DESIGN AND DEVELOPMENT OF A NOVEL METHODOLOGY FOR SECURITY THREAT ORIENTED REQUIREMENTS ENGINEERING

Abstract of the
Thesis submitted in fulfillment of the requirements for
the Degree of

DOCTOR OF PHILOSOPHY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करुणा
ESTABLISHED 1996

in

INFORMATION TECHNOLOGY

by

MD TARIQUE JAMAL ANSARI

Supervised by

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

Submitted to

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY LUCKNOW

JANUARY-2020

ABSTRACT

Nowadays, in the age of information technology, a number of organizations frequently process, manage and exchange their most crucial information using technology-intensive systems which are directly connected to the internet. Such systems are being progressively exposed through the use of information technology and its tools, such as web services that allow other web services, which are itself software systems. This process may be with or without human involvement, to access, manipulate and exploit this sensitive and confidential information. This enhanced transparency has made more accessible sensible business knowledge and the software systems that manage it.

With growing dependency on information technology, it is important to be aware of new and emerging security threats that deliberately target software systems. Such software projects fail at the cost of millions of dollars, with several jobs lost and, unfortunately, with the loss of life. One of the most frequent and severe cyber security attacks ever reported against enterprises in a wide range of industries have been seen in the last few years. While security experts anticipate for another record-breaking year of network infringements and information security risks, it is essential that organizations become knowledgeable of the new cyber threats in development and guarantee that their security measures are strong enough to compete.

Software security is daunting and vital, because so many essential activities are entirely software-dependent. This makes software a very valuable target for attackers whose intentions can be malicious, illegal, adversarial, and profitable. The practically guaranteed presence of vulnerabilities makes it so easy for adversaries to target software which can be manipulated to infringe one or more of the software's security measures or to force the system into extremely dangerous situation. Secure software can't be compelled to malfunction deliberately. When security requirements are not clearly specified, the resulting program may not be tested until implementation for success or failure. In software development process most of the time security requirements consideration often developed independently of other requirements engineering activities. As a result, specific security requirements are often ignored and functional requirements are specified

in blissful ignorance of safety aspects. Requirements engineers are generally well qualified in functional requirements but not in software security. Very few qualified engineers have learned only basic security architectural skills, such as password security, encryption, and decryption. They don't have thorough understanding of accurate security requirements engineering. It comes as no surprise that security requirements engineering is critical to the success of any major software development project.

Several researchers have proposed security requirements engineering techniques, tools, framework, methodology, and norms for eliciting security requirements during the early stages of the software development cycle. Engineering security requirement into the early stages of the development process is profitable, secure and also provides quality software product. Security requirement engineering should be systematic, repeatable and capable of eliciting complete, reliable, clear, simple and easy to analyzable by the other members of the software development process. Typically, security requirements engineering performs different engineering tasks independently from other functional requirements. Some critical security requirements are therefore consistently ignored, and the requirements engineer concentrated only on functional requirements while ignoring important software safety aspects. Numerous security requirement engineering frameworks, techniques, processes and methodologies have been proposed by different authors, but there is still a need to improve them.

The absence of effective and efficient security requirements engineering approach in today's software development process often produces software with exploitable weaknesses. These software weaknesses are known as vulnerability that makes a threat to enter into the software system to perform unauthorized actions within a software system. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. It may be due to inadequate design, config errors or improper and insecure coding strategies.

The elicitation of effective and efficient security requirements is an important and challenging task. It is an important task because there are many problems associated with the consideration of security issues during the software development phases that must be overcome. Generally, software security is not considered by the developers during the early phases of the software development

life cycle. Many security Requirements engineering approach normally does not comprise all significant stakeholders and does not use the well-organized techniques for stakeholder identification and prioritization. Most of the time the security requirements specification is incomplete, unclear, contradictory, not cohesive, disorganized, infeasible, outdated, unable to be validated, and not usable by their expected persons. All elicited security requirements should be well organized in a systematic manner otherwise the software system cannot be evaluated for accomplishment. Therefore, there is a need to develop an approach which is capable of eliciting more effective and efficient security requirements by considering all the issues which are neglected by the previous approaches.

The software system which is to be developed may have several stakeholders. Only some stakeholders have engaged in the production of software applications, but all stakeholders are aligned with the software system. Some stakeholders can assist in the asset identification process. They suggest assets of the system from their point of view. These assets may have vulnerabilities. The threat exploits these vulnerabilities to get access to the system. The risk associated with each identified threat is not the same. The attacker has always targeted the vulnerability with high risk. The requirement engineer categorizes and prioritizes the identified threats.

In order to design and develop an efficient security requirements engineering approach the researcher first determines the selection criteria which influence the software developers in selecting the effective security requirements engineering and priority ranking of these criteria by using the Analytic Hierarchy Process (AHP) model. The study was planned and conducted to identify the different criteria which are considered by the software developer during the selection of effective security requirements engineering approach. Further the priorities of selection criteria were determined by using AHP model. Effective security requirements engineering selection criteria were compared in pairs by the security experts.

Further based on the ranking given by different security experts, we design and develop a novel security requirements engineering approach. The main objective of this research is to design and develop a security requirements engineering methodology by considering available literature analysis and security expert's necessities and that should also be powerful in eliciting security requirements. The proposed methodology is capable of eliciting security requirement which is

effective, efficient, complete, clear, consistent, organized, feasible, up to date and easy to be validated. This methodology is especially suitable for any type of software project, web based applications that requires security from the beginning of the development process.

This research presents a novel Security Threat Oriented Requirement Engineering (STORE) methodology which is a ten step systematic process, which provides an effective, efficient and systematic way of eliciting and documenting security requirements for the software as well as web-based applications from the early phases of software development. In this methodology, security requirements are often discussed in the context of threats. Threat helps the security requirements engineer to calculate the risk associated with it and also represents the adversary's abilities. Stakeholder plays an important role in the STORE methodology. A software system which is to be developed can have several stakeholders, only a few stakeholders are associated with the security of software products. Those stakeholders, who have security concern of the software system, have knowledge about the related assets of the systems which are to be protected from the threats. In STORE methodology we identify and prioritize all such stakeholders based on their importance. It is important to consider every significant stakeholder from the beginning of software development. This proposed methodology considers security threats for identifying security requirements with the help of potential stakeholders. These stakeholders help the requirement engineer in asset identification of the software product.

We have also applied the proposed STORE methodology to the Enterprise Resource Planning (ERP) web-based application software. A college ERP system is capable of managing student records, department, faculties, library, and other information. It has all the information about the students, faculties, staff, library, departments and other confidential information which requires security. The proposed STORE methodology is also compared with the two existing security requirements engineering approaches i.e. MOSRE framework and SQUARE methodology and found that the proposed STORE methodology is better in terms of eliciting complete and well-organized security requirements.

Furthermore the researcher has also validated the proposed STORE methodology. The validation of STORE methodology was done by the security expert evaluation.

This form of validation requires one to construct a systematic evaluation process where security expert's plays a role of assessing the methodology based on some pre-defined criteria. It is necessary for each security expert to understand and experience the operational mechanism of the proposed methodology before participating in the systematic evaluation process. They have to experience the functionality of proposed methodology through the different example problem to show how the STORE methodology presented in this thesis help elicits effective and efficient security requirements.