UDC 004.02

10.20535/2411-2976.22024.13-19

METHOD FOR IMPROVING SECURITY OF IOT DEVICES PAIRING

[1]Stanislav I. Pedan, [1]Maksim V. Melnik, [1]Mykola O. Alieksieiev, [2]İnci Umakoğlu

[1]Educational and Research Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
[2]Kütahya Dumlupinar University, Kütahya, Turkey

Background. The usage of IoT technologies leads to the social, technological and financial development of society. While complex systems play an important role in the IoT, the design, integration and use of simple devices really drive the technology's widespread adoption. At the same time, ensuring a high level of security for simple IoT devices is a difficult task. The reasons for this are device limited computing resources and low power consumption requirements. It prevents the implementation of most modern cryptographic protocols for simple IoT devices. From a security point of view, the most critical communication stage is device pairing, when shared encryption keys are formed to establish a secure communication channel.

Objective. The purpose of the paper is to analyse the main vulnerabilities of a simple IoT device pairing process and develop a method for improving security of this process. The method should provide proximity-based device authentication and pairing process protection against known attacks, such as man-in-the-middle attack.

Methods. The method of pairing process security improvement includes proximity-based device authentication using analysis of the wireless signal strength. The security of the authentication method is proven analytically and by results of practical experiments with measurement of wireless signal strength change with distance and obstacles between devices.

Results. Performed research demonstrated that the proposed method guarantees secure user authentication at a close distance between devices and protection against attacker located at least 10 meters from the paired device. Provided theoretical calculations and experimental results show that the level of attacker's wireless signal power increase required for a successful attack exceeds technical capabilities of existing communication devices.

Conclusions. The article solves an important issue of improving the security of simple device pairing. The proposed method of proximity-based IoT device authentication provides pairing process protection against man-in-the-middle attacks. Mathematical calculations were confirmed by conducting a number of experiments to research wireless signal power change depending on the distance and types of obstacles between devices. The proposed authentication method can be integrated into the existing JustWorks protocol for connecting simple IoT devices using the BLE communication channel.

Keywords*: security; authentication; Internet of Things; main-in-the-middle attack; Bluetooth Low Energy; JustWorks; RSSI.*

Introduction

The Internet of Things (IoT) is a new paradigm in which a large number of devices and sensors cooperate by communicating via Internet, providing innovative services for various challenges and problems of modern life [1]. The application of IoT technologies leads to the social, technological and financial development of a society, providing intelligent management of vehicle traffic, security and surveillance, automation of agriculture, health care and medicine, smart cities and houses, and smart energy consumption [2].

Although complex systems play an important role in the IoT, the design, integration, and use of simple devices drive the widespread adoption of this technology [4].

At the same time, ensuring a high level of security for simple IoT devices is a difficult task due to the fact that their limited computing resources and low power consumption requirements prevent the implementation of most modern cryptographic protocols.

The most critical from the point of view of security is the stage of device pairing, when shared encryption keys are formed to establish a secure communication channel.

A man-in-the-middle attack, successfully implemented when connecting even a simple low-cost IoT device to an existing internal network, allows access to more complex devices on that network that may be storing valuable data or performing mission-critical functions.

The purposes of the research are to analyse main vulnerabilities of simple IoT device pairing process and to develop a method for increasing this process security by proximity-based device authentication and its resistance against known attacks, such as man-in-the-middle (MITM) attack.

1. Simple IoT devices pairing protocol and its security issues

The latest “State of IoT - Spring 2023” report from IoT Analytics [3] shows that the number of global IoT connections will grow to 14.3 billion active IoT devices. Although growth in 2023 was predicted to be slightly lower (16% or to 16 billion active devices) than in 2022, the number of IoT device connections is expected to continue to grow for many years to come. Among the communication technologies of IoT devices, Wi-Fi, Bluetooth and cellular communication dominate. 27% of all connections are Bluetooth connections. Bluetooth Low Energy (BLE) provides reliable connectivity with limited power consumption, which is a better option for battery-powered IoT devices. Examples of such devices can be smart home sensors or trackers of personal belongings.

Simple devices such as sensors and actuators are the foundation of IoT. They provide seamless connectivity and communication between various objects in everyday life: smart home security systems use simple devices such as motion sensors and door sensors to detect any unusual activity and send alerts to the homeowners. A key feature of IoT devices, including the listed simple devices, is their ability to communicate and share data.

Most simple IoT devices are inherently insecure due to their small or limited size, which can only accommodate low-power embedded microcontrollers, simple sensors, actuators, power supplies, and other tiny electronic components. This size limitation, combined with low-power consumption requirements, simple or basic operating systems, and limited computing power, often precludes the adoption of advanced or even modern cryptographic techniques [5]. The active proliferation of simple IoT devices in everyday life, combined with poor security level, makes them a profitable target for cybercriminals.

JustWorks method [6] is used for pairing with simple IoT devices that do not have a user interface (display, microphone, speakers, information input devices such as a keyboard) and, as a result, the ability to enter or confirm an access key. It provides the most accepted pairing mode for BLE devices, as almost all BLE IoT devices do not have any information input and output capabilities, such as light bulbs, smart locks, refrigerators, key fobs, and heart rate monitors. The main feature of this connection mode is that no authentication is required to complete the connection procedure[7]. Anyone can connect to any BLE device that uses JustWorks. As a result, created connection is protected from passive eavesdropping by encryption, but it is powerless against MITM attack.

A MITM attack intercepts communication between two parties to collect or alter data for disruption or financial gain. A MITM attack involves two steps:

1. Interception: The first step is to intercept information from the target before it reaches its destination. One way to do this is to create malicious Wi-Fi hotspots that users can connect to for free. All transactions made within that Wi-Fi are then recorded [9].

2. Decryption: As the level of cybercrime is skyrocketing, the majority of network traffic today is encrypted. This means that after interception, the information must be decrypted to be useful to the attacker. This should be done without notifying the user, application or service provider [9].

The scenario of an attacker taking possession of an IoT device as a result of a MITM attack is presented in Fig. 1.

If attacker first initiates the pairing procedure with the IoT device, IoT device exchanges messages with attacker to generate a shared secret and uses it for secure communication. If only one device can own an IoT device at a time, the authentic owner of IoT device cannot perform the pairing procedure with it. Moreover, the attacker can mask the result of his attack, mislead the user and establish a secure connection with him under the guise of an IoT device.

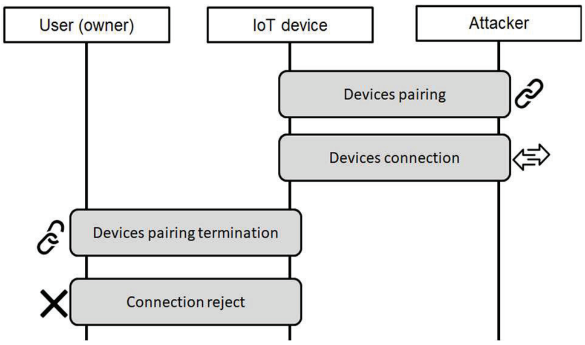

Fig. 1. Actual scenario of pairing attacker with IoT device as a result of a MITM attack

Thus, a successful MITM attack can lead to the acquisition of an IoT device and the ability to access confidential data transmitted over the network.

2. Approaches for improving device pairing security

The security of the pairing process can be improved by device authentication. A common method of authenticating devices that have input (keyboard, camera) and output (display) capabilities is the use of a random PIN number or QR code.

For IoT devices that do not have such input and output capabilities, an additional out-of-band (OOB) channel is typically used, which has a short range. Examples of such channels use cases are transmission of messages through the NFC channel or information transfer via ultrasound (if devices are equipped with a speaker and a microphone).

In the case of the simplest IoT devices, such as temperature measurement device, consisting of a BLE chip and temperature sensor, it is possible to implement the authentication of paired device based on its proximity verification by analysing wireless signal strength.

Scientists from Microsoft Research proposed the Move2Auth[8] method, which provides authentication of simple IoT devices based on determining their proximity. The method requires the user to hold the smartphone and perform one of two hand gestures (randomly selected by the smartphone) in front of the IoT device while the IoT device continues to send packets. Two gestures, i.e., moving the smartphone towards and away from the IoT device and rotating the smartphone, lead to a significant (about 15 dB) change in the received signal strength (RSS) due to the rapid change in antenna attenuation and polarization, respectively. Based on the level of correlation of RSS variations with the readings of smartphone motion sensors (accelerometer and gyroscope), it is possible to reliably detect the proximity of devices. This allows us to effectively distinguish between near and far devices and thus protects the pairing procedure of two nearby devices from a far-away attacker who can arbitrarily increase the transmission power of his signal.

The disadvantage of the proposed approach is the need to directly involve the user, who should perform specific movements with the device. The inaccuracy of performing these movements affects the accuracy of determining the authentication result. Another disadvantage is that such authentication is one-way only and can be implemented for a device that has motion sensors, such as a smartphone. If the second device is, for example, the previously mentioned temperature measurement device, then it cannot authenticate the smartphone that tries to perform the pairing procedure with it.

An important task is development of a secure method of device mutual authentication which does not require direct user involvement. Such a method should be able to distinguish nearby devices and far-away attackers using wireless signal characteristics analysis.

Method for proximity-based IoT device authentication

In this article, instead of using specific movements of the smartphone, it is proposed to bring it as close as possible to the IoT device and conduct mutual authentication based on the strength of the wireless signal.

The signal strength measured by the first device decreases as the distance to the second device increases. This dependence can be described by the following formula:

$$\mathrm{RSSI_{d1}} = \mathrm{RSSI_{d0}} - 20\log(\frac{\mathrm{d1}}{\mathrm{d0}}) \ [1]$$

where d0 – initial distance between devices, d1 – final (increased) distance between devices, $\mathrm{RSSI_{d0}}$ – signal strength on a distance d0, $\mathrm{RSSI_{d1}}$ – signal strength on a distance d1.

According to the obtained experimental data, the RSSI for a distance of up to 10 centimetres has an average value of -10dBm. In order to convert dBm to watts, the following formula can be used:

$$\mathrm{P(W)} = \frac{10^{\frac{\mathrm{P(dBm}}{10}}}{1000}, \ [2]$$

where P(W) – power of signal in Watts, P(dBm) – signal strength in dBm. Thus, according to the formula [1], if the attacker is located at 10 meters distance from the IoT device, his signal strength will be on $20\log\left(\frac{\mathrm{d1}}{\mathrm{d0}}\right) = 20\log\left(\frac{10}{0.1}\right) = 20 \cdot 2 = 40\mathrm{dBm}$ lower, than the authentic device signal strength at a distance of 10 centimetres for the same output power of BLE antenna. In order to create on an IoT device the illusion of locating second device in a close proximity, an attacker needs to increase the signal strength by 40 dBm, or 10 Watts according to the formula [2]. Given FCC and ETSI regulations, the maximum antenna output strength allowed by the BLE protocol is 20 dBm.

Fig. 2 demonstrates a pairing process scenario, similar to the one presented in Fig. 1, but using the proposed protection method. The attacker first initiates the connection with the IoT device. IoT device approves temporary pairing with attacker and establishes a temporary communication channel. IoT device then authenticates the attacker's device by measuring the distance to it based on the wireless signal strength analysis. In the case of connecting to an attacker, the IoT device determines the distance to it, which is greater than the safe distance threshold. It leads to the termination of connection and deletion of information about pairing with the attacker. Next, if the authenticated user performs a temporary pairing procedure with an IoT device, the IoT device successfully authenticates the user and changes the connection status from temporary to permanent. Thus, the proposed authentication method provides resistance of the device pairing procedure to MITM attacks, which increases the overall level of security of simple IoT devices.

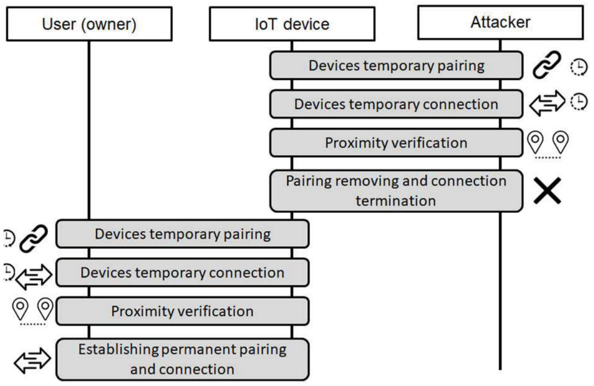
User (owner)
IoT device
Attacker
Devices temporary pairing
Devices temporary connection
Proximity verification
Pairing removing and connection termination
Devices temporary pairing
Devices temporary connection
Proximity verification
Establishing permanent pairing and connection

Fig. 2. Scenario of a pairing process protection from a MITM attack using the proposed method

3. Practical verification of the proposed method

Using proposed authentication method first device measures wireless signal strength of a second device to calculate current distance between devices. If calculated distance is less than the required threshold, it guarantees that the two devices are at a minimum safe distance for secure pairing.

Practical evidence of the proposed method's effectiveness consists of analysing wireless signal power values between two devices located at different distances with different types of obstacles.

Fig. 3 shows the scheme of the experiment, which consists of a device that generates a wireless signal of a fixed strength (Wi-Fi router Netis WF2419R), a device (Laptop Asus F15 FX506H) that is located at a given distance and measures the strength of the received signal. Obstacles of a different physical nature are situated between two devices. Measurements were performed inside residential building and in outdoor conditions. RSSI data was measured and averaged for 60 seconds for each test case using standard software of the Windows operating system.

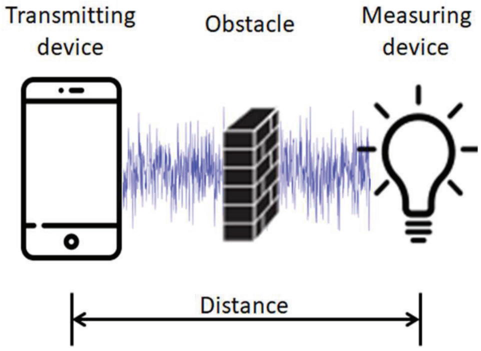

Fig. 3. Scheme of the experiment for measuring wireless signal strength between two devices

The parameters of the experiment, presented in Table 1, are distance and type of obstacle between devices.

Table 1. Parameters of RSSI measurement experiment.

Parameter	Values
Distance, m	0 – 1 with step 0.1 + 1-10 with step 1 + 10-30 with step 5
Obstacle type	No obstacle indoor/outdoor, wood door, metal door, glass, brick wall

Fig. 4 shows the graphs of the received experiment results.

As can be seen from the graphs, the signal strength at a distance of about 10 cm is -10 dBm, and at a distance of 10 meters it decreases to -50..-70 dBm, depending on the type of obstacle between devices. The best signal transmission occurs when there are no obstacles between devices, glass leads to a slight decrease in the signal strength, and a brick wall leads to the maximum drop in the signal strength value.

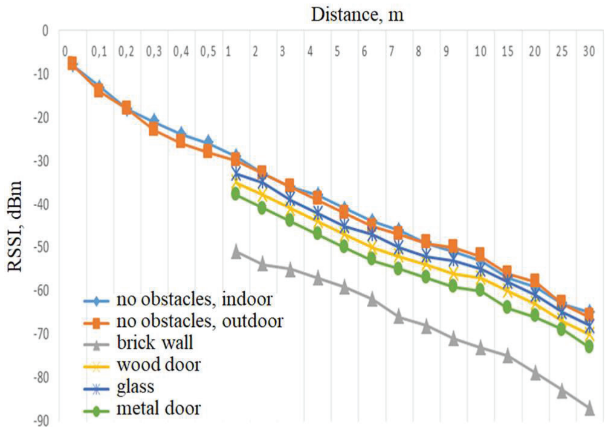

Fig. 4. Results of RSSI measurement for different distances and obstacles between devices

Analysing the obtained results, it can be concluded that at a distance of 10 meters, which is assumed to be the minimum distance that an attacker can approach an IoT device, an attacker must increase the level of his signal by at least 40 dBm to obtain a signal strength corresponding to the IoT device at a safe distance of 10 cm and ensures a positive authentication result. In the presence of an obstacle, the attacker must increase the signal level to a value that even exceeds 40 dBm.

Thus, the obtained practical results confirm the correctness of the theoretical modelling of the method given above.

Conclusions

The active development of IoT technologies and growing number of connected devices requires higher security level of such devices pairing and communication. Simple devices, which are the backbone of IoT industry, do not have technical capabilities to apply complex cryptographic protocols, which reduces their security level, for example, the lack of protection against MITM attacks.

In this article, we propose a method of improving security of IoT devices pairing procedure by using mutual proximity-based authentication. Authentication is based on proximity determination by analysing the power of a wireless signal (such as BLE) strength. The mathematical model of authentication method was confirmed by conducting a number of experiments to study wireless signal strength change depending on the distance and types of obstacles between devices.

The proposed authentication method can be integrated into the existing JustWorks protocol for pairing IoT devices using BLE communication channel.

References

1. Sachin Kumar, Prayag Tiwari and Mikhail Zymbler, Internet of Things is revolutionary approach for future technology enhancement: a review, Journal of Big Data, 2019, Article 6, Number 111.
2. S Choudhary, G Meena, Internet of Things: Protocols, Applications and Security Issues, Procedia Computer Science, 2022, Volume 215, pp. 274-288.
3. IoT Analytics, State of IoT 2023. Retrieved from https://iot-analytics.com/wp/wp-content/uploads/2023/05/Insights-Release-State-of-IoT-2023-Number-of-connected-IoT-devices-growing-16-to-16.0-billion-globally.pdf
4. Tomorrow Bio, Understanding IoT: How Simple Devices Can Drive Big Changes, 2023. Retrieved from https://www.tomorrow.bio/post/understanding-iot-how-simple-devices-can-drive-big-changes-2023-06-4732281520-iot
5. Mohammed Aziz Al Kabir, Wael Elmedany, Mhd Saeed Sharif, Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques, Journal of Cyber Security Technology,2023, Volume 7(4), pp. 199-223.
6. AN1302: Bluetooth Low Energy Application Security Design Considerations in SDK v3.x and Higher, Silicon Laboratories. Retrieved from https://www.silabs.com/documents/public/application-notes/an1302-bluetooth-application-security-design-considerations.pdf
7. Karim Lounis, Mohammad Zulkernine. Bluetooth Low Energy Makes ”Just Works” Not Work. Cyber Security in Networking Conference, Oct 2019, Quito, Ecuador. Retrieved from https://hal.science/hal-02528877/document
8. Zhang, Jiansong, Zeyu Wang, Zhice Yang, and Qian Zhang, Proximity based IoT device authentication, 2017-IEEE conference on computer communications, 2017, pp. 1-9.
9. What Is a Man-in-the-Middle Attack? Definition, Detection, and Prevention Best Practices for 2022, Retrieved from https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

Педан С.І., Мельник М.В., Алєксєєв М.О., İnci Umakoğlu

Метод підвищення безпеки сполучення IoT пристроїв

Проблематика. Застосування технологій IoT забезпечує соціальний, технологічний та фінансовий розвиток суспільства. Хоча складні системи відіграють важливу роль в IoT, саме розробка, інтеграція та використання простих пристроїв насправді сприяє широкому впровадженню та впливу цієї технології. В той же час, забезпечення високого рівня безпеки простих IoT пристроїв є складною задачею по причині того, що обмеженість їх обчислювальних ресурсів та вимоги до низького енергоспоживання не дозволяють реалізувати більшість сучасних криптографічних протоколів. Найбільш критичним з точки зору безпеки є етап сполучення пристроїв, коли відбувається формування спільних ключів шифрування для встановлення захищеного каналу зв’язку.

Мета досліджень. Аналіз основних вразливостей процесу сполучення IoT пристроїв з обмеженими ресурсами та розробка методу підвищення безпеки цього процесу шляхом автентифікації пристроїв по близькості їх розташування та його стійкості проти відомих атак, таких як атака типу «людина посередині».

Методика реалізації. Методом підвищення безпеки процесу сполучення є автентифікація пристроїв по їх близькості основана на аналізі потужності безпровідного сигналу. Безпека методу автентифікації доказана аналітично, а також за допомогою результатів практичних досліджень залежності потужності сигналу від відстані та перешкод між пристроями.

Результати досліджень. Проведені дослідження показали, що запропонований метод дозволяє гарантувати автентифікацію користувача на близькій відстані та захист від атак зловмисника, який знаходиться на відстані не менше 10 метрів. Отримані теоретичні розрахунки та результати експериментів показують, що необхідний рівень підвищення потужності сигналу зловмисника, необхідний для успішної атаки, перевищує технічні можливості існуючих комунікаційних пристроїв.

Висновки. Робота присвячена актуальному питанню підвищення безпеки сполучення IoT пристроїв з обмеженими можливостями. Запропонований метод автентифікації IoT пристроїв по близькості їх розташування шляхом аналізу потужності безпровідного сигналу, що забезпечує стійкість процесу сполучення до атак типу «людина посередині». Приведені математичні розрахунки, на яких базується метод, були підтвердженні шляхом проведення ряду експериментів з дослідження зміни потужності безпровідного сигналу в залежності від відстані та типів перешкод між пристроями. Запропонований метод автентифікації може бути інтегрований до існуючого протоколу JustWorks для сполучення IoT пристроїв, що використовують BLE канал комунікації, у яких відсутні пристрої введення та виведення інформації.

Ключові слова: *безпека; автентифікація; Інтернет речей; атака типу «людина посередині»; Bluetooth Low Energy; JustWorks; RSSI.*