Modeling of Document Security Checkpoint for Preventing Leakage of Military Information

Jung ho Eom

Military Studies, Daejeon University, 62 Daehakro, Dong-Gu, Daejeon, Korea
eomhun@gmail.com

Abstract

In this paper, we designed a document security checkpoint for inspecting leakage of sensitive documents including military information from the internal to the outside network. Our designed model checks all documents when they are downloaded, sent, and printed. The model consists of four modules: authentication module, access control module, misuse monitor module, and tracking module. The authentication module checks the insider's information and after which allows an insider to log on to the system. The access control module authorizes an insider to do operations (read, write) according to his role and security level. The pattern monitor module watches an insider's abnormal access on documents as comparing the insider's actual process to current process profile in database. The tracking module traces documents sent outside and verifies fabrication of documents. The document security checkpoint prevents indiscriminate access to documents and it does not allow access to documents unrelated to the insider's duty and security level. Even though the document is illegally leaked by an insider, it can be tracked by watermarking techniques in tracking module.

Keywords: *Security Checkpoint, Access Control, Misuse Monitor*

1. Introduction

According to the 2011 Cyber Security Watch Survey [1], 46% of respondents said insider attacks is more damaging than outsider attacks. An estimated 63% of them uncovered that most common insider e-crimes were unauthorized access to or use of corporate information. Insiders are the greatest potential threat to information system (IS) security because they understand the information of their system, network structure, and security policies [2]. An insider threat has occurred across all computing environments, causing severe damage to his/her IS and organization [3]. The military information system is no exception. Specifically, if a national defense policy, strategy, and tactics are leaked, these are directly connected with national security.

In this study, we designed a model of document security checkpoint for preventing leakage of military information by insiders. Our designed model focuses on monitoring abnormal/unauthorized access, operations (read or write), and transportation to maintain the confidentiality of military information. It monitors access to documents by the access control module, considering the duty and roles of an insider, documents, and security level. It also watches abnormal access on documents by pattern monitor module. Login and access to unclassified documents are controlled by the authentication module.

2. Background and Related Works

2.1. Background

The insider uses his legitimate authorization to perform some actions that are contrary to the security policy, which might be observed when sensitive information is leaked to some third party or when access to data is given or blocked. The insiders then use their authorization to extend their privileges in a manner that breaks both the access control rules and security policies. An example of such a breach occurs when an insider has a legitimate capability to log in a particular system and abuse that privilege to gain sensitive information or data illegally in the information system [4].

We introduce two cases of information leakage. The first case happened in the Republic of Korea. The part of the Operation Plan (OPLAN) 5027 was leaked by a hacker using IP in China when an officer of ROK-US CFC used an external USB memory to a PC containing the OPLAN 5027 in 2009 [5]. The intelligence authority estimated that it was committed by North Korea's professional hackers. Second case, a foreign intelligence service swiped 24,000 computer files from a US defense contractor in 2011, one of the largest cyber attacks on a Pentagon supplier. Deputy Defense Secretary William Lynn said, "It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies" [6]. The military information leakage by insiders is increasing, and the damage is becoming serious. This paper now focuses on the leakage of military information by insiders and information confidentiality.

2.2. Related Works

Insiders have a profitable advantage over outsiders who might want to cause damage to an organization. Insiders can bypass physical and logical security safeguards that are designed to prevent unauthorized access. Insiders know the security policies, procedures, technology used in their organizations, and the vulnerabilities such as inappropriately enforced policies and procedures or technical flaws of information system. A malicious insider is the one who is motivated to influence an information system adversely through a range of actions that compromise confidentiality, integrity, or availability [4].

Many blocking mechanisms of information leakage have been invented such as the access control model, intrusion detection system (IDS), and the digital rights management (DRM) [5]. Recently, a document-based DRM is used for preventing the information leakage of electric documents by insiders. DRM has been developed for copyright security and piracy prevention of digital contents. This has been used as a means to prevent illegal access to a document or block internal leakage of the document. Figure 1 shows the document DRM system.

The DRM server issues users the license for using content. In addition, it manages users and documents by the manager module. The DRM manager may add users and documents by specific applications. The PC supports document requests or uploads and authorization creation. It allows the user to read documents downloaded from server, according to the user authorization.

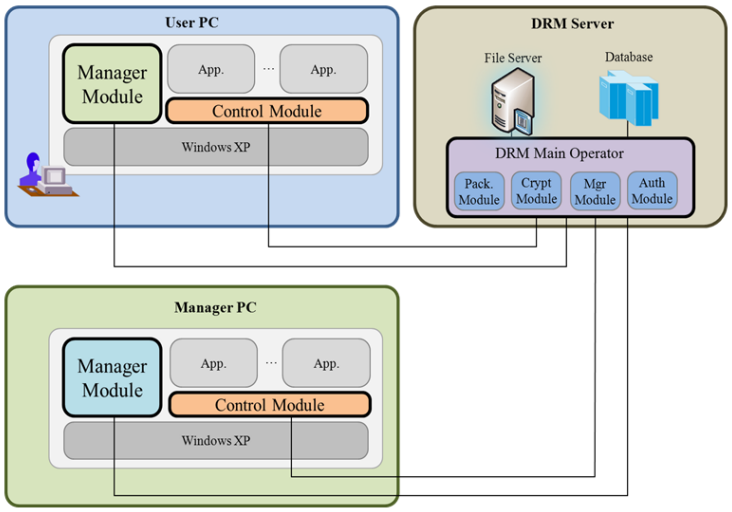

Figure 1. Document DRM

3. Document Security Checkpoint

3.1. Security Requirements

The military information means a type of information created for performing military duties, such as electronic documents, instructions and commands, etc. They are categorized into unclassified and classified information. The unclassified information includes all of the administrative documents and announcements. The classified information is divided into Confidential, Secret, and Top Secret, based on the sensitivity of information, as shown in Table 1 [7].

Table 1. The Example of Insiders in Military Information System

Level	Definition
Top Secret	If leaked, information that have clearly recognized value would likely lead to *catastrophic risks* to national security and military operations
Secret	If leaked, information that have clearly recognized value would likely lead to *conspicuous risks* to national security and military operations
Confidential	If leaked, information that have clearly recognized value would likely lead to *considerable risks* to national security and military operations
Unclassified	Non-confidential information such as general information and announcements

The military personnel are authorized to access military information by their security level. As electronic documents are becoming popular, they could be assigned to specific user or groups by the characteristics of each document and security level. For example, an access control list (ACL) can manage operation permission to documents by each user or group. An ACL can control documents on the server, but it cannot monitor the document downloaded to a user's PC. It also cannot prevent operation on two documents with different security levels. The confidentiality is most important in military information. We indicate vulnerabilities in the security mechanism to apply ACL and derive security requirements according to identified vulnerabilities.

First, it should block indiscriminate access. Insiders should only access documents related to their duties. It also assigns authorization to documents that an insider has access in current work process. It is possible to allow permission by comparing an insider's request and current executed process profile.

Second, confidentiality should not be compromised. It shall not assign permission or authorization to insiders to access documents with security level higher than that of the insider. It should block an operation mode when an insider requests access to each document with different security levels at the same time.

Finally, it should verify the integrity of the document. If the document is engaged in forgery, tampering, and tracking, cyber-military police can identify a leakage path of information by checking hidden information of copyright and ownership.

3.2. Modeling of Document Security Checkpoint

We designed the document security checkpoint for strongly preventing the leakage of military information while it meets the security requirements. Our designed model consists of four modules, as shown Figure 2.

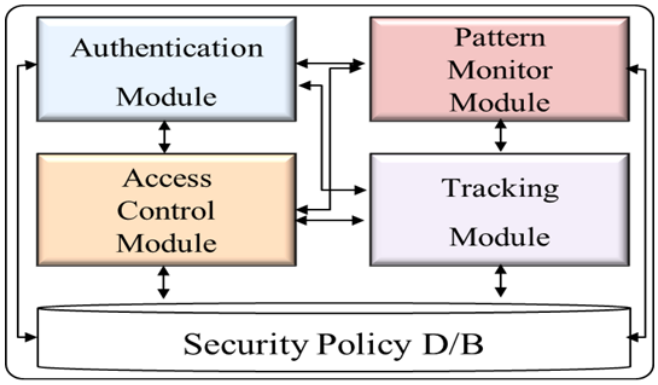

Figure 2. Document Security Checkpoint

An authentication module checks an insider's ID and password to know whether he is a legitimate user when he requests access to the system. The module filters the insider's operation requests to documents using insider information in the database. The module indicates if the insider requests to operate on the document and sends a request to the access control module for checking, whether he has an authorization on the requested operation.

A pattern monitor module monitors the insider's abnormal access on document with their legitimate rights. It prevents unnecessary access to a document upon comparing the insider's actual processing pattern to the current process pattern on profile. Insiders have specific patterns to execute a process related to their duty and role.

An access control module assigns authorization of operation mode to an insider according to the access control policy rules. As shown in Figure 3, an access control module consists of user manager, permission group manager, and authorization processor.

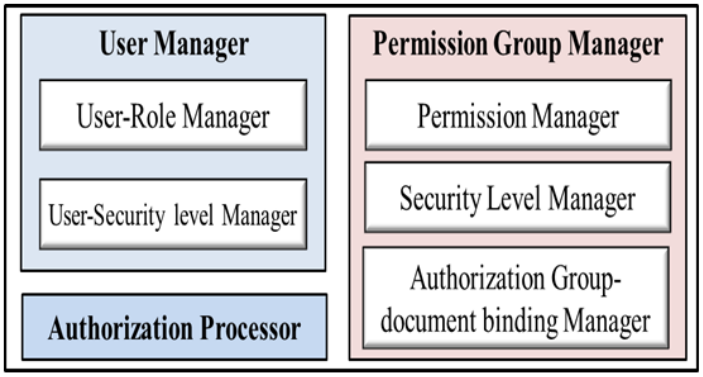

Figure 3. Access Control Module

The user-role manager activates the user role after transmitting the user information from the authentication module. The user- security level manager determines the user's security level depending on the user's ID and role.

The authorization processor assigns operation on documents according to the security transaction generated by the transaction manager and access control policy rules.

The permission manager creates information of operation authorization for transaction configuration using the information of document and operation mode. The security level manager checks the security of user, role, and document. The authorization group-document binding manager determines the binding configuration of the correlation between each authorization group and documents.

A tracking module hides information of copyright and ownership in the documents. It uses text watermarking which adds new information to the document. It creates data with a mark and secret/public key by the marking algorithm. We can select line shift coding, word shift coding, and character coding in technologies inserting text watermarks [8]. A process of inserting marks is described in Figure 4.

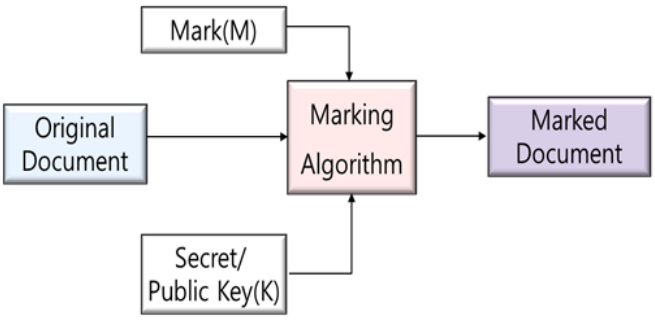

Figure 4. Watermarking Insert Process

4. The Case Study

The document security checkpoint can be minimized to leak document-based military information by reducing vulnerabilities of the existing document security system. Table 2 shows the insiders (military officers) and document information in the military information system.

Table 2. The Example of Insiders in Military Information System

Insider	Tom	Mike	Alex
Rank	Captain	Major	Major
Role	Logistics Officer(LO)	Administration Officer(AO)	Intelligence Officer(IO)
Security level	Secret	Confidential	Secret
Document/ Role/ Security level	Event plan report/AO/Unclassified Officer information data/AO/Secret Weapons status data/LO/Confidential Intelligence analysis report/IO/Secret China cyber-warfare report/IO/Confidential		

Suppose Tom requests a 'read' mode to 'officer information' document. First, the authentication module checks whether he is a legitimate user with the user ID and password. The module then sends Tom's information and operation request to the access control module for checking whether or not he has authorization to read 'officer information' document. It rejects the request because Tom's role (LO) and 'officer information' document's role (AO) are different. It is possible to reject by access control rules and role-based access control algorithm, as presented in Table 3.

Table 3. Role-based Access Control Algorithm

```
if(user identity == user identity in database) {
        if(user-role == document-role) {
            allow(access request);
        }
        else if(user-role != document-role) {
                deny(access request);
        }
        }
else if(user identity != user identity in database) {
       deny(log on);
        }
```

Second, suppose there is an access request to 'officer information' document by Mike. An existing document security system allows access to 'officer information' document because Mike's role (AO) is the same role (AO) that could read 'officer information' document. However, our model does not allow access to the document. It checks Mike's SL (Confidential) to document's SL (Secret) by access control policy rules. Confidentiality algorithm is shown in Table 4.

Table 4. Confidentiality Algorithm

```
if(user's security level < document's security level) {
        deny(access request);
}
else if(user's security level >= document's security level) {
        allow(operation mode);
}
```

Alex frequently accesses on China's cyber-warfare document for writing intelligence analysis report recently. Our model expects that Alex operates 'read' to china cyber-warfare document and 'write' to intelligence analysis document. Thus, if Alex requests ' write mode' to China's cyber warfare, the request is rejected by pattern monitor module.

Table 5. Pattern Matching Algorithm

```
if(user's request = current user's processing pattern) {
        allow(operation mode);
}
else if(user's request != current user's processing pattern) {
        deny(access request);
}
```

Third, suppose a request to access 'China's cyber-warfare' document while working on an 'intelligence analysis' document by Alex. An access control module checks Alex's role (IO) and SL (Secret), document (china cyber-warfare, intelligence analysis) Role (IO), and SL (Confidential, Secret). It denies Alex's request by information flow control algorithm, as indicated in Table 6. If it allows access to Alex, illegal information flow occurs between the reports on China's cyber warfare and intelligence analysis. If Alex requests an operation mode to documents with different security level, the operation should be restricted to 'read' mode.

Table 6. Information Flow Control Algorithm

```
if((The number of f[] == 2) && (f[0] == f1) && (f[1] == f2)) {
        if(f1' security level == f2' security level) {
            allow((f1, f2), "read");
        }
        else if(f1' security level != f2's security level) {
                deny(access request);
        }
}
```

Finally, encrypted document is used in military, but decoding is possible if anyone has the decryption key. In addition, the documents are likely to be forged or tampered. In our model, when Tom sends 'weapons status' document to other logistics officer, a tracking module inserts his information to the document by watermarking algorithm.

5. Conclusion

We designed document security checkpoint for preventing the leakage of sensitive documents relevant to military secrets and enemy information, among others. We indicate weak points in ACL mechanism and derive security requirements for removing identified weak points. Our model allows permission to insiders when access to a requested document is related to their duty and role. The model denies an access to documents when the insider requesting an access to documents has a different security level. Moreover, the model denies an access to documents with each different security

level simultaneously and hides information of copyright and ownership in the documents by a watermarking mechanism. Our model has the benefit of preventing an insider from imposing in-depth threat to military information according to each module's functions.

References

[1] L. Holmlund, D. Mucisko, K. Kimberland and J. Freyre, "2011 Cyber Security Watch Survey", CSO magazine Publishers, **(2011)**.
[2] R. C. Brackney and P. H. Anderson, "Understanding the Insider Threat", Proceeding of a March 2004 Workshop, RAND, **(2004)**.
[3] N. Nguyen, P. Reiher and G. H. Kuenning, "Detecting insider threats by monitoring system call activity", Information Assurance Workshop on Man and Cybernetics Society, **(2003)** June, pp. 45-52.
[4] D. E. Denning, "Information Warfare and Security", Addison Wesley Publishers, **(1999)**.
[5] Y. -h. Choi, J. -h. Eom and T. -m. Chung, "An Implementation of Document DRM for Preventing Information Leakage using RBAC Approach", KSDIM, vol. 7, no. 4, **(2011)** December.
[6] J. -h. Eom, N. -u. Kim, S. -h. Kim and T. -m. Chung, "An Architecture of Document Control System for Blocking Information Leakage in Military Information System", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)** April.
[7] J. -h. Eom, "A Study on An Architecture of the Security improved Document DRM for preventing Information Leakage in Military Information System Environment", KSDIM, vol. 7, no. 1, **(2011)** March.
[8] Y. -m. Kong, H. -G. Choo and W. -Y. Kim, "Feature based Text Watermarking in Document Image", 15th workshop of imagery processing and understanding, **(2003)** January.

Author

Jung ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are information security, cyber warfare, network security.