1. Automatically Locating Malicious Packages in Piggybacked Android Apps

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

Source: *2017 IEEE/ACM 4th International Conference on Mobile Software Engineering and Systems (MOBILESoft). Proceedings*, p 170-4, 2017; **ISBN-13:** 978-1-5386-2669-6; **DOI:** 10.1109/MOBILESoft.2017.6; **Conference:** 2017 IEEE/ACM 4th International Conference on Mobile Software Engineering and Systems (MOBILESoft), 22-23 May 2017, Buenos Aires, Argentina; **Publisher:** IEEE Computer Society, Los Alamitos, CA, USA

Author affiliation: (1) University of Luxembourg, Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg (2) Washington State University, Pullman, WA, United States (3) Singapore Management University, School of Information Systems, Singapore

Abstract: To devise efficient approaches and tools for detecting malicious packages in the Android ecosystem, researchers are increasingly required to have a deep understanding of malware. There is thus a need to provide a framework for dissecting malware and locating malicious program fragments within app code in order to build a comprehensive dataset of malicious samples. Towards addressing this need, we propose in this work a tool-based approach called HookRanker, which provides ranked lists of potentially malicious packages based on the way malware behaviour code is triggered. With experiments on a ground truth set of piggybacked apps, we are able to automatically locate the malicious packages from piggybacked Android apps with an accuracy of 83.6% in verifying the top five reported items. (0 refs)

Inspec controlled terms: invasive software - mobile computing - smart phones - software tools - source code (software)
Uncontrolled terms: malware behaviour code - HookRanker - tool-based approach - piggybacked Android apps - malicious packages detection
Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6115 Programming support - C6130S Data security
IPC Code: G06F9/44 - G06F21/00 - H04M1/725
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village