Designing Secure Web Application using J2EE Security Patterns

Chavada Sandip¹ Prof. Kalpesh Patel²

¹,²Department of Computer Engineering
¹,²L.D. College of Engineering, Ahmedabad, India

Abstract—Today your website is your brand, your business backbone and often your first contact with your customers. If it’s not safe & secure, those critical business relationships can be compromised. A single security breach could be a finished a small business. Security Pattern described a recurring problem that arises in specific context, and it presents a well proven generic solution. During past few years developing secure application using security design pattern is popular area in the field of security. The role of security pattern is fulfilling security requirement and provide well-structured solution for security vulnerabilities. Providing end to end security using J2ee security pattern is differ from traditional infrastructure security design pattern in term of addressing security requirement, mitigating security risks, securing business object and data across logical tires, securing communication and protection the application from unauthorized threats and vulnerabilities. Our approach is to find a J2ee security pattern as a countermeasure to vulnerability. This is the way of providing link between security expertise and software developers to apply security knowledge in software development practice. Security should be considered throughout each stage of software development process to develop secure application [2]. This security engineering approach restricted due to complexity and diffusion of today security knowledge so it is still difficult to integrate security into software development process [9]. In this paper approach for ‘designing secure web application using J2ee security pattern’ is presented which Aim find threat and security requirements of web application and use J2ee security pattern to mitigate vulnerability. So that developer can be specify the threats and vulnerabilities in web application during early stage of development, and then it can be solve using the J2ee security pattern.

Key words: Security pattern, secure software, software vulnerability

I. INTRODUCTION

Due to increase number of vulnerability in web application security has become a critical issue in terms of to develop robust and secure web application. Developer must support software with security measures. However, security concerns must be inform every phase of software development from requirements engineering to design, implementation, testing, and deployment. Due to the vast number of security concern and the fact that not all software engineers are security specialists, creating software with adequate security measures is extremely difficult. Designing secure web application is about designing software to be secure, making sure that software is secure, and educating software developer, architects, and users about how to build secure things [3].

Security pattern is Reusable solution to overcome vulnerability and flaws in software. It provides experts knowledge and mechanism to solve security threats [4]. This is fact that All software developer are not security experts and software developer concern with developing software not with security so they have seldom knowledge about security so it is really hard to integrate security with each phase of software development process. Security pattern can provide brief knowledge about how to use security mechanism where to use, when to use and it also give information of vulnerability and its context to software developer so that they can concern security at early stage. But now again question arise that how developer integrate security pattern in secure software development process. And how apply security pattern so it give guarantee that threats and vulnerabilities are mitigate. Thus issue may cause security damage. Thus, our research aim to answer the two research questions (RQ).

- RQ1: how developer integrate security pattern in secure software development process.
- RQ2: how apply security patterns so it gives guarantee that threats and vulnerabilities are mitigate.

Herein we answer these two questions. Because the security pattern alone does not provide systematic guidelines with respect to application. We propose design methodology which based on Pattern Driven Security Design [5]. Part of that methodology is we adopting for addressing security throughout in our approach of designing secure web application using J2ee security pattern [11]. Our approach provides three major contributions.

- Design secure web application using J2ee security pattern
- Bridging the gap between developers and security experts
- Adapt security pattern to early phase of software development

A. Security Pattern:

The definition of security pattern has the very same key characteristics as general software patterns [6]:

“A security pattern describes a particular recurring security problem that arises in specific contexts and presents a well-proven generic scheme for its solution.”

Now there are many type of patterns set available why we select J2ee security pattern? java is number one programming language in the world and there are seven million developer of java language. And also there is no universal classification of security pattern is available. STRIDE model, ZACHMAN frame work, CIA model and many other are try to represent classification model for security pattern [7]. But they could not enough success to provide well described and well-structured classification model or set of well describe security pattern. While J2ee security pattern are well describe and provide well proven solution for security vulnerabilities.
B. Pattern Driven Security Design:

Pattern-driven security design is secure design methodology which is guide us to addressing what are the security function should be include at requirement, architecture and design level [8]. By applying this design process within structured methodology architects should be able to complete a secure architecture design using security pattern and derive a secure application architecture addressing the known risk and vulnerabilities. Security Pattern Design Methodology addressing security concern in four phases. In security requirement phase it identifies potential security threat, assets and security goal. In architecture phase architect identify potential security pattern that can satisfy the application specific security requirement and mitigate risk. Trade off analysis also include in this phase to find best suitable security solution. Based on these input, design process carried out. Security designer perform factor analysis, tier analysis and design policy. In building portion of lifecycle architecture and designer apply security pattern to the application that satisfy security requirement then they choose their preferred tools and technology to implement application using security pattern.

C. J2ee Security Pattern:

The j2ee security pattern provides security solution for multi-tier application infrastructure. It is complete set of security mechanism to overcome today’s security threats. It is describe by Security Pattern Template[12] for well structure representation. Using Core Security Patterns Catalogue [13] it illustrates how Core Security Patterns are represented in delivering end-to-end security of a J2EE based application architecture and how it is related in aspects of role and responsibilities in logical tiers. Each j2ee security pattern performs security measure individually for ex.

- Authorization Enforcer pattern can be used to manage and delegate authorization processes
- Authentication Enforcer pattern can be used to manage and delegate authentication processes
- Intercepting validator pattern helps performing security validation for input data from clients. Etc

As well as each security measure available as part of API package such as JCA provide basic cryptographic service, algorithms and digital signature, JCE include encryption and description operation, JSSE facilitate secure communication [14].

II. OUR APPROACH

Here we present our approach in which it describe how integrate j2ee security pattern in designing secure web application. Our approach defines and concern security before developing software. It is about secure software not about software security (afterthought paradigm). Here we describe our approach step by step.

1) Step 0: first start with create conceptual model of application. It is very simple architecture which gives us brief idea about

2) Step1: design use case diagram and chose any method to identify the type of assets, threats and countermeasures present in developing application. There are many methods like misuse case, threat profiling, MASG model etc. then based on countermeasure define security requirement of application.

3) Step2: now based on security requirement chose set of security pattern which can fulfill security requirement and mitigate threats.

4) Step3: design class diagram with considering security means class diagram with applying j2ee security pattern.

5) Step4: using definition of applied security pattern create test case in OCL [17]

6) Step5: now give input to USE tools [18] as class diagram (step3) and test case (step4). Execute tests to validate an input model satisfies security requirements and set of security pattern which we applied is create secure and robust design of given application.
III. CASE STUDY

Using our approach we try to design secure shopping cart. In which based on countermeasure we define security requirement and based on that we select set of j2ee security pattern to make secure shopping cart. Using definition of security pattern we try to create test case and using it we make sure that our method can contribute to design secure software using j2ee security pattern. Here we describe authorization enforcer j2ee security pattern. For example our security requirement is that unauthorized actor cannot execute subject controller’s method. To fulfill our requirement we use authorization enforcer security pattern which check if actor role is authorized person then based on its right it can access method.

![Fig. 2: Structure and behaviour of Authorization enforcer](image)

IV. CONCLUSION AND FUTURE PLAN

Proposed work provides the method through which we can build secure web application without revealing large study of security engineering. Using our approach we can integrate security pattern in early phase of software development process. This approach is provide efficient method to provide directory for designing secure web application. For the future work we focus on create more robust and stable application for the distributed environment.

REFERENCES


