기밀 파일 정의를 위한 시그니처 삽입 기법

신규진* · 정구현* · 이태룡* · 양동민** · 이봉환*

*대전대학교,**전북대학교

A Signature Inserting Scheme for Defining Confidential File

Gyu-jin Shin* · Ku-hyun Jung* · Tae-ryong Lee* · Dongmin Yang** · Bong-hwan Lee*

*Daejeon University · **Jeonbuk National University

E-mail : shin111134@naver.com

요 약

최근 기업의 내부 기밀파일 유출이 급증하고 있으며, 이로 인해 기업에 심각한 피해를 주고 있다. 이러한 유출의 대부분은 기업 내부 직원들에 의해 발생되고 있다. 본 논문에서는 다양한 파일 형식의 내부 기밀 파일의 외부 유출 탐지를 위해 기밀 파일 정의를 위한 시그니처 삽입 기술을 제안하고 구현하였다.

ABSTRACT

Recently internal confidential file leakage of industry is substantially increasing, which results in serious damage to enterprises. Most of these outbreaks are caused by internal employees. In this paper, we proposed and implemented a signature insertion scheme for defining confidential file in order to detect the outflow of internal confidential files with various file formats.

키워드

데이터 유출 방지, 시그니처 삽입, 기밀파일, 파일보안

Ⅰ. 서 론

글로벌 경쟁시대에 각 기업의 핵심기술은 기업의 경쟁력만이 아니라 국가의 경쟁력과도 관련이 있다. 우리나라의 산업 기술들은 세계적인 수준이며, 중소기업 및 벤처기업들은 다양한 첨단기술들을 보유하고 있다. 그러나 대기업의 경우에는 고가의 데이터 유출방지(DLP, Data Loss Prevention) 기술을 내부적으로 사용하고 있는 반면, 중소기업이나 벤처기업들은 이러한 기술을 가지고 있지 못하고 있는 것이 현실이다[1][2].

본 논문에서는 고가의 DLP 기술을 사용할 수 없는 중소기업이나 벤처기업들을 위해 파일필드에 고유의 시그니처를 삽입하여 기밀파일을 정의할 수 있는 기법을 제안한다.

Ⅱ. 관련연구

2.1 DLP

네트워크 기반 DLP는 메일, 메신저, 웹 메일, 웹 하드, 웹 게시판, P2P, SNS, 터미널 서비스, 프락시 서비스 등 정보 유출에 대해 네트워크 단에서 감시하고 통제하는 역할을 수행한다. 네트워크 기반 DLP는 Monitor와 Prevent 등 2개의 그룹으로 나뉜다. Monitor는 Network Mirroring 방식으로 운영되며, 감시와 차단 전용으로 다양한 유출 경로에 대한 Coverage가 핵심이다. Prevent는 프록시 방식으로 원천적으로 유출을 사전에 차단하는 방식을 의미하는데, 대표적으로 Mail Proxy와 DB Proxy가 있으며, 사전 통제 기능 때문에 도입 시에는 선호되지만 제공하는 프로토콜이 한정적이고 과도한 차단 현상으로 인해 실제 운영에서는 Monitor 형태가 선호된다. 종점 DLP/Discovery 기술은 USB 등의 미디어와 출력물을 통한 유출방지 기능을 처리한다. 예를 들어 USB로 복사하려는 파일에 주민번호, 계좌번호, 카드 번호 등 개인정보나 주요 기밀문서의 키워드 등이 포함되어 있을 경우, 이를 식별하고 차단한다. 기밀 데이터가 유출될 수 있는 다른 채널들은 접속을 차단하지만 USB나 출력물은 정당한 업무를 수행하기 위해 적극적으로 활용될 수 있기 때문에 통제의 대

상이 된다. 또한 최근 종점 DLP는 RF 통신, 블루투스 통신, 테더링 등 통신에 대한 차단 기능까지 제공한다[3][4].

Ⅲ. 시그니처 삽입 시스템 설계 및 구현

3.1 시스템 구성

시그너처 삽입시스템은 시그니처 탐지 모듈(Signature Detect Module)과 시그니처 삽입 모듈(Signature Insert Module)로 구성된다. 제안시스템은 Windows 7 및 10 환경의 .Net Framework 기반에 일반 파일의 파일 필드에 시그니처를 추가 및 삽입하는 방식으로 구현하였다.

3.2 시그니처 탐지모듈

.Net Framework의 FileSystem Watcher 클래스를 이용한다. FileSystemWatcher는 특정 디렉토리에 존재하는 불특정 File에 대한 감시자 역할을 수행한다. 먼저 특정 경로를 지정한다. 지정된 경로 하위에 복사 또는 생성되는 파일에 대한 감시를 진행한다. 이러한 작업이 감지되었을 때, 미리 지정한 파일 형식의 확장자를 가진 파일일 경우 FileStream을 이용해 해당 파일의 전체를 Byte 단위 임시 버퍼로 복사한다. 해당 버퍼와 관리자가 정의한 시그니처를 비교하여 해당 파일에 시그니처 유무를 확인한다.

3.3 시그니처 삽입모듈

삽입모듈 과정은 MS Office 파일 시그니처 삽입 과정과 일반파일 시그니처 삽입 과정으로 구성된다. MS Office 파일은 XML 형식의 압축파일로 구성되어있기 때문에 파일 필드에 시그니처를 삽입할 경우 해당 압축 파일을 풀 경우 오류가 발생하게 된다. 이에 따라 .Net Framework에서 제공하는 File 클래스 이용해 MS Office 파일은 포맷을 Zip 형식으로 변경한 다음 .Net Framework에서 제공하는 ZipFile 클래스를 이용하여 루트 경로에 시그니처 이름을 가진 XML 파일을 추가한다. 일반 파일의 경우 .Net Framework에서 제공하는 Filestream 클래스를 이용하여 파일 필드 가장 마지막에 시그니처를 헥사 코드로 변환한 뒤 Byte 단위로 삽입한다. 그림 1에서 음영 처리한 부분이 삽입한 시그니처를 나타낸다.

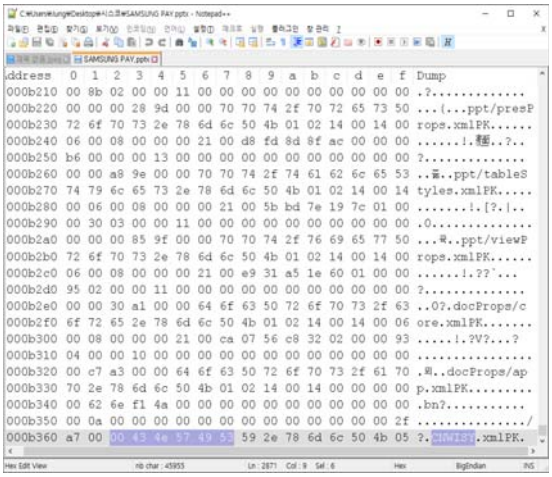

그림 1. 시그니처가 삽입된 파일

Ⅳ. 시스템 동작 및 실험

그림 2는 시그니처 탐지 및 삽입 과정을 나타낸 흐름도이다.

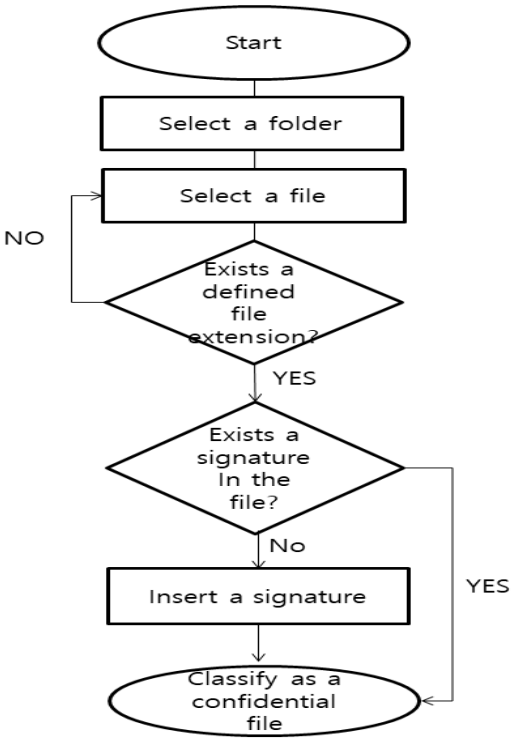

그림 2. 시그니처 탐지 및 삽입 과정

일반파일을 기밀파일로 정의하기 위해서는 시그니처 삽입을 필수로 하여야 한다. 시그니처가 이미 삽입되어 있는 파일도 있기 때문에 중복방지를 위해 사전에 먼저 시그니처를 탐지하여, 없을 경우에만 시그니처를 삽입한다. 먼저 특정 폴더나 새로운 폴더를 지정하여야 한다. 지정된 폴더는 자동으로 열리게 되며 관리자가 미리 지정한 파일확장자를 가진 파일이 해당 폴더에 이동

또는 복사를 시도할 경우, 자동으로 시그니처 탐지 및 삽입을 수행한다. 그림 3은 시그니처 탐지 및 삽입에 대한 메인화면이다.

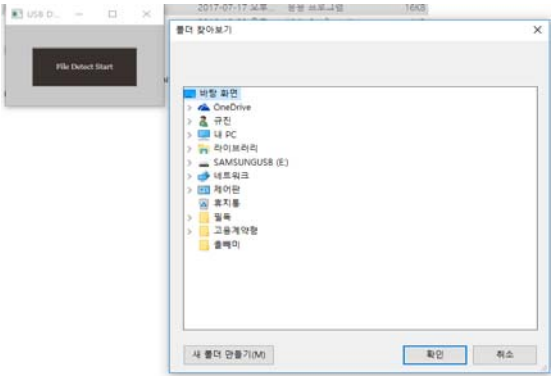

그림 3. 시그니처 관리자 실행 화면

Ⅴ. 결 론

USB 메모리를 이용한 기업 내부 기밀 파일 유출 건수가 나날이 증가하고 있다. 이에 본 논문에서는 기업 내부의 기밀 파일 유출을 방지하기 위해 필요한 기밀 파일에 시그니처를 삽입 기법을 제안하였다. 현재 기업 환경에서 널리 사용되고 있는 파일을 파일의 형태에 따라 MS Office 파일과 일반 파일로 나누어 시그니처를 삽입하는 기업을 제안하고 이를 구현하여 그 성능을 확인하였다. 본 연구 결과는 향후 기밀파일 유출 방지시스템 개발을 위한 기반 연구로 유용하게 활용될 수 있을 것으로 사료된다.

Acknowledgement

이 논문은 2015년 교육부와 한국연구재단의 지역혁신창의인력양성사업(NRF-2015H1C1A1035859) 및 과학기술정보통신부 및 정보통신기술진흥센터의 고용계약형 SW석사과정지원사업의 연구결과로 수행되었음(2015-9-00999).

참고문헌

[1] Jong-shik Lee and Kyeong-ho Lee, “A Study on Security Container to Prevent Data Leaks,” Journal of the Korea Institute of Information Security & Cryptology, vol.24, no.6, pp.1225-1241, 2014.

[2] Miboon Hyun and Sangjin Lee, “The Proactive Threat Protection Method from Predicting Resignation Throughout DRM Log Analysis and Monitor”, Journal of the Korea Institute of Information Security & Cryptology, vol.26, no.2, pp.369-375, 2016.

[3] Sun-Ho Lee and Im-Yeong Lee, “A Study on Security Solution for USB Flash Drive”,Journal of Korea Multimedia Society, vol.13, no.1, pp.93-101, 2010.

[4] Joo-ho Choi and Sung-yul Rhew, “Monitoring System of File Outflow through Storage Devices and Printers”, Journal of the Korea Institute of Information Security & Cryptology, vol.15, no.4, pp.51-60, 2005.