End-User Security Management with Mobile Agents

Yuki KOTEGAWA†, Toshihiro TABATA‡, Yoshiaki HORI‡ and Kouichi SAKURAI‡

†*Graduate School of Information Science and Electrical Engineering, Kyushu University*

6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581, Japan

kotegawa@itslab.csce.kyushu-u.ac.jp

‡*Faculty of Information Science and Electrical Engineering, Kyushu University*

6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581, Japan

{tabata,hori,sakurai}@csce.kyushu-u.ac.jp

Abstract

In LAN (Local Area Network) of universities or companies, the damage of viruses and worms from inside End-Hosts is serious problem. It is demanded that all End-Users keep own End-Hosts secure. However, because some End-Users might not recognize the importance of security, it is difficult to keep all End-Hosts secure. In this paper, a framework of End-User security management is proposed. In our proposal, firstly, when an End-Host is connected to LAN, a mobile agent inspects a security condition of the End-Host. Secondly, security applications such as Firewall and IDS (Intrusion Detection System) are installed into the End-Host dynamically as mobile agents. Finally, other mobile agents manage those security applications. Network administrators can distribute security functions and security policies to all End-Hosts directly and dynamically by using mobile agents.

Keywords: End-User Security, Mobile Agents, Dynamic Installation, Dynamic Management

1 Introduction

In recent years, the damage from viruses and worms is increasing. Especially, in LAN (Local Area Network) of universities or companies, the damage of viruses, worms and intrusion behavior from inside hosts are pointed out as serious problems[1].

It is required that all End-Users keep own End-Hosts secure. In order to protect those End-Hosts from threats such as viruses and worms, End-Users install security applications (e.g. Anti-Virus Application, Personal Firewall and Host-Based IDS (Intrusion Detection System), and so on) into their End-Hosts. Continuous update of those security applications is performed. Moreover, security patches have to be applied to those End-Hosts. However, some End-Users might not recognize the importance of security. Thus, it is difficult to keep all End-Hosts secure.

On the other hand, in order to prevent insider attacks by hosts infected with viruses or worms, Miwa proposed a quarantine mechanism to a host connected to the

network[1]. In the proposed mechanism, security inspection is performed before a host connects to a network. If the host passed the inspection, the connection to the network is permitted. The mechanism guarantees hosts' security at the time of the connection. However, hosts' security after the connection is not considered. A host connected to LAN might not be kept secure.

We consider that a mechanism is required for maintaining hosts' security even after connection of the host to the network. We focus on mobile agent technology [2] for the mechanism which maintains hosts' security even after the connection. Mobile agents can realize installing dynamically security applications into hosts. Moreover, mobile agents manage those security applications continuously. The mobility of mobile agents can save the time and effort of installing security applications. The time and effort of security management is also reduced.

2 Mobile Agents

A mobile agent is not bound to the system where it begins execution. The agent has the unique ability to transport itself from one system in a network to another [2]. Mobile agents can migrate from a host to another host over a network. Mobile agents have various advantages, such as asynchronous execution, load balancing, fault-tolerant, reduction of the amount of communications, and so on. Moreover, mobile agents can also interact with other applications.

Recently, many IDSs using mobile agents are being researched [3]. The Intrusion Detection Agent system (IDA) [4] can trace attackers using mobile agents. In the paper [5], architecture for a distributed stealth intrusion detection and response system (IDRS) based on mobile agents mimicking behavior of social insects is proposed. In this architecture, a mobile agent is overseeing a process, as well as its network connection. Another mobile agent in random checking mode is performing integrity control on the binary code of the system. These researches use mobile agents for the decentralization of IDS, the cooperation between IDSs, or the flexibility of functions.

3 Proposed System

In this section, we propose a system to managing End-User security. Using our proposed system, network administrators can distribute and apply security functions and security policies to all End-Hosts. By using mobile agents, those distributions are performed directly and dynamically. The details of our proposal are described as follows.

3.1 System Architecture

Figure 1 presents a network model assumed in our proposal. End-Hosts receive a network configuration with DHCP. Each End-Host and DHCP Server has a Mobile Agent System (MAS) which is a platform of mobile agents. On the other hand, End-Hosts do not have security applications such as PFW (Personal Firewall) and IDS (Intrusion Detection System). Attacks from the Internet to LAN are prevented by Gateway. Gateway has Firewall, Viruswall, and IDS.

Figure 2 illustrates architecture of our proposed system. Our proposed system consists of *DHCP Daemon*, *Agent Manager (AM)* and *Security Agents (SA)*.

DHCP Daemon distributes dynamically a network configuration such as an IP address to an End-Host. Moreover, DHCP Daemon also interacts with Agent Manager in order to generate Security Agents.

Agent Manager manages Security Agents. Based on communication with DHCP Daemon, Agent Manager creates Security Agents and sends those Security Agents

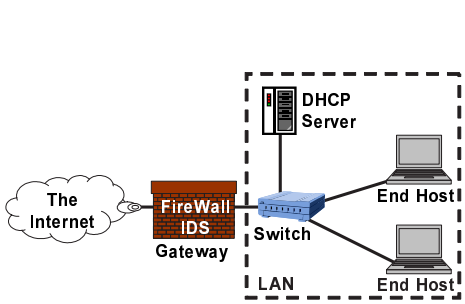

Figure 1: Network Model

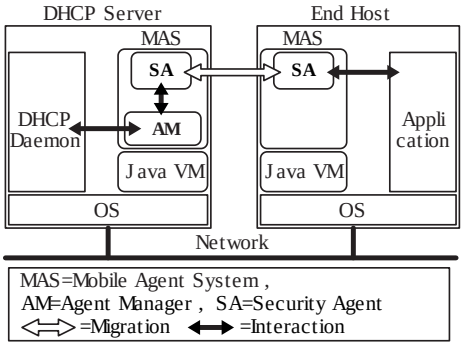

Figure 2: Architecture of Our Proposed System

to End-Hosts. Agent Manager also records information about itineraries of Security Agents.

Security Agents consist of four kinds of mobile agents. The first of Security Agents is *Inspection-Agent*. The second is *ID(Intrusion Detection)-Agent*. The third is *FW(FireWall)-Agent*. The other is *Maintenance-Agent*.

Inspection-Agent checks security of an End-Host. In the security check, infection of viruses and worms is inspected. Moreover, update condition of Anti-Virus application, PFW and IDS is also inspected. The security check is based on the information of registry, names of executing processes and so on.

ID-Agent and/or *FW-Agent* migrate to an End-Host from DHCP Server if the End-Host does not have Anti-Virus, IDS, and/or PFW application. ID-Agent observes malicious behavior (e.g. writing to a system directory, access to some ports). FW-Agent controls ports according to policy rule. Those policy rules of ID-Agent and FW-Agent are reconfigured by the following Maintenance-Agent.

Maintenance-Agent configures rules of ID-Agent and FW-Agent dynamically. Maintenance-Agent migrates to an End-Host when a security patch of operating system is distributed or security policy is modified, and so on. Moreover, Maintenance-Agent also migrates to another End-Host randomly, and checks whether ID and FW rules are applied correctly.

3.2 Procedures

Our proposed system performs three procedures as follows.

The first is *Security Inspection*. An End-Host connects DHCP Server. Before DHCP Daemon distributes an IP address to the End-Host, DHCP Daemon communicates with Agent Manager in order to generate Inspection-Agent. Moreover, DHCP Daemon configures Network Switch in order to isolate the End-Host with VLAN (Virtual LAN). Agent Manager creates Inspection-Agent. Then DHCP Daemon distributes the IP address to the End-Host. Inspection-Agent migrates to the End-Host. Inspection-Agent performs security check on the End-Host and sends the result of the security check to Agent Manager.

The second is *Security Installation*. Agent Manager creates ID-Agent and FW-Agent according to the result sent by Inspection-Agent. Agent Manager sends those Agents to the End-Host. ID-Agent begins to observe ports and processes. FW-Agent begins to perform packets filtering. Then those Agents communicate with Agent Manager after the migration for canceling the isolation against the End-Host. Agent Manager cancels the isolation with VLAN. The End-Host comes to be able to do

communication with other hosts.

The third is *Security Maintenance*. Agent Manager generates Maintenance-Agent when security patch of operating system is distributed or security policy is modified. Then Agent Manager transmits Maintenance-Agent to the End-Host. Maintenance-Agent checks rules of ID-Agent and FW-Agent. If those rules are old, those rules are reconfigured. After the reconfigurations, Maintenance-Agent migrates to another End-Host and reconfigures the End-Host's rules similarly.

3.3 Consideration

In our proposal, security check to an End-Host is performed when the End-Host connects to LAN. During security check, the End-Host is isolated from LAN by using VLAN. If the End-Host does not have sufficient security functions (e.g. PFW, IDS, Anti-Virus application), missing security functions are installed into the End-Host as mobile agents. By using mobile agents, flexible extension can be performed to the End-Host. Because network administrator can distribute security functions and security policies to all End-Hosts directly and dynamically, all End-Hosts can be kept secure.

However, an End-User may dislike that mobile agents are executed on his/her End-Host. Thus, this might require a mechanism for trusting mobile agents.

4 Conclusion

In this paper, mobile agents-based framework for end-user security management was proposed. In our proposed system, security check at the time of connection to LAN, the dynamic installation of security function, and the continuous security management are performed. The mobility of mobile agents can save the time and effort of installing security function. Moreover, the time and effort of security management is reduced.

In future work, we will implement and evaluate a prototype of our proposal.

References

[1] Shinsuke Miwa, "A proposition of the quarantine mechanism for infected PCs", Computer Security Symposium 2003, 2003.

[2] OMG, "Mobile Agent Facility Specification", 2000.

[3] Wayne A. Jansen, "Intrusion detection with mobile agents", ELSEVIER, Computer communications, p. 1392-1401 Volume 25, Issue 15, 2002.

[4] Midori Asaka, Shunji Okazawa, Atsushi Taguchi, and Shigeki Goto, "A Method of Tracing Intruders by Use of Mobile Agents", INET '99 Conference, June 1999.

[5] Serge Fenet and Salima Hassas, "A Distributed Intrusion Detection and Response System Based on Mobile Autonomous Agents Using Social Insects Communication Paradigm", First International Workshop on Security of Mobile Multiagent Systems, Autonomous Agents Conference, 2001.