韓國 컴퓨터情報學會 論文誌
第12卷 第3號, 2007. 7.

2007-12-3-2-4

WiBro에서 공격 이동단말에 대한 역추적기법 연구

박 대 우*, 임 승 린**

A Study of the Back-tracking Techniques against Hacker`s Mobile Station on WiBro

Dea-Woo Park*, Seung-in Lim**

요 약

WiBro가 IEEE802.16e로 국제 표준화 되었다. 국내뿐만 아니라 세계에서도 휴대인터넷으로 WiBro 서비스를 시작하고 있다. 본 논문에서는 불법 공격자인 해커가 휴대인터넷 WiBro의 이동단말을 이용하여 자신의 위치 추적을 피하기 위하여, 피해 시스템을 직접 공격하지 않고 우회 공격을 수행한다. 현재 인터넷망에서 침입 기술에 적극적인 보안을 위한 진보된 알고리즘을 응용하여 효과적인 역추적 기법 등을 연구한다. 공격자인 이동단말에 대한 역추적을 할 때, 실시간 네트워크 로그 감사기록을 이용하고, TCP/IP와 네트워크 기반에서는 Thumbprint Algorithm, Timing based Algorithm, TCP Sequence number 등을 이용한 알고리즘 및 SWT 기법 등을 이용한 역추적 기법 등을 설계하고, 역추적을 실시하였다. 또한 트래픽 폭주 공격에 대해 AS시스템을 이용한 네트워크 트래픽 관리와 통제 및 실시간으로 역추적을 하였다. 본 논문의 연구 결과는 유비쿼터스 환경에서의 WiBro 인터넷에서의 역추적을 실시하고 포렌식 자료를 확보하는데 이바지 할 수 있을 것이다.

Abstract

WiBro has become intentionally standardize as IEEE 802.16e. This WiBro service has been started by a portable internet at home as well as abroad. In this paper, an offender hacker do not direct attack on system on system that It marched an attack directly in damage system because a place oneself in mobile station of portable internet WiBro and avoid to attack hacker's system. At this time, a mobile make use of network inspection policy for back-tracking based on log data. Used network log audit, and presented TCP/IP bases at log bases as used algorithm, the SWT technique that used Thumbprint Algorithm, Timing based Algorithm, TCP Sequence number. Study of this paper applies algorithm to have been progressed more that have a speed to be fast so that is physical logical complexity of configuration of present Internet network supplements a large disadvantage, and confirm an effective back-tracking system. result of research of this paper contribute to realize a back-tracking technique in ubiquitous in WiBro internet network.

▸ Keyword : Algorithm, Forensics, Hacking, Back-tracking, WiBro

• 제1저자 : 박대우
• 접수일 : 2007.5.31, 심사일 : 2007.7.10, 심사완료일 : 2007. 7.23.
* 호서대학교 벤처전문대학원 교수, ** 수원과학대학 컴퓨터정보과 교수

Ⅰ. 서 론

WiBro(Wireless Broadband Internet)는 2.3GHz 주파수 대역을 이용하며 이동단말이 60km/h이상 이동 시에도 가입자당 전송속도 약 1Mbps의 끊김없는(seamless) 휴대인터넷 서비스를 제공한다. WiBro 서비스는 광대역 무선가입자망 기술의 개념인 Wireless MAN (Metropolitan Area Network)에서 출발하여 수신안테나와 가입자 장치(Subscriber Station)를 이용한다. 상용 케이블모뎀은 표준규격인 DOCSIS (Data-Over-Cable Service Interface Specification)을 근간으로 LOS (Line-of-Sight) 통신환경에서 PHY 모드인 OFDM, OFDMA와 MAC 규격에서 IEEE 802.16a[1] 표준화가 추진되었다.

IEEE Std. 802.16-2004(TGd Specification)는 역방향 호환성(Backward Compatibility)을 유지하면서, 단말기의 이동성을 지원하기 위한 표준화 작업을 하고 있다. 역방향 호환성의 의미는 고정형 규격을 지원하는 가입자 이동단말은 이동성을 지원하는 기지국에 의하여 서비스가 제공되어야 한다는 것과, 이동성을 지원하는 가입자 이동단말은 이동성을 제한하였을 때 고정형 기반의 기지국에 의하여 서비스가 제공될 수 있어야 한다는 것이다.

공격자인 해커는 이러한 역방향 호환성을 이용하여 WiBro 이동단말을 사용한 비합법적인 공격을 하여, 사회업무 및 금융거래 등의 목적시스템에 대한 악의적인 직·간접의 피해를 줄 수 있는 것이다. 휴대인터넷인 WiBro 서비스의 이동단말을 통해 이동성을 보장 받으면서, 추적을 따돌리고 안전하고 신속한 사회업무, 금융거래 등의 보안과 안전을 위협한다. 이러한 해커의 비합법적인 행위에 대한 안전성과 보안성을 강화하고, 국가 법질서의 수호를 위해 필수적으로 요구되는 것이 WiBro 이동단말에 대한 역추적과 모바일 포렌식의 자료를 생성하는 것이다.

본 논문의 연구에서 휴대인터넷인 WiBro에 대한 표준화 규격 및 기술 절차를 연구한다. 또한 기존의 역추적 기법으로 이동단말의 역추적 기법, 전향적, TCP 역추적 기법, IP 역추적 기법, 전향적 기법과 대응적 기법에 대해 연구한다.

연구를 통한 설계에서 휴대인터넷인 WiBro에서의 이동단말에 대한 역추적기법 등을 설계하고, 역추적을 실시하여 포렌식 자료를 생성하는 것이다.

Ⅱ. 관련 연구

2.1. WiBro 기술

2003년 9월 IEEE SA(Standard Association)는 TGe(Project P802.16e)의 표준화의 범위는 OFDMA 모드에서의 확장성을 지원하기 위한 128, 512, 1024 FFT 모드의 추가 등과 역방향 호환성의 유예 등이 있었다.

WiBro 규격은 IEEE 802.16-2004 및 IEEE P802.16e/D3 또는 이후 버전으로서 이중화 방식은 TDD(Time Division Duplexing)을 사용하고, 주파수 재사용계수는 1을 만족하여야 하며, 채널대역폭은 9MHz 이상을 가지고, 이동성 시속 60km/h 이상에서 셀 간의 경계구역에서 최소 전송속도 UL 128 kb/s, DL 512 kb/s를 만족하여야 하며, 사업자간 로밍을 제공하여야 하는 등의 5가지 요구사항을 만족하여야 한다.

IEEE 802.16e에서는 이동성을 지원하기 위하여 Handoff[2] 및 Sleep Mode 기능 제공뿐만 아니라, 단말기의 절전 기능을 극대화시키며 광역에서 기지국간 안정성 있는 멀티캐스트/브로드캐스트 서비스를 제공하기 위한 MBS (Multicast & Broadcast Service) 및 Idle Mode 기능, 착신 서비스를 고려한 Paging 기능, 그리고 보다 빠른 핸드오버를 제공하기 위한 FBSS(Fast Base Station Switching) 기능 등이 표준에 반영되었다. 또한 시스템의 성능을 향상시키기 위한 다중안테나 관련 기술인 AAS 및 MIMO(Adaptive Antenna System 및 Multiple-Input Multiple-Output)들이 다수 제안되고 채택되었다. 최근에는 보다 개선된 Channel Coding 방식인 LDPC 기술 등도 채택됨으로써 보다 다양한 기능을 제공한다.

2.2. HSDPA 기술

이동통신의 3.5세대인 HSDPA(High Speed Down link Packet Access)는 그림 1처럼 기존의 휴대전화인 W-CDMA, cdma 2000 1x 등 이동전화와의 결합을 통해 노트북, 휴대전화, PDA등의 다양한 단말기 형태를 통해 서비스가 가능하며, 하나의 단말기에 이동전화, WiBro, DMB 등 다중모드의 지원이 가능해 질 것으로 예상된다. 기존의 W-CDMA와 달리 기지국(Base Station)에서부터 데이터의 전송이 가능한 패킷 네트워크 교환방식이다.

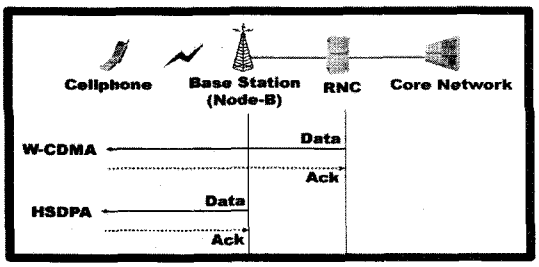

그림 1. 데이터 패킷을 접속하는 HSDPA 네트워크
Fig. 1. HSDPA Network for Access on Data Packet

2.3 이동단말의 역추적 기법

이동단말에서 물리계층의 자원을 효율적으로 제어하는 것을 목적으로 하는 MAC기술은 인증과 암호 키의 교환, 암호화 등의 기능을 수행한다. 물리계층으로의 Privacy Sublayer, 대역할당, 접속설정 및 유지, QoS 관리, 데이터 전송기능 등을 수행하는 MAC CPS(Common Part Sublayer), 외부 네트워크와 송수신하는 데이터의 변환과 매핑, 유료부하 헤더압축 등의 기능을 수행하는 CS(Convergence Sublayer) 등 3개의 부 계층으로 이루어진다. 패킷 데이터의 송수신을 제어하기 위한 MAC계층에서 트래픽 버스트 데이터 할당에 관한 정보와 물리계층의 제어메시지를 포함하고 있는 MAP의 종류에는 Normal MAP, Compressed MAP, HARQ MAP, HARQ지원 Normal MAP Extension, Sub-DL-UL-MAP 등이 있어 이 기능을 통한 위치 추적 및 호 할당과 관련한 로그기록을 확보 한다.

2.4. TCP 역추적 기법

TCP 연결 역추적 기술은 호스트 기반 연결 역추적 기술과 네트워크 기반 연결 역추적 기술의 2가지로 분류된다.

2.4.1 Host 기반 역추적 기법

역추적을 위한 모듈이 인터넷 상의 호스트들에 설치되는 역추적 기법으로 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술이다. 그러나 이러한 방법을 이용하여 역추적을 수행하기 위해서는 인터넷 상의 모든 호스트에 역추적 모듈이 설치되어야 하고, 역추적 경로 상의 단 1개의 시스템에서라도 어떤 문제에 의해서 역추적 정보를 얻을 수 없게 되는 경우가 발생하면 역추적이 불가능하게 되는 단점을 가지고 있다[3,4,5,6].

2.4.2 네트워크 기반 역추적 기법

네트워크상에 송수신되는 패킷들로부터 역추적을 수행할 수 있는 정보를 추출하여 역추적을 수행하는 것으로 제안되고 있는 방법은 대부분 송수신 패킷을 확인할 수 있는 위치에서 공격 연결과 같은 연결 체인에 속하는 연결을 추출하여 역추적을 수행하는 방법을 취하고 있다. 네트워크상에서 얻을 수 있는 패킷으로부터 어떤 정보를 활용해야 공격 연결과 같은 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘만이 제기되고 있는 상황이다[3,7,8].

또 다른 네트워크 기반 연결 역추적 기술로는 액세스 네트워크상에서 동작하는 기술들이 있다. 그러나 액세스 네트워크는 신뢰성있는 서비스인 TCP를 기본으로 하기 때문에 현재의 인터넷 환경에 적용하는 데 많은 어려움이 있는 것이 사실이다[9,10].

2.5. IP 역추적 기법

IP 역추적은 현재 특정 시스템으로 IP 주소가 변경된 패킷을 송신하는 격자인 해커의 시스템을 찾는 기술로서, 중간 경유지를 역추적한 후, IP 주소가 변경된 패킷의 실제 송신지를 추적하기 위한 기술을 말한다.

해커는 IP 주소가 변경된 패킷으로 DoS(Denial of Service)공격이나, DDoS(Distributed Denial of Service) 공격[11]을 한다. IP 주소가 변경되는 경우에는 TCP 연결을 유지할 수 없다. IP spoofing 공격은 IP 주소가 변경된 패킷을 이용하여 공격하고자 하는 목표 시스템에 백도어를 설치하도록 하는 기법 등이 사용 된다.

그림 2에서 IP 패킷 역추적 기법은 해커가 전송하는 패킷에 해당 패킷을 전달한 라우터를 표시함으로써 추적할 수 있게 하는 패킷 표시 기법을 이용한 연구와 다른 여러 기법을 통한 IP 패킷 역추적을 위한 연구[12]가 진행 중이다.

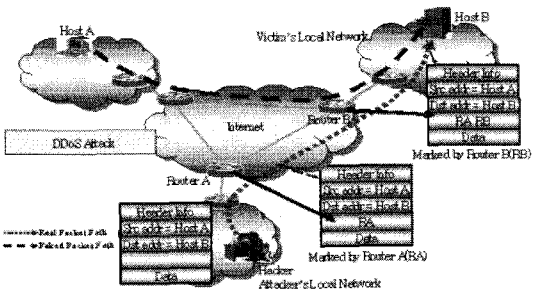

그림 2. IP 패킷 역추적
Fig. 2. Traceback of IP Packet

2.6. 전향적 역추적 기법

2.6.1 링크 검사법

hop-to-hop 역추적 방식에 해당하는 것으로 각 라우터에서는 연결된 링크를 검사하면서 트래픽이 DoS, DDoS 공격으로부터 전송된 패킷인지의 여부를 검사하게 된다. 자동화된 역추적 방법을 제공하지는 못하며 직접적으로 패킷 전송 경로를 조합/판별하는 방법에 해당한다. 따라서 네트워크 관리 측면에서의 오버헤드가 발생하게 된다. 링크 검사법에 대한 구현 결과로 제시된 input debugging 기법에서는 공격 유형(Attack Signature)을 기반으로 공격 트래픽에 대한 판별하고 실제로 전송된 경로를 판별한다.

2.6.2 로깅 기법(Logging)

로깅 기법은 라우터에서 전송된 패킷에 대한 특성 등을 기록해 놓은 후에 데이터 마이닝 등의 추론 시스템을 적용하여 공격 근원지를 검출하는 기법이다. 물론 많은 양의 정보를 저장/관리하고 있어야 하며 데이터 처리량 또한 방대하여 효율적인 대응 기법이라고 할 수는 없다.

이에 대한 해결책으로 확률적인 샘플링 기법 등을 적용하여 처리 데이터를 줄이고, 필터기법 등을 적용하여 처리/판별 과정을 간략화 하는 방법 등이 제시되기도 하였으나 방대한 패킷에 대한 판별 과정에서의 오류 수정 과정 등이 보완되어야 한다.

2.6.3 PPM 기법

스푸핑된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크상에 전송되는 패킷에 대해 네트워크를 구성하는 주요 요소인 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다. 즉, 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더에서 변형 가능한 필드에 대해서 라우터에 해당하는 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다.

각 라우터에서 삽입된 정보는 다시 다음 라우터로 전달되고 최종적으로 목적지 피해 시스템에 전달된다. 각 라우터에서 마킹된 정보가 전달되면 추후에 해킹 공격이 발생하였을 경우 해킹 공격에 해당하는 패킷에 기록된 라우터 정보를 재구성하여 실제적인 패킷의 전달 경로를 재구성하게 된다. 이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링(Node Sampling), 에지 샘플링(Edge Sampling) 및 개선된 패킷 마킹 기법 등이 제시되었다.

2.6.4 iTrace(ICMP Traceback)기법

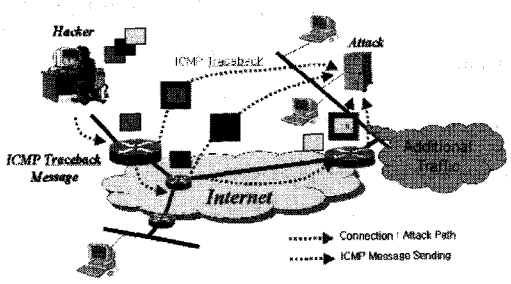

그림 3. iTrace 역추적 기법
Fig. 3. Back-tracking of IP iTrace

iTrace 역추적 기법은 PPM 기법과는 다른 접근 방법으로 수행된다. 라우터에서는 일반적 $\frac{1}{20,000}$의 확률로 패킷을 샘플링 하여 iTrace 메시지를 생성하고 이를 패킷의 목적지 IP로 전송한다. iTrace 메시지는 일반적인 ICMP 메시지와 유사하게 전 단계 라우터 정보와 다음 단계 라우터 정보를 포함하고 있으며 패킷의 payload 정보 등을 포함 하여 전달하게 된다.

그림 3에서 TTL(Time To Live) 필드 값은 255로 설정되어 전달되며 목적지에서는 TTL 값을 보고 네트워크 위상에서의 홉 거리 정보이기 때문에 공격경로 재구성에 사용된다.

2.7 대응적 역추적 기법

2.7.1 오버레이 네트워크 역추적 기법

본 기법은 역추적 라우터 TR(Tracking Router) 모듈을 네트워크에 별도로 설치하고 해킹공격이 발생하였을 경우, 그림 4처럼 네트워크위상에서의 종단시스템과 연결된 라우터에서 전달된 정보를 TR로 전송한다. 즉, 기존의 ingress 필터링 기법과 유사하게 종단 라우터에서 보내진 트래픽정보는 터널링 방식으로 TR 라우터에 전달된다. 각 패킷에 대해 20 바이트 정보의 패킷 서명(Packet Signature) 정보를 생성하여 TR로 전달하게 된다.

2.7.2 해쉬기반 역추적 기법

본 기법은 SPIE(Source Path Isolation Engine) 기반 역추적 서버를 구성하고 전체네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리한다. 그리고 각 라우터에는 DGA(Data Generation Agent) 기능을 탑재하여 운영한다.

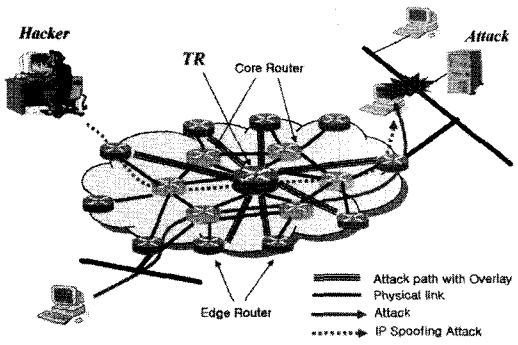

그림 4. 오버레이 네트워크 기반 역추적
Fig. 4. Back-tracking of Network Overlay

DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬 값에 해당하는 IP 헤더 정보와 8 바이트정보의 payload 정보를 수집관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 목적지 시스템에 있는 IDS, IPS 시스템[13]에 의해 해킹을 발견하였을 경우 SPIE 시스템에서는 네트워크 그룹을 관리하는 SCAR 에이전트를 통해 그룹 내 DGA 라우터에 저장된 정보와 해킹 패킷정보를 비교 분석하여 이를 다시 SPIE 시스템에 전달하게 되면 해킹 관련 패킷의 전송경로를 재구성하게 된다.

III. 이동단말 역추적 모델 설계

WiBro단말기는 PDA, 핸드헬드(Handheld)PC, 노트북, 스마트폰 등의 여러 단말기 형태를 가지며, 기존의 시스템에 WiBro를 이용한 송수신을 하는 구조로 되어 있으며, 내부 블록 시스템은 그림 5와 같다.

해거의 WiBro단말기에 대한 역추적은 TCP/IP의 로그 기록을 이용한 IP 역추적 설계 및 포렌식의 생성을 위해 로그기반 침입자 역추적 기법과 TCP/IP 기반 연결 역추적 설계와 네트워크 기반 연결 역추적 알고리즘을 사용한다.

3.1. 로그에 대한 역추적 설계

네트워크의 로그 기록을 통한 추적은 네트워크에서 공격자네 대한 분석과 제어 절차 개발과 설정된 보호 정책을 허용하며 정책 절차상에서 요구된 변경 사항을 저장하도록 해야 한다. 네트워크 보호와 관련된 사건은 로그기록으로 남으며, 감사 대상 자료가 될 수 있으며, 이 자료를 통해 역추적을 한다. 감사 자료의 종류는 크게 두 가지로 분류 된다.

- 네트워크 보안에 관련된 로그 및 감사 기록
  - 시스템과 시스템들 사이의 접속.
  - 시스템에 요청된 서비스 종류(Ftp, Telnet 등).
  - 네트워크에서의 Traffic 양.
- 시스템 보안에 관련된 로그 및 감사 기록
  - 시스템 자원에 관련된 감사 자료(CPU 사용량, I/O 장치 사용량 등).
  - 사용자 로그인 실패 횟수.
  - 사용자 패스워드 실패 횟수.
  - 파일 시스템에 관련된 감사 기록(Read, Write, delete, Create, Append 등).
  - 시스템 파일에 관련된 로그 및 감사 기록.
  - 한 세션 안의 사용자의 지속 시간.
  - 한 세션 안의 사용자의 출력 데이터의 종류 및 양.

감사 기록을 이용하여 역추적을 하면 사용자의 행동 패턴을 통하여 시스템 사용에 대한 감사 추적을 수행 할 수 있다.

별도의 역추적 설비가 없는 시스템에서는 UNIX의 기본적인 로그 정보를 바탕으로 특정 사용자나 호스트의 정체를 파악하기 위해 관련 명령어를 사용하여 침입자를 추적할 수 있다 불법 침입자의 침입흔적은 시스템의 각종 로그 파일에 남는다[14]. 시스템에 대한 스캔 행위, exploit 툴을 이용한 공격, 특정 사용자 계정으로의 접속, root 권한의 획득, 트로이목마 프로그램 설치, 자료 유출 및 삭제 등 공격자의 행위 하나 하나가 모두 시스템에 의해 감시되고 로그로 남게 된다. 일반적으로 사용자 추적에 사용되는 명령어는 finger, users, whodo 등이 있다.

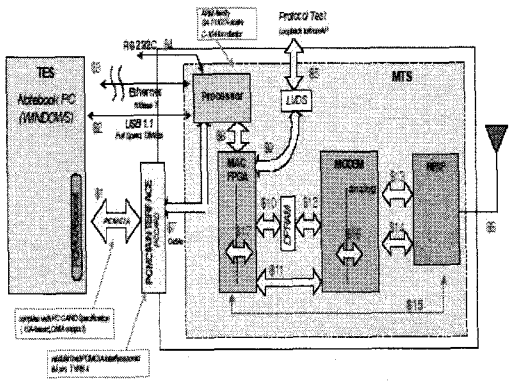

그림 5. WiBro 단말기의 내부 블록 시스템
Fig. 5. Inner Block System in WiBro Mobile Station

또한 현재 사용자가 시스템에서 활동 중일 경우, 사용자의 연결 상태와 활동을 파악하기 위해 netstat 명령어를 사용한다. 사용자 추적에 사용될 수 있는 로그 파일들로는 utmp, wtmp, acct, lastlog, messages 등의 로그 파일들이 있으며, 이러한 로그 파일들은 자동으로 생성된다.

3.2. CIS, AIAA 역추적 설계

CIS(Caller Identification System)는 사용자가 특정 시스템에 접속하고자 할 때, 이전에 거쳐 왔던 모든 시스템에 대한 시스템 목록과 로그인 ID 등의 정보를 요구한다. 그리고 요구에 따라 이전의 경유 시스템 목록을 입력 받게 되면, 모든 경유 시스템과의 통신을 통해 각 시스템에 대해 입력된 시스템 및 로그인 ID 목록이 정당한 것인지를 확인하게 되고, 이러한 목록이 유효할 때만 접속을 허락한다. 이런 형태의 역추적 시스템은 미리 사용자가 지나온 시스템의 목록을 관리하는 것이다.

AIAA(Autonomous Intrusion Analysis Agent) 시스템은 바로 이전의 침입경로와 해킹 흔적을 분석하고 다시 이전의 침입시스템으로 분석을 옮겨가서 최종 경유지 서버까지 거슬러 가면서 침해를 당한 서버의 해킹 피해 분석과 추적을 위한 로그 분석 에이전트를 이용하는 자동화한 역추적 시스템이다.

3.3 텍스트 필터링을 이용한 역추적 설계

이메일 스팸 차단 방법 중 하나이며, 수신된 이메일의 내용을 검사하고 분석해 스팸으로 의심되는 메일들을 제거하는 것으로 본 논문에서는 베이지안(Bayesian) 필터링 방법을 사용하려고 한다.

베이지안식 필터링은 텍스트 분류(Text Classification)를 통해 해커들이 사용하는 특정 개별 단어의 출현 빈도를 모두 기록한 뒤, 비슷한 분류의 텍스트를 계속 샘플 데이터로 추가 시켜나가면서 단어들의 연관을 추적하여 임의의 텍스트가 해당 분류에 속하는지 여부를 알 수 있다.

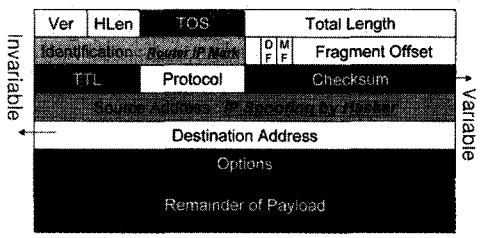

그림 6. IP 패킷 헤더의 spoofing
Fig. 6. Spoofing on Header of IP Packet

그림 6처럼 특정 출발지 주소(Source Address)가 포함되거나, 특정 단어가 포함되면, 이 단어들을 포함하는 패킷과 네트워크에 대한 감시와 통제를 통해 역추적을 실시하도록 설계한다.

3.4 알고리즘 기반의 역추적 설계

3.3.1 Thumbprint based 알고리즘의 설계

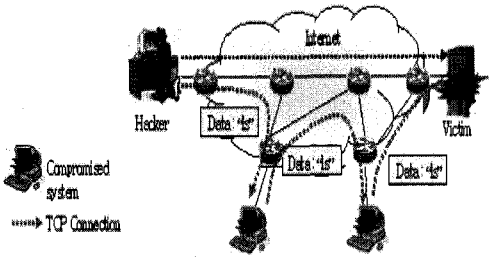

그림 7. 지문기반 알고리즘
Fig. 7. Based Algorithm of Thumbprint

Thumbprint(지문) 알고리즘을 이용하는 방법은 역추적 시스템 전체를 의미하는 것이 아니라 역추적을 위해 공격자의 시스템으로부터 공격 대상 시스템까지의 연결 체인을 구성하는 알고리즘이다. 본 알고리즘은 연결 체인에 속하는 호스트들이 속한 네트워크상에 송수신되는 데이터를 수집하여 비교한다. 그림 7처럼 공격에 사용되는 연결에서 송수신되는 데이터로부터 추출한 내용 정보를 특정 함수를 적용하여 얻어낸 지문이 일정수준 이상 동일한 경우 두 연결은 하나의 연결체인 상에 존재하는 것으로 판단한다.

3.3.2 TCP sequence number 알고리즘 설계

TCP sequence number를 이용하는 알고리즘은 비록 송수신되는 데이터가 암호화 되더라도 데이터의 양은 크게 변하지 않는다는 점에 착안하여 sequence number의 증가 정도를 변동 폭의 조정을 통해 비교하고 연결 체인을 구성하는 알고리즘으로 설계한다.

3.3.3 Timing based 알고리즘 설계

알고리즘은 해커가 입력하는 키보드 입력에 의해 발생하는 데이터 송신 간격은 프로그램이 송신하는 데이터에 비해 매우 크기 때문에, 이를 쉽게 파악할 수 있고, 만약 같은 연결 체인에 속한다면 그 간격이 매우 유사할 것이라는 점을 이용한다. 이 시스템은 ON period와 OFF period를 이용

하여 각각의 상태가 변화하는 시점과 한 상태를 유지하는 시간 간격을 분석하여 같은 연결 체인에 속하는지 여부를 판단하게 된다.

IV. 이동단말 역추적과 포렌식 자료 생성

그림 8과 같은 WiBro 이동단말을 이용하여 실험실 환경에서 해커의 WiBro단말기에 대한 역추적을 실시하고, 역추적 결과로써, 포렌식 자료를 생성한다.

그림 8. WiBro 이동단말
Fig. 8. WiBro Mobile Station

4.1. 침입자 로그에 대한 역추적

WiBro 이동단말은 SKT의 WiBro장치를 USB케이블로 연결한 이동단말과 KTF의 PCMCIA 카드 타입을 WiBro 프로그램이 인스톨된 노트북에 연결하여 사용하였다.

노트북은 CPU는 듀얼코어 2.0GHz, 1024MB MM, Windows XP, 160GB HDD이다.

로그 기록과 IP 추출은 이동단말기는 Qualcom사의 QPST를 이용하였다.

에디터는 IDM의 UltraEditor를 사용 하였다.

실험에서 네트워크상의 사용자의 로그인, 로그아웃 기록과 명령어 실행 기록과 역추적 응용 프로그램을 수행한다. .cshrc, profile등에 미리 규정된 응용 프로그램을 기본 수행하는 것은 물론, shell 인터페이스를 통해 응용 프로그램의 수행을 지시하거나, 한 응용 프로그램 내부에서 fork, exec 등을 통해 다른 응용 프로그램을 구동 시킬 수 있다. 원칙적으로 응용 프로그램의 수행 없이 시스템 자원에 대한 접근이 이루어 질 수 없으므로 사용자별 응용 프로그램 수행 내역은 감사 로깅 시스템에서 네트워크에 대한 불법 접근을 추적할 수 있는 매우 유용한 정보가 된다.

해커의 WiBro 이동단말에서 서버에 침투하는 단계에서의 로그기록은 다음과 같다.

- 일반 사용자 및 시스템 관리자 로그인
  : utmp, wtmp, pacct
- 일반 사용자의 시스템 관리자 권한 획득
  : su, setuid
- 로그 파일을 삭제 및 파일을 변조하려는 시도
  : Shell_history, lastlog, syslog

해커가 네트워크상에서의 침투하는 단계와 이에 대응하는 침해사고 대응과 역추적을 실시한다.

1단계 : 일반 사용자 ID를 이용한 로그인은 허락하고 있다. 콘솔이 아닌 곳에서 슈퍼유저 ID를 사용하여 로그인 감사 로깅 시스템에서는 먼저 슈퍼유저로 시스템에 접근하려는 것을 제한하고 슈퍼유저는 콘솔에서만 접근할 수 있도록 한다.

2단계 : 일반 사용자가 슈퍼유저로 권한을 얻는 경우 su 명령어나 setuid 프로그램을 이용할 것이다. 이러한 경우 로깅 프로세서에서는 로그 프로세스 정보를 커널에서 가져올 때마다 UID와 TTY를 검사하여 콘솔이 아닌 곳에서 일반 사용자가 슈퍼유저의 쉘 권한을 획득하는 것을 감시한다. 내부 사용자의 로깅 프로세스를 기록하여 활동을 감시한다.

3단계 : 침입자는 자신의 활동이 기록되는 것을 감추기 위해 감사 로깅 프로세서의 작동을 중지하려고 시도 하거나 프로세스를 종료시키고 로그 파일을 변경 또는 삭제 하려 할 것이다. 이러한 공격에 대응하여 슈퍼유저 권한을 갖는 사용자라도 감사 로그 파일을 강제로 삭제 할 수 없도록 해야 한다. 또한 로그 및 감사 파일을 변조하려는 경우에는 로그 파일을 수정 할 수 없도록 로그 파일에 강제적으로 파일 잠금을 해야 한다.

4.2. 트래픽 폭주 공격에 대한 역추적

이동단말을 이용하여 인터넷에서 발생 가능한 해킹 공격에 대한 대응방안으로 TCP SYN 공격이나 ICMP ECHO 패킷 등에 대한 공격을 살펴보면 많은 양의 트래픽이 네트워크나 특정 목적지로 트래픽이 전달되는 특성을 보이고 있다. 따라서 해킹 공격에 대한 대응 방안으로는 트래픽 폭주(congestion) 현상에 대한 종단 간 폭주 제어 및 대응 기술로 접근 할 수 있다. DoS 공격이나 DDoS 공격인 경우 하나 이상의 호스트로부터 네트워크상의 목적지 호스트로 많은 양의 트래픽이 전달되는 형태이기 때문에 인터넷에서

의 해킹 공격에 대응하기 위해서는 DoS , DDoS 트래픽 특성을 파악하고 이를 차단하는 방식을 적용할 필요가 있다.

라우터에서의 DoS, DDoS 트래픽 제어 기술은 ACC (Aggregate-based Congestion Control) 및 pushback 기술을 사용하는데. 라우터에서 주기적으로 네트워크 트래픽에 대한 모니터링 과정을 수행 하면서 기존의 침입자에 대한 공격 DB와의 실시간 비교를 통해 Blue, Yellow, Orange, Red 등급으로 분류한다.

만일 Yellow에 해당된다면 감시를, Orange, Red등급이라면 즉시 라우팅의 부하를 줄이면서 역추적을 실시한다. 이때, 사용되는 자율 시스템(AS, Autonomous System)의 AS번호는 2바이트(0~65535)로 구성되어 있는데, 64512~ 65534까지는 사설 AS번호로 내부 네트워크에서 BGP(Border Gateway Protocol)를 적용할 때 사용된다.

AS번호를 사용하면 라우터에서 인접 AS에 대해 검증 정보를 관리하고 인증 과정을 수행하면서 결과적으로 라우팅 테이블에 저장되어 있는 정보를 신뢰하게 된다. 검증 절차를 사용함으로서 AS가 자신의 라우팅 정책과 도달 가능성 정보를 책임 있게 배포 할 수 있다.

따라서 Orange, Red 등급에 대한 AS 시스템들의 라우터 사이에서 연계 트래픽 통제 및 관리를 통해 네트워크에 부하를 줄이고, 외부 네트워크와의 단일 경로를 교환하므로 신뢰성을 가질 수 있으며, 고유한 라우팅 정책을 구현하여 관리의 효율성을 가질 수 있다.

4.3 침입 유도 시스템과 텍스트 필터링 역추적

침입 유도 시스템에는 허니팟(Honeypot)[15], 피쉬볼(Fishbowl) 등이 있다. 허니팟, 피쉬볼 등의 시스템은 침입자가 발견되었을 때, 이 침입자가 시스템의 중요한 자료가 있는 곳으로 접근할 수 없도록 하거나 공격 형태의 분석 및 역추적을 위해 침입자를 유인하는 가상의 서버 시스템이다. 침입자가 취약점을 가진 컴퓨터를 선택하기 위해 많은 수의 컴퓨터를 조사하게 된다. 이 과정에서 허니팟, 피쉬볼은 침입자의 출현을 감지하여 의도적으로 만든 취약점을 드러내 침입자를 유인한다.

침입자가 출현하면 허니팟 시스템이 작동하여 침입자를 유인하며, 그림 9처럼 유인된 침입자의 로그 기록과 IP 등은 Ethereal 등의 프로그램[16]을 통해 TCP/IP패킷에 대한 자료를 확보 할 수 있다.

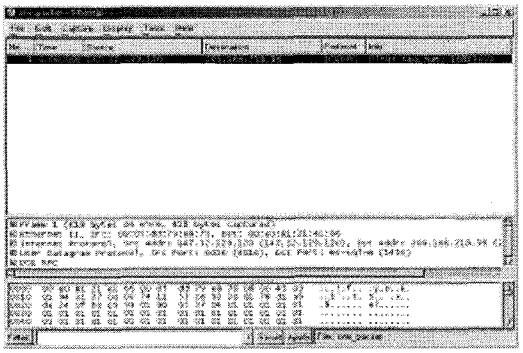

그림 9. Ethereal에서 패킷 캡처
Fig. 9. Captured Packets in Ethereal

또한 베이지안 필터링을 응용한 특정의 출발지 주소나, 목적지 주소, 특정 단어 및 평소 트래픽의 임계점을 넘을 때 즉시 와이브로 이동단말의 역추적을 실시한다. 이때 텍스트 필터링 규칙은 학습된 데이터에 대해서 분석 꼬리표를 달아놓으면 규칙이 수정하여 작동하며, 침입자 및 해커에 대한 인공지능적인 방법으로 규칙을 생성 할 수 있다. 실시간으로 생성된 규칙을 통해 필터링된 이동단말에 대한 패킷은 즉시 역추적 대상이 되며, 역추적과 동시에 AS 시스템의 라우터나, 방화벽 IPS와 연결을 통해 즉시 트래픽과 패킷이 통제된다.

4.4 침입 이동단말에 대한 포렌식자료 확보

이동단말에 대한 역추적을 실시한 후에 포렌식 자료를 생성하기 위해 휴대폰 제조사에서 제공하는 툴을 활용하여야 한다. 모바일 포렌식 분석 도구[17] 뿐만 아니라 기본적인 디지털증거와 내장 메모리에 있는 파일을 직접 추출 해내기 위하여 휴대폰 분석 툴인 QPST를 실행하여 그림 10과 같이 내장 메모리의 루트 디렉토리 등의 자료를 추출할 수 있다.

WiBro 이동단말에서 추출한 디지털증거 파일 은 일반 텍스트 파일이 아닌 관계로 일반 PC 워드에서는 확인 할 수가 없어서 헥사코드 분석 툴인 Ultra Editor를 통하여 이동단말에서 추출된 SMS 메시지의 내용, 발신자 전화번호 및 일시의 확인 자료의 추출 및 포렌식 자료로의 저장이 가능 하였다.

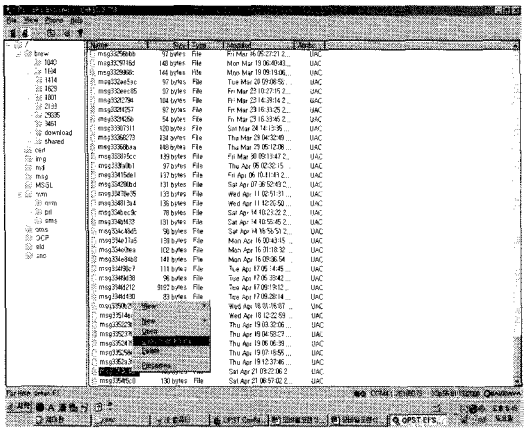

그림 10. 와이브로 이동단말에서 디지털 증거 추출
Fig. 10. Digital Evidence abstraction of WiBro Mobile Station

V. 결론

본 논문에서는 기존의 역추적 기술을 연구하고, 분석하여 WiBro 이동단말 네트워크 시스템에서 해커의 공격 이동단말에 대한 역추적을 실시하였다.

WiBro 이동단말을 이용한 해커의 공격에서, 본 논문은 로그인 세션동안 다양한 응용 프로세스를 실행할 때 응용 프로그램의 수행 내역에 대해서 운영체제의 커널로부터 직접 로그 정책을 관리하고, 네트워크상에서 로그 기록인 사용자의 로그인, 로그아웃 정보와 명령어 실행 정보를 3단계로 나누어 관리하고 기록함으로서 침입자에 대한 역추적을 효율적으로 설계하였다.

역추적 설계 시에 네트워크의 트래픽 폭주공격인 DoS공격, DDoS공격에 대해서는 AS 시스템을 이용한 패킷의 통제와 관리로 WiBro 이동단말을 통한 해킹 공격으로부터 안전하게 보호할 수 있도록 설계 하였다.

또한 WiBro 이동단말을 이용한 해커의 공격에서 보안이 설정된 AS 망을 통과하는 모든 응답 패킷을 텍스트 필터링을 하였고, 네트워크를 통해 들어온 패킷의 경로를 재구성하는 알고리즘을 적용하여 신뢰성 있는 연결 체인을 구성하고 IP의 Payload 패킷을 분석하여 Blue, Yellow, Orange, Red 경고 시스템을 구성하고 패킷을 단계별로 구분하여 Yellow 단계에서는 감시를 하고, Orang 등급과 Red등급은 즉각적인 이동단말에 대한 역추적을 실시하였다.

역추적 실시 후에 로그 기록과 감사 자료를 실시간으로 DB에 반영하고, 네트워크 트래픽을 분산시켜 네트워크 시스템의 안정성을 강화 시켰으며, 해커가 입력하여 발생하는 데이터 발생 빈도 및 특정 데이터를 조사하여 인공지능적인 학습 효과를 이용한 보안 규칙들을 만들어, 신뢰성 있는 역추적 시스템으로서 가치를 평가 받을 수 있다.

또한 침해 사고가 발생하였을 경우에, 역추적과 함께 보안 감사 자료로써, 모바일 포렌식 자료나, 이동단말 포렌식 자료를 생성하여 전체적인 WiBro 이동단말 네트워크 시스템의 안정성 확보와 보안성 강화를 할 수 있다.

향후 연구에서는 유비쿼터스와 IPv6 환경에서의 이동단말에 대한 실시간 역추적 및 포렌식 자료 생성에 대한 연구가 필요하다.

참고문헌

[1] IEEE 802.16a. http://www.ieee802.org/16/tga/. April 2003.

[2] 박대우, 박종진, 전문석. "이동단말사용자의 이동패턴모델 평가에 관한 연구". 한국통신학회논문지. 2002.12.

[3] K. Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders," In F. Guppens, Y. Deswarte, D. Gollamann, and M. Waidner, editors, 6th European Symposisum on Research in Computer Security - ESORICS 2000 LNCS -1985, Toulouse, France, Oct. 2000.

[4] H.T. Jung et al. "Caller Identification System in the Internet Environment.,"Proceedings of the 4th Usenix Security Symposium, 1993.

[5] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent," FIRST Conference on Computer Security Incident Handling & Response 1999.

[6] Steven R. Snapp, James Brentano, Gihan V. Dias, "DIDS(Distributed

[7] S. Staniford-Chen and L.T. Heberlein. "Holding Intruders Accountable on the Internet,"In Proceedings of the 1995 IEEE Symposium on Security and Privacy, 1995.

[8] Y. Zhang and V. Paxson, "Detecting Stepping Stones,"Proceedings of 9th USENIX Security Symposium, Aug. 2000.

[9] D. Schnackenberg, K. Djahandari, and D. Sterene, "Infrastructure for Intrusion Detection

and Response,"Proceedings of DISCEX, Jan. 2000.

[10] D. Schnackenberg, K. Djahandary, and D Strene, "Cooperative Intrusion Traceback and Response Architecture(CITRA),"Proceedings of the 2nd DARPA Information Survivability Conference and Exposition(DISCEXII), June 2001.

[11] 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005.11.

[12] 보안정보/사고노트/WMF 취약점 관련 악성코드 유포 웹사이트 및 메일서버 분석 사례. http://www. krcert.or.kr/index.jsp. 2006.1.

[13] 박대우, 임승린. "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구." 한국컴퓨터정보학회논문지, 제11권 제2호, pp44-50, 2006. 5.

[14] McAfee. "White Paper_Host and Network Intrusion Prevention." http://www.mcafee.com/us/local_ cotent/white_papers/wp_host_ nip.pdf, February,2005.

[15] http://www.honeynet.org/papers/enemy/ddos.txt. 2007.

[16] 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, 2006. 9.

[17] Williamson,B, "Forensic Analysis of the Contents of Nokia Mobile Phones", School of Computer and Information Science Edith Cowan University Perth, 2005.

저 자 소 개

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

임 승 린

1979년 숭실대학교 컴퓨터학과 졸업(학사)
1987년 숭실대학교 대학원 컴퓨터학과 졸업(석사)
1999년 숭실대학교 대학원 컴퓨터학과 졸업(박사)
1989년 수원과학대학 현재 컴퓨터정보과 교수
〈관심분야〉 응용S/W, 정보시스템, DataBase, 컴퓨터 네트워크, 인터넷 시스템, 지식관리시스템,