한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

패스워드 기반의 USB 파일 보호 프로그램

용승림*, 최영철*, 도상원O
O*인하공업전문대학 컴퓨터시스템과
e-mail: slyong@inhatc.ac.kr*, cyc31041@naver.com*, alona@alonalab.krO

Password Based USB File Encryption Program

SeungLim Yong*, Young-Chul Choi*, Sang-Won DoO
O*Dept. of Computer Systems and Engineering, Inha Technical College

● 요 약 ●

본 논문에서는 USB 파일을 보호하기 위한 USB 파일 보호 프로그램을 설계하고 구현한다. USB 파일 암호화 프로그램은 암복호화시 패스워드를 기반으로 하여 사용자 편의성을 고려하고, USB 저장장치의 파일 각각을 패스워드 가반으로 암호화함으로써 파일들의 외부유출을 방지하여 분실 시 보안에 취약했던 USB 저장장치의 안전성을 향상시킨다.

키워드: USB 저장장치,(USB Device), 암호화(encryption), C# WPF

I. Introduction

우리가 일반적으로 사용하고 있는 USB는 파일 보호 기능을 제공하지 않거나, 특정 USB 제조사에서만 자사 솔루션으로 제공하고 있다. 일반적으로 USB 사용자들은 편의를 위해 일반적인 파일부터 공인인증서, 프로젝트 내역 등 민감한 개인적인 정보까지 USB를 통해 보관하고 있어 분실이나 도난시 보안이 되지 않은 USB의 경우 개인정보 유출 등 치명적인 손실을 입을 수 있다.

본 논문에서는 이러한 문제점을 방지하기 위해 파일별로 서로 다른 패스워드를 기반으로 암호화가 가능한 패스워드 기반 USB 파일 보호 프로그램을 설계하고 구현한다.

II. Proposed Application

1. 기존 장치들

USB에 저장되어 있는 정보를 보호하는 방법은 다양하게 존재한다. USB 드라이브 자체를 보안영역으로 지정하는 방법, 드라이브 내의 파일만 암호화시키는 방법, Device 자체에 비밀번호를 걸어 접근제어를 하는 방법 등이 있다.

국내에서 개발되어 시판되고 있거나 무료로 배표되어 사용되는 USB 보안 프로그램들은 표 1과 같다.

Table1. Compare capabilities of domestic and foreign applications

프로그램명	회사명	파일 보호 방식
BitLocker	MicroSoft	드라이브 비트 암호화
TrueCrypt	TrueCrypt	암호화 파티션 생성
USBsafe	SafeHQ	패스워드 기반 보안영역 생성
VeraCrypt	IDRIX	암호화 파티션 생성

2. 소개

패스워드 기반의 USB 파일보호 프로그램(USB-Wizard)은 패스워드 기반 암호화를 통하여 USB에 저장되어 있는 파일 각각을 암호화하여 저장된 파일을 보호한다. 파일은 AES-256 암호화 알고리즘을 이용하여 보호하며 키는 사용자의 패스워드를 기반으로 생성한다. 사용자가 패스워드를 입력하면 SHA-256으로 변환하고, 키 길이를 맞추기 위하여 MD5로 변환한다. 파일의 내용은 암호화된 이후에는 파일의 확장자를 변경하여 사용자 스스로가 파일들을 관리할 수 있게 하고 암호화되기 이전의 파일은 제거되며, 암호화된 내용의 확장자가 변경된 형태로 파일이 생성된다. 사용자 편의를 위하여 간편한 UI를 제공하며 로그파일로 파일을 관리할 수 있는 기능을 제공한다. 암호화 알고리즘은 C#에서 제공하는 Security.Cryptography 라이브러리를 이용하여 구현하였고 C# WPF로 구현하였다.

전체적인 어플리케이션의 흐름도는 그림 1과 같다.

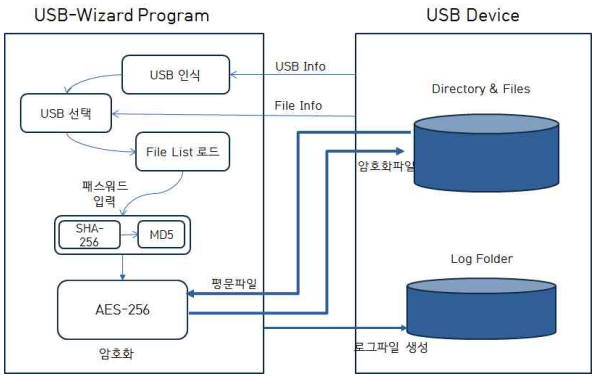

Fig1. System Architecture

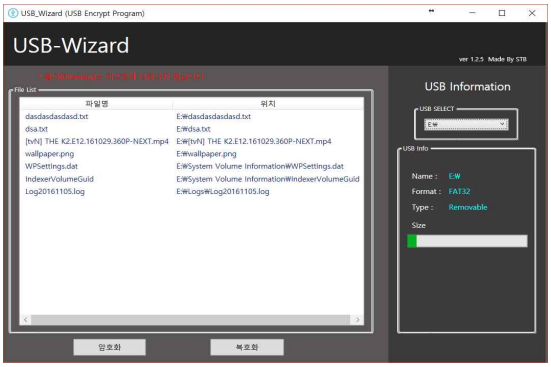

Fig. 2. Screen Shot

3. 기능구현

USB-Wizard의 세부 기능은 다음과 같다.

① 암호화 : 파일은 AES-256 알고리즘을 통하여 보호된다. 암호화 키는 패스워드를 기반으로 생성된다. 사용자가 패스워드를 입력하면 패스워드를 SHA-256으로 변환한 후 나온 해시값을 MD5 알고리즘을 통해 변환하여 파일을 암호화할 키를 생성한다. USB에 저장된 파일은 위에서 생성된 키를 입력으로 AES 알고리즘을 통해 암호화가 된다. 파일 암호화가 수행되면 암호화 이전 파일은 자동으로 제거되며 암호화된 파일만 USB에 확장자명이 변경되어 저장된다.

② 복호화 : 암호화된 파일을 리스트에서 선택하면 패스워드를 입력할 수 있는 창이 뜨고 패스워드를 입력하면 복호화키가 생성되어 파일을 복호화할 수 있다.

③ USB 선택 : USB의 인식을 수행하며 인식이 되었을 때 리스트에 USB의 이름을 출력한다.

④ USB 정보 : 인식된 USB를 선택하였을 때 해당 USB의 정보를 불러와 드라이브의 여분 공간, 이름, 경로 등을 표시하게 된다.

⑤ 로그 저장 : 암호화 및 복호화를 수행할 때 해당 기능을 수행한 시간, 수행한 파일명, 수행 여부를 텍스트 파일로 생성하여 Log 디렉터리를 생성하여 해당 날짜를 파일명으로 하여 저장하게 된다.

구현된 패스워드 기반 USB 파일보호 프로그램은 그림 2와 같다.

III. Conclusions

본 논문에서는 패스워드를 기반으로 한 USB 파일 보호 프로그램을 개발하였다. USB를 삽입하여 파일 리스트에서 파일을 선택하고 암호화 및 복호화를 수행한다. 패스워드를 입력받아 SHA-256과 MD5 알고리즘에 의해 AES-256의 키값을 생성한다. 모든 파일은 AES-256 암호화 알고리즘에 의해 암호화 된다. 암호화와 복호화를 수행할 때 로그 파일에 로그기록을 남기게 된다. 또한 암호화를 해놓았을 때 분실이나 도난 시 패스워드와 해당 프로그램 없이는 복호화를 할 수 없으며 패스워드 사용으로 인해 편의성이 제공된다. 파일 각각을 다른 패스워드로 암호화 할 수 있고 이를 통해서 개인의 소중한 정보를 보호할 수 있다. 로그를 생성하여 파일을 관리할 수 있어 신뢰성이 보장된다.

IV. References

[1] http://www.portablemarket.co.kr/inc/usbsafe.asp
[2] http://blog.naver.com/wondy7/220228479575
[3] http://loowi.blog.me/220873485075
[4] http://roll431.blog.me/50115911350