Advanced Science and Technology Letters
Vol.111 (COMCOMS 2015), pp.277-281
http://dx.doi.org/10.14257/astl.2015.111.53

An Architecture of Security Enhanced Access Control System to prevent leak the internal Information

Un-Ho Lee[1] and Jung-Ho Eom[2*]

[1] #422, Kyounggi R&D Center, 105 Kwanggyo-Ro, youngtong-Gu,
Suwon-si, Republic of Korea
master@i-creative.co.kr
[2] Department of Military Studies, Daejeon University,
62 Daehakro, Dong-Gu, Daejeon-si, 300-716, Republic of Korea
[*]Corresponding Author: eomhun@gmail.com

Abstract. In this paper, we proposed an architecture of the security enhanced access control system to prevent leak the internal information in the business IT environment. Our proposed access control system added insider's contexts information, the security level of document and the level of risk to strongly control insider access to database. Insider's contexts information includes role, task, location, security level and so on. The security level of document means the sensitive level of document contents. The risk level of insider is assessed with the experience of security breaches. The proposed system was added context-aware module and user threat assessment module in existing access control system. So, the proposed system strongly controls the mode of operation (read, write, etc.) with the security level of internal information and insider, insider contexts and the risk level of insider.

Keywords: Access Control, Internal Information, Information Leakage

1 Introduction

The insider threat has emerged as one of the serious security breaches to business and government IT infrastructure. Insider threat is defined as an insider's behavior that puts at risk an organization's IT resources, data, or processes in a disruptive or legitimate(in here, it means that insider abuses his/her the right within the legal boundary) method. The insider threat is especially considered the most serious risk to database system [1]. Insiders can deliberately save data in USB memory stick and their portable disk from database system, and they can illegally use the concealed or hidden data from outside bypass the firewall, IDS and monitoring system at a later time. Malicious insiders may use their legitimate access authorization to leak sensitive data from data server. They then use their legitimate authorization to extend their privileges to break the access control rules. [2-4].

The security enhanced access control and authentication technology are developed to prevent the illegal information leakage by insider. A hierarchical access control techniques have been developed that allows an access to data through the sequential

ISSN: 2287-1233 ASTL

step in the access control techniques. Many of authentication techniques use biometric features that recognize a trait of a human being as fingerprints, hand geometry, iris and so on. Nowadays, authentication systems provide double authentication with password and smartcard or biometrics [5].

Our proposed access control system control access by 3 factors: the security level of internal information, insider's contexts and the threat level of insider. The first factor includes the content and sensitive level of internal information. The second factor includes the insider's role, task, location, and so on. The last factor is to assess behavior out of ordinary user behavior boundary with past user behavior pattern data. Our proposed mechanism allows access by a correlation analysis of the 3 factors.

In this paper, we will describe the framework of proposed system and the module and function of proposed system in section 3. We conclude in section 4.

2 The Framework of Proposed System

The proposed system consists of document control system, security management system and local system. The following figure shows the framework of the proposed access control system.

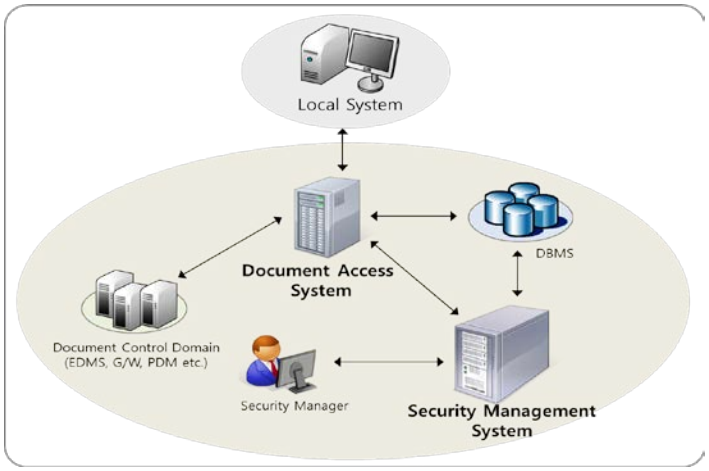

Fig. 1. The Framework of Proposed System

An document control system controls access and operation mode(read, write) to internal information according to authorization information and contexts recognition. This system includes insider authentication, the issues of contexts recognition license, the issues of security policy, DRM management module. A security management system manages electronic data upload & download, insider, authorization group, etc. This system includes some modules such as insider management, policy and authorization management, the analysis of insider's risk level, remote document destruction, export management module, etc. It also manages to process that grant authorization needed to access to internal information to insider. A local system

prevents information leakage by insider according to the security policy when insider draw up electronic document in local system or access to internal information saved in data server through the internal network.

3 The Module and Function of Proposed System

The document access system consists of the following modules. In here, we describe modules that perform the important function. The following figure shows the structure of document access system.

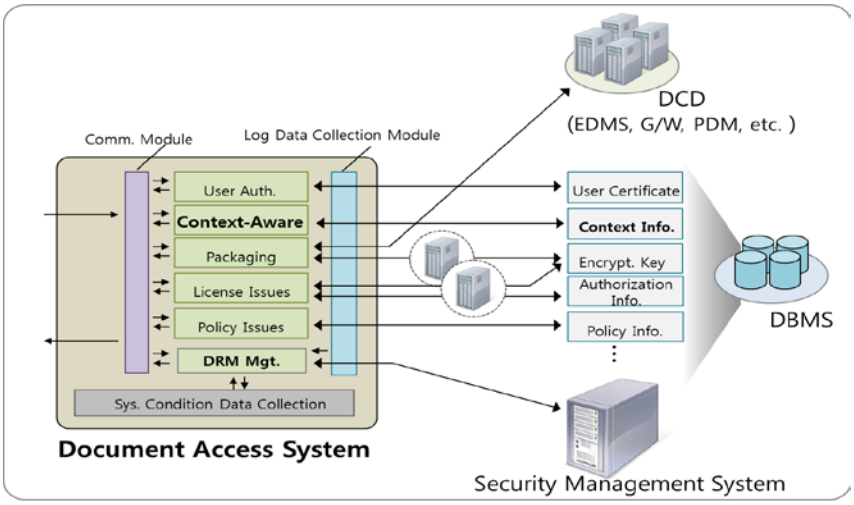

Fig. 2. The Structure of Document Access System

- User Authentication Module: Perform a password and public key based authentication for DRM user
- Context-aware Module: Determine whether access is legal or not as analyzing access location, time, path, system, etc. when insider tries to access document
- Packaging Module: apply DRM to document as encrypting the document with encryption key and attach a packaging header when local system requests download a document
- Licensing Module: Issues encryption key and access authorization information about the document when insider tries to access document applied to DRM
- Log Data Collection Module: Collect the history of the received requests and process from the local system, and delivery it to DRM management module
- DRM Management Module: Transmit log data to the document access system, delivery the information of external export detected from local system to security management system, and order the remote destruction of specific document to local system

The security management system consists of the following modules. We only explain core modules in this system. The following figure shows the structure of security management system.

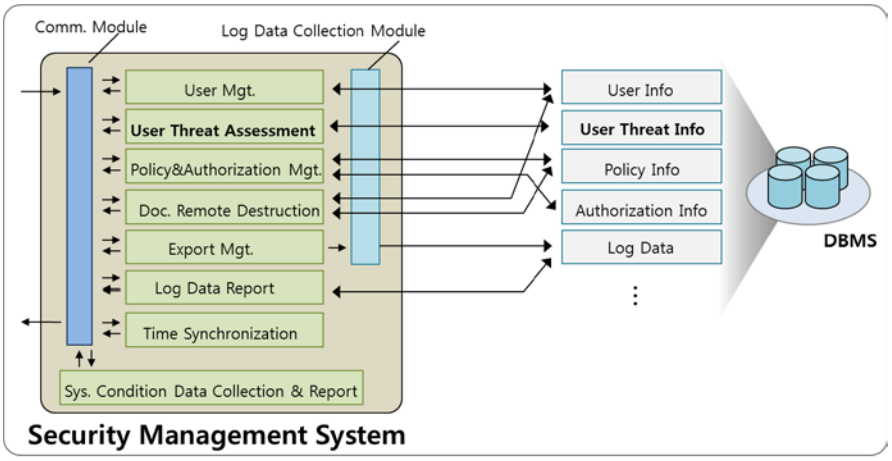

Fig. 3. The Structure of Security Management System

- User Management Module: Provide DRM user information, a document access control policy and access authorization information to security administrator
- User Threat Assessment Module: Assess behavior out of ordinary behavior boundary after recording insider's behavior pattern and define the rules of behavior pattern, when an insider performs an operation on DRM-document
- Policy and Authorization Management Module: manage access authorization according to security policies included insider's authorization to access internal information and the security level of document, etc.
- Document Remote Destruction Module: Transmit automatic destruction order on document expired DRM application period to local system
- Export Management Module: Save and manage information that detect attempts to export the DRM applied document to the external network

4 Conclusion

We proposed the scheme of security enhanced access control system to prevent leak the internal information by insider. The proposed system consists of document control system, security management system and local system. An document control system controls access and operation mode(read, write) to internal information according to authorization information and contexts recognition. A security management system manages electronic data upload & download, insider, authorization group, etc. The mechanism of proposed system was added insider's contexts information, the threat level of insider behavior and the security level of document as assessment factor to grant access authorization. So, the proposed system firstly controls access to database

by first authorization checking factors(for example, ID and password) and approve of operation mode to internal information by added authorization checking factors.

References

1. S. L. Pfleeger, Joel B. Predd, Jeffrey Hunker, and Carla Bulford: Insiders Behaving Badly: Addressing Bad Actors and Their Actions, IEEE Transactions on Information forensics and Security, Vol 5, No.1, pp.169-179 (2010)
2. Imad M. Abbadi, Muntaha Alawneh: Preventing Insider Information Leakage for Enterprises In : The 2nd International Conference on Emerging Security Information, Systems and Technologies, pp.99-106, (2008)
3. Jung-Ho Eom et al: Analysis of Insider Access Pattern for Monitoring Misuse in the DCD, International Journal of Security and Its Applications, Vol.8, No.3, pp.431-440 (2013)
4. Jung-Ho Eom et al: An Application of Data Leakage Prevention System based on Biometrics Signals Recognition Technology, Proceedings of 3rd International Conference on Networking and Technology, ASTL, Vol.63, pp.1-5 (2014)
5. Jung-Ho Eom: The Design of Robust Authentication Mechanism using User's Biometrics Signals, International Journal of Security and Its Applications, Vol.8, No.6, pp.71-80 (2014)

