Computer network threat modelling

A Novokhrestov, A Konev, A Shelupanov and A Buymov
Tomsk State University of Control Systems and Radioelectronics, 40 Lenina Pr., 634050 Tomsk, Russia

E-mail: nak@fb.tusur.ru

Abstract. The paper discusses methods for constructing threat models of information systems and computer networks. The disadvantages of existing approaches are highlighted. The authors propose an approach to building a computer network model, as well as describing threats to information and the system. The proposed approach takes into account the identified shortcomings of existing solutions and is aimed at reducing the impact of the subjective opinion of an expert when compiling lists of threats.

1. Introduction

Continuous development of information technologies and, in particular, computer networks entails the emergence of new types of threats [1]. According to a study by Positive Technologies, in 2018, as part of an external penetration testing, the network perimeter of 92 percent of companies was breached [2]. Moreover, new technologies appear, such as the Internet of things, and the issues of ensuring their security cannot be ignored [3, 4].

Ensuring network security plays a significant role for any organization, although the resources allocated to security can vary significantly. This affects not only the quality of technical equipment, but also the qualifications of specialists working in the organization. The professional level, as well as the subjective opinion of the expert when using existing approaches to describing threats, significantly affects the final result [5].

Thus, the task of developing an effective methodology for describing threats to information security is relevant. The main requirement for such a technique is to minimize the influence of a professional level and the subjective opinion of an expert assessing security.

Currently, the creation of such a technique is carried out at Tomsk University of Control Systems and Radioelectronics as part of the creation of a comprehensive approach to assessing the security of the information systems [6]. In the course of work, the following tasks were identified that needed to be solved:

1. It is necessary to analyze existing computer network models and approaches to building threat models used in compiling threat lists.
2. Develop a computer network model that allows to describe the structure of the system at a level of detail sufficient to compile a list of threats.
3. Develop a computer network threat model that takes into account the maximum possible number of threats.
4. Using the developed models, create a methodology that allows you to put these models into practice to determine lists of threats to real systems.

This article discusses existing approaches to describing threats and describes proposed models for identifying threats to the security of information and systems. Currently, the aim of the study is to increase the number of identified threats. At the same time, issues of determining the relevance of threats and further risk analysis remain outside the scope of work.

2. Literature Review

Existing approaches to identifying and classifying threats can in turn be classified in many ways. So, in [7] methods for constructing threat models are distinguished as based on a description of an attacker, a description of attacked resources, or a description of software. This classification includes the STRIDE threat model [8], privacy tools, attack trees, and attack libraries.

In [9], the authors consider the threat classification problem and various approaches to its solution. They divide the methods for classifying threats into two main groups:

1. Based on attack methods;
2. Based on the impacts of threats.

We cannot ignore the fact that the concepts of "classification of threats" and "modeling of threats" in the context of different works can differ. By classification is meant a description of the characteristics of threats [9]. Threat modeling involves defining a list of security threats used to assess risks [10].

Threat classification methods are often used in the threat modeling process. If there is a classification, it is easier for a specialist to navigate the existing threats. This approach to threat modeling is considered high-level. However, using only the classification of threats, it is difficult to obtain a detailed list of threats that can be used to build a protection system. An example of such an approach is [11].

Approaches in which threats are described in detail are considered low-level. They can be based on the list of attacks [12, 13] or the list of attack scenarios [14]. Some approaches come down to analysis of exploitation of vulnerabilities in the system [15]. The problem with low-level approaches is the frequent confusion of the concepts of threat, attack and vulnerability.

In [16], the authors proposed an approach that has the features of a high and low level approach. The work is aimed at describing the impact of the class of threats, and not the impact of the threat, since the threat changes over time. However, the presented version lacks formalization for its effective application in practice.

The lack of formalization is a problem in many works, which leads to the possibility of ambiguous interpretation of approaches. Existing works aimed at formalization consider attacks rather than threats [17]. For formalization, the mathematical apparatus of graph theory is usually used.

We should also mention the work related to threat modeling for IoT systems. Most approaches are based on considering possible attacks on the system. For example, 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 and administration. In [18], the authors put forward a basic systematics of threats to distributed systems and discuss patterns of specializations and concretizations, as well as build a separate taxonomy for peer-to-peer systems.

In [19], the analysis of threat models is aimed at creating a base of requirements for determining the conditions necessary for the successful implementation of attacks on the system and calculating the consequences. The authors of the article also determine the best practices for the design of secure sensor networks of SCADA systems.

Based on the analysis of work on modeling threats to information systems, a list of key shortcomings of existing approaches was compiled that need to be addressed:

1. Inconsistent description of threats within the same model. Within the framework of one threat model, at one level of abstraction, there can exist a generalized description of threats, as well as a description of particular cases that can be included in general.

2. Lack of separation of threats into those aimed at the system and aimed at information. None of them explicitly describe threats to the information system. All attention is paid to security threats of information processed in the information system.

3. Lack of repeatability. Significant influence of professional level and subjective opinion of an expert.

4. Each of the considered models can take into account certain threats that are not described in others.

3. Proposed approach

The approach to building a protection system based on protection against threats allows us to consider the structure of the protection system at the level of "Type of threat - Type of line of defense". Then the classification of methods and means of protection is reduced to the following types, presented in Figure 1:

1. Protection of information and its carriers from threats to confidentiality, integrity and availability;

2. Protection of information system elements, including software and hardware for information protection, and their settings from threats to confidentiality and integrity;

3. Protection responsible for monitoring the implementation of the rules for working with protected information and software and hardware protection.

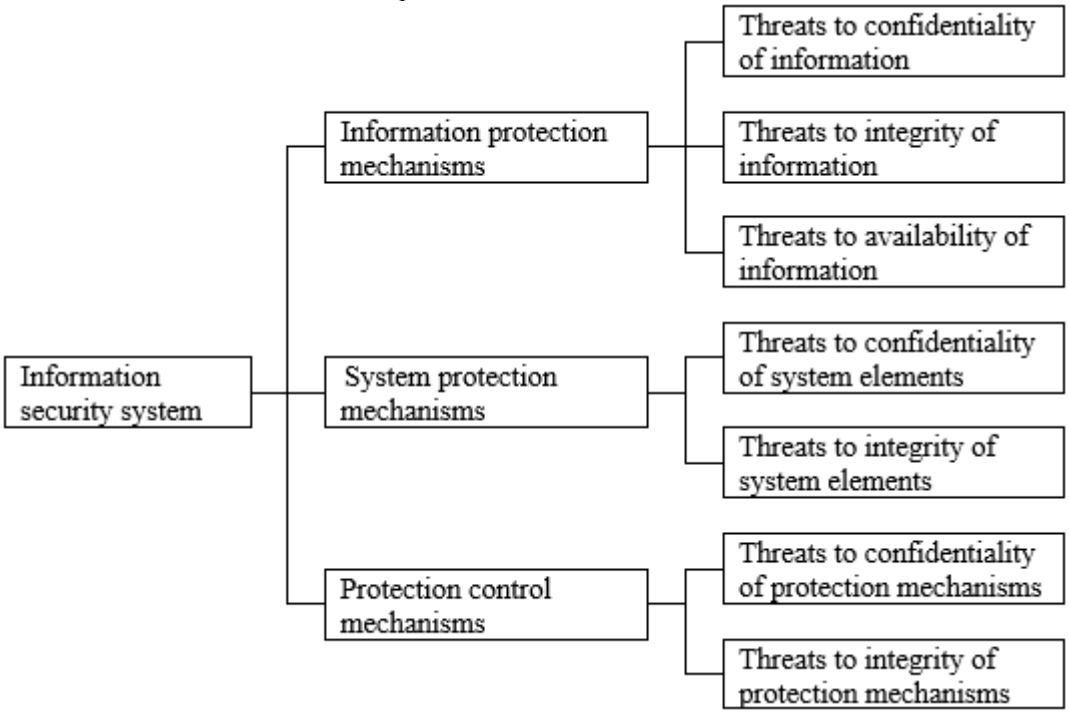

Figure 1. An approach to structuring an information security system.

3.1. Model of threats to information

On any of the elements of the elementary information flow, and therefore on the information, any of three types of unauthorized influence may be exerted: destruction, distortion, substitution. It should be noted that the information flow has two vertexes, and the impact can be exerted on any of them.

With regard to confidentiality, by definition its violation does not imply a violation of integrity or accessibility, although it may lead to this. Confidentiality violation occurs when replacing any of the elements.

Thus, having analyzed all possible types of impact on the information flow, it is possible to build many classes of information threats, presented in table 1.

Table 1. Information threat classes.

	Threats to the elements	Threats to channels
	Classes of threats to the confidentiality	
1.	Replacing either of the two vertexes	
2.		Channel substitution
3.		Channel listening
	Classes of threats to the integrity and availability	
1.	Destruction of information at one of the vertexes	Channel destruction
2.	Distortion of information at one of the vertexes	Channel distortion
3.	Falsification of information	Blocking information in channel

3.2. Model of threats to system

The approach proposed by the authors to construct a computer network model is described in detail in [20]. A computer network model based on attributive metagraphs allows you to describe computer network software components and all possible connections between them.

Only software elements of computer networks (software components of computer networks) and the relationships between them are considered. Software components in this case include application, system, and network software. Relationships are implied not only between elements located at the same level, but also indicating the nesting of one element in another. Application software operates within the operating systems that represent system software. In turn, operating systems operate within the framework of local area networks (or subnets) implemented through network software. Thus, three levels of software for computer networks are distinguished; for convenience, the levels are designated as software level, OS level, LAN level.

The proposed approach to the classification of threats and the developed threat model are based on elementary operations on metagraphs [20, 21]. A computer network is considered as a structure of interacting elements (vertices of the graph) and the connections between them (edges of the graph). Threats are understood as an unauthorized change in the structure of a computer network (graph).

Threats to the integrity and confidentiality of computer network software are addressed. The basic operations on attributive metagraphs include: adding a vertex or edge; Removing a vertex or edge Changing the vertex or edge attribute.

Based on this, classes of threats to the integrity and confidentiality of a computer network are presented in Table 2.

Table 2. Computer network threat classes.

	Threats to elements	Threats to links
	Classes of threats to the integrity	
1.	Threats of addition an element	Threats of addition a link
2.	Threats of removal an element	Threats of removal a link
3.	Threats of substitution an element	Threats of substitution a link
4.	Threats of changing element settings	Threats of changing link settings
	Classes of threats to the confidentiality	
1.	Threats of an element name disclosure	Threats of a link name disclosure
2.	Threats of an element settings disclosure	Threats of a link settings disclosure

3.3. Model of threats to protection system

Management of the information security system implies the regulation of the stages of the life cycle by compiling organizational documentation. In this case, by "organizational documentation" is meant not a document, but the rules fixed in it. Thus, typical threats are aimed at managing processes of information protection system components (firmware, regulatory documents and personnel) from the point of view of incorrect development or application of these rules. The approach to addressing threats to the management of protection systems is based on the Deming cycle, since this constant range of actions is aimed at improving processes. The Deming cycle presents an action algorithm consisting of the following stages:

- design stage;
- stage of implementation;
- stage of control;
- stage of adjustment.

At each stage of the cycle, the corresponding threats to the control processes of the protection systems were considered and typical threats were identified (Table 3).

Table 3. Typical threats arising at the stages of the life cycle of a protection system.

Integrity threats	Confidentiality threats
Incorrect development of process regulations	Disclosure of information on the features of the development of process regulations
Incorrect execution of process regulations	Disclosure of the rules of work specified in the regulations
Incorrect organization of control over the implementation of process regulations	Disclosure of information on the principles of organization of control over the implementation of process regulations
Incomplete correction of possible errors found in the process regulation	Disclosure of information on detected errors found in the process regulations and rules for their correction

4. Conclusions

In the course of the analysis of existing approaches to the description of threats to information systems and, in particular, computer networks and the Internet of things, a list of shortcomings was drawn up that needed to be addressed. In this paper, in addition to the information and system threat models described in previous publications, a threat model for the protection system is added. The general approach to constructing a protection system based on the separation of protection mechanisms into information protection mechanisms, system protection mechanisms and protection control mechanisms is also briefly described.

The approach proposed by the authors makes it possible to reduce the influence of the expert's professional level and his subjectivity in compiling lists of threats. Currently, this approach is used to describe threats to an automated system for commercial accounting of energy resources [22] and to describe threats to Internet of things systems [3]. The application of the proposed approach in both cases made it possible to identify threats that were previously missed by experts in the process of compiling threat models using other methods.

References

This research was funded by the Ministry of Science and Higher Education of Russia, Government Order for 2020–2022, project no. FEWM-2020-0037 (TUSUR).

References

[1] Internet Security Threat Report (ISTR) 2019. Symantec. Available online: https://www.symantec.com/security-center/threat-report (accessed on 12 December 2019).

[2] Penetration testing of corporate information systems: statistics and findings, 2019. Available online: https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019 (accessed on 12 December 2019).
[3] Shelupanov A, Konev A, Kosachenko T and Dudkin D 2019 Threat model for IoT systems on the example of openUNB protocol. *International Journal of Emerging Trends in Engineering Research* **7** 283–290
[4] Perera C, Barhamgi M, Bandara A, Ajmal M., Price B and Nuseibeh B 2019 Designing privacy-aware internet of things applications. *Information Sciences* **512** 238–257
[5] Zahoor A S, Mahmood H S and Javed A 2016 Information security management needs more holistic approach: A literature review. *International Journal of Information Management* **36(2)** 215–225
[6] Shelupanov A, Evsyutin O, Konev A, Kostyuchenko E, Kruchinin D and Nikiforov D 2019 Information Security Methods — Modern Research Directions. *Symmetry* **11(2)** 150
[7] Shostack A 2014 Threat Modeling: Designing for Security (John Wiley & Sons: Indianapolis, USA) pp 59–121
[8] The STRIDE Threat Model. Available online: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) accessed on 12 December 2019
[9] Jouini M and Rabai L 2016 Threat classification: State of art. In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security; Gupta, B., Agrawal, D., Yamaguchi, S., Eds.; IGI Global: Hershey, USA, pp. 368–392
[10] Wenjun X and Lagerström R 2019 Threat modeling – A systematic literature review. *Computers & Security* **84** 53–69
[11] Tang J, Wang D, Ming L and Li X A Scalable Architecture for Classifying Network Security Threats. Available online: http://papersub.academicpub.org/Global/DownloadService.aspx?ID=2514 (accessed on 12 December 2019).
[12] Lakhno V 2016 Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering. *Eastern-European journal of enterprise technologies* **2** 18–25
[13] Pan J and Zhuang Y 2017 PMCAP: A Threat Model of Process Memory Data on the Windows Operating System. *Security and Communication Networks* 4621587
[14] Bodeau D J and McCollum C D 2018 System-of-Systems Threat Model; The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA
[15] Darwisha S, Nouretdinova I and Wolthusen S D 2017 Towards Composable Threat Assessment for Medical IoT (MIoT). *Procedia Computer Science* **113** 627–632
[16] Jouini M, Rabai L and Aissa A B 2014 Classification of Security Threats in Information Systems. *Procedia Computer Science* **32** 489–496
[17] Boukhtouta A, Mouheb D, Debbabi M, Alfandi O, Iqbal F and El Barachi M 2015 Graph-theoretic characterization of cyber-threat infrastructures. *Digital Investigation* **14** S3–S15
[18] Uzunov A V and Fernandez E B 2014 An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces* **36 4** 734–747
[19] Cardenas A A, Roosta T and Sastry S 2009 Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Networks* **7 8** 1434–47
[20] Novokhrestov A, Konev A and Shelupanov A 2019 Model of Threats to Computer Network Software. *Symmetry* **11** 1506.
[21] Novokhrestov A and Konev A 2016 Mathematical model of threats to information systems. *AIP Conference Proceedings* **1772** 060015
[22] Nikiforov D S, Konev A A, Antonov M M and Shelupanov A A 2019 Structure of information security subsystem in the systems of commercial energy resources accounting. *Journal of Physics: Conference Series* **1145** 012018