1. POSTER: Detection of information leaks via reflection in android apps

Gajrani, Jyoti (1); Li, Li (2); Laxmi, Vijay (1); Tripathi, Meenakshi (1); Gaur, M.S. (1); Conti, Mauro (3)
Source: *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, p 911-913, April 2, 2017, *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*; **ISBN-13:** 9781450349444; **DOI:** 10.1145/3052973.3055162; **Conference:** 2017 ACM Asia Conference on Computer and Communications Security, ASIA CCS 2017, April 2, 2017 - April 6, 2017; **Sponsor:** ACM SIGSAC; **Publisher:** Association for Computing Machinery
Author affiliation: (1) MNIT, Jaipur, India (2) SnT, University of Luxembourg, Luxembourg (3) University of Padua, Italy
Abstract: Reflection is a language feature which allows to analyze and transform the behavior of classes at the runtime. Reflection is used for software debugging and testing. Malware authors can leverage re ection to subvert the malware de- tection by static analyzers. Re ection initializes the class, invokes any method of class, or accesses any field of class. But, instead of utilizing usual programming language syn- tax, reflection passes classes/methods etc. as parameters to reflective APIs. As a consequence, these parameters can be constructed dynamically or can be encrypted by malware. These cannot be detected by state-of-the-art static tools. We propose EspyDroid, a system that combines dynamic analysis with code instrumentation for a more precise and automated detection of malware employing re ection. Weflevaluate EspyDroid on 28 benchmark apps employing majorflre ection categories. Our technique show improved results over FlowDroid via detection of additional undetected ows. These flows have potential to leak sensitive and private in- formation of the users, through various sinks. © 2017 ACM. (10 refs)
Main heading: Mobile security
Controlled terms: Android (operating system) - Application programming interfaces (API) - Dynamic analysis - Malware - Program debugging - Reflection - Software testing
Uncontrolled terms: Android - Automated detection - Code instrumentation - Instrumentation - Language features - Software debugging - State of the art - Static analyzers
Classification Code: 723 Computer Software, Data Handling and Applications
Database: Compendex
Data Provider: Engineering Village