Challenges for providing security in the Internet of things

**Tsvetomir Gyuretsov, Jordan Raychev,
Georgi Hristov, Plamen Zahariev**

The cyber security issues and problems worry many developers around the globe. After the Internet of Things (IoT) concepts were announced, many companies around the world have focused their work on the developing of new ways to secure the fast growing network of smart devices. It is essential to find new flexible means for protection, which meet the following basic requirements – adaptability to the fast growing number and types of network of devices, applicability to each main layer in the concept of IoT, low computing power, generation of less traffic over the network and the most important thing - not limiting the application of the smart devices. Another very important aspect, on which developers must focus, is where to implement these security methods. Three layers can be distinguished when we talk about establishing reliable protection for IoT – securing the devices, securing the cloud and securing the local network. All of these points are very important for applying good and secured core for using this new technology. In case of a problem, in one of these layers, all the efforts related with the developing of new protocols, fire walls or software products would be wasted. Many years of experience are accumulated in the establishment and the implementation of the security and the protection systems for the well-known wire and wireless technologies. This presents a solid beginning and a running start for the developers occupied with this hard task. Unfortunately, the specifics of the ideology of the Internet of Things makes these well-known technologies useless in the form we know them.

Предизвикателства при предоставяне на сигурност в интернет на нещата. (Цветомир Гюрецов, Йордан П. Райчев, Георги В. Христов, Пламен З. Захариев). *Проблемът с кибер сигурността вълнува голяма част от разработчиците по целият свят. След обявяването на концепцията на IoT, компании от цял свят започват работа по откриване на нови методи за защита на разрастващата се мрежа от така наречените умни устройства. От съществена важност е откриването на нов вид гъвкава защита, която трябва да отговаря на следните основни изисквания – адаптивност към постоянно разширяващата се мрежа от устройства, приложимост на всяко едно от основните нива в концепцията на IoT, непретенциозност към изчислителна мощност, да генерира минимален трафик в мрежата и най-важното да не ограничава приложението на този вид устройства. Друг много важен аспект, на който трябва да се обърне внимание, е къде трябва да се съсредоточат усилията при имплементиране на тези защити. Разграничават се три ключови етапа при изграждане на надеждна защита, свързана с интернет на нещата – защита на устройството, защита на облачната инфраструктура и защита на локалната мрежа. Всяка една от тези точки е от първостепенна важност за една добра и сигурна среда за използване на този вид нова технология. При евентуален проблем в един от тези слоеве, всички усилия свързани с разработването на нови протоколи, защитни стени и софтуерни продукти за защита биха били безсмислени. Тридесет години опит натрупан в изграждането и прилагането на защита на познатите ни жични и безжични технологии е едно солидно начало и един летящ старт за разработчиците, заели се с тази нелека задача. За жалост спецификата на идеологията IoT прави тези познати технологии неприложими, не и във вида в които ги познаваме.*

Introduction

Internet of things (IoT) is very hot and important topic in the engineering societies and the scientific circles and is essential part of the everyday life of the 21st century people. With the advancement of the technology, these "things" have evolved and are no longer seen as separate devices. In order to provide a better service and to be in help of the people, those devices must communicate and interact between themselves. The main requirement for achieving this is to find an effective way to control all those devices wherever they are physically located. Despite of all benefits, which are brought by the IoT, there is one major reason for concerns – the IoT security.

While the security topic is nothing new to the data networks, it certainly presents new and unique challenges in the area of the Internet of Things. Addressing this problem and ensuring IoT security is a fundamental priority and would help preserve the integrity of the user data and their identity.

Problem statement

What exactly is the Internet of Things? What are the devices and the services that this network consists of? Internet of Things, sometimes referred as Internet of Everything (IoE) is a new concept, which refers to a multiple devices grouped in networks (also known as clusters) that communicate with each other via wireless protocols or other means without any human interaction. While the term "Internet of Things" is relatively new, the concept of devices communicating through the existing networks has been around for quite a while. For example, in the late 1970 there were commercial systems for monitoring and metering of the electrical grid via the telephone lines [6]. Nowadays that concept hasn't changed much. Today, the IoT enabled devices make use of the existing IP networks to communicate with each other in an efficient and secure manner.

Ensuring reliable, resilient, stable and more importantly secure communication between all IoT devices is not an easy task. There are a lot of known procedures and security mechanism to build such secure channels, but how effective and robust are they? That is a question which should be answered right before any new IoT concepts are proposed. For example one can use white- and blacklisting methods to secure the devices from malicious software, but they are not enough. The basic principle of the blacklisting approach is based on a mechanism (block list), which allows all elements to be processed, expect those explicitly mentioned on that particular list. It is an effective way to block some threats, but as the list gets bigger and bigger the physical space (disk space) on the device becomes exhausted and will prevent the further storing of the exceptions. The opposite of this approach is the whitelisting approach. That mechanism is based on a white list which allows all elements that are mentioned on it to go through. This is a more effective way of blocking malicious software, but requires more processing time, which may not be available for the particular device. The third method is called greylisting. It represents a hybrid mechanism that combines the advantages of the white- and the blacklisting approaches. The mechanism works by temporary blocking or allowing certain application until additional step are performed.

Another aspect, which should be considered, is the increasingly larger number of devices that are connected to the Internet. As the number of those devices grows, more potential vulnerabilities and security flaws will emerge. Another problem related to the one described above is the increasing of the network traffic. Because of that, the new security mechanisms should be very resilient and adaptive to that constantly growing network and efficient enough to minimize the networks overhead.

During 2015, Forrester Global Business Technographics published a case study, which is summarized in Fig.1. It shows the biggest threads to the security engineers working in the IoT sphere.

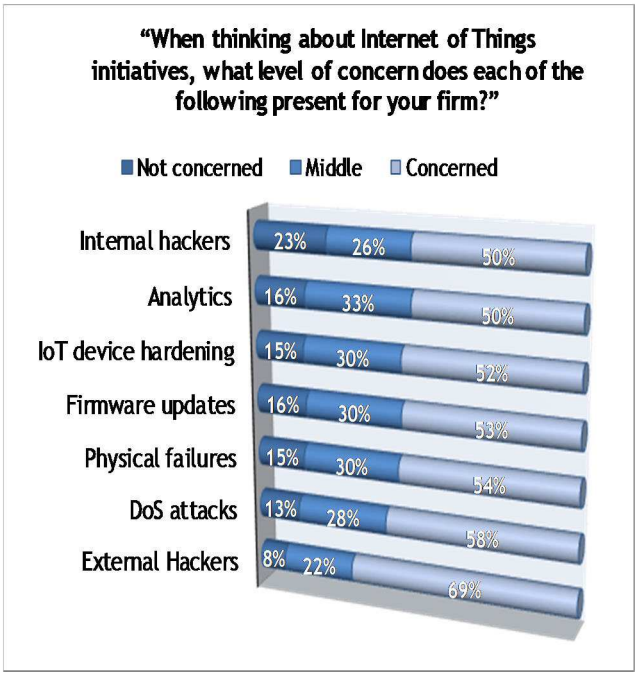

Fig.1. Forrester Global Business Technographics case study summary.

2053 IoT specialists participated in this study, 69% of whom are really concerned about cyber-attacks from the outside. The study shows that most of the security engineers are worried about DDoS (Distributed Denial of Services) attacks, authentication related issues, etc.

Those are just small fraction of all related to IoT problems. Another concern, which was not mentioned earlier, is the life span of the security mechanisms. According to lead scientists from Stanford University, every new security concept must have a life span of at least 15 to 20 years. Table 1 clearly shows the life span of the cryptographic algorithms used today. It can be seen that most of them are used not less than 10 to 15 years, some of them even more than that.

Table 1

Life span of cryptographic algorithms and hash functions

	Algorithm	Year created	Year cracked	Life span, years
Symmetric Algorithm	DES	1979	1994	16
	RC4	1994	2013	19
	RC2	1996	1997	1
	3DES	1998	2015	17
	AES	1998	-	18+
	Camellia	2000	-	18+
Hash functions	MD5	1992	2004	12
	SHA-1	1995	-	21+
	SHA-256	2000	-	18+

There are three main layers, which may be subject to a cyber-attack – the cloud infrastructure, the local network and the device itself. Securing just one of the layers is really not enough, so a multi-layer approach should be considered. In this way if there is a breach in one of the layers, the others may be sufficient enough to preserve the optimal work of the devices in the network.

Secure boot

The first layer on which a security mechanism can and should be implemented is the IoT device itself. When the device is powered on and introduced to its network, it somehow has to prove his authenticity and integrity. This can be achieved by the application of cryptographically generated digital signatures in the same way the applications are signed and verified using similar signatures or to the way a person signs legal documents. Once this step is completed, the device should be authenticated and will be managed from authorized personnel.

Authentication

Authentication or more specifically digital authentication is a security process, in which the credentials, provided by the user or the device, are compared to those in a specialized database. If the credential matches that particular user or device would be successfully authorized. That concept can easily be implemented to the world of Internet of Things. When a device is powered on and connected to the network, it must first authenticate itself and then be able to send or receive any kind of information. Sadly, most of those devices cannot provide any means to be controlled via a graphical user interface (GUI) or a command line interface (CLI). Because of that the well-known authentication processes cannot be used. The device should also have integrated secure storage, which is going to hold the security credentials. Once the device is powered on it can use those credentials in order to authenticate itself and be able to communicate with the rest of the network.

Access control

Access control is a security technique that can be used in order to control (allow or deny) access to particular resources in a computer or a network environment. Nowadays, every device comes with some sort of an operating system (OS). There a plenty of role-based access controls (user account, privilege levels, etc.), which are directly build into the device OS and can be used right away to control the access to the device and its resources. In that way if a component or a device gets compromised, the attacker would have access only to that particular device or resource.

Firewalls

Another possible solution, which can be used, is the old fashioned firewall system. The firewall system is able to monitor the outgoing (from the device) and incoming (towards the device) traffic. Based on a set of predefined security rules, called security policies, the firewall is able to control (allow or deny) that particular network traffic. The tricky part here is to successfully identify the traffic of interest. This can be achieved either by specifying the source and the destination address, the source and destination application ports, the type of the traffic (TCP, UDP, etc.) or any combination of them.

IDS and IPS

The intrusion detection and the intrusion prevention systems (IDS and IPS) are quite similar to the software firewalls, but are much more powerful. They

also monitor and control the outgoing and the incoming traffic, but they can perform much deeper and thorough analysis on it. There are many similarities between IDS and IPS, but they are also quite different. Intrusion detection systems are used to monitor the network (Network intrusion detection system – NIDS) or the device (Host-based intrusion detection system – HIDS) for malicious activity or policy violation, but won't take any action, expect signaling for it. On the other hand, the intrusion prevention system, much like the intrusion detection systems, will examine the network traffic flows, but will also take actions against any malicious activities or security threats. This is achieved by either using a signature-based detection (like the anti-virus software) or by using anomaly-based detection, which uses machine learning to differentiate malicious from trustworthy behavior on the network.

Security updates and patches

Once the device is in operational mode, it will start receiving security updates and patches from its vendor. The main issue here is that there are thousands of devices, so the security patches and the updates must be delivered in a way that will preserve the extremely limited bandwidth that is available.

Conclusion

While the concept of combining devices, sensors and networks to monitor and control devices has been around for quite a while, the Internet of Things (IoT) is relatively new and an extremely interesting topic. There is no question that the IoT has the very potential to dramatically increase the availability of information, which will present a brand new reality of interconnected "smart" devices. Despite of all of the possibilities of this new reality, like everything else, it also has and some disadvantages – in this particular case the problem is the securing of all of these devices. Security at both device and the network layers is essential to the operation of the Internet of Things. The same intelligent systems that enable those devices to perform their tasks must be used to recognize, analyze and prevent the security threats.

This paper is a modified version of work reported in the XXIV National conference with international participation TELECOM, Sofia, Bulgaria, 2016.

Acknowledgements

The work presented in this article is completed as partial fulfillment of a project FNI-16-RU-10 "Development of a prototype of a robotic unmanned aerial platform for remote monitoring of critical infrastructure" and project FNI-16-FEEA-04 "Study of the impact of the controller location in the management plane on the performance of software defined networks", financed under Scientific Fund of the University of Ruse.

REFERENCES

[1] Levis, F. Secure Internet of Things Project. Computer Forum Internet of Things Workshop, Stanford University, 2016.

[2] Security in the internet of things. Lessons from the past for the connected future, Wind River Systems. White Paper, 2015.

[3] Security Guidance for Early Adopters of the Internet of Things (IoT), Cloud Security Alliance, 2015.

[4] Rose, K., S. Eldridge, L. Chapin. The Internet of Things: An Overview, Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC), 2015.

[5] Levis, Ph. Secure Internet of Things Project. Secure Internet of Things Project Workshop, Stanford University, 2014.

[6] Machine to machine, https://en.wikipedia.org/wiki/Machine_to_machine

Eng. Tsvetomir Gyuretsov *– PhD Student, Department of "Telecommunications", University of Ruse "Angel Kanchev". His current research interest includes telemetry systems and protocols, software defined networks, IoT, unmanned aerial vehicles and robotics.*

tel.:082/888 817 e-mail: tsguyretsov@uni-ruse.bg

Eng. Jordan P. Raychev - *PhD Student , Department of "Telecommunications", University of Ruse "Angel Kanchev". His current research interest includes telemetry systems and protocols, software defined networks, IoT, unmanned aerial vehicles and robotics.*

tel.:082/888 817 e-mail: jraychev@uni-ruse.bg

Assoc. Prof. Georgi V. Hristov, PhD - *Department of "Telecommunications" at the University of Ruse "Angel Kanchev". His current scientific interests include communication networks, new generation network architectures, network virtualization technologies, unmanned aerial vehicles, 3D visualization and printing technologies and robotics.*

tel.:082/888 663 e-mail: ghristov@uni-ruse.bg

Assoc. Prof. Plamen Z. Zahariev, PhD - *Department of "Telecommunications" at the University of Ruse "Angel Kanchev". His current scientific interests include IP and sensor networks, cryptography, wireless communications, IoT, 3D technologies and robotics.*

tel.:082/888 663 e-mail: pzahariev@uni-ruse.bg

Received on: 12.12.2016