다수의 이종 IDS Agent 관리를 위한 관리정보 설계와 중앙관리 시스템 구현

정훈조, 정태명

성균관대학교, 전기전자및컴퓨터공학과

Design of Management Information and Implementation of Central Management System for Managing Multiple Heterogeneous IDS Agents

Hoon-Jo Chung, Tai-Myung Chung

Dept. of Electrical & Computer Engineering, SungKyunKwan Univ.

요 약

인터넷 기술이 발전되고 활성화됨에 따라 인터넷에 연결된 호스트들과 네트워크는 외부의 악의적인 침입자에 의해 공격받을 수 있는 잠재성이 나날이 증가하고 있다. 이러한 이유로 네트워크 및 호스트 보안에 대한 관심과 연구활동이 활발해 졌으며, 대표적인 보안 솔루션 중의 하나인 침입탐지시스템이 각광을 받고 있다. 탐지 기술적 분류에 따라 크게 네트워크 기반 침입탐지시스템과 호스트 기반 침입탐지시스템이 존재하며, 한편으로 네트워크 규모의 증대로 다수의 침입탐지시스템의 운용이 필요하다. 이와 같이 이질적인 다수의 침입탐지시스템을 운용하는 경우, 관리의 복잡성과 관리비용의 증대라는 문제점을 내포한다. 본 논문에서는 이질적인 다수의 침입탐지에이전트들을 통합 관리하기 위한 중앙통제 시스템의 구현을 설명하고, 여기에 확장성과 유연성을 부여하기 위한 관리 자료 구조의 설계에 대해 기술한다.

I. 서론

네트워크에서의 사건 정보, 호스트에서의 사용자 행위 추적 등의 자료를 기반으로 호스트나 네트워크에 대한 침입행위를 감시하고 보고하는 침입탐지시스템(Intrusion Detection System, IDS)은 1980년대 후반에 Dorothy Denning이라는 사람에 의해서 창안되었다[1]. 침입탐지시스템은 침입탐지 기법에 따라 오용탐지(misuse detection) 기법과 비정상행위탐지(anomaly detection) 기법으로 분류되며, 감사 데이터의 유형에 따라 호스트 기반 침입탐지시스템과 네트워크 기반 침입탐지시스템으로 분류된다[7].

오늘날까지 개발되어 온 침입탐지시스템의 발전 흐름을 살펴보면 다음과 같다. 최초의 침입탐지시스템은 하나의 호스트에서 발생하는 감사 자료를 이용하여 침입을 탐지하는 호스트 기반의 형태로 출발하였다[2]. 이후, 하나의 네트워크 세그먼트를 통과하는 패킷을 감사 자료로 이용하여 침입을 탐지하는 네트워크 기반 침입탐지시스템에 대한 연구가 활성화되었다[3]. 이 두 가지 탐지 기술을 기반으로 발전해 오던 침입탐지시스템은 서로의 장단점을 보완하여 호스트 기반 침입탐지시스템과 네트워크 기반 침입탐지시스템으로부터 발생한 침입정보와 이들 정보의 통합에서 얻어지는 추가적인 정보를 이용하여 탐지의 신뢰성과 새로운 유형의 침입을 탐지할 수 있는 복합적이며 계층적인 구조로 발전되고 있다[4]. 그리고, 최근의 침입탐지시스템에서는 이동 에이전트를 이용한 침입탐지시스템이나 Gigabit 네트워크 기반의 침입탐지시스템 등과 같이 신기술의 적용이나 고성능의 침입탐지시스템 개발과 같은 방향으로 연구가 진행되고 있다[6][7].

본 논문에서는 오용 탐지 방식의 한 종류로 분류되는 다수의 규칙 기반(rule-based) 침입탐지에

이전트들을 관리하는 중앙통제 시스템의 설계에 대해서 논한다. 또한, 본 논문에서 설명하는 침입탐지시스템은 다른 종류의 침입탐지 에이전트들의 추가와 연동을 지원하는 확장성과 에이전트가 설치된 환경의 특성에 따라 적절한 규칙 항목들을 적용하여 침입에 대처할 수 있는 규칙 항목 설정의 유연성을 보장한다.

본 논문에서는 본문 1절에서 현재 개발되고 있는 RT-HIDS(Real-Time Hybrid IDS)의 전체적인 구성을 설명하고 중앙관리 시스템의 세부적인 구조에 대해서 설명한다. 그리고, 2절에서는 시스템의 확장성과 유연성을 고려한 침입탐지에이전트 규칙 설정 정보의 구성 형태에 대해서 논하며 마지막에서는 향후 계획과 결론에 대해 기술한다.

II. 본문

1. RT-HIDS(Real-Time Hybrid IDS)의 설계

본 절에서는 앞서 간략히 언급한 RT-HIDS의 구성 요소에 대해서 설명한다. 그리고, RT-HIDS의 핵심 구성 요소인, 중앙통제 시스템(Multi-Agent Coordinator, MAC)의 내부 구조에 대해 기술한다.

1) RT-HIDS의 구성형태

RT-HIDS는 호스트 기반 침입탐지에이전트와 네트워크 기반 침입탐지에이전트를 통합 관리할 수 있는 하이브리드형 IDS이다.

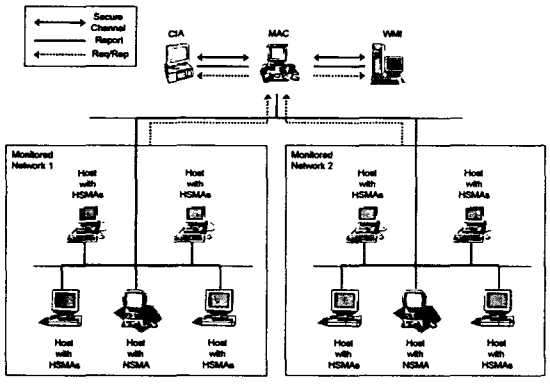

그림 1: RT-HIDS의 네트워크 구성도

[그림 1]은 RT-HIDS의 전체적인 구성을 도식화한 것이다. 각 구성요소들에 대하여 설명하면 다음과 같다.

가. MAC(Multi-Agent Coordinator)

MAC는 감시대상 네트워크에 분산 설치되어 있는 다수의 침입탐지에이전트들을 중앙에서 통합 관리를 수행하는 구성요소이다. MAC는 하위의 다양한 에이전트를 관리하며 한편으로, 이후 설명될 웹 기반 관리 인터페이스(Web-based Management Interface, WMI)에게 정보를 제공하거나 관리 요청을 처리한다.

나. CIA(Central Intrusion Analyzer)

CIA는 단일 지점에서 수집된 정보를 분석하여 침입을 탐지하는 기능을 수행하며, MAC을 통해서 에이전트로부터 보고된 보안관련 이벤트들을 통합 분석하는 상위 수준의 보안위반 분석 기능을 수행하는 구성요소이다. CIA는 다수의 에이전트에서 수집된 정보들을 통합 분석하여, 다중 협동 공격과 같이 단일 에이전트로는 탐지하지 못하는 한계를 극복한다.

다. NSMA(Network Security Monitoring Agent)

네트워크 침입탐지에이전트이며, 사전에 설정된 규칙에 기반하여 네트워크에서 발생하는 오용 행위를 탐지한다. 규칙에 정의된 침입위반 사건이나 통합 침입분석을 위한 부수적인 이벤트들을 MAC에게 보고하는 기능을 수행한다.

라. HSMAs(Host Security Monitoring Agents)

호스트 침입탐지에이전트를 지칭하며, 감시대상 네트워크에 존재하는 각 호스트에서 침입탐지를 수행한다. HSMA는 탐지동작 방식에 따라 몇 가지 종류로 분류되며, 로그분석 침입탐지에이전트, 사용자 행위 추적 침입탐지에이전트, 그리고 시스템 콜(sytem call)을 이용한 침입탐지에이전트 등이 존재한다.

마. WMI(Web-based Management Interface)

웹 기반 관리 인터페이스이며, Java 기술을 이용하여 구현되었다. 이를 통해서 인터넷에 연결되어 웹서비스를 이용할 수 있는 곳이면, 장소에 구애받지 않고 침입탐지시스템의 관리 동작 수행이 가능하며, 감시 대상 네트워크에 대한 감시 활동도 가능하다.

2) MAC의 세부 구조

MAC은 앞서 설명한 바와 같이 이종의 침입탐지에이전트를 중앙에서 관리하는 핵심 구성요소이다. 이는 에이전트로부터 발생한 침입탐지 정보를 WMI에 보고하거나, WMI로부터의 요구 메시지를

처리하며, 에이전트로부터 수신한 이벤트 정보를 수집, 통합하여 CIA에게 전달, 단일 에이전트가 탐지하지 못하는 침입을 탐지 할 수 있도록 하는 기능을 수행한다. [그림 2]는 MAC의 전체 구성과 서브시스템의 관계를 보이고 있다.

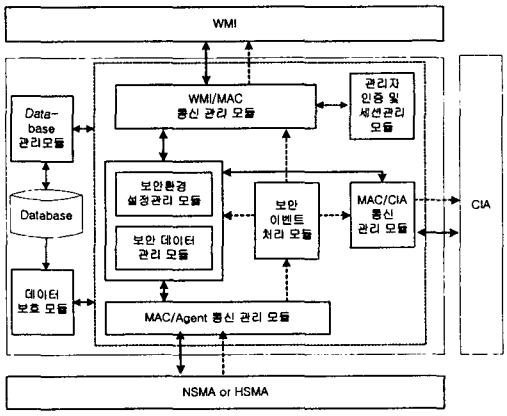

그림 2: MAC의 구성과 서브시스템과의 관계

가. 관리자 인증 및 세션관리 모듈

WMI를 통하여 MAC에 접근을 시도하는 사용자에 대한 식별 및 인증을 수행하고, 인증된 사용자의 연결세션 관리를 수행한다.

나. WMI/MAC 통신관리 모듈

WMI와 MAC 사이에 연결되는 채널을 관리하고, 정보의 교환을 위한 메시지 송수신 기능을 제공한다.

다. 보안환경 설정관리 모듈

침입탐지시스템 운용을 위하여 필요한 보안환경 구성정보를 관리하고, 다수의 에이전트들을 통합관리하기 위해 요구되는 보안항목들에 대한 관리 기능을 제공한다.

라. 보안데이터 관리 모듈

침입탐지시스템을 운영할 때 생성되는 보안관련 정보들을 관리하는 기능을 제공한다. 그러한 정보로는 시스템 감사 정보, 보안 이벤트 정보, 통계 정보 등이 존재한다.

마. 보안이벤트 처리 모듈

이종의 에이전트로부터 발생하는 보안관련 이벤트를 감사 정보와 침입정보에 대한 로그 정보를 기록하고, 관리자에게 통보하는 기능을 제공한다.

바. MAC/Agent 통신관리 모듈

MAC/Agent 사이에 정보 교환을 위하여 요구되는 채널의 생성과 메시지 처리 기능을 제공한다.

사. 데이터 보호 모듈

MAC과 다른 서브시스템들 사이에 형성되는 통신 채널의 기밀성 보장을 위한 암호화 기능과 변조 방지를 위한 데이터 인증 기능을 제공한다.

아. Database 관리 모듈

MAC과 시스템 데이터베이스 사이에 트랜잭션을 처리한다.

2. 보안 규칙 관리 구조 설계

1) 일반적인 규칙 설정 구조

일반적인 규칙 기반 침입탐지시스템의 규칙 설정 형태는 [표 1]과 같다. 가령, 네트워크 기반 침입탐지에이전트(NIDA)와 호스트 기반 침입탐지에이전트(HIDA)의 규칙 정보를 중앙에서 관리하는 시스템이라면, 규칙 설정 정보는 두 개의 에이전트 타입(NIDA과 HIDA)이 정적으로 정의되고 에이전트가 설치된 호스트마다 각각 하나의 규칙 집합이 정의된 평면적인 테이블 형태로 구성된다.

표 1: 일반적인 침입탐지시스템의 규칙 구성 형태

NIDA	*NIDA Instance 1*	*Rule Set 1*
	NIDA Instance 2	*Rule Set 2*
	NIDA Instance 3	*Rule Set 3*
HIDA	*HIDA Instance 1*	*Rule Set 1*
	HIDA Instance 2	*Rule Set 2*

이러한 구조는 다음과 같은 문제점을 가지고 있다. 첫째, 새로운 타입의 에이전트가 추가되어 연동 및 관리되어야 할 경우, 확장성을 제공하지 못한다는 점이다. 가령 새로운 타입의 HIDA를 기존에 동작하던 침입탐지시스템에 추가하여 운용하려 할 경우, 일반적인 침입탐지시스템은 운용중인 침입탐지시스템을 재구성을 하여야만 새로운 HIDA의 추가 운용이 가능하다. 둘째로는 설치한 에이전트의 운용 환경이 변화하는 경우, 새로운 환경에 맞는 규칙 정보들을 적용시키기 위해 새로운 규칙 집합을 적용하기가 어렵다는 문제점이다. 일반적인 침입탐지시스템은 에이전트를 설치하여 운용할 경우 에이전트와 대응되는 하나의 규칙 집합을 구성하고 이를 통하여 단일 규칙 항목 단위로 규칙 집합을 관리한다. 즉, 운용하고 있는 에이전트에 대하여 규칙 집합 단위로 규칙들을 적용할

수 있는 방법을 제시하지 않았다는 점이다.

2) RT-HIDS 시스템의 보안규칙 정보 구조

위에서 언급한 두 가지 주요한 단점을 보완하기 위하여 RT-HIDS에서는 [그림 3]과 같이 규칙 설정 정보를 3차원 형태의 구조로 설계하였다.

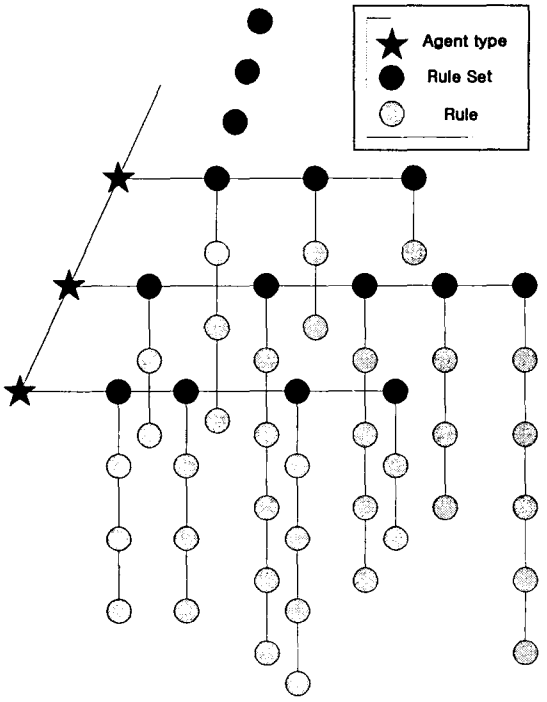

그림 3: 보안규칙 데이터베이스의 논리적 구조

[그림 3]에서 에이전트 타입 노드(★)는 하나의 에이전트 타입을 의미하며 이 노드가 가지고 있어야할 정보는 [표 2]와 같다.

표 2: 에이전트 타입 노드의 구성 요소

Name	Description
Agent type	특정 에이전트 타입의 규칙 정보라는 것을 나타낸다.
Original rule set	새로운 정책을 부여 시에 기본적으로 구성되어야 할 규칙 정보를 유지하고 있다.
Global rule set	특정 에이전트 타입의 규칙 집단을 구성하는 데 있어 각 규칙 집단의 super set에 해당이 되는 규칙 정보들을 관리한다.

규칙 집합 노드(●)는 각 에이전트에 적용할 수 있는 규칙 집합을 의미하며 이에 포함되어야 할 정보는 [표 3]과 같다.

표 3: 규칙 집단 노드의 구성 정보

Name	Description
Rule_Set_ID	규칙 항목 집단의 식별자
Applied AGT ID	현재 규칙 항목 집단이 적용된 에이전트의 식별자

규칙 노드(○)는 규칙 집단 노드에 설정되어 있는 단일 규칙 정보를 의미한다. 이 노드에 설정되는 정보들은 어떤 침입 유형인가에 따라 다른 설정 정보들이 포함된다. 포함되는 정보는 [표 4]와 같다.

표 4: 단일 규칙 노드의 구성 정보

Name	Description
Rule_ID	규칙 항목의 식별자
Rule_Category	규칙 항목의 침입 유형
Rule_Info	유형별 규칙 항목 설정 정보. 예를 들어 서비스 거부 공격인 경우 특정 포트의 단위 시간 당 최대 연결 수를 나타내는 정보가 설정 정보로 입력된다.

이러한 규칙 정보 구성 형태는 새로운 에이전트 추가 시 [그림 3]의 에이전트 타입 노드를 추가하는 형태로 쉽게 시스템을 확장할 수 있다. 그리고 각 에이전트 타입에 따라 규칙 집합 노드인 규칙 집합을 추가하여 에이전트가 설치된 여러 환경에 따라 그 환경에 최적인 규칙 집단을 적용하는 형태로 에이전트의 규칙 정보들을 유연성 있게 적용할 수 있다.

III. 결론 및 향후 계획

규칙 기반의 이종의 에이전트들을 관리하기 위한 중앙통제 시스템은 에이전트의 종류나 설치된 호스트 수와는 상관없이 각각의 호스트에 설치된 에이전트들의 규칙 정보들을 효율적으로 관리하기 위한 구조를 가져야 한다. 그러한 점을 고려하여 논문에서 좀 더 유연성 있는 규칙 설정 형태를 제안하였다. 앞으로의 계획은 현재 설계한 시스템의 구현을 완료하고 확장된 구조를 가지기 위해서 CIA를 중점적으로 설계하여 에이전트들로부터 보

고된 정보를 이용하여 새로운 패턴의 침입 정보들을 정의하고 이를 탐지 할 수 있는 서브시스템을 추가적으로 설계 및 구현할 것이다.

참고문헌

[1] Dorothy E. Denning, "An Intrusion Detection Model," *IEEE Transactions on Software Engineering,* Vol. SE-13, No. 2, pp.222-232, February 1987.

[2] Teresa F. Lunt, "Automated Audit Trail Analysis and Intrusion Detection," *Proceedings of the 11th National Computer Security Conference,* October 1988.

[3] L. T. Heberlin, "A Network Security Monitor," *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy,* Oakland, CA, pp.296-304, May 1990.

[4] S. R. Snapp, et el, "DIDS (Distributed Intrusion Detection System) Motivation, Architecture, and An Early Prototype," *Proceedings of the Fifteen National Computer Security Conference,* Baltimore, MD, October 1992.

[5] Porras, A. and Neumann, P. G., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," *In Proceedings of the National Information Systems Security Conference,* October 1997.

[6] Jhon E. Canavan, "Fundamentals of Network Security," Artech House Publishers. 2000.

[7] Herve Debar, Marc Dacier and Andres Wespi, "Towards a Taxonomy of Intrusion-Detection Systems", *Research Report of IBM Research Division, Zurich Research Laboratory,* Jen. 1998.

[5] Paul Proctor, "Audit reduction and misuse detection in heterogeneous environments: Framework and applications," *In Proceedings of the 10th Annual Computer Security Applications Conference,* pp.117-125, December 1994.