1. An empirical study of potentially malicious third-party libraries in Android apps

Zicheng Zhang (1); Wenrui Diao (1); Chengyu Hu (1); Shanqing Guo (1); Chaoshun Zuo (2); Li Li (3)
Source: *WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, p 144-54, 8 July 2020; **ISBN-13:** 978-1-4503-8006-5; **DOI:** 10.1145/3395351.3399346; **Conference:** WiSec '20: 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 8-10 July 2020, Linz, Austria; **Sponsor:** SIGSAC; **Publisher:** ACM, New York, NY, USA
Author affiliation: (1) Shandong University, China (2) Ohio State University, Columbus, OH, United States (3) Monash University, Monash, VIC, Australia
Abstract: The rapid development of Android apps primarily benefits from third-party libraries that provide well-encapsulated functionalities. On the other hand, more and more malicious libraries are discovered in the wild, which brings new security challenges. Despite some previous studies focusing on the malicious libraries, however, most of them only study specific types of libraries or individual cases. The security community still lacks a comprehensive understanding of potentially malicious libraries (PMLs) in the wild.In this paper, we systematically study the PMLs based on a large-scale APK dataset (over 500K samples), including extraction, identification, and comprehensive analysis. On the high-level, we conducted a two-stage study. In the first stage, to collect enough analyzing samples, we designed an automatic tool to extract libraries and identify PMLs. In the second stage, we conducted a comprehensive study of the obtained PMLs. Notably, we analyzed four representative aspects of PMLs: library repackaging, exposed behaviors, permissions, and developer connections. Several interesting facts were discovered. We believe our study will provide new knowledge of malicious libraries and help design targets defense solutions to mitigate the corresponding security risks. (0 refs)
Inspec controlled terms: Android (operating system) - mobile computing - security of data - software libraries
Uncontrolled terms: library repackaging - Android apps - potentially malicious third-party libraries - security risks
Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6110B Software engineering techniques - C6130S Data security
IPC Code: G06F9/44 - G06F9/46 - G06F21/00
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village