A Relative Study on Security Issues in Semantic Web Services

Subarnarekha Ghosal
M. Tech.
Department of Computer Science & Engineering
SCSE, VIT University
Vellore, Tamilnadu, India

Abstract— Semantic Web is a common framework to share data across several applications and various enterprises. More specifically it is a term for a data web that can be operated by the machines. Semantic Web Services represents the server side of the client server architecture for interactions between two or more machines through World Wide Web. Semantic Web uses Extensible Markup Languages which represents data in a more sophisticated and detailed way which is understandable by the machines. In recent years Semantic Web Services is being used widely. Meanwhile, several security issues regarding the same have popped up. In addition with the emerging technology cloud computing semantic web security has acquired major importance.Thus various solutions to solve this problemhas also been proposed. This paper presents a comparative study of the various security methods that have come up and benefits and drawback of each method.

Keywords: - semantic Web services; access control; PKI, SSL, OWL-S network security

I. INTRODUCTION

Today's web services are mainly human automated and designed exclusively for their understanding and use. But in many fields such as B2B and e-commerce these web services are extended on the field of interoperability. It is implemented through API extracting the hand-coded information extraction code to locate and extract the content of the HTML syntax of a web page presentation layout [8]. But the changes of the presentation of a web page make it necessary to change the structure of the API for maintaining compatibility. The solution is to create a Semantic Web Service whose interfaces, properties and capabilities can be interpreted easily by the machines. Thus, Semantic Web Service has become a popular application domain in the complex internet. No access control method is developed till yet which is actually effective for assuring Web Service Security. This Semantic Web services are applied across various domains including SOA, Cloud Computing etc for implementation of many real life applications such as Web Search, e-commerce, Supply Chain Management, Media Management, Data Integration in Oil & Gas and so on. Now the security related to the same has become an extremely emerging field for research [12] .

The two most primitive type of encryption technology mainly followed by the Semantic Web Services are the PKI (Public Key Infrastructure) and SSL. These encryption methods are validated using certificates and other ownership evidence. Other than this RBAC (Role Based AccessControl) supports the definition of access control policies that are fine grained. Other upcoming technologies such as SBAC (Semantic Based AccessControl) "which considers relations of entities in all domains of access control namely Subject(user), Object(Data/resource), Action(select, open, read, write) and so on"(ref :access control interrelationship). Again, a model primarily based on the security control centre is proposed in this paper for access control of a Semantic Web Service. It is mainly dependant on the basic security infrastructure. Moreover various advancements in aggregating CVSS (Common Vulnerability Scoring System) scores of vulnerabilities of individual nodes in a distributed system yield a practical approach to network security metric. These access control method is mainly based on OWL Ontology and semantic rules are applied for assigning work to the individual nodes and implementing them. Most of the web service protocols use HTTP protocol. Thus a method has also been designed to overcome the security related issues of HTTP Protocol. In this model the Web tools namely WebGoat and WebScarab for testing how this system performs. This has mostly yielded positive results.

II. RELATED WORK

Semantic web services is an extension of web services [6] and thus it adds semantic technology to the pre existent Web Services. Similarly Semantic Web Service Security is a matured version of Web Service Security in terms of service security systems and the corresponding service security standards. Thus it is extremely essential to create a semantic web service environment [13] for the overall system to adapt access control architecture. In this section we briefly describe all methods of implementing security in Semantic Web Services and present a comparative study between all of them.

A. PKI

In order to assure a stable client-server application PKI is used. But the efficiency of this system may be reduced if any of the nodes become mobile causing its performance to degrade. However to give a solution for this Suresh Kumar et.al has proposed a method [1]. The various methods that can be applied to check the status of the online certificates are CRL (certificate revocation list) and OSCP (online certificate status protocol). Thus digital certificate is the solution to the problem faced by PKI because it makes real-time verification possible. Again, for authentication overload in the distributed PKI system cross certification between client-server and the third party can be implemented mainly by using RSA, ECC(Error Correcting Code) [10] and other cryptographic techniques. PKI plays vital role for client privacy as well as privacy of the semantic web.

To provide the next generation of WWW security interoperability between CA-to-CA, CA-to-RA, CA-to-VA is necessary. Intrusion detection, malicious attack prevention and critical intrusion detection are the domains for research in the semantic web service oriented

architecture.PKI may be considered as a very popular means of security for interoperable communications in the coming years. PKI encrypts or decrypts xml credential by X.509 certificates [Fig 1] before it starts transmission in an unsecured channel

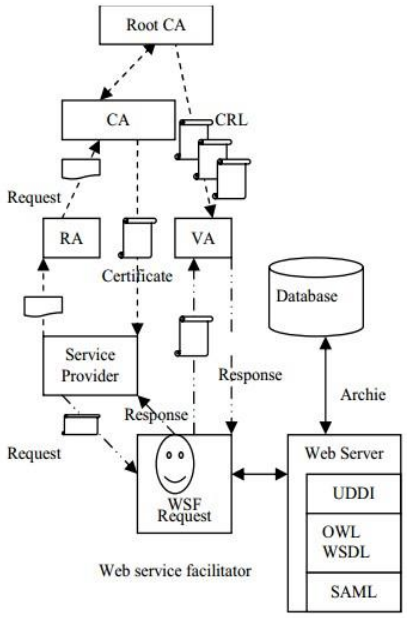

Fig. 1: A typical PKI Architecture for Certificate Validation

B. RBAC

Among the various security solutions available in industry and academics, the privacy algorithm are available which is not sufficient technically, fine grained or transparent ways. Thus a new semantic web system supporting fine grained access control policy is being proposed. The system is based on the authorization model of a formal ontology for role abstraction for simplifying security of administration. RBAC assign permissions to roles. Each user is assigned a particular role. Thus only authorized users are given access to the resources. This model is coupled with a set of control restrictions mainly used in development of Electronic Health Record.

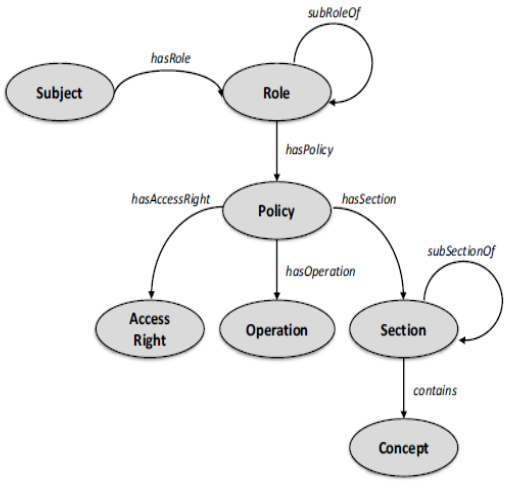

Fig. 2: General RBAC Architecture

RBAC has been widely used due to its simplicity, effectiveness and authorization, however it may not implemented the fine grained access control properly. Thus Flora Amato et al.[2] proposed a semantic based approach is applied to encode RBAC model through ontology including the basic elements of this model and their relationships.It follows the proposed National Institute of Standards and Technology RBAC reference model [11] and handled a major and challenging task of granting access according to the right and need of a particular user[Fig 2]. RBAC fails to consider interrelationships among access control entities.

C. SBAC

To overcome the drawbacks of RBAC, came the Semantic Based AccessControl (SBAC) model. A method to implement SBAC is described here which considers "relationship among the entities in all domains of access control namely Subject(user), Object(Data/resource), Action(select, open, read, write) and so on" [3]. This method reduces the semantic relationships into subsumption problem thereby extending the policies in these domains. Many entities exist in all three domains described above. In many other traditional models all these entities are considered separately without considering their inter relationships. Thus decision making procedure is also carried out separately for each entity without considering their inter relationship. The SBAC model overcomes this problem by the information provided for it. OWL(Web Ontology Language) is used to consider the semantic interrelationships in every domain (subject, object, action) in different levels of ontology. A Horn Clause extension of OWL is used to provide expressiveness to the rules of authorization [4]. This model can be used in cloud systems independently since it provides security to Semantic Web Services also[Fig 3]. Further study in this field may include detection of accuracy is a more complex access control mechanism. Again implementation of SWIRL rule is not possible automatically on semantic web, thus further studies will aim at the same.

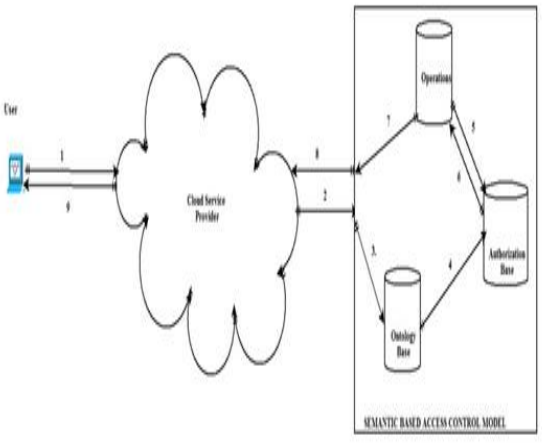

Fig. 3: A typical SBAC Model

D. Access Control Model For Semantic Web Services Based On Security Control Center

The earlier systems may not guarantee sometimes fails to consider the inter relationships between various systems and thus cannot reflect the real states of the entities. Again the semantic services often locate services through word matching thereby it cannot specify the QoS, service time,

reliability etc. The result is the presence of a missing, unwanted data in UDDI. Elisa Bertino[4] proposed a model which consults service parameters during access control. In addition to this Mariemma et al, suggested Semantic Access Protocol (SAC) which considers metadata during access control thereby integrating semantics with external authorization rules. But in all these cases the requester and provider are located in different domains and unaware of each other's name, password and other user identity certificates. Semantic Web Based Securtity Based On Security Control Centre provides a proper solution to the above problems.

This model is a combination of manageable, extendable, unified framework of Security Authentication Services [20], Security Protocols and Access control technology providing proper security to semantic web services. It is a combination of resource object, service object, trusted SOAP messaging, authentication, access control and trust management. The proposed model on one hand is an expansion of security control centre and on the other hand can also focus on security related issues[Fig 4] and some basic elements and functions.

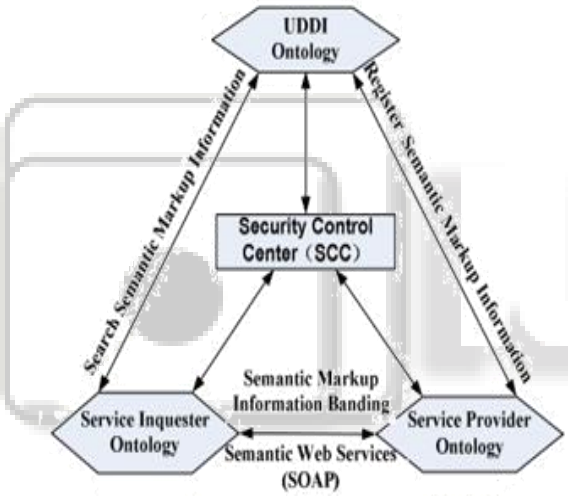

Fig. 4: A model based on security control centre for Semantic Web Service

Different common protocols such as HTTP, FTP, SMTP, SOAP,UDDI,OWL's etc are used here along with network security protocols such as https, SSL, IPSec, VPN, XML Encryption, XML Signature,WS-Security, Transaction security management, User authentication etc are used. The individual components may be very effective but for achieving comprehensive security, web service should be considered as basis of all security infrastructures. Thus there are still many issues to be dealt with in Web Service Applications [21].

E. CVSS Base Scores for Semantics

In evaluation of how effective a system is, a network security metric is often required. One such approach to network security metric is accumulating CVSS Scores [7] for detecting vulnerabilities of the individual components. In this paper the CVSS scores are accumulated through two different aspects. In the first approach the base level is achieved of the metric where "dependency relationship has well defined semantics" [5]. While in the second we acquire the base metrics from different aspects and preserves the scores of individual semantics. The earlier limitations like the loss of semantics while handling interrelationships and other aspects of CVSS has been overcome by this method and simulation may prove better results.

F. Detect HTTP Specification Attacks using Ontology

There are several ways to deal with the upcoming security issues for web services. The main drawbacks of all these are that it is they follow a static method for error detection, lack expressiveness in the rules for detecting errors and lack the expected number of ways an attack can happen. For all these semantic techniques for error detection are being introduced. In the paper published by Rana Faisal Munir et al. [16] proposed HTTP Protocol ontology [Fig 5] to prevent the protocol attacks related to communications. The different abnormalities in HTTP Protocol, smuggling HTTP Request, Splitting HTTP Response are mainly dealt in this method and thus exceeds the performance of any related methods. Ontology not only facilitates in reasoning it also helps in the detection of all variations of protocol related attacks. Protocol grammar is used to detect the attacks related to specific protocols [17]. Intrusion Detection Solutions (IDS) solutions which is based on Ontology includes only data integrity of web resources [18] and for driving

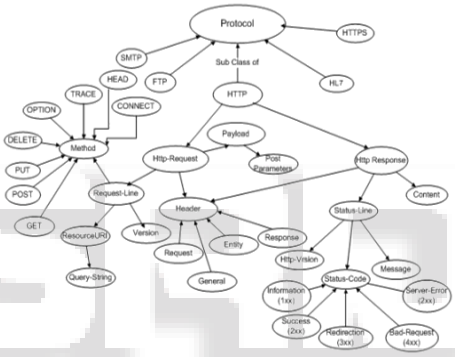

Fig. 5: HTTP ProtocolOntology

the control access with the help of ontology [19] .But specific protocol attacks are not detected by it.

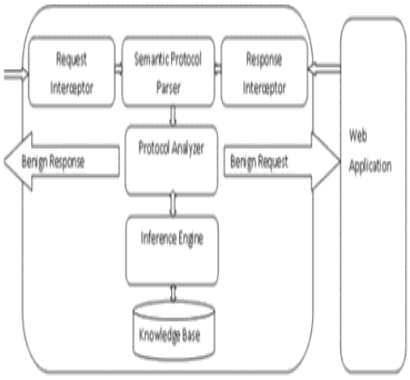

Fig. 6: System Architecture of HTTP Specification Attacks using Ontology

In this ontology fulfils all the requirements present in RFC 2616 for HTTP protocol in depth. This ontology is built with the help of Protg tool, JENA rule language, default reasoned of JENA which can be substituted by racer pro, FaCT++ or Pellet. JAVA provides the interface and coding and JENA library is used for semantic functionality. With the help of ontology the complete conceptual model [Fig 6] of the protocol is generated for easy detection of the vulnerabilities. This ontology can be used properly

for web service security. This can be extended for protocols like SMTP, FTP, HTTTPs etc.

Sl. No	Security Method	Proposed Author	Advantages	Disadvantages
A	PKI	Suresh Kumar et al.	assure astable client-server application	Efficiency reduced when any node becomes mobile
B	RBAC	Flora Amato et al.	Specified for fine grained system and specific user authentication	Fails to consider inter relationships
C	SBAC	M Auxilla et al.	Considers relationship among entities	Lacking accuracy in more complex access control systems
D	Access control based on security control centre	Yang Xin et al.	Relates semantics with external authorization rules	Not suitable for achieving comprehensive security
E	CVSS Base Scores	Pengsu Cheng et al.	Can handle semantic for inter relationships	Can be improved for better results
F	HTTP Specification attacks using ontology	Andres Tom et al.	Prevents protocol attacks related to communications	Does not have any such major drawbacks

III. SUMMARY

In this survey paper a relative study of different approaches in semantic web security has been carried out. Each and every methods or models have its own advantages and disadvantages. Many models have resulted in overcoming the drawbacks of the earlier one. The security related to web service particularly in case of semantic web service has been a major issue through the past few years. Still researchers are searching for an optimised way to provide full security to a Semantic Web Services. PKI is mainly used for client server architecture and digital signatures may be used to overcome performance degradation. RBAC is used for fine grained access control giving access to the data resource for the purpose of security. Another model namely SBAC turns the semantic relationship into subsumption problem thereby extending the policies related to each domain. Access Control Method for Semantic Web Services Based on Security Control Centre makes requestor and sender aware of each other. Again CVSS scores are used to deal with metadata of individual components. Detection of HTTP Specification Attacks using Ontology deals with the protocol related security issues of semantic web. Though recent methods try to overcome the drawbacks of the earlier one, but a model which considers all issues is still a question. The main aim is to proceed towards that role model. The pace in which the research on this area is blooming looking forward to that model is quite obvious.

REFERENCE

[1] Suresh Kumar , Rakesh Kr. Prajapati, Manjeet Singh, Asok De, "Security Enforcement using PKI in Semantic Web," 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM),IEEE. P392~397

[2] Flora Amato, Nicola Mazzocca, Giuseppe De Pietro, Massimo Esposito, "A System for Semantic-Based Access Control," 2013 IEEE Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. P442~446

[3] M. Auxilia ,K. Raja,"A Semantic-Based Access Control for Ensuring Data Security in Cloud Computing," 2012 IEEE International Conference on Radar, Communication and Computing (ICRCC). P171~175

[4] Yang Xin, JianjingShen, Zhigang Si ,"A System for Semantic-Based Access Control," 2010 Sixth International Conference on Natural Computation. P3711~3714

[5] Pengsu Cheng, SushilJajodia, AnoopSinghal, "Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics," 2012 31st IEEE International Symposium on Reliable Distributed Systems. P31~40

[6] B.Carminati,E.Ferrari,P.C.K.Hung,"Web Service Composition: A Security Perspective," 2005 IEEE International Workshop on Challenges in Web Information Retrieval and Integration. P3711~3714

[7] D. Balzarotti, M. Monga, and S. Sicari. Assessing the risk of using vulnerable components.InProceedings of the 1st ACM QoP, 2005.

[8] Sheila A. McIlraith, Tran Cao Son, and HongleiZeng,"Semantic Web Services," IEEE INTELLIGENT SYSTEMS

[9] D.M. Eyers, J. Bacon, K. Moody. OASIS role-based access control For electronic health records. IEE Proceedings-Software, vol. 153, no. 1, 2006, pp.16–23.

[10] B. Thuraisingham,"Building Secure Survivable Semantic Webs", 14th IEEE International Conference on Tools with Artificial Intelligence, ICTAI'-2002.

[11] J.J. Carroll, I. Dickinson, C. Dollin, D. Reynolds, A. Seaborne, K.Wilkinson, Jena: implementing the semantic web recommendations. In: Proc. of the 13th Internat. World Wide Web Conference on Alternate Track Papers & Posters, New York, USA, 2004, pp.74–83

[12] Patel-chneider P, Hayes P,Horrocks I, "OWL: Web Ontology Language Semantics and Abstract Syntax, W3CRecommendation(2004)

[13] Agarwal S, SprickB. ,"Access control for semantic Web services," Proceedings of 1st International Conference on Web Services, 2004.770-773.

[14] AnoopSinghal,Web Services Security: Challenges and TechniquesComputer Security Division, NIST

[15] Anders Toms,Threats, Challenges and Emerging Standards in Web Services Security, Technical report HS-IKI- TR-04-001
[16] Rana Faisal Munir, Nabeel Ahmed, Abdul Razzaq, Ali Hur and Farooq Ahmad, "Detect HTTP Specification Attacks using Ontology," 2011 Frontiers of Information Technology. P75~78
[17] A. Anitha and V. Vaidehi. Context based application level intrusion detection. InInternational conference on Networking and Services, pages 16–21, 2006.
[18] V. Raskin, C.F. Hempelmann, K.E. Triezenberg and Nirenburg. Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool. InProceedings of the 2001 Workshop on New Security Paradigms (NSPW-2001), pages 53–59, 2001.
[19] V. Raskin, C.F. Hempelmann, K.E. Triezenberg and Nirenburg. Ontologyin Information Security: A Useful Theoretical Foundation and MethodologicalTool. In Proceedings of the 2001 Workshop on New Security Paradigms (NSPW-2001), pages 53–59, 2001.
[20] Tse Chu-fai, GUO Da-zhi., "Semantic Web-based spatial information sharing service," Computer Engineering and Design, 2005,26 (10) , pp.2674-2676.
[21] Ravi S.Sandhu et.al, "Role-based access control models", IEEE Computer, 29(2) pp. 38–47,February1996

