A Comprehensive Review of Network Security Assessment Technologies

David Wilson[1]

1. David Wilson, Department of Information Technology, School of Computing and Digital Innovation, University of KwaZulu-Natal, South Africa

Correspondence: Department of Information Technology, School of Computing and Digital Innovation, University of KwaZulu-Natal, University Road, Westville Campus, Durban, 4000, South Africa

Abstract

With the rapid advancement of the Internet and information technology, networks have been deeply integrated into human life. However, the abundant Internet services and applications have also brought about increasingly severe network security issues. Network security assessment technology emerges as a proactive strategy to address these challenges. This paper first elaborates on the basic concepts of network security assessment (e.g., vulnerability, attack probability, risk value) and its research significance, emphasizing its role in proactive risk identification and threat mitigation. It then presents the architecture of network security assessment, which includes five key components: collection and preprocessing of original security events, correlation and merging of network events, security situation assessment, situation prediction, and situation visualization. Focusing on the current research status, the paper classifies assessment methods into three categories based on their principles: mathematical model-based methods, knowledge reasoning-based methods, and pattern recognition-based methods. Finally, the paper summarizes the existing challenges and prospects for future research directions in network security assessment.

Keywords: internet, information technology, network security, network security assessment

1. Introduction

With the rapid development of the Internet and information technology, computer networks have brought tremendous changes to people's ways of production, life, and learning. However, computer networks are like a double-edged sword. While bringing convenience, they also pose a series of problems, among which network security is a relatively serious one that causes great harm to us. Since the early days of computer development, network security issues have always accompanied the evolution of computers. To ensure network security to the greatest extent, people have been continuously checking and fixing operating system vulnerabilities, improving the security performance of devices, designing applications to be complete and rigorous during development, striving to formulate comprehensive and sound network management specifications, and strengthening the scientificity and professionalism of network management, always placing network security in an important position. Nevertheless, a large number of network security incidents still occur worldwide every year. Network security assessment has emerged as a new strategy to cope with network security issues under such circumstances. Network security assessment technology is an active defense technology. It proactively analyzes and assesses existing security risks and hidden dangers when no security incident has occurred, thereby enabling precautions in advance; when a security incident occurs, it promptly analyzes and assesses the threat situation of the incident and takes appropriate risk control measures based on the assessment results to curb the spread of threats.

2. Network Security Assessment Technology

2.1 Basic Concepts

a) Vulnerability: Vulnerability refers to a set of characteristics of the system itself, which attackers can exploit through authorized means to gain unauthorized access to resources on the system or cause adverse impacts on the system.

b) Attack probability: It refers to the likelihood of an attack occurring. Attack probability reflects the current security status of the network or information system, predicts possible security incidents, and serves as the basis for calculating risk values.

c) Risk value: It refers to the threats faced by the network or information system and the impact of threats on assets by exploiting vulnerabilities.

d) Network situation: It refers to the current state and changing trend of the entire network, which is shaped by factors such as the operation status of various network devices, network behaviors, and user behaviors.

e) Network situation awareness: Network situation awareness refers to the ability to acquire, understand, assess, display, and predict the future development trend of security elements that cause changes in the network situation in a network environment.

f) Network situation factor: It refers to important factors that can cause changes in the network situation.

2.2 Research Significance of Network Security Assessment Technology

To address increasingly prominent network security issues, academia and industry have proposed various security defense technologies and methods. In the initial stage of research on network security issues, academia and industry generally believed that network security issues mainly stemmed from vulnerabilities in system design. Therefore, they attempted to eliminate network security incidents by improving system details, increasing protocol complexity, and designing absolutely secure network systems. However, it was later found that this was impractical. In the middle stage, intrusion detection systems and security backup and recovery technologies were proposed, hoping to quickly detect attacks when they occurred, take corresponding measures to control and stop them, and effectively recover the system after it was compromised. In the current research stage, academia and industry believe that while striving to design more secure systems, it is also necessary to improve the system's attack recognition and recovery capabilities, strengthen scanning and detection of the current system, conduct risk assessments for networks and information systems, and implement risk control based on the results.

Network security assessment technology is an active defense technology. Before designing an absolutely secure system, enhancing the system's own defense capabilities remains the most effective way to deal with network security. The significance of network security assessment is reflected in:

a) Understanding the current security risks and threats faced by networks and information systems;

b) Predicting the possibility of potential attacks on networks and information systems, or predicting the network threats caused by attacks that have already occurred;

c) The results of security assessments can provide system managers with necessary defense measures or handling opinions.

3. Architecture of Network Security Assessment

A network security assessment system mainly focuses on the situation awareness of networks and information systems. Based on existing network security infrastructure and technologies, it draws on mature theories and technologies of situation awareness and applies them to the field of network security management. In complex and changing network security environments, it accurately extracts feature information and conducts correlation analysis to represent the macro and overall state of the network, thereby strengthening network management and control and improving network administrators' ability to manage the network.

3.1 Content of Network Security Assessment

The original information for network situation awareness mainly comes from various network security devices, network management devices, and network monitoring devices. Network situation awareness judges the network's security status and reflects the security change trends of networks and information systems by processing the collected data. Specifically, network security assessment mainly includes the following aspects:

a) Collection and preprocessing of original network security events. Collect complex, massive, redundant, and heterogeneous data generated by existing network security devices, network management devices, and network monitoring devices, preprocess them, extract feature information, simplify and store them, providing a data basis for subsequent data analysis and future data auditing.

b) Correlation and merging of network events. Conduct network security event mining based on preprocessed data to identify network attack events that cannot be detected by general network security devices from a macro perspective, improving the accuracy of network security detection and further reducing the false negative rate.

c) Network security situation assessment. It mainly uses corresponding mathematical assessment methods to quantitatively calculate the indicators of network security situation, and uses this value to reflect the security state of the network or information system in a certain period. The requirements for network security situation assessment are to quickly, objectively, and accurately reflect the actual security situation of the network, enabling network administrators to timely and accurately grasp network security dynamics and take effective precautions.

d) Network security situation prediction. Based on network situation assessment, it predicts the future development trend of network security situation, helping administrators take precautions in advance, do a good job in network security protection, and reduce potential losses caused by network security incidents.

e) Network security situation display. It is the presentation of network security situation assessment results, requiring efficient and intuitive all-round and multi-angle display of the current network security situation, so as to facilitate administrators to judge the network security status from various perspectives.

3.2 Current Status of Network Security Assessment Development

After years of research, the theory of network security assessment technology has become relatively mature. Some network security assessment methods are extensions of traditional methods, while others combine current theoretical innovations with situation assessment. Specific assessment methods or ideas include: fault tree model, attack tree model, privilege graph model, attack graph technology, Bayesian technology, support vector machine method, artificial neural network method, fuzzy logic method, analytic hierarchy process, multi-source information fusion theory, attack-defense game theory, evidence theory, set pair analysis theory, rough set theory, and grey relational analysis. An efficient and excellent network security assessment system is often formed by integrating several network security assessment methods.

According to the current status and development trend of network security assessment technology, assessment methods can be divided into three categories based on their principles: mathematical model-based methods, knowledge reasoning-based methods, and pattern recognition-based methods.

3.2.1 Mathematical Model-Based Methods

Mathematical model-based methods were the first to be used in situation assessment. This method constructs an evaluation function based on different factors affecting the network situation, and then aggregates multiple situation factors through the evaluation function to obtain the situation result. By drawing on some methods of traditional general multi-objective decision-making theory to solve situation assessment problems, this method has the advantage of intuitively reflecting the network security situation. For example, traditional weight analysis method and set pair analysis method belong to this model. However, there are many shortcomings in this method. For instance, there is no unified evaluation standard or measurement system for the construction of core evaluation functions and the selection of parameters in mathematical models, which often rely on the knowledge and experience of experts in this field, thus inevitably incorporating experts' subjective opinions.

3.2.2 Knowledge Reasoning-Based Methods

Knowledge reasoning-based methods are mainly used to handle situations that are difficult to address by mathematical models. Knowledge reasoning methods can simulate human thinking patterns, and compared with traditional mathematical models, the evaluation process has a certain degree of intelligence, which to some extent avoids the impact of human subjective factors on the objectivity of situation assessment. On the one hand, knowledge reasoning methods use fuzzy sets, probability theory, D-S evidence theory, etc., to process uncertain information; on the other hand, they aggregate multi-source and multi-attribute information through reasoning. Research hotspots in knowledge reasoning include security situation assessment methods based on fault tree models, attack tree models, privilege graph models, attack graph models, Bayesian networks, and hierarchical approaches.

The fault tree model describes the relationship between system internal faults and their causes. It was first proposed by Helmer to model attackers' intrusion behaviors, and Helmer used the fault tree model to analyze the description, identification, and detection of attackers' intrusions. Domestically, Zhang Tao used the fault tree model to describe and model the vulnerability relationships in computers, applying the theory of privilege escalation. The fault tree model can logically and clearly express the relationships between vulnerabilities in vulnerability assessment. However, the fault tree will grow exponentially with the increase in the number of logic gates and basic events, leading to the problem of combinatorial explosion.

The attack tree model was first proposed by Schneier based on the concept of the fault tree model. The leaf nodes in the attack tree represent attack methods, and the root node represents the attacker's goal. Nodes in the attack tree are divided into AND nodes and OR nodes. An AND node means that the parent node can only be achieved if all child nodes are achieved, while an OR node means that the parent node can be achieved if any child node is achieved. Clark et al. conducted qualitative and quantitative analysis of the attack tree by calculating the cut sets of vulnerabilities and the probability of vulnerabilities being exploited on the attack tree. Due to the clear logical expression ability of attack trees for various possible attack paths, it is convenient to conduct quantitative work such as probability calculation on attack trees. However, in specific applications, the structure of attack trees may become very large and complex. The scale problem of attack tree models restricts their application in practical vulnerability assessment.

The privilege graph model was first proposed by Dacier. Nodes in the privilege graph model represent a set of permissions, and directed edges represent vulnerabilities that cause changes in permission sets. A path in the privilege graph represents the process by which an attacker gains changing permissions by exploiting a series of vulnerabilities, i.e., expressing an attack path. The privilege graph model expresses the attack process of attackers exploiting vulnerabilities to escalate privileges in a graphical way, with good semantics and intuitive expression. However, the privilege graph only considers vulnerabilities related to privilege escalation, which limits its application in practice.

The attack graph technology uses directed graphs to express all possible attack paths through which attackers exploit existing vulnerabilities to attack networks or information systems, comprehensively reflecting the dependency relationships between the exploitation of vulnerabilities in networks or information systems. The attack graph was first proposed by Phillips and Swiler, who used the defined attack graph and attack graph-based algorithms to analyze network vulnerabilities. Fang Ming et al. proposed a distributed network security risk assessment method based on attack graphs. To overcome the insufficient connection between vulnerabilities in attack graphs, they introduced vulnerability correlation technology. Considering that attack graphs lack the ability to process quantitative indicators when describing attack paths, they used the probability of attack path formation to quantify information security risk factors. Aiming at the problem that the attack graph model cannot accurately infer the attacker's intention due to the uncertainty of single-step attack detection results, they introduced a transition probability table into the attack graph model to describe the uncertainty of single-step attack detection results. By collecting security attribute information such as network vulnerabilities, network topology, and asset value, and extracting dynamic attack-defense information such as intrusion detection system alarms, firewall policies, and security management, they generated dynamic attack graphs, adjusted defense measures in real-time to protect the network effectively, and assessed the security status of the network system in real-time. The attack graph model is one of the most effective models currently used in network security assessment to express vulnerabilities in networks or information systems and the correlation between vulnerabilities. However, it ignores factors such as asset distribution and threat distribution in networks or information systems that affect the possibility of attacks, making the assessment results unable to objectively reflect the risk status in the network.

Since the Bayesian network method can make full use of information such as the structure and vulnerabilities of attack graphs without the need to learn the structure and parameters of the network, and due to the advantages of Bayesian networks in probabilistic logical correlation reasoning, the Bayesian network-based method has become a research hotspot in network security situation assessment. In Bayesian network research, Poolsappasit et al. have done representative work. They constructed Bayesian networks based on attack graphs, then established alarm nodes as evidence nodes, and the attack probability of each node is the posterior probability of these evidences. Frigault et al. used Bayesian networks to analyze the inherent risks of networks and proposed dynamic Bayesian networks to include temporal characteristics such as vulnerabilities changing over time. Wu Jinyu pointed out that existing Bayesian attack graph models cannot express the impact of network operating environment factors on the possibility of attacks, and proposed a generalized Bayesian attack graph model, introducing attack benefits and threat state variables into this model. This enables the generalized Bayesian attack graph to include the impact of the business application environment and environmental threat information of the assessed network or information system on the possibility of attacks, as well as the propagation of these impacts in the generalized Bayesian network. The Bayesian network-based method makes full use of the causal correlation advantages and uncertain reasoning ability of Bayesian networks, resulting in relatively accurate assessment results. However, due to the need to establish conditional probability tables for all nodes, Bayesian network-based methods require more prior knowledge. In addition, limited by the complexity of Bayesian network reasoning algorithms, the performance of real-time assessment algorithms based on Bayesian networks is not high, making it difficult to meet the real-time assessment performance requirements of large-scale networks or information systems.

In research on D-S evidence theory-based methods, Sabata and Qu et al. proposed assessment methods based on D-S evidence theory to fuse distributed attack events, thereby achieving network situation awareness. Domestically, Wei Yong and Mei Haibin also proposed methods to conduct network security situation assessment by fusing multi-source data information using D-S evidence theory. Since the D-S evidence theory method assigns credibility to alarms and uses the advantages of D-S evidence theory in information fusion with noise to fuse relevant alarms, it can still obtain good threat situation results when there are false alarms in alarm information. In addition, the D-S evidence theory-based method has the advantages of requiring less prior knowledge and high algorithm performance. However, existing D-S evidence theory-based methods cannot restore attack scenarios, cannot identify attackers' intentions or predict specific upcoming attacks, and lack support for the problem of missing alarms.

The hierarchical assessment idea is also widely used in network security situation assessment. The hierarchical network security assessment method can display the magnitude of threats at different levels, making system threats clearer and more accurate. However, the division of levels in the analytic hierarchy process and the proportion of threats at each level require more prior knowledge, which limits its development to a certain extent.

Although knowledge reasoning-based network security assessment methods are relatively objective, comprehensive, and have a certain degree of intelligence, the biggest challenge they face is that knowledge such as reasoning rules and prior probabilities is difficult to obtain.

3.2.3 Pattern Recognition-Based Methods

With the development of machine learning technology, pattern recognition methods have been introduced into the research of network security situation assessment. This method draws on the concept of data mining algorithms, mainly relying on mining situation patterns from training samples or historical data for situation assessment. This method has strong learning ability, and its process is mainly divided into two stages: pattern establishment and pattern matching. Representative works using this method in network security situation assessment include: support vector machine method, neural network-based method, grey relational analysis, rough set theory, and hidden Markov model-based situation assessment method. In hidden Markov model (HMM)-based methods, Ourston et al. used HMM to model network attack processes, described the change process of network security status using hidden Markov models, and then used this model to assess network security situation. Although pattern recognition-based methods have the characteristics of objectivity in situation assessment, they require a large amount of training data to learn parameters in the model. However, general networks or information systems often find it difficult to obtain such data. Moreover, these methods fail to utilize prior knowledge such as attack correlation, making it difficult to predict specific attacks.

4. Summary

The rapid development of networks and information systems has made security issues increasingly important and severe. Before designing an absolutely secure system, network security defense systems remain the main way to combat network threats, and network security assessment technology is still an important force in network security defense. This paper comprehensively introduces various technical methods of network security assessment. Mathematical model-based methods can conveniently and intuitively reflect the security status of network systems, but the construction of functions and selection of parameters are subjective, varying from person to person and limited by the author's knowledge reserve and subjective will. Knowledge reasoning-based methods are still current research hotspots with many research results. They reduce the risk of subjective influence on network system security evaluation to a certain extent, but the intelligence of this assessment method is low, and it is limited by the formulation of reasoning rules and the acquisition of prior probabilities. Pattern recognition-based methods have good intelligence but require a large amount of training data to learn parameters in the model. Current cloud computing and big data processing technologies can be applied to pattern recognition-based assessment methods to solve the problem of obtaining and training samples. At present, none of these methods are completely universal or optimal; each has its own strengths and weaknesses. To design an efficient, reliable, and comprehensively detecting network security assessment system, it is necessary to integrate multiple methods and learn from each other's advantages.

Looking back at the development history of network security assessment, network security assessment technology has evolved from initial manual assessment to current automatic assessment, from previous local assessment to current overall assessment, and from original single-machine assessment to current distributed assessment. Network security assessment technology is moving towards intelligence, comprehensiveness, and scale.

References

Clark, J., & Wilson, M. (2001). Qualitative and quantitative analysis of attack trees with vulnerability cut sets. *Proceedings of the 10th IEEE International Workshop on Computer Security Foundations* (pp. 87–98). IEEE.

Frigault, M., Wang, L., Singhal, A., & Jajodia, S. (2008). Measuring network security using dynamic Bayesian networks. *Proceedings of the 4th International Workshop on Security Measurements and Metrics* (pp. 23–30). ACM.

Helmer, R. (1995). Modeling attacker intrusion behaviors with fault tree analysis. *Journal of Computer Security, 3*(2), 117–134.

Ourston, D., Matzner, S., Stump, W., & Hopkins, B. (2003). Applications of hidden Markov models to detecting multi-stage network attacks. *Proceedings of the 36th Hawaii International Conference on System Sciences* (pp. 334–342). IEEE.

Phillips, C., & Swiler, L. P. (1998). A graph-based system for network-vulnerability analysis. *Proceedings of the Workshop on New Security Paradigms* (pp. 71–79). ACM.

Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing, 9*(1), 61–74.

Sabata, B., & Qu, G. (2001). Network security assessment using evidence fusion. *Proceedings of the 5th International Conference on Information Fusion* (pp. 1466–1473). IEEE.

Schneier, B. (1999). Attack trees. *Dr. Dobb's Journal, 24*(12), 21–29.

Swiler, L. P., Phillips, C., & Gaylor, T. (2001). A graph-based network-vulnerability analysis system. *Sandia National Laboratories Technical Report*.

Copyrights