Int. J. Communications, Network and System Sciences, **2010, 3, 811-815**
doi:10.4236/ijcns.2010.310109 Published Online October 2010 (http://www.SciRP.org/journal/ijcns)

Solutions for 3 Security Problems and its Application in SOA-FCA Service Components Based SDO

Nannan Wang, Zhiyi Fang, Kaige Yan, Yu Tang, Xingchao An
College of Computer Science and Technology, Jilin University, Changchun, China
E-mail: *wangnannan*_1985@126.*com*, *zyfang@public.cc.jl.cn*, *yankaige*@163.*com*,
mailtangyu@gmail.com, 81435756@*qq.com*

Received June 19, 2010; *revised August* 2, 2010; *accepted September* 10, 2010

Abstract

Service-Oriented Architecture (SOA), which is an open architecture, provides developers with more freedom. However, its security problem goes from bad to worse. By taking an insurance business in Formal Concept Analysis (SOA-FCA) Service Components based Service Data Object (SDO) data model transfer with proxy as an example, the security issue of SDO data model was analyzed in this paper and this paper proposed a mechanism to make sure that the confidentiality, integrity, and non-repudiation of SDO data model are preserved by applying encryption/decryption, digest, digital signature and so on. Finally, this mechanism was developed and its performance was evaluated in SOA-FCA Service Components.

Keywords: Service-Oriented Architecture, Service Data Object, Data Confidentiality, Data Integrity, Data Non-Repudiation

1. Introduction

As a new way and environment for distributed software system, Service-Oriented Architecture (SOA) [1], contains running environment, programming model, architecture and methodologies. Service plays a core role in SOA. The whole IT system is treated as a collection of services, not a collection of application programs. Each service provides a unique function and the granularity of each function can be either big or small. Other applications or services can "consume" this service. SOA aims at providing an exchangeable, highly adaptable and flexible standard. SDO can facilitate this and provide some help. SDO [2], which can simplify and unify the access to heterogeneous data by using a unique API, can also be used in other data process applications. Due to using of a new and open standard in substitution for traditional security parameters, SDO data model has a lot of data security issues. The new standard doesn't take the security into its consideration at the time of its origination. Thus, its security issue, especially data security issue, becomes even worse than before. The confidentiality, integrity, non-repudiation issues should be taking into account, when it comes to data security. Through an in-depth study of insurance business, this paper selects six representative insurance products and abstracts the information on the insurance application to be the entities of formal context. This paper solves the problem of data security, the confidentiality, integrity, non-repudiation on this insurance product based SDO data model.

2. Introduction and Analysis of SOA-FCA Service Components of Insurance

2.1. FCA-Based Business Entity Object

Six representative insurance products based SDO data model were selected by this paper. We abstract the form of insurance application to be objects of formal context and the insurance underwriter, insurance applicant, etc to be attributes. These six representatives involve compulsory insurance for traffic accident of motor vehicles, commercial insurance for motor vehicles, insurance for farming reproducible sow, hail insurance for planting onion, basic property insurance and construction insurance.

FCA provides a formal process for extracting and classifying all the business concepts involved in a particular business system. By excluding the influence of human factor on the analysis result, this rigorous mathematical tool makes the analysis result of the business entity of insurance underwriting module, a core business of insurance, much more objective. Driven by real business operation, eight business entities of insurance underwriting are abstracted from the six representatives. The corresponding E-R diagram is shown in **Figure 1**. There are three business entities that are reused more frequently than others. They are basic information about insurance application, computation sheet of insurance amount and in insurance payment schedule. These three entities are more likely to be reused when new insurance products are introduced. With the business expansion and request update, these entity objects of insurance can be reused directly or reorganized into new entity objects to be used by the new insurance products.

2.2. Analysis of Underwriting Service Component Based on FCA

The well-designed underwriting business entities in 2.1 Section suggest that a specific business function can be achieved by applying some operations such as adding, deleting, editing and querying on certain entities. A service component can be viewed as a combination of certain operations and entities. Real business components in an insurance information system spans across two dimensions of function and insurance category, which will reuse the components to a larger extent. For service components based SDO are reused continuously, the problem of complexity in system will increasingly become serious so it is necessary for us to pay attention to its security issues. Thus more regard must be paid to security requirement of the information transmitted on the internet and we must find a comprehensive solution which can solve the data security issues of SDO data model.

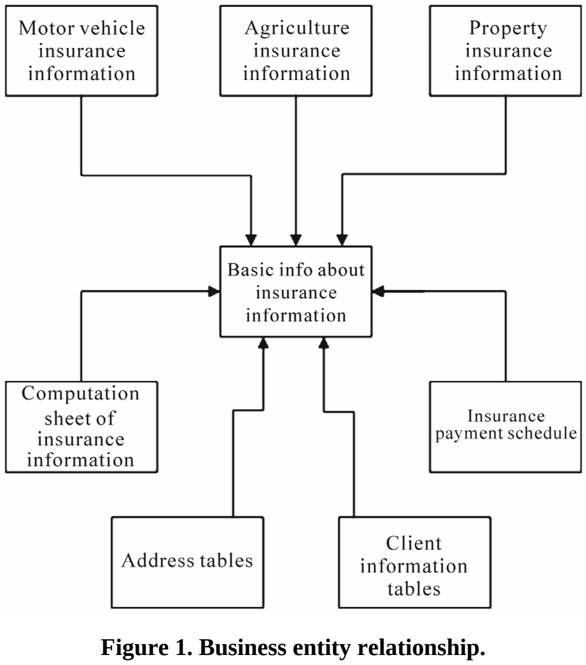
Motor vehicle insurance information
Agriculture insurance information
Property insurance information
Basic info about insurance information
Computation sheet of insurance information
Insurance payment schedule
Address tables
Client information tables

Figure 1. Business entity relationship.

3. Analysis to Data Security Issues of SDO

3.1. Data Confidentiality of SDO

The confidentiality [3] indicated that when the data were transmitted, it cannot be eavesdropped. It means that the information should not be wiretapped, and cannot see the original message even if they got the data. The data encrypted can only be decrypted by authenticated users. In some SOA environments free from protection, the message transmitted on the internet can be easily overheard and intercepted by unauthenticated users.

3.2. Data Integrity and Non-Repudiation of SDO

The data integrity [4] makes sure that the data should not be tampered in the process of transmission. If the data are tempered, the receiver is supposed to know this. The non-repudiation [5], which is also called data signature, means that both the sender and receiver should not deny its transmission and reception respectively. Both integrity and non-repudiation are hard to achieve, as SDO takes little attention to its openness and security.

4. Requirements Analysis and Solutions of Data Security

4.1. Analysis of SDO Data Security Solution

The application message level's encryption of SOA is a reasonable solution. Due to the judgment that public key encryption, private key decryption, public key signature and public key authentication run slow and cannot be used to big sum of numbers, this paper only commits encryption and signature on private data contained in SDO. This brings two major advantages. First, the data processed by this mechanism are also based on the open standard and the receiver can treat them as SDO data. Second, the running speed will not slow down while the numbers of processed data increased correspondingly.

4.2. Overview of Instance and Data Security Requirements

In the real scene of the SOA-SCA (Service Component Architecture), if a service request is submitted by a service consumer, the SDO data submitted by users may be through a number of service providers so as to achieve this service request. Take the example of **Figure 2**; the customer called Tony would like to complete the transfers request between insurance accounts, according to the agents WTAM of insurance services. First of all, a brief security analysis of the service request is carried out in the following aspects: data confidentiality, data integrity and non-repudiation.

It is indispensable to ensure the information confidentiality in the transmission not only from John to the agent WTAM but also from the agent WTAM to the insurance agent so that we can achieve confidentiality of information. In order to ensure the integrity of the information filled by Tony, it is necessary to prevent network hackers tampering with the data, but also to prevent Agents (WTAM in the scene) modifying customer data. For the agent WTAM, it must has non-repudiation of John's insurance accounts operation, and at the same time, for the insurance system, it must not only ensure that users cannot deny their operations of the accounts, but also ensure that the intermediate agents cannot deny account deputy operation that they would like to do instead of customers.

4.3. Security Solutions of Data Confidentiality, Integrity, Non-Repudiation

The design of Data security solution (data privacy, data integrity, data non-repudiation) is shown as follows.

Step 1. Tony, WTAM, Insurance agent First, to generate their own public key, private key, and then their public key will be posted to the CA (certificate authority) respectively, and CA generate their certificate, the certificate contains the public key and their own identity information.

Step 2. If Tony wants to send their service requests to WTAM Service Agent, first he would go to the CA certificate to get WTAM certificate, and then CA replies WTAM certificate encrypted with Tony's public key.

Step 3. Tony analyses WTAM certificate from CA and obtains WTAM public key, and sends confidential data of SDO data to WTAM encrypted with WTAM agent's public.

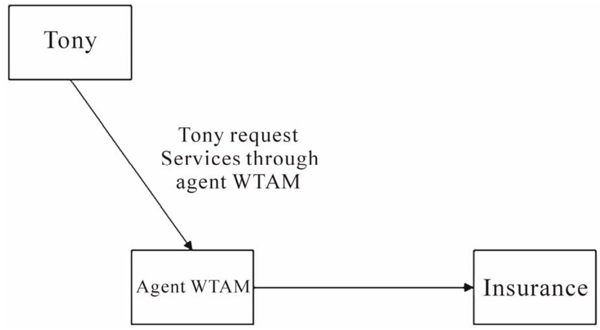

Figure 2. Tony wants to do insurance transfer through agent WTAM.

Step 4. Tony gets the information summary of SDO data to send, and signs the information summary with their private key.

Step 5. Tony calls agent WTAM service and sends SDO data encrypted and signs with Tony signature to the WTAM agent.

Step 6. WTAM agent requires Tony certificate from CA, and resolves certificate to get John public key.

Step 7. WTAM decrypts confidential data of the SDO data with its own private key from Step 5; generates the specific data of information.

Step 8. WTAM verifies the Tony's information signature and makes use of information summary from Step 7 and Tony's public key from step 6, if proved to be successful, then the message from Tony to the WTAM has not been tampered with by third parties illegal in network transmission and after Tony signed, then continues to Step 9, otherwise, there are two errors, one is information may be modified in transmission, that is information integrity has been destroyed, the second is likely Tony's signature failure, in which case, WTAM will be prompted to require Tony to re-send service requests, and tells Tony the specific reasons of errors, the service process is terminated.

Step 9. If step 8 is successful, WTAM requests bank's certificate from the CA and resolves the insurance agent's public key.

Step 10. WTAM encrypts SDO confidential data to be sent to insurance agent with the bank's public key.

Step 11. WTAM adds its signature with its own private key in the SDO data which has been signed by Tony.

Step 12. The SDO encryption data from step 10, WTAM signed data from step 11, and Tony signed data from step 4 will be sent to insurance agent by WTAM.

Step 13. Insurance agent receives encrypted and signature data from WTAM, and uses their own private key to decrypt the encrypted data to obtain the information of confidential data.

Step 14. Insurance agent requests WTAM agent's and Tony's certificate from the CA, and resolves WTAM agent's and Tony's public key.

Step 15. Insurance agent verifies the WTAM agent's signature by WTAM agent's public key from step 14, data from step 4 and step 11, if successful, go to step 16, Otherwise, authentication fails, the WTAM agent's signature may indicate failure, or information being modified in transmission from WTAM to insurance agent, so insurance agent needs to throw an exception to tell WTAM that signature verification failure. WTAM may return to step 6 to re-run step 6 to step 12.

Step 16. Insurance agent verifies the Tony's signature by Tony's public key from step 14, data generated from step 4 and information summary from step 13, if successful, then go to step 17, Otherwise, throws an exception to tell WTAM that signature verification failure, WTAM may also return to step 6, re-run step 6 to step 12. Signature verification failure may be the following reasons: data are modified in WTAM agent's internal, or are modified in data transmission from WTAM to insurance agent, or Tony's failure contained in the customer's data is invalid, or the signature is incorrect, but it has already been used, so that Tony could have been avoided operating Tony's account data without the authorization.

Step 17. Insurance agent runs the requested service from customer Tony, and ends of this process.

It is necessary to note that insurance agent must verify the SDO data contain Tony's signature so that it can operate Tony's accounts, otherwise, the insurance agent will not carry out any operation of Tony's accounts. In other words, if the insurance agent wants to modify any critical data of customers, it must firstly get permission from customers; otherwise, it will not modify any critical data. If the data pass through a number of intermediate agents from producers to consumers, these agents need to sign the key and confidential SDO data, and then verify the signature in the opposite order. If there is any failure in the process of verification, the information from producers to consumers is illegally modified by a third party during transmission.

5. Application of Data Security Solutions in Insurance Business

5.1. Application Environment of Insurance Business

Through analyzing and designing the underwriting business entity object and SOA service components, SOA service function model of insurance transaction system is shown in **Figure 3**.

Application situation and relation of general components, individual components and variant components, which are introduced in Section 3, are clearly expressed in **Figure 3**. Information system is made to be more flexible and effective by SOA service architecture.

5.2. Application Result of Solutions in Insurance Service Components

In Section 4 we use public-key encryption, private-key signature and public-key certificate to design a solution of data security issues. Data security issues are solved by this solution in SOA-FCA service components based

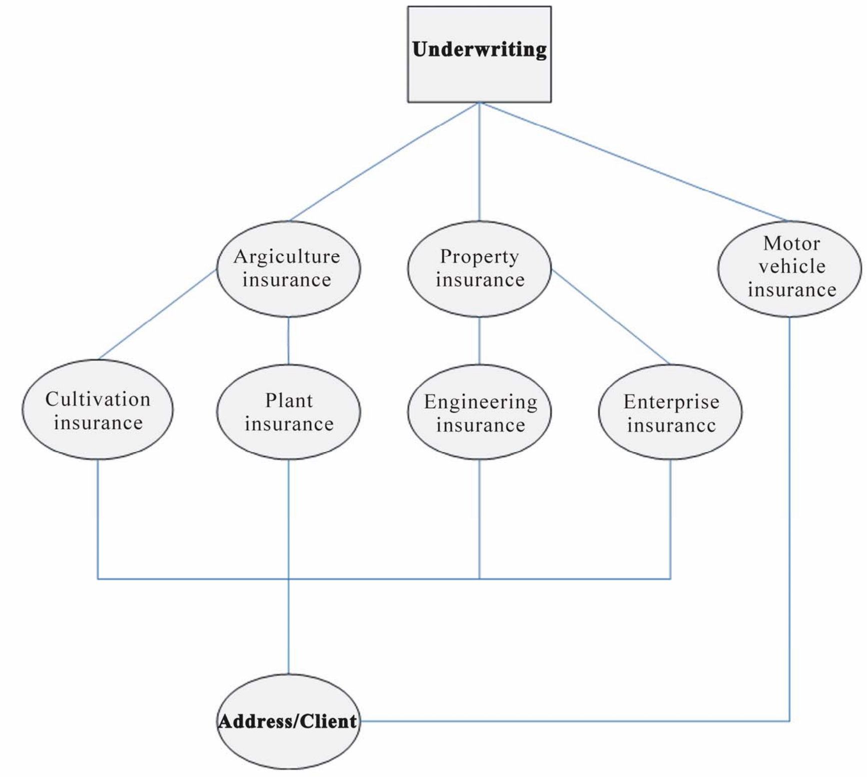

Figure 3. Insurance service function model.

SDO data model. We applied this solution into insurance information system so as to solve the confidentiality, integrity, and non-repudiation of SDO data model when SDO data is transmitted on the internet. In this way, it makes SOA-FCA service components more open, flexible, extensive, meanwhile it also improves and perfects its data security of SDO data model. Through application of data security solution, we solve security issues of SDO data transmitted in insurance information system and better data security issues in SOA-FCA service components based on SDO.

5.3. Performance Analysis

Only the encryption data is processed when the insurance system realizes, and the hardware configuration of the current serve has been greatly improved. The network transmission speed gets a large scale enhancement, although some extra processing and data causing the transmission traffics to increase are added in order to guarantee the security of SDO data, the system performance does not reduce greatly on the condition of without the extra processing and data.

6. Conclusions

SOA, compared with traditional application programs, brings a bigger openness, more flexibility and extendibility. But the openness also leads the security problem at the same time. The human and the machine can access to the data from the service supplier according to the standard protocol at any time or place. SOA service components of Insurance have data security issues in the process of transmission. We solve these data security issues in SOA-FCA Service Components of insurance based SDO data model in our paper, design confidentiality, integrity, and non-repudiation realization scheme of SDO data, and then we carry on realization and analysis; validate the effectiveness of the scheme.

7. References

[1] T. Erl, “Service-Oriented Architecture (SOA): Concepts, Technology, and Design,” Prentice Hall PTR, Upper Saddle River, New Jersey, 2005.

[2] B. Portier and F. Budinsky, “Introduction to SDO,” IBM developerWorks, 2004.

[3] M. John, “Security Models: Encyclopedia of Software Engineering,” Wiley Press, 1994.

[4] M. Benedikt, C. Cheeyonyong, W. F. Fan, *et al.*, “Capturing Both Types and Constraints in Data Integration,” *Proceedings of the ACM SIGMOD International Conference on Management of Data*, San Diego, California, USA, 2003, pp. 277-288.

[5] D. Chaum and H. Van Antwerpen, “Undeniable Signatures,” Advances in Cryptology-CRYPTO’89, LNCS 435. Springer-Verlag, Berlin, 1989.

[6] S. W. Galbraith, “Invisibility and Anonymity of Undeniable and Confirmer Signatures,” Topics in Cryptology-CT-RSA’03, LNCS 2612, Springer-Verlag, Berlin, 2003.