ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ 1578

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΑΠΟΚΡΙΣΗΣ ΕΠΙΘΕΣΕΩΝ

ΑΝΤΩΝΑΤΟΣ ΙΩΑΝΝΗΣ **ΚΡΙΚΑΣ ΒΕΛΙΣΣΑΡΙΟΣ**

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: **ΚΑΡΕΛΗΣ ΔΗΜΗΤΡΙΟΣ**

ΠΑΤΡΑ, ΙΟΥΝΙΟΣ 2016

Πρόλογος / Περίληψη

Η παρούσα πτυχιακή εργασία έχει ως σκοπό τη δημιουργία ενός Web Server με λογισμικό Ubuntu Linux και τον έλεγχο της ασφάλειάς του από κακόβουλες επιθέσεις.

Στο 1^{ο} κεφάλαιο ορίζεται η έννοια ενός δικτύου υπολογιστών και παρουσιάζονται τα μέσα μετάδοσης και οι συσκευές που το αποτελούν.

Στο 2^{ο} κεφάλαιο γίνετε παρουσίαση των ασύρματων δικτύων αναλύοντας τα πρωτόκολλα επικοινωνίας και την ιστορική εξέλιξη των προτύπων των Wireless-LAN. Επιπρόσθετα γίνετε διαχωρισμός των πλεονεκτημάτων και των μειονεκτημάτων των ασύρματων δικτύων.

Εν συνεχεία, στο 3^{ο} κεφάλαιο γίνεται αναφορά στη προστασία των ασύρματων δικτύων και το λόγο που χρειάζονται κάποιο είδος ασφάλειας για την προστασία των διαφόρων δεδομένων και προσωπικών πληροφοριών. Συνεπώς αναλύεται η κρυπτογράφηση δεδομένων και τα πρωτόκολλα κρυπτογράφησης WEP, WPA – WPA2, καθώς και η σύγκριση αυτών.

Στο 4^{ο} κεφάλαιο επιχειρείται αρχικά ο ορισμός και η ανάλυση των επιθέσεων Denial of Service (DoS) και Distributed Denial of Service (DDoS) καθώς και η ανάλυση διαφόρων τρόπων ανίχνευσης και πρόληψης επιθέσεων, κυρίως μέσω υπογραφής και ανίχνευσης ανωμαλιών. Τέλος, γίνεται αναφορά στα μέσα που χρησιμοποιήθηκαν για να πραγματοποιηθεί το πρακτικό μέρος της πτυχιακής και στο σύνολο της διαδικασίας.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

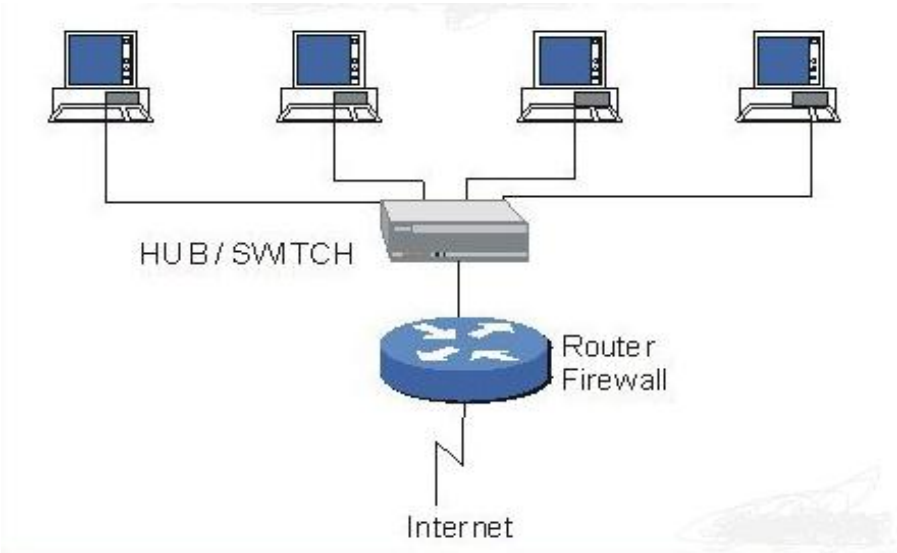
Εισαγωγή

1.1 Γενικά

Ο άνθρωπος χρησιμοποιεί πολλούς αιώνες την επικοινωνία ως μέσο για ανταλλαγή πληροφοριών. Ωστόσο μόλις τον 20ο αιώνα κατάφερε να εξασφαλίσει την απομακρυσμένη επικοινωνία και τη μετάδοση της πληροφορίας μέσω του τηλεφωνικού, του τηλεοπτικού, του ραδιοφωνικού σήματος, καθώς και των υπολογιστικών δικτύων, τα οποία δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Οι ηλεκτρονικοί υπολογιστές κατασκευάστηκαν για να επεξεργάζονται και να διαχειρίζονται την πληροφορία. Αργότερα προέκυψε η ανάγκη διακίνησης της πληροφορίας σε μεγάλες αποστάσεις με αποτέλεσμα να δημιουργηθούν τα δίκτυα υπολογιστών που διαχειρίζονταν και επεξεργάζονταν τις πληροφορίες μεταξύ τους.

1.2 Τι είναι δίκτυο υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο ή περισσότερους αυτόνομους και ανεξάρτητους υπολογιστές και περιφερειακές συσκευές. Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες.



Σχήμα. 1.1 Δίκτυο Υπολογιστών

Η αρχιτεκτονική των δικτύων καθορίζει τον τρόπο με τον οποίο οι υπολογιστές και οι λοιπές συσκευές συνδέονται μεταξύ τους για να σχηματίσουν ένα σύστημα επικοινωνίας που θα επιτρέπει στους χρήστες να διαμοιράζονται πληροφορίες και συσκευές του δικτύου.

Σε ένα δίκτυο δεδομένων περιλαμβάνονται:

- Τερματικοί Κόμβοι: Ελέγχουν τους πόρους του δικτύου (λογισμικό και υλικό).
- Υποδίκτυα: Φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τοπολογία, τερματικοί κόμβοι, πόροι που μπορούν να διαφέρουν πολύ ανά υποδίκτυο.
- Συσκευές διασύνδεσης: Συνδέουν τα ετερογενή υποδίκτυα έτσι ώστε να εξασφαλίζεται η επικοινωνία τερματικών κόμβων που βρίσκονται σε διαφορετικά υποδίκτυα.

Τα δίκτυα φέρουν τους εξής χαρακτηρισμούς, που καθορίζουν και την κατηγορία τους :

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως «ενσύρματα» ή «ασύρματα».
- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως «δημόσια» ή «ιδιωτικά» δίκτυα.
- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως «τοπικά» (LAN και WLAN), «μητροπολιτικά» (MAN και WMAN), «ευρείας κάλυψης» (WAN και WWAN) και «προσωπικά» (PAN και WPAN).

Οι χαρακτηρισμοί με το πρόσθετο W ανταποκρίνονται στον ασύρματο (Wireless) τρόπο σύνδεσης.

Η διαφορά μεταξύ της ενσύρματης και της ασύρματης μετάδοσης εντοπίζεται στο φυσικό μέσο μετάδοσης της πληροφορίας. Τα ασύρματα δίκτυα δεν χρησιμοποιούν ως μέσο μετάδοσης κάποιον τύπο καλωδίου για τη μεταφορά των δεδομένων, αλλά ηλεκτρομαγνητικά κύματα, με συχνότητα συνήθως 2,4 και 5 GHz. Για την ομαλή επικοινωνία μεταξύ των ασύρματων και ενσύρματων δικτύων, απαιτείται η χρήση συγκεκριμένων προτύπων.

1.3 Τύποι, μέσα μετάδοσης, καλώδια

1.3.1 Τύποι δικτύων

Ένα δίκτυο υπολογιστών δημιουργείται όταν δυο ή περισσότεροι υπολογιστές επικοινωνούν μεταξύ τους. Τα δίκτυα μπορούν να κατηγοριοποιηθούν με διάφορες μεθόδους. Οι μέθοδοι που ευρέως κατηγοριοποιούν τα δίκτυα είναι: ανάλογα με το μέγεθος της περιοχής που καλύπτουν, και ανάλογα με την τεχνολογία που χρησιμοποιούν.

Οι τύποι δικτύων που υπάρχουν αυτή την στιγμή αναφέρονται παρακάτω:

- **PAN (Personal Area Network)**: Αυτό το δίκτυο αποτελείται από προσωπικές συσκευές που επικοινωνούν σε κοντινή απόσταση όπως π.χ. ένα κινητό τηλέφωνο με ένα laptop. Αυτά τα δίκτυα χρησιμοποιούν ενσύρματη ή ασύρματη σύνδεση.
- **LAN (Local Area Network)**: Είναι τα τοπικά δίκτυα που καλύπτουν μια σχετικά μικρή περιοχή όπως ένα γραφείο, μια κατοικία, ένα σχολείο, ή μια μικρή επιχείρηση. Αυτά τα δίκτυα χρησιμοποιούν ενσύρματη ή ασύρματη σύνδεση, ή και τα δυο.
- **WLAN (Wireless Local Area Network)**: Είναι τα ασύρματα τοπικά δίκτυα που καλύπτουν μια περιορισμένη γεωγραφικά περιοχή και είναι δημοφιλή σε περιοχές που τα καλώδια δικτύου είναι δύσκολο να εγκατασταθούν. Επίσης εγκαθίστανται σε περιοχές όπου θέλουμε να έχουμε κάλυψη σε φορητούς υπολογιστές, tablet, smartphone. Τέτοιες περιοχές είναι: δημόσιοι χώροι, ξενοδοχεία, καφετέριες, οικίες, γραφεία και σχολεία.
- **MAN (Metropolitan Area Network)**: Αυτά τα δίκτυα καλύπτουν μια ευρύτερη περιοχή μιας πόλης, ή ενός Πανεπιστημίου. Οι τεχνολογίες που χρησιμοποιούνται σε αυτού του είδους τα δίκτυα μπορεί να είναι ασύρματες ή και ενσύρματες (Ethernet με καλώδια οπτικών ινών).
- **WAN (Wide Area Network)**: Αυτά τα δίκτυα καλύπτουν διευρυμένες γεωγραφικά περιοχές και αποτελούνται από πολλά μικρά δίκτυα. Το μεγαλύτερο WAN στον πλανήτη, είναι το διαδίκτυο (Internet).

1.3.2 Μέσα μετάδοσης

Τα μέσα μετάδοσης διακρίνονται σε δυο κατηγορίες. Τα **ενσύρματα** και τα **ασύρματα**. Τα ενσύρματα μέσα σχηματίζονται από μεταλλικούς αγωγούς - καλώδια, ενώ στα ασύρματα, το μέσο μετάδοσης είναι ο ελεύθερος χώρος μεταξύ του πομπού και του δέκτη. Τα ενσύρματα μέσα μετάδοσης είναι τα γνωστά σε όλους χάλκινα καλώδια, τα ομοαξονικά καλώδια και οι οπτικές ίνες. Τα ασύρματα μέσα μετάδοσης είναι οι επίγειες και οι δορυφορικές μικρο - κυματικές ζεύξεις και το σύστημα κυψελοειδούς τηλεφωνίας (κινητή τηλεφωνία).

1.3.3 Καλώδια

Τα καλώδια, που χρησιμοποιούνται στα δίκτυα είναι:

- Καλώδια συνεστραμμένων ζευγών
- Ομοαξονικά καλώδια
- Καλώδια οπτικών ινών

1.4 Συσκευές τοπικών δικτύων

1.4.1 Κάρτα δικτύου

Σχήμα 1.2: *Κάρτα δικτύου*

Η **κάρτα δικτύου** ή **ελεγκτής διασύνδεσης δικτύου** (network interface controller), είναι μια συσκευή που συνδέει έναν υπολογιστή σε ένα τοπικό δίκτυο υπολογιστών. Οι κάρτες δικτύου τοποθετούνται είτε σαν κάρτες επέκτασης σε κάποια κενή θέση του δίαυλου ενός υπολογιστή, ή πάνω στη μητρική κάρτα του υπολογιστή (on-board). Λόγω της διάδοσης και του χαμηλού κόστους του προτύπου Ethernet, όλοι οι υπολογιστές πλέον έχουν κάρτα δικτύου.

1.4.2 Modem

Σχήμα 1.3: *Modem*

Το **μόντεμ** (modem), είναι ένας όρος που προέρχεται από τη σύντμηση των αγγλικών λέξεων **Modulator** (διαμορφωτής) και **Demodulator** (αποδιαμορφωτής).

Είναι μια συσκευή η οποία μετατρέπει το ψηφιακό σήμα που προέρχεται από ένα ηλεκτρονικό υπολογιστικό σύστημα σε αναλογικό σήμα, το οποίο είναι κατάλληλο για την μεταφορά του μέσω κοινής τηλεφωνικής ή άλλου τύπου ενσύρματης γραμμής, ή ακόμα και μέσω ασύρματης ζεύξης. Επίσης διαθέτει και τμήμα αποδιαμόρφωσης για την αντίστροφη διαδικασία, δηλαδή τη μετατροπή του αναλογικού (διαμορφωμένου) σήματος σε ψηφιακό.

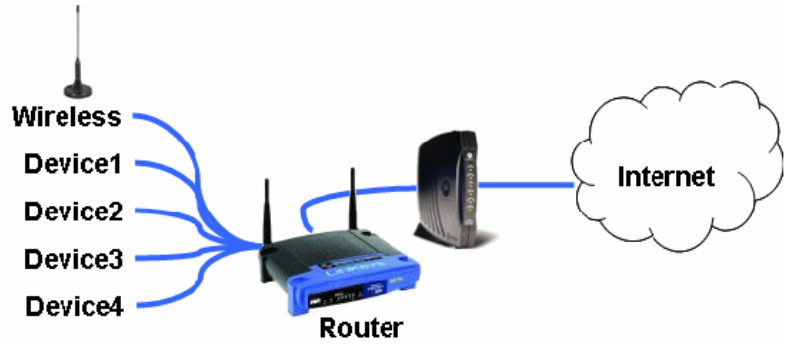
1.4.3 Hub - Switch

Η **πλήμνη** (hub) είναι μια δικτυακή συσκευή στην οποία συνδέονται ενσύρματα υπολογιστές μέσω καλωδίων συνεστραμμένων ζευγών. Χρησιμοποιείται σε τοπικά δίκτυα ethernet. Οι συσκευές αυτές είναι πλέον παρωχημένες, δεδομένου ότι έχουν αντικατασταθεί από τα Switch.

Ο **μεταγωγέας** (switch) είναι μια δικτυακή συσκευή που χρησιμοποιείται στα δίκτυα υπολογιστών. Αποτελεί ένα συνδυασμό του επαναλήπτη (Hub) και της γέφυρας (bridge). Το βασικό χαρακτηριστικό του μεταγωγέα (switch) είναι ότι κάθε θύρα του, προσφέρει καθορισμένο εύρος ζώνης, σε αντίθεση με το Hub, που όλες οι συσκευές οι οποίες συνδέονται σε αυτό μοιράζονται το εύρος ζώνης.

1.4.4 Router

Ο **Δρομολογητής** (router) είναι ένας ειδικός υπολογιστής με δική του CPU και RAM ο οποίος αναλαμβάνει να διασυνδέσει δίκτυα υπολογιστών. Επίσης, αναλαμβάνει την αποστολή και λήψη πακέτων δεδομένων μεταξύ δικτύων υπολογιστών. Η διαδικασία επιλογής διαδρομών μεταξύ των δικτύων, με βέλτιστο τρόπο, χρησιμοποιώντας κατάλληλους αλγόριθμους έτσι ώστε να πραγματοποιηθεί η μετάδοση των δεδομένων από έναν κόμβο αφετηρίας σε έναν κόμβο προορισμού λέγεται δρομολόγηση.
Ο δρομολογητής χρησιμοποιεί ένα ή περισσότερα πρωτόκολλα δρομολόγησης. Με βάση αυτά τα πρωτόκολλα καθορίζει ποιος δρομολογητής είναι κατάλληλος ανά χρονική στιγμή και δρομολογεί τα πακέτα δεδομένων προς αυτούς.



Σχήμα 1.4: *Router*

1.4.5 Wireless Access Point

Στα δίκτυα υπολογιστών, ασύρματο σημείο πρόσβασης ή σταθμός βάσης (Wireless Access Point) είναι μια συσκευή που συνδέει μεταξύ τους άλλες ασύρματες συσκευές επικοινωνίας με σκοπό τη δημιουργία ενός ασύρματου δικτύου. Ο σταθμός βάσης συνήθως συνδέεται με ένα ενσύρματο δίκτυο και μπορεί να μεταφέρει δεδομένα ανάμεσα στις ασύρματες και τις ενσύρματες συσκευές. Όταν υπάρχει ανάγκη, συνδέουμε πολλούς σταθμούς βάσης μεταξύ τους, για να σχηματίσουμε ένα μεγαλύτερο δίκτυο το οποίο επιτρέπει περιαγωγή.

Κεφάλαιο 2

Ασύρματα Δίκτυα

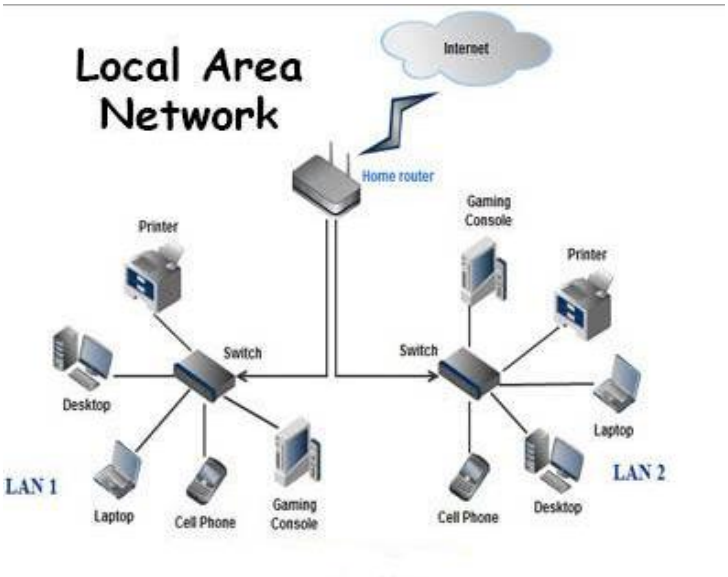
2.1 Γενικά

Ασύρματο δίκτυο είναι ένα σύστημα επικοινωνίας μέσω ηλεκτρομαγνητικών κυμάτων ανάμεσα σε σταθερούς ή κινητούς χρήστες επιτρέποντας την μεταξύ τους διασύνδεση και ανταλλαγή δεδομένων.

Μόλις τα τελευταία χρόνια, τα ασύρματα δίκτυα, άρχισαν να καταλαμβάνουν ένα σημαντικό τμήμα της αγοράς δικτύων. Ολοένα και περισσότερο, οι οργανισμοί και οι επιχειρήσεις διαπιστώνουν ότι τα ασύρματα τοπικά δίκτυα αποτελούν απαραίτητο συμπλήρωμα των παραδοσιακών ενσύρματων δικτύων, για την ικανοποίηση των απαιτήσεων της φορητότητας, της μετεγκατάστασης, της ad hoc δικτύωσης και της κάλυψης τοποθεσιών για τις οποίες είναι δύσκολη η εγκατάσταση καλωδίων.

2.2 Πλεονεκτήματα – Μειονεκτήματα

Στα αρχικά στάδια της τεχνολογίας του, το ασύρματο δίκτυο λόγω των αρκετών μειονεκτημάτων και της έλλειψης προτύπων δεν ήταν ιδιαίτερα διαδεδομένο. Με την τεχνολογική εξέλιξη τα σύγχρονα ασύρματα δίκτυα είναι ιδιαίτερα διαδεδομένα αφού έχουν πλέον χαμηλό κόστος και ποιότητα υπηρεσιών παρόμοια με τα ενσύρματα δίκτυα.



Σχήμα 2.1: *Τοπικό Ασύρματο Δίκτυο (LAN)*

2.2.1 Πλεονεκτήματα

Η χρήση της ασύρματης μετάδοσης έχει μία σειρά από πλεονεκτήματα:

- Κινητικότητα χρήστη: Οι χρήστες μπορούν να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου, δηλαδή σε χώρο που θα έχουν επαρκές σήμα, διατηρώντας την συνδεσιμότητα τους.

- Ευκολία, ευελιξία και απλότητα εγκατάστασης: Μπορεί να γίνει η δικτύωση σε μέρη όπου η καλωδίωση θα ήταν αδύνατη ή μη επιθυμητή.

- Κλιμάκωση, δυνατότητα επέκτασης: Τα ασύρματα δίκτυα μπορούν να διαρθρωθούν σε ένα πλήθος από τοπολογίες, ώστε να ταιριάξουν στις απαιτήσεις των εφαρμογών. Οι τοπολογίες αλλάζουν εύκολα και επεκτείνονται από απλά δίκτυα με μικρό αριθμό χρηστών, έως μεγάλες δομές δικτύων με εκατοντάδες χρήστες.

- Κόστος: Παρόλο που το αρχικό κόστος εγκατάστασης είναι υψηλότερο σε σχέση με λύσεις της ενσύρματης δικτύωσης, το τελικό όμως κόστος για όλη τη διάρκεια ζωής της επένδυσης μπορεί να είναι μικρότερο, ιδιαίτερα σε δυναμικό περιβάλλον που απαιτεί συχνές αλλαγές, αναδιαρθρώσεις και μετακινήσεις. Με την εμφάνιση περισσότερων κατασκευαστών και τον έντονο ανταγωνισμό μεταξύ τους το κόστος έχει πέσει αισθητά, ενώ παράλληλα οι συσκευές έχουν αποκτήσει περισσότερα ποιοτικά χαρακτηριστικά.

- Ταχύτητες μετάδοσης: Όσο αναπτύσσεται η τεχνολογία γίνεται δυνατή η μετάδοση μεγαλύτερων ρυθμών δεδομένων. Ήδη ο μέγιστος ρυθμός μετάδοσης δεδομένων, από τα 2 Mbps που μπορούσαν να επιτευχθούν αρχικά, έφτασε σήμερα σε ταχύτητες πάνω από 400 Mbps ενώ ήδη έχουν εξαγγελθεί ακόμα μεγαλύτερες ταχύτητες.

- Αξιοπιστία-ανεξαρτησία: Ένα ασύρματο δίκτυο κατάλληλα διαμορφωμένο μπορεί να έχει μεγάλη αξιοπιστία. Μπορεί να σχεδιαστεί ώστε να λειτουργεί όταν συμβαίνουν διακοπές ρεύματος και να περιλαμβάνει πολλές εναλλακτικές διαδρομές.

- Εμβέλεια: Η εμβέλεια ενός ασύρματου δικτύου μπορεί να είναι μερικές δεκάδες μέτρα σε κλειστό χώρο, ενώ σε ανοιχτό χώρο οι αποστάσεις που μπορεί να καλυφθούν είναι μεγαλύτερες.

- Συμβατότητα με το υπάρχον δίκτυο: Τα περισσότερα ασύρματα δίκτυα συνδέονται με τα ενσύρματα δίκτυα βάσει προτύπων. Έτσι, η προσθήκη ασύρματης δικτύωσης σε υπάρχουσες δομές δικτύων μπορεί να γίνει με ευκολότερο τρόπο. Πολλές φορές δε, αποτελούν επέκταση ενός ενσύρματου δικτύου.

2.2.2. Μειονεκτήματα

Η χρήση των ασύρματων δικτύων για την μεταφορά πληροφορίας τα κάνουν ευπρόσβλητα σε πολλά φαινόμενα παρεμβολών, τα οποία αλλοιώνουν την επικοινωνία των χρηστών.

Τα μειονεκτήματα των ασύρματων δικτύων μπορούν να συνοψιστούν ως εξής:

- Ασφάλεια: Είναι γνωστό ότι τα δίκτυα υστερούν στον τομέα της ασφάλειας, καθώς υπάρχουν πολλοί τρόποι επίθεσης από επίδοξους εισβολείς. Επιθέσεις παρεμπόδισης των επικοινωνιών (jamming) και καταγραφής δεδομένων που κινούνται στο δίκτυο (sniffing), είναι ιδιαίτερα διαδεδομένες.

- Παρεμβολές: Τα ασύρματα τοπικά δίκτυα, κυρίως όσα βρίσκονται σε ζώνες χαμηλής συχνότητας, είναι ευάλωτα στις παρεμβολές. Μπορεί να δεχτούν και να προκαλέσουν παρεμβολές σε άλλα 2.4 GHz προϊόντα, όπως τα ασύρματα τηλέφωνα ή να δεχθούν παρεμβολές από αρμονικές συχνότητες από συσκευές που εκπέμπουν σε υποπολλαπλάσια της συχνότητας λειτουργίας. Όμως το σημαντικότερο πρόβλημα παρεμβολών προκύπτει από την κακή σχεδίαση ενός ασύρματου δικτύου, όπως μεγαλύτερη ισχύς εκπομπής από το αναγκαίο, ακατάλληλες κεραίες, συσκευές με μικρή ευαισθησία, λάθος επιλογή συχνότητας και τοποθεσίας.

- Προστασία της υγείας των χρηστών: Ο εξοπλισμός που χρησιμοποιείται πρέπει να είναι απολύτως συμβατός με τις διεθνείς και ευρωπαϊκές οδηγίες και να είναι αποδεκτός από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI).

2.3 Πρωτόκολλα Επικοινωνίας

Η δικτύωση μας δίνει τη δυνατότητα διασύνδεσης υπολογιστών με διαφορετικά λειτουργικά συστήματα και επικοινωνίας μεταξύ διαφορετικών εφαρμογών λογισμικού. Για να γίνει εφικτή η επικοινωνία, όλοι οι υπολογιστές και οι εφαρμογές χρησιμοποιούν το ίδιο σύνολο κανόνων και διαδικασιών για την ανταλλαγή δεδομένων. Αυτοί οι κανόνες ονομάζονται **πρωτόκολλο επικοινωνίας** (communication protocol). Έτσι τα δεδομένα μπορούν να αναπαρίστανται διαφορετικά σε κάθε υπολογιστή, όμως στο δίκτυο «ταξιδεύουν» έχοντας μορφή και οργάνωση κοινά αποδεκτές απ' όλους τους υπολογιστές του δικτύου.

Εξαιτίας της πληθώρας διαφορετικών αρχιτεκτονικών υπολογιστών, λειτουργικών συστημάτων, εφαρμογών και τύπων δικτύων υπάρχει πολυπλοκότητα στο είδος και στο πλήθος των πρωτοκόλλων επικοινωνίας. Υπάρχουν π.χ. πρωτόκολλα που ρυθμίζουν την επικοινωνία στο φυσικό μέσο διασύνδεσης, μεταξύ των καρτών

δικτύου και του καλωδίου. Σε αυτά τα πρωτόκολλα δε γίνεται διάκριση μεταξύ των πληροφοριών · όλες μαζί ενσωματώνονται σε πακέτα, δηλαδή αυτοτελείς μονάδες πληροφορίας μήκους μερικών εκατοντάδων bytes που ταξιδεύουν στο δίκτυο.

Τα πρωτόκολλα εξαρτώνται από την ταχύτητα του δικτύου, τον τρόπο επικοινωνίας υπολογιστή - δικτύου κλπ. Υπάρχουν όμως πρωτόκολλα ανωτέρου επιπέδου που έχουν σχέση με την επικοινωνία των εφαρμογών και διακρίνουν τις πληροφορίες, μεταφράζοντάς τις για επεξεργασία από κάποιο πρόγραμμα. Το κάθε πρωτόκολλο έχει τη δυνατότητα να ελέγχει και να διορθώνει λάθη στο επίπεδο που ρυθμίζει.

Τα πιο γνωστά πρωτόκολλα επικοινωνίας είναι:

- Xmodem/Zmodem/Ymodem/Kermit: Απλά πρωτόκολλα επικοινωνίας για σύνδεση μέσω modem. Διαφέρουν ως προς το μέγεθος του πακέτου που χρησιμοποιείται για την αποστολή δεδομένων. Έτσι το Xmodem χρησιμοποιεί μέγεθος 128 bytes για κάθε πακέτο, το Zmodem 512 bytes και το Ymodem 1024 bytes. Το Kermit έχει πακέτα μεταβλητού μεγέθους.

- Ethernet: Το πιο διαδεδομένο πρωτόκολλο επικοινωνίας σε τοπικά δίκτυα υπολογιστών

- Token Ring: Πρωτόκολλο επικοινωνίας που βασίζεται στην ύπαρξη ενός ειδικού πακέτου (σκυτάλη) που ταξιδεύει μέσα στο δίκτυο. Όποιος υπολογιστής είναι ιδιοκτήτης του πακέτου, έχει τον έλεγχο του δικτύου, και μπορεί να αποστείλει δεδομένα.

- FDDI: Πρωτόκολλο επικοινωνίας για μεγάλες ταχύτητες δικτύων με οπτικές ίνες. Χρησιμοποιείται κυρίως σε *δίκτυα κορμού* (backbone) που συνενώνουν μικρότερα δίκτυα Ethernet.

- ATM: Πρωτόκολλο που υποστηρίζει πολύ μεγάλες ταχύτητες επικοινωνίας

- Frame Relay: Άλλο ένα πρωτόκολλο υψηλών ταχυτήτων για δίκτυα κορμού.

- PowerTalk: Πρωτόκολλο επικοινωνίας για υπολογιστές Apple Macintosh

- X.25: Διεθνές πρότυπο για δίκτυα μεταγωγής πακέτου.

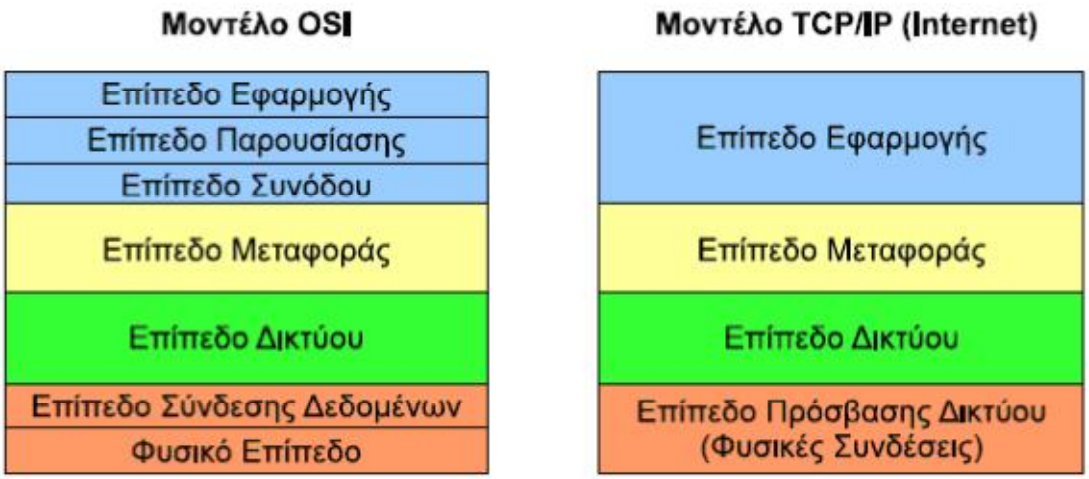
- TCP/IP: Πρωτόκολλο περιγραφής των πακέτων που μεταδίδονται σε ένα δίκτυο. Είναι το ευρέως διαδεδομένο πρωτόκολλο στην κοινότητα του Διαδικτύου (Internet).

- IPX: Πρωτόκολλο με λειτουργία αντίστοιχη του TCP/IP που χρησιμοποιείται σε δίκτυα Novell.

2.3.1. TCP/IP Δίκτυα

Το **TCP/IP** είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων που περιέχει, το TCP ή Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μετάδοσης) και το IP ή Internet Protocol (Πρωτόκολλο Διαδικτύου).

Αυτή η συλλογή πρωτοκόλλων, είναι οργανωμένη σε 4 στρώματα ή επίπεδα (layers) και αποτελεί εξέλιξη του μοντέλου OSI, το οποίο παραμένει έως σήμερα μόνο θεωρητικό και προτείνει την κατάταξη των πρωτοκόλλων δικτύων σε έναν οργάνωση 7 στρωμάτων. Το καθένα τους απαντά σε συγκεκριμένα προβλήματα μεταφοράς δεδομένων και παρέχει μια καθορισμένη υπηρεσία στα υψηλότερα στρώματα. Τα ανώτερα επίπεδα είναι πιο κοντά στη λογική του χρήστη και εξετάζουν πιο αφηρημένα δεδομένα, στηριζόμενα σε πρωτόκολλα χαμηλότερων στρωμάτων για να μεταφράσουν δεδομένα σε μορφές που μπορούν να διαβιβαστούν με φυσικά μέσα. Στο παρακάτω σχήμα φαίνεται η σχέση των δυο μοντέλων.



Σχήμα 2.2: *Σχέση μοντέλου OSI και TCP/IP*

2.4 Πρότυπα WLAN

Το **Institute of Electrical and Electronic Engineers (IEEE)** είναι ένας οργανισμός που, μεταξύ των άλλων, δημιουργεί και δημοσιεύει πρότυπα. Είναι ιδιαίτερα γνωστό για την οικογένεια προτύπων IEEE 802, που καλύπτουν τα τοπικά και μητροπολιτικά δίκτυα (LAN/MAN). Τα ασύρματα τοπικά δίκτυα ορίζονται από το πρότυπο 802.11 του οργανισμού IEEE.

Η **Wi-Fi Alliance** είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος ειδικεύεται στα 802.11 ασύρματα τοπικά δίκτυα (WLAN). Ιδρύθηκε το 1999 με σκοπό την διασφάλιση της συμβατότητας μεταξύ των WLAN προϊόντων διαφόρων κατασκευαστών, μέσω μιας διαδικασίας πιστοποίησης. Όλοι σχεδόν οι κατασκευαστές εξοπλισμού ασύρματης δικτύωσης είναι μέλη του οργανισμού και συμμετέχουν στο πρόγραμμα πιστοποίησης. Το λογότυπο Wi-Fi που φέρουν τα προϊόντα που περνούν την διαδικασία πιστοποίησης, αποτελεί εγγύηση συμβατότητας.

2.4.1 Το πρότυπο IEEE 802.11

Το 1997 το IEEE δημοσίευσε το πρότυπο με τίτλο: "*Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications*". Πρόκειται για ένα λεπτομερές κείμενο 528 σελίδων, το οποίο σε γενικές γραμμές ορίζει τα παρακάτω:

- Την αρχιτεκτονική των ασυρμάτων τοπικών δικτύων
- Διάφορες υπηρεσίες όπως συσχέτιση (association), αυθεντικοποίηση (authentication) και μυστικότητα (privacy)
- Την δομή των πλαισίων (frames)
- Τις λειτουργίες Frequency Hopping Spread Spectrum (FHSS) και Direct Sequence Spread Spectrum (DSSS)
- Τον αλγόριθμο Wired Equivalent Privacy (WEP)

Το πρότυπο ορίζει δύο τύπους φυσικού επιπέδου (PHY): την υπέρυθρη φασματική περιοχή (IR) και την ελεύθερη μπάντα ραδιοσυχνοτήτων στα 2,4 Ghz. Τελικά όμως, για το IR φυσικό επίπεδο δεν έγινε καμία υλοποίηση και έτσι επικράτησε η μπάντα των 2,4 Ghz.

Επίσης ορίζει ρυθμούς μετάδοσης 1 και 2 Mbps και την μέθοδο προσπέλασης μέσου CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), η οποία ερμηνεύεται ως πολλαπλή προσπέλαση με ανίχνευση φορέα και αποφυγή συγκρούσεων. Η χρήση της μεθόδου αυτής, λόγω των μηχανισμών αποφυγής συγκρούσεων, μειώνει τους πραγματικούς ρυθμούς μετάδοσης περίπου στο μισό των ονομαστικών.

2.4.2 Η τροποποίηση IEEE 802.11b

Το 1999 το IEEE δημοσίευσε μια τροποποίηση του αρχικού προτύπου με τίτλο: *"Higher-Speed Physical Layer Extension in the 2.4-Ghz Band"*, η οποία επεκτείνει το αρχικό πρότυπο 802.11, προσθέτοντας τους ρυθμούς μετάδοσης των 5,5 και 11 Mbps στην μπάντα των 2.4 GHz. Η νέα προδιαγραφή υποστηρίζει μόνο την διαμόρφωση DSSS που χρησιμοποιεί τον τύπο διαμόρφωσης Complementary Code Keying (CCK). Επίσης προσθέτει και κάποια νέα χαρακτηριστικά, όπως:

- Δυνατότητα επιλογής μικρότερου προοιμίου (short preamble) των 72 bits στο επίπεδο 2 (OSI) σε αντίθεση με το μεγάλο προοίμιο (long preamble) των 144 bits του αρχικού 802.11. Η δυνατότητα αυτή αποσκοπεί στον ταχύτερο συγχρονισμό των συσκευών. Φυσικά για λόγους συμβατότητας με το αρχικό πρότυπο, ως προεπιλογή χρησιμοποιείται το μεγάλο προοίμιο.
- Δυνατότητα επιλογής καναλιών, σε αντίθεση με την στατική κατανομή καναλιού στο 802.11.

2.4.3 Η τροποποίηση IEEE 802.11a

Επίσης το 1999, το IEEE δημοσίευσε μια τροποποίηση με τίτλο: *"Higher-Speed Physical Layer Extension in the 5 Ghz Band"*, η οποία περιγράφει ένα ασύρματο τοπικό δίκτυο που λειτουργεί στην μπάντα των 5 GHz. Η προδιαγραφή 802.11a χρησιμοποιεί την διαμόρφωση *Orthogonal Frequency Division Multiplexing (OFDM)*, η οποία παρέχει μεγαλύτερους ρυθμούς μετάδοσης έως 54 Mbps έχοντας όμως μικρότερη εμβέλεια. Ένα πλεονέκτημα της χρήσης της μπάντας των 5 GHz είναι η μείωση των προβλημάτων λόγω παρεμβολών, καθώς πρόκειται για μια πιο "καθαρή" μπάντα σε σχέση με τα 2.4 GHz. Ένας λόγος που το πρότυπο αυτό δεν επικράτησε σε σχέση με το 802.11b είναι ότι δεν είναι συμβατό με αυτό.

2.4.4 Η τροποποίηση IEEE 802.11g

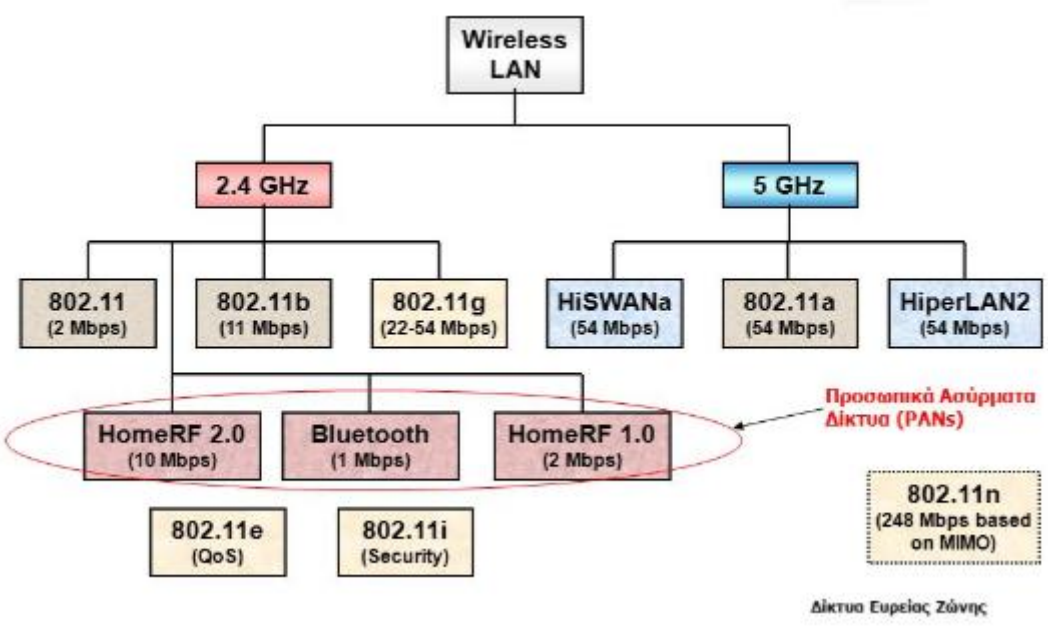
Το 2003 δημοσιεύτηκε μια τροποποίηση με τίτλο: *"Amendment 4: Further Higher Data Rate Extension in the 2.4 Ghz Band"*. Είναι μια επέκταση η οποία προσθέτει ρυθμούς μετάδοσης έως 54 Mbps στην μπάντα των 2.4 GHz χρησιμοποιώντας διαμόρφωση OFDM-DSSS. Το βασικό πλεονέκτημα του 802.11g είναι ότι είναι συμβατό με το 802.11b, οπότε συσκευές 802.11b και 802.11g μπορούν να συνυπάρχουν σε ένα δίκτυο.

2.4.5 Η τροποποίηση IEEE 802.11n

Στις αρχές του 2004, το IEEE ανακοίνωσε ότι σχημάτισε μια νέα ομάδα εργασίας, η οποία ονομάζεται *Task Group n* ή *TGn*. Η ομάδα αυτή ανέλαβε την δημιουργία μιας τροποποίησης του αρχικού προτύπου 802.11, με σκοπό την επίτευξη πραγματικού ρυθμού μεταφοράς τουλάχιστον 100 Mbps. Αυτό σημαίνει ότι ο θεωρητικός ρυθμός μεταφοράς θα πρέπει να είναι τουλάχιστον 200 Mbps. Για να επιτευχθούν τέτοιες ταχύτητες επιβάλλεται η μετάβαση σε νέες τεχνολογίες ασύρματης μετάδοσης και στη συγκεκριμένη περίπτωση, θα χρησιμοποιηθεί η τεχνολογία MIMO (Multiple Input – Multiple Output). Η ονομασία προήλθε από το γεγονός ότι η τεχνολογία αυτή χρησιμοποιεί πολλαπλές κεραίες για την αποστολή και λήψη δεδομένων και οι οποίες λειτουργούν ταυτόχρονα και ανεξάρτητα η κάθε μία. Ήδη έχουν σχηματιστεί "συμμαχίες" κατασκευαστών που έχουν καταθέσει τις προτάσεις τους στο IEEE. Σύμφωνα με τον οργανισμό Wi-Fi (Wi-Fi Alliance) η δημοσίευση της τροποποίησης 802.11n αναμένεται μετά το δεύτερο εξάμηνο του 2006.

2.4.6 Η τροποποίηση IEEE 802.11i

Το 2004 η IEEE δημοσίευσε μια τροποποίηση με τίτλο: *"Amendment 6: Medium Access Control (MAC) Security Enhancements"*, η οποία περιγράφει κάποιες επεκτάσεις στο υποεπίπεδο MAC που αποσκοπούν στην ισχυρότερη ασφάλεια. Περιλαμβάνει πρωτόκολλα όπως τα 802.1X, TKIP, CCMP και άλλα, τα οποία θα αναλυθούν σε επόμενο κεφάλαιο.



Σχήμα 2.3: *Πρότυπα WLAN*

Κεφάλαιο 3

Ασφάλεια στα ασύρματα δίκτυα

3.1 Γενικά

Τα πλεονεκτήματα της χρήσης των ασύρματων δικτύων είναι αναμφίβολα πολλά, με σημαντικότερο την ευελιξία που παρέχουν. Όμως, λόγω του ότι τα δεδομένα που διακινούνται στο δίκτυο μεταδίδονται χρησιμοποιώντας ραδιοσυχνότητες, επιτρέπεται στον οποιονδήποτε να συνδεθεί στο δίκτυο. Αμέσως δημιουργήθηκε η ανάγκη της ασφάλειας του δικτύου, την οποία ήρθαν να καλύψουν οι τεχνικές κρυπτογράφησης. Η εμπιστοσύνη, η ακεραιότητα, η πιστοποίηση και η διαθεσιμότητα της ανταλλασσόμενης πληροφορίας, πλέον οριοθετούνται από τα πρωτόκολλα κρυπτογράφησης, τα οποία βασίζονται σε ήδη γνωστές κρυπτογραφικές μεθόδους, κληρονομώντας έτσι τα όποια μειονεκτήματα και πλεονεκτήματα από άλλες υλοποιήσεις της σύγχρονης επιστήμης της κρυπτογραφίας.

3.2 Κρυπτογράφηση

Κρυπτογράφηση (encryption) είναι ο μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανέναν παρά μόνο από αυτόν που διαθέτει το κατάλληλο κλειδί.

Υπάρχουν δύο οικογένειες αλγόριθμων κρυπτογράφησης:

- Οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι μυστικού κλειδιού)
- Οι ασύμμετροι αλγόριθμοι (ή αλγόριθμοι δημόσιου κλειδιού)

Ο κύριος στόχος της κρυπτογράφησης είναι να παρέχει μηχανισμούς ώστε δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να έχει την ικανότητα να διαβάσει την πληροφορία.

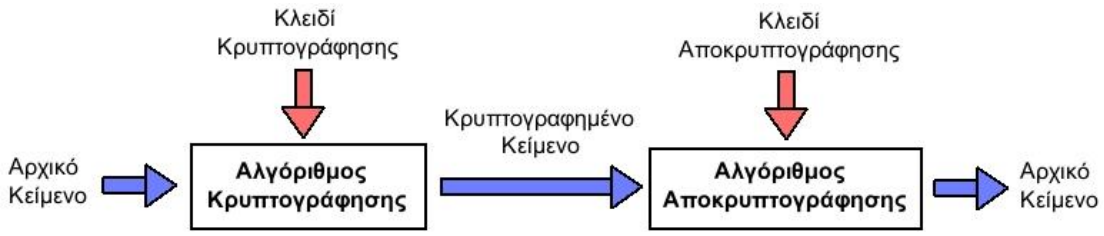
Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες:

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη.

- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- Πιστοποίηση: Οι αποστολείς και οι παραλήπτες μπορούν να εξακριβώνουν τις ταυτότητές τους, καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Βασική ορολογία κρυπτογράφησης:

- Αρχικό κείμενο (plaintext): είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- Κλειδί (key): είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.
- Κρυπτογραφημένο κείμενο (ciphertext): είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.



Σχήμα 3.1: *Διάγραμμα Κρυπτογράφησης*

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου και ενός κλειδιού κρυπτογράφησης. Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης.

3.2.1 Κρυπτογράφηση συμμετρικού κλειδιού

Η κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography) προϋποθέτει την ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση του μηνύματος. Το πρόβλημα που εντοπίζεται στην κρυπτογράφηση συμμετρικού κλειδιού είναι η αδυναμία ανταλλαγής του κλειδιού με ασφαλή τρόπο. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες:

- Αλγόριθμοι ροής: (stream ciphers), οι οποίοι λειτουργούν bit προς bit.
- Μπλοκ αλγόριθμοι: (block ciphers), οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit).

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

3.2.2 Κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρου κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970. Η κρυπτογράφηση των κλειδιών γίνεται με τελείως διαφορετικό τρόπο. Είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Ο αποστολέας και ο παραλήπτης διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες, το ιδιωτικό (private) και το δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να ανακοινώνεται στους παραλήπτες. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού.

3.3 Πρωτόκολλα κρυπτογράφησης ασύρματων δικτύων

Από την έρευνα που πραγματοποιήθηκε σε κεντρικές περιοχές της πόλης των Αθηνών, ακόμη και σήμερα, παρατηρήθηκε ότι είναι αρκετά τα δίκτυα που δεν χρησιμοποιούν κανενός είδους κρυπτογράφηση. Σε αυτά τα ανασφάλιστα δίκτυα είναι προφανές ότι δεν μπορεί να υπάρξει καμία προστασία στους χρήστες που είναι συνδεδεμένοι, στην πληροφορία που ανταλλάσουν, καθώς και στα αποθηκευμένα δεδομένα στο εσωτερικό του δικτύου.

Η κρυπτογράφηση των ασύρματων δικτύων μπορεί να χωριστεί σε δύο βασικές κατηγορίες:

- WEP: Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4, για τον οποίο πλέον υπάρχουν διαδεδομένες τεχνικές εύρεσης του μυστικού κλειδιού.
- Στην οικογένεια WPA/WPA2: Θεωρείται το πιο ασφαλές πρωτόκολλο κρυπτογράφησης. Αντικατέστησε το ανασφαλές WEP και χρησιμοποιεί τον αλγόριθμο CCMP, ο οποίος βασίζεται στον AES.

3.4 Κρυπτογράφηση WEP

Ο τομέας της ασφάλειας των επικοινωνιών θέτει τους ακόλουθους τρεις σημαντικούς στόχους:

- Εμπιστευτικότητα: με τον όρο αυτό περιγράφεται η προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών.
- Ακεραιότητα: η διασφάλιση ότι το στοιχείο δεν έχει τροποποιηθεί.
- Επικύρωση: η υποστήριξη οπουδήποτε μηχανισμού ασφάλειας της αξιοπιστίας των δεδομένων.

Το πρωτόκολλο κρυπτογράφησης WEP παρέχει τις διαδικασίες που βοηθούν στην επιτυχία αυτών των στόχων. Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων στο πρωτόκολλο αυτό εξασφαλίζεται συγχρόνως, χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης RC4 (River Cipher 4), μήκους 64 ή 128 bit. Είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας, ο οποίος δημιουργεί μία ψευδοτυχαία ακολουθία από bit, που συνδυάζεται με το υπό κρυπτογράφηση κείμενο (cipher text) με τη γνωστή συνάρτηση XOR για να παράξει το κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο κείμενο παράγεται χρησιμοποιώντας τα 24 bit του πίνακα αρχικοποίησης (Initialization Vector) και το κλειδί κρυπτογράφησης (pre-shared key) που εισήγαγε ο χρήστης, μήκους 40 ή 104 bit. Το αποτέλεσμα εισάγεται σε μία πύλη XOR μαζί με το αρχικό κείμενο (plain text) ώστε να δημιουργηθεί το τελικό κρυπτογραφημένο κείμενο.

Το πρωτόκολλο WEP χρησιμοποιεί ένα κλειδί μήκους μόνο 40 bit, λόγω περιορισμών που έθεσε η Αμερικάνικη κυβέρνηση, το οποίο ευνοεί τις brute force επιθέσεις. Οι συγκεκριμένες επιθέσεις χρησιμοποιούν όλους τους πιθανούς συνδυασμούς κλειδιών μέχρι να βρεθεί το σωστό, με αποτέλεσμα υπολογιστές με μεγάλη υπολογιστική ισχύ να το σπάσουν πολύ γρήγορα. Όταν οι περιορισμοί κάμφθηκαν, όλοι οι κατασκευαστές προσπάθησαν να το διορθώσουν. Επέκτειναν το μήκος του κλειδιού στα 128 bit χρησιμοποιώντας κλειδί κρυπτογράφησης μήκους 104 bit. Αυτό δεν άλλαξε τον τρόπο επίθεσης, αλλά λόγω της μεγάλης υπολογιστικής ισχύς που χρειάζονταν, καθιστά τις brute force επιθέσεις δυσκολότερες.

Η επικύρωση εξασφαλίζεται μέσω του ελέγχου των πακέτων. Ο αλγόριθμος CRC32 αναπτύχθηκε για να εντοπίζει, να επισημαίνει και πολλές φορές να διορθώνει τα λάθη κατά τη μετάδοση των πακέτων.

3.4.1 Ασφάλεια στο WEP

Η κρυπτογράφηση του πρωτοκόλλου WEP έχει μειωμένα επίπεδα ασφαλείας, γεγονός που το κάνει ιδιαίτερα ευάλωτο σε επιθέσεις. Το μήκος του IV είναι μόλις 24 bit, τα οποία θεωρούνται λίγα για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων. Η τιμή ελέγχου ακεραιότητας (ICV) δεν παρέχει την απαιτούμενη ασφάλεια και δεν αποτρέπει την τροποποίηση των μηνυμάτων από κάποιον εισβολέα.

Επιπλέον, το WEP συνδυάζει το κλειδί της κρυπτογράφησης με το IV, με τέτοιο τρόπο ώστε ο οποιοσδήποτε μπορεί να αποκτήσει το κλειδί της κρυπτογράφησης χρησιμοποιώντας μερικά εκατομμύρια κρυπτογραφημένα πακέτα. Επιπλέον δεν παρέχεται προστασία της ακεραιότητας των διευθύνσεων του αποστολέα και του παραλήπτη.

Οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης (IV), ο οποίος εκπέμπεται συνεχώς μαζί με τα πακέτα. Τη στιγμή που θα επανεκπεμφθεί ο ίδιος πίνακας σε δύο διαφορετικά πακέτα, μπορούμε μέσω της XOR να βρούμε κομμάτια του αρχικού κειμένου. Τμηματικά θα αποκαλυφθεί όλο το μη-κωδικοποιημένο κομμάτι του μηνύματος. Επειδή ο χρόνος εκπομπής του πίνακα αρχικοποίησης δεν είναι ίδιος, έχουν αναπτυχθεί διάφορες τεχνικές για την επιτάχυνση της. Η πιο συνηθισμένη τεχνική είναι ο εξαναγκασμός του σταθμού να εκπέμψει πάλι το πακέτο είτε λόγω απώλειας, είτε απόρριψης, είτε στέλνοντας πακέτα NACK. Με αυτή τη τεχνική, ο σταθμός αναγκάζεται να εκπέμπει συνεχώς, μειώνοντας έτσι ταχύτατα το διαθέσιμο εύρος τιμών του, με αποτέλεσμα σε σύντομο χρονικό διάστημα να επανεκπεμφθεί ο ίδιος πίνακας.

Η ακεραιότητα των δεδομένων δεν είναι καλά προστατευμένη στο WEP, διότι ο αλγόριθμος CRC προστατεύει μόνο από τυχαία λάθη που συμβαίνουν κατά τη μετάδοση. Γι’ αυτό το λόγο τα κρυπτογραφημένα πακέτα μπορούν να αλλοιωθούν ή να υποκλαπούν. Οι εταιρείες αναγκάστηκαν να προβούν σε διορθώσεις του πρωτοκόλλου. Νέες εκδόσεις αναπτύχθηκαν για να εξαλειφθούν τα ελαττώματα του. Η πρώτη αναβάθμιση έγινε με την έκδοση WEP2 η οποία αύξησε το μέγεθος του πίνακα αρχικοποίηση στα 128 bit. Ως αποτέλεσμα, αυξήθηκε ο χρόνος επανεκπομπής του ίδιου πίνακα αρχικοποίησης. Στη συνέχεια ακολούθησαν ακόμα δύο αναβαθμίσεις, το WEPplus (WEP+) και το Dynamic WEP.

3.5 WPA (Wi-Fi Protected Access)

Το 2004 το πρότυπο IEEE με την έκδοση 802.11i ανέπτυξε ένα καινούργιο πρωτόκολλο ασφάλειας για ασύρματη προστατευμένη πρόσβαση, το WPA (Wi-Fi Protected Access). Ουσιαστικά είναι ο αντικαταστάτης του WEP, διότι υπήρχε η ανάγκη στις ασύρματες μεταδόσεις για περισσότερη ασφάλεια. Αποτέλεσε μία ενδιάμεση λύση έως την πλήρη ανάπτυξη της έκδοσης 802.11i με το πρωτόκολλο WPA2. Η WPA κρυπτογράφηση βελτιώνει την WEP και προσθέτει έναν ισχυρό μηχανισμό αυθεντικοποίησης.

Η αυθεντικοποίηση των χρηστών γίνεται με δύο τρόπους λειτουργίας:

- Μέσω της WPA-Personal ή WPA-PSK ο χρήστης συνδέεται σε ένα Access Point και η αυθεντικοποίηση γίνεται μέσω προ-μοιρασμένων κλειδιών (Pre-Shared keys). Επακόλουθο είναι ότι για την καλύτερη ασφάλεια των συνδέσεων παίζει ρόλο το μήκος και η πολυπλοκότητα του κλειδιού.

- Η ασφαλέστερη λειτουργία εκτελείται με την υλοποίηση WPA-Enterprise, η οποία προϋποθέτει την ύπαρξη ενός 802.1x server, μέσω του οποίου ανά τακτά χρονικά διαστήματα, γίνεται ο διαμοιρασμός διαφορετικών κλειδιών για κάθε υπολογιστή, με αποτέλεσμα το σύστημα να είναι πιο ασφαλές, πιο πολύπλοκο και με μεγαλύτερο κόστος.

3.5.1 Ασφάλεια στο WPA

Το WPA χρησιμοποιεί τον RC4 αλγόριθμο, ο οποίος αποτελείται από τον πίνακα αρχικοποίησης μήκους 48 bit και ένα κλειδί χρονικής κρυπτογράφησης μήκους 128 bit. Η ύπαρξη του RC4 και στην καινούργια έκδοση εξασφαλίζει συμβατότητα με τις προηγούμενες εκδόσεις προϊόντων ασύρματης δικτύωσης. Επιπλέον, το WPA εισάγει ένα νέο πρωτόκολλο χρονικής ακεραιότητας κλειδιού, το TKIP (Temporal Key Integrity Protocol), το οποίο αναλαμβάνει δυναμικά την ανανέωση των κλειδιών κατά τη διάρκεια της σύνδεσης. Για να μειωθεί το ποσοστό επανάληψης του ίδιου κλειδιού, χρησιμοποιείται ανά εκπεμπόμενο πακέτο μία ακολουθία αριθμών, το pre-shared key και η εκπεμπόμενη MAC address.

Στο νέο κλειδί που δημιουργείται προστίθεται ο πίνακας αρχικοποίησης και παράγεται μία νέα ακολουθία κλειδιού (keystream). Για την ενίσχυση της ακεραιότητας των πακέτων έχει προστεθεί ένα πεδίο ελέγχου της ακεραιότητας των δεδομένων, το MIC (Message Integration Check). Η τιμή του MIC υπολογίζεται από τον κρυπτογραφικό αλγόριθμο Michael και προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και παραλήπτη. Ένα επιπλέον χαρακτηριστικό είναι ότι υποστηρίζει έναν ειδικό μηχανισμό, ο οποίος ανιχνεύει οποιαδήποτε προσπάθεια παραβίασης του TKIP, με αποτέλεσμα το μπλοκάρισμα της επικοινωνίας.

3.5.2 Αυθεντικοποίηση στο WPA

Η αυθεντικοποίηση στο πρωτόκολλο κρυπτογράφησης WPA-Personal ή WPAPSK έχει σχεδιαστεί για επαγγελματική και οικιακή χρήση. Με αυτή τη μέθοδο η αυθεντικοποίηση των χρηστών γίνεται μέσω του Access Point χρησιμοποιώντας μία φράση 8 έως 63 ASCII χαρακτήρες. Όταν επιλεγούν οι ASCII χαρακτήρες, μία hash function αναλαμβάνει τη μείωση από τα 504 bit (63characters * 8bit) στα 256 bit. Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το 256 bit κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κωδικό ως κλειδί.

3.6 Σύγκριση των πρωτοκόλλων κρυπτογράφησης WEP και WPA

Τα πρωτόκολλα κρυπτογράφησης WPA και WEP χρησιμοποιούν τον αλγόριθμο RC4 για κρυπτογράφηση. Ωστόσο, το WEP χρησιμοποιεί πίνακα αρχικοποίησης μήκους 24 bit με κλειδί κρυπτογράφησης μήκους 40 ή 104 bit, σε αντίθεση με το WPA που χρησιμοποιεί 48 bit IV με 128 bit κλειδί κρυπτογράφησης. Το WEP είναι ανεπαρκές για ασφάλεια, διότι οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης και στις αλλοιώσεις των πακέτων. Στο WPA έχουν ελαχιστοποιηθεί τέτοιου είδους επιθέσεις εξαιτίας του συνδυασμού του πρωτοκόλλου TKIP, του MIC και του μεγαλύτερου μήκους πίνακα αρχικοποίησης. Το κλειδί TKIP χρησιμοποιεί περίπου 300 τρισεκατομμύρια πιθανά κλειδιά για την κρυπτογράφηση του πακέτου. Συνδυάζοντας το με τον 48 bit πίνακα αρχικοποίησης, το TKIP συμβάλλει στην αποτελεσματική ασφάλεια του δικτύου στις επιθέσεις ανάκτησης κλειδιού. Επίσης, το MIC βάζει ένα τέλος στην υποκλοπή πακέτων.

Το WPA-Enterprise και η WPA-PSK κρυπτογράφηση παρέχουν έναν ισχυρό μηχανισμό ασφάλειας, ο οποίος έλειπε από το WEP. Στο WEP η αυθεντικοποίηση του χρήστη γινόταν με τον διαμοιρασμό ενός κοινού κλειδιού. Στο WPA η αυθεντικοποίηση και η κρυπτογράφηση είναι ξεχωριστές λειτουργίες. Η αυθεντικοποίηση στον 802.1x server γίνεται με credentials, και τα κλειδιά διανέμονται αυτόματα.

3.7 WPA2 (Wi-Fi Protected Access Version 2)

Το πρωτόκολλο κρυπτογράφησης WPA2 είναι ο διάδοχος του WPA. Αποτελεί μέρος του προτύπου 802.11i. Η κρυπτογράφηση γίνεται με τον αλγόριθμο CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), ο οποίος για την ανάπτυξή του βασίστηκε στο CCM (Counter Mode with CBC-MAC) του αλγορίθμου AES (Advanced Encryption Standard), για την προστασία της ιδιωτικότητας. Με την είσοδο του νέου αλγορίθμου αντικαταστάθηκε ο RC4. Όπως το TKIP, έτσι και ο CCMP χρησιμοποιεί πίνακα αρχικοποίησης 48 bit, αλλά αντί για την ακολουθία αριθμών ανά πακέτο χρησιμοποιεί AES κλειδιά για την προστασία της εμπιστευτικότητας και ακεραιότητας του πακέτου. Χρησιμοποιεί πίνακα αρχικοποίησης 48 bit με 128 bit κλειδί κρυπτογράφησης το οποίο ελαχιστοποιεί την ευπάθεια του συστήματος σε επαναλαμβανόμενες επιθέσεις. Η ενισχυμένη προστασία που παρέχει το CCMP σε σύγκριση με το TKIP απαιτεί μεγαλύτερη επεξεργαστική ισχύ, και συχνά χρειάζεται νέο ή αναβαθμισμένο hardware.

Κεφάλαιο 4

Συστήματα άμυνας και ανίχνευσης επιθέσεων

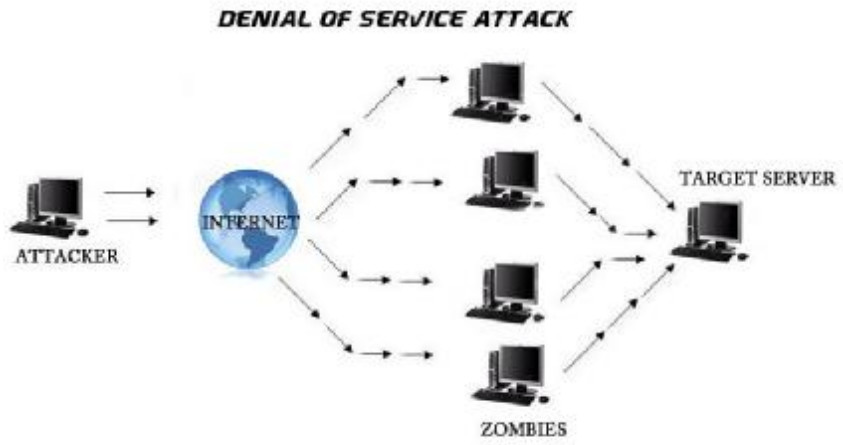
4.1 Γενικά

Τι γίνεται όμως όταν ένα σύστημα δεχτεί επίθεση και πως μπορούμε να την αποτρέψουμε? Σε αυτό το κεφάλαιο θα γίνει παρουσίαση των επιθέσεων DoS και DDoS, θα ταξινομηθούν και αναλυθούν τρόποι με τους οποίους μπορούν αυτές να ανιχνευθούν και να προληφθούν.

4.2 Επιθέσεις Dos

Επιθέσεις άρνησης εξυπηρέτησης (Denial of Service, DoS) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.

Υπάρχουν γενικά δύο μορφές αυτής της επίθεσης. Η μία είναι η επίθεση κατά την οποία η υπηρεσία αναγκάζεται να καταρρεύσει και πρέπει να επανεκκινηθεί. Η άλλη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει αυτούς που πραγματικά θέλουν την υπηρεσία. Οι επιθέσεις Denial of Service (DoS) αποτελούν αδιαμφισβήτητα ένα πολύ σοβαρό πρόβλημα για το Διαδίκτυο.



Σχήμα 4.1: *DoS Attack*

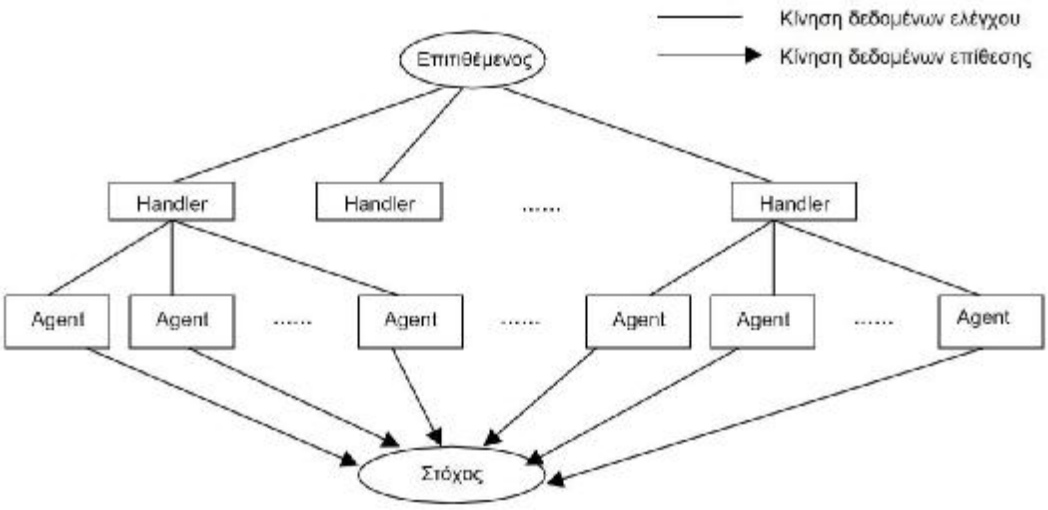
Οι πιο συνηθισμένοι τύποι Denial Of Service επιθέσεων είναι :

- Οι επιθέσεις που εκμεταλλεύονται **αδυναμίες του πρωτοκόλλου TCP/IP**.
- Οι επιθέσεις που εκμεταλλεύονται **αδυναμίες του IPv4**.
- Οι επιθέσεις που προσπαθούν να **εξαντλήσουν όλους τους πόρους** (resources) - μνήμη, CPU, Bandwidth - **του συστήματος στόχου** με αποτέλεσμα την διακοπή της λειτουργίας του.

4.3 Επιθέσεις DDoS

Η κατανεμημένη επίθεση DoS (DDoS - Distributed Denial of Service), είναι μια σχετικά απλή, αλλά ταυτόχρονα πολύ ισχυρή τεχνική που προσβάλλει διαδικτυακούς πόρους. Η επίθεση DDoS αποτελεί μια πολυδιάστατη επίθεση DoS, εντείνοντας το πρόβλημα των DoS και καθιστώντας την πρόληψη και αντιμετώπισή τους πιο δύσκολη.

Οι DDoS επιθέσεις χαρακτηρίζονται από τη ροή πακέτων προερχόμενων από διάφορες πηγές. Αυτές οι επιθέσεις δεσμεύουν τη δύναμη ενός τεράστιου αριθμού συντονισμένων τερματικών του Διαδικτύου για να καταναλώσουν κάποιους κρίσιμους πόρους στο στόχο και να εμποδίσουν την εξυπηρέτηση των κανονικών πελατών. Η συμφόρηση είναι συνήθως τόσο συγκεντρωμένη που καθιστά δύσκολη τη διαλογή των πακέτων επιθέσεων από τα κανονικά πακέτα. Επιπλέον η κλίμακα της επίθεσης μπορεί να είναι μεγαλύτερη από αυτή που το σύστημα μπορεί να διαχειριστεί. Αν δεν έχουν ληφθεί τα απαραίτητα μέτρα, το σύστημα που θα δεχθεί μια τέτοια επίθεση, μπορεί να έχει δυσάρεστες επιπτώσεις, από ξαφνικό τερματισμό και αλλοίωση δεδομένων μέχρι και μερική ή ολική αδυναμία εξυπηρέτησης των πελατών.



Σχήμα 4.2: *Αρχιτεκτονική DDoS επιθέσεων*

Οι επιθέσεις DDoS εκμεταλλεύονται βασικά την αρχιτεκτονική του Διαδικτύου και αυτό είναι που τις κάνει πολύ ισχυρές. Το Διαδίκτυο σχεδιάστηκε με γνώμονα κυρίως τη λειτουργικότητα και όχι την ασφάλεια. Η σχεδίαση του προκαλεί αρκετά κενά ασφάλειας, τα οποία μπορούν να αξιοποιηθούν για επιθέσεις από κακόβουλους χρήστες. Πιο αναλυτικά:

- *Η ασφάλεια του Διαδικτύου* είναι σε μεγάλο βαθμό αλληλοεξαρτώμενη. Ανεξαρτήτως του πόσο ασφαλές μπορεί να είναι ένα σύστημα, το αν θα αποτελέσει θύμα μιας επίθεσης DDoS εξαρτάται από το υπόλοιπο Διαδίκτυο.

- *Οι διαδικτυακοί πόροι* είναι περιορισμένοι. Κανένα διαδικτυακό σύστημα δεν έχει απεριόριστους πόρους. Οι πόροι αυτοί αργά ή γρήγορα μπορεί να καταναλωθούν από έναν ικανό αριθμό χρηστών.

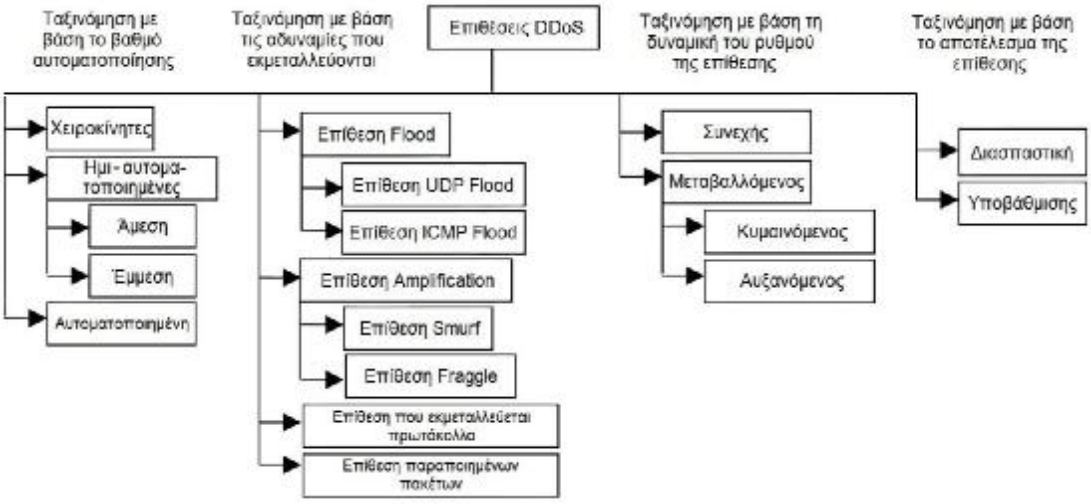
- *Πολλοί εναντίον λίγων*. Αν οι πόροι των επιτιθέμενων είναι περισσότεροι από αυτούς των θυμάτων τους, τότε η επιτυχία της επίθεσης είναι σχεδόν βέβαιη.

- *Οι πληροφορίες και οι πόροι* δεν είναι αλληλένδετα. Οι περισσότερες πληροφορίες που χρειάζονται οι υπηρεσίες βρίσκονται σε τερματικά συστήματα. Παράλληλα για να έχουμε μέγιστη διεκπεραιωτική ικανότητα (throughput), σχεδιάζονται δίαυλοι υψηλού εύρους ζώνης στο ενδιάμεσο δίκτυο. Έτσι οι επιτιθέμενοι μπορούν να εκμεταλλευθούν τους άφθονους πόρους ενός ανυποψίαστου δικτύου για να πλημμυρίσουν το θύμα με μηνύματα.

Παρακάτω γίνεται μια προσπάθεια ανάλυσης της δομής του πεδίου των επιθέσεων DDoS, παρουσιάζοντας τις συνήθεις τεχνικές που χρησιμοποιούνται και ταξινομώντας τους τύπους επιθέσεων DDoS, αλλά και τους αμυντικούς μηχανισμούς που επωμίζονται την αντιμετώπισή τους.

4.3.1 Ταξινόμηση των επιθέσεων DDoS

Για να γίνουν κατανοητές οι επιθέσεις DDoS, κρίνεται απαραίτητη η ύπαρξη κάποιας πρότυπης ταξινόμησης. Η ταξινόμηση αυτή φαίνεται στο Σχήμα 2.3 και αποτελείται από δυο μέρη. Στο πρώτο μέρος οι επιθέσεις ταξινομούνται με βάση το βαθμό αυτοματοποίησης, τις αδυναμίες που εκμεταλλεύονται, το ρυθμό της επίθεσης και το αποτέλεσμά της. Στο δεύτερο μέρος αναγνωρίζονται συγκεκριμένα χαρακτηριστικά κάθε κατηγορίας του πρώτου μέρους.



Σχήμα 4.3: *Ταξινόμηση επιθέσεων DDoS*

4.4 Προβλήματα άμυνας σε επιθέσεις DDoS και ταξινόμηση

Οι επιθέσεις DDoS είναι ένα πρόβλημα δύσκολο να επιλυθεί. Καταρχήν δεν υπάρχουν κοινά χαρακτηριστικά των επιθέσεων DDoS που να μπορούν να χρησιμοποιηθούν για την αναγνώρισή τους. Επιπλέον, η κατανεμημένη φύση των επιθέσεων DDoS δυσκολεύει την καταπολέμηση και την ανίχνευσή τους. Άλλωστε τα αυτοματοποιημένα εργαλεία που πραγματοποιούν την επίθεση DDoS, μπορούν εύκολα να βρεθούν στο Διαδίκτυο. Οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιήσουν παραπλανητικές διευθύνσεις IP για να αποκρύψουν την πραγματική τους ταυτότητα, και αυτό κάνει την ιχνηλάτηση των επιθέσεων DDoS ακόμα πιο δύσκολη. Τέλος, δεν υπάρχει επαρκές επίπεδο ασφάλειας σε όλα τα συστήματα που είναι συνδεδεμένα στο Διαδίκτυο, καθώς υπάρχουν διατηρούμενα κενά ασφαλείας στους εξυπηρετητές του Διαδικτύου.

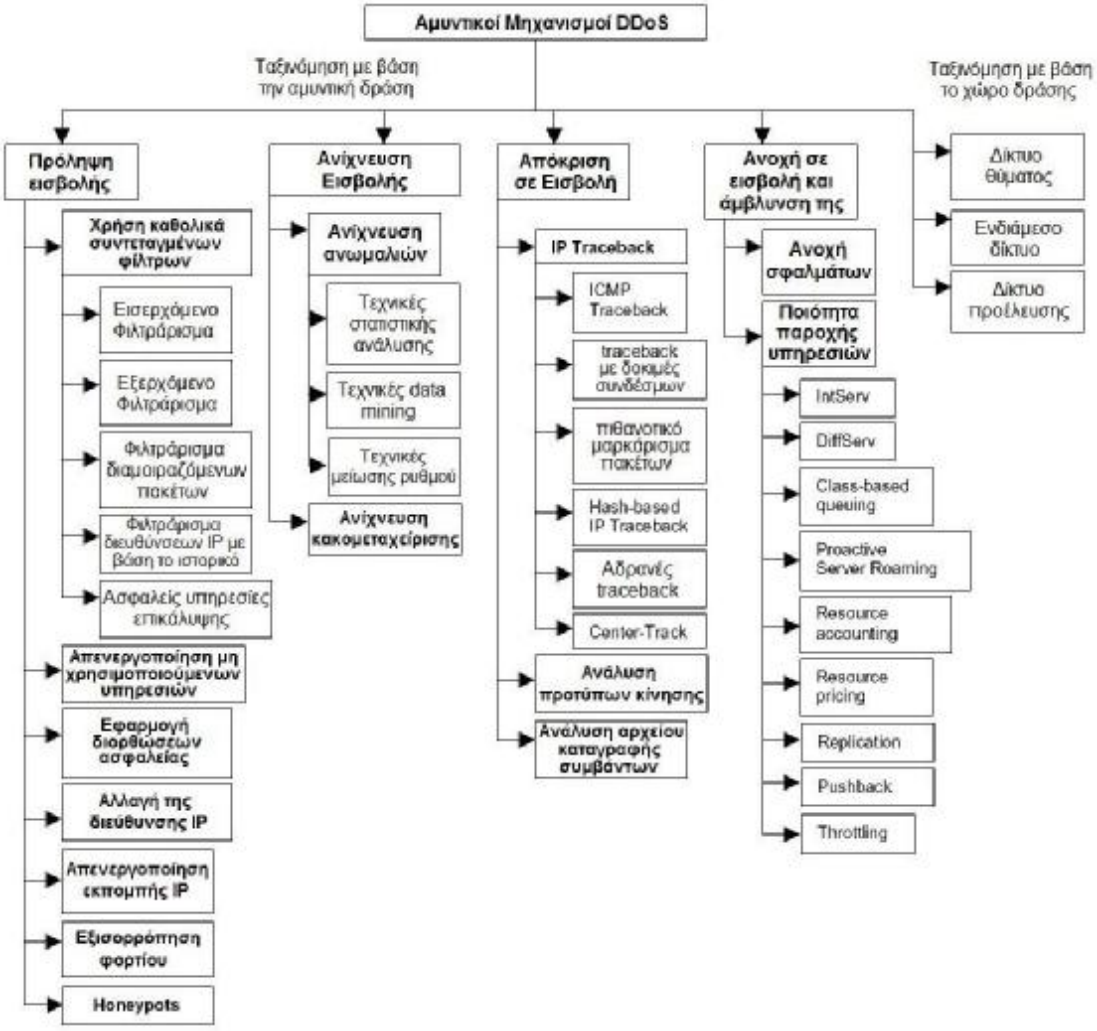
Οι μηχανισμοί άμυνας στις DDoS επιθέσεις μπορούν να κατηγοριοποιηθούν χρησιμοποιώντας δυο διαφορετικά κριτήρια. Η πρώτη κατηγοριοποίηση ταξινομεί τους αμυντικούς μηχανισμούς των DDoS επιθέσεων σύμφωνα με τη δράση που επιτελούν.

Έτσι προκύπτουν οι ακόλουθες τέσσερις κατηγορίες:

- Πρόληψη επίθεσης
- Αναγνώριση επίθεσης
- Ανεκτικότητα και άμβλυνση επίθεσης
- Απόκριση στην επίθεση

Η δεύτερη κατηγοριοποίηση διαχωρίζει τις επιθέσεις DDoS ανάλογα με τον τόπο εκδήλωσης, καταλήγοντας στις τρεις κατηγορίες αμυντικών μηχανισμών που ακολουθούν:

- Δίκτυο του θύματος
- Ενδιάμεσο δίκτυο
- Δίκτυο πηγής



Σχήμα 4.4: *Ταξινόμηση των μηχανισμών άμυνας DDoS*

4.4.1 Ταξινόμηση με βάση την αμυντική δράση

4.4.1.1. Πρόληψη επίθεσης

Η καλύτερη στρατηγική προστασίας για κάθε επίθεση είναι να αποτραπεί πλήρως η επίθεση. Στο στάδιο αυτό γίνεται προσπάθεια να αποτραπεί η εξαπόλυση επιθέσεων DDoS από την αρχή. Υπάρχουν πολλοί αμυντικοί μηχανισμοί DDoS που αποτρέπουν την εκδήλωση επιθέσεων σε συστήματα:

Α) Χρησιμοποιώντας καθολικά συντεταγμένα φίλτρα, τα πακέτα επιθέσεων μπορούν να εμποδιστούν, πριν συγκεντρωθούν σε επικίνδυνες ποσότητες. Οι μηχανισμοί φιλτραρίσματος μπορούν να διαχωριστούν στις παρακάτω κατηγορίες:

- **Το εισερχόμενο φιλτράρισμα** είναι μια προσέγγιση στην οποία ένας δρομολογητής ρυθμίζεται έτσι ώστε να μην επιτρέπει στα εισερχόμενα πακέτα με μη επιτρεπτές διευθύνσεις πηγής να εισέρχονται στο δίκτυο. Είναι ένας μηχανισμός περιορισμού για να αποκόπτει την κίνηση με διεύθυνση IP που δεν συμφωνεί με το πρόθεμα domain που έχει συνδεθεί στο δρομολογητή. Ο μηχανισμός αυτός μπορεί δραστικά να ελαττώσει την επίθεση DoS με απόκρυψη IP αν όλα τα domain τη χρησιμοποιούν. Κάποιες φορές μπορεί να αποκοπεί και κανονική κίνηση από το εισερχόμενο φιλτράρισμα, σε περίπτωση που χρησιμοποιείται φορητή IP για να συνδεθεί ένας φορητός κόμβος σε ένα εξωτερικό δίκτυο.
- **Το εξερχόμενο φιλτράρισμα** είναι ένα εξωτερικό φίλτρο, που διασφαλίζει ότι μόνο πακέτα με εκχωρημένες διευθύνσεις IP μπορούν να εξέρχονται από το δίκτυο. Τα φίλτρα εξερχόμενης κίνησης δεν συμβάλλουν στη μείωση της κατανάλωσης πόρων του δικτυακού τόπου στον οποίο δημιουργείται το πακέτο, αλλά βοηθά στην προστασία άλλων δικτυακών τόπων από πιθανή επίθεση. Εκτός από τη θέση που βρίσκονται, τα φίλτρα εισερχόμενης και εξερχόμενης κίνησης παρουσιάζουν παρόμοια συμπεριφορά.
- **Το φιλτράρισμα διαμοιραζόμενων πακέτων** που βασίζεται στη δρομολόγηση τους είναι μια προσέγγιση ικανή να φιλτράρει ένα μεγάλο μέρος πακέτων με παραπλανητική διεύθυνση IP και να αποτρέψει τα πακέτα επίθεσης να φτάσουν στους στόχους τους, καθώς επίσης και να βοηθήσει στην ιχνηλάτηση της ύποπτης IP. Τα φίλτρα που βασίζονται στη δρομολόγηση χρησιμοποιούν τις πληροφορίες δρομολόγησης για να φιλτράρουν τα πακέτα με παραπλανητικές διευθύνσεις IP, και αυτή είναι η βασική διαφορά τους από το εισερχόμενο φιλτράρισμα. Αν τα φίλτρα που βασίζονται στη δρομολόγηση

είναι τμηματικά τοποθετημένα, είναι εφικτό ένα συνδυαστικό αποτέλεσμα φιλτραρίσματος, έτσι ώστε η ροή παραπλανητικών διευθύνσεων IP να μην φτάνει σε άλλα Αυτόνομα Συστήματα. Επιπλέον, εφόσον η δρομολόγηση στο Διαδίκτυο αλλάζει με την πάροδο του χρόνου είναι μια σπουδαία πρόκληση για τα φίλτρα που βασίζονται στη δρομολόγηση, να ενημερώνονται σε πραγματικό χρόνο. Το μεγαλύτερο μειονέκτημα αυτής της προσέγγισης είναι ότι προϋποθέτει καθολική επίγνωση της τοπολογίας δικτύου, οδηγώντας σε προβλήματα όταν αυτή είναι μεγάλης κλίμακας.

- **Το φιλτράρισμα διευθύνσεων IP που βασίζεται στο ιστορικό** (HIP) είναι άλλος ένας μηχανισμός φιλτραρίσματος με στόχο να αποτραπούν επιθέσεις τύπου DDoS. Σύμφωνα με αυτή την προσέγγιση ο ακραίος δρομολογητής επιτρέπει την είσοδο εισερχόμενων πακέτων σύμφωνα με μια προεγκατεστημένη βάση δεδομένων με IP διευθύνσεις. Η βάση δεδομένων με IP διευθύνσεις βασίζεται στο ιστορικό προηγούμενων συνδέσεων του ακραίου δρομολογητή. Το πλάνο αυτό είναι σθεναρό, δεν χρειάζεται τη συνεργασία ολόκληρης της διαδικτυακής κοινότητας, είναι εφαρμόσιμο σε ένα ευρύ σύνολο ειδών κίνησης και απαιτεί ελάχιστες ρυθμίσεις παραμέτρων. Από την άλλη, αν ήταν γνωστό στους επιτιθέμενους ότι το φίλτρο πακέτων IP βασίζεται σε ιστορικό προηγούμενων συνδέσεων, θα μπορούσαν να παραποιήσουν τον εξυπηρετητή ώστε να συμπεριληφθεί στην βάση δεδομένων με IP διευθύνσεις. Αυτό είναι δυνατόν να αποτραπεί αυξάνοντας το χρονικό διάστημα, στο οποίο πρέπει να εμφανίζονται οι διευθύνσεις IP, ώστε να θεωρούνται συχνές.
- **Οι ασφαλείς υπηρεσίες επικάλυψης** (SOS) είναι μια αρχιτεκτονική στην οποία μόνο τα πακέτα που προέρχονται από έναν περιορισμένο αριθμό κόμβων, που καλούνται servlets, θεωρούνται κανονική κίνηση πελατών. Η κίνηση αυτή μπορεί να φτάσει στα servlets με δρομολόγηση που βασίζεται στον κατακερματισμό εντός ενός δικτύου επικάλυψης. Όλες οι υπόλοιπες αιτήσεις φιλτράρονται από το δίκτυο επικάλυψης. Για να αποκτήσει κάποιος πελάτης πρόσβαση στο δίκτυο επικάλυψης, πρέπει να πιστοποιηθεί σε κάποιο από τα αναπαραγόμενα σημεία πρόσβασης (SOAPs). Το SOS είναι ένα κατανεμημένο σύστημα που προσφέρει εξαιρετική προστασία στον καθορισμένο στόχο με το κόστος της μετατροπής των συστημάτων των πελατών, και για αυτό δεν είναι κατάλληλο για την προστασία δημοσίων εξυπηρετητών.

Β) Η απενεργοποίηση των μη χρησιμοποιούμενων υπηρεσιών είναι άλλη μια προσέγγιση για να αποτραπούν οι επιθέσεις DDoS. Αν οι υπηρεσίες UDP echo ή δημιουργίας χαρακτήρων δεν είναι απαραίτητες, μπορούν να απενεργοποιηθούν. Αυτό βοηθάει στην άμυνα απέναντι σε επιθέσεις που στοχεύουν σε αυτά. Γενικά, αν κάποιες υπηρεσίες δικτύου δεν χρειάζονται ή δεν χρησιμοποιούνται, οι υπηρεσίες αυτές θα πρέπει να απενεργοποιούνται για την αποτροπή επιθέσεων.

Γ) Η εφαρμογή διορθώσεων ασφαλείας, μπορεί να θωρακίσει τους εξυπηρετητές απέναντι στις επιθέσεις DDoS. Οι εξυπηρετητές θα πρέπει να αναβαθμίζονται με τις τελευταίες διορθώσεις ασφαλείας για τα υπάρχοντα σφάλματα και να χρησιμοποιούν τις τελευταίες διαθέσιμες μεθόδους για να περιορίσουν τις συνέπειες των επιθέσεων DDoS.

Δ) Η αλλαγή της διεύθυνσης IP, είναι άλλη μια απλή λύση σε μια επίθεση DDoS με σκοπό να ακυρώσει τη διεύθυνση IP του υπολογιστή του θύματος αλλάζοντάς την με μια νέα. Αυτή η άμυνα ονομάζεται άμυνα κινούμενου στόχου. Όταν η αλλαγή της διεύθυνσης IP ολοκληρωθεί όλοι οι διαδικτυακοί δρομολογητές θα είναι ενημερωμένοι, και οι ακραίοι δρομολογητές θα απορρίπτουν τα πακέτα επιθέσεων. Ενώ αυτή η πράξη αφήνει εκτεθειμένο το σύστημα, αφού ο επιτιθέμενος μπορεί να εξαπολύσει επίθεση στη νέα διεύθυνση IP, είναι μια πρακτική επιλογή για επιθέσεις DDoS τοπικού χαρακτήρα που βασίζονται στις διευθύνσεις IP. Από την άλλη, οι επιτιθέμενοι μπορούν να καταστήσουν την τεχνική αυτή μια μάταια διαδικασία προσθέτοντας στα εργαλεία επιθέσεων DDoS μια λειτουργία ιχνηλάτησης υπηρεσιών domain name.

Ε) Απενεργοποιώντας την εκπομπή IP, τα συστήματα εξυπηρετητών δεν μπορούν πλέον να χρησιμοποιηθούν ως ενισχυτές επιθέσεων ICMP Flood και Smurf. Όμως, η άμυνα σε μια τέτοια επίθεση θα είναι επιτυχημένη, μόνο όταν όλα τα γειτονικά δίκτυα απενεργοποιήσουν την εκπομπή IP.

ΣΤ) Η εξισορρόπηση φορτίου είναι μια απλή προσέγγιση που επιτρέπει στους δικτυακούς παρόχους να αυξήσουν το παρεχόμενο εύρος ζώνης σε κρίσιμες συνδέσεις και να αποτρέψουν το ενδεχόμενο κατάρρευσής τους σε ενδεχόμενη επίθεση. Μια πρόσθετη προστασία για να εξασφαλιστούν οι εξυπηρετητές μπορεί να είναι και η αναπαραγωγή τους σε περίπτωση που κάποιοι από αυτούς καταρρεύσουν κατά τη διάρκεια μιας επίθεσης DDoS. Επιπλέον, σε μια αρχιτεκτονική με πολλαπλούς εξυπηρετητές η εξισορρόπηση φορτίου είναι απαραίτητη ώστε να επιτευχθεί τόσο η βελτιστοποίηση της κανονικής απόδοσης, όσο και η αποτροπή ή άμβλυνση των συνεπειών μιας επίθεσης DDoS.

Ζ) Τα honeypots μπορούν επίσης να χρησιμοποιηθούν για να αποτρέψουν επιθέσεις τύπου DDoS. Τα honeypots είναι συστήματα που έχουν αναπτυχθεί με περιορισμένη ασφάλεια και μπορούν να χρησιμοποιηθούν για να ξεγελάσουν τον επιτιθέμενο ώστε να επιτεθεί στο honeypot και όχι στο πραγματικό σύστημα. Τα honeypots τυπικά έχουν αξία όχι μόνο στην προστασία συστημάτων, αλλά μπορούν επίσης να

χρησιμοποιηθούν για να συλλέξουν πληροφορίες σχετικά με τους επιτιθέμενους αποθηκεύοντας μια εγγραφή της δραστηριότητάς τους και μαθαίνοντας τι τύπου επιθέσεις και εργαλεία επίθεσης χρησιμοποιούν. Στην τρέχουσα ερευνητική δραστηριότητα συζητείται η χρήση honeypots, που μιμούνται όλα τα χαρακτηριστικά ενός κανονικού δικτύου (όπως οι εξυπηρετητές δικτύου, εξυπηρετητές ταχυδρομείου, πελάτες, κτλ.), με σκοπό να προσελκύσουν δυνητικούς επιτιθέμενους DDoS. Η βασική ιδέα είναι να παρασύρουν τον επιτιθέμενο να πιστέψει ότι έχει κατακτήσει το σύστημα (δηλ. honeypot) για επίθεση ως slave και να τον προσελκύσουν να εγκαταστήσει είτε κώδικα handler είτε κώδικα agent μέσα στο honeypot. Αυτό αποτρέπει την κατάκτηση κάποιων κανονικών συστημάτων, παρακολουθεί τη συμπεριφορά του handler ή agent και επιτρέπει στο σύστημα να κατανοήσει καλύτερα πως να προφυλαχθεί από μελλοντικές επιθέσεις DDoS. Όμως, αυτό το πλάνο έχει διάφορα μειονεκτήματα. Πρώτον, αυτή η μέθοδος υποθέτει ότι η επίθεση μπορεί να ανιχνευθεί χρησιμοποιώντας εργαλεία που βασίζονται στην ταυτοποίηση χαρακτηριστικών. Αν αυτό δε συμβαίνει, το πακέτο προωθείται στον προορισμό του σε λειτουργικά δίκτυα. Επιπλέον, ο επιτιθέμενος μπορεί εύκολα να ανατρέψει τη φύση της προσέγγισης του honeypot από τη στιγμή που η προσέγγιση είναι στατική και παθητική με την έννοια ότι δεν είναι ένα δυναμικά ελισσόμενο σχέδιο με ολοκληρωμένη κάλυψη.

Οι προσεγγίσεις πρόληψης προσφέρουν αυξημένη ασφάλεια αλλά ποτέ δεν θα μπορέσουν να εξαφανίσουν πλήρως την απειλή των επιθέσεων DDoS, επειδή θα είναι διαρκώς ευάλωτες σε νέες επιθέσεις, για τις οποίες δεν θα υπάρχουν χαρακτηριστικά και διορθώσεις στη βάση δεδομένων.

4.4.1.2. Ανίχνευση Εισβολής - Επίθεσης

Η ανίχνευση επίθεσης αποτελεί ένα πολύ ενεργό πεδίο έρευνας. Πραγματοποιώντας ανίχνευση επίθεσης, ένας εξυπηρετητής και ένα δίκτυο μπορούν να προστατευτούν απέναντι στο ενδεχόμενο να γίνουν η πηγή μιας επίθεσης δικτύου, ή το θύμα μιας επίθεσης DDoS. Τα συστήματα ανίχνευσης επίθεσης ανιχνεύουν επιθέσεις DDoS, είτε χρησιμοποιώντας μια βάση δεδομένων με γνωστά χαρακτηριστικά, είτε διαπιστώνοντας ανωμαλίες στη συμπεριφορά των συστημάτων.

Η ***ανίχνευση ανωμαλιών*** βασίζεται στην ανίχνευση συμπεριφορών που είναι αφύσικες σε σχέση με κάποιο φυσιολογικό πρότυπο. Πολλά συστήματα και προσεγγίσεις ανίχνευσης ανωμαλιών έχουν αναπτυχθεί για να ανιχνεύσουν τα δυσδιάκριτα σημάδια εκδήλωσης μιας επιθέσεων DDoS.

Α) Ένα κλιμακωτό σύστημα παρακολούθησης δικτύου που καλείται NOMAD σχεδιάστηκε από τον Talpade. Το σύστημα αυτό είναι ικανό να ανιχνεύσει ανωμαλίες του δικτύου κάνοντας στατιστική ανάλυση των πληροφοριών κεφαλίδας των IP πακέτων. Μπορεί να χρησιμοποιηθεί για να ανιχνεύσει τις ανωμαλίες στην κίνηση ενός τοπικού δικτύου και δεν υποστηρίζει κάποια μέθοδο δημιουργίας του ταξινομητή για την άθροιση κίνησης υψηλού εύρους ζώνης από κατανεμημένες πηγές.

Β) Μια άλλη μέθοδος ανίχνευσης επιθέσεων DDoS χρησιμοποιεί τα δεδομένα δρομολογητών Βάσης Διαχείρισης Πληροφορίας (MIB). Τα δεδομένα MIB ενός δρομολογητή περιέχουν παραμέτρους που δείχνουν διαφορετικά στατιστικά πακέτων και δρομολόγησης. Ο Cabrera επικεντρώθηκε στην αναγνώριση στατιστικών προτύπων σε διαφορετικές παραμέτρους, με σκοπό την έγκαιρη αναγνώριση επιθέσεων DDoS. Φαίνεται πολλά υποσχόμενη για πιθανή καταγραφή στατιστικών ανωμαλιών πακέτων ICMP, UDP και TCP σε συγκεκριμένες επιθέσεις DDoS. Ενώ η προσέγγιση αυτή μπορεί να είναι αποτελεσματική για ελεγχόμενα φορτία κίνησης, χρειάζεται να αξιολογηθεί περαιτέρω σε ένα πραγματικό περιβάλλον δικτύου. Αυτό το πεδίο έρευνας θα μπορούσε να παρέχει σημαντικές πληροφορίες και μεθόδους που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση και το φιλτράρισμα επιθέσεων DDoS.

Γ) Ένας μηχανισμός που καλείται δειγματοληψία και φιλτράρισμα πακέτων προκαλούμενη από συμφόρηση προτάθηκε από τους Huang και Pullen. Σύμφωνα με αυτή την προσέγγιση, ένα υποσύνολο απορριφθέντων πακέτων λόγω συμφόρησης επιλέγεται για στατιστική ανάλυση. Αν εξακριβωθεί κάποια ανωμαλία στα στατιστικά αποτελέσματα, αποστέλλεται ένα σήμα στον δρομολογητή για να φιλτράρει τα κακόβουλα πακέτα.

Δ) Οι Lee και Stolfo χρησιμοποιούν τεχνικές εξόρυξης για να ανακαλύψουν πρότυπα χαρακτηριστικών του συστήματος, που περιγράφουν τη συμπεριφορά προγραμμάτων και χρηστών και υπολογίζουν έναν ταξινομητή που μπορεί να αναγνωρίζει τις ανωμαλίες και τις επιθέσεις. Η προσέγγιση αυτή επικεντρώνεται στην αναγνώριση επίθεσης που βασίζεται στον εξυπηρετητή. Μια βελτίωση αυτής της προσέγγισης είναι ένα μοντέλο μετα-ανίχνευσης, που κάνει χρήση αποτελεσμάτων από πολλαπλά μοντέλα για να παρέχει ακριβέστερη αναγνώριση.

Ε) Η Mirkovic πρότεινε ένα σύστημα που ονομάζεται D-WARD, το οποίο κάνει αναγνώριση επιθέσεων DDoS στην πηγή, βασιζόμενοι στην ιδέα ότι οι επιθέσεις DDoS θα πρέπει να αναχαιτίζονται όσο το δυνατόν πιο κοντά στην πηγή. Το D-WARD εγκαθίσταται στους ακραίους δρομολογητές ενός δικτύου και παρακολουθεί την κίνηση που στέλνεται από και προς τους εξυπηρετητές στο εσωτερικό του. Αν

γίνει αντιληπτή κάποια ασυμμετρία στους ρυθμούς δημιουργίας πακέτων από κάποιον εσωτερικό εξυπηρετητή, το D-WARD περιορίζει το ρυθμό πακέτων. Το μειονέκτημα αυτής της προσέγγισης είναι ότι υπάρχει η πιθανότητα να γίνουν πολλές λανθασμένες εκτιμήσεις, καθώς ανιχνεύονται καταστάσεις DDoS κοντά στην πηγή, εξαιτίας της ασυμμετρίας που μπορεί να υπάρξει στο ρυθμό ροής των πακέτων για μια μικρή διάρκεια. Επιπλέον, κάποιες κανονικές ροές πακέτων, όπως στο UDP πραγματικού χρόνου, παρουσιάζουν ασυμμετρία.

ΣΤ) Οι Gil και Poletto πρότειναν μια ευριστική δομή δεδομένων (MULTOPS), που αποφαίνεται αν είναι δυνατή η ανίχνευση διευθύνσεων IP που συμμετέχουν σε μια επίθεση DDoS, έπειτα λαμβάνονται μέτρα για να εμποδιστούν μόνο οι συγκεκριμένες διευθύνσεις. Κάθε συσκευή δικτύου διατηρεί ένα δέντρο πολλαπλών επιπέδων που περιέχει στατιστικά ρυθμών ροής πακέτων για προθέματα υποδικτύων σε διαφορετικά επίπεδα συνάθροισης. Η δομή MULTOPS χρησιμοποιεί δυσανάλογους ρυθμούς από και προς τους εξυπηρετητές και τα υποδίκτυα ώστε να ανιχνεύσει επιθέσεις. Όταν αποθηκεύει τα στατιστικά στοιχεία που βασίζονται στις διευθύνσεις προέλευσης, λέγεται ότι είναι σε λειτουργία προσανατολισμένη στην επίθεση, αλλιώς σε λειτουργία προσανατολισμένη στο θύμα. Για αυτόν τον λόγο μια δομή δεδομένων MULTOPS μπορεί να χρησιμοποιηθεί είτε για να παρακολουθεί εξυπηρετητές που επιτίθενται, είτε για να παρακολουθεί εξυπηρετητές που δέχονται επίθεση. Όταν ο ρυθμός ροής πακέτων από και προς ένα υποδίκτυο φτάσει ένα συγκεκριμένο όριο, δημιουργείται ένας νέος υποκόμβος για να παρακολουθεί εκτενέστερα ρυθμούς ροής πακέτων. Η διαδικασία αυτή μπορεί να συνεχιστεί μέχρι να διατηρηθούν ρυθμοί ροής πακέτων ανά διεύθυνση IP. Έτσι, ξεκινώντας από ένα θολό τοπίο, κάποιος μπορεί με αυξανόμενη ακρίβεια να ανιχνεύσει την ακριβή πηγή της επίθεσης ή τις διευθύνσεις προορισμού. Οι IP διευθύνσεις πηγής που λαμβάνονται είναι πιθανότατα παραπλανητικές, όμως μπορεί να αποδειχτούν χρήσιμες στην επιβολή περιορισμών στον ρυθμό ροής. Ένα από τα μειονεκτήματα της προσέγγισης αυτής είναι ότι απαιτεί νέα ρύθμιση του δρομολογητή και νέες μεθόδους διαχείρισης μνήμης. Επιπλέον, δεν μπορεί να αποτρέψει συμμετρικές επιθέσεις, ούτε να αναγνωρίσει τυχαία παραποιημένες διευθύνσεις IP προερχόμενες από ένα μοναδικό σύστημα ή επιθέσεις DDoS που χρησιμοποιούν πολλά συστήματα zombie.

Η ***ανίχνευση κακομεταχείρισης*** αναγνωρίζει ορισμένα πρότυπα γνωστών απειλών και έπειτα αναζητά την εμφάνιση τέτοιων προτύπων. Κάποια πρότυπα επιθέσεων μπορεί να είναι οποιαδήποτε χαρακτηριστικά, καταστάσεις, διαρθρώσεις πακέτων και αλληλεπιδράσεις μεταξύ γεγονότων που οδηγούν σε κάποιο ρήγμα ή κάποια άλλη κακομεταχείριση. Αυτά τα πρότυπα ορίζονται ως '*υπογραφές*' επιθέσεων. Διάφορα δημοφιλή συστήματα παρακολούθησης δικτύων πραγματοποιούν αναγνώριση βάσει υπογραφής, όπως τα NetRanger της CISCO, NID, SecureNet PRO, RealSecure, NFR-NID και Snort.

4.4.1.3. Απόκριση σε εισβολή

Όταν αναγνωριστεί μια επίθεση, η άμεση αντίδραση είναι να προσδιοριστεί η πηγή της επίθεσης και να φραγεί ανάλογα η κίνηση της. Το έργο της φραγής συνήθως επιτελείται με χειροκίνητο έλεγχο (πχ. με επικοινωνία με τους διαχειριστές των δρομολογητών και ενεργοποιώντας λίστες ελέγχου πρόσβασης), καθώς ένα αυτοματοποιημένο σύστημα απόκρισης μπορεί να προκαλέσει περεταίρω υποβάθμιση της ποιότητας υπηρεσιών, αν γίνει απόκριση σε ένα λανθασμένο συναγερμό. Αυτοματοποιημένα συστήματα απόκρισης επιθέσεων υπάρχουν, αλλά ενεργοποιούνται μόνο μετά από μια περίοδο μάθησης (για αυτά που χρησιμοποιούν νευρωνικούς υπολογιστές για να ανιχνεύσουν την κίνηση DDoS) ή δοκιμών (για αυτά που λειτουργούν με σταθερούς κανόνες). Προς βελτίωση του προσδιορισμού της πηγής επιθέσεων, διάφορες τεχνικές μπορούν να επισπεύσουν την σύλληψη των επιτιθέμενων και να αποτρέψουν άλλες απόπειρες επιθέσεων. Υπάρχουν πολλές προσεγγίσεις που στοχεύουν στην ιχνηλάτηση και αναγνώριση των πραγματικών πηγών επιθέσεων.

Η διαδικασία ***IP traceback*** ακολουθεί τα ίχνη των επιθέσεων προς τα πίσω, δηλαδή προς την προέλευσή τους, έτσι ώστε κάποιος να εξιχνιάσει την πραγματική ταυτότητα του επιτιθέμενου και να επιτύχει την ανίχνευση ασύμμετρων διαδρομών, καθώς επίσης και χαρακτηρισμό μονοπατιών. Κάποιοι παράγοντες που καθιστούν δύσκολη τη διαδικασία IP traceback είναι η ακατάστατη φύση της δρομολόγησης στο Διαδίκτυο και η έλλειψη υπευθυνότητας σχετικά με την πηγή στο πρωτόκολλο TCP/IP. Για αποδοτικό IP traceback είναι απαραίτητος ο υπολογισμός και η ανακατασκευή της διαδρομής της επίθεσης. Είναι επίσης απαραίτητο να υπάρχει χαμηλή επιβάρυνση στη δρομολόγηση. Επιπλέον απαιτείται ένας μεγάλος αριθμός πακέτων για να ανακατασκευαστεί το μονοπάτι της επίθεσης. Σημαντικά επίσης είναι η σθεναρότητα ενάντια σε πολλαπλές επιθέσεις, η μείωση της προστασίας ιδιωτικότητας στην επικοινωνία IP, η βηματική ανάπτυξη και η ανάστροφη συμβατότητα. Σε ένα πρώιμο επίπεδο, μπορεί κανείς να το φανταστεί σαν μια διαδικασία κατά την οποία ο διαχειριστής του συστήματος που βρίσκεται υπό επίθεση καλεί τον παροχέα υπηρεσιών Διαδικτύου του (ISP) και τον ρωτά για την προέλευση των πακέτων που δέχεται. Από τη στιγμή που η χειροκίνητη ιχνηλάτηση είναι μια πολύ κουραστική διαδικασία έχουν γίνει διάφορες προτάσεις στο πρόσφατο παρελθόν για να αυτοματοποιηθεί.

Η διαδικασία ***ICMP traceback*** προτάθηκε από τον Bellovin. Σύμφωνα με τον μηχανισμό αυτό κάθε δρομολογητής πραγματοποιεί δειγματοληψία των προωθούμενων πακέτων με χαμηλή πιθανότητα (1 στα 20.000) και στέλνει ένα μήνυμα ICMP traceback στον προορισμό. Αν συγκεντρωθούν αρκετά μηνύματα ιχνηλάτησης στο θύμα, η πηγή της κίνησης μπορεί να βρεθεί κατασκευάζοντας μια αλυσίδα μηνυμάτων ιχνηλάτησης. Μια σημαντική παράμετρος αυτής της προσέγγισης είναι η επικύρωση των πακέτων ιχνηλάτησης. Παρά το γεγονός ότι η απαίτηση PKI αποτρέπει τους επιτιθέμενους να δημιουργήσουν ψεύτικα μηνύματα ICMP traceback, είναι δύσκολο κάθε δρομολογητής να ενσωματώνει μεθόδους που βασίζονται σε πιστοποίηση. Ακόμα, η κίνηση ICMP δημιουργεί πρόσθετη κίνηση και απαιτείται ένας χάρτης δρομολόγησης για να ανασκευαστεί το μονοπάτι μιας επίθεσης, αφού οι διευθύνσεις IP των δρομολογητών κωδικοποιούνται μέσα στο μήνυμα ICMP traceback. Μια εναλλακτική λύση, η οποία εισάγει ένα bit πρόθεση στο διάγραμμα δρομολόγησης και προώθησης, καλείται ICMP traceback οδηγούμενο εκ προθέσεως.

Για να αντιμετωπιστούν οι επιθέσεις DDoS από αναμεταδότες, ο Barros πρότεινε μια τροποποίηση στα μηνύματα ICMP traceback. Στην προσέγγιση αυτή, οι δρομολογητές στέλνουν μηνύματα ICMP στην πηγή του πακέτου που βρίσκεται υπό επεξεργασία και όχι στον προορισμό του. Αυτή η αντίστροφη ιχνηλάτηση δίνει τη δυνατότητα στο θύμα να αναγνωρίσει τους επιτιθέμενους agents από τα πακέτα αυτά.

Η τεχνική ***traceback με δοκιμές συνδέσμων*** προτάθηκε από τους Burch και Cheswick. Στη μέθοδο αυτή, το θύμα ελέγχει κάθε έναν από τους εισερχόμενους συνδέσμους του σαν σύνδεσμο πιθανής εισαγωγής κίνησης DDoS. Εξάγει συμπεράσματα για το μονοπάτι της επίθεσης πλημμυρίζοντας τους συνδέσμους με μεγάλες ριπές κίνησης και παρατηρεί αν αυτό προκαλεί κάποια διαταραχή στο δίκτυο. Αν παρατηρηθεί κάτι τέτοιο, ο σύνδεσμος αυτός είναι πιθανότατα μέρος ενός μονοπατιού επίθεσης. Η μέθοδος αυτή απαιτεί πολύ καλή γνώση της τοπολογίας του δικτύου, ικανότητα δημιουργίας μεγάλων ποσοτήτων κίνησης σε οποιονδήποτε σύνδεσμο και δεν μπορεί να αντιμετωπίσει πολλαπλούς επιτιθέμενους. Μπορεί επίσης να ειπωθεί, ότι είναι δύσκολο για το θύμα να έχει την ικανότητα δημιουργίας πακέτων που θα πλημμυρίσουν τους συνδέσμους καθώς θα δέχεται μια επίθεση DDoS. Κάποιοι λένε ακόμα ότι η ελεγχόμενη πλημμύρα διάφορων συνδέσμων μπορεί να αποτελεί και η ίδια, μια επίθεση DoS. Οι μηχανισμοί δοκιμών συνδέσμων λειτουργούν καλύτερα όταν υπάρχει μια μοναδική πηγή επίθεσης και έχουν άσχημα αποτελέσματα όταν υπάρχει επίθεση DDoS.

Το ***πιθανοτικό μαρκάρισμα πακέτων*** **(PPM)** προτάθηκε αρχικά από τον Savage, ο οποίος περιέγραψε αποδοτικούς τρόπους κωδικοποίησης τμηματικών πληροφοριών μονοπατιού δρομολόγησης και ενσωμάτωσης δεδομένων ιχνηλάτησης προς τα πίσω σε πακέτα IP. Είναι μια προσέγγιση η οποία μπορεί να εφαρμοστεί κατά τη διάρκεια μιας επίθεσης ή μετά από αυτή και δεν προϋποθέτει επιπλέον κίνηση στο δίκτυο, αποθηκευτικό χώρο στον δρομολογητή ή αύξηση μεγέθους του πακέτου. Ενώ δεν είναι αδύνατη η ανακατασκευή ενός διατεταγμένου μονοπατιού δικτύου χρησιμοποιώντας ένα ακατάστατο σύνολο από δείγματα του δρομολογητή, απαιτείται από το θύμα να λάβει ένα μεγάλο όγκο πακέτων. Το πλεονέκτημα της προσέγγισης αυτής είναι ότι δεν δημιουργείται επιπλέον κίνηση, αφού οι επιπλέον πληροφορίες είναι συνδεδεμένες στα πακέτα. Ακόμα, δεν υπάρχει αλληλεπίδραση με τους ISP και ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί για να ιχνηλατηθούν επιθέσεις αφού έχει ολοκληρωθεί μια επίθεση.

Από την άλλη μεριά, υπάρχει μια ασυμβατότητα προς τα πίσω καθώς το μαρκάρισμα IP στο πεδίο ID έρχεται σε διένεξη με το IPsec στο οποίο η επικεφαλίδα ταυτοποίησης αποκρύπτει την επικεφαλίδα αναγνώρισης. Επιπλέον το πιθανοτικό μαρκάρισμα πεδίου ID απαιτεί κάποιες μετατροπές στις συσκευές δρομολόγησης στο Διαδίκτυο ώστε να δημιουργούν άμεσα τέτοια σημάδια. Η ανακατασκευή ενός μονοπατιού επίθεσης από το θύμα δημιουργεί μεγάλο υπολογιστικό φορτίο. Οι Ioannidis και Bellovin υποστηρίζουν ότι ακόμα και αν το μονοπάτι της επίθεσης αναγνωριστεί, δεν είναι ξεκάθαρο ποια θα πρέπει να είναι τα επόμενα βήματα.

Οι Song και Perrig βελτίωσαν την απόδοση της μεθόδου PPM και πρότειναν τη χρήση αλυσίδων κατακερματισμού για την ταυτοποίηση δρομολογητών. Χρησιμοποιούν ένα πεδίο με μήκος 5 bit, αλλά δεν τεμαχίζουν τα μηνύματα των δρομολογητών. Αυτός ο τρόπος μαρκαρίσματος είναι αποδοτικός και ακριβής όταν λαμβάνουν χώρα πολλές επιθέσεις DDoS και χρησιμοποιείται ένας έξυπνος τρόπος κωδικοποίησης ώστε να μειωθούν οι απαιτήσεις σε αποθηκευτικό χώρο. Από την άλλη, ο μηχανισμός αυτός υποθέτει ότι το θύμα έχει έναν χάρτη των δρομολογητών προς όλους τους επιτιθέμενους.

Ο Dean εισήγαγε μια ενδιαφέρουσα αλγεβρική προσέγγιση στη μέθοδο PPM. Η προσέγγιση αυτή δεν προϋποθέτει έναν χάρτη δρομολογητών για να ανασκευαστεί ένα μονοπάτι επίθεσης. Όμως όπως το σύστημα που προτάθηκε από τον Savage, η μέθοδος αυτή έχει παρόμοια προβλήματα συμβατότητας προς τα πίσω και είναι λιγότερο αποδοτική όταν υφίστανται πολλαπλοί επιτιθέμενοι.

Μαζί με τους παραπάνω αλγορίθμους μαρκαρίσματος, οι Adler και Parker και Lee εξετάζουν κάποιους συμβιβασμούς για διάφορες παραμέτρους στην PPM. Οι Park και Lee προτείνουν την εφαρμογή των κατανεμημένων φίλτρων στους δρομολογητές και τα πακέτα να φιλτράρονται σύμφωνα με την τοπολογία του δικτύου. Το πλάνο αυτό μπορεί να σταματήσει την παραποιημένη κίνηση σε ένα πρόωρο στάδιο. Για να είναι όμως αποτελεσματικό, υπάρχει η απαίτηση για γνώση της τοπολογίας του

δικτύου και της πολιτικής δρομολόγησης ανάμεσα σε αυτόνομα συστήματα, πράγμα το οποίο είναι δύσκολο να επιτευχθεί στο συνεχώς αναπτυσσόμενο Διαδίκτυο.

Μια νέα τεχνική μαρκαρίσματος πακέτων και σχεδιασμού agent προτάθηκε από τους Tupukala και Varadharajan για αναγνώριση της εγγύτερης πηγής (κοντινότερου δρομολογητή) της επίθεσης με ένα μοναδικό πακέτο, ακόμα και σε περίπτωση επιθέσεων με παραποιημένες διευθύνσεις πηγής. Η προσέγγισή τους είναι ένα μοντέλο agent-ελεγκτή ο οποίος κινητοποιείται μόνο κατά τη διάρκεια επιθέσεων και έχει τη δυνατότητα όχι μόνο επεξεργάζεται την κίνηση του θύματος ξεχωριστά, χωρίς να παρεμβαίνει στην φυσιολογική κίνηση, αλλά και να δημιουργεί διαφορετικές υπογραφές για διαφορετικές πηγές επιθέσεων. Το σύστημα αυτό μπορεί να αποτρέψει την κακόβουλη κίνηση στον πλησιέστερο δρομολογητή, έχει γρήγορη απόκριση, υλοποιείται απλά και μπορεί να αναπτυχθεί αυξητικά. Δυστυχώς σε αυτή την προσέγγιση, η πρόληψη περιορίζεται εντός του domain ενός μοναδικού ISP και η αποδοτικότητα μειώνεται καθώς η υποδομή του ISP αναπτύσσεται.

Ο Wang πρότεινε ένα πλαίσιο για ‘αδρανές traceback’ (δηλ. το σημάδεμα και η ιχνηλάτηση των πακέτων προς την διεύθυνση IP της πηγής του επιτιθέμενου γίνεται μόνο αν το υποσύστημα ανίχνευσης επιθέσεων διαπιστώσει ότι πραγματοποιείται μια επίθεση). Το σύστημα αυτό διαφέρει αρκετά από όσα έχουν ως τώρα αναφερθεί. Χρησιμοποιεί την δυνατότητα προγραμματισμού των ενεργών κόμβων, ώστε να παρέχει έλεγχο επί της διαδικασίας απόκρισης σε επίθεση. Οι κόμβοι ενός ενεργού δικτύου επικοινωνούν μεταξύ τους με τη χρήση ειδικά σχεδιασμένων πακέτων, τα οποία λέγονται ‘κάψουλες’ που εμπεριέχουν κώδικα. Ο κώδικας αυτός θα εισάγει αποτελεσματικά μια νέα υπηρεσία (ή θα τροποποιήσει μια υπάρχουσα) στον κόμβο που θα το επεξεργαστεί. Καθώς μια επίθεση βρίσκεται σε εξέλιξη, οι ενεργοί κόμβοι θα ανταλλάξουν πληροφορίες και θα επαναπρογραμματίσουν τα δικτυακά τους στοιχεία, έτσι ώστε να εξουδετερώσουν την DDoS κίνηση όσο πιο κοντά στην πηγή.

Τα ενεργά δίκτυα έχουν χρησιμοποιηθεί και σε άλλες προσεγγίσεις με σκοπό την άμυνα των δικτύων απέναντι στις επιθέσεις DDoS.

Το **AEGIS** είναι άλλος ένας μηχανισμός ο οποίος βασίζεται στα ενεργά δίκτυα. Η τεχνολογία ενεργοποίησης του πυρήνα σε αυτό πλαίσιο είναι το ενεργό δίκτυο, το οποίο ενσωματώνει δυνατότητα προγραμματισμού σε ενδιάμεσους δικτυακούς κόμβους και επιτρέπει στους τελικούς χρήστες να προσαρμόζουν τον τρόπο που οι δικτυακοί κόμβοι διαχειρίζονται τα δεδομένα.

Το ***CenterTrack*** είναι μια αρχιτεκτονική που προτάθηκε από τον Stone, η οποία δημιουργεί ένα δίκτυο επικάλυψης από IP tunnel συνδέοντας όλους τους ακραίους δρομολογητές σε κεντρικούς δρομολογητές παρακολούθησης, και όλη η ύποπτη κίνηση διοχετεύεται από τους ακραίους δρομολογητές στους δρομολογητές παρακολούθησης. Όταν ανιχνευτεί μια επίθεση DoS, οι δρομολογητές που

βρίσκονται στην άκρη του δικτύου, έχουν την εντολή να δρομολογούν ξανά τα πακέτα που έχουν ως διεύθυνση αποστολής τον στόχο της επίθεσης. Οι δρομολογητές παρακολούθησης μπορούν έπειτα να αναγνωρίσουν τα σημεία εισόδου της ροής της κίνησης με την οποία γίνεται η επίθεση. Οι ακραίοι δρομολογητές δεν είναι υποχρεωμένοι να υποστηρίζουν εντοπισμό σφαλμάτων στην είσοδο. Από την άλλη, υπάρχει μεγάλο κόστος σε αποθηκευτικό χώρο και υπολογιστική ισχύ εξαιτίας της απαίτησης από τους ακραίους δρομολογητές να καταγράφουν πακέτα, ώστε να αναγνωρίσουν την κίνηση της επίθεσης.

Η ***ανάλυση προτύπων κίνησης*** είναι άλλη μια μέθοδος απόκρισης στις επιθέσεις DDoS. Κατά τη διάρκεια μιας επίθεσης DDoS, μπορούν να αποθηκευτούν δεδομένα που αφορούν πρότυπα κίνησης και μετά από την επίθεση να αναλυθούν, ώστε να βρεθούν συγκεκριμένα χαρακτηριστικά και γνωρίσματα που μπορεί να υποδεικνύουν μια επίθεση. Τα αποτελέσματα της ανάλυσης των δεδομένων αυτών μπορούν να χρησιμοποιηθούν για να ανανεωθούν η εξισορρόπηση του φορτίου και οι ρυθμιστικές τεχνικές καθώς και για να αναπτυχθούν νέοι μηχανισμοί φιλτραρίσματος, ώστε να αποτραπούν επιθέσεις DDoS.

Η ***ανάλυση του αρχείου καταγραφής συμβάντων*** είναι άλλη μια καλή τακτική που στοχεύει στην απόκριση σε επιθέσεις DDoS. Η επιλογή εγγραφών συμβάντων που έγιναν κατά τη διάρκεια της εκκίνησης και εκτέλεσης της επίθεσης μπορούν να χρησιμοποιηθούν για να βρεθεί ο τύπος της επίθεσης DDoS που έγινε και για να γίνει ανάλυση των στοιχείων. Εργαλεία του δικτύου όπως τα firewall, οι sniffer πακέτων, τα αρχεία καταγραφής του εξυπηρετητή και τα honeypot μπορούν να χρησιμοποιηθούν για την επιλογή των αρχείων καταγραφής συμβάντων.

4.4.1.4. Ανοχή σε επίθεση και άμβλυνση της επίθεσης

Η έρευνα στην ανοχή των επιθέσεων έχει δείξει ότι είναι αδύνατον να αποτραπεί ή να εμποδιστεί εντελώς μια επίθεση DDoS και επικεντρώνεται στην ελαχιστοποίηση των επιπτώσεων της επίθεσης και στην διασφάλιση της ποιότητας των υπηρεσιών. Η ανοχή σε επιθέσεις μπορεί να χωριστεί σε δυο μέρη: στην ανοχή σφαλμάτων και στην ποιότητα των υπηρεσιών (QoS).

- Η ***ανοχή σφαλμάτων*** είναι μια καλά ανεπτυγμένη περιοχή έρευνας, της οποίας οι σχεδιασμοί είναι ενσωματωμένοι στις πιο κρίσιμες δομές και εφαρμόζονται σε τρία επίπεδα: υλικού, λογισμικού και συστήματος. Η ιδέα της ανοχής σφαλμάτων είναι ότι αναπαράγοντας τις υπηρεσίες του δικτύου και διευρύνοντας το φάσμα των σημείων πρόσβασης, το δίκτυο μπορεί να συνεχίσει να προσφέρει τις υπηρεσίες του όταν η κακόβουλη κίνηση προκαλέσει συμφόρηση σε έναν δικτυακό κόμβο.

- Η ***ποιότητα παροχής υπηρεσιών*** **(QoS)** περιγράφει την εξασφάλιση της ικανότητας ενός δικτύου να παρέχει τα προβλεπόμενα αποτελέσματα για διάφορους τύπους εφαρμογών ή κίνησης. Πολλές τεχνικές και συστήματα QoS που είναι ανθεκτικά σε επιθέσεις αναπτύχθηκαν με σκοπό να αμβλύνουν τα αποτελέσματα επιθέσεων DDoS.

Ανάμεσα στις τεχνικές QoS που είναι ανθεκτικές σε επιθέσεις, οι Integrated Services (IntServ) και Differentiated Services (DiffServ) επικράτησαν ως οι κύριες αρχιτεκτονικές. Η IntServ χρησιμοποιεί ένα πρωτόκολλο διατήρησης πόρων (RSVP) για να ρυθμίσει την δέσμευση των πόρων κατά τη διαδρομή που θα περάσει μια συγκεκριμένη ροή κίνησης. Η DiffServ είναι μια αρχιτεκτονική διάκρισης που κάνει χρήση του byte είδους υπηρεσίας (Type of service, TOS) στην κεφαλίδα IP και δεσμεύει πόρους σύμφωνα με το TOS κάθε πακέτου.

Οι τεχνικές ουράς χρησιμοποιούνται και αυτές εκτενώς για την αντιμετώπιση των επιθέσεων DDoS. Υπάρχουν πολλές μέθοδοι ουρών. Η παλαιότερη και πιο ευρέως χρησιμοποιούμενη μέθοδος ουράς, είναι το class-based queuing (CBQ). Το CBQ ή διαμόρφωση κίνησης σχηματίζει διαφορετικές ουρές κίνησης για διαφορετικούς τύπους πακέτων και για πακέτα με διαφορετικό TOS. Έπειτα, για τις ουρές αυτές, μπορεί να δεσμευτεί μια συγκεκριμένη ποσότητα εξερχόμενου εύρους ζώνης. Το CBQ δείχνει να διατηρεί αποδεκτό QoS κατά τη διάρκεια επιθέσεων σε συστοιχία από εξυπηρετητές δικτύου.

Μια αρχιτεκτονική που βασίζεται στην προσφορά των μηχανισμών QoS σε ενδιάμεσους δρομολογητές είναι η VIPnet που προτάθηκε από τον Brustoloni. Στη VIPnet η κανονική κίνηση υποτίθεται ότι είναι η κίνηση που έρχεται από δίκτυα που ενσωματώνουν την υπηρεσία VIPnet. Όλη η υπόλοιπη κίνηση θεωρείται χαμηλής προτεραιότητας και μπορεί να διακοπεί σε περίπτωση επίθεσης.

Μια παρόμοια προσέγγιση με αυτή της VIPnet υιοθετήθηκε από τον Khattab και προτείνει μια διαδικασία που ονομάζεται προκαταβολική περιπλάνηση εξυπηρετητή με σκοπό να αμβλυνθούν επιθέσεις DoS. Σύμφωνα με την προσέγγιση αυτή ο ενεργός εξυπηρετητής προκαταβολικά αλλάζει την τοποθεσία του σε ένα σύνολο εξυπηρετητών για να αμυνθεί απέναντι σε απρόβλεπτες και μη ανιχνεύσιμες επιθέσεις. Μόνο οι κανονικοί πελάτες μπορούν να ανιχνεύσουν τον κινούμενο εξυπηρετητή. Αυτό το σχέδιο περιπλάνησης δημιουργεί ασήμαντο φορτίο σε περιπτώσεις που δεν έχουμε επίθεση και παρέχει καλό χρόνο απόκρισης σε περιπτώσεις επίθεσης.

Χρησιμοποιώντας τις τεχνικές που εφαρμόζονται στην ρύθμιση της ποιότητας των υπηρεσιών (QoS) οι Garg και Reddy πρότειναν μια αμυντική τακτική απέναντι στις επιθέσεις DDoS ρυθμίζοντας την κατανάλωση των πόρων που ανήκει στην κατηγορία υπολογισμού των πόρων. Συνιστούν ότι η ρύθμιση των πόρων μπορεί να γίνει στο

επίπεδο ροών, όπου κάθε ροή λαμβάνει ένα δίκαιο μέρος των πόρων, περίπου όπως γίνεται με τη μέθοδο χρονομερισμού round robin στις CPU. Υπάρχει όμως ακόμα η πιθανότητα να γίνει μια επίθεση άρνησης υπηρεσιών έχοντας έναν μεγάλο αριθμό από εξυπηρετητές να συνδέονται στον εξυπηρετητή, καθένας από τους οποίους απαιτεί το δικό του μέρος πόρων, προκαλώντας έτσι εξάντληση των πόρων, όπως περίπου γίνεται στο πολύ γνωστό πρόβλημα του δείπνου των φιλοσόφων. Η βασική τους ιδέα ήταν να επεκτείνουν τον έλεγχο των πόρων στο υποσύστημα του δικτύου. Χώρισαν την δικτυακή κίνηση σε κλάσεις και η κατηγοριοποίηση γίνεται με βάση την πιθανή κατανάλωσή τους σε πόρους. Άλλοι τέτοιοι μηχανισμοί για ρύθμιση της κίνησης είναι τα firewalling, Ack pacing κτλ.

Στην ίδια κατηγορία του *υπολογισμού των πόρων* συγκαταλέγεται μια προσέγγιση που λέγεται *δημιουργία συμφόρησης στον πελάτη*. Αυτός ο τρόπος αντιμετώπισης προσπαθεί να δημιουργήσει μια διαδικασία συμφόρησης στους υπολογιστές agent και να περιορίσει τη δυνατότητα επίθεσής τους. Οι αλγόριθμοι Client Puzzles της RSA και τα τεστ Turing απαιτούν από τον πελάτη να κάνει κάποιον επιπλέον υπολογισμό ή να απαντήσει σε μια ερώτηση πριν εγκαθιδρυθεί μια σύνδεση. Αυτό κάνει τους χρήστες συστημάτων zombie να παρατηρούν μια υποβάθμιση της απόδοσης, και έτσι ίσως να διακόψουν τη συμμετοχή τους στην αποστολή κίνησης επίθεσης DDoS. Οι Juels και Brainard προτείνουν έναν μηχανισμό εκτίμησης, όπου ο πελάτης πρέπει να λύσει έναν γρίφο με διαφορετική πολυπλοκότητα πριν ο εξυπηρετητής δεσμεύσει πόρους για τα αιτήματά του και αρχίσει να τον εξυπηρετεί. Οι γρίφοι στους πελάτες επιτρέπουν ‘αποδεκτή υποβάθμιση των υπηρεσιών’. Όταν πραγματοποιείται μια επίθεση ο εξυπηρετητής μπορεί να αυξήσει τη δυσκολία των γρίφων που δέχεται ο πελάτης και πρέπει να λύσει πριν ο εξυπηρετητής δεσμεύσει κάποιους από τους πόρους του.

Η *εκτίμηση των πόρων* είναι άλλη μια προσέγγιση που προτάθηκε από τον Mankins με σκοπό να αμβλύνει τα αποτελέσματα επιθέσεων DDoS. Ο Mankins παρατήρησε ότι οι επιθέσεις DDoS έχουν αποτέλεσμα επειδή το κόστος βαρύνει κατά μεγαλύτερο μέρος τον εξυπηρετητή, και κατά τη διάρκεια μιας επίθεσης, η κακόβουλη κίνηση είναι ουσιαστικά αδύνατον να διαχωριστεί από την κανονική κίνηση. Προτείνουν μια αρχιτεκτονική κατανεμημένων πυλών και ένα πρωτόκολλο αμοιβής που επιβάλλει δυναμικά μεταβαλλόμενες τιμές στο δίκτυο, τον εξυπηρετητή και στις πληροφορίες πόρων, με σκοπό να ωθήσει κάποιο από το κόστος έναρξης των υπηρεσιών πίσω στους πελάτες που έχουν αιτήματα. Χρησιμοποιώντας διαφορετικές λειτουργίες αμοιβών και απόκτησης, η αρχιτεκτονική αυτή μπορεί να παρέχει διαφοροποίηση στην ποιότητα των υπηρεσιών και επιπλέον να επιλέγει πελάτες με καλή συμπεριφορά. Αναγνωρίζουν την εφαρμογή ενός μηχανισμού, προτεραιότητας στους επιθυμητούς πελάτες ως κλειδί και τιμωρούν τους πελάτες που δημιουργούν φορτίο στον εξυπηρετητή. Το μειονέκτημα της προσέγγισης αυτής είναι ότι ένας κακόβουλος χρήστης μπορεί να φορτώσει το σύστημα με ψευδή αιτήματα χαμηλού κόστους, ανεβάζοντας μάλιστα έτσι το κόστος για τους κανονικούς χρήστες. Η

προτροπή του Mankins για να λυθεί αυτό, είναι ο διαχωρισμός των πόρων σε κλάσεις και η χρήση διαφορετικών συναρτήσεων κοστολόγησης για κάθε κλάση.

Προτάθηκαν διάφορες αυτόνομες αρχιτεκτονικές που επιδεικνύουν ανεκτικότητα κατά τη διάρκεια επίθεσης κατανάλωσης εύρους ζώνης DDoS. Το XenoService είναι μια δομή ενός κατανεμημένου δικτύου από εξυπηρετητές που ανταποκρίνονται σε μια επίθεση σε οποιονδήποτε ιστότοπο, αναπαράγοντάς τον ιστότοπο ακαριαία και ευρέως στους εξυπηρετητές XenoService, επιτρέποντας έτσι στον ιστότοπο που δέχεται επίθεση να έχει μεγαλύτερη συνδεσιμότητα δικτύου, για να απορροφήσει μια πλημμύρα από πακέτα. Ενώ μια τέτοια δομή μπορεί να εξασφαλίσει το QoS κατά τη διάρκεια επιθέσεων DDoS, είναι απίθανο ένας μεγάλος αριθμός από ISP να υιοθετήσει μια τέτοια δομή γρήγορα.

Η *αρχιτεκτονική* ***pushback*** είναι μια υποσχόμενη τεχνική άμβλυνσης και η ιδέα είναι να ενημερώνονται οι δρομολογητές ώστε να περιορίζουν το ρυθμό ή να απορρίπτουν συγκεκριμένη κίνηση που αναγνωρίζεται ως ανεπαρκής (αθροιστικά). Στον έλεγχο συμφόρησης που βασίζεται στην άθροιση (ACC) μια συνάθροιση ορίζεται ως ένα υποσύνολο της κίνησης με μια αναγνωρίσιμη ιδιότητα. Σύμφωνα με τους Ioannidis και Bellovin, ένα pushback daemon διευκρινίζει αν υπάρχει κάποια ένδειξη επίθεσης τρέχοντας έναν αλγόριθμο αναγνώρισης. Η βηματική εφαρμογή αυτής της προσέγγισης είναι εφικτή και επιπλέον, δεν υπάρχει η ανάγκη των δρομολογητών που ανεβάζουν δεδομένα. Από την άλλη, υπάρχει μεγάλη απαίτηση αποθηκευτικού χώρου για το pushback daemon, ώστε τα πακέτα που χάνονται από τον περιοριστή του ρυθμού και της ουράς εξόδου να μπορούν να αναλυθούν.

4.4.2 Ταξινόμηση με βάση το χώρο δράσης

Σύμφωνα με το χώρο δράσης, διαχωρίζουμε τους αμυντικούς μηχανισμούς απέναντι σε επιθέσεις DDoS, σε αυτούς που δρουν στο δίκτυο του θύματος, στο ενδιάμεσο δίκτυο ή στο δίκτυο προέλευσης.

- *Μηχανισμοί που τοποθετούνται στο δίκτυο του θύματος*. Τα περισσότερα συστήματα που χρησιμοποιούνται για την καταπολέμηση επιθέσεων DDoS έχουν σχεδιαστεί έτσι ώστε να λειτουργούν στην πλευρά του θύματος, αφού αυτή η πλευρά είναι που δέχεται τον μεγαλύτερο αντίκτυπο των επιθέσεων. Το θύμα έχει το μεγαλύτερο κίνητρο να τοποθετήσει ένα σύστημα αντιμετώπισης επιθέσεων DDoS, και ίσως να θυσιάσει ένα ποσοστό από την απόδοση και τους πόρους του συστήματος του για αυξημένη ασφάλεια. Όλοι αυτοί οι μηχανισμοί αυξάνουν τη δυνατότητα του θύματος να αναγνωρίσει ότι

είναι ο στόχος μιας επίθεσης, και να κερδίσει περισσότερο χρόνο για να αντιδράσει.

- *Μηχανισμοί ενδιάμεσων δικτύων*. Οι μηχανισμοί αντιμετώπισης επιθέσεων DDoS που τοποθετούνται στο ενδιάμεσο δίκτυο είναι πιο αποτελεσματικοί από τους μηχανισμούς που τοποθετούνται σε ένα δίκτυο θύματος επειδή η επεξεργασία της κίνησης της επίθεσης μπορεί να πραγματοποιηθεί πιο εύκολα και να οδηγήσει σε ανίχνευση των επιτιθέμενων. Ωστόσο αυτοί οι μηχανισμοί αντιμετώπισης παρουσιάζουν διάφορα μειονεκτήματα που αποτρέπουν την ευρεία χρήση τους όπως το ότι η αύξηση της απόδοσης του ενδιάμεσου δικτύου προκαλεί μεγαλύτερη δυσκολία να ανιχνευτεί η επίθεση αφού το ενδιάμεσο δίκτυο συνήθως δεν αντιμετωπίζει καμία επίδραση από την επίθεση.
- *Μηχανισμοί δικτύων προέλευσης*. Οι μηχανισμοί αντιμετώπισης επιθέσεων DDoS που τοποθετούνται στο δίκτυο προέλευσης μπορούν να σταματήσουν τις ροές επίθεσης πριν αυτές εισέλθουν στον πυρήνα του Διαδικτύου και πριν συναθροιστούν με άλλες ροές επίθεσης. Όντας κοντά στις πηγές, μπορούν να πραγματοποιήσουν ευκολότερη ανίχνευση και έρευνα της επίθεσης. Ο μηχανισμός δικτύου πηγής έχει το ίδιο μειονέκτημα με τον μηχανισμό ενδιάμεσου δικτύου. Αντιμετωπίζει μεγάλη δυσκολία εντοπισμού της επίθεσης αφού αυτή έχει μικρή επίδραση στο δίκτυο της πηγής. Αυτό το μειονέκτημα μπορεί να εξισορροπηθεί από τη δυνατότητά του να θυσιάσει μερικούς από τους πόρους και την απόδοσή του για καλύτερη DDoS ανίχνευση. Όμως ένα τέτοιο σύστημα μπορεί να περιορίσει την κανονική κίνηση από ένα δίκτυο στην περίπτωση αναξιόπιστης ανίχνευσης επιθέσεων.

4.5 Συστήματα ανίχνευσης ανωμαλιών και γενίκευση

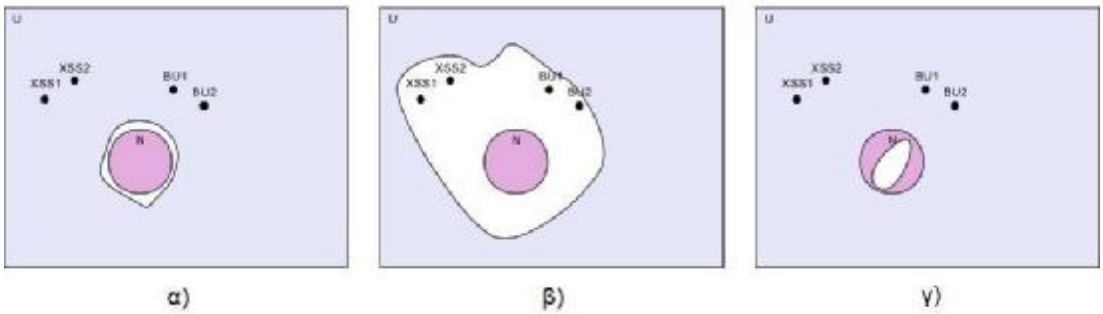
Ένα σύστημα ανίχνευσης ανωμαλιών αναπτύσσει ένα μοντέλο κανονικής συμπεριφοράς από εμπειρικές παρατηρήσεις, δηλαδή το σύνολο των δεδομένων εκπαίδευσης. Για να υπάρχει κανονική συμπεριφορά προϋπόθεση αποτελεί οι χρήστες να χρησιμοποιούν το σύστημα με τρόπο ώστε να μην του αναθέτουν εκτέλεση εργασιών για τις οποίες δεν το προορίζουν οι διαχειριστές του. Παρατηρήσεις που πραγματοποιούνται στη συνέχεια και αποκλίνουν από το μοντέλο κανονικής συμπεριφοράς, επισημαίνονται ως ανωμαλίες. Ένα σύστημα ανίχνευσης ανωμαλιών αναπτύσσει ένα μοντέλο κανονικής συμπεριφοράς, κάτι το οποίο αποτελεί ένα είδος μηχανικής μάθησης (machine learning).

Ένα σύστημα μάθησης μπορεί όχι μόνο απλά να απομνημονεύει τα δεδομένα εκπαίδευσης, αλλά και να *γενικεύει*, δηλαδή να δημιουργεί ένα σύνολο το οποίο αντιπροσωπεύει ένα παράδειγμα. Όταν ένα σύστημα ανίχνευσης ανωμαλιών

γενικεύει, δέχεται σαν είσοδο παρόμοια, αλλά όχι απαραίτητα και ταυτόσημα στιγμιότυπα με το σύνολο δεδομένων εκπαίδευσης, δηλαδή, το σύνολο των στιγμιότυπων που θεωρούνται κανονικά (το κανονικό σύνολο), είναι μεγαλύτερο από το σύνολο των στιγμιότυπων στα δεδομένα εκπαίδευσης. Για τα περισσότερα συστήματα ανωμαλιών (για παράδειγμα αυτά που χρησιμοποιούνται για web servers), το σύνολο των πιθανών νόμιμων δεδομένων στην είσοδο τείνει στο άπειρο και το ολοκληρωμένο σύνολο των κανονικών συμπεριφορών δεν είναι γνωστό και μπορεί να μεταβάλλεται με την πάροδο του χρόνου. Στην περίπτωση αυτή, το σύστημα ανίχνευσης ανωμαλιών θα πρέπει να χρησιμοποιήσει ένα ημιτελές σύνολο δεδομένων εκπαίδευσης. Για τα συστήματα αυτά, όπου το σύστημα δέχεται περισσότερα στιγμιότυπα από όσα παρέχονται στα δεδομένα εκπαίδευσης, η γενίκευση είναι προαπαιτούμενη.

Ο στόχος για ένα σύστημα ανίχνευσης ανωμαλιών είναι να δημιουργήσει ένα μοντέλο το οποίο περιγράφει με ακρίβεια την κανονική συμπεριφορά, όπως παρουσιάζεται στο Σχήμα 4.5α. Αν ο αλγόριθμος γενικεύει πάρα πολύ (υπέρ-γενικεύει), τότε το κανονικό σύνολο είναι πολύ μεγάλο. Στην περίπτωση αυτή, επιθέσεις ‘κοντά’ στα δεδομένα εκπαίδευσης μπορεί να αναγνωριστούν ως κανονικές (λανθασμένο αρνητικό), περιορίζοντας τη λειτουργικότητα του συστήματος. Το Σχήμα 4.5β δείχνει ένα σύστημα ανίχνευσης ανωμαλιών που υπέρ-γενικεύει.

Από την άλλη ένα σύστημα που απλά απομνημονεύει τα δεδομένα εκπαίδευσης χρειάζεται επαρκή χώρο αποθήκευσης για το ολοκληρωμένο σύνολο κανονικών δεδομένων. Προφανώς, αυτό είναι αδύνατον όταν το κανονικό σύνολο είναι άγνωστο ή άπειρο. Ένα τέτοιο σύστημα υπό-γενικεύει και εσφαλμένα αναγνωρίζει κανονικά συμβάντα ως ανώμαλα (λάθος θετικά). Ένα σύστημα που υπό-γενικεύει χάνει κανονικά στιγμιότυπα που είναι μικρές παραλλαγές των δεδομένων εκπαίδευσης. Το Σχήμα 4.5γ δείχνει ένα σύστημα ανίχνευσης ανωμαλιών που υπό-γενικεύει.



Σχήμα 4.5: *Διαγράμματα που δείχνουν: α) την επιθυμητή γενίκευση, β) την υπέρ-γενίκευση και γ) την υπό-γενίκευση. Τα σημεία BU1, BU2, XSS1 και XSS2 αναπαριστούν επιθέσεις, το N αναπαριστά το σύνολο των κανονικών δεδομένων και η γραμμή που περιβάλλει το λευκό σχήμα το σύνολο των δεδομένων που γίνονται δεκτά από το σύστημα ανίχνευσης ανωμαλιών. Το U είναι το σύνολο όλων των πιθανών εισόδων στο σύστημα.*

Το να προσδιοριστεί επιτυχώς το επίπεδο γενίκευσης εξαρτάται από την ροή δεδομένων και την αναπαράσταση που χρησιμοποιείται για αυτά. Οι περισσότερες ροές δεδομένων δεν είναι ακολουθίες τυχαίων bit. Αντιθέτως, αποτελούνται από θέσεις στις οποίες τοποθετούνται τιμές που έχουν αξία για το νόημα των δεδομένων, δηλαδή είναι *δομημένα*. Ένας ακριβής αλγόριθμος ανίχνευσης ανωμαλιών έχει μια αναπαράσταση που ταιριάζει με τη ροή δεδομένων με τρόπο ώστε να διευκολύνεται η ανίχνευση ανωμαλιών. Ως ένα παράδειγμα μπορεί να θεωρηθεί η αποτύπωση της ώρας και της ημερομηνίας. Σε μια ροή δεδομένων, μπορεί να δίνεται ως ένας αριθμός δευτερολέπτων (ή λεπτών, ωρών, ημερών κτλ.) από μια δεδομένη χρονική στιγμή. Για παράδειγμα τα περισσότερα συστήματα UNIX μετρούν τον χρόνο ως τον αριθμό των δευτερολέπτων από τα μεσάνυχτα της 1 Ιανουαρίου, 1970. Η αποτύπωση του χρόνου μπορεί να παρασταθεί με μια πιο φιλική προς τον άνθρωπο μορφή, όπως ΩΩ:ΛΛ:ΔΔ ΗΗ/ΜΜ/ΕΕ. Ωστόσο, η σειρά αυτών των πεδίων είναι διαφορετική σε διάφορους πολιτισμούς, οι μήνες και οι ημέρες μπορεί να παριστάνονται ολογράφως ή με αριθμούς, η χρονολογία μπορεί να δίνεται π.Χ. ή μ.Χ. (χωρίς το έτος 0, και έτσι απλές πράξεις με έτη μπορεί να μη γίνονται σωστά χωρίς ειδική επεξεργασία).

Για παράδειγμα, στα δεδομένα που αποστέλλονται στους web servers, όσον αφορά την αποτύπωση του χρόνου, τρεις διαφορετικές μορφοποιήσεις είναι αποδεκτές σύμφωνα με τα πρότυπα, και ακόμα περισσότερες χρησιμοποιούνται συχνά.

Εντός του συστήματος ανίχνευσης ανωμαλιών, τα δεδομένα μπορεί να αναπαρίστανται ως μια ακολουθία χαρακτήρων, ή μια σειρά λεκτικών μονάδων (πχ. ώρα, λεπτό, δευτερόλεπτο, ημέρα, μήνας, έτος). Οι λεκτικές μονάδες μπορεί είτε να περιέχουν την σχετική τιμή είτε όχι. Με τη χρήση λεκτικών μονάδων ο αλγόριθμος έχει τη δυνατότητα να μαθαίνει τη δομή, το οποίο έχει ως αποτέλεσμα το μοντέλο να αντιλαμβάνεται καλύτερα τη σημασία αυτού που αναπαριστά.

Όταν αναφερόμαστε σε γενίκευση, για παράδειγμα σε μια ημερομηνία, αν αυτή μπορεί να πάρει τιμές από ένα πεπερασμένο σύνολο αρκετά μικρό ώστε να αποθηκευτεί στη μνήμη, η απομνημόνευση της τιμής είναι επαρκής και δεν είναι απαραίτητο να γίνει γενίκευση. Όταν οποιαδήποτε ημερομηνία είναι επιτρεπτή, ο αριθμός των επιτρεπτών τιμών είναι θεωρητικά άπειρος (αν και πρακτικά είναι πεπερασμένος). Στην περίπτωση αυτή, οι λεκτικές μονάδες αποτελούν μια καλύτερη επιλογή, και μπορεί οι τιμές που σχετίζονται με τις λεκτικές μονάδες να μην είναι σημαντικές για να αναγνωριστεί η κανονική συμπεριφορά. Η αναπαράσταση έχει σχέση και με τις αναμενόμενες ανωμαλίες. Αν μια αναπαράσταση ημερομηνίας με ευρωπαϊκή μορφή θεωρείται ανωμαλία (πχ. για το αμερικάνικο σύστημα), τότε η αναπαράσταση θα πρέπει να είναι τέτοια ώστε να εκφράζεται αυτή η διαφορά.

Το παράδειγμα αυτό με την ημερομηνία επιδεικνύει τη διαφορά μεταξύ χαμηλής (ενός μικρού, πεπερασμένου συνόλου) και υψηλής (οποιαδήποτε επιτρεπόμενη ημερομηνία) μεταβλητότητας μιας (ή μέρους μιας) ροής δεδομένων. Το πρόβλημα είναι εντονότερο για δεδομένα τα οποία είναι ουσιαστικά τυχαία (όπως πχ. τα κρυπτογραφημένα δεδομένα). Όταν ένα σύστημα ανίχνευσης ανωμαλιών που υπό-γενικεύει επεξεργάζεται δεδομένα με μεγάλη μεταβλητότητα, πρέπει να προσπαθήσει να απομνημονεύσει τα δεδομένα. Στη χειρότερη περίπτωση των τυχαίων δεδομένων, αυτή η προσέγγιση είναι καταδικασμένη να χρησιμοποιεί υπερβολική μνήμη, και ταυτόχρονα να μην έχει τη δυνατότητα να παρέχει ένα ακριβές σύστημα. Όσο περισσότερες είναι οι περιοχές με μεγάλη μεταβλητότητα, τόσο περισσότεροι συνδυασμοί θα πρέπει να αναπαρίστανται στο μοντέλο κανονικής συμπεριφοράς του ανιχνευτή ανωμαλιών. Το αποτέλεσμα θα είναι ένα μοντέλο το οποίο είναι πολύ μεγάλο για να είναι πρακτικό, και/ή θα παράγει πάρα πολλά λανθασμένα θετικά. Αν από την άλλη, ο αλγόριθμος ανίχνευσης ανωμαλιών γενικεύει αρκετά ώστε να αποφεύγει το πρόβλημα των λανθασμένων θετικών, τα λιγότερο μεταβαλλόμενα μέρη των δεδομένων θα υποφέρουν από υπέρ-γενίκευση και το σύστημα θα είναι επιρρεπές στο να χάνει επιθέσεις. Οι περιοχές δεδομένων με υψηλή μεταβλητότητα απαιτούν μεγαλύτερη γενίκευση από τις περιοχές με χαμηλή μεταβλητότητα. Συμπερασματικά θα πρέπει για κάθε εφαρμογή να επιλέγεται ο κατάλληλος βαθμός γενίκευσης.

Για να βρεθεί η χρυσή τομή, χρειάζονται επιπλέον γενικεύσεις για ένα σύστημα που υπό-γενικεύει, και ένα σύστημα που υπέρ-γενικεύει θα χρειαστεί να μειώσει τη γενίκευση. Αν τα δεδομένα έχουν περιοχές με διαφορετική μεταβλητότητα, αυτές οι τροποποιήσεις θα πρέπει να γίνουν εκεί που το σύστημα υπέρ- ή υπό-γενικεύει. Επιπλέον, για να εντοπιστούν αυτές οι περιοχές, η αναπαράσταση των δεδομένων θα πρέπει να είναι τέτοια ώστε να διευκολύνεται ο διαχωρισμός μεταξύ μερών των δεδομένων που χρειάζονται περισσότερη γενίκευση από αυτά που χρειάζονται λιγότερη γενίκευση.

Συνοψίζοντας, η σωστή γενίκευση είναι απαραίτητη προϋπόθεση για την ανίχνευση ανωμαλιών με ακρίβεια. Για να έχει ένα σύστημα ανίχνευσης ανωμαλιών επαρκή ακρίβεια ώστε να χρησιμοποιηθεί στην πράξη, θα πρέπει να μην υπό-γενικεύει αλλά ούτε και να υπέρ-γενικεύει. Αν η γενίκευση δεν ελέγχεται επαρκώς, η ανίχνευση ανωμαλιών δεν θα είναι ακριβής. Το μοντέλο που χρησιμοποιείται από το σύστημα θα πρέπει να αναπαριστά τα δεδομένα με τέτοιο τρόπο ώστε να γίνεται εφικτή η διάκριση των κανονικών στιγμιότυπων δεδομένων από τα ανώμαλα στιγμιότυπα δεδομένων.

4.6 Ανίχνευση επίθεσης

Καθώς τα δίκτυα συνέδεσαν τα συστήματα μεταξύ τους, οι servers δικτύου έγιναν ευρέως γνωστοί και οι επιτιθέμενοι μπορούσαν να είναι διαχωρισμένοι από τα θύματά τους. Αυτό οδήγησε στην ανάγκη συστημάτων αναγνώρισης επίθεσης που είναι βασισμένα στο δίκτυο, και οι ερευνητές επιχείρησαν αναγνώριση και πρόληψη επιθέσεων σε πολλά επίπεδα του μοντέλου ISO. Φυσικοί περιορισμοί (παραδοσιακές κλειδαριές και άλλα φυσικά μέσα προστασίας) λειτουργούν αποτελεσματικά και αποτρέπουν επιθέσεις σε φυσικό επίπεδο. Οι διάφορες προσεγγίσεις περιλάμβαναν αναγνώριση ασυνήθιστης κίνησης, που βασιζόταν στις IP διευθύνσεις προέλευσης και προορισμού, στο πρωτόκολλο (TCP ή UDP) και τα ports. Δυστυχώς όμως δεν υπάρχει τίποτα το ασυνήθιστο ή επικίνδυνο όταν συνδέεται ένα νέο σύστημα σε έναν web server, έτσι χρειάζεται μια διαφορετική προσέγγιση για την προστασία των web servers.

Η αδυναμία να προστατευτούν οι web servers οδήγησε στην αναζήτηση νέων προσεγγίσεων. Κάποιοι μελετητές περιόρισαν το HTTP σε ένα προφανώς ασφαλές υποσύνολο του πρωτοκόλλου. Άλλες προσεγγίσεις παρακολουθούν τη ροή δεδομένων HTTP στο επίπεδο εφαρμογής του συστήματος OSI, παρά την δυσκολία να χρησιμοποιηθεί αυτή η ροή δεδομένων. Κάποιες από αυτές τις προσεγγίζεις αντιμετωπίζουν τους web servers σαν μια γενική υπηρεσία δικτύου. Η εισερχόμενη και εξερχόμενη κίνηση δεδομένων μοντελοποιούνται είτε ως μια ροή από byte είτε ως ξεχωριστά πακέτα. Μερικές προσεγγίσεις αναζητούν πρότυπα στα πακέτα που στέλνονται στα πρώτα στάδια των συνδέσεων . Άλλες συγκρίνουν την διασπορά χαρακτήρων μεταξύ των φορτίων πακέτων τα οποία έχουν παρόμοιο μέγεθος.
Σε αντίθεση με αυτές τις ανεξάρτητες σε σχέση με το πρωτόκολλο προσεγγίσεις, κάποιοι ερευνητές επικεντρώθηκαν στα αιτήματα HTTP στο επίπεδο εφαρμογής, για παράδειγμα μελετώντας στατιστικά παραμέτρων στα αιτήματα εφαρμογών διεπαφής κοινής πύλης (common gateway interface – CGI). Ωστόσο αυτοί οι ανιχνευτές ανωμαλιών θα πρέπει να εκπαιδευτούν σε δεδομένα που δεν περιέχουν επιθέσεις. Αυτή η απαίτηση δημιουργεί προβλήματα γιατί το Internet σήμερα μαστίζεται από έναν μεγάλο αριθμό γνωστών επιθέσεων, πολλές από τις οποίες είναι ακίνδυνες απέναντι σε σωστά προστατευμένους servers. Τα συστήματα αναγνώρισης επίθεσης με βάση την αναζήτηση υπογραφής όπως το *snort*, μπορούν να χρησιμοποιηθούν για να φιλτράρουν γνωστές ακίνδυνες επιθέσεις, όμως η μεγάλη ακρίβεια που χρειάζεται για την εκπαίδευση, απαιτεί συχνές αναβαθμίσεις στη βάση δεδομένων υπογραφών και προσεκτική ρύθμιση του εκάστοτε συστήματος για να αφαιρεθούν κανόνες που οδηγούν σε λανθασμένο συναγερμό. Αυτή η ανάγκη για χειροκίνητη παρέμβαση αποτελεί μειονέκτημα στην χρήση συστημάτων αναγνώρισης ανωμαλιών. Για την προστασία των web servers, ένας διαχειριστής συστήματος πρέπει να γνωρίζει πότε το σύστημα δέχεται επίθεση και έχει (ή υπάρχει κίνδυνος να) καταληφθεί. Αυτό είναι η αναγνώριση επίθεσης.

Ένα σύστημα αναγνώρισης επίθεσης που προστατεύει web servers πρέπει να αναγνωρίζει νέες επιθέσεις χωρίς ανθρώπινη παρέμβαση. Τα συστήματα αναγνώρισης ανωμαλίας αποτελούν μια λύση, η οποία ικανοποιεί αυτή την απαίτηση. Όλα τα συστήματα αναγνώρισης ανωμαλιών έχουν το κοινό γνώρισμα να μπορούν να ‘μαθαίνουν’ ένα μοντέλο κανονικής συμπεριφοράς. Ανά τα χρόνια,

ερευνητές δοκίμασαν πολλούς διαφορετικούς αλγορίθμους για να εκπαιδεύσουν αυτό το μοντέλο. Κάποιοι από αυτούς τους αλγορίθμους είναι πολλά υποσχόμενοι για χρήση σε πρωτόκολλα επιπέδου εφαρμογής όπως το HTTP. Άλλοι έχουν περιορισμούς οι οποίοι δεν τους επιτρέπουν σε καμία περίπτωση να λειτουργήσουν σε αυτό το πεδίο.

Όποτε το σύνολο των δεδομένων εκπαίδευσης που αναπαριστούν την κανονική συμπεριφορά για το σύστημα αναγνώρισης επίθεσης είναι ημιτελές ή το σύνολο είναι άπειρο, τότε το σύστημα θα πρέπει να κάνει γενίκευση. Ενώ οι ερευνητές έχουν κατανοήσει την χρησιμότητα της γενίκευσης, αυτή δεν έχει ερευνηθεί διεξοδικά.

Η ύπαρξη πληθώρας αλγορίθμων αναγνώρισης ανωμαλίας είναι αποτέλεσμα του γεγονότος ότι δεν υπάρχει μια κατανοητή θεωρία αναγνώρισης επίθεσης και αναγνώρισης ανωμαλίας, τέτοια ώστε να καθοδηγήσει σε κάποιες προσεγγίσεις με καλύτερες προδιαγραφές.

Ένα σύστημα ανίχνευσης επιθέσεων για να είναι αποδοτικό θα πρέπει να πληροί κάποιες δεδομένες προδιαγραφές. Ένα σύστημα ανίχνευσης επιθέσεων ενός web server θα πρέπει:

- Να είναι ακριβές, δηλαδή να αναγνωρίζει τις περισσότερες, ιδανικά όλες, τις επιθέσεις, και σπάνια να αναγνωρίζει ως ύποπτα δεδομένα που δεν περιέχουν επιθέσεις. Θα πρέπει να διατηρεί αυτή την ακρίβεια καθώς ένας ιστότοπος αλλάζει με το πέρασμα του χρόνου.
- Να ανιχνεύει νέες επιθέσεις.
- Να μην δημιουργεί πρόσθετο φορτίο στον διαχειριστή του συστήματος ή στο σύστημα που προστατεύει.

4.6.1 Αρχιτεκτονικές

Μέσα από την έρευνα που έχει πραγματοποιηθεί μέχρι σήμερα σχετικά με το πρόβλημα της αναγνώρισης επίθεσης, έχουν αναπτυχθεί τρεις αρχιτεκτονικές συστημάτων αναγνώρισης επίθεσης:

- η αναγνώριση υπογραφής
- η λειτουργία βάσει προδιαγραφών
- αναγνώριση ανωμαλιών

Κάποιοι ερευνητές δοκίμασαν υβριδικές προσεγγίσεις με σκοπό τα μειονεκτήματα της μιας αρχιτεκτονικής να εξουδετερώνονται με τα πλεονεκτήματα της άλλης.

4.6.1.1 Αναγνώριση υπογραφής

Η αναγνώριση υπογραφής καλείται επίσης και ανίχνευση κακομεταχείρισης. Ένας άνθρωπος μελετά μια επίθεση και αναγνωρίζει τα χαρακτηριστικά (πχ. συμπεριφορά ή/και περιεχόμενο) που την διαχωρίζουν από τα κανονικά δεδομένα ή κίνηση. Ο συνδυασμός αυτών των χαρακτηριστικών είναι γνωστός ως υπογραφή, και γίνεται μέρος μιας βάσης δεδομένων με υπογραφές επιθέσεων. Όταν το σύστημα αναγνώρισης επίθεσης αναγνωρίσει δεδομένα που ταιριάζουν με κάποια υπογραφή, σημαίνει έναν συναγερμό. Τα συστήματα αναγνώρισης επίθεσης με βάση την υπογραφή αποτελούν το μεγαλύτερο μέρος των εν ενεργεία συστημάτων. Είναι σημαντικά αλλά έχουν περιορισμούς όπως διαφαίνεται εν συνεχεία. Όλα τα εμπορικά προϊόντα κατά των ιών χρησιμοποιούν την αναγνώριση υπογραφής, όπως ακριβώς κάνει και το σύστημα αναγνώρισης επίθεσης snort.

Τα συστήματα που βασίζονται στην αναγνώριση υπογραφής έχουν συνήθως γρήγορη απόκριση, και μπορούν συχνά να αναγνωρίζουν με ακρίβεια επιθέσεις για τις οποίες έχουν δεδομένα υπογραφής. Όμως, επειδή είναι απαραίτητη η ύπαρξη κάποιου ανθρώπου που θα αναλύει κάθε επίθεση και θα αναπτύσσει την υπογραφή της, η γρήγορη απόκριση σε νέες επιθέσεις, που τεχνικά είναι υλοποιήσιμη, περιορίζεται σε μια χρονική κλίμακα ωρών ή ημερών. Οι επιθέσεις που προκαλούνται από προγράμματα που αυτοαναπαράγονται (ιοί ή worms) μπορούν να εμφανιστούν και να διαδοθούν μέσα σε δευτερόλεπτα. Όταν εμφανίζονται νέες επιθέσεις, τα συστήματα που προστατεύονται με συστήματα αναγνώρισης επίθεσης με βάση την υπογραφή είναι ευάλωτα μέχρι να είναι διαθέσιμο και εγκατεστημένο ένα ενημερωμένο σύνολο υπογραφών.

Όλα τα συστήματα ανίχνευσης επιθέσεων που βασίζονται στην αναγνώριση υπογραφής χρησιμοποιούν κάποιας μορφής αναγνώριση προτύπων για να διαχωρίσουν τις ακολουθίες που μπορεί να συνδέονται με κάποια επίθεση, είτε αυτή είναι ένας ιός σε ένα αρχείο, είτε είναι μια επίθεση Code Red ενάντια σε έναν web server. Σε πολλά συστήματα αναγνώρισης προτύπων, ένα πρότυπο είναι απλά μια ακολουθία (ιδανικά) η οποία δεν απαντάται πουθενά στα κανονικά δεδομένα. Κάποια συστήματα αναγνώρισης προτύπων περιλαμβάνουν και άλλες πληροφορίες, όπως το που να γίνει η αναζήτηση της ακολουθίας (είτε με απόλυτη θέση, είτε με θέση σχετική στο πρωτόκολλο ή στο σύστημα αρχείων).

Τα συστήματα που βασίζονται στην αναγνώριση υπογραφής υποφέρουν από τα λανθασμένα θετικά, ειδικά όταν αλλάζει η ρύθμιση του συστήματος ή το περιβάλλον. Ο Patton περιέγραψε το φαινόμενο ως στρίγκλισμα (squealing), και

έδειξε πως οι επιτιθέμενοι εκμεταλλεύονται το σύστημα αναγνώρισης επιθέσεων με προσεκτικά κατασκευασμένα λανθασμένα θετικά.

Τα συστήματα που βασίζονται στην αναγνώριση υπογραφής είναι δυνατόν να μην αναγνωρίσουν κάποια επίθεση την οποία θεωρητικά θα έπρεπε να αναγνωρίσουν (λανθασμένο αρνητικό). Όταν δοκιμάστηκαν δυο από τα 'καλύτερα' συστήματα που βασίζονται στην αναγνώριση υπογραφής (snort και ISS RealSecure) ως προς την αποτελεσματικότητά τους, ο Vigna διαπίστωσε ότι παραλλαγές γνωστών επιθέσεων δεν μπορούν να ανιχνευτούν από το σύστημα.

Τα περισσότερα συστήματα που βασίζονται στην αναγνώριση υπογραφής κάνουν ελάχιστη ή και καθόλου γενίκευση. Ένα σύστημα που κάνει αναφέρεται από τον Ning, όπου με αφαίρεση στοιχείων των υπογραφών κατέστη δυνατό να ανιχνευθούν σχετικές παραλλαγμένες επιθέσεις.

4.6.1.2. Λειτουργία βάσει προδιαγραφών

Ένας ειδικός μελετά το πρόγραμμα που πρέπει να προστατευθεί και δημιουργεί κάποιες προδιαγραφές που αναγνωρίζουν τις ενέργειες που επιτρέπεται να κάνει ένα πρόγραμμα (δηλαδή αυτές που σκόπευε ο δημιουργός του). Όταν το σύστημα βρίσκεται σε λειτουργία, η συμπεριφορά του συγκρίνεται με αυτή που έχει τεθεί από τις προδιαγραφές, και οι αποκλίσεις από αυτήν επισημαίνονται ή/και προλαμβάνονται. Το συμπλήρωμα αυτής της προσέγγισης είναι να περιγραφεί η συμπεριφορά που υποδεικνύει επιθέσεις. Κάποιες φορές η περιγραφή αυτών που δεν επιτρέπονται είναι ευκολότερη από την περιγραφή αυτών που επιτρέπονται.

Ένα πρόβλημα με αυτή την προσέγγιση είναι ότι το επίπεδο εξειδίκευσης που χρειάζεται για να δημιουργηθεί ένα κατάλληλο σύνολο προδιαγραφών είναι σημαντικά υψηλότερο από αυτό που απαιτείται να υλοποιηθεί ένα πρόγραμμα. Επιπροσθέτως, κάθε πρόγραμμα χρειάζεται διαφορετικές προδιαγραφές, και κάθε φορά που το πρόγραμμα αλλάζει, οι προδιαγραφές θα πρέπει να αξιολογούνται από κάποιον ειδικό. Αυτές οι απαιτήσεις ανεβάζουν το κόστος, και γι' αυτό η χρήση της είναι περιορισμένη σε εμπορικά συστήματα.

Τα συστήματα που βασίζονται στη λειτουργία βάσει προδιαγραφών παρουσιάζουν επίσης προβλήματα σχετικά με την κατάλληλη χρήση τους. Για παράδειγμα οι Hogland και McGraw επισημαίνουν ότι οι λίστες ελέγχου πρόσβασης, ένα από τα πιο απλά στοιχεία αυτών των συστημάτων, είναι τόσο πολύπλοκες που πρακτικά αποτυγχάνουν στην πράξη.

4.6.1.3. Ανίχνευση ανωμαλιών

Η ανίχνευση ανωμαλιών καλείται επίσης και αναγνώριση με βάση την συμπεριφορά. Τα συστήματα αναγνώρισης ανωμαλιών υποθέτουν ότι οι απόπειρες για επίθεση είναι σπάνιες και ότι έχουν διαφορετικά χαρακτηριστικά από την κανονική συμπεριφορά. Το σύστημα αναγνώρισης επίθεσης δημιουργεί ένα μοντέλο κανονικής συμπεριφοράς από ένα σύνολο δεδομένων εκπαίδευσης. Όταν εμφανίζεται ένα στιγμιότυπο το οποίο δεν ταιριάζει στο μοντέλο που δημιουργήθηκε από την εκπαίδευση, τότε το σύστημα σημαίνει έναν συναγερμό. Το να βρεθεί η κατάλληλη αναπαράσταση των δεδομένων και να επιλεγεί ένας κατάλληλος αλγόριθμος εκμάθησης ώστε να χρησιμοποιηθεί με τα δεδομένα, μπορεί να είναι μια δύσκολη διαδικασία για τα συστήματα αναγνώρισης ανωμαλίας.

4.6.1.4. Υβριδικά συστήματα

Ένα σύστημα αναγνώρισης επιθέσεων βασισμένο σε αυτήν την αρχιτεκτονική κάνει χρήση δυο ή και περισσότερων από αυτές τις αρχιτεκτονικές, έτσι ώστε να εκμεταλλευτεί τα πλεονεκτήματα της μιας για να καλύψει τις αδυναμίες της άλλης. Για παράδειγμα, ο Sekar συνδύασε στατιστικές μεθόδους για αναγνώριση ανωμαλιών με μια μηχανή καταστάσεων που καθορίζουν την επιτρεπόμενη δικτυακή επικοινωνία.

Μόνο ένα υβριδικό σύστημα έχει αναφερθεί για το πρωτόκολλο HTTP. Ο Tombini συνδύασε την αναγνώριση κακομεταχείρισης και ανωμαλιών για να ανιχνεύσει επιθέσεις σε καταχωρημένα αιτήματα HTTP, και ανέλυσε πώς να επιλυθούν οι διενέξεις μεταξύ των δυο αρχιτεκτονικών, ώστε να επιτευχθεί η μέγιστη ακρίβεια. Αυτό το σύστημα είχε αρκετά μειονεκτήματα που εμπόδισαν την εφαρμογή του σε εμπορικά συστήματα.

4.7 Ανίχνευση ανωμαλιών

Η ανίχνευση ανωμαλιών έχει την προοπτική να ανιχνεύει νέες επιθέσεις. Για τον λόγο αυτό έχουν μελετηθεί πολλά μοντέλα και αλγόριθμοι. Ένα σύστημα ανίχνευσης ανωμαλιών χρησιμοποιεί ένα σύνολο δεδομένων εκπαίδευσης, έτσι ώστε να δημιουργήσει ένα κανονικό μοντέλο, και έπειτα επισημαίνει ως ανωμαλία οποιοδήποτε στιγμιότυπο δεδομένων δεν περιλαμβάνεται στο μοντέλο αυτό.

Τα πρώτα συστήματα ανίχνευσης ανωμαλιών ήταν βασισμένα σε στατιστικές μετρήσεις κανονικότητας με πηγή δεδομένων εγγραφές από παρακολούθηση του εξυπηρετητή και δεδομένα δικτύου χαμηλότερων επιπέδων. Ο Forrest εισήγαγε την ιδέα της μοντελοποίησης συμπεριφοράς του προγράμματος καταγράφοντας σύντομες ακολουθίες κλήσεων συστήματος. Η εργασία αυτή δημιούργησε σημαντικό ενδιαφέρον και οδήγησε σε πολλές προτάσεις εναλλακτικών μοντέλων συμπεριφοράς κλήσεων συστήματος, συμπεριλαμβανομένων των ακολουθιών μεταβλητού μήκους και του data mining που βασίζεται σε κανόνες. Δυστυχώς, η παρακολούθηση κλήσεων συστήματος δεν φαίνεται να είναι μια υποσχόμενη προσέγγιση για την αναγνώριση επιθέσεων σε web servers. Παλαιότερη μελέτη με το pH, ένα σύστημα αναγνώρισης επίθεσης βασισμένο σε Linux το οποίο παρακολουθεί ακολουθίες κλήσεων συστήματος, δείχνει ότι οι web servers είναι δύσκολο να παρακολουθούνται στην πράξη, και σε κάποιες περιπτώσεις απαιτούνται ακόμα και μήνες για να επιτευχθεί ένα σταθερό μοντέλο κανονικής συμπεριφοράς.

Ένα άλλο ζήτημα είναι ότι πολλές επιθέσεις σε web servers προκαλούνται από λάθη στις ρυθμίσεις παραμέτρων ή λάθη στον κώδικα της web εφαρμογής. Τα exploit που βασίζονται σε αυτές τις αδυναμίες μπορεί να μην δημιουργήσουν ασυνήθιστα μοτίβα κλήσεων συστήματος γιατί δεν προκαλούν ασυνήθιστη εκτέλεση του κώδικα του web server. Ο web server απλά μεταφράζει το ευάλωτο script, και το ίχνος της κλήσης συστήματος που δημιουργείται από την διαδικασία μετάφρασης είναι παρόμοιο είτε το script είναι ευάλωτο είτε όχι.

Επειδή όλη η I/O συμπεριφορά περνάει συνήθως από τη διεπαφή κλήσεων συστήματος, ουσιαστικά όλες οι επιθέσεις σε web servers θα έπρεπε, θεωρητικά τουλάχιστον να είναι ανιχνεύσιμες παρατηρώντας τα δεδομένα των κλήσεων συστήματος. Ωστόσο, πρώιμες προσπάθειες μοντελοποίησης των δεδομένων κλήσεων συστήματος, δημιούργησαν πολλούς λανθασμένους συναγερμούς, παρά την υιοθέτηση πολύ πιο μελετημένης στρατηγικής από αυτήν που αρχικά πρότειναν ο

Forrest et al. Η ασυμφωνία φαίνεται να είναι φυσικό επακόλουθο της μεγάλης μεταβλητότητας των δεδομένων κλήσεων συστήματος σε σχέση με τις ακολουθίες κλήσεων συστήματος.

4.7.1 Αλγόριθμοι

Ανά τα χρόνια, οι ερευνητές πρότειναν πολλούς αλγόριθμους για την ανίχνευση ανωμαλιών. Κάποιοι από αυτούς τους αλγόριθμους έχουν περιορισμούς (πχ. απαίτηση να έχουν είσοδο ορισμένου μήκους όταν το HTTP είναι μεταβλητού μήκους) που εμποδίζουν τη χρησιμοποίηση τους με το πρωτόκολλο HTTP. Επειδή τα αποτελέσματα που δείχνουν έναν αλγόριθμο που αποτυγχάνει είναι δύσκολο να δημοσιευτούν, μπορούμε να δούμε μόνο πότε ένας αλγόριθμος φαίνεται να λειτουργεί ικανοποιητικά σε μια δεδομένη πηγή δεδομένων και αναπαράσταση, δηλαδή είναι ακριβής τουλάχιστον για τις δοκιμές που πραγματοποιούνται.

4.7.1.1 Συστήματα που βασίζονται σε κανόνες

Τα συστήματα που βασίζονται σε κανόνες αποτελούνται από ένα σύνολο κανόνων που ορίζουν την κανονική συμπεριφορά. Δεδομένου ενός συνόλου παρατηρήσεων κανονικής συμπεριφοράς, οι κανόνες περιγράφουν τα δεδομένα. Για παράδειγμα, αν τα δεδομένα περιέχουν χρονικές τιμές έναρξης και λήξης συνεδρίας, το σύστημα αναγνώρισης επίθεσης μπορεί να δημιουργήσει έναν κανόνα που καθορίζει ότι οι συνεδρίες δεν ξεκινούν πριν τις 6:00πμ, ή ότι δεν μπορούν να διαρκούν πάνω από 8 ώρες. Οι κανόνες μπορεί να είναι σχετικά, πολλαπλά, ξεχωριστά συμβάντα, για παράδειγμα, οι ενέργειες x, y και z να συμβαίνουν εντός συνεδριών τύπου w. Όταν το σύνολο των κανόνων έχει δημιουργηθεί, το σύστημα αναγνώρισης επίθεσης δημιουργεί έναν συναγερμό σε περίπτωση που παραβαίνεται κάποιος κανόνας.

Ένας τύπος συστήματος που βασίζεται σε κανόνες είναι ένα εξειδικευμένο σύστημα. Στην περίπτωση αυτή οι κανόνες δημιουργούνται από ανθρώπους. Η άλλη προσέγγιση είναι το σύστημα ανίχνευσης επιθέσεων να δημιουργεί αυτόματα τους κανόνες.

Μόνο ένα σύστημα ανίχνευσης επιθέσεων στο HTTP χρησιμοποιεί αυτή την προσέγγιση. Οι Vargiya και Chan συνέκριναν τέσσερις στατιστικές τεχνικές για να προσδιορίσουν τα όρια των λεκτικών μονάδων αυτόματα: οριακή εντροπία, συχνότητα, επαυξημένη αναμενόμενη αμοιβαία πληροφορία, και ελάχιστο μήκος περιγραφής (minimum description length, MDL), καθώς και δυο συνδυασμούς

αυτών των μεθόδων. Κατέληξαν στο ότι η συχνότητα και το MDL απέδωσαν καλύτερα στα αυτόματης αναγνώρισης λεκτικών μονάδων. Οι λεκτικές μονάδες χρησιμοποιήθηκαν με ένα σύστημα δημιουργίας κανόνων, το LERAD.

4.7.1.2 Περιγραφική στατιστική

Σε ένα σύστημα με βάση τη στατιστική, το σύστημα ανίχνευσης επιθέσεων παρατηρεί μια κανονική συμπεριφορά και υπολογίζει ένα ή περισσότερα στατιστικά μεγέθη που ένας άνθρωπος ή κάποιο άλλο κομμάτι του συστήματος ανίχνευσης επιθέσεων αναγνωρίζει ως σημαντικό. Οι στατιστικές μέθοδοι που χρησιμοποιούνται μπορεί να είναι απλή ανάλυση συχνότητας, δίκτυα Bayesian, κρυμμένα μοντέλα Markov, ή άλλες. Έπειτα το σύστημα ανίχνευσης επιθέσεων επισημαίνει αποκλίσεις από αυτά τα στατιστικά μεγέθη. Πολλές πρώιμες προσεγγίσεις βασίζονταν στη στατιστική.

Όσον αφορά τα πρωτόκολλα ανώτερων επιπέδων, οι περισσότεροι ερευνητές αντιμετώπισαν την ροή δεδομένων ως μια ακολουθία χαρακτήρων, και εφάρμοσαν στατιστικές μεθόδους στους χαρακτήρες. Για παράδειγμα, οι Wang και Stolfo, μοντελοποίησαν την διασπορά χαρακτήρων σε πακέτα διαφορετικών μεγεθών. Οι Mahoney και Chan, εφάρμοσαν στατιστικές μεθόδους στις κεφαλίδες των πακέτων, με κάποια στατιστικά να αφορούν τα δεδομένα επιπέδου εφαρμογής (πχ. λέξεις κλειδιά του HTTP). Ο Mahoney έπειτα κωδικοποίησε τα πρώτα 48 bytes των πακέτων επιπέδου εφαρμογής από σημαντικές υπηρεσίες (HTTP, SMTP, FTP κ.α.) χρησιμοποιώντας ένα σύνολο στατιστικών μετρήσεων.

Ο Kruegel, ανέλυσε τις παραμέτρους προγράμματος διεπαφής κοινής πύλης (common gateway interface, CGI) χρησιμοποιώντας έναν γραμμικό συνδυασμό από έξι μεγέθη: μήκος χαρακτηριστικών, διασπορά χαρακτήρων, χρησιμοποιώντας ένα μοντέλο Markov, διαχωρίζοντας αν οι λεκτικές μονάδες ήταν τυχαίες ή από ένα σύνολο αλφαριθμητικών, παρουσία ή απουσία χαρακτηριστικών και την σειρά χαρακτηριστικών.

Ο Estevez-Tapiador χρησιμοποίησε και αυτός ένα μοντέλο Markov. Δοκίμασαν το μοντέλο με χαρακτήρες από αιτήματα, και διαπίστωσαν ότι δεν απέδωσε καλά. Ωστόσο όταν έσπασαν τα αιτήματα σε ψεύδο-λεκτικές μονάδες, η απόδοση βελτιώθηκε. Δυστυχώς ο καλύτερος ρυθμός λανθασμένων συναγερμών που αναφέρθηκε ήταν 5,76%.

4.7.1.3 Προσανατολισμένοι γράφοι

Κάποιες αναπαραστάσεις κωδικοποιούν σαφώς τις σχέσεις διαδοχής ως έναν προσανατολισμένο γράφο. Για παράδειγμα τρεις προσεγγίσεις που χρησιμοποιούνται στην ανίχνευση επίθεσης για το HTTP χρησιμοποιούν αυτή την αναπαράσταση: το μοντέλο Markov το οποίο αναφέρθηκε πριν, το ντετερμινιστικό πεπερασμένο αυτόματο (Deterministic Finite Automata, DFA), και τα n-grams. Το μοντέλο Markov και το DFA αποτελούνται από ένα σύνολο κόμβων, με εναλλαγές μεταξύ των κόμβων. Ένα n-gram είναι μια ακολουθία από n στοιχεία, χαρακτήρες ή λεκτικές μονάδες. Ένα σύνολο από n-grams είναι ένα κανονικό μοντέλο. Στα n-grams, ένα στοιχείο a που ακολουθεί ένα στοιχείο b κωδικοποιείται σαν ab ως μέρος μιας ή περισσοτέρων ακολουθιών στο σύνολο.

Οι Wagner και Dean χρησιμοποίησαν έναν προσανατολισμένο γράφο για να αναπαραστήσουν τις κλήσεις συστήματος που γίνονταν από ένα προστατευμένο πρόγραμμα.

Οι Kruegel και Vigna χρησιμοποίησαν έναν προσανατολισμένο γράφο για να αναπαραστήσουν τη σειρά παραμέτρων της διεπαφής κοινής πύλης (CGI) στο μονοπάτι πόρου HTTP, για τον οποίο γίνεται αίτηση.

- *Ντετερμινιστικό πεπερασμένο αυτόματο (DFA).* Για αυτή την προσέγγιση, το σύστημα ανίχνευσης επιθέσεων δημιουργεί ένα ντετερμινιστικό πεπερασμένο αυτόματο από τα δεδομένα εκπαίδευσης, μαθαίνοντας αποτελεσματικά μια (επίσημη) γλώσσα. Συμβολοσειρές οι οποίες δεν είναι μέρος της γλώσσας επισημαίνονται ως ανωμαλίες. Όταν τα δεδομένα που μοντελοποιούνται περιγράφονται από μια γλώσσα (πχ. τα πρωτόκολλα δικτύου), η προσέγγιση αυτή μαθαίνει το υποσύνολο του πρωτοκόλλου που χρησιμοποιείται από τον υπολογιστή που προστατεύει το σύστημα ανίχνευσης επιθέσεων. Άλλοι ερευνητές μελέτησαν την ανίχνευση ανωμαλιών χρησιμοποιώντας μεθόδους κατασκευής μοντέλων συμπεριφοράς προγραμμάτων βασισμένα σε πεπερασμένα αυτόματα.

Στην πράξη η χρήση DFA είναι πρακτική σε πολλές εφαρμογές, και υπάρχουν εκτενείς αναλύσεις αλγορίθμων DFA στην βιβλιογραφία.

- *n-grams και lookahead pairs.* Τα n-grams χρησιμοποιούνται στην ανάκτηση πληροφοριών, στην μέτρηση ομοιότητας εγγράφων ή στην κατηγοριοποίηση κειμένου και για μέτρηση κανονικής συμπεριφοράς στην ανίχνευση επίθεσης. Τα lookahead pairs έχουν παρόμοιο αποτέλεσμα με τα n-grams, αλλά ο Somayaji βρήκε ότι είναι πιο αποδοτικά.

4.7.1.4 Νευρωνικά δίκτυα

Μια ή περισσότερες πηγές δεδομένων χρησιμοποιούνται για να εκπαιδεύσουν το νευρωνικό δίκτυο, ώστε να αναγνωρίζει την κανονική συμπεριφορά. Το νευρωνικό δίκτυο έπειτα αναγνωρίζει τη συμπεριφορά που δεν αντιστοιχεί στην εκπαίδευσή του. Σε άλλα πεδία, τα νευρωνικά δίκτυα έχουν δείξει την ικανότητά τους να αναγνωρίζουν πρότυπα. Τα περισσότερα νευρωνικά δίκτυα απαιτούν είσοδο συγκεκριμένου μήκους, μια απαίτηση που δημιουργεί προβλήματα με δεδομένα μεταβλητού μήκους όπως τα αιτήματα HTTP.

4.7.1.5 Support Vector Machines

Έχοντας υπ' όψιν ότι κάποιοι αλγόριθμοι ανίχνευσης ανωμαλιών υπογενικέυουν , ο Mukkamala εκπαίδευσε μια Support Vector Machine (SVM) στα δεδομένα κίνησης της αξιολόγησης συστημάτων ανίχνευσης επιθέσεων 1998 DARPA/MIT Lincoln Labs. Αυτά τα δεδομένα περιείχαν δυο επιθέσεις HTTP. Συνέκρινε την SVM με ένα νευρωνικό δίκτυο και βρήκαν ότι η SVM ήταν ακριβέστερη και γρηγορότερη. Η χρονική διάρκεια εκπαίδευσης της SVM ήταν 17,77 δευτερόλεπτα συγκρινόμενη με του νευρωνικού δικτύου που ήταν 18 λεπτά.

4.7.1.6 Ανάκτηση πληροφορίας

Εκτός από τα n-grams, για την κατηγοριοποίηση δεδομένων μπορεί να είναι χρήσιμες και άλλες τεχνικές από την ανάκτηση πληροφορίας (information retrieval, IR) για την κατηγοριοποίηση κειμένου ή την μέτρηση απόστασης μεταξύ διαφορετικών κειμένων. Παρά τον παραλληλισμό αυτό, ελάχιστοι ερευνητές το προσπάθησαν.

4.7.1.7 Συνδυασμός πολλαπλών αισθητήρων

Ο Axelsson δείχνει ότι για να αποφευχθεί το σφάλμα βασικού ρυθμού αλλά και να μην υπάρχουν πολλοί λανθασμένοι συναγερμοί, το σύστημα ανίχνευσης επιθέσεων θα πρέπει να έχει υψηλή ακρίβεια ή χαμηλό ρυθμό λάθους (Το σφάλμα βασικού ρυθμού συμβαίνει όταν ένας ανιχνευτής φαίνεται να έχει καλή ακρίβεια, αλλά ο ρυθμός που συμβαίνει μια ανίχνευση να είναι χαμηλός, οδηγώντας έτσι σε

κατώτερη του αναμενομένου απόδοση). Για να αντιμετωπιστεί αυτό το πρόβλημα, μια προσέγγιση είναι να συνδυαστούν αποτελέσματα από πολλαπλούς αισθητήρες ανίχνευσης εισβολής.

4.7.1.8 Ανοσολογικό σύστημα

Το ανοσολογικό σύστημα μπορεί να θεωρηθεί ότι έχει πετύχει τον στόχο που οι ερευνητές συστημάτων ανίχνευσης επιθέσεων προσπαθούν να επιτύχουν. Η ικανότητα να αναγνωρίζει και να καταστρέφει εχθρικές οντότητες (μη ίδιες) χωρίς να επιτίθεται στον ίδιο του τον εαυτό είναι το 'ιερό δισκοπότηρο' της αναγνώρισης επιθέσεων.

Ένας ενδιαφέρων μηχανισμός του ανοσολογικού συστήματος είναι η αρνητική ανίχνευση. Στο ανοσολογικό σύστημα των σπονδυλωτών, τα λεμφοκύτταρα έχουν ανιχνευτές μορίων ή μερών πεπτιδίων που δεν σχετίζονται με το άτομο (είναι ξένα).

Λαμβάνοντας υπ' όψιν αυτό το μέρος της βιολογίας, κάποια συστήματα χρησιμοποιούν αρνητική ανίχνευση για να δημιουργήσουν ανιχνευτές για δεδομένα που δεν εμφανίζονται στην κανονική ροή δεδομένων. Όταν κάποιος ανιχνευτής βρίσκει κάτι αντίστοιχο, εικάζεται ότι υπάρχει μια ανωμαλία. Η αρνητική ανίχνευση έχει το πλεονέκτημα ότι μπορεί εύκολα να διαδοθεί σε όλα τα μηχανήματα που είναι συνδεδεμένα σε κάποιο δίκτυο. Ο Forrest χρησιμοποίησε την αρνητική ανίχνευση για να κάνει ανίχνευση ιών και ο Hofmeyr την χρησιμοποίησε για να κάνει ανίχνευση ανωμαλιών με πρότυπα κίνησης δικτύου. Δυστυχώς, αυτή η προσέγγιση δεν έχει καλή εφαρμογή στους web servers, όπου οι νέες συνδέσεις είναι κάτι το συνηθισμένο.

Άλλη μια ιδέα εμπνευσμένη από την ανοσολογία είναι και αυτή της ανεκτικότητας. Όταν το σύστημα ανίχνευσης επιθέσεων δημιουργεί έναν ανιχνευτή, αυτός θεωρείται ανώριμος. Αν ένας ανιχνευτής εντοπίσει κάποια σχετική τιμή στα πρώτα στάδια της ύπαρξής του, τότε ο ανιχνευτής θεωρείται ότι εντοπίζει τον εαυτό του, και διαγράφεται. Αν ο ανιχνευτής επιβιώσει την περίοδο ανεκτικότητας, τότε ωριμάζει. Όταν ένας ώριμος ανιχνευτής εντοπίσει μια σχετική τιμή, τότε το αίτημα θεωρείται ανώμαλο.

Σε ένα ανοσολογικό σύστημα, η συνδιέγερση των Τ- και Β-κυττάρων απαιτείται από τα άλλα κύτταρα πριν να δημιουργηθεί μια απόκριση ανοσίας. Στο LISYS, ένας ώριμος ανιχνευτής που εντοπίζει κάποια ύποπτη τιμή διαγράφεται, εκτός αν δεχτεί συνδιέγερση. Η ιδέα αυτή σχετίζεται με αυτή του συνδυασμού πολλαπλών αισθητήρων, αν και στην περίπτωση αυτή ο δεύτερος ανιχνευτής είναι ένας άνθρωπος.

4.8 Κατηγορίες ανωμαλιών

Ένα σύστημα ανίχνευσης ανωμαλιών όπως τα SPADE, ADAM, ή NIDES μοντελοποιούν την κανονική κίνηση, και συνήθως την κατανομή των διευθύνσεων IP και των ports. Η επιθετική κίνηση πολλές φορές βγαίνει εκτός αυτής της κατανομής. Η ανίχνευση ανωμαλιών έχει το πλεονέκτημα ότι δεν χρειάζεται η σύνταξη κάποιων κανόνων και ότι μπορεί να ανιχνεύσει νέες επιθέσεις. Έχει όμως το μειονέκτημα ότι δεν μπορεί να προσδιορίσει τη φύση της επίθεσης (εφόσον είναι νέα), και επειδή η κανονική κίνηση μπορεί επίσης να αποκλίνει από το κανονικό μοντέλο, πολλές φορές δημιουργούνται λανθασμένοι συναγερμοί. Ένας ανιχνευτής ανωμαλίας μπορεί μόνο να επιστήσει την προσοχή ενός ειδικού στην ασφάλεια δικτύων, όσον αφορά την ύποπτη κίνηση που ανιχνεύει, ο οποίος εν συνεχεία θα πρέπει να αποφασίσει αν θα πρέπει να γίνει κάποια περαιτέρω ενέργεια.

Οι Mahoney και Chan αναγνωρίζουν πέντε κατηγορίες ανωμαλιών στην επιθετική κίνηση.

- ***Συμπεριφορά χρηστών***. Η επιθετική κίνηση μπορεί να έχει μια νέα διεύθυνση προέλευσης εφόσον προέρχεται από έναν μη εξουσιοδοτημένο χρήστη μιας υπηρεσίας περιορισμένης πρόσβασης (προστατευμένης με κωδικό). Επίσης probes, όπως τα ipsweep και portsweep μπορεί να επιχειρήσουν να αποκτήσουν πρόσβαση σε εξυπηρετητές και υπηρεσίες που μπορεί να μην υπάρχουν, δημιουργώντας ανωμαλίες στις διευθύνσεις προορισμού και τους αριθμούς port.
- ***Εκμετάλλευση bug***. Οι επιθέσεις συχνά εκμεταλλεύονται σφάλματα στο λογισμικό που στοχεύουν, για παράδειγμα μια αδυναμία υπερχείλισης buffer. Τέτοια σφάλματα είναι πιο πιθανόν να βρεθούν σε λιγότερο χρησιμοποιούμενες λειτουργίες του προγράμματος, γιατί σε αντίθετη περίπτωση το σφάλμα πιθανόν να είχε ανακαλυφθεί κατά την κανονική χρήση και να είχε διορθωθεί σε μια πιο νέα έκδοση. Έτσι, τα εναπομείναντα σφάλματα εκμεταλλεύονται μόνο με ασυνήθιστα δεδομένα εισόδου (πχ. ένα υπερβολικά μεγάλο όρισμα σε εντολή που σπάνια χρησιμοποιείται), τα οποία είναι δύσκολο να συμβούν κατά την κανονική χρήση.
- ***Ανωμαλίες στην απόκριση***. Μερικές φορές ένα σύστημα-στόχος μπορεί να δημιουργήσει εξερχόμενη κίνηση που έχει ανωμαλίες ως απόκριση σε μια επιτυχημένη επίθεση, για παράδειγμα, ένας server ηλεκτρονικού ταχυδρομείου-θύμα ο οποίος στέλνει αποκρίσεις εντολών root πίσω στον επιτιθέμενο. Αυτό είναι αντίστοιχο στην μέθοδο ανίχνευσης βασισμένη σε εξυπηρετητή του Forrest, όπου μια κατάληψη ενός server μπορεί να ανιχνευθεί επειδή κάνει ασυνήθιστες ακολουθίες κλήσεων συστήματος.

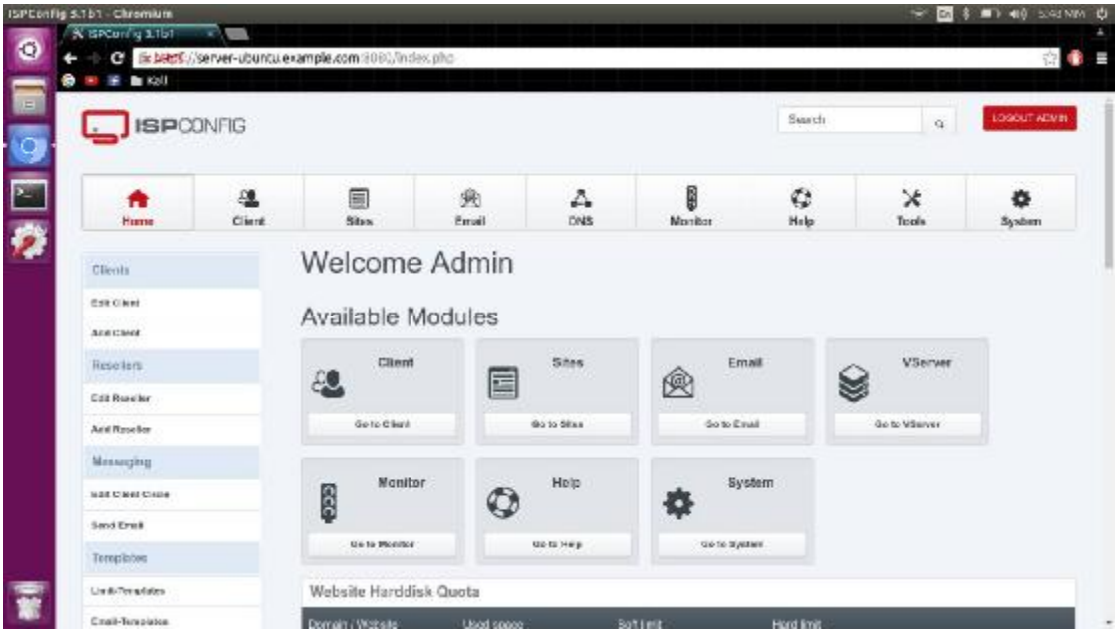
- ***Bug στην επίθεση***. Οι επιτιθέμενοι γενικά πρέπει να προσαρμόζονται οι ίδιοι στα πρωτόκολλα του πελάτη και μπορεί να αποτύχουν να εναρμονιστούν με το περιβάλλον του πελάτη είτε γιατί μπορεί να είναι απρόσεκτοι, είτε γιατί κάποιες φορές δεν το θεωρούν απαραίτητο. Για παράδειγμα, πολλά πρωτόκολλα που είναι βασισμένα σε κείμενο όπως τα FTP, SMTP και HTTP επιτρέπουν εντολές με κεφαλαία ή πεζά γράμματα. Ένας επιτιθέμενος μπορεί να χρησιμοποιεί πεζά γράμματα για ευκολία, ενώ οι κανονικοί πελάτες είναι πιθανό να χρησιμοποιούν πάντα κεφαλαία.
- ***Ελιγμοί***. Οι επιτιθέμενοι μπορεί επίτηδες να χειραγωγούν τα πρωτόκολλα του δικτύου για να αποκρύψουν μια επίθεση από ένα μη επαρκώς προγραμματισμένο σύστημα ανίχνευσης επιθέσεων που παρακολουθεί το επίπεδο εφαρμογής. Τέτοιες μέθοδοι είναι το IP fragmentation, τα επικαλυπτόμενα segments TCP που δεν ταιριάζουν, η εσκεμμένη χρήση εσφαλμένων checksum, μικρές τιμές TTL κ.α. Τέτοια συμβάντα είναι σπάνια στην κανονική κίνηση, γιατί αλλιώς το σύστημα ανίχνευσης επιθέσεων θα είχε προγραμματιστεί να τα διαχειρίζεται αναλόγως.

4.9 Παρουσίαση DDoS σε Web Server

Στην παρουσίαση της πτυχιακής εργασίας χρησιμοποιήθηκαν 2 laptop. Στο πρώτο είχε γίνει format σε λογισμικό *Linux Ubuntu 16.04*.

Σχήμα 4.6: *Ubuntu 16.04*

Μετά την εγκατάσταση του λογισμικού σειρά είχε η εγκατάσταση Server και συγκεκριμένα ένας Web, Mail, Mailinglist, DNS και FTP Server μέσω του πάνελ της *ISPConfig 3.1*.



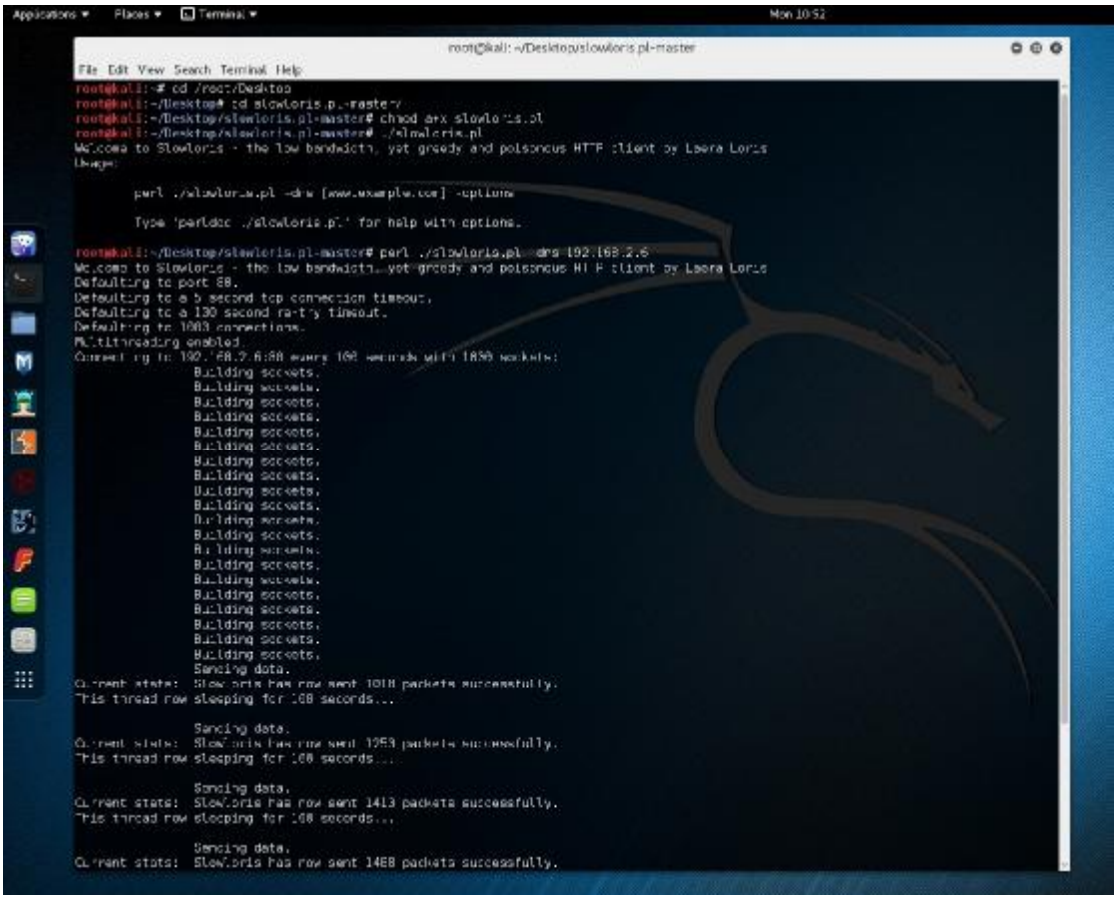
Σχήμα 4.7: *Η αρχική σελίδα του server.*

Κατά την διάρκεια του setup τοποθετήθηκε και firewall στον Server. Συγκεκριμένα το ***UFW*** υπήρχε ως προεπιλογή και ενεργοποιήθηκε με την παρακάτω εντολή:

- *apt-get install ufw*

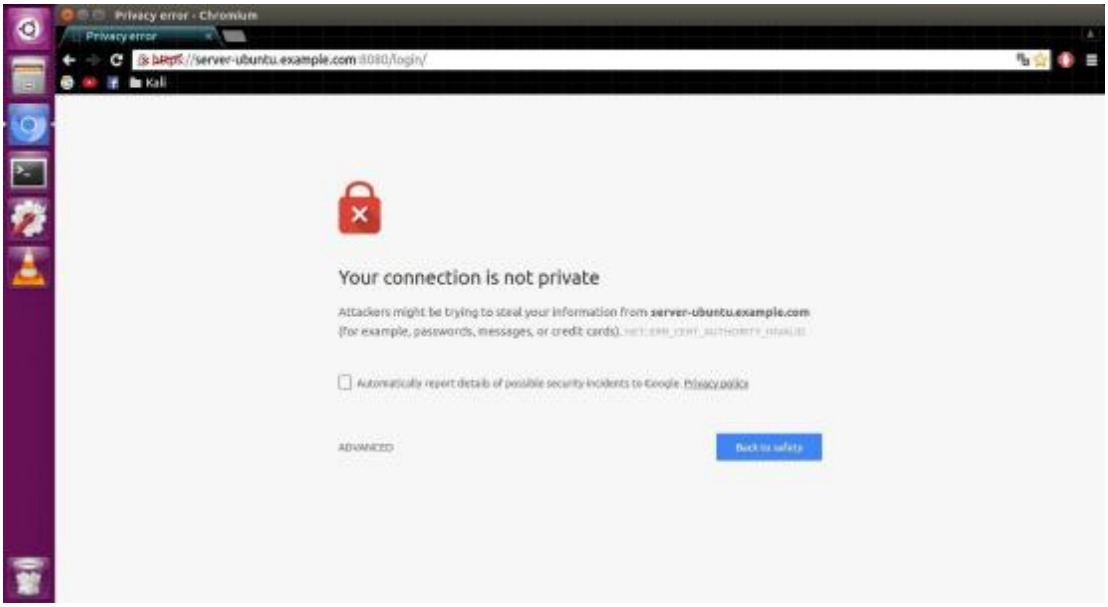
Το δεύτερο laptop περιείχε λογισμικό *Windows 10 Pro*. Εντούτοις πάνω στα windows εγκαταστάθηκε μια εικονική μηχανή (virtual machine) και συγκεκριμένα η *VMware Workstation Pro 12* μέσω της οποίας ανοίγουμε περιβάλλον *Linux Kali 2*.

Έτσι λοιπόν, με τη χρήση ενός συγκεκριμένου tool τρέχουμε τις παρακάτω εντολές σε ένα τερματικό, όπως φαίνεται στο παρακάτω σχήμα:



Σχήμα 4.8: *Η διαδικασία επίθεσης DDoS στέλνει 1000 sockets κάθε 100 δευτερόλεπτα υπερφορτώνοντας τον server.*

Μετά από μερικά δευτερόλεπτα ο server παρουσιάζει το παρακάτω μήνυμα:



Σχήμα 4.9: *Ο "πεσμένος" server.*

Βιβλιογραφία

[1] N. Weiler, Honeypots for Distributed Denial of Service, in: Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109–114.

[2] R.B. Lee, Taxonomies of Distributed Denial of Service networks, attacks, tools and countermeasures, Princeton University, Available from <http://www.ee.princeton.edu/~rblee>.

[3] J. Mirkovic, G. Prier, P. Reiher, Attacking DDoS at the source, in: Proceedings of ICNP 2002, Paris, France, 2002, pp. 312–321.

[4] Cisco, NetRanger Overview, Available from <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/overview.htm>.

[5] Mimestar.com, SecureNet PRO Feature List, Available from <http://www.mimestar.com/products>.

[6] The Open Source Network Intrusion Detection System: Snort, Available from <http://www.snort.org>.

[7] S. Bellovin, The ICMP traceback message, Network Working Group, Internet Draft, March 2000, Available from <http://www.research.att.com/~smb/papers/draftbellovin-itrace-00.txt>.

[8] S. Savage, D. Wetherall, A. Karlin, T. Anderson, Network support for IP traceback, IEEE/ACM Transaction on Networking 9 (3) (2001) 226–237.

[9] W. Zhao, D. Olshefski, H. Schulzrinne, Internet Quality of Service: an overview, Columbia Technical Report CUCS-003-00, 2000.

[10] J. Brustoloni, Protecting electronic commerce from Distributed Denial of Service attacks, in: Proceedings of the 11th International World Wide Web Conference, ACM, Honolulu, HI, 2002, pp. 553–561.

[11] S.M. Mankins, C. Sangpachatanaruk, T. Znati, R. Melhem, D. Moss, Proactive server roaming for mitigating Denial of Service attacks, in: Proceedings of 1st International Conference on Information Technology Research and Education (ITRE), Newark, NJ, USA, August 10–13, 2003.

[12] J. Ioannidis, S.M. Bellovin, Implementing pushback: router-based defense against DDoS Attacks, in: Proceedings of Network and Distributed System Security Symposium, NDSS_02, San Diego, CA, 2002, pp. 6–8.

[13] ISO/TC97/SC16. Reference model of open systems interconnection. Tech. Rep. N. 227, International Organization for Standardization, June 1979.

[14] AXELSSON, S. Intrusion detection systems: A survey and taxonomy. Tech. Rep. 99-15, Dept. of Computer Engineering, Chalmers University of Technology, SE-412 96 Goteborg, Sweden, March 2000. http://www.ce.chalmers.se/staff/sax/taxonomy.ps Accessed 27 Feb 2002.

[15] BAI, Y., AND KOBAYASHI, H. Intrusion detection system: Technology and development. In AINA '03: Proceedings of the 17th International Conference on Advanced Information Networking and Applications (Washington, DC, USA, 2003), IEEE Computer Society, p. 710.

[16] PATTON, S., YURCIK, W., AND DOSS, D. An Achilles' heel in signature-based IDS: Squealing false positives in SNORT. In RAID 2001 Fourth International Symposium on Recent Advances in Intrusion Detection October 10–12, 2001, Davis, CA, USA (2001). Available online only. http://www.raid-symposium.org/raid2001/papers/patton_yurcik_doss_raid2001.pdf Accessed 3 January 2003.

[17] VIGNA, G., ROBERTSON, W., AND BALZAROTTI, D. Testing network-based intrusion detection signatures using mutant exploits. In Proceedings of the 11th ACM conference on Computer and communications security (2004), ACM Press, pp. 21–30.

[18] NING, P., JAJODIA, S., AND WANG, X. S. Abstraction-based intrusion detection in distributed environments. ACM Trans. Inf. Syst. Secur. 4, 4 (2001), 407–452.

[19] SEKAR, R., GUPTA, A., FRULLO, J., SHANBHAG, T., TIWARI, A., YANG, H., AND ZHOU, S. Specification-based anomaly detection: a new approach for detecting network intrusions. In Proceedings of the 9th ACM conference on Computer and communications security (2002), ACM Press, pp. 265–274.

[20] SOMAYAJI, A., HOFMEYR, S., AND FORREST, S. Principles of a computer immune system. In Meeting on New Security Paradigms, 23-26 Sept. 1997, Langdale, UK (New York, NY, USA, 1997), ACM, pp. 75–82.

[21] VARGIYA, R., AND CHAN, P. Boundary detection in tokenizing network application payload for anomaly detection. In Proceedings of the ICDM Workshop on Data Mining for Computer Security (DMSEC) (Nov. 2003), pp. 50–59. Workshop held in conjunction with The Third IEEE International Conference on Data Mining. Available at http://www.cs.fit.edu/˜pkc/dmsec03/dmsec03notes.pdf. Accessed 5 April 2006.

[22] MAHONEY, M. V., AND CHAN, P. K. Learning rules for anomaly detection of hostile network traffic. In ICDM '03: Proceedings of the Third IEEE International Conference on Data Mining (Washington, DC, USA, 2003), IEEE Computer Society, p. 601.

[23] EST´E VEZ-TAPIADOR, J. M., GARC´I A-TEODORO, P., AND D´I AZ-VERDEJO, J. E. Measuring normality in http traffic for anomaly-based intrusion detection. Journal of Computer Networks 45, 2 (2004), 175–193.

[24] MITCHELL, T. M. Artificial Neural Networks. WCB/McGraw-Hill, 1997, ch. 4, pp. 81–127.

[25] MUKKAMALA, S., JANOSKI, G., AND SUNG, A. Intrusion detection using neural networks and support vector machines. In 2002 International Joint Conference on Neural Networks (IJCNN), 12–17 May 2002, Honolulu, HI, USA (Piscataway, NJ, USA, 2002), vol. 2, IEEE, pp. 1702–1707. http://www.cs.nmt.edu/˜IT/papers/hawaii7.pdf Accessed 13 August 2002.

[26] AXELSSON, S. The base-rate fallacy and its implications for the difficulty of intrusion detection. In ACM Conference on Computer and Communications Security (1999), pp. 1–7. http://www.ce.chalmers.se/staff/sax/difficulty.ps Accessed 19 August 2002.

[27] HOFMEYR, S., AND FORREST, S. Immunity by design: an artificial immune system. In Proceedings GECCO-99. Genetic and Evolutionary Computation Conference. Eighth International Conference on Genetic Algorithms (ICGA-99) and the Fourth Annual Genetic Programming Conference (GP-99), 13-17 July 1999, Orlando, FL, USA (San Francisco, CA, USA, 1999), W. Banzhaf, J. Daida, A. Eiben, M. Garzon, V. Honavar, M. Jakiela, and R. Smith, Eds., Morgan Kaufmann Publishers, pp. 1289–96 vol.2.

[28] Matthew V. Mahoney, Philip K. Chan, “Learning Models of Network Traffic for Detecting Novel Attacks”, Florida Tech. technical report 2002-08.

[29] Δημήτρης Γαβρίλης, “Αναγνώριση επιθέσεων άρνησης εξυπηρέτησης”, Διδακτορική διατριβή, Πανεπιστήμιο Πατρών, Πάτρα 2007.

[30] Kenneth III Ingham, “Anomaly detection for HTTP intrusion detection : algorithm comparisons and the effect of generalization on accuracy”, Ph.D. dissertation, Univ. of New Mexico, Albuquerque 2007.

[31] Christos Douligeris, Aikaterini Mitrokotsa “DDoS attacks and defense mechanisms: classification and state-of-the-art”.

[32] https://en.wikipedia.org/wiki/Local_area_network

[33] https://en.wikipedia.org/wiki/Wireless_LAN

[34] https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[35] https://en.wikipedia.org/wiki/Cryptography

[36] https://en.wikipedia.org/wiki/Denial-of-service_attack

[37] http://www.ispconfig.org/

[38] http://www.ubuntu.com/

[39] https://www.howtoforge.com/tutorial/perfect-server-ubuntu-16.04-with-apache-php-myqsl-pureftpd-bind-postfix-doveot-and-ispconfig/