제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

통합 침입 관리 시스템의 침입탐지 정보형식과 전송방법

김성철, 김영호, 원용관
전남대학교 컴퓨터공학과
e-mail : sckim@grace.chonnam.ac.kr

Format of intrusion detection information and transmission method of Integrated Intrusion Management System

Seong-cheoll Kim, Young-ho Kim, Yong-gwan Won
Dept. of Computer Engineering, Chonnam University

요 약

네트워크 발달로 컴퓨터 시스템에 대한 접근이 용이해 지면서 호기심 또는 악의로 시스템을 침입 및 파괴하려는 다양한 형태의 침입 행위가 날로 증가하고 있다. 이러한 침입에 대비하여 대상 시스템에 대한 비 인가된 행위를 탐지 및 구별하고 이에 대응하는 기능을 가진 침입 탐지 시스템(IDS: Intrusion Detection System)에 대한 연구가 폭 넓게 진행 되어 왔으며, 다양한 형태의 IDS 들이 컴퓨터 및 네트워크 시스템에 적용되고 있다. 그러나 일반적인 IDS 는 단일 시스템에 대한 침입을 탐지하고 방어하는 것에 그 목적이 있으므로, 하나의 단위 네트워크 시스템을 효과적으로 보호하기 위해서는 단일 시스템에 대한 침입정보를 신속하게 상호 공유할 필요가 있다. 따라서 개별 Host 나 Network 장비에 분산되어 동작하는 다중의 IDS 에 대해서 통합 관리를 수행하는 통합 침입 관리시스템이 요구 되어진다. 본 논문에서 제안하는 시스템은 각 IDS 들이 침입을 탐지하는 순간 이에 대한 정보를 수집하여 다른 IDS 들에게 침입에 대한 정보를 신속하게 전달하고, 정보의 종류와 수행 기능에 따른 요구사항을 프로토콜에 적절하게 반영 할 수 있는 시스템을 제안한다.

1. 서론

침입(Intrusion)은 컴퓨터가 사용하는 자원에 대하여 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availa-bility)을 저해하는 일련의 행위와, Computer System 의 보안정책을 파괴하는 행위를 말한다[3]. 이러한 침입에 대한 대비책으로 일반적으로 사용하고 있는 것이 방화벽(Firewall)과 IDS(Intrusion Detection System)이다. 하지만 IT 기술의 발전과 함께 해킹기술 또한 발전하고 있으며 이러한 방화벽과 IDS 만으로는 해커의 침입을 차단하는 것에는 한계가 있다. 방화벽은 외부침입에 대한 차단에만 충실할 뿐 내부의 침입에 대해서는 무방비 상태이다[1-2].

IDS 는 방화벽과 함께 활용되는 보안솔루션으로 사용자의 행위를 감시하여 침입을 탐지하는 시스템이다. IDS 는 방화벽과 같이 단순히 네트워크를 통한 외부 침입을 차단하는 단계를 넘어 외부 침입에 의해 방화벽이 해킹 된 후 침입 사실을 탐지해 이에 대응하기 위한 보안 솔루션이다. 또한, IDS 는 해킹수법을 이미 자체적으로 내장, 침입 행동들을 실시간으로 감지, 제어할 수 있는 기능을 제공한다[1-2].

이러한 IDS 는 각 개별 Host 나 네트워크 장비에 분산되어 동작한다. 그러나, 그룹 단위의 Host 나 네트워크 단위의 시스템을 보호하기 위해서는 하나의 시스템에 대한 침입 발생 정보를 신속하게 공유 해야만 한다. 따라서, 각 IDS 들이 침입을 탐지하는 순간 침입 정보를 모든 IDS 들에게 전달하기 위해서는 분산되어 있는 IDS 들을 통합 관리할 필요가 있다[3-4].

현재 분산되어 있는 IDS 들을 통합 하기 위한 연구가 지속적으로 진행되어 오고 있다. SCYLLARUS[4]는 다중의 침입 탐지 시스템으로부터 보고되는 report

를 통합하는 기능을 제공한다. 아직은 prototype 형태이며 완벽한 테스트를 거치지 못했다.

통합된 탐지 전략을 세우기 위해서는 침입탐지기법의 확장 및 서로 다른 방식으로 얻어지는 정보들에 대한 통합이 요구되며, 이에 따른 고 수준의 통신 프로토콜에 대한 정의가 필요하다. 이러한 일련의 작업들을 IETF(Internet Engineering Task Force)내의 IDWG(Intrusion Detection Working Group)에서 수행하고 있다. IDWG 은 침입탐지 시스템에 대한 요구사항 기술과 공통 언어정의, 그리고 침입탐지시스템에서의 통신 프로토콜과 데이터 포맷을 표준화하기 위해 노력하고 있으며 발표된 RFC 는 없고 세 개의 Internet-Draft 가 있다[6-7].

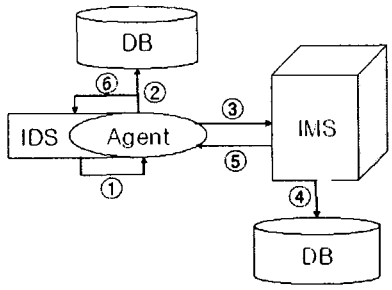
본 논문에서는 분산되어 있는 각 개별 IDS 들을 효과적으로 통합하여 관리하기 위한 시스템을 제안한다. 제안하는 시스템인 통합 침입 관리 시스템(IIMS: Integrated Intrusion Management System)은 각 개별 IDS 에서 발생된 침입 정보를 수집하고 이를 다른 IDS 에게 중계하는 기능을 수행하며, 각종 정보를 저장 및 분석하여 침입 관리 기능을 수행한다. IIMS 는 IDS 에 탑재되는 Management Agent 와 통합 관리의 주요 기능을 수행하는 IMS (Intrusion Management System)로 이루어 진다. 또한 분산되어 있는 각 개별 IDS 들의 통합 관리를 위해 IDWG 에서 제안한 Internet-Draft 인 IDMEF(Intrusion Detection Message Exchange Format)에 따라 IDS 와 통합관리 시스템간의 데이터 포맷을 결정한다. 또한 IDS 와 IMS 간의 통신은 메시지의 종류와 기능에 따라 각기 다른 요구사항이 발생한다. 이러한 요구사항을 프로토콜에 적절하게 반영할 수 있는 통신 모델을 제안한다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 제안된 통합 침입 관리 시스템(IIMS: Integrated Intrusion Management System)의 구조와 IDS 시스템이 갖는 Management Agent 와 IMS(Intrusion Management System)의 각 component 들의 기능과 구조에 대해서 다룬다. 제 3 장에서는 Management Agent 와 IMS 간의 통신 방법에 대해서 살펴보고, 제 4 장에서는 본 연구에 대한 결론을 맺고 향후 연구방향을 살펴본다.

2. 통합 침입 관리 시스템(IIMS)의 구조

개별 Host 나 네트워크 장비에 분산되어 동작하는 IDS 는 그룹단위의 Host 나 네트워크 단위의 시스템을 보호 하는 데에는 한계가 있다. 이러한 한계를 극복하기 위해서는 분산되어 동작하는 IDSs 를 통합하여 관리하여야 한다. 이러한 통합 침입 관리 시스템은 분산되어 동작하는 IDSs 로부터 각종정보를 수집하고, 이를 저장 및 분석하여 IDSs 에게 침입을 통보하는 역할을 수행 하여야 한다.

본 논문에서는 이러한 기능을 수행하는 Agent-Manager 구조의 통합 침입 관리 시스템(IIMS: Integrated Intrusion Management System)을 제안한다. IIMS 는 IDS 와 침입 관리 시스템(IMS: Intrusion Management System)간의 매개체 역할을 수행하는 Management Agent 와 IIMS 의 관리자 역할을 수행하는



<그림 1> IIMS 의 구조도

IMS 로 구성된다. <그림 1>은 IIMS 의 전체적인 구조를 보여주고 있다.

Host 에 침입이 발생하게 되면 IDS 는 intrusion alert 를 발생하고 Management Agent 에 이를 통보(①)한다. Management Agent 는 침입 정보를 Database 에 저장(②)함과 동시에 intrusion report 를 IMS 에 전송(③)한다. IMS 는 Management Agent 로부터 전송 받은 intrusion report 를 Database 에 저장(④)하며, 동시에 이를 분석한다. 분석된 결과에 따라 필요한 경우에 해당 침입 정보를 관리 대상에 포함되어 있는 모든 Management Agent 에게 통보(⑤)한다. IMS 로부터 Management Agent 에 전송된 침입 정보는 Management Agent 의 Database 에 저장하고 IDS 에 통보(⑥)하여 침입의 대응에 이용하게 된다. 이러한 과정에 의하여 하나의 단위네트워크상의 컴퓨터 및 통신망의 자원을 효율적으로 보호할 수 있게 된다.

2.1 Management Agent

Management Agent 는 IDS 와 IMS 간의 매개체 역할을 수행하며 IMS 의 정보요구에 응답한다. Management Agent 의 기능은 IDS 로부터 정보를 수집하는 기능과 수집된 정보를 관리하는 기능, 그리고 IMS 로 정보를 전송하는 기능으로 크게 나뉘어 진다. 이러한 기능을 수행하기 위하여 Management Agent 는 5 개의 component 를 가지고 있다.

- Interface Component
- Agent Analysis Component
- Management Agent DB
- Trap Process Component
- Agent Communication Component

각 component 는 다음과 같이 구성된다. 먼저, IDS 로부터 정보를 수집하기 위해서 IDS 와 Management Agent 간의 Interface Component 가 요구되며, 수집된 정보에 대해서 일반적인 상태정보와 intrusion alert 의 분석을 위해서는 Agent Analysis Component 가, 수집된 정보에 대한 저장 및 관리 역할을 수행하는 Management Agent DB 가 요구된다. 침입에 대해서 IMS 에 정보를 전송하기 위해서는 침입 정보를 처리하는 Trap Process Component, 그리고 IMS 와 Management Agent 간의 통신을 수행할 수 있는 Agent

Communication Component 가 요구된다.

2.2 IMS

IMS(Intrusion Management System)는 분산되어 있는 IDSs 의 통합 관리를 통하여 단위 네트워크상의 같은 침입에 대한 피해를 막는 역할을 수행한다. IMS 의 기능은 정보의 수집, 정보의 중계, 정보의 저장 및 관리 세가지로 나눌 수 있으며 이러한 기능을 수행하기 위하여 IMS 는 5 개의 Component 를 가지고 있다.

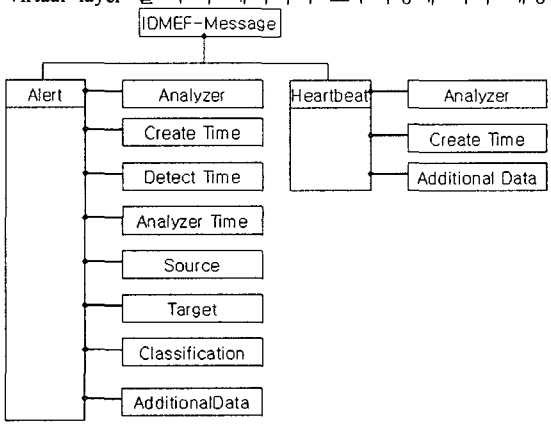
- IMS Analysis Component
- User Interface Component
- Intrusion Distribution Component
- IMS Communication Component
- IMS DB

Management Agent 의 report 는 IMS Communication Component 를 통하여 IMS 에게 전달 되어진다. 이 report 는 IMS Analysis Component 에 의해 분석과정을 거치게 된다. report 는 intrusion report 와 주기적으로 보고되는 각 Host 에 대한 상태 report, IMS 의 요청에 대한 응답으로 나누어 진다. intrusion report 인 경우 User Interface Component 를 통하여 관리자에게 전달하는 동시에 Intrusion Distribution Component 에 통보한다. Intrusion Distribution Component 는 IMS Analysis Component 에서 전달된 intrusion report 를 IMS DB 에 저장하고 각 Management Agent 들에게 intrusion 정보를 전송한다. 주기적으로 보고되는 각 Host 에 대한 상태 report 는 IMS DB 에 저장되며 관리자의 필요나 요구에 의해 User Interface Component 를 통하여 관리자에게 presentation 하게 된다. 관리자가 각 Host 의 정보를 요청할 경우 IMS Analysis Component 는 먼저 해당 정보를 IMS DB 검색하고 해당 정보가 없을 경우에는 Management Agent 에 정보를 요청한다. 요청한 정보에 대한 응답은 IMS Analysis Component 에서 분석 과정을 거친 후 User Interface Component 를 통하여 관리자에게 presentation 한다.

3. Management Agent 와 IMS 간 통신

침입 탐지 시스템의 통합을 위해서는 IDSs 와 관리 시스템간에 교환되는 정보의 모델링이 필요하다. 침입 탐지 시스템의 통합을 위하여 IETF(Internet Engineering Task Force)내의 IDWG(Intrusion Detection Working Group)에서 침입 탐지 시스템의 로그형식에 대한 표준을 Internet-Draft 로 공고한 IDMEF(Intrusion Detection Message Exchange Format)[8-9]가 있으며 <그림 2>는 전체 로그개관을 보여준다. 이러한 침입 탐지에 대한 로그형식을 기반으로 하여 Management Agent 와 IMS 간에 교환되는 정보에 대한 모델링을 수행 하였다.

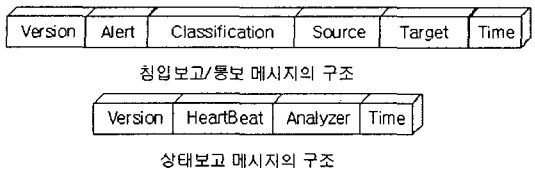
Management Agent 와 IMS 간에 교환되는 메시지는 정보의 종류와 수행기능에 따라 상이한 요구사항을 가지고 있다. 이러한 요구사항을 protocol 에 적절하게 반영하기 위해서는 전송메시지의 요구사항에 맞는 protocol 을 사용할 수 있는 Multiple protocol 이 필요하다. 본 논문에서는 Multiple protocol 을 위해 TCP/IP protocol 의 계층구조에서 응용계층과 전송계층 사이에 Virtual layer 을 두어 메시지의 요구사항에 따라 해당 protocol 을 선택할 수 있게 하였다[7].



<그림 2> 침입 탐지 시스템의 로그형식 표준

3.1 Management Agent 와 IMS 간 메시지 Format

Management Agent 와 IMS 간의 교환되는 정보는 Management Agent 에서 IMS 로 보고되는 report 와 IMS 에서 Management Agent 로 전송되는 message 로 나뉜다. report 는 침입보고, 상태보고, IMS 의 request 에 대한 response 가 있고, message 는 침입통보와 추가 정보 요구와 같은 request 가 있다. Management Agent 와 IMS 간의 교환되는 정보를 <그림 3>과 같이 정의하였다.



<그림 3> 메시지의 구조

· 침입보고/통보 메시지의 구조
Version: 메시지의 현재 버전
Alert: 분석기가 검출한 경고에 관한 정보
Classification: alert 의 이름과 alert 에 관한 정보
Source: alert 을 만드는 이벤트의 원천에 관한 정보
Target: 이벤트의 목표
Time: 메시지의 생성시간과 alert 탐지 시간

· 상태보고 메시지의 구조
Version: 메시지의 현재 버전
HeartBeat: 상태정보를 위한 식별 id 로 구성
Analyzer: 분석기의 정보
Time: 메시지의 생성시간

3.2 멀티 프로토콜을 위한 Virtual layer

Management Agent 와 IMS 간에 교환되는 각각의 정

보 item 들은 메시지의 유형과 기능에 따라 서로 상이한 요구사항들을 갖고 있다. 먼저, Management Agent 에서 IMS 로 보고되는 report 는 침입정보(일반적 침입, 침입), 상태보고, request 에 대한 response 가 있고, IMS 에서 Management Agent 로 전송되는 message 는 침입통보와 request 가 있다. 이러한 정보 item 들은 '신뢰성', '보안성'의 요구사항을 갖고 있으며 이를 <표 1> 에 정의 하였다.

Management Agent→IMS			IMS→Management Agent		
메시지	요구사항	Protocol	메시지	요구사항	Protocol
침입	신뢰성/ 보안성	TCP/ 암호화	침입통보	신뢰성/ 보안성	TCP/ 암호화
일반침입	신뢰성	TCP	request		UDP
상태보고		UDP			
Response		UDP			

<표 1> 메시지에 따른 protocol

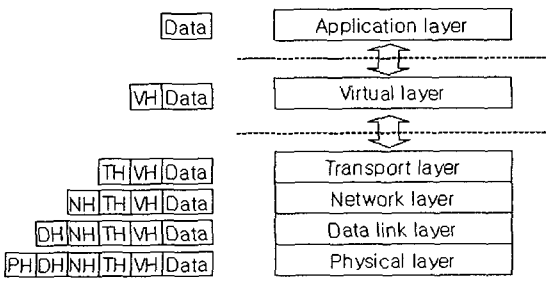
<표 1>에서 Management Agent 에서 IMS 로 보고되는 침입정보를 침입과 일반침입으로 분류하였다. 이는 Alert 메시지에 정의 되어있는 impact 에 따라 분류한 것이고 impact 의 유형은 <표 2>와 같다[6-7]. (impact 의 값: 4, 6, 11→ 침입, 그 이외의 impact→ 일반침입)

"TCP/암호화"는 송신측에서 header 를 제외한 메시지를 DES 를 통하여 암호화 하고 이를 수신측에서 복호화 하는 방식을 사용하였다.

값	키워드	값	키워드
0	Unknown	6	Successful-dos
1	Bad-unknown	7	Attempted-recon
2	Not-suspicious	8	Successful-recon-limited
3	attempted-admin	9	Successful-recon-largescale
4	Successful-admin	10	Attempted-user
5	Attempted-dos	11	Successful-user

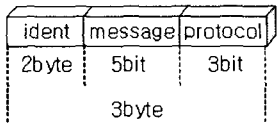
<표 2> impact 의 정의

전송하는 메시지의 유형에 따라 독립적인 protocol 을 사용하기 위하여 본 논문에서는 Virtual layer 를 통하여 multiple protocol 을 가능하게 하였다[5]. Virtual layer 의 구조는 <그림 4>와 같다.



<그림 4> Virtual layer

Virtual layer 은 Application layer 의 메시지에 header 를 첨가하여 Transport layer 에서 메시지에 따라 서로 다른 protocol 을 사용할 수 있게 한다. Virtual layer 의 header format 은 그림 5 와 같이 정의 된다.



<그림 5> Virtual layer 의 header format

□ Virtual layer 의 header format

ident: 식별 *id*, 2byte

message: 전송메시지의 형태(0~4), 5bit
0: Alert, 1: HeartBeat, 2: Distribution, 3: request, 4: response

protocol: 사용 protocol 의 type(0~2), 3bit
0: TCP, 1: UDP, 2: TCP/암호화

4. 결론

본 논문은 분산되어 수행되는 다중의 IDS 를 효과적으로 통합 관리할 수 있는 통합 침입 관리 시스템인 IIMS 를 제안하였다. IIMS 는 하나의 단위 네트워크나 그룹의 컴퓨터 시스템을 보호하기 위하여 침입에 대한 정보를 상호 공유함으로써 공격에 대한 피해를 최소화 할 수 있다. 또한 Management Agent 와 IMS 간 정보 교환시 정보의 종류와 수행기능에 따른 요구사항을 protocol 에 반영하여 통합 침입 관리 시스템의 안전하고 효율적인 정보의 수집 분배를 가능하게 한다. 향후 연구과제로는 통신망 관리 시스템과의 연계 및 다른 단위네트워크 상에 존재하는 IIMS 와의 연동을 통하여 보다 확장된 통합 탐지 시스템에 대한 연구가 필요하다.

참고문헌

[1] *D. Denning.* "An Intrusion Detection Model", IEEE Trans. Softw. Eng.,13(2), Feb. 1987

[2] *B. Mukherjee, L. Heberlein, and K. N. Levitt.* "Network Intrusion Detection." IEEE Network, pages 26-41, May/June 1994

[3] Robert P. Goldman, Walter Heimerdinger, Steven A. Harp, Christopher W. Geib, Vicraj Thomas, Robert L. Carter "Information Modeling for Intrusion Report Aggregation" Proceedings of the DARPA Information Survivability Conference and Exposition, June 2001, p. 329-342

[4] 박정호 "SNMP 기반의 통합침입관리시스템(IMS)의 정보모델과 설계 및 구현" 전남대학교 컴퓨터공학과 석사학위논문 2001.

[5] Behrouz A. Forouzan, "TCP/IP 프로토콜" 미래컴 2000.8.28

[6] IETF Internet Draft (2000), Intrusion Detection Exchange Format Data Model

[7] IETF Internet Draft(1999), Intrusion Detection Exchange Format Requirements