Android Application Analysis using Reverse Engineering Techniques and Taint-Aware Slicing

Abstract

Android is a victim of its own success, not just in the way it has attracted malicious attention, but in its very nature. One of the reasons the OS has succeeded in gaining market share so rapidly is that it is open source; it is essentially free for manufacturers to implement. Android platform provide only coarse-grained permissions to users with regard to how third party applications use sensitive private data. Malicious applications pose a threat to the security of the Android platform. The growing amount and diversity of these applications render conventional defenses largely ineffective and thus Android smartphones often remain unprotected from novel malware.

In this paper, we propose AT2: "Android Taint Analysis Tool", a lightweight tool
uses static method for analyzing Android applications (APKs) and generating a detailed report of the analysis performed. AT2 is a tool which performs a static analysis, gathering as many features of an application as possible. AT2 analyzes Smali code, a disassembled version of the DEX format used by Android's Java VM implementation. The provided application is sliced in order to perform data-flow analyses to backtrack parameters used by a given method. This helps to identify suspicious code regions in an automated way. Several other analysis techniques such as visualization of control flow graphs or identification of ad-related code is also possible.

References

- Researcher to demo hack for logging Android, iOS touchscreen movements - January 30, 2014

- APKdownloads - http://www.apkdownloads.com
- The Effectiveness of Application Permissions - Usenix - www.usenix.org/event/webapps11/tech/final_files/Felt.pdf
  - Highly Precise Taint Analysis for Android Applications 2013 - Christian Fritz, Steven Arzt, Siegfried Rasthofer, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves le Traon, Damien Octeau and Patrick McDaniel - Secure Software Engineering Group, EC SPRIDE,SnT, University of Luxembourg - Penn State University
  - All You Ever Wanted to Know About - Dynamic Taint Analysis and Forward Symbolic Execution(but might have been afraid to ask) 2009 - Edward J. Schwartz, Thanassis Avgerinos,
David Brumley - Carnegie Mellon University Pittsburgh, PA


Index Terms
Computer Science Software Engineering

**Keywords**

Mobile Malware Taint Analysis Android Static Analysis Tool