ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Λογισμικού και Πληροφοριακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών στο Διαδίκτυο των Πραγμάτων

DDoS Attacks on the IoT

Μάγγου Μαριάνθη
Α.Μ. 19049

Εισηγήτρια: Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια

Αθήνα, Ιούνιος 2021

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών στο Διαδίκτυο των Πραγμάτων

DDoS Attacks on the IoT

Μάγγου Μαριάνθη
Α.Μ. 19049

Εισηγήτρια:

Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια

Εξεταστική Επιτροπή:

Καντζάβελου, Επίκουρη Καθηγήτρια
Ioanna Kantzavelou
Digitally signed by Ioanna Kantzavelou
Date: 2021.07.16 14:25:29 +03'00'

Μάμαλης, Καθηγητής
Vasileios Mamalis
Digitally signed by Vasileios Mamalis
Date: 2021.07.17 01:37:20 +03'00'

Μπόγρης, Καθηγητής
Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2021.07.16 18:25:21 +03'00'

Ημερομηνία εξέτασης 13/ 7/ 2021

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Μάγγου Μαριάνθη του Βασιλείου, με αριθμό μητρώου mcse 19049 φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών Επιστήμη της Πληροφορικής και των Υπολογιστών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Η Δηλούσα

Μάγγου Μαριάνθη

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά την κ. Καντζάβελου Ιωάννα που μου έδωσε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον και σύγχρονο θέμα, για τη καθοδήγηση και τη συνεργασία της σε όλη τη διάρκεια της διπλωματικής εργασίας. Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου και το σύζυγό μου Γιώργο, για τη στήριξη και την βοήθεια που μου προσέφεραν σε όλη τη διάρκεια των σπουδών μου στο μεταπτυχιακό πρόγραμμα “Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών” του Πανεπιστημίου Δυτικής Αττικής.

Τέλος αφιερώνω την διπλωματική μου εργασία, στα δύο παιδιά μου Τριανταφυλλιά και Βασιλική με την ευχή να ακολουθούν πάντα τα όνειρά τους, μέχρι να καταφέρουν να γίνουν πραγματικότητα.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία ασχολείται με το IoT - (Διαδίκτυο των Πραγμάτων) και τις DDoS επιθέσεις – (Κατανεμημένη Άρνηση Υπηρεσιών) που δέχεται, καθώς και με ποιους τρόπους μπορεί να γίνει ανίχνευση και αποτροπή των DDos επιθέσεων. Το IoT περιλαμβάνει οποιαδήποτε ηλεκτρική ή ηλεκτρονική συσκευή που συνδέεται στο ίντερνετ χωρίς να είναι υπολογιστής, κινητό, ή tablet. Στόχος του IoT είναι δώσει στους χρήστες όσο γίνεται μεγαλύτερο έλεγχο διαφορετικών συσκευών μέσω διαδικτύου και εξ' αποστάσεως. Ο άνθρωπος, για να επικοινωνήσει με τις IoT συσκευές, χρειάζεται τις αντίστοιχες εφαρμογές, για κινητά ή και υπολογιστές. Το IoT - Internet of Things είναι ένα τεράστιο δίκτυο συνδεδεμένων συσκευών και ανθρώπων, τα οποία συλλέγουν και μοιράζονται δεδομένα, προσφέρουν πολλές υπηρεσίες αλλά και δυνατότητες επικοινωνίας και ενημέρωσης. Αποτελεί την εξέλιξη και το μέλλον του διαδικτύου και επηρρεάζει την καθημερινότητά μας σε σημαντικό βαθμό. Τα πλεονεκτήματα που μας δίνει είναι πολλά, όμως ο τομέας που χρειάζεται περαιτέρω εξέλιξη και έρευνα είναι αυτός της ασφάλειας. Τα IoT δέχονται πολλές επιθέσεις τις οποίες θα ερευνήσουμε στη παρούσα διπλωματική. Θα ερευνηθεί η επίθεση κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service - DDoS), που συμβαίνει όταν ένας εισβολέας επιχειρεί να καταστήσει αδύνατη την παροχή μιας υπηρεσίας. Αυτή μπορεί να επιτευχθεί αποτρέποντας την πρόσβαση σε οτιδήποτε όπως: servers, συσκευές, υπηρεσίες, δίκτυα, εφαρμογές ακόμη και σε συγκεκριμένες συναλλαγές εντός των εφαρμογών. Υπάρχουν πολλοί διαφορετικοί τρόποι ανίχνευσης και αντιμετώπισης των DDoS επιθέσεων, παρόλαυτα οι επιθέσεις συνεχίζονται με αμείωτο ρυθμό, πετυχαίνοντας τις πιο πολλές φορές το στόχο τους.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ασφάλεια, DDoS Επιθέσεις, IoT, Άρνηση Υπηρεσιών, Botnet, Ανίχνευση, ‘Αμυνα, Ηλεκτρονικό Εμπόριο, Οικιακές Συσκευές, Τομέας Υγείας, Ασαφείς Εκτιμητές, Ασύρματα Δίκτυα, Flood, Εξόρυξη Δεδομένων, Μηχανική Εκμάθηση, Συστήματα Ταξινόμησης, Μετριασμού και Πρόληψης.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ:
Ασφάλεια Ηλεκτρονικών Υπολογιστών στο Διαδίκτυο των Πραγμάτων

ABSTRACT

The present thesis concerns the development of IoT - (Internet of Things) and DDoS - (Distributed Denial of Service) attacks, as well as ways in which DDoS attacks can be detected and prevented. IoT includes any electrical or electronic device that connects to the Internet without being a computer, mobile phone, or tablet. The goal of the IoT is to give users as much control as possible over different devices over the internet and remotely. Man, in order to communicate with IoT devices, needs the corresponding applications, for mobile phones or even computers. IoT – Internet of Things is a huge network of connected devices and people, who collect and share data, offer many services and communication and information capabilities. It is the evolution and the future of the internet and it influences our daily life to a great extent. The advantages it gives us are many, but the area that needs further development and research is that of security. IoTs are under a lot of attack which we will investigate in this dissertation. The distributed denial of service (DDoS) attack, which occurs when an attacker attempts to make it impossible to provide a service, will be investigated in more detail. This can be achieved by preventing access to anything such as: servers, devices, services, networks, applications and even specific transactions within applications. There are many different ways to detect and deal with DDoS attacks, however the attacks continue at a steady pace, most often achieving their goal.

KEY WORDS: Security, DDoS Attacks, IoT, Denial of Service, Botnet, Detection, Defense, E-Commerce, Home Appliances, Health Sector, Fuzzy Estimators, Wireless Networks, Flood, Data Mining, Machine Learning, Classification and Pre-Classification Systems.

SCIENTIFIC AREA:

Computer Security on the Internet of Things

Πίνακας Περιεχομένων

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο αναλύεται το αντικείμενο της διπλωματικής εργασίας και γίνεται μια ιστορική αναδρομή σχετικά με το IoT και τις Επιθέσεις DDos.

1.1 Περιγραφή του αντικειμένου της διπλωματικής εργασίας

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι οι Κατανεμημένες επιθέσεις Άρνησης Υπηρεσιών στο διαδίκτυο των πραγμάτων, γνωστό και ώς DDos on IoT – Internet of Things. Αρχιτεκτονική IoT και τομείς εφαρμογής. Τύποι Δικτύων και Πρωτόκολλα. Δυνατότητες και αδυναμίες στην ασφάλεια του IoT. Είδη επιθέσεων DDos και μέθοδοι ανίχνευσης. Ασφάλεια για τους χρήστες και τους οργανισμούς απο τις DDos επιθέσεις σε συσκευές του IoT. Στο τέλος θα παρουσιαστεί προτινόμενος μηχανισμός ανίχνευσης για την αντιμετώπιση DDoS επιθέσεων σε συσκευή του IoT.

1.2 Ιστορική αναδρομή DoS Επιθέσεων

Οι επιθέσεις DoS υπήρχαν κατά τη διάρκεια της δεκαετίας του 1980, αλλά στην αρχή δεν έγινε αντιληπτό, ότι αποτελούσαν μεγάλο κίνδυνο για την ασφάλεια των υπολογιστικών συστημάτων. Αυτό άλλαξε καθώς το Διαδίκτυο γινόταν το σημαντικότερο μέσο επικοινωνίας. Τον Σεπτέμβριο του 1996, μια επίθεση DoS του «SYN Flood» έκανε τον πάροχο υπηρεσιών Internet της Νέας Υόρκης Panix, να βγει εκτός σύνδεσης για μια εβδομάδα, ενώ οι επόμενες επιθέσεις κατάφερα να απενεργοποίιήσουν τους servers του Internet Chess Club και των New York Times. Δύο μήνες αργότερα, κυκλοφόρησε το πρώτο εμπορικό προϊόν ειδικά σχεδιασμένο για επιθέσεις DoS. [1]

Μπορούσε να εντοπίζει επιθέσεις παρακολουθώντας εισερχόμενα πακέτα SYN και να επαναφέρει τις συνδέσεις, όταν ο υπολογιστής που δεχόταν την επίθεση λάμβανε κίνηση δεδομένων με ρυθμό υψηλότερο από ένα συγκεκριμένο όριο. Ωστόσο, απέτυχε να σταματήσει μια επίθεση στον κύριο server της Webcom, η οποία κατάφερε να θέσει εκτός σύνδεσης, χιλιάδες εμπορικούς ιστότοπους. Ο εισβολέας είχε τυχαιοποιήσει τις διευθύνσεις IP και το ποσοστό επίθεσης ήταν 200 πακέτα / δευτερόλεπτο, το οποίο ήταν πολύ υψηλό εκείνη τη στιγμή.

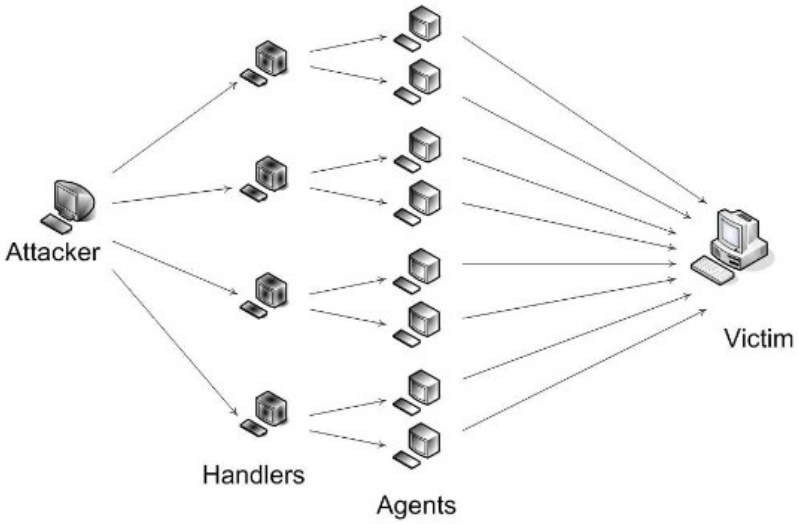
Στις επιθέσεις "SYN Flood", το επιτιθέμενο σύστημα στέλνει μηνύματα SYN στο σύστημα διακομιστή θύματος (victim server system), που φαίνεται να είναι νόμιμο, αλλά στην πραγματικότητα, δεν μπορεί να ανταποκριθεί στα μηνύματα SYN / ACK. Έτσι το τελικό μήνυμα ACK δεν θα σταλεί ποτέ στο victim server system, που γίνεται η επίθεση και λόγω των πολλών ημι-ανοιχτών συνδέσεων, το σύστημα δεν θα μπορεί να δεχτεί νέες εισερχόμενες συνδέσεις.[1]

Τον Ιανουάριο του 1997, ένας έφηβος που ονομαζόταν Khan C. Smith επιτέθηκε στο δίκτυο IRC Undernet και σε αρκετούς ISP στη Νορβηγία, τη Ρουμανία, το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες, με συνδυασμό επιθέσεων «ping» και «SYN Flood». Σε κάθε server που συνδεόταν, αποκτούσε πρόσβαση root, διέγραφε αρχεία και ακύρωνε λογαριασμούς. Η «επίθεση ping», είναι μια από τις πιο απλές επιθέσεις DoS, όπου το θύμα λαμβάνει περισσότερα πακέτα TCP / ICMP, από ό, τι μπορεί να χειριστεί. Στις «IRC-based DDoS attacks», χρησιμοποιείται ένα κανάλι επικοινωνίας IRC για τη σύνδεση του client με τους agents. Οι εισβολείς μπορούν να χρησιμοποιήσουν νόμιμες θύρες IRC για την αποστολή εντολών στους πράκτορες, κάτι που κάνει την παρακολούθηση τους πιο δύσκολη, επειδή οι servers IRC, συνεχίζουν να λαμβάνουν μεγάλους όγκους κυκλοφορίας.[1]

Τον Ιανουάριο του 1998, το DALnet και άλλα δίκτυα IRC έγιναν στόχοι του «smurfing», όπου ο εισβολέας χρησιμοποιεί πακέτα αιτημάτων echo ICMP που κατευθύνονται σε διευθύνσεις εκπομπής IP, από απομακρυσμένες τοποθεσίες για να δημιουργήσουν επιθέσεις DoS. Υπάρχουν τρία μέρη σε αυτές τις επιθέσεις: ο εισβολέας, ο μεσάζων και το θύμα. Ο διαμεσολαβητής λαμβάνει ένα πακέτο αιτήματος echo ICMP, που κατευθύνεται στη διεύθυνση εκπομπής IP του δικτύου του. Αν ο διαμεσολαβητής δεν φιλτράρει την κυκλοφορία ICMP που κατευθύνεται σε διευθύνσεις εκπομπής IP, πολλά από τα μηχανήματα στο δίκτυο θα λάβουν αυτό το πακέτο αιτήματος echo ICMP και θα στείλουν το ίδιο. Όταν όλα τα μηχανήματα ενός δικτύου ανταποκρίνονται σε αυτό το ICMP echo request, το αποτέλεσμα μπορεί να είναι μια μεγάλη συμφόρηση και στη συνέχεια η διακοπή του δικτύου. Παρόμοια είναι η επίθεση "fraggle", η οποία χρησιμοποιεί πακέτα UDP αντί πακέτα echo ICMP.[1]

Κατά την ίδια περίοδο, το Πεντάγωνο, η NASA, πολλά αμερικανικά συστήματα στρατιωτικών δικτύων και εκατοντάδες πανεπιστήμια έγιναν στόχος επιθέσεων DoS που ξεκίνησαν από έναν έφηβο από το Ισραήλ. Ο χάκερ χρησιμοποίησε κυρίως τεχνικές "Teardrop" και "Bonk", οι οποίες εκμεταλλεύτηκαν γνωστά τρωτά σημεία των λειτουργικών συστημάτων Microsoft Windows και πέτυχαν σε εκείνους τους υπολογιστές, που δεν ήταν ενημερωμένοι με τις πιο πρόσφατες ενημερώσεις ασφαλείας. Οι επιθέσεις "Teardrop" εκμεταλλεύονται το γεγονός ότι το Πρωτόκολλο Διαδικτύου απαιτεί κατακερματισμό των πακέτων που είναι πολύ μεγάλα για να χειριστεί ο επόμενος δρομολογητής. Κάθε κατακερματισμένο πακέτο προσδιορίζει μια μετατόπιση στην αρχή του πρώτου πακέτου που επιτρέπει σε ολόκληρο το πακέτο να επανασυναρμολογηθεί από το σύστημα λήψης.[1]

Εικόνα 1.1: DDoS Επίθεση [1]



Ένα μήνα μετά την κυκλοφορία της σχετικής ενημερωμένης έκδοσης κώδικα από τη Microsoft, προέκυψε μια νέα ποικιλία Teardrop, το "Bonk", το οποίο δούλεψε συγκεκριμένα, σε μια ευπάθεια που δημιουργήθηκε. Τον Αύγουστο του 2004, ένα εκτελεστικό στέλεχος της Μασαχουσέτης κατηγορήθηκε ότι με την πρόσληψη χάκερ, ξεκίνησε επιθέσεις DoS και προκάλεσε συνολικές απώλειες 2 δισεκατομμυρίων δολαρίων σε τρεις ανταγωνιστές. Οι επιθέσεις είχαν ξεκινήσει τον Οκτώβριο του 2003 και ήταν κυρίως SYN και HTTP Floods. Σε ένα "HTTP Flood", ο εισβολέας χρησιμοποιεί μεγάλο αριθμό παραβιασμένων υπολογιστών που ταυτόχρονα και ζητούν περιεχόμενο ιστού, όπως εικόνες, από έναν ιστότοπο θύματος. [1]

Μια παραλλαγή είναι η επίθεση "HTTP Spidering", η οποία ξεκινά από έναν δεδομένο σύνδεσμο HTTP και στη συνέχεια ακολουθεί όλους τους συνδέσμους στον ιστότοπο με αναδρομικό τρόπο, εμπνευσμένο από τον τρόπο με τον οποίο οι μηχανές αναζήτησης συλλέγουν τα δεδομένα τους.Μια επίθεση επιπέδου εφαρμογής DDoS (μερικές φορές αναφέρεται ως επίθεση επιπέδου 7 DDoS) είναι μια μορφή επίθεσης DDoS όπου οι εισβολείς στοχεύουν σε διεργασίες επιπέδου εφαρμογής. Η επίθεση υπερ-ασκεί συγκεκριμένες λειτουργίες ή χαρακτηριστικά ενός ιστότοπου με σκοπό την απενεργοποίηση αυτών των λειτουργιών ή λειτουργιών. Αυτή η επίθεση επιπέδου εφαρμογής είναι διαφορετική από μια ολόκληρη επίθεση στο δίκτυο και χρησιμοποιείται συχνά εναντίον χρηματοπιστωτικών ιδρυμάτων για να αποσπάσει την προσοχή του προσωπικού πληροφορικής και ασφαλείας από παραβιάσεις ασφαλείας. [1]

1.3 Πρόσφατες Τάσεις: 2004 έως 2014

Ομάδες εγκληματιών στον διαδίκτυο, ειδικεύονται στην παραβίαση μεγάλου αριθμού υπολογιστών οι οποίοι είναι ευάλωτοι σε επιθέσεις άρνησης υπηρεσίας. Κατασκευάζουν «armies of bots», από μερικές χιλιάδες έως και 1,5 εκατομμύρια υπολογιστές, και τα νοικιάζουν σε επιθέμενους DoS. Τον Μάιο του 2006, ένας 20χρονος «botmaster» καταδικάστηκε σε ποινή φυλάκισης πέντε ετών για παραβίαση 500.000 υπολογιστών. Πουλούσε πρόσβαση σε αυτούς και σε άλλους χάκερ, οι οποίοι τους χρησιμοποίησαν για να ξεκινήσουν επιθέσεις Dos και να στέλνουν μηνύματα spam.[1]

Οι επιθέσεις DoS ξεκινούν από την αρχή των δικτύων υπολογιστών, αλλά δεν θεωρήθηκαν σημαντικό θέμα έρευνας μέχρι που άρχισαν να βλάπτουν ISP, κυβερνητικούς ιστότοπους και το ηλεκτρονικό εμπόριο. Η αποτελεσματικότητα αυτών των επιθέσεων και η επακόλουθη δημοσιότητά τους προκάλεσαν την εισροή νεότερων και ακόμη πιο αποτελεσματικών τεχνικών επίθεσης ενάντια σε ένα όλο και πιο ευρύ φάσμα στόχων. Καθώς οι τεχνικές DoS διανέμονται και ισχυρά εργαλεία επίθεσης είναι άμεσα διαθέσιμα στο Διαδίκτυο, έγινε γρήγορα εμφανές ότι το DoS δεν μπορεί να αντιμετωπιστεί με τον ίδιο τρόπο όπως και άλλα θέματα ασφάλειας υπολογιστών. Για παράδειγμα, οι ιοί αντιμετωπίζονταν πάντοτε με ειδικό λογισμικό προστασίας από ιούς που εκτελείται στον υπολογιστή του θύματος, αλλά οι επιθέσεις DoS στοχεύουν να συντρίψουν εντελώς τον target resource (πόρο-στόχο), έτσι ώστε το θύμα να μην μπορεί να χρησιμοποιήσει μόνο του άμυνα (defence) . Το Διαδίκτυο λειτουργεί με παλιά πρωτόκολλα δικτύωσης, τα οποία προσφέρουν περιορισμένη πρόβλεψη ασφάλειας και αυτό είναι ένα ακόμη πλεονέκτημα για τους επιτιθέμενους. [1]

Το 2013, οι επιθέσεις DDoS επιπέδου εφαρμογής αντιπροσώπευαν το 20% όλων των επιθέσεων DDoS.

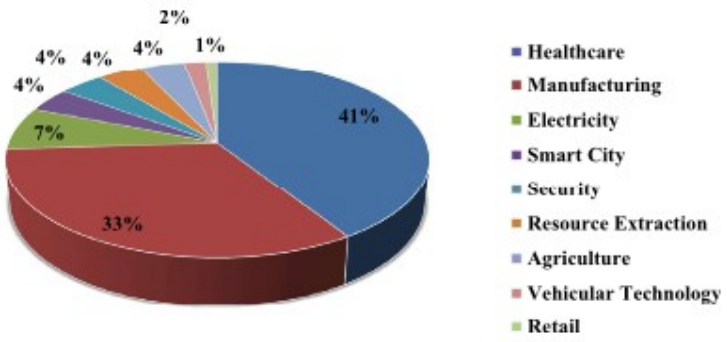
1.4 Ιστορικά Στοιχεία IoT

Η ιδέα της ύπαρξης έξυπνων αντικειμένων κυκλοφόρησε ήδη από τη δεκαετία του '80 όταν εγκαταστάθηκε ο πρώτος διανομέας αναψυκτικών με σύνδεση στο Διαδίκτυο στο Πανεπιστήμιο Carnegie Mellon. Αυτό το μηχάνημα μπόρεσε να κοινοποιήσει τον αριθμό των ποτών που απομένουν και αν είναι αρκετά κρύα ή όχι στον κατάλογό του. Η προσπάθεια αυτοματισμού των καθημερινών μας συσκευών έγινε για πρώτη φορά τη δεκαετία του '90, μεταφέρωντας δεδομένα σε πακέτα μικρού μεγέθους από τον ένα κόμβο στον άλλο. Η ιδέα της επικοινωνίας συσκευής σε συσκευή παρουσιάστηκε για πρώτη φορά από τον Bill Joy στο Παγκόσμιο Οικονομικό Φόρουμ το 1999. Την ίδια χρονιά ο Kevin Ashton επινόησε τον όρο «Διαδίκτυο των πραγμάτων». Με τον όρο IoT, ο Kevin Ashton είχε ως στόχο να ορίσει ένα διασυνδεδεμένο δίκτυο καθημερινών πραγμάτων με το WSN και το RFID, ως τις κύριες τεχνολογίες ενεργοποίησης. [15]

Το 2000 η LG, ανακοίνωσε ότι θα αναπτύξουν ψυγεία που μπορούν να συνδεθούν στο Διαδίκτυο. Κατά τη διάρκεια αυτής της περιόδου ο γραμμικός κώδικας ήταν ακόμα η πιο δημοφιλής τεχνολογία που χρησιμοποιείται στο λιανικό εμπόριο, ωστόσο, το 2003 η Walmart και το Υπουργείο Άμυνας των ΗΠΑ χρησιμοποιούσαν ευρέως την τεχνολογία RFID σε εμπορικό επίπεδο. Κατά τη διάρκεια του ίδιου έτους δημοσιεύθηκαν διάφορα άρθρα που συζητούσαν το Διαδίκτυο των πραγμάτων σε περιοδικά όπως το Guardian. Το 2005, το πρώτο άρθρο για το IoT δημοσιεύθηκε από την ITU-T. Κατά τη διάρκεια του 2011 κυκλοφόρησαν δημοσίως 2128 νέες διευθύνσεις IPv6, οι οποίες μπορούν να επιτρέψουν ένα τεράστιο σύνολο διευθύνσεων. Η Intel δημιούργησε μια ομάδα IoT το 2013 ακολουθούμενη από την Google το 2015, η οποία άρχισε να αναπτύσσει λειτουργικό σύστημα για το IoT.Τα τελευταία δύο χρόνια ο τρόπος με τον οποίο οι άνθρωποι αντιλαμβάνονται το IoT έχει αλλάξει δραστικά, λόγω της εξέλιξης των τεχνολογιών όπως τα ενσωματωμένα συστήματα και τα κυβερνο-φυσικά συστήματα. Μερικές πολύ πρόσφατες στατιστικές του IoT έχουν ως εξής: [15]

- Η Cisco εκτιμά ότι έως το 2020 θα υπάρχουν περίπου 3,5 συνδεδεμένες συσκευές ανά άτομο.
- Μέχρι το 2020, περίπου το 80% των καταναλωτικών υπηρεσιών θα χρησιμοποιούν IoT.
- Σύμφωνα με την IDC, οι παγκόσμιες δαπάνες IoT θα έχουν ετήσιο ρυθμό ανάπτυξης 15,6%, φθάνοντας τα 1,29 τρισεκατομμύρια δολάρια το 2020.
- Το IoT Analytics αναφέρει ότι η περιοχή της Βόρειας Αμερικής αναμένεται να έχει το υψηλότερο CAGR 36% έως το 2021. Ωστόσο, η Ασία θα αναδειχθεί ως η μεγαλύτερη ηπειρωτική αγορά με 616 εκατομμύρια δολάρια έως το 2021.
- Σύμφωνα με το ITAT Analytics, το Smart Cities θα έχει τη μεγαλύτερη ανάπτυξη στο IoT, με CAGR 54% για περίοδο 6 ετών [15].

Εικόνα 1.1: Οικονομικό Αντίκτυπο του IoT [15]



Πίνακας 1. Εγκατεστημένες μονάδες IoT ανά κατηγορία (εκατομμύρια μονάδες). [15]

Category	2016	2017	2018	2020
Consumer services	4000	5250	7,000	12,800
Business: Technology wise	1100	1500	2,100	4,400
Business: Sector wise	1310	1650	2,000	3,200
Grand total	**6410**	**8400**	**11,100**	**20,400**

1.5 IoT – Internet of Things

Το Internet of Things (Διαδίκτυο των πραγμάτων) είναι η έννοια της σύνδεσης οποιασδήποτε συσκευής (εφόσον διαθέτει διακόπτη on / off) στο Διαδίκτυο και με άλλες συνδεδεμένες συσκευές. Το IoT είναι ένα τεράστιο δίκτυο συνδεδεμένων πραγμάτων και ανθρώπων - τα οποία συλλέγουν και μοιράζονται δεδομένα, σχετικά με τον τρόπο που χρησιμοποιούνται και όσον αφορά το περιβάλλον γύρω τους. [23]

Εδώ περιλαμβάνονται πολλά αντικείμενα όπως : τα self-driving αυτοκίνητα, των οποίων οι αισθητήρες είναι σε θέση να εντοπίζουν αντικείμενα που υπάρχουν στην πορεία τους και αυτόματα να επιβραδύνουν το όχημα ή και να το σταματούν αν υπάρχει κίνδυνος. Οι φορητές συσκευές άσκησης, που μπορούν να μετρήσουν τον καρδιακό ρυθμό και τον αριθμό των βημάτων και στην συνέχεια να χρησιμοποιούν αυτά τα στοιχεία για να προτείνουν ασκήσεις προσαρμοσμένες για κάθε άτομο. Οι έξυπνοι φούρνοι μικροκυμάτων, οι οποίοι μαγειρεύουν αυτόματα το φαγητό και για το σωστό χρονικό διάστημα. Τα ψυγεία που έχουν barcode readers και μπορούν να καταλάβουν αν υπάρχει έλλειψη ενός προϊόντος και σύμφωνα με τις προτιμήσεις μας να μας ενημερώσουν και να προβούν σε νέα παραγγελία διαδικτυακά. Οι μπάλες που είναι συνδεδεμένες (Connected Footballs) που μπορούν να εντοπίσουν πόσο γρήγορα και μακριά πετάχτηκαν, καθώς και να καταγράφουν τα στατιστικά μέσω μιας εφαρμογής για μελλοντικούς σκοπούς εκπαίδευσης. [23]

Οι συσκευές και τα αντικείμενα έχουν φτιαχτεί με αισθητήρες οι οποίοι είναι συνδεδεμένοι σε μία πλατφόρμα IoT, η οποία ενσωματώνει δεδομένα απο τις συσκευές και χρησιμοποιώντας ανάλυση στοιχείων βρίσκει πολύτιμες πληροφορίες μέσω των εφαρμογών που χρησιμοποιούν, ώστε να δημιουργηθεί βάση που να μπορεί να καλύψει συγκεκριμένες ανάγκες κάθε φορά. Η πλατφόρμα IoT μπορεί να εντοπίσει ποιές πληροφορίες είναι χρήσιμες και ποιές μπορούμε να τις αγνοήσουμε με ασφάλεια. Έτσι μπορούμε να παίρνουμε έξυπνες αποφάσεις εξοικονομώντας χρόνο και χρήμα. Γίνεται η αυτοματοποίηση πολλών εργασιών οι οποίες είναι επαναλαμβανόμενες, χρονοβόρες ή ακόμα και επίκινδυνες. [23]

IoT στο σπίτι

Οι εγκληματίες του κυβερνοχώρου αποτελούν μία απο τις μεγαλύτερες και σημαντικότερες κατηγορίες απειλών. Η επίθεση σε έξυπνα σπίτια λόγω του αυξανόμενου αριθμού έξυπνων συσκευών είναι συχνό φαινόμενο. Οι οικονομικοί παράγοντες δημιουργούν αδυναμίες ασφάλειας, ενώ οι σχεδιαστικές επιλογές ανταγωνίζονται το κόστος και την πρακτικότητα. Πολλοί από τους κινδύνους είναι κοινωνικοτεχνικής φύσης λόγω του βάθους και της ποικιλίας των προσωπικών πληροφοριών που μπορούν να καταγραφούν και να αποτελέσουν αντικείμενο επεξεργασίας, ενώ οδηγούν στην παραγωγή δεδομένων, για προηγουμένως μη καταγεγραμμένες δραστηριότητες, συνδέοντας στενά τους ανθρώπους και το περιβάλλον τους. Οι διαφορετικές απόψεις των ιδιοκτητών στο έξυπνο σπίτι δημιουργούν ένα περίπλοκο περιβάλλον όσον αφορά το θέμα της ασφάλειας . [35]

Υπάρχουν ζητήματα ασφάλειας από άποψη συνδεσιμότητας, ενσωματωμένης λειτουργικότητας, αδιαφανών συστημάτων και ασυμβατότητας με τις παραδοσιακές προσεγγίσεις ασφάλειας των πληροφοριών, καθώς και ζητήματα ιδιωτικότητας, πρόσβασης και δικαιωμάτων πνευματικής ιδιοκτησίας. Οι οικιακές συσκευές είναι από τις πρώτες που θα αγοραστούν σε πολλά σπίτια και για αυτό το λόγο αποτελούν τους στόχους των επιτιθέμενων. Λόγω των πολλαπλών τρόπων σχεδιασμού δεν δημιουργούνται όλα τα έξυπνα σπίτια ισότιμα. Όπως ακριβώς και σε πολλούς άλλους τομείς των ΤΠΕ, η εφαρμογή βασικής ασφάλειας των πληροφοριών μπορεί να αυξήσει σημαντικά τη γενική ασφάλεια στον τομέα του έξυπνου σπιτιού. Ο σχεδιασμός του έξυπνου σπιτιού ως συστήματος, μας δείχνει την προσεκτική εξέταση της ασφάλειας των σχεδίων έξυπνου σπιτιού που βασίζονται στο υπολογιστικό νέφος. Αποτελείται από ένα πλαίσιο απομόνωσης των εφαρμογών (όπως σχεδιάζεται για τα έξυπνα αυτοκίνητα) και διαχωρισμό του κρίσιμου λογισμικού από μη κρίσιμες εφαρμογές, αλλά και μέτρα ασφάλειας δικτύου και επικοινωνιών. [35]

*Ο εκτελεστικός διευθυντής **Udo Helmbrecht** δήλωσε: [1]«Το έξυπνο σπίτι είναι ένα σημείο έντονης επαφής ανάμεσα στη δικτυωμένη τεχνολογία των πληροφοριών και στον φυσικό χώρο, συνεπώς συνδυάζει κινδύνους ασφάλειας τόσο από το εικονικό όσο και από το φυσικό περιβάλλον. Ο εντοπισμός των απειλών στον κυβερνοχώρο είναι κρίσιμος για την προστασία του έξυπνου σπιτιού και ως εκ τούτου αποτελεί βασικό στοιχείο για τη διασφάλιση της επιτυχούς ανάπτυξής του».[35]*

1 Udo Helmbrecht “Είναι τα έξυπνα σπίτια ευφυή από άποψη ασφάλειας στον κυβερνοχώρο;” https://www.enisa.europa.eu Δελτίο Τύπου EPR06/2015

ΚΕΦΑΛΑΙΟ 2

Στο κεφάλαιο 2 γίνεται αναφορά στους κυριότερους τομείς του IoT όπως είναι: η υγεία (ιατρικές συσκευές – ο βηματοδότης), η βιομηχανία (αυτοματισμοί ICS – SCADA), το ηλεκτρονικό εμπόριο, ο οικιακός τομέας (το έξυπνο σπίτι), ο τομέας μεταφορών (οχήματα – αυτοματοποιημένο φρενάρισμα) και ο οικονομικός τομέας (τράπεζες – έξυπνες συσκευές).

Ταξινόμηση συσκευών στο IoT

Η μέθοδος κατηγοριοποίησης (Classification), με χρήση domains είναι σημαντική, γιατί ασχολείται με την οργάνωση των μελλοντικών συσκευών IoT. Οι συσκευές IoT χρησιμοποιούνται σε διαφορετικά πεδία: όπως η υγεία, οι καταναλωτές και για στρατιωτικούς σκοπούς. Κάθε συσκευή IoT ταξινομείται σε έναν τομέα ανάλογα με τις εφαρμογές του χρήστη. Οι τομείς είναι: σε Υγειονομική περίθαλψη, Χρηματοοικονομικό τομέα, Εμπόριο, Βιομηχανία και Προσωπική Χρήση. Οι συσκευές IoT μπορούν να χωριστούν σε δύο κατηγορίες. Στη πρώτη κατηγορία είναι προσωπική χρήση ή οι συσκευές που χρησιμοποιούνται κυρίως από μεμονωμένα άτομα. Στη δεύτερη κατηγορία ανήκει η εμπορική χρήση ή η χρήση από εταιρείες που ανήκουν σε διαφορετικούς κλάδους.[31]

2.1 Οικιακός Τομέας

Η περιοχή του home domain για IoT devices, αποτελείται από συσκευές που έχουν σχεδιαστεί για να διευκολύνουν τη ζωή των ανθρώπων και να αυτοματοποιούν τις επαναλαμβανόμενες εργασίες που γίνονται μέσα στο σπίτι. Τέτοια παραδείγματα συσκευών τεχνητής νοημοσύνης, είναι η Alexa και το Google Home, οι οποίες μπορούν να ελέγχουν και άλλες συσκευές IoT στο δίκτυο. Υπάρχουν συσκευές στο σπίτι για τον έλεγχο των φώτων, όπως το Philips Hue ή ελέγχουν τη θερμοκρασία όπως το Nest. Επίσης οικιακές συσκευές IoT είναι οι ηλεκτρικές σκούπες, οι συσκευές μαγειρέματος και οι αυτόματες συσκευές για ψώνια. Οι περισσότερες από αυτές τις συσκευές δεν διαθέτουν πολύ υψηλό επίπεδο ασφάλειας, με αποτέλεσμα να δημιουργούνται πολλά αδύναμα σημεία, που αν θέλει κάποιος μπορεί να τα εκμεταλλευτεί. Ενας εισβολέας μπορεί να εκμεταλλευτεί ένα τέτοιο αδύνατο σημείο, αποκτώντας πρόσβαση στο υπόλοιπο δίκτυο και επηρρεάζοντας τη καθημερινότητά μας. [4]

2.2 Τομέας Υγείας

Υπάρχουν πολλές εφαρμογές IoT που έχουν να κάνουν με την υγεία και συγκεκριμένα με αυτές που χρησιμοποιούν οι ασθενείς. Ορισμένες από αυτές τις εφαρμογές αποτελούνται από έξυπνους αισθητήρες, συσκευές απομακρυσμένης παρακολούθησης και επίσης αφομοίωση ιατρικών συσκευών. Αυτές οι συσκευές όχι μόνο μπορούν να διατηρήσουν τους ασθενείς ασφαλείς, αλλά μπορούν επίσης να βελτιώσουν τον τρόπο με τον οποίο οι γιατροί παρέχουν τη φροντίδα στους ασθενείς τους. [32]

Οι συσκευές IoT επιτρέπουν στους ασθενείς να αλληλεπιδρούν συχνά με τους γιατρούς τους από απόσταση. Όλες οι συνδεδεμένες συσκευές παράγουν ένα τεράστιο όγκο δεδομένων, που μπορεί να αποτελέσει πρόκληση για τη διαχείριση τους και την ασφάλειά τους. Όλα αυτά τα δεδομένα πρέπει να προστατεύονται και να διαχειρίζονται σωστά. Μία κοινή συσκευή σε αυτόν τον τομέα είναι ο βηματοδότης (**pacemaker**). Ο βηματοδότης είναι μια ιατρική συσκευή που τοποθετείται κάτω από το δέρμα , για να βοηθήσει στη ρύθμιση και τον έλεγχο του καρδιακού παλμού. Οι βηματοδότες άρχισαν να πωλούνται με δυνατότητα σύνδεσης σε Wi-Fi. Αυτή η ιδιαιτερότητα αυξάνει την ευκολία στην επικοινωνία μεταξύ του ασθενούς και του γιατρού, όμως ο κίνδυνος να δεχτούν επίθεση αυξάνεται. [32]

Πρέπει να ληφθούν πολλά μέτρα ώστε να διασφαλιστούν οι

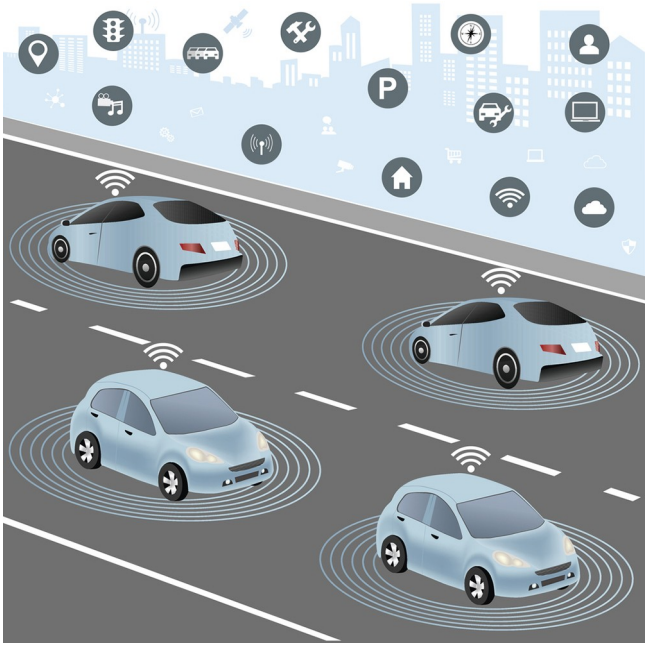
ευαίσθητες πληροφοριες που σχετίζονται με τον ασθενή:

Εμπιστευτικότητα (confidentiality) και Ακεραιότητα (integrity)

2.3 Τομέας Μεταφορών

Ο τομέας της μεταφοράς περιλαμβάνει τις ιδιωτικές μεταφορές και επιχειρηματικές μεταφορές. Οι νέες γενιές αυτοκινήτουν διαθέτουν υλικο και λογισμικό που μπορεί να ενημερωθεί και να έχει πρόσβαση μέσω του cloud. Αυτό επιτρέπει στους κατασκευαστές να ενημερώνουν τις ρυθμίσεις, καθώς και να επηρεάζουν την απόδοση καυσίμου όπως και την ατμοσφαιρική ρύπανση. Τα οχήματα έχουν μια ποικιλία αισθητήρων (sensors), τα οποία βοηθούν στη διατήρηση του οχήματος μέσα σε λωρίδες και το αυτοματοποιημένο φρενάρισμα (automated braking). Οι ενημερώσεις (updates) μπορούν να διορθώσουν τυχόν προβλήματα σε αυτά τα συστήματα. Για τις επιχειρήσεις μεταφοράς (enterprise transportation), υπάρχουν αισθητήρες που μπορούν να αναπτυχθούν και να παρακολουθούν τη διαχείριση του στόλου οχημάτων. [4]

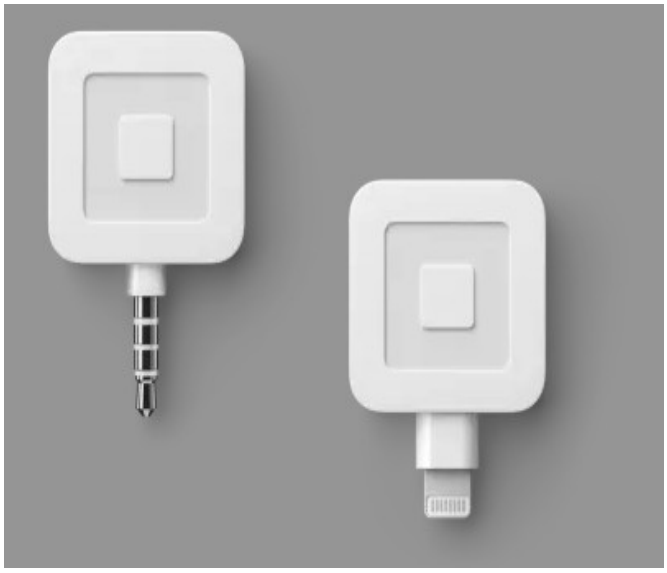
Εικόνα 2.1: Αυτόνομα Αυτοκίνητα IoT [39]



2.4 Ηλεκτρονικό Εμπόριο

Οι καταναλωτές χρησιμοποιούν όλο και πιο πολύ τις διαδικτυακές αγορές, γεγονός που κάνει τις συσκευές IoT να αναπτύσσονται συνεχώς, ώστε να καλύπτουν όλες τις ανάγκες και τισι επιθυμίες των χρηστών. Οι συσκευές IoT βοηθούν τόσο τα φυσικά καταστήματα λιανικής όσο και τις διαδικτυακές επιχειρήσεις λιανικής να συνεχίσουν τη λειτουργία τους, με μεγαλύτερη αποτελεματικότητα και ταχύτητα. Οι IoT συσκευές χρησιμοποιούνται όχι μόνο στα τερματικά σημείων πωλήσεων για την αγορά αγαθών από τους πελάτες, αλλά και για την εκτέλεση άλλων εργασιών, όπως είναι η αυτόματη παρακολούθηση του αποθέματος. Επιτρέπουν σε λίγα άτομα να λειτουργούν μικρότερες επιχειρήσεις, αλλά με περισσότερη ευκολία. Μια συσκευή που ονομάζεται Square card reader, είναι μια πιστωτική και χρεωστική κάρτα που είναι χρήσιμη για οδηγούς ταξί, υπηρεσίες παράδοσης φαγητού και άλλες μικρές εταιρείες. Μπορεί να μπεί σε smartphone και επιτρέπει στους πελάτες να σαρώνουν τις πιστωτικές ή χρεωστικές κάρτες τους, να κάνουν μια πληρωμή, χωρίς να απαιτούνται φυσικά χρήματα στη συναλλαγή. [4]

Εικόνα 2.2: Square Card Reader[25]



2.5 Οικονομικός Τομέας

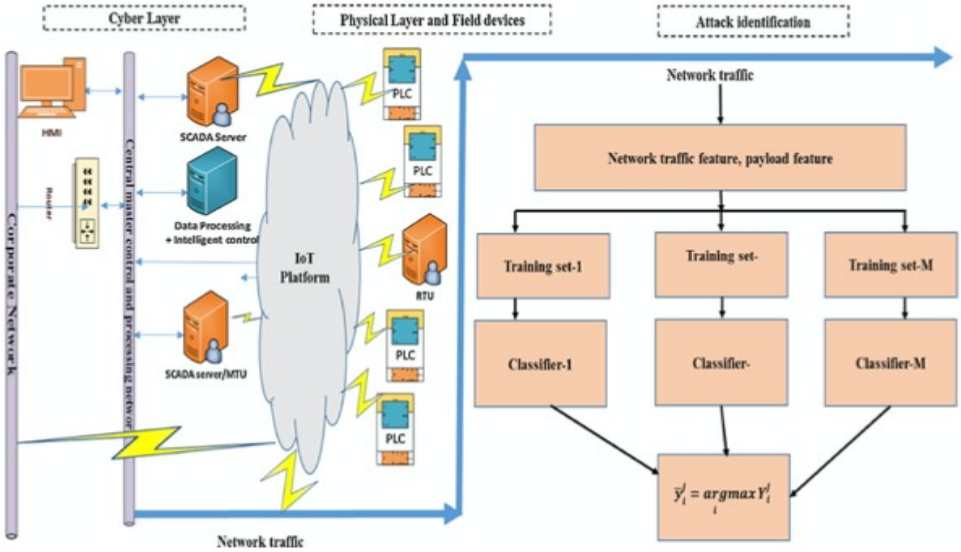
Οι συσκευές IoT στον οικονομικό τομέα συμβάλλουν στη μείωση του κόστους, στην αύξηση της παραγωγικότητας, στη βελτιστοποίηση των λειτουργιών και στη βελτίωση της ζωής. Έτσι η εμπειρία των πελατών στον τραπεζικό τομέα βελτιώνεται σημαντικά. Οι πελάτες χρησιμοποιούν τις έξυπνες συσκευές τους, για να αποκτήσουν πρόσβαση στις τραπεζικές τους πληροφορίες και να δουν μια πλήρη εικόνα των οικονομικών τους, σε πραγματικό χρόνο. Τα δεδομένα πελατών που διατίθενται μέσω συσκευών IoT βοηθούν τις τράπεζες να εντοπίσουν τις επιχειρηματικές ανάγκες των πελατών τους και να αποκτήσουν πληροφορίες για τους πελάτες. [33]

Ορισμένες χρηματοοικονομικές συσκευές περιλαμβάνουν ATM, εφαρμογή για κινητά Venmo και αναγνώστες καρτών Square card readers. Ένα από τα πιο σημαντικά οφέλη, είναι ότι παρέχει εύκολη πρόσβαση σε υπηρεσίες τόσο σε πελάτες πιστωτικών όσο και σε πελάτες χρεωστικών κάρτων. Παρολαυτά συχνές είναι οι παραβιάσεις της ασφάλειας δεδομένων. Γιαυτό το λόγο οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα συλλέγουν πολλές πληροφορίες από τους πελάτες, ώστε να διασφαλίσουν ότι δεν θα υπάρχουν εύκολες παραβίασεις δεδομένων, που θα μπορούσαν να οδηγήσουν σε σοβαρά προβλήματα τόσο για την τράπεζα όσο και για τον πελάτη. Η παραβίαση δεδομένων και άλλες παραβάσεις μπορούν να προκαλέσουν ζημιά στους πελάτες και να βλάψουν τη σχέση τους με τα χρηματοπιστωτικά τους ιδρύματα. [33]

2.6 Βιομηχανικός Τομέας

Τα συστήματα που βασίζονται σε cloud-based systems, στον βιομηχανικό τομέα περιλαμβάνουν βιομηχανικά συστήματα ελέγχου (industrial control systems - ICS), εποπτικό έλεγχο και απόκτηση δεδομένων (supervisory conrol and data acquisition - SCADA) και προγραμματιζόμενους λογικούς ελεγκτές (programmable logic controllers - PLC). Αυτά τα συστήματα ελέγχουν τον κατασκευαστικό εξοπλισμό, καθώς και όργανα, όπως τους αισθητήρες πίεσης. Τα συστήματα ελέγχου βασίζονται σε μεγάλο βαθμό σε παλαιότερες τεχνολογίες και είναι δύσκολο να αναβαθμιστούν και να διορθωθούν. Ο τομέας περιλαμβάνει επίσης συσκευές που βοηθούν στον αυτοματισμό, αυτοματοποιούν το πότισμα, τη σίτιση και την καλλιέργεια. Αυτό περιλαμβάνει αισθητήρες που παρακολουθούν το περιεχόμενο του εδάφους και την υγρασία και το φως του ήλιου. Οι αγρότες μπορούν να χρησιμοποιήσουν αυτά τα εργαλεία για να μελετήσουν και να αποκτήσουν πληροφορίες σχετικά με την απόδοση των καλλιεργειών τους. [4]

Εικόνα 2.3 Προτεινόμενη ασφαλής αρχιτεκτονική για σύστημα βιομηχανικού ελέγχου SCADA-IoT. [38]



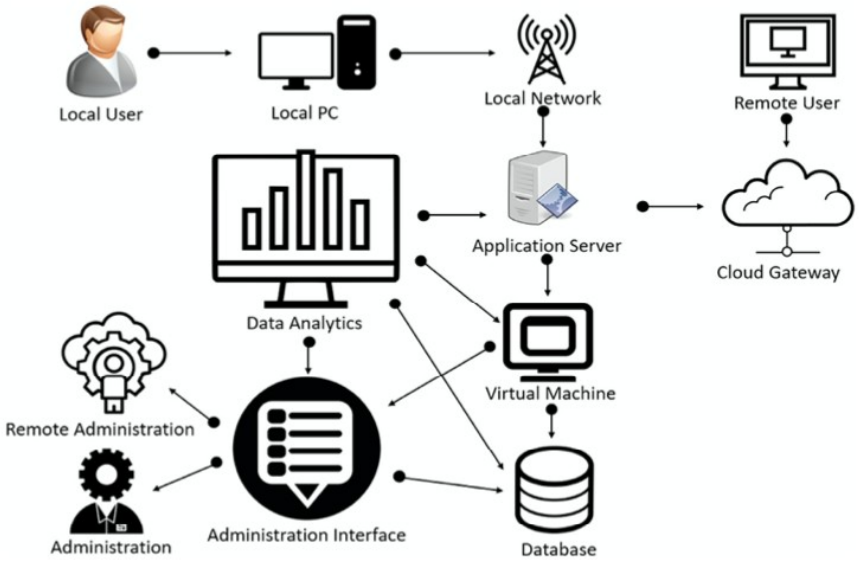
ΚΕΦΑΛΑΙΟ 3

Στο κεφάλαιο 3 υπάρχει αναφορά στην αρχιτεκτονική του IoT, τους τύπους δικτύων και τα λειτουργικά συστήματα που χρησιμοποιούνται στο IoT. Επίσης γίνεται μια πρώτη αναφορά στα προβλήματα ασφαλείας που υπάρχουν στο IoT.

3.1 Αρχιτεκτονική IoT

Το IoT - Internet of Things αποτελείται από συστήματα integrated objects, υπολογιστικών συσκευών (computing devices), ψηφιακών ή μηχανικών μηχανών(mechanical machines) που έχουν τη δυνατότητα να μεταδίδουν και να λαμβάνουν τα δεδομένα μέσω ενός δικτύου χωρίς την ανάγκη ανθρώπινης αλληλεπίδρασης. Κάθε μία από αυτές τις συσκευές μπορεί να λειτουργεί ανεξάρτητα εντός της υπάρχουσας υποδομής Διαδικτύου. Το IoT network μπορεί να είναι οτιδήποτε, όπως καθημερινοί απομακρυσμένοι χρήστες, προμηθευτές και προϊόντα. Αναγνωρίζοντας καταναλωτές και βασικούς προμηθευτές στη βιομηχανία τεχνολογίας πληροφοριών που έχουν εξέχουσα θέση στις τεχνολογίες και σχετίζονται με το Διαδίκτυο των πραγμάτων (IoT), μπορούμε να εντοπίσουμε κινδύνους ασφαλείας.

Εικόνα 3.1: Generic IoT Network Architecture [7]



Η συσκευή που χρησιμοποιείται στη παραπάνω εικόνα, έχει πρόσβαση στο τοπικό δίκτυο στο οποίο είναι συνδεδεμένη. Μόλις συνδεθεί, ο χρήστης αποκτά πρόσβαση στη διεπαφή της εφαρμογής. Η περίοδος σύνδεσης του κάθε χρήστη περιέχονται στην εικονική τους μηχανή(virtual machine). Αυτές οι συνεδρίες εκτελούνται στον application server. Η βάση δεδομένων περιέχει πληροφορίες λογαριασμού του χρήστη, καθώς και άλλα δεδομένα που δημιουργούνται από χρήστες και αρχεία καταγραφής χρήσης(usage logs).

Οι απομακρυσμένοι χρήστες (Remote users) δεν μπορούν να έχουν πρόσβαση σε τοπικά δίκτυα (local networks) και να συνδέονται σε μια πύλη cloud gateway. Στην άλλη πλευρά του δικτύου, ο administrator μπορεί να έχει πρόσβαση στη διεπαφή του διαχειριστή. Έτσι ο διαχειριστής, μπορεί να δει τα αναλυτικά στοιχεία δεδομένων (data analytics) που προέρχονται από τον server εφαρμογών και τις υπάρχουσες συνεδρίες. Ο διαχειριστής μπορει να παρακολουθεί την απόδοση της εφαρμογής (monitor application performance) και να εκτελεί εργασίες συντήρησης(upkeeping tasks). Κάθε διακεκομμένη γραμμή αντιπροσωπεύει ένα πιθανό σημείο εύκολου στόχου καθώς και τα σημεία επίθεσης. [7]

3.2 Τύποι δικτύων IoT

α)Τα **δίκτυα χαμηλής ισχύος και μικρής εμβέλειας** είναι κατάλληλα για σπίτια, γραφεία και άλλα μικρά περιβάλλοντα. Τείνουν να χρειάζονται μόνο μικρές μπαταρίες και συνήθως έχουν χαμηλό κόστος λειτουργίας. [21]

- **Bluetooth:** Είναι καλό για μεταφορά δεδομένων υψηλής ταχύτητας και στέλνει σήματα φωνής και δεδομένων έως και δέκα μέτρα.
- **NFC:** Ένα σύνολο πρωτοκόλλων επικοινωνίας για επικοινωνία μεταξύ δύο ηλεκτρονικών συσκευών σε απόσταση 4 cm (1 ⁄ in) ή μικρότερη. Το NFC προσφέρει σύνδεση χαμηλής ταχύτητας με απλή εγκατάσταση που μπορεί να χρησιμοποιηθεί για την εκκίνηση ασύρματων συνδέσεων με περισσότερες δυνατότητες.
- **WiFi / 802.11:** Το χαμηλό κόστος λειτουργίας WiFi το καθιστά στάνταρ σε όλα τα σπίτια και τα γραφεία. Ωστόσο, μπορεί να μην είναι η σωστή επιλογή για όλα τα σενάρια λόγω του περιορισμένου εύρους και της κατανάλωσης ενέργειας 24/7.
- **Z-Wave:** Ένα δίκτυο πλέγματος που χρησιμοποιεί ραδιοκύματα χαμηλής ενέργειας για επικοινωνία από συσκευή σε συσκευή.
- **Zigbee:** Μια προδιαγραφή βασισμένη στο IEEE 802.15.4 για μια σειρά πρωτοκόλλων επικοινωνίας υψηλού επιπέδου που χρησιμοποιούνται για τη δημιουργία προσωπικών δικτύων περιοχής με μικρά ψηφιακά ραδιόφωνα χαμηλής ισχύος. [21]

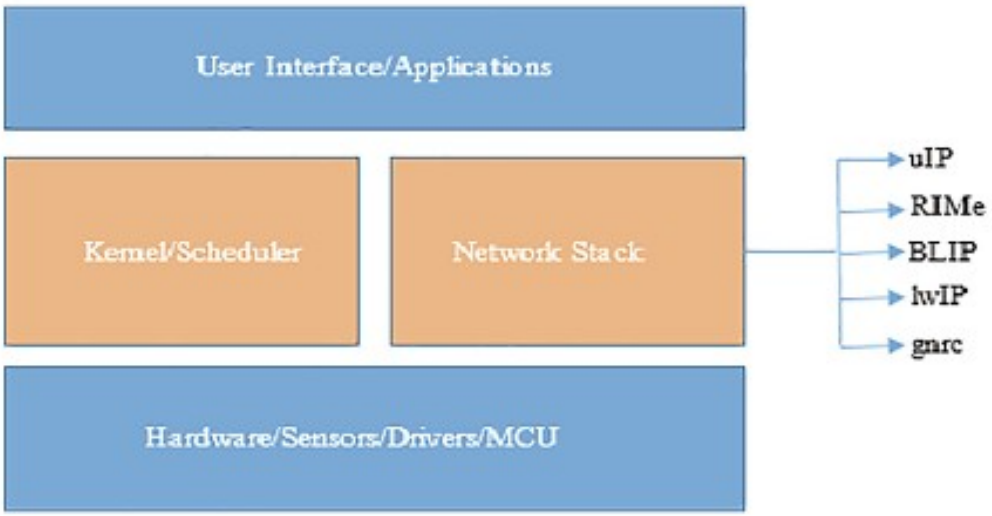
β)Τα **δίκτυα χαμηλής ισχύος ευρείας περιοχής,** επιτρέπουν την επικοινωνία τουλάχιστον 500 μέτρων, απαιτούν ελάχιστη ισχύ και χρησιμοποιούνται για την πλειονότητα των συσκευών IoT. [21]

- **4G LTE IoT:** Υψηλή χωρητικότητα και χαμηλός λανθάνων χρόνος, αυτά τα δίκτυα είναι μια εξαιρετική επιλογή για σενάρια IoT που απαιτούν πληροφορίες ή ενημερώσεις σε πραγματικό χρόνο.
- **5G IoT:** Αν και δεν είναι ακόμη διαθέσιμα, τα δίκτυα 5G IoT αναμένεται να επιτρέψουν περαιτέρω καινοτομίες στο IoT παρέχοντας πολύ πιο γρήγορες ταχύτητες λήψης και συνδεσιμότητα σε πολλές άλλες συσκευές σε μια δεδομένη περιοχή.
- **Cat-0:** Αυτά τα δίκτυα LTE είναι η επιλογή χαμηλότερου κόστους. Βάζουν τις βάσεις για το Cat-M, μια τεχνολογία που θα αντικαταστήσει το 2G.
- **Cat-1:** Αυτό το πρότυπο για το κυψελοειδές IoT θα αντικαταστήσει τελικά το 3G. Τα δίκτυα Cat-1 είναι εύκολο να δημιουργηθούν και προσφέρουν μια εξαιρετική λύση για εφαρμογές που απαιτούν φωνή ή διεπαφή προγράμματος περιήγησης.
- **LTE Cat-M1:** Αυτά τα δίκτυα είναι πλήρως συμβατά με δίκτυα LTE. Βελτιστοποιούν το κόστος και την ισχύ σε μια δεύτερη γενιά τσιπ LTE που έχουν σχεδιαστεί ειδικά για εφαρμογές IoT.
- **Narrowband or NB-IoT/Cat-M2:** Το NB-IoT / Cat-M2 χρησιμοποιεί διαμόρφωση άμεσης αλληλουχίας (DSSS) για την αποστολή δεδομένων απευθείας στον διακομιστή, εξαλείφοντας την ανάγκη για πύλη.
- **Sigfox:** Αυτός ο παγκόσμιος πάροχος δικτύου IoT προσφέρει ασύρματα δίκτυα για τη σύνδεση αντικειμένων χαμηλής ισχύος που εκπέμπουν συνεχή δεδομένα. [21]

Οι συσκευές IoT επικοινωνούν χρησιμοποιώντας πρωτόκολλα IoT. Το πρωτόκολλο διαδικτύου (IP) είναι ένα σύνολο κανόνων που υπαγορεύουν τον τρόπο αποστολής των δεδομένων στο Διαδίκτυο. Τα πρωτόκολλα IoT διασφαλίζουν ότι οι πληροφορίες από μια συσκευή ή έναν αισθητήρα διαβάζονται και κατανοούνται από μια άλλη συσκευή, μια πύλη, μια υπηρεσία. Έχουν σχεδιαστεί και βελτιστοποιηθεί διαφορετικά πρωτόκολλα IoT για διαφορετικά σενάρια και χρήση. Δεδομένης της διαφορετικής σειράς διαθέσιμων συσκευών IoT, η χρήση του σωστού πρωτοκόλλου στο σωστό περιβάλλον είναι σημαντική. [21]

3.3 Λειτουργικά Συστήματα στο IoT

Στα IoT χρησιμοποιούνται διαφορετικά λειτουργικά συστήματα ανοιχτού και κλειστού τύπου, για διάφορες συσκευές περιορισμού πόρων με χαμηλή ισχύ. Χωρίζονται σε μια πλατφόρμα υλικού που περιλαμβάνει αισθητήρες και οικογένειες MCU, ακολουθούμενη από τον πυρήνα (kernel), την επιλογή του προγραμματιστή και τη στοίβα προτύπων, που απαιτείται για την επικοινωνία του δικτύου. Το τελικό επίπεδο θα είναι εφαρμογές που υποστηρίζουν διάφορες διεπαφές χρήστη. [34]



Εικόνα 3.2: Γενική Δομή Λειτουργικού Συστήματος του IoT [34]

Η **Coniki** και το **TinyOS** είναι σήμερα τα πιο δημοφιλή λειτουργικά συστήματα ανοιχτού κώδικα μεταξύ της ερευνητικής κοινότητας, ενώ το FreeRTOS και το RIOT κερδίζουν δυναμική λόγω των δυνατοτήτων τους σε πραγματικό χρόνο. Τα LiteOS, Mantis και NanoRK εξακολουθούν να χρησιμοποιούνται λόγω της εκτεταμένης υποστήριξης ασύρματων δικτύων αισθητήρων, αλλά δεν διαθέτουν υποστήριξη πρωτοκόλλου IoT. Η ανάλυση με τη μορφή σύγκρισης μας δίνει μια σαφή ιδέα, ώστε να επιλεγεί το κατάλληλο λειτουργικό σύστημα σε κάθε περίπτωση. Τα Cooja και Tossim είναι τα πιο δημοφιλή εργαλεία δωρεάν προσομοίωσης με τα καλύτερα στην κατηγορία GUI, ενώ τα Netsim και Qualnet είναι εμπορικά εργαλεία που χρησιμοποιούνται ευρέως για εκπαιδευτικούς σκοπούς. Η Java και η C / C ++ είναι προτιμώμενες γλώσσες, ενώ το **Amazon AWS** και το **Microsoft Azure** είναι ο πιο δημοφιλής **πάροχος υπηρεσιών cloud** για την **κατασκευή προϊόντων IoT**. Η ασφάλεια και η συνδεσιμότητα αποτελούν κορυφαίο μέλημα από την πλευρά του προγραμματιστή μεταξύ των διαθέσιμων ιδιοτήτων IoT. Η εναρμόνιση του IoT με άλλους τομείς διαδραματίζει ζωτικό ρόλο στην επίτευξη παραμέτρου ποιότητας υπηρεσίας, ευφυΐας, κλιμάκωσης και ετερογένειας μεταξύ διαφοροποιημένων συσκευών. [34]

OS	Architecture	Scheduling	Programming Model	Programming Language	Memory		Network protocols	Real-Time Support
					Min RAM	Min ROM		
Contiki	Modular	Cooperative	Event Driven	C	<2kb	<30 kb	uIP, Rime, IPv6, COAP, RPL, 6loWPAN, ContikiRPL	Partial
TinyOS	Monolithic	FIFO	Event Driven	nesC	<1kb	<4kb	TYMO, DIP, 6loWPAN, IPv6, TDMA versions	No
RIOT	Microkernel	Preemptive, Priority-based, tickless	Multithreading	C,C++	~1.5 kb	~5kb	TCP, UDP, 6loWPAN, IPv6, CCN-lite, RPL, COAP	Yes
FreeRTOS	Microkernel	Preemptive, Co-operative, optional tickless	Multithreading (Task+Co-routines)	C	4 kb-9 kb	5 kb-10 kb	Using NABTO platform, TCP, UDP	Yes
LiteOS	Modular	Priority-based Round-robin	Thread, Event-Driven	Lite C++	~4kb	128kbFlash	BMAC, Mint Route, JTAG	No
Mantis	Layered	Preemptive, Priority-based Round Robin.	Multithreading	C	0.5 kb	14 kb	MAC, COMM	No
NanoRK	Monolithic	Preemptive, Harmonized, Monotonic	Multithreading	C	2 kb	18 kb	RT Link, U-Connect, BMAC, WiDom	Yes
OpenWSN	Monolithic	Cooperative	Event-Driven	C	–	–	TCP, UDP, 6loWPAN, IPv6, Http, UDP, RPL, CoAP	No
mbed	Monolithic	–	–	C	~16 kb	–	IPv4, IPv6, TCP/IP, 6loWPAN	–
Nuttx	Monolithic or Microkernel	Preemptive, Priority-based, tickless	Multithreading	C	8 kb	32 kb flash	IPv4, IPv6, 6loWPAN, TCP/IP	Yes

Πίνακας 2. Σύγκριση Λειτουργικών Συστημάτων του IoT [34]

Στον πίνακα 2, απεικονίζονται τα διάφορα λειτουργικά συστήματα που συναντάμε στο IoT. Γίνεται η σύγκριση, σε διάφορους σημαντικούς τομείς όπως είναι: η αρχιτεκτονική, η χρονοδρομολόγηση, τα εργαλεία προγραμματισμού, η μνήμη, τα πρωτόκολλα διαδικτύου, καθώς και αν προσφέρουν υποστήριξη σε πραγματικό χρόνο. [34]

3.4 Πρωτόκολλα στο IoT

Ο προσδιορισμός των πρωτοκόλλων IoT των συσκευών και ο τρόπος σύνδεσης και επικοινωνίας των συσκευών είναι πολύ σημαντικά. Στη στοίβα τεχνολογίας IoT, οι συσκευές συνδέονται είτε μέσω πύλης (gateways), είτε μέσω ενσωματωμένης λειτουργικότητας (built-in functionality). Οι πύλες - gateways αποτελούν μέρος της τεχνολογίας του IoT που μπορεί να χρησιμοποιηθεί για τη σύνδεση συσκευών IoT στο cloud. Αν και δεν απαιτούν όλες οι συσκευές IoT μια πύλη, μπορούν να χρησιμοποιηθούν για τη δημιουργία επικοινωνίας μεταξύ συσκευών ή για τη σύνδεση συσκευών που δεν βασίζονται σε IP και δεν μπορούν να συνδεθούν απευθείας στο cloud. [21]

Τα δεδομένα που συλλέγονται από συσκευές IoT μετακινούνται μέσω μιας πύλης, προ-επεξεργάζονται στην άκρη και στη συνέχεια αποστέλλονται στο σύννεφο. Η χρήση πυλών IoT μπορεί να μειώσει την καθυστέρηση και να μειώσει τα μεγέθη μετάδοσης. Έχοντας πύλες ως μέρος των πρωτοκόλλων IoT, μπορούμε να συνδέουμε συσκευές χωρίς άμεση πρόσβαση στο Διαδίκτυο και να παρέχουμε ένα επιπλέον επίπεδο ασφάλειας, προστατεύοντας τα δεδομένα που μετακινούνται και προς τις δύο κατευθύνσεις. Ο τύπος συνδεσιμότητας που χρησιμοποιείτε ως μέρος του πρωτοκόλλου IoT εξαρτάται από τη συσκευή, τη λειτουργία και τους χρήστες της. Συνήθως, η απόσταση που πρέπει να διανύσουν τα δεδομένα – είτε μικρής εμβέλειας είτε μεγάλης εμβέλειας – καθορίζει τον τύπο της συνδεσιμότητας IoT που απαιτείται. [21]

Το IoT αποτελείται από τα ακόλουθα επίπεδα:

Επίπεδο συσκευής: Ο συνδυασμός αισθητήρων, ενεργοποιητών, υλικού, λογισμικού, συνδεσιμότητας και πυλών που αποτελούν μια συσκευή που συνδέεται και αλληλεπιδρά με ένα δίκτυο.

Επίπεδο δεδομένων: Τα δεδομένα που συλλέγονται, υποβάλλονται σε επεξεργασία, αποστέλλονται, αποθηκεύονται, αναλύονται, παρουσιάζονται και χρησιμοποιούνται σε επιχειρηματικά περιβάλλοντα.

Επιχειρηματικό επίπεδο: Οι επιχειρηματικές λειτουργίες της τεχνολογίας IoT, συμπεριλαμβανομένης της διαχείρισης των αγορών χρέωσης και δεδομένων.

Επίπεδο χρήστη: Οι άνθρωποι που αλληλεπιδρούν με συσκευές και τεχνολογίες IoT. [21]

Πίνακας 2: Πρωτόκολλα στο IoT

LAYERS	PROTOCOLS	EXPLANATION
Application	Advanced Message Queuing Protocol (AMQP)	Ένα επίπεδο λογισμικού που δημιουργεί διαλειτουργικότητα μεταξύ του middleware ανταλλαγής μηνυμάτων.Τυποποιημένα μηνύματα σε βιομηχανική κλίμακα.
	Constrained Application Protocol (CoAP)	Ένα πρωτόκολλο περιορισμένου εύρους ζώνης και περιορισμένου δικτύου που έχει σχεδιαστεί για συσκευές με περιορισμένη χωρητικότητα για σύνδεση σε επικοινωνία από μηχανή σε μηχανή.UDP protocol
	Data Distribution Service (DDS)	Ένα ευέλικτο πρωτόκολλο peer-to-peer επικοινωνίας που κάνει τα πάντα, από τη λειτουργία μικροσκοπικών συσκευών έως τη σύνδεση δικτύων υψηλής απόδοσης.Αυξάνει την αξιοπιστία και μειώνει την πολυπλοκότητα.
	Message Queue Telemetry Transport (MQTT)	Ένα πρωτόκολλο ανταλλαγής μηνυμάτων που έχει σχεδιαστεί για ελαφριά επικοινωνία μεταξύ συσκευών και μηχανών και χρησιμοποιείται κυρίως για συνδέσεις χαμηλού εύρους ζώνης σε απομακρυσμένες τοποθεσίες
Transport	Transmission Control Protocol (TCP)	Προσφέρει επικοινωνία host-to-host, χωρίζοντας μεγάλα σύνολα δεδομένων σε μεμονωμένα πακέτα και στέλνοντας ξανά και επανασυναρμολογώντας πακέτα όπως απαιτείται.
	User Datagram Protocol (UDP)	Ένα πρωτόκολλο επικοινωνιών που επιτρέπει την επικοινωνία μεταξύ των διεργασιών και εκτελείται πάνω από IP. Το UDP βελτιώνει τα ποσοστά μεταφοράς δεδομένων μέσω TCP και ταιριάζει καλύτερα σε εφαρμογές που απαιτούν απώλεια δεδομένων μετάδοσης.
Network	IP	Πολλά πρωτόκολλα IoT χρησιμοποιούν IPv4, ενώ οι πιο πρόσφατες εκτελέσεις χρησιμοποιούν IPv6.
	6LoWPAN	Αυτό το πρωτόκολλο IoT λειτουργεί καλύτερα με συσκευές χαμηλής ισχύος που έχουν περιορισμένες δυνατότητες επεξεργασίας.
Data link	IEEE 802.15.4	Πρότυπο ραδιοφώνου για ασύρματη σύνδεση χαμηλής ισχύος. Χρησιμοποιείται με τα Zigbee, 6LoWPAN και άλλα πρότυπα για τη δημιουργία ασύρματων ενσωματωμένων δικτύων.
	LPWAN	Τα δίκτυα ευρείας περιοχής χαμηλής ισχύος επιτρέπουν την επικοινωνία σε αποστάσεις από 500 μέτρα έως πάνω από 10 χιλιόμετρα σε ορισμένα μέρη.
Physical	Bluetooth Low Energy (BLE)	Το BLE λειτουργεί εγγενώς σε λειτουργικά συστήματα κινητής τηλεφωνίας. Χαμηλό κόστος και μεγάλη διάρκεια μπαταρίας.
	Ethernet	Αυτή η ενσύρματη σύνδεση είναι μια λιγότερο δαπανηρή επιλογή που παρέχει γρήγορη σύνδεση δεδομένων και χαμηλό λανθάνοντα χρόνο.
	Long-Term Evolution (LTE)	Το LTE αυξάνει την χωρητικότητα και την ταχύτητα των ασύρματων δικτύων και υποστηρίζει ροές πολλαπλής διανομής και μετάδοσης.
	Near-field communication (NFC)	Οι συσκευές με δυνατότητα NFC λειτουργούν ως κάρτες ταυτότητας και χρησιμοποιούνται συνήθως για ανέπαφες πληρωμές μέσω κινητού, έκδοσης εισιτηρίων και έξυπνων καρτών.
	Power Line Communication (PLC)	Μια τεχνολογία επικοινωνίας που επιτρέπει την αποστολή και λήψη δεδομένων μέσω των υπαρχόντων καλωδίων τροφοδοσίας.
	Radio-frequency identification (RFID)	Το RFID χρησιμοποιεί ηλεκτρομαγνητικά πεδία για την παρακολούθηση ηλεκτρονικών ετικετών που δεν έχουν ισχύ.Αναγνώριση και έλεγχος ταυτότητας.
	WiFi/802.11	Το Wi-Fi / 802.11 είναι στάνταρ σε σπίτια και γραφεία. Αν και είναι μια φθηνή επιλογή, ενδέχεται να μην ταιριάζει σε όλα τα σενάρια λόγω του περιορισμένου εύρους και της κατανάλωσης ενέργειας 24/7.
	Z-Wave	Ένα δίκτυο πλέγματος που χρησιμοποιεί ραδιοκύματα χαμηλής ενέργειας για επικοινωνία από συσκευή σε συσκευή.
	Zigbee	Μια προδιαγραφή βασισμένη στο IEEE 802.15.4 για μια σειρά πρωτοκόλλων επικοινωνίας υψηλού επιπέδου που χρησιμοποιούνται για τη δημιουργία προσωπικών δικτύων περιοχής με μικρά ψηφιακά ραδιόφωνα χαμηλής ισχύος.

3.5 Η Αρχιτεκτονική Αισθητήρων σε IoT

Σε μια αρχιτεκτονική αισθητήρων περιλαμβάνονται γεννήτριες δεδομένων (data generators) και καταγραφείς δεδομένων (data capturers).

Οι **data generators** είναι μεμονωμένοι αισθητήρες IoT του δικτύου και λειτουργούν στο άμεσο περιβάλλον (immediate environment), καθώς μπορούν να ανιχνεύουν στο περιβάλλον τους φαινόμενα, όπως είναι η διακύμανση της θερμοκρασίας και της πίεσης.

Οι **data capturers** είναι υπεύθυνοι για τη συγκέντρωση δεδομένων και τη δρομολόγηση αυτών σε διάφορα τελικά σημεία, όπως είναι το Cloud (*Τεράστιο δίκτυο απομακρυσμένων servers σε όλο τον κόσμο, που λειτουργεί ώς ένα σύστημα, το οποίο έχει σχεδιαστεί για την αποθήκευση, διαχείριση δεδομένων καθώς και την εκτέλεση εφαρμογών, τα οποία είναι διαθέσιμα όπου και αν βρισκόμαστε*). Οι συσκευές IoT διαχειρίζονται τεράστιο όγκο δεδομένων και γιαυτό απαιτείται ένα αξιόπιστο και ισχυρό δίκτυο, όπως είναι αυτό του fifth generation (5G) network. [8]

Η αρχιτεκτονική των αισθητήρων IoT έχει να αντιμετωπίσει πολλές απειλές στην ασφάλεια (security threats), οι οποίες με τη σειρά τους επηρρεάζουν το δίκτυο. Η ασφάλεια των δεδομένων κατα τη μεταφορά τους έχει μεγάλη σημασία.

Η **Ακεραιότητα** των δεδομένων (Data Integrity) δεν πρέπει να θιγεί, καθώς μέσα στις πληροφορίες που διακινούνται υπάρχουν ευαίσθητες πληροφορίες (sensitive information). Αυτή η παραβίαση μπορεί να συμβεί σε οποιοδήποτε σημείο του δικτύου είτε αυτό είναι data generator, είτε data captur, και κατα τη διέλευση πληροφοριών στα κανάλια επικοινωνίας (communication channels).

Η **Εμπιστευτικότητα** των δεδομένων (Data Confidentiality), έχει να κάνει με τη μη αποκάλυψη των πληροφοριών, σε κάποιον που δεν θέλουμε. Για την αντιμετώπιση αυτής της απειλής, υπάρχουν διάφοροι μέθοδοι κρυπτογράφησης όπως: RSA (Rivest – Shamir – Adleman), DES (data encryption standard), Blowfish και ElGamal μέθοδοι, οι οποίοι όμως δεν μας καλύπτουν εξολοκλήρου σε ότι αφορά τους sensor nodes.

Η **Διαθεσιμότητα** των δεδομένων (Data availability) είναι πολύ σημαντική, σχετίζεται με τους αισθητήρες Rogue που τους συναντάμε σε συσκευές μεσαίου λογισμικού (middleware devices*). Σε αυτό το επίπεδο γίνεται η επίθεση flooding attack σε επιλεγμένους στόχους του δικτύου με σκοπό να διακοπούν οι συνήθεις λειτουργίες του και να μην ανταποκρίνονται οι υπηρεσίες (critical sensor network services).[8]

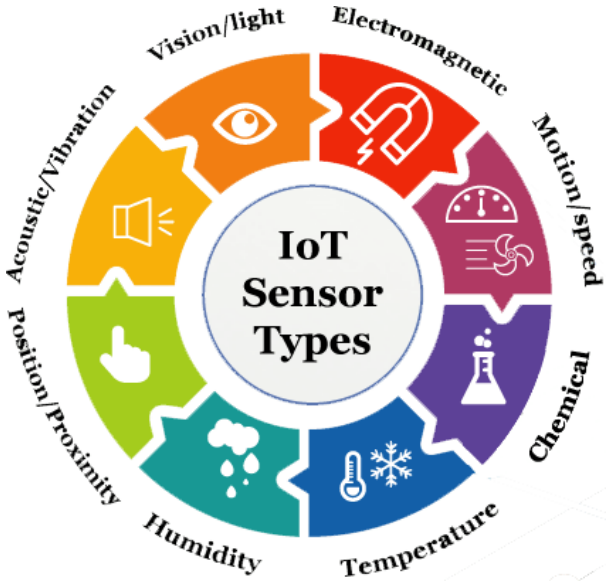
**Οι middleware devices αναφέρονται σε λογισμικό που δίνει τη δυνατότητα στο low level software και στο second level με διάφορες εφαρμογές να επικοινωνούν και να αλληλεπιδρούν μεταξύ τους.*

Τα δίκτυα 5G μας δίνουν πολλά πλεονεκτήματα όπως η ταχύτητα, η αξιοπιστία και το υψηλό εύρος ζώνης, ομώς έχουν κενά ασφαλείας και γίνονται στόχος επιθέσεων όπως: Man-in-The-Middle, η τροποποίηση μηνυμάτων (message modification), οι επιθέσεις ελέγχου ταυτότητας (authentication attacks), οι DoS attacks, οι επιθέσεις επανάληψης (replay attacks) και η υποκλοπή (eavesdrop – ping). Εξαιτίας του μεγάλου αριθμού των συνδεδεμένων συσκευών και του μεγάλου όγκου δεδομένων που κυκλοφορούν μέσα στο IoT, είναι σημαντικό να υπάρχει ένας αποτελεσματικός και ταυτόχρονα ισχυρός μηχανισμός ασφάλειας που να μπορεί να αποτρέψει τις επιθέσεις και ειδικά τις DDoS attacks. [8]

3.6 Αισθητήρες σε IoT

Οι συσκευές που αποτελούν ένα IoT είναι protocol-dependent, δηλαδή εξαρτώνται απο το πρωτόκολλο και επικοινωνούν ασύρματα βασιζόμενες σε πρότυπα, όπως το ZigBee και το 6LoWPAN. Κάποιες συσκευές που έχουν ενσωματομένους αισθητήρες (sensors) είναι : έξυπνα αυτοκίνητα, έξυπνοι σηματοδότες, έξυπνες οικιακές συσκευές (έξυπνες τηλεοράσεις, ψυγεία, πλυντήρια ρούχων), έξυπνα ποδήλατα και συσκευές eHealth, όπως συσκευές βηματοδότη και συσκευές διανομής ινσουλίνης. Το Industrial IoT (IIoT) καθώς και άλλα συστήματα που είναι IoT- based systems είναι ευάλωτα σε επιθέσεις. Αυτοί οι αισθητήρες όχι μόνο “αισθάνονται” τι συμβαίνει στο περιβάλλον γύρω τους, αλλά μπορούν να επεξεργάζονται τα δεδομένα που έχουν συλλέξει και στη συνέχεια να παίρνουν αποφάσεις και να ανταποκρίνονται ανάλογα όταν υπάρχει ανάγκη.[23]

Εικόνα 3.3: IoT Sensor Types [24]



Οι εφαρμογές αισθητήρων για σύγχρονες εφαρμογές περιλαμβάνουν τα ακόλουθα:

1. έξυπνες πόλεις. 2. έξυπνα περιβάλλοντα. 3. έξυπνο νερό 4. έξυπνη μέτρηση 5. λιανική 6. εφοδιαστική 7. βιομηχανικός έλεγχος 8. έξυπνη γεωργία 9. έξυπνη εκτροφή ζώων 10. οικιακός και οικιακός αυτοματισμός και 11. Ηλεκτρονική -Υγεία.

1. smart cities; 2. smart environments; 3. smart water; 4. smart metering; 5. retail; 6. logistics; 7. industrial control; 8. smart agriculture; 9. smart animal farming; 10. domestic and home automation; and 11. e-Health. [23]

3.7 Ασφάλεια IoT

Η ασφάλεια στο δίκτυο IoT είναι ένα δύσκολο πρόβλημα εξαιτίας των περιορισμένων πόρων για την επεξεργασία δεδομένων, την αποθήκευση και την επικοινωνία. Τα πρωτόκολλα επικοινωνίας σε IoT όπως το MQTT (message queuing telemetry transport), έχουν ενσωματωμένη υποστήριξη για ασφάλεια επιπέδου μεταφοράς TLS (transport layer security) που περιλαμβάνει μηχανισμούς επαλήθευσης εμπιστευτικότητας δεδομένων και ακεραιότητας, μηχανισμοί για την προστασία συσκευών IoT από service flooding, άρα ουσιαστικά δεν υπάρχει ασφάλεια όσων αφορά τις επιθέσεις DoS attacks. Η ανάλυση κυκλοφορίας στο δίκτυο, που έχει μεγάλο όγκο δεδομένων όπως το IoT είναι δύσκολη, γιατί η ταξινόμηση των συνδέσεων σε κανονικές ή επικίνδυνες για επίθεση, δεν είναι εύκολα διακριτές και εντοπίσιμες, απο τους αλγόριθμους ή τους χάρτες νευρώνων που υπάρχουν. [4]

Οι **ταξινομητές δικτύου Bayesian** (BN), έχουν πολλές κατηγορίες όπως οι Naïve Bayes, τα δέντρα Naïve Bayes (TANs - tree-augmented Naïve Bayes networks), τα δικτύων Naïve Bayes (BANs - Bayesian network-augmented Naïve Bayes networks), τα Bayesian multinets πολυεθνικών Bayes και τα γενικά δίκτυα Bayesian (GBNs - general Bayesian networks). Οι συγκεκριμένοι ταξινομητές δεν μας παρέχουν ακρίβεια αποτελεσμάτων, γιατί δεν μπορούν να κατηγοριοποιήσουν τις συνδέσεις που θα γίνουν. [4]

Το **Edge computing** προσπαθεί να μειώσει την αμφίδρομη ροή (two-way flow) μεγάλων όγκων δεδομένων, μεταξύ μικροσκοπικών αισθητήρων IoT, κεντρικών BS και πυλών μέσω μιας αποτελεσματικής επεξεργασίας δεδομένων. Ένα ενδιάμεσο άκρο στρώματος (intermediate edge layer) διευκολύνει την αλληλεπίδραση μεταξύ των αισθητήρων IoT και ενός κεντρικού cloud, μειώνοντας τον συνολικό όγκο δεδομένων του δικτύου. Παρόλαυτά, η αποτελεσματικότητα του layer δεν το καθιστά ικανό να σταματήσει επιθέσεις DoS. [4]

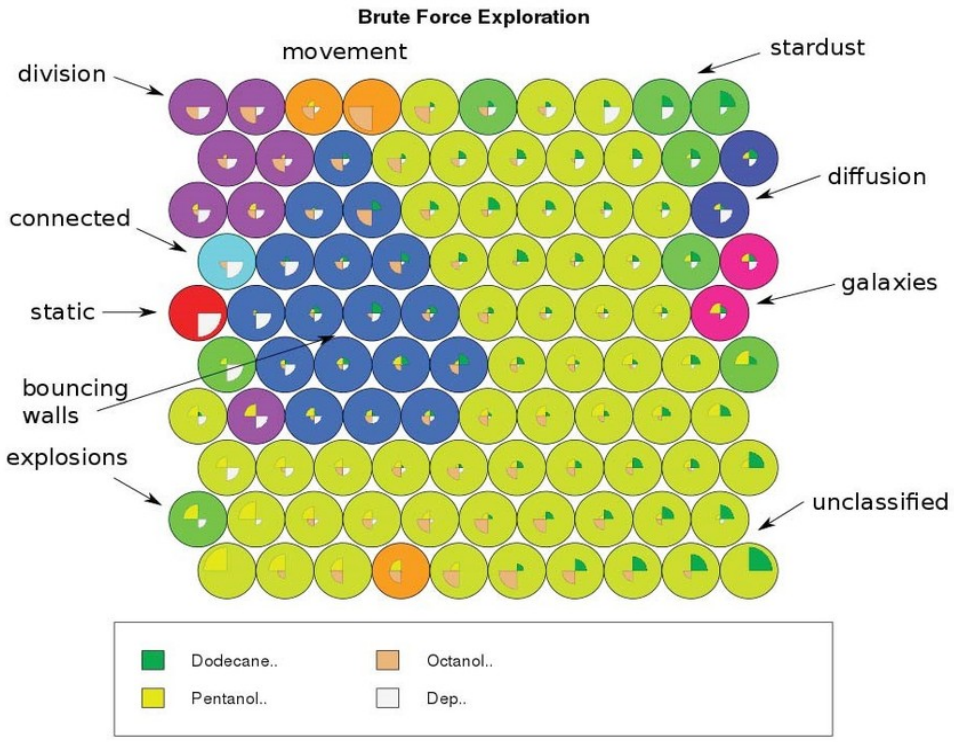
Τα **νευρωνικά δίκτυα** (MLP - Multilayer perceptron) εκπαιδεύονται, μέσω της τροποποίησης των βαρών (weights) των διασυνδέσεων των νευρωνικών δικτύων, μεταξύ των κόμβων και των διαφόρων επιπέδων (input, output or hidden). Τα MLP βασίζονται στα network weights που ενημερώνονται χρησιμοποιώντας καθορισμένες

λειτουργίες κατά τη διάρκεια της περιόδου εκπαίδευσης, όπως ο αλγόριθμος βελτιστοποίησης με βάση την κλίση (gradient-based optimization algorithm). [4]

Το **C4.5** είναι ένας ταξινομητής decision tree-based classifier, που παράγει μια απόφαση βασιζόμενος σε ένα συγκεκριμένο δείγμα δεδομένων. Αυτός ο αλγόριθμος, αποδίδει καλά ακόμη και όταν υπάρχουν ελλιπή δεδομένα. Ένας C4.5-based classifier χρησιμοποιείται για την ανίχνευση DoS attack traffic σε ένα δίκτυο IoT.[4]

Ο **self-organizing map** (SOM), είναι ένας μη επιτηρούμενος αλγόριθμος μάθησης για την ομαδοποίηση όμοιων δεδομένων σε ομάδες στο χώρο εισόδου. Αυτός ο χάρτης είναι μια τεχνική οπτικοποίησης δεδομένων, που παράγει έναν τοπολογικό χάρτη χαμηλών διαστάσεων για να βοηθήσει τους ανθρώπους να αναλύσουν οπτικά τις κατηγορίες δεδομένων σε μικρότερα σύνολα δεδομένων. Μόλις εκπαιδευτεί το νευρωνικό δίκτυο SOM, ο χάρτης συγκλίνει σε μια σταθερή διανομή και δείχνει ένα σαφή διαχωρισμό μεταξύ νόμιμης και επιθετικής κίνησης. Οι εξερχόμενοι νευρώνες θεωρούνται ως μετρήσεις για φυσιολογικά σημεία και σημεία επίθεσης. Αφού δημιουργηθεί ο χάρτης με τα δεδομένα εκπαίδευσης, οι μελλοντικές συνδέσεις μπορούν να ταξινομηθούν ως φυσιολογικές ή ως επιτεθέσεις με βάση την τοποθεσία τους στον χάρτη. Οι SOM έχουν περιορισμένο αριθμό νευρώνων, κάτι που δεν επαρκεί για να γίνει ανάλυση της κυκλοφορίας ενός δικτύου που έχει μεγάλο όγκο δεδομένων. [4]

Εικόνα 3.3: Self-organizing map [4]

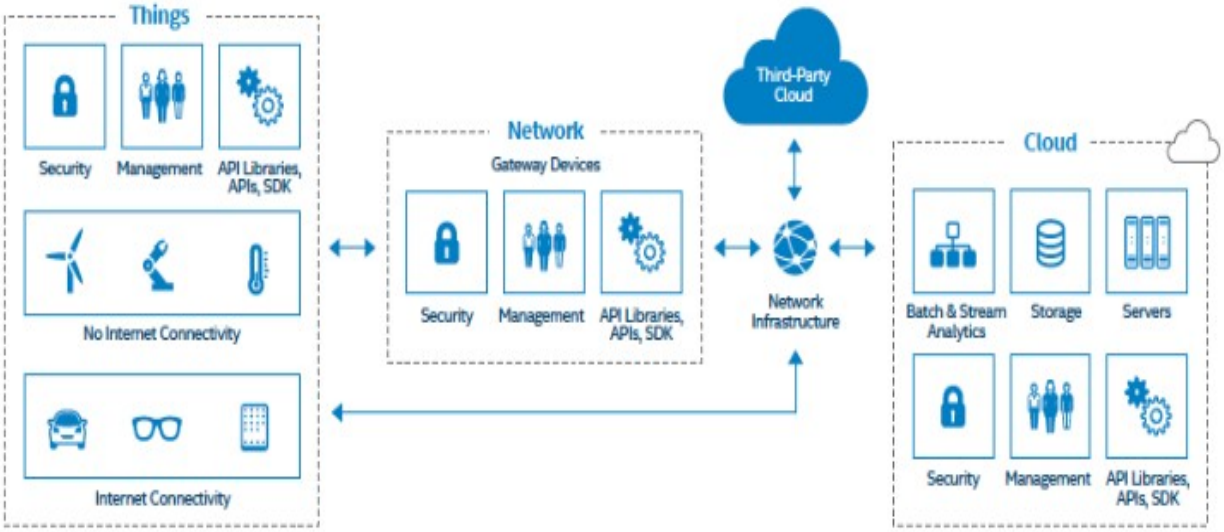


Οι **self-organizing maps Kohonen** (KSOM) μπορούν να αντιμετωπίσουν αυτόν τον περιορισμό, φτιάχνοντας τοπολογικούς χάρτες που αντιπροσωπεύουν. τα δεδομένα εισόδου ανάλογα την ομοιότητα στις τιμές δεδομένων.

Ο χάρτης αντιπροσωπεύει την κίνηση του δικτύου σε ένα δεδομένο σύμπλεγμα (cluster), το οποίο βοηθά στην ταξινόμηση των δεδομένων σε normal ή anomalous, ανάλογα με τη βέλτιστη αντιστοίχιση της θέσης του cluster . Οι χάρτες SOM έχουν δύο αρνητικά: τις μεγάλες καθυστερήσεις και την χαμηλή απόδοση. [4]

Η **Bayesian integration** τεχνική μπορεί να μάθει τις δομές μοντέλων (model structures) και να τις συγκρίνει σε (model classes). Αυτά τα δίκτυα έχουν χρησιμοποιηθεί για την ανίχνευση και τον εντοπισμό ανεπιθύμητων μηνυμάτων (spam). Όμως τα Bayesian network δεν χαρακτηρίζονται για την ακρίβεια τους, εξαιτίας της διαφορετικότητας των δεδομένων και των χαρακτηριστικών τους. Υπάρχουν αρκετές τεχνικές για την επίλυση του προβλήματος, όπως η lazy Bayesian rule (LBR) και η super-parent tree augmented network (super-parent TAN). Αν και αυτές οι δύο τεχνικές μας δίνουν λίγα σφάλματα στην ταξινόμηση έχουν υψηλό υπολογιστικό κόστος. [4]

Εικόνα 3.4: Αρχιτεκτονική IoT απο την Intel [36]



Η Intel μαζί με τους συνεργάτες της όπως φαίνεται στην εικόνα 3.3. καθόρισαν την αρχιτεκτονική IoT, με το όνομα της προδιαγραφής αρχιτεκτονικής συστήματος (SAS - System Architecture Specification) για το IoT, είτε συνδέονται με το Διαδίκτυο είτε όχι.

Αυτή η αρχιτεκτονική παρέχει ασφάλεια δεδομένων και συσκευών.

Αυτή η αρχιτεκτονική έχει 3 στοιχεία:

Τα πράγματα - **Things**, το Δίκτυο - **Network**, το Σύννεφο - **Cloud**. [36]

3.8 Προβλήματα στην ασφάλεια του IoT

Ο εντοπισμός και ο ορισμός του προβλήματος στο δίκτυο IoT είναι από τα πιο δύσκολα θέματα που μπορούμε να επιλύσουμε. Το πως μπορούμε να διευρευνήσουμε τα μεμονωμένα attack vectors - διανύσματα επίθεσης τόσο σε επίπεδο συσκευής όσο και σε επίπεδο δικτύου.

Πως γίνεται η έρευνα και η αναγνώριση των διανυσμάτων επίθεσης?

Απαιτείται να χωριστεί η αρχιτεκτονική IoT σε ζώνες εμπιστοσύνης για τη μοντελοποίηση των φορέων επίθεσης, των απειλών ασφαλείας και της εκμετάλλευσης των αδυναμιών, τόσο σε επίπεδο συσκευής όσο και σε επίπεδο δικτύου. Πρέπει να σκεφτόμαστε την ασφάλεια του IoT σε ένα υψηλότερο επίπεδο και όχι μόνο να εστιάζουμε σε κάποιες συγκεκριμένες εφαρμογές όπως είναι για παράδειγμα η υγεία και η περίθαλψη. Επίσης μπορούμε να χωρίσουμε το δίκτυο IoT σε διαφορετικούς τομείς (π.χ. οικονομικό, υγειονομική περίθαλψη, σπίτι, μεταφορά) και να προσδιορίσουμε ποιες κοινές συσκευές χρησιμοποιούνται τόσο σε ατομικό όσο και σε εμπορικό επίπεδο για να ωφεληθούν οι καταναλωτές και οι επιχειρήσεις. Ο εντοπισμός αδυναμιών σε επίπεδο συσκευής (device-level), καθώς και η ανάδειξη των ευπαθειών ασφαλείας δημιουργούνται σε επίπεδο δικτύου (network level), λόγω της ανάπτυξης συσκευών IoT σε μια επιχείρηση. Κάθε αδυναμία μπορεί να δημιουργεί μία ή περισσότερες απειλές ασφαλείας (security threats), που εισάγουν σημεία διείσδυσης (penetration points) σε ένα δίκτυο IoT. Η ανάπτυξη συσχετισμών (correlations), αναδυκνύεται ώς ένα πρόβλημα μεταξύ των διαφορετικών επιθέσεων και των αδυναμιών (exploited vulnerabilities). [7]

Η ανάπτυξη των συσχετισμών μεταξύ διαφορετικών επιθέσεων και των αδύνατων σημείων σε σχέση με την ασφάλεια είναι οι τοποθεσίες, η κατάσταση δεδομένων και οι στόχοι. Ο προσδιορισμός των έλεγχων ασφαλείας που είναι διαθέσιμοι και μπορούν να εφαρμοστούν για να κλείσουν το τρωτά σημεία, μπορούν να ασφαλίσουν τις συσκευές από πιθανές επιθέσεις DDos. Η χαρτογράφηση απειλών συσκευής για την ανάλυση των απειλών ασφαλείας μπορούν να βοηθήσουν στον εντοπισμό των τρωτών σημείων σε επίπεδο συσκευής. [7]

Τα ερευνητικά προβλήματα αποτελούνται απο τα εξής ερωτήματα - προβλήματα:

α) Με πόσους τρόπους μπορεί να επιτεθεί μια συσκευή, β) ποιές απειλές είναι πιο κρίσιμες σε σχέση με άλλες ήδη αναγνωρισμένες απειλές, γ) ποιες επιθέσεις χρειάζονται άμεσο έλεγχο, δ) ποιοι έλεγχοι ασφαλείας πρέπει να αναπτυχθούν σε επίπεδο συσκευής ή δικτύου για να κλείσουν τις γνωστές αδυναμίες και να ελαχιστοποιηθεί η πιθανότητα εμφάνισης μιας επίθεσης. [7]

Τα πιθανά σημεία διείσδυσης (**potential penetration points**), μπορούν να επιτρέψουν σε έναν εισβολέα να διεισδύσει στο περιβάλλον IoT, εκμεταλλευόμενος τόσο ευπάθειες επιπέδου συσκευής όσο και του δικτύου. Για τον προσδιορισμό των μεμονωμένων φορέων επίθεσης, είναι σημαντικό να υπάρχει σαφής κατανόηση του περιβάλλοντος IoT και των πιο κοινών συσκευών που χρησιμοποιούνται σε κάθε τομέα IoT (π.χ., τομέας υγειονομικής περίθαλψης ή οικονομικού τομέα). [7]

[7] Μέσω της χαρτογράφησης των απειλών σε μια συσκευή device-threat mapping μπορούμε να καταλάβουμε:

- Με πόσους τρόπους μπορεί να επιτεθεί μια συσκευή.
- Ποια απειλή ασφάλειας είναι πιο κρίσιμη από άλλες αναγνωρισμένες απειλές και ποια χρειάζεται άμεσο έλεγχο ασφαλείας ,
- Ποιοι έλεγχοι ασφαλείας πρέπει να αναπτυχθούν σε επίπεδο συσκευής ή δικτύου για να κλείσουν τα γνωστά τρωτά-αδύνατα σημεία για να ελαχιστοποιηθεί η πιθανότητα εμφάνισης μιας επίθεσης.

3.9 Αντιμετώπιση των επιθέσεων σε Δίκτυα IoT

3.9.1 Εικονικά Πρωτότυπα

Το virtual prototype χρησιμοποιεί το υλικό-hardware και το λογισμικό-software μιας συσκευής IoT, για να παράγει μια ολοκληρωμένη ανάλυση συστήματος. Η περιεκτική ανάλυση του συστήματος εφαρμόζει δοκιμές διείσδυσης εντοπίζοντας τα αδύνατα σημεία στο σχεδιασμό του συστήματος και στη συνέχεια υποδεικνύοντας, ποιά σημεία πρόσβασης πρέπει να προστατεύουν. Αυτή η προσέγγιση είναι πολύ σημαντική για την ασφάλεια των συσκευών IoT. Παρολαυτά, μετά τον εντοπισμό των αδύνατων σημείων δεν μπορεί να κάνει περαιτέρω ανάλυση. [7]

3.9.2 Διάνυσμα Επίθεσης

Στο attack vector πρότεινεται ένα διάνυσμα επίθεσης, που χρησιμοποιήται για να ερευνηθούν οι περιβαλλοντικές και οι product-life ενός IoT. Το προτεινόμενο matrix θεωρεί ότι σημαντικό ρόλο παίζει στο σχεδιασμό IoT, το επίπεδο πρωτοκόλλου και προσπαθεί να περιγράψει τον τρόπο με τον οποίο σχεδιάζεται το IoT. Οι συγκριτικές διαφορές επισημαίνονται μεταξύ των τύπων επίθεσης σε περιβάλλοντα IoT και του συμβατικού διαδικτύου. Η προσέγγιση αυτή ενισχύει αποτελεσματικά τις αδυναμίες στα επίπεδα του σχεδιασμού IoT, όμως δεν επαρκούν οι πληροφορίες που δίνονται σχετικά με την ασφάλεια για την προστασία του χρήστη από αυτές τις ευπάθειες και τις επιθέσεις. [7]

3.9.3 Διαχείριση Κινδύνων

Η μέθοδος του risk management χρησιμοποιεί τη διαχείριση κινδύνων για να βοηθήσει στο σχεδιασμό του IoT και των συστατικών του, συμπεριλαμβανομένων παραγόντων που διαμορφώνουν κινδύνους όπως, οι φορείς επίθεσης και οι στρατηγικές διαχείρισης (factors shaping risks). Εδώ έχουμε την ανάπτυξη νέων μεθοδολογιών αξιολόγησης κινδύνων προκειμένου να εξευρεθούν οι πτυχές που επηρεάζουν το IoT και τις πολυάριθμες συσκευές του. Στη διαχείριση κινδύνου και στις προκλήσεις στις συσκευές IoT, είναι σημαντικό πρώτα να δούμε τις λειτουργίες σε επίπεδο συστήματος και μετά τους παράγοντες κινδύνου του IoT. Οι προκλήσεις που σημειώθηκαν περιλάμβαναν την επεκτασιμότητα, τη διαλειτουργικότητα, την αξιοπιστία, την αποδοτικότητα, τη διαθεσιμότητα και την αποθήκευση που οδήγησαν στον κίνδυνο κινδύνων ελέγχου πρόσβασης, κινδύνων δικτύου, κινδύνων κωδικού πρόσβασης, κινδύνων καναλιών και κινδύνων πληροφοριών.

Αυτή η μέθοδος τονίζει τις αδυναμίες στα δίκτυα IoT και εντοπίζει τις επιθέσεις, ωστόσο, δεν υπάρχει μια σειρά προσδιορισμένων λύσεων για τον μετριασμό του κινδύνου, αλλά **μόνο συμπεράσματα** σχετικά με τον τρόπο **αξιολόγησής** τους. [7]

3.9.4 Μοτίβα Ασφάλειας

Αυτή η μέθοδος αντιμετωπίζει τα προβλήματα των vulnerabilities και της ετερογένειας στο IoT, των συσκευών και των δικτύων IoT. Αυτό που προτείνεται, είναι να γίνει αξιολόγηση ασφάλειας για τις κινητές συσκευές IoT, με βάση τα μοτίβα κίνησης (movement patterns) αυτών των συσκευών. Τα movement patterns χρησιμοποιούνται ως μοντέλα ασφαλείας για την αξιολόγηση της ασφάλειας του διαδικτύου IoT , σε κινητές συσκευές IoT. Υπάρχουν τρία μοντέλα δικτύου IoT για κινητά: Random Waypoint, Gauss - Markov και Reference Point Group. Χρησιμοποιώντας τα τρία κινητά μοντέλα, μπορεί να παρουσιαστεί μια διαδρομή επίθεσης και μια ανάλυση ασφάλειας. Αυτό μπορεί να ισχύσει μόνο για τις κινητές συσκευές IoT (mobile IoT devices), αλλά όχι και στις υπόλοιπες συσκευές που εμπλέκονται στο IoT, οι οποίες είναι πάρα πολλές. [7]

3.9.5 Μοντέλο Ταξινόμησης

Το classification model χρησιμοποιείται για την ανάλυση της σχέσης μεταξύ δυνητικού και πραγματικού κινδύνου, ενώ ταυτόχρονα εντοπίζει αδυναμίες στις συσκευές οικιακού αυτοματισμού. Οι ατέλειες ασφαλείας αναφέρονται στα πιθανά τρωτά σημεία και περιλαμβάνουν: προεπιλεγμένες διαμορφώσεις - default configurations, κωδικούς πρόσβασης που είναι εύκολο να σπάσουν - easy to crack passwords, μη κρυπτογραφημένη κίνηση - unencrypted traffic, responses to forged traffic και πλήρης έλεγχος της συσκευής χωρίς έλεγχο ταυτότητας – no authentication. Αυτό το μοντέλο δεν μπορεί να αντιμετωπίσει τις πιο πολλές επιθέσεις σε συσκευές IoT. Αντιμετωπίζει προβλήματα και επιθέσεις που εντοπίζονται κυρίως στις συσκευές του οικιακού αυτοματισμού όπως: το Amazon Echo και το Google Home. [7]

3.9.6 Το μοντέλο Threat

Το threat model χρησιμοποιείται για την προστασία συσκευών IoT που βρίσκονται στο τομέα αυτοματισμού κτιρίων. Τα νέα vector attacks και οι νέες απειλές βασίζονται σε ένα μοντέλο αυτοματισμού κτιρίου που περιλαμβάνει αισθητήρες, ενεργοποιητές και συσκευές χρήστη για να επιτρέπουν την αλληλεπίδραση με το περιβάλλον. Αυτό το μοντέλο περιλαμβάνει και άλλες συσκευές όπως: τηλεοράσεις, κινητά τηλέφωνα και wearables. Η ανάλυση απειλών καθορίζει τις νέες απειλές που ισχύουν για τον αυτοματισμό κτιρίων και το IoT. Δεν συμπεριλαμβάνει τις πιθανές απειλές άλλων συσκευών IoT σε διαφορετικούς τομείς. [7]

3.9.7 Διαλειτουργικότητα και ασφάλεια σε επίπεδο στοίβας

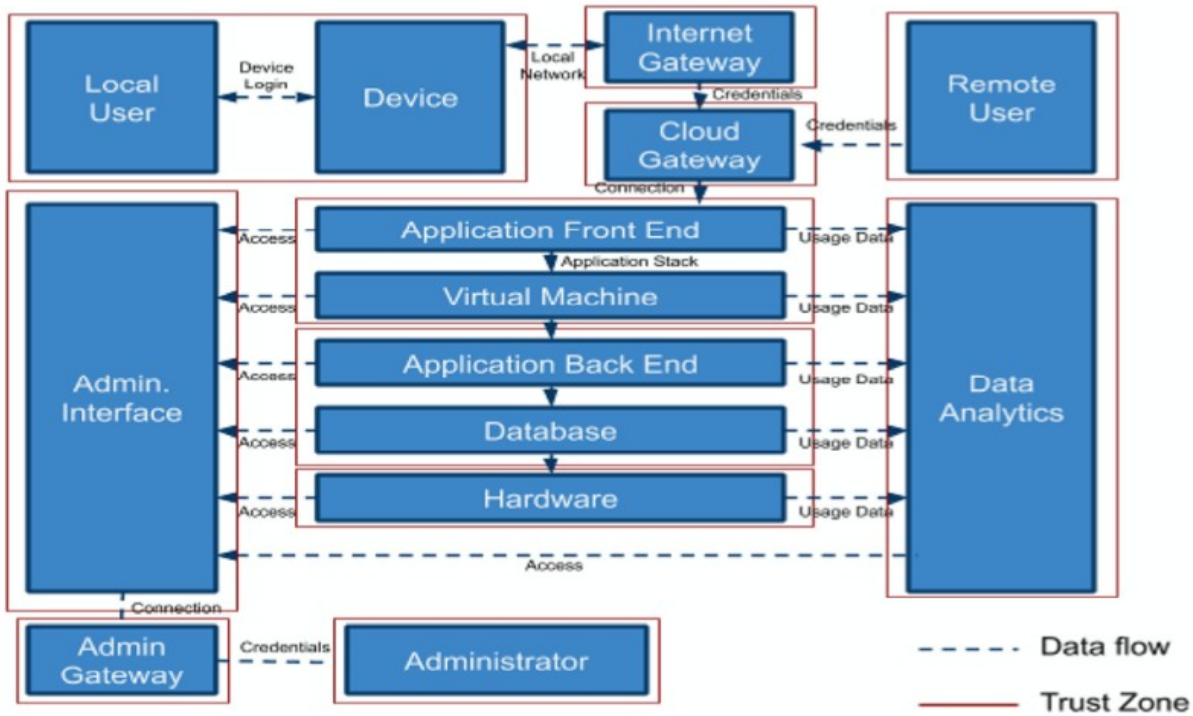
Το συγκεκριμένο μοντέλο βασίζεται σε τυποποιημένες εμπορικές αρχιτεκτονικές, που μπορούν να συγκρίνουν και να αναλύσουν την ασφάλεια και τη διαλειτουργικότητα σε ένα τυπικό περιβάλλον IoT. Οι λειτουργικές προβολές όπως: the Borgia, ITU-T functional view, ISO functional view, Microsoft functional view, SAP functional view, Intel functional view, WS2O functional view, API representations συγκρίνονται βασιζόμενες στα στοιχεία του επιπέδου τους, ώστε να αναγνωρίσουν την καλύτερη

λύση όσον αφορά την αποτελεσματικότητα της αρχιτεκτονικής αναφοράς. Αυτές οι συγκρίσεις των παραδειγμάτων παρέχουν μια ανάλυση της ασφάλειας του συστήματος IoT στα respected environments. [7]

3.9.8 Περιοχή συσκευής

Η περιοχή συσκευής του διαγράμματος δικτύου, αντιπροσωπεύει οποιαδήποτε συσκευή με την οποία ένας χρήστης μπορεί να αλληλεπιδράσει, όπως φαίνεται στην Εικόνα 13. Αυτό μπορεί να περιλαμβάνει οτιδήποτε: από υπολογιστές, smartphone, κάμερες CCTV και βηματοδότες. Αυτές οι συσκευές εκτελούν το λογισμικό, διαθέτουν λειτουργικά συστήματα (OS) και συνδέονται στο Διαδίκτυο. Πολλές συσκευές διαθέτουν ιδιόκτητο υλικό και ιδιόκτητα λειτουργικά συστήματα. Άλλοι κατασκευαστές χρησιμοποιούν λειτουργικά συστήματα ανοιχτού κώδικα (open-source operating systems) που διαθέτουν δωρεάν άδεια χρήσης και χρησιμοποιούνται με τα κοινά στοιχεία (common components). Όσο περισσότερες συσκευές συνδέονται στο Διαδίκτυο μέσω ασύρματων συχνοτήτων, όπως το Wi-Fi και το Bluetooth, τόσο περισσότερο κινδυνεύουν να δεχτούν επίθεση. Για την ελαχιστοποίηση του κινδύνου, υπάρχει η απομακρυσμένη πρόσβαση (remote access) για τις συσκευές στο IoT. [7]

Εικόνα 3.5: Network Divided into Zones Based on Trust **[7]**



3.9.9 Field gateway

Οι IoT πύλες ελαχιστοποιούν το χάσμα μεταξύ του χρήστη και της υποδομής πληροφορικής (IT infrastructure). Μπορούν να αποθηκεύσουν πληροφορίες και στη συνέχεια να προωθήσουν τα δεδομένα με ασφάλεια. Οι Gateways IoT μπορούν να αποδώσουν σε υψηλή επεκτασιμότητα (high scalability), μπορούν να πάρουν intelligent data από ένα data center και να τα προωθήσουν. Οι "smart" IoT gateways παραδίδονται από εταιρείες όπως η Dell, η Intel και η NEXCOM . Το IoT μπορεί να έχει αισθητήρες με δεκάδες λειτουργίες, μέτρηση θερμοκρασίας, φωτός και εξοπλισμού. Το IoT όχι μόνο ανιχνεύει τα συστήματα, αλλά μπορεί επίσης να ελέγξει τα συστήματα. Ενεργοποίηση και απενεργοποίηση φώτων, HVAC και δίκτυα μπορούν να εφαρμοστούν μέσω συνδεδεμένων συστημάτων. [7]

3.9.10 Cloud gateway

Οι πύλες IoT νέας γενιάς, βελτιώνουν την απόκριση και την υποστήριξη των νέων λειτουργικών μοντέλων (operating models). Οι IoT gateways βρίσκονται στα άκρα των συστημάτων όπως: συσκευές, ελεγκτές και αισθητήρες που συνδέονται μέσω του cloud. Μπορούν να μετριάσουν τους κινδύνους με την απομόνωση των συσκευών και των αισθητήρων από τις εξωτερικές απειλές. Οι cloud gateways επιτρέπουν στις συσκευές IoT να αποθηκεύουν απευθείας οποιαδήποτε από τις πληροφορίες τους σε ιδιωτικό χώρο αποθήκευσης cloud, χωρίς να χρειάζεται να συνδεθούν ποτέ σε δημόσιο cloud. Έτσι μειώνουν τον αριθμό των πιθανών επιθέσεων στο δίκτυο, ελαχιστοποιώντας την επιφάνεια επίθεσης (attack surface). [7]

ΚΕΦΑΛΑΙΟ 4

Στο παρόν κεφάλαιο αναφέρονται αδυναμίες ασφάλειας που έχουν οι συσκευές IoT όπως είναι: οι κωδικοί πρόσβασης χαμηλής ασφάλειας, οι ανοιχτές θύρες και οι μη κρυπτογραφημένες υπηρεσίες. Επίσης στη συνέχεια αναφερόμαστε σε κάποιες στρατηγικές άμυνας που εφαρμόζονται απέναντι στις DDos επιθέσεις.

4.1 Αδυναμίες των Συσκευών IoT

Οι συσκευές IoT μας προσφέρουν πολλές ευκολίες όμως παρολαυτά, εχουν και πολλά κενά ασφαλείας που ονομάζονται **Vulnerabilities.** Πιο συγκεκριμένα είναι αδυναμίες του συστήματος που επιτρέπουν σε επιτιθέμενους, να εκτελούν ενέργειες στις οποίες οι νόμιμοι χρήστες και διαχειριστές δεν είναι σύμφωνοι.[7]

4.1.1 Κωδικοί πρόσβασης Hard-coded

Οι κωδικοποιημένοι κωδικοί πρόσβασης θεωρούνται ως μια από τις πιο κοινές ευπάθειες στις συσκευές IoT. Οι συσκευές διαθέτουν κωδικό πρόσβασης - **Admin password,** που αν σπάσει μπορεί να παρακάμψει τη συσκευή ανεξάρτητα από τις επιλογές ασφαλείας που ο χρήστης έχει επιλέξει ακόμα και αν έχει αλλάξει τον κωδικό πρόσβασής του. Οι χρήστες δεν γνωρίζουν την ύπαρξή τους, οπότε δεν μπαίνουν στις συγκεκριμένες ρυθμίσεις ώστε να αλλάξουν και να απενεργοποιήσουν αυτόν τον κωδικό πρόσβασης. [7]

4.1.2 Αδύναμοι κωδικοί πρόσβασης

Ένα άλλο πρόβλημα ασφάλειας στις συσκευές IoT, είναι οι αδύναμοι κωδικοί πρόσβασης - **weak passwords.** Κατά τον καθορισμό κωδικών πρόσβασης στις συσκευές τους, οι χρήστες συχνά επιλέγουν είτε έναν κοινό, είτε έναν εύκολο κωδικό πρόσβασης ή ακόμα και να μη βάλουν καθούλου κωδικό πρόσβασης για τη συσκευή τους. Αυτή τους η ενέργεια κάνει τους επιτιθέμενους να μπορούν εύκολα να μαντέψουν ή να σπάσουν τον κωδικό ενός χρήστη σε μικρό χρονικό διάστημα και χωρίς να καταβάλλουν μεγάλη προσπάθεια. Επιπλέον, οι χρήστες επαναχρησιμοποιούν παλιούς κωδικούς πρόσβασης ή κάνουν μικρές αλλαγές σε αυτούς κάνοντάς τους ακόμα πιο αδύναμους και εύκολους στόχους. Όταν παραβιάζεται κάποιος από τους λογαριασμούς των χρηστών, θέτει σε κίνδυνο όχι μόνο τον ίδιο, αλλά και όλους τους άλλους λογαριασμούς και τα δεδομένα των συσκευών τους που συνδέονται με τον πρώτο. [7]

4.1.3 Command injection flaw

Με τη μέθοδο αυτή οι επιτιθέμενοι για να έχουν πρόσβαση χρησιμοποιούν κώδικα. Αυτό τους επιτρέπει είτε να αποκτήσουν πρόσβαση, είτε να τροποποιήσουν τις συνδεδεμένες βάσεις δεδομένων ή ακόμα και να αλλάξουν το λειτουργικό σύστημα από το οποίο εκτελείται η συσκευή. Σε αυτές τις επιθέσεις χρησιμοποιούνται SQL και JavaScript, όπου ένας εισβολέας μπορεί να εκτελέσει κακόβουλο κώδικα σε διαφορετικές περιοχές εισόδου, όπως το πεδίο σύνδεσης (login field), προκειμένου να τροποποιήσει το περιεχόμενο μιας βάσης δεδομένων.[7]

Οι συσκευές IoT λειτουργούν συνήθως σε διάφορα λειτουργικά συστήματα και είναι ευάλωτες σε command injections. Υπάρχουν πολλές διαφορετικές διαδρομές που μπορεί να ακολουθήσει ένας εισβολέας. Αλλάζοντας τις πληροφορίες που βλέπει ο νόμιμος χρήστης όταν χρησιμοποιεί τη συσκευή, θα μπορούσε να εμποδίσει τη σωστή λειτουργία, ακόμη και να αναγκάσει τη συσκευή, να τον προσθέσει ως αυθεντικό χρήστη, δίνοντάς του ευκολότερη πρόσβαση σε αυτήν και στο δίκτυο. Η μέθοδος μπορεί να χρησιμοποιηθεί και για τη δημιουργία botnets, χωρίς οι χρήστες να το γνωρίζουν.[7]

4.1.4 Ανοιχτές θύρες

Οι πληροφορίες ταξιδεύουν σε ένα δίκτυο και μπορούν να χρησιμοποιούν συγκεκριμένους τύπους θυρών, ανάλογα με τον τύπο των δεδομένων. Όλες οι θύρες-ports by default είναι ανοιχτές, για να επιτρέπουν τη μεταφορά δεδομένων χωρίς να προκύπτουν προβλήματα. Παρολαυτά, οι χρήστες μπορούν να επιλέξουν να κλείσουν τυχόν αχρησιμοποίητες θύρες για να μειώσουν την επιφάνεια επίθεσης για τους εισβολείς. Τα Firewalls παρέχουν συχνά την επιλογή να κλείσουν τις περισσότερες θύρες που δεν χρησιμοποιούνται, αλλά οι χρήστες μπορούν να κάνουν αλλαγές και κατά περίπτωση, ώστε να επιτύχουν την καλύτερη ασφάλεια με τη κατάλληλη διαμόρφωση των ρυθμίσεών τους. [7]

4.1.5 Χωρίς κλείδωμα λογαριασμού

Στην προσπάθεια σύνδεσης με έναν ιστότοπο, μια εφαρμογή ή μια συσκευή, πολλές υπηρεσίες δεν διαθέτουν δυνατότητα κλειδώματος λογαριασμού, όταν εισάγουμε λανθασμένους κωδικούς πρόσβασης. Αυτό επιτρέπει στους εισβολείς να δοκιμάζουν συνεχώς παραλλαγές των κωδικών πρόσβασης, pins ή patterns έως ότου καταφέρουν να γράψουν το σωστό. Μπορούν είτε να το κάνουν χειροκίνητα είτε να δημιουργήσουν λογισμικό που θα τρέχει είτε brute force είτε a dictionary attack. Εδώ μπορούν να χρησιμοποιηθούν όλοι οι διαφορετικοι πιθανοί συνδυασμοί που θα μπορούσε να έχει ο κωδικός πρόσβασης και να γίνεται επίθεση, για ώρες, ημέρες, εβδομάδες ή ακόμα και πολύ περισσότερο. Χρησιμοποιείται η account enumeration και μπορεί να μειώσει σημαντικά το χρόνο της επίθεσης. ‘Ετσι χρειάζεται να μαντέψουμε μόνο το όνομα χρήστη ή μόνο τον κωδικό πρόσβασης, χωρίς να χρειάζεται να βρούμε και τα δύο για να πραγματοποιήσουμε την επίθεση. [7]

4.1.6 Μη κρυπτογραφημένες υπηρεσίες

Η εμπιστευτικότητα των δεδομένων είναι ένα πολύ σημαντικό στοιχείο της ασφάλειας των πληροφοριών. Η ισχυρή κρυπτογράφηση των επικοινωνιών και η αποθήκευση δεδομένων μπορούν να αποτρέψουν τους μη εξουσιοδοτημένους χρήστες, να αποκτήσουν πληροφορίες σε περίπτωση επίθεσης. Αν ένας οργανισμός επιλέξει να χρησιμοποιήσει ασθενέστερα encryption standards για τις υπηρεσίες του, είναι ευάλωτος σε διαρροή πληροφοριών, υποκλοπές και άλλους τύπους αναγνώρισης. [7]

Οι συσκευές στέλνουν πακέτα μέσω δικτύων για τη μετάδοση δεδομένων,έτσι μπορούν εύκολα να υποκλαπούν και να διαβαστούν μέσω πακέτων sniffers. Από εκεί, ο εισβολέας μπορεί είτε να παρακολουθεί σιωπηλά τις πληροφορίες που μεταδίδονται, είτε να επιλέξει να τις χειριστεί, χωρίς να γίνεται αντιληπτός. Χρησιμοποιώντας ισχυρότερες κρυπτογραφίες, εμποδίζουμε τις επιθέσεις και διασφαλίζουμε καλύτερα τα δεδομένα μας. [7]

4.1.7 Μη ασφαλής διεπαφή ιστού

Μια insecure web interface, υπάρχει σε διάφορες μορφές και μπορεί να είναι κακόβουλη ή απλά ανασφαλής. Ένα παράδειγμα μη ασφαλούς διασύνδεσης ιστού, είναι ότι δεν θα μπορούσε να χρησιμοποιήσει σωστό sandboxing για τις user sessions. Αυτό μπορεί να επιτρέψει σε ένα άτομο να χρησιμοποιήσει την JavaScript injection σε μια επίθεση cross-site-scripting (XSS). Παρομοίως, τα πεδία εισόδου ενδέχεται να μην ελέγχονται σωστά, κάτι που μπορεί να επιτρέψει την περαιτέρω injection of commands. Οι ανασφαλείς διεπαφές μπορούν να αναπτύξουν παρεμβατικές μεθόδους παρακολούθησης χρηστών (tracking users) και διαρροής δεδομένων (leak data). Για παράδειγμα μια ψεύτικη ιστοσελίδα που χρησιμοποιείται με αυτόν τον τρόπο, μπορεί να χρησιμοποιηθεί για να ξεκινήσει μια επίθεση phishing attack για να κλέψει account logins και credentials. [7]

4.1.8 Μη ασφαλείς υπηρεσίες δικτύου

Τα Legacy network protocols που είναι παλιά, είναι ευάλωτα σε ένα μεγάλο εύρος επιθέσεων. Πρωτόκολλα όπως το Telnet και το Server Message Block (SMB) διαθέτουν ξεπερασμένα αντίμετρα ή δεν έχουν σχεδιαστεί για ασφάλεια λόγω έλλειψης προεπιλεγμένης κρυπτογράφησης. Οι συσκευές μπορεί να είναι ευάλωτες σε προεπιλεγμένες συνδέσεις όπως login: root με Telnet. Το SMB έχει επίσης ευπάθειες που σχετίζονται με τις μολύνσεις ransomware, Petya και Notpetya. Οι υπηρεσίες δικτύου έγιναν ανασφαλείς από διάφορες πτυχές, όπως buffer overflow, open ports και exploitable UDP services. Μερικά παραδείγματα επιθέσεων που θα μπορούσαν να χρησιμοποιηθούν ενάντια σε ανασφαλείς υπηρεσίες δικτύου περιλαμβάνουν fuzzing attacks καθώς και χρήση ανοιχτών θυρών για να αποκτήσουν πρόσβαση στο δίκτυο. [7]

4.1.9 Μη ασφαλής διεπαφή cloud

Οι Insecure connections δεν μας εξασφαλίζουν την εμπιστευτικότητα δεδομένων. Μια μη ασφαλής διεπαφή cloud μπορεί να χρησιμοποιήσει ανασφαλή πρωτόκολλα, που δεν διαθέτουν τα χαρακτηριστικά της κρυπτογράφησης Secure Socket Layer (SSL). Μια insecure application μπορεί επίσης να επιτρέψει στους εισβολείς να παρακολουθούν τους χρήστες. [7]

Αυτό μπορεί να χρησιμοποιηθεί για τη εισβολή δεδομένων, την πρόκληση ανεπιθύμητης λειτουργικότητας ή την παραβίαση της εμπιστευτικότητας των χρηστών. Πολλές διαφορετικές λειτουργίες καθορίζουν εάν το cloud interface είναι ασφαλές ή όχι όπως: η έλλειψη απαρίθμησης λογαριασμού, η απουσία κλειδώματος λογαριασμού και η μη κρυπτογράφηση δεδομένων ενώ κυκλοφορούν στο δίκτυο. Ένας εισβολέας μπορεί να προσδιορίσει εάν ένας λογαριασμός είναι έγκυρος προσπαθώντας να κάνει reset τον κωδικό πρόσβασης ή χρησιμοποιώντας ένα πακέτο sniffer για να βρει login credentials μέσω unencrypted traffic. [7]

4.1.10 Καταμέτρηση λογαριασμού

Η Account enumeration είναι μια εφαρμογή που σε μια αποτυχημένη προσπάθεια ελέγχου ταυτότητας, επιστρέφει μια απάντηση που δείχνει αν ο έλεγχος ταυτότητας απέτυχε λόγω εσφαλμένου αναγνωριστικού λογαριασμού ή εσφαλμένου κωδικού πρόσβασης. Αυτό επιτρέπει σε έναν εισβολέα να προσδιορίσει τα valid account identifiers που αναγνωρίζονται από την εφαρμογή. Μέσω αυτής της εφαρμογής το σπάσιμο του κωδικού πρόσβασης γίνεται εύκολο επιτρέποντας στους εισβολείς να διακρίνουν το έγκυρο σύνολο των account identifiers. Η κρισιμότητα των μηνυμάτων διαφέρει: Από το "invalid login" ή κάτι πιο συγκεκριμένο όπως "that password is not associated with that email" ή "No account is associated with that email". Αυτά τα μηνύματα επιτρέπουν στους εισβολείς με μικρή προσπάθεια, να καταφέρουν και να εισέλθουν σε ένα λογαριασμό γνωρίζοντας ποια μεταβλητή (variable) είναι η σωστή. Για να αποτρέψουμε κάτι τέτοιο μπορούμε να πούμε στον χρήστη ότι ένα email έχει σταλεί στον λογαριασμό μας ανεξάρτητα από το αν είναι έγκυρο ή όχι. [7]

4.1.11 Cross-site scripting

Το Cross-site Scripting (XSS) είναι μια κοινή αδυναμία των εφαρμογών ιστού που προκύπτει από την μη αξιόπιστη εισαγωγή σε Web browser, χωρίς επικύρωση ή κατάλληλη τροποποίηση. Όταν μια εφαρμογή Ιστού δεν μπορεί να κάνει validate δεδομένα εισόδου και να εξουδετερώσει ορισμένους χαρακτήρες επιτρέπει στις εισόδους να είναι κακόβουλες. Είναι δύσκολο να αποφευχθεί σε συσκευές IoT. Αυτό που κάνει το XSS να το συναντάμε συχνά, είναι ότι υπάρχουν πολλοί τρόποι για να «σπάσει» το data/code barrier στη web stack. [7]

4.1.12 Buffer overflow

Η Buffer overflow είναι μία μέθοδος που εκμεταλλεύεται ένα πρόγραμμα που περιμένει την είσοδο ενός χρήστη. Είναι επικίνδυνη για επιθέσεις σε συσκευές IoT λόγω της περιορισμένης μνήμης τους, των γλωσσών στις οποίες προγραμματίζονται και της ομοιότητας των προγραμμάτων τους. Οι συσκευές IoT χρειάζονται εξοικονόμηση ενέργειας, γεγονός που οδηγεί σε μικρές ποσότητες energy-efficient memory. Όσο μικρότερο είναι το buffer, τόσο πιο εύκολο είναι να κάνει overflow, κάτι που κάνει τις συσκευές IoT να είναι στο επίκεντρο αυτού του είδους των επιθέσεων . Παρόλο που οι εταιρείες βελτιώνουν τις νεότερες συσκευές, οι παλαιότερες συσκευές εξακολουθούν να έχουν αυτήν την αδυναμία. Πολλές συσκευές που χρησιμοποιούνται σήμερα μπορούν να αποτελέσουν το στόχο σε μια επίθεση buffer overflow, εξαιτίας του υλικού με το οποίο έχουν κατασκευαστεί, είτε επειδή έχουν προγραμματιστεί με γλώσσες που είναι ιδιαίτερα ευαίσθητες στην επίθεση, όπως η C. [7]

4.1.13 Αφαίρεση φυσικής αποθήκευσης

Η αφαίρεση της φυσικής αποθήκευσης, όταν **δεν** υπάρχει **επαρκής χώρος** για να γίνει, το τελικό αποτέλεσμα θα είναι η απώλεια δεδομένων. Εάν το επιτρέπει το user configuration, τότε ο χρήστης θα πρέπει να προσθέσει έναν αντικαταστάτη φυσικού χώρου αποθήκευσης στην ομάδα πριν από την αφαίρεση του παλιού. Αυτό επιτρέπει στους εισβολείς να αποκτήσουν πρόσβαση σε πληροφορίες χρηστών, εφόσον τα δεδομένα παραμείνουν **unencrypted**. [7]

4.1.14 Μη Εξουσιοδότηση

Η Εξουσιοδότηση-Authorization καθορίζει αν ένας χρήστης έχει τα δικαιώματα, όσον αφορά τη πρόσβαση σε πόρους και στην εκτέλεση ενεργειών, κάτι που ονομάζεται Role Based Access Control (RBAC). Ο μηχανισμός RBAC παρέχει έναν τρόπο περιορισμού της πρόσβασης στο σύστημα και των ενεργειών σε εξουσιοδοτημένους χρήστες. Στο RBAC, ο έλεγχος πρόσβασης διενεργείται σε σχέση με τους ρόλους και τα προνόμια του χρήστη. Σε περίπτωση που δεν υπάρχει ο κατάλληλος μηχανισμός εξουσιοδότησης, μόλις γίνει ο έλεγχος ταυτότητας ενός χρήστη, ένας χρήστης μπορεί να εκτελέσει ενέργειες που μπορεί να αποδειχθούν καταστροφικές για το σύστημα. [7]

Ο καλύτερος τρόπος να προστατέψουμε το σύστημά μας είναι να γνωρίζουμε τα διαφορετικά είδη επιθέσεων και τις αδυναμίες που υπάρχουν, έτσι ώστε να μπορούμε να κατανοήσουμε εύκολα ποιός επιτίθεται και να τον αντιμετωπίσουμε με τους κατάλληλους τρόπους. Οι πιο πολλές από τις επιθέσεις στις συσκευές IoT, συμβαίνουν κατά τη μετάδοση των δεδομένων.

Εικόνα 4.1: IoT Αδυναμίες [40]

ΚΕΦΑΛΑΙΟ 5

Στο 5ο κεφάλαιο αναλύεται η αρχιτεκτονικη και οι τύποι επίθεσης DDos, όπως επίσης και κάποιοι από τους πιο σημαντικούς λόγους που οδηγούν τους επιτιθέμενους να θέλουν να κάνουν τις συγκεκριμένες επιθέσεις. Υπάρχει ένας διαχωρισμός σε επιθέσεις DDos σε IoT και σε διαφορετικά είδη επιθέσεων που εφαρμόζονται σε IoT.

5.1 Αρχιτεκτονικές DDoS attacks

Τα **DDoS attack networks** χρησιμοποιούν τ**ρεις τύπους αρχιτεκτονικών**: την αρχιτεκτονική **Agent-Handler**, την αρχιτεκτονική που βασίζεται στο **Internet Relay Chat (IRC)** και την αρχιτεκτονική που βασίζεται στον Ιστό **(Web)**.

Η **Agent-Handler αρχιτεκτονική** βασίζεται στο Botnet, στην οποία ο εισβολέας χρησιμοποιεί το botnet για να ξεκινήσει μια επίθεση. Τα botnets αποτελούνται από masters, handlers και bots. Οι χειριστές (handlers) είναι μέσα επικοινωνίας που χρησιμοποιούν οι εισβολείς για να ελέγχουν έμμεσα τα bots. Οι handlers μπορούν να είναι προγράμματα εγκατεστημένα από τους εισβολείς σε μια συλλογή παραβιασμένων συστημάτων (π.χ. διακομιστές δικτύου) για την αποστολή εντολών για την εκτέλεση της επίθεσης. Τα Bots είναι συσκευές που έχουν παραβιαστεί από τους handlers και που θα πραγματοποιήσουν την επίθεση στο σύστημα του θύματος. Οι ιδιοκτήτες και οι χρήστες των συστημάτων bot γενικά δεν γνωρίζουν αυτή την κατάσταση επίθεσης.[5]

Στην **αρχιτεκτονική IRC-based** ο bot master ή ο controller ξεκινά μια επίθεση μέσω των bots στέλνοντάς τους εντολές. Το bot στέλνει την απόκριση ή τις πληροφορίες κατάστασης στον master. Η επικοινωνία τους γίνεται μέσω των δημόσιων συστημάτων συνομιλίας (public chat systems), αντί να γίνεται με τις αρχικές τους διευθύνσεις. Εάν χρησιμοποιούν την αρχική ταυτότητα ή τα ιδιωτικά κανάλια, το σύστημα ανίχνευσης εντοπίζει και αποκλείει εύκολα την τοποθεσία και το σύστημα. Η Internet relay chat (IRC) είναι αυτή που επιτρέπει στους χρήστες να επικοινωνούν χωρίς να πραγματοποιούν έλεγχο ελέγχου ταυτότητας και χωρίς καμία ασφάλεια στις επικοινωνίες των χρηστών. Το IRC παρέχει ένα πρωτόκολλο text-based command syntax protocol, για τον καθορισμό των κανόνων και των κανονισμών στους χρήστες και το οποίο εγκαθίσταται ευρέως στο δίκτυο. Υπάρχει τεράστιος αριθμός υπαρχόντων δικτύων IRC στο Διαδίκτυο, τα οποία μπορούν να χρησιμοποιηθούν ως σημεία δημόσιας ανταλλαγής, αλλά τα περισσότερα δίκτυα IRC δεν περιέχουν ισχυρό έλεγχο ταυτότητας (strong authentication). [5]

Στην **Web - based αρχιτεκτονική**, τα botnets χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το HTTP για την αποστολή εντολών στα bots καθιστώντας έτσι πιο δύσκολη την παρακολούθηση της δομής εντολών (control structure) και ελέγχου των DDos. Όπως τα botnets που βασίζονται στο IRC, τα botnets που είναι web-based, δεν διατηρούν συνδέσεις με διακομιστές εντολών (control servers) ή χειριστές (handlers).

Τα Web bots λαμβάνουν περιοδικά τις οδηγίες χρησιμοποιώντας web requests. Τα Web-based botnets είναι πιο ανθεκτικά, καθώς κρύβονται εντός της νόμιμης κυκλοφορίας του HTTP. Για τη διαμόρφωση και τον έλεγχο των bots χρησιμοποιούνται προηγμένες γλώσσες ανάπτυξης ιστού (PHP, ASP, JSP κ.λπ.) μέσω κρυπτογραφημένης επικοινωνίας μέσω πρωτοκόλλου HTTP ή HTTPS. [5]

5.2 Ταξινόμηση Επιθέσεων DDos στο IoT

Οι επιθέσεις DDoS ταξινομούνται με βάση τον βαθμό αυτοματισμού, ορίζονται ως χειροκίνητες, ημι-αυτόματες και αυτόματες επιθέσεις (Manual, Semi-automatic and Automatic attacks). Στην Manual approach, ο εισβολέας έπρεπε να ολοκληρώσει πολλά βήματα πριν από την έναρξη της τελικής επίθεσης, όπως σάρωση θύρας (port scanning), εντοπισμός διαθέσιμων μηχανών στο δημόσιο ή ιδιωτικό δίκτυο (identifying available machines) για την κατασκευή botnet, εισαγωγή κακόβουλου λογισμικού κ.λπ. Για Semi-automatic ή Automatic attacks, διάφορες εξελιγμένες επιθέσεις-εργαλεία έχουν αναπτυχθεί για να υποστηρίξουν τους επιτιθέμενους στην εκτέλεση όλων των βημάτων αυτόματα για τη μείωση της ανθρώπινης προσπάθειας. Οι εισβολείς μπορούν να διαμορφώσουν τις επιθυμητές παραμέτρους επίθεσης και τα υπόλοιπα γίνονται με αυτοματοποιημένα εργαλεία.[5]

Μια άλλη επίθεση DDoS καθορίζεται ανάλογα με το ποσοστό επίθεσης, δηλαδή πώς ο ρυθμός επίθεσης ποικίλλει σε σχέση με το χρόνο. Χωρίζονται σε επιθέσεις συνεχούς ρυθμού και μεταβλητού ρυθμού. Η επίθεση σε συνεχή ροή και με συνεχή ταχύτητα αφού εκτελεστεί καθιστά πιο δύσκολη την ανίχνευση και την απόκριση. Η επίθεση με μεταβλητό ρυθμό, τροποποιεί το ποσοστό επίθεσης και μπορεί να εφαρμοστεί με κυμαινόμενο ή αυξανόμενο ρυθμό.Με βάση το ρυθμό δεδομένων επίθεσης, η κίνηση σε ένα δίκτυο κατηγοριοποιείται επίσης ως επιθέσεις DDoS υψηλού και χαμηλού ρυθμού. Οι επιθέσεις DDoS ταξινομούνται περαιτέρω ως «by impact», στις οποίες η κανονική υπηρεσία δεν είναι διαθέσιμη σε χρήστες που είναι γνωστοί ως Disruptive. Επίσης υποβαθμίζουν τις υπηρεσίες του συστήματος που δέχεται επίθεση, με αποτέλεσμα να μειώνεται η αποτελεσματικότητα.[5]

Σε άμεσες επιθέσεις (direct attacks), πράκτορες ή μηχανές ζόμπι επιτίθενται απευθείας στο σύστημα των θυμάτων. Στις επιθέσεις reflector attacks, τα ζόμπι στέλνουν πακέτα αιτήσεων σε έναν αριθμό άλλων παραβιασμένων μηχανών (υπολογιστές, δρομολογητές κ.λπ.) που ονομάζονται Zombies ή Bots και στοχεύουν στο σύστημα του θύματος για ένα αποτέλεσμα, που επιθυμεί ο εισβολέας. ΄Ενα παράδειγμα που αφορά αυτήν την επίθεση, είναι η αποστολή τεράστιας επισκεψιμότητας ως αίτημα «ping» (traffic as ‘ping’), με πλαστογραφημένη διεύθυνση IP στο σύστημα των θυμάτων για μείωση του εύρους ζώνης (bandwidth).

Η κύρια ταξινόμηση των επιθέσεων DDoS είναι η «exploited vulnerability», μέσω της οποίας ένας εισβολέας εκτοξεύει επίθεση στο θύμα. Σε αυτήν την ταξινόμηση, η επίθεση πλημμύρας (flood attack) χρησιμοποιείται για να μπλοκάρει το εύρος ζώνης του μηχανήματος ή του δικτύου. Αυτό μπορεί να πραγματοποιηθεί ως πλημμύρα TCP flood, UDP flood και ICMP flood. [5]

Όλες οι επιθέσεις πλημμύρας που δημιουργούνται μέσω DDoS μπορούν να πραγματοποιηθούν ως άμεσες επιθέσεις ή επιθέσεις ανακλαστήρων .

(direct attacks or reflector attacks)

Εικόνα 5.1: Classification of DDos Attacks [5]

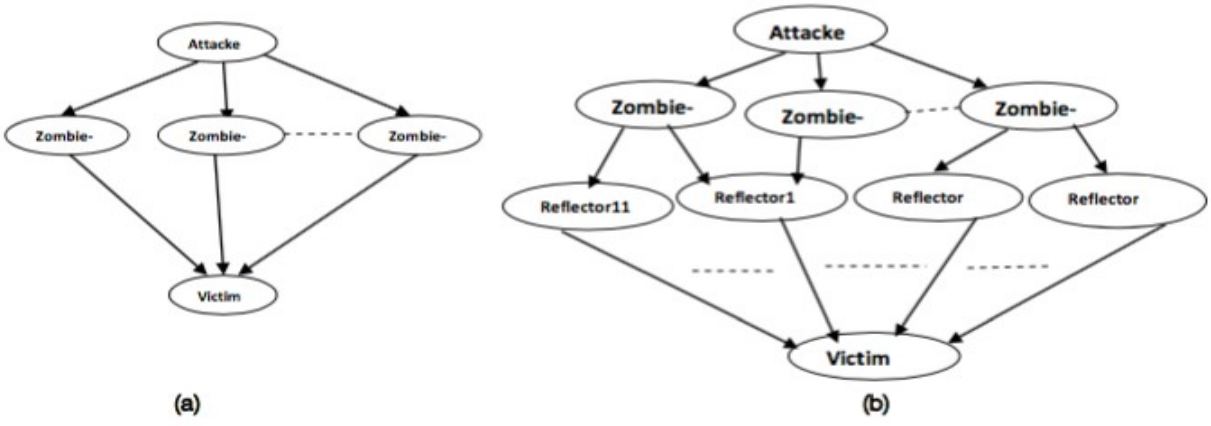
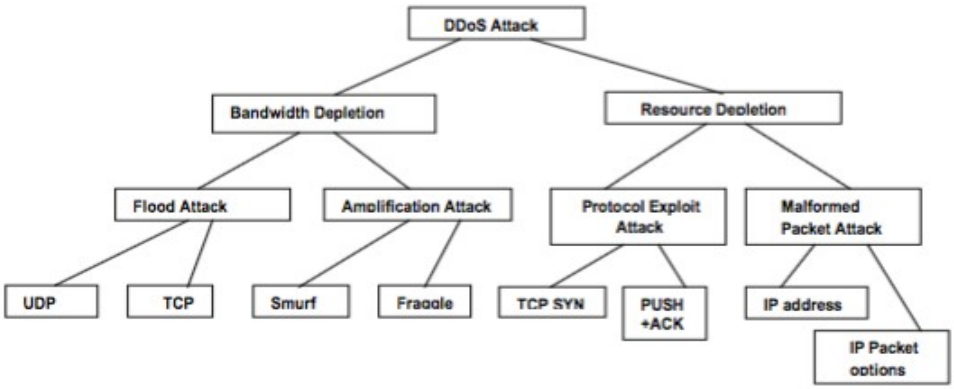


Figure 1 : (a).Direct attack, (b).Indirect attack



Το IoT διαχωρίζεται σε τρία βασικά επίπεδα που είναι: το Επίπεδο Παρατήρησης - Observation Layer, το Επίπεδο Δικτύου - Network Layer και το Επίπεδο Εφαρμογής - Application Layer, οι επιθέσεις DDoS ποικίλλουν με βάση τα επίπεδα: [9]

1) **DDoS στο επίπεδο παρατήρησης**: α)Η RFID είναι μια τεχνική που λαμβάνει δεδομένα και τα διαβάζει από αισθητήρες που περιλαμβάνονται σε συσκευές Internet of Things, χωρίς καμία άμεση παρέμβαση από ανθρώπους, εδώ πραγματοποιούνται επιθέσεις όπως, Jaming και Kill Command Attack. β)Η τεχνική layer relay on Confusion που χρησιμοποιείται για να αποτρέπεται η πρόσβαση σε υπηρεσίες.

2) **DDoS σε επίπεδο δικτύου** είναι η περιοχή, που είναι πιο ευάλωτη σε επιθέσεις, στοχεύοντας ενσύρματα και ασύρματα δίκτυα, όπου αντλούνται τεράστια δεδομένα για την πραγματοποίηση της επίθεσης. Το σύστημα που λαμβάνει τα δεδομένα παραμένει σε καθυστέρηση της απόκρισης στα αιτήματα και οι απαιτούμενοι πόροι μπορούν να γίνουν έως ότου δεν υπάρχουν άμεσες συνδέσεις, πράγμα που οδηγεί τελικά στην μη λειτουργία της υπηρεσίας. Παραδείγματα αυτής της επίθεσης είναι ICMP flood και SYN flood attack.

3) **DDoS στο επίπεδο εφαρμογής** περιέχει τη βασική διεπαφή χρήστη (έξυπνες κυβερνήσεις, έξυπνες πόλεις, έξυπνες συσκευές, κινητές εφαρμογές, ιστός) μέσω του οποίου λειτουργεί χρησιμοποιώντας εφαρμογές. Σε αυτό το επίπεδο δύο τύποι επιθέσεων μπορούν να προκύψουν η Reprogramming Attack και η Path based DoS.

Επειδή οι συσκευές του IoT συνδέονται μεταξύ τους, αυτό δημιουργεί μια κατάλληλη περιοχή για την εμφάνιση κατανεμημένων επιθέσεων άρνησης υπηρεσίας DDoS, και αυτό κάνει την εφαρμογή κακόβουλου λογισμικού (bots και zombies) να διανέμεται εύκολα σε αυτό : 1) **Mirai:** Επηρρεάζει τα Λειτουργικά συστήματα Linux. 2) **Wirex:** Μολύνουν συσκευές Android. Η Google αντιμετώπισε το πρόβλημα και διέγραψε για αυτό το λόγο πολλές εφαρμογές στο Play Store. 3) **Reaper:** Αυτό το bot έχει τη δυνατότητα να αναζητά ευπάθειες και τα τρωτά σημεία στις συσκευές Internet of Things με αποτέλεσμα να έχουν επηρρεαστεί μεγάλες εταιρείες όπως η Cisco και η Linksys. 4) **Torii:** Το Torii έχει καλυφθεί πρόσφατα και έχει τη δυνατότητα να στοχεύσει και να πλήξει σε μεγάλο βαθμό τους πιο πρόσφατους υπολογιστές, smartphone, tablet με σύγχρονα σχέδια (64-bit), x86, ARM, MIPS.[9]

Target	DATE	Description
Russian Defense Ministry's website	March 2018	The attack targeted the ministry's website while they were verifying the names of new weapons.
Boston Globe	November 2017	DDoS is interrupting the newspaper phone, and the editing system is down.
UK National Lottery	September 2017	Preventing clients from setting the lottery.
Bank of Greece Website	May 2016	Rrestricted the servers of the Bank to stay passive for 6 hours.

Εικόνα 5.2: Οι πιο πρόσφατες δημοφιλείς DDos Επιθέσεις [9]

5.3 Λόγοι Επίθεσης DDoS

- **Οικονομικοί:** οι επιθέσεις που ξεκινούν για οικονομικό κέρδος είναι συχνά, οι πιο επικίνδυνες και δύσκολες να σταματήσουν. Πρόκειται κυρίως για εταιρείες που απαιτούν περισσότερες τεχνικές δεξιότητες και εμπειρία.
- **Αργή Απόδοση Δικτύου:** Ο επιτιθέμενος ξεκινά μια επίθεση για να μπλοκάρει τους πόρους του συστήματος, επιτυγχάνοντας με αυτό το τρόπο την επιβράδυνση και την απόδοση του συστήματος στο εσωτερικό δίκτυο.
- **Εκδίκηση:** Οι επιτιθέμενοι αυτής της κατηγορίας έχουν χαμηλότερες τεχνικές δεξιότητες και είναι απογοητευμένοι άνθρωποι από μια αδικία που έχει γίνει στο παρελθόν, εκτελούν τις επιθέσεις ως μια εκδίκηση.
- **Ιδεολογική πίστη:** Οι επιτιθέμενοι εδώ εμπνέονται από τις ιδεολογικές πεποιθήσεις τους για να επιτεθούν στους στόχους τους. Αυτή η κατηγορία είναι μία από τις σημαντικότερες για να ξεκινήσουν επιθέσεις DdoS.
- **Διανοητική πρόκληση:** Εδώ είναι οι νέοι λάτρεις hacking enthusiasts, που θέλουν να επιδείξουν τις ικανότητές τους στις επιθέσεις στα στοχευμένα συστήματα και εκείνοι που προσπαθούν να μάθουν πως να κάνουν επιθέσεις.
- **Μη διαθεσιμότητα υπηρεσίας:** Ο εισβολέας υπερφορτώνει τις υπηρεσίες που προσφέρει το σύστημα των θυμάτων, μέσω ανεπιθύμητης ή ψεύτικης κυκλοφορίας.
- **Cyberwarfare:** Οι εισβολείς αυτής της κατηγορίας ανήκουν συνήθως σε στρατιωτικές ή τρομοκρατικές οργανώσεις μιας χώρας και έχουν πολιτικά κίνητρα να επιτεθούν σε πολλούς τομείς μιας άλλης χώρας.[9]

5.4 Είδη Επιθέσεων DDoS σε IoT

Η DDoS επίθεση είναι πολύ διαδεδομένη στο περιβάλλον δικτύωσης το οποίο χρησιμοποιεί την μη αυτόματη διαμόρφωση της τοπολογίας δικτύου **(manually configuring**). [3]

1.Volume - based : Αυτή η επίθεση στηρίζεται στο μεγάλο αριθμό requests που στέλνουν οι επιτιθέμενοι σε ένα συγκεκριμένο υπολογιστικό σύστημα, προσπαθώντας να “εξαφανίσουν” τη χωρητικότητα του δικτύου. Το σύστημα θεωρεί ότι αυτά τα requests είναι έγκυρα (valid request) ή μη έγκυρα (invalid request) και τα δέχεται δημιουργώντας πρόβλημα χώρου. Τα requests στέλνονται σε διαφορετικά σημεία του συστήματος και οι χάκερ χρησιμοποιούν επιθέσεις ενίσχυσης UDP, στις οποίες στέλνουν αίτημα για δεδομένα σε ένα third-party server. Έτσι μπορούν να πλαστογραφήσουν τη διεύθυνση IP του server ως διεύθυνση επιστροφής (return address). Στη συνέχεια ο third-party server θα στείλει τεράστιο όγκο δεδομένων στον server σαν απάντηση (response). Αυτός ο τρόπος επίθεσης μπορεί να στοχοποιήσει χιλιάδες συστήματα, αλλά ο χάκερ χρειάζεται μόνο τα αιτήματα αποστολής (dispatch requests) για να την πραγματοποιήσει.[3]

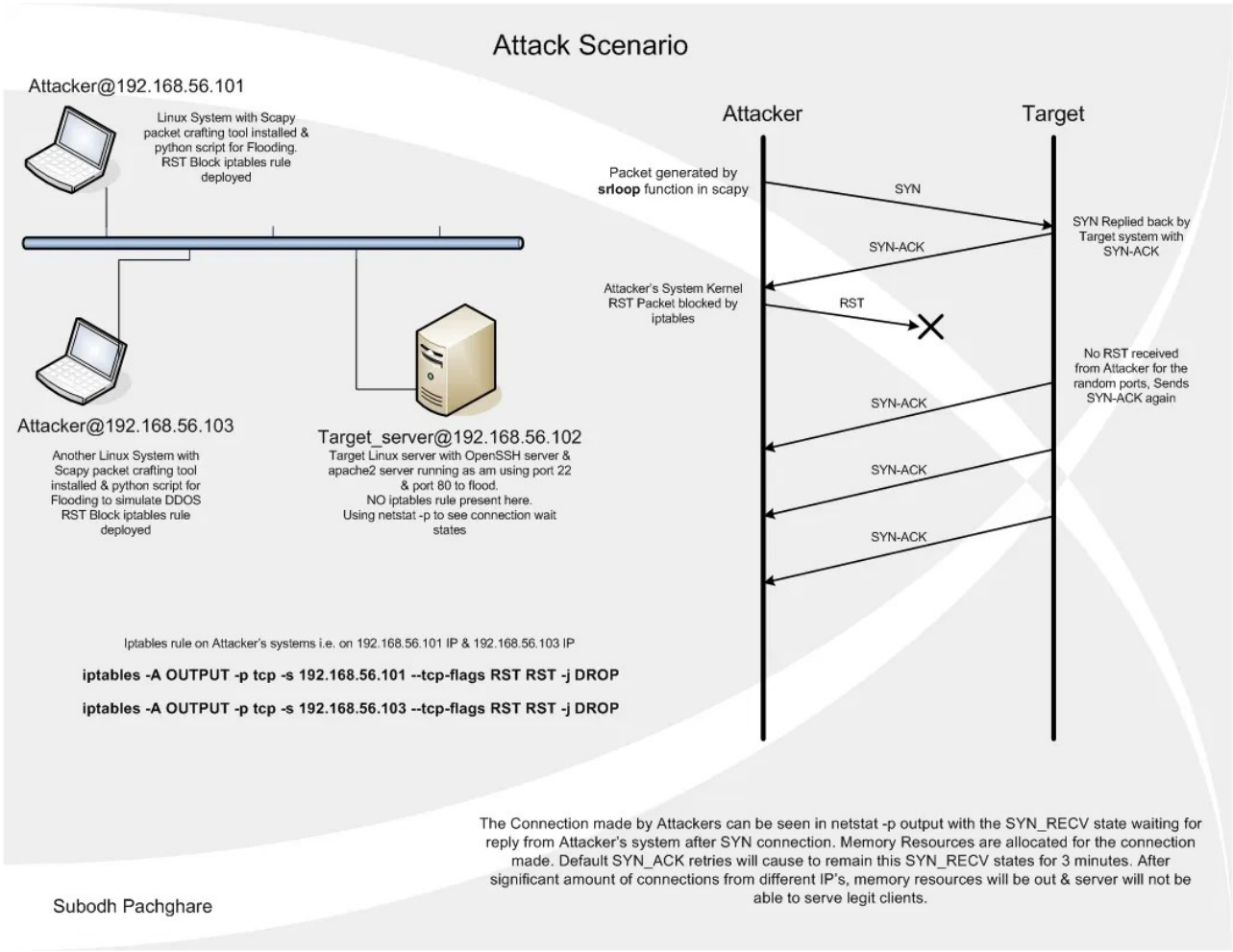
2.Application – Based : Ο χάκερ βρίσκει τα αδύναμα και τρωτά σημεία στο web server για να πραγματοποιήσει την επίθεση στο λογισμικό εφαρμογής και τον οδηγεί, σε αναστολή ή διακοπή λειτουργίας. Στέλνει requests στον server προσπαθώντας να απασχολεί όλη τη βάση δεδομένων, ώστε να σταματάει όλα τα νόμιμα requests, δημιουργώντας πρόβλημα στους νόμιμους χρήστες.[3]

3.Protocol – Based : Στόχος των επιθέσεων αυτών είναι οι servers ή οι load balancers, που εκμεταλλεύονται τις μεθόδους που χρησιμοποιούν τα συστήματα για την επικοινωνία μεταξύ τους. Τα πακέτα σχεδιάζονται, ώστε να δημιουργούν μια ανύπαρκτη απόκριση στους servers, κατά τη διάρκεια ενός regular handshake protocol, όπως μια πλημμύρα SYN flood.[3]

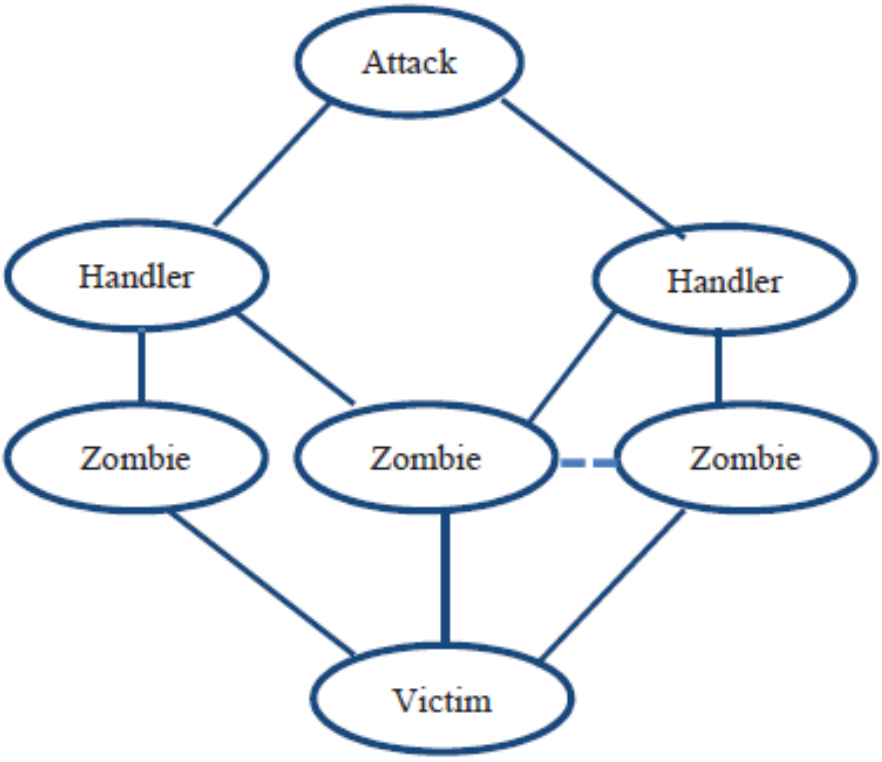
5.4.1 TCP SYN queue flood

Μια επίθεση πλημμύρας SYN εκμεταλλεύεται το "TCP protocol's "three-way handshake" του πρωτοκόλλου TCP. Ένας client στέλνει ένα πακέτο TCP SYN (S flag) για να ξεκινήσει μια σύνδεση με τον server. Ο διακομιστής προορισμού απαντά με ένα πακέτο TCP SYN-ACK (SA flag), αλλά ο client δεν αποκρίνεται στο SYN-ACK, αφήνοντας τη σύνδεση TCP «μισή-ανοικτή». Σε κανονική λειτουργία, ο client πρέπει να στείλει ένα πακέτο ACK (a flag) ακολουθούμενο από τα δεδομένα που θα μεταφερθούν ή μια απάντηση RST για να γίνει επαναφορά της σύνδεσης. Στον server προορισμού, η σύνδεση παραμένει ανοιχτή, σε κατάσταση "SYN_RECV", καθώς το πακέτο ACK ενδέχεται να έχει χαθεί λόγω προβλημάτων δικτύου.[3]

Εικόνα 5.3: TCP SYN queue flood[3]



Σε ένα DDoS, πολλοί εισβολείς κάνουν πολλές τέτοιες μισές συνδέσεις στον target server, σε μια καταιγίδα αιτημάτων (storm of requests). Όταν το buffer SYN του server γεμίσει με μισές ανοιχτές συνδέσεις TCP, σταματά να δέχεται συνδέσεις SYN, με αποτέλεσμα την άρνηση υπηρεσίας σε νόμιμους πελάτες. Τέτοιες επιθέσεις DDoS πραγματοποιούνται γενικά χρησιμοποιώντας «botnets» άλλων παραβιασμένων συστημάτων στο Διαδίκτυο, τα οποία μέσω backdoors και Trojans κατευθύνονται να στέλνουν τεχνητή κυκλοφορία floods SYN σε targeted servers. Για την άμυνα απέναντι σε τέτοιες επιθέσεις, απαιτείται ένα ισχυρό σύστημα παρακολούθησης, καθώς υπάρχει μια πολύ λεπτή γραμμή μεταξύ νόμιμων και πλαστών πελατών. Οι επιθέσεις πλημμυρών SYN μπορούν να μετριαστούν ρυθμίζοντας, τις παραμέτρους του kernel's TCP/IP.[2]Τα botnets είναι δίκτυα που αποτελούνται από υπολογιστές με τηλεχειρισμό ή "bots". Αυτοί οι υπολογιστές έχουν μολυνθεί από κακόβουλο λογισμικό που τους επιτρέπει να ελέγχονται από απόσταση. Ορισμένα botnets αποτελούνται από εκατοντάδες χιλιάδες - ή ακόμα και εκατομμύρια – υπολογιστές. Οι επιτιθέμενοι μπορούν να κατευθύνουν τους υπολογιστές στο botnet για να κατεβάσουν, επιπλέον κακόβουλο λογισμικό, όπως keyloggers, adware και ransomware. [3]

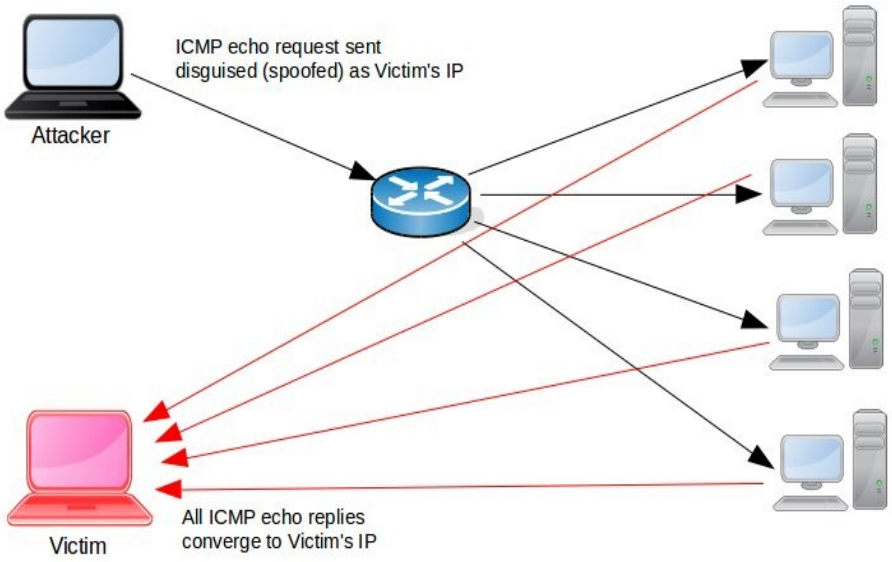


Εικόνα 5.4: Αρχιτεκτονική του DDoS Attack[3]

2 *https://www.howtogeek.com/183812/htg-explains-what-is-a-botnet/*

5.4.3 ICMP Flooding

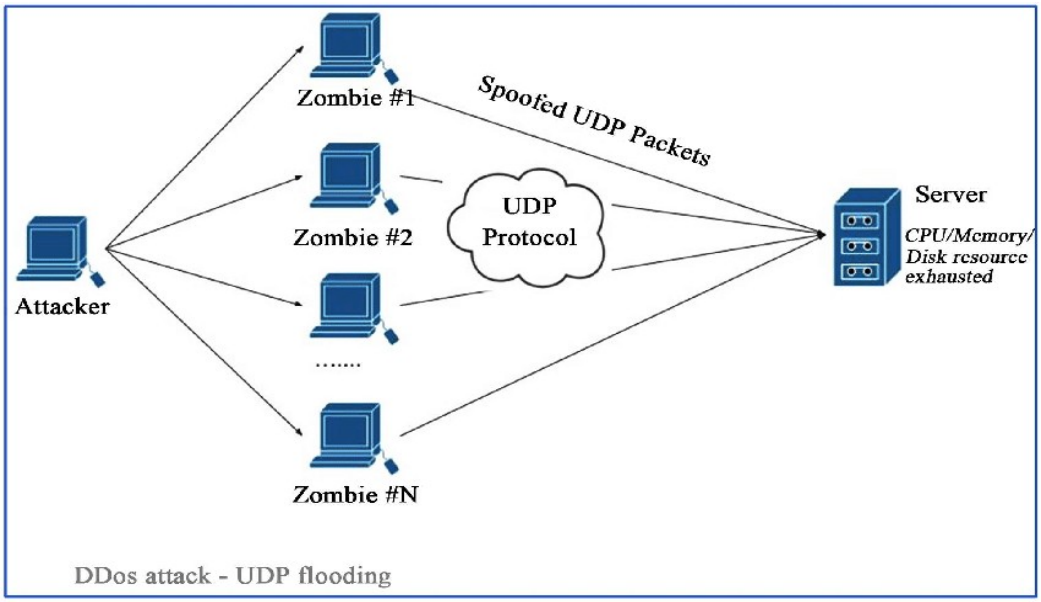
Η επίθεση διαφεύγει τα σφάλματα διαμόρφωσης στις συσκευές του δικτύου. Ο επιτιθέμενος δίνει ένα μεγάλο αριθμό πακέτων ICMP με ψευδή διεύθυνση επιστροφής στο server , ώστε να μην έχει το χρόνο να στείλει σε άλλους διακομιστές. Δεν είναι ανταλλαγή δεδομένων μεταξύ των συστημάτων. Το Network bandwidth εξαφανίζεται εξαιτίας των νομιμων πακέτων που απορρίπτονται από τους servers. Ο επιτιθέμενος εκπαιδεύει ένα slave computer μέσω ενός master computer, για να επεκτείνει την επίθεση του.[3]



Εικόνα 5.6: ICMP Flooding [27]

5.4.4 UDP Flooding

Αυτό το είδος επίθεσης χρησιμοποιεί το UDP, το οποίο είναι ένα πρωτόκολλο που λειτουργεί χωρίς σύνδεση. Δεν δεσμεύεται από μία three-way handshake όπως το TCP και λειτουργεί με lessened overhead, ώστε να μπορέσει να εκκαθαριστεί με τους μικρότερους πόρους. Οι receiving hosts, βλέπουν και ελέγχουν τις εφαρμογές με αυτά τα διαγράμματα, όταν δεν υπάρχει σχετική εφαρμογή , μπορούν να ακούσουν την ανταπόκριση με ένα πακέτο ICMP destination unreachable packet.



Εικόνα 5.7: UDP Flooding [28]

Αυτό που κινητοποίησε τους ανθρώπους ώστε να δοθεί λύση για τις επιθέσεις DDoS Attacks, ήταν η απώλεια εσόδων , η αργή απόδοση του δικτύου και το να μην είναι διαθέσιμες στους νόμιμους χρήστες οι υπηρεσίες. Ο εντοπισμός της επίθεσης είναι δύσκολος, λόγω του μη εντοπισμού των πακέτων που κάνουν την επίθεση, απο τα κανονικά πακέτα.

5.4.5 DDoS Attack σε Ασύρματα Δίκτυα

Μία επίθεση DDoS σε ένα ασύρματο δίκτυο, μπορεί να το θέσει εκτός λειτουργίας για τους νόμιμους χρήστες του. Ο επιτιθέμενος στέλνει ένα τεράστιο όγκο αιτημάτων (**requests)** με σκοπό να προκαλέσει υπερφόρτωση στο server. Χρησιμοποιεί πλαστογραφημένη διεύθυνση IP και οι χρήστες δεν μπορούν να επικοινωνήσουν και να χρησιμοποιήσουν υπηρεσίες για κάποιο χρονικό διάστημα, αφού υπάρχει μεγάλη κυκλοφορία δεδομένων (**traffic)**. Είναι μία από τις πιο επικίνδυνες επιθέσεις που μπορούν να συμβούν σε οποιοδήποτε επίπεδο των ασύρματων δικτύων. Για την προστασία τους χρειάζονται μέτρα υψηλού επιπέδου.[2]

Dos Επιθέσεις σε διαφορετικά επίπεδα των ασύρματων δικτύων

- **Physical Layer** : Το jamming attack είναι μία από τις πιο σημαντικές επιθέσεις που επηρρεάζουν το φυσικό επίπεδο. Επηρρεάζει κυρίως την επικοινωνία ανάμεσα στους νόμιμους χρήστες και η επίθεση μπορεί να πραγματοποιηθεί από οποιαδήποτε θέση στο δίκτυο (mesh network). Υπάρχουν δύο είδη επιθέσεων jamming :a) Channel – Selective Jamming και b) Data- Selective Jamming.

- **Link Layer** : Είναι πολύ ευάλωτο σε selfish επιθέσεις και συγκρούσεις (collisions). Οι selfish επιθέσεις θα βοηθήσουν στη βελτίωση του bandwidth, της απόδοσης και του QoS του selfish κόμβου με αντίτιμο ένα άλλο κόμβο.[2]
- **Network Layer** : Το συγκεκριμένο επίπεδο είναι πολύ εύαλωτο σε διαφορετικούς τύπους επιθέσεων DoS Attacks. Οι επιτιθέμενοι εξαντλούν τους πόρους του δικτύου και με αυτό τον τρόπο υποβαθμίζουν την απόδοση του δικτύου.Black hole attack είναι ένας τύπος επίθεσης dos στον οποίο ο κακόβουλος κόμβος node απορροφά όλη την κίνηση που πηγαίνει προς τον κόμβο στόχου (target node). Στην επίθεση Grey Hole , ο κακόβουλος κόμβος προωθεί επιλεκτικά το πακέτο στον κόμβο προορισμού (destination node). Η επίθεση τύπου Wormhole είναι ένας άλλος τύπος επίθεσης Dos, στην οποία ο επιτιθέμενος σε ένα δίκτυο καταγράφει τα bit σε μια τοποθεσία, τα διοχετεύει επιλεκτικά σε άλλη τοποθεσία και τα μεταδίδει ξανά στο δίκτυο.[2]
- **Transport Layer** : Σε αυτό το επίπεδο περιλαμβάνονται οι SYN flooding attacks και οι desynchronization attacks. Η SYN flooding attack αρνείται την νόμιμη πρόσβαση σε υπηρεσία. Ο επιτιθέμενος δημιουργεί ένα μεγάλο νούμερο από half opened TCP συνδέσεις με ένα θύμα κόμβο αλλά δεν ολοκληρώνει το handshake ώστε να ανοίξει η επικοινωνία. Στην de-synchronization attack ένας κακόβουλος κόμβος, αποσυγχρονίζει έναν επικυρωμένο κόμβο κινητής τηλεφωνίας από το σταθμό βάσης, αναγκάζοντας τον κόμβο κινητού να επαναπροσδιοριστεί.[2]

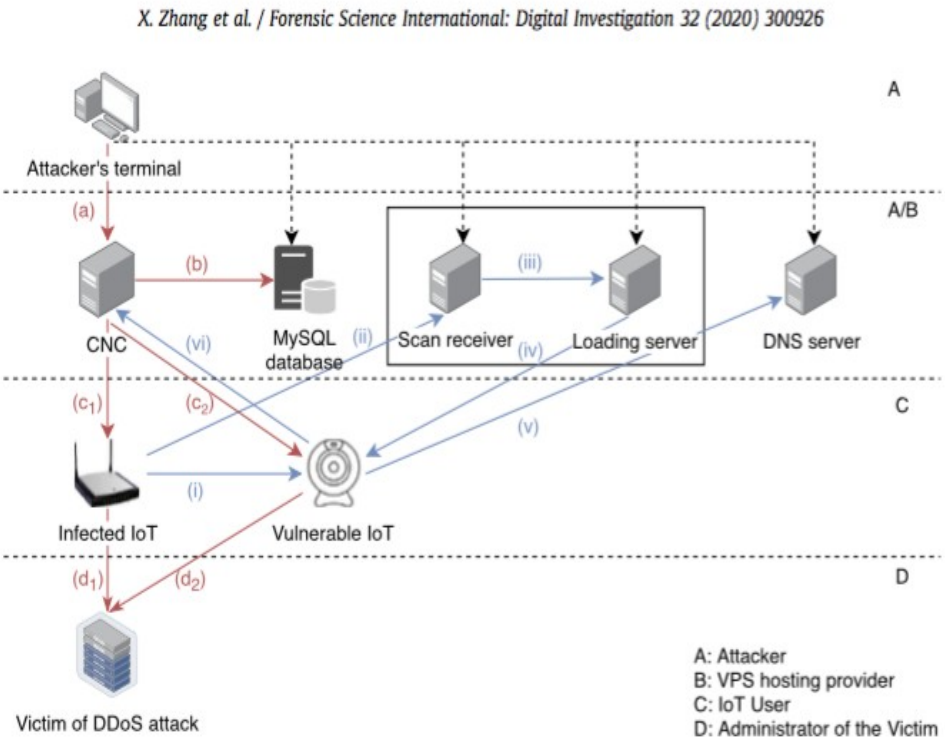
5.4.6 The Mirai botnet

Το **Mirai botnet** είναι διαδεδομένο στις συσκευές **Internet of Things (IoT).** Η δημόσια κυκλοφορία του source code1 που κυκλοφόρησε το 2016 οδήγησε σε ένα μεγάλο αριθμό παραλλαγών Mirai και σε αυξημένη συχνότητα επιθέσεων Distributed Denial of Service (DDoS) (Antonakakis et al., 2017). Το Μιράι, που σημαίνει «μέλλον» στα Ιαπωνικά, παρουσιάζοντας ένα γεγονός περισσότερο από μία φορά, διαμόρφωσε το μέλλον των σημαντικών επιθέσεων που πρόκειται να συμβούν. Πολλές έρευνες για το Mirai μέχρι σήμερα, έχουν επικεντρωθεί σε μια παραδοσιακή ανάλυση κακόβουλου λογισμικού του εκτελέσιμου κώδικα που βρέθηκε σε infected IoT συσκευές, οι οποίες μπορούν να συλλεχθούν από μια infected device ή ένα honeypot*. [5]

*(3*To honeypot είναι ένας υπολογιστής ή ένα σύστημα υπολογιστή που προορίζεται να μιμηθεί πιθανούς στόχους των κυβερνοεπιθέσεων. Μπορεί να χρησιμοποιηθεί για τον εντοπισμό επιθέσεων ή την εκτροπή τους από έναν νόμιμο στόχο. Μπορεί να χρησιμοποιηθεί για την απόκτηση πληροφοριών σχετικά με τον τρόπο λειτουργίας των εγκληματιών στον κυβερνοχώρο).*

3 *https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html*

Πρέπει να διερευνηθούν οι control servers , εάν μπορούν να συλλεέξουν ή να έχουν πρόσβαση από απόσταση, επειδή περιέχουν βασικές πληροφορίες για ολόκληρο το botnet και όχι μόνο γα μια παραβιασμένη συσκευή IoT. Οποιοσδήποτε μπορεί να φτιάξει ένα προσαρμοσμένο (customized Mirai botnet) χρησιμοποιώντας public source code. Παρόλαυτα οι περισσότεροι επιτιθέμενοι δεν μπορούν ή δεν ξέρουν πως να κάνουν αλλαγές στο πηγαίο κώδικα (source code).[5]



Εικόνα 5.8: Mirai botnet Τοπολογία [5]

Στην παραπάνω εικόνα φαίνεται η τοπολογία ενός **Mirai botnet,** όπου οι botnet servers και οι συσκευές IoT, καθώς και ο κεντρικός υπολογιστής εισβολέα DDoS και ο κεντρικός υπολογιστής θύματος έχουν ρυθμιστεί σε ξεχωριστά υποδίκτυα 192.168.1.0/24 και 192.168.4.0/24, αντίστοιχα. Οι συσκευές από τα δύο υπο-δίκτυα μπορούν να επικοινωνούν μεταξύ τους μέσω ενός router. Δεδομένου ότι ο δρομολογητής (router) δεν είναι ένα απαιτούμενο στοιχείο για ένα botnet Mirai, χρησιμοποιήθηκε το router και ως Terminal, στο οποίο ένας εισβολέας μπορεί να συνδεθεί στον CNC server. Οι αλλαγές που έγιναν στον αρχικό Mirai source code ήταν ελάχιστες, συμπεριλαμβανομένης της αλλαγής ορισμένων βασικών διευθύνσεων IP addresses, καθώς και ελάχιστων απαραίτητων αλλαγών στο αρχείο διαμόρφωσης των servers. [5]

Ο διακομιστής βάσης δεδομένων MySQL διαμορφώθηκε για να υποστηρίζει απομακρυσμένη πρόσβαση από τον CNC server. Τα διαπιστευτήρια σύνδεσης (login credentials) του CNC server αποθηκεύτηκαν σε έναν πίνακα της βάσης δεδομένων. Η IP address και τα login credentials της βάσης δεδομένων MySQL ήταν κωδικοποιημένα στον CNC server. Ένα bot (εκτελέσιμο) τροποποιήθηκε για να συμπεριλάβει τη διεύθυνση IP του DNS server. Αυτό κωδικοποιείται στη συσκευή IoT που έχει μολυνθεί με bot. Ένας αδύναμος κωδικός πρόσβασης ορίστηκε στον «root» χρήστη της συσκευής «Vulnerable IoT» και αυτός ο κωδικός πρόσβασης συμπεριλήφθηκε στο λεξικό κωδικών πρόσβασης Mirai για να διασφαλιστεί ότι η συσκευή «Vulnerable IoT» μπορεί να εντοπιστεί από τη μολυσμένη συσκευή IoT. [5]

Σύμφωνα με τον σχεδιασμό του Mirai, ένας attacker πρέπει να έχει πρόσβαση στον CNC server μέσω remote/local Telnet connection. Όταν πραγματοποιείται η σύνδεση, τα user credentials (που βρίσκονται αποθηκευμένα στον database server) πρέπει να επαληθευτούν για σύνδεση(logging in). Αν η σύνδεση είναι επιτυχής, ο CNC server παρέχει ένα dedicated shell όπου μπορεί να γίνει ένας συγκεκριμένος τύπος επίθεσης DdoS. Ο CNC server είναι ένας από τους πιο πολύτιμους servers στο botnet Mirai. Είναι υπεύθυνος για την issuing attacking στα bots και για την αναμονή για την εγγραφή των νέων μολυσμένων συσκευών IoT. Τα κύρια ευρήματα εξήχθησαν από: 1) το εκτελέσιμο αρχείο (executable file) της υπηρεσίας CNC, 2) τα δεδομένα μνήμης (memory data) της διαδικασίας CNC και 3) τα πακέτα δικτύου (network packets) που έχουν χαραχθεί από την εικόνα μνήμης του CNC.[5]

Κάποια εύκολα ανακτήσιμα και πολύτιμα forensic artifacts μπορεί να είναι διαθέσιμα στον server CNC, ο οποίος μπορεί να περιλαμβάνει τα ready-to-compile source code files, τα οποία ο εισβολέας απέτυχε να αφαιρέσει. Σε αυτήν την περίπτωση, η hard-coded database server's IP address και τα login credentials μπορούν να βρεθούν σε αυτό το αρχείο / Mir-ai-Source-Code / mirai / cnc / main.go σε clear-text. Ένα άλλο σημαντικό artifact που περιλαμβάνεται σε αυτό το αρχείο είναι το όνομα του πίνακα της Mirai database, όπου αποθηκεύονται τα user credentials CNC και το command history. Με αυτά μπορεί κανείς να έχει πρόσβαση στο database server και να απορρίψει ολόκληρη τη βάση δεδομένων.[5]

Ο CNC server διατηρεί few queues on the fly, οι οποίες χρησιμοποιούνται για τη διατήρηση των ενεργών - active bots, των διαγραμμένων - deleted bots και των bots που εκτελούν επιθέσεις bots carrying out attacks, αντίστοιχα. Από τη δομή δεδομένων του ClientList που περιλαμβάνεται στο αρχείο πηγαίου κώδικα / Mirai-Source-Code / mirai / cnc / clientList.go, μπορεί να βρεθεί η δομή ClientList data structure. Τα δεδομένα στις ουρές (data in the queues) είναι σημαντικά για την ανάκτηση των πληροφοριών, σχετικά με τα bots από τον server CNC και η απόρριψη μνήμης (memory dump), είναι η πιο σημαντική και μπορεί να είναι η μόνη διαθέσιμη πηγή δεδομένων για την ανάκτηση της ολοκληρωμένης λίστας bots (recovering the integrated list of bots). Το Mirai κυκλοφόρησε για πρώτη φορά σε initial attacks τον Αύγουστο του 2016 και έδινε έμφαση στη περιορισμένη ασφάλεια που έχουν πολλές συσκευές IoT. [5]

Κεφάλαιο 6

Στο κεφάλαιο 6 γίνεται αναφορά στις ανιχνεύσεις των επιθέσεων DDoS και πως αυτές πραγματοποιούνται. Γίνεται κατηγοριοποιήση των ανιχνεύσεων ανάλογα με τις μεθόδους που χρησιμοποιούνται κάθε φορά όπως είναι : οι μέθοδοι ανίχνευσης soft computing, οι μέθοδοι βασιζόμενοι στη προηγούμενη γνώση, οι μέθοδοι εξόρυξης και οι μέθοδοι μηχανικής μάθησης. Τέλος αναφέρονται οι ανιχνεύσεις και οι άμυνες που χρησιμοποιούνται σήμερα.

6.1 Ανιχνεύσεις επιθέσεων DDoS στο IoT

6.1.1 Ανίχνευση της DDoS σε ασύρματα δίκτυα

Υπάρχει ένα πρωτόκολλο το **DSLR** (A DDoS Attack preventing optimized link state routing protocol), που μπορεί να ανιχνεύσει DoS Attack σε ένα ασύρματο δίκτυο. Με αυτό το σύστημα μπορεί να γίνει ανίχνευση και απομάκρυνση των κακόβουλων πακέτων καθώς περνάνε από αυτό. Η λειτουργία του αποτελείται κυρίως απο 3 φάσεις: [3]

1. DDoS detection

2. Attack Identification

3. The DDoS defense phase

Στην πρώτη φάση της ανίχνευσης στο server ανατίθεται, πόσα αιτήματα μπορεί να δεχθεί και να επεξεργαστεί (service capacity), το ανώτερο για συγκεκριμένο χρόνο. Ο server δείχνει στην οθόνη πόσα είναι τα εισερχόμενα πακέτα. Όταν μία επίθεση ανιχνευθεί, ένα DALERT packet στέλνεται σε όλους τους κόμβους, για να τους γνωστοποιήσει ότι έχει εντοπιστεί μια DDoS Attack και μπαίνουν στη φάση της αναγνώρισης (Identification). Οι κόμβοι θα δούν την IP adress από το DALERT packet. Οι κόμβοι δεν μπορούν να δούνε περισσότερες πληροφορίες για το ποιός κάνει την επίθεση. Θα εξετάσουν πρώτα όλη την εισερχόμενη κυκλοφορία και θα σημειώσουν ποιοί host, προσπαθούν να στείλουν πολλά requests, ώστε να τους αναγνωρίσουν ως attacker host. Η πληροφορία αυτή στέλνεται και στους υπόλοιπους κόμβους, χρησιμοποιώντας ένα πακέτο πληροφορίας για τους επιτιθέμενους AIP – Attackers Information Packet. Από εκείνη τη στιγμή και έπειτα μπαίνουμε στη τρίτη φάση που αποτελεί και την άμυνα (defense) για την επίθεση. Αφού έχουν λάβει το πακέτο πληροφορίας οι κόμβοι μπορούν να αναγνωρίσουν τους επιτιθέμενους hosts και να απορρίψουν όλα τα πακέτα που προέχονται από εκείνους, αποτρέποντας την επίθεση.[3]

Το πλεονέκτημα είναι ότι μπορεί να ανιχνεύσει και να εμποδίσει την επίθεση, σε ένα ασύρματο δίκτυο.

Το μειονέκτημα είναι ότι χρησιμοποιεί μεγάλο μέρος ενέργειας, ώστε να εντοπίσει τους επιτιθέμενους, με αποτέλεσμα να δημιουργούνται καθυστερήσεις στο δίκτυο.

6.1.2 Τεχνική IP Traceback

Στην συγκεκριμένη μέθοδο χρησιμοποιούμε IP spoofing, μέσω του οποίου μπορούμε να βρούμε την προέλευση των πακέτων που μεταδίδονται. Το πρόβλημα είναι η ανίχνευση της πηγής μιάς επίθεσης, που οφείλεται σε μία ανακριβή IP address. Η IP traceback, βοηθάει στο φιλτράρισμα και τον έλεγχο των ύποπτων κινήσεων και πραγματοποιείται όταν γίνεται η ανίχνευση της επίθεσης. Χωρίζεται σε IDS και Non-IDS assisted. Η προληπτική προσέγγιση (Proactive approach-In) εντοπίζει τις πληροφορίες με τη μορφή πακέτων καθώς περνούν στο δίκτυο. Το θύμα χρησιμοποιεί τα δεδομένα ανίχνευσης για την αναγνώριση του εισβολέα και ανακατασκευάζει τη διαδρομή επίθεσης. Επίσης είναι περιορισμένη ως Out-of-Band και In-Band information.[3]

6.1.3 Τεχνική σήμανσης πακέτων

Η σήμανση πακέτων, χαρακτηρίζει τις μεθόδους Traceback. Οι τεχνικές που χρησιμοποιούνται για να μαρκάρουμε τα πακέτα είναι PPM - Probabilistic packet marking και DPM - Deterministic packet marking. Στην PPM τα πακέτα “μαρκάρωνται” απο τους routers καθώς περνάνε απο εκείνους. Προκειμένου να μπερδέψουν το θύμα στέλνουν deceived information, αναγκάζοντάς το να ανακατασκευάζει τον τρόπο που περνάνε τα πακέτα επίθεσης. Αυτό μπορεί να γίνει με δύο τρόπους : α) Node marking είναι η σήμανση κόμβου όπου χρησιμοποιεί τη διεύθυνση IP του δρομολογητή.β) Edge marking είναι η σήμανση άκρων όπου χρησιμοποιεί τις άκρες των διαδρομών. Αυτή η μέθοδος χρησμιμοποιεί υψηλό υπολογιστικό φορτίο, εξαιτίας του μεγάλου όγκου στον αριθμό πακέτων. Το μειονέκτημα είναι ο διαθέσιμος χώρος που δεν υπάρχει, λόγω του διαγράμματος επίθεσης που πρέπει να ανακατασκευαστεί. [3]

6.1.4 Παραλλαγή εντροπίας - Entropy Variation

Η μέθοδος της Entropy σχετίζεται με το τη κυκλοφορία του συστήματος και χρησιμοποιήται για την ανίχνευση των ανωμαλιών που μπορεί να παρουσιαστούν. Απεικονίζει τη συγκέντρωση και διάδοση των χαρακτηριστικών της κυκλοφορίας. Η Entropy εξαρτάται μόνο από τις τιμές που υπολογίζονται σε κάθε πεδίο πακέτου. Οι παραλλαγές χρησιμοποιούνται για τον εντοπισμό της πηγής των επιθέσεων DDoS. Μπορεί να διακρίνει μία DDoS attack traffic από μία παραδοσιακή DoS attack. Επίσης διακρίνει την τυχαία αλλαγή των ροών στο router, χρησιμοποιώντας αποκλίνουσες μετρήσεις για κανονικές παραλλαγές (normal variation) ή ροές υψηλής τάσης (high order moments of flow). Ο αλγόριθμος ανίχνευσης έχει κατασκευαστεί ώστε να τρέχει σε ολόκληρους τους routers στο LAN και να για να παρακολουθείται η κυκλοφορία του δικτύου. [3]

6.1.5 Σύστημα ανίχνευσης και πρόληψης εισβολής (IDS / IPS)

Είναι ένα σύστημα με τη μορφή μιας εφαρμογής, που παρακολουθεί το δίκτυο για ύποπτα συμβάντα και δημιουργεί μια αναφορά στον διαχειριστή για να λάβει μέτρα εναντίον τους. Τέτοια συμβάντα μπορούν να είναι: οι Traditional IDS/IPS τεχνικές, όπως η ανίχνευση βάσει υπογραφής, η ανίχνευση ανωμαλιών (Signature Based Detection - Anomaly Detection). [3]

6.1.6 Ανίχνευση βάσει υπογραφής

Η ανίχνευση Signature Based Detection με τη χρήση κανόνων – υπογραφών με προκαθορισμένη βάση γνώσεων, προσπαθεί να εντοπίσει τυχόν επίθεση. Υπάρχει συνεχής ενημέρωση των κανόνων στη βάση δεδομένων. Δημιουργεί μια υπογραφή για κάθε χρήστη που δηλώνει αν ο χρήστης είναι ύποπτος. Το Captcha χρησιμοποιείται για τον προσδιορισμό της υπογραφής αν δηλαδή αντιπροσωπεύει επίθεση ή νόμιμο χρήστη. Η λειτουργία του έχει να κάνει με το φορτίο στο server που αν είναι χαμηλό τότε δεν το μπλοκάρει, σε περίπτωση όμως που το φορτίο ανεβαίνει πανω απο το LLT (low load threshold - χαμηλό όριο φόρτωσης), τότε εντοπίζονται και καθυστερούνται ύποπτοι χρήστες. Εαν φτάσει στο HLT (high level thresold - υψηλό όριο υψηλού επιπέδου), οι ύποπτοι χρήστες μπλοκάρονται. Όταν η κυκλοφορία με παρόμοια υπογραφή είναι έγκυρη, τότε δεν μπλοκάρονται, ούτε καθυστερούν οι χρήστες. Οι χρήστες καθυστερούν και αποκλείονται απο το σύστημα σε περίπτωση επαναλαμβανόμενης αποτυχίας της υπογραφής τους. [3]

6.1.7 Ανίχνευση ανωμαλιών

Η Ανίχνευση ανωμαλιών έχει να κάνει με τον εντοπισμό συμβάντων που φαίνεται να μην είναι φυσιολογικά σε σχέση, με τη συμπεριφορά του συστήματος. Χρησιμοποιούνται τεχνικές όπως είναι η εξόρυξη δεδομένων, η στατιστική μοντελοποίηση και τα κρυφά μοντέλα markov. Μπορεί να αποφασίσει αν μία συμπεριφορά είναι νόμιμη, ανάλογα με τη συμπεριφορά των νόμιμων χρηστών για μια χρονική περίοδο. Δημιουργεί κανόνες για τη μείωση των ψευδών συναγερμών (false alarm), για γνωστές και άγνωστες επιθέσεις.[3]

6.2 Ανιχνεύσεις επιθέσεων DDos με Μεθόδους Soft Computing

6.2.1 ANN

Τα δίκτυα (ANN - Artificial Neural Networks), οι radial basis functions και οι γεννετικοί αλγόριθμοι, χρησιμοποιούνται στην ανίχνευση επιθέσεων DDoS λόγω της ικανότητάς τους, να ταξινομούνται έξυπνα και αυτόματα. Η μέθοδος Soft computing είναι η περιγραφή ενός συνόλου τεχνικών βελτιστοποίησης και επεξεργασίας, που αντέχουν την αβεβαιότητα και την ανακρίβεια των στοιχείων. Χρησιμοποιούνται ώστε να αντιμετωπίζουν ένα περιβάλλον που συνεχώς μεταβάλλεται και είναι self-learning. [6]

6.2.2 LVQ

Υπάρχει το μοντέλο (Linear Vector Quantization- LVQ) που είναι ίδιο με τους self-organizing maps και εφαρμόζει τις τεχνικές αναγνώρισης προτύπων, ταξινόμησης πολλαπλών επιπέδων και συμπίεσης δεδομένων. Στην εποπτευόμενη εκμάθηση, γνωρίζει την παραγωγή στόχου έναντι διαφορετικών μορφών προτύπων εισόδου (input patterns). Το LVQ είναι πιο ακριβές στον προσδιορισμό επιθέσεων DDoS από το μοντέλο(BP - Back propagation). Το LVQ είναι 99,723% πιο ακριβές κατά μέσο όρο έναντι του δοκιμασμένου συνόλου δεδομένων(tested dataset), ενώ η μέση ακρίβεια του BP είναι 89.9259% για το ίδιο σύνολο δεδομένων. Οι ακρίβειες υπολογίζονται με βάση τα ποσοστά των ληφθέντων ψευδών θετικών (False positives) και ψευδών αρνητικών (false negatives) σε κάθε δείγμα δεδομένων δοκιμής. Υπάρχουν 10 δείγματα που χρησιμοποιούνται για τη δοκιμή των συστημάτων για καθένα από τα μοντέλα LVQ και BP. Το νευρωνικό δίκτυο BP εκπαιδεύεται με ένα σύνολο δεδομένων παραλλαγών (entropy variations dataset) ως εισόδους και δυναμικά DDoS ως έξοδους. Επίσης το σύστημα δοκιμάζεται με διακυμάνσεις (tested with variations) στο μέγεθος του δικτύου. Ο αριθμός των νευρώνων στο στρώμα επεξεργασίας σε πραγματικές περιπτώσεις, αυξάνει το μέγεθος του δικτύου καθώς επίσης και τον χρόνο εκπαίδευσης όσο και το κόστος εφαρμογής. [6]

6.2.3 TDNN

Το TDNN - Time Delay Neural Network, είναι ένα νευρωνικό δίκτυο που βασίζεται στη στατιστική γνώση και στο ποιος παράγοντας χρονικής καθυστέρησης (time delay factor) κρύβεται μέσα στο αντιπροσωπευτικό σήμα (representative signal). Δημιουργήθηκε μια αποστρατικοποιημένη ζώνη (DMZ - Demilitarized Zone) και το TDNN υλοποιείται σε μοτίβο δύο επιπέδων (two-layer pattern). Η ενέργεια του κόμβου παρακολουθείται από γειτονικούς κόμβους και οι πληροφορίες επίθεσης αποστέλλονται στην ειδική ενότητα για μια ολοκληρωμένη ανάλυση. Η πολυεπίπεδη δομή επιτρέπει στο σύστημα να διασφαλίσει κατάλληλες ενέργειες ως προληπτική στρατηγική κατά των επιθέσεων DDoS. Τα αποτελέσματα ανίχνευσης στην αναπτυσσόμενη αρχιτεκτονική δείχνουν ότι το προτεινόμενο σχήμα είναι ικανό να δώσει 82,7% σωστό ρυθμό ανίχνευσης σε σύγκριση με το 46,3% με το γενικό σύστημα ανίχνευσης εισβολής (IDS - Intrusion Detection System). [6]

6.2.4 SPUNNID

Το **SPUNNID** είναι ένα σύστημα ανίχνευσης επιθέσεων DDoS, που βασίζεται σε ένα στατιστικό προεπεξεργαστή και ένα τεχνητό νευρωνικό δίκτυο χωρίς επίβλεψη. Χρησιμοποιεί στατιστική προεπεξεργασία για εξαγωγή χαρακτηριστικών από την κυκλοφορία και χρησιμοποιεί ένα μη εποπτευόμενο νευρωνικό δίκτυο, για ανάλυση και ταξινόμηση της κυκλοφορίας ως επίθεση ή κανονική κίνηση.[6]

6.2.5 RBF

Το Radial Basis Function (RBF) είναι μια μέθοδος ανίχνευσης με βάση τα χαρακτηριστικά της ανάλυσης πακέτων επίθεσης. Εφαρμόζεται για να ταξινομήσει τα δεδομένα ως κανονικά ή κάποια που αφορούν πιθανές επιθέσεις. Εάν η εισερχόμενη κίνηση αναγνωρίζεται ως κίνηση επίθεσης, η διεύθυνση IP προέλευσης πακέτων επίθεσης αποστέλλεται στη μονάδα φιλτραρίσματος (Filtering Module) και η μονάδα συναγερμού επίθεσης (Attack Alarm Module) εκτελεί περαιτέρω ενέργειες. Διαφορετικά, εάν η κίνηση είναι κανονική, κατευθύνεται στον προορισμό της. Οι επιθέσεις DDoS σε δημόσια δίκτυα βασίζονται σε στατιστικά χαρακτηριστικά που υπολογίζονται σε σύντομο χρονικό διάστημα και αναλύουν τα εισερχόμενα πακέτα δεδομένων. Ένας μικρός αριθμός στατιστικών παραμέτρων χρησιμοποιούνται για τον καθορισμό της συμπεριφοράς των επιθέσεων DDoS και μια ακριβής ταξινόμηση επιτυγχάνεται με τη χρήση της μεθόδου. [6]

6.2.6 Ανίχνευση Δέντρων

Η ανίχνευση των επιθέσεων μπορεί να θεωρηθεί και ως πρόβλημα ταξινόμησης. Χρησιμοποιούνται για το λόγο αυτό δέντρα αποφάσεων τα οποία μέσα από 15 χαρακτηριστικά (attributes), παρακολουθούν το ρυθμό εισερχομένων / εξερχόμενων πακέτων / byte (incoming/outgoing packet/byte) και συλλέγουν τους ρυθμούς σηματοδότησης TCP, SYN και ACK, για να καθορίσουν το traffic flow pattern. Η μέθοδος του δέντρου αποφάσεων χρησιμοποιείται για την ανάπτυξη ενός ταξινομητή για την ανίχνευση μη φυσιολογικής ροής κυκλοφορίας και για τον εντοπισμό της προέλευσης μιας επίθεσης (origin of an attack).[6]

6.3 Μέθοδοι Ανίχνευσης που βασίζονται στη γνώση

Στις μεθόδους knowledge based τα συμβάντα ή οι ενέργειες δικτύου δοκιμάζονται βάσει προκαθορισμένων κανόνων ή μοτίβων επίθεσης. Οι γενικές παραστάσεις γνωστών επιθέσεων ονομάζονται υπογραφές επίθεσης (attack signatures) και αυτές είναι 24 και μπορούν να διατυπωθούν βάσει πραγματικών επιθέσεων. Οι Knowledge-based μέθοδοι περιλαμβάνουν συστήματα εμπειρογνωμόνων(expert systems), ανάλυση υπογραφής(signature analysis), χάρτες αυτο-οργάνωσης(self-organizing maps) και ανάλυση μετάβασης κατάστασης(state transition analysis). [6]

6.3.1 Δέντρο MUlti-Level για διαδικτυακά στατιστικά πακέτων

Υπάρχει η ευρετική δομή δεδομένων MULTOPS (MUlti-Level Tree for Online Packet Statistics), η οποία παρακολουθεί τα χαρακτηριστικά της κυκλοφορίας των συσκευών δικτύου, όπως οι routers για να εντοπίζουν και να μειώνουν τις επιθέσεις DDoS. Το MULTOPS είναι ένα δέντρο κόμβων (a tree of nodes), που περιλαμβάνει στατιστικά στοιχεία ρυθμού κίνησης για προθέματα υποδικτύου, σε διαφορετικά επίπεδα συγκέντρωσης και ήταν επέκταση και σύγκριση με το δέντρο σε προκαθορισμένο μέγεθος μνήμης.Επίσης δεν μπορεί να εντοπίσει επιθέσεις που έχουν μεγάλο αριθμό ροών επίθεσης και μπορεί να προκαλέσει ζημιά.[6]

6.3.2 Μηχανισμός NetBouncer

Ο μηχανισμός NetBouncer μπορεί να διακρίνει τη νόμιμη και παράνομη χρήση των πόρων και να διασφαλίσει ότι χρησιμοποιούνται μόνο για νόμιμη χρήση. Μπορεί να διαχωρίσει τη ροή της κυκλοφορίας ανάμεσα σε αναγνωρισμένους νόμιμους πελατες και σε πακέτα που λαμβάνονται από πελάτες που δεν περιλαμβάνονται στη νόμιμη λίστα. Μια συσκευή NetBouncer προσκαλεί ένα διαχειριστή να εκτελεί πολλές δοκιμές, ώστε να ελέγξει τον πελάτη και να αποδείξει τη νομιμότητά του. Όταν ο πελάτης αποδείξει την εξουσιοδότησή του (authorization), προστίθεται στη λίστα νομιμότητας και γίνονται δεκτά όλα τα πακέτα από εκείνον. [6]

6.3.3 Αλγόριθμος Αυξημένου δέντρου επίθεσης

Ο αλγόριθμος AAT - Augmented Attack Tree, ανιχνεύει επιθέσεις DDoS attacks και μπορεί να καταγράψει με λεπτομέρειες περιστατικά που προκαλούν οι συγκεκριμένες επιθέσεις. Ένα τέτοιο περιστατικό είναι οι αλλαγές κατάστασης(state changes), από την παρατήρηση της μετάδοσης κίνησης δικτύου (traffic transmission) στον πρωτεύοντα victim server. Ο αλγόριθμος AAT είναι προηγμένος γιατί μπορεί να μας παρέχει πληροφορίες όπως η διαδικασία μετάβασης κατάστασης(state transition process) . [6]

6.3.4 Υπογραφές επίθεσης DDoS

Οι Limwiwatkul και Rungsawang ανακάλυψαν τις υπογραφές επίθεσης DDoS (DDoS attack signatures) αναλύοντας την κεφαλίδα πακέτου TCP / IP packet header, έναντι προκαθορισμένων κανόνων και προϋποθέσεων και αναγνωρίζοντας τη διαφορά μεταξύ της κανονικής και της abnormal ροής κυκλοφορίας. Αυτές επικεντρώνονται κυρίως σε επιθέσεις πλημμύρας ICMP, TCP και UDP.[6]

6.3.5 Κατανεμημένη προσέγγιση

Υπάρχει μια κατανεμημένη προσέγγιση Distributed Approach, η οποία μας βοηθάει στην ανίχνευση DDoS attacks και είναι ανεξάρτητη σύμφωνα με τους Zhang και Parashar. Εδώ αναπτύσσονται αμυντικά συστήματα στο δίκτυο και με τη μέθοδο αυτή εντοπίζονται και σταματάνε οι επιθέσεις εντός του ενδιάμεσου δικτύου (intermediate network). Χρησιμοποιείται μια επικοινωνία IRC μεταξύ των ανεξάρτητων κόμβων ανίχνευσης (independent detection nodes), για ανταλλαγή πληροφοριών σχετικά με επιθέσεις δικτύου και ο συνδυασμός αυτών των πληροφοριών, χρησιμοποιείται για την αντιμετώπιση των επιθέσεων στο δίκτυο(aggregate network attacks). Οι μεμονωμένοι κόμβοι άμυνας (Individual defence nodes) λαμβάνουν πληροφορίες σχετικά με εκτιμήσεις για επιθέσεις global network attacks και σταματούν τις επιθέσεις με αποτελεσματικότητα και ακρίβεια, χρησιμοποιώντας τις συγκεντρωτικές πληροφορίες του δικτύου. [6]

6.3.6 Σύστημα άμυνας DDoS με βάση την περίμετρο

Σε αυτή τη μέθοδο η κυκλοφορία των δεδομένων αναλύεται σε edge routers του δικτύου ενός παρόχου υπηρεσιών διαδικτύου (ISP - Internet Service Provider). Το σύστημα άμυνας DDoS αποτελείται από δύο κύρια συστατικά: (1) Temporal-correlation, δηλαδή εξαγωγή χαρακτηριστικών βάσει χρονικής συσχέτισης και (2) Spatial-correlation, δηλαδή ανίχνευση βάσει χωρικής συσχέτισης. Προσδιορίζει και εντοπίζει με ακρίβεια επιθέσεις DDoS χωρίς να αλλάζει τους υπάρχοντες μηχανισμούς προώθησης IP σε routers. [6]

6.4 Μέθοδοι Ανίχνευσης Εξόρυξης Δεδομένων και Μηχανικής Μάθησης

6.4.1 NetShield

Το NetShield είναι ένα σύστημα που προστατεύει από επιθέσεις τους client hosts, τους network routers και τους network servers. Οι επιτιθέμενοι μπορεί να είναι zombies και χειριστές των επιθέσεων DDoS flood attacks. Προστατεύει οποιοδήποτε δημόσιο δίκτυο που βασίζεται σε IP στο Διαδίκτυο και χρησιμοποιεί την πρόληψη και τον περιορισμό των τιμών, ώστε να μην υπάρχουν αδυναμίες στο σύστημα και συγκεκριμένα στα μηχανήματα προορισμού (target machines). Για την προστασία των πόρων του δικτύου χρησιμοποιεί δυναμικές πολιτικές ασφάλειας ενάντια σε επιθέσεις DDoS flood attacks. [6]

6.4.2 DDoS Container

Το DDoS Container είναι ένα ολοκληρωμένο πλαίσιο για την ανίχνευση επιθέσεων DDoS. Χρησιμοποιεί μια μέθοδο ανίχνευσης βάσει δικτύου για την άμυνα σύνθετων και απλών τύπων επιθέσεων DDoS και λειτουργεί παράλληλα για τον έλεγχο της τρέχουσας κυκλοφορίας σε πραγματικό χρόνο. Καλύπτει τον έλεγχο (stateful inspection on traffic flow streams) και συσχετίζει δράσεις μεταξύ διαφορετικών περιόδων σύνδεσης, με συνεχή παρακολούθηση τόσο των επιθέσεων DDoS, όσο και των νόμιμων εφαρμογών. Τερματίζει τη διαδικασία όταν εντοπίζει μια επίθεση DDoS.[6]

6.4.3 Προληπτική μέθοδος ανίχνευσης

Η προληπτική μέθοδος ανίχνευσης για επιθέσεις DDoS χρησιμοποιεί μια αρχιτεκτονική που περιλαμβάνει μια επιλογή handlers και agents που επικοινωνούν, συμβιβάζονται και επιτίθενται. Πραγματοποιεί ανάλυση συστάδων. Για την έκδοση των αποτελεσμάτων χρησιμοποιήται το σύνολο δεδομένων DARPA dataset. Σε κάθε φάση του σεναρίου επίθεσης διαχωρίζει και μπορεί να εντοπίσει τους δημιουργούς (originators) μιας επίθεσης DDoS, καθώς και την ίδια την επίθεση.[6]

6.4.4 Αυτοματοποιημένο σύστημα ανίχνευσης DDoS μεγάλης κλίμακας

Το LADS - Large-scale Automated DDoS detection System, είναι ένα αυτοματοποιημένο σύστημα ανίχνευσης DDoS μεγάλης κλίμακας, το οποίο κάνει αποτελεσματική χρήση των δεδομένων, που είναι άμεσα διαθέσιμα σε έναν ISP. Αυτό που κάνει αυτό το σύστημα είναι να επιθεωρεί το χώρο σχεδίασης και να ανιχνεύει επιθέσεις εντός δικτύου. Προτείνει μια προσέγγιση triggered, multi- stage που αντιμετωπίζει τόσο την επεκτασιμότητα όσο και την ακρίβεια της επίθεσης. [6]

6.4.5 Ανάλυση άρθρωσης

Ο Rahmani σχεδίασε μια κοινή εντροπία ανάλυση κοινής εντροπίας, για ανίχνευση επίθεσης DDoS χρησιμοποιώντας πολλαπλές διανομές κίνησης (multiple traffic distributions). Οι χρονικές σειρές των IP - flow numbers και των συνολικών μεγεθών κυκλοφορίας(aggregate traffic sizes) εξαρτώνται στατιστικά. Η εμφάνιση μιας επίθεσης επηρεάζει την εξάρτηση (dependence) και προκαλεί μια διακοπή στις χρονοσειρές για τις entropy values [6]

6.4.6 Ανίχνευση επίθεσης DDoS χαμηλού ποσοστού

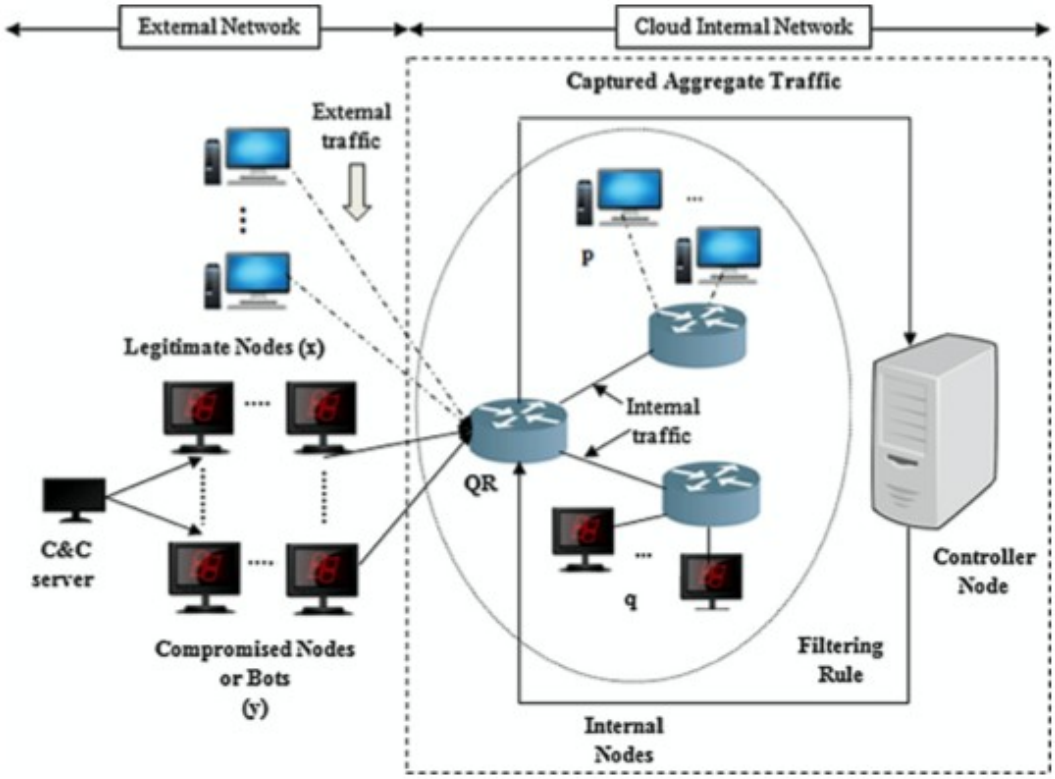
Η ανίχνευση Low-rate DDoS είναι δύσκολο να μπορέσει να ξεχωρίσει την κανονική κίνηση απο μια επίθεση. Υπάρχουν δύο μετρήσεις για πληροφορίες (information metrics) : (i) γενικευμένη μέτρηση εντροπίας (entropy metric) και (ii) μέτρηση απόστασης πληροφοριών, για τον εντοπισμό επιθέσεων low - KK DDoS attacks. Η επίθεση μπορεί να εντοπιστεί με βάση την απόσταση μεταξύ νόμιμης και επιθετικής κίνησης. Η generalized entropy metric είναι πιο ακριβής από την traditional Shannon metric. [6]

6.4.7 FireCol

Το FireCol είναι μια μέθοδος ανίχνευσης που χρησιμοποιεί τις πληροφορίες σαν θεωρία. Εφαρμόζεται σε επίπεδο παροχέα υπηρεσιών Διαδικτύου (ISP-Internet service provider), ως μέρος του συστήματος πρόληψης εισβολής (IPS-intrusion prevention system). Τα IPS δημιουργούν εικονικούς δακτυλίους προστασίας γύρω από τους κεντρικούς υπολογιστές, για να υπερασπιστούν και να συνεργαστούν ανταλλάσσοντας συγκεκριμένες πληροφορίες κίνησης.[6]

6.4.8 Αλγόριθμος συμπλέγματος K-Means

Το μοντέλο ανίχνευσης K-Means clustering algorithm μπορεί να χρησιμοποιηθεί, όταν δημιουργούμε τις αρχικές τιμές για την κυκλοφορία δικτύου και των τιμών κίνησης που έχουν καταγραφεί. Όταν η τρέχουσα κίνηση δικτύου υπερβαίνει την οριακή τιμή, ελέγχεται η κατάσταση του πρωτοκόλλου πακέτου δικτύου για την αναγνώριση μη φυσιολογικών πακέτων (abnormal packets). Αν δεν υπάρχουν abnormal packets, δημιουργείται ένα νέο μοντέλο threshold value model με βάση τη τρέχουσα κατάσταση του δικτύου χρησιμοποιώντας τη μονάδα k-means module.[6]



Εικόνα 6.1: Ανίχνευση επίθεσης DDoS [20]

6.5 Υπάρχουσες Ανιχνεύσεις για DDos Επιθέσεις σε IoT

Η δικτύωση που καθορίζεται από λογισμικό (SDN) και το Internet of Things (IoT) είναι οι τάσεις της εξέλιξης του δικτύου. Το SDN επικεντρώνεται κυρίως στον έλεγχο και τη διαχείριση των δικτύων ανώτερου επιπέδου, ενώ το IoT στοχεύει να ενώσει συσκευές για να επιτρέψει την κοινή χρήση και την παρακολούθηση συμπεριφορών σε πραγματικό χρόνο μέσω της σύνδεσης δικτύου. Το IoT μας επιτρέπει να συλλέγουμε τη κατάσταση των συσκευών και των δικτύων και να τα ελέγχουμε από απόσταση. Από την άλλη πλευρά, ο αναπτυσσόμενος αριθμός συσκευών προκαλεί στο επίπεδο πρόσβασης θέματα ασφαλείας για επιθέσεις δικτύου, όπως είναι η Κατανεμημένη Άρνηση Υπηρεσίας (DDoS).[41]

Υπάρχει ανάγκη βελτίωσης της ασφάλειας στο δίκτυο IoT που βασίζεται σε SDN για τη μείωση των επιθέσεων στις συσκευές IoT. Το SDN χωρίζει ένα δίκτυο σε τρία επίπεδα: επίπεδο εφαρμογής, επίπεδο ελέγχου και επίπεδο δεδομένων. Οι διακόπτες SDN στο επίπεδο δεδομένων δεν έχουν την ικανότητα σκέψης και διαχειρίζονται από έναν κεντρικό ελεγκτή στο επίπεδο ελέγχου. Το πλεονέκτημα είναι ότι υπάρχει ευκολία διαχείρισης. Παρολαυτά, ο ελεγκτής μπορεί εύκολα να αποτύχει και να σημειωθεί βλάβη. Ο τεράστιος αριθμός συσκευών IoT, που είναι συνδεδεμένες στο ίδιο δίκτυο αυξάνει τις επιθέσεις, το οποίο δημιουργεί προβλήματα ασφαλείας στα δίκτυα IoT. Αυτά τα ζητήματα ασφαλείας, περιλαμβάνουν: κακόβουλες επιθέσεις κώδικα, αδυναμία λήψης ενημερώσεων κώδικα ασφαλείας, hacking, έξυπνοι μετρητές, υποκλοπές – eavesdropping, επιθέσεις sniffing και επιθέσεις Distributed Denial of Service (DDoS).[41]

Οι επιθέσεις DDoS στοχεύουν στην κατανάλωση πόρων συστήματος, έως ότου ο στόχος δεν είναι διαθέσιμος, να προσφέρει τις υπηρεσίες του. Οι επιθέσεις DDoS θα μπορούσαν να χωριστούν σε τρεις κατηγορίες: α)επίθεση στο επίπεδο εφαρμογής, β) επίθεση στο πρωτόκολλο και γ)ογκομετρική επίθεση. Τα δίκτυα IoT που βασίζονται σε SDN, επιτρέπουν δυναμικό έλεγχο πρόσβασης σε οικιακά δίκτυα, καθώς και υποστήριξη ταυτότητας και εξουσιοδότησης. Ωστόσο, οι πολλοί και διαφορετικοί τύποι συσκευών και ο τεράστιος αριθμός τους στο IoT, καθιστούν το IoT ιδανικό στόχο για τους επιτιθέμενους DDoS. [41]

Πίνακας 3. Υφιστάμενες λύσεις για την ανίχνευση και την υπεράσπιση Δικτύου SDN έναντι επιθέσεων Distributed Denial of Service (DDoS). [41]

Algorithm	Simulation	Real Implementation	Detection or Defence	Control or Data Plane	Advantages	Disadvantages
Dao et al. [12]	✓	✗	Both	Both	Feasible and accurate in the small network.	Resource consumption is high when confronting mature attacks.
Mousavi et al. [13]	✓	✗	Detection	Both	Low resource consumption and short detection time.	Hard to define the threshold of detection for different applications.
Dong et al. [14]	✗	✗	Detection	Control Plane	Prompt and accurate, improvement in false positive and false negative issues.	No simulation or implementation related to SDN.
Yan et al. [15]	✓	✗	Both	Data Plane	Low false positive.	High latency, especially for the users sharing the same port with the attacker.
Dharma et al. [16]	✗	✗	Both	Control Plane	Further inspection to decrease false positive.	Produce delay to legitimate users.
Shoeb et al. [17]	✗	✗	Both	Both	Able to protect the flow table on the switch.	Hard to define key parameters, such as peak time.

Xiao et al. [18]	✓	✗	Detection	Data Plane	High detection rate and low false positive.	Hard to define key parameters, such as abnormal link utilisation. Limited to link flooding attacks.
Kokila et al. [19], Phan et al. [20]	✓	✗	Detection	Control Plane	High accuracy and low false positive.	Performance is based on the training dataset.
Lim et al. [21]	✓	✗	Both	Data Plane	Capable of localising attackers and transformable countermeasures.	Hard to define the metric and threshold.
Chin et al. [22]	✓	✗	Detection	Data Plane	Effective and scalable.	Require extra device and interface.
Macedo et al. [23]	✓	✗	Both	Control Plane	Associate multiple controllers instead of extra devices to mitigate DDoS attacks.	High-frequency attack may result in continual leader controller election.
Hameed et al. [24]	✓	✗	Both	Data Plane	Allows inter-domain defence of DDoS attacks.	Attack with spoofed IP address will make controllers block normal users.
Sahay et al. [25]	✓	✓	Defence	Data Plane	The collaboration between the controller on the customer side and ISP side enables quick response to DDoS attacks.	The link between ISP controller and customer controller becomes a new threat in this model.

Στους Πίνακες 3 και 4, γίνεται συστηματική ανάλυση κάθε αλγόριθμου. Πιο συγκεκριμένα, παρέχετε η συγκριτική ανάλυση προσομοίωσης ή πραγματικής εφαρμογής. Προτείνει έναν αμυντικό μηχανισμό είτε όχι, την εστίαση του αλγορίθμου όσον αφορά τα δεδομένα και το επίπεδο ελέγχου και μια περίληψη των πλεονεκτημάτων και μειονεκτημάτων των υπαρχόντων αλγορίθμων . [41]

Πίνακας 4. Αντίμετρα σε δίκτυα IoT που βασίζονται σε SDN. [41]

Algorithm	Simulation	Real Implementation	Detection or Defence	Control or Data Plane	Advantages	Disadvantages
Tortonesi et al. [26]	✓	✗	Defence	Data Plane	Capable of edge defence due to the programmable controller in the data plane, the work load on the control plane is shared by the data plane.	The interface between SPF controller and programmable controller needs to be defined. The gateway devices shall support both SDN and programmable controller.
Özçelik et al. [27]	✓	✗	Both	Data Plane	Fog computing enables the mitigation of DDoS attacks at the ingress of the network.	Defence mainly focuses on Mirai botnet and TCP protocol, other attack types might need validation.
Sarwar et al. [28]	✓	✗	Both	Control Plane	Existing trustful users can still interact with the controller during DDoS attacks.	The controller rejects all the new flows under DDoS attacks. A legitimate user without a high trust value will encounter more delays when the network is busy.
Ravi et al. [29]	✓	✓	Both	Both	The real-time training keeps the flow rules that are generated by machine learning up-to-date.	The performance of LEDEM relies on the training dataset. The link between local and universal controllers needs to be defined.
Sharma et al. [30]	✓	✗	Detection	Both	The proposed mechanism is able to detect not only DDoS attacks but also other types of attacks.	New-flow attacks against one network slice might saturate system resources, as it triggers a new flow record and the update in the detection pattern.
Nobakht et al. [31]	✗	✓	Both	Data Plane	Detection is based on the IoT application, which means the behaviour in the network is predictable for a specific application.	The performance of detection might highly rely on the habit of using the application. For a flexible application, it could result to a low accuracy in the detection.

Οι επιθέσεις DDoS έχουν διαφορετικές συμπεριφορές,

για αυτό το λόγο χρησιμοποιούνται διάφορες τεχνικές

για τον εντοπισμό και τον αποκλεισμό αυτών των επιθέσεων.

Κεφάλαιο 7

Στο κεφάλαιο 7 δίνονται κάποιες πρακτικές λύσεις που μπορούν να προσφέρουν μεγαλύτερη ασφάλεια στους χρήστες των συσκευών IoT και πως μπορούν οι χρήστες να έχουν περισσότερο τον ελέγχο των συσκευών τους. Τέτοιες λύσεις μπορεί να είναι: το κλείδωμα του λογαριασμού, η επαλήθευση του χρήστη με δύο τρόπους, οι ενημερώσεις, η κρυπτογράφηση των δεδομένων και η φυσική ασφάλεια των συσκευών. Στο τέλος γίνεται αναφορά στους λόγους που παρά την ανάπτυξη των IoT, οι επιθέσεις DDos συνεχίζουν να αυξάνονται και να επιτυγχάνουν το σκοπό τους τις περισσότερες φορες.

7.1 Έλεγχοι και λύσεις για την ασφάλεια των IoT συσκευών

7.1.1 Λήξη χρόνου λογαριασμού

Με αυτό το τρόπο ένας λογαριασμός κάνει Timeout και μπορεί να αποσυνδέσει τον χρήστη από τον λογαριασμό ή το λογισμικό του, μετά από ένα καθορισμένο χρονικό διάστημα. Αυτό εμποδίζει έναν εισβολέα να αποκτήσει πρόσβαση σε ιδιωτικές πληροφορίες. Το πιο βασικό είναι το κλείδωμα του υπολογιστή αφού περάσει ο καθορισμένος χρόνος. Μια άλλη τεχνική είναι να υπάρχει ένα token που χρησιμοποιεί Bluetooth ή NFC, έτσι ώστε η συσκευή να αναγνωρίζει πότε υπάρχει ο εξουσιοδοτημένος χρήστης, εμποδίζοντας το να κλειδώσει τη συσκευή. Ωστόσο, κάθε φορά που διακόπτεται η σύνδεση, ο υπολογιστής κλειδώνει για να αποτρέψει τη μη εξουσιοδοτημένη χρήση. Παραδείγματα συσκευών είναι το κινητό τηλέφωνο, τα keychains και τα bracelets.[7]

7.1.2 Κλείδωμα λογαριασμού

Το κλείδωμα λογαριασμού λειτουργεί είτε αποτρέποντας εντελώς τις επαναλαμβανόμενες συνδέσεις, είτε απαιτώντας **CAPTCHA*** για να τη προσπάθεια σύνδεσης στο λογαριασμό μετά από έναν καθορισμένο αριθμό αποτυχιών. Εάν ο ιστότοπος απαιτεί CAPTCHA, ο χρήστης θα πρέπει είτε να πληκτρολογήσει μια φράση από μια εικόνα είτε να κάνει κλικ σε εικόνες που ταιριάζουν, με μια κατηγορία για να αποδείξει ότι δεν είναι bot ή σενάριο που προσπαθεί να το υπογράψει. Αν ο ιστότοπος απλώς τους κλειδώσει, θα πρέπει είτε να καλέσουν τη γραμμή βοήθειας είτε να ζητήσουν την επαναφορά του κωδικού πρόσβασης και την αποστολή τους στο email τους. Αυτή η μέθοδος μπορεί να αποτρέψει τους μεμονωμένους εισβολείς, που προσπαθούν είτε να μπούνε σε έναν λογαριασμό, είτε να κάνουν μια επίθεση DoS κατακλύζοντας το σύστημα με πολλά requests.[7]

Ενα **CAPTCHA (**C**ompletely **A**utomated **P**ublic Turing test to tell **C**omputers and **H**umans **A**part) είναι ένας τύπος πρόκλησης – απόκρισης ελέγχου που χρησιμοποιήθηκε για τον υπολογισμό ώστε να εντοπίσει αν ο χρήστης είναι άνθρωπος ή όχι. Αυτή η μορφή CAPTCHA απαιτεί από κάποιον να αξιολογήσει σωστά και να εισάγει μια σειρά από γράμματα ή αριθμούς που είναι αντιληπτά σε μια παραμορφωμένη εικόνα που εμφανίζεται στην οθόνη τους. Επειδή η δοκιμή χορηγείται από έναν υπολογιστή, σε αντίθεση με την τυπική δοκιμασία Turing που χορηγείται από έναν άνθρωπο, ένα CAPTCHA μερικές φορές περιγράφεται ως αντίστροφη δοκιμή Turing. [29]*

7.1.3 Two-Factor authentication

Ο έλεγχος ταυτότητας δύο παραγόντων είναι μια δεύτερη μορφή επαλήθευσης που επιτρέπει σε έναν χρήστη να συνδεθεί σε έναν λογαριασμό χρησιμοποιώντας, εκτός από το όνομα χρήστη και τον κωδικό πρόσβασής του, έναν τυχαία δημιουργημένο κωδικό που αποστέλλεται σε ένα τηλέφωνο ή μια εφαρμογή που επιτρέπει στο χρήστη να αναγνωρίσει ότι είναι αυτός που συνδέεται στον λογαριασμό τους. Όλο και περισσότεροι ιστότοποι χρησιμοποιούν στο σύστημά τους αυτή τη μέθοδο, όπως οι ιστότοποι κοινωνικών δικτύων και στις τραπεζικές συναλλαγές. Με αυτήν τη μέθοδο, ακόμη και αν υπάρχει διαρροή και ένας εισβολέας αποκτήσει πρόσβαση στον κωδικό πρόσβασης ενός χρήστη, θα εξακολουθεί να μην μπορεί να αποκτήσει πρόσβαση στον λογαριασμό του, εκτός αν έχει πρόσβαση και στο τηλέφωνο του χρήστη.[7]

7.1.4 Οδηγίες πολυπλοκότητας κωδικού πρόσβασης

Ένας πολύπλοκος κωδικός πρόσβασης είναι μια πρακτική που καθορίζει κανόνες σχετικά με το τι είναι και τι δεν επιτρέπεται να είναι, σε μια λέξη-κλειδί. Κάποια σημαντικά στοιχεία που πρέπει να προσέχουμε όταν δημιουργούμε ένα κωδικό είναι πόσους χαρακτήρες θα χρησιμοποιήσουμε, το μέγεθος που πρέπει να έχει, αν είναι παρόμοιο με προηγούμενους κωδικούς πρόσβασης και πόσο συχνά πρέπει να τον αλλάζουμε. Όσο πιο δύσκολοι κωδικοί δημιουργηθούν τόσο πιο ασφαλείς θα είναι οι κωδικοί πρόσβασης, ωστόσο οι χρήστες όταν φτιάξουν έναν δυνατό κωδικό πρόσβασης, δύσκολα τον ανανεώνουν και τον αλλάζουν. Έτσι οι αλλαγές που κάνουν περιορίζονται σε ένα γράμμα στον κωδικό πρόσβασης ή στην προσθήκη ενός μόνο αριθμού στο τέλος του. Ένα άλλο πρόβλημα είναι ότι οι χρήστες έχουν σε κοινή θέα και κοντά τους όλους τους κωδικούς πρόσβασης, επειδή δυσκολεύονται να τους θυμηθούν, με αποτέλεσμα στην ουσία να μην έχουν ασφάλεια.[7]

7.1.5 Διαμόρφωση των Θυρών

Όταν οι εισβολείς θέλουν να παραβιάσουν ένα δίκτυο, σαρώνουν το σύστημα για ευπάθειες και αδύναμα σημεία. Αυτό περιλαμβάνει τυχόν θύρες που είναι ανοιχτές και ενδέχεται να τους προσφέρουν μια διαδρομή διείσδυσης στο δίκτυο. Για να διαμορφώσουμε τις θύρες της συσκευής επιλέγουμε ποιες θύρες θα ανοίξουν / κλείσουν, έτσι ώστε οι πληροφορίες που χρησιμοποιούν να μπορούν να μεταδοθούν. Παράλληλα αποτρέπουμε τη χρήση ή την πρόσβαση σε περιττές ή ακούσιες θύρες. Όταν υπάρχουν θύρες ανοιχτές σε ένα δίκτυο που δεν είναι αναγκαίο, ένα δίκτυο γίνεται πολύ πιο ανασφαλές. Ένα δίκτυο με κλειστές θύρες επιτρέπει στους χρήστες να συρρικνώσουν την επιφάνεια επίθεσης μειώνοντας έτσι την απειλή ενός εισβολέα να αποκτήσει πρόσβαση στο δίκτυο. [7]

7.1.6 Διαχείριση ενημερωμένων εκδόσεων κώδικα

Η διαχείριση ενημερωμένης έκδοσης κώδικα επιτρέπει την προώθηση ενημερώσεων σε συσκευές εντοπίζοντας αδυναμίες και αποτρέποντας περισσότερες ζημιές. Αυτό περιλαμβάνει ενημερώσεις που προωθούνται από το λειτουργικό σύστημα και το λογισμικό που χρησιμοποιείται ή τυχόν ευπάθειες. Ένα πολύ σημαντικό κομμάτι της διαχείρισης ενημερώσεων του κώδικα είναι να το δοκιμάσουμε σε μερικές συσκευές πριν το στείλουμε σε ολόκληρο το δίκτυο συσκευών. Με αυτό το τρόπο αποτρέπεται η διακοπή λειτουργίας όλων των συσκευών. Επίσης η προώθηση των ενημερώσεων πρέπει να γίνει με τέτοιο τρόπο ώστε να μην επηρεάζει τη ροή εργασίας των εργαζομένων. Αυτό μπορεί να επιτευχθεί ενημερώνοντας τις συσκευές τη νύχτα ή όποτε εργάζονται όσο το δυνατόν λιγότεροι υπάλληλοι. Ένα μεγάλο ποσοστό παραβιάσεων θα μπορούσαν να είχαν αποφευχθεί αν ο κάθε οργανισμός ασκούσε σωστή διαχείριση των κωδικών. [7]

7.1.7 Ανίχνευση / πρόληψη εισβολής

Εισβολή θεωρείται η απόπειρα πρόσβασης σε μη εξουσιοδοτημένα συστήματα ή πόρους. Η Ανίχνευση / Πρόληψη εισβολής εντοπίζει πότε ένας μη εξουσιοδοτημένος χρήστης έχει πρόσβαση σε διάφορα μέρη του δικτύου και τους εμποδίζει να έχουν πρόσβαση σε οτιδήποτε δεν είναι εξουσιοδοτημένο. Μπορεί επίσης να προειδοποιήσει την εταιρεία για την εισβολή. Η ανίχνευση εισβολής παρακολουθεί απλώς την κυκλοφορία ή παρατηρεί τη συμπεριφορά του συστήματος για να αναζητήσει οτιδήποτε μπορεί να είναι κακόβουλο (π.χ. policy violations και anomalies), αλλά δεν αναλαμβάνει απαραίτητα άμεση δράση για να σταματήσει τη πιθανή εισβολή. Η παρεμπόδιση εισβολής, κάνει το ίδιο πράγμα, αλλά ενεργά λαμβάνει μέτρα για να αποτρέψει και να σταματήσει τυχόν εισβολές που ανιχνεύει στον server στόχο ή σε οποιονδήποτε πολύτιμο πόρο του ιδιωτικού δικτύου δεδομένων. [7]

7.1.8 Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση δεδομένων, κρυπτογραφεί τα δεδομένα έτσι ώστε να προστατεύονται ακόμη και αν ένας μη εξουσιοδοτημένος χρήστης υποκλέψει τα κρυπτογραφημένα πακέτα δεδομένων μέσω ενός καναλιού επικοινωνίας. Αυτός είναι ένας πολύ αποτελεσματικός τρόπος, για να προστατεύσετε τα δεδομένα και να διασφαλίσετε ότι είναι πιο ασφαλή σε περίπτωση επίθεσης. Τα τρέχοντα πρότυπα κρυπτογράφησης (enterprise-grade encryption standards), χρειάζονται χρόνια υπολογιστικής ισχύος για να σπάσουν. Οι κατασκευαστές IoT πρέπει να επικεντρώνονται στον έλεγχο ταυτότητας κατά την παραγωγή συσκευών και την αποστολή τους στην αγορά. Το VPN είναι μια σήραγγα επικοινωνίας μεταξύ δύο ή περισσότερων συσκευών. Για να έχετε ένα ασφαλές κανάλι, μπορείτε να κρυπτογραφήσετε οτιδήποτε μέσα και έξω από τη σήραγγα. Όταν κρυπτογραφείται, ο εισβολέας δεν θα μπορεί να διαβάσει τα δεδομένα όταν παρακολουθεί τις επικοινωνίες.[7]

7.1.9 Προστασία DoS

Η προστασία μπορεί να έχει τη μορφή φυσικής συσκευής ή διαμορφωμένου λογισμικού όπως είναι το firewall. Η προστασία DoS προσφέρεται επίσης ως υπηρεσία, με τους παρόχους υπηρεσιών να φιλτράρουν αυτόματα την κίνηση που ακολουθεί, συγκεκριμένα μοτίβα patterns. Οι εταιρείες πρέπει να γνωρίζουν το συνηθισμένο όγκο επισκεψιμότητας που λαμβάνουν οι ιστότοποί τους σε διάφορες χρονικές στιγμές. Αυτό είναι σημαντικό, ώστε όποτε υπάρχει τεράστια αύξηση της κυκλοφορίας, να είναι σε θέση να το εντοπίσουν νωρίς και να μετριάσουν τις ζημιές. Υπάρχουν πολλές διαφορετικές μέθοδοι για την αποτροπή επιθέσεων DoS που λειτουργούν παρακολουθώντας την εισερχόμενη κίνηση. Αυτές μπορεί να περιλαμβάνουν το φιλτράρισμα της κίνησης από μια συγκεκριμένη διεύθυνση IP, τον περιορισμό του αριθμού των πακέτων που μπορούν να σταλούν από μια μεμονωμένη διεύθυνση IP, καθώς και την προώθηση τυχόν πακέτων από συγκεκριμένες διευθύνσεις IP και την απόρριψή τους χωρίς να τους επιτρέπεται να φτάσουν ποτέ στον επιδιωκόμενο στόχο τους. [7]

Η κορυφαία απειλή για την ασφάλεια στο IoT είναι η επίθεση DDOS με τη συντριπτική πλειοψηφία 51,7% των ερωτηθέντων να το υποστηρίζει. [36]

[4]Ο εισβολέας DDoS έχει εξελιχθεί με όπλα σε συσκευές IoT. Ωστόσο, αυτοί που προσπαθούν να αμυνθούν, εξακολουθούν να εξαρτώνται από τεχνολογίες που αναπτύχθηκαν τη δεκαετία του 2000 και δεν διαθέτουν την ακρίβεια, την επεκτασιμότητα ή τον αυτοματισμό που χρειάζονται για να τον πολεμήσουν στη παρούσα κατάσταση που επικρατεί στον κυβερνοχώρο.

4 Don Shin, John Pescatore, Webcast : “Techniques to Modernize Your DDoS Defenses”,Tuesday, July24, 2018 at 3:30 PM EDT [URL]

8. Συμπεράσματα

Το IoT κάνει τη ζωή μας πιο εύκολη, όμως πολλοί είναι εκείνοι που εκφράζουν την ανησυχία τους, για την ασφάλειά τους. Τα τελευταία χρόνια οι επιθέσεις ασφάλειας στον κυβερνοχώρο και πιο συγκεκριμένα στις συσκευές IoT αυξάνονται. Η ολοένα και αυξανόμενη δημιουργία συσκευών που είναι μέρος ενός IoT, δημιουργεί περισσότερους στόχους και τρωτά σημεία στο Διαδίκτυο των Πραγμάτων. Η ασφάλεια στον κυβερνοχώρο είναι ένα σημαντικό εμπόδιο για το IoT. Οι επιθέσεις DDoS χρησιμοποιούν τους περιορισμένους πόρους σε συσκευές IoT, όπως περιορισμό στο χώρο αποθήκευσης και στη χωρητικότητα δικτύου και μπορούν να προκαλέσουν προβλήματα ασφάλειας, τόσο οικονομικά όσο και ηθικά.

Οι οργανισμοί γνωρίζουν τον αντίκτυπο της ασφάλειας στον κυβερνοχώρο και στις επιχειρήσεις τους. Η ασφάλεια στο IoT είναι πιο σημαντική από άλλα ζητήματα, όπως το κόστος, η ανάλυση δεδομένων και η απόδοση. Οι επιθέσεις DDoS στα Ευφυή Συστήματα Μεταφορών (ITS - Intelligent Transportation Systems) θα μπορούσαν να κατακλύσουν τις επικοινωνίες των συνδεδεμένων αυτοκινήτων και να αποτελέσουν ένα μεγάλο πρόβλημα για τις αυτοκινητοβιομηχανίες. Τα εκτεθειμένα και ευάλωτα συνδεδεμένα συστήματα αυτοκινήτων ανακαλύπτονται εύκολα, κάτι που αυξάνει τους κινδύνους και τις επιθέσεις. Για την επιτυχημένη επίθεση στο τομέα των μεταφορών και συγκεκριμένα των συνδεδεμένων αυτοκινήτων χρειάζεται περιορισμένη κατανόηση της τεχνολογίας και μπορεί να επιτευχθεί από έναν low-skilled επιτιθέμενο. Αντιλαμβανόμαστε τη σπουδαιότητα του ζητήματος, γιατί σε περίπτωση παρεμβολής στο δίκτυο IoT την ώρα που κινείται το όχημα, μπορεί να προκληθεί από ατύχημα ως και θάνατος των επιβαίνοντων καθώς και άλλων εμπλεκόμενων οχημάτων και ατόμων.

Η σημασία της ασφάλειας των δεδομένων και των συνδεδεμένων πραγμάτων, έχει να κάνει με τα δεδομένα που θα δημιουργηθούν από αυτές τις συνδεδεμένες συσκευές. Αυτές οι συσκευές όχι μόνο θα παράγουν δεδομένα, αλλά θα συμπεριφέρονται επίσης, βάσει των συλλεγόμενων πληροφοριών. Εάν υπάρχουν κενά στην ασφάλεια, τότε κακόβουλα άτομα στην κοινωνία μπορούν να δουν, να αποκτήσουν πρόσβαση και να κάνουν κατάχρηση των ίδιων πληροφοριών. Υπάρχουν ευαίσθητες πληροφορίες (π.χ. τομέας υγείας), που θα πρέπει να προστατεύονται πολύ καλά, ώστε να μην πέσουν στα χέρια ανθρώπων που θα ήθελαν να εκμεταλλευτούν αυτό το κενό ασφαλείας και να χρησιμοποιήσουν αυτά τα δεδομένα παραβιάζοντας όχι μόνο το σύστημα ασφαλείας, αλλά παραβιάζοντας και τις ηθικές παραμέτρους. Συνειδητοποιώντας τη σημασία του IoT, οι επενδυτές κάνουν τεράστια επένδυση σε αυτό, παραλείποντας όμως να επενδύσουν και στην ασφάλεια του IoT.

Η ανίχνευση της επίθεσης DDoS μπορεί να αντιμετωπιστεί αποτελεσματικά, με την ταξινόμηση βάσει ροής πακέτων και αλγορίθμων μηχανικής μάθησης. Η εφαρμογή αυτών των αλγορίθμων παρέχει μεγαλύτερη ακρίβεια σε χρόνο και χώρο μνήμης. Σε πρακτικό επίπεδο ασχολήθηκα με έναν μηχανισμό Ανίχνευσης DDos επιθέσεων σε IoT συσκευές και συγκεκριμένα με κάμερες ασφάλειας. Αυτό που διεπίστωσα στη πράξη είναι ότι οι IoT συσκευές έχουν περιοσμένες δυνατότητες ασφάλειας και αναγκάζουν τους χρήστες να ρίξουν τα επίπεδα ασφαλείας ώστε να λειτουργήσουν.

Παράδειγμα, σε ασύρματη ip κάμερα escam εσωτερικού χώρου, απαιτούνταν κάποια requirements, για να μπορέσει η εφαρμογή να δει τη κάμερα και να συνδεθεί μαζί της . Ενδεικτικά, ήθελε να απενεργοποιηθούν: α) το AP Isollation που ενισχύει την ασφάλεια του δικτύου καθώς απομονώνει όλους τους clients στο ίδιο ασύρματο δίκτυο, β) το 5G wifi που σχετίζεται με το εύρος ζώνης γ) τα πρωτόκολλα WPA/WPA2 και οποιεσδήποτε άλλες ρυθμίσεις περιορίζουν το Wi – Fi Access.

Για την ασφάλεια όλων των συσκευών και με βάση τις προυποθέσεις λειτουργίας τους, υπάρχουν δύο προτάσεις που μπορούν να υλοποιηθούν συνδυαστικά,ώστε να πετύχουμε τη μέγιστη ασφάλεια και λειτουργία:

Α’ Πρόταση

Η πρώτη πρόταση είναι να στηθεί ένας IoT Gateway όπου θα συνδέονται όλες οι IoT συσκευές ασύρματα και θα τις διαχειρίζεται.

Υλοποιήθηκε με ένα Rasbery Pi (rasp OS Linux), το οποίο έχει ασύρματη κάρτα δικτύου (είτε ενσωματωμένη είτε USB). Με τις κατάλληλες οδηγίες, μπορούμε να το κάνουμε Access Point, το οποίο δε βγαίνει απευθείας στο Διαδίκτυο.

Χρησιμοποιώντας το iptables, ανακατευθύνουμε όλα τα πακέτα απο την ασύρματη κάρτα δικτύου(wireless), στην ενσύρματη κάρτα δικτύου(wired).

Η κάθε IoT συσκευή θα έχει τη δικιά της IP και περιορισμό στον αριθμό των IP διευθύνσεων, ώστε να καλύπτει τις υπόλοιπες συσκευές. Το δίκτυο αυτό δεν είναι ορατό απο το υπόλοιπο δίκτυο παρά μόνο απο το Rasbery Pi.

Παράδειγμα αν έχουμε 5 συσκευές θα πρέπει να το ρυθμίσουμε να δίνει 6 IP διευθύνσεις . Οι 5 θα πάνε στις συσκευές και η 6 θα χρησιμοποιηθεί από την android συσκευή, για ρυθμίσεις των IoT συσκευών.

Ο μόνος τρόπος για να κάνει επίθεση κάποιος είναι να συνδεθεί στο wireless του Pi ή να μπορέσει να συνδεθεί στο ίδιο το Pi. Αν καταφέρει να πάρει πρόσβαση σε οποιαδήποτε άλλη συσκευή εκτός του Pi, δεν θα μπορέσει να ανιχνεύσει το IoT δίκτυο.

Β' Πρόταση

Σε δεύτερο επίπεδο μπορούμε να φτιάξουμε δύο προγράμματα :

1. ΄Ενα πρόγραμμα που να μπορεί να ελέγχει για DDoS επιθέσεις στο Wireless, δηλαδή να ελέγχει πόσοι προσπαθούν να συνδεθούν .

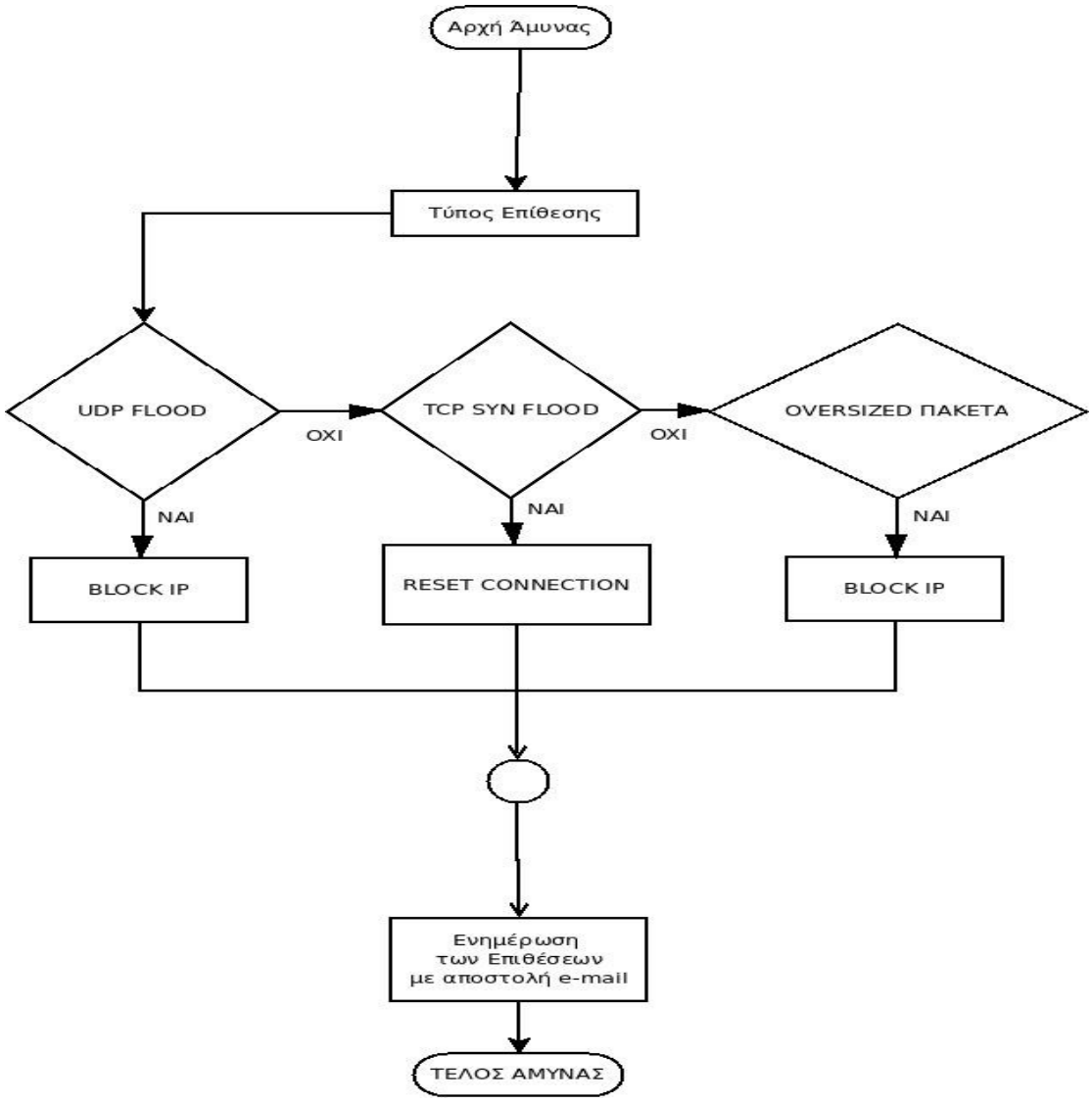
2.`Ενα πρόγραμμα για συγκεκριμένες επιθέσεις όπως είναι:

UDP Flood, TCP SYN και Oversized Πακέτα

Τα δύο προγράμματα μπορούν να χρησιμοποιηθούν συνδυαστικά με τη πρώτη πρόταση που υλοποιήσαμε παραπανω.

Στο παρακάτω διάγραμμα ροής δίνεται παράδειγμα ανίχνευσης για τους 3 τύπους επίθεσης: UDP Flood, TCP SYN και Oversized Πακέτα και με τι τρόπο θα μπορούσαμε να τους αντιμετωπίσουμε και υλοποιείται σε όποια γλώσσα προγραμματισμού θέλουμε

Διάγραμμα ροής 1 : Ανίχνευση DDoS Επιθέσεων και Αντιμετώπιση



Όταν η επίθεση είναι UDP Flood τότε αυτό που πρέπει να γίνει είναι να μπλοκάρουμε την IP, ώστε να σταματήσει. Στην περίπτωση της TCP SYN Flood επίθεσης, πρέπει να γίνει επαναφορά της σύνδεσης ώστε να αντιμετωπιστεί. ΄Οταν ανιχνευθεί η τελευταία επίθεση, στην οποία κάποιος στέλνει υπερμεγέθη πακέτα αυτό που πρέπει να γίνει είναι να κάνουμε block την IP. Αυτο που προτείνεται σε όλες τις περιπτώσεις είναι η ενημέρωση μέσω email για τις ανιχνεύσεις επιθέσεων.

Οι επιθέσεις DDoS συνεχίζουν να πραγματοποιούνται με αμείωτο ρυθμό σημειώνοντας επιτυχίες στο IoT, κάτι που οφείλεται σε διάφορους παράγοντες:

α) Τα λειτουργικά συστήματα των IoT όπως το Coniki και το TinyOS, είναι από τα πιο δημοφιλή λειτουργικά συστήματα ανοιχτού κώδικα, ενώ το FreeRTOS και το RIOT έχουν πολλές δυνατοτήτες σε πραγματικό χρόνο. Παρόλαυτα τα λειτουργικά συστήματα δεν έχουν τις απαιτούμενες ρυθμίσεις και δυνατότητες που απαιτούνται στο τομέα της ασφάλειας.

β) Οι περισσότερες συσκευές IoT δεν διαθέτουν Firewall, κάνοντας έτσι εύκολη τη δουλειά των επιτιθέμενων και αφήνοντας το δίκτυο μας εκτεθιμένο σε πολλούς κινδύνους. Έτσι η επίθεση γίνεται εύκολη υπόθεση αφού δεν υπάρχουν εμπόδια αρκετά ικανά να τους σταματήσουν και να τους εμποδίσουν, ώστε να επιτύχουν το στόχο τους.

γ) Βασικοί κανόνων ασφάλειας που οι περισσότεροι χρήστες δεν γνωρίζουν και δεν ακολουθούν, βάζοντας το IoT σε κίνδυνο και διευκολύνοντας τους DDoS επιτιθέμενους. Η επίγνωση από τους απλούς χρήστες, κανόνων που αφορούν συσκευές όπως smartphones, smart tv, κάμερες ασφαλείας και άλλες έξυπνες συσκευές μπορούν να δημιουργήσουν ένα περιβάλλον μεγαλύτερης ασφάλειας.

δ) Η χρήση παλιότερων τρόπων ανίχνευσης και αντιμετώπισης των επιθέσεων. Οι κατασκευαστές δίνουν μεγάλη βαρύτητα στις υπηρεσίες που προσφέρουν οι συσκευές IoT, παραλείποντας να ασχοληθούν και να μεριμνήσουν σε ότι αφορά την ασφάλεια, θέτοντας σε υψηλό κίνδυνο τους χρήστες (ακόμη και για την ίδια τους τη ζωή). Έτσι αυξάνουν το τελικό κόστος σε περίπτωση που μια συσκευή παραβιαστεί και δεν μπορεί να λειτουργήσει ή πάρει τον έλεγχο της συσκευής ο επιτιθέμενος. Αυτό που πρέπει να γίνει είναι η ασφάλεια να αποτελεί ένας απο τους πιο σημαντικούς στόχους στις εταιρείες και στους οργανισμούς απο την αρχή κατασκευής μιας συσκευής IoT και να αναβαθμίζεται συνεχώς, ώστε να αποφευχθεί το μεγαλύτερο μέρος επιθέσεων DDos.

ε) Οι συσκευές IoT έχουν γίνει το «νέο αγαπημένο» για τους χάκερ DDoS, επειδή ένα πολύ μεγάλο ποσοστό διαχειριστών και χρηστών συσκευών IoT το θεωρούν ως λύσεις plug-and-play και, ως εκ τούτου, δεν λαμβάνουν ούτε τα πιο βασικά μέτρα για την προστασία αυτών των συσκευών από κακόβουλη εισβολή. Αν και είναι ατομικά μικρές και περιορισμένης υπολογιστικής και δικτυακής ικανότητας, οι συσκευές IoT έχουν σημαντικό αθροιστικό δυναμικό όταν χρησιμοποιούνται σε πολύ μεγάλους αριθμούς. Οι περισσότεροι αναλυτές του DDoS συμφωνούν ότι το Mirai είναι μόνο η κορυφή του παγόβουνου και θα δούμε πολύ μεγαλύτερα και ισχυρότερα botnets και επιθέσεις IoT στο μέλλον, δεδομένου ότι ο αριθμός των συσκευών IoT θα μπορούσε να φτάσει έως και 50 δισεκατομμύρια έως το 2020. Το κύριο μέλημα για τους σχεδιαστές / χειριστές botnet είναι η αποκάλυψη των ταυτοτήτων των bots τους, καθώς αυτό θα μπορούσε ενδεχομένως να οδηγήσει στην απομόνωση και τον τερματισμό αυτών των bots, από αυτούς που προσπαθούν να αμυνθούν έναντι των DDoS επιθέσεων.

Παρόλο που η ασφάλεια στο IoT είναι μια μεγάλη πρόκληση, παράλληλα αποτελεί και μια ευκαιρία για νέους τρόπους σκέψης και δράσης.

9. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Georgios Loukas, Gulay Oke. **"Protection against Denial of Service Attacks",** Published by Oxford University Press on behalf of The British Computer Society, (2010).

[2] Ms. Sanam E anto, Ms. S Seetha, Robin K Kuriakose,"**A survey on Dos Attacks and Detection Schemes in Wireless Mesh Networks"**. Department of information Technology, Karunya University, Coimbatore TamiNadu , India . International conference on modeling optimization and computing – (ICMOC-2012) April 10&11, (2012).

[3] Priyanka Kamboj, Munesh Chandra Trivedi, Virendra Kumar Yadav, Dr. Vikash Kumar Singh, **"Detection Techniques of DDoS Attacks**", 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON) GLA University,(2017).

[4] Zubair A. Baig, Surasak Sanguanpong, Syed Naeem Firdous , Van Nhan Vo Tri Gia Nguyen, Chakchai So-In, **"Averaged dependence estimators for DoS attack detection in IoT networks"**, Future Generation Computer Systems 102, (2020) .

[5] Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo, **"IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers"**, DFRWS EU e Proceedings of the Seventh Annual DFRWS Europe, (2020).

[6] K. Munivara Prasad, A. Rama Mohan Reddy & K. Venugopal Rao, **"DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms"**, Global Journal of Computer Science and Technology: Network, Web & Security Volume 14 Issue 7 Version 1.0, (2014).

[7] Syed Rizvia, RJ Orra, Austin Coxa, Prithvee Ashokkumara, Mohammad R. Rizvib, **"Identifying the attack surface for IoT network"**, Department of Information Sciences and Technology, Pennsylvania State University, Altoona, (2020).

[8] Mohamed Litoussia, Nabil Kannoufb, Khalid El Makkaouic,a, Abdellah Ezzatia, **"IoT security: challenges and countermeasures",** November 2-5, Madeira, Portugal, (EICN 2020).

[9] Asmaa Munshi, Nouf Ayadh Alqarni, Nadia Abdullah Almalki,**"DDoS Attack on IoT Devices"**, Department of Cybersecurity College of computer science and engineering University of Jeddah, Kingdom of Saudi Arabia (2020).

[10] Karanpreet Singh, Paramvir Singh, Krishan Kumar, **"Application layer HTTP-GET flood DDoS attacks"**, Department of Computer Science and Engineering, Ambedkar National Institute of Technology, Jalandhar 144011, Punjab, India (2017).

[11] Gang Liu, Wei Quan, Nan Cheng, Hongke Zhang, Shui Yu, **"Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things",** School of Electronic and Information Engineering, Beijing Jiaotong University, China (2019).

[12] Fadaei Fouladi, Orhan Ermiş, Emin Anarim, **"A DDoS attack detection and defense scheme using time-series analysis for SDN"**, Electrical and Electronics Engineering Boğaziçi University, İstanbul, Turkey (2020).

[13] Luying Zhou, Huaqun Guo, Gelei Deng, **"A fog computing based approach to DDoS mitigation in IIoT systems"**, Institute for Infocomm Research, Singapore (2020).

[14] Mohamed Litoussia, Nabil Kannoufb, Khalid, AbdellahEzzatia, Mohamed Fartitchouc, **"IoT security: challenges and countermeasures ",** aLAVETE laboratory, FST, Hassan First University, Settat, Morocco (2020).

[15] Aakanksha Tewari, B.B. Gupta, **"Security, privacy and trust of different layers in Internet-of-Things (IoTs)"**, framework (2020) .

[16] Weizhi Meng, Wenjuan Li, Steven Tug, Jiao Tan, **"Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities"**, Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark (2020).

[17] Aanshi Bhardwaj, Veenu Mangat, Renu Vig, **"Effective mitigation against IoTs using super materials for distributed denial of service attacks in cloud computing"**,UIET, Panjab University, Chandigarh 160023, India (2020).

[18] Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit, **"A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT"**, Indian Institute of Engineering Science and Technology, Howrah, India (2020).

[19] Asmaa Munshi, Nouf Ayadh Alqarni, Nadia Abdullah Almalki, **"DDoS Attack on IoT Devices"**, Department of Cybersecurity College of computer science and engineering University of Jeddah (2020).

[20] Neha Agrawal, Shashikala Tapaswi, **"Low rate cloud DDoS attack defense method based on power spectral density analysis"**, Atal Bihari Vajpayee-Indian Institute of Information Technology and Management, India (2020).

[21] https://azure.microsoft.com/en-gb/overview/internet-of-things-iot/iot-technology-protocols/

[22] https://www.avsystem.com/blog/iot-protocols-and-standards/

[23] https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

[24] IoT Sensor Types - The Pillars of seamless "IoT" transformation. https://buff.ly/2En1L2H @RicardoSGulko

[25] https://squareup.com/us/en/hardware/reader

[26] http://computer-trickster.blogspot.com/2015/04/what-is-dos.html

[27] https://blog.resellerclub.com/a-step-by-step-guide-on-how-to-configure-firewall-in-linux/

[28] https://www.researchgate.net/figure/UDP-Flooding-attack_fig1_327036867

[29] https://el.wikipedia.org/wiki/CAPTCHA

[30] https://studycare.gr/iot-applications/

[31] Syed Rizvi, PhD, Ryan Pipetti, Nicholas McIntyre, Jonathan Todd, Iyonna Williams **"Threat model for securing internet of things (IoT) network at device-level",** Information Sciences and Technology, Penn State University, Altoona, USA (2020).

[**32]** Niewolny,D. **"How the Internet of Things Is Revolutionizing Healthcare".** Freescale. Vilamovska, A., Hattziandreu, E., Schindler, R., Oranje, C., DeVries, H., & Krapelse, J. (2009). RFID Application in Healthcare. Europe: RAND, (2013).

[33] Bosse, J. Brundu, G., Patti, E., Osello, A., Giudice, M., Rapetti, N., Krylovskiy, A., jahn, M., Verda, V., Guelpa, **"The Road to Success: The Value of IoT in Ground Transportation",** IoT Software Infrastructure for Energy Management and Simulation in Smart Cities. IEEE Transactions on Industrial Informatics, Vol. 13, No. 2, pp. 832-840, (2016).

[34] Bimal Patel, Parth Shah, **"Operating system support, protocol stack with key concerns and testbedfacilities for IoT: A case study perspective"** Institute of Technology (CSPIT), Faculty of Technology & Engineering (FTE), Charotar University of Science and Technology (CHARUSAT), Changa, Gujarat, India (2021).

[35] Udo Helmbrecht, "Είναι τα έξυπνα σπίτια ευφυή από άποψη ασφάλειας στον κυβερνοχώρο;"Δελτίο Τύπου EPR06/2015, https://www.enisa.europa.eu/news/enisa-news/prs-in-gr/einai-ta-exipna-spitia-efii-apo-apopsi-asfalias-ston-kivernohoro

[36] Muhammad Saad **"Cyber Security And Internet of Things"**, Department of Computer Science, SZABIST Dubai Campus and 1Tariq Rahim Soomro, College of Computer Science & Information Systems, Karachi (2020).

[37] Don Shin, John Pescatore, Webcast, **"Techniques to Modernize Your DDoS Defenses"**, Tuesday, July 24, 2018 at 3:30 PM EDT https://www.sans.org/webcasts/4-techniques-modernize-ddos-defenses-108315,4

[38] Shamsul Hudaa, John Yearwooda, Mohammad Mehedi Hassanb, Ahmad Almogrenb, **"Securing the operations in SCADA - IoT platform based industrial control system using ensemble of deep belief networks "**, College of Computer and Information Sciences, King Saud University, Riyadh, 11543, Saudi Arabia (2018)

[39] https://www.ansys.com/blog/iot-autonomous-vehicle-electrification

[40] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained

[41]Song Wang, Karina Gomez, Kandeepan Sithamparanathan, Muhammad Rizwan Asghar, Giovanni Russello and Paul Zanna, **"Mitigating DDoS Attacks in SDN-Based IoT Networks Leveraging Secure Control and Data Plane Algorithm",** The University of Auckland, New Zealand**,** (2021).

[42]Natalija Vlajic and Daiwei Zhou, **"IoT as a Land of Opportunity for DDoS Hackers",** York University https://www.computer.org/ (2018)

[43] Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus, **"Detection and Defense Algorithms of Different Types of DDoS Attacks"**, International Journal of Engineering and Technology, Vol. 9, No. 5, (October 2017)

[44] Anup Ingle. Avinash Gour, Ketki Kshirsagar, **"DDoS Attack Detection Algorithms Based on Pattern Classification and Machine Learning"**, Journal of University of Shanghai for Science and Technology, (2021).

10. ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AAM - Attack Alarm Module

AAT - Augmented Attack Tree

AMQP - Advanced Message Queuing Protocol

AIP – Attackers Information Packet

ANN - Artificial Neural Networks

APM - Application Performance Monitoring

ASP - Active Server Pages

ATM - Automated teller machine

BANs - Bayesian Augmented Networks

BLE - Bluetooth Low Energy

BN - Bayesian network

CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart

CATs - Change Aggregation Trees

CoAP - Constrained Application Protocol

DCP - Distributed Change Point

DDos - Distributed Denial of Service

DDS - Data Distribution Service

DMZ - Demilitarized Zone

DoS – Denial of Service

DPM - Deterministic packet marking

EOP - Elevation of Privilege

FFV - Flow Feature Value algorithm

GBNs - General Bayesian Networks

HLT - High Level thresold

HTTPS - Hypertext Transfer Protocol Secure

HVAC - Heating Ventilation Air Conditioning

ICMP - Internet Control Message Protocol

ICS - Industrial Control Systems

IDS - Intrusion Detection System

IoT - Internet of Things

IP - Internet Protocol

IRC - Internet Relay Chat

ISP - Internet Service Provider

IIoT - Industrial IoT

KSOM - Kohonen Self Organizing Map

LAN - Local Area Network

LBR - Lazy Bayesian rule

LLT - Low Load Threshold

LOT - License on Transfer

LTE - Long Term Evolution

LVQ - Linear Vector Quantization

MLP - Multilayer perceptron

MQTT - Message Queue Telemetry Transport

MULTOPS - MUlti-Level Tree for Online Packet Statistics

NFC - Near Field Communication

PHP - Hypertext Preprocessor

PLC - Power Line Communication

PPM - Probabilistic packet marking

RASP - Runtime application self-protection

RBAC - Role Based Access Control

RBF - Radial Basis Function

RFID - Radio-frequency identification

RNN - Random Neural networks

RSA - Rivest, Shamir, and Adleman

SCADA - Supervisory Control and Data Acquisition

SMB - Server Message Block

SMB - Server Message Block

SOM - Self Organizing Map

SQL – Structured Query Language

SSH - Secure Shell

SSHPA - SSHowDowN Proxy Attack

SSL - Secure Socket Layer

SSM - Statistical Segregation Method

SYN - Synchronize

SYN-**ACK** – Synchronize Acknowledge

TANs - Tree-augmented Naïve Bayes Networks

TCP - Transmission Control Protocol

TDNN - Time Delay Neural Network

UDP - User Datagram Protocol

VP - Virtual prototype

VSS - Victim Server System

XSS - Cross-Site Scripting