A maturity model for secure requirements engineering

Mahmood Niazi [a],[*], Ashraf Mohammed Saeed [a], Mohammad Alshayeb [a], Sajjad Mahmood [a], Saad Zafar [b]

[a] Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Saudi Arabia
[b] Faculty of Computing, Riphah International University, Islamabad, Pakistan

A R T I C L E   I N F O

A B S T R A C T

Security is considered to be a critical software quality attribute. Tackling security at the requirements phase helps to avoid the need to rework secure software development issues. The aim of this paper is to develop a Requirements Engineering (RE) Security Maturity Model (RESMM) to assist software development organizations to better specify the requirements for secure software development. To achieve this objective, first, we conducted a systematic literature review (SLR) to identify the requirement practices for secure software development. Then we modified Sommerville's requirements engineering practices. We also conducted a questionnaire survey based on the identified security requirements practices. Next, the RESMM was built based on the results of the SLR, the modified Sommerville practices and feedback from the security practitioners. Finally, two case studies were conducted to assess RESMM. RESMM has 79 practices classified into 7 RE categories. The case study results show that RESMM has a clear structure and is easy to comprehend and use. In addition, the case study participants recommended that software organizations adopt RESMM. RESMM has the ability to identify the RE security maturity levels in software organizations. RESMM can also help software development organizations deliver secure software.

© 2020 Elsevier Ltd. All rights reserved.

---

[*] Corresponding author.
E-mail addresses: mkniazi@kfupm.edu.sa (M. Niazi), g201403260@kfupm.edu.sa (A.M. Saeed), alshayeb@kfupm.edu.sa (M. Alshayeb), smahmood@kfupm.edu.sa (S. Mahmood), saad.zafar@riphah.edu.pk (S. Zafar).