**[네트워크 포렌식을 위한**

**패킷분석 및 데이터 복원]**

**(제안서)**

2016년 03월

호서대학교 공과대학 정보보호학과

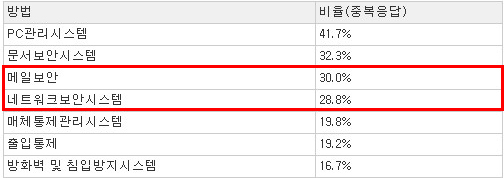
|  |  |  |
| --- | --- | --- |
| **제 출 문** | | |
| **과 제 명** | 포렌식을 위한 네트워크 패킷  분석 및 데이터 복원 | |
| **참여학생** | 학 번 | 성 명 |
| 20111748 | 위푸름 |
| 20123381 | 유진영 |
| 20122343 | 김수진 |
|  |  |
| **수행기간** | 2016.03.01 ~ 2016.00.00 | |
| 본 보고서를 호서대학교 정보보호학과  정보보호 프로젝트 제안서로 제출합니다.  2016년 3월 14일  **호서대학교 정보보호학과 학과장 귀하** | | |

프로젝트의 필요성

최근 국내외에서 기업내부의 기밀정보를 유출하는 경우가 빈번하게 발생하고 있는데,유출사항으로는 아래의 [그림1]과 같이 데이터 유출 다음으로 이메일 및 메신저를 통한 유출이 많음을 확인할 수 있다. 이러한 유출은 기업의 막대한 손실을 불러오며 나아가 핵심기술의 경우에는 국가적 손실까지 불러올 수 있는 위험성이 존재한다.

[그림 1] 기밀정보 유출 경로

하지만 현실은 기업의 담당자는 물론 일반 직원들은 보안에 대한 인식이 저조할 뿐 아니라 중소기업의 경우 교육이 기업내의 보안교육이 제대로 이루어지지 않은 경우가 대부분이며 이에 지속적으로 문제점이 발생하였다. 기업들의 유출방지 대응방안으로는 아래 [그림2]와 같이 가장 많이 적용된 PC관리시스템도 50%가 넘지 않는 상태이며, 그 중에서도 메일 보안 및 네트워크보안시스템의 경우는 겨우 30%정도의 저조한 상태를 보여주고 있다.

[그림2] 기술유출방지 대응 시스템

그나마도 기술유출방지를 위해 인프라가 구축이 되어있고, 각종 보안프로그램이 설치되어 있다 해도 많은 사내 규정과 승인절차에 사용자가 불편함을 느껴, 설치하였다가 삭제하거나, 설치하지 않는 경우도 없지 않다. 또한 기업의 기밀을 유출시키는 원인인 경쟁사의 산업스파이의 경우 이러한 환경에서 사내 기밀문서를 유출할 확률이 높으며, 이를 방지하기 위해 디지털 포렌식을 활용하여 기업 기밀문서의 유출을 최소화 할 수 있다.

이러한 데이터 유출 문제들을 해결하기 위해 근래에 들어서는 디지털상의 자료(메시지 내용, e메일, 로그 등)들도 법정에서 증거로 효력이 입증되면서부터 국가적인 차원에서 해당 분야에 대한 관심이 증가 하고 있다. 하지만 디지털 정보는 원본과 복사본의 구분이 어렵고, 위·변조가 용이하여 증거로서의 진정성을 의심하지 않을 수 없다. 따라서 디지털 정보가 증거로서의 가치를 인정받기 위해서는 정보의 수집·보존·처리 전 과정에서 특별한 절차와 방법을 필요로 한다. 따라서 디지털 정보를 근거로 하여 범죄행위의 사실관계를 규명하고 인과관계를 입증하는 과학적 수사기법인 디지털 포렌식이 요구된다

디지털 포렌식 혹은 컴퓨터 포렌식(Computer Forensic)은 전자적 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 말한다. 과거에 얻을 수 없었던 증거나 단서들을 제공해 준다는 점에서 획기적인 방법이다. 컴퓨터 포렌식은 사이버 해킹 공격, 사이버 범죄 시 범죄자들은 컴퓨터, e메일, IT기기, 스마트폰 등의 운영체제, 어플리케이션, 메모리 등에 다양한 전자적 증거를 남기게 되면서, 사이버 범죄자 추적 및 조사에 핵심적인 요소가 되고 있다.

[표 1] 디지털 포렌식(Digital Forensics)유형

|  |  |
| --- | --- |
| 디지털 포렌식 유형 | 설 명 |
| 네트워크 포렌식  (Network Forensics) | 네트워크로 전송되는 데이터를 대상으로 증거 획득 및 분석 |
| 활성데이터 포렌식  (Volatile data Forensics) | 휘발성 데이터를 대상으로 증거 획득 및 분석 |
| 디스크 포렌식  (Disk Forensics) | 비휘발성 저장매체(하드디스크, SSD, USB, CD 등)를 대상으로 증거 획득 및 분석 |
| 이메일 포렌식  (Email Forensics) | 이메일 데이터로부터 송/수신자,송/수신 시간,내용 등의 증거 획득 및 분석 |
| 웹 포렌식  (Web Forensics) | 웹 브라우저를 통한 쿠키,히스토리,임시파일,설정 정보 등을 통해 사용 흔적 분석 |
| 모바일/임베디드 포렌식  (Mobile/Embedded Forensics) | 휴대폰,스마트폰, PDA, 네비게이션,라우터 등의 모바일 기기를 대상으로 증거 획득 및 분석 |
| 멀티미디어 포렌식  (Multimedia Forensics) | 디지털 비디오,오디오,이미지 등의 멀티미디어 데이터에서 증거 획득 및 분석 |
| 소스코드 포렌식  (Source code Forensics) | 프로그램 실행 코드와 소스 코드의 상관관계 분석,악성코드 분석 |
| 데이터베이스 포렌식  (Datavase Forensics) | 방대한 데이터베이스로부터 유효한 증거 획득 및 분석 |
| 안티포렌식  (Anti-Forensics) | 데이터 완전 삭제,암호화,심층암호(Steganography) |

위의 [표 1]과 같이 디지털 포렌식의 유형 중 네트워크 포렌식은 패킷에 대한 심층분석을 해야 하는 만큼 중요한 기술 임에도 불구하고 국내에서는 아직까지 많은 연구가 이루어지지 않았으며,더욱이 해당 분야에 대한 인력도 충분하지 않은 상태이며 그것을 활용한 실무 분야는 조금씩 활성화 되어가고 있지만, 아직까지 기업에서 그것을 활용한 감사는 진행되지 않고있다. 따라서 기업의 유출된 문서에 대해서는 리스크를 줄이기 위하여 사후 분석 과정이 필요하고 해당 공격패턴분석을 통해 시그니처를 정립해 추후에 공격을 막을 수 있다.

프로젝트 목표 및 내용

2.1 프로젝트 목표

최근 국내외에서 기업 내부의 기밀정보가 e메일·메신저 등 네트워크를 통해 유출되는 경 우가 빈번하게 발생하고 있지만 네트워크를 통한 기술유출 대응방안 연구는 미흡한 실정 이다. 따라서 본 프로젝트의 결과물인 파일 복원기능을 통해 기업의 보안 담당자 혹은 감사원이 유출된 파일에 대한 리스크 분석을 용이하게 하고, 국가별 IP traffic 통계 자료를 통해 기술유출 경로 파악을 용이하게 한다. 또한 I/O Traffic 통계 및 최다 사용 프로토콜 정보를 제공함으로써 기업 내 네트워크 품질 개선을 용이하게 하고자 한다.

프로젝트의 추진전략 및 방법

3.1 개발 환경

OS: window 10

사용 언어: python, c, css, javascript, html

사용 프로그램: VMware, github, sourceinsight, sublime text

3.2 역할 분담

|  |  |
| --- | --- |
| 위푸름 | UI·UX 디자인 및 PPT제작, front-end 개발 |
| 유진영 | Back-end 개발 |
| 김수진 | front-end 개발 |

3.3 일정

프로젝트 결과의 활용 방안 및 기대효과

기업의 보안담당자 혹은 감사원은 의심되는 이용자에 대한 색출과 이용자가 한 행위(파일 전송, 메일전송 등)를 파악하기 위하여 기업 내에 있는 보안관제부서에 해당 이용자의 행위에 대한 네트워크 패킷을 요구하여 분석을 실시할 수 있다.

따라서 회사 내규 등에 임직원 프라이버시 침해가 아닌 기업 리스크관리를 위한 모니터링의 취지를 명확히 밝히고 임직원 동의서를 받은 후 네트워크 패킷 분석을 통한 모니터링으로 비정상 네트워크 트래픽 탐지, 인터넷 사용내역,접근 사이트 내용, 이메일 수신 및 발신 기록 등 다양한 분야에서내부통제 강화 용도로 활용 된다.

IPS와 방화벽의 경우 보통 시그니쳐 기반으로 탐지하여 공격의 유무 판단을 위주로 수행을 한다면 본 프로젝트의 프로그램은 그 행위에 대하여 더 나아가 패킷 심층분석을 통해 외부로 빠져나가는 파일에 대한 실질적인 정보습득과 복원을 수행한다. 이러한 과정에서 유출된 문서의 최종 목적지 추적 및 파일 복원을 통한 해당 유출자에 대한 징계 근거자료로 제출될 수 있다.

네트워크 패킷 분석을 통한 데이터 복원 기술은 패킷들을 파일 및 프로토콜 정보를 이용하여 원래의 파일의 형태로 복원하기 위한 기술이다. 이 기술을 이용하여 프로토콜의 트래픽을 분석할 수 있으며, 파일이 아닌 다양한 제어 패킷들도 수집/복원되고, 이런 정보들을 통해서 비인가 사설 FTP서버 접속 탐지, 특정 프로토콜을 이용한 비인가 서비스 이용 탐지 등과 같은 보안사고를 예방할 수 있다.