Accepted Manuscript

A Permission Verification Approach for Android Mobile Applications

Dimitris Geneiatakis, Igor Nai Fovino, Ioannis Kounelis, Paquale Stirparo

PII: S0167-4048(14)00151-5

DOI: 10.1016/j.cose.2014.10.005

Reference: COSE 840

To appear in: *Computers & Security*

Received Date: 2 January 2014

Revised Date: 6 October 2014

Accepted Date: 14 October 2014

Please cite this article as: Geneiatakis D, Fovino IN, Kounelis I, Stirparo P, A Permission Verification Approach for Android Mobile Applications, *Computers & Security* (2014), doi: 10.1016/j.cose.2014.10.005.

A Permission Verification Approach for Android Mobile Applications

Dimitris Geneiatakis[a,*], Igor Nai Fovino[a], Ioannis Kounelis[a,b], and Paquale Stirparo[a,b]

[a]*Institute for the Protection and Security of the Citizen, Joint Research Centre (JRC), European Commission, Ispra (VA), Italy*
[b]*Royal Institute of Technology (KTH), Stockholm, Sweden*
{*dimitrios.geneiatakis,igor.nai-fovino,ioannis.kounelis, pasquale.stirparo*}*@jrc.ec.europa.eu*

Abstract

Mobile applications build part of their security and privacy on a declarative permission model. In this ~~way~~ 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~~ing~~ 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. ~~, that~~ 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 ~~does~~ 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 ~~randomly selected~~. Results show that our approach can accurately identify whether an application is over-privileged or not, ~~while~~ whilst at the same time guarantee~~ing~~ the need of declaring specific permissions in the manifest.

Keywords: Android, Permissions, Security, Instrumentation, Privacy, Risk assessment

1. Introduction

Mobile Internet is expected to ~~overwhelm~~ overtake the usage of land line Internet [1]. The reason of this success is not only due to the evolution of smartphones and their underlying infrastructures, but also to the one-stop shop model on which the app-stores (*Google Play, Apple store (iOS), etc.*), are based, enabling the users to purchase the desired application and install it directly on their phones without any additional

*Corresponding author