Chapter 10
Dimensions of Robust Security Testing in Global Software Engineering: A Systematic Review

Ali Akber
Institute of Business Management, Pakistan

Syed Sajjad Hussain Rizvi
Hamdard University, Pakistan

Muhammad Waqar Khan
Institute of Business Management, Pakistan

Vali Uddin
Hamdard University, Pakistan

Manzoor Ahmed Hashmani
University Technology PETRONAS, Malaysia

Jawwad Ahmad
Usman Institute of Technology, Pakistan

ABSTRACT

Over the last few decades, software security has become significant in parallel to general software testing. Previously, the scope of software security was relatively limited as compared to the software functionality. But now, in global software engineering, the scope and budget of software security are far more than its basic functionality. This has created a pressing need to devise the separate set of working boundaries between software quality testing, and software security testing in global software engineering. In the past literature, a massive number of software security testing methods has been devised. In this paper, a comprehensive literature review is presented on the recent global software security testing methods. In addition, the strength and limitation of each framework are discussed and analyzed. Finally, this work submits the open areas in the domain of global software security testing methods as one of the deliverables of this research work.

DOI: 10.4018/978-1-5225-9448-2.ch010
INTRODUCTION

It is an open evident that the world of Information and Communication Technology (ICT) is improving more broadly, deeply and rapidly than ever before. Specifically, in global software engineering industry is becoming agiler and market dynamics are getting changed. Systems on modern concepts like networking, IoT, cloud computing, e-commerce etc. are integrating to compete in industry & achieve innovation (Vu et. al. 2011). Apparently, the scenario looks benefiting; however, due to the massive usage in all financial and economic sectors, it is now more prone to the security attacks. In addition, the massive number of data and system security incidents have been reported in the archives. These attacks not only results in the financial loss of an organization but also damages the credibility of their system. Moreover, these security attacks can lead to severe damage to systems, information or its environment (Petrenko et. al. 2012). This has created a pressing need to devise the security methods to make the systems more secure, robust and intrusion free. Although the security framework has already revised for the classical system, the exercise for integrating the security measures into the global software engineering is still not very explored into the recent literature. In order to prevent the attacks in the software of global scope, security testing is indeed very essential to identify vulnerabilities and secure software functionality.

During the past decades due to the intensive development of information and communication engineering has evolved the concept of global software engineering. The framework of global software engineering is far distinguished from classical software engineering in terms of its scope, practices, and model. Classical software testing is mainly related to the functionality of the software, its scope and the requirements whereas, global security testing, on the other hand, ensures the secure software functionality, identification of weakness or loopholes to the system and maintains information confidentiality, integrity, and availability. The software quality standard ISO/IEC 9126 ensures the quality of the software (Coallier et. al. 2001).

Common security issues like SQL injection and cross-site scripting can easily handle through security testing techniques. (Bau et. al. 2010). Various models and application level tools have been devised to handle these basic security issues in classical software engineering. However, the basic security methods are found to be deficient to handle the security attacks at the global level. Given that the scope of global software engineering is far wider than classical software engineering. According to the National Institute of Standards and Technology (NIST), inadequate security testing of software results in a high cost of exposure (Planning, S et. al. 2002). Moreover, it eventually results in a massive catastrophic or non-catastrophic loss for the organization. Especially, the designing and development of e-commerce and mobile commerce based application in global software engineering may have massive
Organizational Compatibility as a Predictor of Telecommuting
www.igi-global.com/chapter/organizational-compatibility-predictor-telecommuting/30251?camid=4v1a

An Experience of Running a MOOC on Information Technology
Valentina Dagiene, Danguole Rutkauskiene and Daina Gudoniene (2016). *International Journal of Human Capital and Information Technology Professionals* (pp. 76-88).
www.igi-global.com/article/an-experience-of-running-a-mooc-on-information-technology/160728?camid=4v1a