개인정보보호 기술을 활용한 디지털 포렌식 수사 모델 연구

A Study on the Digital Forensic Investigator Model using Privacy Protection Technology

장 희 영, 박 구 락, 김 재 웅
공주대학교

Jang hee-young, Park koo-rack, Kim jea-woong
Kongju National Univ.

요약

급속한 현대사회의 정보화로 인하여 개인 정보에 대한 정보 유출 및 위협의 빈도가 높아지고 있는 상황에서 기존의 디지털 포렌식 수사 모델에서 사용하고 있는 해시 검색 프로세스는 개인정보 노출에 취약한 파일이 존재하고 있다. 이에 본 논문에서는 개인정보 노출 취약점 진단을 추가한 해시 검색 프로세스를 제안한다. 이를 통하여 정밀 조사와 일반 조사 대상을 정확하게 파악할 수 있을 것으로 기대된다.

I. 서론

IT 기술의 발전으로 대부분의 데이터들이 정보화가 되어 지고 있고, 개인정보 또한 급속히 정보화가 이루어지고 있는 실정이며, 이로 인하여 매년 수백만 건의 해킹이 시도되고 있다. 과거에는 개인정보가 신분을 확인하는 정도로만 사용되었지만, 현재는 전자상거래, 금융 관리 및 인터넷을 사용한 모든 활동에 대부분 사용이 되어 지고 있다고 할 수 있다. 그러나 이러한 개인정보가 개인의 실수 또는 관리자의 실수나 프로그램의 오류 등으로 인하여 개인정보 유출이 증가하고 개인정보에 대한 위협 빈도가 높아지고 이에 따라 개인정보 침해 사고의 발생 가능성 또한 더욱 증가되고 있다[1].

이에 본 논문에서는 최근 개인정보보호 동향 및 기술, 개인정보 유출 사례를 분석하고 디지털 포렌식 기술을 활용한 개인정보보호 기술을 제안한다.

Ⅱ. 관련연구

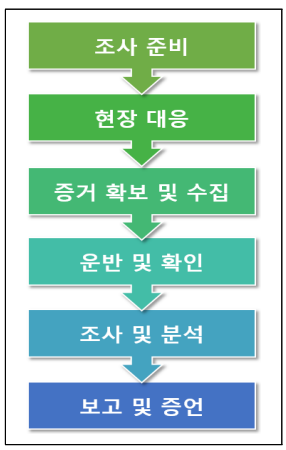
1. 개인정보보호기술

개인정보보호 기술은 크게 기술 기반 정책 및 관리 기반으로 분류할 수 있다. 기술 기반에는 프라이버시 보호 진단 기술, 프라이버시 노출관리 기술, 개인정보보호 통신 기술, 개인정보보호 저장 기술로 분류 된다. 프라이버시 보호 진단 기술은 개인정보 노출의 위험을 진단하는 기술이고, 프라이버시 노출관리 기술은 정보 유출을 방지하기 위해 전체 정보를 저장하거나 사전 에 점검하는 대응하는 기술이다 또한 개인정보보호 통신 기술은 개인정보 사용하기 위해 적용하는 SSL, 응용 보안 등과 같은 보안 기술이 포함된다.

개인정보 보호 정책은 P3P(Platform for Privacy Preferences Project)등과 같이 정책 기반 기술이고, 개인정보 보호 정책 기술은 개인정보가 유출되지 않는지 등을 관리하는 기술이다.[2]

2. 디지털 포렌식 수사 모델

디지털 포렌식은 정보기기 내 자료를 근거로 삼아 그 정보기기를 사용하여 발생한 문제의 사실을 증명하는 보안 서비스이다[3]. 디지털 포렌식 수사 모델을 살펴보면 디지털 포렌식을 수행하기 위한 절차로 정의 하고 있다. 디지털 포렌식 수사 모델을 정리하면 다음의 (그림 1)과 같이 “조사준비, 현장 대응, 증거물 확보 및 수집, 운반 및 확인, 조사 및 분석, 보고 및 증언” 6단계로 정의 할 수 있다[4].



▶▶ 그림 1. 디지털 포렌식 수사 모델

Ⅲ. 제안 모델

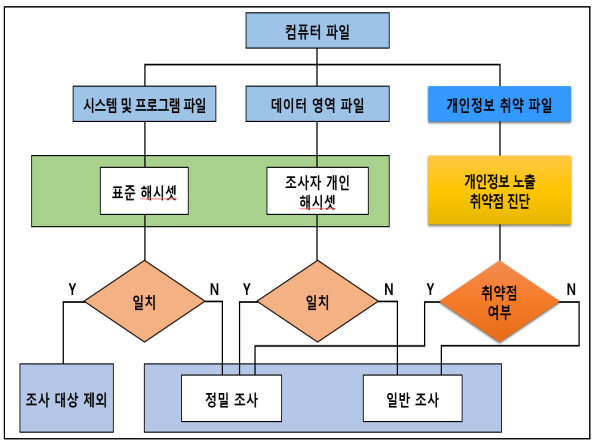
디지털 포렌식 수사 절차 6가지 단계에서는 단계 별로 디지털 기기 및 데이터 유형 숙지, 시스템 파악 및 정밀 수색, 데이터 수집 및 사본 생성, 데이터 무결성 확인, 증거물에 대한 인증, 데이터 분석, 분석된 데이터 및 모든 검증 과정을 기술하고 있다.

본 논문에서는 개인정보보호 기술 중 기술기반 프라이버시 보호진단 기술 중 하나인 개인정보 노출 취약점 진단을 활용하여 6가지 절차 중에서 증거 및 분석에 해당하는 검색 항목 중 해시 검색 항목을 추가하여 기존 검색 프로세스에서 개인정보 노출에 있어 취약한 파일을 구분하고 검사하여 상세하고 체계적인 데이터 분석 모델을 제안한다.

기존의 해시 검색 프로세스는 기 구축된 파일의 해시셋을 사용하여, 조사 분석 대상을 식별하고 검색 수준을 선정 할 수 있는 기술이다. 기존 해시 검색 프로세스는 모든 컴퓨터 파일에서 시스템 및 프로그램 파일과 데이터 영역 파일로 구분되고, 시스템 및 프로그램 파일은 정형화 되어 있기 때문에 표준 해시셋과 비교하여 일치하게 되면 조사 대상에서 제외되고, 표준 해시셋과 일치하지 않으면 정밀 조사 대상이 된다. 데이터 영역 파일은 비정형화되어 있어 조사자 개인 해시셋을 설정하여 비교하고 데이터 영역 파일과 조사자 개인 해시셋이 일치하면 정밀 조사 대상이고, 일치하지 않으면 일반조사 대상이 된다.

하지만 이 프로세스에서는 시스템과 데이터 영역 파일에 대한 검색 구분만 있을 뿐 개인정보 노출에 대한 구체적인 검색 구분이 없어 추후 조사 결과 개인정보 유출 또는 취약점이 발견 되었을 시 다시 개인정보 취약점에 대해서 검사하고 조사해야하기 때문에 비효율적인 방법이라 할 수 있다.

다음의 (그림 2)는 개인정보 노출 취약점 진단을 추가한 제안 모델 해시 검색 프로세스 이다.



▶▶ 그림 2. 제안 모델 해시 검색 프로세스

본 논문에서 제안하는 프로세스는 기존 프로세스처럼 모든 컴퓨터 파일에서 시스템 및 프로그램 파일과 데이터 영역 파일을 구분하여 해시셋을 비교하고 정밀 조사 대상과 일반 조사 대상으로 구분을 하는 것은 방법적으로 같으나, 시스템 및 프로그램 파일과 데이터 영역 파일 외 개인정보에 취약한 파일을 구분하고 파일에 대해 개인정보 노출 취약점 진단을 하여 취약점이 존재하면 정밀 조사 대상으로 구분, 취약점이 존재하지 않을 경우 일반 조사 대상으로 구분할 수 있다. 개인정보 노출 취약점을 진단하여 정밀 조사와 일반 조사 대상으로 구분하게 되어 검사하고 조사하게 되면 기존 프로세스에서 나타날 수 있는 비효율적인 방법을 보완 할 수 있다.

Ⅳ. 결론 및 향후 연구 방향

기존 디지털 포렌식 수사 모델 중 조사 및 분석 단계의 해시검색 프로세스는 개인정보 노출에 취약한 파일에 대한 보완이 필요하다. 본 논문에서는 개인정보 노출 취약점 진단을 추가한 해시 검색 프로세스를 제안함으로서, 개인정보 노출에 취약한 파일을 진단하고 정밀조사와 일반조사 대상을 구분함으로 분석하는데 있어, 체계적이고 효율적인 방법이라 할 수 있다. 또한 디지털 포렌식 수사 모델에 마지막 단계인 보고 및 증언 단계에서도 활용 할 수 있을 것으로 기대된다. 향후 연구에서는 개인정보 노출을 포함한 포괄적인 보안 취약점 진단을 적용한 디지털 포렌식 수사 모델에 관한 연구가 계속되어야 할 것이다.

▌참 고 문 헌▐

[1] 이규안, “개인정보보호를 위한 디지털 포렌식 기법 연구”, 한국전자통신학회, 학술대회, 제 5권, 제 2호, pp. 337-341, 2011.

[2] 남기효, 박상중, 강형석, 남기환, 김성인 “개인정보보호 기술의 최신 동향과 향후 전망”, 한국정보보호학회, 학회지, 제 18권, 제 6호, pp. 11-19, 2008.

[3] 정익래, 홍도원, 정교일, “디지털포렌식 기술 및 동향”, 전자통신동향분석 제 22권, 제 1호, pp. 97-104, 2007.

[4] 이창훈, “개인정보보호법 기반 디지털 포렌식 수사모델 연구”, 한국항행학회, 논문지, 제 15권, 제 6호, pp. 1212-1219, 2011.