On Mobile Malware Infection Rates

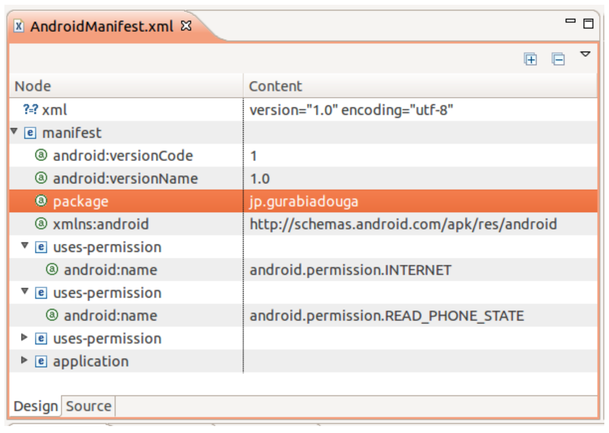
Sourav Bhattacharya and Hien Truong

UNIVERSITY OF HELSINKI

- How prevalent is mobile malware? How to detect susceptibility of a device for infection?
- Estimated Android malware infection rate ~0.26%; Inexpensive instrumentation to detect susceptibility for infection is promising.

Android Package Identification

- Android package name alone is not a reliable identifier
- An Android package can be identified uniquely using:
  - dc: hash of developer cert
  - p: Android package name
  - v: version code

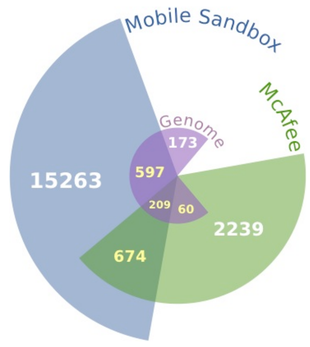


Structure of an Android package

Malware and Carat Datasets

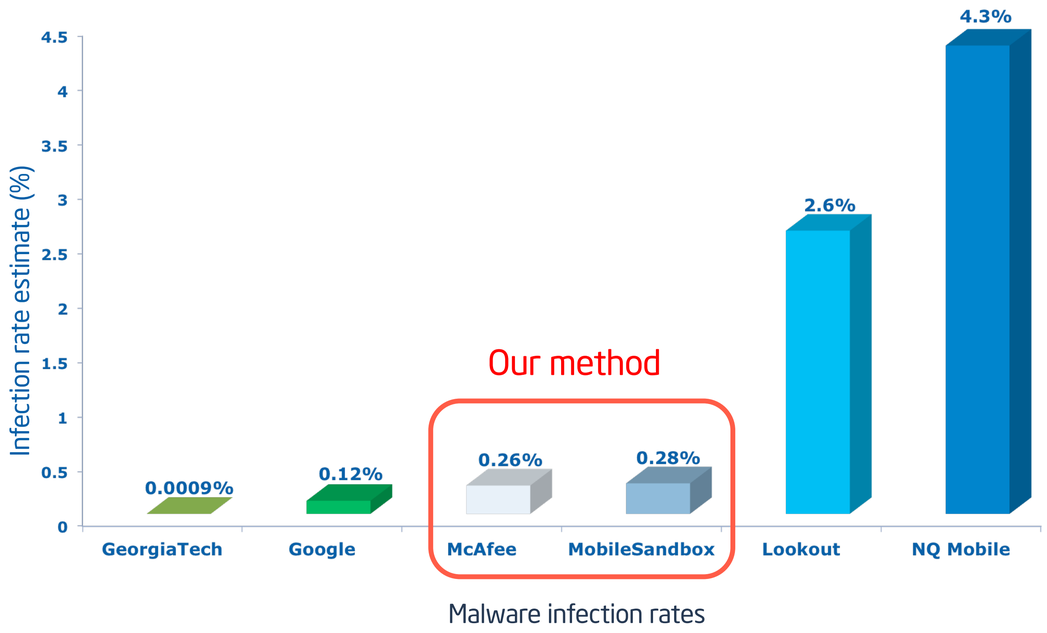
Type	Count
Distinct devices	55,278
Unique developer certificates <dc>	21,486
Unique <dc, p, v> tuples	192,081
Total unique records	5,358,819

Carat dataset



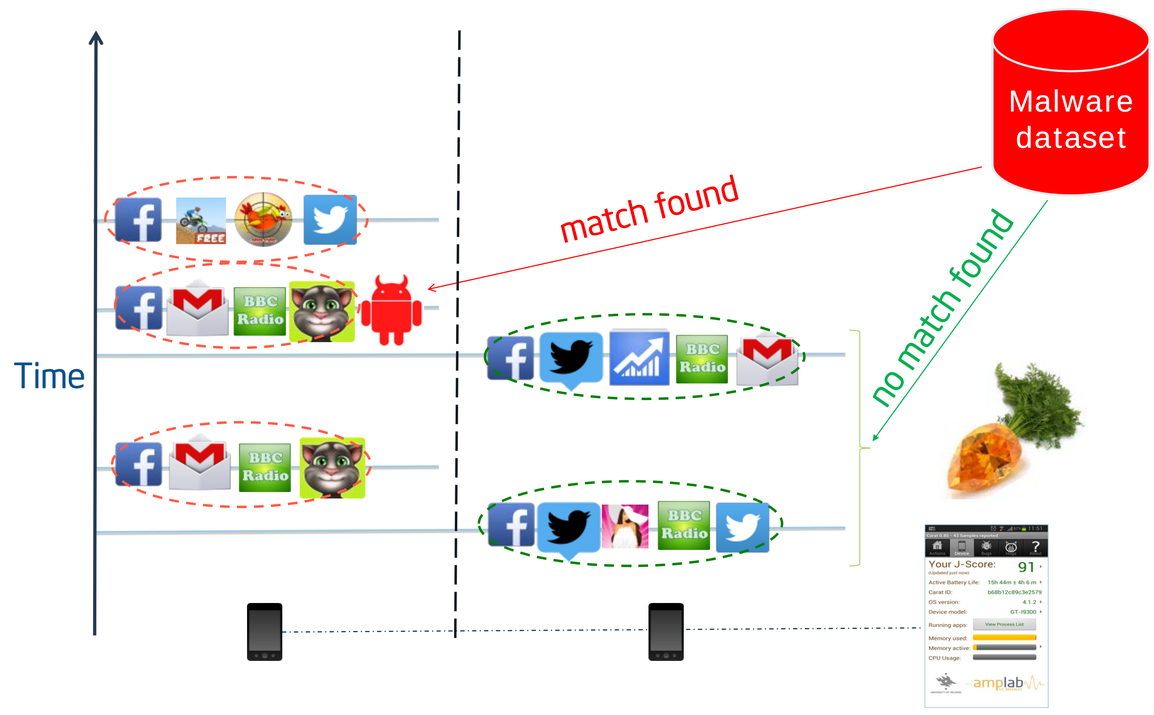
Malware datasets

Prevalence of Mobile Malware[1]



Malware infection rates

Malware Prediction Framework



Device 1 Infected

Device 2 Clean

Carat running on mobile devices

The sets of applications running on a device at various time instants are collected by the installed Carat application. Malware datasets are obtained from anti-virus companies/researchers

Classification Results

Datasets	Precision	Baseline	Gain
McAfee	0.97%	0.21%	4.6X
Mobile Sandbox	0.65%	0.14%	4.8X

Detecting infection using Naïve Bayes classifier

- Naïve Bayes classifier trained after removing known malware apps
- Classification can help anti-malware vendors to narrow down search for new malware

Future Work

- Incorporating time information for better classification and possible prediction of future infection
- Extending device-specific feature extraction based on application types

http://se-sy.org/projects/malware

Reference:

[1] Hien Thi Thu Truong, Eemil Lagerspetz, Petteri Nurmi, Adam J. Oliner, Sasu Tarkoma, N. Asokan, Sourav Bhattacharya, The company you keep: mobile malware infection rates and inexpensive risk indicators, Proceeding of the 23rd international conference on World wide web (WWW), 2014.

Intel CRI for Secure Computing