# An Architecture of Document Control System for Blocking Information Leakage in Military Information System

Jung ho Eom, Nam uk Kim, Sung hwan Kim and Tai Myoung Chung

*Military Studies, Daejeon University, 62 Daehakro, Dong-Gu, Daejeon,*
*School of Information and Communication Engineering, Sungkyunkwan University,*
*Chunchun-dong 300,Jangan-gu, Suwon, Kyunggi-do, Republic of Korea*
*eomhun@gmail.com, {shkim, nukim}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr*

### *Abstract*

*In this paper, we architected a document control system for monitoring leakage of important documents related to military information. Our proposed system inspects all documents when they are downloaded and sent. It consists of 3 modules; authentication module, access control module and watermarking module. The authentication module checks insider information for allow to log on system. The access control module control access authorization to do operations by insiders according to their role and security level. The watermarking module is used to track transmission path of documents. The document control system controls illegal information flow by insiders and does not allow access to documents which are not related to the insider's duties.*

***Keywords:*** *Document Security, Access control, Authentication, Watermarking*

## 1. Introduction

The insider uses his legitimate authorization to perform some behavior that is contrary to the security policy, such as might be observed when sensitive information is leaked to some third party or when access to data is given or blocked. Even if the insider has legitimate authorization to the information or data, he/she uses that access to provide the information to someone who does not have access or to someone who does deny to access. And the insider uses their authorization to extend their privileges in a manner that breaks both the access control and security policies. Insider threat has occurred across all computing environments, causing severe damage to their information system and organization [1, 2].

No exception is in military information system. In military, insiders mean officers, soldiers and civilian war workers. In particular, if information including national defense policy and strategy are leaked by insiders, it is directly connected with national security.

In this paper, we architected document control system for monitoring leakage of military information by insiders in military system. Our proposed system focuses on monitoring insider's unauthorized access, operations and transmission. It monitors access to documents by the access control module, considering the roles of an insider, documents and security level. The authentication module blocks access to unclassified documents not related to insider duties.

This paper organized as follows. We describe related works in Section 2 and document control system in Section 3. We demonstrate our system by case study in Section 4, and finally conclude the paper in Section 5.

## 2. Related Works

In 2011, a foreign intelligence service swiped 24,000 computer files from a US defense contractor in one of the largest ever cyber-attacks on a Pentagon supplier [3]. 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”. He also said “It was large, 24,000 files and data-related to systems that are being developed for the Department of Defense”. “The cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs and the Joint Strike Fighter," he said. The military information leakage by insiders is increasing, and the damage is becoming serious day by day. In this paper, we focus on the leakage of military information by insiders and information confidentiality in the military information system.

The related researches for detecting insider threats have develop rapidly in recent years. The papers related to detection of insider threat are as follows.

Zhang [4] presented an active defense model and framework of insider threat detection and sense. He firstly describes the hierarchical framework which deal with insider penetration from some aspects, and subsequently show a hierarchy-mapping based insider penetrations model, the kernel of the threats detection, and sense and prediction.

Eom [5] proposed framework to defense insider threat at each layered prevention step. As processing, it defenses user-oriented malicious activities by each prevention functions. It defenses high impact on information system from insider malicious activities and mistake to be threat to critical system and sensitive data. The figure and concept of the proposed framework and functions are as following.

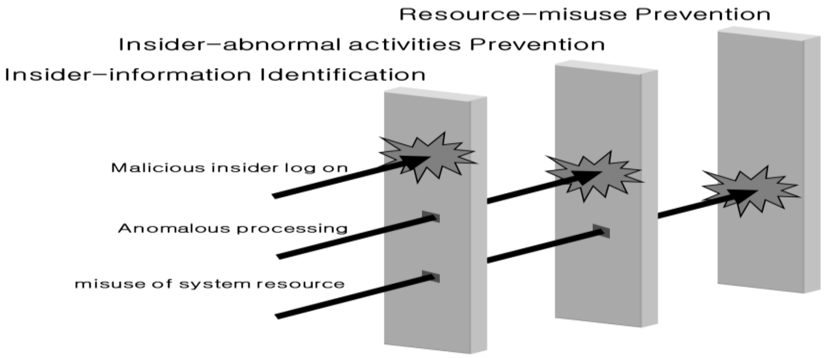
Resource–misuse Prevention
Insider–abnormal activities Prevention
Insider–information Identification
Malicious insider log on
Anomalous processing
misuse of system resource

**Figure 1. Framework of Layered Defense**

- Insider information identification: To identify whether insider is authorized or not. When insider accesses system, it checks insider information by user profile, and identifies whether he/she has security violation or not.
- Insider-abnormal activities prevention: To monitor abnormal insider behavior using attack tree. A tree structure is used represent attacks on a system, with the goal as the root node and different ways of achieving that goal as leaf nodes.
- Resource-misuse prevention: To prevent misuse system resources from insider with authorized rights as comparing insider actual process to the expected processing pattern [6]. The insider has specific patterns to execute process and resource usage related to current his task/role.

## 3. An Architecture of Document Control System

### 3.1. Security Requirements

The military information is categorized into general and classified information. General military information includes all of the administrative documents and announcements communicating in the military information system. The classified military information is divided into 'Confidential, Secret and Top Secret' based on the information's sensitiveness. Military personnel are authorized to operate military information by their security level.

As electronic documents are becoming popular, they could be assigned to specific users or group by characteristics of each document as well as a simple security level. For example, an access control list(ACL) can manage operation permission to documents by each user or group. ACL can control documents on the server, but it can't monitor document downloaded to user's PC. It also can't detect operation on two documents which has each different security level.

First, insiders should access to only documents related to their duties. In case of document DRM mechanism, the authentication module allows access to all documents if insiders are confirmed legitimate insiders. But, when administrative officer requests 'read' operation mode to 'intelligence analysis report', the existing access control system or document DRM assigns permission to him because it does not consider his duty and role. Therefore, indiscriminate access will increase the possibility of military information leakage.

Second, it must be kept confidentiality. It shall not assign permission or authorization to insiders to access documents which have higher security level than insider. If the insider performed 'read or write' operation mode to a higher security level document, confidentiality can be compromised by illegal information leakage from lower level to higher level.

Third, it should block an operation mode when insider requests to access each different security level document at the same time. If it allows 'write' mode to access 'confidential' level-document and 'secret' level-document at the same time, 'secret information is copied to confidential document.

Finally, it should verify document forgery, tampering and tracking. When cyber-military police investigates the leaked document, he can identify a leakage path of military information by checking hidden information of copyright and ownership.

### 3.2. The Design of Document Control System

We designed the document control system for blocking the leakage of military information while it meets the security requirements. Our designed model consists of 3 modules as shown Figure 2.

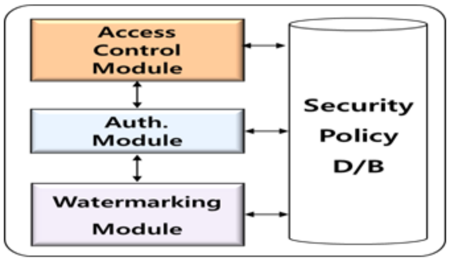

Figure 2. Design of DCS

An authentication [7] module uses user information for authenticating an insider. It checks insider's ID & password whether he is a legitimate user or not when he requests access to the system. If insider has authorization to access the system, it allows permission to the insider.

An access control module assigns authorization of operation mode to an insider according to the access control policy rules. As shown in figure 3, the access control module consists of user-role manager, permission manager, transaction manager, security level manager and authorization processor.

- User-Role Manger: activates the user-role after transmitting the user identifier information from the authentication module.
- Permission Manager: creates the information of operation authorization needed for transacting the information of document and operation mode.
- Transaction Manager: constitutes security transaction using information such as user-role, SL, authorization, etc.
- Security Level(SL) Manager: manages user SL, role SL and document SL.
- Authorization Processor: assigns operation on documents according to the security transaction generated by the transaction manager and access control policy rules.

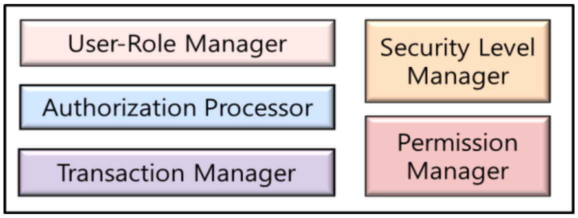

**Figure 3. Access Control Module**

A watermarking module hides information of copyright and ownership in the documents. In this paper, we use 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, word shift and character coding in technologies inserting text watermarks [8].

## 4. The Case Study

Our designed Document Control System can minimize document-based military information leakage by reducing vulnerabilities of the existing document security system in the military information system. The following table 2 shows insiders(military officers) and document information in the military information system.

**Table 1. The Example of Insiders in Military Information System**

| Officers Information | | | | | Documents/Role/SL |
|---|---|---|---|---|---|
| Unit | insider | Rank | Role | SL | |
| 00 unit | A | Major | Education Officer(EO) | Secret | Surgeon plan/MO/Unclassified<br>Officer information/MO/Secret<br>Education data/EO/Confidential<br>Intelligence analysis/IO/Secret<br>CN cyberwarfare/IO/Confidential |
| | B | Major | Medical Officer(MO) | Confidential | |
| | C | Captain | Intelligence Officer(IO) | Secret | |

Suppose insider A requests ‘read’ mode to a ‘officer information’ document. First, the authentication module performs insider authentication with the user information. Insider A can be authenticated because he is a legitimate user. And then, it sends insider A’s information and operation request to the access control module for checking whether he has authorization to read ‘officer information’ document or not. It rejects the request because insider A’s role(EO) and ‘officer information’ document’s role(MO) are different. It is possible to reject by access control rules and role based access control algorithm.

Second, suppose an access request to ‘officer information’ document by ‘insider B’. An existing security system allows access to ‘officer information’ document because insider B’s role(MO) is the same role(MO) that could read ‘officer information’ document. But our model does not allow access to the document. Our model checks insider’s SL(Confidential) to document’s SL(Secret) by access control policy rules in the database.

Third, suppose a request to access ‘china cyber-warfare’ document while working on ‘intelligence analysis’ document by insider C. An access control module checks insider C’s role(IO) and SL(Secret), document(china cyber-warfare, intelligence analysis) Role(IO) and SL(Confidential, Secret). If it allows access to insider C, illegal information flow occurs between ‘china cyber-warfare intelligence analyses. When it is an operation requested for each different security level documents, the operation should be restricted to ‘read’ mode after identifying insider’s security level.

Finally, suppose a leak of ‘intelligence analysis’ document to the third party. It is a very serious threat to the national security. Recently, encrypted document is used, but decoding is possible if anyone has the decryption key. In addition, the documents are likely to be forged or tampered. Therefore, our model hides information of copyright and ownership in the documents by watermarking module.

## 5. Conclusion

We designed document control System for blocking the leakage of important documents including military secrets from internal network to the outside. We indicate vulnerabilities in a security mechanism to apply existing ACL and derive security requirements for reducing identified vulnerabilities.

Our model allows authorization of insiders to request access to the documents related to their role and for preventing indiscriminate access to the military information. It denies to access documents when insider requests access to documents with different security level for confidentiality. It hides information of copyright and ownership in the documents by watermarking module. Our model has benefits of preventing in-depth threat to military information from insider according to each module.

## References

[1] R. C. Brackney and P. H. Anderson, “Understanding the Insider Threat”, Proceeding of a March 2004 Workshop, RAND **(2004)**.

[2] N. Nguyen, P. Reiher and G. H. Kuenning, “Detecting insider threats by monitoring system call activity”, Information Assurance Workshop on Man and Cybernetics Society, pp. 45-52, **(2003)** June.

[3] http://www.zdnet.com.

[4] H. Zhang, J. Ma, Y. Wang and Q. Pei, “An Active Defense Model and Framework of Insider Threats Detection and Sense”, IAS’09, IEEE, pp. 258-261, **(2009)**.

[5] J. Eom, M. Park, S. Park and T. Chung, “A Framework of Defense System for prevention of Insider's Malicious Behaviors”, ICACT2011, **(2011)** January.

[6] J. S. Park and S. M. Ho, “Composite Role-Based Monitoring(CRBM) for Countering Insider Threats”, ISI 2004, LNCS 3073, pp. 201-213, **(2004)**.

[7] Y.-D. Joo and Y.-H. An, "Improvements of a Dynamic ID-Based Remote User Authentication Scheme", The Journal of IWIT, Vol. 11 No. 6, **(2011)** December.

[8] Y. Kong, H.-G. Choo and W.-Y. Kim, "Feature based Text Watermarking in Document Image", 15th workshop of imagery processing and understanding, **(2003)** January.

## Authors

**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.

**Nam uk Kim** received his B.S. and M.S. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2009 and 2012, respectively. He is now currently working toward his Ph.D. in Electrical and Computer Engineering at Sungkyunkwan University. His research interests are information security, network, mobile application security, QoS (Quality of Service) and security in mobile network.

**Sung hwan Kim** received the M.S degree in Computer Science Engineering from Seoul National University, Seoul, Korea, in 2006. He is currently working toward the Ph.D. degree in the School of Information & Communication Engineering, Sungkyunkwan University, Suwon, Korea. His research interests are Cyber security, Cyber warfare and Cyber Attack Assessment.

**Tai myoung Chung** received his first B.S. degree in Electrical Engineering from Yonsei University, Korea in 1981 and his second B.S. degree in Computer Science from University of Illinois, Chicago, USA in 1984. He received his M.S. degree in Computer Engineering from University of Illinois 1987 and his Ph.D. degree in Computer Engineering from Purdue University, W. Lafayette, USA in 1995. He is currently a professor of Information and Communications Engineering at Sungkyunkwan University, Suwon, Korea. He is now a vice-chair of the Working Party on Information Security & Privacy, OECD.