Harmonization of Critical Information Infrastructure Objects Threats

Andrey N. Petukhov[1], Pavel L. Pilyugin[2]

Critical Information Infrastructures Security Division
Moscow Technical University of Communications and Informatics
Moscow, Russia
[1]anpetukhov@yandex.ru, [2] ppl@mail.ru

Karina N. Pilyugina

National Research University of Electronic Technology,

Moscow, Russia

karinakit@mail.ru

Abstract. **This paper discusses the issues of security threat modeling for critical information infrastructure facilities. An analysis is made of the applicability of various approaches to the construction of threat models highlighting the need for harmonization (ensuring internal compliance) of the main aspects of security, including threats. It justifies the expediency of using the "Common Criteria" methodology and SDL procedures for building harmonized threat models. The experience of using such an approach to create models of threats for software-defined networks and the protection profile of an SDN controller is discussed.**

Keywords: **information security, threat model, general criteria, protection profile, software configurable networks.**

I. INTRODUCTION

Critical objects countries may be different in different areas of activity, a general definition for them is not formulated; however, a number of common signs of such objects can be noted.

Critical objects of information infrastructure have a certain specificity from the point of view of security. In fact, it is impossible to justify the level of permissible residual risk, indeed, there is practically no such concept. In addition, there is no mechanism for calculating the real damage from such an information security incident. At the same time, the contingent of "recipients" of damage in this case is much wider than the set of security management entities (and, as a rule, it goes beyond the category of owners of compromised information assets).

In these circumstances, the goal of security management is not so much to achieve a certain level of security (to balance risks with costs), as to exhaust the potential of protection (to do all that is possible).

II. MODELING THREATS TO CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Despite this, it is necessary to have an adequate understanding of the threatening danger. In any particular case, there are features of the structure and form of such representation and a common element is always the typology of the manifestation of danger, the nomenclature of identified and qualified types of such manifestation, external (aggressiveness of the environment) and internal (imperfection of the object) events and situations that cause damage (threat model is the so-called proactive aspect of security management [1]).

Threat modeling is an essential element of information security management, and is a cyclical process activity.

The concept of threat representation hierarchy ("threat tree") put forward in the last century [2] is based on the schemes of successive (evolutionary) solutions for threat modeling. In this case, the attacker's target is represented as the "root node", and the potential means of achieving the target (scripts and resources) are represented as "end nodes". The resulting threat models formally define how you can implement threats from some classes ("roots") in each of the nodes of the threat tree. As a result, the use of hierarchical structures allows us to systematically consider the set of attack vectors against any specific target.

Another methodology for joint functional assessment (harmonization) of threats, assets and vulnerabilities is based on the well-known Clements—Hoffman model [3]. This model comes from the postulate that the security system must have at least one means to ensure security on every possible path of an attacker's impact on information technology ("a system with full overlap").

We can say that the model is "utopian" in nature, because it is almost impossible to build a system with full overlap. The reason for this is that the search for all impacts on the object cannot always be performed. In addition, in reality, each protection barrier provides only some degree of resistance to security threats. And it is important that it is the "resistance" of barriers that determines the amount of residual risk (this fact is especially important for critical objects of information infrastructure).

Nevertheless, it is the Clements—Hoffman model and the "threat tree" model that today determine the main vectors for the development of the methodology for modeling threats in

general and critical information infrastructure facilities in particular.

III. METHODOLOGY OF THREAT MODELING

We can say that the implementation of the threat modeling methodology mainly tend to several types:

- support for risk analysis (feasibility assessment methods);
- decomposition of subject (how the data flows and process flows);
- declarative (base model method);
- harmonization of high-level entities (common criteria methods)

Methods of the first type are a step-by-step process of attack modeling and threat analysis aimed at preparing data for risk analysis. This process involves the harmonization of security objectives and technical requirements for information processing and transmission procedures at each stage. As a result, the dynamic, adaptable and extensible identification of threats, the enumeration of their nomenclature and the procedure for assessing the feasibility are carried out. Some practical implementations allow for an understanding of the risks, taking into account the properties of attackers, allow you to prepare a specification and methods of application of the infrastructure, which can help mitigate the effects of malicious impact on specific information assets.

Another area of application of threat models as a risk management tool is the use of threat modeling results as input for security audits. In this case, the range of threats and their characteristics are formed on the basis of requirements that establish a certain, pre-permissible level of residual risk for each category of information assets. Obviously, this makes this approach inapplicable for critical information infrastructure objects.

Subject decomposition technologies are distinguished not so much by fundamental methodological innovations as by good tools and instruments for visualizing decomposition processes. This ensures a correct evolutionary transition from one level of threat modeling to another. Threat modeling begins with creating a visual representation of the analyzed application or infrastructure, and then this representation highlights its component parts, thus decomposing the subject of analysis. Once the decomposition is complete, the visual representation is used to identify and list potential threats.

One of the common ways to visualize a formal threat modeling process is the use of data flow diagrams (DFD) [5]. These diagrams were created to model information systems; DFD provided only four elements: data streams, data warehouses, processes that change data, and external factors of data change (interactors). However, the description of the threatening effects on the data within such a description has proven to be very effective. And when the ideology of trust calculation ("common criteria") began to prevail in the management of information security, the DFD procedure was supplemented with a special concept of the "boundary of trust", specifically for modeling threats.

First, using these basic concepts, the information infrastructure is described, then, the input of each threat is analyzed for all known categories. After identifying the level of aggression, this allows to establish measures to reduce the level of danger.

Declarative methods of forming threat models assume the presence of regulated information and procedural resources to support the various stages of modeling (the base model). Methods of this type use speculative threat systematization based on the assumption of the internal content of the threat. The low level of constructiveness of such a scheme, and its lack of relations to the used assets and information technologies characteristics, the general nature of expert assessments limit the use of declarative methods in real conditions.

The threats harmonization idea is implemented in the concept of information security management taking into account the requirements and conditions (for the object of management and for the environment) on the basis of an assessment of confidence in the means of implementation of these conditions and ways to meet these requirements ("calculation of trust"). The basic statement of this concept is the international standard reproduced in Russia [6]. One of the key provisions of the standard establishes a set and relationship of the original concepts ("high-level entities") in the field of information security. These relationships show that the essence of the "threat" interacts with the entities "risks", "assets", "threat agents" and "vulnerabilities".

Harmonization reveals these connections and allows you to include their content in the threat model, threats are modeled not by themselves, but in the context of interacting with these entities.

The standard provides a security profile. This is an effective format for interaction information usage. There are several categories in the protection profile which, in aggregate, exhaustively reflect the perceptions of the danger in a harmonized way. In addition to the actual category of "threats", a derived category of "assumptions" is attracted, with the help of which the information assets space is limited and the "boundary" interface with the environment is specified. The "assumptions" related to intrinsic properties and characteristics partly support the idea of the current security of an object (the reactive aspect of security management [1], the ratio of barriers and vulnerabilities of the Clements—Hoffman model [3]). The main tool for representing the reactive aspect in the protection profile is the category of "policy", which corresponds to the possibilities (realized and hypothetical) to counteract the harmful factors of an aggressive environment. To ensure the mutual correctness of "threats", "assumptions" and "policies" in the protection, profile provides a special mechanism, expressed in the form of "security objectives" for the environment and the object itself.

The interaction of threats and risks is a "projection" of the threat onto the space of security criteria. This projection indicates the criteria (properties) of security that "suffer" as a result of the realization of the threat. This indication, together with the qualification of the damage itself, identifies the risk. Therefore, the harmonization methodology implies an indication of the compliance of threats with established safety criteria.

Until recently, three main criteria (aspects, properties) of the security CIA (confidentiality (confidentiality), integrity (integrity) and availability (availability)) traditionally dominated. Detect threats that are not related to the criteria the CIA, demanded the extension of this list ("hexade Parker"), which also highlighted the authenticity, management, or possession (control) and usefulness.

It is important that additional criteria arose in the process of attempts to harmonize threats that were not correlated in the old criteria space with any vulnerabilities or risks. The examples and comments in GOST R ISO/MEK 27033-3-2014, deserving particular attention, illustrate the limitations of the CIA criteria triad and the inability to describe some real-life threats using its elements [7].

However, the application of this developed standard in the case of critical information infrastructure objects causes some difficulties. An information security incident is described by dividing the set of objects states into subsets of admissible and unacceptable states and the safety criteria change abruptly when the state of an object changes from one subset to another. Moreover, in the general case, security criteria can have the same value for object states from different subsets. Finally, one of the possible states of an object can be the cessation of its existence as a result of an incident, which in some cases makes any evaluation of safety criteria meaningless.

IV. SECURITY DEVELOPMENT LIFE-CYCLE

Among the approaches that harmonize threats with other high-level entities (vulnerabilities, assets and threat agents), the Security Development Life-cycle (SDL) methodology attracts attention [8]. In the context of the topic of security of critical objects, the construction of diagrams and the enumeration of threats are of interest.

When constructing diagrams, they usually use the tools for constructing DFD data flow diagrams (including the "trust boundary" element). The element "boundary of trust" shows that the elements located on opposite sides of this boundary function at different levels of authority.

For enumeration of threats in the SDL, the "STRIDE threats to the element" method is used from some universal list:

- **S**poofing of user identity (spoofing subject);
- **T**ampering (intervention and modification);
- **R**epudiation (disclaimer);
- **I**nformation disclosure (leakage and disclosure);
- **D**enial of Service;
- **E**levation of privilege (capture and elevation of privilege) [9].

The methodology assumes that all threats can be grouped into groups from the STRIDE list, and that each type of DFD element corresponds to a specific threat class. For example, this correspondence has the following form:

- External element-SR (Substitution-Disclaimer);
- Process-STRIDE (all kinds of threats);
- Data storage-TRID (Unauthorized Access; Data Leak; Denial of Service);
- Data flow-TID (Unauthorized Access; Data Leak) [8].

Each SDL implementation includes guidance on detailing the threats of each class for each type of DFD element. Typically, these guides have two methodologically inseparable parts.

The first is relatively general and stable and reflects (harmonizes) the specifics of the pair "threat class STRIDE — type element DFD". The most authoritative sources of this part of the manuals (Microsoft, Cisco, IEEE 802, etc.) publish their position on how threats from each STRIDE class are manifested in relation to DFD-elements of different types.

The second part of the SDL threat detail guides applies to a specific DFD element. It represents the rules of attack scenario development and describes the scheme and conditions of threat actions. It also points to specific vulnerabilities that allow you to implement an attack scenario. Thus, the harmonization of threats is carried out.

The knowledge necessary for targeted management should contain, at a minimum, an inventory of information assets (resources and processes), information about the aggressive potential of the environment and the channels for its implementation, as well as an idea of the real possibilities of countermeasures (i.e. "what, from what and what we protect"). In the case of protection of critical objects, vulnerabilities can be methodically subordinate, because in critical objects the vulnerability can be only in three states: already eliminated, eliminated (short-term state) and unknown. Therefore, the harmonization of threats in their modeling for critical information infrastructure is aimed at identifying unknown threats.

In general, all possible combinations of asset-actor-action triples are built. Combinations that are not meaningful or allowed are discarded. The array of data associated with forbidden combinations is an ideal information base for security management, and a threat model.

The methodical decisions in the SDL do not directly operate with the category of damage and do not pursue the goal of minimizing residual risk. They are aimed at achieving the completeness of the considered threats, thereby creating the prerequisites for the exhaustion of the potential of protective actions. At the same time, the SDL fully preserves the "harmonizing" properties, making it possible to consider the manifestations of a threat in the context of a specific element of the information technology (asset), in specific conditions and with consideration of a specific source (actor). In addition, SDL has "evolutionary" properties that allow the decomposition of interacting entities, refining the threat (attack) implementation scenarios, without disturbing the harmonization. Thus, we can conclude about the suitability and feasibility of SDL techniques for modeling security threats to critical information infrastructure facilities.

V. CONCLUSION

The approach using the SDL procedures was applied in the analysis and development of security solutions for critical objects built on the basis of software-defined network technology (SDN) [10]. A protection profile was developed in MTUCI for SDN-controller, the core of the control layer of such a network [11].

A fundamental feature of software-defined networks is the separation of network services for management functions and packet forwarding functions. This creates new classes of attacks on the control center (controller) both from the data plane and in the control plane. Analysis of the structure of devices and the use of the STRIDE model to identify threats allowed us to formulate a general description of the threats. Threats to the controller are considered across all possible interfaces: from applications, control systems, and network devices. These assumptions actually determine and maintain the composition of key assets of SDN-controllers: account data, configuration and management data, log data, operating system, software, hardware, resources and controller interfaces.

This made it possible to prepare specifications of specific threats, assumptions and policies united by common security objectives, both for the object (SDN-controller) and for the environment of its operation. As a baseline, the mode of using the network is considered, when all network infrastructure, computer equipment, communication equipment and communication channels are under single control in the trusted zone, all applications are trusted and provided by the provider. This option is typical for deploying a software-defined network in a single center.

VI. REFERENCES

[1] Петухов А.Н. Информационная база управления кибербезопасностью критических инфраструктур // XI международная научная конференция «Технологии информационного общества (Москва, 15–16 марта 2017) . М., 2017. [Petukhov A. N. Management information base of cybersecurity // XI International Scientific Conference “Information Society Technologies” (Moscow, March 15-16, 2017). Moscow, 2017].

[2] Salter C., Sami Saydari O., Schneier B. et al. Toward A Secure System Engineering Methodology. Washington: National Security Agency, 1998..

[3] Хоффман Л.Дж. Современные меторды защиты информации / Пер. с англ. М.: Сов. радио, 1980. [Hoffman L. Modern methods for computer security and privacy. Moscow: Sovetskoye radio, 1980].

[4] Bundesamt für Sicherheit der Informationstechnik URL: http://www.bsi.de.

[5] Abi-Antoun M., Wang D., Torr P. Checking Threat Modeling Data Flow Diagrams for Implementation Conformance and Security // ASE'07. Atlanta, 2007.

[6] ГОСТ Р ИСО,МЭК15408-1—2012 Информационная техонология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности. Критерии оценки безорпасности информационных технологимй. Часть 1. Введение и общая модель. М., 2012. [GOST R ISO/MEK 15408-1-2012. Information technology. Security techniques. Evaluation Criteria for IT security. Part 1. Introduction and general model. Moscow, 2012].

[7] ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. М., 2014. [GOST R ISO/MEK 27033-3-2014 Information technology. Sewcurity techniques. Network security. Part 3. Reference network scenarios. Threats, design methods and management issues. Moscow, 2014].

[8] Shostack A. Threat Modeling: Designing for Security. Indianapolis: John Wiley & Sons Inc., 2014.

[9] The STRIDE Threat Mode / Microsoft. 2016.

[10] Pilyugin P., Smelyansky R. Modern security issues in SDN // Proceedings of ITSN-2017 International Conference on Information Technologies, Systems and Networks 2017, Chisinau, Republic of Moldova. Chisinau, 2017. P. 182–187.

[11] Петухов А.Н., Пилюгин П.Л. Профили защиты для программно-конфигурируемой среды // Радиоэлектронные устройства и системы для инфокоммуникационных технологий REDS 2018. М., 2018. [Petukhov A.N., Pilyugin P.L. Security profiles for software defined network. International Conference on: The radio-electronic devices and systems for infocommunication technologies. REDS-2018. Moscow, 2018].