해킹기법을 응용한 침입자역추적 시스템

채연주**U 서진철** 임채호* 원유헌**
**홍익대학교 컴퓨터공학과 *한국정보보호센터
**{yjchae, jcseo, won}@cs.hongik.ac.kr *chlim@kisa.or.kr

Intruder Tracing System Using Hacking Methods

Youn-Ju Chae**U Jin-Cheol Seo** Chae-Ho Lim* Yoo-Hun Won**
**Dept. of Computer Engineering, Honglk University
*Korea Information Security Agency

요 약

인터넷에서 해커 등 침입자를 추적하기 위한 방안들이 연구되고 있으나 아직 실용적인 연구성과가 거의 드문 실정이다. 지금까지는 침해사고대응팀(CERT)간의 협력과 상호 정보교류를 통한 대응체계를 통하여 이루어지고 있으나 실제 역추적으로서는 효과적인 방법이 아니며, 에이전트를 이용한 분석방법(AIAA)와 같은 경우도 에이전트의 수동적인 이동이 전제되어야 하는 것이다. 최근 해킹공격에 대한 적극적인 대응 방안으로 역공격 등의 적극적인 방법들이 고려되고 자신의 시스템에 대한 보호방법의 하나로서 받아들여지고 있는 경향이 있으므로 이러한 역공격 방법을 추적시스템에 접목하여 개량된 AIAA 모델로서 침입자 역추적방법을 설계하고 구현하였다. 여기에는 침입자 역공격 모듈과 침입자 미행모듈, AIAA 파견모듈등을 구현하여 자동적인 침입자 추적을 실현하였다.

I. 서론

일반적으로 공격자는 여러 시스템을 경유하여 공격 대상 시스템에 침입하게 되는데, 현존하는 침입자 추적 방법은 공격자의 공격경로를 역으로 한 단계씩 추적하게 된다. 그리고 각 단계에서 해당 시스템 관리자의 도움을 받아 시스템을 분석하고 조사하는 과정을 거치게 되어 실시간 역추적이 불가능하며, 많은 시간이 소요된다.

본 논문에서는 보다 적극적인 방법을 사용한 침입자 역추적 시스템을 제안한다. 기존의 해킹피해 시스템을 자동으로 분석해 주는 AIAA(Autonomus Intrusion Analysis Agent)를 보다 개선하고 자동 역공격 기술과 에이전트 기술을 이용하여 실시간으로 침입자의 경로를 역추적 하는 시스템을 구현한다.

해킹피해 시스템 분석 기술은 실세계의 범죄를 조사하는데 사용하는 법의학(Forensic) 개념을 해킹피해 시스템 분석 방법에 도입하여 보다 체계적이 분석방법론을 제시하고 피해시스템에서 자동 또는 반자동으로 침입자나 해킹혼적 그리고 재침입을 위한 백도어 등을 추적하게 된다. 그리고 모니터링 기술을 통하여 재 침입하는 침입자를 탐지하게 된다. 자동 역공격 기술은 모니터링을 통하여 탐지된 공격자 시스템을 자동으로 공격하여 분석 에이전트를 설치하는 기술로 이는 인터넷 웜과 같은 인터넷 공격기법을 이용한다. 취약점 점검 및 분석 기술, 해킹공격 기술 데이터베이스 등 해킹에 대한 전반적인 기술을 필요로 하며, 기능적으로는 인터넷 웜의 기능을 가지게 된다. 본 시스템은 관리 시스템과 에이전트로 구성되며, 효율적인 침입자 역추적을 위하여 작고 가벼운 에이전트를 구현하여야 한다. 따라서 에이전트 자동 업그레이드, 은닉화, 암호화 채널 구성 등 고난위도의 에이전트 기술을 필요로 하게 된다.

이러한 적극적인 방법을 사용한 역추적 시스템은 공격자를 실시간으로 역추적 할 수 있는 메커니즘을 제공하여 공격자에게 상당한 위협을 줄 수 있고 이를 통하여 중요 정보통신망에 대한 해킹사고 예방 효과 및 대응활동에 활용할 수 있다.

2. 관련 연구 분석

가. 해킹 피해시스템 자동분석 에이전트(AIAA)

AIAA는 기존의 수작업을 통한 해킹피해시스템 분석과 침입자 추적을 대신해서 자동화 된 방법을 제공한다.[1] AIAA는 해킹피해시스템 로그 분석정보, 침입탐지 및 추적 정보 그리고 침입 시 AIAA 관리자에게 침입사실을 알려주는 AIAA 서버와 피해시스템에 탑재되어 피해사항 분석, 침입탐지 및 추적 관련 기능을 수행하는 AIAA 에이전트로 구성된다. 그러나 현재까지 구현된 AIAA의 기능은 해킹피해를 당한 시스템에서 피해를 자동으로 분석해 주는 데는 효율적이지만, 침입자 자동 역추적 기능은 미흡하여 강화가 필요한 상황이다.

나. 침입자 역추적 기술동향

기존의 역추적 시스템의 단점은 침입 탐지 시스템과 동시에 작동하기 때문에 침입자가 거쳐온 모든 지점에 침입 탐지 시스템이 작동하고 있어야하며, 사용자의 인증을 위해 많은 요청/확인 메시지의 전송을 필요로 한다. 이는 통신망의 가역 대역폭을 낭비하게 되며 시스템의 가용성을 저하시키는 요인이 되므로 보안과 성능면에서 좋지 못하다.

다. 미행기술을 이용한 침입자모니터링

미행 기술은 자기 보호 기술을 가진 모듈로써 부정 행위자의 tty를 모니터링 하여 호스트레벨에서의 감시를 수행한다. 또한 부정 행위자가 다른 호스트로 이동하여 공격을 통해 시스템

에 심각한 영향을 미칠 수 있는 관리자 권한을 획득한 경우 모니터링 행위 자체를 노출하지 않으면서 미행하여 그 시스템에 신분확인을 위한 모듈들을 복제함으로써 다시 미행을 위한 거점을 확보할 수 있다. 즉 분산된 모니터링이라 할 수 있다.

라. 유닉스서버 해킹기술 분석

인터넷 웜은 바이러스와 같이 빠른 전파력을 갖고 원격에서 시스템을 공격하고 조작할 수 있는 기술이 사용된다. 에이전트를 설치하는데 사용될 공격 기술에 대하여 알아보기 위해 대표적인 웜인 "Millennium Internet Worm"(이하 mworm)을 통해서 인터넷 웜의 동작원리와 특징을 분석한다.[5]

mworm은 리눅스 시스템의 일반적인 원격 공격 취약성들을 공격하여 접근 권한을 얻어내거나 네트워크를 통해 전파시키는 기능을 가진 스크립트 및 프로그램의 집합이다. 자체적인 확산 기능과 함께 은폐 기능, 스캐닝 기능, 원격 공격 기능, ftp를 이용한 침입 기능 등을 포함하고 있기 때문에 수 시간 내에 많은 시스템을 공격할 수 있는 해킹 기술이다.

```
(Prepare)
mv /bin/ps /bin/.ps;echo "/bin/.ps W$* | grep -v ps | grep -v mw | grep
_
grep" >> /bin/ps ; chmod 755 /bin/ps
if [ -f /etc/rc.d/rc.local ] then
        echo "( sleep 10 ; cd /var/tmp/..../ ; ./mworm ) >>/dev/null & "
    >>
                /etc/rc.d/rc.local
else
        echo "( sleep 10 ; cd /var/tmp/..../ ; ./mworm ) >>/dev/null & "
    >>
                /etc/profile
fi
chattr +ia /var/tmp/..../*.c /var/tmp/...../mwd* /var/tmp/..../prepare /bin/.mws
chattr +ia /etc/rc.d/rc.local /etc/profile /var/tmp/..../mwo* /var/tmp/..../IP
chattr -ia /var/tmp/..../mount_*.c
fi
killall -q -9 syslogd

(Mworm)
./prepare for your d00m mortalz
./IP | mail -s "Mworm is here" trax31337@hotmail.com
logout
_EOF_
./mwd & ./mwd-pop & ./mwd-imap & ./mwd-mountd & ./mwd-ftp &
sleep 60
/bin/.mwsh -c ./bd
```

웜에 의해서 해킹이 이루어질 경우 해킹에 성공한 시스템에는 해킹 스크립트가 복사가 되면서 랜덤하게 다른 시스템을 선택하여 연속적으로 계속 공격이 이루어지게 된다. 이러한 연속적인 공격 기법을 응용하게 되면 해커가 침입해온 경로를 따라 경유지 시스템들을 연속적으로 역공격하여 해커의 근원지를 역추적 할 수 있게 된다.

3. 시스템 설계 및 구현

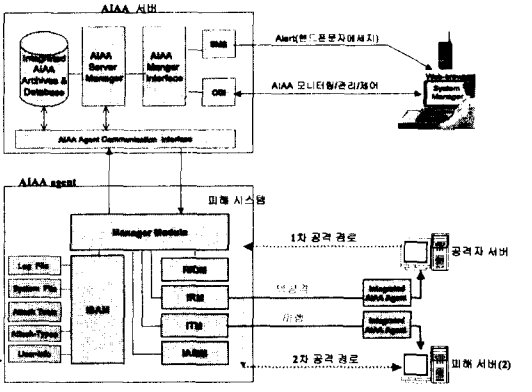
가. 요구사항 분석

침입한 해커의 활동을 분석하여 근원지를 역추적하기 위해서는 네트워크의 중요 중간 기점이 되는 곳에서 지속적으로 로그를 기록하여 역추적에 활용해야 할뿐만 아니라, 이러한 역추적이 실시간으로 이루어지는 시스템이 필요하다. 이와 같이 네트워크의 중요 기점에서 지속적으로 로그를 기록할 경우 어떤 시스템이 침입 당하면, 그 시스템이 침입 당한 시점에 기록된 중요 기점들의 로그를 분석함으로서 해커의 근원지를 파악하는데 중요한 자료가 된다. 역추적 시스템은 현재의 인터넷 환경에서 해커의 역추적을 위한 방법에 대해서 연구하려고 하며, 이러한 역추적을 위해서는 다음과 같은 사항에 대하여 가정을 한다.

- 역추적 서버에서는 역추적을 위한 통신 모듈과 역추적 에이전트로부터 리포트 된 정보를 보존하고 통신 모듈은 항상 서버로 작동하면서 에이전트의 요구에 응답해 주어야 한다.
- 역추적을 위해서는 시스템에서 해킹 피해분석 기능, 실시간으로 재침입 탐지 기능 그리고 실시간 해커 활동 탐지 기능이 필요하다.

나. 시스템 설계

역추적 시스템은 크게 Integrated AIAA 서버와 Integrated AIAA 에이전트로 구성된다. AIAA서버에는 관리용 인터페이스와 매니저 기능, 에이전트와의 통신 인터페이스, 그리고 역공격을 위한 해킹공격 database로 구성된다. Integrated AIAA 에이전트는 에이전트 종합 관리 모듈(Manager Module), 침입 피해분석모듈(Intrusion Signature Analysis Module), 재침입 탐지 모듈(Re-Intrusion Detection Module), 역추적 공격 모듈(Intruder Retracing Module), 침입자 모니터링 모듈(Intruder Activity Monitoring Module), 침입자 추적(미행)모듈(Intruder Tracing Module)로 구성된다. 본 시스템의 개념도는 (그림 1)과 같다



(그림 1) 역추적시스템 개념도

[표1] 역추적시스템의 수행내용

구분	내용
Integrated AIAA 서버	o Manager Interface (CGI, Short Message Service) o AIAA Server Manager o AIAA Agent Communication Interface o 역공격을 위한 해킹 공격 Database
Integrated AIAA 에이전트	o Manager Module o ISAM (Intrusion Signature Analysis Module) o IDM (Intrusion Detection Module) o IRM (Intruder Retracing Module) o IAMM (Intruder Activity Monitoring Module) o ITM (Intruder Tracing Module)

역추적을 위해서 AIAA 서버는 신뢰성 있는 중앙센터 내에 설치하고, 관리자는 웹 브라우저를 통해서 AIAA 서버에 연결한다. 웹 브라우저에서 역추적 사용자는 역추적을 하고자 하는 피해 시스템을 선택하고 로그 분석과 시스템 분석을 실시한다. 그리고 역추적에서 이전 호스트가 발견되거나 이상한 사용이 발견되면 바로 역공격을 통해 직전의 공격시작 시스템을 탈환하고 역추적 에이전트를 복사한다. 이와 같은 행위를 그 이전 공격시작 시스템에 대하여 반복적으로 수행한다.

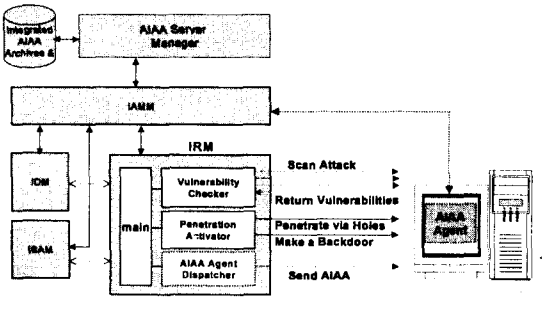
다. 시스템 구현

본 시스템은 위에서 설계 제안된 Integrated AIAA 서버와 Integrated AIAA 에이전트 각각의 기능을 구체화함으로써 구현된다. 특히 Integrated AIAA 서버에서 사용하는 최적의 공격 기법을 생성해내기 위한 알고리즘은 다음과 같다.

```
do 해킹 피해 시스템 분석;
  if (생성된 불법계정 존재 && 역추적 대상 시스템에 동일한 불법계정 존재) {
    then  역추적 대상 시스템에 동일 계정으로 접속;
          역추적 대상 시스템의 local 취약점 분석;
          local 공격;
  }
  else if (백도어 설치 && 역추적 대상 시스템에 동일한 backdoor설치) {
    then  역추적 대상 시스템에 backdoor로 접속;
  }
  else { 원격 취약점 정보수집;
      remote 공격;
  }
```

Integrated AIAA 에이전트는 각 구성요소들을 구체 화하여 구현하였다. **에이전트 종합 관리 모듈(Manager Module)**은 AIAA서버와 통신 채널을 유지하고 정보를 전달받는 등의 기능을 한다. 또한 최소 설치시에 은닉 기능을 수행한다. **침해피해분석모듈(ISAM)**은 시스템로그분석기능, 시스템 프로세스 분석기능, 그리고 파일 변경 검색기능을 갖추고 있고 이러한 검색이 가능하기 위해 해커가 로그를 변경시키지 못하도록 방법을 강구한다. **재침입탐지모듈(IDM)**은 일반적으로 백도어를 만든 후 재침입의 가능성이 높으므로 재침입이 가능한 방법을 미리 예측 후 재침입이 발생하면 근원지 주소를 역추적 하게 된다. **역추적공격모듈(IRM)**은 역추적 대상 시스템과 취약점 정보 그리고 역공격을 하기위한 최적의 공격기법을 결정한다.

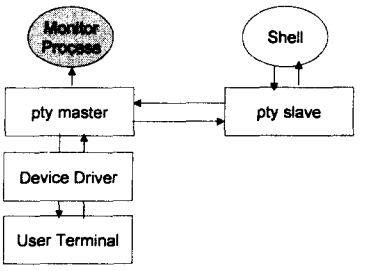
AIAA에이전트는 AIAA서버로부터 전달받은 공격 모듈을 사용하여 역추적 대상 시스템에 대하여 1차 역공격을 수행한다. 1차 공격이 성공한 경우 AIAA 에이전트를 역추적 대상 시스템에 스스로 복제한 후 ① AIAA서버와의 통신채널 확보 ② 해커로부터의 은닉 ③ 시스템 분석 및 재침입 탐지 ④ 역추적 을 수행하여 에이전트로서의 기능을 반복한다. 만일 1차 공격이 성공하지 못한 경우 AIAA에이전트는 이 결과를 AIAA서버에 보고하고 해킹공격 데이터베이스의 AI엔진에서는 차순위의 공격기법을 분석하여 새로운 공격 모듈을 AIAA에이전트에 전달함으로써 역공격이 반복되게 된다.



(그림 2) 역공격 개념도

침입자 모니터링 모듈(IAMM)은 사용자 행위를 감시하기 위해 사용자의 로그인 tty를 모니터링한다. 미행 기술에서 모니터링은 사용자의 터미널(tty)을 부정 행위자가 로그인 할때 동적으로 할당되는 pty에 복사하는 방식으로 수행된다. 이것은 (그림 3)과 같다.

마지막 구성요소인 **침입자 추적모듈(ITM)**은 호스트 레벨에서 행위 감시가 수행되다가 침입자가 다른 제3의 호스트로 공격, 이동하는 경우 침입자가 행한 공격방법과 동일한 기법으로 이동한 호스트에 미행과 탐문을 위한 AIAA에이전트를 복제한다.



(그림 3) 침입자 모니터링 모듈

4. 결론 및 향후 계획

본 논문에서는 해킹공격 등에서 역공격을 이용한 불법 침입자에 대한 역추적 시스템을 제안하여 구현하였다. 이러한 역공격은 지금까지 비윤리적인 측면과 법·제도적으로 시행하기가 어려운 점들이 많이 고려되었으나 최근 자신의 시스템을 방어하는데 있어 적극적인 수단이 요구되는 점, 분산서비스거부공격과 같이 부당하게 해킹에 이용된 중간 경유지시스템에 대한 책임 추궁 등의 분위기에 따라 적극적으로 활용될 가능성이 있다.

다만 이러한 기술이 실용화 수준으로 구현되기 위해서는 다음 영역에 대한 연구가 좀더 진행되어야 한다.

첫째, 이 기술의 핵심은 인접하는 해킹 근원지에 대한 역공격시 가장 효과적인 공격기법을 찾아내는 것으로서 업데이트가 용이한 풍부한 양의 해킹공격 데이터베이스와 고수준의 AI에 의한 해킹기법 분석엔진이 구현되어야 할 것이다.

둘째, 역추적 및 미행을 위한 AIAA에이전트의 자기 복제 시 해커로부터 AIAA에이전트를 은닉할 수 있는 방안이 좀더 연구되어야 할 것이다.

셋째, AIAA서버와 AIAA에이전트간의 정보전달 시 통신채널의 효율적인 암호화 기법에 대해서도 좀더 심도 있는 연구가 이루어져야 할 것이다.

<참고문헌>

[1] Sangyoub Lee, Hyuncheol Jeong, Jeonghyun Park, Chaeho Lim, "Intruder Retracing Using Autonomous Incident Anaysis Agent", FIRST Conference, 1999.6.
[2] H.T.Jung, et. al., "Caller Identification System in the Internet Environment", Proceedings of the USENIX Security Symposium IV, 1993.
[3] RFC 1413: "Identification Server".
[4] 한국정보보호센터, "부정행위자 신분확인용 S/W 설계 및 구현", 1999.12.
[5] 한국침해사고대응지원팀, Millennium Internet Worm 분석 보고서, http://www.certcc.or.kr/
[6] PacketStorm http://packetstorm.securify.com
[7] SecurityFocus http://www.securifyfocus.com
[8] common Vulnerabilities and Exposures http://cve.mitre.org, a unified hack database
[9] Simple Nomad, "Strategies for Defeating Distributed Attacks" http://packetstorm.security.com/papers/contest/Simple_Nomad.doc
[10] Simple Nomad, "Progect Area52" , Phrack 56-06