“Hey, You, Get off of My Market”

Detecting Malicious Apps in Official and Alternative Android Markets

•••

Paper Presented by: Przemysław Warias

Overview

- Evaluate Android Markets (Official and Unofficial)
  - Health of Markets
- DroidRanger

Motivation

- Android was exploding in popularity
- No comprehensive study of Android Markets was done yet
- Malware detection was signature based

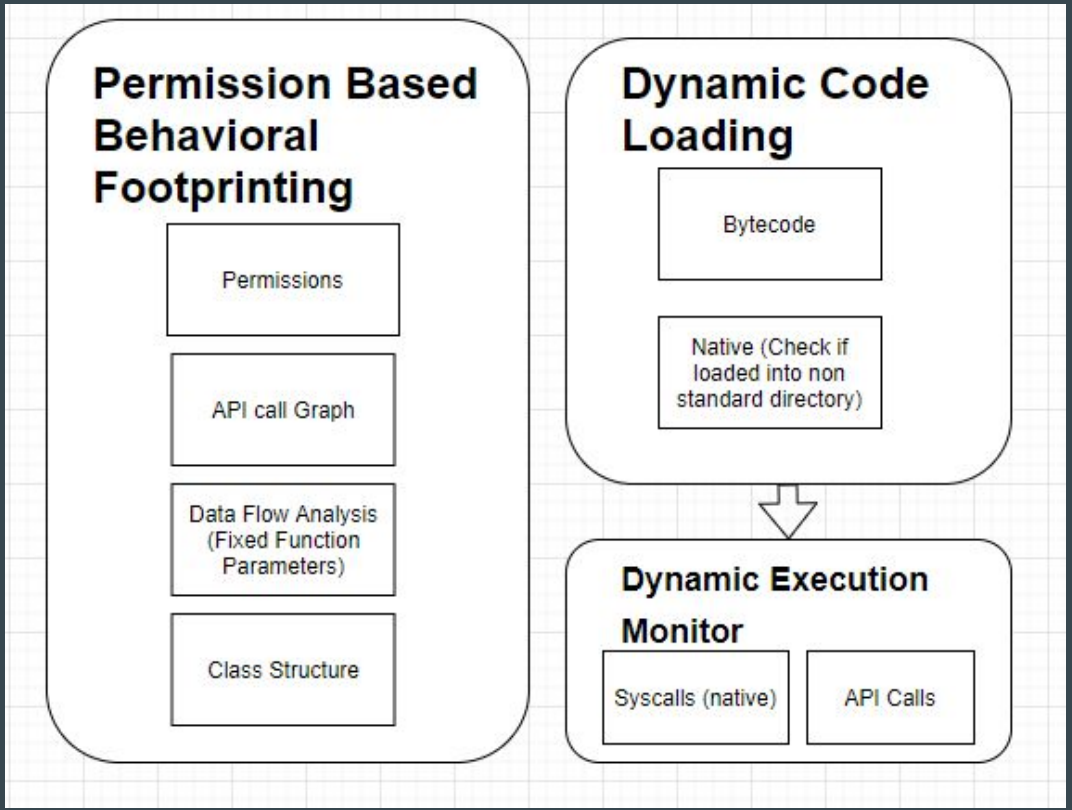
Technical Details

- DroidRanger
  a. Permission based behavioral footprinting
  b. Heuristics based filtering scheme

a. Scalable, efficient and catches known malware
   - Distill known malware to a footprint: API call graph + Permissions
   - Data Flow Analysis: Detect fixed function parameters
   - Example: App has permission to android.provider.Telephony.SMS_RECIEVED and API calls abortBroadcast

b. Used to catch unknown malware
   - Detects dynamic loading of new (untrusted) code, either java binary or native machine code

Technical Details Diagrams



Evaluation

- Collected 200,000+ applications from 5 different markets
  - Android Marketplace (75% of samples)
  - eoeMarket
  - alcatelclub
  - Gfan
  - Mmoovv
- 10 known Malwares used

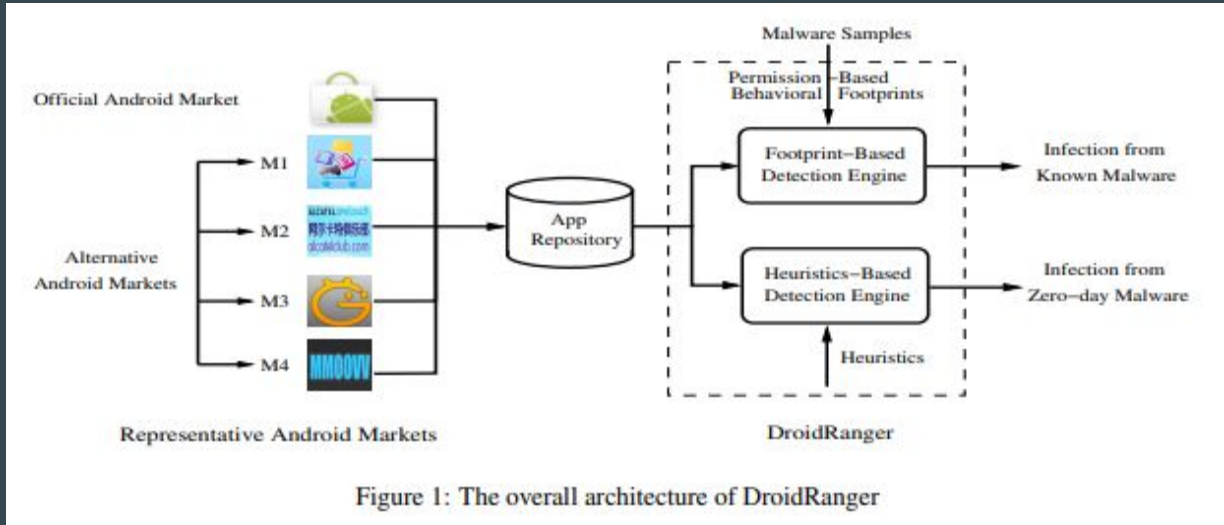


Figure 1: The overall architecture of DroidRanger

Results

- 171 infected apps found (119 unique)
  - Android Market: 32 apps ~0.02% infection rate
  - Other markets 0.20%-0.47%
- Two zero day malware found: Plankton (11 apps on AM) and DroidKungFu
  - Plankton found using dynamic code loading (jar file)
  - DroidKungFu found because of suspicious syscalls

Table 7: The missed known malware families by Lookout Security & Antivirus software (T, D, and M represent the total, detected, and missed number of samples, respectively.)

	ADRD			Bgserv			jSMSHider			BaseBridge			Pjapps		
	T	D	M	T	D	M	T	D	M	T	D	M	T	D	M
version 6.3 (r8472)	8	3	5	1	0	1	9	6	3	4	1	3	31	15	16
version 6.11 (26cf47e)	8	3	5	1	0	1	9	9	0	4	4	0	31	31	0

Table 8: Two zero-day malware families detected by DroidRanger

Malware	Official Android Market	Alternative Markets				Total	Distinct
		M1	M2	M3	M4		
Plankton	11	0	0	0	0	11	11
DroidKungFu	0	9	10	1	9	29	18
Total	11	9	10	1	9	40	29

Contribution

- Showed Android Market has an order of magnitude lower infection rate
- First comprehensive study of the Android Marketplace, and first comparison to alternative markets
- 2 Zero Day Malwares
- Showed there is a need for a more vigorous app vetting process in both official and unofficial marketplaces

Limitations

- Only sampled free apps
- Not applicable to other app stores such as IOS
- Only used two basic heuristics to uncover zero day malware

References

- https://www.csd.uoc.gr/~hy558/papers/mal_apps.pdf (link to paper)\
- Enck et al.

Thank you!

Questions?