CYBERSECURITY OF INTERNET OF THINGS –RISKS AND OPPORTUNITIES

A.A. Karlov

Laboratory of Information Technologies, Joint Institute for Nuclear Research, 6 Joliot-Curie, Dubna, Moscow region, 141980, Russia

E-mail: Alexander.Karlov@cern.ch

The Internet of Things (IoT) is developing at a tremendous rate. It is a combination of devices connected via the Internet and other networks which are capable of receiving information from the outside world, analyzing it and, if necessary, managing external devices as well as providing information for decision-making. The goal is to create a more comfortable, safer and efficient environment for both personal and public life. But like any rapidly evolving Internet technology, there are increasing risks from the point of view of cybersecurity. The most significant cyber-incidents in the world of IoT, the reasons for the occurrence of such cases and possible ways to improve the situation with IoT cybersecurity are considered.

Keywords: Internet of Things, "smart" things, information security, vulnerability, botnet, Mirai

1. Introduction

Kevin Ashton [1] first proposed the concept of the "Internet of Things" (IoT) in 1999, but the development of the IoT market began rapidly only about 10 years later. The notion of "things" refers to any physical objects which have their own IP address and can connect to the network in order to send / receive data - the so-called "smart" things.

According to HIS Markit evaluation, the number of "smart" devices in 2015 was about 14.4 billion, it will increase by 60% to 23.4 billion in 2017, and is projected to reach 30.7 billion by 2020 and 75.4 billion by 2025 [2]. At present, the IoT market has covered practically all areas of human activity: personal life, industry, medicine, urban development, power engineering, agriculture, military, etc.

The use of smart devices in private life in many cases increases the comfort and safety of its users. In medicine, they provide the possibility of constant remote monitoring of patients' condition and can carry out, if necessary, urgent assistance. Industrial Internet of Things (IIoT) is the foundation of a new industrial revolution in which smart manufacturing will play a decisive role in improving production efficiency through better automation and data transmission as well as through data analysis with the use of artificial intelligence for decision making. Smart cities allow optimization of the usage of urban resources, improving mobility of the population and its security.

Unfortunately, the growth in the number of smart devices has not been accompanied by due attention to their safe use. As a result, hundreds of millions of devices were vulnerable in terms of both their own architecture and software, as well as communication protocols. Using cloud services to store and analyze data from these devices increased the danger of unauthorized access to confidential information.

2. The Internet of Opportunities

Smart homes contain devices that provide security (video cameras, motion sensors, electronic locks, etc.), climate control, smart lighting, various household appliances (TV, coffee machine, refrigerator, oven, etc.). These devices can provide information to and to be controlled from the smartphone both directly (via Bluetooth or WiFi), and using Web-based applications. The spectrum of house-oriented devices is continuously growing.

As an example, one can consider the "smart" baby monitor Aristotle [3]. This device is announced as "The First All-in-One Voice Controlled Smart Baby Monitor That Grows with Your Child," which informs parents of the child's condition and can talk to him using the principles of artificial intelligence and a cloud-connected platform for storing data and making decisions. It is interesting that, as the child grows, the device also raises its "intellectual" level (from telling fairy tales to downloading information from the Internet on the school curriculum).

Sometimes smart devices perform a role that is not directly intended for them. During a family quarrel [4], the man began to ask if the woman had called the police. The "intelligent" voice assistant took this statement as a command and called 911. At the other end of the line, this violent dispute was followed and at the critical moment the police forces were sent in and prevented the serious consequences of the incident.

According to the estimates of Zion Research, the global smart home market will grow from USD 24.1 billion in 2016 to USD 53.24 billion by 2022 [5].

Wearable smart gadgets such as fitness trackers, body mounted cameras, smart watches, heart rate monitors, smart clothing, virtual reality glasses, GPS tracking devices, etc. are gaining more and more importance in the everyone's personal life. Some of them initiate users to monitor their physical health, encourage sports activities, expand the horizon of interests, others help to monitor health.

Strong competition in the market of these devices drives the expansion of their functionality with a reduction in price. Modern smart watches can understand voice commands, send and receive messages, search the Internet, record memos, track your heart rate and steps, calculate calories burned,

perform sleep monitoring, register your workout with GPS, offer you your favorite music and much more. Internal memory of 4-8 GB allows to download new applications when they appear.

According to Tractica, the global wearable devices market will grow to 187.2 million units by 2020, more than 10 times in seven years (2013: 17.0 million units). Growth is primarily due to smart watches, fitness trackers and wearable cameras [6].

A separate area called mHealth (an abbreviation for "mobile health") uses wearable devices and wireless communication for real-time health control and services provided by medical professionals. Remote monitoring is especially important for the support of chronic patients (diabetes, cardiovascular disease, tuberculosis etc.), as well as for people who need constant monitoring (e.g. physical and mental health during the prenatal period or during rehabilitation after a serious operation). More information about mHealth can be found in [7].

The team of Professor Dae-Hyeong Kim at Seoul National University in South Korea is developing a wearable device for diabetics based on a graphene plaster. This device can control the blood sugar level by analyzing the composition of sweat on the hand, and, if necessary, enter the dose of metformin stored in the device [8].

The Industrial Internet of Things (IIoT) opens completely new opportunities in many sectors of the industry: manufacturing, transportation, mining, energy production and distribution and many others [9]. The IIoT approach allows the control and optimization of all stages of production, including transportation, storage and use of raw materials and components, obtaining more complete and visual information in the production process, in storage and distribution of final products. This is the way to smart manufacturing; when instead of closed cycles and closed-loops organization there is the possibility of a flexible approach to the production of goods with individual characteristics in accordance with changing requirements of the market and individual customers, the ability to control and optimize all aspects of enterprise activity.

The information created by intelligent devices and industrial control systems allows timely and correct decisions concerning the efficiency of production, the support services and the business model of the enterprise and so helps companies to make better investments decisions. Because of the huge amount of data and its complexity, cloud computing, artificial intelligence, real-time analysis can be used to make decisions.

IoT strategy is the basis for creating cost-effective, comfortable, ecologically clean and smart cities. Data from numerous electronic sensors distributed throughout the city and connected to the Internet and other networks allow the collection, analysis and decision making on key issues of the city's life in real-time: e.g. transportation, lighting, heat supply, waste disposal, goods turnover, etc. It also provides important information and community services to city residents and visitors. Smart cars, private or based on shared mobility solutions, will be able to choose the best way of travel while saving passengers time and operational cost. Intelligent traffic light system can help emergency vehicles to reach incidents with a minimum of delay. Smart street lighting, taking into account weather conditions, the presence of transport and pedestrians, will allow the optimization of electricity costs. There are some places where smart city technologies is being currently implemented successfully: Dubai [10], China [11], Barcelona [12] and many others.

The Smart Agriculture project in Salerno (Italy) [13] is a good example of the IoT approach to integrated accounting and analysis of multiple factors for obtaining the optimal result. It allows real-time data capture from the fields and take into account current and future weather conditions, humidity and other soil characteristics, availability of water, energy resources and others conditions to produce the cost-effective high-quality products.

3. The Internet of Risks

The rapid introduction of IoT technology, along with the huge benefits, brings new and significant risks associated with vulnerabilities present in smart devices. Vulnerabilities refer to both the software and hardware components of these devices, communication protocols, as well as storage and processing of data in smartphones, tablets, data centers and cloud structures.

Widespread use of default passwords and unpatched firmware mean that compromising the devices is relatively easy for the attacker. The developer company often leaves the default password in order to remotely service the device in case of questions from the customer. But even if the instruction says that the default password must be changed when installing the device, the customer does not always care about doing it, considering that he does not represent an interest for intruders. For the same reason, he takes little care of installing patches, which the developer suggests to fix detected vulnerabilities.

Another reason for low security is that the limited computational ressources of smart devices do not allow the implementation of complex cryptographic algorithms, especially as firms are trying to reduce the cost of their products in a competitive environment. As a rule, when choosing devices, for example, for a smart home, customers can not assess the security of the devices and are basically guided by affordable price. Sellers are more interested in increasing sales and are not responsible for giving advice on the security of the proposed product range.

Communication protocols used by smart devices have serious vulnerabilities. ZigBee is a popular smart-home wireless communication standard used by the majority of Internet of Things (IoT) devices today [14]. ZigBee protocol, which lets IoT devices talk to each other, is implemented by major vendors including Toshiba, Philips, Huawei, Sony, Siemens, Samsung, Motorola, and many more. The biggest problem, as pointed out by researchers, is that there is nothing users could do to make their smart devices more secure, and since the flaw affects a broad range of devices, it's unclear how quickly vendors will come up with a fix. The technical paper [15] describes the vulnerabilities of the ZigBee protocol, implemented on Amtel chip. It allowed researchers to develop a worm that penetrates a network of smart devices remotely, quickly infecting nearby devices and spreading across the network like a nuclear chain reaction.

Studies of the Bluetooth protocol also show a lack of security [16, 17]. Currently, more than 8 billion devices use this protocol around the world. Vulnerabilities affect a wide range of devices and are found in protocol implementations on Android, iOS, Windows and Linux. The vulnerabilities can be removed for relatively new devices by installing patches. However, there are more than 2 billion obsolete devices that are no longer supported by manufacturers, and for which patches are not available.

The WiFi Protected Access (WPA) protocol was introduced by the WiFi Alliance in 2003 to provide secure wireless data exchange in networks. The improved version (WPA2) became available in 2004. The protocol is widely used in networks for communication with smart devices. A recent study of this protocol [18] showed serious weaknesses, which allow attackers, by intercepting and decrypting traffic, to gain access to encrypted information such as credit card numbers, passwords, e-mails, etc.

It is quite easy to locate vulnerable devices and hack them by using search engines like Shodan [19] and Censys [20]. These find, for example, vulnerable webcams and access images of places that they control (private rooms, banks, schools, roads, etc.).

This situation significantly increases the number of cases of illegal penetration into private life, into individual firms and organizations.

Furthermore, a huge number of vulnerable devices, largely smart devices, creates new opportunities for cybercriminals: easy detection of vulnerable devices by scanning the Internet allows criminals to organize a large scale infection of the devices and to use them as an army of robots for criminal purposes. As a result: tens of millions of the smart devices can be organized in a powerful botnets (a combination of the words "robot" and "network") to send many millions of malicious requests to their targets.

For example, the malware Mirai, a self-propagating botnet virus, which first appeared in August 2016, is able to compromise smart devices running Linux and combine them into a powerful Mirai botnet. The Mirai-based botnets were used by cybercriminals to organize the most powerful DDoS attacks. Victims were the journalist Brian Krebs's website [21], the French cloud computing company OVN [22], a DNS provider Dyn [23].

During the attack on Dyn servers more than 70 services in USA were blocked during the period from 7 a.m. till 6 p.m. on October 21, 2016, including BBC, CNN, Fox News, PayPal and

VISA. Malicious requests from tens of millions of IP addresses created a total flow of about 1.2 TB / sec, which completely blocked the Dyn Domain Name System Infrastructure.

The lack of attention to the security of smart devices, when their number is rapidly increasing, further increases the risks of using these devices for criminal purposes. The scale of the attacks goes to a completely new level and threatens not only individual organizations, but also vital infrastructure of the state: energy, transportation, informatization, etc.

The lack of security of smart devices is due to a number of reasons: the lack of standards or mandatory official recommendations for the security of the Internet of Things, the huge variety of devices; the lack of legislative acts regulating responsibility between the manufacturer, the seller and the client; to reduce their costs manufacturers save on security. For most users, low cost is more important than security; users do not consider themselves to be a serious target for intruders and do not even care about recommended security measures (strong passwords, patch updates, certified downloads).

6. Conclusion

The growing influence of the Internet of Things on the personal and social life of people, on state activities and interstate relations is obvious. The Internet of Things is an integral element of the new industrial revolution (Industry 4.0) - a new stage in the development of human society [24]. Comprehensive measures should be taken to increase the security of smart devices at all stages, from the manufacture of chips, the design of hardware, the development of core and communication software, the development of applications. Standards and recommendations in this area should be developed at the international level. It is necessary to ensure that the manufacturers of smart devices have a legal responsibility for the security of information in their devices. It is necessary to increase the knowledge of users of smart devices about the security, or lack of it, of the information produced and transmitted by their devices.

References

[1] Arik Gabbal. Kevin Ashton Describes "the Internet Things". Smithsonian Magazine (January 2015). Available at: http://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

[2] IHS TECHNOLOGY. IoT platforms: enabling the Internet of Things. (March 2016). Available at: https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

[3] Edward C. Baig. Mattel's Aristotle is like an Amazon Echo for kids. USA Today. (January 3, 2017). Available at: https://www.usatoday.com/story/tech/columnist/baig/2017/01/03/mattel-brings-artificial-intelligence-and-internet-things-into-kids-rooms/96081330/

[4] Jon Fingas. Smart home gadget ends a violent dispute by calling police (July 9, 2017). Available at: https://www.engadget.com/2017/07/09/google-home-calls-police-on-violent-dispute/

[5] Zion Market Research. Global Smart Home Market is Set for a Rapid Growth and is Expected to Reach around USD 53.45 Billion by 2022. (January 18, 2017). Available at: https://www.zionmarketresearch.com/news/smart-home-market

[6] Tractica Market Research. Wearable Device Shipments to Reach 187 Million Units Annually by 2020. (February 19, 2015). Available at: https://www.tractica.com/newsroom/press-releases/wearable-device-shipments-to-reach-197-million-units-annually-by-2020/

[7] Robert S. H. Istepanian, Bryan Woodward. m-Health: Fundamentals and Applications. (January, 2017). ISBN: 978-1-118-49698-5. Wiley-IEEE Press.

[8] Sam Wong. Graphene smart patch for monitoring diabetes could save lives. New Sientist. (March 22, 2016). Available at: https://www.newscientist.com/article/mg22930661-900-smart-patch-for-diabetes/

[9] The Industrial Internet of Things (IIoT): the business guide to Industrial IoT. I-SCOOP. Available at: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/
[10] Aisha Bin Bishr. How digital technology is transforming Dubai. World Economic Forum. (May 16, 2017). Available at: https://www.weforum.org/agenda/2017/05/how-digital-technology-is-transforming-dubai
[11] Juan Pedro Tomas. China Unicom partners with Shanghai on smart city initiative. RCR Wireless News. (May 13, 2016). Available at: https://www.rcrwireless.com/20160513/asia-pacific/china-unicom-partners-shanghai-smart-city-initiative-tag23
[12] Lucas Laursen. Barcelona's Smart City Ecosystem. MIT Technology Review. (November 18, 2014). Available at: https://www.technologyreview.com/s/532511/barcelonas-smart-city-ecosystem/
[13] Smart Agriculture project in Salerno (Italy)... Libelium Word. (October 24, 2017). Available at: http://www.libelium.com/smart-agriculture-project-in-salerno-italy-to-monitor-baby-leaves-fourth-generation-vegetables-production-for-an-efficient-use-of-fertilizers-and-irrigation/
[14] Elyse Betters and Chris Hall. What is ZigBee and why is it important for your smart home?. Pocket-lint. (September 27, 2017). Available at: http://www.pocket-lint.com/news/129857-what-is-zigbee-and-why-is-it-important-for-your-smart-home
[14] Eyal Ronen, Colin O'Flynn, Adi Shamir, Achi-Or Weingarten. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. Pocket-lint. (September 27, 2017). Available athttp://iotworm.eyalro.net/iotworm.pdf
[15] Luca Carettoni, Claudio Merloni, Stefano Zanero. Studying Bluetooth Malware Propagation: The BlueBag Project. IEEE Security & Privacy (Vol. 5, Issue2, March-April 2007). ISSN: 1540-7993.
[16] Praveen Kumar Mishra. Bluetooth Security Threats. Int. Journal of Computer Science & Engineering Technology. (Vol. 4, No. 02, February 2013). ISSN: 2229-3345.
Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.478.651&rep=rep1&type=pdf
[17] Ben Seri, Gregory Vishnepolsky. BlueBorn Technical White Paper. (2017). ARMIS.
Available at: http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper-1.pdf?t=1510760820326
[18] Mathy Vanhoev, Frank Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. ACM Conference on Computer and Communication Security (CCS 2017).
Available at: https://papers.mathyvanhoef.com/ccs2017.pdf
[19] J.M.Porup. "Internet of Things" security is hilariously broken and getting worse. Arstechnica. (January 23, 2016). Available at: https://arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/
[20] Pierluigi Paganini. Censys, the new search engine for the Internet's secrets. Security Affairs. (December 11, 2015). Available at: http://securityaffairs.co/wordpress/42725/hacking/censys-search-engine.html
[21] Brian Krebs. KrebsOnSecurity Hit With Record DDoS. KrebsOnSecurity. (September 16, 2016, updated September 22 2016). Available at: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[22] Dan Goodin. Record-breaking DDoS reportedly delivered by >145k hacked cameras. Arstechnica. (September 29, 2016). Available at: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/
[23] Lily Hay Newman. What We Know About Friday's Massive East Coast Internet Outage. WIRED. (October 21, 2016). Available at: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
[24] Industry 4.0: the fourth industrial revolution – guide to Industrie 4.0. I-SCOOP. Available at: https://www.i-scoop.eu/industry-4-0/