제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

# XML 기반의 침입차단 로그 메시지 분석 시스템 설계 및 구현*

전석훈* 김석훈* 손우용* 이창우* 송정길**
* ** 한남대학교 컴퓨터공학과

## 요 약

인터넷은 본질적으로 신뢰할 수 없는 네트워크들의 집합체이다. 인터넷상에서는 정보의 흐름을 통제하기가 대단히 어렵기 때문에, 산재한 자원을 충분히 활용하면서, 내부의 중요한 자원을 인터넷으로부터 보호해 줄 수 있는 보안문제가 심각하게 대두되고 있다. 최근 발생하는 바이러스 사고와 시스템 불법 침입에 대한 발생률이 과거보다 훨씬 높으며 다양해지고 있다. 이러한 시기에 불법 행동을 막기 위한 침입 차단에 대한 연구가 활발하게 진행 중이며 계속적인 발전을 하고 있다. 본 논문에서는 침입자의 불법 행동에 대한 로그 정보를 XML 포맷 형식에 맞추어 관리자에게 통보하고, 원격으로 제어 할 수 있는 침입 차단 시스템을 개발하여 관리측면에서 발생하는 문제점을 해결하고자 하였다.

# Design and Implementation of Firewall Log Message Analysis System based on XML

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

## ABSTRACT

The Internet is aggregate of trustless networks essentially. Because the Internet is very difficult to control flowing of information, taking advantage of enough sporadic resource, security problem that can protect internal important stock from the Internet is risen seriously. Recently, virus accident and generation rate about system intrusion that happen become much higher and various than past. On these time, is progressing researcher for invasion cutout to keep away illegal act vigorouslyand do continuous development. In this paper, reporting administrator log information about invader's illegal act depending on XML format form, and I wished to solve problem that happen in administration side developing invasion interception system that can control to remote.

* 본 연구는 '과학기술부 지역협력연구사업(과제번호: R12-2003-004-02001-0) 지원으로 수행되었음'
* 한남대학교 컴퓨터공학과
** 한남대학교 정보통신 · 멀티미디어공학부 교수

## 1. 서 론

과거의 전산망은 소수의 사용자가 데이터 교환을 위하여 사용되었다. 그러나 현재의 전산망은 거대한 데이터 및 전자 상거래, 광고로 많은 양의 정보 교환, 많은 양의 정보를 서로 교환할 수 있는 경로의 발달로 그에 따른 활용과 이익, 편리함이 동반되는 반면, 그에 따르는 위협 요소도 함께 성장하고 있다[2].

이러한 위협에는 바이러스와 불법 행동에 의한 침입들이 있으며, 이를 대비하기 위한 보안 프로그램의 중요성이 점차 증가하고 있는 것이 사실이다. 현재 시장에는 많은 보안관련 제품이 개발되어지고 있지만, 보안 툴의 다양한 작동방법에 대한 관리상 어려움도 적지 않은 불편함을 가져다주고 있다. 또한, 단품 솔루션들이 제공하는 정보보호 서비스에서 관리비용의 증가, 일관된 정보보호정책 적용이나 침해사고 공동대응의 불가 등과 같은 효율성이나 관리 측면에 있어 여러가지 문제를 발생시켰다[3].

본 논문에서는 침입차단시스템의 로그 형식을 XML 형태로 생성하는 FWSLF을 이용하여 원격으로 관리자에게 시스템의 상황을 보고하고 관리자가 원격으로 제어할 수 있도록 구현하였다. 본 논문의 구성은 다음과 같다. 2장에서는 시스템 설계에 필요한 관련연구를 살펴본후 3장에서는 XML 기반의 원격제어에 의한 침입차단 시스템 설계에 대하여 논의한후 4장에서는 실제 구현된 시스템에 대해 기술하고, 끝으로 5장에서 결론 및 향후 연구방향을 제시한다.

## 2. 관련연구

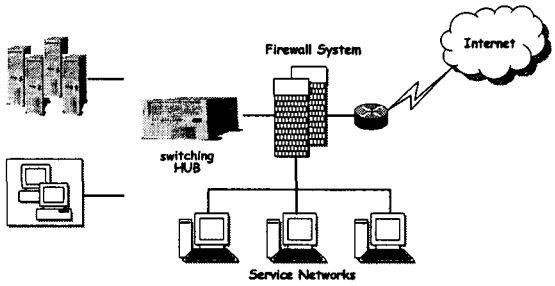
### 2.1 XML(eXtensible Markup Language)

XML은 웹상에서 구조화된 문서를 전송 가능하도록 설계된 표준화된 텍스트 형식의 마크업 언어이다. XML은 인터넷에서 기존에 사용하던 HTML의 한계를 극복하고 SGML의 복잡함을 해결하는 방안으로써 HTML 내부에 사용자가 직접 새로운 태그를 정의할 수 있는 기능을 추가하였다. HTML은 편리하고 쉽게 사용할 수 있다는 장점을 가지고 있으나 고정적이고 확장이 어렵다는 단점이 있다. HTML과는 달리 XML은 자유롭게 문서의 요소와 속성, 개체를 선언하여 자료를 구조적으로 표현할 수 있다. 또 다른 마크업 언어인 SGML은 유연성이나 확장성은 뛰어나지만, 지나치게 복잡한 문제점을 가지고 있다. XML은 HTML과 SGML의 장점을 유지하면서 단점을 극복한 마크업 언어이다[1,7].

### 2.2 방화벽(Firewall) 기술

방화벽(Firewall) 기술은 침입차단시스템으로도 불리는 보안 제품으로 외부망으로부터 내부망으로 접속하는 비인가자의 침입을 차단시켜주는 소프트웨어 혹은 하드웨어를 지칭한다. 방화벽은 접근제어목록(Access Control List : ACL)에 따라 내부 네트워크의 자원들의 보호를 담당하고 있는 가장 널리 보급되어 있는 대표적인 네트워크 보안 장비이다[4].

현재 대표적인 침입차단시스템은 기존의 패킷 필터링과 응용레벨에서의 프록시 기능을 추가한 Stateful firewall 방식이 주를 이루고 있다. Sateful firewall은 동적으로 상태 테이블을 생성 및 관리하고 패킷을 전송할 때 상태 테이블을 통해 감시하므로 응용 레벨의 프록시 방식보다 빠른 장점이 있다[8]. 방화벽 제품은 세계적으로 대표적인 Check Point의 소프트웨어 방식의 FireWall-1과 NetScreen의 NetScreen 시리즈 등이 있으며, 라우터 장비 업체인 Cisco의 PIX Firewall 시리즈도 많이 보급되어 있는 제품 중의 하나이다. 근래의 제품 동향은 초고속망의 사용 증가에 따른 고속 장비의 요구에 따라 NetScreen사와 Cisco, Servgate사 등에서 아미 기가급의 방화벽을 출시하였으며, Nokia에서도 CheckPoint의 방화벽 소프트웨어를 하드웨어 플랫폼에 탑재하는 기가급 솔루션을 내놓고 있다.

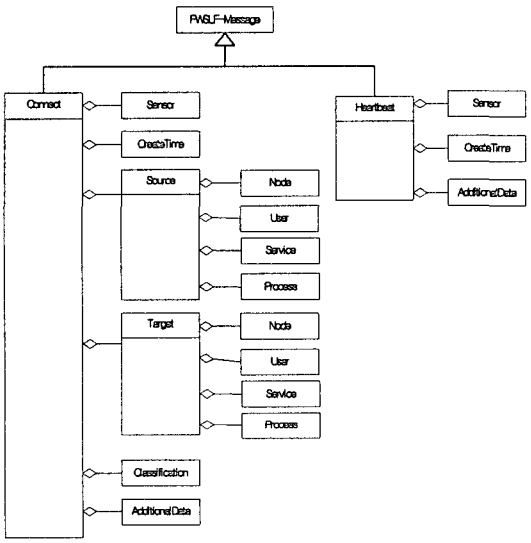



(그림 1) 침입차단 시스템

### 2.3 침입차단 시스템 로그 포맷

FWSLF(침입차단 시스템 로그포맷)는 보안 솔루션의 통합 관리를 위한 표준 형식들 중 침입차단시스템과 관련하여 제정된 표준형식이다

[5]. 접속자가 시스템에 접근하였을 경우 침입차단시스템은 로그 표준 형식에 맞추어 로그 데이터를 생성한 후 원격지에 있는 관리자에게 알려주는 역할을 한다. (그림 2)의 침입차단시스템 로그 형식은 침입차단시스템이 의심스런 침입자의 행동에 대하여 관리자에게 경고를 발생하는데 사용할 수 있도록 설계되어 있다.




(그림 2) 침입차단 시스템 로그 포맷

침입차단시스템 로그 표준 형식의 XML 코드 내용은 크게 Connect와 Heartbeat으로 나누어져 있다. 각각의 메시지 클래스에 대해서 하위 메시지 클래스가 있으며, 이것은 세부적인 정보를 제공하는데 사용된다.

Connect 클래스는 침입차단시스템에서 접속자의 접근 시도와 접근에 의해 발생되는 의심스런 행동에 대하여 로그의 형태의 정보를 표현한다. Connect 클래스는 아래와 같은 하위 클래스들로 이루어져 있다[5].

① Sensor - 로그를 생성한 검출기 정보
② CreateTime - DATETIME, 로그가 생성된 시각
③ Source - 접속을 일으키는 이벤트의 원천
④ Target - 접속을 일으키는 이벤트의 목표
⑤ Classification - 접속의 이름, 또는 다른 보안 시스템이이 어떤 접속인지 결정할 수 있도록 하는 정보.
⑥ AdditionalData - 다른 클래스에 속하지 않는 검출기에서 생성되는 추가적인 정보

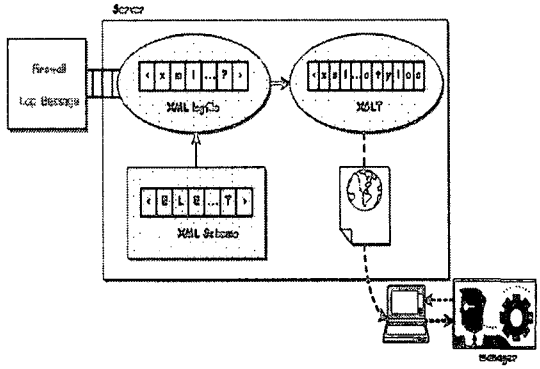
Heartbeat 메시지는 관리자에게 현재의 상태를 알려준다. Heartbeat 클래스는 아래와 같은 하위 클래스들로 이루어져 있다.

① Sensor - Heartbeat 메시지를 보낸 검출기의 id 정보
② CreateTime - DATETIME, Heartbeat가 생성된 시각
③ AdditionalData - 다른 클래스에 속하지 않는 검출기에 의해 생성되는 추가적인 정보

## 3. 시스템 설계

### 3.1 시스템 흐름도

현재 접근한 접속자에 대한 로그 데이터를 이미 정의되어있는 XML 문서로 저장한다. 로그 데이터는 원격지에 있는 관리자의 모니터에 침입차단시스템에 대한 상태가 모니터링 되어지도록 설계하였다. 본 논문에서 구현된 침입차단 시스템의 구조를 살펴보면 (그림 3)과 같다.



(그림 3) 전체 시스템 구성도

### 3.2 XML 스키마 설계

XML 문서 형태로 보내질 데이터들을 좀더 다양한 데이터 타입으로 정의하기 위하여 XML 스키마를 설계하였다.

각각의 메시지들은 또 다른 메시지를 포함하고 있으며 미래를 위한 확장이 가능하도록 설계되어 있다.

```
<?xml version="1.0" encoding="euc-kr"?>
<!–FirewallLOGSchema.xsd -->
<xsd:schemaxmlns:xsd="http://www.w3c.org/2001/XMLSchema"
elementFormDefault="qualified">
<xsd:element name="FirewallSchema">
<xsd:complexType>
<xsd:sequence>
<xsd:element name="Alert">
<xsd:complexType>
<xsd:sequence>
<xsd:element ref="Analyxer" maxOccurs="unbounded"/>
<xsd:element ref="CreateTime" maxOccurs="unbounded"/>
<xsd:element ref="DetectTime" maxOccurs="unbounded"/>
<xsd:element name="Source">
<xsd:complexType>
<xsd:sequence>
<xsd:element ref="Node" maxOccurs="unbounded"/>
<xsd:element ref="User" maxOccurs="unbounded"/>
<xsd:element ref="Process" maxOccurs="unbounded"/>
<xsd:element ref="Service" maxOccurs="unbounded"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="Target">
<xsd:complexType>
<xsd:sequence>
<xsd:element ref="Node" maxOccurs="unbounded"/>
<xsd:element ref="User" maxOccurs="unbounded"/>
<xsd:element ref="Process" maxOccurs="unbounded"/>
<xsd:element ref="Service" maxOccurs="unbounded"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
..... 하략
```

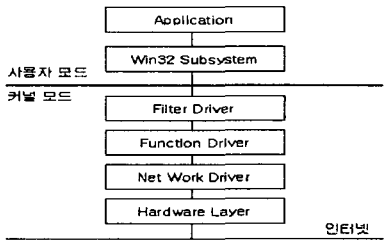
(그림 4) XML Schema 문서

## 4. 시스템 구현

### 4.1 네트워크 디바이스 드라이버 구현

본 논문에 구현한 시스템은 단순한 형태의 패킷 필터링을 사용한 방화벽이다. 패킷 필터링 방식은 다른 방식에 비해 처리 속도가 빠를 뿐만 아니라 새로운 서비스와 쉽게 연동 할 수 있는 유연성을 제공하고 있기 때문이다.

실질적으로 필터링을 하는 곳은 디바이스 드라이버이다. 디바이스 드라이버란 사용자 프로그램과 하드웨어 사이에 위치하여 사용자로부터 하드웨어로 데이터를 전달해주는 중계 역할을 한다. 본 논문에 구현한 디바이스 드라이버는 네트워크와 관련한 네트워크 디바이스 드라이버이다. (그림 5)는 디바이스 스택을 나타낸것으로서 드라이버 계층을 도식화 한 것이다.

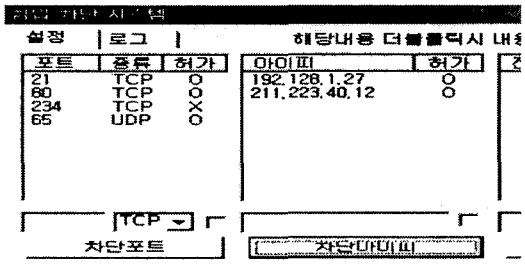



(그림 5) 디바이스 스택

외부망의 모든 패킷은 반드시 네트워크 드라이버를 통해서 시스템으로 전달되어진다. 패킷 필터링은 OSI 모델에서 네트워크층과 전송층에서 만들어진 패킷의 일부 즉, 출발 및 목적지 IP 주소 정보, TCP/IP 출발지 포트, TCP/IP 목적지 포트 중 일부를 필터링 할 수 있도록 구성되어 있다.

### 4.2 침입차단 시스템 구현

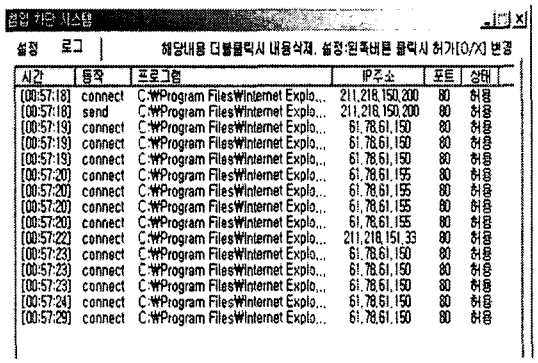
접근 허용에 대한 정보는 관리자에 의해 시스템의 접근을 통하여 관리되어 진다. 관리자는 원격으로 침입 차단 시스템에 접속하게 되고, 포트와 IP 설정 부분을 이용하여 원하는 정보를 표현할 수 있다. 이러한 내용은 원격지에 있는 시스템에 전달되어진다. (그림 6)은 관리자에 의해 관리되어지는 침입 차단 시스템의 제어부분을 구현한 결과이다.




(그림 6) 필터링 설정

어떤 한 접속자가 네트워크를 통해 현재 컴퓨터에 접근하게 되면, 침입차단시스템에는 접속자가 행하는 모든 시도에 대해서 로그가 남게 된다. 시스템은 접속자의 로그를 XML형태로 저장되어 관리자에게 전달되어진다. 관리자는 접속자의 행동에 대한 모든 내용을 실시간으로 모니터

링 할 수 있다. 침입차단시스템에 의해 전달되어진 접속자의 로그 데이터를 모니터링화한 결과는 (그림 7)과 같다.

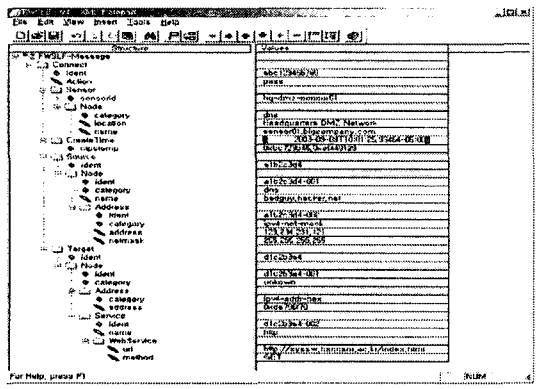



(그림 7) 로그 데이터 모니터링

시스템은 접속자가 시스템에 접근했을 때 접속자에 대한 로그를 XML을 이용해서 로그 표준형식에 맞추어 데이터를 생성하게 된다. 생성되어진 로그 정보는 원격지에 있는 관리자의 컴퓨터에 전달되어지며, 관리자는 원격지에서 시스템에 접근한 접속자의 모든 행동에 대한 정보를 볼 수 있다. 만일 접속자가 불법 적인 행동을 취하게 되면 관리자는 침입차단시스템에 접근을 막는 일련의 행동을 취할 수 있다.

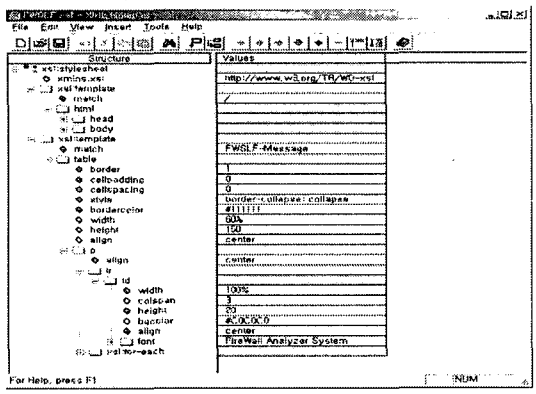
### 4.3 침입차단 로그 XML 구현

(그림 4)의 XML 스키마를 바탕으로 하여 침입차단 로그로 저장되어 변환된 XML 문서는 (그림 8)과 같다.



(그림 8) 침입차단 로그에 대한 XML 문서

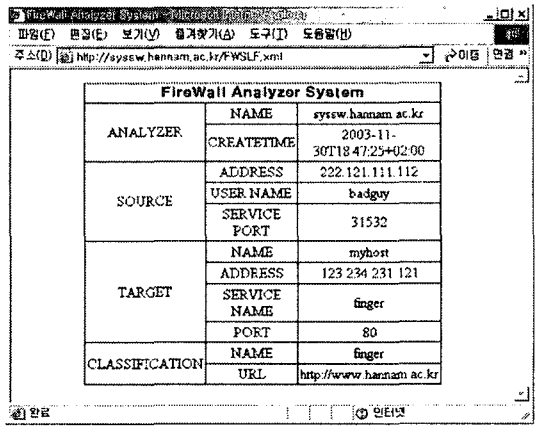
변화하는 로그 형식에 동적으로 대응하기 위하여 웹 상에서 관리할 수 있도록 설계한 XSLT 문서는 (그림 9)와 같다.



(그림 9) XML 문서에 대한 XSLT 문서

### 4.4 XSLT를 적용한 결과

관리자가 실시간으로 모니터링 할 수 있도록 웹 기반 인터페이스를 XSLT를 적용하여 구현한 결과는 (그림 10)과 같다.




(그림 10) XSLT 적용 결과

## 5. 결론 및 향후 연구방향

본 논문에서는 침입 차단 시스템 로그 표준형식에 XML을 사용하여 유연성과 확장성 있는 시스템을 구현하였고, 또한 네트워크 접근에 대한 정보를 원격으로 관리자에게 통보하고, 관리자가 침입차단시스템을 제어할 수 있도록 구현하였다. 앞으로 로그 형식은 불법 행동이 다양해지고 해

킹기술의 발달로 인해 많은 변화가 있을 것으로 전망되고, 세계 표준에 따라 국내의 표준 형식이 개정될 여지가 남아있는 상태이다.

향후 연구 과제로는 침입 탐지 시스템(IDS), 가상사설망(VPN) 등 여러 가지 보안기법과의 연계를 통한 통합 보안관리 시스템(ESM)에 대한 연구가 필요할 것이다.

## 참고문헌


[1] W3C, "Extensible Markup Language (XML) 1.0 (Second Edition)", http://www.w3.org/XML

[2] 한국정보보호진흥원, http://www.kisa.or.kr

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

[4] 방화벽 솔루션, http://www.cisco.com

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

[6] Walter Oney, "Microsoft Programming the Windows Driver Model", 정보문화사, 2001

[7] 송정길 저, "XML 프로그래밍", 생능출판사, 2003.

[8] 이만영 외 공저, "인터넷 보안 기술" 생능출판사, 2002.

[9] IETF, IDWG, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition", draft-ietf-idwg-idmef-xml-10.txt, 2003.7

[10] 오승희 외, "최신 네트워크 보안 기술 동향 분석", 한국정보과학회 추계학술 발표 논문지, 제 30권 2호, 2003.10.

[11] 정영서 외, "네트워크 정보보호 시스템 발전 방향", SK Telecommunications Review, 제 13권 제 2호, 2003. 2.



전 석 훈
2001년 목원대학교 경영학과 졸업(경영학사)
2002년~현재 한남대학교 대학원 컴퓨터공학과 석사과정 재학중

김 석 훈
2001년 배재대학교 정보통신공학과 졸업(공학사)
2003년 한남대학교 대학원 컴퓨터공학과 졸업(공학석사)
2003년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중

손 우 용
1998년 한남대학교 컴퓨터공학과 졸업(공학사)
2000년 한남대학교 대학원 컴퓨터공학과 졸업(공학석사)
2001년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중

이 창 우
1982년 동국대학교 산업공학과 졸업(공학사)
1986년 동국대학교 대학원 산업공학과 졸업(공학석사)
1998년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중

송 정 길
1966년 한남대학교 수학과 졸업(이학사)
1982년 홍익대학교 대학원 전자계산학과(이학석사)
1988년 중앙대학교 대학원 전자계산학과(이학박사)
1990년~1991년 University of illinois 객원교수
1979년~현재 한남대학교 정보통신·멀티미디어공학부 교수