1. Understanding the evolution of android app vulnerabilities

Jun Gao (1); Li Li (2); Pingfan Kong (1); Bissyande, T.F. (1); Klein, J. (1)
Source: *IEEE Transactions on Reliability*, v 70, n 1, p 212-30, March 2021; **ISSN:** 0018-9529; **DOI:** 10.1109/TR.2019.2956690; **Publisher:** IEEE, USA
Author affiliation: (1) University of Luxembourg, Luxembourg (2) Monash University, Clayton, VIC 3800, Australia
Abstract: The Android ecosystem today is a growing universe of a few billion devices, hundreds of millions of users and millions of applications targeting a wide range of activities where sensitive information is collected and processed. Security of communication and privacy of data are thus of utmost importance in application development. Yet, regularly, there are reports of successful attacks targeting Android users. While some of those attacks exploit vulnerabilities in the Android operating system, others directly concern application-level code written by a large pool of developers with varying experience. Recently, a number of studies have investigated this phenomenon, focusing, however, only on a specific vulnerability type appearing in apps, and based on only a snapshot of the situation at a given time. Thus, the community is still lacking comprehensive studies exploring how vulnerabilities have evolved over time, and how they evolve in a single app across developer updates. Our work fills this gap by leveraging a data stream of 5 million app packages to reconstruct versioned lineages of Android apps, and finally, obtained 28 564 app lineages (i.e., successive releases of the same Android apps) with more than ten app versions each, corresponding to a total of 465 037 apks. Based on these app lineages, we apply state-of-the-art vulnerability-finding tools and investigate systematically the reports produced by each tool. In particular, we study which types of vulnerabilities are found, how they are introduced in the app code, where they are located, and whether they foreshadow malware. We provide insights based on the quantitative data as reported by the tools, but we further discuss the potential false positives. Our findings and study artifacts constitute a tangible knowledge to the community. It could be leveraged by developers to focus verification tasks, and by researchers to drive vulnerability discovery and repair research efforts. (0 refs)
Inspec controlled terms: Android (operating system) - data privacy - invasive software - mobile computing - program diagnostics - security of data
Uncontrolled terms: Android apps - obtained 28 564 app lineages - state-of-the-art vulnerability-finding tools - app code - study artifacts - vulnerability discovery - repair research efforts - android app vulnerabilities - Android ecosystem today - growing universe - billion devices - application development - successful attacks - Android users - Android operating system - application-level code - specific vulnerability type - single app - developer updates - data stream - 5 million app packages - versioned lineages
Classification Code: C6130S Data security - C6150G Diagnostic, testing, debugging and evaluating systems - C6190V Mobile, ubiquitous and pervasive computing
IPC Code: G06F9/44 - G06F9/46 - G06F11/36 - G06F21/00
Treatment: Bibliography (BIB) - Practical (PRA)
Database: Inspec
Data Provider: Engineering Village