THE SUMMARY OF Ph. D. DISSERTATION

No. 1

Major	Student Identification Number	SURNAME, Firstname TAKEMORI, Keisuke

Title

Incident Monitoring Techniques of Network Systems against Cyber-terrorisms

Abstract

Recently, security threats have become a pressing problem over world wide network. Many computer viruses have been found, such as CodeRed worm on July 2001, Slammer worm on January 2003, and Blaster worm on August 2003, and have been found and affected many hosts. These worms are circulating around the Internet with self-propagating malicious code. The high volume of network traffic will likely cause a distributed denial of service attack. Therefore, it is expected that SOCs (Security Operation Centers), which can audit victim systems, security logs, and unknown attack techniques, will be established against cyber-terrorism. When computer security incidents occur, the SOC must respond quickly and effectively.

In this paper, we propose advanced monitoring techniques to patrol remote systems, to collect unknown threats, and to analyze security logs for SOC analysts. Also, we develop and evaluate these techniques; and our experimental results show that they can detect anomalies. One of the goals of our research is to try to find ways to improve technical approaches for detecting and identifying security flaws, for limiting the damage from attacks, and for ensuring that systems continue to provide essential services in spite of compromises or failures.

Chapter 1 shows the background and the objectives of this research, and a summary of this paper.

In chapter 2, we propose a remote patrol system for web servers, which detects defacement attacks and denial of service attacks. The system finds all the homepage files on

a web server by analyzing tagged information, and audits file header information or hash based information. We evaluate the patrol technologies of parallel processing approaches, and that the results achieve a low additional load and a constant monitor on the remote network systems.

In chapter 3, we propose a notable platform to find out characteristics of intruders by recording suspicious activities. The system diverts suspicious connections from a real system to a trap system by using an IDS (Intrusion Detection System) even while the connection is ongoing. It provides a synchronous connection flow management between connections with a real system and those with a trap system so as not to be disclosed to the intruders. We preliminarily evaluate performance in practice using FTP and HTTP services, and our results indicate that our proposed system achieves little latency in diverting connections to the trap system. Therefore, we believe that the system gives administrators a platform to understand intruder’s techniques and to protect against the threats they face.

In chapter 4, we propose a novel log analyzer that manages IDS logs installed on widely distributed area. The system attempts to detect anomalies on time-axis based on computing techniques between a long term profile and a short term profile. The experimental results with some real audit data show that the objective alarms are effective with more reliable performance for SOC analysts. The faster an organization recognizes, analyzes, and responds to an incident, the better it can limit damage and lessen recovery costs.

Finally, chapter 5 concludes the results of the research in the paper.