클라이언트/서버 기반의 침해 사고 대응 시스템

서정민*, 전병규**, 장일기**, 이상문**, 남상온***
*지니정보시스템, **충주대학교 컴퓨터과학과
***대원과학대학 컴퓨터정보계열
e-mail:smlee@cjnu.ac.kr

A System for Prevention of Hacking based on Client/Server

Jeong Min Seo*, Byeong Kyu Jeon**, Jang Il Ki**,
Sang Moon Lee**, Nam Sang On***
*Jeenie Information System, Inc., **Dept of Computer Science, Chungju Nat'l Univ.
***Dept. of Computer Info. Daewon Science College

요 약

본 논문에서는 침해사고 발생시 신속하고 정확한 대응을 위하여 컴퓨터 포렌식을 이해하고 이 기법을 활용하여 침해사고 발생시 침해정보와 흔적을 수집, 분석할 수 있는 클라이언트/서버 환경에서의 실시간 침해사고 대응 시스템 구조의 설계 제안하였다. 제안된 시스템의 하드웨어 적용 범위는 특별한 제약을 주지 않고, 구내망이 구축된 시설, 즉 기업이나 기관에 모두 적용될 수 있도록 하였다. 또한 소프트웨어 환경은 윈도우를 기반으로 하고, 통신 환경으로는 인터넷 환경을 지원하기 위하여 TCP/IP Winsock 프로토콜을 채택하였다. 이상과 같은 조건을 만족하고, LAN 상의 서버에 이 시스템을 설치하여 네트워크 내에 있는 모든 컴퓨터를 감시, 제어하고 효율적으로 관리할 수 있도록 하여 기업내 침해사고에 빠르게 대처할 수 있게 하였다..

1. 서론

최근 이슈화 되고 있는 정보통신망 침해사고는 그 강도와 영역이 점차 확대되어 개인의 프라이버시 침해에서 부터 국가 경제 및 국가 안보에까지 총체적으로 위협을 받고 있다.

컴퓨터 침해사고는 어제 오늘의 일이 아니라 이제 현실의 문제가 되었다. 단순하게 형식적으로 컴퓨터를 수단으로 하거나 목적으로 한 범죄의 총체적 모습으로 광의적으로 파악할 것이 아니라 개별적 기술적으로 접근해야 할 필요가 있는 특징을 지니고 있다.

근래의 악의적인 해킹이나 산업 스파이에 의한 정보유출, 내부 직원의 회사기밀, 고객 정보 유출 등의 컴퓨터를 이용한 범죄가 급증하고 있다. 또한 우려할 만한 일은 국제적으로 컴퓨터 해킹사고의 경유지로 우리나라가 활용되는 사례가 많다는 것이다. 이러한 상황에서 기관·기업 내 보안조직의 침해사고대응에서부터 컴퓨터 포렌식 이해와 절차를 충분히 고려한 대응이 이루어져야 불충분한 법적 증거로 인한 기업의 피해를 최대한 줄일 수 있다. 침해사고가 발생된 후 컴퓨터 포렌식 수행여부를 판단하여 필요할 경우 컴퓨터 포렌식을 이용한 시스템 분석절차를 활용하여 대응이 이루어진다면 차후에 발생할 수 있는 법적 책임 소재를 가릴때 중요한 증거로서 사용될 수 있다[1, 2, 3]. 본 논문에서는 이러한 사이버 침해사고 발생시 신속하고 정확한 대응을 위하여 컴퓨터 포렌식을 이해하고 이 기법을 활용하여 침해사고 발생시 침해정보와 흔적을 수집, 분석할 수 있는 클라이언트/서버 기반의 실시간 침해사고 대응 시스템을 구축하여 이 정보를 보서 형태로 작성하여 수사 진행시 중요한 법적 증거로 사용할 수 있도록 하였다.

2. 컴퓨터 포렌식

2.1 기본 개념

일반적으로 포렌식스(Forensics)는 법정에서 변론하는 기술을 묘사할 때 사용하는 웅변술, 토론학 등을 의미하며 포렌식(Forensic)은 법정의, 토론의 등을 의미하는 형용사로서 Forensic Medicine과 같이 쓰이면 법의학을 의미하게 된다. 따라서 Forensic Computing이라고 하면 법전산학으로 불릴 수 있으나 대체적으로 그냥 컴퓨터 포렌식이라는 용어를 많이 사용한다. 디지털 자료는 일반적으로 복사가 쉬울 뿐만 아니라 원본과 복사본의 구분도 어렵고 조작 및 생성, 전송, 삭제가 매우 용이하다. 따라서 디지털 자료가 법적 증거력을 갖게 하기 위해서는 자료의 수집·보관·분석·보고에 이르는 전 과정에 특별한 절차와 방법에 따라 진행해야 한다[4, 5]. 컴퓨터 포렌식은 주로 컴퓨터에 내장된 디지털 자료를 근거로 삼아 그 컴퓨터를 매개체로 이용하여 일어난 어떤 행위의 사실 관계를 규명하고 증명하는 기법이다. 이 기법은 민·형사상의 범죄 수사뿐만 아니라 기업 활동 중에서도 종업원들의 비리를 발견하거나 증거를 확보하는데 이용될 수 있다. 특히 고객과의 분쟁 해결에 있어 중요한 증거자료를 확보하는데 긴요하다. 따라서 컴퓨터 포렌식 기법을 적용해 피해 상황을 제대로 규명하지 못한다면 기업은 엄청난 민사상의 피해를 볼 가능성이 커졌다. 미국 버클리 대학의 한 연구에 의하면 세계에서 생성되는 정보의 약90% 이상이 디지털 형태로 만들어진다고 한다. 이는 디지털 자료가 컴퓨터 해킹등과 같은 컴퓨터 범죄뿐만 아니라 일반 범죄를 수사하는 경우에도 요긴하게 사용되고 법적 증거로 채택 될 가능성이 커지고 있음을 말해준다[6, 7, 8, 9, 10].

주요 국가의 주요 수사기관과 민감한 자료를 다루는 금융, 보험 회사 등에서는 컴퓨터 포렌식 분야의 중요성을 인식하고 전문가 및 다양한 관련 기술 확보뿐만 아니라 디지털 증거의 수집 절차 및 분석 방법 개발 등에 박차를 가하고 있는 실정이다. 또 한 민간 기업에서는 컴퓨터 포렌식에 필요한 수많은 제품들 즉, 무결성 확보도구, 강력한 검색도구, 디스크 복제도구, 디스크 쓰기 방지도구, 다양한 분석 및 보고 소프트웨어 등을 개발해 국내외 시장을 휩쓸고 있다. 그러나 정보통신 강국이라는 우리의 경우, 소수의 중소기업에서 디지털 증거물 분석 소프트웨어를 개발중인 것으로 전해지고 있을 뿐 컴퓨터 포렌식 도구로 사용할 수 있는 대부분의 하드웨어, 소프트웨어 도구를 생산해 판매하고 있는 업체는 전무하다. 또한 일반기업에서 컴퓨터 포렌식 전문가를 확보하고 있는 경우는 거의 없는 것으로 파악되고 있다[11, 12, 13].

2.2 분류 및 대응 방안

컴퓨터나 네트웍을 이요한 일반적인 침해사고의 유형은 다음의 〈표 1〉과 같으며, 이에 대한 대응과 복구 단계는 〈표 2〉와 같은 방법을 이용한다[4, 5].

<표 1 > 일반적인 침해사고 유형별 분류

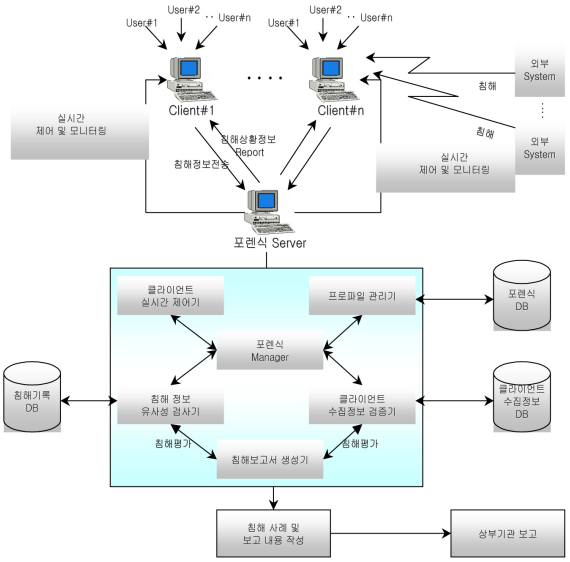
분 류	설 명
홈페이지 변조	해커가 자신의 실력을 과시하거나 해당기관에 망신을 주기 위하여 또는 정치적인 목적으로 해킹을 하여 해당 시스템의 관리자 권한을 절취한 후 메인 화면을 음란물, 낙서 및 욕설, 정치적 구호 등으로 변경하는 것.
웜 (Worm)	네트워크를 통해 자기 자신을 복제(Self-Replication)하고 스스로 전파 또는 공격할 수 있는 독립된 프로그램으로 인터넷상의 모든 취약한 시스템을 짧은 시간에 공격할 수 있는 위협적인 프로그램.
바이러스 (Virus)	자기 자신을 다른 실행 가능한 프로그램에 복제하거나 덧붙여 실행하는 프로그램
백도어 (Back Door)	시스템 공격 후 재차 공격때 쉽게 접속하여 권한을 획득할 수 있도록 설치하는 툴
악성 프로그램	의도적으로 정보통신 이용자에게 피해를 주고자 악의적인 목적으로 만든 프로그램 및 실행 가능한 코드.
트로이 목마	정상적인 프로그램으로 보이지만 실제로는 악의적 기능을 가지고 있는 프로그램.
서비스 거부	시스템의 정상적인 운영을 방해하여 정당한 사용자가 서비스를 받지 못하도록하는 공격.

<표 2> 사고대응 및 복구단계

1단계	취약성제거	공격에 이용된 취약성을 제거. 피해 시스템뿐 아니라 피해 시스템과 똑같은 종류의 시스템에 대해서 모두 분석하고 같은 취약성이 발견되면 이를 제거.
2단계	피해시스템 복구	정상적인 서비스가 이루어지도록 시스템을 복구. 만약 분석이 완벽하게 이루어지지 않았다고 판단된다면 되도록 시스템을 다시 설치하는 것이 바람직. 시스템 복구시는 가장 믿을 만한 백업버전으로 복구.
3단계	관련자통지	사고와 관련된 모든 사람에게 분석결과를 통지. 이 경우 사고와의 관련성에 따라주는 정보의 깊이가 달라져야 함. 외부기관에 주는 정보는 사이트내의 세부정보가 포함되지 않아야하며 상대방이 필요로 하는 정보만 전달.

3. 시스템의 설계

설계 제안된 시스템의 하드웨어 적용 범위는 특별한 제약을 주지 않고, 구내망이 구축된 시설, 즉 기업이나 기관에 모두 적용될 수 있도록 적용하였다. 또한 소프트웨어 환경은 윈도우를 기반으로 하고, 통신 환경으로는 인터넷 환경을 지원하기 위하여 TCP/IP Winsock 프로토콜을 채택하였다. 이상과 같은 조건을 만족하고, LAN 상의 서버에 이 시스템만을 설치하여 기업내 침해사고에 빠르게 대처할 수 있도록 설계하였다.



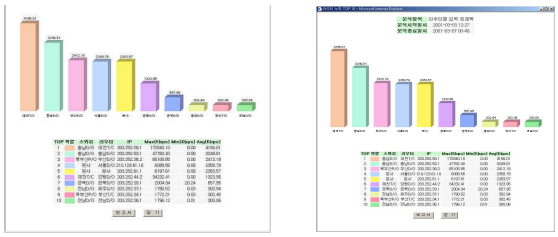
(그림 1) 시스템 구성도

본 시스템은 서버와 클라이언트의 두 부분으로 나누어져 있는데, 서버 기능은 서버 모듈이 수행하도록 구성되었으며, 이 모듈은 각각의 클라이언트의 관리를 위한 시스템으로 네트워크 연결되어 있는 모든 컴퓨터들에 관한 관리 정보를 모니터링하며, 클라이언트와 접속하여 정보를 송수신하며, 클라이언트 정보를 관리하는 역할을 수행한다. 즉 각각의 클라이언트 정보를 획득하여 관련 정보들을 통제 관리, 제어하는 기능을 수행한다. 자세한 기능으로 시스템 감시제어 정보, 실시간 클라이언트 화면 정보, CPU 및 메모리 사용률 감시, 즐겨 찾는 사이트 목록 감시 등이다. 클라이언트 기능은 클라이언트 모듈이 수행하도록 구성하며, 각각의 클라이언트에 설치하여 서버 시스템과 접속하게 하는 역할을 한다. 즉, 서버에서 요구하는 정보를 추출하여 서버로 전달하여 주는 등 상호 교신 하에 감시 및 관리 정보를 송수신하는 기능을 수행한다.

4. 구현 및 실험

구현 시스템의 기능은 네트워크 맵 기반의 실시간 데이터화면 Refresh 기능, 관리 네트워크 맵을 통한 실시간 성능 및 장애 탐지 기능, 관리 항목의 수집을 통한 통계 분석 기능 및 실시간 분석 기능, 심화 분석과 그래픽 기능, 주기적인 보고서 생성 기능, 관리자 Know-how를 통한 지식 정보 관리 기능, 임계값과 Trap을 사용한 논리적 장애 검출 기능 등을 내장하고 있다.

아래의 (그림 2)는 특정 클라이언트를 선택 후 입력 트래픽을 응용프로그램별로 최대•최소•평균값을 계산하여 보여주는 화면으로 그래프는 평균값을 나타낸다.

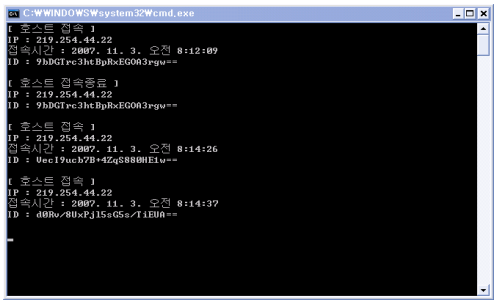


(그림 2) 응용프로그램별 트래픽 정보

아래의 (그림 3)은 특정 클라이언트의 트래픽 자료를 검색하는 화면으로 네트워크를 통해 송•수신 자료의 크기 및 목록, 수신자의 IP 주소, 시간 등의 정보를 검색하는 화면이다.

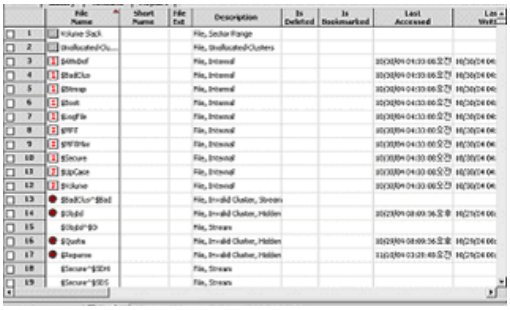
(그림 3) 클라이언트의 송수신 정보 검색

또한 (그림 4)는 현재 클라이언트와 통신하는 상대 클라이언트의 정보를 실시간으로 파일 형식으로 저장하는 화면을 나타내고 있다.



(그림 4) 외부 접속 클라이언트 파일 저장

(그림 5)는 송수신 파일의 유형별 위험성을 나타내주는 화면으로 파일의 종류 및 내용별 일반 파일과 악의적인 파일 등으로 분리하여 보여준다. 이때 관리자의 경험을 이용하여 한계값 등을 셋팅할 수 있다.



(그림 5) 종류별 파일 분류

5. 결론

인터넷 사용 인구가 증가 하면서 인터넷을 통한 전자상거래는 앞으로 더욱더 활발할 것이며 이해 대한 역기능 또한 더욱더 커질 것이 자명하다. 특히 이러한 사이버 공간을 통한 범죄는 사이버 세계의 익명성, 동시성, 광역성 등의 특성으로 인하여 더욱더 발견해 내기 어려운 실정이다. 지금까지 컴퓨터 침해사고 발생시 우리들은 주먹구구식으로 그것들을 해결하려고 하였으며, 사고에 대한 정보공유 및 정보의 문서화가 미미하여 신속한 사고처리에 어려움을 겪어왔다. 본 논문에서는 이러한 사이버 침해사고 발생시 신속하고 정확한 대응을 위하여 컴퓨터 포렌식을 이해하고 이 기법을 활용하여 침해사고 발생시 침해정보와 흔적을 수집, 분석할 수 있는 클라이언트/서버 기반의 실시간 침해사고 대응 시스템을 구축하여 침해 사고시 빠르게 대처할 수 있고 이 정보를 보고서 형태로 작성하여 수사진행시 중요한 법적증거로 사용할 수 있는 클라이언트/서버 구성을 제안하였다. 최근 컴퓨터 포렌식을 우회하는 기법이 등장하여 증거수집, 분석을 하지 못하는 상황이 발생하기도 한다. 이러한 상황을 효과적으로 막아내기 위하여 우회기법들에 대한 연구가 필요하다.

참고문헌

[1] 정계옥, “감사로그를 이용한 포렌식 시스템 설계 및 구현”, 전남대학교, 석사논문, 2003.
[2] 박종성, “자동화된 침해사고 대응 시스템에서의 네트웍 포렌식 정보에 대한정의”, 고려대학교, 석사논문, 2005.
[3] 김계관, “컴퓨터 증거 수집 및 분석에 관한 연구”, 고려대학교, 석사논문, 2005.
[4] 한국정보보호진흥원, http://kisa.or.kr
[5] 사이버 포렌식 협회, http://www.cfpa.or.kr
[6] ITSAC FORUM, http://www.itsac.or.kr
[7] New Technologies, Inc, http://www.forensics-intl.com
[8] Finaldata, http://www.finaldata.com
[9] Cybercrime Research Forum, http://cybercrime.ce.ro
[10] Computer Security Institute, http://www.gocsi.com
[11] 황현욱외2 인, 해킹과 사이버 보안, 전남대학교 출판부, 2003
[12] 이현우외1 인, 사례로 배우는 해킹 사고분석 & 대응, 영진닷컴, 서울, 2003.
[13] 김귀남외4인, 해커를 잡아라, 정일출판사, 2006