SECURITY REQUIREMENT ELICITATION FRAMEWORK FOR SECURE SOFTWARE DEVELOPMENT

Thesis submitted in fulfillment of the requirement for the degree of

Doctor of Philosophy

In

INFORMATION TECHNOLOGY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

Submitted by

VIRENDRA SINGH

Supervised by

Dr. DHIRENDRA PANDEY

Submitted to

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
VIDYA VIHAR, RAEBARELI ROAD,
LUCKNOW – 226025, UTTAR PRADESH, INDIA

JANUARY-2020

ABSTRACT

Security Requirement Elicitation is a significant step during software development process. The main purpose of security requirement elicitation is to collect suitable security needs as well policies form stakeholders or organizations in the right way, security requirement elicitation is important for every organization to develop quality software that can fulfill user's requirement. The majority of the system fails, just because of wrong elicitation practices, which may affect time delay and cost of the software. Without the elicitation it is impossible to find our accurate requirements, security requirement elicitation is the major activity of requirement engineering, which need proper attention by developers and related stakeholders. In this research, authors have proposed an effective requirement elicitation process model and its various approaches to producing a quality requirement during software development.

There are many issues in contexts to requirement engineering. These issues can be anything like issues related to scope, prejudices in issues related to requirements etc. Other issues include confusion of users in understanding the technical details, which often leads to system objectives that are ambiguous. Moreover, sometimes the clients/customers are not completely aware of the abilities and limitations of the domain environment and they also do not understand that the requirements are dynamic in nature and subjected to change.

At the time of design in SDLC, the production and development of a security device for testing software systems is a very comprehensive and expensive activity for any organization. A secure software development process is a tenacious activity that requires evaluating all the security properties as security requirement elicitation is an inseparable part of this

process. Security check profile modus operandi involves eight techniques including questionnaire, brainstorming, data analysis, group discussion, interview, observation, prototyping, requirement workshops. Such characteristics are a keystone in determining and collecting accurate and secure information. In all respects, secure elicitation has become an important need for any organization. Hence, its protection demonstrates its significance and weighting correspondingly, covering all the issues that may increase or decrease the computer organization's quality. Therefore, finding new strategies and taking necessary action at the time of security requirement elicitation becomes the necessities of developers.

In this work, we have considered seven security attributes that are integrity, confidentiality, authentication, effectiveness, availability, access control and authorization. This situation will create multiple choices and choosing the best decision according to the situation is a very tedious exercise, as a solution, we will work on few multiple decision-making methodologies (like AHP, Fuzzy AHP, ANP, and Fuzzy ANP). The Analytical analytic hierarchy process (AHP) is one of the methods for this; it is a structured technique for organizing and analyzing complex decisions. It is a type of application that helps in group decision making. The AHP first decompose the decision problem into a hierarchy of more easily comprehendible sub-problems, each of which can be analyzed independently. Fuzzy logic itself based on uncertainty principle and derived imperious knowledge. When a user has to decide in a situation of uncertainty, the user can use Fuzzy AHP. One more process is there for multiple decision making i.e. analytic network process (ANP), this is a generalized form of the analytic hierarchy process (AHP), and again fuzziness can be applied to this process to decide uncertainty.

AHP and ANP both structures a decision problem into a hierarchy but AHP do it with a goal based on decision criteria and alternatives, while

the ANP solves it as a network. Pair wise comparisons are done in both the systems to weights measure of structure, and rank them accordingly.

Security requirement elicitation is an ever-growing area that involves the development of new technologies and techniques that can be used to build secure software. The intruders are always ready to attack both device and user applications, which may or may not easily lacerate computer security. Such intruders ' main goal is to manipulate the vulnerabilities and gain all the sensitive information or data they can monitor from the running system. Therefore, the secure requirement elicitation provides a platform through which its actions can be managed smoothly to avoid any possible disturbance. The enactment of security requirement elicitation plays an important role in enhancing the protection of any technology. Structured security check profile during the entire SDLC cycle, especially during the design phase, leads to better knowledge of the quality of software and shields against known issues that affect the security of the product. Increasing numbers of security issues or accidents are also a growing concern for business owners and IT industries. Many companies that do not concentrate on security requirement elicitation during the software development process can contain dangerous bugs that can present huge risks to the company.

The last few decades have shown an incredible rise in the production of different types of software according to the user's needs. Requirement Elicitation techniques for security requirements is the crux of the process of development of a software product. Based on the Analytical Network Process (ANP) process, this paper analyzes the weighting of elicitation techniques for security requirements in the production of software applications. In other words, the elicitation strategies of security requirements play an important role in the development of secure software. It also analyzes the relationship between security requirement

elicitation techniques and their objectives through the use of ANP method and also demonstrates the application of fuzzy ANP method to achieve higher accuracy. When developing a secure software framework, the results provide a better platform. With these facts in mind, the proposed study will also clarify the priority weights of security requirement elicitation techniques that can be used to analyze trade-offs between competing software security requirement elicitation techniques and provide a new way for developers when constructing the secure software.

This work has developed a framework and an approach that prioritizes the attributes with the help of FAHP i.e. Fuzzy based analytic hierarchy process. A literature survey reveals that attention towards critical security attributes such as Integrity, confidentiality, Authentication, Effectiveness, Availability, Access Control and Authorization enables developers to enhance security of the software for an extended period of time.