Usage of Threat Modelling Tools for Implementation of ICT Security Standards in IoT Environments

Dalibor Dobrilovic [1], and Rade Dragović,[2]

[1] *University of Novi Sad, Technical Faculty "Mihajlo Pupin" Đure Đakovića b.b., Zrenjanin, 23000, Serbia*
[2] *Institute for standards and technology, Resavska 28, Belgrade, 11000, Serbia*

Abstract

The development of microcontrollers, communication, and sensor technologies resulted with the growing implementation of the Internet of Things (IoT) in various environments. The nature of IoT assumes the complexity of the system. The complexity of the system increases the number of system elements and therefore increases the system vulnerabilities. As a result, it is important to find an efficient and easy-to-use methodology for implementing security standards in newly designed IoT systems. This paper introduces the usage of threat modeling tools for modeling IoT systems and identifying the threats for the modeled systems. The identified threats are further embedded in the framework designed to define and enable the implementation of IoT security standards. The framework is demonstrated in the example of a simple IoT system designed for urban pollution, and noise monitoring.

Keywords

Threat modeling, threat modeling tools, Risk assessment, IoT security implementation framework, ISO security standards implementation, Internet of Things (IoT)

1. Introduction

The growing implementation of the Internet of Things (IoT) in various environments increases the general ICT security risks. The IoT environments being heavily involved in the life of users of its benefits greatly increase the security risks for the individuals using those systems or their services. The complexity of the system and the number of its components and devices give numerous possibilities of system misuse, data compression, and other forms of threats. Therefore, it is highly important to define an easy-to-use and efficient framework for identifying threats and defining the implementation of security standards within the process of designing the system.

This paper introduces the framework based on the usage of threat modeling tools for modeling IoT systems and identifying the threats for the modeled systems. The identified threats are further analyzed to define the implementation of IoT security standards. The methodology is presented on the example of a simple IoT system designed for urban pollution, and noise monitoring.

This paper is structured as follows. After the Introduction and Related Works sections, the modeled IoT system architecture is described, followed by threat modeling and threat analyses. The approach in risk assessment is then presented using the results and reports of threat modeling, thus explaining the proposed framework. At the end, the conclusions are given.

2. Related Work

According to the Open Worldwide Application Security Project (OWASP) [1] the threat modelling is the process taken to identify, communicate, and understand threats and mitigations within the context of protecting something of value. A threat model is a structured representation of all the information

6th International Workshop on Information, Computation, and Control Systems for Distributed Environments (ICCS-DE 2024), July 01–05, 2024, Irkutsk, Russia

EMAIL: dalibor.dobrilovic@tfzr.rs (A. 1); rade.dragovic@instate.biz (A. 2);
ORCID: 0000-0002-3083-5725 (A. 1); 0000-0002-0215-4076 (A. 2);

ICCS-DE 2024 Workshop Proceedings
DOI: 10.47350/ICCS-DE.2024.06

that affects the security of an application. There is a variety of threat modeling methods such as: STRIDE, Process for Attack Simulation and Threat Analysis (PASTA), Trike, Visual, Agile, and Simple Threat (VAST), Attack Trees, Common Vulnerability Scoring System (CVSS), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Quantitative Threat Modeling Method (QTTM), DREAD, MITRE, LINNDUN etc. [2] The STRIDE, a method named on six security threats categories (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges) is the most popular and widely supported by the modeling tools.

In the following text will be presented several works in the area of IoT threat modeling. In [3] the authors utilize the STRIDE threat modeling methodology and the Microsoft Threat Modeling Tool to identify threats present in smart city infrastructure. Authors map offenses, possible evidence sources, and types of threats identified to help investigators understand what crimes could have been committed.

In [4] authors propose an approach aimed at supporting the security analysis of an IoT system with an almost completely automated process for threat modeling and risk assessment. The evaluation of its effectiveness is given for the application of a home automation system. The proposed methodology relies upon a modeling approach of both the architectural components of an IoT system and its security properties.

The contribution presented in [5] identifies and describes current security threats in IoT based on a generic IoT architecture and the main communication protocols that are used in the application, transport, network, and physical layer.

In the paper [6], a general-purpose methodology for assessing the risk is proposed for end-to-end systems. The approach covers static and dynamic features/components of an IoT system. The presented solution is evaluated within the real prototype implementation.

A similar approach for modeling IoT system threats is applied to the threat modeling on the container ecosystem. STRIDE is used as a threat modeling framework. [7]

3. IoT System Architecture

In this section, the general architecture of IoT systems will be described. IoT systems commonly can be presented as multi-layer systems, and the five-layer architecture of IoT systems is one of the most accepted [8]. The IoT system consists of the following layers.

The **Perception Layer** has the same functions as the Physical Layer of the OSI reference model. Sensor nodes or end devices are deployed on this layer. Sensors collect data, i.e. physical parameters of the environment. **The Network Layer** (or the Transport Layer) is designed to establish a connection to the core of the system and its components such as network devices and to transfer data collected by sensors. It is responsible for transferring sensor data from the perception layer to the Processing Layer and vice versa. For this purpose, mainly short and medium-range wireless technologies are used.

The **Processing Layer** or **Middleware Layer** is responsible for analyzing and processing collected data, storing it, and creating reports. This layer includes various technologies such as relational and non-relational databases, cloud computing, big data, etc. The application layer is responsible for delivering data to users and their visualization through user applications and devices. Finally, **The Business Layer** is on top of the system and provides the information needed for system management, business and profit model development, and data protection.

An urban IoT system designed as a sensor network for monitoring traffic noise and meteorological parameters in an urban environment [9] is presented in this section and used for further modeling and framework implementation. Figure 1 a) shows the devices of the first two layers of the IoT system. On the perception layer (I) there are sensor devices (1) for air pollution, weather conditions, and noise monitoring, Wi-Fi access point (AP) devices (2) for connecting sensor nodes with short-range Wi-Fi technology, and Wi-Fi Fi/LoRa gateway devices (3) for connecting (collecting) Wi-Fi APs in a wider area and connecting to the cloud part of the system using longer-range connection technology. Communication components use a combination of TCP/MQTT and LoRa protocols.

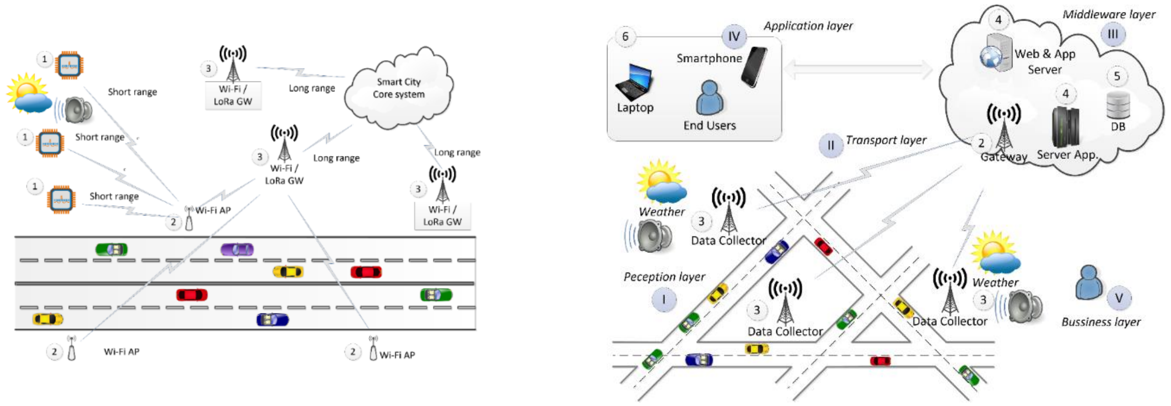


Figure 1: a) the IoT urban monitor system peripheral elements; b) layers of IoT urban monitoring IoT system

The middleware layer (III) contains a server (4) that can be installed on several servers (e.g. Data Analyzes and Application Server) or in a simplified version on one computer and a database (5). The application layer contains APIs for user applications (6) for various devices (mobile phones, laptops, desktops, etc.). The whole system is shown in Figure 1 b).

4. IoT threat modeling

Microsoft Threat Modeling Tool (MTMT) is used for described IoT threat modeling. The modeled system is shown in Fig. 2 a) in a simplified version. The elements of the system are labeled in the same way as in Fig. 1 b) with Roman (I, II, III, IV) and Arabic numerals (1, 2, 3, 4, 5, 6).

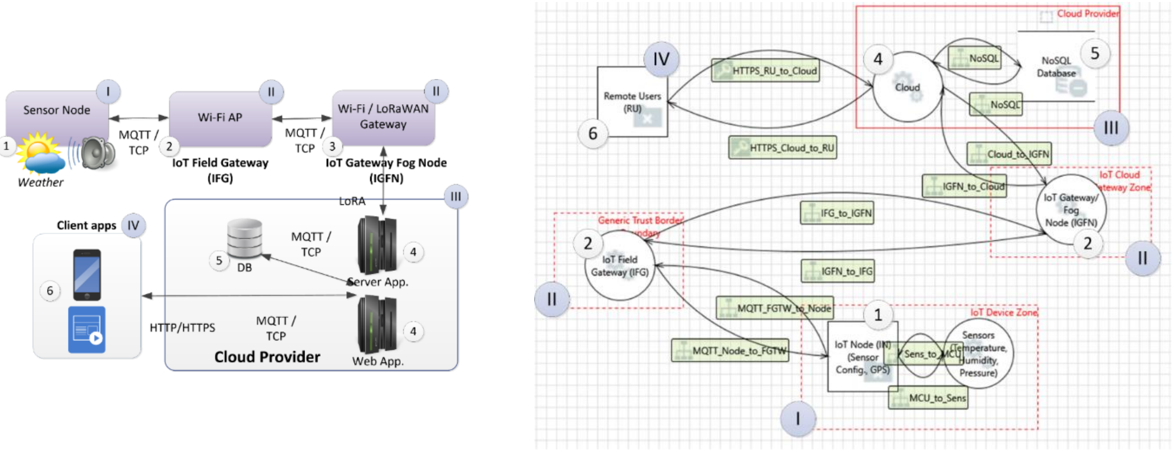
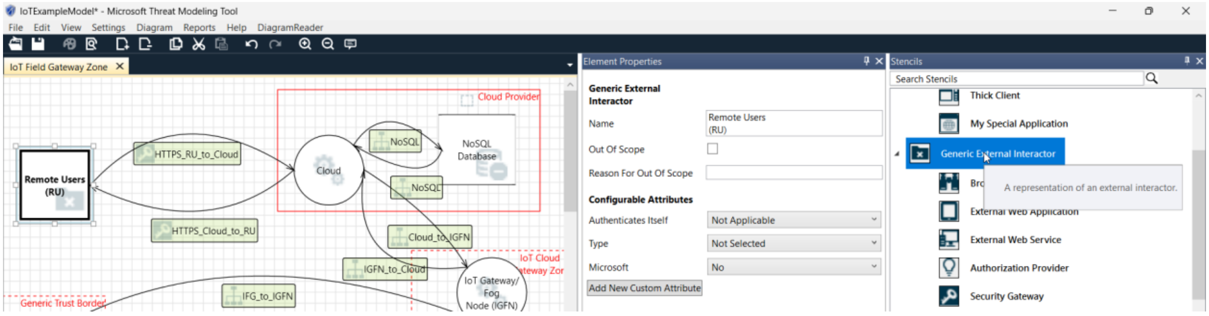


Figure 2: a) Modeled IoT system; b) Model of the system in threat modeling tool.

To model the sensor nodes (1), the *Generic External Interactor* is used in MTMT from the Stencils palette. Parameters can be set in the Element Properties palette as is shown in Fig. 3. If other devices in the External Interactor list correspond to the system being modeled, e.g. mobile phone (Smart Phone) or Browser, these devices can also be selected from the same stencil.



Element Properties

Generic External Interactor

Name: Remote Users (RU)

Out Of Scope: □

Reason For Out Of Scope:

Configurable Attributes

Authenticates Itself: Not Applicable

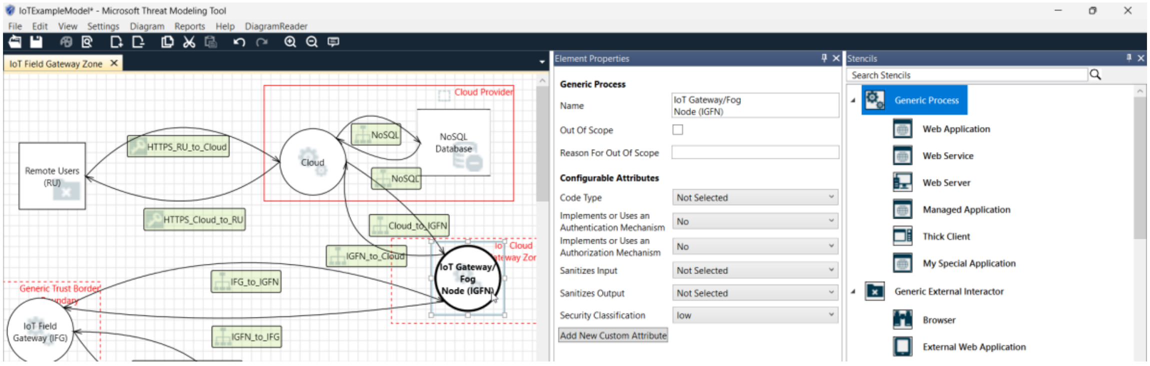
Type: Not Selected

Microsoft: No

Add New Custom Attribute

Figure 3. Use of the Interactor object

To model the Wi-Fi AP (2) and the Wi-Fi/LoRa Gateway device (3) the *Generic Process* is used (Fig. 4.). The *Generic Process* is also used to model the server (4), while the *Generic Data Store* is used to model the Database (5).



Element Properties

Generic Process

Name: IoT Gateway/Fog Node (IGFN)

Out Of Scope: □

Reason For Out Of Scope:

Configurable Attributes

Code Type: Not Selected

Implements or Uses an Authentication Mechanism: No

Implements or Uses an Authorization Mechanism: No

Sanitizes Input: Not Selected

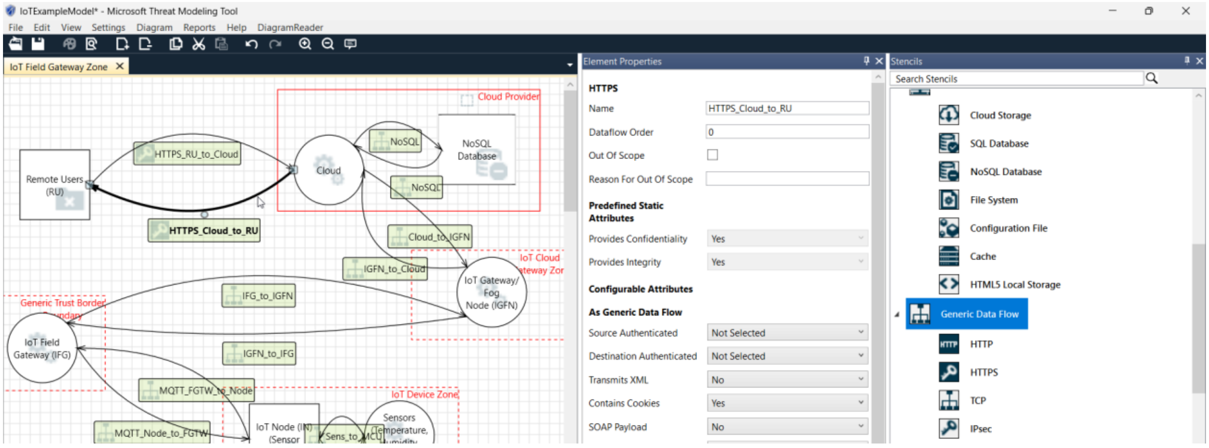
Sanitizes Output: Not Selected

Security Classification: low

Add New Custom Attribute

Figure 4. Use of the Process object

To model the data flow, a *Generic Data Flow* is used. An example of the HTTP protocol is shown in Fig. 5. The same element can be used for MQTT or another protocol and to model the data flow between the sensor and the MCU (microcontroller). Since the sensors are directly connected to the MCU there is no issue of insecure transmission, so the data flow can be checked as *Out of Scope* in the Element Properties palette.



Element Properties

HTTPS

Name: HTTPS_Cloud_to_RU

Dataflow Order: 0

Out Of Scope: □

Reason For Out Of Scope:

Predefined Static Attributes

Provides Confidentiality: Yes

Provides Integrity: Yes

Configurable Attributes

As Generic Data Flow

Source Authenticated: Not Selected

Destination Authenticated: Not Selected

Transmits XML: No

Contains Cookies: Yes

SOAP Payload: No

Figure 5. Using the Data Flow object for the HTTP protocol

Finally, modeling confidence limits, i.e. of separate system elements in which data is protected more than the external space, is done with the *Generic Trust Boundary* object in the Stencils palette, and it is represented in figures with dashed red lines.

4.1. Threat analysis

Threat analysis is performed by clicking on the menu option *Reports > Create Full Report*. To create a report, it is necessary to activate the *Generate Report* option, after which a report with the extension .htm will be created. The part of the report is the threat list, which can be exported to CSV format using the *Switch To Analysis View* option (Table 1).

Table 1
Partial view on exported threat list

Id	Title	Category	Interaction	Priority	Description
47	Elevation Using Impersonation	Elevation Of Privilege	IGFN_to_IFG	High	IoT Field Gateway (IFG) may be able to impersonate the context of IoT Gateway/Fog Node (IGFN) in order to gain additional privilege.
46	Elevation Using Impersonation	Elevation Of Privilege	IFG_to_IGFN	High	IoT Gateway/Fog Node (IGFN) may be able to impersonate the context of IoT Field Gateway (IFG) in order to gain additional privilege.
45	Elevation Using Impersonation	Elevation Of Privilege	Cloud_to_IGFN	High	IoT Gateway/Fog Node (IGFN) may be able to impersonate the context of Cloud in order to gain additional privilege.
44	Elevation Using Impersonation	Elevation Of Privilege	IGFN_to_Cloud	High	Cloud may be able to impersonate the context of IoT Gateway/Fog Node (IGFN) in order to gain additional privilege.
16	Elevation Using Impersonation	Elevation Of Privilege	MQTT_FGTW_to_Node	High	IoT Field Gateway (IFG) may be able to impersonate the context of IoT Node (IN) (Sensor Config., GPS) in order to gain additional privilege.

Threat analysis for the modeled generic IoT system gives the following identified threats classified into six categories (Table 2).

Table 2
The number of threats by category

No.	Threat	Count
1	**S**poofing	7
2	**T**ampering	6
3	**R**epudiation	8
4	**I**nformation Disclosure	6
5	**D**enial Of Service	6
6	**E**levation Of Privilege	12
	Total	**45**

5. Risk assessment

In this section, we will describe the basics of risk assessment. The basic steps are to identify Score, Context, and Criteria as a basis for establishing a framework for the information security management system. A system of early identification of threats and vulnerabilities must be established, and it must react predictively and not preventively. All the time, it is necessary to follow all identified interested parties, both those who have good intentions for the organization's system and those who have different intentions and initiatives.

Risk assessment is the next phase which must consist of risk identification, risk analysis, and risk evaluation. Risk identification is a detailed and long-term job that must identify each and every individual risk, regardless of whether it represents a higher or lower level of risk at the time of identification. This step uses the input from threat modeling explained in the previous section.

The professional framework for risk analysis is represented by the following standards:

- *ISO/IEC 27005* - Information security, cybersecurity, and privacy protection - Guidance on managing information security risks and
- *ISO 31000* - Risk management - Guidelines.

Risk analysis must consider all identified risks from the aspect of likelihood, and consequences and calculate risk levels. All three mentioned criteria must be set in such a way that the analysis observes and projects in real-time with a large knowledge base that is the basis for calculating parameter values.

A risk evaluation must provide a clear answer to a question that is not just a simple number but a multidimensional framework that shows trends and every single evaluation parameter in real-time.

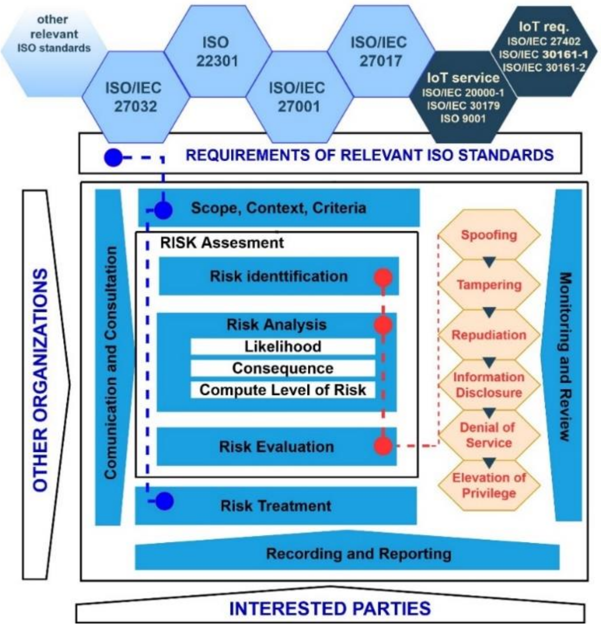


Figure 6: RISK assessment (based on ISO 27005) extended with STRIDE cycle and ISO requirements

STRIDE is a threat modeling methodology used to identify potential security threats in a system and develop appropriate countermeasures. It is an acronym for six types of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE threat modeling is connected to the stages of Risk assessment.

Risk treatment as the next phase is mainly oriented towards acting according to each individually identified requirement of the ISO standard within the matrix. The knowledge acquired in the process of treating risks during the management of the information security system is a significant source for further analysis using the principles of machine learning and artificial intelligence.

STRIDE, threat modeling methodology cannot be established by simply adopting a good methodology, but it needs to be placed alongside existing risk treatment methodologies and in a specific environment that is analyzed by defining the requirements by adopting the requirements of certain specific standards for each specific environment. There is no magic wand that will solve the problems of information security, On the contrary, a complex, multi-layered, and multi-dimensional framework must be established that will require a complete and detailed analysis of the system using a process approach and a complete analysis of threats, vulnerabilities, and risks. The mentioned activity is not a one-time activity but represents a cyclical repetition of the identified elements in each subsequent time parameter that is partially (and in some elements completely) different from the previous one. There are two basic misconceptions that need to be removed from the thinking of the multidisciplinary team: the input parameters for the risk treatment are immutable, and the risk treatment model is immutable. The presented model RISK assessment (based on *ISO 27005*) extended with STRIDE cycle and ISO requirements is an example of a basic layer developed on many years of experience in the field of information security.

5.1. Identification of ISO requirements for information security and IoT

The initial framework for action in the domain of information security is defined within the requirements of the following standards:

- *ISO/IEC 27001*: Information security, cybersecurity and privacy protection - Information security management systems - Requirements,
- *ISO/IEC 27701*: Security techniques - Extension to *ISO/IEC 27001* and *ISO /IEC 27002* for privacy information management - Requirements and guidelines,

- *ISO/IEC 27011*: Information security, cybersecurity and privacy protection - Information security controls based on *ISO/IEC 27002* for telecommunications organizations,
- *ISO/IEC 27032*: Cybersecurity - Guidelines for Internet security,
- *ISO/IEC 22301*: Security and resilience - Business continuity management systems - Requirements and
- *ISO/IEC 20000-1*: information technology - Service management - Service management system requirements

Within enlisted requirements of the standard, it is certainly and inevitably necessary to treat the requirements of the *ISO 9001*: Quality management systems - Requirements standard in the domain of detailed and complete analysis of opportunities and risks as part of a complete and detailed analysis of the organization's processes.

A detailed risk analysis of the process is the place where threats, vulnerabilities, and risks must be fully defined, with a clear and complete connection to the parameters of the information system. It is especially important to respect the dynamism of changes in the initially identified parameters, connections, importance, and influence within the previously defined frameworks. A complete analysis of the process through the implementation of *ISO 9001* requirements is the first and basic phase of the successful design of an information system that bases information security on risk management [10].

From this initial phase, must be established a clear risk matrix that is related to specific process entities and risks at the base level. The implementation of the requirements of the *ISO/IEC 27032* standard through the formation of a Cyber Security Program must be carried out for the entire organization, including all components of information systems through business and IT functions, given the fact that attacks and threats to the information security system can appear from every side and in every moment. It is necessary to implement the requirements of the standards *ISO/IEC 27001*, *ISO/IEC 27701*, *ISO/IEC 27032*, *ISO/IEC 20000-1*, and *ISO/IEC 22301* in areas that include security in the intranet/internet space, i.e. intranet/internet security issues that focus on bridging the results of risk analysis between different domains of information security in the intranet/internet space.

According to the stated standards, it is necessary to implement technical guidelines for solving intranet/internet security risks, including social engineering attacks, hacking, spyware, and attacks using potentially malicious malware software. These technical guidelines should provide controls for the treatment of all identified risks, including controls for preparing responses to attacks from malicious software (malware), reactions to detected unusual events related to information security and monitoring the attack architecture. It is necessary to create a framework for efficient and effective information exchange, coordination, and incident management among related stakeholders in the predictively defined cyberspace of the organization. Interested parties that may be involved are employees, customers, and third parties, which may be different types of organizations or individuals, as well as providers, which include service providers as well as all those identified by the risk matrix.

The analysis of interested parties should not be limited only to cyberspace but should perform a complete analysis of the technological, procedural, and organizational framework, not neglecting the social and other specific general security aspects of the organization.

The corrective reaction is not a satisfactory achievement. The preventive reaction is satisfactory only in the process of implementation of the system. Predictive response is a target function that must be established in the system.

On the example of the identification of threats, vulnerabilities, and risks within the requirements of the *ISO/IEC 27001* standard, the same methodological basis should be established for the requirements of the *ISO/IEC 27701*, *ISO/IEC 27032*, and *ISO/IEC 27011* standards, as well as for the requirements of the *ISO/IEC 20000-1* and *ISO 22301*.

Special attention should be directed to the identification of IoT needs. The initial framework for IoT identification is covered by the following standards:

- *ISO/IEC 27402*: Cybersecurity - IoT security and privacy - Device baseline requirements,
- *ISO/IEC 30161-1*: Internet of Things (IoT) - Data exchange platform for IoT services - Part 1: General requirements and architecture,
- *ISO/IEC 30161-2*: Internet of Things (IoT) - Data exchange platform for IoT services Part 2: Transport interoperability between nodal points,

- *ISO/IEC 30179:2023*: Internet of Things (IoT) - Overview and general requirements of IoT system for ecological environment monitoring, but also other specifically identified for individual system.

6. Conclusion

The framework for the implementation of ISO ICT security standards in IoT systems is presented in this paper. Along with the set of standards that should be implemented to achieve security in IoT environments, the recommendations for their implementation are given. Also, the usage of threat modeling tools for modeling IoT systems and identifying the threats for the modeled systems is presented. The reports of the IoT systems threat modeling are used as input values for a given framework. The proposed methodology is illustrated on the example of a simple IoT system designed for urban pollution, and noise monitoring.

7. References

[1] V. Drake, OWASP, Threat Modeling, Retrieved May 2024. URL: https://owasp.org/www-community/Threat_Modeling.

[2] A. Konev, A. Shelupanov, M. Kataev, V. Ageeva, A. Nabieva, A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats. Symmetry. 2022; Vol. 14(3):549. https://doi.org/10.3390/sym14030549

[3] Y. C. Tok, S. Chattopadhyay, Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling, Forensic Science International: Digital Investigation, Vol. 45, 2023, 301540, https://doi.org/10.1016/j.fsidi.2023.301540.

[4] V. Casola, A. De Benedictis, M. Rak, U. Villano, Toward the automation of threat modeling and risk assessment in IoT systems, Internet of Things, Vol. 7, 2019, 100056,https://doi.org/10.1016/j.iot.2019.100056.

[5] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, I. Kantzavelou, IoT: Communication protocols and security threats, Internet of Things and Cyber-Physical Systems, Vol. 3, 2023, pp 1-13, https://doi.org/10.1016/j.iotcps.2022.12.003.

[6] S. Sicari, A. Rizzardi, D. Miorandi, A. Coen-Porisini, A risk assessment methodology for the Internet of Things, Computer Communications, Vol. 129, 2018, pp 67-79, https://doi.org/10.1016/j.comcom.2018.07.024.

[7] A. Y. Wong, E. G. Chekole, M. Ochoa, J. Zhou, On the Security of Containers: Threat Modeling, Attack Analysis, and Mitigation Strategies, Computers & Security, Vol. 128, 2023, 103140, https://doi.org/10.1016/j.cose.2023.103140.

[8] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications”, Journal of Electrical and Computer Engineering, Vol. 2017, 25 pages, https://doi.org/10.1155/2017/9324035

[9] D. Dobrilović, V. Brtka, G. Jotanović, et al. The urban traffic noise monitoring system based on LoRaWAN technology. Wireless Networks, Vol. 28, pp 441–458, 2022, https://doi.org/10.1007/s11276-021-02586-2

[10] R. Dragović, D. Dobrilovic, D. Dragović (2022, September). Recommendations for the Creation of Usable Critical Infrastructure for the Delivery of Priority Services of State Bodies. In IFIP International Conference on Human Choice and Computers (pp. 161-171). Cham: Springer Nature Switzerland. DOI:10.1007/978-3-031-47990-8_15