Developing File Security for Windows Operation System

Seung-Ju Jang

Dept. of Computer Engineering, Dongeui Univ.

Abstract

This paper designs file security function on Windows O.S. Whenever you use Windows O.S, you need to protect some file data. This paper designs these security protection functions. This paper proposes two security functions on Windows O.S. One is file security. The other is directory access protection. To check the proposed functions well, I experiment the above functions on the Windows O.S. By this experiment, I confirmed that the proposed function worked well.

Keywords : Windows O.S, security, directory access control, file encryption, file decryption

I. Introduction

The Computer is inevitable thing in our life. The most important thing in computer system is file management. It is very important to keep file safe. Safe file management has become important technology as increasing use of computer system. This paper designs file and directory security in Windows O.S. Windows O.S is used in the world-wide computer system. The important files should be kept safe in Windows O.S. This paper designs file and directory protection function in Windows O.S. The function suggested in this paper is composed of the file security and the indicated directory protection.

The suggested file security function is storing encrypting file using encryption algorithm so that cannot access it by unpermitted people. The encrypted file is read by decrypting it. This is designed and implemented user friendly interface. This paper experiments encryption and decryption function of the proposed program normally. I experiment also decrypt or not in case of incorrect password. This paper has also directory protection function in Windows O.S. I design directory access control of Windows O.S.

The suggested directory access control function protects directory access from unpermitted people by directory access permission. I experiment also the suggested directory access. I confirmed the suggested directory access is working well. This paper is composed of chapter 5. Chapter 2 is related research, Chapter 3 is designed Windows O.S security function. Chapter 4 is experiment and evaluation. Chapter 5 is conclusion.

Manuscript received May 5, 2010
Manuscript revised May 20, 2010

II. Related Research

A computer system's security is becoming the important issue until information society. Recently the research about a security operating system has been processed actively. A security Operating System is a consolidated system added with security kernel. The facility of a security operating system has the identification and certification about the user. It has the facility of compulsive access control, random access control, audit, audit log and intrusion detection [1-3]. File security is very important in security O.S. The previous research topic is protected file in file access information. Namely, access token is available to access control for a file [4-7]. A research is also doing for the file security saved in the special device such as a USB. The protection about the file of a special device such as a USB uses an approach of access control. To protect the file of such device, there is a case to implement within inside a kernel's device driver [8-12].

III. Design of Windows Operating System Security Function

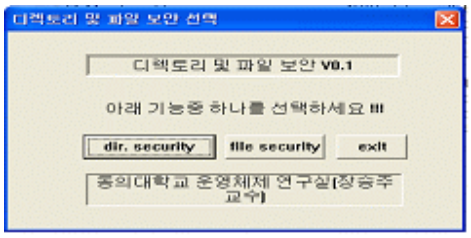
This section explains about inside a windows operating system's a file security facility. I explain also about a directory approach control facility. I use a windows XP operating system to design the facility to propose in this paper. A program language to be used uses also the windows VC++ at the development. Among the design of the file security in Windows O.S, there's a function of design form which is to necessary buttons.

Basically, the program execution is composed of the login form, a member subscription form, a directory approach control form, and file security form. The screen design of member subscription, login, connection exit, or ID registration for a file security is as follows.

[Fig. 1] Login Display using Security Program

After inputting ‘ID’ and ‘Passwd’ in [Fig. 1], you click ‘login’ button, you are linking with a security execution system program which is designed in this paper. To access to the program of this paper, you need user registration for program utility permission. The CMember class code is used for member registration to use file security features. m_pSet.Open() function will open the design form features. m_pSet.AddNew() function allows you to use the Edit box and input personal information for membership. And, it uses data structures for storing personal information that a user inputs. m_pSet.m_id variable gets ID character. The user's password is stored at m_pSet.m_pw variables. The user’s name will be saved in m_pSet.m_name variable. the user's phone number is stored in m_pSet.m_phone variables. the user’s E-mail is stored in m_pSet.m_email variables.

After completing this user information registration, the user can use security feature of file system that is designed in this paper. Users have to login to the system with this level of registration is shown below, controls access to directories and files by using the security features allow you to select the operating system was designed. This system is designed for a user to select what he wants using directory access control function and file security function, when a user logins after system registration.

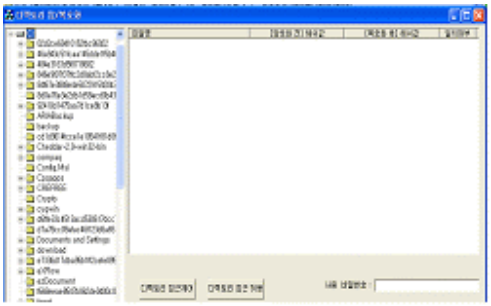


[Fig. 2] File Security or Directory Access Control Selection Menu

[Figure 2] is the selection menu page for directory and file security features. “Dir. security " button can be used for directory access control feature. "file security" button can be used for file security. For the user’s facility, we simplified the screen page.

3.1 Design of Directory Access Control Function

This paper offers a directory access control feature in the directory (or folder) to set a password to control access based on the directory. During the working of directory access control function, you select the 'dir. security 'button on the above [Fig. 2] screen to use the feature. Using 'dir. security' buttons and directory access control function, the following window will appear.



[Fig. 3] Directory Access Control Display Screen in Windows O.S

[Fig. 3] is display screen of directory access control feature in the Windows operating system in this paper. You specify the directory on the left screen, you can set directory access control feature. In other words, by selecting a specific directory, you can set access control capabilities. On this screen, the password needed to access the directory can be set in the “use Password 'field”. After entering your password, you press “control access to directory” button and the access control functions for the specified directory. An Authorized user can only use the setting directory. If you want to access the directory, you use the password which is set in directory access function of proposed program and press the button “allow access to directory”. If the password matches you will be allowed to access to the directory. Thus, a specific directory containing important information will be able to control access.

3.2 File Encryption/Decryption Function Design

In this paper, I design a file encryption / decryption function, we select the menu 'file security' button on the above menu selection screen of [Fig. 2]. On this screen, when you execute the 'file security', the following setup screen [Fig. 4] will appear. [Fig. 4] is file Encryption/Decryption security display screen. [Fig. 4] is program option setting and executing screen for the file encryption/decryption in Windows operating system proposed in this paper. In "Action" menu, there are "ENC" and “DEC” check button to select encryption/decryption. This can be used to select one. You can choose "ECB" or "CBC" in 'operation mode'. In "Algorithm Selection", "3DES" or "SEED" algorithm can be chosen. In "File Selection", You can specify the protection (encryption) file. In "Key value", you can set the value of the secret key. So you can choose the optional features that you want.

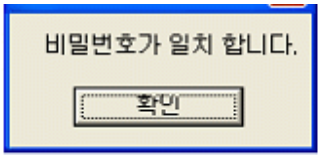
[Fig. 4] File Encryption/Decryption Screen

IV. Experiments and Evaluation

I perform tests and evaluations on the proposed security function for files and directories. The computer system environment for experiments is the Pentium CPU with Windows XP. In addition, the Microsoft .NET compiler (VC + +) was used. I experimented the directory access control and file security to check whether the behavior was normal. When access to the directory using directory access control, it shows the message to enter the secret key. At this point you put a password you set, directory access control feature is turned off. Below is a screen illustration of these features experimentation. [Fig. 5] is screen shot of directory access control function in the experiment.

[Fig. 5] Display Screen for Directory Access Control

When you want to call off the directory access control, select the appropriate directory and enter the password you set for the first time. Under normal circumstances, the directory access control will be lifted if the password is correct. In this case, the following message window will be opened. This window indicates that the directory access control is released.

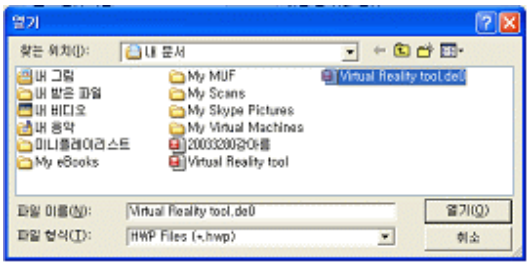


[Fig. 6] Display Screen for Directory Access

In addition, I experiment on a file encryption / decryption capability to design in this paper. File encryption and decryption of files in the Windows operating system to load and perform the encryption and decryption of the encrypted file is being properly experiments. First, create a simple text file. This is a "Hangul" file. This file is generated using a file encryption / decryption experiments. When you run the program that encrypts the general ASCII file using the presented program, it shows the below screen [Fig. 7].

[Fig. 7] Display Screen for Encryption of Windows Files

[Fig. 7] shows the window screen when the proposed file encryption/decryption is running. In this window, it reads the file written in "Hangul". To encrypt a given select ‘encrypt’ in the [Fig. 4]. Select 'ECB' as operation and '3 DES' as the algorithm. The encrypted file is created when you push 'Encryption Run' button. You also need to decrypt the encrypted file. After the encryption process, when you want to decrypt an encrypted file, the following figure is executed the screen.



[Fig. 8] Display Screen for Decryption of Windows Files

In order to perform the decryption process, select 'decoding' on the above [Fig. 8]. The same operation mode and encryption algorithm as are used encryption. To decrypt an encrypted file, I use the same options as encrypting files.

[Fig. 8] is the screen in order to decrypt an encrypted file, It is the file selection screen. The program perform decoding for the selected file, the file contents is shown in [Fig. 9].

[Fig. 9] File Read Screen for Decryption File

As shown above, I have found that the normal file can be read through the decryption process of the encrypted files. The results of these experiments in this paper show of encryption and decryption the general file is normally performed. In addition, the experiment for a directory access control feature is normally performed, too.

V. Conclusion

This paper designed the access control, directory and file security features in the Windows operating system. In the middle of using the Windows operating system, you need to protect important files and directories. This paper designed these capabilities. The features offered in this paper are to set the security function on a particular file in the Windows Operating System and to control the access to a specific directory. The experiment was performed to check a normal operation of access control and security function. I was able to identify the normal operation of access control function and file security function through experiment. The function designed in this paper can block someone's access to a specific directory in the Windows O.S. Blocking access to the directory, you can protect your data safely. In addition, the security of certain files in Windows O.S can be done. By doing so, only the people with specific permissions on files can read the file and we can protect the contents of files. The ability offered in this paper can be applied to a wide range of utilization like a USB device.

Acknowledgment

This work was supported by Dong-eui University Grant.(**2009AA175**)

References

[1] Shin, Dong-Woo, Virtual Device Driver Level Seed Encryprion/Decryption Security File System in Windows System, Gun Koog Univ. M.S Thesis, 2009.

[2] Park, Seung-Gi, A Study of WINDOWS 2000 Server Security, Dongkug Univ. M.S Thesis, 2002.

[3] Han, Suk-Jae, Kim, Wan-Kyung, So, Wo-Young, "Design and Implementation for File Access Control Module for Windows Security O.S.", Korea Cyber Terror Information Society, 2009. 6.

[4] Sung Kyung, Yoon, Ho-Gun, "Design and Implementation of File Security Module for Windows O.S.", Journal of Korea Computer Information Society, 2005.

[5] Shin, Young-Sun, Park, Jin-Seop, Lee, Ji-Young, "Design and Implementation of File Audit System in Windows O.S", Journal of Korea Multimedia Society, 2003.11.

[6] Jang, Seung-Ju, Lee, Jeong-Bae, Design of the Security Cryptography File System Based on the Dynamic Linking Module on the Linux O.S, The KIPS transactions, 2003

[7] Jang, Seung-Ju, "Design of the Encryption Module for File System in the Solaris Kernel", The KIPS transactions, 2003

[8] Choi, Young-Han, Kim, Hyoung-Chun, Hong, Soon-Jwa, "Software Security Testing using Block-based File Fault Injection", Journal of the Korean Institute of Information Security and Cryptology, 2007

[9] Jeong, Han-Jae, Choi, Youn-Sung, Jeon, Woong-Ryul, "Analysis on Vulnerability of Secure USB Flash Drive and Development Protection Profile based on Common Criteria Version 3.1", Journal of the Korean Institute of Information Security and Cryptology, 2007

[10] Lee, Dong-Chun, Kim, Jeom-Goo, Kim, Kui-Nam, "A Study on Specification Scheme of Protection Profile Security Environment for Government's VPN", The Journal of the information assurance, 2003

[11] Kim, Hee-Jeong, Lee, Ju-Young, Cho, Yeong-Yeol, "File Security System for Personal Digital Assistants", Journal of Korea Multimedia Society, 2003, Proceedings of the Korea Multimedia Society Conference, 2003

[12] Kwak, Jin, Hong, Soon-Won, Yi, Wan-Suck, "Vulnerability and Security Requirement Analysis on Security Token and Protection Profile Development based on Common Criteria Version 3.1", Journal of the Korean Institute of Information Security and Cryptology, 2008

Seung-Ju, Jang received a B.Sc. degree in Computer Science and Statistics, and M.Sc. degree, and his Ph.D. in Computer Engineering, all from Busan National University, in 1985, 1991, and 1996, respectively. He is a member of IEEE and ACM. He has been an associate Professor in the Department of Computer Engineering at Dongeui University since 1996. He was a member of ETRI(Electronic and Telecommunication Research Institute) in Daejon, Korea, from 1987 to 1996, and developed the National Administration Multiprocessor Minicomputer during those years. His current research interests include fault-tolerant computing systems, distributed systems in the UNIX Operating Systems, multimedia operating systems, security system, and parallel algorithms.