韓國 컴퓨터情報學會 論文誌
第13卷 第1號, 2008. 1.

2008-13-1-3-2

우회적인 공격에 대한 실제 IP 역추적 실시와 포렌식 자료 생성

윤 병 선*, 김 동 준**, 양 해 술***

A Study on Real IP Traceback and Forensic Data Generation against Bypass Attack

Byung-Sun Youn*, Dong-Jhoon Kim**, Hae-Sool Yang***

요 약

본 논문에서는 자신의 Real IP 주소의 노출을 피하기 위하여 우회적인 공격을 하는 침입자를 대상으로 하여 IP 역추적을 실시한다. Real IP 역추적을 위하여 IP 역추적 서버와 에이전트 모듈을 설계하고 실험실 인터넷 네트워크 시스템에 설치한다. 우회 접속자의 공격 탐지 및 추적 범위를 설정하고, 실제 공격을 하여, 일반적인 IP 접속 자료와 침입탐지 후에 치명적인 공격으로 차단된 Real IP 자료를 생성하여 DB에 저장한다. 공격자의 Real IP는 Whois 서비스로 실체를 확인하고, 이를 법정의 증거자료로 삼기위한 무결성과 신뢰성을 확보한 Forensic 자료를 생성한다. 본 논문 연구를 통하여 유비쿼터스 정보화 사회의 역기능인 사이버 범죄의 예방효과와 효과적인 Real IP 역추적 시스템을 제시하고, 법의 처벌에 대한 Forensic 자료 생성 기준을 확보한다.

Abstract

Execute IP traceback at this paper as target an intruder's attacking that Bypass Attack in order to avoid an exposure of own Real IP address. Design IP traceback server and agent module, and install in Internet network system for Real IP traceback. Set up detection and chase range aggressive loop around connection arbitrariness, and attack in practice, and generate Real IP data cut off by fatal attacks after data and intrusion detection accessed general IP, and store to DB. Generate the Forensic data which Real IP confirms substance by Whois service, and ensured integrity and the reliability that buy to early legal proof data, and was devoted to of an invader. Present the cyber criminal preventive effect that is dysfunction of Ubiquitous Information Society and an effective Real IP traceback system, and ensure a Forensic data generation basis regarding a judge's robe penalty through this paper study.

▸ Keyword : Forensics, Intrusion Detection, IP Traceback, Real IP, Ubiquitous Security.

• 제1저자 : 윤병선, 교신저자 : 김동준
• 접수일 : 2007. 11. 16, 심사일 : 2007. 12.15, 심사완료일 : 2008. 1.25.
* 호서대학교 벤처전문대학원 **배화여자대학 비서행정과 교수 ***호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

컴퓨터와 정보통신의 급속한 기술 발달과 인터넷 인프라의 확충으로 인터넷을 이용한 업무사용의 보편화, 전자상거래의 확산 등 편리함과 신속한 업무처리, 새로운 산업의 창출 등 많은 혜택을 누리고 있다. 그림 1처럼 우리의 일상생활이 컴퓨터와 연계된 유비쿼터스(Ubiquitous) 정보화 사회의 실현[1] 등으로 국가, 기업, 개인 모두에게 정보보안의 중요성은 더욱 증대될 것으로 기대된다.

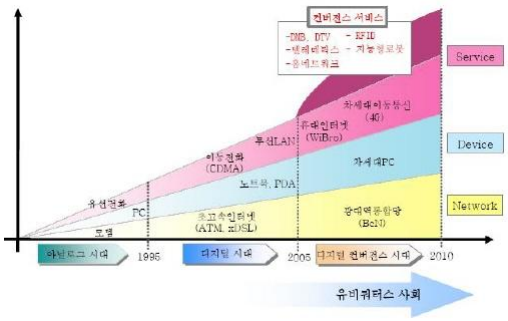

그림 1. 유비쿼터스 정보화 사회의 전망
Fig. 1. A prospect df Ubiquitous Information Society

유비쿼터스 정보화 사회에 대한 역기능으로 불법적인 해킹, 정보유출, 프라이버시 침해, 금융적인 피해 등이 지속적으로 확산되고 있다. 또한 국경을 넘어선 해킹문제로 국익이 침해되고, 개인정보와 기업정보 및 국가기관이나 공공기관 등의 정보보안 문제도 더욱 증가할 것이다.

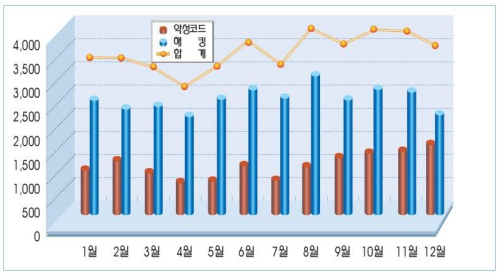

그림 2. 2006년도 국내 침해사고 월별 발생 현황
Fig. 2. The occurrence present situation by an infringement accident month domestic 2006.

그림 2처럼 2006년 사이버 침해사고 월별 발생[2] 원인을 살펴보면 다양해지고 고도화된 해킹수법의 진화를 통해 바이러스 침투[3] 및 해킹에 의한 사고가 증가하고 있다.

취약점[4]으로는 보안패치 미흡, 홈페이지 보안 취약점 방치, 취약한 패스워드 설정 등 기본적인 보안관리 사항 미흡과 웹 방화벽, PMS(Patch Management System), VMS(Virus Management System) 등과 같은 최신 정보보호제품 구비 미흡, 전문 인력 부재, 정보보호에 대한 전반적인 투자부족 등이 간접적인 취약성 원인으로 파악되었다.

또한 인터넷 네트워크를 통한 컴퓨터 시스템의 침입은 불법적인 침입자로부터 시작된다. 우회적인 사고들은 컴퓨터를 공격할 때 IP Spoofing 공격, DoS공격, DDoS공격, DRDOS 공격[5]처럼 복잡한 경로를 거쳐 서 목표 컴퓨터에 접근하고, 이메일, 유해성 게시물을 통한 접속, 웹서버의 권한 탈취를 위한 해킹, 금융거래 접속의 유형으로 침입하기 때문에 침입자의 처음 위치를 식별하기가 어렵다.

이러한 해커의 공격에 대항하기 위해 해커인 침입자를 효율적으로 추적하는 IP 역추적 방안[6]이 필요하며, 또한 추적과 동시에 시스템에 감사 로깅 이용 내역을 기록하여 포렌식(Forensic)[7]자료를 생성하는 호스트와 네트워크 보안 시스템[8]에서의 기록이 필요하다. 또한 인터넷 네트워크 시스템의 안정성을 높이기 위한 분석 도구들을 사용하여 시스템 내에서 수행된 각종 응용프로세스, 외부 통신망을 통해 접근하여 수행된 작업 내역 등의 정보를 기록하고, 해커의 침입에 대한 IP 역추적 정보는 실시간으로 저장하여 추후에 Forensic 자료로서 무결성[9]을 확인하거나, 감사 정책의 효과적인 적용여부를 분석 자료로 제공하여 침입자를 추적하는 방안이 연구 · 제시되어야 한다. 또한 침입자가 침입을 하고, 불법적인 행동 자료를 Forensic 자료로서 법정에 증거자료로 제시하여 채택되게 하는데 어려움이 있다.

본 논문에서는 이러한 네트워크 보안침해 사고에 대응하기 위한 해커의 IP 역추적 방법을 제안하며 공격자의 불법적인 행동에 대해 수사하고 불법 행위에 처벌을 위한 재판의 증거자료로 IP 역추적과 역추적 실시 후의 Forensic 자료를 생성하여 무결성과 신뢰성을 검증 할 수 있는 방안을 연구한다.

2장 관련연구에서는 해커의 우회적인 공격 증가, IP 역추적 기법으로 전향적 기법과 대응적 기법 및 포렌식에 대해 알아보고, 3장에서는 해커의 우회적인 공격에 대한 IP 역추적 모델을 설계한다. 4장에서는 Real IP 역추적을 실시하고 Forensic 자료를 생성하여 검증을 하고 5장에서 결론을 내리고 향후 연구에서 유비쿼터스와 IPv6 무선 환경에서의 역추적 방법과 기법의 필요성을 논의한다.

II. 관련 연구

2.1. 해커의 우회적인 해킹 공격 증가

2001년 이후 부터 인터넷을 통한 외부로의 해킹을 통한 공격은 90%이상이 웹 서비스 서버를 통하여 중요정보의 유출 및 해킹이 빈번하게 이루어지고 있다. 해킹을 시도하거나 불법적인 행위를 하는 인터넷 사용자는 대부분 자신의 IP를 숨기고 우회하여, IP spoofing 공격, DoS 공격, DDoS 공격, DRDOS 공격처럼 접속된 웹 서버에 자신의 기록을 남기지 않거나, 남겨도 변조되거나 우회 접속하여 공격한다.

그림 3처럼 이때 피해를 입은 웹서버로 부터는 실제 일어난 침해사고에 대해 정확한 발원지를 증명 할 수 없어서, 해커의 침입과 해악으로부터 예방과 피해 발생 후 처벌이 어려운 상황이다.

해외로 부터의 발원 및 경유를 통해 이루어지는 해킹 및 정보유출은 공공부문과 금융부문의 인터넷뱅킹 및 전자금융거래와 게임, 포탈, 인터넷쇼핑몰, 일반기업 등 까지도 사고를 당하고 있다.

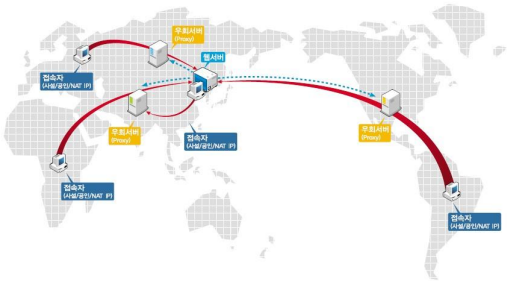

그림 3. 우회 접속 개념도
Fig. 3. A bypass connection key map.

2.2. IP 역추적 기법

IP 역추적기법에는 전향적 역추적기법과 대응적 역추적기법으로 나누어 볼 수 있다[10].

2.2.1. 전향적 역추적 기법

인터넷상에서 침해, 공격하는 해커에 대한 IP 역추적 기법에는 hop-to-hop 역추적 방식에 해당하는 링크 검사법, 라우터에서 전송된 패킷에 대한 특성 등을 기록해 놓은 후에 데이터 마이닝 등의 추론 시스템을 적용하여 공격 근원지를 검출하는 로깅 기법, 스푸핑(spoofing)된 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 PPM 기법, 라우터에서는 일반적 $\frac{1}{20,000}$의 확률로 패킷을 샘플링 하여 iTrace 메시지를 생성하고 이를 패킷의 목적지 IP로 전송하는 iTrace(ICMP Traceback)기법 등이 있다.

2.2.2. 대응적 역추적 기법

오버레이 네트워크 역추적 기법은 역추적 라우터 TR(Tracking Router) 모듈을 네트워크에 별도로 설치하는 방법이고, 해쉬기반 역추적 기법은 SPIE(Source Path Isolation Engine) 기반 역추적 서버를 구성하고 전체네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 네트워크 시스템을 관리한다.

2.3. 포렌식

최근의 사이버 범죄는 공공기관 메일인 것처럼 가장해 개인의 주민등록번호나 계좌번호, 신용카드번호를 입력하게 만드는 피싱(Phishing)이나, 아예 비슷한 사이트로 위장해 접속을 유도한 뒤 개인정보를 취득하는 파밍(Pharming)등 신종 사이버 금융침해사고[11]는 급격하게 증가하고 있다.

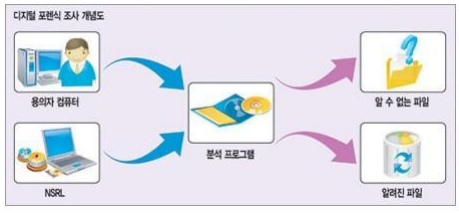

그림 4. 포렌식 개념도
Fig. 4. A Forensic key map.

그림 4처럼 포렌식은 검찰, 경찰, 국가정보원 등 수사기관에서 사이버 상에서 벌어지는 불법행위, 범죄를 수사하고 과학적인 증거 수집 및 분석기법[12]을 통해 법적인 증거를 채택하게 만드는 방법이 포렌식이다. 범행과 관련된 이메일, 핸드폰, 접속기록 등 각종 디지털 데이터와 통화기록 등을 증거로 확보, 분석하며, PC 등 컴퓨터 시스템에서 범죄 자료를 수사하는 컴퓨터 포렌식과 휴대전화, WiBro 이동단말에서의 자료를 수사하는 모바일 포렌식으로 구분 할 수 있다. 또한 포렌식은 증거수집, 증거분석, 증거제출과 같은 절차로 구분된다.

III. 우회공격에 대한 IP 역추적 설계

3.1. 현재 우회공격 상황에 대한 분석

현재 TCP/IP를 이용한 인터넷 사용에서의 해외 도메인에서 접근, 우회적인 Proxy IP, 고의적 IP 숨김 등의 공격으로 인한 기술적 한계는 현재 http(s)를 이용한 웹 서비스의 보안 문제 해결에 걸림돌이며, 웹 서버에서는 악의적 접속자에 대한 원천적인 정보를 갖지 못한다[13].

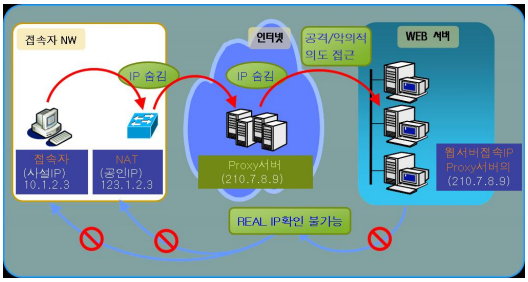

그림 5. IP 우회 공격의 설계
Fig. 5. A design of an Bypass Attack IP.

따라서 그림 5처럼 웹 서버 로그 분석 또한 직전 IP주소에 대해서만 파악이 가능하며, Real IP의 확인 어려워 직전 IP 이외의 접속자에 대한 전체 접속 경로 파악 불가능하다. 정상적인 Proxy와 비정상인 불법 Proxy에 대한 보안 정책의 적용이 어려워 Real IP 기반의 Client 접속 정보 분석 및 활용이 불가능하다.

3.2 Real IP 수집 범위 및 기술 설계

3.2.1. 우회 접속자의 공격 탐지 및 추적 범위

인터넷에서 해커의 Real IP 주소를 숨기고 목표 웹서버에 우회 접속하여 이메일, 유해성 게시물을 통한 접속을 하고, 웹서버의 권한 탈취하여 해킹으로 이어진다. 따라서 그림 6처럼 IP 탐지 및 추적 범위에 대한 설계가 필요하다. 본 연구에서는 웹서비스, 금융, E-mail 추적[14]을 통한 포렌식 자료의 생성 까지를 범위를 설정한다.

3.2.2. Real IP 수집 기술 설계

위 3.1의 문제점을 해결 할 수 있는 첫 번째 방안은 접속 침입자에 대한 실시간 Real IP의 확인이다. TCP/IP 구조상

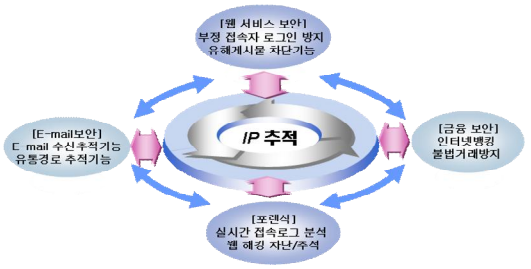

그림 6. IP 추적 범위의 설계
Fig. 6. A design of IP traceback range.

서버에 접속하는 접속자의 최종 IP 주소만을 알 수밖에 없는 인터넷 기술의 한계를 극복하기 위해서, 접속자의 Local IP (사설/공인), NAT IP(공인), 우회 IP(Proxy IP)를 모두 정확히 탐지하도록 설계해야 한다. 본 연구에서는 Real IP 정보를 모두 제공하는 BPBT(Browser Plug-in Based Technology)기술[15]을 이용하여 정보유출의 근원인 외부 네트워크로 부터의 해킹 접근 위치를 정확히 파악하여 Real IP 정보를 통해서 탐지 정책을 적용하여, 탐지 후에 침입방지를 유도하거나 침입차단을 할 수 있도록 연계[16]되어져야한다. 또한 접근제어에 의한 접근차단 정책을 적용하기가 어려울 때는 사후에라도 해킹 발원지에 대한 네트워크에서 IP 추적[17]을 실시하여 정확한 Real IP를 확보 할 수 있어야 한다.

Real IP 모니터링은 고객이 상시 제공하는 중요 웹 서비스를 대상으로 하므로 대규모의 접속자가 발생하더라도 웹 서비스의 성능과 속도에 영향을 주지 않고 웹 서비스와는 독립된 구조로 구성되어 Real IP 모니터링 기능을 제공하여야 한다.

3.3. Real IP 역추적 시스템 설계

그림 7처럼 접속자의 Real IP 역추적을 위한 IP 역추적 시스템을 설계한다.

3.3.1 IP 역추적 에이전트 모듈 설계

Real IP 확인을 위해 목표가 되는 웹 페이지와 게시판, E-mail 서버 등에 IP 역추적 에이전트 코드를 설치하여 해당 웹 페이지 접속 시에 Real IP Plug-in을 실시한다. 웹 페이지의 접속자 웹 브라우저에서 정보를 수집한다. JAVA와 Flash 등 BPBT 기법과 다단계 브라우저 플러그 인 기술을 사용하여 Real IP인 사설 IP, 공인/NAT IP, Proxy IP의 정보와 함께, 운영체제나 브라우저 종류 및 버전 등 접근자의 일반적인 브라우저 정보를 수집한다.

3.3.2 IP 역추적 시스템 서버 모듈 설계

IP 역추적 시스템 서버 모듈은 IP 수집서버 모듈과 IP 저장을 위한 DB 및 관리서버 모듈로 구성되는데 IP 수집서

버 모듈은 에이전트에서 확인된 정보를 수집(gathering)하는 FEP 서버로서 대용량 트래픽의 처리를 위해 병렬처리인 Multi-Thread 방식으로 설계한다.

에이전트 데이터 통신 시 데이터 인증 과정을 통해 무결성의 데이터를 수신하며, 관리서버 인증부분을 청구하고 동시에 에이전트 데이터의 통신 시에도 암호화를 실시한다. 유해게시물에 대한 차단 정보를 제공하고 수집된 데이터를 암호화하여 DB에 저장한다.

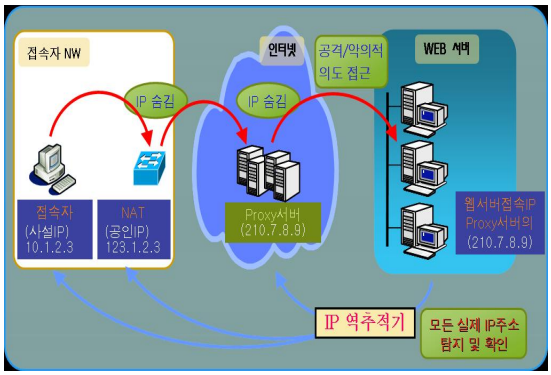

그림 7. IP 역추적 설계 구성
Fig. 7. IP Traceback System design configuration.

IV. Real IP 역추적 실시와 포렌식 자료 생성

해커의 우회적인 공격으로부터, 침입탐지를 실시하고, IP 역추적 시스템을 통한 Real IP 역추적을 실시한다. 탐지된 Real IP 정보 등을 DB에 암호화하여 저장하고, Forensic 자료로 사용하기 위해, 그림 8처럼 공격하는 상황을 구성하여 공격을 한다.

4.1. 실험 환경 설정

서버 및 네트워크에서 IP 역추적 시스템 실험 환경은 다음과 같다.

* 서버 환경 : CPU : Intel Xeon 3.0GHz 2 CPU, Memory : 4GB, HDD : Ultra SCSI 143GB * 2 개, NIC : 10/100/1000 * 2개, OS : Windows, DB : MS SQL
* 에이전트 프락시서버 타입별 환경 : Transparent, Anonymous, High Anomity Mode 설정
* 네트워크 : NIC : 10/100 8개 중 2개의 Giga Port, 자체 보안 및 이중화 용 L7 스위치.

4.2. 네트워크에서 IP 접속 자료 수집

실험에서 인터넷을 통한 해커를 설정하고, Real IP 주소를 숨겨서, 목표 서버에 우회 접속하여 이메일, 유해성 게시물을 통한 접속, 웹서버의 권한 탈취를 위한 해킹, 금융거래 접속의 유형으로 나누어 접속하였다.

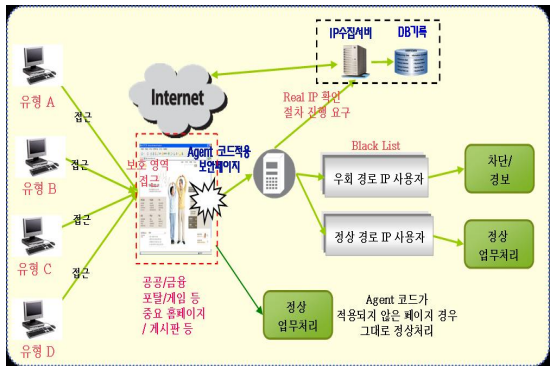

그림 8. 우회 공격에 대한 IP 역추적 시스템 구성
Fig. 8. IP Traceback System configuration regarding an bypass attack.

그림 9에서 접속자에 대한 일반적인 실시간 모니터링을 하였다. 여기에서는 목표 서버에 우회 접속하여, 최종 접속지에 대한 IP는 화면에 모니터링 되고 있으나, 침입자에 대한 Real IP는 추적이 이루어 지지 않는 것이 확인 되었다.

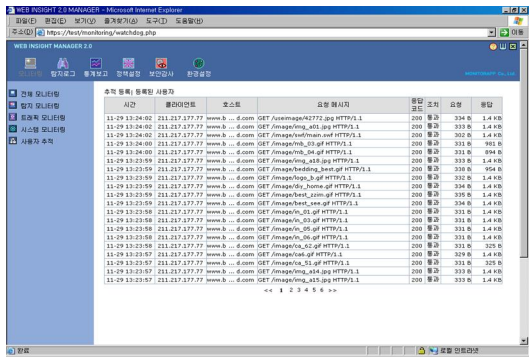

그림 9. 접속자에 대한 일반 모니터링
Fig. 9. General monitoring regarding connector.

4.3. 네트워크에서 Real IP 역추적 자료 수집

실험 시스템에 IP 역추적 시스템 서버를 설치하고, 각 단말에 에이전트 모듈을 인스톨하였다. 그리고 인터넷을 통한

해커역할은 Real IP 주소를 숨기기 위해 목표 서버에 우회 접속하여 이메일, 유해성 게시물을 통한 접속, 웹서버의 권한 탈취를 위한 해킹, 금융거래 접속의 유형으로 나누어 공격을 시도 하였다.

그림 10. IP 역추적 서버에 접속된 탐지 에이전트 기록
Fig. 10. The detection agent record which was accessed to IP Traceback Server.

그림 10에서 침입자에 대한 접속자의 시간과 목표 서버, 공격유형, 공격위험도 및 공격에 대한 조치가 실시간 IP 역추적 서버에 접속된 탐지 에이전트에 탐지되고 있다.

이때 침입차단 서버가 가동되어 정상적인 패킷은 Green 등급으로, 의심이 가는 경우에는 Yellow 등급으로 감시하고, 오용 탐지(Misuse Detection)기반과 한계치 제어(Threshold Control)를 벗어난 비정상적인 트래픽이 유입되었을 때에는 위험도를 Orange와 Red 등급으로 판정하여 Red 등급으로 분류된 패킷을 실시간으로 차단하고 있다. Red 등급의 치명적인 공격자로 판명된 침입자에 대한 IP 역추적을 실시하였다.

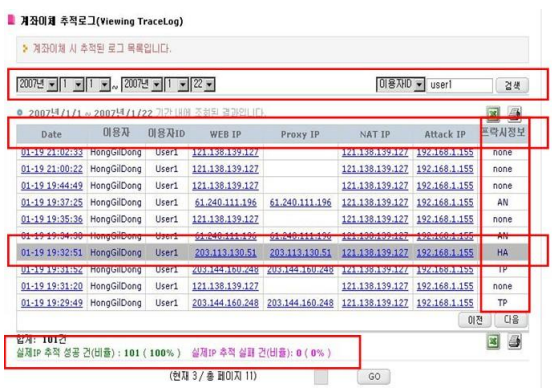

그림 11. Real IP 역추적 기록
Fig. 11. The Real IP Traceback Record

4.4. Real IP 역추적으로 침입자 확인

해커로 추정되는 Red 등급의 치명적인 공격자로 판명된 접속자에 대한 IP 역추적을 실시한 결과 그림 11처럼 Real IP인 웹 브라우저 IP(203.113.130.51) 추적되었고, 사설 IP(192.168.1.55), 가상 NAT IP(121.138.139.127), Proxy IP(203.113.130.51)의 정보와 함께, 접근자의 접속 시간과 차단된 시간 등이 실시간 자료로 나타나 저장되고 있다.

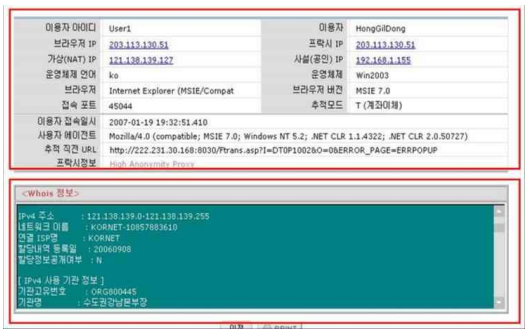

그림 12. Whois 서비스를 이용한 Real IP 확인 작업
Fig. 12. The Real IP confirmation that used Whois service.

그림 12에서는 대한 IP 역추적 자료를 토대로 하여, Whois 서비스를 이용한 Real IP 확인 작업을 수행 하였다. 이 결과 해커로 실험하였지만 IP를 숨기고 우회적인 공격을 시도 하였던 Real IP와 일치함을 보였다. 따라서 해커의 우회적인 공격으로 인한 Real IP 역추적의 시험은 성공 한 것으로 판명되었다.

4.5. 포렌식 자료 생성

Real IP 역추적에 성공하여 침입에 대한 공격이 확인된 자료가 법정에서 증거로 채택되기 위해서는 증거 자료의 무결성과 신뢰성이 확보되어야 한다.

따라서 네트워크에서 수집된 자료가 Forensic에 대한 표준 절차뿐만 아니라 증거 수집 및 분석의 사용된 Forensic 툴에 대한 검증 절차도 진행된다. 이 때문에 디지털 포렌식 과정에서 원본 데이터의 신뢰성을 확보하는 것이 가장 중요한 문제이다. 법률적으로 수사방법에서 범행 현장을 그대로 보존하는 것과 같은 논리이다.

4.5.1. 포렌식 자료 수집

포렌식 자료 생성과정에서 인터넷 네트워크에 로그인 세션

동안 다양한 응용 프로세스를 실행할 때 응용 프로그램의 수행 내역에 대해서 운영체제의 커널로부터 직접 로그 정책을 관리하고, 네트워크상의 사용자의 로그인, 로그아웃 정보와 명령어 실행 정보를 3단계로 나누어 관리하고 기록하여 침입자에 대한 역추적을 시행한다.

또한 네트워크에서는 주변 라우터에 대한 검증 구조를 제공해서 BGP 라우터에 의해 전체적인 라우팅 정보를 항상 정확하게 관리할 수 있으면 안전성이 향상된 라우팅 환경을 기초로 패킷에 대한 역추적 정보 등을 제공한다면 보안 기능이 강화된 라우터를 근간으로 DoS 공격과 DDoS 공격이 발생하였을 경우 공격자에 대한 역추적 근원지에 대한 신뢰성을 확보 할 수 있다.

또한 보안 강화된 AS 망을 통과하는 모든 응답 패킷에 워터마크를 삽입[18]하여 네트워크를 통해 들어온 패킷의 경로를 재구성 하는 알고리즘을 적용[19]하여 신뢰성 있는 연결체인을 구성[20]하고 IP의 Payload 패킷을 분석하여 Green/Yellow/Orange/Red 경고 시스템을 구성[21]하고 패킷을 단계별로 구분하여 네트워크의 부하를 줄일 수 있으며, 해커가 입력하여 발생하는 데이터 발생 빈도 및 특정 데이터를 조사하여 패킷 필터링의 학습 효과를 이용한 정교한 규칙들을 만들어 간다면 신뢰성 있는 역추적 시스템으로서 차후에 침해 사고가 발생하였을 경우 각각의 단계에서 얻어진 데이터를 Forensic 자료를 실시간으로 생성하여 무결성을 검증 할 수 있다.

자료 수집으로 일반적인 브라우저 정보를 수집한다. 위험도를 Red 등급으로 판정된 패킷을 차단하고 있다. 수집된 데이터에서 수사에 필요한 유용한 정보를 끌어내는 것이다. 일부 데이터는 숨겨져 있을 수 있기 때문에 삭제된 파일을 복구하거나 암호화된 파일을 해독하는 기술이 활용된다.

4.5.2 포렌식 자료 분석

Forensic 자료를 생성하기 위해 증거 분석에 활용되는 툴은 여러 가지가 있는데 일반적으로 삭제된 파일을 되살리는 복구 툴, 변형된 파일을 원본 파일로 확인할 수 있는 툴 등이 사용된다. 사진이나 동영상 등 파일 확장자를 'JPEG' 'AVI' 에서 'HWP', 'DLL'등 다른 확장자로 만들어 놓으면 윈도우 탐색기에서는 그 파일의 존재를 찾을 수 없다. 하지만 포렌식 툴을 사용하면 원본 파일 그대로 검색이 가능하다. 일부 데이터를 윈도우에서 숨김 속성을 해 놓거나 파일 확장자를 바꿨을 때는 포렌식툴이 이런 파일을 찾아준다. 보통 하나의 파일 형식은 하나의 파일 확장자와 식별자(Identifier)라 불리는 유일한 값을 가지는데 이 식별자는 파일 생성 시 헤더의 자동으로 저장된다. 따라서 확장자를 바꿀 경우 파일 확장자와 식별자가 일치하지 않으므로 이런 방법을 통해 확장자가 바뀐 파일들을 찾을 수 있다.

4.5.3 포렌식 자료 생성

그림 13과 같이 침입 탐지에 대한 로그 기록을 분석하여 침입자의 공격에 의한 시간과 범죄 사실을 발생시킨 사건에 대한 공격타입과 보안조치에 대한 자료를 확보한다. 여기에는 에이전트에서 수집된 클라이언트에서의 Real IP 역추적에 대한 근거 자료가 표시된다.

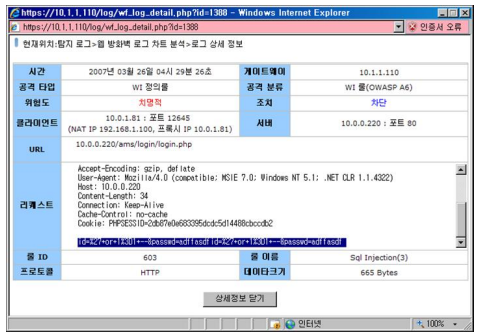

그림 13. 침입 탐지에 대한 로그 기록 분석
Fig. 13. Log record analysis regarding an intrusion detection.

침입자가 남긴 공격타입과 보안조치에 대한 자료에 대한 로그 기록과 일치한 자료는 암호화되어 전송되며, 암호화된 상태로 DB에 저장된다.

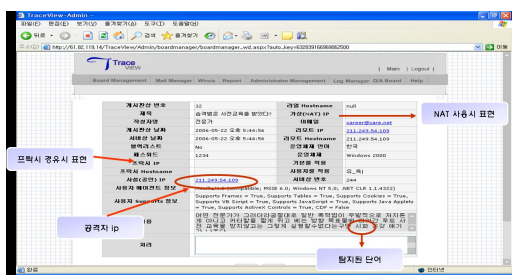

그림 14. IP 역추적 Forensic 생성 자료
Fig. 14. IP Traceback for Forensic generation data.

그림 14에서는 위 침입자의 불법적인 공격에 대한 자료를 토대로 하여 DB에서 암호화와 해싱을 된 자료를 복호화하여 검증한 다음 자료를 추출하면 포렌식 자료로서 무결성을 확보

하게 된다. 또한 그림 13에서의 침입자의 불법적인 공격시간과 그림 14의 자료의 저장에서 나온 시간이 일치함을 증명함으로써, 포렌식 자료로서 신뢰성을 확보하게 된다.

V. 결론

본 논문에서는 유비쿼터스 정보화 사회에 대한 역기능으로 불법적인 해킹, 정보유출, 프라이버시 침해, 금융적인 피해 등이 지속적으로 확산되고 있는 상황에서 자신의 Real IP 주소의 노출을 피하기 위하여 우회적인 공격을 하는 침입자를 대상으로 하여 IP 역추적을 실시한다.

Real IP 역추적을 위하여 시스템을 위하여 IP 역추적 서버와 에이전트 모듈을 설계하고 실험실 인터넷 네트워크 시스템에 설치한다. 우회 접속자의 공격 탐지 및 추적 범위를 설정하고, 실제 웹서비스 보안, 금융보안, E-mail 보안등의 공격을 실시하였다. 일반적인 IP 접속 자료와 침입탐지 후에 치명적인 공격은 Green, Yellow, Orange, Red 등급으로 분류하여 Red 등급으로 분류되어 차단된 패킷의 Real IP 자료를 실시간으로 암호화와 해싱을 하고 DB에 저장한다.

공격자의 Real IP는 Whois 서비스로 실체를 확인하고, 이를 법정의 증거자료로 삼기위해서 암호화와 해싱을 통한 전송 및 저장으로 무결성을 확보하고, 공격 시에 저장된 시간과 DB에서 저장된 자료의 추출을 통해 확인한 자료의 시간의 일치성을 확인하여 신뢰성을 확보한 Forensic 자료를 생성에 성공 하였다.

본 논문 연구를 통하여 유비쿼터스 정보화 사회의 역기능인 사이버 범죄의 예방효과와 효과적인 Real IP 역추적 시스템을 제시하고, 절차를 표준화하여 법의 처벌에 대한 Forensic 자료 생성 기준을 확보하였다.

향후 연구에서는 유비쿼터스와 IPv6 환경에서의 다양한 해커의 침입에 대한 실시간 Real IP 역추적에 대한 연구와 포렌식 자료의 생성 및 수사에서의 활용 방안에 대한 연구가 필요하다.

참고문헌

〔1〕 http://www.nca.or.kr 김창곤(한국전산원 정보화기획단 u-전략팀). 2006.10.

〔2〕 한국정보보호진흥원, 2006년 해킹바이러스 통계-KrCERT. 2007. 9.

〔3〕 Peter Szor. "COMPUTER VIRUS RESEARCH AND DEFENSE." Addison-Wesley, May 2005.

〔4〕 Y. Zhang and V. Paxson, "Detecting Stepping Stones,"Proceedings of 9th USENIX Security Symposium, Aug. 2000.

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

〔6〕 Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, "Packet Tracker Final Report," CERIAS Technical Report 2000-23, Purdue University, 2000.

〔7〕 Kanellis, P., Kiountouzis, E., Kolokotronis, N.,& Martakos, D. (Eds.). "Digital crime and forensic science in cyberspace". Journal of digital forensic practice. Hershey: Idea Group. 2006.

〔8〕 D. Schnackenberg, K. Djahandari, and D. Sterene, "Infrastructure for Intrusion Detection and Response,"Proceedings of DISCEX, Jan. 2000.

〔9〕 이규안, 박대우, 신용태. "포렌식자료의 무결성확보를 위한 수사현장의 연계관리 방법 연구".한국컴퓨터정보학회 논문지, 제11권 제6호, pp175-184, 2006.12.

〔10〕 박대우, 임승린. "WiBro에서 공격 이동단말에 대한 역추적기법 연구"..한국컴퓨터정보학회 논문지, 제12권 제3호, pp175-184, 2007.7.

〔11〕 박대우, 서정만. "Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구".한국컴퓨터정보학회 논문지, 제12권 제2호, pp175-184, 2007.5.

〔12〕 Luoma, V. "Forensics and electronic discovery: The new management challenge". Computers & Security, 25(2), 91-96. 2006.

〔13〕 김태봉, "HTTP(S) 보안을 위한 자동추적 시스템 및 그의 방법", 아이자이어 로보텍스(특허출원 10-2004-0070329), 2004. 9.

〔14〕 김완수, "메일수신자 위치 추적 시스템 및 그의 방법", 트라이옵스 (특허등록 10-0440270-0000), 2005. 7.

〔15〕 김태봉, 최운호, "역추적 기술의 동향 및 적용 사례 분석" 한국정보보호학회, 제15권1호. 2005.2.

〔16〕 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.

〔17〕 Stefan Savage, David Wetherall, Anna Karlin "Practical Network Support for IP Traceback,"Proceedings of the 2000 ACM SIGCOMM Conference, Stockholm, Sweden, pp295-306. Aug. 2000,

〔18〕 Dawn X. Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback,"Proceedings of InfoCom 2001.

〔19〕 이준엽 외 4인, "IP역추적을 위한 새로운 접근: 패킷손실 기반의 논리적 전송경로 추정" 한국정보보호학회 논문지, 제12권 3호, 2002. 6.

〔20〕 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.

〔21〕 Deawoo Park. "A study about dynamic intelligent network security systems to decrease by malicious traffic". International Journal of Computer Science and Network Security, V.6, N.9B. pp 193-199. Sep. 2006.

저 자 소 개

윤 병 선

1985년 조선대학교 전자공학과 졸업 (학사)
2001년 현대정보기술(주) 금융사업부 수석
2005년 (주)헤럴드아이티 창립 대표이사
2006년 서울벤처정보대학원대학교 컴퓨터응용기술학과 (공학석사)
2008년 호서대학교 벤처전문대학원 IT응용기술학과 (박사과정)
〈관심분야〉 정보보호, 추적기법, 포렌식, 유비쿼터스 보안

김 동 준

1970년 고려대학교 이공대학(이학사)
1990년 숭실대학교 컴퓨터학과(공학석사)
1970년 과학기술처 중앙전자계산소
1975년 일신제강(주) 전산과장
1985년 한국전자계산기술(주) 부장
1990년~현재 배화여자대학 비서행정학과 부교수
〈관심분야〉 유비쿼터스 시스템 통합, 인공지능, 정보보안

양 해 술

1975년 홍익대학교 전기공학과(공학사)
1878년 성균관대학교 정보처리학과 (공학석사)
1991년 日本 오사카대학 정보공학과 소프트웨어공학 (공학박사)
1980년 강원대학교 전자계산학과 교수
1986년 日本 오사카대학교 객원연구원
1994년 한국정보처리학회 논문편집위원장
1995년 한국S/W품질연구소 소장
2001년 한국정보처리학회 부회장
1999년~현재 호서대학교 벤처전문대학원 교수
〈관심분야〉 : 소프트웨어공학(S/W 품질보증과 품질평가, 품질감리 및 컨설팅, OOA/ OOD/ OOP, SI), S/W 프로젝트관리, 컴포넌트 기반 개발방법론과 품질평가