Chapter IV
Evolution of Enterprise Security Federation

Gaeil An
Electronics and Telecommunications Research Institute, Korea

Joon S. Park
Syracuse University, USA

ABSTRACT

In this chapter, we discuss the evolution of the enterprise security federation, including why the framework should be evolved and how it has been developed and applied to real systems. Furthermore, we analyze the remaining vulnerabilities and weaknesses in current approaches and propose new approaches to resolve those problems. Then, to overcome those weaknesses and vulnerabilities, we propose the PSM (Policy-based Security Management) architecture for an integrated security framework, and the PM (Packet-Marking) architecture for a cooperative security framework. The PSM architecture is able to efficiently realize the security purposes of an organization by controlling, operating, and managing various kinds of security systems consistently based on security policies. The PM architecture is able to effectively deal with suspicious network traffic without requiring new protocol, while reducing the false-positive problem and perfectly protecting QoS for innocent traffic from attacks. We simulated the PSM and PM architectures to evaluate their performance. The simulation result shows that the PSM architecture can automatically detect and respond against network attacks, and the PM architecture can effectively handle suspicious traffic, such as DDoS traffics.

INTRODUCTION

As Internet service is developed and used by various organizations and applications, the threats of cyber attacks become more critical issues, especially in sensitive applications that may span multiple organizations or systems. In order to protect enterprise systems from cyber attacks, researchers and vendors have introduced new technologies such as the Intrusion Detection System (IDS), Intrusion Prevention System (IPS), firewall, antivirus, and so on (Debar, Dacier, & Wespi, 1999; Malik, 2002). The enterprise security federation for managing and controlling security systems has evolved since its first generation to handle new threats and policy conflicts more effectively and efficiently.

The enterprise security federation can be classified as three frameworks: a simple security framework, an integrated security framework, and a cooperative security framework. The enterprise security federation has developed from an initially simple security framework into a cooperative security framework via an integrated security framework. A simple security framework has difficulty integrating heterogeneous...
security systems made by different multivendors into single management architecture. This problem is addressed by using an integrated security framework, whose purpose is to consistently control and manage various kinds of security systems based on a security policy, while providing for automation of both threat response service and security configuration service (Ahn, Yoon, & Nah, 2005). The key benefit of the cooperative security framework is a better view of global network attack activity (Locasto, Parekh, Keromytis, & Stolfo, 2005).

To address the integrated security framework, we introduce two security management technologies: Enterprise Security Management (ESM) (Check Point, 2000) and Policy-based Security Management (PSM) (Dinesh, 2000; Kim, Kim, & Na, 2005; Tishkov, Kotenko, & Sidelnikova, 2005; Westerinen, Schnizlein, Strassner, Scherling, Quinn, Herzog, Huyhn, Carlson, Perry, & Waldbusser, 2001). We focus, in this chapter, on PSM and propose policy-based security management architecture. The PSM architecture is able to efficiently realize the security purpose of an organization by controlling, operating, and managing various kinds of security systems consistently based on security policies.

We also introduce and analyze several cooperative security frameworks, such as Cisco’s architecture (Turk, 2004), Intel’s architecture (Durham, Govindarajan, Larson, Rajagopal, & Sahita, 2002), and pushback architecture (Mahajan, Bellovin, Floyd, Ioannidis, Paxson, & Shenker, 2002). Even though these cooperative security architectures are effective at mitigating network attacks, they have weak points. Cisco’s architecture has the problem that not only attack traffic, but also innocent traffic, is blocked. Intel’s architecture may experience communication overhead and have difficulty handling false-positive problems, because it has no mechanism for effectively dealing with suspicious traffic. Finally, pushback architecture has demerits in determining precise rate-limit values and in requiring new protocol between routers. To address those problems, we propose a Packet-Marking (PM) architecture as a cooperative security framework that is able to effectively deal with suspicious network traffic without requiring new protocol, while reducing the false-positive problem, and protecting perfectly the Quality of Service (QoS) for innocent traffic from attacks.

**BACKGROUND AND MOTIVATION**

In the early stage of the Internet, security framework was not greatly addressed, because the destructive power and effects of cyber attackers against computer and network systems were not so high. Simple security framework typically consists of several security systems such as IDS or Firewall, and simple security management system for displaying attack information detected by security systems (Debar et al., 1999; Malik, 2002). A firewall accepts or denies incoming traffic according to a set of predefined rules called an access control list (ACL). An IDS detects suspicious traffic based on a predefined attack signature or behavior. A security administrator identifies the source of attack by manually analyzing alert information received from an IDS, and then blocks the attack traffic by directly inserting new ACL into Firewalls.

With the appearance of new types of attacks and an increase of security threat against enterprise networks, the importance of security has more increased. To deal with the security threat, various kinds of advanced security systems have been developed, and the scope of the network to protect has been enlarged. However, a simple security framework has difficulty integrating heterogeneous security systems made by different multivendors into single management architecture, because there is no standard protocol between a security system and a security management system. The simple security framework needs to evolve into a new security framework that is able to consistently control and manage various kinds of security systems, while providing for automation of both threat response service and security configuration service. We will call the new security frame all “integrated security frame.”

Another problem of a simple security framework is that there is no mechanism to provide cooperation between security systems or between security management systems. Cooperation is very important when security systems defeat network attacks that exercise a bad effect on entire networks. One such network attack is the Distributed Denial of Service (DDoS) (Geng & Whinston, 2000; Mirkovic & Reiher, 2004). The first DDoS attack was seen in 1999. In 2003, there was a cyber incident by the DDoS attack executed by a Worm called Slammer (Moore, Paxson, Savage, Shannon, Staniford, & Weaver, 2003). The attack paralyzed Internet for many hours, so that network users could not access the Internet. A DDoS attack is very difficult to detect exactly, because the DDoS attack
Related Content

A Host-Based Intrusion Detection System Using Architectural Features to Improve Sophisticated Denial-of-Service Attack Detections
Ran Tao, Li Yang, Lu Peng and Bin Li (2010). *International Journal of Information Security and Privacy* (pp. 18-31).
[www.igi-global.com/article/host-based-intrusion-detection-system/43055?camid=4v1a](www.igi-global.com/article/host-based-intrusion-detection-system/43055?camid=4v1a)

Computational Complexity Analysis for a Class of Symmetric Cryptosystems Using Simple Arithmetic Operations and Memory Access Time
[www.igi-global.com/article/computational-complexity-analysis-class-symmetric/78530?camid=4v1a](www.igi-global.com/article/computational-complexity-analysis-class-symmetric/78530?camid=4v1a)

A Privacy Protection Model for Patient Data with Multiple Sensitive Attributes
[www.igi-global.com/article/privacy-protection-model-patient-data/2485?camid=4v1a](www.igi-global.com/article/privacy-protection-model-patient-data/2485?camid=4v1a)