Research on network vulnerability assessment based on attack graph and security metrics

Wanzhi Ma
Dept. of Education and Cultural Information Development, Woosuk University, South Korea.

Corresponding author and e-mail: Wanzhi Ma, 997443418@stu.woosuk.ac.kr

Abstract. In recent years, the information security environment is undergoing great changes. On one hand, with the development of technology and the advancement of network integration, network involves in a larger and larger scale, and its structure is becoming more and more complex. On the other hand, the development of attack technology has also taken a qualitative leap. The ability of violent cracking and the scale of botnets are no longer the primary factors that determine the attack effect. On the contrary, attackers are more likely to adopt information-driven complex combination attacks with clear attack targets. These changes have brought great challenges to network security defense. Therefore, from the perspective of building a secure network environment, this paper studies network vulnerability assessment in the field of computer network security, and proposes a method of network vulnerability assessment based on attack graph and security metrics. This method models and constructs the attack graph for the possible network attack behaviors. Besides, taking it as the analysis model, the risk assessment technology is taken to determine the indicators and calculating methods of security metrics so as to realize the evaluation of network vulnerability. Finally, the discussion was conducted based on the results, and a follow-up study was suggested.

1. Introduction

With the rapid development of network technology, people's requirements on network security mechanism are also increasing. Due to the existence of various network system vulnerabilities, potential misoperation, cyber crimes and other dangerous factors, the need for network security evaluation technology is more and more urgent.

As one of the research hotspots in the field of network security, network vulnerability assessment is different from other general performance evaluation techniques. For example, intrusion detection, firewall and virus scanning are all passive detection during or after the attack, while network vulnerability assessment is developed from hacker attack and prevention technology, which is an active detection before the attack. Therefore, it is a key step to build a security model for the attacking behavior when evaluating network vulnerability. On the other hand, the possible behaviors and states of the system can be obtained according to the security model, and further analysis and calculation can be carried out on this basis, providing help for improving the system security policy.

Based on the previous work, the paper proposes a new method of network vulnerability assessment based on attack graph and security metrics. The main features of the method are: attack graph is constructed by simulating the scene of attack process, and form analysis model. Besides, the
Qualitative and quantitative security metrics are developed in virtue of risk assessment technology, and then the overall assessment of network vulnerability is required.

The vulnerability assessment method in the field of network security originates from the hacker attack technology and the prevention technology of hacker attacks. Later, with the expansion of network scale and the increase of the applications, the network vulnerability assessment method has been developed in order to meet the current needs. At the beginning of vulnerability assessment, it is mainly to test more computer system security through utilization of accumulated experience in practice, and it has become the focus of research that how to produce more accurate and complete verification rules. Actually, this method is a kind of rule matching. And then with the constant changes of the network environment, this rule-based assessment method can no longer satisfy the requirements of security evaluation due to its inherent shortcomings.

With the development of mathematical tools, researchers began to use fault trees, graphs, finite-state machine and others as tools to carry out the network vulnerability assessment. The research of vulnerability assessment method has become a new direction. The vulnerability assessment methods have experienced the developments and changes of many stages, and the assessment methods are becoming more and more mature. Evaluation methods and models are becoming more and more abundant. Throughout the development history of vulnerability assessment methods, the developing process of vulnerability assessment can be generally summarized as the following characteristics: ① Developing from manual assessment to automatic assessment; ② Developing from host-based assessment to network-based assessment; ③ Developing from qualitative assessment to quantitative assessment; ④ Developing from rule-based assessment to model-based assessment.

2. Methodology

2.1. The concept of network security vulnerability assessment

The basic attributes of network security include three aspects: confidentiality, integrity and usability. Network vulnerability assessment is the security evaluation for the basic attributes aiming at software vulnerabilities, error distribution and protocol vulnerabilities in the network, and then predicts the possible threats and attacks on the network. Further, based on the analysis of network loss according to the value of network resources, the influence degree of the vulnerabilities on the network security is evaluated and then the defensive scheme is proposed. In the process of vulnerability assessment, three key evaluation points of basic attributes are introduced respectively:

(1) Confidentiality. Confidentiality requirement means that the network information is not allowed to leak, and cannot be accessed and checked by unauthorized persons, and the information in the network cannot be read randomly.

(2) Integrity. Integrity requires that the data in the network is complete and not distorted.

(3) Usability. Usability requires that users are not affected by other factors when obtaining information in the network and they can normally get the information they need.

2.2. Attack graph technology

2.2.1. State attack diagram. In 1998, Swiler proposed the state attack graph method (figure 1) to take network topology information into consideration in security analysis. The nodes in the state attack graph represent the network state after a certain vulnerability is exploited, and the network state information includes the host name, user rights, impact of attack and so on. In the state attack graph, nodes are connected by directed edges, and they indicates the behavior that causes the state changes, including the behavior of network attacker, user and backdoor program. Directed edges point from their original state to the state transferred from certain behaviors happening in the network.
2.2.2. Attribute attack graph. Attribute attack graph is to solve the problem of attribute explosion of attack graph and proposes that the network security elements are used as independent vertices and the same vulnerability on the same host computer only corresponds to an attribute vertex in this graph. As a result, compared with state attack graph, attribute attack graph can be generated in a fast and its structure is simple, which has a better adaptability for large-scale network (figure 2).

2.2.3. Model detection technology. Swiler and other people proposed that the attack graph automatically generated model, and the generation process was relatively complex. To simplify the generation complexity of attack graph, the researchers proposed an automatic generation method of attack graph based on model detection technology (SMV/Nu SMV). Model detection technology is a formalization method to verify whether a system satisfies its specific attributes. The model is shown in figure 3. When using model detection technology to construct attack graph, the network is regarded as a finite-state machine, and state transition represents atomic attack. Besides, CTL (Computation Tree Logic) is adopted for security policy coding. The model detector detects the network, and if it finds
that the security policy is violated, it will produce an attack graph containing all counter cases, that is, all possible attacks on the network. Examples of using CTL to encode security attributes are as follows:

\[ P = AG(\text{network.adversary.privilege} \geq \text{network.priv.root}) \]

That is, the permission of the network attackers should be less than root permission, which is a necessary policy for network security. The advantage of model detection technology is that it can use mature model detection tools to automatically generate attack graph. Since this method generates state attack graph and the model must contain all states of the network, it is easy to cause state explosion which makes it difficult to handle large scale network. In order to simplify the complexity of the algorithm, Ammann proposed the monotonicity hypothesis about network attack, which is that attackers will not repeat the attack actions that can obtain the existing permission. Based on this assumption, the complexity of automatically generating attack graphs is greatly reduced.

![Figure 3. Model detection technology.](image)

2.3. Attack graph model

The attack scene is modeled by using attack graph, focusing on network topology and attack behavior set. Through the attack graph, the path of all possible attack behaviors in the system can be described and the causal relationship between attack actions can be reflected. A simple attack graph example is shown in figure 4.

![Figure 4. An example of attack graph.](image)

The generating algorithm of attack graph focuses on the action sequence in the attack scene model: the movement of the attacker's position, the detection of active host's scanning action, the attack action against the vulnerability, etc. The nodes in the attack graph contain the state information of the object, and the directed edges between the nodes indicate the state changes caused by the attack action.

Formally, the attack graph is represented by the quadruples \( G = (S, R, S_0, S_s) \). Among them, \( S \) is the collection of state nodes; \( R \subseteq S \times S \), and it shows transition relation which is the state change; \( S_0 \subseteq S \) which is the collection of initial states; \( S_s \) is a collection of the target states (that is, the successful
state of attack). The attack path is a group of connected nodes in the attack graph. The first node represents the initial position of the attack, and the last node represents the end of a series of attacks.

For a target state Sn ∈ S, if it starts at the initial state of S0, there is a set of state sequences including S1, S2, ⋯, Sn-1 which leads to the result (Si, Si+1) ∈ R, 0 ≤ i ≤ n-1, S0, S1, ⋯, Sn is an attack path. After the attack graph is generated, the security metrics are carried out based on the analysis of the model.

2.4. The analysis and calculation of security metrics

Network vulnerability assessment needs to take into account many complex factors in attack scene, including network connection state, host attributes, vulnerability types, attackers' technology and tools, attack actions and attack sequences, and the impact caused by attacks. Many of these factors can’t be clearly quantified, directly measured and calculated. Therefore, the core problem of network vulnerability assessment is how to measure and comprehensively evaluate various security characteristics of the system. To carry out security metrics, the system and its security characteristics firstly need to be modeled. Traditional security metrics usually focus on the number of vulnerabilities in the system or the number of security events occurring over a period of time. These metrics ignore the correlation between the components in the network and lack the basis for quantitative calculation. By establishing attack graph as a model of security metrics, it is possible to consider the combination of individual security metrics when evaluating network vulnerability. Then we need to determine the specific security metrics indicators. There are many uncertainties involved in the process of security metrics, and some of them can be quantified while others cannot be directly quantified, therefore, when selecting and analyzing the metrics indicators, the combination of qualitative principle and quantitative principle should be followed, and the purpose is to generate quantifiable data, so that the evaluation results can be compared. Based on the idea of risk assessment, the paper concludes the evaluation of network vulnerability as the evaluation of the system’s security risk, and then the selection and analysis of security metrics can be summarized as the selection and analysis of risk factors.

Risk is generally defined as the potential possibility of capital loss caused by certain threats aiming at for system vulnerability. In the network environment, supposing that an attack action uses a security vulnerability to form a threat T, when T acts on a specific asset and causes loss L, then L not only depends on the severity of the attack action and the vulnerability, but also on the importance of the asset C which is simply written as L ∼ (C, T). The risk value R is determined by the probability P of threat and loss arisen from threat, and is recorded as R ∼ (L, P). It can be concluded that R ∼ (C, L, P), that is, the security risk of the system is determined by the three metrics - asset importance, threat loss and threat rate.

Aiming at the metrics, the combination of qualitative and quantitative methods is used to evaluate the risks.

(1) According to the specific network environment, the importance of assets in the system is given through qualitative analysis, and then the existing vulnerabilities in the system and various possible attack behaviors should be determined. At the same time, according to historical data and expert experience, the probability of various attacks should be determined.

(2) Quantitatively assign or set levels for the above metrics. In this step, the paper refers to the standard CVCS(Common Vulnerability Scoring System). Specific metrics include the following three items:

1) The importance of host criticality Criticality (h), ∀ h ∈ [1, NH], NH is the number of hosts. The metrics are usually assigned different levels based on the role of the host in the system. For example, crucial network components such as hosts, DNS servers, or domain controllers that contain important data, should be given a higher level of importance.

2) The danger degree of attack – Severity (a), ∀ a ∈ [1, NA], NA represents the number of actions. The metrics can be obtained by checking the BaseScore index of CVSS.
3) Loss caused by attacking the host Loss \((a, h) = \text{Severity}(a) \times \text{Criticality}(h), \forall \ h \in [1, NH], \forall \ a \in [1, NA]\). The value of loss should be expressed in numerical value as far as possible, or the amount of time, that is, the time required to repair the loss.

(3) Calculate the probability and risk value of successful attack. According to the attack graph model, the probability of successful attack can be calculated quantitatively. From the perspective of the system layer, the attack action has a certain randomness, and its probability of success is affected by many factors, such as the attacker's knowledge of the target network, the vulnerability utilization technology and tools, and the reliability of the scanning results. By weighting the probability of successful attack action to each corresponding edge of the attack graph, the total success probability of each attack path can be calculated. Supposing that an attack sequence consists of \(n\) attack actions, that is, \(A_1 \rightarrow A_2 \rightarrow \cdots \rightarrow A_n\), and the success probability of \(A_i\) is \(P_i\), \(i = 1, 2, \ldots, n\), the success probability of the attack sequence is shown as:

\[
P = \prod_{i=1}^{n} P_i
\]

The evaluation value is given to the nodes of the attack graph, indicating the loss expectation of the attack state corresponding to the node. Therefore, the total evaluation value of an attack sequence is the total loss expectation of the attack sequence. Assuming that the probability of successful attack from the state \(S_i\) to the state \(S_{i+1}\) is \(P_{i,i+1}\), the success probability from initial state \(S_0\) to the \(i\)th state \(S_i\) according to (4) is

\[
P_{0,i} = \prod_{j=0}^{i-1} P_{j,j+1}
\]

Assuming that the value of loss expectation of \(S_i\) is \(L_i\), the total loss expectation of the attack path is

\[
R = \sum_{i=1}^{n} L_i P_{0,i}
\]

(4) Judge the overall security level of the network according to the overall risk value, and form effective suggestions of security policy.

3. Conclusions
In order to provide a rigorous protection scheme for network security and to bring accuracy to data evaluation, the network vulnerability assessment method based on attack graph and security metrics comes into being, which can reduce deviation problems in computing probability and enhance the objectivity of computing concept. By constructing attack graph as analysis model, the method uses risk analysis technology to carry out security metrics, so that it can analyze and evaluate network vulnerability as a whole.

Future research will adopt more optimized generating algorithm of attack graph aiming at important network resources and improve the automation of security metrics calculation. The following research will verify the network vulnerability assessment methods with attack graph and security measure through data collection, comparative analysis and quantitative verification, so as to highlight the advantages of the model.

References
[1] Xing xujia, Lin chuang, Jiang Yixin. Research on vulnerability assessment of computer system [J]. Computer journal, 2004, 27(1).
[2] Ma Junchun, Sun Jiying, Wang Yongjun, etc. A vulnerability assessment method based on vulnerability point dependence graph[J]. Journal of Dalian maritime university (natural science edition), 2010, 36(4).
[3] Cheng Guangquan, Lu Yongzhong, etc. Evaluation of the importance of complex network nodes and analysis of network vulnerability [J]. Journal of National Defense University of Science
[4] Jin Weixin, Song ping, Liu Guozhu. Vulnerability analysis of interdependent networks based on correlation distribution function [J]. Complex morphology and complexity science, 2016 (12).

[5] Wang Xiujuan, Sun Bodeng. The network vulnerability assessment of bayes attribute international graph [J]. Journal of Beijing university of posts and telecommunications, 2015 (8).

[6] Zhang Hongbin. Encoding method of 3D-HEVC deep image fast frame [J]. China image graphics journal, 2016 (7).

[7] Li Qingpeng, Wang Buhong. Network security metrics method based on probability of attack graph nodes [J]. Computer application research, 2012 (11).

[8] Krusil I V. Software vulnerability analysis[D]. Purdue University, 1998.

[9] Bishop M. A taxonomy of unix system and network vulnerabilities[R]. Technical Report CSE-95-10, Department of Computer Science, University of California at Davis, 1995.

[10] Ritchey R W, Ammann P. Using model checking to analyze network vulnerabilities[J]. Security and Privacy Proceedings. 2000 IEEE Symposium on, 2000:156 - 165.

[11] Ammann P. Scalable, graph-based network vulnerability analysis[J]. In Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002.

[12] Xiangdong Xu, Anthony Chen, Chao Yang. An Optimization Approach for Deriving Upper and Lower Bounds of Transportation Network Vulnerability under Simultaneous Disruptions of Multiple Links[J]. Transportation Research Part C, 2017.

[13] Delu Wang, Jingying Li, Yadong Wang, Kaidi Wan, Xuefeng Song, Yun Liu. Comparing the vulnerability of different coal industrial symbiosis networks under economic fluctuations[J]. Journal of Cleaner Production, 2017, 149.

[14] Jun-Qiang leng, Jing zhai, Qian-Wen li, Lin zhao. Construction of road network vulnerability evaluation index based on general travel cost[J]. Physica A: Statistical Mechanics and its Applications, 2018, 493.

[15] KIJSANAYOTHIN P, HEWETT R. Analytical approach to attackgraph analysis for network security[C]/Proc of International Conference on Availability, Reliability and Security. [S. 1.]: IEEE Computer Society, 2010: 25-32.

[16] Heinz Hofbauer, Andreas Uhl. Identifying deficits of visual security metrics for images[J]. Signal Processing: Image Communication, 2016, 46.

[17] Patrick Morrison, David Moye, Rahul Pandita, Laurie Williams. Mapping the field of.