Security in PKI/PMI-Based Workflow Security Model[*]

Zhiqi Xu
School of Computer Science and Information
Guizhou University
Guiyang, China
xorangeu@163.com

Chaohui Jiang
School of Computer Science and Information
Guizhou University
Guiyang, China
jiangchaohui@126.com

***Abstract* - In consideration of simple workflow security model, there are some defects such as simple authentication, inflexible authorization and absent of audit, etc. However, based on the intensive research of security needs of WfMS, and by involving PKI/PMI technology, an enhanced workflow security model can be a viable choice. This model introduces strong factor authentication by utilizing PKI, T&RBAC access control by utilizing PMI and by utilizing digital signature and DTS to provide non-repudiation and existing services. The requirements of security audit also can be satisfied well. Comparing with simple workflow security model, theory study shows this PKI/PMI-based model improves the safety and flexibility significantly. A convenient and reliable solution for Data Privacy, Data Integrity, data Availability and Non Repudiation is adjusted to the requirements of workflow. The risks from illegal and unauthorized operations are reduced to minimum.**

Keywords-component: Workflow; Security Model; PKI; PMI; Audit.

I. INTRODUCTION

Along with the rapid development of information technology, particularly the widespread applications of E-government, there will be more and more workflow-based applications. For example: Office Automation System and E-Business System. These systems raise the level of information sharing and people's working efficiency greatly and by dividing into well-defined workflow activities such as tasks, roles, policies and processes to accomplish the operations and monitoring, workflow can achieve greater levels of production and work efficiency But the security problem also appeared with it. In general, workflow management system (WfMS) involves multiple departments, and existing heterogeneous application systems are interlaced, especially the web-based distribute WfMS spans greater. Therefore, how to ensure the security of WfMS have become prominent issues.

According to the *Workflow Management Coalition's (WfMC) specification Workflow Security Considerations - White Paper*, basic security issues which existing in the current WfMS include [1]: authentication, authorization, access control, audit, data privacy, data integrity, non-repudiation and security management & administration. Public Key Infrastructure (PKI) and Privilege Management Infrastruc-ture (PMI) are available solutions of information security technology for network security. So integrating with workflow, they can improve the security of the WfMS prominently. By analyzing the simple workflow security model in depth and taking advantages of PKI/PMI-based security platform, a PKI/PMI-based security workflow model has been proposed, which can meet the varieties of workflow-based application systems security requirements.

II. OVERVIEW OF PKI&PMI

PKI is a key management platform which following established standards for all web-based applications. It provides a collection of security services [2]: encryption, decryption, digital signatures and other cryptographic services. In X.509 standard, PKI includes four important parts: digital certificate, CA (Certification Authority) operation agreement, CA management agreements and policies. User's identity information and the public/secret keys are preserved in digital certificates/PKC.

PMI depends on the support of PKI. Its chief purpose is to provide access control and privilege management services. Providing mapping function from user identity to the application, and to achieve independent of the access control mechanism with the specific application and administration is another function of PMI. It simplifies the complexity of access control and makes the development and maintenance of privilege management systems easier. PMI is a license-based technology. The core is resource management and gives the authorized institutions access control of resources to manage. That is to say, resource owners control visitors' privilege. Similar to PKI, user's privilege information is stored in attribute certificates (AC).

III. SIMPLE WORKFLOW SECURITY MODEL

In Reference [3], *John A*, *Miller* had proposed simple workflow security model on the basis of aiming at security problems and solutions of WfMS (Shown in Figure 1).

This security model mainly integrates with Login Agent, Security Agent, Task Manager, Security Database and Applica-tion Database. Security Agent and Security Database are the most important parts for this security model. Both the Login Agent and Task Manager will consult the Security Agent before making permissions. No other access to the Security Database is allowed. There are

[*] This work is partially supported by Science & Technology Project in Guiyang City, Guizhou Province, PRC Grant # ZHU KE GONG 2009-1-051.

two main functions for Security Database: one is role-based access control (RBAC), the other is key management.

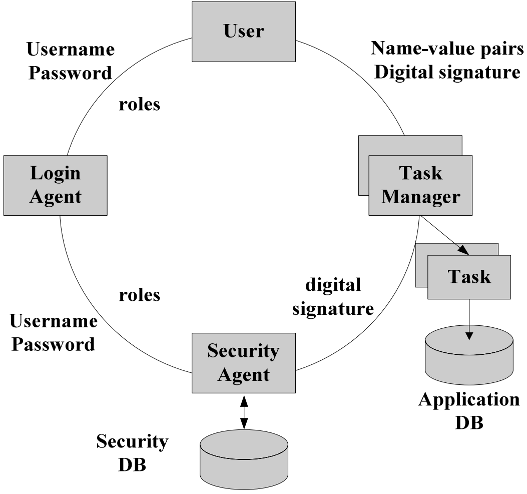

Fig. 1 Simple Workflow Security Model

This security model aims to combine with message encryption, digital signature, RBAC in WfMS effectively. The login process describes as below: first, user logins the WfMS; second, selects a role with the help of Security Agent; third, executes role-based operations (doing what this role is authorized to do). Task Manager will be invoked in this process for authorization though Security Agent. For safety's sake, secure communication is required for all the information exchanges in WfMS.

A. Defects in Simple Workflow Security Model

- Impersonation

In simple workflow security model, Login and Authentica-tion systems use simple factor authentication (username + password) way, which is too weak to intruder.

- Information Leakage

Although WfMC recommends strongly using secure communication channel, most information exchanging in internal network of enterprises is plaintext. That makes attack from inside easier.

- Data Integrity and Non-Repudiation

Because of deficient in audit and verification, it is hard to make sure data integrity between sender and receiver. Even more, it is difficult to make both sides trust the arbitration when disputes arise.

- Defects in Security Database

Security Agent is the only way to access Security Database. That sounds like good news, but for distributed and web-based WfMS, it brings more disadvantages than advantages. Its complex network structure, multi-users business applications and dispersed distribution lead to the security of the database-based authentication and authorization management system complexity and confusion. Attackers may get more opportunities.

- Defects in Role-Based Access Control

RBAC is used to determine what role a subject may perform. The role then determines which tasks a user can execute. But in WfMS, access control mechanism has its own features. First, authorization must walk in step with the current tasks. In other words, when a task starts, user is given the minimum permissions to complete the task, after the task ends, permission is withdrawn immediately. Second, getting and withdrawing permissions are task-driven and automatically. Generally speaking, current task depends on the result of previous. Authorization must be consistent with the sequence of tasks. Third, authorization management must be context-sensitive and timeliness.

In workflow, the stronger of task concept, the higher requirements for access control. So, when the traditional RBAC model applies to WfMS, there are two obvious defects: insufficient dynamic adaptation and short in constraints of privilege [4].

IV. PKI/PMI-BASED WORKFLOW SECURITY MODEL

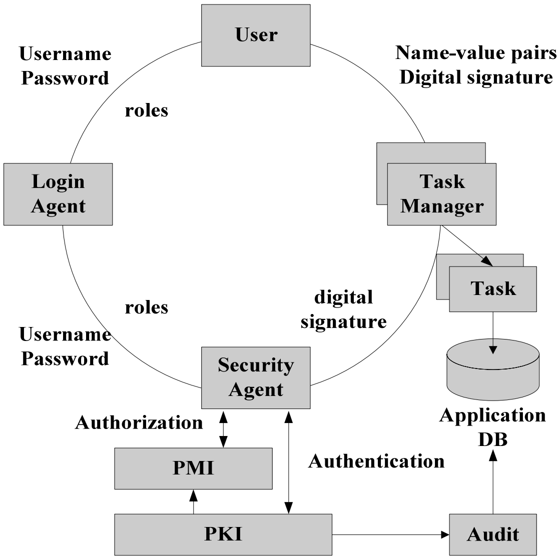

Fig. 2 PKI/PMI-based Workflow Security Model

Comparing with simple workflow security model, PKI/PMI-based workflow security model improves the security of authentication and authorization processes and modifies the policies of access control, adds the security audit module, replaces Security Database with PKI/PMI module. These measures can enhance the security in WfMS effectively. (Shown in Figure 2)

A. PKI/PMI-Based Authentication & Authorization Process

The model does not describe the implementation of PKI and PMI specifically, and assuming that the user already has the secret & public key certificates from PKI and the attribute certificate is issued by PMI which corresponding to PKC. The process of authentication and authorization in WfMS as follow: (Shown in Figure 3).

Step 1. User submits username and password together with PKC to Security Agent through Login Agent.

Step 2. Security Agent verifies User's PKC whether corresponding to who he really is by PKI.

Step 3. When User passes the authentication, attribute certificate is submitted to Security Agent.

Step 4. Security Agent verifies User's AC by PMI.

Step 5. PMI extracts role (privilege) information from AC after verifying successfully.

Step 6. WfMS authorizes user appropriate permission according to the current task strategy and role privilege.

Step 7. User's authentication and authorization completes successfully.

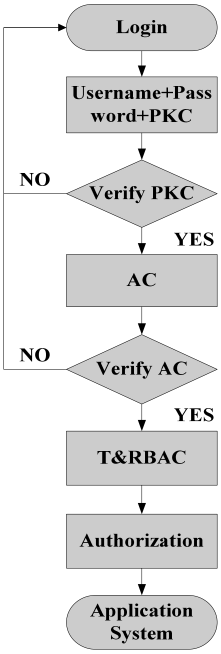

Fig. 3 Process of Authentication & Authorization

B. Improved PMI Authorization Policy – T&RBAC

Traditional RBAC is role-based strategy, organizational structure can be mapped the way to set security policies. It includes five basic elements: User, Role, Object, Operation, and Permission. The Task & Role-Based Access Control (T&RBAC) is based on RBAC and adds Task element. It's more suitable for WfMS environments. (Shown in Figure 4)

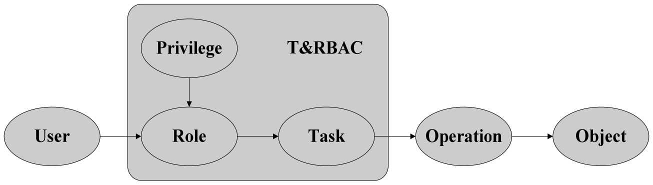

Fig. 4 T&RBAC Model

PMI plays an important role in the workflow access control policies. PMI-based RBAC access control policies [5] include following sub- policies:

1) Subject Policy: Subject is a collection of same privilege (role) users. By operation on subject, we can change and authorize privileges for users.

2) Role Assignment policy: Role assignment shows a list of roles which users can choose. It can be expressed as a pair (Subject, Role).

3) Object Access Policy: Object access policy is to determine which privileges a role has. It can be expressed as a pair (Role, Privilege-List). Privilege List also can be expressed as a pair (Object, Operation-List).

4) Operation Policy: Operation is a set of activities what users can do to the object.

5) Role Hierarchy Policy: Role hierarchy policy defines the relationship between different roles.

6) Source of Authority Policy: Source of authority (SOA) policy defines the trust source of institutions. (credibility institutions which issue AC).

For T&RBAC, it adds two extra new policies on the basis of PMI-based RBAC:

1) Task-based Role Policy: Task-based role policy shows what tasks the role can execute. It can be expressed as a pair (Role, Task).

2) Task-based Privilege Policy: Task-based privilege policy is to determine what privileges a task can have. It can be expressed as a pair (Task, Privilege).

C. Process of Audit

PKI/PMI-based workflow security model introduces security audit module comparing with simple workflow security model. Security audit module is used to provide data integrity service and non-repudiation service. It also records users' activities and operations into audit database automatically to meet security requirements. The process of security audit as following: (Shown in Figure 5)

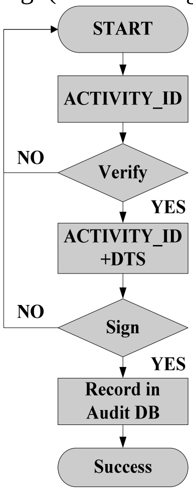

Fig. 5 Process of Audit

Step 1. The operation/activity ID will be submitted to WfMS after user taking an operation.

Step 2. Authentication and verification will be active by PKI and PMI.

Step 3. When user pass the step 2, Digital Time Stamp (DTS) and operation ID will be sent back to user from system automatically.

Step 4. User signs the data from step 3 to generate a digital signature [6] by PKI.

Step 5. WfMS keeps the digital signature into audit database if the verification of digital signature is successful.

Step 6. The process of users' operation complete successfully.

V. Performance Analysis Of Pki/Pmi-Based Workflow Security Model

A. Analysis of Security

By using PKI/PMI technology, PKI/PMI-based workflow security model improves the security of WfMS greatly. It can supply many kinds of security services as below:

- Digital certificate-based strong factor authentication method authenticates users' ID.
- Using message encryption technology ensures data confidentiality during transmission.
- Providing data integrity service through verifying the message digests.
- Non-repudiation service is offered by using digital signature.
- With digital time stamp service, it ensures the existence of data and operations.

B. Analysis of Flexibility

The improved T&RBAC [7] model can make up defects which existing in Discretionary Access Control (DAC), Access Control List (ACL), Mandatory Access Control (MAC) and RBAC model. It can achieve following objects for access control:

- Non-authorization operation can be avoided as much as possible by PKI-based PMI technology.
- With T&RBAC access control policy, authorization for WfMS is much more flexible and safer.
- By using AC of PMI, it reduces the administrators' amount of work effectively and decreases mistakes by administrators.

C. Analysis of Impartiality and Authority

PKI/PMI-based [8] workflow security model contains non-repudiation and digital time stamp services by using security audit module. Ticket Granting Ticket (TGT) (e.g. digital signature, digital time stamp) which generates in this model can be trusted by both sides. So it can achieve fair and impartial, decreasing most disputes to minimum.

V. Conclusions

For workflow to be useful in some domains in which high security is essential. This paper discusses how to combine PKI/PMI technology with WfMS to enhance system's security. PKI/PMI-based workflow security model can achieve the requirements of authentication, authorization, access control, audit, data availability, data privacy, data integrity and non repudiation in WfMS. The paper further considers combination of T&RBAC for access control service. It reduces security threats to minimum such as information leakage, data modification, access refuse, unauthorized operation, forgery, bypass control, etc.

Workflow's security is directly related to the security of the whole WfMS. So construction a safety workflow is very necessary. Only in the foundation of workflow with high security, all kinds of application systems which depend on it can guarantee safe during sharing and transmitting information among different departments. It is highly significant to promote the efficiency of E-Commerce & E-Government, protect valuable information and upgrade the level of security Management & Administration.

References

[1] WFMC-TC-0021019. "Workflow Management Coalition Work-flow Security Considerations White Paper". http:// www.wfmc.org/, Feb 1998

[2] M. Markovic, "Data Protection Techniques, Cryptographic Protocols and PKI Systems in Modern Computer Networks", *Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. 14th International Workshop*, pp: 13-24, doi: 10.1109/IWSSIP.2007.4381086

[3] John A.Miller, Mei Fan, Amit P.Sheth, et. "Security in Web-Based Workflow Management Systems". http:// LSD- IS.cs.uga.edu/, 1997

[4] Ravi S.Sandhu, Edward J Coyne,Hal L.Feinsten, et al. "Role-Based Access Control Models". *IEEE Computer* Volume 29 Num2，2000

[5] WU Li-jun, SU Kai-le, YANG Zhi-hui. "A Role-Based PMI Security Model for E-Government". *Wuhan University Journal of Natural Sciences*，2005.10

[6] W.Ford, M.S.Baum, "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption", Second Edition, Prentice Hall PTR, Upper Saddle River, NJ 07458, 2001.

[7] Li Zhang; Lili Luo; Liyong Zhang, etc. "Task-Role-Based Access Control in Application on MIS", *Services Computing, 2006. APSCC '06. IEEE Asia-Pacific Conference*. pp: 153-159, doi: 10.1109/APSCC.2006.96

[8] Sharon Boeyen.X.509 4th edition: Overview of PKI & PMI Frameworks (Entrust Inc.) http://www.entrust.com/resources/pdf/509_overview.pdf，2000.