IFIP Advances in Information and Communication Technology

Managing risks and improving cyber resilience-assessing mobile application security using a reference model

Pieterse, Heloise
Council for Scientific and Industrial Research (CSIR)
Meiring Naude Drive, Pretoria, 0184
Email: HPieterse@csir.co.za

Mobile devices, especially smartphones, have become an integral part of users' personal and professional lives. Central to the expansive use and prevalence of mobile devices are mobile applications – software developed to enhance the functionality offered by these devices. Mobile applications offer unparalleled support for users, ranging from personal use to work-related activities. However, increased usage of mobile applications can pose serious security risks due to vulnerabilities or faults that may exist within the software. It becomes, therefore, imperative to evaluate mobile applications for security risks before releasing the software for either general or professional use. Such an evaluation of a mobile application is conducted via a security assessment, which aims to determine if a mobile application conforms to specified security requirements. The proper security assessment of a mobile application requires a framework to guide security analysts in applying techniques and approaches to eliminate risks and ensure resilience against attacks. This paper presents a reference model conceptualising the requirements needed to conduct a comprehensive security assessment of mobile applications. The reference model provides an abstraction of the phases, as well as the relationship between the phases, to guide the assessment of mobile application security. The outcome of this paper is a contribution to a commonly accepted domain definition for assessing mobile application security, ensuring that such assessments can be performed consistently and effectively.