보 안 공 학 연 구 논 문 지
제 2 권, 제 4 호, 2005 년 11 월

모바일 에이전트 기반의 오용 침입탐지시스템에 대한 보안정책 관리 모델

김태경 [1], 홍길동 [1], 한석봉 [2]
[1]oo 성균관대학교 전기전자컴퓨터공학부
e-mail : {tkkim, dylee}@rtlab.skku.ac.kr
[2]oo 대학교 oo 과
e-mail : yyy@ssss.ac.kr

Mobile Agent-based Security Policy Management Model for Misuse Intrusion Detection Systems

Tae-Kyung Kim[1],[1], and [1]
[1]Real-Time Systems Laboratory,
School of Information and Communication Engineering,
SungKyunKwan University,
Chunchun-dong 300, Jangan-gu, Suwon, Kyunggi-do,
Republic of Korea
tkkim@rtlab.skku.ac.kr

Abstract

This paper describes the rule propagation model for the misuse intrusion detection system using mobile agents. Misuse detection method is best suited for reliably detecting known use patterns because misuse detection systems can detect many or all known attack patterns. But these systems are of little use for as yet unknown attack methods [1]. In this paper, we presented the mobile agent based policy management model to solve the drawbacks of misuse intrusion detection system. Mobile agent constantly moves around the misuse intrusion detection systems for propagating new attack patterns rapidly with low workload. Also mobile agent can propagate the security policy into heterogeneous security systems such as firewall, ESM (Enterprise Security Management) system.

1 Introduction

Significant progress has been made in the improvement of computer system security. On the other hand, attempted attacks and successful invasions involving an increasing number of computers have become frequent. Thus, security has become a key word for most companies worldwide. Intrusion detection is defined [2] as, "The problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges." Intrusion-detection systems aim at detecting attacks against computer systems and networks. There are two complementary trends in intrusion detection: misuse detection [3][4] uses knowledge accumulated about attacks and looks for evidence of the exploitation of these attacks, and anomaly detection [3] which builds a reference model of the usual behavior of the information system being monitored and looks for deviations from the observed usage. And many of intrusion detection systems use misuse detection method. According to the data of information security 21c [5], 7% of intrusion detection systems use anomaly detection, 43% use misuse detection, 17% use anomaly and misuse detection at the same time, and 33% use other methods.

The drawbacks of the misuse detection approaches are that they have the difficulty of gathering the required information on the known attacks and keeping it up to date with new vulnerabilities and environments. In developing misuse intrusion detection, we propose a mobile agent-based rule propagation method. This method rapidly spreads the rules, which have information about new forms of attacks, to other's misuse detection systems.

Prior to designing a mobile agent-based rule propagation approach, we investigated patterns of the intrusion detection rules. The intrusion detection rules can be divided into two systems: A forward-chaining rule-based system and a backward-chaining rule-based system [6]. A forward-chaining rule-based system is data-driven:

each fact asserted may satisfy the conditions under which new facts or conclusions are derived. Alternatively, backward-chaining rule-based systems employ the reverse strategy; starting from a proposed hypothesis they proceed to collect supportive evidence. Our proposed system uses the forward-chaining rule-based system. The person who finds the intrusion first creates an intrusion detection rule and the rule is propagated to other intrusion detection systems that are not intruded upon by the above intrusion using a mobile agent.

This paper mainly describes dynamic agent-based rule propagation for improving misuse detection efficiency. In section 2, some related works and a mobile agent description are shown. In section 3, the design of mobile agent-based misuse intrusion detection rule propagation model is clarified. Section 4, summarizes this paper.

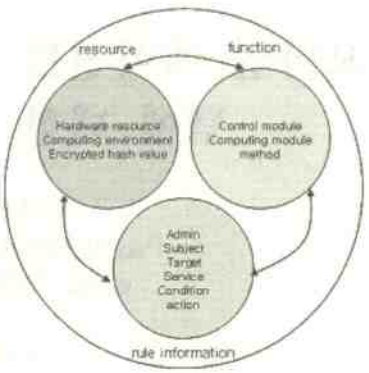

Fig. 1. Mobile Agent Architecture

2 Related Works

In this section, we introduce the overview of mobile agent and describe briefly the characteristics of the typical agent-based intrusion detection systems (IDSs) – EMERALD, AAFID and IA-NSM.

2.1 Overview of Mobile Agent

A mobile agent is a kind of independent program, which can migrate from one node to another node in a distributed network by itself. Compared to traditional distributed techniques such as the Client-Server model and Code On Demand model, a mobile agent has advantages as follows:

- Making proper use of existing resources so as to fulfill user's assignment
- Debasing network traffic
- Balancing network load
- Supporting fault-tolerance
- Supporting mobile user
- Supporting customized services

A mobile agent has its own lifecycle including the states of create, halting, executing, service searching, arriving new host, migrating, returning to the original host and terminating. We use this agent technology in misuse intrusion detection system to spread the rule, which contains the intrusion information. A mobile agent consists of three parts: resource, function and rule information. Figure 1 shows the constitution of mobile agent [17].

The resource section contains the hardware resource, computing environment and encrypted hash value. Computing environment means the serialized state of the agent encoded in the method part. The encrypted hash value is used to check the integrity of the agent. The function part includes control module, communication module and method. The control module controls all functions of the mobile agent including authentication and authorization. The communication module provides a secure communication channel between the agent and IDS. Method module includes a concrete computing code and program [17].

Rule information in the agent is composed of six elements. The elements are administrator, subject, target, service, condition and action information. Admin indicates the operator who makes the intrusion detection rule. Subject describes the object which needs the security service. Target shows the object that needs to be protected from attacks. Service shows which service is controlled by the intrusion detection rule. Condition shows the condition that must be satisfied by an event. Action describes the action that is performed if the condition is satisfied. Mobile agents offer a new paradigm for distributed system environments, but there are two kinds of security issues specific to a mobile agent [17]: malicious agent - protection of the host against agent and protection of other agents, and malicious host - protection of the agent from the host and protection of the network.

We have suggested a security model that provides safety from a malicious agent and a malicious host. Encrypted hash values guarantee the integrity of the mobile agent and protect unauthorized modification of the mobile agent. A trusted third party authenticates a mobile agent. Thus this system is protected from the activities of malicious agents and malicious hosts.

2.2 The characteristics of the typical agent-based IDSs

Agent technology has been academically applied in a variety of fields, particularly in artificial intelligence, distributed systems, software engineering and electronic commerce. Generally, an agent can be defined as a software program capable of executing a complex task on behalf of a user [7]. The use of autonomous agents has been proposed by some other authors as a form of constructing non-monolithic intrusion detection systems [8, 9, 10]. The capacity of some autonomous agents to maintain specific information of their application domains, in this case security, confers great flexibility on these agents and hence, on the entire system. The characteristics of typical agent-based IDS are follows:

- EMERALD

The SRI(Stanford Research Institute) EMERALD(Event Monitoring Enabling Response to

Autonomous Live Disturbance) project addresses the problems of network intrusion via TCP/IP data streams. Network surveillance monitors observe local area network traffic and submit analysis reports to an enterprise monitor, which correlates the reports. EMERALD appears to concentrate the intelligence in a central system and does not incorporate any agent technology [12][13][14].

♦ AAFID

The Autonomous Agents For Intrusion Detection (AAFID) Project is based on independent entities called autonomous agents that perform distributed data collection and analysis. Centralized analysis is done on a per-host and per-network basis by higher-level entities called transceivers and monitors. The architecture allows for computation to be performed (and thus, for intrusion detection to happen) at the point where enough information is available. This can be at the agent, transceiver or monitor level [15].

♦ IA-NSM

The Intelligent Agents for Network Security Management (IA-NSM) Project for Intrusion Detection using intelligent agent technology provides a flexible integration of a multi-agent system in a classical networked environment to enhance its protection level against inherent attacks [16].

As previously mentioned, a mobile agent technology is a growing area of research and new application development in telecommunications. Until now, there was no mobile agent-based rule propagation system in Intrusion Detection Systems. In this paper, the mobile agents are used as carrier and especially negotiate with other intrusion detection systems about intrusion detection rules. And also, we present the mobile agent-based detection rules propagation model for the misuse IDS in distributed network environments.

3 Misuse Intrusion Detection Rule Propagation System Design

This section describes the design details of the mobile agent-based rule propagation system and clarifies the objectives in designing a mobile agent-based rule propagation system to solve the problems of misuse detection. We set up the following goals:

- ♦ Propagate rules in dynamic and distributed environments
- ♦ Security of the mobile agent-based rule propagation system
- ♦ Authentication of the mobile agent
- ♦ Negotiation of the mobile agent and intrusion detection system

When the administrator managing the intrusion detection system finds new attacks, he enters information about the new attacks into the User Interface. Then the information is transmitted to the Rule Executor. The Rule Executor decides whether this rule is applied locally or globally. If the rule is specified locally, the rule is added to the Knowledge-base. Otherwise the Rule Executor generates a rule about new attacks using the Knowledge-base and sends the rule to the Agent Generator. The Agent Generator generates a mobile agent, which contains rule information. The mobile agent migrates to the other IDSs through the Internet, and moves dynamically in distributed environments to propagate the intrusion detection rule. Architecture of the mobile agent generation is shown in Fig. 2.

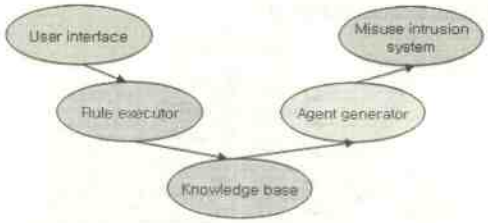

Fig. 2. Procedure of the mobile agent generation

The message types defined are summarized in the following table:

Table 1. Message types between a mobile agent and IDS

Message	Description
Request	request for security policy
Reply	reply that answers a request
Rule	upload and download of security policy between mobile agent and IDS
Ack	Acknowledges a security policy message
Status	informs the status of mobile agent and IDS

The architecture of a mobile agent-based rule propagation system (MARS) is shown in Fig. 3.

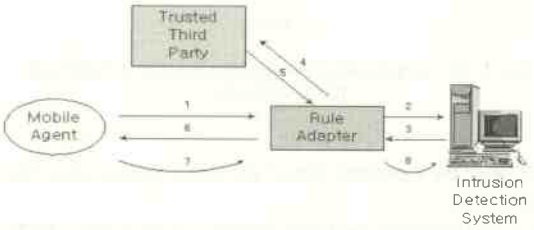

Fig. 3. Architecture of a mobile agent-based rule propagation system (MARS)

The Rule adapter is a function of software that communicates with mobile agents and makes decisions as to whether a rule is necessary to the intrusion detection system. A trusted third party is an authentication server that authenticates the mobile agent. When a mobile agent arrives at the rule adapter(1), The Rule adapter checks the policy conflict(2). If there is no conflict between the rules of the mobile agent and the rules of the intrusion detection system(3), then the rule adapter authenticate the mobile agent using the trusted thirty party(4,5,6). And the rule adapter checks the integrity of the rule using the hash value in the mobile agent(7). Finally, the rule having the

information about the new attack is added to the rules of the intrusion detection system. When there is conflict between the rules of the agent and the intrusion detection rules, the rule adapter informs the mobile agent of the conflict. And the mobile agent returns to the original host to notify the conflict information. Therefore the rule adapter serves as a mediator between the mobile agent and the IDS to offer the capability of negotiation. Fig. 4 depicts the difference between a conventional Intrusion Detection System and MARS.

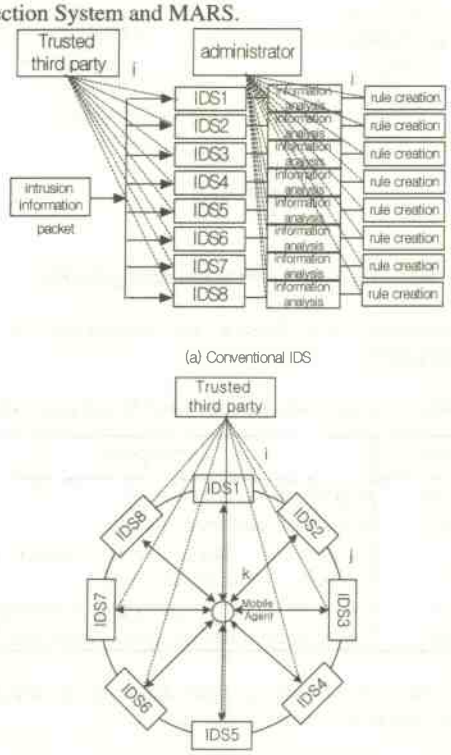

Fig. 4. The comparison of the performance of a conventional IDS and MARS

We listed the workload data of the above two systems like this.

- i: transmission workload between trusted third party and ids
- j: transmission workload between one ids and another ids
- k: transmission workload between mobile agent and ids
- l: transmission workload between administrator and ids
- m: the workload of analysis for intrusion detection rule
- n: the workload of rule creation for intrusion detection system
- p: authentication and authorization of mobile agent, packet and ids
- q: transmission workload of packet from the person who finds the intrusion to ids

Table 2. The workload data of conventional and MARS IDS

Action	Conventional IDS	MARS IDS
Transmission packet	Nq	Q
authentication & authorization	N(i+p)	2N(i+p)
Information analysis	N(l+m)	l+m
rule creation	N(l+n)	l+n
rule propagation		k+(N-1)j

N : Number of IDS

So, the total workload data of a conventional IDS is N(i+p+q+2l+m+n). As the number of IDS increase, the total workload increases (i+p+q+2l+m+n) times. The total workload data of MARS IDS is q+2N(i+p)+2l+m+n+k+(N-1)j. And q+2l+m+n+k is fixed. So as the number of IDS increases, the total workload data increases (2i+2p+j) times. The value of authentication & authorization for the MARS IDS is 2N(i+p) because of mutual authentication & authorization between the IDS and the mobile agent. Fig. 5 depicts the difference between the two systems with respect to total workload data and number of IDS.

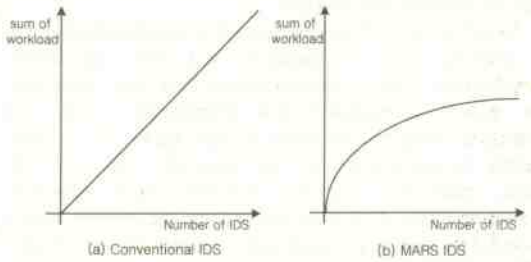

Fig. 5. Sum of workload data

As the number of IDS increases, the MARS IDS is more efficient than the conventional IDS. And mutual authentication between the IDS and the mobile agent guarantees the security of the rules.

4 Conclusion and Future Works

Misuse-based intrusion detection method is used more than any other intrusion detection methods. But this method has the difficulty of protecting a system from unknown attacks. We have presented a mobile agent-based rule propagation model, MARS that solves this problem. The mobile agent can move around the IDSs and quickly propagate the rules. And negotiation between the mobile agent and IDS makes it possible to select, reject, upload and download the rules. And the comparison of the workload of conventional IDS with MARS shows that the cost of MARS is less than that of conventional IDS. We have also proposed a constitution of a mobile agent and a rule adapter to solve the security issues of mobile agent.

In future work we plan to improve and extend MARS in a variety of areas, including enhancing the ability of the rule adapter to alert or cooperate with other security systems such as Firewall and ESM (Enterprise Security Management), and enhancing the mobile agent to efficiently communicate with other security systems in analyzing, complementing, reinforcing, verifying, adjusting monitoring and responding.

References

[1]. R. G. Bace. Intrusion Detection, Macmillan Technical Publishing 2000.
[2]. B. Mukherjee, T. L. Heberlein and K. N. Levitt. Network Intrusion Detection. IEEE Network, May/June 1994.
[3].R. Jagannathan, T. Lunt, D. Anderson, C. Dodd, F. Gilham, C. Jalali, H. Javitz, P. Neumann, A. Tamaru, and A. Valdes. System Design Document: Next-Generation Intrusion Detection Expert System (NIDES). Technical Report A007/A008/A009/A011/A012/A014, SRI International, March 1993.
[4].S. Kumar and E. Spafford. "A Pattern Matching Model for Misuse Intrusion Detection," Proceedings of the Seventeenth National Computer Security Conference, Oct. 1994.
[5].Information Security 21c, the history and kinds of intrusion detection system, http://www.securityinformation.com, July 2001.
[6]. U. Lindqvist and P. A. Porras. Detecting computer and network misuse through the Production-Based Expert System Toolset (PBEST). In Proceedings of the 1999 Symposium on Security and Privacy, Oakland, California, May 1999.
[7]. H. S. Nwana. Software Agents: an Overview. Knowledge Engineering Review, 1996.
[8]. M. Crosbie and G. H. Spafford. Defending a Computer System using Autonomous Agents. Technical Report No. 95-022, Dept. of Comp. Sciences, Purdue University, March 1996.
[9]. M. Crosbie, and E. H. Spafford. "Active Defense of a Computer System using Autonomous Agents", Technical Report CSD-TR-95-008, Department of Computer Sciences, Purdue University, 1995.
[10]. Balasubramaniyan, Jai, J. O. Garcia-Fernandez, E. H. Spafford, and D. Zamboni. An Architecture for Intrusion Detection using Autonomous Agents. Department of Computer Sciences, Purdue University; Coast TR 98-05; 1998.
[11]. S. Stolfo, A. Prodromidis, S. Tselepsis, W. Lee, D. Fan and P. Chan. JAM: Java Agents for Metalearning over Distributed Databases. In Prod. Third Intl. Conf. Knowledge Discovery and Data Mining, 1997.
[12]. G. G. Helmer, J. S. K. Wong, V. Honavar, and L. Miller. Intelligent agents for intrusion detection. In Proceedings, IEEE Information Technology Conference, pages 121--124, Syracuse, NY, September 1998.
[13]. A. Porras and P. G. Neumann. EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances. In Proceedings of the National Information Systems Security Conference, Oct 1997.
[14]. A. Porras and A. Valdes. "Live Traffic Analysis of TCP/IP Gateways," in Networks and Distributed Systems Security Symposium, March 1998.
[15]. B. Jai, J. O. Garcia-Fernandez, E. H. Spafford, and D. Zamboni. An Architecture for Intrusion Detection using Autonomous Agents. Department of Computer Sciences, Purdue University; Coast TR 98-05; 1998.
[16]. K. Boudaoud, H. Labiod, R. Boutaba, Z. Guessoum. Network security management with intelligent agents. Network Operations and Management Symposium, 2000. NOMS 2000.
[17]. L. Qi, L. Yu. "Mobile agent-based security model for distributed system", Systems, Man, and Cybernetics, 2001 IEEE International Conference, 2001.

저자소개

이름(영문이름)

김태경(Kim Tae-Kyung)
1997 년 2 월 단국대학교 수학교육과 (학사)
2001 년 성균관대학교 정보통신공학 (석사)
2005 년 성균관대학교 전기전자및 컴퓨터공학부 (박사)
<주관심 분야 : 네트워크 보안, 그리드 네트워크, 네트워크 QoS>

김민수(Min-Soo Kim)
1987 년 2 월 한양대학교 공과대학 전자공학과 (학사)
1990 년 2 월 한양대학교 공과대학 전자공학과 (석사)
1997 년 3 월 ~ 2002 년 8 월 한양대학교 공과대학 전자통신과 (박사)
1990 년 9 월 ~ 2001 년 2 월 국방과학연구소 연구원
2001 년 3 월 ~ 현재 한중대학교 정보통신과 조교수
<주관심분야 : 스마트 안테나 시스템, 적응 알고리즘, DSP 응용>

이정석(Jung Suk Lee)
1985 년 2 월 광운대학교 전기공학과 (학사)
1990 년 8 월 광운대학교 전기공학과 (석사)
2001 년 8 월 광운대학교 제어계측공학과 (박사)
1990 년 10 월 ~ 1997 년 2 월: 국방과학연구소 항공전자실 선임연구원
2002 년 9 월 ~ 현재: 인하공업전문대학 메카트로닉스과 조교수.
<주관심 분야: 제어계측, 머신비젼, RFID 응용>