Mobile Security
Fall 2015

Patrick Tague

#13 – Mobile Ad Vulnerabilities

Reminder

- Assignment #4 is due today

Class #13

- Brief discussion of ad service vulnerabilities
- Needs for new ad permissions?
- Brief discussion of next project deliverables

Ad Services

- App developers have two primary ways of making money:
  - Charging users for apps directly
  - Getting $$$ from advertisers to include ads in apps

AdMob

- AdMob was founded in 2006 as a multi-platform advertising company, specializing in targeted advertising for many mobile platforms
  - Acquired by Google in 2009 for $750m
  - One of the most used mobile advertising services

- Google claims significant effort goes into monitoring ads, banning bad advertisers, etc.
  - *http://googleblog.blogspot.com/2012/03/making-our-ads-better-for-everyone.html*

Not-so-Nice Ad Services

- Unfortunately, not all ad services are as well regulated as Google's AdMob service
- Some ad libraries used by mobile apps require permissions that would allow them to:
  - Access location data, camera, account details, calendar, call logs, browser bookmarks, contact lists, phone information, phone number, SMS messages
  - Make phone calls, send SMS messages, vibrate
  - Change calendar and contacts

Case Study: Android Ads

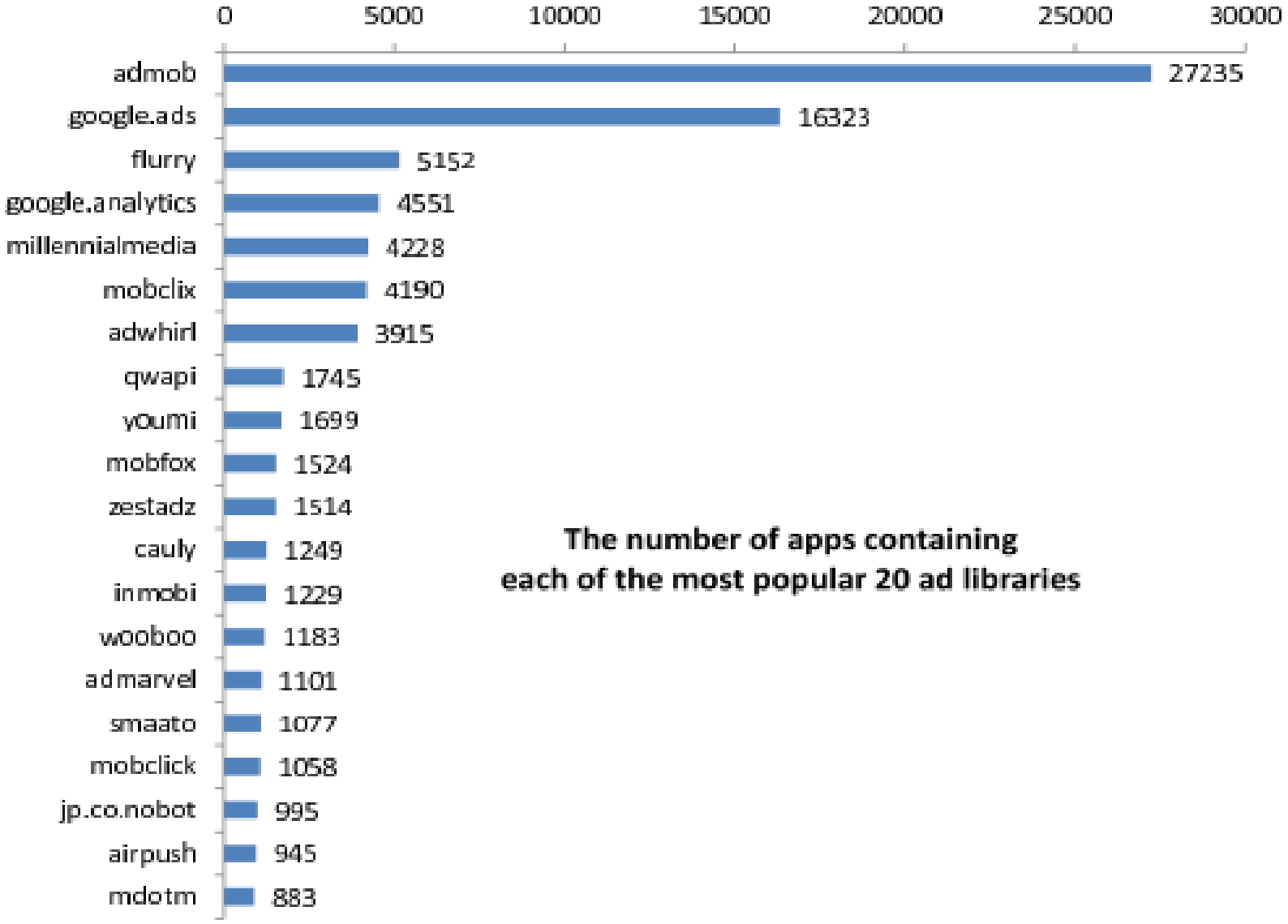
- Researchers at NCSU and TU-Darmstadt did a study of ad library use in Android in 2011
  - [M. Grace, W. Zhou, X. Jiang, A.-R. Sadeghi; WiSec 2012]
  - Collected 100,000 apps from the Android Market
  - Identified 100 common in-app ad libraries by inspecting Android manifest files

```
<manifest ... ...
    package="com.rovio.angrybirdsrio" >
    <application
        <activity android:name="com.rovio.ka3d.App">
            <intent-filter>  <action android:name="android.intent.action.MAIN"> </action>
                <category android:name="android.intent.category.LAUNCHER">    </category>
            </intent-filter>
        </activity>
        ... ...
        <meta-data android:name="ADMOB_PUBLISHER_ID" android:value="a14d6f9cc06f96b">
        <meta-data android:name="ADMOB_INTERSTITIAL_PUBLISHER_ID" android:value="a14d6fa2b901034">
        <meta-data android:name="ADMOB_ALLOW_LOCATION_FOR_ADS" android:value="true"> </meta-data>
        <activity android:name="com.admob.android.ads.AdMobActivity"> </activity>
        <receiver android:name="com.admob.android.ads.analytics.InstallReceiver" >
            <intent-filter >
                <action android:name="com.android.vending.INSTALL_REFERRER"></action>
            </intent-filter>
        </receiver>
        ... ...
    </application>
    <uses-permission android:name="android.permission.INTERNET"> </uses-permission>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"> </uses-permission>
</manifest>
```

Admob Publisher IDs/Settings

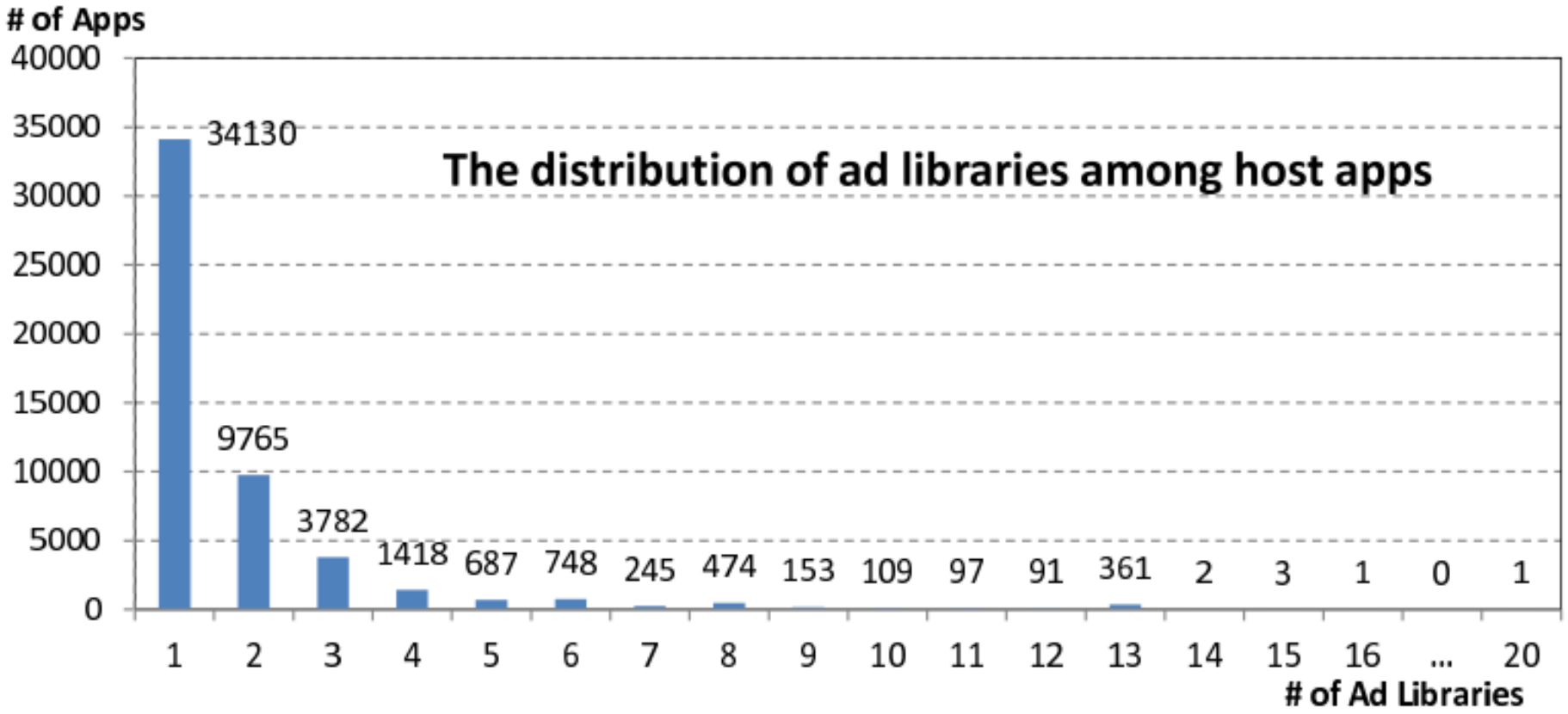
Admob Components

Popular Ad Services

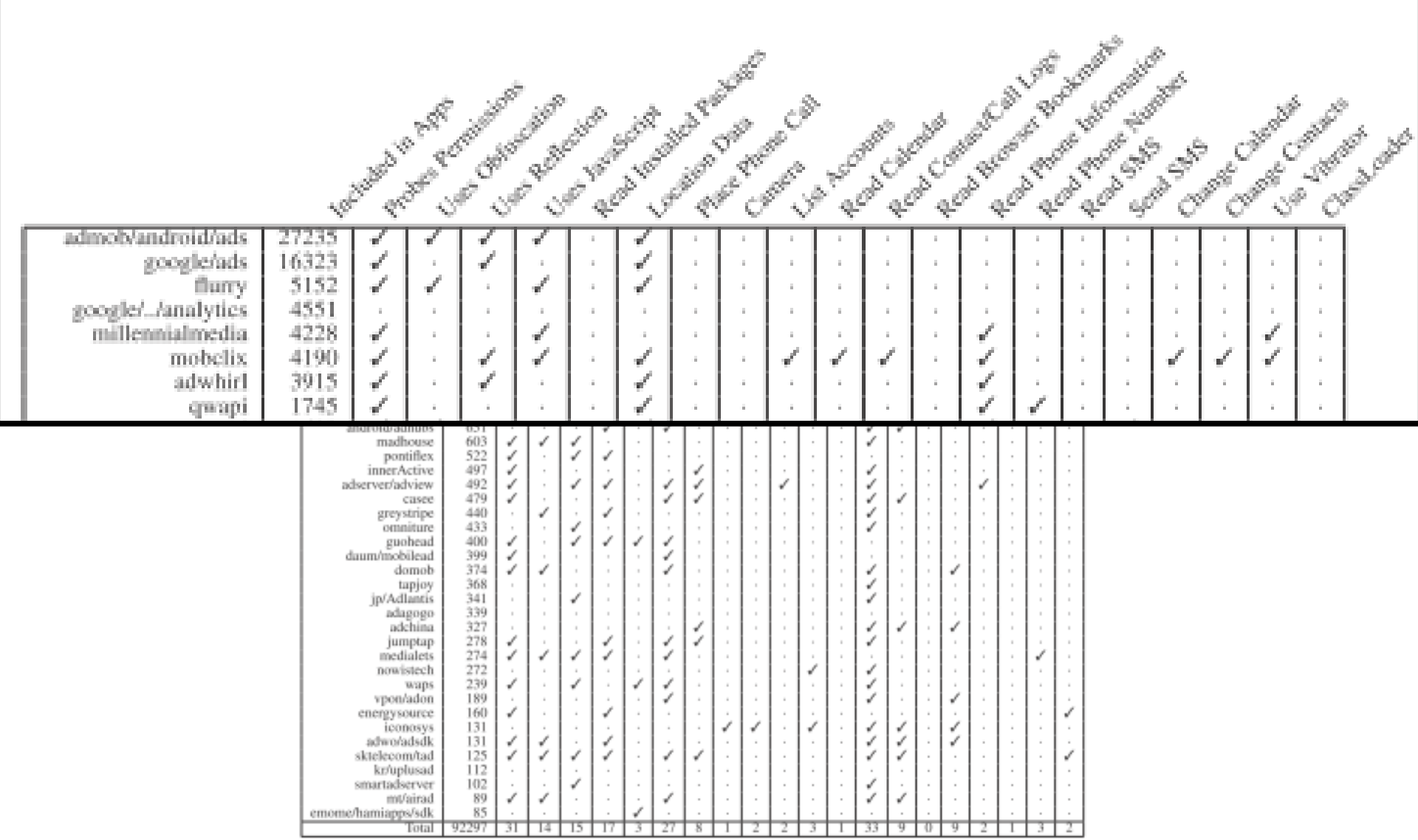


The number of apps containing each of the most popular 20 ad libraries

Multiple Ad Services?



Threat Analysis



		Included in Apps	Probes Permissions	Uses Obfuscation	Uses Reflection	Uses JavaScript	Read Installed Packages	Location Data	Place Phone Call	Camera	List Accounts	Read Calendar	Read Contact/Call Logs	Read Browser Bookmarks	Read Phone Information	Read Phone Number	Read SMS	Send SMS	Change Calendar	Change Contacts	Use Vibrator	ClassLoader
admob/android/ads	27235	✓	✓	✓	✓	·	✓	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·
google/ads	16323	✓	·	✓	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
flurry	5152	✓	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
google/.../analytics	4551	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
millennialmedia	4228	✓	·	·	✓	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	✓	·
mobclix	4190	✓	·	✓	✓	·	✓	·	·	✓	✓	✓	·	·	✓	·	·	✓	·	·	✓	·
adwhirl	3915	✓	·	✓	·	·	✓	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·
qwapi	1745	✓	·	·	·	·	✓	·	·	·	·	·	·	·	✓	✓	·	·	·	·	·	·
madhouse	603	✓	✓	✓	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
pontiflex	522	✓	·	✓	✓	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
innerActive	497	✓	·	·	·	·	·	✓	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
adserver/adview	492	✓	·	✓	✓	·	✓	✓	·	·	✓	·	·	✓	·	·	✓	·	·	·	·	·
casee	479	✓	·	·	·	·	✓	✓	·	·	·	·	·	✓	✓	·	·	·	·	·	·	·
greystripe	440	·	✓	·	✓	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
omniture	433	·	·	✓	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
guohead	400	✓	·	✓	✓	✓	✓	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
daum/mobilead	399	✓	·	·	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
domob	374	✓	✓	·	·	·	✓	·	·	·	·	·	·	✓	·	·	✓	·	·	·	·	·
tapjoy	368	·	·	·	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
jp/Adlantis	341	·	·	✓	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
adagogo	339	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
adchina	327	·	·	·	·	·	·	✓	·	·	·	·	·	✓	✓	·	✓	·	·	·	·	·
jumptap	278	✓	·	·	✓	·	✓	✓	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
medialets	274	✓	✓	✓	✓	·	✓	·	·	·	·	·	·	✓	·	·	·	·	·	✓	·	·
nowistech	272	·	·	·	·	·	·	·	·	·	·	✓	·	✓	·	·	·	·	·	·	·	·
waps	239	✓	·	✓	·	✓	✓	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
vpon/adon	189	·	·	·	·	·	✓	·	·	·	·	·	·	✓	·	·	✓	·	·	·	·	·
energysource	160	✓	·	·	✓	·	·	·	·	·	·	·	·	✓	·	·	✓	·	·	·	·	✓
iconosys	131	·	·	·	·	·	·	·	✓	✓	·	✓	·	✓	✓	·	✓	·	·	·	·	·
adwo/adsdk	131	✓	✓	·	✓	·	·	·	·	·	·	·	·	✓	✓	·	✓	·	·	·	·	·
sktelecom/tad	125	✓	✓	✓	✓	·	✓	✓	·	·	·	·	·	✓	✓	·	·	·	·	·	·	✓
kr/uplusad	112	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
smartadserver	102	·	·	✓	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·	·	·	·
mt/airad	89	✓	✓	·	·	·	✓	·	·	·	·	·	·	✓	✓	·	·	·	·	·	·	·
emome/hamiapps/sdk	85	·	·	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
Total	92297	31	14	15	17	3	27	8	1	2	2	3	1	33	9	0	9	2	1	3	2	

A Few Side Notes

- Since an app has a single list of permissions in the manifest file:
  - An app needs to request whatever permissions are required to support the ad service
  - An ad service inherits whatever permissions are required by the app...

Static Analysis

- A fairly standard combination of permission analysis, java decompiling, and code analysis can further expose exactly what permissions the app is using, what the ad APIs are using, and what data is being collected and sent

- The authors of the paper used these tools to estimate the risks introduced by ad services

- Other tools, such as APKInspector or DIDFAIL, can do similar analysis

Is there anything we can do to protect against malicious advertisers?

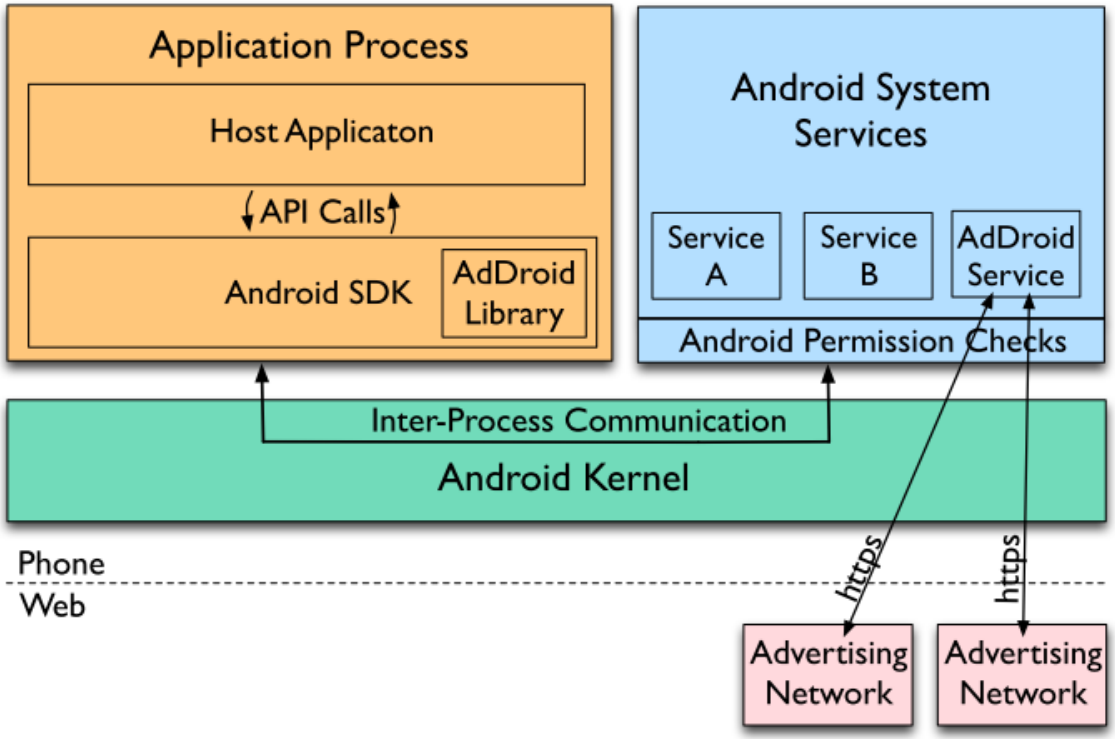
Currently, Not Really

- If we can convince users to check what permissions are requested by an app and only install apps that seem reasonable...

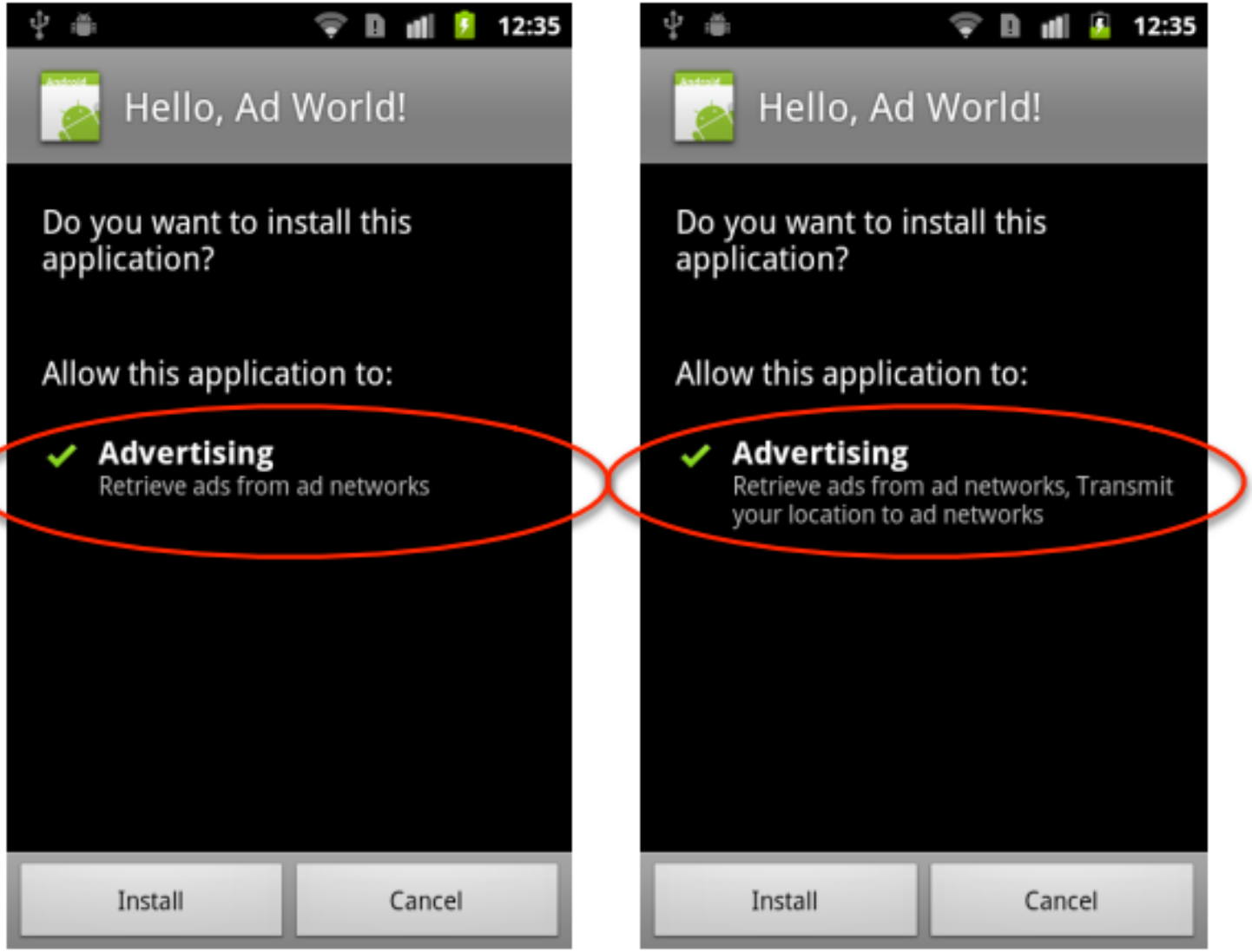
- Otherwise, we would need to change the way ad services are incorporated into Android apps

Ad Privilege Separation

- Another group of researchers suggest separating the privileges used for ads from the rest of the app and adding advertising permissions
  - [Pearce, Felt, Nunez, and Wagner; ASIACCS 2012]



Advertising Permissions



Implications of Android M

- The new permission model in Android Marshmallow has some interesting implications for ad services
  - Many of the permission combinations previously described as “sensitive” are now approved by default
  - Take a look at the list of default permissions that apps no longer need to request, see how you feel about malware and ad services...

Here's an activity for you to try offline

Explore Manifest Files

- Test what permissions and ad services are being used by your favorite apps
- Obtain an .apk using any available technique
  - Browser extension to get .apk from Play store, extract .apk from device, use a web service, etc.
- Use your favorite technique (e.g., apktool) to read the manifest file
  - Anything interesting?

“Interesting” Ad Services?

- If you find any strange or otherwise “interesting” ad services, do a little online studying to find out more

- If the developer is using unusual ad services, what else are they doing?
  - Maybe use some other analysis tools to look for other “features” built into the app

Interesting Findings

- Many apps use multiple ad services - an Angry Birds app includes 7+ ad services
- One version of the Dictionary.com app requests permissions to **monitor phone calls** and **access location**
- Check out the FireEye report about a service they (anonymously) refer to as **Vulna**

A few notes about upcoming deliverables

Progress Presentations

- Progress presentations are in class Nov 10 + 12
- Schedule will be randomized, same rules as before

- Requirements:
  - MAX 8 minutes, including Q&A
  - Things to include:
    - **Brief** reminder of your problem statement & goals
    - Describe any interesting project updates
    - Discuss any roadblocks or challenges faced
    - Summarize any changes to SoW / goals

¾-Term Exam

- The single exam in this course will be on **Nov 17**
  - That's right, presentation one week, exam the next
  - I like to ask questions that make you think, not questions that make you (only) recall
  - Look at the previous years' exams available on Blackboard
    - Under “course content” → “private content”

- Questions about the exam?

Nov 10 & 12:
Progress Presentations

Nov 17:
Exam

Nov 19:
Mobile Dev Best Practices