Review of Literature on Web Services Security Architecture extended to Cloud, Big Data and IOT

Dr.D.Shravani

Rayalaseema University, Kurnool, A.P, India

Abstract- *This Literature Review paper consists of Web Services Security Architecture extended to Cloud, Big Data and IOT.*

Keywords - *Security Engineering, Security Architectures, Web Services, Cloud Computing, Big Data, IOT*

I. INTRODUCTION

The area of present research work consists of Security Architectures, Web Services Security Architecture, Designing Solutions, Dependability, Model Driven Architecture, and Agile Modeling. The area of research work is relatively new one in the IT Industry. The information needed for current research work was collected using the internet medium, articles, magazines and other resources given by experts in the field. A thorough literature survey is conducted with the available resources in pursuing the research work. When searching for required information, large amount of information is found written by diverse knowledgeable authors describing their approach on various aspects of present research work. Some authors' research investigations are presented below.

2.1 REVIEW OF LITERATURE ON MODEL DRIVEN ARCHITECTURE BASED AGILE MODELED LAYERED SECURITY ARCHITECTURE:

Integrating Security into Software Engineering at Architecture Design Phase

System Security Architecture from a Software Engineering viewpoint imposes that strong security must be a guiding principle of the entire software development process. It describes a way to weave security into systems architecture, and it identifies common patterns of implementation found in most security products [Gunnar Peterson].

The Security and Software Development Communities must find ways to develop software correctly in a timely and cost-effective fashion. Theirs is no substitute for working software security as deeply into the development process as possible. System designers and developers must take more proactive role in building secure software. The root of most security problems in software that fails in unexpected ways when under attack. The enforcement of security at the design phase can reduce the cost and effort associated with the introduction of security during implementation. At the architectural level a system must be coherent and present unified security architecture that takes into account security principles (such as principle of least privilege). Architectural Risk Analysis of Software Systems Based on Security Patterns, The importance of software security has been profound, since most attacks to software systems are based on vulnerabilities caused by poorly designed and developed software. Furthermore, the enforcement of security in software systems at the design phase can reduce the high cost and effort associated with the introduction of security during implementation. For this purpose, security patterns that offer security at the architectural level have been proposed in analogy to the well-known design patterns. The main goal of this paper is to perform risk analysis of software systems based on the security patterns that they contain. The first step is to determine to what extent specific security patterns shield from known attacks. This information is fed to a mathematical model based on the fuzzy-set theory and fuzzy fault trees in order to compute the risk for each category of attacks. The whole process has been automated using a methodology that extracts the risk of a software system by reading the class diagram of the system under study [Spyros T Halkidis].

Security Architecture Design

Securing the Software application in any application at the design phase is known as Security Architecture, with a focus on authentication and authorization.," Design Patterns", Design Patterns: Elements of Reusable Object-Oriented Software is a software engineering book describing recurring solutions to common problems in software design. The book's authors are Erich Gamma, Richard Helm, Ralph Johnson and John with a foreword by Grady Booch. The authors are often referred to as the Gang of Four, or GoF. The book is divided into two parts, with the first two chapters exploring the capabilities and pitfalls of object-oriented programming, and the remaining chapters describing 23 classic software design patterns. The book includes examples in C++ and Smalltalk [Erich Gamma].

Model Driven Architecture Security

Linking Model-Driven Development and Software Architecture: A Case Study, A basic premise of model driven development (MDD) is to capture all important design information in a set of formal or semi-formal models which are then automatically kept consistent by tools. The concept however is still relatively immature and there is little by way of empirically validated guidelines. In this paper we report on the use of MDD on a significant real-world project over several years. Our research found the MDD approach to be deficient in terms of modeling architectural design rules. Furthermore, the current body of literature does not offer a satisfactory solution as to how architectural design rules should be modeled. As a result developers have to rely on time-consuming and error-prone manual practices to keep a system consistent with its architecture. To realize the full benefits of MDD it is important to find ways of formalizing architectural design rules which then allow automatic enforcement of the architecture on the system model. Without this, architectural enforcement will remain a bottleneck in large MDD projects. [Anders Mattsson]

Agile Modeling Security

An agile MDA approach for executable UML structured activities, Agile processes allow developers to construct, run and test executable models in short, incremental, iterative cycles. However, the agile development processes tend to minimize the modeling phase and the usage of UML models, because UML is a “unified” (too general) language with a lot of semantic variation points. The current version of UML together with its Action Semantics provides the foundation for building object-oriented executable models. But, constructing executable models using the existing tools and the current standard notations is a tedious task or an impossible one because of the UML semantic variation points. Agile MDA processes try to apply agile principles in the context of executable models. This paper presents a procedural action language for UML structured activities that allows developers to apply agile principles for executable models that contains structured activities. New graphical notations for structured activities are also introduced for rapid creation of tests and procedures [I. Lazar].

Integrating software development security activities with agile methodologies, Because of several vulnerabilities in software products and high amount of damage caused by them, software developers are enforced to produce more secure systems. Software grows up through its life cycle, so software development methodologies should pay special attention to security aspects of the product. This paper focuses on agile methodologies in order to equip them with security activities. We can restrain reduction of agile nature of organization's current process by means of agility measurement and applying an efficient activity integration algorithm with a tunable parameter named agility reduction tolerance (ART). Using this approach, method engineer of the project can enhance his agile software development process with security features to increase product's trust worthiness. [Keramati, H.].

Extending Security in Agile Software Development Methods, Software developers can use agile software development methods to build secure information systems. Current agile methods have few (if any) explicit security features. While several discrete security methods (such as checklists and management standards) can supplement agile methods, few of these integrate seamlessly into other software development methods. Because of the severe constraints imposed by agile methods, these discrete security techniques integrate very poorly into agile approaches. This chapter demonstrates how the security features can be integrated into an agile method called feature driven development [M.Siponen]

Agile Security Requirements Engineering Agile processes have been deemed unsuitable for security sensitive software development as the rigors of assurance are seen to conflict with the lightweight and informal nature of agile processes. However, such apparently conflicting demands may be reconciled by introducing the new notion of abuser stories in the requirements domain. These extend the well established concept of user stories to achieve security requirements traceability and thus open the door to excellent security assurance, precisely because of their informal and lightweight nature. This paper aims to extend agile practices to deal with security in an informal, communicative and assurance driven spirit. [Johan Peeters].

Designing Dependable Solutions

DeMIMA: A Multilayered Approach for Design Pattern Identification Design patterns are important in object-oriented programming because they offer design motifs, elegant solutions to recurrent design problems, which improve the quality of software systems. Design motifs facilitate system maintenance by helping to understand design and implementation. However, after implementation, design motifs are spread throughout the source code and are thus not directly available to maintainers. We present DeMIMA, an approach to identify semi-automatically micro-architectures that are similar to design motifs in source code and to ensure the traceability of these micro-architectures between implementation and design. DeMIMA consists of three layers: two layers to recover an abstract model of the source code, including binary class relationships, and a third layer to identify design patterns in the abstract model. We apply DeMIMA to five open-source systems and, on average; we observe 34% precision for the considered 12 design motifs. Through the use of explanation-based constraint programming, DeMIMA ensures 100% recall on the five systems. We also apply DeMIMA on 33 industrial components. [Gueheneuc]

Real-Time Agility: The Harmony/ESW Method for Real-Time and Embedded Systems Development, Real-time and embedded systems face the same development challenges as traditional software: shrinking budgets and shorter timeframes. However, these systems can be even more difficult to successfully develop due to additional requirements for timeliness, safety, reliability, minimal resource use, and, in some cases, the need to support rigorous industry standards. In Real-Time Agility, leading embedded-systems consultant Bruce Powel Douglass reveals how to leverage the best practices of agile development to address all these challenges. Bruce introduces the Harmony/ESW process: a proven, start-to-finish approach to software development that can reduce costs, save time, and eliminate potential defects. Replete with examples, this book provides an ideal tutorial in agile methods for real-time and embedded-systems developers. It also serves as an invaluable "in the heat of battle" reference guide for developers working to advance projects, both large and small. [Bruce Powel Douglass]

2.2 REVIEW OF LITERATURE ON WEB SERVICES SECURITY ARCHITECTURE:

2.2.1 Web Services Security Development and Architecture: Theoretical and Practical Issues

Web Services Security Development and Architecture: Theoretical and Practical issues, involves Web Services Security Engineering, Web Services Security Architecture, Web Services Security Standards, Web Services Security Threats and Countermeasures [Carlos Gutirez].

Web Services Security Engineering implies, Security Engineering integrated into software development which is one of the major topics developed during the last few years [Kanchan Hans].

Applying security engineering throughout the different steps devised by the different software development methodologies has been a major topic in both scientific and industrial literature [Mouratidis].

Web Services Security Architecture should define the highest level organization of the IT security infrastructure necessary to meet the security requirements specified for the systems to be built by articulating the necessary security mechanisms in such a way that reusability, manageability and (internal/external) interoperability is guaranteed [Asoke K Talukder].

The Web Services Security Architecture, as per National Institute of Science and Technology (NIST) is a layered architecture consisting of Web Service Layer, Web Services Framework Layer and Web Server Layer [Anoop Singhal].

The goal of the Web Services Security Architecture is to summarize out the details of message level security from the mainstream business logic [Marzouk S Mokbel].

In the Web Services Secure application design, authentication and authorization are important research issues, pertaining to Security Architecture [Mail Jiang].

Even though Web Services are existing from the year 2004 onwards, Web 2.0 had made Web as a platform, with mashup applications from the year 2009 [Tim O Rielly].

This Web 2.0 Services Security needs to be investigated for research Moreover extension of these Web 2.0 Services applications in terms of Spatial Web Services Security needs to be investigated for research, in the area of Security Architecture Design [Reza B Far].

Web Services Security Engineering

Identification of Vulnerabilities in Web Services using Model Based Security, In a Service Oriented Architecture, business processes are executed as composition of services, which can suffer from vulnerabilities. These vulnerabilities in services and the underlying software applications put at risk computer systems in general and business processes in particular. Current vulnerability analysis approaches involve several manual tasks and hence, are error prone and costly. Service Oriented architectures impose additional analysis complexity as they provide much flexibility and frequent changes with in orchestrated processes and services. Therefore, it is inevitable to provide tools and mechanisms that enable efficient and effective management of vulnerabilities with in these complex systems. Model Based security engineering is a promising approach that can help to fill the gap between vulnerabilities on the one hand and concrete protection mechanisms on the other. An approach that integrates model based engineering and vulnerability analysis in order to cope with the security challenges of service oriented architecture [Sebastian Hohn].

Security Analysis of Service Oriented Systems: A methodical approach and case study, This work is devoted to the continuous security analysis of service oriented systems during design and operation. Present the ProSecO framework which offers concepts and a process model for the elicitation of security objectives and requirements, evaluation of risk and documentation of security controls. The goal of ProSecO is to provide the analyst at any time during design and operation with information about the security state of the system. Core ideas of ProSecO are interweaved elicitation and documentation of functional and security properties based on system model and the clear separation of business oriented and technical information. The kind of operation ProSecO handles is in wide parts informal and non executable [Frank Innerhofer].

Web Services Security Architectures

Ontology – based authorization model for XML data in distributed systems, this work proposes a semantic – aware authorization framework, SAAF, for applying syntax independent authorization on extensible markup language (XML documents). Our model supports secured data sharing in an open environment without the need for a centralized authority and supports application flexibility. We propose the use of data and application semantics, expressed as resource description framework (RDF) Ontologies, to specify security requirements for XML documents. XML documents are associated with their semantics (RDF ontology's) via mappings. Use these mappings and the corresponding RDF authorizations models to generate access control permissions for the mapped XML documents. The SAAF ensures the preservation of AUTHORIZATION, PERMISSSIONS ON xml DATA even if the syntax and the structure of the data are changed. Their method also aids the detection and removal of inconsistent authorizations on structurally different but semantically similar XML data [Amit Jain].

Secure Service Rating in Federated Software Systems based on SOA, The Service oriented architecture (SOA) paradigm mostly provides a suitable approach as to meet the requirements of flexible distributed software systems. Referring to the activities for the standardization of web service semantics or alternatively the introduction of intelligent search mechanisms future software architectures are supposed to integrate software components as remote services of foreign providers. If the authors assume that such services can be standardized. Example as components of standard business application systems, the vision of a services economy arises where services of the sane type can be marketed by different providers. A service consumer on the other hand could choose the service he likes best at run time. However this vision is clouded by a multiplicity of risks which meet each other in the question of the specific reliability and trust worthiness of service providers in a certain context. Previous research activities picked up these problems where by a lot of promising approaches and frameworks have been developed which concern the negotiation of trust within open network architectures like grids are peer to peer networks. Nevertheless, the genesis of the reuse relationships between two network nodes had been neglected. Presents an approach for the establishment of reputation in federated software systems, where central network instances for the management of evaluations are avoided. Approach the service providers are responsible for this task on their own. The author presents a novel security protocol for the message based exchange of service evaluations that filters service providers from manipulating their own ratings [Nico Brehm].

Forensics over Web Services the FWS Web Services are currently a preferred way to architect and provide complex services. This complexity arises due to the composition of new services by choreography, orchestrating and dynamically invoking existing services. These compositions create service interdependencies that can be misused for monitory or other gains. When a misuse is reported, investigators have to navigate through a collection of logs to create the attack. In order to facilitate that task, the authors propose creating forensics web services (FWS), a specialized web service that when used would securely maintain transactional records between other web services. These secure records can be relinked to reproduce the transactional history by an independent agency. Although there work is ongoing, they show the necessary components of a forensic framework for web services and its success though a case study [Murat Gunestas]

Policy – based security engineering of service oriented systems, in this chapter the authors present a policy based security engineering process for service oriented applications, developed in the SERENITY and MISTICO projects. Security and dependability (S&D) are considered as first class citizens in the proposed engineering process which is based on the précised description of reusable security and dependability solutions. The authors process is based on the concept of S&D pattern as the means to capture the specialized knowledge of security engineers and to make it available for automated processing both in the development process (the focus of this chapter) and later at runtime. In particular, in this chapter they focus on the verification of the compliance with security policies, based on the formal specification of S&D properties. The main advantage of the approach presented in this chapter are precisely that it allows us to define high level policies and to verify that a secure oriented system complies with such policy (developed following the SERENITY approach). They also describe the application of the proposed approach to the verification of S & D properties in the web services (WS) environment. Concretely, they describe the use of SERENITY framework to facilitate the development of applications that use standard security mechanisms (such as WS-Security, WS-Policy, WS-Security Policy, etc.) and to ensure the correct application of these standard mechanisms, based on predefined policies. Finally, the authors show how to verify that the application complies with one or several S & D policies [Antonio Mana]

Security Policies in Web Services, Security is of fundamental concern in computing systems. This chapter covers the role of security policies in Web Services. First, it examines the importance of policies in web services and explains the WS-Policy standard. It also highlights the relation of WS-Policy with other WS-* specifications. Next, it covers different facets of security requirements in SOA implementations. Later, it examines the importance of security policies in web services. It also presents the basic concepts of WS-Security policy language. WS-Security policy specification specifies a standard way to define and publish security requirements in an extensible and interoperable way. A service provider makes use of security policy to publish the security measures implemented to protect the service. Security policies can also be made customizable to meet the security preferences of different consumers. Towards the end, it discusses about the governance of security policies and also future trends in security policies for web services [Deepthi Parachuri].

Web Services Security Standards

Web Services Security – Standards and Industrial Practice, This surveys the context for web services security and discusses the issues and standards at every level of architectural. The authors attempt to evaluate the status of industrial practice with respect to the security of web services. The authors look at commercial products and their supporting levels, and end with some conclusions. The authors see a problem in the proliferation of overlapping and possibly incompatible standards. Reliability is also an important aspect. They discuss some of its issues and consider its effect on security a basic principle of security is the need to ensure all levels of architecture; any weak levels will permit attackers to penetrate the system. These levels include: Business workflow level, catalog and description of web services level, communications level (typically SOAP), and storage of XML documents. There is a variety of standards for web services security and reliability and they will look at most of them [Eduardo B Fernandez].

Security in Service Oriented Architectures – standards and challenges, Service Oriented Architectures (SOAs) have become the defacto standard for defining interoperable architectures on the web with the most common implementation of this concept being in the form of web services. Information exchange is an integral part of SOAs, so designing effective security architectures that ensure data confidentiality and integrity is important. However, selecting a security standard for the architecture is challenging because existing solutions are geared toward access control in relatively static scenarios rather than dynamic scenarios where some form of adaptability is needed. Moreover, when services interact across different domains interoperability becomes a problem because of the lack of a consistent security model to handle service interactions. This chapter presents a comparative analysis of SOA security standards. We discuss the challenges SOA security standards. We discuss the challenges SOA security architecture designers face, in relation to an example travel agent web services scenario, and outline potential mitigation strategies [Anne V D M Kayem].

Web Services Security Threats and Counter Measures

A survey of Attacks in the Web Services World, in the modern electronic business world, services offered to business partners as well as to customers has become an important company asset. This again produces interests for attacking those services either to paralyze the availability or to gain unauthorized access. Though founding on decades of networking experience, Web Services, are not more resistant to security attacks than other open network systems. Quite the opposite is true: Web Services are exposed to attacks well-known from common Internet protocols and additionally to new kinds of attacks targeting Web Services in particular. This chapter presents a survey of different types of such Web Service specific attacks. For each attack a description of the attack execution, the effect on the target and partly the results of practical experiments are given. Additionally, general countermeasures for fending Web services attacks are shown. [Meiko Jensen]

Threat Modeling: Securing Web 2.0 based Rich Service Consumers; this research work proposes a threat modeling approach for Web 2.0 applications. The authors approach is based on applying informal method of threat modeling for Web 2.0 applications. Traditional enterprises are skeptical in adopting Web 2.0 applications for internal and commercial use in public facing situations, with customers and partners. One of the prime concerns for this lack of security over public networks. Threat modeling is a technique for complete analysis and review of security aspects of application. The authors will show why existing threat modeling approaches can not applied to web 2.0 applications, and how our new approach is a simple way of applying threat modeling to web 2.0 application. [Nishtha Srivastava]

Other Selected Readings on Web Services Security

Obtaining security requirements for a mobile grid system, Mobile grid includes the characteristics of the grid systems together with the peculiarities of mobile computing, with the additional feature of supporting mobile users and resources in seamless, transparent, secure and efficient way. The Security of these systems, due to their distributed and open nature is considered a topic of great interest. In this article we present the practical results of applying a secure methodology to a real case, specifically the approach that define, identifying and specify the security requirements. This methodology will help the building of a secured grid application in a systematic and iterative way. [David.G.Rosado]

We provide a conceptual modeling approach for web services security risk assessment that is based on the identification and analysis of stake holder intentions. There are no similar approaches for modeling web services security risk assessment in the existing pieces of literature. The approach is, thus, novel in this domain. The approach is helpful for performing means-end-analysis, thereby uncovering the structural origin of security risks in WS, and how the root-causes of such risks can be controlled from the early stages of these projects. The approach addresses "why" the process is the way it is by exploring the strategic dependencies between the actors of a security system and analyzing the motivations, intents, and rationless behind the different entities and activities in constituting the system.[Subhash C.Misra]

2.3 RESEARCH MOTIVATION AND PROBLEM STATEMENT AND BASIS TO THE THESIS:

Web Services Security Engineering through Web Services Security Architecture

Problem Definition

This research entitled "Designing Dependable Web Services Security Architecture Solutions" addresses the innovative idea of Web Services Security Engineering using Web Services Security Architecture with a research motivation of Secure Service Oriented Analysis and Design. It deals with Web Services Security Architecture for Web Services Secure application design, for Authentication and authorization, using Model Driven Architecture (MDA) based, Agile Modeled Layered Security Architecture design, which eventually results in enhanced dependable (privacy) management. All the above findings are validated with appropriate case studies of Web 2.0 Services, its extension to Web 2.0 Mashups Spatial Web Services and various financial applications.

II.CONCLUSION

This PAPER dealt with Review of Literature on Designing Dependable Web Services Security Architecture Solutions, with general Research Issues on Security Architectures using Model Driven Architecture based Agile Modeling for Security Architectures and Specific Web Services Security Architecture Development issues using Agile Modeling.

REFERENCES

[1] Christos Douligeris, George P.Ninios [2007], "Security in Web Services", Network Security: Current Status and Future Directions, IEEE Inc. Book, pp. 179 – 204.

[1] Constance L Heitmeyer [2008], "Applying Formal Methods to a Certifiably Secure Software System", IEEE Transactions on Software Engineering, January 2008, Vol 34 No1 1.

[2] Coppolino L, Romano L, Vianello V [2011],"Security Engineering of SOA applications via Reliability Patterns", Journal of Software Engineering and Applications, pp. 1 – 8.

[3] David Geer, [2003], "Taking Steps to Secure Web Services", IEEE, October 2003, pp. 1 – 4.

[4] Deepthi parachuri, Dr.Sudeep Mallick [2009], "Security Policies in Web Services", IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch007, pp. 134 – 151.

[5] Dimitris Gritzalis, Javier Lopez [2009],"Emerging Challenges for Security, Privacy and Trust", 24th IFIP TC 11 proceedings Springer, pp. 1 – 4.

[6] Douglas Rodigues, Julio C Estrella, Kalinka R.L.J.C.Branco [2011] "Analysis of Security and Performance aspects in Service Oriented architectures" In International Journal of Security and its application, Vol 5 No 1 pp. 13-30

[7] Durai Pandian M et.al. [2006], "Information Security Architecture – Context aware Access control model for Educational applications", International Journal of Computer Science and Network Security, December 2006, pp. 1 – 6.

[8] D.K.Smetters, R.E.Grinter [2002], "Moving from the design of usable security technologies to the design of useful secure applications", ACM New Security paradigms workshop September 2002 pp 82 – 89

[9] Eduardo B.Fernandez, Maria M. Larrondo-Petrie et.al. [2009], "Web Services Security: Standards and Industrial Practice", IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch008. pp. 152 - 186.

[10] Eduardo B.Fernandez, Nobukazu Yoshika, Hironori Washizaki, Jan Jurjens, Michael VanHilst, Guenther Pernul [2011], "Using Security Patterns to Develop Secure Systems", DOI: 10.4018/978-1-61520-837-1.ch002, IGI Global, pp. 16 – 31

[11] Elisa Bertino, Lorenzo D.Martino, Federica Paci, Anna Squicciarini [2010], "Security for Web Services and Service-Oriented Architectures", Springer Book, Appendix A - Access Control, ISBN 978-3-540-87741-7, pp. 202-204.

[12] Erich Gamma [2009], "Design Patterns Elements of Reusable Object Oriented Software", Addison Wesley Publishers, pp. 1 - 12.

[13] Ferda Tartanoglu, Valerie Issarny, Alexander Romanovsky, Nicole Levy [2003], "Dependability in the Web Services Architecture. Architecting Dependable Systems", LNCS 2677, pp 90-109, 2003, Springer Verlag Heidelberg, pp. 202-204.

[14] Florian Kersch Baum, Philip Robinson [2008], "Security Architectures for Virtual Organizations of Business Web Services", Journal of System Architecture, 11 September 2008, pp. 1 – 23.