BareDroid: Large-Scale Analysis of Android Apps on Real Devices

DEC 17TH, 2015

论文下载：http://cs.ucsb.edu/~yanick/publications/2015_acsac_baredroid.pdf

ABSTRACT && INTRODUCTION

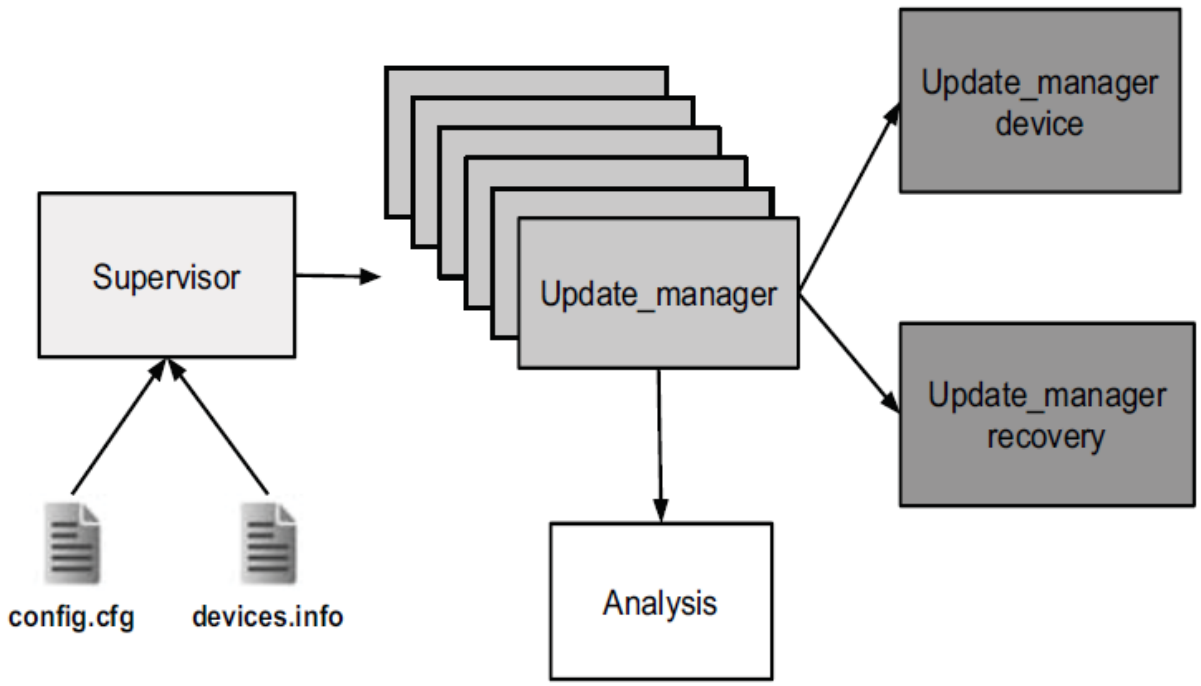
- 真机上跑恶意APP存在难以复原的问题，同时花费成本较高。
- 所以大多数安全研究人员都选择安卓模拟器测试恶意APP，因此现如今大多数恶意APP均会根据模拟器的特征检测是否运行在模拟器的环境中。
- 作者根据以上原因，开发了一套能够在真机上拍摄快照、回复快照的框架。

BareDroid

快照

- 由于每次分析完一个恶意APP后，全分区恢复速度很慢，所以作者根据不同的分区设置了不同的方案：
  1. 系统分区：在boot的时候，当系统分区S1执行完内部代码后，会检测下一个系统分区S2的完整性，以此类推，形成一个可信赖链。因此，只需要每次恢复系统分区S1就行。
  2. 用户分区：对于每一个用户分区Ui，BareDroid会复制三份，两份工作分区Ui1,Ui2,一个干净的初始分区Ui3。当恶意APP在工作分区Ui1上工作时，Ui2恢复到Ui3;当恶意APP在工作分区Ui2上工作时，Ui1恢复。
- 为了保证初始分区Ui3不受到恶意APP的篡改，BareDroid沿用了SElinux作为底层的安全机制：将分区Ui3设置成只读。

多台真实设备形成的phone cloud



- eight Nexus 5 32GB with Android 5.1.0 r3, and one Asus Nexus 7 2012 (WiFi) 32GB using Android 5.1.0 r3

- Supervisor用USB和这些设备通过ADB连接，管理reboot、恢复等功能

实验

Table 1: Time necessary by BareDroid to restore a device

Restoring step	Time (seconds)
restore the `recovery` partition using ADB	0.963
reboot into *recovery mode*	8.923
swap `userdata` partitions	1.976
boot the operating system	19.900
total	**31.762**
if dm-verity detects errors in the `system` partition:	
send `system` partition through ADB	27.927
rewrite `system` partition	35.233
total	**94.922**

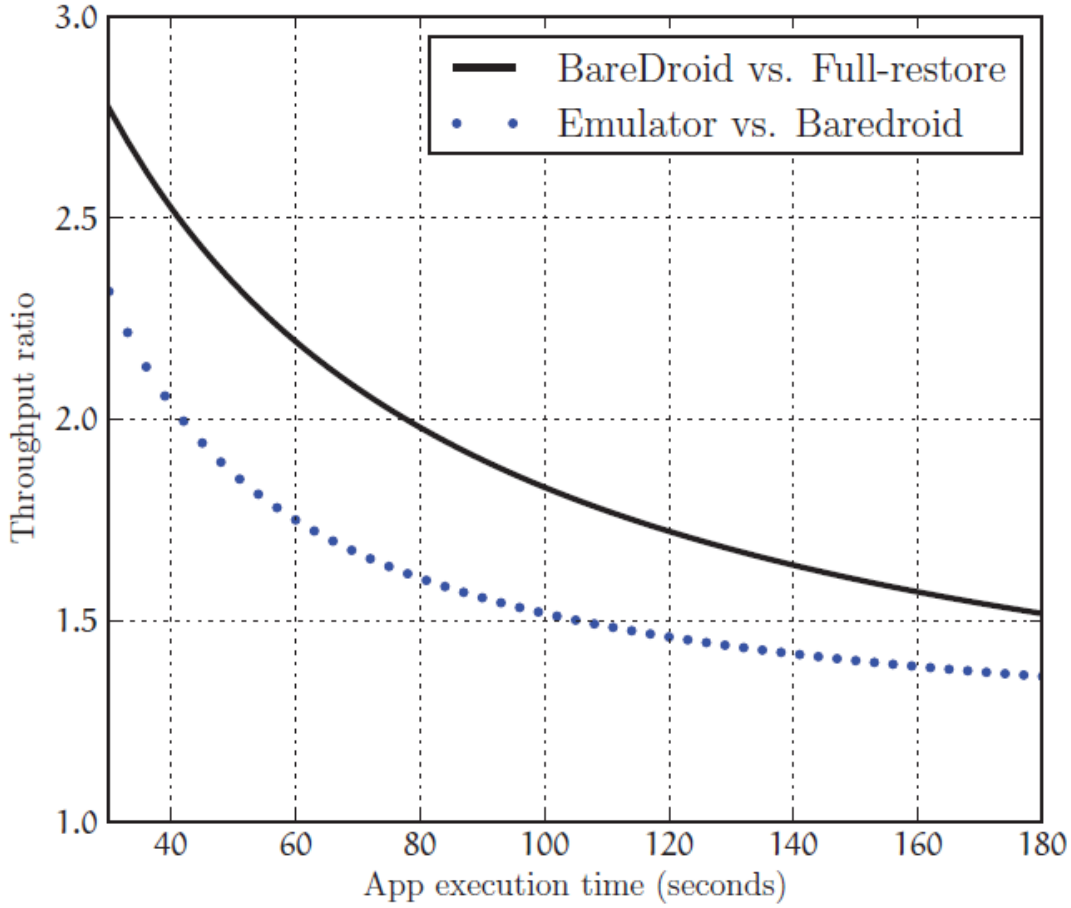


Figure 3: Throughput ratio between the different analyzed systems.

Sample	Emulator-based system	BareDroid
Android.HeHe.1	2 (11.76)%	17
Android.HeHe.2	9 (27.27)%	33
Android.HeHe.3	2 (11.76)%	17
Android.HeHe.4	0* (0.00)%	50
Android.HeHe.5	0* (0.00)%	50
Android.HeHe.6	9 (27.27)%	33
Android_Pincer.A	3 (8.82)%	34
OBAD.1	0* (0.00)%	32
OBAD.2	0* (0.00)%	32
total	**25 (8.39%)**	**298**