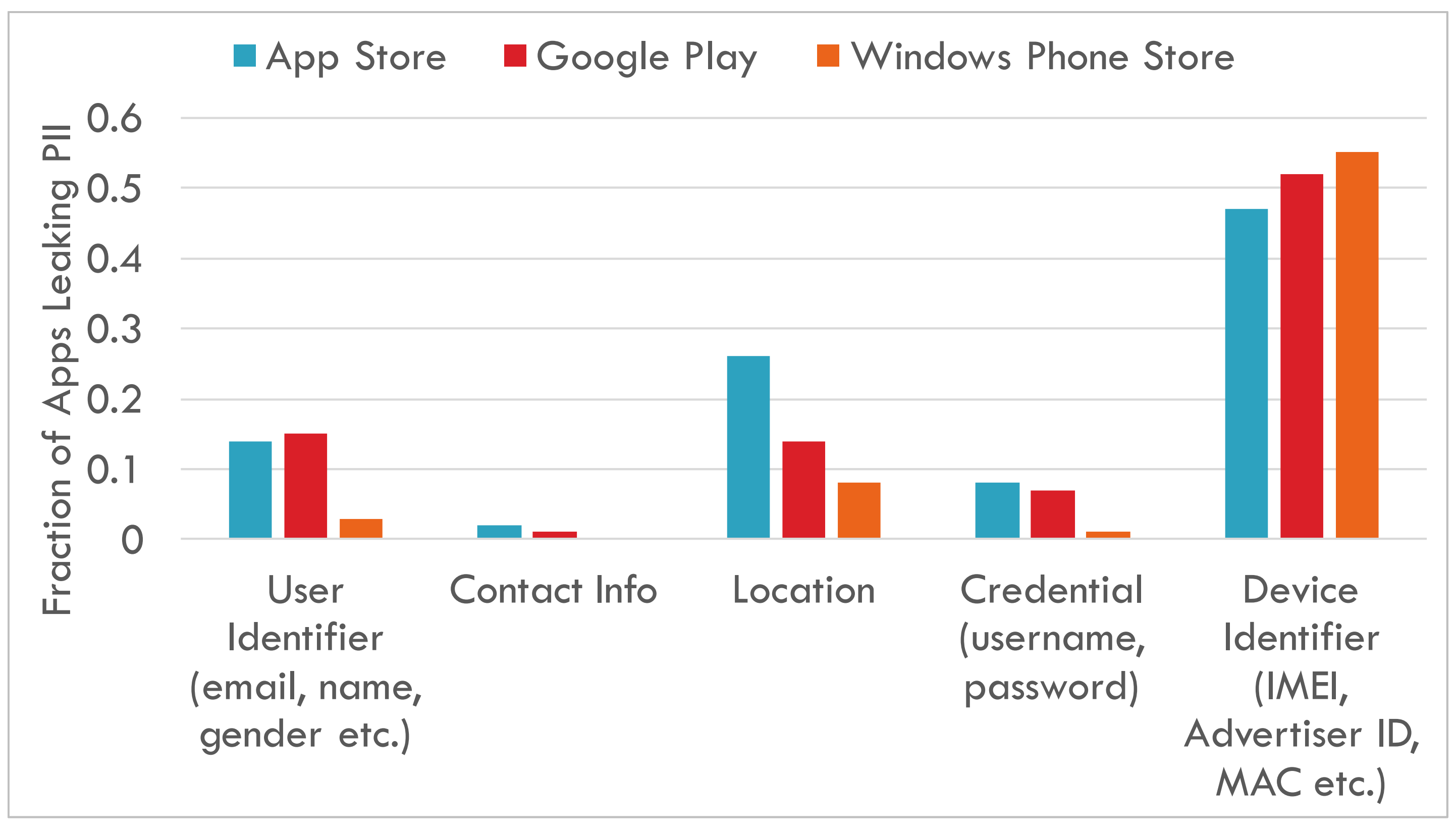
ReCon: Revealing and Controlling PII Leaks in Mobile Networks

Jingjing Ren, David Choffnes, Northeastern U, Ashwin Rao, U of Helsinki, Martina Lindorfer, SBA Research, Arnaud Legout, INRIA Sophia-Antipolis

MOTIVATION

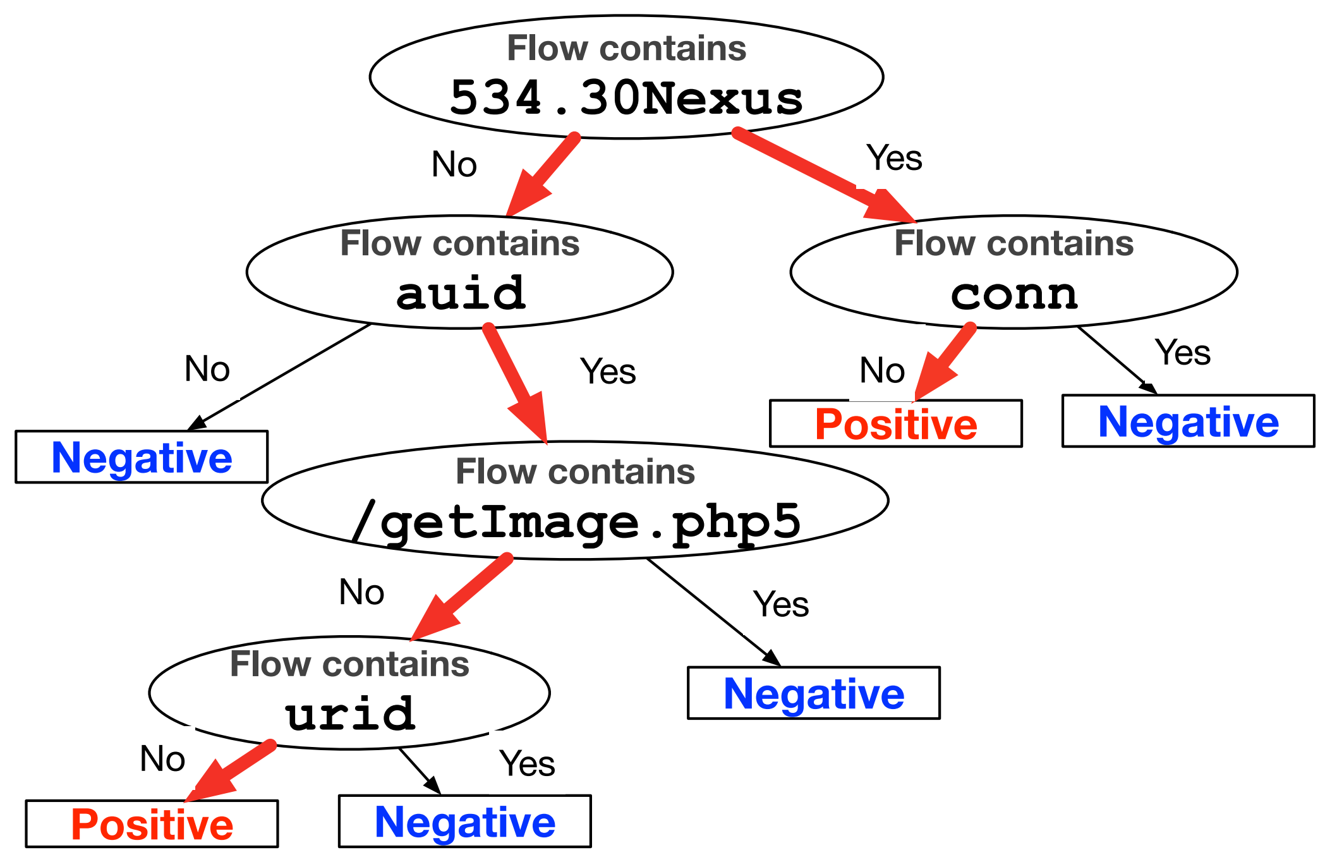
- Mobile devices: ubiquitous and connected to Internet
- Personally Identifiable Information (PII) leaks are pervasive

- **Key questions:**
  - What information is leaked?
  - How is it sent out?
  - Who receives this information?
  - What can users do to control it?



METHODOLOGY

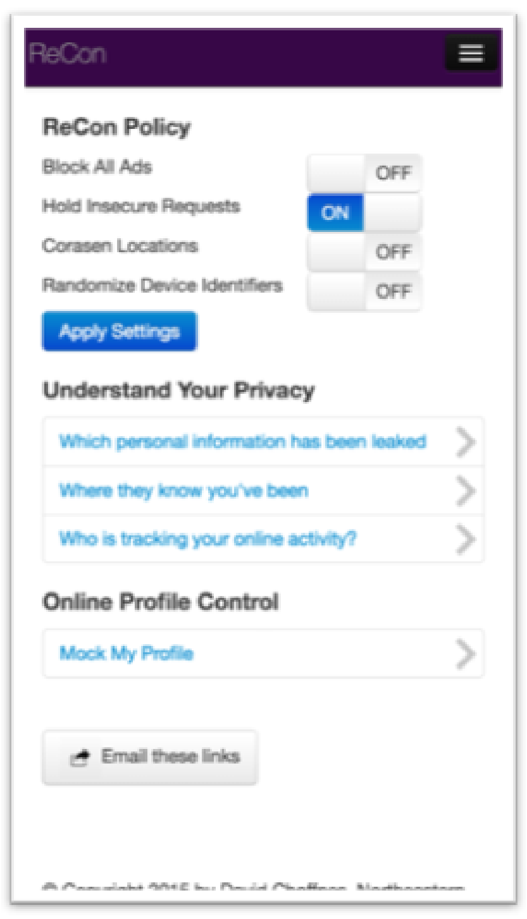
- How to detect PII leaks?
  At the OS, e.g. information flow analysis (IFA)
  - Doesn't cover everything, hard to scale
  Simpler approach: Focus on network traffic
  - Independent of OS, app store
- Our approach: Find PII in network traffic
  Machine Learning classifiers to detect leaks
  Software middleboxes to control leaks
  Works today on all major platforms



An example decision tree classifier

SYSTEM

- Detect PII Leaks
- Allow user feedback
- Block/modify PII
  - Coarsen locations
  - Anonymize



ReCon

ReCon Policy

Block All Ads: OFF
Hold Insecure Requests: ON
Corasen Locations: OFF
Randomize Device Identifiers: OFF

Apply Settings

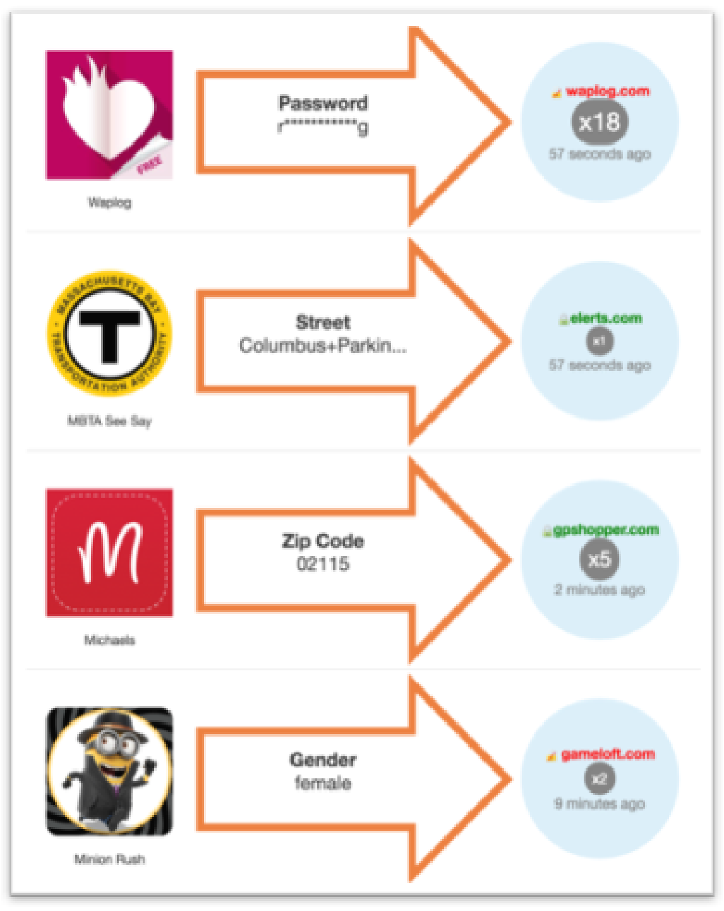
Understand Your Privacy

Which personal information has been leaked
Where they know you've been
Who is tracking your online activity?

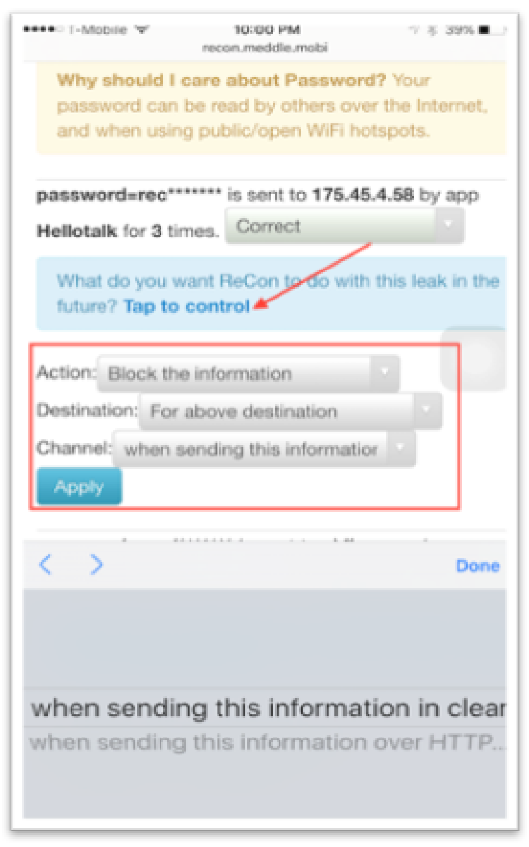
Online Profile Control

Mock My Profile

Email these links



Waplog — Password r***********g → waplog.com x18, 57 seconds ago
MBTA See Say — Street Columbus+Parkin... → elerts.com x1, 57 seconds ago
Michaels — Zip Code 02115 → gpshopper.com x5, 2 minutes ago
Minion Rush — Gender female → gameloft.com x2, 9 minutes ago



T-Mobile 10:00 PM 39%
recon.meddle.mobi

Why should I care about Password? Your password can be read by others over the Internet, and when using public/open WiFi hotspots.

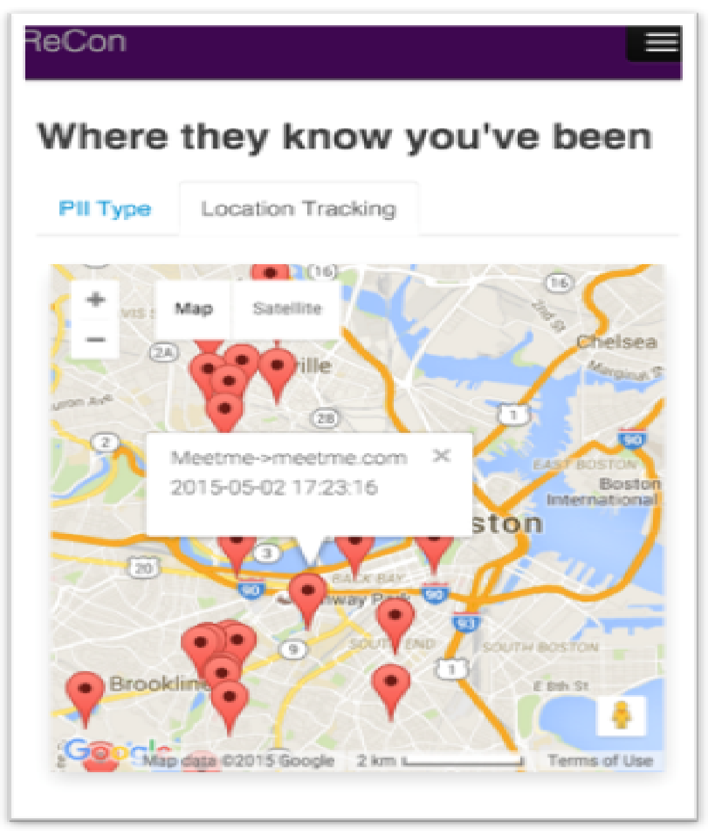
password=rec******* is sent to 175.45.4.58 by app Hellotalk for 3 times. Correct

What do you want ReCon to do with this leak in the future? Tap to control

Action: Block the information
Destination: For above destination
Channel: when sending this informatior
Apply

Done

when sending this information in clear
when sending this information over HTTP...



ReCon

Where they know you've been

PII Type | Location Tracking

Meetme->meetme.com
2015-05-02 17:23:16

USER STUDY

- IRB-approved
- 213 iOS, 225 Android (9/2017)
  - 30,289 PII leaks
  - 200 credential leaks, 168 verified

- Identified 30 apps exposing passwords in plaintext or sending to third parties
  - Used by millions (Pinterest, Grubhub, Match, Epocrates etc.)
  - Responsibly disclosed
  - 17 have fixed the problem

SUMMARY

Documentary film based on data from ReCon
http://www.harvest-documentary.com/

STAFF PICK
harvest
hotdocs 2017
Seattle International Film Festival 2017
BAM CINEMA FEST
OFFICIAL SELECTION ROOFTOP FILMS SUMMER SERIES
11:19
vimeo

- Need for improved transparency/control over PII
- ReCon approach addresses this
  - Learn what information is being leaked
  - Crowdsourcing to determine correctness/importance
  - Allow users to block/change what is leaked

https://recon.meddle.mobi

Sponsored by DATA TRANSPARENCY LAB   Homeland Security   Northeastern University *Cybersecurity and Privacy Institute*