Design and Implementation of Document Access Control Model Based on Role and Security Policy*

Liangjian Mao¹, Shuzhen Yao², Kai Zhang², and Kouichi Sakurai¹

¹ Department of Informatics, Kyushu University, Fukuoka 812-0053, Japan  
² School of Software, BeiHang University, Beijing 100191, China

Abstract. To design a method of document access control with flexibility, generality and fine-granularity, we establish a document access control model, which is an abstract description for general scene of document access. Security policies are presented to describe security constraints, so as to meet security requirements of this model. In order to demonstrate the theories and strategies more intuitively, we design a prototype system of document access control based on XACML-RBAC framework to verify the validity of model and algorithms and the feasibility of mechanism. It realizes the authorization protection of the standard OFFICE documents.

Keywords: Document Protection, Document Access Control, Security Policy, Information Flow, XACML-RBAC.

1 Introduction

1.1 Background and Motivation

Due to the electronic document’s characteristics of convenience to copy, modify and transfer, serious problems such as sensitive information disclosure might be caused. Therefore, the research on the protection of important document has been the hotspot of information security.

The existing mechanisms have some limitations on the functionality, expandability and granularity of access control. One important problem is that they don’t support security policy quite well. When there are a large number of documents in the organization to protect, the privilege management may cause confusion or even security problem. This paper aims to create a Document Access Control Model, on the model base, using the document protection mechanism to implement authorization protection to documents.

1.2 Previous Works

The current document protection technique can be achieved mainly through file encryption, file format conversion and the control of peripherals as well as

* This paper is supported by the National Defense Basic Scientific Research Program of China under grant No. A2120061061, which was accomplished in Software Engineering Institute of BeiHang University.
network protocols [1]. For instance, Microsoft Word and Adobe Acrobat implement their security mechanisms through security passwords, digital signatures and other methods. The WaterBox 7.2 system achieves document protection through limiting the use of some external devices and controlling the network protocol. The Cobra DocGuard system implements it through transforming documents which is in need of protection into other formats. The TotalFileGuard system utilizes transparent encryption and decryption. However, those document protection technologies have some limitations: file encryption and digital signature require users to have high security awareness and technical level, the method of file format conversion needs to use a specific reader and will change the using habits of users. Those technologies also lack the support of access control strategy.

Lzaki and Tanaka [2] present an access control model for the object-based systems, and discuss how to control information flow through roles. But not refer to objects protection. Objects in the model are instances of the class, which are created with attribute values of the class.

Security policies such as Suranj\text{an} and Vidyaraman provide the Document Control Domain (DCD) [3]. It can defense against insider abuse based on the principles of "least privilege and minimum requirements". But it can't satisfy the security requirements of complex system. Specially, Dynamic Security Rules can enforce more specific and finer-grained controls of user's operation actions. Besides, security policies are enforced according to user's role in system.

Microsoft Exchange 2010 delivers new, integrated e-mail archiving and retention functionality. RBAC [4] is a new permission model in Exchange 2010. But it cannot protect documents. Rights Management Services [5] is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use. but it neither supports access control strategy nor assigns roles to different users. If a user copies the content of some document into another current open one, RMS can't monitor the illegal information flow.

Alban and Patrick [6] showed how to model dynamic security rules based on spatial contexts. They use these spatial contexts to write security policies for spatial applications, but not for dynamically controlling user's operation and preventing hidden divulge of document information. we use a method based on analysis of information flow to implement creating Dynamic Security Rules.so as to find out the potential approach that leads the leak of information.

1.3 Challenging Issues

In order to protect documents and sensitive information, we implement a document control model, focusing on the following challenging issues:

The major challenge is how to establish corresponding security policies according to security requirements. So we need to analyze security requirements firstly, and then discuss implementation of consistency of model state.

Secondly, how to assign roles to different users, and define security constraints such as role separation of duty, times of role activation and role dependencies.

How to create Dynamic Security Rules is an important issue. It can monitor user's operations on document in different environment and find out the possible path of information disclosure.