International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Review on the Security Perspectives of Service Oriented Architecture (SOA)

Krishnadas Ravindran

School of Computer Science and Engineering, Vellore Institute of Technology,Vellore-632014, India

Abstract: ***Service Oriented Architecture is basically a service oriented approach in which all the services or application components are interconnected through the use of a network. This makes it possible for the services to interact with one another without any human intervention. But as is the case with any such system, a security architecture is to be adopted. This paper provides an insight to the security aspects of a Service Oriented Architecture. The various frameworks and protocols that could be used in such a scenario are discussed as well as the security architecture that could be designed to avoid bottlenecks.***

Keywords: Service Oriented Architecture (SOA); Quality of Security Service (QOSS); Security protocols; Cryptography; Architecture; Web Service-Security Kerberos (WS-SK); eXtensible Markup Language (XML); Unified Modelling Language (UML); Domain Specific Language DSL;

1. Introduction

A Service Oriented Architecture(SOA) is a type of software design in which the different components of a software are all interlinked in a network and each such application components communicate through the messages passed between them through the very same network. SOA is seen as a vast improvement for businesses and as such is adopted by organisations to ensure more success. The business transactions take advantage of the interoperability of the loosely connected services. But the challenge faced in such a system is the presence of a secured infrastructure. Usage of a service generally requires some kind of identification or personal data from the user. Security flaws could arise in such a scenario and could compromise the individual. So a security framework is a must have for a SOA adopted software. Many such frameworks have been provided by various researchers over the years and many security models too have cropped up for addressing security. Security models utilize techniques like symmetric and public keys and hash function techniques to satisfy the different levels of Quality of Security Service (QoSS) agreements. Also existing security products and technologies are not made full use of and could cause wastage of resources.

2. Security Frameworks

Various types of security frameworks could be adopted for different security concerns like network security and security in a business model. Some of these are discussed in the following paragraphs.

A security framework can be formed in which the challenges to security are completed by the likes of run time management, policy driven security, inventory of service and also through training and auditing with the provision of message level security and security as a service. This level based approach provides a much better service and security.

Faulty reconfiguration is a technique in which the replacement of services is a necessity when a faulty region is discovered. It is based on expansion strategy.

Classification of data and data provenance into three layers, that is, data layer, IS layer and SOA layer to ensure data integrity, security and reliability is another security framework that could be adopted. The underlying idea is the classification of data provenance and the collection and grouping of data.

Inclusion of meta services to improve upon the interaction between a consumer and producer such that security flaws do not happen forms the basis of the next framework. This is made possible due to the two properties possessed by meta services, that is, functional and non-functional property.

P-assertion makes it possible for users to have access rights and thus control the accessibility of information in a system. This type of network utilizes keys to give responsibility to the individual in charge such that the parts of encrypted p-assertions are not decrypted by anyone not holding a key.

AON technology could be considered for a framework as it improves robustness and the locality of an overlay network. Such a framework is designed keeping in mind, the manageable web services and with services as the basis of operation.

A business process model network can be utilized to provide a better security with the use of a DSL definition mechanism. It requires the identification, availability, integrity and confidentiality so as to enhance the productivity of the model.

In general, after observing the aforementioned frameworks and some existing ones, it is found that, XML documents in administration arranged system administration are to be given security by the provenance security while WS-KS is to be given to UML documents. For the improvement of ASB overlay organized AON innovation is more valuable. Future work is to execute a structure for faulty reconfiguration. XML filtering procedure should be made possible with the broken administrations if these are to be given in XML bundles and subsequently the issue of more than one defective locale at once can be settled. Since administrations leave a trace as it utilizes the XML document, security can

be given to these records utilizing provenance security system, Kerberos security and so on. XML separating procedure to review can be utilized to discover deficiencies.

3. Security Protocols

Quality of Security Service (QoSS) follows a set of security protocols that need to be followed during any kind of service interaction. More than one security protocol is used and as such none of them is adjudged the best protocol as the situation or the environment keeps on changing and therefore the protocol best suited for that environment is used. Some of the aforementioned protocols include simple authentication protocol, mutual authentication protocol and other protocols that are modified or made in accordance to the action required. For example, modifications can be made so as to provide authentication and session keys in one protocol. From the discussion, it is evident that a lot of security protocols exist and it is difficult to organize or manage the ones suitable for securing the architecture. Modification of protocols to include more suitable features as said above helps to a large extent. This leads to more efficiency and productivity from a business point of view. QoSS as a whole selects the best protocol for each service requirement and tends to avoid the false sense of security that persist at times.

4. Security Architecture

Security devices and technologies are converted to essential security segments which frame the basic security layer. Besides this, differently developed security parts that make up the developed security layer are acknowledged in view of useful combination and process control. At that point security administrations are given through these two levels to upper security applications. A centralized engineering outline of the security service core for managing the bottlenecks in a distributed form of network could be designed. Such an outline explains viably the security of a large scale data framework. The breakdown of the service oriented architecture helps in the case of large information systems and designing one should be according to the services provided and to solve complexity, inconsistencies, variability and invisibility.

5. Conclusion

The various security protocols discussed as well as the security frameworks could be both integrated in a SOA environment to ensure more efficiency and productivity. If it's a case of a large information system, the breakdown of security architecture and designing one based on the complexity is to be adopted. Just following one principle as opposed to this could improve the current situation but the combination of all the factors put forward by this discussion could lead to a more secure and efficient SOA. Also from the discussion it was seen that a framework has to be formed for faulty configuration. Likewise, frameworks have to be formed for the technologies without one. One last thing that needs more clarity is the way the security protocols are employed. The basis of choice should be without any trial and error and as such, software or technology needs to be developed to provide a smart decision.

References

[1] Wenjun Cheng, Xiaosu Zhan, 'Study on Service-Oriented Security Architecture'
[2] Abdelkader H. Ouda, David S. Allison, Miriam A. M. Capretz, 'Security Protocols In Service-Oriented Architecture'
[3] Abdul Muttalib Khan, Alankar Mishra, Riya Agarwal, 'Security Framework based on QoS and Networking for Service Oriented Architecture'
[4] Rohit Ranchal, Bharat Bhargava, Ruchith Fernando, Hui Lei, 'Privacy Preserving Access Control in Service-Oriented Architecture'