1. Potential Component Leaks in Android Apps: An Investigation into a New Feature Set for Malware Detection (*Open Access*)

Li, Li (1); Allix, Kevin (1); Li, Daoyuan (1); Bartel, Alexandre (2); Bissyandé, Tegawendé F. (1); Klein, Jacques (1)
Source: *Proceedings - 2015 IEEE International Conference on Software Quality, Reliability and Security, QRS 2015*, p 195-200, September 21, 2015, *Proceedings - 2015 IEEE International Conference on Software Quality, Reliability and Security, QRS 2015*; **ISBN-13:** 9781467379892; **DOI:** 10.1109/QRS.2015.36; **Article number:** 7272932; **Conference:** IEEE International Conference on Software Quality, Reliability and Security, QRS 2015, August 3, 2015 - August 5, 2015; **Sponsor:** IEEE Reliability Society; **Publisher:** Institute of Electrical and Electronics Engineers Inc.
Author affiliation: (1) SnT, University of Luxembourg, Luxembourg (2) EC SPRIDE, Technische Universität Darmstadt, Germany
Abstract: We discuss the capability of a new feature set for malware detection based on potential component leaks (PCLs). PCLs are defined as sensitive data-flows that involve Android inter-component communications. We show that PCLs are common in Android apps and that malicious applications indeed manipulate significantly more PCLs than benign apps. Then, we evaluate a machine learning-based approach relying on PCLs. Experimental validations show high performance for identifying malware, demonstrating that PCLs can be used for discriminating malicious apps from benign apps. © 2015 IEEE. (28 refs)
Main heading: Mobile security
Controlled terms: Android (operating system) - Computer software selection and evaluation - Feature extraction - Malware - Software reliability
Uncontrolled terms: Android apps - Experimental validations - Feature sets - Malware detection - On potentials - Sensitive datas
Classification Code: 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing
Open Access type(s): All Open Access, Green
Database: Compendex
Data Provider: Engineering Village