ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 72
IV International Research Conference "Information Technologies in Science, Management, Social Sphere and Medicine" (ITSMSSM 2017)

Analysis of the vulnerabilities of the embedded information systems of IoT-devices through the honeypot network implementation

Anastasia Iskhakova
Faculty of Security
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
shumskaya.ao@gmail.com

Roman Meshcheryakov
Faculty of Security
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
mrv@security.tomsk.ru

Andrey Iskhakov
Faculty of Security
Tomsk State University of Control Systems and Radioelectronics
Tomsk, Russia
iskhakovandrey@gmail.com

Sergey Timchenko
Faculty of Physics and Engineering
Tomsk State University
Tomsk, Russia
tsv@ftf.tsu.ru

***Abstract*— The Internet of Things is now an essential tool in many areas of human life. Researches related to the security of IoT-devices and IoT-networks are extremely relevant over the past ten years. The violation of the confidentiality, integrity of the transmitted data and the availability of smart objects and control devices can lead to major risks and various negative consequences. The article details the conduct of the research experiment on the introduction of a honeypot trap into a smart house IoT-network. The results allow to make a conclusion about the ways of attacks on smart objects, the protocols and services use, the influence of the devices placement in the network on their security level.**

Keywords*— *Internet of Things; IoT-device; smart device; information security; honeypot, IoT-network; attack; trap; unauthorized access

I. INTRODUCTION

According to studies of Cisco [1] the transition to the Internet of Things (IoT) occurred around 2008-2009. Since that time the number of internet-devices (connected to the global Internet) has exceeded the population of the Earth. The number of innovations in this area is constantly growing, which indicates the active development of the Internet of things and relevance of solving the problems associated with the IoT-technologies.

Internet things can form local networks that are united by someone service area or by one function of the action. For example a smart house network consisting of the different sensors can have Internet access and be managed via the web interface. At the same time several smart networks can be integrated into one interconnected network for monitoring and managing the firefighting system of the city. City networks can be integrated by a global Internet network to share information about the fire safety level in any city in the country. This example is a particular case of geographically distributed networks. Their development was promoted by active innovative activity in the field of wireless sensor networks over the last 10 years.

According to [2] in May 2017 the collection of Kaspersky Lab contained more than 7 000 different samples of malicious software for smart devices, and about half of them were added in 2017. Doubtlessly it's needed a comprehensive protection strategy to provide the appropriate level of security for the IoT infrastructure [3]. It should ensure the data protection in the cloud, the data integrity protection while transmitting to the Internet and also safety of the devices manufacture. The direction associated with ensuring the security of IoT-devices is extremely urgent and necessitates the development of new methods and ways of counteraction the malefactors that attack IoT systems[4].

The purpose of this study is to increase the knowledge about the attacks sources and the ways for the unauthorized access to the IoT devices. For more detailed coverage of this subject and for the achievement of this goal several smart devices was experimentally used as honeypot objects [5, 6].

II. USING HONEYPOT IN THE INFORMATION SECURITY

Nowadays people have trusted smart devices with important areas of their lives. We hope that all the IoT-components that we set up and transfer control of our comfort work correctly, are managed only legally and do no harm. As the number of smart devices used by ordinary consumers and commercial companies grow, so will the number of new threats. This is the trend of the development of such systems and the development of computer attacks [7].

To ensure the security of smart objects and configure security settings various methods and tools of computer security are used [8, 9]. One of them is the use of the honeypot trap. The task of honeypot is to be attacked by a hacker, to accept an attack, to be hacked. Organizing honeypot in the network researcher can get information about the beginning, the process and the result of attack and hacking. There are many variations of use this tool of finding out the tactics of an attacker [10]. Regardless of the honeypot trap configuration, its main tasks are to undergo an attack and to pass on details of the committed attack or attempted attack to the owner.

In addition, the trap can be additionally configured to notify the owner of the attack beginning, to collect service or critical information, and so on. The created honeypot usually does not perform any actions for its intended purpose. Any interaction with it from outside means the attack is started.

*The work was partially funded by the Russian Federation Ministry of Education and Science (grant 2.3583.2017/4.6) and the Russian Foundation of Basic Research (grant 16-47-700350 r_a).

This tool enables the researcher to obtain the necessary information, collect statistics on security violations in the monitored network. Despite this, creating honeypot researcher should remember that this is a "window" in his system for an attacker, so it is necessary to consider the basics of computer security as well as professional vigilance in conducting experiments using honeypot traps [11].

III. THE EXPERIMENT SCHEME AND ITS PROGRESS

The task for each of the intruded honeypot objects is to be attacked and undergo an unauthorized investigation and a search for the vulnerabilities. This will subsequently allow researchers to study the attacker's strategy and determine the list of ways to attack the resources.

To implement honeypot was used 9 devices used in the Smart Home systems:

- network video recorder (NVR);
- IP cameras;
- IP door phone,
- TV set-top box (STB);
- such smart devices with the ability to access the Internet as an air-conditioning control system, a kettle, a refrigerator and a smart lighting lamp.

Before the experiment start all devices were updated with the latest software versions. To obtain more complete information about the intruders' tactics it was decided to implement two different versions of the placement of the honeypots: 4 devices (further united in the 1st class) were placed in the demilitarized zone (DMZ) [12]. To simulate the most realistic picture of the location and make the access more complicated for the attacker 5 devices were installed inside the local network (the 2nd class). Access to the devices over the Internet was possible through several open ports using the Port Forwarding technology configured on the edge router. At the same time for the greater complexity of the vulnerabilities exploiting, the standard values of the "proxy ports", responsible for the certain services, have been changed.

On the network video recorder and two IP-cameras were saved the user name and password values set by the manufacturer by default:

- "root" / "pass" (device of the 1st class);
- "ubnt" / "ubnt" (device of the 2nd class);
- "admin" / "4321" (device of 1st class).

In the others devices were installed the passwords that satisfy the following criterion of complexity: at least 7 characters, the use of different registers, at least 1 special symbol, at least 1 digit.

The diagram of the constructed trap-network is shown in the figure 1. Among its components are a switch, a gateway, an analytics server, an intrusion detection system - ViPNet IDS hardware and software complex and smart devices divided into a 2-class location, as described above. There are used also port forwarding and port mirroring technologies to track the interactions from outside.

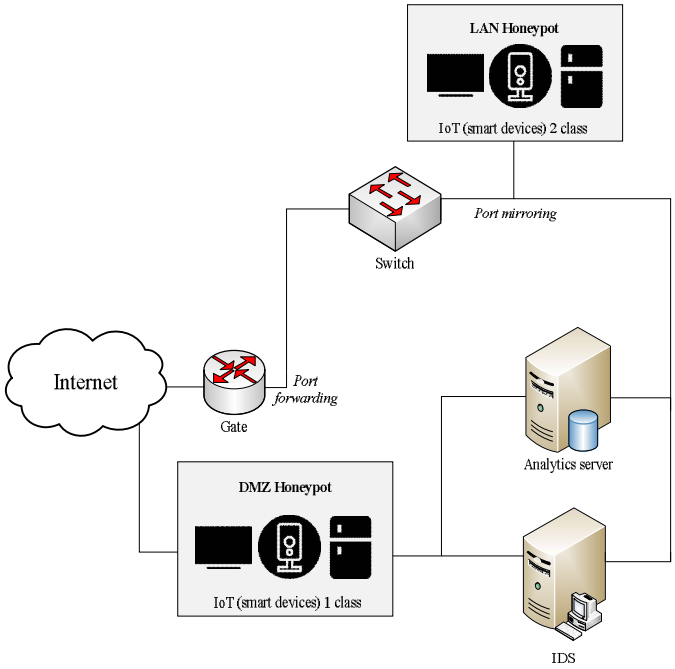

Fig. 1. The schema of a built-up trap network consist of IoT-devices

As follows from the above-stated figure all traffic coming on the smart-devices is duplicated on the server of analytics and the intrusion detection system through the Port-mirroring technology. The hardware-software system ViPNet IDS was selected as the main automation equipment of potential attacks detection [13]. Functioning of this complex is built on the basis of dynamic analysis of network traffic [14], from the data link layer to the application layer of open system interconnection model (OSI model) [15]. As the second tool for carrying out the experiment was selected the analyzer of protocols Wireshark [16] executing the capture of traffic on in advance set up filters and allowing to carry out a "manual" analysis of a set of potentially dangerous requests.

The intrusion detection system fixed the date and time of the events, the type of interaction (the rule that worked), the severity of the action threat, the port that was involved, the used network protocol, the IP address of the device that undergoes the attack, the IP address of the attacking object (the source of the threat). So the honeypot trap provided the detailed report on all connections and interactions to the devices, received requests and the results of the attacker's actions.

The first attempts of connection to open SSH and Telnet-ports were fixed within several minutes after start of devices working. There were registered more than two thousand requests from several hundred unique IP-addresses per day. In a Fig. 2 the interface of the invasions detection system which fixed attempts of an unauthorized research of the placed traps is shown.

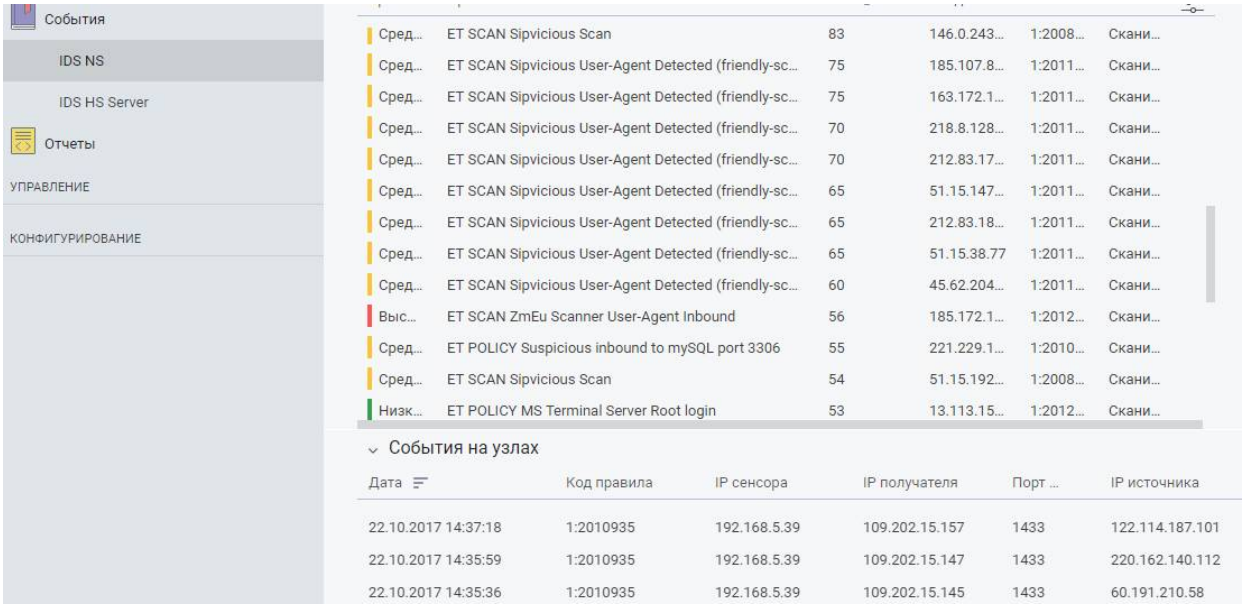

Fig. 2. Monitoring of the attempts to gain unauthorized access to IoT devices

IV. RESULTS FO THE EXPERIMENT

The monitoring period was 3 months. The total of authorization attempts on 9 devices was 520 479, 515 057 of them are unsuccessful attempts and 5 422 - successful ones. At the same time, all fixed facts of unauthorized successful authorization belong to all elements of the 1st class: 2 devices containing standard couples of login/password from the manufacturer and 2 devices with changed password. The analysis of the inquiries which have arrived for this period allows to say that about 80% of connections are carried out on standard ports of the following services: SSH, Telnet, HTTP, FTP, SMB. In case of devices of the 2nd class it should be noted that despite numerous authorization attempts, hasn't been fixed by the analytics systems any successful fact of an unauthorized entrance.

In the Fig. 3 the consolidated diagram of unauthorized requests to smart-devices is provided.

The majority of IP-addresses, from which connection attempts have been fixed on smart-traps, successfully responded to icmp-inquiries. Identification of categories of the attacking devices was carried out by the following methods:

- analysis of network packages headings of the attacking devices;
- check of results of the response to HTTP-inquiries. Often in response to "counter" inquiry the control panel of the device (video recorder, IP-camera or router) opened. It is obvious that by drawing up statistics can't be believed unambiguously that always to HTTP-inquiry responds device which carried out the attack to honeypot. In many cases it is possible to speak about use of the NAT technology [17] at which behind one "external" IP-address there are several attacking devices.

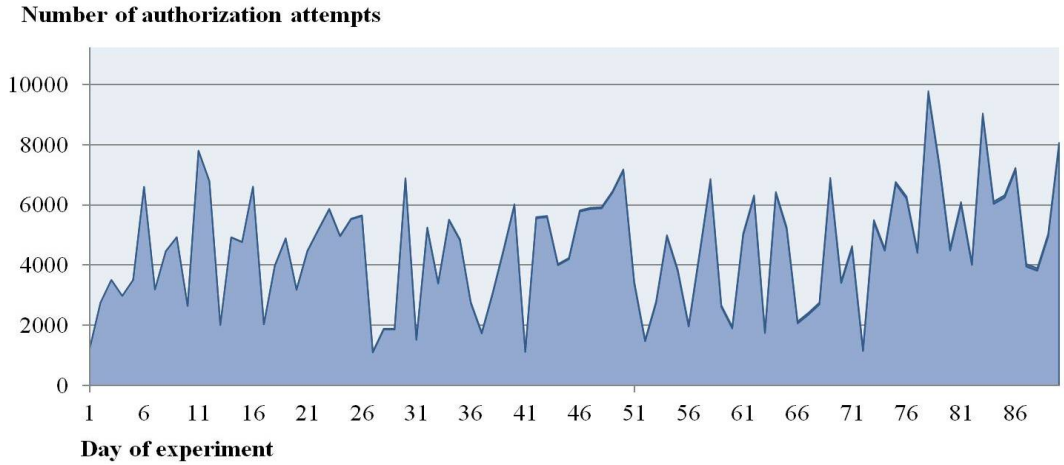

Fig. 3. Attempts of unauthorized gaining of access to IoT-devices

Considering complexity of reliable identification of attacks sources it is possible to give only approximate statistics of devices generating inquiries of passwords selection and trying to use modern vulnerabilities. So, more than 45% of unique IP-addresses of sources can be defined how NVR-services or IP-cameras. More than 20% of devices belong to the class of routers and other network equipment. Other 15% are servers (including the home media-centers and Set-top boxes) and workstations of users. The category of last 20% unambiguously didn't manage to be identified (fig. 4).

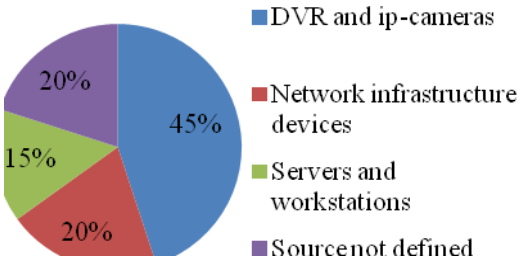

Fig. 4. Traffic sources on the honeypots presented in the form of IoT-devices

It is remarkable that the majority of the devices which were carrying out the attacks to the formed honeypot trap are Iot devices that represent the bot-networks, which united in themselves elements of infrastructure of the Internet of things. In three months of researches it hasn't been fixed any attempt of receiving the RTSP URI stream [18] from cameras. And identification of camera model in the provided trap, and process of obtaining of the RTSP-reference on the manufacturer website didn't represent a labor-consuming task. It once again confirms lack of human activity in the revealed attempts of unauthorized gaining of access.

There are objective explanations to it. The high efficiency of the existing systems and means of counteraction to the DDoS-attacks make malefactors search the new resources which would help them to arrange more and more powerful attacks. Confirmation to that is the bot-network Mirai [19] consisting of hundreds thousands of compromised IoT-devices. In 2016 this network carried out the DDoS-attacks, which cumulative traffic at peak reached about 665 Gb / sec. At the same time this network creation has become possible because of vulnerability of standard logins-passwords from manufacturers by the brute force method according to the dictionary consisting from only 61 combinations.

V. Conclusion

The number of smart-devices constituting infrastructure of the Internet of things is calculated by billions today. Analysts of different companies predict its growth ranging from 20 up to 50 billion. The practical experiment made by authors allows to be convinced that already today a huge number of IoT-infrastructure representatives can be operated by unknown malefactors by means of a pool of command servers. Most of people, acquiring IoT-devices and connecting them into a wide area network without switching on of basic mechanisms of safety, do not think about quite probable negative consequences.

IoT-devices safety is at quite low level often. This is result from the fact that manufacturers are not interested in implementation of additional measures of information security. They advertise the simplicity of production use, but all additional measures of information security impose restrictions and require expenses of resources. This research showed that the minimum actions such as placement of smart-devices abroad of a fire-wall, change of standard passwords and network ports of access allows to be protected from influences a bot-networks.

The experimental attacks to a smart lighting lamp and IP-video cameras can seem innocent while we do not realize that around us the smart cities actively develop. Large settlements worldwide can be completely connected to a network in several years. If devices and systems of the Internet of things do not receive due protection, malefactors will be able to receive over them monitoring and control and to cause chaos in the cities, controlling the lighting systems, traffic flows and other information systems of the vital infrastructure.

References

[1] D. Evans, “The Internet of Things. How the Next Evolution of the Internet is Changing Everything” [Electronic resource]. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (access date: 28.09.2017).

[2] V. Kuskov, M. Kusin, D. Makrushin, Ya. Shmelev and I. Grachev, “The traps of the Internet of Things. Analysis of data collected on IoT-traps of Kaspersky Lab” [Electronic resource]. URL: https://securelist.ru/honeypots-and-the-internet-of-things/30874/ (access date: 14.10.2017).

[3] K. Zhao and L. Ge “A Survey on the Internet of Things Security”, 2013 Ninth International Conference on Computational Intelligence and Security, 2013, pp. 663 – 667.

[4] K. Gupta and S. Shukla, “Internet of Things: Security challenges for next generation networks”, 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016, pp. 315 - 318.

[5] M. Anirudh, S A. Thileeban and D. Nallathambi, “Use of honeypots for mitigating DoS attacks targeted on IoT networks”, 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), 2017, pp. 1 – 4.

[6] A. Tarasenko, The honeypot technology. Part 1: The purpose of the honeypot [Electronic resource]. URL: http://www.securitylab.ru/analytics/275420.php (access date: 10.10.2017).

[7] A. Prokofiev; Y. Smirnova and D. Silnov, “Examination of cybercriminal behaviour while interacting with the RTSP-Server”, 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 2017, pp. 1 - 4.

[8] S. Iskhakov, A. Shelupanov and R. Meshcheryakov, “Assessment of security systems complex networks security“, Dynamics of Systems, Mechanisms and Machines (Dynamics): Proceeding of the International Scientific and Technical Conference, 2014, pp. 1–4.

[9] O. Evsutin, A. Kokurina, R. Meshcheryakov, O. Shumskaya, “An adaptive algorithm for the steganographic embedding information into the discrete fourier transform phase spectrum”, Advances in Intelligent Systems and Computing, 2016.

[10] Q. La, T. Quek and J. Lee, “A game theoretic model for enabling honeypots in IoT networks”, 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1 - 6.

[11] S. Dowling; M. Schukat and H. Melvin, “Data-centric framework for adaptive smart city honeynets”, 2017 Smart City Symposium Prague (SCSP), 2017, pp. 1 – 7.

[12] M. Rouse, DMZ (demilitarized zone) [Electronic resource]. URL: http://searchsecurity.techtarget.com/definition/DMZ (access date: 10.10.2017).

[13] Infotecs, ViPNet IDS [Electronic resource]. URL: https://infotecs.ru/product/setevye-komponenty/vipnet-ids/ (access date: 10.10.2017).

[14] S. Iskhakov, A. Shelupanov, R. Meshcheryakov, "Simulation modelling as a tool to diagnose the complex networks of security systems", Journal of Physics: Conference Series, 2017.

[15] A. K. Maini and V. Agrawal, Networking Concepts, 2014, P. 848.

[16] R. Das and G. Tuna "Packet tracing and analysis of network cameras with Wireshark", 2017 5th International Symposium on Digital Forensic and Security (ISDFS), 2017, pp. 1 - 6.

[17] S. Ganguly and S. Bhatnagar, "Network Address Translation (NAT) and Firewall", VoIP:Wireless, P2P and New Enterprise Voice over IP, 2008, P. 276.

[18] H. Schulzrinne, A. Rao and R. Lanphier, Real Time Streaming Protocol (RTSP) [Electronic resource]. URL: https://www.ietf.org/rfc/rfc2326.txt (access date: 19.10.2017).

[19] B. Krebs, Did the Mirai Botnet Really Take Liberia Offline? [Electronic resource]. URL: https://krebsonsecurity.com/tag/mirai-botnet/ (access date: 19.10.2017).