통합보안 관리를 위한 침입대응 시스템 설계*

이창우** · 손우용** · 송정길***

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), 가상 사설망(VPN), 시스템 보안, 인증 등 관련 솔루션이 대거 등장함에 따라 통합관리가 중요시되어 지고 있다. 이런 문제를 해결하기 위해 제안한 본 로그 분석을 통한 침입 대응시스템은 로그 파일을 XML 형식으로 저장함으로써 XML의 장점인 로그 파일의 검색이 용이하고 빠르게 이루어 질 수 있으며, 데이터의 구조화에 따라 시스템의 로그 파일들을 통합 분석, 관리하는데 이점을 가질 수 있다. 또한, 본 논문에서 제안한 생성된 로그파일을 IP 주소에 의해 소트된 로그와 Port 번호에 의해 소트된 로그, 침입 유형에 의해 소트된 로그, 탐지 시간에 의해 소트된 로그 등 다양한 형태로 변환하기 때문에 다른 침입탐지시스템에서 생성된 로그 파일과 비교 분석이 가능하다.

Design of Intrusion Responsible System For Enterprise Security Management*

Chang-Woo Lee** · Woo-Yong Sohn** · Jung-Gil Song***

ABSTRACT

Service operating management to keep stable and effective environment according as user increase and network environment of the Internet become complex gradually and requirements of offered service and user become various is felt constraint gradually. To solve this problem, invasion confrontation system through proposed this log analysis can be consisted as search of log file that is XML's advantage storing log file by XML form is easy and fast, and can have advantage log files of system analyze unification and manages according to structure anger of data. Also, created log file by Internet Protocol Address sort by do log and by Port number sort do log, invasion type sort log file and comparative analysis created in other invasion feeler system because change sort to various form such as do log by do logarithm, feeler time possible.

Key words : ESM, Insrusion, Security, IDS, Firewall, XML

---

* 본 연구는 '산업자원부 지역협력연구사업(과제번호 : R12-2003-004-02001-0) 지원으로 수행되었음'.

** 한남대학교 컴퓨터공학과

*** 한남대학교 정보통신 · 멀티미디어 공학부

1. 서 론

현재 장비 위주의 네트워크 인프라는 관리의 분산, 통합의 어려움, 트래픽 보장의 어려움, 보안과 인증의 분산 등 여러 가지 문제를 가지고 있다. 특히, 불법적인 침입이 다양해짐에 따라 각각의 통제가 어려우며, 갈수록 다변화 된 침입에 대하여 대처하기가 어렵고, 시스템 환경에 적합한 시스템 개발과 대규모 네트워크에 대한 효율적인 침입 차단 구조를 갖고 있지 않는 등 단일 보안 관리의 문제점이 대두되고 있다.

또한 보안에 있어서 가장 중요한 것은 로그 파일을 통한 침입 분석인데 기존에 개발된 방화벽과 침입탐지시스템은 침입에 대한 로그 파일을 시간에 따른 일련의 기록으로만 남기기 때문에 로그 분석이 효율적이지 못하다. 이러한 문제점 들을 해결하기 위해 대규모화 되어가는 네트워크에서 다양한 보안시스템들을 제어하고 로그 분석을 효율적으로 하기 위한 XML 로그 기반의 침입 대응시스템의 필요성이 대두되고 있다. 따라서 본 논문에서는 로그 분석을 통하여 보다 효과적으로 침입에 대하여 대처하고, 로그 데이터를 XML 기반의 로그 포맷 형태로 변환한 후 다양한 형태의 로그 파일을 생성함으로써, 다른 보안 시스템들과의 연동도 가능하고, 로그 파일을 효율적으로 분석할 수 있도록 구성된 침입 대응시스템을 설계 및 구현하고자 한다.

본 논문의 구성은 2장에서는 침입대응 시스템 설계에 필요한 관련연구를 살펴본 후 3장에서는 침입대응 시스템을 위한 단위별 보안 시스템 설계 및 구현에 대하여 기술하고, 끝으로 4장에서 결론 및 향후 연구방향을 제시한다.

2. 관련 연구

2.1 침입차단 시스템

침입차단 시스템(방화벽 또는 FireWall)은 외부로부터 불법적인 접근이나 해커의 공격으로부터 내부네트워크를 방어하기 위해 내부 네트워크와 외부 네트워크 사이의 통로에 설치하여 두 네트워크간의 트래픽을 제어하기 위한 목적으로 구성된 시스템 혹은 시스템들의 네트워크라고 말할 수 있다. 침입차단 시스템은 내부 네트워크와 외부 인터넷 사이에서 불법적인 접근을 방지하고 내부 네트워크의 정보 자산을 보호하고, 다음에 나오는 목적을 위해 이용할 수 있다.

- 내부의 취약한 부분 네트워크 구성요소를 보호
- 외부로부터 내부로의 불법적인 행동에 대한 내부망의 보호

침입차단 시스템은 미리 설정해 놓은 액세스 규칙에 따라 허용유무를 판단한다. 침입차단 시스템의 가장 기본적인 기능은 외부로부터 내부망의 데이터를 보호하는 것이다[7]. 침입차단 시스템의 주요 기능을 간단히 정리하면 다음과 같다.

- 외부의 불법침입으로부터 내부 네트워크 및 정보 보호
- 서비스 접속 및 거부
- 사용자 인증
- 내부 및 외부 상호 접속된 네트워크에 대한 트래픽 감시 기록

2.2 침입탐지 시스템

침입차단 시스템(방화벽 또는 FireWall)은 외부로부터 불법적인 접근이나 해커의 공격으로부터 내부네트워크를 방어하기 위해 내부 네트워크와 외부 네트워크 사이의 컴퓨터 침입이 무엇인가를 Smaha은 침입 시도에 대하여 아래와 같이 정의를 했다.

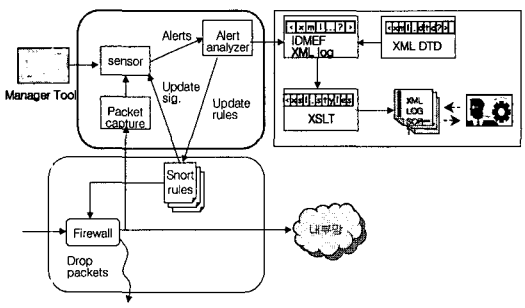
- 시스템에 침투하려는 시도
- 남의 계정과 패스워드를 사용해 시스템에 로그인한 행위

- 운영체제의 보안 메커니즘을 위반하는 행위
- 시스템의 특정 자원을 독점하여 다른 사용자가 시스템의 서비스를 이용하지 못하게 하는 행위
- 중요한 정보를 외부로 누출하는 행위
- 자신의 권한을 남용하는 행위

침입으로 인한 물질 피해, 정신적 피해, 컴퓨팅 자원의 손실 등을 줄이기 위해 침입이 방지되어야 한다. 대부분의 시스템은 침입을 방지하기 위한 기본적인 방법으로 접근 제어 방식과 암호 시스템을 사용하고 있다. 첫 번째로, 접근 제어 방식은 login 절차와 패스워드를 사용하고 여러 자원에 대한 사용 허가권을 이용하여 권한이 없는 사용자가 중요한 정보에 접근하지 못하게 하는 방식이다. 두 번째로, 암호시스템은 정보를 암호화하여 암호 키를 갖고 있지 않다면 그 정보의 내용을 볼 수 없게 하는 방식이다[4].

3.1 시스템 구조 설계

본 논문에서 구현된 시스템의 구조를 살펴보면 (그림 1)과 같이 로그분석을 통한 침입대응 시스템은 침입차단시스템(Firewall), 침입탐지시스템(IDS), 관리툴(Manage Tool), XML 로그 형태의 Sort 된 문서로 구성된다.



(그림 1) 전체 시스템 구성도

외부망에서 접근한 패킷은 침입차단시스템(Firewall)에서 기본 정책에 따른 패킷 필터링을 통한 패킷 차단(Packet Drop)이 일어나게 된다. 침입차단시스템을 통과한 패킷은 패킷 캡쳐를 통해 침입탐지시스템의 Alert analyzer에게 전달되고, Alert analyzer에서 분석된 패킷은 불법적인 침입에 해당되면 rules에 업데이트되어 방화벽을 통해 해당 IP는 차단하게 되고 Analyzer에서 분석된 모든 패킷은 XML 로그 형태로 저장된 후 Sort 기능을 통해 다양한 형태로 분류된다.

3.2 시스템 설계

3.2.1 침입차단 모듈 설계

(1) 패킷 필터링 모듈

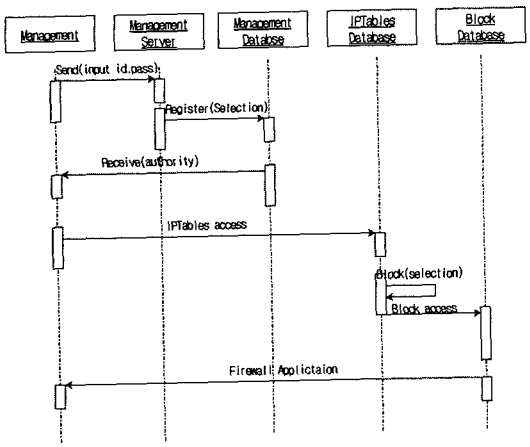
침입차단 시스템에 접속한 상대 컴퓨터에 대한 정보를 알아내기 위한 방법으로 패킷을 이용한다. 패킷에는 상대방에 대한 정보와 접속하려는 컴퓨터의 정보를 가지고 있다. 패킷 필터링을 이용하는 침입차단 시스템은 이러한 패킷 정보를 이용하여 비인가된 사용자의 패킷을 차단하게 된다.

(2) 필터링 데이터 저장 모듈

원격지 컴퓨터로부터 전달되어진 필터링 Data는 침입차단 시스템의 드라이버로 전달된다. 전달된 데이터는 연결 리스트에 저장하여 관리한다.

(3) 패킷 처리 모듈

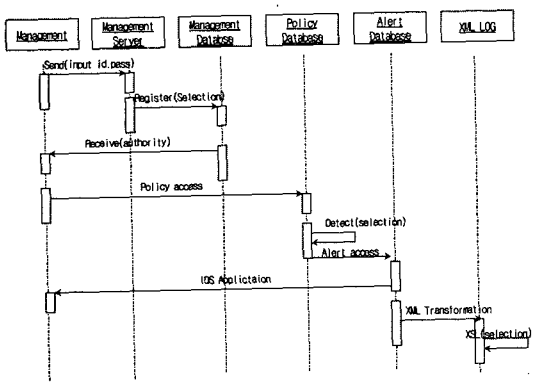
침입차단 시스템으로 전달된 패킷은 필터링에 의해 차단 유무를 검사받게 된다. 모든 패킷은 dispatch_complete 함수를 통과하면서 알맞게 처리된다. 접근을 허용하는 패킷은 안전하게 시스템을 통과하게 되고 접근을 허용하지 않는 패킷은 dispatch_complete 함수에서 처리 되어 시스템에 접근할 수 없게 된다. (그림 2)는 침입차단 모듈에서 침입 차단 시스템 접속에서부터 패킷을 필터링하고 데이터에 저장되어 처리되는 부분을 UML의 Sequence 다이어그램을 이용하여 침입대응시스템에서 침입 차단 과정을 모델링한 것이다.



(그림 2) 침입 차단 모듈 시퀀스 다이어그램

3.2.2 침입탐지 모듈 설계

침입 탐지 과정에서 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 3) 침입 탐지 모듈 시퀀스 다이어그램

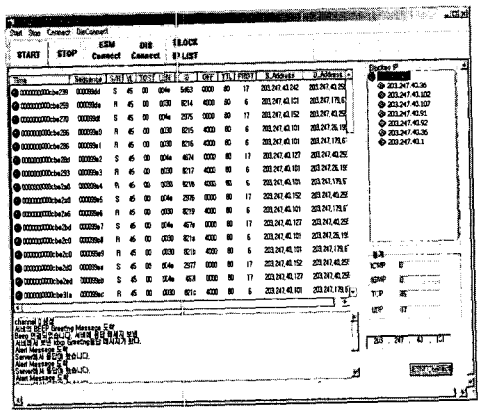
4. 시스템 프로토타입 구현

4.1 시스템 환경

로그 분석을 통한 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. 또한 향후 통합 보안 관리를 위해 메시지 및 로그는 MSXML 4.0 Parser와 DOM 기술을 이용하여 XML로 작성되었고, XSLT을 이용하여 Sort된 다양한 XML 문서로 변환하여 디스플레이 되도록 구현하였다.

4.2 침입차단 시스템 구현

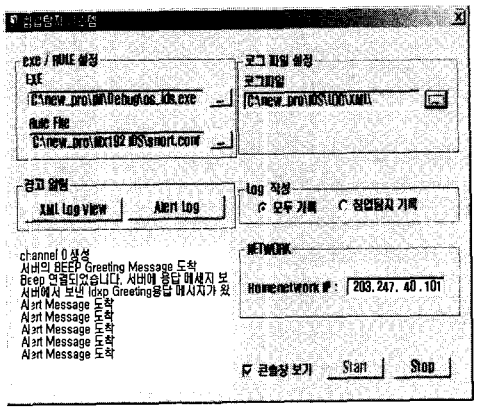
접근 허용에 대한 정보는 관리자에 의해 시스템의 접근을 통하여 관리되어 진다. 관리자는 원격으로 침입차단 시스템에 접속하게 되고, 포트와 IP 설정 부분을 이용하여 원격으로 정보를 표현할 수 있다. 이러한 내용은 원격지에 있는 시스템에 전달되어 진다. (그림 4)는 관리자에 의해 관리되어지는 침입차단 시스템의 제어부분을 구현한 것이다.



(그림 4) 침입차단시스템 제어 부분

4.3 침입탐지 시스템 구현

(그림 5)는 초기 IDS를 설정할 수 있도록 구현한 부분으로서, 화면 상단에 있는 실행 File과 RuleSet의 경로가 나타나는데 이는 pcap을 설치하고 경로를 설정했을 시 프로그램 상에서 자동으로 알아서 설정되도록 되어있다. IDS가 공격받았을 경우 공격 유형에 따라 Alert 메시지들이 해당 경로로 자동 저장된다.



(그림 5) 침입탐지시스템 구현 화면

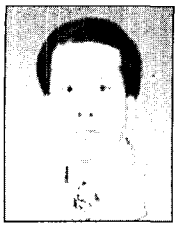
5. 결론 및 향후 연구방향

본 논문에서는 침입대응시스템 환경에서 로그 파일을 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 침입대응 시스템을 구현하였다. 로그분석을 효율적으로 하기 위해 침입탐지 및 차단시스템은 생성된 로그파일을 IP 주소에 의해 소트된 로그와 Port 번호에 의해 소트된 로그, 침입 유형에 의해 소트된 로그, 탐지 시간에 의해 소트된 로그 등 다양한 형태로 변환하기 때문에 다른 침입탐지시스템에서 생성된 로그 파일과 비교 분석이 가능하다.

향후 연구되어야 할 내용은 이기종의 침입차단 시스템, 침입탐지 시스템, 시스템 보안관리 Agent, 네트워크 장비, 인증체계, 자원 관리 등을 통합 모니터링하고 관리할 수 있는 통합보안 관리 시스템(ESM)에 대한 연구가 함께 이루어져야 할 것이다.

참 고 문 헌

[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] Future System, http://www.future.co.kr
[11] 김익수, 김명호, "실시간 침입탐지 및 차단을 위한 시스템", 한국정보과학회 춘계학술발표 논문집, 2000. 3, pp.169-171.
[12] 문호성 외, "보안정책 서버의 경보 데이터 분석 모듈 설계 및 구현", 한국정보처리학회 춘계학술발표 논문집, 2002. 4, pp.59-62.
[12] Judy Novak, Stephen Northcutt, "Network Intrusion Detection", New Riders Publishing, 2003.



이 창 우

1982년 동국대학교 산업공학과 (공학사)
1986년 동국대학교 대학원 산업공학과(공학석사)
1998년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호

손 우 용

1998년 한남대학교 컴퓨터공학과 (공학사)
2000년 한남대학교 대학원 컴퓨터공학과(공학석사)
2001년~2004년 한남대학교 대학원 컴퓨터공학과(공학박사)
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호

송 정 길

1966년 한남대학교 수학과 (이학사)
1982년 홍익대학교 대학원 전자계산학과(이학석사)
1988년 중앙대학교 대학원 전자계산학과(이학박사)
1990년~1991년 University of illinois 객원교수
1979년~현재 한남대학교 컴퓨터공학과 정교수
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 분산시스템, 정보보호