DEPENDABLE WEB SERVICES SECURITY ARCHITECTURE DEVELOPMENT THEORETICAL AND PRACTICAL ISSUES – SPATIAL WEB SERVICES CASE STUDY

D.Shravani[1] Dr.P.Suresh Varma[2] K.Venkateswar Rao[3] Dr.B.Padmaja Rani[4] M.Upendra Kumar[5]

[1]Research Scholar Computer Science Rayalaseema University Kurnool A.P. India
sravani.mummadi@yahoo.co.in
[2]Principal and Professor Computer Science Adikavi Nannaya University Rajahmundry A.P. India
vermaps@yahoo.com
[3]Associate Professor CSE JNTUH CEH Hyderabad A.P. India
kvenkatesearrao_jntuh@yahoo.co.in
[4]Professor CSE JNTUH CEH Hyderabad A.P. India
padmaja_jntuh@yahoo.co.in
[5]Associate Professor CSE MGIT Hyderabad A.P. India
uppi_shravani@rediffmail.com

ABSTRACT

This research "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. In this paper we discuss about Research Methodology for Designing Dependable Agile Layered Security Architectures, with validations on Spatial Web Services Case study.

KEYWORDS

Security Architecture, Web Services Security, Agile Modeling, Dependability, Privacy requirements, Spatial Web Services

Natarajan Meghanathan, et al. (Eds): ITCS, SIP, JSE-2012, CS & IT 04, pp. 79–98, 2012.

DOI : 10.5121/csit.2012.2108

1. INTRODUCTION TO WEB SERVICES SECURITY ARCHITECTURE AND LITERATURE SURVEY

Web Service A Web Service is a method of communication between two electronic devices over a network. The World Wide Web Consortium (W3C) defines a "Web Service" as "a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Services Description Language, known by the acronym WSDL). Other systems interact with the Web Service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards." The W3C also states, "We can identify two major classes of Web services, REST-compliant Web services, in which the primary purpose of the service is to manipulate XML representations of Web resources using a uniform set of "stateless" operations; and arbitrary Web services, in which the service may expose an arbitrary set of operations" [Chris Douligeris].

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].

Designing Dependable Solutions Designing Secure Solutions implies that, the task of developing Information Technology solutions that consistently and effectively apply security principles has many challenges including: the complexity of integrating the specified security functions within the several underlying component architecture found in computing systems, the difficulty in developing a comprehensive set of baseline requirements for security, and a widely accepted security design methods[J J Whitmore]. Dependability implies privacy management of the application [Bhavani Thuraisingham]. Securing the Software application in any application at the design phase is known as Security Architecture, with a focus on authentication and authorization [Durai Pandain M]. Now a days, most of the applications are developed as a Layered Security Architecture pattern, typically having layers like User Presentation layer, Business Logic layer and Database access layer [Heiko Tillwick]. Today Agile Modeling (like Test Driven Development) is used in all Web applications design (our focus on Web Services), because of shortened development time, with customers collaborations with developers (pairs). Unfortunately Agile Modeled architecture is given less importance in literature because of quick development schedule, this research focuses on Secure Agile architecture for web services. Agile Modeling, being an iterative development approach, securing its architecture will provide Privacy information of the user, in the subsequent iterations [Hossein Keeramati].Our security approach is based on Model Driven Architecture (MDA) based Agile Security Modeling for Web Services [Hohn S Lowis].

Literature Survey:
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]

WEB SERVICES SECURITY ARCHITECTURE:

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. DEPENDABLE PRIVACY REQUIREMENTS DESIGNING USING AGILE MODELD LAYERED SOLUTIONS

Agile Security Patterns
The Dependency-Inversion Principal

Dependency Inversion Policy: Dependency inversion can be applied wherever one class sends a message to another. For example, the case of the Button object and the Lamp object [Bruce Powel Douglass].

The Button object senses the external environment. On receiving the Poll message, the Button object determines whether a user has "pressed" it. It doesn't matter what the sensing mechanism is. It could be a button icon on a GUI, a physical button being pressed by a human finger, or even a motion detector in a home security system. The Button object detects that a user has either activated or deactivated it. The Lamp object affects the external environment. On receiving a TurnOn message, the Lamp object illuminates a light of some kind. On receiving a TurnOff message, it extinguishes that light. The physical mechanism is unimportant. It could be an LED on a computer console, a mercury vapor lamp in a parking lot, or even the laser in a laser printer. The Button object receives Poll message, determines whether the button has been pressed, and then simply sends the TurnOn or TurnOff message to the Lamp.

The Button class depends directly on the Lamp class. This dependency implies that Button will be affected by changes to Lamp. This violates DIP. The high level policy of the application has not been separated from the low level implementation. High-level policy is the abstraction that underlies the application, the truths that do not vary when the details are changed. It is the system inside the system, it is the metaphor. Here, the Button now holds an association to a ButtonServer, which provides the interfaces that Button can use to turn something on or off. Lamp implements the ButtonServer interface. Thus, Lamp is now doing the depending rather than being depended on. This allows a Button to control any device that is willing to implement the ButtonServer interface. This provides a great deal of flexibility. (The Figure 1 provides the class diagram for this principle.)

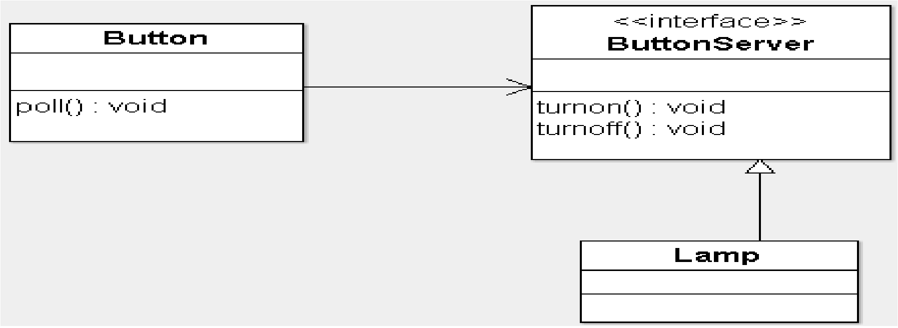


Figure 1: Class Diagram for Dependency Inversion Principal.

Interface Segregation Principle

Interface Pollution: Consider a security system in which Door objects can be locked and unlocked and know whether they are open or closed. This Door is coded as an interface so that clients can use objects that conform to the Door interface without having to depend on particular implementations of Door. Let us consider a TimedDoor which needs to sound an alarm when the door has been left open for too long. In order to do this, the TimedDoor object communicates with another object called a Timer. When an object wishes to be informed about a timeout, it calls the Register function of the Timer. Force Door, and therefore TimedDoor, to inherit from TimerClient. This ensures that TimerClient can register itself with the Timer and receive the TimeOut message. The problem with this solution is that the Door class now depends on TimerClient. Not all varieties of Door need timing. The applications that use those derivatives will have to import the definition of the TimerClient class, even though it is not used. This causes complexity and redundancy. Separate Client Means Separate Interfaces: Door and TimerClient represent interfaces that are used by completely different clients. Timer uses TimerClient, and classes that manipulate doors use Door. Since the clients are separate, the interfaces should be separate too, because clients exert forces on their server interfaces. Include a unique timeOutId code in each timeout registration and repeat that code in the TimeOut call to the TimerClient. (The Figure 2 provides the class diagram for this principle.)

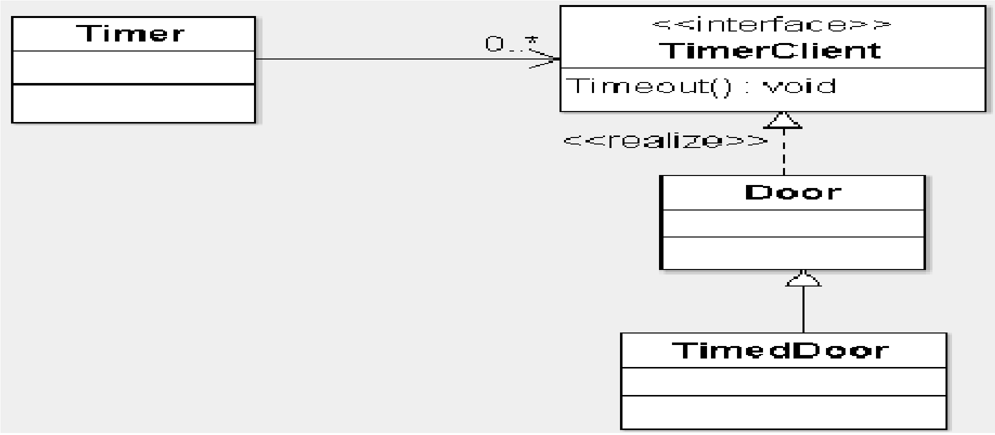


Figure 2. Class Diagram for Interface Pollution

Separation through Delegation: One solution to ISP is to create an object that derives from TimerClient and delegates to the TimedDoor. When it wants to register a timeout request with the Timer, the TimedDoor creates a DoorTimerAdapter and registers it with the Timer. When the Timer sends the TimeOut message to the DoorTimerAdapter, the DoorTimerAdapter delegates the message back to the TimedDoor. This solution conforms to ISP and prevents the coupling of Door clients to Timer. Even if the change to Timer were to be made, none of the users of Door would be affected. Moreover, TimedDoor does not have to have the exact same interface as TimerClient. The DoorTimerAdapter can translate the TimerClient interface into the TimedDoor interface. Thus this is a very general purpose solution. But in this solution, the delegation requires a very small amount of runtime and memory. (The Figure 3 provides the class diagram for this principle.)

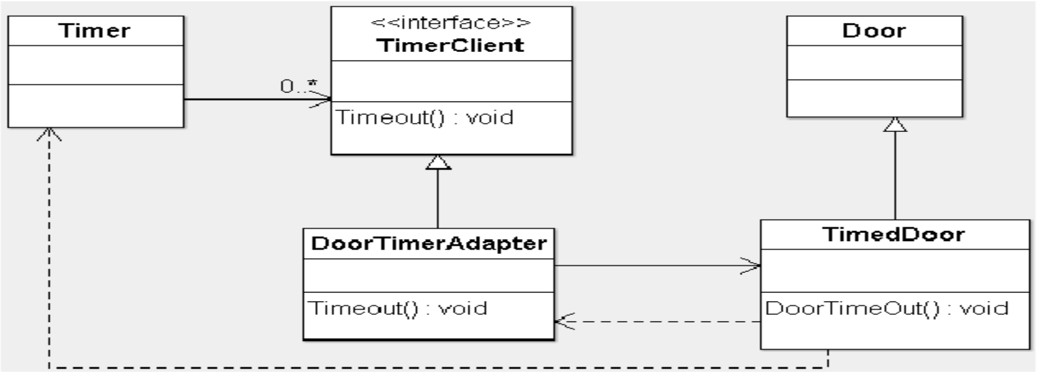
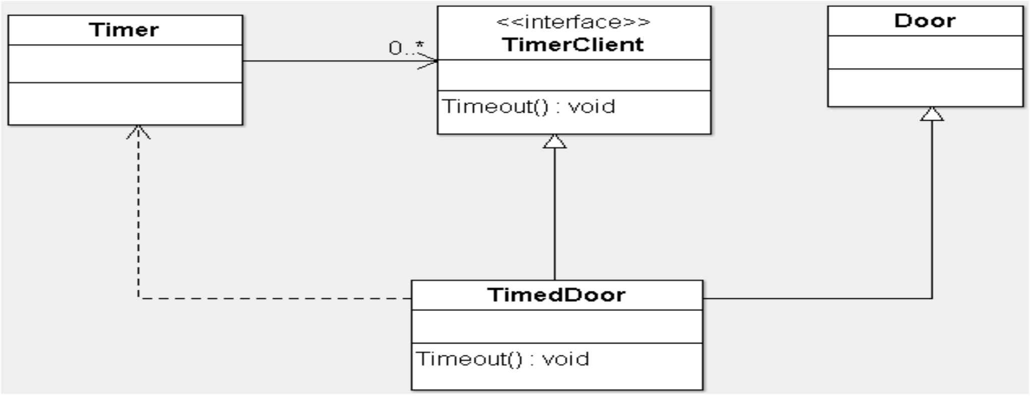


Figure 3 Class Diagram for Separation through delegation.

Separation through Multiple Inheritances: TimedDoor inherits from both Door and TimerClient. Although clients of both base classes can make use of TimedDoor, neither depends on the TimedDoor class. Thus, they use the same object through separate interfaces. (The Figure 4 provides the class diagram for this principle.)



. Figure 4.Class Diagram for separation through Multiple Inheritance.

3. Implementations and Validations – Spatial Web Services Case Study

Spatial Secure Design of CRM Web Services Application

The purpose of the implementation is to develop a Report in which we can track the customer's location, the details and the driving directions to the customer's location. Today there are several web-based maps available on market. Companies like Google, Microsoft and Yahoo provide their own Application Programming Interface (API) for integration web-based maps in applications.
The CRM Application is designed to allow users to track customers and potential customers based on the usage of web service Interfaces. In this implementation we use Google search API to retrieve the details of the customers and MapPoint API is used to generate the map and driving directions to that particular location.

Features: It enables the user to add, update, and delete contact information for a specified contact. It allows the user to navigate among the contact records. It displays the web pages with the given information. It retrieves a map of the contact's city and state/region. It also retrieves the driving directions to the customer's location. The geographic location and distribution of customers is a critical piece of information that is usually missing from customer relationship marketing and data mining applications.

People tend to shop where it is convenient, which usually means close to home or work, hence travel time is important for retail response to promotion. Hence we illustrate the use of spatial modeling and analysis for understanding customer loyalty, assessing competitive threat, identifying customers likely to defect, and targeted print media promotion choices.

WEB APIS Web APIs are a set of application programming interfaces that can be called over standard Internet protocols. Web APIs generally allow remote computers on different platforms to talk to each other using methods that were previously very difficult.

Representational State Transfer(REST) uses HTTP-GET to retrieve data. Similarly HTTP-POST is used to retrieve data as well as updates.

Simple Object Access Protocol(SOAP) is used for communication in between the client and the server.

We integrate features from the Google API and the Microsoft MapPoint API into the CRM Application to further extend its capabilities.

The application uses the Google API to retrieve the first five sites that mention the customer.
The Microsoft MapPoint API retrieves directions to the customer's location.

GOOGLE API

The Google API is currently available using SOAP with the HTTP protocol. Google has made several of its popular features available in an API to developers to use in their own applications.
The Google API supports search requests, retrieving pages from the Google cache, and spelling suggestions. Five Creative Ways to Use the Google API:

1—Build a Google Search Feature

2—Return Random Pages

3—Save the Results of a Google Search to a File

4—Use Google to Check Spelling

5—Use the Google Cache to Retrieved Web Site That Is No Longer Available
MapPoint API

The MapPoint API is implemented as an XML Web service that can be called using the SOAP protocol. MapPoint supports various features such as finding addresses, finding non-addressable places, reverse geocoding, address parsing, finding nearby places, custom locations, routing, map rendering, and Points of Interest (POI).

Five Creative Ways to Use the MapPoint API:

1—Obtain Driving Directions

2—Retrieve a Map

3—Perform a Geocode Lookup

4—Find Nearby Places

5—Obtain Information on Points of Interests

We believe firmly that the true Enterprise Portal is what is beyond CRM -A highly functional, customizable, low-cost, high ROI interface through which the organization can transact with the world. Enterprise portals require different thinking however from the software in a box concept. The starting point for any enterprise portal implementation is to redefine the word “Customer” – in essence to reclaim it from the Customer Relationship Management acronym of CRM. You see, a customer of an enterprise portal is anyone who uses it: staff, management, executives, existing customers, new customers, stakeholders, suppliers…it can be a long list. And for each customer there needs to be a secure role and permissions based access mechanism. These roles and permissions need to extend into the heart of the enterprise software systems so that a supplier accessing the portal gains a completely different experience from a member of staff.

The Figures 5, 6, 7 below, provides the class diagram, sequence diagram and execution screen shot of Spatial Secure Design of CRM Web Services Application respectively

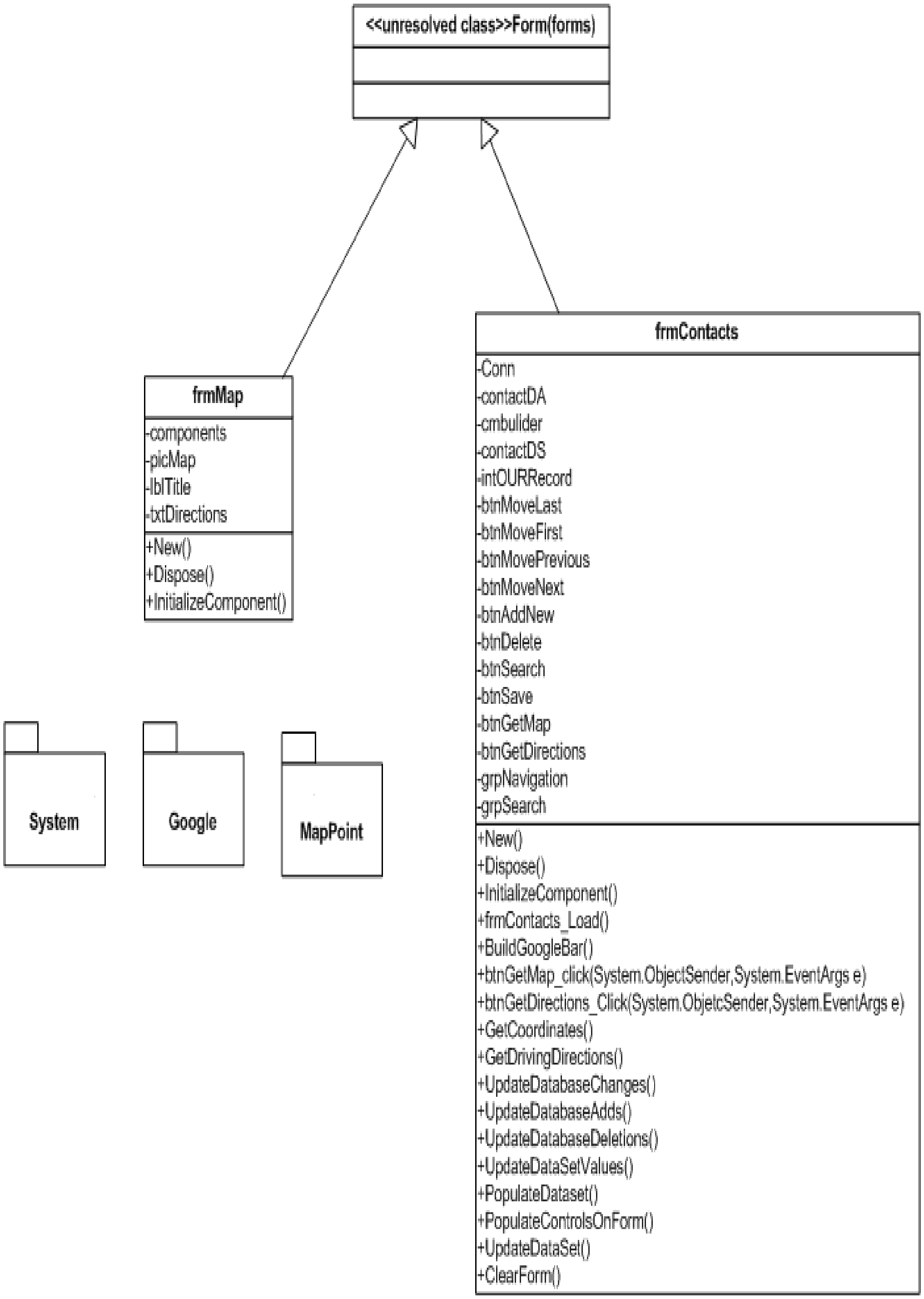


Figure 5 Class diagram of the Secure CRM application

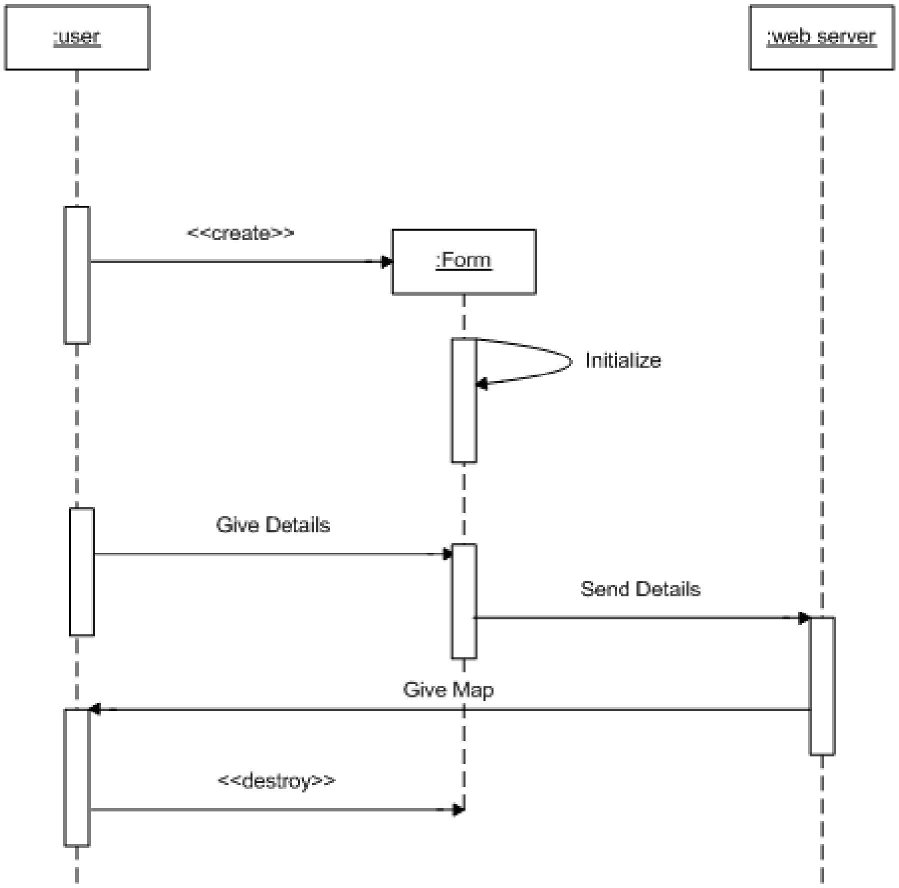
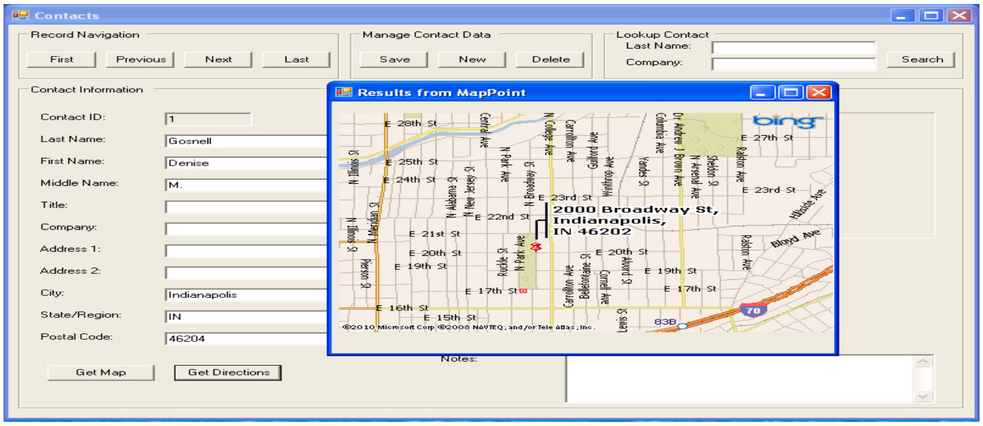


Figure 6 Sequence diagram of the Secure CRM application case study



Last Name:	
Company:	

Contact ID:	1
Last Name:	Gosnell
First Name:	Denise
Middle Name:	M.
Title:	
Company:	
Address 1:	
Address 2:	
City:	Indianapolis
State/Region:	IN
Postal Code:	46204

Figure 7 Execution Screen shot of the Secure CRM application case study

4. CONCLUSIONS

This research on Web Services Security Architecture is done using an innovative idea and novel implementations, of design of Model Driven Architecture (MDA) based Agile Modeling, for authentication and authorization of Web Service secure application design, for privacy management. We had validated our research with implementations on Web 2.0 Services Security Design, with its extension to Web 2.0 Mashup Spatial application, and various financial applications case studies. To start with, a methodology on Model Driven Architecture based Agile Modeled Layered Security Architectures is given based on preliminary research motivation. In this preliminary research, the major part is given to model architectural design rules using MDA so that architects and developers are responsible to automatic enforcement on the detailed design and easy to understand and use by both of them. This MDA approach is implemented in use of Agile strategy in three different phases covering three different layers to provide security to the system. With this procedure a conclusion can be given that with the system security the requirements for that system are improved. To summarize the preliminary work on Model Driven Architecture based Agile Modeled Layered Security Architectures:

The future scope of this work includes adapting agile lean project development strategies for web services security architecture design. This preliminary research on MDA based Agile Layered Security Architecture summarizes that security is essential for every system at initial stage and upon introduction of security at middle stage must lead to the change in the system i.e., an improvement to system requirements.

REFERENCES

[1] Alastair Airchison [2009], “Beginning Spatial with SQL Server 2008”, Apress Publisher, ISBN 978-1-4302-1829-6, Chapter 1, pp. 1 – 37.

[2] Alessandra Bagnato (Eds.), SEC MDA [2009], “Security in Model-Driven Architecture”, European workshop on Security in MDA 2009, Netherlands, ISSN No. 0929 – 0672. pp. 01 – 56.

[3] Anders Mattsson, Bjorm Lundell, Brian Lings, Brian Fitzgerald [2009], January/February 2009, “Linking Model-Driven Development and Software Architecture: A Case Study”, IEEE Transactions on Software Engineering, vol. 35, no. 1. pp. 83-93.

[4] Anoop Singhal, Theodore Winograd [2006], September 2006, "Guide to Secure Web Services”, National Institute of Standards and Technology (NIST) Draft, (800-95).

[5] Annekayem [2009], “Security in Service-Oriented Architectures: Standards and Challenges”, IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch009, pp. 187 –211. .

[6] Antonio Mano, Gimena Pujol, Antonio Munaz [2009], “Policy based Security Engineering of Service Oriented Systems”, IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch006, pp. 118 – 133.

[7] Asoke K. Talukder and Manish Chaitanya [2009], “Architecting Secure Software System” CRC Press, chapter 2, pp. 45 – 90.

[8] A Mohammad, G.Kannan, R.Kannan, T Khdour, S.Bani-ahmad, A.Alarabeyyat, [2011], “Toward Access Control Model for Web Services applications” in International Journal of Research and Reviews in Computer Science (IJRRCS) Vol 2 No 2 pp. 253- 264.

[9] Barbara Russo, Maro Scotto, Alberto Silliti [2010], “Agile Technologies in Open Source Development” IGI Global publishers 2010, pp. 217 – 244.

[10] Basin D, Burri S J, Karjoth G [2011] ,“Separation of duties as a service”, Proceedings of the Sixth ACM Symposium on Information, Computer and Communications Security, ACM, China, pp. 1 – 7 .

[11] Bernard Menezes [2010], “Network Security and Cryptography”, Cengage Learning India Pvt. Ltd., ISBN 978-81-315-1349-1, pp. 245 – 290.

[12] Bhavani Thuraisingham [2011], “Secure Semantic Service Oriented Systems”, Auerbach Publications, Chapter 1, pp. 1 – 17.

[13] Bruce Powel Douglass [2009], “Real-Time Agility, the Harmony/ESW Method for Real-Time and Embedded Systems Development”, Copyright at 2009 Pearson Education, Inc., pp. 1-31.

[14] Carlos Gutierrez, Eduardo Fernandez-Medina, Mario Piattini [2009], “Web Services Security Development and Architecture: Theoretical and Practical issues”, IGI Global, Information Science Reference. ISBN 978-1-60566-950-2, pp. 1 – 14.

[15] Cenzic Inc., [2009], “Web Application Security Trend Reports”, A White Paper, pp. 1 – 4.

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

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

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

[19] David Geer, [2003], “Taking Steps to Secure Web Services”, IEEE, October 2003, pp. 1 – 4.

[20] 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.

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

[22] 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

[23] 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.

[24] 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

[25] 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.

[26] 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

[27] 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.

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

[29] 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.

[30] 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.

[31] Francis HSU, Hao Chen [2009], “Secure File System Services for Web 2.0 Services”, CCSW 09, USA, ACM, November 2009, pp. 1 – 6.

[32] Frank Innerhofer-Oberperfler, Markus Mitterer, et al [2009], “Security Analysis of Service Oriented Systems – A Methodical Approach and Case Study”, IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch002, pp. 33 – 56.

[33] George Spanoudakis and Andrea Zisman [2010] ,“Discovering Services during Service-Based System Design Using UML”, IEEE Transactions on Software Engineering, Vol 36, No.3, May/June 2010, PP 371 – 389.

[34] Giorgia Lodi, Leonardo Querzoni, Roberto Beraldi, Roberto Baldoni [2008], “Combining Service-Oriented and Event-driven architectures for Designing Dependable systems”, pp. 1 – 13.

[35] Gunnar Peterson, LLC, 2007 “Security Architecture Blueprint”, Arctec Group, a White Paper, pp. 1 - 6.

[36] G.Rayana Gouds, M.Sriivasa Rao and Akhilesh Soni [2009], “Semantic Firewall: An approach towards Autonomous Web Security in Service Oriented Environments”, International Journal of Recent Trends in Engineering, Vol. 1, No. 1,ACEEE Academy Publishers pp. May 2009 454— 458.

[37] Halvard Skogsrud [2009], “Modeling Trust Negotiation for Web Services”, IEEE, February 2009, pp. 1 – 6.

[38] Heiko Tillwick and Martin S Olivier [2004], “A Layered Security Architecture: Design Issues”, in Proceedings of the Fourth Annual Information Security South Africa Conference (ISSA2004) July 2004, pp. 1 – 4.

[39] Hiren Bhatt, Arup Dasgupta [2011],“The Disruptive Cloud”, Geo Spatial World, May 2011 pp. 20 – 28

[40] Hohn S, Lowis L, Jurjens J, Accorsi R,, [2009], “Identification of vulnerabilities in Web Services using Model-based architecture”, IGI Global publishers, 2009, pp. 1 -32.

[41] Hossein Keramati, Seyed-Hassan Mirian-Hosseinabadi [2008], “Integrating software development security activities with agile methodologies," aiccsa, IEEE/ACS International Conference on Computer Systems and Applications pp.749-754.

[42] I.Lazar, B. Parv, S. Motogna, I.-G. Czibula, C.-L. Lazar [2007], “An Agile MDA approach for Executable UML Structured Activities”, Studia Univ. Babes-bolyai, Informatics, vol. LII, No. 2, , pp.111-114

[43] Jameela Al-Jaroodi, Alyaziyah Al-dhaheri [2011) “Security issues of Service-oriented middleware”, In International Journal of Computer Science and Network Security Vol 2 No 1, pp. 153 – 160.

[44] James S.Tiller [2011], “Adaptive Security management Architecture”, Auerbach Publications, pp. 1 – 14.

[45] Jeremy Epstein, Scott Matsumotto and Gary McGraw [2006], “Software Security and SOA: Danger, Will Robinson”, IEEE Security and Privacy, January/February 2006, pp. 80–83.

[46] Jim Gray, Microsoft Research [2002], “Real Web Services” Talk at Charles Schwab Technology Summit, Friday, September 20, 2002, a ppt presentation pp. 1 – 23.

[47] Jim Highsmith, Alistair Cockburn [2001],“Agile Software Development: The Business of Innovation”, IEEE Computer September’2001 pp:120 –122

[48] Joao Antunes, Nuno Neves, Miguel Correla, Paulo Verissimo, Rui Neves [2010], “Vulnerability Discovery with Attack Injection”, IEEE Transactions on Software Engineering, Vol. 36, No. 3, May/June 2010, pp. 357-369.

[49] Johan Peeters [2005], “Agile Security Requirements Engineering”, on Requirements Engineering for Information Security, 2005. available at psu.edu 10.1.1.91.4183., pp. 1 – 6.

[50] John Hunt [2006], “Agile Software Construction”, Springer Verlag publishers 2006, pp. 45 – 64.

[51] J J Whitmore [2001], “A method for designing secure solutions”, IBM Systems Journal, Vol 40 No 1 2001, pp. 747 – 768

[52] Kanchan Hans [2010], “Cutting edge practices for Secure Software Engineering”, in International Journal of Computer Science and Security IJCSS Voume 4 Issue 4 pp. 403 – 408.

[53] Kearsten Sohr, Michael Drouieaud, Gail Joon Ahn, Martin Gogolla [2008], “Analyzing and Managing Role-Based Access Control Policies”, IEEE Transactions on Knowledge and Data Engineering, Vol. 20, No. 7, July 2008, pp.924-939.

[54] K.V.S.N.Rama Rao, Anirban Pal, and Manas Ranjan Patra [2009], “A Service Oriented Architectural Design for Building Intrusion Detection Systems”, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009 ACEEE Academy Publishers Poster Paper pp. 11— 14.

[55] Li Liang Xian [2011], “Research of B2B e-Business Application and development technology based on SOA” In W.W.Song et. al. (eds) Information Systems Development Springer Science + Business Media, LLC 2011, pp. 367 – 375.

[56] Lorenzo D Martino, Elisa Bertino [2009], “Security for Web Services: Standards and Research Issues”, International Journal of Web Services Research, Oct-Dec 2009, , Idea Group Publishing USA 2009, pp. 48-74.

[57] Luigi Coppolino, Luigi Romano, Velerio Vianello [2011], “Security Engineering of SOA applications via Reliability patterns”, Journal of Software Engineering and applications pp. 1-8 January.

[58] M.Siponen, R.Baserville, T.Kuvalainen [2009],”Extending Security in Agile Software Development Methods”, pp. 143 – 157.

[59] Marzouk.S.Mokbel, Le Jiajin [2005 – 2008], “Integrated Security Architecture for Web Services and this Challenging”, In Journal of Theoretical and Applied Information Technology JATIT pp. 518 – 525.

[60] Mali, Jiang Cheng-yan [2009], “A research on Web Security Service Architecture” in Journal of Chongqing Electric Power College China, pp. 1 – 34.

[61] Martin Naedele [2003], “Standards for XML and Web Services Security”, IEEE April 2003, pp. 6 – 14.

[62] Mark Harman, Afshin Mansouri [2010], "Search based Software Engineering Introduction to the special issue of the IEEE Transactions on Software Engineering", November December 2010, pp. 737 – 741

[63] Massimo Barloletti, Pierpaolo Degano, Gian Luigi Ferrari, Roberto Zunino [2008] , "Semantics-Based Design for Secure Web Services", IEEE Transactions on Software Engineering, Vol 34, No.1, January 2008, pp. 33 – 49.

[64] Matt Bishop [2003], "Computer Security Art and Science", Pearson education, pp. 56 – 97.

[65] Meiko Jenson, Nils Gruschke, Ralph Herkenhoner [2009], "A Survey on attack of Web Services Classification and Counter measures", Journal Computer Science Research and Development Vol 24 No 4, November 2009, pp. 185 – 197

[66] Michael S Kirkpatrick, Elisa Betrino [2010], "Enforcing Spatial Constraints for Mobile RBAC Systems", ACM 2010 SACMAT10, June 9-11, 2010, Pittsburg, USA, 99. 1 –6.

[67] Michael Juntao Yuan, 2004, "Enterprise J2ME Developing Mobile Java Applications", Pearson Education Inc., ISBN 81-297-0694-6, pp. 145 – 196.

[68] Michele Barletta, Alberto Calvi, Silvio Ranise, Luca Vigano, Luca Zanetti [2011], "Workflow and access control reloaded. A declarative specification framework for the automated analysis of web services" Scalable Computing Volume 12 Number 1 pp. 1-20

[69] Mokbel M.S., Jiajin. L, [2005 – 2008] "Integrated Security Architecture for Web Services and this challenging", Journal of Theoretical and Applied Information Technology JATIT, pp 518 – 525.

[70] Mouratidis and Giorgini [2007], "Security and Software Engineering: Advances and Future Vision." Idea Group Publishing Inc., pp. 1 – 17.

[71] Mordinyi, R.Kuhn, E Schatten [2010], "Towards an Architectural Framework for Agile Software Development" in IEEE 17th International Conference and Workshop on Engineering of Computer Based Systems (ECBS), pp. 276-280.

[72] Munindar P.Singh, Michael N.Huhns [2005], "Service Oriented Computing, Semantics, Processes, Agents", John Wiley & Sons, Ltd, pp. 45 – 97..

[73] Murat Gunestas, Dumminda Wijesekera [2009], "Forensics over Web Services: The FWS", IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch005, 83 – 98.

[74] Nakamura Y, Tatsubori M, Imamura T, Ono K, SCC [2005] ,"Model driven Security based on a Web Services Security Architecture", proceedings of the 2005 IEEE International Conferences on Services Computing, pp. 1 – 15.

[75] Nico Brehm, JorgeMarx Gomez [2009] , "Secure Service Rating in Federated Software Systems based on SOA", IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch004, pp. 83 - 98.

[76] Nina Godbole [2009], "Information Systems: Security Management, Metrics, Frameworks and Best Practices", Wiley India Publishers, Preface pp. 1 – 14.

[77] Nils Agne Narbotten [2009] , "XML and Web Services Security Standards", IEEE Communications Survey and tutorials, Vol 11, No 3, Third Quarter, pp. 4 – 21

[78] Ozgur Erol et al, [2009], "A Framework for Enterprise Resilience using Service Oriented Architecture approach", IEEE Sys Con 2009, 3 rd annual IEEE International Conference March 23 – 26.

[79] Patrick Stuedi, Iqbal Mohammed, Doug Terry, [2010], "Where Store: Location-based Data Storage for Mobile devices Interacting with the Cloud", MCS 10, ‚San Francisco USA, ACM 2010 , (Microsoft Research) , June 15, 2010 , pp. 1 – 10.

[80] Rafuel Accorsi, Claus Wonnemann: Indico. "Information flow analysis of Business Processes for confidentiality requirements", pp. 1-16

[81] Reza B'Far [2005], "Mobile Computing Principals – Designing and Developing Mobile Applications with UML and XML", Cambridge University Press, ISBN: 0-521-69623-2, pp. 146 – 198.

[82] Ross Anderson, 2003, "Security Engineering: A guide to building Dependable Distributed Systems", Wiley publishers, pp. 1 – 19.

[83] Sami Baydeda, Matthias Book, Volker Gruhn (Eds.) [2005], "Model-Driven Software Development", © Springer-Verlag Berlin Heidelberg, pp. 18-22.

[84] Sandeep Chatterjee [2004], "Developing Enterprises Web Services An Architects Guide", Pearson, pp. 67 – 98.

[85] Sasikanth Avancha [2008], "A Framework for Trustworthy Service Oriented Computing", ICISS 2008, pp. 124 – 132.

[86] Sarah Spiekermann, Lorrie Cranor [2009], “Engineering Privacy”, IEEE Transactions on Software Engineering”, Vol 35 No 1 January February 2009 pp. 67 – 82

[87] Satoshi Makino, Takeshi Imamura, Yuichi Nakamura [2004], “Implementation and Performance of WS-Security”, International Journal of Web Services Research, Jan-March 2004, Idea Group Publishing, pp. 58-72.

[88] Sebastian Hohn, Lutz Lowis, Rafael Accorsi, Albert- Ludwig [2009], “Identification of Vulnerability Effects in Web Services using Model-Based Security” IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch001, pp. 1 – 32.

[89] Soumya Simanta, Ed Morris, Sriram Balasubramaniam, Jeff Davenport and Dennis B.Smith [2009], “Information Assurance Challenges and Strategies for Securing SOA Environments and Web Services”, IEEE SysCon 2009—3 rd Annual IEEE International Systems Conference, Vancouver, Canada, March 23 – 26, pp 1 – 4.

[90] Spyvain Halle, Roger Villemaire, Omar Cherkaoui [2009], “Specifying and Validating Data-Aware Temporal Web Services properties”, IEEE Transactions on Software Engineering, Vol 35, No. 5, pp. 669 – 683.

[91] Spyros T Halkidis, Nikoloas Tsantalis, Alexander Chatizigeorgiou, George Stephanides [2008], “Architecture Risk Analysis of Software Systems based on Security Patterns”, IEEE Transactions on Dependable and Secure Computing Vol 5 No. 3, pp. 129 – 142

[92] Srinivasa Narayana, Subbu N Subramanian, Manish Arya, and the Tavent team, [2006], “On engineering Web-based Enterprise applications”, International conference on Management of Data, COMAD 2006 CSI 2006, pp. 113 – 119.

[93] Stephen J Miller [2004], “Agile MDA – A White Paper”, pp. 1 – 6.

[94] Stephan J H Yang, Blue C W Lan, James S.F.Hsieh, Jen-Yao Chung [2007], “Trustworthy Web Services: An experience-based model for trustworthiness evaluation” In International Journal of Information Security and Privacy, Volume 1 Issue 1, Idea Group publishing, pp. 1-17.

[95] Stephan Bode, Anja Fischer, Winfried Kuhnhauser, Matthias Riebisch [2009], “Software Architectural Design meets Security Engineering”, 16th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 109 – 118.

[96] Subhash C.Misra, Vinod Kumar, Uma Kumar [2009] “An Approach for Intentional Modeling of Web Services Security Risk Assessment”, IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch015, pp. 295 – 308.

[97] Sumeet Gupta, Mayank Mathur et al [2009], “Threat Modeling: Security Web 2.0 based Rich Service Consumers”, IGI Global, Information Science Reference, DOI:10.4018/978-1-60566-950-2.ch011, 228 – 246.

[98] S.Michelle Oda, Huirong Fu and Ye Zhu [2009], “Enterprise Information Security Architecture A Review of Frameworks, Methodology, and Case Studies”, IEEE pp. 333 – 337.

[99] Tao Xu, Chunxio Yi, [2011], “SOAP-Based Security interaction of Web Service in Heterogeneous Platforms” In Journal of Information Security pp.1-7.

[100] Tim O Rielly, John Battella [2009], “Web Squared: Web 2.0 five years on”, Web 2.0 summit, 2009, Orielly Inc, pp. 1 – 6.

[101] Vipul Gupta, et. al [2005], “Sizzle: A standards-based end-to-end security architecture for the embedded Internet”, Elsevier, Pervasive and Mobile Computing, pp. 1 – 19.

[102] Wembo Mao, 2004. “Modern Cryptography: Theory and Practice”, Pearson education, pp. 1 – 12.

[103] Wei She, et. al., 2010, “Enhancing Security Modeling for Web Services using Delegation and Pass-on”, International Journal of Web Services Research, Jan-March 2010, Idea Group Publishing USA, pp. 1-21.

[104] Xiaocheng Ge, Richard F Paige, Fiona A.C.Polack, Howard Chivers, Phillip J Brooke, “Agile development of Secure Web Applications”, ACM ICWE 06 pp. 305-312.

[105] Yann-Gael Gueheneuc, Giuliano Antoniol [2008], “DeMIMA: A Multilayered Approach for Design Pattern Identification”, IEEE Transactions on Software Engineering, vol. 34, no. 5. September/October 2008, pp. 667-684.

[106] Zoran Stojanovic, Ajantha Dahanayake, [2005] “Service-Oriented Software System Engineering: Challenges and Practices”, Idea Group Publishing, pp. 34 – 46.