Design and Application of a Network Security Model

Xu Shiping*, Zhang Yuhan, Zhou Ying, Bai Yongqiang, Fu Haipeng
Luoyang Electronic Equipment Test Center of China (LEETC)
Luoyang, China
*e-mail: xsp19821115@126.com

***Abstract*—This paper analyzes the deficiency of P2DR security model, and proposes a kind of new active dynamic security model AD-RPPDRRM, in which risk analysis, management and recovery are imported. On the basis of this model, basic technologies used to implement the defense in depth system are discussed. At last, a defense in-depth system of a typical network is given.**

Keyword - security model; P2DR; defense in depth

I. Introduction

With the development of network and information technology, security affairs, such as cockhorse, worm, DDoS attack, corpse network and network intrusion, occur more and more frequently, complexity and automatism of attack instruments are improved continuously. All of these make the traditional passive static security defense methods face an austere challenge. The traditional passive static security defense technologies could not resolve numerous security threats[1].

In order to resolve the potential security threats, some relatively independent security technologies which focus on the different security problems have been invented, such as firewall, IDS, network virus protection system. However, because the information system and network environment change dynamically, it is difficult to ensure the network work well just using only one security technology. Therefore, for the sake of utilizing the security technologies synthetically, it is necessary to build a holistic security defense system which makes the network have active defense ability. The research of security model and security technology, that had active defense ability, have become of the hotspot of network security domain[2]. This paper proposes AD-RPPDRRM model (Active Dynamic – Risk analysis, Policy, Protection, Detection, Response, Recovery, Management) on the basis of P2DR, and discusses the network defense in depth system according to this model.

II. P2DR Model

The P2DR model has been proposed by ISS in 1990s[3]. Fig.1 illustrates the P2DR model, which has four parts. A security cycle, managed by policy, is constituted by protection, detection, response. The model provides basic defense principles for target system. The basic ideas: The target system is protected by the various security protection methods which are controlled by the security policy, the detection tools are used to detect the state of the target system， and appropriate response is used to recover the target system to “lowest risk” or “safest” state. This model has become the typical security framework in the information security domain.

In this model, detection is the only dynamic factor, and protection is the only measure to resolve the security affairs. Whether the model can play a role, it depends on the correct setting of system and consummate defense measure. It ignores the dynamic character of network security, and focuses on the fixed threats and environmental vulnerability in the great degree. The development of network is dynamic, many new vulnerabilities, viruses, attack programs appear going with issuance of new protocols, operating systems, internet applications. Therefore, the network security model must be dynamic, new security problem needs new security technology.

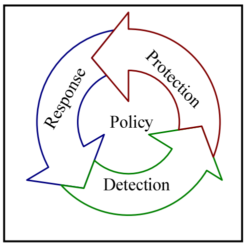

Figure 1. P2DR model

III. An Active Dynamic defense system model

In order to find the new vulnerabilities of the network server and device, and constantly find out the security risks and threats in the network, the network must be dynamic and adaptable. That means the defense system should have some functions, such as protection, real-time intrusion detection, vulnerability scanning, system security decision, and risk analysis.

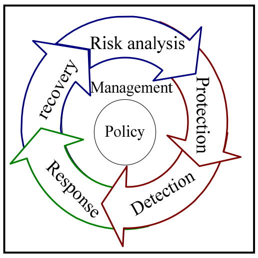

Figure 2. AD-PPDRRM model

This paper proposes a new security model according to security = risk analysis + policy execution + vulnerability

Published by Atlantis Press, Paris, France.

detection + real-time response + recovery. Fig.2 illustrates the AD-RPPDRRM model, which has three layers: technology, management, policy. Security defense technologies are the foundation of this model. Security management is the support of this model. Security policies are the core of this model. Technology layer has five parts: risk analysis, protection, detection, response, recovery. Any part interacts on each other, implementing dynamic feedback.

(1) Risk analysis

Risk analysis is a process that analyzes the possibility of threat occurring and the frangibility of system, and estimates the loss caused by the two factors above. Risk analysis includes risk validation, risk prediction, risk estimation. Risk validation is used to detect the possible risks in the network system and classify them. Risk prediction is used to predict the direct loss and indirect loss while the risk happens. In order to confirm which risk should be dealt with first, risk estimation is used to estimate influence which is caused by the risk for the network system.

(2) Policy

Security policy is the core of this model. Policy is the layout of an action and the description of a process. It controls the life-cycle of an affair. Security policy is the restrictive rules driven by the security requirements, which describe the demands of security behavior that the security system must obey. The aim of security policy is to prevent attacks, and make the loss be lowest by using security measures after the attacks happen. It is necessary to confirm the aim of network security according to the risk analysis results while designing the security policy. In the security program implementation phase, the protection, detection, response, recovery, management of the system should base on the security policy.

The application principles of security policy are as follow.

a) Protection is the basic condition, which includes the static protection measures. It must be implemented in the security defense system.

b) Detection is the extend condition, which provides dynamic detection measures. It must be extended to implement in the security defense system.

c) Response is the expectation result of security controlling and intrusion alleviatting, which reflects the security control degree. It must give priority to implement in the security defense system.

Fig.3 illustrates the basic types of security policy.

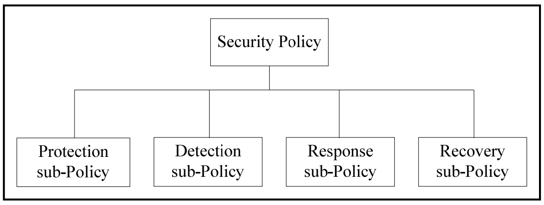

Figure 3. Basic types of security policy

Protection sub-Policy: In allusion to the special security vulnerability, protection sub-policy indicates how to repair the vulnerability and which network layer the vulnerability will affect. Hereby, relevant security product could be confirmed to improve the security level of the target system.

Detection sub-Policy: The aim of Detection sub-policy is to detect the network attacks accurately and efficiently. Therefore, detection sub-policy should definitely give the recognition methods for network attack. Network attack has its own attack mode, it is always associated with some security vulnerabilities.

Response sub-Policy: The aim of Response sub-policy is to give the response measures for intrusion affairs. It includes static response policy and dynamic response policy. Static response policy gives the same response measure for the intrusion affairs that belong to the same type. Dynamic response policy selects the corresponding level response measures according to the threat assessment value of intrusion information.

Recovery sub-Policy: The aim of Recovery sub-policy is to give the recovery measures according to the degree and the position that the target system has been attacked, that make the target system recover to acceptability state as quickly as possible.

(3) Protection

The aim of security protection is to adopt any possible measures to protect the confidentiality, integrality, usability, non-repudiation of the target system. Generally, security protection is implemented by traditional static security technology and method, such as firewall, encryption, authentication.

(4) Response

It is important to give response in time after detecting the security vulnerability, which adjusts the target system to the security state. In order to make the target system provide service naturally, it is necessary to dispose the affair, behavior, process, etc. which would endanger the target system security. Real time response ability would be formed by building the response mechanism. In a sense, the essence of security is exception handling and emergency response.

(5) Recovery

The aim of recovery is to recover the target system from the fault or paralysis state caused by attacks to normal operation state. For example, when the target system has been destroyed, backup system is usually used to recover the data and information of the target system.

(6) Management

The function of security management is to collect, filtrate, gather the security affairs. According to the result of correlation analysis about the security affairs, the global security affairs are obtained, and then the uniform security policy is constituted to handle the security affairs which have been detected.

The basic idea of AD-RPPDRRM model: First of all, according to the dynamic characters of network security, the corresponding security policy is constituted on the basis of risk analysis, risk prediction, risk evaluation, etc. The detection technologies, such as IDS, vulnerability scanning, are used to detect the potential security problem. When the exceptions of target system have happened, security protection measures should respond as quickly as possible according to the security policy, and the recovery measures are used to recover the target system to the acceptability state.

IV. A DEFENSE IN DEPTH SYSTEM BASED ON AD-RPPDRRM MODEL

Defense in Depth is a new idea in the security domain during recent years. It was first proposed in "IATF", and applied to guide the construction of GIG[4]. The basic idea of Defense in Depth is that: building a security system which integrates multi protection measures could efficiently defend the attacks which could break into one certain kind of protection[5]. Therefore, a defense in depth system is a heterogeneous network system built up by distributed sub-system, which adopts centralized management and surveillance, performs interactive protection response. Based on the integration of information assurance and data security techniques, it offers complete solutions about vulnerability defense, attack disposing, and damage recovery. That will improve the system protection effectively.

It is significant for network security to introduce Defense in Depth into security system design. The heterogeneity of defense must be considered sufficiently when building a defense in depth system. That means different defense policies should be deployed between different subnets and defenders to compel the attackers to break through multi defense lines. Build a defense in depth system according to defense closed loop: defense → detection → response → recovery, which is proposed by the AD-RPPDRRM model. Firstly, divide the defense in depth system to two parts: defense breadth and defense depth. Secondly, divide the defenders into three kinds in breadth: host/terminator, LAN and WAN, and deploy different defend policies individually. Thirdly, take different protection measures for different levels in defense depth: application security, network security, data security and host security. The defense measures are described in detail separately in Table.1 and Table.2.

TABLE I. DEFENSE MEASURES IN BREADTH

Defenders	Measure details
Host/terminator	Antivirus, information assurance vulnerability alarm, security system based on host, public acess key/private key machanism, data encryption
LAN	Firewall, 、 mail antivirus 、 IP block list, information assurance vulnerability alarm, vulnerability recovery, LAN security inspection
WAN	Firewall, site keep scanning 、 alarm filtration, system patch, IDS, mail antivirus, information assurance vulnerability alarm, virus scan online, LAN security inspection, system log, Honeypot/Honeynet, technology analysis tool

TABLE II. DEFENSE MEASURES IN DEPTH

level	Measure details
Application security	Application access control, application security inspection
Network security	Firewall, selective gateway, net antivirus, IDS, connection control, network security inspection
Data security	Data encryption 、 data destruct 、 data recovery、database access control, data security inspection, data backup
Host security	Host surveillance, vulnerability scan, safety authority, patch management, host reinforcement, host antivirus, terminator security inspection

V. APPLICATION EXAMPLE

A typical network topology is illustrated as Fig.4. A defense in depth system for inner network is set up by integrating firewall, IDS, vulnerability scanner, honeypot, network evidence system. The first defense line is realized by the honeypot located on the border router. The second one is a firewall, which could block the intrusion and attack from outer net, and hide the inner net's structure, operation, and information efficiently. The third one is an IDS, which offers real-time security service by raising alarm when detecting an attack, intrusion or missing operation. It could find the potential threat and risk, protect the system before actively. The fourth one is vulnerability scanner, which makes periodic scan of the inner net and update the system. That would decrease the possibility of being attacked relatively. Host Firewall, antivirus software and IDS are deployed on the inner network hosts to reinforce the protection. Meanwhile, the network forensics system, which is built on border router, honeypot, IDS and firewall, could record the criminal evidence by abnormal events capture, log and analysis. That will provide direct support for the counterattack.

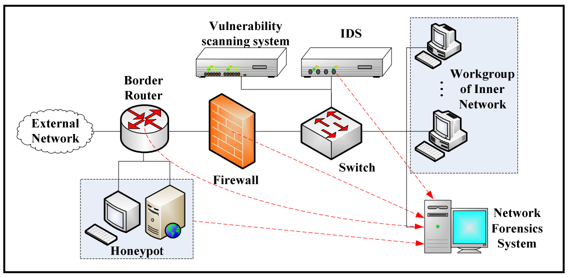

Figure 4. A typical example of defense in depth

VI. CONCLUSION

On the basis of analyzing the classical P2DR security model, importing risk analysis, management and recovery, a kind of new active dynamic security model AD-RPPDRRM is proposed in this paper. Then basic technologies used to implement the defense in depth system are discussed based on the model. With the development of network, the security system must be adapted to suit new attacks and security techniques. How to use multi security measures in one security model frame and play their own advantages efficiently would be researched during the further work.

REFERENCES

[1] Yu W, Chellappan S, Wang X, et al. “Peer-to-peer system-based active worm attacks: Modeling”. Analysis and Defense, Computer Communications (Elsvier), 31, 2008, pp.4005-4017.

[2] Wei Jiang. “Research on active defense based on attack-defense game model”. Harbin: Harbin Institute of Technology. Doctor thesis, 2010.

[3] 《ISO/IEC 15408 Information technology-Security techniques - Evaluation criteria for IT Security》.

[4] Xiaoping Wu, Zemao Chen, et al. “The theory and defense of Information countermeasures”. Wuhan: Wuhan university press, 2008.

[5] Renquan Huang, Weiming Li, et al. “Research on the defense in depth system of air defense information network”. Computer Science, 38(10A), 2011, pp.53-58.

Published by Atlantis Press, Paris, France.