Automatic security verification of mobile app configurations

Gabriele Costa, Alessio Merlo, Luca Verderame, Alessandro Armando

PII: S0167-739X(16)30199-6
DOI: http://dx.doi.org/10.1016/j.future.2016.06.014
Reference: FUTURE 3080

To appear in: *Future Generation Computer Systems*

Received date: 27 August 2015
Revised date: 16 May 2016
Accepted date: 17 June 2016

Automatic Security Verification of Mobile App Configurations

Gabriele Costa[a], Alessio Merlo[a,*], Luca Verderame[a], Alessandro Armando[a,b]

[a] *DIBRIS, Università degli Studi di Genova, Italy*
{alessandro.armando, alessio.merlo, luca.verderame}@unige.it
[b] *Security & Trust Unit, FBK-irst, Trento, Italy*
armando@fbk.eu

Abstract

The swift and continuous evolution of mobile devices is encouraging both private and public organizations to adopt the *Bring Your Own Device* (BYOD) paradigm. As a matter of fact, the BYOD paradigm drastically reduces costs and increases productivity by allowing employees to carry out business tasks on their personal devices. However, it also increases the security concerns, since a compromised device could disruptively access the resources of the organization. The current mobile application distribution model based on application markets does not cope with this issue. In a previous work the concept of secure meta-market has been introduced as a mean to distribute mobile applications always guaranteed to comply with any given BYOD policy. This is achieved through a suitable combination of static analysis (i.e. model checking) and code instrumentation techniques. Although crucial, enforcing security policies over individual applications is not sufficient in general. Indeed, several well documented threats arise from the malicious interaction among applications which are harmless if isolated. In this paper, a novel technique for the security verification of groups of mobile app is proposed. The approach relies on partial model checking (PMC) to extend the existing security guarantees to groups of applications. The experimental results demonstrate the viability of the approach. Moreover, we show through a case study that even a fairly simple security policy can be violated by applications which are compliant if considered one by one.

Keywords: BYOD paradigm, Android Security, Partial Model Checking, Policy Enforcement, Automated Verification

1. Introduction

The relentless evolution of mobile technologies is pushing forward the interest for novel, ubiquitous paradigms. Among them, the *Bring Your Own Device* [13] (BYOD)

[☆] This work has been partially funded by the Italian PRIN project *Security Horizons* (no. 2010XSEMLC).
[*] Corresponding author