ISSN 2347 - 3983
Volume 7, No. 9 September 2019
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter11792019.pdf
https://doi.org/10.30534/ijeter/2019/11792019

Threat Model for IoT Systems on the Example of OpenUNB Protocol

Aleksander Shelupanov[1], Anton Konev[2], Tatiana Kosachenko[3], Danil Dudkin[4]
[1] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, saa@fb.tusur.ru
[2] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, kaa1@keva.tusur.ru
[3] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, 6takos9@gmail.com
[4] Tomsk State University of Control Systems and Radioelectronics, Russian Federation, 725_ddg@fb.tusur.ru

ABSTRACT

The popularity growth of the Internet of Things (IoT) in various areas of life leads to an increase in the number of cyberattacks on this type of system. The construction of a cyberattack protection system begins with a simulation of security threats. Most approaches are based on listing possible attacks on the system. In this article a systematic list of threats aimed at the IoT system based on the developed methodology for constructing a threat model is proposed. As an example, the protocol for wireless data transmission OpenUNB is used. The list of threats includes threats of information transmitted and processed in the system, as well as threats to system elements. The resulting list complements the existing threat models for distributed information systems.

Key words: information security, threat model, IoT, security threat, information system

1. INTRODUCTION

Building an IoT system is a fairly non-trivial task, especially when it comes to industrial scale, so unexpected technologies, such as blockchain and intrusion detection systems trained on the basis of random subspaces, are often used in the development [1]. A well-designed IoT network must meet five different security criteria. It is useful to note that not all leading IoT platforms contain the following properties, and the constant increase in the speed of technological progress along with the transition to new technologies, such as 5G, constantly modifies and supplements the list of problems related to information security [2]. This makes the criteria listed below rather recommendations than requirements. However, this does not negate the fact that consideration of them in the design of any IoT solution makes sense from the point of view of information security [3].

The authentication process provides the system with the ability to identify objects included in it, which is the key mechanism for the operation of the algorithm of any system that involves the processing of confidential data, including both ordinary local network services [4] and large-scale cluster systems [5]. In the context of IoT, the generated data can lead to a number of security and privacy issues. This is especially true for authentication between IoT nodes. Thus, three subcriteria of authentication should be taken into account: the authentication protocol between the IoT devices and the IoT platform, between the IoT platform and users (including ordinary users and the administrator), as well as between the components of the IoT platform itself.

The encryption process prevents unauthorized entities from accessing sensitive data. Due to the amount of information and the limited resources of the IoT devices, encryption is fundamental. Thus, when designing an IoT system, it is necessary to focus on two different aspects: encryption of data stored on target devices, and encryption of data transmitted between system entities.

After the user has been successfully authenticated in the system, the authorization process determines whether this user has rights to access a specific resource or to perform certain actions [6]. As with authentication, authorization is essential in the IoT ecosystem, as the actions of unauthorized attackers can lead to a number of negative consequences [7]. Authorization also implies two subcriteria: user authorization for performing actions within the IoT platform and authorization of IoT devices for performing operations between components of the IoT platform.

Records should be kept of the resources that an individual user consumes during access to the system (e.g., session time or sent/received data during a session). Given the volume of operations carried out within the IoT platform, this criterion is important for system security. Its subcriteria include: accounting for operations that the user performs on data and IoT devices, as well as accounting for operations performed by IoT services components on data and IoT devices.

Detection of abnormal activities means the ability of the system to detect anomalies among normal activities that can signal a security incident. In the context of the Internet of things, we are talking about the platform's ability to detect anomalies in the state of the IoT service or in the normal operation of its components.

A preliminary step to determine the security measures implemented in the IoT system is to determine the list of existing threats. To create a threat model you can use threat libraries, e.g., threat data banks, which include a database of vulnerabilities, as well as a list and description of cyber threats that are most typical for particular information systems. It is the threat modeling that allows the selection of an effective architecture for the protection system of information processes taking place in the system.

2. LITERATURE REVIEW

There are various design methods for IoT systems [8,9]. Depending on the structure of the system, various approaches are being developed, based mainly on assumptions about possible attacks on the system, to identify threats. For example, Anton V. Uzunov et al. rely in their studies on a two-level systematics of threats. The first level of taxonomy includes the following threats: identity attacks, network communication attacks, network protocol attacks, passing illegal data, stored data attacks, remote information inference, loss of accountability, uncontrolled operations. The second level of taxonomy includes cryptography attacks, countermeasure design, configuration/administration.

The concept of a threat pattern is presented in [10], and some threat taxonomy are also discussed. Then the authors put forward the basic systematics of threats for distributed systems and discuss patterns of specializations and instantiations, as well as build a separate systematics for peer-to-peer systems.

The description of SCADA system sensors, as well as the key properties of information security (confidentiality, accessibility, integrity), is presented in [11]. After this an analysis of threat models is carried out in order to form a base of requirements for determining the conditions necessary for successful attacks on the system and calculating the consequences. The authors of the article also determine the most effective practices for designing secure sensor networks.

A listing of the basic principles by which the classification of threats is carried out, as well as a short list of classification of threats, followed by a description of the multi-dimensional classification put forward by the authors as a new model of security threats, are presented in [12].

Researchers from the Department of computer science, Tunisia, identify the following threats: destruction of information, corruption of information, disclosure of information, theft of service, denial of service, elevation of privilege, illegal usage.

A combination of threat library and taxonomy values was proposed in [13] in the form of an extended two-level taxonomy based on templates for distributed systems. And also simple threat models was developed, for example: Location Verification System (LVS) [14].

A threat model for an electricity metering system with classification of threats aimed at information processes and the information system is presented in [15].

3. THREAT MODEL FOR OPENUNB PROTOCOL WIRELESS DATA TRANSMISSION

During the analysis of system security, most approaches involve considering each of its elements separately from the entire system (e.g., only a base station or subscriber unit). Despite the fact that this approach can help in ensuring information security, this does not exclude the likelihood of security threats in situations of interaction between individual system components.

Different protocols [16,17,18] suggest different methods of system architecture. The protocol under study presents a network architecture consisting of two types of devices: a subscriber device, a base station, and a server for data processing (resp., Figure 1).

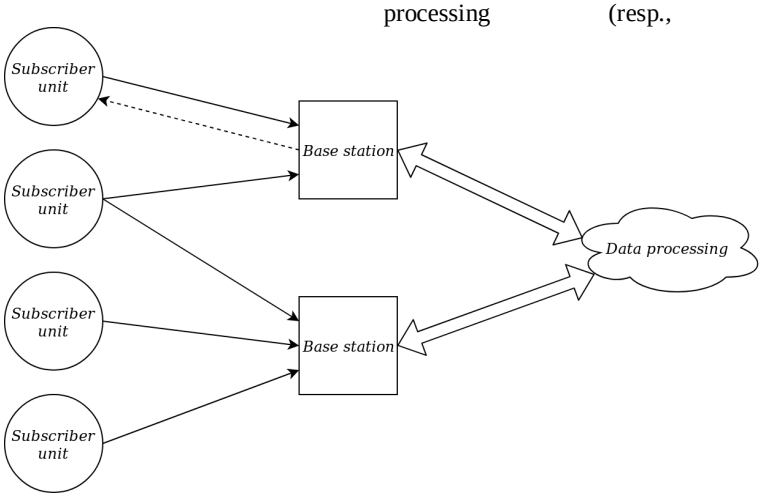

Figure 1: Network architecture

The base station consists of a receiver of data from subscriber devices and a computer for processing the received data. At the request of the customer, the base station can be additionally equipped with a transmitter for sending data to subscriber devices.

The subscriber unit consists of a microcontroller with connected sensors and a transmitter for sending the collected data to the base station.

The following elements of the system are distinguished:
- subscriber device;
- subscriber device firmware;
- control device (base station);

- protocol driver on the base station;
- protocol driver on the server;
- base station operating system;
- server.

Figure 2 shows a threat model. Each information flow of the network model is depicted as a one-way/two-way arrow and symbolizes the direction of information transfer.

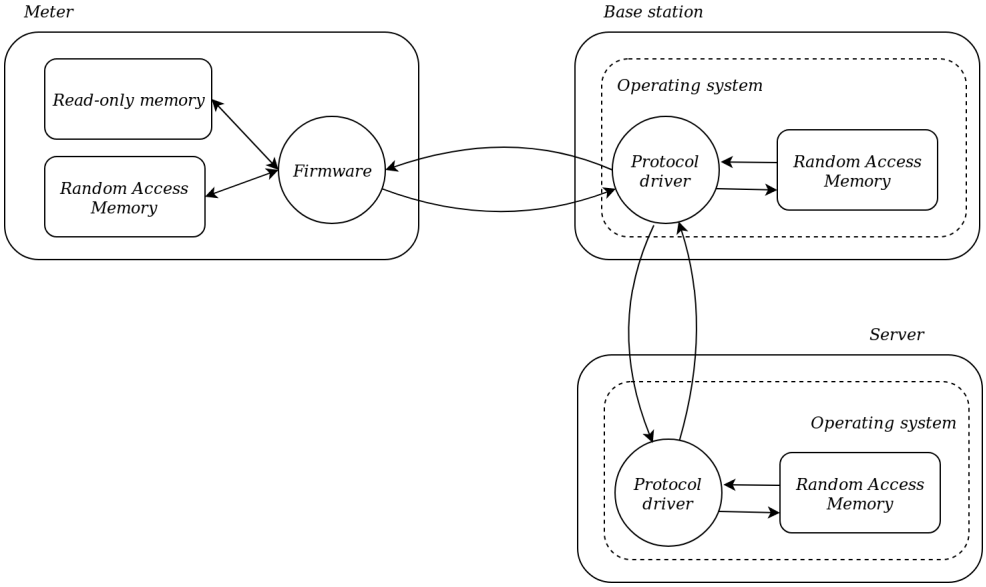

Figure 2: IoT system model

Data security implies a state of data security, in which their confidentiality, availability and integrity are ensured. This approach involves the analysis of the system in terms of three basic properties of information:

- confidentiality;
- integrity;
- availability.

The construction of a threat model based on the approach [19] took place in three stages:

1.definition of the list of threats for each information flow existing in the system;

2.defining protection mechanisms and their sufficiency for each existing information flow;

3.compiling a list of recommendations for eliminating unclosed threats in the system for each existing information flow.

Therefore, the following information processes are characteristic of this system:

- data transmission from the subscriber device to the control device (base station);
- data transmission from the base station to the end device;
- reading data from the RAM of the subscriber device;
- writing data to the RAM of the subscriber device;
- reading data from non-volatile memory of the subscriber device;
- writing data to non-volatile memory of the subscriber device;
- reading data from the base station RAM;
- writing data to the RAM of the base station;
- reading data from the non-volatile memory of the base station;
- writing data to the non-volatile memory of the base station;
- data transfer from the server to the base station;
- data transfer from the base station to the server;
- reading data from server RAM;
- writing data to server RAM;
- reading data from non-volatile memory of the server;
- writing data to the non-volatile memory of the server.

Further, threats were identified for each information flow. These threats are divided into three categories (resp., Table 1):

- privacy threats;
- threats to integrity;
- availability threats.

The main threats aimed at the system were also highlighted (resp., Table 2). The list of threats is based on the model proposed in [20].

Table 1: Threat model of information processed in the system

№	Threats	Information flow between BS (base station) and SU (subscriber unit)	Information flow between firmware and ROM of SU	Information flow between firmware and RAM of SU	Information flow between the driver and RAM of BS	Information flow between BS and Server	Information flow between the driver and server RAM

	Privacy						
1	Unauthorized sending of data to the second element of a pair	Sending data to unauthorized SU	Writing data to the public memory area of the SU's ROM	Writing data to a public memory area of SU's RAM	Writing data to a public area of BS's RAM	Sending data to an unauthorized server	Writing data to a public memory area of server RAM
2	Unauthorized sending of data to the first element of a pair	Sending data to an unauthorized BS	Read unauthorized software information from SU's ROM	Unauthorized reading of information from SU's RAM	Read unauthorized software information from BS's RAM	Sending data to an unauthorized BS	Read unauthorized software information from server RAM
3	Data interception	Interception and analysis of traffic between BS and SU	Data Recovery from SU's ROM	Data Recovery from SU's RAM	Recovery of data from BS's RAM	Interception and analysis of traffic between BS and Server	Data recovery from server RAM
4	Sending of data by unauthorized protocol	Using an unauthorized protocol to transfer information between a BS and an SU	Writing data to the ROM of the SU using an unauthorized driver	Writing data to the RAM of the SU using an unauthorized driver	Writing data to the RAM of the BS using an unauthorized driver	Using an unauthorized protocol to transfer information between BS and Server	Writing data to server RAM using an unauthorized driver
	Integrity						
5	Data destruction	Channel failure or congestion	Overwriting the ROM area of SU	Overwriting the RAM area of SU	Overwriting the ROM area of BS	Failure or congestion of the channel between the BS and the Server	Overwriting the RAM area of server
6	Sending false data to the first element of a pair	Duplication of information on the BS	Write false data to ROM of the SU	Write false data to RAM of the SU	Write false data to ROM of the BS	Duplication of information on the server	Write false data to server RAM
7	Sending false data to the second element of a pair	Duplication of information on the SU	Reading false information from ROM of the SU	Reading false information from RAM of the SU	Reading false information from ROM of the BS	Duplication of information on the BS	Reading false information from server RAM
8	Change intercepted network packets in the first element of a pair	Interception, modification and sending information to the BS	Writing a modified part of the data to the ROM of the AU	Writing a modified part of the data to the RAM of the AU	Writing a modified part of the data to the ROM of the BS	Intercepting, changing a network packet and sending information to the server	Recording a modified network packet data in server RAM

9	Change intercepted network packets in the second element of a pair	Interception, modification and sending information to the SU	Reading the changed part of information from ROM of the SU	Reading the changed part of information from RAM of the SU	Reading the changed part of information from ROM of the SU	Interception, modification and sending information to the BS	Reading the changed network packet of information from the RAM of the server
10	Interference	Distortion of information during transmission over the communicatio n channel between the BS and the SU	Errors during writing to ROM of the SU	Errors during writing to RAM of the SU	Errors during writing to ROM of the BS	Distortion of information during transmission over the communicat ion channel between the BS and the server	Errors during writing to RAM of the server
	Availability						
11	Channel failure	Disconnect a communicatio n channel between BS and SU	Disabling the driver in SU's ROM	Disabling the driver in SU's RAM	Disabling the driver in BU's ROM	Disabling the communicat ion channel between BS and Server	Disabling the server RAM driver
12	Channel overload	Processing a large number of requests, transferring a large amount of information in the channel between the BS and the SU	Sending and processing a large number of requests	Sending and processing a large number of requests	Sending and processing a large number of requests	Processing a large number of requests, transferring a large amount of information in the channel between BS and server	Sending and processing a large number of requests in server RAM

Table 2: Threats to the system

№	A threat	BS	SU	Server	Communication Protocol between SU and BS - OpenUNB	Communication protocol between BS and server - TCP / IP
13	Disconnect / failure of the device / communication channel	BS shutdown / failure	SU shutdown / failure	Server shutdown / failure	Disabling the communication channel between the SU and the BS	Disabling the communication channel between the BS and the server
14	Device / Driver Substitution	Substitution of the BS / BS's driver	Substitution of the US / US's driver	Substitution of the Server / Server driver	Data transfer between SU and BS via unauthorized protocol	Data transfer between BS and server using an unauthorized protocol

15	Change device settings / protocol settings	Change BS settings	Change US settings	Change Server settings	Changing the configuration of the data transfer protocol between the SU and the BS	Changing the configuration of the data transfer protocol between the BS and the server
16	Adding an unauthorized device / communication channel	Adding an unauthorized BS	Adding an unauthorized US	Adding an unauthorized Server	Adding an information leakage channel to SU / BS	Adding an information leakage channel to the BS / server

4. COMPARATIVE ANALYSIS

In the considered methods for designing threat models, the authors identify the following threats to the security of the system:

- unauthorized sending of data to the first element of a pair of devices;
- unauthorized sending of data to the second element of a pair of devices;
- element of a pair of devices;
- signal interception and analysis;
- data transmission by unauthorized protocol;
- data destruction;
- sending false data to the first element of a pair of devices;
- sending false data to the second element of a pair of devices;
- interference;
- channel overload.

These threats intersect with the types of threats that are mentioned in foreign sources. Thus, type 1, 2, 6, 7 threats represent an extended and decomposed version of the threat of the Passing illegal data, type 3 threat is a threat of the Network communication attack, type 4 threat is a threat of the Network protocol attacks, and type 12 threat is a threat of the Denial of service (resp., Table 1). Type 5 threat is the threat of the Destruction of information, and Corruption of Information is type 10 threat in the proposed model. For type 8, 9, 11, 13, 14, 15, 16 threats no analogues were found in other sources.

All types of security threats listed above are considered in our proposed threat model. At the same time, the model developed by us considers in more detail the types of threats relating to each individual element of the system, which suggests that the proposed model provides a more complete description of the types of threats to which the system in question is exposed.

5. CONCLUSION

In this review, 72 types of threats to information processed in the system and 20 types system-targeted threats were identified. Compared with other threat modeling methods, the proposed method covers the entire list of threats to which the OpenUBN protocol wireless data transmission system is exposed.

Not all of the listed threats are relevant for this system, however, drawing up a complete list of all possible threats to which this system is exposed is the first step in determining the actual threats.

The proposed methodology can be used to determine the requirements for an information security system or to form a set of technical and organizational information security measures in various systems, such as IoT systems.

This research was funded by the Ministry of Education and Science of Russia, Government Order no. 2.8172.2017/8.9 (TUSUR).

REFERENCES

1. A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, **Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security**, *Sensors*, 2019, Article DOI 10.3390/s19143119, available at https://www.researchgate.net/publication/334413208_Blockchain_and_Random_Subspace_Learning-based_IDS_for_SDN-enabled_Industrial_IoT_Security
2. R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, **A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions**, *Journal of Network and Computer Applications*, 2019, Article DOI 10.3390/sym10120669, available at https://www.sciencedirect.com/science/article/pii/S1084804517302266?via%3Dihub
3. D. D. López, M. B. Uribe, C. S. Cely, D. T. Murgueitio, E. G. Garcia, P. Nespoli, and F. G. Mármol, **Developing Secure IoT Services: A Security-Oriented Review of IoT Platforms**, *Symmetry*, 2019, Article DOI 10.1016/j.jnca.2017.07.002, available at https://www.researchgate.net/publication/329219367_Developing_Secure_IoT_Services_A_Security-Oriented_Review_of_IoT_Platforms
4. E. B. Panganiban, **Microcontroller-based Wearable Blood Pressure Monitoring Device with GPS and SMS Feature through Mobile App**, *International Journal of Emerging Trends in Engineering Research*, vol.7, no.6, pp.32-35, 2019.
5. E. Rehman, M. Sher, S. H. A. Naqvi, K. B. Khan, and K. Ullah, **Secure Cluster-Head Selection Algorithm Using Pattern for Wireless Mobile Sensor Networks**,

Tehnički Vjesnik, 2019, Article ISSN 1330-3651, available at https://doaj.org/article/f4bb34e0a63941f39dfa871eb0c45d3c

6. A. Konev, A. Shelupanov, and N. Egoshin, **Functional scheme of the process of access control: Methodology for the formation of normative documents on the access control**, in *RPC 2018 - Proceedings of the 3rd Russian-Pacific Conference on Computer Technology and Applications*, 2018, DOI 10.1109/RPC.2018.8482179, available at https://ieeexplore.ieee.org/document/8482179
7. A. E. Yankovskaya, A. A. Shelupanov, and V. G. Mironova, **Construction of hybrid intelligent system of express-diagnostics of information security attackers based on the synergy of several sciences and scientific directions**, *Pattern Recognition and Image Analysis*, vol.26, iss.3, pp. 524–532, 2016.
8. S. V. R. K. Rao, M. S. Devi, A.R.Kishore, and P. Kumar, **Wireless sensor Network based Industrial Automation using Internet of Things (IoT)**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol.7, no.6, pp.82-86, 2018.
9. Dr. J. S. Bhanu, Dr. JKR Sastry, P. V. S. Kumar, B. V. Sai, and K. V. Sowmya, **Enhancing Performance of IoT Networks through High Performance Computing**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol.8, no.3, pp.432-442, 2019.
10. A. V. Uzunov, and E. B. Fernandez, **An extensible pattern-based library and taxonomy of security threats for distributed systems**, *Computer Standards & Interfaces*, vol.36, iss.4, pp.734-747, 2014.
11. A. A. Cardenas, T. Roosta, and S. Sastry, **Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems**, *Ad Hoc Networks*, vol.7, iss.8, pp.1434-1447, 2009.
12. M. Jouini, L. Ben Arfa Rabai, and A. Ben Aissa, **Classification of security threats in information systems**, *Procedia Computer Science*, vol.32, pp.489-496, 2014.
13. A. V. Uzunov, and E. B. Fernandez, **An extensible pattern-based library and taxonomy of security threats for distributed systems**, *Computer Standards & Interfaces*, vol.36, pp.734–747, 2014.
14. S. Yan, R. Malaney, I. Nevat, and G. W. Peters, **Optimal Information-Theoretic Wireless Location Verification**, *arXiv*:1211.0737v2 [cs.IT], 2013.
15. D.S. Nikiforov, A.A. Konev, M.M. Antonov, and A.A. Shelupanov, **Structure of information security subsystem in the systems of commercial energy resources accounting**, in *Journal of Physics: Conference Series*, 2019, DOI 10.1088/1742-6596/1145/1/012018, available at https://iopscience.iop.org/article/10.1088/1742-6596/1145/1/012018
16. P. Singh, and N. S. Gill, **A Secure and Power - Aware Protocol for Wireless Ad Hoc Networks**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol.8, no.1, pp.34-41, 2019.
17. D. Rani, and N. S. Gill, **Lightweight Security Protocols for Internet of Things: A Review**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol.8, no.3, pp. 707-719, 2019.
18. A. Pradhan, and B. Sen, **A brief study on Contention Based Multi-Channel MAC Protocol for MANETs**, *International Journal of Emerging Trends in Engineering Research*, vol.6, no.12, pp.74-78, 2018.
19. A. Shelupanov, O. Evsyutin, A. Konev, E. Kostyuchenko, D. Kruchinin, and D. Nikiforov, **Information Security Methods—Modern Research Directions**, *Symmetry*, 2019, Article DOI 10.3390/sym11020150, available at https://www.mdpi.com/2073-8994/11/2/150
20. A. Novokhrestov, and A. Konev, **Mathematical model of threats to information systems**, in *AIP Conference Proceedings*, 2019, Article DOI 10.1063/1.4964595, available at https://aip.scitation.org/doi/10.1063/1.4964595