Security in Service Oriented Architecture

Sun Jian
Helsinki University of Technology

Abstract. This report is on security of Service Oriented Architecture. It briefs the concept and features of SOA, reviews the solutions and recent researches on this field, summarizes the security methods from several levels - data, function as well as software process. The report intends to present a general picture on SOA security, introducing the major status and facts about it with the author’s understanding. abstract environment.

Key words: security, service oriented architecture

1 Introduction

Service Oriented Architecture (SOA) is becoming more and more popular with the development of Internet. While SOA is adopted by more applications, the security on SOA also becomes a bigger concern. This report reviews the literatures on SOA, especially on its security aspects, and summarizes some major solutions, research progresses as well as open issues on security in SOA.

1.1 Background

Traditional software needs a single point of control. In a standalone application, the application itself is the controller. In applications with Client/Server (C/S) architecture, the server is the controller that handles all the requests. Internet has opened opportunities of distributed applications that no one is the central control point in the whole software. In stead, the application in one system can request the resources in other systems without a central management server in the network. Service oriented architecture provides such a framework.

SOA has changes the software development and usage in many aspects, and it has brought many new areas in research and development. As SOA requires the application to work across the open Internet, security is one of the key fields in SOA.

1.2 Objectives

In this report, the author intends to achieve following goals:

1. Familiarize with the SOA technology and usage scenarios.
2. Understand the major security concerns over SOA.
3. Identify main solutions on security of SOA.
4. Summarize some new progresses on the SOA security researches.
5. Discuss the features and trend on SOA security, identify some pros and cons.

In short, the objective of this report is to present a general picture of SOA security from the author’s understanding.

1.3 Scope of the Study

The scope of this study is limited by following dimensions:

– Only the security aspects of the related materials are reviewed
– Universally accepted standards and specifications are used as primary source as existing solutions
– When studying the new progresses, only the papers in last few years are reviewed

Such limitations can provide authoritative information as well as real recent developments.

1.4 Methodology of the Study

As the nature of this report is an introduction and summarization, the methodology used in this study is mainly literature review. The approach is to search in digital libraries to find a group of good references, then some of them are used as main papers and further reading are based on the links and references from these papers. Websites of some official organizations which handles the standardization, etc. are surfed to acquire first hand information on the standards and specifications.

1.5 Structure of the Report

The report contains five parts:

1. Section 1 introduces the background, objects of the study as well as the scope of the study and the methodology used.
2. Section 2 gives technical overview on SOA, including its features and what are the major security concerns over SOA.
3. Section 3 describes how the security issues are handled in SOA. It includes both the accepted solutions that are widely used and the new proposals that further enhance the security.
4. Section 4 reflects the study and states the author’s opinions on this topic.
5. Section 5 summarizes the study and the report.
2 Overview on SOA and Security

SOA is not a totally new technology. It has evolved from the early distributed architecture, such as DCOM and Object Request Brokers (ORBs) based on the CORBA specification. [2]

2.1 Definition on SOA

There are several definitions on service oriented architecture. Website specializing on SOA www.service-architecture.com defines SOA as “essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed” [2]. Eric Knorr and Oliver Rist wrote in 10 steps to SOA that “SOA is a broad, standards-based framework in which services are built, deployed, managed, and orchestrated in pursuit of new and much more agile IT infrastructures that respond swiftly to shifting business demands” [8]. SOA is “a way of sharing functions (typically business functions) in a widespread and flexible way” [15].

2.2 Features of SOA

While there are different ways of expressing the SOA definitions, the key concept in SOA is service. According to www.w3.org, service is that service providers provide a group of works to deliver the results needed by the service consumers. Generally the result will change the status of the service consumers, but sometimes it may change the status of the service providers, or both.

SOA has following features: [9] [15]

– The service is accessible from external of the enterprise, i.e. the service is open on Internet.
– The service is loosely coupled, i.e. service interfaces are separated from implementation. For example, a service can be implemented with .NET or J2EE and the service consumer can also have different implementations.
– The service interface is coarse-grained, i.e. an interface provides a set of functions instead of a single one.
– The data presentation is neutral, i.e. the data format is independent on the implementation. In practice, XML is a commonly accepted neutral way of presenting data and is the standard in SOA.

There are other features such as Quality of Service, standard interface, etc. The features described above are related with security concerns.
2.3 Security and SOA

Security is always a concern for software. Security is especially important for SOA as most of IT security are human-computer interaction but SOA security is machine-to-machine interaction. [19]

Although SOA has various advantages over the client/server architecture, security is more challenging for SOA. With C/S, the authentication and authorization can be managed by the server, generally with a database at the backend. Security can also be handled at the client side, such as using the workstation's identity for single sign on (SSO). Such central authentication and authorization are not possible for SOA as SOA by nature is distributed.

The main fields of SOA security are from the features of SOA: on the data presentation, XML is used widely as data format, such as in Simple Object Access Protocol (SOAP), the concern is how to guarantee the data is not forged or modified and its integrity; Distribution of the application raised the question such as how to trust, authenticate and authorize the peer side, etc.

Epstein et al emphasize that the security software is not enough for software security solutions. They hold the view that most of security risks are related with management and engineering process. On the technical side, security software such as crypto is not sufficient to make SOA secure. [7]

3 Security Solutions and Challenges

This section will review standards and research progresses on the major security field of SOA security.

3.1 Atomic Level

A common way of protecting data from being attacked is to use secure way of transportation, for instance, transporting SOAP message over HTTPS instead of HTTP. However there is still concern that the data can be modified before entering the secure channel or after leaving the secure channel. The end-to-end security on data message is needed. XML is the data presentation format for SOA, the atomic level security for SOA is XML security. [20]

Security Standards Security on XML was received attention from early days and there are standards defined on it.

XML signature is to sign the XML document digitally to guarantee the integrity and authentication of the sender. In addition to the common digital signature which signs the entire document, XML signature allows to sign portions of a document. When verifying the XML signature, first the signature is verified with public key. Then the digests are calculated and compared to verify the document. [22]

Similar to XML signature, XML encryption can encrypt parts of the documents in different ways, which is beyond the capability of secure transportation.
With this XML encryption allows different parts of the document to be read by different receivers. [18]

XML signature and XML encryption are included in the standard WS Security published by the OASIS \(^1\).

**Vulnerability and Proposed Solutions** The vulnerability of these standards are due to the flexibility of the XML that the data is identified by the tags and the sequence is not important. In calculating digest, a small change of sequence can cause different results, but in XML they can mean same contents. To overcome the effects of free formatting on calculating digest, *XML canonicalization* is proposed to reformat the data based on some requirements. [18]

As for XML encryption, if the encryption parameter comes later, the buffer needed can become the target of denial-of-service attack. Encryption data and encryption key may reference in an endless loop, which is called recursive processing attack. [18]

*XML rewriting attack* is the general term for “the attacks based on the malicious interception, manipulation and transmission of SOAP messages in the network” [20]. Rahaman et. al. recognized one type of XML rewriting attack that bogus elements can be added to the XML message while the signature remains unchanged, because the reference URI keeps the same value. They proposed the concept of “SOAP Account” which keeps the record of the element structure of the SOAP messages, including the number of child elements of root, the number of header elements, the number of references for signing element, the predecessor, successor, and sibling relationship of the signed objects. [11]

While SOAP account can resolve the bogus element issue, attackers may forge SOAP account in a similar way. The researchers further addressed the attack on SOAP account in their next work. They proposed to introduce the module “CheckSOAPAccount” to validate the signature of the SOAP account. These works solved this type of attack but the efficiency is not fully studied. [20]

### 3.2 Function Level

In additional to the message security, the service security is protected by proper access control to the functions, such as authentication and authorization. SOA has access control policy to make sure the consumer are allowed to use the service.

**Security Policy** *Policy* is a logical predicate that determines which message parts must be present, signed, or encrypted. It is a “propositional formula with disjunctions and conjunctions built from any set of base assertions that define predicates”. The presence of message parts are listed in *message predicate*

---

assertion. Digital signature is required with the integrity assertion. And the encryption is required for the parts listed in confidentiality assertion. [4]

WS Security Policy, published by OASIS as a part of WE Security, specifies how to permit certain consumers to some services, as well as the authentication methods and the encryption level.

**SAML, WS Trust and Federated Authentication** Access control handles authentication and authorization in SOA.

*Security Assertion Markup Language* (SAML) is a product of OASIS originally designed to solve single sign on problem. SAML assertions include authentication statements, attribute statements and authorization decision statements which defines the contents but not the methods of transmission. At the server side, *eXtensible Access Control Markup Language* (XACML) is used to represent access control policy and decisions. A XACML access control model has four components: policy enforcement point, policy decision point, policy administration point, and Policy information point. [10][14][16][18].

SAML is the important component in security standard *WS-TRUST*, published by OASIS [12]. Another standard, *WS-Federation*, is more closely integrated with other web service standards and is supported by Microsoft in Windows operating systems [6]. These two major standards are not compatible to each other.

**Developments on Access Control Policy** On the field of access control policy, many new developments were designed and proposed.

*Attribute Based Access Control* (ABAC) is developed based on XACML which defines the policy rules on subjects, resources and their environments. It allows the access control policy to be refined more accurately [18]. Using XACML and ACML, Lamb et. al. designed a role-based access control in which users can connect to data sources but are only allowed to the part that they need [10]. Alam et. al. argued that one key factor to successful usage of SOA is to have sophisticated semantics model to represent and communicate data and proposed the semantics-aware Web services in a secure framework [1]. Nair et. al. proposed to use Trusted Platform Module (TPM), a hardware chip for trusted computing, to enhance the security with federation management [13].

To avoid the errors in security policy configuration and security files, Bharagavan et. al. developed an advisor which can test, model and formally analyze policy-based services and clients. The tool can be used as part of installation in Windows Security Enhancement. [4]

### 3.3 Engineering Level

The security of SOA can not be solved just with one or two techniques. To build secure SOA applications, the engineering process should take the security considerations into design, implementation, management and maintenance, etc. [7]
Distribution of Security Responsibilities  As introduced above, an important way of protecting SOA services is to restrict the access. Traditionally, the access control and firewall are responsibilities of network administrators. Security solution on SOA may require a closer cooperation between network administrators and software engineers, as well as a clear division of responsibilities between them. [5]

Bunge et. al. designed an operational framework that serve this purpose. The access control operations such as authentication and authorization are generally performed at the network edge supervised by the network administrators. To perform the control over SOA traffic, the devices and applications in the network firewall need to be aware of the XML. XML firewall was proposed but not well accepted by the industry. These researchers proposed a framework called Filtering to Inspect XML (FIX) which facilitates analysis, modeling, planning, discussion and deployment of security system. Tectonically, FIX contains a group of techniques such as authentication, authorization, accounting, validation, verification, encryption, decryption, etc. The framework uses different filters for different scenarios and the complexity of security design and related network operation is reduced. [5]

Process for SOA Security  Betancourt explains how to implement SOA security projects, especially for large projects. [3]

The person responsible for SOA security is suggested to be the security enterprise architect (SEA), who is on the SOA governance board and works together with enterprise architect to ensure the security requirements are considered in the architectural design. The key steps for implementing SOA projects include maintaining SOA enablement security decision matrix, identifying risks from both business and technical perspectives, finding out internal and external stakeholders, collecting requirements with right tools, etc. According to him, the SOA security project should follow a software process model, such as waterfall. Only in the late stage that technical details come into the scene — the standards of WS-Security. [3]

Schaad also holds the view that system security is more than just installing security applications or adding security functionalities/components and configure them. Many security problems are due to errors in design and implementation and the solution is to improve the engineering process, especially in architectural design and implementation. Next to this, the security problem occur because of users and administrators using insecure settings and configuration. These need to be resolved from process improvement instead of pure technical side. [21]

When discussing security, people think there is no 100% security, not only due to complexity and challenge in technique, but also because of cost. A typical price for security is system performance, especially security is handled remotely. Remote authorization can cause 70% performance degradation. Security also requires investment in development, deployment and maintenance. In the real world, security is always in trade-off with risks, i.e. security is in high priority only when the risks are not tolerable. [17] [21]
4 Discussion

SOA security receives more and more attention with the growth of SOA applications. The security solution of SOA involves several levels, from the atomic data level, programming function level to the engineering level.

At the low level, the security is solved with standards. Though there are vulnerabilities found with standards, overall speaking, the security solutions are mature and used extensively.

At the programming function level, the solution is maturing but not fully standardized. There are different standards proposed and supported in different applications. The compatibility affects the universal access to the service.

The major challenge on SOA security is from engineering process. Security can not be solved by simply applying one technique. It needs people from all sides, including design, programming, management, administration, maintenance, etc. to be involved. Project management and system architect need to be aware of security risk of SOA; the proper technical solutions need to be taken into design and implementation. In organizations, security issue is commonly handled by IT departments. To meet the challenge of SOA security, traditional IT engineers need to grasp the knowledge of SOA; on the other side, the SOA security solution need to be easy to use by IT departments.

Usability also affects SOA security. The security configuration and settings should be easy to use so that customers and providers will not introduce human errors causing negative effects.

Security does not come for free — efficiency is a common price for security. Efficiency and performance are especially sensitive to security functionalities and enhancement. How to provide just enough security without much overhead us an open issue.

5 Conclusions

In this report, the author has reviewed extensively the documents and files for security issues in service oriented architecture, and summarized the major achievements and progresses, including standards, research papers and other reports and practices. It shows SOA security is gaining more attention in the IT world and it has become one hot topic in SOA.

The security concerns on SOA is mainly from its nature of distribution and its appliance of XML messages. Numerous efforts have been spent on establishing security on SOA applications. Among all the factors, standardization, usability, process improvement are keys to successful SOA security.

References


