ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΡΟΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

ΜΕΛΕΤΗ & ΑΝΤΙΜΕΤΩΠΙΣΗ ΜΟΡΦΩΝ ΕΠΙΘΕΣΕΩΝ ΣΕ ΕΝΣΥΡΜΑΤΑ ΚΑΙ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΥΓΓΡΑΦΕΑΣ: ΚΑΜΠΟΛΗ ΑΓΑΘΗ

ΑΜ: 711131031

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

Δρ. ΜΑΥΡΟΜΜΑΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΑΘΗΝΑ 2022

Μέλη Τριμελούς Εξεταστικής Επιτροπής

Konstantinos Mavrommatis

Digitally signed by Konstantinos Mavrommatis
Date: 2022.08.02 12:03:02 +03'00'

Κωνσταντίνος Μαυρομμάτης

Επιβλέπων Καθηγητής

Stavros Fatouros

Digitally signed by Stavros Fatouros
Date: 2022.08.03 12:33:08 +03'00'

Σταύρος Φατούρος

Αναπληρωτής Καθηγητής

Nikolaos Myridakis

Digitally signed by Nikolaos Myridakis
Date: 2022.08.02 17:08:52 +03'00'

Νικόλαος Μυριδάκης

Επίκουρος Καθηγητής

Περιεχόμενα

Περίληψη 6

Abstract 6

Εισαγωγή 7

Κεφάλαιο1. Βασικές Έννοιες και Ζητήματα Ασφαλείας 9

1.1 Πρόληψη – Ανίχνευση – Αντίδραση 9

1.2 Εμπιστευτικότητα –Confidentiality 10

1.3 Ακεραιότητα – Integrity 11

1.4 Διαθεσιμότητα – Availability 11

Κεφάλαιο 2. Δίκτυα 12

2.1 Τα ΔίκτυαLAN-MAN-WAN 12

2.2 OSI Layers 18

2.3 Πρόσβαση στο Μέσο MAC 20

Κεφάλαιο 3. Επιθέσεις 22

3.1 Sniffing 22

3.2 MACSpoofing 27

3.3 IPSpoofing 31

3.4 DistributedDenialofService (DDoS) 35

3.5 CashPoisoning 38

3.6 Evil Twin Attack 42

3.7 Man in the Middle 43

3.8 WarDriving 44

3.9 Rogue Access Points (Rogue AP) 45

3.10 TCP Syn Flood 45

Κεφάλαιο 4. Ασφαλής Διασύνδεση 47

4.1Firewalls 47

4.2 PacketFilters 49

4.2 CircuitLevelGateways 51

4.3 Ανίχνευση Εισβολών 52

4.5 Honeypots 54

4.6 VPN και ασφάλεια 55

4.7 Radius 55

4.8 IDS Systems 56

Κεφάλαιο 5. Κρυπτογραφικοί Αλγόριθμοι 57

5.1 ΚρυπτογραφικόςΑλγόριθμοςAES 57
5.1.1 ΚρυπτογραφικόςΑλγόριθμοςDESκαι 3DES 59
5.2 Διαδικασία Κρυπτογράφησης 60
5.3 AddRoundKey 63
5.4 SubBytes 64
5.5 ElectronicCodebook 66
5.6 Ασύμμετρα Κρυπτοσυστήματα 67
5.7 RSA 68
5.8 WEP 70
5.9 WPA 71
5.10 WPA2 72
5.11 WPA3 72
Συμπεράσματα 74
Βιβλιογραφία 76

Πίνακας Περιεχομένων Εικόνων

Εικόνα 1. Παράδειγμα ενός Τοπικού Δικτύου Lan 14
Εικόνα 2. Τα Βασικά Χαρακτηριστικά ενός Τοπικού Δικτύου Lan (Cisco, 2013) 15
Εικόνα 3. MetropolitanAreaNetwork 17
Εικόνα 4. Wide Area Network 18
Εικόνα 5. MacSpoofingAttack 27
Εικόνα 6. Τεχνικές Διόρθωσης και Ανίχνευσης Λαθών 30
Εικόνα 7. Μορφή επίθεσης TCP Syn Flood 46
Εικόνα 8. Firewall 48
Εικόνα 9. Λίστα Ελέγχου Πρόσβασης 50
Εικόνα 10. Ροή Ελέγχου ταυτότητας και εξουσιοδότησης Radius 56
Εικόνα 11. AES Advanced Encryption Standard process 59
Εικόνα 12. AddRoundKey () 64
Εικόνα 13. Η επίδραση των Subbytes στον μετασχηματισμό της κατάστασης 65
Εικόνα 14. Sub bytes και S-box 65
Εικόνα 15. Ο μετασχηματισμός των Subbytes στο s-box 66
Εικόνα 16. Μοντέλο Ασύμμετρου Κρυπτοσυστήματος 68

Εικόνα 17. Λειτουργία RSA.. 70

Περίληψη

Σκοπός της παρούσας εργασίας είναι να μελετήσει τις επιθέσεις που δέχονται τα δίκτυα ασύρματα και ενσύρματα καθώς και τους τρόπους αντιμετώπισης τους. Για τον λόγο αυτό, παρουσιάζονται εκτενώς και με σαφήνεια τα εργαλεία που έχουν αναπτυχθεί με την βοήθεια των νέων τεχνολογιών προκειμένου να μετριαστούν οι επιθέσεις. Κάποια από αυτά είναι περισσότερο αποτελεσματικά και άλλα λιγότερα αποτελεσματικά εξαρτώμενα πάντα από τον τύπο της επίθεσης. Το μόνο σίγουρο είναι ότι έχουν γίνει σημαντικά βήματα στην αντιμετώπιση των επιθέσεων από εισβολείς εισάγοντας ένα ευρύ πεδίο μελέτης προς αυτή την κατεύθυνση.

Abstract

The purpose of this paper is to study the attacks on wireless and wired networks and how to deal with them. For this reason, the tools that have been developed with the help of new technologies in order to mitigate the attacks are presented extensively and clearly. Some of them are more effective and others less effective always depending on the type of attack. The only thing that is certain is that important steps have been taken in dealing with invader attacks by introducing a wide field of study in this direction.

Εισαγωγή

Η ασφάλεια των πληροφοριών θεωρείται μείζον ζήτημα στα σύγχρονα υπολογιστικά συστήματα. Η ανάπτυξη αλλά και η χρήση ολοένα και πιο σύγχρονων συστημάτων μπορεί να προσφέρει σημαντικά πλεονεκτήματα όμως ενδέχεται και να δημιουργήσει σημαντικές δυσλειτουργίες αναφορικά με την προστασία αλλά και την διάθεση των δεδομένων ενός δικτύου. Έτσι, η ικανοποίηση της απαίτησης των χρηστών προκειμένου τα δεδομένα ενός δικτύου να είναι ασφαλή, αποτελεί μια και από τις βασικότερες προϋποθέσεις για την αξιοποίηση των νέων τεχνολογιών. Για τον λόγο αυτό, η ασφάλεια σε συνδυασμό με την ποιότητα και την απόδοση θεωρείται απαραίτητη προκειμένου το δίκτυο ενός οργανισμού να λειτουργεί εύρυθμα καθώς οι υπηρεσίες που παρέχει στην πλειοψηφία τους στηρίζονται στις νέες τεχνολογίες.

Στην παρούσα εργασία, ο αναγνώστης έχει την δυνατότητα να μελετήσει βασικές έννοιες και ζητήματα ασφαλείας των δικτύων έτσι όπως περιγράφονται στο πρώτο κεφάλαιο. Πιο συγκεκριμένα, αποτυπώνονται εκτενώς έννοιες που σχετίζονται με την πρόληψη, την ανίχνευση, την αντίδραση, την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών. Στο δεύτερο κεφάλαιο, παρουσιάζονται τα είδη των δικτύων κυρίως τα πιο ευρέως διαδεδομένα όπως το Lan, το Wankαι το Man κάνοντας εκτενή αναφορά στην λειτουργία τους. Επίσης, στο ίδιο κεφάλαιο παρουσιάζονται τα Osi Layers, και η πρόσβαση στο μέσο Mac. Στο τρίτο κεφάλαιο, περιγράφονται αναλυτικά οι επιθέσεις που δέχονται τα δίκτυα καθώς και οι μορφές τους και ο τρόπος που εισβάλουν σε αυτά. Πιο συγκεκριμένα, αναφέρονται οι πιο γνωστές μορφές επιθέσεων όπως: το sniffing, το Cashpoisoning, Mac Spoofing, IP spoofing και το distributeddenialofservice. Στο επόμενο κεφάλαιο, γίνεται λόγος

για την ασφαλή διασύνδεση όπου περιγράφονται με σαφήνεια όπως το firewall και οι μορφές του, το packetfiltering, το circuitlevelgateway, ο τρόπος με τον οποίο γίνεται η ανίχνευση εισβολών σε ένα δίκτυο και το honeypot. Στο πέμπτο κεφάλαιο, αναλύονται οι κρυπτογραφικοί αλγόριθμοι Des, 3Des και Aes. Επίσης, περιγράφεται η διαδικασία και η λειτουργία της κρυπτογράφησης καθώς και οι διάφοροι μετασχηματισμοί που την απαρτίζουν όπως το subbyteskαιτο addroundkey. Ακόμη, γίνεται αναφορά στα ElectronicCodeBooksστα ασύμμετρα κρυπτοσυστήματα και στον αλγόριθμο του ασύμμετρου κρυπτοσυστήματοςRSA.

Κλείνοντας, αποδείχτηκε στην πράξη ότι οι μορφές και ο τρόπος των επιθέσεων που πραγματοποιούνται στα δίκτυα αντιμετωπίζονται αποτελεσματικά μέσα από τα διάφορα εργαλεία που έχουν αναπτυχθεί για την καταπολέμηση και την μετριασμό τους σε πολύ μεγάλο βαθμό.

Κεφάλαιο1. Βασικές Έννοιες και Ζητήματα Ασφαλείας

Στο πρώτο κεφάλαιο παρουσιάζονται βασικές έννοιες καθώς και βασικά ζητήματα της ασφαλείας των δικτύων. Πιο συγκεκριμένα, γίνεται μια εκτενής εισαγωγή σε έννοιες που αφορούν την προστασία των δικτύων από επιθέσεις και σχετίζονται με ορισμούς όπως: αυτές της πρόληψης, της ανίχνευσης και της αντίδρασης. Εκτός από αυτές που θεωρούνται βασικές για την ασφάλεια ενός δικτύου από τυχόν επιθέσεις, έννοιες όπως: η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα είναι εξίσου σημαντικές και αποτελούν τις βασικές προϋποθέσεις για να θεωρηθεί ένα δίκτυο ασφαλές.

1.1 Πρόληψη – Ανίχνευση – Αντίδραση

Η ασφάλεια των πληροφοριών ενός οργανισμού αποτελεί ζήτημα υψίστης σημασίας. Κάθε οργανισμός θέλει να προστατεύσει τα δεδομένα του από επιθέσεις και αλλοιώσεις από μη εξουσιοδοτημένους χρήστες. Επίσης, κάθε οργανισμός επιθυμεί να παρέχει δεδομένα και πληροφορίες στους εξουσιοδοτημένους χρήστες του οι οποίες θα είναι έγκυρες και αξιόπιστες και θα συμβάλουν στην αδιάλειπτη λειτουργία του συστήματος. Ωστόσο, η ασφάλεια των πληροφοριών σχετίζεται με την *πρόληψη (prevention)*: και αφορά στα μέτρα που λαμβάνει ο κάθε οργανισμός ώστε να προληφθούν οι τυχόν φθορές και αλλοιώσεις των συστημάτων του, *την ανίχνευση (detection):* η οποία αφορά τα μέτρα που λαμβάνει ο κάθε οργανισμός ώστε να είναι δυνατόν να ανιχνευτεί ο υπαίτιος που προκάλεσε τυχόν φθορές και αλλοιώσεις στον οργανισμό και την *αντίδραση (reaction):* η οποία αφορά τα μέτρα που λαμβάνονται προκειμένου να επέλθει η αποκατάσταση αλλά και η ανάκτηση των πληροφοριών που αλλοιωθήκαν. Η ασφάλεια ως έννοια, δεν προσδιορίζεται μονομερώς.

Περιλαμβάνει την προστασία και τον έλεγχο και συναντάται σε όλες τις εκφάνσεις της καθημερινής ζωής. Τέτοια παραδείγματα μπορεί να αφορούν την καθημερινότητα των ανθρώπων όπως: αν κάποιος τοποθετήσει κλειδαριά στις πόρτες και τα παράθυρα του σπιτιού του (πρόληψη), τοποθετήσει κύκλωμα συναγερμού (ανίχνευση), αλλά και τον χώρο των πωλήσεων όπως: για παράδειγμα οι παραγγελίες και οι πληρωμές που κρυπτογραφούνται όταν διακινούνται (πρόληψη), η συναλλαγή στην πιστωτική κάρτα (ανίχνευση), αλλά και οι ακυρώσεις συναλλαγών ή οι αλλαγές καρτών (αντίδραση) (Πάγκαλος & Μαυρίδης, 2002).

1.2 Εμπιστευτικότητα –Confidentiality

Σε αρκετές περιπτώσεις, η εμπιστευτικότητα και η ασφάλεια είναι έννοιες που είναι συνώνυμες. Η εμπιστευτικότητα ως έννοια, σχετίζεται με την πρόληψη της μη εξουσιοδοτημένης αποκάλυψης των δεδομένων και των πληροφοριών. Με άλλα λόγια, προλαμβάνει από την μη εξουσιοδοτημένη ανάγνωση. Συνεπώς, τα δεδομένα και οι πληροφορίες ενός συστήματος είναι προσβάσιμα μόνο από εξουσιοδοτημένους χρήστες. Πρακτικά, δεν σχετίζεται μόνο με την προστασία των πληροφοριών από μη εξουσιοδοτημένους χρήστες αλλά έχει να κάνει και με την ύπαρξη αυτών καθαυτών των δεδομένων. Βέβαια, η εμπιστευτικότητα περιλαμβάνει έννοιες όπως: η ιδιωτικότητα (privacy) που αφορά την προστασία προσωπικών δεδομένων συγκεκριμένων προσώπων και την μυστικότητα (secrecy) που αφορά την προστασία προσωπικών δεδομένων των φορέων και οργανισμών (Πάγκαλος & Μαυρίδης, 2002).

1.3 Ακεραιότητα – Integrity

Η ακεραιότητα ως έννοια προσδιορίζει την τάξη των πραγμάτων. Δηλαδή, προλαμβάνει την μεταβολή των πληροφοριών και των δεδομένων από τους μη εξουσιοδοτημένους χρήστες. Με άλλα λόγια, οι πληροφορίες και τα δεδομένα των συστημάτων, μεταβάλλονται μόνο από εξουσιοδοτημένους χρήστες (Πάγκαλος & Μαυρίδης, 2002).

1.4 Διαθεσιμότητα – Availability

Η διαθεσιμότητα των συστημάτων σχετίζεται με την πρόσβαση των εξουσιοδοτημένων χρηστών στις πληροφορίες και στα δεδομένα χωρίς καθυστερήσεις. Πρακτικά αυτό σημαίνει, ότι όταν οι εξουσιοδοτημένοι χρήστες ενός συστήματος επιθυμούν να έχουν πρόσβαση στους πόρους ενός συστήματος αυτό να γίνεται χωρίς άρνηση εξυπηρέτησης. Για λόγους ασφαλείας, κύριο ζήτημα αποτελεί η παρεμπόδιση των επιθέσεων που έχουν ως σκοπό να αποκόψουν την πρόσβαση των μη εξουσιοδοτημένων χρηστών. Τέτοιου είδους επιθέσεις καλούνται επιθέσεις άρνησης παροχής υπηρεσιών (denial of serviceattacks). Οι επιθέσεις άρνησης παροχής υπηρεσιών ουσιαστικά παρεμποδίζουν την εξουσιοδοτημένη πρόσβαση σε δεδομένα και πληροφορίες που θεωρούνται κρίσιμες. Η αντιμετώπιση αυτών των επιθέσεων έχει ως σκοπό να αντιμετωπίσει την σκόπιμη παρά την τυχαία απώλεια διαθεσιμότητας. Ενδεικτικό παράδειγμα τέτοιων επιθέσεων αποτελούν οι συνεχόμενες επιθέσεις από χρήστες προς έναν εξυπηρετητή αποστέλλοντάς μεγάλο αριθμό συνδέσεων (Πάγκαλος & Μαυρίδης, 2002).

Κεφάλαιο 2. Δίκτυα

Σε αυτό το κεφάλαιο, περιγράφονται τα είδη των δικτύων που είναι ευρέως γνωστά όπως: το Lan, Wan, Mankαθώς και ο τρόπος λειτουργίας τους. Επίσης, αναλύονται τα OsiLayers, και τι περιλαμβάνει το κάθε ένα από αυτά. Τέλος, παρουσιάζεται ο τρόπος που γίνεται η πρόσβαση στο μέσο Mac.

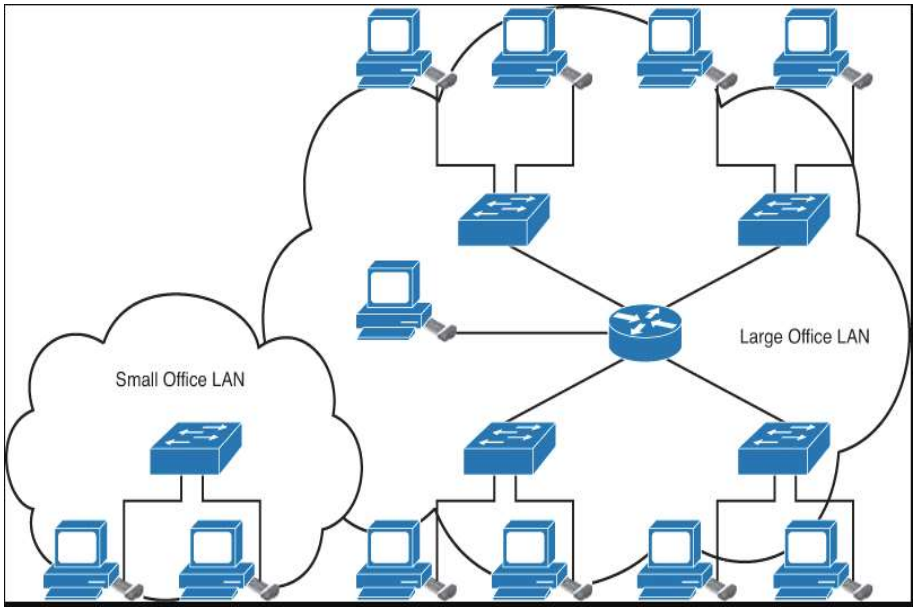
2.1 Τα ΔίκτυαLAN-MAN-WAN

Το LAN (LocalAreaNetworks) αφορά ένα τοπικό δίκτυο. Η ανάπτυξή τους ξεκίνησε από την δεκαετία του 1960, κυρίως για ερευνητικούς και εκπαιδευτικούς σκοπούς. Με την εισαγωγή της τεχνολογίας Ethernet το 1973, επήλθε και η εμπορευματοποίησή τους καθώς και η ευρεία χρήση τους (Cisco, 2013).

Ως κατασκευή είναι μικροσκοπική και αφορά την σύνδεση δύο ή περισσότερων υπολογιστών σε περιοχή περιορισμένου εύρους η οποία δεν ξεπερνά πολλά χιλιόμετρα. Ωστόσο, ένα τοπικό δίκτυο Lan ελέγχεται πλήρως από τον ιδιοκτήτη του. Επίσης, χαρακτηρίζεται από υψηλή ταχύτητα μετάδοσης και τόσο ο σχεδιασμός όσο και η διαχείριση είναι εύκολα να γίνουν. Ένα άλλο χαρακτηριστικό των τοπικών δικτύων είναι ότι η ταχύτητα λειτουργίας τους κυμαίνεται συνήθως 10 έως 1000 Mbps. Επίσης, ένα τοπικό δίκτυο έχει μεγαλύτερη ανοχή στα σφάλματα (Ginni, 2021).

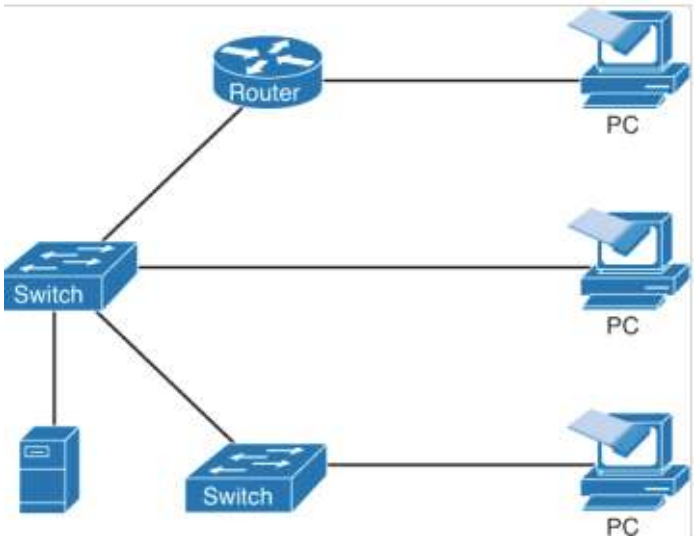
Επίσης, σε ένα τοπικό δίκτυο Lan συμπεριλαμβάνονται καλώδια, σημεία πρόσβασης, δρομολογητές και άλλα συστατικά μέσα από τα οποία επιτρέπεται η σύνδεση των συσκευών με διακομιστές σε άλλα τοπικά δίκτυα. Η ανάπτυξη της εικονοποίησης οδήγησε στην περαιτέρω άνθιση των τοπικών δικτύων Lan δίνοντας

την δυνατότητα στους διαχειριστές του δικτύου να προβαίνουν στην λογική ομαδοποίηση των κόμβων του δικτύου χωρίζοντάς τα με τέτοιον τρόπο χωρίς να παρατηρούνται σημαντικές διαφοροποιήσεις στην υποδομή τους. Για παράδειγμα, μια επιχείρηση με πολλά τμήματα η οποία διαθέτει τμήμα IT, το οποίο διαχειρίζεται τους υπολογιστές της θα μπορούσε να προβεί στην σύνδεσή τους στον ίδιο διακόπτη αλλά ταυτόχρονα θα μπορούσαν να τμηματοποιηθούν ώστε να φαίνονται αλλά και να λειτουργούν ξεχωριστά. Ωστόσο, ένα τοπικό δίκτυο Lan προσφέρει αρκετά πλεονεκτήματα εφάμιλλα με αυτά που προσφέρουν οι ομάδες συσκευών που συνδέονται μεταξύ τους. Ωστόσο, οι συσκευές μπορεί να κάνουν χρήση σύνδεσης στο διαδίκτυο, να προβαίνουν στην κοινή χρήση αρχείων αλλά και στην εκτύπωση αρχείων από εκτυπωτές οι οποίοι είναι κοινόχρηστοι. Τα πλεονεκτήματα από την χρήση των τοπικών δικτύων Lan, είναι αρκετά αλλά με την ανάπτυξη της τεχνολογίας του wi-fi τα τοπικά δίκτυα χρησιμοποιήθηκαν από όλο και περισσότερους φορείς. Μιλώντας για το σήμερα, όλοι οι φορείς από σχολεία μέχρι και επιχειρήσεις κάνουν χρήση τοπικών δικτύων. Εκτός αυτού, η ασύρματη σύνδεση έχει συμβάλλει σημαντικά στην επέκταση των τύπων συσκευών που μπορούν να συνδεθούν στα τοπικά δίκτυα. Οι συσκευές αυτές περιλαμβάνουν υπολογιστές, εκτυπωτές, τηλεοράσεις ακόμη και παιχνίδια.



Εικόνα 1. Παράδειγμα ενός Τοπικού Δικτύου Lan

Γενικότερα, τα τοπικά δίκτυα Lan διακρίνονται σε δύο κατηγορίες: το δίκτυο Lan πελάτη - διακομιστή και το δίκτυο Lanpeer to peer. Πιο συγκεκριμένα, το δίκτυο Lan πελάτη – διακομιστή, περιλαμβάνει συσκευές στις οποίες οι πελάτες βρίσκονται συνδεδεμένοι σε έναν κεντρικό διακομιστή. Από την πλευρά του ο διακομιστής είναι υπεύθυνος για την διαχείριση, την αποθήκευση και την πρόσβαση στις εφαρμογές και στις συσκευές για την κυκλοφορία του δικτύου. Ως πελάτης, μπορεί να θεωρηθεί οποιαδήποτε συσκευή που συνδέεται και έχει πρόσβαση στις εφαρμογές του διαδικτύου.



Εικόνα 2. Τα Βασικά Χαρακτηριστικά ενός Τοπικού Δικτύου Lan (Cisco, 2013)

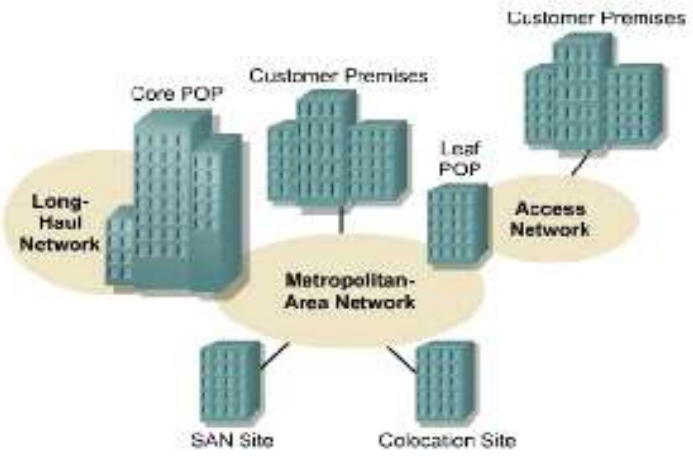
Η σύνδεσή τους στον διακομιστή γίνεται είτε με καλώδια είτε με ασύρματη σύνδεση. Βέβαια, οι χρήστες έχουν την δυνατότητα πρόσβασης σε εφαρμογές, βάσεις δεδομένων και υπηρεσίες οι οποίες εκτελούνται από τον διακομιστή του τοπικού δικτύου. Επίσης, τα περισσότερα δίκτυα επιχειρήσεων αλλά και τα δίκτυα εκπαίδευσης και έρευνας βασίζονται στον τύπο πελάτη – διακομιστή. Η δεύτερη κατηγορία των τοπικών δικτύων Laneίναι τα peertopeerLan. Στην κατηγορία αυτή δεν υπάρχει κεντρικός διακομιστής με αποτέλεσμα να μην μπορεί το δίκτυο να διαχειριστεί μεγάλο φόρτο εργασίας όπως στην πρώτη περίπτωση. Για τον λόγο αυτό τα δίκτυα αυτά είναι μικρότερα. Σε αυτά τα δίκτυα, οι συσκευές μοιράζονται πόρους μέσα από συνδέσεις ασύρματες ή ενσύρματες με την χρήση διακόπτη ή κάποιου δρομολογητή. Τα Peer to peer δίκτυα είναι κατά κύριο λόγο τα οικιακά δίκτυα. Όποιο κι αν είναι το μέγεθος του Lanτα χαρακτηριστικά που απαιτούνται για την λειτουργία του είναι βασικά και διακρίνονται όπως περιγράφονται παρακάτω*:*

α) υπολογιστές: οι οποίοι αποτελούν και τα τελικά σημεία ενός δικτύου όπου η κύρια λειτουργία τους είναι η αποστολή και η λήψη δεδομένων, *β) διασυνδέσεις*: οι

διασυνδέσεις δίνουν την δυνατότητα στα δεδομένα να πηγαίνουν από το ένα σημείο σε κάποιο άλλο και αποτελούνται από τις *κάρτες διασύνδεσης δικτύου (NIC)*, όπου κύρια λειτουργία τους είναι η μετάφραση των δεδομένων τα οποία πηγάζουν από τον υπολογιστή και μεταδίδονται μέσω του τοπικού δικτύου Lan, τα μέσα δικτύου όπως: καλώδια και ασύρματα μέσα τα οποία είναι υπεύθυνα για την μετάδοση σημάτων ανάμεσα στις συσκευές του δικτύου. Ωστόσο, ένα τοπικό δίκτυο Lanπρέπει να περιλαμβάνει συσκευές όπως τα hubs, τους διακόπτες Ethernet, τους δρομολογητές και τα πρωτόκολλα. Για την λειτουργία των μέσων δικτύου θα γίνει εκτενής αναφορά σε επόμενη παράγραφο(Cisco, 2013).

Το MAN (MetropolitanAreaNetwork), χρησιμοποιεί την ίδια τεχνολογία με το LAN. Συνήθως χρησιμοποιεί ένα ή δύο καλώδια χωρίς να συμπεριλαμβάνεται εναλλαγή εξαρτημάτων. Παρέχει ευρεία κάλυψη που είναι εφάμιλλη με αυτή μιας πόλης. Ωστόσο, ένα τοπικό δίκτυο Man μπορεί να ελέγχεται πλήρως από τον ιδιοκτήτη του. Η ταχύτητα μετάδοσης δεδομένων είναι μέση, καθώς ο σχεδιασμός και η διαχείριση δεν είναι εύκολο να διατηρηθεί. Η ταχύτητα λειτουργίας του είναι 1,5 Mbps. Τέλος, υπάρχει μικρότερη ανοχή στα σφάλματα (Ginni, 2021).Τα MAN τα χρησιμοποιούν οι επιχειρήσεις και οι οργανισμοί οι οποίοι συνδέονται στην ίδια γεωγραφική κάλυψη. Τα όρια της γεωγραφικής κάλυψης που ορίζουν κυμαίνονται από 5 έως 50 χλμ. Το Man χρησιμοποιεί τεχνολογίες όπως: η FDDI(fiberdistributiondata) η οποία βοηθά στην μεταφορά των δεδομένων στο πλαίσιο ενός Lan συνδράμοντας με αυτόν τον τρόπο στην μετάδοση πολλών δεδομένων των χρηστών. Η βάση της εν λόγω τεχνολογίας στηρίζεται στις οπτικές ίνες. Η τεχνολογία SMDS (switchedmultimegabitdataservice) η οποία δίνει την δυνατότητα μεταφοράς δεδομένων μιας υπηρεσίας χωρίς σύνδεση εννοώντας ότι η μεταφορά των δεδομένων μπορεί να αποθηκευτούν στην κεφαλή και είναι εφικτό να

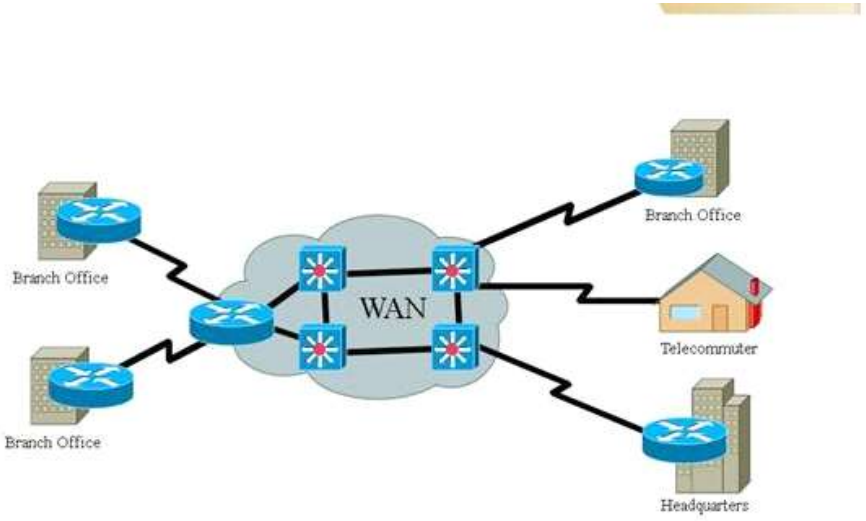
φτάσουν στον προορισμό τους με ανεξάρτητο τρόπο. Τα δεδομένα και οι πληροφορίες μπορούν να μεταδοθούν σε μεγάλη γεωγραφική έκταση. Η τεχνολογία ATM (asynchronoustransfermode), αποτελεί και την πιο συχνά χρησιμοποιούμενη τεχνολογία στα Man δίκτυα. Αφορά τεχνολογία ψηφιακής μεταφοράς δεδομένων σε πραγματικό χρόνο. Ωστόσο, αυτός ο τύπος δικτύου προσφέρει αρκετά πλεονεκτήματα όπως: την αποστολή e-mail με πιο γρήγορο τρόπο, την μεταφορά αρχείων και βάσεων δεδομένων λόγω της χρήσης της οπτικής ίνας αλλά και η διαχείριση του δικτύου γίνεται πιο αποτελεσματικά. Τέλος ένα Man δίκτυο θεωρείται πιο ασφαλές από ένα Lan και ένα Wan (Jan, 2019).



Εικόνα 3. MetropolitanAreaNetwork

Το WAN (WideAreaNetwork), αφορά ένα δίκτυο ευρείας περιοχής χωρίς να ορίζονται όρια στις αποστάσεις. Η χρησιμότητά τους προσφέρει επικοινωνία που πραγματοποιείται σε μεγάλες αποστάσεις παρέχοντας τόσο φωνή όσο και εικόνες, βίντεο καλύπτοντας μεγάλη γεωγραφική έκταση με μέγεθος ίσο όσο μια χώρας ή μιαςηπείρου. Η δικτύωσή του συνδέεται με αρκετές εταιρείες, φορείς και

οργανισμούς. Η ιδιοκτησία του δικτύου δύναται να είναι τόσο ιδιωτική όσο και δημόσια. Ωστόσο, η ταχύτητα μετάδοσης των δεδομένων είναι χαμηλή και η ταχύτητα λειτουργίας του δικτύου κυμαίνεται στα 100Mbps.Τέλος, υπάρχει μικρή ανοχή στα σφάλματα (Ginni, 2021).



Εικόνα 4. Wide Area Network

2.2 OSI Layers

Το μοντέλο OSI είναι ένα μοντέλο κατά κύριο λόγο ιεραρχικό στο οποίο συνδέονται διαφορετικές συσκευές, πρωτόκολλα και εφαρμογές και λειτουργούν μεταξύ τους με την παροχή ενός δικτύου. Ωστόσο, οι εφαρμογές και τα πρωτόκολλα που απαρτίζουν το δίκτυο υπάρχουν σε διαφορετικά επίπεδα του μοντέλου OSI όπως περιγράφονται παρακάτω (Davis, 2008):

Α) Επίπεδο 1 – Φυσικό (Layer 1-Physical): Το Φυσικό επίπεδο είναι υπεύθυνο για την σύνδεση των συσκευών. Η σύνδεση πραγματοποιείται με καλώδια Ethernet και με οπτικές ίνες. Σε αυτό το επίπεδο οι πληροφορίες περνούν μέσα από τα καλώδια με την μορφή ηλεκτρικής ενέργειας και έχουν δυαδική μορφή μηδέν ή ένα (bits),

Β) Επίπεδο 2 – Δεσμός Δεδομένων (Layer 2- DataLink): Σε αυτό το επίπεδο εντοπίζεται η λειτουργία αρκετών πρωτοκόλλων όπως: το PPP και το Frame Relay στην περίπτωση των WAN. Ωστόσο, στην περίπτωση του LAN το πρωτόκολλο που σχετίζεται με αυτό το επίπεδο είναι το Ethernet το οποίο κάνει χρήση διευθύνσεων MAC προκειμένου να εντοπίσει μοναδικές συσκευές στο δίκτυο. Τα δεδομένα του επιπέδου 2 καλούνται και ως πλαίσιο. Ακόμη, σε αυτό το επίπεδο, υπάρχουν διακόπτες Ethernet, οι οποίοι εναλλάσσουν τα πακέτα τους μέσα από ένα πίνακα διευθύνσεων MAC που διατηρούν αντιστοιχίζοντας με αυτόν τον τρόπο τις διευθύνσεις με τις θύρες που εναλλάσσονται. Παραδείγματα λειτουργίας σε αυτό το επίπεδο είναι η θύρα TCP 25 η οποία είναι SMTP, η θύρα 23 είναι Telnet, η θύρα 22 είναι SSH, η θύρα 80 είναι HTTP κ.ο.κ. Οι αριθμοί θύρας έχουν μεγάλη σημασία ειδικά στην διαμόρφωση ενός ACL. Τέλος, στο επίπεδο μεταφοράς τα δεδομένα καλούνται ως τμήμα,

Γ) Επίπεδο 3- Δίκτυο (Layer 3-Network): Το επίπεδο του δικτύου είναι εκείνο στο οποίο διαμορφώνεται το τμήμα της IP διεύθυνσης (TCP/IP). Η διεύθυνση IP είναι υπεύθυνη για το δίκτυο και λειτουργεί σε αυτό το επίπεδο. Για τον λόγο αυτό τόσο οι δρομολογητές όσο και η δρομολόγηση είναι απαραίτητα συστατικά του επιπέδου 3. Έτσι τα δεδομένα σε αυτό το επίπεδο ονομάζονται πακέτα δεδομένων,

Δ) Επίπεδο 4-Μεταφοράς (Layer 4- Transport): Στο επίπεδο μεταφοράς λειτουργούν τα πρωτόκολλα TCP και UDP. Το πρωτόκολλο TCP, εξασφαλίζει την αξιόπιστη

παράδοση των δεδομένων. Επίσης, περιλαμβάνει μηχανισμούς που διορθώνει τα σφάλματα. Σε αυτό το επίπεδο το TCP, παρέχει αριθμούς θύρας τόσο προέλευσης όσο και προορισμού οι οποίες συνδέονται με τις εφαρμογές.

Ε) Επίπεδο 5- Συνεδρία (Layer 5-Session): Κύρια αρμοδιότητα του επιπέδου 5, είναι η έναρξη αλλά και ο τερματισμός της σύνδεσης του δικτύου. Η συνάρτηση RPC η οποία είναι υπεύθυνη για την απομακρυσμένη διαδικασία κλήσης και η SQL η οποία είναι υπεύθυνη για το τμήμα σύνδεσης σε μια περίοδο σύνδεσης αποτελούν χαρακτηριστικά παραδείγματα στο επίπεδο 5,

Στ) Επίπεδο 6- Παρουσίαση (Layer 6-Presentation): Στο επίπεδο 6, περιλαμβάνονται τα δεδομένα της συνεδρίας που παρουσιάζονται στις εφαρμογές. Η κρυπτογράφηση τύπου ASCII, JPG και IPsec αποτελούν παραδείγματα του επιπέδου 6,

Ζ) Επίπεδο 7 - Εφαρμογή (Layer 7-Application): Στο επίπεδο εφαρμογής περιλαμβάνονται τα πρωτόκολλα και οι υπηρεσίες τα οποία αποτελούν την εφαρμογή. Πρωτόκολλα και εφαρμογές όπως: το Telnet, το FTP (FileTransferProtocol), το SMTP (SimpleMailTransferProtocol) αποτελούν ενδεικτικά παραδείγματα του επιπέδου 7.

2.3 Πρόσβαση στο Μέσο MAC

Στα δίκτυα υπολογιστών πολλές φορές οι υπολογιστές αναγκάζονται να κάνουν χρήση του ίδιου μέσου μεταφοράς όπως για παράδειγμα ένα καλώδιο μέσα από το οποίο γίνεται προσπάθεια εισαγωγής των δεδομένων. Συνεπώς, τα πακέτα του ενός υπολογιστή να συγκρούονται με τα πακέτα άλλου υπολογιστή με αποτέλεσμα τα πακέτα δεδομένων που αποστέλλονται από τους υπολογιστές να καταστρέφονται. Για τον λόγο αυτό, είναι αναγκαίο να βρεθεί μια λύση ώστε η αποστολή των δεδομένων μέσω του δικτύου να πληρεί τις παρακάτω συνθήκες: α) όταν εισάγονται δεδομένα

στο καλώδιο να μην επέρχεται η σύγκρουση με άλλα δεδομένα, β) η αποστολή των δεδομένων να εγγυάται την ασφαλή τους λήψη από τον παραλήπτη χωρίς αυτά να καταστρέφονται. Για τον λόγο αυτό έχουν θεσπιστεί κανόνες, οι οποίοι καθορίζουν τον τρόπο εισαγωγής δεδομένων στο καλώδιο και ονομάζεται μέθοδος προσπέλασης (accessmethod). Ωστόσο, οι μέθοδοι προσπέλασης θα πρέπει να συμφωνούν ως προς τον τρόπο εισαγωγής των δεδομένων στο καλώδιο και να εμποδίζουν την είσοδο των δεδομένων στο μέσο την ίδια στιγμή. Έτσι, μέσα από τις μεθόδους προσπέλασης θα πρέπει να εξασφαλίζεται η οργανωμένη αποστολή αλλά και λήψη των δεδομένων του δικτύου. Οι τρόποι αποφυγής ταυτόχρονης χρήσης του ίδιου μέσου μεταφοράς δεδομένων είναι οι ακόλουθοι και περιγράφονται παρακάτω:

Α) Η μέθοδος CarrierSense and Multiple Access - CSMA (Ακρόαση Φέροντος και Πολλαπλής Πρόσβασης): Η μέθοδος αυτή ελέγχει την πρόσβαση στο μέσο (MAC). Κάνει χρήση ανίχνευσης φορέα και έχει την δυνατότητα να αναβάλλει τις μεταδόσεις του εωσότου να μην γίνεται μετάδοση από κανέναν άλλον σταθμό. Η παραπάνω χρήση γίνεται σε συνδυασμό με την δυνατότητα που έχει η συγκεκριμένη μέθοδος να ανιχνεύει τις συγκρούσεις όταν γίνεται μετάδοση πλαισίου από άλλους σταθμούς. Όταν ανιχνευτεί η σύγκρουση ο σταθμός σταματά την μετάδοση του πλαισίου μεταδίδοντας σήμα εμπλοκής αναμένοντας ένα διάστημα μέχρι την αναμετάδοση. Σε αυτήν την μέθοδο περιγράφεται η διαδικασία μετάδοσης όταν ένα πλαίσιο μεταδοθεί επιτυχώς ή όταν ανιχνευθεί σύγκρουση κατά την μετάδοση (Quine, 2008).

Β) Η μέθοδος TokenPassing (Πέρασμα του Κουπονιού): Με την μέθοδο του κουπονιού δίνεται η δυνατότητα στα δίκτυα να κάνουν έλεγχο του φυσικού μέσου μέσα από ένα πλαίσιο ελέγχου όπου το κουπόνι μεταφέρεται σε κάθε κόμβο του δικτύου. Για να μεταδώσει δεδομένα ένας κόμβος είναι απαραίτητο να λάβει το

κουπόνι για να προβεί στην μετάδοση. Όταν πραγματοποιηθεί η μετάδοση των δεδομένων, τότε ο κόμβος αποδεσμεύει το κουπόνι ώστε να αξιοποιηθεί από άλλον κόμβο. Η μέθοδος αυτή πλεονεκτεί καθώς είναι εφικτό να οριστεί το χρονικό πλαίσιο μετάδοσης των δεδομένων από έναν κόμβο (Χριστοπούλου, 2013).

Κεφάλαιο 3. Επιθέσεις

Σε αυτό το κεφάλαιο παρουσιάζονται οι πιο γνωστές μορφές επιθέσεων ο τρόπος λειτουργίας αλλά και αντιμετώπισής τους. Ειδικότερα, παρουσιάζεταιτοsniffing, τοMacSpoofing, τοIPSpoofing, τοDDoS, Cashpoisoning, evil twin attack, man in the middle. Για να γίνουν πιο αντιληπτοί οι τρόποι που λειτουργούν οι συγκεκριμένες επιθέσεις παρατίθενται παραδείγματα της λειτουργία τους.

3.1 Sniffing

Το Sniffing αφορά την διαδικασία μέσα από την οποία ερμηνεύονται και αποκωδικοποιούνται τα δεδομένα που μεταδίδονται με την βοήθεια των καναλιών μετάδοσης όπως για παράδειγμα σε ένα δίκτυο TCP/IP. Το Sniffer είναι μια εφαρμογή που εκτελεί την όλη διαδικασία του Sniffing. Επίσης, ορίζεται και ως αναλυτής του πρωτοκόλλου του δικτύου. Ωστόσο, ο τρόπος λειτουργίας του διαχωρίζεται ως εξής: α) *Η αδιάκριτη λειτουργία*: μέσα από την οποία ο Sniffer, έχει την δυνατότητα να αποσπάσει πληροφορίες από τα δεδομένα που κυκλοφορούν στο δίκτυο και από τις συσκευές που είναι συνδεδεμένες στο σύστημα, β) *Η λειτουργία χωρίς αμφιβολία:* μέσα από την οποία ο sniffer μπορεί να αποσπάσει πληροφορίες και

δεδομένα οι οποίες καταλήγουν στο σύστημα. Τα δεδομένα που μπορεί να κλαπούν αφορούν ευαίσθητες πληροφορίες όπως για παράδειγμα: τα διαπιστευτήρια χρηστών (κωδικοί πρόσβασης και άλλα στοιχεία των λογαριασμών τους), αριθμούς καρτών, μηνύματα ηλεκτρονικού ταχυδρομείου κ.α. Το Sniffing, μπορεί να προκαλέσει επικίνδυνες επιθέσεις που δεν ανιχνεύονται εύκολα. Για τον λόγο αυτόν, το sniffing θα μπορούσε να διακριθεί και σε παθητικό τύπο επίθεσης όπου αυτοί που επιτίθενται να μπορούν να περνούν και απαρατήρητοι μέσα από το δίκτυο. Ευάλωτα σε επιθέσεις sniffing είναι τα πρωτόκολλα στα οποία είτε ο κωδικός πρόσβασης είτε τα δεδομένα αποστέλλονται σε σαφές κείμενο. Παράδειγμα τέτοιων πρωτοκόλλων είναι: το telnet, το http, το SMTP, το IMAP και το FTP (Prabadevi, et. al., 2018).

Πως όμως πραγματοποιούνται αυτού του είδους οι επιθέσεις από τους εισβολείς; Ο εισβολέας πραγματοποιεί επίθεση sniffing ώστε να μπορέσει να αποσπάσει πληροφορίες οι οποίες είναι ευαίσθητες και μπορεί να αφορούν και σε δεδομένα που σχετίζονται με τεχνικές λεπτομέρειες του δικτύου ώστε να διενεργήσει περισσότερες επιθέσεις τέτοιου τύπου. Στην πράξη, αυτό μπορεί να συμβεί με την χρήση εμπορικών εργαλείων λογισμικού. Ωστόσο, καταγράφονται τρεις τρόποι με τους οποίους διενεργούνται οι επιθέσεις Sniffing σε ένα δίκτυο: α) ασύρματο sniffer, το οποίο είναι αποκλειστικά σχεδιασμένο ώστε να αποσπά δεδομένα από τα ασύρματα δίκτυα. Καλείται επίσης και ασύρματο πακέτο sniffer ή ασύρματο δίκτυο sniffer., β) εξωτερικό sniffer, όπου σε αυτό το είδος υπάρχει η δυνατότητα ώστε το sniffer να παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση από μια εξωτερική τοποθεσία σε έναν διακομιστή ιστού συγκεντρώνοντας σχετικές πληροφορίες. Εν ολίγοις, το sniffing όταν πραγματοποιείται από μια θέση που είναι εξωτερική χρησιμοποιεί τα ανάλογα εργαλεία λογισμικού, γ) εσωτερικό sniffer, το οποίο είναι σχεδιασμένο για να εκμεταλλευτεί το εσωτερικό δίκτυο ενός οργανισμού. Ειδικότερα,

ο εισβολέας σε αυτήν την περίπτωση προσαρμόζει ένα μηχάνημα στο εσωτερικό δίκτυο και θέτει σε λειτουργία το sniffer προσπαθώντας να αποσπάσει πληροφορίες και δεδομένα από υπολογιστές που είναι σε σύνδεση μέσω του δικτύου. Έτσι, ο όρος sniffing σχετίζεται με δεδομένα και πληροφορίες που μπορούν να κλαπούν. Οι τρόποι που μπορεί να εφαρμοστεί το sniffing περιγράφεται ως ακολούθως: α) Μέσω του LAN, όπου οι εισβολείς μπορούν να εγκαταστήσουν ένα εργαλείο sniff σαρώνοντας όλες τις διευθύνσεις IP των υπολογιστών που απαρτίζουν το δίκτυο και βρίσκονται σε σύνδεση. Έτσι, πληροφορίες όπως: ανοικτά port, activehosts κ.α μπορούν να κλαπούν, β) μέσω ενός πρωτοκόλλου sniff, όπου οι εισβολείς προσπαθούν να αποσπάσουν πληροφορίες αναφορικά με τα πρωτόκολλα που κάνει χρήση το δίκτυο. Έτσι, οι εισβολείς επιχειρούν να καθοριστεί ένας κατάλογος με τα πρωτόκολλα και τις πληροφορίες που λαμβάνονται. Όταν καταρτιστεί η λίστα των πρωτοκόλλων γίνεται διαχωρισμός ανάλογα με τον τύπο της επίθεσης ώστε να αναπτυχθεί το κατάλληλο sniff. Πιο συγκεκριμένα, αν η λίστα των πρωτοκόλλων εμπεριέχει το UDP, τότε θα δημιουργηθεί ένα UDP Sniff , το οποίο θα προσπαθήσει να αποκρυπτογραφήσει όλες τις λεπτομέρειες που συνδέονται με τις εφαρμογές όπως αυτές του DNS και του Telnet, γ) στην περίπτωση του ARP Sniff, οι εισβολείς σαρώνουν όλες τις IP διευθύνσεις του δικτύου καθώς και τις διευθύνσεις MAC. Έχοντας λάβει αυτές τις πληροφορίες οι εισβολείς μπορούν να πραγματοποιήσουν επιθέσεις για πλαστογραφία, για επιθέσεις δρομολογητών κ.α, δ) από την κλοπή της συνεδρίας του TCP, η οποία θα αποσπάσει το δρομολόγιο της κίνησης ανάμεσα στην πηγή και στον προορισμό. Οι εισβολείς σε αυτήν την περίπτωση, ενδιαφέρονται ώστε να γνωρίζουν όλο και περισσότερα σχετικά με τις θύρες που είναι σε χρήση από το δίκτυο, τις διευθύνσεις IP αλλά και τις προσφερόμενες υπηρεσίες ώστε να επιτεθούν. Έχοντας όλα αυτά τα στοιχεία, οι εισβολείς έχουν την δυνατότητα να δημιουργήσουν

συνεδρίες ανάμεσα στις συσκευές που επικοινωνούν λειτουργώντας ως άνθρωπος που μεσολαβεί συμβάλλοντας με αυτόν τον τρόπο στην διακοπή των υπηρεσιών αλλά και για την καταγραφή των ευαίσθητων δεδομένων, ε) Sniffing σε επίπεδο εφαρμογής, οι επιθέσεις που θα πραγματοποιηθούν σε επίπεδο εφαρμογής γίνονται μέσα από την λίστα των ενεργών εφαρμογών του θύματος. Έτσι, οι εισβολείς επιτίθενται στα πακέτα δεδομένων προκειμένου να αποσπάσουν τις απαραίτητες πληροφορίες για τις εφαρμογές είτε κλέβοντάς τες είτε για να πραγματοποιήσουν περισσότερες επιθέσεις ανάλογα με την φύση της κάθε εφαρμογής που θέλουν να επιτεθούν. Όπως για παράδειγμα η επίθεση που πραγματοποιείται στα διαπιστευτήρια του χρήστη κ.α στ) Sniffing του Web Password, είναι γνωστό ότι όλες οι επικοινωνίες που πραγματοποιούνται στο διαδίκτυο γίνονται μέσα από το πρωτόκολλο του http. Οι εισβολείς μπορούν να αποσπάσουν και να κλέψουν μια συνεδρία http όπου αναλύοντάς την να προκαλέσουν επιθέσεις και poisoning των cookies. Αν και το SSL περιέχει μηχανισμούς ασφαλείας στο http, τα εργαλεία για το sniffing είναι πολύ πιο δραστικά καθώς οι ιστότοποι αποδεικνύονται ευάλωτοι μπροστά τους (Prabadevi, et. al., 2018).

Γενικά οι επιθέσεις Sniffing διακρίνονται σε δύο κατηγορίες: *α) PacketSniffing:* όπου τα πακέτα του δικτύου τίθενται υπό παρακολούθηση. Το παραπάνω δύναται να πραγματοποιηθεί μέσα από την εισαγωγή προγράμματος το οποίο θα έχει υπό την παρακολούθησή του τα πακέτα δεδομένων του δικτύου δημιουργώντας ένα αντίγραφο το οποίο προωθείται στον εισβολέα (Information Security, 1996), *β) NetworkSniffing*, αυτού του είδους οι επιθέσεις έχουν διαφορετική μορφή. Το SniffingClient πραγματοποιείται από τις ενέργειες στις γλώσσες δέσμης του χρήστη, και περιλαμβάνει το Sniffingserverside, το οποίο λαμβάνει μέρος από την πλευρά του διακομιστή κάνοντας χρήση πρωτοκόλλων επικοινωνίας. ToSniffing

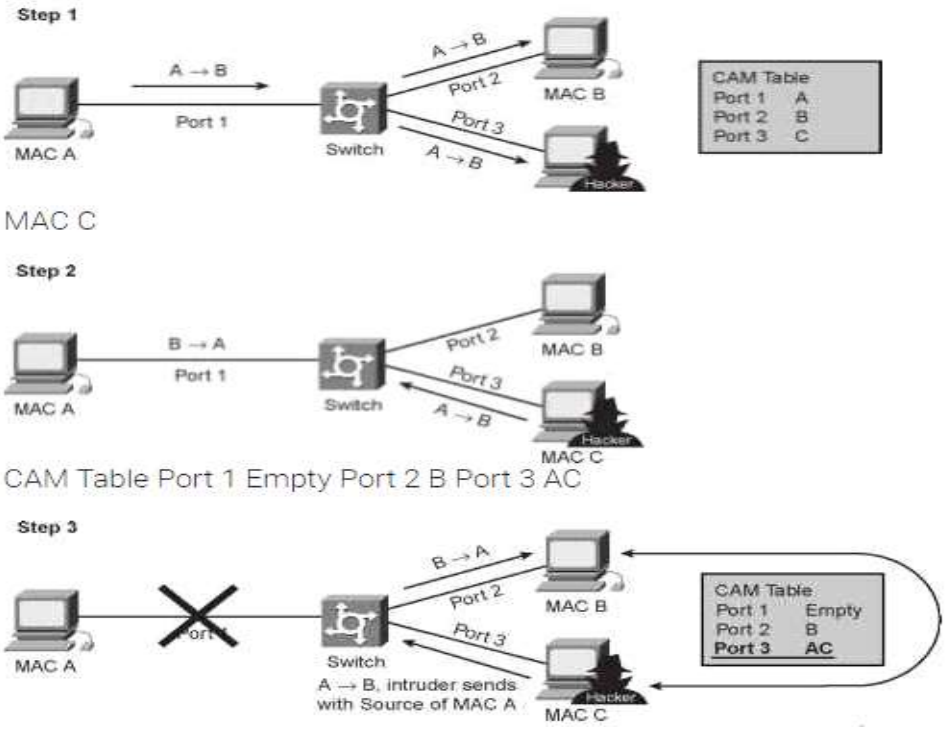
προγράμματος περιήγησης το οποίο κάνει χρήση ιστοτόπων αλλά και εφαρμογές του ιστού για τον εντοπισμό των επιθέσεων. Αυτή η μορφή του Sniffing χρησιμοποιεί πληροφορίες από το casche πρόγραμμα περιήγησης αλλά και από το ιστορικό του. Με αυτόν τον τρόπο οι εισβολείς μπορεί να αποσπάσουν τις πληροφορίες από το δίκτυο εγκαθιστώντας ένα εργαλείο sniffer(Kulshrestha, et. al, 2014). Επίσης, άλλη μορφή επίθεσης είναι το περιεχόμενο sniffing το οποίο καλείται και ως MIME Sniffing. Αυτή η μορφή επίθεσης επιχειρεί να μιμηθεί τις όποιες αλλαγές γίνονται στις εφαρμογές του ιστού καθώς οι εισβολείς στην ουσία επιχειρούν να αλλάξουν το περιεχόμενο ή ακόμα και την μορφή του αρχείου. Η μορφή αυτή βλάπτει και τις δύο πλευρές τόσο τον πελάτη όσο και τον διακομιστή. Για να αποφευχθεί η επίθεση από τους εισβολείς θα πρέπει να υπάρξει προσαρμογή στο περιεχόμενο και στις επιλογές του προγράμματος περιήγησης (Quadri, et. al., 2012 &Pandey, et.al.,2013). Επίσης, η επίθεση Sniffing στον κωδικό πρόσβασης μπορεί να αποσπάσει πολύ ευαίσθητες και ιδιωτικές πληροφορίες όπως για παράδειγμα τα διαπιστευτήρια του χρήστη (Kulshrestha, et. al, 2014).

Ωστόσο, οι επιθέσεις Sniffing στο επίπεδο δικτύου του μοντέλου OSI μπορούν να πραγματοποιηθούν με τους ακόλουθους τρεις τρόπους (Pandey, et. al., 2013): α) με βάση την διεύθυνση IP όπου το sniffing προσπαθεί να αποσπάσει τα πακέτα του δικτύου με βάση το φίλτρο IP, β) μύηση με βάση το MAC, όπου λειτουργεί με όμοιο τρόπο όπως και στην περίπτωση α με εξαίρεση ότι το sniffing προσπαθεί να αποσπάσει τα πακέτα του δικτύου βασιζόμενο στα φίλτρα των MAC διευθύνσεων, γ) με βάση το ARP, όπου το sniffing κάνει χρήση του μηνύματος αίτησης- απάντησης ARP όπου στην συνέχεια επιτίθεται στις μνήμες του με αποτέλεσμα να ανακατευθύνεται το ενδιαφέρον του εισβολέα ανάλογα με την διαμόρφωση που έχει ολοκληρωθεί.

3.2 MACSpoofing

Η επίθεση MacSpoofing αποτελεί μια άλλη μορφή επίθεσης στα πακέτα πληροφοριών και λειτουργεί ως ακολούθως. Ο εισβολέας αναζητά στο δίκτυο έγκυρες MAC διευθύνσεις. Εν συνεχεία, προσπαθεί να λειτουργήσει ως μια από αυτές κάνοντας την εμφάνιση του στην προεπιλεγμένη πύλη αντιγράφοντας όλες τις πληροφορίες που προωθούνται σε αυτήν χωρίς να γίνεται αντιληπτός. Η παραπάνω λειτουργία δίνει σημαντικές πληροφορίες στον εισβολέα αναφορικά με τις εφαρμογές που γίνονται χρήση από το σύστημα. Ως αποτέλεσμα, επιτυγχάνεται η πλαστογράφηση των πληροφοριών CAM στον διακόπτη όπως φαίνεται στο σχήμα που ακολουθεί.

Από το σχήμα προκύπτει ότι από τις συσκευές A, B, C του πίνακα CAM, η συσκευή C είναι ο εισβολέας. Μετά από την πλαστογράφηση της διεύθυνσης MAC



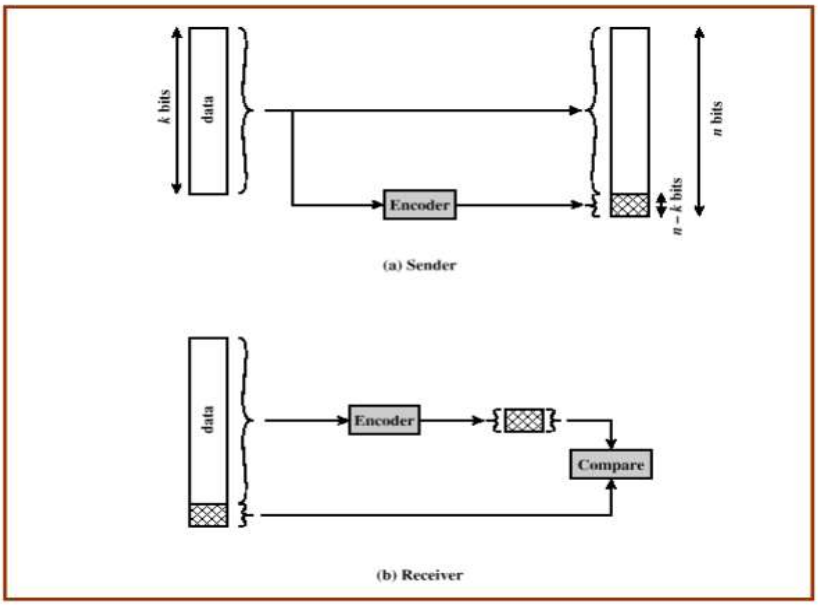
Εικόνα 5. MacSpoofingAttack

της συσκευής Α, ο εισβολέας δηλαδή η συσκευή C, στέλνει μια πλαστή διεύθυνση IP. Στην συνέχεια, ο διακόπτης μαθαίνει εκ νέου την διεύθυνση MAC και προβαίνει σε αλλαγή των καταχωρήσεων του πίνακα MAC. Όταν η συσκευή Β, θα προβεί σε επικοινωνία με την συσκευή Α, ο διακόπτης θα αποστείλει το πακέτο σύμφωνα πάντα με τις καταχωρήσεις του πίνακα CAM όπου σύμφωνα με το σχήμα βρίσκεται στο port 3. Εωσότου, η συσκευή Α αποστείλει ξανά πακέτα δεν αλλάζει κάτι στην ροή που έχουν τα δεδομένα με αποτέλεσμα ο εισβολέας να λαμβάνει αλλά και να παρακολουθεί τα ήδη ενεργά πακέτα εξασφαλίζοντας με αυτόν τον τρόπο την διατήρηση της σύνδεσής του μέχρι να παρέμβει ο διαχειριστής του δικτύου. Ωστόσο, για να μετριαστεί αυτή του είδους η επίθεση, θα πρέπει να έχει προηγηθεί ένας πολύ καλός σχεδιασμός του δικτύου καθώς ο εισβολέας συμπεριφέρεται πολύ έξυπνα. Μια λύση που θα μπορούσε να μετριάσει την επίθεση είναι η χρήση ιδιωτικών VLAN καθώς οι θύρες περιορίζονται σε ένα VLAN οι οποίες επικοινωνούν με άλλες θύρες του ίδιου δικτύου. Μια άλλη μέθοδος σε συνδυασμό με την ασφάλεια των θυρών είναι η χρήση μηχανισμών παρακολούθησης DCHP. Με αυτόν τον τρόπο εξασφαλίζονται μόνο οι έγκυροι διακομιστές DCHP οι οποίοι είναι ενεργοί στο δίκτυο. Ωστόσο, ένας τέτοιος μηχανισμός εξασφαλίζει την ροή αξιόπιστων δεδομένων ανάμεσα στον πελάτη –διακομιστή. Ακόμη, η χρήση DHCP Snooping σε συνδυασμό με το DAI (Dynamic ARP Inspection) αποτελεί την καλύτερη λύση. Έτσι, όταν αποστέλλεται ένα μήνυμα μετάδοσης για μια διεύθυνση IP, ο εισβολέας το αντιλαμβάνεται. Μόνο που η εκπομπή του μηνύματος αποστέλλεται σε όλες τις θύρες εκτός από την θύρα προέλευσης. Με αυτόν τον τρόπο το δίκτυο δεν επιτρέπει την αποστολή είτε των θετικών είτε των αρνητικών επιβεβαιώσεων από πηγές που δεν είναι αξιόπιστες. Τα μη αξιόπιστα μηνύματα DHCP συνήθως λαμβάνονται από το τείχος προστασίας ή από κάποιο εξωτερικό δίκτυο. Ο πίνακας DHCP Snooping

εμπεριέχει στοιχεία όπως τις διευθύνσεις IP και Mac, τον αριθμό του δικτύου, και όλες αυτές τις πληροφορίες που αντιστοιχούν σε μη αξιόπιστες διεπαφές. Βέβαια, ο πίνακας DHCP, δεν περιλαμβάνει δεδομένα που αφορούν κεντρικούς υπολογιστές ή την σύνδεσή τους με αξιόπιστες διεπαφές. Η διαμόρφωση τόσο αξιόπιστων όσο και αναξιόπιστων πηγών είναι εφικτή η ρύθμιση του διακόπτη ώστε να αποτρέπει μη νόμιμα πλαίσια. Ωστόσο, το DHCP Snooping δεν μπορεί να σταματήσει τον εισβολέα ώστε να επιτίθεται σε διευθύνσεις Mac. Το DAI, ορίζει το πόσο έγκυρο είναι ένα πακέτο ARP βασιζόμενο στην δέσμευση διευθύνσεων Mac προς διευθύνσεις IP οι οποίες βρίσκονται αποθηκευμένες σε μια βάση δεδομένων DHCP. Πρακτικά, αυτό σημαίνει ότι μόνο οι έγκυρες διευθύνσεις επιτρέπονται και αφορούν συσκευές του δικτύου που είναι εξουσιοδοτημένες. Οι εισβολείς επειδή λειτουργούν έξυπνα αναμένουν κάποια αναπήδηση του δικτύου για συσκευές που δεν είναι ενεργές (Cisco, 2021).

Σε αυτό το επίπεδο οι τεχνικές ανίχνευσης και διόρθωσης λαθών έχουν την βάση τους στην αποστολή των δεδομένων εξασφαλίζοντας ότι η ακολουθία των bit συμβαδίζει με έναν κανόνα ο οποίος είναι αποδεκτός και περιγράφεται παρακάτω: α*) η ανίχνευση του λάθους:* ο παραλήπτης των δεδομένων καταλαβαίνει ότι τα δεδομένα δεν συμβαδίζουν με τον αποδεκτό κανόνα, *β) διόρθωση του λάθους*, όταν ο παραλήπτης των δεδομένων προβαίνει στην αντικατάσταση ενός τμήματος δεδομένων που συμβαδίζουν με τον αποδεκτό κανόνα. Στα ενσύρματα μέσα τα οποία θεωρούνται και αξιόπιστα η πιο συνήθης πρακτική είναι η ανίχνευση του σφάλματος και η επαναμετάδοση των δεδομένων. Στα μέσα που δεν θεωρούνται αξιόπιστα και συνήθως είναι τα ασύρματα μέσα, η ανίχνευση και η διόρθωση των λαθών θεωρείται απαραίτητη. Στο παρακάτω σχήμα 5β απεικονίζεται η τεχνική ανίχνευσης και διόρθωσης λαθών.

Προκειμένου να ανιχνευτούν τα λάθη χρησιμοποιούνται οι ακόλουθες τεχνικές: *α) ο έλεγχος ισοτιμίας και β) η τεχνική CRC (CyclicRedundancyCheck (Crc), γ) Έλεγχος Πολλαπλής Πρόσβασης*. Στον έλεγχο Ισοτιμίας, γίνεται ένας απλός έλεγχος για την ανίχνευση του λάθους ο οποίος πραγματοποιείται με την προσθήκη ενός bit στο τέλος των δεδομένων. Ο έλεγχος ισοτιμίας αφορά την άρτια ισοτιμία όπου γίνεται προσθήκη ενός λογικού 1 διασφαλίζοντας με αυτόν τον τρόπο την παρουσία άρτιου αριθμού λογικών 1 και με την περιττή ισοτιμία όπου η προσθήκη του λογικού 1 διασφαλίζει την παρουσία του περιττού αριθμού λογικών 1.



Εικόνα 6. Τεχνικές Διόρθωσης και Ανίχνευσης Λαθών

Η τεχνική CRC (CyclicRedundancyCheck), έχει την βάση της στην προσθήκη ενός ακόμη bit προκειμένου να δημιουργηθεί μια νέα λέξη όπου αν διαιρεθεί με μια συγκεκριμένη λέξη θα δώσει υπόλοιπο μηδέν. Πιο συγκεκριμένα, στην φάση της εκπομπής υπολογίζονται τα bit που θα προστεθούν στο τέλος της κάθε λέξης και στην συνέχεια αυτή αποστέλλεται. Κατά την λήψη, η λέξη που λαμβάνεται διαιρείται και

αν το υπόλοιπο που δώσει είναι μηδέν τότε εντοπίζεται το λάθος. Τέλος, στην τελευταία τεχνική, που αφορά τον έλεγχο πολλαπλής πρόσβασης, η χρήση των κοινών μέσων μετάδοσης έχει την βάση της στην υιοθέτηση κανόνων οι οποίοι είναι κοινοί τόσο για τον έλεγχο όσο και για την χρήση του μέσου. Ωστόσο, το περιεχόμενο του κανόνα μπορεί να έχει αρκετές μορφές αλλά στην περίπτωση των δικτύων η τεχνική που είναι η πιο σύνηθες αφορά την πολλαπλή πρόσβαση με ανίχνευση φέροντος όπου σε αυτήν την περίπτωση ο χρήστης ανιχνεύει το αν υπάρχουν εκπομπές και αναμένει εωσότου το μέσονα είναι ξανά διαθέσιμο, στην ανίχνευση συγκρούσεων όταν παίρνουν χώρα πολλές ταυτόχρονες εκπομπές στο κοινόχρηστο μέσο.

3.3 IPSpoofing

Το κύριο πρωτόκολλο προκειμένου να επιτευχθεί η επικοινωνία μέσω του διαδικτύου είναι το IP. Το πρωτόκολλο αυτό περιέχει στοιχεία όπως την δική του κεφαλίδα με όλα τα απαραίτητα συστατικά που την συνοδεύουν τα οποία υποδηλώνουν την πηγή αλλά και τον προορισμό του πακέτου (Postel, 1981). Τα στοιχεία αυτά είναι αναγκαία και έχουν ήδη σχηματιστεί πριν την αποστολή του πακέτου. Ωστόσο, αν η διεύθυνση της κεφαλίδας προέλευσης του πακέτου δεν είναι νόμιμη και είναι πλαστή, τότε το πακέτο θα φανεί ότι στάλθηκε από κάποια άλλη πηγή. Από τα παραπάνω, προκύπτει ότι η πλαστογράφηση της IP διεύθυνσης καλείται και ως IP Spoofing.Η εν λόγω τεχνική χρησιμοποιείται από τους εισβολείς ώστε να καλύψουν την ταυτότητά τους. Κατά κύριο λόγο, η τεχνική του IP Spoofing χρησιμοποιείται για την αποστολή ανεπιθύμητων μηνυμάτων και για τις επιθέσεις του ηλεκτρονικού ψαρέματος αλλά και με την κατανεμημένη άρνηση υπηρεσίας DDoS. Ωστόσο, το IP Spoofing είναι ένα πρόβλημα που δεν έχει εύκολη λύση. Για παράδειγμα, επιθέσεις όπως: DDoS και TCP SYN με πλαστές IP πλημμυρίζουν και

φράζουν το δίκτυο. Τα μηνύματα του ηλεκτρονικού ψαρέματος, κοστίζουν αρκετά στα θύματα των επιθέσεων χάνοντας χρήματα και ο phisher δεν είναι εύκολα εντοπίσιμος. Όσα έχουν προαναφερθεί αποτελούν σημαντικές περιπτώσεις που πρέπει να αντιμετωπιστούν. Ωστόσο, υπάρχουν τρόποι άμυνας από το spoofing. Οι τρόποι άμυνας μπορούν να διακριθούν στις ακόλουθες κατηγορίες: α) Η πρόληψη πριν από την μετάδοση, β) η πρόληψη κατά την μετάδοση και γ) η πρόληψη μετά την μετάδοση (Ferguson, et.al., 2000).

Στην πρώτη περίπτωση, σύμφωνα με το φιλτράρισμα του δικτύου οριζόμενο και ως networkingressfiltering, η κίνηση προωθείται αν η διεύθυνση IP ανήκει στο δίκτυο και απαιτείται αρκετός χρόνος για την ανάπτυξή του στο διαδίκτυο. Ωστόσο, το φίλτρο εμποδίζει το δίκτυο ώστε να χρησιμοποιείται ως θύμα πλαστών διευθύνσεων. Παρόλαυτα, το δίκτυο δεν ήρθε αντιμέτωπο με πλαστά πακέτα δικτύου. Επίσης, σε αυτήν την περίπτωση το φιλτράρισμα, προϋποθέτει από κάθε κόμβο του δικτύου να αναπτυχθεί πριν τεθεί σε εφαρμογή και από τους δρομολογητές απαιτούνται επιπλέον διαμορφώσεις (Soon, et.al., 2009).

Στην δεύτερη περίπτωση, σύμφωνα με το φιλτράρισμα διαδρομής (RBF), γίνεται επέκταση του ingressfiltering βασιζόμενο στην τοπολογία του δικτύου. Σε αυτήν την περίπτωση, συλλέγονται με αυτόνομο τρόπο, οι πληροφορίες που θεωρούνται ύποπτες και γίνονται ενημερώσεις όταν υφίστανται αλλαγές στον πίνακα δρομολόγησης (Mirkovic, et. al., 2006).

Στην βιβλιογραφία, εντοπίζονται οι καταχωρήσεις του πίνακα και η ενημέρωση που γίνεται στην δρομολόγηση όταν πραγματοποιούνται αλλαγές και στο φιλτράρισμα ενός πλαστού πακέτου κάνοντας χρήση των πληροφοριών του πίνακα. Η διαχείριση του συστήματος στην πρώτη περίπτωση γίνεται με το σύστημα Clouseau

και στην δεύτερη περίπτωση με την χρήση του RBF. Η διαχείριση με το σύστημα Clouseau περιλαμβάνει το πακέτο δεδομένων TCP το οποίο φτάνει στον δρομολογητή, παρατηρώντας την αναμετάδοση του από την πηγή. Την ίδια στιγμή, το RBF, προβαίνει σε φιλτράρισμα των πακέτων που είναι πλαστά κάνοντας σύγκριση της διεπαφής που αναμένεται με την εισερχόμενη. Ωστόσο, το RBF λειτουργεί καλύτερα σε μικρότερα δίκτυα και για αυτόν τον λόγο αποτελεί πρόβλημα η ανίχνευση ενός πλαστού πακέτου σε μεγαλύτερο δίκτυο με περισσότερους υπολογιστές και αυτόνομα συστήματα. Βέβαια, αν το πλαστό πακέτο αποσταλεί από ένα δίκτυο σε ένα άλλο αντιμετωπίζεται σαν να έχει προέλθει από άλλη διεπαφή. Στην μέθοδο SMP (Spoofing Prevention Method), ο δρομολογητής ο οποίος είναι ο κοντινότερος στον προορισμό του πακέτου έχει την δυνατότητα να επιβεβαιώνει την αυθεντικότητα της διεύθυνσής του (Bremler-Barr & Levy, 2005). Ακόμη, οι δρομολογητές προβαίνουν σε έλεγχο του πακέτου και των ετικετών του που έχει σχέση με τον προορισμό. Κάθε ζεύγος πηγής και προορισμού του δικτύου έχει ένα μοναδικό κλειδί και είναι από την αρχή γνωστό τόσο στην πηγή όσο και στον προορισμό καθώς επίσης χρησιμοποιείται και σαν μηχανισμός ταυτότητας των πακέτων που εισέρχονται. Ωστόσο, τα κλειδιά υπάρχουν στα πακέτα όταν τα στέλνουν οι δρομολογητές αλλά αφαιρούνται όταν γίνεται έλεγχος ταυτότητας του κλειδιού. Έτσι, όταν ο ISP, εντοπίζει κάποια επίθεση στο δίκτυο ο τρόπος που αμύνεται και προστατεύεται είναι με το να επιτρέπει μόνο τα πακέτα που προέρχονται από το δίκτυο του SPM για να είναι σίγουροι ότι δεν θα υπάρξει κάποια δυσλειτουργία στην κυκλοφορία. Ακόμη, μια άλλη μέθοδος για τον περιορισμό της πλαστογράφησης των IP είναι το Distributed Packet Filtering (Park, et. al., 2001). Σε αυτήν την περίπτωση, υπολογίζεται ένα σύνολο διαδρομών και επιλέγεται η καλύτερη διαδρομή. Έτσι, στο DPF, εφαρμόζεται η συντομότερη διαδρομή. Ωστόσο,

αν το πακέτο έφτασε από διεπαφή που δεν είναι αναμενόμενη, το πακέτο θα πέσει. Βέβαια, το DPF έχει την δυνατότητα να εντοπίσει τον εισβολέα, ωστόσο η ανίχνευση της τοποθεσίας του εισβολέα μπορεί να γίνει βάση διαδρομής και έχει την δυνατότητα να ελαχιστοποιήσει το δίκτυο του εισβολέα σαν ένα πολύ μικρό εύρος δικτύου. Αν τα πλαστογραφημένα πακέτα του δικτύου υποστούν φιλτράρισμα και βρίσκονται κοντά στον εισβολέα οι επιθέσεις είναι δυνατόν να εντοπιστούν (Ohtsuka, Nakamura, Sekiya, & Wakahara, 2007). Το πακέτο που εξέρχεται του δικτύου και πηγαίνει στον επόμενο δρομολογητή φέρει την δική του υπογραφή. Το NLT (Neighboor Link Table) εμπεριέχει πληροφορίες για την τοπολογία του δικτύου, την διεπαφή και τον προηγούμενο δρομολογητή. Για να ανιχνευτούν τα πλαστά πακέτα υποβάλλεται ερώτηση στο NTL για την υπογραφή τους. Ακόμη, το SAVE (Source Address Validation) είναι ένα πρωτόκολλο το οποίο συλλέγει πληροφορίες ώστε να επικυρωθεί η διεύθυνση του πακέτου που εισέρχεται στο δίκτυο (Li et al, 2009). Το πρωτόκολλο αυτό περιέχει μηχανισμούς anti - spoofing σε όλο το δίκτυο, καταγράφοντας την διαδρομή που έχει διασχίσει το πακέτο και εξασφαλίζει την σωστή διαδρομή. Και το RBF δύναται να περιορίσει τις διευθύνσεις IP που υφίστανται επίθεση. Ωστόσο, και το DPF και το SAVE βελτίωσαν το RBF κάνοντας προώθηση μόνο σε πακέτα που προέρχονταν από σωστές διεπαφές. Η επαλήθευση της πηγής της προώθησης των πακέτων για την αντιμετώπιση του spoofing θεωρείται αποτελεσματικός τρόπος αντιμετώπισης (Shue, Gupta & Davy, 2008).

Στην τρίτη περίπτωση, προτείνεται η άμυνα βασισμένη στο TTL (Time to Live) πακέτο υπολογίζοντας την συνολική διαδρομή του πακέτου από την πηγή στον προορισμό. Η τιμή TTL είναι ακριβής και δεν μπορεί να πλαστογραφηθεί εύκολα. Το πεδίο TTL μιας κεφαλίδας διεύθυνσης IP ορίζει και την διάρκεια ζωής του πακέτου.

Κάθε φορά που ένα πακέτο φτάνει στον προορισμό αφαιρείται η αρχική τιμή του για να ληφθεί ο συνολικός αριθμός hop του πακέτου (Wang, et. al., 2007).

3.4 DistributedDenialofService (DDoS)

Η επίθεση της κατανεμημένης άρνησης υπηρεσίας (DDoS-Distributed Denial of Service) σχετίζεται με την προσπάθεια αποδόμησης των συστημάτων του διαδικτύου ή των διακομιστών του ιστού γεμίζοντάς τους συνεχώς με δεδομένα. Τέτοιου είδους επιθέσεις μπορεί να είναι απλές επιθέσεις που ενοχλούν λίγο ή να αφορούν ακόμη και σε διακοπή λειτουργίας ενός οργανισμού. Συνήθως αφορά μια μεγάλη ομάδα από κατανεμημένους υπολογιστές οι οποίοι βρίσκονται σε συνεννόηση μεταξύ τους την ίδια στιγμή προσπαθώντας να «σπαμάρουν» έναν ιστότοπο ή έναν πάροχο υπηρεσιών με αιτήματα δεδομένων. Ο τρόπος που συμβαίνει αυτό είναι η χρήση και η εγκατάσταση κακόβουλου λογισμικού στα συστήματα των χρηστών. Όπως έχει αναφερθεί, οι επιθέσεις αυτές γίνονται από μεγάλο αριθμό υπολογιστών για να επιτύχουν τον στόχο τους. Ωστόσο, για να επιτευχθεί ο έλεγχος των πολλών μηχανημάτων ο πιο εύκολος και οικονομικότερος τρόπος είναι αυτός των εκμεταλλεύσεων. Οι επιθέσεις αυτής της μορφής, προβαίνουν στον έλεγχο των Wi-Fi καμερών με κωδικούς οι οποίοι είναι ήδη προεπιλεγμένοι με στόχο να δημιουργηθεί ένα μεγάλο botnet. Όταν το botnet είναι έτοιμο, οι εισβολείς βρίσκουν την κατάλληλη στιγμή για να επιτεθούν με την αποστολή της έναρξης σε όλους τους κόμβους του και εν συνεχεία με την αποστολή των αιτημάτων τους στον διακομιστή του προορισμού. Αν η επίθεση καταφέρει να κάμψει τις εξωτερικές άμυνες πολύ γρήγορα κατακλύζονται όλα τα συστήματα έχοντας ως αποτέλεσμα την παύση λειτουργίας του διακομιστή. Ως συνέπεια των παραπάνω, είναι η χαμηλή παραγωγικότητα ακόμα και

η παύση μιας υπηρεσίας καθώς οι χρήστες δεν έχουν ούτε πρόσβαση ούτε μπορούν να δουν τον ιστότοπο. Το 2017, ο Kasperky ανέφερε ότι οι επιθέσεις αυτές ενέχουν μεγάλο κόστος για τους οργανισμούς. Για παράδειγμα, στις μικρές επιχειρήσεις το κόστος μπορεί να ανέλθει στις 120.000 δολάρια και στις πιο μεγάλες επιχειρήσεις το κόστος μπορεί να φτάσει ακόμα και τα 2.000.000 δολάρια. Οι επιθέσεις μπορεί να περιλαμβάνουν τα πάντα από μια παιδική φάρσα έως και τον εκφοβισμό των οργανισμών. Ωστόσο, θεωρούνται παράνομες σύμφωνα με το νομικό πλαίσιο περί υπολογιστών και ενέχουν ποινή φυλάκισης έως και δέκα έτη αν η επίθεση πραγματοποιηθεί σε ένα δίκτυο χωρίς άδεια (Petters, 2020).

Για να ανταπεξέλθει ένα σύστημα στις επιθέσεις θα πρέπει να είναι προετοιμασμένο. Με άλλα λόγια, στα συστήματα θα πρέπει να έχουν δημιουργηθεί ειδοποιήσεις προκειμένου να διαγνωστεί μια επίθεση έγκαιρα και να τερματιστεί χωρίς να επηρεαστούν οι χρήστες. Ωστόσο, υπάρχει η δυνατότητα να αποκλειστούν οι διευθύνσεις IP, κάνοντας χρήση του τείχους προστασίας ή ακόμη να κλείσει η κυκλοφορία του κύριου συστήματος και η μετάβαση του σε αντίγραφο ασφαλείας. Βέβαια, υπάρχουν και άλλα σχέδια ανταπόκρισης που μπορούν να εφαρμόσουν οι οργανισμοί. Οι επιθέσεις DDoS έχουν διάφορες μορφές όπως περιγράφεται παρακάτω: α) επιθέσεις επιπέδου εφαρμογής: η μορφή αυτή στοχεύει στην εξάντληση των πόρων του δικτύου, με στόχο να ανακόψει την πρόσβαση στους ιστοτόπους. Έτσι, οι εισβολείς αποστέλλουν ένα περίπλοκο αίτημα όπως πρόσβαση σε βάσεις δεομένων ακόμα και λήψεις οι οποίες είναι μεγάλες καθώς ο διακομιστής προσπαθεί να ανταποκριθεί σε αυτό. Ωστόσο, αν τα αιτήματα αυτά είναι πολλά και αποσταλούν σε σύντομο χρονικό διάστημα το σύστημα θα επιβραδυνθεί. Για παράδειγμα, μια επίθεση πλημμύρας στο http αποτελεί χαρακτηριστικό παράδειγμα επιπέδου εφαρμογής με στόχο έναν διακομιστή ιστού, β) επιθέσεις πρωτοκόλλων: οι επιθέσεις

αυτές έχουν ως στόχο το επίπεδο δικτύωσης των συστημάτων κατακλύζοντας τις βασικές υπηρεσίες δικτύωσης όπως επίσης και το τείχος προστασίας με αιτήματα προς τον στόχο. Πιο συγκεκριμένα, οι υπηρεσίες ενός δικτύου λειτουργούν με μια ουρά προτεραιότητας όπου εισάγεται το πρώτο αίτημα και αφού το επεξεργάζεται εν συνεχεία εισάγεται το δεύτερο αίτημα κ.ο.κ. Ωστόσο, μια επίθεση DDoS μπορεί να κάνει την ουρά τόσο μεγάλη σε ένα σύστημα το οποίο δεν έχει τόσους μεγάλους πόρους για να το αντιμετωπίσει. Γενικότερα, οι υπηρεσίες ενός δικτύου αναφορικά με τα αιτήματα που υπάρχουν στην ουρά, λειτουργούν ως εξής: το πρώτο αίτημα που εισάγεται είναι και αυτό που εξέρχεται πρώτο της ουράς. Έτσι, το πρώτο αίτημα που εισέρχεται στην ουρά, τίθεται υπό επεξεργασία, αποδεσμεύεται και εισάγεται το επόμενο κ.ο.κ. Έτσι, μια μορφή τέτοιου είδους επίθεση είναι η πλημμύρα SYN. Για παράδειγμα, η μορφή αυτή σε μια συναλλαγή TCP/IP αποτελείται από τρεις κατευθυντήριες. Η πρώτη λέγεται SYN και αποτελεί το πρώτο μέρος ενός αιτήματος, η δεύτερη λέγεται ACK και αποτελεί την απάντηση που δίνει ο στόχος και η τρίτη λέγεται SYNACKκαι αποτελεί το μήνυμα της απάντησης που ευχαριστεί για το μήνυμα που έλαβε. Έτσι, σε μια επίθεση SYNδημιουργούνται πακέτα με ψεύτικες διευθύνσεις IP. Πιο συγκεκριμένα, ο στόχος αποστέλλει ένα ACKσε μια εικονική διεύθυνση από την οποία δεν λαμβάνει ποτέ απάντηση αναμένοντας τις απαντήσεις για να τερματίσει γεγονός που από μόνο του εξαντλεί τους πόρους του συστήματος. Μια άλλη μορφή επίθεσης είναι και οι λεγόμενες Volumetric επιθέσεις οι οποίες έχουν σαν στόχο την δημιουργία αρκετά μεγάλου όγκου κίνησης στις συναλλαγές προκειμένου να μπλοκάρει τον στόχο ζητώντας συνεχώς από τον στόχο με αποτέλεσμα την αύξηση του μεγέθους απόκρισης φράζοντας στην ουσία τον διακομιστή.

Οι επιθέσεις του DDoS μπορούν να προληφθούν με προετοιμασία και προγραμματισμό. Η ενεργοποίηση της υπηρεσίας μετριασμού DDoS εκτόπισε την εισερχόμενη κίνηση αποκλείοντας τα πακέτα που εμπεριείχαν κακόβουλα στοιχεία έχοντας ως συνέπεια την αποχώρηση των εισβολέων. Τέλος, οι επιθέσεις DDoSθεωρούνται ιδιαίτερα επιζήμιες για τις επιχειρήσεις (Petters, 2020).

3.5 CashPoisoning

Η CashPoisoning είναι μια επίθεση που αφορά τον κυβερνοχώρο, όπου οι εισβολείς εισαγάγουν πληροφορίες που είναι ψεύτικες σε μια προσωρινή μνήμη συστήματος ονομάτων τομέα που λέγεται DNS ή σε μια προσωρινή μνήμη ιστού με απώτερο σκοπό να αποσπάσουν πληροφορίες από τους χρήστες. Μια τέτοιου είδους επίθεση πραγματοποιείται όταν ένας εισβολέας προσπαθεί να επιφέρει δυσλειτουργία στην κυκλοφορία από έναν διακομιστή που είναι νόμιμος σε έναν διακομιστή που είναι επικίνδυνος. Έτσι, ο εισβολέας εισάγει ψεύτικες πληροφορίες όπως για παράδειγμα μια διεύθυνση ιστοτόπου που είναι αλλοιωμένη στην κρυφή μνήμη οδηγώντας την ανακατεύθυνση των χρηστών σε επικίνδυνους ιστότοπους. Αυτή η επίθεση είναι μια εξαιρετικά επικίνδυνη επίθεση όχι μόνο γιατί δημιουργεί προβλήματα στην επισκεψιμότητα των νόμιμων ιστοτόπων αλλά κατά κύριο λόγο γιατί οι χρήστες που πέφτουν θύματα αυτών των επιθέσεων είναι πραγματικά εκτεθειμένοι σε κακόβουλο λογισμικό και σε υποκλοπή των δεδομένων τους. Όταν η κρυφή μνήμη ενός ιστού δηλητηριάζεται, ο εισβολέας εκμεταλλεύεται τον διακομιστή για να εξυπηρετήσει κακόβουλες αποκρίσεις του πρωτοκόλλου μεταφοράς (HTTP) στους χρήστες του δικτύου (Awati, 2021).

Έτσι, η δηλητηρίαση της κρυφής μνήμης πραγματοποιείται όταν εισάγονται ψευδής πληροφορίες με αποτέλεσμα το πρόγραμμα περιήγησης του ιστού να

επιστρέφει λανθασμένες απαντήσεις στους χρήστες του δικτύου. Οι απαντήσεις που λαμβάνουν οι χρήστες συνήθως τους κατευθύνει σε διαφορετικούς ιστότοπους από αυτούς που είχαν σκοπό να επισκεφτούν. Οι συσκευές επίλυσης DNS δεν έχουν την δυνατότητα να επαληθεύσουν τα δεδομένα που βρίσκονται αποθηκευμένα στην κρυφή μνήμη. Το γεγονός αυτό σημαίνει ότι οι ψευδείς πληροφορίες παραμένουν αποθηκευμένες στην μνήμη cash μέχρι την λήξη του TTL. Αν και η δηλητηρίαση της κρυφής μνήμης ουσιαστικά δεν αποσυνδέει τον πραγματικό ιστότοπο από την αληθινή IP διεύθυνση, ωστόσο αν οι ψευδής πληροφορίες παραμείνουν στην κρυφή μνήμη οι χρήστες του δικτύου θα συνεχίσουν να οδηγούνται σε λάθος ιστότοπους. Οι κίνδυνοι που ελλοχεύουν και σχετίζονται με την δηλητηρίαση της κρυφής μνήμης είναι η μόλυνση από κακόβουλο λογισμικό, η υποκλοπή των δεδομένων των χρηστών και η παρεμπόδιση των ενημερώσεων ασφαλείας. Η πρώτη περίπτωση δίνει την δυνατότητα στους εισβολείς να εγκαταστήσουν κακόβουλο λογισμικό στα συστήματα των χρηστών μέσα από αυτοματοποιημένες λήψεις. Η δεύτερη περίπτωση, μπορεί να οδηγήσει σε παραβίαση των προσωπικών δεδομένων των χρηστών και η Τρίτη περίπτωση μπορεί να παρεμποδίσει σημαντικές ενημερώσεις ασφαλείας των συστημάτων ασφαλείας των χρηστών τα οποία είναι εκτεθειμένα σε ιούς (Awati, 2021).

Η απόκριση σε μια κακόβουλη επίθεση μπορεί να πάρει άλλες διαστάσεις αν υπάρξει προσωρινή αποθήκευση στην μνήμη του προγράμματος περιήγησης που χρησιμοποιούν οι χρήστες ή στην προσωρινή μνήμη του ιστού η οποία προσπελάσετε από αρκετούς χρήστες. Ωστόσο, αν η απόκριση σε μια επίθεση τελικά επιτυγχάνει την προσωρινή αποθήκευση σε μια μνήμη ιστού η οποία είναι κοινόχρηστη, έχει σαν αποτέλεσμα την συνεχή λήψη κακόβουλου λογισμικού από τους χρήστες που την χρησιμοποιούν μέχρι να γίνει εκκαθάριση της προσωρινής μνήμης. Το ίδιο συμβαίνει

και από προγράμματα που χρησιμοποιούνται από μεμονωμένους χρήστες οι οποίοι θα συνεχίσουν να λαμβάνουν κακόβουλο περιεχόμενο μέχρι την εκκαθάριση της προσωρινής μνήμης. Ωστόσο θεωρούνται επιτυχείς οι επιθέσεις από τους εισβολείς όταν: α) ο κωδικός της υπηρεσίας είναι ευάλωτος και επιτρέπει το γέμισμα του πεδίου κεφαλίδας HTTP με πολλές περισσότερες, β) γίνεται η αποστολή ενός κατασκευασμένου μηνύματος το οποίο αποθηκεύεται στην προσωρινή μνήμη, γ) υποχρεώνει τον διακομιστή της προσωρινής μνήμης να προβεί στην εκκαθάριση του ουσιαστικού περιεχομένου της, δ) προβαίνει στην αποστολή του επόμενου αιτήματος όπου η πρότερη εισαγωγή περιεχομένου ουσιαστικά αποτελεί και την απάντηση σε αυτό το αίτημα. Η μορφή αυτή της επίθεσης ουσιαστικά θεωρείται όχι και τόσο εύκολα πραγματοποιήσιμη σε ένα ρεαλιστικό περιβάλλον λόγω του ότι πρέπει να ικανοποιεί πολλές συνθήκες. Παρόλα αυτά, η cachepoisoning επίθεση είναι πιο εύκολα πραγματοποιήσιμη καθώς επιτρέπει την διάκριση απόκρισης HTTP και των μειονεκτημάτων στην εφαρμογή του ιστού. Από την πλευρά του εισβολέα θεωρείται σημαντικό το γεγονός ότι μια εφαρμογή δίνει την δυνατότητα στο πεδίο της κεφαλίδας να συμπληρωθεί με περισσότερες από μια κάνοντας χρήση χαρακτήρων CR (CarriageReturn) και LF(LineFeed). Για να γίνει απόλυτα κατανοητή αυτή η μορφή επίθεσης, παρακάτω παρατίθενται τα ακόλουθα παραδείγματα.

Για παράδειγμα, σε μια ιστοσελίδα όπου το όνομά της ορίζεται από το όρισμα ‘σελίδα’ και εν συνεχεία γίνεται ανακατεύθυνση 302 στην εν λόγω υπηρεσία η διαδικασία που ακολουθείται περιγράφεται στα ακόλουθα τμήματα κώδικα τα οποία παρουσιάζονται παρακάτω:

http://testsite.com/redir.php?page=http://other.testsite.com/

και ο κώδικας redir.php:

```
rezos@dojo ~/public_html $ cat redir.php
<?php
header ("Location: " . $_GET['page']);
?>
```

Έπειτα δημιουργείται το αίτημα με την αφαίρεση της σελίδας από την προσωρινή μνήμη:

```
GEThttp://testsite.com/index.htmlHTTP/1.1
Pragma:no-cache
Host:testsite.com
User-Agent:Mozilla/4.7 [en] (WinNT; I)
Accept:image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
image/png, */*
Accept-Encoding:gzip
Accept-Language:en
Accept-Charset:iso-8859-1,*,utf-8
```

Η κεφαλίδα Pragma: no-cache οφείλει να καταργήσει την σελίδα από την προσωρινή μνήμη εάν αυτή βρίσκεται στην κρυφή μνήμη. Με την χρήση του HTTPResponseSplittingo διακομιστής ετοιμάζει δύο απαντήσεις για ένα αίτημα.

```
GEThttp://testsite.com/redir.php?site=%0d%0aContent-
Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aLast-
Modified:%20Mon,%2027%20Oct%202009%2014:50:18%20GMT%0d%0aConte
nt-Length:%2020%0d%0aContent-
Type:%20text/html%0d%0a%0d%0a<html>deface!</html>HTTP/1.1
Host:testsite.com
User-Agent:Mozilla/4.7 [en] (WinNT; I)
Accept:image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
image/png, */*
Accept-Encoding:gzip
Accept-Language:en
Accept-Charset:iso-8859-1,*,utf-8
```

Η ώρα στην πρώτη κεφαλίδα έχει επιτηδευμένα οριστεί στις 27 Οκτώβρη και η δεύτερη κεφαλίδα που είναι η κεφαλίδα απόκρισης χρησιμοποιείται για την αποθήκευση της απόκρισης στην προσωρινή μνήμη.

Ο παρακάτω κώδικας περιγράφει το πώς αποστέλλεται το αίτημα για την σελίδα που αντικαθίσταται στην προσωρινή μνήμη του διακομιστή.

```
GEThttp://testsite.com/index.htmlHTTP/1.1
Host:testsite.com
User-Agent:Mozilla/4.7 [en] (WinNT; I)
Accept:image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
image/png, */*
Accept-Encoding:gzip
Accept-Language:en
Accept-Charset:iso-8859-1,*,utf-8
```

Ωστόσο, η εκτέλεση των αιτημάτων θα πρέπει να γίνεται κατά την διάρκεια μιας σύνδεσης όταν έχουν ικανοποιηθεί τα προηγούμενα. Πιθανόν αυτή η μορφή επίθεσης να θεωρείται προβληματική για το poisoning της προσωρινής μνήμης και έχει ως αιτία την διαφορετικότητα του μοντέλου σύνδεσης του διακομιστή cachekai των εφαρμογών που επεξεργάζονται τα αιτήματα. Ουσιαστικά, αυτή η μορφή επίθεσης θα μπορούσε να είναι πιο αποτελεσματική σε άλλους διακομιστές. Τέλος, η τεχνική αυτή αντιμετωπίζει προβλήματα σχετικά με το μήκος του URL όπου η τοποθέτηση της κεφαλίδας απόκρισης είναι πρακτικά αδύνατη ώστε να αντιστοιχιστεί το αίτημα με την σελίδα που υφίσταται poisoning (Rezos, 2009).

3.6 Evil Twin Attack

Αυτού του είδους η επίθεση αφορά την πλαστογράφηση της κυβερνοεπίθεσης και αποσκοπεί στην εξαπάτηση των χρηστών για να συνδεθούν σε ένα fakesημείο πρόσβασης Wi-Fi που προσπαθεί να μιμηθεί ένα νόμιμο δίκτυο. Από την στιγμή που

ο χρήστης συνδεθεί σε ένα δίκτυο eviltwin, οι χάκερς έχουν την δυνατότητα πρόσβασης στα πάντα. Αυτές οι επιθέσεις οφείλουν το όνομά τους στην δυνατότητα μίμησης που έχουν των νόμιμων δικτύων wi-fi με αποτέλεσμα να μην μπορεί κάποιος εύκολα να διακρίνει την διαφορά. Η επίθεση eviltwin είναι εξαιρετικά επικίνδυνη και δεν είναι εύκολα αναγνωρίσιμη. Οι χάκερς προτιμούν τοποθεσίες στις οποίες συχνάζει πολύς κόσμος όπως καφετέριες, αεροδρόμια κ.α για να πραγματοποιήσουν την επίθεσή τους. Αυτό συμβαίνει γιατί τα μέρη αυτά έχουν πολλαπλά σημεία πρόσβασης με το ίδιο όνομα και έτσι το ψεύτικο δίκτυο μπορεί να περάσει εύκολα απαρατήρητο. Εν συνεχεία, δημιουργείται ένα καινούριο hotspot κάνοντας χρήση του ίσιου SSID με αυτό του νόμιμου δικτύου. Με αυτόν τον τρόπο έχουν την δυνατότητα χρήσης οποιασδήποτε κοινής συσκευής όπως τηλέφωνα, υπολογιστές κ.α. εκτός αυτού οι χάκερς μπορούν να στήσουν και μια δέσμια σελίδα πύλης όπου απαιτείται από τον χρήστη να εισάγει έναν κωδικό πρόσβασης ή ακόμα και άλλες πληροφορίες για την σύνδεση στο δίκτυο. Έτσι οι χάκερς μπορούν να αναπαραγάγουν εύκολα αυτά τα στοιχεία εξαπατώντας τους χρήστες για να στείλουν τα στοιχεία της σύνδεσής τους. Εκτός αυτού, ένας χάκερ μπορεί να μετακινήσει την συσκευή ή και τον δρομολογητή του ακόμη πολύ πιο κοντά στα υποψήφια θύματα δημιουργώντας ισχυρότερο σήμα. (www.pandasecurity.com).

3.7 Man in the Middle

Η επίθεση maninthemiddle, αποτελεί μια κοινή παραβίαση της ασφάλειας του δικτύου. Σε αυτήν την περίπτωση, ο επιτιθέμενος προσπαθεί να εμποδίσει την επικοινωνία ανάμεσα σε δύο μέρη. Έπειτα, ένας κακόβουλος host προβαίνει στον έλεγχο της επικοινωνίας και της ροής που έχει κάνοντας ενέργειες να αποσπάσει πληροφορίες ή ακόμη και να τις αλλάξει οι οποίες στέλνονται στους αρχικούς συμμετέχοντες. Η επίθεση αυτή έχει δύο μορφές. Στην πρώτη περίπτωση αυτός που

επιτίθεται κρυφακούει και στην δεύτερη περίπτωση αλλοιώνει τα μηνύματα. Η μορφή της υποκλοπής αφορά όταν αυτός που επιτίθεται ακούει ένα σύνολο μεταδόσεων που γίνεται από διαφορετικούς hosts ακόμα και αν ο υπολογιστής του δεν αποτελεί συμβαλλόμενο μέρος της επίθεσης. Δεν είναι λίγοι εκείνοι που πιστεύουν ότι η μορφή αυτή μοιάζει με διαρροή όπου ευαίσθητα δεδομένα μπορούν με εύκολο τρόπο να αποκαλυφθούν σε άλλα μέρη χωρίς να έχουν γνώση οι χρήστες. Η αλλοίωση των μηνυμάτων έχουν την βάση τους στην ικανότητα του θύτη να υποκλέπτει προβαίνοντας στην αλλαγή των περιεχομένων που εξυπηρετούν τον σκοπό τους κάνοντας χρήση μιας fakeIP, ή αλλάζοντας την MACAddress στην προσπάθεια μίμησης άλλου host (Simson, etal., 2003).

3.8 WarDriving

Αυτή η μορφή επίθεσης χαρτογραφεί τα σημεία πρόσβασης και εντοπίζει την πιθανή εκμετάλλευση συνδέσεων στα ασύρματα δίκτυα. Για να πραγματοποιηθεί αυτό πρέπει απαιτείται ένας υπολογιστής, μια ασύρματη κάρτα τύπου Ethernet, και μια κεραία που μπορεί να τοποθετηθεί σε κάποιο αυτοκίνητο. Λόγω του ότι το ασύρματο δίκτυο επεκτείνεται και πέρα από ένα κτήριο, ο κάθε εξωτερικός χρήστης έχει την δυνατότητα εισβολής στο δίκτυο αποκτώντας δωρεάν πρόσβαση στο διαδίκτυο σε πόρους και αρχεία. Η επίθεση μπορεί να γίνει πολύ εύκολα κάνοντας χρήση μιας κεραίας κατεύθυνσης και ενός GPS χαρτογραφώντας τις τοποθεσίες από τα σημεία πρόσβασης 802.11b.

Οι εταιρείες που διαθέτουν ασύρματο LAN καλούνται να προσθέσουν δικλείδες ασφαλείας που θα διασφαλίζουν ότι έχουν πρόσβαση μόνο οι προβλεπόμενοι χρήστες. Οι διασφαλίσεις περιλαμβάνουν τη χρήση του προτύπου

κρυπτογράφησης WiredEquivalentPrivacy (WEP), IPsec ή Wi-FiProtected Access (WPA), μαζί με ένα τείχος προστασίας ή DMZ.

Ο όρος προέρχεται από μια κάπως παρόμοια προσέγγιση για την παραβίαση του τηλεφωνικού συστήματος που ονομάζεται πολεμική κλήση. Η παραβίαση ενός ιδιωτικού δικτύου μπορεί να είναι παράνομη και τουλάχιστον ένα άτομο έχει διωχθεί (techtarget.com)

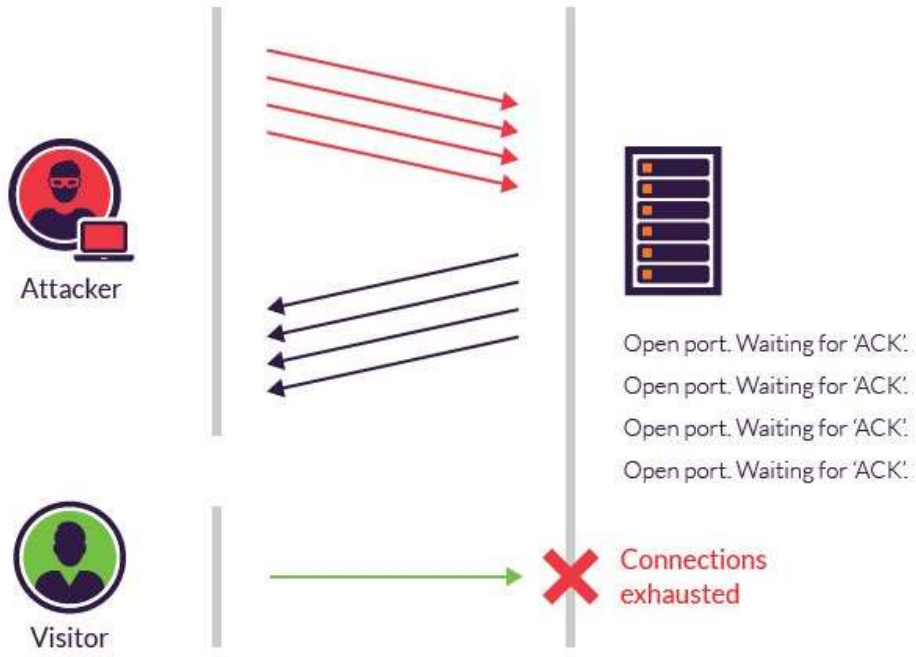
3.9 Rogue Access Points (Rogue AP)

Τα Rogue Access Points στην ουσία αποτελεί ένα «σημείο απατεώνων πρόσβασης» σε οποιοδήποτε σημείο ασύρματης πρόσβασης το οποίο έχει εγκατασταθεί στην ενσύρματη υποδομή του δικτύου δίχως την συγκατάθεση του διαχειριστή του δικτύου δίνοντας στην ουσία πρόσβαση στο ενσύρματο δίκτυο η οποία δεν είναι εξουσιοδοτημένη. Σε πολλές περιπτώσεις τα AP χαρακτηρίζονται ως αδίστακτα και τοποθετούνται από χρήστες που επιθυμούν ασύρματη πρόσβαση όταν δεν διατίθεται (techopedia.com).

3.10 TCP Syn Flood

Σε αυτήν την επίθεση ο παραβάτης αποστέλλει αιτήματα σύνδεσης TCP με ταχύ ρυθμό από αυτόν που μπορεί να επεξεργαστεί το μηχάνημα στόχος με συνέπεια τον κορεσμό του δικτύου. Στο παρακάτω σχήμα περιγράφεται η διαδικασία τα επίθεσης TCP Syn Flood. Τα βήματα της επίθεσης περιλαμβάνουν. Με την δημιουργία μιας «τριπλής χειραψίας» ανάμεσα στον πελάτη και στον διακομιστή η ανταλλαγή πληροφοριών γίνεται ως εξής: α)ο πελάτης επιθυμεί να συνδεθεί στέλνοντας ένα μήνυμα συγχρονισμού syn στον διακομιστή, στην συνέχεια β) ο διακομιστής επιβεβαιώνει ότι έλαβε το μήνυμα στον πελάτη με την αποστολή syn-acknowledgement (συγχρονισμός και επιβεβαίωση) και γ) ο πελάτης με την σειρά του

απαντά με ένα ακόμη μήνυμα acknowledgement και η σύνδεση αποκαθίσταται. Όταν πραγματοποιείται μια επίθεση πλημμύρας ο παραβάτης αποστέλλει συνεχόμενα πακέτα που επαναλαμβάνονται σε κάθε θύρα του διακομιστή στόχου κάνοντας χρήση μιας ψεύτικης διεύθυνσης IP. Ο διακομιστής που δεν γνωρίζει την επίθεση παίρνει πολλά μηνύματα τα οποία είναι νόμιμα αιτήματα για να γίνει η επικοινωνία από κάθε θύρα του. Έτσι ο παραβάτης είτε δεν αποστέλλει την αναμενόμενη επιβεβαίωση του πακέτου είτε δεν λαμβάνει ποτέ το μήνυμα εξ αρχής. Σε κάθε περίπτωση ο διακομιστής που δέχεται την επίθεση αναμένει επιβεβαίωση του πακέτου για ένα χρονικό διάστημα (imperva.com).



Εικόνα 7. Μορφή επίθεσης TCP Syn Flood

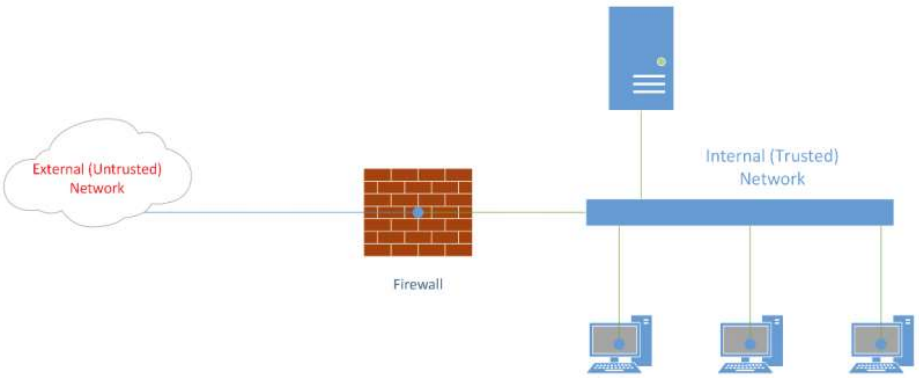
Κεφάλαιο 4. Ασφαλής Διασύνδεση

Σε αυτό το κεφάλαιο, παρουσιάζονται οι ασφαλής διασυνδέσεις που παρέχονται σε ένα δίκτυο. Συγκεκριμένα, παρουσιάζεται ο τρόπος λειτουργίας του firewall και οι μορφές του, η λειτουργία του circuitlevelgateway του packetfilretring, του VPN και της ασφάλειας που προσφέρει, του Radius και του IDS System. Ακόμη, αναλύεται ο τρόπος με τον οποίο γίνεται η ανίχνευση των εισβολών σε ένα δίκτυο καθώς και ο τρόπος που λειτουργούν τα honeypots προκειμένου να προστατέψουν ένα δίκτυο από τις δυσλειτουργίες που προκαλούν οι επιθέσεις.

4.1Firewalls

Το τείχος προστασίας προβαίνει στον διαχωρισμό δύο δικτύων διαφορετικού βαθμού εμπιστοσύνης κάνοντας ουσιαστικά έλεγχο της κίνησης των δεδομένων που ανταλλάσσουν μεταξύ τους. Το τείχος προστασίας διακρίνεται στις ακόλουθες κατηγορίες: α) έχουν ως άμεση προτεραιότητα την προστασία του κόμβου (host) από απειλές που ενδέχεται να δεχτεί από το εξωτερικό περιβάλλον κυρίως μέσω εφαρμογών λογισμικού, ή β)μέσω δικτύου, όπου το τείχος προστασίας στην ουσία χρησιμεύει για την προστασία από απειλές σε όλο το φάσμα του δικτύου οι οποίες μπορεί να προέλθουν από υπολογιστικά συστήματα που είναι ανεξάρτητα ή έχουν ήδη συμπεριληφθεί σε κάποιον εξωτερικό δρομολογητή. Ωστόσο, για να σχεδιαστεί ένα τείχος προστασίας, θα πρέπει να υπόκειται σε βασικές αρχές όπως: α) η κίνηση των δεδομένων που πραγματοποιείται σε ένα δίκτυο θα πρέπει να περνά μέσα από το τείχος προστασίας, β) η κίνηση των δεδομένων που θα περάσει από το τείχος προστασίας θα πρέπει να συνάδει σύμφωνα με την πολιτική προστασίας που το διέπει και γ) το τείχος προστασίας δεν θα πρέπει να παραβιάζεται (Μαυρίδης, 2015).

Βέβαια τα firewalls κατηγοριοποιούνται ως ακολούθως: α) φιλτράρισμα πακέτων (PacketFilters), β) πύλες κυκλώματος(CircuitLevelGateways), γ) πύλες εφαρμογών (ApplicationLevelGateways). Η λειτουργία τους θα περιγράφει αναλυτικά σε επόμενες παραγράφους.



Εικόνα 8. Firewall

Ωστόσο, είναι εφικτή η εγκατάσταση περισσοτέρων του ενός τείχους προστασίας. Για τον λόγο αυτόν, το τείχος προστασίας περιλαμβάνει περισσότερες από μια τοπολογίες. Εν συντομία, οι συνηθέστερες εξ αυτών, είναι η SingleHomedBastionHost, όπου σε αυτήν την τοπολογία είναι δυνατή η σύνδεση του εσωτερικού δικτύου με το διαδίκτυο δια μέσου του packetfiltering. Εκτός αυτού, υπάρχει ένα bastionhoststο δίκτυο όπου μέσω αυτού γίνεται η διοχέτευση της κίνησης πριν τα πακέτα φτάσουν στον προορισμό τους. Η τοπολογία αυτή παρουσιάζει ένα μειονέκτημα. Αυτό είναι ότι σε περίπτωση που ο εισβολέας καταφέρει να αποκτήσει πρόσβαση στο packetfilter, έχει την δυνατότητα να τροποποιήσει άμεσα την πολιτική του έτσι ώστε η κίνηση να μην γίνεται μέσα από το bastionhostαλλά απευθείας από τα εσωτερικά hosts. Μια άλλη τοπολογία τείχους προστασίας είναι το DualHomedBastionHost, όπου η σύνδεση του packetfilteringμε

το εσωτερικό δίκτυο επιτυγχάνεται με το bastionhost. Με αυτόν τον τρόπο δεν είναι δυνατό να παρακαμφθεί. Η επόμενη τοπολογία τείχους προστασίας είναι το dualhomedbastionhost. Σε αυτήν την τοπολογία, αν ο εισβολέας καταφέρει να έχει πρόσβαση στο packetfilterθα πρέπει να περάσει από το bastionhost. Η τελευταία τοπολογία τείχους προστασίας είναι το screenedsubnet όπου το bastionhostσυνδέεται μέσα από ένα δεύτερο packetfilterκαι όχι απευθείας με το εσωτερικό δίκτυο. Σε αυτήν την περίπτωση το εσωτερικό δίκτυο τίθεται σε πλήρη απομόνωση (Μαυρίδης, 2015).

4.2 PacketFilters

Αυτού του είδος το firewall αποτελεί και την πιο κοινή μορφή του. Σε ένα packetfilteringfirewall το κάθε πακέτο δεδομένων που εισέρχεται και εξέρχεται στο δίκτυο ελέγχεται και εξετάζεται. Ωστόσο, ο έλεγχος και η εξέταση αφορούν τις κεφαλίδες του επιπέδου δικτύου (IPHeaders) αλλά και το επίπεδο μεταφοράς (TCP/UDPHeaders) προκειμένου να ληφθούν πληροφορίες σχετικά με: το πρωτόκολλο επικοινωνίας, την διεύθυνση και την θύρα προέλευσης, την διεύθυνση και την θύρα προορισμού. Ωστόσο, τα παραπάνω, υπόκεινται σε έλεγχο από ένα σύνολο κανόνων ώστε να αποφασιστεί για το αν η διέλευση του πακέτου θα επιτραπεί ή θα απορριφθεί. Ειδικότερα, μέσα από τους κανόνες εφαρμόζεται μια λίστα ελέγχου πρόσβασης ACL –AccessControlList όπως φαίνεται στο παρακάτω σχήμα:

#	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Action	Comment
1	192.168.0.0/16	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
2	172.16.0.0/12	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
3	10.0.0.0/8	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
4	any	*	192.168.1.21	80	TCP	permit	Access to web server
5	any	*	192.168.1.31	25	TCP	permit	Access to mail server
6	any	500	192.168.1.2	500	UDP	permit	Access to isakmp
7	any	4500	192.168.1.2	4500	UDP	permit	Access to isakmp-nat
8	any	*	192.168.1.0/24	*	*	deny	Deny all

Εικόνα 9. Λίστα Ελέγχου Πρόσβασης

Από την παραπάνω λίστα ελέγχου πρόσβασης αποτυπώνεται η κίνηση των πακέτων που εισέρχεται στο δίκτυο συμπεριλαμβάνοντας οκτώ κανόνες όπου επιτρέπει την κίνηση από το δίκτυο 192.168.0.0/16 προς το δίκτυο 192.168.1.0/24, από το δίκτυο 172.16.0.0/12 προς το δίκτυο 192.168.1.0/24 και από το δίκτυο 10.0.0.0/8 προς το δίκτυο 192.168.1.0/24. Οι κανόνες που μόλις περιγράφηκαν κάνουν έλεγχο την εισερχόμενη κίνηση των πακέτων με αφετηρία το διαδίκτυο και προορισμό κάποιο εσωτερικό δίκτυο. Σύμφωνα με την λίστα ελέγχου πρόσβασης, οι κανόνες 4 έως 7 επιτρέπουν την κίνηση του πακέτου στον κόμβο 192.168.1.21 στην θύρα 80, όπου βλέπει ο webserver στον κόμβο192.168.1.31 στην θύρα 25 όπου βλέπει ο mailserver, στον κόμβο 192.168.1.2 στην θύρα 500,όπου βλέπει η υπηρεσία isakmp και απαγορεύεται στην 192.168.1.0/24 η κίνηση του δικτύου. Οι παραπάνω κανόνες αντικατοπτρίζουν την εφαρμογή του packetfiltering για την εισερχόμενη και εξερχόμενη κίνηση του δικτύου. Ωστόσο, οι κανόνες αυτοί θα πρέπει να εφαρμοστούν απαράμιλλα καθώς εντοπίζονται οι ακόλουθες δυσλειτουργίες: α) το κάθε πακέτο θα πρέπει να υποβάλλεται σε έλεγχο καθώς θα πρέπει να ικανοποιείται από κάποιον κανόνα προκειμένου να γίνουν οι μετέπειτα ενέργειες. Σε ένα δίκτυο όπου εξυπηρετεί μεγάλη κίνηση πακέτων προκαλούνται αισθητές καθυστερήσεις προκειμένου να εξυπηρετηθούν όλα, β) ο διαχειριστής του δικτύου θα πρέπει να

καθορίζει τους κανόνες για την κίνηση του δικτύου που περιλαμβάνει την εξερχόμενη αλλά και την εισερχόμενη κίνηση, γ) το packetfiltering (stateless) είναι επίφοβο σε επιθέσεις spoofing όπου τα πακέτα κατακερματίζονται σε μικρότερα, ώστε το πεδίο κεφαλίδας να περιλαμβάνεται στα υπόλοιπα τμήματα για να μην ελέγχονται από το firewall. Βέβαια, οι παραπάνω δυσλειτουργίες είναι εφικτό να διορθωθούν διατηρώντας κάθε σύνδεση σε μια κατάσταση state. Με αυτόν τον τρόπο, κάθε πακέτο είτε είναι εξερχόμενο είτε είναι εισερχόμενο φτάνοντας στο firewall είναι σε εδραιωμένη κατάσταση (established)είναι επιτρεπτή η διέλευσή του. Σε περίπτωση που το πακέτο, ξεκινά μια καινούρια σύνδεση, αυτομάτως δημιουργείται μια καινούρια εγγραφή στον πίνακα των καταστάσεων. Οι λίστες πρόσβασης διατηρούνται ορίζοντας την κίνηση των πακέτων που θα επιτραπεί. Τέλος, αν το πακέτο δεν υπόκειται σε κάποια από τις δύο παραπάνω καταστάσεις τότε απορρίπτεται (Μαυρίδης, 2015).

4.2 CircuitLevelGateways

Η βασική λειτουργία των πυλών κυκλωμάτων (circuitgateways) είναι η αποτροπή των απευθείας συνδέσεων ανάμεσα σε ένα κόμβο του προστατευμένου δικτύου και σε έναν κόμβο ενός εξωτερικού δικτύου. Στον αντίποδα του packetfilteringόπου γίνεται εδραίωση της σύνδεσης ανάμεσα στα μέρη που επικοινωνούν, στο circuitlevelgateways υλοποιούνται δυο διαφορετικές συνδέσεις ανάμεσα στους δύο κόμβους και στην πύλη του δικτύου. Στην συνέχεια η πύλη αναλαμβάνει να προωθήσει τα τμήματα που λαμβάνει από την μία σύνδεση στην άλλη. Πιο συγκεκριμένα, η διαδικασία που ακολουθείται είναι η ακόλουθη. Ένας πελάτης επιθυμεί την σύνδεση του με την πύλη. Στην συνέχεια η πύλη ελέγχει αν

είναι επιτρεπτή η σύνδεση, αν είναι τότε αυτή εδραιώνεται. Η πύλη κάνει την προώθηση των πακέτων από το ένα hostστο άλλο χωρίς αλλοιώσεις. Μόλις ολοκληρωθεί η προώθηση η σύνδεση τερματίζεται. Το πιο σύνηθες πρωτόκολλο που κάνουν χρήση οι πύλες είναι το sock. Για την υλοποίησή του ορίζεται ένας sockserver όπου η εκτέλεσή του γίνεται στο gateway, ο sockclient όπου συμπεριλαμβάνεται στην εφαρμογή πελατών κάνοντας χρήση των πρωτοκόλλων και το sockclientlibrary που γίνεται χρήση από τους διακομιστές και τίθεται υπό την προστασία του firewall (Μαυρίδης, 2015).

4.3 Ανίχνευση Εισβολών

Σκοπός της ανίχνευσης εισβολών είναι η ενδελεχής ανίχνευση τυχόν κακόβουλων ενεργειών μέσα από την ανάλυση της καταγραφής εντοπίζοντας τον εισβολέα ο οποίος έχει επιτύχει την απόκτηση της πρόσβασης στο σύστημα. Βασίζεται στην διαφορετική συμπεριφορά που θα εκδηλώσει ο επιτιθέμενος συγκριτικά με έναν χρήστη του δικτύου. Ωστόσο, η καταγραφή είναι μια διαδικασία αρκετά χρονοβόρα. Για αυτόν τον λόγο, υλοποιήθηκαν συστήματα τα οποία προβαίνουν στην ανάλυση της καταγραφής σε πραγματικό χρόνο και ονομάζονται IDS (IntrusionDetectionSystems). Τα συστήματα αυτά διακρίνονται σε κατηγορίες και περιγράφονται σε επόμενα σημεία αυτής της παραγράφου. Έτσι, η ανίχνευση των εισβολών μπορεί να διενεργείται είτε σε επίπεδο δικτύου είτε σε επίπεδο κόμβου. Συνεπώς η κατηγοριοποίηση αυτών των συστημάτων διακρίνεται σε: Α) HotBasedIDS: των οποίων η υλοποίηση γίνεται με την εγκατάσταση του λογισμικού σε κόμβο για να γίνεται έλεγχος της εισερχόμενης και εξερχόμενης κίνησης. Β) Network –BasedIDS: όπου εμπεριέχονται κόμβοι που περιλαμβάνουν διεπαφές του δικτύου οι οποίες προβαίνουν στην καταγραφή της συνολικής κίνησης του δικτύου. Οι διεπαφές αυτές συμπεριλαμβάνουν το networktap το οποίο συνδέεται με την

κατάλληλη διεπαφή του δικτύου καταγράφοντας την συνολική κίνηση του δικτύου και το detectionengine το οποίο αναλύει την καταγραφή της κίνησης. Παρόλαυτα, τα συστήματα αυτά έχουν τα μειονεκτήματά τους και τα πλεονεκτήματά τους. Στα Networkbased συστήματα, ο αριθμός των σημείων του δικτύου που επιλέγεται για έλεγχο είναι σχετικά μικρός. Ωστόσο, τα κρυπτογραφημένα δεδομένα δεν είναι εύκολο να αναλυθούν. Επίσης, δεν εντοπίζεται η εμπλοκή του στην κίνηση των πακέτων. Ουσιαστικά πρόκειται για συσκευές που δεν είναι εύκολο να παραβιαστούν. Δυσλειτουργίες στην ανίχνευση μπορεί να προκληθεί από τον μεγάλο όγκο των δεδομένων. Στα HostBased συστήματα η κρυπτογραφημένη επικοινωνία είναι εφικτή αλλά απαιτείται η εγκατάσταση ενός λογισμικού επιπρόσθετα κάτι που συνεπάγεται και περισσότερους πόρους αλλά και μεγαλύτερο φόρτο εργασίας. Βέβαια η χρήση εξειδικευμένου υλικού δεν απαιτείται καθώς υπάρχει πρόσβαση σε καταγραφή του συστήματος για πιο ακριβής αναλύσεις. Τέλος, η εγκατάστασή τους δεν απαιτεί ειδικές συσκευές ή συστήματα που δεν είναι συμβατά (Μαυρίδης, 2015).

Ωστόσο, τα IDS διακρίνονται σε διάφορους τύπους και μορφές καθώς δεν υπάρχει συγκεκριμένο μοτίβο για την επιλογή τους από το δίκτυο αφού κάθε ένα από αυτά έχει τις δικές του απαιτήσεις. Αν βέβαια, υπάρχουν περιπτώσεις δικτύων που απαιτούν όλες τις περιπτώσεις τότε τα υβριδικά συστήματα είναι η κατάλληλη επιλογή αφού συνδυάζουν όλα τα παραπάνω (Μαυρίδης, 2015).

Ακόμη, στην ανίχνευση εισβολών συγκαταλέγεται και η ανίχνευση των υπογραφών όπου γίνεται έλεγχος της κίνησης του δικτύου η οποία υπόκειται σε ένα σύνολο κανόνων και εντοπίζεται η μη επιθυμητή κατάσταση. Παραδείγματα τέτοιων κανόνων αποτελεί και ο κανόνας ότι « *ο χρήστης δεν θα πρέπει να προβαίνει στην τοποθέτηση αρχείων στο homedirectory άλλου χρήστη*». Έτσι , αν κάτι τέτοιο συμβεί η συμπεριφορά αυτή θα θεωρηθεί ως ύποπτη και αυτομάτως θα ενημερωθεί και ο

διαχειριστής του δικτύου. Τέλος, η ανίχνευση των υπογραφών μπορεί να αναφέρεται και σε περιπτώσεις όπου εντοπίζονται πακέτα με την ίδια διεύθυνση προέλευσης και προορισμού. Αυτή η μορφή επίθεσης αναφέρεται και ως LandAttack (Μαυρίδης, 2015).

Πέρα από την ανίχνευση υπογραφών, μια άλλη συνηθισμένη μορφή ανίχνευσης εισβολών είναι και η ανίχνευση συμπεριφοράς. Σε αυτήν την περίπτωση, γίνεται εντοπισμός των συμπεριφορών που δεν συνάδουν με την φυσιολογική χρήση του συστήματος. Ως φυσιολογική χρήση ορίζεται εκείνη που γνωρίζει το IDS όσο βρίσκεται σε λειτουργία. Συνεπώς, μια τυχόν παρατηρούμενη απόκλιση παρέκκλιση στο σύστημα θεωρείται ως επίθεση. Η συγκεκριμένη μορφή έχει καλύτερο πεδίο δράσης σε στατικά περιβάλλοντα παρά σε δυναμικά(Μαυρίδης, 2015).

Τέλος, η ανίχνευση εισβολών σε ένα δίκτυο μπορεί να προβλεφθεί και συστήματα ανίχνευσης δεύτερης γενιάς, τα οποία ανιχνεύουν τις εισβολές ενημερώνοντας τον διαχειριστή του δικτύου για να κάνει όλα τα απαραίτητα βήματα ώστε να τις αποκλείσει. Η διαδικασία αυτή πολλές φορές απαιτεί χρόνο με συνέπεια να εντοπιστούν δυσλειτουργίες που έχει προκαλέσει ήδη η εισβολή(Μαυρίδης, 2015).

4.5 Honeypots

Προκειμένου να αποφευχθούν οι δυσλειτουργίες που προκύπτουν από τις επιθέσεις, υλοποιείται ένας κόμβος στο δίκτυο ο οποίος ονομάζεται honeypot. Στο honeypot συμπεριλαμβάνονται ευπάθειες με απώτερο σκοπό να ξεγελαστεί ο εισβολέας και να μην επιτεθεί σε εκείνο αλλά να ασχοληθεί με τα υπόλοιπα συστήματα στοχεύοντας στην ανίχνευση, στην μελέτη, στον εντοπισμό της επίθεσης καθώς και στον περιορισμό της ζημιάς που μπορεί να προκαλέσει (Μαυρίδης, 2015).

4.6 VPN και ασφάλεια

Ένα VPN (Virtual Private Network) αποτελεί ένα εικονικό δίκτυο μέσω του οποίου μπορεί κανείς να συνδεθεί στο διαδίκτυο με ασφάλεια. Τα εικονικά δίκτυα προσφέρουν ένα επίπεδο ασφάλειας που διασφαλίζει το απόρρητο και την ανωνυμία όπου οι χρήστες μπορούν να: α) αποκρύψουν την δραστηριότητά τους στο διαδίκτυο αποφεύγοντας την παρακολούθηση, β) αντιμετωπίσουν την λογοκρισία και να περιηγηθούν χωρίς περιορισμούς στο διαδίκτυο (Andreas, 2022).

Κάνοντας χρήση ενός VPN , οι χρήστες μπορούν να αποκρύψουν την αληθινή τους IP κρυπτογραφώντας την σύνδεσή τους στο διαδίκτυο. Αυτό μπορεί να γίνει με την απόκρυψη του ιστορικού περιήγησης σε ιδιωτικό, αφού το VPN έχει αυτήν την δυνατότητα με τον πάροχο υπηρεσιών να μπορεί να δει μόνο την δραστηριότητα του χρήστη η οποία είναι κρυπτογραφημένη, με την αλλαγή της διαδικτυακής παρουσίας των χρηστών αφού τους δίνεται η δυνατότητα μέσω του VPN να συνδεθούν σε ένα διακομιστή άλλης χώρας και να αποκτήσουν πρόσβαση σε τοπικό περιεχόμενο (Andreas, 2022).

4.7 Radius

Το Radius είναι ένα πρωτόκολλο του δικτύου το οποίο προσφέρει κεντρική διαχείριση ταυτότητας και εξουσιοδότησης στους χρήστες που κάνουν χρήση μιας υπηρεσίας δικτύου. Στην ουσία είναι ένα πρωτόκολλο πελάτη/διακομιστή που τελείται σε επίπεδο εφαρμογής κάνοντας χρήση του TCP ή του UDP. Το Radius είναι επί της ουσίας το back end της επιλογής για να ελεγχθεί η ταυτότητα του 802.1χ. εκτός αυτού αποτελεί και μια παρασκηνιακή διαδικασία που εκτελείται σε windows ή

unix. Στο παρακάτω σχήμα αποτυπώνεται η ροή ελέγχου ταυτότητας και εξουσιοδότησης Radius.

Εικόνα 10. Ροή Ελέγχου ταυτότητας και εξουσιοδότησης Radius

Από το σχήμα προκύπτει ότι ο διακομιστής Radius επιστρέφει τρεις απαντήσεις που περιλαμβάνουν: α) την απόρριψη πρόσβασης β) την πρόκληση πρόσβασης, και γ) την πρόσβαση αποδοχής (Cisco, 2006).

4.8 IDS Systems

Το IDS systems θεωρείται ένα σύστημα που ανιχνεύει τις εισβολές. Στην πράξη είναι μια συσκευή λογισμικού που παρακολουθεί το δίκτυο από κακόβουλες δραστηριότητες. Τέτοιες δραστηριότητες συλλέγονται συγκεντρωτικά σε ένα σύστημα διαχείρισης πληροφοριών (SIEM). Το σύστημα αυτό συνδυάζει εξόδους από διάφορες πηγές κάνοντας χρήση τεχνικών συναγερμών για να μπορεί να διακρίνει αυτές τις δραστηριότητες από ψεύτικα alarm. Το εύρος αυτών των συστημάτων ποικίλλει από μικρούς υπολογιστές ως μεγάλα δίκτυα. Μια κοινή

κατηγοριοποίηση μπορεί να είναι σε συστήματα ανίχνευσης εισβολής δικτύου (NIDS) και συστήματα εισβολής με βάση κεντρικούς υπολογιστές (HIDS) (Martinelli, et al.2017).

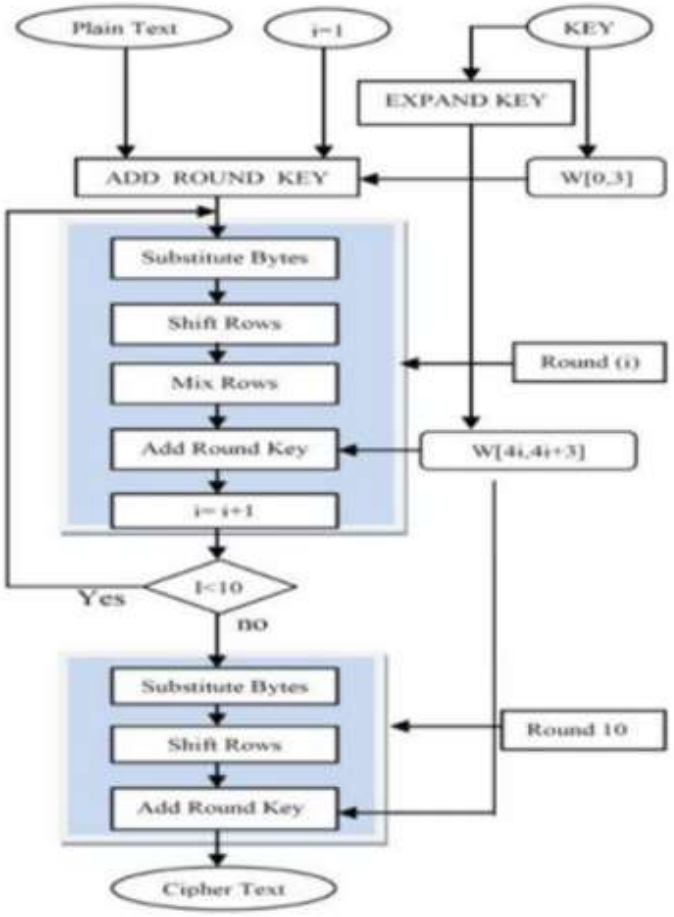
Κεφάλαιο 5. Κρυπτογραφικοί Αλγόριθμοι

Σε αυτό το κεφάλαιο, περιγράφονται οι αλγόριθμοι που χρησιμοποιούνται στην διαδικασία της κρυπτογράφησης. Πιο συγκεκριμένα, παρουσιάζονται οι αλγόριθμοι κρυπτογράφησης AES, DESκαι 3DES. Εκτός των αλγορίθμων κρυπτογράφησης περιγράφεται σχολαστικά η διαδικασία της κρυπτογράφησης καθώς επίσης και οι μετασχηματισμοί της οι οποίοι περιλαμβάνουν τα subbytes, το addroundkey και το RSA. Τέλος, παρουσιάζονται εκτενώς και τα ασύμμετρα κρυπτοσυστήματα.

5.1 Κρυπτογραφικός Αλγόριθμος AES

Ο αλγόριθμος AES (AdvanceEncryptionStandard), αποτελεί ένα συμμετρικό μπλοκ κλειδιών το οποίο είναι κρυπτογραφημένο και αναπτύχθηκε από τους Daemen και Vincent το 1998 (Ritu,et.al., 2013). Ο συγκεκριμένος αλγόριθμος έχει την δυνατότητα υποστήριξης συνδυασμούς δεδομένων 128 bit και μήκη κλειδιών 128, 192, και 256 bit. Για τον λόγο αυτόν ορίζεται και ως αλγόριθμος AES 128, AES, 192, AES 256 bit. Κατά την κρυπτογράφηση και αποκρυπτογράφηση ο αλγόριθμος AES κάνει διάφορους γύρους περίπου 10 όταν αφορά τα 128 κλειδιά και τα 192 κλειδιά

και περισσότερους γύρους γύρω στους 14 όταν αφορά τα 256 κλειδιά ώστε να προβεί στην παράδοση του τελικού κειμένου της κρυπτογράφησης ή ακόμη και για να προβεί στην ανάκτηση ενός απλού κειμένου επιτρέποντας ένα μήκος δεδομένων στα 128 το οποίο έπειτα μπορεί να διακριθεί σε βασικά και λειτουργικά μπλοκ των τεσσάρων. Τα μπλοκ που δημιουργούνται θεωρούνται πίνακας byte και η οργάνωσή τους ορίζεται ως 4 επί 4 ο οποίος ονομάζεται κατάσταση. Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης ξεκινά με την εισαγωγή του RoundKey (Shraddha, 2016). Βέβαια, πριν την έλευση του τελικού γύρου απομένουν εννέα ακόμη. Στην διάρκεια του κάθε γύρου δημιουργούνται οι ακόλουθοι μετασχηματισμοί: Subbytes, Shift σειρές, Mix-στήλες. Ωστόσο, στον τελευταίο γύρο δεν πραγματοποιείται κάποιος μετασχηματισμός. Η διαδικασία της αποκρυπτογράφησης λειτουργεί εντελώς αντίστροφα. Η αποκρυπτογράφηση χρησιμοποιεί τις ακόλουθες συναρτήσεις InverseSubstituteBytes, InverseShiftRows και InverseMixColumns. Κάθε γύρο που πραγματοποιεί ο αλγόριθμος AESυπόκειται στον ακόλουθο μετασχηματισμό (Akash, et. al., 2012). Ο μετασχηματισμός αυτός ονομάζεται μετασχηματισμός υποκατάστατου byte που συμπεριλαμβάνει ένα μπλοκ από δεδομένα μήκους 128 bit γεγονός που σηματοδοτεί ότι σε κάθε μπλοκ περιέχονται 16 byte. Ακόμη στον μετασχηματισμό των υπό bytekάθε ένα από αυτά περιλαμβάνει 8 bit σε ένα μπλοκ δεδομένων το οποίο μετατρέπεται σε άλλο μπλοκ κάνοντας χρήση ενός πλαισίου αντικατάστασης 8 bit γνωστό και ως RijndaelSbox (Ritu, et.al., 2013).



Εικόνα 11. AES Advanced Encryption Standard process

5.1.1 Κρυπτογραφικός Αλγόριθμος DES και 3DES

Το DES (DataEncryptionStandard) αποτελείτο πιο γνωστό κρυπτογραφικό σύστημα το οποία αναπτύχθηκε από την δεκαετία του 1970. Με το πέρασμα του χρόνου το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας υιοθέτησε τον αλγόριθμο και τον υπέβαλε στο Εθνικό Γραφείο Προτύπων ώστε να τον προτείνει για την προστασία κυβερνητικών δεδομένων τα οποία είναι ευαίσθητα και μη ταξινομημένα. Σε αυτόν τον αλγόριθμο το μήκος του κλειδιού είναι 56 bit και το μέγεθος του μπλοκ καθορίζεται στα 64 bit. Ωστόσο, θεωρείται ευαίσθητο στις επιθέσεις όταν γίνεται χρήση ενός αδύναμου κλειδιού. Στην αρχή το κλειδί ήταν 64 Bit αλλά αργότερα τέθηκε από την NSA περιορισμός του κλειδιού σε μήκος 56 bit. Με άλλα λόγια ο

αλγόριθμος κάνει χρήση τα bittου κλειδιού των 64 bit χρησιμοποιώντας το συμπιεσμένο κλειδί 56 bit προερχόμενο από 64 bit κλειδί που έχει κρυπτογραφηθεί σε 64 bitμπλοκ. Ωστόσο, είναι ευέλικτο καθώς χρησιμοποιείται με αρκετούς τρόπους όπως: CBC, ECB, CFB και OFB. Ωστόσο, το DES θεωρείται ασφαλές με την μορφή TripleDES (Karthik, et.al., 2014; Stallings, 2011).

Έτσι, ο αλγόριθμος 3DES, ουσιαστικά είναι ένας αλγόριθμος που προσφέρει τριπλή κρυπτογράφηση κάνοντας χρήση ενός συμμετρικού κλειδιού εφαρμόζοντας τον αλγόριθμο σε ένα μπλοκ δεδομένων τρεις φορές παρέχοντας έτσι μια πιο ασφαλή κρυπτογράφηση πληροφοριών έχοντας ως αποτέλεσμα την ευρεία χρήση του από προμηθευτές και χρήστες (Cisco, 2006).

5.2 Διαδικασία Κρυπτογράφησης

Σκοπός της κρυπτογράφησης των δεδομένων είναι: α) η εμπιστευτικότητα όπου η πρόσβαση στις πληροφορίες που πρόκειται να μεταδοθούν αφορούν μόνο εξουσιοδοτημένους χρήστες, β) ακεραιότητα όπου οι πληροφορίες που πρόκειται να μεταδοθούν να υπόκεινται σε αλλοίωση μόνο από τους εξουσιοδοτημένους χρήστες καθώς επίσης να υπάρχει η δυνατότητα ανίχνευσης της αλλοίωσης, γ) μη απάρνηση όπου σε αυτήν την περίπτωση και ο παραλήπτης αλλά και ο αποστολέας δεν δύναται να απαρνηθεί την γνησιότητα της πληροφορίας και δ) η πιστοποίηση όπου σε αυτήν και ο παραλήπτης και ο αποστολέας έχουν την δυνατότητα να προβούν στην εξακρίβωση των στοιχείων τους καθώς επίσης να διαπιστώσουν από πού προέρχεται και για πού προορίζεται μια πληροφορία με την προϋπόθεση ότι τα στοιχεία τους είναι γνήσια και αληθή. Ως διαδικασία η κρυπτογράφηση μετασχηματίζει ένα μήνυμα σε μορφή που δεν είναι εύκολα κατανοητή κάνοντας χρήση ενός αλγορίθμου

κρυπτογράφησης το οποίο θα μπορεί να διαβαστεί αποκλειστικά και μόνο από τον παραλήπτη του (Αντωνίου, 2011).

Η κρυπτογράφηση είναι μια διαδικασία η οποία διασφαλίζει την προστασία των δεδομένων κατά την διάρκεια της επικοινωνίας. Ένα σύστημα προκειμένου να μεταφέρει με ασφάλεια δεδομένα θα πρέπει να εξασφαλίσει λειτουργίες όπως η μυστικότητα και η ιδιωτικότητα. Ωστόσο, η μη εξουσιοδοτημένη πρόσβαση δεν μπορεί να αποτραπεί εντελώς στα μέσα μετάδοσης (Αραμπατζής, 2019).

Πιο συγκεκριμένα, στην κρυπτογράφηση (encryption), η αρχική πληροφορία μετατρέπεται από τον αποστολέα σε μια διαφορετική μορφή κάνοντας μετάδοση του μηνύματος που προκύπτει μέσα από το δίκτυο. Έτσι, ο αποστολέας του μηνύματος κάνει χρήση ενός αλγορίθμου κρυπτογράφησης και ενός κλειδιού προκειμένου να μετατρέψει ένα απλό κείμενο σε κρυπτοκείμενο. Με άλλα λόγια επιδιώκεται η μετατροπή του αρχικού κειμένου σε κρυπτοκείμενο. Το απλό κείμενο αφορά δεδομένα τα οποία δύνανται να προστατευθούν όταν πραγματοποιείται η μετάδοση, το κρυπτοκείμενο αφορά το κωδικοποιημένο κείμενο το οποίο προκύπτει από τον αλγόριθμο κρυπτογράφησης και χρησιμοποιεί ένα κλειδί και ο αλγόριθμος κρυπτογράφησης όπου η εισαγωγή ενός κειμένου και ενός κλειδιού κρυπτογράφησης έχει ως αποτέλεσμα ένα κρυπτογραφημένο κείμενο. Στην διαδικασία της κρυπτογράφησης σημαντικό ρόλο ενέχουν τα κλειδιά της κρυπτογράφησης τα οποία αποτελούν μια τυχαία σειρά δυαδικών ψηφίων και υλοποιούνται αποκλειστικά για αυτό τον σκοπό. Ωστόσο κάθε ένα από τα κλειδιά είναι μοναδικά και η δημιουργία τους προκύπτει μέσω αλγορίθμου για να διασφαλιστεί η μη προβλεψιμότητά του. Βέβαια, η κρυπτογράφηση συμμετρικού κλειδιού (symmetrickey) σχετίζεται με αλγόριθμο που κάνει χρήση του ίδιου μυστικού κλειδιού και στην αποκρυπτογράφηση και στην κρυπτογράφηση. Ενώ η κρυπτογράφηση ενός

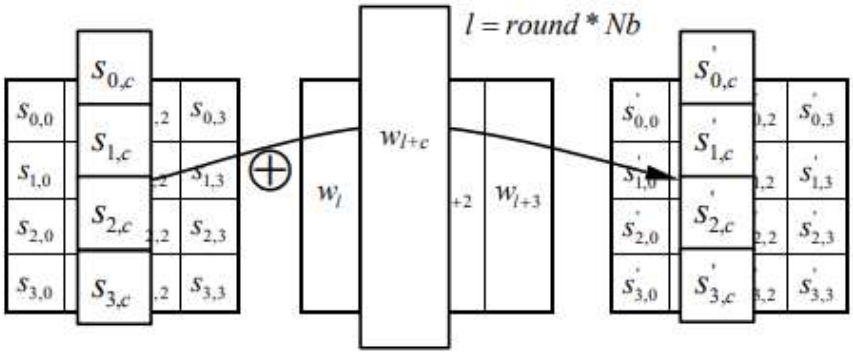
ασύμμετρου (asymmetrickey) ή αλλιώς οριζόμενου δημοσίου κλειδιού σχετίζεται με αλγόριθμο που κάνει χρήση κλειδιού με μοναδικό σκοπό την κρυπτογράφηση. Να σημειωθεί ότι το δημόσιο κλειδί μπορεί να διατεθεί στον οποιονδήποτε ενώ το ιδιωτικό κλειδί θα διατεθεί μόνο στον αποδέκτη του μηνύματος. Ωστόσο, η κρυπτογράφηση σαν διαδικασία κάνει χρήση ενός πρωτότυπου μηνύματος που όπως προαναφέρθηκε είναι ένα απλό κείμενο και με την χρήση ενός κλειδιού μετατρέπεται σε μια μορφή που δεν είναι εύκολα κατανοητή. Ακόμη, η κρυπτογράφηση υλοποιείται αποκλειστικά και μόνο από την πλευρά του αποστολέα κατευθείαν από την πηγή όταν γίνεται η αποστολή δεδομένων από το μηχάνημα (Αραμπατζής, 2019).

Βέβαια, η διαδικασία της κρυπτογράφησης ενέχει και κάποια μειονεκτήματα όπως: α) δεν είναι δυνατή η αποτροπή διαγραφής πληροφοριών από κάποιον εισβολέα, β) το μήνυμα προς μετάδοση είναι δυνατό να μεταβληθεί και να κάνει χρήση διαφορετικού κλειδιού από το ήδη καθορισμένο ή σε κάποιες περιπτώσεις να γίνει καταγραφή όλων των κλειδιών που πρόκειται να χρησιμοποιηθούν στο μέλλον, γ) είναι δυνατό να βρεθεί ένας τρόπος πιο εύκολος χωρίς να είναι απαραίτητα γνωστός στο ευρύ κοινό για την αποκρυπτογράφηση, και δ) ένα αρχείο είναι εφικτό να προσπελαστεί τόσο πριν όσο και μετά από την διαδικασία της κρυπτογράφησης (Αντωνίου, 2011).

Τέλος, η διαδικασία της κρυπτογράφησης χρησιμοποιείται ευρέως σε πολλές εφαρμογές όπως: στα δίκτυα καταστημάτων και στα ATM τους, σε εφαρμογές της σταθερής και κινητής τηλεφωνίας, σε δορυφορικές εφαρμογές και ασύρματα δίκτυα, σε εφαρμογές μέσω του διαδικτύου που σχετίζονται με ηλεκτρονικές δημοπρασίες και ηλεκτρονική ψηφοφορία καθώς επίσης σε στρατιωτικά και διπλωματικά δίκτυα (Αντωνίου, 2011).

5.3 AddRoundKey

Ο μετασχηματισμός στην κρυπτογράφηση και στην αντίστροφη κρυπτογράφηση γίνεται με το addroundkey. Βέβαια το μήκος του κλειδιού έχει μέγεθος ίσο με την κατάστασή του. Για παράδειγμα αν οι λέξεις δηλαδή Nb=4 τότε το μήκος του είναι ίσο με 128bits.Η λειτουργία του ορίζεται ως λειτουργία στηλών μεταξύ των 4 byte μιας στήλης κατάστασης και μιας λέξης του στρογγυλού κλειδιού. Αυτός ο μετασχηματισμός είναι όσο το δυνατόν πιο απλός που βοηθά στην απόδοση, αλλά επηρεάζει επίσης κάθε κομμάτι της εν λόγω κατάστασης. Στον μετασχηματισμό AddRoundKey (), ένα στρογγυλό κλειδί προστίθεται στην κατάσταση με ένα απλό bitwise στην λειτουργία XOR. Κάθε στρογγυλό κλειδί αποτελείται από λέξεις Nb από το χρονοδιάγραμμα κλειδιών αυτές οι λέξεις Nb προστίθενται η καθεμία στις στήλες της κατάστασης, έτσι ώστε όπου [wi] είναι οι βασικές λέξεις χρονοδιαγράμματος και ο γύρος είναι μια τιμή στο εύρος 0 £ γύρος £ Αρ. Στο Cipher, η αρχική προσθήκη RoundKey εμφανίζεται όταν στρογγυλεύει = 0, πριν την πρώτη εφαρμογή της στρογγυλής συνάρτησης. Η εφαρμογή του AddRoundKey ()ο μετασχηματισμός στους γύρους Nr του Cipher συμβαίνει όταν 1 £ γύρο £ Nr.. Η δράση αυτού του μετασχηματισμού όπου l = στρογγυλό * Nb. Το byte διεύθυνση εντός των λέξεων του βασικού χρονοδιαγράμματος (FIPS, 2001).



Εικόνα 12. AddRoundKey ()

5.4 SubBytes

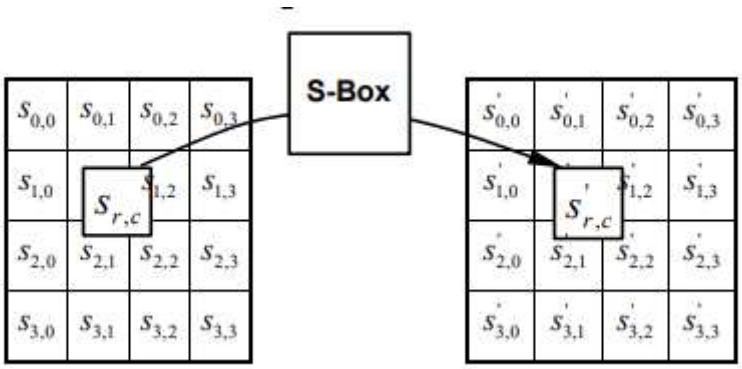
Ο μετασχηματισμός SubBytes () είναι μια μη γραμμική υποκατάσταση byte που λειτουργεί ανεξάρτητα σε κάθε byte της κατάστασης χρησιμοποιώντας έναν πίνακα αντικατάστασης (S-box). Ο πίνακας αντικατάστασης το S-boxo οποίος είναιαναστρέψιμος, κατασκευάζεται συνθέτοντας δύο μετασχηματισμούς: α) παίρνοντας τον πολλαπλασιαστικό αντίστροφο στο πεπερασμένο πεδίο gfto στοιχείο {00} αντιστοιχεί στον εαυτό του, β) εφαρμογή του ακόλουθου μετασχηματισμού πάνω από gf:

$$b_i^{'} = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

Βέβαια, το συσχετικό στοιχείο του μετασχηματισμού του S –box σε μορφή μήτρας δύναται να γίνει σύμφωνα με τα παρακάτω σχήματα(FIPS, 2001).:

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

Εικόνα 13. Η επίδραση των Subbytes στον μετασχηματισμό της κατάστασης



Εικόνα 14. Sub bytes και S-box

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Εικόνα 15. Ο μετασχηματισμός των Subbytes στο s-box

5.5 ElectronicCodebook

Το ECB (ElectronicCodeBook), αποτελεί έναν από τους τρόπους λειτουργίας για ένα μπλοκ κρυπτογράφησης. Βασικό χαρακτηριστικό του μπλοκ είναι ότι κάθε του κείμενο περιέχει μια τιμή η οποία είναι καθορισμένη στην κρυπτογράφησή του και το αντίθετο. Εν ολίγοις, η τιμή του κειμένου θα είναι η ίδια και στο κρυπτογραφημένο κείμενο. Η χρήση του έγκειται στο γεγονός ότι το κείμενο μπορεί να χωριστεί σε αρκετά τμήματα τα οποία κρυπτογραφούνται ανεξαρτήτως από άλλα μπλοκ δεδομένων. Πρακτικά, το ECB μπορεί να παρέχει την υποστήριξη ενός κλειδιού κρυπτογράφησης για κάθε έναν τύπο μπλοκ. Βέβαια, το ECB δεν ενδείκνυται για μπλοκ τα οποία είναι μικρού μεγέθους και ακολουθούν τους δικούς τους τρόπους κρυπτογράφησης. Αυτό συμβαίνει διότι πολλές από τις λέξεις και τις φράσεις χρησιμοποιούνται συνέχεια με αποτέλεσμα να εντοπιστούν τμήματα στο

κρυπτογραφημένο κείμενο τα οποία επαναλαμβάνονται βάζοντας έτσι την βάση για επιθέσεις στα βιβλία κωδικών όπου τα απλά κείμενα είναι όντως εμφανή. Από πλευράς ασφάλειας, ενδέχεται να υπάρξει κάποια βελτίωση αν εισαχθούν στα μπλοκ bitpad. Βέβαια τα μπλοκ που έχουν μέγεθος 64 bit θα πρέπει να περιλαμβάνουν χαρακτηριστικά τα οποία θα αποτρέπουν τις επιθέσεις. Τέλος, αν παρατηρηθούν σφάλματα σε ένα μπλοκ η διόρθωσή τους επηρεάζει αποκλειστικά και μόνο την αποκρυπτογράφησή (TTC, 2005).

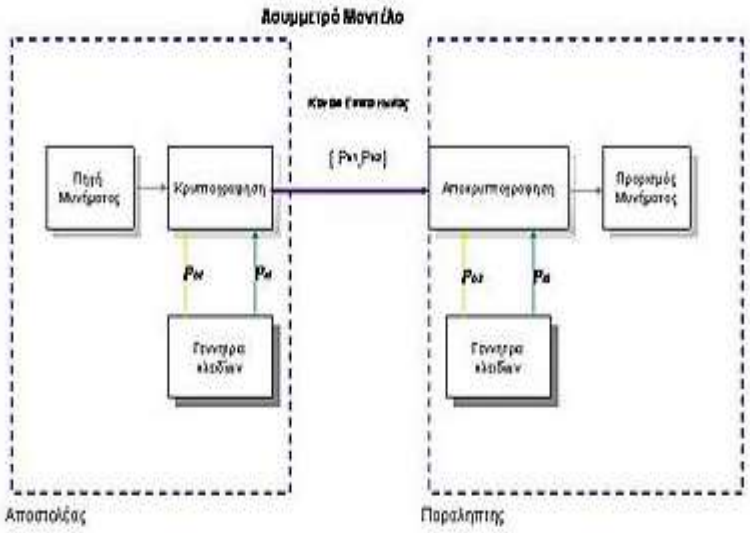
5.6 Ασύμμετρα Κρυπτοσυστήματα

Τα ασύμμετρα κρυπτοσυσήματα ουσιαστικά καλούνται και ως κρυπτοσύστηματα δημοσίου κλειδιού. Η υλοποίησή τους έγκειται στο γεγονός ότι έχουν την δυνατότητα να καλύψουν τις δυσλειτουργίες που προέκυψαν από τα συμμετρικά συστήματα και αφορούν στην μεταφορά των κλειδιών. Κύριο χαρακτηριστικό που διέπει αυτά τα συστήματα είναι ότι διαθέτουν δύο είδη κλειδιών. Ένα κλειδί που είναι δημόσιο και ένα κλειδί το οποίο είναι ιδιωτικό. Το δημόσιο κλειδί μπορεί να διατεθεί σε όλους, κάτι που δεν συμβαίνει με το ιδιωτικό κλειδί το οποίο είναι μυστικό. Τα δύο κλειδιά συνδέονται μεταξύ τους και η λειτουργία τους έγκειται στο γεγονός ότι το ένα κλειδί κάνει κρυπτογράφηση και το άλλο κλειδί κάνει αποκρυπτογράφηση.

Τα ασύμμετρα κρυπτοσυστήματα παρέχουν μια πολύ μεγάλη δυνατότητα η οποία είναι η δημιουργία των ψηφιακών υπογραφών και των ψηφιακών πιστοποιητικών. Για να γίνει περισσότερο κατανοητή η λειτουργία ενός ασύμμετρου κρυπτοσυσήματος παρατίθεται το παρακάτω παράδειγμα:

Από τον αποστολέα παράγονται δύο κλειδιά. Ο παραλήπτης επίσης παράγει δύο κλειδιά. Τόσο ο αποστολέας όσο και ο παραλήπτης προβαίνουν στην ανταλλαγή των

δημόσιων ζευγών. Στην συνέχεια, ο αποστολέας προβαίνει στην δημιουργία μηνύματος κρυπτογραφώντας το με το κλειδί του παραλήπτη και του αποστέλλει το κρυπτογραφημένο μήνυμα. Τέλος, ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το κλειδί του και λαμβάνει το παραγόμενο μήνυμα (Κάτος, 2003).

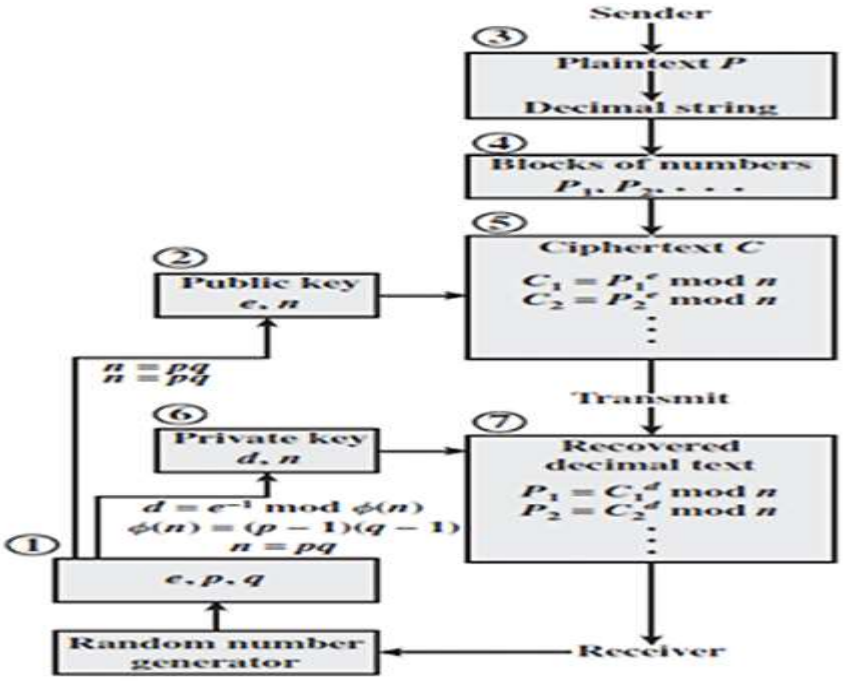


Εικόνα 16. Μοντέλο Ασύμμετρου Κρυπτοσυστήματος

5.7 RSA

Το RSA είναι στην ουσία ένα δημόσιο κλειδί κρυπτοσυστήματος. Πρόκειται για έναν ασύμμετρο κρυπτογραφικό αλγόριθμο και αποτελεί ένα από τα πιο διάσημα κρυπτοσυστήματα δημοσίων κλειδιών που χρησιμοποιούνται για ψηφιακές υπογραφές και για κρυπτογράφηση δεδομένων. Κάνει χρήση ενός μπλοκ χαρτογράφησης το οποίο περιλαμβάνει ένα μπλοκ με μεταβλητό μέγεθος στο κλειδί. Ακόμη, είναι ένα ασύμμετρο κρυπτοσύστημα το όποιο έχει την βάση του στην θεωρία των αριθμών κάνοντας χρήση των δύο πρώτων αριθμών ώστε να

δημιουργηθούν τόσο δημόσια όσο και ιδιωτικά κλειδιά. Το μέγεθός τους κυμαίνεται από 1024 έως 4096 bit. Έτσι τα δύο αυτά κλειδιά χρησιμοποιούνται για την διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης. Έτσι, ο αποστολέας προβαίνει στην κρυπτογράφηση του μηνύματος κάνοντας χρήση του δημοσίου κλειδιού του παραλήπτη όταν αυτό παραδίδεται σε αυτόν με αποτέλεσμα ο παραλήπτης να έχει την δυνατότητα αποκρυπτογράφησης κάνοντας χρήση του δικού του ιδιωτικού κλειδιού (Aman, et. al., 2012; Xin, et. al., 2011).. Βέβαια οι λειτουργίες αυτού του συστήματος δύναται να αποσυντεθούν σε τρεις φάσεις. Α) με την δημιουργία κλειδιών, β) με την κρυπτογράφηση και γ) με την αποκρυπτογράφηση. Βέβαια εντοπίζονται μειονεκτήματα κατά την δημιουργία του και για αυτό τον λόγο δεν προτιμάται για εμπορικούς σκοπούς. Η επιλογή μικρών τιμών για τον σχεδιασμό του κλειδιού θεωρείται σε γενικές γραμμές ισχνή καθώς ο οποιοσδήποτε μπορεί να προβεί στην αποκρυπτογράφηση των δεδομένων κάνοντας χρήση της θεωρίας αλλά και των πιθανοτήτων των επιθέσεων των πλευρικών καναλιών. Αντιθέτως η επιλογή μεγάλων τιμών για τον σχεδιασμό κλειδιών δίνει μεγαλύτερη απόδοση αλλά καταναλώνεται περισσότερος χρόνος (Preetha, et.al., 2013).



Εικόνα 17. Λειτουργία RSA

5.8 WEP

Το WEP (Wired Equivelant Privacy) αποτελεί έναν αλγόριθμο ασφαλείας για τα ασύρματα δίκτυα IEEE802.11. Σκοπός της εισαγωγής του ήταν να προσφέρει εμπιστευτικότητα δεδομένων ισότιμη με αυτή των παραδοσιακών ενσύρματων δικτύων. Στο wep υπάρχουν δύο γνωστές παραλλαγές: α) το πρότυπο WEP των 64bit το οποίο κάνει χρήση ενός κλειδιού 40 bit και δίνεται ως δέκα δεκαεξαδικά ψηφία (0-9 και a-f) το οποίο αναπαρίσταται με 4 bit. Στα παραπάνω ενσωματώνεται και το διάνυσμα αρχικοποίησης που έχει μήκος 24 bit αλλά και του αλγόριθμου κρυπτογράφησης RC4 για την παραγωγή ενός πλήρους κλειδιού 64 bit β) και το πρότυπο WEP των 128 bit το οποίο κάνει χρήση ενός κλειδιού 104bit. Χρησιμοποιείται συνήθως ως 26 δεκαεξαδικά ψηφία (0-9 και a-f). Σε αυτά προσμετράται το διάνυσμα αρχικοποίησης με μήκος 24 bit του αλγορίθμου

κρυπτογράφησης για την παραγωγή του πλήρους κλειδιού των 128 bit. Κύριος στόχος του WEP ήταν η αποτροπή των επιθέσεων τύπου Man in the Middle κάτι που όντως πραγματοποιούνταν. Βέβαια, υπήρξαν κάποιες αναθεωρήσεις στο πρωτόκολλο καθώς το μέγεθος του κλειδιού αυξανόταν αφού εντοπίστηκαν ελαττώματα ασφαλείας στο συγκεκριμένο πρότυπο. Με την αύξηση της υπολογιστικής ισχύος τυχόν εκμεταλλεύσεις από παραβάτες ήταν πιο εύκολη. Το 2004, εξαιτίας ευπαθειών αποσύρθηκε. Μπορεί στις μέρες μας η ασφάλεια που προσφέρει να είναι ξεπερασμένη αλλά υπάρχουν περιπτώσεις που χρησιμοποιείται ακόμα όπως για παράδειγμα σε παλιές συσκευές που δεν υποστηρίζουν ακόμη νέες μεθόδους ασφάλειας (Kasperky.com).

5.9 WPA

Μετά την έκδοση του WEP ακολούθησε το WPA(Wifi Protected Access). Στην ουσία το WPA αντικατέστησε το WEP. Μπορεί να έχουν αρκετές ομοιότητες αλλά το WPA στην ουσία πρόσφερε σημαντικές βελτιώσεις στον τρόπο που έγιναν οι χειρισμοί των κλειδιών ασφαλείας αλλά και στον τρόπο που εξουσιοδοτούνταν οι χρήστες. Το WPA κάνει χρήση ενός πρωτοκόλλου ακεραιότητας προσωρινού κλειδιού (TKIP), το οποίο αλλάζει δυναμικά το κλειδί που κάνουν χρήση τα συστήματα. Αυτό έχει ως αποτέλεσμα οι παραβάτες να μην μπορούν να δημιουργήσουν εύκολα δικό τους κλειδί κρυπτογράφησης σαν κι αυτό που κάνει χρήση ένα δίκτυο που θεωρείται ασφαλές. Ωστόσο το πρότυπο TKIP αντικαταστάθηκε με το πρότυπο AES. Εκτός αυτού το WPA περιλαμβάνει και έλεγχο ακεραιότητας μηνυμάτων προκειμένου να κάνει έλεγχο αν ένας εισβολέας έχει προβεί

στην καταγραφή ή στην τροποποίηση δεδομένων. Τα κλειδιά που έκανε χρήση το WPA ήταν μεγέθους 256 bit. Ακόμη και αυτό από μόνο του δεν ήταν αρκετό για αυτό

5.10 WPA2

Το WPA 2 αποτελεί την βελτιωμένη έκδοση του WPA. Έχει την βάση του σε έναν ισχυρό μηχανισμό ασφαλείας (RSN). Έχει δύο λειτουργίες: α) την προσωπική λειτουργία ή προ-κοινόχρηστο κλειδί (WPA2-PSK) που έχει την βάση του σε έναν κοινό κωδικό πρόσβασης και τον χρησιμοποιούν κυρίως οικιακά περιβάλλοντα β) και η λειτουργία enterprise (WPA2-EAP) και ενδείκνυται για επαγγελματική χρήση. Οι δυο λειτουργίες που περιγράφησαν κάνουν χρήση του CCMP ενός πρωτοκόλλου που βασίζεται στον αλγόριθμο AES(Advanced Encryption Standard) και προσφέρει αυθεντικότητα και ακεραιότητα στο μήνυμα. Το πρωτόκολλο αυτό θεωρείται πιο ασφαλές αλλά και πιο αξιόπιστο από το TKIP καθώς δεν είναι εύκολο για τους εισβολείς να εντοπίσουν μοτίβα (kasperky.com)

5.11 WPA3

Το WPA3 προσέθεσε νέες δυνατότητες για οικιακή και για επαγγελματική χρήση όπως περιγράφεται παρακάτω. Πιο συγκεκριμένα προσέφερε α) εξατομικευμένη κρυπτογράφηση δεδομένων όπου με την σύνδεση σε ένα δημόσιο δίκτυο όπου το WPA3 κάνει εγγραφή μιας νέας συσκευής μέσα από μια διαδικασία διαφορετική από αυτή ενός κοινόχρηστου κωδικού πρόσβασης. Ακόμη κάνει χρήση ενός συστήματος πρωτοκόλλου παροχής συσκευής (DPP) όπου επιτρέπεται στους χρήστες να κάνουν χρήση ετικετών επικοινωνίας κοντινού πεδίου (NFC) ή κωδικών

QR για να επιτρέπουν συσκευές στο δίκτυο, β) Πρωτόκολλο με ταυτόχρονο έλεγχο ταυτότητας του Equals : Χρησιμοποιείται για να δημιουργηθεί μια ασφαλή χειραψία, όπου μια συσκευή δικτύου θα συνδεθεί σε ένα σημείο ασύρματης πρόσβασης και οι δύο συσκευές επικοινωνούν για να επαληθεύσουν τον έλεγχο ταυτότητας και τη σύνδεση. Ακόμα κι αν ο κωδικός πρόσβασης ενός χρήστη είναι αδύναμος, το WPA3 παρέχει μια πιο ασφαλή χειραψία χρησιμοποιώντας Wi-Fi DPP, γ) Ισχυρότερη προστασία από επίθεση ωμής βίας παρέχει προστασία από εικασίες κωδικού πρόσβασης εκτός σύνδεσης, επιτρέποντας στον χρήστη μόνο μία εικασία, αναγκάζοντας τον χρήστη να αλληλοεπιδράσει απευθείας με τη συσκευή Wi-Fi, πράγμα που σημαίνει ότι θα πρέπει να είναι φυσικά παρόν κάθε φορά που θέλει να μαντέψει τον κωδικό πρόσβασης. Το WPA2 στερείται ενσωματωμένης κρυπτογράφησης και ιδιωτικότητας σε δημόσια ανοιχτά δίκτυα, καθιστώντας τις επιθέσεις ωμής βίας σημαντική απειλή (Kaspersky.com).

Συμπεράσματα

Στην παρούσα εργασία έγινε μια προσπάθεια να παρουσιαστούν οι μορφές επιθέσεων στα ασύρματα και ενσύρματα δίκτυα καθώς και οι τρόποι αντιμετώπισής τους. Πραγματοποιήθηκε εκτεταμένη βιβλιογραφική έρευνα σχετικά με τις επιθέσεις που δέχονται τα δίκτυα, τις μορφές τους καθώς περιγράφηκαν τόσο οι τρόποι όσο και οι μέθοδοι που κυρίως χρησιμοποιούνται. Ακόμη, περιγράφονται τα εργαλεία που χρησιμοποιούν οι εισβολείς για να πραγματοποιήσουν μια επίθεση. Αποδείχτηκε ότι κάποιες από αυτές τις επιθέσεις είναι πιο ζημιογόνες από κάποιες άλλες. Ενδεικτικά το sniffingκαι το DDoS φαίνονται να είναι οι πιο καταστροφικές εκμεταλλευόμενες τους πόρους του δικτύου.

Από την βιβλιογραφική ανασκόπηση προέκυψε ότι οι ερευνητές εστίασαν την προσοχή τους στην ανάπτυξη άμυνας ως προς την μετάδοση του πακέτων παραχωρώντας με αυτόν τον τρόπο μια πίστωση προς τον πελάτη και στους ISPπου εφαρμόζουν. Το φιλτράρισμα σε ένα δίκτυο έδειξε ότι λειτουργεί αποτελεσματικά αλλά αποτρέπει τις επιθέσεις μόνο από το δικό του δίκτυο. Ωστόσο, βλέποντας τα πράγματα από την άλλη πλευρά, η υιοθέτηση πολιτικών άμυνας από τις επιθέσεις από την πλευρά του προορισμού των πακέτων μπορεί να εισαγάγει νέα προβλήματα. Επενδύοντας σε πολιτικές άμυνας για την αντιμετώπιση των επιθέσεων αποδεικνύεται στην πράξη μια λύση πολλά υποσχόμενη με καλά αποτελέσματα έχοντας όμως μπροστά του ένα ανυπέρβλητο εμπόδιο που δεν είναι άλλο από το Διαδίκτυο και την αρχιτεκτονική του η οποία περιλαμβάνει μερικές δεκάδες ASES. Κάθε ένα από αυτά περιλαμβάνει δρομολόγια IP που έχουν καθορισμένη τακτική δρομολόγησης στο διαδίκτυο. Ωστόσο τα πρωτόκολλα που διενεργούν την

δρομολόγηση συνεχίζουν να εξελίσσονται. Εφαρμόζοντας έναν αλγόριθμο με διαφορετική δρομολόγηση φαίνεται να μην είναι εύκολη υπόθεση η υλοποίηση ενός μηχανισμού άμυνας απέναντι στις επιθέσεις ώστε να είναι συμβατή με όλους. Έτσι αν η δρομολόγηση αφορά πολλαπλή διανομή των IP πολυεπίπεδο δίκτυο κάνει πιο δύσκολη την προσπάθεια ανάπτυξης μιας αποτελεσματικής πολιτικής άμυνας απέναντι στις επιθέσεις.

Βιβλιογραφία

Ελληνική Βιβλιογραφία

Αντωνίου, Π. (2011). Σημειώσεις Μαθήματος: Ασφάλεια Επικοινωνιακών Συστημάτων- Κρυπτογραφία Πανεπιστήμιο Κύπρου

Αραμπατζής, Α., (2019). Κρυπτογράφηση και Αποκρυπτογράφηση Διαθέσιμο: https://www.homodigitalis.gr/posts/4305 Πρόσβαση στις 28/7/2021

Κάτος, Β., Στεφανίδης, Γ., (2003). Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης Εκδόσεις Ζυγός

Μαυρίδης, (2015). Κεφάλαιο 3- Ασφαλής Διασύνδεση. Ανακτήθηκε από https://repository.kallipos.gr/bitstream/11419/1027/1/05_chapter_03.pdfAccess22/7/2021

Χριστοπούλου, Ε. (2013). Δίκτυα Υπολογιστών Ι. Σημειώσεις Θεωρίας Μαθήματος , ΙΕΚ Κέρκυρας Ακαδημαϊκό Έτος 2013-2014

ΞενόγλωσσηΒιβλιογραφία

Akash KM, Chandra P, Archana T. (2015). Performance Evaluation of Cryptographic Algorithms: DES and AES. IEEE Students' Conference on Electrical, Electronics and Computer Science:1-5.

Aman K, Sudesh J, Sunil M.(2012). Comparative Analysis between DES and RSA Algorithm's. International Journal of Advanced Research in Computer Science and Software Engineering. ;2(7):386-391.

Awati, R. (2021). CachePoisoning. Διαθέσιμο στο https://searchsecurity.techtarget.com/definition/cache-poisoning [Πρόσβαση 15/11/2021]

Cisco, (2004). Metropolitan-Area Network (MANs). Available at: https://slidetodoc.com/ccna-1-v-3-1-module-2-networking-2/ Access at: 29/6/2021

Cisco, (2006). Cisco PIX 515E Security Appliance Getting Started Guide: Obtaining a DES License or a 3DES-AES License" (PDF). Cisco. 2006. [Access 5/8/2021]

Cisco, (2006). How does Radius work. [Access 5/3/2022]

Cisco, (2012). Cisco CCNA Wide Area Networks (WANs) Part I Available at: https://www.certificationkits.com/cisco-certification/cisco-ccna-640-802-exam-certification-guide/cisco-ccna-wide-area-networks-wans-part-i/ Access at: 29/6/2021

Cisco, (2013). Cisco ICND1 Foundation Learning Guide: LANs and Ethernet Availableat:https://www.ciscopress.com/articles/article.asp?p=2092245&seqNum=2 and available at: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html [Acess 28/6/2021]

Cisco, (2021). Mac Spoofing Attack Available at: https://www.ccexpert.us/ccie-security/mac-spoofing-attack.html Access 7/7/2021

Davis, D. (2008) Cisco Administration 101: Understand the OSI model to become a better Cisco troubleshooter Available at: https://www.techrepublic.com/blog/data-center/cisco-administration-101-understand-the-osi-model-to-become-a-better-cisco-troubleshooter/ Access at: 29/6/2021

Ferguson, P. &Senie, D. (2000). Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, rfc2827 (Technical

report). Cisco Systems, Inc.,13625 Dulles Technology Dr.,Herndon, Virginia 20170 USA: Cisco Systems, Inc. and Amaranth Networks Inc

Federal Information Processing Standards Publication (FIPS), (2001). Announcing the Advanced Encryption Standard (AES) Available at:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf Access 30/7/2021

Ginni. (2021).What is the difference between LAN, MAN, and WAN Available at:https://www.tutorialspoint.com/what-is-the-difference-between-lan-man-and-wan [Access 26/6/2021]

Information Security, (1996). Computer Attacks at Department of Defense Pose Increasing Risks: A Report to Congressional Requesters.

Jannas, A. (2019). Networking Fundamentals: Metropolitan Area Network (MAN) Available at: https://www.quickstart.com/blog/networking-fundamentals-metropolitan-area-network-man/ Access at:29/6/2021

Qadri, S., & Pandey, K., (2012). Tag Based Client Side Detection of Content Sniffing Attacks with File Encryption and File Splitter Technique. International Journal of Advanced Computer Research. 2(5),No-3: 215-221.

Quine, A. (2008). Carrier Sense Multiple Access Collision Detect (CSMA/CD) Explained. Available at: https://www.itprc.com/carrier-sense-multiple-access-collision-detect-csmacd-explained/ [Access at 1/7/2021]

Karthik S, Muruganandam A.(2014). Data encryption and decryption by using triple DES and performance analysis of crypto system. International Journal of Scientific Engineering and Research. ;2(11):24-31.

Kulshrestha, A., & Dubey, S. (2014). A Literature Review on Sniffing Attacks in Computer Network". International Journal of Advanced Engineering Research and Science 1(2): 32- 37.

Martellini, Mauricio, Malizia, Andrea (2017). Challenges Cyber and Chemical, Biological, Radiological, Nuclear, Explosives: Threats and Attempts. Saltant. ISBN 9783319621081.

Mirkovic, J., Jevtic, N. &Reiher, P. (2006). A practical IP Spoofing Defense through Route-based Filtering(Technical report). University of Delaware

Mohammed N. Abdul W., Abdulrahman A, Babak E. and Mohamed M, (2018). A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention Received: June 22, 2018; Accepted: July 12, 2018; Published: August 10, 2018

Ohtsuka, T., Nakamura, F., Sekiya, Y. & Wakahara, Y. (2007). Realization of FSN Method for Detecting IPSpoofed Packets by making use of OSPF (Technical Report 577). The University of Tokyo,2-11-16 Yayoi bunkyoku Tokyo, Japan: Graduate School of Frontier Sciences.

Pandey, S., & Chauhan, S., (2013) Secure Content Sniffing for Web Browser: A Survey". International Journal of Advanced Research in Computer and Communication Engineering, 2(9): 3595 – 3601.

Park, K. & Lee, H. (2001). On the Effectiveness of Route- Based Packet Filtering for Distributed Dos Attack Prevention in Power-Law Internets, Vol. 31.

Preetha M, Nithya M.(2013). A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.

Petters, J. (2020). What is a DDoS attack? Identifying Denial of Service Attacks. Available at: https://www.varonis.com/blog/what-is-a-ddos-attack/ Access: 13/7/2021

Postel, J. (1981). Internet Protocol (Technical report). University of Southern California, 4676 Admiralty Way, Marina del Rey, California 90291: Information Sciences Institute.

Prabadevi, B., Jeyanthi, N. (2018).A Review on Various Sniffing Attacks and its Mitigation Techniques. Indonesian Journal of Electrical Engineering and Computer Science.Vol. 12, No. 3, December 2018, pp. 1117~1125, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i3.pp1117-1125

Ritu P, Vikas k.(2013). Efficient Implementation of AES. International Journal of Advanced Research in Computer Science and Software Engineering. ;3(7):290-295.

Rezos, W. (2009). Cache Poisoning Available at: https://owasp.org/www-community/attacks/Cache_Poisoning Access at 18/7/2021

Simson, G. Gene, S. Schwartz. Alan, (2003). Practical UNIX and Internet Security, O'Reilly

Shraddha D. (2016). Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java. International Journal of Computer Trends and Technology. 2016;35(4):179-183.

Shue, C., Gupta & M., Davy, M.P. (2008). Packet Forwarding with Source Verification. Computer Networks: The International Journal of Computer andTelecommunications Networking, 52 (8), 1567-1582

Soon, L., Othman, M., Udzir, N., (2009). IP Spoofing Defense: An Introduction Department of Communication Technology and Network Universiti Putra Malaysia, 43400 Serdang, Selangor E-mail :a leesoon3@gmail.com, b,c{mothman,izura}@fsktm.upm.edu.my

Stallings W.(2011). Cryptography and network Security: Principles and Practice. 5th Edition Pearson Education/Prentice Hall; 2011.

Teach Target Contributor, (2005). Electronic Code Book (ECB). Available at:https://searchsecurity.techtarget.com/definition/Electronic-Code-Book Access 30/7/2021

Wang, H., Jin, C. & Shin, K. G. (2007). Defense against Spoofed IP Traffic using Hop-count filtering. IEEE/ACM Transactions on Networking, 15 (1), 40-53.

Xin Z, Xiaofei T.(2011). Research and Implementation of RSA Algorithm for Encryption and Decryption. 6th International Forum on Strategic Technology. 1118-1121.

Ηλεκτρονικές Πηγές:

https://www.techtarget.com/searchmobilecomputing/definition/war-driving

https://www.imperva.com/learn/ddos/syn-flood/

https://el.wizcase.com/blog/%CE%AD%CE%BD%CE%B1%CF%82-%CF%80%CE%BB%CE%AE%CF%81%CE%B7%CF%82-%CE%BF%CE%B4%CE%B7%CE%B3%CF%8C%CF%82-%CE%B3%CE%B9%CE%B1-

%CE%B1%CF%81%CF%87%CE%B1%CF%81%CE%AF%CE%BF%CF%85%CF%82-%CF%83%CF%84%CE%B1-vpn/

www. techopedia.com

https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa