International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 564-569 1 May 2014

Constructing Solutions to SOA Attacks on SOAP Web services -A Literature Review

Mohamed Ibrahim B[1], Mohamed Shanavas A R[2]
[1]Software Solution Architect & Research Scholar, Camp: Malaysia,
[2]Associate Professor, Jamal Mohamed College, Trichy, India
bmdibrahim@gmail.com, vas0699@yahoo.co.in

Abstract— ***Web Services has emerged as a dominant paradigm for constructing and composing distributed business collaborations over the web. Security is one of the major concerns when developing mission critical business applications and this concern motivates Web Services Security specifications. This paper provides the literature review on the construction of solutions to SOA attacks on SOAP based web services.***

Keywords— SOA, Security Threats, SOA Attacks, Web Services, SOAP, Security Solutions

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].

The basic architecture of SOA consists of three main components: (i) Service Provider, (ii) Service Registry, and (iii) Service Requestor [2]. The service is a basic concept and core of an SOA. It is the technical representation and encapsulation of high-level business functionality [3]. Service Provider is an entity that creates and provides the services; it also makes a description of the services and publishes them in a central registry, called Service Registry (Universal Description, Discovery, and Integration -UDDI) [4]. Service Requestor is an entity that requires certain functions which are published by Service Providers, to perform its own tasks. The three core operations that are performed in basic SOA architecture are: (i) Publish, (ii) Find, and (iii) Bind.

Although an SOA can be implemented using different technologies, web services technology is commonly used [5]. Web Service infrastructures introduce new threats to web-based applications as well as new challenges when it comes to securing them [6]. Though the fundamental technology of Web Services, XML (eXtensible Markup Language), has given provided Web Services with many advantages but unfortunately it also caused many problems in security concerns too [7].

The threats on Web Services include, Message alteration, Loss of confidentiality, Falsified messages, Man in the middle, Forged claims, Capture-replay of message, Replay of message parts, Denial of services, XML external entity attacks, XPath/Field/SQL injection, Harmful SOAP attachments, XML dereference attacks, XML recursion attacks, XML document size attacks, XML flooding, Dictionary attacks, Cookie poisoning, Data tampering, Message snooping, WSDL enumeration, Routing detour, Schema poisoning, Malicious morphing, Memory barrier breach, XML virus, Buffer overflows, Recursive elements, Resource hijacking, Cross site scripting, Eavesdropping, Spamming, IP spoofing, Phishing, Pharming, Malicious programs and Malicious file execution, Worms, Rootkits, Botnets, Identity theft, XML parser attacks, Jumbo payloads, and many more.

The primary sources for the collected literatures are: ProQuest, Google Scholar, and general Google search with restrictive and unrestrictive search criteria on SOA Security and Frameworks for SOAP Web Services Security. The secondary sources of the studied literatures include , Trade Journals, Scholarly Journals, Conference Proceedings, Dissertations & Thesis, Company White Papers, Magazines, Books, Newspaper Articles, Forum Discussions, Blog Articles, and Product Brochures.

For the literatures for relevant and related works, the search was restricted for the resources published from the year 2003 to 2013. No temporal restrictions are applied on the collection of resources for literature study and review to perform it in a comprehensive and comparative manner, however latest articles are focused for critical analysis and discussion as SOA Security is an emerging topic upon today. Moreover, the chosen articles also include those that were cited by the already-selected articles.

The Section II describes the major security goals of a successful SOA implementation, the Section III explores the currently available SOA security standards for SOAP Web Services, the Section III critically analyses the related and previous works for construction of security solutions for SOA attacks, and the Section IV concludes the paper.

II. Major Security Goals of SOA

Security in SOA is more complex than traditional IT application security; the following items should also be considered [8]:

- All entities in SOA must have identities and decouple identities from applications.
- Proper security control must be applied for each service in composite applications.
- Security management across diver's environment.
- Protection of business data in transit and at rest.
- Compliance with a growing set of regulations.

As a matter of fact, SOA brings several additional security issues. In order to overcome these matters, the various

functional and non-functional security requirements are needed to be considered. Some of these requirements such as authentication, end-to-end security, interoperability, access control, auditing, secure configuration, assurance, and compliance have been presented in many literatures, including [9] and [10]. In addition, some technologies and standards such as XML Signature, XML Encryption, WS-Security, XKMS, SAML, and XACML have been developed to support the above requirements.

The following section describes the major security requirements for ensuring security in service oriented environment, particularly on SOAP based web services which are reviewed from the reviewed literatures.

2.1 Authentication
Authentication has to do with verifying an identity. An identity may be a user, a physical device, or a foreign service requestor. Regarding SOA, this means finding out who is calling the service. In User Authentication, the service must able to identify the user which requests the service is the one who claims to be.

2.2 Authorization
Authorization has to do with determining what an identity is allowed to do. Regarding SOA, this means checking whether the caller is allowed to call the service and/or see the result.

2.3 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. Generally the Access Control is handled through key management [11].

2.4 Federation
When a service requires authentication against another external system, federation is used. Federation is an extension of authentication that helps the service provider to establish trust between the provider's security domain and an external domain. So the external provider "trusts" the request and considers it authenticated without expecting an additional credential [12].

2.5 Service Usage
User can limit the actions of service; the user may wish to limit the actions that a service can use in their system. Service usage is tightly system and policy dependent [13].

2.6 Confidentiality/Network Level Security
Unauthorized users should not access the content of service used by an authorized user. Confidentiality is ensured by encrypting the communication [14]. The goal of network level security is to encrypt data packets transmitted to and from the SOA infrastructure. This is to prevent any packet-sniffing tools to intercept any passwords.

2.7 Integrity
The main goal of Integrity is guaranteeing that data can't get manipulated or counterfeited, such that either the data is simply wrong or, even worse, authentication and authorization credentials are faked so that someone can get access to data that the person is not supposed to see. 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 [15].

2.8 Availability
It is possible to attack ("flood") a system in such a way that, while data is not lost or corrupted, the system simply becomes inoperable. A typical form of flooding is a "Denial of Service" (DoS) attack. Availability of services needs to be available according to the Service Level Agreement (SLA). Availability is achieved in network layer. There are two types of availability: availability of network resource and availability of service [15].

2.9 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 [16]. The idea of a policy in SOA security is the capability of the service provider to specify web service's conditions under which the service is provided. For example, the condition may require that the request to a web service be encrypted.

2.10 Non-repudiation
It ensures that the sender of a message cannot deny the message was sent and that the recipient cannot deny the message was received. This can be achieved using techniques such as digital signatures, timestamps and confirmation receipt services [17].

2.11 Accounting
The key concept of Accounting in SOA is to keep track of the consumption of resources; this means tracking service calls for management, planning, and security purposes.

2.12 Auditing/Monitoring
Auditing means to evaluate a security concept and its application with the aim of improving its reliability. Auditing might involve recording all security-relevant information, so that we can detect or analyse security holes and attacks. So, it also includes monitoring, logging, and tracing of all security-relevant data flow. In addition, auditing may be a functional component: when services are manipulating data, this manipulation has also to be audited. Recording all invocations of a service to address the 5 W's of security – Who, What, When, Where & Why. This is crucial to identify an attack and trace the attacker. Also, auditing constitutes a "digital" record of all activities within the SOA infrastructure [18].

2.13 Throttling
It is a concept to control the "bandwidth" offered by a service. Though not directly related to security, throttling is typically used to protect the service infrastructure so that service consumers do not "overuse" the services. In some cases, this can also be used to prevent "denial of service" attacks [19]

2.14 Hack-proof
Even if a genuine service consumer successfully authenticates and has necessary role permissions on a service, it is very

important to ensure that the service boundaries are not crossed to prevent several web-service specific attacks such as XPath injection, XML structure manipulation, schema attacks, etc. [18]

2.15 Compliance
Compliance with regulations and laws is a necessary privacy requirement to ensure that the security deployment meets the requirements of general legislation, sector-specific rules, contractual obligations, and organizational security policies.

2.16 End-to-end Security
Network topologies require end-to-end security to be maintained all across the intermediaries in the message's path. When data is received and forwarded on by an intermediary beyond the transport layer, both the integrity of data and any security information that follows with it may be lost. This forces any upstream message processors to rely on the security evaluations made by previous intermediaries and to completely trust their handling of the content of messages [20, 21].

III. Available SOA Security Standards for SOAP Web Services

The OASIS (Organization for the Advancement of Structured Information Standards) and W3C (World Wide Web Consortium) have over the last years standardized several specifications related to security in Web Services and XML.

Recently a set of security specifications for SOA are emerging in both open-sourced and product based. Some well-known and standard security specifications that may be used as part of SOAP Web Services are explored in the following sub-sections.

3.1 WS-Security
It is an extension to SOAP to apply security to web services, describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. WS-Security specifies an abstract web service security model including security tokens with digital signatures to protect and authenticate SOAP messages. WS-Security specifies a standard way to embed security tokens in the header of a message. The tokens are used to digitally sign or encrypt the message or parts of it and how to embed these parts within the message. The data is encrypted with a symmetric encryption scheme and then inserted into the message according to the standards XML-Signature and XML-Encryption by the W3C [22].

3.2 WS-Trust
Trust is an important interoperability issue, and to allow communication between services and actors from different trust domains. WS-Trust is a WS-* specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange [23].
3.3 SAML
Security Assertion Markup Language (SAML) provides an XML-based standard for the exchange of authentication, entitlement, and attributes information. WS-Federation: This specification defines mechanisms to allow different security realms to federate by allowing and brokering trust of identities, attributes, authentication between participating Web Services. WS-Federation further defines how trust relationships are managed and brokered in a heterogeneous federated environment.

3.4 WS-Secure Conversation
It is a standard defining extensions to the WS-Security standard, and provides a framework for establishing and sharing security contexts, as well as session key derivation.

3.5 WS-Security Policy
It is an addendum to WS-Security that indicates the policy assertions for WS-Policy which applies to WS-Security. WS-Policy specifies a framework for expressing web service constraints and requirements as policies using policy assertions.

3.6 WS-Provisioning
The WS-Provisioning interface is an open standard that is available to other companies that want to develop interoperable provisioning scenarios and systems. WS-Provisioning describes the APIs and schema necessary to facilitate interoperability between provisioning systems and to allow software vendors to provide provisioning facilities in a consistent way. The specification addresses many of the problems faced by provisioning vendors in their use of existing protocols, commonly based on directory concepts, and confronts the challenges involved in provisioning Web services described using WSDL and XML Schema.

3.7 SPML
Service Provisioning Markup Language (SPML) [68] provides an XML framework for managing the provisioning and allocation of identity information and system resources within and between organizations.

3.8 XML-Encryption & XML-Signature
XML Encryption specifies a process for encrypting data and representing the result in XML. XML Signature specifies XML digital signature processing rules and syntax.

3.9 XACML
Extensible Access Control Markup Language (XACML) is a standard that defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies. XACML is the core XML schema defined to represent access control policies.

3.10 XrML
Extensible Rights Markup Language (XrML) is based on XML and describes rights and conditions together with message integrity and entity authentication information.

3.11 XKMS

XML Key Management (XKMS) uses the web services framework to secure inter-application communication using public key infrastructure (PKI).

3.12 SSL
Secure Sockets Layer (SSL) is a protocol developed for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.

3.13 WS-I Basic Security Profile
The WS-I Basic Profile is a specification from the Web Services Interoperability industry consortium (WS-I), provides interoperability guidance for core Web Services specifications such as SOAP, WSDL, and UDDI.

3.14 WS-Routing/WS-Addressing
This specification provides a way to direct XML traffic through a complex environment. It operates by allowing an interim way station in an XML path to assign routing instructions to an XML document. It can be used to avoid Man-in-the-middle attacks which redirect routing of web service call/returns.

3.15 The .NET Passport
It is a Microsoft technology, and also called as Passport Network, is a Web-based service that lets users of participating web sites sign in using a single e-mail address and password. It removes the need for users to remember multiple login IDs and passwords. The same technology can be applied in order to call multiple web services of similar domains.

3.16 SecPAL
SecPAL (Security Policy Assertion Language) is a logic-based authorization language from Microsoft. It is a research project intended to balance syntactic simplicity with policy expressiveness. SecPAL has a flat architecture, but it offers some features which are interesting from the SOA viewpoint, such as delegation of rights, separation of duties, expiration constrains, among others. SecPAL also offers an option of automatic translation of rules into XML syntax, widely accepted in SOA systems.

3.17 System Authorization Facility (SAF)
The System Authorization Facility is part of the z/OS operating system and provides the interfaces to the callable services provided to perform authentication, authorization, and audit logging.

3.18 Resource Access Control Facility (RACF)
Resource Access Control Facility (RACF) is an add-on software product that provides security for a mainframe system. RACF protects resources by granting access only to authorized users of the protected resources. RACF retains information about users, resources, and access authorities in special structures called profiles in its database, and it refers to these profiles when deciding which users should be permitted access to protected system resources.

IV. Related and Previous Works

In the literature of SOA Security on SOAP based Web Services, so many researchers had done research and proposed a number of approaches in the form of various security models, frameworks, and architectures. This section gives a state-of-the-art overview of the frameworks and other solutions provided by the researchers in this field.

Navya Sidharth and Jigang Liu [24] proposed a new framework named “IAPF” for enhancing Web Services Security. This Integrated Application and Protocol-based Framework (IAPF) is addressing to tackle the existing WS Security problems. This proposed framework is organized in a sequence of four steps, (i) Protection against attacks on UDDI, (ii) Protection against attacks on WSDL, (iii) Protection against attacks on SOAP, and (iv) Protection against attacks on openly available web services, to enable web services security implementers; as well as web services implementers to formulate an integrated approach to securing web services. This IAPF standard mainly prevents Denial-of-Service (DoS) attacks.

Deven Shah and Dhiren Patel [25] proposed a security architecture for global SOA. Their strategy is to work on SOAP message interceptor (or Handler) for providing message level security in SOA. A client application uses a handler to encrypt the data before it sends the SOAP message request to the Web service. The Web service receives the request and uses a handler to decrypt the data before it sends the data to the back-end component that implements the Web service. This provides the advantage of making security independent of business functionality.

Deepti Sisodia et al. [26] evaluated the Public Key Infrastructure (PKI) on enforcing security for SOA and proposed an inbuilt security module named “SecSOA” which is based on PKI.

Narges Shahgholi et al. [27] proposed a new framework which aims to protect Web Services against WSDL attacks. In their proposed framework, web services security standards including XML encryption and XKMS have been used for their proposed security component “Trust Web Service”, to which the Service Provider sends the encrypted WSDL file which will be published to UDDI. Arezoo Mirtalebi and Mohammad Reza Khayyambashi [88] also proposed a new security framework for protecting WSDL file of Web Service, based on encryption.

Kamatchi [28] proposed a collaborative security framework for the implementation of SOA with web services. The proposed framework contains security in various formats such as, (i) Security on demand (Service & User verification), (ii) Security on compatibility (Security constraints verification), (iii) Security as necessary (Authentication & Federation), and (iv) Security as compulsory (Encryption & Proxying). And the researcher claims that her collaborative security framework provides the complete security solution to the SOA; however, in the author’s point of view, even though the proposed framework contains various security parameters, the same can be analyzed with various security breaches and the functional deficiencies, and those outcomes should be implemented in the architecture.

Nafise Fareghzadeh [29] presented a comprehensive method for Web Services Security guaranty in SOA. The proposed method specifies how to define security requirements for WS-based SOA systems, describes a WS reference security architecture that guarantees and demonstrates its development and provides us with facilities for obtaining specific security architectures based on the current WS security standards.

Jacqui Chetty and Marijke Coetzee [30] analyzed the information security challenges faced by service-oriented architectures and they proposed an SOA information security framework, based on components, which consist of a variety of controls that can minimize the challenges of SOA information security.

Oldooz Karimi examined in her paper [31] how security applies to Service Oriented Architecture, and this paper addresses the defects of traditional enterprise application integration by combining service oriented-architecture and web service technology.

Wei She and et al. [23] proposed an enhanced security model to facilitate the control of information flow through service chains i.e., composed services, for example service-1 calls service-2, which in turn calls service-3. If there is no security mechanisms provided to control such an information flow, then sensitive information may be leaked, for example to service-1 without the consensus of service-3.

Tao Xu and Chunxiao Yi [32] proposed a security processing model named SIMSA (Security Interactive Model based on SOAP and Authentication) based on SOAP and authentication in order to solve the security issues of heterogeneous platforms. The SIMSA model is mainly based on the extension of SOAP header including signature, encryption and authentication.

Carlos Gutiérrez [33] presented a process named PWSSec (Process for Web Services Security), which enables the integration of a set of specific security stages into the traditional phases of WS-based systems development. PWSSec defines three stages, (i) WSSecReq (Web Services Security Requirements), (ii) WSSecArch (Web Services Security Architecture) and (iii) WSSecTech (Web Services Security Technologies). These facilitate, respectively, the definition of WS-specific security requirements, the development of WS-based security architecture and the identification of the WS security standards that the security architecture must articulate in order to implement the security services.

IV. Conclusion

Among Web service's XML attacks, most of them appear in SOAP messages. So, in many previous studies, those attacks have been analysed and related solutions also have been offered. But very few researches only have done works on preventing WSDL threats. Some promising research works are done to protect web services from WSDL attacks, however again these frameworks depends on encryption. As mentioned earlier, these encryption standards are not full-flexed and prone for security leaks, and also they increase the complexity of web service calls. The authors restrict their study and review of related and previous works based on SOAP based Web Services, though there are many prominent research works that are carried out by the researchers and they are available in the literature of SOA security, especially on RESTful Web Services and GRID based systems which are in fact not within the scope of this literature review.

References

i. *Dirk Krafzig, Karl Banke, Dirk Slama, "Enterprise SOA Service Oriented Architecture Best Practices," Pearson Education, Inc, USA, 2005*

ii. *Johnneth Fonseca, Zair Abdelouahab, Denivaldo Lopes and Sofiane Labidi, "A Security Framework for SOA Applications in Mobile Environment," International Journal of Network Security & Its Applications (IJNSA), Vol.1, No.3, pp. 90-107, 2009*

iii. *Andr´e Miede, Nedislav Nedyalkov, Dieter Schuller, Nicolas Repp, and Ralf Steinmetz, "Cross-organizational Security – The Service-oriented Difference," International Conference on Service Oriented Computing, Springer (ISBN: 978-3-642-16131-5), pp. 72-81, 2010*

iv. *Navya Sidharth and Jigang Liu, "IAPF: A Framework for Enhancing Web Services Security," 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), 2007*

v. *Jacqui Chetty and Marijke Coetzee, "Towards An Information Security Framework For Service-oriented Architecture," Information Security Conference, South Africa, IEEE ISBN: 978-1-4244-5494-5, 2010*

vi. *Vorobiev, A. and Han, J., "Security Attack Ontology for Web Services," Proceedings of the 2nd International Conference on Semantics, Knowledge and Grid (SKG'06), Guilin, China, 2006*

vii. *M. B. Juric, A. Sasa, B. Brumen, and I. Rozman, "WSDL and UDDI extensions for version support in web services," Elsevier at The Journal of Systems and Software, vol. 82, pp.1326–1343, 2009*

viii. *Chu H, You C, Teng C, "Challenges: Wireless Web services," Proceedings of 10th International Conference on Parallel and Distributed Systems (ICPADS 2004), 2004*

ix. *Fielding R., "Architectural Styles and the Design of Network-based Software Architectures," PhD Dissertation, University of California, Irvine, California, USA, 2000*

x. *Gabriel Serme, Anderson Santana De Oliveira, Julien Massiera, and Yves Roudiery, "Enabling Message Security for RESTful Services," IEEE 19th International Conference on Web Services (ICWS), 2012*

xi. *Da Veiga, A. and Eloff, J.H.P., "An Information Security Governance Framework," Information Systems Management, Vol. 24, Issue 4, 2007*

xii. *Torry Harris Business Solutions Inc., White-paper, "Migration and Security in SOA", University of Leeds, 2009*

xiii. *Paul Fremantle et al., "Carbon: Towards a Server Building Framework for SOA Platform," Proceedings of the 5th International Workshop on Middleware for Service Oriented Computing (MW4SOC), New York, USA, 2010*

xiv. *Candolin, C. and Kiviharju, M., "A roadmap towards content based information security," The 6th European Conference on Information Warfare and Security, Shrivenham, UK, 2007*

xv. *Da Veiga, A. and Eloff, J.H.P., "An Information Security Governance Framework," Information Systems Management, Vol. 24, Issue 4, 2007*

xvi. *Anu Soosan Baby, Deepu Raveendran, and Aswathy Josephine Joe, "A Study on Secure and Efficient Access Control Framework for SOA," International Journal of Computer Science and Telecommunications, Vol. 3, Issue 6, pp.71-76, 2012*

xvii. *Ahmed Youssef and Manal Alageel, "Security Issues in Cloud Computing," GSTF International Journal on Computing , Vol. 1 No. 3, 2011*

xviii. Torry Harris Business Solutions Inc., White-paper, "Migration and Security in SOA", University of Leeds, 2009

xix. Paul Fremantle et al., "Carbon: Towards a Server Building Framework for SOA Platform," Proceedings of the 5th International Workshop on Middleware for Service Oriented Computing (MW4SOC), New York, USA, 2010

xx. Web Services Architecture Specification: http://www.w3.org/standards/techs/wsarch

xxi. Garlos Gutierrez, Eduardo Fernandez-Medina, and Mario Piattini, "Web Services Security: Is the Problem Solved?," Information Systems Security, Vol. 13, Issue 3, 2004

xxii. Andr´e Miede, Nedislav Nedyalkov, Dieter Schuller, Nicolas Repp, and Ralf Steinmetz, "Cross-organizational Security – The Service-oriented Difference," International Conference on Service Oriented Computing, Springer (ISBN: 978-3-642-16131-5), pp. 72-81, 2010

xxiii. Wei She, I-Ling Yen, and Bhavani Thuraisingham, "Enhancing Security Modeling for Web Services using Delegation and Pass-on," IEEE International Conference on Web Services (ICWS), China, ISBN: 978-0-7695-3310-0, pp. 545-552, 2008

xxiv. Navya Sidharth and Jigang Liu, "IAPF: A Framework for Enhancing Web Services Security," 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), 2007

xxv. Deven Shah and Dhiren Patel, "Architecture Framework Proposal for Dynamic and Ubiquitous Security in Global SOA," International Journal of Computer Science and Applications, Vol. 6, No. 1, pp. 40-52, 2009

xxvi. Deepti Sisodia, Lokesh Singh, and Sheetal Sisodia, "Web Based Secure SOA," International Journal of Computing Algorithm, Vol. 01, Issue 02, 2012, pp. 63-69

xxvii. Shahgholi, N., Mohsenzadeh, M., Seyyedi, M.A., and Qorani, S.H., "A New SOA Security Framework Defending Web Services against WSDL Attacks," Proceeding of IEEE 3rd International Conference on Social Computing (socialcom), 2011, pp. 1259-1262

xxviii. Kamatchi, "Security Visualization Collaborative Security Framework for Service Oriented Architecture," International Journal of Modeling and Optimization, Vol. 2, No. 4, pp. 558-562, 2012

xxix. Arezoo Mirtalebi and Mohammad Reza Khayyambashi, "A new Security Framework for Protecting WSDL File of Web Service," International Journal of Computer Science and Network Security (IJCSNS), Vol. 12 No.9, 2012

xxx. Jacqui Chetty and Marijke Coetzee, "Towards An Information Security Framework For Service-oriented Architecture," Information Security Conference, South Africa, IEEE ISBN: 978-1-4244-5494-5, 2010

xxxi. Oldooz Karimi, "Security Model For Service-Oriented Architecture," Advanced Computing: An International Journal (ACIJ), Vol.2, No.4, pp. 48-58, 2011

xxxii. Tao Xu and Chunxiao Yi, "SOAP-Based Security Interaction of Web Service in Heterogeneous Platforms," Journal of Information Security, 2011

xxxiii. Carlos Gutiérrez, "Towards a Process for Web Services Security," Journal of Research and Practice in Information Technology, Vol. 38, No. 1, 2006, pp. 57-67