International Journal of Mathematics and
Computer Science, **16**(2021), no. 4, 1077–1086

Elicitation of Resilient Requirements through Countermeasure Decomposition Technique

Thejasvi Nagaraju, Shubamangala B.R.

Department of Computer Science & Engineering
Faculty of Computer Science
Jain University
Bangalore, India

email: thejasviphd@gmail.com, brm1shubha@gmail.com

(Received December 17, 2020, Accepted March 2, 2021)

Abstract

Application security attack deterrence inherently depends on two factors: higher grade Quality of Application Security (QAS) and optimized risk. In turn, these two aspects are dependent on good quality security requirements (SR). Currently, there exists no methodology to either delineate the limitations of SR or to address them effectively. Hence, our study first discovers the reasons of SR limitations and challenges and secondly architects a two module solution to meet SR challenges effectively. The first module of the solution, introduces classification, prioritization and refinement of SR based on examining the risk. The second module provides a framework to elicit resilient SR. Resilient SR enable the application to deter attacks by identifying the attackers objective. SR resultant from these two modules addresses the challenges of SR, enhances QAS and optimizes the risk.

1 Introduction

Quality of Application is defined as its conformance to requirements. Poor requirements lead to poor quality of application (QAS). Security requirements

Key words and phrases: Data Breach, Vulnerability, Resilient Security Requirements, Resilience, Countermeasure.
AMS (MOS) Subject Classifications: 68M25, 62C10.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

(SR) represent the security goals, security objectives and security functionalities of an application [2]. The ideal condition of 100 percent risk mitigation is practically not possible [1]. Determining the risk mitigation level depends on the domain and role of application.

2 Problem Statement

Which Security Requirement deserve most attention?
Introduce attack resistance into an application?

3 Research Methodology

Below Techniques have been utilized in this research:
Application classification and Vulnerability Evaluation
Countermeasure Evaluation, Selection and Decomposition.

4 Survey Findings

Park et al [5] state the need for application security to begin from the security requirements phase. Pinna et al. [6] states the concept of Security Requirements prioritization and its associated risk. Merkow and Lakshmikanth [4] provide contextual understanding of secure and resilient applications but lacks focus on resiliency. Kuusijarvi et al [3] describes key operational resilience only.

5 Experiment & Results - Part 1

Classification and Prioritizing is the action of grading the classified SR. Refinement is the act of decomposing a SR from a high-level into executable atomic statements.

The major contributions of this research are:

Refinement of SR using affinity and tree diagrams. Concept of generation of resilient use cases

Figure 1: Security Requirements to Enhance QAS

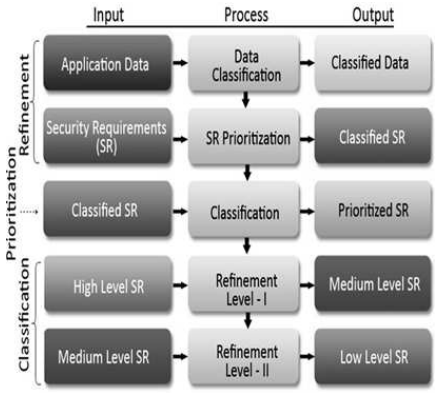

Figure 2: Approach to Classify, Prioritize and Refine Security Requirements

Data	Category	Risk Level	Compliance	Impact Example
Critical	Acute	Very high	Devastating	Financial data

Table 1: Data Division Schema

Rule	Criteria
R1	If Sr does not access data, THEN Sr Category = Strategic Sr

Table 2: Security Requirement Calcification Rule set (R1:R4)

5.1 Module 1 Classification, Prioritization and Refinement of SR

The approach to classify, prioritize and refine security requirements consists of five stages,

5.1.1 Stage 1: Data Classification

The value of business information associated with data, embeds risk into data that is denoted by the term data risk.

(i) Application Data Collection Based on the applications subject, scope and functionalities, the data required for the operation of the application is collected.

(ii) Data division

For each data cluster, risk and the data sensitivity associated with it are assessed and classified which forms a basis for security requirement classification.

5.1.2 Stage 2: Security Requirement Classification

(i) SR is assessed to see if it access critical, important or moderate data. (ii) The data access is associated to risk using IF-THEN rule.

5.1.3 Stage 3: SR Prioritization

Classification of SR plays an instrumental role in discovering, computing, and cataloging the varied risk level present in security requirements.

Implementation of security requirements is executed through deployment of security controls. Considering the risk, a compliance level associated with each SR class is awarded.

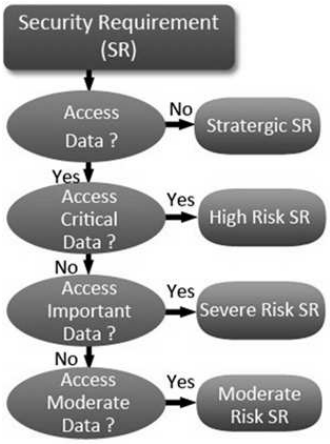

Figure 3: Decision Based Tree Diagram for SR Classification

SR Id	Data Access	SR Classification	Security Requirement
R1	Critical	Critical risk	Access only to business functionality as entitled
R2	Critical	Critical risk	Stronger authentication than passwords
R3	Important	Important risk	Prohibit leakage of PII to unauthorized persons

Table 3: Classification - Online Banking SR

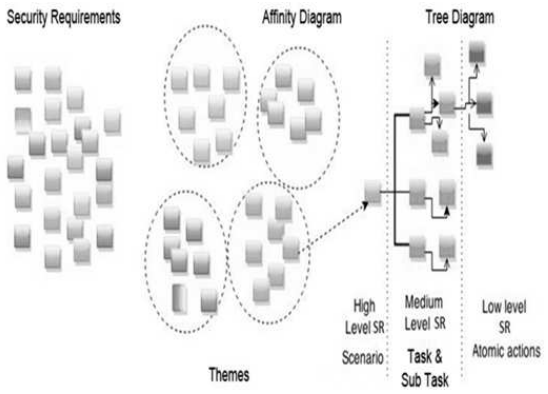

Figure 4: ETree Diagram

SR Id	Security Themes	Critical risk requirements
R1	Authentication	Access only to business functionality to which they are entitled
R4	Authentication	Establishing strong authentication mechanism for consumer facing online transactions

Table 4: Clustering of Critical Risk SR using Anity Diagram

5.1.4 Stage 4: Refinement Level-I

Scenarios are the high-level descriptions of the activities required to achieve a group goal. Scenarios cannot be implemented as such and must be broken into granular level detailed requirements. This is achieved by introducing a decomposition principle.

Affinity diagrams- Security functionalities are denoted by the term theme. This process of discovering the themes and mapping SR to respective themes is carried out by applying the concept of affinity diagrams.

High-level SR are decomposed into tasks and sub tasks. Tasks may be further divided into sub tasks. The number of sub task layers depends upon the complexity of the task, organization policy to accomplish the task and risk involved in the security requirements.

5.1.5 Stage 5: Refinement Level-II

In this level, sub tasks obtained for each SR are converted into a set of atomic actions which provides the finer details for implementation of SR.

Sr Level	Description test	Case
High	Scenario level	Test scenarios, high level test cases
Medium	Taks and sub-task level	task level test case
Low	Action level	Isolated, atomic test case

Table 5: Refinement of Security Requirements

From action-level SR, security use cases can be generated to test the efficiency of the SR.

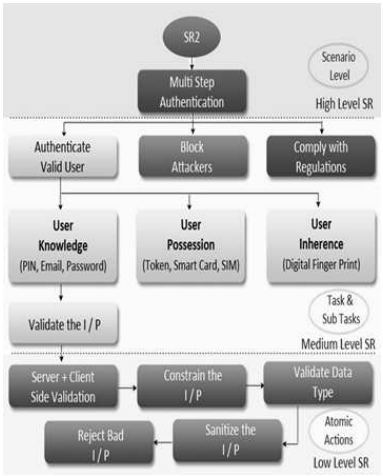

Figure 5: Security Requirement SR2 Refinement Process Illustration

6 Experiment & Results - Part 2

6.1 Elicitation of Resilient Security Requirements

Application resilience objective is entire organizations integrated security solution towards security attacks. Taking this as the goal, a framework to generate resilient security requirements (RSR) is designed in our Experiment.

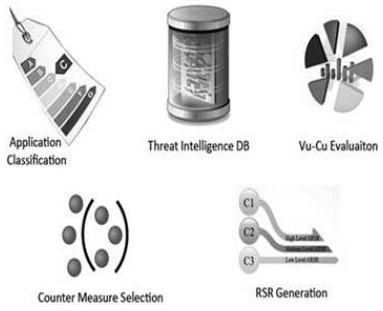

Figure 6: RSR Generation Phases

Vulnerability risk category	Criteria
Critical risk	Allows the compromise of entire organization security, affect the system as a whole
Medium risk	Alters functionalist of normal system behavior, but not a violation of security objectives

Table 6: Data Division Schema

6.1.1 Phase 1: Applications Classification

An organization application has a distinct role and relevance. Applications are classified into five groups

Critical(A1); Important(A2); Strategic(A3); Internal Support(A4); General Support (A5)

This classification aids in finding the solutions for the adequate mitigation which in turn drives the generation of RSR.

6.1.2 Phase 2: Vulnerability Evaluation

Vulnerability evaluation is a key step in generation of RSR. This step appraises the strength of the organizations defenses against the real time attacks.

Vulnerability Risk Classification

.

Vulnerability Identification

The knowledge of application vulnerabilities enhances the potential of organizations to fight against security threats and attacks. From "Threat Intelligent Database" extract different kinds of threats, their targets, their

Vulnerability risk category	Criteria
Critical risk vulnerability	Allows the adversaries for easy compromise of entire organization security.

Table 7: Priority Ranking

App category	App	Risk associated with Vu	Difficult to exploit	counter measures	Priority	ID
Critical (A1)	Logistics	Severe	No	Yes	High	V1
Important (A3)	Telecom	High	No	Yes	Medium	V2

Table 8: Illustration of Vulnerability Evaluation

region, industry sector, past occurrence of breaches.

Vulnerability Prioritization

Vulnerability remediation process involves effort, cost and resource. Hence, designing a hierarchical ranking of vulnerabilities is very essential.

Vulnerability Evaluation

Vulnerability evaluation process is illustrated in Table 8.

This categorization of vulnerabilities aids in identifying the vulnerabilities in the existing applications and plays a key role in selection of countermeasures.

6.1.3 Phase 3: Vulnerability-Countermeasure Evaluation

A countermeasure is a security feature or a security control that mitigates one or more security vulnerabilities.

Finally determine whether the countermeasure provides an adequate level of protection to address the vulnerabilities.

Vulnerability Id	Priority	Existing CM	Replacement
V1	High	2	Yes
V3	Low	3	No

Table 9: Countermeasure Evaluation Matrix

6.1.4 Phase 4: Appropriate Countermeasure Selection

The selection process of a new appropriate countermeasure in place of an existing countermeasure.

7 Conclusion and future work

Innovation of Resilient Use Cases gives a concrete base for application resilience. These resilient requirements are converted into corresponding design, implementation and testing, so the resilience gets blended with the existing application.

References

[1] Ashish Arora, Anand Nandkumar, Rahul Telang, Does information security attack frequency increase with vulnerability disclosure? An empirical analysis, Information Systems Frontiers, **8**, no. 5, (2006), 350–362.

[2] Charles Haley, Robin Laney, Jonathan Moffett, Bashar Nuseibeh, Security requirements engineering: A framework for representation and analysis, IEEE Transactions on Software Engineering, **34**, no. 1, (2008), 133–153.

[3] Jarkko Kuusijärvi, Reijo Savola, Pekka Savolainen, Antti Evesti, Mitigating IoT security threats with a trusted Network element, 11th International Conference for Internet Technology and Secured Transactions, (2016), 260–265.

[4] Mark S. Merlot, Lakshmikanth Raghavan, Secure and resilient software: Requirements, test cases, and testing methods, CRC Press 2011.

[5] Sooyong Park, Harksoo Kim, Youngjoong Ko, Jungyun Seo, Implementation of an efficient requirements-analysis supporting system using similarity measure techniques, Information and Software Technology, **42**, no. 6, (2000), 429–438.

[6] Claudia Pinna, Francesco Galati, Monica Rossi, Clint Saidy, Ramy Harik, Sergio Terzi, Effect of product lifecycle management on new product development performances: Evidence from the food industry, Computers in Industry, **100**, (2018), 184–195.