무결성 관리를 위한 IDS 통합 시스템 설계

김남진* · 강진수* · 김창수*
*부경대학교 전자계산학과

Design of IDS Unified System for Integrity Managements

Nam-jin Kim* · Jin-soo Kang* · Chang-soo Kim*
*Dept. of Computer Science, Pukyung National University
E-mail : pansonnet@ssmcl.pknu.ac.kr

요 약

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 클라이언트와 서버간에 송수신되는 데이터의 무결성이 위배되었을 경우 그 정보를 검증 및 관리할 수 있도록 OpenSSL을 이용한 무결성 위배 데이터 검증 및 관리 시스템을 구성하고, 검증된 데이터를 IDS(Intrusion Detection System)로 전송하여 침입 탐지 정보와 무결성 검증 정보를 통합적으로 관리할 수 있는 IDS 통합 시스템을 제안 및 설계하였다.

키워드
무결성, SSL, IDS, 통합 시스템

Ⅰ. 서 론

1990년대 WWW(World Wide Web)이 알려지기 시작하고, 정보통신 기술이 급속도로 발전하면서 인터넷의 사용은 우리의 생활의 일부로 자리잡게 되었다. 인터넷의 확산으로 인해 사람들은 다양한 정보 공유 및 재활용이 가능하게 되었으나, 인터넷 망의 개방성으로 인한 외부로부터의 불법적인 침입 시도나 전송 데이터에 대한 공격, 인터넷 웜(Worm) 공격 등이 문제가 되고 있다[1]. 이러한 침입시도나 공격에 대해 데이터를 보호하기 위해서 안전한 인터넷 서비스를 위한 인터넷 보안 솔루션에 대한 연구가 활발히 진행되고 있다.

특히, 인터넷의 사용이 인터넷 뱅킹, 전자상거래 등 사용자의 개인정보가 필요한 분야로 확대됨에 따라 데이터 무결성에 대한 관심이 높아지고 있다. 데이터의 무결성이 보장되지 않을 경우 정보 교환 시 메시지 도청 및 수정, 삽입, 송신자의 위장 문제 등이 발생할 수 있으며, 이로 인한 개인 재산권 침해와 개인 정보 유출 등으로 인한 사회 문제를 발생 할 수도 있다.[2]. 그러므로, 인터넷에서 전송되는 데이터의 무결성을 보장하기 위하여 여러 가지 보안 솔루션들이 사용되며, 그 중 대표적인 것이 SSL(Secure Socket Layer)[3]이다.

본 논문에서는 WWW환경에서 클라이언트와 서버간에 송수신되는 데이터의 무결성이 위배되었을 경우 그 정보를 검증 및 관리할 수 있도록 OpenSSL을 이용하여 무결성 위배 데이터를 검증 및 관리할 수 있는 Apache Web Server 시스템을 구성하고, 검증된 데이터를 IDS (Intrusion Detection System)로 전송하여 침입 탐지 정보와 무결성 검증 정보를 통합적으로 관리할 수 있도록 하는 IDS 통합 시스템을 제안 및 설계하였다.

Ⅱ. 관련 연구

1. SSL (Secure Socket Layer)

SSL(Secure Socket Layer)은 Netscape Communications사에서 웹 보안을 위해 개발한 응용 계층의 보안 프로토콜로 데이터의 암호화 및 서버 인증, 메시지 무결성을 제공한다[4]. 이동 네트워크가 발전하면서 이동 네트워크 보안을 위해서 TLS, WTLS, SSL 프로토콜 등이 사용되고 있으며, 이들은 모두 SSL의 구조를 기본으로 한다. SSL 프로토콜은 Handshake Layer와 Record Layer로 구성되며, Handshake Layer는 암호화된 통신을 하기 위한 비밀키, 암호화 알고리즘, 비밀 파라메터 등의

정보를 통신 종단간에 교환한다. 그리고 Record Layer는 Handshake Layer에서 교환된 정보를 바탕으로 URL, 접근인증 자료 등과 같은 HTTP request와 response에 포함되는 모든 정보들을 암호화하여 전송한다. 그림.1은 SSL에서 제공하는 무결성 검증 기능을 도식화 한 것이다. SSL프로토콜은 MD4, SHA등의 해쉬 함수를 사용하여 무결성을 제공한다. 즉, 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 MAC값이 일치하는지 여부로 무결성을 검증한다[5].

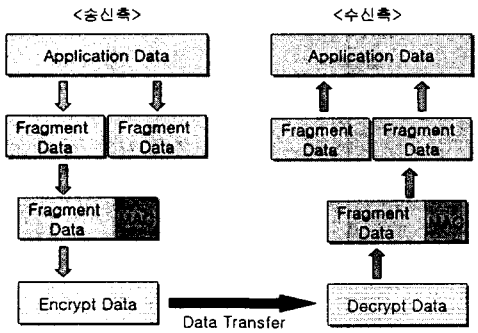


그림 4. SSL 프로토콜의 무결성 제공 개념

2. Apache Web Server와 OpenSSL

(1) Apache Web Server

아파치는 1995 년 그 당시에 가장 인기 있었던 웹 서버중의 하나인 NCSA HTTPD 1.3 버전을 기반으로 탄생하였다. 그 후 기존의 NCSA 웹 서버에 더욱 향상된 기능들을 탑재하여 Apache 웹 서버를 발표하였다[6]. 넷크래프트 웹서버 서베이의 '2003년 2월 웹 서버 소프트웨어 사용 현황 통계'[7]에 따르면 그림 2.에서 보듯이 아파치 웹 서버가 현재 인터넷 웹 서버 중에서 가장 높은 점유율을 차지하고 있다. 그 이유를 들자면 무료 제공 및 지속적으로 패치파일을 제공하고 최고의 퍼포먼스를 내고 있기 때문이다.

서버	사용중인 서버 수	시장 점유율	.com 도메인 보유 서버 수
Apache	22,492,327	62.72%	9,281,986
Microsoft-IIS	9,686,936	27.01%	5,238,165
Zeus	768,900	2.14%	354,710
Unknown	482,254	1.34%	223,477
Netscape-Enterprise	416,567	1.16%	198,504
Rapidsite	381,798	1.06%	256,390
thttpd	236,561	0.67%	3,113
tigershark	229,079	0.64%	158,324
WebSTAR	88,991	0.25%	49,367
Lotus Domino	79,953	0.22%	29,037

그림 5. 2003. 2. 웹 서버 사용 현황 통계

(2) OpenSSL

OpenSSL은 Eric A. Young과 Tim J. Hudson에 의해 개발된 SSLeay 라고 하는 라이브러리를 기본으로 하고 있으며, Secure Sockets Layer (SSL v2/v3)와 Transport Layer Security (TLS v1)를 탑재한 고기능의 Open Source 라이브러리이다.OpenSSL은 SSL 프로토콜을 구현한 라이브러리 중 가장 널리 적용되고 있으며, 거의 모든 플랫폼에 적용이 가능하도록 되어있다[8].

(3) mod_ssl

mod_ssl은 OpenSSL 라이브러리를 이용하여 Apache 웹서버에서 SSL/TLS 프로토콜을 통한 암호화(https 통신을 가능하게 함)를 제공하는 패키지이다[9].

mod_ssl 패키지는 1998년 4월에 Ralf S. Engelschall에 의해 만들어 졌으며, Apache-SSL 웹서버 프로젝트에 사용하기 위해 Ben Laurie이 개발한 것에 의해 유래된다. httpd demon를 SSL 서버화하는 것으로는 이전부터 Apache를 SSL화하는 Apache-SSL이 있었으나, mod_ssl은 Apache-SSL의 프로젝트로부터 분파 한 형태로 탄생하였으며 Apache 소스를 패치하여 변경하는 것이 아니라 Apache module로서 include하는 방법을 사용하며, 클라이언트 인증으로 CRL을 참조할 수 있는 특징을 가지고 있다.

III. IDS 통합 시스템 설계

1. 전체 시스템 개요

본 장에서는 무결성 관리를 위한 IDS 통합 시스템의 전체 구성을 보여주고, 서버에서 무결성 정보를 검증하고 관리하는 시스템의 구성과 검증된 무결성 검증 데이터를 서버로부터 받아들여 통합 관리하는 IDS 통합 시스템의 설계 및 관리에 필요한 각 모듈의 동작에 대해서 설명한다. 그림 3.은 무결성 관리를 위한 IDS 통합 시스템의 전체 구성을 보여준다.

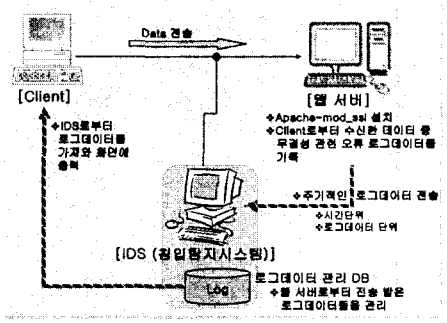


그림 6. IDS 통합 시스템 전체 구성도

웹 서버는 OpenSSL과 mod_ssl을 사용하여 SSL 통신이 가능하도록 구성되어 있으며, 클라이언트와 웹서버는 https 통신을 하여 암호화된 데이터를

주고받는다. 이 때 공격자에 의하여 송수신 데이터에 변조가 발생할 경우 웹 서버의 무결성 위배 정보 검증 및 관리 시스템에서 무결성과 관련된 오류 로그데이터를 기록하게 된다. 기록된 로그 데이터는 주기적으로 IDS에 전송이 되며, 전송된 로그데이터는 IDS에서 통합적으로 관리하게 된다. IDS에 의해 관리되는 무결성 정보는 관리자가 원격지에서 IDS 통합 시스템에 접속하여 침입탐지 정보와 무결성 정보를 통합적으로 관리할 수 있게 한다.

2. 무결성 정보 검증 및 관리 시스템

무결성 정보 검증 및 관리 시스템은 클라이언트로부터 웹 서버가 주요 데이터를 수신할 때 무결성이 위배된 데이터를 수신했을 경우 무결성 위배 정보 로그를 기록하는 모듈과, 기록된 로그 데이터에 대하여 주기적으로 IDS 통합 시스템에 전송하는 기능을 수행하는 모듈로 구성된다. 그림 4.는 무결성 검증 및 관리 시스템의 구성을 나타낸다.

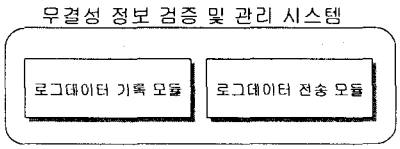


그림 7. 무결성 검증 및 관리 시스템 구성도

본 논문에서는 웹 서버 구축을 위하여 표 1.과 같은 환경에서 시스템을 구성하였고, 클라이언트에서 서버로 전송되는 데이터의 변조를 위해 본 연구실에서 개발한 변조 서버 시스템을 사용하여 데이터의 변조를 수행하였다[11]. 데이터 변조를 수행하게 되면, 웹 서버는 변조에 따른 무결성 오류 정보를 로그파일에 기록하게 된다.

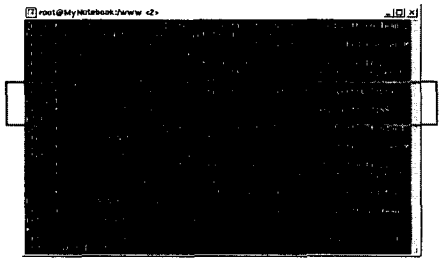
표 1. 웹 서버 구축 환경

항 목	내 용
운영체제	WOW-Linux 7.2 Paran
SSL 라이브러리	OpenSSL 0.9.7
웹 서버	Apache 1.3.28
SSL 모듈	mod_ssl 2.8.14

Apache와 mod_ssl을 설치하면 4가지의 로그파일이 기록되게 된다. 웹 서버 접근에 대한 모든 기록을 남기는 access_log, 에러와 관련된 모든 기록을 남기는 error_log, SSL통신과 관련된 모든 정보를 기록하는 ssl_engine_log, SSL 요청에 대한 기록을 남기는 ssl_request_log로 구성된다. Apache 웹 서버는 이러한 각각의 로그파일에 대하여 자체적으로 관리가 가능하도록 구성되어 있으나[10], 무결성 오류 발생시 클라이언트의 IP등 기록되는 정보가 부족하며 무결성 오류와 관련된 내용만을 뽑아낼 수 없다. 그러므로, 본 논문에서는 데이터 전송시 무결성 오류에 대한 로그를 기록할 수 있는 모듈을 추가하여 무결성 정보만을 관리할 수 있도록 하였고, 로그 데이터 기록 항목을 정의하여 IDS 통합 시스템에서 효율적인 관리가 가능하도록 구성하였다. 그림 5.는 로그 데이터의 포맷을 나타내며, 그림 6.은 원래 Apache에서 기록되는 로그파일과 무결성 로그를 남기는 모듈을 추가했을 경우의 로그파일을 비교한 것이다. (a)에서는 오류 발생시 웹서버와 데이터를 주고받는 클라이언트에 대한 정보가 전혀 기록되지 않으나 (b)에서는 클라이언트와 웹서버에 대한 정보가 기록됨을 볼 수 있다. 이렇게 기록된 로그 데이터는 주기적으로 IDS 통합 시스템으로 전송되어 관리되게 된다.

Date	Time	pid	Error Reason	Server IP	Client IP	Client Port	Error code

그림 8. 무결성 로그 데이터 포맷



(a) Apache의 로그파일

(b) 무결성 정보 기록 모듈을 통해 생성된 로그파일

그림 9. 웹서버에 기록된 로그파일

3. IDS 통합 시스템 설계

웹 서버로부터 전송된 무결성 오류 로그 데이터는 IDS로 전송되어 무결성 로그 데이터 관리 DB에서 관리되며, IDS에 의해 탐지된 침입탐지 정보와 함께 IDS의 관리자 모듈을 통하여 통합적으로 관리할 수 있도록 구성하였다. 본 논문에서 설계한 IDS 통합 시스템에 사용되는 침입탐지 시스템은 본 연구실에서 개발한 네트워크 기반의 침입탐지 시스템을 사용하였다[11].

IDS 통합 시스템은 침입탐지 정보를 관리하는 파트와 웹 서버로부터 전송받은 무결성 정보를 관리하는 파트로 나누어지며, 무결성 정보 관리 파트는 로그 데이터 파일을 저장하고 관리하는 무결성 데이터 관리모듈과 관리자가 무결성 데이터에 대

하여 조회 및 검색을 할 수 있도록 하는 무결성 데이터 보고모듈로 구성된다. 그림 7.은 IDS 통합 시스템의 전체 구성을 나타낸 그림이다.

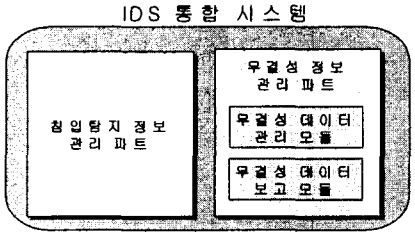


그림 10. IDS 통합시스템 전체 구성도

IDS 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 8.은 클라이언트에서 무결성 로그 데이터를 조회하는 프로토타입 화면이다.

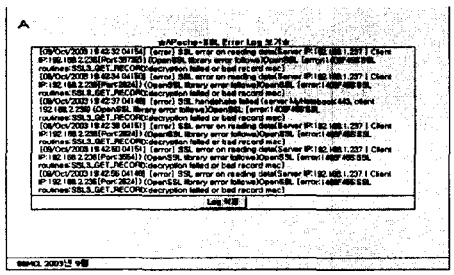


그림 11. 로그 데이터 조회 프로토타입 화면

V. 결 론

본 논문에서는 클라이언트와 서버간에 송수신되는 데이터에 대하여 무결성이 위배되었을 경우 무결성 위배 정보를 효율적으로 검증 및 관리하여 외부의 침입으로부터 대응할 수 있도록 하는 무결성 관리를 위한 IDS 통합 시스템을 설계하였다. 본 논문에서 제안한 시스템은 무결성 정보 검증 및 관리 시스템과 IDS 통합 시스템으로 구성되어 클라이언트와 서버간에 송수신되는 데이터에 대한 무결성을 검증하고 그 정보를 통합적으로 관리하는 방법에 대하여 제안하였으며, 실제 클라이언트와 서버간 변조된 데이터에 대해 무결성을 검증 및 관리하는 모듈을 구현하였다. 그리고 이러한 무결성 위배 정보들의 효율적인 관리를 위해 침입탐지시스템과 연계한 통합 관리시스템을 제안하고 설계하였다.

향후 연구에서는 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.

참고 문헌

[1] 한국정보보호진흥원, "2003년 8월 해킹바이러스 통계 및 분석 월보", 2003.8
[2] 김태호, "네트워크 보안제품 적합성 검증을 위한 무결성 검증 도구 설계 및 구현", p2, 2001.2
[3] Eric Rescorla "SSL and TLS", Addison-Wesley Press, 2001
[4] http://wp.netscape.com/eng/ssl3/draft3 02.txt
[5] 김기욱, 정경훈, 장용호, 김창수, "무선 인터넷 보안을 위한 SSL활용 연구", 한국멀티미디어학회 춘계 학술발표 대회 논문집, 2001
[6] http://apache.kr.net/#intro
[7] http://www.netcraft.com/Survey/Reports/0302/byserver/index.html
[8] http://www.openssl.org
[9] http://www.modssl.org
[10] 정관진, "아파치 로그파일의 이해와 분석", http://www.apache.kr.net/documents/log_story.html,
[11] 김창수, "정보보호시스템 무결성 기능평가 S/W 개발", 한국정보보호센터 연구보고서, 1999
[12] 김남진,강진수,김창수, "네트워크 기반의 실시간 침입탐지 시스템 설계 및 구현", 한국정보보호학회 영남지부 학술발표대회 논문집, 2002.2