Research on Active Controllable Defense Model Based on Zero-PDR Model

Kehe Wu
Department of Computer Science and Technology
North China Electric Power University
Beijing, China
epuwkh@126.com

Tong Zhang, Fei Chen
Department of Computer Science and Technology
North China Electric Power University
Beijing, China
zhtzhangtong@163.com, chenfei0428@126.com

***Abstract*—In the face of more and more complex and unpredictable network security threats, although an increasing number of security products have been deployed in personal computers, application servers and networks, we are still in a passive embarrassment. How to detect and response to network security threats immediately before threats occur or reach the target system is a key issue to solve current security threats. Based on further study of classical PDR protection model and analysis of current network security threats, idea of solving network information security problems is changed from passive protection to the active controllable defense, and Zero-PDR model based on Trojan attack characteristic is proposed. Active Controllable Defense model based on Zero-PDR model is further proposed, which can avoid Trojan attack and the first time attack effectively.**

Keywords- Network Information Security; PDR Model; Zero-PDR Model; Active Controllable Defense

I. INTRODUCTION

With the rapid development of Internet, the human society has been in an information age. The security problem of network has appeared while network provides service to human. At the same time, from network experts to ordinary network users all come to realize that network security problems are serious and the key issue which can become an obstacle to network development and even an important issue[4] to endanger country security. Network information security has become the fifth-largest security field after sea, land, air and space.

From the day of network birth on, the game between application and security has not stopped for a moment. In the information security field, researchers and practitioners have done a great deal of effort to protect information security. From the BLP [10] (Bell and LaPadula) model and Biba [11] model to the Trusted Computer System Evaluation Criteria (TCSEC) proposed by the U.S. Department of Defense, then to the proposal of PDR dynamic protection model as well as other security model, standards and technology, researchers and practitioners has been working towards building a secure network environment.

However, in recent years, network security problems have become more and more serious. Viruses and worms[1] keep our PC from running normally and effectively, backdoors and Trojans keep enterprise confidential information in a leaked risk, DoS/DDoS attacks and hackers' malicious destruction keep enterprise network in the edge of paralysis, not to mention other problems which is caused by applications and improper management. As a result, such as firewall, intrusion detection, intrusion prevention, anti-virus software and so on, more and more security products have been deployed in our network. But the update of vulnerability database, virus signature database and intrusion signature database will always lag behind the event of vulnerabilities, viruses and intrusions. Facing a variety of security threats, the protection lags behind the destruction, and the network is always passive, which makes security practitioners face new challenges. Facing new network security problems, where is our way? Based on analysis of new network security problems and the further study of the PDR protection model, Zero-PDR model is proposed according to the characteristics of Trojan attacks. On the basis of research on Zero-PDR model, idea of solving network information security problems is changed from passive protection to the active controllable defense, and active controllable defense model based on Zero-PDR model is proposed, which can prevent Trojan attacks and the first time attack effectively.

II. ZERO-PDR MODE

A. PDR Model Outline

In December 1995, the U.S. Department of Defense proposed a dynamic model of information security, which is a Protection - Detection - Response multi-link security system, named PDR model [2], as shown in Figure 1.

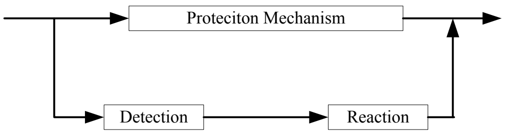

Figure 1. PDR Model

PDR model is a dynamic network security theory model based on closed-loop control, which associated time with security measure for the first time. Winn Schwartau, the proponent of PDR model, said: "For any one thing, if you can not measure it, you can not manage it." Before PDR model, security models and theory, such as TCSEC standards, BLP

978-0-7695-4020-7/10 $26.00 © 2010 IEEE
DOI 10.1109/IITSI.2010.140

model and so on, hadn't given a security measure standard, so it was hard for the practitioners to work out actual solutions. Instead, PDR model added the element of time to security. On one hand, time is quantified and can be calculated; on the other hand, security is no sense without time because attack, protection, detection and response all cost time. Therefore, the proposal of PDR model has offered a method to measure a system's safety and security capabilities, having the epochal significance in the information security and protection field.

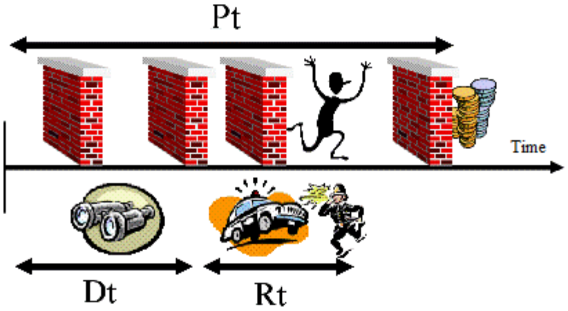

Figure 2. Schematic Diagram of PDR

In Figure 2, Pt means system's total protection time or the time which attackers spend on attacking safe target. Dt means detection time. Rt means response time after system's security protection being attacked. When Pt> Dt + Rt, that is, when protection time is bigger than the sum of detection time and response time, we think protection is effective; instead, when Pt <Dt + Rt, we think the system is unsafe, that is, there is an exposure time Et = Dt + Rt - Pt in system. Et is an important basis for measuring system risk, and determines the balance between system security and costs. Another extreme situation is when Pt = 0, that is, system has no protective measures, and at this time Dt + Rt = Et. In this case, only detection and response mechanisms can ensure system's security, so the more complete detection and response mechanisms is and the faster reaction is, the less time given to intruder is and the smaller losses suffered by system are.

B. Think of PDR Model

Based on the study of PDR model and the analysis of current network environment, the following three points of thought of PDR model are proposed:

1) **Can attack time be considered to be equivalent to protection time in any case?** In PDR model, Pt means system's total protection time or the time which attackers spend on attacking safe target, that is, attack time is considered to be equivalent to protection time. In new network security issues, can attack time equal to protection time exactly?

2) **Protections based on PDR model can not avoid the first time attack, but do all systems allow the first time attack to happen?** PDR model is a closed-loop risk controlling mechanism as shown in Figure 1, using feedback controlling mechanisms after attacks. That is, after attacks occurring, the protection system should detect attacks after Dt time, and then can adjust system to the safe state again by response after Rt time. Obviously, this is a passive way of protection. Intrusion detection systems, vulnerability scanning systems, disaster recovery systems and other means are all the passive protective measures. In passive protection, protections lag behind destructions, for example, update of vulnerability database, virus signatures database and intrusion signature database always lags behind the event of holes, viruses and invasions; as a result, the first time attack can not be avoided. Do all systems can allow the first time attack to happen?

3) **In PDR model, can Dt and Rt equal to zero?** In PDR model, the case when Pt = 0 is discussed, that is, Et = Dt + Rt, Et means the system's exposure time. The smaller Et is, the more complete system's detection and response mechanism is, and the smaller losses suffered by system are. Then, what do Dt = 0 and Rt = 0 represent? When Dt = 0 and Rt = 0, what is the system's protection strategy?

C. Zero-PDR Model

Based on the analysis of a variety of existing security issues in network environment, the following conclusion for the first point of the above three points is made:

"Zero-break Time" makes attack time different from protection time. "Zero-break Time" means that the time which starts from the system being attacked and ends with the breakthrough is equivalent to zero. For example, attackers do not attempt to obtain information by cracking password, but by intercepting information before messages being encrypted or after messages being decrypted, in this case, the break time becomes zero; In addition, Trojan attack is one of the most typical "Zero-break Time" examples. Trojans [8] fake or bind with credible program. After they enter into system, Trojans don't act immediately, instead, they hides them and attack system quietly at the appropriate time. Therefore, Trojans don't need any time to break system, that is, the break time equals to zero. "Zero-break Time" can be seen as a thief who can enter without picking locks. In the "Zero-break Time" situation, system's protection time doesn't equal to zero but attack time equals to zero, making attack time different from protection time.

Based on the analysis of "Zero-break Time", Zero-PDR model is proposed according to Trojan attack.

1) Model Description

- Pt: Protection Time. It means system's total protection time.
- At: Attack Time. It means the time used by attackers when they break systems.
- Dt: Detection Time. It means the time used by detecting attacks.
- Rt: Response Time. It means the time used by responding after systems being broken.
- Et: Exposure Time. It means the time which start from the attack occurring and ends with systems recovering to normal status. Different systems have different requirements for Et.

2) Model Constraints

a) When At=0, Pt≠At:

- *Dt+Rt≤Et.* It means that the time which start from the attack occurring and ends with systems recovering to normal status is within an allowed time range. In another word, if systems can recover to a normal state within Et time, the protection mechanism is useful.
- *Dt-Rt=0.* That is responding immediately when detecting attacks.

If the protection mechanism meets the above two conditions, the protection mechanism is effective.

b) When At≠0，Pt=At:

- *Pt ＞ Dt+Rt,* then the protection mechanism is considered to be effective.

III. Active Controllable Defense Model Based on Zero-PDR Model

The Active Controllable Defense model based on Zero-PDR model is proposed according to more and more intelligent network threat such as Trojans in more and more complex network environment. Based on the analysis of current network environment's characteristics, the following two conclusions for the last two points of the above three points are made:

Some systems can not allow the first time attack happening. For example, Electric Power Dispatching Automation System, is a core system which can affect production and operation in electric power enterprise. Once Electric Power Dispatching Automation System is attacked, it will bring incalculable damage to the national economy. Therefore, the Electric Power Dispatching Automation System does not allowed the first time attack happening. Thus, the traditional passive protection can not meet the security protection needs of Electric Power Dispatching Automation System.

Dt and Rt can equal to zero. When the attack time equals to zero and systems don't allow the first time attack, the passive protection can not ensure the system safe. Only the way on which the idea is changed from passive protection to active controllable defense can ensure system safe effective. In the following discussion of Active Controllable Defense model, Dt and Rt can be allowed to equal zero.

Nowadays, network attacks become more and more automatic and intelligent, and means of attack become more and more diverse [5,6]. In this serious situation, according to the requirements of not allowing the first time attack in some enterprise, the traditional passive protection methods can not be able to cope with current network security problems. Only to change our train of thoughts from passive protection to active controllable defense [9] can we ensure the target system safe in new environment.

Active Controllable Defense means that defense mechanism can detect and respond to attacks in time before network security threats happen or reach the target system, or defense mechanism can control attacks in a certain area and eliminate attacks within given time.

A. Model Description

Based on the study of Zero-PDR model and the description of the Active Controllable Defense concept, the Active Controllable Defense model based on Zero-PDR model is proposed.

When At = 0:

- *Dt = 0, Rt = 0; or (Dt – Rt) = 0* (1)
- *Dt+Rt≤Et* (2)

The concept of Active Controllable Defense contains two meanings:

1) Active Controllable Defense model can detect and respond to attacks in time before network security threats happen or reach the the target system. Facing to threats such as Trojan which have the "Zero-break Time" characteristics, in order to achieve timely detection and response, rules (1) in the model has given the behavior-based defense solution. In the paper name " The Design and Implementation of Security Defense Technology Based on Mandatory Running Control " [3], a specific behavior-based defense solution has been given. Firstly, in the "safe initial state", the "Credible Processes List" has been formed. All processes which are allowed to run by the target system are registed in the " Credible Processes List". Then the target system can detect the processes which intent to run. After detecting, only can the processes which is registed in the "Credible Processes List" be allowed to run. When the process is not in the list, if the user agree to allow the process runing, then the process is added to the list; instead, if the user does not agree to allow the process running, then the process is killed. Dt = 0 and Rt = 0 indidcat the situation which process is in the list, and (Dt - Rt) = 0 indidcat the situation which process is not in the list, that is responding immediately when detecting attacks.

2) The model can control attacks in a certain area and eliminate attacks within given time. For some business systems which can allow the first time attack to happen, if attacks can be eliminated in given time, then the defense mechanism is effective, that is Dt + Rt ≤ Et (the total of detection time and response time is smaller than exposure time which target system allow).

B. Model Analysis

The Active Controllable Defense model based on Zero-PDR model doesn't deny or overthrow the PDR model and the passive defense mechanism. Instead, the Active Controllable Defense model is proposed based on the further study of PDR model and current network security situation. This model focuses on how to detect and respond to attacks in time before network security threats happen or reach the target system. Compared with the traditional passive defense mechanism, Active Controllable Defense model can avoid the first time attack and the threats such as Trojan which have the "Zero-break Time" characteristics, keeping the network active in the face of a variety of security threats.

Active Controllable Defense model based on Zero-PDR model has the following characteristics:

1) The model can avoid the first time attack. Any network security threat can work as the operation of processes in computer operating system. The Active Controllable Defense model based on Zero-PDR model can detect and respond to any one process which require to run. As a result, the model can prevent incredible processes running and avoid the first time attack.

2) The model can use unchanged to respond to changes, preventing threats such as Trojans which have the "Zero-break Time" characteristics effectively. The model uses behavior-based defense solution, and detect the validity of each process by the "Credible Processes List". The model considers the unknown as incredible. Comprared with the traditional methods of making rules such as statistics and data mining, the "Credible Processes List" can use unchanged to respond to changes. No matter how the network security threats change, the model only let the processes in "Credible Processes List" run, preventing network threats effectively.

3) The model can defense both known and unknown threats. In traditional passive protection mechanism, characteristics databases and rules databases are established based on the characteristics of known threats, so it can hard to deal with unknown threats. Instead, the Active Controllable Defense model based on Zero-PDR model considered the unknown as incredible. Only the known and credible behavior can be allowed, preventing the unknown threats effectively.

IV. CONCLUSION

In the face of more and more diverse, intelligent and automatic network security threats, passive threats scanning and checking is difficult to defense network attacks completely, because protection always lags behind destruction. In this case, security practitioners contribute their efforts to the game between security and threats. Therefore, the idea must be changes from passive protection to active controllable defense. In new network environment, on the basis of further study on classical PDR protection model, the Zero-PDR model is proposed according to the threats which have the "Zero-break Time" characteristics. On the basis of the Zero-PDR model, the Active Controllable Defense concept and the Active Controllable Defense model are proposed further. The Active Controllable Defense model based on Zero-PDR model can prevent the threats which have the "Zero-break Time" characteristics effectively, and can detect and respond to attacks in time before network threats happen and reach the target system, preventing the first time attack effectively and keeping network active in the face of threats.

REFERENCES

[1] Jiangling Du. Computer Network Security and Active Defense[J]. Shanxi Finance University Journal, 2008:131~132.

[2] Winn Schwartau. Time-Based Security Explained: Provable Security Models and Formulas for the Practitioner and Vendor[J]. Computer&Security, USA, 1998:693~714.

[3] Liu Jizhen, Wu Kehe, Zhang Tong, Ma Gang. The Design and Implementation of Security Defense Technology Based on Mandatory Running Control[J]. 2009 Fifth International Conference on Information Assurance and Security, 2009:770~773.

[4] HongSheng Yan, XueLi Wang, Jun Yang. Computer Network Security and Defense[M]. Beijing: Electronics Industry Press,2007.

[5] Yuanfei Huang, Liyong Ji, Liping Jin. Exploration of Network Information Security Situation and related hot issues[J]. Telecommunications Science,2009.

[6] Chao Li. Simple Exploration of Network Information Security[J]. Scientific&Technological Information Development and Economic, 2009

[7] YuNing Wang. Current Situation and Defense of Network Information Security[J]. Modern Commerce Industry , 2008

[8] Wenfeng Ruan. Application of Active Defense in Trojan prevention[J]. Computer Security, 2007: 82~92.

[9] Xiangyang Xu. Analysis of Establishing Active Defense System in LAN[J]. Information Security Technology and Application, 2008:39~40.

[10] D.E.Bell, L.LaPaDula. Secure Computer Systems: Mathematical Foundations and Model[J]. Technical Report M74～244, Mitre Corp. , Bedford, MA, May 1973.

[11] K. J. Biba. Integrity Consideration for Secure Computer Systems[J]. Technical Report ESD-TR-76-372,Mitre Corp. , Bedford, MA, April 1979..