

IMPROVING THE SECURITY QUALITY OF USE CASE MODELS THROUGH THE APPLICATION OF SOFTWARE REFACTORING USING GENETIC ALGORITHM

Haris Mumtaz¹, Mohammad Alshayeb^{2*}, Sajjad Mahmood³, Mahmood Niazi⁴

¹*Electrical, Computer and Software Engineering Department, University of Auckland, New Zealand*

^{2,3,4}*Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Saudi Arabia*

¹hmum126@aucklanduni.ac.nz, ²alshayeb@kfupm.edu.sa,

³smahmood@kfupm.edu.sa, ⁴mkniazi@kfupm.edu.sa

Abstract— Use case modelling is an industrial de-facto standard technique to express functional requirements. Security bad smells are design flaws that can potentially degrade the quality of software by affecting a system's ability to prevent malicious activities. The presence of security bad smells in a use case model is likely to propagate security vulnerabilities to other software artefacts. Therefore, the detection and refactoring of security bad smells in use case models is important for ensuring the overall quality of software systems. In this paper, we propose a genetic algorithm-based detection approach to detect security bad smells. A refactoring process is then applied to correct the security bad smells. Finally, the improvement to security is assessed through the statistical analysis of quality metrics. The practicality of the approach is demonstrated by applying it to a set of use case models. The results show that the proposed security bad smell detection and correction technique can significantly improve the quality of use case models.

Keywords— Use Case Refactoring; Software Security; Software Metrics