A Permission verification approach for android mobile applications

Abstract:
Mobile applications build part of their security and privacy on a declarative permission model. In this approach mobile applications, to get access to sensitive resources, have to define the corresponding permissions in a manifest. However, mobile applications may request access to permissions that they do not require for their execution (over-privileges) and offer opportunities to malicious software to gain access to otherwise inaccessible resources. In this paper, we investigate on the declarative permissions model on which security and privacy services of Android rely upon. We propose a practical and efficient permission certification technique, in the direction of risk management assessment. We combine both runtime information and static analysis to profile mobile applications and identify if they are over-privileged or follow the least privilege principle. We demonstrate a transparent solution that neither requires modification to the underlying framework, nor access to the applications’ original source code. We assess the effectiveness of our approach, using a randomly selected varied set of mobile applications. Results show that our approach can accurately identify whether an application is over-privileged or not, whilst at the same time guaranteeing the need of declaring specific permissions in the manifest.

Authors:
GENEIATAKIS Dimitrios
NAI FOVINO Igor
KOUNELIS Ioannis
STIRPARO Pasquale
Publication Year:
2015
Publisher:
ELSEVIER ADVANCED TECHNOLOGY
ISSN:
0167-4048
DOI:
10.1016/j.cose.2014.10.005 [2]