Journal of Theoretical and Applied Information Technology
31st January 2013. Vol. 47 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RISK ASSESSMENT MODEL BASED ON MOBILE AGENT

[1]WANG YING, [2]PENG XINGUANG

[1]Lecturer, Colledge of Computer Science and Technology, Taiyuan University of Technology, China

[2] Prof., Colledge of Computer Science and Technology, Taiyuan University of Technology, China

E-mail: [1] ablewy@163.com , [2] sxgrant@126.com

ABSTRACT

With the rapid development of Internet and communication technology, network information security has become the focus of people's attention. Generally speaking, attackers and virus intrude into the target system by utilizing security vulnerabilities. In this paper, combined Mobile Agent theory with risk assessment technology, a kind of risk assessment model based on Mobile Agent has been brought forward. In order to get the target system's vulnerabilities, Mobile Agent is used to scan the system according to user's particular setting of assessment rules. And then the risk grade of target system is given out for providing user particular assessment result and security advice. On the base of model design, an experiment of Mobile Agent risk assessment model is designed. In the process of experiment, the target system is scanned according to facility condition, and the function of Mobile Agent risk assessment model is primarily implemented.

Keywords: *Vulnerability Scan, Risk Assessment, Mobile Agent*

1. INTRODUCTION

With the rapid development of computer and communication technology, computer network has been extended to every corner of the world. Data flow, information flow and capital flow on the Internet has become indispensable part of today's world. On the one hand, people benefit from the Internet that brings opportunities, on the other hand, also fully felt the ordeal of information security. Therefore, scanning and examining security vulnerabilities of target system actively, then analyzing and assessing risk of the target system according to the scan result are very necessary. And this technique has become the focus of network security research.

Risk assessment technique is a kind of active preventive measures which can detect hidden danger of network actively. The system and network are scanned before hackers' attack, security problems are analyzed, and then security vulnerabilities are detected and improved. Therefore, risk assessment is one of the most important technologies and future trend of network security [1]. In this paper, utilizing autonomous running of Mobile Agent, a kind of risk assessment model is established by bringing Mobile Agent technology into risk assessment technique. The security situation of network system can be analyzed combining with existing vulnerability library and results library. Then corresponding modification scheme can be provided to user. Risk assessment model by using Mobile Agent technology has some advantages, including dynamic executing, asynchronous computing, parallel problem solving and intelligent routing. Accordingly, the speed and efficiency of assessment will be improved dramatically.

The rest of the paper is organized as follows. Section 2 and section 3 introduce the network risk assessment technology and mobile agent technology respectively used in risk assessment model based on Mobile Agent. Section 4 details the model. Section 5 implements a experiment system of the model and describes its performance. Finally we draw a conclusion in section 6.

2. NETWORK RISK ASSESSMENT

Due to the openness of computer system and the complexity of protocols, security vulnerabilities are inevitable. The study of security vulnerabilities facilitates repairing discovered vulnerabilities and detecting hidden vulnerabilities. Consequently possibility of being attacked can be reduced. Complete risk assessment model consists of vulnerability scanning and risk assessment. The principle of risk assessment model is as follows. Firstly, vulnerabilities are detected through vulnerability scanning technique. Then, specific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

vulnerabilities detection report is provided. Finally, system risk grade and security advice are given out by risk assessment technology.

2.1 Vulnerability Scanning Technology

System security vulnerability means some form of vulnerability which exists in computer system hardware, software and protocol. The consequence of the vulnerability is that allowing illegal users to access and intrude system without permission.

The key reason why security vulnerabilities can damage system is that invaders using vulnerabilities to achieve their illegal purpose, such as threaten or damage the reliability, usability, confidentiality and controllability of system or information [2]. Each system platform all has vulnerabilities both in hardware and software, for this reason there is no which means no safety system absolutely. New security vulnerabilities created continuously because of operating system and application software updated every day.

Network vulnerability scanning technique is put forward by Dan Farmer and Wietse Venema in 1995. It can imitate attacker's attack, and assess security of system and network from the Angle of providers. Security vulnerabilities and remedy exist in system can be pointed out accurately by network vulnerability scanning technology. The existing vulnerabilities are detected according to the respond of legal and illegal packets.

One of the key technologies of vulnerability scanning is port scanning technique. It is a kind of strategy and methods which can detect open status of target host' port automatically both in local and remote environment [3]. Certain information of target system including opened ports and operation service can be acquired through port scanning. Existing vulnerabilities can be detected according to port scanning results, because unnecessary opened ports are vulnerabilities, and sometimes a lot of vulnerabilities are related with particular ports and services. TCP connect scanning, TCP SYN scanning, TCP FIN scanning, TCP Xmas scanning and UDP scanning are some typical port scanning methods.

2.2 Risk Assessment Technology

Assessment technology is a kind of technology which can analyze data and produce conclusions according to scan and detection. Computer risk assessment is a set of technologies including vulnerability scanning, vulnerability analysis and system assessment. Risks existed in network or systems are analyzed and assessed, then strict examination is implemented, finally vulnerabilities which are harmful to system are detected.

Risk assessment is a very complicated operation which needs good implementation strategies, standards and methods. At present, there are many standards and methods that have been widely recognized in risk assessment field. These assessment methods including: qualitative analysis and quantitative analysis and half-quantitative analysis (combination of qualitative analysis and quantitative analysis method) [4]. OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation [5] produced by Carnegie Mellon university software engineering institute and COBRA (Consultative, Objective and Bi-functional Risk Analysis) [6] developed by C&A system security company are two mature security assessment system.

3. MOBILE AGENT TECHNOLOGY

In the early 1990s, the General Magic Company puts forward the concept of Mobile Agent in the Telescript commercial system. In brief, Mobile Agent is a type of software agent, with the feature of autonomy, social ability, learning, and most importantly, mobility. More specifically, a Mobile Agent is a process that can transport its state from one host to another in heterogeneous network, with its data intact, and be capable of performing appropriately in the new environment. Mobile Agents provide many advantages. First, they reduce network overloading allowing the code to be executed at data location, instead of fetching remote data from code's emplacement. Also, network latency is decreased. Agents can be used to execute locally where the control is required, reducing latency time in real-time applications. Mobile Agents provide an asynchronous and autonomous execution which is ideal to work with in environments with expensive or fragile network links. Heterogeneity is a natural feature inherent in mobile agents. They are hardware and transport layer independent and hence they provide optimal conditions for uniform system integration. Robustness and fault tolerance are two more advantages easily provided by Mobile Agents. Mobile Agent system consists of mobile Agents and Mobile Agent infrastruction [7]. Mobile Agent infrastruction implements transportation of Agents between hosts based on Agent Transfer Protocol ATP, and offer execution environment and service interface for Agents. Agents are executed in infrastruction. They communicate with each other

Journal of Theoretical and Applied Information Technology
31st January 2013. Vol. 47 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

based on Agent Communication Language ACL and get services from infrastruction.

4. RISK ASSESSMENT MODEL BASED ON MOBILE AGENT

The disadvantage of traditional risk assessment model is that scanning module and assessment module cannot move in the net, therefore the velocity and area of assessment are restricted. Meanwhile, the content of vulnerability library cannot update promptly, thus the accuracy of assessment also limited. The appearance of Mobile Agent technology provides a new train of thought to traditional risk assessment system. The traditional scanning mode and assessment pattern has been improved by using Mobile Agent; at the same time, bandwidth dependence has reduced, consequently, the service ability and work efficiency of the system have been enhanced obviously.

4.1 Assessment Model

In the design of risk assessment model based on Mobile Agent, corresponding Agents are invoked according to the demand of customer. Then target system can be scanned by utilizing Mobile Agent, thus scanning results will be analyzed and risk grade will be assessed. Meanwhile, vulnerability library is updated autonomously to provide accurate assessment results and related suggestions to users. This kind of design thought greatly simplifies the design and implement of risk assessment. How the Mobile Agent used in risk assessment model can be categorized as follows:

- Scanning parameters which determined by users are extracted from user interface.
- Related Mobile Agents are invoked according to the analysis of obtained parameters.
- Scanning operation and scanning results analysis are executed by each Mobile Agent; therefore assessment results can be produced.
- The content of vulnerability library is updated by vulnerability library Agent, in order to enhance the accuracy of the models.

The structure of the risk assessment model based on Mobile Agent is shown in Figure1. As can be seen from the figure, the risk assessment model is divided into three layers: vulnerability scanning layer, scanning result processing layer and scanning assessment setting layer.

- Vulnerability scanning layer: the function of this layer is scanning vulnerabilities according to scanning parameters which determined by user. It mainly consists of some vulnerability scanning Mobile Agents. Various scanning Mobile Agents are used according to different scanning modes. Every Mobile Agent can transfer between different servers; and the mobile schedule is formulated by the model.
- Scanning result processing layer: the function of this layer is ascertaining whether there are existing vulnerabilities by matching with vulnerability library according to the results scanned by scanning Agent. According to scanned vulnerabilities, the risk grade can be assessed, and vulnerability and assessment results will be stored into result library.

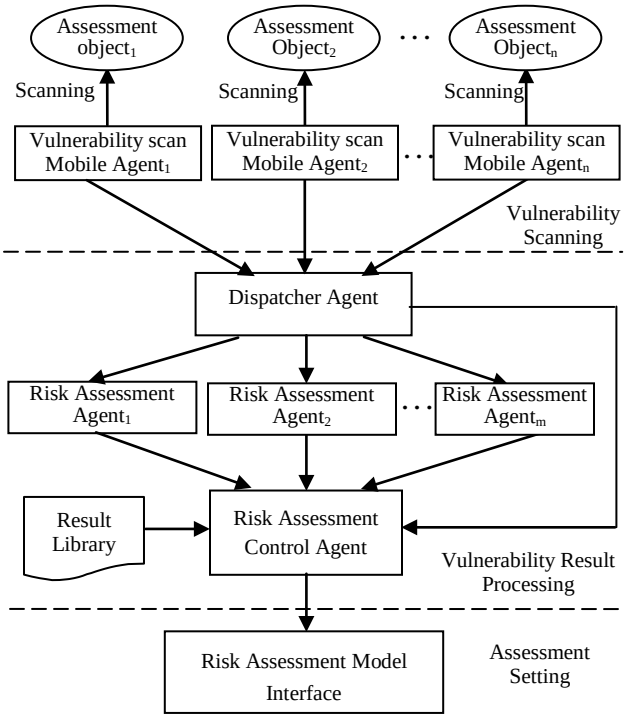

Figure1. Risk Assessment Model Based On Mobile

It mainly makes up of a control Agent, some assessing Agent, a result processing Agent and a vulnerability library Agent.

The control Agent plays the role of unified managing other Agents. Assessment Agent realized risk assessment of target by taking advantage of assessment algorithm on the basis of scanned result. Vulnerability and assessment results are submitted to risk assessment model interface by result processing Agent, and the results will be stored to result library. Vulnerability library Agent can obtain latest vulnerabilities from CVE (Common Vulnerabilities and Exposures) official web site, and store with a certain pattern.

Journal of Theoretical and Applied Information Technology
31st January 2013. Vol. 47 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Assessment setting layer: the function of risk assessment model interface in this layer are both receive assessment setting of user and return assessment result.

4.2 Assessment Algorithm

The core of assessment algorithm is how to illuminate the mechanism and structure of target function, which is establishing proper mathematical model. The risk grade of vulnerabilities is analyzed based on quantitative and qualitative methods. Therefore, the risk grade of entire system can be given out and corresponding security advice is put forward.

Each attack was aimed at one or more vulnerabilities in the system. So the vulnerability grade can be measured with various factors. These factors include sophistication degree, harm degree, risk degree and popularity degree.

In the model, sophistication degree is weighted as 0.2, harm degree is weighted as 0.6, risk degree is weighted as 0.1 and popularity degree is weighted as 0.1. Thus, the risk grade of the vulnerability can be computed by using (1).

Vulnerability risk grade = harm degree* harm weight + sophistication degree* sophistication weight + popularity degree* popularity weight + risk degree* risk weight (1)

And for the risk assessment grade of entire system, it is determined by adopting the bucket principle in the model. The main thought of the bucket principle can be summarize in (2). That is a systematic risk grade is ascertained as the highest risk grade of all vulnerabilities.

$$Q = MAX\ (Q_1, Q_2, Q_3, \ldots, Q_n). \quad (2)$$

Here the Q1、Q2、Q3、….Qn are risk grades of all vulnerabilities.

5. EXPERIMENTAL SYSTEM

Through the analysis of the whole model, the information obtained by vulnerability scanning is the central in the entire risk assessment, and is the key part of our design. According to equipment conditions, an experiment of port scanning on target host has been conducted. A Mobile Agent platform Aglet is adopted in experiment. It is a pure Java development mobile Agent platform of IBM Company.

Firstly, the assessment control module is started when a user sends out an assessment request. Secondly, scanning Agent and assessment Agent which generated in local environment are dispatched to target host executing port scanning and vulnerability scanning. Subsequently vulnerability information is returned to control module. Finally, risk assessment for target system is produced according to vulnerability result. In the system, Aglet Server is responsible for providing MA resides environment, communication mechanism and implement identity authentication of Mobile Agents. Mobile Agents who get authentication have the authority of accessing interface to visit resources. The hosts which provide residence for Mobile Agents are all installed Aglet platform.

In the system of the hosts are all resides MA to install Aglet Server. The latest vulnerability information is stored in local vulnerability library.

The Principle of experimental system is shown in Figure 2.

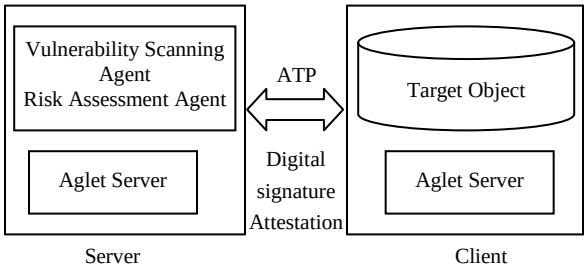

Figure2. The Principle Of Experimental System

The running of Mobile Agent needs the support of Aglet platform. So two PCs installed Aglet platform are used, one is server host named “Richard”, the other is client host named “KFC”, which is the target host of risk assessment.

In the experiment, a kind of routine scan has been conducted on the host named KFC; scanning port range set to 1-20,000. When “scan” button has been pressed down, scanning Agent is created by create () method, and dispatched to target host executed port scanning. The setting interface is shown in Figure 3.

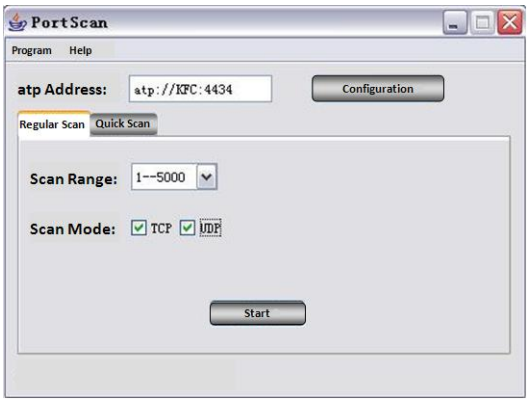

Figure3. The Interface Of Regular Scan Setting

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The scan result showed that the IP address of target host is 219.226.86.144, and some ports, such as 110 and 139 are opened. The scanning operation spent 90 seconds. The detailed description (name, solution, grade) of discovered vulnerabilities are displayed in vulnerability description area. At the same time, risk assessment system grade and Suggestions are given out. The interface of scanning result and assessment are shown in Figure 4 and Figure 5.

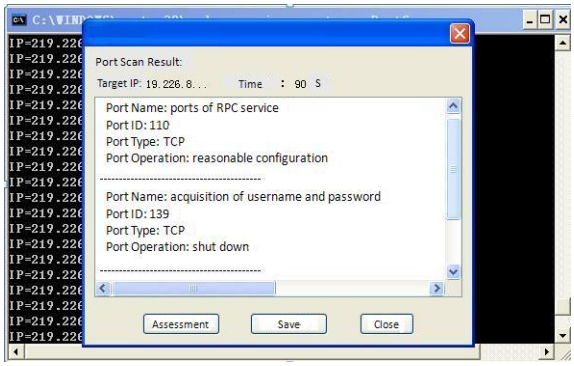

Figure4. The Interface Of Scan Result

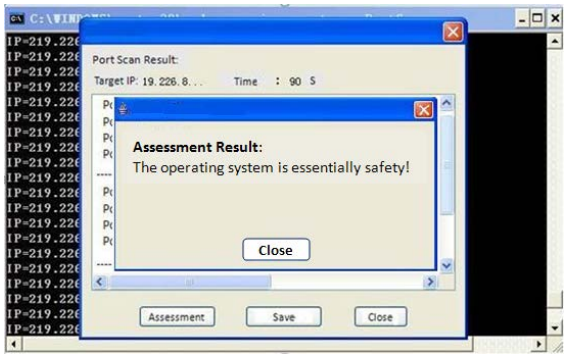

Figure5. The Interface Of Assessment Result

Risk assessment model based on Mobile Agent successfully realized some basic functions of risk assessment. Risk grade of target system has been assessed and improvement advice has been proposed to the user. Through vulnerability scanning and risk assessment of target system, the current safety situation can be obtained. Thus security protection ability of system can be boosted significantly. In addition, the Mobile Agent transferred from local environment to target host without abundant information transitions. Thus network bandwidth can be saved and efficiency of the model can be improved.

6. CONCLUSION

At present, network security has gained widespread attention by all circles of the society. Vulnerability scanning and risk assessment technology occupy an important position in network security field. In this paper, some key technologies and research results are summarized comprehensively; moreover, a kind of risk assessment model based on Mobile Agent is put forward systematically. And on this basis, an experiment of risk assessment has been conducted.

ACKNOWLEDGMENT

This paper is Supported by Shanxi Scholarship Council of China Grant No. 2009-28 and the Natural Science Foundation of Shanxi Province under Grant No. 2009011022-2.

REFERENCES

[1] Newson Alan, "Network threats and vulnerability scanners", Network Security, Dec,2005, pp.13-15.

[2] Panjwani Susmit, Tan Stephanie, Jarrin Keith M, "An experimental evaluation to determine if port scans are precursors to an attack", Proceedings of the International Conference on Dependable Systems and Networks, 2010, pp.602-611.

[3] Ritchey.R.W, Ammann.P, "Using model checking to analyze network vulnerabilities", Proc.IEEE Symposium on Security and Privacy , May 2009, pp.156 –165.

[4] Igor Kotenko, Mihail Stepashkin, "Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle", MMM-ACNS 2005, LNCS 3685, 2008, pp.311-324.

[5] Alberts, Christopher J, Dorofee, Audrey J, "OCTAVESM Method Implementation Guide, v2.0", Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2011.

[6] C&A Systems Security Ltd, COBRA: Introduction to Risk Analysis http://www.ca-systems.zetnet.co.uk/risk.htm

[7] C. Ghezzi and G. Vigna, "Mobile Code Paradigms and Technologies: A Case Study," Proc. the First International Workshop on Mobile Agents, LNCS 1219, Springer-Verlag, 2006, pp. 39-41.