# 윈도우 운영체제의 파일 보안 모듈 개발

이성헌* · 장승주*

*동의대학교

# Implementation of a File Security Module in the Windows Operating System

Seong-Heon Lee* · Seung-Ju Jang**

*Dong-Eui University

E-mail : kkulee@deu.ac.kr, sjjang@deu.ac.kr

## 요 약

본 논문에서 제안하는 파일 보안 기능은 암호 알고리즘을 이용하여 파일을 저장함으로써 허락되지 않은 사용자의 접근을 제한하도록 한다. 암호화하여 저장된 파일은 복호화 알고리즘으로 복호화해서 파일 데이터를 읽게 된다. 이러한 기능은 사용자들이 편리하게 사용할 수 있도록 사용자 인터페이스를 설계하여 프로그램으로 구현한다. 보안 기능으로 구현된 파일 암호화 및 복호화 프로그램을 구동시키고 정상적으로 동작하는지의 여부를 실험하게 된다. 또한 복호화 시 암호화 할 때의 설정과 설정이 틀릴 경우 복호화가 되는지의 여부도 실험한다. 이 프로그램의 개발을 통해서 윈도우 서버 및 개인용 컴퓨터 내의 중요한 파일에 대한 보안을 강화시킬 수 있다.

## ABSTRACT

The file security function, which this paper suggests, restricts the access of an unauthorized users by using password algorithm and saving file. Saved files that are encrypted are read by decrypting them with decryption algorithm. These features are user interface to design the program for user friendly. The security function implements both file encryption and decryption programs and tests whether the experiment works or not. In addition, when a decryption is progressed and the settings of between decryption and encryption are different each other, the security function also checks the possibility of decryption. We can enhance the security on important files stored in Windows servers or personal computers by developing this program.

## 키워드

file security, module, password algorithm

## Ⅰ. 서 론

컴퓨터 시스템을 구동하기 위한 운영체제를 이용한 데이터 파일의 생성은 급증하고 있는 추세이다. 그러나 운영체제 내의 데이터 파일을 안전하게 관리하는 것은 중요한 문제가 되었다. 따라서 본 논문에서는 이러한 컴퓨터 시스템 내의 파일에 대한 보안 기능을 제공하여 파일을 안전하게 관리할 수 있도록 한다. 이러한 개발을 통해서 보다 안정된 운영체제 파일 보안 기능의 제공으로 안전한 시스템을 개발하고자 한다.

윈도우 운영체제 내에서 파일 보안과 관련한 기술을 PDA등 임베디드 시스템 환경에 접목할 경우 중요한 데이터에 안전한 관리를 보장할 수 있다. 윈도우 운영체제 파일 보안 기술은 차세대 컴퓨터 시스템 관련 핵심 기술로써 중요한 의미를 가진다.[1]

컴퓨터 시스템 보안은 정보화 사회가 되면서 중요한 이슈가 되고 있다. 최근에는 보안 운영체제에 대한 연구가 활발히 진행되고 있다. 보안 운영체제는 기존의 커널에 보안 기능을 통합시킨 보안 커널이 추가로 이식된 운영체제이다. 보안 운영체제의 기능은 사용자에 대한 식별 및 인증, 강제적인 접근 통제, 임의적인 접근 통제, 감사

및 감사 기록, 침입 탐지 등의 기능을 가지고 있다. 이러한 보안 운영체제에서 파일의 보안은 더욱 중요하다. 파일을 보호하는 기존의 연구 내용으로는 파일의 접근 권한에 대한 엑세스 정보를 관리하여 이루어지는 경우가 있다. 또한, USB 장치와 같은 특수 장치 내에 저장된 파일에 대한 보안을 위한 연구가 진행되고 있다. USB와 같은 특수 장치내의 파일에 대한 보호는 접근 제어 기법 등을 이용한다.[2][3]

## II. 파일의 보안 기술 개발

본 논문은 윈도우 운영체제의 중요한 파일에 대한 보안 모듈 개발을 목표로 한다. 기존 윈도우 운영체제 내의 파일을 보호하고자 한다. 기존의 윈도우 운영체제는 중요한 데이터 파일에 대한 보호 기능이 없다. 본 논문은 이러한 중요한 파일에 대해서 사용자가 지정을 하면 암호화 등을 통해서 보호를 할 수 있도록 한다. 사용자가 필요할 경우 이 기능을 하는 모듈을 이용하여 사용할 수 있도록 개발한다. 또한 사용자의 편리성을 위해서 쉽게 사용이 가능하도록 한다.[5]

윈도우 운영체제 내에서 중요한 데이터를 보관하는 파일에 대한 보안을 하는 것은 아주 중요한 일이다. 본 논문은 윈도우 운영체제에서 중요한 파일에 대한 보안 기술을 개발한다. 개발되는 기술은 다음과 같이 동작된다.

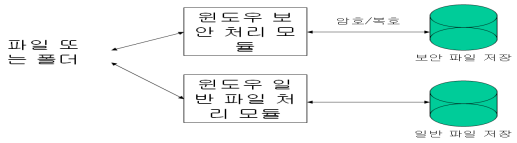



그림 1. 특정 파일에 대한 보안 수행 과정

그림1은 윈도우 운영체제에서 특정한 파일에 대한 보안을 수행하는 과정을 보여준다. 일반 파일을 지정하여 보안 파일로 변환하는 과정이다. 사용자가 보호하고자하는 파일을 지정하면 보안 프로그램이 동작되어서 해당 파일을 암호화 등을 수행하여 보호하게 된다.

## III. 파일 보안 프로그램 설계

본 논문에서 파일 보안을 위한 기능 설계 내용은 다음과 같다.

- 사용자가 편리하게 사용할 수 있도록 하는 인터페이스 설계
- 사용자가 지정한 파일에 대한 암호화 기능 설계
- 사용자가 지정한 파일에 대한 데이터를 버퍼로 읽기 기능 설계
- 버퍼로 읽어들인 데이터를 암호 알고리즘을 사용하여 암호화 하는 기능 설계
- 암호화된 버퍼 데이터를 새로운 파일로 저장하는 기능 설계
- 사용자가 지정한 암호화된 파일에 대한 복호하 기능 설계
- 복호화를 하기 위하여 암호화된 파일로부터 버퍼로 데이터를 읽어들이는 기능 설계
- 버퍼로 읽어들인 암호화 데이터를 복호 알고리즘을 사용하여 복호하 하는 기능 설계
- 버퍼 내의 복호화된 데이터를 파일에 저장하는 기능 설계

### 3.1 사용자가 지정한 파일에 대한 데이터를 버퍼로 읽기 기능 설계

본 논문에서 설계한 윈도우 운영체제에서 파일 보안 기능을 사용자가 편리하게 사용할 수 있도록 사용자 인터페이스를 설계한다. 사용자가 편리하게 사용할 수 있도록 설계된 화면은 다음과 같다. 본 프로그램을 실행 하고자 할 경우에 아래의 모양과 같은 아이콘을 두 번 누리게 되면 실행이 되게 된다. 파일 보안 프로그램을 실행하게 되면 다음과 같은 화면이 동작하게 된다.

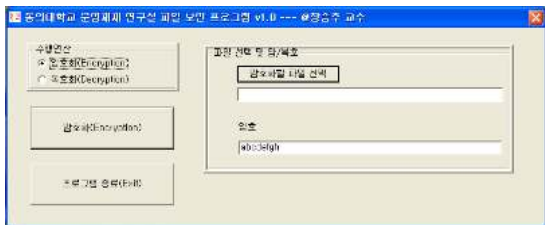



그림 2. 보안 프로그램 실행 화면

파일 보안 프로그램 동작 화면에서 수행 연산 부분은 파일에 대한 암호, 복호화 여부를 결정하는 기능이다. 먼저 사용자가 원하는 연산이 암호화일 경우는 암호화 버튼을 누른다. 그리고, 파일 선택 및 암/복호에서 암호화할 파일 선택 부분에서 암호화하고자 하는 파일을 선택한다. 복호화 기능은 암호화된 파일을 정상적으로 되돌려놓고자 할 경우에 사용하는 기능이다. 세부적인 기능은 아래에 자세히 설명한다.

### 3.2 사용자가 지정한 파일에 대한 암호화 기능 설계

사용자가 지정한 파일에 대한 암호화 기능은 수행연산에서 암호화 버튼을 누르고 파일 선택 및 암/복호에서 암호화할 파일을 선택하게 된다. 그러면 아래와 같이 파일 선택을 할 수 있는 창이 뜨게 된다. 그러면 자신이 암호화하고자 하는 파일을 선택하면 된다. 아래 화면은 RCI.hwp 파

일을 선택하는 화면이다.

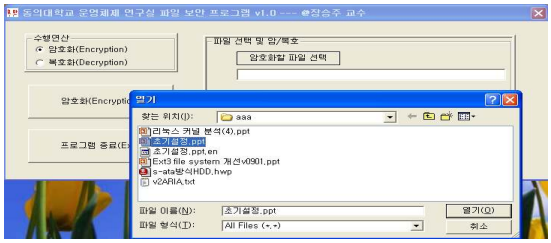


그림 3. 암호화할 파일 선택 화면

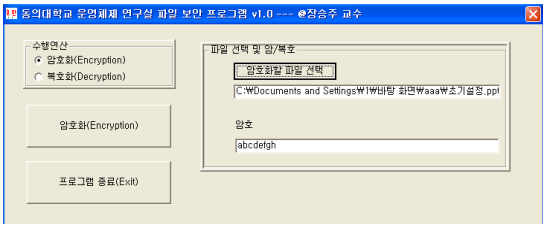
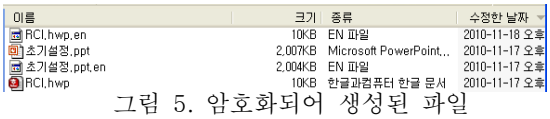


그림 4. 암호화할 파일 경로 설정

그림 4와 같이 설정이 끝나면 좌측 중간에 있는 암호화(Encryption) 버튼을 누르게 되면 해당 파일이 암호화 되게 된다. 지정된 파일이 암호화 되게 되면 지정된 폴더 내에 그림 5와 같이 새롭게 암호화되어 생성된 파일이 만들어지게 된다.



| 이름 | 크기 | 종류 | 수정한 날짜 |
|---|---|---|---|
| RCI.hwp.en | 10KB | EN 파일 | 2010-11-18 오후 |
| 초기설정.ppt | 2,007KB | Microsoft PowerPoint... | 2010-11-17 오후 |
| 초기설정.ppt.en | 2,004KB | EN 파일 | 2010-11-17 오후 |
| RCI.hwp | 10KB | 한글과컴퓨터 한글 문서 | 2010-11-17 오후 |

그림 5. 암호화되어 생성된 파일

새롭게 암호화되어 생성된 파일은 확장자가 “en"이 추가되게 된다. 일반 사용자 파일을 암호화 및 복호화할 경우에 사용하는 암호 알고리즘은 triple-DES 를 사용한다.

3.3 사용자가 지정한 파일에 대한 복호화 기능 설계

사용자가 암호화한 파일에 대해서 정상적으로 파일 열기를 할 경우에 먼저 암호화된 파일을 복호화해야 한다. 복호화를 하기 위해서는 수행연산에서 복호화 버튼을 선택한다. 그러면 그림 6와 같은 사용자 화면이 나타난다.

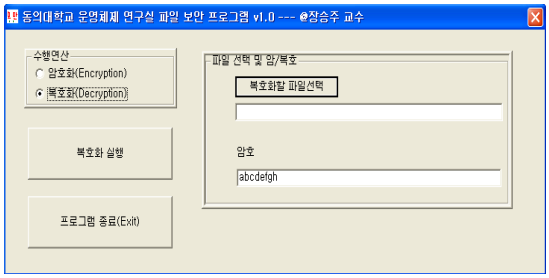


그림 6. 암호화된 파일을 복호화된 화면

복호화할 파일을 선택하게 되면 복호화할 파일 선택 아래에 그림 7과 같이 경로가 나타난다.

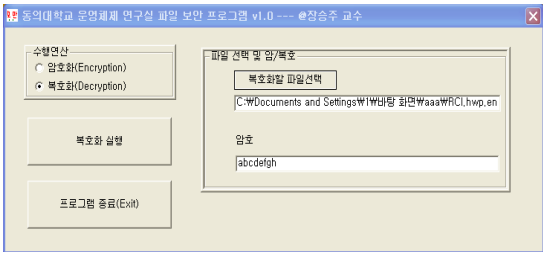


그림 7. 복호화할 파일 선택후 경로 설정 화면

그림 7과 같이 복호화할 파일이 지정되고 나면 왼쪽 중간의 복호화 실행 버튼을 누르면 암호화된 파일이 복호화되게 된다. 암호화된 파일을 복호화 한후에 해당 파일 열기를 통해서 정상적으로 파일이 복호화 되었는지를 확인하게 된다. 아래 그림 8은 정상적으로 파일이 열린 화면을 보여준다.[6][7]

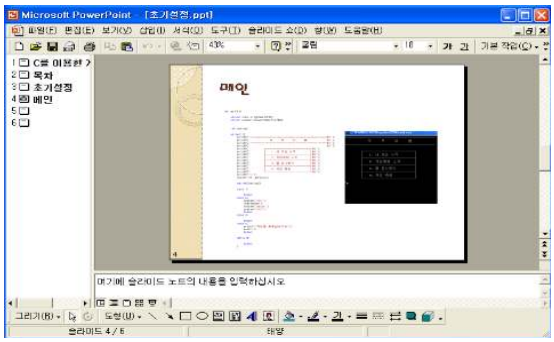


그림 8. 복호화한 후 파일 열기 화면

## Ⅳ. 실험

본 논문의 설계 결과를 실제 시스템에 구현하여 실험을 하였다. 실험을 위해서 사용된 시스템 환경은 다음과 같다.

- O 인텔 팬티엄4 CPU 3.00 HZ
- O 1.37GB 메인 메모리
- O Microsoft Windows XP 운영체제
- O Visual Studio 6.0 compiler 환경

본 논문에서 구현한 윈도우 운영체제에서 보안 프로그램의 기능은 크게 두가지 이다. 하나는 일반 파일을 허가되지 않은 사용자가 접근하지 못하도록 차단하는 암호화 기능이다. 다른 하나는 허가된 사용자가 암호화된 파일을 복호화하여 정상적인 파일로 볼 수 있도록 해 주는 기능이다.

먼저 일반 파일을 허가된 사용자만 볼 수 있도록 암호화하는 기능의 실험 결과를 보인다. 정상적인 파일을 열었을 때의 화면은 아래와 같다.

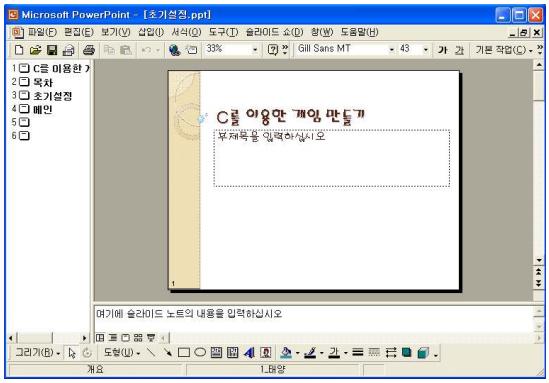



그림 9. 일반적으로 사용하는 ppt 파일을 열기로 파일 읽기 화면

그림 9은 일반적으로 많이 사용하는 ppt 파일을 열기하여 읽은 화면을 보여준다. 일반 파일에 대해서 사용자가 암호화한 후 암호화된 파일을 열었을 경우에 화면은 다음과 같다.

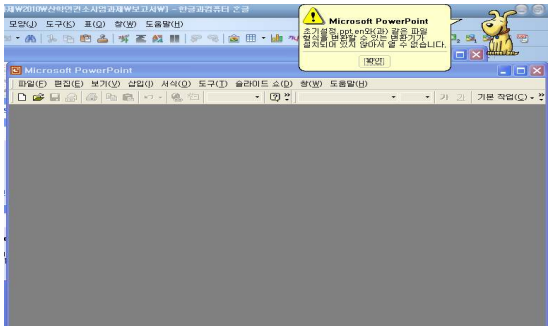



그림 10. 암호화된 ppt 파일을 열고자할 경우 오류 메시지가 발생되는 화면

그림 10는 암호화된 ppt 파일을 열고자할 경우 오류 메시지가 발생되는 화면이다. ppt 파일을 암호화하게 되면 보안 프로그램에서 파일의 확장자로 ".en"을 붙이게 된다. 파워포인터 읽기 프로그램은 확장자가 ppt인 파일에 대해서 열기가 가능하기 때문에 위와 같은 오류 메시지가 출력된다.

암호화된 파일에 대해서 사용자가 해당 파일을 복호화 한 후, 해당 파일을 열어서 수행한 화면은 위에서 보는 것과 같이 수행된다. 이와 같이 일반 파일을 본 논문에서 개발한 암호화 기능을 이용하여 암호화하게 되면 허가된 사용자 외에는 파일을 정상적으로 읽을 수 없음을 확인할 수 있다.

위 실험 결과에서 보듯이 윈도우 운영체제에서 일반 파일을 읽기를 하면 모든 사용자들이 볼 수 있다. 본 논문에서 설계 및 개발한 윈도우 운영체제에서 파일 보안 프로그램을 이용하여 보안을 수행한 후 허가된 사용자 외에는 접근은 가능하지만 파일 데이터를 읽기가 불가능함을 알 수 있다. 허가된 사용자의 경우는 암호화된 파일을 본 논문에서 개발한 프로그램을 이용하여 복호화함으로써 정상적으로 읽기가 가능함을 알 수 있다.

## V. 결 론

본 논문에서는 윈도우 운영체제에서 구동되는 파일 보안 기능을 설계 및 개발하였다. 개발된 기능은 사용자가 윈도우 운영체제 내의 파일에 대해서 보안을 하고자 할 경우에 사용이 가능하다. 본 논문에서 개발한 기능의 상세 내용은 윈도우 운영체제 내의 파일에 대한 보안 모듈 설계, 윈도우 운영체제 내의 파일에 대한 보안 모듈 개발, 기존 윈도우 운영체제 내의 파일과의 연동 모듈 시험, 개발 모듈 통합 및 통합 시험 등을 수행하였다.

본 논문의 구현 결과를 실제 실험을 수행하였다. 실험은 실제 윈도우 운영체제가 탑재된 시스템 환경에서 이루어졌다. 본 논문에서 구현한 윈도우 운영체제에서 보안 프로그램의 기능은 크게 두 가지 이다. 하나는 일반 파일을 허가되지 않은 사용자가 접근하지 못하도록 차단하는 암호화 기능이다. 다른 하나는 허가된 사용자가 암호화된 파일을 복호화 하여 정상적인 파일로 볼 수 있도록 해 주는 기능이다. 실험 결과 본 논문에서 구현한 파일 보안 기능이 정상적으로 동작함을 확인할 수 있었다.

## 참고문헌

[1] 국가정보원, 2009 국가정보보호백서, 제2편 제6장 개인정보보호 활동, 2009년 4월
[2] 한국정보보호진흥원, 중소기업 정보보호 예상 피해유형과 대응사례, 2006.11
[3] 한국정보보호진흥원, 2008 정보시스템 해킹·바이러스 현황 및 대응, 2008.12
[4] SANS Institute, 20가지 가장 치명적인 보안 위협, 2007
[5] Apspect Security, Starting Out With Application Security, http://www.aspectsecurity.com/owasp.htm,2007
[6] Yinghua Wu, Jianping Wu, Ke Xu, Mingwei Xu, "The Design And Implementation of Router Security Subsystem Based on IPSec", IEEE Computer Society, Vol 1. pp.160-165, 8. 2002.
[7] Dieter Gollmann, Computer Security, WILEY, Vol, 2. pp.234-251, 2006.