Journal of Electronic Research and Application, 2024, Volume 8, Issue 4
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Penetration Study of Key Technologies for Cybersecurity Risk Assessment

Lin Ma*

Zhejiang Testing & Inspection Institute for Mechanical and Electrical Products Quality, Hangzhou 310051, China

***Corresponding author:** Lin Ma, malin4050@163.com

Abstract: In recent years, with the frequent occurrence of cyber security incidents, people have paid more attention to it. Information security risk assessment is a very important research topic. This paper gives a brief overview of the theory of cybersecurity risk assessment, focuses on the description of the current mainstream cybersecurity risk assessment methods, classifies and compares the existing methods according to the nature of the methods, and analyses the advantages, disadvantages, and application scope of each method. Finally, the main factors affecting the evaluation results are summarized and refined, and future research hotspots in this field are proposed. Through the empirical analysis of the three factors, the influence of the correlation of the three factors, the uncertainty of the evaluation indexes, and the timeliness of the evaluation on the evaluation results are concluded, which provides a reference for future research on evaluation methods.

Keywords: Risk assessment; Correlation; Real-time analysis; Uncertainty analysis; Quantitative analysis

Online publication: August 13, 2024

1. Introduction

In recent years, with the continuous promotion of the national information technology development strategy, the information technology and Internet industry have also developed rapidly [1]. With the progress of information technology and the rapid development of the Internet industry, network security has become a focus of attention, and it is also a key issue that urgently needs to be solved in the new era [2].

2. Basic concepts of cybersecurity risk assessment

A security incident is a situation on a system, a service, or a network that can be identified as a situation that causes a failure of a system's security policy, a loss of a system's privileges, or a system's inability to function properly [3].

The main components of cybersecurity risk evaluation are assets, vulnerabilities, threats, risks, events, and security measures. A so-called security event is the process by which a vulnerability is exploited, thereby increasing the risk of network security and developing into a security event, that is, a network system, that develops from a potential, normal system state into an obvious, abnormal system state after being induced by a

cyber-attack [4]. By analyzing the interrelationships between the factors, we find that the presence of more flaws within an asset implies more potential threats, conversely, if more effective protective measures can be taken, the danger of the system can be reduced. This can be summarized in **Figure 1**.

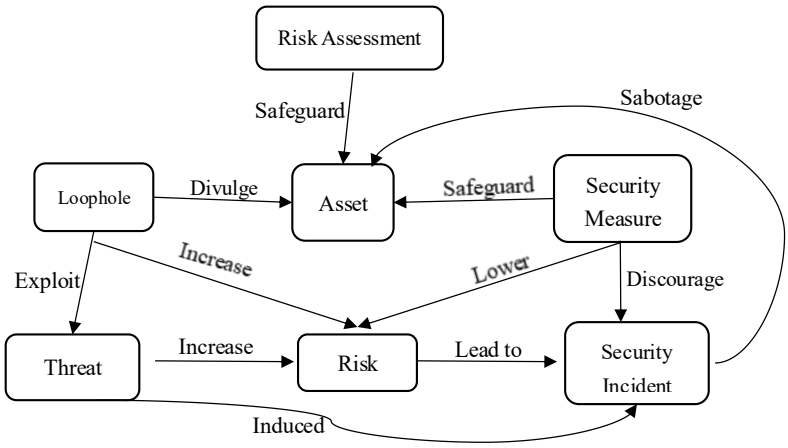

Figure 1. Relationship model between elements of cybersecurity risk assessment

In cybersecurity risk evaluation, the causal relationship between factors is summarized as follows:

(1) Attackers can take advantage of these weaknesses to trigger some security events, thus increasing the risk of the network.

(2) The security measures taken can prevent security incidents, thus reducing the risk of the network.

(3) Vulnerabilities may increase the risk of a system, but do not directly trigger a security incident in the system, but are exploited in the system by other parts of the system, thus triggering an attack on the system.

(4) There are flaws in the system that leak assets to malicious users.

(5) When a vulnerability in a system is used to carry out a single attack that exposes the assets of that system to an attacker, it creates a single threat or increases the danger one at a time.

(6) Security measures are mainly aimed at mitigating or preventing the occurrence of security events to reduce cyber risks.

From the current research, the primary goal of network security risk evaluation is to identify the possible risks in the network and then propose the best protection strategy to control these risks [5-8]. **Figure 2** shows the specific relationships in the principles of cybersecurity risk evaluation, described as follows:

(1) Asset identification: Quantifying the value of assets such as software and hardware in the network system and their degree of impact on the security of the network system.

(2) Vulnerability identification: Detecting the vulnerabilities existing in the network system and analyzing the possibility of their exploitation.

(3) Threat identification: Identifying the harmfulness of potential threats caused by vulnerabilities and the types of attack events they trigger.

(4) Security risk confirmation: Confirming the risk status caused by vulnerabilities and threats.

(5) Security event analysis: Analysis and calculation of the possibility of security events caused by system vulnerabilities and threats and the damage that will be caused to the network system after the security event.

(6) Security strategy program formulation: Combining the five aspects above, developing a reasonable security protection program for the network system's risk situation.

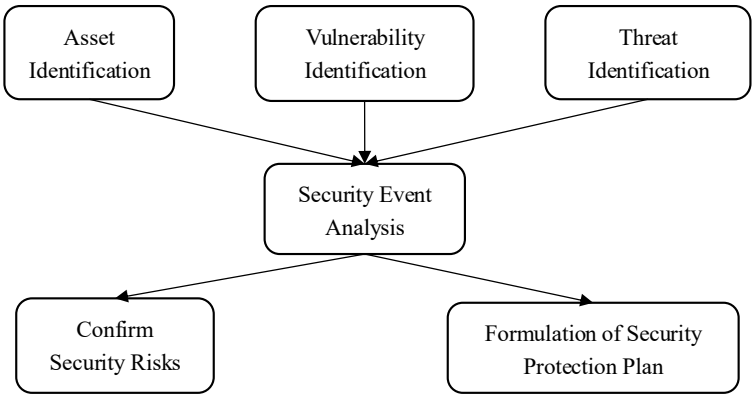

Figure 2. Principle of network security risk assessment

3. Network security risk assessment implementation process

This paper combines the attack graph risk analysis module and the intelligent optimization algorithm protection strategy selection module to propose a network security risk assessment implementation process oriented to risk analysis and risk management, the specific content is shown in **Figure 3**.

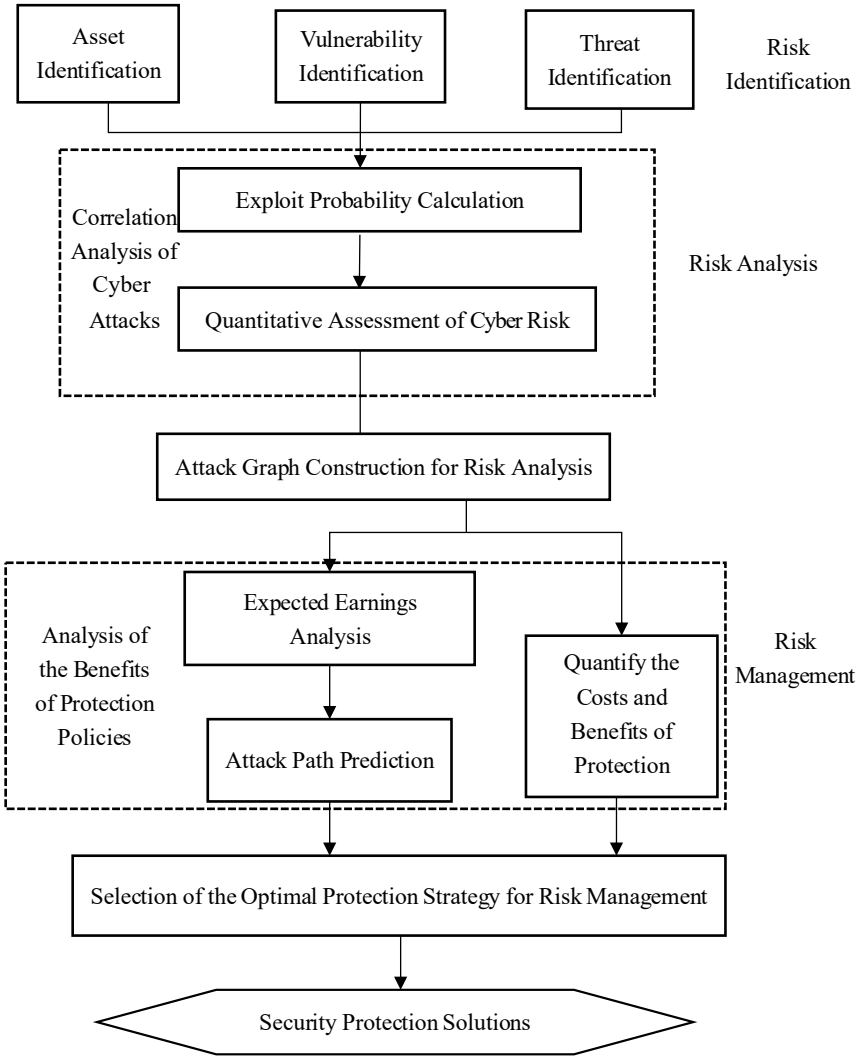

Figure 3. Implementation process of network security risk assessment

(1) Asset identification: The resources in the network system mainly include data, software, and hardware, and a cyber-attack will lead to the loss of resources, that is, the integrity, availability, and security of the network system is damaged.

(2) Vulnerability identification: Vulnerability identification mainly includes two parts, identifying the type of vulnerability, and assessing the possibility of vulnerability exploitation and the degree of harm.

(3) Threat identification: By identifying the potential threats generated by the vulnerabilities and identifying them through the threat database, the threats generated by them are evaluated.

(4) Network attack correlation analysis: By analyzing and calculating the probability of security events caused by weaknesses or threats existing in the network, and analyzing the losses caused by these security events.

(5) Quantitative assessment of network risk: Analyzing the degree of harm of security events triggered by vulnerabilities and threats, and taking corresponding security precautions for different levels of risk.

(6) Attack path prediction: Based on the expected return and cumulative probability, the attacker's intention to attack is surmised and the attack path is predicted to formulate corresponding defense strategies.

(7) Protection strategy benefit analysis: On this basis, using the intelligent optimal algorithm and the cost-benefit model, to achieve the balance of the cost and benefit of the defense strategy.

(8) Security strategy program formulation: On this basis, the vulnerability, threat, risk, and harm of the attack on the information system are clarified through the establishment of a unified security risk evaluation system.

4. Research on key technologies for cybersecurity risk assessment

4.1. Qualitative assessment method

Qualitative assessment methods are based on elements such as threats, vulnerabilities, and security measures faced by the system, and based on the knowledge and experience of the assessor, the network security level is assessed and judged [9]. The expert evaluation method, Delphi method, and fault tree method are the main means of qualitative evaluation [10].

(1) Expert evaluation method: Experts from various parties evaluated the potential risks in the network system based on their knowledge and experience, combined with relevant evaluation guidelines, and assigned corresponding risk weights.

(2) Fault tree analysis method: This method focuses on the results of the faults and follows the corresponding steps to find the causes of the faults. When using the fault tree analysis method, because each element in the tree structure is closely related, this makes the process of risk analysis also from the whole to the local.

(3) Delphi method: The Delphi method is a method of qualitatively analyzing the level of risk. It adopts the form of anonymity to ask for opinions from several experts who do not know each other, and several experts work independently, and then synthesize according to their respective opinions, and finally arrive at a more objective and precise evaluation.

4.2. Quantitative risk assessment methods

Different from the qualitative risk assessment method, the quantitative risk assessment method takes the numerical value as the standard to assess the network security risk, quantifies the network security risk assessment, and then uses the computer to measure the security risk in the network and the degree of impact; the results of the measurement are to visualize the data embodied in the assessment results, so it has the

advantages of being more objective, scientific, and rigorous [11-14]. In the quantitative risk evaluation, there are some representative evaluation methods as follows [15]:

(1) Decision tree method: Decision tree analysis is a top-down tree structure constructed based on probability theory, and each decision may cause several different events.

(2) Cluster analysis: Cluster analysis is a method of classifying data objects according to their similarity.

(3) Factor analysis method: The goal of factor analysis is to portray the connection between multiple indicators with a few factors, that is, to group multiple indicators with high correlation into one category, and to reflect the main information of the original indicators with a few factors, which reduces the complexity and ambiguity of the evaluation indicator system.

4.3. Integrated risk assessment method

The integrated risk assessment method is a method that organically combines both qualitative and quantitative methods [16]. There are two main methods: the assessment method based on the index system and the assessment method based on the modeling method.

4.3.1. Risk assessment based on the index system

This form of risk assessment is mainly based on the index system to assess the network risk [17]. Specifically, the network risk assessment is quantified to reflect the security factors affecting the network risk, and then, combined with the characteristics of the reflected factors, it is divided into several groups, thus forming a risk indicator system, and finally, the constructed indicator system is used as the basis to assess the risk in the network.

4.3.2. Risk assessment based on the modeling method

This method can combine each risk factor with the state of the system and can scientifically model each risk factor to obtain the safety level of the system. On this basis, a new risk evaluation method is proposed.

(1) Evaluation method based on graph model: Combining the correlation between security events and network security, a visual attack behavior and network security evaluation model is established. Zhang *et al.* combined complex networks with attack graph theory and proposed a risk evaluation method for railway train information security based on attack graph theory [18]. Semertzis *et al.* proposed a quantitative evaluation method for system attack behavior based on an attack graph, whose main research contents include [19]: (I) Establishing a probability model for information threat scenarios based on the attack graph. (II) Based on the probabilistic model for attack scenarios. (III) Based on this model construct the probability model of the information threat scenario.

(2) Evaluation method based on the theoretical model of artificial intelligence: Due to the topology of complex networks having the characteristics of vagueness and uncertainty, and artificial intelligence is suitable for modeling them, the risk evaluation method based on artificial intelligence is studied on this basis. Currently, Bayesian networks and Hidden Markov Models are widely used in the field of risk evaluation.

5. Summary

This paper launched a systematic comprehensive analysis of the literature on cybersecurity risk assessment and came up with four categories of factors, such as relevance, real-time, uncertainty, and quantification, which have an impact on the assessment results. The analysis results showed that the technology of cyber

risk assessment is not mature enough, and it is necessary to further study the related technology of cyber risk assessment, optimize the assessment algorithm, and look for more reasonable and accurate assessment methods and assessment standards. On this basis, this paper also put forward the issues that need to be further studied in the next step: (1) To further reduce the subjectivity and uncertainty of evaluation. (2) Based on the evaluation results, to automatically generate security recommendations for managers to make decisions to make the evaluation process more automated. (3) Due to the differences in the types of networks, the main controlling factors affecting the evaluation results vary. (4) To explore an environment that can simulate actual network attacks to enhance the efficiency of risk evaluation of the system.

Disclosure statement

The author declares no conflict of interest.

References

[1] Liu F, Yang Y, You Y, 2021, Research on the risk evaluation of ship network security information based on artificial intelligence technology. Ship Science and Technology, 43(12): 151–153.

[2] Liu J, Ling X, Zhang L, et al., 2022, A Framework for Cybersecurity Risk Assessment Based on Tactical Correlation. Computer Science, 49(09): 306–311.

[3] Zhang J, Wang Q, Zhao S, 2022, Research on the application of HAZOP-LOPA coal mine safety risk evaluation method based on Bayesian network. Mining Safety and Environmental Protection, 49(01): 114–120.

[4] Deng Y, Meng M, Zhang Y, et al., 2021, Knowledge mapping and visualization analysis of metro safety research based on CiteSpace. Journal of Civil Engineering and Management, 38(05): 57–63.

[5] Mu L, Li W, Chen H, et al., 2021, Current Status and Insights of Global Cyber Biosecurity Research. Science and Technology Management Research, 41(06): 28–32.

[6] Wang P, 2021, Design of Network Security Protection for Intelligent Devices in Nuclear Power Plants. Automation Instrumentation, 42(S1): 314–318.

[7] Lin L, 2021, Research on Safety Risk Assessment of Petrochemical Plants Based on Fuzzy Comprehensive Evaluation Method. Energy and Environmental Protection, 43(07): 100–104 + 113.

[8] Luo Y, 2021, Research on Safety Risk Assessment of Network System Based on Combinatorial Optimization Theory. Microcomputer Applications, 37(07): 144–146 + 162.

[9] Yan W, 2022, Security risk assessment and control of wireless network based on convolutional neural network. Journal of Shenyang University of Technology, 44(05): 565–569.

[10] Wang S, Liu C, Liu S, et al., 2021, An attack tree-based security risk assessment method for 4G networks. Computer Engineering, 47(03): 139–146 + 154.

[11] Lu Y, Chen L, 2021, Research on network security situational awareness risk assessment technology based on FAHP. Computer and Digital Engineering, 49(05): 957–960 + 976.

[12] Qiang R, 2022, Random forest algorithm-based security risk assessment method for communication networks. Automation and Instrumentation, 2022(11): 189–193.

[13] Kang W, 2022, Security risk assessment method for power monitoring network based on improved AHP algorithm. Automation and Instrumentation, 2022(10): 171–174.

[14] Xu IL, Chen T, 2021, Optical communication data security risk assessment model based on blockchain. Automation and Instrumentation, 2021(11): 40–44.

[15] Ding Y, Wang R, Li L, et al., 2022, BN-MNA model and application for safety risk assessment and control of

assembled building construction. Journal of Civil Engineering and Management, 39(04): 153–161 + 184.

[16] Zhao D, Chen C, Yi L, 2021, A temporal risk assessment model for disaster evolution network. Chinese Journal of Safety Science, 31(03): 171–177.

[17] Cai J, Ma Q, Tan S, 2022, Research on the construction of scientific and technological security risk assessment and monitoring and early warning system. Science and Technology Progress and Countermeasures, 39(24): 100–108.

[18] Zhang F, Chen Y, 2019, Current status and improvement measures of pantograph crack fault detection. Shandong Industrial Technology, 2019(17): 116.

[19] Semertzis I, Goyel H, Rajkumar VS, et al., 2024, Towards Real-Time Distinction of Power System Faults and Cyber Attacks on Digital Substations Using Cyber-Physical Event Correlation. 12th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2024: 1–6.