PRZEGLĄD TELEINFORMATYCZNY
No. 3-4, 2019

Device authentication methods in Internet of Things networks

Michał JAROSZ

Institute of Teleinformatics and Cybersecurity, Faculty of Cybernetics, MUT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warsaw, Poland
michal.jarosz@wat.edu.pl

ABSTRACT: The article describes the basic requirements of authentication systems used in Internet of Things networks, and problems and attacks that may hinder or even prevent the process of authentication. The current methods used in device authentication are also presented.

KEYWORDS: Internet of Things, IoT, device authentication, device identification

1. Introduction

The Internet of Things (IoT) is currently one of the fastest developing branches of IT. The Internet of Things means a distributed network connecting physical objects that can collect data from the environment (using sensors), interact with the environment (using actuators), and communicate with each other, other devices and computers. Data collected by these devices may be collected and analysed to develop actions resulting in savings, increased efficiency or improved products and services [5]. It is estimated that by 2021 there will be 21 billion IoT devices connected to the Internet [37], and one of the major challenges is to ensure proper device authentication [42]. This problem applies not only to Internet of Things devices used in industrial or medical environments, but also to devices in households.

The number of attacks on IoT devices is continuously growing; the reason is undoubtedly the increasing use of IoT devices in various environments, but also insufficient security of IoT devices [40]. According to respondents [34], the area that needs the most improvements is device authentication and authorisation.

Identification is a process in which an entity declares its identity. This is then followed by the authentication process. It checks whether the identity actually exists and whether the entity declaring the identity can use it [26]. The subject of this article is an Internet of Things device. The authentication process is important in the context of access control to secured resources.

The purpose of this article is to review the current methods applied in the authentication of devices used in Internet of Things networks. The second section shows examples of architecture models. The third section includes the requirements to be met by a system for authenticating Internet of Things devices. Problems and threats that occur in IoT device authentication systems are discussed (section 4) based on the four-layer architecture described in the second section. The next section (section 5) describes the current methods of device authentication in Internet of Things networks. The last section summarises the entire paper (section 6).

2. Architecture of Internet of Things systems

The system architecture shows how to divide a system into layers, each with defined functions and interactions with other layers. A model can be used to determine whether system elements of the same layer meet specific requirements. We can find many models in the literature on the construction of Internet of Things systems, but the most common architectures are as follows:

a) three-layer,
b) four-layer.

Figure 1 shows layers of the architecture models described. Other examples of architecture models are described in articles [25], [28] and [41].

Three-layer architecture [22] is the basic architecture model of Internet of Things systems. The first layer is the Perception Layer. This layer receives events from the external environment, such as temperature, humidity, speed or location. This is done using sensors that are built-in or connected to the device. The data received can be pre-processed by the device. Another layer is the Network Layer, whose task is to send data from the perception layer to the application layer. Data are transmitted by wire or wirelessly using technologies such as 3G, 4G, Wi-Fi, Zig-Bee, Bluetooth or LoRa. The last layer is the Application Layer. Elements of this layer are responsible for providing application-specific services to the user. The Application Layer does not participate in the authentication process, but may require device authentication.

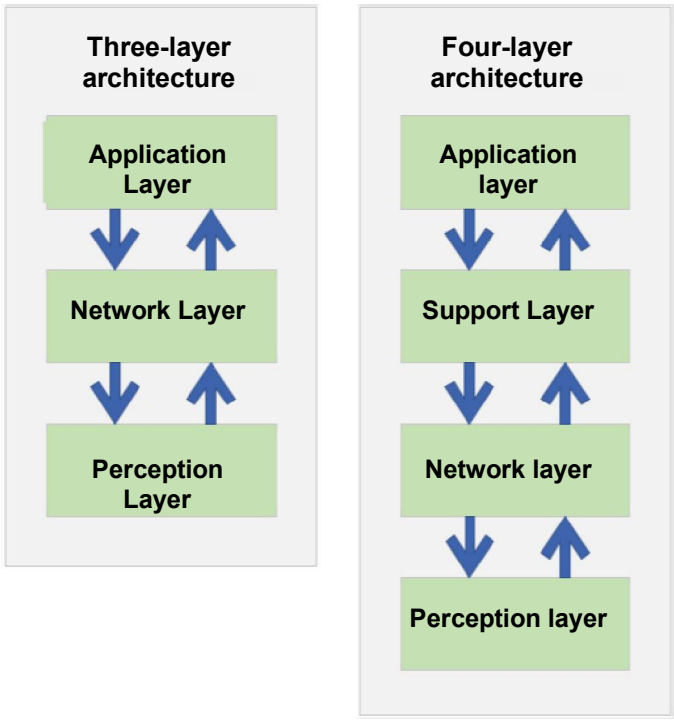

Fig. 1. Example models of Internet of Things system architectures

The four-layer architecture [39] is based on the three-layer architecture. It has the same layers as the three-layer architecture, but it features an additional Support Layer. This layer is responsible for processing and storing data received by sensors in the Perception Layer. These processes usually use cloud services, but can also be performed by a regular computer or disk array. The use of such services is advisable when Internet of Things devices do not have sufficient resources to carry out the task. This is the most common model in literature. The model is used later in this article, as it contains all the layers utilised in the authentication process.

3. Requirements for authentication systems

Authentication is a process confirming the identity of an entity or group of entities. For this purpose, the entity sends its identifier and element confirming the identity. Such an element can be [26]:

a) something known by the entity (e.g. password, PIN),
b) something owned by the entity (e.g. key, token),

c) something that the entity is (e.g. a signature based on the device network traffic),
d) entity location (physical location based on GPS or logical location based on an IP address, for example),
e) something the entity does (e.g. secret handshake).

Because the Internet of Things can consist of millions of devices, a very important requirement for the authentication system is the identifier uniqueness for the entity or group of entities. When two different entities present the same identifier, it may lead to a situation where entity A gains access to information intended for entity B, which of course is unacceptable. If the entity can be clearly identified through a device identifier or the data collected by the device, an appropriate level of privacy and protection of identifiers should be provided during their use and processing.

It should be ensured that the identifier is not changed during assignment, transfer or use [38]. The identifier must be human- and machine-readable and should not contain important information about the identified entity. It is also required to ensure the scalability of identifiers so that each device in the system receives its own identifier. It is impossible to specify in advance how many identifiers the authentication system should be able to process. Even simple environments could grow over time, and a change of the authentication system because of the limited number of processed identities means unnecessary problems. Devices come from different manufacturers and can send data to various applications (not necessarily belonging to the same organisation), so existing standards as well as limitations and capabilities of devices should be considered when developing an identifier generation system. The identifier assigner should keep track of which identifiers are used and which are not. By "disabling" unnecessary identities, it is possible to restrict network access for unauthorised devices.

The authentication process itself should be resistant to the attacks described in Part 4. In addition to these guidelines, we should keep the limitations of IoT devices in mind. These include:

- low memory capacity - the program to be executed by the device must fit into the memory in addition to the authentication system,
- low computing power - since many Internet of Things devices are equipped with processors with low computing power, authentication processes should be as fast as possible, meaning as few calculations as possible,
- low network bandwidth - Internet of Things networks use devices and protocols characterised by low power consumption. However, their limitation is low bandwidth. Therefore the device should send as little data as possible during authentication. It is also necessary to consider the

situation when the device does not have access to the Internet or an authentication server,

- the lowest possible energy consumption - Internet of Things devices can work in hard-to-reach environments where power cannot be supplied. Therefore, IoT devices are made of energy-saving components. It is essential that they are able to operate as long as possible on battery power. The authentication system should ensure the lowest possible CPU load, as far as possible, should not connect to third devices,
- inability to connect additional devices - since Internet of Things devices are small and do not have (or have few) additional ports, the authentication system should not use additional components. It should also be noted that the authentication system will be used in devices of various manufacturers, which may mean different output ports. In the event of a failure, the device can be replaced with another model or even a device from a different manufacturer.

The authentication system must not require a response from the operator, because IoT devices communicate themselves without human intervention. Credentials should be sent in encrypted form so that third parties cannot read them.

4. Problems and threats in authentication systems for Internet of Things devices

This section describes possible problems and attacks that occur in IoT device authentication systems. As mentioned earlier, a four-layer architecture model was used, as it contains all the layers necessary to present the threats. These attacks and problems are assigned to one layer, but some of them may also occur in other layers.

4.1. Support Layer

a. Storage attack - the authentication system can be based on an authentication server. The attack involves changing the credentials on the server or device. The result is the inability to authenticate the device or group of devices. The effects can be more severe if data replication is done between multiple authentication servers [4].
b. Malicious insider attack - an event when a person with authorised access to the system uses its privileges in a negative way. Such a person operates

within the network and most often has direct access to particular data of interest [4].

c. Disaster recovery - this problem occurs, for example, when the only authentication server fails and it needs to be restored. IoT devices cannot perform the authentication process during server recovery. This can be prevented by using at least 2 authentication servers, but it must be ensured that both have the same set of credentials and that the credentials are updated.
d. Brute force attack - obtaining credentials by checking all possible combinations. Rainbow tables can be used to save computing power.
e. Privacy - because Internet of Things devices can be assigned directly to a person, or the data obtained from the device can be used to clearly identify a person, the problem of credentials storage and anonymisation of data obtained from IoT devices should be taken into account.

4.2. Network Layer

a. Eavesdropping - this attack involves eavesdropping between Internet of Things devices or between a device and a server, and obtaining credentials or private data [4].
b. Replay attack - the attacker eavesdrops on the transmission between twos or between a device and a server to obtain credentials. Then the attacker tries to authenticate their data using the obtained credentials [4].
c. Denial of Service (DoS) - an attack preventing the provision of or access to services. It is usually done by sending a large number of requests to the device or by interfering with the transmission [6].
d. Man-in-the-Middle - the attacker acts as an intermediary between devices so that they do not know about its existence. The attacker can change the content of packets sent in real time [6].
e. Device heterogeneity - devices communicate with each other using different communication protocols, so it is important that the authentication system does not rely only on one communication protocol [1].

4.3. Perception Layer

a. Node capture - the attack consists in taking control of the device. If successful, the attacker can obtain credentials and also has network access with the privileges of the captured device [29].
b. Fake and malicious node - the attack involves adding an additional device to the organisation's Internet of Things network. The device sends fake

data. The purpose is to interfere with transmission in the organisation's network. The device added to the system may use the power supply of another node [4].

c. Node tempering - the attack involves replacing the device, changing the device elements to infected ones or adding infected elements to the device [6].
d. Sybil attack - a malicious node has multiple identities (new or taken over from other nodes). This way, it can send data as other nodes or participate in a voting process several times, for example [6].
e. Cryptanalysis - the field dealing with key recovery or data recovery before encryption. Attacks used in cryptanalysis include side-channel attacks [6], timing attacks [4] and brute force attacks.
f. Implementation errors - during implementation of the authentication system the programmer inadvertently makes errors in the code. The attacker can use exploit to take control of the device. In some cases, companies introduce errors into the developed systems on purpose (backdoor).
g. Configuration errors - errors made by people implementing the authentication system, e.g. weak passwords, many entities with the same password, vulnerable algorithms.
h. 0-day attack - the system has a security vulnerability unknown to the manufacturer. The vulnerability could be used to execute malicious code in a device. There is no universal form of protection against this group of attacks. One way to solve this problem may be providing the ability of using other cryptographic methods that are not susceptible to the discovered attack or enabling updates of software on the IoT device [4].

5. Device authentication methods in Internet of Things networks

Many methods of authenticating Internet of Things devices have been developed [7], [30], so this section presents only some of them, focusing on the properties of elements used in authentication systems.

Every IoT device should have its own unique identifier. This can be done manually by the user or the identifier is assigned automatically based on the device's features. If identifier is assigned manually to the device, the applicable standards can be applied, such as FIWARE (using the NGSI standard) or Watson IoT (Table 1). Identification standards are described in paper [10]. Automatic identification is carried out by analysing the device communication. An example of such identification is shown in articles [15], [33]. However, there are two problems with automatic identification based on a device communication analysis:

1) the device will probably not be identified correctly when it starts generating other traffic (e.g. updates),

2) this method is not suitable when there are several identical devices performing the same task in the network.

Table 1. Types of identifiers used in Watson IoT[1]

Customer Type	ID	Identifier Format
Applications	a	a:orgId:appId
Scalable applications	A	A:orgId:appId
Devices	d	d:orgId:deviceType:deviceId
Gateways	g	g:orgId:typeId:deviceId

Based on [35]

Some authentication systems are designed to be used only in specific cases, e.g. for medical purposes [2], [27] or in a smart home [17]. The advantage of personalised systems is the selection of appropriate methods and components for the task. For example, in the case of device authentication in a medical environment, the authentication system is adapted to better data protection compared to IoT devices in a home environment, but the latter may operate faster.

Authentication may apply to not only one communication party, but to both. When only one party is authenticated, it is called a one-way authentication, whereas authentication of both parties of communication is a two-way authentication. There may also be a situation in which a trusted third party is used for authentication (three-way authentication). The disadvantage of three-way authentication might be the increased number of packets to be generated and processed by an IoT device. The best option is to use two-way authentication - then both parties are sure that the data sent comes from a device that has permission to send data and that the data go to a trusted place.

Authentication can be based on:

1) context,
2) identity.

Ad. 1) Context-based authentication has been described to some extent at the beginning of this part of the article. A device is authenticated according to its physical characteristics or behaviour. In the previously described case, the researchers have shown that identification can be based on the analysis of the device's network transmission. Then the data are used to create a fingerprint for the authentication process.

[1]orgId - organisation identifier; appId - application identifier, deviceId - device identifier (e.g. serial number), deviceType - device type identifier, typeId - gateway type identifier

Ad. 2) In this type of authentication, the device sends or uses an additional element it owns in addition to the identifier. The simplest element is the password/key. However, its main disadvantage is the distribution of a new password/key, e.g. when the old password has been cracked. The key-based authentication method is used in the Directed Path Based Authentication Scheme (DPAS) [18]. The solution to the problem of long-term use of the same password for authentication may be one-time passwords [24]. One-time passwords are changed after each use. The use of one-time passwords[2] presented in paper [24] is resistant to replay attacks and cryptanalysis methods. Asymmetric cryptography can be used instead of passwords. However, it requires more computing power than symmetric cryptography. When using asymmetric cryptography instead of the RSA algorithm, many researchers have been experimenting with elliptic curve cryptography (ECC) [20], [31]. The authentication scheme presented in article [31] is resistant to replay attacks. RSA is considered a safe algorithm since it is based on the factoring of large numbers. The security of elliptic curve cryptography is based on the computational complexity of discrete logarithm search on elliptic curves. In the case of IoT devices, algorithms are based on elliptic curves, because the key used for encryption is shorter than in RSA, with the same security level [36]. The generated keys are used in HMAC *(*keyed-hash message authentication code) [19], [23]. The authentication method presented in paper [19] is resistant to brute force attacks and Men-in-the-Middle attacks. The authentication method presented in paper [23] is resistant to Man-in-the-Middle attack, DoS and cryptanalysis (including side-channel attack). In addition to asymmetric cryptography in HMAC, researchers also create their own systems [17]. The system described in article [17] is resistant to DoS attacks (DDoS), Men-in-the-Middle attacks, replay attacks and brute force attacks.

Public key infrastructure is used instead of keys only, so that public key authenticity is ensured. Examples of authentication systems for Internet of Things devices using public key infrastructure are presented in papers [21] and [32]. The authentication method presented in paper [32] is resistant to node tempering and cryptanalysis. However, in the event of a DoS attack (DDoS), such infrastructure can authenticate the compromised device, even when the certificate has already been revoked. Certificate-based device authentication is also used in the DTLS protocol applied in Internet of Things systems [11].

The element used in the authentication process can also be generated by means of hardware. This is done through a Trusted Platform Module (TPM) [8]. Such a module is responsible for operations involving cryptography (key

[2] Information about vulnerabilities and resistance to attacks has been taken from the cited articles. Many more examples of authentication systems with a list of their vulnerabilities are presented in [7].

generation and storage, encryption). Also, each module has its own unique and secret RSA private key and unique identifier. Naturally, the given IoT device must be equipped with a TPM module. A less popular solution is Physical Unclonable Function (PUF) [14]. PUF is a physical structure made at the chip production stage, which cannot be cloned or changed. It is completely random and is not known even to the manufacturer. The structure generates a response to a signal (request) sent to it. A device is authenticated according to a request-response pair. Using PUF reduces the risk of device cloning because it is impossible to create two identical PUF modules. In some solutions we can find weak PUFs, such as SRAM PUF, which is not unidirectional and mathematically unclonable [3]. They are also vulnerable to numerous attacks (some of which are described in [16]). Instead, it is recommended using strong PUFs, which can generate multiple request-response pairs. There are also systems that feature a unique serial number that can be connected to an IoT device, such as the Maxim DS2411 system. It is used in the authentication scheme presented in paper [9]. The disadvantage of such a system is that its serial number can be read and then used via a program (without involving the module) in another device, which makes it easier to replace an IoT device with another one.

Tables 2 and 3 show the main advantages and disadvantages of authentication systems utilising different elements.

Authentication systems featuring an identifier with an additional element to confirm identity should be used whenever possible. This ensures greater certainty as to the device identity.

6. Conclusion

The article presents the methods of device authentication in Internet of Things networks. Two models of the Internet of Things system architecture have been described in the initial sections. Based on the architecture model, it is easier to identify problems and threats in the authentication systems of Internet of Things devices. A proper threat identification is one of the basic elements of risk analysis in the system design process. Attacks and problems that may pose a threat to device authentication systems in Internet of Things networks have been described based on the four-layer architecture. The article also presents the basic requirements for an identifier and the authentication system itself in relation to Internet of Things devices. The last part shows the properties and methods used in the current authentication systems, including their advantages and disadvantages. It has been described which attacks a given authentication scheme is susceptible to in the mentioned authentication systems.

Credentials are usually stored in a database or file. Recently, there have been many articles using distributed registers [12], [13]. The advantages of distributed registers include decentralization, invariability of stored data and data replication between nodes. As presented in the introduction, the intense development of the Internet of Things forces users to utilise effective and secure authentication systems. Therefore, it is important to continue research on authentication systems and cryptographic protocols for such devices.

Literature

[1] ALI I., SABIR S., ULLAH Z., *Internet of Things Security, Device Authentication and Access Control: A Review*. International Journal of Computer Science and Information Security, Vol 14, No 8, 2016, pp. 456-466.

[2] ALMULHIM M., ZAMAN N., *Proposing secure and lightweight authentication scheme for IoT based E-health applications*. 2018 20th International Conference on Advanced Communication Technology (ICACT), 2018, pp. 481-487.

[3] BRAEKEN A., *PUF Based Authentication Protocol for IoT*. Symmetry 2018, 10 (8), 352, 2018, pp. 1-15.

[4] BURHAN M., REHMAN R., KHAN B., BYUNG-SEO K., *IoT Elements, Layered Architectures and Security Issues: A comprehensive Survey*. Sensors 2018, pp. 1-37.

[5] DAVIES R., *The Internet of Things – Opportunities and challenges*. European Parliamentary Research Service, 2015, pp. 1-8.

[6] DEOGIRIKAR J., VIDHATE A., *Security Attacks in IoT: A Survey*. International Conference on I-SMAC, 2017, pp. 32-37

[7] FERRAG M.A., MAGLARAS L.A., JANICKE H., JIANG J., *Authentication Protocols for Internet of Things: A Comprehensive Survey*. Hindawi, Security and Communication Networks, Vol. 2017, 2017, pp. 1-41.

[8] FURTAK J., ZIELIŃSKI Z., CHUDZIKIEWICZ J., *Procedures for sensor nodes operation in the secured domain*. Concurrency and Computation: Practice and Experience, 2019, Vol. 0, pp. 1-13.

[9] HASAN A., QUERSHI K., *Internet of Things Device Authentication Scheme using Hardware Serialization*. 2018 International Conference on Applied and Engineering Mathematics, 2018, pp. 109-114.

[10] KOO J., OH S.-R., KIM YG., *Device Identification Interoperability in Heterogeneous IoT Platforms*. Sensors 2019, 2019, pp. 1-16.

[11] KOTHMAYR T., SCHMITT C., HU W., BRÜNIG M., CARLE G., *A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication*. Local Computer Networks Workshops, 2012, pp. 956-963.

Table 2. Advantages and disadvantages of authentication systems

Element	Advantages	Disadvantages	Comments
Context	+ IoT device does not require configuration.	- The device can change "its behaviour", such as communication, and then authentication could fail. - It is possible to generate similar network traffic to pretend to be another device.	
Password/key	+ Simple implementation. + Symmetric cryptography is fast.	- Problem of redistributing a new password/key. - The password/key must be stored by the transmitting and receiving devices.	• Passwords can be easy to crack because they are shorter than keys and are not always created at random.
One Time Password	+ The password is used only once. + Resistant to many attacks, including replay attacks.	- In the case of access to a device with a software password generator, it is possible to clone the generator.	

Table 3. Advantages and disadvantages of authentication systems - continued

Component	Advantages	Disadvantages	Comments
RSA, ECC	+ No key distribution problem.	- Slower than symmetric cryptography. - Public key is not authenticated. - Requires more computing power than symmetric cryptography.	
Certificate (PKI)	+ Ensures public key authentication. + Ensures non-repudiation. + Easy identity management.	- Slower than symmetric cryptography. - Communication with a trusted third party is required, e.g. to track the list of revoked certificates.	• Uses asymmetric cryptography.
TPM	+ Secure storage of cryptographic keys. + Hardware-based generation of keys, random numbers.	- A special module is required. - Module damage prevents device authentication.	
PUF	+ Unclonable. + Not susceptible to physical attacks.	- A special module is required. - They may have a high bit error rate.	• Strong PUFs recommended.
Serial number	None.	- Additional module required. - Does not protect against device replacement.	

[12] LAU C., YEUNG A., YAN F., *Blockchain-based Authentication in IoT Networks*. 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018, pp. 1-8

[13] LEE C., KIM K., *Implementation of IoT System using BlockChain with Authentication and Data Protection*. 2018 International Conference on Information Networking (ICOIN), 2018, pp. 936-940.

[14] MAES R., VERBAUWHEDE I., *Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions*. Towards Hardware-Intrinsic Security, 2010, pp. 1-37.

[15] MEIDAN Y., BOHADANA M., SHABTAI A., GUARNIZO J.D., OCHOA M., TIPPENHAUER N.O., ELOVICI Y., *ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis*. SAC `17 Proceedings of the Symposium on Applied Computing, 2017, pp. 506-509.

[16] MUKHOPADHYPAY D., *PUFs as Promising Tools for Security in Internet of Things*. IEEE Design & Test, Volume 33, Issue 3, 2016, pp. 103-115.

[17] NICANFAR H., JOKAR P., LEUNG V., *Smart Grid Authentication and Key Management for Unicast and Multicast Communications*. 2011 IEEE PES Innovative Smart Grid Technologies, 2011, https://ieeexplore.ieee.org/document/6167151

[18] NING H., LIU H., LIU Q., JI G., *Directed Path Based Authentication Scheme for the Internet of Things*. Journal of Universal Computer Science vol. 18, no. 9, 2012, pp. 1112-1131.

[19] RABIAH A., RAMAKRISHNAN K., LIRI E., KAR K., *A Lightweight Authentication and Key Exchange Protocol for IoT*. Workshop on Decentralized IoT Security and Standards 2018, 2018, pp. 1-6.

[20] SCHIMTT C., NOACK M., STILLER B., *TinyTO: Two-way Authentication for Constrained Devices in the Internet-of-Things*. Internet of Things, 2015, pp. 239-258

[21] SCHUKAT M., CARTIJO P., *Public key infrastructures and digital certificates for the Internet of things*, 2015 26th Irish Signals and Systems Conference (ISSC), 2015, https://ieeexplore.ieee.org/abstract/document/7163785

[22] SETHI P., SARANGI S.R., *Internet of Things: Architectures, Protocols, and Applications*. Journal of Electrical and Computer Engineering, 2017, pp. 1-25.

[23] SHAH T., VENKATESAN S., *Authentication of IoT Device and IoT Server Using Security Vaults*. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2017, pp. 819-824.

[24] SHIVRAJ V., RAJAN M., SINGH M., BALAMURALIDHAR P., *One time password authentication scheme based on elliptic curves for Internet of Things (IoT)*. 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015, pp. 1-6.

[25] SPIESS P. I INNI, *SOA-based Integration of the Internet of Things in Enterprise Services*. 2009 IEEE International Conference on Web Services, 2009, pp. 968-975.

[26] STEWART J.M., *CompTIA Security+ Review Guide*. Sybex, Indianapolis, 2014.

[27] TASALI Q., CHOWDHURY C., VASSERMAN E., *A Flexible Authorization Architecture for Systems of Interoperable Medical Devices.* SACMAT`17, 2017, pp. 9-20.

[28] TORKAMAN A., SEYYEDI M.A., *Analyzing IoT References Architecture Model*. International Journal of Computer Science and Software Engineering, Volume 5, Issue 8, August 2016, pp. 154-160.

[29] TRIPATHY B.K., ANURADHA J., *Internet of Things (IoT) Technologies, Applications, Challenges and Solutions*. CRC Press, Boca Raton, 2017.

[30] TRNKA M., CERNY T., STICKNEY N., *Survey of Authentication and Authorization for the Internet of Things*. Hindawi, Security and Communication Networks Volume 2018, 2018, pp. 1-17.

[31] WANG K.H., CHEN C.M., FANG W., WU T.Y., *A secure authentication scheme for Internet of Things*. Pervasive and Mobile Computing 42, 2017, pp. 15-26.

[32] WON J., SINGLA A., BERTINO E., BOLLELLA G., *Decentralized Public Key Infrastructure for Internet-of-Things*. Milcom 2018 Track 5, 2018, pp. 1-7.

Electronic sources

[33] ALUTHGE N., *IoT device fingerprinting with sequence-based features*, 2017, https://helda.helsinki.fi/handle/10138/234247 (accessed on 12.05.2019)

[34] *An overview of the IoT Security Market Report 2017-2022*, https://iiot-world.com/reports/an-overview-of-the-iot-security-market-report-2017-2022/ (accessed on 12.05.2019)

[35] *Connecting applications, devices and gateways*, IBM, https://www.ibm.com/support/knowledgecenter/en/SSQP8H/iot/platform/reference/security/connect_devices_apps_gw.html (accessed on 12.05.2019)

[36] ECC 101: What is ECC and why would I want to use it?, https://www.globalsign.com/en/blog/elliptic-curve-cryptography/ (accessed on 20.06.2019)

[37] *Gartner Identifies Top 10 Strategic IoT Technologies and Trends,* https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends, 2018 (accessed on 12.05.2019)

[38] *Identifiers in Internet of Things*, Alliance for Internet of Things Innovation, Version 1.0, 2018, https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf, (accessed on 10.05.2019)

[39] Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Network. Overview of the Internet of things, TELECOMMUNICATION STANDARIZATION SECTOR OD ITU, 2012, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items (accessed on 12.05.2019)

[40] *The Internet of Things (IoT) – Threats and Countermeasures*, https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/ (accessed on 12.05.2019)

[41] *The Internet of Things Reference Model*, Cisco 2014, http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (accessed on 10.05.2019)

[42] Top 10 IoT security challenges, https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/, 2017 (accessed on 12.05.2019)

Sposoby uwierzytelniania urządzeń w sieciach Internetu Rzeczy

STRESZCZENIE: W artykule opisano podstawowe wymagania systemów uwierzytelniania stosowanych w sieciach Internetu Rzeczy oraz problemy i ataki, które mogą utrudnić lub nawet uniemożliwić przeprowadzenie procesu uwierzytelniania. Przedstawiono również obecne metody stosowane w uwierzytelnianiu urządzeń Internetu Rzeczy.

SŁOWA KLUCZOWE: Internet Rzeczy, IoT, uwierzytelnianie urządzeń, identyfikacja urządzeń

Received by the editorial staff on: 12.07.2019