Usable Mobile Security

Intel Institute for Collaborative Research in Helsinki, Finland

N. Asokan

Professor, Department of Computer Science

Intel ERIC, Oct 2013

About Finland

Home to leading universities

University of Helsinki: Traditional university

Aalto[1] University: Helsinki U. of Tech. + schools of design & business

Tampere University of Technology

...

Innovation hub

Local giants: Nokia, Ericsson, Nokia-Siemens, ...

Recent arrivals: Intel, Samsung, Huawei, ...

New tigers: Rovio, Supercell, ..., lots of startups

1. http://en.wikipedia.org/wiki/Alvar_Aalto

UNIVERSITY OF HELSINKI

Aalto University

ICRI-SC Helsinki personnel

Two researchers funded by Intel

- Postdoc: Sini Ruohomaa
- Graduate student: Thomas Nyman

Matching funding by University

- Postdoc (50%): Hien Truong
- Graduate student: Sourav Bhattacharya (full-time from Jan)
- Graduate student: Jian Liu
- Graduate student: Tanel Dettenhorn (fill-time from Jan)

Intel researchers pursuing PhD

- Elena Reshetova (SSG/OTC)
- Brian McGillion (MCG)

Secure Systems group http://www.cs.helsinki.fi/group/secures/

Initial topics

Mobile security that is easy to use and inexpensive to deploy.

1. **Next generation hardware TEEs**: how to safely expose hardware-based *TEE functionality to app developers*?

2. **Novel applications of platform security**: can *existing platform security* mechanisms address security needs of *new usage scenarios*?

3. **Malware insights**: can we use *lightweight instrumentation* on a device to predict if it will (eventually) get malware?

How prevalent is mobile malware?

domains. We make several important observations. The mobile malware found by the research community thus far appears in a minuscule number of devices in the network: 3,492 out of over 380 million (less than 0.0009%) observed during the course of our analysis. This result lends cre-

The Core of the Matter:
Analyzing Malicious Traffic in Cellular Carriers

Charles Lever, *Georgia Institute of Technology*, chazlever@gatech.edu
Manos Antonakakis, *Damballa*, manos@damballa.com
Brad Reaves, *Georgia Institute of Technology*, brad.reaves@gatech.edu
Patrick Traynor, *Georgia Institute of Technology*, traynor@cc.gatech.edu
Wenke Lee, *Georgia Institute of Technology*, wenke@cc.gatech.edu

NDSS 2013

?


Study: 32.8 Million Android Phones Infec...

techland.time.com/2013/04/17/study-32-8-million-android-phones-infected-with-malware

TIME Tech

SECTIONS

Search TIME

SECURITY

Study: 32.8 Million Android Phones Infected with Malware

By Techlicious / Fox Van Allen | April 17, 2013 | 9 Comments

Share | Tweet 107 | +1 22 | Share 20 | Read Later

Do you have an anti-virus app on your Android phone yet? If not, a new study conducted by security firm NQ Mobile suggests you're playing with fire: The number of malware threats to your Android phone has increased 163% over the past year alone.

The study, which looked at over 5.3 million apps available in 406 different online stores, identified 65,227 different pieces of potentially dangerous malware last year. A quick look at the trend suggests that malware is growing at an exponential rate – there were only 1,649 such malware discoveries in 2009.

In total, 32.8 million Android phones were infected with malware in 2012 – more than triple the number of the year before. The majority of these infections involve spyware or adware, while about a quarter are designed to steal and profit off of your personal data. A smaller minority is designed to make your phone permanently unusable, something we'd all no doubt like to

Email | Print | Share

Follow @techland

Our plan

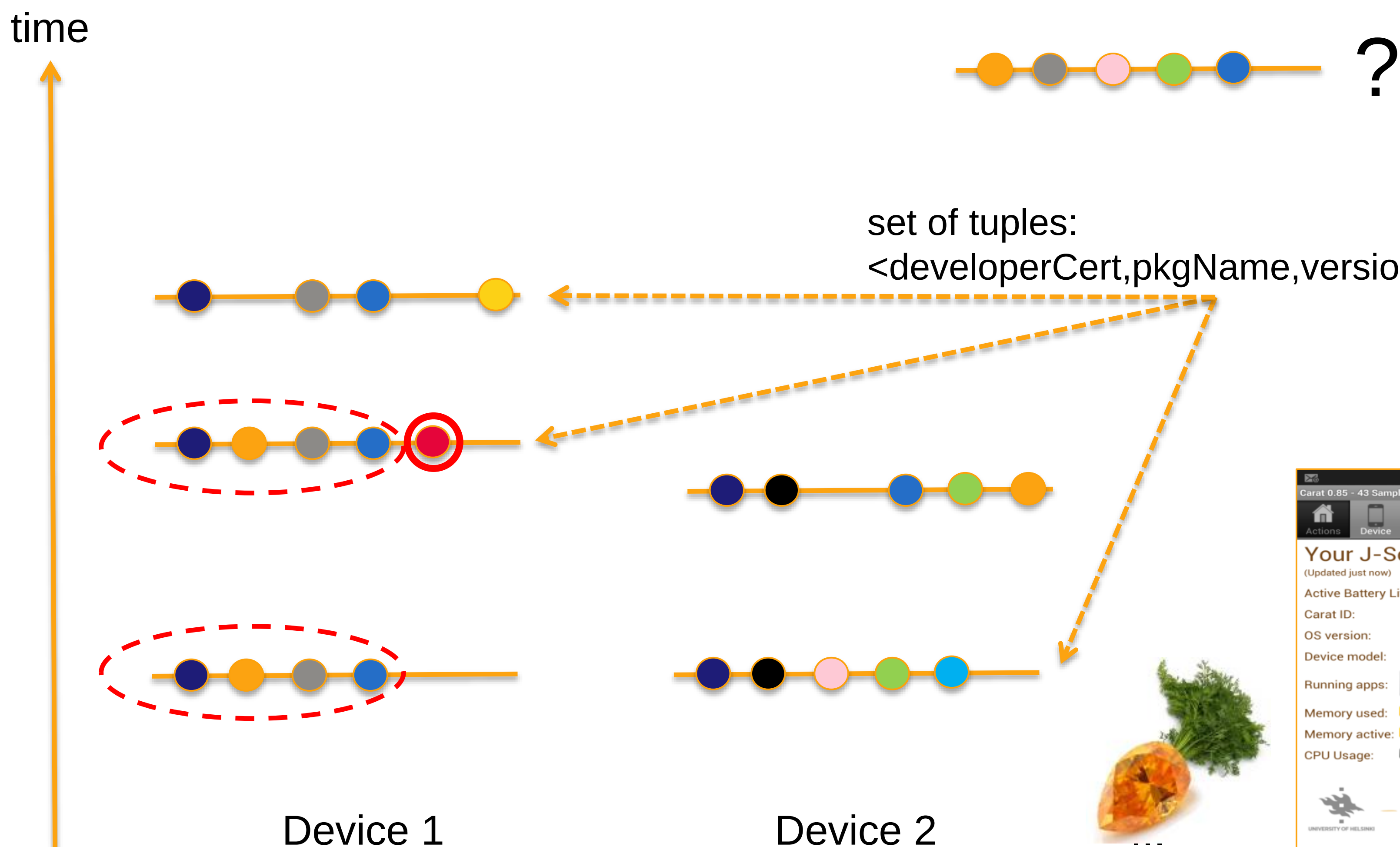
Get realistic **data** directly from devices

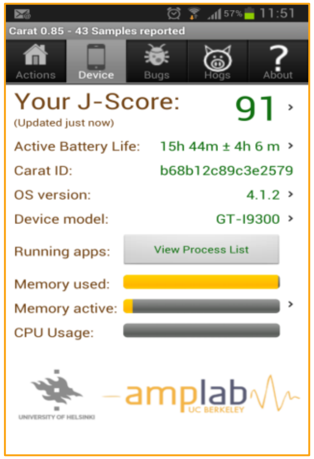
Estimate malware infection rate (for Android)

Identify **risk factors**

- See if we can predict likelihood of infection!

“The Company you Keep”





http://carat.cs.berkeley.edu

Incidence of infection

Type	Malware Genome	Mobile Sandbox	McAfee	Total
No. of dc matches (bad devcerts)	6	150	31	158
No. packages <dc,p,v> with bad devcerts	3,501	4,925	3,761	5,006
No. packages matching <dc,p,v>	0	30	4	32
No. infected devices (only dc match)	4,716 (15.3%)	7,424 (24.1%)	7,143 (23.2%)	7,843 (25.5%)
No. infected devices (<dc,p,v> match)	0 (0%)	40 (0.13%)	18 (0.06%)	56 (0.18%)

Data collected from 30 719 devices over 9 weeks

Classifying based on set of apps

Can the set of apps run on device predict infection?

Classification attempt using Naïve Bayes (5-fold CV)

	Infected (prediction)	Clean (prediction)
Infected (actual)	9	47
Clean (actual)	753	29910

Classifying based on set of apps

Recall (9/56) and precision (9/762) low?

- for classifying infected devices
- Lightweight instrumentation: at virtually no cost

***Supplementing* AV tools, not replacing them**

- Could serve as inexpensive early warning?
- Focus on a small subset for closer analysis
- Competition: baseline = 0.18%!

Predicting zero day malware

Multinomial Naïve Bayes

Malware divided into 4 groups

- 2 groups constitute “unknown malware” in each round(6 combinations)
- training set: 50% clean devices + devices infected by known malware (2 combinations)
- test set: 50% clean devices + devices infected by unknown malware

6 rounds, TP/FP ratio 5.0 times better than baseline

	Infected (prediction)	Clean (prediction)
Infected (actual)	32	304
Clean (actual)	3558	180420

Predicting previously unknown malware

Multinomial Naïve Bayes

Malware divided into 4 groups.

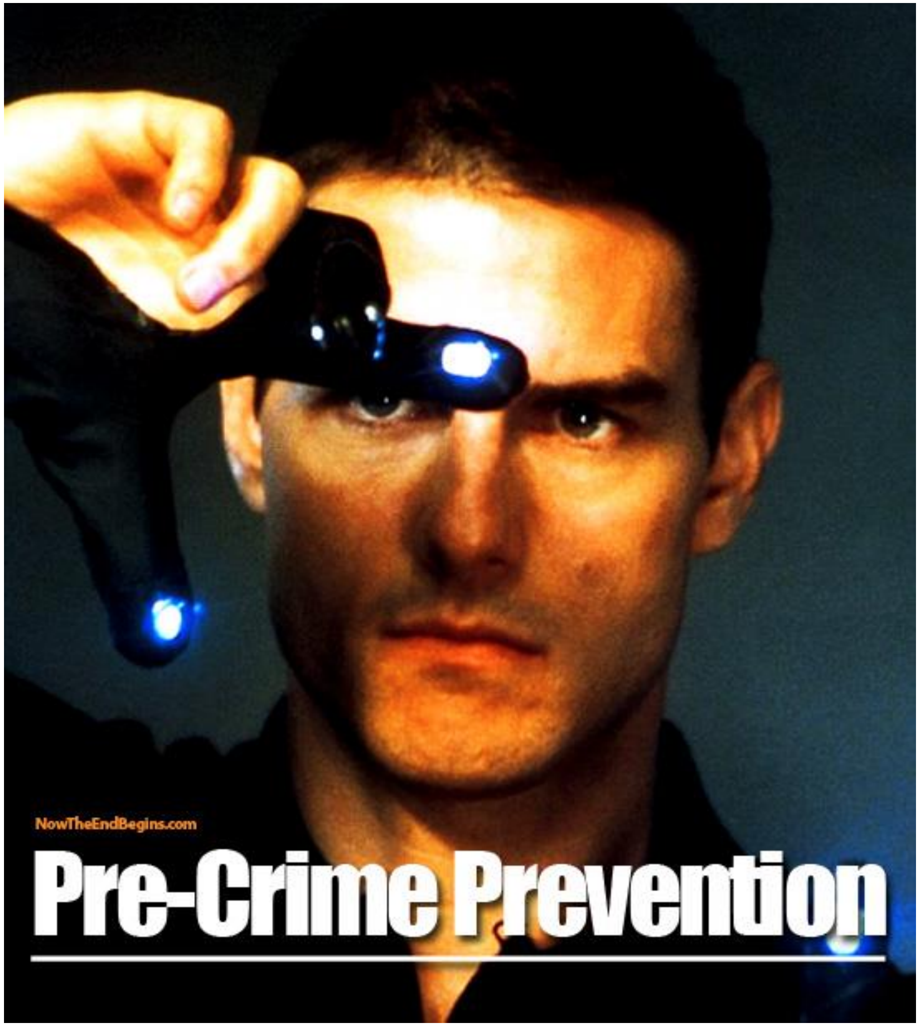
- 2 groups constitute “unknown malware” in each round(6 combinations)
- devices in training set (50% of all) containing unknown malware marked “clean” (2 combs.)
- devices in test set (50% of all) containing known malware removed before prediction

6 rounds, TP/FP ratio 2.4 times better than baseline

	Infected (prediction)	Clean (prediction)
Infected (actual)	12	156
Clean (actual)	2776	181202

Application: Help AV vendor searching for new malware

Identify vulnerable devices **before** they are infected?



Application: Help enterprise IT admin identify users for training

1. Secure Open Access to TEEs

Question: how to safely expose hardware-based *TEE functionality to app developers*?

Rationale:

- TEE hardware widespread; limited access to app developers
- Emerging standardization (Global Platform, TPM.2, TPM Mobile)

Use case: eg, Apps use TEE crypto for app-specific secure storage.

Stakeholder liaison: Brian McGillion (MCG)

Tanel Dettenhorn, Grad student

2. Novel Applications of Platsec

Question: can *existing platform security* mechanisms address security needs of *new usage scenarios*?

Rationale: Gap in platform security research and deployment.

Sub themes:

- how to securely migrate apps between devices using *existing lightweight isolation mechanisms*?
- can we aggregate feedback from social circles to *ease user burden of authorizing apps*?

Stakeholder liaison: Elena Reshetova (SSG/OTC)

3. Malware Insights

Question: can we use *lightweight instrumentation* on a device to predict if it will (eventually) get malware?

Rationale:

- signals indicative of user's habits (e.g., set of apps) may predict susceptibility to malware.

Use case: (1) cheaply identify suspicious apps for further analysis (2) corporate IT admin can monitor "health indicator" of BYO devices of employees

Stakeholder liaison: Igor Muttik (McAfee)

1) Hien Truong, Postdoc 2) Sourav Bhattacharya, PhD student

Summary

Intel Collaborative Research Institute for Secure Computing expands to Finland.

Theme of research: usable mobile security

Began operations in August:

1. Next generation hardware TEEs
2. Novel applications of platform security
3. Malware insights