On an Interactive Network Security Measure*

LUO Huiqiong1  WANG Jiahao1  ZHAO Qiang2
(1. School of Computer Science and Engineering, UESTC  Chengdu  610054  China;  
2. Graduate School of Computer Applications, China Academy of Engineering Physics,  Sichuan  Mianyang  621900  China)

Abstract  An interactive network security measure and a description of its function as well as its principle are presented. Based on the existing security loopholes and bugs in operating systems, this measure focuses on the restrictive condition of security and the establishment of configuration files. Under the control and administration of the secure management of configuration files, each system module brings much flexibility, adaptability and high-level security. The security detecting and managing software used in UNIX based on this measure has obtained good results, achieving the goal of automatically detecting and handling inner and outer system-violation and system abuse.

Keywords  network security;  UNIX;  security management;  configuration files

The development of the global information highway has brought great impetus and impact to every domain of the world: science, technology, economy and culture as well. Information security of network as an integrated system engineering needs a long period of tackling key problems and planning in such fields as researching and application. The threats to network security can be classified as: hacking, inside attack, computer virus, leak of secret message and modification of key data in network. All these attacks and invasions aim at wrecking information that is stored in a server by different ways.

In this article we investigate a kind of interactive network security measure — host based information safety precaution. According to this measure and based on existing security loopholes and bugs in operating systems, we investigate possible modes of attacks, intrusion detection system, auto-audit and tracing back technique. And with the help of this measure, we exploit a security-based detecting and managing software used in UNIX.

1 Principle of Interactive Network Security Measure

The principal of interactive security measure is to provide a customized environment to system managers and normal users, so security managers can guarantee the system’s security by controlling this environment through modifying the configuration files. The files configured by security managers in manage interface prescribe restrict conditions, which can be adjusted correspondingly to the requirements of idiographic targets[1]. Any change of the restrictions to system managers and normal users are equal to that of the configuration files. Obviously, it is more difficult to attack a strictly restricted system. The interactive security measure provides great flexibility, adaptability and higher level security. To realize this interactive security measure, we must achieve these functions:

1) First, we should analyze the source of unsecured information which can cause malfunction of host computer. Then, we can control them to resist the wreck of the unsecured information.

2) Subsequently, investigation of security algorithm should be done to help computer recognize the character of those attacks automatically. For example, since analyzing the information traffic’s statistic characteristics in network by self-similarity analysis method can exactly reflect the true operation
traffic’s strict self-similarity, we can set up correct network traffic model and detect those attacks whose characters are different from the model’s description.

3) Based on statistics, we can generate security restrictions by automatically auditing and analyzing the behavior of online users, by automatically analyzing system’s audit logs and system’s loophole’s distribution, by positively detecting systems and monitoring system’s tasks, and by recognizing misbehavior mode through expert system. Undoubtedly, this can be a useful measure to detect and monitor misbehaviors in network.

4) After achieving a normalized security restriction, we can use it to generate our configuration files. Composed of configure information which must be referenced by system when starting, configuration files include controlling information, communication interface, security policy, etc, and can be classified into two groups: one is the system configuration for host computer and monitor. It contains information used by this security system itself, among which, the system configurations of host computer are under surveillance of monitor. The system configuration of monitor can be leaved from monitoring and control. The other group is composed of agents in host computer, and the controlling information and security policies to each module of those agents. They are configured by security manager and saved in database. These kinds of configuration files are firstly extracted out from database by monitor, and then downloaded by host computer. While these configuration files are updated by security manager, the copies of them in host computers are updated too.

2 Application of Interactive Security Measure in UNIX

In UNIX operating system, unsecured information which can cause malfunction to host computer generally comes from two sources: network and client. Thus, four modules are pivotal in the system: login module, password module, network information module and shell module. Here, we modify these four modules to guarantee system’s security\[2,3\].

To reconstruct these four modules, we must set up corresponding security inspection conditions and configuration files based on demands of system’s security. With the cooperation of those four modules and configuration files, we can achieve host based information protection.

1) By reconstructing login module, we can estimate the validity of user’s password and judge whether the user’s accessing to the host is in authorized time. Whether the accessing is successful or not, it is recorded. By reconstructing this module, we can detect the attempts of attacks in time.

2) By reconstructing password module, we can effectively standardize user’s password form, strengthen password’s creating rule and increase the difficulty of decryption.

3) By reconstructing UNIX’s network information module, we increase access control and intrusion detection functions to IP addresses, user IDs, ports and access time.

4) By reconstructing secure shell module, we can provide customized shell to manager and user. Then we can restrict their behavior by configuring correspondingly configuration files, and record their behavior.

These reconstructed modules can initiative exam system configuration. Through automatically auditing and analyzing the behavior of online users, initiative analyzing audit logs and the distribution of system’s loopholes, and through positive system detecting and monitor of system’s audit, we can effectively identify most misbehavior to server\[4\]. On the other hand, the restricted shell can monitor and limit the tasks of system and protect its security. In this software, we have effectively controlled users’ and system managers’ access range and commands through our reconstructed secure shell (SSH). The general structure is as Fig.1 shows. In this figure, translate agent is the connector of the host computer and monitor, and it provides configuration files to shell and network information modules.
3 Conclusions

By taking into account the existing security loopholes and bugs in operating systems, interactive network security measure probes into the potential attacking ways, and defense methods as the detecting method of system class invasion and automatic audition, and aims to achieve a high level of security defense through the dynamic establishment of security controller and management of configuration files. The security detecting based management software used in UNIX is applied in the security management of information network of enterprises. The repeated testing and trial of this measure demonstrates that it can automatically detect and handle inner and outer system-violation and system abuse. And because this measure consumes only a few of system resource while in gear, it can hardly affect the normal users. Through interactive network security measure, we greatly enhance our system’s security and performance.

References

Brief Introduction to Author(s)

LUO Huiqiong (罗惠琼) was born in 1950. She is specializing in computer system architecture and presently working as a Professor in UESTC.

WANG Jiahao (王佳昊) was born in 1978. He is now pursuing M.S degree at UESTC. He is specializing in computer system architecture and computer security.

ZHAO Qiang (赵强) was born in 1958. He is now a superintendent of Graduate School of Computer Application, China Academy of Engineering Physics, specializing in computer security.