ISSN 2047-3338

A Study on Secure and Efficient Access Control Framework for SOA

Anu Soosan Baby[1], Deepu Raveendran[2] and Aswathy Josephine Joe[3]
[1,2,3]SCSE, VIT University,Vellore, TamilNadu, India
[1]anusoosanbaby@gmail.com, [2]deepu.raveendran71@gmail.com, [3]aswathy.joe@gmail.com

***Abstract*– One of the major problems in Service Oriented Architecture is ensuring a secure infrastructure environment. SOA play a major role in providing security standards for the web and hence there is intensification in the need for developing a secure framework. The major objective of this review is to analyze various frameworks for Service Oriented Architectures, to compare and contrast its pros and cons. The paper discusses various security threats and vulnerabilities an SOA can have in today's scenario and also various security services offered by SOA. The paper finally comes with a proposal of secure SOA framework model.**

***Index Terms*– SOA, Authorization & Security Service, Authorization Service and Intelligent Data Mining in SOA**

I. INTRODUCTION

THE Service Oriented Architecture is defined as an open, agile, extensible, federated and composable architecture comprised of autonomous QoS capable, vendor diverse, interoperable, discoverable and potentially reusable services implemented as Web-Service for organizing and utilizing distributed capabilities that may be under the control of different ownership domains [1]. SOA can establish an abstraction of business logic and technology which provides loose coupling between these domains [2].

An SOA block can either acts as Service Provider or as Service Consumer. The Service Provider creates a web service and possibly publishes its interface and access information to service registry. The provider also has to decide what category of service should be listed in for given broker service and what sort of trading partner service are required to use the service. The Service Consumer or WS-Client locates entries in broker registry using various find operations and then binds to Service Provider inorder to invoke one of its services. Whichever Service the Service Consumer needs, they have to take it into the brokers, and then bind it with respect to respective service and then use it.

One of the major design issues of SOA is meeting its security requirements, since it affects interaction of services and applications in SOA environment [3]. With the introduction of Web 2.0, Web 3.0 and second generation internet based services, the traditional security approaches such as Secure Socket Layer/ Transport Layer Service (SSL/TLS), and Virtual Private Network (VPN) become obsolete. Hence the organization should extend SOA security framework to adopt with these new generation technologies [4]. The various aspects of SOA security are Authentication, Privacy, Auditing and Authorization. Authentication entails identity validation, Privacy guarantees disclosure of individuals data such as user identity and resource location, Auditing guarantee's that the messages sender cannot deny having send it and Authorization which establishes what action a user is allowed to perform [2], [5].

Ideally a security framework for an SOA should emphasize particular aspect of protection that is designed for web services as it is considered as the backbone of SOA implementation [2], [4]. An important approach to the problem of security is represented by the development of policy based security services providing all functions for security management relevant to applications. WS-Policy and WS-Federation as illustrated in Fig. 1.

Despite the promising features of Web Service Security standards, the main challenge in SOA is the choices of variety of security policies available for the service provider and consumer to achieve both straight forward and secure inter communication [7]. There is always a conflict between loose service access that the service consumer may ask for and the security policies that the service provider may insist upon. The service provider needs these security policies to prevent any vulnerability that may result from unconditional and unsafe access requested by service consumer. This conflict requires providing an intermediary between service providers

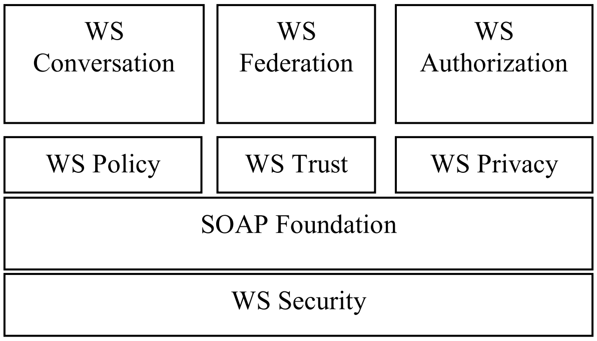

Fig. 1. Roadmap of Web Service Security Specification [6]

and consumer to organize policy concerns [4], [8].

The WS- Security standards are not designed for compatibility with SOA applications and enterprise characteristics such as reusability and agility, since security policies in those standards are not easily reused and maintained among various SOA enterprises [9]. This paper analyzes various key security requirements in a service Requirements in a Service oriented architectures and various SOA security frameworks that meets these security requirements.

II. SOA SECURITY REQUIREMENTS

The major security requirements for ensuring security in service oriented environment are:-

A. User Authentication

The service must able to authenticate the user to ensure validity of users. The service must able to identify the user which requests the service is the one who claims to be [10].

B. Access Control

The service must enforce certain constraints upon that are accessing the service. Service must enforce specified security policy related to access control. Access is to be granted based on their authentication. Access control handled through key management [11].

C. Service Usage

User can limit the actions of service; the user may wish to limit actions that the service can use in their system. Service usage is very much system and policy dependent [10].

D. Confidentiality

Unauthorized users should not access content of service used by an authorized user. Confidentiality is ensured by encrypting the communication [12].

E. Integrity

Integrity of service being used must be protected. The service produces intended content that should not be altered by an unauthorized person. Integrity is ensured on the communication layer [11].

F. Availability

Availability of services needs to be available according to the service level agreement. Availability is achieved in network layer. There are two types of availability: availability of network resource and availability of service [11].

G. Privacy

Privacy is the claim of individuals, groups, and institutions to determine for themselves, when, how and to what extend information about them is communicated to others. Privacy is the ability to disclose information to other parties and under what circumstances [13].

III. SOA SECURITY FRAMEWORKS

A. A New Security Framework against Web Services XML attacks in SOA

This work proposes a new security framework by combining Web-Service Security standards such as XML encryption and XML signatures, to resolve XML security threats especially WSDL attacks [11], [14]. The proposed framework is aimed at protecting web service against possible XML attacks such as Recursive Payloads, oversized Payloads, and WSDL attacks such as WSDL Scanning and WSDL tampering WSDL is a popular XML file format used for describing web services [8], [15]. The attackers analyze and misuse WSDL information and tamper with parameters within WSDL documents so WSDL contains all the information about web services [15]. So if there wouldn't be any kind of security on WSDL the attackers can easily discover the Web services. The proposed framework also uses asymmetric encryption to provide security of WSDL files and protect them against WSDL attacks. Initially Service Provider requests for pair of keys (private and public) from TWS (Trust Web Service) using SOAP. TWS is responsible for generating public and private key. The TWS sends a SOAP request to XKMS to store the generated public key; XKMS pass this message to PKI. PKI deliver the response to public key storage to XKMS which pass it to TWS [16].

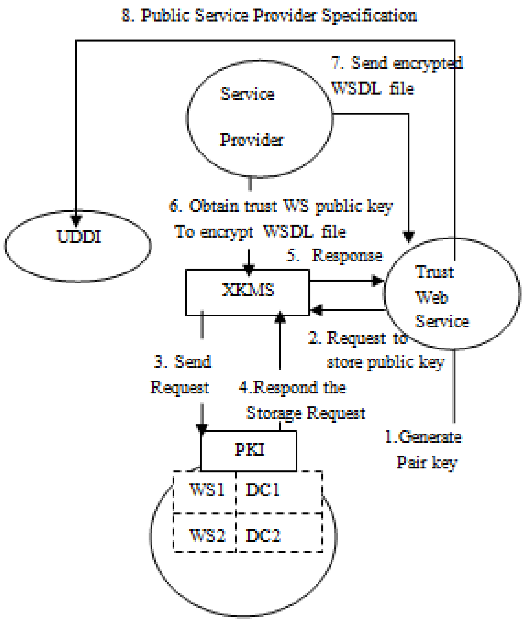
8. Public Service Provider Specification
7. Send encrypted WSDL file
Service Provider
UDDI
6. Obtain trust WS public key To encrypt WSDL file
5. Response
XKMS
Trust Web Service
2. Request to store public key
3. Send Request
4.Respond the Storage Request
1.Generate Pair key
PKI
WS1
DC1
WS2
DC2

Fig. 2. Framework against Web Service XML attacks [15].

Advantages

It does not need any secure channel to distribute the key. It is not necessary to create shared key for each connection. The key once created may be used many times.

Disadvantages

It does not support symmetric encryption. Symmetric encryption is useful for synchronous transmission of SOAP messages and for faster encryption.

This framework affords more cost since infrastructure needed to manage public and private keys are huge.
It uses complex infrastructure.

B. *Intelligent Security And Access Control Over SOA*

This paper proposes intelligent SOA security framework by introducing two most promising services: Authentication and Security Service (NSS) and Authorization Service (AS). These services are constructed as an extension of WS security standards with addition of intelligent mining techniques inorder to improve performance and effectiveness [17]. In this paper three different mining techniques are used: association rule which help to predict the attacks, Online Analytic Processing Cubes for Authorization, and clustering and mining algorithm that facilities access control rights representation and automation [18]. The main benefits in using data mining are prediction of potential attack on receipt of SOAP messages and to classify service consumers based on request message and the attacks that these messages may cause [19].

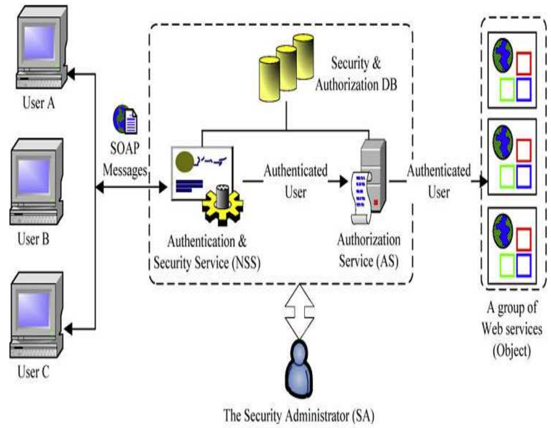
User A
User B
User C
SOAP Messages
Security & Authorization DB
Authenticated User
Authenticated User
Authentication & Security Service (NSS)
Authorization Service (AS)
A group of Web services (Object)
The Security Administrator (SA)

Fig. 3. Intelligent security Access Control over SOA [22]

Authentication and Security Service (NSS)-It is divided into two basic parts: authentication and intelligent security. The authentication part is responsible for authenticating service consumers which uses different types of authentication tokens: the intelligent security sections main function is to drop or accept incoming request SOAP messages through the use of data mining core. The intelligent cores uses Association rule for predicting web attack that may occur. The main functionality of proposed NSS therefore includes authenticating the service consumers, parsing the incoming SOAP message requests, storing security components inside database, blocking potential attack that harm the service provider by utilizing mining engine embedded in it [18], [20].

The main structure of NSS can be divided into four parts. First the consumer sends SOAP message to request for a service on providers side. Secondly, the Authentication part of NSS authenticate service consumer by validating his/her credential and forwards SOAP message request to intelligent part. Then, the Intelligent Security part of NSS parse the SOAP message store security features inside security database, predicts the attacks that arise from SOAP message using Association rule mining and classify the service consumer accordingly based on degree of trust level which depends on number of suspicious SOAP messages send. Finally a security report is generated to Service provider and SOAP message response forwarded to consumer informing whether the request is accepted or denied [17].

Authorization service - Authorization Service (AS) is another intelligent security service on proposed SOA security framework. AS is responsible for authorization. AS uses OLAP cube for classifying users as well as objects and their associated authorization roles on the basis of common attributes they have. The interaction between the authorization roles and vector framework manages access control requirements for web services in an SOA environment. Authorization Structure is an Attribute Role Based Access Control model which is a hybrid of Role Based Access Control and Attribute Based Access Control technique [17], [19].

The data mining can predict possible attacks by examining the correlation among violations as well as security features and policies to produce a new security strategy. The mining can easily recognize relationship between authentication token such as user-id/password and potential security threat that result from that token. In recognizing the relationship between violations and applied token, the mining model produces a rule. This rule illustrates security challenges in service provider's side. As a result the administrator in service provider's side can change security policy to deploy stronger token or hybrid token for authentication and thus improving security. The mining technique also used to classify security ratings of consumers [19].

The consumers are classified into three categories: clean, suspect and prohibited. Clean includes those consumers which are trustworthy, those which never sends any harmful messages or never induced any attacks. Suspect includes those consumers who had some messages dropped due to high probability of dangerous content in the message. For consumers in suspicious list, Security service request further credentials to ensure that they are trustworthy. Prohibit includes consumers who have induced an attack and they are not allowed to access the service [17].

Advantages

It can efficiently predict possible attacks. Enhanced security is provided by classifying service consumers.

Disadvantages

The compatibility of newly deployed security with service provider and service consumer is not tested, i.e. there is no proper auditing. As a result unnecessary dropping of XML packet occurs.

C. *SOA Information Security Frameworks*

It proposes an SOA information security framework, based on components, which consist of variety of controls that can minimize the challenges of SOA information security [20]. These controls collectively provide direction for strategic, management/operational and technical levels to implement SOA information security. Management and executives can use the framework as a reference for implementing SOA information security.

The controls used in the frame work ensure that day-to-day IT operations are within an organization. In the proposed framework each component within a level provides direction to those managerial levels such as strategic, managerial/operational, and technical regarding SOA information security [21].

SOA information security component provides directions at strategic level. The SOA information security governance component develops best practices for design, development, deployment, maintenance, versioning and testing of service contracts and services. Strategic management must decide how these policies become enforceable and how security policies must be aligned to current IT information practices [22].

The components at management/operational level is responsible for ensuring that service contracts and services are designed and deployed, service contracts, services and service inventories are protected, security state information is maintained and employees are familiar with SOA information security policies, practices and frameworks [22]. The components at technical level provides directions for implementing standards and technologies, which allow service contracts and services to interact with one another, in a secure manner. The SOA information security model provides feedback such as auditing of security state information, to the SOA information security management component [22].

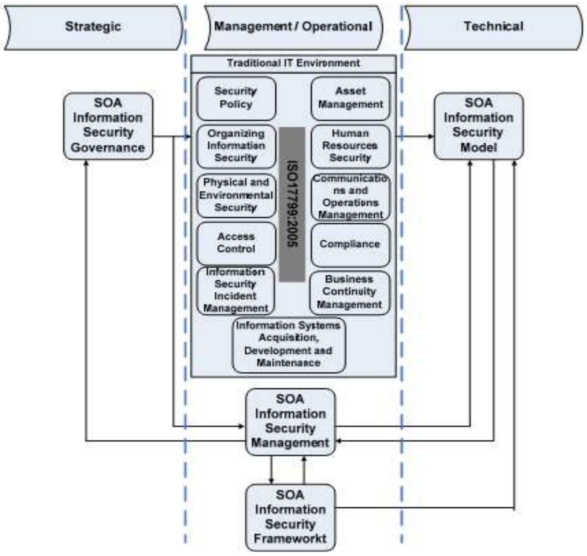
Strategic
Management / Operational
Technical
Traditional IT Environment
SOA Information Security Governance
Security Policy
Asset Management
Organizing Information Security
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Compliance
Information Security Incident Management
Business Continuity Management
Information Systems Acquisition, Development and Maintenance
ISO17799:2005
SOA Information Security Model
SOA Information Security Management
SOA Information Security Frameworkt

Fig. 4. SOA Information Security framework [10]

Advantages

The framework provides managers and developers with effective information security components for an SOA.

It provides guidelines and controls which addresses SOA information security challenges.

Disadvantages

The proposed framework can be used by organization as a starting point only.

The framework concentrates on security at managerial level.

D. Security Framework For Service Oriented Architecture:- Catherina Candolin

The security framework proposed in the framework relies on following security architecture showed in Fig. 5.

The architecture is based on Internet Protocol stack with two additions, the host layer and packet layer. In the architecture, the network infrastructure is protected physically or with some radio level schemes on MAC layer using link encryption and authentication, on the packet layer using packet level authentication (PLA) [23]. The communication level is protected on the network level mainly with IPsec and IKE protocol for key exchange. The host layer based on HIP architecture adds a cryptographic namespace to the Internet stack, thus enabling authentication, mobility, multi homing and easier IPV4 to IPV6 transition. The transport layer provides services such as data origin authentication, confidentiality and integrity verification [23].

Management and Access Control	Privacy	MLS	CBIS,SOA Security	APPLICATION	CONTENT LEVEL
			SSL/TLS, SSH	TRANSPORT	COMMUNICATION LEVEL
			HIP	HOST LAYER	
			IPSEC, IKE	IP	
			PLA	PACKET LAYER	
			Link level Encryption Link level authentication	MAC	NETWORK LEVE;L
			Frequency hopping, Impulse technology	PHYSICAL	

Fig. 5. Proposed SOA Framework-Catherina Candolin [9]

Advantages

Layer wise security service classification is provided.

The security framework defines what are the services deployed at various levels and by what means.

Disadvantages

Issues related to key revocations. Two issues in key revocations are spreading of revocation information and storing of revocation information at nodes. Spreading involves broadcasting that have the risk that everyone may not receive broad cast. Storing is a heavy burden for small user devices.

Issues related to Service aggregation. The storage requirements as well as processing time would be too huge

IV. ANALYSIS

The different frameworks analyzed in the paper are Security framework against Web Service XML attacks, Intelligent Security and Access Control Framework over SOA, SOA Information Security Frameworks, and Security Frameworks for SOA. The Analysis result shows that Intelligent Security and Access Control over SOA provide better security compared with other frameworks.

Table 1 analyzes various security features offered by different frameworks and protection it offers from potential threats. Table 2 analyzes various security frameworks that meet the key security requirements. From Table 2, it is clear that Intelligent Security and Access Control framework meet all the security requirements for an SOA framework.

TABLE I
FRAMEWORKS SECURITY FEATURES AND POSSIBLE RISKS

Framework	Major Security Feature Used	Protection from Possible Threats
A new Security Framework against Web Service XML attacks in SOA	XML Encryption and XML signatures	WSDL attacks (WSDL Scanning, WSDL tampering), XML attacks (Recursive Payloads, Oversized Payloads
Intelligent Security and Access Control over SOA	Mining (Association, OLAP cube, clustering)	SOAP attacks
SOA Information Security Frameworks	Strategic level security using components	Service Contracts, Service States ,Service inventories
Security Framework for Service Oriented Architecture	Packet Level Authentication, Information Key Exchange	Phishing attacks

V. CONCLUSION

In this paper various security frameworks for Service Oriented Architecture has been analyzed. All the four security frameworks have advantages and disadvantages. Among the various security frameworks analyzed, intelligent security and access control over SOA is found to be more efficient, since it meets most of SOA security requirements. The future work will be focused on extending intelligent access control for SOA by incorporating auditing for testing the compatibility of newly created policies with service consumer before deploying it in the service provider's side and by collaborating proper training data to the mining algorithm for greater and efficient results.

TABLE II
SECURITY FRAMEWORK Vs SECUITY REQUIREMENTS

Security Requirements / Frameworks	User Authentication	Access Control	Service Usage	Confidentiality	Integrity	Availability	Privacy
A new Security Framework against Web Service XML attacks in SOA	✓	✓	×	✓	✓	✓	✓
Intelligent Security and Access Control over SOA	✓	✓	✓	✓	✓	✓	✓
SOA Information Security Frameworks	✓	✓	✓	×	×	×	✓
Security Framework for Service Oriented Architecture	✓	✓	×	✓	✓	✓	×

REFERENCES

[1] Dirk Krafzig, Karl Banke, Dirk Slama, "Enterprise SOA-Service Oriented Architecture Best Practices", Pearson Education, Inc, USA, 2005.

[2] Thomas Erl," Service Oriented Architecture- Concepts, Technology and Design", pearson Education Inc., USA, 2005.

[3] Jeremy Epstein, Scott Matsumoto, Gray McGraw, "Software Security and SOA: Danger", Will Robinson, IEEE Security and Privacy Trans 4 (2006), 80-83.

[4] "Securing web 2.0: Are your Web Applications Vulnerable?" White Paper, Hewlett-Packard Development Company, L.P, 2007.

[5] David Geer, "Taking steps to secure Web Services", IEEE computer 36(2003), pp. 14-16

[6] Steve Graham, Doug Davis, Simeon Simeonov, Glen Daniels, Peter Brittenham,Yuichi Nakamura, Paul Fremantle, Dieter König, Claudia Zentner, "Building Web Services with Java – Making sense of XML, SOAP, WSDL, and UDDI", second ed., Sams Publishing, USA, 2005

[7] JohnViega, Jeremy Epsten, "Why applying standards to Web Services is not enough", IEEE Trans. 4 (2006),pp.25-31.

[8] Shahgholi, N.,Mohsenzadeh, M.,Seyyedi, M.A.,Qorani, S.H., "A new security framework against Web services' XML attacks in SOA," Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on , vol., no., pp.314-319, 19-21 Oct. 2011

[9] Candolin, Catharina, "A Security service for Service Oriented architectures". Miltary Communications Conference, 2007, MILCOM 2007. IEEE.

[10] Nikandar, P.;,"An architecture for authorization and delegation in distributed object oriented agent systems." PhD thesis, Helsinki University of Technology, 1999. Governance Framework. Information Systems Management, 2008(24): p. 361-372.

[11] Da Veiga, A. and J.H.P. Eloff, “An Information Security Governance Framework. Information Systems Management”, 2008(24): p. 361-372.

[12] Candolin, C. and Kiviharju, M., “A roadmap towards content based information security”; in European Conference on Information Warfare and Security, Shrivenhamn, UK, 2007.

[13] Westin, A.F., “Privacy and Freedom”, New York, NY: Atheneum, 1967.

[14] N. Sidharth and J Liu, “IAPF a framework for enhancing Web Service Security” COMPASAC. 31st annual international of computer software and Applications Conference, pp. 23-30, 2007.

[15] Shahgholi, N., Mohsenzadeh, M. Seyyedi, M.A. Qorani, S.H. , "A New SOA Security Framework Defending Web Services against WSDL Attacks," Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom) , vol., no., pp.1259-1262, 9-11 Oct 2011.

[16] E. Mordian and A Hakkanson, “Possible attacks on XML Web Services, “IJCSNS International journal of Computer Science and Network Security”, Vol. 6,pp. 154-170, January 2006.

[17] Hany F. EL Yamani, Miriam A.M. Capretzand David S. Allison: “Intelligent security and access control framework for service-oriented architecture”, In Proceedings of Information and Software Technology, 2010,pp. 220-236.

[18] Hany F., EL Yamani, Miriam A.M. Capretz: “Use of Data Mining to Enhance Security for SOA”, In proceedings of 3rd International Conference on Convergence and Hybrid Information Technology, 2008, pp. 551-558

[19] Xiao Feng Zhang, Ho-fai Wong, W.K. Cheung, “Privacy-aware service-oriented platform for distributed data mining”, in the Proceeding of the 8th IEEE International Conference on and Enterprise Computing and the 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE’06), 2006, pp. 44–48.

[20] Chetty, J, Coetzee, M., "Towards an information security framework for service-oriented architecture," Information Security for South Africa (ISSA), 2010, vol., no., pp.1-8.

[21] Nikander, P. Ylitalo, J. Wall, J; “Integrating Security, Mobility, and Multi-homing in a HIP way; In Proceedings of Network and Distributed Systems” Security Symposium (NDSS'03), pp 87-99, Sandi ego, USA, February 2003.

[22] Miller J., L. Candler and H. Wald (2009)” Information Security Governance”.

[23] Canddin, C. Lundberg J, Kari H; “Packet Level authentication in military networks”. In proceedings of the 6th Australian Warfare & IT security Conference, Geelong, Australia, 2005.

Anu Soosan Baby received her B.Tech degree from Viswajyothi Engineering collage of technology (VJCET) affiliated to Mahathma Gandhi (MG) University Kerala, India. She is currently working as a Research Scholar towards M.Tech degree in Computer Science at Vellore Institute of Technology (VIT) University, Vellore, India. Her current research areas include Natural Language Processing, Image Processing, Data Mining and Software Engineering.

Deepu Raveendran recieved his B.Tech degree from Toc H Institute of Science & Technology affiliated to Cochin university of Science & Technology Kerala, India. He is currently working as a research scholar towards M.Tech degree in Computer Science at Vellore Institute of Technology (VIT) University, Vellore, India. His current research areas include. His current research areas include Data Mining and Digital Image Processing.

Aswathy Josephine Joe received her B.Tech degree from Loord Engineering Collage affiliated to Kerala University, Trivandrum, Kerala, India. She is currently working as a Research Scholar towards M.Tech degree in Computer Science at Vellore Institute of Technology (VIT) University, Vellore, India. Her current research areas include Information Security, wireless networks, Advanced Software Engineering