1. Understanding Android App piggybacking: A systematic study of malicious code grafting

Li Li (1); Daoyuan Li (1); Bissyande, T.F. (1); Klein, J. (1); Le Traon, Y. (1); Lo, D. (2); Cavallaro, L. (3)

Source: *IEEE Transactions on Information Forensics and Security*, v 12, n 6, p 1269-84, June 2017; **ISSN:** 1556-6013; **DOI:** 10.1109/TIFS.2017.2656460; **Publisher:** IEEE, USA

Author affiliation: (1) University of Luxembourg, Interdisciplinary Centre for Security, Luxembourg (2) Singapore Management University, Singapore (3) Royal Holloway, University of London, United Kingdom

Abstract: The Android packaging model offers ample opportunities for malware writers to piggyback malicious code in popular apps, which can then be easily spread to a large user base. Although recent research has produced approaches and tools to identify piggybacked apps, the literature lacks a comprehensive investigation into such phenomenon. We fill this gap by: 1) systematically building a large set of piggybacked and benign apps pairs, which we release to the community; 2) empirically studying the characteristics of malicious piggybacked apps in comparison with their benign counterparts; and 3) providing insights on piggybacking processes. Among several findings providing insights analysis techniques should build upon to improve the overall detection and classification accuracy of piggybacked apps, we show that piggybacking operations not only concern app code, but also extensively manipulates app resource files, largely contradicting common beliefs. We also find that piggybacking is done with little sophistication, in many cases automatically, and often via library code. (0 refs)

Inspec controlled terms: invasive software - mobile computing
Uncontrolled terms: Android app piggybacking - malicious code grafting - Android packaging model - malware writers - malicious code piggybacking - malicious piggybacked apps - library code
Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6130S Data security
IPC Code: G06F9/44 - G06F21/00
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village