1. MoonlightBox: mining android API histories for uncovering release-time inconsistencies

Li Li (1); Bissyande, T. (2); Klein, J. (2)

Author affiliation: (1) Monash University, Faculty of Information Technology, Melbourne, VIC, Australia (2) University of Luxembourg, Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg

Abstract: In most of the approaches aiming at investigating Android apps, the release time of apps is not appropriately taken into account. Through three empirical studies, we demonstrate that the app release time is key for guaranteeing performance. Indeed, not considering time may result in serious threats to the validity of proposed approaches. Unfortunately, even approaches considering time could present some threats to validity when release times are erroneous. Symptoms of such erroneous release times appear in the form of inconsistencies with the APIs leveraged by the app. We present a tool called MoonlightBox for uncovering time inconsistencies by inferring the lower bound assembly time of a given app based on the used API lifetime information: any assembly time below this lower bound is considered as manipulated. We further perform several experiments and confirm that 1) over 7% of Android apps are subject to time inconsistency, 2) malicious apps are more likely to be targeted by time inconsistency, compared to benign apps, 3) time inconsistencies are favoured by some specific app lineages. We eventually revisit the three motivating empirical studies, leveraging MoonlightBox to compute a more realistic timeline of apps. The experimental results confirm that time indeed matters. The accuracy of release time is even crucial to achieve precise results. (0 refs)

Inspec controlled terms: Android (operating system) - application program interfaces - data mining - invasive software

Uncontrolled terms: MoonlightBox - Android apps - API lifetime information - malicious apps - time inconsistencies - Android API histories mining

Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6130S Data security - C6150E General utility programs - C6170K Knowledge engineering techniques

IPC Code: G06F9/00 - G06F9/44 - G06F9/46 - G06F15/18 - G06F21/00 - G06N5/04

Treatment: Practical (PRA)

Database: Inspec

Data Provider: Engineering Village