A Multi-agent Cooperative Model and System for Integrated Security Monitoring*

Xianxian Li and Lijun Liu

School of Computer Science and Engineering, Beihang University, Beijing, China
{lixx, liulijun}@buaa.edu.cn

Abstract. The increasing complexity of various network threats has made the integration and cooperation of multiple security monitoring technologies necessary in network security defense. However, most existing works have focused on certain special monitoring technologies such as intrusion detection, and studies on integrated security monitoring system are quite insufficient. In this paper, a novel formal model called MCSM (Multi-agent Cooperation model for Security Monitoring based on knowledge) is proposed. In MCSM, the integrated security monitoring is modeled as a FSA (Finite State Automata) with multiple agents, and a general knowledge structure for multiple agents is constructed. We have successfully developed an IMS (Integrated Monitoring System) called ACT-BroSA (Broad-spectrum security Scan and Analysis system) based on MCSM. Results of experiments show that the integrated monitoring capability is significantly improved.

Keywords: Network security, Security monitoring, Multi-agent cooperation, Knowledge Management.

1 Introduction

With the increasing complexity of different network threats, relying on any single technology is not enough to meet the secure defense requirements. Then it brings about an important area: how to integrate multiple security monitoring technologies in network defense? In some cases, integrating multiple detection technologies can improve the integral monitoring effect significantly. For example, we can check the vulnerable situation of the object host and eliminate false alarms by integrating IDS (Intrusion Detection System) and vulnerability scan system [1, 2, 3], and the combination of IDS and security audit system may be used to automatically extract intrusion evidences.

To integrate multiple security monitoring systems, we face two basic challenges: cooperating and uniformly managing the knowledge for different systems, because various security systems are heterogeneous in architectures and working mechanisms. Unfortunately, to the best of our knowledge, there is no efficient solution available to construct a compact integrated security monitoring system up to now.

* This work is supported by Program for New Century Excellent Talents in University.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 329 – 341, 2006.

In this paper we propose a novel formal model called MCSM (Multi-agent Cooperation model for Security Monitoring based on knowledge) for constructing the IMS. In MCSM, every monitoring system is modeled as an agent and multi-agent technology is used to model the integration and cooperation of multiple monitoring technologies. The model consists of two levels: the KAM (Knowledge Action Model) and the CDM (Cooperation Detection Model). In the KAM, we build a general knowledge structure for multi-type monitoring systems based on predicate logic. This structure can support efficient scan algorithms and provide the unified knowledge management for integrating multiple systems. In CDM, we further describe how the knowledge structure can affect their cooperation. Then the cooperating and scheduling mechanisms of multi-agents are modeled with the FSA (Finite State Automata).

Based on MCSM, we have proposed a novel method for constructing IMS which includes a new architecture and the supporting technologies, and successfully developed the ACT-BroSA (Broad-spectrum security Scan and Analysis system). In ACT-BroSA, we implemented the integration and cooperation of multiple security monitoring systems. We also evaluated the efficiency of the scan algorithm and the effect of the cooperative monitoring, which are the most important aspects of MCSM. In the field of modeling security system using multi-agent, most existing works focused on certain technologies such as firewall [6, 7, 10] and IDS [8, 9]. Research works on the integration and cooperation of multi-type systems are still quite few. In the system development field, the existing solutions [4, 5] provided by the industry community focused too much on the integration of special security products through extern interfaces, but the general cooperation mechanism and the theoretical model study were neglected. Our work mainly focuses on the modeling and constructing of integrated security system, and we believe it is an important complement to current works.

2 Related Work

Many efforts have been made on the modeling of security system based on multi-agent technology [8-15, 18]. A multi-agent based model for distributed intrusion detection and response is proposed in [8, 10]. [9] and [12] explore the implementation of intrusion detection and firewall framework based on the mobility of agent. They all focus on special security technology, but the integration and cooperation of multi-type security technologies are not discussed.

In [14], an intelligent network security management model based on multi-agents is proposed. It refers to the decision making and the cooperation of agents based on interactions, but the detailed cooperation and decision mechanisms are not described. [15] constructs a model for the network security management and proposes a new multi-agent architecture. The main focus is the agents' function and the model architecture rather than the cooperation mechanism.

The works in [16] and [17] focus on the cooperation mechanism of multi-agents. In [16], the knowledge is defined as a character of agent and the knowledge structure is discussed. [17] describes the cooperation mechanism between agents and proposes a