Internal Network Security Attack Probability in Attack Graph

Boreda Varsha[1], Dutta Sai Eswari[2] & M. Sreelaxmi[3]

[1]Assistant Professor, CSE Dept, KMIT, Narayanaguda, Telangana, varsha5592@gmail.com
[2]Assistant Professor, CSE Dept, KMIT, Narayanaguda, Telangana, saieswari3@gmail.com
[3]Assistant Professor, CSE Dept, AAR Mahaveer Engg. College, Telangana, sreelaxmiguggilla@gmail.com

Abstract: **Security metrics in the networks may provide quantifiable proof to help security specialists in making sure about PC networks. In any case, research on security measurements dependent on the attack graph isn't relevant to the qualities of inward assault; consequently, here proposed an inside network security metric strategy dependent on attack likelihood. This methodology has the accompanying advantages: it gives the technique for attack graph rearrangements with observing the nodes which could solve the attack graph exponential development with the network size while extracting the hidden of internal attacks and improving the productivity of the whole strategy; the strategy for attack likelihood estimation dependent on simplified attack graph can streamline the accuracy and unpredictability of inner attacks and improve the exactness of the methodology.**

Index Terms— **internal attack, attack graph, exponential growth.**

1. INTRODUCTION

According to the definition and analysis of internal attacks provided by Computer Emergency Response Team (CERT) [1], the internal attacks have the transparency to defense intercepts, such as access control or firewalls. Internal attacks also have the camouflage system privileges, high risk to access the core confidential resources easily, and the complexity of gradual attacks. The security metric as a proactive defines technology, whose role is actively analysing and evaluating what is existing in the current security risks or potential security risks before the attacks.

When the attack action occurred, the security metric method needs to analyze and assess the threat of attack incidents, then predict the attack paths, and take the analysis method in network security can be divided in to two types: one is the unknown vulnerabilities in a network, mainly considering the prevention measures; the other one is the known vulnerabilities in a network, repairing the weak parts of the network and improving the security of the whole network [2]. As for the unknown vulnerabilities, the information security experts have already carried out a lot of research; the main methods are as follows:

(i) Analysis protocol vulnerabilities, such as ARP address resolution protocol: researchers try to find out the protocol vulnerabilities, sum up the vulnerability in some areas, give the solutions for the lack of agreement, and achieve the purpose of prevention.

(ii) Analyze the source code of the software: mistakes are unavoidable when programming, such as buffer overflow vulnerabilities. By studying some important codes, researchers take necessary precautions against possible errors and give patches of software, so as to improve the overall safety of software.

Although these methods are effective, they are very abstract and not easy to implement, and the results are relatively few. But if we start from the known network security vulnerabilities, it is relatively easy, for example, all kinds of graph theory-based model checking methods, such as attack graph. The attack graph is a sort of graph hypothesis technique to pass judgment on the network security by contemplating the nodes and the connection between nodes in the network.

By building the genuine network into a hypothetical graph hypothesis model, the attack graph can give us numerous spots to think profoundly, some of the time with unforeseen outcomes. For instance, building a model from the realized perspectives to improve or admire the real components permits us to concentrate on the most significant or significant parts of cybersecurity, disregarding the optional and rapidly deciding the security of the network.

The attack graph model has extraordinary preferences over other evaluation models, getting one of the most broadly utilized and most considered security measurements models. In spite of the fact that the attack graph can outwardly demonstrate the starting point and goal of the network attack, it can't quantitatively describe the network security.

So as to direct quantitative investigation of the chance of attacks, we present the aggregate reachable likelihood for every node. Most importantly, we proposed an inward network security metric strategy dependent on attack likelihood to tackle the issue of the current security measurements with attack graph

2. RELATED WORK

The numerous existing researches on network security metrics based on attack graph mainly focus on the representation of attack graph models, the metrics of indicators, and the conclusions of network security metric. Those early researchers conducted research mainly including the following aspects.

The representation of attack graph models. Xie et al. [3] firstly explored three sources of uncertainty in the attack graph, but the attack graph model they established is carrying on probability derivation only when the attack behaviors are determined, resulting in the fact that the probability of uncertainty testing data is not calculated in the final derivation process.

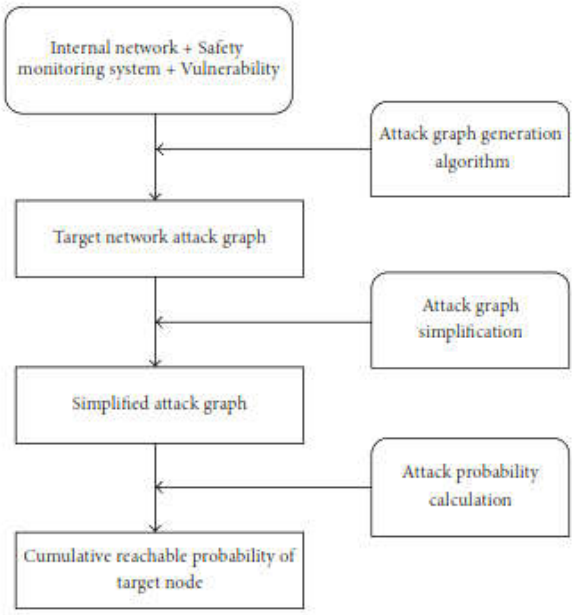


Fig 1: The schematic diagram of internal network security metric based on attack probability

Wang et al. [4] proposed the probabilistic attribute description of the attack graph based on the probability of attacks and the cost of the network deployments, using the method of cumulative reachable probability to evaluate the safety of the

whole network, but they did not take into account the impacts of other uncertain factors.

The metrics of indicators: Li et al. [5] used CVSS to evaluate vulnerabilities and proposed a general approach for the network security metrics based on vulnerabilities, but they only considered the probability of a single vulnerability node, while ignoring the vulnerability of the vulnerability node in the whole system, especially the indicators between the vulnerability nodes.

The conclusions of network security metric: in terms of attack probability calculation, Wang et al. [6] use Bayesian network algorithm to calculate the risk probability for internal nodes and quantify the node variables, the node variable values, and the conditional probability distribution. Based on the improved likelihood weighting algorithm, the calculation of Bayesian network node parameter is more convenient; the internal threat forecast also is more accurate. However, this approach did not take into account the vulnerability of their own indicators. Zhang et al. [7] proposed satisfying the temporal order of attack evidence, using the Bayesian network algorithm to analyze the security for all attack paths. However, the probability confidence of nodes in the attack graph is complicated and lacks mathematical theory, and the computational model is also too complicated to work efficiently.

Proposed an internal network security metric of the attack probability based on the attack graph model [8]. Because of the internal attack's characteristics of camouflage and complexity, we decided to add the monitoring event node and the key-value pair in the attack graph. Compared with other security metrics, our internal network security metric improved the efficiency and the accuracy obviously with the help of attack graph simplification method and cumulative reachable probability calculation method [9].

3. Internal Network Security Metric Based on Attack Probability

3.1 Method Overview

In order to understand the characteristics and the occurrence environment for the internal attacks, first of all, according to the original attack graph and the attack evidence provided by the security monitoring system, we could get the temporal difference relationship of the monitoring event nodes and simplify the attack graph with the temporal difference relationship [10].

Second, we divide the simplified attack graph into key-value pairs and then calculate the probability of the key-value pairs. Third, we calculate the cumulative reachable probability by the method of attack probability calculation we proposed. Finally, the quantitative evaluation of the current internal network is represented by the cumulative reachable probability of target node. The specific steps are shown in the above Figure 1.

3.2 The Attack Graph Model

Based on the complexity of internal attacks, internal attack events are mostly multistep and continuous attack behaviors. An attack event includes multiple attack subtargets and a series of related sub attack events; that is, from a resource node to the next resource, the event requires a minimum set of basic attack actions [11].

In the initial stage, the attacker has a certain system access or operating authority and through an

atomic attack can help the attacker to reach the next state node, so as to obtain more resources and permissions to achieve the next attack subtarget [12]. Therefore, in the attack graph model constructed in this paper, the resource state node is mapped to the original attribute node; the attack action node is mapped to the original atomic attack action node.

The attack graph model includes the following contents

(1) The Atomic Attack: An attack action is a different instruction or a set of operations, which could divide into different basic actions. For example, to open a word file, we need two methods. Method 1: open the file by double- clicking it; Method 2: click on the file, and then click "Enter" to open it. These two methods can open the file but are composed of different operations; we will set those different but similar function operations or instructions as one basic action. And from one resource state node to another resource state node, the attacker needs a combination of multiple basic actions to achieve; such a series of basic actions is called the atomic attack. An atomic attack is the minimum set of basic actions that an attacker needs from a resource state node to another resource state node.

(2) The Monitoring Event Node: In order to simplify the attack graph, the monitoring event node is introduced in the attack graph model. Because each atomic attack contains a series of the basic attack actions, although the internal attack has camouflage, some basic actions more or less will trigger the security monitoring system, and attacks and other related information will be recorded in alarm log.

The set of information recorded in the alarm log is called attack evidence. The monitoring event node refers to the attacker from one resource state to the next resource state, and the implementation of atomic attack triggers the monitoring system, recorded in the alarm log as attack evidence. We use one monitoring event node to record one kind of atomic attack's set of basic actions execute time sequence.

Fig 2: 'AND' Relationship between two state nodes.

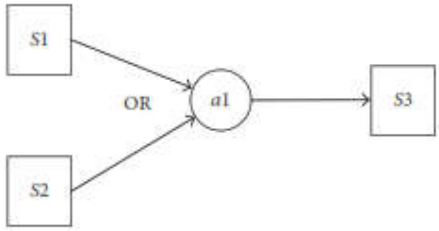


Fig 3: 'OR' Relationship between two state nodes.

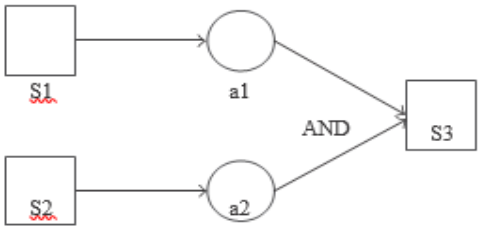


Fig 4: The "AND" relationship between two attack action nodes.

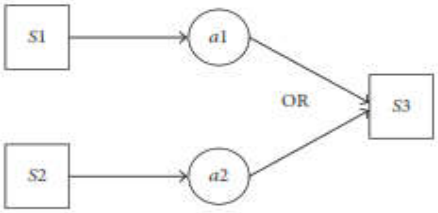
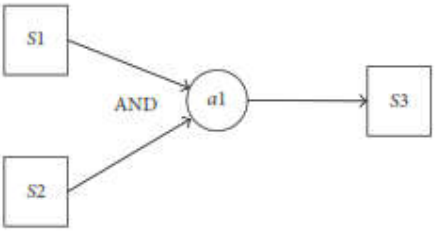


Fig 5: The "OR" relationship between two attack action nodes.



The cumulative reachable probability of the first resource state node in the key-value pair. Then, we can calculate the cumulative reachable probability of current action node.

4.CONCLUSION

In our paper, has to analyses an internal network security metric method based on attack probability to solve the problem of the existing security metrics based on attack graph lacking the simulation results show that the method of attack graph simplification has a significant improvement in efficiency, and the method of attack probability calculation improves the quantitative analysis accuracy obviously. The next step of the work will focus on the refinement attack probability calculation, finding a more comprehensive internal network to improve the accuracy of the final probability value.

References:

[1] G. Yang, J. Ma, and A. Yu, "Study on internal threat detection," Journal of Information Security, vol. 1, no. 3, 2016.

[2] X. Lu, "Research on information system security metrics theory and method," *Computer Science*, vol. 35, no. 11, pp. 42–44, 2008.

[3] P. Xie, J. H. Li, X. Ou et al., "Using Bayesian networks for cyber security analysis," in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems & Networks*, vol. 23, pp. 211–220, 2010.

[4] L. Wang, T. Islam, T. Long et al., "An Attack Graph-Based Probabilistic Security Metrics," in Proceedings of the Conference on Data & Applications Security XXII, 5094, pp. 283–296, 2008.

[5] Q. Li, B. Wang, X. Wang et al., "Network security measurement method based on probability of attack graph node," Application Research of Computers, vol. 30, no. 3, pp. 906–908, 2013.

[6] H. Wang, G. Yang, and D. Han, "Study on internal threat prediction based on Bayesian networks," Application Research of Computers, vol. 30, no. 9, pp. 2767–2771, 2013.

[7] S. Zhang, G. Li, S. Song et al., "Application of Bayesian Rea- soning in the Confidence Calculation of Attack Graph Node," Journal of Software, vol. 21, no. 9, pp. 2376–2386, 2010.

[8] N. Prosaposin, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, pp. 61–74,2012.

[9] X. Chen, B. Fang, Q. Tan et al., "Study on inference algorithm of internal attack intention based on probability attack graph," Journal of Computers, vol. 37, no. 1, pp. 62–72, 2014.

[10] Y. Ye, X.-S. Xu, Y. Jia, and Z.-C. Qi, "An attack graph-based probabilistic computing approach of network security," Jisuanji Xuebao/Chinese Journal of Computers, vol. 33, no. 10, pp. 1987–1996, 2010.

[11] X. Ou, S. Govindavajhala, and A. W. Appel, "MULVAL: a logic- based network security analyzer," in Proceedings of the 14th Usenix Security Symposium, pp. 113–117, Baltimore, MD, USA,2005.

[12] D. Wu, D.-G. Feng, Y.-F. Lian, and K. Chen, "Efficiency evaluation model of system security measures in the given vulnerabilities set," Journal of Software, vol. 23, no. 7, pp. 1880–1898, 2012.