The Analysis and Design of Port Secure Data-Exchange Interface

Wang Shuqiu[1, a], **Huang Lei**[2, b]

[1]*School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China*
[2]*School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China*
[a]*16120619@bjtu.edu.cn*, [b]*lhuang@bjtu.edu.cn*

Keywords: Port, Web Service, Data-sharing, Interface security.

Abstract: In recent years, China's port information level has been improved steadily, with extraordinary achievements in optimizing business process, improving operational efficiency and logistics. However, with the computing environment getting increasingly complex, the data-exchanging between different systems tend to face a large number of complex and diverse security challenges, which would lower the efficiency and accuracy. The paper aims to design a set of security technology solutions based on the combination of the specific security requirements and the existing security technology.

1. Introduction

This paper is mainly associated with the actual production and operation of Guangzhou Port. With the production business system growing much larger, the network structure and the environment become more complex. In the exchange of information through the Internet, it is inevitable that there is eavesdropping, tampering, loss of information and other aspects of security risks, which will affect the efficiency and accuracy of enterprise data transmission. Based on the Web Service data interaction model, this paper focuses on the analysis and comparison of the existing security technology and develops the appropriate solution for the security problems faced by the production business system in the external data exchange and sharing.

2. Literature Review

2.1 The development of data-sharing security

With the rapid development and application of Internet technology, the construction and management of MIS security has become the focus of information construction in recent years. Various industries strengthen network security construction to ensure the smooth flow of data platform and exchange of data and information security through the network, transmission and data aspects.

Published by CSP © 2018 the Authors

2.2 The development of Web Service platform security

Foreign research on information and network security started early and had a solid foundation. Many standardization organizations, companies and research institutions are carrying out the Web Service security standards research and protocol development. Among them, W3C and IETF, OASIS jointly developed a set of security norms and standards, such as XML encryption, XML signature, XML key management specifications, which is of great significance for data exchange and transmission of security.

Y.Cheng and P.S.Tan [1] discussed the existing mature security mechanism, such as Circle-of-Trust (COT), WS-Security, W3C XML encryption technology and digital signature, followed by the introduction of the principles of SOA framework and the mechanism built by the SOA-based concept which helps reduce total costs. Mipro explored the security mechanisms of SOA from the perspective of standardization, technology and enforceability. First, the SOA security solutions were summarized, and then the author separately discussed the advantages, disadvantages as well as compatibility issues of Web Service components and traditional SOA architecture.

Domestic Web Service research covers a wide range of industries, but the relevant security research is still in the theoretical research and application stage. Most researchers use the combination of enterprise and external data sharing of special security needs with the existing security technology, to build efficient and feasible process and technical framework, thereby improving the efficiency and security of data exchange.

Pang Shan applied SOAP message extensibility security to XML data encryption and digital signature technology [2], for the purpose of enhancing the security of data exchange in Web Service environment, and propose a method of generating a unique identity with a timestamp or other random function to ensure uniqueness. Based on WS-Security mechanism, the article "Web Service Security Research and Implementation Based on SOAP Protocol" [3] mainly implements the SOAP message security extension and SOAP message monitoring gateway to ensure the Web Service end-to-end security.

Throughout the domestic and international research, we can see that although the security management logic framework is not mature enough, there are many relative application research at home. From a long-term point of view, with the enterprise's technical environment, risk changes, information security needs are changing at any time, the corresponding security strategy and system framework also need to be immediately replaced. This is a dynamic process.

3. Case Analysis

3.1 Port business analysis

The current production system and external data sharing are using a variety of interface programs, especially for Web Service. The external entity and the production business system respectively distribute the data sharing service through the Web Service. When the two-system client performs the addition and deletion of data, the system will convert the data or data request parameters into XML format, trigger the data sharing service of the other party, and send the encapsulated XML data to each other’s Data synchronization work. The overall principle of the interaction mechanism is that both parties take the initiative and trigger interaction with each other.

3.2 Current situation of data-sharing security

The normal operation of the port is inseparable from the coordination between different departments and units of operation. At present, there are some security issues:

•The Web Service messaging process cannot track the user and the message itself, which means that the messaging channel is an open, insecure channel that may face any illegal behavior such as being intercepted or tampered with at any time. The parties to the communication in the network may be fake and cannot guarantee that the user has the information not to be unauthorized access to avoid theft of the user's trade secrets.

•In the unsafe service system, if there are no access or restrictions on method call, it is possible to suffer hackers DoS (Denial of Service) attacks. This is because the hacker can intercept the SOAP message at any time, and then imitate the message or repeat the message itself, which may lead to system crashes.

•The current system deploys Web Service within the Intranet, only called by the business partners. Although the method can effectively separate the internal network from the Internet, but it cannot fundamentally guarantee the confidentiality transmission and non-repudiation, and for the reason that the business partners often come from different product systems, we cannot give full trust.

3.3 Analysis on the security requirement of port enterprises' external data-sharing

•Web Service is not a simply point-to-point topology--SOAP messages can be received, processed or forwarded by the intermediate node, resulting in the risk of leakage or loss of security information. Therefore, to ensure the security of the Web Service data level should ensure that SOAP messages from the issue to the reception of the entire transmission process is safe, that is, "end to end" security.

•Element-level security of VPN or SSL security technology is based on the data flow of the security channel, which means that they take the entire XML text encryption package method. In this process, the intermediate node must decrypt the encrypted message in order to obtain information about whether it is forwarded to the next destination node, which may reveal some important information during the message delivery process, and cannot realize the granular security.

3.4 Security requirements of port enterprise

In this paper, we need to consider the actual data security processing speed, security application model, system architecture and other issues. Web Service security research is mostly based on the SOAP security research. SOAP and XML security technologies can be combined to incorporate content such as XML encryption, XML signatures, and other security technologies into the original message. The difference between XML encryption and traditional encryption technology is that the former can directly transform the serialized message. There are several notable features of the current interfaces design of the port system:

•Different interfaces have different security requirements for different data.

•Port system uses event triggered or timed automatically trigger.

•Port system shares large amounts of data and develops various interface types. The developer should combine the complexity of development and security requirements level, then select the appropriate security processing and encryption algorithm.

SOAP transfers in the form of XML rather than binary encoding. Port enterprises should cope with the relationship between data security and real-time data transmission to make the transmission of information as short as possible, thereby enhancing the transmission efficiency.

Based on the analysis of the existing business processes in the port, the actual security problems in the Web Service data sharing and the security requirements of the enterprises themselves, this paper argues that the method of XML encryption and signature processing of SOAP messages should not be used for the safe handling of data. By emulating the XML security processing framework, this paper uses encryption parameters. For the digital signature, the difference is that it will add some parameters to verify the integrity of the transfer certificate or encryption key, which will be described in detail in the next chapter.

4. Safe Interface Design

4.1 Total architecture design

According to the process of dealing with the message, the original Web Service-based RFID middleware has been modified mainly for the SOAP request message processing functions. The function modules are shown in the following figure:

1) Message routing (listen / forward): Listen to the message, check from the SOAP request message <Header> specified message whether the user is the final receiver, if it is then call the legitimacy of the method of certification and the identity; if not the SOAP message will continue transforming to the next receiver, until find the final receiver.

2) XML schema validation: Determine whether the SOAP message format conforms to the predefined XML Schema specification and filters it to ensure that the incoming SOAP message is valid in format.

3) Authentication and authorization: Obtain a user name security token (UsernameToken) from the node <Header> by XML parsing the SOAP message. Check whether the Username and Password in the UsernameToken exist in the service provider's identity library. If the identity does exist, then grant the matched right to the user (based on the user's attribute information, context information, to determine whether the request sent by the request is granted within the scope of permission, and the implementation of decision-making, that is, to allow/reject SOAP request).

4) Secure processing: Decrypt the encryption key and encryption request message using the key (public / private key), recalculates the signature value, and verifies the message integrity.

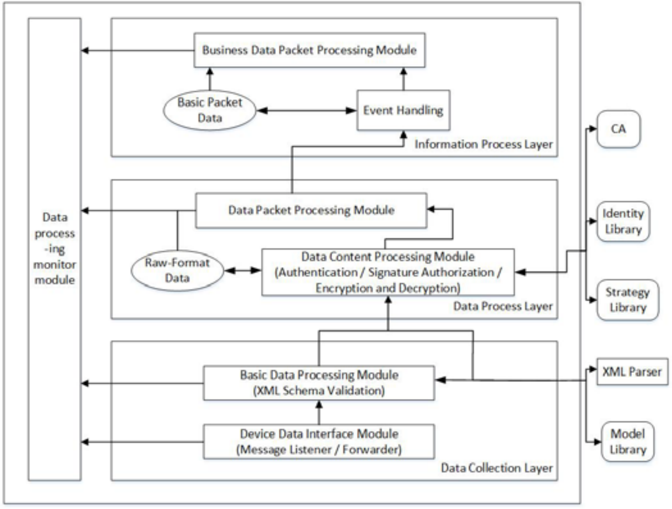
Business Data Packet Processing Module
Basic Packet Data
Event Handling
Information Process Layer
CA
Data Packet Processing Module
Raw-Format Data
Data Content Processing Module (Authentication / Signature Authorization / Encryption and Decryption)
Data Process Layer
Identity Library
Strategy Library
Data process -ing monitor module
Basic Data Processing Module (XML Schema Validation)
Device Data Interface Module (Message Listener / Forwarder)
Data Collection Layer
XML Parser
Model Library

Fig. 1 The security flowchart of RFID accessing Web Service

4.2 Specific module design

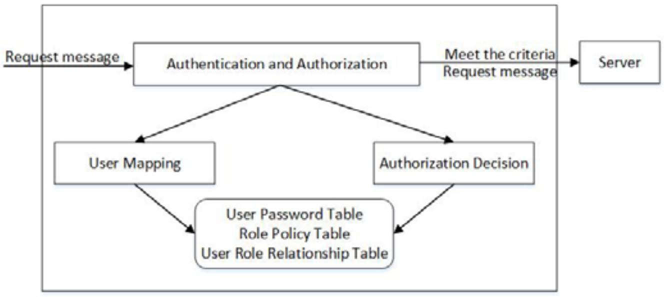

Fig. 2 The flowchart of authentication and authorization

4.2.1 Authentication and authorization

Use Usemame Token for identity authentication and authorization. It is the most common way to verify a user's identity using a username and password. The basic principle is that the user add their own user name and password in the Soap head when requesting. SOAP request side establish a shared password with the SOAP server to verify the legitimacy of the password in order to achieve the function of authentication users.

In order to enhance the security and ensure the security of password transmission in the SOAP packet, we do not use the hash value of the calculated password to send the digest to the SOAP server. Instead, we add Nonce (random number) and TimeStamp (time Poke) for non-reversible encryption operation.

4.2.2 Data encryption and signature

a) Encryption algorithm selection: In this scheme, the data information is encrypted in combination with symmetric encryption and asymmetric encryption. The process can be mainly divided into the following steps: encrypt the original data using symmetric encryption; encrypt the key of symmetric encryption mentioned above using asymmetric encryption; combine all the parameters of information into a string, calculate its hash value, and finally make the signature of the value.

b) Digital certificate: The scheme needs the service requestor and the service provider to use the keytool-genkeypair tool locally to generate their own key pair, then use the keytool-certreq tool to generate a digital certificate issuance request and send the public key to the certification center--Versign. After verifying the identity, the certification center uses the private key to digitally sign the public key and generate the certificate. All the public key exchange must be done in advance.

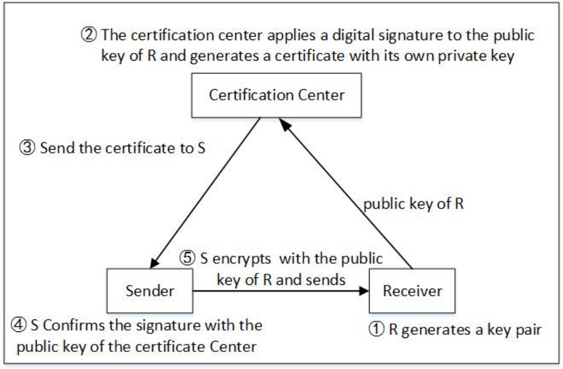
② The certification center applies a digital signature to the public key of R and generates a certificate with its own private key
Certification Center
③ Send the certificate to S
public key of R
⑤ S encrypts with the public key of R and sends
Sender
Receiver
④ S Confirms the signature with the public key of the certificate Center
① R generates a key pair

Fig. 3 The figure of certificate generation, issue and use

When the public key is used for encryption and the private key is used for decryption, it can be used for key exchange; otherwise, it can be used for digital signature. It is necessary to manage any key that is generated and update the key according to the security requirements of the CA or port enterprise.

5. Conclusion

The paper studies the status quo of port development, and puts forward the security problems exist in the present information system when exchanging and sharing data, combining with the security situation of the whole production business system and external data sharing. After deep analysis of the different characteristics between Web Service and other distributed applications and introduction of existing safety standard and mainstream security technology, the paper analyzes the demands of external data sharing security interface system of Guangzhou Port's production business system. Referring to the existing model, the technical scheme of the external data sharing security interface system based on Web Service is put forward, and the preliminary system function is designed. A detailed analysis and design of the functional modules in the framework is made from the aspects of confidentiality, completeness, non-repudiation, authentication and authorization, which can improve the security in the process of Web Service communication and user access control.

References

[1] Y Cheng, PS Tan, Y Cheng, and PS Tan, "Achieving high availability and security of web services for SOA-based applications," SIMTech technical reports, Volume 6, Number 1, Jan-Jun 2005.

[2] Pang Shan, Zheng Qiang, Pan Luping, "Study on Web Services Security Based on SOAP Protocol," Computer and Modernization, 2009 (5): 123-126.

[3] Wang Shiran, Chen Jinsong, "Research and Implementation of Web Services Security Based on SOAP Protocol," Coal Science and Technology, June 2011.

[4] Zhang Hongzhong, "Security Analysis and Application of Web Services in Monitoring and Management of Data Exchange Platform," unpublished.

[5] Zhang Lechen, "Analysis on the Construction of Port Information in China," Science and Technology Innovation and Application, 2014 (4): 50-51.

[6] Wang Fang, "Study and Implementation of Message Layer Security Mechanism in Web Services Platform," unpublished.

[7] GSVRK Rao, "Threats and security of Web services - a theoretical short study & Information Technology," 2004, 2:783-786 vol.2.

[8] K Bhargavan, C Fournet, AD Gordon, CG Kaler, R Pucella, "Checking the security of web services configurations," US, 2005.

[9] Gerić, S, "Security of Web services based service-oriented architectures," Mipro, International Convention, 2010:1250-1255.

[10] H Koshutanski, F Massacci, "A Logical Model for Security of Web Services?" First International Workshop on Formal Aspects of Security&Trust Istituto Di Informatica E Telemetica, 2003.