Morpheus: Automatically Generating Red Pills to Detect Android Emulators

IRA A. FULTON SCHOOLS OF engineering
ARIZONA STATE UNIVERSITY

Yiming Jing, Ziming Zhao, Gail-Joon Ahn and Hongxin Hu
Arizona State University and Clemson University

sefcom
security engineering for future computing

Motivation

Dynamic analysis systems built on VMs/emulators are the latest and key approach of screening malware. However, emerging evasive Android malware has been attempting to detect emulators with heuristics (red pills) and bypass analysis.

Introduction

- Emulators are widely used in dynamic analysis

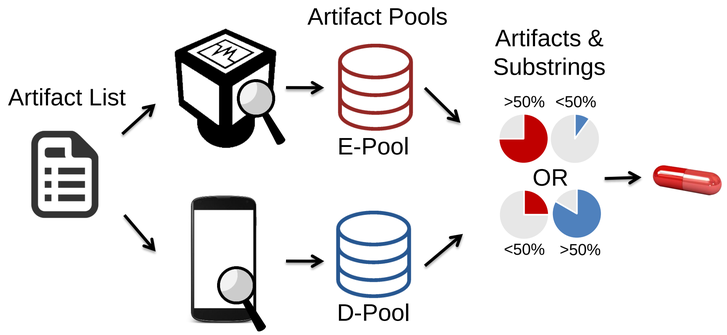
QEMU VirtualBox

- Emulators can be easily detected (and evaded)

```
if getDeviceID().contains("000000000") ||
   getFileStreamPath("/sys/qemu_trace").exists()
      stay_dormant(); // Possibly Emulator
else
      do_evil();      // Device
```

- Key observations on red pills for Android apps
  - Red pills are derived from artifacts that are visible/readable to apps
  - Red pills imply discrepancies
  - Red pills are accessible with few lines of Java code
- We propose Morpheus to automatically and systematically discover red pills

System Workflow



Discovered Red Pills

- We chose three types of visible/readable artifacts
  1. **Files** under /proc and /sys
  2. Android **APIs**
  3. Android system **properties**
- Discovered red pills

# of Instances	# of Red Pills			
	File	API	Property	Total
QEMU (16)	2,961	163	132	3,256
VirtualBox (11)	4,782	150	160	5,092
Q & V (27)	2,121	81	82	2,284
Total	9,864	394	374	**10,632**

- **Software-emulated hardware** contributes most of the discovered red pills
  - isTetheringSupported() → Network
  - /proc/acpi → Power
  - /sys/class/i2c-dev → Audio
  - gsm.version.baseband → Cellular

Evaluated Red Pills

- We evaluated

Top 30 red pills

9 dynamic analysis systems

128 distinct Android devices

- Accuracies of the top 30 red pills

- 17 red pills achieved **>90%** accuracy
- 3 red pills achieved **100%** accuracy
  - /proc/ioports contains a substring "0ff\0:"
  - /sys/devices/system/cpu/cpu0/cpufreq
  - /sys/devices/virtual/misc/android_adb

Conclusion

Morpheus discovers red pills in a more proactive manner. The results will help design robust malware analysis systems and understand the important implications of emulator detection techniques for mobile apps. Currently we are investigating research challenges in eliciting and realizing requirements for a detection-resistant polymorphic emulator and a red pill scanner.

Acknowledgements & Contact Info

This work was supported in part by the National Science Foundation and National Research Foundation.

- **Web: http: //honeynet.asu.edu/morpheus**
- **Email: ymjing@asu.edu**