UNIVERSITI TEKNOLOGI MARA

THE DOCTORAL RESEARCH ABSTRACTS

Volume: 11, Issue 11 April 2017

ELEVENTH ISSUE

INSTITUTE of GRADUATE STUDIES

IGS Biannual Publication

18

Name : AHMAD SALAH MAHMOUD AL-AHMAD

Title : PENETRATION TESTING MODEL FOR MOBILE CLOUD COMPUTING APPLICATIONS

Supervisor : ASSOC. PROF. DR. HJ. SYED AHMAD SHEIKH ALJUNID **(MS)**
DR. NORMALY KAMAL ISMAIL **(CS)**

Mobile cloud computing (MCC) technology possess features mitigating mobile limitations and enhancing cloud services. MCC application penetration testing issues are complex and unique which make the testing difficult for junior penetration testers. It is complex as MCC applications have three intersecting vulnerability domains, namely mobile, web, and cloud. The offloading process adds uniqueness and complexity to the MCC application penetration testing in terms of generating, selecting and executing test cases. To solve these issues, this thesis constructs a model for MCC application penetration testing that reduces the complexity, tackles the uniqueness and assists junior testers in conducting penetration tests on MCC applications more effectively and efficiently. The main objectives of this thesis are to discover the issues in conducting penetration testing on MCC applications and to construct and evaluate MCC application penetration testing model. Design science research methodology is applied with four phases: (i) Theoretical framework construction phase (ii) Model construction phase entails designing the components and processes of MCC application penetration to reduce the complexity and address offloading; (iii) Model implementation phase implements the components and processes of the model into model guidelines and integrated tool called PT2-MCC. This tool manages the repositories, generates and selects test cases, and implements the mobile agent component; (iv) Model evaluation phase applies case study approach and uses an evaluation framework to evaluate the model against selected testing quality and performance attributes. In model evaluation phase, a junior penetration tester conducted two case studies on two MCC applications built by extending two open source native mobile applications. The tester uncovered more vulnerabilities using the constructed model and in less time compared to using the benchmark OWASP Security Testing Guidelines for mobile Apps model, i.e. it uncovered twenty and eight security vulnerabilities in the MCC HerdFinancial and MCC FourGoats applications respectively. The constructed test case selection technique selects a set of test cases that cover the designated entry points and fit with the user requirements. The results analysis showed that the constructed model has successfully tackled both the complexity and uniqueness of MCC application penetration testing by encompassing these multiple vulnerabilities' domains and MCC offloading. This model can significantly increase the efficiency and effectiveness of the penetration test on MCC applications as the evaluation has shown it has helped the junior tester to uncover 65% more security vulnerabilities within 11% less time compared to the benchmark model. The model evaluation is however limited to SQL injections and XSS vulnerabilities only; nevertheless, these two are the most common vulnerabilities for MCC. The main theoretical contribution is the MCC application penetrating testing model. Likewise, this thesis has two practical contributions, namely the PT2-MCC integrated tool that represents the model implementation and the two MCC test bed applications that can be applied as benchmark MCC penetration testing applications. This thesis is significant because it moderates the lack of testing models to detect security vulnerabilities in the MCC applications and help junior penetration testers to be more effective and efficient when testing MCC applications.