# 패킷 리덕션 방식의 침입탐지 시스템 설계 및 구현

정신일† · 김봉제 · 김창수

(부경대학교)

# Design and Implementation of Intrusion Detection System of Packet Reduction Method

*Shin-Il JUNG† · Bong-Je KIM · Chang-Soo KIM*

*Pukyong National University*

*(Received June 8, 2005 / Accepted June 28, 2005)*

**Abstract**

Many researchers have proposed the various methods to detect illegal intrusion in order to improve internet environment. Among these researches, IDS(Intrusion Detection System) is classified the most common model to protect network security.

In this paper, we propose new log format instead of Apache log format for SSL integrity verification. We translate file-DB log format into R-DB log format. Using these methods we can manage Web server's integrity, and log data is transmitted verification system to be able to perform both primary function of IDS and Web server's integrity management at the same time. The proposed system in this paper is also able to use for wire and wireless environment based on PDA.

***Key word** : Intrusion Detection System, Integrity, Verification, SSL*

## Ⅰ. 서 론

정보 통신 기술의 발달로 인터넷은 사람들의 생활의 일부로 자리 잡게 되었고, 사람들은 다양한 정보를 공유하거나 재활용할 수 있게 되었다. 그러나 사용자의 수가 증가함에 따라 네트워크를 통한 보안 침해 사례가 증가하고 있으며, 그 피해 상황 역시 계속적으로 증가하고 있다. <표 1>은 한국정보보호진흥원(Certcc-KR)에서 발표한 "2004년 3월 침해사고 접수 및 처리현황"으로 다양한 공격기법을 활용하는 것은 거의 동일하며 발생 건수도 지속되고 있음을 보여주고 있다(한국정보보호진흥원, 2004).

이러한 침입시도나 공격으로부터 데이터를 보호하기 위하여 인터넷 보안 솔루션에 대한 연구가 활발히 진행되고 있으며, 대표적인 것으로는 침입탐지시스템(IDS : Intrusion Detection System), 침입차단시스템, 가상사설망, PKI, SSL 등이 있다. 특히 인터넷 뱅킹, 인터넷 트레이딩, 전자상거래 등 사용자의 개인정보 보호가 필수적인 데이터의 사용이 증가함에 따라 전송되는 사용자 데이터의 무결성을 보장하는 방법과 해킹피

† Corresponding author : 051-620-6471, sijeong@pknu.ac.kr

* 이 논문은 2002년도 부경대학교 연구년교수 지원에 의하여 연구되었음.

해로부터 웹 서버를 안전하게 지킬 수 있는 방법에 대한 관심이 증가하고 있다(이종후, 류재철 2000). 이렇게 인터넷에서 전송되는 데이터의 무결성을 보장하기 위한 방법 중 대표적인 것이 SSL (Secure Socket Layer)이다(Eric Rescorla, 2001).

<표 1> 해킹 기법 별 구분

| 공격수법 | 2003 | 2004 | | | | | | | | | | | | 2004년 총계 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| 사용자도용 | 46 | 0 | 2 | 0 | | | | | | | | | | 2 |
| S/W보안오류 | 1,620 | 0 | 1 | 0 | | | | | | | | | | 1 |
| 버퍼오버플로우 | 1,160 | 18 | 16 | 4 | | | | | | | | | | 38 |
| 구성설정오류 | 9,899 | 563 | 294 | 53 | | | | | | | | | | 910 |
| 악성프로그램 | 5,837 | 154 | 148 | 118 | | | | | | | | | | 420 |
| 프로토콜취약점 | 0 | 0 | 0 | 1 | | | | | | | | | | 1 |
| 서비스거부 | 30 | 0 | 0 | 0 | | | | | | | | | | 0 |
| E-mail관련 | 6,900 | 529 | 232 | 20 | | | | | | | | | | 781 |
| 취약점정보수집 | 4,937 | 153 | 146 | 790 | | | | | | | | | | 1,089 |
| 사회공학 | 0 | 0 | 0 | 0 | | | | | | | | | | 0 |
| 총계 | 30,429 | 1,417 | 839 | 986 | | | | | | | | | | 3,242 |

따라서 본 논문에서는 웹 환경에서 클라이언트와 서버간에 송수신되는 데이터의 무결성이 위배되었을 경우, SSL을 이용하여 데이터 무결성 위배 정보를 검증 및 관리할 수 있는 무결성 위배 관리 시스템을 구성하였다. 이러한 무결성 위배가 발생할 경우 웹 서버를 통해 위배 로그 데이터를 IDS(Intrusion Detection System)로 전송하여 침입 탐지정보와 함께 데이터의 무결성 검증 정보를 통합적으로 관리할 수 있도록 하는 IDS와 연계된 SSL 무결성 정보 관리 시스템을 구현하였다. 그리고, 본 시스템은 유선 환경뿐만 아니라 PDA기반의 무선 환경에서도 IDS에 접속하여 무결성 정보를 관리할 수 있도록 구성되어 있다. 본 연구의 구성은 제2장에서 관련 연구로 IDS 및 무결성 검증 시스템의 테스트를 위해 사용되는 변조 시스템에 대하여 설명하고, 3장에서는 본 연구에서 제안하는 SSL 무결성 검증을 위한 IDS 관리 시스템의 설계 및 구현에 대하여 기술한다. 4장에서는 구현된 시스템의 구현결과에 대하여 기술하고, 5장에서는 결론을 제시한다.

## Ⅱ. 관련 연구

본 장에서는 SSL 무결성 검증을 위한 IDS 관리를 위한 데이터 무결성 변조 시스템에 대하여 설명한다.

### 1. 침입탐지 시스템

가. 침입탐지 시스템 개요

침입탐지 시스템이란 네트워크를 통해 네트워크 시스템 자원을 오용하거나 비정상적인 행위로 데이터를 훼손하거나 서비스 불능상태로 만드는 보안 위협들을 탐지하여 그에 대응할 수 있는 시스템을 말한다. 침입 탐지 시스템은 네트워크 트래픽 또는 서버에 대해 의심스러운 행위를 감시 추적하며 감지된 행동에 따라 경고를 발생하거나 위협적인 행위를 차단할 수 있다(Stephen Northcutt, Judy Novak, 2001).

침입탐지 시스템은 침입 행위의 결과에 따라서 오용(Misuse) 탐지와 비정상적(Anomaly) 탐지 시스템으로 구분되며(<표 2>참조), 침입 자료

<표 2> 오용탐지 모델과 비정상적 탐지 모델의 비교

| 구분 | Misuse 방식 | Anomaly 방식 |
|---|---|---|
| 장점 | • 시스템 자원 비중이 적음<br>• 탐지 확률이 높음 | • 보편적인 통계적 처리 방법을 이용가능<br>• Misuse방식과 비교하여 보안 인적 자원 비중이 적음 |
| 단점 | • 신규 해킹 출현 시마다 새로운 signature 반영이 필요<br>• Signature 관리를 위한 보안 전문 인력이 필요 | • 시스템 자원의 비중이 요구됨<br>• 통계적 기준을 정함으로 탐지 결과의 확실성이 떨어짐 |

기반에 따라 호스트 기반 침입탐지 시스템과 다중 호스트 기반 침입탐지 시스템 그리고 네트워크 기반 침입탐지 시스템으로 분류된다.

(1) 침입 행위의 결과에 따른 분류

① 비정상적 탐지 모델

비정상적 탐지 모델(Anomalous Intrusion Detection)은 정상적인 행위패턴에서 벗어난 행위를 탐지하는 방법으로, 컴퓨터 자원의 비정상적인 행위에 근거하여 정의된 규정에서 이탈하는 경우로 예약된 시간을 위한하는 경우가 된다.

② 오용 탐지 모델

오용 탐지 모델 (Misuse Intrusion Detection)은 이미 알려진 공격패턴을 이용하는 것으로 시스템이나 응용 소프트웨어의 취약점이나 정의된 규정으로 침입을 할 경우 데이터베이스 또는 저장된 데이터를 이용하여 불법 침입을 탐지하는 방법으로 대부분의 IDS는 이러한 방법을 응용하고 있다.

(2) 침입 자료 기반에 따른 분류

① 호스트 기반 침입 탐지

컴퓨터 자체의 프로세스와 그것의 변수 그리고 OS에서 기본적으로 제공하는 로그 기록 등을 통해서 감사 자료를 수집하여 자체적인 불법 침입을 탐지하는 방법이다.

② 네트워크 기반 침입 탐지

네트워크 환경에서 전송되고 있는 패킷(packet)들을 수집하여 프로토콜의 불법적인 수정 또는 변경에 대해 감사 자료를 활용하여 불법 침입을 탐지하는 방법이다.

③ 다중호스트 기반 침입 탐지

다중호스트(multi-host) 환경에서 다양한 방법으로 각 호스트에 불법 침입하는 형태를 통합적으로 분석하여 불법 침입을 탐지하는 방법이다.

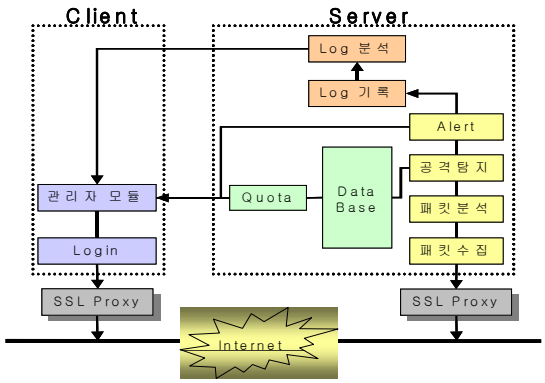
<표 3>은 네트워크 기반과 호스트 기반의 불법 침입 탐지에 대한 장·단점을 기술한 것이다.

<표 3> 호스트 기반과 네트워크 기반 침입 탐지 시스템 비교

| 구분 | 호스트 기반 | 네트워크 기반 |
|---|---|---|
| 장점 | • 콘솔 작업자의 공격을 차단 | • 저렴한 비용으로 효과적인 보안 처리가 가능<br>• 대규모 네트워크 지원<br>• 호스트 공격 전에 탐지 가능 |
| 단점 | • 관리와 유지보수가 어려움<br>• 대규모 네트워크 지원이 곤란<br>• 호스트 성능에 영향을 미침 | • 콘솔 작업자의 공격 탐지 못함 |

나. 네트워크 기반의 침입탐지 시스템

본 연구에서 적용한 침입탐지 시스템은 대부분의 IDS기법이 지원하는 네트워크 기반의 침입탐지 시스템을 구현하였다. 본 연구의 IDS는 서버에 탑재되어 실제 침입을 탐지하여 보고하는 침입탐지 보고 모듈과 침입 탐지를 위한 각종 설정 및 침입 탐지 로그 정보를 관리하는 관리자 모듈로 구성되어 있다. 관리자 모듈은 웹 환경에서 동작하도록 구성하여 원격지에서도 시스템 관리와 감독이 가능하도록 구현되어 있으며, SSL 통신을 통하여 클라이언트와 서버간의 안전한 통신을 보장한다. [그림 1]은 침입탐지 시스템의 전체 구성을 나타낸 것이다.



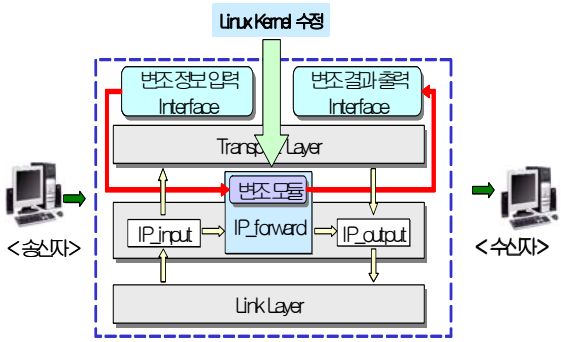

[그림 1] 네트워크 기반 IDS 구성도

## 2. 데이터 변조 시스템

데이터 무결성 변조 시스템은 응용계층의 전송 데이터를 중간에서 가로채어 변조시킨 후 목적지로 전달하는 역할을 수행한다. 변조 시스템은 RedHat 6.2기반에서 gcc를 이용하여 구현하였고, 데이터를 실제 변조하는 기능을 수행하는 패킷 변조 모듈과 변조할 패킷에 대한 정보 입력 및 변조 결과 조회 기능을 가진 사용자 인터페이스 모듈로 이루어진다(김창수, 2002).

### 가. 패킷 변조 모듈

변조모듈은 리눅스 시스템의 패킷 전송 원리를 이용하여 리눅스 시스템에서 제공하는 라이브러리를 이용하여 구현하였다(R Magnus, U Kunitz, M Dziadzka, DVerworner, M Beck, H Böhme, 1999). [그림 2]는 본 연구에서 구현한 변조 모듈의 전체 구성도를 나타낸 것이다.




[그림 2] 패킷 변조시스템 구성도

링크 계층을 통과한 패킷은 우선 ip_input버퍼에 저장되어 패킷의 목적지 주소를 확인한다. 목적지가 해당 호스트라면 전송계층으로 패킷이 전달되지만, 만약 그렇지 않다면 ip_forward와 ip_output버퍼를 통해 외부로 전송된다. 본 시스템에서는 패킷 변조 모듈을 ip_forward 버퍼루틴에 구현하여 변조 모듈에서 변조된 데이터는 ip_output버퍼를 거쳐 원래의 목적지로 전송되도록 설계되어 있다.

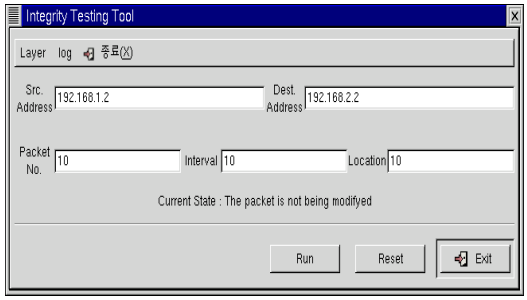
### 나. 사용자 인터페이스 모듈

사용자 인터페이스 모듈은 사용자가 선택한 패킷의 정보를 입력하여 패킷을 변조하고, 패킷의 변조 전·후 내용을 출력하는 기능을 수행한다. <표 4>는 패킷 변조를 위해 입력해야 할 항목의 내용을 나타낸 것이다.

<표 4> 패킷 변조를 위한 입력정보 항목

| 항 목 | 내 용 |
|---|---|
| Src Address | 변조할 패킷의 송신지 주소 |
| Dest Address | 변조할 패킷의 수신지 주소 |
| Packet No. | 변조할 패킷의 순서 번호 |
| Interval | 변조할 패킷의 간격 |
| Location | 패킷의 변조 시작점 |

[그림 3]은 변조를 위한 정보를 입력하기 위한 사용자 인터페이스를 나타낸 것으로 원 주소와 목적지 주소 그리고 변조할 패킷의 상대적인 번호 등에 대한 정보들이 입력된다.




[그림 3] 패킷 변조 입력 정보

## Ⅲ. IDS 관리 무결성 검증 시스템

본 장에서는 침입탐지 시스템과 연계된 유무선 통합 무결성 정보 관리 시스템의 전체 구성에 대해서 설명하고, 클라이언트로부터 받은 데이터에 대한 무결성 정보를 검증하고 관리하는 서버 시스템의 구성과 기록된 로그 데이터를 서버로부터 받아들여 유선 및 무선 환경에서 통합 관리가 가

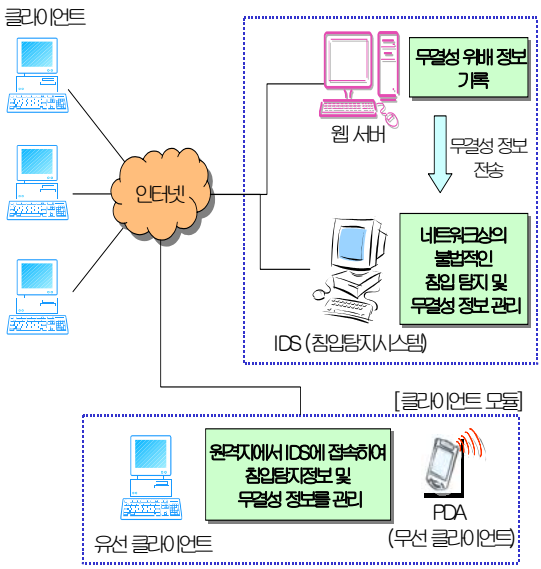
능한 IDS와 연계된 무결성 관리 시스템 구성에 대하여 설명한다.

## 1. 시스템 개요

일반적인 네트워크 구성에서 침입탐지 시스템은 침입탐지 시스템 내에 존재하는 모든 시스템을 관리하도록 되어 있다. 이러한 구성에서 관리자 클라이언트가 탐지 시스템 외부에 존재할 경우 네트워크 내부의 서버 간 통신에서 침입탐지 시스템은 웹 서버에 대한 공격은 탐지할 수 있으나 데이터 전송과 관련된 데이터 무결성은 관리하지 않으며, 만약 침입자가 외부 클라이언트와 서버 사이에 존재할 경우 전달되는 패킷이 위조 또는 변조 받을 가능성이 존재한다. 따라서 서버는 데이터의 무결성을 보장하기 위해 보안 모듈을 설치하는 것이 타당하며, Apache 웹 서버의 경우 SSL 모듈을 이용하여 데이터의 무결성을 보장할 수 있다(김창수, 2002).

본 연구서는 Apache와 mod_ssl, OpenSSL을 이용하여 구성한 보안통신이 가능한 웹 서버 시스템에 무결성 정보만을 관리할 수 있도록 하는 데이터 무결성 검증 및 관리 시스템을 구성한다. 그리고 무결성 정보를 IDS로 전송하여 침입탐지 정보와 함께 무결성 정보를 통합적으로 관리할 수 있는 시스템을 구현하였으며, 무결성 정보의 관리는 내부 네트워크뿐만 아니라 웹 환경을 통해서 원격지에서 통합 관리가 가능하도록 구성하였다.

[그림 4]는 무결성 정보관리 시스템의 전체 구성도를 나타낸 것이다. 웹 서버는 Apache+OpenSSL+mod_ssl을 사용하여 SSL 통신이 가능하도록 구성되어 있으며, 클라이언트와 웹서버는 https 통신을 하여 암호화된 데이터를 주고받는다. 이 때 외부 침입자에 의하여 송수신 데이터에 변조가 발생할 경우 웹 서버의 데이터 무결성 검증 및 관리 시스템에서 무결성과 관련된 오류 로그데이터를 기록하게 된다. 기록된 로그 데이터는 주기적으로 IDS에 전송이 되어 관리된다. 전송된 무결성 정보는 관리자가 유선 또는 무선 환경의 원격지에서 IDS에 접속하여 침입탐지 정보와 무결성 정보를 통합적으로 관리할 수 있도록 구성된다.




[그림 4] IDS와 연계된 정보관리 시스템 구성도

## 2. 무결성 검증관리 시스템

### 가. 구성환경

본 논문에서 설계하고 구현한 데이터 무결성 정보 검증 및 관리 시스템은 Apache 웹 서버 환경에서 무결성 정보를 관리할 수 있도록 설계되어 있다. 제안된 시스템은 리눅스 기반으로 보안통신이 가능하도록 설정하기 위하여 <표 5>와 같은 웹 서버 환경을 구성하였다. 시스템 구성은 Apache와 OpenSSL 그리고 mod_ssl를 활용하여 access_log, error_log, ssl_engine_log, ssl_request_log의 4가지 로그파일들이 기록될 수 있으며, 이 중 SSL 통신과 관련된 정보는 ssl_engine_log와 ssl_request_log에 기록되도록 하였다.

<표 5> 웹 서버 구성 환경

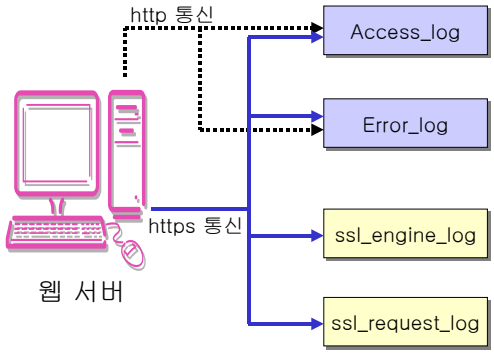
| 항 목 | 내 용 |
|---|---|
| 운영체제 | WOW-Linux 7.3 Paran |
| SSL 라이브러리 | OpenSSL 0.9.7 |
| 웹 서버 | Apache 1.3.28 |
| SSL 모듈 | mod_ssl 2.8.15 |
| DB | MySQL 3.23.38 |

<표 6>은 Apache+mod_ssl 웹 서버 시스템에서 각각의 로그 파일에 기록되는 항목들을 요약한 것으로 각 항목들에 대한 기록 내용 나타낸 것이다.

<표 6> Apache 웹 서버의 로그기록

| 항 목 | 내 용 |
|---|---|
| access_log | • 웹 서버에 접근되어지는 모든 정보를 기록<br>• 방문자 정보를 얻는데 중요한 역할을 담당 |
| error_log | • 웹 서버 운영중 발생하는 모든 오류 정보를 기록 |
| ssl_engine_log | • https 통신을 통해 동작하는 내용에 대한 정보를 기록 (error / warn / info / trace / debug / NULL로 구분됨) |
| ssl_request_log | • https 통신으로 웹 서버에 접근되어지는 정보를 기록 |

[그림 5]는 Apache 웹 서버에서의 로그 데이터 기록 방법에 대하여 나타내고 있다. Apache 웹 서버는 access_log와 error_log에 대하여 자체적으로 관리할 수 있는 기능 및 프로그램을 제공하지만[8], 보안 통신을 하는 중에 기록되는 SSL과 관련된 로그 데이터에 대한 관리 기능은 제공하지 않는다. 그리고 무결성 오류가 발생했을 경우 필요로 하는 주요 정보(Client/Server IP, Port Number등)가 기록되지 않으며, 오류와 관련된 내용만을 기록할 수 있는 것이 아니라 SSL 통신과 관련된 모든 내용을 기록하도록 구성되어 있다.




[그림 5] Apache 웹 서버의 로그 기록 방법

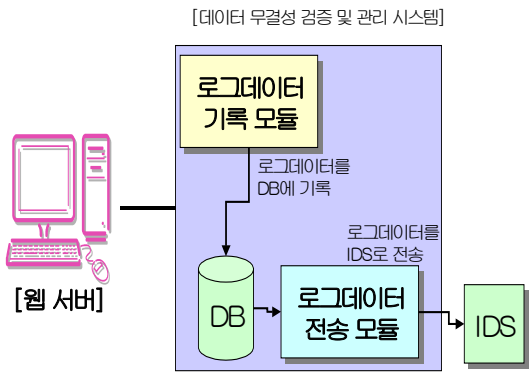
따라서 본 연구에서는 데이터 전송시 발생하는 무결성 오류에 대한 정보를 기록할 수 있는 모듈을 추가하여 무결성 정보만을 관리할 수 있도록 하였고, 파일로 기록되는 로그 데이터를 DB에 기록하여 효율적으로 관리할 수 있도록 구성하였다. 그리고 로그 데이터 기록 항목을 재정의하여 IDS와 연계된 SSL 무결성 관리 시스템을 통해 효율적인 정보 관리가 가능하도록 하였다.

나. 데이터 무결성 관리시스템 구성

[그림 6]은 데이터 무결성 관리 시스템을 나타낸 것으로, 클라이언트와 서버가 통신을 할 때 서버가 무결성이 위배된 데이터를 수신했을 경우 무결성 위배 정보를 기록하는 로그데이터 기록 모듈과 IDS에서 무결성 검증 정보를 통합적으로 관리할 수 있도록 서버에 기록된 로그 데이터를 주기적으로 IDS에 전송하는 기능을 수행하는 로그데이터 전송 모듈로 구성된다.

(1) 로그데이터 기록 모듈

로그데이터 기록 모듈에서는 클라이언트와 서버간의 통신에서 무결성 에러가 발생하게 되면 무결성 로그데이터 기록 함수를 통하여 오류 로그를 데이터베이스에 기록하게 된다. 본 연구에서는 로그데이터의 데이터베이스 기록을 위해 MySQL을 사용하였다.



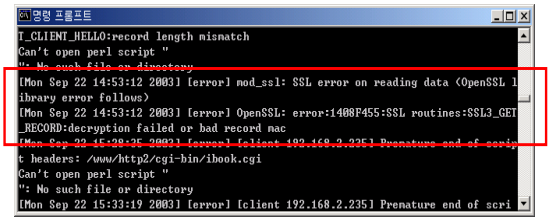

[그림 6] 데이터 무결성 관리시스템 구성

기존의 Apache 웹 서버에서 무결성 에러가 발생하였을 때 error_log와 ssl_engine_log에 기록되는 로그데이터의 형식은 [그림 7]과 같다. (a)와 (b)에서 볼 수 있듯이 하나의 무결성 오류에 대하여 mod_ssl의 모듈에서 기록하는 SSL 통신 시 무결성 에러가 발생하였다는 정보와 OpenSSL 함수에 의해 기록되는 OpenSSL 라이브러리로부터 받아오는 오류 내용에 대한 정보를 받아와 출력하게 되다. 이 경우 하나의 에러 발생에 대해서 두 Line으로 로그 데이터가 기록되기 때문에 관리하기가 어려워지며, 오류 발생시 서버와 통신을 하는 클라이언트에 대한 정보가 기록되지 않기 때문에 오류에 대한 구체적인 정보를 얻을 수 없다. 따라서 본 연구에서는 통합 관리 시스템을 통한 로그 데이터를 효율적으로 관리하기 위하여 오류 발생 시 기록되는 로그 데이터의 포맷을 새로 정의하여 로그 DB에 기록되도록 구성하였다.

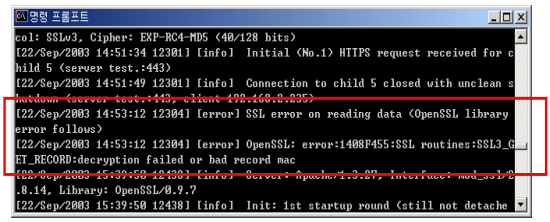
[그림 8]은 오류 발생 시 데이터베이스에 저장되는 로그 데이터의 포맷을 나타낸 것으로, 각 필드의 항목과 관련 내용은 다음과 같다.

① Data : 오류가 발생하여 로그 데이터가 기록된 날짜

② Time : 오류가 발생하여 로그 데이터가 기록된 시간




(a) error_log 파일 내용




(b) ssl_engine_log 파일 내용

[그림 7] 무결성 오류 발생시 Apache 로그 기록 내용

③ Pid : 프로세스 ID

④ Error Reason : 오류 발생 원인에 대하여 기록

⑤ Server IP : 웹 서버의 IP를 기록

⑥ Client IP : 웹 서버와 통신하는 클라이언트의 IP를 기록

⑦ Client Port : 클라이언트와 서버 간 연결되어 있는 Port 번호 기록

⑧ Error Code : 오류에 대한 구체적인 내용을 기록

| Data | Time | Pid | Error Reason | Server IP | Client IP | Client Port | Error Code |
|---|---|---|---|---|---|---|---|

[그림 8] 무결성 에러 로그들에 대한 데이터베이스 포맷

위와 같이 기록된 로그 데이터는 로그 데이터 전송 모듈을 통하여 주기적으로 IDS 통합 시스템으로 전송되어 관리되도록 구성하였다

(2) 로그 데이터 전송 모듈

로그 데이터 전송 모듈은 웹 서버에 저장된 무결성 로그 데이터를 IDS에 주기적으로 특정 크기의 데이터를 전송하는 기능을 수행한다. 이는 IDS로 주기적으로 전송하기 위하여 전송 모듈은 cron에 등록하여 주기적으로 실행되도록 설정되며, 설정된 전송 모듈은 주기적으로 실행되어 로그 데이터 DB에 접속하게 된다. 그리고, SQL의 쿼리문을 사용하여 전송하고자 하는 로그 데이터의 범위를 결정한 후 선택된 로그 데이터를 IDS로 전송하게 된다.

## 3. IDS연계 통합 관리 시스템

가. 구성환경

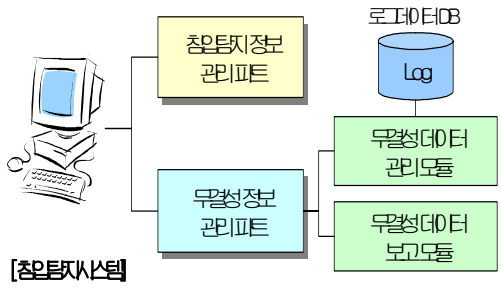
웹 서버로부터 전송된 무결성 오류 로그 데이터는 IDS로 주기적으로 전송되어 무결성 로그 데이터 관리 DB에 기록되며, IDS에 의해 탐지된 침입탐지 정보와 함께 IDS의 관리자 모듈을 통하여 통합적으로 관리되게 된다. 본 연구에서 사용된 IDS의 구성 환경은 <표 7>과 같다.

IDS와 연계된 무결성 데이터 통합 관리 시스템은 침입탐지 정보를 관리하는 파트와 웹 서버로부터 전송 받은 무결성 정보를 관리하는 파트로 나누어지며, 무결성 정보 관리 파트는 로그 데이터 파일을 저장하고 관리하는 무결성 데이터 관리 모듈과 관리자가 무결성 데이터에 대하여 조회 및 검색을 할 수 있도록 하는 무결성 데이터 보고 모듈로 구성된다.

<표 7> IDS 구성 환경

| 항 목 | 내 용 |
|---|---|
| 운영체제 | Solaris 2.8 (SunOS 5.8) |
| SSL 라이브러리 | OpenSSL 0.9.7 |
| 웹 서버 | Apache 1.3.21 |
| Compiler | gcc 2.95.2 |
| Java Language | Java SDK 1.1.7 |
| DB | MySQL 3.23.38 |

[그림 9]는 침입탐지 시스템과 연계하여 무결성 정보를 관리할 수 있도록 하는 IDS 통합 관리 시스템의 전체 구성을 나타내고 있다. 침입탐지시스템은 탐지정보 관리영역과 무결성 정보 관리 영역 그리고 전송된 로그 데이터 관리 영역으로 구성되어 있다.



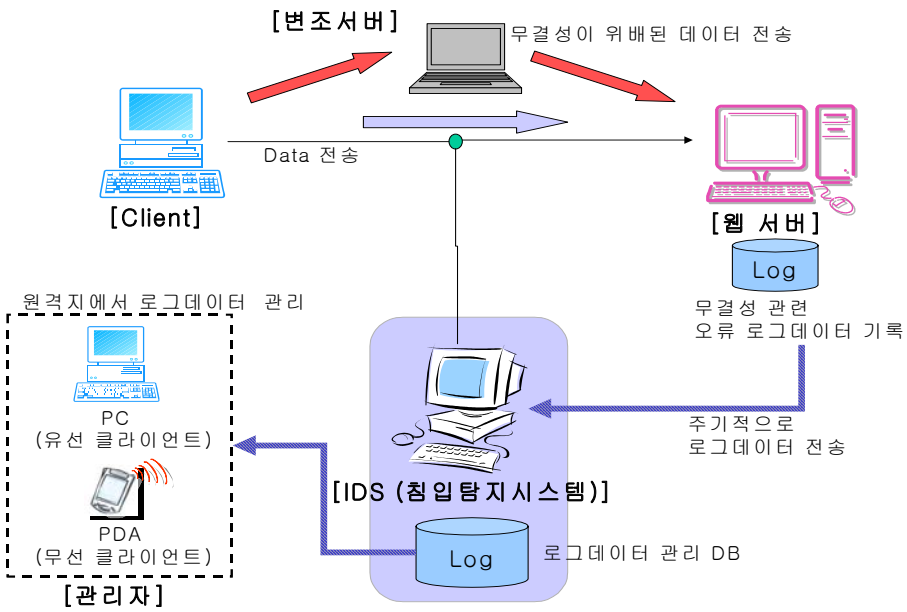

[그림 9] IDS 통합 관리 시스템 구성도

나. 무결성 데이터 관리 모듈

무결성 데이터 관리 모듈은 웹 서버로부터 전송 받은 로그 데이터를 관리하는 기능을 수행한다. 웹 서버로부터 전송 받은 로그 데이터는 무결성 데이터 관리 모듈을 통하여 DB에 저장되며, 로그 데이터가 커지는 것을 막기 위하여 로그 데이터를 백업하는 기능을 수행한다.

다. 무결성 데이터 보고 모듈

통합관리 시스템의 관리자 모듈은 WWW (World Wide Web) 환경에서 동작하도록 구성되어 있어 관리자는 인터넷 접속이 가능한 유선 및 무선 환경의 원격지에서 웹 브라우저를 이용하여 IDS 통합관리 시스템에 접속해 침입탐지 정보 및 무결성 정보의 관리를 할 수 있다. 관리자는 무결성 데이터 조회 인터페이스를 통하여 웹 서버로부터 전송 받은 로그 데이터를 조회할 수 있으며 검색이 가능하도록 구성된다. 그리고 원격지에서 로그 데이터의 삭제가 가능하도록 한다.




[그림 10] 제안된 IDS 전체 구성도

## Ⅳ. 구현 및 테스트 결과

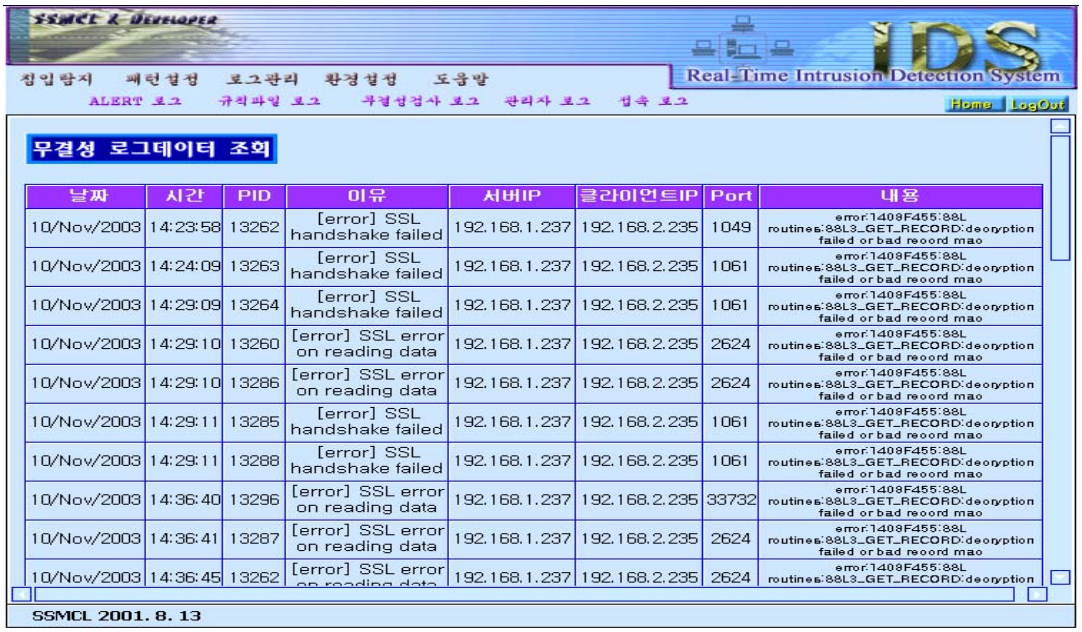
### 1. 구현된 전체 시스템 구성

본 연구에서는 [그림 10]과 같이 웹 서버와 침입탐지시스템의 외부에 있는 클라이언트간의 데이터 무결성을 보호하고 무결성 위배 정보를 효율적으로 관리하기 위한 통합 관리 시스템을 설계 및 구현하였다. 본 시스템이 어떻게 동작하는지 확인하기 위하여 무결성이 위배된 데이터가 전송되었을 때 웹 서버 및 IDS 통합 시스템의 처리 내용에 대하여 살펴보도록 한다.

클라이언트와 웹 서버는 OpenSSL을 이용하여 SSL 보안 통신을 하게 된다. 이 때 변조 서버 시스템을 통하여 클라이언트에서 서버로 보내는 데이터를 변조하여 전송하였을 때 웹 서버에 설치된 무결성 정보 검증 및 관리 시스템을 통해 무결성 위배 로그 데이터가 DB로 저장되는 것을 확인한다. 그리고 주기적으로 무결성 정보 검증 및 관리 시스템에서 무결성 위배 로그 데이터가 IDS 통합 시스템으로 전송되어 기록되면 관리자는 유선 클라이언트 또는 무선 클라이언트에서 IDS 통합 시스템에 접속하여 무결성 로그 데이터를 관리하도록 하였다.

### 2. 정상 탐지 수행 결과

[그림 11]은 무결성 위배 정보가 DB에 기록된 것을 캡처한 것이다. IDS로 전송되었을 때 효율적인 로그 데이터 관리가 가능하도록 무결성 오류와 관련된 로그 데이터들만 정의된 포맷에 맞추어 기록되었으며, 추가적인 정보가 기록됨을 확인할 수 있다. [그림 12]는 관리자가 침입탐지서버 시스템으로부터 불법 침입에 대한 정보들을 유선의 클라이언트에 전달하게 되는데, 본 연구에서는 관리자가 무선환경에서도 이러한 정보들을 검색할 수 있도록 PDA 환경에서 로그 데이터를 조회할 수 있도록 구성하였다. 이러한 서비스를 위해서 PDA 환경에 적합한 관리 모듈의 개발이 필요하다.




| 날짜 | 시간 | PID | 이유 | 서버IP | 클라이언트IP | Port | 내용 |
|---|---|---|---|---|---|---|---|
| 10/Nov/2003 | 14:23:58 | 13262 | [error] SSL handshake failed | 192.168.1.237 | 192.168.2.235 | 1049 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:24:09 | 13263 | [error] SSL handshake failed | 192.168.1.237 | 192.168.2.235 | 1061 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:29:09 | 13264 | [error] SSL handshake failed | 192.168.1.237 | 192.168.2.235 | 1061 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:29:10 | 13260 | [error] SSL error on reading data | 192.168.1.237 | 192.168.2.235 | 2624 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:29:10 | 13286 | [error] SSL error on reading data | 192.168.1.237 | 192.168.2.235 | 2624 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:29:11 | 13285 | [error] SSL handshake failed | 192.168.1.237 | 192.168.2.235 | 1061 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:29:11 | 13288 | [error] SSL handshake failed | 192.168.1.237 | 192.168.2.235 | 1061 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:36:40 | 13296 | [error] SSL error on reading data | 192.168.1.237 | 192.168.2.235 | 33732 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:36:41 | 13287 | [error] SSL error on reading data | 192.168.1.237 | 192.168.2.235 | 2624 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac |
| 10/Nov/2003 | 14:36:45 | 13262 | [error] SSL error on reading data | 192.168.1.237 | 192.168.2.235 | 2624 | error:1408F455:SSL routines:SSL3_GET_RECORD:decryption |

[그림 11] 유선환경의 로그 데이터


[그림 12] 무선 환경의 로그 데이터

## V. 결 론

본 연구에서는 클라이언트와 서버간에 송수신되는 데이터의 무결성이 위배되었을 경우 무결성 위배 정보를 효율적으로 관리하는 침입탐지 시스템를 설계하였으며, 이와 연계하여 유무선 통합 SSL 무결성 정보 관리 시스템을 구성하였다. 제안한 시스템은 데이터 무결성 기능을 추가하기 위해 SSL 기법을 이용하여 IDS 외부에 있는 클라이언트 시스템과 IDS 내부에 있는 서버 간의 송수신되는 데이터 무결성 기능을 검증하는 것은 물론 변조된 데이터에 대해 관리가 가능한 시스템 환경을 제안하였다. 그리고 관리자가 무선 환경에서도 이러한 무결성 위배 정보를 관찰할 수 있는 기능들도 포함하고 있다.

## 참고 문헌

이종후, 류재철 “인터넷 보안”, Telecommunication Review, 제 10권 5호, 2000.

George Reese, Randy Jay Yarger, Tim King, "Managing & Using MySQL, 2nd Edition", O'Reilly, 2002. 4.

Horie, T., Harada, T., Tanaka, K., “Adaptive Access Policy for the Linux Kernel”, Applications and the Internet Proceedings. pp.82~88, 2005. 1.

김창수, “네트워크 기반의 침입탐지 시스템”, 부경대학교 연구보고서, 2002. 6.

J.Viega, M. Messier, P. Chandra, "Network Security with OpenSSL", O'REILLY, 2002. 6.

R Magnus, U Kunitz, M Dziadzka, DVerworner, M Beck, H Böhme "Linux Kernel Internals" pp.258~315, 1999.

Stephen Northcutt, Judy Novak,"Network Intrusion Detection An Analyst's Handbook", Information Publish, 2001.

Wagner,D. and Scheneier,B. , "Analysis of the SSL 3.0 Protocol", 2nd USENIX Workshop on Electronic Commerce Proceedings, 1996.

정관진, “아파치 로그파일의 이해와 분석”, http://www.apache.kr.net/documents/log_storyII.html

이영무, “최강 MySQL 바이블”, 가메출판사, 2003. 3.

한국정보보호진흥원 “3월 해킹바이러스 통계 및 분석 월보” 2004. 3.

Eric Rescorla "SSL and TLS", Addison-Wesley Press, 2001.