UDC 004.056.5 (043.2)

A.D. Pinchuk, R.S. Odarchenko, DSc, O.O. Polihenko, Doctoral Candidate
(National Aviation University, Ukraine)

Analyzing of existing cyber threat classification models

Nowadays cyber threat intelligence plays a crucial role in ensuring cybersecurity and cyber resilience of every organization. Each cyber threat should be classified properly to perform effective respond or mitigate it. Thus, this paper provides a comprehensive analysis of existing cyber threat classification models, exploring their methodologies, strengths, and limitations. The findings serve as a valuable resource for cybersecurity professionals and researchers seeking to develop or refine threat classification systems.

A threat is essentially an adversary's objective, encompassing his planned actions or goals against a target system. It can be characterized as the ability of an adversary to attack a target system. According to [1], most approaches to the classification of cyber threats fall into two main categories: those based on the methods used in cyberattacks and those based on the consequences of cyberattacks.

Classification based on attacks techniques

Here, the next models can be highlighted: a model of three orthogonal dimensions, a hybrid model, and a pyramidal model of classifying information security threats.

The three orthogonal dimensions model, proposed by Lucas-Som Ruf et al. in [2], aims to enhance the understanding of threats and simplify existing models. This is achieved by introducing a three-dimensional approach that categorizes threats along three independent axes: motivation, location and agent (fig.1).

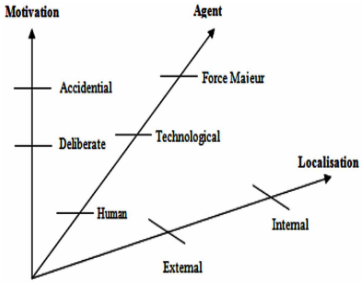

Fig. 1. The three orthogonal dimensions model [2]

While this model offers a comprehensive perspective on threat classification, its primary limitation is the lack of consideration for the consequences of these threats.

The hybrid model, also known as the *C3* model, was introduced in [3] and takes into account three key criteria: frequency of cyber threats, focus domain of the cyber threat and source of the cyber threat (fig.2).

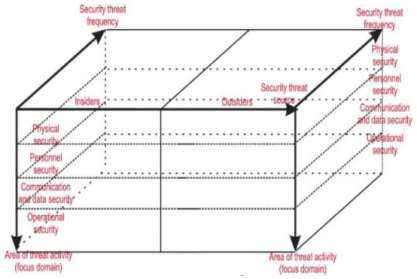

Fig. 2. The basic C3 model [3]

Although frequency is considered in the model, it is not necessarily the most critical factor, as low-frequency threats can sometimes cause more significant damage than high-frequency ones, and vice versa. Similarly, the source of the threat is crucial, but both insider and outsider threats can lead to severe consequences. Therefore, a better focus should be placed on understanding the nature of the threat source rather than just its category.

The pyramidal model, presented in [4], classifies intentional security threats within a hybrid framework, focusing on three key factors: the cybercriminal's prior knowledge of the system, criticality and losses (fig.3).

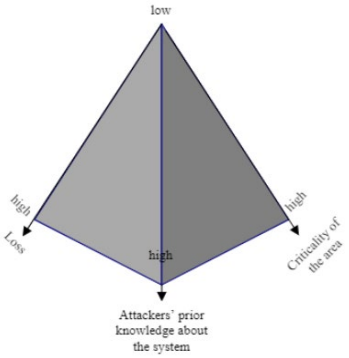

Fig. 3. Information Security Threats Pyramid Classification

Although the model does not explicitly mention the source of the threat (insider or outsider), the authors consider this factor within the "Attacker's prior knowledge" category. Insider threats are regarded as particularly significant since insiders typically possess more extensive knowledge of the system.

Overall, the model focuses on dynamic classification of cybersecurity threats that may impact organizations. It helps to identify and localize threats by assessing the criticality of system components, potential loss of sensitive information, and the attacker's knowledge. However, this classification does not address the overall impact of each threat.

Classification based on cyberattack impact

Here, it possible to consider the following classification methods: STRIDE, ISO and NIST.

The STRIDE model, developed by Microsoft, is utilized to identify and categorize threats at the network, host, and application levels [5-6]. It classifies known threats based on the objectives or motivations of adversaries, and the acronym STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege (EoP). This model aims to understand the mindset of cyber attackers by evaluating threats from their perspective. Over time, STRIDE has evolved to include additional threat-specific tables and variants such as STRIDE-per-Element and STRIDE-per-Interaction [7].

Fig. 4. The STRIDE model

While the model is widely adopted, it has several drawbacks: time-consuming, static analysis, subjective, requires ongoing support, limited to software.

The ISO model, based on the ISO 7498-2 standard, identifies five primary impacts of security threats [8]: destruction of information and/or resources, distortion or modification of information, theft, removal or loss of information and/or resources, disclosure of information, and interruption of services.

These categories are mutually exclusive, providing a comprehensive classification system that encompasses all types of threats and is organized into a flexible structure. However, while the model offers a broad coverage of threats, it does not account for all the possible consequences that may result from these threats.

The NIST classification (NIST, 2012) outlines several categories of security threats, including errors and omissions, fraud and theft, employee sabotage,

loss of physical and infrastructure support, malicious hackers, industrial espionage, malicious code, foreign government espionage, and threats to personal privacy [8].

However, this classification does not encompass all potential threats. It lacks a comprehensive grouping system, leading to situations where different threats may be categorized under the same heading, such as system destruction. Furthermore, the complexity of cyber threats and the broad range of identified threats in previous studies complicate the process of selecting an appropriate classification model.

Conclusion. Thus, while various cyber threat classification models offer useful frameworks for categorizing and understanding security risks, each has its limitations. Some models, such as the Three Orthogonal Dimensions and ISO models, provide broad categorizations but fail to address the full consequences of threats. Others, like the Pyramidal and Hybrid models, focus on specific aspects of threats but may overlook critical dimensions such as the impact or source. The STRIDE and NIST models, though widely adopted, are limited by subjectivity, complexity, and a lack of comprehensiveness.

To develop a more effective cyber threat classification system, future models should strive for a balance between detailed categorization, adaptability, and inclusion of both static and dynamic threat factors. Integrating these elements will enhance the ability to assess and mitigate the evolving landscape of cybersecurity threats comprehensively.

References

1. Izrailov, Konstantin & Chechulin, Andrey & Vitkova, Lidia. (2020). Threats Classification Method for the Transport Infrastructure of a Smart City. 1-6. 10.1109/AICT50176.2020.9368828.
2. Ruf L, AG C, Thorn A, GmbH A, Christen T, Zurich Financial Services AG, Gruber B, Credit Suisse AG., Portmann R, Luzer H, Threat Modeling in Security Architecture - The Nature of Threats. ISSS Working Group on Security Architectures, http://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture_Threat-Modeling_Lukas-Ruf.pdf.
3. Geric, Sandro & Hutinski, Željko. (2007). Information system security threats classifications. Journal of Information and Organizational Sciences. 31.
4. Alhabeeb, Mohammed & Almuhaideb, Abdullah & Le, Phu & Bala, Srinivasan. (2010). Information Security Threats Classification Pyramid. 208-213. 10.1109/WAINA.2010.39.
5. Swiderski F, Snyder W. Threat Modeling. Microsoft Press; 2004.
6. Meier J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A. Improving we application security: threats and counter measures. Satyam Computer Services, Microsoft Corporation; 2003.
7. Threat Modeling: 12 Available Methods. SEI Blog. https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.
8. Islam, Tariqul & Manivannan, D. & Zeadally, Sherali. (2016). A Classification and Characterization of Security Threats in Cloud Computing. INTERNATIONAL JOURNAL OF NEXT-GENERATION COMPUTING. 7.