오용탐지모델 기반의 침입 탐지시스템 설계 및 구현

강진수, 김남진, 김창수
부경대학교 전자계산학과

Design and Implementation of IDS based on Misuse Detection Models

Jin-Soo Kang, Nam-Jin Kim, Chang-Soo Kim
Dept. of Computer Science, Pukyong National University

요 약

본 논문은 불법 침입 탐지를 위한 정보시스템 구축에 있어 많은 연구가 진행되고 있는 침입 탐지 시스템(IDS: Intrusion Detection System)중 네트워크 기반의 오용(Misuse) 탐지 모델을 이용하여 침입 탐지 시스템을 설계 및 구현하였다. 구현된 침입 탐지 시스템은 K4 인증 기준을 모델로 삼았으며, 탐지하는 시그너처의 분류상 Content, DoS, Probing을 대상으로 설계되었으며, 원격으로 시스템의 관리와 감독이 가능하도록 구현하였다.

Ⅰ. 서론

초고속통신망 보급률 100명당 57명으로 세계 1위라는 자랑 뒤엔 40%라는 전세계 해킹의 경유지로 이용당하고 있다는 사실을 인정하지 않을 수 없다. 2002년 3월 한국정보보호진흥원(CERTCC-KR)에서 발표한 "2002 3월 침해 사고 접수 및 처리 현황"을 보면 연도별 해킹 건수는 증가하고 있으며[1], [표 1]은 2000년부터 월별 국내 해킹 현황을 나타낸 것으로 매년 증가하고 있음을 보여주고 있다. [표 2]는 최근 다양한 해킹 기법을 나타낸 것으로 가장 많은 공격기법은 취약점 정보수집을 이용한 기법이 주류를 이루고 있으며, 다음은 버퍼 오버플로우와 악성 프로그램을 이용한 기법을 적용하고 있다.

이러한 해킹 피해를 막기 위해서 정부에서는 2001년 7월1일자로 정보통신기반보호법과 같은 정보보호 관련법률을 시행하고 있는데, 이 법이 지정한 국가주요 기관산업에 대한 정보보호 시스템 구축시 침입탐지 시스템의 역할이 기존의 방화벽만으로 구성된 정보보호시스템의 허점을 보완하리라 기대하고 되고 있다. 침입탐지시스템이 차세대 보안 솔루션으로 부각되는 주된 이유는 방화벽이 해킹되었을 경우 이에 따른 피해를 최소화하고 네트워크 관리자 부재시에 시스템 자체적으로도 해킹 등에 대응할 수 있는 보안 솔루션에 대한 요구가 늘고 있는 상황에서, 침입

탐지시스템이 이 같은 요구를 해결할 수 있기 때문이다.

[표 1] 월별 국내 해킹피해 현황

월	2000년	2001년	2002년
1월	108	261	589
2월	113	438	324
3월	129	384	303
4월	117	537	·
5월	137	658	·
6월	117	432	·
7월	278	364	·
8월	239	705	·
9월	237	522	·
10월	156	304	·
11월	227	334	·
12월	85	384	·
합계	1,943	5,323	1,216

[표 2] 해킹 공격 기법

해킹공격기법	건수	비고
사용자도용	23	개인사용자계정 도용
S/W보안오류	0	-
버퍼오버플로우	45	snmp,named/bind 취약점
구성•설정오류	1	사용자 권한 설정 오류
악성 프로그램	45	Nimda 웜,트로이목마
프로토콜 취약점	1	-
서비스 거부 공격	1	서비스 거부
E-mail관련공격	3	스팸메일관련 공격
취약점 정보수집	184	named/bind, ftpd, rpc스캔
사회공학	0	-

본 연구에서는 비정상적인 방법으로 시스템에 불법 접속을 시도하는 행위와 시스템 내부에서 시도되는 침입관련 행위, 그리고 정상적인 네트워크 서비스를 방해하는 침입 시도 등을 네트워크 패킷 분석을 통하여 탐지할 수 있으며, 웹 기반에서 동작하여 원격지에서도 관리가 가능한 시스템을 개발하고자 한다.

Ⅱ. 관련 연구

본 장에서는 침입 탐지 모델을 크게 두 가지의 탐지모델[3, 4]로 분류하여 그 내용을 간략히 알아보고, 공격시나리오에 대해서 살펴본다.

1. 침입탐지 방법의 분류

가. 침입행위의 결과에 따른 분류

1) 비정상적 탐지 모델

비정상적(anomaly) 탐지 모델은 정상적인 행위패턴에서 벗어난 행위를 탐지하는 방법으로, 컴퓨터 자원의 비정상적인 행위에 근거하여 정의된 모델을 이탈하는 경우를 침입으로 간주한다. 그 종류로는 통계적인 방법, 특징 추출 방법, 예측 가능 패턴 생성 방법, 그리고 신경망을 이용한 방법 등이 있다.

2) 오용(misuse) 탐지 모델

오용 탐지 모델은 이미 알려진 공격패턴을 이용한 탐지 방법으로, 시스템이나 응용소프트웨어의 취약점을 통하여 시스템에 침입할 수 있는 잘 정의된 공격을 정의하여, 정의된 모델과 일치하는 경우를 침입으로 간주한다. 종류로는 조건부 확률방법, 전문가 시스템방법, 상태 전이 분석(State Transition Analysis) 방법, 그리고 키 입력 관찰 방법, 모델 기반 침입탐지방법, 패턴 매칭 등이 있다.

나. 침입자료의 기반에 따른 분류

1) 호스트 기반 침입

Program, Process의 변수, OS에서 기본적으로 제공하는 Log기록을 통해서 감사자료를 수집, 침입탐지에 이용하는 방법이다.

2) 네트워크 기반 침입

Network 상에 흐르고 있는 packet을 수집하여 protocol을 해석, 감사자료로 사용하는 방법이다.

3) 다중호스트 기반 침입

다중호스트에서 순차적인 아닌 다중적으로 단일 host에 침입하는 형태의 침입을 탐지하는 방법이다[3,5,6,7].

2. 네트워크 기반의 공격 시나리오

전통적인 네트워크 공격 기법의 일반적인 공격절차는 가장먼저 공격대상에 대한 정보수집 단계이며, 그 다음 수집한 정보를 바탕으로 시스템 침입 단계를 거치게 된다. 그리고 지속적인 침입 및 다른 시스템의 공격을

위한 공격 전이 단계를 거치게 된다[7].

• 정보수집단계 : 공격대상 네트워크에 어떠한 호스트가 있으며, 이 호스트가 어떠한 서비스를 제공하는가, 그리고 네트워크가 어떻게 구성되어 있는가를 파악하여 최종 공격 대상을 찾아내는 단계

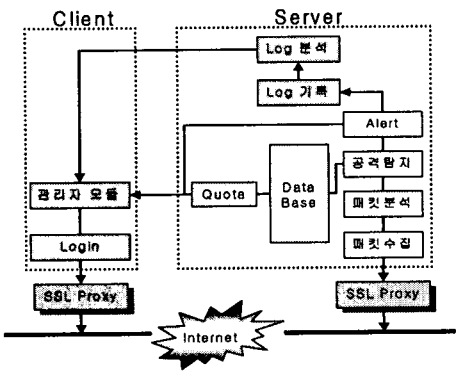
• 시스템 침입단계 : 실제 개별 시스템에 침입하는 단계로 정보수집단계에서 수집한 정보를 바탕으로 가장 취약한 부분을 공격

• 공격전이 단계 : 1차적인 침입으로부터 얻은 정보 및 추가 작업을 통하여 시스템 침입을 확대하고 다른 시스템에 침입하는 단계

이러한 전통적인 침입에 대하여 방어자의 보안수준이 향상함에 따라 백오리피스, 네트웍 스캐닝, 인터넷 웜, 백도어, 악성 에이전트, 사회공학기법(Social Engineering)등의 새로운 공격기법들이 나타나게 되었다. 이러한 기법들은 공격기법의 새로운 패러다임인 분산화, 자동화, 은닉화의 특징을 보인다.

Ⅲ. 침입탐지시스템의 설계 및 구현

본 절에서는 침입 탐지 시스템의 내부 모듈들의 구성과 구현된 침입 탐지 시스템 인터페이스에 따른 각 부분의 세부적인 사항들을 살펴보도록 한다. 아래의 [그림 1]은 침입 탐지 시스템의 전체 모듈을 나타낸다.

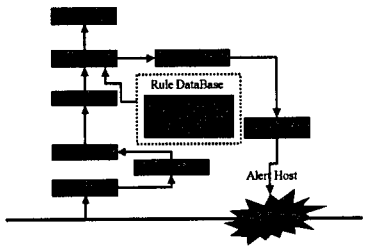


[그림 1] 침입 탐지 시스템 전체 모듈

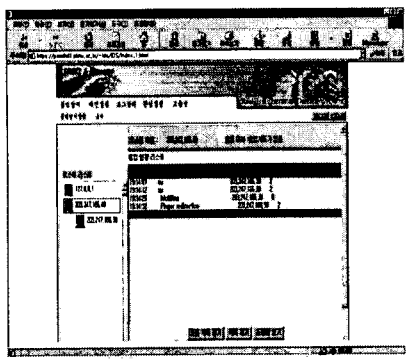
본 침입 탐지 시스템은 서버에 탑재되어 실제로 침입을 탐지하는 서버 모듈과 침입 탐지 보고, 탐지를 위한 설정 및 침입 탐지 로그 정보를 웹 환경에서 관리할 수 있도록 이루어진 관리자 모듈인 클라이언트 모듈로 구성되어 있다. 서버와 클라이언트는 인터넷 환경에서 동작을 하므로 SSL(Secure Socket Layer)통신을 통하여 두 모듈간의 안전한 통신을 보장한다[10].

1. 침입 탐지 모듈

네트워크를 연속적으로 모니터링하고, 침입 행위를 감지하는 모듈로 패킷 수집 모듈, 패킷 분석 모듈, 침입 판정 모듈로 이루어진다. [그림 2]는 본 논문에서 구현한 침입탐지 시스템의 전체적인 구성도을 나타낸 것이며 ,[그림 3]은 [그림 2]의 설계 방법에 따라 구현된 화면을 캡처한 것이다.



[그림 2] 침입 탐지 구성도

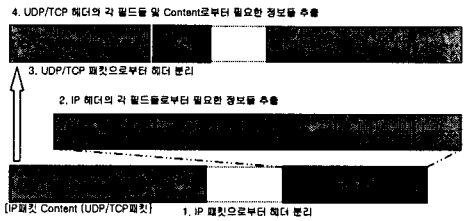


[그림 3] 침입탐지 전체구성 화면

1) 패킷 수집 모듈

Libpcap 라이브러리를 이용하여, promiscu-

ous mode에서 하위 계층의 모든 패킷들을 수집하는 부분이다. [그림 4]는 통신 프로토콜의 각 계층에 따른 패킷의 헤더(header)와 내용을 구분하여 나타낸 것으로, 침입탐지 시스템이 요구하는 탐지 항목으로 사용된다 [2,5,6].



[그림 4] 계층별 패킷 정보 추출 항목

2) 패킷 분석 모듈

패킷 수집 모듈로부터 탐지되는 로컬 네트워크상의 모든 패킷들 중에서 탐지 대상으로 지정된 패킷을 제외한 패킷들을 제거하는 부분이다[9].

3) 침입 판정 모듈

침입 판정 모듈은 패킷 분석 모듈로부터 전달받은 정보와 이미 저장되어 있는 침입 유형에 대한 규칙 정보와 비교함으로써 침입 여부를 판정하게 된다([표 3] 참조).

[표 3] 침입 여부 판정 방법

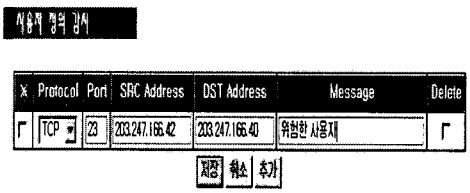
종 류	방 법
패킷 헤드 탐지 (Packet Head Detection)	단순 정보에 의한 침입 탐지
패킷 트래픽 탐지 (Packet Traffic Detection)	패킷의 트래픽을 이용하여 침입을 탐지
패킷 내용 탐지 (Packet Content Detection)	입력 명령어들을 조합하여 침입을 탐지

2. 규칙 데이터베이스

규칙 데이터베이스는 각 모듈에서 탐지될 침입 패턴들에 대한 모든 자료들을 보관하는 기능을 수행한다.

1) 주소지와 포트 기반의 규칙

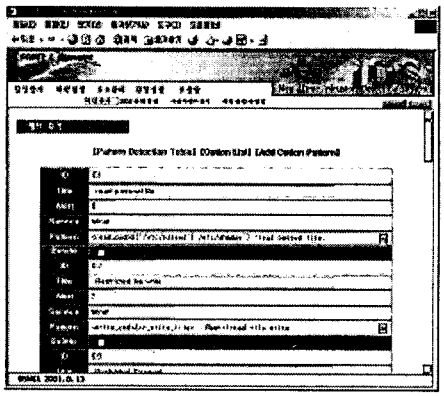
패킷 헤더의 정보를 이용한 침입 여부를 판정하는 기능 모듈에 대한 데이터베이스로서, 관리자가 직접 특정 호스트에 대한 탐지를 설정할 때 사용된다([그림 5] 참조).



[그림 5] 주소와 포트 기반의 침입 설정

2) 침입관련 스트링 기반의 규칙

[그림 6]은 패킷 분석 모듈로부터 얻어진 정보와 사용자의 데이터 정보를 비교하여 침입 여부를 판정하는 침입 판정 모듈에 대한 데이터베이스 유형을 나타낸 것이다.



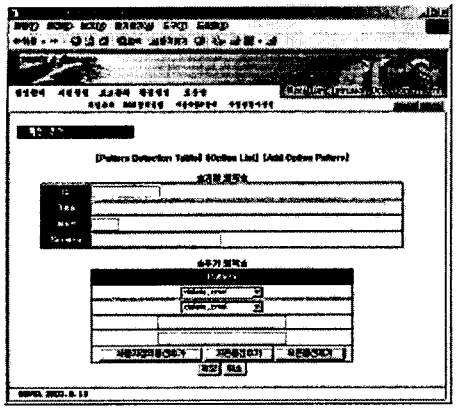
[그림 6] 침입관련 스트링기반 침입규칙

본 연구에서 구현한 침입탐지 시스템은 데이터베이스에 침입탐지 규칙 추가를 용이하게 하기 위해서 [그림 7]과 같은 형태의 인터페이스를 구현하여 쉽게 규칙을 추가할 수 있도록 구성하였다.

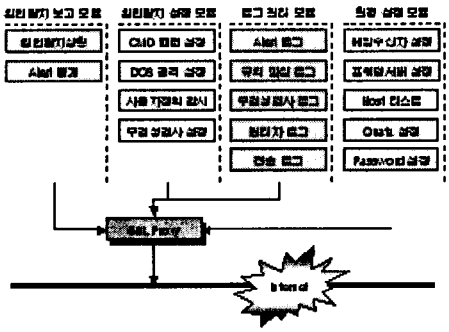
3. 관리자 모듈

침입 탐지 시스템의 탐지 상황 및 다양한 설정 값들을 관리할 수 있는 모듈로서, 사용자가 인터넷 상에서 직접 자신의 시스템에 알맞은 설정을 할 수 있게 해준다. 관리자 모듈은 침입 탐지 보고 모듈, 설정 모듈, 로그 관리 모듈, 환경 설정 모듈로 구성되어

있다([그림 8] 참조).



[그림 7] 침입탐지 규칙 추가 기능



[그림 8] 구현된 IDS 전체 구성도

1) 침입 탐지 보고 모듈

침입 탐지보고 모듈은 침입이 탐지되었을 때 관리자에게 침입을 알려주는 모듈로써, 설정해 둔 침입 레벨에 따라 [표 4]와 같이 분류하여 침입레벨에 따른 대응을 실시간으로 하며, 침입한 사건에 대한 통계는 통계데이터로 저장되어 침입상황분석에 사용된다.

[표 4] 침입 레벨에 따른 대응행동

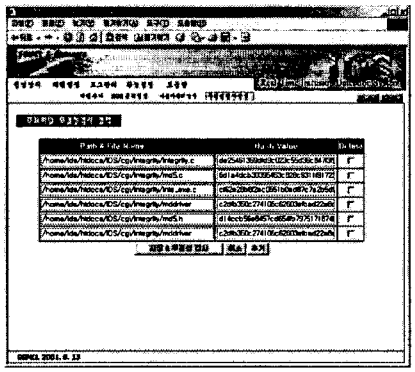
레벨정도	대 응 행 동
레벨1	리스트
레벨2	팝업창+리스트
레벨3	팝업창+리스트+소리
레벨4	팝업창+리스트+소리+메일
레벨5	팝업창+리스트+소리+메일+disconnect

2) 침입 탐지 설정 모듈

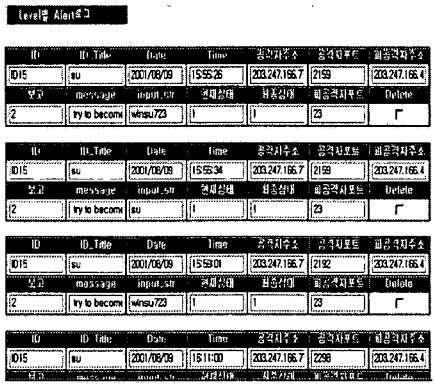
원격지에서 인터넷을 통해 침입탐지 세부 항목들을 설정할 수 있는 기능을 추가하였다. 이러한 기능에는 CMD(command) 패턴 설정, DOS(Denial Of Service) 공격 설정, 사용자 정의 감시과 [그림 9]의 무결성 검사 설정 기능 등이 포함되어 있다[11,12].

3) 로그 관리 모듈

본 연구의 로그관리 모듈 기능으로는 Alert 로그 파일 관리 및 검색, 규칙파일 로그 정보 , 무결성 검사 로그, 관리자 로그, 접속 로그 관리 기능 등이 포함된다. [그림 10]은 레벨 2의 Alert 로그 파일 검색 결과를 나타낸 것이다.



[그림9] 무결성 검사 설정

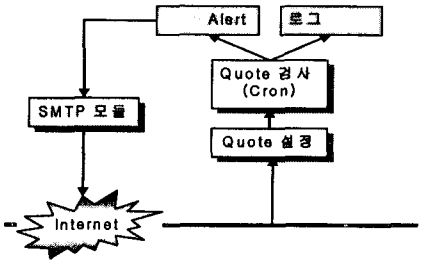


[그림 10] Alert 로그 검색결과

4) 환경 설정 모듈

침입탐지 시스템을 사용하기 위한 각종 환

경 설정 기능으로는 메일 수신자 설정, 포워딩 서버 설정, 접속 Host 리스트 설정, 관리자 Password 설정, Quota 상태 검색 및 관리 기능 등이 포함된다. 그리고 [그림 11]과 같이 Quato 상태 검색 및 관리 기능에는 하드디스크 용량 일정치 초과와 로그 정보 저장의 한계치 초과 정보 등을 검색 및 관리하는 기능이 있다[8].



[그림 11] Quota 설정 모듈

Ⅳ. 결 론

본 연구에서 구현된 침입 탐지 시스템은는 패킷 헤더의 정보를 수집·추출하는 엔진과 추출된 각각의 패킷 정보들을 조합하여 미리 정의된 침입탐지 패턴 규칙을 적용하여 침입을 판단하는 엔진으로 분리하여 구현하였다. 이는 침입탐지 과정에서 발생할 수 있는 시스템 부하를 줄여주고, 실시간 특성을 가지는 판정 결과를 가질 수 있다. 또한, 관리자가 새로운 침입탐지 유형에 대해 쉽게 추가하여 적용할 수 있도록 편리한 인터페이스를 제공하며, 침입탐지 기능뿐만 아니라 시스템 자체의 중요 데이터에 대한 무결성 검사 기능을 추가하여 Cron을 통해 주기적으로 체크함으로써 중요 데이터의 변경여부를 체크할 수 있는 기능을 가진다. 웹 환경의 관리자 모듈은 원격지에서도 시스템을 편리하게 관리할 수 있도록 하며, 시스템 자체의 자원의 초과 사용으로 인한 침입 탐지 시스템의 부적절한 동작 중단을 방지하기 위해서 주기적인 디스크 쿼터 검사를 통한 오동작 방지 기능을 가진다.

[참고문헌]

[1] 한국정보보호진흥원(CERTCC-KR),"2002년 3월 침해 사고 접수 및 처리 현황 http://www.certcc.or.kr/

[2] 한국전산원, "유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구 NCA VI-RER-95105, 1995. 12.

[3] 한국정보보호센터, 침입 탐지 모델 분석 및 설계, Sep, 1996.

[4] 포항공과대학 전자계산소, Security Plus for UNIX3, 1998.

[5] 한국 정보보호진흥원 기술문서 - 네트워크 공격기법의 패러다임 변화와 대응방안 2000. 12.

[6] 양동수, 외 4명, "네트워크 기반의 침입탐지 시스템 및 관리 모듈 설계 및 구현", 한국해양정보통신학회 춘계학술대회발표집, Vol. 5, No. 1, pp. 680- 683. 2001. 5.

[7] 김창수, "네트워크 기반의 침입탐지시스템", 부경대학교 SSMCL 연구보고소, pp. 1- 400, 2002. 1.

[8] 한빛미디어, "UNIX Systems Programming for SVR4", 데이비드 커리, 2001.

[9] 인포북, 네트워크침입탐지와 해킹분석핸드북 Stephen Northcutt, Judy Novak 저, 2001. 10. 26

[10] 성안당. "TCP/IP 시큐리티 실험(Linux /FreeBSD 대응)", Masato Terada, Makoto Kayashima, 2001.

[11] Atkins, Buis, Hare, Nachenberg, Kelley, Nelson, Phillips, Ritchey, Steen, Internet Security, New Riders Publishing, 1996.

[12] T. H. Ptacek and T. N. Newsham, "Insertion, evasion, and denial of service: Eluding network intrusion detection.", Technical report, Secure Networks, Inc., Jan 1998.