CSE 484 / CSE M 584: Computer Security and Privacy

Web Privacy [finish]
Mobile Platform Security [start]

Spring 2017

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Admin

- **Today:** finish web privacy, start mobile security
- **Friday:**
  - Lab #2 due (8pm)
  - Guest lecture: Jon McClintock, Amazon Security
- **Monday:**
  - Guest lecture: David Aucsmith
  - Former senior director of Microsoft's Institute for Advannced Technology in Governments (among many other cool things)

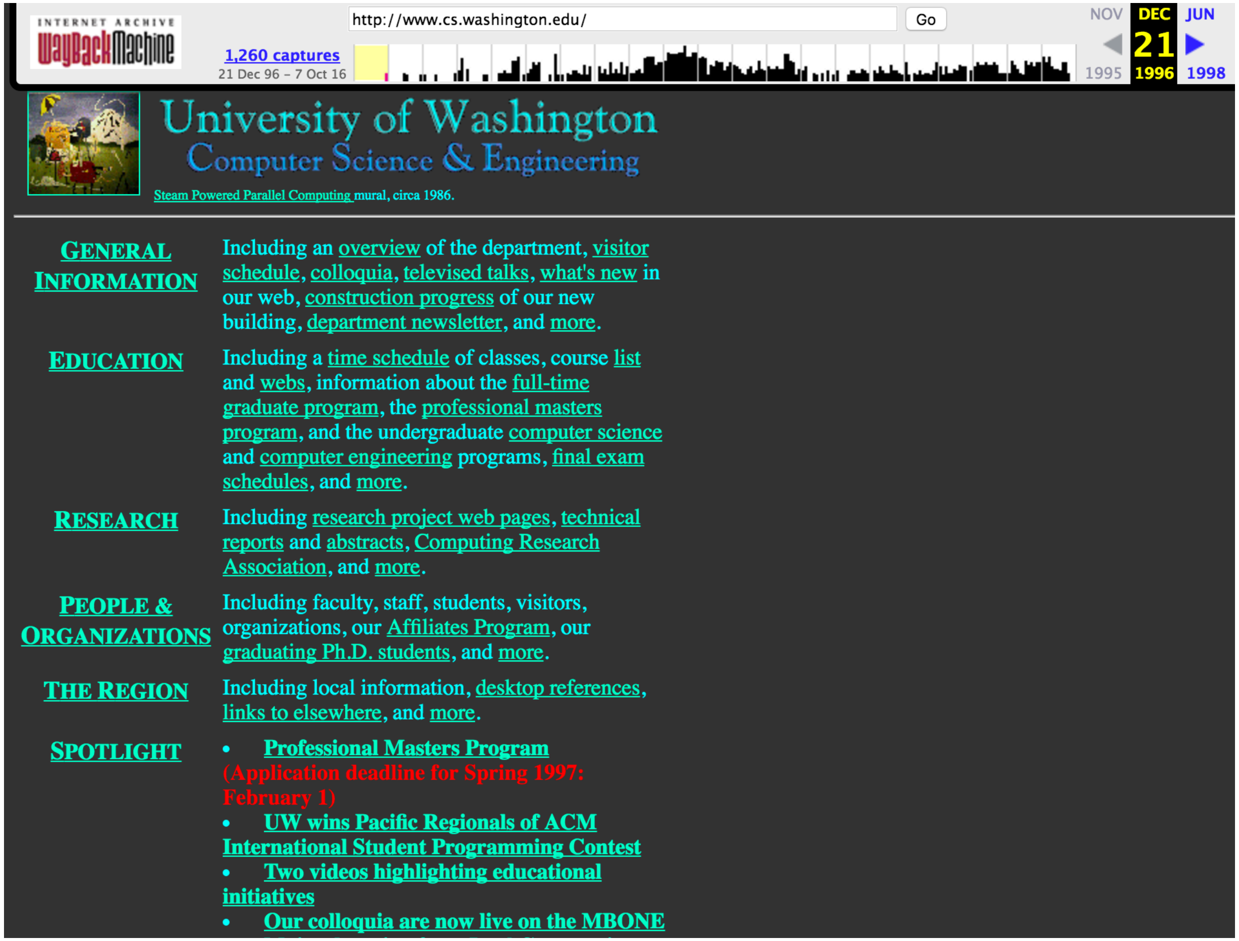
How has this changed over time?

- The web has existed for a while now…
  - What about tracking before 2011? (our first study)
  - What about tracking before 2009? (first academic study)

- Solution: time travel!

  [USENIX Security '16]

The Wayback Machine to the Rescue



University of Washington
Computer Science & Engineering

Steam Powered Parallel Computing mural, circa 1986.

GENERAL INFORMATION — Including an overview of the department, visitor schedule, colloquia, televised talks, what's new in our web, construction progress of our new building, department newsletter, and more.

EDUCATION — Including a time schedule of classes, course list and webs, information about the full-time graduate program, the professional masters program, and the undergraduate computer science and computer engineering programs, final exam schedules, and more.

RESEARCH — Including research project web pages, technical reports and abstracts, Computing Research Association, and more.

PEOPLE & ORGANIZATIONS — Including faculty, staff, students, visitors, organizations, our Affiliates Program, our graduating Ph.D. students, and more.

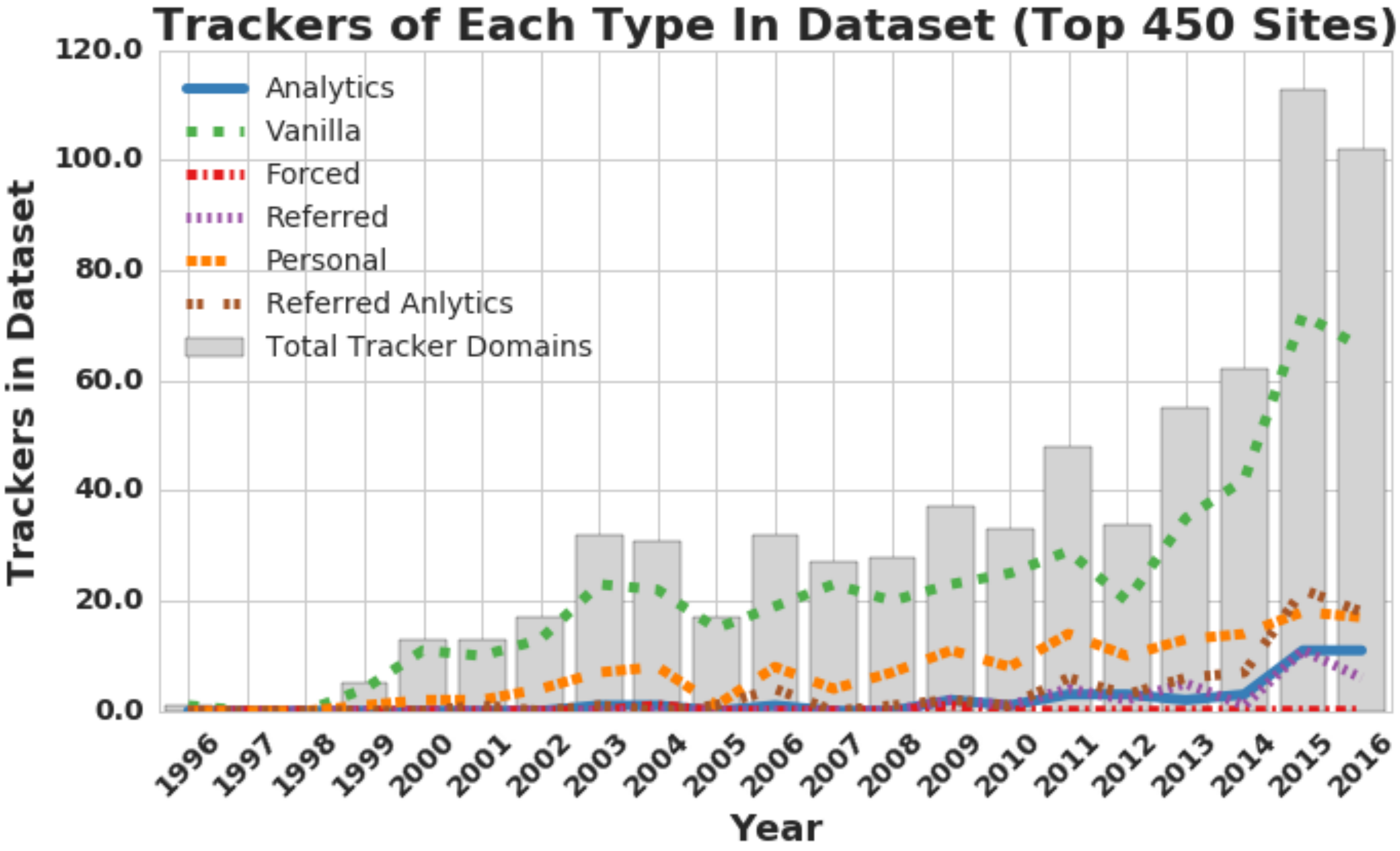
THE REGION — Including local information, desktop references, links to elsewhere, and more.

SPOTLIGHT
- Professional Masters Program (Application deadline for Spring 1997: February 1)
- UW wins Pacific Regionals of ACM International Student Programming Contest
- Two videos highlighting educational initiatives
- Our colloquia are now live on the MBONE

Time travel for web tracking: http://trackingexcavator.cs.washington.edu

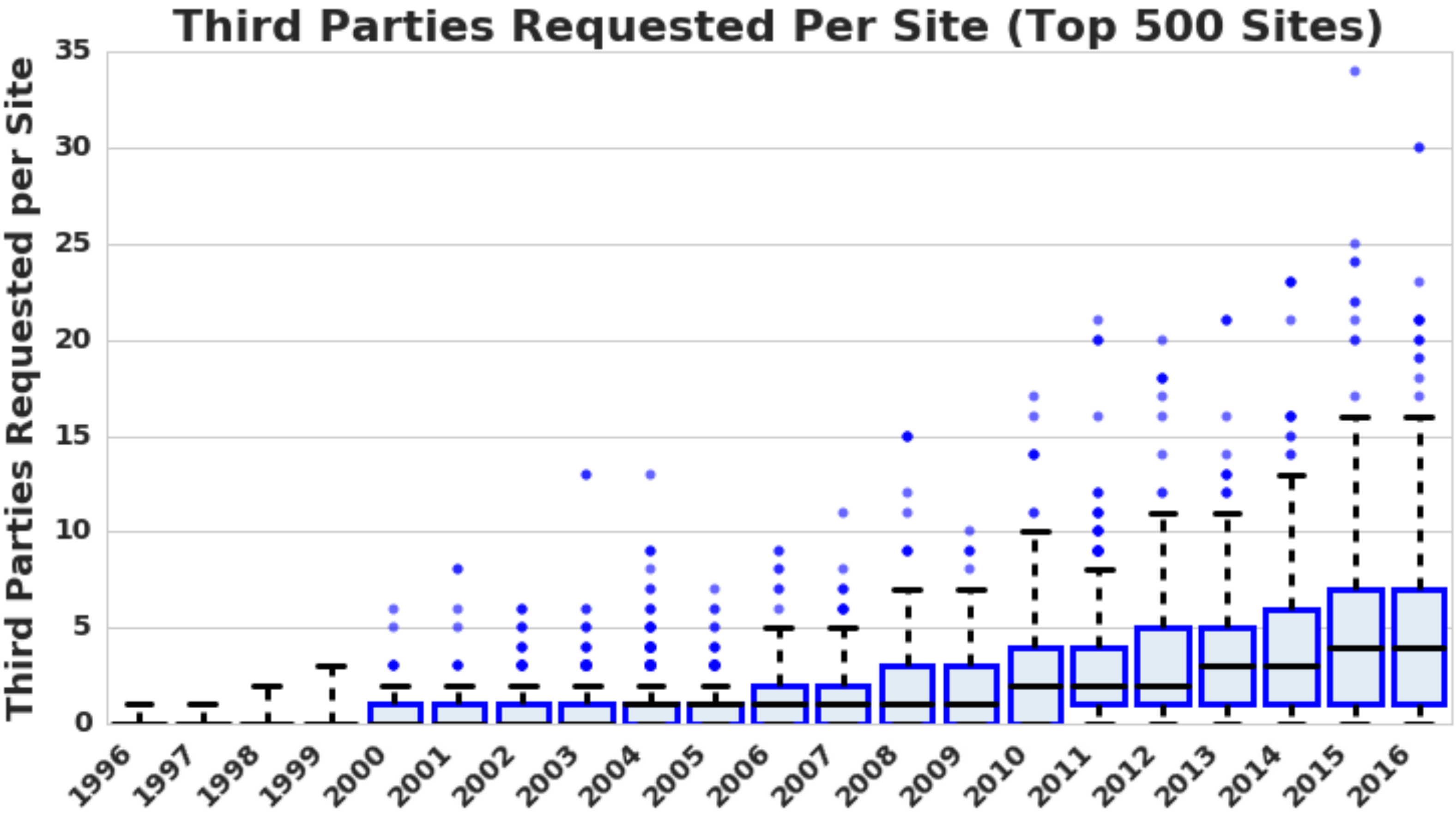
1996-2016: More & More Tracking

- More trackers of more types



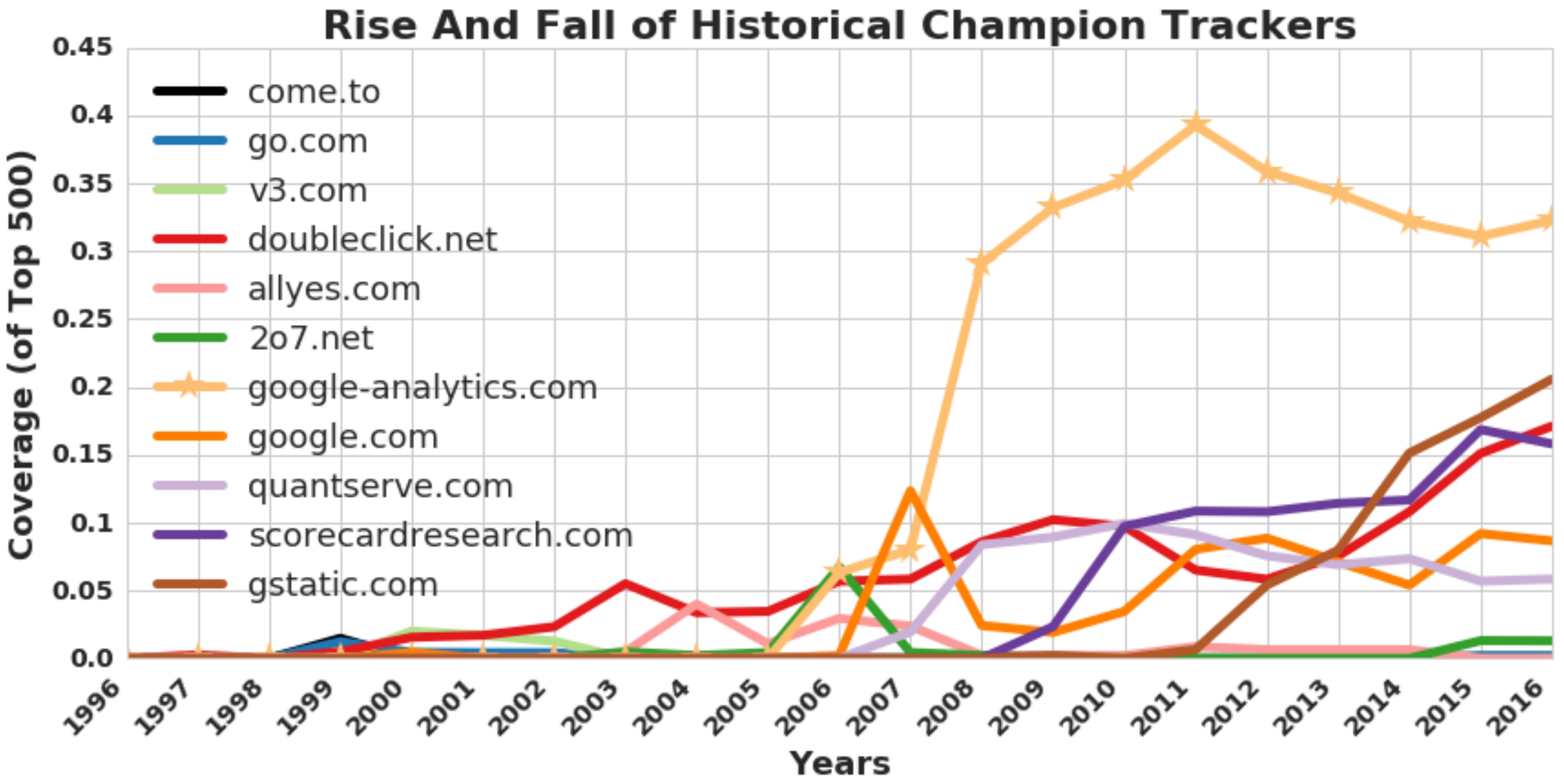
1996-2016: More & More Tracking

- More trackers of more types, more per site



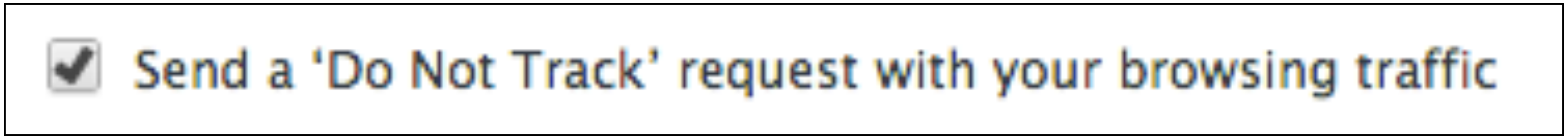
1996-2016: More & More Tracking

- More trackers of more types, more per site, more coverage



Defenses to Reduce Tracking

- Do Not Track proposal?



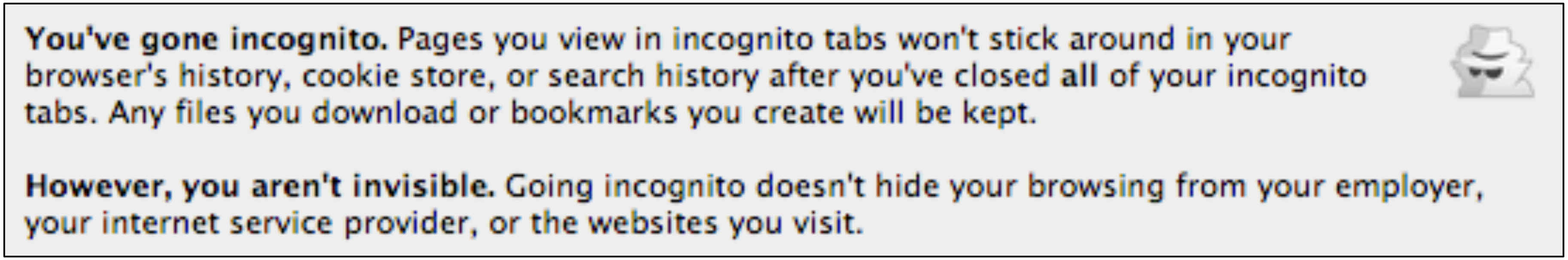
☑ Send a 'Do Not Track' request with your browsing traffic

Do Not Track is not a technical defense: trackers must honor the request.

Defenses to Reduce Tracking

- Do Not Track proposal?
- Private browsing mode?

Private browsing mode protects against local, not network, attackers.

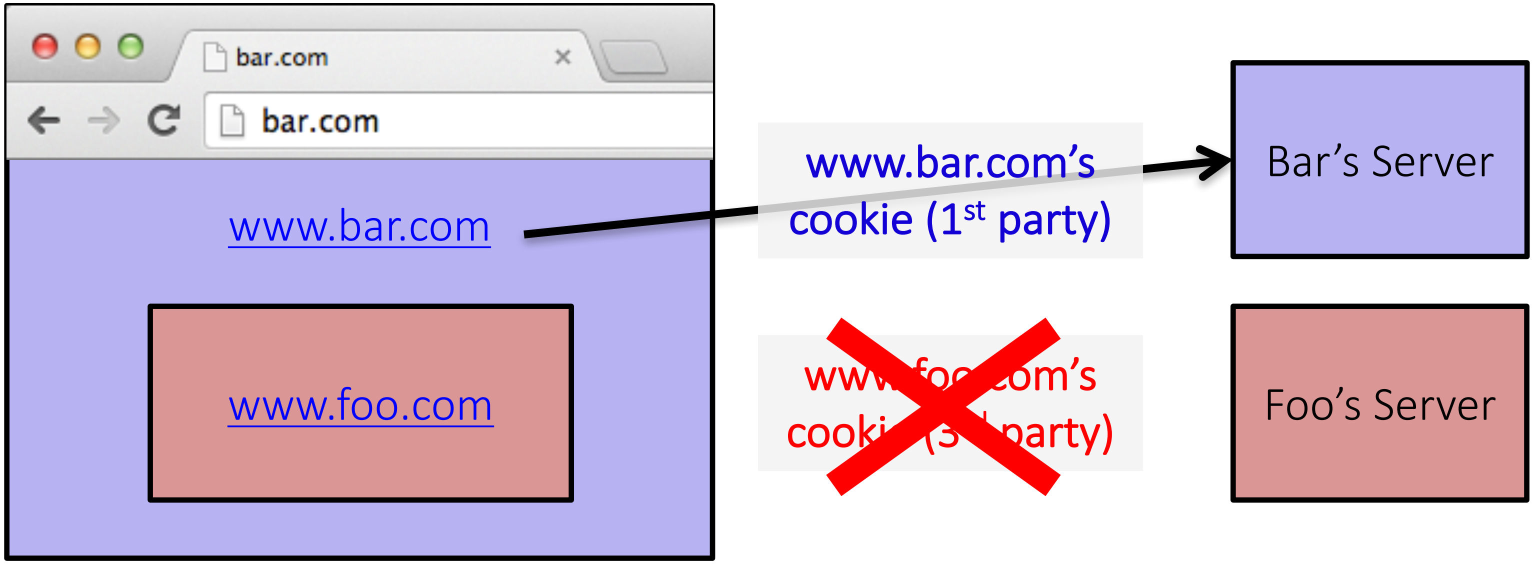


You've gone incognito. Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

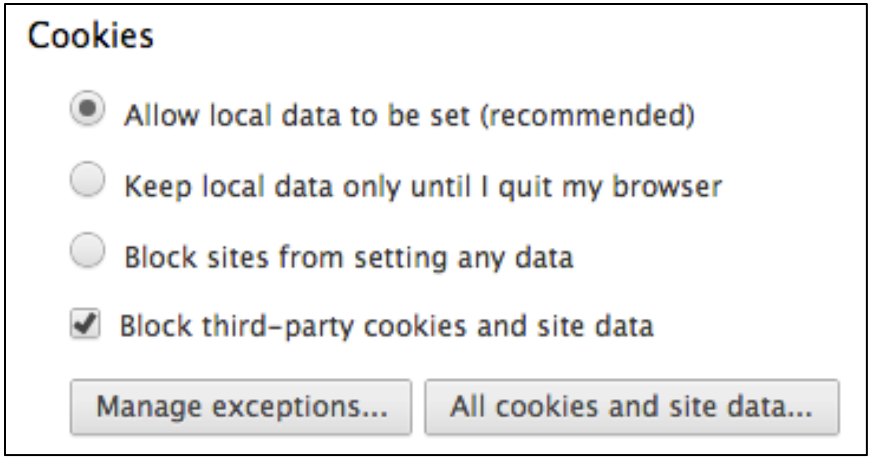
Defenses to Reduce Tracking

- Do Not Track proposal?
- Private browsing mode?
- Third-party cookie blocking?



bar.com
bar.com
www.bar.com
www.foo.com
www.bar.com's cookie (1st party)
~~www.foo.com's cookie (3rd party)~~
Bar's Server
Foo's Server

Quirks of 3rd Party Cookie Blocking



Cookies

● Allow local data to be set (recommended)

○ Keep local data only until I quit my browser

○ Block sites from setting any data

☑ Block third-party cookies and site data

In some browsers, this option means third-party cookies cannot be set, but they CAN be sent.

So if a third-party cookie is somehow set, it can be used.

How to get a cookie set?

One way: be a first party.

Facebook Google Twitter etc.

Defenses to Reduce Tracking

- Do Not Track header?
- Private browsing mode?
- Third-party cookie blocking?
- Browser add-ons?

"uses algorithmic methods to decide what is and isn't tracking"; incorporates code from UW for handling social media buttons

Often rely on blacklists, which may be incomplete.

MOBILE PLATFORM SECURITY

Roadmap

- Mobile malware
- Mobile platforms vs. traditional platforms
- Deep dive into Android
  - – Continued next Wednesday
  - – Background for Lab #3

Questions: Mobile Malware

Q1: How might malware authors get malware onto phones?

Q2: What are some goals that mobile device malware authors might have?

Q3: What technical things might malware authors do?

Smartphone (In)Security

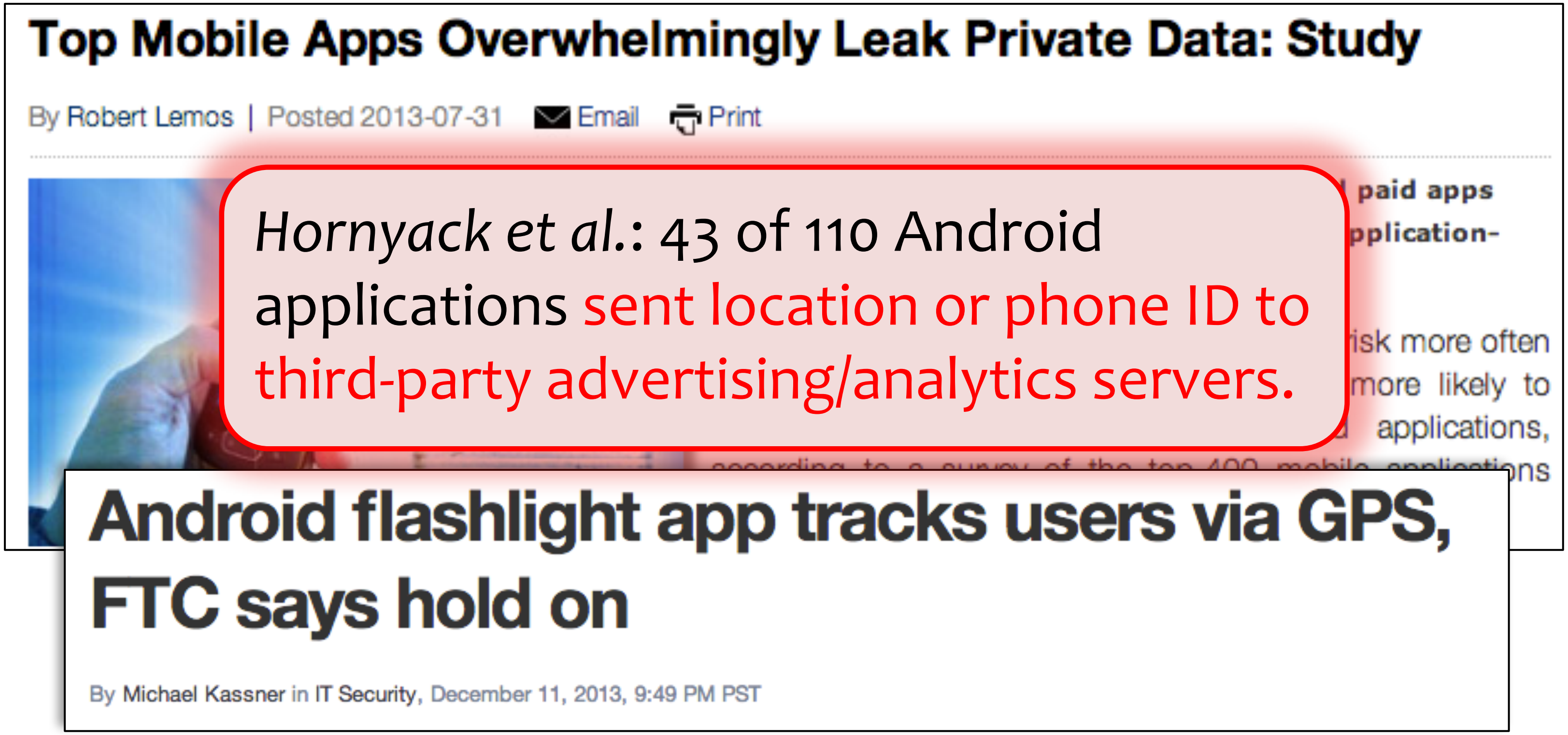
Users accidentally install malicious applications.

Over 60% of Android malware steals your money via premium SMS, hides in fake forms of popular apps

By Emil Protalinski, Friday, 5 Oct '12 , 05:50pm

Smartphone (In)Security

Even legitimate applications exhibit questionable behavior.



Top Mobile Apps Overwhelmingly Leak Private Data: Study

By Robert Lemos | Posted 2013-07-31 Email Print

paid apps
pplication-

isk more often
more likely to
applications,
according to a survey of the top 400 mobile applications

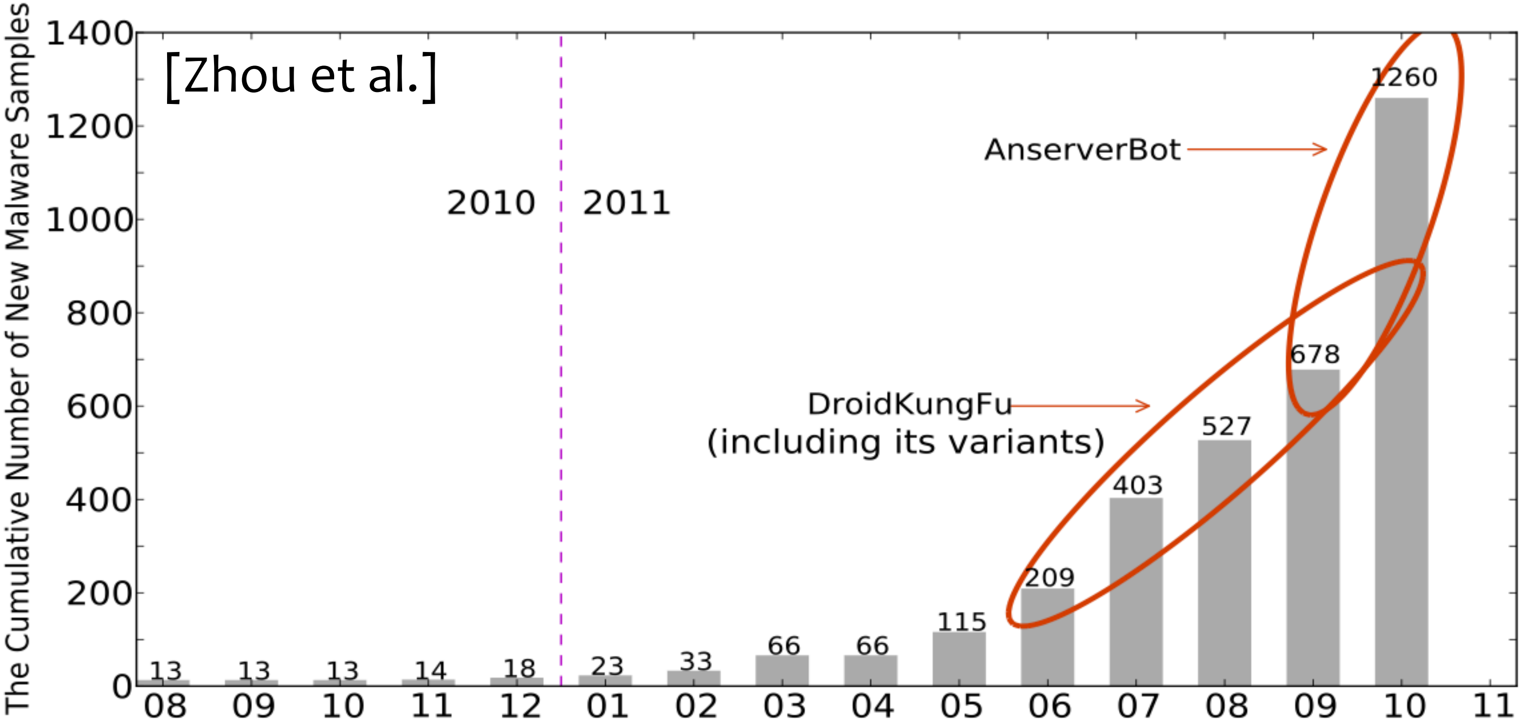
Hornyack et al.: 43 of 110 Android applications sent location or phone ID to third-party advertising/analytics servers.

Android flashlight app tracks users via GPS, FTC says hold on

By Michael Kassner in IT Security, December 11, 2013, 9:49 PM PST

Malware in the Wild

Android malware is growing.
Today (2016): millions of samples.



Mobile Malware Attack Vectors

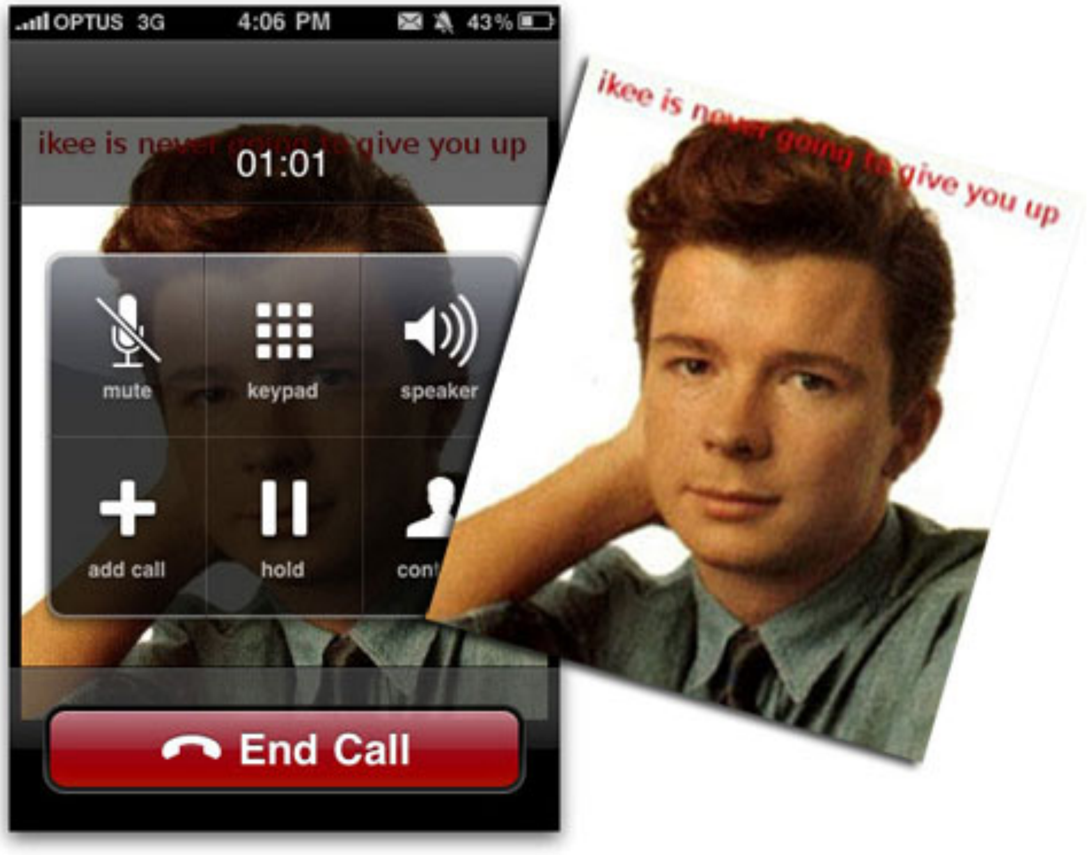
- Unique to phones:
  - Premium SMS messages
  - Identify location
  - Record phone calls
  - Log SMS
- Similar to desktop/PCs:
  - Connects to botmasters
  - Steal data
  - Phishing
  - Malvertising

Mobile Malware Examples

- **DroidDream** (Android)
  - Over 58 apps uploaded to Google app market
  - Conducts data theft; send credentials to attackers
- **Zitmo** (Symbian,BlackBerry,Windows,Android)
  - Poses as mobile banking application
  - Captures info from SMS – steal banking 2nd factors
  - Works with Zeus botnet
- **Ikee** (iOS)
  - Worm capabilities (targeted default ssh password)
  - Worked only on jailbroken phones with ssh installed

Mobile Malware Examples

"ikee is never going to give you up"


OPTUS 3G
4:06 PM
43%
ikee is never going to give you up
01:01
mute
keypad
speaker
add call
hold
cont
End Call
ikee is never going to give you up

[Zhou et al.]

(Android) Malware in the Wild

What does it do?

	Root Exploit	Remote Control		Financial Charges			Information Stealing		
		Net	SMS	Phone Call	SMS	Block SMS	SMS	Phone #	User Account
# Families	20	27	1	4	28	17	13	15	3
# Samples	1204	1171	1	256	571	315	138	563	43

Why all these problems with mobile malware?

Background: Before Mobile Platforms

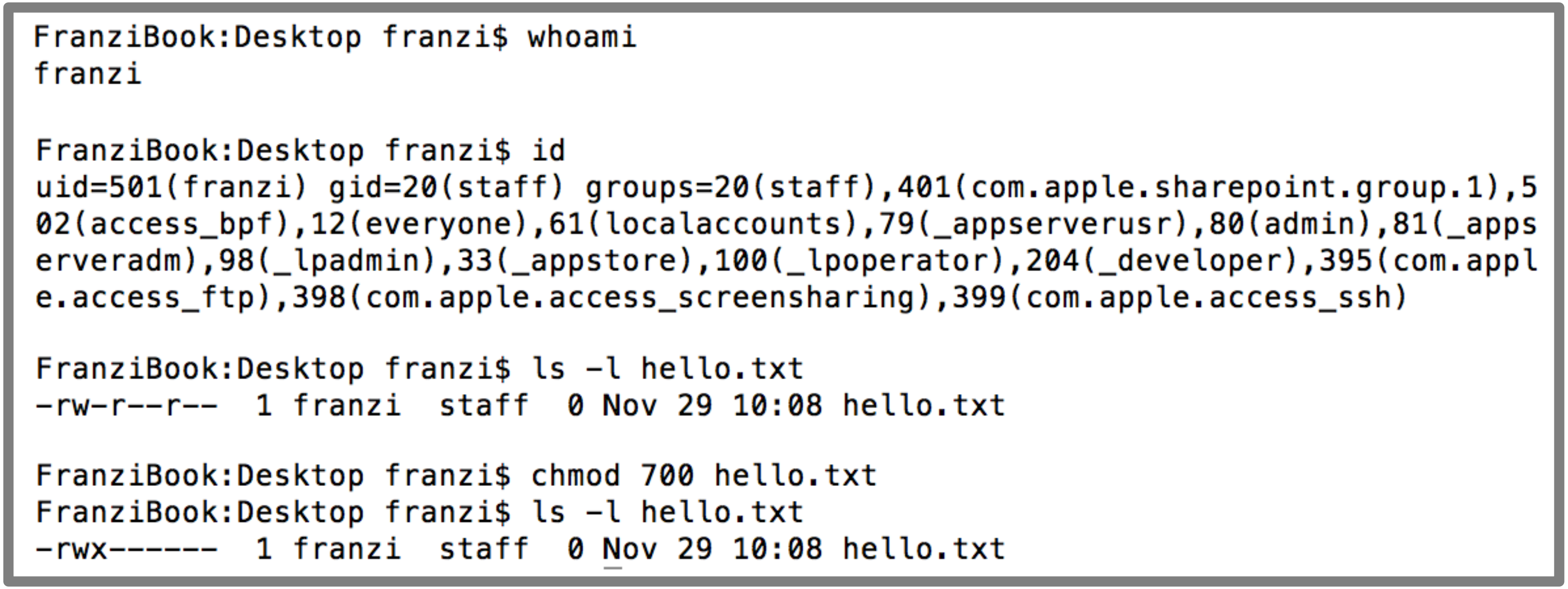
Assumptions in traditional OS (e.g., Linux) design:

1. There may be multiple users who don’t trust each other.
2. Once an application is installed, it’s (more or less) trusted.

Background: Before Mobile Platforms

Assumptions in traditional OS (e.g., Linux) design:

1. **There may be multiple users who don’t trust each other.**
2. Once an application is installed, it’s (more or less) trusted.



```
FranziBook:Desktop franzi$ whoami
franzi

FranziBook:Desktop franzi$ id
uid=501(franzi) gid=20(staff) groups=20(staff),401(com.apple.sharepoint.group.1),5
02(access_bpf),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_apps
erveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),395(com.appl
e.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh)

FranziBook:Desktop franzi$ ls -l hello.txt
-rw-r--r--  1 franzi  staff  0 Nov 29 10:08 hello.txt

FranziBook:Desktop franzi$ chmod 700 hello.txt
FranziBook:Desktop franzi$ ls -l hello.txt
-rwx------  1 franzi  staff  0 Nov 29 10:08 hello.txt
```

Background: Before Mobile Platforms

Assumptions in traditional OS (e.g., Linux) design:

1. There may be multiple users who don't trust each other.
2. **Once an application is installed, it's (more or less) trusted.**

Apps can do anything the UID they're running under can do.

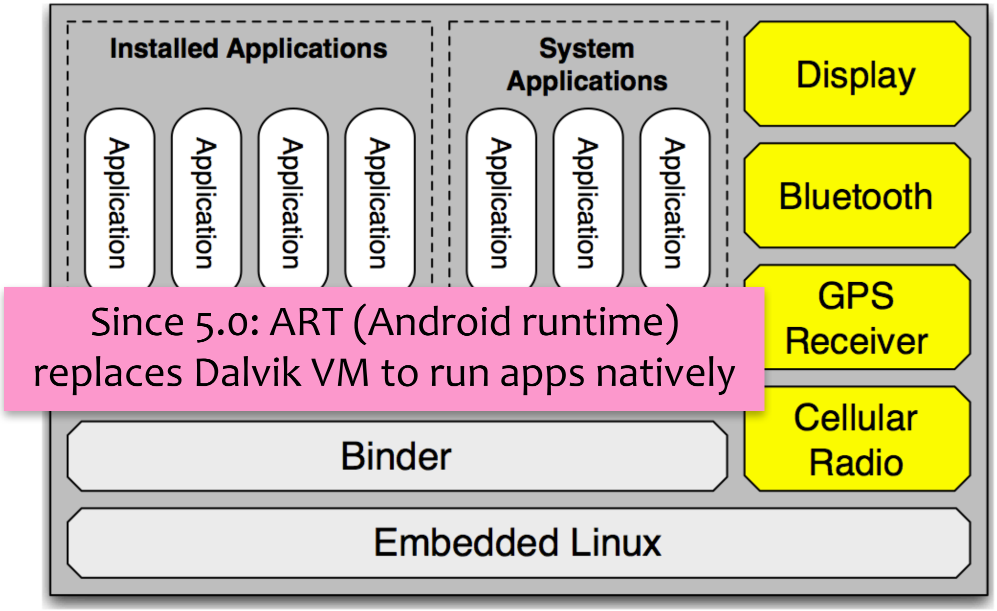
What’s Different about Mobile Platforms?

- Applications are isolated
  - Each runs in a separate execution context
  - No default access to file system, devices, etc.
  - **Different than traditional OSes** where multiple applications run with the same user permissions!

- **App Store:** approval process for applications
  - Market: Vendor controlled/Open
  - App signing: Vendor-issued/self-signed
  - User approval of permissions

More Details: Android

[Enck et al.]



Since 5.0: ART (Android runtime) replaces Dalvik VM to run apps natively

- Based on Linux
- Application sandboxes
  - Applications run as separate UIDs, in separate processes.
  - Memory corruption errors only lead to arbitrary code execution in the context of the **particular** application, not complete system compromise!
  - (Can still escape sandbox – but must compromise Linux kernel to do so.) ← allows rooting

Android Applications

- Activities provide user interfaces.
- Services run in the background.
- BroadcastReceivers receive messages sent to multiple applications (e.g., BOOT_COMPLETED).
- ContentProviders are databases addressable by their application-defined URIs.

- AndroidManifest.xml
  - Specifies application components
  - Specifies required permissions

Rooting and Jailbreaking

- Allows user to run applications with root privileges
  - e.g., modify/delete system files, app management, CPU management, network management, etc.
- Done by exploiting vulnerability in firmware to install `su` binary.
- Double-edged sword…
- Note: iOS is more restrictive than Android
  - Doesn't allow "side-loading" apps, etc.