Literature Survey on Agile Security Architecture Model

M.Upendra Kumar
Associate Professor CSE MGIT Hyderabad India

Abstract
In this paper a detailed literature survey on significant topics of Agile Security Engineering are provided to find out the problem statement and find out basis of research.

Keywords — *Literature Survey, Agile Modelling, Security Architecture.*

I. INTRODUCTION

LITERATURE SURVEY

1.1 REVIEW OF LITERATURE AGILE SECURITY ARCHITECTURE MODEL

The area of present research work consists of Software Engineering, Security Engineering, Software Architecture, Security Architecture, Layered Pattern, Model Driven Architecture (MDA), Agile Software Development, Designing Solutions, Dependable Privacy Requirements, Next Generation Secure Web Engineering Applications Case Study using Agile Modeling, Web Services, and Web 2.0. The area of research work is relatively new one in the Information Technology 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.

1.1.1 REVIEW OF LITERATURE ON MDA EXTENDED AGILE LAYERED MODELED SECURITY ARCHITECTURES

Software Engineering

Next generation software developers need to face the same problems for software engineering design complexity and structure, for software economics, and performance improvement as faced traditionally and evolutionary software development [8]. Software Engineering as projected for year 2049, estimates that security design, agile design modeling, web engineering, web science, web 2.0 services, needs systematic development strategy, which can provide efficient maintenance of these applications for even 20 years [9]. CHARMY provides a framework for design and verification of architecture specification [26]. Enterprise architectures needs a quantitative approach using patterns based approach [27].

Secure Software Engineering or Security Engineering

Security Professionals who have expertise in integration of security and software engineering principles have great job placement requirements [13]. Integrating security into software development needs a long vision and strategy as it has its own challenges [14].

Software Architecture

Software architecture design and development needs a strategy for emerging discipline [20]. Unified Modeling Language (UML) is the defacto standard for software systems modeling and its new versions is UML 2.0 which came supporting for new software applications domain [21]. Object oriented systems can be made more reusable with the usage of design patterns which are solutions for recurring design problems [23]. DEMIMA is a multiple layers approach used for identifying design pattern in software applications [48].

Security Architecture

Security requirements elicitation using common criteria and UMLSec can be traced to design phase by specifying a methodology called SecReq [41]. Security patterns can be detected in software using architectural approach using reverse engineering tools [43]. One of the major obstacles for secure software development is complexity of emerging software systems development [15]. Security architectures can be implemented for security requirements by enforcing threat modeling [24]. Security architectures are required for enterprises which can be implemented at various layers using a design framework for improving security of enterprise completely [32].

Security patterns can be applied at all phases of software development and they can be evaluated for their effectiveness for each phase of their application and integration [33]. Security patterns can be classified based on the phase they are integrated and implemented. Security patterns are specializations of design patterns applied for security

[34]. Enterprise architectures for security design require various frameworks and methodology, for securing business strategy of enterprises, with case study of Oakland University [38]. Vulnerabilities on secure applications can be discovered by applying various attack injections on them, so that dependability of the system can be known [42].

Layered Security Architecture

Secure information systems can be designed using layered architecture as a security model at various levels of system layers. Dependency among various layers pertaining to security requirements will result by using design approach of a layered architecture for a security [46]. Pattern templates which can be usable can be developed for Security Architectures design, for real world applications [44]. Enterprise security architectures can be developed using tools like SABSA layered architecture [45]. Layered software architecture performance can be evaluated using layered architecture using tool called SHARPE [47]. Layered approach can be used for information systems using a novel approach for security architecture design for network security simulation [49]. Enterprise Policy design can be provided more abstraction and can be refined easily based on a layered approach [50].

Model Driven Architecture (MDA)

MDA extended UML design can be used for extend role based access control with Secure UML and UMLSec for designing access control mechanisms [39]. Model driven development can be linked to Software architectures and can be validated by case study [52]. Developing next generation software applications complexity can be reduced and needs a research strategy using model driven development [53]. Model driven architectures can relate to requirements based on concepts of views and traces and this is validated using Service Oriented architectures (using Web Services) [54]. Model driven architectures can be used for business rules and its modeling languages [69].

Agile Methodologies and Security

Software developers need to integrate security with agile development methodologies for providing systems with reasonable security like authentication and / or authorization in them. Integrating agile methodologies with security enhances overall product trust worthiness [77]. Agile processes based on extension of MDA approach, create flexibility for developing, executing and testing in weekly, incremental and iterative phases, using executable UML design [61]. Traditionally it was felt that agile processes are in contradiction to developing secure software because of their light weight and not very formal approach. Abuser stories can be used for agile security requirements [91]. One of the predominant usages of agile processes is extreme programming which needs to give architecture important relevance and should be made security [25].

Agile Software development basically uses a people oriented approach for organized teams [55]. Documentation of Agile architectures can be done extending Views and Beyond (V and B) architecture documentation [56]. Most successful usage of agile software development is applied by using extreme programming methodology for changing requirements [57]. Java programming language can be used following agile software development by using extreme programming test driven development [58]. Microsoft Visual Studio Visual C# programming language can also be implemented using agile patterns [60]. Agile software development has many approaches like extreme programming, feature driven development, lean development, scrum etc. [59]. Agile Software Engineering extends traditional software engineering principles tailed to agile specific methodology for reducing cost and time in software development [62]. Empirical software engineering approach can be used for agile development by following systematic approach for extreme programming and scrum [63].

Python open source scripting language can be used effectively for agile software development for web applications development [64]. Open source development now a day is only using agile development with support of many tools like Java Bugzilla for bugs identification and resolution etc [65]. Pair programming is one of the most important agile development methodologies with good performance [66]. Pair programming most of the time success depends on personality of pair of customers and developers [67]. Agile teams now think that having agile architectures design, improves success rate of agile projects [68].

Agile development can be used for systems engineering using collaborating engineering approaches [70]. Agile methods can be used effectively because of their short life cycle development for security analysis and design for information security and information warfare with fastness [72]. This literature survey paper on agile security approaches provides in depth analysis of existing security agile models covering all areas of life cycle and iterations [73]. Agile security can be extended for security requirements with models proposed, for inter linking between requirements and design [74]. Agile security engineering can be achieved for security assurance using a research methodology and using empirical studies [75].

Agile plus model extends traditional model for requirements phase for better requirements elicitation [76]. Agile Security can be implemented

for Information Technology management using agile modeling with various threats modeling for real world Information Technology scenarios [78]. Secure software development in agile process can be achieved for dependability risk assessment [79]. Agile security solutions can be implemented for network security, irrespective of underlying network protocols used for communications [80].

Agile authorizations can be used for security usability at individual level, for obtaining privacy requirements management of individuals [81]. Agile processes can be extended for dependability integration for designing and developing acceptable secure software [82]. Various agile security models are proposed for all phases of life cycle for better security vulnerability assessments [83]. Various security metrics are proposed for risk management for agile software development for providing dependable risk identification and risk mitigation [90].

Designing Solutions

Software engineering for developing secure systems needs to focus upon dependability design of systems [16]. Designing for security, needs application of engineering principles for security architecture design [28]. Solutions for Designing security requires a systematic approach modeling security architectures for obtaining increased trust (an attribute of dependability of Information Technology Security solutions [84]. From end users security perspective, providing security is much more than providing just enough security but rather it is more about the designing of useful secure application, whose design can be more reusable [85].

Dependability

Instead of integrating security late at the end of life cycle, it always better in terms of saving cost, effort involved if security is integrated at early requirements specification phase or even at design phase. Security patterns are to security architectures in relation with design patterns are to software architectures. Risk analysis (a feature of Dependability) on software systems can be performed on software applications based on the internal security patterns they have hidden in them [35]. Major objective of security engineering should be to build dependable distributed systems. Various dependability approaches are available based on software architecture approach for improving software dependability and quality attributes [86]. Dependable and secure computing in terms of design of secure architectures for dependable and also fault tolerant systems are needed for addressing various domains of users and their areas of applications [87]. Security requirements engineering framework based on vulnerabilities in requirements, design, implementation etc. is proposed for analyzing security attacks and their required countermeasures [92]. Many methodologies are available for Security Requirements engineering starting from inception of requirements elicitation to documentation of security requirements [93].

Designing Dependability for Agile Modeling

Securing India's future regarding web science needs dependability design using agile modeling [18]. Risk management can be balanced between agile methods and traditional plan driven methods [71].

Privacy Management

Security enforcement needs to focus on users privacy management in the policies, for development of secure software applications [17]. Information security management for metrics, frameworks requires best practices for privacy management of web services and web 2.0 [19]. The relationships between requirements and architecture knowledge can be obtained and refined (as they are inter related), by following various interactions in iterative development processes [22]. Based on users profiles and their classification can be done using various security patterns needed [40]. Security testing for quality assurance can use fuzzy techniques, with many open source tools available, for providing flexibility for developing own customized tools for privacy management using fuzzing [88]. Privacy management is an attribute of dependability for secure software engineering application design [89]. Legal rules for privacy requirements and security requirements needs to be analyzed and regulated for obtaining accurate security requirements and provide better privacy protection and works within the lines of legal aspects of computing [94]. Security Requirements and specifications can be found for buggy software and their privacy ramifications can be inter related [95]. Engineering principles can be applied for privacy management for policy by architecture using a layered approach at data storage layer, processing layer and storage layer [96]. Security requirements engineering process as applied to Rational unified process (RUP) with a case study and other Security requirements strategies are proposed for better security requirements elicitation [97].

Evolution of software engineering as web engineering

Web Engineering is the application of pragmatic approach for designing effective web based applications [117]. Model driven approach can be applied for web engineering requirements using NDT [51].

REVIEW OF LITERATURE ON NGSWEA CASE STUDY

Agile Modeling for web services and web 2.0

Service Oriented Engineering using Agile and Lean software development applies advanced information technology solutions for changing customer requirements in demanding business environments [116]. Security architectures are developed for case studies like web based healthcare insurance systems with privacy preservation of patients [28]. Network security architectures can be used with integration of patterns concepts, with reusability of patterns of protocols which can be open in interconnections [30]. For educational applications like e-learning, access control mechanisms can be designed for security architectures, extending role based access control for context aware (what the user in doing at that instance of time called a context) access control [31]. Security architecture implemented using a secure application design for police force based on mobile domain [36]. Agile Process as applied to Web Engineering with a case study on financial enterprises like fortune 500, for deeper analysis is investigated for inter dependency of agile modeling and web engineering [98]. Agile software development using feature driven development for dependable risk assessment with a case study on web applications is proposed [99]. Developing new generation enterprise applications uses emerging competencies with a paradigm called software 2.0 which coins the term Web Science and it uses integrated technologies like Web 2.0, Web Services, Cloud computing, Web Engineering etc [100]. Agile software development can be used for web services design for services responsibility and their interactions designs [103]. Model driven architecture is applied to web services security architecture, with a validation of case study [106]. Applying traditional security engineering principles to service oriented architectures and web services has many pitfalls and these dangers need to be taken care of [107].

Web services

SOA security Architecture practicing is right for security, the same option leads to disaster if security done in wrong [108]. Principles of network security using cryptography can be applied on case studies like Web Services using protocols like WS-Security [111]. Dependability for web services also involved trust negotiation policies for autonomous services using state machine based modeling approach [110]. Design of architecture for securing Web services is a methodological approach in designing safety architectures for complete development life cycle of web service based systems [112]. Service based systems are composed of autonomous services requires UML based frame work for new methods processes and tools [113]. Service Oriented systems can be secured semantically by designing access control and accountability for secure infrastructure and storage issues [114]. Security vulnerabilities of Web services can be identified using model based approach. Web services composition, business processes, orchestration of processes and services needs to be designed for security. Evolving security challenges of web services for Service Oriented Architectures needs to integrate model based engineering and vulnerability identification. Trust worthiness is an attribute of dependability which can be implemented as a framework for service oriented computing for designing scalable solutions [109]. Threat modeling and threat analysis for web applications and web services applications in particular are proposed for security risk assessment [104]. Dependability for fault tolerance using Web services security architectures is proposed for better security requirements elicitation [105].

Web 2.0

Major predominant application of Web 2.0 mashups is used by business analytics using business intelligence mashup tools for enhanced user experiences [115]. For web 2.0 rich service consumers threat modeling is required using informal methods. Web 2.0 applications have access to wide range of public like customers and partners, which needs to be secured [101]. Various application areas of Web 2.0 are proposed like e-learning, intelligence social networking, marketing research, image retrieval, personalized technologies are proposed [102].

CONCLUSIONS

This Paper dealt with Review of Literature on Designing Dependable Agile Layered Security Architecture Solutions, with case study on Next Generation Secure Web Engineering Application. After going through the detailed study of literature survey, it is found that there is a need to develop a comprehensive procedure for designing agile security model which extends MDA for securing web 2.0 services for authentication so that this work paves a way for secure web engineering applications design and development. An attempt is made to investigate a detailed procedure for agile security model for secure web 2.0 engineering application in further papers. In the next paper, theoretical analysis on these topics is provided with initial case study validations, so that work can be elaborated on.

REFERENCES

[1] Siv Hilde Houmb, Shareeful Islam, Eric Knauss, Jan Jurjens, Kurt Schneider," Eliciting Security Requirements and Tracing them to Design: An Integrating of Common Criteria, Heuristics, and UMLsec", 2009, PP. 1-6.

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

[3] Michaela bunke and Karsten Sohr, "An Architecture Centric approach to Detecting Security Patterns in

Software", Springer, ESSoS LNCS 6542, 2011, PP. 156 – 166.

[4] Santiago Moral-Garcia, Roberto Ortiz, Santiago Moral Rubil, Javier Garzia, "A new pattern template to support the design of security architectures: A case study", International Journal on Advances in security, Vol 4 no 3&4, year 2011, PP. 173 - 184.

[5] Shahram Jalaliniya, Farzaneh Fakhredin, "Enterprise Architecture and Security Architecture Development", Master Thesis, Department of Informatics, Lund University, June 2011, PP.1 -95.

[6] Heiko Tillwick, Martin S Olivier, "A Layered Security Architecture: Design Issues", in Proceedings of the Fourth Annual Information Security South Africa Conference (ISSA 2004), July 2004, PP. 1 -6.

[7] Vibhu Saujanya Sharma, Pankaj Jalote, Kishor S.Trivedi,"Evaluating Performance Attributes of Layered Software Architecture", CBSE 2005 LNCS 3489 PP. 66-81.

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

[9] George Farah," Information Systems Security Architecture: A Novel Approach to Layered Protection", SANS Institute, September 2009, PP. 15-16.

[10] Marshall Abrams and David Bailey, "Abstraction and Refinement of Layered Security Policy", Information Security, PP. 126-135.