International Journal of Smart Home
Vol.7, No.6 (2013), pp.227-236
http://dx.doi.org/10.14257/ijsh.2013.7.6.22

Security Measures of Personal Information of Smart Home PC

Mi-Sook Seo[1] and Dea-Woo Park[2]
[1, 2]*Department of Integrative Engineering, Hoseo Graduate School of Venture, 9, Banpo-daero, Seocho-gu, Seoul, Republic of Korea*
msseo@smsinfo.co.kr, prof_pdw@naver.com

Abstract

DB servers for managing personal information have security systems for enhancing security, but security systems do not fully operate in user's smart home PC, and it is thus necessary to analyze vulnerabilities for protecting personal information, and to study self-diagnosis of security. This study aims to search and encrypt information related to protecting personal information in a smart home PC to enhance security and to delete files so that they cannot be recovered. The analysis of vulnerabilities detected in a smart home PC aims to check user account, shared folders, service firewall, screen savers, and automatic patch updates. A quantitative analysis and expression about vulnerabilities after checking them is carried out to make and show a check list for enhancing security. Smart home PC security management is then managed and operated by a server semi-automatically. It is expected that this study will contribute to reducing financial damages and people's distress by further protecting personal information in a smart home PC, and enhancing national cyber security.

Keywords: *smart home PC, vulnerability, personal information security, privacy*

1. Introduction

Smart home PCs are connected to the internet as a typical means for information exchange and work. Therefore, users take various protection measures for protecting their smart home PC [1] from hacking and personal information theft associated with their smart home PC. In particular, smart home PC security (prevention of internal information from being stolen) is an internal user's access point connected to a DB server.

Hackers attack smart home PCs in addition to the DB servers of which security is enhanced to collect important information. Internal users of the smart home PC steal, modify or counterfeit data. The aforementioned hacking has sharply been increasing as shown in Figure 1.

However, there is an issue that smart home PC users do not fully understand the necessity of security to be set for smart home PC security. The terms of security are not easy for ordinary users to understand, and the process of setting security is not easy for ordinary users to use.

In general, while personal computer users who use the Windows OS for smart home PCs are vulnerable to hacking, hacking patterns against terminals and users are diversified [2]. Including personal information are not looked after because smart home PC users do not remember in which folder they saved them, they are automatically saved or users can't check or remember the location for backup [3].

[2] Corresponding Author

ISSN: 1975-4094 IJSH

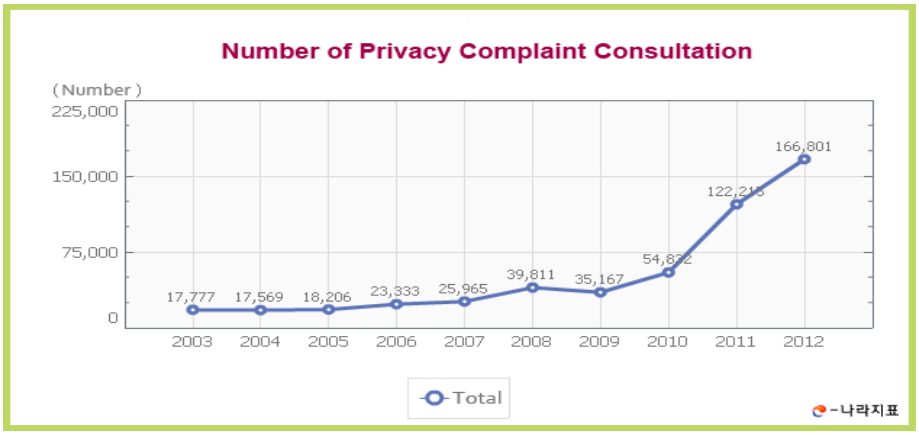

Figure 1. Number of Reported Hackings about Personal Information

Personal information files accessed through websites including data sharing systems are saved in user's hard disk as temporary files in the personal computer and also thus not looked after.

Therefore, it is necessary to study a method of: strengthening security by analyzing vulnerabilities for protecting personal information in a smart home PC; smart home PC users carrying out quantified security diagnosis [4] and taking measures against violation of The Information Privacy Act currently enforced [5].

This study aims to check all sorts of vulnerabilities of the windows system in a smart home PC, for example, checking user account, network and shared folders, services and firewall, screen savers and automatic update, to search files with personal information to encrypt and completely delete in addition to taking semi-automatic measures.

For quantified security diagnosis, this study aims for technology and security methods for statistics on a team and institution basis by giving scores to the checked data for complement and management and transmitting the security diagnosis data for protecting personal information to manager's server.

2. Related Study

2.1. Enactment and Enforcement of Information Privacy Act

The Information Privacy Act is being implemented in many countries of the world (United States, United Kingdom, *etc*.,) [6]. The Information Privacy Act was enacted on March 29, 2011 and has been enforced since March 30, 2012 in South Korea. This act aims to protect personal secrete from maliciously collecting, stealing, misusing and abusing personal information to promote people's right and profit, and to specify matters associated with processing personal information in order to implement people's dignity and values.

The Information Privacy Act specifies that people who process personal information should fully take technical, physical protective measures for safely managing the personal information. The Information Privacy Act also specifies to take necessary measures required for ensuring safety, for example, encryption, according to the method specified in the presidential decree in order to avoid unique identification information to be lost, stolen, modified or corrupted where a person who processes personal information processes the unique identification information. The person who processes personal information should

apply the method specified below to destroy the personal information according to the provision of Article 21 of the act.

1) Electronic file: permanently delete it so that it can never be recovered

2) Records other than those not specified above, prints, letters and other recorded media: crush them into pieces or burn up

2.2. Technical and Managerial Protective Measures for Personal Information

Apply the provision of article 30 about the measures for safety of unique identification information according to the provisions of article 21 (measures for ensuring safety of unique identification information) and article 24-3 of the act. In this case, “Article 29 of the Act” is regarded as “Article 24-3 of the Act”, and “personal information” as "unique identification information".

Article 30 (Measures for ensuring safety of personal information)

① A person who processes personal information should take measures for safety specified in the following provisions according to the provision of Article 29 of the Act.

1) Establish and enforce internal management plans for safely handling personal information.

2) Apply limited access and access right to personal information.

3) Apply encryption technology or take equivalent measures for safely saving and transmitting personal information.

4) Take measures for preventing storing, counterfeiting and modifying access records to tackle personal information hackings.

5) Install and update security programs for personal information.

6) Provide storages or take physical measures, for example, locking devices, for safe storage of personal information.

② The minister of the Ministry of Public Administration and Security (MPAS) can provide necessary support, for example, building a system so that the person who handles personal information can take measures for ensuring safety according to the provision of ①.

③ The detailed criteria of measures for ensuring safety according to ① should be specified and announced by the minister of MPAS [7].

2.3. Analysis of Smart home PC Vulnerability and Security

Smart home PC vulnerabilities are analyzed for 5 types of checking user account, checking network and shared folders, checking services and firewall, checking screen savers and automatic update [8].

Smart home PC security refers to comprehensive security technology for protecting computer terminals (server) or basic resources (operating system) therein owned by a company or a person. The scope of smart home PC security application covers both hardware security and software security for computer terminals [9].

3. Searching, Encrypting and Deleting Personal Information in Smart Home PC

3.1. Searching Personal Information in Smart Home PC

Searching should be done in a manner including important information, for example, resident registration number, foreigner registration number, driver's license number, phone number, passport number, business registration number, bank account number, e-mail, credit card number, address and new address, without opening files with personal information in a smart home PC. Searching should be enabled for various types of electronic documents, for example, TXT, PDF, TIF, RTF, PST, EML, MS Office documents, hangul documents, and outlook documents.

Searching should be supported for compressed files (zip, gzip, alzip, bzip, 7Z, BZ2, rar, tar), multi-step compressed files, personal information included in OLE objects in files, counterfeited and modified extensions and hidden files/folders.

3.2. Encrypting Personal Information saved in Smart Home PC

Search the personal information files saved in a smart home PC to encrypt them with the national encryption algorithm developed by the NSRI (National Security Research Institute) as shown in Figure 2.

Features of aria are described below.

* Block size: 128 bits (16 bytes)

* Key size: 128/192/256 bits (the same specification as AES)

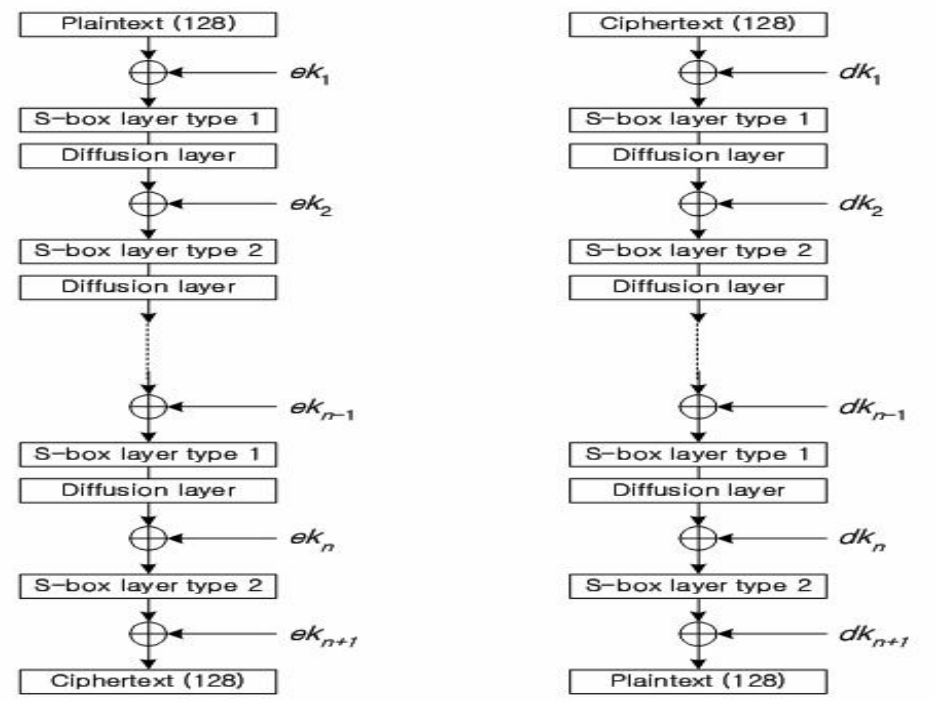

Figure 2. Encryption Round using SP-Network

* Entire architecture: Involutional Substitution-Permutation Network

* Number of rounds: 12/14/16 (depends on the key size)

3.3. Completely Deleting Personal Information saved in Smart Home PC

Files in the windows file system are divided into, saved and managed as file data and meta data.

The file data means actual data of the files, and the meta data means incidental information including file name, file size, execution right and clusters in which file data are saved.

When a user deletes or formats a file, some of the meta data are deleted but the file data are not corrupted at all.

If a file is deleted, completely delete it so that the file data and some of meta data (file name, file size) can be initialized and cannot be recovered.

Figure 3. shows an example with a saved file and how to delete the file (05 following the size is the address of the cluster where the file is saved).

FAT1	FAT2	Directory		clusters	
11100 100	11100 100	filename, size, 05	…	filedata	…

Figure 3. Deleting File

A. Overwrite data in the cluster in which the file data is saved according to the established number and method (Overwrite three times with the once-random value –0x00-0xFF, and once with the once-random value for fast writing).

FAT1	FAT2	Directory		clusters	
11100 100	11100 100	filename, size, 05	…	Garbage value	…

Figure 4. Initializing File Name

B. Initialize file name in the cluster in which the file data is saved as shown in Figure 4.

FAT1	FAT2	Directory		clusters	
11100 100	11100 100	_____, 0byte,05	…	Garbage value	…

Figure 5. Initializing File Size

C. Initialize file size in the cluster in which the file data is saved as shown in Figure 5.

FAT1	FAT2	Directory		clusters	
11100 000	11100 000	_____, 0byte, 05	…	Garbage value	…

Figure 6. Permanently Deleting File

D. Delete the file in the cluster in which file data is saved as shown in Figure 6.

The method of deleting a file described above is to permanently delete files by overwriting in the cluster where the file data is saved at least 3 times, and deleting file name and file size.

4. Checking and Quantifying Smart Home PC Vulnerability

Analyze, check and quantify vulnerability items of the smart home PC operating system of Windows for management thereof.

4.1. Checking and Quantifying User Account

* Guest account management

Check if using guest account is restricted, and an ordinary user account, not a guest account, is created and used where access by an unspecified number of general users is required.

* SAM file access statistics

Check if only system operator can access the SAM file in which password for the relevant user account is encrypted and saved.

* Set minimum length policy check of password.

Check if the minimum password length setting of a user is applied.

* Set maximum period of use policy check of password.

Check if the period of using user password is specified.

* Check user's memory of recent password (check the memory policy for the recent password).

Check if the recent password memorization is specified in order to avoid just previous password to be reused right after changing password.

* Check expired password setting.

Check if "no limit to period of using password" of the current logon user is specified.

* Trivial password

Check if there is no password, if the password is the same as the user ID or can be easily derived. Quantify and manage the result.

4.2. Checking and Quantifying Shared Folder

* Check shared folder setting for management.

Check if the shared folder for management is specified.

* Check user shared folder setting.

Check if shared folders created by a user are specified to quantify and manage them.

4.3. Checking and Quantifying in Service Firewall

* Check alert service.

Check if the alert service sends management alert messages to connected other computers.

* Telnet security setting (service not used)

Check if NTLM authentication is used for the telnet service, and authentication is carried out by entering ID/password to check security setting.

* Check computer browser service.

Check if the list of all computers in the network is updated and managed, and the service which sends this saved list to computers through a browser.

* Check fast user switching · compatibility service.

Check the service which enables one user to log on to use a PC used by a plurality of users while another user who used the PC does not log off.

* Check messenger service.

Check the service for delivering messages through a network.

* Check netmeeting remote desktop sharing service.

Check the service which enables a user to access his/her own computer remotely and allows the user to share the background screen of his/her computer with other computers.

* Check firewall setting.

Check if a firewall for controlling external access to user's computer is specified.

4.4. Screen Saver

* Check automatic logon.

Check if the current logon user is specified to implement automatic logon without entering password.

* Check screen saver activation setting.

Check if the screen saver is specified to operate.

* Check automatic execution setting of the screen saver.

Check if the standby time of the screen saver is within 5 minutes.

* Check screen saver screen lock setting.

Check if the screen saver is protected with password.

4.5. Automatic Update of Security Patch

* Check installation of a vaccine program.

* Check if the vaccine program is executed.

* Check if the vaccine program engine is periodically updated so that the latest version thereof is used.

* Check if the operating system is automatically updated.

5. Security Management of Personal Information Vulnerability of Smart Home PC

5.1. Contents of Vulnerability Security Management of Smart Home PC

The result of vulnerability diagnosis and personal information diagnosis of a smart home PC is provided to a relevant user as diagnosis scores/total scores by items. If the smart home PC is vulnerable, the user can click the automatic modification button to check vulnerabilities and to ensure security.

The user can select the result of personal information search to execute the encryption button shown in Figure 7 and enhance security by encrypting personal information.

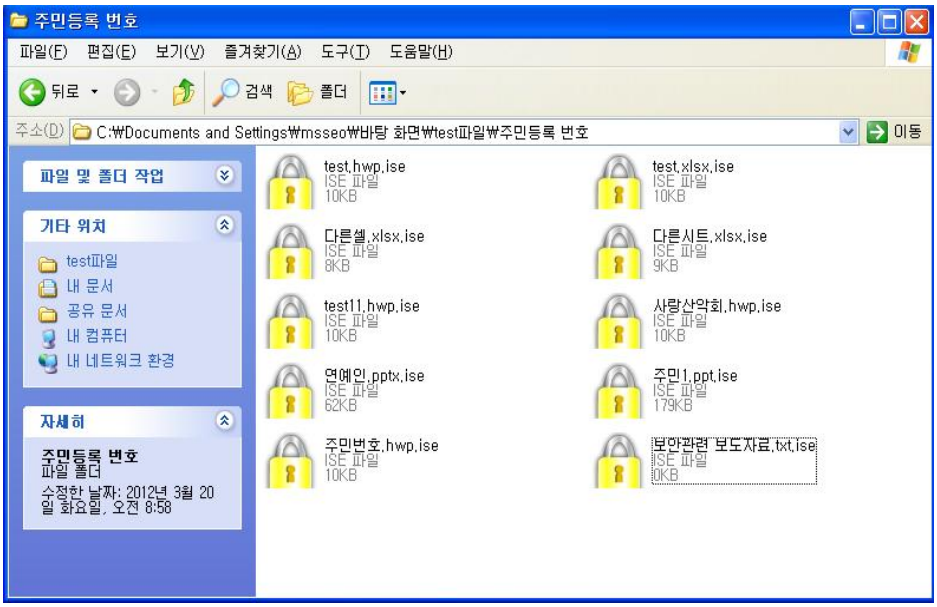

Figure 7. Encrypted Personal Information File

5.2. Operating Automatic Vulnerability Security

Vulnerabilities found in a smart home PC are diagnosed through computer virus scanning and treated with the virus vaccine shown in Figure 8. The security program for enhancing vulnerability to security of a user operates to be semi-automatically updated in the smart home PC.

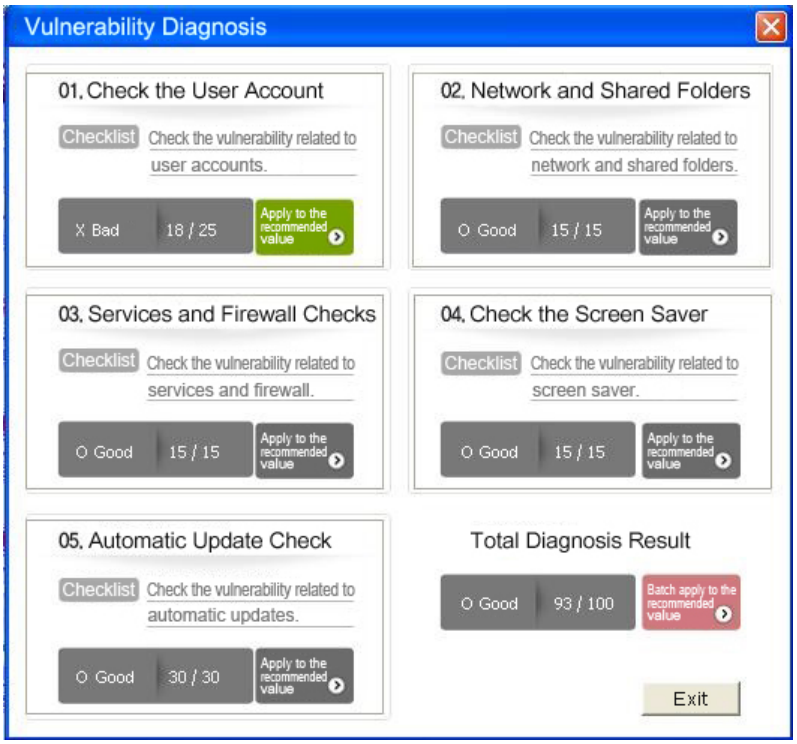

Figure 8. Result of Vulnerability Diagnosis and Automatic Security Update

6. Conclusion

It is necessary to study smart home PC information security because personal information theft is increasing, and user's personal important information in a smart home PC is increasingly stolen as the Information Privacy Act has been enforced. It is possible to enhance smart home PC security and to minimize personal information theft in a smart home PC by means of PC security setting, smart home PC security patches, and personal information management.

This study aims to automatically analyze and check smart home PC vulnerabilities to keep the security level for protecting personal information and to implement semi-automatic update. Another aim is to search personal information in a smart home PC to safely encrypt personal information files, or to permanently delete files so that the personal information files of which the period of use has elapsed cannot be recovered in order to eliminate vulnerabilities concerning personal information protection in a smart home PC to enhance security.

It is necessary to further study scroll machines and automatic update of settings for eliminating vulnerabilities.

References

[1] Ministry of Public Administration and Security, Standards and measures ensuring the safety of personal information commentary, **(2011)** September.
[2] D. W. Park, "Study on Real-time Cooperation Protect System Against Hacking Attacks of WiBro Service", Journal of information and communication convergence engineering, vol. 9, no. 4, **(2011)** August, pp. 353-357.

[3] S. Alcalde Bagüés, L. A. Ramon Surutusa, M. Arias, C. Fernández-Valdivielso and I. R. Matías, "Personal Privacy Management for Common Users", International Journal of Smart Home, vol. 3, no. 2, **(2009)** April, pp. 89-106.
[4] S. H. Kwon and D. W. Park, "Hacking and Security of Encrypted Access Points in Wireless Network", Journal of information and communication convergence engineering, vol. 10, no. 2, **(2012)** June, pp. 156-161.
[5] M. S. Seo and D. W. Park, "The Pattern Search and Complete Elimination Method of Important Private Data in PC", Proceedings of the Korean Institute of Information and Communication Sciences Conference, vol. 17, no. 1, **(2013)**, pp. 213-216.
[6] S. K. Lee, "A Study on the Legislative Scheme and the Current Status of Personal Information Protection of the United States", Korean Constitutional Law Association, vol. 18, no. 2, **(2012)**, pp. 195-214.
[7] National legislation Information Center, Privacy Protection Rules, http://www.law.go.kr, **(2013)** March.
[8] W. H. Nam and D. W. Park, "A Study on Cloud Network and Security System Analysis for Enhanced Security of Legislative Authority", The Journal of the Korean Institute of Information and Communication Engineering, vol. 15, no. 6, **(2011)**, pp. 1320-1326.
[9] B. Y. Park, J. W. Yang and C. H. Seo, "System Design and Implementation for Security Policy Management of Windows Based PC and Weakness Inspection", Journal of the Korea Institute of Information Security and Cryptology, vol. 18, no. 1, **(2008)**, pp. 23-30.

Authors

Mi-Sook Seo, was born in Dae-Gu, South Korea in 1971. She is in master course studies in the Department of Integrative Engineering at the Hoseo Graduate School of Venture, South Korea. Currently, she is CEO of the Security Management Solution (Co.). She received the degree in Computer Science from the Korea National Open University in 2000. She is research interests are Computer Security, hacking, information protection, IT convergence, and network security.

Dea-Woo Park, was born in Seoul, South Korea in 1959. He is an Associate Professor of the Department of Integrative Engineering at the Hoseo Graduate School of Venture, South Korea. Professor Park received the B.S. degree in computer science from Soongsil University in 1995. He then received the M.S. degree in 1998. He received the Ph. D. degree from the computer science department of Soongsil University in 2004. He has worked as the head of researcher and developer laboratories at Magic Castle Co., Ltd. He has lectures Computer Network Security at adjunct professor and part-time lecturer in Soongsil University for 10 years. Also he worked a senior researcher of KISA. His research interests are hacking, forensics, information security of computers and networks, mobile communication security, and national cyber security.

