제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

보안네트워크 프레임워크에서 이기종의 침입 탐지 시스템 연동을 위한 경보데이터 처리

박상길*, 김진오*, 장종수*
*한국전자통신 연구원 정보보호 연구본부
e-mail : wideideal@etri.re.kr

Alert Data Processing for heterogeneous Intrusion Detection Systems in Secure Network Framework

Sang-Kil Park*, Jin-Oh Kim*, Jong-Soo Jang*
*Electronic and Telecommunication Research Institute

요 약

네트웍을 이용한 외부의 침입을 탐지하기위해 침입탐지시스템이 1980 년대부터 연구되었다. 침입탐지 시스템은 침입을 발견하면 경보데이터나 로그데이터를 생성하는데, 서로 상이한 데이터 집합으로 인해 별도의 데이터 매핑이 필요한 문제점을 해결하고자 IETF 의 침입탐지 관련 그룹인 IDWG 에서 IDMEF 를 제안하였다. 본 논문에서는 이러한 IDMEF 형식을 지원하는 경보데이터 구조를 설계하고, 이를 통하여 상위의 보안제어서버에서 상이한 침입탐지 시스템으로부터의 경보데이터를 저장, 관리할 수 있는 방법을 제공한다. 이러한 기본적인 경보데이터 관리 이외에 저장된 경보데이터를 통한 공격자 정보 추출, 피해 호스트 정보 추출등의 부가적인 방법 또한 제공한다.

1. 서론

인터넷을 이용한 유요한 정보의 제공과 멀티미디어의 활용으로 인해 인터넷에 대한 관심이 증대되는 반면, 이를 악용하여 허가없이 타인의 정보를 추출, 변조하거나 경쟁상대의 서비스제공을 방해하는 등의 공격이 증대되고 있다. 또한 불특정 다수를 대상으로한 블라인드 공격또한 증대되고 있는 실정이다. 전세계의 인터넷을 운영하는 핵심체인 ICANN(Internet Corporation for Assigned Names and Numbers)측의 발표에 의하면 2002 년 10 월 22 일 전세계의 인터넷 트래픽을 관리하는 중앙 DNS 서버에 대한 다량의 분산서비스 거부 공격으로 인해 13 대 중 7 대의 서버가 다운되었다. 관리자의 적극적인 빠른 대응으로 인해 DNS 서버가 복구되어 인터넷의 이용에 극심한 불편을 초래하지는 않았지만, 인터넷에 대한 공격이 얼마나 심각한 결과를 초래하는지 보여주는 사건이었다. 또한 2003 년 1 월 25 일에는 Slammer 웜을 통한 불특정 다수로의 서비스 거부공격과 동일한 결과를 갖는 웜이 활동하였다. 네트워크나 호스트에 위치하는 이러한 공격을 탐지하고 관리자에게 현재의 공격상태, 위협도, 대응방안에 대한 정보를 경보메시지 또는 Alarm 을 통하여 전달한다. 이러한 메시지의 내용은 유사하지만, 침입탐지 시스템마다 상이한 형식을 이용함으로 인해 통합보안시스템이나 다수의 침입탐지 시스템을 운용하기 위해서는 이러한 경보데이터의 표준이 필요로 하게 되었다.

2. 경보데이터 처리를 위한 표준화

2.1 CIDF(Common Intrusion Detection Framework)

1980 년 Denning 의 침입탐지 시스템의 정의와 함께 침입탐지 시스템은 꾸준히 개발되고 있다. 1998 년 SRI, UC Davis 등에서 침입탐지 시스템을 복잡한 대규모의 네트워크 환경에 적용하도록 침입탐지시스템 설계와 구현을 위한 방법으로서 CIDF 가 논의되었다. CIDF 는 상호 협력하는 침입탐지 및 대응 시스템 들에 대한 프레임워크를 설계하기 위해 필요한 기능 블록들을 제시하며, 대규모 네트워크 환경에서 침입에 적절한 대응을 취하기 위해 이종의 침입탐지 시스템

이 정보를 교류하고, 이러한 정보를 이용하여 침입탐지 및 대응을 효율적으로 하기 위한 침입과 관련된 정보를 표현하기 위한 프레임워크로서 이용된다.

2.2 IDWG(Intrusion Detection Working Group)

미국방성(DoD)의 DARPA 에서 추진한 과제를 통해 CIDF 가 침입탐지 시스템간의 데이터를 교환하고자 하는 행동은 IETF 의 IDWG 로 이관되었고, IDMEF(Intrusion Detection Message Exchange Format)등의 draft 가 논의되어 현재 rfc 로 추진중이다. 이들 연구는 이종의 침입탐지 시스템들이 서로 상호 동작하도록 목적을 가지고 있으며, 침입탐지 시스템을 구성하는 요소들이 지닐 수 있는 가능한 모든 역할을 블록별로 정의하고 있다. IDWG 에서는 이와 더불어 침입탐지 엔진이 관리자에게 전달하는 경보메시지에 대해 XML 등을 이용한 침입탐지 관련 정보의 암호화등을 제공한다. 이러한 제안에 대하여 현재 IDMEF 에 관련된 library 가 구현되어 제공되고 있고, IAP(Intrusion Alert Protocol), IDXP(Intrusion Detection exchange Protocol)등의 프로토콜을 적용한 시스템이 구현되고 있다.

2.2.1 IDMEF 를 이용한 Alert 표현

IDWG 는 침입탐지 시스템간에 주고받는 경보데이터에 대한 요구사항을 발표했으며, 이를 구현하기 위한 XML 규약을 정한 "IDMEF Data Model and XML" 문서의 데이터 모델로서 Alert Class, 이를 상속하는 ToolAlert, CorrelationAlert, Overflowalert 클래스 가 모델링되었다. 또한, Analyzer 의 동작상태를 확인하기 위해 Heartbeat Class 필드를 통해 침입탐지시스템이 동작중인지 확인한다.

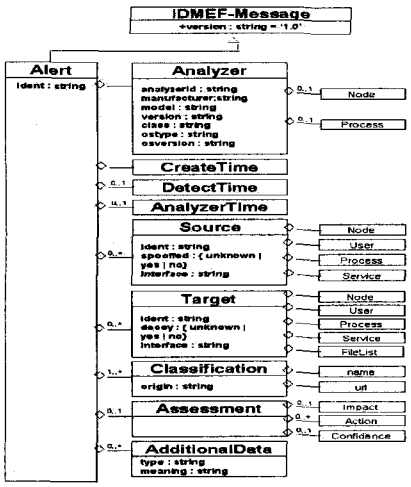

그림 1 IDMEF 의 Alert core Class

위 그림은 IDMEF 중 Alert 에 관해 설명하는 핵심 클래스를 UML Diagram 으로 표현한 것이다.

3. 경보데이터 관리 프레임워크

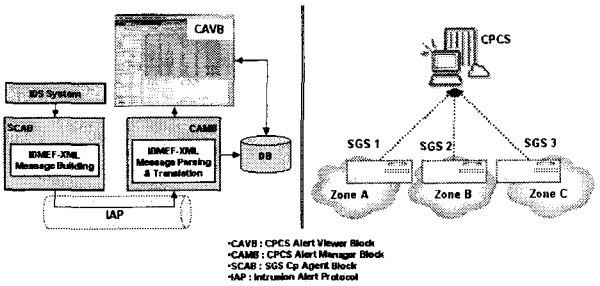

그림 2 경보데이터 처리 흐름과 경보데이터관리 프레임워크

침입탐지 시스템의 경보데이터를 중심으로 구현된 프레임워크를 살펴보면 다음과 같다. 전체적인 프레임워크는 중앙의 보안제어서버와 관리되는 복수개의 네트워크기반 침입탐지시스템으로 구성된다. 침입탐지시스템은 외부로부터의 침입이 발생되면 IETF 의 IDWG 에서 제안한 IAP 를 통하여 IDMEF 형식의 경보데이터를 보안제어서버의 경보관리모듈로 전송하며, 경보관리 모듈은 이를 저장/가공하여 침입자를 선별한다. 침입탐지 시스템의 경우 Signature(룰 파일)을 보면 카테고리화가 가능하도록 구분되는 Signature ID 를 갖는다. 경보데이터를 소스 데이터로 침입에 관련된 정보를 생성/관리하는 관리자는 서로 상이한 Signature ID 를 수신하게 되면, 이를 동일한 규칙을 갖도록 Mapping 하여야만 한다. 이 논문에서 사용한 프레임워크에서는 이러한 Signature 를 각각의 침입탐지 시스템이 사전에 각각의 시스템에 가지고 시작하는 것이 아니라, 중앙의 CPCS 를 통하여 카테고리화 된 signature 를 수신하여 각 시스템에 적용시킨다. 사전에 카테고리화 되어 있기 때문에 경보데이터를 수신하여 다시 한번 Mapping 하는 별도의 작업을 대신하게 된다. 또한 원격지에 SGS 가 존재하므로 시스템의 시간 동기화 및 침입탐지 엔진의 연관성 분석의 정확성을 제공하기 위하여 NTP(Network Time Protocol)을 설치하여 시스템의 시간 동기화를 제공하였다.

3.1 경보데이터 생성

침입으로 판명된 트래픽에 대하여 침입탐지 시스템은 침입과 관련된 정보를 경보데이터를 생성한다. 이렇게 생성된 경보데이터는 침입탐지 시스템에 따라 상이한 형식을 갖게 된다. SCAB 는 이러한 경보데이터를 libidmef library 를 수정한 Ladon-idmef 를 이용하여 경보데이터 관리 프레임워크에서 적용한 경보메시지를 생성한다. 이렇게 생성된 경보메시지는 IAP 프로토콜을 이용하여 CPCS 의 CAMB 에 전달된다.

3.2 경보데이터 처리

SPAB 가 IAP 프로토콜을 이용하여 CPCS 에 전달한 경보메시지는 CAMB 가 수신하여 IDWG 에서 정의 배포한 IDMEF 형식 준수여부를 IDMEF-message.dtd 와의 유효성 확인을 한다. 본 프레임워크를 테스트 베드 내

에서 적용하기 위해 CPCS 는 Tomcat 을 이용하여 web-server 역할을 수행하게 하였으며, 적절한 위치에 dtd 파일을 존재 한 후, XML 데이터를 생성하는 SCAB 가 경보데이터의 데이터에 dtd 가 존재하는 URI 를 삽입한다. 수신된 경보데이터가 오류가 없으면 데이터베이스에 XML 파일을 저장하고, 경보데이터 파싱 모듈로 전달한다.

경보데이터 파싱 모듈은 CPAB 를 Java 로 구현하였기에 XML 문서의 효율적인 파싱을 위해 JDOM package 를 이용한다. 수신된 경보데이터를 CPCS 의 CPAB 및 다른 블록에서 사용가능하도록 Alert 객체를 생성한다. 표 1 과 같이 생성된 Alert 객체는 큐를 이용하여 일정시간마다 데이터베이스에 저장하는 동시에 경보데이터를 기반으로 연관성 분석을 실행하는 모듈의 소스 데이터로서 공급한다.

표 1. CPAB 가 사용하는 Alert 객체

Alert 객체 필드	내 용	default
SGSID	경보데이터를 생성하는 SGS 의 ID	0
ATTACKID	MODELING 된 SIGNATURE ID	0
ATTACKTYPE	ATTACK 의 CATEGORY 화	0
DETECTDATE	침입 탐지 날짜	NULL
DETECTTIME	침입 탐지시간	NULL
SRCADDR	침입에 사용된 근원지 주소	NULL
SRCPORT	침입에 사용된 근원지 포트	0
PROTOCOL	침입에 사용된 프로토콜	0
TARGETADDR	침입에 적용된 목적지 주소	NULL
TARGETPORT	침입에 적용된 목적지 포트	0
SERVNAME	프로토콜이 TCP 일 경우 WELL-KNOWN NAME	NULL
ATTACKMSG	공격에 대한 정보제공 메시지	NULL
URL	공격에 대한 참조 URL	NULL
IMPACT	공격의 심각성	0
COMPLETION	공격의 성공여부	0
TYPE	공격의 종류	0
ACTCATEGORY	공격에 대한 ACTION 종류	0
CONFIDENCE	공격탐지에 대한 신뢰도	0
MANUFACTURER	탐지엔진의 제조회사	NULL
MODEL	탐지엔진의 모델명	NULL
VERSION	탐지엔진의 버전	NULL
OSTYPE	탐지엔진이 설치된 운영체제 종류	NULL
OSVERSION	탐지엔진이 설치된 운영체제 버전	NULL
CATEGORY	탐지엔진이 설치된 네트워크 종류	NULL
SGSLOCATION	SGS 의 설치 위치	NULL
SGSNAME	SGS 의 호스트 이름	NULL
SGSADDRESS	SGS 의 IP ADDRESS	NULL
SGSNETMASK	SGS 의 NETMASK	NULL

CPAB 는 변환된 Alert 객체를 프레임워크 관리 GUI (CAVB)에 전달한다. Alert 데이터와 부수적으로 생성되는 공격자정보, 연관성분석, 요주의 호스트정보, 경보데이터 분포 데이터를 Viewer 에 전달하여 사용자에게 출력한다.

3.3 경보데이터의 연관성 분석

공격 연관성 분석기능은 관리 도메인 내의 이벤트 간의 상호연관성 분석을 통해 침입 탐지율의 증가와 더불어 침입탐지 정확도의 증가를 목표로 하다. 이는 일반적인 침입탐지시스템에서 검출하지 못한 공격을 검출하는 것을 목표로 하며, 분산서비스 거부 유형의 공격을 검출한다. 이러한 공격은 네트워크의 유용성을 심각하게 떨어뜨리게 되는데 이러한 네트워크 차원의 공격탐지를 위해 7 개의 세분화된 카테고리를 통하여 연관성 분석 데이터를 생성한다.
이를 산출하는 근거로는 시간당 경보데이터의 발생수를 기준으로 검출한다. 예를 들어 60 초내에 60 개의 동일한 주소를 갖는 Alert 데이터가 발생하였다고 하면 이는 클래스 1 에 해당하는 연관성 분석 데이터를 생성한다.

표 2. 경보데이터의 연관성 분석 방법

분 류	분 류 방 법
카테고리 1	특정 소스가 특정 타겟에대해 특정 공격을 수행
카테고리 2	특정 소스가 특정 타겟에 대해 공격을 수행
카테고리 3	특정 타겟으로 특정 공격이 수행
카테고리 4	특정 소스가 특정 공격을 수행
카테고리 5	특정 소스가 공격을 수행
카테고리 6	특정 타겟으로 공격이 수행
카테고리 7	특정 공격이 수행

3.3 공격 정보 생성

데이터베이스에 저장되어 있는 경보데이터에 대하여 주기적으로 근원지 주소, 목적지주소, Impact(0)의 누적치, Impact(1)의 누적치, Impact(2)의 누적치, Impact(total)의 값을 미리 설정된 한계치와의 비교를 통하여 잠재적인 공격자와 잠재적인 피해호스트를 선별한다. 선별된 정보는 사용자에 의하여 요주의 호스트로 분류될 수 있으며, 이를 이용하여 적절한 대응까지 추진할 수 있다.

3.4 통계처리

일정주기마다 독립적인 Thread 로 운영되는 데몬에 의하여 경보테이블에 저장되어 있는 경보데이터에 대하여 총공격회수, 공격종류의 수, 10 분 단위의 최근 1 시간 공격회수, 침입탐지 시스템별 경보데이터 발생빈도, 프로토콜별 경보데이터 발생 빈도, 근원지 주소를 기반으로 가장 빈번한 Top5 공격자 호스트 주소 및 회수, 목적지 주소를 기반으로 가장 빈번한 피해호스트 주소 및 회수를 생성하여 테이블에 저장한다. 이렇게 저장된 데이터는 Viewer 를 통하여 주기별로 업데이트 되어 사용자로 하여금 현재 네트워크의 문제가 무엇이며, 관심을 가지고 관리하여야 할 네트워크 도메인이 무엇인지에 관한 정보를 제공한다.

3.5 Alert Viewer(CAVB)

경보데이터를 처리하는 보안제어서버의 경보데이터 처리 모듈로부터 생성되는 각종 데이터를 사용자에게 GUI 환경으로 제공하기 위한 기능 모듈이다.

Alert Viewer 는 침입탐지시스템에서 발생한 IDMEF

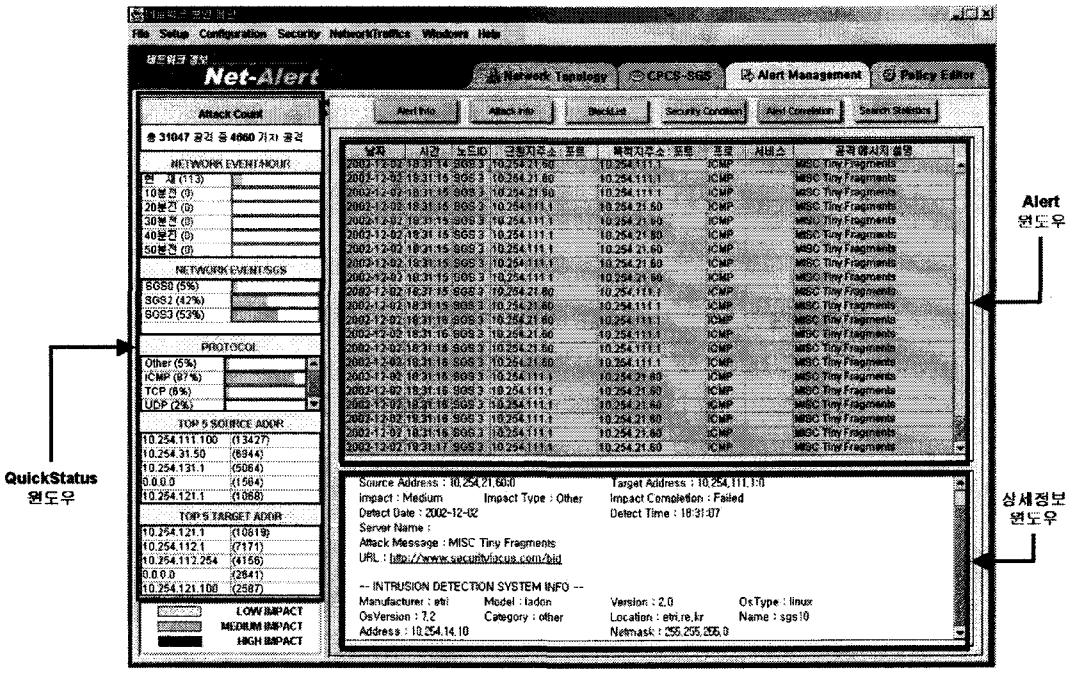

그림 3 Alert Viewer 의 전체적인 모습

형식의 경보데이터를 XML 문자열로 입력받은 후, 파싱하여 생성된 경보데이터를 경보데이터 판넬에 출력하다. 이는 경보데이터 Impact 의 값에 따라 미리 설정된 색으로 표현된다. 사용자가 하나의 경보데이터 레코드를 선택하면 그림 2 의 아래부분의 상세정보 윈도우처럼 <IDMEF Alert> 데이터로부터 정보를 추출하여 사용자에게 경보데이터의 세부사항을 보인다.

그림 3 의 좌측부분의 "QuickStatus 윈도우"는 일정주기마다 데이터베이스를 조회하여 서버의 경보데이터 관리모듈에 의해 생성되어 있는 경보데이터 통계값을 읽어서 화면에 진행바와 누적수의 형태로 표시하다. 이러한 "QuickStatus 윈도우를 통하여 사용자는 반복적으로 데이터베이스를 조회하지 않더라도, 현재의 네트워크의상황을 파악할 수 있으며, 이를 기반으로 통계처리하고자 하는 목표물을 좀 더 쉽게 파악할 수 있다.

4. 결론 및 향후계획

상이한 침입탐지 시스템에 대하여 운용성을 제공하기 위하여 설계/구현된 CAMB 는 Snort 와 Snort 기반으로 변형된 Signature 를 이용하는 침입탐지 시스템을 이용하여 프레임워크 상에서 구현 및 운용하였다..

경보데이터를 생성 및 파싱 하는 블록에 대하여 IDMEF 메시지 포맷에 있는 ToolAlert 과 Correlation Alert, OverflowAlert 객체를 지원하도록 수정하여야 할 필요가 있다. 현재 분당 1000 여개의 경보데이터를 처리할 수 있으나, 기가비트 침입탐지 시스템을 지원하기 위하여, Alert Suppression/Aggregation 을 통해 불필요한 경보데이터전송을 지양하고, 경보데이터 생성/수신/파싱에 대한 Throughput 을 높일 필요가 있다.

참고문헌

[1] 박상길, 장종수, 손승원, 노봉남, "안전한 네트워크 구성을 위한 정책기반 보안 프레임워크", 한국통신학회 논문지, 제 27 권 제 8C 호, pp.748~757, 2002 년 8 월.

[2] Sang-Kil Park, Jong-Soo Jang, Bong-Nam Noh, "A Design of Secure Network Framework using PBNM", in Proc. A*PNOMS2002*, pp. 523-524, Sept. 2002.

[3] 박상길, 김진오, 장종수, 노봉남, "IDMEF 를 지원하는 경보데이터 관리 모듈의 설계 및 구현", 제 6 회 차세대 통신소프트웨어 학술대회, pp.944~948, 2002 년 12 월

[4 S. Northcutt, M. Cooper, Fearnow, K. Fredrick, *Intrusion Signature and Analysis*. New Riders. 2001

[5 Edward G. Amorso, *Intrusion Detection : An Introduction Internet Surveillance, Correlation, Traps, Trrace Back and Response* . Intrusion.Net Books. 2001

[6] http://www.darpa.mil/ ITO 및 ISO 문서

[7] http://www.ietf.org/ IDWG draft 문서

[8] http://www.jdom.org/ JDOM 관련 Package