Security mechanisms for Internet of Things (IoT)

Georgios Mavridis

UEL
University of
East London

Master of Science Thesis

Greece, Piraeus 2017

Security mechanisms for Internet of Things (IoT)

A Thesis

Submitted to the Faculty

Of

University of East London

By

Mavridis Georgios

In partial fulfilment of the

Requirements for the Degree

Master of Science

Information Security and Forensics

September 2017

Abstract

Internet of Things (IoT) is a concept that involves various objects and methods of communication to exchange information. Today, IoT is primarily a vision that dictates that everything should be interconnected over the internet. IoT is currently and for sure will be, the foundation for future development because it brings new opportunities for novel services. All objects will be connected and communication need to happen between all, while CIA triad (at least) should not be compromised, at all. This aspect leads to major security challenges, which will be treated hereinafter.

Acknowledgments

During my time, as Master Student I have had the great opportunity to work with many knowledgeable and helpful persons. I am deeply indebted to all of you who have supported and encouraged me during working on my master thesis.

I want to express my sincere gratitude to my supervisor Dr. Nikolaos Aroukatos for the guidance and assistance during my thesis studies, my teachers, Mr. Dimitris Mitsis, Dr. Spiridon Chountasis, Drs Evangelia Vagana, Phd and Dr. Emmanouil Georgakakis during this journey. Last but not least, to Mr. Kostantinos Dalakouras without his understanding, encouragement, persistence, motivation and kindness it would be difficult for me to reach at this point.

My most sincere appreciation to Dr. Ioannis Karamitsos for his support, comments and initial input during this effort and for his suggestion to develop my research aligned with business needs.

Finally, I must express my very profound gratitude to my family, for providing me with unfailing support and continuous encouragement throughout this journey.

Thank you all, once again.

Table of contents

List of figures

List of tables

Abbreviations

Abbreviation	Description
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
ACL	Access Control Lists
ATM	Automatic Teller Machine
BC	Before Christ
BLE	Bluetooth Low Energy
BOPS	Biometric Open Protocol Standard
CAN	Controller Area Network
CBOR	Concise Binary Object Representation
CCTV	Closed Circuit TV
CIA	Confidentiality, Integrity, Availability
CoAP	Constrained Application Protocol
DevID	Device IDentifier
EPC	Electronic Product Code
EU	European Union
GSM	Global System for Mobile
HAN	Home wireless Area Network
HCD	HardCopy Devices

HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of things
IOT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
Ipv6	Internet Protocol version 6
IR	Infra-Red
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
M2M	Machine to Machine
MACsec	MAC SECurity
MQTT	MQ Telemetry Transport or Message Queue Telemetry Transport
MQTT-SN	MQTT for Sensor Networks
NFC	Near field communication

OSI	Open Systems Interconnection
PLC	Programmable Logic Controller
PoS	Point of Sales
QR	Quick Response
RFID	Radio frequency identification
S/N	Serial Number
SIEM	Security Information and Event Management
SS	Secure Sockets Layer
TCP	Transaction Control Protocol
TEDS	Transducer Electronic Data Sheet
TLS	Transport Layer Security
UDIDs	Unique Device Identifiers
UDP	User Datagram Protocol
USB	Universal Serial Bus
USD	United States Dollar
VoIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wireless Area Network
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Networks
WW I	World War I
WW II	World War II
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Chapter 1
Introduction

1.1. Historical Background

The Internet of Things (IoT) is not a newly introduced term to ICT industry. Back in 1982, four students of Carnegie Mellon University, Mike Kazar, David Nichols, John Zsarnay and Ivor Durham wired up a vending machine so that they could see the availability and coolness of the soda cans in each dispensing column, remotely, over ARPANET. After that, it was mentioned by Kevin Ashton in 1999, while having a presentation at Proctor & Gamble (Ashton, 2009) trying to explain the value of the recently introduced technology of RFID in supply chain industry. Since then, the need of interconnection of all available objects over internet is increasingly demanding. Big consulting companies calculate the number of these connected objects to reach 20bn by 2020, while the market is estimated to reach 3bn USD.

The IoT industry is flourishing since the amount of computations that a computer can execute almost doubles biyearly, while the size and the amount of power needed is almost half for the same period. This means that smaller and more powerful devices are available for interconnection and data exchange offering a wide range of applications.

The Internet of Things covers several different domains and technologies, introducing challenges regarding interoperability between different stacks, and implementation of standards on low powered and low energy devices. All these combined, bring new challenges in security and questions regarding how to ensure confidentiality, integrity and availability.

As all innovative developments and IoT as well, ensure the users a superior life right now and in the years to come, but there is a great security concern. Especially today, the privacy is increasingly concerned by the public. To make IoT pervade people’s everyday life, the security of the IoT must be strengthened.

Security of IoT is crucial to the development of IoT industry. The IoT is an immature technology. The key issue that affects the development of IoT is that a mature and complete security models and standards is lacking. Compared to the traditional network, IoT integrates many different networks such as WSN, RFID systems, mobile vehicle network, xG [1] technologies, WiMAX, personal area network, VPNs and so many others. As the IoT environment becomes more and more complex and demanding, the security issues coped, are more and more complex than any other existing network systems.

My motivation for conducting the research in IoT, is the lack of sustainable and flexible solutions which to address some of the main security issues. Some early security mechanisms and solutions are now being implemented, but they still need improvement and standardization. The full potential of IoT goes beyond the enterprise centric systems and moves towards a user inclusive IoT, in which IoT devices and contributed information flows provided by people, are encouraged. This will allow new user-centric IoT information flows and new cohort of services of high value for the society.

Security is one of the main IoT challenges nowadays. An important consideration is which protocol stack provides best security and privacy services. Security can be provided at different levels so deciding the optimal choice, is not simple process. Since IoT is a relatively new concept, it is still unknown and not explored by many companies and employees in industry. This limited knowledge, may cause them to be afraid of, or totally unaware of the potential security and privacy issues connected to their deployment of IoT. Therefore, many organizations want to know more about the potential threats, benefits, disadvantages, challenges and solutions regarding security regarding IoT. Additionally, they need to know what competence in information security is necessary to realize cost effective security in conjunction with their deployment of IoT. This knowledge and competence should help in facilitating their transition from a non-IoT-business to an IoT-business, as it will enable both employees and management to understand & address their

[1] 3G, 4G, 4,5G, 5G , etc.

doubts & concerns in terms of their investments and the potential security risks. In this way, managers can make a balanced risk-benefit analysis of the adoption of IoT for a specific application or family of applications.

1.2. Thesis Aims and Objectives

The overall aim of this thesis is to assess the security mechanisms in the IoT area. This will include a review and comparison of the current IoT protocol stacks, advantages and disadvantages of different security mechanisms applied in IoT. In this thesis, a distributed security mechanism end-to-end was developed for IoT applications.

To achieve this, the following objectives will be met:

- Identify security requirements introduced in IoT
- Compare and review established protocol stacks in IoT based on privacy, confidentiality, integrity and availability to determine advantages and disadvantages of different protocol stacks
- Suggest guidelines of which protocol stacks to use based on different security requirements, technologies and/or domains.
- Developed a distributed security mechanism for IoT applications end-to-end.

1.3. Thesis Outline

This chapter gives the historical background of IoT, introduces this thesis aims and objectives and provides the outline of the thesis. The rest of the thesis is structured as follows:

Chapter 2, Information Security. This chapter provides an overview of Information Security, illustrates the CIA model, discusses on security elements and provides an overview of countermeasures and security policies.

Chapter 3, Internet of Things (IoT). This chapter gives an overview of Internet of things (IoT), analyses the fundamental and provides the IoT roadmap over the time.

Chapter 4, IoT Technologies. This chapter provides an overview of the most important IoT technologies and ends with a comparison table with pros and cons per technology.

Chapter 5, Architecture of IoT. This chapter discusses the IoT reference model, The IoT framework and standards and analyzes the six-layered architecture.

Chapter 6, Security in IoT. This chapter concludes the challenges IoT ecosystem is facing will discussing the IoT protocols related to Security.

Chapter 7, Proposed Distributed Security Mechanism. This chapter describes the proposed distributed security mechanism to cover end to end, from IoT device to web server.

Chapter 8, Implementation of the Proposed Distributed Security Mechanism. This chapter describes the implementation of the relevant mechanism and provides the results.

Chapter 9, Conclusion. This chapter describes the conclusion of this thesis along with implementation action plan, best practices along with a quick implementation reference card.

On Appendix 1, all IoT relevant standards from various international organizations are presented.

Chapter 2
Information Security

2.1 Historical background of Information Security

Information security processes and techniques are as old as the information each self. From the very first years of communication, the value of security mechanisms was very well comprehended. Julius Caesar was one of the first to use these practices by inventing the Caesar cipher at 50 B.C., to make his messages unreadable if they were found to unwanted hands. From the mid of the 16th century various, governments around the globe, created organizations to secure the information and communication (e.g. the UK Secret Office and Deciphering Branch in 1653).

More recently, during 19th century and because of the two World Wars many authorities were created to protect the privacy of information; exchange of war related information between allies of the World War II, brought into the picture the necessity of encrypting the information to become unreadable. This brought us to the Enigma Machine [2,] which was invented at the end of WWI by Arthur Scherbius, but adopted by Nazis before and during the WWII to encrypt warfare related data. Enigma was successfully decrypted by Alan Turing [3].

At the end of the 20th century and early years of the 21st, a speedy development in telecommunications, hardware and software occurred while data encryption is happening. Things are getting smaller and smaller, more powerful and even cheaper, bringing computing closer to everyone, appealing not only to businesses but to individuals as well. The Internet expansion and availability also helped on all these objects to be interconnected and made information publicly available.

[2] https://en.wikipedia.org/wiki/Enigma_Machine

[3] https://en.wikipedia.org/wiki/Alan_Turing

The rapid growth of electronic business was used even for criminal acts, stimulated the need for protecting computers, networks and information.

2.2 Information Security Definition

Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security counter-measures of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within or outside the organization's perimeter) and consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats. (Hilton & Cherdantseva, 2013)

Information security is built around the three main pillars of CIA triad: Confidentiality, Integrity and Availability of IT frameworks and to the applicable information setting the targets that:

- is revealed to authorized parties (**Confidentiality**)
- is not subject to unapproved modification of information (**Integrity**) and
- information is accessed by authorized parties when requested (**Availability**).

2.3 The CIA Model

The Confidentiality, Integrity and Availability triad (CIA triad), is a model that was built to guide policies for information security within an organization. The model is also sometimes referred to as the CIA triad (Confidentiality, Integrity and Availability). These three pillars are considered the three most crucial components for security.

2.3.1 Confidentiality

Confidentiality is equal to privacy. Sensitive information is prevented from reaching the wrong people, while making sure that the right people can in fact receive it. Access must be provided to the authorized to view the data.

Some examples of practices used to ensure confidentiality is data encryption include bit not limited to, user names and passwords, two-factor authentication, biometrics, security tokens, hardware and soft tokens, etc.

2.3.2 Integrity

Integrity means maintaining the consistency, accuracy, and reliability of data over its entire life cycle. Data must be altered only by authorized people.

Measures include file permissions and user access controls, version controlling maybe used to prevent erroneous changes or accidental deletion by authorized users, which is a problem as well, checksums and cryptographic checksums for integrity verification; backups must be available to restore the data at its original state in case of permanent loss.

2.3.3 Availability

Availability means maintaining the service always available, offering adequate bandwidth and preventing network bottlenecks are equally important, redundancy and disaster recovery to ensure systems availability. Backup copies should be stored in a different location from the original data storage, firewalls IDS and proxy servers can be used to prevent intruders.

It is critical to comprehend that Data Protection Act prerequisites go beyond the traditional way or transmitted and stored data. he seventh data protection guideline identifies security requirements on collecting, storing and processing of personal data.

So, the security measures you put in place should seek to ensure that:

- only authorized people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

Organizations need to make sure that

- make sure you have the right physical and technical security measures to ensure data protection
- have in place all relevant processes and procedures to cope with security breaches cases

- when never new applications are being designed, security and privacy need to be taken in to account from the very beginning
- they keep track of the data sharing across the departments or/and with external parties if needed
- backup policies to be in place to ensure that data recovery will be successful
- make sure that all employees are aware of cyber threats and actively following any security plan
- have a data retention policy that allows them to destroy unneeded or “expired” data
- comply with all regulatory authorities
- at least follow and ensure the CIA triad

There are so many threads that need to be considered when coping with Information security. In *Table 1 : IoT security threats*, I am trying to summarize the most important ones.

Table 1 : IoT security threats

Security issue	
Insecure Web interface	Account Enumeration Weak Default Credentials Credentials Exposed in Network Traffic Cross-site Scripting (XSS) SQL-Injection Session Management Weak Account Lockout Settings
Insufficient Authentication/Authorization	Lack of Password Complexity Poorly Protected Credentials Lack of Two Factor Authentication Insecure Password Recovery

	Privilege Escalation Lack of Role Based Access Control.
insecure Network	Vulnerable Services Buffer Overflow Open Ports via UPnP Exploitable UDP Services Denial-of-Service DoS via Network Device Fuzzing.
Lack of Transport Encryption	Unencrypted Services via the Internet Unencrypted Services via the Local Network Poorly Implemented SSL/TLS Misconfigured SSL/TLS.
Privacy Concerns	More than the critical to the functionality data are collected Collected sensitive data Data are not anonymized Unencrypted data collection Unprotected personal information Unauthorized access to personal information No retention policies applied
Insecure Cloud Interface	Account Enumeration No Account Lockout Credentials Exposed in Network Traffic.
Insecure Mobile Interface	Account Enumeration No Account Lockout Credentials Exposed in Network Traffic.
Insufficient Security Configurability	Lack of Granular Permission Model Lack of Password Security Options No Security Monitoring No Security Logging.
Insecure Software/Firmware	Not updated devices Unencrypted file updates Unencrypted connection transmissions

	Ensuring the update file does not expose sensitive data Unsigned and unverified updates
Poor Physical Security	USB Ports available on devices Storage Media available on devices

2.4 Security elements

For the security domains, it’s important to identify key elements for the information security. In the following sections, the key elements definitions are described.

2.4.1 Asset

Asset is any datum, device, or in general any module of the organization’s universe that supports information-driven processes. Assets can include hardware, software and information as well. Assets should be always protected under the CIA triad framework

2.4.2 Threat

In computer security, a threat is anything that can possibly make a damage. A danger is something that could possibly happen, or not. Dangers can prompt assaults on computer systems and that's only the tip of the iceberg.

2.4.3 Vulnerability

Any Weaknesses or gap in security mechanisms that can be exploited by threats to benefit from unauthorized access to an asset is a vulnerability

2.4.4 Risk

When a treat threat is exploiting a vulnerability then a risk may be identified, the possibility for loss, damage or destruction of an asset

2.4.5 Exposure

Exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either allows an attacker to conduct information gathering activities or to hide activities.

2.4.6 Countermeasures

Countermeasure indicates any action, device, process, or technique that potentially may lead to reduce threats, vulnerabilities, or any attacks by preventing it or minimizing the damage. Corrective actions need to be taken even if it decided to simply mitigate the risk

2.4.7 Security Policies

Security Policy means the set/rules adopted by an organization to ensure that IT and network infrastructure follows the principles of data security, users are taking all appropriate measures to ensure that the CIA triad is respected when contacting any form of business activity in or out of the organization’s borders

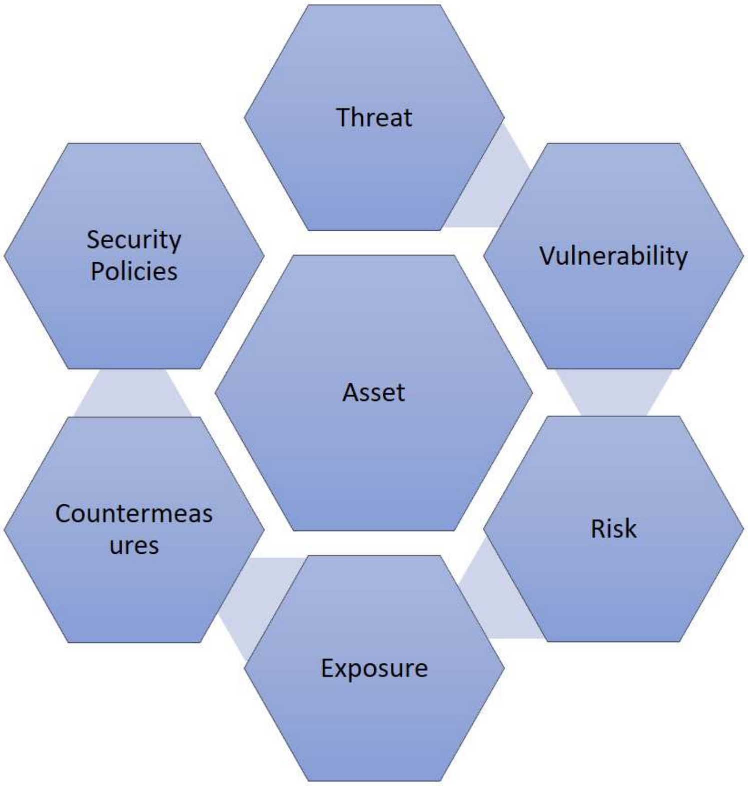

Figure 1 : Security elements

2.5 Summary

Information security is the practice that dictates the physical and logical protection of data which nowadays is an asset. Information security technology helps organizations to acquire, process and store data. Therefore, data protection is essential to achieve CIA principals as described in this chapter. Failure to comply with CIA requirements may lead to financial implications and disciplinary actions.

In this section, a historical background of Information Security is provided, an analysis of CIA triad, analyze security of the elements, countermeasures and security policies while on the next session we will refer to Internet of Things.

Chapter 3
Internet of Things (IoT)

3.1 Background for the Internet of Things

The Internet of Things (IoT) was first used by Kevin Ashton in 1999, (Ashton, 2009) who defines IoT as uniquely identifiable objects (things) and their virtual representations in an Internet-like structure. From a technical point of view, the IoT presents network of uncountable number of global connected objects - devices, sensors or actuators, providing different services over the Internet. Fundamentally, IoT means a shift from reactive to proactive systems; from delayed problem management to automatic sense-and-respond capabilities.

The **Internet of Things (IoT)** has been defined in Recommendation ITU-T Y.2060 (06/2012) (ITU, 2012) as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies".

The most vital part of achieving IoT is communication, is communication. No matter how smart or capable the devices are, if they cannot transmit and communicate then they cannot be a part of the IoT ecosystem. How this communication is performed is less important, since the actual physical and link layer communication within IoT can be realized in many ways.

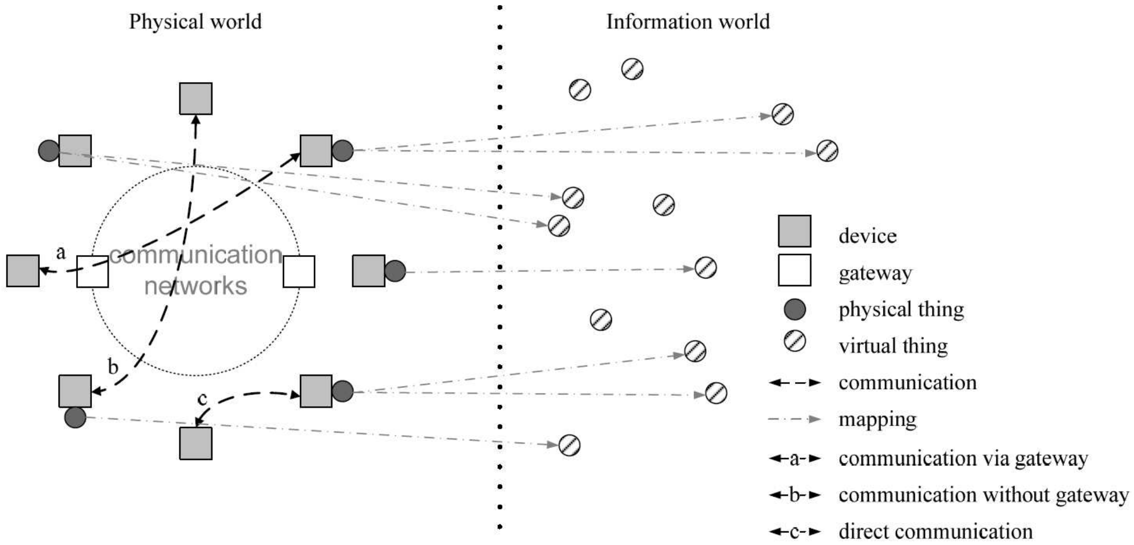

Figure 2: Overview of the Internet of Things (ITU, 2012)

Physical devices can communicate through communication network:

- Through a gateway, for example CCTV cameras that monitor a place
- Without a gateway
- Directly, for example two devices that are close to each other via Bluetooth or ZigBee protocols – smart home devices

A physical thing can be mapped into the information world via one or more virtual things, while virtual things do not necessarily need to be associated with any physical thing. For example, a physical thing might execute multiple applications and thereby have multiple identities in the virtual world.

3.2 Fundamental characteristics

The fundamental characteristics of the IoT are the following:

- Interconnectivity: Anything can be interconnected with the global information and communication infrastructure

- Things-related services: The IoT can provide thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. To provide thing-related services within the constraints of things, both the technologies in physical world and information world will change

- Heterogenicity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks

- Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

- Scalability: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

3.3 IoT Roadmap

It is widely accepted that RFID’s were the ancestors of IoT. Originally used in supply chain industry for tracking purposes, very fast moved to the Vertical market such as security, surveillance, transportation, food safety and others enabled by the network evolution. These days is mainly used for monitoring and controlling of remote or distant objects

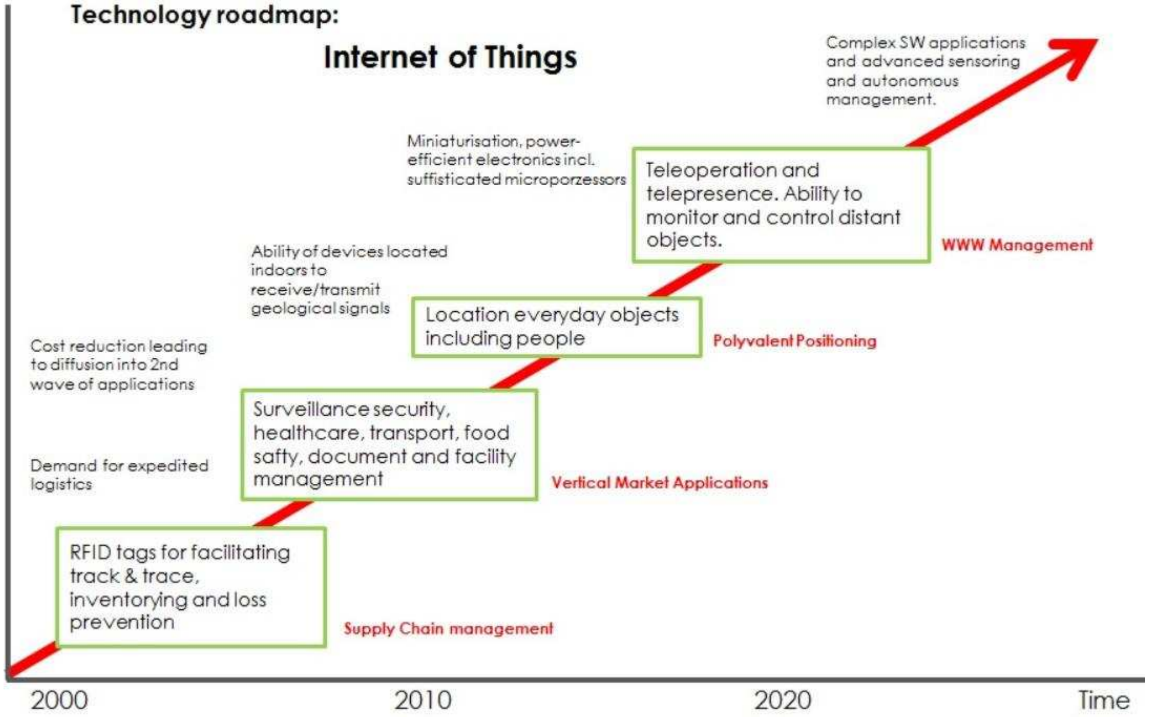
Technology roadmap:
Internet of Things
Complex SW applications and advanced sensoring and autonomous management.
Miniaturisation, power-efficient electronics incl. suffisticated microporzessors
Teleoperation and telepresence. Ability to monitor and control distant objects.
WWW Management
Ability of devices located indoors to receive/transmit geological signals
Location everyday objects including people
Polyvalent Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance security, healthcare, transport, food safty, document and facility management
Vertical Market Applications
Demand for expedited logistics
RFID tags for facilitating track & trace, inventorying and loss prevention
Supply Chain management
2000
2010
2020
Time

Figure 3 : IoT Roadmap

According to the Gartner analysis [4] 8,4 billion IoT devices are expected to be connected by the end of 2017, showing an increase of 31% from 2016, while this number is expected to reach 20,5 billion IoT connected devices by 2020. The total market is expected to reach 3 trillion USD.

3.4 Summary

In this section, we presented the IoT background, analyze the fundamental characteristics and provide the IoT roadmap over the years. In the next section, we will analyze the IoT technologies.

[4] Source : http://www.gartner.com/newsroom/id/3598917

Chapter 4
IoT Technologies

4.1 Introduction

In this chapter, some of the core IoT technologies presented which includes Radio Frequency Identification (RFID), Near Field Communications (NFC) and Wireless Sensor Gateway (WSN).

IoT brings so many new challenges to organizations that may affect "business as usual", while the number of technicalities from an architectural point of view up to system design is increasing. According to Jones (2016) the top 10 IoT technologies for 2017 and 2018 are as following:

- IoT Security
- IoT Analytics
- IoT Device (Thing) Management
- Low-Power, Short-Range IoT Networks
- Low-Power, Wide-Area Networks
- IoT Processors
- IoT Operating Systems
- Event Stream Processing
- IoT Platforms
- IoT Standards and Ecosystems

In the following sections, a description of the common IoT technologies are presented.

4.2 IoT Technologies

There are many technologies involved in IoT implementation and below you may find a reference to the most import ones.

4.2.1 RFID

A. RFID and near-field communication brought into the picture into 2000. RFID technology uses electromagnetic fields to transfer data, for identifying and tracking tags attached to objects. The most well-known use of that technology is the implantation of RFID microchips in pets allowing identification of animals.

4.2.2 NFC

Near Filed Communication is a short-range wireless technology at 13.56 MHz, that requires 4 cm to operate. NFC is currently widely used on smartphones technology enabling digital transactions (credit/debit cards over PoS), exchange of content and connect NFC enabled electronic devices on close range.

4.2.3 WSN

A Wireless Sensing Network (WSN), is a network consisting of distributed autonomous devices using sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Can be used in a variety of applications from military use up to sensing fires in forests and monitoring metrics onto human bodies

4.2.4 IoT Wireless Technologies

Wireless technologies have an important role in the IoT ecosystem for the connectivity and aggregation of IoT devices with the Wireless Sensor Gateway. In the following sections presented the description of the most used wireless technologies.

4.2.5 WiFi

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. Vic Hayes has been named as father of WiFi. It was invented by NCR Corporation in Nieuwege in the Netherland back at 1991. Today, worldwide there are Wi-Fi devices that delivers the high-speed Wireless Local Area Network (WLAN) connectivity to millions of offices, homes, and public locations such as hotels, cafes, and airports and so many. Availing Wi-Fi to notebooks and handhelds devices has pushed Wi-Fi to the point to the point of “defacto” communication protocol based on IEEE802.11 standard.

4.2.6 Zigbee

ZigBee, created by the ZigBee Alliance at 2001, is one of the protocols developed for enhancing the features of wireless sensor networks. It is a low power wireless network protocol based on the IEEE 802.15.4 standards. With range of approx. 100 meters at a bandwidth of 250 kbps, Zigbee devices are deployed star and cluster tree topologies. It is widely used in smart home automation.

4.2.7 Bluetooth

Bluetooth low energy devices that have BLE emended hardware into them can beckon their presence and availability to connect; powered by lithium cell batteries can be up and running for a year.

4.2.8 Z-Wave

A wireless technology that allows smart devices to talk to each other, designed for smart home automation. Is easy and faster for development. Z-wave has full mesh networking capabilities without the need of a coordinator node and is very scalable, enabling control of up to 232 devices.

4.2.9 6LoWPAN

6LoWPAN stands for IPv6 over Low Power Wireless Personal Area Networks. 6LowPAN is a network protocol that defines header compression and encapsulation mechanisms allowing IPv6 packets to be sent and received over IEEE 802.15.4 based networks. It’s specifically developed for low-power devices with limited processing capabilities, which can be able to participate in the IoT.

4.2.10 Lora

LoRaWAN is a Low Power Wide Area Network (LPWAN). LoRaWAN is a media access control (MAC) layer protocol designed for public networks in large-scale with a single operator. It is built using Semtech’s LoRa modulation as the underlying PHY.

4.2.11 Sigfox

Another wireless wide range technology is Sigfox which comes with a range between Wi-Fi and cellular. Sigfox uses free ISM band to transmit data over the very narrow spectrum. Sigfox is designed to handle low data-transfer speeds of 10 to 1,000 bps using an Ultra Narrow Band (UNB) technology.

4.3 Comparison table

In the following table, the pros and cons of the different IoT wireless technologies are presented.

Table 2: Pros and cons of important IoT technologies

	Pros	**Cons**
WIFI	Low cost	High power consumption
	Easy installation	Interferences
	Scalable	Limited range
		Less secure
Bluetooth	Ad hoc Connection	Low data rates
	2,4GHz frequency	Interferences
	Pico nets	Short ranges
		High power consumption
Zigbee	Low power	Low data rate (250Kbps)
	Multiple topologies supported	Expensive
	Up to 2km range	May require regulatory licenses for frequency other than 2,4GHz

	Scalable with less configuration	
Zwave	Ultra-low power	Low data rate (100Kbps)
	Support mesh topology	Limited nodes (232)
	Smart home automation	
6LoWPAN	Low power	Not suitable for big payloads
	Less physical layer overhead	Small packets, 218 bytes, 103 for payloads
	easy to install	
RFID	Low power	Difficulties in reading for fluids or metals
	Not easily replicable, hence secure	Invasive technology
Thread	Simple for retail	Not suitable for low bandwidth devices
	Secure	Only for home automation
	Open protocol	
	Mesh topology	

4.4 Summary

In this chapter, we discuss the IoT technologies and provide more details on the most important technologies. At the end, a comparison table showing pros and cons for the respected technologies is provided. On the next chapter, the IoT architecture is provided.

Chapter 5
Architecture for IoT

4.1 IoT reference model

In the early years of IoT the reference model was illustrated by a three-tier model having on the bottom the physical layer, on top of that the transport (network) layer and the far top the application layer. But as years elapsed, more layers are being added as shown in the following figure:

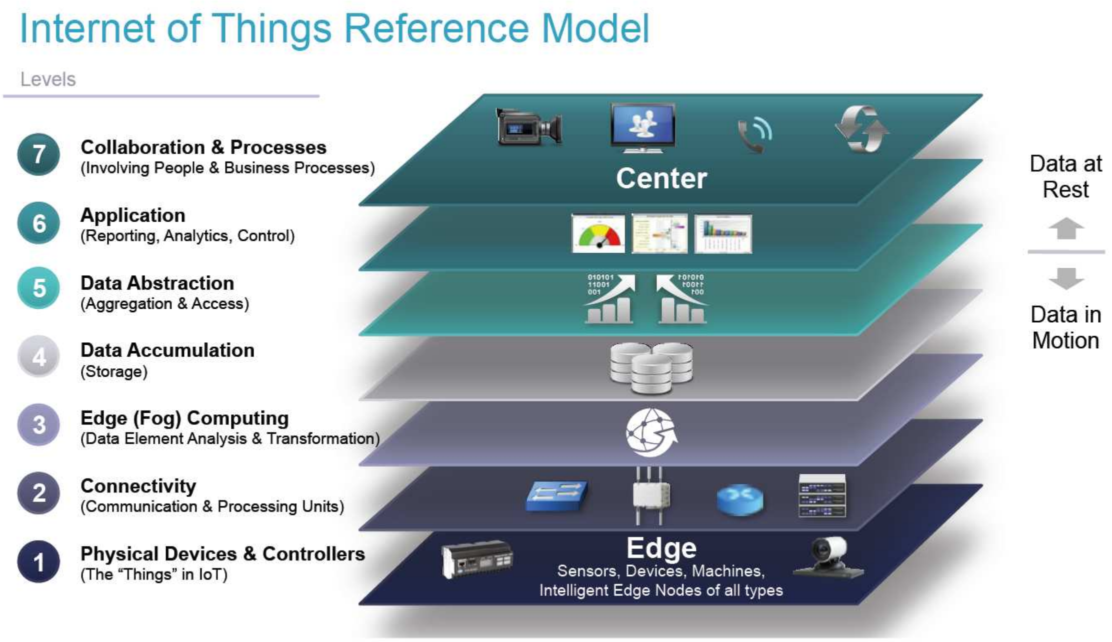
Internet of Things Reference Model
Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
Data at Rest
Data in Motion

Figure 4 : IoTReference Model (Cisco, 2014)

- Level 1

The Model starts with Level 1: physical devices and controllers that might control multiple devices. These are the “things” in the IoT, and they include a wide range of endpoint devices that send and receive information. Devices are diverse, and there are no rules about size, location, form factor, or origin. Some devices will be the size of a silicon chip. Some will be as large as vehicles. The IoT must support the entire range.

- Level 2

  Communications and connectivity level. Major objective of this level is reliability, and timely transmission between devices, across and between networks

- Level 3

  Many devices may generate tens of information within a time window and the complete set of information may be not needed to be transferred to other levels e.g. a room temperature sensor. These types of information may need to be remain within the fog computing [5]. Main activities performed here are data evaluation formatting, decoding/decrypting, basic calculations (e.g. summarizations), assessments/thresholding

- Level 4

  Data Accumulation and data at rest activities are performed. Here its decided if data need to be stored to become available to applications, or to be transferred to upper levels. Event-based data are converted to query-based processing data, in order differences between the real-time networking world and the non-real-time application world bridged.

- Level 5

  Data abstraction functions are executed to render data in such a way to make them available to applications. Reconciliation, assurance, completeness checks and consolidation activities are performed

- Level 6

[5] Also known as Edge Computing or fogging, fog computing facilitates the operation of compute, storage and networking services between end devices and cloud computing data centers (webopedia, n.d.)

The application level where information interpretation occurs. Data at rest from previous level are being processed from applications. No much work needed here as levels 1-5 have done the work properly. The users are expected to do their work much better and easier

- Level 7

  Here is where IoT data interact with humans and processes. Data from previous levels are not useful at all, unless actions are triggered based on business logic

4.2 IoT Frameworks and Standards

One of the most important issues that a researcher must study is the lack of standardization mainly due the great number of vendor offering different devices ready to be adopted by IoT architecture. Moreover, IoT architecture is not yet standardized and therefore several models are currently available. A reference of available standards from various international organizations is provided on Appendix 1.

4.2.1 Six Layered Architecture

Xu Cheng et.al (2017) was proposed a six-layered architecture based on the network hierarchical structure as shown in the following figure

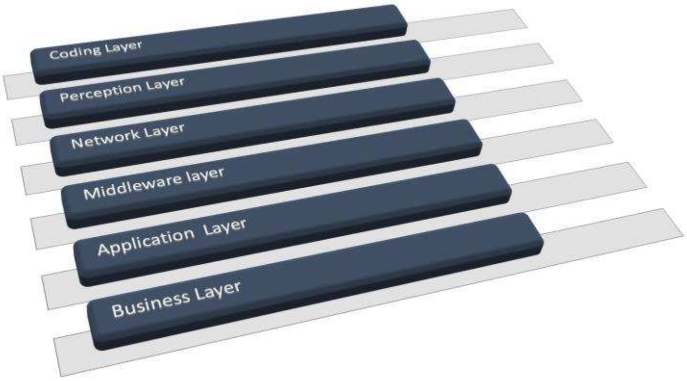

Figure 5 : Six (6) layer IoT Architecture

- **Coding Layer**: Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to identify the objects.

- **Perception Layer:** This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc. of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

- **Network Layer**: This layer receives the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems, present in the Middleware Layer through the transmission mediums like WiFi, Bluetooth, WiMAX, Zigbee, GSM, 3G etc. with protocols like IPv4, IPv6, MQTT, DDS etc.

- **Middleware Layer**: It processes the information received from the sensor devices which includes the technologies like Cloud computing, Ubiquitous computing ensuring a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

- **Application Layer**: This layer realizes the applications of IoT for all kinds of industry, based on the processed data. This layer is very helpful in the large-scale development of IoT network. The IoT related applications could be smart homes, smart transportation, smart planet etc.

- **Business Layer**: It manages the applications and services of IoT and is responsible for all the research related to IoT. It generates different business models for effective business strategies.

4.3 Summary

Different IoT architecture presented in this chapter described the main characteristics for each level. In the next chapter, the security requirements are presented for each level of the IoT architecture with the security technology challenges.

Chapter 6
Security in IoT

6.1 Introduction

Any IoT implementation requires substantial amount of technologies to be able to support the offered services in terms of software, hardware, and network as well. There are many challenges need to be analyzed when we are talking about security of an IoT environment.

- The biggest challenge in IoT world is the objects themselves, either physical or virtual. By nature, IoT is based on the development of objects as much as possible and the more objects we have the more potential problems may have. Tens of years back we had only to protect our PC to access the internet, now we need to care about PCs, Smartphones, smart devices, car, wearables, anything practically that is connected over the net.
- The more devices we have the more difficult is to administer them. Firmware updates for devices or OS updates are crucial to maintain the security at a high level. Even the users may be difficult if they have some tens of devices to maintain them updated to the latest security releases
- Communication and information transmittal. Regardless of the number of IoT devices the information that is being captured need to be somehow transmitted to the next level for further processing. Authentication and privacy protection should be a fundamental element of IoT security while encryption needs to be applied
- Unauthorized access to smart devices
- Security was left aside for some devices, even a couple of years back from vendors that did not take any consideration about security and offered to the public unprotected devices

- Lack of experience and lack of expertise may be the backdoor to security breaches A smart refrigerator that can report that the milk is finished for a mean consumer is a major step forward, but, on the other hand, this smart device if it's not properly maintained can be compromised and offer access to other connected devices on the same network.

To solve these challenges, there are hundreds of available solutions for implementation which actually make things fuzzier; from proprietary protocols in IoT, ZigBee and Z-Wave, to protocols well established and supported widely like TCP, IP, HTTP or SMTP and open standards from IEEE, IETF or W3C for standardized protocols like 6LowPAN or CoAP.

A set of several studies were considered to stipulate the following summarization for security requirements, challenges, threats and potential solutions ((Farooq, 2015), (Huang, 2015), (Nguyen, 2015), (Commission., n.d.), (Arseni, 2015), (Anon., 2012), (Polk, 2011))

Table 3 : Extended CIA model

Requirement	Details
Authenticity	Only legal users should be allowed to access the system or sensitive information
Authorization	The privileges of device components and applications should be limited as so they are able to access only the resources they need to do their addressed tasks
Confidentiality	Information transmission between the nodes should be protected from intruders
Integrity	Related information should not be tampered [

Availability and Continuity	To avoid any potential operational failures and interruptions, availability and continuity in the provision of security services should be ensured

Security Threats

For each IoT protocol layer, different threats and risks are presented. In the following table, the risks for each IoT layer described.

Table 4 : Security threats

Layer	Risks
Perception	Spoofing, signal jamming, outage, eavesdropping
Network	Wormhole, forwarding, man in the middle, floods
Support	Dos, unauthorized access, data tampering
Application	Sniffers/loggers, DDoS, social and session hijacking, injections

IoT attacks

Since IoT devices are exposed in Internet there are many types of attacks that described in the following table.

Table 5 : IoT attacks

Attacks	Risks
Spoofing	Authenticity, integrity and confidentiality
Signal/Radio Jamming	Availability and integrity

Device-tampering/Node-capturing	Availability, integrity, authenticity and confidentiality
Path-based DoSAttack	Availability and authenticity
Node Outage	Availability and authenticity
Eavesdropping	Confidentiality

Cryptographic Algorithms

For the secure communication protection between IoT devices and network there are developed different symmetric or asymmetric cryptography algorithms as presented in the following table.

Table 6 : Frequently used Cryptographic Algorithms

Type	Algorithm	Purpose
Symmetric Encryption	Advanced encryption standard (AES)	Confidentiality
Asymmetric Encryption	Rives Shamir Adelman (RSA)/Elliptic curve cryptography (ECC)	Digital Signatures, Key Transport
Asymmetric Key Agreement	Diffie-hellman (DH)	Key Agreement
Hashing	SHA-1/SHA-256	Integrality

6.2 IoT Protocols related to Security

In the previous chapters a detailed analysis of IoT protocols presented. For the security purpose, I have selected the most appropriate important IoT protocols to be analyzed and compared them. All these protocols are assigned to the transport or application layers of IoT protocol stack.

6.2.1 DTLS

Datagram Transport Layer Security (DTLS) is a protocol that provides security for datagrams. The protocol is based on the TLS protocol to offer similar security.

Although it was designed for security. researchers from Royal Holloway, University of London in 2013, managed to recover plaintext from a DTLS connection using the OpenSSL implementation of DTLS when Cipher Block Chaining mode encryption was used.

6.2.2 QUIC

Quick UDP Internet Connections (QUIC) uses the User Datagram Protocol (UDP) and support a group of composite connections that are present in between two endpoints. QUIC could give the security protection just like Transport Layer Security or like Security Sockets Layer with the feature of minimizing transport latency and no of connections. QUIC is also designed to estimate the bandwidth in either direction so that congestion problem should be avoided.

6.2.3 CoAP

Constrained Application Protocol (CoAP) is an Internet Application Protocol for controlled devices defined by RFC 7228, extended by RFC7252 for IoT applications. CoAP is designed in such way to avail different devices to operate on a constrained network and between devices on different constrained networks all interconnected by internet. CoAP is also used SMS on mobile communication networks for SMS.

CoAP is designed to translate to HTTP for web integration, to support multicast, offer low overhead, and simplicity, services very critical to IoT. CoAP runs on a variety of devices supporting UDP like protocols.

6.2.4 MQTT

Message Queue Telemetry Transport (MQTT) is a light-weight messaging protocol specially designed for IoT and M2M communication introduced by Andy Stanford-Clark and Arlen Nipper in 1999. designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The requirements were to minimize bandwidth and device resource requirements, while making sure reliability and assurance of delivery will be catered as well. These make MQTT ideal for IoT and M2M environment. Security was also implemented in V3.1 where user name and password could be passed. Encryption is implemented with SSL.

MQTT working model is based on Publisher/Subscriber mode (see *Figure 6 : MQTT working model*) which means that a publisher makes available a set of information through a broker, who makes this information accessible to the ones that are interested for (subscribers).

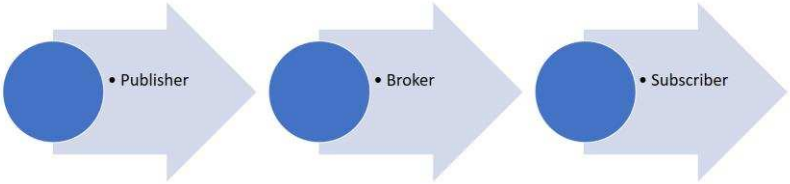

Figure 6 : MQTT working model

6.2.5 JSON

JavaScript Object Notation or JSON uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types, it was introduced by Douglas Crockford in 2000 and defined by RFC 7159. It is a very commonly used for asynchronous communication and is a language-independent. It was originally derived from JavaScript, but many programming languages are handling JSON-format data structures.

6.2.6 CBOR

Concise Binary Object Representation (CBOR) is a binary data format based on JSON and defined by RFC 7049, that results in compact message size. It is used for the CoAP Internet of Things protocol.

In the following table, a comparison between the two most important security protocols for IoT being used, is presented:

Table 7 : Comparison between the two most important security protocols

Features	**QUIC**	**DTLS**
Layer	Transport	Transport
Security	Yes	Yes
Interoperability	Yes	Partial
Objective	Composite connections	Communication privacy for UDP
Delivery	Not guaranteed	Not guaranteed
UDP	Yes	Yes

6.3 Summary

In this chapter, the security n IoT is discussed providing more details on the IoT protocols related to security. In the next chapter, a distributed security mechanism for IoT is proposed.

Chapter 7
Proposed Distributed Security Mechanism (DSM) for IoT systems

7.1. Introduction

In the previous chapter, the layered architecture for IoT associated with the security mechanisms and the IoT security needs presented. IoT security spans over multiple layers, such as applications, networks and perception layers.

Nowadays, the research addresses the security mechanisms between the devices and not the complete end-to-end path. This gap is covered in this thesis with the development of a Distributed Security Mechanism (DSM).

Relevant security research is trying to cope with IoT security:

- A security mechanism developed by Doukas et.al. (Doukas, 2012) provided a good base for securing IoT devices. However, it does not cover the entire path and it leaves a security gap between the device and the WSN gateway.
- Another mechanism proposed by Vucinic et.al. (Vuˇcini´c, 2015) was designed with heavy resources management offered a DTLS-based security. This mechanism, applied a data object encryption inside a data transmission payload. The security of data objects is provided with symmetric encryption by an extra protection layer for the data communication.
- Kumar et.al (Kumar, 2016) used minimal code size and memory consumption for using DTLS mechanism. In the following sections, a conceptual design and the implementation flow of a distributed security is presented.

In this chapter, a distributed end-to-end security mechanism provides a symmetric encryption for data objects combined with the native wireless security to offer a layered security technique between the IoT device, WSN gateway and Web Server. The WSN gateway provides additional protection by securing data using Transport Layer Security (TLS).

IoT devices have a vital important role in the IoT ecosystem but due to limited resources there are few protocols and standards they can support. The Internet Engineering Task Force (IETF) has developed protocols and standards to support IoT devices such as Datagram Transport Layer Security (DTLS) and Constrained Application Protocol (CoAP) as described in the previous chapters.

In the next sections, the conceptual design of the proposed DSM mechanism is presented in detail.

7.2. Conceptual design

The proposed design covers three IoT components: The IoT device, the WSN gateway, and the Web Server. The proposed solution secures data communication in IoT devices using an AES-128 symmetric encryption to data between the IoT device and the WSN gateway. Then, the data are formatted in JavaScript Object Notation (JSON) and sent as a CoAP or HTTP-POST to the WSN gateway. Data is encrypted using a secret public key and can be decrypted with the same public key. This public key is shared with the destination, and the Web Server.

Wireless communications between IoT device and the gateway are secured at the Data Link Layer, using wireless standards such as IEEE 802.15.4 and protocols such as a Low Power wireless personal area network (6LoWPAN), that are capable of supporting AES 128-bit symmetric encryption. These standards are described in detail in Appendix 1. By using a PSK-shared key, only authorized devices are connected to the network and can receive traffic. By encrypting data objects at the device level (perception layer), only the device and the destination will be able to read the encrypted data. In the following paragraphs, the device-to-gateway security and the gateway-to-Internet security is described.

7.2.1.Device - to WSN Gateway security

For this communication part, the security can be achieved by using hardware based symmetric encryption in the Data Link Layer (DLL). Wireless transmission can be provided using ZigBee or 6LoWPAN interface modules. When connecting to the network, devices are secured with a PSK which is installed on each authorized device, and it is required for initiating communication between WSN gateway and the IoT device. Any unauthorized devices will not be able to decrypt data without the correct PSK.

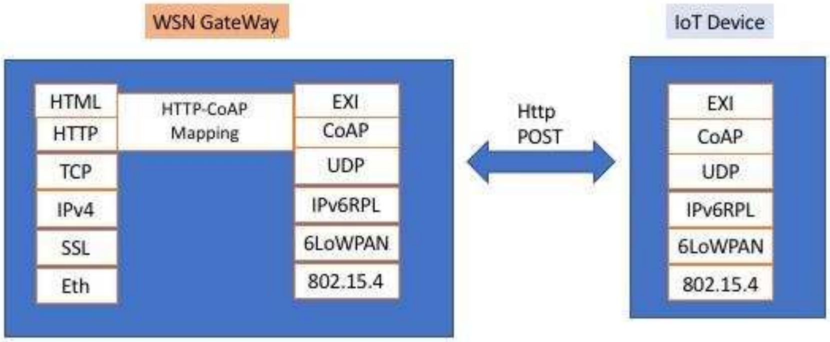

Figure 7:IoT device- WSN Gateway Connectivity

Confidentiality is assured between the IoT device and the destination by encrypting data at the object level. Object layer security exists at the application layer inside the payload of a transmission packet. Objects in this context refer to a container of information, which has been formatted to be human readable. Different formats exist for the Web including JSON and XML.

This level of encryption is used as a primary layer of protection and it can be combined with the offered wireless security for stronger security between the IoT device and the WSN gateway. It works as a second protection level in case of wireless network compromised.

Security is applied at the Data Link Layer (DLL) in the form of hardware based AES encryption secured with a PSK. The second layer of security, is applied only to the contents of the data object. Addressing and source information remain not encrypted in this layer. The data object is encrypted with a symmetric key, which has only been shared with the server, so that no intermediaries will be able to decrypt the data.

7.2.2.WSN Gateway to Internet Security

WSN gateways are devices with enough resources to run operating systems and protocols necessary to securely transfer traffic across the Internet. A WSN gateway, may take the form of a microcomputer with a Linux-based operating system. The gateway has sufficient resources to apply heavy security and communication protocols that cannot be supported by IoT devices. Once data received by the gateway, they are processed and prepared for transmission to the remote server. The gateway is configured with Secure Socket Layer (SSL) tools, which are used to create a secure HTTPS connection between the gateway and the server. Gateway can forward secure communication to the server over the Internet using the configured secure socket layer.

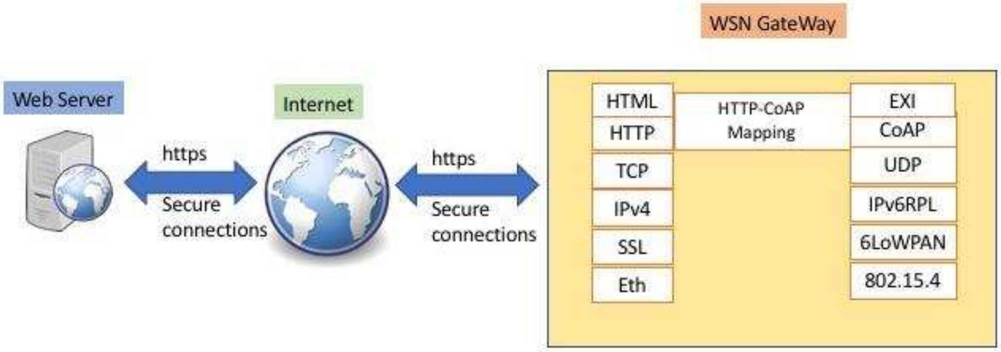

Figure 8 : WSN Gateway – Internet Connectivity

The gateway acts as an intermediate with many resources to support these security measures and secure data before sending it over the Internet. Data sent from the IoT device, will be sent to the gateway using protocols such as CoAP and HTTP and sent across the Internet using HTTPS (HTTP over TLS) to the web server. In the proposed security mechanism, the payload of the packets is formatted as a JSON object and encrypted using AES 128-bit symmetric encryption. This data object will exist inside the transmission payload, while the packet header information such as source and destination address, remains unencrypted.

The JSON object is not readable by the gateway or any other entity other than the intended destination. Similarly, if the server sends a command back to the device, the data object is encrypted using the pre-shared symmetric key and is forwarded to the device for decryption. Security is applied at the Data Link Layer in the form of hardware-based AES encryption secured with a PSK. Only authorized devices should be in possession of the PSK. The second layer of security is applied only to the contents of the data object. Addressing and source information remain unencrypted in this layer. The data object is encrypted with a symmetric key, which has only been shared with the server, so that no intermediaries will be able to decrypt the data.

7.2.3. Web Server Security

The transmitted messages to the server are encrypted with the server's public key, which is installed in the gateway. Only the server can decrypt messages using its corresponding private key. The private key is located on the server and is not shared with any other device. The detailed flowchart of the proposed security mechanism with the relevant sequential processes that are mapped to the three IoT system components is shown in *Figure 9 : Proposed security mechanism*.

Once HTTPS packets received from the server, they are decrypted using the private key. The encrypted data object can then be decrypted using the symmetric secret key from the originating device.

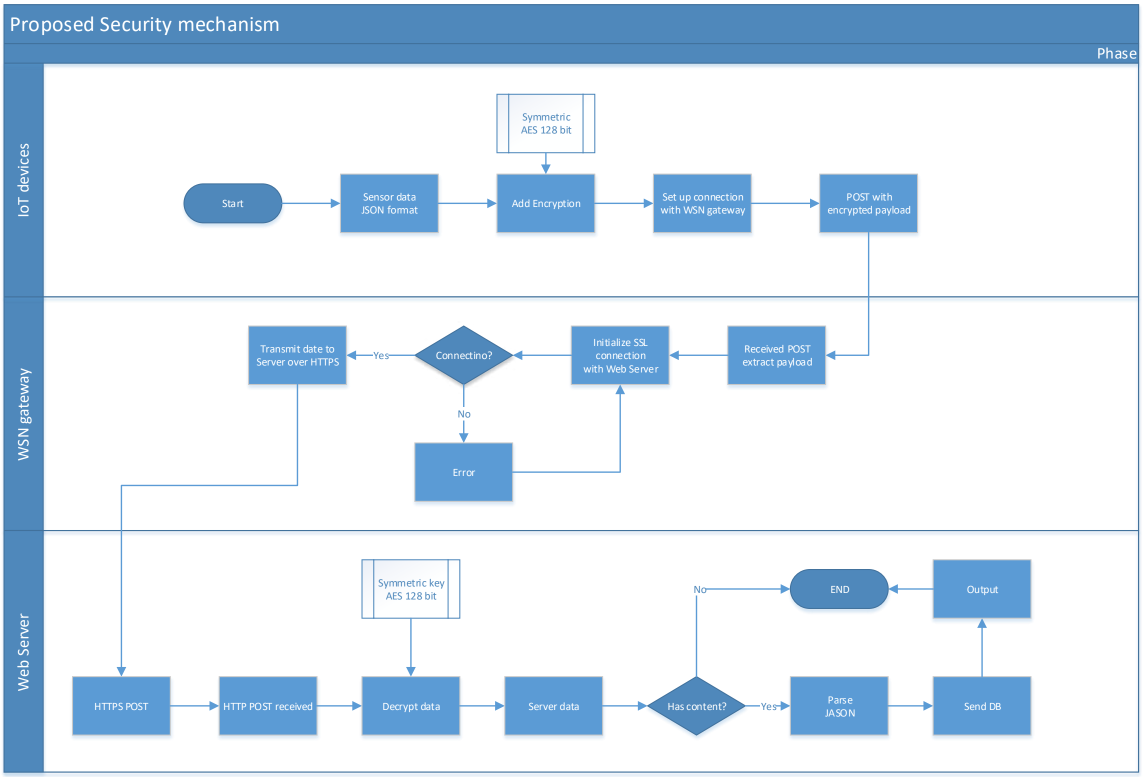

Figure 9 : Proposed security mechanism

If the key is only present on one IoT device and the server, it can be used to authenticate data received from either party. If the key is shared with multiple devices, the devices are authenticated as part of a group. This scenario maintains the confidentiality of IoT data whenever it passes over a public network.

7.3. End-to-End Security Mechanism

In the previous sections the security mechanism is presented distinctly in all IoT path including all systems and platforms. The end to end security path is shown on *Figure 10 : End-to-End Security Mechanism Connectivity*.

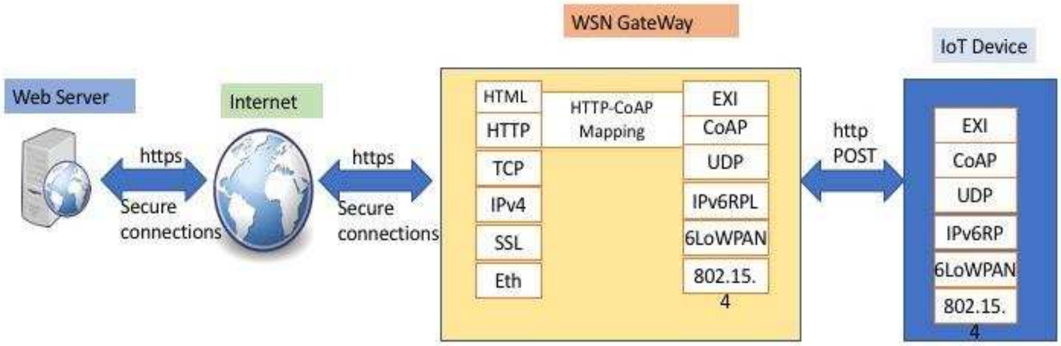

Figure 10 : End-to-End Security Mechanism Connectivity

7.4. Summary

In this chapter, a proposed distribution mechanism is discussed for securing end to end IoT implementations. On the next chapter, we discuss how the implementation was made for the distributed security mechanism.

Chapter 8
Implementation of the proposed DSM security mechanism

The distributed security mechanism (DSM) has been implemented using real-time hardware configurations. This chapter describes the implementation, hardware specifications and configurations of the three IoT system components.

8.1. IoT device setup

For the hardware underlying the IoT device, an Arduino Uno microcontroller was used with an additional Ethernet shield added for connectivity. Arduino was connected directly to a wireless router via an Ethernet cable. A “DHT11” temperature and humidity sensor was connected to the Arduino. The Arduino hardware set up is shown in *Figure 11 : Arduino Uno* microcontroller. The Arduino connects onto and reads data from the sensor and then parses the data into JSON format before encryption. The device automatically begins the sensor reading process as long as device is powered.

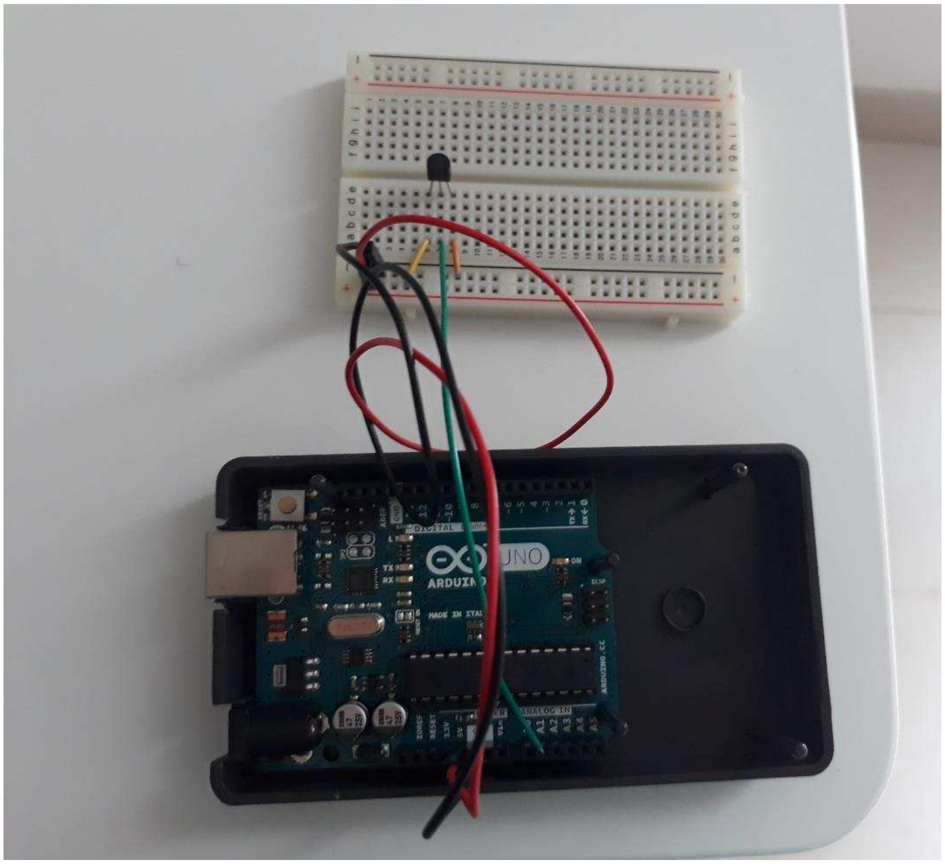

Figure 11 : Arduino Uno microcontroller

The temperature data are parsed as JSON format with 16 bytes length, to match AES requirements. Encryption with AES-128 is taking place. The encrypted output may contain special characters, which are not web-friendly and therefore it is encoded using the Base64 character set.

A web client has been prepared and installed on the Arduino to establish a connection to the IoT gateway. Once a connection is established, the Arduino uses a POST method to send data to the gateway via HTTP. The encrypted data are added to the contents of the HTTP POST before using SEND method. As soon as the POST message is sent, the Arduino receives a response back from the gateway confirming that the POST was received, waits for a period, and then restarts the processes. Receipt confirmation improves the reliability of the connection between the two stations.

The header information contains the destination IP address and the web service address, in our case the “index.php". The encrypted sensor data are added to the contents of the post through the variable “dataEncoded”. If an error is received while attempting to connect to the gateway, the response is read when the POST reaches the gateway. If no errors are received, the connection is established and the packet is sent.

8.2. WSN Gateway Setup

The WSN gateway was built on a Raspberry Pi (Pi) model. The gateway hardware is shown in *Figure 12 : WSN gateway based on Raspberry Pi (Pi*). The Pi is a microcomputer with enough resources to perform security processes that are resource-intensive for the IoT device. The Pi contains a 700-MHz CPU, 512 MB, and a SD card reader that acts as its storage memory. In this case, an 8GB SD card was used for storage. The Pi connects to the wireless router through a wireless USB adapter. The Pi was installed with a PSK to access the wireless network that is secured with AES 256-bit symmetric encryption.

A web application running on Apache web server was installed on the Pi to receive and process data from the IoT device. When a POST is received from the Arduino, the encrypted payload (sensor data) is stripped. The gateway does not contain the symmetric key to decrypt data from the Arduino; however, it just forwards it to the server over a secure connection.

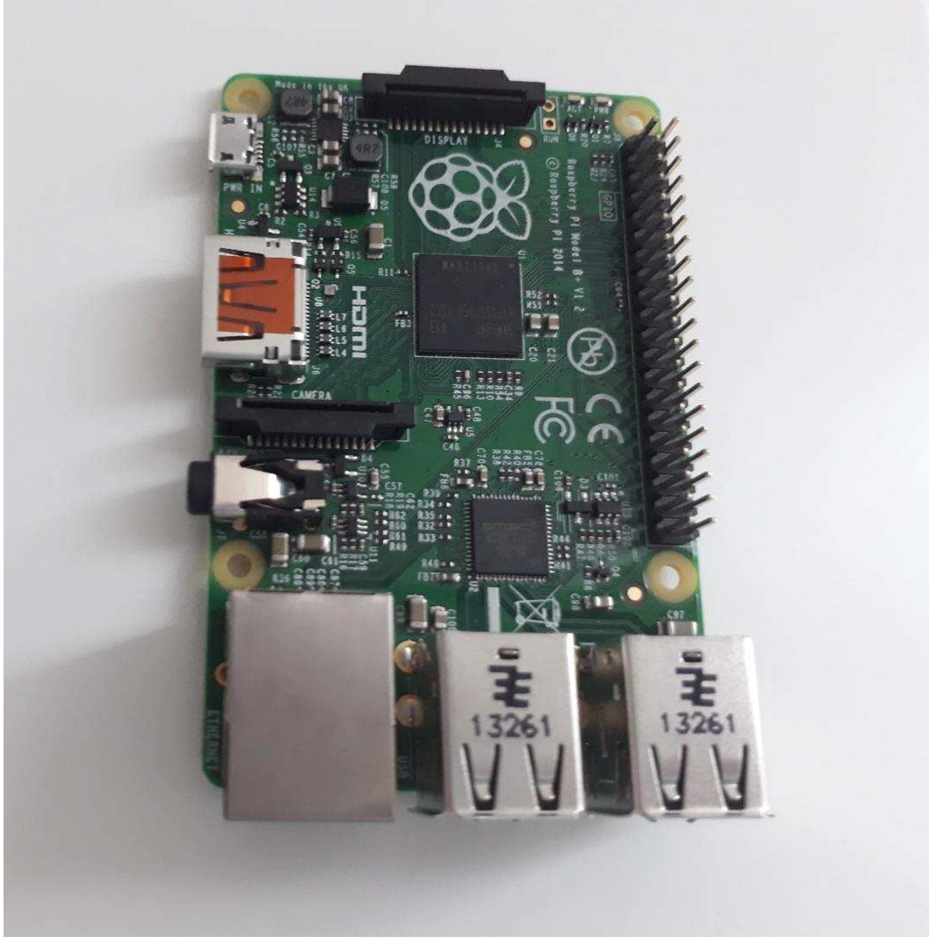

Figure 12 : WSN gateway based on Raspberry Pi (Pi)

The Pi (WSN gateway) connects to the server using SSL connection and posts the data to the server via an HTTPS POST. For testing purposes, the security certificate was not signed by a certificate authority, and therefore, the verification of the certificate with a trusted third party was disabled in the code (VERIFYPEER and VERIFYHOST), to avoid error messages during connections. In a real environment, this is not recommended because the connection may be declined.

8.3. Web Server Setup

For testing purposes, the server was set up on a laptop within an IP address from the local area network. This server, represents the online server to which data would be posted. An Apache web server was installed and configured on the laptop. A security certificate was created, and the server was set up to receive HTTPS connections using SSL/TLS. As soon as the connection is established by the gateway, an HTTPS POST will be sent to the server carrying the encrypted data.

On server side, a web service that handles the decryption process was installed. The cipher text and the symmetric key are passed to the service. The cipher text is decoded from base64 into its original form. Then it's processed using a cipher-text, which is another reference for AES-128. The final stage of the process is to parse the decrypted output and upload it to a database along with the date and the original encrypted message for reference. A web page was also created to demonstrate the working solution. The web page allows the user to view the latest sensor results, which are stored in the database.

8.4. Results

In this section, an example of the captured packet sent from the IoT sensor device, is presented. The captured packet explains the encrypted and not-encrypted data from the sensor. The capturing probe is installed at a point between the IoT device and the WSN gateway.

In *Table 8 : A secured captured packet extract from the IoT sensor* is presented, after it has been transmitted from IoT device and reassembled by the gateway. The packet includes the header information such as the destination and source address. It also includes the encrypted sensor data in the POST contents (i.e., "JonZFcoBlDk8Bf02fCAshsQ==").

Table 8 : A secured captured packet extract from the IoT sensor

```
0000   50   4e   23   25   20   2f   77   83   54   34   76   65   72   6c   39   54
POST/webserver/webclient.php HTTP/1.1

0010 32 23 3c 31 2e 38 30 0d 43 6f 6e 34 23 20 39 2f          Host:192.168.2.1
```

```
0020 65 32 8d 32 42 68 0a 48 6f 23 4b 23 58 46 50 4e           Content -Type:
text/plain

0030 70 6e 69 0a 61 43 5a 47 31 69 59 50 4e 23 25 20      Content-Length:24

0040 20 61 59 3a 48 53 47 2c 90 65 54 18 23 0d 79 3c      JonZFcoBlDk8Bf02fCAshsQ==
```

8.5. Summary

In this chapter, the implementation of the distributed security mechanism to offer end to end security coverage is presented along with the implementation results.

Chapter 9
Conclusion

With the continuous growth of the emerging IoT technologies, the concept of Internet of Things will be inevitably developing on an even larger scale. This emerging technology will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by embedding intelligence into the objects around us. In this thesis, the vision of IoT was discussed and a well-defined architecture for its deployment presented. Then we highlighted various enabling technologies and few of the related security threats and challenges. Finally, we concluded with security practices, implementation action plan and a quick reference check list.

9.1. IoT security action plan

As already stated, many IoT devices aren't built with security in mind, we need to mitigate that risk by having an action plan. Apart from the traditional endpoint measures like firewalls and IPs, we must set aside more:

- Be aware of what is out there for you. Inventory. As soon as you know what and of what type, then a vulnerability assessment can take place to identify potential risks and set a plan to address them.
- Do not have big networks. Separate and isolate if possible parts of your network by using even internal firewalls and access control lists (ACL). Do not allow IoT devices to have direct access to your servers or other mission critical infrastructure.
- Admins. Hackers usually break into workstations and other endpoints as a staging ground to launch more attacks. Frequently change passwords and never use default passwords.
- Patch all connected devices. Patching systems, applications and devices limits the number of exploits and vulnerabilities that an attacker can use to break into other areas of your network from a compromised IoT device

- Monitor the network, Security Information and Event Management (SIEM) tools are becoming increasingly advanced and can monitor for a wide range of anomalies over network traffic. Adding more rules on these tools is an easy task.
- Follow recommendations of Regulatory authorities and various institutions (i.e. IEEE, ITU etc.)
- Employee awareness can help towards boosting IoT security; do not allow everyone in the company to procure such devices without following a set of rules and specifications

9.2. IoT Security Practices

Successful IoT implementations rely on the percentage of benefit they deliver to our life while following a balanced foundation of security, trust, and data integrity to achieve this you need to

- IoT security considerations should be taken into consideration from inception to deployment. Security expenditure needs to be justified against potential losses due to security related incidents
- Eighty percent of IoT applications are not tested for security vulnerabilities before production, according to a report by Ponemon Institute, IBM and Arxan (Larry Ponemon, 2017). This is a huge number of potentially vulnerable exposed devices
- Patch the devices. Many IoT product makers and app developers rely on the end user to install updates and configure security settings, which is transferring the responsibility and accountability to the end user. Companies should be able to remotely push security patches and updates as soon as they're available to prevent vulnerabilities
- Encryption is critical to IoT environment. It shows that a selected IoT vendor cares about security and privacy. HTTPs, HTTP Strict Transport Security, or always On SSL should be the default protocols to work with. Devices should include authentication mechanisms to communicate with back end systems

- Privacy must remain on the top of priorities. End users must be aware of the personal data generated and collected using the devices, what sort of actions are being taken on the collected and stored data along with the disclosure and retention policies. The Recent General Data Protection Regulation in Europe (EU, n.d.) requires verifiable consumer agreement to how each of these three inputs are managed via notice and consent.

9.3. Quick implementation reference card

In *Table 9*, a quick reference card if provided as a check list for secure IoT implementations.

Table 9 : Quick implementation reference card

	Check
Network segmentation is needed to isolate IoT systems from rest IT architecture	
Any data that is beyond the required ones for the operation must be denied, if option is offered	
Any unused physical ports must be disabled	
Alerts and security notifications must be available	
Cloud interfaces, if any, need to be reviewed for security vulnerabilities	
Encryption must be enabled between all solution components	
Minimize the use of ports to the required ones	
All devices must be easily updatable/configurable especially for security issues	
Authorized personnel/users must have access to the devices and the collected information	
Password recovery mechanisms must be secure, if exist	

Use strong passwords	
Enabling two-factor authentication, if available	
SSL/TLS implementations are up to date and properly configured	
Enable lockout mechanism, if available	
Change default usernames and passwords	
Web interface must use HTTPS to ensure maximum protection	
Ensure that update files are signed and then validated by the device before installing	
Ensure that user roles can be properly segregated in multi-user environments	
Force password expiration after a specific period	
Products must be tamper resistant	
Data retention policy must be in place and is well-matching the relevant regulatory authority’s requirements	
Review all required network services for vulnerabilities	

Appendix 1
Standards

Cryptography

The IEEE 1363[6]. The IEEE P1363 project develops Standard Specifications for Public-Key Cryptography. Within this project the following standards are developed.

IEEE 1363-2000: Standard Specifications for Public Key Cryptography [7]

> Specifications include mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys and private keys.

IEEE 1363a-2004: Standard Specifications for Public Key Cryptography - Amendment 1: Additional Techniques [8]

> Additional specifications to IEEE P1363, includes mathematical primitives for secret value (key) derivation, public-key encryption, digital signatures, and identification, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys and private keys.

IEEE Std 1363-2000 and Std 1363a-2004 Revision Project 9

> The standards document IEEE 1363-2000 expired in 2005, an amendment to the standard has been published in the form of Std 1363a-2004. The working group also has the option of making additional technical or editorial changes to the merged document, including adding or removing techniques. This section of the site contains documents relevant to the revision process.

[6] http://grouper.ieee.org/groups/1363/

[7] http://grouper.ieee.org/groups/1363/P1363/index.html

[8] http://grouper.ieee.org/groups/1363/P1363a/index.html

[9] http://grouper.ieee.org/groups/1363/P1363-Reaffirm/index.html

Lattice-Based Public-Key Cryptography (P1363.1)

Specifications based on hard problems over lattices supplemental to those considered in IEEE 1363 and IEEE P1363a, including mathematical primitives for secret value (key) derivation, public-key encryption, identification and digital signatures, and cryptographic schemes based on those primitives.

Password-Based Public Key Cryptography (P1363.2)

Specifications for performing password-based authentication and key exchange, supplemental to the techniques considered in IEEE P1363 and IEEE P1363a.

Identity-Based Public Key Cryptography using Pairings (P1363.3)

Common identity-based public-key cryptographic techniques that use pairings, including mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, as well as cryptographic schemes based on those primitives are specified in this standard. Also, related cryptographic parameters, public keys and private keys, are specified. The purpose of this standard is to provide a reference for specifications of a variety of techniques from which applications may select Devices and sensors/actuators.

Devices and sensors

- IEEE 21451-1-2010 [10]

  ISO/IEC/IEEE Standard for Information technology -- Smart transducer interface for sensors and actuators -- Part 1: Network Capable Application Processor (NCAP) information model. Adoption of IEEE Std. 1451.1-1999. This standard defines an object model with a network-neutral interface for connecting processors to communication networks, sensors, and actuators. The object model containing blocks, services, and components specifies interactions with sensors and actuators and forms the basis for implementing application code executing in the processor.

[10] http://standards.ieee.org/findstds/standard/21451-1-2010.html

- IEEE 21451-4-2010 [11]

  ISO/IEC/IEEE Standard for Information technology -- Smart transducer interface for sensors and actuators -- Part 4: Mixed-mode communication protocols and Transducer Electronic Data Sheet (TEDS) formats. Adoption of IEEE Std 1451.2-1997. A digital interface for connecting transducers to microprocessors is defined. A TEDS and its data formats are described. An electrical interface, read and write logic functions to access the TEDS and a wide variety of transducers are defined. This standard does not specify signal conditioning, signal conversion, or how the TEDS data is used in applications.

- IEEE 21451-7-2011 [12]

  Information technology--Smart transducer interface for sensors and actuators--Part 7: Transducers to RFID systems communication protocols and TEDS formats. ISO/IEC/IEEE 21451-7:2011 defines data formats to facilitate communications between RFID systems and smart RFID tags with integral transducers (sensors and actuators). It defines new TEDS formats based on the ISO/IEC/IEEE 21451 series of standards. It also defines a command structure and specifies the communication methods with which the command structure is designed to be compatible.

- IEEE P24151-1-4 [13]

  Standard for a Smart Transducer Interface for Sensors, Actuators, and Devices - XMPP for Networked Device Communication. The purpose of this standard is to provide session initiation and protocol transport for sensors, actuators, and devices. The standard addresses issues of security, scalability, and interoperability. This

[11] http://standards.ieee.org/findstds/standard/21451-4-2010.html

[12] http://standards.ieee.org/findstds/standard/21451-7-2011.html

[13] https://standards.ieee.org/develop/project/21451-1-4.html

standard can provide significant cost savings and reduce complexity, leveraging current instrumentation and devices used in industry. This standard defines a method for transporting IEEE 1451 messages over a network using XMPP to establish session initiation, secure communication, and characteristic identification between networked client and server devices using device Meta identification information based on the IEEE 1451 TEDS.

- IEEE 2410-2015 [14]

  IEEE Standard for Biometric Open Protocol. Identity assertion, role gathering, multilevel access control, assurance, and auditing are provided by the Biometric Open Protocol Standard (BOPS). The BOPS implementation includes software running on a client device (smartphone or mobile device), a trusted BOPS server, and an intrusion detection system. The BOPS implementation allows pluggable components to replace existing components' functionality, accepting integration into current operating environments in a short period of time. The BOPS implementation provides continuous protection to the resources and assurance of the placement and viability of adjudication and other key features. Accountability is the mechanism that proves a service-level guarantee of security. The BOPS implementation allows the systems to meet security needs by using the application programming interface. The BOPS implementation need not know whether the underlying system is a relational database management system or a search engine. The BOPS implementation functionality offers a "point-and-cut" mechanism to add the appropriate security to the production systems as well as to the systems in development. The architecture is language neutral, allowing REST, JSON, and SSL or TLS to provide the communication interface. The architecture is built on the servlet specification, open SSL, Java, JSON, REST, and an open persistent store.

[14] https://standards.ieee.org/findstds/standard/2410-2015.html

- IEEE P1912 [15]

  Standard for Privacy and Security Architecture for Consumer Wireless Devices. This standard describes a common communication architecture for diverse wireless communication devices such as, but not limited to, devices equipped with NFC, home area network, WAN, WPAN technologies or RFID considering proximity; and specifies approaches for end user security through device discovery/recognition, simplification of user authentication, tracking items/people under user control/responsibility, and supports alerting; while supporting privacy through user controlled sharing of information independent of the underlying wireless networking technology used by the devices.

- IEEE 2600-2008 [16]

  IEEE Standard for Information Technology: Hardcopy Device and System Security. This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users, and others on the selection, installation, configuration and usage of hardcopy devices (HCD) and systems; including printers, copiers, and multifunction devices. This standard identifies security exposures for these HCDs and systems, and instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.

Networking for IoT

- IEEE 802.1X-2010 [17]

  IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control, covering common architecture, functional elements, and protocols for mutual

[15] http://standards.ieee.org/develop/project/1912.html
[16] https://standards.ieee.org/findstds/standard/2600-2008.html
[17] https://standards.ieee.org/findstds/standard/802.1X-2010.html

authentication and secure communication between the clients of ports attached to the same. Port-based network access control allows a network administrator to restrict the use of IEEE 802 LAN service access points (ports) to secure communication between authenticated and authorized devices. This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE MAC Security.

- IEEE 802.1AE-2006 [18]

  IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security, specifies "how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802 LANs to communicate.", amended by IEEE 802.1AEbw-2013 expanding security capabilities. This standard specifies how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802 LANs to communicate. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.

- IEEE 802.1AR-2009 [19]

  Standard for Local and metropolitan area networks – Secure Device Identity, enables the secure association of locally significant device identities with manufacturer provisioned identities for use in provisioning and authentication protocols. A secure device identifier (DevID) is cryptographically bound to a device and supports authentication of the device's identity. Locally significant identities can be securely associated with an initial manufacturer-provisioned DevID and used in provisioning and authentication protocols to allow a network administrator to establish the

[18] https://standards.ieee.org/findstds/standard/802.1AE-2006.html
[19] https://standards.ieee.org/findstds/standard/802.1AR-2009.html

trustworthiness of a device and select appropriate policies for transmission and reception of data and control protocols to and from the device.

- IEEE 11-2012 [20]

  IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications developed by WG802.11 – Wireless LAN Working Group and IEEE 802.15.4-2015, IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).This revision specifies technical corrections and clarifications to IEEE Std 802.11 for wireless local area networks (WLANS) as well as enhancements to the existing medium access control (MAC) and physical layer (PHY)

- IEEE project 15.9 [21]

  IEEE Draft Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams provides guidelines for support of key management in IEEE 802.15.4. A message exchange framework based on information elements as a transport method for KMP datagrams and guidelines for the use of some existing KMPs with IEEE Std 802.15.4™ are defined in the recommended practice. A new KMP is not created in this recommended practice. In support of KMP transmission and reception, a generic multiplexed data service layer that can be used to transmit large packets from the upper KMP to another peer is also provided in this recommended practice. The multiplexed data service provides a fragmentation and multiplexing layer for those packets so they can be delivered over smaller MAC layer frames and multiplexed on the recipient end to the right processing service.

[20] https://standards.ieee.org/findstds/standard/802.11-2012.html

[21] https://standards.ieee.org/develop/project/802.15.9.html

- IEEE 802.21a-2012 [22]

  IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services – Amendment for Security Extensions to Media Independent Handover Services and Protocol. Amendment to IEEE Std 802.21-2008. Extensions to IEEE Std 802.21-2008 are provided for security mechanisms to protect media independent handover services and mechanisms to use MIH to assist proactive authentication to reduce the latency due to media access authentication and key establishment with the target network.

- The IEEE 1888 [23]

  The standard identifies gateways for field-bus networks, data storage for archiving and developing data sharing platforms, and application units as important system components for developing digital communities, i.e., building-scale and city-wide ubiquitous facility networking infrastructure. The standard defines a data exchange protocol that generalizes and interconnects these components (gateways, storage, application units) over the IPv4/v6-based networks. This enables integration of multiple facilities, data storage, application services such as central management, energy saving, environmental monitoring, and alarm notification systems.

Infrastructure systems (note – intranets may incorporate IoT while not necessarily connected to the public internet.)

- IEEE 692-2013 [24]

  IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations, developed by WG 3.2 – Security Systems Working Group addresses security system equipment for “detection, assessment, surveillance, access control, communication, and data acquisition”. Criteria for the design of an integrated security

[22] https://standards.ieee.org/findstds/standard/802.21a-2012.html
[23] https://standards.ieee.org/findstds/standard/1888-2014.html
[24] https://standards.ieee.org/findstds/standard/692-2013.html

system for nuclear power generating stations are provided in this standard. Requirements are included for the overall system, interfaces, subsystems, and individual electrical and electronic equipment. This standard address equipment for security-related detection, surveillance, access control, communication, data acquisition, and threat assessment.

- IEEE C37.240-2014 [25]

  IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. Cybersecurity measures require that a balance be achieved between technical feasibility and economic feasibility and that this balance addresses the risks expected to be present at a substation. Further, cybersecurity measures must be designed and implemented in such a manner that access and operation to legitimate activities is not impeded, particularly during times of emergency or restoration activity.

P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)

This standard defines an architectural framework for the Internet of Things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety." Furthermore, this standard provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. The reference architecture also addresses how to document and, if strived for, mitigate architecture divergence. This

[25] http://standards.ieee.org/findstds/standard/C37.240-2014.html

standard leverage existing applicable standards and identifies planned or ongoing projects with a similar or overlapping scope. (IEEE, 2017)

10 Bibliography

Ashton. K (2009). That internet of things thing. RFiD Journal, 22(7):97–114

Giusto, D. Iera, A, G. Morabito, G, and Atzori, L (2010). The Internet of Things 20th Tyrrhenian Workshop on Digital Communications. Springer New York Dordrecht Heidelberg London.

Sun, G., Huang, S., Bao, W. Y., Yang, Y., and Wang, Z. (2014). A privacy protection policy combined with privacy homomorphism in the internet of things. In Computer Communication and Networks (ICCCN), 2014 23rd International Conference on, pages 1–6. IEEE.

Fink, G.A, Zarzhitsky, D.V, Carroll, T. E, and Farquhar, E. D (2015). Security and privacy grand challenges for the internet of things. In Collaboration Technologies and Systems (CTS), 2015 International Conference on, pages 27–34.

Zhang, R. Zhang, Y. and Ren, K. (2012), "Distributed Privacy-Preserving Access Control in Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1427–1438.

Weinberg, B.D, Milne, G.R, Andonova, Y. G, and Hajjat, F. M (2015) Internet of things: Convenience vs. privacy and secrecy. Business Horizons, 58(6):615–624.

Ndibanje, B. Lee, H.J. and Lee, S.G. (2014), "Security Analysis and Improvements of Authentication and Access Control in the Internet of Things," Sensors, vol. 14, no. 8, pp. 14786–14805.

Stankovic, J.A. (2014). Research directions for the internet of things. IEEE INTERNET OF THINGS JOURNAL, 1(1):3–9

11 References

Anon., 2012. [Online]
Available at: http://www.itu.int/rec/T-REC-Y.2060-201206-I
[Accessed 21 07 2017].

Arseni, S. H. S. F. O. V. A. a. S. G., 2015. *Analysis of the Security Solutions Implemented in Current Internet of Things Platforms..* Romania, s.n.

Ashton, K., 2009. *That 'Internet of Things' Thing - In the real world, things matter more than ideas..* [Online]
Available at: http://www.rfidjournal.com/articles/view?4986

BBC, 2017. *BBC News.* [Online]
Available at: http://www.bbc.com/news/technology-37510502
[Accessed 01 08 2017].

Cisco, 2014. *The Internet of Things Reference Model.* [Online]
Available at: IoT_Reference_Model_White_Paper_June_4_2014-2.pdf
[Accessed 17 17 2017].

Commission., E., n.d. *IoT Privacy, Data Protection, Information Security..* [Online]
Available at:
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753
[Accessed 21 07 2017].

Doukas, C. M. I. K. V. M. F. V., 2012. Enabling data protection through PKI encryption in IoT m-health devices. In: The12thIEEEInternationalConferenceonBioinformatics Bioengineering (BIBE). pp. 25-29.

EU, n.d. *EU General Data Protection Regulation (GDPR).* [Online]
Available at: http://www.eugdpr.org/
[Accessed 03 08 2017].

Farooq, M. W. M. K. A. a. M. S., 2015. A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications. pp. 1-6.

Greeberg, A., 2015. *Hackers Remotely Kill a Jeep on the Highway—With Me in It.* [Online]
Available at: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[Accessed 01 08 2017].

Hilton, J. & Cherdantseva, Y., 2013. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. 09.

http://www.idtheftcenter.org, 2017. *Identity Theft Resource Center.* [Online]
Available at: http://www.idtheftcenter.org/2016databreaches.html
[Accessed 03 08 2017].

Huang, X. C. P. L. H. a. Y. Z., 2015. SecIoT: A Security Framework for the Internet of Things. Security and Communication Networks. Volume 9, pp. 3083-3094.

Huang, X. C. P. L. H. a. Y. Z., 2015. SecIoT: A Security Framework for the Internet of Things. Security and Communication Networks. pp. 3083-3094.

IEEE, 2017. *IoT Architecture - Internet of Things (IoT) Architecture.* [Online]
Available at: https://standards.ieee.org/develop/wg/IoT_Architecture.html
[Accessed 20 08 2017].

ITU, 2012. *itu.int.* [Online]
Available at: http://handle.itu.int/11.1002/1000/11559-en?locatt=format:pdf&auth
[Accessed 9 7 2017].

Jones, N., 2016. *Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018.* [Online]
Available at: http://www.gartner.com/newsroom/id/3221818
[Accessed 2 8 2017].

Koerner, B., 2014. *wired.com.* [Online]
Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
[Accessed 01 08 2017].

KS, A., 2016. *What are the Top 5 IOT Hacks?.* [Online]
Available at: http://electronicsforu.com/technology-trends/must-read/top-5-iot-hacks
[Accessed 01 08 2017].

KS, A., 2016. *What are the Top 5 IOT Hacks?.* [Online]
Available at: http://electronicsforu.com/technology-trends/must-read/top-5-iot-hacks
[Accessed 01 08 2017].

Kumar, S. K. S. T. H., 2016. A hitchhiker's guidetothe(datagram)transportlayersecurityprotocol for smart objects and constrained node networks.

Kushner, D., 2013. *The Real Story of Stuxnet.* [Online]
Available at: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
[Accessed 01 08 2017].

Larry Ponemon, N. J., 2017. *10 Key Findings From the Ponemon Institute's Mobile & IoT Application Security Testing Study.* [Online]
Available at: https://securityintelligence.com/10-key-findings-from-the-ponemon-institutes-mobile-iot-application-security-testing-study/
[Accessed 02 08 2017].

Nakashima, E., 2016. *Washington Post.* [Online]
Available at: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.68c15bead84b
[Accessed 02 08 2017].

Nakashima, K. D. a. E., 2017. *Washington post.* [Online]
Available at: https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.3e20f5274841
[Accessed 01 08 2017].

Nguyen, K. L. M. a. O. N., 2015. Survey on Secure Communication Protocols for the Internet of Things. Ad Hoc Networks. pp. 17-31.

Polk, T. a. T. S., 2011. [Online]
Available at: http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf
[Accessed 19 07 2017].

Sanger, D., 2012. *NY Times.* [Online]
Available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[Accessed 01 08 2017].

Technopedia, n.d. *Internet protocol (IP).* [Online]
Available at: https://www.techopedia.com/definition/5366/internet-protocol-ip
[Accessed 01 08 2017].

Vuˇcini´c, M. T. B. R. F. D. A. D. L. G. R., 2015. Object security architecture for the Internet of Things. Ad Hoc Networks 32(0. pp. 3-16.

webopedia, n.d. *What is fog computing? Definition by webopedia.* [Online]
Available at: http://www.webopedia.com/TERM/F/fog-computing.html
[Accessed 14 07 2017].

wikipedia, 2017. *CBC.* [Online]
Available at: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#CBC
[Accessed 14 8 2017].

Wikipedia, 2017. *CBOR.* [Online]
Available at: https://en.wikipedia.org/wiki/CBOR
[Accessed 17 8 2017].

Wikipedia, 2017. *COAP.* [Online]
Available at: https://en.wikipedia.org/wiki/Constrained_Application_Protocol
[Accessed 17 8 2017].

Wikipedia, 2017. *DTLS.* [Online]
Available at: https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security
[Accessed 11 8 2017].

Wikipedia, 2017. *IPv6.* [Online]
Available at: https://en.wikipedia.org/wiki/IPv6
[Accessed 12 8 2017].

Wikipedia, 2017. *JSON.* [Online]
Available at: https://en.wikipedia.org/wiki/JSON
[Accessed 17 8 2017].

Wikipedia, 2017. *UDP.* [Online]
Available at: https://en.wikipedia.org/wiki/User_Datagram_Protocol
[Accessed 12 8 2017].

Wikipedia, n.d. *6LoWPAN.* [Online]
Available at: https://en.wikipedia.org/wiki/6LoWPAN
[Accessed 3 8 2017].

Wikipedia, n.d. *Barnaby Kack - Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Barnaby_Jack
[Accessed 02 08 2017].

Wikipedia, n.d. *Mirai (malware).* [Online]
Available at: https://en.wikipedia.org/wiki/Mirai_(malware)#cite_note-29
[Accessed 01 08 2017].

Wikipedia, n.d. *Stuxnet - Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Stuxnet
[Accessed 01 08 2017].

Xu Cheng, M. Z. F. S., 2017. *International Journal of Engineering Trends and Technologies,* Volume 47, pp. 381-381.

Zetter, K., n.d. *An Unprecedented Look at Stuxnet, the World's First Digital Weapon.* [Online]
Available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[Accessed 01 08 2017].