한국컴퓨터정보학회 동계학술대회 논문집 제22권 제1호 (2014. 1)

컴퓨터포렌식 지원을 위한 시스템 블랙박스 설계

장은겸°, 이중인*, 안우영**
°대전대학교 컴퓨터공학과
*(주)리얼타임테그
**대전보건대학 바이오정보과
e-mail: jangegu@nate.com°, jilee@realtimetech.co.kr, wyahn}@hit.ac.kr**

A Design of System Black-Box for Computer Forensics

Eun-Gyeom Jang°, Joong-In Lee*, Woo-Young Ahn**
°Dept. of Computer Engineering, Daejeon University
*Realtimetech Co., Ltd
**Dept. of Bio Information, Daejeon Health Sciences College

● 요 약 ●

컴퓨터 시스템을 기반으로 이루어지는 범죄 행위로부터 법적인 보호를 받기 위해 관련 법안이 개정되고 이를 수용하기 위한 컴퓨터 포렌식 지원 기술이 다각도로 연구되고 있다.
그러나 시스템 침해자의 시스템 공격 후 본인 흔적을 지우고 나가는 경우 침해자 추출이 어렵다. 또한 휘발성 정보의 손실이 발생하며 디스크에 저장된 비휘발성 정보의 경우 파일의 삭제 및 생성에 의해 디스크 저장영역의 중복된 사용으로 완전한 정보를 추출하는데 문제를 가지고 있다. 이러한 문제를 해결하기 위해 본 연구에서는 시스템 침해자의 공격 형태 및 상황, 환경을 유추하기 위해 행위자를 중심으로 휘발성의 정보를 수집하여 공격 당시의 시나리오의 재현이 가능한 컴퓨터시스템 블랙박스를 설계하였다.

키워드: 컴퓨터포렌식스(Computer Forensics), 접근제어(Access Control), 블랙박스(BlackBox)

I. 서 론

컴퓨터 포렌식스 도구들의 대부분은 디스크를 조사하여 침해의 흔적을 추적한다. 그러나 디스크에 저장된 데이터는 시간이 지남에 따라 파일의 삭제 및 생성이 반복되면서 디스크 표면의 데이터 저장 영역이 덮어 쓰는 현상에 의해 완전한 데이터를 복원할 수 없는 가능성이 크다. 완전한 데이터를 복원할 수 없다면 증거로서의 완전성을 인정받지 못한다. 또한 디스크에 저장된 증거 데이터가 누가 활용하고 접근 및 관련이 있는지에 대한 정보 또한 추적하기 어렵다. 즉, 증거는 있지만 누가 그 증거와 관련이 있는지 식별이 되어야 증거로서 가치가 있다.

따라서 본 연구에서는 시스템의 로그 및 이벤트, 프로세스 상태 정보를 감시하여 공격 로그를 확보하여 시스템 피해시 공격의 시나리오가 재현될 수 있도록 시스템에 블랙박스를 설치하여 역추적 및 공격 시나리오 추출이 가능하도록 하였다.

II. 컴퓨터 포렌식스 디지털증거관리

미국의 NIST에서 최초의 표준화된 디지털 증거 표준 가이드라인을 제시하고 이 가이드라인에 따라 증거 수집 및 분석이 이루어지도록 법적으로 보장하고 있다. 현재까지 관련된 국제 표준은 제정된 바가 없으며 증거 관리 도구의 신뢰를 위해서 미국에서는 NIST에서 검증을 시행하고 있다. 국내외에서 디지털 증거 관리 전문화된 도구로 EnCase, FTK, Safeback, dd, AFF, DEAS, FinalData가 존재한다.

III 컴퓨터시스템 블랙박스 설계

제안한 블랙박스 모델은 크게 3개의 영역으로 나눈다. 시스템 영역에서 정보를 수집하는 “시스템 정보 수집 모듈”, 네트워크 영역에서 정보를 수집하는 “네트워크 정보 수집 모듈”, 수집된 증거를 통합 관리하는 “시스템 통합 모듈”이다.

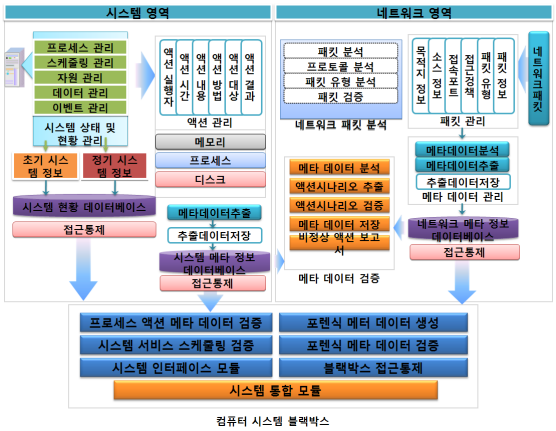

그림 8 컴퓨터시스템 블랙박스
Fig. 1. Computer System Black-Box

그림 1은 제안 시스템의 기본 모델로서 시스템 영역과 네트워크 영역에서 수집되어 로그 정보를 포렌식스 입장에서 유용하게 활용될 수 있도록 메타 정보를 수집하고 관리한다. 메타데이터는 수집된 정보의 육하원칙을 중심으로 관리되어 추후 문제가 발생하였을 경우, 편리하고 효율적인 증거물 관리가 될 수 있도록 한다.

시스템과 네트워크 영역에서 감지된 로그는 메타데이터를 추출하여 어떠한 개체가 이벤트를 발생했는지에 대한 육하원칙을 적용하여 로그를 관리한다. 그렇게 관리된 로그들은 시스템 프로세스 스케줄링에 의해 관리되어 시나리오 정보를 제공한다. 그러나 수집된 정보의 관리를 위해 제일 중요한 사항은 접근제어이다. 접근제어에 의해 증거물로서의 가치가 인정되고 인증되지 못한 정보 및 불법적인 수정에 의한 모든 증거물은 가치를 인정받지 못하고 시스템 관리에서 정보를 제공하지 못한다.

정보의 무결성 강화를 위해 비 신뢰적인 프로세스에 의한 중요 개체로의 접근을 차단하고 프로세스의 악의 행위를 차단하기 위해 무결성 강화 모델을 적용한다. 그림 2에서와 같이 동급의 등급의 주체라 하여도 개체에 대한 쓰기 권한이 없고 단지 생성된 개체에 대한 읽기 권한만이 주어져 생성된 개체에 대한 무결성을 강화한다.

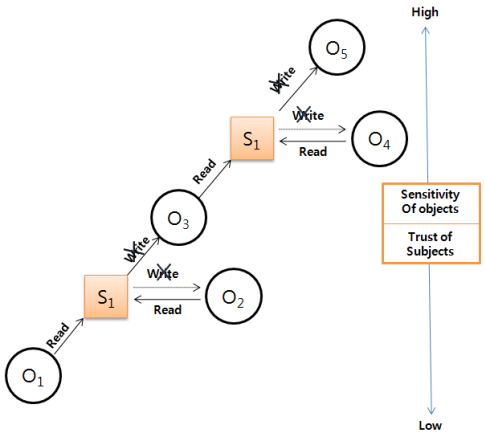

그림 2. 무결성 강화 접근 모델
Fig. 2. integrity tighten Control model

본 연구에서 제시한 모델은 설계영역으로 실제 시스템을 일부 구현하여 개인 PC 모델의 시스템에서 테스트하였다. 프로세스 로그를 일부 손실하여 추출하는 결과를 얻었으나, 과도한 이벤트 발생에 의한 결과로 유추하고 있다.

Ⅳ. 결 론

본 논문에서는 사이버에서 발생하는 악성 코드를 비롯한 시스템 오작동 등의 문제를 유추하거나 추적할 수 있는 로그 정보를 관리하는 기술을 설계하였다. 본 연구에서는 전체 영역을 구현하여 테스트를 하지는 못하였으나, 추후 로그 정보의 메타 데이터 추출 및 관리 기술의 보완을 필요로하며 제안한 접근제어 모델을 세부적으로 적용하여 안전하고 효율적인 시스템을 유지할 것이다.

참고문헌

[1] Eun-Gyeom Jang, "An Assurance Mechanism of Intrusion Data for Making Digital Evidence in Digital Computing Environment", Journal of KSII, Vol. 11, No. 4., August. 2010.

[2] Eun-Gyeom Jang, "A Study on Comparison of Road Surface Images to Provide Information on Specific Road Conditions," Journal of The Korea Society of Computer and Information, Vol. 17, No. 4, 2012.

[3] Kwank, Byong-Sun, "A study on Problems and improvements of digital forensic investigation", Journal of The Korean Law Association, Vol 42., May. 2011.