Faculty of Sciences and Technology
Department of Informatics Engineering

IOT SECURITY ASSESSMENT

IoT Security Assessment in an IoT Smart City Scenario

Armando José Martins de Oliveira

Dissertation in the context of the Master in Informatics Security,
advised by Professor Edmundo Monteiro and presented to the
Faculty of Sciences and Technology / Department of Informatics Engineering

September 2019

1 2 9 0

UNIVERSIDADE Ð
COIMBRA

Abstract

Although IoT is not a new concept, it was not until recent years that we have seen strong adoption of it. As with any other recent and unproven technology, there is still a lack of consensus around it, resulting in a lack of standards and frameworks allowing the creation of architectures and models that would permit a common view and interoperability between all IoT stakeholders. This undefinition also impacts security as there is also a lack of common standards and best practices for IoT security. One possible approach to IoT security and the one that is more obvious is the adoption of global accepted “traditional ICT” security frameworks. But it is still not clear at this point if this approach will fit and will be adequate to all IoT particularities and scenarios. The main objective of this work is to apply a security risk assessment methodology to specific IoT use case in the domain of smart cities. This will permit to understand what challenges today’s IoT systems in the domain of smart cities face in terms of security, to find what are the main security risks these use cases, what traditional security controls could mitigate these risks and what are the possible constraints when applying traditional security controls to the IoT scenario.

The methodology used to formulate these conclusions is composed of several steps. First on a research of the state of the art of IoT security, reviewing the work done, in this area, by the most known entities in the information security domain. Second, on a definition of an IoT use case scenario that will be the testing environment to the next phase. Third, in the use of a risk assessment framework to assess the risks that the IoT scenario will face and treatment of those risks using “traditional ICT” security controls. Finally in the identification of possible problems that IoT characteristics pose when applying these controls.

The contribution of this work is, a summary of the main IoT characteristics and the IoT security concerns identified by some research work in this domain, the identification of the security risks present in a traffic management scenario and possible security measures to mitigate these risks and the identification of possible problems when applying security measures to mitigate these risks and important what risks cannot be mitigated with today’s security controls due to IoT specific characteristics.

Concerning the state of the art in IoT security the main conclusions are that currently, there is a strong effort from different entities to progress in this area of IoT. Nevertheless, all the works reviewed, state that there are still many problems to achieve this. First it is important to define common standards and common approaches in the architectures, protocols, platforms, that will allow a solid definition recommendation for IoT security. Nowadays each stakeholder is employing their own approach resulting in a weak posture in security, fragmentation in models, and incompatibility between solutions. Another aspect that can influence IoT security is that IoT has some specific characteristics that can bring new threats and add new vulnerabilities. As an example, IoT devices are more limited in terms of resources, restricting the security features that can be implemented, being cryptography one of this security features.

Some other areas that support the development of IoT security, like laws, regulations, auditing and compliance, are also being explored. In the case of laws and regulations, it was been seen some efforts from some governments in the definition of laws and regulations adapted to the IoT case, trying to set up a baseline of security best practices. In the case of security auditing and compliance of IoT environments, there is nothing very specific for the IoT case and common methodologies are used.

IoT is going to be part of many of our future day to day life is, and it is vital that security is on the top of our concerns. More critical are the scenarios where human safety can be jeopardized by a lack of IoT security. The strong physical component of IoT can add additional attack vectors to human safety. One of the important use cases for IoT are Smart Cities. IoT will enable this new concept of cities that are more efficient and functional. However, Smart Cities will inherit the security issues of IoT. It is crucial then to assess the concrete overall risks and more specifically, cybersecurity risk that these new cities will encounter and what type of measures can be used to overcome these risks. Imagine the scenario where a traffic management solution of a smart city is hacked and attacked putting in danger the lives of people or merely causing the chaos in traffic.

The security risks present in the specific scenario and at some extend, to the IoT case, are different from the risks present in traditional ICT. For example, IoT scenarios are more concerned with integrity and availability that with confidentiality and physical security is a bigger concerned in these types of scenarios. When it comes to security controls, IoT is not adopting correctly the best practices already in use in traditional ICT. The security development best practices are an example. Also, applicability of traditional security controls to IoT can be more difficult as specific characteristics of IoT don't permit it. As an example, the application of security update can be more difficult as IoT devices are more real time depend that traditional ICT systems or constrained IoT devices don't support strong cryptographic functions.

There is still a long way for IoT security. More standards adapted to IoT are needed, security best practices need to be implemented in IoT and new or adapted security controls need to be defined.

Keywords

IoT; security; auditing; assessment; IoT auditing; IoT security; IoT assessment; traffic management; smart city; risk assessment; risk management; risk analysis; risk treatment;

Contents

Acronyms

6LoWPAN	IPv6 over Low -Power Wireless Personal Area Networks
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
APT	Advanced Persistent Threat
AV	Anti-virus
CBOR	Concise Binary Object Representation
CIA	Confidentiality/Integrity/Availability
CIS	Center for Internet Security
CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
DLP	Data leakage prevention
DTLS	Datagram Transport Layer Security
ENISA	European Union Agency for Network and Information Security
FW	Firewall
GDPR	General Data Protection Regulation
IAM	Identity and access management
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LLN	Low-Power and Lossy Networks
LoRa	Long Range
LTE	Long-Term Evolution
MQTT	Message Queuing Telemetry Transport
MITM	Man in the middle
NIST	National Institute of Standards and Technology

OS	Operating System
OWASP	Open Web Application Security Project
PP	Protection Profile
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RMF	Risk Management Framework
SB	Senate Bill
SIEM	Security Information and Event Management
T2T	Thing-to-Thing
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XXE	XML External Entity
XSS	Cross-site scripting

List of Figures

List of Tables

1 Introduction

The term IoT was first used in 1999, by Kevin Ashton, at that time in the context of object tagging using RFID[1]. IoT concept and definition has come to several changes in the following years, expanding its scope to include new technologies, objects, and protocols[2]. Even nowadays, it is still a fuzzy concept not well defined or with different interpretations. Can use different technologies like wireless sensors networks(WSN), Low power Wireless Personal Area Networks (LoWPAN), to technologies such as Radio-Frequency Identification (RFID), just to name a few[3] and can be used in many different contexts as smart homes, smart cities, smart industry, smart health, IoT in military applications and others.

All these aspects contribute to the lack of common IoT standards, models, architectures, protocols, and frameworks that are common to the "traditional ICT world." These "common agreements" are an essential tool to achieve interoperability and a shared common view, allowing the definition of robust standards. However, what happens is that there is significant fragmentation in many aspects of IoT being one of the reasons the significant number of stakeholders involved in the process. So before starting to use IoT technology in our daily lives and in critical systems, efforts should be made to "unify" IoT as much as possible. This is particularly true for IoT security[4].

As already said, IoT systems are used (or planned to be used) in critical aspects of our lives and span many vertical applications like smart cities, healthcare, military, energy, cars among others. These systems have and will have more and more impact on modern society to a point where they are close to autonomous and auto sufficient. Any cyber-attack on these types of systems can have a significant impact and critical consequences on people's lives. Also, these systems are more complex than they look at first glance. They are not only composed of the "thing" itself (that interact with the physical world) but a complex set of systems (networks, middleware, clouds, fogs, backends, and applications). As more and more devices are connecting to "IoT ecosystems," interacting and inter exchanging sensitive information, the more urgent is to reach a universal and stable agreement in all aspects of IoT, including security. This is even more critical as some characteristics of IoT like pervasiveness, privacy, cyber-physical will require that IoT enforces more strict security measures that "traditional ICT." If the predicted evolution of connected devices sustains, then in 2020, we will have around 31 billion devices connect [5], more than 3 times earth population and around 75 billion[6], showing clearly the urgency of the security aspect of IoT. Because all of this, security is a paramount in IoT either being defining security requirements and standards for IoT, defining and implementing security controls or performing security assessment and auditing.

IoT Security will have, due to specific IoT characteristics, some challenges either in general or when compared with "traditional ICT." First, as already seen, IoT has broad applicability ranging from more "relaxed" environments to more critical ones. This means that within IoT, there will be different security needs adapted to the used case. On the other hand, IoT is different from "traditional ICT," and all the security methodologies will need to adapt.

Most of this work, of developing common standards, protocols, security requirements, and security controls, is currently being done by different organizations, for the different IoT aspects with the aim to reach a common definition that serves as a base of work to the different stakeholders involved.

One of the ways to contribute to this endeavor is to understand what are the security risks that these types of systems will face and whether current security controls can help to mitigate these risks or if new security controls are needed. Due to the different scenarios where IoT can be used, the objective to achieve a common set of measures might be overwhelming or at least too generic to be applied to specific IoT use cases. As with "traditional ICT," each system has specific security requirements, and in the IoT case, security requirements for different scenarios will even be more significant. So, an approach is to analyze concrete IoT scenarios, allowing the identification of specific and commons risks with the hope that a common baseline is found.

1.1 Objectives

The main objective of this work is to apply a security risk assessment methodology to specific IoT use case in the domain of smart cities. This will permit to understand what challenges today's IoT systems in the domain of smart cities face in terms of security, to find what are the main security risks these use cases, what traditional security controls could mitigate these risks and what are the possible constraints when applying traditional security controls to the IoT scenario. These conclusions can be extrapolated at some extend to the general case of IoT. These conclusions can be used in the definition of new or adapted security controls that are better suited to IoT.

To accomplish this goal is essential to understand first, what is IoT and what an IoT system nowadays entails and understand the state of the art of current IoT security research. This information will allow a better definition of the security risks present in these types of systems and more specifically, in a particular use case of IoT – a traffic management solutions scenario. This set of security risks is obtained using a process of risk analysis taking into consideration the literature review done before. The outcome of this risk assessment is then used as input to a risk response phase where risks are treated using current security controls.

Due to the multititle and different scenarios where IoT can be applied, this security assessment exercise has the advantage of catching the specific risks of this particular scenario, however, this option also reduced scope and has the disadvantage of only catching a partial view and possibly missing important points when a more integrated analysis is done. Nevertheless, this is a small contribution to the IoT security problematic and similar analysis can be done to other specific cases where IoT is used, allowing conclusions about common and different points in terms of security.

1.2 Methodology

The methodology used in this work is based on a literature review of research work in the IoT area and current accepted standards/best practices from globally accepted sources like IEEE, ISO, NIST, ENISA, OWASP, CIS, CISCO among others. This will allow comprehension of the current state of the art in respect of IoT mainly the defining of IoT, the proposed architectures of IoT, subcomponents, and protocols, IoT security, and IoT security auditing.

This state-of-the-art research will enable the definition of specific IoT security challenges and security needs that will be the input to the next phase of this work composed of a security assessment exercise to a specific IoT traffic management scenario in the context of a Smart city. This security assessment will use the methodology define in NIST SP800-30[7] risk assessment framework and include all the relevant threats and vulnerabilities that are the result of the research done in the first phase of this work. This assessment goal is to identify all the risks that traffic management solutions can face today, and what are identified the most important risks.

These risks are then subject to a risk treatment plan, where security controls from NIST SP 800-53[8] and security controls from the research work done in the first phase, are used with the objective of mitigating the impact of the security problems identified in the risk analysis.

Finally, a discussion concerning the applicability of current security controls to the this particular IoT scenario is done taking into consideration all the IoT characteristics reviewed in this work, and how these characteristics can hinder the applicability.

1.3 Structure

The rest of this dissertation is organized as follows. Chapter 2 gives a general introduction to IoT, common architectures, models, protocols, and a summary of characteristics specific to IoT environments.

Chapter 3 reviews some literature, articles, and research work related to IoT security, IoT compliance, and auditing. In this chapter, research and analysis of the main security concerns related to IoT either at a higher level but also aspects related to security in IoT protocols are done. The specific IoT characteristics identified in Chapter 2 are also analyzed in light of the security concerns that these characteristics can add to the IoT case. A small overview of the primary ICT security and ICT auditing frameworks are also given in this chapter.

Chapter 4 will introduce and describe the IoT scenario that it is used as an example of the risk assessment and risk treatment exercise done in the following chapters.

Chapter 5 defines the risk assessment methodology and the assumption used in this process.

Chapter 6 uses the risk assessment procedure defined in chapter 5 and applies it to the scenario described in chapter 4 and taking into consideration all the research work done in the previous chapters. This chapter also defines a possible risk treatment plan for the identified risks and analyses where the applicability of "ICT" security controls can be hinder by the specific characteristics of IoT and discusses the results obtained with this work and possible improvements.

Chapter 7 gives a final conclusion and directions of future work.

2 IoT Overview

Understanding the state of the art of the main aspects of IoT is an essential task to better accomplish the ultimate objective of this work. To be able to assess the security of a system, it is essential to understand the definition of that system, what are the proposed architectures and protocols. It is also critical to understand what the key characteristics of IoT are. This chapter review some of the literature related to these subjects. This is not by far an extensive research, as this is not the final objective of this work. There are many different proposals related to these matters and proper research on these topics would need by itself a full dissertation. The objective, in this case, is to set a shared understanding and ground for the following phases of the work.

2.1 IoT Definition

Being a relatively old concept and due to changes in the scope and with the inclusion of new technologies and areas of application, the definition of IoT, nowadays, is not consensual, and it has changed and evolved over time. Although different entities have their own definition, we can find a joint base among them. This is understandable as the initial focus of IoT has simple RFID devices with no other functionality, and today, IoT encompasses a wide range of applications and technologies.

Some authors are vague in the definition mentioning only the existence of devices that collect and process data [9]. Other authors already included a critical characteristic of IoT: the "cyber-physical" aspect, including also the existence of sensors, actuators, and interconnectivity [10]. A step further is done by authors in [11] where ubiquity and intelligence are also included and by authors in [12] with the introduction of a specific characteristic of the network: dynamic and self-configuring. People are also a critical factor in IoT, as mentioned by authors of [13]. Finally, a definition that, that seems the one that catches most of what are IoT ecosystems today, is suggested by authors in [14] where important elements of IoT like cloud computing, mobile computing, embedded systems, big data, low-price hardware are mentioned.

All these definitions have a common base that points IoT as an interconnected "collection" of "things" that interacts with the physical world, interchanging, and processing information to achieve a goal. Other vital concepts of current IoT ecosystems are cloud integration, the intelligence aspect of the whole system, the cyber-physical, pervasiveness, and the tremendous amount of information produced. To present discussion, the definition adopted is one strongly based on the definition present in[14] that captures the main characteristics of IoT nowadays: "The Internet of Things (IoT) paradigm is the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and other technological advances that are evolving and expanding rapidly and that have a strong interaction with the physical world in a combination of information technology (IT) and operational technology (OT). "

2.2 IoT Architectures

IoT architectures, as in the case of "traditional ICT," allow us to view and think IoT as a whole, capturing the primary and critical aspects of it. Accordingly, with[15] a reference model simplifies, clarifies, identifies, standardizes, and organizes. This reference model will also permit a reliable and comprehensive definition of IoT security needs. There is not only one IoT architecture, as in the case of "traditional ICT," but in the IoT, the case can be even more problematic, mostly because of the fragmentation and heterogeneity in IoT applicability and technologies. In this respect, it is crucial to define a reference architecture or a small set of reference architectures that would allow a consistent approach of all stakeholders to IoT[16], [17], [18]. Many recognized international organizations are making efforts to put some order in this fragmentation analyzing the many proposals from different application domains of IoT and trying to "consolidate" this information in a reference architecture[9], [18], [16].

The approach followed by ENISA on one of their works related to IoT security was to analyze already existent IoT architectures from the different application domain and abstracted them in a high-level reference model that encompasses key elements of those architectures [9],Table 1. This work proposes an architecture with four layers: the devices layer where sensors, actuator, embedded devices, mobiles devices are included; the communication layer where all the communications are handled; the backend and cloud platforms layer where all the information produced is analyzed; and the "use case" layer where the different IoT application domains are . A similar architecture is proposed by Cisco but with further refinement on the "backend" layer[15] -Table 2. The proposed solution is composed of seven layers: Physical Devices and Controllers, Connectivity, Edge (Fog) Computing, Data Accumulation, Data Abstraction, Application and Collaboration, and Processes. Compared with ENISA proposed model[9], the backend and cloud platforms layer of ENISA model is further divided into Edge (Fog) Computing, Data Accumulation, Data Abstraction giving more relevance to the data in IoT. There are other research works on this matter [1] [19], and in all of them, we can find similarities and a common base: the physical device layer, the communication layer, and the "backend" layer. ISO also has a standard about IoT reference architecture - ISO/IEC 30141:2018, but it is not available to the general public. Nevertheless, the most comprehensive and detailed study found about IoT architectures is the one done by ISO/IEC, where a detailed analysis of different IoT architectures is done[16].

If we compare IoT architectures with "traditional ICT" architectures, we find some key differences. For example, IoT architectures have one layer that is not present in ICT - the device layer and strongly relays on the services provided by the "backend/cloud" layer. This is mainly because IoT fundamental components are the "things"(as implied in the IoT definition) itself strongly connected to the physical world. Also, in IoT, the user layer can be seen from two different perspectives: the user that interacts with the "thing" and the user that interacts with the backend systems.

Layer	Name	Function
4	Use cases	Where analytics and visualization for the different use cases (transport, energy, health care, smart home, etc.) are located
3	Cloud platform, backend and services	Where web-based services, database, storage, rule decision, device management, rules engine, and process automatization are located
2	Communications	Where the communication is located: PAN, LAN, and gateway
1	Devices	Where actuators and sensors, embedded systems, smartphones, wireless devices are located

Table 1 – High-level reference model(adapted from [9])

Layer	Name	Function
7	Collaboration & Processes	Where the applications are used to achieve a specific objective
6	Application	Where data is consumed and presented
5	Data Abstraction	Creates abstractions of data at rest to be used by application layer
4	Data Accumulation	Data at rest where useful information is "stored"
3	Edge (Fog) Computing	Conversion and aggregation of data flows into information
2	Connectivity	Provides connectivity between all layers and within a specific layer
1	Physical Devices & Controllers	Where all the "things" are located

Table 2 – Internet of things reference model(adapted from [15])

This brief introduction to IoT architectures allows the definition of the arquitectural models considered in this work and from where the IoT scenario at study will be based on. The reasoning behinf this choice was to consider "general" architectures applicable to all IoT scenarios. There are many other proposals for IoT architectures, either general IoT architetures or architetures of specific cases of IoT. This brief review gives an idea of some of these proposals and a complete review if out of scope of this work.

2.3 IoT Protocols

As with IoT architectures, comprehension, definition, and standardization of IoT protocols allow a consistent approach, of all stakeholders, to IoT. As with IoT architectures, there is a multitude of protocols in IoT[2] that we can see from some of the proposals in [3], [9], [20]. This is again due to the high fragmentation in IoT but also to the fact that different IoT domains might require different requirements in protocols (mainly at lower layers). Different vendors are developing their own protocols most of the time proprietary, and this vast amount of protocols makes the overall interoperability hard. This fragmentation is also due to the different communication needs that different IoT scenarios might have and to the fact that IoT, as a group of technologies, has evolved over time, so there are still traces of that evolution at the protocols level. When we think in IoT security is inevitable that we include protocol security as a big concern. This fragmentation makes definition of security a difficult task, as more protocols means more probability of vulnerabilities.

As there are many protocols proposals, it would be impossible, and not the focus of this work, to analyze it all. The reasoning behind the choice was to analyze a small part of the overall IoT protocols, but the ones that industry believes that have the most important characteristics in terms of reliability, power-efficiency, and internet connectivity and that will fit and adapt better to the current technologies[3]. Although in some cases IoT devices use the same stack as "traditional ICT," due to limitations of IoT devices, new protocols were designed to better cope with low processing power, low power capabilities and low connectivity capabilities that characterize IoT. Also, it is essential that IoT communication protocols are designed to guarantee interoperability between all components and also with the existent "Internet," enabling the adoption without any problems[3]. IoT protocols should then adopt the approach of the proved internet protocols and adapt accordingly with the specific characteristics of IoT and not follows an entirely disruptive approach defining completely new protocols. In this respect, some protocols start to have more attention due to these characteristics. The definition of common protocols like 6LoWPAN and CoAP is an important step to uniformize the IoT protocols allowing better integration with current Internet technologies[2].

One example is the protocols stack adopted by ENISA. ENISA defines an "indicative set of communication protocols" used by IoT [9] -Figure 1 using four layers. The data link layer either wired or wireless short-range (ZigBee, Bluetooth/Bluetooth Low Energy (BLE), Wi-Fi/Wi-Fi HaLow, Near Field Communication (NFC) or Radio Frequency Identification(RFID)) and wireless longer-range radio protocols such as LoRaWAN, SigFox NarrowBand-IoT or LTE-M[9]. On the routing layer, we have the Channel Aware Routing Protocol (CARP) and Routing Protocol for Low-Power and Lossy Networks (RPL). One the encapsulation layer IPv6 over Low -Power Wireless Personal Area Networks (6LowPAN), Thread and in the session layer Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), Message Queuing Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP).

Also in line with the requirements of interoperability compatible with existent with current internet protocols and also deal with the specific characteristics of IoT (e.g., low resources, low power, etc.), we have the proposal from IEEE and IETF and presented in [3]. The stack is in Figure 2. Defined in five layers: the physical layer (IEEE 802.15.4), the media access control layer(IEEE 802.15.4), the adaptation layer(6LoWPAN), the networking and routing layer(IPV6, ROLL RPL) and the application layer(CoAP)

Another "IoT protocol stack" is presented by authors in [20] - Figure 3. Composed by five layers, we can see many similarities with the one presented in both Figure 1 and Figure 2, only having a "new" Transport Layer with protocols UDP and DTLS, and a Data Format layer with protocols/formats Binary, JSON, CBOR.

Session		AMQP,CoAP,DDS,MQTT,XMPP
Network	Encapsulation	6LowPAN, Thread
	Routing	CARP, RPL
Datalink		Bluetooth/BLE, WI-FI/ WI-FI HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Figure 1 – Indicative listing of communication protocols for IoT(adapted from [9])

Application	CoAP
Networking/routing	IPV6, ROLL RPL
Adaptation	6LoWPAN
MAC	IEEE 802.15.4, IEEE 802.15.4e
PHY	IEEE 802.15.4

Figure 2 – Communication protocol stack in IoT(adapted from [3])

Looking at the three proposals, some similarities can be found. On the datalink "layers," meaning the layers that manage the physical medium, the protocol most common is the IEEE 802.15.4. 802.15.4 standard was designed with the unique characteristics of IoT in mind to "provides for ultra-low complexity, ultra-low-cost, ultra-low power consumption, and low data rate wireless connectivity among inexpensive devices, especially targeting the communications requirements of what is now commonly referred to as the Internet of Things[21]. Some of the main features are data rates of maximum 250 kbps, support for critical latency devices, automatic network establishment, fully handshake protocol for transfer reliability, low power consumption[21], and having102 bytes available to higher layers.

Data Format	Binary, JSON, CBOR
Application Layer	CoAP, MQTT, XMPP, AMQP
Transport Layer	UDP, DTLS
Internet Layer	Ipv6/IP routing
	6LoWPAN
Network/Link Layer	IEEE 802.15.4 MAC
	IEEE 802.15.4 PHY /Physical radio

Figure 3 – IoT Layers (adapted from [20])

At a higher layer, there is what is called the encapsulation or adaptation layer where are the protocols 6LoWPAN. This is the layer that will "encapsulate" or "adapt" IPv6 packets to the constraints of lower layer like 802.15.4. Is this layer that allows the interoperability of IoT devices with the "normal internet protocols." It also implements mechanisms for packet compression, fragmentation, and reassembly, among other functionalities[3].

On the so-called routing layer, there is one routing protocol that is more common - RPL. This is also a protocol with IoT defined in rfc6550[22]. It is a protocol IPv6 Routing Protocol for Low-Power and Lossy Networks. Basically, it is a routing protocol that can operate in Low-Power and Lossy Networks (LLN), and the router device itself is constrained in terms of resources. It operates in networks with high loss rates, low data rates, and instability providing mechanisms for multipoint-to-point traffic as well as point-to-multipoint traffic and support for point-to-point [22].

On the application layer, there are many protocols. One of them is the Constrained Application Protocol(CoAP) initially defined in rfc7252[23]. As the name implies, this is a constrained protocol designed for constrained devices and networks. It follows the model of HTTP using request and response interactions, application endpoints, and URIs. It can easily interoperate with HTTP but keeping low overhead and simplicity[23]. Usually, as shown in Figure 3, CoAP (or any other IoT application level protocol) uses DTLS as transport layer, making use of the security features of DTLS. This protocol is not going to be detailed in this chapter as although it is used by IoT systems, it is not exclusively to IoT.

The use of network protocols and the word internet in the IoT does not mean that IoT environments need necessarily Internet connectivity. As in the "traditional ICT" world, it means that IoT devices need a way to send and receive information that they process[9].

This brief introduction to IoT protocols allows the definition of the common communications models considered in this work and from where the IoT scenario at study will be based on. The reasoning behind this choice was to consider standard communications stacks instead of the proprietary protocols. There are other proposals for IoT communication stacks, either proprietary or for specific use cases of IoT that are out of scope.

2.4 IoT Characteristics

It is crucial to understand the differentiator characteristics of IoT and to perceive how these characteristics can influence IoT security. These specific characteristics of IoT will somehow influence the way that security is defined and built, in a way that is different from security in "traditional ICT." In this section, the main differentiator characteristics of IoT are presented, and in Chapter 3, the security problems arising from it are described.

The first characteristic of IoT that is almost evident by definition is the **high number of devices**. The explosion of "things" is a direct consequence of the IoT definition, where every physical "thing" can be connected to the network[24].

Another crucial essential characteristic of IoT is the **strong interaction with the physical world**. All IoT current definitions mention the existence of layers of sensors and actuators interacting with our physical world. This layer of sensors and actuators are the most important source of information in IoT and also the main channel to output "information." IoT is defined as a cyber-physical system.

Pervasiveness is also a specific characteristic of IoT that is not often found in "traditional ICT." IoT is becoming present in almost all aspects of our society and our daily life, from more "relaxed" environments to more critical ones[9][25]. In the foreseen future IoT devices will be present almost everywhere: cars, at home, in our body, in roads, health. Despite the advantages that this brings, there is also the advantage that society will be more dependent on these systems.

This "explosion" and pervasiveness aspects lead to another key characteristic of IoT - **big data**[26], [9], [25]. The amount of information that these systems will produce is overwhelming in the sense that it will be needed a high number of resources to deal and process it, but also it will allow a valuable amount of new information and knowledge.

Another important characteristic of IoT is the fact that, mainly, the **devices in the device layer, are resources constrained.** This means that they have low processing power, are power and memory constrained, and also have a limitation on networking capabilities like slow and less reliable connections [9][26][2].

Lack of security awareness and security motivation not only due to the constrained aspect of IoT devices but also to the fact that manufactures and vendors are not aware of possible security problems in IoT. Also to the fact that there is no economic motivation for including security in IoT devices (e.g., due to the low-cost aspect of IoT devices, time to market,), there is no software background in the manufacturer (e.g., the background is "regular devices" development)

Other characteristics of IoT, again mainly of the devices in the **device layer, is the lack of physical control and lack of "single physical location**"[26] or extremely **mobile**[6]. Usually, these devices are deployed in "public" and not secured areas

Heterogeneity is identified as one of the main problems in IoT[9]. Due to the number of stakeholders involved and the different applicable areas(e.g., home, industrial, cars, military, etc.), there is a multitude of hardware platforms, firmware/OS, protocols, etc. [26].

Some of the environments where IoT systems are used are **more real-time dependent** than "traditional ICT." In some cases, decisions need to be taken without significant delay as they are somehow linked to situations in the real world that need a fast reaction.

System complexity, "dispersion" and extension of boundaries, where a system can integrate subsystems from different stakeholders. This is not exclusive of IoT as the trend is to move away from the traditional concept of a system with well define perimeters and boundaries.

Long-life aspect of IoT devices. Some IoT systems include IoT components designed for being used for long periods.

Thing-to-Thing (T2T) communication where IoT devices have the possibility to communicate directly amongst themselves without support from the network. This is also not exclusive to IoT, but it will increase with IoT use, boosted by the added value such as network performance, lower latency, and lower energy requirements [2].

Interdependence where systems that are not only dependent on human actions but also receive "orders" from other devices making the systems autonomous [26][6].

IoT is usually associated with bid data an high number of devices ut all these characteristics are extremely important to IoT and to IoT security. Some of them are not exclusively to IoT and are also present in traditional ICT systems. Nevertheless the conjuntion of some IoT characteristics with others, can have a bigger impact on security. One example is the big data and high number of IoT devices. Big data is not exclusive to IoT, however together with the high number of IoT devices increases for example the risks to privacy.

This chapter sets the bases for the rest of this work, defining a common understanding of IoT in terms of the definition of IoT, IoT architectures and protocols, and the specific characteristics of IoT that can influence how security is defined. This brief overview of IoT sets the boundaries for the IoT security review done in the following chapter.

3 IoT Security Compliance

The number of threats and successful attacks against IoT devices and systems increased in the last years and is expected to continue this trend, as the use of IoT systems continues to increase across the entire spectrum of our daily life activities and critical infrastructures[9]. One of the most known attacks against IoT devices was performed by the Mirai malware compromising hundreds of thousands of IoT devices to build a massive botnet that was later used to other types of attacks (e.g., DDoS). This attacks (at least the first version of it) took advantage of IoT devices, like IP cameras and routers, with default settings, like default passwords and specific OS version and was used in attacks to "traditional ICT" systems[27].

Although this was an important attack, the major impacts were economic, and the real target was not even the IoT systems, but they were used as a way to target other systems. Of course, we can never say that there were no other security implications like privacy, but alone, this attack had no direct implications on safety. Nevertheless, this attack showed how bad security is defined and implemented in these types of IoT devices and how some simple and basic security controls (i.e. strong password and change of default credentials) were not followed. This attack maybe could be avoided if these simple security controls were applied.

Security of IoT devices is even more important as these types of attacks can be used to cause significant problems to human safety and also to privacy. This is due to the connection of these systems to the physical world[9]. This is even more evident in IoT systems used in critical systems where increased importance on safety and resilience must be done to levels higher than "traditional ICT" and less critical IoT systems[26] [9]. One of these examples is the security of vehicles where a successful attack can cause severe damages to human life. Privacy is also a significant concern in IoT since IoT drastically changes the relation of information systems with personal data. IoT introduces new ways of data collection, analysis, use, and protection that need to be analyzed and addresses correctly to achieve trustable services[9].

That is why IoT security and security compliance must be the topmost concerns of IoT environments, and any risks to these systems that can lead to issues with human safety should be our primary concern. Security without proper auditing and compliance checks can be ineffective either because the security requirements and controls were not defined correctly or they were defined correctly but not implemented, implemented incorrectly or not working as expected. Therefore, it is crucial to understand the current state of the art of IoT security and the main requirements to have secure IoT systems. In this chapter, a review of the state of the art of IoT is done focusing on understanding the main threats and vulnerabilities, and the proposed controls to mitigate these risks.

3.1 IoT Security frameworks

Security is a critical aspect of information systems, but this is even more critical in IoT systems mainly due to the "link" with the real world. The strong interaction of IoT sensors and actuators with the physical world can transform relative small security issues, in these types of systems, into a situation that can severely harm and damage individual privacy and safety[2]. Also, the scale of impact is much bigger than in "traditional ICT" due to the higher number of "things"[2].

Security in IoT depends on the protection of all systems, entities, and layers involved(e.g., devices, cloud, backend systems, communications, operations, personal) [9]. Nevertheless, the focus in this chapter will be more directed to the IoT device layer and IoT communications layer, as backend layers and cloud are somehow similar to "traditional ICT." This said it is important to note that even with this similarity, interactions with the IoT devices can bring new and additional security problems to these systems.

IoT security is not an entirely new area of research. IoT technologies are based on current ICT technologies and therefore inherit a significant number of security concerns and security methodologies[9]. As we see in the architectures and protocols sections, there are many IoT systems that are based on "traditional ICT," and the protocols are similar. Also, well-known security and auditing frameworks and best practices can be used in the IoT case.

As in other situations, security can be viewed and defined as a whole, defined as a global strategy, or focusing on specific aspects of technology and more granularly. Overall, in this work, the reviewed literature specific to IoT security covers all these aspects, either very broad in the sense that tries to include IoT as a whole defining generic security orientation or more focused in some specific IoT aspects like protocols. Also, in the case of IoT as there are many applicability areas security can be defined to specific areas of action as different areas will have different security requirements as for example a nuclear plant or a smart home case. This review the state of the art in IoT security either in terms of security issues in IoT or in recommendations and controls to secure it and either in a more global way or more detailed.

3.1.1 ENISA

ENISA has done extensive work in the IoT security domain resulting in a set of baseline security measures for IoT[9]. The approach followed by ENISA was to look at the IoT security problem as a whole, including different types of IoT scenarios. ENISA is aware of the difficulties that defining a set of common security measures to all possible IoT scenarios have, as they have to cater to all specific IoT scenarios specificities. The methodology followed was to identify gaps in current security controls and to define baseline security measures that can mitigate these gaps. The gaps were identified using a risk assessment procedure with threat modeling to the different IoT scenarios considering the current security controls and IoT threats. The identified gaps are:

- IoT security fragmentation and lack of regulations
- lack of security awareness in IoT
- design and development security problems
- interoperability problems
- lack of economic incentives to foster security
- product lifecycle management problems

If we look at the identified gaps, we see that they are “common sense” more or less stable measures in the “traditional ICT” world, but due to the nature of IoT, they are not yet implemented in IoT.

To overcome these gaps, ENISA defines a set of baseline measures. The final set of recommendations are high level and are in line with the identified gaps:

- standardization and regulations of IoT security
- IoT security awareness
- secure software and hardware development cycle
- interoperability consensus
- economic incentives for IoT security
- secure IoT service lifecycle
- clarify liability among IoT stakeholders.

As can be seen, although the process to reach these conclusions was detailed and technical, the final set of recommendations is instead a high level and can be seen as “basic common sense” when compared to “traditional ICT.” This shows the status of IoT security when compared to “traditional ICT.”

3.1.2 NIST

NIST also has a comprehensive and detailed report on the global status of standardization in IoT security [26]. This analysis is more focused on the existent standards, IoT related or relevant for IoT, their market adoption, and the applicability of different IoT scenarios. The final result is a gap analysis of the possible missing standards concerning the identified security needs of different IoT scenarios. In this work, NIST does an extensive analysis of existent standards related to security, in all the domains (e.g., network security, information security management, encryption, IAM and others) that are considered relevant to the IoT case. NIST enumerates the IoT specific characteristics that can affect the security of IoT systems. The following list summarizes the characteristics defined by NIST[26]:

- direct connections to non-owner networks, where IoT devices connect to vendors networks
- highly distributed systems with a variety of owners, where an IoT system is composed by different IoT subsystems crossing the boundaries of different owners
- autonomous aspect of IoT, where IoT devices work without intervention of users
- low-capability computing hardware either in processing power, storage or power
- static systems where updates are not or cannot be done and configurations cannot be changed as needed
- data processed data locally and remote
- collection of massive volumes of data
- highly heterogeneous systems either in operating systems, network interfaces and protocols or in functionality
- proprietary protocols
- no centralized management capabilities
- remotely controlled by manufacturers
- deployed in physically unrestricted locations

- statistical errors when sensing and acting on physical objects
- collection, storage, and use of personal data
- created through combinations of existing IoT systems for an application not envisioned by the original end
- long life of components
- poorly connection (dropped packets, interrupted connections)

With this information and information about relevant standards, an evaluation of the applicability of current standards to security needs in different IoT scenarios is done as also the level of adoption of the current standards in the actual market. Also, an analysis of possible gaps (missing standards) is done, taking into consideration the security requirements defined or the different IoT scenarios. The conclusion for the identified gaps in standards per domain are:

- **Cryptographic**: explore blockchain technology for IoT security;
- **Cyber Incident Management**: remediation recommendations for when software updates are not possible;
- **Hardware Assurance:** recommendations for avoiding malware in firmware;
- **Identity and Access Management:** in this case only the recommendation that existing standards should be reviewed for assessing the sufficient applicability on IoT
- **Information Security Management Systems**: management system standards based upon ISO/IEC 27002 should be considered for IoT;
- **IT System Security Evaluation:** in this case only the recommendation that existing standards should be reviewed for assessing the sufficient applicability on IoT;
- **Physical Security**: new standards should be created as there are no standards for IoT;
- **Security Automation and Continuous Monitoring**: since IoT ecosystem is heterogeneous develop standards that are tailored to the various use cases of IoT and to the various vendors;
- **Software Assurance:** standards for avoiding vulnerabilities in software should be researched
- **Supply Chain Risk Management**: existent generic standards (e.g., ISO/IEC 27036), not specific to IoT, should be reviewed for the IoT case
- **System Security Engineering**: existent generic standards (e.g., ISO/IEC 15026) should be reviewed for the IoT case[26]

The main conclusion is that concerning existent standards, there is a good foundation that can be used, either IoT specific standards or standards that should be reviewed to assess the adaptability to IoT. Nevertheless, in some domains, new standards should be created. In terms of market adoption of these standards, the situation is different as most of the cases, the adoption is slow.

3.1.3 ISO

ISO is also working in IoT security are with some in-progress standards. For example, ISO/IEC 27030 defines guidelines for security and privacy in the Internet of Things, but this standard is still under development[28].

3.1.4 Cloud Security Alliance

The "Security Guidance for Early Adopters of the Internet of Things (IoT)" [25], from Cloud Security Alliance, although from 2015, gives some recommendations of security controls that must be implemented by an early adopter of IoT. The meaning of "early adopters" is in the sense that IoT is still very immature with respect to security, and the "first adopters" should implement these recommendations. This is somehow similar to the work of ENISA[9] where a set of security recommendations is done as a conclusion of the work. In this case, the set of recommendations are more specific and detailed. These recommendations are based on a set of IoT characteristics that challenges the secure deployment of these systems. These characteristics are in line with the characteristics identified in 2.4, where the specific IoT characteristics are identified but are more focused on the security perspective:

- Some IoT systems are poorly designed and implemented, with a complex configuration using differs protocols and technologies.
- IoT still lacks mature technology and processes
- IoT still lacks mature guidance and processes for management and maintenance of the device
- IoT introduces unique physical security issues.
- IoT introduces complex privacy concerns.
- IoT still lacks mature guidance and processes for IoT development
- IoT still lacks mature standards, guidance, processes for authentication and authorization od edge devices
- IoT still lacks mature guidance and processes for incident response activities
- IoT still lacks mature standards, guidance, processes for logging and audit
- Lack of methods and processes to achieve situational awareness of secure posture of IoT assets
- IoT still lacks mature standards, guidance, and processes for IoT virtualization[25]

A set of seven security controls are suggested to "early adopters" which are very similar to controls to the "traditional ICT" case[25]

- Privacy-by-design approach to IoT development and deployment
- Secure systems engineering on development and deploying of IoT Systems with the use of threat Modeling and secure development
- Implement layered security protections to defend IoT assets
- Implement data protection including data at rest, in transit, in use and DLP
- Define lifecycle controls for IoT devices
- Authentication and authorization framework for the IoT Deployments, including mutual authentication between users, devices and cloud and identity and access management.

- Define and implement a logging/audit framework for the organization's IoT ecosystem

3.1.5 Center for Internet Security

An interesting work was done by the Center for Internet Security - CIS, analyzing the applicability of the CIS Critical Security Controls (version 6) to the IoT case [29]. An evaluation of the applicability of each CIS control is done and possible challenges identified. This is not a work were security recommendations are done, but where the applicability of the CIS controls is evaluated and possible challenges to apply it is evaluated. In all CIS controls were identified problems that could make the applicability to IoT case, difficult. Below there are some examples of the possible challenges of each control when used in the IoT case.

- **#1 - Inventory of Authorized and Unauthorized Devices**
  This control is crucial to IoT as organizations need to keep track of the high number and the different types of IoT devices. Nevertheless, the practical application might face some challenges as current methodologies to implement this control can be unpractical in some IoT scenarios. For example, network scans used to discover devices might cause abnormal behavior IoT devices when scanned as they are not ready to be probed or protocols might be proprietary, and there are no tools yet to do the scan.
- **#2 - Inventory of Authorized and Unauthorized Software**
  This is similar to control #1. Organizations need to keep track of the high number of firmware and software versions that exist in the IoT ecosystems. However, in some cases, some of the methodologies used to implement this control might not work in IoT. For example, proprietary operating systems/firmware might not have remote query capabilities. Also, remote probing can be delicate due to a multitude of firmware/OS and might not be desirable to an unreliable response to probes.

- **#3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
  This control is also applicable in IoT, but there are many challenges to applying it. First "hardening" of IoT devices can be painful as these devices do not have the same security features as "traditional ICT," and when they have, the configuration is not easy to do. Also, due to the many different IoT devices systems, maintaining and keeping a baseline configuration is a difficult task.

- **#4 - Continuous Vulnerability Assessment and Remediation**
  This control is also important in IoT. Implementation has some challenges. Vulnerability scanners might not be ready for IoT protocols and vulnerabilities. Also, as in control #1, direct probes of IoT devices, might not be desirable(e.g., in critical IoT scenarios) as IoT devices can have erroneous behavior.

- **#5 - Controlled Use of Administrative Privileges**
  Applicable in IoT but can be challenging to implement. First, some IoT devices might not even have the notion of regular and administrative accounts, and when they have the type of protection for using that "admin account," it is weak.

- **#6 - Maintenance, Monitoring & Analysis of Audit Logs**
  Applicable control and very important, but some devices might not have logging features or remote monitoring capabilities. Also, audit systems might not be prepared to correlate IoT events.

- **#7 - Email and Web Browser Protections**
  Although it might be possible in some cases, it is not common to have these types of interfaces in IoT devices. So it does not apply to the IoT case.

- **#8 - Malware Defenses**
  Important to IoT but might face some problems to implement. First, the real-time operation of some IoT devices might not be compatible with the delays in malware defenses. Second, these malware defenses, mainly system malware defenses, might not even exist in IoT, due to the high number of different types of IoT systems.

- **#9 - Limitations and Control of Network Ports, Protocols and Services**
  Important control but adaptations might be needed for example, to new IoT protocols and the old concept of "network ports" and services, as new IoT protocols might have a different concept of ports.

- **#10 - Data Recovery Capability**
  IoT system ultimate destination of data should be backend systems. Nevertheless, some device might store data locally. It is important to understand what devices and which data is saved locally and how to add recovery capabilities in these cases.

- **#11 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
  Important, but as in control #9, some new IoT protocols might add additional constrained to the configuration of network devices and these devices might still not exist.

- **#12 - Boundary Defense**
  Boundaries are a blurred concept in IoT as there is, for example, heavy usage of the cloud and in some cases, the IoT systems are composed of different IoT subsystems owned by different stakeholders. So it is difficult to define a boundary and defense measures.

- **#13 - Data Protection**
  Applicable and very important, but one of the most difficult to implement. First, on the protection of data in transit, IoT devices might not have a cryptographic mechanism to ensure this. However, more important is the data protection on acquisition and storage as these devices are deployed with no physical security.

- **#14 - Controlled Access**
  One of the most important aspects of IoT, where some devices still lack the concept and mechanism of access control white no authentications and authorization methods.

- **#15 - Wireless Access Control**

As relevant IoT protocols rely on wireless communications, access control is important. Nevertheless, IoT protocols might not be ready either to implement access controls or only allow basic and not scalable access control features.

- **#16 - Account Monitoring and Control**
  Account monitoring might not be easy to implement in some devices, and first devices need to have this "concept" of accounts, and second, they need to either centralize account registering or make available methods to "remote monitor" accounts locally on devices.

- **#17 - Security Skills Assessment and Appropriate Training to Fill Gaps**
  One of the main constrains to this control is, in fact, the topic of this works: understand the security needs of IoT. Even if the correct assessment and gap analysis are done, it is essential to understand how to fill those gaps.

- **#18 - Application Software Security**
  Important control to IoT and one of the main concerns points. For example, the lack of secure development methodologies and lack of security verification in third party developed devices. Also, the lack of updates to systems.

- **#19 - Incident Response and Management**
  Some constraints in the applicability of this control might e related to lack of knowledge and diversity of IoT devices in the forensics operations and lack os operational capabilities related to logging and auditing (from control #6)

- **#20 - Penetration Tests and Red Team Exercises**
  Applicable, but as in the case of #1, when considering pen-testing exercises suing the network, tools might not be ready for the multitude of IoT protocols or might not be desirable to probe the IoT device.

3.1.6 OWASP

The OWASP project compiled a list of the most common and more critical vulnerabilities in IoT. This list called IoT Top 10 vulnerabilities, is a joint effort of the security industry to help developers, manufacturers, enterprises, and consumers to make better decisions when dealing with IoT systems[30]. This is a list with similar objectives of the list done by OWASP project but for web applications and the objective is to have a practical and straightforward reference in terms of IoT security. Table 3 lists the top 10 vulnerabilities present in both IoT and web applications. In this same table, there is also the comparison between IoT top 10 from 2014 and 2018 where the "evolution" of IoT principal vulnerabilities can be seen. Comparing the changes from 2014 to 2018 there is still a strong focus on authentication/authorization problems and with vulnerabilities in the "interfaces" (web interfaces, APIs, mobile interfaces, cloud interfaces) and for example new concerns in 2018 like the need for device management. It is not an entirely "fair" comparison, but comparing which vulnerabilities are only present in the IoT case and finding the probable reasons for this:

- Lack of Transport Encryption - due to the new IoT protocols, lack of security awareness and constrained resources
- Poor Physical Security - due to the strong "physical" aspect of IoT and wide physical boundaries of IoT systems.
- Insufficient Security Configurability and Insecure Software/Firmware - due to the constrained resources and lack of security awareness
- Lack of Device Management - due to the lack of security awareness, proprietary systems, and multiple stakeholders.
- Insufficient Privacy Protection- due to the lack of security awareness, pervasiveness, and high data collection

The OWASP Internet of Things Top 10 Project (2014)	**The OWASP Internet of Things Top 10 Project (2018)**	**The OWASP Ten Most Critical Web Application Security Risks**
1. Insecure Web Interface 2. Insufficient Authentication/Authorization 3. Insecure Network Services 4. Lack of Transport Encryption 5. Privacy Concerns 6. Insecure Cloud Interface 7. Insecure Mobile Interface 8. Insufficient Security Configurability 9. Insecure Software/Firmware 10. Poor Physical Security	1. Weak, Guessable, or Hardcoded Passwords 2. Insecure Network Services 3. Insecure Ecosystem Interfaces 4. Lack of Secure Update Mechanism 5. Use of Insecure or Outdated Components 6. Insufficient Privacy Protection 7. Insecure Data Transfer and Storage 8. Lack of Device Management 9. Insecure Default Settings 10. Lack of Physical Hardening	A1:2017 - Injection A2:2017 - Broken Authentication A3:2017 - Sensitive Data Exposure A4:2017 - XML External Entities (XXE) A5:2017 - Broken Access Control A6:2017 - Security Misconfiguration A7:2017 - Cross-Site Scripting (XSS) A8:2017 - Insecure Deserialization A9:2017 - Using Components with Known Vulnerabilities A10:2017 - Insufficient Logging & Monitoring

Table 3 – IoT top vulnerabilities vs Web top vulnerabilities[31][32]

3.1.7 State-of-the-Art and Challenges for the Internet of Things

The work State-of-the-Art and Challenges for the Internet of Things presents a global overview of the security aspects of IoT[2]. This document defines a set of possible vulnerabilities and threats that could compromise an individual IoT device or the network as a whole:

- Vulnerable Software/Code
- Privacy threat
- Cloning of things
- Malicious substitution of things
- Eavesdropping attack
- Man-in-the-middle attack
- Firmware attacks
- Extraction of private information
- Routing attack
- Elevation of privilege

- Denial-of-Service (DoS) attack

Until now, all the literature reviewed is somehow focused and related to IoT. Nevertheless, the extensive work done already for "traditional ICT" cannot be excluded. Organizations like ISO and NIST have a solid set of security standards and frameworks that can have applicability in the IoT case. As an example, ISO 27002 and NIST SP 800-53 are two of the most comprehensive catalog of security controls used in "traditional ICT" that IoT environments could benefit from. In fact, ISO 27002 is currently under review for the inclusion of, among others, controls related to IoT. It is true that, as they are today, some of these frameworks, due to the particularities of IoT, might be facing some challenges when applied to IoT. Applicability of technical controls will depend for example on the existence of security feature in IoT systems that allow the implementation of the control in IoT(e.g., AV, FW, etc.) or the "strength" of the control in IoT(e.g., cryptographic controls are an example of controls that might not have "strong" implementation in IoT devices due to IoT low power and memory capabilities). Overall administrative controls should be easy to implement as they cover management situations. Another example is the controls that deal with physical and environmental security, that due to the high number of devices and the localization of some of them can be challenging to implement in IoT. The bottom point is that current security framework is an important source of information and a starting point for IoT security, but that might need adaptation.

This section summarizes the work done by different organizations in the area of IoT security and identifies the main security challenges that IoT has. It is clear that similar security concerns are commonly identified by different organizations. The next section will discuss the security aspects of IoT communication protocols.

3.2 IoT Protocol security

Protocols are an essential aspect of any "information and communication" system and so are hey also an important part of IoT systems. A correct security review of IoT must also pass with a more focused review of protocol security. There is a multitude of IoT protocols and stacks, some of them proprietary. A complete review is not in the scope of this work, and this section will analyze the security issues of the stack presented in Figure 2. This analysis is strongly based on the work done in [3] and [26]. In both of these works, the authors did an extensive analysis of security features provided by current IoT protocols for each layer and identified the still existent security problems and limitations that need to be addressed. Security problems identified are mainly related to protocol design, lack of security features, and protocol vulnerabilities.

3.2.1 Data link layer

At the data link layer is the 802.15.4 protocol. 802.15.4 supports security services for data confidentiality, data integrity, and replay protection[26]. This is achieved through hardware support for symmetric encryption using AES with 128-bit keys using different security modes[3]. 802.15.4 protocol also provides access controls mechanisms using ACLs where a particular address is associated with security parameters (e.g., security suite used, keys, IV) [3]. Some of the identified issues identified in the protocols that can hinder security are that there is not a keying system, some potential problems with the management of IV values that can be used to recover plain text and not being able to protect acknowledgment messages what can lead to acknowledgment forging.

3.2.2 Adaptation layer

At the adaptation layer, there is 6LoWPAN protocol. There is no security mechanism current define in the protocol specification. Sensitive information should be protected by mechanisms from layers above like application, transport, and network[26]. But there are discussions about the possible security vulnerabilities and security requirements for this protocol[3][33] mainly when used with 802.15.4. Some of the possible security problems are: forging of or accidentally duplicating EUI-64 interface addresses, security problems with neighbor Discovery and mesh routing. Other issues related to 6LoWPAN is the compression used in UDP ports and the possible effects of overloading. This may increase the risk of application getting the wrong type of payload[3][34]. Another issue is fragmentation attacks as this protocol fragments original IPv6 packets to be able to use a smaller packet size of 802.15.4, and there is no authentication in this layer[3]. Some proposal to guarantee security in this layer (confidentiality, integrity authentication, and non-repudiation) is to adopt IPSec although constrained IoT devices might not cope with the request. For the fragmentation attack, there is the proposal of adding additional fields to 6LoWPAN like timestamps and nonce to protect against fragment replays.

3.2.3 Transport layer

Transport layer is usually implemented in UDP/DTLS, and it is out of scope of this analysis.

3.2.4 Application Layer

At the application layer is the CoAP protocol. CoAP security is strongly based on lower layers(e.g., the transport layer DTLS) to transparently apply security to all CoAP messages [3]. CoAP also defines four security modes defining different ways how authentication and key negotiation is performed: NoSec providing no security(DTLS is disabled), PreSharedKey using a list of pre-shared individual or group of symmetric keys, RawPublicKey using public/private keys but not in a PKI infrastructure and Certificates using X.509 certificate and a PKI infrastructure[3] [26]. Some concerns about CoAP security are the risk of amplification where an attacker created a small packet and uses CoAP to turn it into a larger attack packet, using this to cause denial-of-service attacks by using the amplifying properties of the protocol and the inherent use of UDP, susceptible to IP spoofing. Some mitigation measures for the amplification attack can be to restrict the amount of traffic that CoAP “networks” can generate(this is similar to the current DDoS protection measures). Spoofing can be mitigated by DTLS or using “authentication” tokens in the request and reply[26]. Regarding key management, there is no defined solution in CoAP. Keys are assumed to be available or resulting from DTLS handshake[3]. One of the many issues with this layers is that it is using security services from DTLS and DTLS have some issues: no group key management, no multicast, also some issues with big DTLS messages that are fragmented by lower layers and also with the possible use of “gateways/proxies/reverse proxies.” Some proposal involves offloading many cryptographic functions to other more powerful devices. Also, another proposal involves building security in the CoAP protocols itself.

The IoT communication stack analyzed in this section still has security problems that should be addressed to improve overall security, mainly when it comes to mass adoption of IoT. In fact one of the main problem identified in all layer is the problem with the management of cryptographic keys that will enable other security features like identification, authentication and secure communication. The next section will briefly introduce the security auditing theme in IoT and laws and regulation related to IoT.

3.3 IoT Auditing, laws and regulations

Security without proper auditing can be ineffective. Security auditing or assessment is a way to confirm and establish solid proof that security policies are being followed and security controls are implemented and working as expected. From [35] auditing/assessment is "the determination of security and privacy control existence, functionality, correctness, completeness, and potential for improvement over time."

If, for IoT security, there is already some work done, what concerns IoT security auditing the case is entirely different as there is not much information about it and there are not specific auditing methodologies for the IoT case. Being IoT a recent concept and lacking specific auditing procedures, it is vital to understand the "traditional ICT" auditing methodologies to better evaluate the applicability to the IoT case. Some of the most important frameworks and standards related to "general" auditing and security auditing are NIST SP 800-53Ar4, NIST SP 800-115, ISO/IEC 19011, ISO/IEC 27007, ISO/IEC 27006.

NIST SP 800-53Ar4 and ISO/IEC 19011 are generic procedures with similar approaches, although with some differences. Both define an audit objective with some criteria and use a general methodology to collect pieces of evidence. These pieces of evidence are then evaluated against the objectives to find the audit results. The type of methods, to collect evidence, defined in both frameworks, is similar and includes interviews, examinations, and testing. Depending on the level of assurance required in the audit, these methods can be more or less intrusive and more or less comprehensive. NIST defines this with two attributes: depth and coverage. ISO 19011 also characterizes the audit methods, using the level of involvement between auditor and auditee (with or without human interaction) and the location of the auditor (remote or on-site). ISO/IEC 19011 also states that, when it is not practical or possible to examine all available information, sampling must be used. Sampling must be done in a way that assures representativeness of the full scope and that the information provided by the samples can fulfill the audit objectives. ISO 19011 defines the following criteria to perform sampling: judgment base sampling and statistical sampling. NIST SP 800-115, adds and complements NIST SP 800-53Ar4 describing assessment techniques with a more technical focus. ISO 27007 also complements ISO 19011 with specific requirements for auditing information security management systems (ISMS based on ISO 27001). These are two of the most known frameworks for generic auditing that might be applicable to IoT.

Another point of view of auditing is given by authors of [36] where it is suggested that auditing is better done when the full audit "domain" is divided into "sub-domains." In this respect, seven sub-domains are defined: user domain, workstation domain, LAN domain, LAN-to-WAN domain, wan domain, remote access domain, and system/application domain. For example, the workstation domain includes the systems (physical hardware, operating system) that are used by the user. Of course, interactions between each subdomain must be accounted and not overlooked.

Another worldwide recognized framework for security certification is the common criteria framework - ISO/IEC 15408. Although not specifically tailored to the IoT case (or to any case in particular), it might have good applicability in these systems. The main challenge is to create protection profiles adequate to the IoT case. Some vendors are already using this framework and have created PPs to evaluate their products [37][38].

One of the few reflections done specifically about IoT security auditing is done by authors in [39]. Although not focused on the "pure" auditing procedure per se and more on a risk management approach, authors state the fact that auditing IoT is not an easy task. Authors conclude first that there is no consensus around what is IoT and that there are no universally accepted standards for IoT security. Authors advice to follows an audit approach based on risk assessment to better frame the audit objectives and the scope. Then authors define an IoT audit framework based on different groups of security controls: general baseline controls, data-related controls, analysis, and learning-related controls, and business and process alignment controls. For each group of controls, relevant sources are given from where the specific controls can be drawn. Another work-related specifically to IoT audit is described in [40]. Authors follow the same risk assessment approach as in [39] but this time based their controls on NIST SP 800-53. The method proposed is to first define an "expanded" version of the "TCP/IP" model with more layers and then to analyses the applicability of controls, with priority P1 from NIST SP 800-53. These control objectives are then adapted to the IoT specific case and assigned to the layers of the "expanded" version of the "TCP/IP" model. This assignment will allow to find overlapping and duplicated controls in each layer. The authors' conclusion is that, from all the practical analyses to different IoT scenarios that they have done using this method, the result was always the same list of 12 controls leading to the conclusion that this can be applied to any IoT scenario only with small adjustments.

Beyond all the technical details and security concerns that are related to IoT, the rapid rate that IoT environments change brings new legal and regulatory challenges that are broad and complex. It is important that legal structures adapt and follow this rapid evolution in technology[9]. This is clearly important in security matters. One import aspect of increasing the level of security is the existence of robust regulations and laws. In this respect, IoT is still very incipient. Besides all the laws and regulations that apply indirectly to IoT (e.g., GDPR), there is not much specific regulation on IoT. California state was the first to try to regulate IoT with the SB-327[41], [42] but also, in this case, it shallows touches IoT security. Another law - "Internet of Things Cybersecurity Improvement Act of 2017" regulates IoT systems purchased by federal agencies and its scope is though limited as it does not strictly impose security measures to IoT but defines the security requirements that must be observed when buying these systems. UK government is also making some efforts in this respect with a definition of mandatory industry requirements to ensure consumer smart devices enforce a basic level of security [43]. The goal is to force these requirements mandatory. This is not extensive research on the topic, but the literature review clearly shows that there is still much to be done in this area of IoT.

3.4 Summary of the main security concerns of IoT

The main conclusions that can be taken from this literature review are that IoT security needs are not that different from "traditional ICT." Nevertheless, these security needs are not backed up with the needed security tools, or these tools are not available yet. In fact, most of the time, the security requirement is clear, but the security controls needed are not applied. One example is the secure development of software and hardware that is a reliable methodology in "traditional ICT" but is not applied to the IoT case; another example is the patching of systems. However, as already seen in the previous chapters, IoT has some particular and specific characteristics that will present new security challenges[25] [9]. New threats and vulnerabilities specific to these systems will present new risks that must be considered, and with the rapid development of IoT, need to be continuously assessed. These are, in fact, the points where a new security "thinking" must be done. Some of the new security issues that IoT will introduce are:

The high number of devices brings additional concerns in terms of security as, for example, among other issues, increases the attack surface, regular routine update and maintenance operations will be a challenge [25] and of course the use of compromised IoT devices for massive DDoS attacks[26], [9].

The cyber-physical aspect of IoT is one of the most critical aspects of IoT that requires strong security[26]. Security problems in these types of systems can have direct and severe effects on human safety[9]. There are many examples of possible attacks, taking advantage of this physical interaction, which can cause severe incidents. One good example is the recent "smart cars" where it was shown that an attack could interact with sensors and actuators (e.g., brake) of the vehicle possible causing accidents.

Pervasiveness - will have an impact on **privacy** aspects as these devices are more and more collecting, storing and using sensitive data and this can jeopardize aspects of our privacy, and in some cases, the user is not aware of it[26][6]. Per se, this characteristic is not enabling attacks but increases the attack surface, the probability of a successful attack, and the changes and increases the consequences of attacks. For example, in the IoT scenario for health monitoring, an attacker can compromise the privacy of a user's health information with more success, and a successful attack could have adverse consequences.

Big data[26], [9], [25] - The type and amount of information produced by these systems will allow fists, more and different type of information that can be obtained in case of a system compromise, and also a stronger correlation of data allowing more "knowledge."

D**evices in the device layer, are resources constrained -** This fact has many implications for security. It will hinder common security measures from being applicable. One example is cryptography that requires an enormous amount of processing power, making some algorithms not feasible for IoT. Also, the usual security features of OS like memory management might not be possible in these constraint devices. Also constrained devices means that DoS attacks(to the device itself) will be more probable and in this case protocols and operating systems will need to be designed with this in mind and always with the goal of fail-safe behavior.

Lack of security awareness and security motivation - this will lead to the lack "common security measure." manufactures and vendors are not including these measures (e.g., lack or weak access controls[30]) in the device. Alternatively, the security controls are not yet available (e.g., IoT firewall, antivirus, etc.) [25]. Or the security controls are not yet available (e.g., IoT firewall, antivirus, etc.) [25].

Lack of physical control and lack of "single physical location"[26]. In "traditional ICT," a key point when defining security, is implementing physical security of systems. However, in the case of IoT, this is not always possible, creating many security implications (e.g., access to data, access to cryptographic keys, etc.) [29]. On the high **mobility** side, devices will be more exposed to dangerous networks, increasing the compromise possibilities[6].

Heterogeneity - leads to f**ragmentation** in standards, security approaches, protocols, etc., meaning, among others, more vulnerabilities, an increased attack surface, more challenges to device management and security management[29].

More real-time dependent - This has implications in the possible security controls used, as these measures cannot introduce actions that can cause delays. For example, some real-time systems cannot wait for the decision of antivirus or an IPS when these introduce considerable delays.

D**ifferent needs in CIA** as usually, in traditional IT systems, confidentiality is the most crucial aspect of security, then integrity, and in last availability. As IoT systems are used in different, security objectives will be prioritized very differently. In some cases, these systems have more strict security needs in integrity and availability than in confidentiality. This aspect is mainly due to the "physical aspect" of IoT and the need for human safety. That is why some IoT systems must have more concerns on safety and resilience that "traditional ICT"[26]. As an example, in a traffic management system, it is more critical to guarantee that an attacker cannot modify instructions to the system that ensuring that these instructions(or any other data) cannot be seen.

System complexity, "dispersion" and extension of boundaries - IoT systems are highly distributed[26] making security definition and accountability harder to define[9]. One example is the substantial usage of the cloud systems where it is harder to define security responsibilities, and perimeter security is less effective[25]. This is also reflected in the location of IoT data. Data can be processed locally, remotely, or in both locations[26], making security and privacy hard to define and control. This lack of boundaries is also characterized by the lack of exclusive controls of some IoT devices; many IoT systems can be remotely controlled by manufacturers[26].

Long-life of IoT components will imply in some cases, static systems without possibility, for example, that software can be updated, or configuration changed [26], [29].

Thing-to-Thing (T2T) communications will allow communication of devices without a "system view" or a "control point." Monitoring and filtering tools, for example, will be more challenging to implement. [2].

Interdependence will allow attacks to a secure system to be directed, not to the target system, but to weaker systems that have a relationship with the first, influencing the behavior of it[6].

Table 4 present the summary of the main IoT security concerns from the different organizations. Although the type of finding present by the different organization is done at different levels, i.e., some are more generic and other concrete vulnerabilities, some of them are identified by different organizations (signalized in the table with the same color).

- The fragmentation, heterogeneity and proprietary aspect of the whole ecosystem
- The design and development process of IoT systems
- The IoT device lifecycle management
- The IoT update management
- The IoT physical security
- The privacy concerns in IoT

Main challenges for IoT security

ENISA[9]	**NIST**[26]	**OWASP**[30]	**State-of-the-Art and Challenges for the Internet of Things Security**[2]	**Security Guidance for Early Adopters of the Internet of Things (IoT)** [25]
IoT security fragmentation and lack of regulations	remotely controlled by manufacturers	Weak, Guessable, or Hardcoded Passwords	Vulnerable Software/Code	systems are poorly designed and implemented
lack of security awareness in IoT	no centralized management capabilities	Insecure Network Services	Privacy threat	IoT still lacks mature technology and processes
design and development security problems	highly dynamic systems	Insecure Ecosystem Interfaces	Cloning of things	lacks management and maintenance of the device
interoperability problems	proprietary protocols	Lack of Secure Update Mechanism	Malicious substitution of things	unique physical security issues
lack of economic incentives to foster security	highly heterogeneous (operating systems, network interfaces/protocols, functions, etc.)	Use of Insecure or Outdated Components	Eavesdropping attack	complex privacy concerns
product lifecycle management problems	collection of massive volumes of data	Insufficient Privacy Protection	Man-in-the-middle attack	lacks mature guidance and processes for IoT development
	data processed data locally and remote	Insecure Data Transfer and Storage	Firmware attacks	lack standards and processes for authentication and authorization
	static systems (e.g., not updates, configuration cannot be changed as needed)	Lack of Device Management	Extraction of private information	lacks guidance and processes for incident response activities

ENISA[9]	**NIST**[26]	**OWASP**[30]	**State-of-the-Art and Challenges for the Internet of Things Security**[2]	**Security Guidance for Early Adopters of the Internet of Things (IoT)** [25]
	low-capability computing hardware (processing, storage, power, etc.)	Insecure Default Settings	Routing attack	lacks standards and processes for logging and audit
	autonomous aspect of IoT	Lack of Physical Hardening	Elevation of privilege	Lack of methods and processes to achieve situational awareness of secure posture of IoT assets
	highly distributed systems with a variety of owners		Denial-of-Service (DoS) attack	lacks standards, guidance, and processes for IoT virtualization
	direct connections to non-owner networks			complex configuration
	deployed in physically unrestricted locations			Differs protocols and technologies
	statistical errors when sensing and acting on physical objects			
	collection, storage, and use of personal data			
	created through combinations of existing IoT systems for an application not envisioned by the original end			
	long life of components			
	poorly connection (dropped packets, interrupted connections)			

Table 4 – IoT main security concerns summary

This literature review from this chapter, allowed to address many aspects of IoT security. These aspects included general IoT security concerns, technical vulnerabilities of IoT, an overview of IoT protocol security concerns, IoT auditing and IoT regulation. The information reviewed, in an essential part of this work as it sets the foundations for the following phases of this work, where these security aspects are considered in the assessment of a particular IoT scenario.

4 IoT in SmartCities

IoT, most of the time, is not used alone but usually is an enabling part of more significant systems using IoT to achieve their objectives. Among these use cases, there are many differences, either in terms of technology and security requirements. Some examples are the "smart" counterparts of regular "services": smart health, smart cars, smart cities, smart industry, smart homes, etc. One of the uses cases with more expression currently are smart cities. IoT enables smart cities in many areas, like waste management, power management, and traffic management. Being smart cities a concept with more and more acceptance, it is important to understand what type of security threats these systems can face and what vulnerabilities they have. This chapter introduces briefly the concept of smart cities and describes the IoT scenario that is going to be used in this work.

4.1 SmartCity overview

Reports forecast that by 2030, 60% of the population will be living in cities. This will bring some challenges on how the current model of cities will handle this increase[44]. It is urgent then to find ways to cope with this demand and increased pressure in already high-density places. One of the ways to achieve this is with the introduction of technology that can help to manage better either people or resources. Today's new concept of cities that will encompass this is called Smart Cities. This new concept of a smart city is going to bring several benefits to people's lives. Among are economical and environmental benefits and measures to improve citizen's lives. Although these types of solutions are still young and, as in any other young technology, open to security discussing[45].

Smart city solutions are strongly based on IoT technology and will inherit all IoT strengths and weaknesses, and this includes the security weaknesses of IoT. In this respect is of great importance to assure that these cities of the future are secure and will not increase or create new risks for people living in it. Attacks to smart cities could have severe consequences for human lives, to the environment and economy. Attacks on water treatment facilities can pose a danger to human lives or to the environment. Attacks to power facilities can cause economic damages[45]. There are many examples of "sub functionalities" in a smart city where small security problems can cause severe impacts on human lives. The reasoning behind the choice of the "sub scenario" of smart cities used in this work was to find a scenario where a security incident could cause a high impact on human safety. Although there are many options, like water management, energy, health, the final choice was the traffic management use case.

4.2 Traffic management

The management of vehicles is one of the critical aspects of cities and is also one of today's main problems, mainly in big cities. Traffic problems have, just to name a few, substantial economic and environmental consequences. Also, there is an impact on people's quality of life. Without a doubt that this is a good example where a "smart" solution could bring new solutions and advantages. Traffic management is today, together with others, one of the main use cases for IoT in smart cities. Organizations hope that a smart solution with real-time data and real-time decisions can mitigate the current traffic issues that cities face today. With solutions like this, decisions can be based on accurate and real-time data, for example of actual traffic "hot points" and can make better decisions to "reroute" the traffic to less congestionated roads. However, traffic congestion is not the only function of smart traffic management solutions. For example, it can be used to help in an emergency where traffic rerouting or blocking is needed (e.g., in a fire situation or accident) or detecting hazard conditions like wrong-way driving. There are many situations where security breaches on a system like this can cause different types of damage. Economical and environment damages where the rerouting of traffic is done to the most congestionated point or safety damage when all traffic lights are set to green. Being this type of systems new either in terms of technology and in applicability in real use cases, it is important to understand what type of security risks are present in it.

4.3 Scenario description

The scenario used in this work is fictitious. Nevertheless, it is based on real smart city(with traffic management) solutions that are being tested in some cities and in solutions proposed in the research literature. In the design of this fictitious scenario, the "common" and basic features of the different proposals were used. Figure 5 shows the final architecture based in the IoT architectures from section 2.2 composed by a device layer(with sensors and actuators), a fog layer, a cloud/backend layer all of them connected by a communication layer.

The device layer is composed of acoustics sensors and inductive loops sensors and actuators in the form of traffic lights, informative panels, and "smart" traffic signals. The sensor's objective is to obtain essential data that will help the decision process. For example, the speed of vehicles, the number of vehicles stopped the number of vehicles per hour, etc. On the other hand, the actuators will "display" the information resulting from the decision process. Traffic lights will go green or red to manage traffic flows, "smart traffic signs" will change accordingly to the needs and information panels will give informative data (e.g., alerting the offended driver and other drivers that there is a wrong way driving condition).

Figure 6 shows the communications layer responsible for connecting all the layers in the whole system. At the device layer side, the protocols used are IEEE 802.15.4 and also IEEE 802.11 with the use of concentrators and gateways. If needed, IoT devices can use the Full Function Device and Reduced Function Device of 802.15.4 where an IEEE 802.15.4 device can act as an "802.15.4 bridge" for devices that cannot reach the concentrator. The network topology is mainly star, with the concentrators/gateways being the central point. On the network/adaptation layer, 6LowPAN is used in the device layer and IPv6 in the communication with fog and cloud. On the application layer, CoAP is the primary protocol to communicate with devices. The fog layer(the traffic management controller) is responsible for managing real-time decisions of a small number of sensors and actuators. This layer has a "limited view" of only some sensors and actuators and makes real-time "standard" decisions based on instructions received previously from the cloud/backend layer. If needed, this layer will request help from services in the cloud/backend layer. The cloud/backend layer has a global view of the systems and is responsible for making global decisions and instructing traffic management controller layers. It is also responsible for making available interfaces for regular users and administrative users (e.g., normal users consult traffic status, administrative users consult reports of the systems). Figure 4 shows how these systems can be implemented in a real scenario. The acoustic sensors are marked as ◎ and the inductive loop sensors as ●. The actuators are traffic lights and traffic signals. The red communication arrows are the communication from the sensors and actuators towards gateways/concentrators, and the blue communications arrows are the possible use of Full Function Device and Reduced Function Device modes. Communication from gateways towards traffic management controller(fog) is done via LTE and from traffic management controller toward cloud also using 5g or fiber.

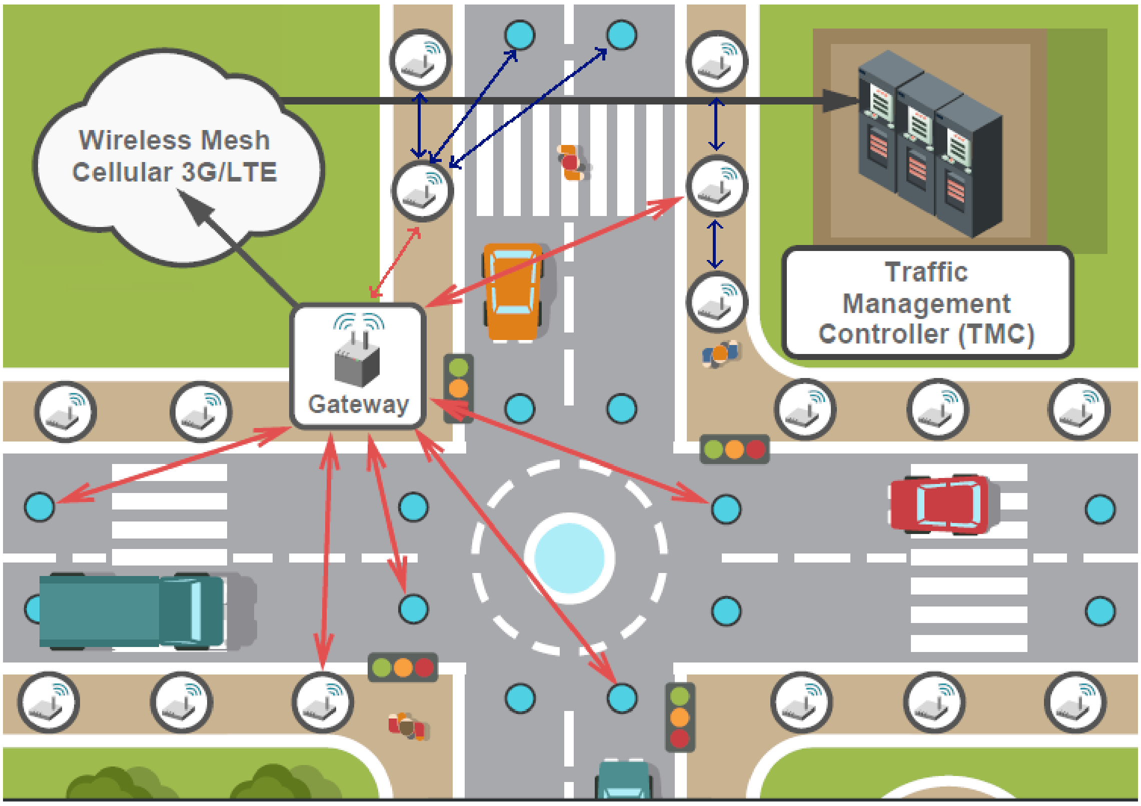

Figure 4 – IoT traffic management scenario (picture copied from [46])

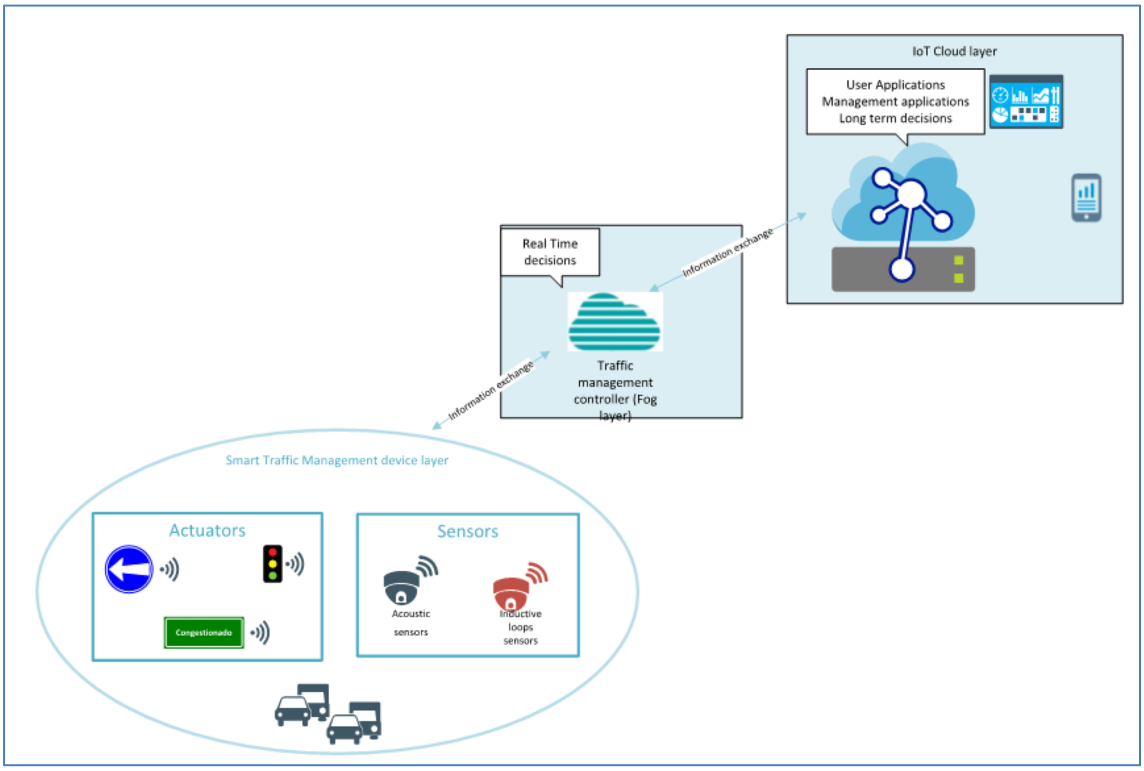

Figure 5 – IoT traffic management solution high-level architecture

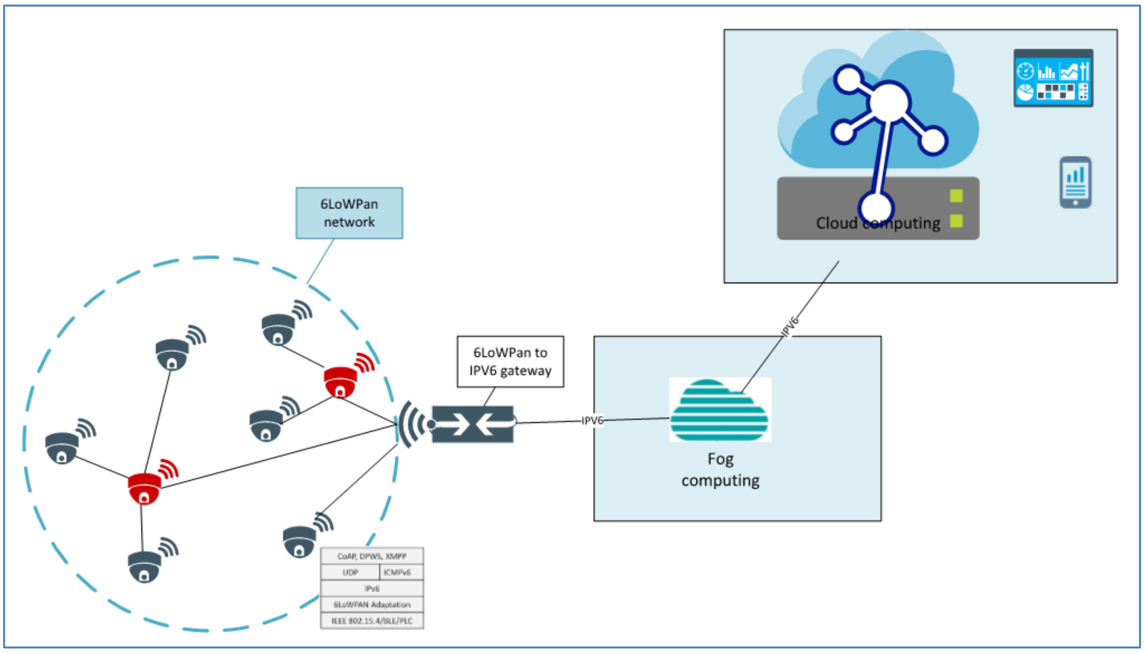

Figure 6 – IoT traffic management solution network architecture

There are many other functionalities that of traffic management solution can have. For example, interacting with the vehicles that use the road, receiving information from the vehicles, and providing information to the vehicles. This functionality, depending on the possible features, would increase the level of criticality that these systems would have. Imagine when traffic management systems can interact, systems in autonomous cars!

The scenario described in this chapter is are the one used in the risk assessment exercise, done in the following chapter, taking into consideration the security concerns reviewed in the previous chapters.

5 Metodology for Security Assessment in IoT

A security assessment is a process of determining how effectively an entity (e.g., information system, a server, network, procedure, device, etc.) is in line with the defined security requirements[47]. The security requirements are defined around the three fundamental properties of security (i.e., confidentiality, integrity, and availability) using tools like security policies, security plans, standards, baselines, etc. The assessment also has a different goal from a security audit, as defined in section 3.3. The objective of an audit is to obtain evidence that defined controls/policies are implemented, where an assessment objective is to assess if security objectives are being followed and possibly to defined or help to define the measures to implement to achieve those objectives. In any case, the assessment process, like any other security process, should not be a onetime process and should be included in every step of the lifecycle of the object being assessed. In this work, the security assessment objective is to identify the security risks present in a traffic management system. The results of this assessment, where possible risks to the systems are identified, are then used as the input to another process called risk response(or risk treatment), where security controls to respond to these risks, are defined. This chapter defines the adaptation of the methodology of risk assessment defined in NIST SP800-30 rv1framework [7] and the application to the scenario described in Section 4.3.

5.1 Risk assessment

Organizations, in general, are exposed to threats. These threats can have adverse effects on many aspects of the organization. The degree of warm of these effects depends on many factors, not only on the threat itself but also on the impact and likelihood that these threats can cause. The risk assessment is the process where this analysis is done. Risk assessment is a fundamental part of the overall and broader process called risk management and allows a systematic and reproducible process of identification, estimation, and prioritization of risk present in the organization[7]. Risk management is a comprehensive and complete process where the final goal is to manage these risks identified by the risk assessment process. Risk management, including risks assessment subprocess, is a common practice in an organization to protect traditional ICT systems and will continue to be an essential part of IoT systems[26]. The risk assessment methodology defined by NIST SP800-30 rv1framework [7] is also by itself a comprehensive methodology but defines a flexible approach that can be adapted to many organizations and situations. In the following section, the application of this framework, to the scenario at evaluation, is explained.

5.1.1 Purpose

The objective of this risk assessment is to identify threats and vulnerabilities that can result in risks, impacting a traffic management solution. Traffic management solutions will be a reality in the future, and it is important to understand what are the risks that these types of solutions might have. This analysis is an initial assessment, and it is based on the final architectural design of the traffic management solution as defined in the previous chapters. With this early assessment risks present in the foreseen solution are identified, avoiding the propagation to further phases and tackling the security in an early stage. The outcome of this analysis will be a list of prioritized risks that will be the input to the risk response process where identified risks can be managed. The added value of this exercise is that it can give insights on how different and specific risks are in IoT, and how the current security controls are ready to respond to these new risks. This process can then be reused in similar use cases.

5.1.2 Scope

IoT systems are part of organizations with specific characteristics and requirements. Risk assessment (and risk management) should always be defined accordingly with these aspects of the organization. For example, risk appetite is different from organization to organization; the validity of a risk assessment can also be different; the risk monitoring conditions will also be different. The risk assessment frameworks are also flexible and "allow" only the definition and use of some parts of the framework that are needed to a specific case. This is to say that, as the objective is to assess possible risks to a traffic management solution, some considerations that are part of the complete risk assessment procedure, are not going to be defined(e.g., risk monitoring conditions, etc.).

Risks can be identified in the different layers of the IoT architecture. As the objective of this work is mainly to understand the specific risks to IoT and being the main differentiator the device layer, the scope will be mainly on the IoT device layer as defined in section 2.2. As for the three layers, defined in [7] where risks can be identified, all the layers are considered, but only when directly related to the device layer. Taking this into consideration, risks directly to the cloud environment used in the solution are not considered as also risk to the possible web or mobile applications that are used in the solution. We can consider that the cloud is managed by a cloud provider, and risks are transferred to the cloud provider by means of contractual enforcement of security measures. However, risk identification is better done when assessed, taking into consideration all the layers of IoT architecture (section 2.2) and all the layers of risk as defined in [7]. This is because an exercise of risk assessment in only part of a bigger system is always restrictive. The interactions between different components are not considered, and possible threats and vulnerabilities not found because they are only visible when seeing the big picture. The same happens when not considering the interactions between different but cooperating systems where the risk of a systemic attack is not also considered(e.g., traffic management systems with the fire management systems). In terms of risk tolerance (or risk appetite), as these systems can have a direct impact on human safety, the risks that can be tolerated are very few, making the risk tolerance low.

5.1.3 Assumptions and constraints

One of the main constraints of this assessment is the fact that the scenario used fictitious, and the scenario description might lack "real" information to assess the risks correctly. Smart cities and IoT, are a relatively new concept, so there is still a lack of knowledge of specific threat and real vulnerabilities that these entities might face. Therefore, “common” threats and vulnerabilities are going to be considered in this assessment, as also all the security-related information from the literature review done in the previous chapters(i.e., ISO, NIST, ENISA, OWASP, etc.). These “common” threats and vulnerabilities are based on the “database” available on NIST SP800-30[7].

Threats

Threat sources considered are the ones from table D-2 of NIST SP800-30 [7] and the threat sources not present in the previous table and that are mentioned in the literature review done in the previous chapters. Although all threats are relevant, in this work, only adversarial threat sources are considered. Likewise, threat events primary source of information is also Table E-2 from NIST SP800-30 [7] and any other threat events that are referenced in the literature review done in the previous sections. Again, although all threats are relevant, in this work, only adversarial threat events are considered. Concerning the degree of confirmation needed for threat events to be considered relevant to the risk assessment, it is the one indicated by “possible” in table E-4 [7] (i.e., threat events that can possibly affect IoT).

Vulnerabilities

Vulnerability information is mainly derived from the literature review done in the previous chapters. The vulnerabilities considered are the ones affecting mainly the device layer of the IoT architectures (e.g., hardware, software, firmware, internal controls). Vulnerabilities that might affect the system indirectly, for example, related systems are not considered. Table F-2 from NIST SP800-30 [7] is used to define the degree of severity of the vulnerability.

Likelihood

Likelihood of occurrence determination is supported by the previous literature review done in the previous chapters and is determined using the scale values and procedure from tables G-2, G-4, and G-5 from [7].

Impacts

The impacts of a successful attack are determined, taking into consideration the level of exposure of the vulnerability and the consequences. In this respect, table H-3 from NIST SP800-30 [7] is used for measurement of the impact level.

Risk Tolerance and Uncertainty

Low-risk tolerance is assumed, as, in these types of systems, even a lower risk could have an adverse effect on people's safety. Also, there is a considerable amount of uncertainty of possible threats and vulnerabilities in these systems, as this type of systems are still not well known and have little real implementation.

5.1.4 Risk model and analytic approaches

The analytic approach used in this assessment is orientated to the threats that can affect the scenario. For these threats, possible vulnerabilities existent in the system components are assessed for relevance, and the level of likelihood and impact is measured. The risk model used is based on the factor threat, vulnerability, impact, and likelihood and follows the risk model present in NIST SP800-30. In terms of the assessment approach, the qualitative assessment is used as this scale of values is more adequate in a scenario where there isn't much information about concrete threats and vulnerabilities.

5.1.5 Threat identification

Threat identification is the first step of the risk assessment framework defined in NIST SP800-30[7]. As already mentioned, risk assessment is not a "one-way" procedure but an interactive process that can "revisit" previous steps. It is perfectly acceptable and desirable that this step is further refined in later stages.

Threat source identification and characterization is the first phase in the threat identification procedure, followed by the identification of the threat events that these sources can initiate.

Threat sources

Threat sources are the entities that can originate a threat event. As already state, only adversarial threats are considered. Table 5, adapted from NIST SP800-30[7], identifies and characterizes all the relevant threat sources used in the assessment. Adversarial threat sources are characterized by the capability, intent, and targeting, using the qualitative scales values defined in tables D-3, D-4, and D-5 of NIST SP800-30[7].

Identifier	**Threat Source (as in NIST SP800-30**[7]**)**	**Capability**	**Intent**	**Targeting**
ADVERSARIAL				
TS-1	Individual – Outsider (any individual with no direct or indirect link to traffic management system)	Very Low	Moderate	Low
TS-2	Individual – Insider (any individual with direct or indirect link to traffic management system)	Low	Moderate	High
TS-5	Group - Ad hoc (a group without specific organization or objective)	Moderate	Moderate	Moderate
TS-6	Group – Established(a group with specific organization, objective, working methodology)	High	High	High
TS-7	Organization – Competitor (any organization with the same business objective. E.g., another city)	Moderate	High	High
TS-8	Organization – Supplier (any organization with direct or indirect participation in the supply chain)	Moderate	High	High

Identifier	Threat Source (as in NIST SP800-30[7])	Capability	Intent	Targeting
TS-9	Organization – Partner (any organization with direct benefits from the relations with the city)	Moderate	High	High
TS-10	Organization – Customer (the user of the system)	Low	Moderate	High
TS-11	Nation-State	Very High	Very High	Very High

Table 5 – Threat source identification as it is defined in NIST SP800-30 in table D-7 [7]

Threat events

Threat events are actions initiated by threat sources, and that can cause warm. The following tables describe the possible threat events that can affect the traffic management scenario. Each table contains a set of threat events belonging to a specific category and the level of relevance for this security assessment. This threat event list is strongly based on NIST SP800-30[7]), adapted and augmented to the specific scenario.

Table 6 lists possible threat events that attackers can use to perform reconnaissance of the network and systems and obtain valuable information for later stages of attacks.

Perform reconnaissance and gather information		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-1	Perform RF perimeter network reconnaissance/scanning Adversary uses commercial or free software to scan IoT sensors, actuators and gateways RF perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks	Predicted
TE-2	Perform network sniffing of exposed wireless networks An adversary with access to exposed wireless data channels used to transmit information uses network sniffing to identify components, resources, and protections	Predicted
TE-3	Perform malware-directed internal reconnaissance Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.	Predicted

Table 6 – Threat events for "Perform reconnaissance and gather information" from NIST SP800-30[7] and adapted to IoT scenario

Table 7 list all possible threat events related to the different types of tools that an attacker can create to pursue an attack.

Craft or create attack tools		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-4	Create counterfeit/spoof IoT device Adversary creates duplicates of legitimate actuators or sensor "web interface"; when users visit a counterfeit site, the site can gather information or download malware.	Predicted
TE-5	Create and operate false front organizations to inject malicious components into the supply chain. Adversary creates false front organizations with the appearance of legitimate suppliers of IoT devices or IoT systems in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain	Predicted

Table 7 – Threat events for "Craft or create attack tools" from NIST SP800-30[7] and adapted to IoT scenario

Table 8 lists all the methodologies used by an attacker to deliver and install tools with malicious capabilities. The threats related to the supply chain are of great importance

Deliver/insert/install malicious capabilities		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-6	Deliver malware by providing removable media Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems. Or adversary has physical access to unprotected USB ports	Predicted
TE-7	Insert untargeted malware into downloadable software and/or into commercial information technology products Adversary corrupts or inserts malware into common IoT firmware, free OS, and others. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.	Predicted
TE-8	Insert targeted malware into organizational information systems and information system components Adversary inserts malware into organization IoT devices specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).	Predicted

Deliver/insert/install malicious capabilities		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-9	Insert specialized malware into organizational information systems based on system configurations Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.	Predicted
TE-10	Insert tampered critical components into organizational systems Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.	Predicted
TE-11	Install general-purpose sniffers on organization-controlled information systems or networks Adversary installs sniffing software onto internal organizational IoT devices.	Predicted

Table 8 – Threat events for "Deliver/insert/install malicious capabilities" from NIST SP800-30[7] and adapted to IoT scenario

Table 9 lists all threat events that can lead to the real exploit and compromise of an IoT system. Threats related to vulnerable code are very important as IoT system is considered to have insecure development procedures with little security awareness. Also the threats to mission-critical systems are important as traffic management systems are critical systems with the potential to jeopardize human safety.

Exploit and compromise		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-12	Exploit poorly configured or unauthorized information systems exposed to the network Adversary gains access through the network to information systems that do not meet organizational configuration requirements.	Predicted
TE-13	Exploit recently discovered vulnerabilities Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place	Predicted
TE-14	Exploit vulnerabilities on internal organizational information systems Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities	Predicted
TE-15	Exploit vulnerabilities using zero-day attacks Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations	Predicted

Exploit and compromise		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-16	Exploit insecure or incomplete data deletion at the end of life devices Adversary obtains unauthorized information due to insecure or incomplete data deletion in a device that reaches the end of life and was reused	Predicted
TE-17	Compromise critical information systems via physical access Adversary obtains physical access to organizational information systems and makes modifications.	Predicted
TE-18	Compromise organizational information systems to facilitate exfiltration of data/information Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information	Predicted
TE-19	Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware) Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers	Predicted

Table 9 – Threat events for "Exploit and compromise" from NIST SP800-30[7] and adapted to IoT scenario

Table 10 lists all threat events related to the effective conduction of an attack. Threats to the wireless communications are significant as these channels are usually insecure.

Conduct an attack (i.e., direct/coordinate attack tools or activities)		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-20	Conduct wireless jamming attacks Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients	Predicted
TE-21	Conduct simple Denial of Service (DoS) attack Adversary attempts to make an resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.	Predicted
TE-22	Conduct Distributed Denial of Service (DDoS) attacks Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.	Predicted
TE-23	Conduct brute force login attempts/password guessing attacks Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.	Predicted
TE-24	Conduct network traffic modification (man in the middle) attacks Adversary intercepts/eavesdrops on sessions between organizational systems. Adversary then relays messages making them believe that they are talking directly to each other over	Predicted

Conduct an attack (i.e., direct/coordinate attack tools or activities)		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
	a private connection, when in fact the entire communication is controlled by the adversary.	
TE-25	Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components	Predicted

Table 10 – Threat events for "Conduct an attack" from NIST SP800-30[7] and adapted to IoT scenario

Table 11 list all the threat events that are related to the final result and objective of attacks

Achieve results (i.e., cause adverse impacts, obtain information)		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-26	Obtain sensitive information through network sniffing of external networks Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications	Predicted
TE-27	Cause deterioration/destruction of critical information system components and functions Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern	Predicted
TE-28	Cause integrity loss by polluting or corrupting critical data Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.	Predicted
TE-29	Obtain unauthorized access Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization	Predicted
TE-30	Obtain information by opportunistically stealing or scavenging information systems/components Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components	Predicted

Table 11 – Threat events for "Achieve results" from NIST SP800-30[7] and adapted to IoT scenario

Table 12 lists all threat events that have the finality to maintain presence after an attack

Maintain a presence or set of capabilities		
Identifier	**Threat Event (as in or adapted from NIST SP800-30[7])**	**Relevance**
TE-31	Obfuscate adversary actions Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations	Predicted

Table 12 – Threat events for "Maintain a presence or set of capabilities" from NIST SP800-30[7] and adapted to IoT scenario

In this chapter, the assumptions and methodology for the security assessment done in the next chapter were defined, as also the threats considered relevant for the specific IoT scenario. In the next chapter, the security assessment will make use of this information to identify the concrete security risks.

6 Application of the proposed methodology

In this chapter, the proposed methodology for the security assessment, and the particular IoT security concerns and vulnerabilities identified in Chapter 3 are combined to reach a prioritized list of risks that affect the traffic management scenario described in Section 4.3. The security concerns and vulnerabilities identified and used in this procedure are exclusively derived from the literature review done in the previous chapters, and no other sources are used (e.g., personal knowledge of specific issues or other sources). The objective is to have solid conclusions based solely on the background information from the literature review. These security risks are then subject to a risk treatment process, where a concrete action of treatment for the risk is defined.

6.1 Vulnerabilities and predisposing conditions identification

Table 13 lists all the relevant vulnerabilities and predisposing conditions, grouped by domains, as identified in Chapter 3. These vulnerabilities and predisposing conditions are categorized with a severity level derived from the degree of leverage that these vulnerabilities can add to threats events. The severity scale used is taken from table F-2 and F-5 of NIST SP800-30[7].

Identifier	Vulnerability or predisposing condition	Severity
Physical boundaries		
V-1	Lack of physical security	Moderate
V-2	Sensors and actuators in public locations	High
V-3	Lack of physical hardening (e.g., secure storage of crypto material)	High
V-4	Unsecure physical ports (e.g., USB)	High
Logical boundaries		
V-5	Large attack surface	Moderate
V-6	“Dispersion” and extension of boundaries between many stakeholders	Very Low
V-7	High mobility	Very Low
Hardware		
V-8	Network constraints	Moderate

Identifier	Vulnerability or predisposing condition	Severity
V-9	Power constrained	Moderate
V-10	Cpu constrained	Moderate
Cyberphysical		
V-11	strong interaction physical world note:this is not a vulnerability to the device itself but for the surrounding environment, as for example people	Very High
Network security controls		
V-12	Lack of network security measures (e.g., host fw, DLP)	High
Security awareness		
V-13	Lack of security awareness	Low
V-14	"Long" supply chain	Moderate
Incident handling		
V-15	Lacks mature guidance and processes for incident response activities	High
Malware protection		
V-16	Lack of malware protection	Very High
V-17	Lack of common operating system security measures (e,g. process isolation, memory management)	Very High
Logging and auditing		
V-18	Lacks mature standards, guidance, processes for logging and audit	High
V-19	Lack of logging features in IoT devices	High
Permissions, Privileges, Authentication, and Access Controls		
V-20	Devices lack of access controls	High
V-21	Lacks mature standards, guidance, processes for authentication and authorization	High
V-22	Hardcoded Passwords	Very High
V-23	Weak and Guessable password	Very High
Privacy		
V-24	Insufficient Privacy Protection	Low
V-25	Access to large amounts and types of personal data	Very Low
V-26	Collecting, storage and use data without user awareness and control	Very Low
Storage		
V-27	Insecure Data Storage in devices	High
Device Management		
V-28	Lack of device management	High

Identifier	Vulnerability or predisposing condition	Severity
V-29	Patching not available	High
V-30	Lack of secure update mechanism	Moderate
V-31	Patching not always possible	Very High
V-32	Lacks mature guidance and processes for management and maintenance of the device	Moderate
V-33	Can be remotely controlled by other parties (e.g., manufacturers)	Very Low
System development		
V-34	Vulnerable Software/Code	
V-35	Software development insecure	
V-36	Re-purposing and combinations of existing IoT systems	Very Low
V-37	Lacks mature guidance and processes for IoT development	Low
V-38	Use of Insecure or Outdated Components	
V-39	Proprietary protocols	High
V-40	Fragmentation in security standards	High
IoT Virtualization		
V-41	IoT still lacks mature standards, guidance, and processes for IoT virtualization	Very Low
Networking		
V-42	Insecure network services	
V-43	Insecure data transfer	Moderate
V-44	Insecure ecosystem interfaces	Moderate
V-45	6LoWPAN compression of UDP ports	Moderate
V-46	6LoWPAN fragmentation attacks	Moderate
V-47	CoAP amplification	Moderate
V-48	Direct and spontaneous *connections* without a system view.	Moderate
V-49	802.15.4 acknowledgment messages not protected	Moderate
V-50	Strong use of wireless communications	High
Key Management		
V-51	No keying system in 802.15.4	Moderate
V-52	No key management in CoAP	Moderate
Configuration		
V-53	Insecure default settings	
Regulations		
V-54	Lack of laws and regulation	Low

Table 13 – Vulnerabilities of common IoT scenarios and specific to traffic management case

This list of vulnerabilities is the one considered in the risk anaylisy process in the next section.

6.2 Risk Assessment

Risk determination is the combination of possible security threat events with the enabling vulnerabilities and the determination of the likelihood and impact that these threat events can have on the IoT systems. Table 16 in Appendix A – Risk Identification, shows this exercise for the scenario mentioned above taking into account the defined threats and security vulnerabilities. Conservative threat source identification is used in the sense that as there are a low-risk tolerance and a considerable amount of uncertainty about risks to these types of systems, all possible threats sources are considered. Table 14 is based on Table 16 and is the resulting list of the risk analysis process, prioritized by risk level.

An analysis of the resulting risk yield that the risk with a higher score(Very high) for the traffic management scenario is the risk of obtaining IoT device credentials employing brute force attacks. This risk can result in attackers to have unauthorized access to the systems and possible leveraging other attacks like increasing their privileges. Mainly this risk is due to the fact that many IoT devices are having weak or default passwords and sometimes no access controls at all.

Among the risks with level "High" there are risks related to the disclosure of confidential information in unprotected wireless networks by means of sniffing attacks, the risks to the availability of the systems (e.g. DoS, DDoS, RF jamming), risks to physical security of IoT devices, risks related to the the lack of logging and monitoring, risks related to MiTM attacks and risk related to code vulnerabilities of IoT devices.

The "moderate" risks are related to attacks on the IoT supply chain, data integrity attacks, data exfiltration, and malware.

"Low" risks are related to reconnaissance attacks.

Threat Event	Risk	Risk level
Conduct brute force login attempts/password guessing attacks	Unauthorized access to systems Elevation of privileges	Very High
Insert untargeted malware into downloadable software and/or into commercial information technology products	Use of compromised software like firmware, operating systems, drivers, etc. Attacker obtain leverage in traffic management system allowing different types of attacks	High

Threat Event	Risk	Risk level
Obfuscate adversary actions	No view on attacks Not possible to reconstruct the attack methodology Incident response difficult More probability to APT to endure	High
Conduct wireless jamming attacks	IoT device stops communicating with decisions systems and between each other leading to potentially serious conditions in traffic management like congestion or accidents Individual sensors may be disabled or degraded by RF interference motion sensors from transmitting activity to a security officer monitoring station	High
Conduct simple Denial of Service (DoS) attack	IoT sensors and actuators became unavailable leading to safety concerns to people or lead to situations like traffic congestion Availability attacks	High
Compromise critical information systems via physical access	IoT devices can be destroyed causing malfunction in the traffic management systems IoT sensors can be manipulated to report wrong data possible causing incorrect behavior in the system causing severe damage to people's safety. Cloning of things Malicious substitution of things	High
Exploit poorly configured or unauthorized information systems exposed to the network	Accessing IoT devices Possible elevation of privilege Exploitation of vulnerabilities	High
Exploit recently discovered vulnerabilities	Attacker gain access to IoT devices allowing different levels of control like remote code execution, elevation of privilege, injection of data, etc	High
Exploit vulnerabilities on internal organizational information systems	Many risks depending on the vulnerability. Some examples are code execution, elevation of privileges, etc. In the worst-case scenario complete controls of devices and systems.	High
Conduct network traffic modification (man in the middle) attacks	Obtaining sensitive and confidential information Injection of attacker's data in the traffic management systems allowing the manipulation of system behavior. This can lead to severe causes in people's safety.	High
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Cloning of things Malicious substitution of things	Moderate

Threat Event	Risk	Risk level
Obtain sensitive information through network sniffing of external networks	Allowing the attacker to obtain confidential information	Moderate
Conduct Distributed Denial of Service (DDoS) attacks	IoT sensors and actuators became unavailable leading to safety concerns to people or lead to situations like traffic congestion Availability attacks that are more difficult to stop	Moderate
Cause deterioration/destruction of critical information system components and functions	Destruction of sensors and actuator can cause cascade effects on system	Moderate
Cause integrity loss by polluting or corrupting critical data	Integrity attack to data in the traffic management systems allowing the manipulation of behavior. This can lead to severe causes in people's safety.	Moderate
Obtain unauthorized access	Escalations of privileges	Moderate
Obtain information by opportunistically stealing or scavenging information systems/components	Obtaining confidential information from unattended devices leveraging other attacks.	Moderate
Compromise organizational information systems to facilitate exfiltration of data/information	Exfiltration of confidential information	Moderate
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware)	Supply chain attacks Possible compromise of IoT manufacturers allowing attacker to manipulate and compromise firmware, hardware, and software that gives leverage to other types of attacks.	Moderate
Exploit vulnerabilities using zero-day attacks	Attackers gain access to IoT devices with a high probability of being undetected for longer periods of time allowing different levels of control like remote code execution, elevation of privilege, injection of data, etc. IoT APTs	Moderate
Exploit insecure or incomplete data deletion at the end of life devices	Obtaining sensitive information like credentials, cryptographic keys, etc that can be used to other types of attacks like cloning of IoT devices, unauthorized access, etc	Moderate
Deliver malware by providing removable media	Infection of IoT devices with malware	Moderate
Insert targeted malware into organizational information systems and information system components	Compromised systems by means of malware. Attacker obtain leverage in traffic management system allowing different types of attacks IoT APT	Moderate
Insert specialized malware into organizational information systems based on system configurations	Compromised systems by means of malware taking advantage of a weakness in configurations. Attacker obtains leverage in traffic management system allowing different types of attacks.	Moderate

Threat Event	Risk	Risk level
Insert tampered critical components into organizational systems	Cloning of things Malicious substitution of things	Moderate
Install general-purpose sniffers on organization-controlled information systems or networks	Obtaining different types of confidential information like password, sensor information, etc	Moderate
Create counterfeit/spoof IoT device	Cloning of things, like sensors and actuators allowing attackers devices to interact with systems obtaining or providing false information	Moderate
Create and operate false front organizations to inject malicious components into the supply chain.	Use of already compromised IoT devices either in software or hardware that can be controlled by the attacker.	Moderate
Compromise organizational information systems to facilitate exfiltration of data/information	Exfiltration of personal information Privacy attacks	Low
Perform RF perimeter network reconnaissance/scanning	Attacker acquires information about RF presence and possible knowledge about technologies involved	Low
Perform network sniffing of exposed wireless networks	Attacker acquires information about the infrastructure and technology	Low
Perform malware-directed internal reconnaissance	Attacker acquires internal information not available possible not available from external methods	Low

Table 14 – Listing of risk prioritized by risk level

This prioritized list of risks is now subject to a risk treatment phase in the following section, where measures are defined with the objective to reduce the impact of the risk.

6.3 Risk response

Risk response or risk treatment is guided by the defined risk strategy. Risk response options are applied, following the risk strategy, to the identified risks resulting from the risk assessment phase. Risk response options considered are(as defined in NIST SP 800-39[49]): accept the risk, avoid the risk, mitigate the risk, share the risk, or transfer risk. Taking into consideration the criticality of a traffic management system there will only be considered two risk treatment options: risk acceptance to the “Low”level risks and risk mitigation to the other types of risks. Risk mitigation is achieved using the controls from NIST SP 800-53[8] and mitigation measures taken from the literature review done in chapter 3.

6.3.1 Risk mitigation

Risk mitigation is the prescription of security control that will reduce the impact of the risk to an acceptable level. Table 15 lists the set of security controls used to mitigate each of the risks identified in the previous section.

Threat Event	**Risk**	**Risk level**	**Controls** from NIST SP 800-53[8]
Conduct brute force login attempts/password guessing attacks	Unauthorized access to systems Elevation of privileges	Very High	AC-1 Access Control Policy and Procedures AC-2 Account Management AC-3 Access Enforcement AC-5 Separation of Duties AC-6 Least Privilege AC-7 Unsuccessful Logon Attempts
Insert untargeted malware into downloadable software and/or into commercial information technology products	Use of compromised software like firmware, operating systems, drivers, etc. Attacker obtain leverage in traffic management system allowing different types of attacks	High	AT-1 Security Awareness and Training Policy and Procedures AT-2 Security Awareness Training all MAINTENANCE CONTROLS SA-1 System and Services Acquisition Policy and Procedures SA-3 System Development Life Cycle SA-4 Acquisition Process SA-6 Software Usage Restrictions SA-9 External Information System Services SA-12 Supply Chain Protection SA-15 Development Process, Standards, and Tools SA-19 Component Authenticity SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-4 Information System Monitoring SI-7 Software, Firmware, and Information Integrity SI-16 Memory Protection
Obfuscate adversary actions	No view on attacks Not possible to reconstruct the attack methodology Incident response difficult More probability to APT to endure	High	AU-1 Audit and Accountability Policy and Procedures AU-2 Audit Events AU-6 Audit Review, Analysis, and Reporting AU-9 Protection of Audit Information

Threat Event	Risk	Risk level	Controls from NIST SP 800-53[8]
Conduct wireless jamming attacks	IoT device stops communicating with decisions systems and between each other leading to potentially serious conditions in traffic management like congestion or accidents Individual sensors may be disabled or degraded by RF interference motion sensors from transmitting activity to a security officer monitoring station	High	SC-5 Denial of Service Protection SC-6 Resource Availability all the CONTINGENCY PLANNING CONTROLS SC-40 Wireless Link Protection SC-24 Fail in Known State
Conduct simple Denial of Service (DoS) attack	IoT sensors and actuators became unavailable leading to safety concerns to people or lead to situations like traffic congestion Availability attacks	High	SC-5 Denial of Service Protection SC-6 Resource Availability all the CONTINGENCY PLANNING CONTROLS SC-24 Fail in Known State
Compromise critical information systems via physical access	IoT devices can be destroyed causing a malfunction in the traffic management systems IoT sensors can be manipulated to report wrong data possible causing incorrect behavior in the system causing severe damage to people's safety. Cloning of things Malicious substitution of things	High	all MAINTENANCE CONTROLS all MEDIA PROTECTION CONTROLS all PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS
Exploit poorly configured or unauthorized information systems exposed to the network	Accessing IoT devices Possible elevation of privilege Exploitation of vulnerabilities	High	AT-1 Security Awareness and Training Policy and Procedures AT-2 Security Awareness Training CM-8 Information System Component Inventory

Threat Event	Risk	Risk level	Controls from NIST SP 800-53[8]
Exploit recently discovered vulnerabilities	Attacker gain access to IoT devices allowing different levels of control like remote code execution, elevation of privilege, injection of data, etc	High	CA-7 Continuous Monitoring CA-8 Penetration Testing SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-4 Information System Monitoring SI-7 Software, Firmware, and Information Integrity CM-8 Information System Component Inventory
Exploit vulnerabilities on internal organizational information systems	Many risks depending on the vulnerability. Some examples are code execution, elevation of privileges, etc. In the worst-case scenario complete controls of devices and systems.	High	CA-7 Continuous Monitoring CA-8 Penetration Testing SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-4 Information System Monitoring SI-7 Software, Firmware, and Information Integrity CM-8 Information System Component Inventory
Conduct network traffic modification (man in the middle) attacks	Obtaining sensitive and confidential information Injection of attacker data in the traffic management systems allowing the manipulation of behavior. This can lead to severe causes in people's safety.	High	SC-8 Transmission Confidentiality and Integrity SC-12 Cryptographic Key Establishment and Management SC-13 Cryptographic Protection SC-17 Public Key Infrastructure Certificates SC-23 Session Authenticity SC-24 Fail in Known State

Threat Event	Risk	Risk level	Controls from NIST SP 800-53[8]
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Cloning of things Malicious substitution of things	Moderate	AT-1 Security Awareness and Training Policy and Procedures AT-2 Security Awareness Training CA-4 Security Certification CA-7 Continuous Monitoring SA-1 System and Services Acquisition Policy and Procedures SA-4 Acquisition Process SA-9 External Information System Services SA-12 Supply Chain Protection SA-19 Component Authenticity
Obtain sensitive information through network sniffing of external networks	Allowing the attacker to obtain confidential information	Moderate	SC-8 Transmission Confidentiality and Integrity SC-12 Cryptographic Key Establishment and Management SC-13 Cryptographic Protection SC-17 Public Key Infrastructure Certificates SC-40 Wireless Link Protection
Conduct Distributed Denial of Service (DDoS) attacks	IoT sensors and actuators became unavailable leading to safety concerns to people or lead to situations like traffic congestion Availability attacks that are more difficult to stop	Moderate	SC-5 Denial of Service Protection SC-6 Resource Availability all the CONTINGENCY PLANNING CONTROLS SC-24 Fail in Known State
Cause deterioration/destruction of critical information system components and functions	Destruction of sensors and actuator can cause cascade effects on system	Moderate	all MEDIA PROTECTION CONTROLS all PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

Threat Event	Risk	Risk level	Controls from NIST SP 800-53[8]
Cause integrity loss by polluting or corrupting critical data	Integrity attack to data in the traffic management systems allowing the manipulation of behavior. This can lead to severe causes in people's safety.	Moderate	all MEDIA PROTECTION CONTROLS SC-8 Transmission Confidentiality and Integrity SC-12 Cryptographic Key Establishment and Management SC-13 Cryptographic Protection SC-17 Public Key Infrastructure Certificates SC-23 Session Authenticity SC-28 Protection of Information at Rest
Obtain unauthorized access	Escalations of privileges	Moderate	AC-1 Access Control Policy and Procedures AC-2 Account Management AC-3 Access Enforcement AC-5 Separation of Duties AC-6 Least Privilege AC-7 Unsuccessful Logon Attempts AU-1 Audit and Accountability Policy and Procedures AU-2 Audit Events AU-6 Audit Review, Analysis, and Reporting AU-9 Protection of Audit Information
Obtain information by opportunistically stealing or scavenging information systems/components	Obtaining confidential information from unattended devices leveraging other attacks.	Moderate	all MAINTENANCE CONTROLS all MEDIA PROTECTION CONTROLS all PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS
Compromise organizational information systems to facilitate exfiltration of data/information	Exfiltration of confidential information	Moderate	AU-6 Audit Review, Analysis, and Reporting SC-7 Boundary Protection

Threat Event	Risk	Risk level	Controls from NIST SP 800-53[8]
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware)	Supply chain attacks Possible compromise of IoT manufacturers allowing attacker to manipulate and compromise firmware, hardware, and software that gives leverage to other types of attacks.	Moderate	SA-1 System and Services Acquisition Policy and Procedures SA-4 Acquisition Process SA-6 Software Usage Restrictions SA-9 External Information System Services SA-12 Supply Chain Protection SA-19 Component Authenticity
Exploit vulnerabilities using zero-day attacks	Attackers gain access to IoT devices with a high probability of being undetected for longer periods of time allowing different levels of control like remote code execution, elevation of privilege, injection of data, etc. IoT APTs	Moderate	CA-7 Continuous Monitoring CA-8 Penetration Testing SI-3 Malicious Code Protection SI-4 Information System Monitoring
Exploit insecure or incomplete data deletion at the end of life devices	Obtaining sensitive information like credentials, cryptographic keys, etc that can be used to another type of attacks like cloning of IoT devices, unauthorized access, etc	Moderate	all MAINTENANCE CONTROLS all MEDIA PROTECTION CONTROLS
Deliver malware by providing removable media	Infection of IoT devices with malware	Moderate	SI-3 Malicious Code Protection SI-7 Software, Firmware, and Information Integrity SC-41 Port and I/O Device Access
Insert targeted malware into organizational information systems and information system components	Compromised systems by means of malware. Attacker obtain leverage in traffic management system allowing different types of attacks IoT APT	Moderate	SI-3 Malicious Code Protection SI-7 Software, Firmware, and Information Integrity
Insert specialized malware into organizational information systems based on system configurations	Compromised systems by means of malware taking advantage of a weakness in configurations. Attacker obtains leverage in traffic management system allowing different types of attacks.	Moderate	SI-3 Malicious Code Protection SI-7 Software, Firmware, and Information Integrity CM-8 Information System Component Inventory

Threat Event	**Risk**	**Risk level**	**Controls** from NIST SP 800-53[8]
Insert tampered critical components into organizational systems	Cloning of things Malicious substitution of things	Moderate	IA-1 Identification and Authentication Policy and Procedures IA-3 Device Identification and Authentication IA-4 Identifier Management IA-5 Authenticator Management IA-7 Cryptographic Module Authentication
Install general-purpose sniffers on organization-controlled information systems or networks	Obtaining different types of confidential information like password, sensor information, etc	Moderate	CM-1 Configuration Management Policy and Procedures CM-2 Baseline Configuration CM-3 Configuration Change Control CM-5 Access Restrictions for Change
Create counterfeit/spoof IoT device	Cloning of things, like sensors and actuators allowing attackers devices to interact with systems obtaining or providing false information	Moderate	IA-1 Identification and Authentication Policy and Procedures IA-3 Device Identification and Authentication IA-4 Identifier Management IA-5 Authenticator Management IA-7 Cryptographic Module Authentication

Table 15 – Security controls to mitigate identified risks

The question now is how these security controls, used to mitigate the risks, are applicable in this IoT scenario and how IoT characteristics can hinder the applicability and efficacy of these security controls. This is the analysis done in the following section.

6.3.2 Security controls applicability to IoT

As already seen, IoT technologies have particular characteristics that can hinder the applicability of the security control defined as mitigation measures in the previous section. It is important then to analyze what are the controls that might be affected by this. The following paragraphs analyze each security control domain and type, used in the risk mitigation section, and identifies what are the possible constraints when using these controls.

Access Control

Most of the time, IoT devices lack the "awareness" of the different types of users that exist in a "normal device." Concepts like the configuration of privileges, "root" and regular user accounts and similar are not yet possible in IoT devices. Most of the times there is only one user with all the possible privileges. The applicability of wireless access control controls might also have some problems as authentication is not well supported on the network protocols yet.

Audit and Accountability

This domain of controls is strongly based on the ability of device logging. As have been seen, IoT device, due to hardware constraints or to simple fact that it is not implemented, lack most of the times logging features. Correlation might also be challenging to achieve, as there is the need for "SIEM" tools to understand the IoT specificities.

Configuration Management

The size in the number of devices and the size in the number of technologies will not allow a smooth implementation of these controls. IoT devices are very different in terms of technology, platforms and protocols. A configuration management system will need to cope will all these different and allow an integrated and consolidated view of all device configuration. Also, controls on this domain are based on the automated inventory of components using "scan probes" that might be not possible to use in IoT.

Identification and Authentication

Identification and authorization are one of the most critical aspects of the success of IoT deployments. Due to the high number and the physical dispersity of IoT devices, it is of high important be correctly identify and authenticate the devices. This is achieved usually with cryptographic tools like cryptographic keys, but the size of deployments makes it challenging to implement and to manage. Another important aspect is the need for devices to support this type of cryptographic authentication. Strong authentication (2-factor authentication) is also challenging to implement as these devices are most of the time unattended and do not have a user behind.

Physical security

Physical security controls are maybe the most difficult to implement in some scenarios. IoT devices by default are placed in physical locations that are no longer confined to the "traditional datacenter." Instead, they are located in public open areas, and it is of top most concerns to ensure the highest physical security possible,

System and Services Acquisition Policy and Procedures

The high number of devices and different platforms and stakeholders, increases the IoT supply chain making it very difficult to ensure that all these stakeholders have a firm security policy.

System and Communications Protection

The strong use of wireless communication in the IoT environments increases the need for secure communications. There are many aspects of IoT that can make this challenging to achieve. First, IoT devices are constraints in terms of resources, making the use of cryptography a problematic task. Also, the support of the network protocols for secure communication is still not perfect adding to this the key management problems related to the high number of devices, and distribution. Another aspect is the non-existence of common communication security tools like firewalls

System and Information Integrity

This is also one of the most critical domains of controls. Due to the lack of reliable, secure developing procedures, lack of economic and law incentives to build secure systems, IoT firmware and software has today a considerable amount of security vulnerabilities. To this adds the fact that there are many IoT manufacturers, many and different IoT technologies and platforms, proprietary protocols and constrained devices. All this only aggravates the situation concerning IoT security vulnerability. One of the controls to mitigate this is the timely application of security updates. Only this control has many problems in implementation. One is the fact that the updates need to be available, and has been seen this is not most of the time the case, IoT devices do not have security updates available. Second there is the need to distribute these updates in a secure manner to the enormous amount of IoT devices. Even if this is all possible it might be the case that the update cannot be applied in a timely manner, for example if the IoT devices need to "reboot." Another control that can mitigate the security issues caused by IoT vulnerabilities is the use of "malware" detection and prevention tools. In this domain we have the traditional local malware protection tools (e.g. antivirus) and the networks protection tools (e.g. IPS/IDS). Also in this case there is the need that these tools are available for the IoT case, supporting all types of technologies, platforms, protocols and handling with the fact that IoT devices are resource constraint, but also need to take into consideration that these type of systems are more "real-time" that "traditional ICT" and are very sensitive to the latencies that these tools might introduce.

Incident Response

One of the aspects of incident response is the possible isolation of the offending device in the containing phase. Most of the cases the device is placed in some type of quarantine until the recover phase is finished. Putting an IoT device in quarantine might not be always possible as these devices are used in critical and real-time situations. Also, controls in this domain are often linked with forensics aspects, that due to the high number of hardware platforms, OS, protocols might be a challenging task.

The risk identified in this assessment is specific to the IoT scenario as are the security controls defined to mitigate these risks. There are some aspects of IoT that makes the applicability of "traditional" security controls difficult. It is important in some cases to adapt these security controls to better cope with IoT characteristics and in other situations to make sure that IoT has the support to implement these controls.

6.4 Discussion

All the literature reviewed for this work is unanimous defining IoT as an unproven technology. Due to the recent mass adoption of it, IoT is still missing many of the "tools" that exist in the "traditional ICT." This is reflected in many aspects like the slow definition of standard protocols and of common architectures, the nonexistence of laws and regulations, and the nonexistence of IoT specific security information. IoT is still in an early stage of adoption, and real use cases are not that common. With the increased adoption of IoT, more elements will be available to improve the different aspects of IoT, including security.

Nevertheless, many international organizations, in the field of IT security are already working on the definition of IoT security "standardization." Most of this work is based on the current security standards and controls used in ICT and in the evaluation of the applicability to the IoT case. Conclusions and recommendations are elicit based on a gap analysis of current standards and controls when exposed to IoT threats. The conclusions of most of these works are that, existent ICT security frameworks and controls are a useful base to IoT security, but due to the IoT differences, the differences in IoT threats and to the IoT vulnerabilities, the applicability might be difficult for some controls[21] and that there might be controls, that would need to be adapted or created for IoT.

In respect to IoT security auditing, the case is different as there is no specific research work on this matter. Some of the articles reviewed for this assignment, use the audit "view "of compliance to a baseline of security controls. This is a valid approach, although not evaluating the applicability of current audit methodologies to the IoT case. Nevertheless, "generic" ICT auditing methodology is a good starting point for IoT auditing as they use, in most of the process, generic definitions and procedures.

IoT has particular characteristics that are different from "traditional ICT." For example IoT has a strong physical component with sensors and actuators interacting with the physical world and with people. Adding to this, the IoT pervasiveness, the overwhelming number of devices and all the other characteristics that make these devices more limited in the possibility of security features, there are increased motivation and reasons to develop and use IoT systems that are secure.

All the research done on IoT security is very useful, but there is the need to understand how these security concerns manifest in real IoT scenario and the level of impact that each security concern has. This is where risk management process a fundamental tool in determining the specific risk to a concrete scenario.

Not all the risks are impacting the IoT in the same way, and not all the security vulnerabilities are given the same importance. All this depends on the specific situation and it is important to understand the accurate determination of the existent risks and their criticality level in a specific scenario. One example of the difference between literature research and the real risks found in the traffic management scenario is the risks to privacy. When comparing the result for the main risk of the traffic management systems with the "general" IoT security concerns, there is a difference in respect to privacy.

Privacy attacks are a big concern in IoT. All the reviewed literature scores this as high risk. However this scenario, in particular, does not collect valuable personal information(basically uses the number of cars, the speed, the volumetry, etc) and this translated to a low risk to privacy. This shows two things. One is that not all IoT use cases will be affected by the same security concerns in a similar way and the other is showing how risk assessment is a fundamental tool for understanding the concrete risks that a specific use case has.

Concerning the IoT use case analyzed in this work, some of the conclusions are that privacy is not a big concern and that exfiltration(confidentiality) of information in these types of systems is not as critical as it is in "traditional ICT". These types of systems are more concerned with the integrity and availability of the information than with confidentiality. These systems can better "support" that an attacker knows how many cars are in the street and that traffic light X is going to change to red, than to have their data changed and unavailable(e.g. attacker being able to change the status of a traffic light or making unavailable the whole system). Physical security of IoT systems is very important.

Physical security concerns paired with the cyber-physical aspects leads critical to safety concerns. For example attacks trying to deceive IoT sensors, leading the system to misbehave (devices will need to use a fail-safe approach) or to produce wrong results (e.g., deceiving a sensor to make the system turn all traffic light to green) can be a reality. Now we do not only need to worry about social engineering but also with "sensing engineering".

Malware, as in "traditional ICT" systems, is also an important risk, although in the IoT case it might be that malware controls are still unavailable, or at least they are not as efficient as in the ICT case. One of the key aspects of the scenario assessed is that is strongly based on wireless communications using protocols that are not yet ready for mass deployment of secure communication and access controls. This increases the risks to data confidentiality via sniffing attacks and more important to integrity using MiTM techniques. Availability attacks are mainly caused by jamming the radio frequency signal or using the fact that IoT devices are most of the time constraints devices in terms of processing power and network. Vulnerabilities due to insecure developing practices are also a big concern as these vulnerabilities are multiplied by the number of different platforms that exist in the IoT ecosystem today, compared with the ICT case where vulnerabilities are more restricted to a set of 10 platforms.

Although risk assessment is a critical process to understand the concrete risks that impact a solution, it has some limitations. In the case assessed in this work, the amount of uncertainty that there is, either in terms of real threat and vulnerabilities and also to the fact that the scenario is fictitious makes this exercise less precise. In fact, there is not much knowledge of possible new threats and different vulnerabilities to these scenarios as the implementation of traffic management systems is still in the infancy. Nevertheless, this will only change when these types of systems are more common in real implementations and there will be more information about it. Until now this exercise, although with many uncertainties, is useful to assess the possible risk taking into account the information available. And also the fact that the security literature review could be more extensive, including more aspects of technical vulnerabilities. Another aspect is the fact that an analysis was done to a specific scenario of IoT – traffic management has the advantage of giving concrete insight about security in this type of system but also removes the "global view" of the security risks in the more generic IoT cases.

The applicability of "traditional" security controls in these systems is also challenging in some cases because the existent controls are not adapted to the IoT characteristics and also because some of the security features needed to implement the controls, are not support into the IoT devices. There is the need to adapt or create new controls to IoT in some cases and to implement the needed security features in IoT.

Identity management and authentication is a fundamental aspect to be able to achieve secure IoT mass deployments. One of the big problems to achieve this is the management of cryptographic keys and the support of cryptographic algorithms by constraint IoT devices. Another aspect is the update of IoT devices. In this case there are three main problems. There is the need to ensure that IoT devices have security updates available, to find a secure update mechanism and there is the need to accommodate the sensitivity of IoT devices to real time updates.

Secure communications are also a big concern of IoT. This is also related to the managements o cryptographic keys, but also to the support of the underlaying protocols. Controls and support by IoT devices related to logging, monitoring and auditing should also be supported and adapted to IoT case.

Physical security needs to be "re designed" as IoT devices are not confined to a controled physical location, but are exposed to public areas.

7 Conclusion

IoT systems have much in common with traditional ICT systems but also have many differences. The current state of IoT security is still incipient, and it is urgent to look at it as a separated domain of research, however always "importing" all the good security practices and the knowledge that for years have served with good results ICT systems. In this work, a brief introduction of IoT was given where aspects like IoT definition, IoT architectures and IoT protocols where reviewed.

Following this first introducing a review of the state of the art in IoT security was done, where the main security concerns of IoT security were reviewed either in terms of general security concerns or in more technical details and vulnerabilities. This initial review set the grounds concerning IoT security to a second phase of the work, where a concrete IoT security assessment problem was analyzed at the light of the information collected in the first phase.

In this second part of the work, a fictitious scenario of a traffic management solution was defined, stating the IoT technologies used. This scenario was after the object used to apply a risk assessment methodology from NIST with the objective to find out the main security risks that these type of solutions face. This risk analysis took only into consideration the security vulnerabilities and concerns found in the first part of this work. These security risks were then managed using a risk treatment approach also from NIST.

The risk treatment involved the used of "ICT" security controls from NIST SP 800-53[8] and from the research done in the first part of this work. Finally the applicability of these controls was analyzed taking into consideration the specific IoT characteristics, also from the first phase of the work, and how they can hinder the applicability of "ICT security controls"

The sources used for the IoT security review target mainly the "main security organizations" in the current international panorama, like NIST, ENISA, CISCO, OWASP, CIS, and some IEEE research. This was not by far a complete review of all the work related to IoT security, as mainly time constraints not allowed to have a more complete security review at all levels (e.g. more high-level security problems, more technical security problems). The fact that IoT is a "vast" and heterogenous environment, with many technologies and protocols also contributes to this fact. So the focus was to obtain a good overview of the main IoT security concerns and some technical problems related for example to protocols.

This is one of the points where this work could be improved. A better understanding of the concrete security problems at "lower levels" like in the many protocols that IoT is built on. Another point that "weaken" this work was the fact that the scenario used was fictitious, making the analysis less realistic and an improvement would be to apply this analysis to a real traffic management scenario(or any other IoT scenario).

References

[1] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," *IEEE Softw.*, vol. 33, no. 1, pp. 112–116, 2016.

[2] G.-M. O., "State-of-the-Art and Challenges for the Internet of Things Security draft-irtf-t2trg-iot-seccons-16," 2018.

[3] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[4] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, 2018.

[5] Statista.com, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)." [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[6] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The Effect of IoT New Features on Security and Privacy : New Threats , Existing Solutions , and Challenges Yet to Be Solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, 2019.

[7] NIST, "Guide for Conducting Risk Assessments SP800-30rev1," *NIST Spec. Publ. 800-30 Revis. 1*, no. September, p. 95, 2012.

[8] J. Task Force Transformation Initiative, "NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations JOINT TASK FORCE TRANSFORMATION INITIATIVE," *NIST Spec. Publ.*, vol. 800–53, no. 4, 2015.

[9] ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, no. November. 2017.

[10] ENISA, "ENISA webpage on IoT." [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot.

[11] (EU), "SWD(2016) 110 final IOT Advancing the Internet of Things in Europe," pp. 5–38, 2016.

[12] IERC, "IERC IoT Web page." [Online]. Available: http://www.internet-of-things-research.eu/about_iot.htm.

[13] ISO/IEC, "ISO/IEC 20924:2018 - Internet of Things (IoT) -- Vocabulary (preview)," *ISO/IEC 20924:2018*, 2018. [Online]. Available: https://www.iso.org/standard/69470.html.

[14] K. Boeckl *et al.*, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (Draft NISTIR 8288)," 2018.

[15] Cisco, "The Internet of Things Reference Model," *Internet of Things World Forum*, pp. 1–12, 2014.

[16] ISO, "Study Report on IoT Reference Architectures / Frameworks," no. August, pp. 1–76, 2014.

[17] IEEE, "IEEE P2413." [Online]. Available: http://grouper.ieee.org/groups/2413/.

[18] IEEE P2413, “Standard for an Architectural Framework for the Internet of Things (IoT) IEEE P2413,” *Ieee*, no. April, pp. 1–12, 2016.

[19] F. Carrez *et al.*, “Internet of Things – Architecture IoT - A Final architectural reference model for the IoT v3,” 2013.

[20] I. R. Waz, M. A. Sobh, and A. M. Bahaa-Eldin, “Internet of Things (IoT) security platforms,” *Proc. ICCES 2017 12th Int. Conf. Comput. Eng. Syst.*, vol. 2018-Janua, pp. 500–507, 2018.

[21] IEEE, “IEEE 802.15 WPAN™ Task Group.” [Online]. Available: http://www.ieee802.org/15/pub/TG4md.html.

[22] T. Winter *et al.*, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550,” *Internet Eng. Task Force RFC 6550*, pp. 1–157, 2012.

[23] Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol (CoAP),” Jun. 2014.

[24] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, “IoT security: Ongoing challenges and research opportunities,” *Proc. - IEEE 7th Int. Conf. Serv. Comput. Appl. SOCA 2014*, pp. 230–234, 2014.

[25] B. Russell *et al.*, “Security Guidance for Early Adopters of the Internet of Things (IoT),” *Mob. Work. Gr. Peer Rev. Doc.*, no. April, pp. 1–54, 2015.

[26] M. Hogan and B. Piccarreta, “Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT),” *NIST Interaganecy Rep. 8200*, pp. 1–185, 2018.

[27] Wikipedia, “Mirai (malware).” [Online]. Available: https://en.wikipedia.org/wiki/Mirai_(malware). [Accessed: 08-Jul-2019].

[28] “ISO/IEC WD 27030.” [Online]. Available: https://www.iso.org/standard/44373.html.

[29] C. for I. Security, “Internet of Things Security Companion to the CIS Critical Security Controls (Version 6),” no. October, pp. 1–21, 2015.

[30] OWASP, “Internet of Things Top Ten,” p. 12, 2011.

[31] OWASP, “OWASP Internet of Things Project.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main.

[32] OWASP, “Top 10-2017 Top 10 - OWASP,” 2017. [Online]. Available: https://www.owasp.org/index.php/Top_10-2017_Top_10. [Accessed: 06-Jun-2019].

[33] G. Montenegro, “RFC 4944 - Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” vol. 52, no. 15, pp. 1–30, 2007.

[34] J. Hui and A. R. Corporation, “RFC 6282 - Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,” pp. 1–24, 2011.

[35] R.S. Ross, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” *NIST Spec. Publ.*, no. August 2009, pp. 1–487, 2014.

[36] M. M. Weiss, *Auditing IT Infrastructures for Compliance, 2nd Edition*. 2015.

[37] Redalertlabs.com, “IoT Security and Common Criteria Framework.” [Online]. Available: https://www.redalertlabs.com/blog/iot-security-and-common-criteria-framework.

[38] E. Logic, “X-Ware IoT Platform SC Security Target,” 2018. [Online]. Available:

https://www.commoncriteriaportal.org/files/epfiles/[ST] X-Ware IoT Platform SC Security Target V2.0.pdf.

[39] ISACA, "IS Audit Basics: Auditing the IoT." [Online]. Available: https://www.isaca.org/Journal/archives/2018/Volume-5/Pages/auditing-the-iot.aspx.

[40] M. Jekot and Y. Pavlosoglou, "An IoT Control Audit Methodology," vol. 6, pp. 1–12, 2017.

[41] Senate Bill, "SB-327 Information privacy: connected devices." [Online]. Available: http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[42] B. Schneier, "New IoT Security Regulations." [Online]. Available: https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html.

[43] "Consultation on the Government ′ s regulatory proposals regarding consumer Internet of Things (IoT) security Consultation on the Government ′ s regulatory proposals regarding consumer Internet of Things security .," no. May, pp. 1–18, 2019.

[44] A. Gaur, B. Scotney, G. Parr, and S. McClean, "Smart city architecture and its applications based on IoT," *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 1089–1094, 2015.

[45] M. Vitunskaite, Y. He, T. Brandstetter, and H. Janicke, "Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership," *Comput. Secur.*, vol. 83, pp. 313–331, 2019.

[46] P. Masek *et al.*, "A Harmonized Perspective on Transportation Management in Smart Cities : The Novel IoT-Driven Environment for Road Traffic Modeling," no. i.

[47] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "Technical guide to information security testing and assessment.," 2008.

[48] B. Schneier, "Attack Trees," *Dr. Dobb's Journal*, 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html. [Accessed: 27-Jul-2019].

[49] National Institute of Standards and Technology, "Managing Information Security Risk, NIST SP 800-39," *NIST Spec. Publ. 800-39*, no. March, p. 88, 2011.

Appendices

Appendix A – Risk Identification

Table 16 list all the identified risk and corresponding level of the risk

Perform reconnaissance and gather information												
		Threat Source Characteristics[i]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Perform RF perimeter network reconnaissance/scanning	All	Very High	Very High	Very High	Predicted	Very High	Sensors and actuators in public locations large attack surface Strong use of wireless communications	Very High	Very High	Low	Attacker acquires information about RF presence and possible knowledge about technologies involved	Low
Perform network sniffing of exposed wireless networks	All	Very High	Very High	Very High	Predicted	Very High	Sensors and actuators in public locations large attack surface Strong use of wireless communications	High	Very High	Low	Attacker acquires information about the infrastructure and technology	Low

Perform reconnaissance and gather information												
		Threat Source Characteristics[i]										
Threat Event	Threat Sources	Capability	Intent	Targeting	Relevance	Likelihood of Attack Initiation	Vulnerabilities	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk	Risk level
Perform malware-directed internal reconnaissance	Individual – Insider Group - Established Organization - Competitor Organization - Supplier Organization - Partner Organization - Customer Nation-State	Very High	Very High	Very High	Predicted	Moderate	Lack of malware protection Lacks mature standards, guidance, processes for logging and audit	Moderate	Moderate	Low	Attacker acquires internal information not available possible not available from external methods	Low

Craft or create attack tools											
		Threat Source Characteristics[ii]									
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Create counterfeit/spoof IoT device	All	Very High	Very High	Very High	Predicted	High	Sensors and actuators in public locations Lacks mature standards, guidance, processes for authentication and authorization No keying system in 802.15.4 No key management in CoAP	Moderate	Moderate	High	Cloning of things, like sensors and actuators allowing attackers devices to interact with systems obtaining or providing false information	Moderate
Create and operate false front organizations to inject malicious components into the supply chain.	Group - Established Organization - Competitor Organization - Supplier Organization - Partner Nation-State	Very High	Very High	Very High	Predicted	Moderate	Long supply chain Lack of security awareness	Low	Low	Very High	Use of already compromised IoT devices either in software or hardware that can be controlled by the attacker.	Moderate

Deliver/insert/install malicious capabilities												
		Threat Source Characteristics[iii]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Deliver malware by providing removable media	All	Very High	Very High	Very High	Predicted	High	Unsecure physical ports (e.g., USB) Lack of security awareness Lacks mature standards, guidance, processes for logging and audit Lack of malware protection	Low	Moderate	High	Infection of IoT devices with malware	Moderate
Insert untargeted malware into downloadable software and/or into commercial information technology products	Group – Established Organization – Competitor Nation-State	Very High	Very High	Very High	Predicted	High	"Long" supply chain Lack of security awareness Lack of malware protection Lack of common operating system security measures (e,g. process isolation, memory management) Proprietary protocols	High	High	High	Use of compromised software like firmware, operating systems, drivers, etc. Attacker obtain leverage in traffic management system allowing different types of attacks	High
Insert targeted malware into organizational information systems and information system components	Group – Established Organization – Competitor Nation-State	Very High	Very High	Very High	Predicted	High	Lack of malware protection Lack of common operating system security measures (e,g. process isolation, memory management) Proprietary protocols	Moderate	Moderate	High	Compromised systems by means of malware. Attacker obtain leverage in traffic management system allowing different types of attacks IoT APT	Moderate

Deliver/insert/install malicious capabilities												
		Threat Source Characteristics[iii]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Insert specialized malware into organizational information systems based on system configurations	Group – Established Organization – Competitor Nation-State	Very High	Very High	Very High	Predicted	Moderate	Lack of device management Lacks mature guidance and processes for management and maintenance of the device Lack of malware protection Insecure default settings	Moderate	Moderate	High	Compromised systems by means of malware taking advantage of a weakness in configurations. Attacker obtains leverage in traffic management system allowing different types of attacks.	Moderate
Insert tampered critical components into organizational systems	Individual - Insider Group - Established Organization - Competitor Organization - Supplier Organization - Partner Nation-State	Very High	Very High	Very High	Predicted	High	Lack of physical security Sensors and actuators in public locations Large attack surface "Long" supply chain	Moderate	Moderate	High	Cloning of things Malicious substitution of things	Moderate

Deliver/insert/install malicious capabilities												
		Threat Source Characteristics[iii]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Install general-purpose sniffers on organization-controlled information systems or networks	Individual - Insider Group - Established Organization - Competitor Organization - Supplier Organization - Partner Nation-State	Very High	Very High	Very High	Predicted	Moderate	Lacks mature standards, guidance, processes for logging and audit Lack of logging features in IoT devices Devices lack of access controls Lacks mature standards, guidance, processes for authentication and authorization Hardcoded Passwords Weak and Guessable password Lack of device management Lacks mature guidance and processes for management and maintenance of the device	Moderate	Moderate	High	Obtaining different types of confidential information like password, sensor information, etc	Moderate

Exploit and compromise												
		Threat Source Characteristics[iv]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Exploit poorly configured or unauthorized information systems exposed to the network	All	Very High	Very High	Very High	Predicted	Very High	Insecure default settings Insecure network services Lack of security awareness Proprietary protocols Lack of device management Lacks mature standards, guidance, processes for logging and audit Lack of logging features in IoT devices	High	Very High	High	Accessing IoT devices Possible elevation of privilege Exploitation of vulnerabilities	High

Exploit and compromise												
		Threat Source Characteristics[iv]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Exploit recently discovered vulnerabilities	All	Very High	Very High	Very High	Predicted	High	Lack of malware protection Patching not available Lack of secure update mechanism Patching not always possible Lacks mature guidance and processes for management and maintenance of the device Lack of network security measures (e.g., host fw, DLP) Lacks mature standards, guidance, processes for logging and audit Lack of logging features in IoT devices Vulnerable Software/Code Software development insecure Re-purposing and combinations of existing IoT systems	High	High	High	Attacker gain access to IoT devices allowing different levels of control like remote code execution, elevation of privilege, injection of data, etc	High

Exploit and compromise												
		Threat Source Characteristics[iv]										
Threat Event	Threat Sources	Capability	Intent	Targeting	Relevance	Likelihood of Attack Initiation	Vulnerabilities	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk	Risk level
Exploit vulnerabilities on internal organizational information systems	Individual – Outsider Group – Established Organization - Competitor Organization – Supplier Organization – Partner Nation-State	Very High	Very High	Very High	Predicted	Very High	Vulnerable Software/Code Software development insecure Re-purposing and combinations of existing IoT systems Lacks mature guidance and processes for IoT development Use of Insecure or Outdated Components Proprietary protocols Lack of security awareness Lack of device management Patching not available Lack of secure update mechanism Patching not always possible Lacks mature guidance and processes for management and maintenance of the device	High	Very High	High	Many risks depending on the vulnerability. Some examples are code execution, elevation of privileges, etc. In the worst-case scenario complete controls of devices and systems.	High

Exploit and compromise												
		Threat Source Characteristics[iv]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Exploit vulnerabilities using zero-day attacks	Group – Established Organization – Competitor Nation-State	Very High	Very High	Very High	Predicted	Moderate	Vulnerable Software/Code Software development insecure Lacks mature guidance and processes for IoT development Use of Insecure or Outdated Components Lacks mature standards, guidance, processes for logging and audit Proprietary protocols	Moderate	Moderate	High	Attackers gain access to IoT devices with a high probability of being undetected for a longer period of time allowing different levels of control like remote code execution, elevation of privilege, injection of data, etc. IoT APTs	Moderate
Exploit insecure or incomplete data deletion at the end of life devices	All	Very High	Very High	Very High	Predicted	High	Lack of security awareness Lack of device management Lacks mature guidance and processes for management and maintenance of the device Insecure Data Storage in devices Lack of physical hardening (e.g., secure storage of crypto material)	Moderate	Moderate	High	Obtaining sensitive information like credentials, cryptographic keys, etc that can be used to other types of attacks like cloning of IoT devices, unauthorized access, etc	Moderate

Conduct an attack (i.e., direct/coordinate attack tools or activities)												
		Threat Source Characteristics[v]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Compromise critical information systems via physical access	all	Very High	Very High	Very High	Predicted	Very High	Lack of physical security Sensors and actuators in public locations Lack of physical hardening (e.g., secure storage of crypto material) Unsecure physical ports (e.g., USB) Insecure Data Storage in devices	High	High	High	IoT devices can be destroyed causing a malfunction in the traffic management systems IoT sensors can be manipulated to report wrong data possible causing incorrect behavior in the system causing severe damage to people's safety. Cloning of things Malicious substitution of things	High
Compromise organizational information systems to facilitate exfiltration of data/information		Very High	Very High	Very High	Predicted	High	Insufficient Privacy Protection Access to large amounts and types of personal data	Moderate	Moderate	Low	Exfiltration of personal information Privacy attacks	Low
							Lack of network security measures (e.g., host fw, DLP)	Moderate	Moderate	High	Exfiltration of confidential information	Moderate

Conduct an attack (i.e., direct/coordinate attack tools or activities)												
		Threat Source Characteristics[v]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware)	Group – Established Nation-State	Very High	Very High	Very High	Predicted	High	Lack of security awareness "Long" supply chain	Moderate	Moderate	High	Supply chain attacks Possible compromise of IoT manufacturers allowing attacker to manipulate and compromise firmware, hardware and software that gives leverage to other types of attacks.	Moderate

Achieve results (i.e., cause adverse impacts, obtain information)												
		Threat Source Characteristics[vi]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Conduct wireless jamming attacks	all	Very High	Very High	Very High	Predicted	Very High	Sensors and actuators in public locations Strong use of wireless communications	High	Very High	High	IoT device stops communicating with decisions systems and between each other leading to potentially serious conditions in traffic management like congestion or accidents Individual sensors may be disabled or degraded by RF interference motion sensors from transmitting activity to a security officer monitoring station	High
Conduct simple Denial of Service (DoS) attack	all	Very High	Very High	Very High	Predicted	High	Sensors and actuators in public locations Strong use of wireless communications Network constraints Power constrained Cpu constrained	High	High	High	IoT sensors and actuators became unavailable leading to safety concerns to people or lead to situations like traffic congestion Availability attacks	High

Achieve results (i.e., cause adverse impacts, obtain information)												
		Threat Source Characteristics[vi]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Conduct Distributed Denial of Service (DDoS) attacks	Group – Established Organization – Competitor Nation-State	Very High	Very High	Very High	Predicted	High	Sensors and actuators in public locations Strong use of wireless communications Network constraints Power constrained Cpu constrained	Moderate	Moderate	High	IoT sensors and actuators became unavailable leading to safety concerns to people or lead to situations like traffic congestion Availability attacks that are more difficult to stop	Moderate
Conduct brute force login attempts/password guessing attacks	All	Very High	Very High	Very High	Predicted	Very High	Devices lack of access controls Lacks mature standards, guidance, processes for authentication and authorization Hardcoded Passwords Weak and Guessable password	High	Very High	Very High	Unauthorized access to systems Elevation of privileges	Very High

Achieve results (i.e., cause adverse impacts, obtain information)												
		Threat Source Characteristics[vi]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Conduct network traffic modification (man in the middle) attacks	Individual – Outsider Individual - Insider Group - Ad hoc Group - Established Organization - Competitor Organization - Partner Organization - Customer Nation-State	Very High	Very High	Very High	Predicted	High	Insecure network services Insecure data transfer Insecure ecosystem interfaces Sensors and actuators in public locations Strong use of wireless communications	High	High	High	Obtaining sensitive and confidential information Injection of attacker data in the traffic management systems allowing the manipulation of behavior. This can lead to severe causes in people's safety.	High
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Group - Established Organization - Competitor Organization - Supplier Organization – Partner Nation-State	Very High	Very High	Very High	Predicted	Moderate	"Long" supply chain Lack of security awareness	Moderate	Moderate	High	Cloning of things Malicious substitution of things	Moderate

Maintain a presence or set of capabilities													
		Threat Source Characteristics[vii]											
Threat Event	Threat Sources	Capability	Intent	Targeting	Relevance	Likelihood of Attack Initiation	Vulnerabilities	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk	Risk level
Obtain sensitive information through network sniffing of external networks	All	Very High	Very High	Very High	Predicted	Very High	Insecure network services Insecure data transfer Insecure ecosystem interfaces Sensors and actuators in public locations	Very High	Very High	Moderate	Allowing attacker to obtain confidential information	Moderate
Cause deterioration/destruction of critical information system components and functions	all	Very High	Very High	Very High	Predicted	High	Lack of physical security Sensors and actuators in public locations Lack of physical hardening (e.g., secure storage of crypto material)	High	High	Moderate	Destruction of sensors and actuator can cause cascade effects on system	Moderate
Cause integrity loss by polluting or corrupting critical data	all	Very High	Very High	Very High	Predicted	High	Lack of physical security Sensors and actuators in public locations Insecure network services Insecure data transfer Insecure ecosystem interfaces	Moderate	Moderate	High	Integrity attack to data in the traffic management systems allowing the manipulation of behavior. This can lead to severe causes in people's safety.	Moderate

Maintain a presence or set of capabilities												
		Threat Source Characteristics[vii]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Obtain unauthorized access	Individual – Insider Organization - Supplier Organization - Partner	Moderate	High	High	Predicted	Low	Devices lack of access controls Lacks mature standards, guidance, processes for authentication and authorization Hardcoded Passwords Weak and Guessable password Lacks mature standards, guidance, processes for logging and audit Lack of logging features in IoT devices	High	Moderate	High	Escalations of privileges	Moderate
Obtain information by opportunistically stealing or scavenging information systems/components	All	Very High	Very High	Very High	Predicted	High	Lack of physical security Insecure Data Storage in devices	Moderate	Moderate	High	Obtaining confidential information from unattended devices leveraging other attacks.	Moderate

Coordinate a campaign												
		Threat Source Characteristics[viii]										
Threat Event	**Threat Sources**	**Capability**	**Intent**	**Targeting**	**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk level**
Obfuscate adversary actions	Individual - Insider Group - Established Organization - Competitor Nation-State	Very High	Very High	Very High	Predicted	High	Lacks mature standards, guidance, processes for logging and audit Lack of logging features in IoT devices Lack of device management Lacks mature guidance and processes for management and maintenance of the device	High	High	High	No view on attacks Not possible to reconstruct the attack methodology Incident response difficult More probability to APT to endure	High

Table 16 – Adversarial risk determination

[i] Combination of the highest values from all considered threat sources in each row

[ii] Combination of the highest values from all considered threat sources in each row

[iii] Combination of the highest values from all considered threat sources in each row

[iv] Combination of the highest values from all considered threat sources in each row

[v] Combination of the highest values from all considered threat sources in each row

[vi] Combination of the highest values from all considered threat sources in each row

[vii] Combination of the highest values from all considered threat sources in each row

[viii] Combination of the highest values from all considered threat sources in each row