Rage against the virtual machine | Proceedings of the Seventh European Workshop on System Security

By Michalis PolychronakisColumbia UniversityView Profile

Abstract

Antivirus companies, mobile application marketplaces, and the security research community, employ techniques based on dynamic code analysis to detect and analyze mobile malware. In this paper, we present a broad range of anti-analysis techniques that malware can employ to evade dynamic analysis in emulated Android environments. Our detection heuristics span three different categories based on (*i*) static properties, (*ii*) dynamic sensor information, and (*iii*) VM-related intricacies of the Android Emulator. To assess the effectiveness of our techniques, we incorporated them in real malware samples and submitted them to publicly available Android dynamic analysis systems, with alarming results. We found *all* tools and services to be vulnerable to most of our evasion techniques. Even trivial techniques, such as checking the value of the IMEI, are enough to evade some of the existing dynamic analysis frameworks. We propose possible countermeasures to improve the resistance of current dynamic analysis tools against evasion attempts.

Formats available

You can view the full content in the following formats:

References

[1]

http://googlemobile.blogspot.com/2012/02/android-and-security.html.

[2]

http://vrt-blog.snort.org/2013/04/changing-imei-provider-model-and-phone.html.

[3]

http://blog.sfgate.com/techchron/2013/10/10/stanford-researchers-discover-alarming-method-for-phone-tracking-fingerprinting-through-sensor-flaws/.

[4]

http://code.google.com/p/openintents/wiki/SensorSimulator.
