1. Understanding Android App Piggybacking

Li Li (1); Daoyuan Li (1); Bissyande, T.F. (1); Klein, J. (1); Le Traon, Y. (1); Lo, D. (2); Cavallaro, L. (3)
Source: *2017 IEEE/ACM 39th International Conference on Software Engineering: Companion (ICSE-C)*, p 359-61, 2017; **ISBN-13:** 978-1-5386-1589-8; **DOI:** 10.1109/ICSE-C.2017.109; **Conference:** 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE), 20-28 May 2017, Buenos Aires, Argentina; **Publisher:** IEEE Computer Society, Los Alamitos, CA, USA
Author affiliation: (1) University of Luxembourg, Interdisciplinary Centre for Security, Luxembourg (2) Singapore Management University, School of Information Systems, Singapore (3) Royal Holloway, University of London, Information Security Group, United Kingdom
Abstract: The Android packaging model offers adequate opportunities for attackers to inject malicious code into popular benign apps, attempting to develop new malicious apps that can then be easily spread to a large user base. Despite the fact that the literature has already presented a number of tools to detect piggybacked apps, there is still lacking a comprehensive investigation on the piggybacking processes. To fill this gap, in this work, we collect a large set of benign/piggybacked app pairs that can be taken as benchmark apps for further investigation. We manually look into these benchmark pairs for understanding the characteristics of piggybacking apps and eventually we report 20 interesting findings. We expect these findings to initiate new research directions such as practical and scalable piggybacked app detection, explainable malware detection, and malicious code location. (0 refs)
Inspec controlled terms: Android (operating system) - invasive software
Uncontrolled terms: Android application piggybacking - Android packaging model - benign applications - malicious applications - benchmark applications - malware detection - malicious code location
Classification Code: C6130S Data security - C6150J Operating systems - C6190V Mobile, ubiquitous and pervasive computing
IPC Code: G06F9/44 - G06F9/46 - G06F21/00
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village