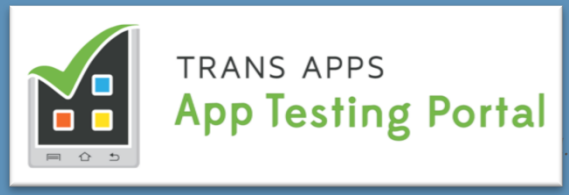
Multi-App Security Analysis

Looking for Android™ App Collusion

Rogan Creswick

creswick@galois.com

galois



Android™ Security

Engineering ease

- Documented APIs to read / modify private data
- Precedent for saying “ok” to application requests

Limited support for user control

- All-or-nothing approach to permissions

Run-time protections are often impractical

- Impacts battery life
- Degrades performance

DARPA Trans Apps

Afghanistan

- 3000 devices (at peak)

2013 Inauguration

- 100 devices
- DC National Guard
- National Park Service
- Arlington Country Fire
- DC Fire Department
- DC Police Department

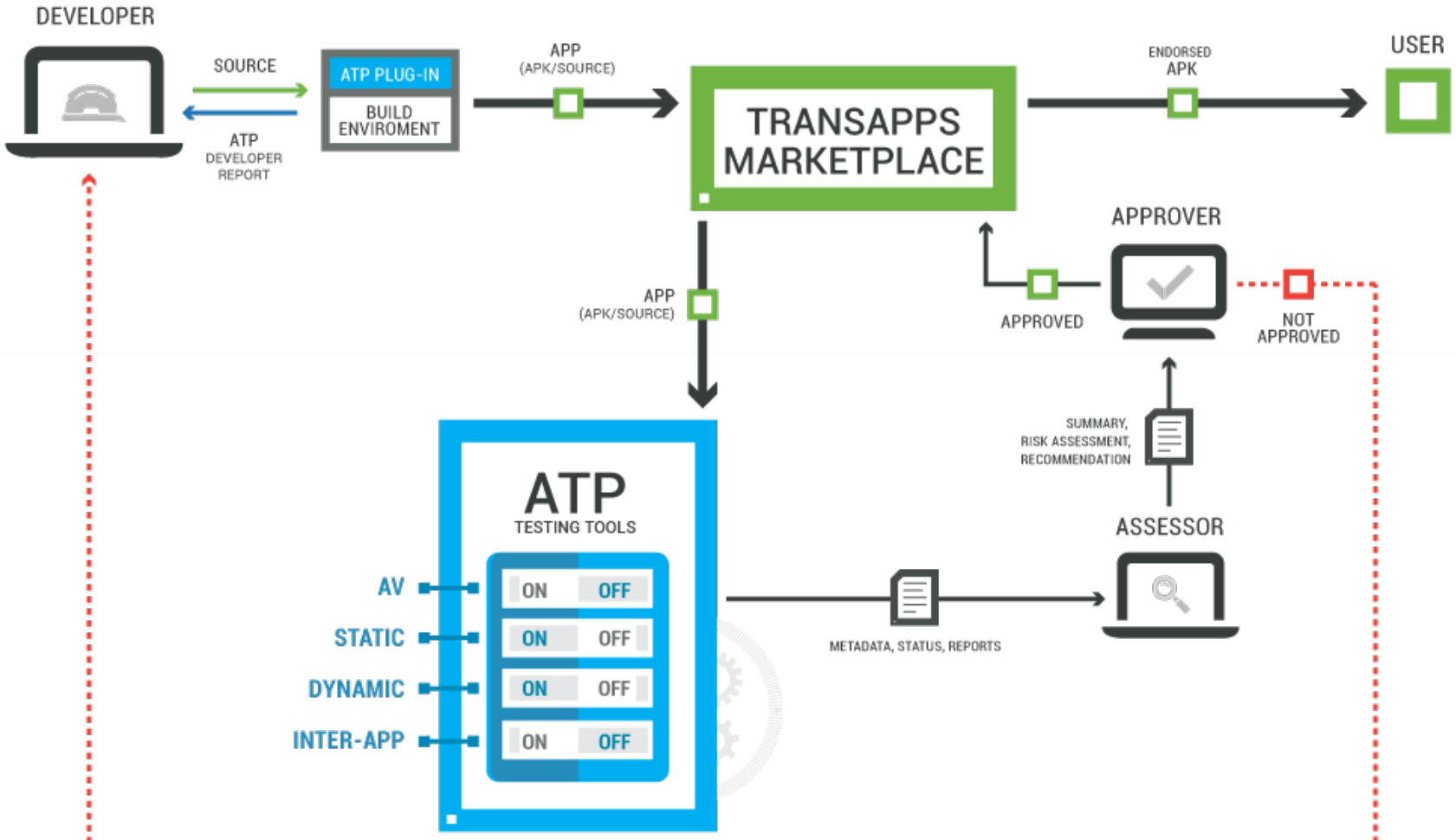
2014 Boston Marathon

- 60 devices
- Massachusetts National Guard Civil Support Team

galois

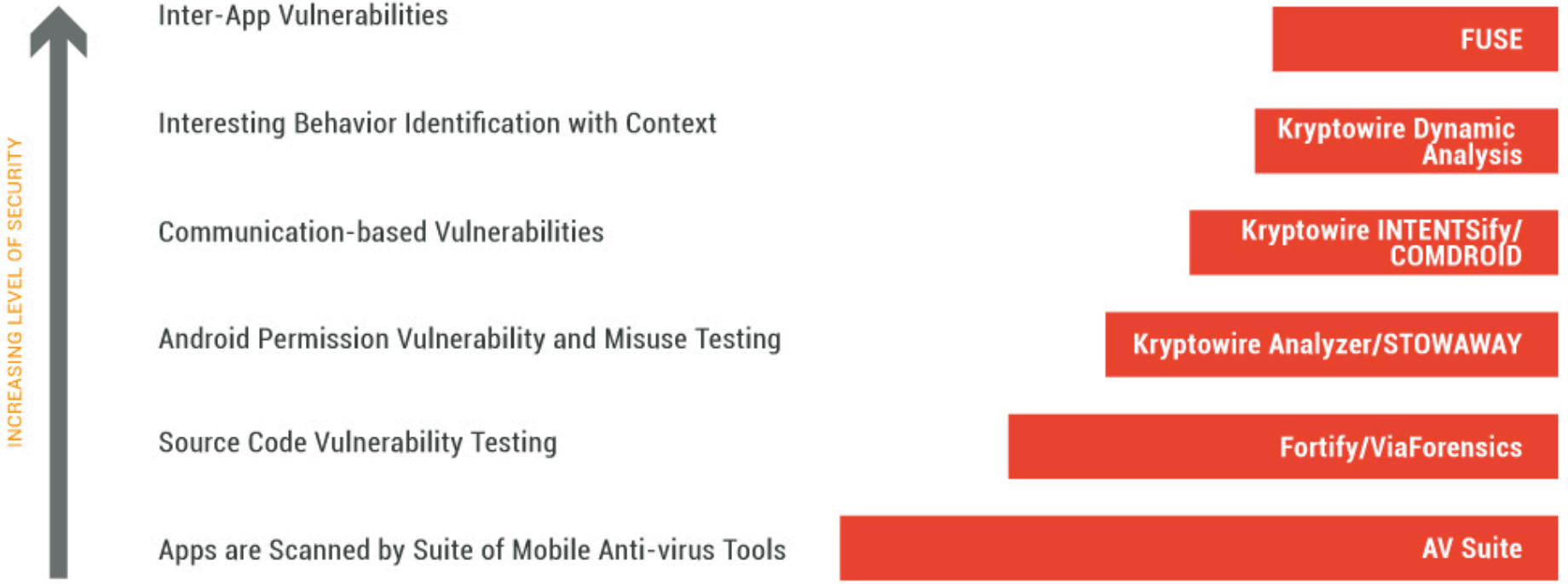
App Testing Portal Workflow

Seamless integration with TA Marketplace

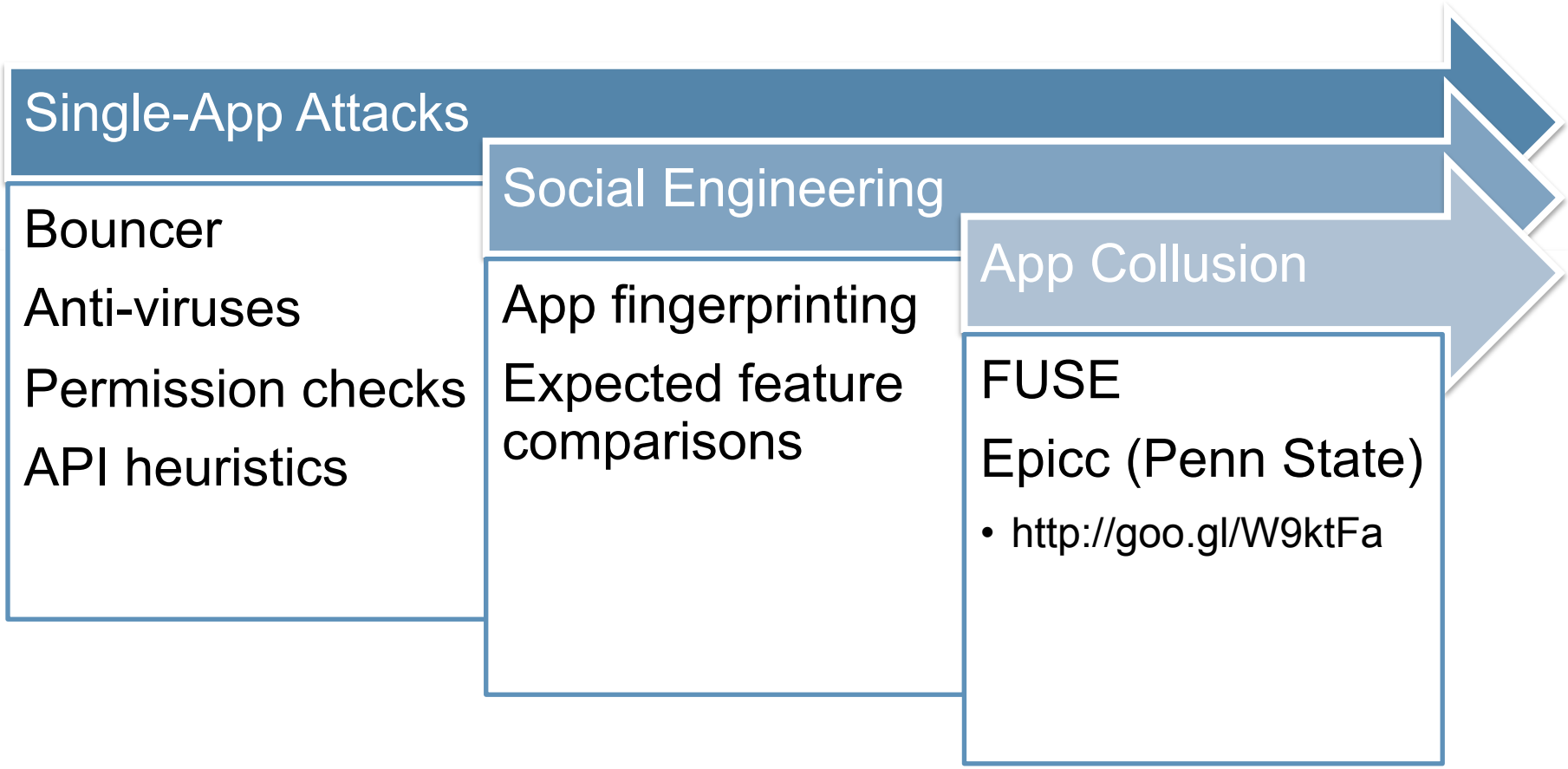


Multi-Dimensional App Security Testing

ATP combines multiple testing tools and approaches to address the broadest range of threats



Looking Forward: Multi-App Collusion



Real-World Examples

Malicious installation of packages

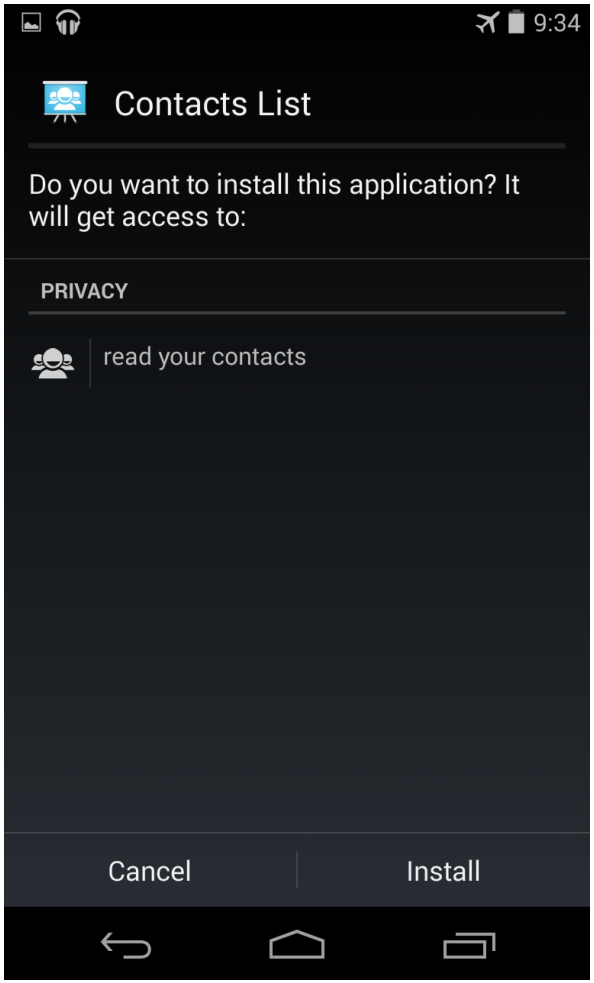
- Andre Moulu: http://goo.gl/Gpb8Jk
- Samsung Galaxy S3's packaged 'Kies.apk' exposed an API to install apps from external storage.
- 'ClipboardSaveService.apk' exposes an API to write to external storage.

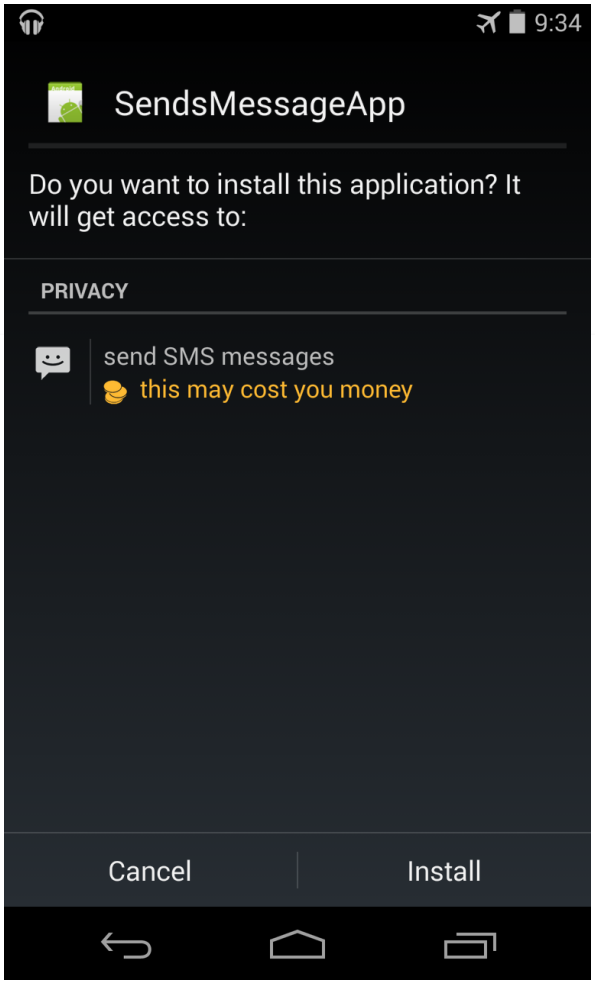
Inadvertent GPS sharing

- Image metadata contains more details than many people expect.
- Posting pictures likely shares your GPS coordinates with someone.

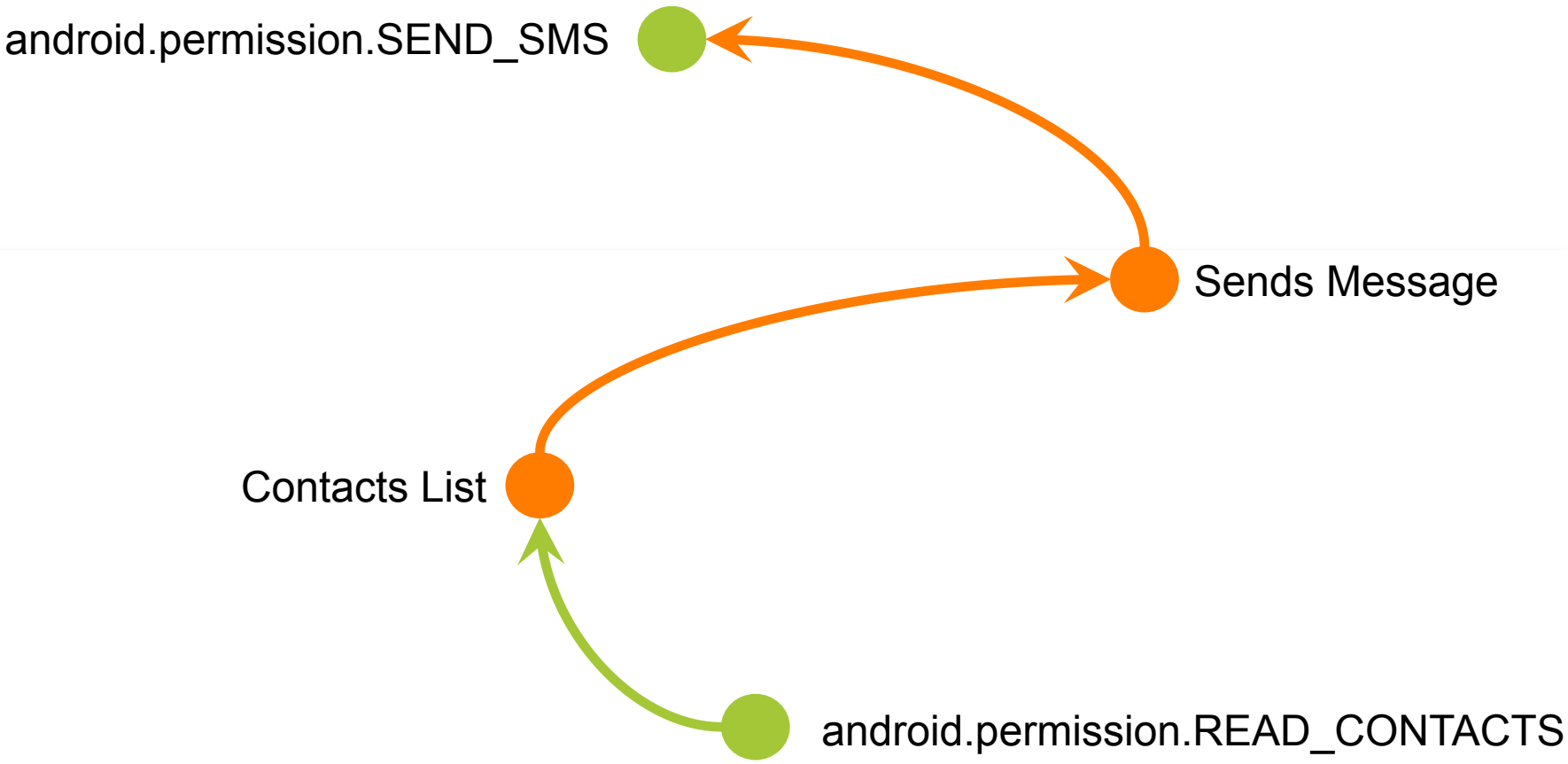
App Demonstration

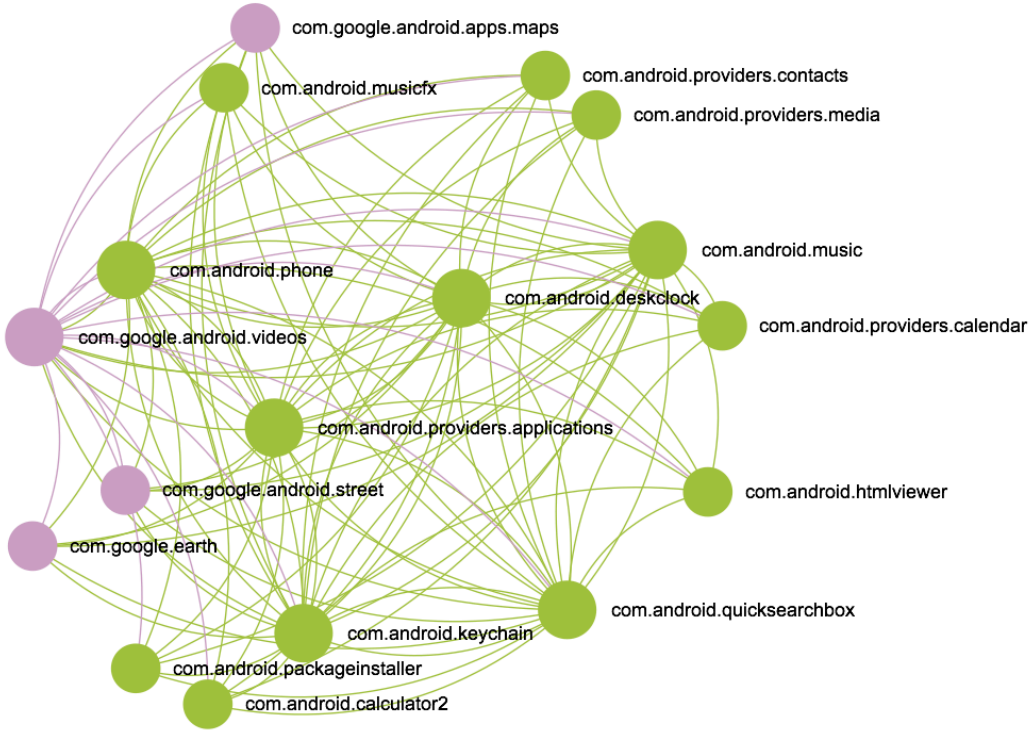
Approving some “benign” apps





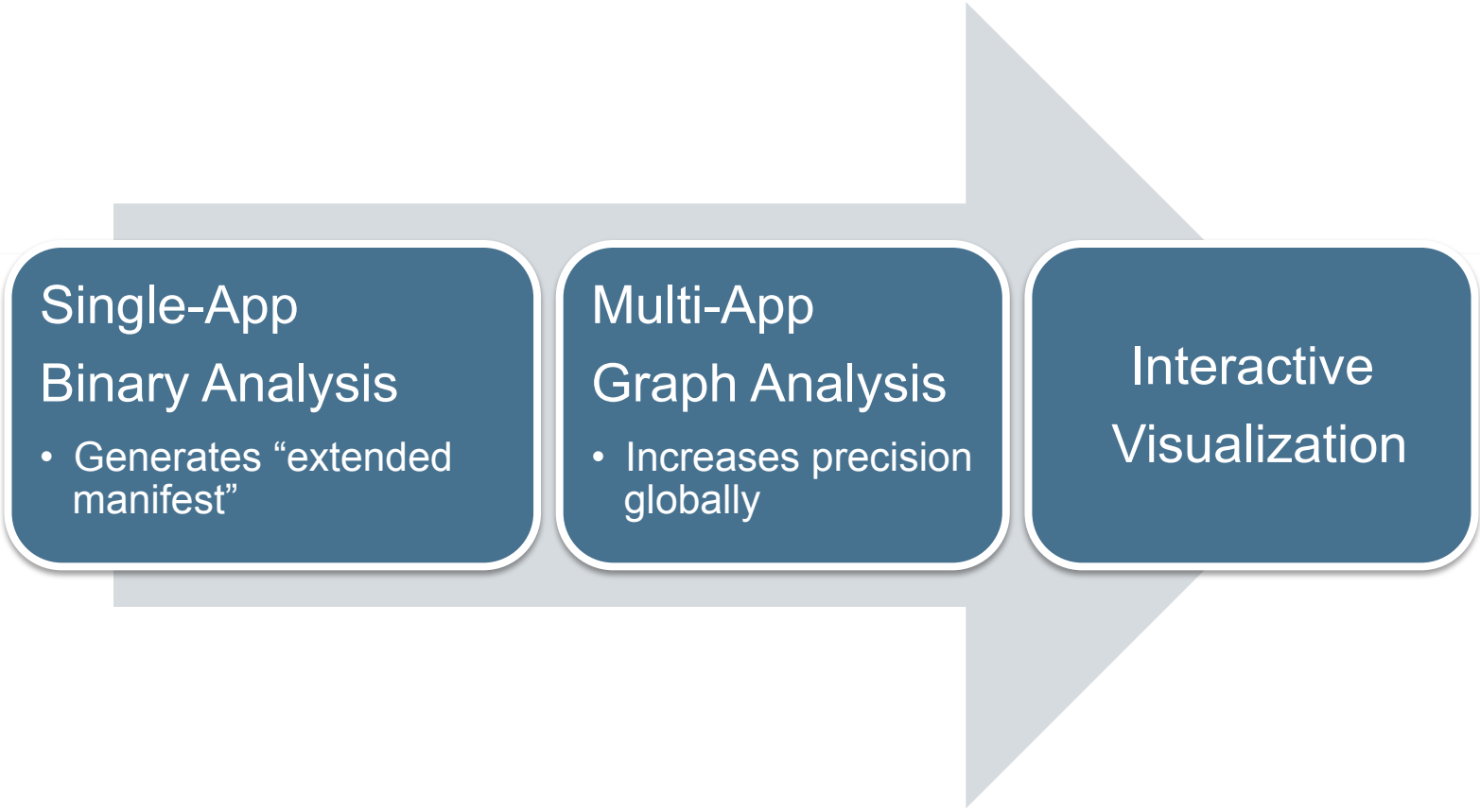
These apps collude to exfiltrate data





FUSE Demonstration

FUSE Architecture



Challenges

Performance	• Analysis time / app varies a lot • Soundness vs. precision
Covert Channels	• Vibration + Accelerometer • Off-device storage as side channel
Goals	• Improve precision / performance • Address native / non-Dalvik apps

Thank You!

Contact

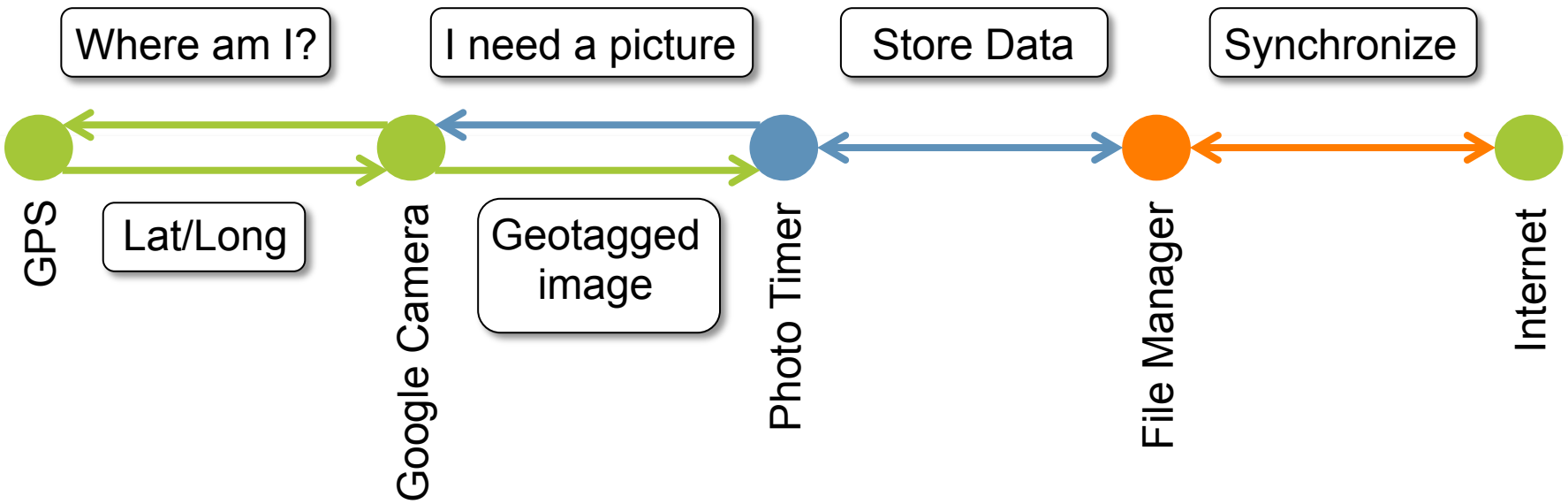
- FUSE:
  - Rogan Creswick:
  - creswick@galois.com
- ATP:
  - Melanie Matsuo:
  - melanie.matsuo.ctr@darpa.mil

Funded by DARPA

- A part of the DARPA Transformative Apps program:
  - http://goo.gl/5wTfUa

TRANS APPS
App Testing Portal

The Anatomy of a Colluding App



The File Manager now handles your precise location.

The Android™ Permission Model

Access to capabilities is controlled by *Permissions*

- Web activity: “INTERNET” Permission
- Installing software: “INSTALL_PACKAGES” Permission

Permissions fall into five protection levels

- Dangerous, Normal
- Signature, System, Signature Or System

The protection level is a *user interface* aspect

- Users *are not* prompted for confirmation of ‘normal’ permissions (only ‘dangerous’ permissions)

Android™ Security Advice

- Don't enable developer mode
- Don't enable sideloading
- Only use official channels
- Study the permissions
- Use protection software