποτελεσματική ροή κυκλοφορίας, πιο γρήγορη φόρτωση των ιστοσελίδων και των προγραμμάτων καθώς και βελτιστοποιημένες ενημερώσεις και εκκινήσεις εφαρμογών.

- Hardware firewall/IPS-IDS: Το τείχος προστασίας συμβάλλει στην ενίσχυση της ασφάλειας του δικτύου, φιλτράροντας την κίνηση των δεδομένων. Το IPS-IDS είναι built-in μαζί με το τείχος προστασίας, ανιχνεύει τυχόν παραβιάσεις και τις αποτρέπει. Όσον αφορά στο τείχος προστασίας, υπάρχουν δύο επιλογές, το stateless και το statefull firewall. Βασικό χαρακτηριστικό του πρώτου είναι ότι δεν εξετάζει την κατάσταση των συνδέσεων αλλά μόνο τα ίδια τα πακέτα. Συγκεκριμένα παρακολουθεί την κίνηση του δικτύου και περιορίζει ή αποκλείει τα πακέτα βασισμένο στις διευθύνσεις προέλευσης ή προορισμού καθώς και σε άλλες στατικές τιμές. Ουσιαστικά χρησιμοποιεί ένα πολύ απλό σύνολο κανόνων που δεν λαμβάνει υπόψιν του την πιθανότητα ότι πιθανόν να ληφθεί ένα πακέτο που προσποιείται ότι είναι αυτό που είχε ζητηθεί. Από την άλλη πλευρά, το stateful firewall γνωρίζει τις συνδέσεις που περνούν από αυτό. Προσθέτει και διατηρεί πληροφορίες σχετικά με τις συνδέσεις των χρηστών σε ένα πίνακα που αναφέρεται ως πίνακας κατάστασης. Μετά χρησιμοποιεί αυτόν τον πίνακα προκειμένου να εφαρμόσει τις πολιτικές ασφαλείας για τις συνδέσεις των χρηστών. Επιλέχθηκε το stateful firewall διότι λόγω της υψηλής ευαισθησίας του στη καθυστέρηση μπορεί να ανιχνεύει τις ανεπαίσθητες διαφορές των διαφόρων πρωτοκόλλων και να προσαρμόζεται σε αυτά με αποτέλεσμα να προστατεύεται η μετάδοση από καθυστερήσεις. Επιπλέον, το stateful firewall έχει τη δυνατότητα να αποθηκεύει τη κατάσταση της κάθε συνόδου και να κλείνει τη κάθε θύρα όποτε πρέπει με αποτέλεσμα τη καλύτερη και πιο γρήγορη μετάδοση των δεδομένων χωρίς απώλειες.

- Router: οι δρομολογητές επιλέχθηκαν με βάση τον αριθμό των χρηστών που υποστηρίζουν, τα πρωτόκολλα και τις τεχνικές ασφαλείας που χρησιμοποιούν.

  Τα πρωτόκολλα που υποστηρίζουν οι routers είναι τα RIPv1 and RIPv2 (Routing Information Protocol version 1 και 2) και το EIGRP (Enhanced Internet Gateway Routing Protocol).

  Οι δρομολογητές που χρησιμοποιούν το πρωτόκολλο RIP αρχικά αποστέλλουν ένα μήνυμα απαιτώντας να λάβουν τους πίνακες δρομολόγησης από τις γειτονικές συσκευές. Οι γειτονικοί δρομολογητές ανταποκρίνονται με τη σειρά τους στο αίτημα RIP στέλνοντας ολόκληρους τους πίνακες δρομολόγησης πίσω στον αιτούντα, ο οποίος χρησιμοποιεί έναν αλγόριθμο προκειμένου να συγχωνεύει όλες αυτές τις ενημερώσεις στον δικό του πίνακα. Σε τακτά χρονικά διαστήματα, οι δρομολογητές αυτοί στέλνουν περιοδικά τους πίνακες δρομολόγησής τους στους γείτονές τους ώστε να μπορούν να μεταδοθούν οποιεσδήποτε αλλαγές στο δίκτυο.

  Οι δρομολογητές χρησιμοποιούν το πρωτόκολλο EIGRP ως εναλλακτική στο πρωτόκολλο RIP. Το πρωτόκολλο αυτό χρησιμοποιεί classless IP υποδίκτυα και με αυτό τον τρόπο βελτιώνει την αποτελεσματικότητα των πρωτοκόλλων δρομολόγησης. Δεν υποστηρίζει βέβαια ιεραρχίες δρομολόγησης όπως το

πρωτόκολλο RIP αλλά επιτυγχάνει τους στόχους της ευκολότερης διαμόρφωσης καθώς και της καλύτερης απόδοσης.

- Οι τεχνικές ασφαλείας είναι:
  - Το firewall του router, στο οποίο κάθε θύρα (port) θα πρέπει να ελέγχεται.
  - Mac Address Filtering, που δίνει την δυνατότητα να φιλτράρονται οι Mac addresses που προσπαθούν να συνδεθούν και αν υπάρχουν στην λίστα του router τότε τους επιτρέπεται η σύνδεση.
  - SSL VPN (Secure Sockets Layer - Virtual Private Network): Το χαρακτηριστικό αυτό προσθέτει υποστήριξη για απομακρυσμένη πρόσβαση χρηστών. Συγκεκριμένα επιτρέπει στους χρήστες να εγκαθιδρύσουν ένα ασφαλές VPN tunnel χρησιμοποιώντας τον φυλλομετρητή.
  - Υποστήριξη PKI (Public Key Information): Επιτρέπει στους χρήστες να ανταλλάσσουν δεδομένα με ασφάλεια καθώς και να επιβεβαιώνουν την ταυτότητα των άλλων χρηστών.
  - Κρυπτογράφηση AES (Advanced Encryption Standard) έως 256 bits: Η κρυπτογράφηση αυτή είναι η καλύτερη διαθέσιμη κρυπτογράφηση και επιπλέον επιτρέπει τη διαχείριση των κωδικών ασφαλείας των χρηστών.
  - Δυναμική και στατική ασφάλεια θυρών (ports).

- Switches: Επιλέχθηκε συγκεκριμένος τύπος switches τα οποία επιτυγχάνουν ταχύτητες που μπορούν να υποστηρίξουν τον αριθμό των χρηστών προσφέροντας παράλληλα υψηλή ποιότητα.

  Το πρωτόκολλο που επιλέχθηκε για τα switches είναι το STP (Spanning Tree Protocol), το οποίο έχει ως κύριο σκοπό να διασφαλίσει ότι δεν δημιουργούνται βρόχοι όταν υπάρχουν περιττές διαδρομές στο δίκτυο. Επιπλέον τα switches που επιλέχθηκαν είναι managed τα οποία προσφέρουν περισσότερο έλεγχο στην δικτυακή κίνηση και προσφέρουν προηγμένες λειτουργίες για τον έλεγχο αυτής. Μερικές από αυτές τις λειτουργίες είναι:

  - QoS: Δίνει προτεραιότητα στην κίνηση του δικτύου και διαχειρίζεται το διαθέσιμο εύρος έτσι ώστε να εξυπηρετείται η πιο σημαντική κυκλοφορία δεδομένων. Μπορεί να γίνει διαμόρφωση σε ένα switch με την εισαγωγή κανόνων που επιτρέπουν διαφορετικές συσκευές να δώσουν προτεραιότητα σε συγκεκριμένα πακέτα δεδομένων.

- SNMP: Είναι το πρωτόκολλο που δίνει την δυνατότητα για τη διαχείριση και παρακολούθηση του δικτύου. Χρησιμοποιείται για την παρακολούθηση της απόδοσης του δικτύου καθώς και για την επίλυση προβλημάτων του.

- VLANs: Επιτρέπουν στους διαχειριστές να ομαδοποιούν συσκευές μαζί χωρίς να χρειάζεται να έχουν καινούργια καλώδια ή να κάνουν αλλαγές στην δομή του δικτύου. Τα VLANs βοηθούν στην μείωση της περιττής κυκλοφορίας και επιτρέπουν στους διαχειριστές του δικτύου να εφαρμόζουν πρόσθετα μέτρα ασφαλείας στις επικοινωνίες του δικτύου.

- DoS Protection: Προλαμβάνει τις επιθέσεις DoS (Denial Of Service)

- Ασφάλεια θυρών: Προσφέρει τη δυνατότητα να κλειδωθούν οι Mac διευθύνσεις στις θύρες και με αυτό τον τρόπο περιορίζει τον αριθμό τους και παρέχει μεγαλύτερη ασφάλεια.

- Αποφυγή συμφόρησης: Ένας TCP (Transmission Control Protocol) αλγόριθμος αποφυγής συμφόρησης είναι απαραίτητος για να μειώσει και να εμποδίσει τις απώλειες εξαιτίας ελλείψεων συγχρονισμού.

- Remote Access: Ανάλογα με τον αριθμό των επιπλέον χρηστών που θα συνδέονται από το ασύρματο δίκτυο, έχουμε προμηθευτεί access points τα οποία παρέχουν ασφάλεια και υψηλή ταχύτητα στη σύνδεσή τους (WPA, WPA2). Στην περίπτωση αυτή επιλέχθηκε WPA2 κωδικοποίηση διότι συνοδεύεται με το πρωτόκολλο CCMP (που είναι βασισμένο στο πρωτόκολλο AES) το οποίο είναι πιο δύσκολο να παραβιαστεί σε σχέση με το πρωτόκολλο TKIP που υποστηρίζει η κωδικοποίηση WPA.

  Τα βασικά χαρακτηριστικά που επιλέχθηκαν είναι τα ακόλουθα:

  - DFS (Dynamic Frequency Selection): Είναι ένας μηχανισμός που επιτρέπει σε μία συσκευή χωρίς άδεια να ανιχνεύσει τη παρουσία ενός συστήματος στο κανάλι που χρησιμοποιεί και αν το επίπεδο του είναι πάνω από ένα καθορισμένο όριο, να εγκαταλείπει αυτό το κανάλι και να επιλέγει ένα εναλλακτικό.

  - Forwarding DMZ (Demilitarized Zone): Αποτελεί μία μέθοδο ασφαλείας που διαχωρίζει το τοπικό δίκτυο (LAN) από τα υπόλοιπα μη ασφαλή δίκτυα. Αυτό δημιουργεί μία επιπλέον δικλείδα ασφαλείας αφού εμποδίζει τους μη εξουσιοδοτημένους χρήστες να αποκτήσουν απευθείας πρόσβαση στο δίκτυο.

  - WDS (Wireless Distribution System): Είναι ένα σύστημα που επιτρέπει την ασύρματη επικοινωνία των σημείων πρόσβασης σε ένα

δίκτυο. Του επιτρέπει να επεκταθεί χρησιμοποιώντας πολλά σημεία πρόσβασης χωρίς να απαιτείται ενσύρματη καλωδίωση.

- IP και MAC Binding: Επιτρέπει την κατοχύρωση στατικών διευθύνσεων για ένα πελάτη. Υποστηρίζει μέγιστο όριο 32 καταχωρήσεων.

- VoIP: Επιλέχθηκαν συσκευές οι οποίες παρέχουν υψηλή ποιότητα στις κλήσεις και στα βίντεο. Τα χαρακτηριστικά που παρουσιάζουν είναι τα ακόλουθα:

  - CDP (Cisco Discovery Protocol): Το πρωτόκολλο αυτό χρησιμοποιείται για τον διαμοιρασμό πληροφοριών μεταξύ όλων των συσκευών Cisco σχετικά με την έκδοση του λειτουργικού συστήματος και τις διευθύνσεις IP. Επιλέχθηκαν συσκευές Cisco διότι παρέχουν ασφάλεια και αξιοπιστία σε όλους τους τύπους κίνησης στο δίκτυο, παρέχοντας παράλληλα συνεπή και συνεχή παροχή υπηρεσιών σε όλους τους χρήστες.

  - Πιστοποιητικά: Απαραίτητα για την ομαλή λειτουργία των συσκευών VoIP.

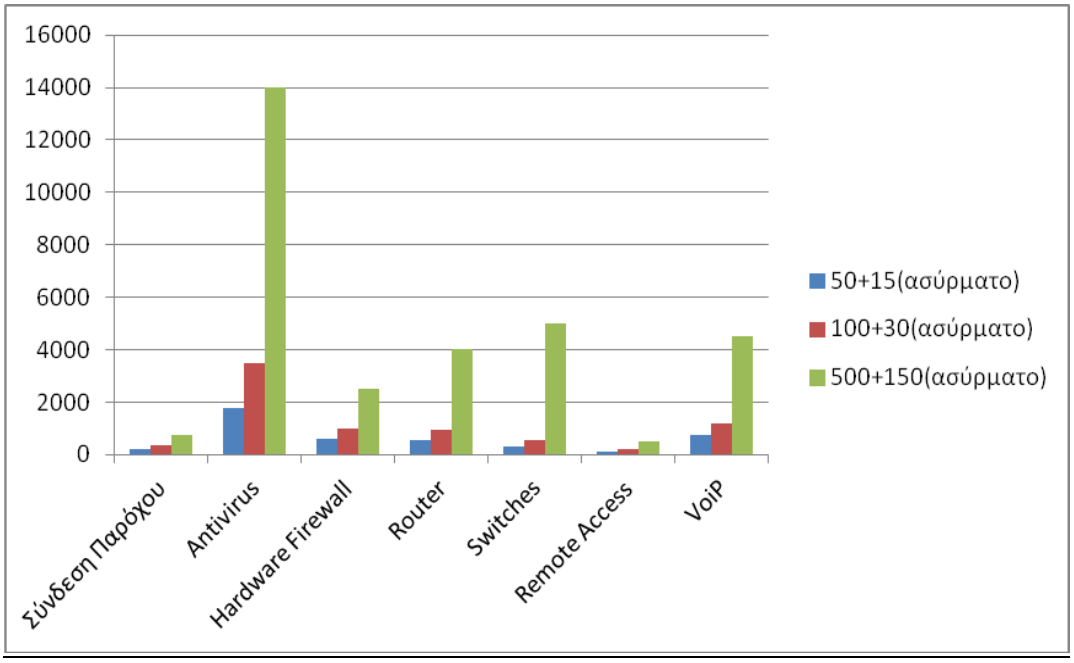
  - Κρυπτογράφηση με τη χρήση του SRTP (Secure Real – Time Transfer Protocol): Παρέχει κρυπτογράφηση, πιστοποίηση ταυτότητας και επιβεβαίωση της σωστής αποστολής των μηνυμάτων τόσο στις unicast όσο και στις multicast εφαρμογές.

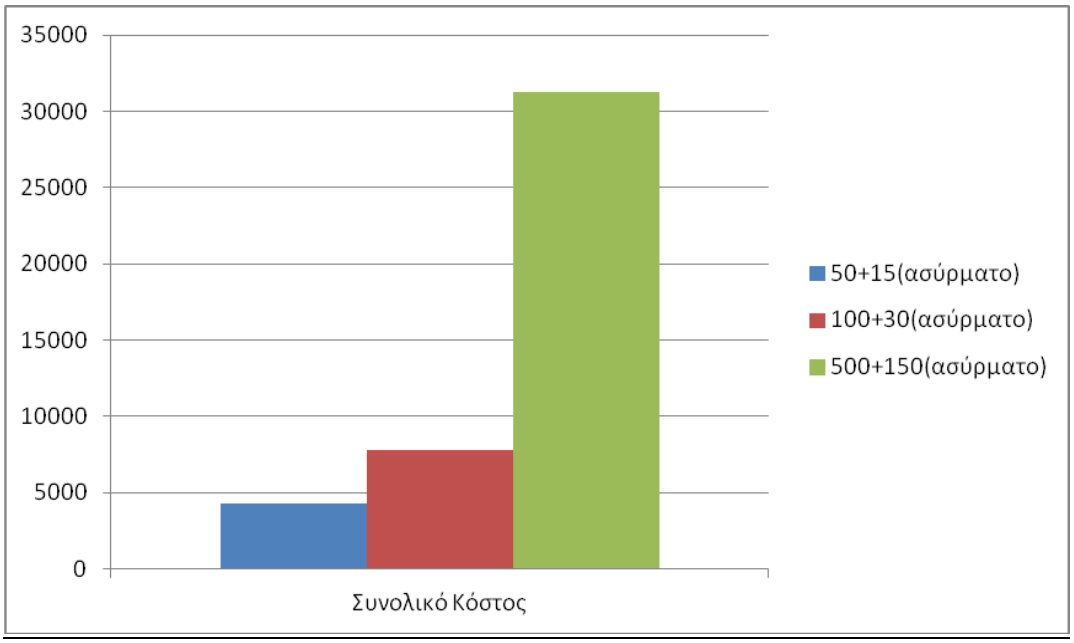
  - Κρυπτογράφηση σήματος με τη χρήση του TLS (Transport Layer Security): Η κρυπτογράφηση αυτή παρέχει ιδιωτικότητα και ακεραιότητα των δεδομένων που στέλνονται καθώς και αυθεντικοποίηση των χρηστών.

  - Κρυπτογραφημένα αρχεία ρυθμίσεων: Απαραίτητη συνθήκη ώστε να διασφαλιστεί ότι δεν θα αλλάξουν οι ρυθμίσεις των αρχείων από κάποιο μη εξουσιοδοτημένο χρήστη.

Εξοπλισμός/Υπηρεσίες	**Αριθμός χρηστών**		
	50+15(ασύρματο)	**100+30(ασύρματο)**	**500+150(ασύρματο)**
Σύνδεση Παρόχου	4 VDSL Γραμμές - 200€	7 VDSL Γραμμές 350€ / Μισθωμένη Γραμμή	15 VDSL Γραμμές - 750€/ Μισθωμένη Γραμμή
Antivirus	1.760€/χρόνο	3.500€/χρόνο	14.000€/χρόνο
Hardware Firewall	600€	1.000€	2.500€

IPS-IDS			
Router	550€	950€	4.000€
Switches	1 switch(48 port)+1 switch (8 port) - 300€	2 switch(48 port)+1 switch(8 port) - 550€	11switch(48 port) – 5.000€
Remote Access	1 Access Point - 100€	2 Access Points- 200€	5 Access Points - 500€
VoIP	5 συσκευές-750€	8 συσκευές- 1.200€	30 συσκευές- 4.500€
Συνολικό Κόστος	≈ 4.300€	≈ 7.800€	≈ 31.300€





2η περίπτωση

Στην δεύτερη περίπτωση της ανάλυσης θα χρησιμοποιήσω μόνο τις 3 κλάσεις QoS και συγκεκριμένα τις streaming, interactive και background κλάσεις. Η απουσία της conversational κλάσης η οποία περιλαμβάνει εφαρμογές με υψηλή ευαισθησία στις καθυστερήσεις και υψηλές απαιτήσεις ποιότητας και ασφάλειας του δικτύου, μου επιτρέπει να επιλέξω εξοπλισμό και υπηρεσίες τα οποία δεν έχουν τόσο υψηλό κόστος και απαιτήσεις για τους χρήστες.

Streaming class	Interactive class	Background class
Video streaming, audio streaming	Web browsing, remote control	File transfer, email, telemetry-monitoring

Ανάλογα με τον αριθμό των χρηστών, εξέτασα τους εξοπλισμούς και τις υπηρεσίες που χρησιμοποιήθηκαν, ανέλυσα τα επιμέρους κόστη και εξήγαγα το συνολικό τελικό κόστος.

Οι εφαρμογές που επιλέχθηκαν ήταν οι ακόλουθες:

- Σύνδεση παρόχου: Περιλαμβάνει γραμμές VDSL μεγάλης ευρυζωνικότητας ανάλογα με τον αριθμό των χρηστών. Σε σύγκριση με το πρώτο μέρος της ανάλυσης, επιλέχθηκε μικρότερος αριθμός γραμμών ανάλογα με τον αριθμό των χρηστών εφόσον οι απαιτήσεις δεν είναι τόσο υψηλές. Μια άλλη εναλλακτική είναι η χρήση της ADSL, ωστόσο θα χρειαστεί μεγαλύτερος αριθμός γραμμών.

- Antivirus: Επιλέχθηκε δωρεάν antivirus εφόσον δεν υπάρχουν ιδιαίτερα υψηλές απαιτήσεις για την ασφάλεια του δικτύου. Το δωρεάν antivirus παρέχει το βασικό πακέτο κάλυψης στο δίκτυο και προστασίας από κακόβουλες επιθέσεις χωρίς τη δυνατότητα τεχνικής υποστήριξης σε περίπτωση προβλήματος.

- Hardware firewall/IPS-IDS: Το τείχος προστασίας συμβάλλει στην ενίσχυση της ασφάλειας του δικτύου, φιλτράροντας την κίνηση των δεδομένων. Το IPS-IDS είναι built-in μαζί με το τείχος προστασίας, ανιχνεύει τυχόν παραβιάσεις και τις αποτρέπει. Σε σχέση με το πρώτο μέρος της ανάλυσης, εδώ επιλέχθηκε stateless firewall διότι ελλείψει της κλάσης Conversational που παρουσιάζει πολύ υψηλές απαιτήσεις, το firewall αυτό επαρκεί για να παρακολουθεί τη κυκλοφορία του δικτύου και να περιορίζει ή να αποκλείει τα πακέτα με βάση τις διευθύνσεις προέλευσης, προορισμού ή με άλλες στατικές τιμές. Δεν είναι επομένως αναγκαία η ύπαρξη stateful firewall που να προσαρμόζεται δυναμικά στα διάφορα πρωτόκολλα εφόσον δεν υπάρχουν ιδιαίτερα υψηλές απαιτήσεις βάση των εφαρμογών που χρησιμοποιούνται.

- Router: Τα router επιλέχθηκαν με βάση τον αριθμό των χρηστών που υποστηρίζουν και με τις τεχνικές ασφαλείας που χρησιμοποιούν. Επίσης επιλέχθηκαν routers με χαμηλότερο κόστος για τους λόγους που αναφέρθηκαν παραπάνω.

  Τα πρωτόκολλα που υποστηρίζουν τα routers είναι τα RIPv1 and RIPv2 (Routing Information Protocol version 1 και 2)

  Οι δρομολογητές που χρησιμοποιούν το πρωτόκολλο RIP αρχικά αποστέλλουν ένα μήνυμα απαιτώντας να λάβουν τους πίνακες δρομολόγησης από τις γειτονικές συσκευές. Οι γειτονικοί δρομολογητές ανταποκρίνονται με τη σειρά τους στο αίτημα RIP στέλνοντας ολόκληρους τους πίνακες δρομολόγησης πίσω στον αιτούντα, ο οποίος χρησιμοποιεί έναν αλγόριθμο προκειμένου να συγχωνεύσει όλες αυτές τις ενημερώσεις στον δικό του πίνακα. Σε τακτά χρονικά διαστήματα, οι δρομολογητές αυτοί στέλνουν περιοδικά τους πίνακες δρομολόγησής τους στους γείτονές τους ώστε να μπορούν να μεταδοθούν οποιεσδήποτε αλλαγές στο δίκτυο.

- Οι τεχνικές ασφαλείας είναι:

    - Το firewall του router, στο οποίο κάθε θύρα (port) θα πρέπει να ελέγχεται.

    - Mac Address Filtering, που δίνει την δυνατότητα να φιλτράρονται οι Mac addresses που προσπαθούν να συνδεθούν και αν υπάρχουν στην λίστα του router τότε τους επιτρέπεται η σύνδεση.

    - Δυναμική και στατική ασφάλεια θυρών (ports).

- Switches: Επιλέχθηκε ίδιος αριθμός switches τα οποία επιτυγχάνουν ταχύτητες που μπορούν να υποστηρίξουν τον αριθμό των χρηστών, αντίστοιχα με το πρώτο μέρος της ανάλυσης. Σε αυτήν την περίπτωση χρησιμοποιήσαμε unmanaged switches, διότι είναι εύκολα στην χρήση (plug and play) και είναι ήδη παραμετροποιημένα. Η διαφορά τους με τα managed έγκειται στο κόστος τους το οποίο είναι χαμηλότερο καθώς και στο ότι δεν γίνεται να αλλάξουν οι ρυθμίσεις τους με αποτέλεσμα να μην μπορούν να παραμετροποιηθούν κατάλληλα για τις ανάγκες του δικτύου.

  Το πρωτόκολλο που επιλέχθηκε για τα switches είναι το STP (Spanning Tree Protocol), το οποίο έχει ως κύριο σκοπό να διασφαλίσει ότι δεν δημιουργούνται βρόχοι όταν υπάρχουν περιττές διαδρομές στο δίκτυο. Επιπλέον τα switches που επιλέχθηκαν είναι managed τα οποία προσφέρουν περισσότερο έλεγχο στην δικτυακή κίνηση και προσφέρουν προηγμένες λειτουργίες για τον έλεγχο αυτής. Επιλέχθηκαν οι βασικές λειτουργίες οι οποίες είναι:

  - SNMP: Είναι το πρωτόκολλο που δίνει την δυνατότητα για τη διαχείριση και παρακολούθηση του δικτύου. Χρησιμοποιείται για την παρακολούθηση της απόδοσης του δικτύου καθώς και για την επίλυση προβλημάτων του.

  - VLANs: Επιτρέπουν στους διαχειριστές να ομαδοποιούν συσκευές μαζί χωρίς να χρειάζεται να έχουν καινούργια καλώδια ή να κάνουν αλλαγές στην δομή του δικτύου. Τα VLANs βοηθούν στην μείωση της περιττής κυκλοφορίας και επιτρέπουν στους διαχειριστές του δικτύου να εφαρμόζουν πρόσθετα μέτρα ασφαλείας στις επικοινωνίες του δικτύου.

  - Ασφάλεια θυρών: Προσφέρει τη δυνατότητα να κλειδωθούν οι Mac διευθύνσεις στις θύρες και με αυτό τον τρόπο περιορίζει τον αριθμό τους και παρέχει μεγαλύτερη ασφάλεια.

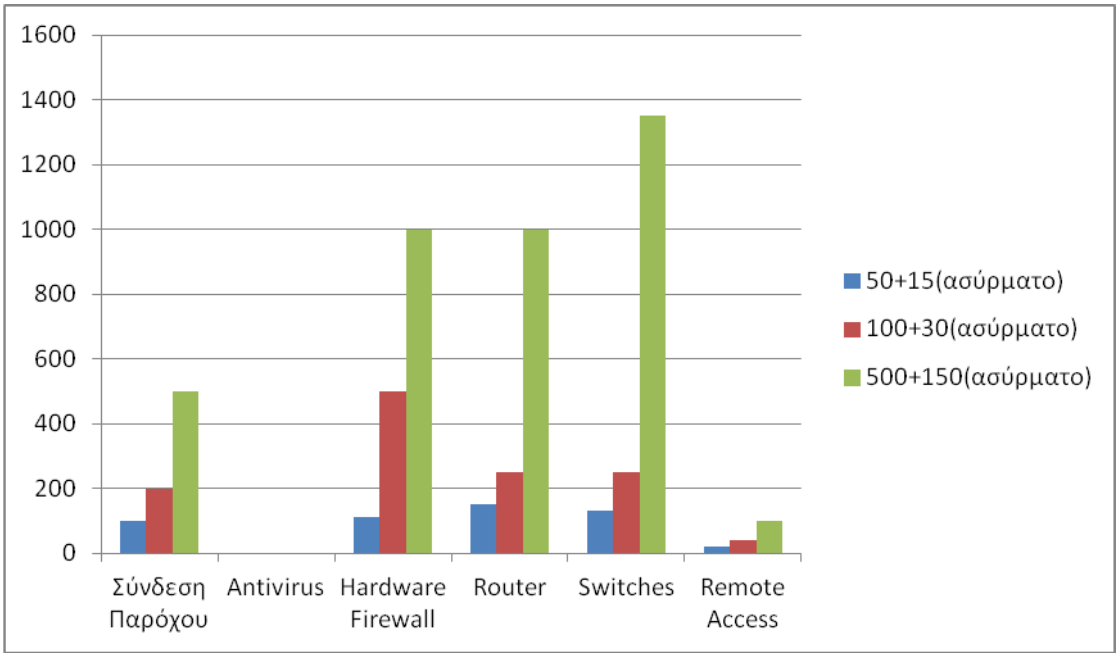
- Remote Access: Ανάλογα με τον αριθμό των επιπλέον χρηστών που θα συνδέονται από το ασύρματο δίκτυο, έχουμε προμηθευτεί access points τα οποία παρέχουν ασφάλεια και υψηλή ταχύτητα στη σύνδεσή τους. Στην περίπτωση αυτή και επειδή δεν απαιτείται τόσο υψηλή ασφάλεια, επιλέχθηκε η κωδικοποίηση WPA που περιλαμβάνει το πρωτόκολλο TKIP.

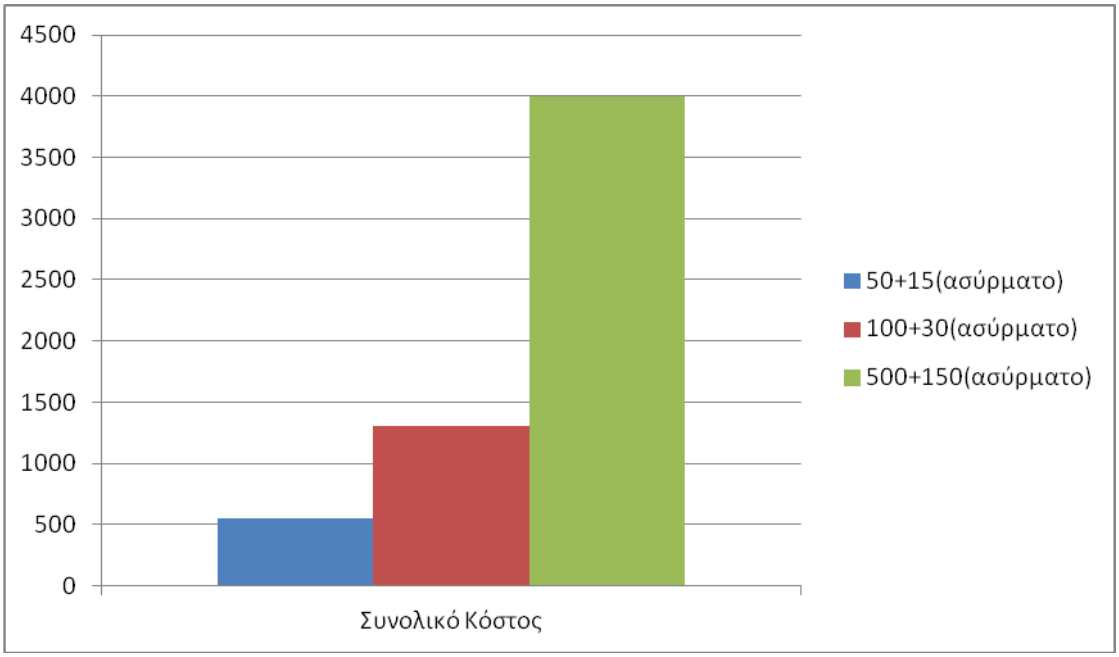
  Τα βασικά χαρακτηριστικά που επιλέχθηκαν είναι τα ακόλουθα:

  - DFS (Dynamic Frequency Selection): Είναι ένας μηχανισμός που επιτρέπει σε μία συσκευή χωρίς άδεια να ανιχνεύσει τη παρουσία ενός συστήματος στο κανάλι που χρησιμοποιεί και αν το επίπεδο του είναι πάνω από ένα καθορισμένο όριο, να εγκαταλείπει αυτό το κανάλι και να επιλέγει ένα εναλλακτικό.

- Forwarding DMZ (Demilitarized Zone): Αποτελεί μία μέθοδο ασφαλείας που διαχωρίζει το τοπικό δίκτυο (LAN) από τα υπόλοιπα μη ασφαλή δίκτυα. Αυτό δημιουργεί μία επιπλέον δικλείδα ασφαλείας αφού εμποδίζει τους μη εξουσιοδοτημένους χρήστες να αποκτήσουν απευθείας πρόσβαση στο δίκτυο.
- WDS (Wireless Distribution System): Είναι ένα σύστημα που επιτρέπει την ασύρματη επικοινωνία των σημείων πρόσβασης σε ένα δίκτυο. Του επιτρέπει να επεκταθεί χρησιμοποιώντας πολλά σημεία πρόσβασης χωρίς να απαιτείται ενσύρματη καλωδίωση.
- IP και MAC Binding: Επιτρέπει την κατοχύρωση στατικών διευθύνσεων για ένα πελάτη. Υποστηρίζει μέγιστο όριο 32 καταχωρήσεων.

Εξοπλισμός/Υπηρεσίες	**Αριθμός χρηστών**		
	50+15(ασύρματο)	**100+30(ασύρματο)**	**500+150(ασύρματο)**
Σύνδεση Παρόχου	2 VDSL /5ADSL Γραμμές - 100€	4 VDSL/10 ADSL Γραμμές - 200€	10 VDSL/25 ADSL Γραμμές - 500€
Antivirus	Free Antivirus	Free Antivirus	Free Antivirus
Hardware Firewall	110€	500€	1.000€
IPS-IDS			
Router	150€	250€	1.000€
Switches	1 switch(48 port)+1 switch (8 port) - 130€	2 switch(48 port)+1 switch(8 port) - 250€	11 switch(48 port) – 1.350€
Remote Access	1 Access Point - 20€	2 Access Points-40€	5 Access Points - 100€
Συνολικό Κόστος	≈ 550€	≈ 1.300€	≈ 4.000€





10.2.2 Πρόταση μεθοδολογίας επιλογής αντίστοιχων μηχανισμών

Μια επιχείρηση χρειάζεται να λάβει υπόψιν της δύο είδη δαπανών με στόχο να υπολογίσει τα συνολικά οικονομικά κόστη και να καθορίσει τον οικονομικό της σχεδιασμό. Αυτές οι δαπάνες περιλαμβάνουν το κόστος για την κατασκευή του δικτύου (CAPEX) και το κόστος για τη λειτουργία και τη συντήρηση του δικτύου (OPEX). Τα δύο αυτά οικονομικά μεγέθη είναι καθοριστικά για τον υπολογισμό του συνολικού κόστους και αποτελούν τη βάση πάνω στην οποία θα στηριχθεί η μεθοδολογία επιλογής των αντίστοιχων μηχανισμών.

Στη παρούσα μελέτη θεωρήσαμε ενιαία τη διαχείριση των προσφερόμενων υπηρεσιών ανεξάρτητα από τη τεχνολογία του δικτύου. Η τεχνοοικονομική ανάλυση υποδιαιρέθηκε σε δύο περιπτώσεις και χρησιμοποιήθηκε η κατηγοριοποίηση υπηρεσιών 3GPP, σύμφωνα με την οποία καθορίζονται 4 διαφορετικά επίπεδα υπηρεσιών (conversational, streaming, interactive και background), τα οποία διαφοροποιούνται ανάλογα με το επίπεδο ευαισθησίας των δεδομένων στην καθυστέρηση.

Η πρώτη περίπτωση συμπεριέλαβε και τα 4 επίπεδα υπηρεσιών και επομένως το τελικό συνολικό κόστος καθορίστηκε από μεγαλύτερη οικονομική ευελιξία, επιτρέποντάς μας να επιλέξουμε τεχνολογίες και υπηρεσίες με μεγαλύτερα κόστη. Η δεύτερη περίπτωση συμπεριέλαβε 3 επίπεδα υπηρεσιών εξαιρώντας αυτό που αφορά σε υπηρεσίες με τη μέγιστη ευαισθησία στην καθυστέρηση (απουσίασε η conversational class) και περιλαμβάνει το VoIP και video conferencing. Αυτή η διαφοροποίηση οδήγησε στην απαίτηση για χαμηλότερη ποιότητα υπηρεσιών και επομένως οι μηχανισμοί που επιλέχθηκαν δεν ήταν απαραίτητο να είναι αντίστοιχης ποιότητας με τη πρώτη περίπτωση, επιτρέποντάς μας να μειώσουμε το τελικό συνολικό κόστος.

Επιπρόσθετα, μία επιχείρηση, ανάλογα με το μέγεθός της, τα άτομα που απασχολεί καθώς και τον αριθμό των χρηστών, είναι λογικό να παρουσιάζει διαφορές τόσο στην ποσότητα, όσο και στην ποιότητα των μηχανισμών που θα επιλέξει προκειμένου να είναι πλήρως λειτουργική. Επομένως, η επιλογή των εξαρτημάτων καθώς και το συνολικό κόστος τους μεταβάλλεται ανάλογα με τα παραπάνω χαρακτηριστικά. Στις 2 παραπάνω περιπτώσεις που μελετήσαμε, ο αριθμός των χρηστών καθόρισε σε πολύ μεγάλο βαθμό τις επιλογές που πραγματοποιήσαμε.

Τέλος, σημαντικό ρόλο στην επιλογή των μηχανισμών που επιλέχθηκαν καθόρισαν οι οικονομικές δυνατότητες της επιχείρησης. Στις 2 παραπάνω περιπτώσεις που μελετήθηκαν θεωρήθηκε ότι οι οικονομικές δυνατότητές των επιχειρήσεων ήταν στο ίδιο επίπεδο οπότε δεν αποτέλεσαν μεταβλητά μεγέθη που επηρέασαν την τελική επιλογή.

Η μεθοδολογία μείωσης του συνολικού κόστους καθορίστηκε συναρτήσει των 2 αναλύσεων κόστους CAPEX και OPEX, για κάθε περίπτωση ξεχωριστά, και παράλληλα λαμβάνοντας υπόψιν την κατηγοριοποίηση υπηρεσιών 3GPP για την κάθε περίπτωση καθώς και το μέγεθος και τις οικονομικές δυνατότητες της κάθε επιχείρησης. Το συνολικό κόστος προσδιορίστηκε από τις ανωτέρω παραμέτρους και παρουσιάστηκε στη προηγούμενη παράγραφο. (52)

10.2.2.1 Ανάλυση κόστους τοπικών δικτύων υπολογιστών (LANs)

Η κατασκευή και η λειτουργία ενός τοπικού δικτύου υπολογιστών, αποτελούν ένα δύσκολο έργο, ιδιαίτερα σε μεγάλης έκτασης δίκτυα όπου το κόστος είναι αρκετά υψηλό και ο σχεδιασμός της αρχιτεκτονικής του δικτύου παρουσιάζει πολύ υψηλές απαιτήσεις. Πολλοί συντελεστές μπορούν να θεωρηθούν ασήμαντοι και να μη

ληφθούν υπόψη, γεγονός που μπορεί να οδηγήσει σε σημαντικές αστοχίες και παραλείψεις. Για το λόγο αυτό είναι απαραίτητη η όσο το δυνατόν πιο λεπτομερής περιγραφή των περισσότερων παραγόντων που περιλαμβάνονται σε μία επιχείρηση.

Τα δύο βασικά μέρη ενός δικτύου είναι τα έσοδα και τα έξοδα, με το βασικό κανόνα να αποτελεί ότι τα έσοδα πρέπει να ξεπερνούν τα έξοδα. Ένα κύριο ζήτημα αποτελεί το γεγονός ότι ενώ τα έξοδα σε μία επιχείρηση είναι κατά κανόνα προβλέψιμα εφόσον προκαθορίζονται από την ίδια την επιχείρηση και υπολογίζονται εκ των προτέρων, τα έσοδα δεν μπορούν να προβλεφθούν ποτέ επακριβώς διότι εξαρτώνται από τους εκάστοτε χρήστες .

Οι 3 βασικοί άξονες που καθορίζουν τα έσοδα και τα έξοδα ενός τοπικού δικτύου είναι οι ακόλουθοι:

- Υποδομή του δικτύου: Αποτελεί όλα τα υλικά που θα χρησιμοποιηθούν για τη εγκατάσταση του δικτύου και τη μετάδοση των δεδομένων (καλώδια, αγωγοί, switches, routers, κ.τ.λ.).
- Παροχή υπηρεσιών: Αποτελεί όλες τις υπηρεσίες που παρέχονται από μια επιχείρηση ανάλογα με το αντικείμενό της.
- Χρήστες του δικτύου: Αποτελούν τους τελικούς χρήστες οι οποίοι εργάζονται στην επιχείρηση ή διαθέτουν δικαιώματα πρόσβασης σε αυτή.

10.2.2.2 Ανάλυση κόστους CAPEX και OPEX

Οι σημαντικότεροι παράγοντες που διαμορφώνουν το κόστος CAPEX για την εγκατάσταση ενός νέου τοπικού δικτύου, αφορούν στα αρχικά κόστη για τις οικοδομικές εργασίες που απαιτούνται, καθώς και την αγορά των αγωγών και των καλωδίων. Ανάλογα με το μέγεθος της επιχείρησης αλλά και την τοποθεσία της (αστικό ή αγροτικό περιβάλλον), το συνολικό κόστος ανάπτυξης αυξάνεται, διότι απαιτείται υψηλότερο CAPEX.

Τα ζητήματα στα οποία οφείλουμε να εστιάσουμε προκειμένου να διατηρήσουμε το CAPEX σε χαμηλά επίπεδα, είναι τα ακόλουθα:

- Προσεκτικός σχεδιασμός του δικτύου.
- Χρήση κατάλληλων και συμφερουσών τεχνολογιών.
- Χρήση του δικτύου σε όσο το δυνατόν μεγαλύτερο ποσοστό από το σύνολο των χρηστών.
- Χρήση ασφαλών πολιτικών κατά τη διάρκεια της εγκατάστασης.

Τα έξοδα λειτουργίας (OPEX) περιλαμβάνουν τα έξοδα για τη μισθοδοσία, τη συντήρηση, την παροχή ηλεκτρικής ενέργειας, το κόστος συντήρησης χώρων κ.τ.λ. Ανάλογα με το μέγεθος της επιχείρησης καθώς και τον ήδη εγκατεστημένο εξοπλισμό, τα έξοδα OPEX διαφοροποιούνται και μεταβάλλουν το συνολικό κόστος.

Τα ζητήματα στα οποία οφείλουμε να εστιάσουμε προκειμένου να διατηρήσουμε το OPEX σε χαμηλά επίπεδα, είναι τα ακόλουθα:

- Χρήση εξοπλισμού υψηλής διάρκειας ζωής.
- Χαμηλή κατανάλωση ενέργειας.
- Χρήση outsourcing δηλαδή συμφωνίας της επιχείρησης με κάποια άλλη επιχείρηση ή οργανισμό για την εκτέλεση εκ μέρους τους κάποιων από τις εργασίες (π.χ. συντήρηση).

Τα έξοδα CAPEX και OPEX πρέπει να διατηρηθούν στα όσο δυνατόν χαμηλότερα δυνατά επίπεδα. Ο στόχος αυτός θα επιτευχθεί με μια επιχειρησιακή μεθοδολογία που στοχεύει στη βελτίωση της πορείας ανάπτυξης του έργου αυτού, λαμβάνοντας υπόψιν όλες τις σχετικές παραμέτρους. (53)

10.2.2.3 Μεθοδολογία επιλογής μηχανισμών

Το πλαίσιο της οικονομικής μοντελοποίησης περιλαμβάνει βελτιστοποίηση τόσο των κεφαλαιακών (CAPEX) όσο και των επενδυτικών εξόδων (OPEX) για τις τεχνολογικές επιλογές που είναι εφαρμόσιμες στα τοπικά δίκτυα υπολογιστών. Με βάση την ανωτέρω ανάλυση, καταλήξαμε στην ακόλουθη πρόταση μεθοδολογίας επιλογής μηχανισμών, η οποία στην ανάλυση παραδείγματος που πραγματοποιήσαμε μεταβλήθηκε ανάλογα με τον αριθμό των χρηστών και την κατηγοριοποίηση των υπηρεσιών 3GPP.

1. Σύνδεση παρόχου

   Οι επιλογές που υπάρχουν για σύνδεση παρόχου είναι πολλές, αλλά, αναλόγως με τις ανάγκες μίας επιχείρησης, μπορούμε να επιλέξουμε τον κατάλληλο πάροχο. Εάν οι απαιτήσεις δεν είναι ιδιαίτερα υψηλές, θα επιλέξουμε γραμμή ADSL – VDSL που υπόσχεται μία καλή απόδοση στο δίκτυο. Εάν οι απαιτήσεις είναι υψηλές, μπορούμε να διαλέξουμε μία μισθωμένη γραμμή χωρίς καθυστερήσεις, με στόχο τη σταθερή απόδοση του δικτύου. Η επιλογή της οπτικής ίνας δεν είναι ακόμα διαθέσιμη στην Ελλάδα, οπότε δεν λαμβάνεται υπόψιν.

2. Antivirus

   Ανάλογα με τις απαιτήσεις ποιότητας υπηρεσιών, επιλέγουμε είτε αγορά αδειών σε antivirus, η οποία παρέχει υψηλότερη ασφάλεια και υποστήριξη των χρηστών, είτε free antivirus το οποίο παρέχει τη βασική προστασία.

3. Hardware firewall/ IPS - IDS

   Το τείχος προστασίας επιλέγεται με βάση το επίπεδο ασφαλείας που θέλουμε στο δίκτυο. Υπάρχουν 2 είδη firewall, το stateless και το stateful firewall. Το πρώτο είδος firewall συνήθως επιλέγεται εάν δεν έχουμε ιδιαίτερες απαιτήσεις ασφαλείας, ενώ το δεύτερο όταν θέλουμε να αποθηκεύουμε τη παραμικρή αλλαγή στη κατάσταση σύνδεσης των χρηστών. Είναι προφανές ότι το stateful firewall κοστίζει υψηλότερα, αυξάνοντας έτσι τα έξοδα CAPEX της επιχείρησης. Τα IPS – IDS επιλέγονται είτε μαζί με τα firewall είτε ξεχωριστά είτε καθόλου. Αν υπάρχει ανάγκη για υψηλή ασφάλεια και φιλτράρισμα της κίνησης στο δίκτυο, θα επιλεχθεί κάποιο firewall που συνοδεύεται από IPS –

IDS και όχι ξεχωριστά, ώστε να μειωθεί το κόστος αγοράς τους. Σε αντίθετη περίπτωση μπορούμε να το παραλείψουμε.

4. Routers

   Τα routers επιλέγονται με βάση την ασφάλεια και την ταχύτητα που απαιτούμε, αλλά και την οικονομική δυνατότητα κάθε επιχείρησης. Υπάρχουν κάποιες τεχνικές υψηλές ασφαλείας που συμπεριλαμβάνονται σε κάποια routers αλλά αυξάνουν το συνολικό τους κόστος. Τέτοιες είναι το firewall στο router, το Mac address filtering, το SSL VPN, η υποστήριξη PKI, η κρυπτογράφηση AES και η ασφάλεια των θυρών (δυναμική και στατική).

5. Switches

   Ο αριθμός των switches καθορίζεται ανάλογα με τον αριθμό των χρηστών.

   Τα switches διακρίνονται σε managed και unmanaged ανάλογα με το αν θέλουμε να παρακολουθούμε τη κίνηση στο δίκτυο και να θέτουμε διάφορες παραμέτρους ασφαλείας ή όχι. Τα managed switches που παρέχουν αυτές τις υπηρεσίες είναι επομένως πιο ακριβά και αυξάνουν τα κόστη CAPEX μιας επιχείρησης. Κάποιες από τις λειτουργίες που προσφέρουν τα managed switches είναι ο έλεγχος της κίνησης, το QoS, τα VLANs, η προστασία DoS και η αποφυγή συμφόρησης.

6. Remote access

   Τα access points επιλέγονται ανάλογα με τον αριθμό των χρηστών που συνδέονται από το ασύρματο δίκτυο, τους χώρους που θέλουμε να καλύψουμε καθώς και τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται. Κάποια επιπλέον χαρακτηριστικά που μπορούμε να επιλέξουμε αλλά αυξάνουν το κόστος CAPEX της επιχείρησης, είναι ο μηχανισμός DFS, η μέθοδος ασφαλείας Forwarding DMZ, το WDS και το IP και MAC binding.

7. VoIP

   Το VoIP επιλέγεται μόνο εφόσον απαιτούμε υπηρεσίες υψηλής ποιότητας όπως είναι το video conferencing. Το κόστος του ποικίλει και μεταβάλλεται ανάλογα με το αν του προσθέσουμε επιπλέον χαρακτηριστικά όπως είναι το πρωτόκολλο CDP, η χρήση πιστοποιητικών, η κρυπτογράφηση με τη χρήση του SRTP, η κρυπτογράφηση σήματος με τη χρήση του TLS και τα κρυπτογραφημένα αρχεία ρυθμίσεων.

Παρακάτω παρουσιάζεται ένας πίνακας μεθοδολογίας επιλογής των κατάλληλων μηχανισμών σε μια επιχείρηση, με βάση και την ανάλυση παραδείγματος που πραγματοποιήθηκε στο προηγούμενο κεφάλαιο.

ΕΠΙΛΟΓΗ ΜΗΧΑΝΙΣΜΩΝ	ΥΨΗΛΕΣ ΑΠΑΙΤΗΣΕΙΣ/ΚΟΣΤΗ	ΧΑΜΗΛΕΣ ΑΠΑΙΤΗΣΕΙΣ/ΚΟΣΤΗ
Σύνδεση παρόχου	Μισθωμένη γραμμή/ VDSL	VDSL - ADSL
Antivirus	Αγορά αδειών σε antivirus	Free Antivirus
Hardware firewall/ IPS - IDS	Stateful Firewall / NAI	Stateless Firewall / NAI
Routers	<u>Τεχνικές ασφαλείας:</u> • Firewall • Mac Address Filtering • SSL VPN • Υποστήριξη PKI • Κρυπτογράφηση AES • Ασφάλεια θυρών	<u>Τεχνικές ασφαλείας:</u> • Firewall • Mac Address Filtering • Ασφάλεια θυρών
Switches	Managed switches <u>Επιπλέον Χαρακτηριστικά:</u> • QoS • SNMP • VLANs • Ασφάλεια θυρών • Προστασία DoS • Αποφυγή συμφόρησης	Unmanaged switches
Remote Access	Access points <u>Επιπλέον Χαρακτηριστικά:</u>	Access points

	• DFS • Forwarding DMZ • WDS • IP και MAC Binding	
VoIP	NAI <u>Επιπλέον Χαρακτηριστικά:</u> • CDP • Πιστοποιητικά • Κρυπτογράφηση με SRTP • Κρυπτογράφηση σήματος με TLS • Κρυπτογραφημένα αρχεία ρυθμίσεων	OXI

10.3 Μελέτη περίπτωσης

Το δίκτυο υπολογιστών σε μια επιχείρηση αποτελεί το κομβικό μέσο με το οποίο οι εργαζόμενοι και οι χρήστες μπορούν να χρησιμοποιήσουν και να μοιραστούν υπηρεσίες, αξιοποιώντας παράλληλα και τη χρήση του Internet. Θεωρείται απαραίτητο για την εύρυθμη λειτουργία της επιχείρησης και βοηθάει στην μέγιστη δυνατή απόδοση των στόχων της χάρη στη μείωση του χρόνου που απαιτείται για την απόκτηση και χρήση πληροφοριών και υπηρεσιών. Επομένως, οδηγεί στη μείωση των δαπανών μια επιχείρησης και επιπλέον, ανάλογα και με τη λειτουργία της πιθανώς βοηθάει και στο μέγιστο δυνατό αποτέλεσμα του αντικειμένου της.

Στο παράδειγμα που θα παραθέσω παρακάτω, η εταιρεία αυτή ασχολείται με τη δημιουργία παιχνιδιών υπολογιστών, επομένως η χρήση δικτύου υπολογιστών κρίνεται όχι απλά επιπλέον σημαντική αλλά απολύτως απαραίτητη.

Ένας άλλος τομέας όμως που πρέπει να εστιάσουμε είναι η ασφάλεια που απαιτείται για το εκάστοτε δίκτυο, η οποία, αν δεν επιτευχθεί πιθανώς θα φέρει τα αντίθετα αποτελέσματα και μπορεί να στοιχίσει στην επιχείρηση πέρα από μεγάλα χρηματικά ποσά, πιθανώς και την ίδια την ύπαρξη της. Φυσικά η ασφάλεια είναι ένας τομέας που προϋποθέτει κόπο και χρήμα, επομένως ανάλογα με τα χρήματα που θέλει να δαπανήσει μια εταιρεία μπορεί να πετύχει μεγαλύτερη ασφάλεια και επίτευξη των

στόχων της, αλλά δυστυχώς με αυτό τον τρόπο αυξάνονται οι δαπάνες όχι μόνο για την απόκτηση του κατάλληλου εξοπλισμού, αλλά κυρίως για τη συντήρησή του. Βέβαια, στην επιλογή μη υψηλής δαπάνης για την ασφάλεια του δικτύου, η επιχείρηση ρισκάρει να χάσει πολύ περισσότερα χρήματα σε περίπτωση επιθέσεων. Επομένως, είναι στην κρίση της, αλλά και στην οικονομική δυνατότητα της να αποφασίσει που θα εστιάσει περισσότερο.

Σε αυτή τη διπλωματική επομένως, θα αναλύσουμε με οικονομικά στοιχεία τα μέρη που είναι αναγκαία ή προαιρετικά για την ασφάλεια της επιχείρησης, και θα τα αξιολογήσουμε ανάλογα με την ποιότητα υπηρεσιών. (54)

10.3.1 Ανάλυση Δικτύου Επιχείρησης

Στην επιχείρηση GC που θα χρησιμοποιήσουμε ως πρότυπο το QoS κυμαίνεται ανάλογα με τις δαπάνες που θα πραγματοποιηθούν, τόσο τις κεφαλαιακές όσο και τις λειτουργικές. Θα αναλυθούν τα 2 είδη δαπανών που αφορούν αποκλειστικά στην ασφάλεια του δικτύου της επιχείρησης, ανάλογα πάντα με τη ποιότητα υπηρεσιών QoS που θέλει να προσφέρει. Επομένως θα πραγματοποιηθεί μια συγκριτική αξιολόγηση των δαπανών που στοχεύουν στην δικτυακή ασφάλεια, με την χρήση 2 παραδειγμάτων που το ένα εστιάζει στην επίτευξη υψηλής ποιότητας υπηρεσιών και το άλλο στην επίτευξη χαμηλής ποιότητας υπηρεσιών πάντα με γνώμονα το κόστος.

10.3.1.1 Περιγραφή της Επιχείρησης

Η εταιρεία λογισμικού Gaming_Center (GC) ασχολείται με τη δημιουργία παιχνιδιών υπολογιστών καθώς και με την αναβάθμιση ήδη υπαρχόντων παιχνιδιών. Η έδρα της βρίσκεται στο κέντρο της Αθήνας σε ένα κτίριο 3 ορόφων και απασχολεί 50 χρήστες.

Οι χρήστες αυτοί αποτελούνται από τα ακόλουθα άτομα:

- Τον CEO user που είναι ο διευθυντής της εταιρείας, λαμβάνει όλες τις κεντρικές αποφάσεις και έχει δικαιώματα admin σε κάθε τομέα της εταιρείας. Ο CEO user έχει δικό του γραφείο στον 3^{ο} όροφο της εταιρείας.

- Τους 3 project users που είναι οι δεύτεροι στην ιεραρχία και ρόλος τους είναι να αποφασίζουν τα projects που θα υλοποιηθούν, καθώς και να εγκρίνουν νέα project και να ρυθμίζουν την προτεραιότητα των εργασιών. Οι project users βρίσκονται στον 3^{ο} όροφο και έχουν ο καθένας δικό του γραφείο.

- Τον call_center user που βρίσκεται επίσης στον 3^{ο} όροφο σε δικό του γραφείο. Αναλαμβάνει όλα τα τηλεφωνήματα που δέχεται ή κάνει η εταιρεία καθώς και την ηλεκτρονική αλληλογραφία.

- Τους software users που είναι συνολικά 28 άτομα και αναλαμβάνουν το κομμάτι της ανάπτυξης λογισμικού για τη δημιουργία παιχνιδιών. Χωρίζονται σε 2 κατηγορίες, στους software_a users που αποτελούνται από 10 άτομα και βρίσκονται στον 1^{ο} όροφο και στους software_b users που αποτελούνται από

18 άτομα και βρίσκονται στον 2ο όροφο. Οι πρώτοι αναλαμβάνουν το κομμάτι του development για την αλλαγή ή αναβάθμιση των ήδη τρεχόντων παιχνιδιών, ενώ οι δεύτεροι ασχολούνται με τη δημιουργία καινούργιων παιχνιδιών.

- Τους graphics users που είναι συνολικά 10 άτομα και αναλαμβάνουν το κομμάτι της εγκατάστασης και ελέγχου γραφικών στα παιχνίδια. Χωρίζονται σε 2 κατηγορίες, τους graphics_a users που αποτελούνται από 3 άτομα και βρίσκονται στον 1ο όροφο και τους graphics_b users που αποτελούνται από 7 άτομα και βρίσκονται στον 2ο όροφο. Οι πρώτοι αναλαμβάνουν τον έλεγχο και την αναβάθμιση των γραφικών στα ήδη τρέχοντα παιχνίδια, ενώ οι δεύτεροι αναλαμβάνουν την ανάπτυξη των γραφικών στα παιχνίδια που σχεδιάζονται αυτή την περίοδο από τους software_b users.

- Τους coding users είναι συνολικά 5 άτομα και έργο τους είναι να ελέγχουν το τελικό αποτέλεσμα μέσω simulation tests για να βεβαιωθούν για την άριστη ποιότητα του και να το προωθήσουν στο στάδιο της πώλησης. Οι coding users βρίσκονται στον 1ο όροφο.

- Τους advert users που είναι 2 άτομα και αναλαμβάνουν το κομμάτι της προώθησης, διαφήμισης και πώλησης των παιχνιδιών που έχουν ολοκληρωθεί. Τα γραφεία τους βρίσκονται στον 1ο όροφο.

Data Store	**Location**	**Application**	**Used by User**
Print/file server	1ος όροφος	Gaming_work	All
Email server	1ος όροφος	Email	All
Management server of company	1ος όροφος	Company management system	CEO user, project users
Management server of network	1ος όροφος	Management	CEO user, project users
DHCP server	1ος όροφος	Addressing	All
DNS server	1ος όροφος	Naming	All
NAT server	1ος όροφος	Addressing	All

USER COMMUNITY NAME	SIZE OF COMMUNITY	LOCATION OF COMMUNITY	APPLICATIONS USED BY COMMUNITY
CEO user	1	3ος όροφος	Email, web search
Project users	3	3ος όροφος	Email, web search
Call_center user	1	3ος όροφος	Email, web search
Software_a users	10	1οςς όροφος	Email, web search, gaming_work,unity
Software_b users	18	2ος όροφος	Email, web search, gaming_work,unity
Graphics_a users	3	1ος όροφος	Email, web search, gaming_work,unity
Graphics_b users	7	2ος όροφος	Email, web search, gaming_work,unity
Coding users	5	1ος όροφος	Email, web search, gaming_work
Advert users	2	1ος όροφος	Email, web search

ΠΕΡΙΓΡΑΦΗ ΧΩΡΟΥ

1ος ΟΡΟΦΟΣ

Στον 1ο όροφο στεγάζονται 4 ξεχωριστοί χώροι με συνολικά 20 άτομα. Στον πρώτο βρίσκονται οι εργαζόμενοι που ασχολούνται με την αναβάθμιση των ήδη τρεχόντων παιχνιδιών και οι οποίοι είναι οι 10 software_a users και οι 3 graphics_b users. Στο δεύτερο χώρο βρίσκονται οι 5 test_coding users και στο 3ο οι 2 advert users. Στο τέταρτο χώρο βρίσκεται το server room.

2ος ΟΡΟΦΟΣ

Στον 2ο όροφο βρίσκονται σε έναν ενιαίο χώροι οι εργαζόμενοι που δουλεύουν πάνω στο σχεδιασμό των νέων παιχνιδιών και είναι συνολικά 25 άτομα. Συγκεκριμένα είναι οι software_b users και οι graphics_b users.

3ος ΟΡΟΦΟΣ

Στον 3ο όροφο στεγάζονται 5 γραφεία και ένας χώρος αναψυχής με καφετέρια και πρόσβαση στο διαδίκτυο για τα μέλη της εταιρείας. Στα γραφεία βρίσκονται ο CEO user,οι 3 project users καθώς και ο call_center user.

10.3.1.2 Πρόταση Μεθοδολογίας Επιλογής Εξοπλισμού και Υπηρεσιών της Επιχείρησης

ΚΟΣΤΗ

Οι δαπάνες σχετικά με την ασφάλεια του δικτύου εστιάζουν σε 3 διαφορετικά μέρη. Το πρώτο αφορά στο server room που βρίσκεται στον 1^{ο} όροφο και τα μέρη που το απαρτίζουν μπορούν να ποικίλουν σε είδος, ποσότητα και ποιότητα ανάλογα με τα χρήματα που θα δαπανηθούν. Το δεύτερο μέρος είναι τα εξαρτήματα και ο εξοπλισμός ασφαλείας κατά μήκος όλου του κτιρίου που επίσης ποικίλλουν με βάση την προηγούμενη αναφορά, και τέλος το τρίτο μέρος αφορά στα επιπλέον κόστη λόγω extra υπηρεσιών ή εξαρτημάτων. Τα τελευταία προφανώς αφορούν το προαιρετικό κομμάτι και προστίθενται καθαρά με στόχο την υψηλότερη ποιότητα υπηρεσιών αλλά αυξάνουν αρκετά τα κόστη.

Παρακάτω θα ακολουθήσει η ανάλυση των εξαρτημάτων και των υπηρεσιών στα 3 παραπάνω μέρη που αναφέρθηκαν.

SERVER ROOM

Το server room είναι το πιο σημαντικό μέρος που ασχολείται με την ασφάλεια και τις διεργασίες του δικτύου της εταιρείας, και βρίσκεται στον 1^{ο} όροφο. Οι επιλογές που υπάρχουν για τη δόμηση και τη συντήρησή του ποικίλλουν σημαντικά και θα παρουσιαστούν παρακάτω:

- Rack
- Switches
- Routers
- Patch Panel
- Fire Alarms
- Cooling system
- Ups
- Generators
- Server farm
- Surveillance
- IPS-IDS
- Firewall
- Nas Backup

WHOLE BUILDING

Σχετικά με την ασφάλεια και την ποιότητα του δικτύου σε ολόκληρο το κτήριο, υπάρχουν αρκετές επιλογές που μπορούν να επιλεχθούν ανάλογα με τις προτιμήσεις και την οικονομική δυνατότητα της επιχείρησης. Αυτές είναι οι ακόλουθες:

- Καλώδια
- Σύνδεση παρόχου
- Antivirus
- Firewall
- Router
- IPS-IDS
- Switches

EXTRA EQUIPMENT/SERVICES

Κάποιες επιπλέον υπηρεσίες ή εξοπλισμοί που προσφέρουν ασφάλεια στην δικτύωση της επιχείρησης αλλά προφανώς επιπλέον κόστος, είναι οι/τα παρακάτω:

- Τεχνικός Δικτύου
- VoIP
- Cloud server

Μια άλλη επιλογή για την εγκατάσταση του server στην επιχείρηση, είναι να λειτουργεί σε cloud, μια επιλογή που ναι μεν μειώνει τα λειτουργικά και κεφαλαιακά έξοδα της επιχείρησης, αλλά παράλληλα μειώνει κατακόρυφα και την ασφάλειά της.

Για το παράδειγμά μας θα χρησιμοποιήσουμε τα εξής:

EQUIPMENT/SERVICES	**QUALITY OF SERVICE/SECURITY**	
	HIGH	LOW
ΚΑΛΩΔΙΑ	Cat7 μήκους 1χλμ - 1200€	Cat6 μήκους 1χλμ - 350€
ΣΥΝΔΕΣΗ ΠΑΡΟΧΟΥ	5 VDSL Γραμμές(50 Mbps) - 250€ / μήνα	4 ADSL Γραμμές (24 Mbps) - 90€ / μήνα
ANTIVIRUS	Small Office Security (50 χρήστες) - 1760€ χρόνο	Free antivirus
FIREWALL	Check Point 1100 Security appliance - 531€	NETGEAR ProSAFE FVS318G - 110€

IPS-IDS		-
Router	Cisco-D 866VAE-K9 - 527€	Cisco RV042 - 150€
Switches	3 Cisco SLM224GT - 480€	3 TP-LINK TL-SG1024D v4 - 300€
Nas	Synology Diskstation D51515+ - 800€	Synology Diskstation DS216j - 170€
Remote Access	3 TP-LINK TL-WA901ND - 150€	1 TP-LINK TL-WA901ND - 50€
VoIP	5 Cisco SPA 303 3-Line IP Phone - 355€	-
	Συνδρομή για VoIP Τηλεφωνία- 115€ / χρόνο	
Τεχνικός Δικτύου	Ετήσιο συμβόλαιο 60 ωρών - 2000€	Ανά επίσκεψη - 50€
Τελικό κόστος	≈ 8000€	≈ 1700€

Καλωδίωση

Τα CAT 7 καλώδια διαφέρουν από τα προηγούμενα πρότυπα Ethernet καλωδίων συμπεριλαμβανομένων και των CAT 5 και CAT6. Το μεγαλύτερο πλεονέκτημα των CAT 7 καλωδίων είναι η θωράκιση των συνεστραμμένων ζευγών του, η οποία βελτιώνει σημαντικά την αντίσταση στον θόρυβο. Επίσης ενώ είναι μια πιο ακριβή λύση, θεωρείται πιο ανθεκτικό και έχει μεγαλύτερη διάρκεια ζωής από τα υπόλοιπα καλώδια, βελτιώνοντας έτσι την συνολική απόδοση της επένδυσης, και επίσης είναι η καλύτερη επιλογή καλωδίωσης έχοντας στο μυαλό το μέλλον.

Σύνδεση Παρόχου

Λόγω του αντικειμένου της επιχείρησης η ανάγκη για γρήγορη σύνδεση στο Internet είναι μεγάλη. Για το high QoS επιλέξαμε την χρήση 5 γραμμών VDSL με σκοπό να έχουμε redundancy, και για το low QoS επιλέξαμε 4 ADSL γραμμές οι οποίες δεν παρέχουν ταχύτητες όσο του VDSL, ωστόσο είναι μια οικονομική λύση η οποία μπορεί να ανταπεξέλθει στις απαιτήσεις του συστήματος.

Antivirus

Για το antivirus σε high QoS διάλεξα το Karspersky Small office security για 50 χρήστες το οποίο προστατεύει τα ευαίσθητα δεδομένα από κακόβουλες επιθέσεις. Προσφέρει επίσης ασφάλεια σε online συναλλαγές καθώς και backup και κρυπτογράφηση των αρχείων και λειτουργεί σε πραγματικό χρόνο για τον εντοπισμό

οποιασδήποτε απειλής. Επίσης οι αναβαθμίσεις είναι πολύ συχνές προσφέροντας ασφάλεια από καινούργιες απειλές. Για low QoS υπάρχουν αρκετά free antivirus τα οποία παρέχουν μια βασική προστασία χωρίς κόστος.

Firewall

Για το high QoS όσο αναφορά το Hardware Firewall διάλεξα το συγκεκριμένο γιατί ήταν μια λύση η οποία παρείχε όλα τα πρότυπα ασφαλείας σε μια συσκευή όπως Firewall, Antivirus, IPS-IDS, VPN(IPSec) έλεγχο τον εφαρμογών, φιλτράρισμα του URL καθώς και των πακέτων του δικτύου. Το Αντίστοιχο για το low QoS Firewall ανιχνεύει τα πακέτα του δικτύου και έχει VPN.

Routers

Το Router για το high QoS επιλέχθηκε για την υποστήριξη των VDSL γραμμών και γιατί παρέχει ασφάλεια μέσω του in-built Firewall. Για το low QoS επιλέχθηκε ένα router για την υποστήριξη των ADSL γραμμών το οποίο να είναι οικονομικό.

Switches

Το switch για το high QoS επιλέχθηκε γιατί προσφέρει υπηρεσίες και ασφάλεια χωρίς όμως να κοστίζει αρκετά. Είναι ένα layer 2 switch και τα πιο σημαντικά του πλεονεκτήματα είναι:

- Περιλαμβάνει εργαλεία που διαχειρίζονται μέσω φυλλομετρητών και απλοποιούν την εγκατάσταση, την διαχείριση και την αντιμετώπιση προβλημάτων.
- Η δυνατότητα δημιουργίας αρκετών VLANs
- Έχει ενσωματωμένο RMON λογισμικό για την βελτίωση της διαχείρισης της κυκλοφορίας, την παρακολούθηση και την ανάλυση του δικτύου.
- Η δυνατότητα να γίνεται προτεραιοποίηση σε περίπτωση καθυστέρησης ευαίσθητων δεδομένων.
- Υποστήριξη του IPv6 μαζί με το IPv4
- Φιλτράρει τις MAC διευθύνσεις
- Υποστήριξη αλγόριθμων ασφαλείας 802.1χ Radius και HTTPS
- Παρέχει ασφάλεια στις θύρες(ports), με το να κλειδώνει MAC διευθύνσεις σε θύρες.
- Παρέχει ασφάλεια ενάντια σε επιθέσεις DoS

Το switch για το low QoS επιλέχθηκε γιατί είναι πολύ οικονομικό δεδομένου ότι θα χρησιμοποιηθεί σε επιχείρηση καθώς και πολύ εύκολο στην εγκατάσταση του.

Nas Storage

Οι επιχειρήσεις με 50 ή λιγότερους υπαλλήλους χρειάζονται να αποθηκεύουν τις ολοένα αυξανόμενες ποσότητες των κρίσιμων επιχειρηματικών και οικονομικών δεδομένων με σκοπό της προστασία τους σε περίπτωση απώλειας. Αν και οι προϋπολογισμοί τους είναι περιορισμένοι, οι ανάγκες για backup είναι μεγάλες και πολύ σημαντικές. Σε αυτήν την περίπτωση η χρήση του NAS είναι μια οικονομική λύση και βοηθάει τις μικρές επιχειρήσεις για να συγκεντρώνουν και να δημιουργούν αντίγραφα ασφαλείας όλων των αρχείων τους σε μια θέση, έτσι ώστε να έχουν πρόσβαση σε αυτά τα αρχεία από οπουδήποτε. Με αυτήν την λογική χρησιμοποιούνται NAS backup και στις 2 περιπτώσεις μας, με την διαφορά τους να είναι στον αριθμό των σκληρών δίσκων που μπορούν να υποστηρίξουν(άρα και στην συνολική χωρητικότητα τους) , στην ταχύτητα αντιγραφής των δεδομένων καθώς και στο ότι ο NAS του high QoS χρησιμοποιεί το επίπεδο κρυπτογράφησης δεδομένων AES-NI.

Access Points

Όσο αφορά τα Access Points, επειδή δεν θα χρησιμοποιούνται από τους υπαλλήλους για επαγγελματικό σκοπό, ωστόσο θέλουμε να υπάρχει ένα επίπεδο ασφαλείας(wpa-wpa2) ούτως ώστε να μην μπορεί να εισέλθει εύκολα στο δίκτυο κάποιος κακόβουλος χρήστης. Στο high QoS χρησιμοποιούμε 3 Access points(1 σε κάθε όροφο) για να υπάρχει πρόσβαση από όλο το κτήριο, και στο low quality χρησιμοποιούμε 1 στο Lounge room που θα ξεκουράζονται οι εργαζόμενοι.

VoIP

Το VoIP είναι μια τεχνολογία που επιτρέπει στους χρήστες να πραγματοποιούν κλήσεις χρησιμοποιώντας το ευρυζωνικό διαδίκτυο. Ο κυριότερος λόγος για την χρήση του είναι ότι είναι πού φθηνότερο από το συμβατικό τηλέφωνο, καθώς και ότι παρέχει την δυνατότητα για την σύγκλιση όλων των μορφών επικοινωνίας(πχ video conference,calls,emails) στο διαδίκτυο σε ένα ενιαίο δίκτυο με αποτέλεσμα την μείωση του κόστους εγκατάστασης και συντήρησης. Παρόλα αυτά θα το δούμε μόνο στο high QoS δίκτυο καθώς πρόκειται για μια επένδυση που αυξάνει σημαντικά το κόστος.

Συντήρηση Δικτύου

Για επιχειρήσεις μέχρι 50 εργαζόμενους είναι οικονομικά ασύμφορο να απασχολούν με πλήρη απασχόληση έναν τεχνικό δικτύου, για αυτό υπάρχουν διάφορες άλλες πιο οικονομικές λύσεις. Στην περίπτωση του high QoS ένα ετήσιο συμβόλαιο συντήρησης και επίλυσης προβλημάτων είναι μια καλή λύση και θα κρατήσει το δίκτυο σε υψηλό επίπεδο. Στην περίπτωση του low QoS η εταιρία θα χρησιμοποιήσει μια πιο οικονομική λύση στην οποία θα καλείται τεχνικός δικτύων μόνο όταν υπάρχει κάποιο πρόβλημα που επηρεάζει την λειτουργία του.

10.3.1.3 Συμπέρασμα

Επομένως παρατηρούμε ότι για την απόδοση ποιότητας υπηρεσιών στα τοπικά δίκτυα υπάρχουν πολλές δυνατότητες ανάλογα με την οικονομική ευχέρεια της κάθε επιχείρησης. Στην παραπάνω μεθοδολογία επιλογής υπηρεσιών και εξοπλισμού επιλέχθηκαν οι 2 ακραίες περιπτώσεις και υπολογίστηκε το βασικό bugdet ανάλογα με το αν η συγκεκριμένη επιχείρηση που παρουσιάστηκε επιθυμούσε υψηλό ή χαμηλό QoS Στις 2 αυτές αντίστοιχες περιπτώσεις παρατηρούμε μια διαφορά τιμής περίπου στα 6000 €. Κάθε επιχείρηση μπορεί να κινηθεί μέσα σε αυτό το πλαίσιο ανάλογα πάντα με τις οικονομικές της δυνατότητες και σύμφωνα με τη μεθοδολογία που παρουσίασα στην επιλογή εξοπλισμού και υπηρεσιών, ώστε να πετύχει, ανάλογα και με τους πόρους της το επιθυμητό για την ίδια αποτέλεσμα.

11. Μελλοντικές Τάσεις στην Ασφάλεια και στην Ποιότητα Υπηρεσιών των Τοπικών Δικτύων

Στη σημερινή εποχή και με τη συνεχή εξέλιξη της τεχνολογίας, είναι πλέον σαφές ότι η εξασφάλιση της ασφάλειας και της ποιότητας παροχής υπηρεσιών στα τοπικά δίκτυα είναι ένα ζήτημα που θα απαιτεί ολοένα και περισσότερες ενέργειες.

Όσον αφορά στον τομέα της ασφάλειας, η ολοένα και μεγαλύτερη εξέλιξη του κακόβουλου λογισμικού θέτει σε αμφισβήτηση ακόμα και τα καλύτερα antivirus κυκλοφορούν στην αγορά. Επίσης, ενώ όλο και περισσότεροι πωλητές ασφαλείας προσφέρουν μέσα άμυνας ενάντια στις κακόβουλες επιθέσεις, οι περισσότερες δεν προσφέρουν μεγάλη εγγύηση αφού το κακόβουλο λογισμικό συνεχίζει να εξελίσσεται. Επίσης, επειδή είναι γεγονός ότι οι πωλητές ασφαλείας προσφέρουν τις περισσότερες λύσεις σε επιχειρήσεις ή προσωπικούς υπολογιστές, είναι φανερό ότι οι επιθέσεις κακόβουλου λογισμικού θα επικεντρωθούν κυρίως στις κινητές συσκευές που είναι πολύ περισσότερο ευάλωτες με αποτέλεσμα να δημιουργηθούν ακόμα μεγαλύτερα προβλήματα.

Ένα επίσης μεγάλο θέμα που θα οδηγήσει σε μεγάλα κενά ασφαλείας είναι ότι η μεγάλη και συνεχής εξάπλωση του Internet Of Things (IoT) θα οδηγήσει σε μεγάλα προβλήματα λόγω της πολυπλοκότητας της αρχιτεκτονικής του, της μεγάλης ποικιλίας πρωτοκόλλων και προτύπων που περιέχει αλλά και των προϊόντων του που διαθέτουν πολύ αδύναμα χαρακτηριστικά ασφαλείας.

Μία λύση στα παραπάνω προβλήματα είναι οι πάροχοι υπηρεσιών που χρησιμοποιούν μεθόδους όπως η τεχνητή νοημοσύνη, η μάθηση της γλώσσας μηχανής, οι προηγμένοι αλγόριθμοι και η οπτικοποίηση των δεδομένων, με σκοπό να βοηθήσουν τις επιχειρήσεις να αναγνωρίζουν και να αντιμετωπίζουν κατάλληλα τις επιθέσεις. Τέτοιοι υπεύθυνοι είναι οι Managed Security Service Providers (MSSPs) δηλαδή οι υπεύθυνοι για τη διαχείριση παροχής υπηρεσιών ασφαλείας. Επομένως, με τη βοήθειά τους υπάρχει η προοπτική να δημιουργηθούν προϊόντα που θα παρουσιάζουν αυτές τις αυξημένες δυνατότητες και θα τις «μεταφράζουν» σε πραγματικά και ουσιαστικά μέτρα ασφαλείας.

Μία άλλη προοπτική που υπάρχει και θα βοηθήσει στην εξασφάλιση της ασφάλειας των επιχειρήσεων και όχι μόνο, είναι η ανάπτυξη εκ μέρους τους του SDN(software-defined networking) και η χρήση των APIs RESTful, του αυτοματισμού, του προγραμματισμού του δικτύου καθώς και προηγμένων χαρακτηριστικών όπως είναι η πολλαπλή μίσθωση(multi-tenancy) και η μικρό-κατάτμηση(micro-segmentation). Ήδη από το 2016 πολλές επιχειρήσεις εκπαίδευσαν εργαζομένους τους πάνω στο SD-WAN(software-defined WAN) και υπάρχει η ελπίδα ότι από το 2017 πολλές επιχειρήσεις θα έχουν MPLS(multiprotocol label switching) WAN και θα κάνουν αναβαθμίσεις των router τους με σκοπό να μεταβούν σε SD-WAN. Επομένως,

υπάρχει η προσδοκία να υπάρχει χρήση υβριδικών WANs η οποία θα συνεχίσει να μεγαλώνει στα επόμενα χρόνια.

Μία ακόμα τάση που κυκλοφορεί τα τελευταία χρόνια είναι η έναρξη οργανισμών και επιχειρήσεων πάνω σε cloud. Για τέτοιου είδους εγχειρήματα κυκλοφορούν πολλές πιστοποιήσεις ασφαλείας cloud όπως οι Cloud Security Alliance's (CSA), Certificate of Cloud Security Knowledge (CCSK) και (ISC)2 Certified Cloud Security Practitioner (CCSP). Καθώς με τον καιρό έχουμε περισσότερες γνώσεις πάνω στην ανάπτυξης μια επιχείρησης σε περιβάλλον cloud, η υιοθέτηση αυτής της μεθόδου θα επιταχυνθεί αν και πρέπει και πάλι η αντίστοιχη επιχείρηση να πάρει σοβαρά εσωτερικά μέτρα ασφαλείας αλλιώς και πάλι μπορεί να κινδυνεύσει από επιθέσεις.

Επίσης, υπάρχει η πρόβλεψη ότι το IPV6 θα προσπεράσει το IPV4 που φτάνει στην αιχμή του. Συγκεκριμένα, οι επιχειρήσεις τελευταία υιοθετούν το IPV6 το οποίο έχει αναπτυχθεί από τους περισσότερους παρόχους δικτύου, και αναμένουμε ότι αυτή η κατάσταση θα συνεχίσει να αυξάνεται με πολύ έντονους ρυθμούς, γεγονός που ενισχύεται από το ότι το IPV6 τρέχει πλέον σχεδόν σε όλες τις κινητές συσκευές και τα προσωπικά κομπιούτερ.

Συμπερασματικά, είμαστε ακόμα στα αρχικά στάδια του IoT, του περιβάλλοντος cloud, της τεχνητής νοημοσύνης και του αυτοματισμού για να προβλέψουμε το μέλλον στα βήματα που θα γίνουν σχετικά με την ασφάλεια των τοπικών δικτύων. Παρόλα αυτά, επικρατεί αισιοδοξία ότι οι εξελίξεις στα προϊόντα και τις υπηρεσίες IT θα οδηγήσουν σε μεθόδους και μέσα όπου θα ενισχύσουν την ασφάλεια και θα προστατέψουν τις επιχειρήσεις από πιθανές επιθέσεις και διαρροή των δεδομένων τους.

Όσον αφορά στην ποιότητα υπηρεσιών (QoS), αδιαμφισβήτητο γεγονός είναι ότι θα αποτελέσει πολύ ουσιαστική παράμετρο στη μελλοντική εξέλιξη των τοπικών δικτύων. Οι 3 πιο σημαντικοί άξονες πάνω στους οποίους θα επικεντρωθούν οι μελλοντικές εξελίξεις, είναι οι ακόλουθες:

- Η οπτικοποίηση του δικτύου, η οποία επιτρέπει την ταυτόχρονη συνύπαρξη πολλών αρχιτεκτονικών δικτύου σε μία κοινή υποδομή.
- Η εσωτερική διαχείριση του δικτύου, η οποία βελτιώνει την επεκτασιμότητα των λειτουργιών διαχείρισης, διανέμοντας τη λογική αυτής της διαχείρισης σε όλους τους κόμβους του δικτύου.
- Ο σχηματισμός νέων μηχανισμών μεταφοράς δεδομένων, ο οποίος θα στοχεύει στην υποστήριξη διαφορετικών τύπων επικοινωνιών σε ιδιαίτερα δυναμικά σενάρια τοπικών δικτύων.

Το λογισμικό που πρόκειται να αναπτυχθεί τα επόμενα χρόνια και θα στοχεύει στην υψηλή ποιότητα υπηρεσιών, θα έχει τα εξής ακόλουθα χαρακτηριστικά:

- Έλεγχος των πόρων, δηλαδή διαχείριση των πόρων που χρησιμοποιούνται κατά το δοκούν (εύρος ζώνης, εξοπλισμός, εγκαταστάσεις ευρείας περιοχής κ.τ.λ.). Ένα χαρακτηριστικό παράδειγμα θα ήταν η μείωση του εύρους ζώνης που καταναλώνεται μέσω μιας διασύνδεσης, προκειμένου να δοθεί προτεραιότητα σε κάποια διαφορετική πρόσβαση.

- Πιο αποτελεσματική χρήση των πόρων του δικτύου, με τη χρήση εργαλείων διαχείρισης και ανάλυσης δικτύων, έτσι ώστε να παρέχεται γνώση των λεπτομερειών χρήσης των πόρων και να γίνεται στόχευση στους αντικειμενικούς στόχους της εκάστοτε επιχείρησης.

- Προσαρμοσμένες υπηρεσίες, όπου το QoS, θα επιτρέπει στους παρόχους υπηρεσιών διαδικτύου να προσφέρουν στους πελάτες τους προσεκτικά προσαρμοσμένες διαβαθμίσεις στην ποιότητα υπηρεσιών.

- Συνύπαρξη κρίσιμων εφαρμογών, με τη χρήση τεχνολογιών οι οποίες θα διασφαλίζουν ότι το δίκτυο χρησιμοποιείται αποτελεσματικά από εφαρμογές κρίσιμης σημασίας που είναι οι πιο σημαντικές στη κάθε επιχείρηση. Επιπλέον θα εξασφαλίζουν ότι το εύρος ζώνης και οι ελάχιστες καθυστερήσεις που απαιτούνται από ευαίσθητες εφαρμογές, θα εξυπηρετούνται με σωστό τρόπο και χωρίς να δημιουργούν προβλήματα στη κυκλοφορία του δικτύου.

Συμπερασματικά, το QoS αποτελεί εξίσου σημαντική παράμετρο με τη ασφάλεια για την εξέλιξη των τοπικών δικτύων. Μελλοντικά, η στόχευση της βελτίωσης ποιότητας υπηρεσιών θα επικεντρωθεί στη καλύτερη αξιοποίηση του δικτύου, τη μείωση του κόστους και την εξυπηρέτηση των χρηστών και πελατών, οδηγώντας τις επιχειρήσεις σε νέες μεθόδους και πρακτικές επίτευξης των στόχων τους. (55)

ΕΠΙΛΟΓΟΣ

Η ασφάλεια των τοπικών δικτύων είναι ιδιαίτερα σημαντική στις μέρες μας. Όπως πολλά πρόσφατα περιστατικά μας έχουν δείξει, οι συνέπειες μιας επίθεσης μπορεί να είναι καταστροφικές τόσο οικονομικά όσο και για το "όνομα" ενός οργανισμού. Αξίζει ταυτόχρονα να τονιστεί ότι επιτυχημένες επιθέσεις γίνονται ακόμα και σε ιδιαίτερα μεγάλους οργανισμούς ή και κρατικά, ακόμα, δίκτυα πέραν πάσης υποψίας. Η συνεχής λοιπόν ενημέρωση, τόσο των απλών χρηστών όσο και των διαχειριστών δικτύων, είναι απαραίτητη. Μια επίθεση σε ένα σύστημα υπολογιστή μπορεί να συμβεί ανά πάσα στιγμή και από οπουδήποτε. Ως εκ τούτου, η χρήση των τεχνικών ασφάλειας σε έναν υπολογιστή ή σε ένα σύστημα δικτύου της εταιρείας θεωρείται πλέον ζωτικής σημασίας. Η προστασία των περιουσιακών στοιχείων του δικτύου μιας εταιρείας απαιτούν την ανάπτυξη ενός σχεδίου ασφάλειας και πολιτικής που αποφασίζουν τι πρέπει να προστατεύεται και από ποιον και στη συνέχεια την εφαρμογή των κατάλληλων μέτρων ασφαλείας για να σταματήσουν οι απώλειες. Το σύστημα πρέπει να παρακολουθείται συνεχώς για την απειλή και τις επιθέσεις που προέρχονται από το εσωτερικό και το εξωτερικό ενός συστήματος δικτύου με την παρακολούθηση όλων των πόρων μιας εταιρείας. Αυτή η μελέτη διαπίστωσε ότι κανένα σύστημα του δικτύου δεν είναι απρόσβλητο από επιθέσεις και προσδιόρισε την πηγή των τρωτών σημείων του συστήματος να είναι η έλλειψη πολιτικής ασφάλειας, η διαμόρφωση και τα τρωτά σημεία της τεχνολογίας.

Όσον αφορά στην εφαρμογή του QoS σε ένα τοπικό δίκτυο, μπορεί να έχει ελάχιστες επιπτώσεις σε αυτό όταν βρίσκεται στην ίδια περιοχή. Είναι προφανές ότι, αν το LAN επεκτείνεται σε WAN, τότε η εφαρμογή του QoS σε ένα δίκτυο θα είναι υψίστης σημασίας αφού το δίκτυο θα μπορεί να προσφέρει προνομιακή μεταχείριση για τη ρύθμιση της κυκλοφορίας, όπως τη χρήση του VoIP. Η διαμόρφωση QoS σε ένα τέτοιο συγκλίνον δίκτυο προσφέρει μικρό χρόνο αναμονής, χαμηλή διακύμανση και υψηλή διαθεσιμότητα. Επιπλέον, στην περίπτωση ύπαρξης πολλών διαφορετικών μεταγωγέων και δρομολογητών πρέπει να σχεδιαστούν και να εφαρμοστούν διαφορετικές διαμορφώσεις QoS σε ένα τέτοιο δίκτυο.

Συμπερασματικά, η ασφάλεια των δικτύων είναι ένα πολύ σημαντικό και εκτεταμένο θέμα, το οποίο εμπεριέχει μια μεγάλη ποσότητα πληροφοριών. Θεωρείται πολύ χρήσιμη για την ανάπτυξη της κοινωνίας μας και παίζει σημαντικό ρόλο στη ζωή των ανθρώπων. Είναι απαραίτητη επομένως η έρευνα και ο έλεγχος όλο και περισσότερων τεχνολογιών, οι οποίες μπορούν να χρησιμοποιηθούν για την εγγύηση της ασφαλείας των πληροφοριών του δικτύου, με την παράλληλη βέβαια εφαρμογή του QoS.

Βιβλιογραφία – Παραπομπές

1. Andrew S. Tanenbaum & David J. Wetheral (2012) "Δίκτυα Υπολογιστών"
2. Jie Wang & Zachary Kissel (2015) "Introduction to Network Security, Theory and Practice"
3. Μακρόπουλος Νικόλαος (2014) "Πρωτόκολλο TCP/IP" (σελ.11)
4. Natarajan Meghanathan " A tutorial on Network Security: Attacks and Controls"
5. Timo Kiravuo , Mikko Sarela, Jukka Manner (2013) "A Survey of Ethernet LAN Security"
6. Avi Kak (2016) "PGP, IPSec, SSL/TLS, and Tor Protocols"
7. Κώστας Λιμνιώτης (2006) "Σχεδίαση Εικονικών Δικτύων" (σελ.16)
8. Robbie Mayers "Attacks on TCP/IP Protocols"
9. Avi Kak (2016) "Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing"
10. A Vananthi, B. Sowjanya Rani (2012) "Cloning Attack Authenticator in Wireless Sensor Networks"
11. Κώστας Λιμνιώτης (2006) "Σχεδίαση Εικονικών Δικτύων"
12. Avi Kak (2016) "Buffer Overflow Attack"
13. Τοκαλίδης Χρήστος (2008) "Δοκιμές διείσδυσης στο διαδίκτυο"
14. Avi Kak (2016) "TCP/IP Vulnerabilities and DoS Attacks: IP Spoofing, SYN Flooding, and The Shrew DoS Attack"
15. Avi Kak (2016) "DNS and the DNS Cache Poisoning Attack"
16. Μαρία Σιαπέρα (2016) "Ασφάλεια δικτύων και συστημάτων με την βοήθεια τειχών προστασίας"
17. Tamirat Atsemegiorgis (2013) "Building a Secure Local Area Network"
18. Μαρία Σιαπέρα (2016) "Ασφάλεια δικτύων και συστημάτων με την βοήθεια τειχών προστασίας" (σελ.47)
19. S. Nishmi Niroshan, A.B.M Ishan Udayanga , A.G.R.D Senevirantha (2016) "IEEE 802.11 Standards in Wireless Network Security and Wireless Network Attacks and Counter Measures"

20. Devharsh Trivedi (2014) “Advanced WLAN Technologies”

21. Boris Bellalta, Luciano Bononi, Raffaele Bruno, Andreas Kassler (2015) “Next generation IEEE 802.11 Wireless Local Area Networks”

22. Sourangsu Banerji & Rahul Singha Chowdhury (2013) “On IEEE 802.11: Wireless LAN Technology”

23. Lochan Verma & Mohammad Fakharzadeh, Sunghyun Choi (2015) “WiFi On Steroids: 802.11ac and 802.11ad”

24. Swetank Kumar Saha, Viral Vijay Vira, Anuj Garg, Dimitris Koutsonikolas “60 GHz Multi-Gigabit Indoor WLANS: Dream or Reality?”

25. Yulong Zou, Jia Zhu, Xianbin Wang, Lajos Hanzo “A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends”

26. Arinze Nwabude (2008) “Wireless Local Area Network (WLAN): Security risk and counter measures”

27. Κτάνης Δημήτριος (2012) “Επιθέσεις άρνησης εξυπηρέτησης υπηρεσιών DOS” (σελ. 16-17)

28. Κτάνης Δημήτριος (2012) “Επιθέσεις άρνησης εξυπηρέτησης υπηρεσιών DOS”

29. Αστέριος Αλμπανάκης (2011) “Ζητήματα και απαιτήσεις ασφαλείας συστημάτων VoIP” (σελ.49-50)

30. Τοκαλίδης Χρήστος (2008) “Δοκιμές διείσδυσης στο διαδίκτυο” (σελ.15)

31. Abhijit Bodhe , Mayur Masuti, Dr A.S.Umesh (2016) “Wireless Lan Security Attacks and CCM Protocol With Some Best Practices in Deployment of Services”

32. Αστέριος Αλμπανάκης (2011) “Ζητήματα και απαιτήσεις ασφαλείας συστημάτων VoIP”

33. Robin Gareiss (2009) “The True Cost of Voice Over IP”

34. Ιωάννα Πίσαρη (2004) “Μελέτη δυνατότητας εφαρμογής VoIP πάνω σε LANs και WANs”

35. Ιωάννα Πίσαρη (2004) “Μελέτη δυνατότητας εφαρμογής VoIP πάνω σε LANs και WANs” (σελ.51)

36. Bradley R.Smith, Garcia-Luna-Aceves “Best Effort Quality of Service”

37. Implement the DiffServ QoS Model (2006) – Cisco

38. Dr. Ying-Dar Lin (1999) “Internet Qos- IntServ and DiffServ”

39. Μιχαλάκη Ευαγγελή (2012) “Μηχανισμοί QoS σε δίκτυα τεχνολογίας WiMax” (σελ.60)

40. Telecom, media and technology(2014) “Optimize network OPEX and CAPEX while enhancing the quality of service”

41. Δημήτρης Ζεϊλανιπούρ, Στέλλα Αριστείδου, Σοφία Καζέλη “Internet Protocol QoS”

42. Μιχαλάκη Ευαγγελή (2012) “Μηχανισμοί QoS σε δίκτυα τεχνολογίας WiMax” (σελ.60)

43. Δημήτρης Ζεϊλανιπούρ, Στέλλα Αριστείδου, Σοφία Καζέλη “Internet Protocol QoS” (σελ.26)

44. https://fenix.tecnico.ulisboa.pt/downloadFile/3779571633469/qos.pdf

45. Σπυρώνης Ιωάννης (2011) “Μοντέλο για τεχνοοικονομική ανάλυση δικτύων οπτικών ινών” (σελ. 104)

46. Ελισάβετ Π. Διαμάντη, Αντώνιος Χ. Μακρής , Επαμεινώνδας Β. Λούκουτος (2009) “Τεχνοοικονομική Μελέτη Ασύρματων Τοπικών Δικτύων σε Εσωτερικούς και Εξωτερικούς Χώρους”

47. Χρήστου Βασίλης (2012) “Δίκτυα 4G – Τεχνοοικονομική Ανάλυση 4G”

48. Χουζούρης Ιωάννης (2008) “Τεχνοοικονομική Ανάλυση της WiMAX Τεχνολογίας”

49. Cornelia Capler (2009) “UMTS Networks and Beyond”

50. Jaana Laiho, Achim Wacker, Tomas Novosad (2006) “Radio Network Planning and Optimisation for UMTS”

51. 3GPP TS 23.107 V14.0.0 (2017) – 3rd Generation Partnership Project

52. Σπυρώνης Ιωάννης (2011) “Μοντέλο για τεχνοοικονομική ανάλυση δικτύων οπτικών ινών”

53. Αθανασοπούλου Αλεξία – Μοντέλο για Τεχνο-Οικονομική Ανάλυση Δικτύων Οπτικών Ινών

54. Kongadzem Eve Mary Leikeki (2014) “Designing a Local Area Network for Telemedicine”

55. Jorge Carapinha, Roland Bless κ.α. (2010) “Quality of Service in the Future Internet”

Εικόνες:

1. http://www.just2good.co.uk/images/gif/wirelessLAN.gif (2010, Wireless LAN for a Library: Issues and Challenges, Sivapackiyanathan Ketheeswaren)

2. http://www.whatisnetworking.net/wp-content/uploads/2015/02/TCP-IP-model-vs-OSI-model.png

3. https://res.cloudinary.com/peerlyst/image/fetch/c_limit,w_700/http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/091515_2139_Attacksover2.jpg (2015, Attacks over DNS, Joe Shenouda)

4. https://media.licdn.com/mpr/mpr/AAEAAQAAAAAAAA3DAAAAJDY4ZTYwMTVlLTBiZWUtNDQ1MC1iYTRjLTQ3MDY2MjllNWEyZQ.png (2017, Difference Between http:// and https:// , Willem van Heerden)

5. http://techgenix.com/content/ws/img/upl/image0031268491809957.jpg

6. http://thesurgeagency.com/wp-content/uploads/ipsec_tunnel.jpg

7. https://image.slidesharecdn.com/pptonsqlinjection-140405095723-phpapp01/95/ppt-on-sql-injection-9-638.jpg?cb=1396692018 (2014, A Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm, Faisal Md Abdur Rahman & Parves Kamal)

8. http://daanet.com.au/media/600/1458619798.EAGLE_DMZ.gif

9. http://www.rubikinfotech.com/assets/images/uploads/images/interation_detection.jpg (Example of the most common intrusion detection and prevention deployment topography(bastion NUX, April 6, 2011)