Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 169 (2020) 179–182

Procedia Computer Science

www.elsevier.com/locate/procedia

Postproceedings of the 10th Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence, BICA*AI 2019 (Tenth Annual Meeting of the BICA Society)

Information security of Internet things

Dmitry Bagay*

National Research Nuclear University MEPhI, 115409, Russia, Moscow, Kashirskoe shosse, 31, web-domen150796@yandex.ru

Abstract

The development of methods of information protection against cyber threats is a priority and the most labor-intensive direction in the development of the IoT sector. The relevance of the topic is growing due to the growing user interest in the Internet of things. Basic for studying in this work was the traditional IoT architecture format, which consists of three "slices". This perception, network and application levels. Each "cut" characterizes its key problems in the field of information security. The most difficult part is the network layer. The arising difficulties are provoked by the features of the structure (multivariance of things, different methods of networks) and a high numerical index of objects. The Internet of things accumulates information data from a huge number of devices that have different formats and various characteristics. As a result, there are failures of DoS, which arise due to a heavy load on the network, as well as disruptions in the operation of programs.

Keywords: Information security, Internet of things, IoT, DDoS-attacks, Smart house, Cyberthreats, Security at the network level, Application-level security, Vulnerability of software

1. Main text

* Dmitry Bagay. Tel.: +7-495-788-56-99
E-mail address: web-domen150796@yandex.ru

10.1016/j.procs.2020.02.132

The development of The IOT concept is associated with the large-scale introduction of wireless technologies, machine-to-machine integration and the transition to cloud computing and IPv6 over the past two to three years. The popularity of the Internet of things is explained by a unique feature of the revolutionary technology: it has the ability to unite a person and a "thing" in any time period and in different locations thanks to a variety of communication networks. In official documents the term "thing" is usually replaced with terms such as node, object, or device. The main components of the Internet of things are USN sensor networks and RFID radio frequency identifier. The thing in the USN means of a single sensor or system of sensors and RFID special label or tag. Protocol IPv.6 – 6LoWPAN – base network-based USN. According to experts, in two years the number of devices connected to the Internet will reach 50-100 billion units. Today, many devices connected via the Internet can operate completely independently, without the presence of a person. A good example is various modern systems and complexes: control systems, lighting control systems, automatic irrigation systems, traffic lights, fire and security alarm sensors, etc. The Key problem of the development of the Internet of things remains information security in this area.

The multi-stage system of the Internet of things is defined by three main characteristics:

- generalized information data (complex information about the object obtained in any time period and in any location);
- reliable transmission (through routing, communication protocols, encryption and coding, network security);
- intelligent processing of the received data (thanks to various calculations, methods and technologies of analysis and processing of Big Data data and obtaining the necessary information from users).

According to these characteristics, the structure of the Internet of things is divided into three levels: network level, application level and perception level. The main purpose of the perception level is to obtain reliable reading from sensors and RFID tags.

The network layer provides ubiquitous access, data transfer, processing and storage of information. It consists of two levels – the access level (mobile networks) and the main exchange level (Internet, next/new generation NGN networks and other private networks). Virtually all sensor networks use wireless technologies: WPAN (wireless private networks), WLAN (wireless local area networks), WMAN (wireless urban networks), WWAN (wireless global networks) and satellite networks. These network formats use IP-based communication protocols.

The application layer processes and analyzes the information to make the right decision, and performs control functions in applications and services. The application layer accumulates and processes the received information data, ensure the efficiency and continuity of energy supply systems, logistics etc. Under the information security at the level of perception means any physical device security perceptions and the security of the information-gathering process. Most of the perception devices that are deployed in a maintenance-free environment in the absence of common rules and standards are distinguished by their technical simplicity, weak power supply and protective mechanism.

Due to the above information, the Internet of things cannot provide a single standardized system of information security protection, and resist various attacks, unauthorized access and external cyber threats. The problems of information security at the level of perception are particularly relevant, since the wireless sensor network at this level is a source of information. They are divided into the following categories: physical capture of sensor nodes, leak sensor, capture the gateway node, DoS attack, threat of integrity of data, depletion of energy source, the threat of overload, the threat of the site was copied and threats of route establishment in a network of illegitimate sensors.

Threats to the information security of existing communication networks extend to the Internet of things, which is based on them. This is directly related to unauthorized access, information interception, privacy, integrity, DOS attacks, exploits, viruses, network worms, etc. In addition, there are inter-network authentication issues that can be the cause of DOS attacks.

Ensuring the information security of the Internet of things goes to a fundamentally new level. It is provoked by two factors-heterogeneity of structure (variety of things, different technologies of networks) and increase in number of devices. The Internet of things collects huge amounts of information from different devices and processes data of different formats that come from sources with heterogeneous characteristics. As a result, problems arise at the network level that are particularly difficult to solve. These include network scalability problems caused by the low-predictable volume of data transfer from a large number of nodes, and leading to the possibility of DoS and DDoS attacks.

Particular attention is paid to the vulnerabilities of software that can disrupt the operation of information security systems after implementation.

Key causes of vulnerability: errors in the core of the program, mistakes when creating complex multi-level software, the use of unprotected code, incomplete exception handling, the use of raw arrays with the possibility of their overrun by criminals, mistakes in processing Big Data, database errors, lack of consolidation of database queries, lack of scalability or performance of software, web vulnerabilities, errors in distributed applications, cloud and virtual platforms. In addition, individual errors in the Internet of things appear due to the variety of platforms and operating systems. When designing and creating software, it is important to emulate the behavioral responses of IOT devices, that is, it is necessary to design a multifunctional simulator of the external environment. Due to technical limitations in devices (processor performance, memory, power supply), IoT faces the most difficult task – to ensure that the differences between the device and the simulator are minimal. In addition, for the release of a debugged working application, it is necessary to conduct its full testing, including comprehensive testing of the interaction of all modules, load testing and performance testing.

Another reason for the vulnerability of the software can be backdoors – backdoor) - parts of the code that were prescribed by the developer for further use when viewing data, or to control the computer from a remote point (in the case of the OS). The backdoor can be random errors in the program code, which at a certain combination of keys or selection of constants, or other actions in the application are able to provide access to data. Manufacturers also install them on their equipment to be able to test and control the device. The danger is that cybercriminals, thanks to backdoors, can take advantage of this "back door" and carry out unauthorized access.

The urgency of the problem of information security of the Internet of things is emphasized by the attack on the provider Dynamic Network Services (DYN). In October 2016, the largest Internet portals experienced unprecedented scale DDoS attacks. Malicious traffic came to the servers of these sites are no longer infected with malware computers, and ordinary household appliances that have access to the Internet: TVs, refrigerators, toasters and video cameras. Hacking any of these devices is very simple: the devices use simple factory passwords that users do not change at the beginning of operation. The attackers, using a botnet consisting of 130,000 devices, were able to cause large-scale failures in the work of Internet portals, sending a large amount of" garbage " traffic to the DNS server owned by DYN.

Mirai is a hacker-created program that hacks Internet-connected devices and uses them to organize DDoS attacks.

From one point of view, the program first infects the home PC using e-mail viruses, and then all other devices that are connected to the PC: router, printer, set-top box and so on. If we consider a corporate network, Mirai can capture even IP cameras that are used for video surveillance.

From another point of view, the program constantly scans the Internet, searches for IOT devices connected to it and infects them using standard, factory-installed login and password combinations. As long as the device does not reboot – it remains infected. If the default password is not changed after reboot, the device is infected again.

Receiving access control devices, Mirai turns them into a botnet. In most cases, the program is focused on devices created on the basis of Busybox – a shortened set of UNIX command-line utilities, which is used as the main interface for embedded OS. The malware targets only certain platforms: x86, SH4, SPARC, MIPS, PPC, ARM, ARM7. The infection is caused by a brute force attack on the Telnet port for which the default administrator credentials are set.

According to confirmed data with the help of malware Mirai hackers tried to completely disconnect from the Internet Liberia. In addition, the program was used to organize DDoS attacks during the us election, DDoS attacks on Brian Krebs, DDoS attacks on the Internet provider DYN.

Overall, the IP addresses of Mirai-infected devices have been seen in 164 countries. As can be seen from the map below, the Mirai botnet is highly dispersed, appearing even in such remote places as Montenegro, Tajikistan and Somalia.

According to the source code of a botnet, Mirai consists of the following components:

- command center (C&C), which contains a MySQL-database of all infected IoT devices (bots) and carries out the distribution of teams to the intermediate distribution servers teams;
- component receiving results of the scanning bots (Scan, Receiver), whose task is to collect results from bots and their subsequent redirection component, download the bot on the affected device (Distributor);
- component loading, which delivers the binary of the bot on the affected device (it uses the 'wget' utility and tftp, but if they do not exist in the operating system, the component uses its own boot loader);
- bot, which after running on the infected device connects to the command center scans a range of IP addresses (SYN-scan) on the subject of vulnerable IoT devices and sends the results of the scanning component Scan Receiver to load malicious code on the device.

Besides, Mirai is able to run GRE IP ETH GRE, SYN, ACK, STOMP threads, and the threads on DNS.

The infection is quite simple: the Internet is scanned on open 80/23 (web/telnet) ports and accounts are selected.

The source code of Mirai malware, with which you can create such a botnet, is freely distributed on the Internet, it can be downloaded and used by anyone who has enough knowledge and experience to configure a malicious attack. Often, devices connected to the Internet have factory passwords that users do not change. In addition, determining that your TV, router or printer with Internet access is used in a botnet is quite problematic for most users. However, you can hack such a device without much effort – the program goes through 60 standard combinations (login / password), which are used by manufacturers, and gets access to the device.

The total number of jailbroken devices, most of which are video camera, at the peak of the attack was about 490 thousand Power of a DDoS attack from a botnet Mirai in peak times reached 1 TB/sec. Due to the use of this botnet to attack the dyn provider, access difficulties have been noted by giants such as Spotify, Soundcloud, GitHub and even Twitter.

The botnet simultaneously sends a huge number of requests to DYN-owned servers. At first glance, these requests are indistinguishable from legitimate, because of this system provider DYN was not able to identify them among the many normal, user requests.

If earlier it did not make sense for an attacker to use such devices, because their bandwidth was low, now everything is different. Cybercriminals began to use the technique of amplification attacks via DNS. In particular, when an attacker sends 12-byte packets in the amount of 20 pieces to the server, then to the attacked server comes already 100 packets of 100 kilobytes each. In other words, a huge set of routers, the individual capabilities of each of which are small, the attackers rallied, turning into a tool for DDoS attacks. In the near future, there will be more and more potentially interesting products and services of the Internet of things for such attacks.

The power of DDoS attacks is constantly increasing. First, the attack on the site of Brian Krebs (612 GB / sec), followed by OHY and finally provider DYN (1.2 TB/sec). This involves a huge number of devices from the Internet of things that have access to the Internet.

A huge number of illegitimate requests are sent to a specific server or set of servers, after which they are unable to process incoming requests and become unavailable.

Another relevant example is the attacks on the industrial Internet of things (M2M). These devices also attack, but the bulk of such cases remain in the shadows. Only a small number of precedents, in particular the Stuxnet attack, become public.

The development of the Internet of things is the final process of mass integration of computer technologies, communication technologies and various sectors of the industrial industry. In addition to threats from traditional communication networks (threats of information distortion, repetition, eavesdropping, disclosure), IOT applications face additional security problems at the application level: the use of cloud computing, intellectual property rights, data processing, protection of confidential information, etc.

References

[1] Alekseev V. Modules Bluetooth, Wi-Fi and NFC production u-blox connectBlue for the "Internet of things", part 1. Bluetooth-enabled modules // Wireless technologies. 2015. Vol.2. No. 39. P. 27 - 32.

[2] Perera, C. and etc. Context Aware Computing for The Internet of Things: A Survey. Communications Surveys & Tutorials, IEEE, 2014, V.16, Issue 1, P. 414-454.

[3] Goldstein B. S., Curly A. E. post-NGN Communication networks. SPb.: BHV-Petersburg, 2013, P. 160.

[4] Khan R. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, Frontiers of Information Technology (FIT) - 2012 10th International Conference on, 2012. - 257 – 260 p.

[5] Zhi-Kai Zhang. IoT Security: Ongoing Challenges and Research Opportunities, Service-Oriented Computing and Applications (SOCA) - 2014 IEEE 7th International Conference on, 2014. – 1-5 p.

[6] Zhi-Kai Zhang. Emerging Security Threats and Countermeasures in IoT - ASIA CCS '15 Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015. – 1-6 p.

[7] Nefedova M. UPD. DDoS attack on the DNS provider Dyn caused failures in the largest sites. // Hacker Magazine. No. 226, 2017 – 23 p.

[8] Baoquan Z., Zongfeng Z., Mingzheng L., Evaluation on security system of internet of things based on Fuzzy-AHP method, E -Business and E -Government (ICEE). - International Conference on 2011, 2011 – 1-5 p.