ISSN NO: 2770-4491
Date of Publication:10-08-2022

Security in the Internet of Things: A Review

Diyorbek Umidjon ugli Jurayev
Tashkent University of Information Technologies

Abstract: The aim of the research is to study the impact of global machine-to-machine interaction on the technological safety and stability of the life support systems of modern society. The article discusses the most likely threats to the violation of confidentiality, availability and integrity of information circulating in information networks that are designed to manage industrial facilities.

Keywords: Internet of things, security, communication technologies, protection, hacking.

Introduction

One of the modern trends in the development of global information systems is the so-called Internet of Things (for example, the contactless payment system Apple Pay; cars controlled from a smartphone, etc.). The official definition of this term is given in ITU-T Y.2060, Overview of the Internet of Things: "...the Internet of Things (Internet of Things, IoT) is a global information society infrastructure that provides advanced services by organizing communication between things (physical or virtual) based on existing and developing compatible information and communication technologies" [1, 2].

At the same time, a number of experts in the field of information security note that the spread of the interaction of technical systems without human intervention carries quite serious security threats [3, 4]. On the one hand, remote control of systems such as "Smart Home" allows you to organize your living space with great comfort; and on the other, sensors and controls of life support systems, once in the hands of an attacker, significantly increase the risks in the field of information security.

Objective: assessment of information security of Internet of Things objects.

Materials and methods: Security is understood as the level of security of confidential data used by objects during their work. The system's resistance to common hacking methods (phishing, MITM and DDoS attacks) is considered as the main security characteristic.

To assess the security of the information security of the Internet of Things structures, an analysis of the architecture of its elements and a detailed analysis of possible hacking methods are used. in our opinion, the most preferable is the assessment of vulnerability from currently popular phishing, MITM attacks, as well as methods of social engineering.

The most popular systems were selected as objects for research:

1. Apple Pay is a mobile payment system from Apple Corporation. It was presented on September 9, 2014. With the help of Apple Pay programs, users of iPhone 6/6+, 6s/6s+, SE, iPhone 7/7+, Apple Watch can pay for purchases using NFS technology ("near contactless communication") in combination with the Wallet and Touch ID program, as well as for payments on the Internet.

2. The ZigBee Wireless Standard is a specification of top–level network protocols (APS (application support sublayer) application layer and NWK network layer) using lower-level services (MAC access control level and PHY physical layer) and regulated by the IEEE 802.15.4 standard. ZigBee and IEEE 802.15.4 describes wireless personal computing networks (WPAN).

3. Tesla Model S electric cars are five–door electric vehicles manufactured by the American company Tesla Motors. The prototype was first shown at the Frankfurt Motor Show in 2009; deliveries of the car to the United States began in June 2012 [5].

Research results: Currently, various standards for managing Internet things are gaining popularity. They offer ready-made sets of management protocols and make it possible to deploy their network quickly enough to manage devices [6].

ZigBee is a wireless standard, an IEEE 802.15.4 add-on, with which devices connected to the IoT communicate with each other. Samsung, Philips, Motorola and other major manufacturers use this standard for their devices. Researchers at the Vienna-based Cognosce company have discovered a critical flaw in ZigBee that can compromise any smart home.

The main problem is that manufacturers use standard communication keys (link key) for their devices, in pursuit of compatibility with devices of other manufacturers, cheapness and user convenience. The use of standard link keys jeopardizes the safety of the network as a whole. In addition, the ZigBee standard itself does not adequately address the issue of security and safety of keys, that is, secure initialization and transmission of encrypted keys inside the network are highly vulnerable. With a simple sniffing, an attacker is able to reverse the key exchange and infiltrate the network using a standard link key. As a result, the devices are open to MITM attacks, and the network, the active network key and all communications within the network are compromised [7].

After experiments with IoT bulbs, motion sensors, temperature sensors and door locks, Cognosec concluded that manufacturers equip devices for home use with only the necessary minimum of functions to meet the minimum standard. Unfortunately, this is a common practice that leaves users no choice, even if they want to increase the security standard on their device (at least by changing passwords and installing additional security software) [8]. According to the researchers, this problem is much more serious than the shortcomings in the ZigBee standard itself.

Owners of new electric cars by Tesla Motors also face similar security system shortcomings. [9]. For example, in September 2016, Tencent Keen Security Lab researchers demonstrated remote hacking of the Tesla Model S P85 and Model 75D. As a rule, to implement such attacks, researchers compromise the on-board software of the car itself, but the specialists of the Norwegian company Promon decided to approach the issue from the other side and attack the Android application.

Contactless payment systems using smartphones also have a number of vulnerabilities. Consider as an example the most popular system - Apple Pay. The essence of her work is that instead of using a plastic card or cash, any purchase can be paid for using an Apple gadget. Payment occurs when the user brings his iPhone or Apple Watch to the contactless terminal. After a few seconds, a message appears on the screen about the possibility of making a payment and an offer to confirm the transaction through a fingerprint scanner or password.

The Apple Pay system consists of 4 main parts:

1. The main mechanism is based on the technology of close NFC data transmission (at a distance of up to 20 cm), in connection with the Secure Element chip, which is an industry standard in the field of financial operations. a special Java application is running on this chip.

2. Secure Element – an area of shared memory separated from the system memory. In this area, the user's bank card data is stored in encrypted form. no program has access to it, data is not transferred anywhere, and even Apple cannot influence this strategy..

3. Secure Enclave is a component that manages the authentication process and launches payment transactions, as well as stores a fingerprint for Touch ID.

4. Apple Pay Servers is the server part that manages the status of credit and debit cards in the Wallet application, together with the device number stored in the Secure Element. Apple Pay Servers are also responsible for transcoding payment information inside applications.

Apple Pay has a multi-level protection system: a unique device identifier, dynamically generated security codes for each payment transaction, biometric information - a fingerprint.

Conclusions:

In the course of the work carried out on vulnerability analysis , the following conclusions were made:

1. No modern "Smart Home" system is really safe. One of the main reasons for the insufficient quality of information security is the desire of manufacturers to reduce the cost of their products as much as possible in order to attract the maximum number of customers, who, as a rule, when choosing a product, give preference not to security, but to functionality and price.

2. Even such popular wireless standards as ZigBee are not vulnerable. The reasons for their presence also lie in the desire to reduce the cost of products as much as possible, observing the minimum requirements of information security.

3. Tesla electric cars with the possibility of remote control, which are gaining popularity, also have a

ISSN NO: 2770-4491
Date of Publication:10-08-2022

number of problems with remote control of the car. The risk in this case depends not so much on the car manufacturer itself, as on the mobile devices from which the vehicle is monitored.

References:

1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *2012 international conference on computer science and electronics engineering* (Vol. 3, pp. 648-651). IEEE.
2. Lu, X., Qu, Z., Li, Q., & Hui, P. (2015). Privacy information security classification for internet of things based on internet data. *International Journal of Distributed Sensor Networks, 11*(8), 932941.
3. Irshad, M. (2016, December). A systematic review of information security frameworks in the internet of things (iot). In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 1270-1275). IEEE.
4. Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers*, *14*(2), 375-393.
5. Miloslavskaya, N., & Tolstoy, A. (2019). Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*(1), 103-119.
6. Yang, X., Li, Z., Geng, Z., & Zhang, H. (2012). A multi-layer security model for internet of things. In *Internet of things* (pp. 388-393). Springer, Berlin, Heidelberg.
7. Liu, Y., & Zhang, S. (2020). Information security and storage of Internet of Things based on block chains. *Future Generation Computer Systems*, *106*, 296-303.
8. Lu, X., Li, Q., Qu, Z., & Hui, P. (2014, October). Privacy information security classification study in internet of things. In *2014 International Conference on Identification, Information and Knowledge in the Internet of Things* (pp. 162-165). IEEE.
9. Zhao, Y. L. (2013). Research on data security technology in internet of things. In *Applied mechanics and materials* (Vol. 433, pp. 1752-1755). Trans Tech Publications Ltd.