1. Negative Results on Mining Crypto-API Usage Rules in Android Apps

Jun Gao (1); Pingfan Kong (1); Li Li (2); Bissyande, T.F. (1); Klein, J. (1)

Source: *2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR)*, p 388-98, 2019;
DOI: 10.1109/MSR.2019.00065; **Conference:** 2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR), 25-31 May 2019, Montreal, QC, Canada; **Publisher:** IEEE, Piscataway, NJ, USA

Author affiliation: (1) University of Luxembourg, Luxembourg (2) Monash University, Melbourne, VIC, Australia

Abstract: Android app developers recurrently use crypto-APIs to provide data security to app users. Unfortunately, misuse of APIs only creates an illusion of security and even exposes apps to systematic attacks. It is thus necessary to provide developers with a statically-enforceable list of specifications of crypto-API usage rules. On the one hand, such rules cannot be manually written as the process does not scale to all available APIs. On the other hand, a classical mining approach based on common usage patterns is not relevant in Android, given that a large share of usages include mistakes. In this work, building on the assumption that "developers update API usage instances to fix misuses", we propose to mine a large dataset of updates within about 40 000 real-world app lineages to infer API usage rules. Eventually, our investigations yield negative results on our assumption that API usage updates tend to correct misuses. Actually, it appears that updates that fix misuses may be unintentional: the same misuses patterns are quickly re-introduced by subsequent updates. (0 refs)

Inspec controlled terms: Android (operating system) - application program interfaces - cryptography - data mining - mobile computing
Uncontrolled terms: data security - systematic attacks - Android apps - crypto-API usage rule mining - API misuse patterns
Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6150E General utility programs - C6130S Data security - C6170K Knowledge engineering techniques
IPC Code: G06F9/00 - G06F9/44 - G06F9/46 - G06F15/18 - G06F21/00 - G06N5/04
Treatment: Practical (PRA)
Database: Inspec
Data Provider: Engineering Village