이기종간 침입탐지 정보에 대한 웹기반 관리 시스템 설계*

김은수** · 김석훈*** · 송정길****

요 약

최근 컴퓨터 네트워크의 발전에 따라 해킹사고도 급증하고 있으며 그 방법도 다양해지고 있다. 이러한 시기에 정보보호에 대한 관심이 높아지면서 많은 기업이 각종 보안시스템을 도입하고 있다. 그러나 해킹에 대응하기 위해서 대부분의 보안장비가 독자적인 이기종간의 기술을 적용해 제품간의 연동과 보안요소만으로 대처하기에는 많은 어려움이 있고, 이를 운용하는데 엄청난 조직, 장비, 인력 소요가 증대되고 있는 실정이다. 이러한 문제점을 해결하고자 이기종간 침입탐지 정보에 대한 보안요소를 통합하여 해킹으로부터 효율적으로 대응할 수 있는 웹 기반 관리 시스템을 설계 및 구현하였다.

Design and Implementation of the Intrusion Detection Data Web-based Management System on Heterogeneous Environments*

Eun-Soo Kim** · Seok-Hun Kim*** · Jung-Gil Song****

ABSTRACT

The hacking accident is increasing repidly according to development of latest computer network and the method becomes various. But, to correspond to hacking, it is lot of difficulties to cope gear and security element between product because most radiant mercuries apply technology between individual digenomic species and It is real condition that great setup, equipment, manpower disturbance are enlarged to apply this. Designed and embody Site-Based executive system that can integrate security element about IDS information between digenomic species to solve these problem and correspond efficiently from hacking.

Key words : Instrusion, Security, IDS, IDMEF, XML

---

* 본 연구는 '산업자원부 지역협력연구사업(과제번호 : R12-2003-004-02001-0) 지원으로 수행되었음'.

** 한남대학교 교수학습지원센터

*** 한남대학교 컴퓨터공학과

**** 한남대학교 정보통신 · 멀티미디어 공학부

1. 서 론

정보화 사회의 활성화와 정보통신 인프라로서 인터넷의 중요성이 급속히 부각되는 반면에, 인터넷으로 인한 여러 가지 정보보안 문제점들 또한 심각해 지고 있다. 또한 각종 운영체제와 이기종간 시스템들의 보안 취약점과 해킹 기법뿐만 아니라, 취약점을 검색하기 위한 검색 및 해킹 도구들이 점차 공개 및 확산되고 있다. 이러한 상황과 더불어 해킹이 계속 증가 추세에 있으며, 그 대안으로써 보안관련 제품들이 빠르게 연구 개발되고 있는 상태이다[1].

다양한 보안 제품들이 시장에 나오게 되면서 단 하나의 보안 제품으로 보안을 보장하기보다는 다양한 보안 제품들 간의 특성을 살리도록 상호 연동을 통하여 보안도를 높이려고 하고 있다. 예를 들어 실제 시스템의 침입을 탐지하는 침입 탐지 시스템은 내부 네트웍의 관문에 설치된 침입 차단 시스템으로부터 입수된 정보의 도움으로 실제 침입을 정확하게 판단할 수 있으며, 침입 차단 시스템은 침입 탐지 시스템의 분석 결과를 이용하여 차단해야하는 접속을 막을 수 있다. 또한 침입 탐지 시스템들도 네트웍 상의 패킷을 분석하는 네트웍 기반, 호스트에서 사용된 명령어들을 분석하는 호스트 기반 등 성격이 다양하기 때문에 각 시스템에서 탐지한 결과를 출력한 로그의 형식을 관리하고 종합 분석할 필요가 있다. 현재 여러 종류의 침입탐지 시스템이 개발되고 있으나 이기종 시스템간의 정보표현과 결과보고 방법이 그에 대한 의견 통일이 어려우며, 많은 과탐지(false positive)가 존재하여 관리자를 피곤하게 하는 요소가 되고 있다. 또한 분산 서비스 거부 공격에 적절히 대응하지 못하고 있으며 알려지지 않는 공격에 대하여 즉각적인 대응이 어렵다. 이러한 환경에서도 중요한 서비스를 지속적으로 제공하여 사용자의 신뢰도를 떨어트리지 않아야 하고, 침입이 발생하더라도 침입자를 즉각적으로 색출하여 대응할수 있는 기반이 마련되어야 한다[1, 2].

본 논문에서는 이러한 이기종 시스템 환경에서 침입탐지 정보를 효과적으로 관리할 수 있는 웹 기반 관리 시스템을 설계하였다. 또한, 침입이 발생하더라도 시스템 및 네트워크 서비스를 지속적으로 제공하기 위하여 이기종 보안 시스템들간의 상호 호환성과 확장성을 제공하기 위하여 침입탐지 시스템간의 표준 메시지 교환 형식인 IDMEF(Instruction Message Exchange Format)의 확장을 통해 메시지 형식을 정의하고, 이를 사용하는 웹 기반 관리 시스템을 구현하였다. 본 논문의 구성은, 2장에서는 시스템 설계에 필요한 관련연구를 살펴본 후 3장에서는 이기종간 침입탐지 정보의 웹기반 관리 시스템의 설계와 시스템에 대하여 논의한 후 4장에서는 실제 구현된 웹 기반 관리 시스템에 대해 기술하고, 끝으로 5장에서 결론 및 향후 연구방향을 제시한다.

2. 관련 연구

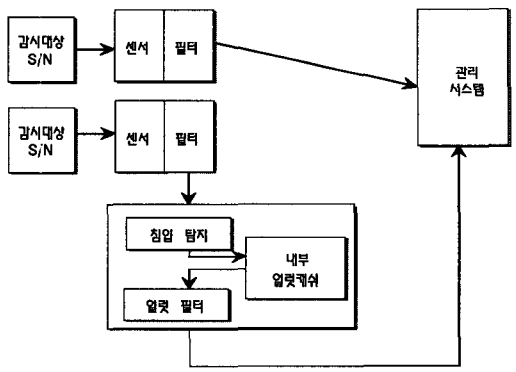
2.1 IDS(Intrusion Detection System)

IDS는 Intrusion Detection System(침입탐지 시스템)의 약자로, 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. IDS는 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다. 침입이란 시스템에 대한 고의적 불법적인 행위를 말하며 시스템의 불법침입, 중요정보의 유출 및 변경, 훼손, 불법적인 사용, 그리

고 컴퓨터 바이러스 및 서비스거부 등과 같은 구체적인 형태로 나타난다. 침입탐지시스템은 이러한 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말하며 간단하게는 로그 파일분석에서부터 복잡한 실시간 침입탐지시스템까지 다양한 소프트웨어가 존재한다. 침입탐지 기법은 크게 비정상적인 침입탐지 기법과 오용 침입탐지 기법으로 나눌 수 있다[5, 12].

〈표 1〉 IDS의 분류

항 목	N-IDS	H-IDS
탐지대상	네트워크를 통과하는 패킷	시스템 내부 사용자들의 활동
설치단위	네트워크	세그먼스 호스트
기반기술	패킷 캡처링	프로세스 모니터링
	프로토콜별 패킷 분석	실시간 로그분석
	패킷 조각모음	TTY 모니터링

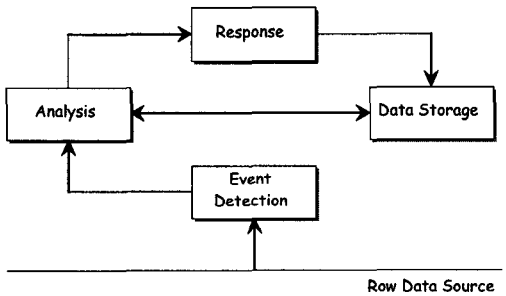


(그림 1) 일반적인 기업의 분산 컴퓨팅 환경에서의 IDS구조와 필터내부 프로세싱

Host기반의 IDS는 시스템 감사를 위해서는 기술적인 어려움이 크고, 비용 또한 비싸다, 그리고 로그분석 수준을 넘어 시스템 콜 레벨 감사까지 지원해야 하기 때문에 여러 벤더의 운영체제를 위한 제품을 개발하는 것 또한 시간적, 기술적으로 어렵다는 것이 업계의 중론이다. 이에 비해 N-IDS의 경우 운영체제의 제약이 없고 네트워크 단에서 독립적인 작동을 하기 때문에 구현과 구축 비용이 저렴하다.

2.2 IDS 일반적인 모델

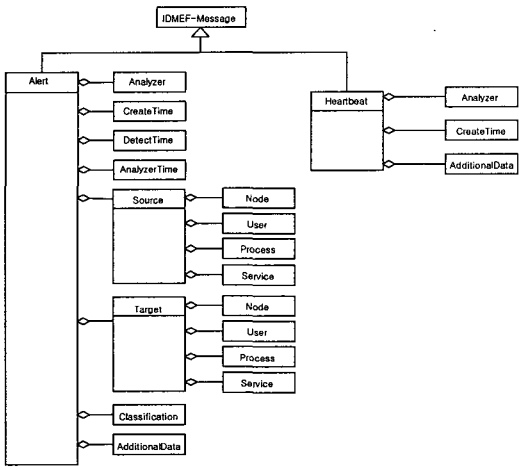
ISO/IEC에서 정의하는 침입 탐지의 기본 모델은 그림과 같이, 원시 데이터(raw data source), 사건 탐지(event detection), 분석(analysis), 대응(response), 데이터 저장소(data storage)의 5가지 요소로 구성된다.



(그림 2) ISO/IEC 침입탐지 기본 모델

2.3 침입탐지 시스템 로그형식 표준

IDMEF(Instruction Dectection Message Exchange Format)는 IETF에서 제안하고 있는 메시지 교환으로써, 침입 탐지 시스템과 그 응답 시스템 및 관리 시스템간에 정보를 공유하기 위한 데이터 형식과 교환 절차를 정의한다. 서로 다른 종류의 탐지 시스템간의 메시지의 상호 교환을 위하여, IDMEF는 침입탐지 시스템을 포함한 다양한 보안 관리 시스템들이 침입탐지 시스템에서 생성되는 로그를 사용할 수 있도록 침입탐지 시스템의 로그 형식에 대한 표준을 정의한다. IDMEF를 위한 데이터 모델은 UML(Unified Modeling Language)로 명세되었으며, XML로 구현되고 있다. 그림은 IDMEF 모델에 정의된 주요 클래스간의 관련성을 보여준다[4].



(그림 3) IDMEF 클래스 개요

IDMEF 메시지 타입은 크게 Alert와 Heartbeat의 두 가지 형태로 구성된다. Alert는 침입정보를 생성한 IDS의 이름, 침입정보를 발생시킨 이벤트, 공격의 개시시스템과 목표시스템에 대한 정보 등을 포함한다. Heartbeat는 분석모듈이 관리모듈에게 상태정보를 제공할 때 사용된다.

2.4 이기종 보안 제품 연동 방안

2.4.1 OPSEC(Open Platform for Security)

체크포인트(Check Point) 사에서 제안된 OPSEC은 확장 가능한 개방된 관리 프레임워크를 통하여 네트워크 보안의 모든 측면을 통합하고 관리하며, 제 3의 응용으로 하여금 공개된 API를 통하여 OPSEC 프레임워크로 접속될 수 있도록 한다. 확장형 기업 정책 관리 및 정책 강화 프레임워크라 할 수 있는 OPSEC은 현재 OPSEC 협력관계에 있는 270여개 이상의 세계적인 보안 업체들이 안전한 엔터프라이즈 네트워킹을 위한 모든 요소들을 중앙 집중식으로 관리 할 수 있게 하기 위해 중요한 역할을 하고 있다[6].

OPSEC은 보안 기능을 위한 몇 개의 프로토콜과 API의 집합으로 구성되어 있으며, 제공하는 SDK(Software Development Toolkit)을 이용하여 모든 제품들간의 통합이 가능하다.

2.4.2 ASEN(Adaptive Security for Enterprise Network)

ASEN은 이기종 보안 제품 간의 연동을 위해 어울림정보기술에서 개발한 보안프레임워크이다. 어울림 정보기술은 SECUREWORKS 제품들과의 연동을 위한 ASEN API를 제공하므로, ASEN API를 이용하여 SECUREWORKS 제품군과 이기종 보안 제품들은 손쉽게 연동할 수 있다.

ASEN 프레임워크의 설계 목적은 다양한 보안제품으로 구성된 다수의 시스템을 모니터링하고, 상호 유동적으로 결합하여 작동할 수 있는 통신 모델과 제어 모델을 제시함으로써 불필요한 중복작업을 피하고, 보안위협에 보다 능동적으로 대응할 수 있는 기반을 만드는 것이다. 이를 위해 ASEN은 다음의 사항들에 대하여 정의하고 있다[7].

- 상호 통신 방법의 정의, 제품간 또는 통합관리 서버와의 통신에 있어서 통신방법과 구조를 제안
- 상호 인증 방법의 정의, 통신에 있어서 신뢰성을 갖기 위한 상호인증 방법을 제시
- Security Device의 관리정보 표현방법 정의
- 보안정책 적용, 서로 다른 제품간의 보안정책을 설정하기 위해 어떠한 방법으로 보안정책을 표현하고 전송하는 가에 대하여 제시
- 통합관리에 필요한 기반 정보를 정의

2.4.3 SNMP

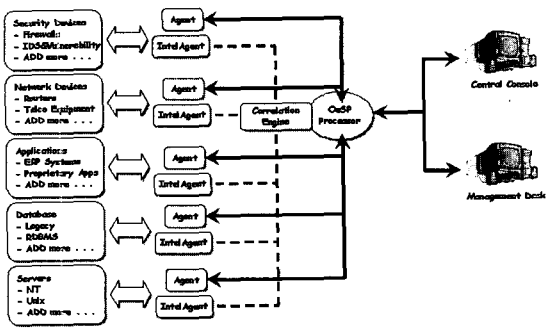
국내외 많은 보안업체에서는 이기종 통합 보안관리를 위하여 SNMP 기반의 API를 이용하고 있으며, 본 절에서는 eSecurity사의 OeSP(Open eSecurity Platform)와 IBM Tivoli의 Risk Manager를 살펴보기로 한다.

첫째, eSecurity 사에서 개발한 통합보안관제

솔루션인 OeSP는 SNMP v1/v3를 이용하여 제3의 응용에서 사용할 수 있는 API를 제공하고 있다. 특히, 세계 최다의 에이전트(약 120개 : 어플리케이션과 장비간의 연동을 위함)를 지원하고, 제 3의 응용에서 사용할 수 있는 API 제공으로 손쉽게 에이전트 확장이 가능함을 장점으로 하고 있다. 그러나, 공개적으로 API를 제공하지 않아 어떤 형태로 지원되는지 파악할 수 없는 단점이 있다[8].

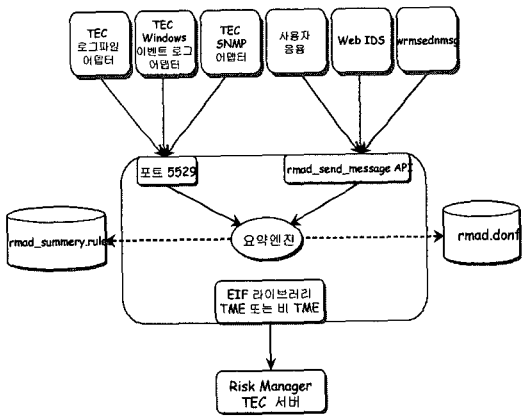
OeSP는 중앙집중형, 룰 베이스 에이전트로 작동하며, 이러한 에이전트들은 각 보안 장비들과 콘솔간에 통신을 지원하며 통신은 SNMP를 이용하여 엔터프라이즈 보안 관리 솔루션을 제공한다. e-Security 플랫폼은 4개의 요소로 구성되어지며 다음과 같은 기능을 지원한다.

- Open e-Security Platform : 모든 보안 관련 장비를 하나의 GUI 콘솔에서 통합관리를 할 수 있도록 지원
- e-Security Agent : 각 장비와 콘솔간의 통신을 담당
- e-Security Administrator Workbench : 멀티 벤더의 장비들에 설치된 에이전트들을 룰 기반의 에이전트로 생성하고 서로간의 관계를 설정하고 관리하는 기능을 제공
- e-Security Management Desk : 침입에 대응하여 통보, 장애티켓발행, SLA관리와 관련된 워크플로를 관리



(그림 4) OeSP 구조

둘째, IBM Tivoli Risk Manager는 침입 검출을 위한 관리 시스템으로서, 여러 가지의 포함된 센서 응용과 타사 센서 응용으로부터 침입 감지 경고를 받는 기능을 제공한다. 침입 검출 시스템은 실시간으로 서비스 거부 공격 또는 스캐닝 및 대량 공격의 침입을 발견하고 감시한다. 또한, Risk Manager는 잘못된 경고와 실제 경고를 분리할 수 있도록 침입 검출 경고의 자동 처리를 제공한다[9]. (그림 5)는 Tivoli Risk Manger가 어댑터 혹은 응용으로부터 이벤트를 수집하여 TEC(Tivoli Enterprise Console) 서버로 전달하는 기능을 개략적으로 표현한다.



(그림 5) Tivoli 기능 개요

② CreateTime - DATETIME, Heartbeat가 생성된 시각

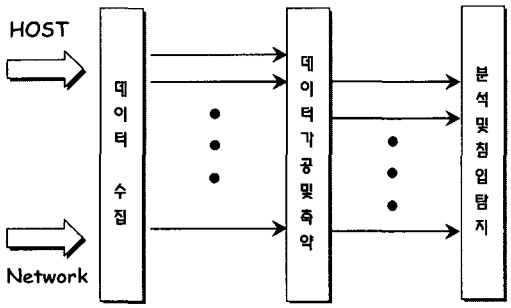
③ AdditionalData - 다른 클래스에 속하지 않는 검출기에 의해 생성되는 추가적인 정보

3. 시스템 설계

3.1 침입탐지 모듈 설계

본 논문에서 가장 핵심적인 부분이라 할 수 있는 침입탐지 모듈은 HOST나 Network에서

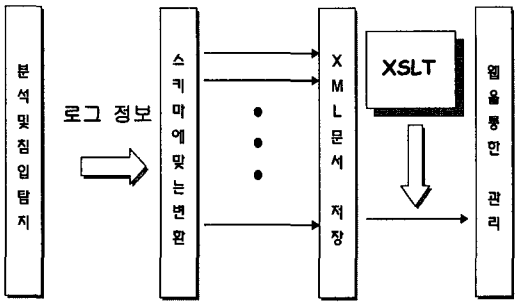
수집된 데이터를 애플리케이션을 통해 가공 및 축약하여 미리 정의한 패턴의 침입행위와 일치하는지를 분석하여 침입 여부를 탐지해내도록 설계되었다. 다른 Network 기반의 침입탐지 시스템과 동일한 패킷수집과 네트워크 스캐닝을 통해 수집하거나, 호스트의 Port 스캐닝을 통해 수집한 데이터는 애플리케이션을 통해 필요한 부분을 가공, 축약된 뒤 미리 정의하여 저장되어진 수많은 침입 행위의 패턴과 비교하게 되고, 일치하는 경우 침입행위로 간주하여 침입 정보 저장모듈로 보내지게 된다.



(그림 6) 침입탐지 모듈

3.2 정보저장 및 웹관리 모듈 설계

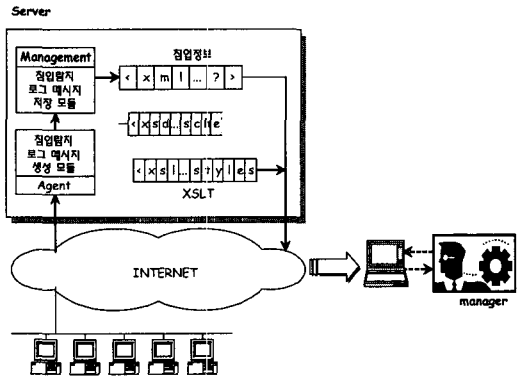
분석 및 침입탐지를 통해 침입행위로 간주된 로그 정보들은 스키마에 맞게 변환되어지고 XML 문서에 저장된다. 이 저장된 정보는 XSLT를 통하여 가공되어지고 웹을 통한 관리가 이루어 질 수 있도록 웹에 게시된다. 물론 침입여부에 대해서 서버에 직접 접근하지 않고 웹을 통한 원거리 모니터링이 가능하므로 관리자의 편의성과 실시간 감시에 비중을 둔 설계라 할 수 있을 것이다. 이 모듈에서 가장 중심이 되는 부분은 침입탐지 모듈에서 넘어온 로그 정보를 정의된 스키마에 맞게 XML문서로 저장하는 부분이다. 만약 침입탐지 모듈에서 침입행위로 간주되면 시스템은 이벤트를 발생시키고 XML문서를 업데이트 하게 되므로 실시간 모니터링이 가능하도록 설계하였다.



(그림 7) 로그저장 및 웹 게시 모듈

3.3 전체 시스템 구조

인터넷을 통해 접근이 가능한 서버에 다수의 접속자가 접속을 할 경우 IDS는 패턴을 분석하여 침입여부를 판단한 뒤, 침입행위로 간주되는 패턴과 일치할 경우 그 로그를 미리 정의된 명세에 의해 XML문서로 저장한다. 이 문서는 새로운 침입행위로 인해 이벤트가 발생할 경우 지속적으로 업데이트 되며 XSL을 통해 웹에 게시한다. 모니터는 인터넷망을 통해 원거리에서도 쉽게 침입자의 침입여부를 확인할 수 있고 적절한 조치를 취하게 된다.



(그림 8) 전체 시스템 구조도

3.4 스키마 설계

3.4.1 스키마의 요구사항

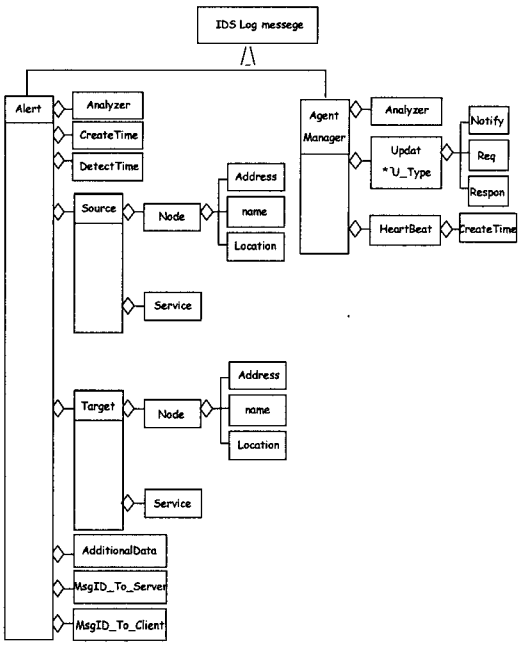
침입탐지 로그를 저장하기 위한 XML문서의 스키마를 정의하기 위해서는 다음 표와 같은 요구사항을 충족 시켜주어야 한다.

〈표 2〉 요구사항 정의

요구사항	내 용
일반 요구사항	기존 RFC, IPv4 및 IPv6 등과의 관계를 정의
메시지 포맷 요구사항	메시지 포맷의 국제화/지역화, Manager에 의한 데이터 Filtering/Aggregation 등 메시지 포맷의 독립성을 정의
통신 메커니즘 요구사항	전송메시지 신뢰성보장, Firewall의 경계를 가로질러 구성요소간 메시지 전송 등 메시지 전송 특성, 인증, 비밀성, 무결성, 부인방지서비스 등 정보보호서비스 특성. 서비스거부공격 방지, 메시지의 유해한 복사 등 공격에 대한 방어 특성 등을 정의
메시지 내용 및 의미 요구사항	침입탐지 메커니즘, 이벤트 식별자, 소스와 대상의 식별자, 장치(Device) 주소, 날짜와 시간, 상세 데이터 등 스키마의 메시지 내용 및 의미 정의
Alert 정의 및 정의 절차 요구사항	스키마 Alert 표준 리스트의 확장성과 정의 절차와 구현의 독립성을 정의

3.4.2 스키마의 구조 설계

앞에서 살펴본 침입탐지 시스템 스키마의 요구사항은 IDMEF와 유사하다. 그러나 본 논문에서 XML Schema를 사용하여 XML문서를 정의하는 이유는 IDMEF에서처럼 DTD를 사용하여 XML문서를 정의할 경우에는 좀더 다양한 데이터 타입을 설정하지 못하게 되기 때문이다. 본 논문에서의 데이터모델의 구성은 다음과 같다.



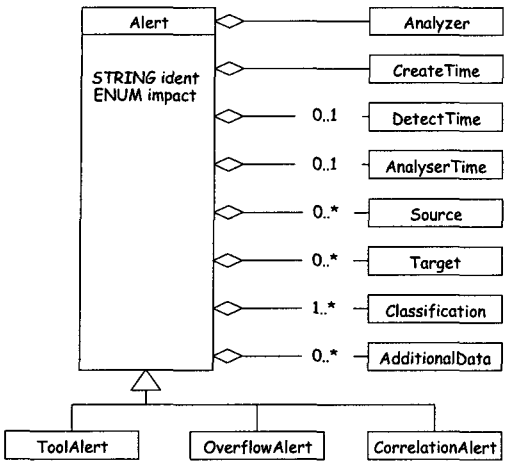
(그림 9) 데이터모델 구성도

4. 시스템 구현

4.1 네트워크 디바이스 드라이버 구현

4.1.1 메시지 수집

침입탐지 시스템에 의해서 바악된 접속과 침입에 대한 경고는 Alert 클래스에서 관리한다. ToolAlert Class 에서는 공격 도구나 트로이 목마 같이 악의적인 프로그램을 사용하여 침입을 시도할 때 관련된 정보를 제공하기 위하여 사용되고 CorrelationAlert클래스는 여러개의 경고 정보들 간의 상관관계를 표현하기 위하여 사용하며 OverflowAlert 클래스는 buffer overflow 공격에 관련된 추가적인 정보를 제공한다. 다음 그림은 Alert 클래스 및 메시지 수집에 관련된 클래스들의 관계 및 Alert클래스의 클래스 다이어그램이다.

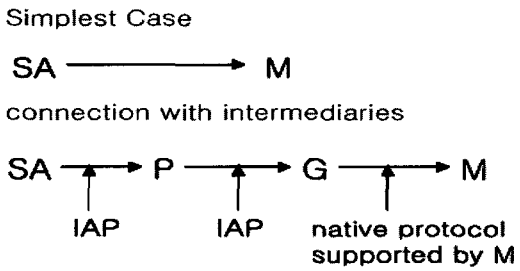


(그림 10) Alert 클래스

4.1.2 분석 및 침입탐지

IAP는 네트워크 상에서 Sensor/Analyzer(SA)와 Manager 사이에 침입 Alert 자료를 교환하기 위한 프로토콜로서 IP 네트워크를 통하여 민감한 Alert 자료를 전송하기 위해 필요한 전송특성과 보안특성을 제공할 수 있도록 구현하였다.

IAP의 동작내용은 다음과 같다.



(그림 11) IAP의 동작

SA가 잠재적인 침입을 감지하고 Alert 자료를 만든 후 만들어진 Alert 자료를 Manager로 전송하면 Alert 자료를 받은 Manager는 Alert 자료를 분석하여 침입여부를 결정하여 저장모듈로 전송한다.

4.2 로그 저장 및 관리 모듈 구현

4.2.1 스키마 구현 및 저장

본 논문에서 IDS의 로그를 저장하는 XML의 정의를 위한 XML Schema 는 IDMEF를 기반으로 하여 XML스키마의 문법을 사용하여 구현하였다.

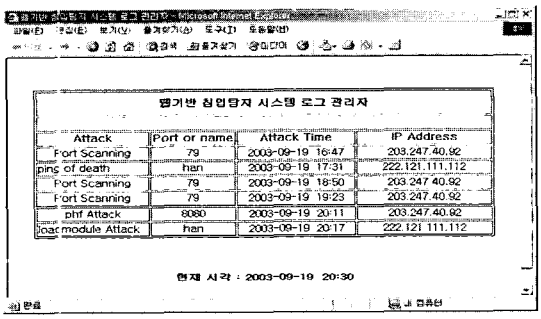
(그림 12) 침입탐지 정보에 대한 XML Schema

위 스키마를 바탕으로 하여 저장된 XML문서는 각 공격별로 저장되며 다음 그림은 Port Scanning 침입에 대한 XML 문서이다.

(그림 13) Port Scanning에 대한 XML문서

4.2.2 XSL을 통한 웹 관리

본 논문에서는 저장된 XML 파일을 XSLT를 사용하여 실시간으로 웹을 통한 관리가 이루어지도록 구현하였다. 이러한 실시간 모니터링 및 관리는 침입에 대한 관리자의 빠른 인지를 통해 피해를 최소화하고 상습적인 공격자에 대한 발빠른 대처를 이루게 한다. 다음은 웹기반 침입탐지 시스템의 웹 인터페이스이다.



(그림 14) 웹 인터페이스

5. 결론 및 향후 연구방향

침입자의 공격에 의한 여러 가지 침해 사고는 관리자의 지속적인 각 시스템의 패치 및 시스템 로그의 체계적인 분석을 통하여 줄일 수 있다.

본 논문에서는 침입탐지 및 관련 분야 및 침입탐지 시스템의 표준화 성향에 대해 제시하고, 침입탐지 로그의 표준인 IDMEF를 분석하였다. 또한 DTD로 이루어진 IDMEF를 XML Schema로 재정의 하고 XML문서로 저장하도록 하였다. 그리고 보안 관리자의 부재중에 생기는 침입에 대한 차선책으로 웹기반 인터페이스를 XSLT를 통해 구현하여 실시간 모니터링 및 침입자의 악의적인 공격에 손쉽게 대처할 수 있도록 하였다.

향후 연구 방향으로는 ESM 개발을 위하여 이기종 보안 장비들을 동시에 관리할 수 있는 추론 엔진 개발을 주도적으로 추진하는 것이 필요할 것이다.

참 고 문 헌

[1] 한국전자통신연구원, 인터넷 보안 시스템-기술시장 보고서, 2002. 12.

[2] 한국정보보호진흥원, 해킹 바이러스 통계 및 분석 자료, http://certcc.or.kr.

[3] 인터넷보안기술포럼(ISTF), 로그형식 표준안, http://www.istf.or.kr.

[4] ISTF-005/R 침입탐지시스템 로그형식 표준, http://www.istf.or.kr, 2003. 4.

[5] IDS 개발현황 한국정보보호 진흥원 표준화 특집, http://www.kisa.or.kr.

[6] Check Point Software, OPSEC SDK Documentation, http://www.opsec.com.

[7] 어울림 정보기술, ASEN Documentation, http://oulim.co.kr.

[8] OeSP, eSecurity, http://www.esecurityinc.com.

[9] IBM, IBM Tivoli USers Guide, http://www.tivoli.com.

[10] SAINT, http://www.macrotek.co.kr.

[11] Jack Koziol, "Intrusion Detection with Snort", SAMS, 2003.

[12] Judy Novak, Stephen Northcutt, "Network Intrusion Detection", New Riders Publishing, 2003.

김 은 수

1994년 서울산업대학교 시각디자인과(이학사)

1997년 서울산업대학교 대학원 시각디자인과(이학석사)

2004년 한남대학교 대학원 컴퓨터공학과(공학박사)

2004년~현재 한남대학교 교수 학습지원센터 강의전담교수

관심분야 : 웹디자인, 멀티미디어디자인, 정보보호

김 석 훈

2001년 배재대학교 정보통신 공학과(공학사)
2003년 한남대학교 대학원 컴퓨터공학과 (공학석사)
2003년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호

송 정 길

1966년 한남대학교 수학과 (이학사)
1982년 홍익대학교 대학원 전자계산학과(이학석사)
1988년 중앙대학교 대학원 전자계산학과(이학박사)
1990년~1991년 University of illinois 객원교수
1979년~현재 한남대학교 컴퓨터공학과 정교수
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 분산시스템, 정보보호