The Case Study of Information Security System for International Airports

Hangbae Chang[1], Moonoh Kim[2], Hyuk-jun Kwon[3], and Byungwan Han[4]

[1] Daejin University,
San 11-1 Sundan Dong, Pocheon Si, Gyonggi Do, 487-711, Korea
hbchang@daejin.ac.kr
[2] Yonsei University
134 Sinchon-Dong, Seodaemun-Gu, Seoul, 120-749, Korea
perrang2@yonsei.ac.kr
[3] Yonsei University
134 Sinchon-Dong, Seodaemun-Gu, Seoul, 120-749, Korea
junkwon@yonsei.ac.kr
[4] Tongwon College
Sinchon Ri, Silchon Eup, Gwanju-Si, Gyonggi Doul, 464-711, Korea
bwhan@tongwon.ac.kr

Abstract. With continuing security concerns for airport operations, the protection of internal operational protocols of an international airport has become more critical than ever before. Therefore, the Information Security System (ISS) was developed for Incheon International Airport which can protect the critical information related to airport operations. The developed ISS includes a document access control server/client agent, a user access control service linker, and an operational log file database. The ISS was developed in consideration of information life cycle of airport workflow. As a result, it can securely protect the computer system at Incheon International Airport by (1) performing real-time encoding of the users who accessed the protected files and folders, (2) limiting the user's capability to edit the protected documents, (3) tracking transmitted files to the outside companies, (4) blocking the user's access to portable storage devices, and (5) inserting security water marks on the printed outputs. With the implementation of the ISS, the real-time information system audit environment has been securely established at the Incheon International Airport Corporation.

1 Introduction

Construction of the Incheon International Airport (IIA) was completed in December 2000 and its design is shown in Fig. 1. with two major runways and a passenger terminal of 496,000m^2. Recently, the IIA was selected as the best airport worldwide by ACI and IATA in 2005 [1]. Airport security can be classified into two categories: facility security and computer security. The physical facilities of the IIA are well protected by the airport security force that is in charge of the fences around the

M. Denko et al. (Eds.): EUC Workshops 2007, LNCS 4809, pp. 22–30, 2007.

airport, passenger terminal, transportation center, auxiliary facilities and free economic zone. The computer information security system has become more complex because most corporations like Incheon International Airport Corporation (IIAC) uses an integrated information system which shares information through intranet, groupware, knowledge management system and electronic document management system. This paper focuses on the computer information security system which would not only protect the information on the airport operations from outsiders but also prevent the internal employees from illegally releasing the protected information to the outsiders.

Fig. 1. Design of the Incheon International Airport

Although the construction and operation of the Incheon International Airport can be considered a very successful one, there are some areas in the corporate information security which can be improved.

- Lack of response plan for emergency: There are several emergency scenarios for the airport facilities but there is a lack of the security and response plan for emergency failure of the computer system.
- Lack of integration of emergency response systems: The current emergency response system at IIA are not well integrated and for an emergency situation such as illegal entry or fire through the electronic CAD drawings to locate the point of emergency, integration of CCTV and sensors, and broadcasting system to announce the emergency and evacuation plan.
- Lack of protection of corporate information: The critical information such as various internal documents and CAD drawings of the IIA facilities are not well protected and can be accessed and released to the outsiders by the malicious internal employees.

Recently, as reported in the Chosun newspaper on November 25th 2005, there was an incident at IIA which involved an internal employee who illegally accessed and released the design documents for the system integration project of IIA valued over $150 million. This project was to integrate the security system, the communication system and the airport information system. The internal employee accessed the 250 related documents for the bidding purpose, saved them in CD and supplied it to a company who is interested in winning this security system integration project. This

information apparently would have given an advantage to this company over other competitors. The internal employee was later arrested by the police and this incident was considered a clear sign of computer system vulnerability to the internal intrusion at IIA. Such an internal security breach is more damaging than the external security breach because the internal employee is more knowledgeable with the computer system at IIA. This paper focuses on the development of the computer information security protection software and its implementation at IIA.

2 Corporate Information Protection Methods

As discussed earlier, the critical corporate knowledge can be leaked out by internal users in a number of ways. In this section, various knowledge protection methods are discussed [2].

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 after literature reviews.

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 corporate-wide 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 Document Security Technology

The document security technology restricts discreet use of documents by controlling software packages used for preparing such documents such as Notepad, Word and Excel and enabling the management of the documents according to user authority. This technology can be applied to simple documents such as web pages and image files with a single extension.

2.3 Policy and Contract Approach

For the ultimate security of corporate knowledge, a contract like a non-disclosure agreement should be signed by everyone including the internal staff, collaborating

companies, suppliers and customers. This contractual protection of the corporate knowledge will give a clear message to all parties that the legal action will be pursued upon illegal handling of the confidential files.

3 Computer Security Protection System Development

As shown in Fig. 2, during a typical flow of the information in its life-cycle from creation to delivery, security holes can be identified as follows [2]:

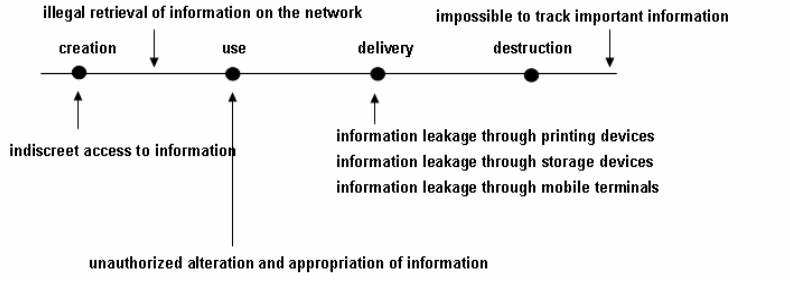

Fig. 2. Identification of security holes throughout the life cycle of information

- Indiscreet access to information: Without the access control system for newly created information, anybody may access the information indiscreetly. Then the value of information is diminished and the potential of information leakage is high.
- Unauthorized alteration and appropriation: Without the document security system, the information can be altered, misappropriated and misused by anybody.
- Indiscreet leakage of information: Without the device control system, the information can be distributed through the printing devices, portable storage devices and mobile terminals.
- Impossible to track important information: Without the document tracking system, it is difficult to track those who are involved in the information leakage and make them accountable for the damages caused by the information leakage.

3.1 Real-Time Encryption of User Files and Folders

As shown in Fig. 3, information created by users must be encrypted selectively or compulsorily according to the corporation's information security policy. If a separate security folder is designated and the access right policy is defined, all information stored in the security folder should be encrypted automatically. In addition, information in the subfolders of the security folder should be encrypted in the same way. Information copied or moved to other folders should remain as encrypted. The standard documents stored in the central computer server should be controlled by an individual user's access level[3, 6].

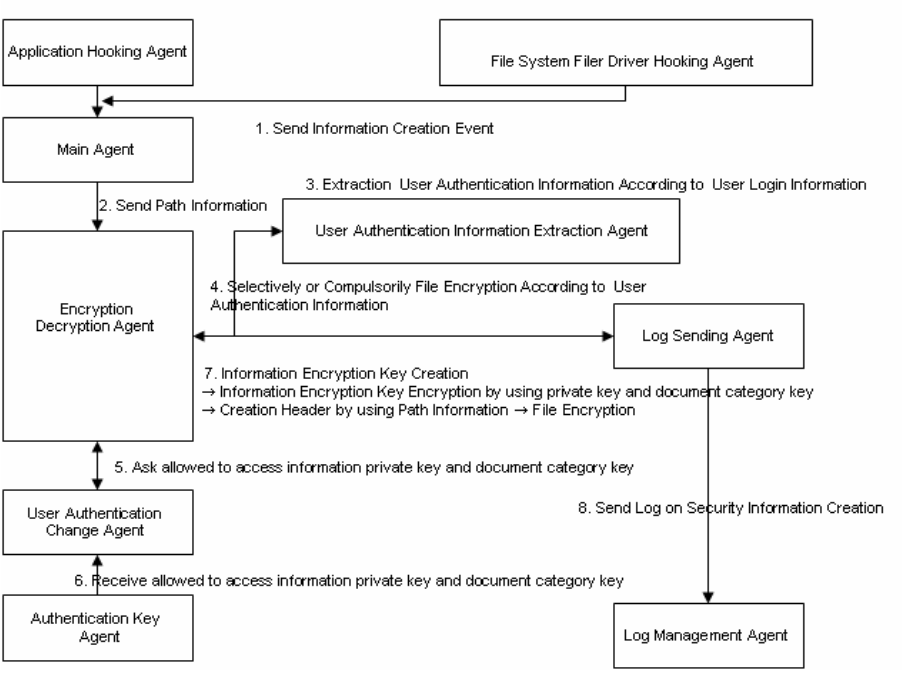

Fig. 3. Process of real-time encryption of user files and folders

3.2 Real-Time Authentication of User's Access Right

All users should be given appropriate levels of access right depending on their status within corporation with respect to reading, editing, printing, releasing, effective date, and auto destruction. The user authentication should be performed in a real-time to verify his/her level of access right. When multiple users at different levels of access right collaborate on the same project, the original data used to create information should be protected separately.

3.3 Watermarking to Printouts

When the confidential information is printed, all printouts should contain watermarking so that printing activities can be monitored. The image of the output should be then sent to the management server which would record the document ID, the staff ID who printed and the time of printing and show on the output.

3.4 Security Code to Mobile Storage Devices

The information security protection system can apply a lock on all files created by a user but it will be cumbersome for a user to unlock all of his files most of which may not be considered confidential. Therefore, it is difficult to prevent an internal user who originally created the document without a security protection from copying it into his mobile storage devices such as floppy disks, USB memory disks, CD-RW,

and PDA. To prevent an illegal release of the confidential document through such external devices, it is necessary for the corporation to limit a user from using his/her personal devices. The information security system should assign the security code to all external devices including as laptop computers.

3.5 Security File for Outside Transmission

Although it is possible to control the document among internal users, when collaborating with people external to the corporation, it is not possible to share the encrypted files. Therefore, a user authentication and his/her access control level should be transmitted along with the encrypted file in the form of the executable file format. When the external user runs the executable file the file can be accessed without installing a separate program in his computer. For external (or internal) users, the file will be preset with the maximum allowed number of access along with the expiration date. If the external user tries to use the file after exceeding the allowed number of access in an allowed time period, the file will be automatically destroyed.

4 Implementation of Information Security System

The developed Information Security System (IIS) was implemented in the computer system at the Incheon International Airport Corporation, which is running Hand Software Groupware under Windows XP environment. As shown in Fig. 5. and 6, when a user log into the computer system, according to the access control policy, the user will be provided with the appropriate level of access control. The user will be then continuously monitored and controlled by the ISS. The standard operational documents within Incheon International Airport Corporation (IIAC) are classified as confidential and the access to these corporate documents is controlled by the ISS. Depending on a user's access rights, he/she can modify the corporate documents. If a user tries to access the file without an appropriate level of authority, he/she will be provided with the encoded message with a warning[5, 8, 10].

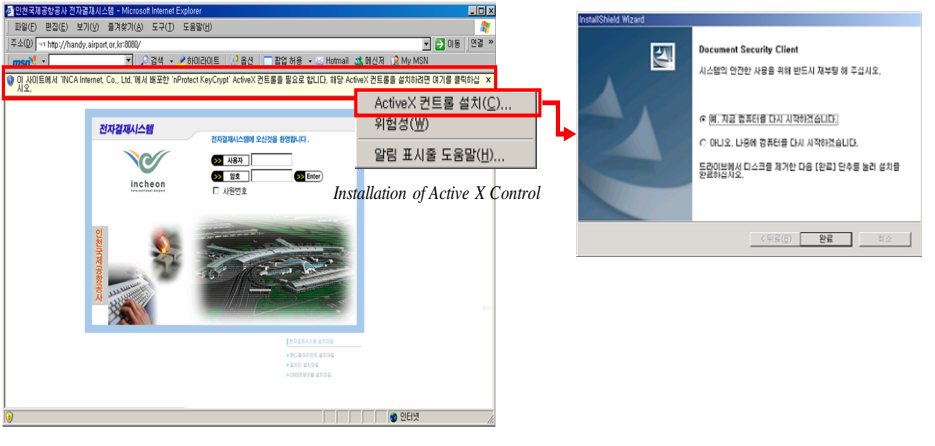

Fig. 4. Installation of Information Security System at IIAC

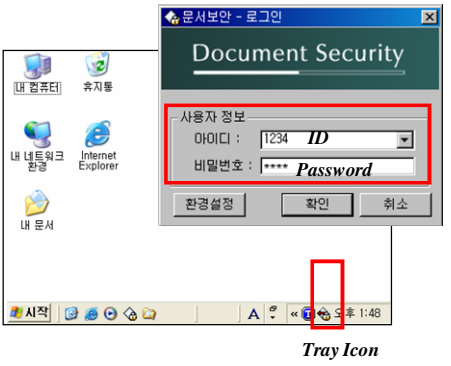

Fig. 5. System Level Protection of Corporate Documents

When the encoded document is to be transmitted to the outside, the encode file and the access right of the external user are transmitted in an executable file format. As shown in Fig. 6, in order to create an externally transmittable file, an internal user must click on the right button on the mouse and create the external user's right and his/her password to open the file. The information security system automatically converts the file into executable file such as "document1.exe". When the external user clicks on the exe file and enters his/her supplied password, the file will be open with a designated level of access right.

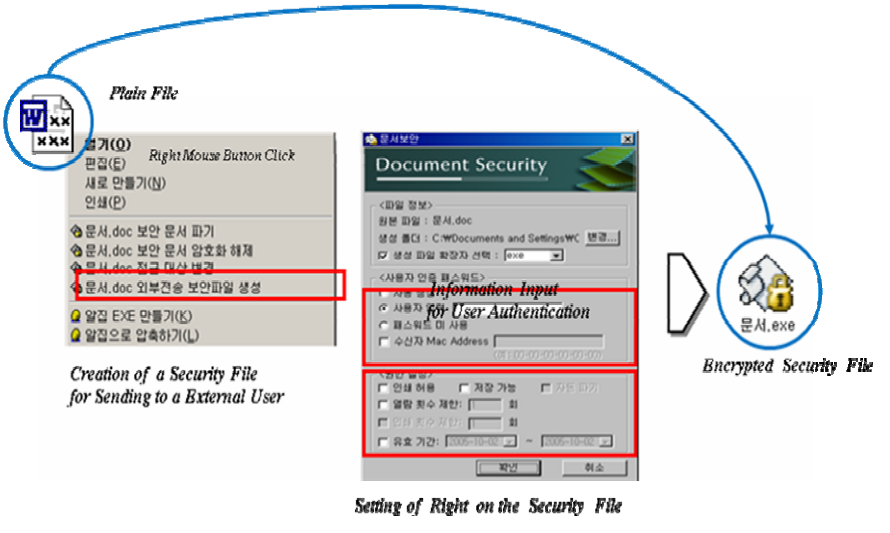

Fig. 6. Creation of Executable File for the Transmission to Outside

Finally, when the confidential document is printed, the information on the user is automatically printed on the output. As can be seen from Fig. 7, the basic watermarking of the IIAC logo, user ID, time of printing will be displayed on the printout. This

will alert the user about his/her identity is being disclosed not only to his/her corporation but also to whomever the output is provided.

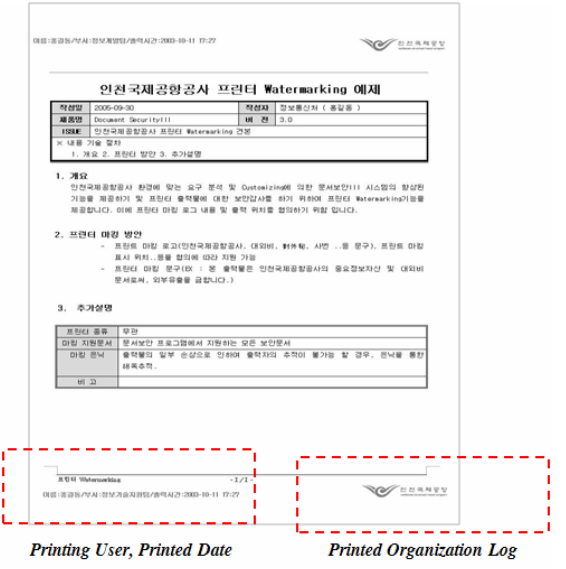

Fig. 7. Print Water Marking

5 Summary and Conclusion

The Information Security System (ISS) was developed and implemented at the Incheon International Airport Corporation (IIAC) where over 1,000 employees share numerous documents in the file formats of doc, xls, ppt, gif, bmp, pdf, txt, zip, and dwg. The ISS presented in this paper not only would provide the secure environment for sharing information at IIAC but also efficient working environment without unnecessary interruptions. Once the airport information security is compromised, the ISS will quickly detect and track down the source of such information leakage.

The information leakage points are identified and used to design the ISS to prevent such leakage. The ISS is designed to prevent the information leakage by deploying (1) real-time user authentication and user file and folder encoding technology, (2) external memory device and printing device control through water marking technology (3) external transmission control of the internal document by creating the executable file with security information.

The proposed ISS include a number of security control features which would not only stop the illegal access to the valuable corporation information but also track down if such an illegal access has taken place. However, when all of these security control functions are implemented, users may find the ISS constantly interfering with their daily job functions. Therefore, in the future, the proposed ISS should be expanded to become a virtual file system which can protect the confidential corporate information including the intermediate and temporary files.

Acknowledgement

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

References

1. IIAC Newsletter, Issue 60 (May 2006)
2. Otwell, K., Aldridge, B.: The Role of Vulnerability in Risk Management. In: IEEE Proceedings of the 5th Annual Computer Security Applicant Conference, pp. 32–38 (1989)
3. Wagner, G.: Agent-Oriented Analysis and Design of Organizational Information Systems. In: Proc. of Fourth IEEE International Baltic Workshop on Databases and Information Systems, Vilnius (Lithuania) (May 2000)
4. Weiser, M.: The Computer for the 21st Century. Scientific American 265(3) (September 1991)
5. Suematsu, Y., Takadama, K., Nawa, N., Shimohara, K., Katai, O.: Analyzing levels of the microapproach and its implications in the agent-based simulation. In: Proceedings of the 6thInternational Conference on Complex Systems, Chuo University, Tokyo, Japan, pp. 44–51 (September 2002)
6. Wagner, G.: The Agent-Object-Relationship metamodel: Towards a uni-fied conceptual view of state and behavior. Technical report, Eindhoven Univ. of Technology, Fac. of Technology Management, Information Systems (May 2002), http://AOR.rezearch.info
7. Bellifemine, F., Poggi, A., Rimassa, G.: Developing Multi-agent Systems with JADE. In: Castelfranchi, C., Lespérance, Y. (eds.) ATAL 2000. LNCS (LNAI), vol. 1986, pp. 89–103. Springer, Heidelberg (2001)
8. Bergenti, F., Poggi, A.: Ubiquitous Information Agents. International Journal of Cooperative Information Systems 11(3-4), 231–244 (2002)
9. Ayesh, A., Bechkoum, K.: Framework of multi-agents internet security system. In: AI 2000. Appl Inform (2000)
10. Lalana, K., Tim, F., Anupam, J.: Developing secure agent systems using delegation based trust management. In: Falcone, R., Barber, S., Korba, L., Singh, M.P. (eds.) AAMAS 2002. LNCS (LNAI), vol. 2631, Springer, Heidelberg (2003)