인터넷 해킹피해 시스템자동분석에이전트(AIAA) 및 침입자 역추적 지원도구 구현

임 채 호† · 원 유 헌††

요 약

AIAA는 인터넷 서버 등에서 해킹으로 피해를 당하였을 때 침입자의 흔적을 자동으로 분석해주는 도구로서 침해사고처리담당자가 피해시스템에 에이전트 형태로 설치하여 운영하게 된다. AIAA는 마스터/에이젼트 형태로 구성되고 에이젼트에서는 정상적인 시스템의 로그분석모듈, 침입자가 설치한 불법프로그램을 점검하는 모듈로 구성되어 침입자가 남긴 흔적을 마스터로 보고하게 된다. 특히 침입자의 재차 침입을 모니터링하고 탐지할 수 있는 침입탐지 모듈을 탑재하여 침입자의 침입경로를 실시간으로 탐지, 마스터에게 보고함으로써 침입자를 역추적할 수 있도록 지원하게 된다.

Implementation of Autonomous Intrusion Analysis Agent(AIAA) and Tool for using Intruder Retrace

Chae-Ho Lim† · Yoo-Hun Won††

ABSTRACT

Autonomous Intrusion Analysis Agent(AIAA) is Incident Response Team staff's tool that scans, analyses, reports and alerts the traces of intrusion based on system logs and intruder's backdoors inside compromised system. This AIAA is dispatched to the compromised system by IR staff after security incident is reported to the IR team. AIAA is intelligent to recognize to check out who is intruder from all the user accounts and to report the suspected candidates to the master control system in IR team. IR staff who controls AIAA with master system can pick up an intruder from the canidates reported by AIAA agent and review all related summary reports and details including source host's name, finger information, all illegal behavior and so on. AIAA is moved to compromised system by the staff to investigate the signature of intrusion along the trace of victim hosts and it is also operated in secret mode to detect the further intrusion. AIAA is alive in all victim systems until the incident is closed and IR staff can control AIAA operation and dialogue with AIAA agent in Web interface.

1. 서 론

한국정보보호센터가 운영하고 있는 정보통신망 침해사고대응지원팀은 '96년부터 국내외 해킹피해사고를 접수하여 피해시스템의 분석, 피해내용 분석, 침입자 경로 분석과 해킹방법 분석 등의 기술지원을 하고 있다. 특히 침입자의 해킹경로를 분석하여 해커의 출발지를 찾아내는데 주력하여 우회경로로 이용된 시스템의 해킹 피해 유무도 점검하는 등의 피해 확산방지 노력도 진행 중에 있다[5]. 다음 <표 1>은 정보보호센터로 접수된 해킹사고 현황을 보여주고 있는데, 작

† 정 회 원 : 한국정보보호센터 팀장
†† 정 회 원 : 홍익대학교 전자계산학과 교수
논문접수 : 1999년 10월 15일, 심사완료 : 1999년 11월 4일

년에 비하여 급격한 증가추세에 있음을 알 수 있다.

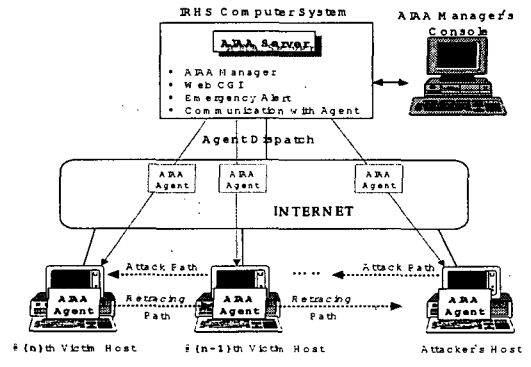
〈표 1〉 국내 인지된 해킹사고 현황

구 분	'97	'98	'99.8	계	%
대 학(ac.kr)	32	80	129	241	48
기 업(co.kr)	25	69	122	216	43
비영리(or.kr)	2	3	15	20	4
연구소(re.kr)	3	4	2	9	2
기 타(지역)	2	2	13	17	3
합 계	64	158	281	503	100

CERTCC-KR에 접수되는 해킹사고의 급격한 증가는 해킹사고의 분석 처리 등 대응에 들어가는 인력 소요가 계속 늘어나야 함을 말한다. 현재 접수된 해킹사고는 대부분 피해기관이 자발적인 분석을 하지 못하고 있어 CERTCC-KR요원이 원격지에서 분석을 대행하고 있다. 접수된 해킹사고에 대하여 피해시스템 분석 및 해당 기관 피해 분석에 최소 4~5시간이 소요되고 있으며 해킹사고의 역추적과 연락 등을 통하여 지원이 종료되기 까지는 약 1주일이 소요되고 있다[4].

이렇게 늘어나는 해킹사고에 비하여 대응인력은 늘지 않고 있어 해킹피해시스템에 대한 분석을 인간의 수동적인 분석 보다 자동으로 분석할 수 있는 해킹피해시스템 자동 분석 기술이 필요로 하게 되었다. 이러한 기술은 해킹 피해시스템에서 침입자가 남긴 흔적을 로그를 분석하는 기능과 침입자를 분석하기 위한 침입탐지 및 추적 모듈이 필요로 한다[4].

다음 (그림 1)은 자동 분석시스템인 해킹피해시스템 자동분석에이전트(Autonomous Incidentr Analysis Agent)를 이용한 침입자 역추적 개념도를 보이고 있다.



(그림 1) AIAA를 이용한 침입자 역추적 기본 개념

이러한 개념을 바탕으로 요구사항 분석과 시스템의 설계, 구현 및 결과를 보이고자 한다.

2. 요구사항 분석

AIAA은 기존의 수작업을 통한 해킹피해시스템 분석과 침입자 추적하는 어려움을 없애 자동화된 방법을 이용한다. 신속하고 정확한 침해사고 대응업무 지원과 근본적인 침해사고 방지를 위한 불법침입자 추적을 위해 침입자 흔적을 알아낼 수 있는 로그정보 분석 기능과 불법침입 발견 즉시 추적할 수 있도록 침입탐지 기능과 침입사실 알람기능을 동시에 제공해야 할 것이다.

로그정보분석기능은 syslog, messages, web-log 등의 시스템과 응용프로그램의 로그, .cshrc, .rlogin, /etc/hosts.equiv 등의 시스템 파일 분석 그리고 트로이목마프로그램 및 뒷문(backdoor) 프로그램 등 해킹프로그램을 분석하여 침입흔적을 찾는 기능으로 관리자 및 공격자 관점에서 분석할 필요가 있다.

- 시스템관리자 관점에서의 분석

침해사고 피해 시스템의 여러 로그정보로 침입자 확인, 침입 방법, 침입자의 출발 호스트 등의 정보를 확인할 수 있으며 침입자들이 이용하는 웹서버, Imapd 등의 서버취약점을 이용한 침입시도 서버의 로그를 분석하여 알아낸다.

- 침입자 관점에서의 분석

지능적인 침입자의 경우 로그를 삭제하는 경우가 많으므로 공격자가 침입하여 어떤 식의 시나리오로 행동할 것임을 미리 분석하여 침입자가 흔히 이용하는 트로이목마 시스템프로그램, 뒷문 디렉토리나 프로그램 등과 침입자가 설치하는 각종 mscan 등 각종 공격도구 등 로그 파일에서는 알아낼 수 없는 여러 침입흔적을 분석한다.

침입자의 재차침입을 즉각적으로 알아내기 위하여 침입자 시나리오에 기반을 둔 침입탐지규칙을 적용, 침입탐지와 즉각적인 경고(Alerting and Alarming)를 한다. 이때 경고는 전자우편, 디지털 이동통신 메시지 서비스 등이 포함되며 침입 수준과 위험성 정도에 따라 경고하거나 필요시 접속을 강제적으로 끊어버리게 된다.

결국 AIAA를 이용한 침입자 추적에는

- 침입자 흔적 분석 : 로그 및 침입도구 분석
- 침입탐지, 감시 : 침입자의 활동 감시, 경보
- 침입자 역추적 : 반자동 역추적 정보 수집

등이 요구된다.

3. 관련 연구

3.1 침입탐지 기술

침입탐지기술은 AIAA에서 해킹피해시스템 분석시 재차 침입해오는 침입자를 탐지하여 역추적 등에 이용하고 침입자를 확인하는데 필요한 기술이다. 여기에서는 지금까지 침입탐지기술로서 알려진 여러 기법들을 분석하였다.

3.1.1 오용탐지기술(Misuse)

- 전문가시스템

전문가시스템은 공격에 관한 규칙집합을 가지고 있어 감사 이벤트가 전문가시스템 내에서 의미를 가지는 사실로 변환이 되고, 추론엔진은 이 규칙들과 사실을 기반으로 침입을 판단한다. 전문가시스템기법은 감사자료에 의미를 부여함으로서 감사자료의 추상화 정도를 증가시킨다[12]. 전문가시스템에서 규칙기반언어(rule-based language)는 공격에 관한 전문가의 지식을 모델링하기 위한 자연스러운 도구이다. 이 접근방식은 알려진 취약점을 이용하려는 시도들에 관한 증거를 찾기위해 감사 자료를 체계적으로 탐색할 수 있도록 한다. 또한 보안정책이 적절히 적용되고 있는지 검증하는데 사용될 수도 있다. 하지만 전문가시스템의 전체적 성능은 아직 낮은 정도이며 늦은 처리속도로 인해 프로토타입에서만 사용되며 상용 제품들은 보다 효율적인 접근방식을 취한다. 대표적인 시스템으로는 RUSSEL이라는 규칙기반언어를 사용한 ASAX(Advanced Security audit trail Analysis on uniX)[13] 등이 있다.

- 흔적 분석(Signature Analysis)

흔적분석은 전문가시스템과 동일한 방식으로 지식을 획득하지만 지식을 사용하는 방식이 다르다. 공격에 대한 의미적 기술은 감사 자료에서 곧바로 검색이 가능한 형태의 정보로 변경된다[12]. 예를 들면, 공격 시나리오는 공격시 생성되는 감사이벤트 시퀀스로 변경되거나 시스템에 의해 생성된 감사자료에서 탐색할 수 있는 데이터 패턴으로 변경된다. 이 기법은 공격에 관한 기술이 저수준에서 이루어진다. 흔적분석기법은 아주 효율적인 구현이 가능하므로 상업적인 침입탐지 제품에 응용되고 있다. 이 방식의 주약점은 다른 지식기반 접근방법과 마찬가지로 새로 발견된 취약점에 대해 자주 갱신을 해주어야 한다는 것이다.

- 페트리넷(Petri-net)

페트리넷은 '95년 퍼듀대학에서 기존 패턴 매칭 방법을 개선한 것으로 침입에 관한 시그너처를 표현하기 위해서 칼라페트리넷(CPN)을 사용하였다[14]. CPN은 일반성, 개념적 단순성, 그래프 표현성 등의 장점을 가지고 있다. 시스템 관리자는 공격의 시그너처를 작성하고 IDIOT 시스템에 통합할 수 있다. CPN의 일반성으로 아주 복합한 시그너처도 쉽게 작성할 수 있다. 그러나 복잡한 시그너처를 감사자료와 비교하는 작업은 상당히 많은 계산비용을 요구한다. 이를 구현한 시스템으로는 '96년 COAST에서 개발한 IDIOT(Inrusion Detection System In Our Time)[15]가 있다.

- 상태전이분석

상태전이분석은 '92년 UCSB에서 제안한 것으로 개념상으로는 모델기반 추론과 동일하다. 이 기법은 공격을 목표와 상태 전이의 집합으로 기술하며 상태전이 다이어그램으로 표현한 것으로 일반적으로 STAT라 부른다[16]. STAT 기반 침입탐지 방식이 처음 설계되고 도구로 개발된 것이 '92년 개발한 UCSB에서 개발한 USTAT[17]이며 멀티 호스트로 확장한 것이 NSTAT이다. 현재 DARPA 프로젝트로 수행 중인 네트워크 기반 침입탐지시스템이 NetSTAT[18]이다. STAT는 일부 상용 제품에서도 사용되고 있다.

- 신경망

신경망은 타당한 방법으로 새로운 입력-출력쌍을 얻기위해 두 집합의 정보간 관련성을 학습하고 일반화하는데 사용되는 알고리즘 기법이다. 신경망은 이론적으로 지식기반 침입탐지 방식에서 공격을 학습하고 감사 스트림에서 탐색하는데 사용될 수 있다. 입출력간의 관계를 알 수 있는 믿을만한 방법이 없으므로 신경망은 공격을 추론하거나 설명할 수 없어 주로 비정상행위 탐지기법으로 많이 연구되었으나 최근에는 지식기반 프로파일을 구성하여 오용탐지 기법으로도 사용된다.

3.1.2 비정상행위 침입탐지(Anomaly Detection)

● 통계적 기법

가장 널리 사용되는 방법으로서 사용자나 시스템 행동은 시간에 따라 샘플링된 여러 가지 변수들에 의해 측정된다. 각 세션의 로그인, 로그아웃시간, 자원 지속성, 세션당 소비된 프로세서-메모리-디스크양 등이 변수의 예가 될 수 있다. 많은 상용시스템에서 비정상행위 탐지를 위하여 도입하는 기법이 통계적 기법이다. 대부분 시스템들은 변수들의 평균을 유지하고 있으면서 변수의 표준편차에 기반해서 임계값을 넘어섰는지를 검사하게 된다. 그러나 이러한 방식은 자료를 충실히 표현하기에는 너무 단순한 문제가 있었다[12]. 보다 발전된 형태로 장기 및 단기간 사용자 활동 프로파일을 비교하는 방식이 개발되는데, 사용자의 행동이 바뀜에 프로파일들은 따라 정기적으로 갱신되는 모형은 SRI에서 제안한 방식으로 시스템으로는 NIDES[20], ENERALD[19] 등이 있다.

● 전문가시스템

전문가 시스템은 행동기반 침입탐지에서도 이용된다. 주어진 기간동안의 사용자 활동 기록에 기반해서 사용자의 행동을 통계적으로 기술하는 규칙 집합을 구축한다. 현재 활동을 이 규칙들과 비교하여 비정상행위를 탐지하게 되는 것이다. 새로운 사용패턴을 적응시키기 위해 주기적으로 규칙베이스를 갱신하게 되는데, AT&T의 ComputerWatch는 적절한 사용 정책을 기술하는 규칙 집합에 기반하여 사용자들의 행동을 검사하여 타당한 패턴에 맞지 않는 행동을 찾아낸다. 전문가시스템 접근방식은 정책기반 사용 프로파일에는 유용하지만 많은 양의 감사정보를 처리하는데는 통계적인 접근방식보다 덜 효율적이다[12].

● 신경망

신경망은 이론적으로 오용탐지에 적합하나 통계적 기법과 유사하게 비정상행위 탐지에 많이 사용되었다. 통계적 기법에 비해 신경망을 사용하는 경우의 잇점은 변수들간의 비선형적 관계를 표현하는 간단한 방법을 가지는 것과 신경망을 자동적으로 학습하는데 있다. 그러나 신경망은 여전히 많은 계산을 요구하기 때문에 침입탐지 분야에서는 널리 사용되고 있지는 않으며 개발된 시스템으로 SecureNet 등이 있다[12].

● 컴퓨터 면역학

컴퓨터 면역학은 적절한 행위를 나타내는 참조 감사들의 집합을 수집한 후 정상 시퀀스를 나타내는 참조 테이블과 비교하여 일치하는 않는 시퀀스만을 추출하여 비정상행위 프로파일을 구성하고 발생한 이벤트가 프로파일과 일치하면 비정상행위로 판정한다. 이 방법은 바이러스 탐지를 위하여 Forrest 등이 제안한 방식[21]으로 현재 네트워크 서비스의 정상행위를 모델링에 사용되고 있다.

● 데이터마이닝

데이터마이닝은 데이터베이스 분야에서 활용해 오던 분석 및 예측 기법 중의 하나로 수집된 많은 데이터 중에서 중요한 특징을 결정하기 위하여 사용되었다. 이 방식은 Columbia 대학의 JAM(Java Agents for Meta-learning)[22]에서 비정상행위 탐지 기법으로 사용하고 있다. JAM은 데이터 마이닝 응용 프로그램을 평가하는 데에 있어 일반적 접근 방법인 meta-learning을 채용하는, 분산환경에서의 이식성과 확장성을 제공하는 에이전트 기반 데이터 마이닝 시스템이다. '98년 MIT Lincoln Lab.에서 평가한 자료[23]에 의하면 STAT나 통계적 기법보다 성능이 뛰어난 것으로 보고되고 있다.

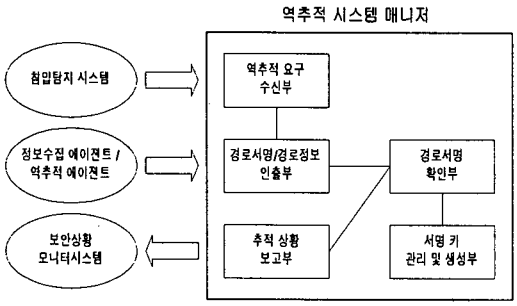
● HMM(Hidden Markov Model)

HMM은 음성인식분야나 DNA 시퀀스 모델링분야에서 광범위하게 사용되는 확률적인 모델기법으로서 생성메커니즘을 알 수 없는 이벤트들을 모델링하고 평가하는 강력한 도구이다. 이벤트 시퀀스의 시스템 호출을 하나씩 읽으면서 HMM에서 해당 시스템 호출을 보려면 어떤 전이와 출력이 필요한지를 추적한다. 침입 이벤트시퀀스는 하나 이상의 드문 상태전이와 출력을 가질 것이다. 따라서 정상행위를 기반으로 정해진 임계값보다 낮은 상태전이나 출력을 요구하는 시스템 호출을 검사함으로써 침입을 탐지한다. HMM으로 구현된 시스템은 없지만 New Mexico 대학에서의 논문[24]에는 통계적 기법이나 데이터 마이닝보다 성능이 뛰어난 것으로 보고 있다.

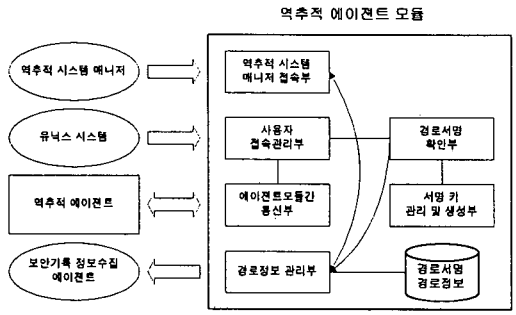
3.2 침입자역추적 기술

역추적 기술은 CIS(Caller Identification System)[6]과 RFC1413에서 정의된 신원확인서버[28]가 대표적이다. CIS는 TCPWrapper의 필터링 개념을 도입하여 어

떤 시스템에 로그인하는 이용자는 자신의 그 이전에 거쳐왔던 시스템과 로그인ID등의 정보를 주어야만 로그인할 수 있는 프로토콜을 제안한 것으로 최종 시스템에서는 어떤 이용자가 거쳐온 모든 시스템의 기록정보를 확인할 수 있다. 신원확인서버는 CIS와 유사한 개념으로서 신원확인을 위한 서버가 있어 사용자가 거쳐온 시스템의 모든 신원정보를 확인할 수 있는 것이다. CIS와 신원확인서버에 의한 역추적은 국내에서 일부 연구가 시도되었으나 실용적이지 못한 관계로 더 이상 연구가 진행되지 못하였다.



(그림 2) 역추적 시스템 매니저



(그림 3) 역추적 에이전트

실제 각 시스템이 가진 로그기록을 바탕으로 자동으로 이루어지지 않은 침입자 역추적에 관한 연구가 최근 시도되었다[1]. 시스템은 효율적인 역추적을 위하여 역추적 시스템 매니저 모듈과 역추적 에이전트로 구성되며, 이들은 다른 기능 모듈들과 함께 각각 매니저 시스템과 에이전트 시스템을 구성한다. 다음 (그림 2)와 (그림 3)은 역추적매니저와 에이전트의 기능을 블록다이어그램으로 보이고 있다. 역추적 시스템 매니저는 설계된 역추적 시스템 매니저 모듈은 역추적 요구 수신부, 경로 서명/경로 정보 인출부, 추적 상황 보고부, 경로 서명 확인부, 그리고 서명키 관리 및 생성부로 구성되어 있다. 역추적 에이전트 모듈은 사용자 접속관리부, 에이전트 모듈간 통신부, 경로 정보 관리부, 경로 서명 확인부, 서명키 관리 및 생성부, 그리고 역추적 시스템 매니저 접속부로 구성되며, 경로 서명 및 경로 정보를 저장하기 위한 안전한 데이터베이스를 갖는다.

4. 시스템 설계

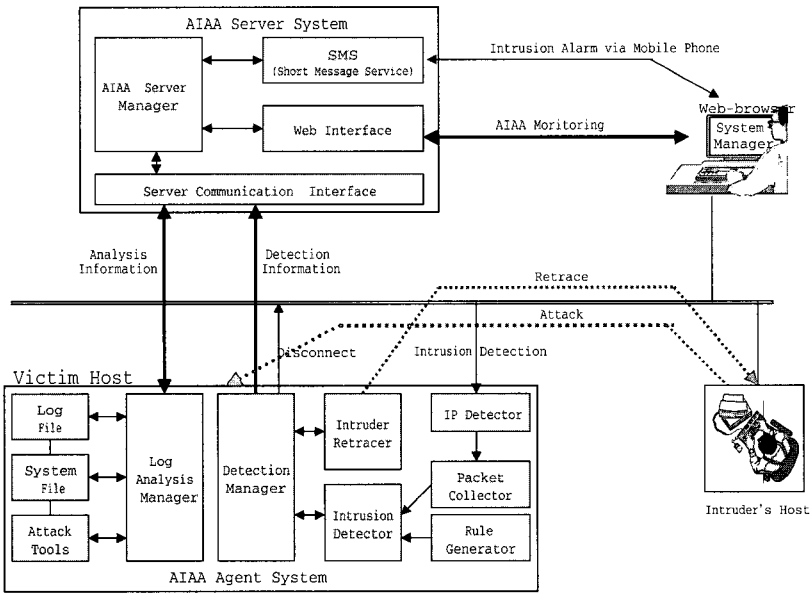
4.1 개요

AIAA은 해킹피해시스템 로그 분석정보, 침입탐지 및 추적 정보 그리고 침입시 AIAA 관리자에게 침입사실을 경고하는 AIAA 서버와 피해시스템에 탑재되어 피해사항 분석, 침입탐지 및 추적관련 기능을 수행하는 AIAA 에이젼트로 구성된다.

AIAA는 시스템 피해분석과 침입탐지가 동시에 수행된다. 만약 이미 의심스러운 이용자로 판명된 침입자가 시스템에 접근하면, AIAA에이젼트의 IP 탐지기(IPD : Detector)에서 침입자의 발신자 IP 주소를 파악하고 PC(Packet Collector)에서 IP 패킷을 수집한다. 침입탐지모듈(ID : Intrusion Detector)에서는 미리 침입탐지 규칙 생성기에서 미리 만들어진 규칙에 의해 침입을 판정하고 침입탐지관리자(DM : Detection Manager)에게 침입관련 정보가 전달된다. 이 정보는 서버통신인터페이스(SCI : Server Communication Interface)를 통하여 AIAA 서버 관리자의 관리자에게 침입사실을 경보하고 관련상황을 웹으로도 전달한다. 관리자는 침입탐지 경보나 이미 해킹 피해를 당한 시스템에 대한 분석을 위해 로그분석, 비정상상적인 파일이나 의심스러운 파일 등을 분석한다. 특히 로그분석관리기(LAM : Log Analysis Manager)는 관리자의 지시사항을 받아 피해시스템의 로그를 분석한다.

4.2 AIAA 서버

AIAA 서버는 AIAA 에이젼트와 대화하면서 분석상황과 침입자탐지 및 추적상황을 종합적으로 모니터링 관리하는 역할을 한다. AIAA 서버는 모니터링하고 에이젼트에 지시하는 역할을 담당하는 서버관리자와 관리자



(그림 4) AIAA 구성 블럭다이어그램

에게 침입경보를 디지틀이동전화로 통보하는 SMS(Short Message Service), 관리자가 종합상황정보를 직접 관리할 수 있도록 해주는 웹인터페이스(Web Interface)로 구성되어 있다. 관리자는 웹인터페이스를 통하여 에이전트관리, 침입탐지관련 구성, 로그분석에 필요한 각종 대상 파일의 정의, 침입자 역추적 구성 등의 기능을 하게 된다.

4.3 AIAA 에이전트

에이전트는 피해시스템의 로그를 분석하는 로그분석관리자(LAM)와 침입탐지 및 추적 기능을 수행하는 침입탐지관리자(DM)으로 구성된다. LAM은 각 에이전트들의 시스템 로그 파일을 검색하고 관리하는 기능을 제공한다. 로그파일검색모듈에서는 syslog, messages, wtmp, utmp, web log, ftp log, 사용자 지정 로그 등을 검색 및 관리하다. 시스템파일모듈은 .cshrc, .rlogin, .rhost, /etc/hosts.equiv 등의 시스템과 사용자 주요 파일을 검색 및 관리하는 기능을 제공하고, 최근에 생성, 변경 및 접근된 파일 검색도 한다. 수상한 파일이 발견되면 시스템관리자는 파일내용 조사를 통해 침입자를 추적한다. 공격프로그램모듈은 해킹프로그램이나 백도어 프로그램 목록DB를 이용하여 침입자가 시스템에 관련프로그램을 설치했을 경우 이를 검색한다.

5. AIAA의 구현과 시험

5.1 AIAA의 구현

5.1.1 구현 환경

AIAA서버 시스템과 에이전트시스템은 Solaris 2.5.5 환경에서 개발하였고, SunOS, Linux에서도 설치·운영할 수 있다. 그리고 GUI를 제외한 모든 모듈은 C언어로 개발되었고, 웹기반 GUI는 CGI와 html을 기본으로, 동적 메뉴화면은 JDK1,1,5기반의 Java Applet으로 구현하였다.

5.1.2 서버의 구현

서버관리자모듈은 에이전트시스템에 설치되는 침입탐지정보를 관리하는 기능과 피해시스템에서 분석된 로그파일, 주요 시스템 파일, 공격도구정보를 관리하는 기능을 담당하며, AIAA 전체 시스템을 통합 및 관리하는 역할을 한다. SMS(Short Message Service) 모듈은 에이전트시스템에서 침입규칙에 위반되는 불법시도가 발견되었을 때 관리자에게 경고 메시지를 전송해주는 기능을 수행한다. 실제 시스템 구현은 이동통신 사업자가 제공하는 SMS서비스를 이용하였다. 011(Cellular Phone)경우 SMTP를 이용하고 나머지는 WEB CGI의

GET/POST 방법을 이용하여 구현하였다. Web 인터페이스모듈은 Java 클래스파일을 이용한 동적메뉴 CGI와 로그분석시스템을 위한 검색선택 폼 html로 구현했고, 에이전트와의 통신을 위해 데이타를 웹상에서 주고받는 파싱CGI로 구현하였다. 웹GUI기본메뉴는 AIAA 에이져트시스템의 설치 및 설치현황을 볼 수 있는 역추적 시스템관리 메뉴, 불법접근 IP, 침입패턴 탐지규칙과 정보를 볼 수 있는 접속로그 검색메뉴, 피해시스템의 피해파일 정보열람과 분석상황을 볼 수 있는 파일검색메뉴, 피해시스템의 syslog, messages 등의 시스템로그 정보열람 및 분석상황을 볼 수 있는 시스템 로그 검색메뉴, 불법침입자를 역추적에 관련된 정보열람 및 분석을 위한 역추적메뉴, 피해시스템 분석방법 등의 AIAA관련 도움을 위한 보안자료실 메뉴를 가지고 있다. 서버통신모듈은 서버관리자모듈과 에이전트시스템의 피해분석 정보, 침입탐지 및 추적관련 데이터들의 통신을 관리하는 기능을 수행한다.

5.1.3 에이전트 구현

LAM모듈은 서버시스템이 로그 분석요청을 하였을 때 피해시스템의 로그 파일, 주요 시스템 파일, 공격도구 등의 정보 분석결과를 서버시스템에 전송한다. 공격도구 분석은 현재까지 알려진 해킹 & 백도어 프로그램 목록DB를 이용하여 분석하고, 로그파일과 시스템 파일 분석결과와 더불어 효과적인 분석과정을 수행할 수 있다. 주요 해킹 & 백도어 프로그램 등의 공격도구 DB목록은 다음과 같다.

killinetd imap imap2 imapver netcat brute.sh z0ne sniffer rootkit chfn chsh inetd phfscan phpscan nmap chkexploit eipscan lsp imapvun imapd_scan.sh mscan sirc ipw ircbnc icat ts2 mendax boink bonk bonk2 fear smurf ssping tear2 eardrop wipe

DM모듈은 패킷캡처라이브러리(Packet Capture Library)를 이용하여 침입자가 에이전트에 접속하고 수행하는 모든 Packet 정보를 잡아, 접속탐지와 패턴탐지 모듈에서 분석하여 규칙생성기에서 설정한 탐지규칙에 위반되는 결과를 Server시스템에 전달하는 역활을 수행한다. 또한 침입자 탐지가 되면 침입자역추적모듈을 이용하여 불법접속을 끊거나, 해당 피해시스템의 에이전트 시스템에서 직접적인 추적 또는 다른 AIAA 에이전트시스템을 통해 침입자를 추적할 수 있도록 구현하였다.

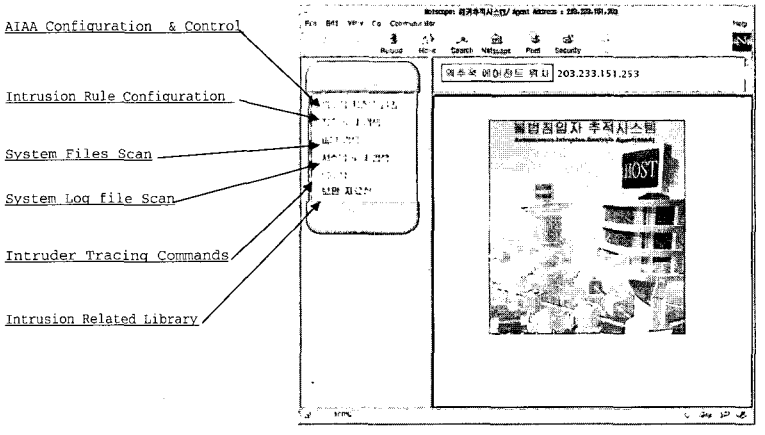
5.1.4 주메뉴의 구성

AIAA의 주메뉴는 피해시스템 로그정보 분석, 침입탐지 및 추적기능 복합적으로 수행할 수 있도록 구현하였다. (그림 5)는 AIAA의 웹 주메뉴로 역추적시스템 관리메뉴, 접속로그 검색 메뉴, 파일 검색 메뉴, 시스템 로그 검색 메뉴, 역추적 메뉴 및 보안 자료실 메뉴로 구성되어 있다.

5.2 AIAA 시험 분석

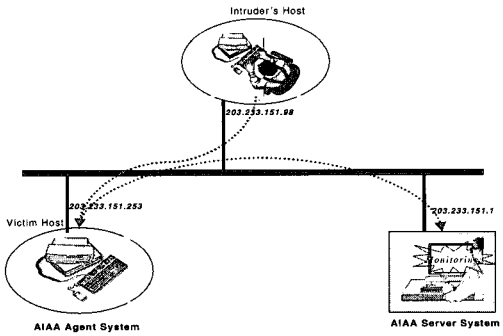
5.2.1 AIAA 시험 환경

AIAA의 시험환경은 (그림 6)과 같이 서버시스템과 에이전트 시스템을 각각 Solaris 2.5.5가 탑재된 SUN



(그림 5) AIAA의 초기 화면 및 메뉴

시스템에 설치하고, 공격자시스템서 목표시스템으로 해킹공격을 하면 AIAA 에이전트시스템의 침입탐지기에서 침입상황을 탐지하여 AIAA 서버시스템에 침입사실을 통보한다. 동시 AIAA 서버시스템에서는 해킹피해시스템를 피해분석을 진행하는 환경을 구축하여 시험하였다.



(그림 6) AIAA 시험 환경

5.2.2 시스템의 침입흔적 분석

피해시스템을 분석하기 위하여 먼저 주요 시스템 파일 점검을 통해 불법적인 파일 생성이나 접근을 분석한다.

다음 분석 화면은 rlogin, rsh의 remote 접속 명령어를 이용하여 인증 과정없이 시스템에 접속할 수 있는 "+ +"을 포함하는 .rhosts 파일을 검색하는 화면이다. 검색 결과는 /usr1/staff/leesy라는 사용자가 홈디렉토리에 불법적인 .rhosts파일을 포함하고 있다는 것을 보여준다.

위의 분석결과를 이용하여 /usr1/staff/leesy의 디렉토리에서 3일 이내에 새로 생성된 파일들을 검색한 결과, 수상한 .hacking, Temp등의 파일이 생성된 것을 알 수 있다.

다음 화면은 불법 침입자로 의심되는 leesy에 대한 접속 로그 정보를 분석하기 위하여 wtmpx log파일을 검색한 결과 많은 접속이 이루어졌다는 것을 보여준다. 또한 검색 결과에서 불법침입자가 접근한 불법 호스트는 law-k.kisa.or.kr나 sun450.kisa.or.kr로 kisa.or.kr 도메인에서 접근한 것을 알 수 있다.

5.2.3 침입탐지 및 역추적 시험분석

AIAA 에이전트는 의심스러운 접속이나 불법행위를 시도하는 사용자를 탐지하기 위하여 침입패턴을 미리 지정하고 침입의 위험성 정도에 따라 경보방법을 다음 사례와 같이 결정하며 침입패턴에 따라 수준과 경보 메시지 내용을 지정할 수 있다.

다음 (그림 7)은 침입탐지시스템의 탐지규칙 설정화면과 탐지된 결과를 보여주고 있다.

불법침입자가 시스템 분석을 통해 알 수 있었던 것처럼 미리 생성해둔 .rhosts 파일을 이용하여 rlogin을 이용하여 원격 접속해 showmount-e 명령어를 수행한 것을 침입탐지 시스템이 탐지한 결과이다. rlogin에 의한 불법적인 접근은 탐지 규칙 설정에서의 Alert Level이 2로 설정되어 있으므로 Screen Display와 함께 시스템 관리자에게 SMS나 Pager를 이용한 경보로 보내게 된

```
# System Intrusion Detection Rule
# Service          Token                    AlertLevel
# Alert Level 3 : Screen Display
# Alert Level 2 : Screen Display , SMS , Pager
# Alert Level 1 : Screen Display , SMS , Pager , Disconnect

TELNET  rlogin,-l,-froot                    2       "Somebody Executed rlogin -froot "
HTTP            /cgi-bin/test-cgi?          1       "/cgi-bin/test-cgi Attack"
TELNET  mount,nfs               1           "Somebody mounted NFS filesystem"
RLOGIN  rlogin,-l,-froot                    2       "Somebody Executed rlogin -froot RL"
RLOGIN  mount,nfs                           1       "Somebody mounted NFS filesystem"
FTP             ~root                       1       "Somebody executed cd ~root"
FTP             site,exec                   2       "Somebody Executed site exec"
SMTP            |                           2       "Somebody executed '|' attack"
SMTP            decode                      2       "Somebody executed 'decode' attack"
TELNET  showmount,-e        2               "Somebody Executed 'showmount -e'"
RLOGIN  showmount,-e        2               "Somebody Executed 'showmount -e'"
```

(그림 7) 침입탐지 규칙과 경보 형태

다. 관리자는 시스템 분석을 통하여 불법침입자와 호스트에 대한 충분한 정보를 파악한 후 traceroute나 whois를 이용하여 역추적을 할 수 있다. 또한 다른 AIAA 에이전트 시스템을 이용한 역추적을 시도할 수도 있을 것이다.

6. 결론 및 향후과제

AIAA는 해킹피해시스템의 해킹흔적과 피해상황을 분석하고 침입자의 경로를 파악하여 침입자를 역추적할 수 있는 여러 가지 도구를 지원함으로서 해킹사고에 종합적으로 대응할 수 있도록 하는 도구이다.

이를 위하여 해킹흔적 분석을 위한 로그분석 모듈, 해커들의 도구를 찾아내는 모듈을 기본적으로 구현하였으며, 추후 침입하는 침입자를 탐지하는 소규모 침입탐지시스템과 침입자 역추적용 도구들을 구현하였다.

이 시스템은 해킹사고시 실제 적용 활용하고 있으며 CERTCC-KR 해킹사고 담당 직원들의 인력과 시간을 덜어주고 있다. 추후에는 해커들의 침입시 면밀하게 감시하면서 실제 시스템을 보호할 수 있는 가상시스템과의 연계를 연구하고자 한다.

참 고 문 헌

[1] 한국정보보호센터, "정보통신시스템 침해사고방지 기술 개발", 1999. 1.

[2] 한국정보보호센터, "'98 해킹 및 대응 현황", 1998. 12.

[3] 한국정보보호센터, "'98 CERTCC-KR 연보", 1999. 3

[4] 신 훈, 정윤종, 임채호, 김종섭, "해킹피해시스템 분석과 수사기법에 관한 연구", WISC, 1998.

[5] 이현우, 이상엽,정현철, 정윤종,임채호, "대규모 네트워크취약점 검색공격 패턴분석 및 탐지도구 개발", WISC '99, '99. 9.

[6] H. T. Jung, et. al., "Caller Identification System in the Internet Environment," Proceedings of the USENIX Security Symposium IV, 1993.

[7] Sangyoub Lee, Hyuncheol Jeong, Jeonghyun Park, Chaeho Lim, "Intruder Retracing Using Autonomous Incident Analysis Agent," FIRST Conference, 1999. 6.

[8] Taekyoung Kwon, Myeongho Kang, Jooseok Song, "An Adaptable and Reliable Authentication Protocol for Communication Networks," IEEE INFOCOM '97, Kobe, Japan.

[9] Simson Garfinkel & Gene Spafford, "Practical UNIX & Internet Security," 2nd Ed, O'Reilly & Associates, Inc. 1996.

[10] W. Richard Stevens, "Advanced Programming in the UNIX Enviroment," Addison Wesley, pp.415-425, 1992.

[11] Larry J. Hughes, Jr. "Actually Useful Internet Security Techniques," new riders, 1995.

[12] H. Debar, M. Dacier, and A. Wespi, Towards a Taxonomy of Intrusion Detection Systems, Research Report RZ 3030, IBM Research, June 1998.

[13] N. Habra, B. L. Charlier, A. Mounji, I. Mathieu, "ASAX : Software Architecture and Rule-Based Language for Universal Audit Trail Analysis," Proceedings of ESORICS '92, European Symposium on Resarch in Computer Security, November 23-25 Toulouse, Springer-Verlag 1992.

[14] Sandeep Kumar, Classification and Detection of Computer Intrusions, Department of Computer Sciences, Purdue University, PhD Dissertation, Coast TR 95-08, 1995.

[15] Mark Crosbie, et. al., IDIOT Users Guide, Department of Computer Sciences, Purdue University, CSD-TR-96-050, Coast TR 96-04, 1996.

[16] P. A. Porras, STAT-A state transition analysis tool for intrusion detection, M.S. thesis, Computer Science Dep., University of California Santa Barbara, June 1992.

[17] K. Ilgun, USTAT : A real-time intrusion detection system for UNIX, M.S. thesis, Computer Science Dep., University of California Santa Barbara, July 1992.

[18] R. A. Kemmerer, "NSTAT : A Model-based Real-time Network Intrusion Detection System," Computer Science Dep., University of California Santa Barbara, Technical Report TRCS97-18, November 1997.

[19] P. A. Porras, P. G. Neumann, "EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances," 1997 Na- tional Information Systems

Security Conference, 1997.

[20] Anderson, Lunt, Javits, Tamaru, Valdes, Detecting Unusual Program Behavior Using the Statistical Components of NIDES, Computer Science Lab., SRI International, SRI-CSL-95-06, 1995.

[21] Computer immunology S. Forrest, S. Hof-meyr, and A. Somayaji. Communications of the ACM, Vol.40, No.10, pp.88-96, 1997.

[22] W. Lee, S.J. Stolfo, and K. Mok, "A Data Mining Framework for Building Intrusion Detection Models," 1999 IEEE Symposium on Security and Privacy, 1999.

[23] Results of DARPA 1998 Offline Intrusion Detection Evaluation, http://ideval.ll.mit. edu/

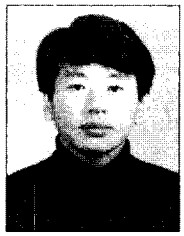
[24] C. Warrender, S. Forrest, B. Pearlmutter, "Detecting Intrusions Using System Calls : Alternative Data Models," 1999 IEEE Symposium on Security and Privacy, 9-12 May 1999.

[25] David A. Curry, "UNIX System Security," Addison Wesley, pp36-80, 1992.

[26] W. Venema, "TCP Wrapper : Network Monitoring, access control, and booby traps," Proceedings of the USENIX Security Symposium III, 1992.

[27] Bruce Schneier, "Applied Cryptography," 2nd Ed., Wiley, pp39-40, 1996.

[28] RFC 1413 : "Identification Server".



임 채 호

e-mail : chlim@kisa.or.kr

1986년 2월 홍익대학교 컴퓨터공학과(학사)

1991년 8월 건국대학교 전자계산학과(석사)

1995년 2월 홍익대학교 전자계산학과(박사수료)

1985년~1992년 시스템공학연구소 연구원

1992년~1994년 대전실업전문대학 전산과 교수

1995년 시스템공학연구소 초빙연구원

1996년~현재 한국정보보호센터 팀장

원 유 헌

e-mail : woh@cs.hongik.ac.kr

1972년 2월 성균관대 수학과 졸업(학사)

1975년 8월 한국과학기술원 전자계산학과(석사)

1985년 8월 고려대(이학박사)

1975년~1976년 한국과학기술연구소 연구원

1986년~1987년 R.P.I 객원 교수

1976년~현재 홍익대학교 전자계산학과 교수

관심분야 : 컴파일러, 프로그래밍 언어디자인, 소프트웨어 공학, 분산언어, 객체 지향언어, 하드웨어 기술언어, 시스템 및 네트워크 보안, 분산시스템 보안 등