공학석사 학위논문

내·외부 침입탐지시스템 통합 모듈 설계에 관한 연구

2002년 8월

부경대학교 산업대학원

전산정보학과

박 철 동

공학석사 학위논문

내·외부 침입탐지시스템 통합 모듈 설계에 관한 연구

지도교수 김 창 수

이 論文을 工學碩士 學位論文으로 提出함

2002년 8월

부경대학교 산업대학원

전산정보학과

박 철 동

< 차 례 >

< **표 차례** >

< 그림 차례 >

A Study on the Integrated Module Design of Internal and External Intrusion Detection System

Chul-Dong Park

Department of Computer and Information
Graduate School of Industry
Pukyong National University

Abstract

As the information communication techniques have been rapidly developing and internet users have been continuously increasing every year. But the damages of hacking are on the increase lately too. Currently, many researches for detection of intrusion are studying, and many intrusion detection tools. In this thesis, we consider the design integrated module design of internal and external intrusion detection system based on network. And the model designed this thesis is based on the network using a state transition analysis, pattern matching and sniffing detection.

Ⅰ. 서 론

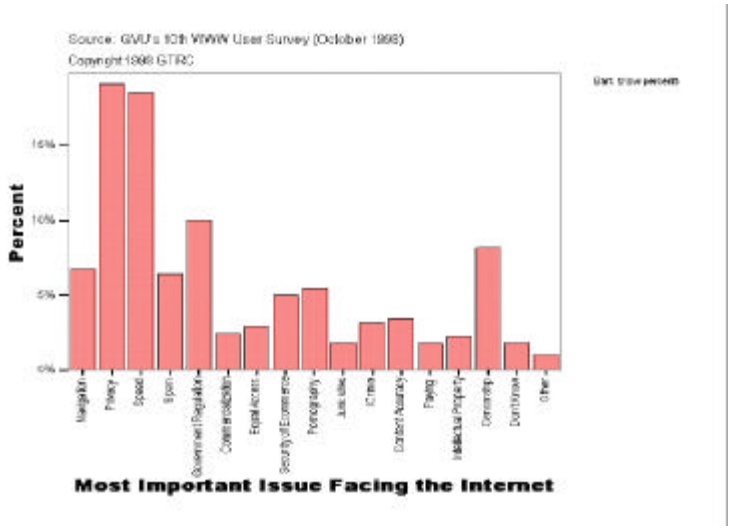
인터넷을 이용하여 멀티미디어 정보를 쉽고 자유롭게 사용할 수 있게 됨으로써 그 사용이 폭발적으로 증가하고 있다. 우리나라에서도 최근 인터넷 열풍에 힘입어 초기에 주로 정보검색과 학술적 목적에 사용되었던 인터넷이 최근에는 제품에 대한 광고나 판매 등 상업적 용도로 그 사용 영역이 점차 확대되고 있는 추세이다. (주)인터넷 매트릭스의 2001년 8월 통계를 따르면 7세 이상 응답자 중 '월평균 한번 이상' 인터넷 이용자는 2,412만 명, 그리고 16세 이상 응답자 중 '월평균 한번 이상' 인터넷 이용자는 1,863만 명으로 나타났다.([그림 1-1] 참조). 이는 인터넷을 비롯한 통신/네트워크 사용의 양적 팽창을 단적으로 보여주는 예이다.

시점 / 유형	이용자 수(만 명)							
	1999.10	2000.12	2000.8	2000.12	2001.3	2001.6	2001.9	2000년 12월 대비 증가
A	943	1,393	1,640	1,904	2,093	2,223	2,412	508
B	786	1,276	1,474	1,811	1,956	2,093	2,279	468
C	786	1,168	1,299	1,519	1,633	1,726	1,863	344
D	665	1,080	1,178	1,453	1,522	1,615	1,745	292

[그림 1-1] 국내 인터넷 이용자 수

유형 A. 만 7세이상 '한달에 한번 이상' 인터넷 이용자
유형 B. 만 7세이상 '일주일에 한번 이상' 인터넷 이용자
유형 C. 만 16세이상 '한달에 한번 이상' 인터넷 이용자
유형 D. 만 16세이상 '일주일에 한번 이상' 인터넷 이용자

국외의 경우도 http://www.nw.com/ 의 자료를 참고로 하면 호스트 수는 99년 1월 43,230,000개를 넘었고 인터넷 이용자 수는 http://www.c-i-a.com/ 의 자료에 의하면 1억 4천 7백만 명이 넘는 것으로 추정되고 2005년에는 7억 2천만 명에 이를 것으로 예상되고 있다.



[그림 1-2] 인터넷의 문제점

네트웍 사용의 증가와 함께 사용분야가 다양해지자 공중망을 이용하는데 따른 보안문제가 최근 심각하게 대두되고 있다. Graphic, Visualization, & usability Center's (GVU)의 10th WWW User Survey 문서에 따르면 설문 응답자의 70% 이상이 통신망에서의 프라이버시 제공이 반드시 필요하다는 조사결과가 나왔으며 ([그림 1-2]참조), 또한 사용자들이 응답한 인터넷에서 직면하게 되는 가장 중요한 문제점으로 개인정보의 보안과 암호화의 필요성도 함께 지적하고 있다. 사용자들의 보안문제에 대한 인식이 높아지고 있고 보안 서비스에 대한 요구도 증가하고는 있으나, 시스템 관리자와 같은 전산 전문가들을 제외하고는 보안의 문제를 해결하기 위해 무언가 조치를 취할 수 있는 사용자는 드물고, 실제 우리나라의 경우도 시스템 관리자들이 보안 문제에 관심은 많으나 적절한 조치를 취한 경우는 많지 않다.

또한 보안 체계가 허술하고 사용자 정보보호 기능이 미비하거나 없는 경우가 많아서 개인 정보의 유출과 사용자의 부인 행위 등의 사고들이 많이 발생하고 있다.

정보통신분야의 발전과 인터넷의 개방은 인터넷을 이용한 기본적인 통신 서비스는 물론, 가상 대학, 전자 상거래, 멀티미디어 서비스들과 같은 교육 및 사회 전반에 걸쳐 다양한 서비스 지원을 가능하게 하였다. 이러한 기능은 정보의 지역적 한계성을 벗어나 여러 나라들로부터 다양한 정보를 얻거나, 우리나라의 여러

우수한 정보들을 홍보함에 있어서도 큰 역할을 담당하고 있다. 그러나, 극히 일부 사용자들로부터 인터넷의 개방성과 사용의 용이성은 불법적인 목적에 악용되는 부작용 현상이 나타나고 있는데, 그 단편적인 예로 [표 1-1]에서의 연도별 침해사고 자료와 [표 1-2]의 2001년 월별 국내 해킹 피해자료를 살펴보면, 실제로 인터넷으로 인한 컴퓨터 바이러스 및 정보 자원에 대한 침입이 날로 증대되고 있음을 볼 수 있다[1].

[표 1-1] 연도별 침해사고 접수 현황

년도	'96	'97	'98	'99	'00	'02.1월	전체
회수	147	64	158	572	1943	589	8806

(※ 주 : 정보보호센터 제공 자료.)

[표 1-2] 2001년 월별 국내 해킹 피해 접수 현황

월	'01.1	'01.2	'01.3	'01.4	'01.5	'01.6	'01.7	'01.8	'01.9	'01.10	'01.11	'01.12	전체
회수	261	438	384	537	658	432	364	705	522	304	344	384	5333

(※ 주 : 정보보호센터 제공 자료.)

이러한 인터넷을 이용한 불법 침입은 단순 정보 누출에서 끝나는 것이 아니라, 전화, 항공, 금융, 연구망, 기업은 물론 국가 기관등 각 분야에서 중요한 업무처리에 있어 커다란 문제를 발생시킨다. 만일 적성 국가로부터의 사이버 테러가 발생하게 된다면 경제와 사회 전반에 걸친 혼란은 물론, 국가의 안보에 있어 심각한 문제를 발생시킬 수 있다. 따라서 전산망 보호 체계의 구축과 정보보호에 있어 여러 가지의 보안 방법들에 대한 필요성이 대두되고 있다[16]. 현재까지의 우리나라 보안 시스템 개발 상황을 살펴보면 방화벽이나 시스템에서의 침입탐지, 암호 등 보안의 일부 분야에 있어서는 시스템들의 개발이 있어 왔으나, 네트워크로부터의 침입탐지에 대한 개발이 미약함으로 균형성있는 보안 시스템 운영에 어려움

이 있었다[2]. 그리고 네트워크를 이용한 침입탐지 시스템 개발을 통하여 안정적인 보안 체계의 현실화를 이룩할 필요가 있다.

따라서 본 논문에서는 네트워크 상에서 패킷을 이용한 정보 교환에 있어 비정상적인 방법으로 네트워크에 연결되어 있는 시스템으로의 불법 접속, 시스템 내부에서 시도되는 침입관련 행위, 그리고 정상적인 네트워크 서비스를 방해하는 침입시도 등을 내·외부에서 탐지할 수 있는 시스템을 설계하고자 한다.

Ⅱ. 관련 연구

네트워크를 이용하여 네트워크 혹은 시스템으로부터 침입을 탐지하기 위한 방법들이 꾸준히 연구되어 왔다. 본 절에서는 침입 판정에 있어 주류를 이루는 방법들의 개요와 특징을 살펴보고, 기존에 개발된 침입탐지 시스템에 대하여 살펴본다. 그리고 시스템이나 네트워크 상에서 발생할 수 있는 여러 가지 공격 기법들로부터 네트워크를 중심으로 시도되고 있는 침입 유형들을 조사하고, 이로부터 침입을 탐지할 수 있는 방법들을 몇 가지 유형으로 분류하여 본다.

2.1 침입탐지 분류 방법

침입탐지 시스템은 탐지 시스템의 탐지 영역을 중심으로 분류하는 데이터 소스(Data Source) 기반의 분류 방법과 탐지 방법을 중심으로 이루어지는 침입탐지 모델 기반의 분류하는 방법으로 크게 나눌 수 있다[5,6,12,15]. 또한 각 분류 방법들은 특징별로 아래에서 설명한 것처럼 보다 구체적인 기준에 의해 세분화된다.

- ㅇ 데이터 소스를 기반으로 하는 침입탐지 분류 방법
  - · 단일 호스트 기반의 침입탐지 시스템
  - · 다중 호스트 기반의 침입탐지 시스템
  - · 네트워크 기반의 침입탐지 시스템

- ㅇ 침입탐지 모델을 기반으로 하는 침입탐지 분류 방법
  - · 비정상적인 탐지 모델 기반의 침입탐지 시스템
    - 통계적인 방법(Statistical approaches)
    - 특징 추출(Feature Selection)
    - 예측 가능 패턴 생성(Predictive Pattern generation)
    - 신경망을 이용한 방법(The use of Neural Networks)

· 오용 탐지 모델 기반의 침입탐지 시스템
  - 전문가 시스템(Expert Systems)
  - 키 입력 관찰(Keystroke monitoring)
  - 모델에 근거한 침입탐지(Model based Intrusion Detection)
  - 상태 전이 분석(State Transition Analysis)

특히 침입탐지 모델을 기반으로 하는 침입탐지 분류 방법들 중 일부 침입탐지 모델들은 본 논문에 요구되는 침입 패턴 분석과 유형별 분류 및 탐지 방법 등을 연구하는데 많은 기반 정보들을 제공하였다. 따라서, 침입탐지 모델을 기반으로 하는 침입탐지 분류방법들을 자세히 살펴보면 다음과 같다[6,12,18].

2.1.1. 비정상적인 침입탐지 기법

비정상적 탐지 모델은 정상적인 행위패턴에서 벗어난 행위를 탐지하는 방법으로, Computer 자원의 비정상적인 행위에 근거하여 정의된 모델을 이탈하는 경우를 침입으로 간주한다. 그 종류로는 통계적인 방법(Statistical approaches), 특징 추출(Feature Selection) 방법, Anomaly measures의 결합 방법, 예측 가능 패턴 생성(Predictive Pattern generation) 방법, 그리고 신경망(Neural Networks)을 이용한 방법 등이 있다.

2.1.2. 오용 침입탐지 기법

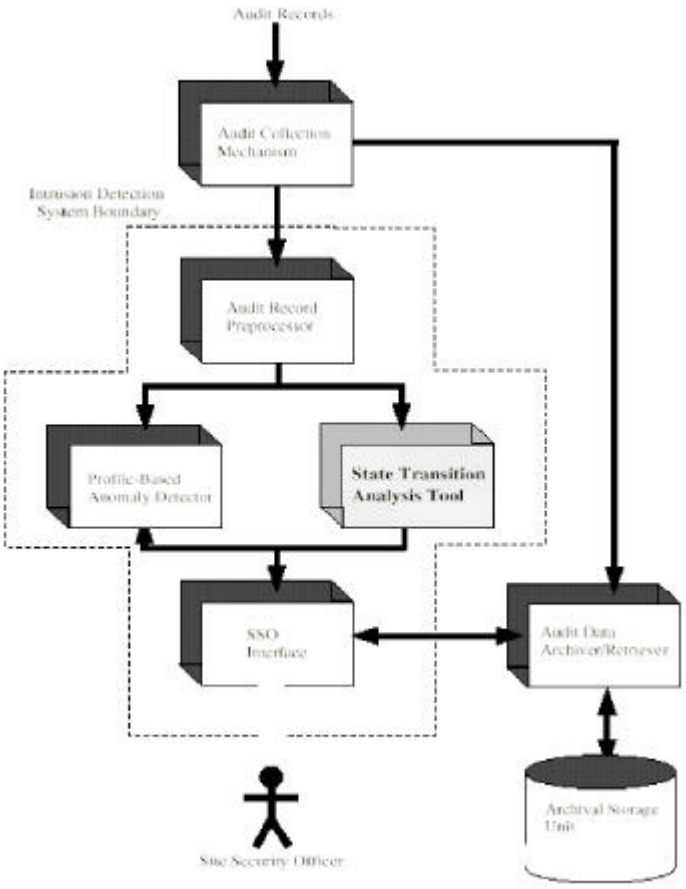
오용 탐지 모델은 이미 알려진 공격패턴을 이용한 탐지 방법으로, System이나 응용 소프트웨어의 취약점을 통하여 System에 침입할 수 있는 잘 정의된 공격을 정의하여, 정의된 모델과 일치하는 경우를 침입으로 간주한다. 종류로는 조건부 확률(Conditional Probability) 방법, 전문가 시스템(Expert Systems) 방법, 상태 전이 분석(State Transition Analysis) 방법, 그리고 키 입력 관찰(Keystroke monitoring) 방법, 모델 기반 침입탐지(Model-based Intrusion Detection)방법, 패턴 매칭(Pattern Matching) 등이 있다.

2.2 외부 침입탐지 시스템 유형

2.2.1. STAT

STAT(State Transition Analysis Tool)는 Porras가 Penetration State Transition Analysis라는 모델에서 만든 보안 응용 도구이다[15]. STAT는 침입을 상태 전이 다이어그램으로 표현하며, 시스템의 감사기록을 이용하여 시스템에 영향을 줄 수 있는 행위들에 대하여 기록을 남긴다. 또한, STAT는 전문가 시스템을 이용한 실시간적 처리 시스템으로서 다중 사용자의 감사 기록 분석을 위해 규칙 기반의 분석(rule-based analysis) 방법을 사용하여 단순한 침입 Rule chain부터 다양한 유형의 침입 행동을 탐지한다.

STAT의 구성은 침입탐지 감시 모듈에서 1차 필터링 작업을 하는 전처리기(Preprocessor), 어떤 공격에 대하여 취약점을 노출시킬 수 있는 특징을 가진 파일들의 집합으로 구성된 fact-base와 입력된 자료 그리고 fact-base의 내용을 근거로 새로운 정보의 추론을 위한 상태 전이 다이어그램에 대한 규칙을 나타내는 rule-base로 구성된 지식 베이스(Knowledge-base), 전처리기로부터의 입력받은 정보를 근거로 새로운 정보의 탐색에 있어 전문가 시스템의 다른 여러 가지 요소들을 사용하는 알고리즘들을 사용하여 새로운 정보를 추론하는 Inference Engine, SSO(Site Security Officer)에게 침입 상황을 보고하거나 침입에 대한 조치를 취하는 Decision Engine으로 구성되었다. [그림 2-1]은 STAT의 구성도로서 각 모듈간의 관계를 잘 나타내고 있다.



[그림 2-1] STAT 구성도

STAT에서 침입탐지를 위해 사용하는 여러 규칙들과 요소들을 살펴보면 fact-base나 rule-base, state descript, 시스템내의 파일, 디렉토리의 소유권한(group ID, Effective ID, Real ID), 접근 권한(Permission mode, owner), 사용하는 프로세스 등 주로 시스템의 정보나 내부의 자원들이 중심이 되어 침입 여부를 판정하는데 기본 자료로서 제공되어 진다.

그러나, STAT는 시스템 중심의 침입탐지 시스템으로 침입 판정을 위한 판정 데이터들이 시스템 내부의 자원들만을 중심으로 이루어져 있으므로 네트워크 패킷들을 이용한 침입탐지에 있어서 그 기능이 제대로 발휘될 수 없다.

2.2.2. IDIOT

IDIOT (Intrusion Detection In Our Time)는 1996년 Purdue대학의 COAST 연구실에서 개발한 침입탐지 시스템으로서 효과적인 오용 탐지 방법으로 접근을 시도한 전문가 시스템이다[9,13,20]. IDIOT는 시스템의 상태를 나타내는 동그란 원형태의 "state"와 transition인 thick bar로 표시하는 Colored Petri nets을 기반으로 한 패턴 매칭 엔진을 구현하였다. IDIOT는 패턴들을 크게 세 가지로 나누어 설명하고 있는데 그 내용은 아래와 같다.

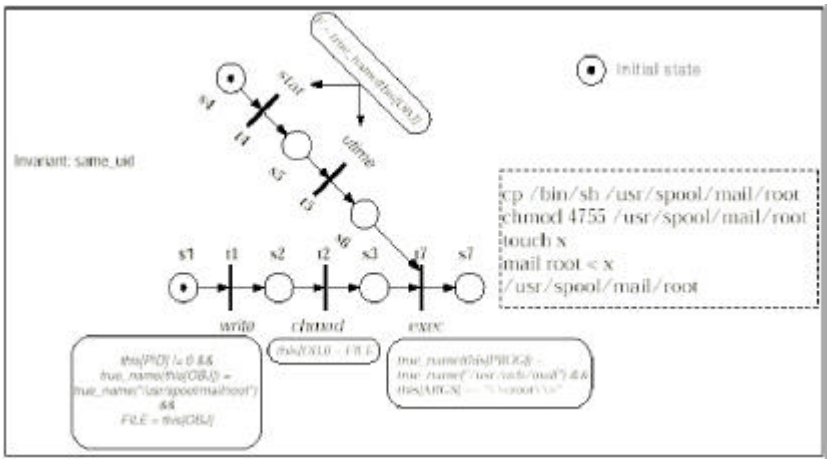
- Written and tested patterns
  실제 환경에서 사용되는 검증되는 침입 패턴들

- Written and not tested patterns
  IDIOT에서 구현은 되었으나 시간이나 audit trail의 제약성들로 검증과정을 거치지 않은 패턴들

- Theoretical patterns
  IDIOT에서는 검증할 수 없는 부분으로, 특별한 목적에서 시험적으로 구현

Colored Petri Automation(CPA)은 적어도 하나 이상의 초기 상태(intial state)와 CPA에 의해서 일치되는 string의 집합으로 정의되는 마지막 상태(final state)가 존재하며, 매칭되는 패턴들은 각 초기 상태에서 마지막 상태까지 상태의 진행 동안 merge 혹은 duplication된다.

그러나 IDIOT에서 적용되는 모델은 CP-Nets의 concurrency, local transition variables, start state, final state 등의 정의에 대한 부분적인 수정을 하여 적용하였으며, CP-Nets과는 달리 이분화되는 것을 허락하지 않으며, 실제 시스템 기반의 탐지요소들을 중심으로 개발된 탐지 시스템으로 네트워크 패킷 분석에 대한 탐지 요소와 구체적인 방법을 제시하지 못함에 따라, 네트워크 기반의 침입탐지에 있어서는 한계성을 가지고 있다. [그림 2-2]는 IDIOT에서 실제 침입탐지시 사용되는 Petri nets에 대한 예를 보여 주고 있다.



[그림 2-2] IDIOT에서 사용하는 Colored Petri net 예제

2.2.3. NADIR

NADIR(Network Anomaly Detection and Intrusion Reporter)을 Los Alamos National 연구소의 ICN(Integrated Computing Network)에서 시스템 침입에 대하여 실시간적인 보안 탐지를 제공하는 오용 탐지 시스템(Misuse Detecting System: Automated expert system)으로서 시스템의 동작은 각 호스트나 사용자에 대한 사전 정보를 기반으로 한다[14]. 사전에 네트워크에 대한 보안 정책과 모든 사용자 및 데이터들에 대한 보안 등급 설정을 요구하고, 중앙 시스템에 의해 네트워크 호스트들로부터 사용되는 프로토콜에 대한 정보, 제공되는 서비스들로부터 발생되는 네트워크 트래픽 등의 데이터를 수집 등, 네트워크 수준에서의 침입들이 탐지된다. NADIR는 세 가지의 서비스 노드들로부터 데이터를 입력받는데 각각의 노드들의 역할은 다음과 같다.

- NSC(Network Security Controller)
  ICN에서의 접근제어와 인증

- CFS(Common File System)
  파일 저장 시스템(37 TByte)

ㅇ SAM(Security Assurance Machine)

CFS내의 분류되지 않은 파일들을 down-partition하려는 모든 시도들을 기록하거나 인증

이러한 세 개의 노드들로부터 매일 축적되는 individual audit record들은 거의 40,000개에 달하며, 네트워크 보안 정책으로부터 네트워크 각 사용자들의 보안 정책을 위반하는 행동에 대한 탐지를 할 수 있다. 네트워크 관리자의 요구에 따라 로그온 실패 횟수, 패스워드 입력오류 등, 일별 혹은 주간별로 각 사용자들에 대한 통계 분석 요약과 같은 방법을 취하기도 한다. 그러나 이와 같은 방법은 네트워크 사용자에 대한 사전의 철저한 분석, 보안 정책 수립, 보안 관리자들의 보안 관리능력을 요구하며 막대한 파일 저장 시스템 등, 네트워크 사용에 있어 아주 높은 보안성 유지와 관리 능력을 요구한다.

2.3 내부 침입탐지시스템 유형

2.3.1 Sniffing탐지 시스템

스니핑은 Ethernet LAN환경에서 모든 네트워크 트래픽을 분석하여 불법적으로 정보를 수집하는 공격기법이다. 이더넷 인터페이스는 LAN상의 개별 호스트를 구별하기 위해 MAC주소를 갖게 되며, 모든 이더넷 인터페이스의 MAC주소는 서로 다른 값을 갖는다. 따라서 로컬 네트워크상에서 각각의 호스트는 유일하게 구별될 수 있다. 이더넷에서 패킷의 전송과정을 살펴보면 같은 임의의 컴퓨터에서 전송된 패킷은 같은 LAN상의 모든 컴퓨터에 broadcasting된다. 따라서 같은 네트워크내의 컴퓨터는 다른 컴퓨터로 전송되는 모든 트래픽을 볼 수 있다. 하지만 네트워크 성능 저하 등의 이유로 이더넷 인터페이스는 자신의 MAC주소를 갖지 않는 트래픽을 무시하는 필터링 기능을 가지고 있다. 이 필터링에 의해 자신의 MAC address를 가진 트래픽만을 보도록 한다. 이더넷 인터페이스에서 네트워크상의 모든 패킷을 볼 수 있도록 하는 기능을 설정할 수도 있는데 이를 “promiscuous mode"라 하며, Sniffing기법은 이러한 “promiscuous mode"를 이용하여 내부망에서 전송되는 모든 트랙픽을 도청하는 기법이다.

이러한 Sniffer를 탐지하기 위한 방법으로 스위칭 허브를 사용하는 기법과 주기

적으로 호스트가 “promiscuous mode"로 설정되어 있는지 점검하여 Sniffer를 탐지하는 기법이 있다. 다음은 로컬 네트워크 내에서 Sniffer를 탐지할 수 있는 기법들이다.

- ICMP를 이용한 방법
  ICMP를 이용한 방법은 본 논문에서 설계한 Sniffer 탐지 시스템에서 적용한 방법으로 같은 LAN상에서 Sniffier로 의심되는 host에게 거짓 ICMP패킷을 전송하여 이에 대한 응답여부로 침입을 탐지하는 방법이다.

- PING을 이용한 방법
  대부분의 Sniffer는 일반 TCP/IP 스택상에서 동작하기 때문에 request를 받으면 그에 해당하는 response를 전달하게 된다. ping을 이용한 Sniffer 탐지 방법은 의심이 가는 시스템에서 ping을 보내는 기법으로 이때 전송되는 request패킷에 MAC주소를 위장하여 보내는 방법이다.

- ARP를 이용하는 방법
  ping방법과 유사한 방법으로 non-broadcast로 위조된 ARP request를 보냈을 때 ARP response가 오면 상대방 호스트가 Sniffer인 것으로 탐지하는 방법이다.

- DNS방법
  일반적으로 sniffing 프로그램은 사용자의 편의를 위하여 스니핑한 시스템의 IP주소를 보여주지 않고 도메인 네임을 보여주기 위하여 Inverse-DNS lookup을 수행하게 된다. 이러한 성질을 이용하여 DNS트래픽을 감시하여 Sniffer를 탐지하는 방법이다. 이 방법은 외부·내부 네트워크 모두에서 사용할 수 있는 방법이다. 원격에서 테스트 대상 네트워크로 Ping sweep을 보내고, 들어오는 Inverse-DNS lookup을 감시하여 Sniffer를 탐지하며, 로컬에서 사용할 경우에는 위조된 IP주소로 IP datagram을 보내고 이에 대한 DNS lookup이 있는지 검사하여 Sniffer를 탐지한다.

이처럼 관리자가 Sniffer탐지 도구를 이용하여 주기적으로 Sniffer의 설치 여부를 감시함으로써 내부 공격자를 탐지할 수 있지만, 이 자체만으로는 외부에서 들

어오는 다양한 공격 기법들을 대처하기 힘들다.

2.3.2 ARPwatch

ARPwatch는 ARP트래픽을 모니터링하여 MAC/IP 매칭을 감시하는 프로그램으로 초기에 설정된 ARP 엔트리가 변하게 되면 이를 탐지하여 관리자에게 메일로 통보해 주는 도구이다. 내부 공격의 많은 기법들이 위조된 ARP를 사용하기 때문에 내부 공격자를 쉽게 탐지 할 수 있다. [그림 2-3]은 "arpwatch -d"를 실행하여 초기 ethernet/ip쌍에 대한 데이터베이스를 만든 것이다. 이후 "arpwatch"를 실행하게 되면 추가되거나 변경되는 ethernet/ip쌍에 대하여 메일을 통하여 ARP를 이용한 공격을 탐지한다.

0:x:x:a3:x:6a	172.x.x.1	963475326
0:x:x:c4:x:3e	172.x.x.1	963473482
8:x:x:79:x:ea	172.x.x.71	963465559
0:x:x:c4:x:3e	172.x.x.80	963474080
0:x:x:28:x:47	172.x.x.82	963469967
8:x:x:b7:x:72	172.x.x.45	963475326
...	...	...

arp.dat 파일("arpwatch -d"로 모니터링한 결과)

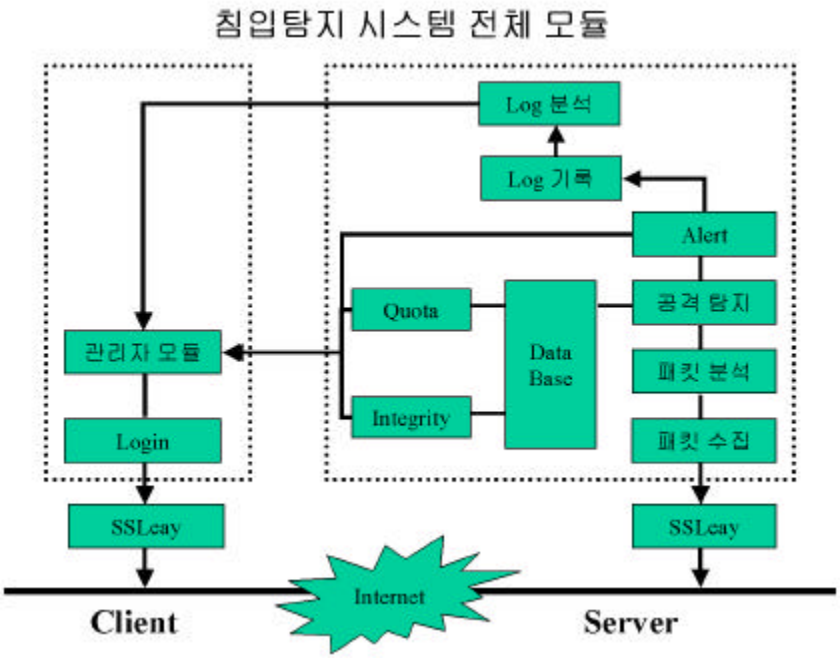
[그림 2-3] ARPwatch 실행 결과

Ⅲ. 내 · 외부 침입탐지시스템 통합 모듈 설계

네트워크를 이용한 침입 방법에는 특정 프로토콜의 패킷 헤더를 변조한 침입, 그리고 네트워크 트래픽을 이용한 서비스 거부 공격 등의 외부 침입과 침입에 취약한 프로토콜을 이용한 네트워크 내부로의 침입 있으며, 이러한 네트워크 상에서 침입 시도는 해가 갈수록 증가되고 다변화되고 있다. 본 장에서는 기존의 상용 침입탐지 시스템 제품들에서 제시하는 네트워크 기반에서의 침입탐지 항목들과 실제 발생되고 있는 해킹 사례들 그리고 몇몇 침입탐지 관련 연구 논문들을 종합 분석 및 정리하고 이를 기반으로 내·외부 침입탐지시스템 통합 모듈 설계에 대해 설명한다.

3.1. 외부 침입탐지시스템 모듈 설계

본 절에서는 내·외부 침입탐지시스템 모듈 중 외부 침입탐지 시스템 모듈들에 대한 상세 설계에 대해 살펴본다. 아래 [그림 3- 1]은 본 논문에서 설계된 실시간 외부침입탐지 시스템의 전체적인 구조를 나타낸다.



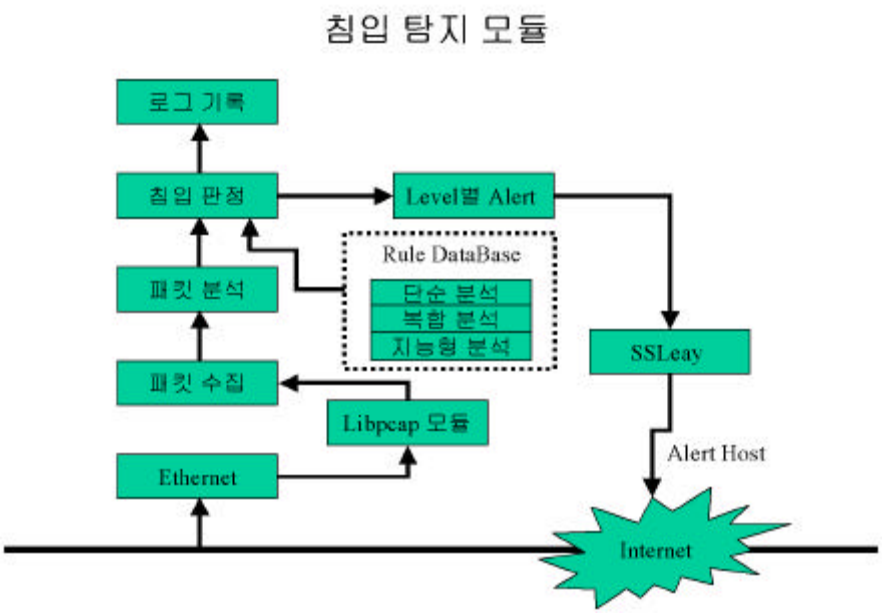
[그림 3-1] 외부 침입탐지 시스템 전체 구조

외부 침입탐지시스템은 크게 침입을 탐지하는 서버(Server) 모듈과 침입탐지 보고 분석, 탐지를 위한 설정 그리고 침입탐지 로그 정보를 관리할 수 있는 관리자 모듈인 클라이언트(Client) 모듈로 구분되어 있다. 그리고 서버와 클라이언트 사이의 안전한 통신을 보장하기 위해서 SSL(Secure Socket Layer)을 사용하였다.

3.1.1. 외부 침입탐지 모듈

네트워크를 연속적으로 모니터링하고, 침입 행위를 감지하는 모듈이다([그림 3-2]참조). 네트워크의 모든 패킷들을 수집하고 수집된 패킷을 이용하여 침입과 관련된 패킷들을 찾아낸다. 그리고 침입 가능성이 있거나 침입과 관련성이 있는 패킷으로 간주할 수 있는 정보들을 침입 유형에 대한 규칙 정보와 비교함으로써 침입 여부를 판정한다. 그리고 침입으로 판정되었을 경우, 침입 사실에 대한 정보

를 관리자 모듈로 보고한다.



[그림 3-2] 외부 침입탐지 모듈

가. 네트워크 패킷 수집 모듈

네트워크 패킷 수집 모듈은 네트워크로부터 침입탐지를 위한 초기 작업이 이루어지는 부분으로 네트워크 기반의 침입탐지의 기본 자료가 되는 패킷들을 수집한다. 침입탐지 시스템은 네트워크 상에 있는 모든 패킷들을 감시 및 분석하며, 탐지하는 시스템이 설치된 호스트의 네트워크 상태가 모든 패킷을 수신할 수 있도록 Promiscuous mode로 되어 있어야 하고, 가공되지 않은 Ethernet layer or IP layer에서의 패킷(low packet)을 처리할 수 있어야 한다.

나. 네트워크 패킷 분석 및 Reduction 모듈

침입탐지 수집모듈로부터 탐지되는 로컬 네트워크상의 모든 패킷들 중에서 실시간 침입탐지 시스템으로부터 침입관련 패킷으로 규정된 탐지 대상 패킷들과 무관한 패킷들을 제거(drop)하고 침입탐지의 효율성을 높이기 위해서는 패킷의 분

석과 reduction 기능을 필요로 한다. 침입 판정을 위한 침입 유형과 비교할 때 사용될 수 있는 데이터로 가공하는 모듈이다. 또한, 패킷 reduction은 몇 가지 구체적인 기능을 제공함으로서 침입 판정 모듈에서 모든 네트워크 패킷들로부터의 침입 여부를 결정하는데 있어 발생되는 overhead를 줄일 수 있다.

1) Packet filtering(패킷 필터링)

네트워크 상에 사용되고 있는 수많은 종류의 패킷들 중에서 기존의 침입 사례나 침입 관련 보고서들로부터 침입과 관련된 패킷들만을 추출하는 필터링 작업을 실시한다. 이 과정으로부터 침입 판정 모듈에서는 침입과 관련 없는 패킷들에 대한 침입 여부를 확인 절차를 생략함으로써 보다 신속한 침입 판정에 효율성을 제공할 수 있다. 예를 들어 Internet Protocol로써 사용되는 ARP, RARP, IP, ATALK, 등의 여러 프로토콜로부터 네트워크 침입과 긴밀한 연관성을 갖는 ICMP, IP(TCP, UDP) 패킷들만을 대상으로 필터링(packet filtering)을 하게된다.

2) 단순 침입탐지(Simple Intrusion Detection)

패킷 reduction 과정에서 얻을 수 있는 또 다른 효과는 Source probing(로컬 네트워크로의 접속이 허락되지 않는 주소지로부터의 접근을 탐지)과 Port probing (공격자가 사용이 제한된 특정 서비스 혹은 포트를 사용하여 접속하는 것을 탐지) 등과 같은 명확하고 단순한 침입 형태들은 침입 행위 판정 모듈의 도움 없이 하나의 패킷 분석만으로도 침입 여부 판정이 가능하다는 장점을 살려 자체적인 판정이 가능하다는 것이다.

따라서, reduction 과정에서 탐지된 침입들은 침입 판정 모듈에서 시행되는 침입탐지 과정을 다시 거치게되는 중복 과정이 생략됨으로써 전체 시스템의 효율성을 향상시킨다. 만일 이러한 패킷이 다른 침입 형태와 연결된 가능성에 대하여서는, 단순 침입탐지 이후에도 관리자의 요구에 따라 지속적인 감시를 함으로써 구체적인 침입 행위의 증거 자료들을 확보할 수 있을 것이다.

3) 패킷 재구성(Packet Reformatting)

Reduction 모듈은 패킷 재구성 기능을 제공함으로 침입 판정 모듈에서 최소의

정보와 최적의 정보 구성이 이루어진 데이터로부터 능률적인 판정기능을 수행할 수 있다.

패킷으로부터 침입을 판정하기 위해서는 특정 프로토콜에서 사용하는 패킷 헤더와 데이터가 삽입되는 내용(contents)으로부터의 침입 관련 여부의 측정이 필요하다. 따라서 침입 판정 모듈에서는 일부 침입탐지 항목들에 대한 패킷의 내용으로부터 침입 여부를 판정하기 위해 여러 개의 패킷들의 재조합 과정이 필요하고, 이렇게 재조합된 내용(Command, Directory, file name, 등)들로부터 침입을 판정하게 된다.

다. 침입 판정 모듈

패킷 Reduction 모듈로부터 전달되는 정보는 어느 정도 침입의 가능성이 있거나 침입과 관련이 있는 패킷으로 간주할 수 있으며 이러한 정보와 이미 저장되어 있는 침입 유형에 대한 규칙 정보를 비교함으로써 침입 여부를 판정하게 된다.

네트워크의 패킷을 이용한 침입탐지 방법은 단순 정보에 의한 침입탐지와 여러 패킷으로부터 수집된 정보를 기준으로 침입을 탐지하는 방법이 있다. 또한 여러 패킷으로 수집된 정보를 기준으로 침입을 탐지하는 경우 패킷의 트래픽을 이용하여 침입을 탐지하는 방법과 입력 명령어들을 조합하여 침입을 판정하는 방법이 있다.

[그림 3-3]은 침입행위 판정 모듈에 대한 내부 구성도이다. 이는 판정 작업의 성격에 따라 단순 분석기(Simple Analyzer), 고난도 분석기(Complex Analyzer), 지능형 분석기(Intelligent Analyzer)로 구성된다.

[그림 3-3] 침입 판정 모듈의 내부 구성도

시스템의 기능확장과 성능에 있어서 효율성을 고려하여, 본 논문에서는 단순 분석기와 고난도 분석기를 하나의 프로세스에서, 그리고 지능형 분석기를 새로운 프로세스에서 처리하도록 하였다.

라. 침입탐지 로그 파일(Alert 로그 파일)

Alert 로그 파일은 침입탐지 시스템이 탐지한 공격자의 모든 침입 관련 사항들에 대한 기록을 보관한다. 로그 파일 생성은 침입탐지에 의해 침입보고 모듈로 전송되는 내용을 동일한 형태로 기록하고 추후 사용자에게 침입에 대한 근거 자료 및 침입 상황에 대한 통계 자료로써 제공된다.

3.1.2. 규칙 데이터베이스(Rule DataBase)

규칙 데이터베이스는 분석기가 침입을 탐지시, 각 분석기들이 탐지하게 될 침입 패턴들이나 Audit Record Collector에서 전처리 기능, 기타 침입 판정의 근거가 되는 모든 자료들을 보관한다. 규칙 데이터베이스에는 주소지와 포트를 기반으로 한 침입탐지 규칙 데이터베이스와 침입 관련 스트링을 기반으로 한 침입탐지 규칙 데이터베이스가 있다.

가. 주소지와 포트를 기반으로 한 침입탐지 규칙 데이터베이스

패킷 헤더의 정보를 이용한 침입 여부를 판정하는 기능 모듈에 대한 데이터베이스로서, [표 3-1]과 같은 형식으로 관리되며 내부 구조는 [그림 3-4]과 같다.

[표 3-1] 주소지와 포트 기반의 침입탐지 규칙 데이터베이스

체크 비트	서비스	포트 번호	소스 주소	목적지 주소	alert 메시지
✓	TCP	23	203.247.166.27	203247.166.40	특정 서비스를 사용하는 특정 주소

```
typedef  struct{
    char proto[5];
    char port[5];
    char src[20];
    char dst[20];
    int checkpoint;
    char message[100];
} filter;
filter  filterbuf[FILTER];
```

[그림 3-4] 주소지와 포트 기반의 침입탐지 규칙의 내부 구조

[표 3-1]에서 데이터베이스의 각 항목들의 경우의 수를 조합함으로써 더욱더 다양한 침입탐지 규칙을 적용할 수 있다. 체크 비트는 이러한 규칙들을 실제 침입탐지시 적용할 것인지 아닌지를 결정한다. 예를 들어서 특정 주소에서 특정 목적지와 특정 서비스를 사용하는 침입을 탐지할 경우 체크 비트 체크, 서비스, 목적지 주소, 소스 주소에 대한 값을 저장함으로써 규칙을 설정할 수 있다.

나. 침입 관련 스트링을 기반으로 한 침입탐지 규칙 데이터베이스

[그림 3-5]는 입력되는 침입 관련 스트링과 관련된 데이터베이스에 대한 구조를 나타내고 있다. 내부에 선언되어 입력되어지는 내용들은 다음과 같이 선언된 정의를 기준으로 침입을 탐지하기 위한 보안 데이터베이스를 구축하게 된다.

```
id          ID2
title       serial patten 1
alert       1
service     telnet
begin
<read>&"/bin/sh"&"/mail/root": ID2 first intrusion message
"chmod"&"4755"&"/mail/root":
"touch"
"mail"&"root"&"<"
"/mail/root":very dangerous state
end
```

[그림 3-5] 침입패턴 탐지 규칙 데이터베이스

1) 보안 데이터베이스 구조와 정의들

- **id** : 특정 침입패턴에 대한 식별자

- **title:** 침입 패턴에 대한 Title - 침입종류에 대한 제목

- **alert**: 침입종류에 따라 침입의 위험도와 관리자에게 침입 사실을 알리는 침입보고 방법을 정의

- **service:** 침입 패턴을 탐지하고자 하는 서비스를 정의.
  여기서의 서비스란, TCP를 기반으로 하는 네트워크 서비스로서 telnet , e-mail, http, ftp, rsh, rlogin, pop3과 같은 응용계층에서 제공되는 서비스들로 한정된다.

- **begin ~ end** : 탐지할 침입에 대한 규칙을 선언한다.
  규칙에 대한 설정은 [그림 3-6]에서 정의한 기호를 이용하여 표현한다. 또한 사용자가 특정 침입 패턴이 발생했을 시 전송 받을 사용자 정의 메시지를 추가할 수 있도록 하였다. 2장에서 [그림 2-2]에서 예제로 보여준 IDIOT의 탐지 항목은 본 시스템의 데이터베이스에서는 [그림 3-9]의 begin과 end 사이의 내용으로 정의되어 탐지된다.

<•••>	동일한 속성을 갖는 침입 탐지 인자들의 집합	
"•••"	침입과 연관된 특정 입력 스트링	*"cd /root"*
&	AND	
|	OR	

[그림 3-6] 입력된 패턴탐지 규칙에 사용되는 기호 정의

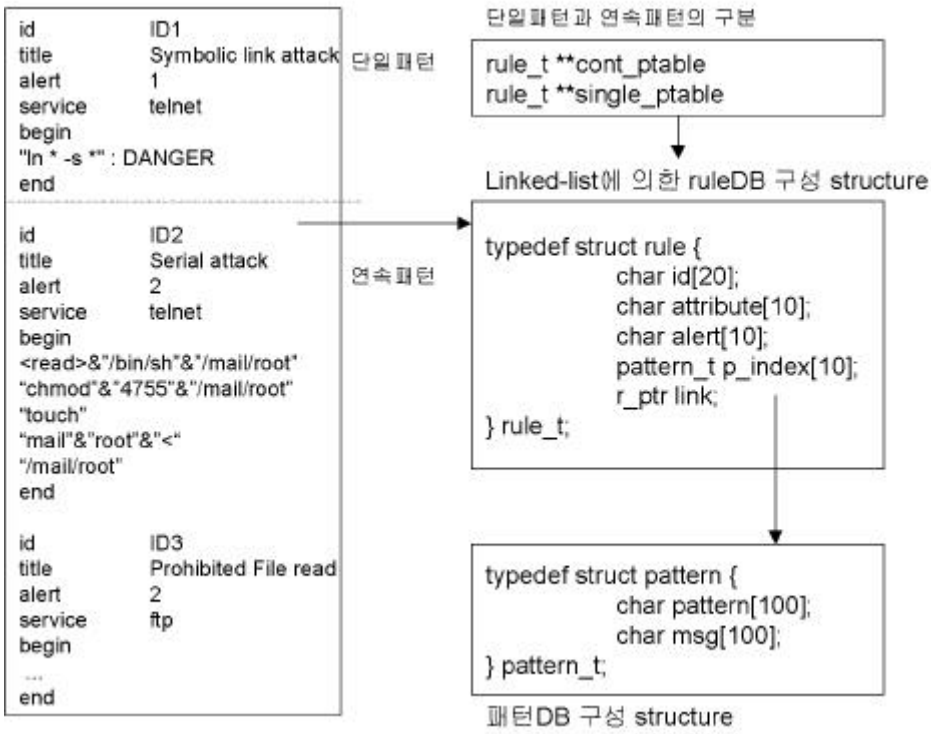
2) 침입탐지 규칙 설정

[그림 3-6]에서 정의된 기호에 대한 자세한 설명과 [그림 3-7]의 begin~end 사이에 선언된 내용을 중심으로 사용자가 패턴 탐지 규칙을 선언하는 방법에 대하여 설명하기로 한다.

<read>&"/bin/sh"& "/mail/root" 라는 규칙 선언은 연속된 패턴의 침입 유형으로, “<” 과 “>”사이에 입력되는 문자열은 침입탐지와 관련하여 특징을 갖는 명령들 혹은 인자들의 집합을 표시하는 것이고, 실제 시스템내의 파일이나 디렉토리를 읽는 것과 관련된 명령어들을 포함하고 있는 ‘read.key"라는 파일의 확장명을 제외한 파일명만을 표기한 것이다. 그리고 “/bin/sh"처럼 큰따옴표 사이에서 정의된 문자열은 침입탐지와 관련한 탐지 문자열을 선언한 것이다. 그리고 ’&‘는 보통 연산자에서 사용하듯이 AND 역할을 한다. 그러므로 begin과 end사이에 선언된 「<read>&"/bin/sh"& "/mail/root"」의 정의는 다음과 같다.

※「<read>&"/bin/sh"& "/mail/root" : MESSAGE」
read.key에 선언된 명령어로서 “/bin/sh"과 ”/mail/root"라는 스트링이 하나의 명령열에서 입력된 것을 탐지하고 MESSAGE를 사용자에 출력한다. MESSAGE는 사용자의 요구에 따라 해당 규칙에 포함하거나 미포함할 수 있다.

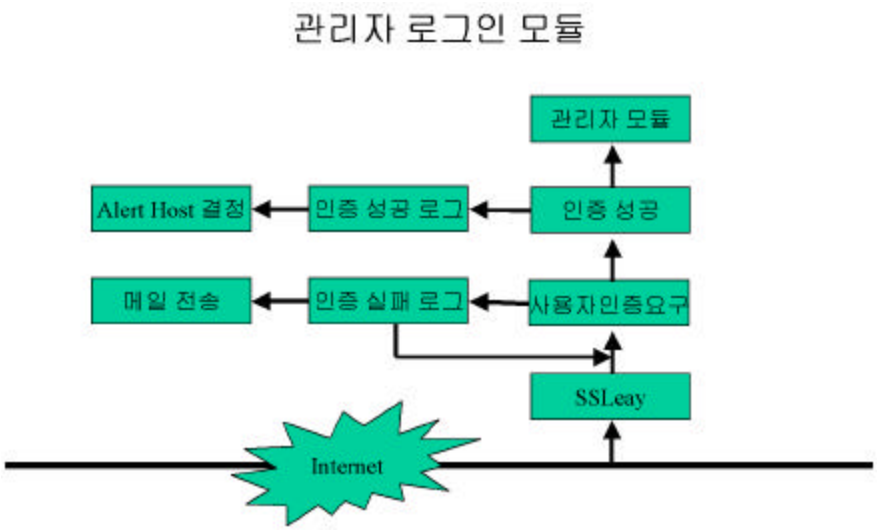
이러한 문법 정의는 사용자가 새로운 침입 패턴에 대한 추가와 패턴 정의가 쉽게 이루어진다는 장점이 있다. [그림 3-5]는 연속된 침입 패턴에 대한 내용을 나타낸 것으로 단일 패턴에 대한 규칙 설정에 있어서도 동일한 방법으로 선언하면 된다. 보안 데이터베이스에 저장된 단일과 연속 패턴에 대한 규칙선언과 내부 구성은 [그림 3-7]에서 보는 바와 같다.



[그림 3-7] **침입 패턴 규칙과 내부** Structure

3.1.3. 관리자 로그인 모듈

본 논문에서 설계한 침입탐지 시스템은 웹브라우저를 이용하여 관리자가 인터넷을 통해 원격으로 관리할 수 있는 기능을 제공하고 있다. 그러므로 침입탐지 시스템이 설치된 특정 로컬 시스템이 아닌 인터넷이 연결된 곳이라면 어디서든지 관리자가 침입 상황을 보고 받을 수 있으며, 침입탐지에 필요한 설정값 및 그 외의 설정값들을 관리할 수 있다.



[그림 3-8] 관리자 로그인 모듈

웹브라우저는 그 특성상 다양한 사용자에게 개방되어 있는 형태로 사용되지만, 이를 침입탐지 시스템 관리에 이용하기 위해서는 침입탐지 시스템의 중요한 옵션 설정(규칙 추가, 로그 관리 등)을 인가된 관리자에게만 수행할 수 있도록 하여야 한다. 그러므로 본 논문에서는 로컬 호스트에서 유닉스의 DES 암호화 알고리즘을 이용하여 관리자의 ID와 패스워드를 생성하도록 하였다. 원격 로그인시 ID와 패스워드를 입력하게 되는데, 이때 미리 생성된 ID와 패스워드를 비교하여 관리자의 로그인 여부를 결정하게 된다. 그리고 사후 처리를 위하여 로그인의 성공과 실패에 대한 로그 기록을 남기는데, 이때 로그 기록은 동일한 형태를 구조로 저장되며, 이들을 각각 다른 데이터 파일에 남기도록 하였다. 또한, 3회 이상 로그인 실패시 그 사실에 대해서 관리자에게 메일을 전송하도록 하였다.

[표 3-2]은 로그인의 성공과 실패에 대한 로그 기록의 형태를 보여준다.

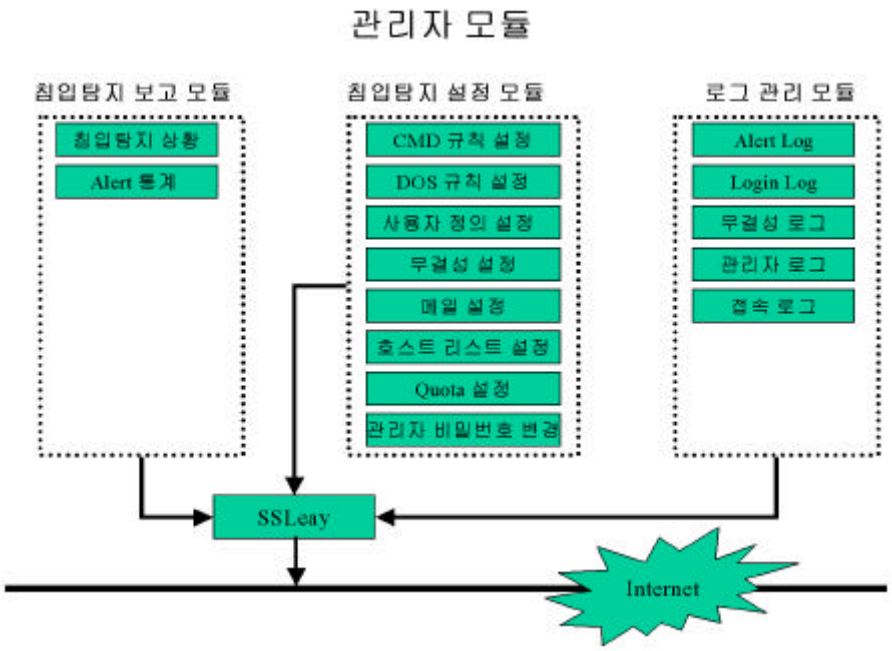
[표 3-2] 로그인 로그기록 형태

접속 주소	ID	접속 시간
203.247.166.27	admin	Wed Oct 11 22:11:52 2000

그리고 로그인 및 관리자 전체모듈은 웹을 기반으로 하기 때문에 데이터 송·수신시 보안 취약점을 내포하고 있다. 그러나 본 논문에서는 서버와 클라이언트 사이에 데이터 송·수신시 SSL(Secure Socket Layer)을 이용하여 데이터 무결성 및 암호화를 제공한다.

3.1.4. 관리자 모듈

관리자의 원격 로그인 성공시 수행될 수 있는 모듈로써 침입탐지 시스템의 탐지 상황 및 다양한 설정값들을 관리할 수 있는 모듈이다. 즉, 침입이 발견되었을 때 침입 상황을 파악할 수 있고 침입 발견시 기록되는 경고(alert) 정보에 대한 통계 데이터를 볼 수 있도록 하였다. 또한, 침입 발견을 위한 다양한 규칙, 중요 데이터의 무결성 처리 그리고 다양한 로그 정보들이 저장되는 저장 공간을 관리할 수 있는 Quota 등에 대하여 설정할 수 있다. 그리고 로그 정보들을 관리할 수 있는 모듈이다.



[그림 3-9] 침입탐지 시스템 관리자 모듈

관리자 모듈은 크게 침입탐지 상황 모듈, 설정 모듈, 로그 관리 모듈의 3가지 모듈들로 구성되어 있다.

가. 침입탐지 보고 모듈

침입탐지 보고 모듈은 침입판정 모듈로부터 탐지 내용을 사용자에게 지정된 형식으로 전송한다. 본 시스템에 있어서는 C 언어로 구현한 침입을 탐지하는 시스템 엔진 부분과 웹 브라우저와 자바를 이용하여 침입 결과에 대한 내용을 사용자가 확인할 수 있는 관리자 부분으로 나뉘어 있다. 따라서 침입탐지 보고 모듈은 시스템 엔진과 사용자 관리 부분사이에서 Socket을 사용하여 UDP 패킷을 전송함으로 시스템에서 요구하는 데이터들을 송/수신한다.

나. 침입탐지 설정 모듈

침입탐지 설정 모듈은 침입 발견을 위한 다양한 규칙(rule) 설정, 중요 데이터의 무결성 처리를 위한 설정 그리고 다양한 로그 정보들이 저장되는 저장 공간을 관리할 수 있는 Quota 등에 대하여 설정할 수 있다.

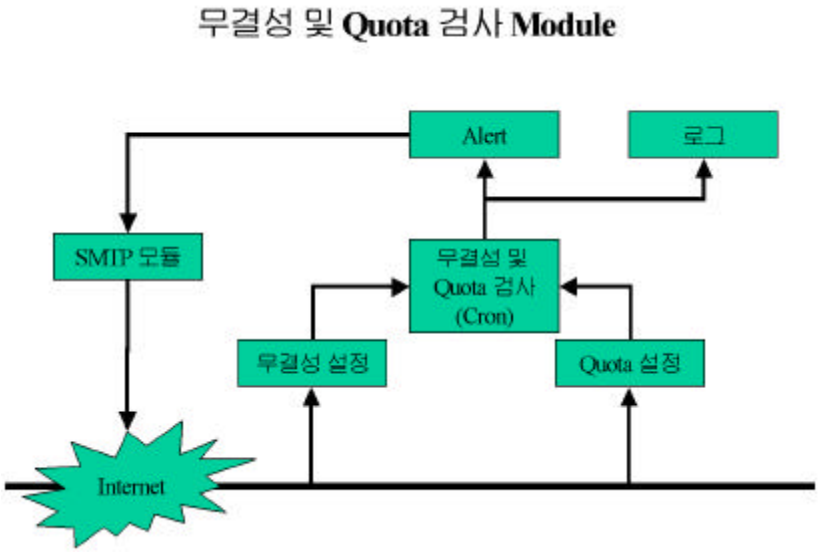
다. 로그 관리 모듈

로그 관리 모듈은 침입탐지 시스템에서 기록되는 로그 파일들을 관리한다. 지난 로그 정보들을 확인할 수 있고 더 이상 로그 정보로서 저장할 필요가 없어진 정보들을 삭제할 수 있다.

3.1.5. 데이터 무결성 및 Quota 검사 모듈

침입탐지 시스템에서 중요한 파일들(침입 판정시 적용될 규칙 정보, 탐지시 기록되는 로그 정보 등)에 대한 무결성 검사와 침입탐지 시스템이 설치된 하드디스크 파티션 용량을 검사하여 사용중인 하드디스크 용량이 일정한 한계치를 초과하였을 경우 관리자에게 메일을 전송한다.

아래의 [그림 3-10]은 무결성 및 Quota를 검사하는 모듈을 나타낸다.



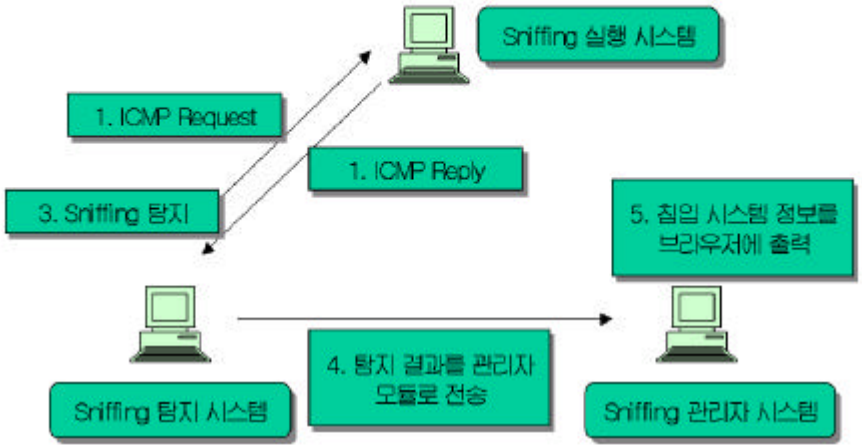
[그림 3-10] 무결성 및 Quota 검사 모듈

무결성 검사를 통하여 특정 파일의 다양한 정보변경 유무를 판단하는데, 이때 검사되는 정보로는 파일의 내용, 파일의 퍼미션, 파일의 소유자(uid)와 그룹(gid) 그리고 파일이 가장 최근에 수정된 날짜 등이 있다.

또한, 침입탐지 시스템을 장시간 구동시켰을 경우 다량의 로그 정보들이 계속해서 기록된다. 이때 하드디스크의 여유공간 부족으로 인하여 침입탐지 시스템이 중단되는 경우가 발생할 수 있다. 그러므로 침입탐지 시스템이 설치된 하드디스크의 파티션 용량을 체크함으로써 과도한 로그 정보로 인한 침입탐지 시스템의 중단을 미연에 예방할 수 있다.

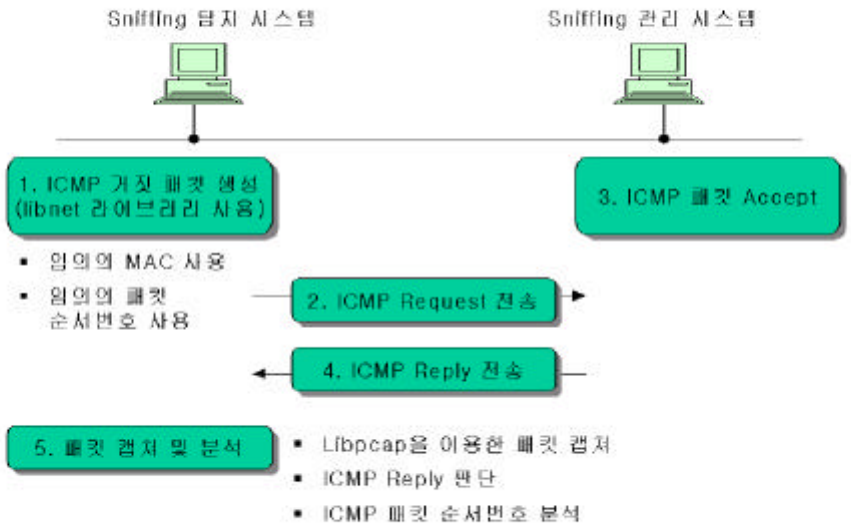
3.2. 내부 침입탐지시스템 모듈 설계

본 절에서는 내·외부 침입탐지시스템 모듈 중 내부 침입탐지 시스템 모듈들에 대한 상세 설계에 대해 살펴본다. 아래 [그림3-11]은 본 논문에서 설계된 실시간 내부침입탐지 시스템의 전체적인 구조를 나타낸다.



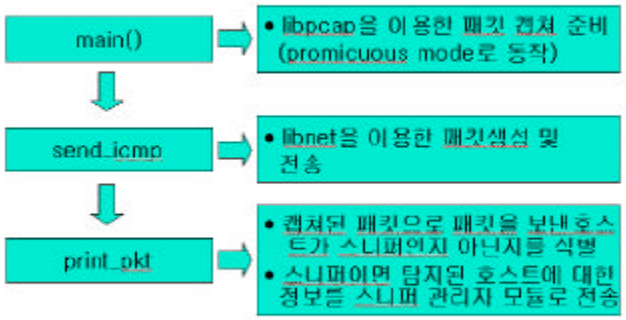
3.2.1. 내부 침입(Sniffing)탐지 모듈

스니핑 탐지 시스템에서는 libnet라이브러리를 이용하여 실제 거짓 패킷을 만들고 libpcap라이브러리를 이용하여 캡쳐된 패킷을 분석함으로써 침입을 탐지한다. 스니핑 탐지 시스템 모듈 흐름도는 [그림3-12]와 같다. 위의 그림을 살펴보면 우선 스니핑 탐지 host에서 같은 LAN상에 도달할 수 없는 임의의 MAC 주소와 패킷 sequence number로 거짓 패킷을 생성한다. 이렇게 생성된 패킷을 ICMP request를 이용하여 스니핑이 의심되는 host에 송신한다. 만약 ICMP request패킷을 송신한 host가 스니퍼로서 promiscuous mode로 동작하고 있다면 자신의 MAC 주소와 같지 않은 ICMP request패킷을 받아들이고 이에 대한 응답으로 ICMP reply신호를 스니핑 탐지 host에 보낸다. 스니핑 탐지 host는 libpcap라이브러리를 이용하여 ICMP reply패킷을 캡쳐하고 분석하여 분석된 패킷의 sequence



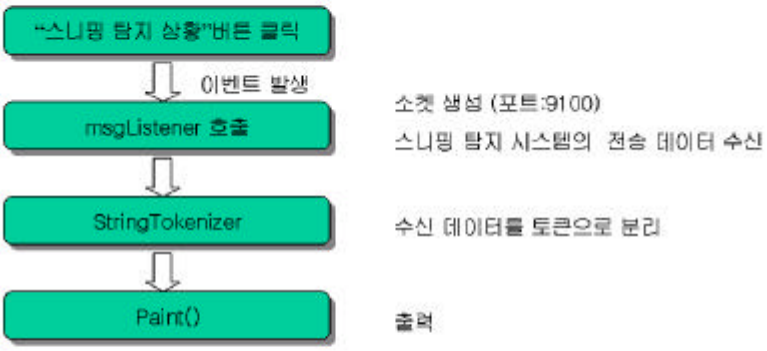
[그림3-13]은 스니핑 탐지 시스템의 주요 모듈이다. main함수에서는 libpcap라이브러리를 이용하여 자신의 이더넷 장치를 promiscuous mode설정한 후 외부로부터 수신되는 패킷을 캡쳐할 준비를 한다. send_icmp은 libnet라이브러리를 이용하

여 거짓 패킷을 생성하는 부분으로 이 함수에서 임의의 sequence number를 ICMP패킷에 삽입하여 스니핑이 의심되는 host로 전송한다. print_pkt함수는 침입 host로부터 전송된 ICMP reply패킷을 분석하여 수신된 패킷이 침입 host로부터 전송된 패킷이 침입 host에서 수신된 패킷인지 여부를 확인하여 맞다면 ICMP reply를 통해 송된다.[10]



3.2.2. 내부 침입(Sniffing) 관리자 모듈

스니핑 관리자 시스템은 탐지 시스템으로부터 전송된 내부 침입자의 정보를 웹 정에



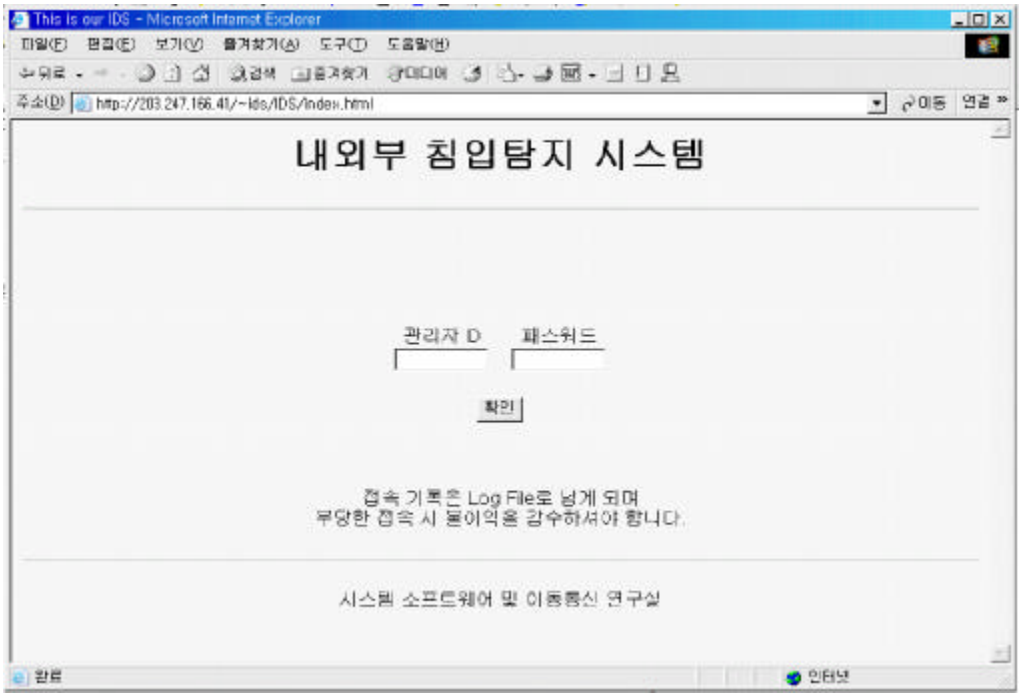
탐지 시스템에서 전송된 침입자에 대한 침입정보가 관리자 시스템으로 전송되면 관리자 시스템에 msgListener 이벤트를 발생시킨다. 이 함수에서 UDP소켓을 열어 탐지 시스템으로부터의 스니퍼에 대한 정보를 수신하고 StringTokenizer함수로 수신 데이터의 토큰을 분리하여 브라우저 상에 스니퍼의 IP, 침입날짜, 침입시간 등을 출력한다.

3.3. 제안한 내·외부 침입탐지시스템

본 논문에서 제안한 내·외부 침입탐지 시스템은 침입 상황을 웹기반으로 브라우저 상에서 탐지한다. 그리고 내·외부 각각에 대하여 침입 상황을 판단할 수 있도록 내부와 외부의 침입을 분리하여 탐지하도록 설계하였다.

3.3.1. 로그인

로그인(login) 처리는 웹상으로 접근하는 관리자를 인증하기 위해 사용된다.

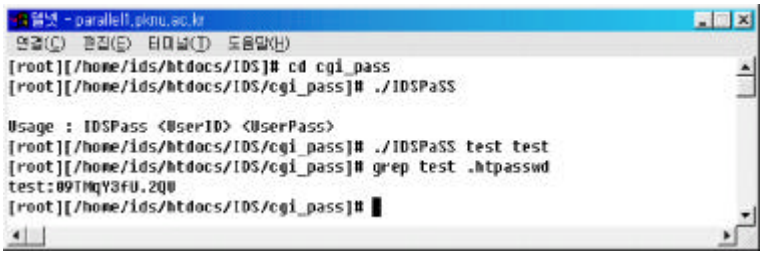


[그림 3-15] 로그인(login) 화면

위 화면은 로그인을 위한 첫 화면이다([그림 3-15]참조).

로그인을 하기 전에 관리자의 ID와 패스워드를 만들어야 한다. 이러한 작업은 자체 계정 생성 프로그램인 IDSPaSS를 사용한다.

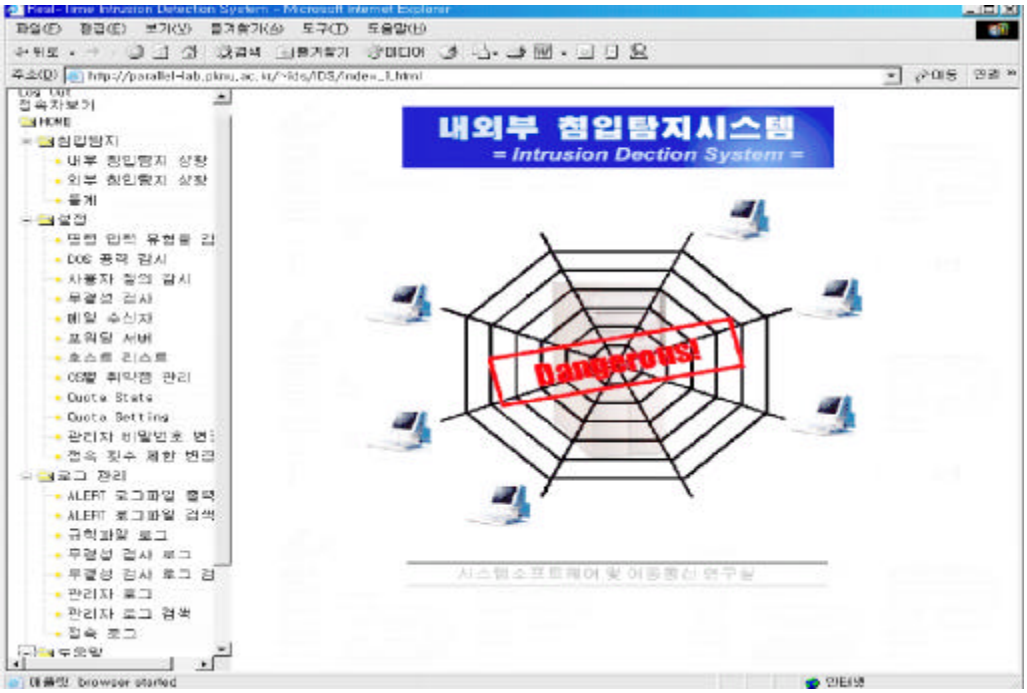
다음은 관리자의 ID와 패스워드를 만들기 위해서 IDSPaSS 명령어를 사용하여 test라는 계정을 만드는 과정을 나타내고 있다([그림 3-16]참조).



[그림 3-16] 관리자 ID와 패스워드 생성 화면

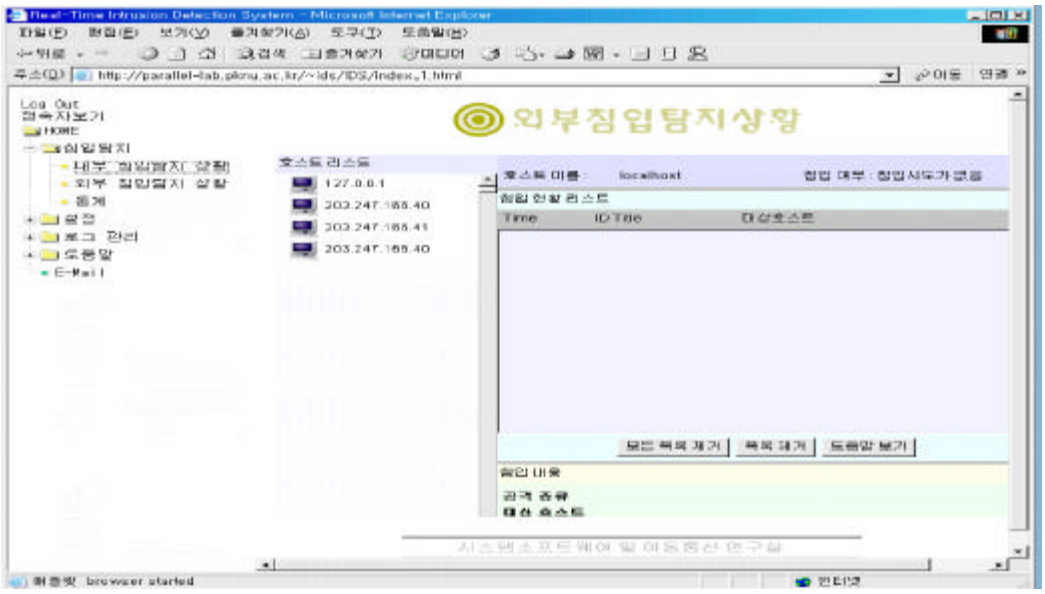
생성된 ID와 패스워드는 .htpasswd라는 파일에 저장된다.

그리고 다음의 [그림 3-17]은 로그인을 성공한 경우의 내·외부 침입탐지 시스템의 시작 화면을 나타낸다.

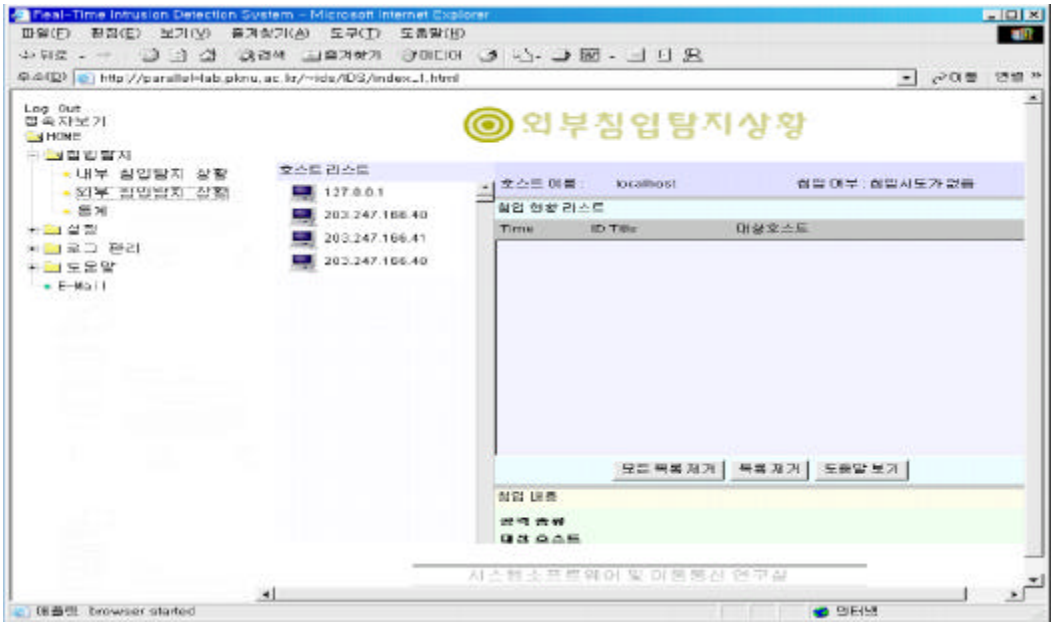


[그림 3-17] 로그인(login) 성공 화면

[그림 18, 19]는 내·외부 침입탐지 시스템 각각의 메인 화면이다.



[그림 3- 18] **내부(Sniffing)탐지 시스템 메인 화면**

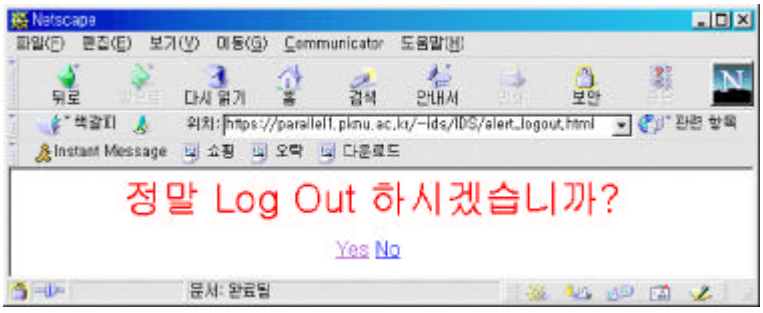


[그림 3- 19] **외부 침입탐지 시스템 메인 화면**

3.3.2. 로그아웃

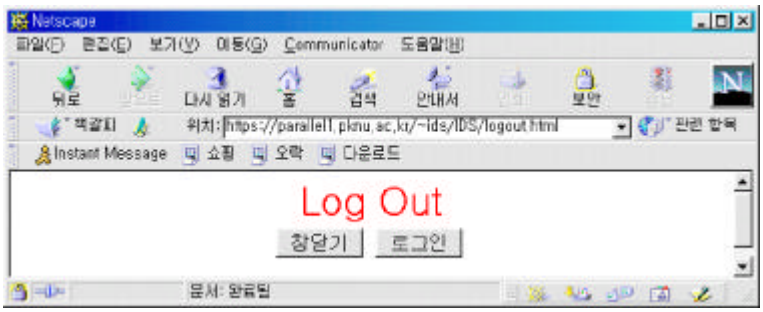
관리자가 내·외부 침입탐지 시스템을 통한 관리작업을 종료할 때 필요한 작업이다. 로그아웃(logout)은 로그인을 통해 생성된 접속자 ID와 접속 호스트 주소를 삭제하는 역할을 하게 된다.

[그림 3-17]에서 좌측 상단의 'Log Out' 메뉴를 선택하게 되면 다음의 로그아웃 확인 페이지로 이동하게 된다([그림 3-20]참조).



[그림 3-20] 로그아웃(logout) 화면1

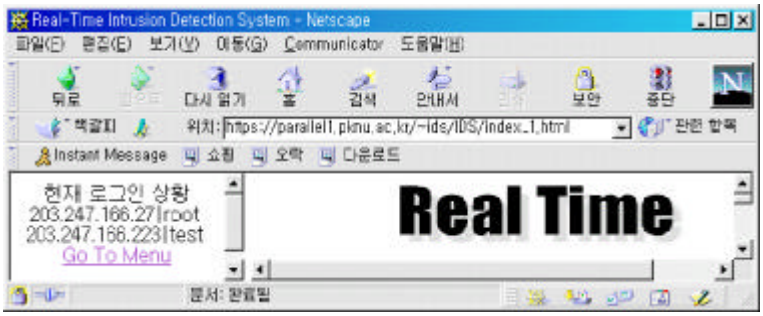
'No'를 선택하게 되면 이전 화면으로 돌아가게 된다. 만약 'Yes'를 선택하게 되면 로그인에 의해 생성된 정보를 삭제하고 다음의 화면으로 이동하면서 로그아웃이 된다([그림 3-21]참조).



[그림 3-21] 로그아웃(logout) 화면2

3.3.3. 접속자 보기

로그인을 정상적으로 하게 되면([그림 3-17] 참조) 좌측 상단의 '접속자 보기' 메뉴를 통해 현재 접속 중인 관리자 목록을 확인할 수 있다.



[그림 3-22] 접속자 보기 화면

현재 'root'와 'test'라는 관리자가 각각 IP 203.247.166.27와 203.247.166.223에서 침입탐지 시스템으로 로그인을 한 상태이다([그림 3-22]참조).

3.3.4 침입탐지

가. 내·외부 침입탐지 상황

침입탐지 시스템인 서버에서 내부 혹은 외부의 침입을 탐지하였을 경우 관리자 화면인 클라이언트로 탐지 사실을 보고(alert)한다([그림 3-23]참조).

[그림 3-23] 침입탐지 상황 화면

침입탐지 상황은 내부와 외부 각각에 대해 확인할 수 있으며, 침입탐지 상황 화면은 크게 '호스트 리스트', '침입현황 리스트', 그리고 '침입내용'으로 구성된다.

'호스트 리스트'는 로컬 호스트를 포함하여 침입을 탐지할 호스트 목록을 나타낸다. 이 부분에 호스트를 등록하기 위해서는 [그림 3-17]에서 '설정' 메뉴의 '호스트 리스트' 메뉴를 이용하여 설정할 수 있다.

'침입현황 리스트'는 침입현황을 리스트로 보여준다. 그리고 '모든 목록 제거' 또는 '목록 제거' 버튼을 이용하여 침입현황 리스트의 내용을 삭제할 수 있다. 그리고 침입현황 리스트에서 한 항목을 선택한 후, '도움말 보기' 버튼을 클릭하면 선택한 침입에 대한 상세 설명을 볼 수 있다.

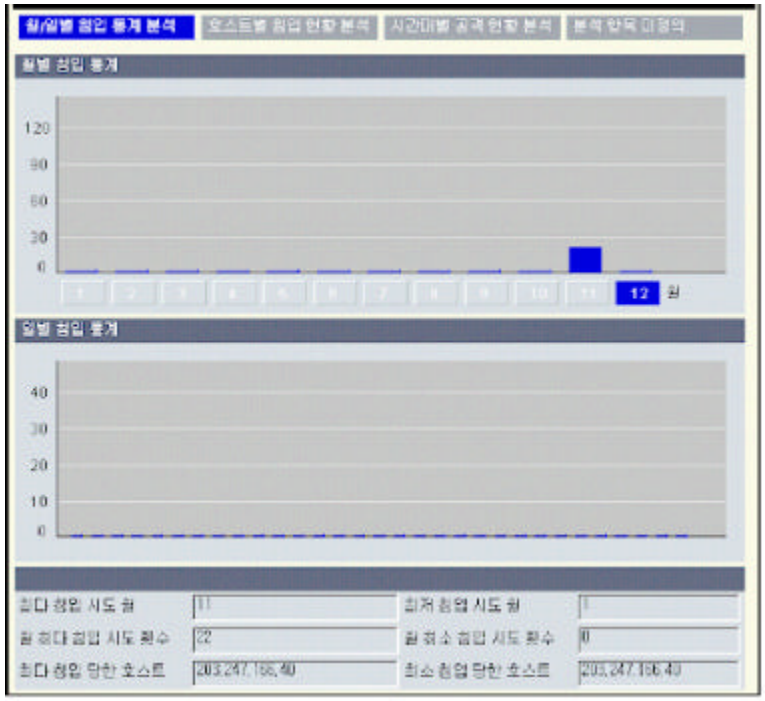
'침입내용'은 '침입현황 리스트' 항목의 구체적인 내용을 출력하는 부분이다.

공격종류는 공격 사이트가 취한 공격의 형태를 나타낸다. 대상호스트는 공격을 당한 호스트이며 공격사이트는 공격을 가한 호스트이다. 대상호스트 포트, 공격사이트 포트는 각각 공격을 당한, 공격을 가한 호스트의 포트를 나타낸다. 공격

날짜와 공격 시간은 공격이 발견된 시간과 날짜이며 위험수준은 1,2,3,4 단계로 나누어지며 다중공격인 경우, 진행정도를 빨간 네모 박스로 나타낸다. 경고 메시지는 대응조치나 상태, 기타 내용을 담고 있다.

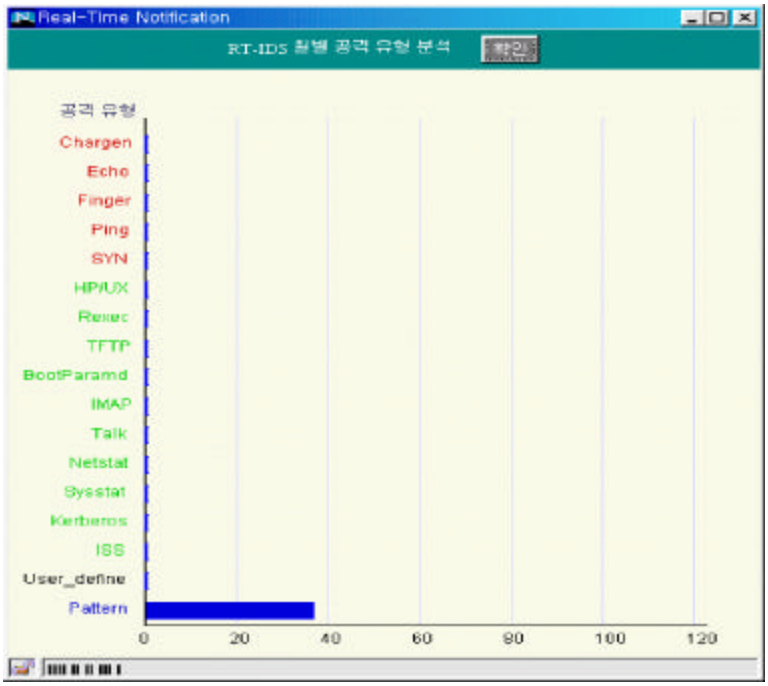
나. 통계

침입한 사건에 대한 통계데이터를 그래픽적으로 출력한다.



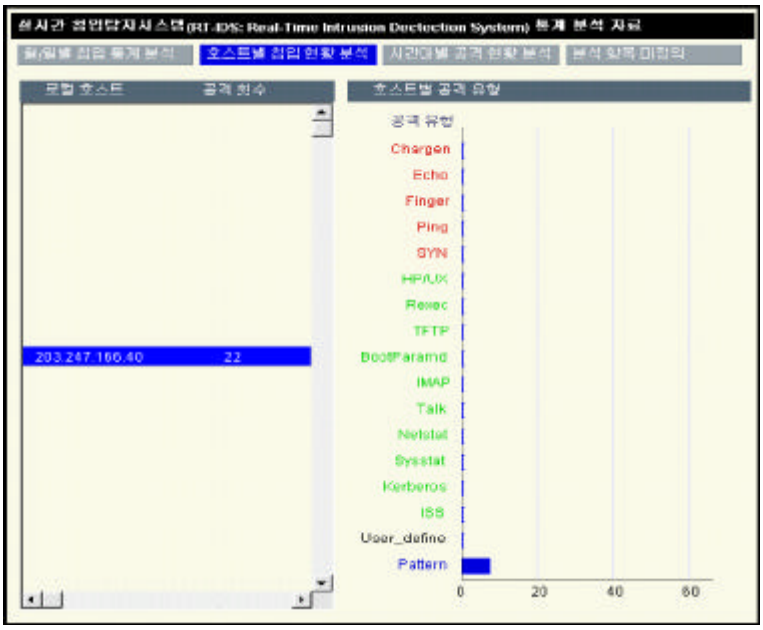
[그림 3-24] 월/일별 침입 통계 화면

기본적으로 월별과 일별 침입상황을 출력한다([그림 3-24]참조). 일별은 각 날짜별 침입 횟수를 나타낸다. 월별은 일별의 합으로 나타난다. 하단 부분은 침입한 결과 로그를 토대로 몇 가지 정보를 추출한 것이다. 다음은 위 화면에서 출력 가능한 화면들이다. 다음은 월별 침입 통계에서 각 월에 해당하는 버튼을 클릭한 경우 나타나는 분석 결과 화면이다. 공격 유형별로 보다 자세한 결과를 출력한다([그림 3-25]참조). 확인버튼을 클릭함으로써 창을 닫을 수 있다.



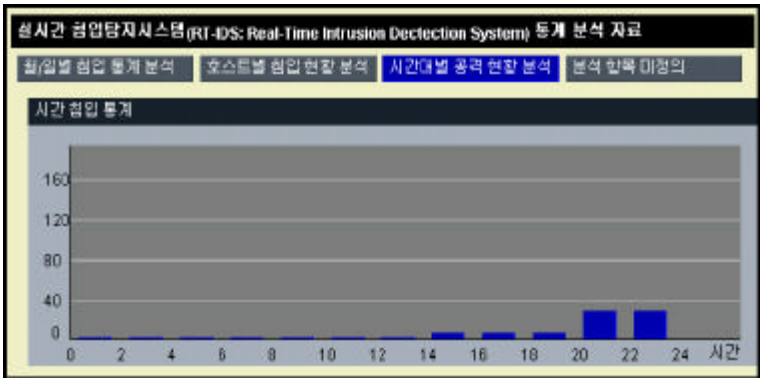
[그림 3-25] 침입 유형별 통계 화면

다음은 통계 출력화면의 상단에 있는 호스트별 침입상황 분석을 클릭한 경우 나타나는 화면이다([그림 3-26]참조).



[그림 3-26] **침입 호스트별 통계 화면**

아래 화면은 침입 로그 정보를 침입이 발생한 시간대별로 분석한 통계화면이다 ([그림 3-27]참조).

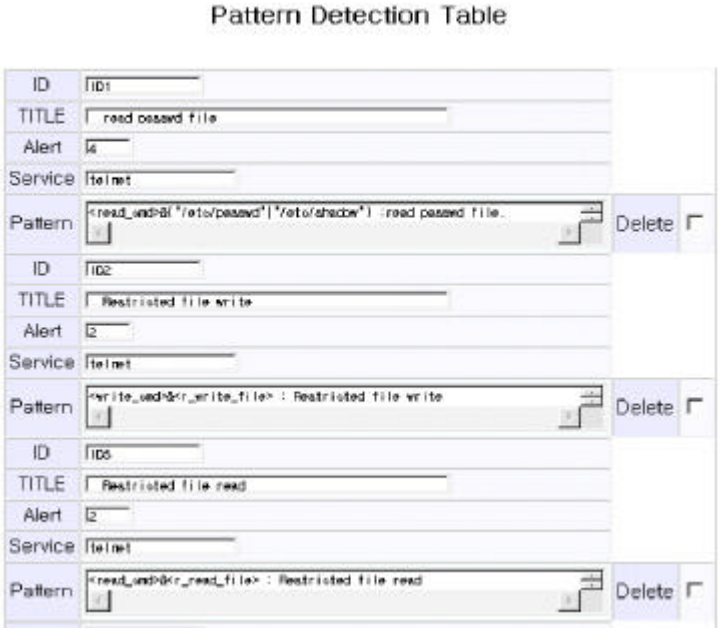


[그림 3-27] **침입 시간대별 통계 화면**

3.3.5. 설정

가. 명령입력 유형을 감시

다음은 명령 입력 유형을 감시하기 위한 명령어에 대한 침입 규칙(Command Rule)**을 추가, 삭제, 수정하기 위한 화면이다**([**그림** 3-28]**참조**).



[**그림** 3-28] **명령 입력 유형 감시 규칙 관리 화면**

ID**는 공격 유형을 구분하기 위하여 설정한다.** TITLE**은 공격 유형을 말로 설명한 것이다.** Alert**은 공격 유형의 위험도를 나타낸다.** Service**는 호스트가 제공하는 서비스 중 공격에 이용된 서비스를 입력한다.** Pattern**은 공격을 탐지할 수 있는 규칙으로 단순 명령어를 지정할 수도 있고, 다중 명령어를 지정할 수도 있다. 다음은 다중 명령어를 적용한 예시이다.**

```
<read> & /bin/sh & /mail/root
chmod & 4755 & /mail/root
touch
mail & root & <
/mail/root
```

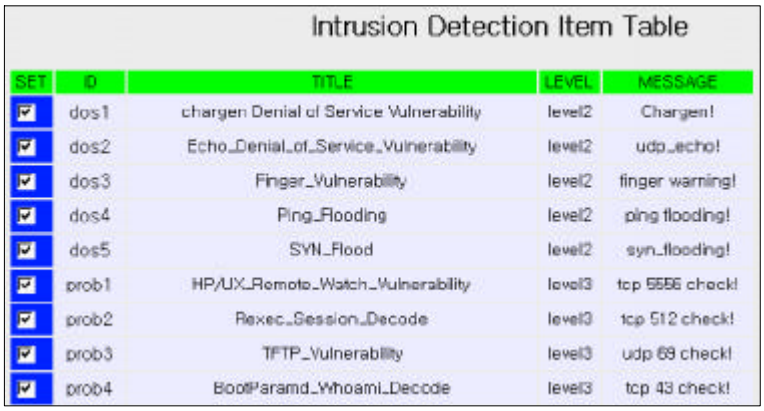
"<", ">" **사이에 입력되는 문자열은 침입탐지와 관련하여 특징을 갖는 명령들 혹은 인자들의 집합을 표시한다. 이러한 문자열은** symdb **디렉토리의 문자열**.key

파일로 정의되어 있다. “&”는 AND 연산을 뜻하고 “|”는 OR 연산을 뜻한다. 위 예시의 첫번째 라인의 경우 <read> 집합체에 속한 어떤 명령어나 인자, /bin/sh, /mail/root를 모두 포함할 경우 침입 탐지하게 된다.

하단에 저장, 취소, 추가 버튼을 이용하여 설정할 수 있다. 규칙을 삭제할 경우, 우측의 Delete를 체크하여 저장함으로써 삭제할 수 있다.

나. DOS 공격 감시

다음 화면은 DOS 공격을 감시할 것인지를 결정하기 위한 화면이다([그림 3-29]참조).

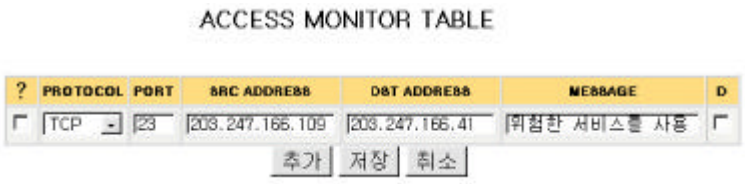


[그림 3-29] DOS 공격 유형 감시 관리 화면

'SET'의 체크 여부에 따라 해당 DOS 공격의 침입 여부를 Alert하게 된다. 'SET'을 체크하지 않게 되면, 침입 여부는 로그로 남기나 모니터링 호스트에 Alert을 하지 않는다. 좌측의 SET 필드를 설정한 후, 하단의 save 버튼을 클릭하여 설정을 변경할 수 있다.

다. 사용자 정의 감시

사용자 정의 감시는 관리자가 차단할 호스트, 프로토콜, 포트, 그리고 이러한 설정에 해당하는 침입을 발견했을 경우 Alert 전송할 때 필요로 하는 메시지를 설정할 수 있다([그림 3-30]참조). 관리자가 직접 특정 호스트에 대한 탐지를 설정할 때 유용하다.

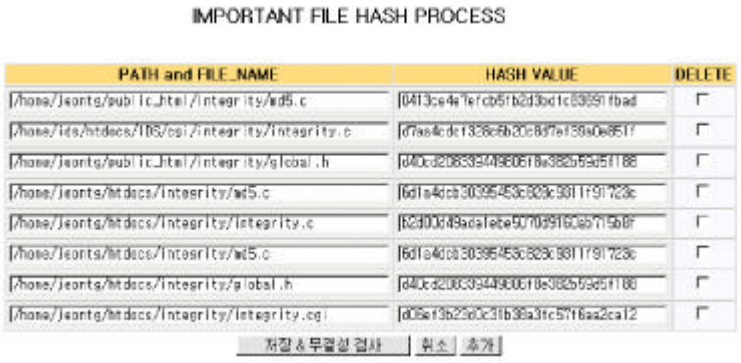


[그림 3-30] 사용자 정의 감시 관리 화면

"?"는 '사용자 정의 감시'의 SET 필드와 같은 역할을 한다. 즉, 탐지시 Alert 메시지를 전송할 것인지 아닌지를 결정할 때 이용한다. "PROTOCOL"은 TCP, UDP, ICMP를 제공한다. 그리고 탐지할 Source, Destination, Port를 설정할 수 있으며, 이러한 설정에 해당하는 침입을 발견했을 경우 Alert을 전송할 때 필요로 하는 메시지를 설정할 수 있다. 마지막 필드 "D"를 체크하여 저장함으로써 설정한 규칙을 삭제할 수 있다. 새로운 규칙을 생성하기 위해서는 추가 버튼을 클릭하여 설정한다.

라. 무결성 검사

다음은 무결성 검사 대상이 되는 파일과 그 해쉬 값이다. 무결성 검사를 하기 위한 새로운 파일을 추가할 수 있고 더 이상 무결성 검사로서의 중요도가 낮은 파일을 무결성 검사에서 삭제할 수 있다. 그리고 "저장 & 무결성 검사" 버튼을 이용하여 각 파일의 무결성을 검사할 수 있다([그림 3-31]참조).



[그림 3-31] 무결성 검사 관리 화면

마. 메일 수신자

메일을 수신할 메일 수신자의 E-mail 주소를 관리하는 화면이다([그림 3-32]참조).

[그림 3-32] 메일 수신자 관리 화면

사. 포워딩 서버

메일 전송시 포워딩을 지원해 줄 서버를 설정하는 화면이다([그림 3-33]참조). 메일을 포워딩 할 수 있는 서버 주소를 입력한다.

[그림 3-33] 메일 포워딩 서버 관리 화면

아. 호스트 리스트

침입을 탐지할 시스템을 설정할 수 있는 화면이다([그림 3-34]참조).

[그림 3-34] 호스트 리스트 설정 화면

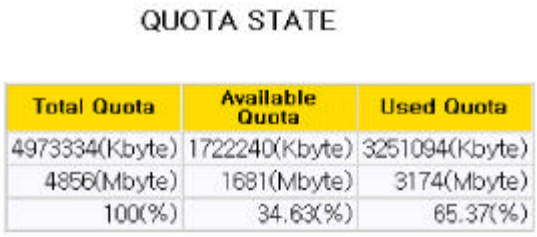
자. OS별 취약성 관리

운영체제(Operation System)**별 취약성을 관리할 수 있는 화면이다**([그림 3-35] **참조**).

[그림 3-35] OS별 취약성 관리 화면

차. Quota State

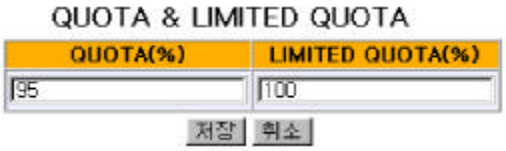
다음은 파티션에 대한 Quota **상태를 출력하는 화면이다**([그림 3-36]**참조**).



[그림 3-36] Quota 상태 화면

카. Quota Setting

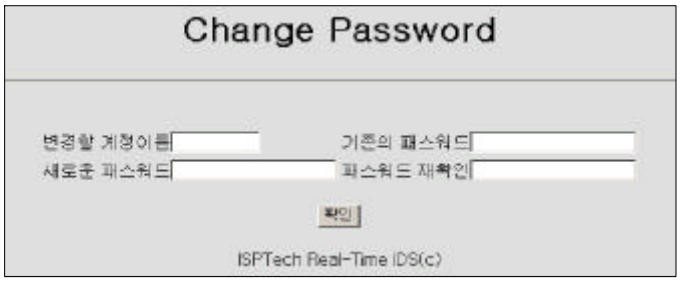
다음은 Quota를 설정하는 화면이다([그림 3-37]참조).



[그림 3-37] Quota 관리 화면

타. 관리자 비밀번호 변경

원격으로 로그인하는 관리자의 비밀 번호를 변경하는 화면이다([그림 3-38]참조).



[그림 3-38] 패스워드 변경 화면

3.3.6 로그관리

가. Alert 로그파일

침입탐지시 기록되는 정보인 Alert 로그 정보(alert.log)를 관리할 수 있다([그림

3-39]참조).

[그림 3-39] Alert 로그파일 관리 화면

나. Alert 로그파일 검색

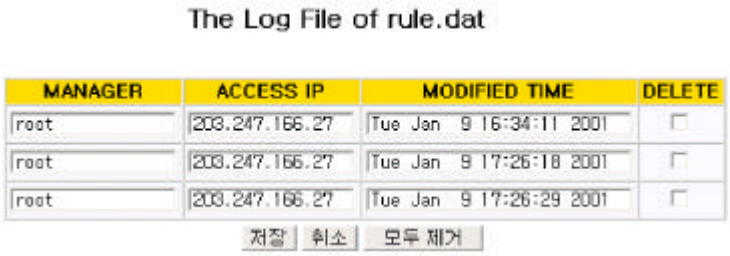
Alert 로그 파일 검색은 레벨별로 침입 로그 정보를 검색하도록 되어 있다. 각 레벨 버튼을 클릭함으로써 각 레벨별 침입 로그를 확인할 수 있다([그림 3-40]참조).

[그림 3-40] Alert 로그파일 검색 화면

위 화면은 레벨 3을 선택하여 레벨 3에 해당하는 Alert 메시지를 검색한 출력 결과이다.

다. 규칙 파일 로그

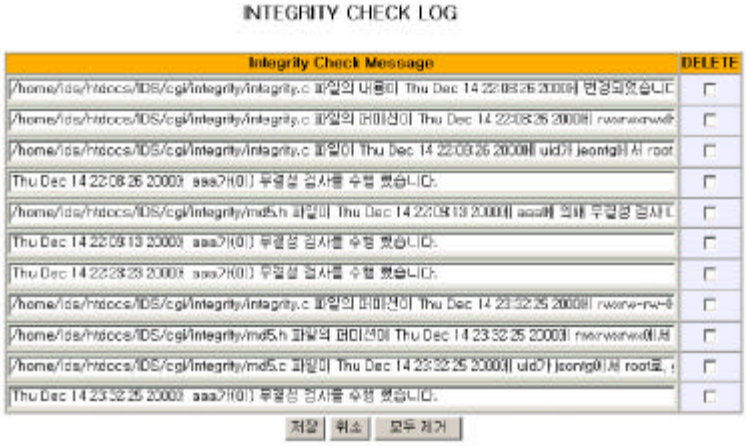
규칙 파일 로그는 규칙 파일(rule.dat)에 관한 접근 로그를 나타내고 있다([그림 3-41]참조). "MANAGER"는 규칙 파일에 접근한 관리자의 ID이다. "ACCESS IP"는 접속한 호스트의 주소를 나타내며, "MODIFIED TIME"는 접속 시간을 나타낸다. "DELETE" 필드를 체크함으로써 삭제가 가능하다.



[그림 3-41] 규칙 파일 로그 관리 화면

라. 무결성 검사 로그

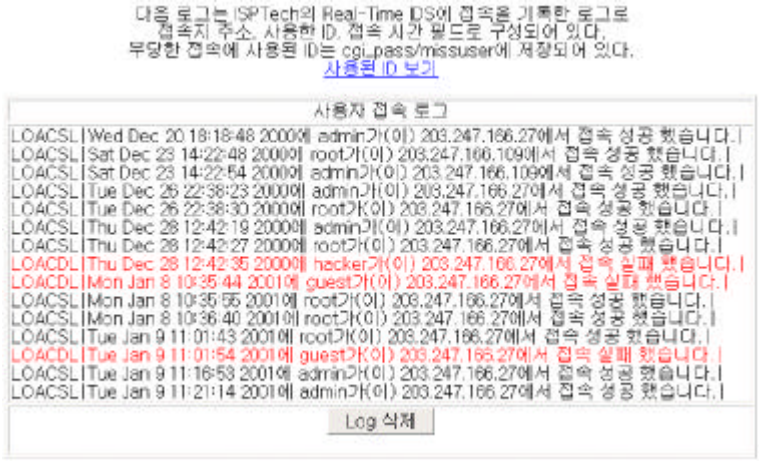
무결성 검사 로그 화면은 파일에 대한 무결성 검사와 무결성 검사 사실에 대한 로그화면이다([그림 3-42]참조).



[그림 3-42] 무결성 로그 관리 화면

마. 접속 로그

접속 로그는 접속에 관련된 로그를 출력하는 화면이다([그림 3-43]참조). “사용된 ID 보기”는 부당한 접속을 시도한 경우 cgi/missuser 디렉토리에 남은 해당 ID를 화면에 출력하게 된다. “SUCCESS LOG"는 접속에 성공한 경우, ”FAULT LOG"는 접속에 실패한 경우 로그에 기록이 남게 된다. 하단의 “Success Log 삭제” 및 “Fault Log 삭제” 버튼을 클릭함으로써 해당 로그 파일의 내용을 삭제할 수 있다.



[그림 3-43] 접속 로그 관리 화면

Ⅳ. 결 론

기존의 대부분의 침입탐지 시스템들에서 적용되고 있는 침입탐지 알고리즘과 침입탐지 기능의 특징들은 시스템내의 여러가지 자원으로부터 침입 시도에 대한 탐지 및 침입 후 변화된 자원들의 상태로부터 침입에 대한 사실을 알 수 있었다.

하지만 기존 네트워크 기반의 침입탐지 시스템들은 외부침입에 대한 탐지는 가능하지만 침입탐지 시스템을 통과하거나 내부에 존재하는 침입위협을 탐지할 수 있는 기능을 활발히 제공하지 못하고 있다.

따라서 본 논문에서 설계한 내·외부 침입탐지 시스템은 다양한 침입 방법들에 의해서 생성되는 패킷 유형과 침입 징후들을 분석하고, 침입 패턴에 대한 정형화된 모델을 사용하여 결과를 상태별로 정리함으로써, 외부 침입에 대처할 수 있는 시스템을 설계하였으며, 내부의 의심가는 호스트에 대한 탐지 기능을 제공함으로써 내부 침입탐지 기능도 제공하였다.

침입탐지 시스템의 설계는 패킷 헤더의 정보를 중심으로 한 엔진과 추출된 각각의 패킷 contents들을 조합하고 시스템 혹은 관리자가 정의한 침입탐지 패턴 규칙을 적용하는 엔진으로 분리하였다. 이는 침입 판정의 특징에 따라 침입탐지 과정에서 발생할 수 있는 시스템 부하의 분산과 판정 결과의 실시간적인 특성을 부여한다.

또한 판정 규칙 설정에 있어 관리자가 침입탐지 항목에 대한 기능 설정(on 또는 off)만으로 시스템을 관리하는 제한적인 시스템 운영과는 달리 본 침입탐지 시스템에서는 관리자에게 일부 침입탐지 유형에 있어 탐지 항목을 추가할 수 있는 기능성을 부여하였다. 물론 추가적인 탐지 규칙에 있어서도 관리자가 쉽게 이해하고 적용할 수 있도록 설계하였다.

그리고 침입탐지 시스템 뿐만 아니라 침입탐지 시스템이 설치된 시스템 자체의 데이터 보안을 위해 중요한 데이터에 대한 무결성 검사 기능을 cron에 등록하여 주기적으로 체크함으로써 중요한 데이터의 변경여부를 체크하는 기능을 제공하고 있다. 그리고 시스템 자체의 자원의 초과 사용으로 인한 침입탐지 시스템의 부적절한 동작 중단을 미연에 방지하기 위해서 partition quota를 주기적으로 검사하

여 일정 한계치 이상의 하드디스크를 사용할 경우 관리자에게 그 사실을 알려주도록 하였다.

본 논문에서 설계한 내·외부 침입탐지 시스템의 다양하고 강력한 기능들을 활용하여 외부의 침입탐지에 적절히 대응할 수 있으며, 내부의 의심가는 침입에 대한 탐지를 가능케 한다. 또한 침입차단 시스템과의 연결 기능을 개발하여 침입탐지와 침입차단을 동시에 가능케 함으로써 로컬 네트워크에서의 보안 기능이 한층 더 강화될 수 있을 것이다.

참고 문헌

[1] 김상정, 이현우, 신훈, 정윤종, 박정현, 임휘성, 임채호, *정보시스템 해킹방지 기술 현황 및 시스템 설계*, 한국통신정보보호학회 종합학술발표회 논문집 Vol.6 No.1, 1997.6

[2] 변경근, 심영철, 신훈, 임휘성, 임채호, *전산망보안점검 도구의 설계 및 구현*, 한국통신정보보호학회 종합학술발표회 논문집 Vol.6 No.1, 1997.6

[3] 이경하, 은유진, 김기현, 임채호, 정태명, *네트워크 패킷을 기반으로 한 실시간 침입탐지 시스템*, 한국통신정보보호학술대회, 1997.11

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

[5] 한국전산원, *유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구* NCA VI-RER-95105, 1995.12

[6] 한국정보보호센터, *침입탐지 모델 분석 및 설계*, Sep, 1996

[7] 한국정보보호센터, *대규모 전산망에서의 침입탐지를 위한 기본 시스템 개발에 대한 연구*, 1997

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

[9] Crosbie, M.; Dole, B.; Ellis, T.; Krsul, I.; Spafford, E.: *IDIOT - Users Guide*, Technical Report TR-96-050, Purdue University, COAST Laboratory, Sept. 1996

[10] D.B. Chapman, *Network (In)Security Through IP Packet Filtering*, Sep,1992

[11] D.Russel & G.T.Gargemi Sr, *Computer Security Basics*, O'Reilly, 1992

[12] D. E. Denning, *"An Intrusion-Detection Model"*, IEEE Transaction on Software Engineering, Vol. SE-13, No.2, Feb 1987 222-232

[13] Habra, N.; Le Charlier, B.; Mounji, A.; Mathieu, I.: *ASAX: Software architecture and rule-based language for universal audit trail analysis*, Deswarte, Y.; Eizenberg, G. (eds.): Proc. of the 2nd European Symposium on Research in Computer Security (ESORICS' 92), Toulouse, France, Nov. 1992, 435 - 450

[14] Hochberg, J.; Jackson, K.; Stallings, C.; McClary, J.; DuBois, D.; Ford, J.: *NADIR: An automated system for detecting network intrusions and misuse*, Computers and Security 12(1993)3, May, 253 - 248

[15] Illgun, K.; Kemmerer, R. A.; Porras, Ph. A.: *State transition analysis: A rule-based intrusion detection approach*, IEEE Transactions on Software Engineering March. 1995 181 - 199

[16] S.Garfinkel & G.Spafford, *Practical UNIX & Internet Security*, O'Reilly Associates, 1996

[17] S. M.Bellovin, *Packets Found on an Internet*, Aug, 23, 1993

[18] S.Kumar, *"Cassification and Detection of Intrusions."*, PhD thesis, Purdue University, West Lafayette, IN 47907, 1995

[19] Safford, Schales, Gess *The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment*, USENIX, 1993

[20] Sandeep Kumar and Eugene Spafford. *An Application of Pattern Matching in Intrusion Detection*. Technical Report 94-013, Purdue University, Department of Computer Science, March 1994

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

[22] W. R. Stevens., "TCP/IP Illustrated, volume Volume 1-The Protocols of Professional Computing Series.", Addison-Wesley, 1994

[23] http://download.iss.net/manual/rs25.tar.Z

[24] http://download.iss.net/manual/attack25.tar.Z

[25] http://www.inzen.com

[26] http://www.penta.co.kr

[27] http://rtlab.skku.ac.kr/~protect/

감사의 글

본 논문이 나오기까지 여러 방면에서 많은 도움을 주신 모든 분들에게 고마운 감사의 마음을 전하고자 합니다.

먼저 열심히 생활할 수 있도록 용기를 주시고, 학문적인 것 뿐만 아니라 인생의 가르침을 함께 베풀어주신 김창수 교수님께 진심으로 깊은 감사를 드립니다. 또한 바쁘신 와중에도 부족한 논문의 심사를 위해 격려와 지도를 해주신 정신일 교수님, 여정모 교수님께 감사를 드립니다. 그리고 학업에 도움을 주신 박만곤 교수님, 박승섭 교수님, 박지환 교수님, 윤성대 교수님, 이경현 교수님, 김영봉 교수님, 박흥복 교수님, 정순호 교수님께 감사드립니다.

항상 따뜻하게 맞아주었던 시스템 소프트웨어 및 이동통신 연구실 선후배님께 감사의 마음을 전합니다. 특히 많은 도움을 주었던 황현숙님, 박미경님, 양동수님, 김기욱님께 감사를 드립니다. 그리고 강병식 교수님을 비롯하여 대학원 동기인 변옥남님, 장용호님, 정동호님, 현영숙님에게 고마운 마음을 전합니다.

본 과정을 무사히 마칠 수 있도록 곁에서 격려하며 지켜봐주신 (주)유엔아이 백숭기 사장님과 하태경 이사님께 또한 감사를 드립니다.

이 글을 보지 못하고 눈감으신 아버님과 항상 저에게 용기를 주기 위해 헌신하신 어머님께 사랑의 마음을 담아 감사를 드립니다. 또한 묵묵히 저를 지켜봐주신 장인어른, 장모님께 진심으로 감사드립니다. 남편의 역할을 다하지 못함에도 불구하고 변함없이 사랑과 지지를 보내준 아내 장미영과 아들 성욱에게 이 기쁜 마음을 전하고 싶습니다.

마지막으로 논문을 마무리하는데 물심양면으로 도와주신 남난숙님과 고정흡님 그리고 김태우님을 비롯한 푸른모임 여러분들에게 고마움을 전합니다.

박 철 동 씀