ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΠΟΤΙΜΗΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Διπλωματική Εργασία

του

Λαζαρίδη Γεώργιου

Θεσσαλονίκη, Μαΐος 2019

ΑΠΟΤΙΜΗΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Λαζαρίδης Γεώργιος

Πτυχίο Ηλεκτρονικού Μηχανικού Τ.Ε, ΑΤΕΙΘ, 2014

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/06/2019

Ιωάννης Μαυρίδης	Παναγιώτης Φουληράς	Χρήστος Γεωργιάδης
.....	.....	.....

Λαζαρίδης Γεώργιος

.....

Περίληψη

Η παρούσα εργασία εστιάζει στην αποτίμηση της ασφάλειας και της ιδιωτικότητας στο Διαδίκτυο των Πραγμάτων (Internet of Things – IoT). Αρχικά, παρουσιάζει τη νομοθεσία γύρω από τα προσωπικά δεδομένα και τις επικοινωνίες, τόσο σε ευρωπαϊκό επίπεδο όσο και σε εθνικό. Μελετά το state-of-the-art στον τομέα της ασφάλειας του IoT και αναλύει πιθανούς κινδύνους και ευπάθειες που μπορούν να επηρεάσουν την εύρυθμη λειτουργία συσκευών που χρησιμοποιούν τη τεχνολογία αυτή, καθώς επίσης και να παραβιάσουν την ιδιωτικότητα των χρηστών. Παρουσιάζονται τρόποι αντιμετώπισης των ευπαθειών του IoT και αναλύονται δυο «ειδικές» μηχανές αναζήτησης οι οποίες είναι σε θέση να σαρώνουν τον παγκόσμιο ιστό και να εντοπίζουν συσκευές οι οποίες είναι συνδεδεμένες σε αυτό. Αναλύοντας τα στοιχεία των συσκευών αυτών, «banners», τα οποία δίνουν οι μηχανές αναζήτησης, οι ερευνητές ασφάλειας μπορούν να εντοπίζουν ευπάθειες στις IoT συσκευές. Τέλος, γίνεται μια σύνοψη όσων εξετάστηκαν στην εργασία αυτή και ακολουθούν κάποια συμπεράσματα. Η διπλωματική εργασία κλείνει με μελλοντικές επεκτάσεις που μπορούν να βελτιώσουν την ασφάλεια και την ιδιωτικότητα των IoT οικοσυστημάτων.

Λέξεις Κλειδιά: Διαδίκτυο των Πραγμάτων (IoT), ασφάλεια, ιδιωτικότητα, νομοθεσία, ευπάθειες, επιθέσεις, μηχανή αναζήτησης, Ιστός των Πραγμάτων (WoT), Shodan, Censys

Abstract

This thesis focuses on the evaluation of the security and privacy for the Internet of Things (IoT). Initially, it presents the legislation on personal data and communications, both at European and national level. It studies state-of-the-art reports in the field of IoT security and analyzes potential threats and vulnerabilities, which can affect the proper functionality of the devices that use this technology and violate the privacy of users. Moreover, ways to address the vulnerabilities of IoT are given as well as the analyzation of two "special" search engines is made, that can access smart devices and devices that are part of the Internet of Things and identify vulnerabilities using the banners obtained. Finally, a summary is made of all of those examined in this research and some conclusions follow. The thesis ends with future extensions that can improve the security and privacy of IoT ecosystems.

Keywords: Internet of Things (IoT), security, privacy, legislation, vulnerabilities, attacks, search engine, Web of Things (WoT), Shodan, Censys

Πρόλογος – Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Ιωάννη Μαυρίδη για την ευκαιρία που μου έδωσε μέσω αυτής της διπλωματικής εργασίας να ασχοληθώ ενεργά με τον τομέα της ασφάλειας σε IoT συστήματα.

Ένα μεγάλο ευχαριστώ στην οικογένεια μου τόσο για την οικονομική όσο και για την ηθική υποστήριξη που μου προσέφεραν όλοι, καθ' όλη τη διάρκεια του Μεταπτυχιακού κύκλου σπουδών μου.

Τέλος, θέλω να ευχαριστήσω τη γυναίκα μου, για την ηθική της υποστήριξη.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Λίστα ακρωνύμιων

IoT	Internet of Things
RFID	Radio Frequency Identification
DR	Demand Response
ΑΠΕ	Ανανεώσιμες Πηγές Ενέργειας
ARPA	Advanced Research Project Agency
TCP	Transmission Control Protocol
ISDN	Integrated Services Digital Network
MDMS	Meter Data Management System
RTU	Remote Terminal Unit
DDoS	Distributed Denial of Service
CPS	Cyber Physical Security
PKI	Public Key Infrastructure
DSS	Decision Support System
HTTP	Hypertext Transfer Protocol
ENISA	European Union Agency for Network and Information Security
CFAA	Computer Fraud and Abuse Act
SQL	Structured Query Language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
SSH	Secure Shell
DVR	Digital Video Recorder
CCTV	Closed Circuit Television
WoT	Web of Things
HTML	Hyper Text Markup Language
API	Application Programming Interface
RAM	Random Access Memory
OS	Operating System
IPv4	Internet Protocol version 4
SDO	Standards Developing Organizations

1 Εισαγωγή

1.1 Γενικό υπόβαθρο

Το 1999, ένας ειδικός στα συστήματα Radio Frequency Identification (RFID), ο Kevin Ashton, χρησιμοποίησε για πρώτη φορά τον όρο «Internet of Things» ή «Διαδίκτυο των Πραγμάτων», παρόλο που στο MIT Auto-ID, η ιδέα του καινούριου αυτού όρου είχε ήδη εμφανιστεί στους κόλπους των επιστημόνων τουλάχιστον μια δεκαετία νωρίτερα [Sundmaeker, 2010]. Ο όρος όμως Internet of Things (εφεξής IoT), μπορεί να έχει διαφορετική ανάλυση, μιας και ο κάθε επιστήμονας τον αντιλαμβάνεται από διαφορετική οπτική γωνία.

Οι κοινωνίες του 21ου αιώνα έχουν χαρακτηριστεί μεταβιομηχανικές ή «κοινωνίες της γνώσης και της πληροφορίας». Η γνώση και η πληροφορία καθίστανται βασικές παραγωγικές δυνάμεις προσδίδοντας νέο περιεχόμενο στις παραγωγικές και στις κοινωνικές σχέσεις. Συνιστούν μια νέα μορφή κεφαλαίου, το κοινωνικό, που τείνει να αντικαταστήσει την κυριαρχία του βιομηχανικού κεφαλαίου με τη δημιουργία νέων κοινωνικών ελίτ, των πανεπιστημίων, των κυβερνητικών θεσμών, αυτών που βασίζονται στην ανάπτυξη της γνώσης και της πληροφορίας. Οι βασικές κοινωνικές διακρίσεις και η δημιουργία πλούτου δεν θα βασίζονται πλέον στην ιδιοκτησία βιομηχανικού κεφαλαίου αλλά στην δυνατότητα πρόσβασης και αξιοποίησης της γνώσης και της πληροφορίας. Οι εξελίξεις αυτές οφείλονται στην πρόοδο της πληροφορικής και των επικοινωνιών που οδήγησαν στην εκμηχάνιση των υπηρεσιών και στην σχετική αυτονόμησή τους από την βιομηχανική παραγωγή.

Η αξία της πληροφορίας είναι πολύ σημαντική, όταν αυτή συνδέεται με έναν χρήστη του διαδικτύου και την ταυτότητα αυτού ή πολύτιμές προσωπικές του πληροφορίες. Οι πληροφορίες αυτές σε ορισμένες περιπτώσεις μπορούν να χρησιμοποιηθούν κακόβουλα εναντίον του, όταν λαμβάνονται και επεξεργάζονται χωρίς τη συγκατάθεσή του. Στις μέρες μας, όπου όλες οι πληροφορίες είναι διάχυτες, οι επιχειρήσεις έχουν αναπτύξει μεθόδους καταγραφής και παρακολούθησης του χρήστη, όσον αφορά την περιήγηση του στο διαδίκτυο ή τις προτιμήσεις του σε προϊόντα που αγοράζει. Έτσι λοιπόν, τα θέματα ασφαλείας που εγείρονται από την ετερογένεια της τεχνολογίας αυτής (IoT) είναι πολύ σημαντικά και αποτελούν ένα ευρύ πεδίο για έρευνα.

1.2 Σκοπός της εργασίας

Όλο και περισσότερες συσκευές συνδέονται με το διαδίκτυο - από καταναλωτικά προϊόντα όπως είναι οι κάμερες και οι βηματοδότες μέχρι και βιομηχανικός εξοπλισμός όπως οι ανεμογεννήτριες και οι σταθμοί παραγωγής ηλεκτρικής ενέργειας - τα όρια του οποίου μετατοπίζονται πέρα από τις συσκευές που αποτελούνται απλά από μια οθόνη για την προβολή δεδομένων, σε ένα πολύ ευρύτερο φάσμα του κόσμου γύρω μας. Καθώς η τεχνολογία της πληροφορικής αναπτύσσεται ραγδαία και όλο και περισσότερες συσκευές είναι σε θέση να συνδέονται σε ένα δίκτυο (Internet, Bluetooth, LoRaWAN), όπως οι ηλεκτρονικοί υπολογιστές, τα κινητά τηλέφωνα, οι έξυπνες οικιακές συσκευές ή οι έξυπνοι μετρητές και αισθητήρες, ο αριθμός των συσκευών IoT αυξάνεται καταιγιστικά.

Το IoT είναι μια πολλά υποσχόμενη τεχνολογία που αναμένεται να έχει οικονομικό αποτέλεσμα 1,9 τρισεκατομμυρίων δολαρίων αλλά και δημιουργεί μια νέα αγορά της τάξης των 300 δισεκατομμυρίων δολαρίων. Η ανάπτυξη της τεχνολογίας του IoT συμβάλλει στη βελτίωση της ζωής του ανθρώπου και αυξάνει την ανταγωνιστικότητα, αλλά ταυτόχρονα μπορεί να εκθέσει τους χρήστες σε κινδύνους που εγείρουν θέματα ασφάλειας και ιδιωτικότητας των πληροφοριών που διαχέουν στο διαδίκτυο. Η τεχνολογία του IoT μπορεί να απειλήσει την ιδιωτική ζωή αλλά και τα δημόσια και ιδιωτικά συμφέροντα, με αποτέλεσμα η δημιουργία αντιμέτρων σε αυτές τις απειλές, να αποτελεί κρίσιμο ζήτημα.

Όποια και να είναι η πορεία εξέλιξης του διαδικτύου, οι κίνδυνοι ασφαλείας φαίνεται να ακολουθούν. Καθώς το IoT επεκτείνεται, οι κίνδυνοι αυτοί παίρνουν νέες διαστάσεις πολύ πέρα από τις γνωστές απειλές για κλεμμένους κωδικούς πρόσβασης εφαρμογών ή πιστωτικών καρτών.

Τα τελευταία χρόνια, παρατηρείται μια εγρήγορση στον τομέα της έρευνας για την ασφάλεια των IoT συσκευών. Η παρούσα διπλωματική θα κάνει μια εκτενή μελέτη και παρουσίαση δύο εργαλείων – μηχανών αναζήτησης, τα οποία είναι σε θέση να διαβάζουν τα «banners» οποιασδήποτε IoT συσκευής είναι συνδεδεμένη στο διαδίκτυο. Με τη βοήθεια αυτής της πληροφορίας που συλλέγει η μηχανή αναζήτησης, ο ερευνητής με τη σειρά του μπορεί να εντοπίσει κενά ασφαλείας και ευπάθειες σε οποιαδήποτε συσκευή αποτελεί κομμάτι του δικτύου IoT. Θα μελετηθεί επαρκής αριθμός ερευνητικών αναφορών και θα σχολιαστεί το αποτέλεσμα. Επιπρόσθετα, θα

παρουσιαστούν οι κύριες ευπάθειες ασφάλειας και ιδιωτικότητας των IoT συσκευών αλλά και γενικότερα των IoT οικοσυστημάτων καθώς και τρόποι αντιμετώπισης τους.

1.3 Δομή της εργασίας

Η παρούσα εργασία χωρίζεται σε οχτώ κεφάλαια. Στο πρώτο κεφάλαιο δίνεται ένα γενικό υπόβαθρο σχετικά με το IoT, παρουσιάζεται ο σκοπός συγγραφής της εργασίας, δίνεται η δομή της και η θεωρητική θεμελίωση των όρων «ασφάλεια» - «ιδιωτικότητα». Στο δεύτερο κεφάλαιο γίνεται μια ιστορική αναδρομή στο IoT και στο πως ξεκίνησε. Δίνεται ο ορισμός του και μια περίπτωση εφαρμογής της τεχνολογίας αυτής στα έξυπνα δίκτυα ηλεκτρικής ενέργειας. Στο τρίτο κεφάλαιο παρουσιάζεται η ευρωπαϊκή αλλά κι η εθνική νομοθεσία που διέπει την προστασία των προσωπικών δεδομένων και τις επικοινωνίες γενικά, αλλά και ειδικά στο περιβάλλον του IoT. Στο τέταρτο κεφάλαιο, παρουσιάζονται τα ζητήματα ασφάλειας και ιδιωτικότητας, επιθέσεις και τρόποι προστασίας των δεδομένων στους έξυπνους μετρητές ηλεκτρικής ενέργειας. Επιπρόσθετα, στο κεφάλαιο αυτό γίνεται μια αναλυτική παρουσίαση των τύπων επιθέσεων αλλά και των μηχανισμών προστασίας σε IoT περιβάλλοντα. Στο πέμπτο κεφάλαιο γίνεται εκτενής αναφορά στην εύρεση ευπαθειών αξιοποιώντας τις πληροφορίες που συνέλλεξαν οι μηχανές αναζήτησης στα πλαίσια της τεχνολογίας IoT και σε ορισμένα πραγματικά περιστατικά. Στο έκτο κεφάλαιο μελετάται ο τρόπος λειτουργίας της μηχανής αναζήτησης Shodan ενώ στο έβδομο κεφάλαιο η μηχανή αναζήτησης Censys. Τέλος στο όγδοο κεφάλαιο παρουσιάζεται μια γενική σύνοψη όλης της παρούσας διπλωματικής εργασίας μαζί με τα όποια συμπεράσματα προέκυψαν από τη βιβλιογραφική έρευνα που έγινε και παρουσιάζονται σε θεωρητικό επίπεδο ορισμένες μελλοντικές επεκτάσεις.

1.4 Ορισμός ιδιωτικότητας και ασφάλειας

Η επεξήγηση του όρου «ιδιωτικότητα» δεν είναι μια απλή υπόθεση, μιας και κινείται περισσότερο σε φιλοσοφικό επίπεδο, παρά σε τεχνολογικό. Στον πιο απλό της ορισμό, η ιδιωτικότητα μπορεί να οριστεί ως η κατάσταση αποφυγής ανεπιθύμητων χρηστών ή εισβολέων στα προσωπικά δεδομένα. Όταν ένας χρήστης διατηρεί την ιδιωτικότητα του, είναι απόλυτα σίγουρος πως κανένας άλλος χρήστης δεν έχει πρόσβαση στα προσωπικά του δεδομένα, γενικότερα δεν τον παρακολουθεί ή δεν τον ενοχλεί, με άλλα λόγια τα προσωπικά δεδομένα του παραμένουν αόρατα για όλους τους

υπόλοιπους χρήστες ανά τον κόσμο και επιτρέπεται η πρόσβαση σε αυτά, μόνο με την παραχώρηση της άδειας του εκάστοτε χρήστη.

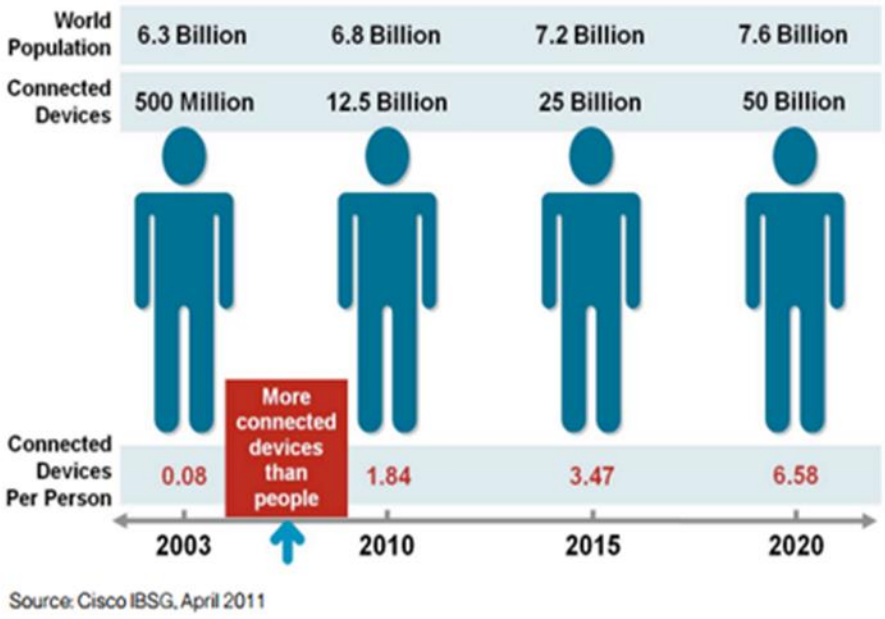
Από την άλλη πλευρά, ο όρος «ασφάλεια», μπορεί να αποδοθεί με μεγαλύτερη σαφήνεια. Η ασφάλεια ορίζεται ως η κατάσταση αποφυγής απειλών ή κινδύνων. Οποιοδήποτε μέτρο σχετίζεται με την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας αποτελεί κομμάτι της ασφάλειας. Ένα απλό και κατανοητό παράδειγμα της ιδιωτικότητας και της ασφάλειας είναι η κατοικία ενός ανθρώπου. Μέσα σε αυτό, κάποιος διαμένει, κοιμάται ή κάνει τις προσωπικές του δραστηριότητες. Οι πόρτες, τα παράθυρα και οι τοίχοι του οικήματος προστατεύουν την ιδιωτικότητα του εκάστοτε ανθρώπου που ζει σε αυτό και κανείς από έξω δεν γνωρίζει τις ενέργειες που συμβαίνουν εσωτερικά. Οι κλειδαριές στις πόρτες και τα παράθυρα, καθώς και ένας αυλόγυρος περιμετρικά του σπιτιού προσφέρουν ασφάλεια στον ένοικο, αποτρέποντας εισβολείς να μπούνε στο εσωτερικό του. Το παράδειγμα αυτό, αποτελεί μια μικρογραφία της κατάστασης που επικρατεί στον τομέα της τεχνολογίας σχετικά με την ασφάλεια και την ιδιωτικότητα των προσωπικών δεδομένων που ανταλλάσσουν οι IoT συσκευές μεταξύ τους.

2 Το Διαδίκτυο των Πραγμάτων

2.1 Πως ξεκίνησε

Τον Ιανουάριο του 2009, μια ομάδα ερευνητών στην Κίνα μελέτησε ορισμένα δεδομένα δρομολόγησης στο διαδίκτυο, κατηγοριοποιημένα ανά εξάμηνο, από το Δεκέμβριο του 2001 έως το Δεκέμβριο του 2006. Αξιοποιώντας και τις ιδιότητες του νόμου του Moore, τα ευρήματά τους έδειξαν ότι το διαδίκτυο διπλασιάζεται σε μέγεθος κάθε 5,3 χρόνια. Λαμβάνοντας υπόψη τον αριθμό αυτό σε συνδυασμό με τον αριθμό των συσκευών που συνδέονται με το διαδίκτυο το 2003 (500 εκατομμύρια, όπως καθορίστηκε από τη Forrester Research) και τον παγκόσμιο πληθυσμό, σύμφωνα με το Γραφείο Απογραφής των Η.Π.Α., η Cisco IBSG υπολόγισε τον αριθμό συνδεδεμένων συσκευών ανά άτομο [Evans, 2011].

Επεξεργάζοντας περαιτέρω αυτούς τους αριθμούς, η Cisco IBSG εκτιμά ότι το IoT «γεννήθηκε» επίσημα πλέον, κάποια στιγμή μεταξύ του 2008 και του 2009 (Εικόνα 1). Σήμερα, το IoT συνεχίζει να εξελίσσεται με ραγδαίους ρυθμούς [Evans, 2011].



Εικόνα 1 - Η εξέλιξη του IoT στο χρόνο

Υπάρχει μια πληθώρα συνεδρίων, εκθέσεων, καθώς και άρθρων σχετικά με τον μελλοντικό αντίκτυπο της «επανάστασης της τεχνολογίας των πληροφοριών» και σχετικά με τις νέες ευκαιρίες στην αγορά, με επιχειρηματικά μοντέλα αλλά και προβληματισμούς και προκλήσεις σχετικά με την ασφάλεια, την ιδιωτική ζωή και την λειτουργία των έξυπνων συσκευών. Η εκτεταμένη εφαρμογή των συσκευών IoT υπόσχεται να μεταμορφώσει πολλές πτυχές του τρόπου με τον οποίο ζούμε. Για τους καταναλωτές, τα νέα προϊόντα IoT όπως οι οικιακές συσκευές που έχουν την δυνατότητα να συνδεθούν στο διαδίκτυο ή οι συσκευές διαχείρισης ενέργειας οδηγούν στα λεγόμενα «έξυπνα σπίτια», που προσφέρουν μεγαλύτερη ασφάλεια αλλά και χαμηλή κατανάλωση πόρων [Ashton, 2009].

Άλλες προσωπικές συσκευές IoT είναι οι φορητές συσκευές παρακολούθησης της υγείας (ηλεκτρονικό πιεσόμετρο, θερμόμετρο, καρδιογράφος) και οι δικτυωμένες ιατρικές συσκευές έχουν αλλάξει ριζικά τον τρόπο παροχής των υπηρεσιών υγειονομικής περίθαλψης. Αυτή η τεχνολογία υπόσχεται να είναι επωφελής για τα άτομα με αναπηρίες, τους ηλικιωμένους και γενικότερα για τις ευπαθείς ομάδες, επιτρέποντας τη βελτίωση των επιπέδων της ανεξαρτησίας και της ποιότητας της ζωής με ένα προσιτό κόστος [Ashton, 2009].

Τα δικτυωμένα οχήματα, τα ευφυή συστήματα κίνησης και οι αισθητήρες ενσωματωμένοι σε δρόμους και γέφυρες αποτελούν κι αυτά παραδείγματα IoT συσκευών. Η ιδέα των «έξυπνων πόλεων», συμβάλλει στην ελαχιστοποίηση της συμφόρησης και της κατανάλωσης ενέργειας. Η τεχνολογία του IoT προσφέρει την ευκαιρία να μετασχηματιστεί και να εξελιχθεί η γεωργία, η βιομηχανία, η παραγωγή και η διανομή ενέργειας με την αύξηση της διαθεσιμότητας πληροφοριών μέσω της χρήσης ειδικών αισθητήρων [Evans, 2011][Ashton, 2009].

Όσον αφορά τις μελλοντικές εξελίξεις, η Cisco IBSG προβλέπει ότι θα υπάρχουν 50 δισεκατομμύρια συσκευές συνδεδεμένες με το διαδίκτυο μέχρι το 2020. Είναι σημαντικό να σημειωθεί ότι αυτές οι εκτιμήσεις δεν λαμβάνουν υπόψη την ταχεία πρόοδο στον τομέα του διαδικτύου ή την πρόοδο της τεχνολογίας των συσκευών αλλά παρουσιάζονται με βάση τα δεδομένα που είναι γνωστά ως σήμερα [Jakobs, 2011].

Ωστόσο, το IoT εγείρει πολλά ζητήματα και προκλήσεις στον τομέα της ασφάλειας και της ιδιωτικότητας, που πρέπει να εξεταστούν και να αντιμετωπιστούν προκειμένου να γίνεται η ανταλλαγή πληροφοριών με ασφάλεια. Ένας μεγάλος αριθμός επιχειρήσεων και ερευνητικών οργανισμών έχουν προσφέρει ένα ευρύ φάσμα

προβλέψεων για τις πιθανές επιπτώσεις του IoT στην οικονομία κατά τα επόμενα πέντε έως δέκα χρόνια [Evans, 2011].

2.2 Ορισμός

Ο όρος IoT χρησιμοποιήθηκε για πρώτη φορά στα τέλη της δεκαετίας του 1990 από τον Kevin Ashton. Ο Ashton, ο οποίος είναι ένας από τους ιδρυτές του Auto-ID Center στο MIT, δημιούργησε τον όρο αυτό για να ταυτοποιήσει μέσω ραδιοσυχνοτήτων (RFID), προϊόντα εταιρικών αλυσίδων εφοδιασμού με το διαδίκτυο. Με αυτό τον τρόπο μπορούν να παρακολουθήσουν (εντοπισμός, μέτρηση και καταγραφή) τα προϊόντα χωρίς την ανάγκη της ανθρώπινης παρέμβασης. Ως αποτέλεσμα αυτής της τεχνικής, εδραιώνεται πλέον ο όρος IoT [Madakam, 2015].

Το βασικό όραμα του IoT είναι η δημιουργία και η σύνδεση δισεκατομμυρίων αισθητήρων με σκοπό τη δημιουργία έξυπνων συσκευών, οι οποίες θα έχουν την δυνατότητα να συνδεθούν και να μοιράζονται πληροφορίες μεταξύ τους, με σκοπό να ενισχύσουν τις λειτουργικές ανάγκες του τελικού χρήστη. Αυτό γίνεται με τη συλλογή, την επεξεργασία και την ανάλυση των δεδομένων που παρέχονται, επιτρέποντας ενέργειες σε πραγματικό χρόνο, για λογαριασμό του χρήστη και των συνδεδεμένων συσκευών [Madakam, 2015].

Το IoT εξελίχθηκε παράλληλα με το διαδίκτυο. Αρχικά στα πρώτα στάδια της εξέλιξης της τεχνολογίας, υπήρχε η δυνατότητα ελέγχου μιας έξυπνης συσκευής από τον άνθρωπο μέσω ενός υπολογιστή και μετά μέσω μιας κινητής συσκευής (smartphone ή tablet). Στην τελευταία εξέλιξη του IoT, οι έξυπνες συσκευές επικοινωνούν και παρέχουν πληροφορίες στο διαδίκτυο, χωρίς την ανθρώπινη παρέμβαση, σε μια κλίμακα που δεν έχει υπάρξει ποτέ πριν καταγεγραμμένο [Uckelmann, 2011].

Η τεχνολογία συνεχίζει να προχωρά με απίστευτους ρυθμούς και η διαδικασία της ενσωμάτωσης μπορεί να μην είναι εύκολη, αλλά είναι αναμφισβήτητα απαραίτητη. Η σύγκλιση του διαδικτύου και του τομέα της ασφάλειας έχει ήδη συμβεί σε τεχνικό επίπεδο. Αν τελικά θα είναι επιτυχής, τα οφέλη θα είναι σημαντικά.

2.3 Έξυπνα δίκτυα

Περιγραφή έξυπνου δικτύου

Το έξυπνο δίκτυο ηλεκτρικής ενέργειας (Smart Grid) στην ουσία είναι η εξέλιξη του υπάρχοντος ηλεκτρικού δικτύου, όπου ενσωματώνονται καινοτόμες τεχνολογίες

επικοινωνιών και πληροφοριών, κάνοντας χρήση «έξυπνων συσκευών» που λειτουργούν και επικοινωνούν με αυτόματο τρόπο. Ο σκοπός της κατασκευής των έξυπνων δικτύων είναι η δημιουργία ενός ολοκληρωμένου συστήματος για την καλύτερη διαχείριση των ενεργειακών πόρων και την παρακολούθηση της ενέργειας. Για να επιτευχθεί η δημιουργία ενός έξυπνου δικτύου χρησιμοποιούνται καινοτόμες υποδομές δικτύων και ειδικές συσκευές ελέγχου και μέτρησης, όπως οι έξυπνοι μετρητές. Όλες οι συσκευές συνδέονται με ένα κεντρικό σύστημα, το οποίο σε πραγματικό χρόνο, λαμβάνει και διαχειρίζεται όλες τι πληροφορίες από τους αισθητήρες και τους έξυπνους μετρητές. Με τη χρήση έξυπνων συσκευών οι καταναλωτές έχουν τη δυνατότητα να ελέγχουν το φορτίο τους και να εξοικονομούν ενέργεια [Song Tan, 2017].

Ένα έξυπνο δίκτυο μπορεί να παρομοιαστεί με έναν υπολογιστή. Οι αισθητήρες τοποθετούνται σε διάφορες θέσεις στο δίκτυο και συλλέγουν πληροφορίες σχετικά με τις συνθήκες λειτουργίας του, συμπεριλαμβανομένου της ποιότητας των χαρακτηριστικών της προσφερόμενης ηλεκτρικής ενέργειας αλλά και άλλων χαρακτηριστικών, μεταδίδοντας αυτές τις πληροφορίες (σε μερικές περιπτώσεις συνεχώς ή και στιγμιαία) σε υπολογιστικά συστήματα της εκάστοτε εταιρείας ηλεκτρικής ενέργειας. Τα συστήματα αυτά μπορούν να πραγματοποιούν αλλαγές με αυτόματο τρόπο, στις ρυθμίσεις του εξοπλισμού του δικτύου χωρίς να είναι απαραίτητη η ανθρώπινη παρέμβαση. Σε πολλές περιπτώσεις, αυτές οι αλλαγές γίνονται ώστε να αντιμετωπίσουν προληπτικά ζητήματα, προτού αυτά προκαλέσουν σοβαρά προβλήματα στους πελάτες. Οι πληροφορίες μπορούν να αποθηκευτούν για μελλοντική χρήση ή ανάλυση και λήψη αποφάσεων από τους χρήστες [Song Tan, 2017].

Οι δυνατότητες που παρέχει η επικοινωνία των έξυπνων δικτύων επιτρέπει την άμεση ενημέρωση με θέματα που σχετίζονται με τη ζήτηση, την τιμολόγηση ή τη διακοπή των φορτίων (πολιτικές Demand Response - DR). Αφορούν προγράμματα διαχείρισης της ζήτησης με σκοπό την εξομάλυνση των αιχμών της καμπύλης φορτίου της ηλεκτρικής ενέργειας, παρέχοντας στους καταναλωτές αντίστοιχα οικονομικά κίνητρα για μείωση της κατανάλωσης τους σε ώρες που παρατηρούνται οι μέγιστες ημερήσιες αιχμές ζήτησης. Λόγω του ότι η ζήτηση μεταβάλλεται, υπάρχουν κατάλληλα εφεδρικά συστήματα σε περίπτωση που η ζήτηση αυξηθεί. Ένα σημαντικό πλεονέκτημα του έξυπνου δικτύου είναι η προσφορά αλληλεπίδρασης μεταξύ φορτίου και παραγωγής σε πραγματικό χρόνο. Συνεπώς, τα σφάλματα ανιχνεύονται πολύ πιο εύκολα και εντοπίζονται γρήγορα οι εναλλακτικές διαδρομές για την ροή του ρεύματος.

Τα έξυπνα δίκτυα προωθούν την «πράσινη ενέργεια» η οποία μπορεί εύκολα να ενσωματωθεί σε ένα τέτοιο σύστημα, καθώς κάθε καταναλωτής μπορεί να γίνει και ο ίδιος παραγωγός ενέργειας, χρησιμοποιώντας φωτοβολταϊκά συστήματα, ανεμογεννήτριες, μικρά υδροηλεκτρικά συστήματα ή κυψέλες υδρογόνου. Με αυτό τον τρόπο, η ενέργεια που δεν καταναλώνεται ή δεν χρειάζεται κάποιος χρήστης, μπορεί να πωληθεί στους υπόλοιπους καταναλωτές. Με τους μετρητές κατανάλωσης ενέργειας ο χρήστης γνωρίζει σε πραγματικό χρόνο την ποσότητα ενέργειας που καταναλώνει (Smart metering).

Ένα έξυπνο δίκτυο παρέχει τις εξής δυνατότητες: [Jawurek, 2012]

• **«Ευφυής» συνύπαρξη** της κεντρικής και διεσπαρμένης παραγωγής με αποτέλεσμα τη μείωση της χρήσης άνθρακα και τον αποδοτικότερο χειρισμό της ηλεκτρικής ζήτησης.

• **Ενεργή συμμετοχή** του πελάτη με βάση αμφίδρομη ροή ενέργειας και επικοινωνίας.

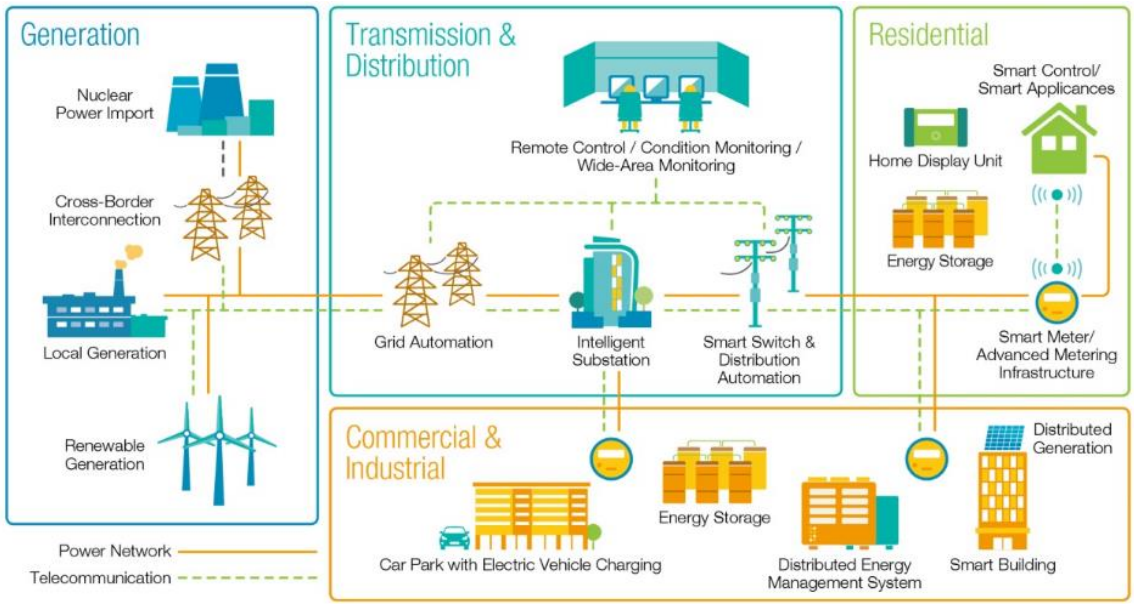
• **Αυξημένη αξιοπιστία**.

• **Αποκεντρωμένη παραγωγή** Οι καταναλωτές μπορούν να γίνουν ταυτόχρονα και παραγωγοί (prosumers).

• **Ελαστικότητα στη ζήτηση ενέργειας** με την ευκολότερη διείσδυση στις ΑΠΕ.

• **Εξοικονόμηση ενέργειας – Μείωση απωλειών.**

• **Προστασία του περιβάλλοντος**.



Εικόνα 2 – Αρχιτεκτονική ενός έξυπνου δικτύου ηλεκτρικής ενέργειας

3 Νομικό πλαίσιο IoT

Τις τελευταίες δεκαετίες, η ιδέα του IoT εξελίσσεται σε μεγάλο βαθμό και αυτό έχει ως αποτέλεσμα να εφαρμόζεται σε πάρα πολλούς τομείς. Η χρήση του IoT δεν γνωρίζει γεωγραφικά σύνορα και η θεωρητική του προσέγγιση γίνεται από διαφορετικές οπτικές γωνίες, με αποτέλεσμα να μην υπάρχει ένα σαφές νομικό πλαίσιο που να εφαρμόζεται στην Ευρωπαϊκή Ένωση. Ως εκ τούτου, κρίνεται απαραίτητη η δημιουργία ενός νομικού πλαισίου που θα προάγει μια εποικοδομητική ανάπτυξη του IoT.

3.1 Ευρωπαϊκή νομοθεσία

3.1.1 Νομοθεσία πριν το IoT

3.1.1.1 1995/46

Η προστασία της ιδιωτικότητας των πολιτών, στα πλαίσια της Ευρωπαϊκής Ένωσης, επιτυγχάνεται με την οδηγία 95/46/ΕΚ, η οποία αποτελούσε το σημαντικότερο νομοθετικό εργαλείο της Ένωσης. Η συγκεκριμένη οδηγία είχε ως στόχο να εξασφαλίσει στα κράτη μέλη της Ε.Ε, την προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων και κυρίως την προστασία της ιδιωτικής ζωής των πολιτών. Ένας επιπλέον στόχος αυτής της οδηγίας είναι να εναρμονίσει τις εκάστοτε εθνικές νομοθεσίες για την προστασία προσωπικών δεδομένων και ταυτόχρονα να διασφαλίσει την ελεύθερη κυκλοφορία τους. Η οδηγία διακρίνεται σε δύο βασικά σημεία. Πρώτο σημείο αποτελεί η έννοια των προσωπικών δεδομένων ως επώνυμων δεδομένων, δηλαδή δεδομένα που μπορούν να συνδεθούν σε ένα φυσικό πρόσωπο. Δεύτερο σημείο της οδηγίας είναι η έννοια της αυτοματοποιημένης επεξεργασίας των προσωπικών δεδομένων, που είναι και το πεδίο πάνω στο οποίο εφαρμόζεται και συνίσταται στη αποθήκευση, συλλογή και χρήση [EU portal].

Ένας ακόμη στόχος της οδηγίας 95/46/ΕΚ είναι να προστατεύει τα δικαιώματα και τις ελευθερίες των πολιτών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, με τον καθορισμό των κατευθυντήριων γραμμών που καθιστούν νόμιμη αυτήν την επεξεργασία. Οι κατευθυντήριες γραμμές αφορούν:

- Την ποιότητα των δεδομένων. Δηλαδή τα δεδομένα προσωπικού χαρακτήρα οφείλουν να συγκεντρώνονται για συγκεκριμένους και νόμιμους σκοπούς και να αποτελούν αντικείμενο θεμιτής επεξεργασίας.

- Τη νόμιμη επεξεργασία των δεδομένων. Αυτό σημαίνει ότι, η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται μόνο αν ο πολίτης συναινέσει στην ενέργεια αυτή ή αν συντρέχουν υποχρεωτικοί λόγοι για να γίνει αυτή η επεξεργασία. Ένας λόγος είναι η εκτέλεση σύμβασης κατά την οποία ο εμπλεκόμενος αποτελεί το συμβαλλόμενο μέρος. Δεύτερον, ο υπεύθυνος της επεξεργασίας οφείλει να τηρεί τη νομική υποχρέωση. Τρίτος λόγος είναι η διαφύλαξη του ζωτικού συμφέροντος του εμπλεκόμενου πολίτη, ενώ τέταρτος είναι η επεξεργασία των δεδομένων για λόγους δημοσίου συμφέροντος. Τέλος, όταν ο υπεύθυνος της επεξεργασίας των δεδομένων υλοποιεί κάποιο θεμιτό συμφέρον.
- Τις ειδικές κατηγορίες επεξεργασίας. Η διάταξη αυτή απαγορεύει την επεξεργασία δεδομένων που σχετίζονται με την εθνικότητα, τις προσωπικές απόψεις, τις θρησκευτικές και πολιτικές πεποιθήσεις, την ερωτική ζωή και την υγεία. Επίσης, η διάταξη εκφράζει τις επιφυλάξεις σχετικά με την υπεράσπιση των ζωτικών συμφερόντων του πολίτη.
- Την ενημέρωση των πολιτών σχετικά με την επεξεργασία δεδομένων. Ο υπεύθυνος της επεξεργασίας των δεδομένων θα πρέπει να παρέχει στον πολίτη κάποιες από τις πληροφορίες, όπως είναι η ταυτότητα του υπεύθυνου της επεξεργασίας των δεδομένων, ο λόγος της επεξεργασίας τους και ποιοι θα χρησιμοποιήσουν τα δεδομένα.
- Το δικαίωμα πρόσβασης των πολιτών στα προσωπικά τους δεδομένα. Κάθε πολίτης είναι απαραίτητο να έχει το δικαίωμα να εξασφαλίσει από τον υπεύθυνο της επεξεργασίας πρώτον, ότι τα προσωπικά του δεδομένα υφίστανται ή όχι κάποια επεξεργασία και αν υφίστανται να του κοινοποιούνται. Δεύτερον, η διόρθωση, η διαγραφή, ακόμη και η απαγόρευση της πρόσβασης στα προσωπικά του δεδομένα, δεν πρέπει να τύχουν επεξεργασίας και να κοινοποιούνται οι αλλαγές αυτές σε τρίτους.
- Τις εξαιρέσεις και τους περιορισμούς. Οι βασικές αρχές που σχετίζονται με την ποιότητα των δεδομένων, την πληροφόρηση του εμπλεκόμενου πολίτη, το δικαίωμα πρόσβασης στα δεδομένα και την κοινοποίηση των τροποποιημένων δεδομένων μπορούν να έχουν περιορισμένη πρόσβαση. Αυτό συμβαίνει για να εξασφαλιστεί η κρατική και η δημόσια ασφάλεια, η άμυνα, οι ποινικές παραβάσεις, το οικονομικό συμφέρον ενός κράτους μέλους της Ε.Ε και τέλος η προστασία του πολίτη.

- Το δικαίωμα αντίταξης στην επεξεργασία δεδομένων. Σε αυτή την περίπτωση ο εμπλεκόμενος πολίτης έχει το δικαίωμα να αρνηθεί την όποια επεξεργασία των δεδομένων που τον αφορούν για θεμιτούς λόγους. Επίσης, έχει το δικαίωμα να αντιταχθεί στην επεξεργασία των δεδομένων με σκοπό τη διερεύνηση. Τέλος, ο εμπλεκόμενος πολίτης θα πρέπει να είναι ενημερωμένος προτού κοινοποιηθούν τα προσωπικά του δεδομένα σε τρίτους για ερευνητικούς σκοπούς και να έχει το δικαίωμα να αρνηθεί αυτή την κοινοποίηση.
- Την εμπιστευτικότητα και την ασφάλεια της επεξεργασίας. Σε αυτό το σημείο ο υπεύθυνος της επεξεργασίας των δεδομένων είναι ο κύριος υπεύθυνος που έχει την εξουσία να αναθέτει την επεξεργασία τους σε τρίτα πρόσωπα ή υπεργολάβους. Ακόμη, ο υπεύθυνος επεξεργασίας των δεδομένων είναι αυτός που εφαρμόζει τα απαραίτητα μέτρα για να προστατεύσει τα δεδομένα από τυχαία ή παράνομη καταστροφή, απώλεια, διάδοση και πρόσβαση χωρίς έγκριση και αλλοίωση.
- Την κοινοποίηση των αποτελεσμάτων της επεξεργασίας σε ελεγκτική αρχή. Αρχικά, η αρμόδια ελεγκτική αρχή θα πρέπει να είναι ενήμερη από τον υπεύθυνο επεξεργασίας των δεδομένων πριν την τέλεση οποιασδήποτε επεξεργασίας. Ακόμη, η ελεγκτική αρχή πρέπει να εξετάζει τους πιθανούς κινδύνους που ελλοχεύουν σχετικά με τα δικαιώματα και τις ελευθερίες των εμπλεκόμενων πολιτών. Τέλος, οι ελεγκτικές αρχές είναι υποχρεωμένες να τηρούν ένα μητρώο των κοινοποιημένων αποτελεσμάτων επεξεργασίας, ώστε να διασφαλίζεται η δημοσιότητα των αποτελεσμάτων [EU portal].

3.1.1.2 2002/58

Η οδηγία 2002/58/ΕΚ (e-Privacy), η οποία νομοθετήθηκε στις 12/07/2002, αποτελεί ένα νομοθετικό εργαλείο που ανταποκρίνεται στις σύγχρονες τεχνολογικές προκλήσεις και στη ραγδαία ανάπτυξη της τεχνολογίας. Η οδηγία αυτή, έρχεται να αντικαταστήσει την οδηγία 97/66/ΕΚ που αφορά την προστασία της ιδιωτικότητας αλλά και των προσωπικών δεδομένων στις τηλεπικοινωνίες. Η οδηγία 2002/58/ΕΚ δημιουργήθηκε με σκοπό την εισαγωγή ενός νέου ρυθμιστικού πλαισίου, στο οποίο εισάγεται και η χρήση του διαδικτύου. Πέρα από αυτά, η οδηγία μεριμνεί για όλες τις δυνατότητες του διαδικτύου, που σχετίζονται με την παραβίαση της ιδιωτικότητας του χρήστη, όπως τα spyware, cookies, worms,. Ο βασικός στόχος που έχει η οδηγία είναι η προστασία των χρηστών του διαδικτύου, ανεξαρτήτως της τεχνολογίας που εφαρμόζεται

[EU portal]. Τέλος, η οδηγία προβλέπει, μέσω ειδικής ρύθμισης και τη χρήση των cookies, αποκλειστικά και μόνο για θεμιτούς σκοπούς και με την όρο ότι η χρήση τους είναι εν γνώσει του κάθε χρήστη.

3.1.1.3 2006/24

Η οδηγία 2006/24/ΕΚ αποτελεί τροχοπέδη στην προστασία των προσωπικών δεδομένων σχετικά με την αποθήκευση των δεδομένων αυτών από τους παρόχους υπηρεσιών επικοινωνίας. Τα προσωπικά δεδομένα αφορούν δεδομένα κίνησης (traffic data) και δεδομένα τοποθεσίας (location data) και όχι το περιεχόμενο των επικοινωνιών. Με άλλα λόγια, τα δεδομένα που αποθηκεύονται σχετίζονται με την πηγή, τον προορισμό, την ημερομηνία, τη διάρκεια, τον τύπο της επικοινωνίας και τον προσδιορισμό του μέσου της επικοινωνίας ή την τοποθεσία της. Είναι απαραίτητο να διασφαλιστεί η διατήρηση των δεδομένων για κάποιο χρονικό διάστημα, επειδή έχουν μεγάλη σημασία για να διερευνούν, να διαπιστώνουν και να διώκουν τα ποινικά αδικήματα. Αυτό ονομάζεται φύλαξη ορισμένων κατηγοριών δεδομένων (Data Retention), από αυτούς που παρέχουν υπηρεσίες στο διαδίκτυο, η οποία φύλαξη θεωρείται εξαιρετικά σημαντική στον τομέα του ηλεκτρονικού εγκλήματος [EU portal].

Επίσης μία σειρά από συστάσεις της Ευρωπαϊκής Επιτροπής όπως είναι για παράδειγμα η R (99) 5 που αφορά την προστασία της ιδιωτικότητας στο διαδίκτυο, η R (89) 9 που αφορά τον προσδιορισμό των ηλεκτρονικών εγκλημάτων και η R (95) 13 που αφορά τα ζητήματα της ποινικής διαδικασίας στην πληροφορική και ηλεκτρονική τεχνολογία, σχετίζονται σε μεγάλο βαθμό με την προστασία της ιδιωτικότητας στον ευρωπαϊκό χώρο [EU portal].

Τέλος, η νομοθεσία 95/46/ΕΚ θεσπίστηκε σε μια χρονική περίοδο όπου το διαδίκτυο δε χρησιμοποιούνταν και δεν ήταν ευρέως διαδεδομένο, με αποτέλεσμα η Ευρωπαϊκή Επιτροπή να έχει ήδη δημιουργήσει ένα νέο νομοθετικό πλαίσιο. Στις μέρες μας πολλά εκατομμύρια πολιτών της Ευρωπαϊκής Ένωσης χρησιμοποιούν το διαδίκτυο σε καθημερινή βάση, με αποτέλεσμα να θεωρείται αναγκαία η αναθεώρηση της ισχύουσας νομοθεσίας σε ευρωπαϊκή κλίμακα [EU portal].

3.1.1.4 2009/387

Η χρήση των ραδιοσυχνοτήτων (RFID) επέφερε το 2009, τη θέσπιση συστάσεων από την Ευρωπαϊκή Επιτροπή προκειμένου να ασφαλίζει και να προστατεύει τις εφαρμογές που χρησιμοποιούν την τεχνολογία των ραδιοσυχνοτήτων. Τα RFID

αποτελούν τον προάγγελο τον IoT και σηματοδοτούν μία νέα εποχή στην κοινωνία της πληροφορίας. Αυτό σημαίνει ότι ηλεκτρονικές συσκευές που αποτελούνται από μικροεπεξεργαστές έχουν ως σκοπό την επεξεργασία των δεδομένων και γίνονται ολοένα και μεγαλύτερο κομμάτι της καθημερινότητας. Δηλαδή, σύμφωνα με την οδηγία 387/2009/EC νομοθετούνται οι τεχνικές προδιαγραφές, για να μπορούν οι χρήστες να χρησιμοποιούν αυτήν την τεχνολογία.

Η RFID τεχνολογία δύναται να χρησιμοποιηθεί από λιανοπωλητές για να ελέγχουν τα αποθέματα των εμπορευμάτων τους εναρμονισμένοι με το νομικό πλαίσιο της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων. Από τη σκοπιά των τεχνικών που δημιουργούν εφαρμογές RFID, θα πρέπει οι εφαρμογές αυτές να διέπονται από τους κανόνες των αρχών προστασίας των προσωπικών δεδομένων (data protection by design). Τέλος, οι καταναλωτές πρέπει να έχουν τις ακριβείς πληροφορίες που έχουν συλλεχθεί από τις εταιρίες και τις δημόσιες αρχές και να γνωρίζουν το σκοπό της χρήσης τους. Τα κράτη μέλη της ΕΕ μπορούν να χρησιμοποιήσουν αυτή τη σύσταση, χωρίς όμως να είναι υποχρεωμένα [EU portal].

3.1.2 Νομοθεσία μετά το IoT

3.1.2.1 2014/8

Η οδηγία 8/2014/ΕΚ, η οποία νομοθετήθηκε τον Σεπτέμβριο του 2014, είναι η πρώτη οδηγία που αφορά το IoT αλλά δεν έχει δεσμευτικό χαρακτήρα. Λόγω του χαρακτήρα της, η οδηγία αυτή απλά συστήνει τρόπους προστασίας της ιδιωτικότητας του χρήστη, ο οποίος χρησιμοποιεί συσκευές IoT που συνδέονται στο διαδίκτυο και φοριούνται (wearable IoT) ή αφορούν την αυτοματοποίηση της οικίας του. Η διασφάλιση των προσωπικών δεδομένων του χρήστη θεωρείται επιτακτική ανάγκη, μιας και οι συσκευές IoT γίνονται όλο και πιο ευφυείς με αποτέλεσμα να είναι σε θέση να καταγράφουν την καθημερινότητα των χρηστών. Οι χρήστες της IoT τεχνολογίας, θα πρέπει να είναι πλήρως ενημερωμένοι από πριν, γύρω από μια πιθανή παραβίαση της ιδιωτικότητας των προσωπικών τους δεδομένων, έτσι ώστε να καταφέρουν να την εμπιστευτούν και να τη χρησιμοποιούν σε ακόμα μεγαλύτερο βαθμό στην καθημερινότητά τους. Τέλος, η συγκεκριμένη οδηγία, εστιάζει σε τρείς τομείς, οι οποίοι αξιοποιούνται καθημερινά από τον μέσο χρήστη της IoT τεχνολογίας, την τεχνολογία που φοριέται (wearable IoT), την IoT τεχνολογία στις οικιακές συσκευές (home

automation) και την ποσοτικοποίηση των προσωπικών στοιχείων (quantified self) [EC, 2014].

Υπάρχουν κάποια προβλήματα, άξια προσοχής, σχετικά με την τεχνολογία IoT, τα οποία φανέρωσε η ευρωπαϊκή ομάδα εργασίας (working party) [Wessing, 2015]. Το πρώτο πρόβλημα εστιάζεται στον ελλιπή έλεγχο στη ροή πληροφοριών. Συγκεκριμένα, η αλληλεπίδραση ανάμεσα στους χρήστες, στις IoT συσκευές και στα συστήματα που λειτουργούν στο παρασκήνιο (backend), δημιουργεί δεδομένα, τα αποθηκεύει και τα μοιράζει μεταξύ των συσκευών. Ωστόσο, τα δεδομένα αυτά δεν είναι στην απόλυτη ευχέρεια του τελικού χρήστη, αν και τον αφορούν.

Το δεύτερο πρόβλημα σχετίζεται με την απουσία της συγκατάθεσης του χρήστη. Με άλλα λόγια, οι περισσότερες IoT συσκευές δεν απαιτούν τη συγκατάθεση του χρήστη και δεν ικανοποιούν τις απαραίτητες συνθήκες για την παραγωγή, την αποθήκευση και τον διαμοιρασμό των δεδομένων. Το τρίτο πρόβλημα αφορά την παρέκκλιση στη χρήση των δεδομένων. Οι ενδιάμεσοι και μη σχετικοί φορείς τις περισσότερες φορές διαθέτουν ακατέργαστες πληροφορίες με σκοπό τη δημιουργία νέων δεδομένων για διαφορετικούς σκοπούς από τους αρχικούς.

Τέταρτο πρόβλημα είναι η δυσχέρεια στην επίτευξη της ανωνυμίας. Αυτό σημαίνει ότι το να χρησιμοποιεί κάποιος χρήστης IoT συσκευές φανερώνει προσωπικά χαρακτηριστικά του. Αυτό με τη σειρά του οδηγεί στη σκιαγράφηση του χρήστη μέσα από την αποκάλυψη διάφορων αναγνωριστικών στοιχείων όπως για παράδειγμα η MAC διεύθυνση των IoT συσκευών.

Εκτός από τα παραπάνω προβλήματα, η ευρωπαϊκή ομάδα εργασίας θέσπισε ορισμένους κανόνες με βάση την οδηγία αυτή, που εστιάζουν στο σύνολο των ενδιαφερόμενων ομάδων σχετικά με την IoT τεχνολογία [Wessing, 2015].

Αρχικά, κατά τη διαδικασία της διαχείρισης των δεδομένων, θα πρέπει όλοι οι συμμετέχοντες, να έρθουν σε συμφωνία σχετικά με τα ζητήματα ιδιωτικότητας των προσωπικών δεδομένων. Με άλλα λόγια, θα πρέπει να σχεδιάζονται οι νέες εφαρμογές του IoT ακολουθώντας συγκεκριμένα πρότυπα ιδιωτικότητας (Privacy by Design, Privacy by Default). Επιπρόσθετα, άλλος κανόνας που θεσπίστηκε, ορίζει τη διαγραφή των δεδομένων που δεν έχουν επεξεργαστεί (raw data), αφού πρώτα έχουν αποκτηθεί τα απαραίτητα δεδομένα. Τέλος, το ιδιωτικό απόρρητο του κάθε χρήστη πρέπει να είναι σεβαστό από όλους τους συμμετέχοντες και να ενημερώνουν τον χρήστη για τις πληροφορίες που τον αφορούν και διακινούνται.

Επίσης, αυτοί που κατασκευάζουν το υλικό (hardware) και το λογισμικό (software) θα πρέπει αρχικά, να ενημερώνουν τους χρήστες για οποιαδήποτε λεπτομέρεια που αφορά την επεξεργασία των δεδομένων. Επιπλέον, θα πρέπει τα προσωπικά δεδομένα να έχουν τέτοια μορφή ώστε να επιτυγχάνεται η φορητότητά τους και ο ενδιαφερόμενος χρήστης να μπορεί να έχει πρόσβαση σε αυτά. Τέλος, τα προσωπικά δεδομένα θα πρέπει να προστατεύονται και να ανανεώνονται οι υπηρεσίες τους με γνώμονα τα πρότυπα αντιμετώπισης ηλεκτρονικών επιθέσεων.

Στο επίπεδο των προγραμματιστών εφαρμογών για IoT συσκευές θα πρέπει πρώτον, να υπάρχει ενημέρωση των χρηστών αναφορικά με τη συλλογή προσωπικών ή μη δεδομένων από τις εκάστοτε IoT εφαρμογές και δεύτερον, να έχουν τη δυνατότητα οι χρήστες να επεξεργάζονται ή να διαγράφουν τα δεδομένα που συλλέγονται και τους αφορούν.

Αναφορικά με τα μέσα κοινωνικής δικτύωσης, οι χρήστες θα πρέπει να είναι ενήμεροι ότι χρησιμοποιώντας τις IoT συσκευές τους, οι πληροφορίες τους δεν θα είναι κοινοποιήσιμες στο ευρύ κοινό παρά μόνο αν ο ίδιος το επιθυμεί και δεν θα εμφανίζονται σε αποτελέσματα των μηχανών αναζήτησης.

Σε περίπτωση που κάποιος κάτοχος IoT συσκευής δεν επιθυμεί την επεξεργασία των προσωπικών του δεδομένων, αυτό δεν θα πρέπει να του επιφέρει κάποιου είδους ποινή ή μειωμένες δυνατότητες στις IoT εφαρμογές. Επίσης, αυτοί που δεν χρησιμοποιούν συσκευές IoT άμεσα, θα πρέπει να ενημερώνονται ότι δύναται να συλλεχθούν οι πληροφορίες τους ακόμη και από την απλή παρουσία τους στο χώρο.

Με τη σειρά τους οι οργανισμοί προτυποποίησης πρέπει να προωθούν διαλειτουργικές μορφές δεδομένων, να επιδιώκουν την ανωνυμία στο διαδίκτυο μεριμνώντας ώστε τα δεδομένα που συλλέγονται να επεξεργάζονται με τη χρήση πιο λίγων πιστοποιητικών ταυτοποίησης. Τέλος, θα πρέπει να υιοθετήσουν τη χρήση πρωτοκόλλων κρυπτογράφησης και επικοινωνίας για τα IoT συστήματα, πιστοποιητικά ασφάλειας και απορρήτου με σκοπό την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας.

3.1.2.2 2016/679 (GDPR)

Στις 27 Απριλίου 2016 τα όργανα του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου θέσπισαν τον κανονισμό 2016/679, με σκοπό να προστατεύσει τα φυσικά πρόσωπα από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη

κυκλοφορία αυτών των δεδομένων. Αυτός ο κανονισμός νομοθετήθηκε για να καταργήσει την οδηγία 95/46/ΕΚ του 1995, επειδή υπήρξε ραγδαία εξέλιξη της τεχνολογίας και των εφαρμογών που χρησιμοποιούν τα προσωπικά δεδομένα. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων ή αλλιώς το GDPR, εφαρμόζεται σε οργανισμούς εντός και εκτός της Ευρωπαϊκής Ένωσης, με την προϋπόθεση οι διεθνείς αυτοί οργανισμοί να προσφέρουν τα προϊόντα ή τις υπηρεσίες τους ή να επεξεργάζονται τα δεδομένα των πολιτών της ΕΕ. Το GDPR δύναται να εφαρμοστεί σε εταιρείες που αποθηκεύουν και επεξεργάζονται τα προσωπικά δεδομένα των πολιτών της ΕΕ [EU GDPR.ORG, 2016].

Ένα ακόμη σημείο του κανονισμού που πρέπει να τονιστεί ότι οι πολίτες πλέον έχουν πιο μεγάλο έλεγχο των δεδομένων τους και η πρόσβαση σε αυτά είναι ευκολότερη. Επίσης, ο κανονισμός κάνει πιο εύκολη τη διαγραφή και τη φορητότητα των δεδομένων. Επεξηγηματικά, όταν κάποιος χρήστης θελήσει να διαγράψει εντελώς ή να μεταφέρει τα δεδομένα του σε έναν διαφορετικό πάροχο, αυτό πρέπει να γίνεται με τηρώντας τους κανονισμούς ασφάλειας και ιδιωτικότητας. Ο νέος αυτός κανονισμός παρέχει στους πολίτες ορισμένα οφέλη. Πιο συγκεκριμένα, τους προσφέρει το δικαίωμα στη λήθη, να αποφασίζουν οι ίδιοι αν θα δώσουν τα προσωπικά δεδομένα τους προς επεξεργασία ή αν θα τα μεταφέρουν, να έχουν εύκολη πρόσβαση στα δεδομένα τους και τελικώς να έχουν τις απαραίτητες γνώσεις να αντιμετωπίσουν τις παραπάνω καταστάσεις.

Σύμφωνα με τον κανονισμό για το GDPR, κάθε οργανισμός που διαθέτει πάνω από 250 εργαζομένους οφείλει να έχει έναν Επόπτη Προστασίας Δεδομένων (Data Protection Officer). Ο Επόπτης Προστασίας Δεδομένων είναι ο αρμόδιος για τη διασφάλιση της συμμόρφωσης του οργανισμού με το GDPR και είναι αυτός που πρέπει να ειδοποιεί τους εμπλεκόμενους πολίτες αλλά και τις αρχές εντός προκαθορισμένου χρόνου, σε περίπτωση που υπάρχει απώλεια ή διαρροή των δεδομένων. Για να μπορέσει να καταφέρει όσα αναφέρθηκαν παραπάνω, ο Επόπτης Προστασίας Δεδομένων πρέπει να κάνει κάποια προετοιμασία. Από τη μεριά τους οι πολίτες έχουν το δικαίωμα να πάρουν τα δεδομένα στην κατοχή τους σε ψηφιακό αντίγραφο και οι εταιρίες να μπορούν να διαγράψουν τα δεδομένα και να εγγυηθούν για την ασφάλειά και την ιδιωτικότητα τους.

3.1.2.3 Γνωμοδότηση 2018/C 440/02 (INT/846)

Η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (EESC) δημοσίευσε στις 19 Σεπτεμβρίου το 2018, τη γνωμοδότηση 2018/C 440/02 που αφορά την εμπιστοσύνη, την ιδιωτικότητα και την ασφάλεια των πολιτών και των επιχειρήσεων στο IoT. Η γνωμοδότηση αναφέρει ότι η εξέλιξη του διαδικτύου τα τελευταία είκοσι χρόνια έχει αλλάξει την καθημερινή ζωή των πολιτών, δημιουργώντας τους νέες ανάγκες και συνήθειες. Επίσης, η γνωμοδότηση αναφέρει ότι τα επόμενα χρόνια το IoT θα επιφέρει αλλαγές σε διάφορους τομείς, όπως είναι η γεωργία, οι μεταφορές, ο τομέας της ενέργειας και η κοινωνία.

Υπάρχουν μεγάλες νομικές προκλήσεις που αντιμετωπίζουν η ΕΕ και τα κράτη μέλη της. Αυτό συμβαίνει επειδή κάποια από τα χαρακτηριστικά του IoT, όπως είναι η αυτονομία και η αλληλεξάρτηση ανάμεσα στις συνδεδεμένες συσκευές, δημιουργούν καινούργιες τεχνολογίες, όπως είναι το υπολογιστικό νέφος (cloud) και η τεχνολογία του Blockchain.

3.2 Ελληνική νομοθεσία

Στην Ελλάδα, υπάρχουν νομικά κενά σε σχέση με την IoT τεχνολογία. Οι μόνες οδηγίες της ΕΕ που νομοθετήθηκαν στο ελληνικό δίκαιο είναι οι 46/95/EC και η 58/2002/EC με τους νόμους 2472/1997 και 3471/2006 αντίστοιχα [Εθνικό Τυπογραφείο].

3.2.1 Ν.2472/97

Ο Ν.2472/97 θεσπίζει μέτρα για την προστασία των πολιτών κατά την επεξεργασία των προσωπικών δεδομένων. Συγκεκριμένα ο νόμος προστατεύει την επεξεργασία των προσωπικών δεδομένων και έχει ως σκοπό να προστατεύει τα δικαιώματα και τις ελευθερίες των χρηστών. Τέλος, μέσω του συγκεκριμένου νόμου θεσπίστηκε και συγκροτήθηκε με αυξημένες αρμοδιότητες και δικαιώματα, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

3.2.2 Ν. 3471/06

Ο νόμος αυτός εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων και διασφαλίζει το απόρρητο των επικοινωνιών σε δημόσια δίκτυα. Όσο αναφορά τη διασφάλιση του απορρήτου στις τηλεπικοινωνίες, δεν επιτρέπει την ακρόαση, την υποκλοπή, την αποθήκευση και την παρακολούθηση των επικοινωνιών από τρίτους χρήστες, χωρίς τη συγκατάθεσή τους. Ακόμη, δεν επιτρέπει να εγκαθιστούν επιτήδειοι

κατασκοπευτικό λογισμικό και υποχρεώνει τους παρόχους να διαγράφουν μετά το πέρας της επεξεργασίας ή να καθιστούν ανώνυμα δεδομένα σχετικά με την κίνηση και τη θέση του χρήστη. Κλείνοντας, οι πάροχοι υπηρεσιών διαδικτύου θα πρέπει να λαμβάνουν μέτρα σχετικά με την ασφάλεια των δεδομένων και παράλληλα θα πρέπει να ενημερώνουν τους χρήστες για οποιαδήποτε κακόβουλη πράξη υποστούν τα δεδομένα τους.

4 Ζητήματα ασφάλειας και ιδιωτικότητας

Η ασφάλεια, η ιδιωτικότητα αλλά ταυτόχρονα και η ευχρηστία θα πρέπει να διασφαλίζονται κατά τη δημιουργία ενός IoT οικοσυστήματος. Οι χρήστες της IoT τεχνολογίας θα πρέπει να είναι ενημερωμένοι από πριν, σχετικά με ιδιότητες της. Με αυτό τον τρόπο θα μπορούν να εκμεταλλευτούν όλα τα οφέλη του IoT αλλά να αποφύγουν αρνητικές και επίφοβες λύσεις στον τομέα αυτό. Νέα ζητήματα ασφάλειας και ιδιωτικότητας προκύπτουν, εξαιτίας της δυνατότητας που προσφέρει η IoT τεχνολογία. Ουσιαστικά, επιτρέπει σε διάφορες έξυπνες συσκευές – αντικείμενα, να συνδέονται απευθείας με το διαδίκτυο, δίνοντας τους τη δυνατότητα να επικοινωνούν με άλλες έξυπνες συσκευές και να ανταλλάσσουν δεδομένα. Κάποιες βασικές αρχές θα πρέπει να διασφαλιστούν στα πλαίσια της IoT τεχνολογίας όπως είναι η ιδιωτικότητα, η διαθεσιμότητα, η εμπιστευτικότητα, η αξιοπιστία, η ακεραιότητα, η αυθεντικοποίηση και η εξουσιοδότηση.

Σε ένα IoT οικοσύστημα, σημαντικό ρόλο έχουν τα RFID συστήματα, καθώς και τα ασύρματα δίκτυα αισθητήρων, τα οποία διαθέτουν εξαιρετικά περιορισμένους υπολογιστικούς πόρους και ταυτόχρονα περιλαμβάνουν μικρές πηγές ενέργειας για τη λειτουργία τους. Κατά το στάδιο όπου σχεδιάζονται οι προτάσεις διευθέτησης διάφορων ζητημάτων ασφάλειας, θα πρέπει οι ειδικοί να μεριμνήσουν για τους παραπάνω δυο περιορισμούς. Αξίζει να σημειωθεί πως τα κενά ασφαλείας που εντοπίζονται στο διαδίκτυο, θα βρίσκονται και σε ένα IoT περιβάλλον, καθώς η λειτουργία του IoT εξαρτάται άμεσα από το διαδίκτυο. Σε τρία βασικά επίπεδα εστιάζουν οι αρχιτεκτονικές της IoT τεχνολογίας, στο επίπεδο της αντίληψης, στο επίπεδο της μεταφοράς και στο επίπεδο των εφαρμογών. Διάφορες τεχνικές ασφάλειας θα πρέπει να περιλαμβάνονται σε καθένα από τα τρία παραπάνω επίπεδα που αναφέρθηκαν, σε ένα IoT περιβάλλον.

4.1 Βασικές αρχές ασφάλειας

❖ **Εμπιστευτικότητα**

Οι διαχειριστές των IoT συστημάτων, θα πρέπει να διαθέτουν κάποιου είδους άδεια για να έχουν τη δυνατότητα να επεξεργάζονται ευαίσθητα προσωπικά δεδομένα. Με τον τρόπο αυτόν, θα επιτυγχάνεται η αρχή της εμπιστευτικότητας των προσωπικών δεδομένων των χρηστών. Πιο αναλυτικά, με τη χρήση της κρυπτογραφίας, είτε

συμμετρικής είτε ασύμμετρης, μπορεί να επιτευχθεί η εμπιστευτικότητα των ευαίσθητων πληροφοριών. Για την επιλογή του είδους κρυπτογράφησης που θα χρησιμοποιηθεί, θα πρέπει πρώτα να μελετηθούν οι υπολογιστικές δυνατότητες της IoT συσκευής που πρόκειται να χρησιμοποιήσει τέτοιους αλγορίθμους [Alam, 2011].

- **Ιδιωτικότητα**

Το IoT εφαρμόζεται σε διάφορους τομείς της καθημερινής ζωής του ανθρώπου, όπως είναι η ιατρική (απομακρυσμένη παροχή ιατρικής φροντίδας), τα έξυπνα σπίτια ή και η διαχείριση της κυκλοφορίας των αυτοκίνητων, κάνοντας χρήση πολλές φορές, ευαίσθητων προσωπικών δεδομένων. Η ιδιωτικότητα του χρήστη προστατεύεται με τη χρήση διάφορων τεχνικών στη ροή πληροφοριών (Information Flow Control). Η χρήση αυτών των τεχνικών, επιτυγχάνει τον χαρακτηρισμό της πληροφορίας με δεδομένα (metadata) που αφορούν το λόγο που δημιουργήθηκαν καθώς και το λόγο που στάλθηκαν, με αποτέλεσμα να τελεσφορείται η ιδιωτικότητα των IoT χρηστών. Το μόνο αρνητικό σημείο στη χρήση τέτοιων τεχνικών, είναι η υψηλή χρήση υπολογιστικής ισχύος από τις IoT συσκευές.

Εκτός των παραπάνω τεχνικών, την ιδιωτικότητα σε IoT συστήματα μπορεί να προασπίσει η χρήση πρωτοκόλλων ελέγχου πρόσβασης, με σκοπό τη χρήση τεχνικών που επιτυγχάνουν την ανωνυμία του χρήστη. Πιο αναλυτικά, η χρήση μιας διαδεδομένης «data stream classification» τεχνικής, η οποία ονομάζεται Continuously Anonymizing Streaming data via adaptive cLustEring (CASTLE), μπορεί να επιτύχει την ιδιωτικότητα των δεδομένων που ανταλλάσσουν οι IoT συσκευές και να περιορίσει τις καθυστερήσεις μετάδοσης τους. Στη συνέχεια, η παροχή πρόσβασης γίνεται αφού ταυτοποιηθεί ο χρήστης καθώς και δεν γίνεται ανάθεση ενός domain name σε έναν IoT κόμβο. Έτσι, η χρήση του προαναφερθέντος Domain Name System (DNS), το οποίο είναι τεχνολογικά εξελιγμένο συγκριτικά με αυτό που χρησιμοποιείται σήμερα, προστατεύει την ιδιωτικότητα των χρηστών IoT συσκευών [Sicari, 2014].

- **Ακεραιότητα**

Διάφοροι φορείς, όπως είναι οι κυβερνητικές αρχές, οι πάροχοι υπηρεσιών διαδικτύου, καθώς και ελεγκτικοί μηχανισμοί θέτουν ως προϋπόθεση τη μη αλλοίωση των δεδομένων που ανταλλάσσονται σε ένα IoT περιβάλλον είτε με δόλια μέσα είτε από την ύπαρξη σφαλμάτων σε αυτά. Κατά τη σχεδίαση αξιόπιστων IoT συστημάτων, η ακεραιότητα των δεδομένων διαδραματίζει σημαντικό ρόλο. Για να πραγματοποιηθεί αυτό χρησιμοποιούνται κώδικες αυθεντικοποίησης μηνύματος (Message Authentication

Code, MAC) οι οποίοι με τη σειρά τους απαιτούν τη χρήση συναρτήσεων κατακερματισμού (hash functions). Οι δυνατότητες της κάθε συσκευής, όπως για παράδειγμα η υπολογιστική ισχύς της ή η κατανάλωση ενέργειας, είναι χαρακτηριστικά που καθορίζουν τις τεχνικές που θα χρησιμοποιηθούν.

❖ **Διαθεσιμότητα**

Με τον όρο διαθεσιμότητα ορίζεται η ιδιότητα ενός χρήστη να έχει πρόσβαση χωρίς κάποια καθυστέρηση στις υπηρεσίες ενός IoT δικτύου. Στο επίπεδο της ασφάλειας απαραίτητη είναι η χρήση διάφορων τεχνικών που αποσκοπούν στο να αποτρέψουν κακόβουλες επιθέσεις που στόχο έχουν την παρεμπόδιση της πρόσβασης σε αυτά των νόμιμων χρηστών. Η διαθεσιμότητα των δεδομένων και των υπηρεσιών σε ένα σύγχρονο IoT περιβάλλον, δεν διαβεβαιώνεται από κανένα πρωτόκολλα ασφαλείας από μόνο του. Για να υπολογιστεί η διαθεσιμότητα ενός IoT συστήματος, πρέπει να συνδυαστούν πολλές τεχνικές αλλά και μετρήσεις από πραγματικά δεδομένα.

❖ **Αυθεντικοποίηση**

Η αυθεντικοποίηση έχει να κάνει με την επαλήθευση της ταυτότητας κάποιου χρήστη. Σε ένα IoT περιβάλλον, η αυθεντικοποίηση πρέπει να επιτυγχάνεται και από την πλευρά του αποστολέα και από την πλευρά του παραλήπτη, δηλαδή ο παραλήπτης των δεδομένων πρέπει να ταυτοποιήσει τον αποστολέα και τις πληροφορίες. Επιπλέον, η αυθεντικοποίηση στο IoT οικοσύστημα επιτυγχάνεται με τη χρήση ισχυρών μηχανισμών και πρωτοκόλλων όπως το Datagram Transport Layer Security (DTLS), το οποίο εφαρμόζεται μεταξύ του επιπέδου μεταφοράς και των εφαρμογών στο μοντέλο OSI (Open Systems Interconnection) του ISO. Το παραπάνω πρωτόκολλο, το οποίο δύναται να λειτουργήσει στο IPv4 καθώς και στο IPv6, περιλαμβάνει πλήθος γνωστών αλγορίθμων αυθεντικοποίησης. Επιπρόσθετα, με τη χρήση των προτύπων κωδικοποίησης EPC (Electronic Product Code), αλλά και με το ucode εξασφαλίζεται η αυθεντικοποίηση των IoT συσκευών. Η κωδικοποίηση EPC είναι ένα πρότυπο ταυτοποίησης προϊόντων με τη χρήση ετικετών ανάγνωσης, παγκόσμιας κλίμακας και η μορφή του είναι Uniform Resource Identifier (URI). Με τη σειρά του ο μηχανισμός ucode, ταυτοποιεί αντικείμενα και τοποθεσίες, χρησιμοποιώντας 128 bit και αποτελεί θεμέλιο λίθο για την υλοποίηση ενός IoT συστήματος. Από την άλλη πλευρά η χρήση τέτοιων προτύπων έρχεται σε αντίθεση με την επάρκεια υπολογιστικών πόρων στις IoT συσκευές [Sicari, 2014] [Roman, 2013] [Wikipedia].

❖ **Εξουσιοδότηση**

Υπάρχουν μηχανισμοί ελέγχου πρόσβασης στα IoT συστήματα, οι οποίοι είναι υποχρεωμένοι να δημιουργούν μοντέλα, ώστε να διασφαλίζουν την εξουσιοδοτημένη πρόσβαση σε δεδομένα και πόρους. Πλέον θεωρείται επιτακτική ανάγκη να είναι ιδιωτική και να υπάρχει περιορισμένη πρόσβαση στα δεδομένα, καθώς το IoT εξελίσσεται με ραγδαίους ρυθμούς. Οι λίστες ελέγχου πρόσβασης (Access-control lists | ACL) που καθορίζουν τα δικαιώματα που έχουν οι χρήστες καθώς και οι ρόλοι των χρηστών (Role-based access control | RBAC) αποτελούν τα δύο βασικά στοιχεία που χρησιμοποιούνται στον έλεγχο πρόσβασης. Στο RBAC γίνεται ανάθεση ρόλων με σκοπό την απόκτηση αδειών χρήσης. Το περιεχόμενο κάθε εφαρμογής διαφοροποιεί ανάλογα τους ρόλους, οι οποίοι έχουν δυναμικό χαρακτήρα και μπορούν να τροποποιηθούν σε ένα πραγματικό σενάριο IoT. Υπάρχει όμως και ένα μειονέκτημα στις λίστες ελέγχου, το οποίο είναι ότι σε ένα IoT περιβάλλον που εμπεριέχει αρκετούς διαδραστικούς χρήστες, υστερεί στην απονομή των ελάχιστων δυνατών δικαιωμάτων ανά χρήστη [Sicari, 2014] [Roman, 2013].

- **Αξιοπιστία**

Εφαρμογές και υπηρεσίες, όπως για παράδειγμα στον τομέα της υγείας, μπορούν να θεωρηθούν ευάλωτες σε επιθέσεις κακόβουλων χρηστών. Στην περίπτωση που αυτές βασίζουν τη λειτουργία τους σε IoT συσκευές, θα πρέπει να θεωρούνται αξιόπιστες. Επίσης, η αξιοπιστία έχει σχέση με τη συχνότητα ανανέωσης των δεδομένων που στέλνονται, δηλαδή όταν στέλνονται λανθασμένα δεδομένα, είτε για δόλιο σκοπό είτε από σφάλμα, πιθανόν να οδηγήσουν σε μη επιθυμητές καταστάσεις. Τέλος, για να εξασφαλιστεί η αξιοπιστία σε μια IoT συσκευή, θα πρέπει να δημιουργηθεί ένας μηχανισμός «διαπραγμάτευσης εμπιστοσύνης» (trust negotiation), ο οποίος βασίζεται στην ανταλλαγή διαπιστευτηρίων με τη χρήση P2P (Peer-to-Peer), πριν επιτευχθεί η μετάδοση των δεδομένων [Alam, 2011].

4.2 Ασφάλεια στην αρχιτεκτονική του IoT

Σε ένα IoT περιβάλλον δεν υπάρχουν μόνο ζητήματα ασφαλείας αναφορικά με το διαδίκτυο, τα δίκτυα αισθητήρων ή τις κινητές επικοινωνίες, αλλά προκύπτουν και άλλα σημαντικά ζητήματα ασφαλείας που έχουν να κάνουν με την εξουσιοδότηση, την ιδιωτικότητα και την επεξεργασία ή την αποστολή των δεδομένων. Τα πρώτα στοιχεία που έρχονται σε επαφή με τις διάφορες πληροφορίες είναι τα δίκτυα ασύρματων αισθητήρων και τα RFID συστήματα. Έτσι, για να επιτύχουν την εμπιστευτικότητα και

την ακεραιότητα των δεδομένων, γίνεται χρήση τεχνικών, όπως είναι η κρυπτογράφηση και οι ψηφιακές υπογραφές. Η πολυπλοκότητα των δικτύων καθώς και η ύπαρξη διαφορετικών πρωτοκόλλων μεταφοράς δεδομένων στα δίκτυα που χρησιμοποιούνται σε ένα IoT σύστημα, δυσχεραίνουν την κατάσταση στον τομέα της ασφάλειας.

Θέματα αυθεντικοποίησης και εξουσιοδότησης συναντώνται στο επίπεδο των IoT εφαρμογών μιας και αυτό αφορά την καθημερινή ζωή των ανθρώπων. Για να γίνει πιο σαφές ο τομέας που θα διασφαλιστεί η αρχιτεκτονική του IoT μπορεί να κατηγοριοποιηθεί στα επίπεδα της αντίληψης, της μεταφοράς και των εφαρμογών. Στο επίπεδο της αντίληψης περιλαμβάνονται οι αισθητήρες και τα δίκτυα αισθητήρων. Στο επίπεδο μεταφοράς περιλαμβάνεται το δίκτυο πρόσβασης και τέλος, στο δίκτυο κορμού περιλαμβάνονται τα δίκτυα LAN, ενώ στο επίπεδο των εφαρμογών συναντώνται οι IoT πλατφόρμες και ό,τι έχει να κάνει με την υποστήριξή τους. Κάθε επίπεδο περιέχει διαφορετικές τεχνικές ασφάλειας.

4.2.1 Ασφάλεια στο επίπεδο της αντίληψης

Η συλλογή διάφορων δεδομένων επιτυγχάνεται στο επίπεδο της αντίληψης. Το συγκεκριμένο επίπεδο, μπορεί να χωριστεί σε δυο μεγάλες υποκατηγορίες, τους κόμβους, οι οποίοι αποτελούνται από αισθητήρες και ενεργοποιητές καθώς και το δίκτυο των κόμβων, το οποίο επικοινωνεί με το επίπεδο μεταφοράς. Το εν λόγω επίπεδο, περιλαμβάνει τεχνολογίες όπως είναι το RFID, το WSN και το RSN.

4.2.1.1 Ασφάλεια στα RFID

Στα IoT συστήματα χρησιμοποιείται ευρέως η τεχνολογία RFID με σκοπό να ταυτοποιεί αντικείμενα με ανέπαφο τρόπο. Η τεχνολογία αυτή όμως παρουσιάζει αρκετά προβλήματα ασφάλειας, θέτοντας σε κίνδυνο τα δεδομένα των χρηστών.

- Ενιαία κωδικοποίηση

Η διεθνής κοινότητα δεν έχει ορίσει κοινό πρότυπο που αφορά την κωδικοποίηση των RFID ετικετών, με αποτέλεσμα να χρησιμοποιούνται τα δύο ευρέως πιο γνωστά πρότυπα, το EPC και το UID (Unique Identifier). Επειδή δεν έχει οριστεί ένα κοινό πρότυπο, το οποίο θα χρησιμοποιούν οι χρήστες, αυτό εγείρει διάφορα ζητήματα, όπως για παράδειγμα τη δημιουργία λαθών κατά την ανάγνωση των ετικετών, ακόμα και αδυναμία στην ανάγνωση των ετικετών από τον αντίστοιχο μηχάνημα ανάγνωσης.

- Ταυτόχρονη αποστολή δεδομένων

Υπάρχει πιθανότητα κάποιες ετικέτες RFID να στέλνουν στον ίδιο χρόνο δεδομένα στους αναγνώστες, το οποίο έχει ως αποτέλεσμα τη δημιουργία προβλημάτων στη διαδικασία της ανάγνωσης και ως εκ τούτου δεν επιτυγχάνεται. Για να επιτευχθεί η επίλυση του παραπάνω προβλήματος είναι αναγκαία η χρήση τεχνικών κατά των συγκρούσεων των δεδομένων (anti-collision), τα οποία θα βάζουν σε σειρά τις πληροφορίες που μεταδίδονται. Τέλος, η ύπαρξη αλγορίθμων για την αποτροπή και την αλληλοεπικάλυψη των πληροφοριών των RFID ετικετών, πρέπει να προβλεφθεί.

4.2.1.2 Ασφάλεια στα ασύρματα δίκτυα αισθητήρων (WSN)

Τα ασύρματα δίκτυα αισθητήρων διαρθρώνονται σε μια δυναμική τοπολογία δικτύου και είναι κατανεμημένα δίκτυα πολλαπλών βημάτων μετάδοσης (multihop). Το γεγονός ότι υστερούν σε υπολογιστική ισχύ, χωρητικότητα και εμβέλεια, συμβαίνει λόγω του χαμηλού τους κόστος αγοράς και αυτό οδηγεί στο να προκύπτουν ζητήματα ασφάλειας. Η καταγραφή των δεδομένων που επιτυγχάνεται με τη χρήση των ασύρματων δικτύων αισθητήρων, ανήκουν στο τμήμα του επιπέδου αντίληψης. Οι πιθανοί κίνδυνοι που αντιμετωπίζουν τα δεδομένα των ασύρματων δικτύων αισθητήρων ενός IoT συστήματος είναι η πιθανή υποκλοπή πληροφοριών, η αλλοίωση του περιεχομένου τους και η παράνομη αναδρομολόγηση. Η εμπιστευτικότητα, η αυθεντικοποίηση, η ακεραιότητα και ο χρόνος ανανέωσης των δεδομένων (refresh rate) αποτελούν σημαντικά ζητήματα ασφάλειας. Τα προβλήματα αυτά μπορούν να λυθούν με τη χρήση κρυπτογραφικών αλγορίθμων, τη διαχείριση κλειδιών, την ασφαλή δρομολόγηση και την τήρηση της εμπιστευτικότητας στους κόμβους.

4.2.1.3 Το πρόβλημα της ετερογένειας

Ένα IoT περιβάλλον, συλλέγει έναν πολύ μεγάλο όγκο πληροφοριών με διαφορετικούς τρόπους και με διαφορετικά πρωτόκολλα αλλά και σε διαφορετικές μορφές (XML, JSON, Raw data), τα επεξεργάζεται και τελικά τα αποθηκεύει ή τα αποστέλλει σε άλλες συσκευές. Οι πληροφορίες που συλλέχθηκαν, θα πρέπει πρώτα να ακολουθούν το ίδιο πρότυπο και να έχουν ομοιογένεια μεταξύ τους και στη συνέχεια να είναι σε θέση να αναλυθούν με ευκολία. Κρίνοντας από τα παραπάνω, σοβαρά ζητήματα συμβατότητας έρχονται στην επιφάνεια, αναφορικά με τη μορφή των πληροφοριών αλλά και τα πρωτόκολλα επικοινωνίας διαμέσου των οποίων γίνεται ο διαμοιρασμός των δεδομένων. Με τη χρήση του κατάλληλου υλικού (hardware) και λογισμικού (software), τα οποία θα επιτυγχάνουν την κοινή κωδικοποίηση των δεδομένων, τα διάφορα δίκτυα

με διαφορετικές φιλοσοφίες, όπως τα RFID δίκτυα (RSN) ή τα δίκτυα αισθητήρων θα επιτύχουν τη λειτουργία τους με ομοιογένεια. Καταλήγοντας σε ένα συμπέρασμα, η ασφάλεια εξαρτάται από την πολυπλοκότητα στο επίπεδο αντίληψης στα IoT συστήματα, τα οποία αποτελούνται από κόμβους διάφορων αισθητήρων και από αισθητήρες RFID. Τα μεγαλύτερα όμως προβλήματα είναι η αδυναμία ύπαρξης επεξεργαστικής ισχύος καθώς και τα ζητήματα ετερογένειας στις IoT συσκευές. Επιπλέον, οι κόμβοι του IoT δικτύου θα πρέπει να αντιμετωπίζονται σε σχέση με τους τερματικούς σταθμούς και όχι μόνοι τους. Εγγύηση για την ασφάλεια σε ένα IoT σύστημα δεν αποτελούν οι προτεινόμενες λύσεις που αναφέρθηκαν, οι οποίες μπορούν να εξασφαλίσουν κάποια ασφάλεια στο επίπεδο της αντίληψης.

4.2.2 Ασφάλεια στο επίπεδο μεταφοράς

Το επίπεδο μεταφοράς είναι αυτό που εξασφαλίζει τη μετάδοση, την επεξεργασία και την αποθήκευση των δεδομένων και παρέχει στο επίπεδο αντίληψης ένα χώρο που μπορεί να μεταδώσει και να αποθηκεύσει πληροφορίες, ώστε να τις χρησιμοποιούν εφαρμογές ανώτερου επιπέδου. Αυτό οδηγεί το επίπεδο αντίληψης να ολοκληρώσει με επιτυχία τους στόχους του. Με βάση τις λειτουργίες του επιπέδου μεταφοράς, αυτό μπορεί να κατηγοριοποιηθεί σε τρεις υποκατηγορίες, το δίκτυο πρόσβασης, το δίκτυο κορμού καθώς και τα τοπικά δίκτυα. Το επίπεδο της μεταφοράς μπορεί να παρομοιαστεί ως ένα συνονθύλευμα από ετερογενή δίκτυα.

4.2.2.1 Δίκτυο πρόσβασης

Οι πληροφορίες που είναι συσσωρευμένες στο επίπεδο της αντίληψης, περνάνε πρώτα από το δίκτυο πρόσβασης, το οποίο είναι υπεύθυνο για τη διευθέτηση ζητημάτων ασφάλειας που δεν διευθετήθηκαν στο προηγούμενο επίπεδο. Τα ασύρματα δίκτυα Wi-Fi, τα δίκτυα ad hoc καθώς και κυψελωτά δίκτυα 3G/4G περιλαμβάνονται στα δίκτυα πρόσβασης, και μπορούν να χωριστούν σε δύο υποομάδες ανάλογα με τα δομικά στοιχεία τους. Η πρώτη υποομάδα αποτελείται από τα ασύρματα δίκτυα, όπως είναι τα ad hoc δίκτυα, τα οποία δεν απαιτούν την ύπαρξη κάποιου σταθμού βάσης, ενώ η δεύτερη υποομάδα αποτελείται από τα Wi-Fi και τα κυψελωτά δίκτυα, τα οποία απαιτούν την ύπαρξη ενός σταθμού βάσης.

❖ Ζητήματα ασφάλειας στα δίκτυα Wi-Fi

Τα πιο διαδεδομένα δίκτυα στον τομέα των ασύρματων επικοινωνιών είναι τα Wi-Fi, τα οποία στη βιβλιογραφία μπορούν να εμφανιστούν και ως IEEE802.11. Σε ένα

IoT περιβάλλον, σημαντικό ρόλο διαδραματίζει στα δίκτυα Wi-Fi η ασφάλεια. Κι αυτό συμβαίνει διότι διάφορες επιθέσεις έχουν αναφερθεί, όπως το phishing, οι επιθέσεις DoS και DDoS και πολλές άλλες, οι οποίες εκμεταλλεύονται ευπάθειες στα δίκτυα Wi-Fi και δημιουργούν προβλήματα ασφάλειας στις IoT συσκευές και τους χρήστες. Πιθανές λύσεις στα παραπάνω προβλήματα ασφάλειας μπορούν να προσφέρουν οι κρυπτογραφικοί αλγόριθμοι καθώς κι ο έλεγχος πρόσβασης στα Wi-Fi δίκτυα. Όσον αφορά τις κρυπτογραφικές μεθόδους που χρησιμοποιούνται, όπως τα πρωτόκολλα WPA/WPA2, εξασφαλίζουν την κρυπτογράφηση των δεδομένων που αποστέλλονται, καθώς και ότι μόνο ο παραλήπτης που κατέχει το κλειδί αποκρυπτογράφησης, είναι σε θέση να διαβάσει τα δεδομένα. Η παραπάνω τεχνική κρυπτογράφησης σε δίκτυα Wi-Fi, ακολουθεί το πρότυπο του κρυπτογραφικού αλγορίθμου AES και στηρίζεται στο πρωτόκολλο Temporal Key Integrity Protocol (TKIP). Τέλος, αναφορικά με τον έλεγχο πρόσβασης, η είσοδος των διαπιστευμένων χρηστών στο διαδίκτυο επιτυγχάνεται με τη χρήση πιστοποιητικών τύπου PPPoE.

❖ Ζητήματα ασφάλειας στα δίκτυα ad hoc

Ένα ασύρματο ad hoc δίκτυο χαρακτηρίζεται ως ένας τύπος ασύρματου δικτύου, ο οποίος είναι αποκεντρωμένος. Το δίκτυο αυτό ονομάζεται ad hoc διότι δε βασίζεται σε κάποια υποδομή που προϋπήρχε, όπως είναι οι δρομολογητές στα ενσύρματα δίκτυα ή τα ασύρματα access points στα διαχειριζόμενα ασύρματα δίκτυα. Αντίθετα, κάθε κόμβος συμμετέχει στη δρομολόγηση, προωθώντας τα δεδομένα προς τους άλλους κόμβους, κι έτσι ο καθορισμός του ποιοι κόμβοι προωθούν δεδομένα γίνεται δυναμικά με βάση τη συνδεσιμότητα του δικτύου. Γι’ αυτό το λόγο, τέτοια δίκτυα συναντώνται και σε IoT περιβάλλοντα. Πέρα όμως από την κλασική δρομολόγηση, τα ad hoc δίκτυα δύναται να χρησιμοποιούν την υπερχείλιση με σκοπό την προώθηση των δεδομένων [Wikipedia, 2018]. Τα ασύρματα κανάλια επικοινωνίας ενός ad hoc δικτύου είναι συνήθως στόχος κακόβουλων χρηστών για να επιτύχουν υποκλοπές δεδομένων. Η ασφάλεια σε ad hoc δίκτυα, σε ένα IoT οικοσύστημα, μπορεί να αφορά τους εξής τομείς, τους κόμβους, τη δρομολόγηση και τα δεδομένα αυτά καθαυτά.

Στο επίπεδο των κόμβων, για να επιτευχθεί η ασφάλεια των δεδομένων αλλά και να εξαλειφθεί οποιαδήποτε κακόβουλη επικοινωνία, θα πρέπει να υπάρχει ταυτοποίηση του κάθε κόμβου με όλους όσους επικοινωνεί. Αν δεν πραγματοποιηθεί η παραπάνω ταυτοποίηση, μη νόμιμοι χρήστες θα είχαν πρόσβαση σε μεταδιδόμενα δεδομένα, εξαιτίας της μη εξουσιοδοτημένη κυριότητα ενός κόμβου. Σχετικά με τη δρομολόγηση

σε ad hoc δίκτυα, μια τεχνική που εφαρμόζεται για να αποφευχθούν επιθέσεις τύπου DDoS/DoS είναι η κρυπτογραφία. Τέλος, σε ότι έχει να κάνει με τα δεδομένα στα ad hoc δίκτυα, θα πρέπει να χρησιμοποιηθούν μηχανισμοί διαχείρισης κλειδιού με σκοπό την αποφυγή διαρροών και αλλοιώσεων των δεδομένων.

- Ζητήματα Ασφαλείας στα κυψελωτά δίκτυα 3G/4G

Σε IoT οικοσυστήματα, τα οποία χρησιμοποιούν τα κυψελωτά δίκτυα 3G/4G ως μέσο πρόσβασης, δημιουργούνται σοβαρά προβλήματα που αφορούν τη διαρροή δεδομένων των χρηστών του καθώς και την απώλεια πακέτων δεδομένων. Η χρήση τεχνικών αυθεντικοποίησης καθώς και τεχνικών κρυπτογράφησης δύναται να βελτιώσουν σημαντικά τα παραπάνω προβλήματα. Επιπρόσθετα, η χρήση καρτών SIM από το κυψελωτά δίκτυα στις συσκευές IoT, δίνει τη δυνατότητα στο χρήστη να επαληθεύει την ταυτότητα του. Η χρήση των παραπάνω διαπιστευτηρίων, όπως οι πληροφορίες ταυτοποίησης και οι κωδικοί πρόσβασης δύναται να προάγουν τη νομιμότητα της επικοινωνίας τους.

4.2.2.2 Δίκτυο κορμού

Η μετάδοση των δεδομένων σε ένα IoT οικοσύστημα επιτυγχάνεται χάρη στο δίκτυο κορμού, το οποίο μπορεί να ταυτιστεί με το διαδίκτυο, μιας και αυτό είναι το μέσο το οποίο μεταδίδει τα δεδομένα σε κάθε ενδιαφερόμενο. Αυτό έχει ως αποτέλεσμα, τα ζητήματα ασφάλειας που εντοπίζονται στο διαδίκτυο, να «κληρονομούνται» και από το δίκτυο κορμού του IoT. Τα τελευταία χρόνια, η αυξανόμενη χρήση IoT συσκευών και γενικότερα συσκευών που συνδέονται στο διαδίκτυο και άρα χρησιμοποιούν IP διευθύνσεις, εξάντλησαν το εύρος διευθύνσεων που ακολουθεί το πρωτόκολλο IPv4. Αυτό είχε ως αποτέλεσμα τη δημιουργία και χρήση του πρωτοκόλλου IPv6. Οι τεχνολογίες που χρησιμοποιούνται με το πρωτόκολλο αυτό, όπως για παράδειγμα η 6LoWPAN, υιοθετούν τη χρήση του κατακερματισμού (hash), την επανασυναρμολόγηση των πακέτων, τη συμπίεση καθώς και την ανάθεση διευθύνσεων στις κεφαλίδες (header).

4.2.2.3 Τοπικά δίκτυα περιοχής

Σε επίπεδο τοπικού δικτύου περιοχής (LAN), θα πρέπει να προβλεφθούν οι διαρροές δεδομένων καθώς και η προστασία των διακομιστών, στα πλαίσια της IoT τεχνολογίας. Για την αποφυγή οποιασδήποτε ανεπιθύμητης κατάστασης, κρίνεται σκόπιμο ο έλεγχος πρόσβασης στον δίκτυο να είναι απαραβίαστος χαρακτηριστικό.

Ακόμη, για να διασφαλιστεί η προστασία του συστήματος σε ικανοποιητικό βαθμό, θα πρέπει να γίνουν ορισμένες ενέργειες. Πρώτα απ' όλα, θα πρέπει να γίνει σάρωση και στη συνέχεια να απομακρυνθεί οποιοδήποτε κακόβουλο λογισμικό επηρεάζει το δίκτυο και στη συνέχεια να καλυφθούν τα όποια κενά ασφαλείας εντοπιστούν στις υπηρεσίες του. Επιπλέον, η χρήση λειτουργικών συστημάτων τα οποία ενημερώνονται σε τακτά χρονικά διαστήματα σχετικά με κενά ασφαλείας και ελαττώματα στη χρήση, καθώς και η χρήση ισχυρών κωδικών πρόσβασης, μπορούν να χαρακτηριστούν ως σημαντικά και αναγκαία μέτρα για να είναι ασφαλές ένα IoT σύστημα σε επίπεδο τοπικό δίκτυο περιοχής.

Το επίπεδο μεταφοράς είναι πολύ σημαντικό από τη σκοπιά της ασφάλειας, επειδή μπορεί να τοποθετηθεί στο ενδιάμεσο των συστημάτων IoT. Τα ζητήματα ασφάλειας που προκύπτουν σε αυτό το επίπεδο, σχετίζονται με τα διαφορετικά και ετερογενή δίκτυα που το απαρτίζουν, όπως τα 3G, 4G, Bluetooth δίκτυα. Για να ξεπεραστούν τα παραπάνω ζητήματα, μπορούν να χρησιμοποιηθούν ορισμένες τεχνικές, όπως για παράδειγμα η tight coupling ή η loose coupling. Έπειτα, η πιο διαδεδομένη μορφή επίθεσης στο επίπεδο αυτό είναι αυτή της άρνησης πρόσβασης (DDoS). Τέλος, εκτός των παραπάνω ζητημάτων, το επίπεδο μεταφοράς σε IoT συστήματα είναι ευάλωτο και σε άλλων ειδών επιθέσεις, όπως είναι η κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS), τα Trojans και οι διαφόρων τύπων ιοί. Για να αντιμετωπιστούν αυτά τα θέματα ασφάλειας, οι υπεύθυνοι ασφαλείας πρέπει να χρησιμοποιούν συστήματα ανίχνευσης και πρόληψης των επιθέσεων αυτών καθώς και μηχανισμούς αυθεντικοποίησης και ανίχνευσης.

4.2.3 Ασφάλεια στο επίπεδο εφαρμογών

Ένα επίπεδο υψηλότερα από το επίπεδο μεταφοράς, μπορεί να τοποθετηθεί το επίπεδο υποστήριξης των εφαρμογών, το οποίο είναι σε θέση να επεξεργαστεί τα δεδομένα που λαμβάνει, να πραγματοποιεί υπολογισμούς όπως και να προσφέρει κατά τη διαδικασία λήψης αποφάσεων. Μια επιπλέον λειτουργία στο επίπεδο εφαρμογής είναι η αναγνώριση και το φιλτράρισμα κακόβουλης πληροφορίας, που πιθανότατα θα περάσει από το επίπεδο αυτό. Γενικότερα, το επίπεδο των εφαρμογών μπορεί να κατηγοριοποιηθεί σε διαφορετικές κατηγορίες, σε συνάρτηση με τις λειτουργίες που εκτελούνται, όπως για παράδειγμα την επικοινωνία Machine-to-Machine (M2M), το υπολογιστικό νέφος (cloud) και το ενδιάμεσο λογισμικό (middleware).

Σε ένα IoT περιβάλλον, όπου βασικό ρόλο διαδραματίζουν οι M2M επικοινωνίες, που επιτυγχάνονται είτε με τη χρήση καλωδίων είτε με τη χρήση ασύρματων (Wi-Fi/Bluetooth) ή κυψελωτών δικτύων (3G/4G), ελλοχεύουν κίνδυνοι για την ασφάλεια των δεδομένων. Σε αυτό το επίπεδο, σημαντικά ζητήματα αποτελούν η αξιοπιστία, η ιδιωτικότητα, η ακεραιότητα, η εξουσιοδότηση, η αυθεντικοποίηση και η διαθεσιμότητα των δεδομένων, γι' αυτό το λόγο γίνονται προσπάθειες έρευνας πάνω σε διάφορες τεχνικές που επιτυγχάνουν την ανωνυμία των δεδομένων. Τέτοιες τεχνικές μπορούν να είναι το μοντέλο που διαφυλάσσει ευαίσθητα δεδομένα (k-anonymity algorithm), η χρήση τυχαιοποιημένων δεδομένων καθώς και η δημιουργία νέων κλειδιών αυθεντικοποίησης. Τέλος, σημαντικό ρόλο στην ασφάλεια των δεδομένων αποτελεί η θέσπιση κανόνων και μέτρων από την Πολιτεία, για την απώλεια και τη διαρροή ευαίσθητων δεδομένων, όταν ένας χρήστης αποφασίσει να αλλάξει πάροχο υπηρεσιών διαδικτύου.

Σημαντικοί κίνδυνοι ελλοχεύουν σε επίπεδο ασφάλειας των πληροφοριών, ακόμα και όταν τα δεδομένα επεξεργάζονται εκτός της IoT συσκευής και με τη βοήθεια του cloud. Πιο συγκεκριμένα, τέτοιοι κίνδυνοι μπορεί να είναι μια πιθανή απομόνωση πληροφοριών, ο κατακερματισμός των πακέτων που αποτελούν τα δεδομένα, όπως και προβλήματα στην πρόσβαση στην πλατφόρμα που τα επεξεργάστηκε τα δεδομένα και κατ' επέκταση στην ανάκτηση τους. Πολλές φορές, οι πλατφόρμες του cloud γίνονται στόχοι κακόβουλων επιθέσεων, με αποτέλεσμα να βρίσκονται σε κίνδυνο κρίσιμα και ευαίσθητα δεδομένα μεγάλων εταιριών. Παράδειγμα αποτελούν εταιρίες και οργανισμοί, όπως νοσοκομεία ή χρηματιστηριακές εταιρίες, οι οποίες είναι αντίθετες με τη χρήση του cloud για την αποθήκευση ή την επεξεργασία των δεδομένων που κατέχουν. Ένα είδος κακόβουλων επιθέσεων σε υπολογιστικά νέφη, είναι η κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS), η οποία δύναται να προκαλέσει ασυνέχεια στην αποστολή και λήψη πακέτων δεδομένων, δεν επιτρέπει την πρόσβαση σε αποθηκευμένα δεδομένα του συστήματος και προκαλεί ακόμα και τον τερματισμό της λειτουργίας του συστήματος-στόχου. Ένα δεύτερο είδος ευπάθειας σε συστήματα cloud, είναι η δυνατότητα που δίνει στον χρήστη να έχει πρόσβαση σε αυτό από οποιοδήποτε σημείο του κόσμου και χρησιμοποιώντας οποιοδήποτε μέσο (PC, laptop, smartphone). Γι' αυτό το λόγο, ένα τέτοιο σύστημα, όπως είναι το υπολογιστικό νέφος, θα πρέπει να δίνει πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες του, με τη χρήση διαπιστευτηρίων εξακρίβωσης της ταυτότητας, μιας και στην περίπτωση μιας παραβίασης από μη

εξουσιοδοτημένο χρήστη, καθίσταται δύσκολη η ανίχνευση των ηλεκτρονικών αποτυπωμάτων του.

Με απλά λόγια, το ενδιάμεσο λογισμικό είναι ένας ευρύς όρος, ο οποίος καλύπτει όλα τα κατανεμημένα λογισμικά που χρειάζονται για την υποστήριξη της συνεργασίας πελατών και διακομιστών. Στην περίπτωση ενός IoT συστήματος, το middleware θα πρέπει να χειριστεί έναν μεγάλο και δυναμικό όγκο δεδομένων, με αποτέλεσμα να πρέπει να διαθέτει ικανό μέγεθος αποθηκευτικού χώρου και η χωρητικότητα του αυτή να είναι γραμμικά επεκτάσιμη. Εκτός από το παραπάνω, το middleware είναι υπεύθυνο για την διαχείριση των εισερχόμενων αιτημάτων, τα οποία παραμένουν ενεργά για συγκεκριμένο χρόνο και δύναται να φτάσουν περισσότερα του ενός, ταυτόχρονα. Επομένως, βασική προϋπόθεση του middleware είναι η εισαγωγή τεχνικών που θα ορίζουν σειρά προτεραιότητας κατά την επεξεργασία των αιτημάτων, για να μην απαιτείται η χρήση μηχανισμών αναμονής για τα επείγοντα αιτήματα.

4.3 Επιθέσεις - τρόποι προστασίας στους έξυπνους μετρητές

Υπάρχουν πολλές απειλές που αντιμετωπίζουν οι συσκευές και κατά επέκταση οι χρήστες της τεχνολογίας του IoT. Για παράδειγμα, σε ένα έξυπνο δίκτυο ηλεκτρικής ενέργειας, μπορούν να συμβούν επιθέσεις και αλλοιώσεις των δεδομένων, συμπεριλαμβανομένης της παραβίασης της ιδιωτικής ζωής μέσω της κλοπής δεδομένων, της κλοπής ηλεκτρικού ρεύματος, της διακοπής των υπηρεσιών, της υλικής ζημίας στις συσκευές, της άρνησης παροχής υπηρεσιών και της απάτης στην αγορά . Η πειρατεία σε έξυπνες μετρήσεις, η παραβίαση της ασύρματης επικοινωνίας ή η υποκλοπή των δεδομένων από τους servers, μπορεί να παρέχει λεπτομερείς μετρήσεις πληροφοριών για τα προσωπικά δεδομένα των χρηστών. Αυτές οι πληροφορίες είναι επίσης απαραίτητες για τη χρέωση της υπηρεσίας, αλλά και για την ανταπόκριση στη ζήτηση και τη πρόβλεψη του φορτίου στο έξυπνο δίκτυο [Ghansah, 2012].

Υποκλοπή στην περίπτωση των έξυπνων δικτύων ηλεκτρικής ενέργειας θεωρείται η κατάσταση κατά την οποία ένας εισβολέας κλέβει ή συγκεντρώνει δεδομένα που προορίζονται για ένα έξυπνο δίκτυο. Σε αυτήν την επίθεση, ο εισβολέας συνδέει το σήμα μετάδοσης μεταξύ της πηγής δεδομένων όπως για παράδειγμα, ενός αισθητήρα κατοικίας, και του κέντρου ελέγχου του έξυπνου δικτύου. Ο εισβολέας μπορεί με κατάλληλο ειδικό λογισμικό να παρεμβαίνει μεταξύ της επικοινωνίας δεδομένων και του χρόνου αποκωδικοποίησής τους. Αυτό μπορεί να επιβραδύνει την υποκλοπή, αλλά

ορισμένοι επιτιθέμενοι θα μπορούσαν να έχουν πρόσβαση στους κοινούς αλγόριθμους αποκωδικοποίησης και με αρκετές δοκιμές να αποκαλύψουν και να κατανοήσουν τον τρόπο ανάγνωσης των δεδομένων [Li, 2012] [Zhao, 2018].

Υπάρχουν διάφορες καταστροφικές συνέπειες από τις επιθέσεις των κακόβουλων χρηστών στον τομέα αυτό. Για παράδειγμα, διάφοροι επιτήδειοι, όπως πάροχοι, εταιρείες, καθώς και κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες για διαφορετικούς σκοπούς. Οι εταιρείες μάρκετινγκ θα μπορούσαν να χρησιμοποιήσουν αυτές τις πληροφορίες για στοχευμένο μάρκετινγκ ή για την εισαγωγή μη ανταγωνιστικών τιμών. Οι επιτήδειοι μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να παρακολουθήσουν την καθημερινή δραστηριότητα μιας οικογένειας, προγραμματίζοντας έτσι τη διάπραξη αξιόποινων πράξεων (διάρρηξη ή άλλα εγκλήματα). Επίσης, κακόβουλοι χρήστες στοχεύουν στην κλοπή ηλεκτρικής ενέργειας, μεταβάλλοντας την ένδειξη του μετρητή είτε με παραβίαση του μετρητή είτε με αλλαγή των πληροφοριών μετά από την αποκωδικοποίηση του κλειδιού κρυπτογράφησης.

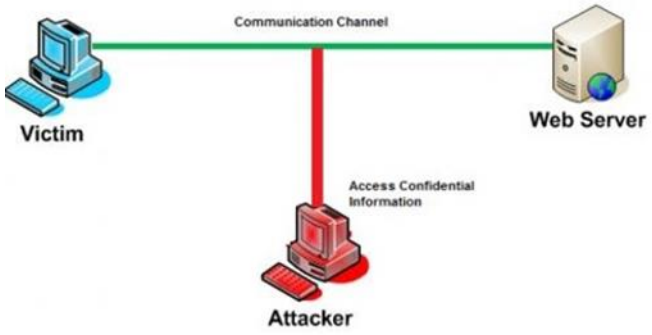
Τέλος, είναι πιθανό να συμβούν δυσλειτουργίες στο δίκτυο, να υπάρξουν λανθασμένες μετρήσεις κατανάλωσης ενέργειας καθώς και διακοπή της λειτουργίας των έξυπνων δικτύων εφόσον ο κακόβουλος χρήστης καταφέρει να εκμεταλλευτεί τις ευπάθειες και να αποκτήσει πρόσβαση στο σύστημα των έξυπνων μετρητών [Kim, 2013].

4.3.1 Τύποι επιθέσεων

Αρκετοί ερευνητές έχουν εντοπίσει διάφορους τύπους επιθέσεων που θα μπορούσαν να απειλήσουν τις λειτουργίες ενός έξυπνου δικτύου. Ένας αναλυτικός κατάλογος αυτών των επιθέσεων παρέχεται από τον Πίνακας 1 και περιλαμβάνει κάθε πιθανή ευπάθεια ασφάλειας σε ένα οικοσύστημα IoT, αναλύοντας πιθανούς τρόπους επιθέσεων σε κάθε επίπεδο (Application layer, Transport layer κτλ). Επιπρόσθετα, παρουσιάζονται ορισμένοι από τους σημαντικότερους τύπους επιθέσεων που συναντώνται πιο συχνά.

Ένας από τους πιο συνηθισμένους τύπους επιθέσεων στα κανάλια επικοινωνίας είναι η επίθεση Eavesdropping. Εφόσον ο επιτιθέμενος έχει αποκτήσει πρόσβαση στο κανάλι επικοινωνίας, μπορεί να παρακολουθεί τα πακέτα που ανταλλάσσονται μεταξύ του αποστολέα και του παραλήπτη. Ο επιτιθέμενος θα είναι σε θέση να γνωρίζει προσωπικά δεδομένα καταναλωτών καθώς και την ενεργειακή τους συμπεριφορά,

παρακολουθώντας απλά την δικτυακή κίνηση, χωρίς να χρειάζεται να επεμβαίνει σε αυτήν. Οι επιθέσεις αυτού του τύπου εξελίσσονται συνεχώς, μιας και υπάρχουν σημαντικά οικονομικά και πολιτικά κίνητρα από αυτούς που εκμεταλλεύονται τα προσωπικά δεδομένα καταναλωτών, με απώτερο σκοπό το κέρδος [Yilin, 2012].

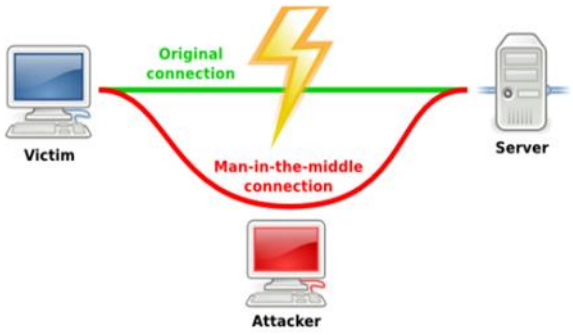


Εικόνα 3 – Τυπική επίθεση eavesdropping

Η επίθεση man-in-the-middle είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος χρήστης ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να τροποποιήσει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. Σε αντίθεση με την επίθεση eavesdropping, οι επιθέσεις αυτού του τύπου, δεν υποκλέπτουν απλώς τη δικτυακή κίνηση στο κανάλι επικοινωνίας, αλλά την παραποιούν. Συνήθως, τρείς τύποι δεδομένων είναι αυτοί, που είναι περισσότερο επιρρεπείς σε τέτοιου είδους επιθέσεις: [Yilin, 2012]

- **Δεδομένα μετρήσεων κατανάλωσης**: Η παραποίηση αυτών των δεδομένων, όπως στην περίπτωση των έξυπνων μετρητών, δίνει μια εσφαλμένη εικόνα της κατάστασης του δικτύου στο διαχειριστή, αναγκάζοντάς τον να λαμβάνει λανθασμένες αποφάσεις σχετικά με την απαιτούμενη παραγόμενη ενέργεια. Το πρόβλημα αυτό εντείνεται, όταν τροποποιούνται δεδομένα μετρητών μιας ευρείας περιοχής, όπως για παράδειγμα κατά την αποστολή τους από το συναθροιστή του συστήματος AMI (Advanced Metering Infrastructure) στο σύστημα διαχείρισης δεδομένων (MDMS), οπότε και θα υπάρχουν σημαντικές διαφοροποιήσεις ανάμεσα στην πραγματική ζήτηση και σε αυτή που αντιλαμβάνεται το κέντρο ελέγχου.

- **Παραποίηση σημάτων τιμής:** Η παραποίηση σημάτων τιμής, όπως για παράδειγμα η λήψη από τους μετρητές ενός σήματος αρνητικής τιμής, το οποίο έχει παραποιηθεί στο κανάλι επικοινωνίας, θα έχει ως αποτέλεσμα την ενεργοποίηση όλων των συσκευών μιας κατοικίας, λόγω της χαμηλής τιμής της παραγόμενης ενέργειας, με αποτέλεσμα μια μη αναμενόμενη και ανεπιθύμητη αύξηση του φορτίου αιχμής.
- **Παραποίηση εντολών:** Οι εντολές, οι οποίες αποστέλλονται από το κέντρο ελέγχου στους μετρητές, μπορούν να παραποιηθούν από κάποιον που παρακολουθεί το κανάλι επικοινωνίας. Συγκεκριμένα, μπορεί να τροποποιήσει την εντολή που αποστέλλεται από το κέντρο, ώστε να αναγκάσει το μετρητή να αποσυνδεθεί, διακόπτοντας την παροχή ισχύος στην κατοικία.



Εικόνα 4 - Τυπική επίθεση man-in-the-middle

Spoofing υπηρεσιών (data spoofing)

Με τον όρο «spoofing» εννοούμε την κατάσταση κατά την οποία κάποιος εισβολέας προσποιείται ότι είναι κάποιος νόμιμος χρήστης με σκοπό την απόκτηση της πρόσβασης σε κάποιο υπολογιστικό σύστημα, ώστε να περιορίσει τους πόρους ή να υποκλέψει χρήσιμες πληροφορίες. Στο επίπεδο του δικτύου ηλεκτρικής ενέργειας, τα δεδομένα από απομακρυσμένες τερματικές μονάδες (Remote Terminal Units), αισθητήρες (sensors) και έξυπνους μετρητές μεταδίδονται στο κέντρο ελέγχου για την περαιτέρω επεξεργασία τους. Αν κάποιος εισβολέας πραγματοποιήσει επίθεση σε μία συσκευή αλλά ταυτόχρονα τροποποιήσει τα συλλεγόμενα δεδομένα που προέρχονται από αυτήν, τότε ο χειριστής θα αντιλαμβανόταν μία ομαλή λειτουργία στο δίκτυο και έτσι η επίθεση θα ήταν απαρατήρητη. Με άλλα λόγια, κατά την διάρκεια μιας επίθεσης «spoofing», ο εισβολέας μπορεί να συνεχίσει να στέλνει εντολές σε κάποια συσκευή ή κάποιον ελεγκτή, με σκοπό να προκαλέσει μία κακόβουλη ενέργεια, ενώ ο χειριστής θα

εξακολουθούσε να μην γνωρίζει την πραγματική κατάσταση του συστήματος [Zhang, 2015].

Επίθεση επανάληψης (replay attack)

Στην περίπτωση αυτή, ο κακόβουλος χρήστης μπορεί να αναπαράγει κάποια μηνύματα, τα οποία έχει λάβει προηγουμένως, από το κανάλι επικοινωνίας που παρακολουθεί, με σκοπό την αποστολή τους, είτε στο κέντρο ελέγχου είτε στο μετρητή, ανάλογα με τον αποστολέα του πακέτου. Η αναπαραγωγή αυτών των μηνυμάτων, είτε πρόκειται για μετρήσεις ηλεκτρικής ενέργειας, είτε σημάτων τιμής, μετά από κάποιο χρονικό διάστημα από την πραγματική τους αποστολή, είναι σε θέση να δημιουργήσει σημαντικό πρόβλημα στην ευστάθεια της λειτουργίας του δικτύου [Yilin, 2012].

Cross-Site Scripting (XSS)

Κατά τη χρήση της Cross-Site Scripting ευπάθειας που χρησιμοποιεί ένας κακόβουλος χρήστης, μπορεί με ευκολία να στείλει scripts (δέσμες ενεργειών) τα οποία είναι κείμενα που εκμεταλλεύονται τον διερμηνέα του περιηγητή. Με αυτό τον τρόπο, ο κακόβουλος χρήστης είναι σε θέση να αλλοιώσει δεδομένα που βρίσκονται στη βάση δεδομένων αλλά και άλλων εσωτερικών πηγών. Οι επιθέσεις αυτού του είδους, μπορούν να πραγματοποιηθούν είτε από χρήστες που βρίσκονται εντός ενός τοπικού δικτύου, συμπεριλαμβανομένου του διαχειριστής, είτε από οποιοσδήποτε χρήστης εκτός του δικτύου αυτού. Αυτό που ουσιαστικά επιτυγχάνει ο κακόβουλος χρήστης είναι να στείλει μη έμπιστα δεδομένα στο σύστημα εκμεταλλευόμενος το κενό ασφαλείας Cross-Site Scripting, το οποίο είναι εύκολα ανιχνεύσιμο και πολύ διαδεδομένο στους κόλπους των κακόβουλων χρηστών. Σφάλματα που οφείλονται στο XSS, μπορούν να συμβούν όταν τα δεδομένα του χρήστη που περιλαμβάνονται σε μια ιστοσελίδα, μέσω μιας εφαρμογής στέλνονται στον περιηγητή, δεν είναι σωστά επικυρωμένα ή κωδικοποιημένα (escaped content) [Barcena, 2015].

IoT Asset	Threat
IoT Devices	- Malware - Exploit Kits - DDoS

	- Counterfeit by malicious devices - Privacy exposure - Modification of information
	- Man-in-the-middle - IoT communication protocol hijacking - Interception of information - Network reconnaissance - Session hijacking - Information gathering - Replay of messages
	- Power outage - Failures of devices - Failure of system - Loss of support services
	- Data / Sensitive information leakage
	- Software vulnerabilities - Third parties' failures
	- Natural Disaster
	- Device modification - Device destruction (sabotage)
IoT Ecosystem Interface/Management Devices	- Malware - Exploit Kits - DDoS - Counterfeit by malicious devices - Privacy exposure - Modification of information
	- Power outage - Failure of system - Loss of support services
	- Data / Sensitive information leakage
	- Software vulnerabilities - Third parties' failures
	- Natural Disaster - Environmental Disaster
	- Device destruction (sabotage)
Communications	- Man-in-the-middle - IoT communication protocol

	hijacking - Interception of information - Network reconnaissance - Session hijacking - Information gathering
	- Network Outage - Loss of support services
	- Device modification
Infrastructure	- Exploit Kits - Targeted attacks - DDoS - Counterfeit by malicious devices
	- Network reconnaissance
	- Network Outage - Loss of support services
	- Software vulnerabilities - Third parties' failures
	- Natural Disaster - Environmental Disaster
	- Device destruction (sabotage)
Platform & Backend	- Malware - Targeted attacks - DDoS - Privacy exposure - Modification of information
	- Failure of system - Loss of support services
	- Data / Sensitive information leakage
	- Software vulnerabilities - Third parties' failures
	- Natural Disaster - Environmental Disaster
	- Device destruction (sabotage)
Decision making & Support	- IoT communication protocol hijacking - Replay of messages
	- Loss of support services
Applications & Services	- Software vulnerabilities

	- Third parties' failures
	- Loss of support services
Information	- Targeted attacks - Privacy exposure - Modification of information
	- Man-in-the-middle - IoT communication protocol hijacking - Interception of information - Network reconnaissance - Session hijacking - Information gathering - Replay of messages
	- Loss of support services
	- Data / Sensitive information leakage

Πίνακας 1 - Απειλές σε IoT οικοσυστήματα

4.3.2 Μηχανισμοί προστασίας

Σε ένα εκτενές και πολύπλοκο δίκτυο, όπως είναι το Smart Grid, οι μηχανισμοί ασφαλείας που υλοποιούνται στα συνηθισμένα δίκτυα υπολογιστών, δεν επαρκούν για να αντιμετωπίσουν τις επιθέσεις που γίνονται σε αυτό. Στο έξυπνο δίκτυο, οι μηχανισμοί ασφαλείας εστιάζουν στον αντίκτυπο που έχουν οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές του, όπως οι υποσταθμοί και το δίκτυο διανομής. Για το λόγο αυτό, η ασφάλεια στο έξυπνο δίκτυο αναφέρεται συνήθως ως Cyber-Physical Security (CPS) [Yilin, 2012]. Οι μηχανισμοί CPS που χρησιμοποιούνται για την έγκαιρη ανίχνευση σφαλμάτων και βλαβών από τέτοιες επιθέσεις στο έξυπνο δίκτυο και τις υποδομές του, καθώς και για την άμεση αντιμετώπισή τους είναι:

Κρυπτογράφηση Δημοσίου Κλειδιού (PKI)

Η κρυπτογράφηση του δημοσίου κλειδιού (public key cryptography – PKI) είναι μια τεχνική, η οποία μπορεί να εξασφαλίσει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, όταν αυτά διακινούνται σε κανάλια επικοινωνίας. Στην τεχνική αυτή, το κέντρο ελέγχου και ο μετρητής δημιουργούν από ένα ζεύγος κλειδιών κρυπτογράφησης,

με το δημόσιο κλειδί να αποστέλλεται στην οντότητα με την οποία ανταλλάσσουν πληροφορίες και δεδομένα. Κατά την αποστολή ενός πακέτου σε έναν έξυπνο μετρητή, το κέντρο ελέγχου κρυπτογραφεί το περιεχόμενο του πακέτου με το ιδιωτικό κλειδί και στη συνέχεια, εφόσον το λάβει ο μετρητής, μπορεί να το αποκρυπτογραφήσει μέσω του δημόσιου κλειδιού του κέντρου ελέγχου. Με αυτό τον τρόπο, μπορεί να γνωρίζει ο μετρητής ότι η πληροφορία προήλθε όντως από το κέντρο ελέγχου, ωστόσο δεν εξασφαλίζεται η ακεραιότητα των δεδομένων, μιας και οποιοσδήποτε έχει το δημόσιο κλειδί του κέντρου ελέγχου, μπορεί να διαβάσει και να τροποποιήσει το περιεχόμενο του πακέτου.

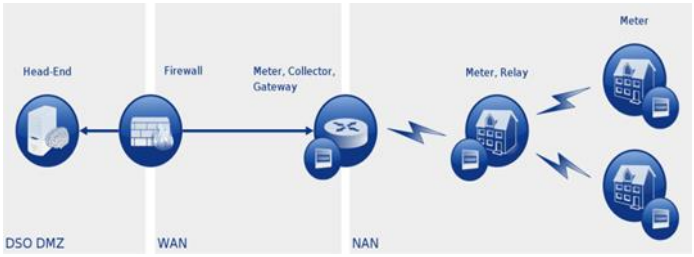
Εναλλακτικά, εφόσον έχει ήδη κρυπτογραφηθεί η πληροφορία από το κέντρο ελέγχου, το κρυπτογραφημένο μήνυμα κρυπτογραφείται εκ νέου με το δημόσιο κλειδί του εκάστοτε έξυπνου μετρητή. Στην περίπτωση αυτή, μόνο ο συγκεκριμένος μετρητής μπορεί να αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό κλειδί του, και στη συνέχεια με το δημόσιο κλειδί του κέντρου ελέγχου, εξασφαλίζοντας και την ακεραιότητα των δεδομένων που διακινούνται και στις δύο περιπτώσεις. Η ανταλλαγή των κλειδιών μπορεί να γίνει διαμέσου ενός ασφαλούς καναλιού επικοινωνίας για να αποφευχθούν επιθέσεις eavesdropping ή man-in-the-middle, που διακινδυνεύουν την εμπιστευτικότητα των κλειδιών.

Η κρυπτογράφηση δημοσίου κλειδιού, παρόλα τα πλεονεκτήματά της, προϋποθέτει οι έξυπνοι μετρητές να έχουν επαρκή μνήμη και υπολογιστική ισχύ για την κρυπτογράφηση των δεδομένων. Αυτό όμως αυξάνει σημαντικά το κόστος τους, μιας και θα κληθούν να επιβαρυνθούν οι καταναλωτές με αυτό, οπότε μπορεί να λειτουργήσει ως τροχοπέδη στην υιοθέτηση του έξυπνου δικτύου. Αλλά και το κέντρο ελέγχου καλείται να διαχειριστεί έναν τεράστιο αριθμό από κλειδιά κρυπτογράφησης, όχι μόνο από τους μετρητές, αλλά και από τους υποσταθμούς, τα RTUs και τις άλλες υποδομές του δικτύου. Η διαχείριση όλων αυτών των κλειδιών, εισάγει σημαντικό λειτουργικό κόστος για το έξυπνο δίκτυο [Baumeister, 2011] [Griffin, 2017].

Τείχος Προστασίας (Firewall)

Τα firewalls αποτελούν ίσως την πιο συνηθισμένη τεχνική προστασίας στα επιμέρους δίκτυα του Smart Grid. Η βασική τους λειτουργία είναι να ελέγχουν τη δικτυακή κίνηση στη συσκευή που προστατεύουν, ώστε να απορρίπτουν κάποια πακέτα, τα οποία φαίνονται ύποπτα ή δεν ικανοποιούν τις προϋποθέσεις προστασίας, που έχει

θέσει ο χρήστης. Είναι αρκετά αποδοτική μέθοδος προστασίας, και συνήθως τοποθετούνται στους δρομολογητές των επιμέρους δικτύων αλλά και στο κεντρικό σύστημα συλλογής δεδομένων, μιας και είναι το πλέον ευπαθές σημείο του έξυπνου δικτύου και αυτό που εκμεταλλεύονται συνήθως οι κακόβουλοι χρήστες, για την πραγματοποίηση επιθέσεων [Yan, 2011].



Εικόνα 5 - Τοποθέτηση Firewall στο Meter Data Management System

Τεχνικές Αυθεντικοποίησης

Πέρα από την κρυπτογραφία δημοσίου κλειδιού, η οποία μπορεί να προστατέψει την ιδιωτικότητα των δεδομένων που διακινούνται στο δίκτυο επικοινωνίας, απαραίτητη είναι και η χρήση κάποιων τεχνικών αυθεντικοποίησης στο σύστημα M.D.M.S.. Σωστή παραχώρηση προνομίων στις βάσεις δεδομένων του συστήματος επαρκεί, ώστε τα δεδομένα των καταναλωτών να είναι ορατά και επεξεργάσιμα μόνο από μια μικρή ομάδα εξουσιοδοτημένων χρηστών. Με αυτό τον τρόπο θα απορρίπτονται ερωτήματα στη βάση δεδομένων, τα οποία έχουν σκοπό να εκμεταλλευθούν ευαίσθητες πληροφορίες.

Αυτοματοποιημένες λύσεις λογισμικού (DSS)

Εκτός από τις παραπάνω τεχνικές προστασίας των IoT οικοσυστημάτων από κακόβουλη χρήση, μπορούν επίσης να χρησιμοποιηθούν και αυτοματοποιημένες λύσεις λογισμικού. Με άλλα λόγια, με τη ραγδαία εξέλιξη της τεχνολογίας τα τελευταία χρόνια, έχουν αναπτυχθεί ευφυή Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems - DSS), τα οποία επιτρέπουν στους χειριστές τους να έχουν μια εικόνα της ευπάθειας που απειλεί το σύστημά τους μέσω των οπτικών αναλύσεων (Visual Analytics) που προσφέρουν, καθώς επίσης και των τεχνικών μετριασμού και αντιμέτρων (mitigation and countermeasure engine), τα οποία προσφέρουν μια «computer without human» αντίδραση σε περίπτωση που κάποιος κακόβουλος χρήστης προσπαθήσει να παραβιάσει την ασφάλεια και την ιδιωτικότητα ενός IoT οικοσυστήματος.

4.3.3 Η καταγραφή δεδομένων

Είναι ευρέως γνωστό ότι οι πάροχοι υπηρεσιών όπως για παράδειγμα YouTube, οι πάροχοι περιεχομένου όπως το Google, το Facebook και η Amazon ή και τρίτα μέρη όπως το DoubleClick, συλλέγουν μεγάλο αριθμό προσωπικών δεδομένων από τους χρήστες τους, κατά την περιήγηση τους στο διαδίκτυο. Η συλλογή και ανάλυση ευρείας κλίμακας προσωπικών πληροφοριών αποτελεί την κύρια δραστηριότητα των περισσοτέρων από αυτές τις εταιρείες, οι οποίες χρησιμοποιούν τα δεδομένα για εμπορικούς σκοπούς. Τα προσωπικά στοιχεία μπορούν να χρησιμοποιηθούν, για παράδειγμα, για στόχευση της αγοράς (marketing segment), και την προβολή σχετικών διαφημίσεων, ανάλογα με τα ενδιαφέροντα του χρήστη [Bucklin, 2009].

Εκτός από τα παραπάνω, τα δεδομένα μπορούν να χρησιμοποιηθούν και από κρατικούς οργανισμούς και κακόβουλους χρήστες, οι οποίοι με διάφορες τεχνικές και εργαλεία μπορούν να υποκλέψουν τα προσωπικά δεδομένα.

Ορισμένα προγράμματα θυγατρικών όπως για παράδειγμα το pay-per-sale [Dellarocas, 2007], απαιτούν την «παρακολούθηση» ώστε να ακολουθούν τον χρήστη από τον ιστότοπο όπου τοποθετείται η διαφήμιση, στον ιστότοπο όπου πραγματοποιείται η πραγματική αγορά [Joye, 2013]. Οι προσωπικές πληροφορίες στον ιστό μπορούν να δοθούν οικειοθελώς από τον χρήστη συμπληρώνοντας φόρμες web ή μπορούν να συλλεχθούν έμμεσα χωρίς την γνώση τους μέσω της ανάλυσης των κεφαλίδων, των αιτήσεων HTTP, των ερωτημάτων στις μηχανές αναζήτησης ή ακόμα και με τη χρήση κακόβουλων προγραμμάτων με τη χρήση της γλώσσας προγραμματισμού JavaScript αλλά και μέσω των προγραμμάτων Flash που βρίσκονται ενσωματωμένα σε ιστοσελίδες. Μεταξύ των δεδομένων που συλλέγονται, μπορούμε να βρούμε πληροφορίες τεχνικού χαρακτήρα, όπως το πρόγραμμα περιήγησης που χρησιμοποιείται, το λειτουργικό σύστημα, η διεύθυνση IP ή ακόμα και πολύ πιο ευαίσθητες πληροφορίες, όπως η γεωγραφική θέση του χρήστη, οι προτιμήσεις του ή ακόμα και το ιστορικό των ιστοσελίδων που επισκέπτεται. Δυστυχώς, τα δεδομένα που συλλέγονται δεν σταματούν εδώ. Για παράδειγμα, οι υπηρεσίες webmail είναι γνωστές για τη σάρωση και την επεξεργασία των μηνυμάτων ηλεκτρονικού ταχυδρομείου του χρήστη, ακόμη και αν έχουν ληφθεί από έναν χρήστη που δεν επέτρεψε κανένα είδος ελέγχου μηνυμάτων.

5 Εύρεση ευπαθειών με τη χρήση μηχανών αναζήτησης

5.1 Οι κοινές μηχανές αναζήτησης

Όλο και περισσότερες υπηρεσίες προσφέρονται δημοσίως στο διαδίκτυο. Επιπλέον, οι μεγαλύτερες εταιρείες συνήθως χρησιμοποιούν κατανεμημένα δίκτυα και υπηρεσίες για τους υπαλλήλους τους, τόσο στο εσωτερικό όσο και στο εξωτερικό περιβάλλον εργασίας των επιχειρήσεων. Ταυτόχρονα, το λογισμικό που υλοποιεί τις υπηρεσίες αυτές καθίσταται όλο και πιο πολύπλοκο και πιο δύσκολο να ασφαλιστεί από τις επιθέσεις και τις απειλές κακόβουλων χρηστών. Αυτό φυσικά προσελκύει την προσοχή των επιτιθέμενων.

Σε έρευνα του, ο Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) της Ευρωπαϊκής Ένωσης επιβεβαίωσε ότι οι επιθέσεις που βασίζονται στον ιστό, καθώς και οι επιθέσεις σε δικτυακές εφαρμογές, συγκαταλέγονται στις τρεις σημαντικότερες απειλές του 2015 [ENISA, 2016]. Συχνά υπάρχουν άμεσες συνέπειες από αυτές τις επιθέσεις, όπως οι απώλειες στις πωλήσεις, αλλά οι επιθέσεις μπορεί επίσης να συνεπάγονται έμμεσες και μακροπρόθεσμες επιπτώσεις όπως η απώλεια της φήμης των επιχειρήσεων.

Ως εκ τούτου, η ζήτηση και το ενδιαφέρον των παρόχων, των διαχειριστών συστημάτων και του υπεύθυνου προσωπικού τεχνολογίας πληροφοριών για την ασφάλεια των συστημάτων, έχει αυξηθεί τα τελευταία χρόνια. Ωστόσο, η μεγάλης κλίμακας έλεγχοι με συμβατικές δοκιμές διείσδυσης που χρησιμοποιούν εργαλεία γενικής χρήσης, όπως το Nmap ή το Nessus, είναι συνήθως δαπανηρές και χρονοβόρες. Επιπλέον, πρέπει να ληφθούν υπόψη οι νομικές πτυχές, πράγμα που σημαίνει πως οι συμβατικοί έλεγχοι διείσδυσης προσεγγίζουν άμεσα τα συστήματα-στόχους.

Ιδιαίτερα στην Ευρωπαϊκή Ένωση απαγορεύεται η πρόσβαση στο σύστημα χωρίς την ρητή συγκατάθεση του παρόχου του συστήματος στον οποίο ανήκει ο υπό εξέταση στόχος, όπως αναφέρεται στην οδηγία 2013/40 / ΕΕ, του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου (άρθρα 2 έως 7). Αυτός ο νομικός περιορισμός είναι ένα τεράστιο πρόβλημα για τους οργανισμούς που φιλοξενούν υπηρεσίες τρίτων ή δεν έχουν συμβατική έγκριση ελέγχου. Ομοίως, στις ΗΠΑ, μπορεί να χρησιμοποιηθεί ο νόμος για την απάτη και την εκμετάλλευση υπολογιστών (CFAA), ο οποίος έχει ως κύριο στόχο την ανάθεση ποινικού αδικήματος και όχι την εκμετάλλευση ή κατοχή δυνητικών εργαλείων που μπορούν να χρησιμοποιηθούν για την προετοιμασία επίθεσης.

5.2 Μηχανές αναζήτησης και ευπάθειες

Σύμφωνα με τον Kunder (2016), οι πληροφορίες στο διαδίκτυο περιλαμβάνονται σε περισσότερες από 45 δισεκατομμύρια ιστοσελίδες. Η εύρεση σχετικών ιστοσελίδων και πληροφοριών σε γενικές γραμμές συχνά δεν είναι ασήμαντη. Για να βελτιωθεί η ιχνηλασιμότητα των πληροφοριών και η χρηστικότητα των χρηστών, το περιεχόμενο των μεμονωμένων ιστότοπων συστηματικά και αυτόματα αναπροσαρμόζεται και δομείται.

Αυτή η εργασία εκτελείται από μηχανές αναζήτησης γενικής χρήσης όπως το Google, το Bing, το DuckDuckGo ή το Yahoo. Με τη βοήθειά τους, οι χρήστες μπορούν εύκολα να αναζητήσουν πληροφορίες χρησιμοποιώντας εγκατεστημένους φυλλομετρητές ή ειδικές διεπαφές υπηρεσιών. Ο John (2010) έδειξε ότι κάθε μέρα συγκεκριμένα αυτοματοποιημένα ερωτήματα αποστέλλονται στις μηχανές αναζήτησης για την ανίχνευση κάποιας ευπάθειας. Ο Imperva (2011) διερεύνησε ένα botnet το 2011 και ανακάλυψε ότι κατά μέσο όρο 22.000 έως και 80.000 από αυτά τα ερωτήματα στέλνονταν σε μια γνωστή μηχανή αναζήτησης της οποίας το όνομα δεν αναφέρεται.

Οι υπολογιστές botnet προέρχονταν κυρίως από το Ιράν, την Ουγγαρία και τη Γερμανία. Η εκστρατεία επικεντρώθηκε στην αναγνώριση των τρωτών σημείων στο Cross-Scripting (XSS) και την SQL (Structured Query Language).

Ένα ερώτημα, που ονομάζεται Google dork, είναι ένα κανονικό ή εκτεταμένο ερώτημα αναζήτησης, το οποίο επιστρέφει ευαίσθητες πληροφορίες ή συμβουλές για την αποτροπή της ευπάθειας. Το ερώτημα αυτό ονομάζεται και Google dorking ή hacking Google. Αυτή η μέθοδος εισήχθη από ερευνητές ασφάλειας, οι οποίοι συγκέντρωσαν αυτά τα dorks στην ιστοσελίδα τους.

Ένα dork αποτελείται συχνά από δύο μέρη: Το πρώτο μέρος εντοπίζει μια ευπάθεια και το δεύτερο μέρος χρησιμοποιείται για την εστίαση του στόχου. Για παράδειγμα, το ακόλουθο dork αναζητά απαρχαιωμένους διακομιστές ιστού Apache HTTP στον τομέα "destination.com"

Apache / 2.0.63 site: destination.com

Η καταλληλότητα των αποτελεσμάτων εξαρτάται σε μεγάλο βαθμό από την επιλογή μιας κατάλληλης μηχανής αναζήτησης. Παρόλο που οι καθιερωμένοι και γνωστοί κινητήρες όπως το Google, το Bing ή το Yahoo προορίζονται να εξυπηρετήσουν τον ίδιο σκοπό, η κάλυψή τους για συγκεκριμένα θέματα διαφέρει, τόσο ως προς την ποσότητα όσο και ως προς την ποιότητα των αποτελεσμάτων. Εκτός από τη βάση

δεδομένων ευρετηρίου, ο περιφερειακός προσανατολισμός διαδραματίζει σημαντικό ρόλο [Toffalini, 2016].

Η παγκόσμια κυριαρχία της μηχανής αναζήτησης Google, κατέχει μερίδιο αγοράς άνω του 90%. Εάν η διαδικασία αναζήτησης επικεντρωθεί στη Ρωσία ή την Κίνα, η απόφαση για τη χρήση της μηχανής αναζήτησης θα αλλάξει επειδή η μηχανή αναζήτησης Yandex έχει διείσδυση στην αγορά περίπου 40% στη Ρωσία, ενώ στην Κίνα η Baidu είναι ηγέτης της αγοράς με περίπου 70%.

Σε αντίθεση με τις μηχανές αναζήτησης γενικού σκοπού, οι μηχανές αναζήτησης που σαρώνουν το διαδίκτυο, σε μια καθορισμένη περιοχή θεμάτων, όπως υπηρεσίες που φιλοξενούνται, για τον εντοπισμό ευπαθειών SSL/TLS ή συγκεκριμένα τρωτά σημεία σε λογισμικό, όπως XSS ή SQL injection. Παρόμοια με τις μηχανές αναζήτησης γενικής χρήσης, οι πληροφορίες που λαμβάνονται είναι εσωτερικά επεξεργασμένες και συγκεντρωμένες για να παρέχουν στους χρήστες μια γρήγορη και ολοκληρωμένη απάντηση για τα ερωτήματά τους.

Η κύρια διαφορά των συγκεκριμένων μηχανών αναζήτησης, οι οποίες προσφέρονται σε ερευνητές ασφάλειας, σε σύγκριση με τα συμβατικά εργαλεία ανάλυσης ευπαθειών, είναι η έλλειψη άμεσης επαφής των χρηστών με τα συστήματα στόχους, διότι οι πληροφορίες μπορούν να ανακτηθούν απευθείας από τη μηχανή αναζήτησης. Μερικές από τις υπάρχουσες μηχανές αναζήτησης για συγκεκριμένες θεματικές περιοχές είναι:

- Shodan
- Censys
- ERIPP
- PunkSPIDER
- Netcraft

Η μηχανή αναζήτησης ERIPP δεν είναι πια διαθέσιμη και τα αποτελέσματα των μηχανών αναζήτησης Netcraft και PunkSPIDER επιστρέφουν μόνο ένα μικρό σύνολο ή τρωτά σημεία τα οποία είναι πλέον ξεπερασμένα ή πληροφορίες ιστότοπων τα οποία δεν είναι χρήσιμα στους ερευνητές για ανάλυση. Συνεπώς, αυτές οι μηχανές αναζήτησης δεν είναι πλέον αποτελεσματικές, με αποτέλεσμα μόνο η Shodan και η Censys να επιλέγονται για περαιτέρω εξέταση. Η μηχανή αναζήτησης Shodan επικοινωνεί συστηματικά με διευθύνσεις IP από οποιαδήποτε περιοχή [Lee, 2017].

Σύμφωνα με τα διαθέσιμα αποτελέσματα, ένας προκαθορισμένος κατάλογος θυρών σαρώνεται με αυτόν τον τρόπο. Σε περίπτωση επιτυχούς σύνδεσης με το σύστημα που αποτελεί τον στόχο, αποθηκεύονται οι μετα-πληροφορίες (metadata) που ανακτώνται για την εκτέλεση των υπηρεσιών, οι αποκαλούμενες «πληροφορίες banner». Για παράδειγμα, οι πληροφορίες banner για μια υπηρεσία OpenSSH είναι το SSH-2.0-OpenSSH 6.7p1 Debian-5 + deb8u3.

Επιπλέον, οι διαθέσιμες στο κοινό πληροφορίες, όπως τα πλήρως εξουσιοδοτημένα ονόματα τομέα (Fully Qualified Domain Name ή FQDN), συμπληρώνουν την καταχώρηση μιας διεύθυνσης IP. Η μηχανή αναζήτησης Shodan διατίθεται από το 2009 και αναπτύχθηκε από τον John Matherly. Σύμφωνα με το CNN Money [Goldman 2013], η βάση δεδομένων της Shodan υπολογίζεται ότι περιέχει 500 εκατομμύρια κεντρικούς υπολογιστές και τις αντίστοιχες διευθύνσεις IP τους [Nasir, 2014].

Σε αντίθεση με τις μηχανές αναζήτησης γενικής χρήσης όπως η Google, η Shodan επικεντρώνεται ρητά στις ευπάθειες. Η ανίχνευση κάποιας ευπάθειας με τη μηχανή αναζήτησης Shodan υποστηρίζεται με δύο τρόπους. Από τη μία πλευρά, μπορούν να γίνουν αιτήματα για συγκεκριμένες ευπάθειες. Τα λεγόμενα ερωτήματα Shodan είναι συγκρίσιμα με τα dorks της Google. Από την άλλη πλευρά, η Shodan καθορίζει άμεσα τα επιλεγμένα τρωτά σημεία και τα επιστρέφει μαζί με το πραγματικό αποτέλεσμα του ερωτήματος. Το ακόλουθο ερώτημα Shodan μπορεί να χρησιμοποιηθεί, για παράδειγμα, για την ανίχνευση φωνητικών τηλεφώνων IP από τον κατασκευαστή Snom στην περιοχή δικτύου 11.11.11.0/24 που λειτουργεί στη θύρα 5060 [Vlajic, 2018].

port: 5060 snom net: 11.11.11.0/24

Ακολουθώντας αυτή την προσέγγιση, απαιτείται εκτεταμένη λίστα με ερωτήματα Shodan υψηλής ποιότητας.

5.3 Μαζικές επιθέσεις – Σύντομη ιστορική αναδρομή

5.3.1 Επιθέσεις DDOS

Η μεγαλύτερη επίθεση στον κόσμο μεγέθους 1Tbps τύπου DDoS, εκτοξεύτηκε από 152.000 έξυπνες συσκευές οι οποίες είχαν παραβιαστεί. Αν κάποιος έχει στην κατοχή του έξυπνες συσκευές που συνδέονται με το διαδίκτυο όπως τηλεόραση, αυτοκίνητο, ψυγείο ή θερμοστάτες μπορεί να είναι ήδη μέρος του botnet που αποτελείται από εκατομμύρια τέτοιες συσκευές οι οποίες χρησιμοποιήθηκαν για να εκτοξεύσουν τη

μεγαλύτερη DDoS γνωστή επίθεση μέχρι τώρα, με ταχύτητα αιχμής πάνω από 1Tbps, στην εταιρία OVH που στεγάζεται στη Γαλλία.

Καθώς το Internet of Things και οι συνδεδεμένες συσκευές σε αυτό μεγαλώνουν σταδιακά, συνεχίζονται να μεγαλώνουν οι περιοχές επίθεσης, δίνοντας έτσι στους επιτιθέμενους ένα μεγάλο αριθμό από σημεία εισόδου που μπορούν να επηρεάσουν κάποιον χρήστη με τον ένα ή τον άλλο τρόπο. Το IoT συχνά αναπτύσσεται σε ένα μεγάλο αριθμό από συσκευές μέσα από σπίτια, επιχειρήσεις, νοσοκομεία, ακόμα και ολόκληρες πόλεις, αλλά συχνά γίνονται στόχοι επιθέσεων από κακόβουλους χρήστες και χρησιμοποιούνται ως όπλα για διαδικτυακές επίθεσης λόγο της έλλειψης μέτρων ασφαλείας και της μη επαρκούς κρυπτογράφησης. Ο Octave Klaba, ο ιδρυτής της OVH, αποκάλυψε στο Twitter ότι η εταιρία του χτυπήθηκε από δύο ταυτόχρονες DDoS επιθέσεις που μαζί ξεπερνούσαν το 1Tbps.

Μία φωτογραφία που ανέβασε ο Klaba δείχνει τις πολλαπλές επιθέσεις DDoS που ξεπερνούν τα 100Gbps, συμπεριλαμβανομένου και μίας που έφτανε τα 799 Gbps μόνη της, κάνοντας τη την μεγαλύτερη DDoS επίθεση που έχει καταγραφεί ποτέ. Σύμφωνα με τον ιδρυτή της OVH, η μαζική επίθεση DDoS πραγματοποιήθηκε από ένα δίκτυο με πάνω από 152.000 IoT συσκευές συμπεριλαμβανομένου CCTV κάμερες και προσωπικά μηχανήματα για βίντεο. Οι IoT συσκευές συνήθως δεν έχουν ενεργοποιημένες ως προεπιλογή τις αναβαθμίσεις για την ασφάλεια, κάτι το οποίο δίνει τη δυνατότητα στους επιτιθέμενους να παραβιάσουν αυτές τις συσκευές ανά πάσα ώρα και στιγμή και με μεγάλη ευκολία (Gubbi, 2013).

5.3.2 Επίθεση με χρήση drone

Οι επιστήμονες στον τομέα της ασφάλειας έχουν αναπτύξει ένα ιπτάμενο drone με ενσωματωμένο εργαλείο παρακολούθησης ικανό να καταγράφει δεδομένα από συσκευές που είναι συνδεδεμένες στο διαδίκτυο, γνωστές και ως IoT. Η εφαρμογή του project επέτρεπε στους ερευνητές να πετάξουν το drone πάνω από το Austin του Texas (USA), ενσωματώνοντας το δικό τους σύστημα καταγραφής που είχαν δημιουργήσει και να συλλέξουν πολύτιμες πληροφορίες.

Μέσα σε 18 λεπτά πτήσης το drone βρήκε περίπου 1600 συνδεδεμένες συσκευές, από τις οποίες 453 ήταν κατασκευασμένες από τη Sony και 110 από τη Philips. Ο τρόπος ουσιαστικά, με τον οποίο οι ερευνητές κατάφεραν να εντοπίσουν όλες τις έξυπνες

συσκευές ήταν ανιχνεύοντας το πρωτόκολλο ZigBee, το οποίο χρησιμοποιούσαν οι εκάστοτε συσκευές.

Όταν οι IoT συσκευές επικοινωνούν ασύρματα μέσω του πρωτοκόλλου ZigBee, αυτό το πρωτόκολλο είναι ανοιχτό στο επίπεδο του δικτύου. Οπότε όταν οι συσκευές αυτές άρχισαν να συνδέονται και έστελναν beacon αιτήματα, οι ερευνητές κατέγραφαν τα δεδομένα που αντάλλασσαν οι συσκευές χρησιμοποιώντας το πρωτόκολλο ZigBee. Το ZigBee είναι ένα γνωστό πρωτόκολλο που χρησιμοποιείται για την ασύρματη επικοινωνία σε οικιακούς χώρους από την πλειοψηφία των IoT συσκευών σήμερα. Το χρησιμοποιούν εταιρίες όπως Toshiba, Philips, Huawei, Sony, Siemens, Samsung, Motorola αλλά και πολλές άλλες.

Ο Tobias Zillner και ο Sebastian Strobl από την Cognosec έχουν ανακαλύψει μερικά κρίσιμα κενά στην ασφάλεια του πρωτοκόλλου ZigBee, που επιτρέπουν στους κακόβουλους χρήστες να εισβάλουν σε ένα ZigBee δίκτυο και να πάρουν υπό τον έλεγχό τους όλες τις συνδεδεμένες συσκευές σε αυτό, όπως για παράδειγμα έξυπνες κλειδαριές από πόρτες, συστήματα συναγερμού ακόμα και να ελέγξουν τα φώτα ή την θέρμανση. Αυτή η ευπάθεια στην πραγματικότητα δημιουργείται στον τρόπο όπου το πρωτόκολλο ZigBee διαχειρίζεται τα κλειδιά για την πιστοποίηση των IoT συσκευών και τα προσθέτει στο mesh network (meshnet), επιτρέποντας στους κακόβουλους χρήστες να συλλέξουν τα κλειδιά αυτά για να επιτύχουν την αυθεντικοποίηση. Το χειρότερο σημείο που επεσήμαναν οι ερευνητές ήταν ότι οι χρήστες δε μπορούσαν να κάνουν κάτι για να ασφαλίσουν περισσότερο τις συσκευές τους και από τη στιγμή που το κενό ασφαλείας επηρεάζει μία μεγάλη γκάμα από συσκευές, είναι πολύ δύσκολο να προσδιοριστεί πότε οι εταιρίες θα δημιουργήσουν μία διόρθωση.

Το Persirai IoT botent, το οποίο στοχεύει IP κάμερες, έρχεται μετά το Mirai και μεγαλώνει τον κίνδυνο των IoT botnets. Οι ερευνητές στο Trend Micro έχουν ανακαλύψει ένα καινούριο IoT botnet το οποίο ανακαλύπτει 120.000 IP κάμερες εκτεθειμένες για επίθεση. Το botnet με την επωνυμία Persirai, ανακάλυψε περισσότερα από 1.000 μοντέλα από διαφορετικές IP κάμερες. Το botnet αυτό, επιτίθεται κυρίως σε IoT συσκευές και συνεχίζει τις καταστροφικές συνέπειες του Mirai botnet, το οποίο λίγους μήνες νωρίτερα είχε σπείρει το χάος με τις επιθέσεις σε DVRs (Digital Video Recorders) και CCTV (Closed circuit television) κάμερες για να εκτοξεύσει μία μαζική DDoS επίθεση το Οκτώβριο του 2016.

Οι ερευνητές ανακάλυψαν το Persirai, όταν εντόπισαν τέσσερις command and control servers και βρήκαν ευπάθειες που σχετίζονταν με αυτούς όπως αναφέρει ο Jon Clay, υπεύθυνος για τις απειλές στις επικοινωνίες στο Trend Micro. Καθώς έκαναν ανάλυση στο κακόβουλο λογισμικό, βρήκαν ότι στόχευε IP κάμερες. Χρησιμοποιώντας το εργαλείο Shodan, εντόπισαν περισσότερες από 120.000 συσκευές οι οποίες ήταν εκτεθειμένες στο διαδίκτυο. Οι IP κάμερες είναι ορατοί στόχοι για κακόβουλα λογισμικά που στοχεύουν το IoT γιατί συνήθως χρησιμοποιούν το Universal Plug and Play (UPnP) πρωτόκολλο που επιτρέπει στις συσκευές να ανοίξουν μία πόρτα στο δρομολογητή (router) και να λειτουργήσουν σαn server (W3C, 2013).

Η πιο εμφανής διαφορά ανάμεσα στο Mirai και στο Persirai ήταν ότι το Mirai χρησιμοποιούσε brute-force τεχνικές για να κλέψει τα στοιχεία των χρηστών, ενώ το Persirai χρησιμοποιούσε μία zero-day ευπάθεια η οποία είχε δημοσιευτεί κάποιους μήνες νωρίτερα. Οι επιτιθέμενοι που εκμεταλλεύονταν αυτό το κενό μπορούσαν να πάρουν το αρχείο με τους κωδικούς, το οποίο τους έδινε και πρόσβαση στη συσκευή. Η κάμερα που είχε καταληφθεί από την επίθεση μπορούσε να χρησιμοποιηθεί για να ανακαλύψει και άλλα θύματα, τα οποία μπορούσαν να μολυνθούν από την ίδια zero-day ευπάθεια. Από εκεί και μετά μπορούσαν να συνεχίσουν να κλέβουν αρχεία κωδικών και να εξασφαλίζουν την ικανότητα να εκτελούν διάφορες εντολές συστήματος και να διαδίδουν τον κακόβουλο κώδικα.

Ο Clay δηλώνει ότι η συγκεκριμένη zero-day ευπάθεια που αφορά το Persirai θα συνεχίσει να είναι μία απειλή. Το λογισμικό διαγράφει τον εαυτό του μόλις μολύνει το μηχάνημα και τρέχει μόνο στη μνήμη. Αυτό κάνει πολύ πιο δύσκολο να εντοπιστεί ο κώδικάς του μόλις διαγραφεί. «Οι επιτιθέμενοι πίσω από αυτή την ενέργεια είναι πολύ πιθανόν να κυνηγήσουν και άλλες ευπάθειες και να ψάξουν για άλλες συσκευές IoT με παρόμοια κενά ασφαλείας» εξηγεί ο ίδιος. Ο επιτιθέμενος μπορεί να φτιάξει ένα μεγαλύτερο ή και ξεχωριστό botnet με αυτές τις συσκευές. Οι κάτοχοι IP καμερών θα πρέπει να κρατούν τις συσκευές τους ενημερωμένες με τις τελευταίες αναβαθμίσεις στην ασφάλεια του λογισμικού τους και να χρησιμοποιούν πιο περίπλοκους κωδικούς για να είναι πιο ισχυροί απέναντι σε μία brute-force επίθεση. Οι περισσότεροι χρήστες δε ξέρουν ότι οι IP κάμερες είναι εκτεθειμένες στο διαδίκτυο και συνήθως δεν αλλάζουν τον προεπιλεγμένο κωδικό τους, εξηγούν οι ερευνητές. Οι περισσότεροι δε γνωρίζουν καν εάν η κάμερά τους πραγματοποιεί μία DDoS επίθεση. Οι κατασκευαστές πρέπει να βελτιώσουν τη διαδικασία πιστοποίησης και να χρησιμοποιήσουν παραπάνω στοιχεία

από τον κωδικό, όπως βιομετρικά χαρακτηριστικά ή έλεγχο ταυτότητας δύο παραγόντων (two-factor authentication) για να δυναμώσουν την ασφάλεια των συσκευών τους [Kolias, 2017].

Ερευνητές ασφάλειας από την SEC Consult ανακάλυψαν πως μερικοί «τεμπέληδες» κατασκευαστές οικιακών δρομολογητών (router) και συσκευών IoT έχουν επαναχρησιμοποιήσει τις ίδιες συλλογές από hardcoded κλειδιά κρυπτογράφησης, αφήνοντας γύρω στα τρία εκατομμύρια IoT συσκευές ευάλωτες σε ενέργειες κακόβουλων χρηστών.

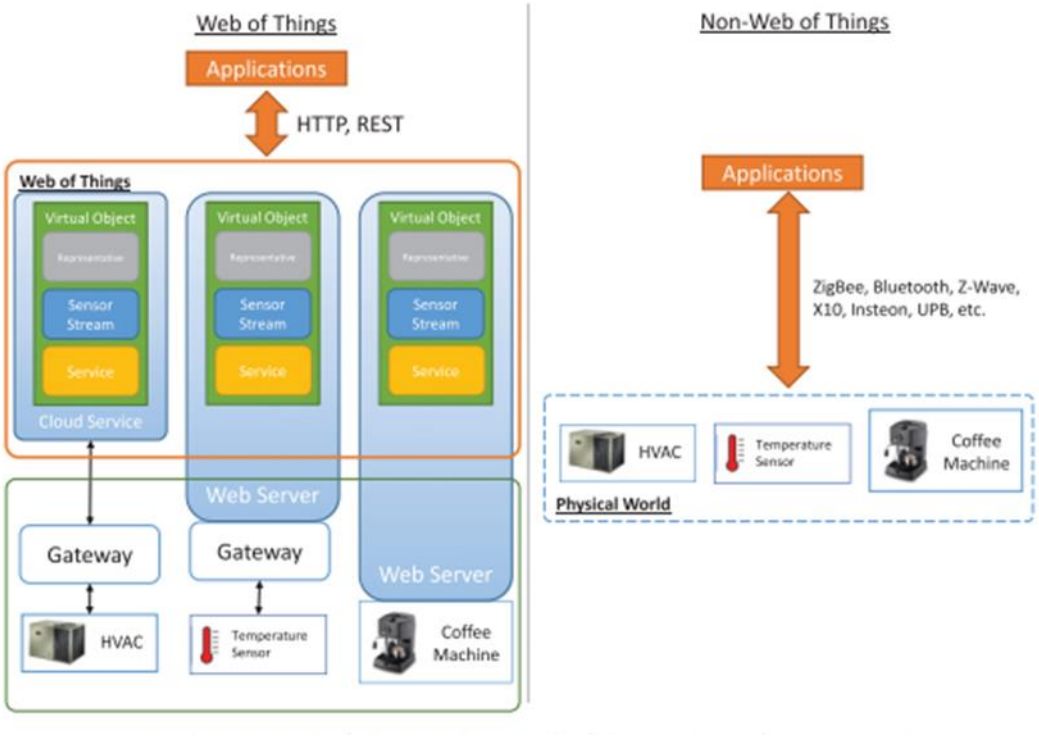
Η βρετανική εταιρία ασφάλειας καταναλωτών BullGuard έχει αναπτύξει έναν σαρωτή IoT, ο οποίος επιτρέπει τον έλεγχο των IoT συσκευών για τον εντοπισμό τρωτών σημείων και αν οι συσκευές αυτές μπορούν εύκολα να γίνουν στόχος κακόβουλων χρηστών. Από τα αποτελέσματα μια έρευνας που διεξήχθη με το παραπάνω εργαλείο, εντοπίστηκαν σχεδόν 200 εκατομμύρια συσκευές που θα μπορούσαν να είναι ευάλωτες.

5.4 Web of Things

Ο Ιστός των Πραγμάτων (Web of Things) προκύπτει από την εφαρμογή τεχνολογιών ιστού στο Διαδίκτυο των Πραγμάτων για την πρόσβαση σε πληροφορίες και υπηρεσίες φυσικών αντικειμένων. Στο WoT, κάθε φυσικό αντικείμενο διαθέτει ψηφιακό αντίγραφο που συνήθως αναφέρεται ως "Εικονικό αντικείμενο" ή "Web Thing" [Guinard, 2011]. Αυτά τα αντικείμενα είναι κατασκευασμένα σύμφωνα με την αρχιτεκτονική μεταφοράς αντιπροσωπευτικής κατάστασης (REST) και έχουν πρόσβαση με πρωτόκολλο HTTP μέσω του REST API. Ένα Web Thing μπορεί να έχει μια παράσταση HTML ή JSON, το API REST για την πρόσβαση στις ιδιότητες και τις ενέργειες του και μια σημασιολογική περιγραφή βασισμένη στο OWL. Τα Web Things είναι ενσωματωμένα στο Web με τρεις τρόπους. Μπορούν να φιλοξενούνται απευθείας από διακομιστές Web ενσωματωμένους σε φυσικά αντικείμενα. Με έξυπνη βελτιστοποίηση, ένας Web Server μπορεί να λειτουργήσει σε έναν ενσωματωμένο υπολογιστή με μόνο 200 bytes μνήμης RAM και 7KB κώδικα.

Για αντικείμενα που δεν μπορούν να τροποποιηθούν, τα εικονικά τους αντικείμενα μπορούν να φιλοξενούνται από τον διακομιστή Web ενσωματωμένο σε μια συσκευή πύλης ή από μια υπηρεσία σύννεφο. Σε αυτές τις ρυθμίσεις, η συσκευή πύλης μεταφράζει τις κυκλοφορίες σε HTTP στην ιδιόκτητη επικοινωνία του φυσικού αντικειμένου. Αυτοί οι τρεις τρόποι ενσωμάτωσης παρουσιάζονται στην Εικόνα 6.

Μια επισκόπηση των τεχνολογιών που επιτρέπουν τη γεφύρωση φυσικών αντικειμένων στο διαδίκτυο παρέχεται σε αυτό το σημείο. Στο WoT, οι εφαρμογές αλληλοεπιδρούν με τα φυσικά αντικείμενα με το γνωστό πρωτόκολλο HTTP και REST API. Αυτό απλοποιεί την πρόσβαση σε φυσικά αντικείμενα, επιτρέποντας να χρησιμοποιηθούν σε εφαρμογές Web και να συγχωνευθούν με υπάρχοντες πόρους στο Web. Ενισχύει τη δημιουργία υπηρεσιών προστιθέμενης αξίας στον κυβερνοχώρο, εκθέτοντας ικανότητες ανίχνευσης και ενεργοποίησης σε μια παγκόσμια ανοικτή αγορά. Ουσιαστικά, το WoT μετατρέπει τον πραγματικό κόσμο σε βιβλιοθήκη πόρων λογισμικού που είναι εύκολα προσβάσιμο μέσω του διαδικτύου [Jabbar, 2016].



Εικόνα 6 - Σύγκριση Web of Things και μη Web of Things λύσεων

5.5 Ανακάλυψη και αναζήτηση στο Web των Πραγμάτων

Οι Web of Things μηχανές αναζήτησης (WoTSearchEngines) μπορούν να χαρακτηριστούν ως οι «βιβλιοθηκάριοι» του WoT. Ανακαλύπτουν και συλλέγουν πόρους WoT σε ένα συγκεκριμένο πεδίο εφαρμογής και επιτρέπουν στους χρήστες να «αναζητήσουν» τους πόρους αυτούς. Για συντομία και συνέπεια, χρησιμοποιούμε τον όρο WoTSE για αμφότερα τα συστήματα σχεδιασμένα ειδικά για WoT και IoT ή τηλεμετρικές λύσεις που μπορούν να προσαρμοστούν στο WoT. Οι WoTSE

εμφανίζονται σε διαφορετικά σενάρια χρήσης με διαφορετικές μορφές και εφαρμογές στη βιβλιογραφία:

• Εντοπισμός Φυσικών Αντικειμένων: Στα πρώιμα έργα, τα WoTSE χρησιμοποιούνται συνήθως για τον εντοπισμό φυσικών αντικειμένων, τα οποία φέρουν ετικέτες με παθητικές ετικέτες RFID.

• Εύρεση οντότητας με δυναμική κατάσταση: Ένα WoTSE μπορεί να αναζητά φυσικά αντικείμενα όπως για παράδειγμα μια αίθουσα συσκέψεων, με βάση τις καταστάσεις πραγματικού χρόνου π.χ. «διαθέσιμες», που προέρχονται από τις μετρήσεις των αισθητήρων τους.

• Αναζήτηση Υπηρεσιών Ενεργοποίησης: Πολλές επιστημονικές έρευνες καταδεικνύουν τη χρήση του WoTSE ως μέσου όρου για την ανάκτηση υπηρεσιών που προσφέρονται από φυσικά αντικείμενα όπως είναι η αλλαγή της έντασης ενός λαμπτήρα.

• Ανάκτηση δεδομένων: Πρωτότυπα των υπηρεσιών εντοπισμού EPC απεικονίζουν τη χρήση του WoTSE για την ανάκτηση αρχείων δεδομένων που σχετίζονται με ένα μεμονωμένο φυσικό αντικείμενο. Κάθε μορφή WoTSE στη βιβλιογραφία έχει τα δικά της χαρακτηριστικά και τεχνικές προκλήσεις. Ωστόσο, ορισμένα χαρακτηριστικά είναι αμετάβλητα μεταξύ τους. Ως εκ τούτου, μπορούμε να οικοδομήσουμε ένα κοινό μοντέλο για να παρουσιάσουμε την πλειοψηφία των διαφορετικών WoTSE.

Αναζήτηση WoT vs Αναζήτηση Ιστού

Καθώς το περιεχόμενο στο WoT είναι προσβάσιμο μέσω του διαδικτύου, οι μηχανές αναζήτησης WoT θεωρούνται μερικές φορές μια μικρή επέκταση των μηχανών αναζήτησης ιστού. Ωστόσο, αυτό δεν συμβαίνει, λόγω των μοναδικών χαρακτηριστικών του WoT (Εικόνα 7). Οι υπάρχουσες μηχανές αναζήτησης ιστού αντιμετωπίζουν τέσσερα θέματα στο WoT. Πρώτον, το WoT κατέχει τεράστιο αριθμό σύντομων, δομημένων κειμένων και περιεχομένου μη κειμένου (π.χ. ροές αισθητήρων, λειτουργικότητα), ενώ οι μηχανές αναζήτησης ιστού βελτιστοποιούνται για μακρά, αδόμητα κείμενα. Επομένως, μόνο η επεξεργασία κειμένων δεν είναι επαρκής για το WoT. Δεύτερον, το WoT στερείται τους ρητούς συνδέσμους του ιστού. Η πλειονότητα της σχέσης μεταξύ φυσικών αντικειμένων υπάρχει υπό μορφή λανθάνουσας συσχέτισης. Επομένως, τόσο οι μηχανισμοί ανίχνευσης όσο και οι μηχανισμοί ανάλυσης συνδέσμων όπως το Page Rank, δεν ισχύουν άμεσα για το WoT. Τρίτον, το WoT έχει μια διαφορετική αλλά μεγάλη δυναμική. Για παράδειγμα, οι αισθητήρες στο WoT

ενημερώνουν το περιεχόμενό τους από μία φορά ανά δευτερόλεπτα έως 1.000.000 φορές το δευτερόλεπτο.

Επομένως, οι μηχανισμοί αποθήκευσης και οργάνωσης στο ευρετήριο μηχανών αναζήτησης ιστού που αναλαμβάνουν αργό μεταβαλλόμενο περιεχόμενο δεν μπορούν να αντιμετωπίσουν το WoT. Τέλος, το WoT είναι και μεγαλύτερο και μικρότερο από τον ιστό. Αναμένεται να περιέχει πάνω από 50 δισεκατομμύρια συσκευές μέχρι το 2020, ενώ ο ιστός διαθέτει σήμερα μόνο ένα δισεκατομμύριο ιστότοπους. Ωστόσο, οι εφαρμογές WoT αλληλοεπιδρούν με κοντινούς πόρους για το μεγαλύτερο μέρος του χρόνου ζωής τους. Για παράδειγμα, οι φυσικές εφαρμογές που αλληλοεπιδρούν με τα έξυπνα σπίτια. Οι τρέχουσες μηχανές αναζήτησης ιστού ενδέχεται να μην μπορούν να κλιμακωθούν για να εξυπηρετήσουν πάνω από 50 δισεκατομμύρια συσκευές. Επίσης, δεν είναι εξοπλισμένα για την ανάκτηση πόρων σε άμεση γειτνίαση με χρήστες αναζήτησης. Τα αναφερόμενα ζητήματα υποδηλώνουν ότι απαιτούνται νέες τεχνικές και μηχανισμοί για την υλοποίηση του WoTSE, παρά την ισχυρή θεμελίωση της υπάρχουσας βιβλιογραφίας στο Web Search [Jaehak, 2016].

5.6 Επισκόπηση των Βιομηχανικών Έργων και Προτύπων

Ορίζουμε τα βιομηχανικά έργα ως δημόσια διαθέσιμα και, προαιρετικά, εμπορικά προϊόντα και υπηρεσίες. Επιλέγουμε δύο ομάδες βιομηχανικών έργων για την αξιολόγησή μας βάσει παραπομπών σε ερευνητικά πρωτότυπα και πηγές ειδήσεων IoT. Η πρώτη ομάδα είναι αυτόνομες μηχανές αναζήτησης WoT. Το Shodan υποστηρίζει ότι είναι «η πρώτη μηχανή αναζήτησης στον κόσμο για συσκευές συνδεδεμένες στο διαδίκτυο». Σχεδιάστηκε και αναπτύχθηκε από τον John Matherly το 2009. Η μηχανή αναζήτησης Censys , που αναπτύχθηκε από το Πανεπιστήμιο του Michigan το 2015 και το Qadium, το οποίο είχε 20 εκατομμύρια δολάρια σε χρηματοδότηση μέχρι το 2016, προσφέρουν παρόμοιες υπηρεσίες. Ουσιαστικά, τα συστήματα αυτά αποτελούν εργαλεία για την πραγματοποίηση πειραμάτων για ερευνητικούς σκοπούς στο διαδίκτυο. Ωστόσο, μπορούν να προσαρμοστούν για αναζήτηση συσκευών στο WoT. Η Shodan και η Censys μπορούν να ανιχνεύσουν και να αποκτήσουν πρόσβαση σε ένα ευρύ φάσμα ευάλωτων συσκευών δικτύου από κάμερες Web, μόνιτορ μωρών, ATM και ιατρικές συσκευές.

Η μηχανή αναζήτησης, από την άλλη πλευρά, είναι ειδικά σχεδιασμένη για WoT. Αντί να ανοίγει δημόσιες διευθύνσεις IPv4, η IoT μηχανή αναζήτησης Thingful χτίζει το σύνολο δεδομένων της από πηγές δεδομένων αισθητήρων στον παγκόσμιο ιστό. Αυτοί οι πόροι εκτίθενται για αναζήτηση μέσω γραφικού χάρτη. Η δεύτερη ομάδα είναι ένας μηχανισμός αναζήτησης που προσφέρεται στο πλαίσιο της εμπορικής πλατφόρμας Cloud IoT - πλατφόρμα IoT της Amazon Web Service (AWS IoT) ή η πλατφόρμα IBM Watson IoT (Watson IoT). Αυτοί οι μηχανισμοί αναζήτησης λειτουργούν σε αντικείμενα και πόρους του ερευνητή, που συνδέονται με την πλατφόρμα. Η προσφερόμενη δυνατότητα αναζήτησης είναι βασική, όπως το φιλτράρισμα αντικειμένων με το αναγνωριστικό και τα metadata τους. Πρέπει να σημειωθεί ότι ενώ τα αντικείμενα αναζήτησης μπορούν να διανεμηθούν φυσικά σε ολόκληρο τον πλανήτη, το πεδίο της δυνατότητας αναζήτησης που προσφέρεται σε έναν χρήστη εξακολουθεί να είναι περιορισμένο στο δικό του «σιλό» δεδομένων. Επιλέγουμε πρότυπα για ανάλυση με βάση το τεχνικό τοπίο της ομάδας ενδιαφέροντος WoT και τις αναφορές των ερευνητικών πρωτοτύπων. Εστιάζουμε σε πρότυπα που καθορίζουν ολόκληρη τη διαδικασία εντοπισμού και αναζήτησης και επιλέγουμε την υπηρεσία Discovery EPCglobal, την υπηρεσία Discovery BRIDGE (WP2) και την υπηρεσία Discovery Extensible Supply Chain Discovery (ESCD) της Afilias. Αυτά τα πρότυπα περιστρέφονται γύρω από την «Υπηρεσία Ανακάλυψης», η οποία βρίσκει πληροφοριακά συστήματα σε ένα δίκτυο όπως το Internet, το οποίο περιέχει τις πληροφορίες που αντιστοιχούν σε ένα δεδομένο αναγνωριστικό αντικειμένου. Επομένως, από την προοπτική του Meta-path, αυτά τα πρότυπα είναι πολύ παρόμοια(Chen, 2016).

(a) Industrial Works

Work	Metapath	Scope	User Type	Collection Type	Discovery Scheme	Mobility Support	Debut Year	Managing Organization	Cost
Censys	R	G	H	R	A	N/A	2015	University of Michigan	Free
Shodan	R	G	H	R	A	N/A	2009	John Matherly	From $19 USD/month
Thingful	R	G	H	R	A	N/A	2013	Umbrellium	Free
Qadium	R	G	-	-	A	-	2013	Qadium	-
AWS IoT	R	G	H,M	R	P	N/A	2015	Amazon	$5USD - $8USD per 1 million messages
Watson IoT	R	G	H,M	R	P	N/A	2015	IBM	$0.01USD per MB exchanged

(b) Standards

Work	Metapath	Scope	User Type	Collection Type	Discovery Scheme	Mobility Support	Debut Year	Managing Organization	Current State
EPCglobal Discovery Service	R=>S	G	H	R	P	N/A	2003	340 companies in 3 action groups	On-going
BRIDGE Discovery Service (WP2)	R=>S	G	H	R	P	N/A	2008	30 partners, coordinated by GS1	Ended. Deliverables include requirements and high-level design
Afilias ONS and Discovery Service [afilias:2008,rezafard:2008]	R=>S	G	H	R	P	N/A	2008	Afilias plc	On-going. Internet-draft submitted to IETF.

Εικόνα 7 – Χαρακτηριστικά των Web of Thing μηχανών αναζήτησης

6 Η μηχανή αναζήτησης Shodan

6.1 Τι είναι η μηχανή αναζήτησης Shodan

Η Shodan είναι μία μηχανή αναζήτησης πολύ διαφορετική από το Google και τις άλλες, καθώς, αντί να κάνει αναζητήσεις στον παγκόσμιο ιστό, αναζητώντας σελίδες, κινείται στα «δρομάκια» και τα «στενά» του Ίντερνετ- μία «σκοτεινή» Google, σύμφωνα με δημοσίευμα του CNN, που αναζητά servers, webcams, εκτυπωτές, routers και γενικότερα οτιδήποτε μπορεί να είναι συνδεδεμένο και να συνθέτει αυτό που ονομάζουμε Ίντερνετ.

Εκτελώντας μια αναζήτηση και χρησιμοποιώντας τη λέξη-κλειδί «default password», η Shodan επιστρέφει πληροφορίες σχετικά με συσκευές όπως οι εκτυπωτές, οι servers και τα συστήματα ελέγχου που χρησιμοποιούν ως username τη λέξη «admin» και ως κωδικό πρόσβασης το «1234». Επίσης, αξίζει να σημειωθεί πως πολλά από τα συστήματα ελέγχου τα οποία μπορεί να βρει κανείς με τη Shodan δε χρησιμοποιούν καθόλου κωδικό πρόσβασης, με αποτέλεσμα να είναι δυνατή η πρόσβαση στο web interface της συσκευής με τη χρήση ενός και μόνο web browser. Όπως επισημαίνει ο John Matherly, δημιουργός της Shodan, δεν τίθεται απλά θέμα έλλειψης ασφαλείας αλλά πολλά από αυτά τα συστήματα δεν θα έπρεπε να είναι συνδεδεμένα στο διαδίκτυο τελικά, καθώς πολλοί κατασκευαστές αντί να συνδέσουν άμεσα έναν υπολογιστή με ένα σύστημα θέρμανσης, προτιμούν να τα συνδέσουν και τα δύο σε έναν web server, οπότε και είναι εκτεθειμένες και οι δύο πλευρές σε πιθανές ευπάθειες.

Η μηχανή αναζήτησης Shodan παρέχει δεδομένα αναζήτησης για διευθύνσεις IP και μερικές άλλες πληροφορίες. Αν και υπάρχουν πολλές μηχανές αναζήτησης στις μέρες μας, η μηχανή αναζήτησης Shodan είναι μία από τις πιο ισχυρές μηχανές αναζήτησης. Η Shodan επιτρέπει στον χρήστη να βρει συγκεκριμένους τύπους υπολογιστών συνδεδεμένους στο Internet χρησιμοποιώντας διάφορα φίλτρα. Ορισμένοι την έχουν χαρακτηρίσει ως μηχανή αναζήτησης των banner υπηρεσιών, τα οποία είναι μετα-δεδομένα (metadata) που στέλνει ο διακομιστής στον πελάτη. Αυτά μπορεί να είναι πληροφορίες σχετικά με το λογισμικό διακομιστή, ποιες επιλογές υποστηρίζει η υπηρεσία, ένα μήνυμα καλωσορίσματος ή οτιδήποτε άλλο που μπορεί να μάθει ο πελάτης πριν από την αλληλεπίδραση με το διακομιστή.

Η μηχανή αναζήτησης Shodan, έχει σχεδιαστεί για να ανιχνεύει τον παγκόσμιο ιστό και να προσπαθεί να εντοπίσει και να δείξει τις συνδεδεμένες συσκευές. Η Shodan

συλλέγει πάνω από 500 εκατομμύρια συσκευές IoT σε ένα μήνα. Επίσης, συλλέγει δεδομένα κυρίως σε εξυπηρετητές ιστού (HTTP θύρα 80), αλλά υπάρχουν και ορισμένα δεδομένα από τις υπηρεσίες FTP (21), SSH (22), Telnet (23), SNMP (161) και SIP (5060). Χρησιμοποιώντας το Shodan, οι ερευνητές αναγνώρισαν χιλιάδες συσκευές που αντιμετωπίζουν το Διαδίκτυο που σχετίζονται με το σύστημα βιομηχανικών ελέγχων [Simon, 2016].

Shodan (https://www.shodan.io/***)***

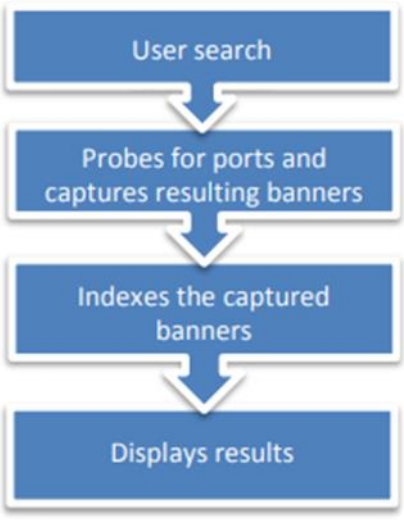
Η Shodan είναι μια μηχανή αναζήτησης για συσκευές συνδεδεμένες στο διαδίκτυο. Αναπτύχθηκε και ξεκίνησε να λειτουργείτο 2009 από τον προγραμματιστή John Matherly, ο οποίος το 2003 συνέλαβε την ιδέα της αναζήτησης συσκευών που συνδέονται στο διαδίκτυο.

Το όνομα Shodan είναι μια αναφορά στον SHODAN, έναν χαρακτήρα από τη σειρά βίντεο παιχνιδιών Shock System. Με τον ίδιο τρόπο που χρησιμοποιεί κάποιος το Bing ή το Google για να αναζητήσει και κατόπιν να αλληλοεπιδράσει με έναν ισότοπο, μπορεί να χρησιμοποιήσει το Shodan για να αναζητήσει και στη συνέχεια να αλληλοεπιδράσει με όλες τις συσκευές που είναι συνδεδεμένες στο Internet. Με τη βοήθεια αυτής της online πλατφόρμας, μπορεί κάποιος να αναζητήσει, να συλλέξει πληροφορίες αλλά και να αλληλοεπιδράσει με κάμερες, έξυπνα ρολόγια, φανάρια της τροχαίας, κεραίες τηλεοπτικών σταθμών, δρομολογητές, διακόπτες, οχήματα, τηλεοράσεις, ψυγεία, αιολικά πάρκα, ιατρικές συσκευές, εκτυπωτές και πολλές ακόμα «συνδεδεμένες» συσκευές.

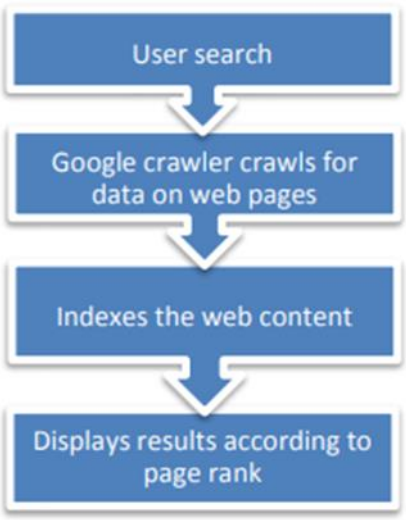
6.2 Τρόπος λειτουργίας της Shodan

Παρόλο που η μηχανή αναζήτησης Shodan μοιάζει με τη μηχανή αναζήτησης της Google ή κάποιας άλλης εταιρείας, διαφέρει κατά πολύ στον τρόπο λειτουργίας και στα αποτελέσματα που εξάγει. Η Shodan ανιχνεύει τις επικεφαλίδες των υπηρεσιών από τις συσκευές που είναι συνδεδεμένες στο διαδίκτυο. Έχει τη δυνατότητα να ανιχνεύει υπηρεσίες των θυρών που φαίνονται στον παρακάτω πίνακα αλλά και πολλές άλλες. Δεδομένου ότι σχεδόν κάθε συσκευή διαθέτει μια διεπαφή απομακρυσμένης σύνδεσης (web interface) για εύκολη πρόσβαση, η Shodan αποθηκεύει τις διευθύνσεις των συσκευών, μαζί με τις διαθέσιμες θύρες και τις επικεφαλίδες, σε μια βάση δεδομένων. Επιπρόσθετα, ο χρήστης δύναται να χρησιμοποιήσει διάφορα φίλτρα στις αναζητήσεις

του, ώστε να συγκεκριμενοποιήσει τα αποτελέσματα που θα εξάγει. Αυτή η βάση είναι διαθέσιμη για προσπέλαση από τον καθένα μέσω της ηλεκτρονικής σελίδας του εργαλείου.



Εικόνα 8 - Αναζήτηση με Shodan



Εικόνα 9 - Αναζήτηση με Google

Η μηχανή αναζήτησης Shodan λειτουργεί 24 ώρες το 24ωρο και συλλέγει πληροφορίες σχετικά με 500 εκατομμύρια συσκευές και υπηρεσίες κάθε μήνα. Χρησιμοποιώντας τη Shodan, ο χρήστης μπορεί να βρει πολλά και ιδιαίτερα «αποτελέσματα», όπως κάμερες ασφαλείας, φανάρια δρόμων, συστήματα θέρμανσης, οικιακούς αυτοματισμούς και άλλα συστήματα που είναι συνδεδεμένα στο διαδίκτυο [Matherly, 2016].

Κάποιοι πιο επίμονοι ενδεχομένως να ανταμειφθούν και με αποτελέσματα όπως συστήματα ελέγχου πυρηνικών σταθμών, καθώς και εξοπλισμού εργαστηρίων. Και, όπως επισημαίνεται στο σχετικό δημοσίευμα του CNN, το πλέον τρομακτικό της όλης υπόθεσης είναι πως πολύ λίγοι από αυτούς τους «προορισμούς» διαθέτουν κάποιου είδους ασφάλεια, για να εμποδίσει τους επίδοξους «εισβολείς».

Επίσης, αξιοσημείωτο είναι πως πολλά από τα συστήματα ελέγχου τα οποία μπορεί να βρει κανείς με τη Shodan δεν ζητούν καν κωδικούς, το μόνο που χρειάζεται είναι ένας web browser. Δυνατότητες της εν λόγω μηχανής αναζήτησης παρουσιάστηκαν στη συνδιάσκεψη Defcon, όπου αποκτήθηκε πρόσβαση σε πληθώρα «στόχων», από πόρτες γκαράζ μέχρι συστήματα φαναριών οδικής κυκλοφορίας και έναν υδροηλεκτρικό σταθμό. Ειδικοί επισημαίνουν πως ένα τέτοιο εργαλείο θα μπορούσε να χρησιμοποιηθεί με πολύ καταστροφικά αποτελέσματα, εάν πέσει σε λάθος χέρια.

Ωστόσο, μέχρι τώρα η Shodan χρησιμοποιείται για καλούς σκοπούς. Ο Matherly έχει περιορίσει τις αναζητήσεις σε 10 αποτελέσματα εάν ο χρήστης δεν έχει λογαριασμό ενώ αν κάποιος είναι πιστοποιημένος χρήστης μπορεί να δει 50 αποτελέσματα. Εάν κάποιος επιθυμεί να αξιοποιήσει τις πλήρεις δυνατότητες της μηχανής αναζήτησης, πρέπει να παρέχει στον δημιουργό λεπτομερή στοιχεία για το ποιόν και τους σκοπούς του, καθώς και πληρωμή.

Οι κύριοι χρήστες της αυτή τη στιγμή είναι επαγγελματίες του χώρου της ασφάλειας, ακαδημαϊκοί και υπηρεσίες ασφαλείας, που χρησιμοποιούν τη Shodan κυρίως για τον εντοπισμό και την επισήμανση τρωτών σημείων, που μπορούν να εκμεταλλευτούν κακόβουλοι εισβολείς.

Ο Matherly αναγνωρίζει ότι η μηχανή αναζήτησής του μπορεί να χρησιμοποιηθεί για «ξεκίνημα» από άτομα με κακές προθέσεις, ωστόσο, όπως επισημαίνει, οι κακόβουλοι χρήστες έχουν συνήθως πρόσβαση σε botnets, με μεγάλους αριθμούς μολυσμένων υπολογιστών, για να εξυπηρετούν τέτοιους σκοπούς χωρίς να εντοπίζονται [Matherly, 2016].

6.3 Βασικές λειτουργίες και χρήση φίλτρων

Φίλτρα

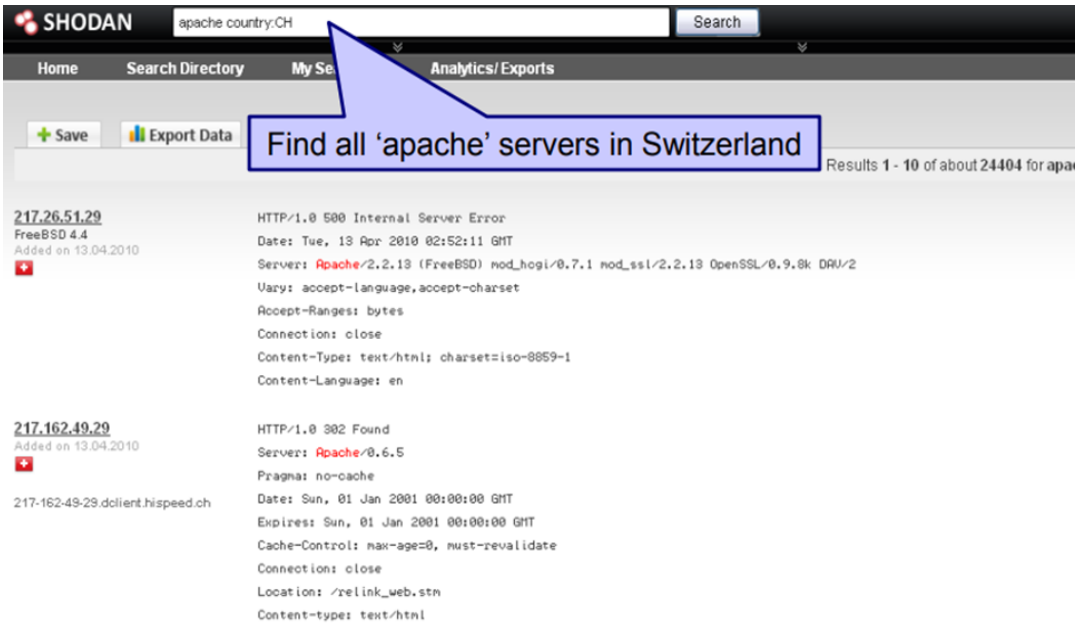
- χώρα: τα αποτελέσματα των φίλτρων κατά κωδικό χώρας δύο χαρακτήρων
- όνομα κεντρικού υπολογιστή: τα αποτελέσματα των φίλτρων κατά συγκεκριμένο κείμενο στο όνομα του κεντρικού υπολογιστή ή τον τομέα
- net: τα αποτελέσματα φίλτρων με συγκεκριμένη περιοχή IP ή υποδίκτυο
- OS: αναζήτηση συγκεκριμένων λειτουργικών συστημάτων
- θύρα: να περιορίσετε την αναζήτηση συγκεκριμένων υπηρεσιών

Εικόνα 10 - Χρήση φίλτρων στη Shodan

Φίλτρο χώρας

Το φιλτράρισμα ανά χώρα μπορεί να επιτευχθεί κάνοντας κλικ στον χάρτη χώρας (διατίθεται από το αναπτυσσόμενο μενού) ή περνώντας τον δείκτη του ποντικιού πάνω από μια χώρα για τον αριθμό των σαρωμένων υπολογιστών για μια συγκεκριμένη χώρα.

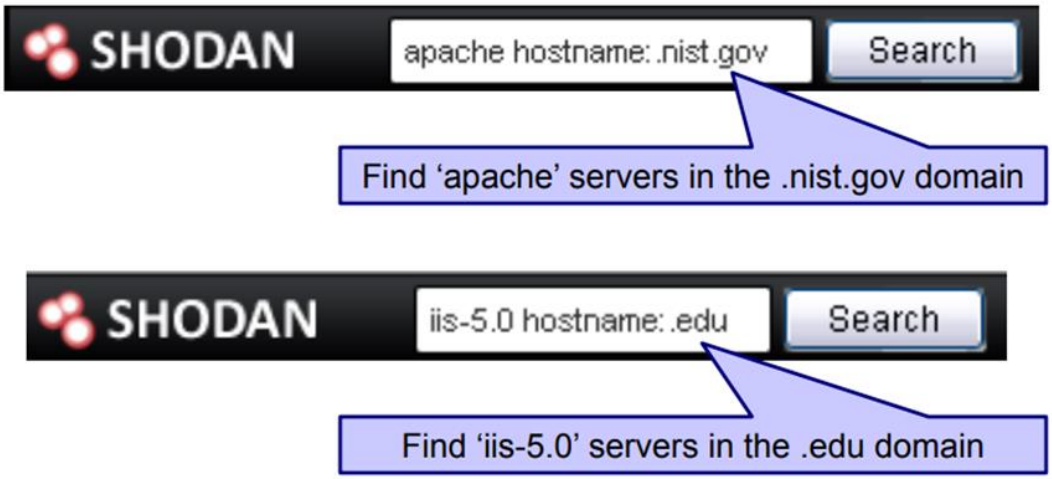
Αναζήτηση server



Εικόνα 11 - Αναζήτηση server στη Shodan

Φίλτρο ονόματος κεντρικού υπολογιστή

Τα αποτελέσματα αναζήτησης μπορούν να φιλτραριστούν χρησιμοποιώντας οποιοδήποτε τμήμα ενός ονόματος υπολογιστή ή ονόματος τομέα.



Εικόνα 12 - Αναζήτηση φίλτρο ονόματος κεντρικού υπολογιστή

Φίλτρα Net / OS

Το φίλτρο δικτύου επιτρέπει στον χρήστη να επεξεργαστεί τις αναζητήσεις με τη χρήση της συμβολής IP / CIDR . Επίσης, Το φίλτρο OS επιτρέπει να βελτιώσει ο χρήστης τις αναζητήσεις από το λειτουργικό σύστημα

Φίλτρο θυρών

Το Shodan μπορεί να φιλτράρει τα αποτελέσματα αναζήτησης κατά θύρα. Η τρέχουσα συλλογή περιορίζεται στις θύρες 21 (FTP), 22 (SSH), 23 (Telnet) και 80 (HTTP), ενώ η συντριπτική πλειοψηφία της συλλογής είναι HTTP .

Εξαγωγή (export)

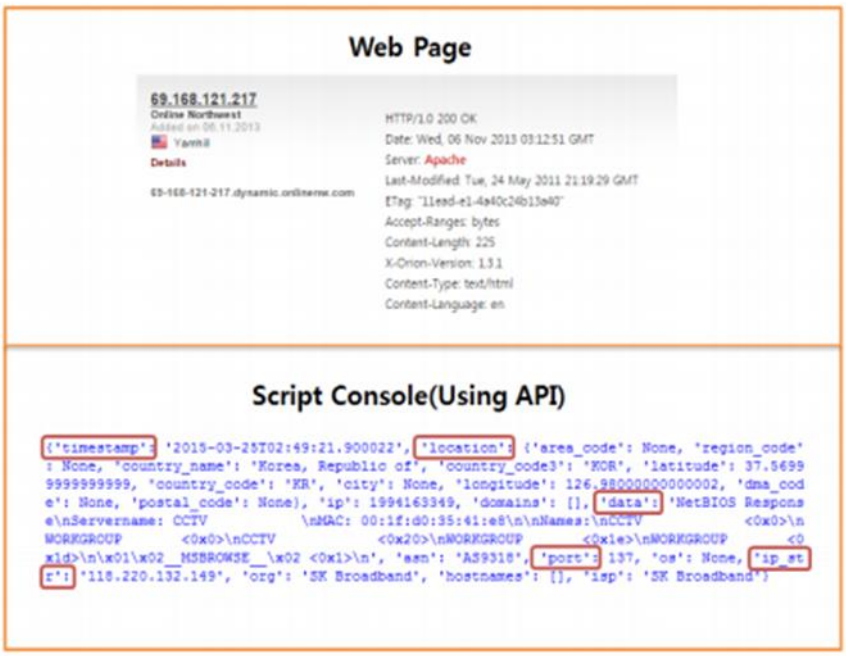
Η μηχανή Shodan επιτρέπει στον χρήστη να εξάγει έως και 1.000 αποτελέσματα ανά πίστωση σε μορφή XML. Οι πιστώσεις μπορούν να αγοραστούν online. Επίσης, υπάρχει διαθέσιμο αρχείο εξαγωγής δεδομένων δείγματος μετά την απαραίτητη διαδικασία.

Εικόνα 13 - Ενδεικτικό XML από εξαγωγή δεδομένων

6.4 Συλλογή πληροφοριών από συσκευές IoT με τη Shodan

Τα είδη πληροφοριών που παρέχει η Shodan

Τα είδη πληροφοριών που μπορούν να παρέχονται από τη μηχανή αναζήτησης Shodan μπορούν να χωριστούν σε δύο τύπους. Το πρώτο παρέχεται από την ιστοσελίδα ενώ το δεύτερο παρέχεται από την κονσόλα σεναρίου χρησιμοποιώντας το API της μηχανής αναζήτησης. Αρχικά, οι πληροφορίες που παρέχονται από την ιστοσελίδα έχουν μόνο βασικά δεδομένα όπως διεύθυνση IP, συνδεδεμένη χώρα, συνδεδεμένη πόλη, όνομα διακομιστή. Ωστόσο, οι πληροφορίες που παρέχονται από την κονσόλα σεναρίων έχουν πιο χρήσιμα δεδομένα από τις ιστοσελίδες όπως ο αριθμός θύρας, η ευθυγράμμιση, το γεωγραφικό πλάτος/μήκος, συμπεριλαμβανομένων των δεδομένων της ιστοσελίδας. Η σύγκριση τους των δύο τύπων πληροφοριών φαίνεται στην παρακάτω εικόνα.

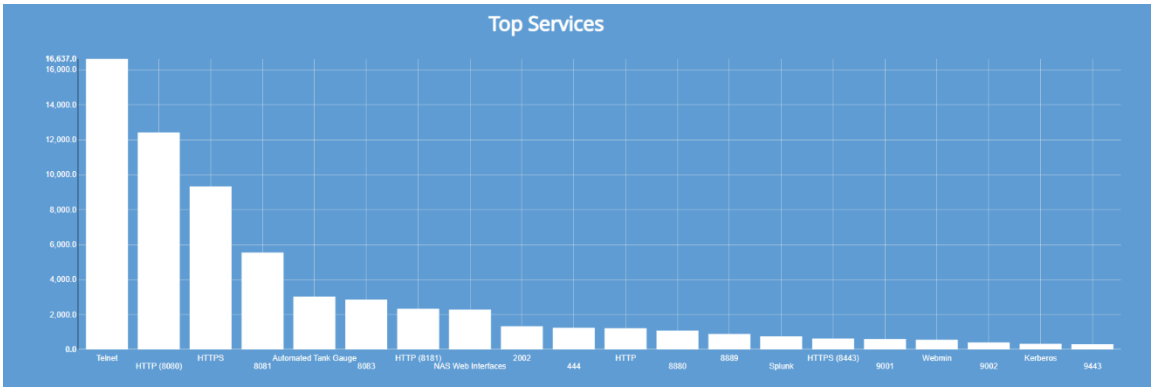


Εικόνα 14 - Σύγκριση πληροφοριών μεταξύ ιστοσελίδας και API script

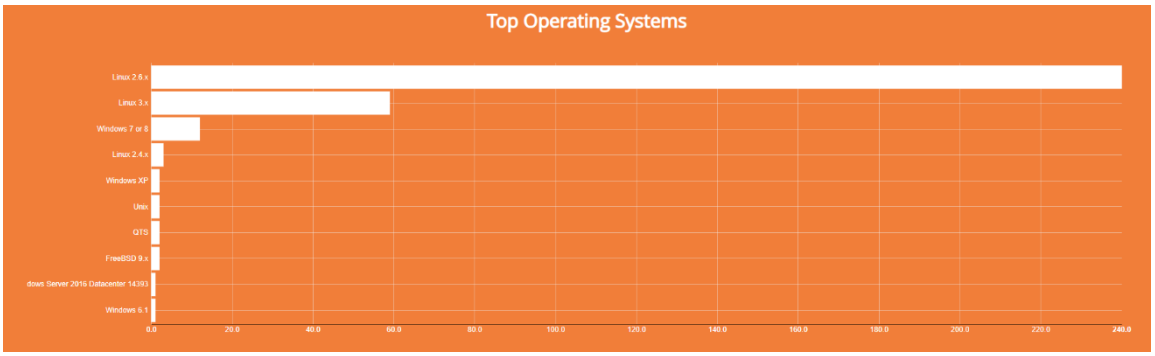
Στατιστικά δεδομένα - διαγράμματα

Στα παρακάτω στατιστικά δεδομένα και διαγράμματα, παρουσιάζονται πληροφορίες που συνέλεξε η μηχανή αναζήτησης Shodan σε παγκόσμια κλίμακα, χρησιμοποιώντας ως όρο αναζήτησης τη λέξη «default password». Ο όρος αυτός, περιέχεται στο banner από μεγάλο αριθμό συνδεδεμένων συσκευών ανά τον κόσμο, καταδεικνύοντας πως πολλές IoT συσκευές χρησιμοποιούν τους εργοστασιακούς κωδικούς ασφαλείας καθιστώντας τες ευάλωτες σε κακόβουλες πράξεις επιτήδειων.

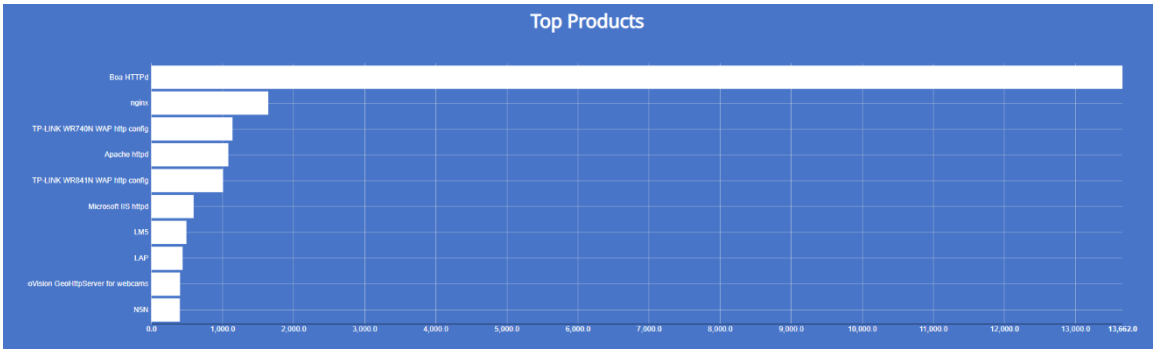
Εικόνα 15 - Λίστα χωρών με συσκευές με εργοστασιακούς κωδικούς ασφαλείας



Εικόνα 16 - Υπηρεσίες οι οποίες καθίστανται ευάλωτες σε επιθέσεις



Εικόνα 17 – Κατάταξη των πιο ευάλωτων λειτουργικών συστημάτων



Εικόνα 18 - Κατάταξη των πιο ευάλωτων προϊόντων σε ευπάθειες

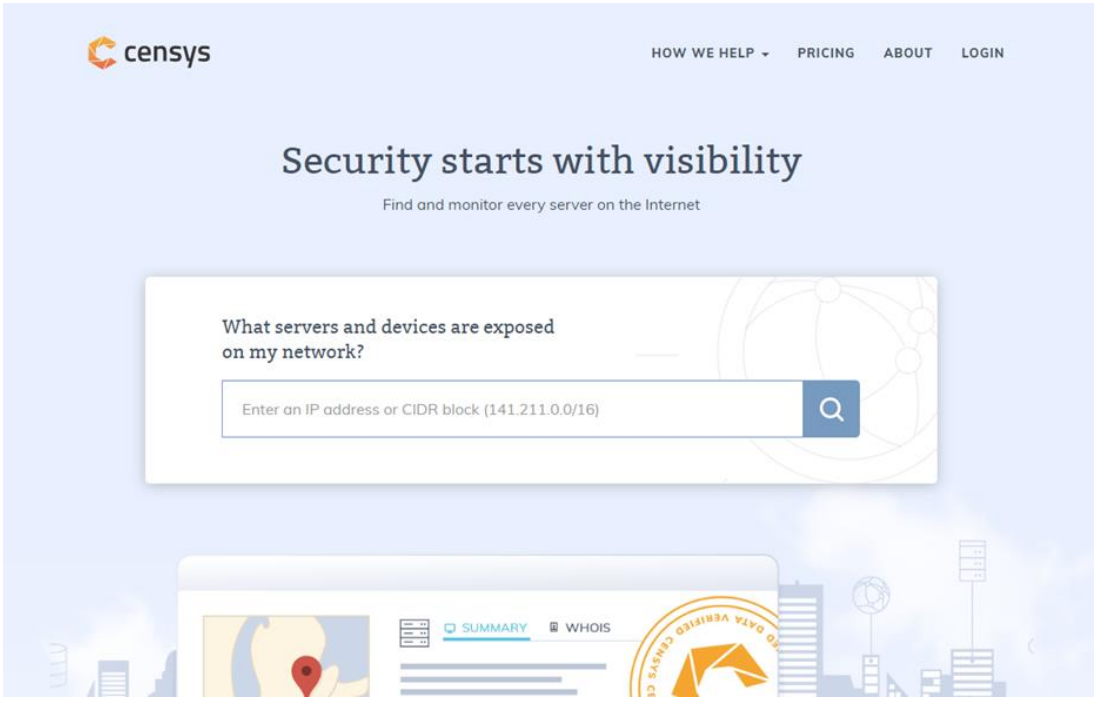
7 Η μηχανή αναζήτησης Censys

Η μηχανή αναζήτησης Censys δεν μοιάζει καθόλου με τις συμβατικές γνωστές μηχανές αναζήτησης. Αυτή η μηχανή αναζήτησης κρατά αρχεία καταγραφής όλων των συσκευών που είναι συνδεδεμένες με το διαδίκτυο και θεωρείται περισσότερο σαν ένα έργο ανοικτού κώδικα.

Censys (https://censys.io/)

Το Censys είναι μια μηχανή αναζήτησης που κυκλοφόρησε τα τελευταία χρόνια και δεν μοιάζει καθόλου με τις συμβατικές. Αυτή η μηχανή αναζήτησης κρατά αρχεία καταγραφής όλων των συσκευών που είναι συνδεδεμένες με το διαδίκτυο και θεωρείται περισσότερο σαν ένα έργο ανοικτού κώδικα. Κατασκευάστηκε από το Πανεπιστήμιο του Michigan με την αρωγή και του Πανεπιστημίου του Illinois το 2015, από την ομάδα ερευνητών ασφαλείας που ανέπτυξε το εργαλείο ZMap, του πιο πολυχρησιμοποιημένου εργαλείου για την ευρεία σάρωση του διαδικτύου. Τα τελευταία χρόνια, η συγκεκριμένη ομάδα έχει διεξάγει χιλιάδες ευρείες σαρώσεις του διαδικτύου χρησιμοποιώντας τρισεκατομμύρια ανιχνευτές. Με τον τρόπο αυτό, έχει καταφέρει να διαδραματίσει σημαντικό ρόλο στην εύρεση και την ανάλυση κάποιων από τις σπουδαιότερες διαδικτυακές ευπάθειες όπως είναι το FREAK, Logjam, DROWN, Heartbleed και το Mirai botnet [Antonakakis, 2017].

Σήμερα, το Censys έχει γίνει το χρυσό πρότυπο στην ασφάλεια των δεδομένων και έχει καταφέρει να δώσει σημαντικά αποτελέσματα σε όσους χρησιμοποιούν την πλατφόρμα αυτή, όπως είναι οι ερευνητές ασφαλείας, πολυεθνικές εταιρείες και κυβερνητικοί χρήστες. Για την καλύτερη εξυπηρέτηση της συνεχούς αυξανόμενης ζήτησης, το φθινόπωρο του 2017, η πλατφόρμα Censys ξέφυγε από τα όρια του πανεπιστημίου και εξελίχθηκε σε εταιρεία, προσφέροντας βελτιωμένες υπηρεσίες, τεχνική υποστήριξη και μια ακόμα πιο ολοκληρωμένη και ισχυρή προβολή του διαδικτύου [Durumeric, 2015].



Εικόνα 19 - Βασικό UI της μηχανής αναζήτησης Censys

Τρόπος λειτουργίας του Censys

Ο τρόπος λειτουργίας αυτής της καινοτόμου και ανοιχτού κώδικα μηχανή αναζήτησης είναι η εξής: Η Google παρέχει την υποδομή για τη λειτουργία της Censys και οι επιστήμονες του Πανεπιστημίου του Illinois βοηθούν ώστε να εκτελείται σωστά. Πιο συγκεκριμένα, το εργαλείο αυτό σαρώνει τις διευθύνσεις IPv4 και συλλέγει πληροφορίες από τις ιστοσελίδες και τους host servers. Η μηχανή αναζήτησης χρησιμοποιεί κάποια εργαλεία, για να συγκεντρώσει τις απαιτούμενες πληροφορίες. Το ZMap, έναν σαρωτή δικτύου και το ZGrab, έναν σαρωτή στο επίπεδο των εφαρμογών.

Η σύσταση του εργαλείου ZMap από τους ερευνητές το 2013 αποτελούσε μια σημαντική ανακάλυψη σε σχέση με την ικανότητα να ανιχνεύει και να συλλέγει κάποιος δεδομένα από ολόκληρο το διαδίκτυο. Παλαιότερες τεχνικές απαιτούσαν πολύ χρόνο ή και τη χρήση υπολογιστών υψηλής ισχύος. Το ZMap άλλαξε τη διαδικασία της σάρωσης του διαδικτύου, επιτρέποντας μια σάρωση του συνόλου του χώρου του IPv4 σε λίγα λεπτά, εκτελώντας τη διαδικασία αυτή σε έναν μόνο υπολογιστή.

Μόλις γίνει η συλλογή των πληροφοριών, το Censys τις αποθηκεύει στη βάση δεδομένων(ZDb). Η ZDb περιέχει όλα τα δεδομένα σχετικά με το πώς διαμορφώνονται οι host και οι ιστοσελίδες. Οι ερευνητές μπορούν στη συνέχεια να αλληλοεπιδράσουν με

αυτά τα δεδομένα μέσω της μηχανής αναζήτησης του Censys, μέσω ενός μηχανισμού δημιουργίας αναφορών αλλά και μέσω του SQL engine [Durumeric, 2015].

Το Censys εκτελεί πλήρεις αναζητήσεις στα protocol banners και εξετάζει ένα μεγάλο αριθμό από συμπληρωματικά πεδία, καθημερινά. Βρίσκει τις συσκευές και τα δίκτυα που είναι ευάλωτα και δημιουργεί αναφορές σε συγκεκριμένα πρότυπα και τάσεις. Τέλος, επιστρέφει τα αποτελέσματα πολύ γρήγορα, σε χρόνο λιγότερο από ένα δευτερόλεπτο. Αξίζει να σημειωθεί, πως το Censys μπορεί να αποκαλύψει τις αδυναμίες και τις ευάλωτες συσκευές, τους κατόχους τους όπως επίσης και την τοποθεσία τους κατά προσέγγιση.

Παρακάτω, παρουσιάζεται η χρήση της μηχανής αναζήτησης Censys η οποία μπορεί να εντοπίσει συγκεκριμένες ευάλωτες συσκευές και δίκτυα και να δημιουργήσει στατιστικές αναφορές σχετικά με τα γενικά πρότυπα και τάσεις χρήσης. Το Censys επιστρέφει αυτά τα αποτελέσματα σε ένα δευτερόλεπτο, μειώνοντας δραματικά την προσπάθεια κατανόησης των host που αποτελούν το διαδίκτυο. Παρακάτω θα παρουσιάσουμε την αρχιτεκτονική της μηχανής αναζήτησης Censys και θα αξιολογήσουμε πειραματικά την απόδοσή της. Θα εξετάσουμε επίσης τις εφαρμογές της Censys και θα δείξουμε πώς οι ερωτήσεις που τέθηκαν στις πρόσφατες μελέτες είναι απλές για να απαντηθούν.

Η Censys εκθέτει δεδομένα σε ερευνητές μέσω μιας δημόσιας μηχανής αναζήτησης, του API REST, των προσβάσιμων στο κοινό πινάκων στο Google Big Query και του συνόλου των δεδομένων που μπορούν να μεταφορτωθούν. Η διεπαφή αναζήτησης επιτρέπει στους ερευνητές να πραγματοποιούν αναζητήσεις πλήρους κειμένου και να διερευνούν οποιοδήποτε από τα δομημένα πεδία και ετικέτες που παράγονται κατά τη διάρκεια της σάρωσης και της μεταγενέστερης επεξεργασίας (π.χ., 443.https.cipher_suite). Υποστηρίζει αναζητήσεις πλήρους κειμένου, κανονικές εκφράσεις και αριθμητικές κλίμακες και τα ερωτήματα μπορούν να συνδυαστούν με τη λογική Boolean. Αυτά τα ερωτήματα μπορούν να εκτελεστούν σε ένα τρέχον στιγμιότυπο από κεντρικούς υπολογιστές IPv4 που είναι προσβάσιμοι από το κοινό.

Μετά την εκτέλεση ενός ερωτήματος, οι χρήστες μπορούν να διερευνήσουν διαδραστικά τους κεντρικούς υπολογιστές, τους ιστότοπους και τα πιστοποιητικά που αντιστοιχούν στο ερώτημά τους, καθώς και να δημιουργήσουν στατιστικές αναφορές κατάλληλες για άμεση χρήση στην έρευνα. Ως απλό παράδειγμα, η Censys μπορεί να

αναγνωρίσει το σύνολο των host που υπάρχουν στις Η.Π.Α. που είναι ευάλωτα προς το Heartbleed με το ερώτημα.

443.https. heartbleed.vulnerable: true AND location.country_code: US

Από εκεί, η Censys μπορεί να εξάγει μια πλήρη λίστα αντιστοιχιών διευθύνσεων IP και να καταγράψει τη διανομή των πιο κοινών ευάλωτων μοντέλων συσκευών. Αυτά τα ερωτήματα ολοκληρώνονται σε λιγότερο από ένα δευτερόλεπτο. Για να διευκολύνουμε πιο περίπλοκες αναλύσεις, δημοσιεύουμε ανεπιτυχείς αλληλεπιδράσεις εφαρμογών και καθημερινά στιγμιότυπα των δομημένων δεδομένων. Αυτά μπορούν να αναζητηθούν χρησιμοποιώντας SQL μέσω πινάκων Google Big Query προσβάσιμων στο κοινό ή μεταφορτωμένοι σε μορφή JSON.

Η Censys εκθέτει επιπλέον δεδομένα μέσω ενός δημόσιου API REST που επιτρέπει στους ερευνητές να εξάγουν ακατέργαστα αποτελέσματα αναζήτησης, να αντλούν στατιστικά δεδομένα και να προβάλλουν την ιστορική κατάσταση συγκεκριμένων ξενιστών και δικτύων. Η σάρωση του διαδικτύου έχει ήδη δείξει μεγάλες δυνατότητες για την αποκάλυψη προβλημάτων ασφάλειας και την κατανόηση της ασφάλειας σύνθετων κατανεμημένων συστημάτων. Μεταφέροντας τη σάρωση στο νέφος (cloud), η Censys μειώνει δραματικά την προσπάθεια που απαιτείται για να διερευνήσει αυτά τα ερωτήματα, επιτρέποντας στους ερευνητές να επικεντρωθούν στην ερώτηση πιο σημαντικών ερωτήσεων και όχι στη μηχανική απάντησης. Επιπλέον, η Censys επιτρέπει στην κοινότητα ασφαλείας να αυξήσει την παγκόσμια κάλυψη πρωτοκόλλων και παρέχει μια εύχρηστη λύση για την κατανόηση του αυξανόμενου αριθμού ενσωματωμένων συσκευών στο διαδίκτυο. Ταυτόχρονα, ελαχιστοποιεί την περιττή σάρωση από ερευνητικές ομάδες και ελαχιστοποιεί την εισερχόμενη κυκλοφορία δικτύου που παρακολουθείται από τους φορείς εκμετάλλευσης δικτύου.

Όλα τα πρωτόκολλα στην αρχική ανάπτυξη της μηχανής αναζήτησης Censys χρησιμοποιούν το ZGrab και ενθαρρύνοντας και άλλους ερευνητές να εξετάσουν το ενδεχόμενο να το χρησιμοποιήσουν ως σημείο εκκίνησης για την ανάπτυξη άλλων σαρωτών εφαρμογών. Επιπρόσθετα, το ZGrab απελευθερώνεται και διατηρείται ως ένα αυτόνομο εργαλείο ανοιχτού κώδικα ως μέρος του έργου ZMap. Το ZGrab μπορεί να χρησιμοποιηθεί ανεξάρτητα από τη Censys και συνεργάζεται με το ZMap. Το ZMap

αναγνωρίζει γρήγορα τους hosts και το ZGrab παράγει δομημένα δεδομένα για κάθε έναν από αυτούς τους ξενιστές.

Επικύρωση, εξαγωγή

Τα πρωτογενή δεδομένα JSON που παράγονται από σαρωτές εφαρμογών που συνδέονται με την εφαρμογή, συλλέγονται από τη Censys, όπου επικυρώνονται, μετατρέπονται σε δομημένο σχήμα και επισημαίνονται με πρόσθετα μεταδεδομένα (metadata), όπως π.χ. κατασκευαστής και μοντέλο συσκευής, στην κεντρική βάση δεδομένων. Η Censys επικυρώνει τα δεδομένα σάρωσης με δύο τρόπους. Αρχικά, το ZMap επεκτάθηκε για να ανιχνεύει τις αποκλίσεις στις απαντήσεις δικτύου κατά τη διάρκεια του σταδίου ανακάλυψης του κεντρικού υπολογιστή. Εάν ο ρυθμός απόκρισης σάρωσης πέσει κάτω από ένα καθορισμένο όριο ανά πάσα στιγμή, τότε ποικίλλει περισσότερο από ένα καθορισμένο ποσό κατά τη διάρκεια της σάρωσης, φτάνει ένας μέγιστος αριθμός.

@tag (port = 443, proto = "https", subproto = "tls") def dell_idrac (d): subject = d.443.https.certificate.subject if subject.ou == "Ομάδα Απομακρυσμένης Πρόσβασης" .gr == "Dell Inc.": επιστροφή {"hw_manufacturer": "Dell Inc.", "hw_model": "iDRAC",:

Εδώ εμφανίζεται η ετικέτα για κάρτες απομακρυσμένης διαχείρισης Dell iDRAC. Εάν συμβούν αποτυχίες αποστολής ή αν το libpcap δεν μπορεί να διατηρήσει και να αποθέσει έναν ορισμένο αριθμό πακέτων, η σάρωση τερματίζεται αυτόματα και επαναπρογραμματίζεται. Δεύτερον, η Censys επικυρώνει μια σάρωση κατά την ολοκλήρωσή της και απορρίπτει ότι σαρώσεις, στις οποίες τα ποσοστά απόκρισης του ZMap ή του σαρωτή εφαρμογής πέφτουν έξω από ένα στατικό δεσμό ή αποκλίνουν περισσότερο από το 10% του μέσου όρου των σαρώσεων που ολοκληρώθηκαν τις τελευταίες δύο εβδομάδες. Τέλος, οι απορριφθείσες ανιχνεύσεις ελέγχονται χειροκίνητα κατά το τέλος της διαδικασίας. Αυτοί οι έλεγχοι πραγματοποιούνται κατά κύριο λόγο προκειμένου να ανιχνευθούν παροδικά αποτυχίες δικτύου, το ανθρώπινο σφάλμα στη διαμόρφωση και τα σφάλματα κωδικοποίησης.

Οι σαρωτές εφαρμογής εξάγουν ακατέργαστα δεδομένα σχετικά με κάθε πτυχή της χειραψίας εφαρμογών σε μορφή ανάλογη με τη χειραψία του δικτύου. Για παράδειγμα, στην περίπτωση του Transport Layer Security (TLS), οι παράμετροι πελάτη

και διακομιστή εξάγονται ως μέρος των μηνυμάτων Client και Server. Παρόλο που αυτά τα δεδομένα είναι απαραίτητα για κάποια έρευνα, πολλά από αυτά τα πεδία δεν είναι χρήσιμα κατά την αναζήτηση για κεντρικούς υπολογιστές ή συσκευές αναγνώρισης και θα προκαλούσαν άσκοπες βλάβες στη βάση δεδομένων μας.

Ομοίως, τα συνήθως αναζητούμενα πεδία είναι ένθετα βαθιά μέσα στα μηνύματα του πρωτοκόλλου του δικτύου, καθιστώντας τα δύσκολα να βρεθούν. Για τον σκοπό αυτό, αρχικά αποθηκεύεται και δημοσιεύεται η έξοδος του πρωτογενή σαρωτή εφαρμογών, αλλά στη συνέχεια εξάγονται σημαντικές τιμές και μετασχηματίζονται τα δεδομένα χειραψίας σε δομημένες εγγραφές που συμμορφώνονται με ένα δημοσιευμένο σχήμα. Τα αρχεία εξακολουθούν να εκτελούνται με έναν ντετερμινιστικό τρόπο κατά τη διάρκεια αυτής της διαδικασίας. Με άλλα λόγια, η εγγραφή έχει τον ίδιο κρυπτογραφικό κατακερματισμό αν δεν έχουν συμβεί αλλαγές διαμόρφωσης, πράγμα που επιτρέπει να μειωθεί αργότερα η φόρτωση, απορρίπτοντας εγγραφές που δεν περιέχουν αλλαγές.

Στατιστικά δεδομένα - διαγράμματα

Στα παρακάτω στατιστικά δεδομένα και διαγράμματα, όπως και στην περίπτωση της Shodan, παρουσιάζονται πληροφορίες που συνέλεξε η μηχανή αναζήτησης Censys σε παγκόσμια κλίμακα, χρησιμοποιώντας ως όρο αναζήτησης τη λέξη «default password». Ο όρος αυτός, περιέχεται στο banner από μεγάλο αριθμό συνδεδεμένων συσκευών ανά τον κόσμο, καταδεικνύοντας πως πολλές IoT συσκευές χρησιμοποιούν τους εργοστασιακούς κωδικούς ασφαλείας καθιστώντας τες ευάλωτες σε κακόβουλες πράξεις επιτήδειων.

Εικόνα 20 - Λίστα χωρών με συσκευές με εργοστασιακούς κωδικούς ασφαλείας

Tag	Hosts	Frequency
http	16,750,776	88.87%
https	9,578,410	50.82%
ssh	3,651,775	19.37%
ftp	2,446,166	12.98%
cwmp	2,349,424	12.46%
smtp	1,920,746	10.19%
embedded	1,425,200	7.56%
pop3	1,383,235	7.34%
imap	1,350,433	7.16%
database	1,296,175	6.88%

Εικόνα 21 - Υπηρεσίες οι οποίες καθίστανται ευάλωτες σε επιθέσεις

8 Σύνοψη - συμπεράσματα και μελλοντικές επεκτάσεις

8.1 Σύνοψη και συμπεράσματα

Συνοψίζοντας τα όσα γράφτηκαν στην παρούσα βιβλιογραφική έρευνα, δόθηκε αρχικά ο ορισμός του όρου Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) και στη συνέχεια περάσαμε σε μια ιστορική αναδρομή σχετικά με το IoT. Επίσης, γίνεται αναφορά στα έξυπνα δίκτυα ηλεκτρικής ενέργειας (Smart Grid) και στα χαρακτηριστικά που τα διακρίνουν. Στη συνέχεια γίνεται μια εκτενής αναφορά στα θέματα ασφάλειας και ιδιωτικότητας που παρατηρούνται στα IoT οικοσυστήματα και αναφέρονται κάποια μέτρα αντιμετώπισης τέτοιων καταστάσεων. Επισημαίνονται επίσης τα χαρακτηριστικά των μηχανών αναζήτησης IoT συσκευών και παρουσιάζονται οι διαφορές που έχουν από τις κοινές μηχανές αναζήτησης που χρησιμοποιούνται ευρέως σήμερα. Ακόμα, παρατίθενται ευπάθειες και επιθέσεις που έχουν λάβει χώρα κατά των «ειδικών» αυτών μηχανών αναζήτησης του IoT. Τέλος, γίνεται μια εκτενής έρευνα και χρήση δυο μηχανών αναζήτησης IoT, της Shodan και της Censys, όπου και δίνονται λεπτομέρειες χρήσης αυτών και των αποτελεσμάτων που επιστρέφουν στο χρήστη.

	IP Device Search Engine	
	Shodan	***Censys***
Techniques to Collecting the Information	SYN Scan / Banner grab	SYN Scan / Banner grab
Scan Range	Horizontal Scan	Horizontal scan
SYN Scan Tool	Unknown	Zmap
Banner grab tool	Unknown	Zgrab
scan server	Distributed	Distributed
Target ports	41 ports	35 ports
Scan period	Unknown	Automatically scheduled

Εικόνα 22 - Σύγκριση μεταξύ Shodan και Censys

Καταλήγοντας σε ένα συμπέρασμα, η ποικιλία των πεδίων εφαρμογής του IoT που συναντώνται στις μέρες μας καθιστούν τη χρήση IoT οικοσυστημάτων μια απόλυτα πετυχημένη λύση. Πολλά είναι τα παραδείγματα στη καθημερινή ζωή πλέον, όπου εντοπίζονται τέτοιες λύσεις όπως για παράδειγμα η παρακολούθηση των τιμών του περιβάλλοντος, οι έξυπνες πόλεις, η διαχείριση πόρων (ενέργεια, νερό), η απογραφή και η διαχείριση των προϊόντων, τα έξυπνα σπίτια ή η εφαρμογή IoT λύσεων στον τομέα της υγείας και της ασφάλειας. Παρά την επιτυχημένη χρήση IoT λύσεων σε όλο και περισσότερους τομείς, έχουν διαπιστωθεί δύο πολύ σημαντικά προβλήματα τα οποία έγκεινται στην απώλεια της ασφάλειας αλλά και της ιδιωτικότητας στις επικοινωνίες και τις υπηρεσίες που προσφέρουν τα IoT οικοσυστήματα, γεγονός που καθιστά δημοσίως διαθέσιμα τα προσωπικά δεδομένα και εφικτή την ανεπιθύμητη επικοινωνία σε περίπτωση που κάποιος κακόβουλος χρήστης θελήσει να εκμεταλλευτεί τα κενά ασφαλείας σε τέτοια οικοσυστήματα. Κλείνοντας, όσο εξελίσσεται η τεχνολογία του IoT, τόσο γίνεται μεγαλύτερη η χρήση αλλά και η υιοθέτηση ασύρματων δικτύων για την ανταλλαγή δεδομένων. Αυτή όμως η παράμετρος μπορεί να φέρει στο προσκήνιο νέα ζητήματα ασφάλειας αναφορικά με την παραβίαση της ιδιωτικότητας. Αρκετές έρευνες έχουν αποδείξει πως τα ασύρματα κανάλια αυξάνουν τον κίνδυνο παραβίασης λόγω της δυνατότητας απομακρυσμένης πρόσβασης που παρέχουν, η οποία ενδεχομένως να εκθέσει το σύστημα σε υποκλοπές και επιθέσεις. Ως εκ τούτου, η προστασία της ιδιωτικότητας αποτελεί ένα πραγματικό ανοιχτό ζήτημα που μπορεί να περιορίσει την ανάπτυξη του IoT.

8.2 Μελλοντικές επεκτάσεις

Όσο αναφορά τις μελλοντικές επεκτάσεις στα ζητήματα της ασφάλειας αλλά και της ιδιωτικότητας σε IoT συσκευές αλλά και σε IoT οικοσυστήματα γενικότερα, μπορούμε να εστιάσουμε σε δύο τομείς, οι οποίοι αναπτύσσονται ραγδαία τα τελευταία χρόνια και παρασύρουν μαζί τους και σχετικά νέες τεχνολογίες, όπως είναι το IoT και το βελτιώνουν κατακόρυφα. Το πρώτο πράγμα που θα μπορούσε να βελτιώσει την ασφάλεια των IoT οικοσυστημάτων είναι η χρήση μιας «Blockchain-based» τεχνολογίας, η οποία προς το παρόν, θα καθιστούσε τα IoT συστήματα άτρωτα σε θέματα ασφάλειας [Christidis, 2016]. Το δεύτερο στοιχείο το οποίο θα βελτιώσει κατά πολύ περισσότερο το θέμα της ιδιωτικότητας είναι η θεσμοθέτηση περισσότερων «standards». Με τον όρο «standards», εννοούμε τα πρότυπα που εκδίδονται από γνωστούς οργανισμούς

ανάπτυξης προτύπων (Standards Developing Organizations - SDO), τα οποία γενικά αναφέρονται στη βιομηχανία ή σε οργανισμούς στον τομέα των προτύπων που αναπτύσσουν και δημοσιεύουν πρότυπα ειδικά για τη βιομηχανία, χρησιμοποιώντας ανοικτές και διαφανείς διαδικασίες [NIST, 2018]. Σίγουρα θα μπορεί να βελτιωθεί σε ακόμα περισσότερους τομείς η τεχνολογία αυτή του IoT, κάτι που σίγουρα θα συμβεί τα επόμενα χρόνια μιας και η ερευνητική δουλειά που γίνεται είναι συστηματική και «καρποφόρα».

Βιβλιογραφία

Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami, 2013. Internet of things (IoT): A vision, architectural elements, and future directions. Fut. Gen. Comput. Syst. 29, 7 (2013), 1645–1660.

P. G. P. F. S. Harald Sundmaeker, Vision and Challenges for Realising the Internet of Things CERPIoT, CERP-IoT European Commission, 2010.

Deva Evans (2011), CISCO, The Internet of Things How the Next Evolution of the Internet Is Changing Everything.

Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal, 22 July.

Jakobs, K. et al (2011). Project Report: "Standardising the Internet of Things- What the Experts Think." RWTH Aachen University. CoSc Department, Informatik 4 and Research Group on Electronic Business. 2011.

Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, Internet of Things (IoT): A Literature Review Journal of Computer and Communications, 2015, 3, 164-173.

Uckelmann, D., Harrison, M., & Michahelles, F. 2011. An Architectural Approach Towards the Future Internet of Things. In D. Uckelmann, M. Harrison, & F. Michahelles (Eds.), Architecting the Internet of Things: 1-24. Berlin: Springer.

Song Tan, Debraj De, Wen-Zhan Song, Senior Member, IEEE, Junjie Yang, and Sajal K. Das, Fellow, IEEE: Survey of Security Advances in Smart Grid: A Data Driven Approach, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 1, FIRST QUARTER 2017.

Marek Jawurek, Florian Kerschbaum, and George Danezis(2012), Privacy technologies for smart grids { A survey of options. Technical Report MSR-TR-2012-119, Microsoft Research, November 2012.

J. Hota, "Scope and challenges of Internet of Things: An Emerging Technological Innovation", International Conference on Futuristic Trends in Computational analysis and Knowledge management, 2015.

N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna, "Cookieless monster: Exploring the ecosystem of webbased device fingerprinting," in Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013, pp. 541–555.

A. Mosenia, N. K. Jha, "A comprehensive study of security of Internet-of-Things", IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586-602, Oct./Dec. 2017.

Ghansah I (2012) Smart grid cyber security potential threats, vulnerabilities and risks. Public interest energy research (PIER) program interim report, May 2012

X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Communications Magazine, 50 (8) (2012), pp. 38-45.

J. Kim, L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures", IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1294-1305, Jul. 2013.

MO, Yilin, et al. Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 2012, 100.1: 195-209.

Y. Zhang, L. Wang, Y. Xiang, C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations", *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707-1721, Jul. 2015.

M. B. Barcena, C. Wueest, "Insecurity in the Internet of Things", Symantec Tech. Rep., 2015.

P.H. Griffin, "Secure authentication on the Internet of Things", South-eastCon 2017, pp. 1-5, 2017.

Yan, Ye; Qian, Yi; SHARIF, Hamid. A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In: Wireless Communications and Networking Conference (WCNC), 2011 IEEE. IEEE, 2011. p. 909-914.

Joye M. and Libert B. (2013), A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data, Published in A.-R. Sadeghi, Ed., Financial Cryptography and Data Security (FC 2013), vol. 7879 of Lecture Notes in Computer Science, pp. 111{125, Springer, 2013.

Dellarocas, C., and Viswanathan, S. The holy grail of advertising: Allocative efficiency and revenue implications of "pay-per-action" advertising in environments with quality uncertainty. Paper presented at the Workshop on Information Systems Economics, Montreal, December 2007.

M. de Kunder, The size of the world wide web (the internet) (2012).

John, P., Yu, F., Xie, Y., Abadi, M., Krishnamurthy, A.: “Searching the Searchers with Searchaudit”; Proceedings of the 19th USENIX Conference on Security, USENIX Security’10, Washington, DC, 2010.

Imperva, 2011: “Hacker Intelligence Initiative, Monthly Trend Report #3, August 2011, Hacker Intelligence Summary Report - The Convergence of Google and Bots”; Report, Aug 2011.

F. Toffalini, M. Abb´ı, D. Carra, and D. Balzarotti, “Google dorks: Analysis, creation, and new defenses,” in Proceedings of the 13th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment-Volume 9721. Springer-Verlag New York, Inc., 2016, pp. 255–275.

S. Lee, S.H. Shin, B.H. Roh, "Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning", Proc. 9th IEEE Int'l Conf. Ubiquitous and Future Networks (ICUFN 17), July 2017.

M. Nasir, “Tracking and Identifying Individual Users in a Web Surfing Session,” Computer and Network Security, Middlesex University, London, Tech. Rep., January 2014.

Natalija Vlajic and Daiwei Zhou, IoT as a Land of Opportunity for DDoS Hackers, Computer, vol. 51 July 2018, pp.26-34.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645–1660, 2013.

C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, "DDoS in the IoT: Mirai and other botnets", *Computer*, vol. 50, no. 7, pp. 80-84, Jul. 2017.

D. Guinard, V. Trifa, F. Mattern, E. Wilde, "From the internet of things to the web of things: Resource-oriented architecture and best practices" in Architecting the Internet of Things, New York, NY USA:Springer, pp. 97-129, 2011.

Jabbar, S., Khan, M., Silva, B. N. and Han, K. A REST-based industrial web of things’ framework for smart warehousing. The Journal of Supercomputing(2016), 1-15.

Jaehak Y, Bang H-C, Lee H, Lee YS (2016) Adaptive internet of things and web of things convergence platform for internet of reality services. J Supercomput 72(1):84–102.

Yuanyi Chen, Jingyu Zhou, and Minyi Guo. (2016) A context-aware search system for internet of things based on hierarchical context model. Telecommun. Syst. 62, 1 (2016), 77–91.

Simon, K. (2016, November 14). Vulnerability analysis using google and shodan. In International conference on cryptology and network security (pp. 725–730). Springer International Publishing.

J. Matherly, Complete Guide to Shodan, 2017.

Durumeric, Z.; Adrian, D.; Mirian, A.; Bailey, M.; Halderman, J.A. A search engine backed by internet-wide scanning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 542–553.

M. Antonakakis et al., "Understanding the Mirai Botnet", Proc. 26th USENIX Security Symp., pp. 1093-1110, 2017.

K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

Draft NIST Interagency Report 8200, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), 2018.

Bucklin, Randolph E. and Catarina Sismeiro (2009), ‘‘Click Here for Internet Insight: Advances in Clickstream Data Analysis in Marketing,’’ Journal of Interactive Marketing, 23 (1), 35-48.

Baumeister, T.: Adapting PKI for the smart grid. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 249–254 (2011)

Zhao, Z.; Chen, G. An Overview of Cyber Security for Smart Grid. In Proceedings of the 2018 IEEE 27th International Symposium on Industrial Electronics, Cairns, Australia, 13–15 June 2018; pp. 1127–1131.

EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/ 2016.

Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll. Interoperability of SecurityEnabled Internet of Things. s.l. : Springerlink.com, 2011.

S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead. s.l. : Elsevier B.V., 2014.

Rodrigo Roman, Jianying Zhou, Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. s.l. : Elsevier B.V., 2013.

Wikipedia. Ucode system. [Ηλεκτρονικό] https://en.wikipedia.org/wiki/Ucode_system.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 8/2014 on the on Recent Developments on the Internet of Things. Brussels : s.n., 2014.

Taylor Wessing. The Internet of Things and privacy in Europe and the USA. [Ηλεκτρονικό] 2015.

Ελληνική Νομοθεσία. Εθνικό Τυπογραφείο. [Ηλεκτρονικό] http://www.et.gr/index.php/.

Access to European Union law. Νόμοι της Ευρωπαϊκής Ένωσης. [Ηλεκτρονικό] http://eur-lex.europa.eu/homepage.html.