Computing and Informatics, Vol. 27, 2008, 731–741

THE DEVELOPMENT OF SECURITY SYSTEM FOR SHARING CAD DRAWINGS IN U-ENVIRONMENT

Hangbae Chang, Kyung-Kyu Kim, Yeongdeok Kim

Daejin University, San 11-1
Sundan-Dong, Pochen-Si, Gyeonggi-Do, Korea
&
Yonsei University,134 Sinchon-Dong
Seodaemun-Gu, Seoul, Korea
&
Woosong University, 17-2 Jayang-Dong
Dong-Gu, Daejeon, Korea
e-mail: hbchang@daejin.ac.kr, kyu.kim@yonsei.ac.kr, ydkim@wsu.ac.kr

Revised manuscript received 10 January 2008

Abstract. Because most CAD drawings are composed of a collection of files with various extensions, there exist problems associated with the processing speed and the accuracy of CAD files encryption (decryption) using file based secure methods. In this study, an innovative system of securing CAD files based on the workplace against illegal piracy of design knowledge in ubiquitous environment is presented. The proposed technology is to store all design files in the secure workplace which can be accessed by the authorized users and design applications only using Application Programming Hooking at user level and System Service Table at kernel level. The technology is demonstrated in this paper using its implementation example in an automobile company to verify it and CAD files can be shared among users without a concern of its leakage to the competitors by internal user.

Keywords: Ubiquitous security, information sharing, API hooking, system service table

1 INTRODUCTION

Ubiquitous computing names the third wave in computing, just now beginning. First were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, or the age of calm technology, when technology recedes into the background of our lives. Alan Kay of Apple calls this "Third Paradigm" computing. Ubiquitous computing has as its goal the enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user. A number of researchers around the world are now working in the ubiquitous computing framework. Their work impacts all areas of computer science, including hardware components, network protocols, interaction substrates, applications, privacy, and computational methods. As envisioned by Mark Weiser, one of the goals of ubiquitous computing is to provide the dynamic and stable collaboration environment by sharing information and cooperating with multiple agents which are users, objects, and events. Especially in the field of manufacturing industry, there are frequently times when the design knowledge has to be shared with the internal users, suppliers, collaborators and customers. When the paper drawings were shared with different parties involved in the design and construction process, it was difficult for others to extract the design knowledge from the paper drawings for their unauthorized use. With recent advances in electronic design files, Computer Aided Design (CAD) has become a common place to store the design knowledge. CAD data files are culmination of the design knowledge of the engineering companies.

However, this cooperative environment gives rise to security problems such as illegal intrusion or threat of access to critical information by internal or external users is occurring at the same time. Even though there are many kinds of security systems for networks or servers, such as Virtual Private Network (VPN), Intrusion Prevention System (IPS), and Firewall, to prevent illegal intrusion upon information by external users, these security systems to protect illegal leakage of information by internal users are not warranted [1]. Internal users should inevitably have an access to critical information as required by their duties and, at the same time, protect the leakage of information they have an access to. Due to work efficiency as well as technological limitations, the best way to prevent internal information from being leaked out has been leaving it to just internal users' conscience. Therefore, there is a desperate need to develop security technology which controls the leakage of internal information in proper methods without damaging work efficiency in Figure 1 [2].

In this study, the essential information security technology based on the workplace was designed to protect the inappropriate leakage of important information composed of various file formats (DWG, JPG, STD) such as drawings different from common documents (Word, Power Point, Excel). To control an access to this workplace using authorized user and application, we used Application Hooking at user level and System Service Table at kernel level [3].

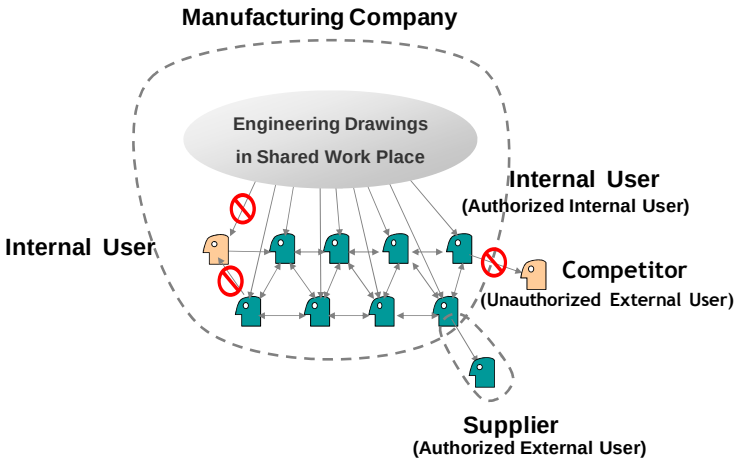

Fig. 1. Collaboration with multiple users by limited sharing engineering drawings

2 RELATED STUDIES

As the information technology evolves, it has become easier to share and distribute the electronic CAD files leading to the efficient and collaborative design environment. However, the recent collaborative software such as DBMS (Data Base Management System), PMIS (Project Management Information System), KMS (Knowledge Management System) made CAD data more difficult to secure. If the CAD files fall into the competitor's hands by internal users, the engineering company will lose its competitive advantage over its competitors [3]. Therefore, it is critical to secure the CAD files so that such valuable intellectual property is not lost to competitors. In this section, we present studies of securing CAD files against illegal piracy of design knowledge.

2.1 Device Control Technology

The device control technology addresses the channel of knowledge leakage through portable storage devices such as USB memory device, CD, and DVD. Since this technology controls a variety of devices installed on the PC, it is difficult to implement such a restrictive security policy on a corporatewide basis. Besides, it is nearly impossible to control all such possible hardware devices without negatively affecting the productivity. As a result, this device control technology can be applied to the limited number of internal users dealing with simple tasks.

2.2 Digital Right Management System

The Digital Right Management System is a technology to secure information over the whole sectors from creating electronic document containing information to using, transmitting, and deleting of it, it restricts discreet use of documents by controlling word applications according to user authority. This technology can be applied to common document file, web page, and image file which constituted with minimum environmental change and single file format (one application manipulates only one extension file).

However, in case of CAD files composed of a collection of files with various ex-tensions (one application manipulates N extensions files), the encryption and decryption operations on files would become inefficient because they should be performed on different extension names and the links among these CAD files have to be managed accordingly [4].

2.3 Intermediate Design File Format

CAD files can be shared in an intermediate format such as Autodesk's DWF (Design Web Format) without giving away a significant amount of design knowledge. These intermediate design formats provide drawings on the digital blue print without divulging the critical design knowledge that facilitated the civil infrastructure design. In addition, these files can be password protected by using zip software so that they can be transmitted securely over the internet. The password can be set to be expired after a certain time period which would limit the access to the authorized person for the authorized time window.

However, this method was developed not for securing information but for maintaining the integrity as well as sharing information, so it may be let out when the third user gets the password. Since it simply controls only the access to file, it cannot have secure function to prevent leakage of drawings such as preventing illegal copy, controlling authority, and tracking log.

3 DEVELOPMENT OF VIRTUAL SECURE DISK

CAD drawings which are composed of various file formats are difficult to encrypt them by file based method, because so it produces problems for encryption processing speed and accuracy. Therefore CAD drawings and source codes cannot be secured by simply encrypting some numbers of file. Hereby, we have needs to develop technology to secure important information in the whole process from creating temporary file to deleting it independent to file format with maintaining user work environment.

In this study, we developed a technology to save all work results for authorized application only to Virtual Secure Disk (VSD) and to protect other accesses to it by other unauthorized programs for design or developmental project with requiring

security. In here, VSD is an encrypted virtual file system which only allows certified users and applications.

To overcome the limitation of the existing document security methods, the VSD technology is proposed which can allow only authorized users and specific CAD software to have an access to VSD in an efficient working environment. The VSD is a virtual disk which is physically a single file, but is recognized as a disk drive by the operating system. When the file input/output occurs, encryption and decryption is performed automatically in sector unit. As shown in Figure 2, the VSD is accessible by the designated CAD program only but not by other programs like Microsoft Word. Therefore, the user won't be able to save any CAD files in general disks. Figure 4 shows physical disks and a mounted Virtual Secure Disk.

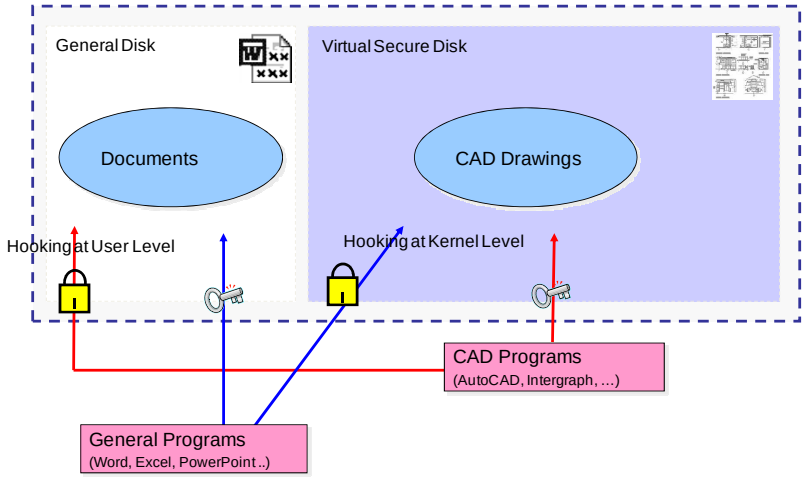

Fig. 2. Workplace based CAD drawing security concept

3.1 Creating Virtual Securing Disk

Physically, VSD exists as one recognizable disk drive on one file or operating system. As shown in Figure 3, when user commands to install this disk, it holds virtual disk volume in specific space within common hard disk and creates VSD driver with referring appropriate information(physical position for disk, disk partition etc.). This VSD driver interacts with file system in operation system which arranges the file management rule.

3.2 Access Control to Virtual Secure Disk

When the application module accesses files stored in the disk driver and the VSD driver, the access control device determines whether a space in which a corresponding

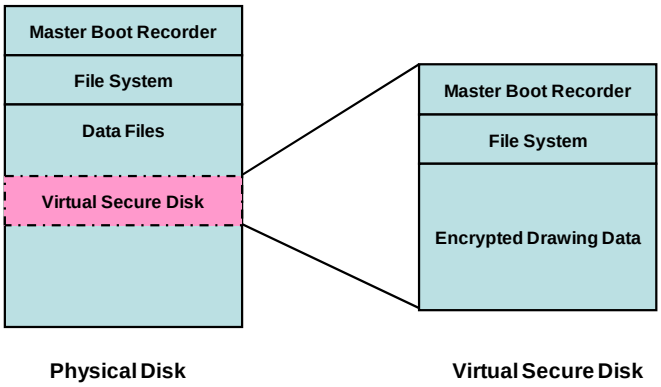

Fig. 3. Logical architecture for virtual secure disk

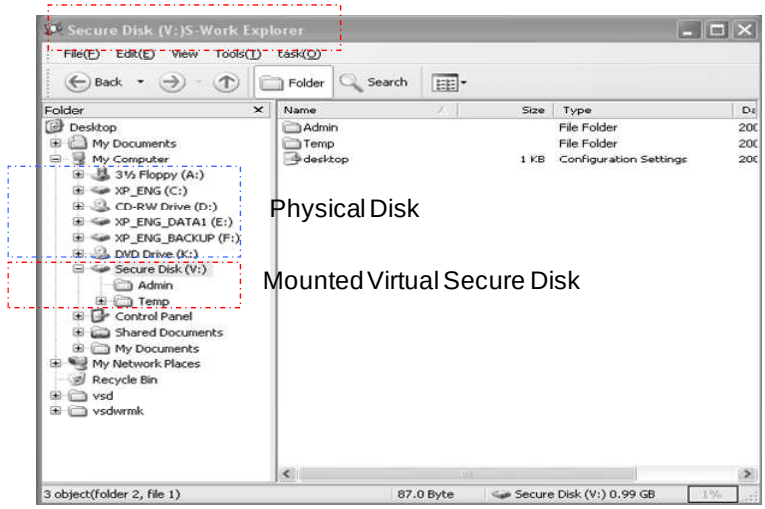

Fig. 4. Installed virtual secure disk

task is performed is the disk driver or the VSD driver, and decides access by determining whether the application module is authorized for access to a corresponding file. Based on the predefined security policy, authorized applications such as CAD Program, Development Program, and Design Program can read (write) all information in Virtual Secure Disk, but cannot read (write) it in General Disk. On the other hand, unauthorized applications such as Word Program, Excel Program, and Power Point Program can read (write) all information in General Disk, but cannot read (write) it in VSD. At this time, we use Application Programming Hooking (API) at user level and System Service Table Hooking at kernel level for controlling access to Virtual Secure Disk. 'Hooking' means the technology to rearrange the execution

sequence for user defined tasks before starting application and hands over the execution priority after completing the user's task. API hooking technology is used for controlling the access of authorized application to VSD at user level [5]. However, because API hooking technology cannot be appended to all programs installed in User PCs, for controlling access to VSD for unauthorized (common) applications, we hook System Service Table (SST) which is an essential route in the execution process of general applications. Whenever a user calls a function at user level, Operating System finds system function address for the called function in kernel level which is defined in SST and makes system function execute. SST Hooking make the user defined tasks execute in New SST before starting system function at kernel level [6]. For example, 'CreateFile()' Win32 API function is used for opening file in common application. This user level function is implemented by 'NtCreateFile()' contained in 'Kernel32.dll' at system level. We make 'ZwCreateFile()' which is the user defined function between 'CreatFile()' and 'NtCreateFile()'.

3.3 Encryption of CAD Drawings in VSD

When VSD is stolen by internal user, a user can operate VSD and read it by using general file system. For preventing this dangerous situation, we should encrypt it. Generally the Input/Output speed is significantly slower than the calculating speed of Central Processing Unit (CPU), so CPU must wait in idle status until it is completed the disk Input/Output process. In respect of this, we encrypt all CAD drawings of Input/Output to/from Virtual Secure Disk by sector unit for CPU idle time, so there is no time delay problem and the efficiency of the data encryption is improved. As mentioned above, the method we suggested is different than file based secure method from the starting point of applying security and its subject to securing method, encryption method, and supporting file format. First, in case of applying security method and its subject, file based secure method opens file throughout temporary file format and applies secure method in initial saving time, but workplace based secure method controls the creating route for temporary path and sets up the security in time of creating file. In case of secure method, file based method encrypts for one unified file format but workplace based secure method automatically encrypts all files without their format by saving them on specific disk. Finally, file based method is influenced by file format since it encrypts files by analyzing the structure of specific file, but workplace based method is not concerned to supporting file format since it controls access for applications which manipulate various file format (Test program: Auto CAD, Pro Engineer, CATIA, Matlab, Solid Edge, MS Visio, Acrobat Distiller, Solid Works, Photoshop, Illustrator, etc.).

4 CASE STUDY OF VIRTUAL SECURE DISK

The software utilizing the VSD technology is tested for "AutoCAD 2005" design program under "Windows XP" environment. When an authorized user logs in, s/he

is allowed to create VSD along with the existing file system on his/her computer. The user now can create an architectural design drawings using AutoCAD 2005. After the user completes the design, he/she tries to save the CAD file to a general hard disk. As shown in Figure 5, an error message appears on the screen to inform the user that the design cannot be saved and advises him/her to save it to the VSD. On the other hand, when the user tries to save the work performed in Note Pad to the VSD, a similar error message appears on the screen to inform him/her that the Note Pad file cannot be saved on VSD and advises him/her to save it on the general hard disk.

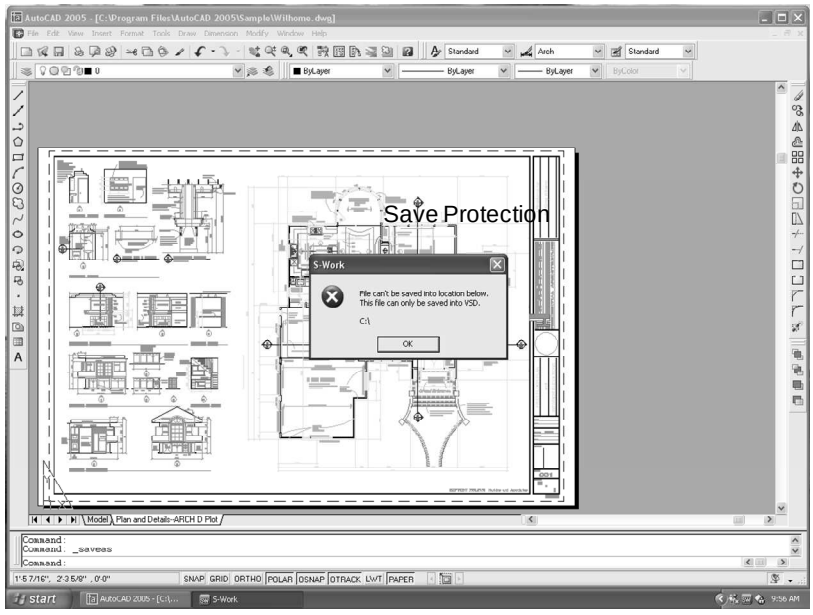

Fig. 5. Failed Attempt to Save the CAD files in general hard disk

Then we measured the data loading time and the speed of data encryption (and de-cryption) by changing the size of data in this secure environment. As a result, there is no difference between before and after applying security. Table 1 shows the speed of data encryption (decryption).

When the Security Explorer is used to copy the CAD file for the external user, the internal user has to follow the following steps: 1) select CAD files to be copied for the external user, 2) select the external user who would receive CAD files, and 3) select a method to send CAD files, i.e., E-mail or portable storage device. The authorization to distribute the CAD files will be determined according to the internal company security policy and logs by the internal user are saved for later use in case when the security policy is violated by the internal user.

Data Size	Normal Drive	Virtual Secure Disk
50 MB	4 sec	6 sec
180 MB	32 sec	34 sec
212 MB	35 sec	32 sec
422 MB	73 sec	75 sec
703 MB	138 sec	138 sec
1.59 GB	320 sec	340 sec

Table 1. Time of drawing data loading

5 SUMMARY AND CONCLUSIONS

Ubiquitous computing is a post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities. As opposed to the desktop paradigm, in which a single user consciously engages a single device for a specialized purpose, someone "using" ubiquitous computing engages many computational devices and systems simultaneously, in the course of ordinary activities, and may not necessarily even be aware that they are doing so. There are a variety of terms in use to describe this paradigm, many of which are associated with a particular institution or perspective. Some of these are general (pervasive computing, ambient intelligence, and more recently, everyware), while others primarily concern the objects involved (physical computing, the Internet of things, haptic computing, things that think, and spime). At managerial level, many tasks in ubiquitous environment are processed by interaction between computational elements rather than by performing individual actions. Especially in the field of manufacturing industry, the internal users should share engineering drawings (Computer Aided Design, CAD) to finish a design task. At the same time the security accidents of leaking the CAD drawing information by internal user within company increase significantly; the security technology for preventing information leakage has been developed. But the CAD drawings, which are composed of various formatted files, should be encrypted by its extension and controlled with separate methods since the existing technologies depend on file based information encryption. Therefore there are some problems related to the encryption speed and preciseness for drawing information. To overcome the limitations of literature reviews, we developed the security technology based on the workplace to prevent the illegal leakage of drawing information by internal user. In the result of this study, a workplace was developed based on security technology, which controls the access to specific storage (Virtual Security Disk) and encrypts (stores, manages) the CAD drawing files by sector according to user and application authority using API hooking technology and System Service Table hooking technology.

This developed technology has better efficiencies in encryption method, supporting file format, and the time and subject of applying technology in comparison with the file based encryption method in Table 2.

As the developed technology was applied to a major automobile company in Ko-

Items	File based Secure	Workplace based Secure
Time and Subject Of Security Applying	Work-Completed Specific File	All Files in Work Cycle
Encryption	Encryption by Block	Encryption by Sector
File IO Speed by Encryption	Speed Change	No Change
Supporting File Format	Specific file format	Not related to file format

Table 2. Time of drawing data loading

rea following a working scenario to verify the applicability and security of technology, the use of CAD drawings could be controlled safely by internal users. A technology developed in this study allows authorized application and user access to the specific drive which has important information without partitioning new physical drive in typical file system. This technology is expected to be applied in developing information security technology for computing environment (a central server processes minimum tasks and stores sharing file and program, and User PCs carry out most tasks but they manage hybrid information storages which are for personal and organizational work).

This computing environment means the transition computing stage step between 'Thin Client' (because central servers have most information, the degree of security is high but the work efficiency is low) and 'Fat Client' (because clients have most personal and organizational information in their storages, the degree of security is not) [7].

Acknowledgement

This research is supported by the ubiquitous Computing and Network (UCN) Project, the Ministry of Information and Communication (MIC) 21st Century Frontier RnD Program in Korea.

REFERENCES

[1] Chechanowicz, Z.: Risk Analysis: Requirements, Conflicts and Problems. Computer and Security, Vol. 16, 1997.

[2] Von Solms, B.: Information Security Governance: COBIT or ISO 17799 or both? Computer and Security, Vol. 24, 2005.

[3] Green, R.: CAD Manager: Drawing Security. Cadalyst, May 2005.

[4] Lee, Y. H.—Hwang, D. J.: Design and Implementation of Agent Based Dynamic Digital Rights Management. Journal of Information Processing Association, D. Vol. 8D, No. 5, October 2001, pp. 613–622.

[5] Nagar, R.: Windows NT File System Internals: A Developer's Guide. O'Reilly and Associates, 1997.

[6] Deker, E. N.-Newcomer, J. M.: Developing Windows NT Device Drivers: A Programmer's Handbook. Addison-Wesley, 1999.

[7] Otwell, K.—Aldridge, B.: The Role of Vulnerability in Risk Management. IEEE Proceedings of the 5th Annual Computer Security Applicant Conference, pp. 32–38, 1989.

Hangbae Chang received the Ph. D. degree in information system management from Yonsei University, Korea, in 2006. Since 2007, he has been with the Department of Business Administration, Daejin University, where he is currently a Professor. Before joining the university, he was a research member of senior technical staff at the Soft Camp Corporation which is an Information Security Company in Korea. His research interests include information security management system, ubiquitous computing, and business based information strategy.

Kyung-Kyu Kim received the Ph. D. degree in business administration from University of Utah, in 1986. From 1986 to 1990, he was a Professor of accounting and MIS in Penn State University and from 1990 to 2002, a Professor of information systems at the University of Cincinnati. Since 2002, he has been with the Graduate School of Information from Yonsei University where he is currently a Professor. His research interests are ubiquitous business strategy, knowledge management system, and supply chain management.

Yeongdeok Kim received the Ph. D. degree in computer engineering from Daejeon University, in 2002. Since 2002, he has been with the Department of Computer Information Science and Engineering, Woosong University, where he is currently a Professor. His interests are ubiquitous application and security service, home networking security, information security policy, internet ethics, and internet security.