ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

ΠΜΣ «Ασφάλεια Ψηφιακών Συστημάτων»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ:

Έμπιστα περιβάλλοντα για πράγματα του διαδικτύου

Φοιτητής:

Αζναουρίδης Χρίστος Νεκτάριος

Επιβλέπων Καθηγητής:

Κωνσταντίνος Λαμπρινουδάκης

Σεπτέμβριος 2019

ΠΙΣΤΟΠΟΙΗΣΗ

Πιστοποιείται ότι η Διπλωματική Εργασία με θέμα

«Trusted Environments For Internet of Things**»**

Του φοιτητή του Τμήματος Ψηφιακών Συστημάτων

Χρίστου - Νεκτάριου Αζναουρίδη του Ιωάννη

(ΑΜ. ΜΤΕ 1702)

Παρουσιάσθηκε δημόσια και εξετάσθηκε στο Τμήμα Ψηφιακών Συστημάτων

Ο Επιβλέπων

Κωνσταντίνος Λαμπρινουδάκης

Καθηγητής ΤΨΣ

Αριθμός Διπλωματικής Εργασίας:

Θέμα «Trusted Environments For Internet of Things**»**

Φοιτητής	Επιβλέπων
Χρίστος-Νεκτάριος Αζναουρίδης	Κωνσταντίνος Λαμπρινουδάκης

Ευχαριστίες

Πρώτα από όλα θα ήθελα να ευχαριστήσω τον επιβλέποντα την διπλωματική μου διατριβή, Καθηγητή Κωνσταντίνο Λαμπρινουδάκη του Τμήματος Ψηφιακών Συστημάτων, της Σχολής Τεχνολογιών Πληροφορικής και Τεχνολογιών, του Πανεπιστημίου Πειραιώς, για την επιστημονική, πνευματική και ηθική στήριξη που μου παρείχε.

Παράλληλα θα ήθελα να ευχαριστήσω το διδακτικό προσωπικό του ΤΨΣ για τις πολύτιμες γνώσεις που μου μετάγγισε κατά τη διάρκεια των σπουδών μου, διευρύνοντας τους επιστημονικούς μου ορίζοντες και καλλιεργώντας την αγάπη μου για την έρευνα.

.

Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου για την ηθική συμπαράσταση και τον εποικοδομητικό σχολιασμό κατά την εκπόνηση της παρούσας διατριβής.

.

Πρέπει να επισημάνω ότι τυχόν αβλεψίες ή λάθη της μελέτης αυτής βαρύνουν αποκλειστικά εμένα.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Κατά τη διάρκεια των τελευταίων ετών η επάρκεια των αποτελεσματικών ασύρματων πρωτοκόλλων, οι βελτιωμένοι αισθητήρες, οι φτηνότεροι επεξεργαστές, οι καθιερωμένες εταιρείες που αναπτύσσουν το απαραίτητο λογισμικό διαχείρισης και εφαρμογών έχουν τελικά αναγάγει την έννοια του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) σε κυρίαρχο ρεύμα.

Ο όρος «Internet of Things» γνωστός επίσης και ως «Internet of Objects» αφορά τη χρήση πρότυπων πρωτοκόλλων του Διαδικτύου για τη δημιουργία ενός ασφαλούς περιβάλλοντος επικοινωνίας τύπου human-to-thing ή thing-to-thing σε ενσωματωμένα δίκτυα. Σχηματικά ο όρος περιγράφει τρία πράγματα και την αρμονική τους συλλειτουργία. Το πρώτο είναι τα **Αντικείμενα** που είναι ενσωματωμένα με αισθητήρες, το δεύτερο είναι τα **Συστήματα** επεξεργασίας των δεδομένων και το τρίτο είναι το **Δίκτυο** μέσω του οποίου ανταλλάσσονται τα δεδομένα και υλοποιείται η επικοινωνία. Ουσιαστικά πρόκειται για ένα δίκτυο φυσικών αντικειμένων σε επικοινωνία, που μέσω της διαδικτυακής συνδεσιμότητας καθίσταται δυνατή η συλλογή και η ανταλλαγή δεδομένων μεταξύ των αντικειμένων αυτών.

Η ταχεία ανάπτυξη των συνδεδεμένων συσκευών στο διαδίκτυο εκτιμάται ότι θα κυμανθεί μεταξύ 25 και 50 δισ. ευρώ μέχρι τα τέλη του 2020. Σε αυτές θα περιλαμβάνονται όλες οι οικιακές συσκευές, οι συσκευές που αφορούν την υγεία και τη βελτίωση της φυσικής κατάστασης, ο βιομηχανικός εξοπλισμός, οι κατανεμημένοι αισθητήρες, τα αυτοκίνητα, καθώς και μια σειρά νέων συσκευών που βρίσκονται στο στάδιο της ανάπτυξής τους.

Η νέα αυτή τεχνολογική εποχή, όπου κάθε μικρή συσκευή γύρω μας θα βρίσκεται διασυνδεδεμένη με το διαδίκτυο, απαιτεί την ανάπτυξη της κυβερνο-ασφάλειας (Cyber Security) με ένα ρυθμό, τουλάχιστον ίδιο με το ρυθμό αύξησης των διασυνδεδεμένων νέων συσκευών, ώστε να αποφευχθούν ζητήματα με σημαντικό αντίκτυπο.

Στα πλαίσια της παρούσας μεταπτυχιακής διατριβής παρουσιάζεται και αναλύεται η κυβερνασφάλεια στην περίπτωση των συσκευών που έχουν υιοθετήσει και χρησιμοποιούν την τεχνολογία του IoT. Στα πρώτα Κεφάλαια της μελέτης αναλύεται κάθε πτυχή της IoT τεχνολογίας ενώ στη συνέχεια γίνεται αναφορά στα υποδείγματα (models) σύνδεσης των συσκευών με τα συστήματα επεξεργασίας μέσω διαδικτύου, με την εισαγωγή της IoT τεχνολογίας. Στα επόμενα Κεφάλαια γίνεται αναφορά στην

επιφάνεια επίθεσης και τα πλέον τρωτά (ευάλωτα) σημεία του Internet of Things, καθώς και στα αντίμετρα που είναι δυνατόν να αναληφθούν για προστασία, όπως και στις μεθοδολογίες διενέργειας των δοκιμών διείσδυσης.

Στην μεταπτυχιακή διατριβή επίσης συμπεριλαμβάνεται και αναλύεται η αναγκαιότητα ανάπτυξης ενός πλαισίου κυβερνο-ασφάλειας που να αναφέρεται και να αφορά τις συσκευές που υιοθετούν τη τεχνολογία του Internet of Things, τις τυχόν ευπάθειες του IoT και την περίπτωση της έρευνας όπου θα παρουσιασθούν τα ευρήματα των ευάλωτων συσκευών IoT. Προκλήσεις πάνω σε θέματα ασφάλειας, όπως τα ζητήματα εμπιστευτικότητας και ιδιωτικού βίου καταγράφονται και αναλύονται από κάθε άποψη διεξοδικά.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

- Αξιόπιστο Περιβάλλον
- Αισθητήρας
- Αλυσίδα Εμπιστοσύνης
- Back-End Data-Sharing Model
- Bluetooth
- Cyber Security
- Διαδίκτυο
- Διαδίκτυο των Αντικειμένων
- Διαδίκτυο των Πραγμάτων
- Δίκτυο
- Ενσωματωμένα Συστήματα
- Embedded Systems
- Επικοινωνία δεδομένων
- Επεξεργασία δεδομένων
- Gateway
- Internet
- Internet of Objects
- Internet of Things
- IoT
- Κενά Ασφαλείας
- Κυβερνασφάλεια
- Κυβερνο-ασφάλεια
- Malware
- Μοντέλα σύνδεσης
- Νεφοϋπολόγισμοί
- Παγίδευση Κύματος
- Περιβάλλον Ασφάλειας
- Piconet
- Πλατφόρμα IoT
- Power Line Communication
- Πρωτόκολλο IPv4
- Πρωτόκολλο IPv6
- Scatternet
- Σύνδεση συσκευών
- Τεχνολογία του IoT
- Trusted Environments
- Τρωτότητα
- Vulnerability
- Υποδείγματα σύνδεσης
- ZigBee
- Z-Wave

ΠΙΝΑΚΑΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

Κεφάλαιο 1ο

Κεφάλαιο 2ο

Κεφάλαιο 3ο

Κεφάλαιο 4ο

Κατά τις τελευταίες δεκαετίες το Διαδίκτυο έχει επιφέρει σημαντική επανάσταση στους τομείς των υπολογιστών και των επικοινωνιών. Από το 1969, τότε που το πρώτο μήνυμα στάλθηκε στο ARPANET πολλά πράγματα έχουν αλλάξει. Στις μέρες μας το 56,1% του παγκόσμιου πληθυσμού έχει πλέον πρόσβαση στο Διαδίκτυο με μια διαρκώς διευρυνόμενη τάση. Όλο και περισσότερες εφαρμογές αναπτύσσονται, όλο και περισσότερα πράγματα πλέον γίνονται με τη βοήθεια του διαδικτύου και των υπολογιστών

Η ταχεία ανάπτυξη του Διαδικτύου και η συνεχής σμίκρυνση των νέων ηλεκτρονικών συσκευών, οδηγούν σταδιακά στη ραγδαία αύξηση του αριθμού των συνδεδεμένων στο διαδίκτυο αντικειμένων. Έξυπνα κινητά τηλέφωνα, ηλεκτρικές συσκευές, ηλεκτρονικά βιβλία, αυτοκίνητα, συστήματα παραγωγής, αλλά και ηλεκτρονικές ετικέτες προϊόντων, έχουν πλέον τη δυνατότητα να συνδεθούν στο διαδίκτυο και να αλληλεπιδράσουν τόσο μεταξύ τους όσο και με ανθρώπους και υπολογιστές. Διαμορφώνεται έτσι ένα νέο, δυναμικό και ταχέως επεκτεινόμενο περιβάλλον που ονομάζεται Internet of Things-IoT. Θα μπορούσαμε να πούμε ότι το «Διαδίκτυο των Υπολογιστών» μεταλλάσσεται σε «Διαδίκτυο των Αντικειμένων».

Δημιουργείται ένα περιβάλλον από «έξυπνες» συσκευές, που με τη βοήθεια του Internet επικοινωνούν με άλλες συσκευές, αντικείμενα, περιβάλλοντα και υποδομές, με τα οποία αλληλεπιδρούν και έτσι παράγεται ένας τεράστιος όγκος δεδομένων με σημαντική χρηστικότητα στην οικονομία, στην παραγωγή, στην αγορά, στην κοινωνία, αλλά και στην απλή καθημερινή ζωή του ανθρώπου.

Θεμελιώδης προϋπόθεση για την ομαλή και αποδοτική λειτουργία αυτού του περιβάλλοντος είναι η ασφάλεια και η αξιοπιστία. Τα συνδεδεμένα και αλληλεπιδρώντα αντικείμενα πρέπει να διασφαλίζονται από παράγοντες όπως οι κακόβουλες ενέργειες, το σφάλμα της ανθρώπινης παρέμβασης, το τυχαίο γεγονός, την αστοχία, τις ασαφείς οδηγίες και οι επικρατούσες κάθε φορά συνθήκες. Με απλά λόγια η όλη λειτουργία της τεχνολογίας Internet of Things πρέπει να επιτελείται σε «Trusted Environment». Έτσι τα παραγόμενα και μεταβιβαζόμενα δεδομένα και πληροφορίες, όντας αληθή και αξιόπιστα, θα επιτυγχάνουν το μέγιστο δυνατό επιθυμητό αποτέλεσμα, στην οικονομία, στην κοινωνία και στην απλή ανθρώπινη καθημερινότητα

Η παρούσα διατριβή φιλοδοξεί να παρουσιάσει και να περιγράψει την αρχιτεκτονική των συστημάτων του «Διαδικτύου των Αντικειμένων», να αποτυπώσει τις ραγδαίες εξελίξεις που συντελούνται με τη συνεχώς διευρυνόμενη ανάπτυξη νέων

εφαρμογών του Διαδικτύου αυτού, τόσο στην απλή ανθρώπινη καθημερινότητα, όσο επίσης στην οικονομία και την παραγωγή. Έτι περεταίρω στοχεύει στο να καταδείξει τις αλληλεπιδράσεις μεταξύ των συσκευών του Διαδικτύου των Αντικειμένων, καθώς επίσης και μεταξύ των συσκευών με το νεφοϋπολογιστικό περιβάλλον, να προβάλλει τη σύνθεση εφαρμογών με την αξιοποίηση των υπηρεσιών που διαθέτει η πλατφόρμα του Διαδικτύου των Αντικειμένων και όλα αυτά σε ένα περιβάλλον αξιοπιστίας και ασφάλειας.

Το **κεντρικό ερευνητικό ερώτημα** συνίσταται

Η μελέτη συγκροτείται από Κεφάλαια και διαρθρώνεται ως ακολούθως:

Στο **1ο Κεφάλαιο** γίνεται εκτενής αναφορά στην τεχνολογία του Διαδικτύου των Αντικειμένων (Απαρχή, ιστορική εξέλιξη, ορισμός και περιγραφή του IoT, πεδίο εφαρμογών, χρηστικότητα, σημαντικότητα και τεχνολογικά χαρακτηριστικά των IoT εφαρμογών)

Στο **2ο Κεφάλαιο** η αναφορά περιλαμβάνει τα υποδείγματα ενοποίησης και επικοινωνίας στο IoT. Ειδικότερα παρουσιάσθηκαν οι τύποι device-to-device, device-to-cloud, device-to-gateway, Back-End Data-Sharing Model και τα Πρωτόκολλα IPV4, IPV6 στο Internet of Things.

Στο **3ο Κεφάλαιο** θίγεται το ζήτημα της ασφάλειας στο IoT. Οι έξι βασικές αρχές ασφάλειας των υπολογιστικών συστημάτων και δικτύων δηλαδή η Εμπιστευτικότητα, η Ακεραιότητα, η Διαθεσιμότητα, η Ιδιωτικότητα, η Αυθεντικότητα και η Μη Αποποίηση ανάγονται σε στόχους ασφάλειας για το IoT. Στο Κεφάλαιο προβάλλονται τα κοινά προβλήματα αξιοπιστίας στο Internet of Things και αξιολογούνται τα Wi Fi Networks (802.11), Z-Wave, ZigBee, Powerline, Bluetooth Low Energy, και άλλα RF πρωτόκολλα. Αναλύονται μείζονα ζητήματα ασφαλείας όπως έρευνες των OWASP και Symantec έχουν προβάλει και γίνεται αναφορά στις ευπάθειες που παρουσιάζει το σύστημα.

1. Διαδίκτυο των Αντικειμένων

1.1 ΕΙΣΑΓΩΓΗ

Στην καθημερινότητά μας όλο και περισσότερο συναντάμε πλήθος αντικειμένων που λειτουργούν διασυνδεδεμένα με το διαδίκτυο. Από το πολύ κοντινό ιστορικά, αλλά πολύ μακρινό για την επιστήμη των Υπολογιστών και του Ψηφιακού Κόσμου, έτος 1999 συναντάμε τον όρο Internet of Things. Ο όρος που εκφράζει ένα ενοποιημένο και συλλειτουργούν περιβάλλον, εμπεριέχει μια διαρκώς διευρυνόμενη δυναμική που φέρνει επανάσταση σε τομείς όχι μόνο της παραγωγικής διαδικασίας αλλά και της καθημερινής ζωής του ανθρώπου.

Το αντικείμενο της παρούσας ενότητας είναι η περιγραφή και η ανάλυση αυτού που στα ελληνικά αποδίδεται με όρο Διαδίκτυο των Αντικειμένων, τα στοιχεία συγκρότησής του, το πεδίο εφαρμογής του, οι τάσεις που διαμορφώνονται στο μέλλον και οι ευκαιρίες ανάπτυξης που προσφέρονται από το διαρκώς μεταβαλλόμενο εξωτερικό περιβάλλον

1.2 ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ (INTERNET OF THINGS)

1.2.1 Ιστορική αναφορά

Γύρω στα τέλη της δεκαετίας του 1990, ο Kevin Ashton, ένας από τους ιδρυτές του Auto-ID Center στο MIT, εισήγαγε τον όρο «Διαδίκτυο των Πραγμάτων» όταν η ομάδα στην οποία ήταν μέλος επινόησε έναν τρόπο διασύνδεσης των αντικειμένων με το διαδίκτυο μέσω μιας ετικέτας RFID. Έτσι προτάθηκε η αρχική ιδέα και καθιερώθηκε η χρήση του πιο επιστημονικού όρου Internet of Things (IoT) για την περιγραφή της τεχνικής αυτής.

Η ανάπτυξη του Διαδικτύου των Πραγμάτων (IoT) κατευθύνθηκε αρχικά από τις ανάγκες κυρίως των μεγάλων εταιρειών που επωφελούνται σε υπερθετικό βαθμό από την πρόβλεψη και γενικά την ικανότητα προβλεπτικότητας, που παρέχεται από την δυνατότητα ακολούθησης όλων των υποσυστημάτων δια μέσου των αλυσίδων εμπορευμάτων στις οποίες είναι ενσωματωμένα

Πριν το Internet λάβει τη σημερινή του μορφή, το 1974, τα τραπεζικά ATM’s ήταν ουσιαστικά τα πρώτα online αντικείμενα. Το 1989 εμφανίσθηκε η πρώτη τοστιέρα που συνδέθηκε με το Διαδίκτυο. Το 2008 τα αντικείμενα που ήταν online, συνδεδεμένα

στο Διαδίκτυο ήταν περισσότερα από τους ανθρώπους που είχαν πρόσβαση σε αυτό. Το 2015 οι πωλήσεις στα smartπhones εκτιναχτήκαν στις 1,4 δις συσκευές, αριθμός που αναμένεται να ξεπεράσει τα 6 δις το 2020. Το ίδιο έτος (2015) ο αριθμός των διασυνδεδεμένων πραγμάτων έφτανε τα 5 δις, η δε παγκόσμια αγορά των wearables εκτοξεύτηκε κατά 223%, Επίσης κάνουν την εμφάνισή τους και τα «έξυπνα ρούχα» και προβλέπεται να κυκλοφορήσουν μέχρι το 2020, 10,2 εκατομμύρια κομμάτια,

Η φράση Internet of Things χρησιμοποιήθηκε για πρώτη φορά σε μια παρουσίαση του Ashton, την οποία έκανε το 1999 και από τότε ο όρος αυτός καθιερώθηκε στην επιστήμη και την πρακτική. Στη ραγδαία εξέλιξη της τεχνολογίας IoT συνέβαλαν σημαντικά, η ταχεία διάδοση του ασύρματου internet και των ενσωματωμένων αισθητήρων. Έτσι εξελίχθηκε και υιοθετήθηκε ως επαγγελματικό αλλά και προσωπικό εργαλείο.

Ο Jason Handley, της εταιρείας Duke Energy (Director of Smart Grid Technology and Operations), αντιλαμβάνεται ένα ενοποιημένο περιβάλλον και κάνει λόγο για *«ένα κόσμο όπου όλα θα είναι συνδεδεμένα μεταξύ τους, η ενέργεια θα είναι αποδοτική και όλα θα οδηγούνται από τη γνώση που παίρνουμε με τη χρήση advanced analytics»*.

1.2.2 Γενική περιγραφή του IoT

Ο όρος «Internet of Things» αναφέρεται στη χρήση πρότυπων πρωτοκόλλων του Διαδικτύου που αφορούν στην επικοινωνία Ανθρώπων – Αντικειμένων (human-to-thing) ή Αντικειμένων με Αντικείμενα (thing-to-thing), σε ενσωματωμένα δίκτυα. Μερικές φορές το Διαδίκτυο των Αντικειμένων αναφέρεται ως μια πανταχού παρούσα τεχνική δικτύωσης και υπολογιστικής πληροφορικής.

Μια άλλη απλή προσέγγιση του όρου, είναι ότι συνιστά ένα δίκτυο φυσικών πραγμάτων, συσκευών, οχημάτων, κτιρίων και άλλων αντικειμένων που δημιουργούν ένα περιβάλλον ενοποιημένο και ενσωματώνονται με ηλεκτρονικά, λογισμικά, αισθητήρες και διαδικτυακή συνδεσιμότητα που επιτρέπει σε όλα αυτά τα αντικείμενα να συλλέγουν και να ανταλλάσσουν δεδομένα μεταξύ τους.

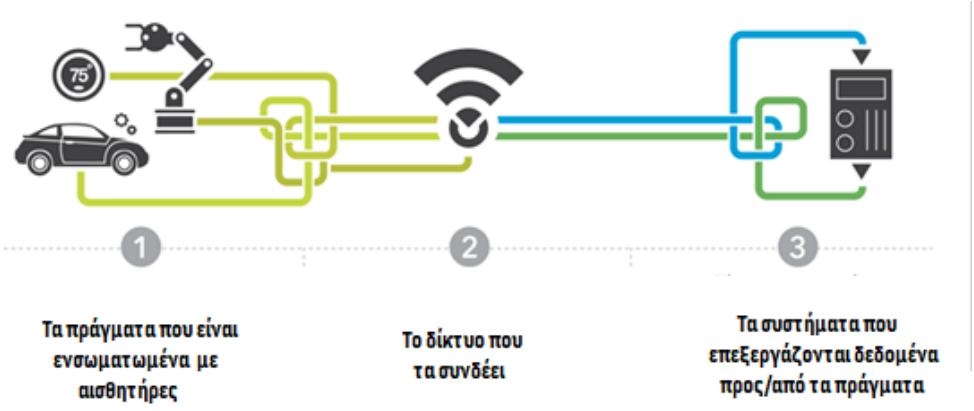
Κατά άλλους το Διαδίκτυο των Αντικειμένων περιλαμβάνει όλες τις διασυνδεδεμένες συσκευές με το Internet, η δε λειτουργία του στηρίζεται στις υπολογιστικές δυνατότητες των συσκευών αυτών ανάλογα με το ενσωματωμένο

λογισμικό, που έχουν. Το Internet of Things - IoT δηλαδή αποτελείται από «έξυπνες» συσκευές, που αλληλεπιδρούν και επικοινωνούν με άλλες συσκευές, αντικείμενα, περιβάλλοντα και υποδομές με αποτέλεσμα την παραγωγή μεγάλου όγκου δεδομένων, σημαντικής χρηστικότητας για τον άνθρωπο.

Παρά την ποικιλία των ορισμών και των προσεγγίσεων του Internet of Things, η έννοια και η ουσία του παραμένει σε όλους αυτούς παρόμοια. Όλοι οι ορισμοί περιγράφουν σενάρια στα οποία η δυνατότητα δικτυακής συνδεσιμότητας και υπολογιστικής ικανότητας επεκτείνεται σε έναν αστερισμό αντικειμένων, συσκευών, αισθητήρων και καθημερινών πραγμάτων, που συνήθως δεν θεωρούνται υπολογιστές. Η δυνατότητα αυτή επιτρέπει στις συσκευές να δημιουργούν (γεννούν), να ανταλλάσσουν και να καταναλώνουν δεδομένα (data), συχνά με ελάχιστη ανθρώπινη παρέμβαση.

Το Internet of Things (Διαδίκτυο των Πραγμάτων) αφορά αντικείμενα της καθημερινότητας του ανθρώπου, από βιομηχανικές μηχανές μέχρι συσκευές wearable με ενσωματωμένους αισθητήρες, για συλλογή δεδομένων και ανάληψη δράσεων ή λειτουργιών σε αυτά, μέσα σε ένα δίκτυο. Αποτελεί το τεχνολογικό μέλλον που αναμένεται να διευκολύνει σημαντικά τη ζωή όλων. Για παράδειγμα, ένα κτίριο που για την αυτόματη ρύθμιση της θέρμανσης ή του φωτισμού του χρησιμοποιεί αισθητήρες (sensors) ή ο εξοπλισμός παραγωγής που προειδοποιεί έγκαιρα το προσωπικό συντήρησης για κάποια επικείμενη βλάβη, λειτουργούν με αυτή τη φιλοσοφία.

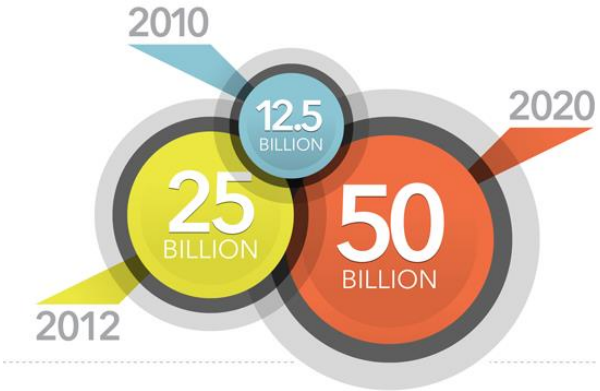
Το Internet of Things συνίσταται από τρία κύρια μέρη τα οποία εμφανίζονται σχηματικά στο διάγραμμα που ακολουθεί και συγκεκριμένα τα Πράγματα (με τους αισθητήρες), τα Συστήματα επεξεργασίας και ανάλυσης των δεδομένων και το Δίκτυο που τα συνδέει μεταξύ τους. Το «Διαδίκτυο των Αντικειμένων» είναι η διασύνδεση των καθημερινών αντικειμένων, τόσο μεταξύ τους, όσο και με το διαδίκτυο.



Σχήμα 1.1 Το Internet of Things (IoT)

Με βάση την παραπάνω γραφική απεικόνιση της διασύνδεσης πραγμάτων – συστημάτων – διαδικτύου, για λόγους κατανόησης του τρόπου λειτουργίας και των δυνατοτήτων της τεχνικής του Internet of Things, παρατίθεται το παράδειγμα του «έξυπνου ψυγείου» που θα μπορεί να ενημερώνει τους χρήστες για τα προϊόντα που πλησιάζουν στην ημερομηνία λήξης αλλά και θα μπορεί να παραγγέλνει μόνο του, μέσω του διαδικτύου, τα προϊόντα που εξαντλούνται.

Αν αναλογιστούμε ότι πάρα πολλά από τα πράγματα είναι συνδεδεμένα με το διαδίκτυο και ότι ακόμη περισσότερα είναι δυνατόν να διασυνδεθούν, μπορούμε να αντιληφθούμε τα σημαντικά οικονομικά οφέλη που θα προκύψουν από την ανάλυση και επεξεργασία της ροής των δεδομένων (data streams). Βιομηχανικά περιουσιακά στοιχεία αλλά και απλά καθημερινά αντικείμενα μπορούν να επικοινωνούν μεταξύ τους με τη χρήση της τεχνολογίας IoT και ο αριθμός τους θα τείνει αυξητικά με την πάροδο του χρόνου. Όπως έχει δείξει το άμεσο παρελθόν και όπως με ακρίβεια προβλέπεται για το μέλλον που έπεται, ο νέος αυτός κόσμος των διασυνδέσεων θα βαίνει διαρκώς διογκούμενος.



Σχήμα 1.2 Η διαχρονική αύξηση των συνδέσεων

Η άμεση και κύρια συνέπεια της υιοθέτησης και της εφαρμογής της τεχνολογίας του IoT καθώς και της διεύρυνσής της, είναι η παραγωγή μεγάλου όγκου δεδομένων, από την επεξεργασία του οποίου συμπεραίνονται δράσεις εντολών και ελέγχου των αντικειμένων, που διευκολύνουν σε πολλούς τομείς την ανθρωπογενή δράση. Παράλληλα την καθιστούν πιο ασφαλή ενώ περιορίζουν πολυεπίπεδα την αρνητική επίδραση στο περιβάλλον. Το IoT με απλά λόγια ως τεχνολογία συνθέτει ένα νέο κόσμο διασυνδεδεμένων αντικειμένων.

1.2.3 Περιγραφή εφαρμογών του IoT

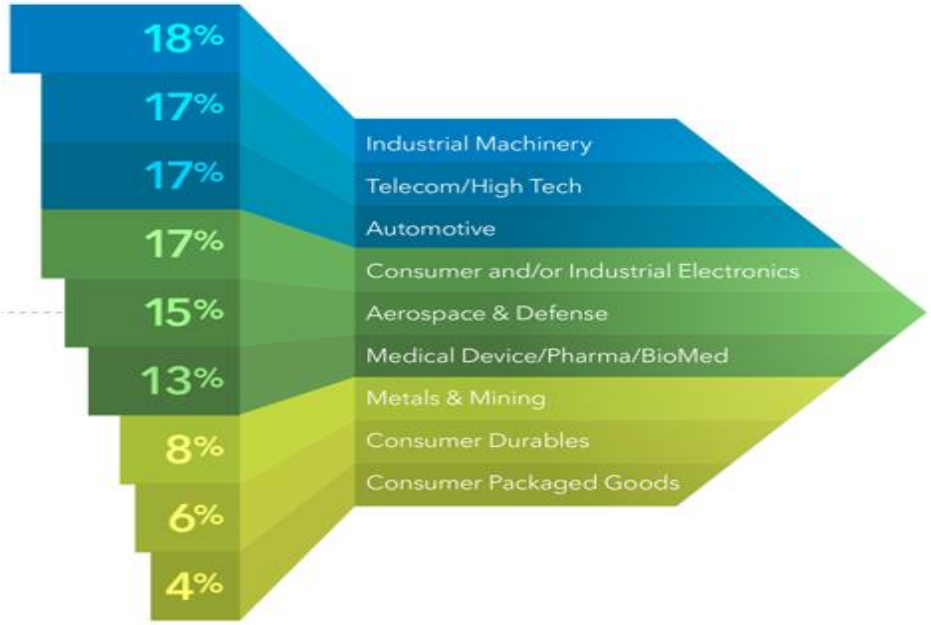
Είναι εντυπωσιακό το μέγεθος του πεδίου εφαρμογών του Internet of Things στον πραγματικό κόσμο. Το πεδίο αυτό αφορά και επηρεάζει τόσο μεμονωμένα άτομα όσο και ευρύτερα σύνολα ανθρώπων. Η εφαρμογή μπορεί να επεκτείνεται στις λειτουργίες των «έξυπνων» πόλεων, στην περιβαλλοντική διαχείριση, στους υδάτινους πόρους, στην ασφάλεια, στην αντιμετώπιση εκτάκτων αναγκών, στο «έξυπνο» λιανεμπόριο, στην ανεφοδιαστική αλυσίδα, στο βιομηχανικό έλεγχο, στη γεωργία, στη κτηνοτροφία, στο «έξυπνο» σπίτι, στην παροχή ηλεκτρονικών υπηρεσιών υγείας και σε άλλους πάρα πολλούς τομείς.

Παρακάτω αναφέρουμε ενδεικτικούς τομείς εφαρμογών του I o T:

- Έξυπνες πόλεις: Διαχείριση κυκλοφορίας, διαχείριση αποβλήτων, δομική υγεία, ηχητικοί αστικοί χάρτες, ευφυή συστήματα μεταφοράς.
- Έξυπνο περιβάλλον: Πρόβλεψη σεισμών, ανίχνευση δασικών πυρκαγιών, μέτρηση της ποιότητας του αέρα και της ρύπανσης, πρόληψη χιονοστιβάδων και κατολισθήσεων.
- Έξυπνο νερό: Διασφάλιση ποιότητας νερού, πρόληψη διαρροών, διαχείριση στάθμης δεξαμενών, αναγνώριση και πρόληψη ποτάμιων πλημμυρών.
- Καταστάσεις έκτακτης ανάγκης και Ασφάλεια: Έλεγχοι πρόσβασης περιμέτρου, ανίχνευση ακτινοβολίας και υγρών, ανίχνευση εκρηκτικών και επικίνδυνων αερίων, διαχείριση υπηρεσιών έκτακτης ανάγκης.
- Έξυπνο λιανεμπόριο: Έλεγχος αλυσίδας εφοδιασμού, πληρωμές με τη χρήση της πρότυπης τεχνολογίας «επικοινωνίας κοντινού πεδίου» NFC, διαχείριση έξυπνων προϊόντων, απομακρυσμένη διαχείριση μηχανημάτν αυτόματης πώλησης.
- Έξυπνη εφοδιαστική αλυσίδα: Διασφάλιση συνθηκών ποιότητας στις αποστολές, εντοπισμός αντικειμένων, παρακολούθηση στόλου, γεω-τοποθέτηση, διαχείριση αποστολών / παραδόσεων.

- Βιομηχανικός έλεγχος: Εφαρμογή M2M (Machine to Machime), έλεγχος περιβάλλοντος (HVAC), έλεγχος θερμοκρασίας, παρουσία όζοντος, αυτοδιάγνωση οχήματος, διαχείριση αποθήκης αποθεμάτων.
- Έξυπνη γεωργία: Παρακολούθηση της ποιότητας του κρασιού, άρδευση καλλιεργειών, έλεγχος του θερμοκηπίου, διαχείριση πάρκων.
- Έξυπνη κτηνοτροφία: Φροντίδα των νεογέννητων ζώων, παρακολούθηση των ζώων, παρακολούθηση του περιβάλλοντος, μέτρηση επιπέδων τοξικών αερίων, παρακολούθηση της υγειονομικής περίθαλψης των ζώων, διαχείριση ιστορικού τροφίμων.
- Έξυπνα σπίτια (αντίστοιχα έξυπνα γραφεία, ξενοδοχεία): Έλεγχος θερμοκρασίας και υγρασίας, απομεμακρυσμένος αυτοματισμός, έλεγχος αστραπής και ατμόσφαιρας, ενεργειακή απόδοση, συστήματα ανίχνευσης εισβολών, συναγερμοί πυρκαγιάς και ασφάλειας.
- Ηλεκτρονική υγεία (ehealth): Ανίχνευση πτώσης, παρακολούθηση αθλητικής δραστηριότητας, επιτήρηση ασθενών, παρακολούθηση εξοπλισμού, οθόνες κατάστασης υγείας και φυσικής κατάστασης, οθόνες υπεριώδους ανίχνευσης.

Τα δεδομένα (data) του Internet of Things χρησιμοποιούνται στη βιομηχανική παραγωγή, την υγειονομική περίθαλψη, τις τηλεπικοινωνίες, το λιανεμπόριο, τις μεταφορές και την ενέργεια. Ειδικότερα είναι διαδεδομένα στους παρακάτω βιομηχανικούς τομείς με τα αντίστοιχα ανά τομέα ποσοστά. εδώ περιλαμβάνονται οι βιομηχανίες μηχανών και μηχανημάτων, οι βιομηχανίες τηλεπικοινωνιών και υψηλής τεχνολογίας, οι αυτοκινητοβιομηχανίες, οι βιομηχανίες ηλεκτρονικών, οι αεροδιαστημικές και οι αμυντικές βιομηχανίες, οι βιομηχανίες ιατρικού εξοπλισμού, οι φαρμακοβιομηχανίες, οι μεταλλευτικές και εξορυκτικές βιομηχανίες, οι βιομηχανίες καταναλωτικών αγαθών και συσκευασμένων αγαθών.



Σχήμα 1.3 Η διάδοση του IoT ανά βιομηχανικό τομέα

1.2.4 Η σημαντικότητα του Internet of Things

Απόρροια της ευρείας εφαρμογής της τεχνολογίας του Internet of Things είναι τα σημαντικά αποτελέσματα που επιφέρει και τα οποία συνίστανται κυρίως σε οικονομικά οφέλη και όχι μόνο, που αποκομίζονται από την ανάλυση των data streams. Με την εφαρμογή του Internet of Things σε κάποιο τομέα δημιουργούνται αλληλουχίες συνεπειών όπως αυτές που παρουσιάζονται παρακάτω.

α) Οι έξυπνες λύσεις μεταφορών επιταχύνουν την ροή της κυκλοφορίας, μειώνουν την κατανάλωση των καυσίμων, θέτουν σε προτεραιότητα τα προγράμματα επισκευής οχημάτων και τελικά σώζουν ζωές.

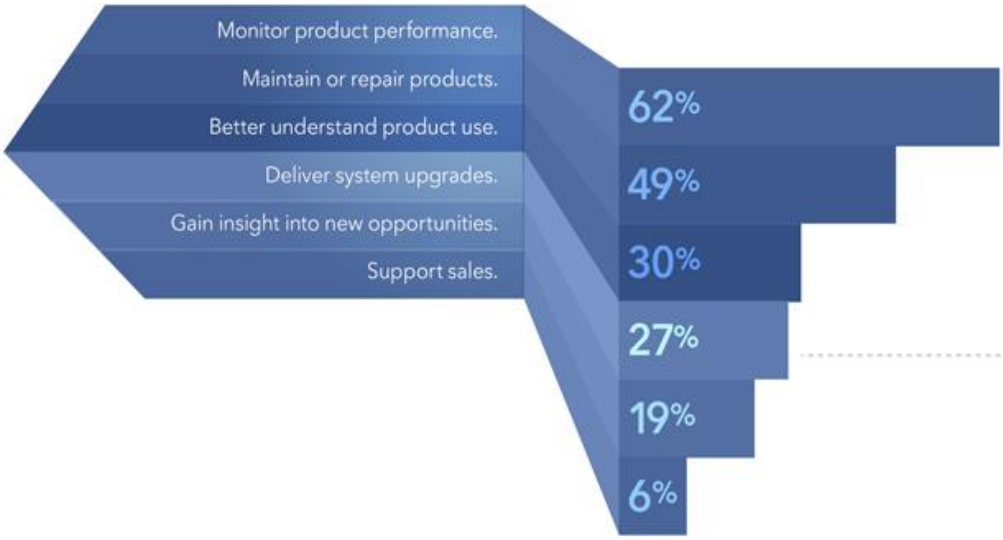
β) Τα έξυπνα ηλεκτρικά δίκτυα (smart electric grids) συνδέουν πιο αποτελεσματικά τις ανανεώσιμες πηγές ενέργειας, έτσι βελτιώνεται η αξιοπιστία του συστήματος και οι καταναλωτές χρεώνονται με βάση μικρότερες προσαυξήσεις.

γ) Οι μηχανές αισθητήρων παρακολούθησης κάνουν διαγνώσεις και προβλέπουν τα θέματα συντήρησης που εκκρεμούν , τα βραχυπρόθεσμα stock out των αποθεμάτων διαχειρίζονται ευκολότερα και ταχύτερα, και μπορούν να θέτουν ακόμα και τις προτεραιότητες στα προγράμματα του προσωπικού που είναι υπεύθυνο για τις επισκευές, για να καλύψουν αποτελεσματικότερα τόσο τις ανάγκες επισκευών του εξοπλισμού αλλά και τις περιφερειακές ανάγκες.

δ) Τα data driven συστήματα, στη βάση των υποδομών των «έξυπνων πόλεων» καθιστούν ευκολότερο για τους δήμους να υλοποιούν αποτελεσματικά προγράμματα για τους δημότες τους, όπως τις διαδικασίες διαχείρισης αποθεμάτων, διαχείρισης αποβλήτων, διαχείρισης θέσεων στάθμευσης, την επιβολή του νόμου και άλλα εξ' ίσου σημαντικά προγράμματα.

Ο τρόπος με τον οποίο οι κατασκευαστές προϊόντων χρησιμοποιούν τα δεδομένα των αισθητήρων της τεχνολογίας Internet of Things αφόρα κυρίως την παρακολούθηση της απόδοσης προϊόντος, την επισκευή και συντήρηση προϊόντος, την κατανόηση της καλύτερης χρήσης προϊόντος, τις επικαιροποιήσεις των συστημάτων διάθεσης και παράδοσης προϊόντων, την ανίχνευση πληροφοριών για διαφαινόμενες νέες ευκαιρίες, την υποστήριξη των πωλήσεων των προϊόντων και την προώθηση της ανταγωνιστικότητας και της επιχειρηματικότητας.

Οι παράγοντες παρουσιάζονται στο παρακάτω σχήμα με την αντίστοιχη κλιμάκωση των ποσοστών ενός εκάστου



Σχήμα 1.4 Η χρήση των δεδομένων των αισθητήρων της τεχνολογίας IoT

Η χρήση των δεδομένων Internet of Things θα μπορούσε να βελτιώσει το επενδυτικό περιβάλλον, δημιουργώντας προϋποθέσεις ανάπτυξης των εταιριών και κατ' επέκταση οικονομικής μεγέθυνσης των χωρών. Σύμφωνα με μελέτες που πραγματοποιήθηκαν για λογαριασμό κατασκευαστών, τα IoT δεδομένα θα μπορούσαν

να χρησιμοποιηθούν περισσότερο στρατηγικά και άρα περισσότερο αποτελεσματικά εάν οι οργανισμοί και οι εταιρίες διέθεταν:

Σχήμα 1.5 Προϋποθέσεις βέλτιστης χρήσης των IoT data

Τα ποσοστά σημαντικότητας της κάθε προϋπόθεσης βέλτιστης αξιοποίησης των δεδομένων είναι τα αναγραφόμενα παραπάνω.

Έρευνα του **Internet of Things Barometer** που πραγματοποιήθηκε σε δέκα τρείς (13) χώρες (ΗΠΑ, Βραζιλία, Ιρλανδία, Ηνωμένο Βασίλειο, Γερμανία, Ιταλία, Ισπανία, Νότια Αφρική, Κίνα, Ινδία, Ιαπωνία, Αυστραλία και Νέα Ζηλανδία) το έτος 2017, ανάμεσα σε χίλια τριακόσια (1300) στελέχη επιχειρήσεων, κατέδειξε πως από τις επιχειρήσεις που υιοθέτησαν λύσεις IoT :

- Το 84% ανέφερε ότι η αξιοποίηση του IoT ενισχύθηκε σε σχέση με το προηγούμενο έτος.
- Το 51% θεωρεί ότι η συγκεκριμένη τεχνολογία αυξάνει τα έσοδά τους ή δημιουργεί νέες πηγές εσόδων
- Το 66% των εταιριών συμφωνεί ότι ο ψηφιακός μετασχηματισμός είναι αδύνατος χωρίς το IoT.
- Το 67% των χρηστών μεγάλης κλίμακας επισημαίνουν ότι έχουν αξιόλογες αποδόσεις από την χρήση του IoT.
- Το 53% όσων απάντησαν από την περιοχή Ασίας – Ειρηνικού, ανέφεραν ως το κορυφαίο πλεονέκτημα του IoT, την αυξημένη ανταγωνιστικότητα που προκαλεί στην αγορά, έναντι ποσοστών 35% στην Αμερικανική ήπειρο και 33% στην Ευρώπη.

- Το 51% των εταιριών αυτοκινητοβιομηχανίας υπογράμμισαν ότι το IoT τις βοηθά να διαφοροποιηθούν ενισχύοντας την εμπορική τους μάρκα.
- Το 7% αναφέρει ότι προβληματίζεται από τα θέματα ασφάλειας στην υιοθέτηση της τεχνολογίας του Διαδικτύου των Αντικειμένων.

Στην ίδια έρευνα καταγράφεται ότι σε διεθνές επίπεδο, το ποσοστό των εταιριών που διαθέτουν περισσότερες από πενήντα χιλιάδες (50000) διασυνδεδεμένες συσκευές, διπλασιάστηκε κατά τους τελευταίους 12 μήνες. Στην πρώτη γραμμή των μεγαλύτερων έργων IoT διεθνώς, βρίσκονται οι εταιρίες ενέργειας και οι επιχειρήσεις κοινής ωφέλειας, με εφαρμογές όπως η «έξυπνη» μέτρηση (smart metering) και η παρακολούθηση της λειτουργίας αγωγών (pipeline monitoring). το εύρος των πλεονεκτημάτων από την χρήση του IoT μεγαλώνει όσο διευρύνεται η υιοθέτησή του. Η έκθεση επισημαίνει ότι όσο αυξάνεται η κλίμακα των έργων IoT παρατηρείται άνοδος των απαιτήσεων διασύνδεσης.

Στο σχεδιασμό των εταιριών εντάσσεται η χρησιμοποίηση ενός μείγματος τεχνολογιών από σταθερές ευρυζωνικές γραμμές έως χαμηλής ενεργειακής κατανάλωσης ευρυζωνικά δίκτυα (LP-WAN), αναλόγως των εφαρμογών IoT που αξιοποιούν. Στα έργα μεγάλης κλίμακας χρησιμοποιούνται κατά βάση τέσσερις (4) διαφορετικές επιλογές διασύνδεσης, με τις ασύρματες επικοινωνίες και το Wi-Fi να είναι οι πιο δημοφιλείς από αυτές. Αυξημένο ενδιαφέρον υπάρχει και για τις νεότερες τεχνολογίες όπως είναι το Narrowband IoT, με το 28% των εταιριών να το εξετάζουν, παράλληλα με άλλα χαμηλής ενεργειακής κατανάλωσης ευρυζωνικά δίκτυα (LP-WAN) για να υποστηρίξουν νέα έργα IoT.

Η σημαντικότητα του Internet of Things πέρα από τον κόσμο των κρατικών και μη κρατικών δρώντων, των επιχειρήσεων και της μαζικής αγοράς, επεκτείνεται και στο ατομικό επίπεδο του κάθε ενός. Μπορούμε να υποθέσουμε για παράδειγμα πως μας έχει τελειώσει το γάλα στο σπίτι. Καθώς επιστρέφουμε από τη δουλειά, λαμβάνουμε μία αυτόματη ειδοποίηση στο κινητό από το ψυγείο μας, που μας υπενθυμίζει να σταματήσουμε σε ένα κατάστημα για γάλα. Ένα άλλο παράδειγμα που καταδεικνύει τη σημαντικότητα του Internet of Things στο ατομικό επίπεδο, μπορεί να αφορά το σύστημα ασφάλειας στο σπίτι, που ενεργοποιείται, απενεργοποιείται και γενικά παρακολουθείται από απόσταση μέσω του κινητού, tablet ή υπολογιστή. Ένα τέτοιο σύστημα παρέχει τον έλεγχο από απόσταση των κλειδαριών ή του συναγερμού. Με

αντίστοιχο τρόπο μπορούμε να μετράμε τα ενεργειακά δεδομένα, μπορούν να ρυθμίζονται οι θερμοστάτες, τα κλιματιστικά, ο φωτισμός του σπιτιού, το άνοιγμα των παραθύρων, οι ηλεκτρικές συσκευές, το πότισμα του κήπου, και άλλα πολλά.

Σχήμα 1.6 Σημαντικότητα του Internet of Things στο ατομικό επίπεδο

Τις προκλήσεις της νέας αυτής τεχνολογίας αναγνωρίζει και το **Ευρωπαϊκό Κοινοβούλιο** (ΕΚ) μέσω της Έκθεσής του σχετικά με το «Διαδίκτυο των Αντικειμένων». Η Έκθεση, που συντάχθηκε από την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας του ΕΚ, αποσκοπεί στη δημιουργία ενός κανονιστικού και νομικού πλαισίου το οποίο αποβλέπει αφενός στην προστασία του Ευρωπαίου καταναλωτή και αφετέρου στην ενθάρρυνση των δημόσιων και ιδιωτικών επενδύσεων. Η Ευρωπαϊκή Επιτροπή έθεσε ως στόχο την αξιοποίηση των δυνατοτήτων του IoT προς όφελος των Ευρωπαίων πολιτών. Η Ανακοίνωση της ΕΕ προβλέπει την τυποποίηση των τεχνολογιών που χρησιμοποιούνται από το «Διαδίκτυο των Αντικειμένων», την αυξημένη χρηματοδότηση για σχετικά έργα Έρευνας, Τεχνολογικής Ανάπτυξης και Καινοτομίας και τη διασφάλιση της προστασίας των προσωπικών δεδομένων των πολιτών.

Πέραν των σημαντικών βελτιώσεων σε συλλογικό και ατομικό επίπεδο που προσφέρει η εισαγωγή και η εφαρμογή του Internet of Things, δεν πρέπει να μας διαφύγει το γεγονός πως μια μικροσκοπική ετικέτα RFID σε κάθε προϊόν που αγοράζουμε, μπορεί να αποκαλύψει, αν συνδυαστεί και με άλλα δεδομένα, σημαντικές

πληροφορίες για τις καταναλωτικές και κοινωνικές μας συνήθειες. Παράλληλα η ταχεία διάδοση της τεχνολογίας του «Διαδικτύου των Αντικειμένων» θέτει νέες προκλήσεις για το νομικό μας σύστημα και αφήνει ανοιχτά ηθικά ερωτήματα για τα όρια της τεχνολογίας, όπως τον βαθμό της ιδιωτικότητας που είμαστε διατεθειμένοι ως κοινωνία να θυσιάσουμε, προκειμένου να επιτύχουμε μεγαλύτερη ασφάλεια, οικονομία ή ευκολία στη καθημερινότητά μας.

1.3 ΤΕΧΝΟΛΟΓΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΗΚΑ ΤΩΝ "Ι ο Τ" ΕΦΑΡΜΟΓΩΝ

Οι εφαρμογές IoT περιγράφουν ενσύρματα ή ασύρματα «έξυπνα» δίκτυα. Τα δίκτυα αυτά αποτελούνται από κόμβους (μικροσυσκευές) που συνδέονται μεταξύ τους με τη χρήση τεχνολογιών επικοινωνίας χαμηλού κόστους. Ως παράδειγμα αναφέρεται το δίκτυο Wireless Sensor Network – WSN.

Τα δίκτυα αυτά εκτός του ότι λειτουργούν αυτόνομα, παρέχουν τη δυνατότητα της αμφίδρομής επικοινωνίας μέσω του Παγκόσμιου Ιστού, ανθρώπου – συσκευής. Στις εφαρμογές IoT η πιο δημοφιλής χρησιμοποιούμενη αρχιτεκτονική είναι η Representational State Transfer – REST, η οποία είναι προσβάσιμη από τον Παγκόσμιο Ιστό. Οι χρήστες του συστήματος μέσω αυτής χρησιμοποιώντας Universal Resource Identifier (URI) για τον εκάστοτε πόρο, αποκτούσαν απευθείας πρόσβαση στην εκάστοτε συσκευή και τις επιμέρους διεπαφές. Η πρόσβαση αυτή δεν περιλαμβάνει μόνο προβολή των δεδομένων, αλλά και μεταβολή ή διαγραφή αυτών.

Με τη χρήση resources επιτυγχάνεται η επαναχρησιμοποίηση του κώδικα και η σημαντική μείωση της πολυπλοκότητας της εφαρμογής. Τα δεδομένα των resources είναι σε διάφορες μορφές, όπως XML, JSON, text, HTML. Ενδιαφέρον παρουσιάζουν τα resources που καταναλώνουν σημαντικό υπολογιστικό χρόνο, κάθε φορά που καλούνται. Αυτό είναι κάτι που αντιβαίνει στον τρόπο με τον οποίο λειτουργεί μια εφαρμογή IoT, στην οποία οι κύκλοι κλήσης-εκτέλεσης είναι σύντομοι. Ωστόσο υπάρχουν αρκετές εφαρμογές για τις οποίες αυτό είναι αναπόφευκτο. Υπάρχουν μικροσυσκευές που λειτουργούν με μπαταρίες, επομένως η χρήση τέτοιου είδους resources πρόκειται να επηρεάσει παράγοντες όπως η ενεργειακή κατανάλωση μιας μικροσυσκευής.

Οι εφαρμογές IoT μπορούν να βοηθήσουν τόσο στην επίλυση προβλημάτων που αφορούν τη βιομηχανία (πχ τηλεδιαχείριση βιομηχανικού εξοπλισμού), όσο και

την απλή καθημερινότητα των ανθρώπων (πχ ενεργοποίηση οικιακών συσκευών από απόσταση).

Η αναγκαιότητα ενσωμάτωσης σύγχρονων λειτουργικών συστημάτων σε κάθε μικροσυσκευή είναι ανεξάρτητη από τη φύση της IoT εφαρμογής. Οι λόγοι είναι ότι με τη χρήση σύγχρονων λειτουργικών συστημάτων:

1. Επιτυγχάνεται η μέγιστη εκμετάλλευση των διαθέσιμων πόρων μνήμης και επεξεργαστή.

2. Διασφαλίζεται η αξιοπιστία γενικά, ακόμα και στις περιπτώσεις σφαλμάτων.

3. Ο προγραμματιστής του συστήματος υλοποιεί εφαρμογές σε υψηλό επίπεδο με τη χρήση έτοιμων συναρτήσεων των λειτουργικών συστημάτων που επιτελούν σύνθετες λειτουργίες (πχ διαχείριση συμβάντων και διεργασιών).

4. Τα σύγχρονα λειτουργικά συστημάτα παρέχουν έτοιμα network stack (όπως το TCP/IP), απαλλάσσοντας τον προγραμματιστή από την υλοποίηση custom network stack.

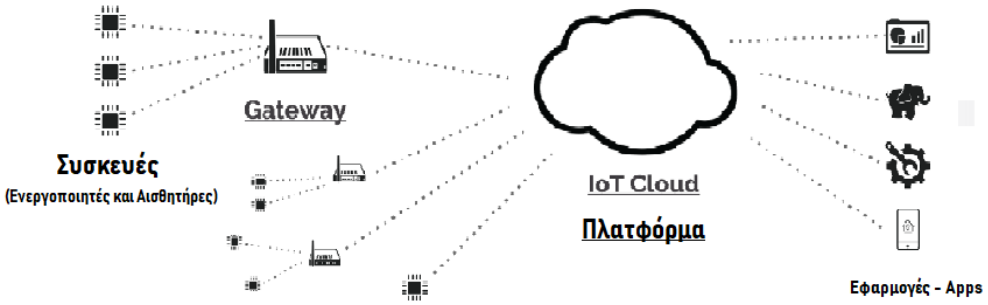
2. Υποδείγματα ενοποίησης στο IoT

2.1 ΕΙΣΑΓΩΓΗ

Η συνδεσιμότητα που επιτελείται στα πλαίσια του Internet of Things ώστε να οδηγεί στην αποτελεσματική επικοινωνία, στην επαύξηση των υπολογιστικών δυνατοτήτων των συσκευών, στην αλληλεπίδραση και την επικοινωνία με άλλες συσκευές, αντικείμενα, περιβάλλοντα, υποδομές και τελικά οδηγεί στη παραγωγή και μεταφορά δεδομένων, συντελείται με διάφορους τρόπους. Οι κύριες μεθοδολογίες (μοντέλα) διασύνδεσης και η φιλοσοφία τους αποτυπώνονται στο παρόν Κεφάλαιο.

Η κατάλληλη συνδεσιμότητα μπορεί να προσδώσει μεγάλη αξία και πολλές δυνατότητες στις εφαρμογές των ενσωματωμένων συστημάτων. Στα βιομηχανικά συστήματα παραγωγής και γενικά στην οικονομική δραστηριότητα βελτιώνει την αξιοπιστία και την παραγωγικότητα, ενώ στις πιο απλές περιπτώσεις της ανθρώπινης καθημερινότητας αποδεικνύεται σημαντικά χρηστική.

Η διασύνδεση των συσκευών και η επέκταση της συνδεσιμότητας από ένα στενό σε ένα ευρύτερο πλαίσιο, όπως για παράδειγμα από το τοπικό LAN στο ευρύ WAN, αποτελούν το καθοριστικό στοιχείο της συγκρότησης του Διαδικτύου των Αντικειμένων, μια τυπική τοπολογία του οποίου δίνεται στο σχήμα που ακολουθεί.



Σχήμα 2.1. Απεικόνιση τυπικής τοπολογίας Internet of Things

Σχεδιαστικά τη μεγαλύτερη πρόκληση για IoT συσκευή αποτελεί η υλοποίηση μιας ισχυρής και ασφαλούς πρόσβασης στο WAN ή στο Διαδίκτυο. Εδώ βέβαια υπεισέρχεται δυναμικά και ο παράγοντας κόστος υλοποίησης. Για παράδειγμα, η απευθείας διασύνδεση ενός αισθητήρα θερμοκρασίας με WiFi ή Ethernet στο Διαδίκτυο είναι αρκετά δαπανηρή, ενώ το κόστος διευρύνεται, όσο μεγαλώνει ο αριθμός των αισθητήρων που πρέπει να συνδεθούν. Ωστόσο η διαρκής μείωση του κόστους των WiFi και Ethernet και η ωριμότητα των πρωτοκόλλων τους, εκτιμάται πως θα συντελέσουν στην αύξηση των συνδέσεων.

2.2.1 Επικοινωνία συσκευής προς συσκευή (device-to-device)

Η επικοινωνία συσκευής προς συσκευή αντιπροσωπεύει την περίπτωση όπου δύο ή περισσότερες συσκευές συνδέονται άμεσα και επικοινωνούν μεταξύ τους. Οι συσκευές μπορούν να επικοινωνούν σε πολλούς τύπους δικτύων, συμπεριλαμβανομένων του Διαδικτύου και των δικτύων IP, συχνότερα όμως χρησιμοποιούν πρωτόκολλα όπως τα Bluetooth, Z-Wave και ZigBee.

Σχήμα 2.2. Device to Device επικοινωνία

Το μοντέλο αυτό επικοινωνίας χρησιμοποιείται συνήθως στα συστήματα οικιακού αυτοματισμού, για τη μεταφορά ενός σχετικά μικρού «πακέτου» πληροφοριών μεταξύ των συσκευών, με χαμηλό ρυθμό μετάδοσης δεδομένων. Τέτοιες συσκευές μπορεί να είναι ηλεκτρικοί λαμπτήρες, θερμοστάτες, κλειδαριές θυρών, που μεταβιβάζουν η μία στην άλλη μικρές ποσότητες πληροφοριών. Κάθε μοντέλο συνδεσιμότητας έχει διαφορετικά χαρακτηριστικά, υποστηρίζει ο Tschofenig, με την επικοινωνία Device to Device *«η ασφάλεια απλοποιείται ειδικά επειδή υφίσταται η τεχνολογία υψηλών συχνοτήτων* (radio technology) *και μικρής εμβέλειας* [καθώς και μια] *σχέση ενός προς ένα, μεταξύ αυτών των δύο συσκευών»*.

Το υπόδειγμα επικοινωνίας «συσκευή προς συσκευή» είναι ιδιαίτερα δημοφιλές στην περίπτωση των φορητών wearable συσκευών IoT, όπως για

παράδειγμα αυτές που παρακολουθούν και καταγράφουν τους καρδιακούς παλμούς σε συνδυασμό με ένα smart watch, όπου τα δεδομένα δεν είναι απαραίτητο να διαμοιράζονται σε πολλούς ανθρώπους.

Υπάρχουν αρκετά πρότυπα που αναπτύσσονται γύρω από το Device to Device, όπως είναι το Bluetooth Low Energy (επίσης γνωστό και ως Bluetooth Smart ή Bluetooth Version 4.0+) το οποίο είναι δημοφιλές μεταξύ των φορητών και των wearable φορητών συσκευών, επειδή οι χαμηλές απαιτήσεις του για ισχύ, σημαίνουν ότι οι συσκευές μπορούν να λειτουργούν για μήνες ή χρόνια, με μία απλή μπαταρία. Πρόσθετο θετικό στοιχείο αποτελεί και η μικρότερη πολυπλοκότητά του, που μπορεί να μειώσει το μέγεθος και το κόστος του.

2.2.2 Επικοινωνία συσκευής προς cloud (device-to-cloud)

Η επικοινωνία συσκευής προς Cloud περιλαμβάνει τη σύνδεση μιας συσκευής IoT απευθείας με μια διαδικτυακή υπηρεσία Cloud, όπως ένας πάροχος υπηρεσιών internet εφαρμογών, κατά την ανταλλαγή δεδομένων και τον έλεγχο μηνυμάτων. Η διασύνδεση αυτή συχνά χρησιμοποιεί παραδοσιακές ενσύρματες συνδέσεις όπως το Ethernet ή το Wi-Fi, αλλά κάλλιστα μπορεί επίσης να χρησιμοποιεί την κυψελοειδή τεχνολογία. Η συνδεσιμότητα Cloud επιτρέπει στον χρήστη (και σε μια εφαρμογή) να αποκτήσει απομακρυσμένη πρόσβαση σε μια συσκευή, ενώ ενδέχεται επίσης να υποστηρίζει την προώθηση επικαιροποιήσεων (ενημερώσεων) του λογισμικού στη συσκευή.

Μια περίπτωση χρήσης επικοινωνίας device-to-cloud βασισμένη στη κυψελοειδή τεχνολογία, θα μπορούσε να είναι μια έξυπνη ετικέτα που παρακολουθεί το κατοικίδιο ζώο μας ενώ εμείς δεν είμαστε κοντά. Η επιτυχία της ανίχνευσης του κατοικίδιου απαιτεί επικοινωνία κυψελοειδούς τεχνολογίας που να καλύπτει μια ευρεία περιοχή και αυτό γιατί δεν θα μπορούσαμε να γνωρίζουμε την ακριβή θέση του ζώου. Ένα άλλο σενάριο, αναφέρει ο Tschofenig, θα μπορούσε να είναι η απομεμακρυσμένη παρακολούθηση με ένα προϊόν όπως το Dropcam, όπου χρειαζόμαστε το εύρος ζώνης που παρέχεται από το WiFi ή το Ethernet. Στην περίπτωση αυτή πρέπει να μεταφέρουμε τα δεδομένα στο Cloud και αυτό έχει νόημα επειδή παρέχει πρόσβαση στο χρήστη όταν αυτός είναι μακριά. Έτσι αν ο χρήστης που βρίσκεται μακριά θελήσει

να δει τι παίζει στην κάμερα που βρίσκεται στο σπίτι του, επικοινωνεί με την υποδομή του Cloud. Σαν αποτέλεσμα της επικοινωνίας αυτής, η εικόνα της κάμερας αναμεταδίδεται από την υποδομή του Cloud στην IoT συσκευή του χρήστη.

Σχήμα 2.3. Device to Cloud επικοινωνία

Από την άποψη ασφάλειας, το ζήτημα εδώ είναι πιο περίπλοκο από ότι στην περίπτωση επικοινωνίας τύπου Device to Device, επειδή περιλαμβάνει δύο διαφορετικούς τύπους διαπιστευτηρίων, τα διαπιστευτήρια πρόσβασης στο δίκτυο (όπως η κάρτα SIM της κινητής τηλεφωνικής συσκευής) και, στη συνέχεια, τα διαπιστευτήρια πρόσβασης στο Cloud. Επιπλέον έκθεση της IAB αναφέρει ότι η διαλειτουργικότητα είναι ένα ζήτημα στην περίπτωση επικοινωνίας τύπου Device-to-Cloud όταν γίνεται προσπάθεια να ενοποιηθούν συσκευές που φτιάχνονται από διαφορετικούς κατασκευαστές δεδομένου ότι η συσκευή και η υπηρεσία cloud είναι συνήθως από τον ίδιο πωλητή.

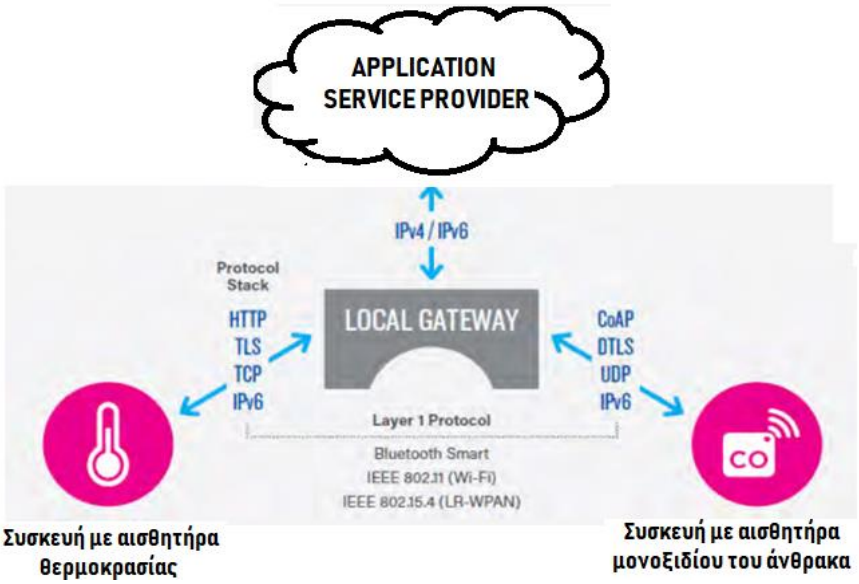
Ο Tschofenig δήλωσε πως έχει συντελεστεί πρόοδος στην κατασκευή συσκευών Wi-Fi που κάνουν Cloud συνδέσεις, ενώ καταναλώνουν λιγότερη ενέργεια με πρότυπα όπως τα LoRa, Sigfox και Narrowb.

2.2.3 Επικοινωνία συσκευής προς Πύλη (device-to-gateway)

Στο μοντέλο επικοινωνίας Device-to-Gateway, οι συσκευές IoT συνδέονται βασικά με μια ενδιάμεση συσκευή για να αποκτούν πρόσβαση στην υπηρεσία Cloud. Αυτό το μοντέλο συχνά περιλαμβάνει λογισμικό εφαρμογών (application software) που λειτουργεί σε μια τοπική gateway συσκευή (όπως ένα smartphone ή ένας διανομέας "hub"), η οποία έχει το ρόλο του ενδιάμεσου, μεταξύ μιας συσκευής IoT και μιας υπηρεσίας Cloud. Αυτή η πύλη (gateway) θα μπορούσε να παρέχει ασφάλεια, καθώς επίσης και άλλες λειτουργίες, όπως δεδομένα ή μετάφραση πρωτοκόλλου.

Αν το application-layer gateway είναι ένα έξυπνο τηλέφωνο, αυτό το λογισμικό μπορεί να λάβει τη μορφή μιας εφαρμογής που ως ζευγάρι με την IoT συσκευή, επικοινωνεί με μια υπηρεσία Cloud. Αυτό θα μπορούσε να είναι μια συσκευή φυσικής κατάστασης που συνδέεται με το Cloud μέσω μιας εφαρμογής smartphone ή θα μπορούσαν να είναι εφαρμογές αυτοματισμού για το σπίτι, που περιλαμβάνουν συσκευές συνδεδεμένες σε ένα διανομέα (hub).

Οι συσκευές gateway μπορούν επίσης να γεφυρώσουν το χάσμα διαλειτουργικότητας μεταξύ συσκευών που επικοινωνούν με διαφορετικά πρότυπα. Ως παράδειγμα μπορούμε να αναφέρουμε τους πομποδέκτες Z-Wave και Zigbee της «SmartThings» που έχουν τη δυνατότητα να επικοινωνούν και με τις δύο «οικογένειες» συσκευών.



Σχήμα 2.4 Device to Gateway επικοινωνία

Από το παραπάνω σχήμα καθίσταται εμφανές πως η διαφορά στο μοντέλο επικοινωνίας που περιγράφει (Device to Gateway), σε σχέση με το προηγούμενο μοντέλο Device to Cloud, βρίσκεται στην ενδιάμεση συσκευή, την παρεμβολή της τοπικής gateway συσκευής.

Σημειώνεται ότι η διαφορά μεταξύ ενός IoT Gateway και ενός IP Router έγκειται στο γεγονός ότι ο μεν IP Router διασυνδέει συσκευές που μοιράζονται μια κοινή διεπαφή και διαχειρίζεται όμοια κίνηση πακέτων (παράδειγμα αποτελούν οι συσκευές που συνδέονται μέσω WiFi ή Ethernet και χρησιμοποιούν IP πρωτόκολλο), ο δε IoT Gateway από την άλλη μεριά, λειτουργεί ως μια πύλη που γεφυρώνει πρωτόκολλα και διεπαφές. Έτσι συλλέγει δεδομένα (data) από διάφορες διεπαφές επικοινωνίας, προωθεί ποικίλους τύπους κίνησης και μετατρέπει τις ροές δεδομένων (data streams) σε κοινό πρωτόκολλο. Έτσι επιτυγχάνεται η πρόσβαση δια μέσου του WAN.

Κάποιες από τις συσκευές που συνδέονται δια ενός IoT Gateway είναι δυνατόν να χρησιμοποιούν IP, ενώ άλλες, πρωτόκολλα που βασίζονται σε PAN, όπως για παράδειγμα τα Bleutooth, ZigBee και 61ο WPAN. Ορισμένες από τις συσκευές που είναι απλοί αισθητήρες μπορεί να απαιτείται να συνδεθούν σε είσοδο ADC έτσι ώστε το ανεπεξέργαστο αναλογικό τους σήμα να ψηφιοποιείται πριν μεταφερθεί στο IoT Cloud. Στην υλοποίηση ενός IoT Gateway διακρίνουμε δύο προσεγγίσεις. Αυτή του απλού IoT Gateway, με κόστος υλοποίησης που βαρύνει τα nodes και αυτή του IoT Gateway με ενσωματωμένο έλεγχο, που παρέχει επεξεργαστικούς πόρους και εφαρμογές λογισμικού. Στην περίπτωση αυτή το κόστος επιβαρύνει τον IoT Gateway.

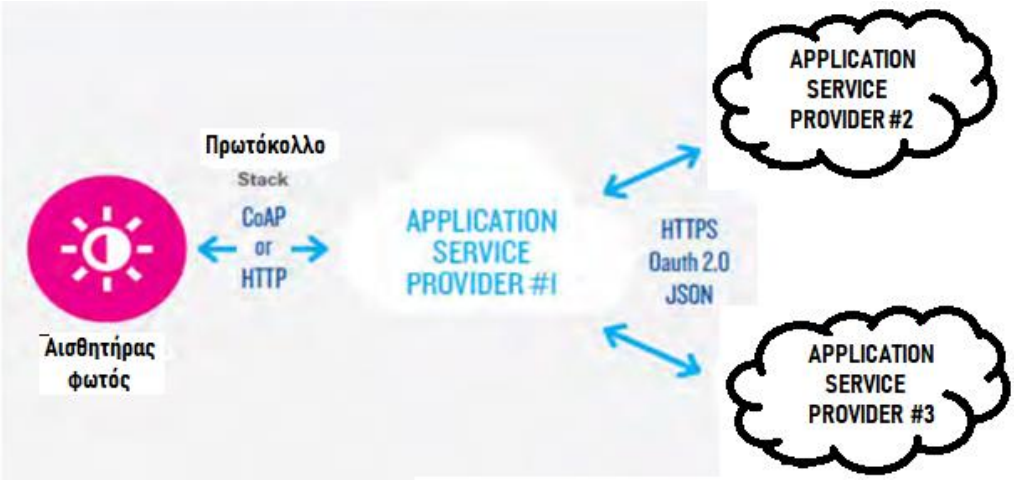
2.2.4 Back-End Data-Sharing Model

Το υπόδειγμα Back-End Data-Sharing ουσιαστικά επεκτείνει το μοντέλο επικοινωνίας μιας συσκευής προς Cloud (Single Device-to-Cloud), έτσι ώστε τόσο στις συσκευές IoT όσο και στα δεδομένα των αισθητήρων να μπορούν να αποκτούν πρόσβαση εξουσιοδοτημένα τρίτα μέρη. Σύμφωνα με αυτό το μοντέλο, οι χρήστες μπορούν να εξάγουν και να αναλύουν δεδομένα έξυπνων συσκευών από μια υπηρεσία Cloud, σε συνδυασμό με δεδομένα που συλλέγονται από άλλες πηγές και στη συνέχεια να τα στέλνουν σε κάποιες άλλες υπηρεσίες για συγκέντρωση και ανάλυση.

Αυτή η προσέγγιση είναι μια επέκταση του μοντέλου επικοινωνίας Single Device-to-Cloud, η οποία μπορεί να οδηγήσει στη δημιουργία σιλό δεδομένων όπου οι συσκευές IoT μεταφέρουν τα δεδομένα μόνο σε έναν πάροχο ενιαίων υπηρεσιών εφαρμογών.

Μια αρχιτεκτονική Back-End Data-Sharing επιτρέπει όπως τα δεδομένα που συλλέγονται από τις ροές data μιας συσκευής IoT, να συγκεντρώνονται και να αναλύονται. Έτσι για παράδειγμα, ένας εταιρικός χρήστης που είναι υπεύθυνος σε ένα συγκρότημα γραφείων θα μπορούσε να ενδιαφέρεται, να ενοποιήσει και να αναλύσει τα δεδομένα κατανάλωσης ενέργειας και υπηρεσιών κοινής ωφέλειας, τα οποία παράγονται από όλους τους αισθητήρες IoT και τα διαδικτυακά βοηθητικά συστήματα, που λειτουργούν στις εγκαταστάσεις.

Συχνά στο μοντέλο Single Device-to-Cloud τα δεδομένα που κάθε αισθητήρας ή σύστημα IoT παράγουν, «κάθονται» σε ένα αυτόνομο σιλό δεδομένων.



Σχήμα 2.5 Υπόδειγμα Back-End Data-Sharing

Μια αποτελεσματική αρχιτεκτονική Back-End Data-Sharing θα επέτρεπε στην εταιρεία να έχει εύκολη πρόσβαση και να αναλύει τα δεδομένα στο Cloud, που παράγονται από όλο το φάσμα των συσκευών του κτιρίου. Επίσης, αυτό το είδος αρχιτεκτονικής διευκολύνει τις ανάγκες φορητότητας των δεδομένων (data portability needs). Αποτελεσματικές αρχιτεκτονικές του τύπου Back-End Data-Sharing επιτρέπουν στους χρήστες να μετακινούν τα δεδομένα τους, όταν μετακινούνται μεταξύ IoT υπηρεσιών, αίροντας τα παραδοσιακά εμπόδια του σιλό δεδομένων.

Το υπόδειγμα Back-End Data-Sharing προτείνει μια προσέγγιση ενοποιημένων υπηρεσιών Cloud. Οι διεπαφές προγραμματισμού εφαρμογών Cloud (Applications Programming Interfaces-APIs) είναι απαραίτητες για την επίτευξη της διαλειτουργικότητας των δεδομένων, των έξυπνων συσκευών, που φιλοξενούνται στο Cloud.

.

2.2.5 Πρωτόκολλα IPV4, IPV6 στο Internet of Things

Το 1983 αναπτύχθηκε το πρωτόκολλο IPv4 (Internet Protocol version 4), σήμερα παρά το γεγονός ότι θεωρείται ξεπερασμένο από άλλες διευθύνσεις IP, εξακολουθεί ακόμη να κατευθύνει τις περισσότερες διαδικτυακές υπηρεσίες. Για τις επιχειρήσεις που επιθυμούν να αξιοποιήσουν το Διαδίκτυο των Πραγμάτων, η κατανόηση της διαφοράς μεταξύ του IPv4 και του διαδόχου του, του IPv6 και η αναγνώριση του τρόπου με τον οποίο τα πρωτόκολλα αυτά μπορούν να τις επηρεάσουν - συμπεριλαμβανομένης της ασφάλειας του κυβερνοχώρου - είναι κρίσιμη.

Σύμφωνα με το NJIT (Ινστιτούτο Τεχνολογίας του Νιου Τζέρσεϋ), το IPv4 είναι ένα *«πρωτόκολλο χωρίς σύνδεση που χρησιμοποιείται σε δίκτυα μεταβλητών πακέτων»*, το οποίο παρέχει τη λογική σύνδεση μεταξύ των συσκευών δικτύου εντοπίζοντας κάθε μια συσκευή. Επειδή οι διευθύνσεις IPv4 έχουν μήκος 32 bits μόνο, η χωρητικότητα του συγκεκριμένου πρωτοκόλλου ήταν πάντα εγγενώς περιορισμένη σε σχεδόν 4,3 δισεκατομμύρια μοναδικούς συνδυασμούς. Αυτό το όριο έχει επιτευχθεί, σύμφωνα με την ARIN (American Registry for Internet Numbers), η οποία ανακοίνωσε τον Σεπτέμβριο του 2015 ότι η ομάδα δωρεάν διευθύνσεων IPv4 είχε μειωθεί στο μηδέν.

Το πρωτόκολλο IPv6, αποτελεί την ενημερωμένη και βελτιωμένη έκδοση του IPv4. Οι βελτιώσεις αφορούν ότι πρώτα απ 'όλα, το IPv6 μπορεί να υποστηρίξει σημαντικά περισσότερους κόμβους από το IPv4 επειδή οι διευθύνσεις του έχουν μήκος 128 bits. Ως εκ τούτου, αντί να περιορίζεται σε 4,3 δισεκατομμύρια διευθύνσεις IP, η χωρητικότητα του IPv6 είναι - για όλους τους πρακτικούς σκοπούς - σχεδόν απεριόριστη. Λαμβάνοντας υπόψη το γεγονός ότι το IoT αναπτύσσεται έντονα, με πολλά δισεκατομμύρια «Things» να αναμένεται να συνδεθούν σε σύντομο χρόνο και ότι κάθε συσκευή που συνδέεται με το Διαδίκτυο απαιτεί τουλάχιστον μία διεύθυνση IP, η εκθετικά αυξημένη χωρητικότητα του IPv6 πρέπει να θεωρείται κρίσιμη για την υποστήριξη των αυξανόμενων συνδέσεων. Τα τρία δυνατά σημεία του πρωτοκόλλου IPv6 για το Internet of Things είναι η ασφάλεια (Security), η ευελιξία (Scalability) και η συνδεσιμότητα (Connectability).

Επιπρόσθετα, το IPv4 σχεδιάστηκε σε μια εποχή πριν να προβλεφθούν οι απειλές του κυβερνοχώρου του σημερινού συνδεδεμένου κόσμου. Ως αποτέλεσμα, το

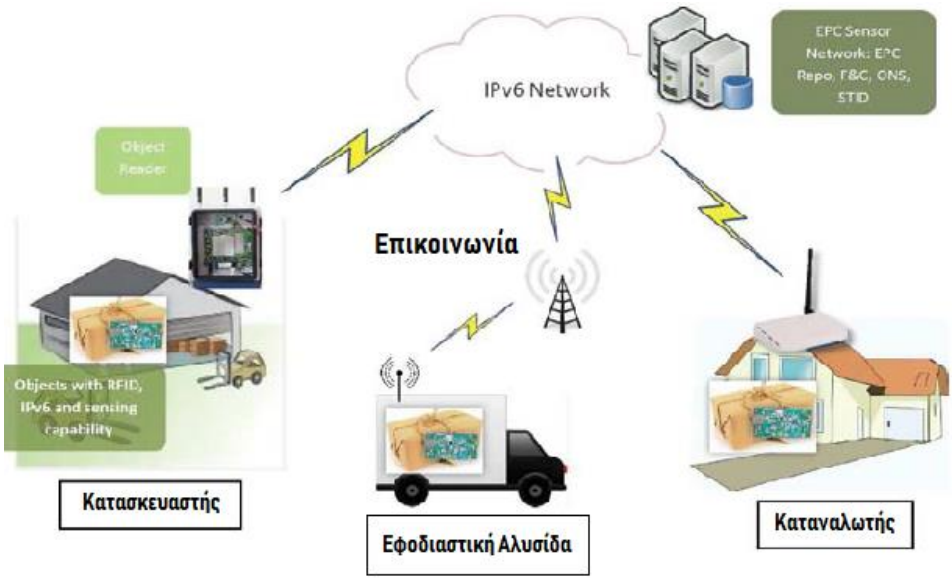
IPv6 προσφέρει καλύτερες λύσεις ασφάλειας για τις επιχειρήσεις που χειρίζονται ευαίσθητα δεδομένα που απλά δεν έχουν την οικονομική δυνατότητα να διακινδυνεύσουν μια παραβίαση ή το χρόνο διακοπής που προκύπτει από ένα «hack».

Υπάρχουν εμπόδια για τις επιχειρήσεις που θέλουν να εφαρμόσουν το IPv6, συμπεριλαμβανομένης της πολυπλοκότητας των αναβαθμίσεων των υποδομών και του εξοπλισμού. Ωστόσο, η ασυμβατότητα του IPv4 με το νεότερο πρωτόκολλο μπορεί να κοστίσει χρόνο και χρήμα. Παρόλο ότι η μετάβαση στο IPv6 δεν πραγματοποιείται σε μια νύχτα και μπορεί να επιφέρει ταλαιπωρία για την αναβάθμιση, την αναμόρφωση και τη δοκιμή της υφιστάμενης υποδομής, το νεότερο πρωτόκολλο προσφέρει στις επιχειρήσεις την ευκαιρία που προσδοκούν για βελτίωση της αποτελεσματικότητας, καλύτερη διαλειτουργικότητα, περισσότερη ασφάλεια και τελικά αύξηση της διαρκείας του IoT.

Καθώς το Διαδίκτυο των Πραγμάτων συνεχίζει να αναπτύσσεται, οι ειδικοί υπολογίζουν πως ο συνολικός αριθμός συσκευών IoT μέχρι το 2025 θα φτάσει τα 100 δισεκατομμύρια. Υπό αυτή την προοπτική, οι συσκευές που απαιτούν πραγματική συνδεσιμότητα με το Διαδίκτυο δεν θα μπορούν να βασίζονται στο IPv4, το πρωτόκολλο που χρησιμοποιούν σήμερα οι περισσότερες υπηρεσίες Internet.

Η ενεργοποίηση μιας νέας τεχνολογίας αποτελεί τη βασική προϋπόθεση. Έτσι το προέκυψε το IPv6. Το IPv6 είναι μια μακρόπνοη και πολυαναμενόμενη αναβάθμιση του αρχικού πρωτότυπου πρωτοκόλλου του Internet (IP), το οποίο υποστηρίζει όλες τις επικοινωνίες σε αυτό. Το πρωτόκολλο IPv6 είναι απαραίτητο διότι το Διαδίκτυο εξαντλείται από πρωτότυπες διευθύνσεις IPv4. Επισημαίνεται πως το IPv4 μπορεί να υποστηρίξει 4,3 δισεκατομμύρια συνδεδεμένες συσκευές, αντίστοιχα το IPv6 με δύο (2) στις εκατόν είκοσι οκτώ (128) διευθύνσεις ισχύος, διαθέτει για όλες τις πρακτικές χρήσεις ανεξάντλητες δυνατότητες. Αυτό αντιπροσωπεύει περίπου 340 τρισεκατομμύρια διευθύνσεις, γεγονός που ικανοποιεί τη ζήτηση από τις εκτιμώμενες 100 δισεκατομμύρια συσκευές IoT που θα τεθούν σε λειτουργία στο εγγύς μέλλον (2025).

Ένα παράδειγμα σύνδεσης και επικοινωνίας με αναφορά στη διαχείριση προϊόντος, δίνεται παρακάτω. Το παράδειγμα περιγράφει μια κατάσταση σε αυστηρό έλεγχο.



Σχήμα 2.6 Αρχιτεκτονική διαχείρισης προϊόντων, Πρωτόκολλο IPv6

Στο σχήμα απεικονίζεται η διαδικασία παραγωγής ενός προϊόντος και η εφοδιαστική αλυσίδα που διέπεται από EPC Network, τα προϊόντα έχουν δυνατότητα ανίχνευσης και επικοινωνίας λόγω της ετικέτας RFID που φέρουν. Τα σύγχρονα δίκτυα EPC είναι σε θέση να σύλλαβου αντικείμενα σε πραγματικό χρόνο και ονομάζονται EPC Sensor Network EPCSN. Αξιοποιώντας οι κατασκευαστές την αρχιτεκτονική EPCSN μπορούν να διαχειριστούν με αυτοματοποιημένο τρόπο τον κύκλο ζωής των προϊόντων, τα δεδομένα που συλλέγονται μπορούν να χρησιμοποιηθούν σε big data αναλύσεις και οι τελικοί χρήστες να αντιληφθούν τις «έξυπνες» υπηρεσίες που τους παρέχονται.

Βασική πάντως πρόκληση για αυτούς που εξελίσσουν και αναπτύσσουν το Διαδικτύου είναι, ότι το IPv6 δεν είναι εγγενώς διαλειτουργικό με το IPv4 καθώς και τα περισσότερα λογισμικά χαμηλού κόστους που είναι διαθέσιμα για ενσωμάτωση σε συσκευές IoT που λειτουργούν μόνο στο IPv4. Οι περισσότεροι ειδικοί ωστόσο, πιστεύουν ότι το IPv6 είναι η καλύτερη επιλογή συνδεσιμότητας και θα επιτρέψει στο IoT να αξιοποιήσει τις δυνατότητές του

3. Αξιόπιστο και Ασφαλές Περιβάλλον Λειτουργίας

3.1 ΕΙΣΑΓΩΓΗ

Το αξιόπιστο και ασφαλές περιβάλλον σαν έννοια και ουσία αποτελεί το ζητούμενο σε όλους τους τομείς της ανθρώπινης δράσης και της ανθρωπογενούς δημιουργίας καθώς και τον ακρογωνιαίο λίθο κάθε επιστημονικής προσπάθειας. Εκφράζει τη δυνατότητα ενός συστήματος (ή μιας συσκευής) να εκτελεί την αποστολή του επαρκώς για σχεδιαζόμενη χρονική περίοδο και επικρατούσες λειτουργικές συνθήκες. Η συνέπεια ενός τέτοιου περιβάλλοντος απειλείται από παράγοντες όπως το σφάλμα, το τυχαίο, οι επικρατούσες συνθήκες, οι ασαφείς οδηγίες, η αστοχία και η αρνητική ανθρώπινη βούληση.

Στην έρευνα του **Internet of Things Barometer** που πραγματοποιήθηκε το 2017, επισημαίνεται πως το ζήτημα της **ασφάλειας** στο IoT παραμένει το μεγαλύτερο εμπόδιο για την υιοθέτησή του από τις επιχειρήσεις. Ωστόσο, από τα στελέχη εταιριών με 10.000 ή και περισσότερες διασυνδεδεμένες συσκευές σε λειτουργία, μόλις το 7% αναφέρει ότι τους προβληματίζει η ασφάλεια . Οι επιχειρήσεις κάνουν περισσότερα βήματα για την αντιμετώπιση των θεμάτων ασφαλείας, αναλαμβάνοντας πρωτοβουλίες όπως είναι η αύξηση της εκπαίδευσης γύρω από την ασφάλεια για το προσωπικό τους, η συνεργασία με εξειδικευμένους παρόχους ασφαλείας και η πρόσληψη περισσότερων ειδικών γύρω από την ασφάλεια των τεχνολογιών πληροφορικής.

Στόχο του παρόντος Κεφαλαίου αποτελεί η επισήμανση των θεμάτων αξιοπιστίας και ασφάλειας στο Internet of Things, καθώς και των σχετικών λύσεων.

3.2 ΟΙ ΣΤΟΧΟΙ ΤΗΣ ΑΞΙΟΠΙΣΤΙΑΣ ΚΑΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IoT

Ως αρχές ασφάλειας των υπολογιστικών συστημάτων και των δικτύων γενικά, έχουν καθοριστεί η Εμπιστευτικότητα (Confidentiality), η Ακεραιότητα (Integrity), η Διαθεσιμότητα (Availability), η Ιδιωτικότητα (Privacy), η Αυθεντικότητα (Authenticity) και η Μη Αποποίηση Ευθυνών (Non-Repudiation).

Η Αρχή της Εμπιστευτικότητας (Confidentiality) επιτάσσει όπως στην ευαίσθητη πληροφορία, πρόσβαση να αποκτούν μόνο οι εξουσιοδοτημένοι χρήστες.

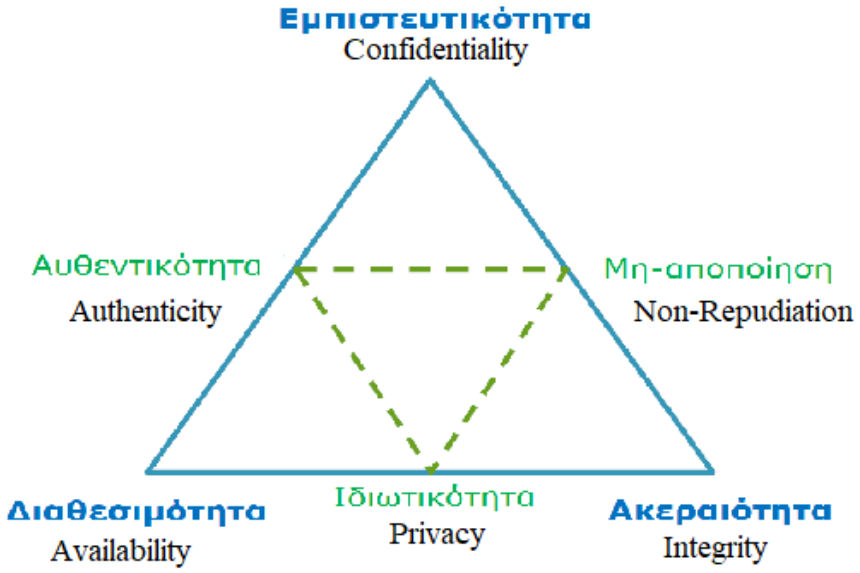
Η Αρχή της Ακεραιότητας (Integrity) θεσπίζει την προστασία των δεδομένων και των προγραμμάτων από εσκεμμένες κακόβουλες ενέργειες ή από τυχαίες αλλοιώσεις.

Η Αρχή της Διαθεσιμότητας (Availability) επιτρέπει σε όλους τους χρήστες που είναι εξουσιοδοτημένοι, να έχουν διαρκώς διαθέσιμους για χρήση, τους πόρους ενός πληροφοριακού συστήματος

Η Αρχή της Ιδιωτικότητας (Privacy) δίνει τη δυνατότητα στο χρήστη να καθορίζει ποιες από τις προσωπικές του πληροφορίες θα συλλέγονται και από ποιους.

Η Αρχή της Αυθεντικότητας (Authenticity) διασφαλίζει ότι η ταυτότητα ενός χρήστη ή ενός μηνύματος είναι πραγματικά αυτή που δηλώνεται. Με την αρχή αυτή καθιερώνεται η πιστοποίηση της ταυτότητας χρήστη – μηνύματος.

Η Αρχή της Μη Αποποίησης Ευθυνών (Non-Repudiation) απαγορεύει στον κάθε χρήστη να αρνηθεί ενέργεια με σοβαρό αντίκτυπο (όπως για παράδειγμα την αποστολή κακόβουλου email, την οποία έκανε.



Σχήμα 3.1 Θεμελιώδεις στόχοι ασφάλειας

Οι παραπάνω θεμελιώδεις αρχές που αποτελούν τους στόχους της ασφάλειας των υπολογιστικών συστημάτων και των δικτύων, αποτελούν επίσης κύριους στόχους ασφάλειας και στο Internet of Things.

3.3 ΚΟΙΝΑ ΠΡΟΒΛΗΜΑΤΑ ΑΞΙΟΠΙΣΤΙΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IoT

Η κινητικότητα και η εύκολη επικοινωνία μεταξύ συσκευών στο Internet of Things αποτελεί ταυτόχρονα ένα μεγάλο πλεονέκτημα, αλλά και ένα μεγάλο μειονέκτημα.

Σε αυτή την ενότητα αξιολογείται η ασφάλεια ορισμένων από τις κοινές τεχνολογίες του Διαδικτύου των Αντικειμένων (IoT) που χρησιμοποιούνται για επικοινωνία. Για τους σκοπούς αυτής της αξιολόγησης, υποθέτουμε ότι ο «εισβολέας» βρίσκεται εντός της εμβέλειας της ασύρματης μετάδοσης της συσκευής και μπορεί να αλληλεπιδράσει με αυτήν. Οι επιθέσεις αυτού του είδους μπορούν να επιτευχθούν με χρήση κεραίας έξω από το κτίριο, για παράδειγμα από το χώρο στάθμευσης,. Ορισμένες από τις επιθέσεις απαιτούν από τον εισβολέα να βρίσκεται στο ίδιο τοπικό ασύρματο δίκτυο. Όλες οι τεχνολογίες που αναφέρονται ακολούθως είναι δυνητικά επιρρεπείς σε ραδιο-παρεμβολές (radio jamming), επιτρέποντας σε έναν κακόβουλο εισβολέα να διακόψει τη συνδεσιμότητα με τη συσκευή.

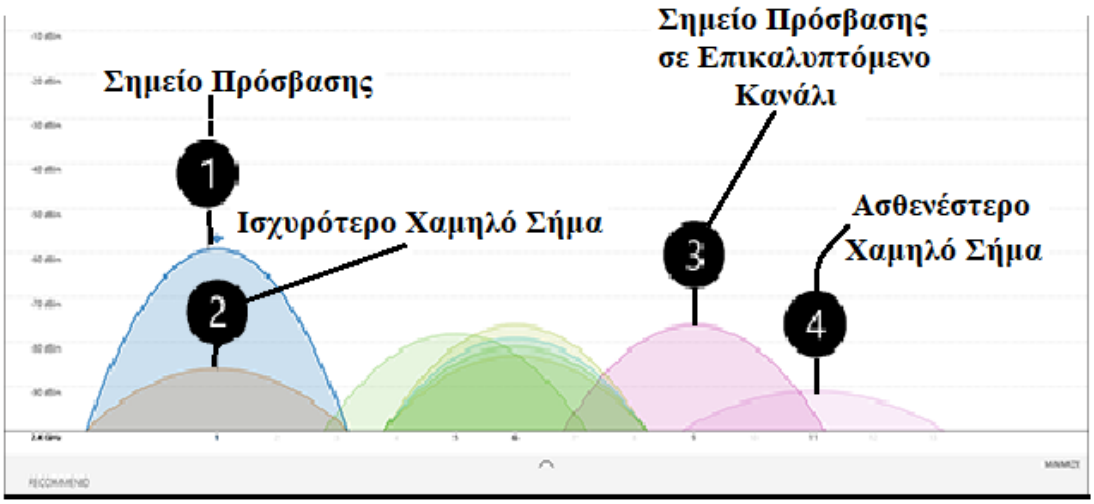
Η αξιολόγηση αφορά τα Wi Fi Networks (802.11), πρωτόκολλο Z-Wave, πρωτόκολλο ZigBee, Powerline, Bluetooth Low Energy, και άλλα RF πρωτόκολλα.

3.3.1 Wi Fi Networks (802.11)

Στον κόσμο των ασύρματων δικτύων γενικά, ο όρος Wi Fi είναι συνώνυμος με την ασύρματη πρόσβαση, παρά το γεγονός ότι πρόκειται για ένα συγκεκριμένο εμπορικό σήμα (Trademark) που ανήκει στο μη κερδοσκοπικού χαρακτήρα Wi Fi Alliance Group. Το Wi Fi με άλλα λόγια αποτελεί μια οικογένεια τεχνολογιών ραδιοσυχνοτήτων που χρησιμοποιείται κατά βάση στην ασύρματη τοπική δικτύωση (Wireless Local Area Networking – WLAN) και στηρίζεται στην οικογένεια προτύπων IEEE 802.11, που είναι μέρος των πρωτοκόλλων IEEE 802.

Για τα δίκτυα καταναλωτών υπάρχουν δύο ζώνες συχνοτήτων με τα δικά τους η κάθε μια πλεονεκτήματα και μειονεκτήματα. Πρόκειται για τις συχνότητες 2,4 GHz και 5 GHz. Ένας δρομολογητής (router) μπορεί να μεταδίδει στη μια ή και στις δύο ζώνες δικτύου ανάλογα με τις απαιτήσεις του χρήστη. Οι ασύρματοι δρομολογητές που αποτελούν τα σημεία πρόσβασης των καταναλωτών, χρησιμοποιούν ένα προκαθορισμένο κανάλι το οποίο ορίζεται εργοστασιακά. Η απεικόνιση ενός δικτύου συχνότητας 2,4 GHz σε γράφημα, δίνεται παρακάτω. Στο γράφημα ορίζονται τα σημεία

πρόσβασης, τα σημεία του ισχυρότερου και του ασθενέστερου χαμηλού σήματος, τα επικαλυπτόμενα κανάλια και το σημείο πρόσβασης σε αυτά.



Σχήμα 3.2 Γράφημα δικτύου συχνότητας 2,4 GHz

Η πρόσβαση στο δίκτυο Wi-Fi του σπιτιού ή ενός γραφείου, επιτρέπει σε έναν δικτυακό εισβολέα να εκτελέσει επιθέσεις κατά οποιασδήποτε συνδεδεμένης συσκευής. Το πρότυπο ισοδυνάμου ενσύρματης ιδιωτικότητας WEP (wired equivalent privacy) που αποτελεί έναν αλγόριθμο ασφάλειας των ασυρμάτων δικτύων και επικυρώθηκε το 1999, πρέπει να θεωρείται ανασφαλές και δεν πρέπει να χρησιμοποιείται.

Το 2003 ήταν διαθέσιμο από την Wi Fi Alliance Group. το πρότυπο ασφάλειας Wi Fi Protected Access (WPA), ενώ ένα χρόνο μετά – το 2004 – ήταν διαθέσιμο το πιο ασφαλές και πιο περίπλοκο Wi Fi Protected Access II (WPA 2). Παρά το γεγονός ότι η κρυπτογράφηση WPA 2 είναι ευρέως προσαρμοσμένη, οι εισβολείς έχουν τη δυνατότητα της βίαιης παραβίασης των αδύναμων κωδικών πρόσβασης και ακολούθως της απόκτησης πρόσβασης στο δίκτυο. Η παραβίαση αυτή συντελείται μέσω επιθέσεων τύπου dictionary attack που πραγματοποιούν. Τον Ιανουάριο του 2018 η Wi Fi Alliance ανακοίνωσε την έκδοση του Wi Fi Protected Access III (WPA 3), ενός προτύπου ασφαλείας με αρκετές βελτιώσεις πάνω στο προηγούμενο WPA 2.

Ορισμένοι πάροχοι ευρυζωνικών υπηρεσιών δεν επιτρέπουν στους χρήστες να αλλάξουν τους Κωδικούς Πρόσβασης στο Wi-Fi, ενδεχομένως βοηθώντας με αυτό τον τρόπο, τους βίαια επιτιθέμενους στους λογαριασμούς. Κάποιοι προμηθευτές

χρησιμοποιούν το πρωτόκολλο Wi-Fi Protected Setup (WPS), το οποίο δίνει έμφαση στη χρηστικότητα και την ασφάλεια και καθιερώνει τέσσερις τρόπους για τη προσθήκη μιας νέας συσκευής στο οικιακό δίκτυο. Οι τρόποι αφορούν: τη μέθοδο του WPS PIN, τη μεθοδολογία «με το πάτημα ενός κουμπιού», τη μέθοδο επικοινωνίας «εγγύς πεδίου» και τη μέθοδο του USB στη μεταφορά δεδομένων.

Το WPS το οποίο αναπτύχθηκε το 2006, επίσης από το Wi Fi Alliance Group, και το οποίο από καιρό διαπιστώθηκε ότι είναι ευάλωτο στις βίαιες επιθέσεις στο WPS PIN. Συγκεκριμένα το Δεκέμβρη του 2011, αποκαλύφθηκε ένα σημαντικό ελάττωμα ασφαλείας του WPS το οποίο επηρεάζει τους ασύρματους δρομολογητές (routers) με το χαρακτηριστικό WPS PIN, το οποίο τα πιο πρόσφατα μοντέλα έχουν ενεργοποιημένο από προεπιλογή. Το ελάττωμα επιτρέπει σε έναν απομακρυσμένο εισβολέα να ανακτήσει το WPS PIN μέσα σε λίγες ώρες με μια βίαιη επίθεση.

Ορισμένοι κατασκευαστές για την ασφάλεια υιοθετούν και εφαρμόζουν τον τρόπο της «απομόνωσης» του πελάτη για Wi-Fi σημεία πρόσβασης. Όμως οι πάροχοι του διαδικτύου δεν ενεργοποιούν συνήθως αυτή την επιλογή στους οικιακούς δρομολογητές, ώστε να επιτρέπουν σε συσκευές να συνεργάζονται μέσα στο οικιακό δίκτυο. Ως αποτέλεσμα αυτού, οι συσκευές που είναι συνδεδεμένες στο δίκτυο μπορούν συνήθως να έχουν πρόσβαση μεταξύ τους (όχι μόνο η gateway), πράγμα που είναι μια καλή και επιθυμητή διάταξη.

3.3.2 Πρωτόκολλο Z-Wave

Το Z-Wave είναι πρωτόκολλο ασύρματων επικοινωνιών σχεδιασμένο για εφαρμογές οικιακού αυτοματισμού. Το πρωτόκολλο αυτό χρησιμοποιεί χαμηλής ισχύος αξιόπιστα ραδιοκύματα που εύκολα ταξιδεύουν ανάμεσα από τοίχους, δάπεδα, και άλλα σταθερά εμπόδια και μπορεί να προστεθεί σε οποιαδήποτε οικιακή ηλεκτρική ή ηλεκτρονική συσκευή, όπως ο φωτισμός, τα ηλεκτρικά ρολά, οι θερμοστάτες κ.α. Το Z-Wave μπορεί να έχει εφαρμογές σε κατοικίες που ήδη υπάρχουν, μετατρέποντας για παράδειγμα τους απλούς ηλεκτρικούς διακόπτες σ «έξυπνους», ενταγμένους σε ένα ενιαίο δίκτυο.

Σήμερα υπάρχουν χιλιάδες πιστοποιημένα Z-Wave προϊόντα και πλήθος εταιριών δραστηριοποιείται στο χώρο, με στόχο να παρέχουν στις οικογένειες τη δυνατότητα να παραμείνουν συνδεδεμένες με τα σπίτια τους και μεταξύ τους. Σε αυτές τις εταιρίες απευθύνονται άτομα που είτε διαθέτουν έξυπνα σπίτια ή έξυπνα οικιακά προϊόντα και επιθυμούν να προσθέσουν νέες λειτουργίες, είτε θέλουν να μετατρέψουν τα συμβατικά σπίτια τους σε «έξυπνα».

Η απεικόνιση ασύρματων επικοινωνιών για εφαρμογές οικιακού αυτοματισμού με τη συνδρομή του πρωτοκόλλου Z-Wave των δίνεται παρακάτω.

. **Σχήμα 3.3** Z-Wave, Ασύρματη επικοινωνία-Οικιακός αυτοματισμός

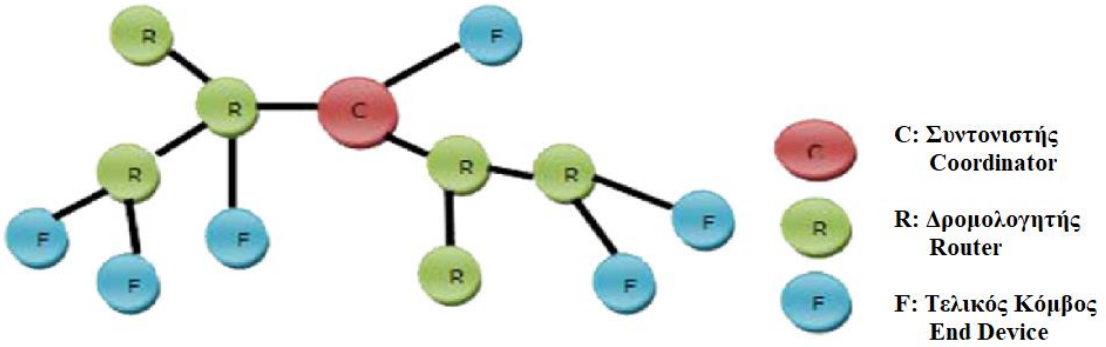
Το πρωτόκολλο Z-Wave αφ' εαυτού θεωρείται ασφαλές. Ωστόσο, οι ερευνητές βρήκαν στο παρελθόν αδυναμίες στην εφαρμογή. Οι αδυναμίες αυτές επηρέασαν συγκεκριμένους κατασκευαστές και τους επέτρεψαν να πάρουν τον πλήρη έλεγχο των συσκευών στα δίκτυα Z-Wave. «*Αυτή η ευπάθεια δεν οφείλεται σε ελάττωμα της προδιαγραφής του πρωτοκόλλου Z-Wave, αλλά προκύπτει εξ' αιτίας ενός σφάλματος εφαρμογής, στην απενεργοποίηση της χρήσης του προσωρινού κλειδιού, μετά την αρχική ανταλλαγή του κλειδιού του δικτύου, κατά τη διάρκεια εισαγωγής ενός κόμβου σε αυτό το δίκτυο*». Δήλωσαν οι συγγραφείς σχετικής μελέτης, Behrang Fouladi και Sahand Ghanoun. Παρόμοιες παγίδες εφαρμογής ενδέχεται να επηρεάσουν και άλλους κατασκευαστές έξυπνων συσκευών οικιακής χρήσης.

3.3.3 Πρωτόκολλο ZigBee

Το Πρωτόκολλο ZigBee αφορά την αυτόματη επικοινωνία σε δίκτυα μικρής εμβέλειας και χαμηλού ρυθμού μετάδοσης δεδομένων. Οι συχνότητες των δικτύων που βασίζονται στο Πρωτόκολλο αυτό μπορεί να είναι 868 MHz ή 915 MHz ή 2,4 GHz ενώ η μετάδοση των δεδομένων γίνεται με μέγιστο ρυθμό 250 Kbits/sec. Το ZigBee κατά βάση βρίσκει πεδίο εφαρμογής σε συσκευές που λειτουργούν με μπαταρία.

Βασικά χαρακτηριστικά του ZigBee αποτελούν η απλότητα, η χαμηλή κατανάλωση ενέργειας, ο χαμηλός ρυθμός μεταφοράς δεδομένων, εμβέλεια για την κάλυψη οικιακών αναγκών, το χαμηλό κόστος, η υποστήριξη 65.535 συσκευών ανά δίκτυο, η αξιόπιστη μεταφορά δεδομένων, η αυτοδιαμόρφωση και η υποστήριξη πολλαπλών τοπολογιών δικτύου.

Σε ένα δίκτυο ZigBee, όπως αναπαριστάται στο διάγραμμα που ακολουθεί υπάρχουν τρεις (3) κατηγορίες συσκευών (Nisha Ashok Somani και Yask Patel, 2012). Ο Συντονιστής (Coordinator), ο Δρομολογητής (Router) και ο Τελικός Κόμβος (End Device).



Σχήμα 3.4 Μορφή δικτύου ZigBee

Ο ρόλος του Συντονιστή είναι η δημιουργία διακλαδώσεων του δικτύου και η ενδεχόμενη σύνδεση με άλλα δίκτυα. Επιπλέον η επιλογή της συχνότητας εκπομπής του δικτύου και η αποθήκευση πληροφοριών σχετικά με το δίκτυο (όπως τα κλειδιά ασφαλείας). Σε κάθε δίκτυο όπως φαίνεται και στο σχήμα υπάρχει μόνο ένας Συντονιστής. Ο Δρομολογητής λειτουργεί σαν ενδιάμεσος κόμβος στο δίκτυο, όπου

υπάρχουν πολλοί τέτοιοι κόμβοι που αναμεταδίδουν δεδομένα από άλλες συσκευές. Οι δρομολογητές έχουν τη δυνατότητα να συνδέονται με υπάρχοντα δίκτυα, βοηθώντας στην εξάπλωσή τους. Οι τελικοί κόμβοι μπορεί να είναι είτε συσκευές μπαταρίας είτε συσκευές χαμηλής κατανάλωσης. Οι δυνατότητες των συσκευών αυτών περιορίζονται στη συγκέντρωση πληροφοριών από τους αισθητήρες και στην επικοινωνία με τους Συντονιστές και τους Δρομολογητές. Οι κόμβοι δεν μπορούν να αναμεταδίδουν δεδομένα σε άλλες συσκευές. Ο κάθε κόμβος μπορεί να υποστηρίζει μέχρι 240 συνδέσεις στην ίδια συχνότητα.

Το πρότυπο ZigBee είναι η πρώτη επιλογή σε εφαρμογές IoT και ειδικότερα σε εφαρμογές έξυπνων σπιτιών (Ankur Tomar, 2011). Οι βασικοί λόγοι εστιάζονται στο χαμηλό κόστος των αισθητήρων ZigBee (έως και 400% μικρότερο, των αισθητήρων των αντίστοιχων προτύπων όπως το Wi-Fi ή το Bluetooth), στην ταχύτητα που παρόλο είναι μικρότερη αυτό δεν είναι αισθητά αντιληπτό, στη μικρότερη κατανάλωση ρεύματος και στο γεγονός ότι μπορεί να διαχειριστεί περισσότερους κόμβους.

Ομοίως με το Z-Wave, το πρωτόκολλο ZigBee θεωρείται ασφαλές από την έκδοση ZigBee PRO και μετά. Ωστόσο κάποιες ανησυχίες έχουν εκφρασθεί σχετικά με την υποστήριξη ανταλλαγής κλειδιών για απλό κείμενο “over the air” (plain text OTA) σε συγκεκριμένα προφίλ τα οποία προορίζονταν να χρησιμοποιηθούν από κατασκευαστές κατά την αρχική επικοινωνία των συσκευών. Ερευνητές έχουν διαπιστώσει ότι ορισμένοι κατασκευαστές έχουν κάνει κακή χρήση αυτού του χαρακτηριστικού.

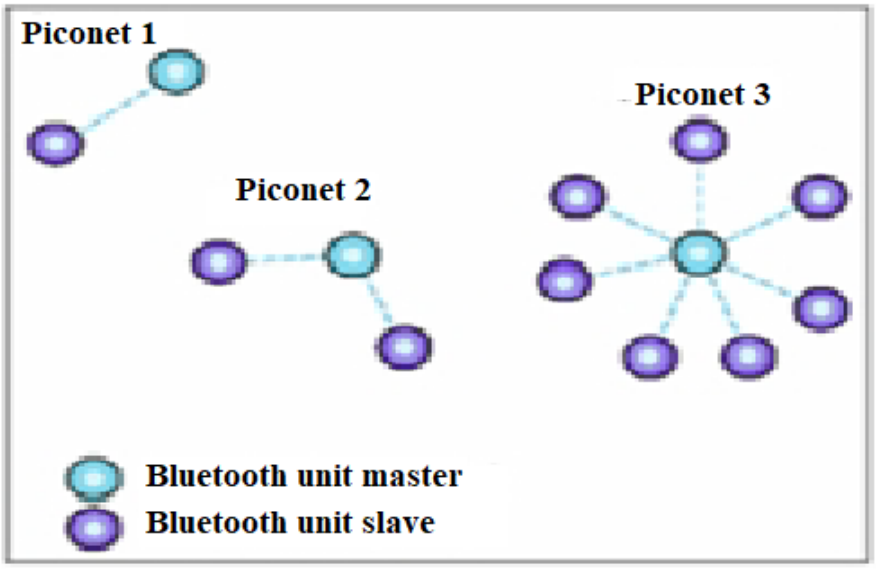
Ένα άλλο θέμα ασφάλειας αφορά το κοινόχρηστο δικτυακό κλειδί του πρωτοκόλλου. Κλέβοντας έναν από τους κόμβους ενός δικτύου ZigBee, κάποιος εισβολέας θα μπορούσε να αποκτήσει πρόσβαση στην εσωτερική μνήμη του κόμβου και να ανακτήσει το δικτυακό αυτό κλειδί, παρέχοντας πρόσβαση στο δίκτυο**.** Ένα τέτοιο σενάριο μπορεί να αποδειχθεί ιδιαίτερα επικίνδυνο σε συγκεκριμένες ρυθμίσεις που χρησιμοποιούνται για οικιακά δίκτυα, τα οποία έχουν αισθητήρες που αναπτύσσονται έξω από το σπίτι, όπως για παράδειγμα είναι ένας εξωτερικός ηλεκτρικός λαμπτήρας.

3.3.4 Bluetooth Low Energy

Το Bluetooth αποτελεί βιομηχανικό πρότυπο για προσωπικά ασύρματα δίκτυα (Wireless Personal Area Networks – WPAN) και βασίζεται στο πρωτόκολλο IEEE 802.15. Ως τηλεπικοινωνιακή τεχνολογία αφορά μικρές αποστάσεις και μεταδίδει σήματα σε ψηφιακές διατάξεις, παρέχοντας ασύρματη επικοινωνία μεταξύ PDAs, κινητών τηλεφώνων, προσωπικών φορητών υπολογιστών, ψηφιακών φωτογραφικών μηχανών και καμερών. Το Bluetooth είναι μια ασφαλής, οικονομική και παγκοσμίως διαθέσιμη τεχνολογία (Chatschik Bisdikian, 2001), ένα παγκόσμιο πρότυπο. Σύμφωνα με τους Wayne Staab και Steve Armstrong (2013) αντικαθιστά τα καλώδια μεταξύ των σταθερών και κινητών συσκευών, διευκολύνει τη μετάδοση δεδομένων, προσφέρει τη δυνατότητα χρήσης των ομότιμων δικτύων και παρέχει συγχρονισμό μεταξύ όλων των προσωπικών συσκευών.

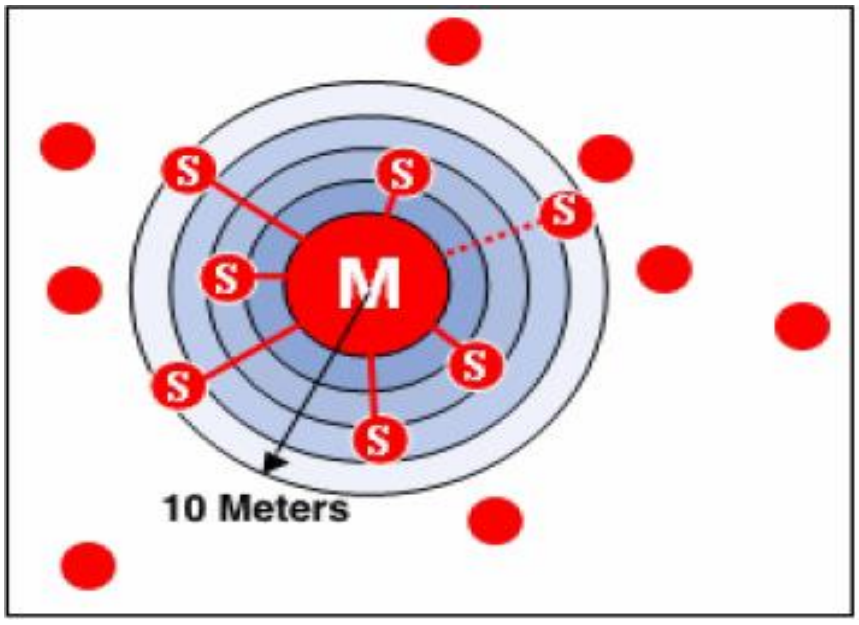
Όσον αφορά τις προδιαγραφές του Bluetooth επισημαίνονται: η βραχεία εμβέλεια (περίπου 10m) ή προαιρετικά μια μεσαία εμβέλεια (περίπου 100 m), η ασύρματη ζεύξη ικανή για μετάδοση φωνής και δεδομένων, η μέγιστη ταχύτητα μετάδοσης 720 kbps ανά κανάλι, η λειτουργία στη φασματική ζώνη (ISM ζώνη) των 2.4 GHz, η υλοποίηση αμφίδρομης επικοινωνίας με τη χρήση της μεθόδου μετάδοσης με διασπορά φάσματος Frequency Hopping, τη διαμοίραση των δεδομένων σε «πακέτα», τη μετάδοση των «πακέτων» μέσω των εβδομήντα (70) διακριτών καναλιών εύρους 1 MHz το κάθε ένα, την απευθείας σύνδεση από συσκευή σε συσκευή (point-to-point) και τη δυνατότητα της ταυτόχρονης σύνδεσης έως και επτά (7) συσκευών με τη χρήση μιας συχνότητας (James Kardach, 1999).

Όταν μια συσκευή Bluetooth βρεθεί εντός της εμβέλειας μίας άλλης, τότε δημιουργείται το ομότιμο δίκτυο ad-hoc με συνδεσμολογία από σημείο σε σημείο (point-to-point) ή/και σημείου με πολλαπλά σημεία (point-to-multipoint). Η βασική δομική μονάδα ενός δικτύου Bluetooth είναι το Piconet. Η μονάδα αυτή απεικονίζεται στο διάγραμμα που ακολουθεί όπου αποτυπώνονται οι συσκευές master και slave. Οι περιπτώσεις που εμφανίζονται ως piconet 1, piconet 2 και piconet 3 δείχνουν πως το κάθε δίκτυο Piconet διαθέτει μια συσκευή master και έχει τη δυνατότητα να μοιράζεται κανάλια ασύγχρονης επικοινωνίας με περισσότερες από επτά (7) ενεργές συσκευές slave ταυτόχρονα.



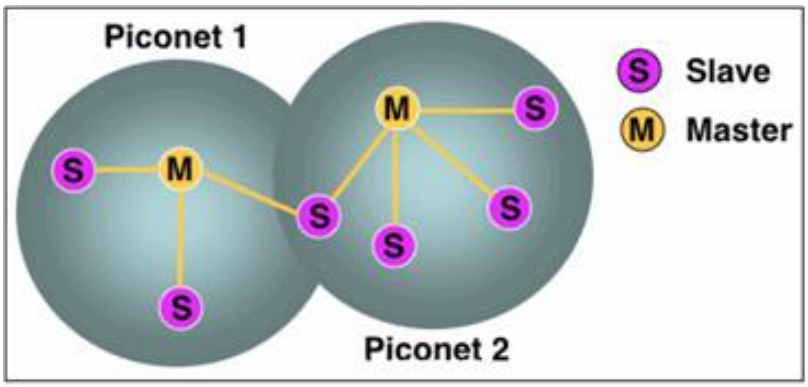
Σχήμα 3.5 Δομική μονάδα δικτύου Bluetooth

Επιπλέον μπορεί να υποστηρίξει έως 255 συσκευές slave σε κατάσταση αναμονής. Το δίκτυο παρουσιάζεται ακολούθως.



Σχήμα 3.6 Δίκτυο Piconet

Όπως φαίνεται στο σχήμα που ακολουθεί, οι συσκευές slave μπορούν να συμμετέχουν σε διάφορα και διαφορετικά Piconets και οι συσκευές master ενός Piconet να γίνουν slave σε κάποια άλλη συσκευή. Όσον αφορά δε τις συνδέσεις των κόμβων αυτές μπορεί να πραγματοποιούνται ως σύγχρονές ή ασύγχρονες.



Σχήμα 3.7 Scatternet

Το Bluetooth Low Energy, γνωστό επίσης και ως Bluetooth Smart, χρησιμοποιείται συχνά για έξυπνες οικιακές συσκευές που δεν χρειάζονται σύνδεση στο διαδίκτυο, όπως είναι οι κλειδαριές θυρών ή οι ηλεκτρικοί λαμπτήρες. Οι χρήστες μπορούν συνήθως να ελέγχουν αυτές τις συσκευές χρησιμοποιώντας ένα κινητό τηλέφωνο και μια αποκλειστική εφαρμογή (app). Το πρότυπο Bluetooth Smart είναι αρκετά ευέλικτο και αφήνει ανοικτό χώρο για ελαττωματικές εφαρμογές (faulty implementations) που θα μπορούσαν να επιτρέψουν σε δυνητικούς κακόβουλους επιτιθέμενους τον εξ αποστάσεως έλεγχο των συσκευών αυτών. Για παράδειγμα, πρόσφατα, η εφαρμογή Bluetooth LE για ένα προσωπικό φορητό wearable βραχιόλι ενδείξεων γυμναστικής (wearable fitness bracelet) ήταν πλήρως ανασχεδιασμένη, επιτρέποντας την έκθεση της συσκευής σε επίθεση.

3.3.5 Συγκριτικά στοιχεία των Προτύπων Επικοινωνίας

Στην παρούσα υποενότητα παρουσιάζονται υπό μορφή πίνακα ποσοτικοποιημένο συγκριτικά στοιχεία των τριών ασύρματων προτύπων που εκτέθηκαν προηγουμένως.

Σύγκριση των Προτύπων Ασύρματης Επικοινωνίας				
Παράμετροι	**Wi-Fi**	**Bluetooth**	**ZigBee**	**Z-wave**

Ζώνη συχνοτήτων Frequency band	2,4 GHz	2,4 GHz	2,4 GHz	NA
Physical/Mac layers	IEEE 802.11b	IEEE 802.15.1	IEEE 802.15.4	NA
Range Εύρος	75m έως 90m	9 m	Indoors έως 30 m Outdoors έως 100 m	NA
Current Consumption	400 mA (Tx mode) 20 mA (Standby mode)	60 mA (Tx mode)	25-35mA(Tx mode) 3 mA (Standby mode)	NA
Row data Rate	11Mbps	1Mbps	250 Kbps	NA
Protocol Stack size	1 MB	250 KB	32 KB 4 KB για περιορισμένες λειτουργίες και συσκευές	NA
Typical network joint time	Variable 1 sec typically	>3 sec	30 ms typically	NA
Interference avoidance method	Direct Sequence Spread Spectrum-DSSS	Frequency Hopping Spread Spectrum- FHSS	Direct Sequence Spread Spectrum-DSSS	NA
Minimum quiet bandwidth required	22 MHz static	15 MHz dynamic	3 MHz static	NA
Maximum number of nodes per network	32 per access point	7	64 K	NA
Αριθμός καναλιών	13	19	16	NA

3.3.6 Power Line Communication-PLC

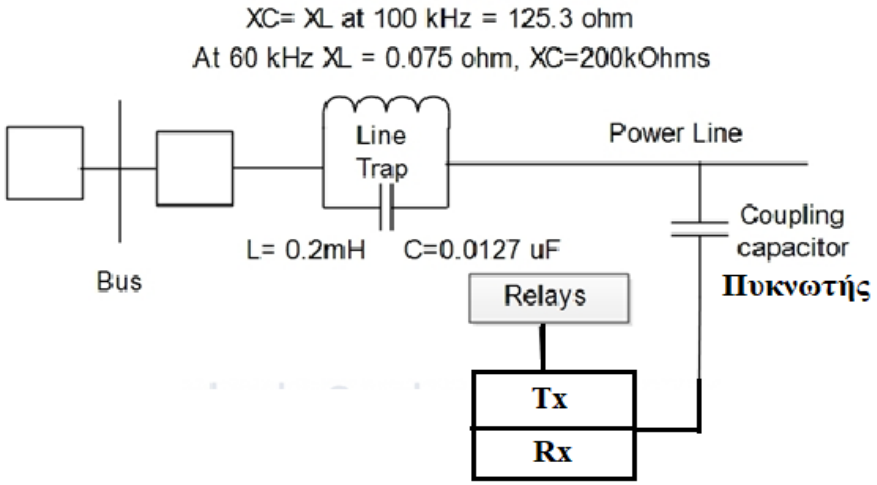
Η επικοινωνία Power Line συναντάται σε ένα ευρύ πεδίο εφαρμογών που αφορά από τον οικιακό αυτοματισμό μέχρι την πρόσβαση στο διαδίκτυο και την ταχεία μετάδοση ψηφιακών δεδομένων. Εκτός από Power Line Communication συναντάται και ως Power Line Carrier-PLC ή ως Power Line Digital Subscriber Line –PDSL.

Στην PLC εντάσσεται κάθε τεχνολογία που επιτρέπει τη μεταφορά δεδομένων με ταχύτητες μικρού ή μεγάλου εύρους, μέσω γραμμών μεταφοράς ηλεκτρικής ενέργειας, χρησιμοποιώντας προηγμένη τεχνολογία διαμόρφωσης. Ειδικότερα με την PLC μεταφέρονται τα δεδομένα σε έναν αγωγό, ο οποίος παράλληλα χρησιμοποιείται για τη μεταφορά και διανομή ηλεκτρικής ενέργειας στους καταναλωτές. Κατά συνέπεια είναι σαν οποιαδήποτε άλλη τεχνολογία επικοινωνίας, με την οποία ο αποστολέας διαμορφώνει τα προς αποστολή δεδομένα, τα εισάγει στο μέσο και κάποιος δέκτης αποδιαμορφώνει τα δεδομένα αυτά για να τα διαβάσει. Η κύρια διαφορά είναι ότι η PLC δεν χρειάζεται άλλη επιπλέον καλωδίωση, αλλά επαναχρησιμοποιεί υπάρχουσες καλωδιώσεις ή μοιράζεται υπάρχουσες συνδέσεις στο Internet. Λαμβάνοντας υπόψη τη διαπερατότητα των γραμμών μεταφοράς ηλεκτρικής ενέργειας, αυτό σημαίνει ότι με την PLC, σχεδόν όλες οι συσκευές που λειτουργούν στη γραμμή μπορούν να ελέγχονται.

Η Powerline επικοινωνία ελαχιστοποιεί τα κόστη υποδομών και συντηρήσεων, αφού υλοποιείται μέσω των υφιστάμενων γραμμών μεταφοράς ηλεκτρικής ενέργειας. Έτσι αποφεύγεται η δημιουργία νέων διαύλων επικοινωνίας διαμέσου εμποδίων όπως κτίρια, λόφοι, υπόγεια κ.α που παρεμποδίζουν τις ασύρματες επικοινωνίες, και η Powerline επικοινωνία αναδεικνύεται σε μια συμφέρουσα οικονομική επιλογή μεταξύ άλλων μεθόδων.

Το παρακάτω διάγραμμα που αφορά κύκλωμα PLC, αποτελεί τυπικό σχήμα παγίδευσης κύματος, με κατάλληλο πυκνωτή ζεύξης και επαγωγέα, που έχει τιμές μονάδας για ένα σύστημα 60Hz. Το κύκλωμα PLC συντονίζεται σε συχνότητα PLC όπου **XL = XC**. Αυτό το κύκλωμα απαρτίζεται από έναν επαγωγέα και έναν κατάλληλο πυκνωτή σύζευξης συνδεδεμένο παράλληλα και εγκατεστημένο στην αρχή της θέσης της γραμμής μετάδοσης και στις δύο άκρες. Αυτές ονομάζονται παγίδες γραμμών ή παγίδες κύματος.

Η γραμμή μεταφέρει συχνότητα ισχύος 50 ή 60 Hz καθώς και συχνότητα 100 kHz από τον πομπό. Ένας δέκτης συχνοτήτων συνδέεται ηλεκτρικά στην power line μέσω ενός πυκνωτή που έχει αντίσταση **XC = 1 / 2πfC** η οποία είναι αντιστρόφως ανάλογη προς τη συχνότητα "f".

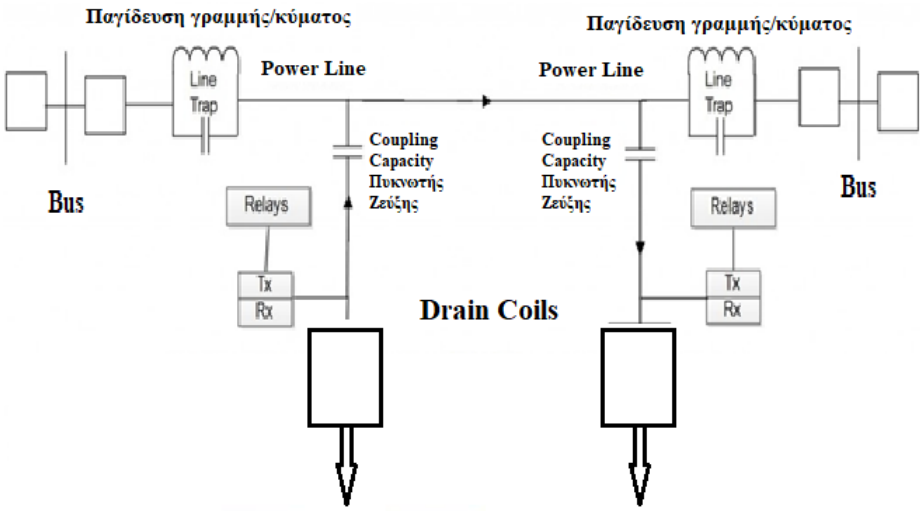


Σχήμα 3.8 PLC, παγίδευση κύματος

Ως εκ τούτου ένας πυκνωτής ζεύξης υψηλής συχνότητας προσφέρει χαμηλή αντίσταση, ενώ σε συχνότητα ισχύος 50 ή 60Hz προσφέρει υψηλή αντίσταση. Με τη βοήθεια αυτής της τεχνικής, η χαμηλή ισχύς του σήματος PLC υπερτίθεται στην power line.. (Όταν χρησιμοποιείται CVTS, δεν απαιτείται χωριστός πυκνωτής σύζευξης και για σκοπούς ζεύξης χρησιμοποιείται πυκνωτής CVT)..

Το κύκλωμα συντονίζεται όταν:
XL = XC οι τιμές του πυκνωτή αντίστασης και του επαγωγέα δίδονται ως
XL σε 100 kHz = 125,3Ω
XL στα 60 Hζ = 0,075Ω
XC στα 100 kHz = 125,3Ω
XC στα 60 Hz = 200 kΩ

Σε ένα ολοκληρωμένο σχέδιο Power Line Communication (PLC) οι παγίδες γραμμής ή παγίδες κύματος εγκαθίστανται και στα δύο άκρα της γραμμής μεταφοράς, όπως αναλυτικά παρουσιάζονται στο ακόλουθο σχήμα.



Σχήμα 3.9 Ολοκληρωμένο σχέδιο Power Line Communication (PLC)_

` Το κύκλωμα γείωσης (grounding circuit) περιέχει ένα πηνίο αποστράγγισης (drain coil), ένα διάκενο τόξου και ένα σύνδεσμο γείωσης (earth link) για την παροχή της κατάλληλης ασφάλειας που απαιτείται κατά την εργασία σε αυτόν τον εξοπλισμό. Το πηνίο αποστράγγισης που είναι ένας καθαρός επαγωγέας ο οποίος προσφέρει χαμηλή αντίσταση σε συχνότητα 60Hz, που μπορεί να ρεύσει κατά τη διάρκεια της βλάβης του πυκνωτή ζεύξης, βοηθά στη γείωση της υψηλής τάσης.

Υπό αυτές τις συνθήκες, η υψηλή τάση μπορεί να προκαλέσει βλάβη στον εξοπλισμό PLC, αλλά τα drain coils λόγω της χαμηλής αντίστασης εκτρέπουν και εμποδίζουν τις τυχαίες υψηλές αιχμές της τάσης. Κατά τη διάρκεια της εργασίας στον εξοπλισμό PLC οι σύνδεσμοι γείωσης πρέπει να κλείνονται ώστε να αποφεύγεται ο κίνδυνος υψηλής τάσης από φορτισμένο πυκνωτή.

Τα δύο κύρια πρωτόκολλα του οικιακού αυτοματισμού που χρησιμοποιούν το Powerline είναι τα:

- X10 (επίσης υποστηρίζεται μέσω RF)
- Insteon (ένα υβρίδιο RF και Powerline)

Μία από τις κύριες ανησυχίες γύρω από αυτά τα πρωτόκολλα της Powerline επικοινωνίας, είναι ότι τα σήματα μπορούν εύκολα να παρουσιάσουν διαρροές, να «εξαερωθούν» προς τα επόμενα συνδεδεμένα δίκτυα, επιτρέποντας έτσι σε ανθρώπους κοντά στο δίκτυο, όπως είναι οι γείτονες κάποιου, να μπορούν να κατασκοπεύουν αυτές τις επικοινωνίες. Για να αντιμετωπιστεί η αδυναμία αυτή, τα εν λόγω

πρωτόκολλα καθώς και άλλα συστήματα που βασίζονται στο Powerline, τυπικά υποστηρίζουν την κρυπτογράφηση.

3.3.7 Άλλα RF Πρωτόκολλα

Ορισμένοι προμηθευτές έχουν εφαρμόσει το δικό τους πρωτόκολλο (radio protocol) για τις συσκευές που παράγουν και εμπορεύονται. Το γεγονός αυτό μπορεί να έχει ως αποτέλεσμα τα πρωτόκολλα αυτά να είναι ευάλωτα σε παρόμοιες επιθέσεις με αυτές που δέχονται τα πρότυπα που περιγράφηκαν προηγουμένως. Για παράδειγμα, το Lightwave RF θεωρείται ότι είναι ευάλωτο σε επιθέσεις επανάληψης.

Η μέθοδος του Lightwave RF χρησιμοποιείται στις περιπτώσεις οικιακού αυτοματισμού με την τοποθέτηση «έξυπνων εκδόσεων» ηλεκτρικών διακοπτών, πριζών, λαμπτήρων κ.α. έναντι των συμβατικών. Πλέον επεκτάθηκε και στον έλεγχο της θέρμανσής, εξελίσσοντας το σύστημα σε single shot για τον έλεγχο ολόκληρου του σπιτιού.

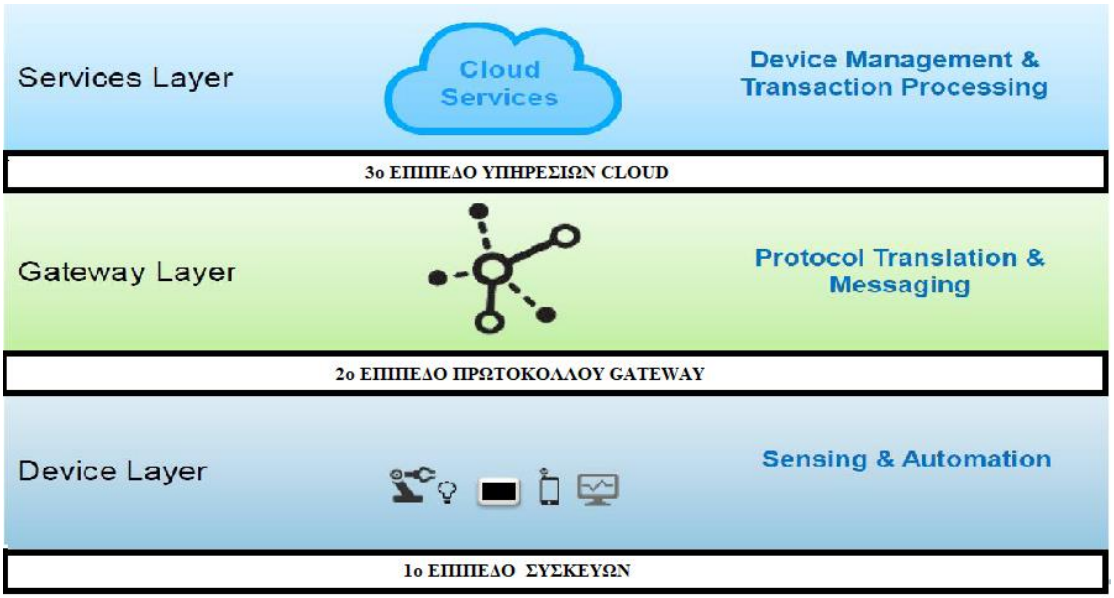
3.4 ΜΕΙΖΟΝΑ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IoT

Σύμφωνα με το Open Web Application Security Project – OWASP (μια online κοινότητα που παρέχει τεκμηρίωση, μεθοδολογίες, εργαλεία, τεχνολογία και αρθρογραφία στον τομέα των Web εφαρμογών), υπάρχουν αρκετά τρωτά σημεία στην ασφάλεια του Internet of Things. Ως οι πιο κοινές περιπτώσεις αναφέρονται οι παρακάτω:

- Ο μηχανισμός ταυτοποίησης εξουσιοδότησης κρίνεται ανεπαρκής
- Υφίσταται απουσία κρυπτογράφησης κατά τη μεταφορά data
- Η διεπαφή Cloud είναι μη ασφαλής
- Το λογισμικό – firmware δεν είναι ασφαλές
- Το Web Interface δεν είναι ασφαλές
- Μη ασφαλείς υπηρεσίες δικτύου
- Ευπάθειες σε ζητήματα ιδιωτικότητας
- Ανεπαρκές σύστημα παραμετροποίησης της ασφάλειας
- Στο υλικό των συσκευών και των υλικών μέσων διαπιστώνεται κακή ασφάλιση.

Σε μια πλατφόρμα IoT, η **διασφάλιση end-to-end** (ολοκληρωτικά, απ' άκρη σε άκρη) αποτελεί μια διαδικασία η οποία πρέπει να πραγματοποιείται σε όλα τα επίπεδα επικοινωνίας. Έτσι σε μια διαστρωμάτωση παραδείγματος χάριν τεσσάρων επιπέδων, πρέπει να πραγματοποιηθεί στα επίπεδα συσκευής, μεταφοράς, εφαρμογής και δικτύου ή σε μια διαστρωμάτωση τριών επιπέδων, στα επίπεδα συσκευής, πρωτοκόλλου Gateway και υπηρεσιών Cloud.

Γενικά υπάρχουν αρκετοί τρόποι απεικόνισης της διαστρωμάτωσης ενός δικτύου Internet of Things, που αποτελούν παραλλαγές κυρίως των δύο προαναφερθεισών. Στο παρακάτω σχήμα παρουσιάζεται μια διαστρωμάτωση τριών επιπέδων σε μια πλατφόρμα IoT.



Σχήμα 3.10 Πλατφόρμα IoT με διαστρωμάτωση τριών επιπέδων

Έρευνα της Symantec καταλήγει σε ευρήματα που η ανάλυσή τους εγείρει σημαντικές ανησυχίες για την ασφάλεια των συσκευών στο Διαδίκτυο των Αντικειμένων. Κατά τη διάρκεια της έρευνας της Symantec ανέκυψαν ζητήματα όπως:

- Γύρω στο 19% όλων των δοκιμασθέντων εφαρμογών που χρησιμοποιούνται σε κινητά τηλέφωνα για τον έλεγχο συσκευών IoT, δεν χρησιμοποιούσαν συνδέσεις Secure Socket Layer (SSL) στο Cloud.

- Καμία από τις συσκευές που αναλύθηκαν δεν παρέσχε αμοιβαία πιστοποίηση αυθεντικότητας, μεταξύ του πελάτη (client) και του εξυπηρετητή (server).
- Ορισμένες συσκευές δεν επιβάλουν και συχνά δεν παρέχουν τη δυνατότητα ισχυρών πρωτοκόλλων επικοινωνίας. Οι συσκευές δεν έχουν το απαιτούμενο από άποψη υπολογιστικής ισχύος hardware, ώστε να μπορούν να διασφαλίσουν την επιβολή ασφαλών πρωτοκόλλων επικοινωνίας.
- Ορισμένες IoT Cloud διεπαφές δεν υποστηρίζουν τον έξεγχο ταυτότητας δύο παραγόντων (2FA).
- Πολλές IoT υπηρεσίες δεν διαθέτουν μέτρα κλειδώματος ‘η καθυστέρησης για την προστασία των λογαριασμών των χρηστών, απέναντι σε βίαιες κακόβουλες επιθέσεις.
- Ορισμένες συσκευές δεν εφαρμόζουν προστασία κατά της συλλογής λογαριασμών (account harvesting).
- Πολλές από τις IoT Cloud πλατφόρμες περιλάμβαναν τις κοινές ευπάθειες των Web εφαρμογών.
- Εντοπίσθηκαν δέκα (10) θέματα ασφαλείας σε δεκαπέντε (15) Web Portals που χρησιμοποιούνται για τον έλεγχο IoT συσκευών, χωρίς όμως να εκτελούν σε βάθος ελέγχους (deep tests). Έξι από αυτά αφορούσαν πολύ σοβαρά ζητήματα, επειδή επέτρεπαν τη μη εξουσιοδοτημένη πρόσβαση στα συστήματα backend.
- Οι περισσότερες από τις υπηρεσίες IoT δεν παρέχουν συχνές ενημερώσεις firmware με σκοπό την κρυπτογράφηση.

Συμπερασματικά, διαπιστώνεται ότι εξακολουθούν να υπάρχουν πολλές συσκευές που δεν χρησιμοποιούν κρυπτογραφημένες επικοινωνίες ή σωστό έλεγχο ταυτότητας (authentication). Είναι πολύ σημαντικό σήμερα, για λόγους ασφαλείας, οι έξυπνες οικιακές συσκευές ή οι IoT συσκευές να χρησιμοποιούν τον αμοιβαίο έλεγχο ταυτότητας (mutual authentication) και την κρυπτογράφηση (encryption).

Οι συσκευές IoT έχουν συχνά λιγότερη μνήμη και πιο αργές CPUs, επομένως μπορεί να μην είναι σε θέση να χρησιμοποιούν τις ίδιες μεθόδους κρυπτογράφησης όπως συμβαίνει με τους παραδοσιακούς υπολογιστές, αυτό όμως δεν μπορεί να αποτελεί δικαιολογία για την έλλειψη μιας ισχυρής κρυπτογράφησης. Υπάρχουν αποτελεσματικές κρυπτογραφικές μέθοδοι σχεδιασμένες για συσκευές μικρής κλίμακας, όπως η κρυπτογράφηση ελλειπτικής καμπύλης ECC (Elliptic Curve

Cryptography), οι οποίες μπορούν να χρησιμοποιηθούν. Αυτό "τρέχει" σε μια έξυπνη συσκευή και είτε είναι το λογισμικό firmware είτε η εφαρμογή, πρέπει να επαληθευτεί μέσω μιας αλυσίδας εμπιστοσύνης.

Το πιο χαμηλό επίπεδο ασφαλείας (1ο επίπεδο) βρίσκεται εντός του επεξεργαστή, είναι το πρώτο βήμα της ακολουθίας εκκίνησης και ονομάζεται ρίζα εμπιστοσύνης/ασφάλειας. Τα επόμενα βήματα ή στάδια της ακολουθίας αυτής, συνιστούν τα ανώτερα επίπεδα εμπιστοσύνης/ασφάλειας και από κοινού με τη ρίζα εμπιστοσύνης αποτελούν την **αλυσίδα εμπιστοσύνης/ασφάλειας**. Ένα σύστημα για να θεωρείται ασφαλές πρέπει τα ανώτερα επίπεδα ασφάλειας, να εμπιστεύονται τα χαμηλότερα επίπεδα ασφάλειας.

Αν πάρουμε για παράδειγμα τη διαδικασία εκκίνησης μιας IoT Gateway. Η διαδικασία αυτή μπορεί να περιλαμβάνει μέχρι και τρείς bootloaders. Οι bootloaders εκκινούν τον υπολογιστή (booting). Ο ρόλος τους τόσο στην εκκίνηση όσο και στην αναβάθμιση ενός υπολογιστικού μηχανήματος είναι καθοριστικός. Αυτός είναι και ο λόγος που γίνονται συχνά στόχοι επιθέσεων. Οι επιθέσεις στοχεύουν συνήθως την τροποποίηση του κώδικα, έτσι που όταν «φορτωθεί» το Λειτουργικό Σύστημα να μπορεί να μεταβληθεί σε υποχείριο και κατά συνέπεια να παρέχει δυνατότητα εξαπόλυσης επιθέσεων όπως Denial of Service ή επιθέσεων στον πυρήνα του Λειτουργικού Συστήματος για τη δημιουργία κενών ασφαλείας.

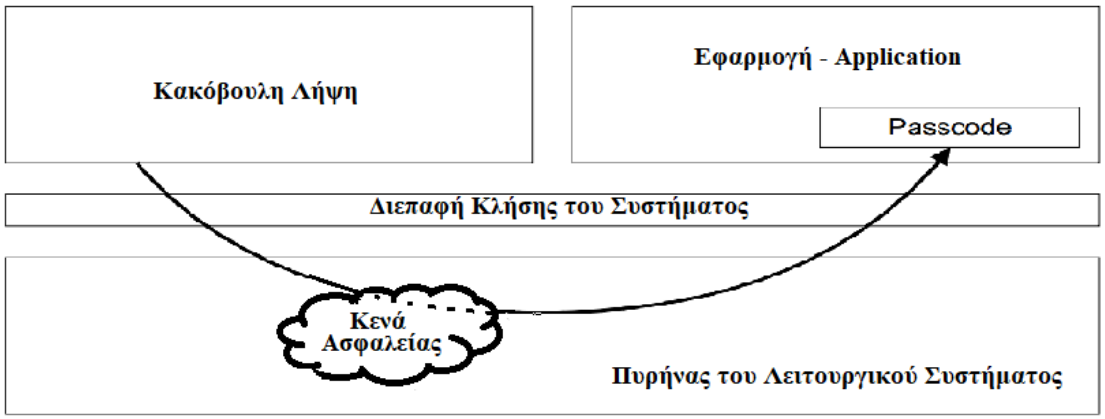
Αν από τους τρείς bootloaders του παραδείγματός μας ο πρώτος και ο δεύτερος (ο ROM bootloader και ο bootstrap bootloader) προστατεύονται στο εσωτερικό του επεξεργαστή, διασφαλίζεται το περιβάλλον για για το επόμενο βήμα της φόρτωσης του Λειτουργικού Συστήματος ή της αναβάθμισης του συστήματος. Στην αλυσίδα εμπιστοσύνης αν κάθε επίπεδο ταχτοποιείται και θωρακίζεται, τότε και τα αμέσως ανώτερα επίπεδα καθίστανται πιο ασφαλή.

Η προστασία του κώδικα και η διασφάλιση της συσκευής δημιουργούν μια αξιόπιστη γραμμή βάσης. Οι προμηθευτές θα πρέπει να παρέχουν προς τους χρήστες έναν απλό και αυτοματοποιημένο τρόπο ενημέρωσης - επικαιροποίησης των συσκευών τους, ώστε να διασφαλίζεται πως τα απλά, τα κοινά ζητήματα ασφαλείας θα μπορούν να διορθώνονται γρήγορα και αποτελεσματικά.

Οι συσκευές IoT πρέπει να δέχονται ως πρότυπο μόνο το «υπογεγραμμένο» λογισμικό firmware. Όπου ενδείκνυται, στη συνολική στρατηγική διαχείρισης συσκευών, πρέπει να παρέχονται πλήρη αναλυτικά στοιχεία των χαρακτηριστικών ασφαλείας.

Ένα άλλο αδύναμο σημείο πολλών IoT υπάρχει στις διεπαφές ελέγχου του Cloud. Εν προκειμένω, οι χρήστες δεν θα πρέπει να αναγκάζονται να χρησιμοποιούν τις ρυθμίσεις του Cloud, εάν το μόνο που θέλουν να κάνουν είναι απλά κάποιες βασικές εργασίες, όπως για παράδειγμα η ενεργοποίηση του φωτισμού των κατοικιών.

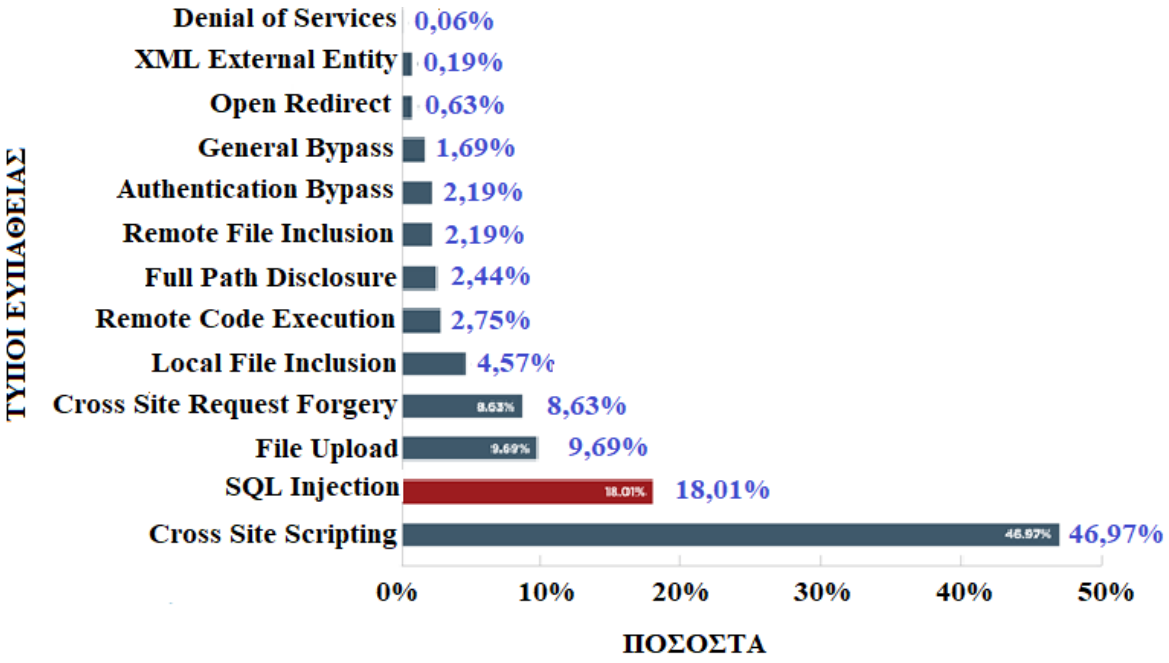
Οι προμηθευτές πρέπει οπωσδήποτε να επιτρέπουν τη χρήση ισχυρών, σύνθετων κωδικών πρόσβασης. Ο περιορισμός του ελέγχου ταυτότητας (authentication) με απλούς τετραψήφιους κωδικούς PIN δεν προστατεύει επαρκώς τη συσκευή και ειδικά εάν αυτό το ζήτημα συνδυάζεται με την έλλειψη κάποιου μηχανισμού προστασίας από βίαιες επιθέσεις. Όμως ακόμα και όταν χρησιμοποιούνται ισχυροί κωδικοί πρόσβασης, διαπιστώνεται ότι οι κοινές τρωτότητες/ευπάθειες σε Web εφαρμογές, όπως η τεχνική έκχυσης κώδικα «SQL injection», γνωστή και ως διάνυσμα επίθεσης σε ιστοτόπους ή η εξ αποστάσεως εισαγωγή αρχείων, εξακολουθούν να υπάρχουν συχνά σε αυτές τις πύλες ελέγχου του Cloud. Η εκμετάλλευση κενών ασφαλείς από κακόβουλο λογισμικό δίνεται διαγραμματικά παρακάτω.



Σχήμα 3.11 Εκμετάλλευση των κενών ασφαλείας

Οι προμηθευτές πρέπει να διασφαλίσουν ότι οι υπηρεσίες τους δεν είναι ευάλωτες στις πρώτες δέκα ευπάθειες που αναφέρει η OWASP για τις εφαρμογές του ιστού. Για συσκευές IoT όπως οι συναγερμοί καπνού, είναι επίσης σημαντικό ο πωλητής να έχει εξετάσει και προβλέψει τι θα συμβεί αν υπάρξει διακοπή ρεύματος ή μπλοκάρισμα του δικτύου. Η πρόβλεψη μπορεί να αφορά για παράδειγμα αν θα ειδοποιηθεί ο χρήστης ή αν θα παρακαμφθεί η δυσλειτουργική συσκευή ασφαλείας.

Οι τύποι των ευπαθειών και τα ποσοστά της κάθε μιας από αυτές εμφανίζονται στο παρακάτω γράφημα.



Σχήμα 3.12 Ευπάθειες του συστήματος ανά τύπο και ποσοστό

Στο εγγύς μέλλον αναμένεται ότι πολλοί άνθρωποι θα μπορούν να έχουν μια ποικιλία συσκευών συνδεδεμένων σε οικιακά δίκτυα. Αυτό θα οδηγήσει σε ευφυέστερους smart hubs που θα επιτρέπουν την υλοποίηση εντολών του τύπου «εάν αυτό … τότε εκείνο» (if this, then that), βασισμένες σε λογικούς συλλογισμούς και λογικές συνθήκες. Η εξέλιξη αυτή θα επαυξήσει την πολυπλοκότητα του όλου προβλήματος, καθώς σήμερα ένα πρόβλημα σε μία συσκευή μπορεί να προκαλέσει τον τερματισμό της λειτουργίας μιας άλλης.

Υπάρχουν ήδη διαθέσιμες εφαρμογές που επιτρέπουν σε κάποιον να κάνει ακριβώς αυτό το πράγμα. Προκειμένου να εκτελεστούν οι ενέργειες, η εφαρμογή πρέπει να έχει εξουσιοδότηση πρόσβασης σε έξυπνες συσκευές. Αυτό καθιστά τον έξυπνο κόμβο/διανομέα (smart hub) ένα ιδανικό κεντρικό σημείο επίθεσης, καθώς η αλλαγή τέτοιων κανόνων μπορεί να προκαλέσει καταστροφικές συνέπειες σε όλες τις συσκευές που είναι συνδεδεμένες στο δίκτυο. Με όλα αυτά τα ζητήματα που προκύπτουν και που επηρεάζουν τις συσκευές στα διάφορα επίπεδα, προς το παρόν δεν είναι εύκολη η ανάπτυξη και η εγκατάσταση πολλών έξυπνων συσκευών, με ασφαλή τρόπο στο σπίτι.

3.5 ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

3.5.1 Γενικά

Η ιδιωτικότητα (privacy) είναι όπως έχει προαναφερθεί σε άλλο μέρος της παρούσας διατριβής, μια βασική και θεμελιώδης αρχή/στόχος της ασφάλειας των υπολογιστικών συστημάτων, των δικτύων και του IoT. Σύμφωνα με την αρχή της ιδιωτικότητας, ο χρήστης πρέπει να είναι αυτός που θα καθορίζει ποιες προσωπικές του πληροφορίες θα συλλέγονται και από ποιους.

Ο σεβασμός των δικαιωμάτων και των προσδοκιών της ιδιωτικής ζωής πρέπει να αποτελεί αναπόσπαστο μέρος της διασφάλισης της εμπιστοσύνης στο Διαδίκτυο. Παράλληλα να επηρεάζει επίσης την ικανότητα των ατόμων να μιλούν, να συνδέονται και να επιλέγουν με ουσιαστικούς τρόπους.

3.5.2 Το υπόβαθρο της διασφάλισης της ιδιωτικότητας στο IoT

Τα ατομικά δικαιώματα και προσδοκίες του ιδιωτικού βίου των ατόμων, μερικές φορές εντάσσονται στα ζητήματα δεοντολογικού χειρισμού των δεδομένων. Το γεγονός αυτό υπογραμμίζει τη μεγάλη σημασία του σεβασμού των προσδοκιών του ατόμου, όσον αφορά την προστασία της ιδιωτικής του ζωής και τη χρηστή χρήση των δεδομένων του.

Αυτές οι παραδοσιακές προσδοκίες των ανθρώπων σχετικά με την προστασία της ιδιωτικότητάς τους μπορεί να αμφισβητηθούν στα πλαίσια λειτουργίας του Διαδικτύου των Αντικειμένων. Αυτό συμβαίνει επειδή το IoT αναφέρεται συχνά σε ένα μεγάλου εύρους δίκτυο συσκευών με αισθητήρες που έχουν σχεδιαστεί για τη συλλογή δεδομένων του περιβάλλοντός τους και το περιβάλλον αυτό περιλαμβάνει συνήθως δεδομένα που αφορούν και σχετίζονται με τους ανθρώπους.

Αυτά τα δεδομένα προφανώς παρέχουν πλεονέκτημα στους ιδιοκτήτες των συσκευών, αλλά συχνά ωφελούν και τρίτους, όπως τους κατασκευαστές ή τους

προμηθευτές των συσκευών αυτών. Προβληματισμός γύρω από τη συλλογή και τη χρήση των IoT δεδομένων γεννιέται, όταν τα άτομα που παρατηρούνται από τις IoT συσκευές, έχουν διαφορετικές προσδοκίες για την προστασία της ιδιωτικής τους ζωής, σχετικά με το πεδίο εφαρμογής και χρήσης των προσωπικών τους δεδομένων, από εκείνες που έχουν οι συλλέκτες των δεδομένων.

Φαινομενικά αβλαβείς συνδυασμοί ροών IoT δεδομένων μπορούν να θέσουν σε κίνδυνο την ιδιωτική ζωή. Όταν οι ατομικές ροές δεδομένων (individual data streams) συνδυαστούν ή συσχετιστούν, συχνά δημιουργείται ένα πιο ακριβές ψηφιακό πορτραίτο του ατόμου, από αυτό που μπορεί να δημιουργήσει μια μεμονωμένη ροή δεδομένων IoT. Για παράδειγμα, μια οδοντόβουρτσα με δυνατότητα σύνδεσης μπορεί να καταγράψει και να μεταδώσει αβλαβή δεδομένα σχετικά με τις συνήθειες βουρτσίσματος των δοντιών ενός ατόμου. Αν αυτό συνδυαστεί με το γεγονός ότι και το (συνδεδεμένο) ψυγείο του χρήστη αναφέρει την απογραφή των τροφών που αυτός καταναλώνει και επιπλέον μια συσκευή καταγραφής των προσωπικών του fitness δεδομένων καταγράφει και αναφέρει τα στοιχεία της σωματικής δραστηριότητάς του, ο συνδυασμός αυτών των ροών δεδομένων που προκύπτουν από τις τρείς συσκευές, σκιαγραφεί μια πολύ πιο λεπτομερή και ιδιωτική περιγραφή της συνολικής υγείας του ατόμου.

Το αποτέλεσμα σώρευσης των δεδομένων μπορεί να είναι ιδιαίτερα ισχυρό όσον αφορά τις IoT συσκευές. Αυτό συμβαίνει επειδή πολλοί παράγουν πρόσθετα μετα-δεδομένα (metadata) όπως πληροφορίες γεωγραφικής θέσης time stamps κλπ τα οποία εξειδικεύουν περισσότερο την εικόνα και το προφίλ του χρήστη.

Υπάρχουν περιπτώσεις που ο χρήστης μπορεί να αγνοεί πως μια συσκευή IoT συλλέγει δεδομένα σχετικά με το άτομό του και ενδεχομένως τα μοιράζεται με τρίτους. Αυτός ο τύπος συλλογής δεδομένων γίνεται όλο και πιο διαδεδομένος στα διαρκή καταναλωτικά προϊόντα (συσκευές) όπως είναι οι έξυπνες τηλεοράσεις και οι συσκευές βιντεοπαιχνιδιών. Αυτά τα είδη προϊόντων, συνήθως διαθέτουν φωνητική αναγνώριση ή χαρακτηριστικά οπτικής θέασης, που σε συνεχή βάση ακούνε συνομιλίες ή παρακολουθούν δραστηριότητες πχ σε ένα δωμάτιο και μεταδίδουν επιλεκτικά τα δεδομένα αυτά, σε μια υπηρεσία Cloud για επεξεργασία, η οποία κάποιες φορές περιλαμβάνει και ένα τρίτο μέρος.

Ένα άτομο μπορεί να κάνει χρήση τέτοιων συσκευών χωρίς να γνωρίζει ότι οι συνομιλίες ή οι δραστηριότητές του παρακολουθούνται και τα δεδομένα τους συλλέγονται προκειμένου να «αξιοποιηθούν». Τα διάφορα είδη χαρακτηριστικών και

λειτουργιών αυτών των συσκευών μπορεί να προσφέρουν κάποια πλεονεκτήματα σε έναν ενημερωμένο χρήστη, μπορούν όμως να δημιουργούν και προβλήματα προστασίας της ιδιωτικής ζωής, όσων δεν γνωρίζουν την παρουσία και τη λειτουργία των συσκευών αυτών και δεν ασκούν σημαντική επίδραση επί του τρόπου με τον οποίο χρησιμοποιούνται οι πληροφορίες που συλλέγονται. Ανεξάρτητα από το εάν ο χρήστης γνωρίζει και συναινεί στη συλλογή και την ανάλυση των δεδομένων του, οι καταστάσεις αυτές υπογραμμίζουν την αξία των εξατομικευμένων ροών δεδομένων για εταιρείες και οργανισμούς που επιδιώκουν να συλλέξουν και να επωφεληθούν από τις πληροφορίες στο Internet of Things.

Η ζήτηση αυτού του είδους πληροφοριών αναδεικνύει επίσης τις νομικές και ρυθμιστικές προκλήσεις που αντιμετωπίζει το Δίκαιο για την προστασία των προσωπικών δεδομένων και του ιδιωτικού απορρήτου. Η αντιμετώπιση των προβλημάτων περί ιδιωτικού απορρήτου είναι κρίσιμη, επειδή τα προβλήματα αυτά έχουν άμεσες επιπτώσεις στα βασικά δικαιώματα του ατόμου και στη συλλογική ικανότητα όλων να εμπιστεύονται το Διαδίκτυο. Υπό μια ευρεία προοπτική, οι άνθρωποι αφενός αναγνωρίζουν πως η ιδιωτικότητά τους είναι εγγενώς πολύτιμη και αφετέρου έχουν προσδοκίες για το ποια δεδομένα, σχετικά με αυτούς, μπορούν να συγκεντρωθούν και για το πώς μπορούν τρίτοι, να χρησιμοποιούν τα δεδομένα αυτά.

Αυτή η γενική έννοια περί προστασίας της ιδιωτικής ζωής ισχύει για τα δεδομένα που συλλέγονται από τις συσκευές Internet of Things, αλλά αυτές οι συσκευές μπορούν να υπονομεύσουν την δυνατότητα του χρήστη να εκφράζει και να επιβάλλει τις προτιμήσεις του περί απορρήτου. Εάν οι χρήστες χάσουν την εμπιστοσύνη τους στο Internet επειδή οι προτιμήσεις τους σχετικά με το απόρρητο δεν γίνονται σεβαστές στο Διαδίκτυο των Πραγμάτων, τότε η μεγαλύτερη αξία του Διαδικτύου μπορεί να μειωθεί σημαντικά.

3.5.3 Οι μοναδικές πτυχές της ιδιωτικότητας του Internet of Things

Γενικά, οι ανησυχίες για την προστασία της ιδιωτικής ζωής ενισχύονται από τον τρόπο με τον οποίο το Internet of Things επεκτείνει τη σκοπιμότητα και την εμβέλεια της παρακολούθησης και της ανίχνευσης. Τα χαρακτηριστικά των συσκευών

IoT και οι τρόποι με τους οποίους χρησιμοποιούνται, επαναπροσδιορίζουν τη συζήτηση πάνω στα ζητήματα της ιδιωτικότητας, επειδή αλλάζουν δραματικά τον τρόπο με τον οποίο συλλέγονται, αναλύονται, χρησιμοποιούνται και προστατεύονται τα προσωπικά δεδομένα.

Το παραδοσιακό μοντέλο διαδικτυακής ιδιωτικότητας, «notice and consent» (ειδοποίησης και συναίνεσης) στο οποίο οι χρήστες επιβεβαιώνουν τις προτιμήσεις τους για την προστασία της ιδιωτικής τους ζωής, αλληλεπιδρώντας άμεσα με τις πληροφορίες που παρουσιάζονται στην οθόνη ενός υπολογιστή ή κινητού τηλεφώνου (π.χ. κάνοντας κλικ στο "Συμφωνώ"), αποτυγχάνει όταν τα συστήματα δεν παρέχουν μηχανισμό αλληλεπίδρασης. Οι συσκευές IoT συχνά δεν έχουν user interface ώστε να ρυθμίζονται οι προτιμήσεις απορρήτου και σε πολλές διαμορφώσεις IoT, οι χρήστες δε γνωρίζουν ή δεν ελέγχουν, τον τρόπο με τον οποίο τα προσωπικά τους δεδομένα συλλέγονται και χρησιμοποιούνται. Αυτό προκαλεί ένα χάσμα μεταξύ των προτιμήσεων απορρήτου των χρηστών και της συμπεριφοράς συλλογής δεδομένων, των IoT συσκευών.

Μπορεί να υπάρχουν λιγότερα κίνητρα για τους πωλητές IoT να προσφέρουν στους χρήστες έναν μηχανισμό ώστε αυτοί να εκφράζουν τις προτιμήσεις τους για την προστασία της ιδιωτικής τους ζωής, εάν θεωρούν τα δεδομένα που συλλέγονται ως μη προσωπικά δεδομένα. Ωστόσο, η εμπειρία δείχνει ότι τα δεδομένα που παραδοσιακά δεν θεωρούνται προσωπικά δεδομένα ενδέχεται να είναι προσωπικά ή να γίνουν προσωπικά δεδομένα σε συνδυασμό με άλλα δεδομένα.

Αν υποθέσουμε ότι θα μπορούσε να αναπτυχθεί ένας αποτελεσματικός μηχανισμός που να επιτρέπει στο χρήστη να εκφράζει συνειδητά τη συναίνεσή του περί των προτιμήσεών του, σχετικά με την ιδιωτικότητα σε IoT συσκευές, αυτός ο μηχανισμός πρέπει να χειρίζεται τον μεγάλο αριθμό συσκευών IoT, που ο χρήστης με τη σειρά του πρέπει να ελέγχει. Σε κάθε περίπτωση είναι μη ρεαλιστικό να πιστεύουμε ότι ένας χρήστης θα αλληλεπιδρά άμεσα με την κάθε συσκευή IoT που συναντά κατά τη διάρκεια μιας ημέρασ για να εκφράσει τις προτιμήσεις απορρήτου.

Αντίθετα, οι μηχανισμοί αλληλεπίδρασης της ιδιωτικότητας πρέπει να είναι επεκτάσιμοι στο μέγεθος του προβλήματος του Internet of Things, ενώ εξακολουθούν να είναι ολοκληρωμένοι και πρακτικοί από την άποψη του χρήστη. Το Διαδίκτυο των Αντικειμένων μπορεί να απειλήσει τις προσδοκίες ενός προσώπου για το απόρρητο σε κοινές καταστάσεις.

Υπάρχουν κοινωνικοί κανόνες και προσδοκίες ιδιωτικότητας που διαφέρουν στους δημόσιους έναντι των ιδιωτικών χώρων, όμως πρακτικά οι συσκευές IoT θέτουν υπό αμφισβήτηση την τήρηση των κανόνων αυτών. Για παράδειγμα, οι IoT τεχνολογίες και συστήματα επιτήρησης όπως οι κάμερες παρακολούθησης ή τα συστήματα εντοπισμού θέσης, που κανονικά λειτουργούν σε δημόσιους χώρους, μεταφέρονται και σε παραδοσιακά ιδιωτικούς χώρους όπως το σπίτι, το γραφείο ή το προσωπικό όχημα, όπου όμως οι προσδοκίες του ατόμου για το απόρρητο της ιδιωτικής του ζωής είναι πολύ διαφορετικές. Με αυτόν τον τρόπο, αμφισβητείται αυτό που πολλές κοινωνίες αναγνωρίζουν ως «δικαίωμα να μείνει κάποιος μόνος» στον προσωπικό του χώρο.

Επιπρόσθετα, οι προσδοκίες των πολιτών για το απόρρητο της ιδιωτικότητάς τους σε χώρους που θεωρούνται δημόσιοι (όπως πάρκα, εμπορικά κέντρα, σιδηροδρομικοί σταθμοί) αμφισβητούνται και τελικά παραβιάζονται από την αυξημένη φύση και έκταση της παρακολούθησης στους χώρους αυτούς. Οι συσκευές IoT λειτουργούν συχνά σε περιβάλλοντα όπου η εγγύτητα εκθέτει πολλούς ανθρώπους στην ίδια δραστηριότητα συλλογής δεδομένων. Για παράδειγμα, ένας αισθητήρας παρακολούθησης γεωγραφικής θέσης τοποθετημένος σε ένα αυτοκίνητο, θα καταγράφει και θα μεταδίδει τα δεδομένα της θέσης σχετικά με όλους τους επιβάτες του οχήματος, ανεξάρτητα από το αν όλοι οι επιβάτες επιθυμούν ή όχι να εντοπίζεται η τοποθεσία τους. Μπορεί ακόμη να παρακολουθούνται και να ανιχνεύονται άτομα και σε κοντινά οχήματα.

Σε τέτοιου είδους καταστάσεις, μπορεί να είναι πολύ δύσκολο ή αδύνατο να γίνει διάκριση, μεταξύ των ατομικών προτιμήσεων περί απορρήτου της ιδιωτικής ζωής του κάθε ενός. Αναλύσεις σε big data που έχουν δημιουργηθεί από συγκεντρώσεις δεδομένων προσωπικού χαρακτήρα, αντιπροσωπεύουν ήδη ένα σημαντικό κίνδυνο εισβολής στην ιδιωτική ζωή των ανθρώπων καθώς και πιθανών διακρίσεων. Ο κίνδυνος αυτός ενισχύεται στο Internet of Things από το μέγεθος της κλίμακας, το βαθμό ευκολίας και τη μεγαλύτερη οικειότητα της συλλογής προσωπικών δεδομένων.

Οι συσκευές IoT μπορούν λόγω μεγάλης διεισδυτικότητας, να συλλέγουν πληροφορίες για τα άτομα, με πρωτοφανή βαθμό εξειδίκευσης. Η συσσωμάτωση και η συσχέτιση των δεδομένων που συλλέγονται, μπορούν να δημιουργήσουν λεπτομερή προφίλ των ατόμων, τα οποία δημιουργούν το ενδεχόμενο για διακρίσεις και άλλες βλάβες. Η πολυπλοκότητα αυτής της τεχνολογίας μπορεί να δημιουργήσει καταστάσεις που εκθέτουν το άτομο σε σωματική, εγκληματική, οικονομική ή συκοφαντική βλάβη. Η πανταχού παρουσία, η οικειότητα και η κοινωνική αποδοχή πολλών συσκευών IoT,

μπορεί να δημιουργήσει μια ψευδαίσθηση ασφάλειας και να ενθαρρύνει τα άτομα να αποκαλύψουν ευαίσθητες ή ιδιωτικές πληροφορίες χωρίς να έχουν πλήρη επίγνωση ή εκτίμηση των πιθανών συνεπειών από αυτό.

3.5.4 Ερωτήματα για τη διασφάλιση της ιδιωτικότητας των χρηστών

Όλα τα ζητήματα που αφορούν την προστασία του απορρήτου της ιδιωτικής ζωής των ανθρώπων, θα αποτελούσαν μια πρόκληση, ακόμα και αν τα ενδιαφέροντα, τα κίνητρα και τα συμφέροντα των συμμετεχόντων στο IoT οικοσύστημα ήταν απόλυτα ευθυγραμμισμένα. Ωστόσο, γνωρίζουμε ότι στην πραγματικότητα μπορεί να υπάρχουν μη ισορροπημένες ή αθέμιτες σχέσεις και συμφέροντα μεταξύ εκείνων που εκτίθενται στη συλλογή προσωπικών δεδομένων και εκείνων που συγκεντρώνουν, αναλύουν και χρησιμοποιούν τα δεδομένα αυτά.

Στην πηγή των δεδομένων μπορεί να εκδηλωθεί μια ανεπιθύμητη εισβολή που να παραβιάζει τον ιδιωτικό χώρο, συχνά χωρίς τη συγκατάθεση, τον έλεγχο, την επιλογή ή ακόμα και τη γνώση των ατόμων που αφορά. Εντούτοις, ο συλλέκτης των δεδομένων μπορεί να θεωρήσει ότι αυτό αποτελεί έναν ωφέλιμο πόρο που μπορεί να προσθέσει αξία σε προϊόντα και υπηρεσίες καθώς και να παρέχει νέες ροές εσόδων.

Λόγω της αμφισβήτησης της προστασίας του ιδιωτικού βίου που έχει ανακύψει στο IoT αλλά και των νέων ιδεών που έχουν εκφραστεί γύρω από αυτή, πρέπει στο πλαίσιο του Internet of Things να τεθεί μια σειρά βασικών ερωτημάτων, κατά την επανεξέταση των μοντέλων διαδικτυακής προστασίας της ιδιωτικής ζωής. Ορισμένα από τα **ερωτήματα που τίθενται** έχουν ως εξής:

- Στα πλαίσια του IoT, ποια σχέση αναπτύσσεται στην αγορά μεταξύ των πηγών από τις οποίες προέρχονται τα δεδομένα και των συλλεκτών των δεδομένων αυτών και πως μπορούν να επιλυθούν ζητήματα που ανακύπτουν από τη σχέση αυτή;
- Τα προσωπικά δεδομένα έχουν τόσο προσωπική όσο και εμπορική αξία, η οποία εκτιμάται διαφορετικά από τις πηγές που προέρχονται τα στοιχεία και διαφορετικά από αυτούς που τα συλλέγουν. Η διαφορετική αξιακή προσέγγιση των δύο μερών αφορά τα στοιχεία τόσο μεμονωμένα όσο και συνολικά. Και τα

δύο μέρη έχουν νόμιμα συμφέροντα που μπορεί να συγκρούονται. Τίθεται λοιπόν ο προβληματισμός, πώς αυτά τα ξεχωριστά συμφέροντα θα συγκλίνουν κατά τρόπο που να οδηγηθούμε σε δίκαιους και συνεκτικούς κανόνες αποδεκτούς από τις πηγές και από τους συλλέκτες, που θα διέπουν την πρόσβαση, τον έλεγχο, τη διαφάνεια και την προστασία;

- Πώς μπορούν στο πλαίσιο του Διαδικτύου των Αντικειμένων οι πολιτικές και οι πρακτικές απορρήτου να είναι άμεσα διαθέσιμες και κατανοητές;
- Ποιες είναι οι εναλλακτικές λύσεις που προτείνονται έναντι του παραδοσιακού μοντέλου προστασίας του απορρήτου «Ειδοποίηση και Συναίνεση», για μια διαφορετική αντιμετώπιση των μοναδικών πτυχών του Διαδικτύου των Πραγμάτων (IoT);
- Ποιο είναι ένα αποτελεσματικό μοντέλο για την έκφραση, την εφαρμογή και την επιβολή τόσο των προσωπικών προτιμήσεων περί απορρήτων, όσο και των συλλογικών από πολλαπλά μέρη (multi-party) προτιμήσεων; Θα μπορούσε πραγματικά να κατασκευαστεί ένα τέτοιο μοντέλο και, αν ναι, πώς θα μοιάζει; Πώς θα μπορούσε αυτό να εφαρμοστεί σε συγκεκριμένες περιστάσεις που αφορούν μεμονωμένες προτιμήσεις απορρήτου;
- Υπάρχει αγορά για την εξωτερική ανάθεση (outsourcing) της διαχείρισης των ρυθμίσεων απορρήτου σε εμπορικές υπηρεσίες που έχουν σχεδιαστεί (αποσκοπούν) να θέτουν τις προτιμήσεις των χρηστών σε ισχύ;
- Έχει σχεδιαστεί ρόλος για έναν «πληρεξούσιο» (εξουσιοδοτημένο proxy) επί της προστασίας των προσωπικών δεδομένων, ο οποίος θα εκφράζει και θα επιβάλλει τις προτιμήσεις ενός χρήστη σε μια σειρά συσκευών, εξαλείφοντας έτσι την ανάγκη της άμεσης αλληλεπίδρασης μεταξύ του χρήστη και κάθε μίας από αυτές τις συσκευές;
- Τα πρότυπα και οι προσδοκίες για την προστασία της ιδιωτικής ζωής συνδέονται στενά με το κοινωνικό και πολιτιστικό πλαίσιο του κάθε χρήστη. Το πλαίσιο αυτό ποικίλλει από μια εντοπισμένη ομάδα ή ένα έθνος σε κάποια άλλη ομάδα ή έθνος. Πολλά σενάρια IoT περιλαμβάνουν δραστηριότητες ανάπτυξης συσκευών και συλλογής δεδομένων με πολυεθνική ή παγκόσμια εμβέλεια που διαπερνούν τα κοινωνικά και πολιτισμικά σύνορα. Γεννιέται λοιπόν εδώ ο προβληματισμός τι σημαίνει αυτό για την ανάπτυξη ενός ευρέως

εφαρμόσιμου προτύπου προστασίας της ιδιωτικής ζωής για το Διαδίκτυο των Πραγμάτων;

- Πώς μπορούν να προσαρμοστούν οι συσκευές και τα συστήματα IoT ώστε να αναγνωρίζουν και να σέβονται ολόκληρο το φάσμα των προσδοκιών των χρηστών, για την προστασία της ιδιωτικής τους ζωής, καθώς και τους διαφορετικούς νόμους που ισχύουν σε κάθε τόπο;
- Πως μπορούν να ενθαρρυνθούν οι κατασκευαστές IoT συσκευών να ενσωματώσουν από τη φάση του σχεδιασμού, τις βασικές αρχές προστασίας του απορρήτου της ιδιωτικής ζωής, στις δικές τους βασικές αξίες;
- Πώς θα ενθαρρυνθεί η συμπερίληψη του προβληματισμού γύρω από την ασφάλεια και την προστασία της ιδιωτικής ζωής των καταναλωτών, στη κάθε φάση ανάπτυξης και λειτουργίας του προϊόντος;
- Πώς θα συνδυαστεί η λειτουργικότητα με τις απαιτήσεις περί απορρήτου;
- Κατ 'αρχήν, οι κατασκευαστές πρέπει να αναμένουν ότι τα προϊόντα και οι πρακτικές που σέβονται την προστασία της ιδιωτικής ζωής, οικοδομούν τη μακροπρόθεσμη εμπιστοσύνη με τους πελάτες, δημιουργούν την ικανοποίηση των πελατών και ενισχύουν την πίστη τους προς το σήμα της εταιρίας (customer loyalty). Είναι όμως αυτό ένα αρκετά σημαντικό κίνητρο αν τεθεί απέναντι στις ανταγωνιστικές επιθυμίες για απλότητα σχεδιασμού και ταχύτητα στην αγορά;
- Πρέπει να σχεδιάζονται συσκευές με προεπιλεγμένες ρυθμίσεις που έχουν διαμορφωθεί (ρυθμιστεί) για τον πιο συντηρητικό τρόπο συλλογής δεδομένων (δηλ. να αποκλεισθεί η από προεπιλογή, συλλογή δεδομένων);
- Πώς πρέπει να προστατεύσουμε τα δεδομένα που συλλέχθηκαν από το Διαδίκτυο και φαίνεται να μην είναι προσωπικά στο σημείο συλλογής ή έχουν «αποχαρακτηριστεί», αλλά μπορεί σε κάποιο σημείο στο μέλλον να γίνουν προσωπικά δεδομένα (επειδή τα δεδομένα μπορούν να επαναπροσδιοριστούν ή να συνδυαστούν με άλλα δεδομένα);

Το Internet of Things δημιουργεί μοναδικές προκλήσεις στην προστασία της ιδιωτικής ζωής, που υπερβαίνουν τα ζητήματα της προστασίας των προσωπικών δεδομένων που υπάρχουν σήμερα. Εκ του λόγου αυτού αλλά και επειδή η κατάσταση εξελίσσεται δυναμικά, πρέπει να αναπτυχθούν στρατηγικές που να σέβονται τις επιμέρους επιλογές διαφύλαξης της ιδιωτικής ζωής σε ένα ευρύ φάσμα προσδοκιών, ενώ ταυτόχρονα θα ευνοούν την καινοτομία στη νέα τεχνολογία του IoT.

3.6 ΔΙΕΥΡΥΝΣΗ ΤΟΥ IoT-ΕΠΙΠΕΔΟ ΣΥΣΚΕΥΩΝ-ΤΡΩΤΟΤΗΤΑ

Ο όρος ασφάλεια περιλαμβάνει ένα ευρύ φάσμα διαφορετικών εννοιών. Αναφέρεται στη βασική παροχή υπηρεσιών ασφαλείας, συμπεριλαμβανομένης της εμπιστευτικότητας, της γνησιότητας, της ακεραιότητας, της εξουσιοδότησης, της μη άρνησης και της διαθεσιμότητας. Αυτές οι υπηρεσίες ασφαλείας μπορούν να υλοποιηθούν μέσω διαφορετικών κρυπτογραφικών μηχανισμών, όπως κρυπτογράφηση μπλοκ (αλγόριθμος που κρυπτογραφεί χύδην δεδομένα, λειτουργώντας σε ομάδες δυαδικών ψηφίων σταθερού μήκους, Block Ciphers), λειτουργίες κατακερματισμού (hash functions) ή αλγόριθμοι υπογραφής (πρότυπο επεξεργασίας πληροφοριών για ψηφιακές υπογραφές, signature algorithms). Για καθέναν από αυτούς τους μηχανισμούς, μια συμπαγής βασική υποδομή διαχείρισης κλειδιών είναι θεμελιώδης για τη διαχείριση/χειρισμό των απαιτούμενων κρυπτογραφικών κλειδιών.

Η διασφάλιση της αξιοπιστίας, της ευελιξίας, της ασφάλειας και της σταθερότητας των εφαρμογών και των υπηρεσιών, είναι ζωτικής σημασίας για την προώθηση της εμπιστοσύνης στη χρήση του Διαδικτύου. Οι χρήστες του Διαδικτύου πρέπει να αισθάνονται υψηλό βαθμό εμπιστοσύνης. Να θεωρούν ότι το Διαδίκτυο, οι εφαρμογές του και οι συνδεδεμένες με αυτό συσκευές είναι αρκετά ασφαλείς, ώστε να επιτελούν τα είδη δραστηριοτήτων που απαιτούνται σε σχέση με την ανοχή του κινδύνου που συνδέεται με τις δραστηριότητες αυτές.

Το Internet of Things δεν διαφέρει από αυτή την άποψη και η ασφάλεια σε αυτό είναι ουσιωδώς συνδεδεμένη με την ικανότητα των χρηστών να εμπιστεύονται το περιβάλλον τους. Αν οι άνθρωποι δεν πιστεύουν ότι οι συνδεδεμένες συσκευές τους και οι πληροφορίες τους είναι λογικά ασφαλείς από κακή χρήση ή βλάβη, προκαλείται διάβρωση της εμπιστοσύνης τους, με επακόλουθο την απροθυμία χρήσης του Διαδικτύου. Αυτό έχει παγκόσμιες συνέπειες, για το ηλεκτρονικό εμπόριο, τη τεχνολογική καινοτομία, την ελευθερία του λόγου και σχεδόν κάθε άλλη πτυχή των online δραστηριοτήτων. Πράγματι, η διασφάλιση των συνθηκών αξιοπιστίας και ασφάλειας στα προϊόντα και τις υπηρεσίες του διαδικτύου θα πρέπει να θεωρείται κορυφαία προτεραιότητα για τον τομέα.

Καθώς όλο και περισσότερες συσκευές συνδέονται στο Διαδίκτυο, εμφανίζονται νέες ευκαιρίες για βελτίωση των πιθανών τρωτών σημείων ασφαλείας που προκύπτουν. Τα κενά ασφαλείας μπορεί να οφείλονται σε διάφορες αιτίες και εκεί είναι που πρέπει να γίνεται η εστίαση και η παρέμβαση. Έτσι ενδεικτικά μπορούμε να αναφέρουμε:

1. Χαμηλού επιπέδου ασφάλειας IoT συσκευές, θα μπορούσαν να αποτελέσουν στην περίπτωση εκδήλωσης Κυβερνοεπιθέσεων (Cyber attacks), τα σημεία εισόδου, επιτρέποντας σε κακόβουλα άτομα να επαναπρογραμματίσουν μια συσκευή ή να προκαλέσουν κάποια δυσλειτουργία.

2. Οι κακώς σχεδιαζόμενες συσκευές μπορούν να αφήσουν τα δεδομένα ενός χρήστη εκτεθειμένα σε κλοπή, έχοντας τις ροές δεδομένων (stream data) ανεπαρκώς προστατευμένες.

3. Η αποτυχία ή η δυσλειτουργία των ίδιων των συσκευών μπορεί επίσης να δημιουργήσει ευπάθειες στην ασφάλεια και την αξιοπιστία.

Αυτά τα προβλήματα είναι εξίσου μεγάλα ή ακόμη μεγαλύτερα για τις μικρές, φθηνές και ευρέως διαδεδομένες (πανταχού παρούσες) έξυπνες συσκευές του Διαδικτύου των Αντικειμένων, όπως για τους υπολογιστές που παραδοσιακά αποτελούσαν τα τελικά σημεία σύνδεσης στο Internet. Ανταγωνιστικά κόστη και τεχνικοί περιορισμοί στις IoT συσκευές προκαλούν τους κατασκευαστές τους να σχεδιάζουν χαρακτηριστικά ασφαλείας είτε ανεπαρκή είτε ακόμη και ακατάλληλα για αυτές τις συσκευές, δημιουργώντας έτσι πιθανώς μακροχρόνια διατηρήσιμα προβλήματα και ευπάθειες ασφαλείας, μεγαλύτερα από τους αντίστοιχους παραδοσιακούς υπολογιστές.

Μαζί με πιθανές ανεπάρκειες του σχεδιασμού ασφάλειας που προαναφέρθηκαν, η απόλυτη αύξηση του αριθμού των συσκευών IoT αλλά και η φύση αυτών, θα μπορούσε να αυξήσει τις δυνατότητες και τις πιθανότητες επίθεσης. Όταν συνδυάζεται ο εξαιρετικά υψηλός βαθμός διασύνδεσης των IoT συσκευών – λόγω της φύσης τους – με χαμηλά επίπεδα ασφάλειας, εμφανίζονται προβλήματα. Κάθε μη ασφαλής συσκευή που είναι συνδεδεμένη online, επηρεάζει ενδεχομένως την ασφάλεια και την ανθεκτικότητα του Διαδικτύου όχι μόνο τοπικά, αλλά και σε παγκόσμιο επίπεδο. Για παράδειγμα, ένα μη προστατευμένο ψυγείο ή τηλεόραση στις ΗΠΑ που είναι μολυσμένο με κακόβουλο λογισμικό, ενδέχεται να στείλει χιλιάδες ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου σε παραλήπτες παγκοσμίως, χρησιμοποιώντας τη σύνδεση Internet Wi-Fi στο σπίτι του ιδιοκτήτη.

Μέρα με τη μέρα, οι άνθρωποι γίνονται πιο συνδεδεμένοι και εξαρτώμενοι από IoT συσκευές για βασικές υπηρεσίες. Η εξέλιξη αυτή απαιτεί οι συσκευές που χρησιμοποιούνται να είναι ασφαλείς, έστω και αν ευρέως αναγνωρίζεται ότι καμία συσκευή δεν μπορεί να είναι απόλυτα ασφαλής. Αυτό το αυξανόμενο επίπεδο εξάρτησης των ανθρώπων από τις συσκευές IoT και τις υπηρεσίες Internet με τις οποίες αυτές αλληλεπιδρούν, αυξάνει επίσης τις διαδρομές για τους παραβάτες (pathways for wrongdoers) και κατά συνέπεια τις πιθανότητες, αυτοί να αποκτήσουν πρόσβαση στις συσκευές. Ίσως θα μπορούσαμε να αποσυνδέσουμε τις τηλεοράσεις που έχουν συνδεθεί με το Διαδίκτυο και έχουν πληγεί από κυβερνοεπιθέσεις, όμως δεν είναι εύκολο να απενεργοποιήσουμε έναν έξυπνο μετρητή ισχύος ή ένα σύστημα ελέγχου κυκλοφορίας ή ένα εμφυτευμένο βηματοδότη εάν πέσουν θύματα κακόβουλης συμπεριφοράς. Αυτός είναι ο λόγος για τον οποίο η ασφάλεια των IoT συσκευών και υπηρεσιών είναι μείζονος σημαντικότητας σημείο συζητήσεων και πρέπει να θεωρείται κρίσιμο ζήτημα. Όλο και περισσότερο εξαρτόμαστε από αυτές τις συσκευές για ουσιώδεις υπηρεσίες, έτσι η συμπεριφορά τους μπορεί να έχει παγκόσμια εμβέλεια και αντίκτυπο.

Όταν οι σκέψεις μας και οι ενέργειές μας αφορούν το Internet of Things και τις συσκευές που λειτουργού σε αυτό, είναι πολύ σημαντικό να κατανοούμε πως η ασφάλεια που παρέχεται δεν είναι απόλυτη. Η ασφάλεια των συσκευών IoT δεν αποτελεί δυαδική πρόταση ή διωνυμική επιλογή μεταξύ του ασφαλούς ή ανασφαλούς. Αντίθετα, είναι χρήσιμο να αντιλαμβανόμαστε την ασφάλεια του IoT ως ένα φάσμα ευπάθειας συσκευών. Το φάσμα αυτό κυμαίνεται από ολοκληρωτικά μη προστατευμένες συσκευές που δεν διαθέτουν χαρακτηριστικά ασφαλείας, μέχρι συστήματα υψηλής διασφάλισης με πολυεπίπεδα χαρακτηριστικά ασφαλείας. Σε ένα ατέρμονο παιχνίδι «γάτας και ποντικού» εξελίσσονται νέες απειλές κατά της ασφάλειας και οι κατασκευαστές συσκευών και οι φορείς εκμετάλλευσης δικτύων ανταποκρίνονται συνεχώς, για να αντιμετωπίσουν τις νέες αυτές απειλές.

Η συνολική ασφάλεια και η ανθεκτικότητα του Internet of Things αποτελεί συνάρτηση του τρόπου αξιολόγησης και διαχείρισης των κινδύνων ασφαλείας. Η ασφάλεια μιας συσκευής είναι συνάρτηση του κινδύνου ότι θα παραβιαστεί η συσκευή, της ζημιάς που θα προκαλέσει η παραβίαση και του χρόνου καθώς και των πόρων που απαιτούνται για την επίτευξη ενός συγκεκριμένου επιπέδου προστασίας.

Εάν ένας χρήστης απαιτεί ασφάλεια και δεν μπορεί να ανεχθεί την έκθεση σε υψηλό βαθμό κινδύνου, όπως συμβαίνει στην περίπτωση του χειριστή ενός

συστήματος ελέγχου κυκλοφορίας ή ενός ατόμου με εμφυτευμένη ιατρική συσκευή που έχει δυνατότητα σύνδεσης στο Internet, μπορεί να αντιλαμβάνεται ως δικαιολογημένη μια δαπάνη σημαντικών πόρων για την προστασία του συστήματος ή της συσκευής από ενδεχόμενη επίθεση. Ομοίως, εάν ο χρήστης δεν ανησυχεί από το γεγονός ότι το «έξυπνο» ψυγείο του μπορεί να πληγεί κακόβουλα και να χρησιμοποιηθεί για την αποστολή ανεπιθύμητων μηνυμάτων (spam), τότε μπορεί να μην θεωρεί ότι είναι υποχρεωμένος να πληρώσει για ένα μοντέλο με πιο εξελιγμένο σχεδιασμό ασφαλείας, που κάνει τη συσκευή του πιο δαπανηρή και περίπλοκη.

Διάφοροι παράγοντες είναι αυτοί που επηρεάζουν τον υπολογισμό του κινδύνου καθώς και τον υπολογισμό του μετριασμού του κινδύνου. Οι παράγοντες περιλαμβάνουν:

- Τη σαφή κατανόηση των σημερινών κινδύνων για την ασφάλεια
- Τους πιθανούς μελλοντικούς κινδύνους
- Το εκτιμώμενο οικονομικό ή άλλο κόστος μιας βλάβης σε περίπτωση επέλευσης των κινδύνων και
- Το εκτιμώμενο κόστος για τον μετριασμό των κινδύνων.

Ενώ τέτοιου είδους εξισορροπήσεις ασφαλείας-κινδύνου γίνονται συχνά από μεμονωμένο χρήστη ή είναι οργανωσιακής προέλευσης, είναι σημαντικό επίσης να εξετάζεται η αλληλεξάρτηση των IoT συσκευών ως μέρος ενός μεγαλύτερου οικοσυστήματος IoT. Η δικτυακή συνδεσιμότητα συσκευών IoT σημαίνει ότι οι αποφάσεις ασφαλείας που υλοποιούνται τοπικά - σχετικά με μια συσκευή IoT - μπορούν να έχουν επιπτώσεις σε άλλες συσκευές σε παγκόσμιο επίπεδο. Σαν θέμα αρχών, οι υπεύθυνοι για την ανάπτυξη έξυπνων αντικειμένων προοριζόμενων για το Internet of Things, έχουν υποχρέωση να διασφαλίζουν ότι οι συσκευές αυτές δεν εκθέτουν ούτε τους δικούς τους χρήστες, ούτε άλλους χρήστες σε ενδεχόμενη βλάβη.

Από οικονομικής ή επιχειρηματικής άποψης οι πωλητές των συσκευών έχουν συμφέρον να μειώσουν το κόστος, την πολυπλοκότητα και το χρόνο τους στην αγορά. Για παράδειγμα, οι συσκευές IoT που αποτελούν εξαρτήματα μεγάλου όγκου παραγωγής (high volume components), και χαμηλού περιθωρίου κέρδους (low margin) και που ήδη αντιπροσωπεύουν ένα κόστος που προστίθεται σε αυτό του προϊόντος στο οποίο είναι ενσωματωμένα, γίνονται αρκετά συνηθισμένα. Η προσθήκη περισσότερης μνήμης και ο ταχύτερος επεξεργαστής για την εφαρμογή ή την επαύξηση των μέτρων

ασφαλείας, θα μπορούσαν εύκολα να καταστήσουν αυτό το προϊόν εμπορικά μη ανταγωνιστικό.

Από οικονομικής άποψης, το έλλειμμα ασφάλειας στις IoT συσκευές έχει ως αποτέλεσμα μια αρνητική εξωτερίκευση, όπου το κόστος επιβάλλεται από το ένα μέρος (ή μέρη) σε άλλο μέρος ή άλλα μέρη. Κλασικό παράδειγμα αποτελεί η ρύπανση του περιβάλλοντος, όπου ενώ κάποιοι με τις δραστηριότητές τους επιβαρύνουν το περιβάλλον μολύνοντάς το, το κόστος αποκατάστασης (αρνητική εξωτερίκευση) των πράξεων αυτών που ρυπαίνουν, βαρύνουν άλλα μέρη. Το ζήτημα είναι πως το κόστος που εξωτερικεύεται και τελικά επιβάλλεται στους άλλους, δεν συμπεριλαμβάνεται κανονικά στη διαδικασία λήψης αποφάσεων, εκτός αν - όπως συμβαίνει στην περίπτωση της ρύπανσης - επιβάλλεται φόρος σ' αυτόν που ρυπαίνει, προκειμένου να αναγκαστεί να μειώσει την ποσότητα των ρύπων.

Στην περίπτωση της ασφάλειας πληροφοριών, όπως συζητείται από τον Bruce Schneier, ανακύπτει μια κατάσταση εξωτερίκευσης όταν ο πωλητής που δημιουργεί το προϊόν δεν φέρει το κόστος που προκαλείται από οποιαδήποτε ανασφάλεια. Στην περίπτωση αυτή, ο νόμος περί ευθύνης, μπορεί να επηρεάσει τους πωλητές ώστε να λογοδοτήσουν για την εξωτερίκευση και να αναπτύξουν περισσότερα προϊόντα ασφαλείας.

Οι συσκευές IoT τείνουν να διαφέρουν από τους παραδοσιακούς υπολογιστές και τις υπολογιστικές εν γένει συσκευές σε σημαντικά σημεία που προκαλούν ζητήματα ασφαλείας:

1. Πολλές συσκευές του Internet of Things, όπως αισθητήρες και άλλα καταναλωτικά προϊόντα, έχουν σχεδιαστεί για να αναπτυχθούν σε τεράστιες κλίμακες, που είναι τάξεις μεγέθους πέρα από εκείνες των παραδοσιακών συσκευών που συνδέονται στο Διαδίκτυο. Ως αποτέλεσμα, η δυνητική ποσότητα διασυνδέσεων μεταξύ αυτών των συσκευών αποδεικνύεται πρωτοφανής.

2. Πολλές από τις ως άνω συσκευές θα είναι σε θέση να δημιουργήσουν συνδέσμους και να επικοινωνούν με άλλες συσκευές από μόνες τους με έναν απρόβλεπτο και δυναμικό τρόπο. Ως εκ τούτου, τα υπάρχοντα εργαλεία, οι μέθοδοι και οι στρατηγικές που σχετίζονται με την ασφάλεια του IoT ίσως χρειαστούν μια νέα εκτίμηση.

3. Πολλές εφαρμογές IoT θα αποτελούνται από συλλογές όμοιων ή σχεδόν πανομοιότυπων συσκευών. Αυτή η ομοιογένεια μεγεθύνει τις πιθανές επιπτώσεις οποιασδήποτε τρωτότητας της ασφάλειας, από τον απόλυτο αριθμό των συσκευών που

έχουν όλες τα ίδια χαρακτηριστικά. Για παράδειγμα, η ευπάθεια του πρωτοκόλλου επικοινωνίας μιας εταιρικής μάρκας λαμπτήρων με δυνατότητα σύνδεσης στο Internet, μπορεί να επεκταθεί σε κάθε μάρκα και μοντέλο κάποιας συσκευής που χρησιμοποιεί το ίδιο πρωτόκολλο ή που μοιράζεται τα ίδια βασικά σχεδιαστικά ή κατασκευαστικά χαρακτηριστικά.

4. Πολλές συσκευές Internet of Things θα αναπτυχθούν με μια αναμενόμενη διάρκεια ζωής πολύ μεγαλύτερου χρόνου, από αυτόν που συνήθως σχετίζεται με τον εξοπλισμό υψηλής τεχνολογίας. Επιπλέον, αυτές οι συσκευές ενδέχεται να αναπτυχθούν σε συνθήκες που καθιστούν δύσκολη ή αδύνατη την αναδιάταξη ή την αναβάθμισή τους. ή αυτές οι συσκευές ενδέχεται να επιβιώσουν περισσότερο χρόνο από ότι η εταιρεία που τις δημιούργησε, η οποία με τον τερματισμό της λειτουργίας της αφήνει ορφανές συσκευές χωρίς μέσα και υπηρεσίες μακροπρόθεσμης υποστήριξης.

5, Αυτά τα σενάρια καταδεικνύουν ότι οι μηχανισμοί ασφαλείας που είναι επαρκείς κατά τη φάση της ανάπτυξης ενδέχεται να μην επαρκούν για την πλήρη διάρκεια ζωής της συσκευής καθώς οι απειλές ασφάλειας εξελίσσονται διαρκώς. Ως εκ τούτου, αυτό μπορεί να δημιουργήσει ευπάθειες που θα μπορούσαν να παραμείνουν για μεγάλο χρονικό διάστημα. Αυτό έρχεται σε αντίθεση με το πρότυπο των παραδοσιακών συστημάτων ηλεκτρονικών υπολογιστών τα οποία αναβαθμίζονται κανονικά, με ενημερώσεις του λογισμικού λειτουργικού συστήματός τους καθ 'όλη τη διάρκεια ζωής του υπολογιστή, για την αντιμετώπιση των απειλών κατά της ασφάλειας. Η μακροπρόθεσμη υποστήριξη και διαχείριση των συσκευών IoT αποτελεί σημαντική πρόκληση για την ασφάλεια.

6. Πολλές συσκευές IoT σχεδιάζονται σκόπιμα χωρίς καμία δυνατότητα αναβάθμισης ή η διαδικασία αναβάθμισής τους είναι δυσκίνητη ή μη πρακτική. Για παράδειγμα το 2015 Fiat Chrysler αναγκάστηκε να ανακαλέσει 1,4 εκατομμύρια οχήματα προκειμένου να διορθώσει μια ευπάθεια που επέτρεπε σε έναν εισβολέα να πλήξει ασύρματα το όχημα. Αυτά τα αυτοκίνητα έπρεπε να μεταφερθούν σε έναν αντιπρόσωπο της Fiat Chrysler για manual αναβάθμιση ή ο ίδιος ο ιδιοκτήτης έπρεπε να εκτελέσει την ίδια την αναβάθμιση με ένα κλειδί USB. Η πραγματικότητα είναι ότι ένα υψηλό ποσοστό αυτών των αυτοκινήτων πιθανώς δεν θα αναβαθμιστεί ποτέ, επειδή η διαδικασία αναβάθμισης παρουσιάζει προβλήματα για τους ιδιοκτήτες, αφήνοντάς τους συνεχώς ευάλωτους σε απειλές κυβερνοασφάλειας, ειδικά όταν το αυτοκίνητο φαίνεται να έχει καλές επιδόσεις.

7. Πολλές συσκευές IoT λειτουργούν με τρόπο που ο χρήστης έχει ελάχιστη ή και καθόλου πραγματική αντίληψη για την εσωτερική λειτουργία τους ή τις ακριβείς ροές δεδομένων που αυτές παράγουν. Αυτό δημιουργεί ένα θέμα ευπάθειας στην ασφάλεια, όταν ένας χρήστης πιστεύει ότι μια συσκευή IoT εκτελεί ορισμένες λειτουργίες, ενώ στην πραγματικότητα αυτή μπορεί να εκτελεί και άλλες ανεπιθύμητες λειτουργίες ή να συλλέγει περισσότερα δεδομένα από αυτά που σκόπευε ο χρήστης.

8. Οι λειτουργίες μιας συσκευής θα μπορούσαν επίσης να αλλάξουν χωρίς προειδοποίηση όταν ο κατασκευαστής παρέχει μια ενημέρωση, αφήνοντας έτσι το χρήστη ευάλωτο, στις αλλαγές που ο ίδιος ο κατασκευαστής με αυτόν τον τρόπο έχει επιλέξει να κάνει.

9. Ορισμένες συσκευές IoT είναι πιθανό να αναπτυχθούν σε χώρους όπου η φυσική ασφάλεια είναι δύσκολη ή αδύνατη. Οι επιτιθέμενοι μπορεί να έχουν άμεση φυσική πρόσβαση σε συσκευές IoT. Εδώ θα πρέπει να ληφθούν υπόψη τα χαρακτηριστικά αντιμετώπισης/προστασίας (Anti tamper) από παραβιάσεις, καθώς και άλλες καινοτομίες σχεδιασμού για την υλοποίηση της ασφάλειας.

3.7 ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

3.7.1 Γενικά

Υπάρχουν πολλές προκλήσεις για την ανάπτυξη της ασφαλούς υλοποίησης του Διαδικτύου των Αντικειμένων και πολλές από τις υφιστάμενες στην αγορά τεχνολογίες ασφάλειας, αναμένεται να διαδραματίσουν ένα σημαντικό ρόλο στην άμβλυνση των IoT κινδύνων μέσα σε μια επιχείρηση.

Ωστόσο, το IoT εισάγει νέες προκλήσεις για την μηχανική της ασφάλειας. Πολλές από αυτές θα επωφεληθούν από την στοχευμένη έρευνα ή τη βιομηχανική συνεργασία, προκειμένου να προσδιοριστούν οι βέλτιστες μακροπρόθεσμες προσεγγίσεις για την επίλυση των σχετικών ζητημάτων ασφάλειας.

3.7.2 Πολύπλοκες διαμορφώσεις λόγω κακής σχεδίασης συστημάτων

Το Internet of Things περιλαμβάνει edge devices, πρωτόκολλα μηνυμάτων, πρωτόκολλα μεταφοράς, διεπαφές προγραμματισμού εφαρμογών (application programming interfaces - APIs), αναλύσεις δεδομένων, αποθήκευση, λογισμικό και διάφορες άλλες τεχνολογικές έννοιες. Πολλά συστήματα IoT είναι κακώς σχεδιασμένα και υλοποιημένα, χρησιμοποιώντας ποικίλα πρωτόκολλα και τεχνολογίες που δημιουργούν πολύπλοκες διαμορφώσεις. Οι συσκευές edge είναι αφ' εαυτού πολύπλοκες συσκευές, αποτελούνται από πολλαπλά επίπεδα τεχνολογίας και απαιτούν τη κατανόηση του hardware υλικού, του firmware, του λογισμικού και μιας πληθώρας πρωτοκόλλων. Όλα αυτά μπορούν να εφαρμοστούν σε μυριάδες περιπτώσεων, σε πολλές βιομηχανίες.

Πριν ασφαλίσουμε ένα σύστημα, είναι σημαντικό να κατανοήσουμε πρώτα τις λειτουργικές και τεχνολογικές του λεπτομέρειες που πρέπει να διασφαλιστούν. Αυτό θα απαιτήσει από τους μηχανικούς ασφαλείας να συνεργαστούν στενά με αυτούς που σχεδιάζουν και αναπτύσσουν τις ικανότητες του IoT, ώστε οι απαιτήσεις ασφαλείας να καθοριστούν και να εισαχθούν νωρίς κατά τη διαδικασία σχεδιασμού του συστήματος. Προς τούτο, προτείνεται η χρήση μιας μεθοδικής προσέγγισης της μηχανικής της ασφαλείας των συστημάτων, για κάθε IoT εφαρμογή εντός μιας επιχείρησης.

Η υιοθέτηση μιας προσέγγισης μηχανικής ασφαλείας συστημάτων για τις εφαρμογές IoT, επιτρέπει στους σχεδιαστές να εντοπίζουν περιοχές πολυπλοκότητας που μπορούν να απλοποιηθούν. Σαν παράδειγμα μπορούμε να αναφέρουμε τον περιορισμό του αριθμού των πρωτοκόλλων και των διεπαφών όσο αυτό είναι δυνατό.

3.7.3 Ελλείψεις ώριμων IoT τεχνολογιών

Τα πρότυπα υποστήριξης του IoT δεν έχουν ακόμη αναπτυχθεί πλήρως, αφήνοντας την αγορά ανοικτή σε ανταγωνιστικές πλατφόρμες, πρωτόκολλα και διεπαφές. Αυτή η έλλειψη προτύπων οδηγεί σε αυξημένη πολυπλοκότητα που μπορεί να δημιουργήσει τρωτά σημεία και παρέχει στους επιτιθέμενους έναν τρόπο να διεισδύσουν στην επιχείρηση.

3.7.4 Περιορισμένη καθοδήγηση για ασφαλή ρύθμιση

Η καθοδήγηση σχετικά με την ασφαλή ρύθμιση των λειτουργικών συστημάτων περιορισμένων δυνατοτήτων είναι από περιορισμένη έως ανύπαρκτη. Περιορισμένη είναι η καθοδήγηση κατά βάση για τη συντήρηση και τη διαχείριση του κύκλου ζωής των συσκευών IoT.

Η εκτέλεση αναβαθμίσεων firmware, λογισμικού και patch ενημερώσεων για IoT συσκευές απαιτεί μια νέα προσέγγιση που θα προβλέπει υποχρεώσεις, ευθύνες και ενέργειες σε όλη την αλυσίδα παραγωγής. Τα IoT περιουσιακά στοιχεία ενός οργανισμού πρέπει να είναι σε θέση να συνεχίσουν να λαμβάνουν ενημερωμένες εκδόσεις κώδικα και ενημερώσεις λογισμικού καθ ' όλη τη διάρκεια του κύκλου ζωής τους. Διότι εάν οι συσκευές IoT μένουν πίσω από τις απαιτούμενες ενημερώσεις ασφαλείας, θα είναι πολύ πιο εύκολο για τους εισβολείς να εκμεταλλευτούν τα κενά ασφαλείας και να υλοποιήσουν τα κακόβουλα σχέδιά τους. Από την άποψη αυτή, οι οργανισμοί θα πρέπει να εξετάσουν την πιθανότητα οι συσκευές IoT τελικά να μην υποστηριχθούν, δεδομένου ότι οι ημερομηνίες σταδιακής κατάργησης τίθενται σε ισχύ από τον κάθε πωλητή.

Η παρακολούθηση των IoT συσκευών, καθώς και του λογισμικού και του firmware σε κάθε συσκευή, είναι επίσης ένα ζήτημα. Ο αριθμός των συσκευών IoT αποτελεί από μόνος του μια πρόκληση για την αποτελεσματική διαχείρισή τους.

3.7.5 Προβλήματα φυσικής ασφάλειας

Το Internet of Things εισάγει ένα προβληματισμό γύρω από τα θέματα φυσικής ασφάλειας, επειδή πολλές από τις IoT edge devices θα αναπτυχθούν σε εκτεθειμένα περιβάλλοντα, επιτρέποντας έτσι στους επιτιθέμενους να τις «αποκτήσουν» πιο εύκολα για περαιτέρω εργαστηριακή ανάλυση. Οι επιτιθέμενοι που διαθέτουν επαρκείς πόρους, μπορούν να υλοποιήσουν ένα reverse engineer επ’ αυτών των συσκευών για να πετύχουν το αποτέλεσμα που επιδιώκουν.

Σε ιδανική περίπτωση για την αντιμετώπιση επιθέσεων, θα μπορούσε να γίνει χρήση μέσων προστασίας ανθεκτικών στις παραβιάσεις, ωστόσο τέτοιο δεν είναι πάντα εφικτό. Το γεγονός ότι πλήθος IoT εφαρμογών επιζητά και χρησιμοποιεί πολύ χαμηλού κόστους συσκευές, προκαλεί σύγκρουση μεταξύ της ικανότητας των συσκευών αυτών να αντέχουν σε επιθέσεις και παραβιάσεις και των περιοριστικών οικονομικών παραμέτρων που τίθενται.

3.7.6 Λοιπά θέματα ασφαλείας

Τα θέματα σχετικά με τους κινδύνους για την προστασία της ιδιωτικής ζωής στο Διαδίκτυο των Αντικειμένων είναι πολύπλοκα και όχι πάντα προφανή. Επίσης κάποια ζητήματα δεν είναι εύκολα αναγνωρίσιμα ενώ κάποια άλλα δεν μπορούν να επιλυθούν με την απλή επιβολή μέτρων προστασίας της εμπιστευτικότητας, της ταυτότητας ή της τοποθεσίας κατά τις συναλλαγές.

3.7.6.1 Η διαθεσιμότητα των βέλτιστων πρακτικών

Η διαθεσιμότητα των βέλτιστων πρακτικών για όσους σχεδιάζουν και αναπτύσσουν το Internet of Things είναι περιορισμένη. Πολλοί από αυτούς (developers) δεν έχουν ακόμη εξοικειωθεί με τις βέλτιστες πρακτικές ασφαλούς ανάπτυξης και επέκτασης. Η βιασύνη που επιδεικνύεται στη δημιουργία νέων, βασισμένων στο IoT δυνατοτήτων, θα οδηγήσει πιθανώς σε περιορισμένη εστίαση στην ασφάλεια της νέας λειτουργικότητας που δημιουργείται.

3.7.6.2 Ελλείψεις προτύπων

Υπάρχει έλλειψη προτύπων για τον έλεγχο ταυτότητας και την εξουσιοδότηση των IoT edge devices. Η απαίτηση για συσκευές χαμηλής κατανάλωσης καθώς και φορητές wearable συσκευές φέρνει μια πληθώρα νέων, απλούστερων ασύρματων πρωτοκόλλων, τα οποία συχνά δημιουργούν ένα πλέγμα μεταξύ τους (συνδέονται) χωρίς όμως να εφαρμόζουν κάποια ώριμη και ασφαλή κρυπτογράφηση και έναν ώριμο και ασφαλή έλεγχο ταυτότητας. Τα πρωτόκολλα αυτά μπορούν να επιτεθούν «on the fly» και χωρίς φυσική επαφή.

Ορισμένες συσκευές IoT δεν διαθέτουν δυνατότητες ελέγχου ταυτότητας, ενώ άλλες έχουν περιορισμένη υποστήριξη. Πολύ λίγες έχουν δυνατότητες που υποστηρίζουν τον έλεγχο ταυτότητας πολλαπλών παραγόντων (multi-factor authentication). Επίσης, δεν είναι σαφές πόσο χρήσιμος είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων για IoT edge devices γενικά. Ένα από τα πρωταρχικά οφέλη της παραδοσιακής ταυτοποίησης δύο παραγόντων (2-factors authentication) είναι ότι

ένας από τους παράγοντες είναι «out of band» σε σχέση με τον άλλο. Όμως, στην περίπτωση των IoT συσκευών, μπορεί να χρειαστεί να αποθηκευτούν στην ίδια συσκευή και οι δύο πιστοποιήσεις (π.χ. κλειδιά), χάνοντας έτσι το «εκτός ζώνης» πλεονέκτημα.

Παρόλο που είναι διαθέσιμα ορισμένα πρότυπα ή εμπορικές επιλογές (όπως για παράδειγμα η πιστοποίηση αυθεντικότητας, οι εμπορικοί ή ημι-εμπορικοί πάροχοι ταυτότητας σαν τη Google), υπάρχει έλλειμμα ικανότητας στη δημιουργία προφίλ για συγκεκριμένες συσκευές και δεν έχουν πλήρως διερευνηθεί οι επιλογές εξουσιοδότησης και οι συνέπειες πάνω στην ιδιωτικότητα από τη χρήση αυτών των υπηρεσιών.

3.7.6.3 Ανυπαρξία βέλτιστων πρακτικών για IoT δραστηριότητες απόκρισης

Δεν υπάρχουν βέλτιστες πρακτικές για IoT δραστηριότητες απόκρισης Οι οργανισμοί μέσω σχεδιασμού και προγραμματισμού πρέπει να είναι σε θέση να συμβιβάσουν τις IoT συσκευές, τα κλειδιά και τα πιστοποιητικά. Αυτός ο σχεδιασμός πρέπει να περιλαμβάνει και την εκτέλεση αναλύσεων επί των συμβιβασμένων συστημάτων και συσκευών

3.7.6.4 Δυσκολίες με τις edge devices

Οι IoT edge devices για γεγονότα που αφορούν την ασφάλεια δημιουργούν μοναδικές δυσκολίες. Πολλές από αυτές τις edge devices θα είναι μοναδικού σκοπού αισθητήρες, οι οποίοι ενδέχεται να μην είναι σε θέση να παρακολουθούν όλες τις αλληλεπιδράσεις με τη συσκευή.

Άλλες συσκευές ενδέχεται να έχουν περιορισμένη ικανότητα να δημιουργήσουν μια RF σύνδεση, με σκοπό την αποστολή audit logs, λόγω περιορισμών που θέτει η χρήση μπαταρίας.

Η επίγνωση σχεδόν σε πραγματικό χρόνο της κατάστασης ασφαλείας των IoT συσκευών δεν αποτελεί εύκολη υπόθεση.

Μια άλλη πρόκληση είναι η συγκέντρωση log δεδομένων, από πολλά διαδεδομένα IoT τμήματα, ενός συστήματος διαχείρισης μεμονωμένων συμβάντων και στη συνέχεια η δυνατότητα άντλησης νοημοσύνης από τις δραστηριότητες που αναπτύσσονται εντός των τμημάτων αυτών.

3.7.6.5 Περιορισμένες διασυνδέσεις για αλληλεπίδραση IoT συσκευών

Περιορισμένες διασυνδέσεις διαθέσιμες για να αλληλεπιδρούν με συσκευές IoT και με συσκευές και εφαρμογές ασφαλείας. Δεν επικεντρώνεται ακόμη στον εντοπισμό μεθόδων που οδηγούν στην επίτευξη της επίγνωσης μιας κατάστασης που αφορά την ασφάλεια των IoT περιουσιακών στοιχείων ενός οργανισμού.

Η ενσωμάτωση των συσκευών IoT στο υφιστάμενο σύστημα ασφαλείας κάποιου οργανισμού, παρέχει μια γνώση της κατάστασης αναφορικά με την πρωταρχική στάση του οργανισμού στα θέματα ασφαλείας. Δυστυχώς, συνήθως δεν υπάρχουν διαθέσιμες διεπαφές για σύνδεση με τα υπάρχοντα συστήματα SIEM και ως εκ τούτου οι επιλογές για σύνδεση με συστήματα «διαχείρισης ταυτότητας και πρόσβασης» αλλά και με άλλα συστήματα ασφαλείας, είναι συνήθως περιορισμένες.

Δεδομένου ότι συμβαίνει αυτό, είναι πιθανό ότι σύντομα θα αυξηθούν τα ενδιάμεσα προϊόντα για να υποστηριχθεί η διαμεσολάβηση μεταξύ του πλήθους των IoT συσκευών και των υποδομών ασφαλείας ενός οργανισμού.

3.7.6.6 Ρυθμίσεις πλατφόρμας – Εικονικές πλατφόρμες

Τα πρότυπα ασφαλείας για ρυθμίσεις πλατφόρμας που περιλαμβάνει και εικονικές IoT πλατφόρμες οι οποίες υποστηρίζουν πολλαπλές μισθώσεις, είναι ανώριμα. Αυτό περιλαμβάνει τις περιπτώσεις χρήσης όπου το Cloud εκτείνεται στη συσκευή (π.χ. δύο επιχειρήσεις που φιλοξενούνται ως ενοικιαστές στην ίδια φυσική πλατφόρμα IoT). Ως αποτέλεσμα προκύπτει η ανάγκη για λύσεις ελαφρές αλλά και ασφαλείς, λύσεις virtualization / isolation.

3.8 Η ΚΑΘΟΛΙΚΗ ΑΣΦΑΛΕΙΑ ΣΤΟ INTERNET OF THINGS

Ως καθολική ασφάλεια στο Διαδίκτυο των Αντικειμένων γνωστή με τον όρο end-to-end security, νοείται η επίτευξη ασφάλειας απ’ άκρου σε άκρο σε μια IoT πλατφόρμα. Το end-to-end security αποτελεί μια διαδικασία που εφαρμόζεται σε όλα τα επίπεδα επικοινωνίας. Αν ανατρέξουμε στο σχήμα 3.10 του 3ου Κεφαλαίου που απεικονίζει μια πλατφόρμα IoT με διαστρωμάτωση τριών επιπέδων επικοινωνίας, η απαιτητική διαδικασία end-to-end security εφαρμόζεται στο επίπεδο των συσκευών (device layer), στο επίπεδο IoT Gateway (Gateway layer) και στο επίπεδο υπηρεσιών Cloud (Cloud services layer).

Στο **επίπεδο των αντικειμένων/συσκευών** η ασφάλεια που έχει σχεδιαστεί πρέπει να προσαρμόζεται στα διάφορα πρωτόκολλα επικοινωνίας, να εξασφαλίζει τη διαλειτουργικότητα της συσκευής, να υπηρετεί τους περιορισμούς χαμηλού κόστους και χαμηλής κατανάλωσης, να προσαρμόζει υφιστάμενες λύσεις ασφάλειας σε συσκευές με περιορισμένη μνήμη και επεξεργαστική ισχύ κλπ. Βέβαια πάντα θα υπάρχουν και οι περιπτώσεις αδυναμίας πλήρους ασφαλισμένης συσκευής. Η ανασφάλεια ενός αντικειμένου/συσκευής κυρίως οφείλεται σε οικονομικούς λόγους καθώς και στη σημαντικότητα του ρόλου που διαδραματίζει. Σε κάθε περίπτωση η πεποίθηση ότι μια μικρή και φθηνή συσκευή, που δε χειρίζεται σημαντικά στοιχεία, πληροφορίες και δεδομένα δεν απαιτεί υψηλή προστασία, είναι παρακινδυνευμένη, όπως στην περίπτωση που η φαινομενικά ασήμαντη συσκευή ανήκει σε δίκτυο τοπολογίας mesh μαζί με άλλες που συνδέονται σε IoT Gateway. Κενά ασφαλείας που προκύπτουν από ανάλογες πεποιθήσεις, προκαλούν έμπειρους επιτιθέμενους να ενεργήσουν με απροσδόκητους τρόπους. Σε ένα κρυπτογραφικό σύστημα **η τάξη της ασφάλειας** είναι αποτέλεσμα του συνδυασμού του αλγόριθμου κρυπτογράφησης και του μήκους που έχει το κλειδί κρυπτογράφησης.

Στο **επίπεδο IoT Gateway** οι απαιτήσεις ασφάλειας είναι πολλαπλάσιες από αυτές των απλών συσκευών. Εδώ μπορούν να χρησιμοποιηθούν κάποιες από τις έτοιμες λύσεις ασφάλειας των υπολογιστικών συστημάτων (32 και 64 bit) επειδή οι Gateways έχουν ισχυρότερους επεξεργαστές και μεγαλύτερη μνήμη.

Ο ρόλος ενός IoT Gateway στην ασφάλεια μιας πλατφόρμας IoT είναι:

- Η δημιουργία μόνωσης μεταξύ των επιπέδων device layer και cloud layer. Για όλες τις συσκευές αποκλείεται η πρόσβαση σε κρυπτογραφικά μυστικά άλλων συσκευών του αυτού ή άλλου επιπέδου.
- Έλεγχος επικοινωνίας συσκευών. Για όλες τις συσκευές επιτρέπεται η αποστολή και η λήψη δεδομένων, αποκλειστικά και μόνο της τάξης στην οποία ανήκουν.
- **Διαχείριση της ποιότητας υπηρεσίας (QoS)**. Καμία σύνδεση δε μπορεί να δεσμεύει όλο το bandwidth του δικτύου. Τίθενται προτεραιότητες για είδη πακέτων τα οποία επιλέγει κατά βούληση ο διαχειριστής του δικτύου και έτσι τα ουσιώδη (πχ μηνύματα) προωθούνται άμεσα.

Κρίσιμα για ένα IoT Gateway είναι η επιτάχυνση των κρυπτογραφικών διαδικασιών, η διαχείριση του κύκλου ζωής των κλειδιών, οι ρίζες εμπιστοσύνη και η απομόνωση των εφαρμογών και των ροών δεδομένων (data streams).

Στο **επίπεδο υπηρεσιών Cloud** οι προκλήσεις ασφάλειας βαρύνουν τον πάροχο. Το υλικό (hardware) και το λογισμικό (software) πρέπει να υποστηρίζουν ταυτόχρονα δισεκατομμύρια συσκευών, χωρίς να επηρεάζεται η ασφάλειά και η διαθεσιμότητά του Cloud, Τα δεδομένα των εφαρμογών να διαχωρίζονται μεταξύ τους και να είναι ορατά μόνο στον κάτοχό τους και να καθορίζονται πολιτικές ανάκτησης δεδομένων.

4. Κακόβουλες Επιθέσεις

4.1 ΕΙΣΑΓΩΓΗ

Στο πεδίο της κυβερνοασφάλειας, τρωτότητα (vulnerability) είναι η/οι αδυναμία/ες τις οποίες κάποιος μπορεί να εκμεταλλευθεί ώστε να εκδηλώσει επίθεση σε συσκευή ή σε υπολογιστικό σύστημα. Η τρωτότητα συντίθεται από τα ευάλωτα σημεία που επιτρέπουν σε κάποιο μη εξουσιοδοτημένο πρόσωπο, οντότητα ή οργανισμό να επιτεθεί με κακόβουλες προθέσεις.

Ο όρος attack surface αντιπροσωπεύει το σύνολο αυτών των σημείων όπου ο επιτιθέμενος μπορεί να προσπαθήσει είτε να εισαγάγει είτε να εξαγάγει δεδομένα από

το υπολογιστικό περιβάλλον. Για να εκμεταλλευθεί την τρωτότητα ο επιτιθέμενος πρέπει να διαθέτει κάποιο κατάλληλο εργαλείο ή τεχνική (malware) με τη βοήθεια των οποίων να μπορεί να συνδεθεί με το αδύναμο σημείο, προσβάλλοντας κακόβουλα το σύστημα. Με βάση όσα προεκτέθηκαν γίνεται αντιληπτό πως οι έννοιες vulnerability και attack surface είναι ταυτόσημες.

Τα κυβερνοεγκλήματα που διαπράττονται αποτελούν προσβολές/αδικήματα κατά ατόμων ή συνόλων με πρόθεση να προκαλέσουν βλάβη σε αυτά. Η βλάβη περιλαμβάνει αρνητικές συνέπειες στη φήμη, τη σωματική ή ψυχική κατάσταση, απώλειες και αλλοιώσεις στοιχείων, απειλές, εκβιασμοί, παραβιάσεις της ιδιωτικότητας, κλοπή πνευματικών δικαιωμάτων, οικονομικές επιθέσεις, συλλογή ή διασπορά πληροφοριών, υβριδικό πόλεμο και άλλα πολλά. Για την επίτευξη των σκοπών τους οι επιτιθέμενοι χρησιμοποιούν σύγχρονα τηλεπικοινωνιακά δίκτυα όπως το Internet και κινητά τηλέφωνα.

Η διεύρυνση των δικτύων και ο πολλαπλασιασμός των κακόβουλων επιθέσεων και των κυβερνοεγκλημάτων (cybercrimes) που όλο και εντείνονται, απαιτεί τη διαχείριση της τρωτότητας (vulnerability management) δηλαδή την άσκηση πρακτικών ταυτοποίησης, αποκατάστασης και μετριασμού των ευπαθειών του λογισμικού, των IoT υπολογιστικών συστημάτων και συσκευών.

Η εστίαση της παρούσας θεματικής ενότητας αφορά το είδος, την ένταση και τις συνέπειες των επιθέσεων που εκδηλώνονται στο Διαδίκτυο των Αντικειμένων από επιτιθέμενους με κακόβουλες προθέσεις.

4.2 ΙΣΟΖΥΓΙΟ ΑΠΕΙΛΩΝ ΚΑΙ ΑΝΤΙΜΕΤΡΩΝ

Προκειμένου να χαρτογραφήσουμε το περιβάλλον των επιθέσεων που δυνητικά απειλούν το Internet of Things, διαμορφώνουμε ένα ισοζύγιο Απειλών και Αντιμέτρων. Το ισοζύγιο δίνεται στον παρακάτω πίνακα.

ΑΠΕΙΛΕΣ	ΑΝΤΙΜΕΤΡΑ
• Computer crime • Vulnerabilities • Eavesdropping • Malware • Spyware	• Computer access control • Application security ✓ Antivirus software ✓ Secure coding

• Ransomware • Trojans • Viruses • Worms • Rootkits • Bootkits • Keyloggers • Screen scrapers • Exploits • Backdoors • Logic bombs • Payloads • Denial of service • Web shells	✓ Secure by default ✓ Secure by design ✓ Secure operating systems • Authentication ✓ Multi-factor authentication • Authorization • Data-centric security • Encryption • Firewall • Intrusion detection system • Mobile secure gateway • Runtime application self-protection (RASP)

Πηγή: Wikipedia

Το πλαίσιο της επίθεσης σε συσκευές ή στο ασύρματο δίκτυο διαμορφώνεται από τα στοιχεία που περιλαμβάνονται στις απειλές του παραπάνω ισοζυγίου. Ο επιτιθέμενος μπορεί να αποκτήσει φυσική πρόσβαση και να εξαπολύσει επίθεση, να εκδηλώσει τοπική επίθεση μέσω Ethernet ή Wi-Fi, να επιχειρήσει κατά των υποδομών του Cloud, να εγκαταστήσει επιβλαβές λογισμικό και να πραγματοποιήσει επιθετικές ενέργειες στο ασύρματο δίκτυο.

4.3 ΕΠΙΘΕΣΕΙΣ ΣΕ ΣΥΣΚΕΥΕΣ

4.3.1 Γενικά Ιστορικά Στοιχεία

Επιθετικές συμπεριφορές κατά επικοινωνιακών και υπολογιστικών υποδομών συναντάμε καθ' όλη τη διάρκεια του 20ου αιώνα. Από το 1903 όταν ο Nevil Maskelyne προσέβαλε μια επίδειξη που αφορούσε την ασφάλεια της ασύρματης τηλεγραφίας στέλνοντας επιβλαβή σήματα Morse μέσω ενός projector μέχρι και τις μέρες μας οι επιθέσεις συνεχίζονται αυξανόμενες εκθετικά.

Ενδεικτικά αναφέρονται τα παρακάτω: Το 1949 δημοσιοποιήθηκε σε paper η «Θεωρία και οργάνωση περίπλοκων αυτομάτων» του John von Neumann που έθετε το θεωρητικό υπόβαθρο περί ιών που πλήττουν τα υπολογιστικά μηχανήματα. Η πρώτη γνωστή περίπτωση πειρατικής διείσδυσης σε δίκτυο αναφέρεται το 1967 όταν μέλη μιας λέσχης υπολογιστών, από ένα προαστιακό γυμνάσιο του Σικάγου πέτυχαν πρόσβαση στο δίκτυο APL της IBM. Στα ενδιάμεσα χρόνια τα επιβλαβή γεγονότα αυξήθηκαν σημαντικά. Το 1981 ο γνωστός Captain Zap, κατά κόσμο Ian Murphy, ήταν ο πρώτος cracker που έμελε να δικαστεί και να καταδικαστεί ως εγκληματίας. Το 1983 η ομάδα 414s κατάφερε να εισέλθει σε εξήντα (60) συστήματα υπολογιστών ιδρυμάτων από το Εθνικό Εργαστήριο του Los Alamos ως το Memorial Sloan-Kettering Cancer Center του Μανχάταν. Το 2012 ένας Σαουδάραβας hacker, δημοσίευσε πάνω από 400.000 πιστωτικές κάρτες στο διαδίκτυο. Το 2014 το ανταλλακτήριο Bitcoin, Mt.Gox κατέθεσε πτώχευση μετά από κλοπή $ 460 εκατομμύριων από hacker λόγω αδυναμιών στο σύστημά του και άλλων $ 27,4 εκατομμυρίων που έλειπαν από τραπεζικούς λογαριασμούς. Το 2016 έγινε προσπάθεια κλοπής $ 951 εκατομμύριων από την Bangladesh Bank τελικά εκλάπησαν $101 εκατομμύρια.

Η παραπάνω αναφορά σε γεγονότα κυβερνοεπιθέσεων είναι απολύτως ενδεικτική και λίαν περιοριστική, καθημερινά εκδηλώνονται χιλιάδες ανάλογες επιθέσεις σε όλο τον κόσμο που χρήζουν ανάλυσης και άμεσης αντιμετώπισης.

Η νέα κατάσταση που έχει διαμορφωθεί έχει εισάγει καινούργιες έννοιες και νέους όρους τόσο στην επιστήμη όσο και στην καθημερινή πρακτική. Έτσι μαθαίνουμε για crime ware, για κουλτούρα και ηθική του hacker, για πρακτικές hacking, για malware, για hacking εργαλεία, για application security, ακόμα και για μανιφέστο του hacker (1986). Τα είδη και η ένταση των επιθέσεων παρουσιάζονται στις παραγράφους που ακολουθούν.

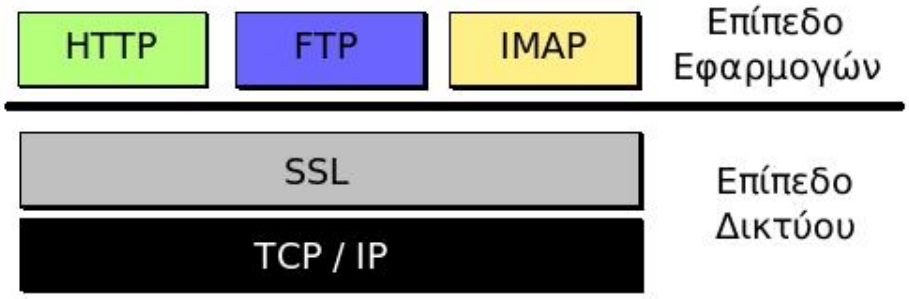
4.3.2 Επίθεση με άμεση πρόσβαση στη συσκευή

Ο επιτιθέμενος μπορεί με κάποιο τρόπο να έχει αποκτήσει φυσική πρόσβαση στη συσκευή, γεγονός που το δίνει σημαντικό πλεονέκτημα στη πραγματοποίηση των κακόβουλων σχεδίων του, αφού συνιστά το υψηλότερο επίπεδο πρόσβασης που είναι δυνατόν να επιτευχθεί και να επιτρέψει ένα **πρώτο κύκλο επιθέσεων**. Έχοντας αυτό

το πλεονέκτημα ο εισβολέας μπορεί να πραγματοποιήσει επιθετικές ενέργειες ως ακολούθως:

Επιθετική Ενέργεια 1η: Επέμβαση για τροποποίηση των ρυθμίσεων της συσκευής. Η τροποποίηση των ρυθμίσεων επιτρέπει την υλοποίηση των παρακάτω ανεπιθύμητων ενεργειών.

- Επαναφορά εργοστασιακών ρυθμίσεων: Με την αλλαγή αυτή ο κωδικός πρόσβασης (password) είτε δίνεται είτε μπορεί εκ' νέου να οριστεί με την πρώτη είσοδο.
- Εγκατάσταση πιστοποιητικού SSL: Το πρωτόκολλο Secure Sockets Layer έχει ως αποστολή την παροχή ασφάλειας κατά τη διαβίβαση ευαίσθητων δεδομένων (σήμερα τείνει να αντικατασταθεί από το πρωτόκολλο Transport Layer Security – TLS). Τα δύο αυτά σημαντικά πρωτόκολλα ασφαλείας χρησιμοποιούνται κατά βάση στις ηλεκτρονικές αγορές και τις συναλλαγές, διασφαλίζοντας την απρόσκοπτη υλοποίησή τους.



Σχήμα 4.1 Πρωτόκολλο SSL

Το Πρωτόκολλο SSL όπως φαίνεται στο παραπάνω σχήμα λειτουργεί πριν το Πρωτόκολλο Διαδικτύου TCP / IP και μετά τις υψηλού επιπέδου εφαρμογές. Με τα πρωτόκολλα SSL και TLS διασφαλίζεται η πιστοποίηση του Server από τον Client, του Client από τον Server και ένας κρυπτογραφημένος δίαυλος επικοινωνίας. Η χειραψία φαίνεται στο σχήμα που ακολουθεί.

Σχήμα 4.2 Πρωτόκολλο SSL - Χειραψία δύο συσκευών

Στην επίθεση με εγκατάσταση πρωτοκόλλου SSL, ο επιτιθέμενος ανακατευθύνει την κίνηση σε Server που ελέγχει.

- Δημιουργία ζεύγους : Ο επιτιθέμενος πραγματοποιεί την επίθεσή του κατά της συσκευής στην οποία έχει αποκτήσει φυσική πρόσβαση δημιουργώντας ζεύγος με κάποια άλλη συσκευή. Χαρακτηριστικό παράδειγμα αποτελεί το Bluetooth.

Επιθετική Ενέργεια 2η: Επέμβαση για ανάγνωση της μνήμης και του firmware. Κάθε υπολογιστής διαθέτει ένα ολοκληρωμένο κύκλωμα που ελέγχει τις λειτουργίες της μνήμης, τις λειτουργίες ανάγνωσης και γραφής στη μνήμη και συνδέει τη μνήμη με τα υπόλοιπα μέρη του υπολογιστή. Το κύκλωμα αυτό είναι ο Ελεγκτής Μνήμης (Memory Controller). Η ανάγνωση ή η γραφή στη μνήμη ονομάζεται προσπέλαση (access). Ο δυνητικός επιτιθέμενος, ως επιθετική ενέργεια μπορεί να επιδιώξει την ανάγνωση της μνήμης ή/και του Firmware μέσω JTAG και RS 232 ή μπορεί να επιδιώξει την εγγραφή προσαρμοσμένου Firmware. Μια άλλη παραπλήσια ενέργεια είναι η ενδεχόμενη προσπάθεια συγκόλλησης μιας κεφαλής σύνδεσης στα pads του

PCB. Η απόκτηση πρόσβασης στο firmware προσφέρει στον επιτιθέμενο δυνατότητες για:

- Εντοπισμό ευάλωτων σημείων
- Εύρεση κενών ασφαλείας,
- Εύρεση κλειδιών κρυπτογράφησης,
- Back doors,
- Εγγραφή τροποποιημένου firmware με εξειδικευμένα κενά ασφαλείας.

Επιθετική Ενέργεια 3η: Επέμβαση για κακόβουλη αναβάθμιση. Όταν μια συσκευή από την κατασκευή της υποστηρίζει αναβαθμίσεις που δεν απαιτείται να είναι ψηφιακά υπογεγραμμένες από τον κατασκευαστή ή κρυπτογραφημένες, παρέχουν στον επιτιθέμενο τη δυνατότητα να επιχειρήσει κακόβουλη αναβάθμιση μέσω καρτών SD, USB ή μέσω του τοπικού δικτύου.

4.3.3 Επίθεση μέσω Ethernet ή Wi-Fi

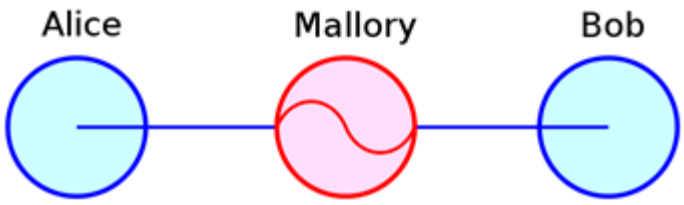
Ένας **δεύτερος κύκλος επιθέσεων** μπορεί να εκδηλωθεί μέσω Ethernet ή Wi-Fi με απόκτηση ενσύρματης ή ασύρματης πρόσβασης στο τοπικό δίκτυο. Στο Internet of Things οι επιθέσεις στηρίζονται στους τρόπους με τους οποίους οι συσκευές δέχονται τις εντολές. Οι τρόποι αυτοί είναι η απλή άμεση σύνδεση και το Cloud Polling

Με τον τρόπο της **Άμεσης Σύνδεσης**, η κάθε συσκευή εντοπίζεται στο τοπικό δίκτυο μέσου των δικτυακών πρωτοκόλλων Simple Service Discovery (SSDP) και Universal Plug and Play (UPnP). Η παραμετροποίηση της συσκευής γίνεται μέσω web interface εφαρμογής κινητού τηλεφώνου ή με το εξειδικευμένο σετ υπο-ρουτινών Application Programming Interface (API). Η παραμετροποίηση μέσω Διαδικτύου είτε γίνεται αυτόματα μέσω UPnP είτε απαιτεί διάνοιξη θύρας εισερχόμενης κίνησης (inbound port) στον IoT Gateway ή στον τοπικό router. Σε ένα τέτοιο περιβάλλον οι επιθέσεις εκδηλώνονται στις άμεσες συνδέσεις.

Επιθετική Ενέργεια 4η: Εκμετάλλευση των ευπαθειών των άμεσων συνδέσεων. Ο επιτιθέμενος στην περίπτωση αυτή εκμεταλλεύεται τις ευπάθειες που παρουσιάζονται στις άμεσες συνδέσεις των συσκευών για να εκδηλώσει την επίθεσή του. Ως τέτοιες ευπάθειες καταγράφονται:

- Εκτέλεση αιτημάτων επί των οποίων ο αποστολέας δεν έχει ταυτοποιηθεί (πχ: παραμετροποίηση συσκευής, λήψη δεδομένων, εκτέλεση διαχειριστικών λειτουργιών, κ.α.)
- Ανεπιθύμητη εγκατάσταση αναβαθμίσεων του firmware
- Υπερχειλίσεις των buffers
- Υπερχείλιση της μνήμης
- Ευπάθειες καταγεγραμμένες από το OWASP Top Ten Project
    - Cross-site Scripting (XSS)
    - Μη επικυρωμένες ανακατευθύνσεις
    - Μη επικυρωμένες προωθήσεις
    - Έκθεση κρίσιμων δεδομένων, κ.α.

Με τον τρόπο του **Cloud Polling** η συσκευή ελέγχει διαρκώς τον Cloud Server ώστε να διαπιστώσει αν υπάρχουν εντολές προς εκτέλεση ή ενημερώσεις για το firmware. Εν συνεχεία τον ενημερώνει για την τρέχουσα κατάστασή της. Οι επιθέσεις που πραγματοποιούνται σε ένα τέτοιο περιβάλλον είναι τύπου Man in the Middle (MITM).



Σχήμα 4.3 Περιγραφή της επίθεσης Man in the Middle

Η MITM είναι επίθεση κατά την οποία ο επιτιθέμενος εκπέμπει μυστικά προκειμένου να μεταβάλλει την επικοινωνία δύο μερών που επικοινωνούν άμεσα μεταξύ τους. Στο παραπάνω σχήμα ο επιτιθέμενος είναι ο Mallory που παρεμβάλεται στην απρόσκοπτη επικοινωνία των Alice και Bob.

Επιθετική Ενέργεια 5η: Η τεχνική της επίθεσης παρμένη από την πολεμική στον πραγματικό κόσμο, συνίσταται σε ενεργή παρακολούθηση, όπου ο εισβολέας πραγματοποιεί ανεξάρτητες συνδέσεις με τα θύματα και στέλνει μηνύματα μεταξύ τους δίνοντάς τους την εντύπωση ότι μιλούν άμεσα ο ένας στον άλλο, ενώ στην

πραγματικότητα η συνομιλία ελέγχεται από τον επιτιθέμενο. Σε μια τέτοια διαδικασία ο επιτιθέμενος ανακατευθύνει τη κίνηση της επικοινωνίας των δύο μερών με επιθέσεις επιπέδου δικτύου. Ως τέτοιες αναφέρονται:

- ARP poisoning
- Τροποποίηση παραμέτρων του συστήματος DNS (Domain Name System).
- Παρεμβολή HTTPs με εργαλείο πιστοποιητικά υπογεγραμμένα από τον ίδιο τον επιτιθέμενο
- Παρεμβολή HTTPs με εργαλείο το SSL Strip.

4.3.4 Επίθεση στις υποδομές του Cloud

Οι κυριότεροι κίνδυνοι που εμφανίζονται στο Cloud εντοπίζονται στα παρακάτω:

1. Ο χρήστης παραχωρεί μέρος του ελέγχου στον πάροχο αφού η παροχή υπηρεσίας του Cloud χρησιμοποιεί την υποδομή του παρόχου. Η service level agreement (SLA), η συμφωνία δηλαδή μεταξύ παρόχου πελάτη αφήνει κενά σε επίπεδα ασφαλείας.

2. Τα εργαλεία με τα οποία παρέχονται, διαδικασίες, πρότυπο τυποποιημένης μορφής και οι υπηρεσίες (ασφάλειας δεδομένων, φορητότητα και μετάβαση σε άλλο πάροχο), δεν έχουν φτάσει σε υψηλό επίπεδο.

3. Στο Cloud προσφέρεται η κοινή διαχείριση αρχείων και πόρων, αυτή παρουσιάζει μειονεκτήματα στην ασφάλεια σε σχέση με την αρχιτεκτονική multi-tenant επειδή υπό συνθήκες κοινής διαχείρισης θα μπορούσε να επιτευχθεί μία επίθεση τύπου guest hopping.

4. Το Cloud προσφέρει πρόσβαση μέσω παγκόσμιου ιστού και κοινόχρηστων δικτύων. Επομένως είναι αυξημένο το ρίσκο, ειδικά όταν συνδυάζεται με απομακρυσμένη σύνδεση.

5. Ένας κίνδυνος εμφανίζεται κατά τη διαγραφή των αρχείων. Όταν θέλουμε να σβήσουμε τα πάντα από το δίσκο υπάρχουν άπειρες τεχνικές, στο Cloud όμως δεν μπορούμε να κάνουμε κάτι τέτοιο. Μοιραζόμαστε το δίσκο και με άλλους πελάτες και στην πραγματικότητα το σβήσιμο δεν γίνεται πάντα σε πραγματικό χρόνο.

6. Δεν υφίσταται διασφάλιση εσωτερικά, μέσα από την υποδομή για την περίπτωση που το κακό ξεκινάει από μέσα.

Οι συσκευές IoT εκτελούν υπηρεσία Cloud**.** Γίνονται μετρήσεις που καταγράφονται σε log files και αποστέλλονται σε Cloud Server μέσω IoT Gateway. Η υπηρεσία αυτή δίνει τη δυνατότητα διαχείρισης των συσκευών μέσω Cloud, έτσι που οι ρυθμίσεις των συσκευών σε ορισμένες περιπτώσεις γίνονται αποκλειστικά μέσω Cloud με τη διαμεσολάβηση Web περιβάλλοντος ή/και εφαρμογής κινητού και όχι τοπικά.

Επιθετική Ενέργεια 6η: Η επίθεση που εκδηλώνεται εδώ είναι επίθεση brute force που στοχεύει στην αποκάλυψη του κωδικού πρόσβασης. Στο ίδιο πλαίσιο επιθέσεων κατά των υποδομών Cloud εντάσσονται και επιθέσεις σε ευπάθειες που αφορούν:

- SQL Injections
- Blind SQL Injections
- XSS
- path traversal
- Ανέβασμα κακόβουλων αρχείων με σκοπό την απομακρυσμένη εκτέλεση κώδικα (RCE44)
- Ευπάθειες που περιγράφονται στη λίστα top 10 του OWASP

Καθοριστικός εδώ παράγοντας για την αποτροπή είναι η χρήση ισχυρών κωδικών, το IP ban, ταυτοποίηση two factor authentication (2FA), πρόσφατες ενημερώσεις των Cloud Servers, οι ασφαλείς συνδέσεις HTTP / SSL, αυστηροποίηση της διαδικασίας ανάκτησης κωδικών κλπ

4.3.5 Επίθεση με εγκατάσταση κακόβουλου λογισμικού

Το κακόβουλο λογισμικό που αποδίδεται με τους όρους malware, badware και malicious software είναι ένα σοβαρότατο πρόβλημα που στρέφεται κατά της ασφάλειας των υπολογιστικών, πληροφοριακών και επικοινωνιακών συστημάτων. Το λογισμικό αυτό αφορά προγράμματα που στρέφονται κατά της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας και περιλαμβάνει κώδικα για την

αναπαραγωγή του και τη μετάδοσή του. Η αναπαραγωγή σημαίνει τη μόλυνση από πρόγραμμα σε πρόγραμμα στο σύστημα, η δε μετάδοση, την εξάπλωση της μόλυνσης από το μολυσμένο σύστημα σε άλλα συστήματα

Υπάρχουν πολλά είδη κακόβουλου λογισμικού, όπως ιοί (viruses), σκουλήκι (warm), δούρειοι ίπποι (Trojan horses), spyware, adware, rootkits, bots, zombies. Από αυτά κάποια για την εκτέλεσή τους χρειάζονται πρόγραμμα ξενιστή ενώ κάποια άλλα δεν χρειάζονται πρόγραμμα ξενιστή. Τέλος μπορούν να καταταγούν στα ιομορφικά (που αναπαράγονται από μόνα τους) και τα μη ιομορφικά.

Ενδεικτική κατάταξη / κατηγοριοποίηση του κακόβουλου λογισμικού παρουσιάζεται στον πίνακα που ακολουθεί.

Κατηγοριοποίηση Κακόβουλου Λογισμικού			
Χρήση ξενιστή	Μη χρήση ξενιστή	Ιομορφικό	Μη ιομορφικό
Trapdoor	Worm	Virus	Backdoor
Trojan Horses	-	Worm	Trojan Horses
Logic Bombs	-	-	Logic Bombs
Virus	-	-	-

Επιθετική Ενέργεια 7η: Εγκατάσταση κακόβουλου λογισμικού για μόλυνση του υπολογιστικού συστήματος και μετάδοση αυτής και σε άλλα συστήματα. Η επιθετική αυτή ενέργεια μπορεί να εκδηλωθεί με τους εξής τρόπους:

- Αποστολή ηλεκτρονικής αλληλογραφίας
- Χρήση αφαιρούμενων αποθηκευτικών μέσων
- Ενσωμάτωση εκτελέσιμου κώδικα σε ιστοσελίδες html
- Χρησιμοποίηση υπηρεσιών διαδικτυακής επικοινωνίας
- Χρησιμοποίηση τοπικών και ευρείας περιοχής δικτύων για τη διοχέτευση κακόβουλου λογισμικού (worm) και την αυτόματη ευρεία μετάδοσή του.

Στην πρώτη περίπτωση, το κακόβουλο λογισμικό επισυνάπτεται σε ηλεκτρονικό μήνυμα είτε σκόπιμα από τον επιτιθέμενο, είτε είναι συνέπεια αυτόματης μετάδοσης (mail worm).

Στη δεύτερη περίπτωση χρησιμοποιούνται τα γνωστά εξωτερικά αποθηκευτικά μέσα USB, CD, DVD, floppy disk. Για τη μετάδοση των κλασσικών ιών η δεύτερη αυτή περίπτωση επίθεσης είναι η πλέον συνηθισμένη.

Στην τρίτη περίπτωση ενσωματώνεται κώδικας σε σελίδες html. Ο κώδικας είναι εκτελέσιμος και ως εκ τούτου με την επίσκεψη στην συγκεκριμένη ιστοσελίδα πραγματοποιείται η μόλυνση.

Στην τέταρτη περίπτωση για την επίθεση χρησιμοποιούνται οι υπηρεσίες συνομιλίας instant messengers, internet telephony, video conferencing, IRC clients, σε πραγματικό χρόνο, οι υπηρεσίες ομάδων συζήτησης και τα προγράμματα ανταλλαγής αρχείων.

Στην πέμπτη περίπτωση οι επιτιθέμενοι εκμεταλλεύονται κενά ασφαλείας και ευπάθειες πρωτοκόλλων, υπηρεσιών, λειτουργικών συστημάτων και εφαρμογών και μεταδίδουν μέσω LAN και WAN που εκτελούν πρωτόκολλα TCP/IP, κακόβουλο λογισμικό (πχ επίθεση υπερχείλισης καταχωρητή).

Με βάση τα προεκτεθέντα αν ο επιτιθέμενος καταφέρει με κάποιο τρόπο να εγκαταστήσει επιβλαβές λογισμικό σε IoT συσκευή, τότε αυτή με τη σειρά της θα εξαπολύει επιθέσεις προς άλλες συσκευές του τοπικού δικτύου (για παράδειγμα προς Smart TVs). Υπάρχει και η περίπτωση το κακόβουλο λογισμικό να έχει εγκατασταθεί σε συσκευές όπως δικτυακούς σκληρούς δίσκους NAS και IP routers του τοπικού δικτύου και οι επιθέσεις προς τις IoT συσκευές να εκδηλώνονται από εκεί. Για το λόγο αυτό καλό θα ήταν, το δίκτυο IoT με τη χρήση VLANs ή άλλης σχετικήσ μεθόδου να διαχωρίζεται από το υπόλοιπο δίκτυο.

4.4 ΕΠΙΘΕΣΕΙΣ ΣΕ ΑΣΥΡΜΑΤΑ ΠΡΟΤΥΠΑ ΠΡΩΤΟΚΟΛΛΑ

Οι επιθέσεις στα ασύρματα πρότυπα πρωτόκολλα μπορούν να εκδηλωθούν ως εξής διαζευκτικά ή συνδυαστικά:

- Ιχνηλάτηση της κίνησης (sniffing)
- Έκχυση πακέτων (packet injection)
- Attack on information in transit
- Παραβίαση (tampering/forging)

- Παρεμβολές (jamming)
- Εξάντληση της μπαταρίας μέσω αδιάκοπων αιτημάτων
- Επιθέσεις συγκρούσεων και ανισοτήτων χρήσης (collision/unfairness attacks)
- Επιθέσεις απληστίας, ανακατεύθυνσης, μαύρων τρυπών (greed, misdirection, black hole)
- Άρνηση παροχής υπηρεσιών (Denial of Service –DoS)
- Sybil Attack
- Επιθέσεις πλημμύρας και αποσυγχρονισμού (flooding, desynchronization)
- Wormhole Attack

Με την **επιθετική ενέργεια «sniffing»** ο εισβολέας παρακολουθεί «οσφραίνεται την κίνηση των δεδομένων που ρέουν σε πραγματικό χρόνο μέσω των συνδέσεων του δικτύου υπολογιστών. Η γνώση της κίνησης του δίνει το πλεονέκτημα να εκδηλώσει την επίθεσή του σε συνδυασμό με την επόμενη επιθετική ενέργεια.

Η **έγχυση πακέτων (injection)** στη δικτύωση υπολογιστών είναι μια διαδικασία παρεμβολής, σε μια καθιερωμένη σύνδεση δικτύου. Αυτό γίνεται μέσω της κατασκευής πακέτων που εμφανίζονται σαν να είναι μέρος της κανονικής ροής επικοινωνίας. Η διαδικασία έγχυσης πακέτων επιτρέπει σε ένα τρίτο μέρος να διακόπτει ή να αναστέλλει μια επικοινωνία μεταξύ δύο μερών,

Ανάλογη είναι και η **Attack on information in transit**, όπου ο επιτιθέμενος μπορεί να παρακολουθεί τη ροή της κυκλοφορίας και να αναλαμβάνει δράση προκειμένου να διακόψει, να διασπάσει, να προσαρμόσει και να κατασκευάσει πακέτα που να παρέχουν λανθασμένες πληροφορίες στους χρήστες, δημιουργώντας τους μείζονα προβλήματα.

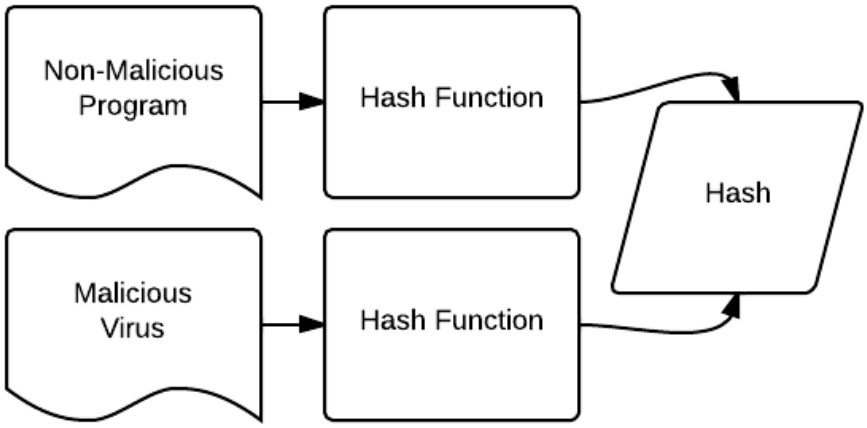
Η **επίθεση τύπου tampering/forging** έχει σα στόχο τα αρχεία καταγραφής του κεντρικού υπολογιστή προορισμού. Ο εισβολέας εγχέει, χειρίζεται ή δημιουργεί (πλαστογραφεί) κακόβουλες καταχωρίσεις στο log file, επιτρέποντάς του έτσι να παραπλανήσει τον έλεγχο ιστορικού, να καλύψει ίχνη επίθεσης ή να εκτελέσει άλλες κακόβουλες ενέργειες. Ο κεντρικός υπολογιστής στόχος δεν ελέγχει πια σωστά την πρόσβαση στο αρχείο καταγραφής. Τα μολυσμένα δεδομένα επηρεάζουν to log file και τις λειτουργίες του.

Οι **επιθέσεις παρεμβολών ή παρακώλυσης επικοινωνιών**, γνωστές και ως jamming, είναι οι επιθέσεις που σκόπιμα ή μη προκαλούνται στο πομπό, το δέκτη ή το

σημείο ασύρματης πρόσβασης προκειμένου να διακοπεί, να παρακωλυθεί ή να στρεβλώσει η επικοινωνία, από παρεμβολές ή θορύβους.

Υπάρχουν επιθέσεις που μέσω **αδιάκοπων αιτημάτων** προσπαθούν να προκαλέσουν ζημιά εξαντλώντας τη μπαταρία.

Με την **collision attack** επιχειρείται η εύρεση δύο εισόδων (inputs) που παράγουν την ίδια hash value. Εκφράζοντας με μαθηματικό τρόπο τη συγκεκριμένη επίθεση, θα λέγαμε πως η collision attack βρίσκει δύο διαφορετικά μηνύματα τα m1 και m2, έτσι ώστε hash(m1)=hash(m2), Εν προκειμένω ο επιτιθέμενος δεν έχει κανένα έλεγχο επί των μηνυμάτων τα οποία καθορίζονται από αλγόριθμο αυθαίρετα.



Σχήμα 4.4 Collision Attack

Σαν παράδειγμα: Θεωρώντας μια υποθετική συνάρτηση hash, μια collision attack ξεκινά με μια αρχική τιμή εισόδου

hash (hello)=89232323.

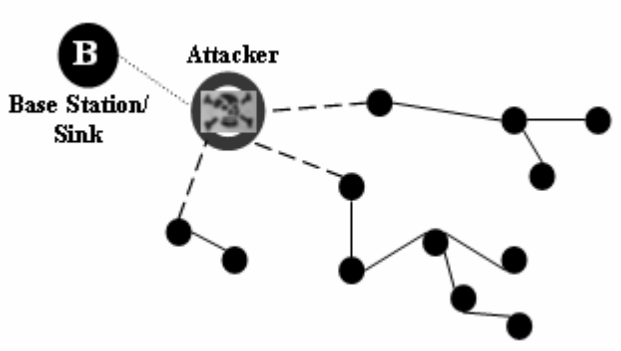
Ο επιτιθέμενος πρέπει να βρει μια διαφορετική είσοδο, η οποία να παράγει το ίδιο hash με την προηγούμενη είσοδο. Αυτό θα γινόταν γενικά με μια μέθοδο brute-force δοκιμάζοντας όλους τους πιθανούς συνδυασμούς μέχρι να βρεθεί κάποιος. Ας υποθέσουμε ότι βρίσκεται μια collision για αυτή την είσοδο στην υποθετική συνάρτηση hash.

hash (8571935798325698)=89232323

Ο εισβολέας γνωρίζει τώρα δύο εισόδους με το ίδιο αποτέλεσμα. Τότε ο επιτιθέμενος μπορεί να προσφέρει τη λήψη ενός αρχείου και να επιδείξει το hash για να αποδείξει την ακεραιότητα του αρχείου αυτού. Στη συνέχεια θα μπορούσε να απενεργοποιήσει (να σβήσει) τη λήψη αρχείου για ένα άλλο διαφορετικό αρχείο που

θα είχε το ίδιο hash. Το άτομο που θα κατέβαζε το (κακόβουλο) αρχείο δεν θα μπορούσε να γνωρίζει τη διαφορά. Το αρχείο θα φαινόταν έγκυρο, καθώς θα έχει το ίδιο hash με το υποτιθέμενο πραγματικό αρχείο.

Με την **επίθεση Black hole**, ένας κακόβουλος κόμβος ενεργεί σαν μαύρη τρύπα που έλκει όλη την κυκλοφορία στο δίκτυο. Ο τρόπος λειτουργίας αυτής της επίθεσης δίνεται σχηματικά παρακάτω όπου όλη η κυκλοφορία έλκεται στο σημείο B που αποτελεί το base station / sink

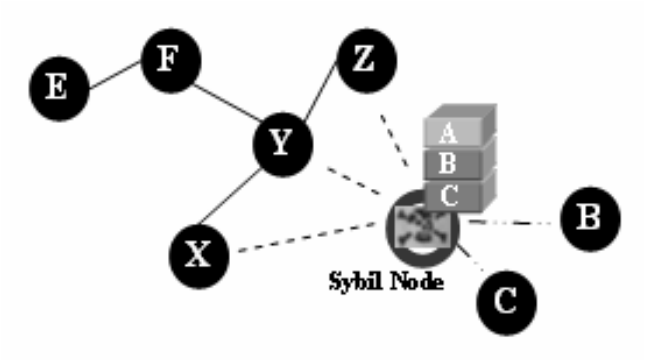


Σχήμα 4.5 Επίθεση black hole

Ειδικά σε ένα πρωτόκολλο που βασίζεται σε πλημμύρα (Flooding), ο εισβολέας ακούει τα αιτήματα για διαδρομές στη συνέχεια απαντά στους κόμβους-στόχους.

Η **άρνηση παροχής υπηρεσίας (DoS)** παράγεται είτε από την ακούσια αποτυχία κόμβων ή από μια κακόβουλη επιθετική ενέργεια. Στην απλούστερη εκδοχή της, η επίθεση DoS προσπαθεί να εξαντλήσει τους διαθέσιμους πόρους τον κόμβο θύμα, στέλνοντας επιπλέον πακέτα που δεν χρειάζονται και έτσι εμποδίζει τους νόμιμους χρήστες του δικτύου να έχουν πρόσβαση σε υπηρεσίες ή πόρους στους οποίους έχουν δικαίωμα. Ως επίθεση DoS δεν εννοείται μόνο η προσπάθεια του αντιπάλου να υπονομεύσει, να διαταράξει ή να καταστρέψει ένα δίκτυο, αλλά και κάθε γεγονός που μειώνει στο δίκτυο τη δυνατότητα παροχής μιας υπηρεσίας. Στο φυσικό επίπεδο οι επιθέσεις DoS θα μπορούσαν να είναι παρεμβολές (jamming) και tempering, στο στρώμα σύνδεσης, collision, εξάντληση (exhaustion) και unfairness, στο επίπεδο του δικτύου, παραμέληση (neglect), απληστία (greed), λάθος κατεύθυνση (misdirection), μαύρες τρύπες (black holes) και στο επίπεδο μεταφοράς αυτή η επίθεση θα μπορούσε να εκτελεστεί με κακόβουλες πλημμύρες (flooding) και αποσυγχρονισμό (desynchronization).

Σε περιπτώσεις ασύρματου δικτύου αισθητήρων, οι αισθητήρες μπορεί να χρειαστεί να συνεργαστούν για να ολοκληρώσουν ένα έργο. Εδώ μια **επίθεση Sybil** μπορεί να εκδηλωθεί ως επίθεση όπου ένας κόμβος πλαστογραφεί τις ταυτότητες περισσότερων του ενός κόμβων. Η επίθεση μπορεί να αφορά στην κατανεμημένη αποθήκευση (distributed storage), το μηχανισμό δρομολόγησης (routing), τη συγκέντρωση των δεδομένων, το voting, τη δίκαιη κατανομή πόρων, την ανίχνευση κακής συμπεριφοράς. Η επίθεση Sybil δηλαδή προσπαθεί να υποβαθμίσει την ακεραιότητα των δεδομένων, την ασφάλεια και η χρήση πόρων. Ένα δίκτυο ομότιμων χρηστών (reer-to-peer) είναι ευάλωτο σε επίθεση Sybil.



Σχήμα 4.6 Επίθεση Sybil

Σημειώνεται ότι η ανίχνευση κόμβων Sybil δεν αποτελεί εύκολη υπόθεση. Η πιθανότητα ανίχνευσης ύπαρξης ενός Sybil κόμβου προκύπτει από τη σχέση:

$$\Pr(detection) = 1 - (1 - \sum_{allS,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}\ S-(m-M)}{\binom{n}{c}\qquad\qquad c})^r$$

Όπου:

n ο αριθμός των κόμβων

s ο αριθμός των κόμβων Sybil

m οι κακόβουλοι κόμβοι

g οι καλοί κόμβοι

c ο αριθμός των κόμβων που μπορούν να δοκιμαστούν κάποια στιγμή από ένα κόμβο, εκ των οποίων S είναι ο αριθμός των κόμβων Sybil, M είναι οι κόμβοι

οι κακόβουλοι οι ελαττωματικοί και G είναι ο αριθμός των καλών κόμβων.

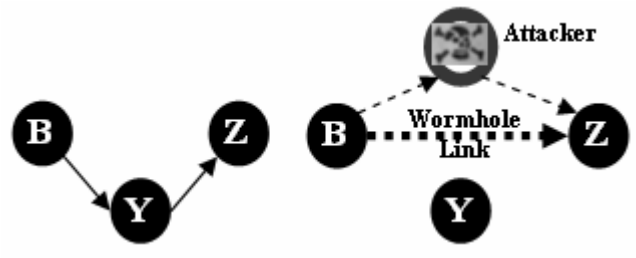
r ο αριθμός των γύρων επανάληψης της δοκιμής.

Η **επίθεση πλημμύρας (flooding attack)** που εκδηλώνεται σε ασύρματο δίκτυο χρησιμοποιεί ως όπλο πακέτα HELLO, για να «πείσει» τους αισθητήρες του wireless sensor network (WSN) Σε αυτό το είδος επίθεσης, ένας εισβολέας με υψηλή ραδιομετάδοση (high radio transmission) που ονομάζεται φορητός επιτιθέμενος (laptop-class attacker) στέλνει HELLO πακέτα σε έναν αριθμό κόμβων αισθητήρων, οι οποίοι είναι διασκορπισμένοι σε μια μεγάλη περιοχή εντός ενός WSN.

Έτσι οι αισθητήρες πείθονται πως ο αντίπαλος είναι γείτονάς τους. Κατά συνέπεια, κατά την αποστολή των πληροφοριών στο basis station οι κόμβοι-θύματα προσπαθούν να περάσουν από τον εισβολέα καθώς γνωρίζουν ότι είναι γείτονάς τους και τελικά παραπλανόνται από τον επιτιθέμενο.

Στην **επίθεση σκουληκότρυπας (wormhole)** ο επιτιθέμενος καταγράφει πακέτα ή bits σε μια τοποθεσία στο δίκτυο και σήραγγες σε μια άλλη τοποθεσία. Το tunneling ή η αναμετάδοση των bits θα μπορούσε να γίνει επιλεκτικά. Η επίθεση wormhole αποτελεί μια σημαντική απειλή κατά του WSN επειδή αυτό το είδος επίθεσης δεν απαιτεί συμβιβασμό του αισθητήρα στο δίκτυο, μπορεί να εκτελεστεί ακόμα και στην αρχική φάση όταν οι αισθητήρες ξεκινούν να ανακαλύπτουν τις γειτονικές πληροφορίες.

Στο σχήμα που ακολουθεί απεικονίζεται η επίθεση wormhole. Όταν ένας κόμβος B μεταδίδει το αίτημα δρομολόγησης πακέτου, ο εισβολέας λαμβάνει αυτό το πακέτο και το επαναλαμβάνει στη γειτονιά του. Κάθε γειτονικός κόμβος που λαμβάνει αυτό το επαναλαμβανόμενο πακέτο θα θεωρήσει ότι ευρίσκεται στην περιοχή (range) του κόμβου B και θα σηματοδοτήσει αυτόν τον κόμβο ως γονέα του.



Σχήμα 4.7 Επίθεση wormhole

5. Ευπάθειες και μέτρα αντιμετώπισης

5.1 ΟΙ ΔΕΚΑ ΚΟΡΥΦΑΙΕΣ ΕΥΠΑΘΕΙΕΣ & ΤΑ ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Στην ασφάλεια του IoT υπάρχει η εσφαλμένη αντίληψη ότι όλα είναι γύρω από τη συσκευή, το δίκτυο ή τον πελάτη. Υπάρχουν πολλά πεδία (surface agents) που εμπλέκονται και κάθε μια από αυτά χρειάζεται να αξιολογηθεί.

Απαιτείται μια ολιστική προσέγγιση και τα στοιχεία που πρέπει να ληφθούν υπόψη είναι:

- Οι συσκευές του Διαδικτύου των Αντικειμένων
- Το Cloud
- Η εφαρμογή κινητού τηλεφώνου (mobile application)

- Οι διασυνδέσεις του δικτύου (network interfaces)
- Το λογισμικό (software)
- Η χρήση κρυπτογράφησης (encryption)
- Η χρήση ταυτοποίησης αυθεντικότητας (authentication)
- Η φυσική ασφάλεια (θυρών USB)

Παρακάτω θα αναλυθούν οι δέκα (10) κορυφαίες κατηγορίες που καλύπτουν ολόκληρη τη συσκευή και ολόκληρη την επιφάνεια έτσι ώστε να αποκτηθεί μια καλή εκτίμηση της συνολικής ασφάλειας.

5.1.1 Ανασφαλής διεπαφή ιστού

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στο web interface, συμπεριλαμβανομένων των εσωτερικών και εξωτερικών χρηστών (συγκεκριμένη εφαρμογή).

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί αδύναμα διαπιστευτήρια, συλλαμβάνει διαπιστευτήρια απλού κειμένου ή απαριθμεί λογαριασμούς για πρόσβαση στην διεπαφή ιστού. Η επίθεση θα μπορούσε να προέρχεται από εξωτερικούς ή εσωτερικούς χρήστες (εύκολη εκμετάλλευση).

Αδυναμία ασφάλειας (security weakness): Μια ανασφαλής διαδικτυακή διασύνδεση μπορεί να είναι η αιτία όταν υπάρχουν ζητήματα απαρίθμησης λογαριασμού, έλλειψης κλειδώματος λογαριασμού, ή αδύναμα διαπιστευτήρια. Οι ανασφαλείς διεπαφές (web interfaces) είναι διαδεδομένες, καθώς πρόθεση είναι αυτές οι διεπαφές, να εκτίθενται μόνο σε εσωτερικά δίκτυα. Ωστόσο, οι απειλές από τους εσωτερικούς χρήστες μπορεί να είναι εξίσου σημαντικές με τις απειλές από εξωτερικούς χρήστες. Τα ζητήματα σχετικά με το web interface είναι εύκολο να εντοπιστούν όταν η διεπαφή εξετάζεται manually μαζί με τα αυτοματοποιημένα εργαλεία ελέγχου για τον εντοπισμό άλλων θεμάτων, όπως η δημιουργία σεναρίων (scripting) μεταξύ ιστοτόπων (εύκολη ανίχνευση).

Τεχνικές επιπτώσεις (technical impacts): Οι μη ασφαλείς διεπαφές ιστού (web interfaces) μπορούν να έχουν σαν αποτέλεσμα την απώλεια δεδομένων ή τη διαφθορά, την έλλειψη λογοδοσίας ή την άρνηση πρόσβασης και μπορούν να οδηγήσουν σε πλήρες device takeover (Σοβαρή επίδραση).

Επιχειρηματικές επιπτώσεις (Business Impacts): Εξετάζοντας τις επιχειρηματικές επιπτώσεις που θα έχουν οι χαμηλού επιπέδου ασφάλειας web interfaces, διαπιστώνεται ότι προκαλούνται ζημιές στις συσκευές. Οι ζημιές θα έχουν αρνητικό αντίκτυπο στους πελάτες και θα βλάψουν το εμπορικό σήμα της εταιρίας.

Είναι η διεπαφή μου στον παγκόσμιο ιστό (Web Interface) ασφαλής;

Ο έλεγχος για μια μη ασφαλή διαδικτυακή διασύνδεση στον παγκόσμιο ιστό περιλαμβάνει:

1. Τον προσδιορισμό εάν τα προεπιλεγμένα όνομα χρήστη και κωδικός πρόσβασης μπορούν να αλλάξουν, κατά την αρχική ρύθμιση (set up) του προϊόντος.
2. Τον προσδιορισμό εάν ένας συγκεκριμένος λογαριασμός χρήστη κλειδώνει μετά από 3 έως 5 αποτυχημένες προσπάθειες σύνδεσης (login).
3. Τον προσδιορισμό εάν οι έγκυροι λογαριασμοί μπορούν να αναγνωριστούν με τη χρήση μηχανισμών ανάκτησης κωδικού πρόσβασης ή νέων σελίδων χρήστη
4. Την επανεξέταση της διεπαφής για θέματα όπως, scripting μεταξύ ιστοτόπων, αίτημα μεταξύ ιστοτόπων, πλαστογράφηση και έγχυση SQL.

Πως θα κάνω τη διεπαφή μου στον παγκόσμιο ιστό (Web Interface) ασφαλή;

Ένα ασφαλές Web Interface απαιτεί:

1. Προεπιλεγμένους κωδικούς πρόσβασης και ιδανικά προεπιλεγμένα ονόματα χρηστών, τα οποία πρέπει να αλλάξουν κατά την αρχική ρύθμιση.
2. Εξασφάλιση ότι οι μηχανισμοί αποκατάστασης του κωδικού πρόσβασης είναι ισχυροί και δεν παρέχουν στον εισβολέα εκείνες τις πληροφορίες που να υποδεικνύουν έναν έγκυρο λογαριασμό.
3. Διασφάλιση ότι η διεπαφή ιστού δεν είναι ευαίσθητη σε XSS, SQLi ή CSRF.
4. Διασφάλιση ότι τα διαπιστευτήρια (credentials) δεν εκτίθενται στην εσωτερική ή εξωτερική κυκλοφορία του δικτύου.
5. Διασφάλιση οι αδύναμοι κωδικοί πρόσβασης δεν επιτρέπονται.
6. Εξασφάλιση κλειδώματος του λογαριασμού μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.

Σενάρια επιθέσεων

Σενάριο 1ο:

Η διεπαφή ιστού (web interface) παρουσιάζει τη λειτουργία "Forgot Password", η οποία κατά την εισαγωγή ενός μη έγκυρου λογαριασμού ενημερώνει τον επιτιθέμενο εισβολέα ότι ο λογαριασμός δεν υπάρχει. Μόλις εντοπιστούν έγκυροι λογαριασμοί, η διαδικασία υφαρπαγής του κωδικού μπορεί να ξεκινήσει για αόριστο χρονικό διάστημα αν δεν υπάρχουν έλεγχοι κλειδώματος του λογαριασμού.

Account john@doe.com does not exist

Σενάριο 2ο:

Το web interface είναι ευαίσθητο στο scripting μεταξύ ιστοτόπων

http://xyz.com/index.php?user=<script>alert(123)</script> ... Response from browser is an alert popup

Στις παραπάνω περιπτώσεις, ο εισβολέας είναι σε θέση να προσδιορίσει εύκολα αν ένας λογαριασμός είναι έγκυρος ή όχι και είναι επίσης σε θέση να προσδιορίσει ότι ο ιστότοπος είναι ευαίσθητος σε scripting μεταξύ ιστοτόπων (XSS).

5.1.2 Ανεπαρκής ταυτοποίηση εξουσιοδότηση

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στο web interface, στο mobile interface ή στο cloud interface, συμπεριλαμβανομένων των εσωτερικών και εξωτερικών χρηστών.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί αδύναμους κωδικούς πρόσβασης, ανασφαλείς μηχανισμούς ανάκτησης κωδικών πρόσβασης, φτωχά προστατευμένα διαπιστευτήρια ή έλλειψη ελέγχου επιλεκτικής πρόσβασης (granular access) για πρόσβαση σε συγκεκριμένη διεπαφή. Η επίθεση μπορεί να προέρχεται από εξωτερικούς ή εσωτερικούς χρήστες.

Αδυναμία ασφάλειας (security weakness): Ο έλεγχος ταυτοποίησης ενδέχεται να μην είναι επαρκής όταν χρησιμοποιούνται αδύναμοι κωδικοί πρόσβασης ή δεν προστατεύονται επαρκώς. Ο ανεπαρκής έλεγχος ταυτοποίησης / εξουσιοδότησης επικρατεί, καθώς θεωρείται ότι οι διεπαφές θα εκτίθενται μόνο σε χρήστες εσωτερικών δικτύων και όχι σε εξωτερικούς χρήστες άλλων δικτύων. Συχνά διαπιστώνεται η παρουσία ελλείψεων σε όλες τις διεπαφές. Πολλά ζητήματα αναφορικά με τον έλεγχο ταυτότητας / εξουσιοδότησης είναι εύκολο να εντοπιστούν κατά την εξέταση της διεπαφής manually, αλλά επίσης μπορούν να ανακαλυφθούν και μέσω αυτοματοποιημένων ελέγχων.

Τεχνικές επιπτώσεις (technical impacts): Η ανεπαρκής πιστοποίηση / εξουσιοδότηση μπορεί να έχει ως αποτέλεσμα την απώλεια δεδομένων ή τη διαφθορά, την έλλειψη λογοδοσίας ή την άρνηση πρόσβασης και μπορεί να οδηγήσει σε πλήρη «συμβιβασμό» της συσκευής ή / και των λογαριασμών των χρηστών.

Επιχειρηματικές επιπτώσεις (Business Impacts): Εξετάζοντας τις επιχειρηματικές επιπτώσεις των «συμβιβασμένων» λογαριασμών χρηστών και ενδεχομένως των συσκευών, διαπιστώνουμε ότι όλα τα δεδομένα θα μπορούσαν να κλαπούν, να τροποποιηθούν ή να διαγραφούν. Ο προβληματισμός που ανακύπτει είναι πόσο θα μπορούσαν να βλάψουν οι πελάτες μιας εταιρίας;

Η επάρκεια ταυτοποίησης εξουσιοδότησης

Ο έλεγχος για ανεπαρκή ταυτοποίηση περιλαμβάνει:

- Τη χρήση απλών κωδικών πρόσβασης όπως "1234", αποτελεί ένα γρήγορο και εύκολο τρόπο για να διαπιστωθεί εάν η πολιτική κωδικού πρόσβασης είναι επαρκής σε όλες τις διεπαφές.
- Τον έλεγχο της επισκεψιμότητας (κυκλοφορίας) του δικτύου, προκειμένου να διαπιστωθεί αν τα διαπιστευτήρια μεταδίδονται με καθαρό κείμενο.
- Την ανασκόπηση των απαιτήσεων γύρω από τους ελέγχους του κωδικού πρόσβασης, όπως η πολυπλοκότητα του κωδικού, ο έλεγχος ιστορικού του κωδικού, η λήξη του κωδικού και η αναγκαστική επαναφορά του κωδικού πρόσβασης για νέους χρήστες.
- Τη διαπίστωση για το αν απαιτείται εκ νέου έλεγχος αυθεντικότητας για ευαίσθητα χαρακτηριστικά

Ο έλεγχος για ανεπαρκή εξουσιοδότηση περιλαμβάνει:

- Ανασκόπηση των διαφόρων διεπαφών προκειμένου να προσδιοριστεί το αν οι διεπαφές αυτές επιτρέπουν τον διαχωρισμό των ρόλων. Για παράδειγμα, όλες οι λειτουργίες θα είναι προσβάσιμες από τους διαχειριστές (administrators), αλλά οι χρήστες θα έχουν διαθέσιμο ένα πιο περιορισμένο σύνολο χαρακτηριστικών.
- Ανασκόπηση των ελέγχων πρόσβασης και έλεγχος κλιμάκωσης προνομίων

Τρόποι βελτίωσης των διαδικασιών ταυτοποίησης και εξουσιοδότησης

Ο επαρκής έλεγχος της ταυτότητας και της εξουσιοδότησης απαιτεί:

1. Διασφάλιση ενός ισχυρού κωδικού πρόσβασης
2. Βεβαίωση ύπαρξης επιλεκτικής πρόσβασης (granular access) όταν αυτό και όπου είναι απαραίτητο
3. Διασφάλιση της σωστής προστασίας των διαπιστευτηρίων
4. Εφαρμογή ταυτοποίησης δύο παραγόντων όπου είναι δυνατόν
5. Εξασφάλιση ότι οι μηχανισμοί αποκατάστασης κωδικού πρόσβασης είναι ασφαλείς
6. Βεβαίωση ότι απαιτείται επανέλεγχος της ταυτότητας (re-authentication) για ευαίσθητα χαρακτηριστικά/λειτουργίες.
7. Διασφάλιση διαθέσιμων επιλογών για ελέγχους διαμόρφωσης / ρύθμισης του κωδικού πρόσβασης
8. Εξασφάλιση ότι τα διαπιστευτήρια (credentials) μπορούν να ανακληθούν
9. Ύπαρξη απαραιτήτως ελέγχου ταυτότητας της εφαρμογής (app authentication)
10. Ύπαρξη απαραιτήτως ελέγχου ταυτότητας της συσκευής (device authentication)
11. Ύπαρξη απαραιτήτως ελέγχου ταυτότητας του διακομιστή (server authentication)
12. Διαχείριση της ταυτότητας του πιστοποιημένου χρήστη (credential info), της ταυτότητας του χρήστη της συσκευής, της ταυτότητας του

χρήστη της εφαρμογής πίνακα χαρτογράφησης στο διακομιστή ελέγχου ταυτότητας

13. Εξασφάλιση ότι το κλειδί token/session ταυτοποίησης, που εκδίδεται στον πελάτη είναι πάντα διαφορετικό.
14. Διασφάλιση ότι τα ID χρήστη, συσκευής και εφαρμογής είναι παγκοσμίως μοναδικά

Σενάρια επιθέσεων

Σενάριο 1ο : Η διασύνδεση απαιτεί μόνο απλό κωδικό χρήστη.
Username = Bob; Password = 1234

Σενάριο 2ο : Το όνομα χρήστη και ο κωδικός πρόσβασης προστατεύονται ελάχιστα όταν μεταδίδονται μέσω του δικτύου.
Authorization: Basic YWRtaW46MTIzNA==

Στις παραπάνω περιπτώσεις, ο εισβολέας είναι σε θέση είτε να μαντέψει εύκολα τον κωδικό πρόσβασης είτε είναι σε θέση να πιάσει και καταγράψει τα διαπιστευτήρια καθώς διασχίζουν το δίκτυο και στη συνέχεια να τα αποκωδικοποιήσει, αφού τα διαπιστευτήρια προστατεύονται μόνο χρησιμοποιώντας την κωδικοποίηση Base64.

5.1.3 Ανασφαλής Υπηρεσίες Δικτύου

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στη συσκευή μέσω δικτυακής σύνδεσης, συμπεριλαμβανομένων των εξωτερικών και εσωτερικών χρηστών.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί ευάλωτες υπηρεσίες δικτύου για να επιτεθεί στην ίδια τη συσκευή ή να αποβάλει επιθέσεις από τη συσκευή. Η επίθεση μπορεί να προέρχεται από εξωτερικούς ή εσωτερικούς χρήστες.

Αδυναμία ασφάλειας (security weakness): Οι ανασφαλείς δικτυακές υπηρεσίες ενδέχεται να είναι επιρρεπείς σε επιθέσεις υπερχείλισης buffer ή επιθέσεις που δημιουργούν μια κατάσταση άρνησης παροχής υπηρεσιών, αφήνοντας τη συσκευή

απρόσιτη για τον χρήστη. Οι επιθέσεις άρνησης εξυπηρέτησης κατά άλλων χρηστών μπορούν επίσης να διευκολυνθούν όταν είναι διαθέσιμες μη ασφαλείς υπηρεσίες δικτύου. Οι ανασφαλείς υπηρεσίες του δικτύου μπορούν συχνά να ανιχνευθούν με αυτοματοποιημένα εργαλεία όπως οι port σαρωτές και οι fuzzers.

Τεχνικές επιπτώσεις (technical impacts): Οι μη ασφαλείς υπηρεσίες δικτύου μπορούν να οδηγήσουν σε απώλεια δεδομένων, διαφθορά, άρνηση εξυπηρέτησης ή διευκόλυνση επιθέσεων σε άλλες συσκευές.

Επιχειρηματικές επιπτώσεις (Business Impacts): Εξετάζοντας τις επιχειρηματικές επιπτώσεις των συσκευών που έχουν καταστεί άχρηστες από επίθεση «άρνησης υπηρεσίας» ή ότι η συσκευή χρησιμοποιείται για τη διευκόλυνση επιθέσεων κατά άλλων συσκευών και δικτύων διαπιστώνουμε ότι θα μπορούσαν να βλαφθούν οι πελάτες καθώς και οι άλλοι χρήστες.

Είναι οι δικτυακές μου υπηρεσίες ασφαλείς;

Ο έλεγχος για υπηρεσίες ανασφαλών δικτύων περιλαμβάνει:

- Προσδιορισμό εάν υπάρχουν ανασφαλείς υπηρεσίες δικτύου, μέσω ελέγχου της συσκευής μας για ανοιχτές θύρες, χρησιμοποιώντας port σαρωτή.
- Εντοπισμό ανοιχτών θυρών, όπου η κάθε μια μπορεί να δοκιμαστεί χρησιμοποιώντας οποιοδήποτε αριθμό αυτοματοποιημένων εργαλείων που αναζητούν τρωτά σημεία DoS, ευπάθειες που σχετίζονται με τις υπηρεσίες UDP, ευπάθειες που σχετίζονται με την υπερχείλιση buffer και τις fuzzing επιθέσεις.
- Έλεγχο των θυρών του δικτύου, προκειμένου να βεβαιωθεί ότι είναι απολύτως απαραίτητες και αν υπάρχουν κάποιες θύρες που εκτίθενται στο Internet χρησιμοποιώντας το UPnP.

Τρόποι βελτίωσης της ασφάλειας των δικτυακών υπηρεσιών

Η ασφάλιση των υπηρεσιών δικτύου απαιτεί:

- Διασφάλιση ότι μόνο οι απαραίτητες θύρες είναι εκτεθειμένες και διαθέσιμες.
- Διασφάλιση ότι οι υπηρεσίες δεν είναι ευάλωτες σε υπερχείλιση buffer και fuzzing επιθέσεις.

- Διασφάλιση ότι οι υπηρεσίες δεν είναι ευάλωτες σε επιθέσεις DoS που μπορούν να επηρεάσουν τη συσκευή ή άλλες συσκευές ή / και χρήστες στο τοπικό δίκτυο ή σε άλλα δίκτυα.
- Διασφάλιση ότι οι θύρες ή οι υπηρεσίες δικτύου δεν εκτίθενται στο Internet (για παράδειγμα μέσω του UPnP).
- Ανίχνευση και αποκλεισμός της μη κανονικής κυκλοφορίας της αίτησης υπηρεσίας, στο στρώμα gateway υπηρεσίας.

Σενάρια επιθέσεων

` Σενάριο 1ο: Η επίθεση fuzzing προκαλεί συντριβή της υπηρεσίας δικτύου και της συσκευής.

GET %s%s%s%s%s%s%s%s%s%s%s%s%s%s HTTP/1.0

Σενάριο 2ο: Οι θύρες είναι ανοιχτές στο Διαδίκτυο, ενδεχομένως χωρίς τη γνώση του χρήστη, μέσω του UPnP.

Port 80 and 443 exposed to the internet via a home router.

Στις παραπάνω περιπτώσεις, ο εισβολέας μπορεί να απενεργοποιήσει πλήρως τη συσκευή με ένα HTTP GET ή να αποκτήσει πρόσβαση στη συσκευή μέσω του Διαδικτύου, μέσω της θύρας 80 και / ή της θύρας 443.

5.1.4 Έλλειψη κρυπτογράφησης μεταφοράς

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στο δίκτυο με το οποίο είναι συνδεδεμένη η συσκευή, συμπεριλαμβανομένων των εξωτερικών και εσωτερικών χρηστών.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί την έλλειψη κρυπτογράφησης μεταφοράς για να δει τα δεδομένα που διαβιβάζονται μέσω του δικτύου. Η επίθεση μπορεί να προέρχεται από εξωτερικούς ή εσωτερικούς χρήστες.

Αδυναμία ασφάλειας (security weakness): Η έλλειψη κρυπτογράφησης των μεταφορών επιτρέπει την προβολή δεδομένων (ορατά δεδομένα) καθώς μεταφέρονται μέσω τοπικών δικτύων ή μέσω Διαδικτύου. Η έλλειψη κρυπτογράφησης των μεταφορών επικρατεί στα τοπικά δίκτυα, καθώς είναι εύκολο να υποτεθεί ότι η τοπική κυκλοφορία δικτύου δεν θα είναι ευδιάκριτη. Ωστόσο στην περίπτωση ενός τοπικού ασύρματου δικτύου, η λανθασμένη διαμόρφωση (αυτού του ασύρματου δικτύου) μπορεί να καταστήσει την κυκλοφορία ορατή, σε οποιοδήποτε εντός αυτής ασύρματο δίκτυο. Πολλά ζητήματα με την κρυπτογράφηση μεταφοράς είναι εύκολο να εντοπιστούν απλά με την προβολή της κίνησης δικτύου και την αναζήτηση αναγνώσιμων δεδομένων. Τα αυτοματοποιημένα εργαλεία μπορούν επίσης να αναζητήσουν τη σωστή εφαρμογή της κρυπτογράφησης κοινής μεταφοράς, όπως τα πρωτόκολλα SSL και TLS.

Τεχνικές επιπτώσεις (technical impacts): Η έλλειψη κρυπτογράφησης μεταφοράς μπορεί να οδηγήσει σε απώλεια δεδομένων και ανάλογα με τα δεδομένα που εκτίθενται, θα μπορούσε να οδηγήσει σε πλήρη έλεγχο της συσκευής ή των λογαριασμών των χρηστών.

Επιχειρηματικές επιπτώσεις (Business Impacts): Εξετάζοντας τις επιχειρηματικές επιπτώσεις των εκτεθειμένων δεδομένων καθώς αυτά ταξιδεύουν σε διάφορα δίκτυα, βλέπουμε ότι τα δεδομένα θα μπορούσαν να κλαπούν ή να τροποποιηθούν από τρίτους, γεγονός που θα μπορούσε να βλάψει τους χρήστες μας, με την έκθεση των δεδομένων τους.

Η χρήση κρυπτογράφησης μεταφοράς.

Ο έλεγχος για έλλειψη κρυπτογράφησης μεταφοράς περιλαμβάνει:

- Ανασκόπηση της κυκλοφορίας δικτύου της συσκευής, της mobile εφαρμογής και των τυχόν συνδέσεων στο Cloud. για να προσδιοριστεί εάν έχουν μεταβιβαστεί κάποιες πληροφορίες σε καθαρό κείμενο.
- Εξέταση της χρήσης των πρωτοκόλλων SSL ή TLS για επιβεβαίωση ότι είναι ενημερωμένα και σωστά εφαρμοσμένα.
- Έλεγχο της χρήσης οποιωνδήποτε πρωτοκόλλων κρυπτογράφησης για να βεβαιωθεί ότι συνιστώνται και γίνονται αποδεκτά.

Τρόποι χρησιμοποίησης της κρυπτογράφησης μεταφοράς

Η επαρκής κρυπτογράφηση μεταφοράς απαιτεί:

- Διασφάλιση ότι τα δεδομένα είναι κρυπτογραφημένα με τη χρήση πρωτοκόλλων όπως τα SSL και TLS, κατά τη διέλευσή τους στα δίκτυα.
- Διασφάλιση ότι για την προστασία των δεδομένων κατά τη μεταφορά, χρησιμοποιούνται άλλες (industry standard) τεχνικές κρυπτογράφησης, εάν δεν είναι διαθέσιμα τα SSL ή TLS.
- Διαβεβαίωση ότι χρησιμοποιούνται μόνο αποδεκτά πρότυπα κρυπτογράφησης και ότι αποφεύγεται η χρήση ιδιόκτητων πρωτοκόλλων κατά την κρυπτογράφηση.
- Εξασφάλιση της κρυπτογράφησης του ωφέλιμου φορτίου μηνυμάτων (message payload).
- Εξασφάλιση του ασφαλούς κλειδιού κρυπτογράφησης (secure encryption key handshaking).
- Εξασφάλιση της επαλήθευσης της ακεραιότητας των δεδομένων που έχουν ληφθεί.

Σενάρια επιθέσεων

` Σενάριο 1ο: Η διεπαφή Cloud χρησιμοποιεί μόνο http

http://www.xyzcloudsite.com

Σενάριο 2ο: Το όνομα χρήστη και ο κωδικός πρόσβασης μεταδίδονται με σαφήνεια μέσω του δικτύου.

http://www.xyzcloud.com/login.php?userid=3&password=1234

Στις παραπάνω περιπτώσεις, ο επιτιθέμενος έχει τη δυνατότητα να βλέπει καθαρά τα ευαίσθητα δεδομένα λόγω έλλειψης κρυπτογράφησης μεταφοράς.

5.1.5 Προβληματισμοί για την προστασία της ιδιωτικότητας

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στην ίδια τη συσκευή, στο δίκτυο με το οποίο είναι συνδεδεμένη η συσκευή, στην

εφαρμογή για κινητά και στη σύνδεση στο Cloud, συμπεριλαμβανομένων των εξωτερικών και εσωτερικών χρηστών.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί πολλαπλούς τρόπους όπως ο ανεπαρκής έλεγχος ταυτότητας, η έλλειψη κρυπτογράφησης μεταφοράς ή οι ανασφαλείς υπηρεσίες δικτύου για τη θέαση προσωπικών δεδομένων που δεν προστατεύονται σωστά ή συλλέγονται χωρίς λόγο. Η επίθεση μπορεί να προέρχεται από εξωτερικούς ή εσωτερικούς χρήστες.

Αδυναμία ασφάλειας (security weakness): Επικρατούν ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής, που προκύπτουν από τη συλλογή προσωπικών δεδομένων, πέραν της έλλειψης κατάλληλης προστασίας των δεδομένων αυτών. Οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής είναι εύκολο να γίνουν κατανοητές, με μια απλή εξέταση των δεδομένων που συλλέγονται, καθώς ο χρήστης θέτει σε λειτουργία και ενεργοποιεί τη συσκευή. Αυτοματοποιημένα εργαλεία επίσης μπορούν να αναζητούν συγκεκριμένα μοντέλα δεδομένων (data patterns), τα οποία ενδέχεται να υποδεικνύουν τη συλλογή προσωπικών ή άλλων ευαίσθητων δεδομένων.

Τεχνικές επιπτώσεις (technical impacts): Η συλλογή προσωπικών δεδομένων καθώς και η έλλειψη προστασίας των δεδομένων αυτών μπορεί να οδηγήσει σε έκθεση των προσωπικών δεδομένων ενός χρήστη (χωρίς τη βούλησή του).

Επιχειρηματικές επιπτώσεις (Business Impacts): Κρίνεται επιβεβλημένη η εξέταση των επιχειρηματικών επιπτώσεων των προσωπικών δεδομένων που συλλέγονται χωρίς λόγο ή δεν προστατεύονται σωστά. Τα δεδομένα θα μπορούσαν να κλαπούν και να χρησιμοποιηθούν χωρίς τη συγκατάθεση αυτών τους οποίους αφορούν. Έτσι οι πελάτες μας θα μπορούσαν να υποστούν βλάβη από την έκθεση αυτών των προσωπικών δεδομένων.

Υπάρχουν προβλήματα προστασίας των προσωπικών δεδομένων στη συσκευή μας;

Ο έλεγχος για την προστασία της συσκευής από προβλήματα που πλήττουν την ιδιωτικότητα περιλαμβάνει:

- Προσδιορισμό όλων των τύπων δεδομένων που συλλέγονται από τη συσκευή, την εφαρμογή για κινητά και οποιεσδήποτε διασυνδέσεις στο Cloud.
- Διερεύνηση ότι η συσκευή και τα διάφορα εξαρτήματά της συλλέγουν μόνο ότι είναι απαραίτητο για την εκτέλεση της λειτουργίας τους.

- Διερεύνηση αν οι πληροφορίες ταυτοποίησης προσώπου μπορούν να εκτίθενται σε τρίτους επειδή δεν είναι σωστά κρυπτογραφημένες τόσο ενώ βρίσκονται «σε ηρεμία» στα μέσα αποθήκευσης, όσο και κατά τη διάρκεια της διαμετακόμισης μέσω δικτύων
- Διαπίστωση του ποιος έχει πρόσβαση σε προσωπικές πληροφορίες που έχουν συλλεχτεί και προσδιορισμός του αν τα δεδομένα αυτά μπορούν να καταστούν μη αναγνωρίσιμα (de-identified) ή ανώνυμα.
- Προσδιορισμός εάν τα δεδομένα που συλλέγονται υπερβαίνουν αυτό που απαιτείται για την ορθή λειτουργία της συσκευής (Έχει ο τελικός χρήστης επιλογή για αυτή τη συλλογή δεδομένων;).
- Προσδιορισμός εάν υπάρχει πολιτική διατήρησης δεδομένων (retention policy).

Πως μπορούν να αποτραπούν τα προβλήματα για την προστασία της ιδιωτικής ζωής

Η ελαχιστοποίηση των προβλημάτων γύρω από την ιδιωτικότητα απαιτεί:

- Διασφάλιση ότι συλλέγονται μόνο δεδομένα κρίσιμα για τη λειτουργικότητα της συσκευής.
- Εξασφάλιση ότι τα δεδομένα που συλλέγονται είναι τα λιγότερο ευαίσθητα (δηλαδή δε γίνεται προσπάθεια να συλλέξουν ευαίσθητα δεδομένα).
- Εξασφάλιση ότι όλα τα δεδομένα που συλλέγονται αποχαρακτηρίζονται ή καθίστανται ανώνυμα.
- Διασφάλιση ότι τα δεδομένα που συλλέγονται προστατεύονται σωστά με κρυπτογράφηση.
- Βεβαίωση ότι η συσκευή και όλα τα στοιχεία της προστατεύουν σωστά τα προσωπικά στοιχεία των ατόμων.
- Εξασφάλιση ότι μόνο τα εξουσιοδοτημένα άτομα έχουν πρόσβαση σε συλλεγμένες προσωπικές πληροφορίες.
- Εξασφάλιση ότι τα όρια διατήρησης (retention limits) καθορίζονται για τα δεδομένα που συλλέγονται.
- Εξασφάλιση ότι στους τελικούς χρήστες παρέχεται "ειδοποίηση και επιλογή", εάν τα στοιχεία που συγκεντρώνονται υπερβαίνουν τα αναμενόμενα από το προϊόν.

- Εξασφάλιση ότι εφαρμόζεται η πρόσβαση «βάσει ρόλων», στον έλεγχο / εξουσιοδότηση των δεδομένων που συλλέγονται ή αναλύονται.
- Εξασφάλιση ότι τα δεδομένα που έχουν αναλυθεί, είναι αποχαρακτηρισμένα (de-identified).

Σενάρια επιθέσεων

` Σενάριο 1ο: Συλλογή προσωπικών δεδομένων.
Date of birth, home address, phone number, etc.

Σενάριο 2ο: Συλλογή οικονομικών και / ή υγειονομικών πληροφοριών
Credit card data and bank account information.

Στις παραπάνω περιπτώσεις, η έκθεση των δεδομένων οποιουδήποτε από τα παραδείγματα, θα μπορούσε να οδηγήσει σε κλοπή της ταυτότητας ή έλεγχο των λογαριασμών.

5.1.6 Ανασφαλής Cloud Interface

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στο διαδίκτυο

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί πολλαπλούς τρόπους όπως ανεπαρκή έλεγχο ταυτότητας, έλλειψη κρυπτογράφησης μεταφοράς και καταμέτρηση λογαριασμών, για πρόσβαση σε δεδομένα ή ελέγχους μέσω του ιστότοπου Cloud. Η επίθεση θα προέρχεται πιθανότατα από το Διαδίκτυο.

Αδυναμία ασφάλειας (security weakness): Υπάρχει ανασφαλής διασύνδεση στο Cloud όταν χρησιμοποιούνται, εύκολα να ανιχνευτούν διαπιστευτήρια ή όταν είναι δυνατή η καταμέτρηση λογαριασμών. Οι ανασφαλείς Cloud διεπαφές είναι εύκολο να ανακαλυφθούν απλά εξετάζοντας τη σύνδεση στο Cloud Interface και προσδιορίζοντας εάν χρησιμοποιείται πρωτόκολλο SSL ή χρησιμοποιώντας τον μηχανισμό επαναφοράς κωδικού πρόσβασης για τον εντοπισμό έγκυρων λογαριασμών, που μπορούν να οδηγήσουν σε απαρίθμηση λογαριασμών

Τεχνικές επιπτώσεις (technical impacts): Μια ανασφαλής διασύνδεση στο Cloud θα μπορούσε να οδηγήσει σε compromise των δεδομένων του χρήστη και έλεγχο της συσκευής.

Επιχειρηματικές επιπτώσεις (Business Impacts):Επιβάλλεται η εξέταση των επιχειρηματικών επιπτώσεων μιας μη ασφαλούς διασύνδεσης στο Cloud αφού τα δεδομένα θα μπορούσαν να κλαπούν ή να τροποποιηθούν και να χαθεί ο έλεγχος επί των συσκευών. Ενέργειες που θα μπορούσαν να βλάψουν οι πελάτες και το εμπορικό σήμα της εταιρίας.

Είναι το Cloud Interface ασφαλές;

Ο έλεγχος για ένα ανασφαλές Cloud Interface περιλαμβάνει:

- Προσδιορισμό εάν το προεπιλεγμένο όνομα χρήστη και ο κωδικός πρόσβασης μπορούν να αλλάξουν κατά την αρχική ρύθμιση του προϊόντος.
- Προσδιορισμό εάν ένας συγκεκριμένος λογαριασμός χρήστη κλειδώνει μετά από 3 έως 5 αποτυχημένες προσπάθειες σύνδεσης.
- Προσδιορισμό εάν οι έγκυροι λογαριασμοί μπορούν να αναγνωριστούν, χρησιμοποιώντας μηχανισμούς αποκατάστασης κωδικών πρόσβασης ή σελίδες νέων χρηστών.
- Επανεξέταση της διεπαφής για θέματα όπως scripting μεταξύ ιστοτόπων, πλαστογράφηση αιτήσεων μεταξύ τοποθεσιών και έγχυση SQL.
- Ανασκόπηση όλων των διεπαφών του Cloud για ευπάθειες (διεπαφές API και διεπαφές Web που βασίζονται σε Cloud).

Πως μπορούμε να κάνουμε το Cloud Interface ασφαλές

Το ασφαλές Cloud Interface απαιτεί:

- Οι προεπιλεγμένοι κωδικοί πρόσβασης και τα ιδανικά προεπιλεγμένα ονόματα χρηστών πρέπει να αλλάξουν κατά την αρχική ρύθμιση (initial setup).
- Διασφάλιση ότι οι λογαριασμοί χρηστών δεν μπορούν να απαριθμηθούν χρησιμοποιώντας λειτουργίες όπως μηχανισμούς επαναφοράς (reset) κωδικού πρόσβασης.
- Εξασφάλιση κλειδώματος λογαριασμού, μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.

- Διασφάλιση ότι η Cloud-based διεπαφή του ιστού δεν είναι ευαίσθητη σε XSS, SQLi ή CSRF.
- Διασφάλιση των διαπιστευτηρίων από έκθεση στο διαδίκτυο.
- Εφαρμογή ταυτότητας δύο παραγόντων εάν είναι δυνατόν.
- Εντοπισμό ή αποκλεισμό των μη φυσιολογικών αιτημάτων / προσπαθειών

Σενάρια επιθέσεων

` Σενάριο 1ο: Η επαναφορά κωδικού πρόσβασης υποδεικνύει αν ο λογαριασμός είναι έγκυρος

Password Reset "That account does not exist."

Σενάριο 2ο: Το όνομα χρήστη και ο κωδικός πρόσβασης προστατεύονται ελάχιστα όταν μεταδίδονται μέσω του δικτύου.

Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

Στις παραπάνω περιπτώσεις, ο εισβολέας είναι σε θέση είτε να καθορίσει έναν έγκυρο λογαριασμό χρήστη είτε να συλλάβει και καταγράψει τα διαπιστευτήρια καθώς διασχίζουν το δίκτυο. Και στη συνέχεια να τα αποκωδικοποιήσει, αφού τα διαπιστευτήρια προστατεύονται μόνο χρησιμοποιώντας την κωδικοποίηση Base64.

5.1.7 Ανασφαλής Mobile Interface

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στην εφαρμογή για κινητά.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί πολλαπλούς τρόπους όπως ανεπαρκής έλεγχος ταυτότητας, έλλειψη κρυπτογράφησης μεταφοράς και απαρίθμηση λογαριασμού, για πρόσβαση σε δεδομένα ή στοιχεία ελέγχου μέσω της διεπαφής για κινητά.

Αδυναμία ασφάλειας (security weakness): Υπάρχει μια μη ασφαλής mobile interface όταν χρησιμοποιούνται εύκολα να ανιχνευτούν διαπιστευτήρια ή αν είναι δυνατή η απαρίθμηση λογαριασμού. Οι ανασφαλείς mobile διεπαφές είναι εύκολο να ανακαλυφθούν, απλά ανατρέχοντας στη σύνδεση με τα ασύρματα δίκτυα και προσδιορίζοντας αν είναι εν χρήση το SSL ή χρησιμοποιώντας τον μηχανισμό επαναφοράς κωδικού πρόσβασης, για τον εντοπισμό έγκυρων λογαριασμών που μπορούν να οδηγήσουν σε απαρίθμηση λογαριασμών.

Τεχνικές επιπτώσεις (technical impacts): Μια ανασφαλής mobile διασύνδεση μπορεί να οδηγήσει σε έλεγχο επί των δεδομένων του χρήστη και έλεγχο επί της συσκευής.

Επιχειρηματικές επιπτώσεις (Business Impacts): Επιβάλλεται η εξέταση των επιχειρηματικών επιπτώσεων μιας μη ασφαλούς mobile διασύνδεσης αφού τα δεδομένα θα μπορούσαν να κλαπούν ή να τροποποιηθούν και να χαθεί ο έλεγχος επί των συσκευών. Ενέργειες που θα μπορούσαν να βλάψουν οι πελάτες και το εμπορικό σήμα της εταιρίας.

Είναι το Mobile Interface ασφαλές;

Ο έλεγχος για ένα ανασφαλές Mobile Interface περιλαμβάνει:

- Προσδιορισμό εάν το προεπιλεγμένο όνομα χρήστη και κωδικός πρόσβασης μπορού να αλλάξουν κατά την αρχική ρύθμιση του προϊόντος.
- Προσδιορισμό εάν ένας συγκεκριμένος λογαριασμός χρήστη μπορεί να κλειδωθεί μετά από 3 έως 5 αποτυχημένες προσπάθειες σύνδεσης.
- Προσδιορισμό εάν οι έγκυροι λογαριασμοί μπορούν να αναγνωριστούν, χρησιμοποιώντας μηχανισμούς αποκατάστασης κωδικών πρόσβασης ή σελίδες νέων χρηστών.
- Έλεγχο αν τα διαπιστευτήρια (credentials) είναι εκτεθειμένα ενώ είμαστε συνδεδεμένοι σε ασύρματα δίκτυα.
- Έλεγχο αν είναι διαθέσιμες επιλογές αυθεντικοποίησης δύο παραγόντων.

Πως μπορούμε να κάνουμε το Mobile Interface ασφαλές

Το ασφαλές Mobile Interface απαιτεί:

- Οι προεπιλεγμένοι κωδικοί πρόσβασης (passwords) και τα ιδανικά προεπιλεγμένα ονόματα χρηστών (usernames) πρέπει να αλλάζουν κατά την αρχική ρύθμιση.
- Διασφάλιση ότι οι λογαριασμοί χρηστών δεν μπορούν να απαριθμηθούν, χρησιμοποιώντας λειτουργίες όπως μηχανισμοί επαναφοράς κωδικού πρόσβασης.
- Εξασφάλιση κλειδώματος λογαριασμού μετά από 3 έως 5 αποτυχημένες προσπάθειες σύνδεσης.
- Διαβεβαίωση ότι τα διαπιστευτήρια δεν είναι εκτεθειμένα ενόσω είμαστε διασυνδεδεμένοι σε ασύρματα δίκτυα.
- Εφαρμογή, εάν είναι δυνατόν της ταυτοποίησης δύο παραγόντων (two factor authentication).
- Υλοποίηση μιας τεχνικής θωράκισης (obfuscation technic) των εφαρμογών για κινητά (mobile apps).
- Εισαγωγή Μηχανισμού (anti-tempering mechanism) αντιμετώπισης παραβιάσεων εφαρμογών για κινητά.
- Διασφάλιση της μνήμης της εφαρμογής για κινητά από τη δυνατότητα hacking.
- Περιορισμό στην εκτέλεση της εφαρμογής για κινητά, σε κακόβουλο OS περιβάλλον

Σενάρια επιθέσεων

` Σενάριο 1ο: Η επαναφορά κωδικού πρόσβασης υποδεικνύει αν υπάρχει λογαριασμός ή όχι.

Password Reset "That account does not exist."

Σενάριο 2ο: Το όνομα χρήστη και ο κωδικός πρόσβασης προστατεύονται ελάχιστα όταν μεταδίδονται μέσω του δικτύου.

Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

Στις παραπάνω περιπτώσεις, ο εισβολέας είναι σε θέση είτε να καθορίσει έναν έγκυρο λογαριασμό χρήστη είτε να συλλάβει και καταγράψει τα διαπιστευτήρια καθώς διασχίζουν το δίκτυο. Και στη συνέχεια να τα αποκωδικοποιήσει, αφού τα διαπιστευτήρια προστατεύονται μόνο με τη χρήση της κωδικοποίησης Base64.

5.1.8 Ανεπαρκής ρύθμιση παραμέτρων ασφαλείας

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στη συσκευή.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί την έλλειψη επιλεκτικής αδειοδότησης (granular permissions), για να αποκτήσει πρόσβαση στα δεδομένα ή να αποκτήσει τον έλεγχο της συσκευής. Ο επιτιθέμενος θα μπορούσε επίσης να χρησιμοποιήσει την έλλειψη επιλογών κρυπτογράφησης, καθώς και την έλλειψη επιλογών κωδικού πρόσβασης (password), για την εκτέλεση άλλων επιθέσεων που οδηγούν στον έλεγχο της συσκευής (compromise of the device) ή / και των δεδομένων. Η επίθεση θα μπορούσε ενδεχομένως να προέλθει από οποιονδήποτε χρήστη της συσκευής είτε σκόπιμα είτε τυχαία.

Αδυναμία ασφάλειας (security weakness): Υπάρχει ανεπαρκής διαμόρφωση (configurability) των παραμέτρων ασφαλείας, όταν οι χρήστες της συσκευής έχουν περιορισμένη ή καθόλου δυνατότητα να μεταβάλλουν τους ελέγχους ασφάλειάς της. Η ανεπαρκής δυνατότητα ρύθμισης της ασφάλειας είναι εμφανής. όταν η διεπαφή ιστού (web interface) της συσκευής δεν έχει επιλογές για τη δημιουργία ευνοϊκών δικαιωμάτων χρήστη ή, επιβάλλοντας τη χρήση ισχυρών κωδικών πρόσβασης. Η manual ανασκόπηση της διεπαφής ιστού και των διαθέσιμων επιλογών θα αποκαλύψει αυτές τις ελλείψεις.

Τεχνικές επιπτώσεις (technical impacts): Η ανεπαρκής δυνατότητα ρύθμισης της ασφάλειας θα μπορούσε να οδηγήσει σε «συμβιβασμό» της συσκευής (compromise of the device), είτε πρόκειται για εκ προθέσεως ή για τυχαία απώλεια δεδομένων.

Επιχειρηματικές επιπτώσεις (Business Impacts): Επιβάλλεται η εξέταση των επιχειρηματικών επιπτώσεων, στη περίπτωση που τα δεδομένα κλαπούν ή τροποποιηθούν ή χαθεί ο έλεγχος επί των συσκευών. Οι ενέργειες αυτές θα μπορούσαν να βλάψουν τους πελάτες της εταιρίας.

Είναι το Security Configurability ασφαλές;

Η διακρίβωση για ανεπαρκή διαμόρφωση ασφάλειας περιλαμβάνει:

- Έλεγχο της διαχειριστικής διεπαφής (administrative interface) της συσκευής για επιλογές ενίσχυσης της ασφάλειας, όπως η αναγκαστική δημιουργία ισχυρών κωδικών πρόσβασης.
- Ανασκόπηση της διεπαφής διαχείρισης για τη δυνατότητα διαχωρισμού των διαχειριστών χρηστών (admin users) από τους κανονικούς χρήστες.
- Ανασκόπηση της διεπαφής διαχείρισης για επιλογές κρυπτογράφησης.
- Ανασκόπηση της διεπαφής διαχειριστή (administrative interface) για επιλογές που επιτρέπουν ασφαλή καταγραφή διαφόρων συμβάντων ασφαλείας.
- Ανασκόπηση της διαχειριστικής διεπαφής για επιλογές ενεργοποίησης ειδοποιήσεων και ειδοποιήσεων προς τον τελικό χρήστη για συμβάντα ασφαλείας.

Πως μπορούμε να βελτιώσουμε το Security Configurability

Η επαρκής διαμόρφωση της ασφάλειας απαιτεί:

- Διασφάλιση της δυνατότητας διαχωρισμού των κανονικών χρηστών από τους administrative χρήστες.
- Εξασφάλιση της δυνατότητας κρυπτογράφησης δεδομένων σε κατάσταση ηρεμίας ή διέλευσης/μετάδοσης.
- Εξασφάλιση της δυνατότητας επιβολής πολιτικών, ισχυρών κωδικών πρόσβασης.
- Εξασφάλιση της δυνατότητας ενεργοποίησης της καταγραφής συμβάντων ασφαλείας.
- Εξασφάλιση της δυνατότητας ειδοποίησης των τελικών χρηστών για συμβάντα ασφαλείας.

Σενάρια επιθέσεων

` Σενάριο 1ο: Δεν υπάρχει δυνατότητα επιβολής πολιτικών ισχυρών κωδικών πρόσβασης.

Admins and users are allowed to create passwords for their accounts.

Σενάριο 2ο: Δεν υπάρχει δυνατότητα ενεργοποίησης της κρυπτογράφησης δεδομένων σε κατάσταση ηρεμίας.

Password or other sensitive data stored on the device may not be encrypted.

Στις παραπάνω περιπτώσεις, ο εισβολέας μπορεί να χρησιμοποιήσει την έλλειψη αυτών των ελέγχων για να αποκτήσει πρόσβαση σε λογαριασμούς χρηστών που προστατεύονται με αδύναμους κωδικούς πρόσβασης ή πρόσβαση σε δεδομένα σε κατάσταση ηρεμίας.

5.1.9 Ανασφαλές Software/Firmware

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει πρόσβαση στη συσκευή ή / και στο δίκτυο όπου βρίσκεται η συσκευή. Επίσης, όποιος μπορεί να αποκτήσει πρόσβαση στον διακομιστή.

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί πολλαπλούς τρόπους όπως η λήψη αρχείων ενημέρωσης (update files) μέσω μη κρυπτογραφημένων συνδέσεων. Το ίδιο το αρχείο ενημέρωσης δεν είναι κρυπτογραφημένο ή είναι σε θέση να εκτελεί τη δική του κακόβουλη ενημέρωση, μέσω της «πειρατείας» στο ιεραρχημένο και αποκεντρωμένο σύστημα DNS (Domain Name System). Ανάλογα με τη μέθοδο ενημέρωσης και διαμόρφωσης συσκευών, η επίθεση μπορεί να προέρχεται από το τοπικό δίκτυο ή το διαδίκτυο.

Αδυναμία ασφάλειας (security weakness): Από μόνη της η έλλειψη δυνατότητας για update (ενημέρωση) μιας συσκευής προκαλεί αδυναμία στην ασφάλεια. Οι συσκευές θα πρέπει να έχουν τη δυνατότητα ενημέρωσης όταν διαπιστώνονται ευπάθειες και όταν οι ενημερώσεις του software / firmware μπορεί να είναι ανασφαλείς, επειδή τα ενημερωμένα αρχεία και η σύνδεση δικτύου μέσω του οποίου αυτά παραδίδονται, δεν προστατεύονται επαρκώς. Το software / firmware μπορεί επίσης να είναι ανασφαλές εάν περιέχει hardcoded ευαίσθητα δεδομένα όπως είναι τα διαπιστευτήρια. Τα ζητήματα ασφάλειας που αφορούν το software / firmware είναι σχετικά εύκολο να ανακαλυφθούν με μια απλή επιθεώρηση της κυκλοφορίας του δικτύου. Αυτό συμβαίνει κατά τη διάρκεια της ενημέρωσης για να ελεγχτεί η κρυπτογράφηση ή χρησιμοποιώντας έναν hex editor, για να επιθεωρηθεί το ίδιο το αρχείο ενημέρωσης, για ενδιαφέρουσες πληροφορίες.

Τεχνικές επιπτώσεις (technical impacts): Το ανασφαλές software / firmware θα μπορούσε να οδηγήσει σε compromise των δεδομένων των χρηστών, έλεγχο της συσκευής και επιθέσεις σε άλλες συσκευές.

Επιχειρηματικές επιπτώσεις (Business Impacts): Επιβάλλεται η εξέταση του επιχειρηματικού αντίκτυπου, στη περίπτωση που τα δεδομένα κλαπούν ή τροποποιηθούν και χαθεί ο έλεγχος επί των συσκευών οι οποίες περιέρχονται στον έλεγχο τρίτων, με σκοπό την επίθεση σε άλλες συσκευές. Οι ενέργειες αυτές θα μπορούσαν να βλάψουν τους πελάτες της εταιρίας και να προκαλέσουν ζημιές σε άλλους χρήστες.

Είναι το Software/Firmware μας ασφαλές;

Αρχικά πρέπει να σημειώσουμε ότι είναι πολύ σημαντικό οι συσκευές να έχουν κατά κύριο λόγο τη δυνατότητα να ενημερώνονται και να εκτελούν τακτικά ενημερώσεις.

Ο έλεγχος για ανασφαλείς Software/Firmware ενημερώσεις περιλαμβάνει:

- Επανεξέταση του ίδιου του αρχείου ενημέρωσης (update file) για έκθεση ευαίσθητων πληροφοριών, σε μορφές αναγνώσιμες από τον άνθρωπο, από κάποιον που χρησιμοποιεί για επεξεργασία ένα hex edit εργαλείο.
- Ανασκόπηση της παραγωγής του αρχείου ενημέρωσης (update file) για τη σωστή κρυπτογράφηση, χρησιμοποιώντας αποδεκτούς αλγόριθμους.
- Έλεγχος της παραγωγής του αρχείου ενημέρωσης (update file) για να βεβαιωθεί ότι έχει υπογραφεί σωστά με hash.
- Ανασκόπηση της μεθόδου επικοινωνίας που χρησιμοποιείται για τη μετάδοση της ενημέρωσης.
- Εξέταση του διακομιστή ενημέρωσης του Cloud για να διασφαλιστεί ότι οι μέθοδοι κρυπτογράφησης μεταφοράς είναι ενημερωμένες και έχουν ρυθμιστεί σωστά και επίσης ότι ο ίδιος ο διακομιστής δεν είναι ευάλωτος.
- Έλεγχο της συσκευής για σωστή επικύρωση, των υπογεγραμμένων με hash αρχείων ενημέρωσης.

Πως μπορούμε να βελτιώσουμε την ασφάλεια του Software/Firmware

Η ασφάλιση του λογισμικού / firmware απαιτεί:

- Διασφάλιση της δυνατότητας της συσκευής να ενημερώνει (κρίνεται πολύ σημαντικό, χρειάζεται μηχανισμό ασφαλούς ενημέρωσης).
- Διασφάλιση ότι το αρχείο ενημέρωσης κρυπτογραφείται χρησιμοποιώντας αποδεκτές μεθόδους κρυπτογράφησης.
- Διασφάλιση ότι το αρχείο ενημέρωσης μεταδίδεται μέσω κρυπτογραφημένης σύνδεσης.
- Βεβαίωση ότι το αρχείο ενημέρωσης δεν εκθέτει ευαίσθητα δεδομένα.
- Βεβαίωση ότι η ενημέρωση έχει υπογραφεί και επαληθευτεί πριν επιτραπεί η μεταφόρτωση και η εφαρμογή της ενημερωμένης έκδοσης.
- Διασφάλιση ότι ο διακομιστής ενημέρωσης είναι ασφαλής.
- Εφαρμογή ασφαλούς εκκίνησης αν είναι δυνατόν (αλυσίδα εμπιστοσύνης).

Σενάρια επιθέσεων

` Σενάριο 1ο: Το αρχείο ενημέρωσης μεταδίδεται μέσω HTTP.
http://www.xyz.com/update.bin

Σενάριο 2ο: Το αρχείο ενημέρωσης δεν είναι κρυπτογραφημένο και μπορούν να προβληθούν δεδομένα αναγνώσιμα από τον άνθρωπο.

v ñ] Ü Qw û] ˇ3DP Ö ∂] ˇ3DPadmin.htmadvanced.htmalarms. html

+Στις παραπάνω περιπτώσεις, ο εισβολέας είναι σε θέση είτε να «συλλάβει» το αρχείο ενημέρωσης είτε να καταγράψει το αρχείο και να προβάλει τα περιεχόμενά του.

5.1.10 Φτωχή φυσική ασφάλεια

Παράγοντας απειλής (threat agent): Θεωρείται οποιοσδήποτε έχει φυσική πρόσβαση στη συσκευή

Φορείς επίθεσης (attack vectors): Ο επιτιθέμενος χρησιμοποιεί τρόπους όπως θύρες USB, κάρτες SD ή άλλα μέσα αποθήκευσης, για πρόσβαση στο λειτουργικό σύστημα και ενδεχομένως σε οποιαδήποτε δεδομένα αποθηκεύονται στη συσκευή.

Αδυναμία ασφάλειας (security weakness): Οι αδυναμίες φυσικής ασφάλειας είναι παρούσες όταν ένας εισβολέας μπορεί να αποσυναρμολογήσει μια συσκευή για να αποκτήσει εύκολη πρόσβαση στο μέσο αποθήκευσης και σε οποιαδήποτε δεδομένα αποθηκεύονται σε αυτό το μέσο. Υπάρχουν επίσης αδυναμίες όταν δίνεται η δυνατότητα να χρησιμοποιούνται θύρες USB ή άλλες εξωτερικές θύρες, για απόκτηση πρόσβασης στη συσκευή, χρησιμοποιώντας λειτουργίες / χαρακτηριστικά που προορίζονται για διαμόρφωση ή συντήρηση.

Τεχνικές επιπτώσεις (technical impacts): Η ανεπαρκής φυσική ασφάλεια θα μπορούσε να οδηγήσει σε configuration της ίδιας της συσκευής και όλων των δεδομένων που είναι αποθηκευμένα σε αυτή τη συσκευή.

Επιχειρηματικές επιπτώσεις (Business Impacts): Τα δεδομένα ενδέχεται να κλαπούν ή να τροποποιηθούν και η συσκευή να ελέγχεται για σκοπούς διαφορετικούς από αυτό που είχε αρχικά προβλεφθεί. Οι ενέργειες αυτές θα μπορούσαν να βλάψουν τους πελάτες της εταιρίας και το εμπορικό της σήμα.

Είναι επαρκής η φυσική ασφάλεια;

Η διερεύνηση για τη κακή φυσική ασφάλεια περιλαμβάνει:

- Έλεγχο για το πόσο εύκολα μπορεί να αποσυναρμολογηθεί μια συσκευή, έτσι ώστε να αποκτηθεί πρόσβαση στα δεδομένα της ή να αφαιρεθούν από τη συσκευή αυτή τα μέσα αποθήκευσης δεδομένων.
- Έλεγχο της χρήσης εξωτερικών θυρών, όπως USB, για να καθοριστεί εάν μπορούν τα δεδομένα της συσκευής να καταστούν προσβάσιμα χωρίς την αποσυναρμολόγησή της.
- Ανασκόπηση του αριθμού των φυσικών εξωτερικών θυρών για να διαπιστωθεί εάν όλες απαιτούνται για τη σωστή λειτουργία της συσκευής.
- Έλεγχο της διαχειριστικής διεπαφής (administrative interface) για να προσδιοριστεί εάν οι εξωτερικές θύρες, όπως οι θύρες USB, μπορούν να απενεργοποιηθούν.
- Ανασκόπηση της administrative interface για να προσδιοριστεί αν οι διαχειριστικές δυνατότητες μπορούν να περιοριστούν μόνο στην τοπική πρόσβαση.

Τρόποι βελτίωσης της φυσικής ασφάλειας της συσκευής

Η επαρκής φυσική ασφάλεια απαιτεί:

- Διασφάλιση ότι το μέσο αποθήκευσης των δεδομένων δεν μπορεί να αφαιρεθεί εύκολα.
- Διασφάλιση ότι τα αποθηκευμένα δεδομένα είναι κρυπτογραφημένα, σε ηρεμία.
- Βεβαίωση ότι οι θύρες USB ή άλλες εξωτερικές θύρες δεν μπορούν να χρησιμοποιηθούν για απόκτηση κακόβουλης πρόσβασης στη συσκευή.
- Βεβαίωση ότι η συσκευή δεν μπορεί εύκολα να αποσυναρμολογηθεί.
- Βεβαίωση ότι απαιτούνται μόνο οι απαιτούμενες εξωτερικές θύρες, όπως το USB, για τη λειτουργία του προϊόντος.
- Διασφάλιση ότι το προϊόν έχει τη δυνατότητα να περιορίζει τις διαχειριστικές δυνατότητες

Σενάρια επιθέσεων

` Σενάριο 1ο: Η συσκευή μπορεί εύκολα να αποσυναρμολογηθεί και το μέσο αποθήκευσης είναι μια μη κρυπτογραφημένη κάρτα SD.

SD card can be removed and inserted into a card reader to be modified or copied.

Σενάριο 2ο: Οι θύρες USB υπάρχουν στη συσκευή.

Custom software could be written to take advantage of features such as updating via the USB port to modify the original device software.

Και στις δύο περιπτώσεις, ο εισβολέας μπορεί να έχει πρόσβαση στο αρχικό λογισμικό της συσκευής και να κάνει τροποποιήσεις ή απλά να αντιγράψει συγκεκριμένα δεδομένα στόχους.

5.2 ΘΕΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Το Internet of Things παρέχει σε όλους τους οργανισμούς ισχυρά εργαλεία για τη συλλογή και ανάλυση δεδομένων. Αυτά τα δεδομένα έρχονται σε πολλές μορφές και σε πολλές περιπτώσεις με το IoT. Υπάρχουν δεδομένα που συλλέγονται απευθείας ενώ άλλα μπορούν να παραχθούν μέσω προσεκτικής ανάλυσης.

Καθώς οι οργανισμοί και οι επιχειρήσεις αρχίζουν να υιοθετούν το IoT, διαπιστώνουμε την τοποθέτηση αισθητήρων, βιντεοκαμερών και άλλου hardware

υλικού με στόχο τη συλλογή πληροφοριών. Αυτά τα στοιχεία (components) του Διαδικτύου των Αντικειμένων θα αναπτυχθούν ευρύτατα σε δημόσιους χώρους, καθώς και σε ιδιωτικές κατοικίες, ενώ σε ορισμένες περιπτώσεις ακόμη, θα φοριούνται και από τους ανθρώπους. Πολλά στοιχεία του IoT θα περιλαμβάνουν τη χρήση συσκευών συστημάτων παρακολούθησης GPS (Global Positioning System), αυτές οι συσκευές μπορούν να παρέχουν υπηρεσία εντοπισμού θέσης ατόμων ή περιουσιακών στοιχείων ατόμων (π.χ. αυτοκίνητα / τηλέφωνα κλπ).

Μια άλλη πτυχή του IoT είναι ότι πολλά συστήματά του θα αλληλεπικαλύπτονται όσον αφορά τους τύπους των δεδομένων που συλλέγονται. Το γεγονός αυτό, αυξάνει τη δυνατότητα έκθεσης ευαίσθητων πληροφοριών συνολικά, ακόμη και αν τα δύο συστήματα συλλογής λειτουργούν υπό εντελώς διαφορετικές οντότητες. Σε αυτές τις περιπτώσεις, επιχειρηματικοί δρώντες ή κακόβουλοι επιτιθέμενοι μπορούν να χρησιμοποιήσουν αυτά τα συγκεντρωμένα δεδομένα. ώστε να επιτύχουν τους στόχους που έχουν θέσει, χωρίς τα άτομα που παρακολουθούνται να γνωρίζουν κάτι.

Μία από τις μοναδικές προκλήσεις που σχετίζεται με την ιδιωτική ζωή στο διαδίκτυο είναι ότι σύντομα θα υπάρχει η δυνατότητα να κατακλυστεί η κοινωνία με συσκευές συλλογής δεδομένων και αισθητήρες. Αυτές οι συσκευές, ενδεχομένως να χρησιμοποιηθούν κάποιες φορές κακόβουλα και άλλες φορές μπορεί να συλλαμβάνουν/συλλέγουν κατά λάθος πληροφορίες για άτομα που δεν έχουν συναινέσει στην παρακολούθησή τους.

Από την άποψη του ιδιοκτήτη ενός συστήματος, είναι σημαντικό να γίνει κατανοητό ποιες ενέργειες επιτρέπονται πάνω στα δεδομένα ιδιωτών που συλλέγονται κατά λάθος. Ωστόσο οι αισθητήρες IoT θα πρέπει να χρησιμοποιηθούν επίσης με τρόπους που βελτιώνουν την εμπειρία των πελατών. Σε αυτές τις περιπτώσεις, ο πελάτης θα ειδοποιηθεί ότι αλληλεπιδρά με κάποιο σύστημα IoT. Πρέπει να εξεταστεί επακριβώς ποια δεδομένα εξακολουθούν να υφίστανται για κάθε χρήστη και τον αντίκτυπο που έχει αυτό, πάνω στη συμμόρφωση με τους κανονισμούς περί προστασίας της ιδιωτικής ζωής. Το ίδιο ισχύει και για τη συμμόρφωση με βιομηχανικά πρότυπα όπως το PCI, το οποίο απαιτεί την κρυπτογράφηση του PII τόσο σε κατάσταση ηρεμίας όσο και κατά τη μεταφορά. Εκτός από την επαλήθευση ότι όλες οι ευαίσθητες πληροφορίες προστατεύονται επαρκώς, είναι επίσης σημαντικό να εξεταστούν και οι κίνδυνοι που σχετίζονται με την αλυσίδα εφοδιασμού. Αν τα συστατικά στοιχεία που συνθέτουν το σύστημα του διαδικτύου των αντικειμένων είναι

compromised στην αλυσίδα εφοδιασμού, ο κίνδυνος έκθεσης ευαίσθητων πληροφοριών είναι υψηλός.

Μια άλλη πτυχή σχετίζεται με το ποιος έχει πρόσβαση στα αποθηκευμένα απόρρητα ιδιωτικά δεδομένα. Τα δεδομένα αυτά είναι πιθανόν να παρασχεθούν σε τρίτους, έτσι η πρόσβαση σε οποιαδήποτε ευαίσθητη πληροφορία θα πρέπει να καταγράφεται, για τους σκοπούς του ελέγχου και επιπλέον να ελέγχεται η συμμόρφωση προς τις ακολουθούμενες πολιτικές.

Δεδομένης της πολυπλοκότητας του τοπίου, για τη διαφύλαξη της ιδιωτικότητας στο Internet of Things, είναι σημαντικό για κάθε οργανισμό που προσφέρει δυνατότητες βασισμένες στο IoT, να δαπανήσει τους κατάλληλους πόρους, προκειμένου να εξασφαλίσει και να διαφυλάξει τις ευαίσθητες πληροφορίες των ενδιαφερομένων. Καθώς δομείται ένα IoT σύστημα, ακολουθώντας βάσει σχεδιασμού τις αρχές τήρησης του ιδιωτικού απορρήτου, πρέπει να επιτραπεί η ενσωμάτωση των κατάλληλων διασφαλίσεων του απορρήτου της ιδιωτικής ζωής, εντός του συστήματος. Για κάθε συγκεκριμένο οργανισμό ή επιχείρηση, αυτές οι αρχές μπορούν να ακολουθηθούν κατά τον σχεδιασμό της υλοποίησης των διαφόρων συνιστωσών (components) που αποτελούν ένα σύστημα IoT. Η ομάδα εργασίας της Ευρωπαϊκής Ένωσης (ΕΕ) για την προστασία των δεδομένων (άρθρο 29) εξέδωσε οδηγία το Σεπτέμβριο του 2014, δηλώνοντας ότι «όλοι οι εμπλεκόμενοι στο IoT θα πρέπει να υιοθετήσουν αυτές τις αρχές, σε εφαρμογές εντός οποιαδήποτε περιοχής του κόσμου».

Οι ενότητες που ακολουθούν, παρέχουν μια ειδικά για το IoT εικόνα αυτών των αρχών, που μπορούν να χρησιμοποιήσουν οι οργανισμοί και οι επιχειρήσεις, προκειμένου να ενισχύσουν τα προγράμματα προστασίας της ιδιωτικότητάς τους, για την υποστήριξη των εφαρμογών IoT.

Αρχές προστασίας, από το σχεδιασμό

Οι χρήστες των IoT συστημάτων θα πρέπει να ενημερώνονται για όλα τα δεδομένα που συλλέγονται από αυτά ή σχετικά με αυτά και θα πρέπει να τους δίνεται η δυνατότητα να εξαιρούνται από τις πρακτικές συλλογής δεδομένων σε granular επίπεδο. Αναγνωρίζοντας τις ανησυχίες ότι πολλές από τις συσκευές IoT ενδέχεται να μην έχουν σωστή διεπαφή χρήστη (user interface), οι εταιρείες πρέπει να βρουν κατάλληλες μεθόδους ώστε να παρέχουν την επιλογή και την ειδοποίηση στους καταναλωτές.

1. Πρόδραση όχι αντίδραση, πρόληψη όχι θεραπεία

Στο πλαίσιο ενός IoT συστήματος, είναι σημαντικό να εξεταστούν οι πιθανές επιπτώσεις επί της ιδιωτικής ζωής για όλους τους ενδιαφερόμενους, πριν το σύστημα τεθεί σε κατάσταση λειτουργίας. Στην αρχή, η ανάλυση θα επικεντρωθεί στους τύπους των δεδομένων που συλλέγονται, για να γίνει κατανοητό ποιά είναι ευαίσθητα και ποιες ρυθμίσεις ισχύουν για κάθε τύπο δεδομένων. Στη συνέχεια, θα γίνει μια πιο εμπεριστατωμένη ανάλυση, για να κατανοηθούν οι έμμεσες συνέπειες επί της ιδιωτικής ζωής των λειτουργιών των διαφόρων συνιστωσών του IoT.

Όταν ασχολούμαστε για παράδειγμα με εφαρμογές που παρακολουθούν συνδεδεμένα οχήματα, θα ήταν σημαντικό να καταλάβουμε αν η παρακολούθηση αυτή εκθέτει τα σχέδια/μοτίβα οδήγησης, που αν και ανώνυμα, θα μπορούσαν τελικά να αναχθούν σε ένα άτομο ή ομάδα ατόμων, αν συνδυαστούν με δεδομένα που συλλέγονται από άλλα συστήματα. Μια άλλη περίπτωση αφορά το θέμα της συλλογής δεδομένων για ανάλυση από έξυπνους μετρητές, οι οποίοι τροφοδοτούνται στις εταιρείες κοινής ωφελείας. Εάν η πρόσβαση στα δεδομένα αυτά δεν ελέγχεται αυστηρά, οι επιτιθέμενοι μπορούν να συμπεράνουν πότε ένα άτομο είναι στο σπίτι, δίνοντας έτσι την ευκαιρία και για φυσικές επιθέσεις.

Εξετάζοντας το απόρρητο των δεδομένων στο σύνολό τους, σε σχέση με το απόρρητο των δεδομένων της ιδιωτικής ζωής που συλλέγονται από ένα και μόνο σύστημα, παρέχεται η δυνατότητα για εντοπισμό των δυνητικά σοβαρών προβλημάτων προστασίας της ιδιωτικότητας, πριν την έκθεση και την εκμετάλλευσή τους από αδίστακτα άτομα.

2. Η μυστικότητα ως προεπιλογή

Οι οργανισμοί και οι επιχειρήσεις που αναπτύσσουν IoT δυνατότητες πρέπει αυτό να το λάβουν σοβαρά υπόψη και να ενσωματώνουν στα συστήματά τους ελέγχους προστασίας της μυστικότητας. Οι έλεγχοι θα αφορούν τη διασφάλιση του απορρήτου τόσο των συσκευών όσο και των εφαρμογών που παρέχονται από οποιονδήποτε προμηθευτή.

3. Προστασία του απορρήτου ενσωματωμένη στο σχεδιασμό

Οι οργανισμοί που εφαρμόζουν IoT λειτουργικότητα, το πρώτο που θα αντιμετωπίσουν είναι η κατανόηση των ανησυχιών των ενδιαφερομένων (ομάδων συμφερόντων) για την προστασία των δεδομένων της ιδιωτικής τους ζωής. Ως εκ

τούτου, είναι κρίσιμη η διεξαγωγή ανάλυσης για τον προσδιορισμό των στοιχείων δεδομένων που θα επεξεργαστεί ένα σύστημα IoT. Αυτό ιδανικά, θα πρέπει να πραγματοποιηθεί σε συνδυασμό με τη συνιστώμενη ανάλυση απειλών και μάλιστα από νωρίς στο σχεδιασμό του συστήματος IoT.

Μόλις γίνουν κατανοητές οι δυνητικές έμμεσες επιπτώσεις από τη συλλογή των δεδομένων, μπορούν από την αρχή να σχεδιαστούν στο σύστημα IoT οι κατάλληλες διασφαλίσεις, σε σχέση με το να σχεδιαστούν εκ των υστέρων, μετά από αυξημένη ανησυχία ή εκμετάλλευση των δεδομένων από τρίτους. Επίσης, οι εταιρείες θα πρέπει να επανεκτιμήσουν το πρόγραμμα κοινοποίησης παραβιάσεων των προσωπικών τους δεδομένων, για να καλύψουν τις πτυχές που σχετίζονται με το Διαδίκτυο.

4. Πλήρης Λειτουργικότητα – Θετικό Άθροισμα όχι Μηδενικό Άθροισμα

Συνήθως υπάρχει μια ισορροπία μεταξύ των στόχων της λειτουργικότητας και της ασφάλειας που πρέπει να διατηρηθούν, για να διασφαλιστεί ότι κάθε συγκεκριμένο σύστημα λειτουργεί σωστά, πληροί τους επιχειρησιακούς στόχους και εξακολουθεί να είναι ασφαλές. Το ίδιο μπορεί να λεχθεί και για την προστασία της ιδιωτικής ζωής.

Στην περίπτωση του IoT, είναι εξαιρετικά σημαντικό να γίνουν από νωρίς οι συμβιβασμοί μεταξύ λειτουργικότητας και ασφάλειας-προστασίας της ιδιωτικής ζωής, κατά τη φάση της διαδικασίας του σχεδιασμού, προκειμένου να διασφαλιστεί η ισότιμη επίτευξη όλων των στόχων. Ο εντοπισμός ενός προβλήματος προστασίας των ιδιωτικών δεδομένων, στην επιχειρησιακή ζωή ενός συστήματος IoT, θα καταστήσει προκλητική τη διαδικασία του εκσυγχρονισμού των ελέγχων τήρησης απορρήτου. Σε συμμόρφωση με την αρχή Privacy-by-Design, ο εντοπισμόw και η εφαρμογή αυτών των συμψηφισμών (λειτουργικότητας/ασφάλειας) πρέπει να γίνει όταν το κόστος είναι σχετικά μικρό, δηλαδή κατά τη διάρκεια του σχεδιασμού του συστήματος IoT.

5. Ασφάλεια από άκρο σε άκρο - Προστασία κύκλου ζωής

Στο πλαίσιο του IoT, τα δεδομένα που συλλέγονται θα έχουν μεγάλη διάρκεια ζωής. Είναι σημαντικό να εξεταστεί η πλήρης διάρκεια ζωής των συλλεγόμενων δεδομένων, τόσο εντός του οργανισμού συλλογής όσο και στο κάθε τρίτο μέρος προς το οποίο παρέχονται. Οι ενδιαφερόμενοι (stakeholders) πρέπει να γνωρίζουν πότε τα δεδομένα παρέχονται σε τρίτους, τους ελέγχους που χρησιμοποιούνται για τη διασφάλιση τους, τον τρόπο με τον οποίο διατίθενται και τον χρόνο στον οποίο δίνονται τα δεδομένα.

Η προστασία του κύκλου ζωής ισχύει επίσης για τα δεδομένα δεύτερης τάξης (πληροφορίες σχετικά με τα άτομα, που συνάγονται ή προσδιορίζονται βάσει πρωτογενών δεδομένων). Για παράδειγμα, εάν ένας αισθητήρας στο αυτοκίνητό μας συλλέγει πληροφορίες για «πόσο μακριά», «πού», «πόσο γρήγορα» και άλλα χαρακτηριστικά των οδηγικών μας συνηθειών, τότε εύκολα κάποιος θα μπορούσε να συμπεράνει διάφορα πράγματα γύρω από εμάς. Τα πράγματα αυτά ενδεχομένως να αφορούν τις αγορές μας ή τις συνήθειες της εργασίας μας, ή το που κοινωνικοποιούμαστε ή που αλληλεπιδρούμε και άλλες προτιμήσεις μας. Ο ιδιοκτήτης των δεδομένων (π.χ. η εταιρεία αυτοκινήτων) μπορεί να διαγράψει τα πρωτογενή μας δεδομένα κατά την πώληση του οχήματός μας, αλλά στην πραγματικότητα να κρατήσει όλες τις υπονοούμενες πληροφορίες (κοινωνική σύνδεση, συνήθειες αγορών κλπ.) για ενδεχόμενη αξιοποίηση.

6. Ορατότητα και διαφάνεια

Οι ενδιαφερόμενοι θα πρέπει να είναι σε θέση να αναγνωρίζουν εύκολα τα δεδομένα που συλλέγονται από αυτούς για οποιοδήποτε συγκεκριμένο σύστημα IoT, καθώς και τις σχεδιαζόμενες ή πιθανές χρήσεις αυτών των δεδομένων. Θα πρέπει επίσης να επιτρέπεται στα ενδιαφερόμενα μέρη να επιλέγουν τη συλλογή δεδομένων, τόσο σε coarse όσο και σε granular επίπεδο. Για παράδειγμα, αν μια εφαρμογή παρακολουθεί τα πρότυπα οδήγησης (π.χ. για λόγους ασφάλισης), ο χρήστης θα πρέπει να είναι σε θέση να εξουσιοδοτήσει ρητά τη χρήση των δεδομένων του για το σκοπό αυτό (coarse επίπεδο). Ο χρήστης πρέπει επίσης να είναι σε θέση να παρέχει ρητή εξουσιοδότηση για μεμονωμένα στοιχεία δεδομένων, εάν κάτι τέτοιο είναι επιθυμητό, για παράδειγμα η αποθήκευση μοτίβων οδήγησης ή του ιστορικού που λαμβάνεται μέσω GPS.

7. Σεβασμός για το απόρρητο των χρηστών

Η διατήρηση της προστασίας της ιδιωτικότητας των πληροφοριών των ενδιαφερομένων μερών, θα αποτελέσει τελικά έναν παράγοντα που εισάγει διακρίσεις για τις επιχειρήσεις της εποχής του IoT. Με τόσες πολλές ευκαιρίες για τη χειραγώγηση της ιδιωτικής ζωής των χρηστών, οι οργανισμοί που λαμβάνουν τα απαραίτητα μέτρα για τη διασφάλιση των ευαίσθητων πληροφοριών, θα κριθούν πολύ πιο ευνοϊκά από εκείνους που δεν το κάνουν. Με αυτό τον τρόπο, είναι σημαντικό να ενσταλάξουμε μια νοοτροπία ευαισθητοποίησης για την ιδιωτικότητα, μέσα στον οργανισμό. Αυτό θα

μπορούσε να περιλάβει τον διορισμό ενός ή περισσοτέρων «υπερασπιστών της ιδιωτικότητας», για την αξιολόγηση των επιπτώσεων πάνω στην ιδιωτική ζωή, του κάθε νέου συστήματος IoT που εφαρμόζεται. Ιδανικά σε αυτούς τους ανθρώπους (υπερασπιστές) θα παρέχεται εξουσία, να επιβάλλουν αλλαγές στα σχέδια του IoT συστήματος, σε περίπτωση που εντοπιστούν προβλήματα και εκφραστούν ανησυχίες για την προστασία της ιδιωτικής ζωής.

Το απόρρητο των χρηστών επηρεάζεται επίσης έμμεσα. Στην περίπτωση ορισμένων συσκευών IoT, για παράδειγμα έξυπνα γυαλιά, ο χρήστης έχει συναινέσει σε ρήτρες προστασίας της ιδιωτικής ζωής, αλλά το παρατηρούμενο αντισυμβαλλόμενο μέρος πιθανότατα δεν το έχει πράξει. Πρέπει να διεξαχθούν περαιτέρω έρευνες ώστε να κατανοηθούν οι επιπτώσεις και να καθοριστούν οι κανονισμοί που απαιτούνται για την περίπτωση που ισχύσουν αυτά τα σενάρια.

8. Εκτίμηση των επιπτώσεων στην ιδιωτική ζωή

Εάν διαπιστωθεί ότι μια συσκευή συλλέγει, επεξεργάζεται ή αποθηκεύει προστατευμένες πληροφορίες που αφορούν το ιδιωτικό απόρρητο (PPI), τότε απαιτούνται αυστηρότεροι έλεγχοι. Αυτοί οι έλεγχοι πρέπει να είναι ένα μείγμα πολιτικών και τεχνικών. Για παράδειγμα: Η παροχή της συσκευής ενδέχεται να απαιτεί περισσότερες διοικητικές εγκρίσεις.

- Θα πρέπει να διερευνηθεί από τον εσωτερικό έλεγχο ή να υλοποιηθεί συμμόρφωση με πρότυπα, προκειμένου να καθοριστεί εάν είναι βιώσιμο το να υπάρχουν δεδομένα PPI για συσκευές IoT.
- Τα δεδομένα που είναι αποθηκευμένα στη συσκευή θα πρέπει να κρυπτογραφούνται χρησιμοποιώντας επαρκώς ισχυρούς κρυπτογραφικούς αλγόριθμους.
- Τα δεδομένα που μεταδίδονται από / στη συσκευή πρέπει να κρυπτογραφούνται με επαρκώς ισχυρούς κρυπτογραφικούς αλγόριθμους.
- Η πρόσβαση στη συσκευή, τόσο φυσική όσο και λογική, πρέπει να περιορίζεται σε εξουσιοδοτημένο προσωπικό.

Υπάρχουν διάφορες συστάσεις σχετικά με τις απαιτήσεις περί της προστασίας της ιδιωτικής ζωής που πρέπει να λαμβάνονται υπόψη, βάσει της γεωγραφικής περιοχής, όπως:

- Βόρεια Αμερική
    - ✓ Διαδίκτυο των Αντικειμένων
    - ✓ Προστασία της ιδιωτικής ζωής και της ασφάλειας σε έναν συνδεδεμένο κόσμο.
    - ✓ Έκθεση προσωπικού της Ομοσπονδιακής Επιτροπής Εμπορίου (FTC).

- Ευρώπη
    - ✓ Συστάσεις για την προστασία της ιδιωτικής ζωής για το Διαδίκτυο,
    - ✓ Το WP29 της ΕΕ (Ευρωπαϊκός συμβουλευτικός φορέας για την προστασία των δεδομένων).
    - ✓

5.3 ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΑΠΕΙΛΩΝ

Η μοντελοποίηση απειλών, στην επιστήμη της ασφάλειας στον κυβερνοχώρο είναι μια δομημένη προσέγγιση για τον εντοπισμό, την ποσοτικοποίηση και την αντιμετώπιση των απειλών. Η μοντελοποίηση απειλών επιτρέπει στο προσωπικό ασφαλείας του συστήματος να γνωστοποιεί την ενδεχόμενη ζημιά των ελαττωμάτων ασφαλείας και να προτεραιοποιεί τις προσπάθειες αποκατάστασης.

Η μοντελοποίηση απειλών καλύπτει τα assets, αναφέρεται στο ποια δεδομένα και εξοπλισμός πρέπει να εξασφαλιστούν, στις απειλές που μπορεί να εκδηλώσει στο σύστημα ένας επιτιθέμενος και στα τρωτά σημεία της συσκευής. Παρακάτω προσεγγίζεται μια προσομοίωση απειλών, για συσκευές IoT:

ΒΗΜΑ 1: Προσδιορισμός των Assets:

Αυτό αφορά την καταγραφή σε κατάλογο των διαφόρων στοιχείων του συστήματος IoT που πρόκειται να αναπτυχθούν. Εξετάζονται όχι μόνο οι συσκευές IoT αλλά και οι αποθήκες δεδομένων και οι εφαρμογές με τις οποίες επικοινωνούν οι συσκευές και οι χρήστες που αλληλεπιδρούν με το σύστημα.

ΒΗΜΑ 2: Δημιουργία συστήματος, επισκόπηση αρχιτεκτονικής:

Αυτό το βήμα παρέχει μια σταθερή βάση για την κατανόηση όχι μόνο της αναμενόμενης λειτουργικότητας του συστήματος IoT, αλλά και του τρόπου με τον

οποίο ένας εισβολέας θα μπορούσε να καταχραστεί το σύστημα. Η αρχή γίνεται με τη διαδικασία τεκμηρίωσης της αναμενόμενης λειτουργικότητας και στη συνέχεια αφιερώνεται χρόνος για την εξέταση και την τεκμηρίωση των περιπτώσεων κατάχρησης του συστήματος. Είναι επίσης σημαντικό να δημιουργηθεί ένα αρχιτεκτονικό διάγραμμα που να περιγράφει λεπτομερώς το νέο σύστημα IoT και τον τρόπο διασύνδεσης του συστήματος με άλλους επιχειρησιακούς υπολογιστικούς πόρους και συστήματα ασφαλείας. Αυτό το διάγραμμα μπορεί επίσης να χρησιμεύσει ως σημείο εκκίνησης για τον προσδιορισμό των ορίων εμπιστοσύνης, των μηχανισμών ελέγχου ταυτότητας και εξουσιοδότησης καθώς και για την καταγραφή συνθέσεων.

Η δημιουργία της αρχιτεκτονικής του συστήματος ενισχύεται μέσω της χρήσης ανάλυσης περίπτωσης. Το παρακάτω παράδειγμα χρησιμοποιεί περιπτώσεις από τον τομέα της υγειονομικής περίθαλψης και μπορεί να παρέχει πληροφορίες σε θέματα ασφαλείας, για εφαρμογές IoT.

- Ένα άτομο φοράει κάποιο είδος monitor που αναφέρει μέσω του Cloud στον ιατρό του.
- Σε ακραίες περιπτώσεις, θα αποσταλούν αυτόματα οι πρώτες ανταποκρίσεις.
- Θα παραχθεί αυτόματα μια νέα συνταγή φαρμακείου (με κάποιον κανόνα) ή εναλλακτικά θα κατευθύνονταν οι πληροφορίες συνταγών σε πολλά φαρμακεία που θα ανταγωνίζονταν για την αγορά.
- Θα προγραμματιστεί αυτόματα ένα ραντεβού.
- Θα ενημερωθούν τα αρχεία υγείας.
- Εάν αποσταλεί ιατρική απάντηση, τα δεδομένα μεταφέρονται σε ασθενοφόρο.

Μια εμφυτευμένη συσκευή λαμβάνει κάποια εντολή. Στο παράδειγμα αυτό τα ερωτήματα που ανακύπτουν είναι:

- Η συσκευή χρησιμοποιεί PKI;
- Εάν ναι, μπορεί η συσκευή να επιβεβαιώσει την κατάσταση ανάκλησης του αποστολέα;
- Μπορεί η συσκευή να επικυρώσει το μήνυμα;
- Μπορεί η συσκευή να δημιουργήσει έναν ασφαλή σύνδεσμο ή συνεδρία με τον αποστολέα;
- Μπορεί η συσκευή να ζητήσει επιβεβαίωση;

Ένας γιατρός καθιερώνει μια επικοινωνιακή συνεδρία με smart home/ home monitor, τα ερωτήματα που ανακύπτουν είναι:

- Είναι ασφαλισμένο το κανάλι επικοινωνίας με PKI;
- Τα PII και τα ιατρικά δεδομένα μεταφέρονται με ασφάλεια;
- Η διαδικασία του login διασφαλίζει ανωνυμία;

Ένα νοσοκομείο μεταφέρει το αρχείο ή τη διάγνωση ενός ασθενούς σε υπολογιστή ή PDA.

- Μπορεί ο ασθενής να αλληλεπιδράσει με υπηρεσίες του νοσοκομείου, όπως ο προγραμματισμός ενός άλλου ραντεβού;
- Μπορεί ο ασθενής να επιβεβαιώσει την αυθεντικότητα του μηνύματος;
- Μπορεί ο ασθενής να αφαιρέσει αποτελεσματικά το μήνυμα;

Η αιμοδοσία ενός ασθενή γίνεται από έναν ηλεκτρονικό αναλυτή.

- Είναι ο αριθμός παρακολούθησης για τον δότη προστατευμένο τοπικά ή κεντρικά;
- Θα ενημερωθεί άμεσα ο ασθενής για οποιαδήποτε διαπίστωση;
- Εάν ο ασθενής έχει SDT ποιοι οργανισμοί θα ειδοποιηθούν;
- Ποιοι είναι οι μηχανισμοί της εμπιστοσύνης;
- Θα χειριστεί το πακέτο αίματος ένα ρομπότ;
- Το φαρμακείο ή ο γιατρός του ασθενούς θα μιλήσουν για κάποια συγκεκριμένη διαπίστωση/εύρημα;
- Το κέντρο συντήρησης θα ενημερωθεί για την κατάσταση του αναλυτή;

Σε περίπτωση έκτακτης ανάγκης, αποστέλλονται πολλαπλές πρώτες ανταποκρίσεις (responders).

- Τα ιατρικά δεδομένα μεταφέρονται με ασφάλεια στο σωστό ασθενοφόρο;
- Μπορούν οι ανταποκρινόμενοι να επικοινωνούν με τα δεδομένα ασθενών με ασφάλεια;
- Γίνεται το παραπάνω μέσω σημείου προς σημείο ή μέσω κεντρικής δρομολόγησης (central routing);

- Είναι η ασφάλεια, η εμπιστοσύνη και η προστασία της ιδιωτικής ζωής διαχειριζόμενη από πολλές αλυσίδες εμπιστοσύνης;
- Η αντλία έγχυσης έχει επικοινωνία κλειστού βρόχου με τον ελεγκτή / οθόνη;

Ο γιατρός εκτελεί τηλεχειρουργική με τη χρήση ρομπότ

- Είναι το κανάλι επικοινωνίας αξιόπιστο και ασφαλές;
- Το διακριτικό όνομα του ρομπότ είναι αξιόπιστο με την κονσόλα;
- Η επικοινωνία εξαρτάται από το DNS;
- Ποια είναι η ισχύς των αλγορίθμων και του μήκους κλειδιών που χρησιμοποιεί το IP VPN;
- Ποια είναι η αλυσίδα εμπιστοσύνης και η διαχείριση CRL για ολόκληρη την τοπολογία;
- Τα κανάλια εφεδρικής επικοινωνίας εμπιστεύονται στο ίδιο επίπεδο με το πρωτεύον;
- Οι πάροχοι φαρμάκων και τα αρχεία ενημερώνονται σε πραγματικό χρόνο;

Μια κυβερνητική υπηρεσία εκδίδει μια προειδοποίηση για την υγεία που επηρεάζει τις εμφυτευμένες συσκευές.

- Σε ποια σειρά κοινοποιούνται τα ενδιαφερόμενα μέρη; (γιατροί, φαρμακεία, κατασκευαστές, διαχειριστές συστημάτων κ.λπ.).
- Το μήνυμα ταχτοποιείται και επαληθεύεται;
- Σε περίπτωση ανάκλησης μιας συσκευής, ποιες βάσεις δεδομένων πρέπει να ενημερωθούν;
- Η διαχείριση του αποθέματος είναι τέτοια που να διασφαλίσει ότι όλες οι συσκευές διαχειρίζονται σωστά;

Μια εμφυτευμένη ή φορητή συσκευή χρειάζεται ενημέρωση.

- Η ενημέρωση γίνεται με απομακρυσμένη διαχείριση;
- Υπάρχει αμφίδρομη εμπιστοσύνη μεταξύ της συσκευής και του κεντρικού διακομιστή;
- Είναι το κανάλι ασφαλές και αξιόπιστο;

- Η διαχείριση του αποθέματος διασφαλίζει ότι όλες οι συσκευές διαχειρίζονται σωστά;
- Τα ενδιαφερόμενα μέρη ενημερώνονται εάν αλλάξουν οι διαδικασίες ή οι οδηγίες;
- Αναφέρεται το φαρμακείο εάν εμπλέκονται τα ναρκωτικά;

Ο ιατρός ελέγχου για μια συγκεκριμένη συσκευή αντικαθίσταται από άλλο γιατρό.

- Τα διαπιστευτήρια διαχειρίζονται κεντρικά ή τοπικά;
- Υπάρχει αμφίδρομη εμπιστοσύνη μεταξύ του γιατρού και της συσκευής;
- Μπορεί η συσκευή να ενημερωθεί από απόσταση για να εκχωρήσει νέα εμπιστοσύνη;

Ο κατασκευαστής τροποποιεί τις οδηγίες του για μια τηλεχειριζόμενη ιατρική συσκευή.

- Είναι σωστή η διατήρηση της διαμόρφωσης, ώστε οι ενδιαφερόμενοι να γνωρίζουν την έκδοση των συσκευών / οδηγιών;
- Περιλαμβάνονται τα ιατρικά πανεπιστήμια ως μέρος των ενδιαφερομένων;
- Υπάρχει μια έγκυρη βάση δεδομένων για τη διαχείριση των ρυθμίσεων;

Σε περιβάλλον συνδεδεμένου οχήματος, ένα ασθενοφόρου / όχημα πρώτης ανταπόκρισης συντονίζει τα αρχεία ασθενών με ιατρικό πάροχο.

- Είναι οι επικοινωνίες προστατευμένες με PKI;
- Υπάρχει αμφίδρομη εμπιστοσύνη μεταξύ του ασθενοφόρου και του ιατρού;
- Τα αρχεία ασθενών καθαρίζονται μετά την αποστολή του ασθενούς;
- Διαχειρίζεται εξ αποστάσεως εξοπλισμό επί του σκάφους;

Ένας ασθενής με εμφυτευμένη συσκευή καλεί 911.

- Τα δεδομένα ασθενών διατίθενται στον αποστολέα;
- Μπορεί ο αποστολέας να δρομολογήσει δεδομένα σε απομακρυσμένο πάροχο ή ιατρό;

- Υπάρχει μια σχέση εμπιστοσύνης αμφίδρομη;
- Τα αρχεία ασθενών ενημερώνονται αυτόματα;
- Είναι δυνατή η ασφαλής επικοινωνία των πληροφοριών με ένα ασθενοφόρο;

Ένα ιδιωτικό Cloud αναπτύσσεται στη Νότια Αμερική για να εξυπηρετεί απομακρυσμένες ιατρικές κοινότητες.

- Μπορεί η υποδομή να ελεγχθεί, για να εξακριβωθεί ότι πληρούνται τα πρότυπα ασφαλείας;
- Το σύστημα υποστηρίζει συσκευές που είναι συνδεδεμένες εξ αποστάσεως;
- Υπάρχει αμφίδρομη εμπιστοσύνη με τους απομακρυσμένους πελάτες;
- Πώς επαληθεύεται η ταυτότητα των ενδιαφερομένων;

Οι νανο-βιοϊατρικές συσκευές αναπτύσσονται εξ αποστάσεως.

- Υπάρχουν σχέσεις αξιόπιστης (έμπιστης) αμφίδρομης επικοινωνίας με την κεντρική εγκατάσταση;
- Είναι κάθε στοιχείο στην τοπολογία αξιόπιστο;
- Οι ενότητες (modules) που ανακτώνται προστατεύονται σωστά, όσον αφορά ευαίσθητες ιατρικές πληροφορίες (σωματική ασφάλεια);
- Το απόθεμα παρακολουθείται με ασφάλεια;

Μόλις ολοκληρωθεί η προβολή της λογικής αρχιτεκτονικής, είναι σημαντικό να προσδιοριστούν και να εξεταστούν οι συγκεκριμένες τεχνολογίες που θα αποτελέσουν το IoT σύστημα. Αυτό περιλαμβάνει την κατανόηση και την τεκμηρίωση λεπτομερών χαμηλότερου επιπέδου, σχετικά με τις συσκευές IoT, όπως ο επεξεργαστής και το λειτουργικό σύστημα. Αυτό θα παρέχει τις πληροφορίες που απαιτούνται για την κατανόηση των συγκεκριμένων τύπων ευπάθειας, που τελικά ενδεχομένως θα εκτεθούν και παράλληλα θα καθορίσει διαδικασίες, για το πώς και πόσο συχνά πρέπει να εφαρμόζονται οι ενημερώσεις κώδικα και firmware.

Η κατανόηση και η τεκμηρίωση των πρωτοκόλλων που χρησιμοποιούνται από κάθε συσκευή IoT θα επιτρέψει επίσης την ενημέρωση της αρχιτεκτονικής, ειδικά εάν

εντοπιστούν κενά στην κρυπτογράφηση που εφαρμόζεται, στα δεδομένα που μεταδίδονται σε όλο το σύστημα και την οργάνωση.

ΒΗΜΑ 3: Αποσύνθεση του συστήματος IoT.

Το στάδιο αυτό επικεντρώνεται στην κατανόηση του Κύκλου Ζωής των δεδομένων καθώς ρέουν μέσω του συστήματος. Αυτή η κατανόηση θα επιτρέψει τον εντοπισμό των ευάλωτων και αδύναμων σημείων της αρχιτεκτονικής της ασφάλειας που πρέπει να αντιμετωπιστούν. Απαιτείται ο προσδιορισμός και η τεκμηρίωση των σημείων εισόδου για δεδομένα μέσα στο σύστημα. Σε ένα IOT σύστημα, αυτά τα σημεία εισόδου είναι κάποιου είδους αισθητήρες.

Απαιτείται ο εντοπισμός της ροής των δεδομένων από τα σημεία εισόδου, η τεκμηρίωση των διαφόρων στοιχείων που αλληλεπιδρούν με αυτά τα δεδομένα σε όλο το σύστημα και ο προσδιορισμός στόχων υψηλού προφίλ για επιτιθέμενους - αυτές μπορεί να είναι σημεία εντός του συστήματος που συγκεντρώνουν ή αποθηκεύουν δεδομένα ή μπορεί να είναι αισθητήρες υψηλής αξίας που απαιτούν σημαντικές προστασίες για να διατηρηθεί η συνολική ακεραιότητα του συστήματος. Με το τέλος αυτής της δραστηριότητας θα έχει υλοποιηθεί μια καλή κατανόηση της επιφάνειας επίθεσης του νέου συστήματος IoT.

Μόλις διαχωρίσουμε το σύστημα IoT, το επόμενο βήμα θα πρέπει να είναι ο σχεδιασμός μιας αρχιτεκτονικής κατάλληλης για την προστασία του συστήματος. Μια θεωρητική προστατευτική αρχιτεκτονική θα μπορούσε να είναι αυτή όπου κάποια από τα στοιχεία του SdP μπορούν να εισαχθούν. Με βάση τα σχόλια του Junaid, συμπεριλαμβάνουμε ένα πλασματικό διάγραμμα το οποίο μπορούμε να προσαρμόσουμε στο περιβάλλον του IoT. Ενέργειες:

- Δεν επιτρέπετε σε τίποτα να συνδεθεί με αυτά
- Επαλήθευση της ταυτότητας στις πύλες
- Χρησιμοποίηση εξουσιοδότησης για την ανύψωση της εμπιστοσύνης
- Μείωση των κλοπών των κλειδιών
- Άρνηση όλων των συνδέσεων
- Απαιτείται άδεια για την έναρξη της επικοινωνίας
- Χρήση ανεξάρτητης θύρας επικοινωνίας για τους διαχειριστές
- Καταγραφή ελέγχου

- Επικοινωνία με τους ακροδέκτες και ενημέρωση του Root
- Χρησιμοποίηση ασφαλούς εκκίνησης
- Χρησιμοποίηση hardened OS
- Λίστα επιτρεπόμενων εφαρμογών (application whitelisting)
- Παρακολούθηση ακεραιότητας αρχείων
- Καταγραφή ελέγχου
- Ανταπόκριση ενημερώσεων

ΒΗΜΑ 4: Προσδιορισμός και καταγραφή των απειλών.

Το δημοφιλές **μοντέλο STRIDE** μπορεί να εφαρμοστεί στην ανάπτυξη του συστήματος IoT. Απαιτείται η χρήση γνωστών αποθετηρίων (αποθηκών) ευπάθειας για την καλύτερη κατανόηση του περιβάλλοντος, όπως είναι η κοινή βάση δεδομένων MITER για τις ευπάθειες και τις εκθέσεις. Η αποκάλυψη των μοναδικών απειλών σε οποιαδήποτε συγκεκριμένη παραλλαγή του IoT, θα καθοδηγείται από αυτούς τους τύπους απειλών:

Sppofing Identity	Εξετάστε το σύστημα για απειλές που σχετίζονται με την πλαστογράφηση της ταυτότητας μηχανής και την ικανότητα ενός εισβολέα να ξεπεράσει αυτοματοποιημένες σχέσεις εμπιστοσύνης μεταξύ συσκευών. Ελέγξτε προσεκτικά τα πρωτόκολλα ελέγχου ταυτότητας που σκοπό έχουν να δημιουργήσουν ασφαλείς επικοινωνίες μεταξύ διάφορων συσκευών (M2M) και μεταξύ συσκευών και εφαρμογών που χρησιμοποιούν τα δεδομένα που παρέχονται από αυτές τις συσκευές. Εξετάστε τη διαδικασία παροχής των ταυτοτήτων σε κάθε IoT συσκευή και βεβαιωθείτε ότι υπάρχουν οι κατάλληλοι διαδικαστικοί έλεγχοι για τον περιορισμό της δυνατότητας εισαγωγής μιας συσκευής απατεώνα (rogue device), στο σύστημα.
Παραβιάζοντας δεδομένα	Εξετάστε τη διαδρομή των δεδομένων σε ολόκληρο το σύστημα IoT. Προσδιορίστε τα σημεία στο σύστημα που παρέχουν μια ευκαιρία να παραβιάζουν τα δεδομένα σε σημεία συλλογής,

	επεξεργασίας, μεταφοράς και αποθήκευσης. Ελέγξτε προσεκτικά την εφαρμογή των μηχανισμών έγκρισης για να εξασφαλιστεί ότι οι παραβιάσεις δεδομένων αντιμετωπίζονται αποτελεσματικά.
Αποκήρυξη	Εξετάστε το σχεδιασμό του συστήματος IoT για κόμβους εντός του, που είναι κρίσιμοι πάροχοι δεδομένων. Αυτοί πιθανώς είναι σύνολα αισθητήρων που παρέχουν διάφορα δεδομένα για ανάλυση. Στην περίπτωση του IoT, είναι σημαντικό να μπορέσουμε να εντοπίσουμε back data σε μια πηγή και να διασφαλίσουμε ότι ήταν πράγματι η αναμενόμενη πηγή που παρείχε αυτά τα δεδομένα. Εξετάστε το IoT για αδυναμίες που θα επέτρεπαν σε έναν εισβολέα την έγχυση ενός rogue κόμβου που θα τροφοδοτούσε κακόβουλα δεδομένα στο σύστημα σε μια προσπάθεια να προκαλέσει σύγχυση σε upstream διαδικασίες ή να θέσει το σύστημα εκτός λειτουργίας. Βεβαιωθείτε ότι οι επιτιθέμενοι δεν είναι σε θέση να πλήξουν την σκοπούμενη λειτουργικότητα των συστημάτων IoT, π.χ. οι παράνομες λειτουργίες είναι απενεργοποιημένες ή δεν επιτρέπονται. Αλλαγές κατάστασης και χρονικές παραλλαγές (διακοπή της αλληλουχίας μηνυμάτων) πρέπει να ληφθούν υπόψη.
Αποκάλυψη πληροφοριών	Εξετάστε τη διαδρομή των δεδομένων σε όλο το σύστημα IoT, συμπεριλαμβανομένων των συστημάτων επεξεργασίας backend. Βεβαιωθείτε ότι οποιαδήποτε συσκευή που επεξεργάζεται ευαίσθητες πληροφορίες, έχει αναγνωριστεί και ότι τα κατάλληλα στοιχεία ελέγχου κρυπτογράφησης έχουν εφαρμοστεί ώστε να υπάρξει προφύλαξη από ενδεχόμενη αποκάλυψη αυτών των πληροφοριών. Προσδιορίστε τους κόμβους αποθήκευσης δεδομένων στο πλαίσιο του IoT συστήματος και βεβαιωθείτε ότι οι έλεγχοι κρυπτογράφησης δεδομένων σε κατάσταση

	καθυστέρησης (data-at-rest) έχουν εφαρμοστεί. Εξετάστε το σύστημα IoT για περιπτώσεις, κατά τις οποίες οι συσκευές IoT είναι ευάλωτες στο να κλαπούν φυσικά και διασφαλίστε ότι οι κατάλληλοι έλεγχοι, όπως ο μηδενισμός του κλειδιού, έχουν ληφθεί υπόψη.
Άρνηση παροχής υπηρεσίας	Εκτελέστε μια δραστηριότητα που χαρτογραφεί κάθε σύστημα IoT σε επιχειρησιακούς στόχους, σε μια προσπάθεια να διασφαλιστεί ότι ο κατάλληλος σχεδιασμός της συνέχισης των λειτουργιών (Continuity of operation planning - COOP) έχει συντελεστεί. Ελέγξτε τη διακίνηση που παρέχεται σε κάθε κόμβο στο σύστημα και βεβαιωθείτε ότι αρκεί να αντέξει τις σχετικές επιθέσεις DoS. Εξετάστε τις δομές μηνυμάτων (π.χ., τα λεωφορεία δεδομένων), τις δομές δεδομένων, την ακατάλληλη χρήση μεταβλητών και το API, που χρησιμοποιούνται εντός των εφαρμοστέων συνιστωσών IoT και προσδιορίζουν εάν υπάρχουν τρωτά σημεία που θα επέτρεπαν σε έναν rogue κόμβο να πνίξει τις μεταδόσεις ενός νόμιμου κόμβου. Οι φορείς υλοποίησης του IoT θα πρέπει επίσης να εξετάσουν το ρυθμό περιορίζοντας τα API's για να μετριάσουν τις επιθέσεις DoS.
Ανύψωση του προνομίου	Εξετάστε τις δυνατότητες διαχείρισης που παρέχονται από τις διάφορες IoT συσκευές, που αποτελούν ένα σύστημα IoT. Σε μερικές περιπτώσεις υπάρχει μόνο ένα επίπεδο ελέγχου ταυτότητας, η οποία επιτρέπει τη διαμόρφωση των στοιχείων της συσκευής. Σε άλλες περιπτώσεις ενδέχεται να είναι διαθέσιμοι ξεχωριστοί, διακριτοί λογαριασμοί διαχειριστή. Προσδιορίστε περιπτώσεις όπου υπάρχουν αδυναμίες στην ικανότητα διαχωρισμού των διοικητικών λειτουργιών, από τις λειτουργίες επιπέδου χρήστη, εντός των κόμβων IoT. Προσδιορίστε τις αδυναμίες στις μεθόδους ελέγχου ταυτότητας που χρησιμοποιούνται από τους κόμβους IoT, προκειμένου να σχεδιαστούν οι κατάλληλοι έλεγχοι ταυτότητας στο σύστημα.

Παρακάμπτοντας τη φυσική ασφάλεια	Εξετάστε τους μηχανισμούς φυσικής προστασίας που προσφέρει η κάθε συσκευή IoT και σχεδιάστε μετριασμούς όπου αυτό είναι δυνατόν, έναντι οποιωνδήποτε εντοπισμένων αδυναμιών. Αυτό είναι ιδιαίτερα αληθινό για εφαρμογές IoT που είτε τοποθετούνται δημόσια, είτε σε απομακρυσμένες περιοχές.
Εισβολές κοινωνικής μηχανικής	Εκπαιδεύστε το προσωπικό σας απέναντι στις προσπάθειες της κοινωνικής μηχανικής και παρακολουθείστε τακτικά τα assets για ύποπτη συμπεριφορά.
Λάθη εφοδιαστικής αλυσίδας	Κατανοήστε τις διάφορες τεχνολογικές συνιστώσες που συνθέτουν συσκευές και συστήματα IoT και παρακολουθείστε (ανιχνεύστε τα τρωτά σημεία που σχετίζονται με οποιαδήποτε από αυτά τα τεχνολογικά επίπεδα.
Εισβολές δικτύου	Παρακολουθείτε τακτικά τα δίκτυα για ύποπτες συμπεριφορές.

5.4 ΕΠΙΦΑΝΕΙΑ ΕΠΙΘΕΣΗΣ

Το έργο IoT Attack Surface Areas παρέχει έναν κατάλογο επιφανειών επίθεσης που πρέπει να κατανοηθούν από τους κατασκευαστές, τους υπεύθυνους ανάπτυξης, τους ερευνητές στον τομέα της ασφάλειας και όσους επιθυμούν να αναπτύξουν ή να εφαρμόσουν τεχνολογίες IoT στους οργανισμούς τους. Παρακάτω θα αναφερθεί η επιφάνεια επίθεσης καθώς και τα τρωτά σημεία της συγκεκριμένης επιφάνειας επίθεσης.

Έλεγχος πρόσβασης οικοσυστήματος

Σιωπηρή εμπιστοσύνη μεταξύ των στοιχείων Ασφάλεια εγγραφής

Σύστημα παροπλισμού

Απώλεια διαδικασιών πρόσβασης

Μνήμη συσκευής

Ονόματα χρηστών καθαρού κειμένου

Κωδικοί πρόσβασης καθαρού κειμένου

Τριών μερών πιστοποιήσεις, κλειδιά κρυπτογράφησης

Συσκευές φυσικών διεπαφών, εξαγωγή firmware

Γραμμή διεπαφής γραμμής εντολών (CLI)

Διασύνδεση γραμμής εντολών διαχειριστή (CLI)

Προσαρμογή προνομίου

Επαναφορά στην κατάσταση ανασφάλειας

Αφαίρεση μέσων αποθήκευσης

Αντοχή σε παραβίαση

Θύρα εντοπισμού σφαλμάτων

Αναγνώριση συσκευής / Έκθεση σειριακού αριθμού

Διεπαφή Web συσκευής SQL Injection

Σεναριοποίηση (scripting) μεταξύ ιστοτόπων

Αίτημα πλαστοπροσωπίας μεταξύ τοποθεσιών

Καταμέτρηση ονόματος χρήστη

Αδύναμοι κωδικοί πρόσβασης

Κλείδωμα λογαριασμού

Γνωστά πιστοποιητικά προεπιλογής

Firmware συσκευής

Κωδικοποιημένα (hardcoded) διαπιστευτήρια

Ευαίσθητη αποκάλυψη πληροφοριών

Ευαίσθητη αποκάλυψη διευθύνσεων URL

Κλειδιά κρυπτογράφησης

Κρυπτογράφηση (συμμετρική, ασύμμετρη)

Εμφάνιση έκδοσης υλικολογισμικού και / ή τελευταία ημερομηνία ενημέρωσης

Backdoor λογαριασμοί

Ευάλωτες υπηρεσίες (web, ssh, tftp κ.λπ.)

Λειτουργία που σχετίζεται με την ασφάλεια

Έκθεση API

Υποβιβασμός firmware

Υπηρεσίες δικτύου συσκευών

Αποκάλυψη πληροφοριών

CLI χρήστη

Διαχειριστική injection CLI

Άρνηση παροχής υπηρεσίας

Μη κρυπτογραφημένες υπηρεσίες

Κακή εφαρμογή κρυπτογράφησης

Υπηρεσίες δοκιμών / ανάπτυξης

Υπερχείλιση buffer UPnP

Ευάλωτες υπηρεσίες UDP DoS

Firmware συσκευής

Μπλοκ ενημέρωσης OTA

Επανάληψη επίθεσης

Έλλειψη επαλήθευσης ωφέλιμου φορτίου

Έλλειψη ελέγχου ακεραιότητας μηνυμάτων

Διοικητική διεπαφή

SQL injection

Σεναριοποίηση (scripting) μεταξύ ιστοτόπων

Cross-site Request Forgery

Απαρίθμηση χρήστη

Αδύναμοι κωδικοί πρόσβασης

Κλείδωμα λογαριασμού

Γνωστά προεπιλεγμένα διαπιστευτήρια

Επιλογές ασφαλείας / κρυπτογράφησης

Επιλογές καταγραφής

Έλεγχος ταυτότητας δύο παραγόντων

Αδυναμία σκουπίσματος της συσκευής

Τοπική αποθήκευση δεδομένων

Μη κρυπτογραφημένα δεδομένα

Δεδομένα κρυπτογραφημένα με κλειδιά που εντοπίστηκαν

Έλλειψη ελέγχων ακεραιότητας δεδομένων

Χρήση του στατικού κλειδιού Clou / dec

Διασύνδεση Web

SQL injection

Σεναριοποίηση μεταξύ ιστοτόπων

Cross-site Request Forgery

Απαρίθμηση χρήστη

Αδύναμοι κωδικοί πρόσβασης

Κλείδωμα λογαριασμού

Γνωστά προεπιλεγμένα διαπιστευτήρια

Κρυπτογράφηση μεταφοράς

Μη ασφαλής μηχανισμός ανάκτησης κωδικού πρόσβασης

Έλεγχος ταυτότητας δύο παραγόντων

API υποστήριξης τρίτου μέρους

Μη κρυπτογραφημένο PII έστειλε κρυπτογραφημένο PII

Πληροφορίες σχετικά με τη συσκευή διαρρέουν

Η τοποθεσία έχει διαρρεύσει

Μηχανισμός ενημέρωσης

Ενημέρωση που αποστέλλεται χωρίς κρυπτογράφηση

Οι ενημερώσεις δεν έχουν υπογραφεί

Ενημέρωση εγγράψιμης τοποθεσίας

Ενημέρωση επιβεβαίωσης

Ενημέρωση ελέγχου ταυτότητας

Κακή ενημέρωση

Έλλειψη μηχανισμού ενημέρωσης

Δεν υπάρχει μηχανισμός μη αυτόματης ενημέρωσης

Εφαρμογή κινητού

Εμπιστευμένη από συσκευή ή το cloud

Καταμέτρηση ονόματος χρήστη

Λογαριασμός κλειδώματος λογαριασμού

Γνωστά προεπιλεγμένα διαπιστευτήρια

Αδύναμοι κωδικοί πρόσβασης

Ασφαλής αποθήκευση δεδομένων

Κρυπτογράφηση μεταφοράς

Μη ασφαλής μηχανισμός ανάκτησης κωδικού πρόσβασης Έλεγχος ταυτότητας δύο παραγόντων

API Backend προμηθευτή

Εγγενής εμπιστοσύνη του Cloud ή της κινητής τηλεφωνίας

Αδύναμος έλεγχος ταυτότητας

Αδύναμοι έλεγχοι πρόσβασης

Επιθέσεις εισβολής

Κρυφές υπηρεσίες

Επικοινωνία με το οικοσύστημα

Έλεγχοι υγείας Καρδιάς

Εντολές οικοσυστήματος

Αποσπάσματα

Πιέζοντας ενημερώσεις

Κυκλοφορία δικτύου

LAN

LAN στο Διαδίκτυο

Σύντομη εμβέλεια

Μη τυποποιημένα

Ασύρματο (WiFi, Z-κύμα, Zigbee, Bluetooth)

Πρωτόκολλο fuzzing

Έλεγχος ταυτότητας / Εξουσιοδότηση

Σχετικές τιμές ελέγχου ταυτότητας/εξουσιοδότησης (κλειδί περιόδου λειτουργίας, διακριτικό, cookie, κ. λπ.) αποκάλυψη.

Επαναχρησιμοποίηση του κλειδιού περιόδου λειτουργίας, διακριτικό, κ. λπ. Έλεγχος ταυτότητας device to device.

Device to mobile έλεγχος ταυτότητας εφαρμογών. Device to cloud σύστημα έλεγχος ταυτότητας

Εφαρμογή για κινητές συσκευές στον έλεγχο ταυτότητας συστήματος cloud

Εφαρμογή Web για έλεγχο ταυτότητας συστήματος cloud

Έλλειψη δυναμικού ελέγχου ταυτότητας

Προστασία προσωπικών δεδομένων

Αποκάλυψη δεδομένων χρήστη

Αποκάλυψη θέσης χρήστη/συσκευής

Διαφορικό απόρρητο

Hardware Υλικό (αισθητήρες)

Ανίχνευση χειραγώγησης περιβάλλοντος αλλοίωση (φυσικά)

Επιζήμια (σωματικά)

Οι επιφάνειες επίθεσης θα συνδυαστούν τώρα με τις πιο κοινές ευπάθειες που αντιμετωπίζει το Διαδίκτυο των πραγμάτων:

Ευπάθεια απαρίθμησης όνομα χρήστη. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διοικητική διεπαφή, η διεπαφή ιστού συσκευών, η διασύνδεση cloud και η εφαρμογή για κινητά. Με αυτήν την ευπάθεια δίνεται η δυνατότητα συλλογής

ενός συνόλου έγκυρων ονομάτων χρηστών, αλληλεπιδρώντας με τον μηχανισμό ελέγχου ταυτότητας.

Ευπάθεια αδύναμου κωδικού πρόσβασης. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διοικητική διεπαφή, η διεπαφή ιστού συσκευών, η διασύνδεση cloud και η εφαρμογή για κινητά. Δίνεται η δυνατότητα να οριστούν κωδικοί πρόσβασης λογαριασμών, που μπορούν εύκολα να «σπάσουν» όπως για παράδειγμα οι '1234' ή '123456'.

Ευπάθεια κλειδώματος λογαριασμού. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διοικητική διεπαφή, η διεπαφή ιστού συσκευών, η διασύνδεση cloud και η εφαρμογή για κινητά. Με αυτό το θέμα ευπάθειας δίνεται η δυνατότητα να συνεχίσει να στέλνει προσπάθειες ελέγχου ταυτότητας μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.
Ευπάθεια συσκευών χωρίς κρυπτογράφηση. Η επιφάνεια επίθεσης για αυτήν την ευπάθεια είναι οι υπηρεσίες δικτύων συσκευών. Οι υπηρεσίες δικτύου δεν είναι κατάλληλα κρυπτογραφημένες για την αποτροπή της παρακολούθησης από τους εισβολείς.

Ευπάθεια έλλειψης ελέγχου ταυτότητας δύο παραγόντων. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διαχειριστική διεπαφή, το περιβάλλον web cloud και η εφαρμογή για κινητά. Η έλλειψη μηχανισμών επαλήθευσης δύο παραγόντων, όπως ένα διακριτικό ασφαλείας ή ένας σαρωτής δακτυλικών αποτυπωμάτων.

Ευπάθεια κακής εφαρμογής της κρυπτογράφησης. Στόχευση υπηρεσιών δικτύου συσκευών. Η κρυπτογράφηση που υλοποιείται εντούτοις δεν είναι σωστά ρυθμισμένη ή δεν ενημερώνεται σωστά, π.χ. SSL v2.

Ευπάθεια αποστολής ενημερώσεων χωρίς κρυπτογράφηση. Στοχεύει τον μηχανισμό ενημέρωσης και οι ενημερώσεις μεταδίδονται μέσω του δικτύου χωρίς τη χρήση του TLS ή την κρυπτογράφηση του ίδιου του αρχείου ενημέρωσης.

Εγγράψιμη ενημερωμένη τοποθεσία στοχεύει τον μηχανισμό ενημέρωσης. Η θέση αποθήκευσης για τα αρχεία ενημέρωσης είναι εγγράψιμη σε όλο τον κόσμο, επιτρέποντας έτσι την τροποποίηση και τη διανομή firmware σε όλους τους χρήστες.

Ευπάθεια άρνησης εξυπηρέτησης. Η επιφάνεια επίθεσης για αυτήν την ευπάθεια είναι η υπηρεσία δικτύου συσκευών. Η υπηρεσία μπορεί να δεχθεί επίθεση κατά τρόπο που να μην επιτρέπει την εξυπηρέτηση στην εν λόγω υπηρεσία ή σε ολόκληρη τη συσκευή.

Τρωτότητα αφαίρεσης μέσων αποθήκευσης. Στοχεύει στις φυσικές διεπαφές της συσκευής και δίνει τη δυνατότητα φυσικής απομάκρυνσης των μέσων αποθήκευσης από τη συσκευή.

No manual μηχανισμός ενημέρωσης. Στοχεύει τον μηχανισμό ενημέρωσης και δεν υπάρχει δυνατότητα χειροκίνητης επιβολής ελέγχου επιτήρησης για τη συσκευή.

Έλλειψη μηχανισμού ενημέρωσης. Στοχεύει τον μηχανισμό ενημέρωσης και δεν υπάρχει δυνατότητα ενημέρωσης της συσκευής.

Εμφάνιση έκδοσης Firmware ή / και η τελευταία ημερομηνία ενημέρωσης. Στοχεύει το Firmware της συσκευής και δεν εμφανίζεται η τρέχουσα έκδοση Firmware και / ή δεν εμφανίζεται η τελευταία ημερομηνία ενημέρωσης.

5.5 ΑΝΑΛΥΣΗ FIREWARE

Το έργο «IoT Περιοχές Επιφάνειας Επίθεσης» (Attack Surface Areas), παρέχει έναν κατάλογο επιφανειών επίθεσης που πρέπει να κατανοούν οι κατασκευαστές, οι υπεύθυνοι ανάπτυξης, οι ερευνητές στον τομέα της ασφάλειας και όσοι επιθυμούν να αναπτύξουν ή να εφαρμόσουν τεχνολογίες IoT στους οργανισμούς τους. Παρακάτω θα αναφερθεί η συγκεκριμένη επιφάνεια επίθεσης και τα τρωτά σημεία της.

Έλεγχος πρόσβασης οικοσυστήματος

Σιωπηρή εμπιστοσύνη μεταξύ των στοιχείων

Ασφάλεια εγγραφής

Σύστημα παροπλισμού

- Απώλεια διαδικασιών πρόσβασης

Μνήμη συσκευής

- Ονόματα χρηστών καθαρού κειμένου
- Κωδικοί πρόσβασης καθαρού κειμένου
- Πιστοποιητικά τρίτου μέρους
- Κλειδιά κρυπτογράφησης

Φυσικές διεπαφές συσκευής

- Εξαγωγή Firmware

Διεπαφή γραμμής εντολών χρήστη (CLI)

- Διασύνδεση διεπαφής γραμμής εντολών διαχειριστή (CLI)
- Προσαρμογή προνομίων

Επαναφορά στην κατάσταση μη ασφάλισης

- Αφαίρεση μέσων αποθήκευσης
- Αντοχή σε παραβίαση

Θύρα εντοπισμού σφαλμάτων

- Έκθεση ταυτότητας συσκευής / σειριακού αριθμού
- Διασύνδεση Web συσκευής

SQL injection

Σεναριοποίηση (scripting) μεταξύ ιστοτόπων

- Αίτημα μεταξύ τοποθεσιών
- Καταμέτρηση ονόματος χρήστη πλαστογραφίας
- Αδύναμοι κωδικοί πρόσβασης
- Κλείδωμα λογαριασμού
- Γνωστά πιστοποιητικά προεπιλογής
- Firmware συσκευής

Κωδικοποιημένα (hardcoded) διαπιστευτήρια

- Αποκάλυψη ευαίσθητων πληροφοριών
- Αποκάλυψη ευαίσθητων διευθύνσεων URL
- Κλειδιά κρυπτογράφησης
- Κρυπτογράφηση (συμμετρική, ασύμμετρη)
- Εμφάνιση έκδοσης Firmware και / ή τελευταία ημερομηνία ενημέρωσης
- Backdoor λογαριασμοί

Ευάλωτες υπηρεσίες (web, ssh, tftp κ.λπ.)

Λειτουργία σχετιζόμενη με την ασφάλεια

Απεικόνιση API

Υποβιβασμός Firmware

Υπηρεσίες δικτύου συσκευών

Αποκάλυψη πληροφοριών Χρήστη CLI

Διοικητικός CLI Injection

Άρνηση παροχής υπηρεσίας

Μη κρυπτογραφημένες υπηρεσίες

Κακή εφαρμογή υπηρεσιών κρυπτογράφησης Test / Development

Υπερχείλιση buffer UPnP

Ευάλωτο UDP

Υπηρεσίες DoS

Firmware συσκευής

Μπλοκ ενημέρωσης OTA

Επανάληψη επίθεσης

Έλλειψη επαλήθευσης ωφέλιμου φορτίου

Έλλειψη ελέγχου ακεραιότητας μηνυμάτων

Διαχειριστική διεπαφή

SQL injection

Σεναριοποίηση μεταξύ ιστοτόπων

Αίτηση πλαστοπροσωπίας μεταξύ τοποθεσιών

Καταμέτρηση ονόματος χρήστη

Αδύναμοι κωδικοί πρόσβασης

Κλείδωμα λογαριασμού

Γνωστά προεπιλεγμένα πιστοποιητικά

Επιλογές ασφαλείας / κρυπτογράφησης

Επιλογές logging

Έλεγχος ταυτότητας δύο παραγόντων

Αδυναμία σκουπίσματος (wipe) της συσκευής

Αποθήκευση τοπικών δεδομένων

Μη κρυπτογραφημένα δεδομένα

Δεδομένα κρυπτογραφημένα με κλειδιά που εντοπίστηκαν

Έλλειψη ελέγχων ακεραιότητας δεδομένων

Χρήση στατικού ίδιου κλειδιού enc / dec

Cloud Web Interface

SQL injection

Σεναριοποίηση μεταξύ ιστοτόπων

Αιτήματα πλαστοπροσωπίας μεταξύ τοποθεσιών

Καταμέτρηση ονόματος χρήστη

Αδύναμοι κωδικοί πρόσβασης

Κλείδωμα λογαριασμού

Γνωστά προεπιλεγμένα πιστοποιητικά

Κρυπτογράφηση μεταφοράς

Μη ασφαλής μηχανισμός ανάκτησης κωδικού πρόσβασης

Έλεγχος ταυτότητας δύο παραγόντων

API υποστήριξης τρίτου μέρους

Μη κρυπτογραφημένο PII έστειλε κρυπτογραφημένο PII

Πληροφορίες σχετικά με τη συσκευή διαρρέουν

Η τοποθεσία έχει διαρρεύσει

Μηχανισμός ενημέρωσης

Η ενημερωμένη έκδοση αποστέλλεται χωρίς κρυπτογράφηση

Οι ενημερώσεις δεν έχουν υπογραφεί

Η ενημέρωση της τοποθεσίας είναι εγγράψιμη

Ενημέρωση επιβεβαίωσης

Ενημέρωση ελέγχου ταυτότητας

Κακή ενημέρωση

Έλλειψη μηχανισμού ενημέρωσης

Δεν υπάρχει μηχανισμός μη αυτόματης ενημέρωσης

Εφαρμογή κινητού

Σιωπηρή αξιοπιστία από συσκευή ή Cloud
Καταμέτρηση ονόματος χρήστη
Κλείδωμα λογαριασμού
Γνωστά πιστοποιητικά προεπιλογής
Αδύναμοι κωδικοί πρόσβασης
Ασφαλής αποθήκευση δεδομένων
Κρυπτογράφηση μεταφοράς
Μη ασφαλής μηχανισμός ανάκτησης κωδικού πρόσβασης
Έλεγχος ταυτότητας δύο παραγόντων

API Backend προμηθευτή
Εγγενής εμπιστοσύνη του Cloud ή της εφαρμογής κινητής τηλεφωνίας
Αδύναμος έλεγχος ταυτότητας
Αδύναμοι έλεγχοι πρόσβασης
Επιθέσεις injection
Κρυφές υπηρεσίες
Επικοινωνία με το οικοσύστημα
Έλεγχοι υγείας
ΠΑΛΜΟΙ ΚΑΡΔΙΑΣ
Εντολές οικοσυστήματος
Αποσπάσματα
Πιέζοντας ενημερώσεις (pushing updates)

Δίκτυο
Traffic LAN
LAN στο Διαδίκτυο
Βραχεία εμβέλεια (Short range)
Μη τυποποιημένα
Ασύρματο (WiFi, Z-κύμα, Zigbee, Bluetooth)
Fuzzing Πρωτόκολλο

Έλεγχος Ταυτότητας / Εξουσιοδότηση
Τιμές που σχετίζονται με την πιστοποίηση / την εξουσιοδότηση (κλειδί συνδιάλεξης, διακριτικό, cookie, κλπ.)

Επαναχρησιμοποίηση κλειδιού περιόδου, διακριτικού, κλπ.
Έλεγχος ταυτότητας συσκευής προς συσκευή
Έλεγχος ταυτότητας συσκευής προς εφαρμογή κινητού
Έλεγχος ταυτότητας συσκευής προς σύστημα cloud
Έλεγχος ταυτότητας εφαρμογής κινητού προς σύστημα cloud
Έλεγχος ταυτότητας εφαρμογής Web προς σύστημα cloud
Έλλειψη δυναμικού ελέγχου ταυτότητας

Μυστικότητα
Αποκάλυψη δεδομένων χρήστη
Ανακάλυψη τοποθεσίας χρήστη / συσκευής
Διαφορετική ιδιωτικότητα

Υλικό Hardware (Αισθητήρες)
Αίσθηση χειρισμού περιβάλλοντος
Παραβίαση (Φυσική)
Βλάβη (Φυσική)

Οι επιφάνειες επίθεσης θα συνδυαστούν τώρα με τις πιο κοινές ευπάθειες που αντιμετωπίζει το Διαδίκτυο των πραγμάτων:

Ευπάθεια απαρίθμησης όνομα χρήστη. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διοικητική διεπαφή, η διεπαφή ιστού συσκευών, η διασύνδεση cloud και η εφαρμογή για κινητά. Με αυτήν την ευπάθεια δίνεται η δυνατότητα συλλογής ενός συνόλου έγκυρων ονομάτων χρηστών, αλληλεπιδρώντας με τον μηχανισμό ελέγχου ταυτότητας.

Ευπάθεια αδύναμου κωδικού πρόσβασης. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διοικητική διεπαφή, η διεπαφή ιστού συσκευών, η διασύνδεση cloud και η εφαρμογή για κινητά. Δίνεται η δυνατότητα να οριστούν κωδικοί πρόσβασης λογαριασμών, που μπορούν εύκολα να «σπάσουν» όπως για παράδειγμα οι '1234' ή '123456'.

Ευπάθεια κλειδώματος λογαριασμού. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διοικητική διεπαφή, η διεπαφή ιστού συσκευών, η διασύνδεση cloud και η εφαρμογή για κινητά. Με αυτό το θέμα ευπάθειας δίνεται η δυνατότητα να συνεχίσει να στέλνει προσπάθειες ελέγχου ταυτότητας μετά από 3-5 αποτυχημένες προσπάθειες σύνδεσης.

Ευπάθεια συσκευών χωρίς κρυπτογράφηση. Η επιφάνεια επίθεσης για αυτήν την ευπάθεια είναι οι υπηρεσίες δικτύων συσκευών. Οι υπηρεσίες δικτύου δεν είναι κατάλληλα κρυπτογραφημένες για την αποτροπή της παρακολούθησης από τους εισβολείς.

Ευπάθεια έλλειψης ελέγχου ταυτότητας δύο παραγόντων. Οι επιφάνειες επιθέσεων για αυτό το θέμα ευπάθειας είναι η διαχειριστική διεπαφή, το περιβάλλον web cloud και η εφαρμογή για κινητά. Η έλλειψη μηχανισμών επαλήθευσης δύο παραγόντων, όπως ένα διακριτικό ασφαλείας ή ένας σαρωτής δακτυλικών αποτυπωμάτων.
Ευπάθεια κακής εφαρμογής της κρυπτογράφησης. Στόχευση υπηρεσιών δικτύου συσκευών. Η κρυπτογράφηση που υλοποιείται εντούτοις δεν είναι σωστά ρυθμισμένη ή δεν ενημερώνεται σωστά, π.χ. SSL v2.

Ευπάθεια αποστολής ενημερώσεων χωρίς κρυπτογράφηση. Στοχεύει τον μηχανισμό ενημέρωσης και οι ενημερώσεις μεταδίδονται μέσω του δικτύου χωρίς τη χρήση του TLS ή την κρυπτογράφηση του ίδιου του αρχείου ενημέρωσης.

Εγγράψιμη ενημερωμένη τοποθεσία στοχεύει τον μηχανισμό ενημέρωσης. Η θέση αποθήκευσης για τα αρχεία ενημέρωσης είναι εγγράψιμη σε όλο τον κόσμο, επιτρέποντας έτσι την τροποποίηση και τη διανομή firmware σε όλους τους χρήστες.

Ευπάθεια άρνησης εξυπηρέτησης. Η επιφάνεια επίθεσης για αυτήν την ευπάθεια είναι η υπηρεσία δικτύου συσκευών. Η υπηρεσία μπορεί να δεχθεί επίθεση κατά τρόπο που να μην επιτρέπει την εξυπηρέτηση στην εν λόγω υπηρεσία ή σε ολόκληρη τη συσκευή.

Τρωτότητα αφαίρεσης μέσων αποθήκευσης. Στοχεύει στις φυσικές διεπαφές της συσκευής και δίνει τη δυνατότητα φυσικής απομάκρυνσης των μέσων αποθήκευσης από τη συσκευή.

No manual μηχανισμός ενημέρωσης. Στοχεύει τον μηχανισμό ενημέρωσης και δεν υπάρχει δυνατότητα χειροκίνητης επιβολής ελέγχου επιτήρησης για τη συσκευή.

Έλλειψη μηχανισμού ενημέρωσης. Στοχεύει τον μηχανισμό ενημέρωσης και δεν υπάρχει δυνατότητα ενημέρωσης της συσκευής.

Εμφάνιση έκδοσης Firmware ή / και η τελευταία ημερομηνία ενημέρωσης. Στοχεύει το Firmware της συσκευής και δεν εμφανίζεται η τρέχουσα έκδοση Firmware και / ή δεν εμφανίζεται η τελευταία ημερομηνία ενημέρωσης.

6. Επίλογος

Το Internet of Things αντιπροσωπεύει μία επαναστατική αλλαγή στον τρόπο που χρησιμοποιείται το πλήθος των συσκευών και συστημάτων εντός των κτιρίων μας, ενώ παρέχει τη δυνατότητα για μεγάλη αύξηση της παραγωγικότητας με παράλληλη βελτίωση της συνολικής εμπειρίας των χρηστών. Έτσι στο σημερινό κόσμο των δισεκατομμυρίων αισθητήρων και έξυπνων συσκευών που διασυνδέονται και μοιράζονται πληροφορίες, αναβαθμίζοντας τη συνολική εμπειρία των τελικών χρηστών, τα ζητήματα του ασφαλούς περιβάλλοντος λειτουργίας αναδεικνύονται σε μείζονος σημασίας παράμετρο.

Στα παραδοσιακά συστήματα ελέγχου πρόσβασης, όλα αρχίζουν και τελειώνουν με την εισαγωγή ενός PIN ή τη σάρωση μιας κάρτας. Η πόρτα ξεκλειδώνει και ο εξουσιοδοτημένος χρήστης αποκτά πρόσβαση στο χώρο. Όταν όμως το σύστημα εκμεταλλευτεί τις δυνατότητες που παρέχει η τεχνολογία του IoT, η πόρτα γίνεται το σημείο εκκίνησης για μια πλήρως προσαρμοσμένη εμπειρία σε ολόκληρη την εγκατάσταση.

Η ασφάλεια στο IoT απαιτεί την κατάρτιση και την υιοθέτηση ενός ολοκληρωμένου σχεδίου απόκρισης σε περίπτωση παραβίασης, που θα αναπτύσσει μια προληπτική στρατηγική και θα βασίζεται στην αποδοχή πως τίποτα δεν είναι 100%

ασφαλές. Θεμελιώδες στο σχεδιασμό είναι το πόσο γρήγορα και αποτελεσματικά μπορούμε να αντιδράσουμε στην εκάστοτε απειλή.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΝΑΦΟΡΕΣ

Al-Sakib Khan Pathan, Hyung-Woo Lee και Choong Seon Hong, *Security in Wireless Sensor Networks: Issues and Challenges* (ISBN 89-5519-129-4, 2006)

Bisdikian, Ch., *An Overview of the Bluetooth Wireless Technology*. (IBM Research Division, 2001)

Boeckl K., et al, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, (National Institute of Standards and Technology, US June 2019) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

Broadband Internet Technical Advisory Group – BITAG, *Internet of Things security and privacy recommendations.* (working Group Report, Nov 2016)

Bude C., and Kervefors A., *Internet of Things Exploring and Securing a Future Concept*, Bachelor's Thesis, (KTH Royal Institute of Technology, Information and Communication Technology, Stockholm, 2015)

Carlton Shepherd, et al. *Secure and Trusted Execution: Past, Present and Future A Critical Review in the Context of the Internet of Things and Cyber -Physical Systems,* Royal Holloway, University of London, 2014)

Dixon, R.C., *Spread Spectrum Systems*, Second Edition, (John Wiley and Sons, Inc., New York 1984).

EY (Global Organization), *Cybersecurity and the Internet of Things*, (UK, March, 2015)

Farahani Shahin, *ZigBee Wireless Networks and Transceivers*. (Elsevier 2008).

Finneran, M., *Voice Over WLANs the complete guide*. (Newnes 2008).

Groopman Jessica and Owyang Jeremiah, The internet of trusted things, Blockchain as the foundation for autonomous products & ecosystem services (KALEIDO Insights, January, 2018)

Hahm, Oliver, et al. *Operating Systems for Low End Devices in the Internet of Things: a Survey."* (2015).

Holdowsky J., Mahto M., Raynor M., Cotteleer M., *Inside the Internet of Things IoT,* (Deloitte University Press, 2015)

Karagiannis, V., et al. *A survey on application layer protocols for the internet of things*. Transaction on IoT and Cloud Computing 3.1 (2015): 1117.

Kardach, J., *Bluetooth Architecture Overview*. (Intel Corporation 1998).

King J., *A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet*, Master's Thesis, (Luleå University of Technology Department of Computer Science, 2015)

Κουρουτζίδης, Θ. Ν., *Σχεδίαση Εφαρμογών για το Διαδίκτυο των Αντικειμένων με το Contiki OS* (Θεσσαλονίκη: ΑΠΘ, Διπλωματική Εργασία, 2016

Kovatsch F., M., *Scalable Web Technology for the Internet of Things,* A thesis submitted to attain the degree of Dr. sc. ETH Zurich, (Diss. ETH No. 22398, 2015)

Μάγκος Ε. *Ασφάλεια Η/Υ και Προστασία Δεδομένων*, Σημειώσεις, (Κέρκυρα. Ιόνιο Πανεπιστήμιο, 2007)

Malekzadeh, M., Ebady, S., Abadi, S., *Damage Measurement of Collision Attacks On Rerformance of Wireless Sensor Networks*, Information Engineering and Electronic Business, 2014, 6, 22-32 Published Online December 2014 in MECS http://www.mecs-press.org/

Mendez, D., Papapanagiotou, I., Yang, B., *Internet of Things: Survey on Security and Privacy,* (Purdue University, 2018)

Meola A., *How the Internet of Things will affect security & privacy*

(article Dec 2016) https://www.businessinsider.com/iot

Mclaurin Ken, *When one cyberattack becomes a thousand: Protecting the IoT* , (article Feb 2015) https://www.embedded-computing.com/

Mirza Abdur Razzaq, et al, *Security Issues in the Internet of Things (IoT): A Comprehensive Study,* (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

OWASP, *The ten most critical web application security risks*, Release 2013

Palattella, M. R., et al, *IoT - IPv6 integration handbook for SMEs,* (European Project STREP of the 7th Framework Program Grant 288445, 2014).

Παπάζογλου, Χ., Σκλήρης, Κ., Χαρίση, Γ., Παρουσίαση Αισθητήρων και Δικτύων για έξυπνα Σπίτια (Θεσσαλονίκη, Πανεπιστήμιο Μακεδονίας, 2016)

Piyare, Rajeev, and Seong Ro Lee. *Towards internet of things (iots): Integration of wireless sensor network to cloud services for data collection and sharing*. arXiv preprint arXiv:1310.2095 (2013).

Ρούσης, Δ., *Πύλη Διαδικτύου Αντικειμένων. Σχεδιασμός και Υλοποίηση,* (Θεσσαλονίκη: ΑΠΘ, Διπλωματική Εργασία, 2017)

Saravana K.M, Dr. A. Kovalan, G.N.Basavaraj, Rajkumar *Network Security Vulnerability and Attacks on Wireless Sensor Networks: Survey* International Journal of Scientific & Engineering Research, Volume 3,Issue 9,September- 2012 ISSN 2229-5518

Schor, Lars, Philipp Sommer, and Roger Wattenhofer, *Towards a zero configuration wireless sensor network architecture for smart buildings*. Proceedings of the First ACM Workshop on Embedded Sensing Systems for Energy Efficiency in Buildings . ACM, 2009.

Sitenkov D., *Access Control in the Internet of Things*, Master Thesis, Swedish ICT 2015)

Sklavos N., Zaharakis I. D., Kameas A., Kalapodi A., *Security & Trusted Devices in the Context of Internet of Things (IoT)*, School of Science and Technology, Hellenic Open University, Patras, 2017)

Stanislav Beran, Edoardo Pignotti, and Peter Edwards, Trusted Tiny Things: Making Devices in Smart Cities More Transparent, (University of Aberdeen, 2014)

Sutterlin, P., and Downey, W., *A Power Line Communication Tutorial Challenges and Technologies* (Echelon Corporation USA)

Tanenbaum, A., Wetherall, D., *Δίκτυα υπολογιστών*, (Αθήνα: Εκδόσεις Κλειδάριθμος. 2012).

Taylor P et al, *Internet of Things, realizing the potential of a trusted smart World*, Royal Academy of Engineering, London, March 2018, ISBN: 978-1-909327-37-5

Tomar, A., *Introduction to Zigbee technology*. (Global Technology Centre Volume 12011).

Τσαρμπόπουλος, Ν., *Η μετάβαση του Διαδικτύου από το IPv4 στο IPv6*, (άρθρο στο Ενημερωτικό Δελτίο της ΕΕΤΤ, Τεύχος 17 Ιούνιος 2008)

U.S. Department of Homeland Security, *Strategic Principles For Securing The Internet of Thingw (IoT)*, (Nov, 2016)

Vasseur J. and Dunkels A.. *Interconnecting Smart Objects with IP: The Next Internet*. (Morgan Kaufmann, 2010).

Veracode White Paper, *The Internet of Things: Security Research Study*, (US, 2014) https://www.veracode.com/

Περιοδικό IT Professional Security, *Cloud Computing και ασφάλεια*, (Τεύχος 14, 2010)

Περιοδικό IT Professional Security, *USB Drives: οΔούρειος Ίππος για τα IT συστήματα*, (Τεύχος 14, 2010)

Piconets (2014), ιστότοπος http://www.cyprus-technology.net/2014/08/piconets.html

IEEE 802.11, (2016) ιστότοπος https://el.wikipedia.org/wiki/IEEE_802.11

Wind River, *Security in the Internet of Things Lessons from the past for the Connected* future (White Paper, 2015)

Yosra Ben Saied, *Collaborative Security for the Internet of Things*, Doctorate Thesis, (Telecom Sudparis et L'Universite Pierre et Marie Curie. Paris, 2013)

ZigBee Protocol (2016) ιστότοπος http://www.ARM.com