Security Middleware Framework of Classified Application System

Yizheng Tao, Xinglan Li*, Shan Gao and Gongliang Li
Institute of Computer Application on China Academy of Engineering Physics, MianYang, China
*Corresponding author

***Abstract*—For classified applications need to quickly adapt to the business and security policy change, using middleware technology and framework, abstract classified application system security common public features, put forward the classified application business logic and security logic separation of security middleware framework, and construct the classified application system security framework prototype, and verified by multiple classified applications show that application of classified security middleware framework based on public security interface and dynamic allocation strategy module, which can achieve the requirement of the application of classified grading protection system, able to quickly respond to business and security policy changes.**

Keywords-classified application system; grading protection; authorization management; security middleware framework

I. INTRODUCTION

Application systems are increasingly becoming an important party and government departments and military units research and production activities, the main carrier of the soul and the management and administrative activities, a steady increase in its size and complexity, these units with the deepening of information technology, supporting scientific research, model development , manufacturing, technical condition, test & experiments and collaborative management systems and other business applications more and more, the increasing size and complexity, and closely with the research and production business unit, management processes of integration, becoming operational support units, carrier soul and life development. With the continuous increase in the size and complexity of application systems, application systems can not quickly adapt to business changes and application and data security and security policy is a major key issues constraining the rapid development of application systems and applications.

Application system is usually involve large amounts of complex data manipulation, storage, and processing of these data and automate business processes, and access control rules and security policies. Its notable features include:

1) relates generally persistent and database storage of data;
2) involve large amounts of data, a medium-sized systems often contain several GB or more of data, database-recording store;
3) relates in general large numbers of people (thousands) concurrent access to data and security requirements;
4) involves a large number of operational data user interface screen;
5) the application system to meet national classification protection requirements[1-2]

II. COMMON SECURITY AND CONFIDENTIALITY REQUIREMENTS

A. *Division of Authority*

Application of the division of authority, including management roles and permissions, user account authorization granularity of control in two ways, Security requirements for management roles and permissions include:

a) "three" different security management roles and their corresponding user accounts;

b) "three" user rights should be independent of each other, mutual restraint, the corresponding user account authority shall satisfy the following work requirements: 1) the daily operation of the system administrator responsible for system maintenance, including user to add / delete user state management; 2) security and confidentiality of the system administrator is responsible for the daily security management, including user permissions management, policy settings;3) security auditors are responsible for important operating system administrators, security and confidentiality of the operating behavior and system administrator's user review of the anomalies can be found in the audit trail analysis;

c) "three" operating in the system should generate audit records. Granular control of user accounts authorization in accordance with the requirements of the principle of minimizing the authorization of user account privileges for fine-grained control.

B. *Confidentiality Identified*

Dense security requirements identified include:

a) shall provide mandatory security classification marking function of the information generated by setting the appropriate security classification identification;

b) an electronic identification should be dense and message body can not be separated and must not be tampered with;

c) if the issues related to technical conditions restrictions can not be achieved b) requires the system to deal with the security classification identifies modify operation generates audit records.

C. Authentication

Authentication including user ID(identification), user authentication, identification and re-identification of treatment failure, etc.,

1) User ID requirements, security requirements for user IDs include: a) User ID generated by the system administrator unity; b) shall ensure that the user ID in the system life cycle is unique, when a user account is deleted, its identity no longer be used; c) the user ID security audit events should be associated with the system to ensure the verifiability of security incidents; d) maintenance of administrative user ID is subject to authorization, to ensure that the user ID file from unauthorized access, modification or deleted.

2) requires user authentication, user authentication security requirements, including: user authentication a) application login should be based on unified digital certificate authentication system; b) ensure that all users have access to the identity authentication, user authentication mechanism can not be bypassed; c) user authentication information should not be visible, user authentication information storage and transmission of passwords should take protective measures.

3) Identification of failure handling requirements, when the user authentication failed attempts in a row up to 5 times, the system should be carried out the following process: a) lock allows the user to try up to 30 min after the account, or restored by the system administrator; b) forming audit events and alarms.

4) re-identification requirements, user authentication is successful, the operation when its idle time more than 10 min, the system respond to user re-authentication.

D. Access Control

Access control including access control policy and access control granularity, information security is an essential part of the application.

1) Access control policy requirements, in accordance with national needs and BMB 17-2006 8.3.2, according to the main categories, object class mandatory access control information.

2) Access control granularity Access control requirements should include: a) the system user ID file, list of user rights and other operations, the implementation of mandatory access control; b) operation of the audit event mandatory access control; c) according to the minimum principle of delegation were awarded the "Three members' commitment to complete the tasks required minimum permissions and "between the three," the formation of mutual checks and balances. At the same time, the need for enhanced access control requirements, subject information and important information control to a single user, to control object information category.

E. Input/Output Control

Input/Output control functional requirements shall include: a) application of the system of business-related electronic data input/output should be subject to authorization and control to the user, the input authorization operations and electronic data / output operations should generate audit records; b) application system file printout should be controlled to the user and the file type, file, and print authorized to operate output operations should generate audit records.

F. Information Exchange Control

Information exchange between applications (send / receive), should be controlled to the user and the file type, authorizing the operation and information exchange operation should generate audit records.

G. Security Audit

Security Audit feature requirements include: the design should be authentication, access control and other security features designed to. a) security audit function and closely integrated; b) audit events to be associated with a unique user identity association; c) provides basic security audit event entry table , you can choose to configure; d) the user can customize the security audit events. At the same time, enhancement requests, on the basis of satisfying the above requirements, the offer allows users to customize different specific audit findings responds function.

Audit scope requirements, application system following events should generate an audit record: a) Start the system on / off; start b) audit function on/off; c) the user add/delete users permission to change the user status changes, auditing configuration change; d) All users of the authentication event; e) system data input/output authority operation, the data input / output operations; f) authorized to operate inter-application system of information exchange, information exchange operation; g) "three" other important operating and user operation; h) other events and security-related applications or specifically defined auditable events. Meanwhile, enhancement requests on the basis of satisfying the above requirements, the audit record query, backup, delete and other operations to generate audit records.

Content requires audit records, audit records include: a) audit records audit events should include the time, place and event type, subject, object, and the result (success/failure) and other information; time b) audit records generated by the environment in which the application system uniquely determined clock generation.

Audit records protection requirements, audit records protection requirements include: a) providing an audit record storage space setting function, enter audit storage space will be full processing capabilities, audit log I/O functions, by an authorized user configuration and operation; b) audit storage space will be filled in time when an alarm; c) should be able to prevent modifications to the audit records, forgery and unauthorized deletion. At the same time, enhancement requests, on the basis of satisfying the above requirements, the audit storage space is full, Auto save audit data or overwrite the oldest audit data.

Audit records access request, the audit record lookup functionality requirements include: a) Check out audit records subject to authorization; b) to authorized users audit records check, classification, sorting and other functions; c) provide supporting statistics audit data analysis for an authorized user Features. Meanwhile, enhancement requests on the basis of satisfying the above requirements, the audit information should also have the ability to generate statistical reports.

H. *Other Common Requirements*

Other security applications common requirements: including backup and recovery, information integrity protection, operating system security, database security, and its own security systems and other requirements.

III. SECURITY MIDDLEWARE FRAMEWORK OF APPLICATION SYSTEM

Based on large-scale study of the characteristics of complex applications and information systems classified protection requirements, based on the basis of "Java EE component-based development platform,"[3-5], the use of object-oriented, aspect-oriented and component-based development methods, design hierarchical, modular reusable application security middleware architecture. And the specific content of each module of the security member comprises, between the carding layer, multiplexing between the modules, and defines the interfaces between them. Operational responsibilities in accordance with the law of the hierarchical decomposition, application security middleware framework as shown in Figure 1, From the bottom can be divided into three layers: security service providers, application security middleware layer (application system generality Security Abstract), application layer.

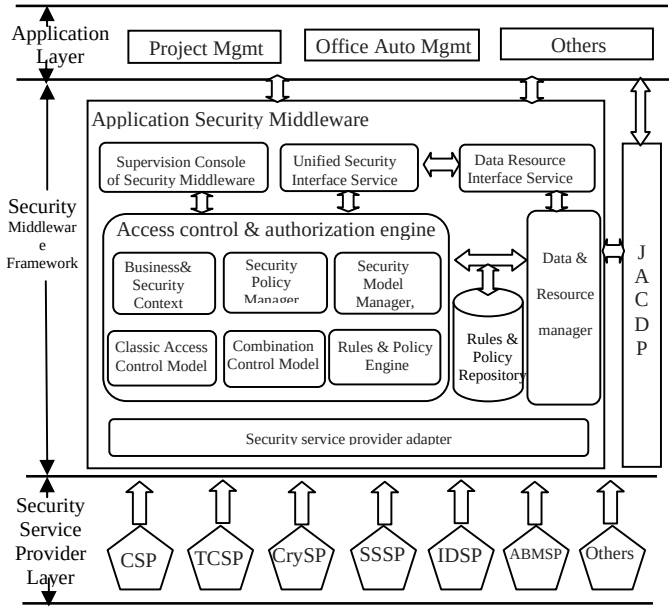

FIGURE I. APPLICATION SECURITY MIDDLEWARE FRAMEWORK

Abbreviation is described as follows in Figure I.

CSP: Certificate Service Provider.

TCSP: Trusted Computing Service Provider.

CrySP: Cryptographic Service Provider.

SSSP: Secure Storage Service provider.

IDSP: Invasion perception and active Defense Service Provider.

ABMSP: Abnormal Behavior Mining Service Provider.

Application of health service providers.

JACDP: Java EE Component-based software Development Platform.

Security Service Provider Layer: security services package a variety of existing security service providers, such as certificate services, PKI/CA certification services, trusted computing services, encryption services, storage security services, intrusion perception and active defense services, users abnormal behavior mining services, the layer has a very versatile and can be another layer of unified security services provided by an intermediate layer of application security to provide direct service multiplexing, or interfaces to provide services, shielding the underlying technical complexity.

Application security middleware layer: integration of various classical, popular access control model[4-5] (such as RBAC, DAC, MAC, ABAC, TMAC, etc.) and authorization management and research projects combined access control model and resource management server application, the layer is the main contents of this research project, the layer from bottom to top in turn are divided into security service provider interface layer, access control and authorization management engine layer, service layer interfaces.

Application level: complex application systems for large-scale business, "Java EE component-based development platform," based on the use of various security services provide security middleware applications developed to meet a variety of applications classified protection requirements.

IV. APPLICATION SECURITY VERIFICATION

Application security middleware framework of this study, the application of technology to build Java EE middleware framework prototype, combined with Java EE component-based software support platform [3-5], has been in research management, model management system, fund management system units, OA office management system has been preliminary application, middleware, security policy management framework, roles and user roles effect interface shown below Figure III.

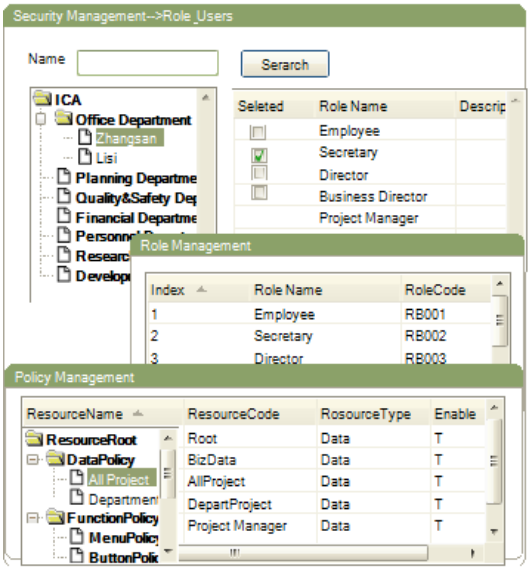

FIGURE II. SECURITY MIDDLEWARE FRAMEWORK APPLICATION EFFECT

Application System dynamic security policy configuration and test results as shown below Figure III

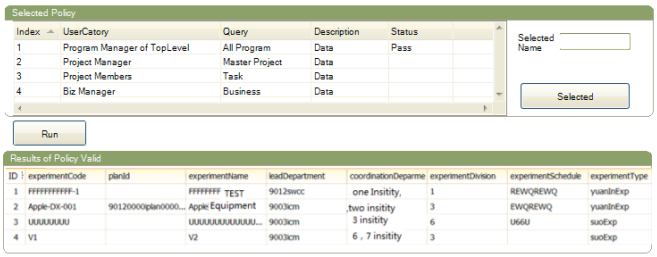

FIGURE III. DYNAMIC POLICY CONFIGURATION

After a preliminary application verification, application security middleware framework enables application logic and rights management systems business logic separation and decoupling, rule-based rights policy dynamically configurable, enabling fine-grained data level dynamic access control; and be able to implement preliminary permission logic changes without modifying the code rights management, rights management to improve the reusability and improve the efficiency of information systems development, adapt quickly to changes in business and security policies.

V. CONCLUSION

In order to respond quickly to business applications and security policy changes, based on Java EE development platform, application systems for public security and confidentiality of common features, build application business logic and security logic separate security middleware framework, defined the framework composition structure, and established a prototype middleware framework to achieve the application business logic and security logic separation and decoupling, dynamic rule-based security policy can be configured to achieve a fine-grained level dynamic data access control; application shows, it is possible to achieve a preliminary permission logic changes without modifying the code rights management, rights management to improve the reusability, improve efficiency and develop strategies to adapt quickly to changes in business and security applications.

ACKNOWLEDGEMENTS

The research work was supported by high CNC machine tools manufacturing equipment, No 2013ZX04006011.

REFERENCES

[1] BMB17-2006, involving state secrets information systems graded protection technical requirements, the State Secrecy Bureau, 2006

[2] Martin Flower with, Huaimin, Zhou Bin translated. Patterns of Enterprise Application Architecture (Enterprise Architecture Model) [M], Machinery Industry Press, 2010.4

[3] Yizheng Tao, Zhijie Wu, etc., based on J2EE Web application presentation layer architecture research [J], Computer Application Research, 2005-12-30,2005 supplement 660-661

[4] Yizheng Tao, Wu Zhijie, Tang Dingyong like J2EE-based software support platform component technology research [J], Computer Engineering and Design, 2009,30 (14): 3326-3330

[5] Yizheng Tao, Xinglan Li, Guanghong, Yang Shan Gao, Permission Management Middleware Research of Oriented Information System, 2014 International Conference on Information Management and Management Engineering (IMME 2014): 59-67