한국컴퓨터정보학회 동계학술대회 논문집 제19권 제1호 (2011. 1)

포렌식을 위한 웹로그 시나리오 작성 시스템

장혜숙°, 이진관*, 이종찬*, 박상준*, 박기홍*
°*군산대학교 컴퓨터정보공학과
e-mail: {hs5486, leejinkwan, chan2000, lubimia, spacepark}@kunsan.ac.kr

Web Log Scenario Make for Forensic

Hae-Sook Jang°, Jin-Kwan Lee*, Jong-Chan Lee*, Sang-Joon Park*, Ki-Hong Park*
°*Dept of Computer Information Engineering, Kunsan National University

● 요 약 ●

수많은 웹로그 히스토리의 자료에서 컴퓨터 사이버범죄에 대한 증거자료로 채택되기 위한 기술적인 웹 포렌식 자료의 추출에 사용되는 웹 포렌식 알고리즘은 필수적인 요소이다. 본 논문에서는 웹 로그 시나리오 작성을 제안하고 설계하여, 웹 포렌식을 통한 컴퓨터 사이버범죄에 대한 학문적 기술적 발전에 기여하고자 하는데 본 논문의 목적이 있다. 수많은 웹로그 자료에서 컴퓨터 사이버 범죄에 대한 증거 자료로 채택되기 위한 기술적인 웹 포렌식 자료의 추출에 사용되는 웹 로그 분석 알고리즘은 필수적인 요소이다. 본 논문에서는 웹 포렌식 알고리즘을 제안하고 설계하여, 실제 기업의 웹 서버 시스템에 제안한 알고리즘을 구현해 본다. 웹 서버에서 웹 로그 분석을 위해 사용한 웹 포렌식 알고리즘과 플로우를 설계하고 코딩을 통한 구현을 한다. 구현 결과 웹 포렌식을 통한 컴퓨터 사이버 범죄에 대한 학문적 기술적 발전에 기여하고자 하는데 본 논문의 목적이 있다.

키워드: 웹로그(web log), 포렌식(forensic), 안티포렌식기법(Anti-Forensic)

I. 서 론

컴퓨터 포렌식이라는 용어는 1991년 Portland에서 열린 IACIS (International Association of Computer Specialists)에서 처음으로 사용되었다[1].

우리나라 경우 2004년12월 21일 신설한 '디지털증거분석센터 (Digital Forensics Center)'의 첨단범죄 증거분석, 증거분석 절차의 표준화 및 보급, 전문 수사기법 연구개발 등의 업무수행 결과에 큰 영향을 받은 것이다. 또한 2005년 10월 13일 포렌식 기술과 법률절차 등 제반 절차를 연구하기 위한'대한민국 디지털 포렌식 학회'를 출범하여 사이버범죄와 디지털 포렌식 분양에서 정보교류와 연구 활동을 적극 추진하고 있다.

대검찰청 컴퓨터수사과, 서울중앙지검 컴퓨터수사부를설치한 이후 연130% 이상씩 컴퓨터범죄 단속 실적이 급격히 증가하고 있다. 특히 2000년도 이후 급격한 상승률을 기록하면서 2005년 현재 약 2만 여명의 검거실적을 보이고 있다. 컴퓨터범죄 증가추세에 맞추어 첨단수사기법 ·첨단컴퓨터기기 도입 및 인력 증원과 직원들의 컴퓨터수사 능력배양을 통하여 지속적으로 컴퓨터범죄를 단속하고 있다.

주요 실적으로는 황우석 사건 수사, 현대자동차사건 수사, 외환은행 헐값매각 비리 사건(론스타 사건) 수사, 바다이야기 사건 수사, 일심회 사건 수사 등 사회적으로 이슈가 된 중요사건에서 디지털 증거를 수집·분석하여 범죄혐의를 입증하는 결정적인 증거자료를 확보하였다. 또한 첨단기술유출 사건에서 중요한 열쇠가 된 이메일을 복구, 분석하여 범죄혐의를 입증하는 증거자료로 제출하는 등 중요사건 수사 때마다 그 역량을 발휘하고 있다. 2005년도 디지털 증거 수집·분석 지원 실적 88건에서 2006년도 333건으로 전년대비 약 378% 증가하고 있다.

따라서 본 연구에서는 아래와 같은 필요성을 인식하고 Anti-Forensic에 대응하는 효율적인 방법 및 운영 시스템을 개발한다.

II. 관련 연구

2.1 국내 동향

한국정보사회진흥원의 2006년 조사 결과에 따르면, 국내 기업의 정보보호(보안) 제품 이용률은 90.6% 이고 방화벽, 침입 탐지·차단 및 방지 제품 이용업체 비율이 2003년부터 전반적으로 증가하고 있다. 하지만 일반 정보보호(보안) 제품은 법정 분쟁에 대비한 통합적인 기능을 제공하지 못한다. 일반 정보보호(보안) 제품은 사고에 대응한 절차를 간략하게 로그로서 기록하지만 이러한 기록이 차후에 있을 수 있는 법정 분쟁에 대비하여, 사고 대응 절차에서 획득한 데이터를 증거로서 제출할 수 있는 요건을 만족하지 못하는 경우가 존재한다. 정보화와 더불어 개인과 기업, 공공기관의 업무에서도 인터넷을 사용한 업무가 급격히 증가하고, 저장기술과 사용기술도 같이 발전하였다. 또한 정보의 보관방법도 종이, 테이

프와 같은 기존의 저장 장치에서 컴퓨터, PDA, 이동식 USB 저장 장치 등으로 다양화되고 있다.

현재 컴퓨터 범죄에서 디지털 증거의 압수, 수색 및 분석을 위한 다양한 방법이 연구되어 활용되고 있다. 경찰청 사이버 테러 대응 센터의 사이버 방지 및 해킹 기술동향 자료[1]에 의하면 1997년 126건에서 2003년 51,722건으로 급격한 증가 및 검거 현황을 보여주고 있다. 현재 한국에서는 원격 포렌식 시스템의 구축이 거의 전무한 상태이다.

2.2 포렌식

포렌식에서 수집된 데이터는 법정에서의 증거자료로써의 효력을 발휘하기 위해서는 데이터의 특성을 잘 알아 안전하게 다루어져야 한다[2,3].

포렌식의 분류로는 그림 1과 같이 나눌 수 있다. 데이터 포렌식과 시스템 포렌식을 나누는 보다 상세한 기준은, 휘발성 관련 된 데이터 쪽은 데이터 포렌식으로, 시스템에서 확인할 수 있는 증거는 시스템 포렌식으로 분류한다.

본 논문에서는 추적성 및 프로세싱 확보 차원에서 네트워크 포렌식 및 시스템 포렌식에 대하여 연구하고자 한다.

그림 1. 포렌식의 분류 및 기술
Fig. 1. Classification and description of the forensic

2.3 로그 정보

컴퓨터 시스템에 불법적으로 침입한 공 자는 흔적을 남기게 되는데 이러한 흔적이 저장되어 지는 곳을 로그 정보 파일이라 할 수 있다. 이러한 로그 정보 파일에는 시스템에 대한 스캔 행위, exploit 툴을 이용한 공격, 특정 사용자 계정으로의 접속, root 권한의 획득, 트로이 목마 설치, 자료 유출 및 삭제 등 공격자의 행위들이 기록되어 진다.

이미 시스템에는 이러한 로그가 다량 존재하며, 이를 분석하고 조합하고 추리하여 공격자의 행동을 추적하는 것이 포렌식 관점에서의 로그 히스토리의 의미라 할 수 있을 것이다.

로그 정보에 대한 분석 작업은 실제 범죄에 대한 분석 작업과 비슷한 형태를 지닌다. 다음은 실제 범죄가 일어났을 대 분석 방식으로 다음 두가지를 생각할 수 있다[4].

1) 다의성 포렌식 분석(Equivocal Forensic Analysis)

수집된 정보를 최대한 객관적으로 검토하고 모든 것에 의문을 가지고, 이용 가능한 증거 자체의 출처와 의미를 입증하여 조사관의 가설과 견해를 발전시켜 나가는 방법이다.

2) 행동 증거 분석(Behavioral Evidence Analysis)

수사의 초점, 용의자 범위 제한, 범죄자 선택 이해, 용의자들의 인터뷰 등을 통해 도움을 줄 수 있는 형태로 증거를 압축시키는 방법이다.

III. 본 론

3.1 Service Web Log Analyzer(SWLA)

3.1.1 웹로그를 통한 이용자 검색

본 논문에서는 웹서비스(아파치 2.x버전), 파일 전송 서비스(홈페이지 내용을 갱신할 목적으로 사용), 터미널 서비스(SSH, Telnet)가 사용 가능하다는 가정하에 연구하였다. 그림2는 서비스 웹로그 분석기(SWLA)의 위치를 보여주는데 SWLA가 어떠한 웹로그를 읽어들여야하는지는 Web Log List Properties라는곳에 관리자가 직접 명시를 해주게 된다.

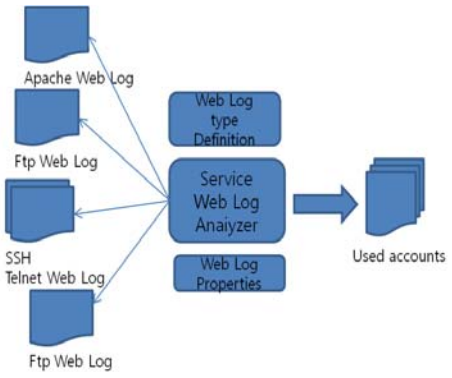

그림 2. 서비스 웹로그 분석기
fig. 2. Service Weblog Analyzer

3.1.2 Web Log List Properties

Web Log List Properties는 단순한 텍스트 파일이다. SWLA가 시작시 읽어들이는 웹로그 정보파일이다. 각 프로퍼티들은 '=' 을 기준으로 Key 와 Value로 매칭되게 되는데 항목들이 늘어날수록 SWLA가 분석해야하는 웹로그 양은 많아지게 됨으로 분석시간이 길어지게 된다.

① APACHE_WEB_LOG = /var/log/apache2/access_log
② FTP_WEB_LOG = /var/log/auth.log

③ SSH_WEB_LOG = /var/log/auth.log

위 3개의 항목은 Web Log List Properties의 내용이다. XXX_WEB_LOG형식에서 XXX는 어떤서비스를 사용하고 있는지를 나타내고 있다.

3.1.3 이용자 리스트 및 이용자 리스트 객체 생성

SWLA가 처리하고 난 최종결과물은 User Usage Shifter로 보내게 된다. User Usage Shifter는 일종의 임시 장소이다.

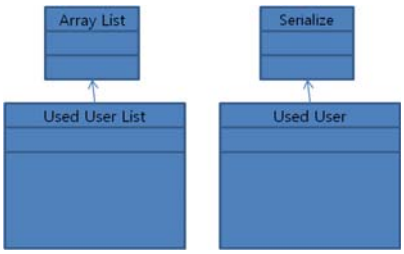

그림 3. 이용자 리스트 와 이용자 객체
fig. 3. User list and user objects

그림 3의 UsedUserList 객체의 경우는 Serialize를 구현하게 되는데 이것은 리스트(객체)를 파일시스템에 저장해놓았다가 필요시에 불러들이기위해서이다. 모든 웹로그 분석이 끝나면 UUS에게 파일 형태의 UsedUserList를 넘기게 된다. 오브젝트 파일형태로 저장하게 되면 다른 관리프로그램에서도 불러들여 사용가능하기 때문이다.

Ⅳ. 결 론

4.1 실험 평가

Linux PC를 구성하고 다중도메인 환경이라는 가정하에 진행하였다.

4.1.1 가상 평가 시스템 구축

표1. 평가시스템 환경
Table 1. Environmbental assessment system

분류	세부내용	
H/W	Pentinum4 2.8GB	
	Memory 512MB	
	Hard Drive 160GB	
S/W	OS	Gen too Linux TM
	LDAP	Open LDAPTM2.3.33
	WEB 서버	Apache2.059-r2
	SSH 서버	Open SSH 4_5pl_r2
	FTP 서버	Pure FTP 1.0.21-rl

표1은 가상의 환경을 구현하기위해 사용된 시스템이다. 실제 웹로그 데이터는 운영중인 서버를 테스트하기 어렵기 때문에 가상으로 구성하여 작업하였다.

4.1.2 SWLA를 사용한 이용자 분석

그림 4. 하루동안 사용된 이용자 검색 속도비교
fig. 4. Users browsing speed was used during the day compared

그림4는 SWLA와 기본 FIND 명령어를 통한 하루동안 사용된 이용자검색 속도를 비교한 것이다. 파일시스템을 검색한 결과보다 웹로그를 통하여 검색한 시간이 훨씬 빠른 것을 볼 수 있다.

4.2 기대 효과

본 논문은 웹로그 분석을 사용하여 웹서버를 통해 발송된 데이터들을 검색하였다. 디지털 증거 식별 및 수집 도구 모듈을 상이한 기능을 필요로 하는 모든 시스템에 쉽게 적용시켜 포렌식 증거 통합 DB를 이용하여 사이버 범죄에 효과적으로 대응하는 시스템 구축 및 개발이 용이할 것이다.

참고문헌

[1] Luoma. V., Forensics and electronic discovery: The new management challenge, Computer & Security, 25(2), 91~96, 2006

[2] Gary L Palmer. “A Road Map for Digital Forensic Research”, Technical Report DTR-T0010-01, Report for th First Digital Forensic Research Workshop(DFRWS), 2001.

[3] Venansius Baryamureeba, Florence Tushabe, "The Enhanced Digital Investigation Process Model", Digital Forensic Research Workshop, 2004.

[4] Kanellis, P., Kiountouzis, E,. Kolokotronis, N., & Martakos, D. (Eds.). “Digital crime and forensc science in cyberspace”. Journal of digital forensic practice. Hershey:Idea Group. 2006.