DESIGN AND DEVELOPMENT OF SECURITY TEST CASE OPTIMIZATION FRAMEWORK

Thesis submitted in fulfillment of the requirements for
the Degree of

DOCTOR OF PHILOSOPHY

in

INFORMATION TECHNOLOGY

Submitted by
MOHD. WARIS KHAN

Supervised by
Dr. DHIRENDRA PANDEY
Department of Information Technology
Babasaheb Bhimrao Ambedkar University, Lucknow

Co-Supervised by
Dr. SUHEL AHMAD KHAN
Department of Computer Science
Indira Gandhi National Tribal University, Amarkantak

Submitted to

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY LUCKNOW

DECEMBER-2018

ABSTRACT

Software security testing is a multifaceted process intended to reveal the flaws in the security structure of the software system. A perfect security mechanism of an information system has to protect data and maintain the functionality of the software application even in situations of malicious attacks. The primary objective of applying security testing is to ensure the operational ability of the software system to prevent it from failing at times of breaches and attacks. Unfortunately, security testing has its logical limitations that have to be overcome and researchers and software developers are therefore engaged in finding out new techniques to enhance the security of an application before it is delivered to the end user or organization. The logical barriers and exhaustive testing process is no guarantee that the software delivered is completely flawless or could withstand any attack, and to tackle this problem it is imperative to include the security testing process as a regular exercise from the first to the last stage of the software development life cycle.

Software security testing uncovers the vulnerabilities and flaws in the software system and ensures the protection of data and other resources from potential and possible intruders. We live in a world where information is of highest importance and hence the protection of crucial information is paramount in this information era. Software applications are an indispensable and inseparable part of our lifestyle, from mobile applications to highly advanced and complex software systems used in industries, banking and power plants, everything runs on software systems and thus it makes this the responsibility of developers to create robust software systems for the end users.

Since, a majority of software applications are written with the help of web based technologies, which can be accessed from anywhere at anytime,

making them exposed and vulnerable to any kind of malicious attacks. Therefore, developers and researchers need to critically analyze the problems related to security and potential threats to software. Since, software security is a highly complex mechanism; developers need to carefully take each step towards designing a secure application keeping in mind the requirements. In the absence of predefined practice of using optimization with respect to the security attributes when designing a software application, a thorough review of the related literature was undertaken to study the current practices in the field of software security. Experts and researchers in the field of software security have used various methodologies but none have quantified the security attributes with respect to its weightage and ranked them respectively. In this thesis, we have devised a framework that takes under consideration the importance of security attributes by ranking them according to their weights and optimizing the faults in the later phase. It is evident that there is a strong need of optimization of security test cases to architect a secure design for a software application, so as to diminish the time and cost incurred to develop an application and also to avert the exhaustive process of rework. Optimization of security test cases, can trim the exorbitant time consumed in the development process since it focus on the exact security attributes required in a specific task of fault detection and subsequently its mitigation. It also dwindle the unreasonable cost of development of the software.

A viable framework is being presented after a thorough assessment of software security attributes and its usability in various testing scenarios. This framework incorporates seven phases, including Security Test Plan Specifications, Identification of Security Attributes, Evaluation of Security Attributes, Test Case Execution & Capturing the Results, Optimization and finally Validation. The Security Test Plan Specifications is a brainstorming activity and for best efficacy it must be

the first step in the architecture of secure software system that must be coextending to software development. For generating a master test plan and assessing the testability of the entire designed software general project information and user requirements are used, whereas development of a detailed phase-wise test plan more specific software information is taken under consideration. Although there are many factors affecting security testing of software system, but researcher identify a set of elements that have a significant contribution in influencing the design of security testing.

The next step in the development process is Identification of Security Attributes, where all seven security attributes namely authentication, authorization, confidentiality, availability, integrity, non-repudiation and resilience are mapped according to the security requirements to provide a strong foundation for the security test plan specification. Quantitative estimation of these attributes helps in achieving the ultimate objective of ensuring a superior and satisfactory level of design hierarchy.

Further, these attributes will be evaluated through fuzzy ANP method and ranked in accordance to their respective weightage. Evaluation of security attributes will decide the accentuation on particular attributes on priority basis in respect to the type of vulnerability that is encountered during test case execution. Due to high correlation among the factors of security testing, complex measures are undertaken to optimize security test cases.

Test case execution is carried out according to the respective security attributes to find faults that occur during testing; and the results are captured. In the next step, the captured faults are optimized using Ant Colony Optimization (ACO) technique, where all the paths in each iteration are explored and the best path is selected. The path which covers

all the faults in minimum execution time is the considered the best path. The next step is Validation that provides evidential support which corroborates that the measures undertaken has fulfilled the intended purpose. In order to strengthen the process of optimization of a security test suite, statistical analysis has been rendered. Finally, the process of Review and revision is carried out as and when required, which facilitates a retrospect of the entire development activity and aid in making changes wherever necessary. An empirical validation of the model is also carried out using tryout data.

For the assessment of superior level secure design in the proposed framework, Average Percentage Fault Detection (APFD) is used for optimizing the security test cases. APFD is used to analyze results obtained from various tests based on traditional techniques as well as tests based on ACO technique, and has been experimentally validated using the tryout data. The proposed model has shown satisfactory results with respect to Mobile Payment Wallet project. It is apparent from the validation of the proposed framework that it may be significantly helpful to keep in check the potential faults and vulnerabilities from the early design phase till the end. Like any other research, the current work may also suffer from certain limitations, therefore to achieve a generalized result and implementation of the proposed model, further study may be conducted on a large sample of data.