사이버 공격에 대한 시스템 정보 비교 및 분석 기술

윤현수*, 김용현**, 김동화**, 신동규*, 신동일*
*세종대학교 컴퓨터공학과
**국방과학연구소
e-mail:sug3nt7smd0djw@gmail.com

System Information Comparison and Analysis Technology for Cyber Attacks

Hyeon-Su Youn*, Yong-Hyun Kim**, Dong-Hwa Kim**, Dong-Kyoo Shin*, Dong-Il Shin*
*Dept of Computer Engineering, Se-jong University
**Agency for Defense Development

요 약

정보통신 기술이 발달하여 삶의 질을 높여주는 반면 미흡한 보안정책과 다양하고 강력한 해킹 기술들로 인한 피해가 늘어나는 추세이다. 이러한 해킹 피해 규모는 점차 커지게 되어 국가기반시설까지 영향을 미치고 있다. 본 논문은 어떠한 시스템에 사이버 공격이 행해졌을 때, 디지털 포렌식 기술과 공격트리를 융합하여 그 공격의 방법과 경로를 밝혀주는 기술에 대한 내용이다. 제안하는 기술은 각 기관의 특성에 맞게 해킹의 경로나 방법을 사용자에게 알리는 기능을 갖추었기 때문에 기관의 시스템 및 네트워크의 피해를 평가하는데 도움이 되며 그에 따른 솔루션들이 빠르게 결정될 것으로 기대된다.

1. 서론

21세기 정보통신 기술 및 유비쿼터스 기술의 발전은 국가 및 사회의 경쟁력 강화와 발전에 기반이 되고 있는 추세이다. 하지만 정보화 추진의 역기능으로 발생하는 다양한 보안문제는 국가 및 사회의 안정을 해치는 현실적인 위협으로 대두되고 있으며, 이러한 위협은 미래 유비쿼터스 사회로 발전함에 따라 더욱 심화될 것으로 예측된다[1].

지난 2016년 12월 5일, 국방부가 “군 인터넷 백신 체계 해킹사고 조사를 진행하던 중 국방망 일부 컴퓨터가 악성코드에 감염된 것으로 식별되었다.” 라고 밝힌 바 있다. 이어 최근 2017년 2월 7일 해병대 당국은 “사이버 지식정보방 PC에 연결된 프린터가 오작동하고 해킹 당했다는 메시지가 떴지만 바이러스 침투 등의 피해는 없었다.” 고 말했다.

이처럼 이제 해킹 공격은 단순한 개인 대 개인의 문제가 아니라 범국가적인 차원에서 당연히 주의해야할 문제가 되었다. 이러한 해킹 공격으로 인해 특정 시스템이 공격당하게 되면 시스템에는 공격당한 곳의 정보가 어떻게든 수정되어 있기 따름이며 그 흔적은 시스템의 어딘가에는 존재할 것이다. 따라서 본 논문에서는 해킹 공격을 당한 후 공격에 대한 것들을 비교 및 분석하는 시스템을 제안한다. 2장에서는 시스템의 주요 정보 중 휘발성 정보 등을 수집하는 방법에 대한 설명과 수집된 정보에 대한 필요한 설명 및 정보 수집을 위한 간략한 공격트리를 제시한다. 휘발성 정보는 시스템의 전원을 차단하는 순간 사라지는 데이터를 의미하며, 이는 레지스터, 캐쉬, RAM 들의 휘발성 매체에 저장되어 있다. 이러한 정보를 얻기 위해서는 시스템의 전원을 차단하기 전에 시스템 정보를 얻기 위한 명령어 및 도구를 이용한다. 이렇게 디스크 분석으로는 획득할 수 없는 활성 데이터를 수집하고 이를 분석하는 것을 라이브 포렌식(Live Forensic)이라고 한다[2]. 3장에서는 2장에서 설명한 시스템의 주요 휘발성 정보 등을 비교하는 방법과 이후 피해 평가에 적용하는 방법에 대해 설명한다.

2. 관련 연구

본 논문에서 제안한 시스템에서는 어느 정도의 디지털 포렌식 개념이 들어가 있다. 시스템이 공격당했을 때 해당되는 공격방법과 공격경로를 도출하기까지 디지털 포렌식의 절차를 따라간다고 볼 수 있기 때문이다.

디지털 포렌식(Digital Forensics)이란 사이버 범죄, 정보 유출 등과 관련된 디지털 증거가 법적 증거력을 갖게 하기 위해 디지털 데이터를 수집, 보관, 분석, 보고하는 과학적이고 논리적인 절차와 방법을 의미한다. 포렌식 기술은 컴퓨터 관련 범죄수사를 위한 국가기관 뿐만 아니라, 회계 부정 방지, 기업 내부 기밀유출 방지 등 기업에서의 내부 보안 강화를 위해 활용될 수 있다[3].

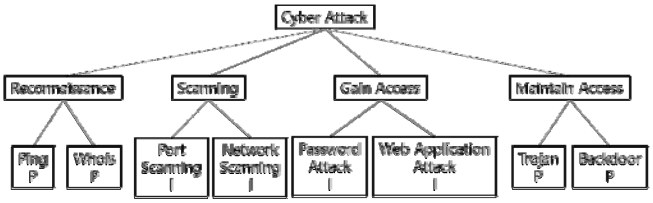
디지털 포렌식 중 라이브 포렌식으로 얻을 수 있는 휘발성 정보들은 컴퓨터 시스템이 종료되면 사라지는 특성

을 갖고 있다. 본 논문에서는 이러한 특성을 지닌 휘발성 정보를 이용하여 공격자의 공격방법과 공격 경로를 도출해낼 수 있는 기술을 설명한다.

시스템의 휘발성 정보는 여러 가지가 있다. 다양한 휘발성 정보들은 시스템 내에서 명령 프롬프트를 이용한 명령을 통해 알아낼 수 있기도 하고, 실제 공격을 받았을 때 특정 명령 입력 시, 내용이 달라졌다는 것을 알 수 있다[4].

(그림 1) 정보 수집 구성

그림 1과 같이 정보수집이 완료 되었다면 수집된 정보를 분석해야한다. 그런데 수집된 정보를 분석할 때 어떤 공격이 쓰였고 어떤 경로를 통해 공격이 이루어졌는지를 도출해야 하는데 도출하기 위해서는 공격트리를 제작해야 한다.



(그림 2) 공격 트리 일부 목록

위 그림 2는 사용자가 쓰임에 따라 작성해야하는 공격 트리 목록 중 일부를 노드형태로 표현한 것이다. 이 트리에서 부모노드는 공격의 목표를 의미하고 자식노드들에는 가능한 공격과 불가능한 공격을 각각 P와 I로 분류해놓았다[5].

3. 정보 비교 방법 및 결과

제안한 시스템을 사용하기 위해서는 '백업을 위한 수집'과 '정보를 비교하기 위한 수집' 이 필요하다. 수집한 데이터에는 시스템의 주요 휘발성 정보들이 포함되어 있으며 이 정보들을 이용하면 후에 사용자가 입은 피해에 대한 평가를 할 수 있어 굉장히 유용할 것으로 예상된다.

3.1 덤프 파일 수집(DFC, Dump File Collect)

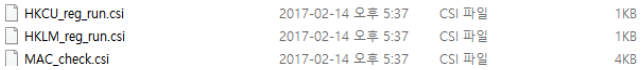
DFC는 백업을 위해 정상적인 시스템의 상태를 수집하는 작업이다. 본 논문에서는 자체적으로 DFC 작업이 가능한 간단한 프로그램을 만들어 실행하였다. DFC 작업의 결과로 수집된 파일에 sid(System Information Dump)라는 임의의 확장자가 붙여져 저장되어진다. 이 파일들은 후에 정보를 비교할 때 비교되어지는 대상파일이 된다.

(그림 3) 백업을 위해 수집된 SID 파일들의 예

위 그림 3의 파일들은 순서대로 HKEY_CURRENT_USER의 자동실행되는 파일들을 저장시킨 파일, HKEY_LOCAL_MACHINE의 자동실행되는 파일들을 저장시킨 파일 그리고 ARP 테이블을 저장시킨 파일들이다.

3.2 현재 상태 수집(CSC, Current State Collect)

CSC는 사용자가 원할 때, 그 때의 시스템의 상태를 수집하는 작업이다. CSC 작업의 결과로 수집된 파일에 csi (Current System Information)라는 임의의 확장자가 붙여져 저장되어진다. 이 파일들은 SID 파일들과 비교하기 위해 만들어지는 파일들이다.

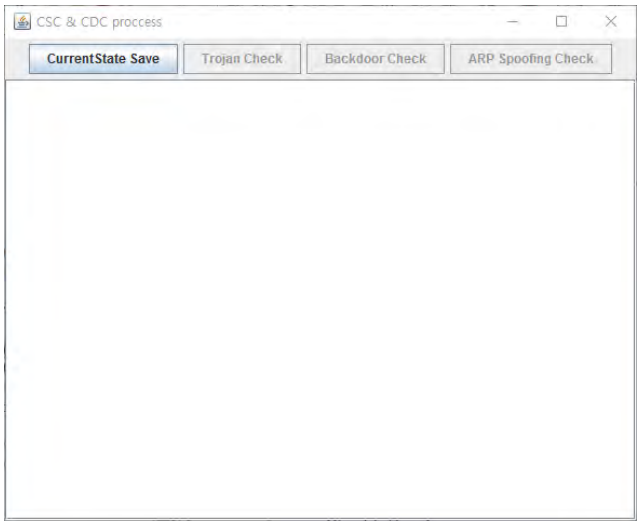


(그림 4) SID 파일과 비교하기 위한 CSI 파일들의 예

위 그림 4는 그림3의 파일과 같은 HKEY_CURRENT_USER의 자동실행되는 파일들을 저장시킨 파일, HKEY_LOCAL_MACHINE의 자동실행되는 파일들을 저장시킨 파일 그리고 ARP 테이블을 저장시킨 파일들이다.

3.3 DFC와 CSC 비교(CDC, Comparison DFC and CSC)

CDC는 DFC와 CSC를 비교하기 위한 과정이다. 이 과정은 제안한 시스템의 가장 핵심적인 작업이라고 봐도 무방하다. DFC 과정을 거친 후, CSC 과정이 이루어지는데 사실 CSC와 CDC는 같은 프로그램에서 작업이 이루어진다고 할 수 있다. DFC 작업의 결과로 얻은 SID 파일과 CSC 작업의 결과로 얻은 CSI 파일은 텍스트로 짜여져있다. CDC 작업을 통해 서로 동일한 파일명을 가진 SID와 CSI 파일을 텍스트 형식으로 비교하게 된다.

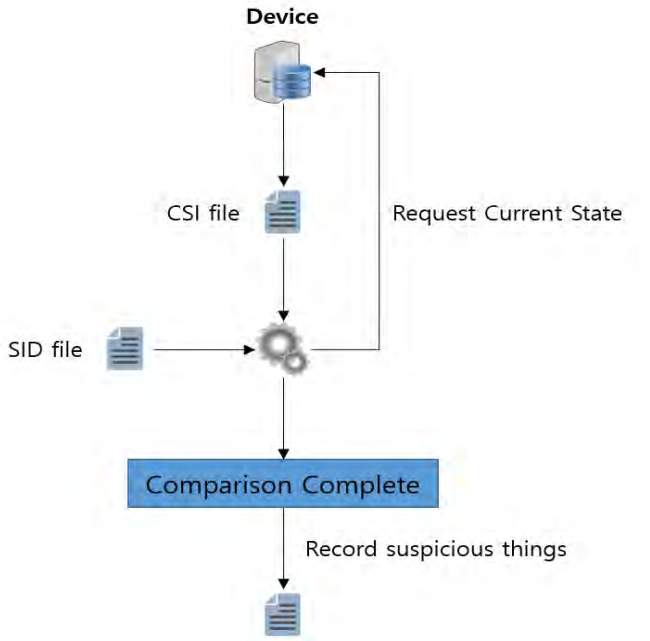


(그림 5) CSC와 CDC 작업이 이루어지는 프로그램의 예

위 그림 5에서 Current State 버튼을 누르면 오른쪽에 3가지의 공격에 대한 체크를 할 수 있는 버튼이 활성화되며 각 공격에 대한 체크를 하는 버튼을 누를 시, 공격으로 인해 수정된 파일의 내용 및 정보, 그 경로가 아래의 텍스트 뷰에 쓰여진다.

3.4 시스템 작업 과정

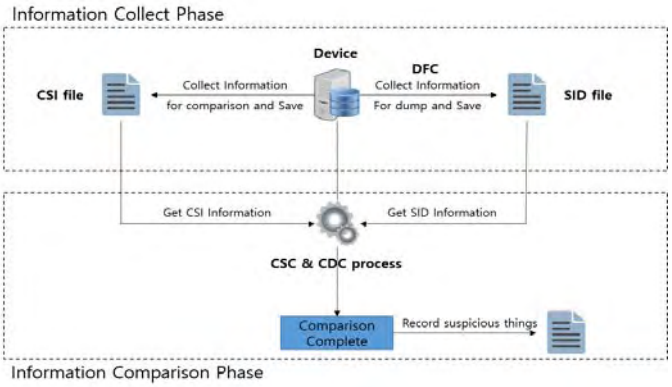
제안한 시스템에서 핵심 작업과정은 바로 CDC인데, 아래 그림은 CDC의 작업 구조와 그 과정을 보여준다.



(그림 6) CDC 작업 구조 및 과정

그림 6에서 제일 상단의 Device는 서버와 같은 것들을 의미한다. 제일 좌측에 있는 SID 파일은 비교되기 전 미리 저장이 되어 있어야 하며, CSI 파일은 프로그램이 요청할 시, 저장이 된다. SID, CSI 두 파일이 모두 저장되면 비교작업이 이루어지고 의심스러운 부분을 파일로 저장한다.

4. 시스템 설계 구조 및 단계



(그림 7) 시스템 설계 구조

그림 7은 제안하는 시스템의 구성도이다. 시스템의 단계에는 Information Collect Phase와 Information Comparison Phase 두 단계로 나뉘어 진다. 먼저 Information Collect Phase에서는 CSC, DFC 과정이 이루어져 시스템의 정보를 획득할 수 있게 해준다. Comparison Information Phase에서는 Collect Information Phase에서 얻은 정보들을 비교해 주는 CDC 작업이 이루어진다. 비교 작업이 완료되면 의심스러운 부분들을 분석하여 공격방법, 공격경로 등을 파일로 저장하는 것으로 끝이 난다.

5. 결론

본 논문에서는 시스템의 정보를 수집하여 파일로 저장하고 이 파일을 이용하여 시스템이 받은 공격의 방법 및 경로를 파악할 수 있게 만들었다. 제안한 시스템을 이용하면 공격당한 시스템의 피해에 대한 평가가 가능할 것으로 예상된다.

ACKNOWLEDGEMENT

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

참고문헌

[1] 김건우, 홍도원. “고속 디지털 포렌식 기술.” 정보보호학회지, 19(5), 45-51.

[2] 한지성, 이상진. “라이브 포렌식을 위한 윈도우즈 물리 메모리 분석 도구.” 정보보호학회논문지, 21(2), 71-82.

[3] 김승권, 김상국, 최종화. “미래 사이버전 및 대비방안.” 정보과학회지, 26(1), 75-86.

[4] Brezinski, D., and Tom Killalea. “Guidelines for evidence collection and archiving.” No. RFC 3227.

[5] Schneier, B. “Attack trees.” Dr. Dobb’s journal, 24(12), 21-29.