The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

IOT SECURITY OPTIMIZATION

DUŠAN BOGIĆEVIĆ
University of Nis, Faculty of Electronic Engineering, dusan.bogicevic@gmail.com

IVAN TOT
University of Defence, Military Academy, Serbia, ivan.tot@va.mod.gov.rs

RAMO ŠENDELJ
Univerzitet Donja Gorica, ramo.sendelj@udg.edu.me

Abstract: *This paper deals with the safety of the Internet of Things (IoT) and research of IoT architecture. It is based on theoretical foundations of IoT. The points that could be potential places for an attack on the system are presented in this paper. Architecture that is proposed is based on the physical organization of devices and sensors, as well as on their communication with the servers and applications across different types of networks. Besides the physical part, the paper proposes a software architecture that would enhance the security of Internet devices.*

Keywords: *IoT, architecture, organization, sensors*

1. INTRODUCTION

The term Internet of Things (IoT) came into existence some 15 years ago. It was conceived as a world of objects that exchange data. Data exchange is not between man and machine, but the communication between machines (M2M) is introduced. Kevin Ashton in his work from 2002, published under the title IoT said: "We need an internet for things, a standardized way for computers to understand the real world". [8]

After the appearance of social networks where people communicate with each other, we come into an era where "social devices network" is created - network that controls systems, collects data, analyzes and reacts depending on the data. "...The Internet of Things (IoT) promises to be the most disruptive technology since the advent of the World Wide Web. Projections indicate that up to 100 billion uniquely identifiable objects will be connected to the Internet by 2020, but human understanding of the underlying technologies has not kept pace. This creates a fundamental chal-lenge to researchers, with enormous technical, socioeconomic, political, and even spiritual, consequences. IoT is just one of the most significant emerging trends in technology but some people, such as Nikola Tesla had a vision of IoT almost 100 years ago, "when wireless is perfectly applied the whole earth will be converted into a huge brain ... " [7].

One of the leading companies in the field of IT Microsoft is developing support through its services for IoT called Microsoft Azure IoT Suite. Google has bought company Nest engaged in the production of "smart" thermostats. Also, Google owns Android, one of smartphones' operating systems. These two giants in the field of IT have devoted their resources and attention into studying IoT, from which we can conclude that this is something in our time (the present) and what awaits us in the future.

In 1965 Japanese researchers led by Yoshiro Hatano determined that the man should have a day walk with over 10,000 steps[1]. Today we can analyze this statement by studying people and their movements. In addition to the movement we can analyze how much time people spend in their homes, in front of computers, what they like to buy, who they socialize with and much more. These data are now realistic, without observing the sampled population. The questions that arise are: Are all these data safe? and Why are these data are stored on the Internet?

It is good to analyze this data. For example, if our doctor looks at our physical activity, he can alert us to the possible harmful consequences. Alarm for our bad habits can be sent through software, and when we get to the doctor, he can have an accurate picture of our movement based on data and information obtained from the software. The image obtained in this way can contribute to better diagnosis and make our body back into a healthy state. The data collected this way about our movement can also be analyzed by an intruder, and to come to the conclusion that we spend two hours outside of home while doing some physical activity. In this way a burglar would have the information when he needs to organize a robbery.

These two examples intended to show the importance of information on the movements that are on the Internet in the case of medical treatment, and even more important objective, to protect information sent by devices (sensors). This paper is devoted to Internet of things.

2. PARTS OF IOT ARHITECTURE

IoT architecture basically consists of three parts. These three parts are shown in image 1. [1]

[1]http://www.slideshare.net/mazlan1/internet-of-things-iot-we-are-at-the-tip-of-an-iceberg

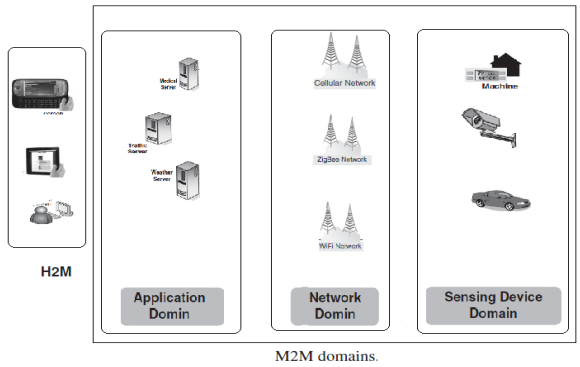

Image 1: IoT architecture

2.1 Application domain

Application domain (image 1) represents servers' architecture that participates in data processing, communication with other devices and communication with a human.

The purpose of these servers is similar to servers in banks, where data are collected, processed and stored. These servers with their services provide communication via Web, mobile and desktop applications with a human, and in addition to H2M communication provide M2M communication.

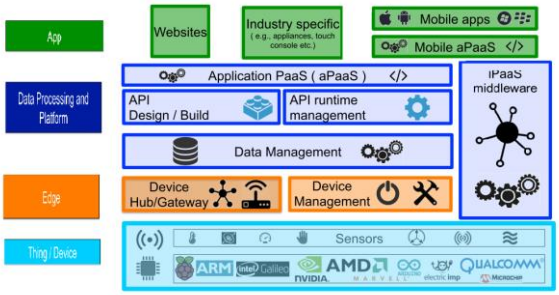

Image 2: IoT stack[2]

In the case of IoT stack, application domain is divided into:

- **application part** which serves as a user interface for device management. This part represents Web, mobile and desktop applications that communicate with servers in order to exchange information and send commands.

- **the part associated to the platform and data processing** which purpose is to make as much as possible realistic picture of actual objects, that is the real world. In this part, virtual objects we manage and which send us information live. If we IoT imagine as a human body, this would be his brain, a place where all the information from sensors are collected and the place which provides management.

2.2 Network domain

The network part of IoT uses existing technologies (Ethernet, WiFi, Bluetooth, ZigBee, GSM, etc.) for data exchange. The objective of this layer is to transfer information from device to server and vice versa. What is expected from this exchange is that it is safe and reliable. For IoT, the most significant is the wireless communication (radio communication) where it is necessary to take care of security. Most wireless networks have some cryptographic algorithms implemented. Wifi has implemented WEP and WAP methods of protection. 90% of data that are present on the Internet are personal data, and in 70% of cases non-encrypted traffic is used[3].

If we look at IoT stack (image 2), the network part represents border section. Devices are equipped with implemented communication interfaces on one side, as well as servers on the other side through which the communication is accomplished and management of devices is ensured (image 1).

2.3 Device domain

Device (or sensor, actuator) domain is the beginning of IoT. It is the layer in which reality becomes virtual world. This is the place where data is received and converted into digital data used by servers (image 1). Types of devices used for collecting data can be in range from simple sensors such as sensors for heat, temperature, light, moisture etc. to location sensors, cameras and other complex sensors or devices (image 2). The number of connected devices exceeds the number of human population. In 2010 the number of devices was almost two times higher than the number of human population.[4]

This layer collects data from one or more sensors. Its aim is to process collected data mostly as analog values and forward it in digital format to the next layer. The collected data is processed on a specific hardware, which has its own software (firmware).[2]

Device domain, depending on the complexity and purpose of the device, can also have a management layer for devices. If we take a camera as an example, it sends us a picture as an information, but we may want to move it. The movement of the camera requires that we have a layer of software and hardware that will allow its management via the camera interface it provides.

3. BASIC ORGANISATION AND IOT SECURITY

IoT architecture is not based on one device, but on sets of devices that in a variety of ways collect information. In case of IoT, the most used term is environment, so we can see the prefix "smart" like smart homes, smart streets, smart parking, smart garbage cans, smart cities etc... Smart environments can be defined as sets (federation) of sensors and actuators that are designed for home, building, city, transport etc…[3][9]

[2]http://www.slideshare.net/sumitcan/iot-architecture

[3] http://www.slideshare.net/jvermillard/the-5-elements-of-iot-security

[4]http://www.slideshare.net/mazlan1/internet-of-things-iot-we-are-at-the-tip-of-an-iceberg

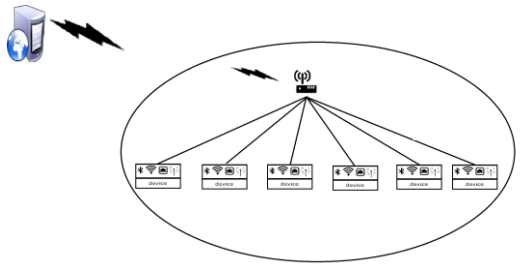

Image 3: Smart devices communication example

IoT is a complex system with a large number of sensors. The most perfect organization that works with the largest number of sensors is the human body. Every part of our body has its own task from touch receptors to nerve cells in the brain. Architecture which the IoT should aim is the architecture of the human body.

If we consider an IoT device with its sensor (sensors), we can forward its data to other devices and services. However, if we have an environment that consists of multiple devices that collect data and all of them send data to servers, then it is necessary to secure each communication. This approach increases hardware and software requirements for each device, whereby the price of each device increases.

4. POINTS OF POTENTIAL ATTACK

Each part of the IoT architecture may represent a potential point of attack. [4]

4.1 Security of device

Places that are the least sensitive to direct attacks are physical devices (sensors), because of their technology, which primarily consists of electrical circuits designed to convert received analog information from the environment into digital format. The devices themselves may offer to potential attacker only the information they possess. Attacks on this part of architecture, beside illegal reading the values from the sensors, may be realized by giving false values, whereby an attacker could test the system. By testing the system, one can get specific values that are important for its functioning. For example, if the humidity sensor sends a huge value, it is possible that the flood occurred, and the system will react by shutting off the water.

Security on the device layer should be realized through physical protection and devices' access control.

4.2 Network security

The next part of the IoT architecture that is sensitive to attacks are networks that are used in the exchange of information. The attacks in this part can also be realized by collecting information from one or more devices. Such attacks where the traffic is only observed, are known as sniffing. Depending on the type of network used in communication (WiFi, Bluetooth, ZigBee...), depends the method of attack, given the specific character of the technologies used for the particular network. Another way of using the network layer for the attack is the phishing scheme using legitimate participants address.

Security in this part can be implemented by using cryptography algorithms which collecting information make difficult. As mentioned before, most wireless technologies already have some form of protection implemented, so those methods of protection should certainly be used, with possible improvement of existing algorithms. [5]

4.3 Application security

When considering the application layer, firstly one should pay attention to the application user. Logging on to the system should be the only place where the legitimate user may enter the system. However, it can also be the place of interest for potential attacks. This is the place where the greatest number of attacks is expected, so it represents a challenge for programmers. In addition to software protection, user education about the importance of the system and possible threats is essential.

5. ADVANCE ORGANIZATION

An approach that can relieve a server with a large number of connections and communication and management interfaces, is to introduce a central device, which would secure communication and provide management between the server and the sensors or the specific devices that need to be controlled. In this way, managed devices can be organized into the physical and logical parts. As said before, IoT is a large and complex system. To quote a Chinese strategist Sun Tzu: "Management of many is the same as management of few. It is the matter of organization."

This approach may relieve the individual peripheral devices in a way that they would possess only one communication interface (Image 4).

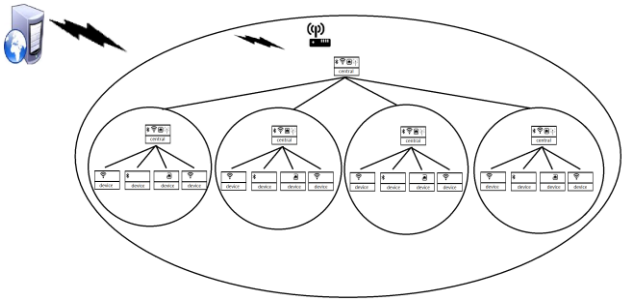

Image 4: Advance organization

In cases where there are multiple devices (sensors, actuators, etc.) that need to be controlled and are spatially apart, multiple control units can be used, which would represent logical or physical parts. These devices would

be central to local devices and would be connected to the main central device. The main central device would have the task of maintaining secure communication with the server, while allowing management of peripheral devices using multiple technologies such as wireless, Ethernet, GSM, BT etc. which provides a significant management functionality and security in case of loss of communication over a single medium. In this way if we want we can receive the data from a peripheral device through WiFi, BT or GSM even if it has only one interface, through which it is connected to a local (central) device. In addition to introducing the main central device, it would be desirable to allow a local central device to be able to take over the functionality of central device to provide redundancy in case of main central device failure.

One additional advantage is the reduction of the number of used addresses (IPv6 is not yet fully incorporated in Europe).

In case of a house with IoT devices (Image 5), which provide control of lights, air conditioning, heating etc., communication would start through the management application, which would address a server. Server would receive a command which needs to be executed and forward it over a network to a central device. Central device would translate the command into the command for a specific device and forward it for execution through local central device if it exists. For each command it is necessary to provide the confirmation that it is realized. Feedback should be returned from the local to the central device in the home, and then to the server, which would send it to the application to confirm the user that it has been successfully executed.

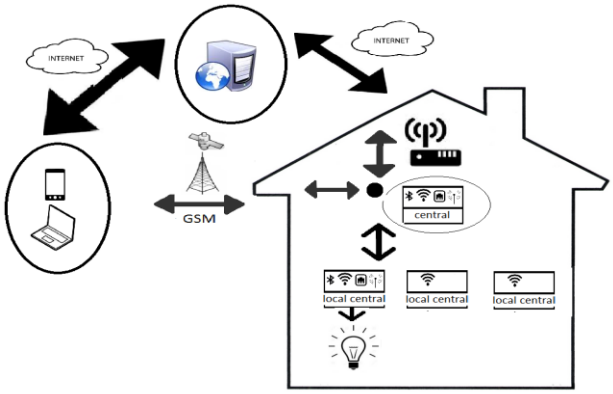

Image 5: Smart home example

Communication between central device and peripheral devices should be a compromise of price, quality and conditions that are present in the given case. By using a wired connection confidence would be achieved, while the security would be increased by using cryptography algorithms.

Regarding the security of the central device, it should have X.509 encryption standard implemented. Also, it very important to enable all devices that are capable of encrypting communication to be updatable since "you can't secure what you can't update". A very common mistake is a firmware update via HTTP protocol which is not secured and in that way could inflict some kind of damage in case there is a backdoor.[6]

6. CONCLUSION

The approach presented in this paper is aimed to propose a way to reduce the price of devices that we manage. In addition to price, their complexity decreases, and a central device is introduced. The possibility of protection increases while greater functionality for all devices is provided.

REFERENCES

Books:

[1] D. Minoli, "Building the internet of things with IPv6 and MIPv6: The Evolving World of M2M Communications", John Wiley & Sons Inc., Hoboken, New Jersey, 2013.

[2] Gunther Gridling, Bettina Weiss, "Introduction to Microcontrollers Courses 182.064 & 182.074", Vienna University of Technology, Institute of Computer Engineering, Embedded Computing Systems Group, 2007.

[3] Dirk Slama, Frank Puhlmann,Jim Morrish & Rishi M. Bhatnagar ,,Enterprise IoT Strategies & Best Practices for Connected Products & Services", O'Reilly Media, Sebastopol, United States of America, 2015.

[4] H. Chaouchi, "The Internet of Things: Connecting Objects to the Web", John Wiley & Sons Inc., Great Britain and the United States, 2010.

[5] Fei Hu ,,Security and Privacy in Internet of Things (IoTs)", CRC Press, New York, United States of America, 2016.

[6] Peter Waher ,,Learning Internet of Things", Packt Publishing, Birmingham, UK, 2015.

[7] IEEE Computer. The Internet of Things: The Next Technological Revolution. Special Issue, February 2013.

[8] Kai Sachs, Ilia Petrov and Pablo Guerrero (Eds.),, From Active Data Management to Event-Based Systems and More", Springer-Verlag Berlin, Heidelberg, 2010, pp. 242-259.

[9] Ovidiu Vermesan , Peter Friess,, Internet of Things - From Research and Innovation to Market Deployment", River Publishers, Gistrup, Denmark, 2014,pp 7-141

[10] Uckelmann, Dieter, Harrison, Mark, Michahelles ,, Architecting the Internet of Things", Springer-Verlag Berlin, Heidelberg, 2011, pp. 229-252