EXPERIMENTAL RESEARCH AND CAPABILITY VALUATION ON SECURITY OF SOA-SCA BASED SDO

Peng Xu, Zhiyi Fang, Hang Su and Chuyi Wei
College of Computer Science and Technology, Jilin University, Changchun, P.R. China

Keywords: SOA, SCA, SDO, data confidentiality, data integrity, non-repudiation of data.

Abstract: By using technologies such as encryption, decryption, message digest, and digital signature and so on, this paper designed respective solutions for some security problems of SDO (Service Data Objects) data model, a concrete business processes based on SOA-SCA (Service Component Architecture) as well as security solutions for data confidentiality, integrity and non-repudiation of SDO data model based on the business processes. In addition, the design goals of security solution were analyzed in detail. Finally, the solution was achieved by using development tools WID (WebSphere Integration Developer) and WPS (WebSphere Process Server). The test and capability analysis for this realization was performed too.

1 INTRODUCTION

SOA (Service Oriented Architecture) is the new phase of the construction methods and environment for distributed software system. SOA includes a set of new construction methods and environments for distributed software system such as running environments, programming model, structure style and relevant methodology, which cover the whole life cycle for service: Modeling - Development - Integration - deployment - Operation - Management. Compared with the traditional applications, SOA mainly considers in which way and how to expose services, as well as to expose what services. In this way, we can combine the services provided by the old system to construct a new application. If using traditional methods, this may require re-development, all from the beginning.

Disadvantages of traditional application architecture lead to the existing application architecture model's sluggish response on the changing business needs and results in the increase of our investment. SOA can help us to improve business value better and faster, and in this way we can get the ability of quick response and reuse.

Because of the inherent openness of SOA and a number of standard protocols used by SCA (Ben, 2007), which makes SOA security issues, especial for data security problem, very serious, researches on security issue of SDO became a very helpful thing. This paper focuses on the SDO data's confidentiality, integrity and non-repudiation and does research to address my solutions to these issues.

2 REQUIREMENT ANALYSIS

2.1 Overview SOA Security

SOA security issues are result from using new open standards instead of traditional security parameters. There are two aspects make the security issues more prominent. For one thing, these new standards are completely open and no one holds them. For another, it seems that nobody considered security issues when designing these standards. Let's have a look at what serious security problems the SOA architecture may bring on.

2.2 Security of Authorization and Authentication in SOA

Authentication is a process to verify the identity of visitors. It is related with authority verification but has some differences. Authority verification is to verify whether a user is allowed to access the services it calls, while authentication is to prove that the identity of whom visiting your service now is the same with that the user declared. In an unsafe SOA

Xu P., Fang Z., Su H. and Wei C. (2008).
EXPERIMENTAL RESEARCH AND CAPABILITY VALUATION ON SECURITY OF SOA-SCA BASED SDO.
In *Proceedings of the International Conference on Security and Cryptography*, pages 337-341
DOI: 10.5220/0001929203370341

environment, it is difficult to achieve trusted authentication. Because of the coarse-grain security checking mechanism for interaction between computers, a SOA services may be attacked by illegal users. SOA services have neither authentication nor authority verification. If a mainframe's resources were used by illegal users, it will be a serious security issue.

2.3 SOA may Lead to 'Denial of Service Attacks'

Because the unsafe SOA open for all users, illegal users can send a large number of service requests to the server, which will result in service providers' abnormal work. Therefore, a group of illegal users' request may bring on denial of service attacks and SOA may lose the ability to monitor the service level it provides if serious. (The service level is the qualitative measurement for SOA). If there is an attack, unsafe SOA can't tell you whether it has been overloaded and will make system administrator can not react on the security issues in the first time.

2.4 SOA may Lead to Auditing Problem

An audit log is a basic requirement for IT security. In order to check the security performance and analyze security problems, the system administrator must have the accurate system behavior log in his hand. Because unsafe SOA don't have message and transaction log mechanism, there's no way to determine who had used the service and where the service originate from when a service was called, which will result in no audit trail can be used to investigate the security gap after the incident and no way to determine who and damaged the system and when it happened.

2.5 Data Security Problem of SDO

2.5.1 Analysis for Confidentiality of SDO Data

Confidentiality is to make sure that there's no eavesdropping in the transmission. Even if the data is intercept by illegal user, he will not understand the real meaning. If architecture can not guarantee a high degree confidentiality, that is not fully secure.

In an unsafe SOA environment, illegal users can eavesdrop and intercept the SDO data transmitting on the net. If the SDO data manufacturers sent to suppliers contains confidential information, for example, something like a list of materials required, the necessary quantity of each material, the very arrival date, and didn't do additional processing, illegal users could analyze the SDO data he has got very easily and find these clear message he wants after he intercepted the SDO data due to the standards SDO based. What's worse, if illegal users modified the SDO data and transmitted it to suppliers, it will result in huge economic losses. Therefore, the possibility of SDO data's being abuse by illegal users is very high.

2.5.2 Analysis for Integrity and Non-repudiation of SDO Data

When a service provider received a call from the requesting party, it must be verified to ensure that the data is sent from the requesting party and the data has been neither changed in transmission nor forged by illegal third-party. That is data integrity. The requesting party can not deny that it had sent the request of the services, namely, the non-repudiation of data. Data integrity and non-repudiation is very important for the service providers and petitioner exchanging data on the net.

3 SOLUTIONS FOR DATA SECURITY PROBLEM OF SDO

For most security problem in the SOA-SCA environment there is a suit of solution. A big solution also contains a number of small solutions, and every solution resolves a security problem in a specific area of SOA. Security solutions for SOA will be hinged on its security architecture and the needs of each application. I will provide specific solutions for data security (data confidentiality, integrity and non-repudiation) (Matt, 2004) of SOA-SCA.

Security framework of Traditional application is based on the interaction between human and computer, while SOA allows interaction between computers. However, the developers paid very little attention to that interaction. I think this is because SOA lacks of internal security. In SOA-SCA environment, we should embed these functions that ought to be achieved by the equipment into the application program.

Since it is not so fast for public key encryption and private key decryption as well as signing with the private key and verifying with public key, they are not suitable to operate on mass data. Owning to this, my solution doesn’t sign or encrypt all the data.

The SDO data to be processed is only the confidential information. There are two advantages by doing this way. Firstly, the solution will not run slower because of increasing data. Secondly, after being processed by the solution, the SDO data's format is still based on open standards, so the receiver can still treat it as SDO.

3.1 Solution for Confidentiality of SDO Data

Take manufacturers for example, assume that the supplier system want to send a SDO services call to the manufacturer. First, manufacturer must send a public key to CA (certificate authority) (Wenbo, 2003), and supplier request a certificate from CA. The certificate supplier received contains a public key which matches manufacturer's private key. Second, the supplier encrypts its message with the public key in the certificate, and sends the encrypted message and its certificate to the manufacturer. Then, SOA security solutions intercept the information and check the validity of the certificate through CA. Doing this can verify the identity of the supplier. Once the authentication checked, the encrypted SDO data can be sent to the manufacturer. After received the SDO data, manufacturer can use its private key to decrypt the data and process it.

As shown in Figure 1 , if the supplier wants to send SDO data to manufacturer, the process will be as follows:

1. Manufacturer sends its public key to CA, and holds private key on its own side.
2. Supplier requests the certificate that contains manufacturer's public key from CA.
3. Supplier gets manufacturer's public key by analyzing the certificate received in Step 2.
4. Supplier sends the SDO data encrypted with the public key got in Step 3 and its certificate together to manufacturer.
5. SOA security solutions send manufacturer's certificate got in Step 4 to CA to validate its authentication. If succeed, go to Step 6. Otherwise, tell the supplier by send message that certificate validation failed and withdrawal.
6. SOA security solutions send manufacturer the SDO data encrypted with its public key.
7. When received encrypted data from Step 6, manufacturer decrypt the data by using its private key to get clear data

When the message processed with encryption keys by the security solutions for data confidentiality, it will be converted to encrypted SDO data. In other words, the message meets the SDO format, but the content is encrypted. By doing this, system could receive messages as SDO and process it, rather than rely on custom or proprietary messaging standards. At the same time, we realized the SDO data confidentiality, and the system still based on open standards.

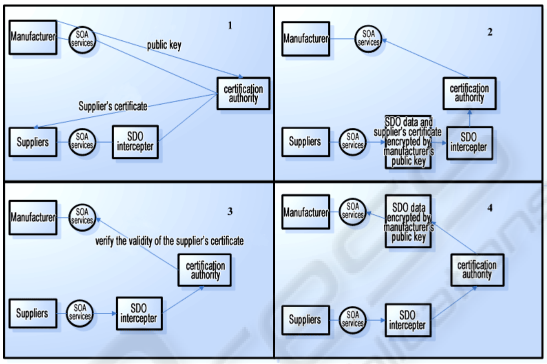

Figure 1: Process of use public/private key encryption and certificate in unsafe SOA.

The solution involves only two systems. When there are multiple systems, every interaction between two systems should follow the solution above to send and receive SDO data.

3.2 Solution for Integrity and Non-repudiation of SDO Data

We will solve it by using digital signatures. As shown in Figure 2. When sending message, sender needs to append a message digest signed with its private key. When received the information, receiver need to decrypt the signed message digest with sender's public key. If the message digest from decryption is the same with that generated from

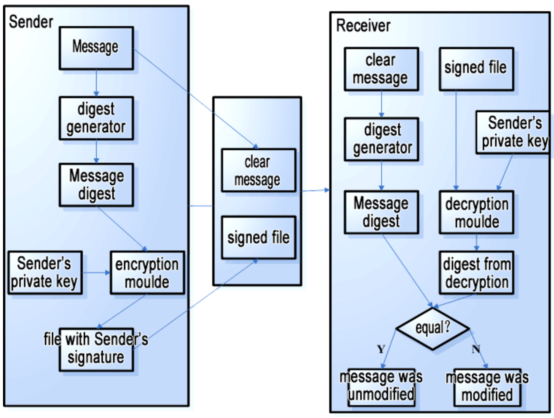

Figure 2: Principles for the realization of data integrity and non-repudiation.

received clear data, it means that the message has not been modified by a third party when transmitting, or it is likely that the message has been modified and the data integrity was destroyed. There is another situation that no signed digest is in the message, which means that sender didn't confirm this message and data non-repudiation destroyed.

Also take communications between supplier and manufacturer as an example, assume that supplier want to send SDO data to the manufacturer, the process will be as follows:

1. Firstly, supplier and manufacturer need to generate their own pair of public key and private key, and then send public key to CA, and CA will generate certificate for them.
2. Supplier generate message digest of SDO data.
3. Supplier makes a digital signature for message digest from Step 2 with its private key.
4. When receive the message with supplier's signatures, manufacturer will request the supplier's certificate, which contains its public key, from CA first.
5. Manufacturer decrypt the SDO data received in Step 4 with its private key to get clear data, and then generate message digest.
6. By using the public key in supplier's certificate and the message digest from Step 5, Manufacturer verifies SDO data signed by supplier.
7. If succeed in Step 6, the SDO data was not modified when transmitting in the net, and includes the supplier's signature.
8. If the validation failed, there are two kinds possibility. For one thing, SDO data was modified in the transmission, which means the data integrity was destroyed. For another, there's no supplier's signature in the received SDO data, or the signature information in the SDO data is wrong, which means non-repudiation of data was destroyed.

4 SYSTEM DESIGN

By using WID and WPS, the system realized such a service that an intermediate agents ACME transfers between bank accounts on behalf of customers. Fig.3 shows main functional modules.

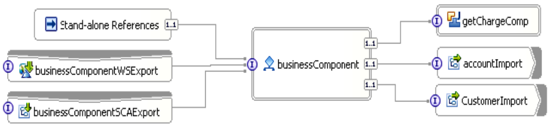

Figure 3: System Module.

According to Fig.3, the system mainly contains the following modules: module for the account services of the relative bank system, customer service module of ACME, fees module of ACME, a module in charge of the information exchange between modules, and a CA module to provide certificates to every customers. The modules division, as well as the services provided by every module is according to the SOMA (Service-Oriented Modeling and Architecture) method (Abdul, 2008).

5 SYSTEM TEST

5.1 Test Case

Assume that a customer of ACME, John, have respectively account in two banks, Bank A and Bank B. Now he wants to transfer $10,000 to Bank B account from Bank A account, but he did not want to go to bank. ACME has integrated account services of the two banks, so he wanted to complete this through ACME.

Since encryption, decryption or signature with RSA (Murdoch, 2001) is not suitable for mass data, the system will process the confidential information of the SDO data only (choos transfer accounts here).

5.2 Test Result

Under the server WPS v6, a stand-alone reference was exported by WID and we can design a JSP page to call SCA services in the test.

Here is the data accrued when system running:

```
[2/24/08 16:32:30:047 CST] 000000bb SystemOut
O
Nn5yBtUN4Ntd+e8+h9tFnE3QikRYAPMeVRzWD
6V9yHrOqjkw2queTuWbuDHVkjqMusSf4XAxT6h
XbpbImVO86A==SDOXJ/8OfXCTbSK5PjT7aGft
MJmBtYQNCPbxHeDOmYYb353BSdMCz6ccldjd
a3tPNAXCwPk2mDHmMoS8rz3J6c8kA==          --
ACME
[2/24/08 16:32:30:047 CST] 000000bb SystemOut
O customer signature verification success -- ACME
[2/24/08 16:32:30:094 CST] 000000bb SystemOut
O
WpLLkdB2iRjioDOmpksZC4jUPKT85j6r3iqx1pNb
T2MaaHIXHyz3whL/IBOhNUBSuq9nuHksYFzom
fX/BOdURQ==SDOXJ/8OfXCTbSK5PjT7aGftMJ
mBtYQNCPbxHeDOmYYb353BSdMCz6ccldjda3t
PNAXCwPk2mDHmMoS8rz3J6c8kA==SDOCSlV
Lg5gmNlFvCC1pNy6BtALDhddZJ20x/07nF+yf53s
0IblhNH4ErKCo6wiSW1GVXCjD+wkMHJKJVGi
1YnuyQ==--bank
```

```
[2/24/08 16:32:30:109 CST] 000000bb SystemOut
O deduct amount: 10000 -- bank
[2/24/08 16:32:30:109 CST] 000000bb SystemOut
O ACME signature verification success -- bank
[2/24/08 16:32:30:109 CST] 000000bb SystemOut
O customer signature verification success -- bank
[2/24/08 16:32:30:109 CST] 000000bb SystemOut
O deduct money from bank
```

From line 2 to line 6, this is the encrypted data and signature created when John processing amount of account transfer. The data contains two parts, and they are separated by the keyword “SDO”. First part is the data encrypted with public key of ACME, and the second part is the signature data obtained from the digest of account transfer amount which signs with John’s private key. The data is output data for John and input data for ACME.

When ACME got the encrypted data and signature in line 2 to line 6, it verifies John's signature and data integrity. According to the system log, verifying succeeded. After verified the signature data (Raghavan, 2000) and integrity, ACME use its private key to obtain the clear data in the first part, and then use public key of the BANK to encrypt. Finally, ACME appends its signature to the data above.

In the line 10 to line 16, the data is the output of ACME, and also input of BANK. The data contains three parts, which also use the keyword "SDO" to separate. The first part is the data encrypted with the public key of BANK. The second part is the signature data obtained from the digest of account transfer amount which signs with John’s private key. The third part is signature of ACME. Once gets the data, the bank will decrypt it to clear data, “10000”. According to the log, the decryption succeeded and the clear data of amount was found. Then, the bank will verify the signature of ACME and it of John. According to the log, the two works are all successful, too. After completion of these works, BANK will treat with the account of John.

According to the operating data and analysis above, we can conclude that, the SDO data in SOA-SCA environment achieved the goal of data confidentiality, integrity and non-repudiation on the way from producer to consumer.

5.3 Analysis for System’s Performance

Although the system added some extra processing and extra data which increased network traffic to guarantee the secrecy, integrity and undeniably of the SDO data, the hardware of the servers and the bandwidth been has greatly enhanced. Also, we processed only confidential data when carrying out the system. So, comparing with not having these extra operations and data, system's performance has not large scale reduction.

6 CONCLUSIONS

SOA has greater openness, flexibility and scalability than traditional applications. Meanwhile, security issues of SOA bring about greater challenge. Any person or computer in any time and any place can visit the service as long as it follows the standards. SCA is an application framework based on SOA. SDO is the data model based on SCA. This paper designed the solution to guarantee confidentiality, integrity and non-repudiation of SDO data when calling the SCA application, and then achieved it using WID, WPS.

REFERENCES

Ben MargolisandJoseph Sharpe, 2007. *SOA for the Business Developer: Concepts, BPEL, and SCA*, MC Press, First Edition.

Matt Bishop, 2004. *Introduction to Computer Security*, Addison-Wesley Professional

Wenbo Mao, 2003 .*Modern Cryptography: Theory and Practice*, Prentice Hall PTR

Abdul Allam, Ali Arsanjani, 2008. *“Service-Oriented Modeling and Architecture”*, Technical paper of IBM Global Services. Version 2. 14-34.

Murdoch Mactaggart, 2001. *Introduction to Encryption*, IBM developerworks, China

Raghavan Srinivas, 2000. *Security’s Evolvement and Idea of Java,* IBM developerworks, China