Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.3 No.2, 2014, pp.40-46

DOI: https://doi.org/10.51983/ajcst-2014.3.2.1737

Collaborative Security Framework for Service Based Systems: Issues and Solutions

R.Kamatchi
K.J.Somaiya Institute of Management Studies and Research, Mumbai
E-mail: ka_iyer@yahoo.co.in
(Received 13 September 2014; Revised 30 September 2014; Accepted 16 October 2014; Available online 24 October 2014)

Abstract - **The Service oriented architecture is evolving as a new technology, which is currently adopted by many fields like Healthcare, Educational sector etc. It is highly adoptable with web services as an interoperable technology. There are various security mechanisms proposed for the individual security issues which works independently. This paper is providing a collaborative security framework for the implementation of Service Oriented Architecture with web services and analyzing its Security benefits .This paper adopts the Survey of concerning literature, Experience survey, Analysis of examples under the exploratory method as a research model to explore and develop a collaborative security model. The paper provides a complete security model which analyses the various conditions like no service availability, services with partial security services. This model also provides the security as service solution to the security requirement problem arises with the best match services. This collaborative model addresses the major security issues.**

Keywords: Service Oriented Architecture, Service Provider, Security broker, Matchmaker, Security Framework

I. INTRODUCTION

The seamless interoperability characteristics of web services also introduce security concerns that do not exist in traditional distributed messaging techniques like RMI and CORBA. This is because of the reason that the SOAP based XML messages are not firewall proof and this could lead to intruders gaining access to sensitive systems using the interfaces provided by the WSDL files for service access.

Moreover, traditional websites designed using non-SOA frameworks allow users to interact with an application remotely through a web browser but a web service allows other applications to interact directly with it. This makes the web services more vulnerable to security problems.

To prevent the system from the major part of the security problems, the combined collaborative security mechanisms are required to be implemented. The first section of this paper is discussing about the various security components used in this holistic approach. The second section is describing the detailed flow of operations involved and the final section is providing the algorithm for the implementation of a collaborative security framework.

II. BACKGROUND STUDY

The extensive literature survey performed related to the Service Oriented Architecture and the security issues pertaining to the same. The Amelia study [1] explains in detail about the extensive requirement of authentic services in Educational system for ensuring the identity of true services in the open web environment. The Eric Pullier [2] chapters describe the enterprise service oriented environment. The WSDL files are the vulnerable point for the attackers to hack the sensitive information. The malicious user may gain access to the WSDL locations by querying the UDDI registries and the details may be used for enumerating and profiling a web service. This kind of several security issues are handled individually by the implementation of Authentication service, Single Sign on etc. The extensive study reveals the fact that the single security framework which can address most of the security issues would be more practical with the current business scenario. The main objective of this paper is to provide a collaborative security framework and to validate the same with a case analysis.

III. SERVICE ORIENTED ARCHITECTURE

SOA is a new computation technology, not only satisfies user's application needs, but also included service broker and service provider interaction. All these are related to standard SOA. [3] The SOA can add flexibility to system architectures, as it is possible to describe a service rather than the set of separate systems that provides the parts required to complete a task.

Basic components and functionalities of SOA:

Basically The SOA contains two parts

1. Service
2. Connections

A. Service

A service is a function or some processing logic or business processing that is well-defined, self-contained, and does not depend on the context or state of other services. Example of simple Service is Loan Processing Services, which can be self-contained unit for processing the Loan applications. Other examples may be Weather Services, which can be used to get the weather information. Any application on the network can use the Weather Service to get the weather information.

B. Connections

Connections means the link connecting these self-contained distributed services with each other, it enables the client to Services communications.

SOA contains three main components

1. Service Client
2. Service Provider
3. Service registry

These components must use standard text formats familiar to both the service provider and the service client to enable provision and use of the service.

IV. SECURITY PARAMETERS

The security parameters can be defined into the following two categories [4] [5].

A. Functional aspects of security

a. Authentication—verifying identity of users.
b. Authorization— deciding whether or not to permit action on a resource.
c. Data confidentiality— protecting secrecy of sensitive data.
d. Data integrity— detecting data tampering
e. Non-repudiation -- making sure neither the sender nor the receiver can deny the message they sent or received.
f. Protection against attacks—making sure attackers do not gain control over applications.
g. Privacy—making sure that the application does not violate the privacy of the users.

B. Nonfunctional aspects of security

These aspects are nonfunctional in the sense that they do not directly relate to security. Instead, they are required to make sure that a security solution works well in an enterprise setting.
These are:
a. Interoperability—this concern is specific to SOA, where different security solutions must not break compatibility of services that are otherwise compatible.
b. Manageability—this concern is bigger for SOA, as a security solution needs to protect many different services.
c. Ease of development—this concern is common for any security solution. Be it SOA or traditional application development, complexity reduces adoption of any security solution.

V. SOA SECURITY

1. Content level: This level of security protects the content such as information and services in store or in transit.
2. Communication level: This level provides end-to-end security between communicating nodes. Security services include data origin authentication, confidentiality and integrity verification. This includes the communication link between the client, service provider and the service registry.
3. Network level: This is concerned with protecting the network infrastructure and includes services such as access control and denial – of – service protection. This encompasses the whole architecture of SOA.

Under these categories various security solutions can be applied independently to ensure the security aspects.

A. Security Concerns:

The major security concerns are like security rules created with the firewall for the filtrations. This may put a restriction on the requestors or consumers in such a way that it will accept only requests or the web services with some specific characteristics. The composition of web services contributes to the formation of a complete process. So, the data delivery among the services is also playing equally an important role. This data delivery and the usage has increased the security constraints among the services. Compatibility among the web services makes the service composition process simple and flexible.
The service transactions among various applications have raised the need for the support of a security conscious composition of web services. To have security compatibility among the services, the following requirements are to be fulfilled.

1. The language to express the constraints
2. A service can do the process of matchmaking.

The services provided by the SP will be having certain security mechanisms described by the creator. The services requested by the consumers will be having certain security specifications. The security parameters of the services participating in a process should be compatible with each other to have a smooth flow of process execution. This compatibility checking can be performed into two classes.

1. Security capabilities
2. Security constraints

.

B. Security Capabilities*:*

This describes the security features of a particular web service which includes the strategies and the techniques. Each and every web service needs to have a security features embedded within it. These parameters can be specified by the security policies.

C. Security Constraints:

The security constraints are specified by the consumers during the utility of various services. These constraints can be classified into three categories

1. Compatibility constraints: These are the constraints which is required for the association of related services. These are the set of rules which needs to be imposed on other services in order to have smooth association of various services to invoke a particular process.
2. General constraints: These are the general conditions required for all the services participating in an activity. For example the X.509 certification can be made mandatory for all the services involved in the process of Examination.
3. Final constraints: These are the conditions required for the final output of a particular process.

The security constraints with compatibility parameters will be included in a WSDL document. This information will be stored in the extension fields of WSDL document. The required constraints by the consumers will be specified in the SOAP messages. This constraints requirement will be

submitted to the broker. This broker which is a web service on its own can be utilized by any application which needs to perform the security process choreography.

VI. SYSTEM COMPONENTS

The components involved in this model can be separated into two categories

a) Security broker
b) Security service components

A. Security Broker:

The security broker is similar to the middleware which is placed in between and evaluates the security constraints and helps the services to smoothly participate with the process choreography. [6][7]

(I) Modeler: The modeler receives a service description as an input to refer to the final web service. It does the following

1. Models the business process
2. It prepares the workflow
3. It identifies the set of services to perform the activities and reads the relationship among them.

(II) Locator: The services required to perform the activity will be spread across the network. That needs to be identified and accumulated to perform the process. The locator takes the description from the modeler and performs the location identification.

(III) Matchmaker: The security constraints will be analyzed and the security matchmaking composition will be prepared by the matchmaker. This will read the compatibility constraints and the security constraints specified with each service. Then it will map the services compatible with each other into a single flow. Each process will be in need of an initial service to accept the input from the consumer and one final service to produce the required output. The initial service will accept the input and perform the activity and forward its output as an input to the next activity in the sequence. While forwarding the output it will also forward the security constraints and compatible constraints specified with the same. [8][9]

B. Security Service Components*:*

(a) Authentication service: This service is responsible for the authentication of the service requested by the consumers. This authenticates the originality of the services requested.

(b) Authorization service: This service authorizes a particular service requested by the consumer with respect to its originality and the access rights that consumer has about the same service.

(c) Access control service: This service describes the access rights of the user on the requested service.

The service access requested by the consumer will be authorized only when the above mentioned three services return an OK message to the requestor. Then the complete access will be approved.

(C) Federated interface:

The federated interface contains the details about the user credentials and the access rights information passed on through the same. This will be useful with the COI (Community of Interest) groups wherein the boundary of the user groups is definite and their service access must be similar with maximum retrievals. [10][11].

(d) Proxied interface:

This interface helps the user to hide his identity in the communication and also does the process of filtering as when required.

VII. PROCESS ALLOCATION ALGORITHM

The following algorithm explains the detailed steps involved with the service modeling process. The process invoked by the user in turn, invokes various services corresponding to each and every requirements specified. As a whole a single process can be invoked and framed together to create a whole application.

S1: Services Si, i = 1….n will be defined and the process requirements Ri, I = 1….n will be collected wherein the i defines the parameters defined by the user and the service specifications.

S2: Workflow preparation:

a) Requirements gathered from the user will be compared against the service specifications in the following way.

b) Sij, i, j=1…n will be compared with Ri to identify the specific service. Assign a new variable n with 0.

Sij = Ri then n=n+1;

c) The service with max (n) and higher performance will be identified.

S3: Security modeling (SM):

Sij, i, j=1…n which are identified by step2 will be modeled to Pi, i=1...n. Pi defines the processes involved in a single application. The individual services Sij are the set of activities which will be performed sequentially to achieve the desired outcome.

S4: Matchmaking

SM → SCA (Security Capability Authority)

To compare the compatibility constraints of the services with the user requirements. Assign a temporary variable m with 0.

a) Rci = Scij wherein i, j = 1. n, (i = security parameters like privacy, confidentiality etc.) Then m=m+1.

b) If the maximum of n is identified and that single service will be identified and assigned to the individual activities of the process list.

c) Pi=Sij i=1…n.

S5: Session ID exchange

C----- → AS thru PI, wherein
C = client
AS = Authentication Service
PI = Proxied Interface
Client (session ID)

S6: Key exchange:

a) C ←----→ AS thru PI
b) PI--- → cache the data for filtering

c) FI ---- → Stored the data for federation.
S7: C--→ AS (Encrypted credentials)
AS--- →FDB (Federated Database)
(Client ID, Credentials)
If data verified to be true then go to step8 or display error message.
S8: AS --- →C
(Service token, OK)
S9: C --→ SP
(ST, SN, ID)
S10: SP---- → AS
(ST, SN)
S11: AS --→ AAS (Authentication & Authorization Service)
(ST, ID)
If authorized go to S12 else display error message to SP and go to step 7.
S12: AAS -→ ACS (Access Control Service)
(ST, SN)
If access rights are yes then go to step3 or display "Access denied" message to SP.
S13: ACS --→ SP
Access permitted
SP -→ FI
To store the authorized user details
SP --- → Client
To invoke the services.
S14: Go to step 9 to invoke the next service in the workflow.
Detailed description of the steps involved:

Step1: Process choreography:
a) Each and every process is a collection of services belonging to various service providers. First the identification of needed services will be done.
b) The needed services may be belonging to different service providers with their own security aspects. This should be verified before the access. The identification may be carried out with the requirement specification mentioned by the consumers.

Step2: Workflow preparation:
a) The service specification by the client will be handed over to the browser.
b) The services satisfying the maximum requirements specified by the consumers will be identified. The services satisfying the above mentioned criteria may be more in number. All services with the specification details will be identified and accumulated.
c) The services based on the activity will be accumulated and the tree structure of the same will be prepared. This tree structure will be containing the service which satisfies the maximum requirements will be in higher priority and followed by the nodes in decrement order of requirement specifications.

Step3: Performance analysis
a) The set of services will be analyzed and the services with the maximum performance attributes will be identified. Each and every service definition assures a specific percentage of the performance level. This is specified with the policies of the same service.
b) The performance parameters can be verified from the WSDL extensions of the corresponding services.

Step 4: Security modeling
a) The services identified by the locator from the service registry will be narrowed to the actual service after the performance analysis. A single service for a particular purpose will be identified. In the same way the complete activity list will be replaced with a specific service.
b) The service requirements specified by the consumer will be containing the security capabilities and the security constraints. At the same time the service description also contains its own security constraints which will be verified against the requirements specified by the consumers.
c) The modeler will prepare the final workflow model with the services which satisfies the initial and the final constraints.
Step 5: Security matchmaking

a) The workflow model prepared by the modeler will be handed over to the matchmaker in order to verify the compatibility constraints. The services belonging to a single workflow should work sequentially to provide a complete solution to a process defined.
b) The SCA (Secure Capability Authority) is in charge of evaluating web service security capabilities. Based on its evaluation, it will issue signed SAML assertions certifying such capabilities.
c) The compatibility element present with the WSDL extensibility element will be verified and the final workflow tree will be prepared and stored with the database.

Step 6: Session ID generation:
a) Once the complete workflow is prepared will be stored with the EIS database in order to execute the process. All the services involved in the workflow will be executed sequentially.
b) The process execution will select the first activity in the workflow and the corresponding service name will be taken from the server database.
c) Now the client will send an ID for invoking the session with the server. This ID will be sent to the Authentication Server (AS) through proxied interface.

Step 7: Proxied interface:
a) This interface will help the clients to contact the server with hiding the user details. This interface will communicate with AAA server on behalf of the clients and the replies can be forwarded to the clients back.
b) This interface can have the filters in order to verify the incoming and outgoing SOAP messages. The SOAP messages with unauthorized access or identity can be filtered.

Step 8: Key generation process

a) This process will happen between the consumer and Authentication Server (AS). The key generated by this process will be used for the encryption and decryption of the credentials transferred between them.

b) The set of algorithms are available with the security as a service (SAS) component which will avoid the mismatch among the algorithms used by the consumer and the authentication server.

c) By using any of the available cryptography algorithms, the key will be generated and exchanged between the consumer and the Authentication server (AS).

Step 9: Token generation process

a) Client requests for the token from the Authentication service in order to start the session. But for producing the token, the AS is in need of the user credentials which describes the details about the user.

b) The client details are verified from the federated database which contains the details about the registered services and the users.

c) After successful verification of the credentials, the token will be generated and can be used for the complete execution of the activities present with the workflow. But this token will be applicable only for that particular session. For the new session, once again the complete process of key generation will take place.

Step 10: Federated Identity:

a) As soon as the user submits their credentials for verification for the first time with the AS, those details will be saved with the federated database.

b) In the same way the registration of services will keep a cop o the service details from the WSDL file (service name, creator, security parameters) etc with the federated database.

c) The federated database will be used every time whenever the registered user and the service are accessed.

Step 11: Service invoke:

a) Once the token is received by the user, and then the services can be invoked directly based on the workflow details stored by the matchmaker.

b) The consumer will provide the token details, service name to the concerned service provider.

c) The service provider is required to verify the identity and the access rights that the consumer is having with the requested service.

Step 12: Authorization:

a) The service provider will send the details of the user and the service requested to the authorization service.

b) The authorization service will verify the user credentials stored in the federated database against the details provided by the service provider about the consumers.

c) If the details are verified and approved then the user will be authorized to user the specified services.

Step 13: Access control:

a) The details about the service will be forwarded to the access control service to verify the rights to the users on the requested service.

b) If the service is having complete access to the users, then the service access will be allowed to the corresponding user.

c) This access rights acknowledgement will be stored with the proxied interface. So, that the further access can be monitored and filtered based on access rights provided to the same.

S14: Termination

a) Once the complete session gets over then the token will be discarded and the new session will start with the session ID request.

b) Each session will execute a complete process which executes a collection of services sequentially.

VIII. PROCESS DIAGRAM

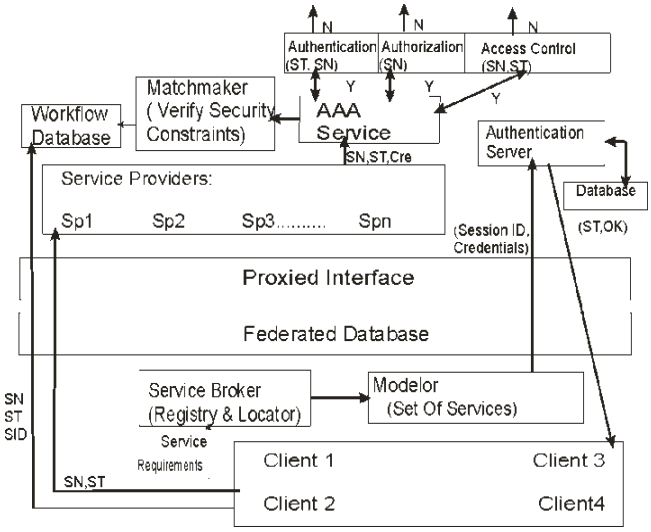

Fig 1. Security framework

The above mentioned diagram is clearly indicating the collaborative security model wherein the Authentication, Authorization and Availability parameters are fulfilled by the AAA service. The confidentiality parameters are fulfilled by the proxied interface with the usage of cryptographic techniques. The federated database provides the access control. This collaborative security framework provides the complete security solution to the Service Oriented Architecture.

IX. FINDINGS

The above mentioned diagram provides the collaborative security solution to the main security issues listed in the beginning of this paper. The security benefits can be listed as:

Issue: Authentication
Solution: SSO
Functionality:

1. The single sign on interface allows the user to have a single entry point through which the communication between the consumer and the service provider will be performed. The complete session is authenticated and approved.
2. The service token is generated for each session.
3. Every session completely starts with a new session ID and the service token.
4. The service token for a particular customer is different for different sessions to avoid the duplication or the security breach of the tokens generated by the Idp.
5. The tokens are known only to the Service provider and the token generator (AS), other than the client.

Issue: Confidentiality
Solution: Encryption & Decryption
Functionality:
1. Each and every message transaction among the client, Authentication and Authorization service with the Service Provider is encrypted before the transaction.
2. The key used for the encryption is generated newly for every session and discarded after the session gets completed.
The same client with the same service access in different sessions is initiated by different session id and followed by a unique key and preceded by the service token provided by the Authentication service.
3. The credentials are encrypted and sent through the proxied interface to get filtered and decrypted only at the receivers end in order to maintain the confidentiality.

Issue: Access Control
Solution: ACS
Functionality:
1. Each and every authenticated service can be sent through the Access control service in order to provide the access rights to the clients with the requested services
2. All the user credentials are verified with the federated database and the approved clients and the services are only passed through the ACS in order to ensure the access rights.
3. This will limit the user access towards the services by which the unauthorized usage of services can be avoided.
The Services registered with the federated database are only being allowed to pass through the ACS.
4. This helps the service creator to hide the confidential data from the user access and also enables the user to have an access only with the authorized services.
5. The ACS and the AAS are working hand in hand to ensure the reliability and the authority of the services.
6. It enables the service providers to provide only the authorized resources to be made available to the client.
7. Even though the user credentials are approved, the session can be denied when the authorization is not permitted.

Issue: Compatibility
Solution: Matchmaker
Functionality:
1. The compatibility constraints are stored into the WSDL extensibility element which will be compared against the requirements specified by the user.
2. The security constraints must be matched against capabilities issued by a SCA.
3. The locator and the modeler proposed in the EIS system are only identifying the services which can satisfy the user requirements without analyzing the core security functions.
4. The matchmaker compares the general, final and the compatibility constraints. Once the compatibility constraints are verified then the final web service is identified and allocated to the activity.
5. Wherever the compatibility among the services is could not be achieved, then the usage of SAS (Security as Service) can be made and the required security parameters can be implemented.

Issue: Privacy
Solution: Proxied Interface
Functionality:
1. The entire communication is happening through the proxied environment in order to preserve the identity of the consumer and the service provider.
2. This helps the entire system to avoid spoofing attacks and the sniffing attacks. This is also avoiding the duplication of services. As the original information is handled by the proxied interface, the originality is not revealed to any of the users.

X. CONCLUSION

The proposed model provides the holistic security approach for the service modeling process which involves various security measures like authorization, authenticity, access control, message transparency etc. The implication benefits of the proposed algorithm were tested with the case of Education Information System and the implication benefits were realized under e-learning and virtual learning methods. This collaborative mechanism can create a secured seamless working environment for the Educational Information System. This complete process should be handled with each and every service identification and process correlations by which the complete process choreography can be secured.

REFERENCES

[1] Amelia Maurizio, James Sager, "Service Oriented Architecture: Challenges for Business and Academia ", Proceedings of the 41st Hawaii International Conference on System Sciences – 2008, pp. 1-7.
[2] Eric Pulier, Hugh Taylor, "Understanding Enterprise SOA", Manning Publications CO., 2006. Pg. no. 23-25, 139-150.
[3] Amelia Maurizio, James Sager, "Service Oriented Architecture: Challenges for Business and Academia ", Proceedings of the 41st Hawaii International Conference on System Sciences – 2008, pp. 1-7.
[4] L.Cherbakov, R.Harishankar, S.Kalyana, "Impact of service orientation at the business level", IBM Journal, Volume 44, Issue 4, pp. 2.
[5] Pascal BouNassar, YouakimBadr, "Towards Integrating Security Services in e-learning Platforms", IEEE 978-1-4244-3834-1/09, pp. 573-576.

[6] “SOA Security”, RamaRao Kanneganti, Prasad Chodavarapu, Manning Publications Co, ISBN: 1-932394-68-0, pp. 08-09.
[7] “Forming a Security Certification Enclave for Service-Oriented Architectures”, Proceedings of the IEEE Services Computing Workshops (SCW’06), pp. 1-8.
[8] “A Distributed e-Education System Based on the Service Oriented Architecture”, 2008 IEEE International Conference on Web Services, pp. 791-794.
[9] “A security framework for service oriented architectures”, 1-4244-151 3-06107, IEEE, Pg.No.1-6.
[10] “Introduction to Web service architecture”, K.Gottschalk, S.Graham and J.Snell, IBM Journal, Volume 41, Number 2, 2002, pp. 3, 4.
[11] “A Service Oriented Architecture Framework for Collaborative Services, IvarJørstad, SchahramDustdar, Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE’05), pp. 1-8.