Journal of Security Engineering
Vol. 1, No. 1, August, 2005

컴퓨터 포렌식스 지원을 위한 침해대응시스템 설계*

임의열, 장재혁, 최용락
대전대학교 컴퓨터공학과
e-mail : {imten,jhjang}@zeus.dju.ac.kr, yrchoi@dju.ac.kr

Design of Intrusion Response System for Computer Forensics

Ui-youl Im, Jae-hyeok Jang, Yong-rak Choi
Department of Computer Engineering, Daejeon University

요 약

In this paper, we present the system which provides automated and integrated technologies by setting a relation as Manager, correspondence interface and Agent according to given Computer Forensics process and we concrete the evidence collecting system. Central Manager analyses and guesses the gained evidences by each agent and can get the legal evidences easily through Manager even though Agent manager is not a professional which can analysis and guess evidences. Correspondence interface performs Integrity, storage and transportation of gained evidences and can get originality and authenticity of the digital evidences. And Agent is added to not only evidence collecting technology also intrusion detection technology so it is possible to cope with a intrusion directly moving together with Trace Back System.

1. 서론

최근 정보통신 관련 기술의 비약적인 발전으로 비즈니스 커뮤니케이션의 70%가 전기, 전자적으로 이루어지고 있다. 이에 따른 순기능과 더불어 각종 해킹사고 및 사이버 범죄와 같은 역기능은 갈수록 증가하고 공격수법 또한 점차 지능화, 다양화되고 있다. 이러한 보안 침해사고에 따른 시간적, 경제적 피해의 규모는 이전과는 비교할 수 없을 정도로 증가하고 있으며 기업의 생존까지 위협하고 있다.

이에 따라 미국을 중심으로 기술 선진국들은 보안침해사고에 대하여 디지털 전자적 증거를 수집, 분석 및 대응할 수 있는 컴퓨터 포렌식스(Computer Forensics) 기술 개발에 집중하고 있다. 그리고 다양한 보안침해사건의 사실관계를 확정 또는 증명하기 위한 법의학적 해석과 안전한 비즈니스 커뮤니케이션의 제도적 정착을 위하여 국가적 전략산업으로 개발하고 있다. 이러한 활동들을 뒷받침할 수 있는 핵심적 컴퓨터 포렌식스 도구의 개발분야는 새로운 전문적 기술의 인기 직종으로 부상하고 있다[1,2,3].

국내의 경우, 컴퓨터 포렌식스 기술이 확보되지 않는다면 국내외에서 일어나는 모든 보안침해사고에 대하여 국가 자존적 해석이나 사실증명이 불가능하고 외국에 의뢰하여 결과를 통보 받아야 하는 안타까운 현실을 초래할 수밖에 없다. 따라서, 적기에 디지털 전자적 증거물을 분석하고, 법적 효력을 갖는 증거물로 제시할 수 있는 컴퓨터 포렌식스 기술을 개발하여 각종 보안침해사고로 발생하는 역기능들에 대해 법적 구속력을 제공해야 한다.

또한, 정보보안 사고는 법적 판단에 필요한 증거자료가 결정적인 역할을 하고 있는 상황에서 사이버 범죄 대처와 기업의 정보자산 보호에 큰 역할을 할 수 있도록 내부자 정보유출을 비롯한 정보보안 사고 발생시의 상황을 그대로 재현할 수 있는 보안사고 원인분석 기능을 갖추어, 모든 트래픽과 다른 시스템간의 연관성을 저장한 후 감식 기술로 분석하여 당시 상황을 그대로 재현한 증거자

* 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

료분석 개발이 시급하다.

컴퓨터 포렌식스는 각종 보안침해사고에 대하여 법의학적으로 인정받을 수 있는 미래사회의 고도로 발달된 새로운 업종이다. 현재, 사이버테러 및 각종 보안침해사고에 대하여 사회적 인식과 '공인탐정관련법' 등 국내외적으로 정보보호 정책 및 사회적 규제가 강화되는 추세이나, 이에 대한 기업의 연구인력 및 기술수준은 매우 미흡한 실정이다[7,8].

따라서, 외국의 컴퓨터 포렌식스 기술을 조기에 도입하여 국내의 기술로 정착시키고, 국산 우수제품을 사용하여 향상된 포렌식스 도구들을 연구 개발함으로써 미래 산업에 적절한 준비를 해야 한다. 본 연구에서는 국내외 컴퓨터 포렌식스 기술을 분석하여 시스템의 안전성을 보장하고 법적 대응에 필요한 침입증거자료를 제공할 수 있는 시스템을 제안한다

2. 컴퓨터 포렌식스 기술

컴퓨터 포렌식스는 "정보처리 기기를 통하여 이루어지는 각종행위에 대한 사실관계를 확정하거나 증명하기 위해 행하는 각종 절차와 방법"이라고 정의 할 수 있다. 그러므로 컴퓨터 포렌식스는 단순히 과학적인 컴퓨터 수사 방법 및 절차뿐만 아니라 법률, 제도 및 각종 기술 등을 포함하는 종합적인 분야이다.

2.1 국내외 기술 현황

현재까지 제시된 컴퓨터 포렌식스 도구들은 크게 두 가지 형태로 구분할 수 있다. 즉, 컴퓨터 포렌식스에 관련된 전반적인 기능을 제공하는 도구와 각 기능별로 포렌식스 과정을 수행하는 부분적인 도구이다.

국내에서 공개된 컴퓨터 포렌식스 관련 증거 수집 방법 및 도구는 거의 전무하며 또한, 상업용 증거 수집 도구들 역시 삭제된 파일에 대해 복원 및 복구 기능 등을 주로 제공하기 때문에 상당히 제한적인 분야에만 개발되어 있다. 검찰청이 부분 기능을 제공하는 컴퓨터 포렌식스 도구를 연속적으로 개발하고 있으며, KDL 도 컴퓨터 파일, 이메일, 네트워킹, 추적등을 합법적으로 전자 증거물을 찾을 수 있는 컴퓨터 포렌식스를 개발하고 있다. 그러나, 순수한 국내의 기술력은 미흡하며, 외국에서 발표된 일부 도구들을 도입 연구하는 수준이다. 외국의 포렌식 도구 업체로는 유타 주 프로보 소재의 액세스데이터 디벨롭먼트, 캘리포니아 주 파사데나 소재의 가이던스 소프트웨어, 오리건 주 그레샴 소재의 뉴테크놀러지스 아모 등이 있으며, 여기에 대학교 연구소의 개발자들과 메사추세츠 주 캠브릿지 소재의 앳스테이크 같은 보안 컨설턴트 등도 있다. 이 업체들은 대상 컴퓨터 내부의 저장장치에 남겨져 있는 수 기가바이트의 데이터를 분석하는 강력한 도구를 제공한다[5,7,8].

2.2 국내외 도구 분석

(1) EnCase(Guidance Software)

EnCase 는 조사자가 많은 양의 컴퓨터 증거를 쉽게 관리하고 파일 스택과 할당되지 않은 데이터를 볼 수 있는 GUI(Graphical User Interface)의 특징을 가진 강력한 컴퓨터 포렌식 도구이다.

통합된 기능의 EnCase 는 목표로 하는 드라이브의 초기 사전 검토, 증거의 이미지를 획득하고, 데이터를 검색하고 복구해서 기록하고, 모든 같은 애플리케이션에서 컴퓨터 포렌식 조사 처리의 기능을 모두 수행하도록 조사자에게 제공한다.

Guidance Soft 사의 EnCase 는 해킹범죄가 발생했던 당시의 시간 검증 및 파악된 파일의 디렉토리 구조파악을 통하여 인위적으로 숨겨지거나 증발한 파일들의 정보를 알아내는 범행시간 추적 포렌식스 제품이다. EnCase 는 현재 가장 강력한 기능을 가진 컴퓨터 포렌식스 도구로 알려져 있으며 1980년대부터 개발되어 현재는 버전 4 가 개발되어 널리 쓰이고 있다. EnCase 는 포렌식스 소프트웨어가 갖추어야 할 증거 보존 및 분석 기능을 모두 갖추고 있으며, 미 연방 법원의 EnCase 를 통해 얻은 결과물을 법적인 증거로 채택한 판례로 인해 더욱 성능을 인정받고 있는 도구이다.

EnCase 의 주요기능은 다음과 같다.

- 증거 자료의 무결성 보장
- 유연한 이미지 추출 방법 제공
- 사용자 정의 스크립트 작성을 통한 자동화 작업 가능.
- 파일의 정확한 시간대 추적
- 삭제된 파일, 폴더 및 비할당 클러스터 영역 검색 및 복구
- 뛰어난 보고 기능

(2) AccessData Forensic Toolkit

AccessData 포렌식 툴킷(FTK)은 컴퓨터 시스템의 포렌식 조사를 수행하기 위한 완벽한 방식을 제공하는 편리한 컴퓨터 포렌식 도구이다. 전체 텍스트 색인은 신속한 기능을 제공하며, 삭제된 파일 복구와 파일 슬랙 분석이 우수하다.

또한, FTK 는 비밀번호 복구와 암호화 파일 식별 프로그램들 같은 다른 AccessData 유틸리티들과 함께 상호 작용이 가능하다. 그리고, FTK 는 255 개의 다른 파일 형식으로 접근가능 하도록 Stellent 의 Outside In Viewer 기술을 결합하였다. FTK 는 EnCase, Snapback, SafeBack 그리고 리눅스 DD 에 의해서 얻어진 증거 파일들을 지원할 수 있다.

(3) Foundstone Forensic Toolkit

Foundstone 포렌식 도구는 권한이 없는 행위에 대해 NTFS 디스크 파티션 파일을 조사하는 것으로 몇몇 Win32 명령 라인의 도구를 포함한다. 이

러한 공개 소스 툴은 숨은 파일과 데이터 스트림을 찾기 위해 디스크를 스캔하고 디스크의 데이터 속성을 변경하지 않고 MAC 시간과 함께 기록한다.

(4) Windows Event Log Analysis

마이크로소프트의 WinNT/2K 는 시스템 이벤트와 애플리케이션 이벤트, 그리고 보안 이벤트를 기록하기 위하여 바이너리 파일로 이벤트 로그를 구성할 수 있다. 이러한 이벤트 로그는 동적 라이브러리 파일을 링크하거나 기록 및 실행을 통하여 서술적 메시지를 저장한다. 이벤트 뷰어는 이 파일들의 정보를 결합시켜 표시하고 데이터를 볼 수 있는 편리한 방법을 제공한다.

따라서, 원격 시스템에서 이벤트 로그 파일을 볼 때, 조사를 위해 어떤 시스템에서 다른 곳으로 이벤트 로그 파일을 복사하는 것은 오역의 결과를 가져올 수 있다. 이벤트 뷰어는 원격의 로그 파일로부터 이벤트가 기록된 데이터를 읽는다. 하지만 이벤트 메시지 파일에 대응시키기 위해서 로컬 시스템의 기록을 탐색해야 한다.

이외의 도구로 DumpEvt, Unix Log Analysis, Network Analysis 와 데이터 복구 기능을 제공하는 Magic recovery, LiveData, LiveData Partition Recovery, Recovery Expert 등이 있다.

2.3 기존 기술의 문제점

(1) 기존 Computer Forensics 도구의 문제점

컴퓨터 포렌식스란 법과 연결된 컴퓨터 작업이라고 알려져 있지만 실질적으로 필요로 하는 증거와 일정한 규칙, 컴퓨터 시스템을 점검하는데 있어서는 적절한 실습, 데이터 복구와 보존, 데이터 암호 알고리즘, 암호화 및 크래킹 기법, 정보저장 매체분석, OS 와 Media 의 특징, 데이터 숨기는 법, 바이러스와 악의적인 프로그램 숙지, 이미지 저장과 가상 서버, 상업적인 도구에 대한 사용법을 알아야 하는 종합적인 컴퓨터 전문 분석인 것이다.

하지만 현존하는 컴퓨터 포렌식스 도구의 문제점은 여러 가지로 나타나고 있으며, 사용자가 이러한 기능을 만족하지 못하는 문제점을 가지고 있다.

- 증거의 무결성
- 분석 기술의 부족
- 데이터 포렌식에 한정
- 응용프로그램 레벨의 운영
- 사용자 중심의 기능 부족

(2) 발전된 Computer Forensics 도구의 필요성

컴퓨터와 인터넷의 활용증가와 더불어 어린이 포르노, 각종 음란 사이트 개설, 내부인의 불법적 계좌이체, 위협 편지, 사기, 지적 재산 도난 등의 전자적 증거를 추적하고 법적인 책임을 부과하는 것이 새로운 사회적 문제가 되고 있다. 이러한 문제들은 사용된 컴퓨터를 면밀히 전자적으로 조사하고, 특정 키워드 탐색, 로그파일 분석 등을 통한 불법적인 행위의 시간 및 방법을 구체적으로 증명해야 하는 대단히 난해한 작업이다.

컴퓨터 포렌식스는 각종 보안침해사고에 대하여 법의학적으로 인정받을 수 있는 미래사회의 고도로 발달된 새로운 업종이다. 현재, 사이버테러 및 각종 보안침해사고에 대하여 사회적 인식의 제공과 함께 '공인탐정관련법' 등 국내외적으로 정보보호 정책 및 사회적 규제가 강화되는 추세이나, 이에 대한 기업의 연구인력 및 기술수준은 매우 미흡한 실정이다.

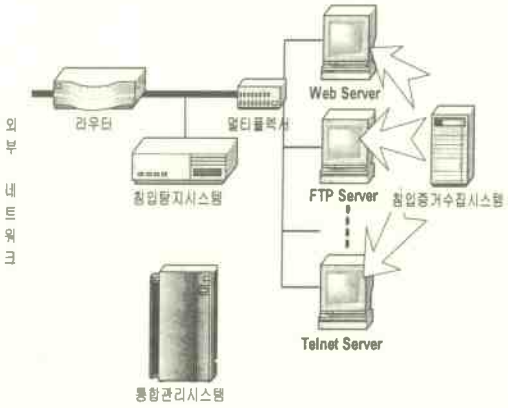
컴퓨터 포렌식스는 전자적 증거를 제공하는 법의학적 측면 및 보안침해사고를 기술적으로 복구하는 산업재해 복구 측면에서 새로운 제품과 업종의 탄생에 대한 큰 영향을 미칠 것이며, 이러한 지속적인 연구 개발을 통하여 SecuOS 플랫폼에 감사 및 추적 기능이 반드시 필요하다.

3. 침해사고대응 시스템

3.1 시스템 구성 및 기능

시스템 침해에 대한 시스템 대응은 세 개의 영역으로 구성된다. 네트워크 및 시스템 공격을 감지하는 침입탐지시스템, 침입증거확보 및 세션을 인증하는 침입증거수집 시스템, 전반적인 침해를 관리하고 법적 대응 및 시스템 관리를 위한 통합관리시스템으로 이루어진다.

그림 1 은 시스템 구성을 나타낸다.



(그림 1) 시스템 구성도

각 개체별 기능은 다음과 같다.

- Web Server, FTP Server, Telnet Server 등: 네트워크를 이용한 응용 서비스 제공시스템 (감시시스템)
- 침입탐지시스템: 네트워크 패킷을 감시하여 침입을 탐지하고 탐지 정보를 기반으로 통합관리시스템과 침입증거 수집시스템에 이벤트를 발생시켜 대응할 수 있도록 처리하는 시스템
- 침입증거수집시스템: 네트워크 연결 세션 및

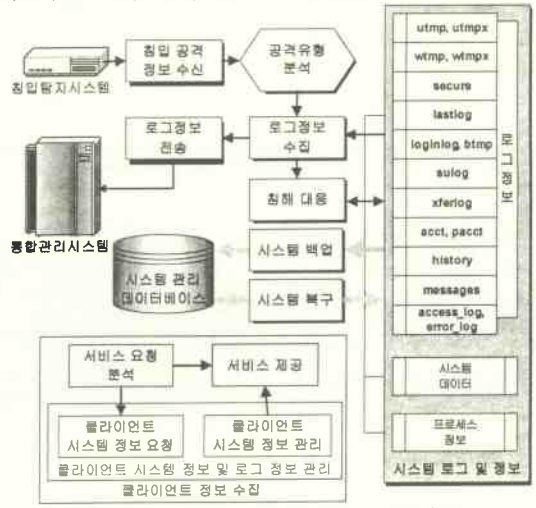
침입 근거를 확보하고 시스템 보호를 위한 복구기능을 제공하는 시스템

- 통합관리시스템: 침입탐지시스템과 침입증거 수집시스템으로부터 전송된 침입정보를 기반으로 네트워크 현황 파악 및 법적 대응 침입 증거를 확보하는 시스템

3.2 침입증거수집시스템 구성 및 기능

침입탐지시스템의 침입 및 위험 경고 이벤트에 의해 침입증거를 수집, 침입 대응, 시스템 복구 기능을 제공한다. 또한 클라이언트 요청 서비스에 대한 인증세션을 제공한다. 증거수집시스템은 공격 이벤트가 침입탐지시스템으로부터 전송되었을 경우와 네트워크 연결자의 서비스 요청 보안 등급에 따라서 기능이 제공된다.

공격 이벤트가 발생했을 경우, 시스템 공격 유형을 분석하고 분석된 공격 유형에 따라 로그정보를 수집하여 통합관리시스템에 전송한다. 또한 공격유형에 따라서 서비스 종료 및 네트워크 세션 종료, 공격자의 모든 이벤트 추적의 대응기능을 제공한다. 시스템 백업 및 복구는 정기적으로 행하여 시스템 상태유지 지원기능을 제공한다. 네트워크 연결자의 서비스 요청 보안등급에 따른 기능은 로컬 사용자의 일반적인 명령 및 서비스는 원활한 기능을 제공하고 권한 상승, 파일 수정 및 생성, 파일 업로드, 시스템 명령의 경우 네트워크 연결 요청자 영역의 시스템 정보(HDD ID, CPU ID, CD-ROM ID, MAC Address, IP Address)를 확보하여 시스템 로그와 함께 정보를 관리한다. 확보된 정보는 시스템 관리 데이터베이스에 보관되고 추후 법적공방시 증거자료로 활용된다. 침입증거 수집 시스템은 그림 2 와 같이 구성된다.



(그림 2) 침입증거 수집시스템 기능도

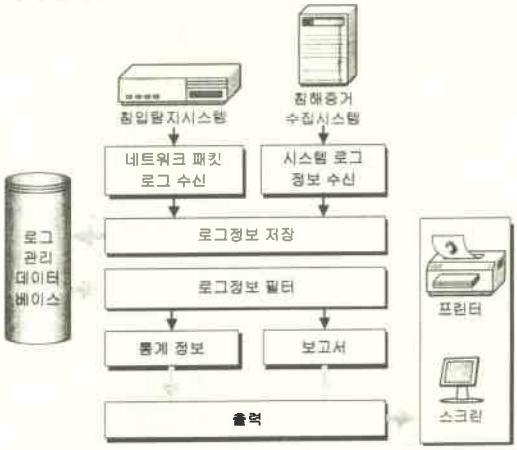
침입증거 수집시스템의 기능 모델은 다음과 같다.

- 공격유형 분석: 탐지된 시스템 공격정보를 이용하여 위험 등급을 설정하고 대응 레벨을 제공
- 로그정보 수집: 공격 유형에 따른 로그 수집
- 침해 대응: 공격 유형에 따른 공격자 역추적 및 세션 종료, 서비스 종료 설정
- 시스템 백업: 정기적인 시스템 정보 백업
- 시스템 복구: 공격에 의한 시스템 피해시 침해 정보를 복구
- 서비스 요청 분석: 네트워크 연결자의 서비스 요청을 보안등급으로 구분
- 클라이언트 시스템 정보 요청: 네트워크 연결자 시스템 정보를 수집할 수 있는 프로그램 실행
- 클라이언트 시스템 정보 관리: 연결 요청자의 시스템 정보와 모든 이벤트 로그 수집 및 저장

3.3 통합관리시스템 구성 및 기능

관리시스템은 컴퓨터 포렌식스 절차 중 통신 인터페이스를 통하여 증거물 인증 단계와 증거물 보관 및 이송 단계를 수행하고, 전송된 패킷 정보와 시스템 침입증거 수집시스템의 로그 정보를 확보하여 네트워크 현황 파악 및 법적 대응정보 확보 기능을 제공한다.

수집된 탐지 정보 및 침해증거는 로그 관리 데이터베이스에 저장되어 관리된다. 즉 네트워크 및 시스템 정보를 취합하여 침해 근거를 확보한다. 확보된 정보는 로그정보 필터에 의해 통계 정보 보고서와 텍스트 보고서로 작성되어 결과를 출력한다. 그림 3 은 통합관리시스템의 구성 및 기능을 나타낸다.



(그림 3) 통합관리시스템 기능도

통합관리시스템의 기능은 다음과 같다.

- 네트워크 패킷로그 수신: 침입탐지시스템에서

침입 및 위험로그 감시 정보를 수신

- 시스템 로그 정보 수신: 피해시스템의 로그정보를 수신
- 로그정보 저장: 피해시스템의 시스템 및 네트워크 로그정보를 데이터베이스에 저장
- 로그정보 필터: 시스템 공격과 관련된 정보를 필터링
- 통계정보: 공격 형태 및 시간, 대상에 대한 통계정보
- 보고서: 시스템 공격과 관련된 로그의 필터링 결과를 정렬
- 출력: 시스템 침해증거물을 스크린 및 프린터로 출력
- 로그 관리 데이터베이스: 시스템 및 네트워크 침해증거 저장소

3.4 침입 탐지시스템

네트워크 패킷을 감시하여 침입 및 위험요소를 식별하여 침입증거 수집시스템과 통합관리시스템에 이벤트 발생시키고 감시 패킷을 수집한다.

침입 탐지시스템은 네트워크의 트래픽을 감시하여 시스템 침입의 위험 및 침해 패턴을 탐지하고 각각의 시스템 영역에서 호스트를 감시하여 불법 행위와 공격 유형을 분석하여 통합관리시스템과 침입증거 수집시스템에 경고 메시지와 침해 위험 패킷을 전송한다. 그림 4 는 네트워크 및 시스템 침입탐지시스템의 구성 및 기능 모듈을 나타낸다.

(그림 4) 침입탐지시스템 기능도

침입탐지시스템의 기능은 다음과 같다.

- 패킷 수신: 네트워크에 흐르는 패킷을 수신
- 패킷 분석: 수신된 패킷을 서비스, 대상별 분석
- 패킷 폐기: 정상 패킷 폐기
- 침입 및 위험: 패킷 분석을 통해 침입 및 위험성 판다
- 공격유형 분석: 탐지정책에 따른 공격유형 및 피해시스템 분석
- 공격유형 전송: 공격 대상시스템에 공격 정보 전송
- 패킷정보 전송: 공격으로 감지된 패킷을 통합관리시스템에 전송

4. 제안시스템 성능 평가

4.1 기능별 성능 테스트

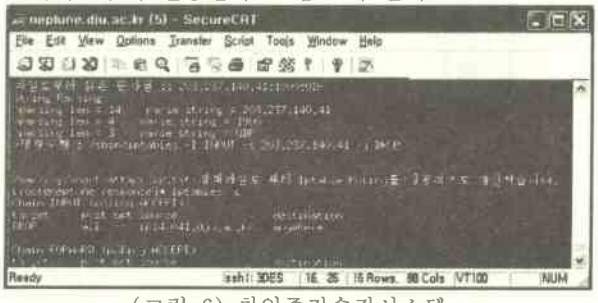
제안시스템은 네트워크 패킷을 감시하는 침입탐지와 공격대상 시스템의 증거수집, 수집된 침해증거물 통합관리 영역으로 나누어 기능을 테스트한다.

하나, 네트워크 침입탐지시스템은 패킷을 감시하고 공격 유형을 판별하여 통합관리시스템과 침입증거수집 시스템에 공격 이벤트와 패킷 감시로그를 전송한다. 그림 5 는 테스트 화면이다.

(그림 5) 침입탐지시스템 실행

Nmap 스캐닝 공격을 탐지하여 시스템 공격 이벤트를 관리시스템과 증거수집시스템에 전송한다.

둘, 증거수집시스템은 탐지시스템으로 인해 공격유형을 파악하고 근원지 IP 를 차단한다. 또한 공격자 로그 정보와 현재 시스템의 로그를 수집하여 관리시스템에 전송한다. 그림 6 과 같다.



(그림 6) 침입증거수집시스템

셋, 관리시스템은 탐지시스템과 증거수집시스템에 서 전송된 정보를 기반으로 분석하고 리포트를 작성한다. 통합관리시스템에 전송된 로그들은 시스템 현황을 파악할 수 있고, 직접 또는 간접적인 공격 정보를 가진다.

4.2 성능 분석

네트워크 패킷 탐지시스템은 외부의 공격을 탐지하여 침입탐지시스템이 공격자의 로그를 수집할 수 있도록 한다. 또한 공격 패킷 로그들을 통합관리시스템으로 전송하여 공격자의 근원지 IP 주소와 공격 로그 이벤트를 확보한다.

침입증거수집시스템은 공격이 발생하였을 경우, 시스템에 남겨진 휘발성 및 비 휘발성 로그를 수집한다. 또한 일반적 시스템 운영상에 클라이언트가 요청한 서비스(권한상승, 파일 생성 및 수정, 파일 업로드, 시스템 제어 명령)의 보안 등급을 판별하여 클라이언트 시스템 정보(HDD ID, CPU ID, MAC address, IP Address)를 확보하여 근원지 정보를 수집한다. 이렇게 수집된 정보는 통합관리시스템에 전송한다. 통합관리시스템은 확보된 근원지 정보, 네트워크 패킷 로그, 피해시스템 로그, 공격 클라이언트 시스템 정보를 기반으로 법적 증거로 활용한다. 제안시스템은 네트워크 환경에서 탐지시스템은 외부자의 공격을 탐지하고 시스템 내부자의 공격은 침입증거수집시스템에서 기능을 제공하여 좀 더 안전한 시스템을 지원한다.

5. 결론

본 제안시스템은 사이버상에서 발생하는 시스템 침해로부터 피해자를 보호하기 위하여 법적 공방 근거자료 확보를 연구하였다. 침해대응을 위한 증거수집시스템은 네트워크 패킷 탐지, 시스템 침입증거수집, 증거 통합관리영역으로 구성된다. 제안시스템의 성능 테스트는 각 기능을 영역별로 실행하여 증거를 수집하는 기능에 중점을 두었다.

그러나 일반적인 시스템의 영역에서는 탐지시스템의 성능에 따라 본 시스템의 안전성이 고려될 수 있으나, 본 연구는 포렌식스 지원을 위한 연구이므로 증거수집을 위한 제안 시스템이다. 또한 수집된 정보가 법적 효력을 발휘하기 위해서는 탐지시스템과 증거수집시스템은 신뢰되어야 한다. 즉, 신뢰되지 못한 시스템에서 수집된 정보는 증거물로서 효력을 발휘할 수 없기 때문이다.

제안시스템은 컴퓨터 포렌식스의 증거물 확보를 위한 시스템을 연구하였다. 추후, 본 연구에서 미흡한 부분인, 각 시스템별 세부기능과 시스템간에 전송되는 증거물의 신뢰성 및 인증 기능을 제공하도록 계속해서 연구하고 개발할 것이다.

참고문헌

[1] Warren G.Kruse II, Jay G.Heiser. "COMPUTER FORENSICS: Incident Response Essentials", Addison Wesley.

[2] Gray Palmer. A Road Map for Digital Forensics Research. Technical Report DTR-T001-01. DFRWS. November 2001. Report From the Fiest Digital Forensic Research Workshop(DFRWS).

[3] John R. Vacca. "COMPUTER FORENSICS: Computer Crime Scene Investigation", Charles River media.

[4] Farmer, D, Venema, W, "Computer Forensics Analysis Class Handouts", 1999, at: http://www.fish.com/forensics /class.html

[5] Michael G, Noblett, Mark M. Pollitt, Lawrence A. Presley, "Recovering and Examining Computer Forensics Evidence", Forensics Science Communication Volume 2 Number 4, October 2000, at: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

[6] Legal Information Institute, Federal Rules of Evidence 2003, at: http://www.law.cornell.edu/rules/fre/overview.html

[7] 황현욱, 김민수, 노봉남, 임재명, "컴퓨터 포렌식스: 시스템 포렌식스 동향과 기술", 정보보호학회지, 제 13권, 제 4호 2003.

[8] 고병수, 박영신, 최용락, "보안침해사고 대응을 위한 컴퓨터 포렌식스 기술동향" 한국인터넷정보 학회지, 4권 1호, 2003, pp.37-46

[9] 이성진, 외 8인, "해킹피해시스템 증거물 확보 및 복원에 관한 연구: A study on Computer Forensics", 한국정보보호진흥원, 2002

[10] 박종성, 최운호, 문종섭, 손태식, "자동화된침해사고대응시스템에서의 네트워크 포렌식 정보에 대한 정의", 정보보호학회 논문지, 제 14권, 제 4호, 2004.

[11] 정조민, 이지율, 이구연, "역추적 에이저트를 이용한 시스템 설계 및 구현", 강원대학교 산업기술연구소 논문집, 제22권 B호, 2002.

[12] 박영신, 고병수, 최용락, "침입자 역추적을 위한 IP 헤더 마킹기법에 관한 연구", 한국인터넷정보학회 추계학술발표, 2003 pp.323-326.

[13] 김영모, 고은주, 최용락, "컴퓨터 포렌식스 지원하는 시스템의 요구사항", 한국정보보호학회 충청지부학술발표, 2004, pp.215-223.

저자소개

임 의 열(UiYoul Im)

e-mail: imten@zeus.dju.ac.kr
2004 년 대전대학교 정보통신공학과 (공학학사)
현재 대전대학교 컴퓨터공학과 (석사과정)
관심분야: DRM, 컴퓨터 포렌식스

장 재 혁(JaeHyeok Jang)

e-mail: jhjang@zeus.dju.ac.kr
2000 년 대전대학교 컴퓨터공학과 (공학학사)
2002 년 대전대학교 컴퓨터공학과 (공학석사)
현재 대전대학교 컴퓨터공학과 (박사과정)
관심분야: 컴퓨터 포렌식스, DRM, PKI

최 용 락(YongRak Choi)

e-mail: yrchoi@dju.ac.kr
1989 년 중앙대학교 전자계산학과 (박사)
1982~1986 년 한국전자통신연구원 선임연구원
현재 대전대학교 컴퓨터공학과 교수
관심분야: 컴퓨터통신보안, 컴퓨터 포렌식스, DRM