2012 IEEE 18th International Conference on Parallel and Distributed Systems

Cyber Attacks Prediction Model Based on Bayesian Network

Jinyu Wu[1, 2]
[1]Institute of Information Engineering,
Chinese Academy of Sciences,
Beijing, P. R. China.
[2]School of Computer Science,
Beijing University of Posts and Telecommunications,
Beijing, P. R. China.
eyoudian19@gmail.com

Lihua Yin
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, P. R. China
yinlihua@nelmail.iie.ac.cn

Yunchuan Guo
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, P. R. China
guoyunchuan@nelmail.iee.ac.cn

***Abstract*—Cyber attacks prediction is an important part of risk management. Existing cyber attacks prediction methods did not fully consider the specific environment factors of the target network, which may make the results deviate from the true situation. In this paper, we propose a cyber attacks prediction model based on Bayesian network. We use attack graphs to represent all the vulnerabilities and possible attack paths. Then we capture the using environment factors using Bayesian network model. Cyber attacks predictions are performed on the constructed Bayesian network. Experimental analysis shows that our method gets more accurate results.**

Keywords- network security; quantitative assessment; cyber attacks prediction; attack graph; Bayesian network

I. INTRODUCTION

Cyber attacks prediction is an important step of risk management. The prediction results reflect the security situation of the target network in the future, and security administrators can take corresponding measures to enhance network security according to the results. To quantitatively predict the possible attack of the network in the future, attack probability plays a significant role. It can be used to indicate the possibility of invasion by intruders. As an important kind of network security quantitative evaluation measure, attack probability and its computing methods has been studied for a long time. Many models have been proposed for performing evaluation of network security. Graphical models such as attack graphs become the main-stream approach. Attack graphs which capture the relationships among vulnerabilities and exploits show us all the possible attack paths that an attacker can take to intrude all the targets in the network. However, existing analysis methods [1], [3], [4], [5], [6] did not consider the specific environment factors of the target network.

Let us look at an example shown in Fig. 1. Consider 4 running circumstances which have the same network and the same vulnerabilities in the network: (1) Web Server, FTP Server and Mail Server have about the same frequency of use by users; (2) Web Server has been heavily used, but FTP Server and Mail Server have been rarely used; (3) all of the data in Web Server, FTP Server and Mail Server are not important; (4) the data in FTP Server is very important and valuable, while the data in Web Server and Mail Server are not. We can easily conclude by common sense that Web Server in case 2 will be more likely attacked by intruder than that in case 1, and FTP Server in case 4 will be more likely attacked by intruder than that in case 3.

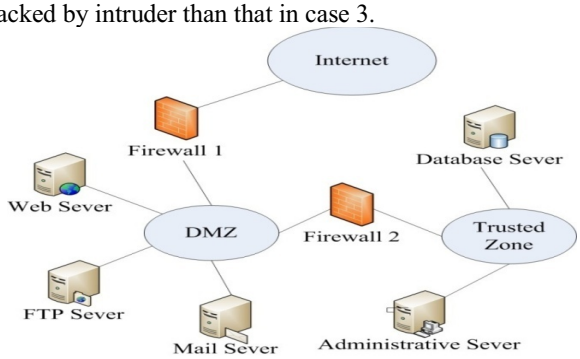

Figure 1. An example network.

Therefore, the environment information is important for getting accurate results of security evaluation.

In this paper, we propose a cyber attacks prediction model based on Bayesian network (BN). We model the influencing factors of attack probability by using Bayesian network model. After constructing the Bayesian network, we compute the attack probabilities on the constructed Bayesian network. Experimental analysis shows that our method leads in more accurate results.

II. THE CYBER ATTACKS PREDICTION MODEL

In our cyber attacks prediction model, we use attack graph to capture the vulnerabilities in the network. In addition we consider 3 environment factors that are the major impact factors of the cyber attacks in the future. They are the value of assets in the network, the usage condition of the network and the attack history of the network.

A. The Vulnerabilities in the Network

Without vulnerabilities, the network will be attack-free in technical point of view. Intruders exploit vulnerabilities in the hosts of the network to intrude the target and get what

1521-9097/12 $26.00 © 2012 IEEE
DOI 10.1109/ICPADS.2012.117

they want. So we have to find out all the vulnerabilities in the network and analyze them in global vision.

A lot of vulnerability scan tool such as Nessus, X-Force and etc, can be used to find out all the vulnerabilities in the network. Then we can use attack graph generation tool like the MulVAL attack graph toolkit [2] to generate the corresponding network attack graph which gives the full view of all the vulnerabilities and their interdependence. There are two kinds of node in the attack graph: condition nodes and exploit nodes.

B. The Value of Assets in the Network

All the devices in the network have different values according to the values of the data in the devices, the importance of the position the devices in the network and etc. For example, a host containing important data is more valuable than the one that has not, and a host is the gateway of the network is more valuable than the one that is not. The more valuable the device is, the more possible it will be attacked by the intruder. To capture the value of assets in the network, we use the BN structure shown in Figure 2 to model the factor of the values of assets.

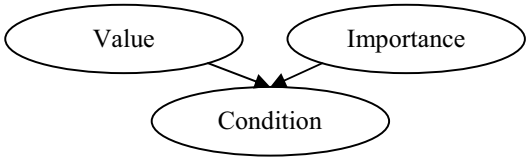

Figure 2. BN structure that captures the value of assets.

C. The Usage Condition of the Network

The traffics to different hosts or servers may differ from each other. The hosts or servers with big traffic may be more risky since they are often important hosts or servers, and intruders may have more contacts and understanding with them. To capture the affect of the usage condition of each host or server, we use the BN structure shown in Figure 3 to model the factor of the usage condition of the network.

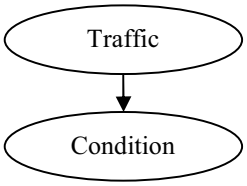

Figure 3. BN structure that captures the usage condition.

D. The Attack History of the Network

If we want to know the security environment of a network, analyzing the attack history of the network is a good choice. The attack history tells us which hosts/servers are more often attacked by intruders and which vulnerabilities are more often exploited. The same scene is likely to repeat itself. The attack history of the network is often recorded by the security audit logs and the audit logs are often in the form of the alarm records. Considering the false positives of alarms, we use the BN structure shown in Figure 4 to model the factor of the attack history of the network.

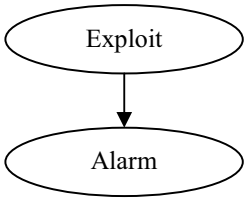

Figure 4. BN structure that captures the attack history.

III. PRELIMINARY RESULTS AND FUTURE WORKS

After integrating the attack graph and the 3 environment factors by Bayesian network, we apply the state-of-the-art Bayesian network probability computing algorithms to compute the attack probabilities of each node. The experiment results show that our method leads to more accurate results due to considering the major environment factors and connecting them using Bayesian network.

Our further works include developing more efficient method for real time security evaluation.

ACKNOWLEDGMENT

This work was partially supported by the National Natural Science Foundation of China (61070186, 61100181).

REFERENCES

[1] S. Jha, O. Sheyner, J. Wing, "Two formal analyses of attack graphs," Proc. of the 15th IEEE Computer Security Foundations Workshop, 2002, Cape Breton, IEEE Computer Society, pp.49-63.

[2] X. Ou, W. Boyer, M. McQueen, "A scalable approach to attack graph generation," Proc. of the 13th ACM Conf. on Computer and Communications Security, 2006, ACM Press, pp. 336-345.

[3] V. Mehta, C. Bartzis, H. Zhu, "Ranking Attack Graphs," Proc of the 9th International Symposium on Recent Advances in Intrusion Detection, Alexandria, 2006, Springer Press, pp.127-144.

[4] Y. Ye, X. Xu, Y. Jia and etc, "An Attack Graph-Based Probabilistic Computing Approach of Network Security," Chinese Journal of Computers, 2010, vol. 33(10), pp.1987-1996.

[5] P. Xie, J. Li, X. Ou, and etc, "Using Bayesian Networks for Cyber Security Analysis," Proc. 40th IEEE/IFIP Int'l Conf. Dependable Systems and Networks, 2010.

[6] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Transactions on Dependable and Secure Computing, 2012, Vol. 9, No. 1, pp.61-74.