韓國 컴퓨터情報學會 論文誌
第11卷 第2號, 2006. 5.

2006-11-2-1-9

분산 환경에서의 침입방지를 위한 통합보안 관리 시스템 설계

이 창 우*, 김 석 훈**, 송 정 길***

Design of Enterprise Security Management System for Intrusion Prevention in Distributed Environment

Chang-Woo Lee*, Seok-Hun Kim**, Jung-Gil Song***

요 약

인터넷의 사용자 증가와 네트워크 환경이 점점 복잡해지고 제공되는 서비스 및 사용자의 요구사항들이 다양해짐에 따라 안정적이고 효과적인 환경을 유지하기 위한 서비스 운용관리는 점점 어려워지고 있다. 또한 초창기 보안은 침입차단시스템에 국한되었지만, 최근에는 침입탐지시스템(IDS), 침입차단시스템(Firewall), 시스템 보안, 인증 등 관련 솔루션이 대거 등장함에 따라 통합 관리가 중요시되어 지고 있다. 따라서 대규모 네트워크 환경에서 다양한 형태의 침입을 탐지하기 위해서는 호스트 혹은 네트워크 기반에서의 감시 및 탐지, 침입 여부에 대한 판정과 더불어, 각 시스템이 제공하는 침입 정보의 통합 분석을 통하여 광범위한 분석을 가능하게 하는 통합 보안 관리 시스템의 개발이 필요하다. . 따라서, 본 논문에서는 보안 시스템간의 통합보안 관리를 위하여 각 시스템 사이에 침입 정보를 교환하고 정보 전송을 제어할 수 있는 통합 보안 관리 시스템을 제안하고자 한다.

Abstract

The service use management for keeping up stable and effective environment is hard little by little by according to increase of internet user and being complicated network environment of the Internet little by little, being various of the requirements of the service which is provided and the user demand. And the beginning flag security was limited in IDS, But recently the integrated civil management is coming to be considered seriously according to adventting IDS, Firewall, Security of system. The development of integrated security civil management system to analyze widely through observation and detection at Network or host base, the judgment of attack, and integrated analysis of infiltration information is necessary because of detecting the various type attack.

▸ Keyword : 침입탐지시스템(IDS), 침입차단시스템(Firewall), 통합보안관리시스템(ESM), XML

• 제1저자 : 이창우 • 교신저자 : 김석훈
• 접수일 : 2006.03.2, 심사완료일 : 2006.05.18
* 한남대학교 컴퓨터공학과 박사과정, ** 한남대학교 컴퓨터공학과 박사과정, *** 한남대학교 컴퓨터공학과 교수

Ⅰ. 서 론

네트워크와 컴퓨터의 발달로 인하여 보안사고 발생시 신속한 침해 사고 대응서비스를 통한 대응체계를 갖추기 위해 다양한 종류의 보안 솔루션들이 개발되고 있다. 최근 일반 기업, 금융권, ISP 등의 정보보호 관리 담당자 혹은 시스템 및 네트워크 담당자들은 단품 솔루션들이 제공하는 정보보호 서비스에서 관리비용의 증가, 일관된 정보보호정책 적용이나 침해사고 공동대응의 불가 등과 같은 효율성이나 관리 측면에 있어 여러가지 문제를 발생시켰다[1,2].

이로 인하여 인터넷이라는 개방된 환경에서 무방비 상태로 노출되어 있는 기업정보를 안전하게 보호하기 위해 복잡한 정보보호 솔루션들을 일관성 있는 정책으로 중앙에서 통합관리하고 잠재되어 있는 위험요소들을 사전에 파악하여 능동적으로 대처하고자 하는 요구에서 등장한 것이 통합보안관리(Enterprise Security Management : ESM) 시스템이다[3,5].

ESM은 침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상사설망(VPN) 등 다양한 종류의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템으로 보안 관리보다는 통합 시스템 관리의 형태로 시스템 관리의 영역에서 먼저 출발하여 Firewall, VPN, 바이러스 검사, 컨텐츠 필터링, URL 모니터링/필터링, 침입탐지 등 별개의 보안 구성 요소를 일관적인 전체로 결합하여, 인증과 감시, 허가에서 네트워크 관리에 이르기까지 모든 것들을 망라하는 통합관리로 연구되고 있다.

최근 통합 보안 관리 시스템들은 업체별 보안 시스템간의 상호 연동이 어려운 실정이고, 대응 조치 또한 체계적이지 못하며, 개별 단위 보안 시스템들 사이에 메시지 제어에 대한 방안을 고려하지 않고 있다. 따라서, 본 논문에서는 보안 시스템간의 통합보안 관리를 위하여 각 시스템 사이에 침입 정보를 교환하고 정보 전송을 제어할 수 있는 통합 보안 관리 시스템을 제안하고자 한다.

본 논문의 구성은 2장에서는 통합보안 관리 시스템 설계에 필요한 관련연구를 살펴본 후 3장에서는 통합보안 관리 시스템을 위한 단위별 보안 시스템 설계에 대하여 기술하고, 4장에서는 통합보안 관리 시스템을 위한 단위별 보안 시스템을 위해 구현한 프로토타입 시스템을 제안한 다음 마지막으로 결론 및 향후 연구방향을 제시한다.

Ⅱ. 관련 연구

2.1 침입차단 시스템(Firewall)

침입차단시스템은 빌딩 공사를 할때 빌딩의 한 부분에서 다른 부분으로 불이 번지는 것을 막기 위해 설계된 것이다. 이론적으로 침입차단시스템은 이와 유사한 목적을 제공한다. 여기서, 침입이란 비 인가된 정보로의 접근 및 정보조작, 그리고 시스템 무력화를 위한 고의적이고도 불법적인 시도를 의미한다[10].

침입차단시스템은 인터넷과 같은 외부 네트워크와 내부 네트워크 사이에 놓이며, 외부 네트워크로부터 내부 네트워크로의 침입을 감지하여 정보와 자원들을 보호한다.

- Packet Filtering - 가장 간단한 형태의 방화벽의 기능으로, 미리 설정된 접근 제어 규칙에 따라 해당 패킷의 통과 여부를 결정.
- Application-Level Proxy - 특정 응용 서비스에 대해 내부망과 외부망을 연결시켜주는 중간 매개자 역할.
- Circuit-Level Proxy - 통상 Session 단위로 클라이언트·서버간의 가상의 circuit을 형성하여 데이터 전송.
- Stateful Packet Inspection - 접속에 대한 상태를 관측하여, 패킷의 통과 여부를 결정하는 동적 액세스 규칙을 적용.

2.2 침입탐지 시스템(IDS)

IDS(침입탐지시스템)의 기본 기능은 비 인가자의 불법적인 자원의 사용 및 변조, 파괴행위에 대한 탐지를 궁극적 목표로 하고 있다. 하지만 현재 상용 IDS는 기본 기능만으로는 시장에 진출할 수 없을 정도의 다양한 기능들을 가지고 있다. 그중 가장 중요한 기능은 실시간 네트워크 감시기능이라 할 수 있다[5].

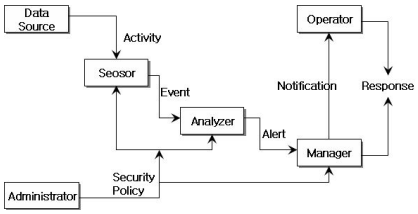

그림 1. 침입탐지 시스템
Fig 1. Intrusion detection system

침입탐지 시스템은 네트워크와 시스템의 정보를 침해 하는 침입을 탐지하여 네트워크 관리자에게 효과적으로 네트워크를 관리 할 수 있도록 판단하여 결정의 자료를 제공하는 시스템이다. 침입탐지 시스템은 자료수집, 축약, 침입판단, 통보 및 대응 모듈로 구성된다.

2.3 통합보안관리 시스템(ESM)

통합보안관리 기술은 침입탐지 시스템, 가상사설망 시스템 등 다양한 종류의 보안 시스템들을 상호 연동하여 각 기능을 통합 관리하는 중앙집중식 관리체계로서, 보안관제서비스 업체, 보안 시스템 개발 업체들간에 컨소시움 형태나 독립적인 통합 보안관리시스템으로 개발되고 있다[17].

통합보안관리 기술 수준은 현재 자사 제품에 대한 모니터링 기능이 구현되어 있지만, 앞으로는 보안 프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전하고 있으며, 수집된 자료를 분석하여 보안사건에 대한 리포팅 기능과 함께 각 보안시스템에 대한 세부 정책관리 기능이 가능한 단계로 발전할 것으로 예상되고 있다. 즉, 보안정책을 수립하고 수립된 보안정책에 따라 시스템을 구현하며, 이를 모니터링 하거나 신속하고 효과적인 조치를 위해 각종 경보 기능을 제공하는 등 일련의 워크플로우를 일관되게 지원하는 것이 그것이다.

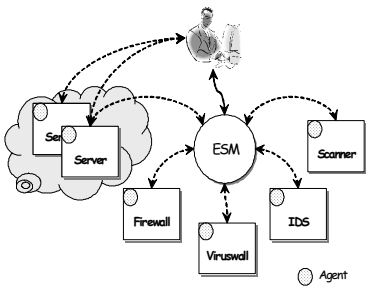

그림 2. 통합보안 관리 시스템
Fig 2. Enterprise security system

2.4 침입차단 시스템 로그 데이터 모델

Firewall 로그 형식에서 가장 상위 클래스는 FWSLF-Message로 모든 종류의 메시지를 총칭한다. 시스템에서 접속시의 메시지를 의미하는 Connect 클래스와 시스템의 동작 상태를 의미하는 Heartbeats 클래스가 크게 적용된다. Firewall 로그 데이터 모델의 세부적인 내용을 UML의 클래스 다이어그램으로 설계한 결과는 (그림 3)과 같다.

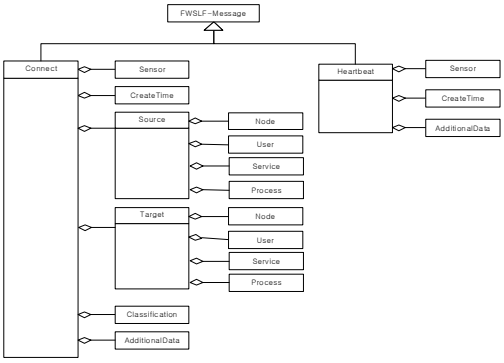

그림 3. 침입차단 시스템 로그 클래스
Fig 3. Firewall System Log Class

(그림 3)에서 정의한 각각의 클래스 모델을 XML 문서의 규칙과 형식을 만족하기 위하여 표준 DTD로 정의한 결과는 다음과 같다.

```
// FWSLF-Message 클래스 DTD
<!ENTITY % attlist.fwslf "version CDATA #FIXED '1.1'">
<!ELEMENT FWSLF-Message ((Connect| Heartbeat)*)>
<!ATTLIST FWSLF-Message %attlist.fwslf;>

// Connect 클래스 DTD
<!ENTITY % attvals.criticaltype "(unknown|normal|
 suspicious | warning | critical )">
<!ENTITY % attvals.actiontype "(unknown |
pass | block | protect) ">
<!ELEMENT Connect (Sensor, CreateTime,
Source, Target, Classification, AdditionalData*)>
<!ATTLIST Connect ident CDATA '0'
criticality %attvals.criticaltype 'unknown'
action %attvals.actiontype 'unknown'>

// Heartbeats 클래스 DTD
<!ELEMENT Heartbeat (Sensor, CreateTime, AdditionalData*)>
<!ATTLIST Heartbeat ident CDATA '0'>
```

2.5 침입탐지 시스템 로그 데이터 모델

IDS 로그 형식에서 가장 상위 클래스는 IDSLF-Message로 모든 종류의 메시지를 총칭한다. 시스템에서 검출하는 메시지를 의미하는 Alerts 클래스와 시스템의 동작 상태를 의미하는 Heartbeats 클래스가 크게 적용된다. IDS 로그 데이터 모델의 세부적인 내용을 UML의 클래스 다이어그램으로 설계한 결과는 그림 4와 같다.

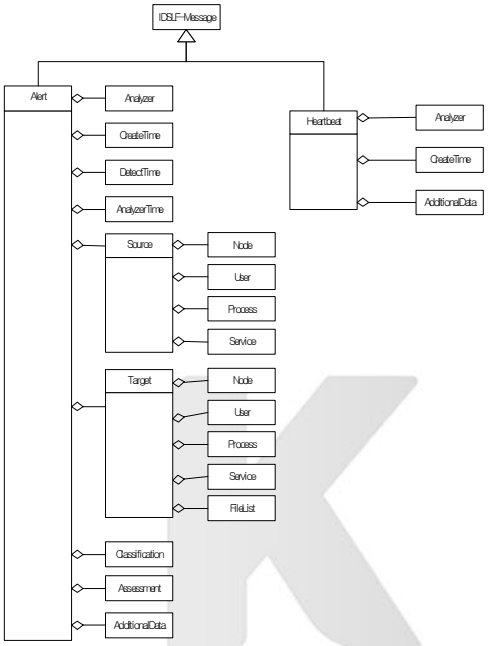

그림 4. 침입탐지 시스템 로그 클래스
Fig 4. IDS System Log Class

(그림 4)에서 정의한 각각의 클래스 모델을 XML 문서의 규칙과 형식을 만족하기 위하여 표준 DTD로 정의한 결과는 다음과 같다.

```
// IDSLF-Message 클래스 DTD
<!ENTITY % attlist.idslf "version CDATA #FIXED '1.1'">
<!ELEMENT IDSLF-Message ((Alert | Heartbeat)*)>
<!ATTLIST IDSLF-Message %attlist.idslf;>
```

```
// Alter 클래스 DTD
<!ELEMENT Alert(Analyzer, CreateTime, DetectTime?,
AnalyzerTime?, Source*, Target*, Classification+,
Assessment?, (ToolAlert | OverflowAlert | CorrelationAlert)?,
AdditionalData* )>
<!ATTLIST Alert ident CDATA '0' >

// Analyzer 클래스 DTD
<!ELEMENT Analyzer (Node?, Process? )>
<!ATTLIST Analyzer analyzerid CDATA '0'
 manufacturer CDATA   #IMPLIED
 model        CDATA   #IMPLIED
 version      CDATA   #IMPLIED
 class        CDATA   #IMPLIED
 ostype       CDATA   #IMPLIED
 osversion    CDATA   #IMPLIED>
```

III. 시스템 설계

본 논문에서 설계한 시스템의 구조를 살펴보면 (그림 5)와 같이 침입대응 시스템은 침입차단시스템(Firewall), 침입탐지시스템(IDS), 통합보안 관리부(ESM)로 구성된다. 전체 시스템에서 센서(sensor)는 데이터를 수집하여 분석기(analyzer)에서 전송하고 분석기는 이를 분석하여 경보를 발생한다. 분석기에 의해 발생된 정보는 인접한 경보 메시지 관리자(Alert message Manager)에게 전송되고, 관리된다. BEEP/IDXP를 통하여 통신하는 침입탐지 요소들 사이에서 데이터 분류와 처리를 수월하게 한다.

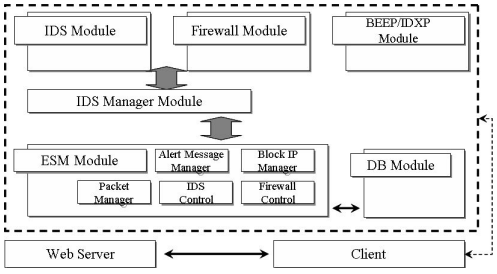

그림 5. 통합 보안관리 시스템 구성도
Fig 5. Composition of ESM system

3.1 침입차단 모듈 설계

■ 패킷 필터링 모듈

침입차단 시스템에 접속한 상대 컴퓨터에 대한 정보를 알아내기 위한 방법으로 패킷을 이용한다. 패킷에는 상대방에 대한 정보와 접속하려는 컴퓨터의 정보를 가지고 있다. 패킷 필터링을 이용하는 침입차단 시스템은 이러한 패킷 정보를 이용하여 비 인가된 사용자의 패킷을 차단하게 된다.

■ 필터링 데이터 저장 모듈

원격지 컴퓨터로부터 전달되어진 필터링 Data는 침입차단 시스템의 드라이버로 전달된다. 전달된 데이터는 연결 리스트에 저장하여 관리한다. 전달되어진 필터링 데이터를 연결 리스트에 추가시키는 부분을 구현 소스는 부록에 수록되어 있다.

■ 패킷 처리 모듈

침입차단 시스템으로 전달된 패킷은 필터링에 의해 차단 유무를 검사받게 된다. 모든 패킷은 dispatch_complete 함수를 통과하면서 알맞게 처리된다. 접근을 허용하는 패킷은 안전하게 시스템을 통과하게 되고 접근을 허용하지 않는 패킷은 dispatch_complete 함수에서 처리 되어 시스템에 접근할 수 없게 된다.

(그림 6)은 침입차단 모듈에서 침입 차단 시스템 접속에서부터 패킷을 필터링하고 데이터에 저장되어 처리되는 부분을 UML의 Sequence 다이어그램을 이용하여 침입대응 시스템에서 침입 차단 과정을 모델링한 것이다.

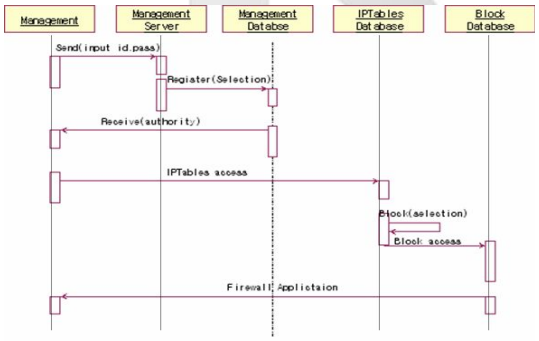

그림 6. 침입 차단 모듈 시퀀스 다이어그램
Fig 6. Sequense Diagram of Firewall Module

3.2 침입탐지 모듈 설계

침입 탐지 과정은 보안 관리자는 시스템의 대응 및 분석 제어를 위하여 Management를 통해 Management Server에 접근하여 인증을 통하여 권한을 획득하게 된다. 외부망에서 내부망으로의 접근은 Policy Server의 Policy Database를 통해 수집된 정보를 분석하여 그 결과를 보고 및 Alert Database에 저장되게 된다. Alert Database에 저장된 로그 데이터는 XML 변환 모듈을 통해 XML 문서로 변환 된 후 XSLT로 작성된 대응 및 분석결과를 보안 관리자에게 웹상으로 전송하여 관리하도록 설계하였다.

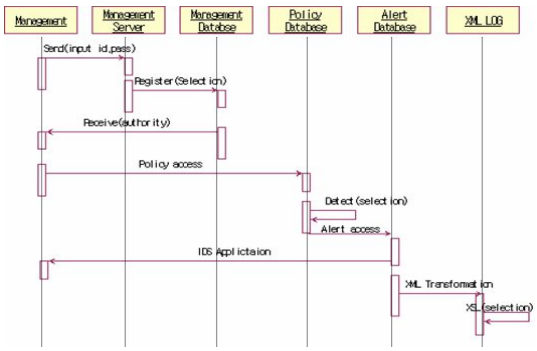

그림 7. 침입 탐지 모듈 시퀀스 다이어그램
Fig. 7 Sequense Diagram of intrusion detection Module

IV. 시스템 구현

4.1 시스템 환경

침입대응 시스템 구현을 위해 Windows 2000 Server 상에서 윈도우 기반의 Developer Tool인 Visual C++ 6.0 Enterprise를 사용하였고, MS-SQL Server 2000 Enterprise Edition 상에 구현된 Database를 ODBC (Open DataBase Connectivity)를 이용하여 연동하였다.

4.2 침입차단 시스템 구현

접근 허용에 대한 정보는 관리자에 의해 시스템의 접근을 통하여 관리되어 진다. 관리자는 원격으로 침입차단 시스템에 접속하게 되고, 포트와 IP 설정 부분을 이용하여 원격으로 정보를 표현할 수 있다. 이러한 내용은 원격지에 있는 시스템에 전달되어 진다. (그림 8)은 관리자에 의해 관리되어지는 침입차단 시스템의 제어부분을 구현한 것이다.

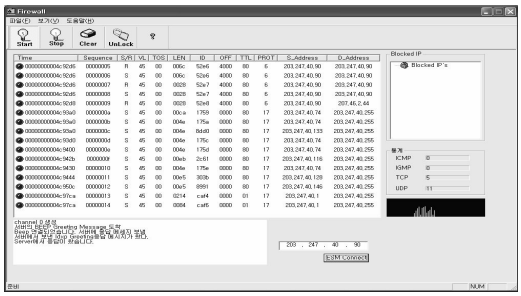

그림 8. 침입차단시스템 제어 부분
Fig. 8 Control of Firewall System

패킷 필터링은 가장 간단한 형태의 방화벽의 기능으로, 통상 IP헤더와 상위 프로토콜 헤더의 정보만을 이용해 미리 설정된 액세스 제어 규칙에 따라 해당 패킷의 통과여부를 결정한다. 필터링 연결 리스트에 연결되어 있는 IP Block DATA와 외부에서 접근한 패킷의 정보를 비교하여 접근허용 유무를 판별하여 접근이 허가된 패킷은 내부망으로 전달하고, 허가되지 않은 패킷은 방화벽에서 처리한다. (그림 9)는 접근 차단할 IP 목록을 설정하거나 해제할 수 있도록 구현한 부분이다.

그림 9. IP Blocking 구현 화면
Fig. 9 Implementation of IP Blocking

4.3 침입탐지 시스템 구현

(그림 10)은 초기 IDS를 설정할 수 있도록 구현한 부분으로서, 화면 상단에 있는 실행 File과 RuleSet의 경로가 나타나는데 이는 pcap을 설치하고 경로를 설정했을때 프로그램 상에서 자동으로 알아서 설정되도록 되어있다. IDS가 공격받았을 경우 공격 유형에 따라 Alert 메시지들이 해당 경로로 자동 저장된다.

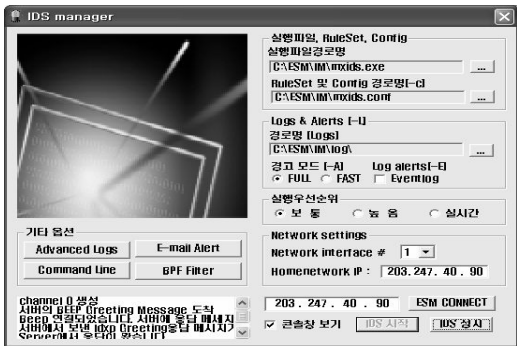

그림 10. 침입탐지시스템 구현 화면
Fig. 10 Implementation of IDS System

4.4 통합보안 관리 시스템 구현

통합 보안관리 시스템의 프로토타입은 크게 ESM, IDS, Firewall 세부분으로 나뉘어져 있으며 작동순서는 다음과 같다.

- 중앙 통제 시스템인 ESM을 가동시킨다.
- IDS와 Firewall을 ESM에 접속시킨다.
- ESM을 통하여 IDS와 Firewall을 켠다.
- 해당 공격은 IDS에 감지되고, Firewall을 통과하면서 차단되며 이는 ESM에 보고된다.
- ESM에서는 해당하는 공격들에 대한 정보와 분석은 Packet Analyzer를통해 확인할 수 있다.

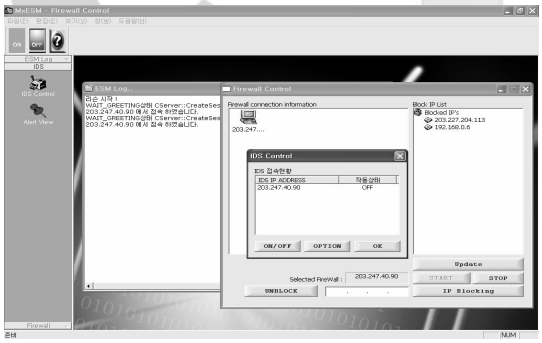

그림 11. 통합보안관리시스템 구현 화면
Fig. 11 Implementation of ESM System

4.5 웹기반의 인터페이스 구현

(그림 12)와 (그림 13)은 필요하지 않은 경보의 전송을 방지하기 위하여 XML 기반의 파일을 사용하여 요구사항을 만족하는 행위들에 대하여 사전 정의되어 공식적으로 문서화된 명세로써, 관리자가 자신이 필요로 하는경보에 대한 속성을 XML DTD로 표현하여 교환하고, 관리자가 침입에

대한 빠른 인지를 통해 피해를 최소화 하고 상습적인 공격에 대한 빠른 대응을 위하여 실시간으로 모니터링 할 수 있도록 웹 기반 인터페이스를 적용하였다.

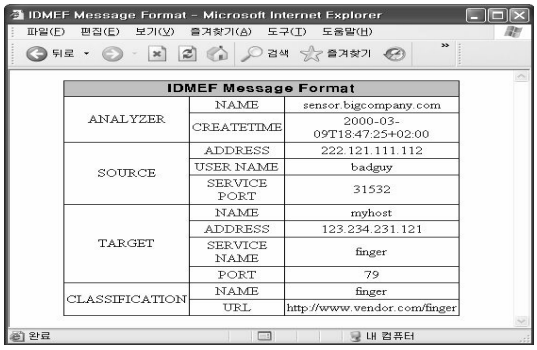

그림 12. 웹기반의 침입차단 로그 인터페이스
Fig. 12 Firewall Log Interface of Web base

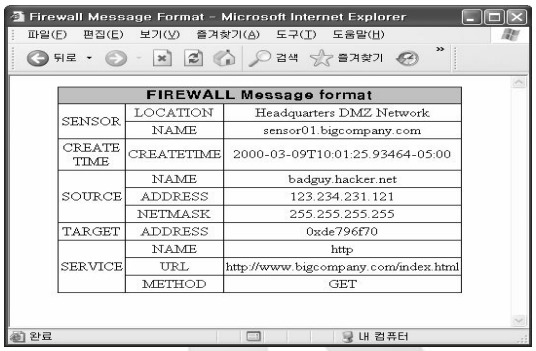

그림 13. 웹기반의 침입탐지 로그 인터페이스
Fig. 13 IDS Log Interface of Web base

V. 결론 및 향후 연구방향

본 논문에서는 침입대응시스템 환경에서 로그파일을 XML 형식의 변환을 통하여 데이터의 구조화에 따라 시스템의 로그 파일들을 분석 및 관리할 수 있도록, 로그 데이터의 상호 처리 능력을 향상시키고, 데이터의 공용성과 프로그램의 유연성을 향상시킨 통합보안 관리 시스템을 설계하였다.

향후 연구되어야 할 내용은 이러한 설계를 바탕으로 IDXP/BEEP 프로토콜을 기반으로 실제적인 구현을 통하여 다량의 정보가 교환되는 분산 환경에서의 통합보안 관리 시스템 구현과 시스템에 대한 성능평가가 함께 이루어져야 할 것이다.

참고문헌

[1] 한국정보보호진흥원, http://www.kisa.or.kr.
[2] 인터넷보안기술포럼(ISTF), http://www.istf.or.kr.
[3] 한국전자통신연구원, 인터넷 보안 시스템- 기술시장 보고서, 2002. 12
[4] W3C, “Extensible Markup Language (XML) 1.0 (Second Edition)”, http://www.w3.org/xml
[5] Tech Report_보안정책, http://www.itdata.co.kr/column/200205/tech/secu.htm
[6] DMTF, Distributed Management Task Force, http://www.dmtf.org.
[7] IETF internet Draft(2003), Intrusion Detection Exchange Format Data model
[8] IETF internet Draft(2003), Intrusion Detection Exchange Format Data Requirements
[9] ISTF-004/R 침입차단시스템 로그형식 표준, http://www.istf.or.kr.
[10] Judy Novak , Stephen Northcutt, "Network Intrusion Detection", New Riders Publishing, 2003
[11] Randy Heffner, "Enterprise Application Security Integration", IT Trends 2002, December 2001.
[12] DMTF Specification, White Paper "CIM Core Policy Model for CIM schema release 2.4", http://www.dmtf.org, 2000. 5.
[13] Deron Powell, "Enterprise Security Management(ESM): Centralizing Management of Your Security Policy", SANS Institute, December 2000.

[14] A Study on the Development of Countermeasure Technologies against Hacking and Intrusion in Computer Network Systems, KISA final development report, January 1999.
[15] 손우용, 송정길, "통합보안 관리 시스템의 침입탐지 및 대응을 위한 보안정책 모델", 한국컴퓨터정보학회 논문집, 제 9권 2호, pp.81~87, 2004.6.
[16] 김강, 전종식, "보안정책 기반 침입탐지 시스템 모델 설계", 한국컴퓨터정보학회 논문집, 제 8권 4호, pp.81~86, 2003.12.

저 자 소 개

이 창 우

1986 동국대학교 산업공학과 (공학석사)
1998~현재 한남대학교 컴퓨터공학과 박사과정
<관심분야> 정보보호, XML, 분산처리시스템

김 석 훈

2003 한남대학교 컴퓨터공학과 (공학석사)
2003~현재 한남대학교 컴퓨터공학과 박사과정
<관심분야> XML, 모바일 컴퓨팅, 정보보호, VoIP

송 정 길

1988 중앙대학교 전자계산학과 (이학박사)
1979~현재 한남대학교 컴퓨터공학과 교수
<관심분야> 정보보호, XML, 분산처리시스템