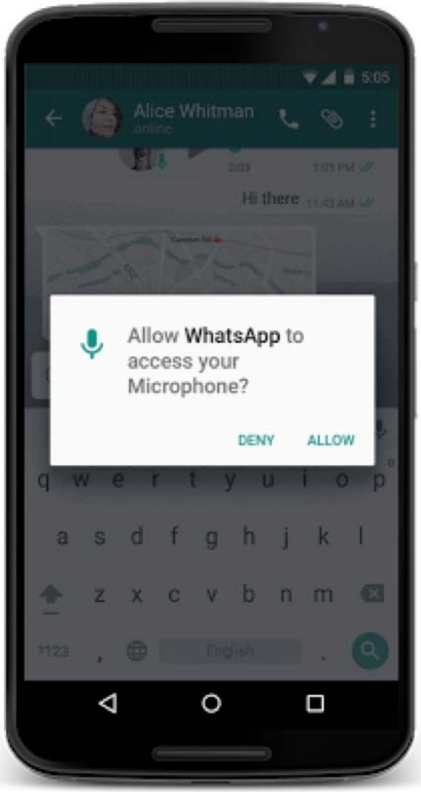
50 Ways to Leak Your Data:
An Exploration of Apps' Circumvention of the Android Permissions System

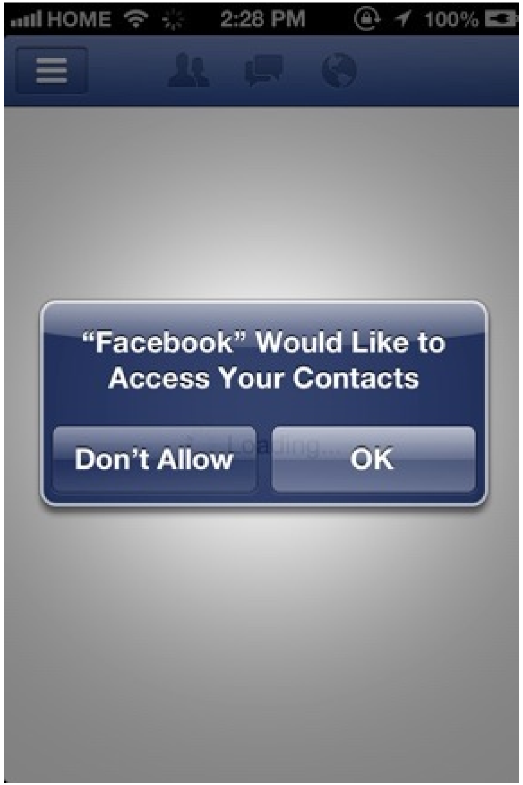
Serge Egelman, U.C. Berkeley / ICSI / AppCensus

Jointly with:
Joel Reardon, University of Calgary
Álvaro Feal, IMDEA Networks / Universidad Carlos III
Primal Wijesekera, U.C. Berkeley / ICSI
Amit Elazari Bar On, U.C. Berkeley
Narseo Vallina-Rodriguez, IMDEA Networks / ICSI / AppCensus

PRIVACYCON



Allow **WhatsApp** to access your Microphone?



“Facebook” Would Like to Access Your Contacts

Apps and Permissions

- Governs access to:
  - Location data
  - Address book
  - Photo library
  - Persistent identifiers

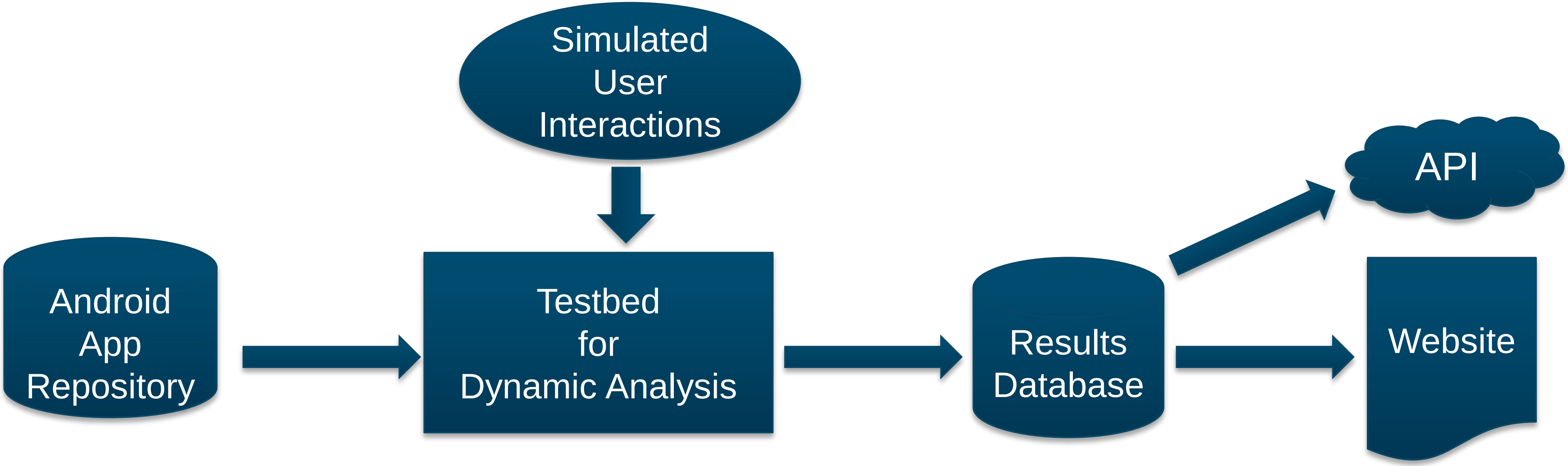
- Supports notice and choice:
  - Apps show requests for data
  - Users allow or deny access

Does this work in practice?

Monitoring Data Flows

Instrumented Android: Access to sensitive resources (e.g., location, call logs, network state, various identifiers, etc.)

Lumen: Network traffic, remote servers, HTTP/HTTPS payloads

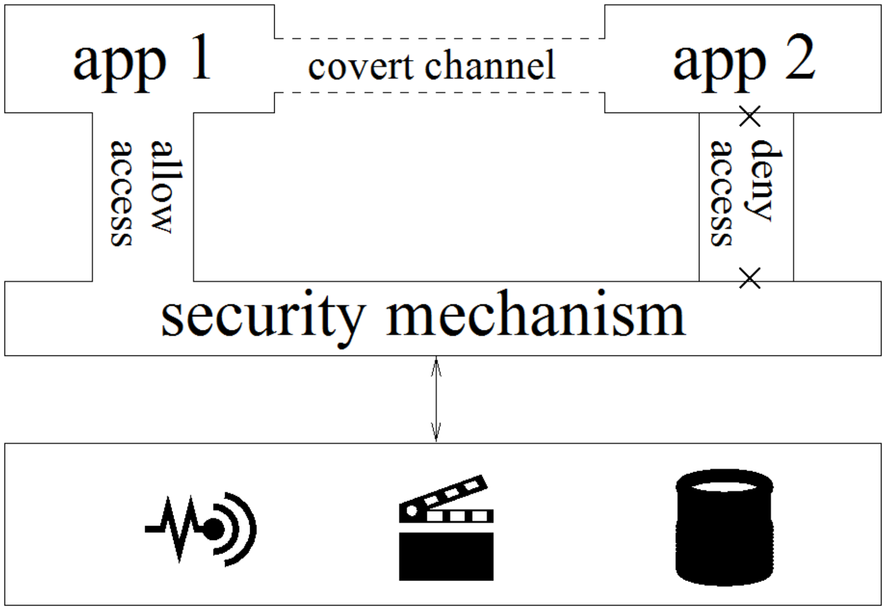

Simulated User Interactions
Android App Repository
Testbed for Dynamic Analysis
Results Database
API
Website

https://search.appcensus.io

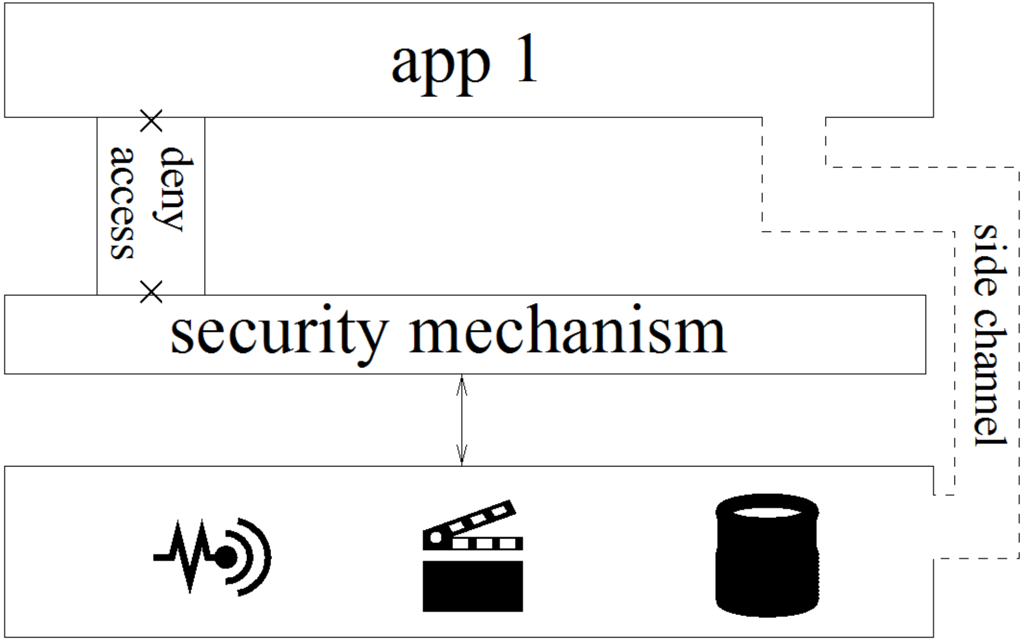
Browse
Services
Blog
About
AppCensus
AppSearch
Search for Android apps in our analysis database
Terms of Service | Privacy Policy

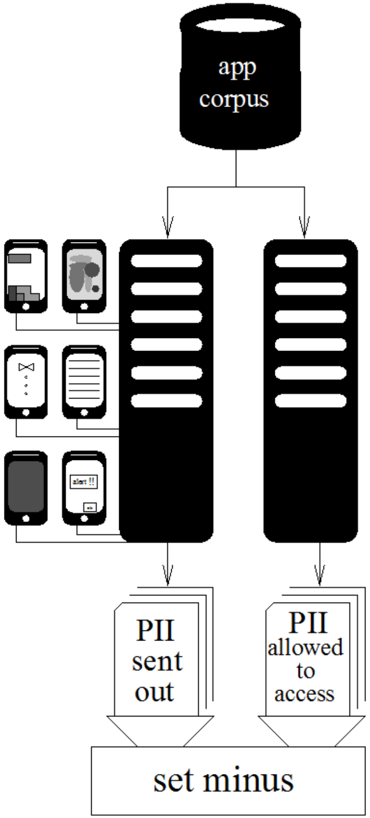
Uncovering Deceptive Practices

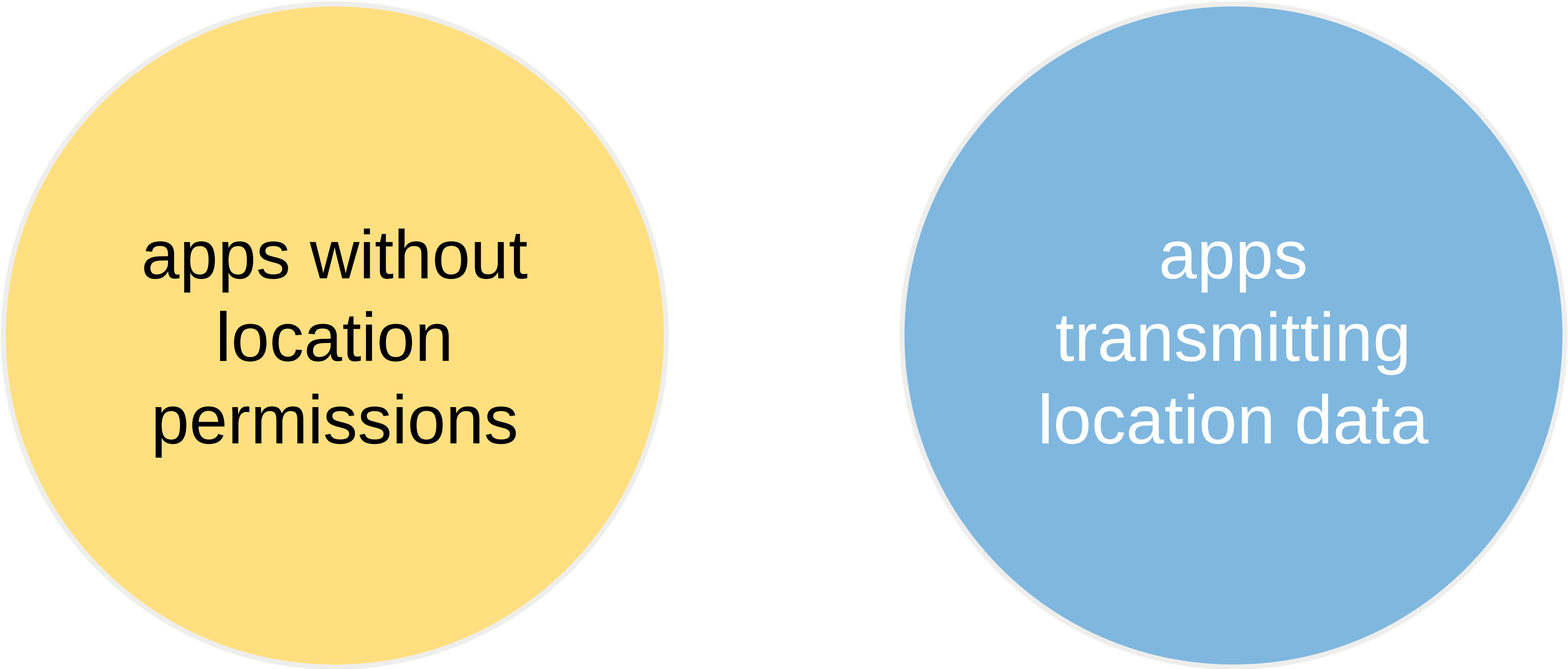
Covert Channels



Side Channels

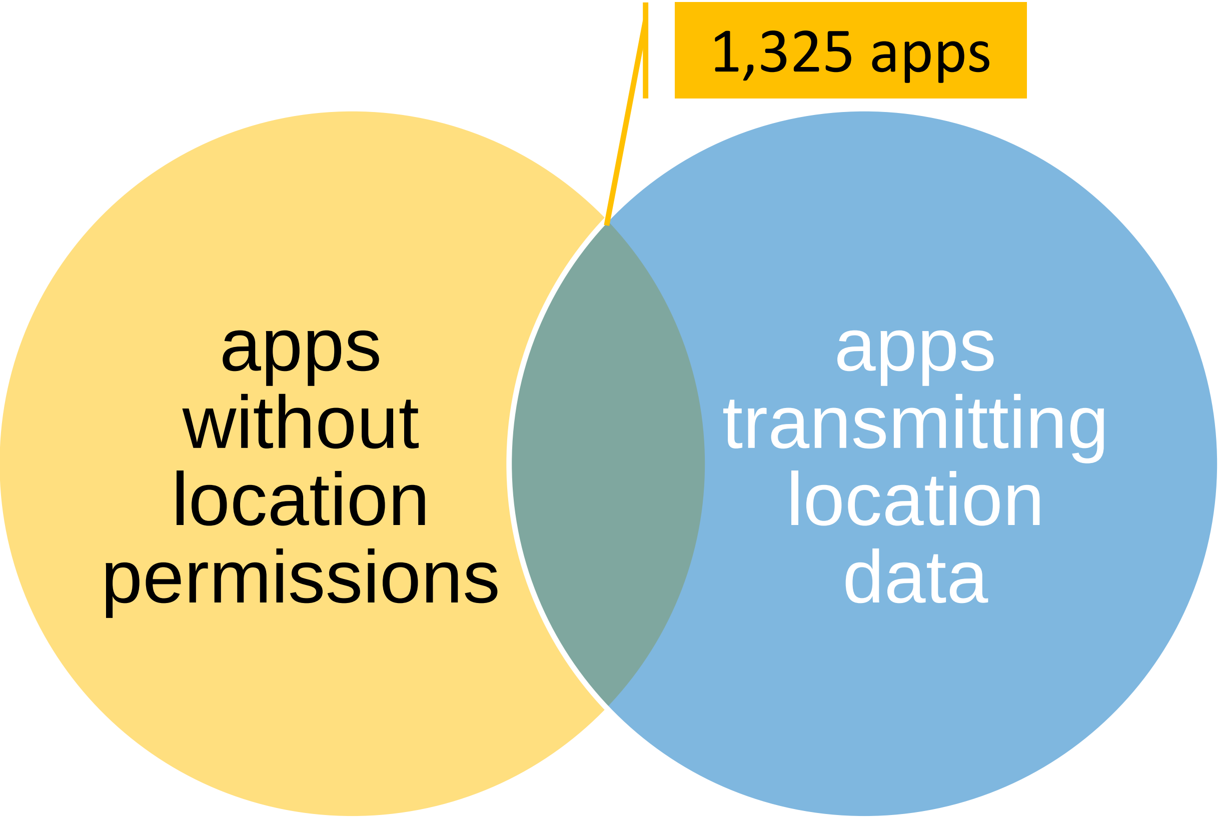



app corpus
alert !!
PII sent out
PII allowed to access
set minus



apps without location permissions

apps transmitting location data



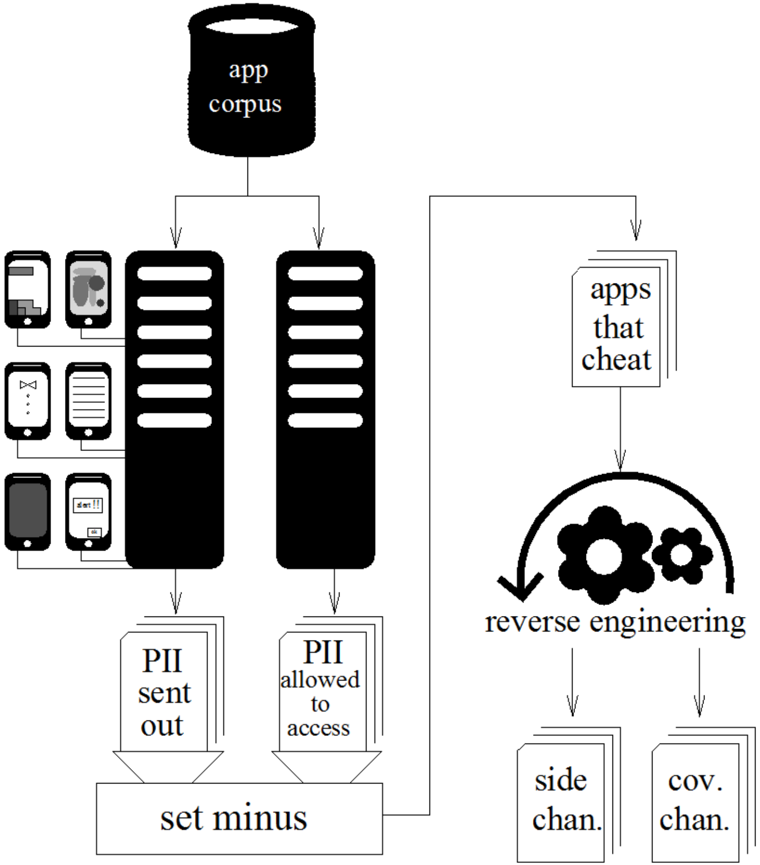
1,325 apps

apps without location permissions

apps transmitting location data

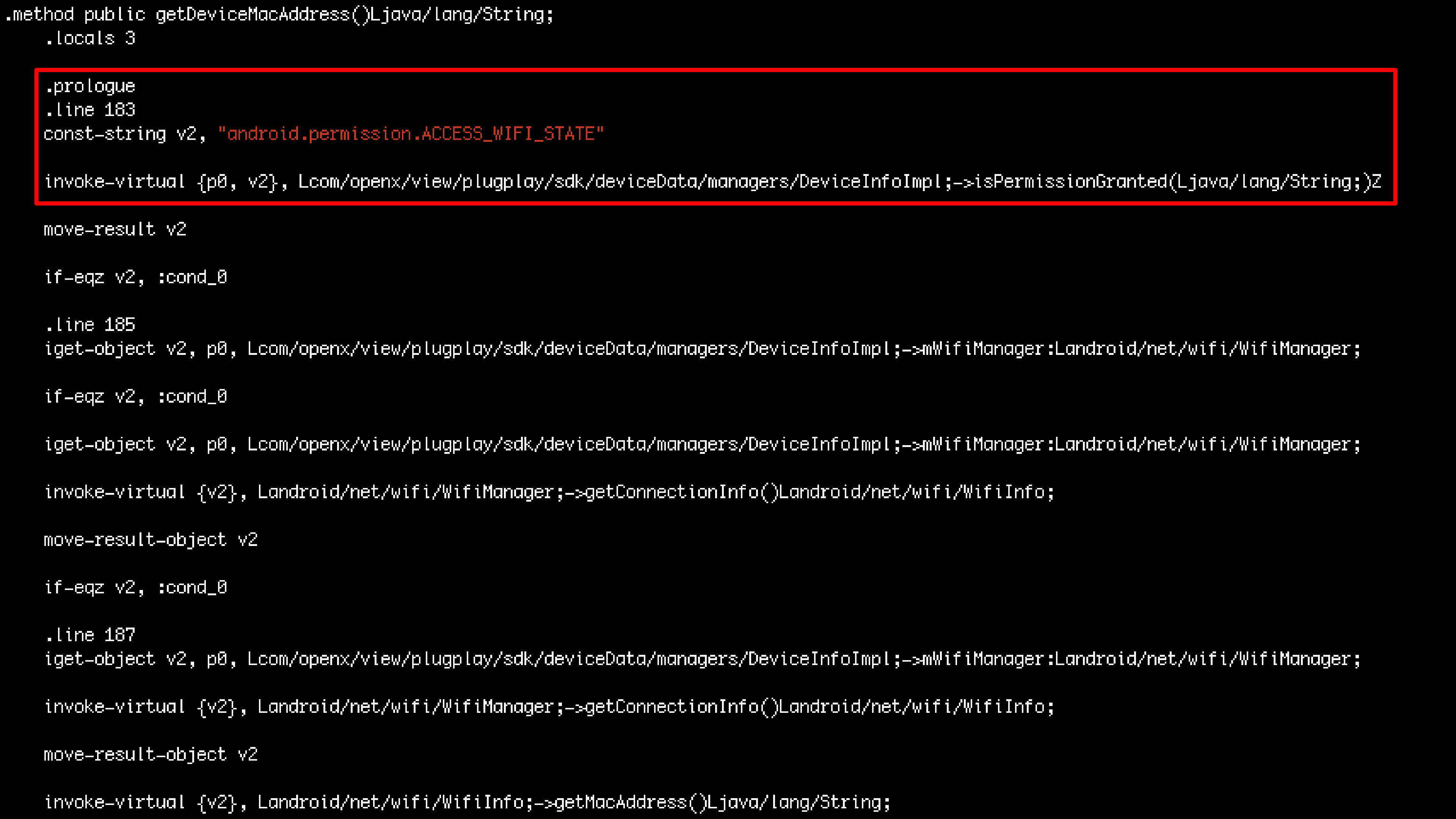
Findings

more than 80,000 apps

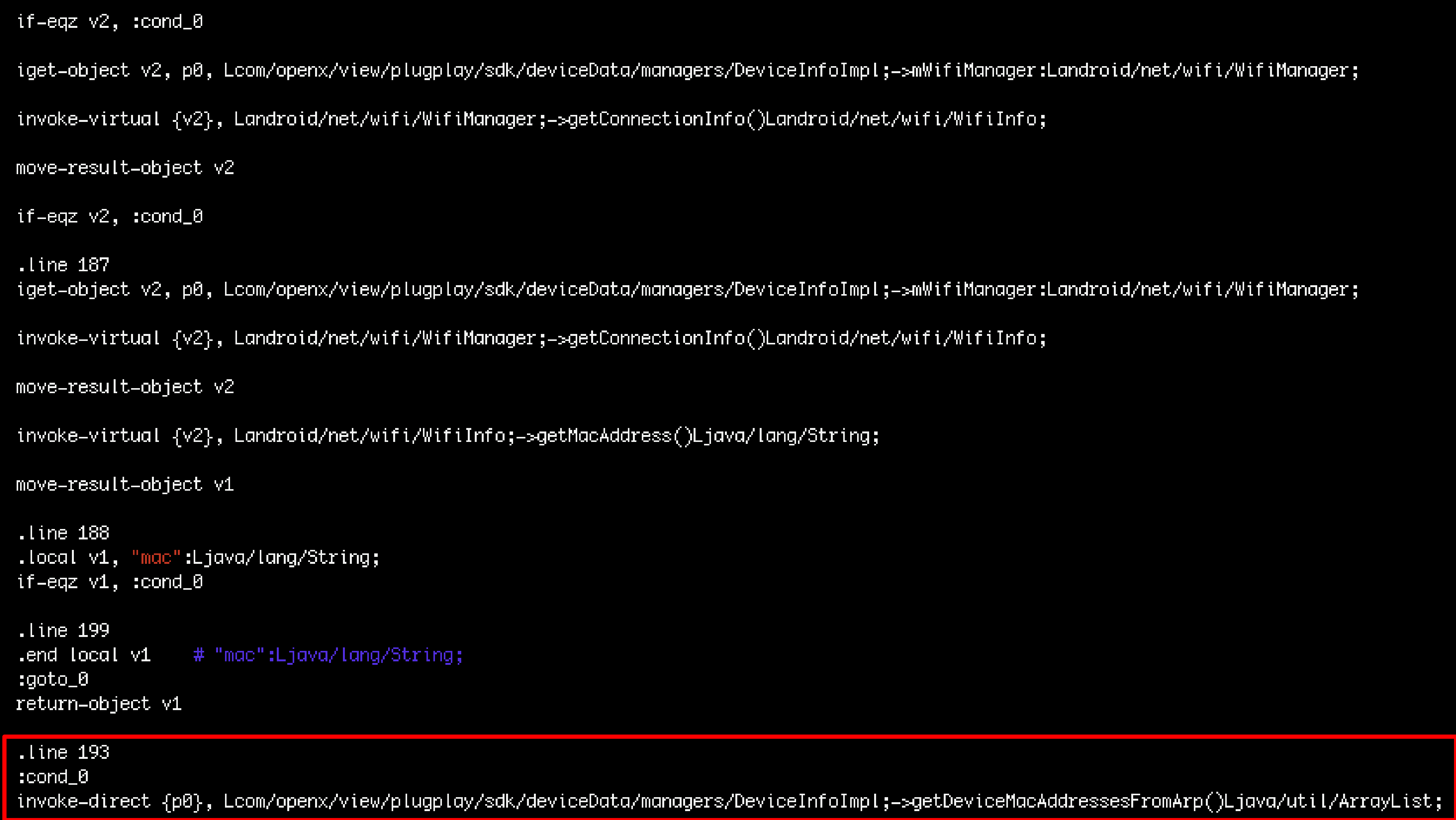


Look in `/proc/`, Brock

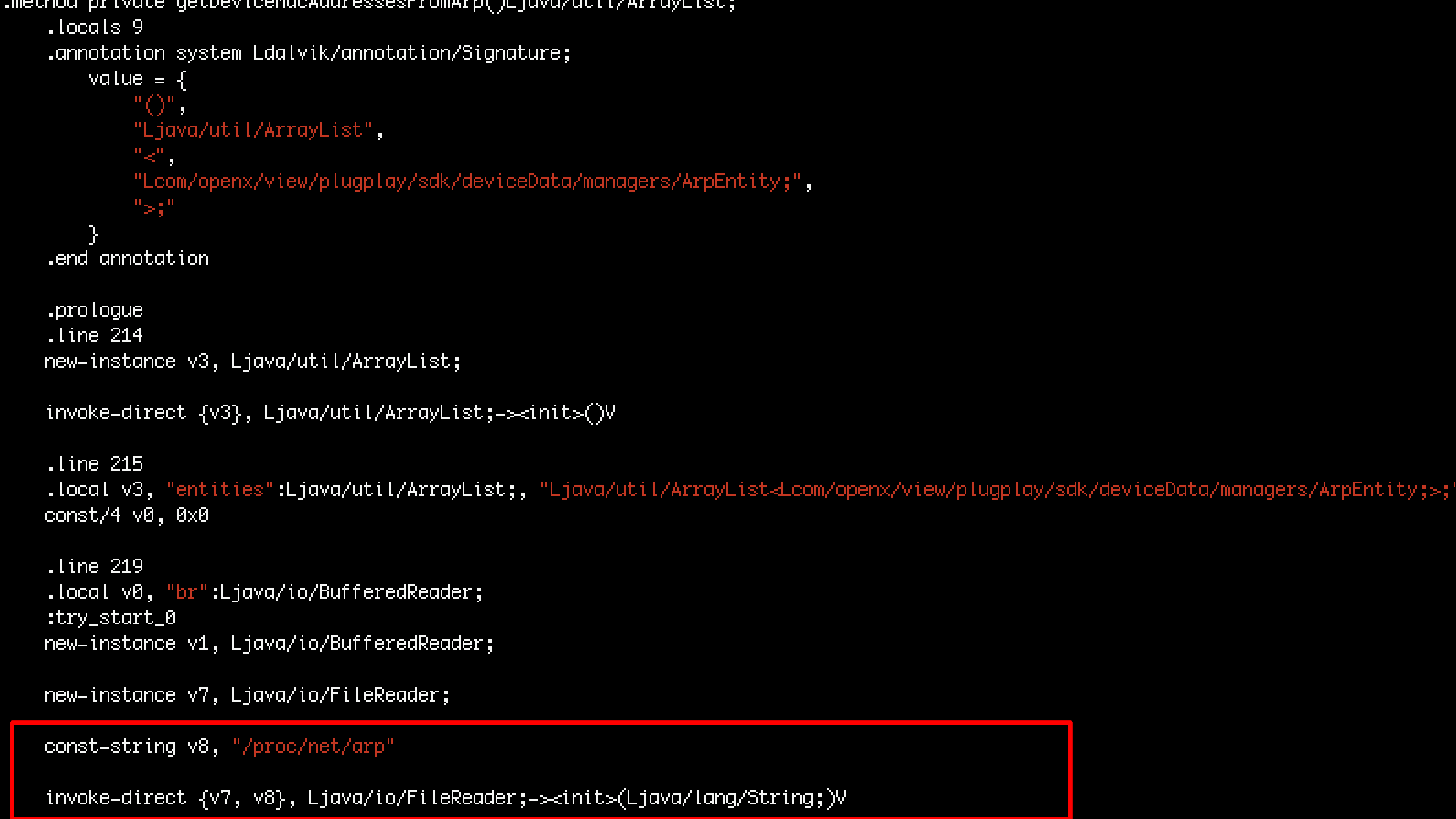
- `/proc/` is a virtual filesystem
  - Hardware information
  - Information on running processes
  - System state
  - Networking information (e.g., ARP table)
- `/proc/net/arp` is readable by any app



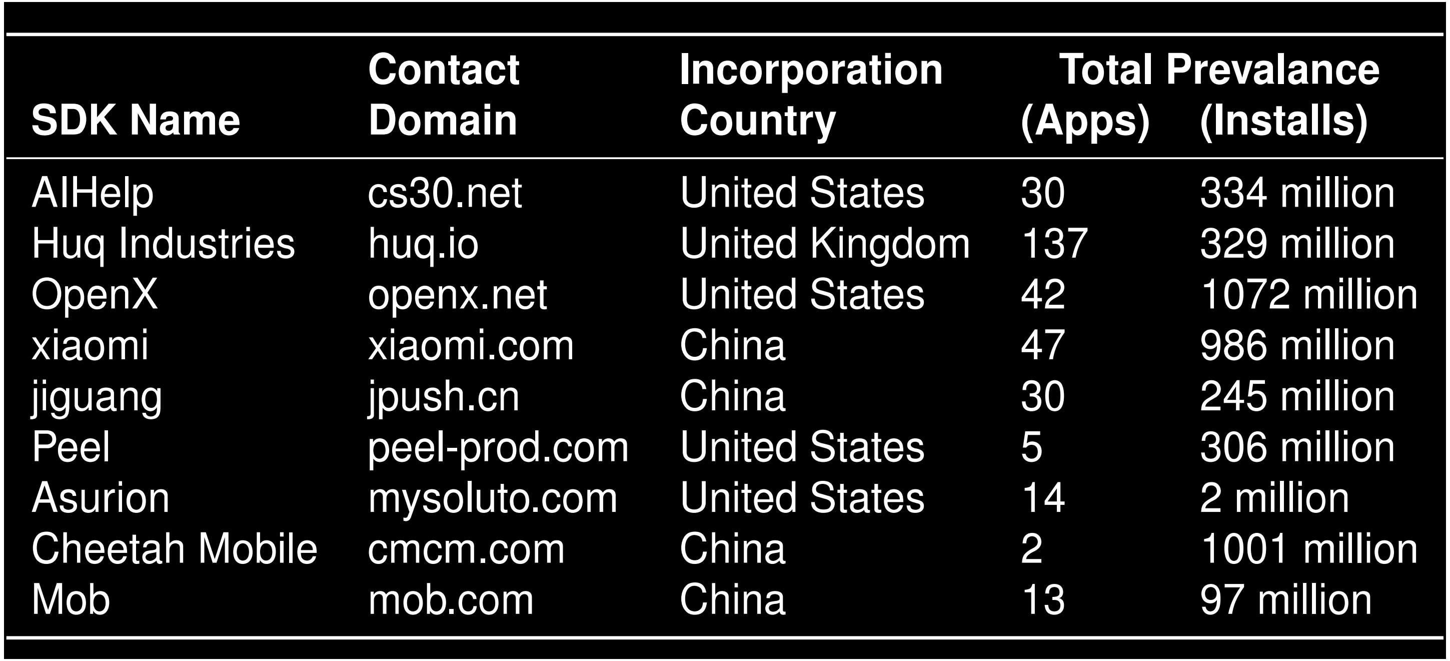
```
.method public getDeviceMacAddress()Ljava/lang/String;
    .locals 3

    .prologue
    .line 183
    const-string v2, "android.permission.ACCESS_WIFI_STATE"

    invoke-virtual {p0, v2}, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->isPermissionGranted(Ljava/lang/String;)Z

    move-result v2

    if-eqz v2, :cond_0

    .line 185
    iget-object v2, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;

    if-eqz v2, :cond_0

    iget-object v2, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;

    invoke-virtual {v2}, Landroid/net/wifi/WifiManager;->getConnectionInfo()Landroid/net/wifi/WifiInfo;

    move-result-object v2

    if-eqz v2, :cond_0

    .line 187
    iget-object v2, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;

    invoke-virtual {v2}, Landroid/net/wifi/WifiManager;->getConnectionInfo()Landroid/net/wifi/WifiInfo;

    move-result-object v2

    invoke-virtual {v2}, Landroid/net/wifi/WifiInfo;->getMacAddress()Ljava/lang/String;
```



```
if-eqz v2, :cond_0

iget-object v2, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;

invoke-virtual {v2}, Landroid/net/wifi/WifiManager;->getConnectionInfo()Landroid/net/wifi/WifiInfo;

move-result-object v2

if-eqz v2, :cond_0

.line 187
iget-object v2, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;

invoke-virtual {v2}, Landroid/net/wifi/WifiManager;->getConnectionInfo()Landroid/net/wifi/WifiInfo;

move-result-object v2

invoke-virtual {v2}, Landroid/net/wifi/WifiInfo;->getMacAddress()Ljava/lang/String;

move-result-object v1

.line 188
.local v1, "mac":Ljava/lang/String;
if-eqz v1, :cond_0

.line 199
.end local v1    # "mac":Ljava/lang/String;
:goto_0
return-object v1

.line 193
:cond_0
invoke-direct {p0}, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->getDeviceMacAddressesFromArp()Ljava/util/ArrayList;
```



```
.method private getDeviceMacAddressesFromArp()Ljava/util/ArrayList;
    .locals 9
    .annotation system Ldalvik/annotation/Signature;
        value = {
            "()",
            "Ljava/util/ArrayList",
            "<",
            "Lcom/openx/view/plugplay/sdk/deviceData/managers/ArpEntity;",
            ">;"
        }
    .end annotation

    .prologue
    .line 214
    new-instance v3, Ljava/util/ArrayList;

    invoke-direct {v3}, Ljava/util/ArrayList;-><init>()V

    .line 215
    .local v3, "entities":Ljava/util/ArrayList;, "Ljava/util/ArrayList<Lcom/openx/view/plugplay/sdk/deviceData/managers/ArpEntity;>;"
    const/4 v0, 0x0

    .line 219
    .local v0, "br":Ljava/io/BufferedReader;
    :try_start_0
    new-instance v1, Ljava/io/BufferedReader;

    new-instance v7, Ljava/io/FileReader;

    const-string v8, "/proc/net/arp"

    invoke-direct {v7, v8}, Ljava/io/FileReader;-><init>(Ljava/lang/String;)V
```



SDK Name	Contact Domain	Incorporation Country	Total Prevalance (Apps)	(Installs)
AIHelp	cs30.net	United States	30	334 million
Huq Industries	huq.io	United Kingdom	137	329 million
OpenX	openx.net	United States	42	1072 million
xiaomi	xiaomi.com	China	47	986 million
jiguang	jpush.cn	China	30	245 million
Peel	peel-prod.com	United States	5	306 million
Asurion	mysoluto.com	United States	14	2 million
Cheetah Mobile	cmcm.com	China	2	1001 million
Mob	mob.com	China	13	97 million

Ask the Router, Piotr

- UPnP
  - Protocol to get configuration data from WiFi routers
  - Peel smart remote apps use this to collect BSSID

Check the IMEI, Guy

- Protected by the “Phone State and Identity” permission
  - Apps that have the permission write it to the filesystem
    - Salmonads: /sdcard/.googlex9/.xamdecoq0962
      - 6 apps (~18M installs)
    - Baidu: /sdcard/backups/.SystemConfig/.cuid2
      - 153 apps
      - Samsung Health (>500M installs)
      - Samsung Browser (>500M installs)

Grab the MAC, Jack

- Another hardware-based identifier
  - Every device connected to the Internet has one
- Unity
  - Native C++ libraries
  - Outside of Android permissions system
  - Impact: >12,000 apps

Look at a Picture, Victor

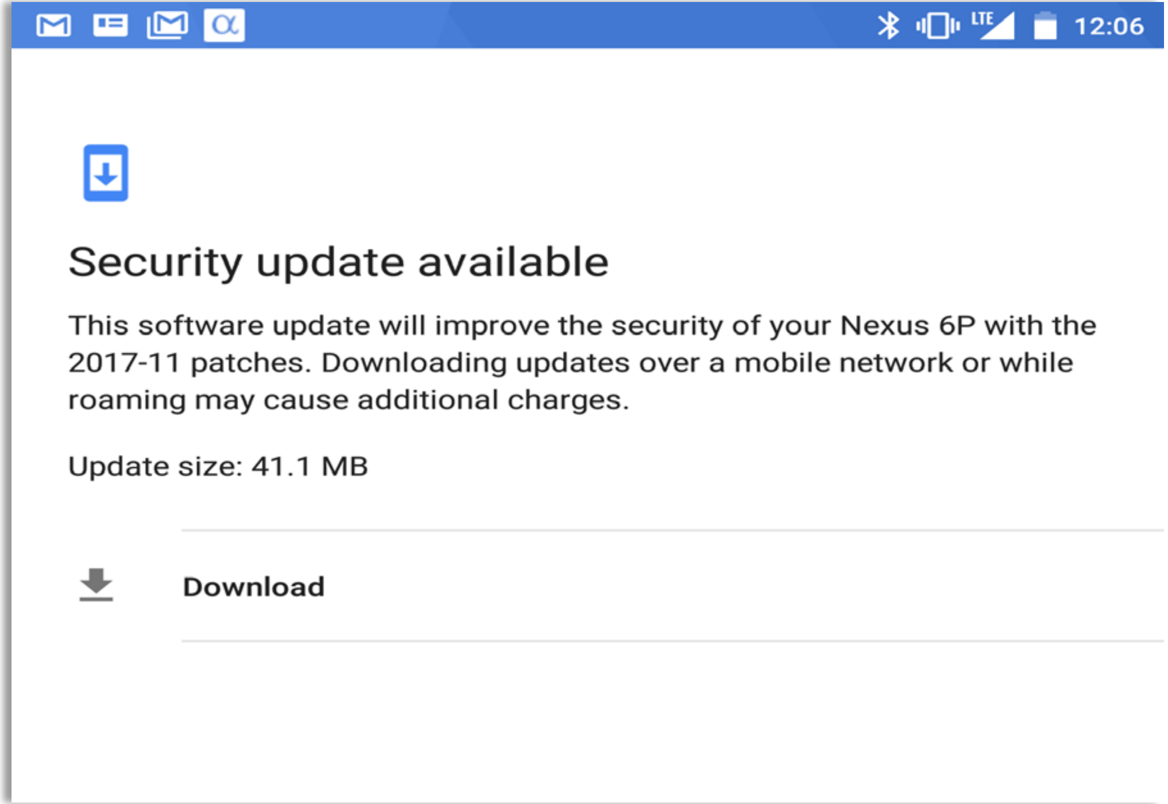
- Photos contain metadata (EXIF)
  - Often contains GPS coordinates

- Shutterfly app reads geolocation from photos

Conclusions

- Android permissions protect certain personal data
  - Often, same data is unprotected on the filesystem

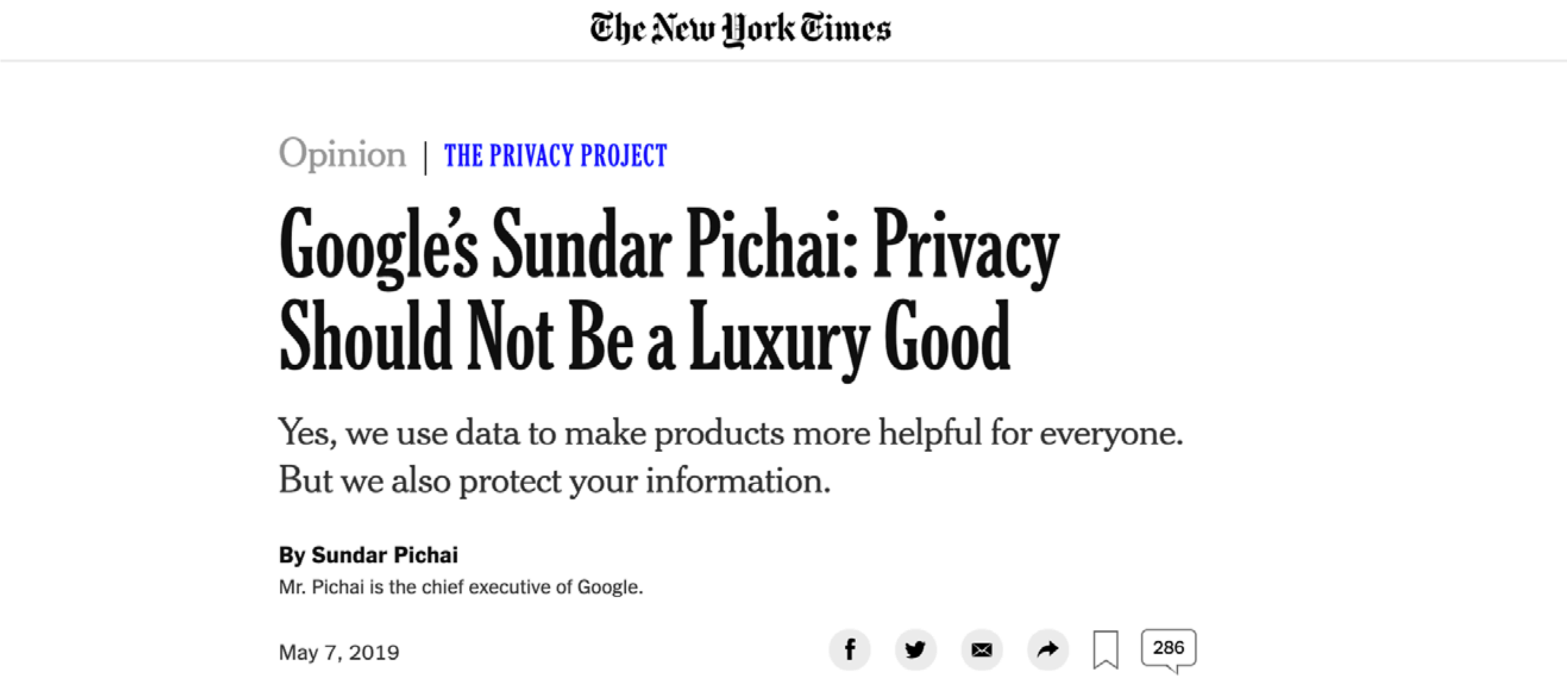
- Google gave us a bug bounty
  - Fixed in Android Q (fall 2020?)



Security update available

This software update will improve the security of your Nexus 6P with the 2017-11 patches. Downloading updates over a mobile network or while roaming may cause additional charges.

Update size: 41.1 MB



The New York Times

Opinion | THE PRIVACY PROJECT

Google's Sundar Pichai: Privacy Should Not Be a Luxury Good

Yes, we use data to make products more helpful for everyone. But we also protect your information.

By Sundar Pichai

Mr. Pichai is the chief executive of Google.

May 7, 2019

Serge Egelman

U.C. Berkeley / ICSI / AppCensus, Inc.

egelman@cs.berkeley.edu

@v0max

Sponsors: DHS, NSF, NSA, the Rose Foundation, the E.U. Horizon 2020 Innovation Action program, the Data Transparency Lab, and the Center for Long-Term Cybersecurity at U.C. Berkeley.