A RECONFIGURABLE SECURITY MANAGEMENT SYSTEM WITH SERVICE ORIENTED ARCHITECTURE

Ing-Yi Chen and Chao-Chi Huang
Department of Computer Science and Information Engineering
National Taipei University of Technology, Taipei, Taiwan, 106, ROC

Keywords: Service Oriented Architecture, Information Security Management System, Service-Oriented Software Engineering.

Abstract: This paper proposes an Information Security Management System (ISMS), which is essentially a service-oriented mechanism. The system supports distributed process changes in run-time and as needed. In addition, this study uses a Service-Oriented Software Engineering (SOSE) development methodology for designing and building a Service Oriented Architecture (SOA) ISMS. These features represent significant improvements upon existing systems because, they allow for a dramatic increase in the ease and efficiency with which system modification can occur. They also allow for the reuse of existing services and their recombination, either with other existing services, or with new software, in order to create new processes. The features afforded by this system hold tremendous potential for use within a range of industries and organizations, especially those that seek to provide on-line services to their customers or product users.

1 INTRODUCTION

Increasing attention is being given to Information Security (Wade H, 2007) as network technologies and infrastructures rapidly develop. Many organizations, such as schools, manufacture industries and so on, are looking for a consolidated security approach to better manage business information services.

Information security protects information and network systems from various kinds of threats and enables them to run continuously. Hence, careful consideration is given to information security mechanisms when building and constructing information systems, to increase robustness.

To achieve this goal, the information security market consists of a complex mix of platforms and services (Chin-Chen Chang, 2003) that provide two related but very different types of functional capabilities. The relationship is illustrated in Fig. 1.

In the following representation (Fig.1), information security services imply a comprehensive approach, encompassing a complete set of lifecycle services for designing, building, integrating, managing, and evolving sound security solutions.

The other part in the Figure 1 is the information security management platforms, which are the systems of management concerned with information security. ISO27001:2005 are standardized methodologies, and represent internationally accepted "best practices" for designing and measuring information security platforms. Security architectures that employ these methodologies are divided into five operational categories: (1) Auditing, (2) Access control, (3)Flow control, (4)Identification and credentials, and (5)Solution integrity.

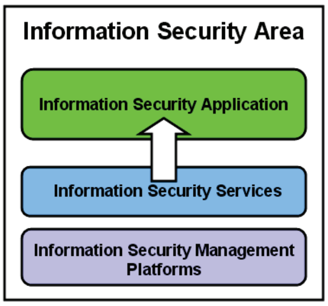

Information Security Area
Information Security Application
Information Security Services
Information Security Management Platforms

Figure 1: The structure of information security.

These five subsystems can be meshed together, so they work interactively with each other, in an

Chen I. and Huang C. (2008).
A RECONFIGURABLE SECURITY MANAGEMENT SYSTEM WITH SERVICE ORIENTED ARCHITECTURE.
In *Proceedings of the Tenth International Conference on Enterprise Information Systems - ISAS*, pages 357-362
DOI: 10.5220/0001716903570362

information security management system. In these subsystems, access control plays an important role.

Even when solutions (Sanchez, 2007) (Manik Dey, 2007) for information security management are in place, some problems remain. One persistent problem has been the issue of adapting security management systems to various needs. Such challenges persist because a gap exists between the security management systems and the requirements of various domains.

In the past, information security management systems were typically designed to meet specific goals rather than the strategic objectives of a security management service provider as a whole. Thus, their design architectures have made it difficult for them to make changes in response to changing demands. In addition, the effort taken to implement a security management project is redundant.

As these systems become more complex, a major need has emerged, - to improve service, there is a need to develop an architecture that can integrate the basic functions of security management with specific domain needs.

Reusable information security modules reduce costs by shortening system development cycles. By taking advantage of previously created assets from some single sign-on projects, developers can save themselves from recreating an asset from scratch. This also helps eliminate redundancies across the organization further reducing costs.

Fortunately, a technological evolution in the form of Service-Oriented Architecture (SOA) (Arsanjani, 2007) provides a foundation for achieving software reuse. One of the key features of SOA use is that it allows for the user to benefit from software reuse.

The implementation of Service-Oriented Architecture (SOA) using web service technologies is currently the approach of choice in systems integration and management. The defining feature of SOA is that it describes domain applications as a collection of processes each spanning a functional boundary (Blevec, Y., 2007). There has been extensive discussion on web services and SOA technology, in numerous papers. Hence this paper proposes a security management system based on SOA, without engaging in an in-depth discussion of the framework itself.

It is perhaps sufficient to note that service-oriented architecture represents a critical new application development style in the software area. As noted, traditional software engineering methodologies are inadequate to permit the engineering of these critical new applications.

Service Oriented Software Engineering (SOSE) has addressed this issue by providing a methodology capable of overcoming these challenges. There is some existing research on SOSE, including that of Harri Karhunen (Karhunen, 2005). This project, seeks to propose an adaptable information security management server (ISMS) for Single Sign-On environments using SOA technology and the Software Engineering methodology. In addition, this paper serves to provide a case-study of security management scenario into the use of this framework.

2 USING SOA DEVELOPMENT TO BRIDGE THE INFORMATION SECURITY DOMAIN GAP

SOA provides a mechanism for more formal reuse which occurs when services are accessed by service clients to perform a given function. The service client does not really need to know what code they are reusing. They just need to know that the service is providing the function that they require.

In a Service-Oriented Architecture, assets are represented as services. These services are like building blocks that can be reused and assembled into larger applications or services.

The service interface is the essence of the integration design. Combined with the use of standard protocols, interfaces are the essential ingredient for creating a loose coupling where service clients and service providers can communicate regardless of programming language and platform. Services are to be independent, in that clients need not understand the inner workings of a service component.

The proposed architecture uses SOA technology to connect the current security management module with security management needs. Conceptually, there are four major levels of abstraction within SOA.

Since the provider already has security management software, it would prefer reusing the existing functionality to writing new security management applications that replace the original system. Hence, by adopting an SOA approach and implementing it using supporting technologies, the information security service provider should be able to build flexible systems that allow for the speedy and efficient change of function processes. This efficiency is primarily the result of the extensive component re-use afforded by the architecture.

3 RELATED WORKS

3.1 Single-Sign on Research Projects

As the trend toward informationization and integration grow, enterprises have introduced various kinds of information systems in order to improve working efficiency. Every system offers its own security mechanism to protect itself and to ensure the security of its data. The difficulties in management are further magnified by the increasing number of information systems.

Using SSO, a user only needs to be authenticated once - when logging into the front-end system. Then, the user's identity is passed on to the back-end or external applications without requiring additional identity verification from the user. The SSO approach focuses on security integration between these network products.

3.2 Identity Management Research Projects

Identity Management is a useful tool for an administrator. It provides a comprehensive, process-oriented, and policy-driven security approach that helps organizations consolidate identity data and automate the deployment across the enterprise.

Constructing a mechanism for Identity Management can solve the problem of maintaining accounts. But Identity Management mechanisms must also consider Account Synchronization technology in order to combine all required information systems. Therefore, a well designed Account Synchronization component is the key to Identity Management.

3.3 Service Oriented Software Engineering (SOSE)

Several existing modeling methodologies such as Object-Oriented Analysis and Design (OOAD) were introduced. These provided a disciplined approach for software analysis and development. They became common practice and eventually constituted a starting point for implementing distributed applications. While the OOAD methodology is a required precursor, it is not, in itself sufficient to produce SOA technology.

While these traditional methods reinforce general software architecture principles such as information hiding, encapsulation, and modularization, SOA introduces additional themes such as service choreography and service bus that require additional consideration. Hence, a key requirement for development of a SOA is to adopt a solution development methodology that designs and builds SOA components.

4 THE PROPOSED SYSTEM ARCHITECTURE

Figure 2 shows the architecture of the SOA-based information security management system. This architecture consists of four parts: a single sign-on module, the system management portal, a process module, and an identity management subsystem.

This project uses a security management scenario at a University as the application domain. In the following representation (Fig.2), the existing synchronization engine is responsible for providing a means of synchronizing user accounts to various directories.

Since there is a function gap between the existing synchronization engine and business needs, the SOA technology is applied as a bridge between them. For this purpose, each application function of the existing synchronization engine needed to be transformed into a service or services.

SOA technology allows service assemblers to place multiple synchronization services into processes. After the synchronization related processes are ready, a series of steps is executed by invoking synchronization services.

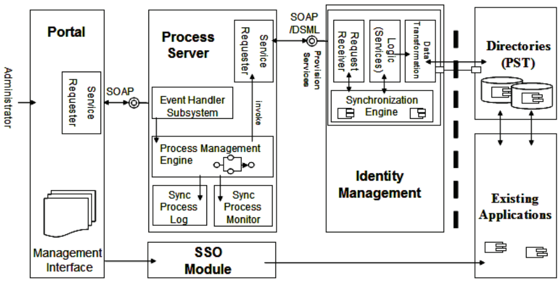


Figure 2: Architecture of the Information Security Management System.

The Single Sign-on module is the element of the system that provides resource protection, and authentication. A very important component of this module is the Security Control Proxy. The Security Control Proxy regards the concept of reverse proxy as the infrastructure. Reverse proxy can connect both front and back-ends to applications on the server. In addition, the back-end server only accepts requests through the Single Sign-on module

The unified authorization function of the Single Sign-on module is composed of two key components. These are the Authorization Service and the Authorization Database. The module also manages all for the protected resources by means of object-orientation.

The system management portal is essentially a control center. It allows administrators to employ a friendly interface to present the authority immediately. Since all access control authority information is stored in a LDAP Directory, administrators can manage all authority resources very easily.

In order to manage the register model of each system, and maintain the accounts of SSO system and account relation, this ISMS system must set up an Identity and Policy management mechanism. The underlying purpose in designing the management module is to offer a unified user and group management mechanism for the single sign-on environment. This improves the efficiency of authorization management in order to reduce the cost of managing each system individually, and accelerates the efficiency with which upgrades are made.

Because of diversity in platforms and specifications for systems, the identity and policy management module must establish mould to synchronize accounts. So, the problem of identity and policy management module primary treatment lies in the data synchronization technology.

The identity management demands between systems can be divided into three basic categories:

Type 1: The initial identity synchronization

This synchronization function creates account information for identity integration. The information includes basic user information

Type 2: Sign-on Account synchronization (SSO necessary information)

These operations include creating accounts for login on the SSO system and accounts for auto-login to existing systems.

Type 3: Account maintenance

Synchronization work mainly maintains user information which already exists in databases by means of the identity and policy management module.

The identity and policy management module includes: A synchronization engine, a synchronization service interface, and an information transformation module. The synchronization service interface can, through a link with SOAP protocol, offer process management servers a service connection foundation.

The identity and policy management module can receive new treatment demands sent from the process engine. Then the information transformation module will begin to update the identity update, in order to meet the structural requirements of different platforms.

In this system, the event handler subsystem and the service request receiver act as an interface for expressing network service connections separately. This synchronization subsystem system can use the request receiver interface as a service provider through the web services interface.

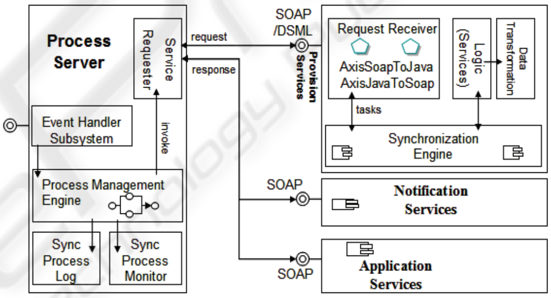


Figure 3: The architecture of the identity management process.

Each circle in Figure 3 represents a reference point to the steps in an authority management process. Every reference point contains a record of the corresponding network service information. The management process server can invoke the request receiver interface via the service requestor in order to execute each of the steps.

5 METHODOLOGY

5.1 The Design Methodology of an Information Security System

The Information security architecture is a design of the processes and technologies needed to achieve security. A proven methodology is important for this design. All security architectures start with the definition of a business context, that is, the balance of business drivers and acceptable risks. The business context is the result of decisions made through the analysis of internal and external factors.

5.2 Service Oriented Software Engineering

To facilitate the adoption of SOA, this project establishes this security management system in phases. This system will focus on the security management process. This phase includes exposing existing security management system functionality as services to other security management applications.

5.2.1 Service Identification

This project initially uses a top-down approach starting with business modeling. This allowed the users to make progress on business models iteratively and incrementally.

Typically, migration to an SOA solution involves integration of existing systems by decomposing them into services, operations, business processes and rules. The domain scenario of the ISMS can further decompose the functional areas into processes, sub-processes and high-level business use-cases.

One step of service identification is an analysis of existing assets, in order to maximize the reuse of the synchronization service engine. When performing an existing synchronization service engine analysis, a bottom-up approach is applied to identify candidate services. During this activity, technical constraints related to existing systems are also considered. The use of this approach assists in identification of potential risks.

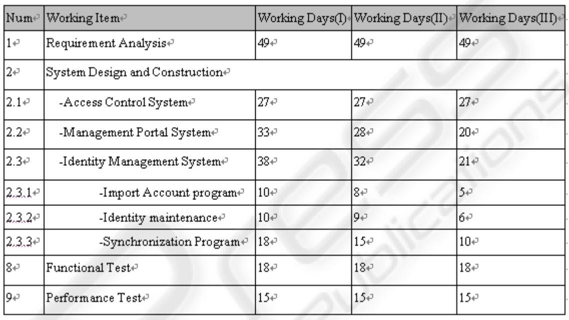
After the candidate services have been identified, the services are categorized into a service hierarchy. The categorization reflects the composite nature of services and helps to determine composition and layering. Categorizations are typically identified through functional area analysis, during domain decomposition activities.

6 EVALUATION

In the previous scenarios, information security projects have always spent a lot of time on customizing applications for specific domains. If core applications of those systems could be analyzed and reused, it would considerably reduce the effort required for future projects.

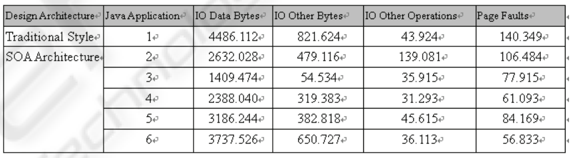
In this paper, an example of an academic project has been given. The subject university featured in this case graduates approximately ten thousand students each year. At the same time there are about ten thousand new students entering the university. Information for each of these students, in addition to employee, faculty and existing student information updates, must be incorporated into the system.

Table 1: The comparison of task results from different design architectures.



Num	Working Item	Working Days(I)	Working Days(II)	Working Days(III)
1	Requirement Analysis	49	49	49
2	System Design and Construction			
2.1	-Access Control System	27	27	27
2.2	-Management Portal System	33	28	20
2.3	-Identity Management System	38	32	21
2.3.1	-Import Account program	10	8	5
2.3.2	-Identity maintenance	10	9	6
2.3.3	-Synchronization Program	18	15	10
8	Functional Test	18	18	18
9	Performance Test	15	15	15

Table 2: The efficiency differences between the two kinds of security system structures.



Design Architecture	Java Application	IO Data Bytes	IO Other Bytes	IO Other Operations	Page Faults
Traditional Style	1	4486.112	821.624	43.924	140.349
SOA Architecture	2	2632.028	479.116	139.081	106.484
	3	1409.474	54.534	35.915	77.915
	4	2388.040	319.383	31.293	61.093
	5	3186.244	382.818	45.615	84.169
	6	3737.526	650.727	36.113	56.833

The biggest difference between the two design architectures discussed by this paper lies in the number of levels into which job components are divided. Hence, this paper measures the efficiency differences between the two kinds of structures when carrying out the same job.

This research adopted the efficiency tool embedded in Microsoft Windows to collect efficiency information. The content collected is the I/O amount of data on each of the respective servers.

In testing the entire procedure, it is joined account numbers of 10 users through an Identity Management System. The identity management system will send out a request for account creation to the identity synchronization program. Then, the identity synchronization program will connect to all of its information systems in order to create the account and update identity information.

The test results from the procedure described above are displayed in Table2. The test results show four important values. These following meanings:

1. IO Data Bytes and IO Other Bytes: Show the in and outflow volumes when executing the

account synchronization. This value represents the resources consumed by the process.

2. IO Other Operations: These are the operations of the operation system, when executing account synchronization - for example the tasks of network communication. The higher the number is, the larger the work load for the systematic server to deal with is.
3. Page Faults: these shows the error time when account synchronization occurs. The higher the number value is, the more work the server must deal with.

7 EXPERIMENTAL RESULTS

The project was used to test an SOA-based ISMS implemented with a software engineering methodology. In the ISMS, the operation management portal provides administration pages that have all been initially demonstrated using the interfaces illustrated in figure 6.

Additionally, this paper analyzed the traditional and SOA development styles. Doing so revealed that the service-oriented development model was capable of reusing existing programs, and reducing the number of steps required in completing tasks.

The system also added additional subdivisions to job-components, presenting a unified service process model. Thus, whenever a new system began to combine, the necessary service components were available for use. The system was not affected by low-level operations concerns.

In contrast, the traditional development lifecycle, required components to be distributed independently, during the construction phase. Moreover, its hierarchical structure had the potential of overweighting the server.

8 CONCLUSIONS

This paper, presented a mechanism for applying SOA architecture to security management in single sign-on environments.

This research has successfully demonstrated an information security management system using Service-Oriented Architecture. The ISMS not only makes identity synchronization more effective, but also reduces the gap between the basic identity management engine and application domain needs.

The ISMS system employed reused identity management functions in a complex domain. In doing so, the SOA technology was found to be very effective in addressing traditional reuse problems. For an existing identity management engine, it is advisable to have a service set that can guarantee a high degree of support.

In terms of evaluation result, the model driven development for SOA is a prescriptive method that includes several complementary approaches to identifying services for the security management domain.

ACKNOWLEDGEMENTS

This research was supported by the Ministry of Economic Affairs, Taiwan, and R.O.C. under grant NSC 95-2221-E-027 -016.

REFERENCES

Wade H. Baker,Linda Wallace, “Is Information Security Under Control?: Investigating Quality in Information Security Management” , *IEEE Security & Privacy*, 5(1), 36-44, 2007.

Chin-Chen Chang; Wei-Bin Lee, “Taiwan: focus on the information security market”, *IT Professional* , 5(5), 26 - 29, 2003.

Sanchez, L.E.,Villafranca, D.,Fernandez-Medina, E., Piattini, M., “Practical approach of a secure management system based on ISO/IEC 17799”, The First International Conference on Availability, Reliability and Security(ARES 2006) , 26-28 Oct. 2007

Manik Dey, “Information security management - a practical approach”, AFRICON 2007 , 26-28 Oct. 2007

Arsanjani, A., Liang-Jie Zhang, Ellis, M. Allam, A., Channabasavaiah, K., “S3: A Service-Oriented Reference Architecture”, *IT Professional,* 9(3), 10-17, 2007.

Blevec, Y., Ghedira, C., Benslimane, D., Delatte, X, “Service-Oriented Computing: Bringing Business Systems to the Web”, *IT Professional,* 9(3), 19 - 24, 2007.

Gold, N.; Mohan, A.; Knight, C.; Munro, M., “Understanding service-oriented software”, *Software, IEEE*, 21(2), 71 – 77, 2004.

Karhunen, H.; Jantti, M.; Eerola, A., ” Service-oriented software engineering (SOSE) framework”, 2005 International Conference on Services Systems and Services Management, 13-15 June 2005.