

Information Security of the Internet of Things

Anton D. Nazarov¹^a, Dmitriy M. Nazarov¹^b and Stefan Talu²^c

¹Ural State University of Economics, Yekaterinburg, Russia

²Technical University of Cluj-Napoca, Cluj-Napoca, Romania

Keywords: Internet of Things, Information Security, Vulnerability, Security Threats.

Abstract: At present, the impact of “computer-computer” interaction on functional reliability of the systems that ensure the well-being of society is of great theoretical and practical interest. There is the need for high-quality data protection of the Internet of Things in connection with the fastest-growing user demand for such the technology as the Internet of Things. The article discusses the most important issues related to information security of the IoT and indicates ways of addressing the needs identified.

1 INTRODUCTION

Global information networks are actively developing in a direction of ensuring communication of physical and virtual ICT-based objects in order to provide innovative services to society, for example, shopping (contactless payment), controlling a vehicle with smartphones, energy consumption (remote observation with sensors and video cameras) services. This phenomenon was called the Internet of Things (hereinafter referred to as IoT).

The key features of the Internet of Things are as follows.

1. Physical objects connected in a computer network can contact each other and with the outside world.

2. In the IoT network, computers, smartphones, various powerful computers and almost anything interact.

3. The Internet of Thing makes a person's life easier without interference in linked devices that control world around them through digital means (Evsutin, Kokurina, and Meshcheryakov, 2019; Hong et al., 2018).

4. The main task of the technology is to improve the quality of life by ensuring cohesion through artificial intelligence in the interaction of all members of society and the authorities.

2 PROSPECTS OF THE INTERNET OF THINGS

The network offers broad prospects in:

- the agricultural sector: the use of data on humidity, temperature of the fertile layer, and plant nutrition obtained from the sensors can help improve the soil quality;


- industry: reduction in the number of scheduled inspections of equipment with the use of sensor data (Castilho, 2017; Huang, 2011);


- packaging logistics: tracking a package allows to simplify its delivery from the manufacturer to the store or from the store to the buyer;


- the smart home construction: conserving water, electricity, gas resources by the smart meter installation; home safety management; functional programming according to the user's specific requirements;

- medicine: collecting and transmitting data to the IT database for subsequent analysis of devices; monitoring of the patient's condition, automated warning of changes; decreasing energy intensity of hospital-specific equipment, reducing the operating cost; health control through regular monitoring of physical condition data using wearable devices, “smart” clothes and shoes;

- trade: “spot” work with each “online” buyer when searching for the required product; analysis of

^a <https://orcid.org/0000-0002-8299-1834>

^b <https://orcid.org/0000-0002-5847-9718>

^c <https://orcid.org/0000-0003-1311-7657>

sales, automated price increase or decrease in order to ensure maximum sales volume and to prevent overproduction;

- forensics: supervision of offenders who are sentenced to house arrest with the use of biometric technology;

- environmental protection: monitoring animal populations by detecting them on the surface of the Earth by the radio signal emanating from an electronic device placed on an individual (Irshad, 2017);

- transport: it will be able to make an independent traffic situation assessment without a person, to plan and change the traffic pattern.

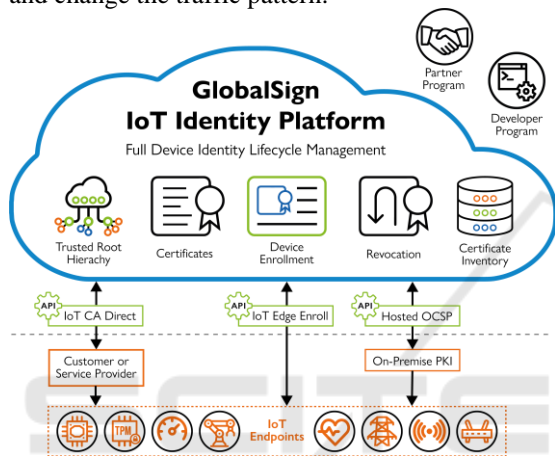


Figure 1. IoT identity device.

3 RESULTS AND DISCUSSION

Today, one of the main problems of the IoT is the Internet security of this network. The problem has the following factors: the rapidly changing situation in the industry; the desire of numerous individuals and organizations to gain influence on the network, to establish their own order and laws; unrealistic forecasts. Technical vulnerability which plays a special role includes not necessarily clear, or having a feedback active influence of the subject on the object; negative impact of a set of conditions posing a threat to information security; intentional and malicious acts aimed at violating availability, integrity, confidentiality of data.

A person or organization who have thought about committing illegal acts can take over the device, inject a malicious element, and change the program if they are aware of the problems and configuration flaws in the application or general control software of the system (Hong et al., 2018).

Natural threats, such as earthquakes, fires, floods, can cause “natural” harm to computer systems. It is better to use a backup to minimize their negative impact.

Enormous malicious damage to the IoT is possible from authorized and unauthorized people. They can be unskilled amateurs using readily available hacking tools, as well as dangerous hackers who are well aware of the system vulnerabilities, who predict its reaction to the specific codes and scripts. The new generation of Internet of Thing devices already have new built-in threats to information security that provide access to attacks from manufacturers.

Malicious acts aimed at violating availability, integrity, confidentiality of data often focus on the personal ambition of the hacker or obtaining rewards. Such actions can have different forms: an active network attack in order to detect the possibility of the Internet provider to obtain information on the sites and web applications used; passive network attacks in order to find information which can become the subject of theft; attacks from websites initiated by computers; the use of persons who have access to data not readily available to the general public.

The most common types of hacker attacks are:

A. Hardware failure. This malfunction is connected to the fact that most IoT devices for outdoor environments can easily be subject to negative physical effects.

B. Reconnaissance attacks for the illegal identification of vulnerabilities of systems and services.

C. Inaccessibility of a computer or network resource for users which is very difficult to recover due to low memory capacity, limited computing power.

D. Access to physical or IP connected device by unauthorized users for:

- interception, spoofing of messages while maintaining the anonymity of the hacker access to the channel for the information exchange by interlocutors;

- compromising the channel by violating the transfer protocol by misrepresentation or information changing;

- fraudulent use of access to the site received from a user who does not know the fundamentals of network security by fake login pages (Irshad, 2017).

E. Violation of privacy:

- data mining that allows to bring out the facts which are not subject to disclosure in databases;

- obtaining secret information about individuals or organizations by hacking, using malicious software;

- unauthorized telephone tapping;
- the UID tracking location and movements of users wishing to remain anonymous;
- password reuse attacks by guessing a combination of characters, checking all possible combinations using special tools.

F. Misuse of the network for material income generation by theft of intellectual property, personal data, and brand.

G. Attacks on the technology management, the operational status of the devices (denial of service which leads to the shutdown of the system); structure management using Trojans or other viruses.

4 CONCLUSION

Today, there is not a single secure Internet of Thing system in the world. The main reasons for this are the desire of the manufacturer to lower the cost of the product; lack of necessary standards and recommendations for ensuring the network information security; impossibility of authorization and authentication of many components used in the system into the global network (Huang, 2011).

Systematic and purposeful work is essential for creating the effective Internet of Things security, including:

- monitoring the vulnerability of devices during the production stage;
- the use of modern standards for the secure application development in creating software;
- creation of opportunities for software updates;
- minimizing the vulnerability of P-code (device independent code) through logistics management, ranging from the production stage to the stage of equipment installation at the facility;
- prevention of physical capture of structures that receive and process information of a certain type, and form sensations;
- improvement of the security protection of the sensor network perception node in an environment which is not served by people,
- prevention of sensor problems (seizure of a gateway node, information leakage, violation of data integrity, depletion of energy sources, overloads, denial of service, installation of illegitimate devices, unauthorized copying of a node);
- protection of communication networks from unauthorized access, interception of information, breach of confidentiality, viruses, network worms, the use of software vulnerabilities in order to attack a computer system, the use of a set of software tools to

conceal processes, files, drivers, as well as events occurring in the system and its parameters;

- exclusion of the authentication problem which can result in information attacks on the network;
- addressing the software vulnerabilities caused by developer-made errors and the program kernel, processing of incomplete exception types, use of code with weak protection, insufficient processing of arrays that can become full of hackers, errors in Big Data and database processing, improper indexing or incorrect database queries, violations in distributed operating applications, virtual platforms, clouds;
- creation of software simulations of the outdoor environment for servers;
- avoidance of significant discrepancies between the emulator and device at the stage of power supply, processor performance, memory;
- complex load, performance, interaction of modules testing;
- exclusion of access to data as a result of using a keyboard shortcuts or through certain actions.

The use of the Internet of Things in many areas is still significantly limited by information security problems. However, the thorough analysis of the situation, achievements in this field and the recommendations submitted by the specialists will help address these issues, promote further practice-based implementation of this technology.

REFERENCES

- Castilho, S. D., Godoy, E. P., Castilho, T. W. L., & Salmen, A. F. (2017). Proposed model to implement high-level information security in internet of things. *2nd International Conference on Fog and Mobile Edge Computing*, FMEC 2017, pages 165-170. doi:10.1109/FMEC.2017.7946425
- Evsutin, O. O., Kokurina, A. S., and Meshcheryakov, R. V. (2019). A review of methods of embedding information in digital objects for security in the internet of things. *Computer Optics*, 43(1): 137-154. doi:10.18287/2412-6179-2019-43-1-137-154
- Hong, S., Park, S., Park, L. W., Jeon, M., & Chang, H. (2018). An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on research trends in the security field in south korea. *Future Generation Computer Systems*, 82: 769-782. doi:10.1016/j.future.2017.10.019
- Huang, M. (2011). Research on information security evaluation of internet of things electronic commerce based on AHP. doi:10.4028/www.scientific.net/AMR.217-218.1355
- Irshad, M. (2017). A systematic review of information security frameworks in the internet of things (IoT). *Proceedings - 18th IEEE International Conference on*

- High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems*, HPCC/SmartCity/DSS 2016, pages 1270-1275. doi:10.1109/HPCC-SmartCity-DSS.2016.0180
- Lavrova, D. S. and Vasil'ev, Y. S. (2017). An ontological model of the domain of applications for the internet of things in analyzing information security. *Automatic Control and Computer Sciences*, 51(8): 817-823. doi:10.3103/S0146411617080132
- Liu, Y., & Zhang, S. (2020). Information security and storage of internet of things based on block chains. *Future Generation Computer Systems*, 106, 296-303. doi:10.1016/j.future.2020.01.023
- Miloslavskaya, N. and Tolstoy, A. (2017). Ensuring information security for internet of things. *IEEE 5th International Conference on Future Internet of Things and Cloud*, FiCloud 2017, pages 62-69. doi:10.1109/FiCloud.2017.17
- Miloslavskaya, N. and Tolstoy, A. (2020). IoTBlockSIEM for information security incident management in the internet of things ecosystem. *Cluster Computing*, 23(3): 1911-1925. doi:10.1007/s10586-020-03110-5
- Nour, B., Sharif, K., Li, F. and Wang, Y. (2020). Security and privacy challenges in information-centric wireless internet of things networks. *IEEE Security and Privacy*, 18(2): 35-45. doi:10.1109/MSEC.2019.2925337
- Semin, V. G., Khakimullin, E. R., Kabanov, A. S. and Los, A. B. (2017). Problems of information security technology the 'internet of things'. *International Conference "Quality Management, Transport and Information Security, Information Technologies"*, IT and QM and IS 2017, 110-113. doi:10.1109/ITMQIS.2017.8085775
- Wang, Z., Yao, Y., Tong, X., Luo, Q. and Chen, X. (2019). Dynamically reconfigurable encryption and decryption system design for the internet of things information security. *Sensors (Switzerland)*, 19(1). doi:10.3390/s19010143
- Wei, P. and Zhou, Z. (2018). Research on security of information sharing in internet of things based on key algorithm. *Future Generation Computer Systems*, 88: 599-605. doi:10.1016/j.future.2018.04.035
- Yan, T. and Wen, Q. (2011). Building the internet of things using a mobile RFID security protocol based on information technology. doi:10.1007/978-3-642-23777-5_24
- Yang, X., Hou, Y., Ma, J. and He, H. (2019). CDSP: A solution for privacy and security of multimedia information processing in industrial big data and internet of things. *Sensors (Switzerland)*, 19(3). doi:10.3390/s19030556
- Yorio, Z., Oram, R., El-Tawab, S., Salman, A., Heydari, M. H. and Park, B. B. (2018). Data analysis and information security of an internet of things (IoT) intelligent transit system. *Systems and Information Engineering Design Symposium*, SIEDS 2018, pages 24-29. doi:10.1109/SIEDS.2018.8374744
- Zhang, L. and Zhu, S. (2015). Food security information platform model based on internet of things. *Advance Journal of Food Science and Technology*, 8(5): 312-315. doi:10.19026/ajfst.8.1515.