Internet of Things: Privacy and Security Implications

Roberto Ferreira

Lusofona University of Porto, Portugal
rober@live.com.pt

Abstract. The Internet of Things or IoT has become one of the major concerns relative to security. IoT has a big impact on our lives. Certain aspects need to be reviewed in order to understand their features and their flaws. And knowing their weaknesses, we can prepare and develop better solutions that allow us to use these devices in a safe and responsible way. This paper gives an overview of what is Internet of Things and implications in security and privacy of the IoT which will be divided in Attacks and Threats, Security and Privacy in IoT and a Demonstration of Security breach in a CCTV System.

Keywords: Internet of Things, IoT, Security, Privacy.

1 Introduction

Internet of Things is becoming an increasingly growing topic. We can find IoT devices pretty much everywhere like home appliances, home energy management, home security and safety, health and fitness, information and entertainment. IoT devices like refrigerators, coffee machines, thermostats, smart bands, smart watches, intelligent ovens, smart bulbs etc. It has attracted strong interest from both academia and industry. But what is IoT after all? IoT are all devices that are capable to identify and communicate data between each other. These devices can collect a vast amount of information about the environment and how they are used, with or without the active involvement of the human being [1].

IoT is a network of physical objects. The Internet is not only a network of computers, but it has evolved into a network of devices of all type and sizes, vehicles, smart phones, homes appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, all connected, all communicating and sharing information based on stipulated protocols in order to achieve smart reorganizations, positioning, tracing, safety, control and even personal real time online monitoring, upgrade, control and administration [2].

Enterprises and government agencies are embracing a digital transformation that is reinventing business models to better serve customers and drive new growth. The rapid adoption of new technologies and innovations is driving a global rethinking of traditional business processes and creating new ways to generate better business outcomes and quality-of-life improvements. Over a million new IoT devices are connected to the internet dally and that process is accelerating. Experts predict that between 25 and 50 billion new IP-enabled IoT devices will be deployed and online by 2020.

This is being called the Fourth Industrial Revolution-a period of explosive productivity improvements driven by innovation and the combination of technologies that unlock new business models [3].

This rapid innovation and adoption of this Internet of Things devices bring privacy and security challenges. Along in this paper we will get to know more IoT security and privacy problems and try to solve them.

2 Attacks and Threats

Internet of things devices are rapidly becoming ubiquitous while IoT services are becoming pervasive. Their success has not gone unnoticed and the number of threats and attacks against IoT devices and services are on the increase as well. Cyber-attacks are not new to IoT, but as IoT will be deeply interwoven in our lives and societies, it is becoming necessary to step up and take cyber defense seriously. With the necessity of secure IoT has resulted in a need to comprehensively understand the threats and attacks on IoT infrastructure [4].

According to [5], in the future, maybe the year 2020 with IPv6 and 5G network, millions of heterogeneous things will be the major factor of concern at that time. The IoT can be viewed in different dimensions by the different sections of academia and industry. Whatever the viewpoint, the IoT has no yet reached maturity and is vulnerable to all sort of threats and attacks.

Security issues are divided in three dimensions, based on phase, architecture and components. The IoT devices requires five phases, from data collection to data delivery to the end users.

Phase 1, Data collection, acquisition or perception, foremost step is to collect or acquire data from devices or things. Based on the characteristic of the thing, different types of data collectors are used. Thing may be static body (body sensors or RFID tags) or dynamic vehicle (sensors and chips).

Phase 2, Storage, the data collected in phase 1 should be stored. If the thing has its own local memory, data can be stored. Generally, IoT components are installed with low memory and low processing capabilities. The cloud takes over the responsibility for storing the data in the case of stateless devices.

Phase 3, Intelligent processing, the IoT analyzes the data stored in the Cloud Data Centers and provides intelligent services for work and life in hard real time. As well as analyzing and responding to queries, the IoT also controls things. There is no discrimination between a boot and a bot, the IoT offers intelligent processing and control services to all things equally.

Examples of such IoT systems are pervasive healthcare, advanced building management systems, smart city services, public surveillance and data acquisition, or participatory sensing application [8].

Phase 4, Data Transmission, the data transmission occurs in all phases, from sensors, RFID tags or chips to Data Centers, from Data Centers to processing units and from processors to controllers, devices or end users.

Phase 5, Delivery, delivers the processed data to things on time without errors or alteration, is a sensitive task that must always be carried out.

In all five phases occurs a variety of attacks. Data leakage, sovereignty, breach and authentication are the major concerns in the data perception phase. The image demonstrates the variety of attacks in every single phase.

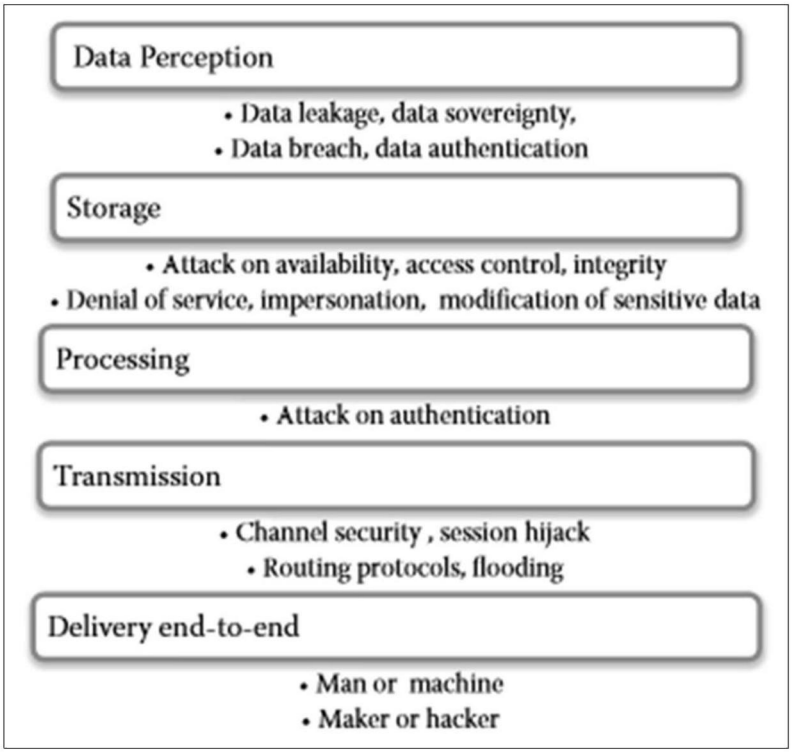

Fig.1. Attacks based on Phase

Relative to the architecture, the IoT has not yet been confined to a specific one. Different vendors and applications adopt their own layers. The attacks based on architecture, its assumed to have four layers. Sensing/Perception layer where External Attack, which attack, or worm hole and sewage pool are the most common to happen. The next layer, Network layer are routing protocol and address compromise. In the Transport Layer are Denial of Service and Man-in-the-Middle. And finally, the Application layer, which are more common attacks like, revealing sensitive data, data destruction, user authentication or intellectual property.

According to [6], the most common cyber attacks in IoT are Man-in-the-Middle, Data & Identity Theft and Denial of Service, between others.

The Man-in-the-Middle concept is where an attacker or hacker is looking to interrupt and breach communications between two separate systems. It can be a dangerous attack, because it is one where the attackers secretly intercept and transmits messages between two parties when they are under the belief that they are communicating directly with each other. As the attacker has the original message, they can trick the recipient into thinking they are still getting a legitimate message. Many cases have already been reported within this threat area, cases of hacked vehicles and hacked “smart refrigerators”.

In Data & Identity theft, careless safekeeping of Internet connected devices like, mobile phones, iPad´s, smartwatch´s are playing into the hands of malicious thieves and opportunistic finders. The more details that can be found about a user, by the IoT devices, the easier and the more sophisticated a target attack aimed at identity theft can be.

Denial of Service (DoS) attack happens when a service that would usually work is now unavailable. There can be many reasons for unavailability, but it usually refers to an infrastructure that cannot cope due to capacity overload. In DDoS, Distributed Denial of Service attacks, many systems attack one target. This often done through a botnet, where many devices are programmed (often unbeknownst to the owner) to request a service at the same time to a system.

The attacks based on components, by [5], the IoT connects “everything” through the internet. These things are heterogenous in nature communicating sensitive data over a distance. Apart from attenuation, theft, loss, breach and disaster, data can also be fabricated and modified by compromised sensors. Verification of the end user at the entry level is mandatory, distinguishing between humans and machines is extremely important.

3 Security and Privacy Preservation in IoT

For the use of the IoT to be safe and private, there must be a series of concepts that must be understood.

The Internet of Things is the interconnection of billions of smart things around us, with the ability to collect, store, process and communicate information about themselves and their physical environment. IoT systems will deliver advanced services of a whole new kind base on an increasingly fine-grained data acquisition in an environment densely populated with smart things. Privacy is a very broad and diverse notion for which literature offers many definitions and perspectives. From a historic view, the notion of privacy shifted between media, territorial, communication and bodily privacy to an increasing use and efficiency of electronic data processing information, privacy has become the predominant issue today. So according to [8], the definition of privacy of IoT is the guarantee of:

- Awareness of privacy risks imposed by smart things and services surrounding the data subject
- Individual control over the collection and processing of personal information by the surrounding smart things
- Awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subjects personal control sphere

About security, based on the security issues discussed before there are necessary countermeasures so that authenticity, confidentiality, integrality, privacy and availability be

preserved. According to [7], some of the countermeasures are certification, access control, data encryption and security in cloud computing.

Relative to certification, it's a secure way of confirming the identity of both parties which communicate with each other. This can be achieved by using a Public Key Infrastructure or through a third party like a certificate authority that facilitates interactions between the users to assure the properties of data exchange [7].

Access Control is another mechanism which gives secure environment of IoT by limiting the access control for machines, objects or people which are illegal to access the resources. Access control can be implemented by using encrypted passwords, confidential directories or files, configurating and update rights etc.

Nowadays, there is a myriad of access control models that are applied to different Internet of Things scenarios in which security is required. The most popular models are Mandatory Access Control (MAC), Discretionary Access Control (DAC), RoleBased Access Control (RBAC) which are traditional access control models that do not consider additional parameters such as resources information and dynamic information (such as time, location). In order to provide a more flexible mechanism, the Attribute-Based Access (ABAC) was proposed, in which authorization decisions are based on attributes that the users must prove (eg: age, location, roles, etc.). One of the main advantages of ABAC is requests do not have to be known a priori by targets, providing a higher level of flexibility for open environments, compared to RBAC models. Nevertheless, in ABAC everyone must agree on a set of attributes and their meaning when using ABAC, which is not easy to accomplish. IoT scenarios imposes significant restrictions on privacy and access control, tradition access control approaches solution was not designed with these aspects [10].

Insufficient Authentication/Authorization regards to access control, can result in a data loss or corruption, lack of accountability or denial of access and can lead to a complete compromise of the device and/or user accounts. Attackers uses weak passwords, insecure password recovery mechanisms, poorly protected credential or lack of granular access control to access to an interface. Attack could come from Internal or external users. So, to make it secure according to [9]:

- Ensuring that the strong passwords are required
- Ensuring granular access control is in place when necessary
- Ensuring credential are properly protected
- Implement two factor authentications where possible
- Ensuring that password recovery mechanisms are secure
- Ensuring re-authorization is required for sensitive features
- Ensuring options are available for configuration password controls

Data Encryption technique is used to maintain confidentiality as well as integrity of the information. This way data that is intercepted by an attacker, encryption prevents that data from being deciphered [7].

According to [11], current cryptographic models and security schemes are based on widely adopted encryption algorithms, and privacy standards. Confidentiality is ensured in most of the cases with Advanced Encryption Standard (AES). The asymmetric algorithm RSA serves for asymmetric algorithm encryption, digital signatures, as well as for key management. SHA standards are used as secure hash functions. Alternatively, Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC) supplement the privacy schemes, basically in asymmetric cryptography. The applied suites have been designed for general purpose uses and their functionality is based on significant processing power, good memory resources and power availability. Since the applicability of these cryptographic models and security schemes is a bit unclear, detailed analysis is needed, in order to be ensured, that they can be implemented in the specified resources of IoT. Especially in the case, of minimizes capabilities of hand-held and portable devices [11].

Lack of encryption can result in data loss and depending on the data exposed, could lead to a complete compromise of the device or user accounts. There for according to [9], enough encryption requires:

- Ensuring data is encrypted using protocol such SSL and TLS while transiting networks
- Ensuring other industry standard encryption techniques are utilized to protected data during transport
- Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols

Relative to Cloud Computing, cloud is just a name for a huge data storage capacity with high performance and affordable low cost. In the essential, working with IoT large number of sensors nodes collects and analyses huge amount of data, storing and processing of data where cloud computing can be used very effectively. So, cloud computing security is very important to prevent attacks to that data [7]. So, according to [9], An insecure cloud interface could lead to compromise of user data and control over the device, enough cloud computing security requires:

- Default passwords and ideally default usernames to be changed during initial setup
- Ensuring user accounts cannot be enumerated using functionality such as password reset mechanisms
- Ensuring account lockout after 3-5 failed login attempts
- Ensuring the cloud-based web interface is not susceptible to XSS, SQLi or CSRF
- Ensuring credentials are not exposed over the internet

- Implement two factor authentications if possible

4 Demonstration of Security breach in a CCTV System

Security cameras are meant to monitor homes, public spaces, stores among other locations, however their main purpose is to monitor robberies or any suspicious behavior. The goal of security cameras is to protect those who use them and not the contrary. So, I tried to test the security of these CCTV systems, for academic reasons, that are connected to the internet and I did have access to a few. The one´s that I had access to, simply had default usernames and passwords, like username=admin and password=12345, like the Fig.2.

Fig.2. Login online to a CCTV system

But those that did not have the default credentials, it is possible to enter multiple times different combinations of users and passwords that can be obtained throw lists of millions of different records online. That is, I automatically can test various combinations of usernames and passwords until eventually find the correct one and get access to the CCTV system like Fig.3, through brute force cracking tools like Hydra. In this case it was easy to access to the CCTV system, because the user didn't change the default username and password. And this is more common than we think, especially in IoT devices that have weak security features. A solution to this situation would be the manufactors of the CCTV systems to force the users to change at least the password to a different and stronger one and have a maximum of login try's, like 6, until the device block and notice the user. Some companies have already done this in their devices, but others don't. Once I have access to de CCTV system, I can see what the cameras can see. But I'm not suppose to. The same camera system that is supposed to protect the user property, is a privacy and possible security breach. I can monitor when the owner arrives at the property and when he leaves, comprehending is routine and then take advantage of it by for example to steal the house. Use it as botnet to DDOs attack. Or even have access to the local network through the IoT device.

Fig.3. Access and control of the CCTV system

5 Conclusions

This paper has as main objective to understand what IoT is, how it works and what its vulnerabilities are regarding its security and privacy.

First, I have provided a basis for better understand how these devices are used in quotidian and how these have great potential in the future. Then I discuss the possible attacks according to their operation and definition of the most common attacks. Next, regarding to preservation of IoT security and privacy, I outline the main concepts that should be present in these devices so that they can be considered safe and a brief notion of privacy regarding to IoT devices.

In the demonstration of security breach, it was possible to demonstrate that is not hard to access to this IoT devices, because most of them don't offer any resistance at hall. Some IoT devices simply did not reach their maturity and therefore constitute a possible threat for those who use them.

IoT devices are capable of sensing and storing data from the environment around them and how they are used, which can jeopardize the safety of those using them or even be used as botnets in DDoS attacks.

So, the IoT devices are fantastic but, the safety levels are not adequate unless the companies responsible for their production have security and privacy in mind when developing them.

References

1. Keyur, k .P.; Sunil, M. P.; Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges . vol. 6, Issue No.5, (May 2016).
2. CNCS,Homepage,https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/, last access 2018/12/21
3. Fortinet: Understanding the IoT explosion and its impact on enterprise security, (2017)
4. Mohamed A.; Geir M. K.; Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attackers, Norway, (2015)

5. Fei Hu.: Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations, pp.27-39, Taylor & Francis Group, (2016)
6. GlobalSign, https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot/, last access 2018/12/21
7. Mayuri, A. B.; Sudhir, T. B.; Internet of Things: Architecture, Security Issues and Countermeasures, vol.125, No.14, (September 2015).
8. Jan, H. Z.; Oscar G. M.; Klaus, W.; Privacy in the Internet of Things: Threats and Challenges, (28 May 2015)
9. OWASP, Internet of Things Top Ten, (2014)
10. Y. Andaloussi; M. D. El Ouadghiri; Y. Maurel; J. M. Bonnin; H.Chaoui; Access control in IoT environments: Feasible scenarios, (2018)
11. Nicolas, S.; I. D. Zaharakis; Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations, (November 2016)