

# 침입탐지시스템과 연계된 SSL 무결성 정보 관리 시스템 구현

김남진\*, 강진수\*, 김창수\*, 김진천\*\*

\*부경대학교 전자계산학과

\*\*경성대학교 컴퓨터공학과

## Implementation of Management System for SSL Integrity Data with Intrusion Detection System

Nam-jin Kim\*, Jun-soo Kang\*, Chang-soo Kim\*, Jin-chun Kim\*\*

\*Dept. of Computer Science, PuKyong Nat'l University

pansonnet@ssmcl.pknu.ac.kr, ids@pknu.ac.kr, cskim@pknu.ac.kr

\*\*Dept. of Computer Engineering, KyungSung University

jckim@star.ks.ac.kr

### 요약

네트워크 상에서 송수신되는 데이터를 외부의 침입으로부터 보호하는 것은 매우 중요하며, 그 중 데이터의 무결성을 검증하고 보장하기 위한 방법으로 SSL(Secure Socket Layer)을 사용한다.

본 논문에서는 웹 환경에서 클라이언트와 서버간에 송수신되는 데이터의 무결성이 위배되었을 경우, 그 정보를 검증 및 관리할 수 있는 무결성 위배 데이터 검증 및 관리 시스템을 OpenSSL을 이용하여 구성하고, 웹 서버를 통해 기록된 무결성 위배 로그 데이터는 IDS(Intrusion Detection System)로 전송하여 침입 탐지 정보와 함께 데이터의 무결성 검증 정보를 통합적으로 관리할 수 있도록 IDS와 연계된 무결성 정보 통합관리 시스템을 제안 및 설계하고자 한다.

### 1. 서 론

정보통신 기술의 발달로 인터넷은 사람들의 생활의 일부로 자리잡게 되었고, 사람들은 다양한 정보를 공유하거나 재활용할 수 있게 되었다. 그러나, 사용자의 수가 증가함에 따라 네트워크를 통한 컴퓨터 시스템 침입으로 인한 보안 침해 사례가 증가하고 있으며, 그 피해상황 역시 커지고 있는 실정이다. 2003년 9월 한국정보보호진흥원(CCRTCC-KR)에서 발표한 2003년 9월 침해 사고 접수 및 처리 현황"을 참고하면 최근 국내의 해킹은 방법과 대상이 다양해지고 발생 건수가 꾸준히 늘어나고 있음을 볼 수 있다[1].

표 1. 해킹탐지 보고 현황

구분	2002	2003												2003 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
일반 해킹	6,884	1,120	612	934	923	1,012	1,078	995	1,311	1,179				9,458
밀번 험	2,071	974	522	1,159	771	221	307	48	423	119				4,645
스팸발송	5,537	469	592	1,308	1,616	1,004	436	774	301	122				7,322
합계	15,192	2,563	1,826	3,400	3,310	3,187	1,818	1,819	2,058	1,429				21,329

표 2. 공격수법 별 구분

공격수법	2002	2003												2003 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
사용자도용	147	12	9	7	4	1	3	3	1	1				41
SW보안인증	802	190	34	863	452	92	14	0	3	1				1,616
비밀번호 зло	243	445	28	26	43	42	47	42	392	26				1,022
구성설정도용	4,358	733	802	2,059	1,300	2,301	395	392	243	101				8,475
악성프로그램	4,112	1,148	557	1,222	934	308	450	185	544	119				5,475
프로토콜종류도용	1	0	0	0	0	0	0	0	0	0				0
서버스거부	18	29	0	0	0	0	0	1	0	0				39
F-mailなり	1,043	258	248	1,018	1,617	1,905	269	353	137	83				5,925
취약점정보수집	3,271	703	535	1,219	930	303	440	171	175	113				4,523
사회학습	0	0	0	0	0	0	0	0	0	0				0
총계	15,676	3,468	2,017	6,456	5,930	4,880	1,829	1,151	1,455	423				27,711

이러한 침입시도나 공격으로부터 데이터를 보호하기 위해 인터넷 보안 솔루션에 대한 연구가 활발히 진행되고 있으며, 특히 인터넷 뱅킹, 전자상거래 등 사용자의 개인정보 보호가 필수적인 데이터의 사용이 증가되면서 데이터 무결성에 대한 관심이 증가하고 있다. 이렇게 인터넷에서 전송되는 데이터의 무결성을 보장하기 위한 방법 중 대표적인 것이 SSL (Secure Socket Layer)[2]이다.

본 논문에서는 웹 환경에서 클라이언트와 서버간에

송수신되는 데이터의 무결성이 위배되었을 경우, SSL을 이용하여 그 정보를 검증 및 관리할 수 있는 무결성 위배 데이터 검증 및 관리 시스템을 구성하고, 웹 서버를 통해 기록된 무결성 위배 로그 데이터를 IDS(Intrusion Detection System)로 전송하여 침입 탐지 정보와 함께 데이터의 무결성 검증 정보를 통합적으로 관리할 수 있도록 하는 IDS와 연계된 SSL 무결성 정보 관리 시스템을 제안 및 설계하였다.

## 2. 관련 연구

### 2.1 SSL의 개요

SSL(Secure Socket Layer)은 Netscape Communications사에서 Netscape 웹 브라우저 보안을 위해 제안한 응용 계층 보안 프로토콜로써, 데이터의 암호화 및 서버 인증, 메시지 무결성 기능을 제공한다. 그림 1은 네트워크 계층에서의 SSL의 위치와 프로토콜의 구조를 나타낸 것이다. SSL은 웹 보안을 염두에 두고 만든 프로토콜이기 때문에 TCP 상위계층에 존재하며, 응용계층의 데이터에 대한 보안을 수행한다.

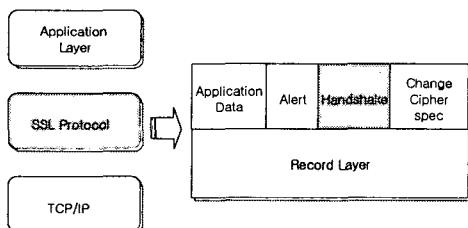


그림 1. SSL 프로토콜의 위치 및 구조

SSL 프로토콜은 Handshake Layer와 Record Layer로 구성되며, Handshake Layer는 Application Data 프로토콜, Alert 프로토콜, Handshake 프로토콜, Change Cipher Spec 프로토콜로 구성된다. 그림 2는 SSL에서 제공하는 무결성 제공 기능을 도식화 한 것이다. 클라이언트는 서버에게 Handshake 프로토콜을 통해 안전한 통신을 요청하고, 서버는 그 요청에 응답하여 통신에 필요한 파라미터들을 설정한다. 설정된 파라미터들은 Change Cipher Spec 프로토콜로 사용될 수 있도록 활성화되고, 데이터들은 Application Data 프로토콜을 통하여 SSL에 의하여 보호되어 전송된다. 전송과정에서 발생한 오류는 Alert 프로토콜을 통해 처리되며, 각 프로토콜의 모든 데이터는 Record layer를 통하여 전송된다[3]. SSL Record의 Data Fragment에 대해 MAC값을 계산한 후, Data

fragment와 MAC값을 함께 암호화하여 전송한다. 그리고 수신측의 SSL은 암호화된 SSL Record를 복호화 한 후, 수신된 MAC값과 Data fragment에서 계산한 MAC값의 일치 여부로 무결성을 검증한다[4].

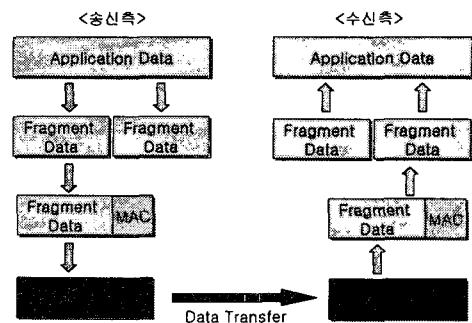


그림 2. SSL 프로토콜의 무결성 제공 과정

## 3. IDS 통합 시스템 설계

### 3.1 전체 시스템 개요

본 장에서는 침입탐지 시스템과 연계된 무결성 정보 통합관리 시스템의 전체 구성에 대해서 설명하고, 클라이언트로부터 받은 데이터에 대한 무결성 정보를 검증하고 관리하는 서버 시스템의 구성 및 기록된 로그 데이터를 서버로부터 받아들여 통합 관리하는 IDS와 연계된 SSL 무결성 정보 관리 시스템의 구성에 대하여 설명한다. 그림 3은 무결성 관리를 위한 IDS 통합 시스템의 전체 구성을 보여준다.

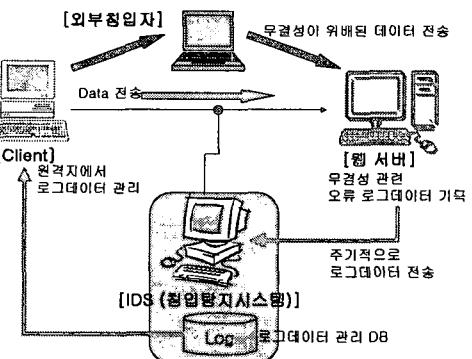


그림 3. IDS 통합 시스템 전체 구성도

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 무결성 위배 정보

검증 및 관리 시스템에서 무결성과 관련된 오류 로그 데이터를 기록하게 된다. 기록된 로그 데이터는 주기적으로 IDS에 전송이 되며, 전송된 로그데이터는 IDS에 의해 관리된다. 시스템은 관리자가 IDS에 의해 관리되는 무결성 정보는 관리자가 원격지에서 IDS에 접속하여 IDS에 의해 탐지되는 침입탐지 정보와 웹서버에 의해 탐지되어 전송된 무결성 정보를 통합적으로 관리할 수 있도록 구성된다.

### 3.2 무결성 정보 검증 및 관리 시스템

무결성 정보 검증 및 관리 시스템은 클라이언트와 서버가 통신을 할 때, 서버가 무결성이 위배된 데이터를 수신했을 경우 무결성 위배 정보를 기록하는 로그 데이터 기록 모듈과, IDS에서 무결성 검증 정보를 통합적으로 관리할 수 있도록 서버에 기록된 로그 데이터를 주기적으로 IDS에 전송하는 기능을 수행하는 로그데이터 전송 모듈로 구성된다. 그림 4는 무결성 검증 및 관리 시스템의 구성을 나타낸 그림이다.

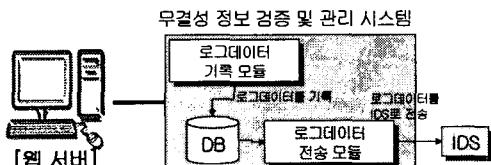


그림 4. SSL을 통한 무결성 검증 및 관리 시스템 구성도

본 논문에서는 무결성 정보 검증 및 관리 시스템의 구성을 위하여 표 3과 같은 환경에서 웹 서버를 구성하였고, 클라이언트에서 서버로 전송되는 데이터의 무결성을 위배시키기 위해서 본 연구실에서 개발한 변조 서버 시스템을 사용하여 데이터의 변조를 수행하였다[5].

표 3. 웹 서버 구축 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

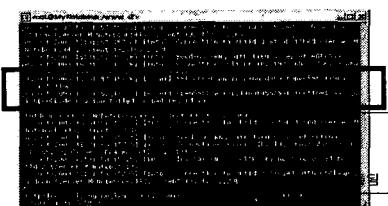
데이터 변조를 수행하게 되면, 웹 서버는 변조에 따른 무결성 오류 정보를 로그파일에 기록하게 된다. Apache+OpenSSL+mod\_ssl을 이용하여 웹 서버를 구축하면 access\_log, error\_log, ssl\_engine\_log, ssl\_request\_log의 4가지 로그파일이 기록되는데, 이중 ssl\_engine\_log에 SSL통신과 관련된 모든 정보가 기록되게 된다[8]. Apache 웹 서버는 이러한 각각의 로그파일에 대하여 자체적으로 관리할 수 있는 기능

을 제공하지만[6], 무결성 오류가 발생했을 경우 필요로 하는 주요 정보(Client/Server IP, Port Number 등) 가 기록되지 않으며 무결성 오류와 관련된 내용만을 뽑아내는 기능은 제공하지 않는다. 그러므로, 본 논문에서는 데이터 전송시 무결성 오류 로그를 기록할 수 있는 모듈을 추가하여 무결성 정보만을 관리할 수 있도록 하였고, 로그 데이터 기록 항목을 재정의하여 IDS와 연계된 SSL 무결성 관리 시스템을 통해 효율적인 정보 관리가 가능하도록 하였다[9][10]. 그림 5는 오류 발생시 저장되는 로그 데이터의 포맷을 나타낸다.

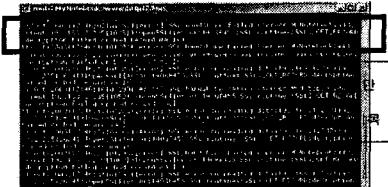
Data	저장된 시간
Time	저장된 날짜
Pid	프로세스 ID
Error Reason	에러 발생 이유
Server IP	서버IP
Client IP	클라이언트IP
Client Port	서버와 연결된 클라이언트의 포트번호
Error Code	에러내용

그림 5. 무결성 로그 데이터 포맷

그림 6의 (a)는 원래 Apache 로그파일의 내용을 나타낸 것이고, (b)는 무결성 정보 검증 및 관리 시스템의 로그를 나타낸 것이다. 이렇게 기록된 로그 데이터는 주기적으로 IDS 통합 시스템으로 전송되어 관리되게 된다.



(a) Apache의 로그파일



(b) 무결성 정보 검증 및 관리시스템 로그파일

그림 6. 웹서버에 기록된 로그파일

### 3.3 IDS 통합 시스템 설계

웹 서버로부터 전송된 무결성 오류 로그 데이터는 IDS로 주기적으로 전송되어 무결성 로그 데이터 DB에 기록되며, IDS에 의해 탐지된 침입탐지 정보와 함께 IDS의 관리자 모듈을 통하여 통합적으로 관리가

가능하다. 본 논문에서 설계한 침입탐지 시스템과 연계된 무결성 정보 통합관리 시스템에 사용되는 침입탐지 시스템은 본 연구실에서 개발한 네트워크 기반의 침입탐지 시스템을 사용하였다[7].

통합관리 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 보고모듈로 구성된다. 그림 7은 침입탐지 시스템과 연계하여 무결성 정보를 관리할 수 있도록 하는 IDS 관리 모듈의 구성을 나타낸 그림이다.

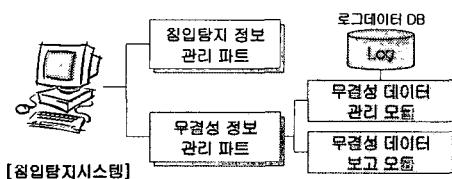


그림 7. IDS 관리 모듈 구조도

통합관리 시스템의 관리자 모듈은 WWW (World Wide Web) 환경에서 동작하도록 구성되어 있어 관리자는 인터넷 접속이 가능한 원격지에서 웹 브라우저를 이용하여 IDS 통합관리 시스템에 접속해 침입탐지 정보 및 무결성 정보의 관리를 할 수 있다. 그림 8은 원격지의 클라이언트에서 무결성 정보 관리 시스템에 접속하여 무결성 로그 데이터를 조회하는 화면을 보여준다.

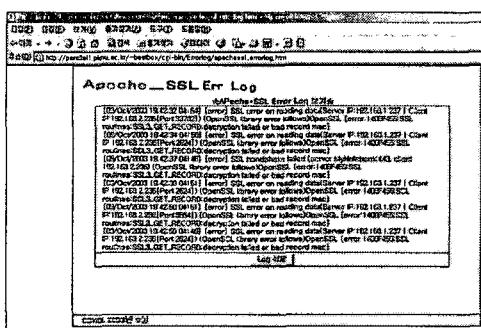


그림 8. 무결성 위반 로그 데이터 출력 메시지

4. 절문

본 논문에서는 클라이언트와 서버간에 송수신되는 데이터의 무결성이 위배되었을 경우, 무결성 위배 정보를 효율적으로 검증 및 관리하여 외부의 침입으로

부터 대응할 수 있도록 하는 침입탐지 시스템과 연계된 SSL 무결성 정보 관리 시스템을 설계하였다. 본 논문에서 제안한 시스템은 무결성 정보 검증 및 관리 시스템과 IDS 통합 시스템으로 구성되어 있으며, 클라이언트와 서버간에 송수신되는 데이터에 대한 무결성을 검증하고 그 정보를 통합적으로 관리하는 방법을 제안하고 실제 클라이언트와 서버 사이의 변조된 데이터에 대해 무결성을 검증 및 관리하는 모듈을 구현하였다. 그리고 이러한 무결성 위배 정보들의 효율적인 관리를 위해 침입탐지시스템과 연계한 통합 관리시스템을 제안하고 설계하였다.

향후 연구로는 무결성 정보 검증 및 관리 시스템에서 로그 데이터의 용량 관리 기능 및 로그 데이터 전송과 관련된 옵션 기능의 추가 작업이 필요하며, 원격지에서 IDS 통합 시스템에 접속하였을 때 사용자가 편리하게 조회하고 관리할 수 있도록 인터페이스의 개선 및 기능 추가 작업을 수행해야 한다. 마지막으로, 유선환경에서의 관리 뿐 아니라 무선환경에서도 IDS 통합 시스템을 조회 및 관리할 수 있도록 시스템을 구성할 계획이다.

### [참 고 문 헌]

- [1] 한국정보보호진흥원, “2003년 9월 해킹바이러스 통계 및 분석 월보”, 2003, <http://www.certcc.or.kr>
  - [2] Eric Rescorla “SSL and TLS”, Addison-Wesley Press, 2001
  - [3] 이동훈, 임채훈, “SSL 3.0과 TLS 1.0의 비교분석”, 2000.11, (주)퓨처시스템 기술 문서
  - [4] 김기육, 정경훈, 장용호, 김창수, “무선 인터넷 보안을 위한 SSL 활용 연구”, 한국멀티미디어학회 춘계 학술발표 대회 논문집, 2001
  - [5] 김창수, “정보보호시스템 무결성 기능평가 S/W 개발”, 한국정보보호센터 연구보고서, 1999
  - [6] <http://apache.kr.net/#intro>
  - [7] 김남진, 강진수, 김창수, “네트워크 기반의 실시간 침입탐지 시스템 설계 및 구현”, 한국 정보보호학회 영남지부 학술발표대회 논문집, 2002.2
  - [8] 정관진, “아파치 로그파일의 이해와 분석”, [http://www.apache.kr.net/documents/log\\_story.html](http://www.apache.kr.net/documents/log_story.html)
  - [9] J. Viega, M. Messier, P. Chandra, “Network Security with OpenSSL”, O'REILLY, 2002. 6.
  - [10] Wagner,D. and Schneier,B., “Analysis of the SSL 3.0 Protocol,” 2nd USENIX Workshop on Electronic Commerce Proceedings, 1996.