Evaluation of the suitability of the mobility common criteria protection profiles for enterprise mobility management

Jill Dove

Abstract:

Mobile Devices are now ubiquitous in the enterprise, enabling flexible working and new business opportunities. However, the protection of enterprise data on mobile devices is a difficult contemporary business problem.

A set of three Mobility Protection Profiles (PPs) have been released under the Common Criteria (CC) standard. The Mobility PPs aim to provide a comprehensive set of Security Functional Requirements (SFRs) which address the threats to enterprise data on mobile devices. These can be used by vendors to achieve an independent evaluation of their mobility solutions, thus providing a level of assurance to their enterprise customers.

This study performs an “Evaluation of the suitability of the Mobility Common Criteria Protection Profiles for Enterprise Mobility Management”.

To conduct this evaluation, the study first reviews Enterprise Mobility Management (EMM) solutions, focusing on Mobile Device Management (MDM) and Mobile Application Management (MAM) on Android devices. This information is used to construct a conceptual model of the operation of a typical EMM solution. This conceptual model is then used to identify gaps and inconsistencies within the Mobility Pps.

This study concludes that in general the Mobility PPs provide good coverage of the capabilities provided by MDM solutions. However, they do not recognise the importance of compliance reporting, which is especially relevant due to the fragmentation of Android device management. Although the application of security controls by the MDM Agent on behalf of the administrator is well specified in the PPs, the use of administrator and user roles is not, as it lacks clarity, both in terms of their intent, and content.

The PPs are less consistent in their coverage of the capabilities provided by MAM solutions, and by extension the capabilities that are commonly used to manage dual-persona mobile devices. Although there are a considerable number of SFRs that explicitly cover the protection of enterprise resources, containerisation and the provision of secure services to managed apps, they are disjointed and have significant gaps. For example, the role of public app stores is not recognised. There are also gaps in the SFRs relating to managed app authentication, authorisation, per-app Virtual Private Network (VPN) and Data Loss Prevention.

The role of bundled apps is especially ambiguous. The PPs acknowledge their existence, but for understandable reasons they are not included within their scope. However, with their use of shared services, bundled apps are a significant threat to data leakage.