Design and Application of a Policy-driven Interactive Security Model

Guo Ronghua*, Zhou Ying, Zhang Yuhan, Bai Yongqiang, Du Jiawei
Luoyang Electronic Equipment Test Center of China (LEETC)
Luoyang, China
*e-mail: guorh05@gmail.com

***Abstract*—It is difficult to build a perfect security system due to passive protection methods or isolative security devices. Principles of several interactive models are analyzed at first. And then a policy-driven interactive security model, which implements an integrated security system between many devices by the interactive policy, is proposed. At last, some application patterns of the model are discussed in a typical network.**

Keywords- policy-driven; interaction; security model; information security

I. INTRODUCTION

With the rapid development of internet and the network society coming, networks are ubiquitous to deeply impact every way of politics, economy, culture, military and society. The progress of internet makes for realizing more efficient shares in source and information, but brings many new challenges to information security as well. To assure the security of a network, security technologies and products covering all ways of information security are developed continuously. Traditional security technologies and products are merely to protect a network to some extent as a result of passive protection and isolative operation. Facing various network attack behaviors, it is impossible to satisfy the security requirements only depending on a single technology or a single security protection method (such as a firewall) [1, 2]. Therefore, the combination of all security technologies and the interaction between security devices are needed to better dynamicly detect changing features of network security events, and efficiently supply the security protection ability of an information system. More and more internal and international researchers are centralized to investigate the interaction between some security protection devices or between some security device and a network device, such as the interaction between an IDS (intrusion detection system) and a firewall [3-5], an IDS and a router [6], an IDS and a Honeypot [7].

An interactive security model based on policy-driven method, which implements an integrated security system between many devices by the interactive policy, is design to efficiently integrate the security resources in the network. The model will bring a composition of forces "1+l>2" by cooperative operations to avoid the "Cannikin Law". Some application patterns of the model are discussed in a typical network in the end.

II. SEVERAL TYPICAL INTERACTION MODELS

A. IDS-centered interactions

(1) The interaction between an IDS and a firewall

There are two kinds of interactions, that is, direct and indirect interaction, between an IDS and a firewall according to the way of information interaction. Direct interaction is implemented by unifying development interfaces and transmitting security incidents according to a fixed protocol; communications are achieved in the indirect interaction by the interactive consoles (the third software). Whether it is a direct or indirect indirection, the basic principles of interaction between an IDS and a firewall: Interactive mechanisms take effect to notify automatically the firewall in the built security system when it is necessary to block (defined rules) detected attacks. And then, correlative rules of the firewall, such as adding access control rules, are modified dynamicly to block the attack source. In a word, the objective to control the whole security system is achieved by interactions between the two.

(2) Interaction between an IDS and a router

The interaction between an IDS and a router mainly bases on the new network middleware technology (Universal Plug and Play, UPnP) developed by Microsoft. Due to the devices supporting UPnP technology can connect automatically to each other through a network, and without relying on any specific device drivers, the UPnP protocol may be used as an interactive language to implement the interaction based on standard protocols between an IDS and a router. Concrete realization of the technology is to embed UPnP control units in IDSs and implement UPnP protocols in routers. According to the network status, routers trigger the control unit in real time to accomplish corresponding controls and managements of a network after that the network is detected by an IDS. And then routers decide to forbid or allow specific network connections.

(3) Interaction between an IDS and a vulnerability scanner

The pattern matching-based intrusion detection method is applied in most IDSs at present. Due to new vulnerabilities found constantly, the event library needs to update in time to reduce system underreports. But, the event library becomes more and more larger with updating continuously, and more time is consumed to travel once all events in the library. It is inevitable to decline the detection efficiency of an IDS. The interaction between an IDS and a vulnerability scanner (VS) is proposed to address the above-mentioned problems.

Published by Atlantis Press, Paris, France.

The basic interactive principle: Firstly, periodic vulnerability scanning is required for a system by the interaction between the two; secondly, security vulnerabilities in the system will be patched up in time according to scan results; thirdly, scan results should be transmitted to the IDS; lastly, to reduce the scale of the event library and shorten the event-matching time, attack features of the patched vulnerabilities in the event library will be deleted by the IDS. The system may update the vulnerability database and retrieval the event library at the same time. The attack features of newly discovered security vulnerabilities will be added dynamicly up to the event library. Thus the event library may be updated automaticly in real time, and the purpose to improve the detection efficiency of IDS is achieved.

B. Interaction among a firewall, a switch and a network anti-virus system

A network anti-virus system (NAVS) is composed of four interrelated subsystems including a system center, servers, clients and a monitoring console, which work together to protect the whole network from viruses. The control center can be deployed hierarchically. The default strategy will take effect when a virus is detected by a client, and the message will be reported simultaneously to the system center.

The basic principle of interaction: The event of infecting viruses will be reported to the system center in time when viruses are detected by a client. The system center communicates with a firewall or a switch through an agent or a security operation center (a system to centrally manage network security resources), and requires to block the possible infecting channel of viruses by using their functions of disconnecting networks.

C. Interaction between a LPS and a CA

It is very important for a LPS (Leakage Protection System) to assure an inner-network security. Integrating cryptography technology, operating system core technology with network drive technology, a logical inner-network security field, which implements access control, data protection and log record for storing and transmitting all hosts' important information, is constructed to avoid efficiently illegal leaking and destroying the important information from the inner-network by all possible ways. As a creditable authority organization, a CA (Certificate Authority) awards the digital certificate to authenticate its identification. The digital certificate, as a creditable certificate to exchange messages with each other, authenticates the validity of an agent (such as a person or a server) in a creditable field. With unique, credible, reliable and secure features, the digital certificate supplies an efficient solution for the network information security. Some services, such as confidentiality, non-repudiation and access control, can be obtained for network applications by using the digital certificate.

The basic interactive principle between the two: All asserts in the network security field, which are monitored and controlled by a LPS, are awarded digital certificates by a CA. And then the relationship between a digital certification and its corresponding user is built. Those managements in the network security field, such as device security, terminal assets, illegal access, user identity, and comprehensive security audit, can be achieved by the interaction between the two.

III. A POLICY-DRIVEN INTERACTIVE SECURITY MODEL

A policy is a description of action plan and process summarization, which could be a principle of action. And a security policy is a guideline of working to ensure network secure, which is driven by security requirements. It describes the requirements of system's security action. We implement security policy to achieve that actions could be taken effectively to limit the losses when the system is attacked. A policy-driven security frame is built in this paper, which combines an antivirus system, an IDS, a vulnerability scanner, a firewall and network switch devices. Fig.1 illustrates a policy-driven interactive security model of basic system.

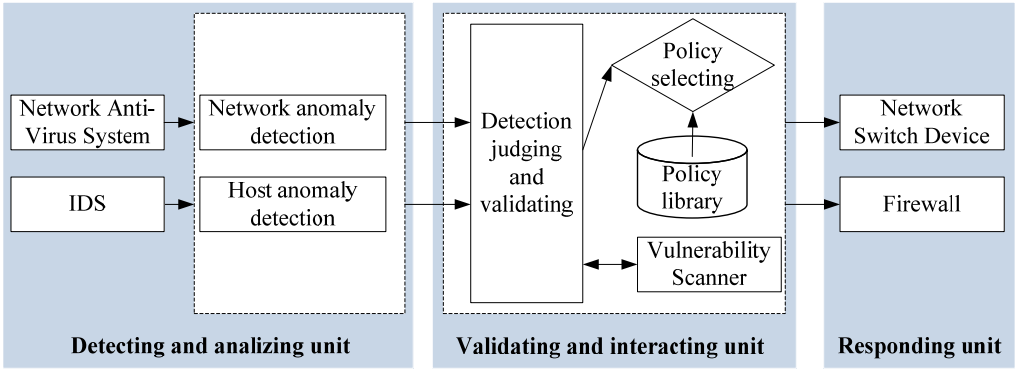

Figure 1. A policy-driven interactive security model

This model consists of three parts as follows: (1) Detection and Analysis Unit accomplishes anomaly detection of network connect ports and workstation hosts. Then indicators about the criticality and lethality of the abnormal event are submitted after analysis. These two indicators reflect the flux and position of abnormal event's data. The

Published by Atlantis Press, Paris, France.

analysis results are handed to the Detection, Invalidation and Interactive-policy Unit as inputs. (2) Detection, Invalidation and Interactive-policy Unit is the core of this system model. A judgment about the abnormal events is firstly given on the basis of input data. Then interactive policies are chosen from policy library according to the judgment, and improve the detection accuracy by vulnerability scanner. (3) The Response Unit deals with the abnormal events following the interactive policy given by Detection, Invalidation and Interactive-policy Unit.

IV. THE APPLICATION OF THE INTERACTIVE SECURITY MODEL

As depicted in Fig.2, the inner net and outer net are segregated by a firewall in a typical network topology. All the security protection servers are located in security server district, including anti-virus center (NAVS), vulnerability scanner (VS), leakage protection system (LPS) and Certificate Authority (CA). The IDS and inspection engine connect to the switch bypass. Terminal (or server) T1, T2 …, Tn build up a LAN--Group 1.

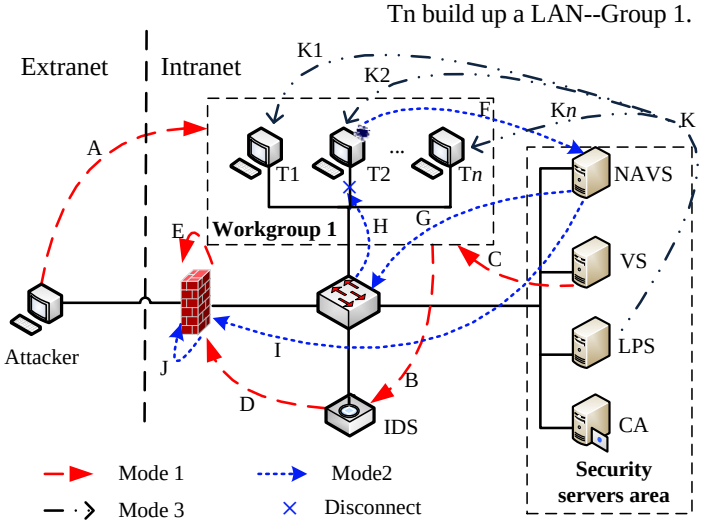

Figure 2. An application of the model in a typical network

The security protection system, which is built up by IDS, VS, NAVS, LPS, CA and firewall etc., has three interactive application modes:

Mode 1: As depicted by red in Fig.2, the interactive response is realized by IDS, firewall and VS. The process of intrusion detection, validation, and response is as follows: A--Attack; B--Detect intrusion; C--Validate the attack; D--Attack confirmed, and the security protection system interactively responds; E--Add new rules to block the intrusion. A specific port or service can be forbidden by the firewall according to the security requirements to accomplish intrusion interruption.

Mode 2: As depicted by blue in Fig.2, the interactive response is realized by firewall, switch and anti-virus software. There are two different kinds of responses to different protection targets: Response 1: F--Detect virus; G--Virus confirmed, and the security protection system interactively responds (NAVS and switch); H--Disconnect the network and stop the virus infection. When a certain port (T2 for example) in group 1 is infected, the detection report would be submitted to NAVS immediately. The infected network will be segregated (disconnect T2 and the switch) at once through NAVS and switch interactive response. Then the virus inflection could be effectively interrupted. Response 2: F--Detect virus; I--Virus confirmed, and the security protection system interactively responds (NAVS and switch); J--Add new rules, and disconnect the intranet to the extranet. Rebuild the connection after the virus is cleaned up.

Mode 3: As depicted by black in Fig.2, the interactive response is realized by LPS and CA. A USB Key is created by CA, and managed by LPS server. There are associations between USB Key and intranet terminals (IP or MAC). So it must be authorized by USB Key when the terminal is logged in.

V. CONCLUSION

An interactive security model based on policy-driven is proposed after discussing several traditional security technologies in this paper. This model, which could defend against intrusion and virus infection, implements an integrated dynamic security system by the interactive policy. It is demonstrated that implementing security interaction in a typical network could be realized not only by security protection devices or proxy, but also by a security management platform, which carry out the security policies and manage the security resources.

REFERENCES

[1] Yin Shuming, “Research and design of security defense architecture based on firewall and intrusion detection,” Changsha: Central South University, Master thesis, 2005.

[2] Wang Wenqi, “Research on intrusion detection and coordinated-control of security protection,” Xi’an: Northwestern Polytechnical University, Ph.D thesis, 2006.

[3] Huseyin Cavusoglu, Srinivasan Raghunathan, Hasan Cavusoglu, “Configuration of and interaction between information security

technologies: the case of firewalls and intrusion detection systems," Information systems research, 20(2), 2009, pp.198-217

[4] Baoyi Wang, Haipeng Yang, Shaomin Zhang, "Research on application of interaction firewall with IDS in distrbution automation system," Advances in electronic engineering, communication and management Vol.1, Lecture notes in electrical engineering, Vol.139, 2012, pp.527-532

[5] Jiang Ji, "IDS and firewall interaction mechanisms and security protocols," Kunming: Kunming University of Science and Technology, Master thesis, 2006.

[6] Wang Baoping, Zhang Zhe, Zhang Xingang, "Research of IDS and router coupling based on UPnP and Iptables," Journal of Henan University (Natural Science), 39(4) , 2009, pp.424-427.

[7] Dang Rui, "Research of interaction between intrusion detection and honeypot," Xi'an: Northwestern Polytechnical University, Master thesis, 2004.

Published by Atlantis Press, Paris, France.