Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 38 (2012) 2799 – 2807

Procedia Engineering

www.elsevier.com/locate/procedia

International Conference on Modeling, Optimization and Computing (ICMOC-2012)

Security Requirements Engineering Process for Web Applications

P.Salini[a] ,S.Kanmani[b,a]*

[a]*Department of Computer Science and Engineering, Pondicherry Engineering College, Pillachavady, Puducherry, 605014, India*
[b]*Department of Information Technology, Pondicherry Engineering College, Pillachavady, Puducherry, 605014, India*

Abstract

In the recent years, tasks such as the Security Requirements Elicitation, the Specification of Security Requirements or the Security requirements Validation are essential to assure the Quality of the resulting software. An increasing part of the communication and sharing of information in our society utilizes Web Applications. Last two years have seen a significant surge in the amount of Web Application specific vulnerabilities that are disclosed to the public because of the importance of Security Requirements Engineering for Web based systems and as it is still under estimated. Therefore a thorough Security Requirements analysis is even more relevant. In this paper, we propose a Model oriented Security Requirement Engineering Process for Web Applications and applied our Process for E-Voting system. By applying Modeling technologies to Requirement phases, the Security requirements and domain knowledge can be captured in a well-defined model and it is better than traditional process.

Keywords: Web Security ,Security Requirements, Security Requirements Engineering and Web Applications

1. Introduction

The requirements must be clear, comprehensive, consistent and unambiguous. This statement has significance for security requirements and if you say application must be secure, it is not security requirements. It is hard to construct secure web applications or to make statements about security unless we

* Corresponding author. Tel.: 09994738640.
E-mail address: salini@pec.edu.

1877-7058 © 2012 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.06.328

know what to secure, against whom and at what extent. To this day, not one web application technology has shown itself invulnerable to the inevitable discovery of vulnerabilities that affect its owners' and users' security and privacy. Most security professionals have traditionally focused on network and operating system security. Assessment services have typically relied heavily on automated tools to help find holes in those layers. Security Requirements engineering (SRE), a phase that comes before design and programming, will play a more important role that determines the success of Web Applications Design.

In fact Security requirements engineering should be as complex and well thought out as the design and programming, yet its insufficiencies have led to many projects with poor Security requirements and blamed as the major reason for many web applications' failures. Therefore, Security requirements engineering is now moving to the forefront of gaining increased significance in software engineering for services oriented web applications. Web applications requirements have new characteristics causing them to change more rapidly. This makes traditional Security requirements modeling and validation methods insufficient to provide adequate support for web applications. So it is essential to capture the corresponding security needs and requirements to fulfill business goals, build trustworthy systems, and protect assets. Most requirement documents were written in ambiguous natural languages which are less formal and imprecise and it is hard to analyze and integrate with artifacts in other phases of software life cycle.

The Security requirements of the web applications come from not only the general domain analysis and the personalized, diverse users' requirements, but also the availability of the related web services. Web applications Security requirements are also evolving while they are widely used. Most of the methodologies that have been proposed for the development of Web applications focus only on Non Security requirements and paying no attention to the Security requirements engineering. Therefore, SRE for Web applications is challenged to explore sound engineering approaches for eliciting, describing, validating and managing Security requirements of Web applications and its integration with the artifacts of other phases can be cost effectively improved and can effect a significant reduction of the problems currently encountered in the SDLC for Web Applications due to poor Security Requirements Engineering and Management.

1.1. The importance of Web Applications Security

The importance of Securing Web Applications is that, often a web application is the only thing standing in the way of an attacker and sensitive business information, firewalls can only stop network service attacks and depending on the application an attacker may be able to View or manipulate sensitive information, Obtain unauthorized access to an application and also able to take control of the whole application.

Web Applications Security is about protecting assets and assets may be tangible or they may be less tangible. When to analyze your infrastructure and applications, you can identify potential threats and each threat presents a degree of risk. Web Applications Security is about risk management and implementing effective countermeasures. The Web Applications Security goals are Authentication, Authorization, Auditing, and (CIA) Confidentiality, Integrity and Availability. The security requirements identified in requirements engineering phase have to satisfy all these security goals of web applications. To build secure Web applications, threats, vulnerability and security requirements for network, host and applications should be identified. An ever-increasing number of attacks target your application. They pass straight through your environment's front door using HTTP. The reliance on firewall and host defences are not sufficient when used in isolation. To secure web applications, means it involves security at three layers: the network layer, host layer, and the application layer.

The development of Secure Web applications has several characteristics that differ from the development of other kinds of applications. On the one hand, many different kinds of stakeholders participate in the development process: analysts, customers, users, graphical designers, marketing, multimedia and security

experts, etc. On the other hand, the main features of these systems are the navigational structure, the user interface and the personalization capability. So along with analysis of domain of the business, the infrastructure or the environment where you use web applications must be analyzed.

1.2. Overview of this paper

In this paper we present a process for Security Requirements Engineering for Web Applications (MOSRE-WebApp). So, the remainder of this paper is structured as follows: First we establish a process MOSRE-WebApp in Section 2 followed by Section 3 presents the result analysis, discussion and comparison of SRE methods with proposed work and last Section 4 concludes with future works.

2. MOSRE-WebApp Process

Web application has become more and more critical in every domain of the human society. Transportation, communications, entertainment, health care, military, e-commerce, and education; the list is almost endless. These systems are used not only by major corporations and governments but also across networks of organizations and by individual users. Such a wide use has resulted in these systems containing a large amount of critical information and processes which inevitably need to remain secure. Therefore, although it is important to ensure that Web Applications are developed according to the user needs, it is equally important to ensure that these applications are secure.

However, the common approach towards the inclusion of security within a Web Applications is to identify security requirements after analysis, means that security enforcement mechanisms have to be fitted into a pre-existing design, leading to serious design challenges that usually translate into the emergence of computer systems afflicted with security vulnerabilities. Recent research has argued that from the viewpoint of the traditional security paradigm, it should be possible to eliminate such problems through better integration of security and requirements engineering. Security should be considered from the early stages of the development process and security requirements should be defined alongside with the system's requirements specification.

The Security Requirements Engineering is the process of eliciting, specifying, and analyzing the security requirements for system fundamental ideas like "what" of security requirements is, it is concerned with the prevention of harm in the real world and considering them as functional requirements. Many methods have been developed that facilitate this kind of requirements analysis and the development of security requirements. The internet has already created social and economic opportunities for people around the world. But even there are many Challenges to Web Applications Security like threats, attacks, phishing spyware, worms, Trojans and virus which cause to denial of service hacking into and defacing web sites and destroying. Here we present the proposed work; MOSRE-WebApp a model oriented Security Requirements Engineering Process for Web Applications. So the completeness, consistency, traceability and reusability of Security Requirements can be cost effectively improved.

Our Process follows the spiral process model which is iterative and all phases of Requirements Engineering are covered in this Process.

2.1. Inception

Inception is to establish the ground work, before to start the elicitation and analysis of security requirements for web applications. Different steps are involved in the inception phase of MOSRE-WebApp.

Step 1 Identify the Objective of the Web Applications

The Web Applications objective must be identified from the customer requirements who needs the Web Application. This process will help to understand the domain of the application that customer needs.

Step 2 Identify the Stakeholders

The identification of stakeholders plays an important role in security requirements engineering. The stakeholders include the Architect, developer, customers/end users, security experts, requirements engineering team and other interested people. Each stakeholder is responsible to find the assets and security goals. The security experts help in finding the security requirements and security mechanisms to obtain high level of security to the Web Applications. The stakeholders will have multiple view points on the security requirements of the system. It may be conflicting security requirements and the stakeholders will help to prioritize the assets and security requirements of the system. So care to be taken to prepare the list of stakeholders, to improve the effectiveness of preliminary communication and collaboration between the stakeholders.

Step 3 Identify the Assets

The next step is to identify the assets of the targeted system. Assets may be business or system assets (e.g.: data, money, and password). From our survey it is found that assets identification is an important step in security requirements engineering. This could range from confidential data, such as customer or database, to Web pages or Web site availability.

The assets should be identified in the context of the software system, so the objective of software system is to be identified first. To identify the assets different techniques like interview, questionnaire, and brainstorming can be used. The stakeholders help in finding the assets. Assets should be viewed not only at developer or customer/end user perspective but also in attacker's point of view. Assets can be identified from existing documents. The identified assets have to be categorized and prioritized with regard to different stakeholders need. Assets can be categorized under Confidentiality, Integrity and Availability and prioritized as low medium and high level of preference. Example password can be categorized under confidentiality. After the list of assets is identified and categorized, the level of security to be implemented in the web application is fixed. Five levels of security can be implemented for web applications based upon the value of the assets.

Inception phase of security requirements engineering should be worked with high level of collaboration and care.

2.2. Elicitation

The next phase in security requirements engineering is elicitation, the stakeholders and requirements engineering team will work together to identify the problem, propose the solution and specify the set of security requirements. There are different steps involved in the elicitation phase of security requirements engineering.

Step 4 Select an Elicitation Technique

The elicitation phase starts some ground work to be done for selecting the elicitation technique. Requirements elicitation is called as capturing, requirements discovery or requirements acquisition. The process of requirements elicitation can be complex, mainly if the problem domain is unknown for the analysts. Some of the elicitation techniques are, misuse cases, Issue Based Information Systems (IBIS), Joint Application Development (JAD), Interviewing, Brainstorming, Sketching and Storyboarding, Use

Case Modeling and Questionnaire and Checklist A suitable method can be chosen from these elicitation techniques based on the requirements engineering community or expert's choice, level of the security to achieve, cost –effort benefit and organizational policies.

Step 5 High level of Architecture Diagram of Web Applications

With the objective of web application we can identify the number of tiers in the web applications. So draw a rough architecture diagram with high level of abstraction of the web applications. Network or hierarchical style of Architecture can be chosen based on the application domain. This diagram can be extended in detail with low level of abstraction in the next phase of design.

Step 6 Elicit Non-Security goals and Requirements

Once the business goals are identified, and then the non-security goals and requirements of the web applications are to be elicited. The collaborative requirement gathering is adopted to gather non-security goals and requirements. A general classification of requirements for Web applications are Functional requirements and Non Functional requirements. Functional requirements are capabilities that a system must exhibit in order to solve a problem. We consider Security Requirements, as one of the functional requirements for a Web Application because Web Application has become a target of choice for hackers/hacking operations. The Gartner group estimates that 75% of attacks now target Web Applications. [1]

The non-security requirements are categorized as essential and non essential requirements and prioritized according to the Stakeholders preference.

Step 6 Generate Use Cases Diagram for the Web Applications

The non security requirements are gathered; for better understanding and then the use case modeling of the web applications should be developed. Use Case Modeling is a technique which was developed to define requirements [2]. A use case model consists of actors, use cases and relationships between them [3]. It is used to represent the environment by actors and the scope of the system by use cases (functional requirements). An actor is an external element to the system that interacts with the system as a black box. A use case describes the sequence of interactions between the system and its actors when a concrete function is executed. An actor can take part in several use cases and a use case can interact with several actors. The use case is the set of scenarios that encompass the non-security requirements of the system created by the developers and users of the system.

Step 7 Identify the Security Goals / Security Objectives

The security goals / security objectives can be identified with respect to assets, business goals and organizational principles that is the security policies of the organization. The list of security goals can be identified and the security goals can be of main goals and sub goals. The main goals are the top goals, e.g. Confidentiality, Integrity and Availability, that to be identified for the web applications based on the level of security we need.

There are many security sub goals/objectives for web applications and are based on the application domain and security policy of the organization, e.g. Prevent attackers from obtaining sensitive customer data, including passwords and profile information which comes under confidentiality. Prevent tampering, trail and access control which comes under the top security goal Integrity. The techniques like Facilitated Application Specification Technique (FAST), survey and interviews can be used to identify the security goals / security objectives.

Step 8 Identify Threats and Vulnerabilities

By identifying the assets, business goals and security goals the threats to the web applications can be identified. The overall system threats and vulnerabilities can be identified during this step. The list of threats and vulnerabilities can be developed for the web applications. The main threats to a Web application are: Profiling, Denial of service, Unauthorized access, Arbitrary code execution, Elevation of privileges, Information gathering, Sniffing, Spoofing, Session hijacking, SQL injection, Network eavesdrop-

ping, Password cracking, Viruses, Trojan horses, and worms. Some of the vulnerabilities to the web application are unnecessary protocols, Open ports, Web servers providing configuration information in banners, Weak IIS Web access controls including Web permissions, Weak NTFS permissions, Poor input validation in your Web applications, Unsafe, dynamically constructed SQL commands, Weak or blank passwords, and Passwords that contain everyday words.

Step 9 Risk Assessment

The next step is to assess and determine the risk when the threats and vulnerabilities occur. The impact of threats and vulnerabilities are analysed and risk determination process [18] is carried out. To do risk determination process any of risk assessment test models [5] like National Institute of Standards and Technology (NIST) model, NSA's INFOSEC Assessment Methodology, Butler's Security Attribute Evaluation method (SAEM) ,CMU's "V-RATE" method ,Yacov Haimes's RFRM model can be used or Microsoft risk based on DREAD method [6] can be used.

Step 10 Categorize and Prioritize the Threats and Vulnerabilities for mitigation

The threats and vulnerabilities can be Categorized with respect to the security goals and security policies of the organization and prioritized based on the level of security and assets to be secured, e.g. tamper threat Categorized under top security goals Integrity, unauthorized users under Confidentiality, and Integrity. This process can be done with the help of a survey or interview between the stakeholders.

Step 11 Generate Misuse Cases Diagram for the Web Applications

The detailed set of misuse case diagram [7] of the web applications should be developed that encompass the most significant threats to the system e.g. tamper misuse case, unauthorized users misuse case.

Step 12 Identify Security Requirements

The security requirements [19] are the counter measures that the Web Applications should have, as the functional requirements, e.g. Threat – password attack, wire tap, tamper, and Security goals – Availability - password attack, wire tap and Integrity - tamper. The Security requirements to prevent these threats are Prevent password attack, encrypt communication, authenticate, validate data and lock data.

Step 13 Generate Use Cases Diagram for the Web Applications considering Security Requirements

The security requirements are gathered; for better understanding, the use case diagram of the Web Applications should be generated, that encompass the security requirements of the system created by the developers and users of the system.

2.3. Elaboration

In this phase the detailed view of the web applications with security requirements can be understood with models and diagrams, which gives clear idea of the application in design and implementation phase.

Step 14 Generate Structural Analysis models

Next step of security requirements engineering is to develop different analysis models. These models form the solid foundation for the design of security requirements. The data models, flow models and behavioural models are the structural analysis models that can be used to show the functional requirements and data flow.

Step 15 Develop UML diagrams

Develop UML diagrams for detailed view of security requirements and for better understanding of the secure web applications. High level of class diagram and sequence diagrams can be developed. These diagrams can be used to generate code and test cases for testing the security requirements. The navigational model consists of a navigation class diagram and a navigation structure diagram. Security based modelling can be done using SecureUML and UMLsec.

2.4. Negotiation and Validation

In this phase the security requirements are categorized as essential and non essential requirements and prioritized according to the level of security and Stakeholders preference of security requirements. Then rough effort time and cost are estimated to implement security requirements.

The validation is done by the security experts and engineers with the requirements of the stakeholders. Review or Walk-through is a technique which consists in reading and correcting the requirements definition documentation and models. Such a technique only validates the good interpretation of the information. Traceability Matrix consists of a comparison of the application objectives with the requirements of the system [8]. A correspondence is established between objectives and how they are covered by each requirement. This way, inconsistencies and non-covered objectives will be detected.

2.5. Specification

Specification is the last phase in security requirements engineering Process. The security requirements specifications are modeled and they are validated with the stakeholders and this specification forms the source for the design of security requirements. This phase is executed in parallel with each other phases of requirements engineering. Scenario or use case modeling can be used to specify the functional requirements with security requirements and non functional requirements for web applications.

In this MOSRE-WebApp Process, object modeling is used to model the components of the web applications and the concept of encapsulation with the function and data in data modeling, reusability of some of the security requirements against different threats, and the functions can be extended to implement the security requirements, the concept of inheritance is adopted here.

3. Discussion

We have identified the list of security requirements and they are based on the business and system assets by applying MOSRE-WebApp Process for Online Voting system. Based on the identified list of threats, vulnerabilities and security requirements we found that using our MOSRE-WebApp Process for web applications we will be able to get better set of security requirements. There are many methods to elicit security requirements but concentrating less on the phases of requirements engineering [15, 16, 17, 20 and 22]. In this section we compare results obtained from MOSRE-WebApp Process, Haley and colleagues security requirements engineering framework [11]. We consider the percentage of vulnerabilities, threats and security requirements found with each method as the parameters for comparison. Table 1. Shows comparison MOSRE-WebApp Process with Haley and colleagues security requirements engineering framework.

Table 1. MOSRE-WebApp Process with Haley and colleagues SRE Framework

Parameters	**Proposed MOSRE-WebApp Process**	**Haley and His Colleagues SRE Framework**
Completeness of SR	Yes	No
Interaction between other req.	Yes	No
Resolve Conflicts	Yes	No

Stakeholders and Vulnerability Identification	Yes	No
Approach	Model based	Problem based
Multilateral	Yes	No
Risk Assessment	Yes	No
Complexity	Simple	Complex
RE Phases	Includes all	Only Elicitation and Analysis
Traceability to Design	Easier	Hard
Categorize and prioritize	Yes	No
Elicitation techniques	Used	No
Modeling	Part of Process	Not used
Misuse cases and use cases Diagrams	Used	No

From a technical point of view, the most difficult task of the methodology is where security objectives are identified from functional descriptions, such as functional requirements. This has been the observation from several projects using MOSRE-WebApp Process to elicit security requirements. MOSRE-WebApp Process requires expertise on at-least three dimensions: (i) information structuring and analysis, (ii) requirements engineering, and (iii) security. There as on is that it is rarely intuitive what the overall security goals and objectives are, and it is not easy to simply extract these from highly abstract system information, incomplete sets of functional Requirements and early draft system architecture. MOSRE-WebApp Process, provides some support, with use case, misuse case models.

4. Conclusion and Future Work

Security Requirements have to be considered in the early phase of Requirements Engineering [12, 13, and 14], so a Model oriented Security Requirements Engineering Process is developed for Web Application and evaluated for a E-Voting Web Application, The main aim of MOSRE-WebApp is to extend security requirements engineering by seamlessly integrating elicitation, traceability and analysis activities. The motivation for this is that requirements engineering activities are often executed by other people than those writing the code, and often without much contact between the two groups. This applies in particular to security requirements, which is a major quality, attribute of today's system. It is therefore important to develop both the ability of the people involved in the development to identify potential security aspects, and the capabilities of the development team to solve these needs in practice through secure design.

As future work the Security Requirements identified from RE Phase should be carried to Design phase because good design will give Vulnerability free Web Applications and implement them. We also intent to do penetration testing and find the results based how far our application is vulnerable.

Acknowledgements

Our sincere thanks to reviewer and for their valuable comments.

References

1. CLUSIF, Web Application Working Group, "Web application security, managing web application security risks", Technical Studies, http://www.clusif.asso.fr/, March 2010.
2. Jacobson, I. (1995). Modeling with Use Cases: Formalizing Use Case Modelling. Journal of Object-Oriented Programming,
3. UML (2003). Unified Modeling Language. Version 1.5. www.omg.org
4. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan , "Improving Web Application Security :Threats and Countermeasures", Microsoft Corporation, Published: June 2003
5. R. Mead, E.D. Houg, and T.R. Stehney, Security Quality Requirements Engineering (Square) Methodology, tech. report CMU/SEI-2005-TR-009, Software Eng. Inst., Carnegie Mellon Univ., 2005.
6. Swiderski, Frank, Syndex, "Threat Modeling", Microsoft Press, 2004
7. Guttorm Sindre, AndreasL.Opdah," Eliciting security requirements with misuse cases", RequirementsEng(2005)10:34–44, Springer-Verlag London Limited 2004.
8. M. José Escalona, Nora Koch ,"Requirements Engineering for Web Applications – A Comparative Study", Journal of Web Engineering, Vol. 2, No.3 (2004) 193-212 , Rinton Press.
9. Lee, H., Lee, C., Yoo, C. (1998). A Scenario-based Object-oriented Methodology for Developing Hypermedia Information Systems. Proceedings of 31st Annual Conference on Systems Science. Sprague R.
10. Bieber M., Galnares, R., Lu, Q. (1998). Web Engineering and Flexible Hypermedia. The Second Workshop on Adaptive Hypertext and Hypermedia, Hypertext´98, Pittsburg, USA.
11. C.B. Haley, R. Laney, J.D. Moffett, and B. Nuseibeh, "Security Requirements engineering: A Framework for Representation and Analysis," IEEE Transaction on Software Eng. Vol 34, no. 1, pp. 133-152, Jan/Feb 2008.
12. Eric Dubois , Haralambos Mouratidis, "Guest editorial: security requirements engineering: past, present and future", Requirements Eng (2010) 15:1-5, Published online: 1 January 2010, Springer-Verlag London Limited 2009.
13. Benjamin Fabian , SedaGurses , Maritta Heisel,Thomas Santen • Holger Schmidt," A comparison of security requirements engineering methods", Requirements Eng (2010) special issue security requirements engineering ,15:7-40, Published online: 26 Nov 2009, Springer-Verlag London Limited 2009.
14. Siv Hilde Houmb , Shareeful Islam ,Eric Knauss • Jan Jurjens • Kurt Schneider," Eliciting security requirements and tracing them to design: An integration of Common Criteria, heuristics, and UMLsec Requirements Eng (2010) special issue security requirements engineering ,15:63-93, Published online: 28 Nov 2009, Springer-Verlag London Limited 2009.
15. M. A. Hadavi, V. S. Hamishagi, H. M. Sangchi, " Security Requirements Engineering; State of the Art and Research Challenges", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol I,IMECS 2008, 19-21 March, 2008, Hong Kong
16. Hui Wang, Zongpu Jia, Zihao Shen," Research in security requirements engineering process",1285-1288,IEEE ,2009
17. Smriti Jain, Maya Ingle ,"Software Security Requirements Gathering Instrument "(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011 pg:116-129
18. Chandrabose A , Alagarsamy K ,"Security Requirements Engineering – A Strategic Approach". International Journal of Computer Applications (0975 – 8887) Volume 13– No.3, January 2011 pg:25-32.
19. Dhirendra Pandey, Ugrasen Suman ,A. K. Ramani,"Security Requirement Engineering Issues in Risk Management ", International Journal of Computer Applications (0975 – 8887)Volume 17– No.5, March 2011,pg:12-14.
20. Donald Firesmith: "Engineering Security Requirements", in Journal of Object Technology, vol. 2, no. 1, January-February 2003, pages 53-68. http://www.jot.fm/issues/issue_2003_01/column6
21. A. Apvrille and M. Pourzandi, "Secure Software Development by Example," IEEE Security & Privacy, vol. 3, no. 4, 2005, pp. 10–17.
22. Graham, Dan. "Introduction to the CLASP Process." Build Security In, 2006. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/requirements/ 548.html.