The method of increasing the security of IoT devices by implementing the dynamic change of the Bluetooth address

Inna Mykhalchuk[1,*,†], Yurii Shcheblanin[1], Oleksandr Toroshanko[1,†] and Hanna Martyniuk[2,3,†]

[1] *Taras Shevchenko National University of Kyiv, Volodymyrska Str., 60, Kyiv, 01601, Ukraine*

[2] *Mariupol State University, Preobrazhenska Str., 6, Kyiv, 03037, Ukraine*

[3] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zalizniak Str., 3/6, Kyiv, 03142, Ukraine*

Abstract

The paper examines the possibilities of use and vulnerability of devices that, according to the concept of construction and use, belong to the Internet of Things. Modern technological solutions for collecting and transmitting primary data mostly focus on Internet of Things devices. They are actively used in various spheres of industry and everyday life. At the same time, the low price, technological limitations and the lack of uniform standards affected their security level. There are known cases when attackers, exploiting the vulnerabilities of Internet of Things devices, launched an attack on the company's information system and caused financial and reputational damage. Typical solutions for the construction of IoT systems, in most cases, allow attackers to implement attacks on vital components of such systems and create a threat to the lives of users, causing reputational and financial losses. Such devices are connected to the control unit with Bluetooth technology and are identified by the name of the device and its Bluetooth address. These parameters are the main vector of the intruder's attack on Internet of Things devices. The paper proposes a method of increasing the level of security of IoT devices by introducing a dynamic change of the Bluetooth address. The central control unit of the Internet of Things devices will initiate the process of dynamic, random over time, change of the Bluetooth address of the devices, which will limit the time interval of possible influence of the attacker on the device.

Keywords

IoT, protection methods, data analysis, attack vector, network security, Bluetooth, access control systems, attack classification, information security

1. Introduction

Privacy and security issues become especially relevant when it comes to the Internet of Things (IoT). IoT is a concept that defines the connection of various physical objects to the Internet for data exchange and interaction [1]. These objects can include any devices or sensors that can receive, transmit and process data. IoT allows data to be collected in real-time, providing the opportunity for optimal management and monitoring of various systems. This technology is used in various fields, such as industry, agriculture, medicine, transport, home automation ("Smart Home" technology) and others. At the same time, IoT technology is one of the main attack vectors, attackers can use these systems for various purposes, such as collecting information about users, affecting network resources or the process of managing connections of IoT devices, affecting vital end devices IoT, etc. [2, 3, 4], which requires increased attention to IoT security issues. Security mechanisms of IoT

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

inna.mykhalchuk@knu.ua (I. Mykhalchuk); shcheblanin.yurii@knu.ua (Y. Shcheblanin); oleksandr.toroshanko@knu.ua (O. Toroshanko); ganna.martyniuk@gmail.com (H. Martyniuk)

0000-0002-1802-7653 (I. Mykhalchuk); 0000-0002-3231-6750 (Y. Shcheblanin); 0000-0002-2354-0187 (O. Toroshanko); 0000-0003-4234-025X (H. Martyniuk)

systems are aimed at ensuring the protection of devices from unauthorized access, protection of network connections from attacks and detection of possible threats.

This includes the use of various techniques such as encryption, authentication, authorization, buffer overflow protection, and others [5]. It is also important to take into account the technological features of the functioning of IoT devices, monitor potential threats and use a comprehensive approach to their protection, including technical and organizational measures, such as compliance with security protocols, conducting training and raising awareness among users.

2. Formulation of the research task

Ensuring cybersecurity in IoT systems requires the development and implementation of a comprehensive protection system that includes both technical and organizational mechanisms. Technical protection mechanisms include encryption, authentication and authorization, access control, monitoring and analysis of security events and other methods that allow you to protect devices and their data from cyber criminals [6].

Organizational security mechanisms include security policies, security audit procedures, training, and user awareness of safe practices. For example, educating users about password security and prohibiting them from using the same password on multiple devices can reduce the risks of a hack. In addition, security mechanisms in IoT systems are important from the point of view of protection against cyber terrorism. In today's world, cyber terrorists can use different methods to attack IoT systems, such as DDoS attacks, malware distribution, phishing and social engineering [7].

These attacks can paralyze the functioning of IoT devices, significantly reduce their reliability and resilience, and lead to data loss and leakage of confidential information. Another aspect of relevance is the rapid growth in the number of IoT devices used in various industries such as transportation, industry, healthcare, and others. These devices collect and process large amounts of data, which can lead to serious problems related to the protection of confidential information and ensuring the safety of users in case of compromise.

Therefore, the development and implementation of effective protection mechanisms in IoT systems is an extremely important task that will reduce the risks of hacking and cyber-attacks, ensure the safety and confidentiality of devices and the information stored on them, as well as ensure the stability and reliability of devices in various fields of use. One of the main problems in IoT systems is the lack of safety and security standards and regulations. This means that device manufacturers can take different approaches to securing and protecting their devices, which can create vulnerabilities and risks for users [8, 9].

In addition, software updates and patches that contain fixes for identified vulnerabilities are not always distributed to users in a timely and efficient manner. Another challenge is the complexity of securing IoT systems, as they can contain a large number of different components and devices that communicate with each other over wireless networks. This leads to an increase in attack vectors and a decrease in the effectiveness of protection. In this regard, the development and implementation of effective protection mechanisms in IoT systems is an extremely difficult task that requires a comprehensive approach. To ensure the security of IoT systems, it is necessary to consider all elements of the system as a whole structure and ensure their interaction from the point of view of security and protection [10]. To do this, it is necessary to develop and use new technologies and standards that allow protection against various types of attacks, as well as increase the efficiency of updating and patching software.

3. A method of increasing the security of IoT devices

Technologically, IoT devices can be combined into specialized subsystems that, with the help of a central control unit, interact with each other and solve certain tasks. As an example, consider the "smart home" system shown in Figure 1 [11].

The main elements of the IoT system are [12–15]:

- Connected devices - are physical devices or sensors capable of collecting and transmitting data over the network (for example, temperature, humidity and motion sensors that connect to the information transmission network).
- Data collection tools - are components that provide collection, aggregation and processing of data received from connected devices (for example, cloud platforms, local servers or embedded data collection systems).
- Communication networks - are network resources that provide data transfer between connected devices and data collection devices (for example, Wi-Fi, Bluetooth, ZigBee, Z-Wave, LTE, NB-IoT, and others).
- Cloud services - cloud platforms provide resources to store, process and analyze the large amount of data received from connected devices, and they can also provide tools for IoT application development and system management.
- Analytics and artificial intelligence - these components provide processing and analysis of information from a large volume of data collected from connected devices, and can use machine learning algorithms and other artificial intelligence techniques to obtain valuable information and predict future events. For example, data analysis can help predict technical problems with devices before they occur, as well as optimize energy consumption and ensure high efficiency of systems built using IoT devices.
- Management systems - are components that provide management of connected IoT devices and applications. They can provide interfaces for monitoring and controlling devices using mobile applications or web interfaces.
- Security blocks - the components that protect connected IoT devices and data from malicious attacks. These may include cryptographic protocols, remote authentication methods and other security methods.

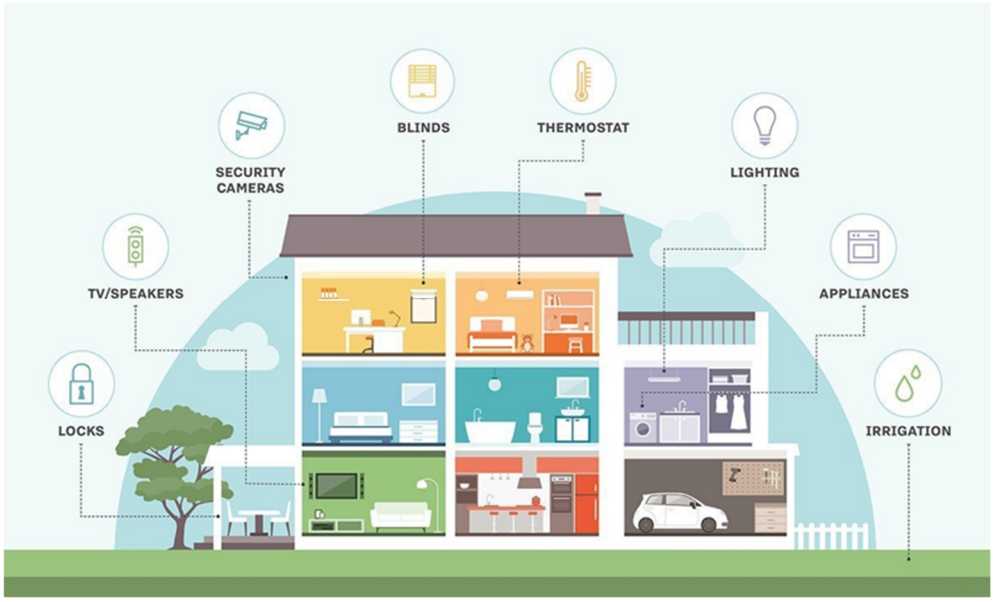

Figure 1: Smart home system.

Because the concept of a "smart house", to increase capabilities, involves the connection of additional IoT devices, the probability of implementing attacks on the system as a whole, due to the vulnerabilities of individual IoT devices, also increases.

To develop a method of increasing the security of IoT devices in the "smart home" system, we will classify threats according to their origin and methods of implementation [16]:

1. By origin:

- Internal threats: These are threats arising from the actions of service company employees who have access to IoT devices. Such threats may include abuse of privileges, misuse of data or intentional distortion of the functions of devices and the "smart home" system as a whole.
- External threats: these are threats that come from outside the boundaries of the "smart home" system and are aimed at its components. Such threats may include hacker attacks, phishing attacks, viruses, and more.

2. By methods of implementation:

- Security attacks: These are threats used to hack IoT devices and gain unauthorized access to them and the system in which they function. Such threats are implemented by intercepting the technological data of IoT devices, making changes to the functioning of the system, disclosing confidential data, etc.
- Privacy attacks: These are threats used to violate the privacy of IoT users. Such threats may include location tracking, interception of messages, collection of user information, etc.
- Availability attacks: These are threats used to interfere with the normal functioning of IoT devices and smart home subsystems. Such threats may include DDoS attacks on the device, jamming the data transmission channels between the IoT device and the control unit, making changes to the settings of IoT devices and subsystems, etc.

3. By type of IoT devices:

- Threats to Home IoT Devices: These are threats arising from connecting home devices to the Internet, such as routers, routers, home security systems, etc. Such devices can become the target of attacks due to their vulnerabilities and lack of protection.
- Threats to industrial IoT devices: These are threats arising from connecting industrial devices to the Internet, such as manufacturing process sensors, medical equipment, access control systems, etc. Such devices can be the target of hacker attacks or be used as entry points to hack other systems on the network.

4. By the scale of influence:

- Local threats: These are threats that affect individual IoT devices or small groups of devices, such as home networks.
- Global threats: These are threats that have a large-scale impact on IoT systems, such as large-scale hacking attacks on the critical network infrastructure or energy and transport management systems.

One of the most common threats to IoT systems are attacks on the network layer. These attacks can include various methods such as intercepting traffic, modifying data packets, injecting forged packets into the network, sending fake requests, and more. Another type of threat to IoT systems is application layer attacks. These attacks can include exploits, software hacking, phishing attacks, and other methods. Another type of threat to IoT systems is hardware-level attacks. These attacks may include exploits that exploit vulnerabilities in physical access to IoT devices [17].

Most often, Bluetooth technology is used to connect IoT devices to the "smart home" control unit and the Internet. Bluetooth is a wireless data transmission standard designed to provide short-range connections between various electronic devices, allowing information to be exchanged between various devices without the need for cables. Bluetooth works over short distances, usually within a few meters, and uses radio waves to exchange data wirelessly. This technology is widely used for transmission, establishing connections between devices, as well as connecting IoT devices to the network. Bluetooth supports different versions with different capabilities and data rates.

The use of wireless technologies allows to reduce the risk of system hacking due to physical access to IoT devices, at the same time, Bluetooth technology has several potential security disadvantages that must be taken into account when using it [18].

A Bluetooth connection can be vulnerable to data interception attacks, especially over open or weakly secured connections. To reduce the likelihood of this, it is recommended to use Bluetooth 4.0 and above technology, which involves the use of the Bluetooth LE Privacy function. This feature implements the process of generating "advertisement packets" with random MAC addresses, which prevents an attacker from identifying and affecting the device.

But how do surrounding devices see that the device has a different address? When first connected, a special trusted relationship is established between the devices, after the connection, the two devices will have different encryption keys, one of which is for privacy. This key is called the Identity Resolution Key (IRK). IRK allows the first device to translate these random MAC addresses that appear in "advertisement packets" from the second device into the real MAC address of the second device. This feature is available to devices that you trust. Privacy Bluetooth Smart operates with Bluetooth version 4.0 of the core specification [19, 20].

But not all devices of the IoT system can support Bluetooth version 4.0, the following types of threats are relevant for such devices [21]:

- Bluejacking and Bluesnarfing: Bluejacking involves sending unknown messages or contacts on other users' Bluetooth devices without their proper consent. Bluesnarfing is an attack in which an attacker can gain unauthorized access to data on a Bluetooth device.
- Pairing attacks: The pairing process of Bluetooth devices can be vulnerable to attacks, especially if weak or common PIN codes are used. Using Authorized Devices: Attacks that use devices that are already authorized to connect to the system.

Each Bluetooth device has a unique address. This address consists of 6 bytes and is similar to a MAC address, in the format MM:MM:MM:XX:XX:XX, where the upper three bytes, labelled M, contain information about the manufacturer of the chip. By the remaining three lower X bytes, an attacker can determine the device model, which significantly reduces the device's security [19].

To reduce the vulnerability of IoT devices implemented using Bluetooth technology, it is possible to implement dynamic replacement of the Bluetooth address of IoT devices, this will ensure the anonymity of the devices, and reduce the risk of their tracking and identification.

The main idea of this method is to initiate the process of dynamically changing the device's Bluetooth address on the side of the control unit according to a random law.

Since attackers usually discover a device by its Bluetooth address, dynamically changing the Bluetooth address reduces the likelihood of hacking attacks or interception of the connection. If a device consistently uses the same address, it can make it vulnerable to eavesdropping or identifying its owner. Changing the address allows you to preserve the privacy of the user and makes it difficult to determine his identity. Changing the Bluetooth address also allows you to exclude prohibited devices from the network.

The block diagram of the method of dynamic replacement of the Bluetooth address of the "smart home" IoT devices is shown in Figure 2.

The sender application is a special software deployed in the IoT device network control unit. The database of which stores the list of IoT devices identified and authenticated in the system and implements the function of generating the Bluetooth address of the IoT device according to a random law. The newly generated Bluetooth address is encrypted and transmitted to the recipient's application. The receiver application, this special software is deployed in the IoT device, where the generated Bluetooth address of the device is decoded and the process of rewriting the new Bluetooth address to the IoT device memory is initiated.

The receiving application generates a message about the status of the IoT device and transmits it to the control unit (sending application), where the technological information is checked and, in the

case of its confirmation, the Bluetooth address of the IoT device is overwritten (replaced) in the database of the control unit.

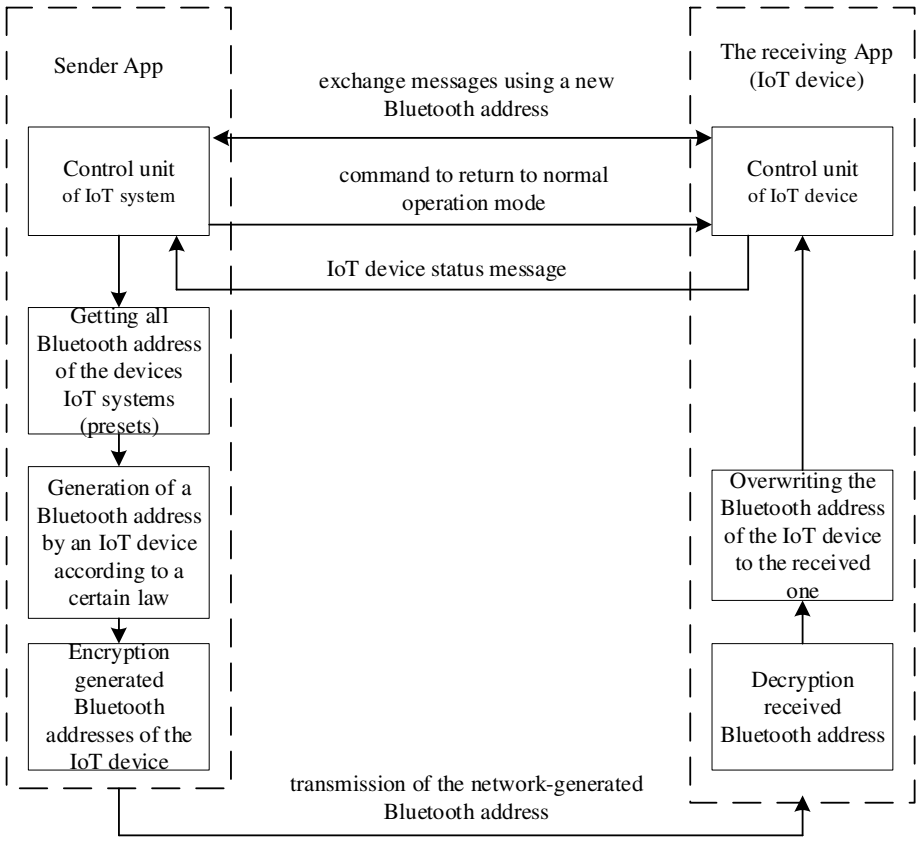

Figure 2: Structural diagram of the implementation of the method of dynamic replacement of the Bluetooth address.

The sender application transmits to the IoT device (receiver application) a command to complete the address replacement cycle and return to normal operation mode to the new Bluetooth address.

The receiver application (IoT device) switches to normal operating mode and transmits data to the control unit.

4. Conclusions

Enhancing security in an IoT system that uses Bluetooth networking is a critical task because IoT devices often collect and share critical information. At the same time, the locations of the devices allow attackers to stay in their area of operation for a long time, and use specialized software and hardware tools to implement attacks on the IoT device and the IoT system as a whole.

The work analyzed the structure of the "smart home" system implemented using IoT devices, classified threats and determined that the most vulnerable are those implemented using Bluetooth technology. A method of dynamically changing the Bluetooth address of IoT devices was proposed, the implementation of the method will allow to significantly increase the security of IoT devices that are outside the controlled zone and concerning which an attacker can carry out illegal actions (collection of network data for their analysis and compromise, etc.).

The directions of further research will be focused on the development of a method of increasing the security of the central control unit of the IoT system.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] S. Greengard, The Internet of Things, The MIT Press, London, England, 2015.

[2] K. Oliynyk, 5 Essential Steps to Ensure Secure Communication with IoT Devices, 2023. URL: https://webbylab.com/blog/5-essential-steps-to-ensure-secure-communication-with-iot-devices.

[3] Y. Shcheblanin, B. Oliinyk, O. Kurchenko, O. Toroshanko, N. Korshun, Research of authentication methods in mobile applications, CEUR Workshop Proceedings 3421 (2023) 266–271. URL: https://ceur-ws.org/Vol-3421/short14.pdf.

[4] D. Ivanova, V. Diordiev, Means of implementing the concept of "Smart Home", in: Proceeding of Problems of mechanization and electrification of technological processes, Melitopol, 2019, pp. 51–52. URL: http://elar.tsatu.edu.ua/bitstream/123456789/8228/1/СБОРНИК%20МЕА-2019-51-52.pdf.

[5] F. Hu, Security and Privacy in Internet of Things (IoTs), CRC Press, Boca Raton, USA, 2016.

[6] F. Chantzis, I. Stais, P. Calderon, E. Deirmentzoglou, B. Woods, The definitive guide to hacking the world of the Internet of Things (IoT), No Starch Press Inc, San Francisco, USA, 2023.

[7] L. Goeke, Security Challenges of the Internet of Things, 2023. URL https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1.

[8] O. Solomentsev, et al., Data processing through the lifecycle of aviation radio equipment, in: Proceedings of IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), IEEE, Lviv, Ukraine, 2022, pp. 146–151. doi: 10.1109/CSIT56902.2022.10000844.

[9] M. Zaliskyi, et al., Heteroskedasticity analysis during operational data processing of radio electronic systems, in: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), Data science and security, volume 290 of Lecture Notes in Networks and Systems, Springer, Singapore, 2021, pp. 168–175. doi: 10.1007/978-981-16-4486-3_18.

[10] B. Russell, D. Van Duren, Practical Internet of Things Security, Packt Publishing, Great Britain, 2018.

[11] D. Spivey, Home Automation. For Dummies. For Dummies, Wiley, New Jersey, 2014.

[12] M. Kranz, Building the Internet of things: implement new business models, disrupt competitors, and transform your industry. Wiley, New Jersey, 2017.

[13] A. Bahga, V. Madisetti, Internet of Things (IoT): A Hands-On Approach. URL: http://www.internet-of-things-book.com.

[14] S. Li, L. D. Xu, Securing the Internet of Things, Syngress is an imprint of Elsevier, Cambridge, MA, USA, 2022.

[15] I. Ostroumov, et al., A probability estimation of aircraft departures and arrivals delays, In: O. Gervasi, et al. (Eds.), Computational Science and Its Applications – ICCSA 2021. ICCSA 2021, volume 12950 of Lecture Notes in Computer Science, Springer, Cham, 2021, pp. 363–377. doi: 10.1007/978-3-030-86960-1_26.

[16] B. Zhurakovskyy, I. Zeniv, Internet of Things technologies, NTU, Kyiv, 2021.

[17] P. Ghole, Attacks on IoT devices using Bluetooth, 2023. URL: https://www.einfochips.com/blog/attacks-on-iot-devices-using-bluetooth/.

[18] M. Kofler, Hacking and Security: The Comprehensive Guide to Penetration Testing and Cybersecurity, Wubbeling, Rheinwerk Computing, 2023.

[19] M. Woolley, Bluetooth technology protecting your privacy, 2015. URL: https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/.

[20] A.V. Garist, Vulnerability analysis of bluetooth technology, Scientific Notes of the Tavria National University named after V.I. Vernadsky, Radio engineering and telecommunications, 33(72) (2022) 27–31.

[21] N. Frolova, I. Mykhalchuk, O. Tyshchenko. Protection of public WI-FI access points, Journal of the National University "Chernihiv Polytechnic", Technical Sciences and Technologies 1 (2022) 123–135.