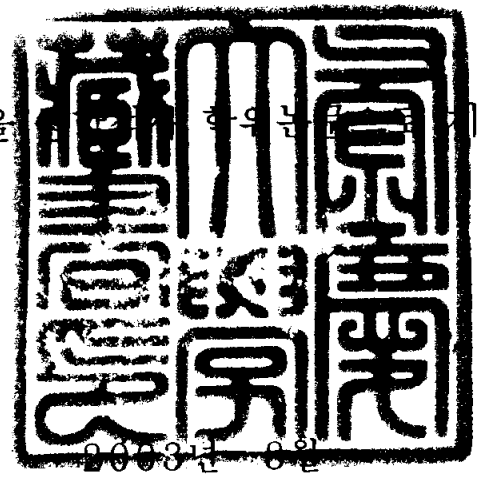
공학석사 학위논문

계층적 구조의 침입 탐지와 역추적 기술을 이용한 능동형 침입 대응모델 연구

지도교수 윤 종 락



이 논문을 [illegible] 학위논문으로 제출함

2003년 8월

부경대학교 산업대학원

정보통신공학과

이 윤 근

이 논문을 이윤근의 공학석사
학위논문으로 인준함

2003년 6월 21일

주 심 공학박사 장 주 석 

위 원 공학박사 김 석 태 

위 원 공학박사 윤 종 락 

< 차 례 >

< 표 차례 >

< 그림 차례 >

A Study on the Active Intrusion Response Model using Layered Intrusion Detection and Traceback Technique

Youn-geun Lee

Department of Telematics Engineering
Graduate School of Industry
Pukyong National University

Abstract

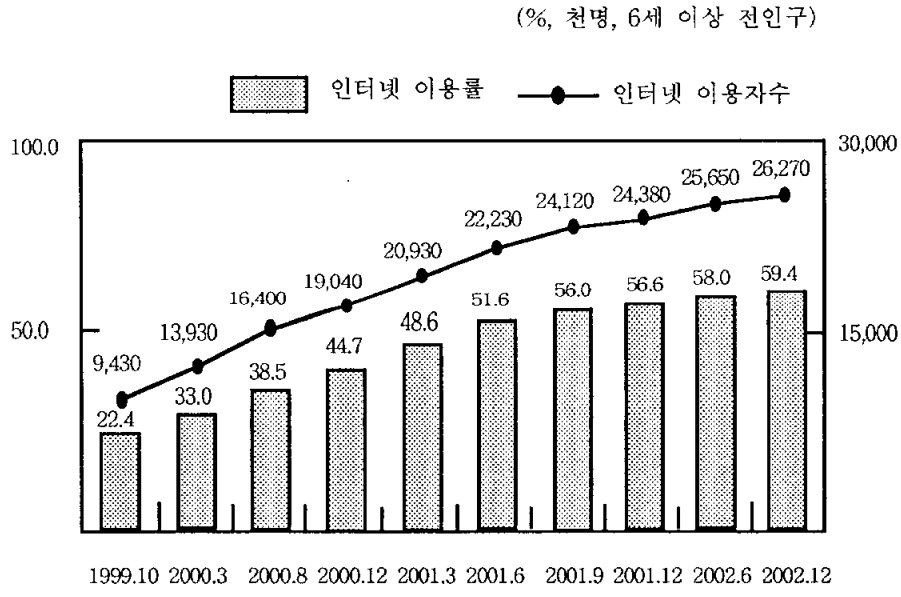
As information communication techniques have been rapidly developed and internet users have been sharply increased, attacks on the computer infrastructures are also becoming an increasingly serious problem. Previous IDSs(Intrusion Detection Systems) lack the ability to protect intrusion efficiently, since these systems just detect known attack patterns under a single network environment.

In this thesis, I proposed the active intrusion response model that is appropriate for a large scale network environment. This model consists of a layered intrusion detection system, a hacker decoy system, and a traceback system. The layered intrusion detection system detects intrusion regionally and globally. The hacker decoy system captures hacker's tool, motives, and attack patterns. The results of above two systems are transmitted the traceback system that can trace the attacker's origin in the internet.

Ⅰ. 서 론

오늘날 인터넷 기술의 발전은 전세계에 걸쳐 급격한 사회변화를 촉진시키고 있다. 컴퓨터와 인터넷이 만들어 낸 새로운 공간인 사이버 공간에서 기본적인 통신 서비스는 물론, 가상대학, 전자상거래, 멀티미디어 서비스 등과 같은 다양한 서비스 지원으로 인터넷 사용 인구의 폭발적인 증가와 인터넷 기반 사회의 조기 확대를 가져왔다.

우리나라도 전체가구의 78.5%가 PC를 보유하고 있고, 그 가운데 86.9%가 인터넷을 사용한다. 한국인터넷정보센타 통계에 따르면 2002년 12월 기준, 만 6세 이상 인구 중 '월평균 1회 이상' 인터넷을 이용하는 인구의 비율은 59.4%이며, 이용자수는 2,627만 명에 이르는 것으로 나타났다[그림 1].



[그림 1] 국내 인터넷 이용률 및 이용자 수

전세계적으로도 Network wizard사의 자료에 따르면 호스트 수는 2003년 1월 171,638,297개를 넘었다[22]. 그리고 Computer Industry Almanac사의 자료에 의하면 전세계 인터넷 이용자수는 2002년 12월 6억 6천 6백만명이 넘는 것으로 추정되고, 2005년에는 10억명에 이를 것으로 예상되고 있다[21].

이렇듯 인터넷은 사람들에게 자유로운 정보 교환과 경제적 이익, 나아가 일상생활의 유익성과 편리함을 제공함으로써 급속한 이용자 증가율을 가져왔으나, 컴퓨터 해킹, 바이러스 등 데이타와 네트워크에 대한 내·외부의 불법 도청, 변조, 파괴 등 각종 정보화 역기능으로 인한 위험도 또한 급속도로 높아져 가고 있다.

한 예로 2003년 1월 25일 국내에서 일어난 인터넷 대란 사고의 예를 들더라도 인터넷이 얼마나 쉽게 붕괴될 수 있는지를 보여준다. 최초 해외에서 유입된 376 바이트 패킷 크기의 작은 웜 바이러스 하나가 네트워크를 통해 단 10분만에 보안성이 취약한 수많은 시스템을 감염시켰다. 감염된 시스템으로부터 생성된 대량의 트래픽으로 인해 국내 관문국의 DNS(Domain Name Server)가 IP(Internet Protocol) 주소변환 과정을 처리하지 못함으로써 초유의 인터넷 마비사태를 불러온 것이다.

또한 세계 각국이 미래 전쟁에 있어서 물리적 군사력 뿐만 아니라 적국의 네트워크와 시스템을 마비시킬 수 있는 사이버공격 능력을 갖춘 정보전 부대를 창설, 강화하는데서 보더라도 일반 개인 사용자 뿐만 아니라 국방, 금융, 교통, 통신, 항공, 연구망, 기업 등 모든 사회 기반 시설이 연결된 인터넷 네트워크와 시스템에 대한 보호가 얼마나 중요한지를 알 수 있다.

그러나 1.25 인터넷 대란에서도 드러났듯이 갈수록 지능적이고 다양해지는 내·외부 사이버 공격에 대해서 기존의 침입 탐지 시스템만으로는 능동적인 대응이 어렵게 되었다. 왜냐하면 기존의 침입 탐지 시스템들이 단일 시스템 혹은 단일 환경 하에서의 침입 탐지 기능만을 제공하므로 보안의 대상이 제한될 뿐만 아니라 침입을 탐지하더라도 침입을 관리자에게 통보하여 관리자의 판단을 요구하므로 실시간적인 침입 탐지와 능동적인 대응이 어렵기 때문이다.

따라서 본 논문은 대규모 네트워크 환경 하에서 계층적 구조의 통합 침입 탐지와 침입자 역추적 기술을 유기적으로 연계한 능동형 침입 대응 모델을 제시함으로써 침입 패킷을 탐지, 차단하는 수동적 대응에 그치지 않고, 탐지와 동시에 침입자를 역추적하는 능동적인 대응을 하고자 한다.

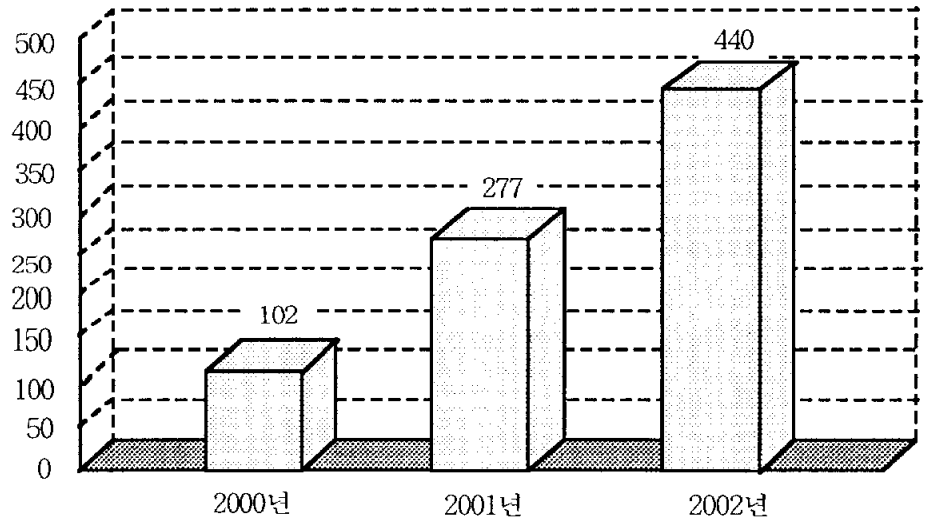
본 논문은 다음과 같이 구성된다. 먼저 2장에서는 1.25 인터넷 대란을 비롯한 최근 보안침해 사고를 분석하고, 3장에서는 기존 침입 탐지 시스템에 대해 분석하며, 4장에서는 계층적 구조의 통합 침입 탐지 모델과 역추적 기술의 종류와 장단점을 기술한다. 5장에서는 본 연구에서 제안하고자 하는 능동형 침입 대응 모델을 제시하고, 마지막 6장에서는 결론 및 향후 연구 과제에 대해서 기술한다.

Ⅱ. 최근 해킹사고 동향

2.1 최근 보안침해사고 분석

최근의 보안침해 사고를 보면 과거와 달리 바이러스와 해킹이 결합되는 등 갈수록 지능화, 대형화 되고 있는 추세이고, 이러한 경향은 앞으로도 훨씬 심화될 것으로 예상된다. 2003년 1월 25일 발생한 웜 바이러스의 경우를 보더라도 하나의 컴퓨터가 감염되면, 감염된 컴퓨터가 다시 다른 컴퓨터들을 공격하는 양상이 많이 나타나고 있다. 즉, 피해자와 가해자가 따로 있는 것이 아니라 피해자가 동시에 가해자가 되어 버리는 것이다.

2002년 12월 국가정보원에서 발표한 「2002년도 사이버테러대응실적」을 참고하면 2002년 국가 공공기관의 해킹사고 발생건수는 440건으로 정보화의 역기능으로 해마다 해킹 사고도 급증하는 것을 볼 수 있다[그림 2][2].



[그림 2] 연도별 국가 공공기관 해킹사고 발생현황

2002년도 기관별 해킹사고 발생현황을 살펴보면 [표 1]에서와 같이 대학이 304건으로 전체의 69.1%로 가장 큰 비중을 차지하고 그 다음으로 지자체, 산하기관, 행정기관 순으로 발생하여 상대적으로 보안이 취약한 교육기관에서 사고가 급증하고 있는 추세이다. 민간부문도 2003년 3월 한국정보보호진흥원에서 발표한 월별 해킹피해 통계자료를 살펴보면 [표 2]에서와 같이 최근 해킹과 웜 바이러스 공격이 갈수록 증가하고 공격수법도 다양해지고 있음을 볼 수 있다[1].

[표 1] 2002년도 기관별 해킹 사고 발생 현황

기관	중앙행정기관	지자체	산하기관	연구기관	대학	기타	총계
건수	21	72	25	11	304	7	440
비율(%)	4.8	16.4	5.7	2.5	69.1	1.6	100

(국가정보원 제공자료)

[표 2] 월별 해킹 피해 통계

구 분	2002년										2003년
	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	1월
해 킹	424	394	541	451	583	548	442	606	618	781	1120
웜바이러스	28	14	251	361	198	205	172	433	451	798	974
스팸릴레이	7	5	758	936	1132	627	529	462	591	486	469
합 계	459	413	1550	1748	1913	1380	1143	1501	1660	2065	2563

(한국정보보호진흥원 2003년 3월 자료)

이렇듯 인터넷은 개방성과 확장성이라는 본질때문에 위험에 항시 노출될 수 밖에 없고 해킹, 바이러스 등 사이버 공간의 위험 요소도 계속 증가하고 있는 실정이다. 따라서 정보화 사회의 안전성과 신뢰성을 확보하기 위해서는 네트워크 보호 체계의 구축과 정보 보호에 있어 여러가지의 보안 방법들에 대한 연구의 필요성이 대두되고 있다[15].

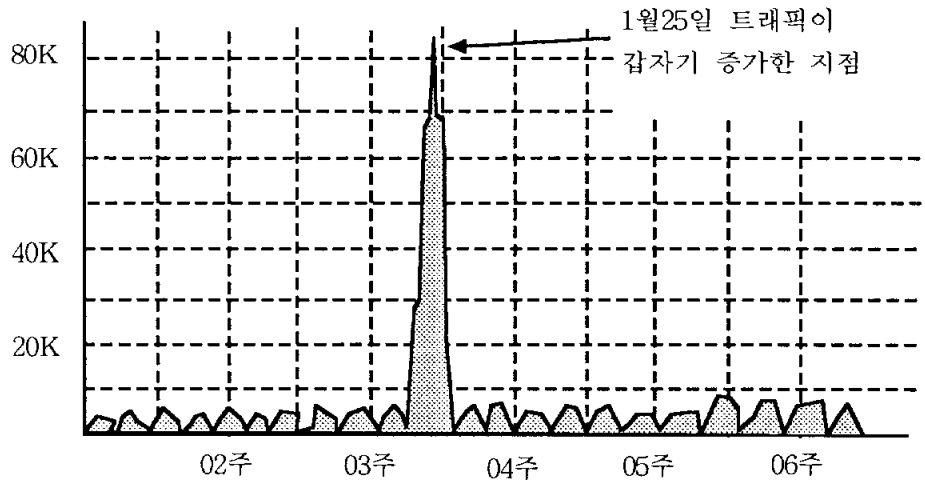
2.2 1.25 인터넷 대란

2003년 1월 25일 발생한 인터넷 대란은 정보화 못지않게 신뢰성 높은 정보 보호가 얼마나 중요한지 보여준 사건이었다. 사회의 모든 기반 산업이 연결된 인터넷 네트워크가 작은 웜 바이러스 패킷 하나로 10분만에 마비가 된 사건의 사고경위와 원인을 분석한다.

2.2.1 인터넷 대란의 사고 경위

2003년 1월 25일 14시 10분경부터 미국, 호주 등으로부터 유입된 것으로 추정되는 슬래머 웜 바이러스에 의해 인터넷 이용시 접속이 지연되고 일부 인터넷 사이트 접속이 불가능해지면서 시작된 인터넷 대란은 약 10분이 경과한 후 국내 주요 ISP(Internet Service Provider)의 DNS 서버와 IDC 내부망이 과부하로 인해 서비스 불능 상태에까지 빠졌다. 국내 모 IDC의 트래픽 현황을 살펴보면 1월 25일 갑자기 트래픽이 급증하여 다른 서버들의 네트워크 이용이 거의 불가능했다는 것을 알 수 있다[그림 3][4].

주요 ISP 업체들이 라우터에서 문제가 된 UDP(User Datagram Protocol) 1433, 1434 포트로의 패킷들을 차단하고 감염된 MS SQL(Microsoft Structured Query Language) 서버들이 재부팅과 보안패치를 적용함으로써 사태는 일단락 되었다.



[그림 3] 국내 모 IDC내 네트워크 트래픽량

2.2.2 인터넷 대란의 원인 분석

인터넷 대란은 슬래머(slammer) 웜 바이러스의 네트워크 공격에 의한 트래픽 급증으로 백본망과 하부 네트워크망의 붕괴에 의한 것이었다.

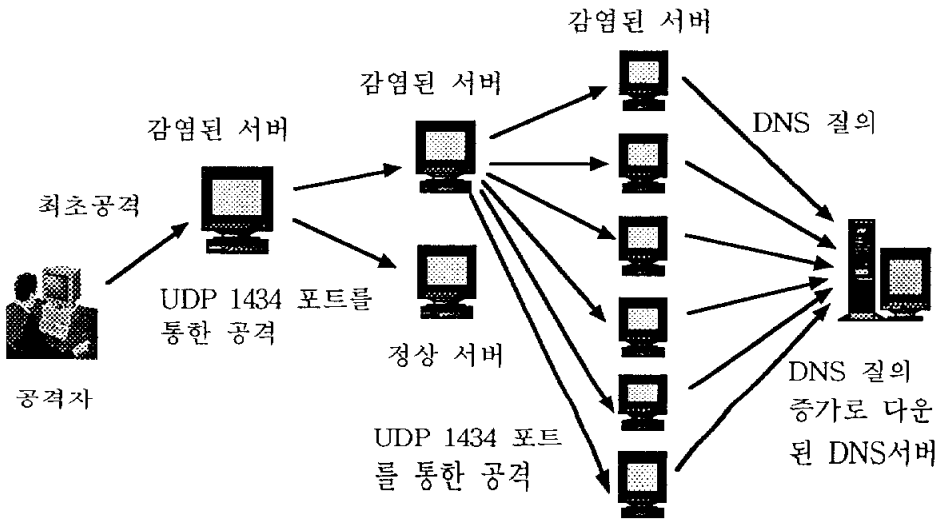
그 원인은 첫째, 슬래머 웜 바이러스에 의한 주요 DNS 서버의 과부하에 의한 것이었다. 슬래머 웜 바이러스는 376 바이트 크기의 메모리 상주형 웜으로 UDP 1434 포트를 통해 404 바이트 크기의 공격 패킷을 초당 최대 1만개에서 5만개를 생성한다. 이렇게 전송된 패킷들에 의해 취약성이 있는 MS SQL 서버가 감염되고, 다시 감염된 서버는 다른 서버들에게 대량의 패킷을 보냄으로써 일시에 트래픽이 폭주해 장애가 발생했던 것이다[그림 4].

둘째, 슬래머 웜은 다른 서버들을 감염시키기 위해 랜덤하게 선택된 IP 주소로 공격 패킷을 보내는데 그 중 93.2%가 해외로의 연결을 시도했기 때문에 국제 인터넷 교환기의 라우터에 심각한 병목 현상을 유발했고, 이로 인해

국내 DNS 서버의 과부하를 초래한 것이다.

1월 25일 발생한 인터넷 대란 사태로 국내에서만 8800여개의 시스템이 슬래머 웜에 감염되었다. 국내에서 뿐만 아니라 미국, 일본, 유럽, 중국, 대만 등 인터넷 인프라 구축이 발달된 세계 각국에서 피해를 입었다. 미국에서의 대표적인 피해 사례로 뱅크 오브 어메리카는 현금 인출기들이 사용 불능 상태에 빠졌고, 컨티넨탈 항공사는 전산 시스템의 지체로 수작업으로 고객 서비스를 시행했으며, 시애틀시 911은 응급 연락망이 다운되었다.

인터넷 대란 사태에서 보듯이 갈수록 지능화, 대형화되는 사이버 공격을 효율적으로 막기 위해서는 기존의 단위 시스템 위주의 침입 탐지 설계가 아닌 계층적 구조의 통합 침입 탐지와 역추적 기술을 유기적으로 연계한 능동형 침입 대응 모델이 필요한 것이다.



[그림 4] 슬래머 웜 바이러스의 전파경로

Ⅲ. 침입 탐지 시스템에 대한 분석

현재까지 보안 시스템은 크게 방화벽과 침입 탐지 시스템으로 나뉜다. 1세대 보안 솔루션으로 일컬어지는 방화벽은 외부와 내부의 경계를 두고 내·외부간에 오가는 트래픽을 감시해 허용되지 않은 접근을 차단함으로써 내부 정보자산을 외부의 불법 침입과 해킹으로부터 보호하는 시스템이라고 할 수 있다.

그러나 인증을 받은 사용자나, 인증받은 사용자로 가장한 침입자의 공격 또는 내부 네트워크 사용자에 의해 자행되는 네트워크 침입, 전자우편과 같은 정상적인 애플리케이션 속에 숨어 들어오는 악성 바이러스나 웜 공격에 대해 방화벽은 효율적으로 대처할 수 없다. 이러한 공격에 효과적으로 대처하기 위해 2세대 보안 솔루션으로 일컬어지는 침입 탐지 시스템이 등장하였다. 본 장에서는 기존에 개발된 침입 탐지 시스템의 분류 방법과 침입 탐지 기법 및 구조에 대해 분석한다.

3.1 침입 탐지 시스템의 분류

침입 탐지 시스템은 침입을 판단하는 자료의 출처에 따라 분류하는 데이터 소스(Data Source) 기반의 분류 방법과 탐지 방법을 중심으로 이루어진 침입 모델을 기반으로 분류하는 방법으로 크게 나눌수 있다[5,6,13,14]. 여기서 다시 각 분류 방법들은 구체적인 기준에 의해 특징별로 다음과 같이 세분화 된다.

① 데이터 소스를 기반으로 하는 분류 방법

o 단일 호스트 기반(Host Based)

단일 호스트로부터 생성되고 수집된 감사 데이터를 침입 여부 판정에 사용하며, 하나의 호스트를 탐지 영역으로 한다.

o 다중 호스트 기반(Multihost Based)

여러 호스트들로부터 생성되고 수집된 감사 데이터를 침입 여부 판정에 사용하며, 여러 대의 호스트를 그 탐지 영역으로 하기때문에 호스트간의 통신을 통해 침입 판정에 필요한 정보를 교환한다.

o 네트워크 기반(Network Based)

네트워크의 패킷 데이터를 수집하여 침입 여부 판정에 사용하며, 침입 탐지 시스템이 설치된 네트워크 전체 영역을 탐지 대상으로 한다.

데이터 소스를 기반으로 하는 침입 탐지 시스템의 장단점은 [표 3]과 같이 간략히 비교할 수 있다.

[표 3] 데이터 소스 기반 침입 탐지 시스템의 장단점

구분	호스트 기반	다중 호스트 기반	네트워크 기반
장점	· 내부자의 해킹 차단 · 비정상적인 침입 탐지 가능	· 내부자의 해킹 차단 · 비정상적인 침입 탐지 가능	· 네트워크 트래픽에 영향이 없음 · 모든 트래픽 정보를 기록 및 재생 가능
단점	· 서버마다 설치 필요 · 서버 자원을 사용함으로 부하가 커짐	· 서버마다 설치 필요 · 네트워크 트래픽이 커짐 · 실시간 대응이 곤란	· 실시간 패킷 분석, 침입 탐지에 한계 · 내부자의 해킹 차단이 어려움

② 침입 모델을 기반으로 하는 분류 방법

o 비정상적인 행위 탐지(Anomaly Detection)[12]

정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있다가 프로파일에서 벗어나는 행위들을 탐지하는 방법으로 정상적인 프로파일을 생성하기 위해 기존의 많은 데이터를 분석해야 하기 때문에 구현 비용이 많이 드는 단점이 있으며 그 종류는 다음과 같다.

- 통계적인 방법 (Statistical Approaches)
- 특징 추출 (Feature Selection)
- 비정상적인 행위 측정방법들(Anomaly Measures)의 결합
- 예측 가능한 패턴 생성 (Predictive Pattern Generation)
- 신경망을 이용한 방법 (The use of Neural Networks)

o 오용 침입 탐지(Misuse Detection)

사전에 공격에 대한 특징 정보를 가지고 있다가 시스템의 알려진 취약점들을 이용하여 공격하는 행위들을 탐지하는 방법으로 시스템 감사 정보에 대한 의존도가 높고 상대적으로 구현 비용이 저렴한 장점이 있으며 그 종류는 다음과 같다.

- 조건부 확률 (Conditional Probability)
- 전문가 시스템 (Expert System)
- 상태 전이 분석 (State Transiton Analysis)
- 키 입력 관찰 (Keystroke Monitoring)
- 모델에 근거한 침입 탐지 (Model-Based Intrusion Detection)

위와 같은 분류 기준을 가지고 기존 침입 탐지 시스템을 분류하여 보면 [표 4]와 같다[3].

[표 4] 침입 탐지 시스템의 기술적 분류

IDS	데이터 소스			침입 모델		특 성
	Host	Multi host	Network	비정상	오용	
RealSecure			○			
ASAX		○			○	규칙기반 언어
CMDS		○		○	○	규칙기반 전문가시스템
GASSATA					○	패턴 매칭
AID		○			○	실시간 전문가시스템
NID			○	○	○	
NADIR			○	○	○	규칙기반 전문가시스템
NetRanger			○		○	
OmniGuard	○				○	규칙기반
POLYCENTER	○				○	
Stalker		○			○	
IDES/NIDES		○		○	○	
STAT					○	상태전이도
Haystack	○			○	○	
MIDAS	○			○	○	전문가 시스템
W&S				○		규칙 기반
Argus			○			
Courtney			○			SATAN 탐지기
IDIOT					○	패턴 매칭
SAINT		○			○	데이터 분석 도구
UNICON Watcher			○	○	○	
Watcher	○					

3.1.1 비정상적인 행위 탐지 기법

(1) 통계적인 방법

과거의 경험적인 자료를 토대로 비정상적인 행위의 탐지를 주로 통계적으로 탐지하는 방법으로 정확성이 상당히 높으나 어떤 행위가 비정상인지를 판가름할 수 있는 임계치를 설정하기가 힘들고, 사용자가 추가되거나 제공하는 서비스가 제거되는 것들과 같이 측정 데이타 요인들이 바뀔 때마다 프로파일을 갱신해야 하는 등 지속적인 훈련이 필요한 단점이 있다.

(2) 특징 추출

특정 침입 패턴을 추출하는 방법으로, 경험적인 침입 탐지 측정도구의 집합을 설정하고, 침입의 예측, 분류 가능한 침입 탐지 도구의 부분집합을 결정하여 침입을 예측, 분류한다

(3) 비정상적인 행위 측정 방법들의 결합

여러 비정상적인 행위 측정 방법들을 사용하여 도출된 각각의 결과를 통합하여 특정 행위가 비정상적인지를 측정하는 방법이다

(4) 예측 가능한 패턴 생성

특정 행위를 이루는 이벤트의 순서와 상호관계를 설명하고, 시간 기반 규칙에 따라 각각의 이벤트에 시간을 부여하여 기존의 설정된 이벤트와 비교하여 침입을 탐지하는 방법이다.

(5) 신경망을 이용한 방법

명령어의 순서를 신경망으로 학습시켜서 다음에 수행될 명령어를 미리 예측하여 사용자가 실행한 명령어 순서와 비교해 침입을 탐지하는 방법으로 여러가지 감사 데이터가 섞여 있는 경우에도 잘 처리할 수 있는 장점이 있는

반면, 신경망의 토폴로지와 각각의 구성요소 사이에 주어지는 가중치를 여러 번 학습시킨 후에야 결정할 수 있는 단점이 있다.

(6) 데이터 마이닝(Data Mining) 방법

최근 활발히 연구되고 있는 분야로서 통계적인 방법에서 한 단계 발전한 형태로 방대한 양의 데이터 속에서 쉽게 드러나지 않는 유용한 정보를 찾아내는 정보 추출 방법인 데이터 마이닝 기법을 이용, 사용자가 시스템에 로그인하여 로그 아웃하는 동안 실행하는 일련의 명령어들의 연관관계를 가지고 비정상적인 침입을 판별하는 방법이다[10].

3.1.2 오용 침입 탐지 기법

(1) 조건부 확률

이벤트 패턴 중에서 특정 이벤트가 침입일 확률을 조건부 확률 공식을 통하여 계산하는 방법이다.

(2) 전문가 시스템

If-then 규칙에서 공격 패턴들에 대한 지식을 표현하고, 감사 추적 이벤트와 일치하는 사건들을 명시한다. 일치하는 공격 패턴을 발견할 경우 If-then 규칙에 따라 rule의 action을 수행하는 방법이다.

(3) 상태 전이 분석

공격 패턴을 특정 시스템의 상태 전이의 순서로 표현하는 방법으로 하나의 state에서 발생하는 이벤트에 따라 정해진 다음의 state로 이동시킨다.

(4) 키 입력 관찰

사용자의 키 입력을 감시하여 공격 패턴을 나타내는 특정 키 입력 순서를 패턴화하여 침입을 탐지하는 방법이다

(5) 모델에 근거한 방법

특정 모델을 만들어 관련된 공격 패턴들을 데이터베이스로 구축하고, 특정 공격 패턴이 발생하는 경우 데이터베이스를 참조하여 침입을 탐지하는 방법이다.

3.2 침입 탐지 시스템의 구조

호스트 기반이나 네트워크 기반 침입 탐지 시스템은 공통적으로 데이터 수집 및 축약 모듈, 분석 및 침입 탐지 모듈, 데이터 관리 인터페이스 모듈, 침입 탐지 대응 모듈 등 4가지의 모듈로 이루어 진다[그림 5][3].

(1) 데이터 수집 및 축약 모듈

데이터 수집 및 축약 모듈은 침입 탐지 시스템에서 가장 먼저 수행되는 모듈이다. 수집된 모든 감사 데이터를 이용하여 바로 침입 탐지 분석 작업을 수행하는 것은 데이터의 양이 너무 많기 때문에 실시간으로 수행하는 것은 불가능하다. 보통 수집된 감사 데이터의 90% 이상이 불필요한 정보이기 때문에 불필요한 데이터를 제거하고, 일련의 정해진 형태로 변환하는 축약 작업을 해야 한다

(2) 분석 및 침입 탐지 모듈

분석 및 침입 탐지 모듈은 침입 탐지 시스템의 핵심 구성 요소로서 데이터 수집 및 축약 모듈에서 생성한 축약 데이터를 분석하고, 저장된 침입 정보나 프로파일과 비교하여 침입 여부를 판정하는 역할을 한다.

분석 및 침입 탐지 모듈에서는 침입을 탐지하기 위해 비정상적인 행위 탐지 기법과 오용 침입 탐지 기법 등을 사용한다.

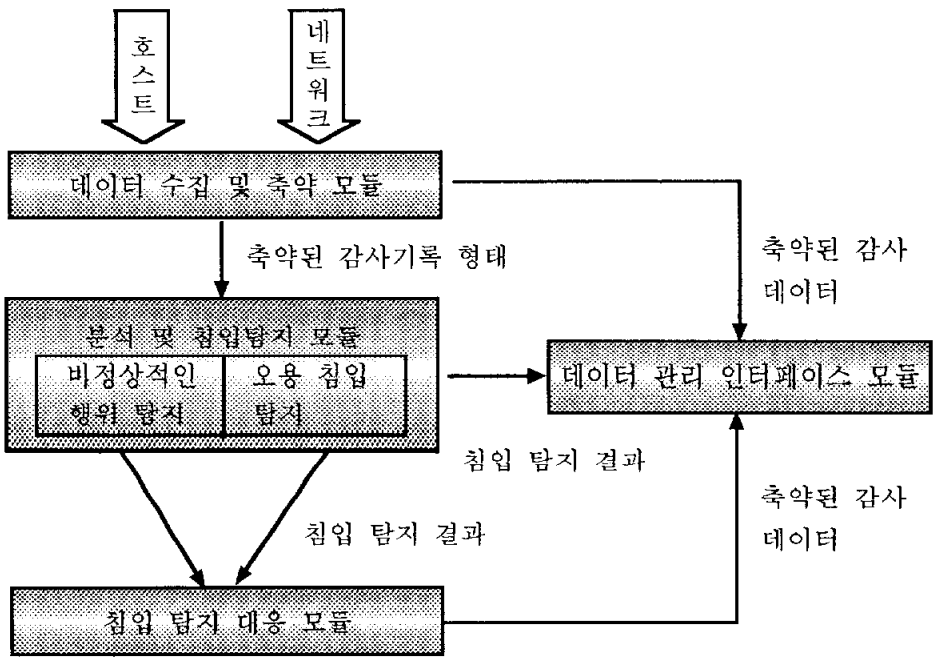
(3) 데이터 관리 인터페이스 모듈

데이터 관리 인터페이스 모듈은 데이터 수집 및 축약 모듈에서 생성된

축약 감사 데이터, 분석 및 침입 탐지 모듈에서 사용하는 침입 시나리오나 프로파일, 침입이 탐지 되었을 경우 발생하는 분석 결과 등 침입 탐지 시스템에서 발생하는 모든 데이터의 저장 및 관리를 수행한다. 데이터 관리 인터페이스 모듈은 소규모 DBMS(DataBase Management System)처럼 데이터 관리에 관한 모든 기능을 제공한다. 이렇게 보관된 데이터들은 추후 시스템 관리자가 보안 관련 정보들을 검사하고 분석하는 데 있어 효과적인 수단을 제공할 뿐만 아니라 추적을 위한 증거로서도 필요하다.

(4) 침입 탐지 대응 모듈

침입 탐지 대응 모듈은 침입이 탐지되었을 경우 수행되는 대응 행동을 담당한다. 최종적으로 침입이라고 판단되면 침입의 일련 진행 상황을 시스템 관리자에게 시각적으로 사전에 경고를 보내 관리자의 판단에 의거 관련 대응 조치를 취하게 한다.



[그림 5] 침입 탐지 시스템의 구성요소

Ⅳ. 계층적 구조의 통합 침입 탐지와 역추적 기술

기존의 침입 탐지 시스템은 호스트 기반 또는 네트워크 기반의 단일 시스템 하에서 탐지 기능을 제공하여 대규모 네트워크 환경 하에서 갈수록 다양해지는 침입에 대해 능동적으로 대처하는 데 어려움이 많았다. 이번 장에서는 능동적인 침입 대응 모델의 기반 기술인 계층적 구조의 통합 침입 탐지 모델과 역추적 기술에 대해 분석 한다.

4.1 하이브리드형(Hybrid Type) 침입 탐지

침입 탐지 시스템은 침입 여부를 판정하는 데 있어 크게 2가지 종류의 에러를 유발할 수 있다. 첫째는 침입이라고 판정하였는 데 실제로는 침입이 아닌 경우 과탐지(False-Positive Error)가 발생할 수 있고, 두번째는 침입이 아니라고 판정하였는데 실제로 침입인 경우 미탐지(False-Negative Error)가 발생할 수 있는데, 실제 대부분의 침입 탐지 시스템이 이러한 종류의 에러를 가지고 있다. 이러한 에러율을 줄이기 위해 알려지지 않은 공격을 탐지하는 데 비정상적인 행위 탐지 방법이 사용되지만 갈수록 지능화되는 침입 기법으로 정상 행위와 의심스런 행위간의 식별력이 어려워 에러율이 높아지게 된다. 오용 침입 탐지 방법은 알려진 침입 기법에 대해서만 탐지가 가능하고, 새로운 침입 방법에 대해서는 사람이 직접 분석하여 지속적으로 그 결과를 첨가해야 하므로 유지 및 관리 비용이 증가하게 된다. 하이브리드형 침입 탐지 방법은 비정상적인 행위 탐지 방법과 오용 침입 탐지 방법을 모두 사용하여 침입 탐지의 정확도를 높인 것이다.

4.2 계층적 구조의 통합 침입 탐지 모델

대규모 네트워크 환경 하에서 전체적으로 통합된 침입 탐지를 하기 위해서는 침입 탐지 기법의 확장 및 서로 다른 방식으로 얻어지는 정보들에 대한

통합이 요구되며, 이에 따른 고수준의 통신 프로토콜에 대한 정의가 필요하게 된다. 그리고 여러 호스트에서 발생한 보안 관련 이벤트들의 상호 관계에 대해 분석하여 하나의 이벤트가 다른 이벤트에 어떤 영향을 미치는지를 파악하는 것도 고려 되어야 한다.

계층적 구조의 통합 침입 탐지 시스템은 복잡한 구조를 지닌 대규모 네트워크 환경 하에서 침입 탐지의 광범위한 분석을 가능하게 하고, 그 종류로는 AAFID, EMERALD, GrIDS, JAM, JI-Nao, NetSTAT 등이 있다.

4.2.1 AAFID

AAFID(Autonomous Agents For Intrusion Detection) 구조의 시스템은 퍼듀 대학에서 에이전트를 이용하여 개발한 침입 탐지 시스템이다[16].

기존의 침입 탐지 시스템은 중앙 집권식 시스템에서 침입 탐지를 수행하여 중앙 시스템 자체가 침입의 대상이 될 수 있으며, 하나의 호스트에서만 감사를 수행하므로 감사 대상이 제한적이 된다.

AAFID 시스템은 계층적이고 분산된 에이전트의 구조를 가짐으로써 하나의 에이전트가 서비스를 중지해도 다른 에이전트들이 수행을 계속할 수 있도록 하며 각 에이전트들이 독립적으로 수행하므로 전체의 시스템을 다시 시작해야 하는 번거러움이 없다. 또한 각 계층에 있는 에이전트들은 수집한 정보를 간단히 정리해서 상위 계층으로 전달하므로 침입자가 분산 공격을 시도할 때 쉽게 감지할 수 있다.

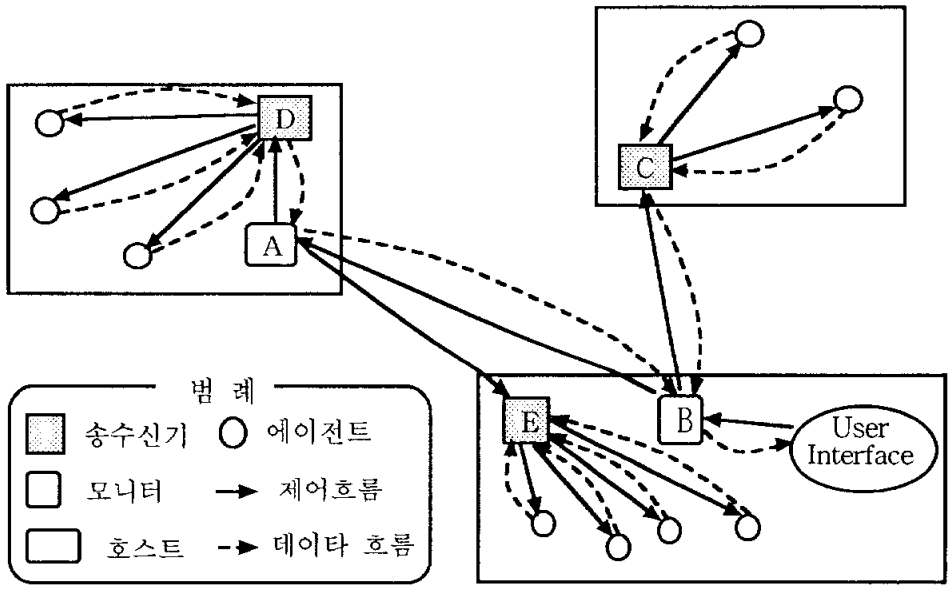
AAFID 시스템은 기본적으로 [그림 6]과 같이 에이전트(agents), 송수신기(transcivers), 모니터(monitors)의 세가지 요소로 구성된다. 이 구성 요소들은 AAFID 개체(entities)나 간단히 개체라고 부르고, 이 개체들로 구성된 전체 침입 탐지 시스템을 AAFID 시스템이라고 한다.

AFFID 시스템은 네트워크상에서의 여러 호스트들에 분포될 수 있다. 에이전트는 호스트에서 발생한 관심있는 이벤트들을 감시하는 데, 각각의 호스트는 많은 에이전트들을 포함할 수 있다. 모든 에이전트들은 자신이 속한 호스트상에서 비정상적인 행위를 감지하면 송수신기에게 보고하게 된다. 송수신

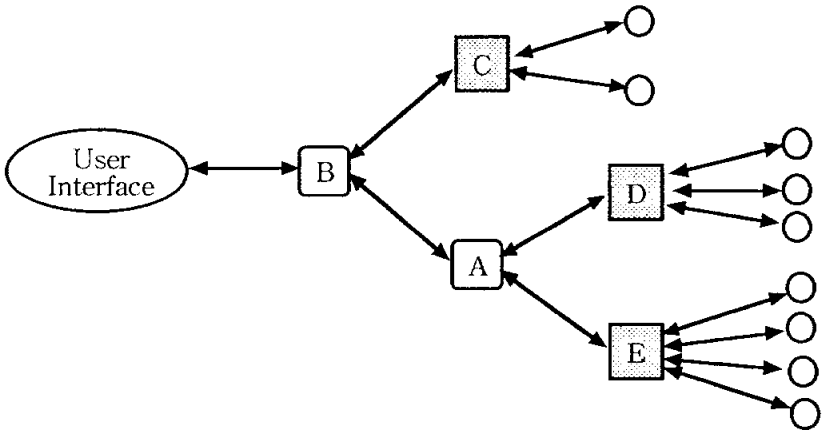
기는 각 호스트마다 하나씩 존재하며 호스트에서 동작하는 에이전트들을 감독하고 제어하고, 에이전트들에게서 수신한 데이터들을 요약해 하나 혹은 그 이상의 모니터들에게 그 결과를 보고 한다.

각각의 모니터는 여러 송수신기들의 동작을 감독한다. 모니터는 네트워크상의 데이터에 접속하기 때문에 고수준의 상호 연관관계를 분석하고 여러 호스트들 사이의 연관된 침입을 탐지할 수 있다. 모니터들은 계층적 구조로 구성될 수 있기 때문에 하위 계층의 모니터가 상위 계층의 모니터에게 보고할 수 있으며, 송수신기는 모니터의 고장을 대비해 하나 이상의 모니터에게 보고할 수 있다.

마지막으로 모니터는 사용자 인터페이스로 정보를 제공하고 제어 명령어들을 받는다. AFFID 시스템의 논리적 구조는 [그림 7]과 같다.



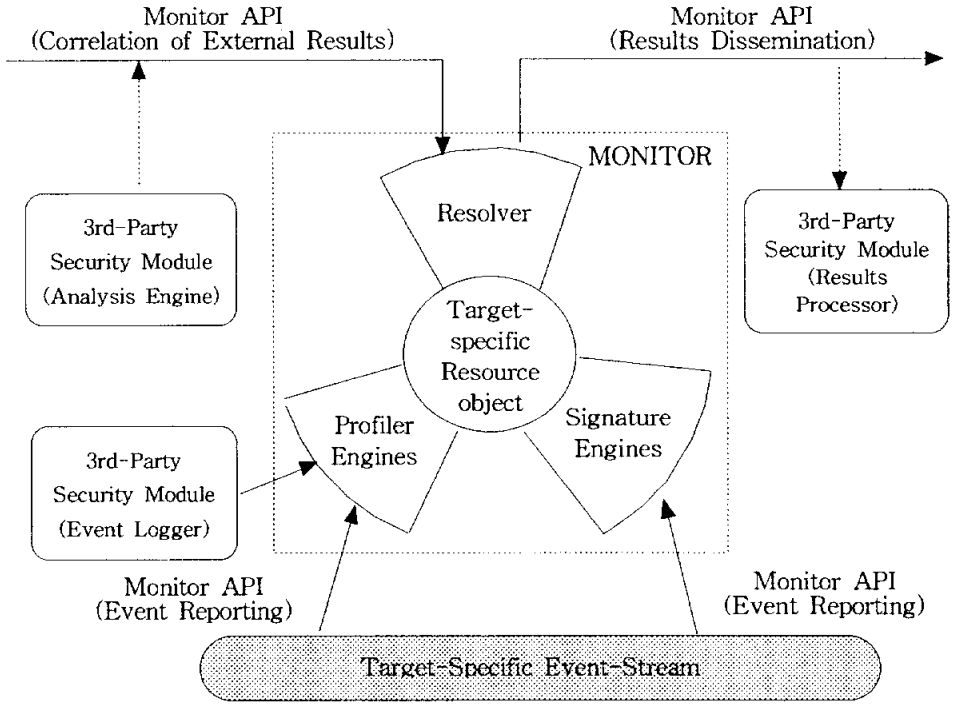
[그림 6] AAFID 시스템 구성 요소의 물리적인 표현



[그림 7] AAFID 시스템의 논리적 구조

4.2.2 EMERALD

EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbances) 시스템은 네트워크 서비스의 실시간 보호를 제공하기 위해 통계 기반 분석과 서명 분석을 결합한 능률적인 침입 탐지 기능을 제공하며, 광범위한 침입 탐지 기능과 네트워크에서 일어날 수 있는 중요한 공격에 대한 대응 능력을 제공하기 위해 분산되어 있는 모니터의 분석을 종합하는 프레임워크(Framework) 개념이 도입된 것으로 일반적인 모니터의 구조는 [그림 8]과 같다[17].



[그림 8] 일반적인 EMERALD 시스템의 모니터 구조

EMERALD 시스템은 탐지 메시지의 교환을 위해 호환성을 지원하는 스크립트 기반 메시지 인터페이스를 제공한다. 모니터는 분석 엔진과 Resolver (해석기)로 구성되는데, 분석 구조는 목표 대상으로부터 얻어진 이벤트들을 프로파일 엔진에서는 통계 기반 분석을 하고, 서명 엔진에서는 규칙 기반 코드 분석을 각각 실시한 후 요약한 보고를 Resolver에게 보낸다.

Resolver는 각각의 엔진에서 만들어진 요약 보고를 종합적으로 분석하고 조정하는 역할을 담당한다. 이렇게 하나의 이벤트에 대한 다른 분석 기법을 적용, 종합함으로써 EMERALD 모니터는 쉽게 계층적으로 통합된 탐지 구조를 가질 수 있다. EMERALD 시스템은 다른 응용 도메인으로 크게 확장할

수 있는 분석 기술을 지원하고, 상호 운용성, 재사용성, 무한한 확장성을 제공한다. 또한, 네트워크에 독립적으로 분산되어 있는 모니터를 사용하여 대규모 네트워크에서 계층적인 구조를 이루어 비정상적인 행위를 탐지한다.

4.2.3 GrIDS

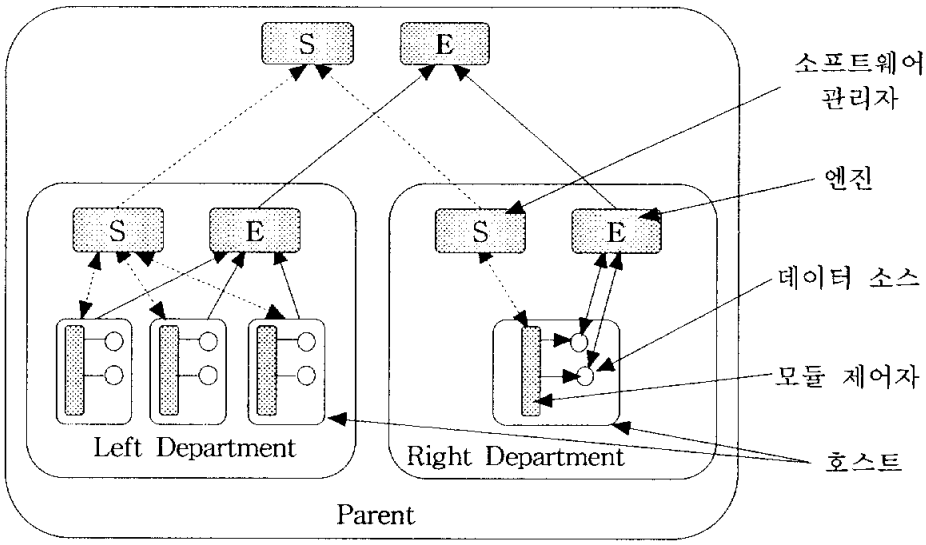
GrIDS(Graph-Based Intrusion Detection System for Large Networks) 시스템은 호스트들의 행위와 호스트들 사이의 네트워크 트래픽에 대한 데이터를 수집하고, 이렇게 모인 정보를 네트워크의 행위를 대표할 수 있는 행위 그래프로 표현한다. 이는 대규모의 자동화된 침입 공격을 거의 실시간으로 탐지하는 것을 가능하게 한다[18]. GrIDS 시스템은 네트워크 관리자들로 하여금 어떤 사용자들이 호스트 혹은 호스트 그룹의 특정 서비스를 이용하는지에 대한 정책을 제시할 수 있게 하며, 이에 따른 행위 그래프의 특성들을 분석함으로써 기술된 정책의 위험성을 탐지하고 보고할 수 있다.

GrIDS 시스템은 그래프 표현을 위해 계층적인 축약 설계를 이용하여 대규모 네트워크를 탐지 가능하게 하고, 초기의 프로토타입은 특히 웜 공격을 탐지하는 데 성공적이었다.

구조는 [그림 9]와 같이 세 부분으로 구성된 단순한 계층을 묘사한다. 모든 GrIDS 소프트웨어는 표준화된 인터페이스를 지닌 모듈들로 형성되며, 이러한 모듈들은 각 호스트에 위치한 모듈 제어 프로세스에 의해 수행되거나 멈추고 제어된다. 각 부분은 소프트웨어 관리자와 그래프 엔진으로 구성되고, 소프트웨어 관리자는 계층적이고 분산적인 모듈들을 관리하며, 계층적인 구성은 사용자 인터페이스를 통해 동적으로 재배열 될 수 있다. 기타 여러 모듈들 또한 이와 비슷하게 자동적으로 동작 유무가 결정된다.

GrIDS 데이터 소스들은 호스트와 네트워크 상의 행위를 모니터링 하는 모듈들이며, 탐지된 행위의 보고를 엔진으로 보낸다. 그래프 엔진은 이러한 데이터 소스 모듈들로부터의 입력을 그래프로 표현하며, 이러한 그래프의

묶음을 상위 엔진으로 보낸다. 이를 바탕으로 상위 엔진은 동시적인 결과 그래프를 생성한다. 이러한 구성 요소 이외에도 사용자와의 상호작용을 위한 사용자 인터페이스 모듈이 존재하며, 이는 관리 기능 및 디스플레이 기능 등을 수행한다.



[그림 9] GrIDS 전체 시스템 구조

대규모 네트워크 환경에 적합한 다른 계층적 구조의 통합 침입 탐지 시스템에 대해 살펴보면 JAM, Ji-Nao, NetSTAT 등이 있다.

JAM(Java Agents for Meta-learning over distributed databases) 시스템은 침입 패턴에 대한 빠른 분배를 위해 분산 환경에서 메타 학습의 이식성과 확장성을 제공하는 에이전트 기반의 데이터 마이닝 시스템이다.

Ji-Nao 시스템은 네트워크 하부 구조로 침입하는 것을 막기 위해 침입 탐지와 네트워크 하부 구조의 상호 보완적 접근 및 안전한 연결 프로토콜을 제공하는 시스템이다.

그리고 NetSTAT(Network-based Intrusion Detection Approach) 시스템은 STAT(State Transition Analysis Tool)의 도메인 독립적인 핵심모듈을 사용하고 종합 모듈로 확장하는 방법을 제공하는 시스템으로 호스트와 네트워크 기반의 침입 탐지 시스템을 자동 배치하며, 공격 시나리오를 자동 분석하는 기능을 제공한다.

4.3 역추적 기술

침입자 역추적 기술은 침입자의 근원지를 추적하는 기술로서, 현재까지 많은 방안들이 연구되고 있으나 아직 실용적인 연구성과가 거의 드문 실정이다. 인터넷의 익명성과 침입자가 직접적인 해킹이 아닌 여러 시스템을 경유하여 단계별로 공격 대상 시스템에 침입하기 때문에 인터넷을 구성하고 있는 프로토콜의 특성상 침입 근원지에 대한 역추적이 매우 어렵게 되는 것이다. 현재 국제적으로도 역추적 기술과 관련하여 표준화 작업이 진행되지 않고 있으며, 인터넷 국제 표준화 기구(IETF)에서도 단지 몇개의 인터넷 국제 표준(RFC)만이 나오고 있는 상태다. 기존의 역추적 기술에 대해 분석해 보면 다음과 같다.

4.3.1 로그정보 기반 침입자 역추적 기술

UNIX 시스템에서 사용되는 기본적 로그정보를 이용하여 침입자의 흔적을 찾아내는 가장 기본적인 방법으로 UNIX 계열 시스템에서는 커널과 각종 응용 프로그램 등에서 많은 종류를 로그를 남기고 있다. 이러한 로그 파일들을 분석하여 침입자가 남기고 간 다양한 흔적을 찾아 역추적을 수행 한다. 침입자 추적시 사용될 수 있는 로그 파일들은 시스템 로그와 네트워크 서비스 로그들이 있다. 시스템 로그 파일들은 wtmp, utmp, pacct, syslog, sulog, messages 등이 있고, 네트워크 서비스 로그 파일들은 www, ftp 등이 있다

[7].

로그 파일 분석은 침입자에 의해 특정 로그 파일들이 삭제 당하거나 로그 내용이 편집될 수 있는 등 침입자의 흔적을 지워버릴 수 있는 가능성이 높기 때문에 실시간 역추적 시스템을 구성하는 데는 부적합하다.

4.3.2 신원확인 서버 기반 침입자 역추적 기술

실시간 침입 탐지 시스템과 신원확인 서버를 이용하여 침입자를 역추적하는 대표적인 방식으로 CIS(Caller Identification System)[8]와 RFC (Request For Comment) 1413에서 정의된 신원확인 서버[9]가 있다.

CIS는 TCPWrapper의 필터링 개념을 도입하여 어떤 시스템에 로그인 하는 사용자는 자신의 그 이전에 거쳐왔던 시스템과 로그인 ID 등의 정보를 주어야만 로그인 할 수 있는 프로토콜을 제안한 것으로 침입자 탐지가 이루어졌을 때 모든 시스템의 정보를 확인 할 수 있기 때문에 실시간으로 최초 네트워크 접점지를 찾아낼 수 있게 된다. 신원확인 서버는 CIS와 비슷한 개념으로서 신원확인 서버가 사용자가 거쳐온 이전 경유지 시스템의 모든 신원정보를 확인할 수 있는 것이다.

두 방식 모두 사용자의 인증을 위해 많은 요청과 확인 메시지의 전송을 필요로 하기 때문에 통신망의 가역 대역폭을 낭비하게 되며 인가된 사용자의 시스템 접근 시간을 저하시켜 시스템의 가용성이 효율적이지 못한 문제점이 있다.

4.3.3 미행 기술을 이용한 침입자 역추적 기술

미행 기술은 특정 사용자를 추적하기 위한 기법으로 모니터링 행위 자체를 보호함으로써 신분 확인을 위한 시간을 확보하고, 침입자가 이동하는 경우 미행 모듈 자신을 이동 경로에 복제시켜 영역 확장을 함으로써 침입자의 신분 확인에 필요한 정보를 수집 가능하게 한다. 이러한 미행기술을 이용한 침입 자동 대응 시스템도 연구되고 있다[10].

미행 기술은 모니터링, 자기 보호, 복제와 같이 세 부분으로 구성된다. 침입자가 시스템에 머무르는 동안 로그인 tty를 모니터링하여 호스트 레벨에서의 감시를 수행한다. tty는 사용자가 로그인 할 때마다 동적으로 할당되는 pty를 통해 감시되고 침입자의 터미널을 복사하는 방식으로 미행을 수행하게 된다. 침입자가 다른 호스트로 이동하여 관리자 권한을 획득했을 경우, 모니터링 행위 자체를 보호하면서 미행하여 그 시스템에 신분확인을 위한 모듈들을 복제함으로써 다시 미행을 위한 거점을 확보할 수 있다.

호스트 레벨에서의 행위 감시가 수행되다가 침입자가 다른 호스트로 이동하는 경우 이를 추적하기 위해 네트워크 레벨의 감시가 수행되는 분산된 모니터링을 하게 된다.

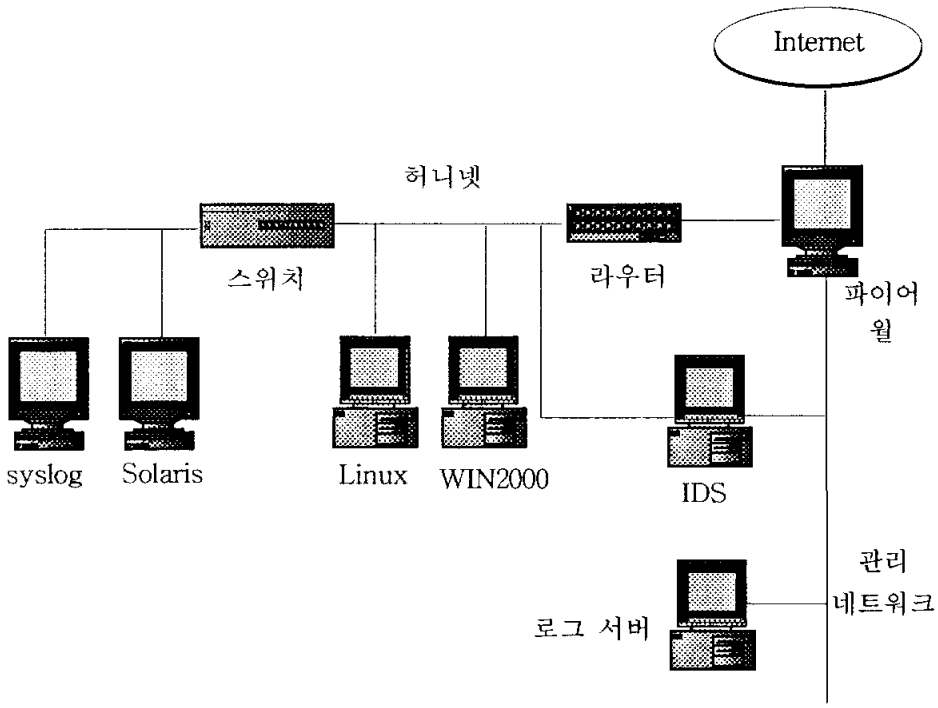
4.3.4 허니넷(Honeynet)

허니넷이란 해커들이 시스템을 탐색하고 부당하게 이용하기 위해서 사용하는 해킹 도구, 그들이 사용하는 전술, 해킹 동기 등에 대한 정보를 습득하고, 습득된 정보를 이용하여 역추적 기술 등 대응 방안을 구축하기 위한 목적으로 구축된 다중 시스템으로 구성된 네트워크를 말한다. 즉, 해커들의 근원지를 역추적 하기 위해 해커들을 시스템에 접속한 상태로 머무르게 하는 일종의 가상 네트워크라 할 수 있다[19].

해커 유인체계의 의미로 허니넷과 허니팟(Honeypot)이 사용되고 있으나, 허니팟은 해커를 속일 목적으로 공격당하도록 설계된 하나의 시스템으로서 리코스 테크놀러지사의 Mantrap[20] 등을 들 수 있다.

허니넷은 하나의 시스템이 아닌 다중 시스템으로 구성되는 네트워크로 구성은 [그림 10]과 같다. 허니넷은 다중 시스템으로 구성되기 때문에 실제 네트워크 구성과 거의 동일하게 구성할 수 있기 때문에 수집된 정보를 바탕으로 실제 네트워크의 보안을 향상 시킬 수 있다. 허니넷은 파이어월 뒤에 위치하여 해커가 사용하는 모든 데이터에 대한 수집과 제어를 수행하며, 허니넷에 위치하는 모든 시스템은 흔히 접할 수 있는 표준 시스템으로 고의

적으로 취약하게 설계할 필요가 없다. 따라서, 허니넷에서 발견되는 모든 취약점은 실제 네트워크상에서도 존재하는 것이 된다.



[그림 10] 허니넷 구성도

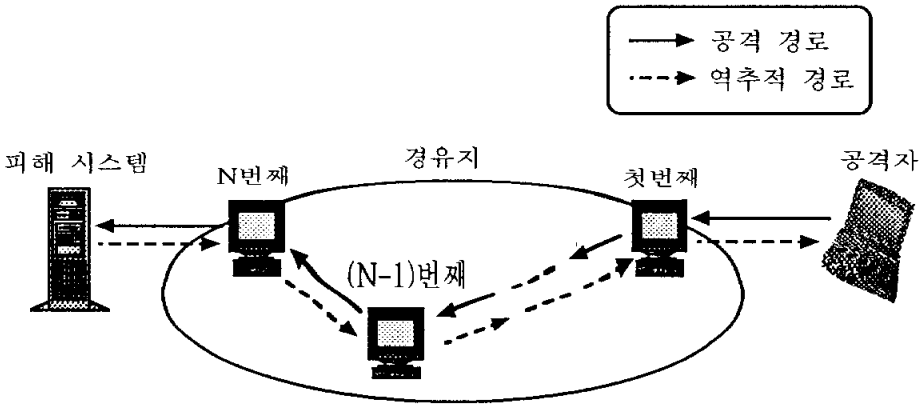
V. 능동형 침입 대응 모델

이번 장에서는 본 논문에서 제시하고자 하는 능동형 침입 대응 모델을 설계하고자 한다. 즉, 대규모 네트워크 환경 하에서 침입 발생시 계층적 구조의 통합 침입 탐지 시스템과 에이전트 침투를 이용한 역추적 시스템을 결합하여 침입 탐지와 동시에 침입 근원지를 찾을수 있도록 한다.

5.1 기본 개념

해킹 등의 인터넷 공격을 시도하는 공격자는 주로 신분을 감추기 위해 자신의 시스템으로 직접 공격하는 것이 아니라 N개의 경유지 시스템들을 해킹하여 피해자의 시스템에 마지막으로 공격한다[그림 11].

침입 탐지와 동시에 공격자를 찾기 위해서는 경유한 N개의 시스템들에 대해 차례대로 에이전트를 침투시켜 역추적 하여야 한다.

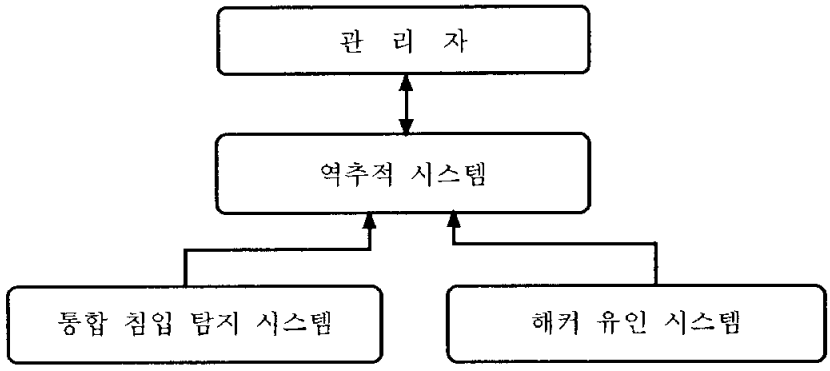


[그림 11] 역추적 경로

5.2 전체 시스템 구조

능동형 침입 대응 모델은 크게 통합 침입 탐지 시스템, 해커 유인 시스템, 역추적 시스템 세 부분으로 이뤄진다[그림 12].

대규모 네트워크 환경 하에서 발생한 침입에 대하여 통합 침입 탐지 시스템에서 실시간으로 탐지하고, 해커 유인 시스템에서 해커의 침입에 대한 성향과 해킹 기법을 분석한다. 역추적 시스템에서는 통합 침입 탐지 시스템과 해커 유인 시스템에서 넘겨받은 각종 로그 및 이벤트 관련 정보를 근거로 능동 에이전트를 해킹 경유 시스템에 침투시켜 침입 근원지를 역추적하고 관리자와의 인터페이스를 통해 역추적 결과를 보여주는 구조로서 해커의 공격에 대한 탐지와 역추적 기술의 유기적인 연계로 적극적이고 능동적인 대응 체계를 구축한다.



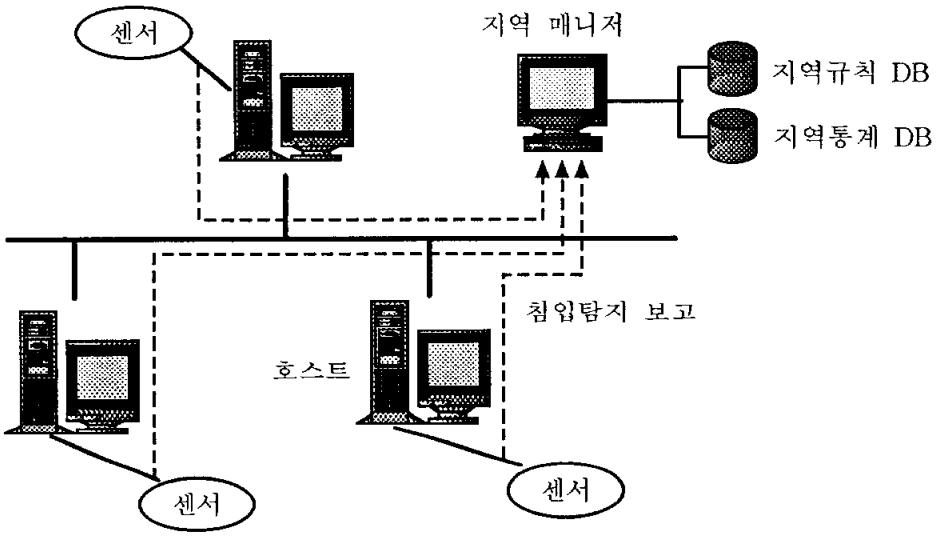
[그림 12] 능동형 침입 대응 모델 구조

5.2.1 계층적 구조의 통합 침입 탐지 시스템 구현

최근의 해킹 공격 기법은 대규모 네트워크 환경 하에서 갈수록 복잡하고 다양해져 기존의 침입 탐지 시스템들처럼 단일 환경 또는 단일 시스템하에서 침입을 탐지하는 방법으론 적절하게 대응하기가 어렵다.

능동형 침입 대응 모델의 통합 침입 탐지 시스템 부분은 대규모 네트워크 환경 하에서 효율적으로 침입을 탐지하기 위해 지역 매니저(Local Manager)와 전역 매니저(Global Manager)로 이뤄진 계층적 구조의 모델을 제안한다.

지역 매니저는 각 호스트의 센서들이 오용 침입 탐지와 비정상적인 행위 탐지 결과를 통합 판정하는 모듈로서 지역 네트워크를 담당하는 서버 안에서 프로그램이 수행된다. 지역 매니저는 센서 라우터와 지역 규칙 데이타베이스, 지역 통계 데이타베이스로 구성된다[그림 13].

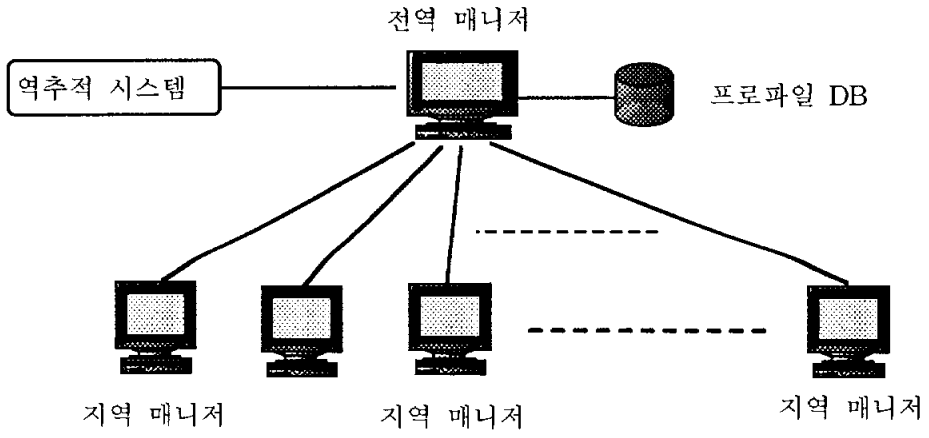


[그림 13] 지역 매니저 구성도

센서는 각 호스트마다 설치되어 침입을 탐지하여 지역 매니저에게 결과를 통보하는 역할을 담당 하는 것으로 플랫폼에 독립적이어서 이기종간에 구성이 가능하며 동적으로 시스템에 추가, 삭제가 가능하다.

지역 매니저에 있는 센서 라우터는 센서에 대한 정보를 관리하며, 센서의 연결 및 해제를 담당한다. 지역 규칙 데이타베이스는 하나의 호스트에서 발생하는 오용 침입을 탐지하는 데 사용되고, 지역 통계 데이타베이스는 사용자 행위의 임계치를 설정하여 사용자의 현재 행위와 프로파일 값을 비교하여 침입 여부를 판정하는 데 사용된다. 지역 매니저는 각 센서들로부터 수집한 정보를 바탕으로 지역 네트워크 수준의 통합 판정을 수행하고 전역 매니저에게 정보를 제공한다.

전역 매니저는 여러 지역 매니저에서 얻어지는 정보를 바탕으로, 지역 매니저에서 미처 탐지하지 못한 침입을 탐지할 수 있는 전역 네트워크 수준에서 침입 탐지를 수행한다[그림 14].



[그림 14] 전역 매니저 구성도

전역 매니저의 프로파일 데이타베이스는 각 호스트의 구조와 운영체제, 이벤트 형태, 이벤트 데이터의 의미 등을 고려하여 관련 정보를 관리, 저장한다.

이렇게 지역 매니저와 전역 매니저는 계층적으로 이루어지며, 네트워크의 규모가 커지더라도 같은 매커니즘을 적용할 수 있다. 그리고 전역 매니저는 역추적 시스템과 연결되어 통합 침입 판정 결과를 제공하여 침입 근원지를 찾게 한다.

5.2.2 해커 유인 시스템 구현

능동형 침입 대응 모델의 해커 유인 시스템 부분은 허니넷을 이용한 것으로 역추적 시스템과 연결되어 역추적의 기지로 활용한다[그림 15].

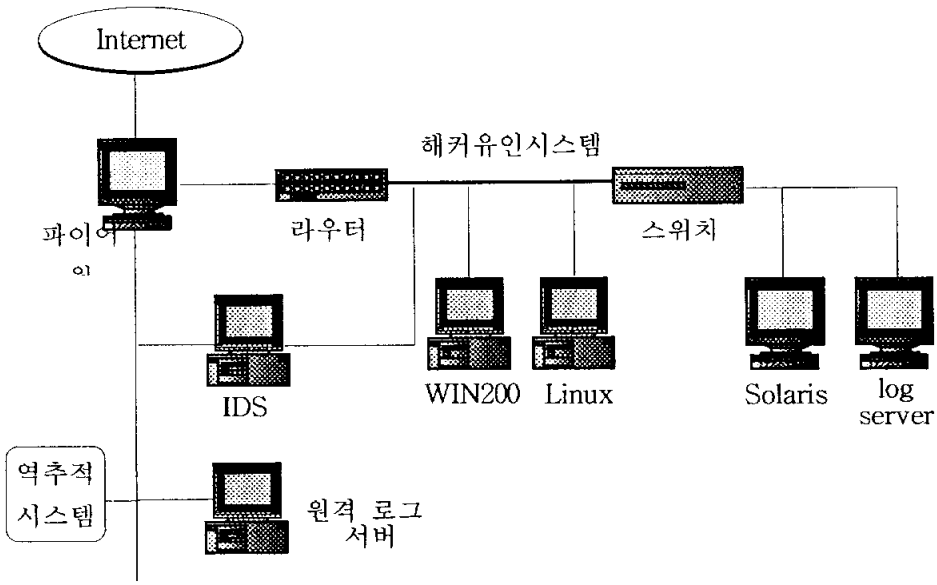
해커 유인 시스템에서 수집한 침입자의 해킹 도구, 방법, 성향 등을 역추적 시스템에 실시간으로 제공하여, 역추적 시스템이 침입자의 해킹 패턴에 따라 다른 에이전트 침투 시나리오를 갖도록 하고 보다 빠르게 침입자를 역추적할 수 있는 기본 자료를 제공한다.

해커 유인 시스템에서는 들어오거나 나가는 모든 트래픽을 의심스러운 것으로 정의하여 엄청나게 많은 정보들 중 어떤 정보가 정상 트래픽인지, 어떤 정보가 악의적인 행위인지 판단해야 하는 어려움을 해결한다.

해커 유인 시스템을 구성하는 데 있어 가장 중요한 것은 데이터 제어와 수집인데 본 논문에서는 데이터 제어를 [그림 15]에서 파이어월과 라우터의 접근 제어 기능을 이용한다. 데이터 제어는 모든 패킷에 대해 갈 수 있는 방향을 제어하는 것을 의미하는 데, 파이어월과 라우터에서 데이터 제어를 함으로써 해커 유인 시스템이 침입자에 의해 분산 서비스 공격이나 시스템 스캔 등과 같이 다른 시스템들을 공격하는 경유지로 이용하는 것을 막는다. 해커 유인 시스템은 파이어월 뒤에 위치 시키며, 파이어월은 외부로 나가는 데이터에 대해 서비스나 포트 등을 적절히 제어해 취약점을 노출시켜 침입자가 계속 해커 유인 시스템에 남아 있게 할 수도 있다. 라우터는 해커 유인 시스템과 파이어월을 분리하여 침입자가 해커 유인 시스템이 실제 시스템과

같다고 느끼게 하고 파이어월의 접근 제어를 보조하는 기능을 담당한다.

해커 유인 시스템 내부에서의 데이터 수집은 IDS가 담당하는데, 수집된 데이터는 내부에 저장하지 않고 원격 로그 서버에 저장해, 침입자가 내부에 저장된 데이터를 변조, 삭제할 가능성을 없애고, 침입한 시스템이 해커 유인 시스템이란 걸 모르게 한다.

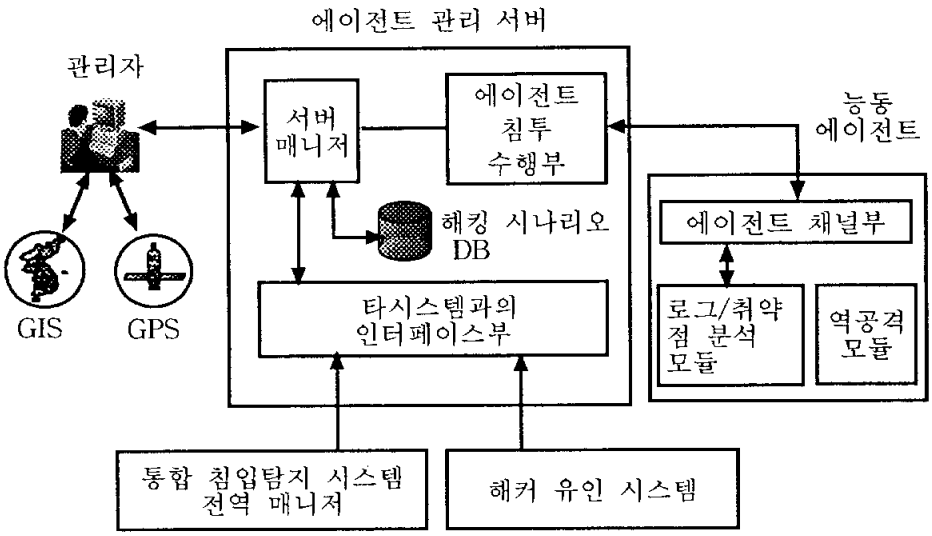


[그림 15] 해커 유인 시스템 구성도

5.2.3 역추적 시스템 구현

능동형 침입 대응 모델의 역추적 시스템 부분은 통합 침입 탐지 시스템 전역 매니저의 침입 판단 결과와 해커 유인 시스템의 해킹 기법 등 관련 정보들을 바탕으로 침입 근원지를 역추적하고 관리자와의 인터페이스를 통해 역추적 결과 통보 및 관리자의 매니저 기능을 제공한다.

본 논문에서 제시하고자 하는 역추적 시스템은 크게 에이전트 관리 서버와 능동 에이전트로 나눠 설계한다. 에이전트 관리 서버는 다시 서버 매니저, 해킹 시나리오 데이타베이스, 해커 유인 시스템 및 통합 침입 탐지 시스템 전역 매니저와의 인터페이스부, 에이전트 침투 수행부로 나눠 구성한다. 능동 에이전트는 에이전트 채널부, 로그 및 취약성 분석 모듈, 역공격 모듈로 구성한다[그림 16].



[그림 16] 역추적 시스템 구성도

(1) 에이전트 관리 서버

에이전트 관리 서버는 보안시설이 잘 되어 있는 중앙 센터에 설치하고, 관리자는 원격에서 웹 브라우저를 통해 관리 서버에 접속한다. 에이전트 관리 서버에는 관리자 인터페이스를 위한 CGI 프로그램이 있고 관리자 위주의 편리한 윈도우 환경을 제공한다.

o 서버 매니저(Server Manager)

에이전트 관리 서버 내의 서버 매니저는 각종 정보를 관리자에게 보고하고, 통합 탐지 시스템 전역 매니저에게서 보고되는 실시간 침입 탐지 결과를 기반으로 역추적 공격 수행 결정을 하며, 관리자와 해커 유인 시스템에 의해 입력, 보고 되는 해킹 기법 등을 해킹 시나리오 DB에 저장한다.

o 타시스템과의 인터페이스부

서버 매니저와 해커 유인 시스템 및 통합 침입 탐지 시스템 전역 매니저 사이의 인터페이스로서 실시간 침입 탐지 결과와 해킹 기법 등을 서버 매니저에게 전달한다

o 에이전트 침투 수행부

능동 에이전트를 자동으로 침투시켜 주는 일을 수행하는 것으로 능동 에이전트로부터 보고되는 침입 경유 시스템들의 로그 분석 및 취약점 분석 결과를 서버 매니저에게 전달하고, 해킹 시나리오 데이타 베이스에서 선택된 가장 적합한 해킹 방법을 바탕으로 능동 에이전트를 침입 경유 시스템에 침투시키는 역할을 담당한다.

o 해킹 시나리오 DB

운영체제, 해킹 기법, 시스템 취약점별로 적합한 해킹 공격 시나리오를 데이타베이스에 저장하고 있다가, 능동 에이전트로부터 보고되는 해당 시스템의 취약점 정보를 기반으로 인공지능 엔진에 의해 생성된 최적의 공격 시나리오를 서버 매니저에게 전달한다.

(2) 능동 에이전트

능동 에이전트는 침입 중간 경유지로 사용된 호스트에 침투되어, 그 호스트의 로그 자료 및 취약성을 분석하여 이전 경로를 찾아내는 일을 수행한다.

o 에이전트 채널부

에이전트 관리 서버의 에이전트 침투 수행부와 보안을 위한 은닉된 통신 채널을 유지하고, 로그 및 취약성 분석 모듈로부터 정보를 전달받고, 각 모듈로 명령을 전달하는 기능을 수행한다.

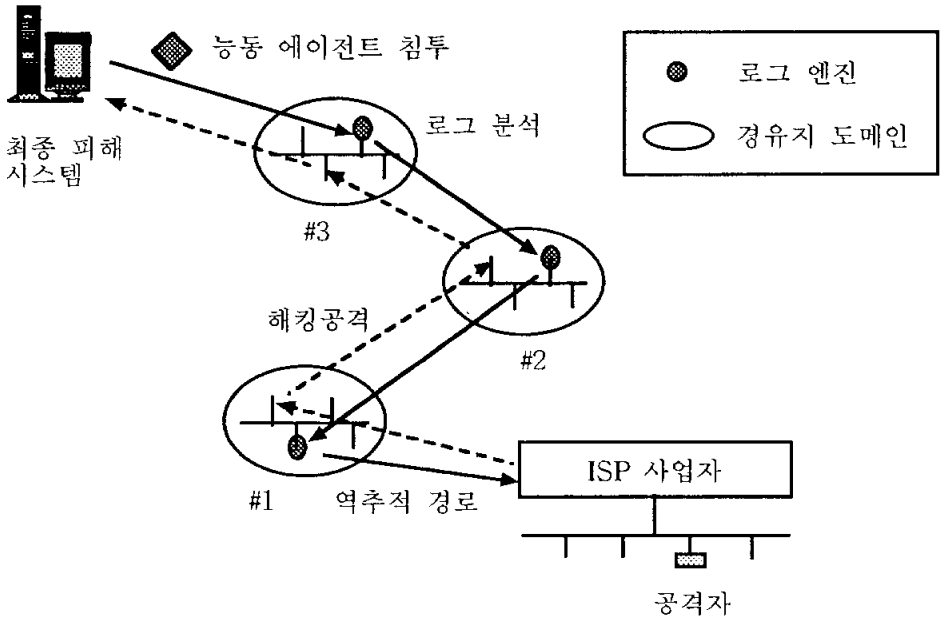
o 로그 및 취약성 분석 모듈

먼저 능동 에이전트 침투를 위해 먼저 대상 호스트의 취약성을 분석하고, 그 결과를 에이전트 채널부를 통해 에이전트 관리 서버에 통보한다. 능동 에이전트가 호스트에 침투하면 시스템의 로그, 프로세스 등을 분석하여 이전 경로를 파악하는 기능을 담당한다. 만약 침입자에 의해 중간 경유지의 로그가 삭제되거나 변조되었을 때 이전 경로를 찾기가 어려운데, 이 때 해커 유인 시스템의 침입자 정보를 참고하거나 패킷 모니터링 기능을 담당해 재침입시 침입 패턴을 검색해 이전 경로를 파악한다.

o 역공격 모듈

에이전트 채널부를 통해 공격 명령을 전달받아 침입 이전 경로 시스템을 공격해 능동 에이전트를 복제하는 기능을 수행한다.

네트워크에서 침입을 역추적 수행하는 과정은 [그림 17]과 같다



[그림 17] 역추적 수행 과정

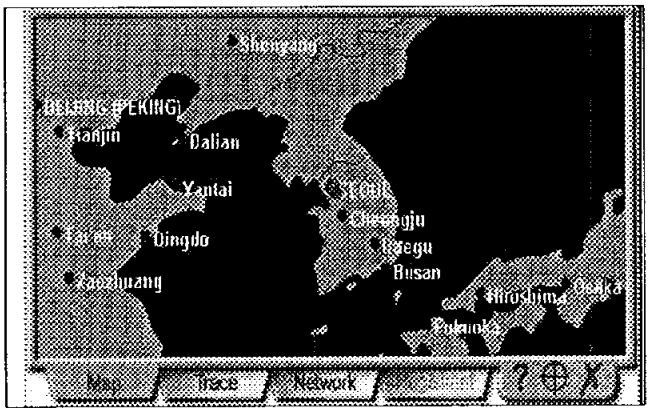
① 능동 에이전트가 #3 도메인에 침투해 도메인의 로그 엔진을 분석해 이전 경로인 #2 도메인의 특정 호스트에서 접속된 것을 확인

② 다시 #2 도메인에 침투해 도메인의 로그 엔진으로부터 #1 도메인의 특정 호스트에서 접속된 것을 확인

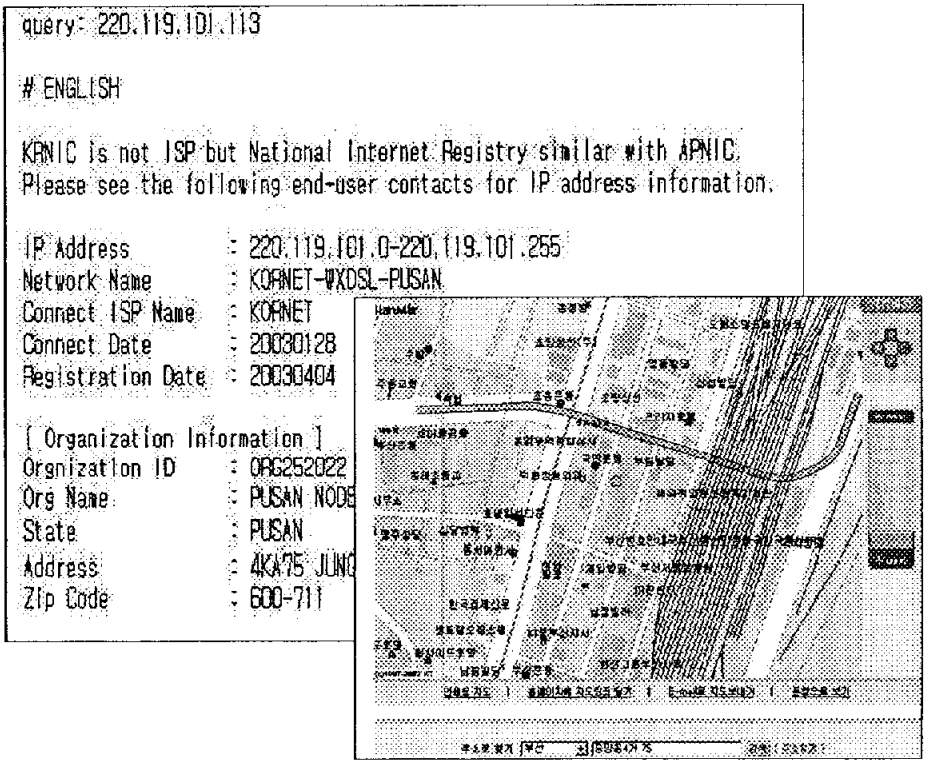
③ #1 도메인에 침투해 도메인의 NMA(Network Management Application)로부터 ISP 사업자의 PPP 접속 번호를 확인

④ ISP 사업자로부터 공격자의 신원을 확인

관리자의 웹 브라우저에서는 역추적 결과를 확인 할 수 있는데 지리정보시스템(GIS) 혹은 위치추적시스템(GPS)과 연동하여 결과를 보다 시각적으로 나타내 줄 수 있다[그림 18][그림 19].



[그림 18] 침입자를 추적해 지도상에 나타낸 화면



[그림 19] 추적된 IP에 대한 WHOIS 검색과 GIS 연동하여 출력한 화면

Ⅵ. 결 론

최근의 해킹사고를 보면 1.25 인터넷 대란에서도 볼 수 있듯이 해킹 공격이 갈수록 지능화, 대형화 되고 있는 추세를 보이고 있어 기존의 침입 탐지 시스템들처럼 단위 시스템의 보안 장비 만으로는 대규모 네트워크를 효율적으로 보호할 수 없다. 또한, 해커들은 공격 대상 시스템을 침입할 때 직접 공격하는 것이 아니라, 자신의 신분을 감추기 위해 여러 다른 중간 경유 시스템들을 이용해서 공격한다. 따라서, 기존의 침입을 탐지하는 수동적인 대응만으로는 사고 후 시스템을 복구하는 수준에 머물 수 밖에 없고, 실시간으로 침입을 탐지하여 침입자를 밝힐 수 없는 실정이다.

본 논문에서는 대규모 네트워크 환경 하에서 침입을 실시간으로 탐지하기 위한 계층적 구조의 통합 침입 탐지 시스템과 해커의 공격 기법, 성향 등을 알 수 있는 해커 유인 시스템, 에이전트를 이용해 침입자를 바로 역추적할 수 있는 기술을 유기적으로 연계한 능동형 침입 대응 모델을 제시하여 침입 피해를 최소화 하고, 침입 탐지와 동시에 해커를 역추적하는 보다 적극적인 대응를 하고자 하였다.

능동형 침입 대응 모델은 통합 침입 탐지 시스템의 지역 매니저와 전역 매니저가 계층을 이뤄 각각 지역, 전역 수준의 네트워크 침입을 실시간으로 탐지하여 역추적 시스템에게 알리고, 해커 유인 시스템은 해커의 공격 도구, 기법, 성향 등을 역추적 시스템에 제공하는 구조를 이뤘다.

역추적 시스템에서 통합 침입 탐지 시스템 전역 매니저의 침입 판단 결과를 보고 받으면, 능동 에이전트를 이전 공격 경유 시스템들에게 차례대로 침투시켜 침입 근원지를 역추적 하도록 하였다. 이 때 해커 유인 시스템이 제공한 공격자의 해킹 기법과 능동 에이전트가 알려온 대상 시스템의 취약점 분석 결과에 따라 다른 능동 에이전트 침투 시나리오를 가지도록 하였다.

또한 역추적 시스템 관리자의 웹 브라우저는 GIS 혹은 GPS와 연동시켜 침입 근원지 주소와 같은 역추적 결과를 시각적으로 보여줘 침입자 검거의

편의를 제공하도록 하였다.

본 논문에서 제안한 방식이 효율적으로 실행되려면 향후 다음과 같은 영역에 대한 연구가 필요하다.

첫째, 해커들에 의해 해킹 공격에 이용되는 경유지 시스템들의 로그 자료가 변조, 삭제 등 손상을 입을 경우 능동 에이전트가 로그 분석을 통한 이전 침입지의 파악이 어렵게 된다. 이런 경우 능동 에이전트가 시스템에 은닉하여 패킷 모니터링을 통해 알고 있는 침입 패턴과 같은 침입자를 찾아가는 기술과 같은 이차 침투 시나리오에 대한 연구가 진행되어야 한다.

둘째, 통합 침입 탐지 시스템과 해커 유인시스템, 역추적 시스템을 에러 없이 연결할 수 있는 표준화된 인터페이스부에 대한 연구가 필요하다.

세째, 능동 에이전트와 에이전트 관리 서버간의 데이터 교환시 암호통신 프로토콜에 대한 심도 있는 연구가 필요하다.

참 고 문 헌

[1] 한국정보보호진흥원, *정보보호뉴스 3월호*, 2003. 3.

[2] 국가정보원 정보보안119, *http://www.nis.go.kr*, 2002. 12.

[3] 은유진, 이정효, 김기현, 박정호, "호스트 기반 침입탐지시스템 구현 모델," Workshop on Information Security and Cryptography 98, pp.4-15, 1998. 9.

[4] 국가보안기술연구소, *CRYPTOPIA 2003년 제7권 1호*, 2003. 2.

[5] 한국전산원, 유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구, NCA VI-RER-95105, pp.17-23, 1995. 12.

[6] 정보통신교육원, *정보보안 교재*, pp.315-380, 1998. 4.

[7] 정현철, "UNIX 로그 분석을 통한 침입자 추적 및 로그 관리 : Part1," Technical Report CERTCC-KR-TR, pp.4-19, 2001. 11.

[8] Hyun Tae Jung, Hae Lyong Kim, Yang Min Seo, Ghun Choe, Sang Lyul Min, Chong Sang Kim, "Caller Identification System in the Internet Environment," In Proceedings of the 4th USENIX security symposium, pp.1-5, 1993.

[9] M. St. Johns, RFC1413 : "Identification protocol," 1993. 1.

[10] 장희진, 김상욱, "보안스킴의 자동확장성을 지원하는 미행 메커니즘," 정보보호학회논문지 제11권 제4호, pp.2-9, 2001. 8.

[11] Wenke. Lee, Salvatore J. Stolfo, "Data mining approaches for intrusion detection," In Proceedings of the 7th USENIX security symposium, San Antonio, TX, pp.1-2, 1998

[12] J. Ryan, M. J. Lin, R. Miikkulaine, "Intrusion Detection with Neural Networks," Advanced in Neural Information Processing Systems 10, Cambridge, MA, pp.1-7, 1998

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

[14] S. Kumer, E. H. Spafford, "A pattern matching model for misuse intrusion detection," In Proceedings of the 17th National Computer Security Conference, pp.1-10, 1994. 10.

[15] S.Garfinkel & G.Spafford, *Practical Unix & Internet Security*, O'Reilly Associates, pp.1-24, 1996.

[16] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, "An Architecture for Intrusion Detection using Autonomous Agents," Purdue University, pp.4-9, 1998. 6.

[17] P. A. Porras & P. G. Neumann, "EMERALD," Computer Science Laboratory SRI International, pp.1-13, 1997. 11.

[18] Staniford-Chen, S, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D.Zerkle, "GrIDS," In Proceedings of the 19th National Information Systems Security conference, pp.1-8, 1996.

[19] Know Your Enemy : Honeynets, http://project.honeynet.org

[20] About Mantrap, http://www.recourse.com

[21] Computer Industry Almanac Inc., http://www.c-i-a.com, 2002. 12.

[22] Network Wizards, http://www.isc.org/ds/WWW-200301/index.html, 2003. 1.

감사의 글

21세기 시작과 함께 기대 반, 두려움 반으로 어렵게 시작한 석사 과정을 어느덧 졸업 논문 완성과 함께 마무리하게 되었습니다. 그 동안 많은 도움을 주신 분들에게 작은 지면을 빌어 감사의 마음을 전하고자 합니다.

먼저 본 논문이 완성 될 수 있도록 아낌없는 지도와 많은 조언을 해주시고, 부족한 저에게 인생의 가르침을 함께 베풀어주신 윤종락 지도교수님께 진심으로 깊은 감사를 드립니다. 그리고 지금은 미국에 교환 교수로 나가 계시지만 학기 시절 지도교수님으로서 학교 생활을 열심히 할 수 있도록 용기를 주시고, 가르쳐 주신 정신일 교수님께 감사 드립니다. 그리고 바쁘신 와중에도 부족한 저의 논문을 검토해주시고 세심한 지도를 마다하지 않으신 장주석 교수님과 김석태 교수님께 깊은 감사 드립니다. 또한 대학원 과정에서 저에게 많은 가르침을 주신 하덕호 교수님, 정연호 교수님께도 감사 드립니다.

회사 생활을 하면서 본 과정을 논문 완성과 함께 무사히 마칠 수 있도록 많은 배려와 아낌없는 격려를 해주신 과장님, 팀장님, 그리고 선배님 모든 분들에게 진심으로 감사 드립니다.

저에게 항상 끊임없는 배움의 소중함을 가르쳐주신 아버님, 형님들, 그리고 학업을 잘 마무리 할 수 있도록 믿고 격려해 주신 장인 어른, 장모님께 깊은 감사 드립니다.

마지막으로 어려운 여건 속에서도 저를 믿고 변함없는 사랑과 성원을 보내준 아내에게 사랑어린 감사의 말을 전하며, 건강하게 무럭무럭 자라고 있는 사랑하는 우리 아들 찬혁이와 찬호에게 이 기쁜 마음을 전하고자 합니다.

지금 학업이 끝난 것이 아니라 항상 배우고자 하는 열의로 보다 나은 미래를 만드는 데 노력을 다해 감사한 모든 분들에게 보답하고자 합니다.

2003년 7월 11일

이 윤 근