Journal of Electronics and Sensors
Short Communication

Internet of Things (IoT) is Smart Homes and the Risks

Beretas C

PhD Candidate in Cyber Security at Innovative Knowledge Institute (Paris Graduate School) Paris, France

Received: 22 July, 2019**; Accepted:** 13 August, 2019**; Published:** 20 August, 2019

***Corresponding Author**: Beretas C. PhD Candidate in Cyber Security at Innovative Knowledge Institute (Paris Graduate School) Paris, France. E-mail: c_beretas@yahoo.com

Abstract

Undoubtedly is a technological revolution that has certainly focused on the interest of software development companies, companies of IT, hardware design, networks and artificial intelligence. A technological revolution that started a few years ago and has evolved rapidly, thanks to the technological evolution of IT and networks. It is a combination of many communication protocols, sensors and other intelligent technologies, the correlation between smart technologies, networks and services that all together complete processes in order to achieve the result for which they were installed. In advanced technology countries, both simple users and industry use IoT where sensors are simplified and automated at home and in industry, there is continuous monitoring, control and prediction of product failure for the benefit of efficient production of high quality products and control production at each stage of product processing / production. Someone could well think and say that all this is fantastic and that we have solved the problem of organization, easy life without further thoughts and worries since everything is done automatically.

An IoT in an intelligent house could literally regulate everything, using sensors and appropriate software could talk with a human person, as well as someone could appropriately entice all that security and literally take full control of the premises of a home with consequences from minimal to catastrophic including the complete destruction of a home.

Keywords: IoT, Internet of Things; Sensors; Security; Smart Homes; Surveillance; Networks; Cloud; Technology

Introduction

Several security advisors expressed their concerns about the safety of IoT a few years ago was something new and unknown in our days is something very familiar, complex, with many possibilities, connected to any type of network virtually unlimited, as an architecture can be gigantic and spread in quite large areas, receiving information from hundreds of different sensors where practically it can handle everything.

In a home, an IoT with the right sensors can control everything, such as filling a pool, automatically watering the garden according to the temperature and humidity of the ground, lighting the house indoors and outdoors by taking data from the sensors according to the actual illumination that exists, the disbelief and closing of the doors by taking data from the sensors and the identification of the human voice. The management of electrical appliances in the kitchen, temperature control in the oven and cooking based on the food found, water management using sensors that detect the real need for water and prevent over-consumption, control of hot water and electric power support if the water is not hot enough to reach the desired temperature levels. The above are just a few examples of using IoT, as easily as they sound, they are also dangerous, as long as we think about two things, the first is that IoT have access to the internet, every device connected to the internet is vulnerable to attacks. Secondly, if at some point in the IoT infrastructure it is violated, then the attacker could access all of these devices in a home and manage them as attacker wants. Based on the above, if there are no techniques and methods of confidentiality and validity at operating system level, none IoT is safe enough for the simplest reason that IoT play in different roles, connect to complex networks, include sensors from different manufacturers and different capabilities, mass gathering and processing of data, and then sending these data over networks to other platforms and services. When talking about the protection and safety of an IoT, we should always be intimidating its self-protection and the guarantee of its operating system without interference from third parties. Let's analyze the risks further.

Smart Homes and the Risks

As described above in the introduction to this article, IoTs can significantly improve the quality of life of humans. The security of an IoT is a matter of little concern with the services it offers, most users believe that connecting such a device to their network is safe while others are wondering why someone should try to break their own IoT since they have nothing important to hide from the others and the attackers do not have to win something to boast that they have committed a major violation of an IoT. Of course, all this is a mistaken thought and logic because we can not know the intentions of every man and even the neighbor thought. Let's analyze the level structure of an IoT. Each IoT is divided into 3 internal levels:

1. Interaction with its sensors.
2. Interaction with the Internet or other local networks and devices.
3. The level of data publishing, whether it is a cloud application. A device that performs functions in conjunction with the data processed by the IoT.

Further analysis of the above levels of an IoT indicates separately for each level the risks and dangers that exist. Below, the risks and dangers are thoroughly analyzed.

1. There must be a secure connections between the sensor and the IoT to prevent fake sensor combinations, this involves applying an appropriate security policy to ensure that the specific sensor is the one to be and that through it the sensor will interact with the IoT data in a secure manner. It should be borne in mind that the guarantee of the data that will interact

with IoT with the sensor should be ensured because, on the basis of these data, decisions will be made.

2. Storing the data is very important, and their perception could feed users with false data. The IoT should use secure and encrypted data transfer methods, storage space must also be safe, any tampering of the storage site poses a risk to both the data and the IoT itself. Creating a secure parallele storage system could control and restore fake files and let users know about it.

3. When transferring the data, some kind of attack on the IoT network, whether can be a man in the middle attack or can also come from the internet. Therefore, an algorithm for self-protection of the IoT network is needed. There are some algorithms that are used for data accurancy, but without the right security policies they cannot do much.

4. The kernel of an IoT is a red flag for attackers, it could hide a malware and loging forever the habits, data, and peculiarities of each user, giving the possibility to external attackers to create an online user profile and be able to know everything from its transitions, lifestyle, and especially personal data.

5. An incorrect security policy, a wrong software, a vulnerable sensor could burn a home. Literally, they could burn a house, if a sensor had been tampered by an outside attacker, it could affect, for example, a sensor who is responsible for oven temperature, an attack would probably have caused the overheating of the oven to provoke fire. And if we assume that there was a fire alarm sensor connected to IoT in the house, then an attacker might well be able to deactivate it.

6. Unauthorized users should not have access to IoT data management, operation, and publishing, the metadata often revealing important data sources. Authorized users should be granted partial access per level and not full access everywhere. Providing full access management everywhere at all levels then a DDOS attack could give complete access.

7. Most of the security techniques that have been created are mainly aimed at the accuracy of the information transferred to the IoT network. Thinking that in case of set-up elements are the sensors and the storage media, the possibility of contamination of the operating system remains second degree, a malware could work for years and log user habits, it will be a back door for the attackers, a back door of violation of human privacy.

8. The use of default features by the manufacturer itself makes it a vulnerable IoT network structure, anyone who has physical access and knows the IoT model is easy to try to access by identify for its factory settings and factory passwords. This is a very serious attack, the first thing people have to do is change the default password and in some cases the default settings.

9. User accounts with incorrectly restricted permissions, no password, access to services without user authentication, are red shield for IoT security, can easily break the security of the IoT network that depending on the type of installation in a home will also have consequences.

10. When an IoT device is installed in a home in which there is a computer network that interacts with the IoT, should be ensured the harmonic communication with each other. If the computing network is unsafe then easily can break an IoT security. An IoT cannot protect a vulnerable computing network, and a vulnerable computing network cannot protect an IoT.

11. It is important that where they store the data either if they will be stored locally on the premises, so there should be a way of data accuracy and backup, while

in the case of Cloud the physical access is not permitted, should be ensured encryption of data information there, while is important to creating a recovery plan for information where something goes wrong.

12. The management of a IoT through a web environment is the backdoor of an IoT network mainly through Wi-Fi networks. The violation of a Wi-Fi and then access to the home network of the home allows external attackers to try illegally entering the IoT device through its web console, where any successful access, the attackers would have full control over the functions through the sensors throughout the home.

Conclusion

The above risks and dangers are the ones that someone should take care of and think about when installing an IoT in a home. The security of a network such about an IoT security is not easy, especially when it comes to other types of networks and other IoT devices. The current security situation of an IoT has grown quite a bit, but not to a great extent to the safety of an IoT, most techniques focus on data security and encryption and not on IoT's own protection. Its growth is rapid and will remain an upward course for years to come. Users have loved it, and every day new companies are part of the list that wants to upgrade their equipment for more productive product creation process, also the demand for creating smart homes is growing, the power of the artificial intelligence has been enter in our life, user-friendliness and automation is especially eager for new users.

Reference

1. Etter D 2016. IoT Security: Practial Guide Book
2. Perry Lea. 2018. IoT Hackers Handbook.

***Citation*:** Beretas C (2019), Internet of Things (IoT) is Smart Homes and the Risks. J Electron Sensors; 2(1): 1-4.

DOI: 10.31829/2689-6958/jes2019-2(1)-105