



Improving Mobile Security

with forensics, app analysis and big data

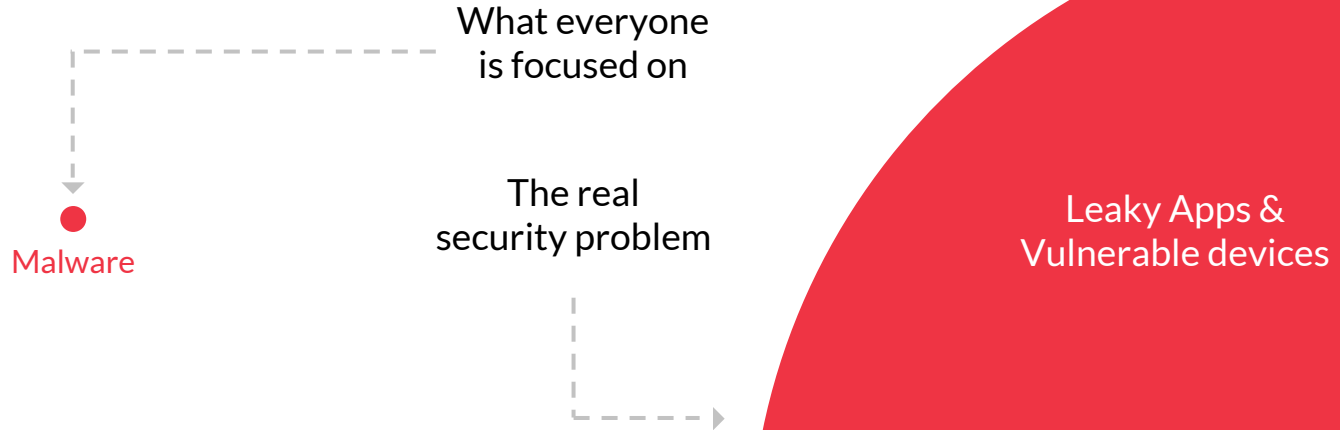


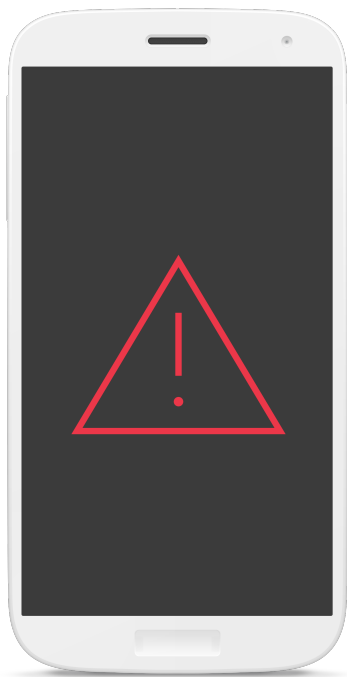
Andrew Hoog

CEO and Co-founder of NowSecure

- Computer scientist & mobile security researcher
- Author of two mobile forensics + security books
- Enjoyer of occasional science fiction
- Drinker of red wine

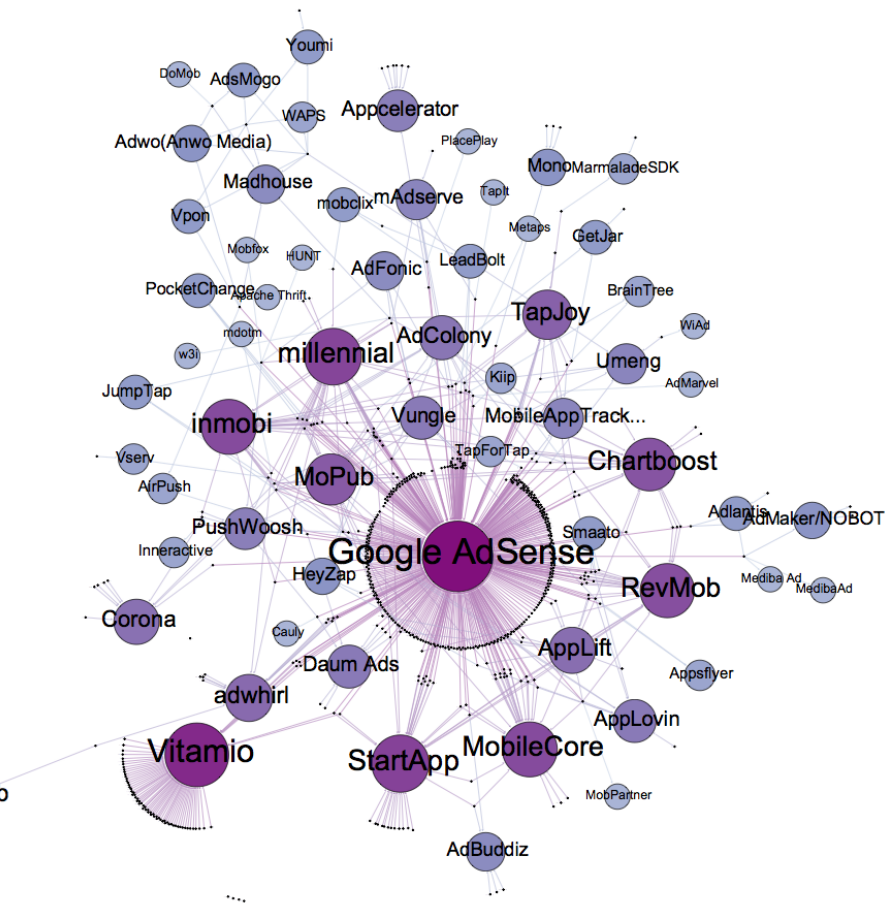
What's the problem? It's not malware.





48%

of Android apps have at least one
high risk security or privacy flaw



50%

of popular apps send data
to an ad network

** Some to as many as 16 different ad networks*

Remote Attack Surface

- SDK downloads a zip file over http without TLS or verification
- Create a .dex file that contains code you want to execute
- Add the .dex to the requested zip file, modify the network response and, you can gain remote code execution



EXAMPLE:



“An integrated mobile advertising platform enabling advertiser to optimize ad efficiency and app developer to acquire the highest media benefit. “

Adlibr Scale

Integrated ad network SDK and service

7,200+

App

ADLIB ad is displayed on **7,200+** apps from 2,200+ publishers

12%

Traffic Increase

Consistent monthly traffic increase by **12%**

80B

Monthly Impression

8 billion times of monthly display

27M

Monthly Click

27M+ times of monthly clicks

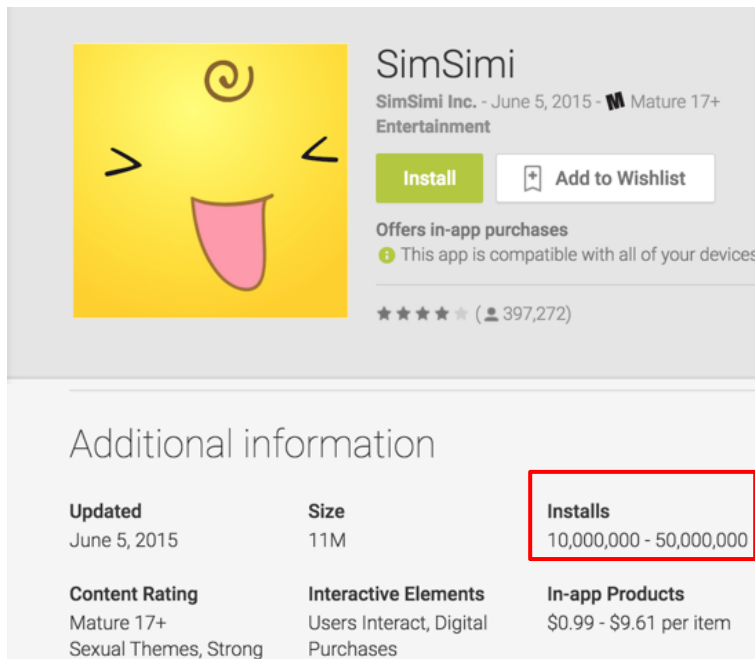
80%

Coverage

(26M+ of monthly UVs)

Data from ADLIB as at 2015 Apr

Example target



SimSimi
SimSimi Inc. · June 5, 2015 · Mature 17+
Entertainment

Install **Add to Wishlist**

Offers in-app purchases
This app is compatible with all of your devices

★★★★★ (397,272)

Additional information

Updated June 5, 2015	Size 11M	Installs 10,000,000 - 50,000,000
Content Rating Mature 17+ Sexual Themes, Strong	Interactive Elements Users Interact, Digital Purchases	In-app Products \$0.99 - \$9.61 per item

- A network-based attacker can modify traffic to gain control of the device due to a flaw in Adlibr SDK
- The attacker can access current app data, world accessible data and chain with an exploit to gain elevated permissions

Sample data leaked (http)

```
imei=352584060111000
mac=f8:a9:c2:4f:f3:80
androidid=88c8584b54bd9c00
serial=062f2dfb344be87b
conn=wifi
country=US
dm=Nexus+5
dv=Android4.4.2
lat=41.83720397949219
long=-87.9613037109375
mcc=310
mnc=410
mmidid=mmh_AC78B68BD2E528CC0FC78AFB342E58CF_9099A5181F956
FCAFB4AC9946DF71CCACB322F59
root=0
pkid=com.ismaker.android.simsimi
pknm=SimSimi
plugged=true
sdkversion=5.1.0-13.08.12.a
ua=Dalvik%2F1.6.0+%28Linux%3B+U%3B+Android+4.4.2%
3B+Nexus+5+Build%2FKOT49H%29
```

- Many ad networks send data in clear, including geolocation
- ID derived from hardware can be tracked across time and locations
- App pkg is identified, enabling attacker to find target

Data destinations

One app, several countries



Destination address	IP	Country
ad.adlibr.com	211.236.244.152	KR
ad.doubleclick.net	173.194.33.156	US
ads.mp.mydas.mobi	216.157.12.18	US
adtg.widerplanet.com	117.52.90.81	KR
androidsdk.ads.mp.mydas.mobi	211.110.212.68	KR
ajax.googleapis.com	74.125.28.95	US
androidsdk.ads.mp.mydas.mobi	216.157.12.18	US
app.simsimi.com	54.235.200.56	US
astg.widerplanet.com	117.52.90.85	KR
bank81.mi.ads.mp.mydas.mobi	216.157.13.15	US
capp.simsimi.com	174.129.197.187	US
cdn.millennialmedia.com	96.17.8.146	US
d.appsdtd.com	52.6.198.255	US
dcys-en.ijinshan.com	114.112.93.204	CN
landingpages.millennialmedia.com	216.157.12.21	US
mtab.clickmon.co.kr	114.207.113.177	KR
once.unicornmedia.com	192.33.167.222	US
rtax.criteo.com	74.119.117.100	US

Testing the Exploit

Process

1. Modify network traffic to inject our payload
2. App executes our code
3. Download busybox
4. Establish reverse shell
5. [Optional] Privilege Escalation



mitmproxy is a very effective tool for this type of scripting

fo·ren·sic

fə'renzik, fə'rensik/

noun

plural noun: **forensics**

1. scientific tests or techniques used in connection with the detection of crime.

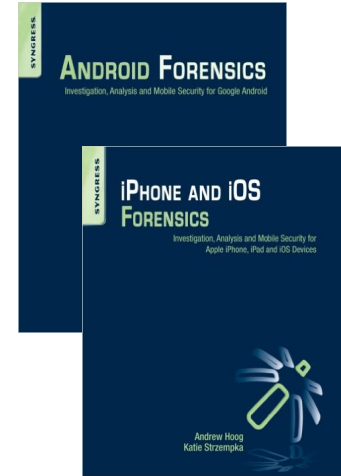
Forensics -> Security

by Andrew Hoog

- Bored CIO, departing employee investigation, amazed at what Windows stored
- Certification (GCFA, CCE)
- Recognized as expert witness in my first case (US Federal Court)
- Developed a mobile forensics business
- During one mobile device case (2010), found device owner's:
 - name, credit card #, address, bank statements, username/passwords and more
 - all stored in plain-text

Forensic & Security Books

- Wrote two books on mobile forensics and security (Android & iOS)
 - Starting 2nd editions
- Working on 2 new books:
 - Mobile Incident Response (for Android and iOS)
 - Mobile App Testing
- All books will be released free on <https://nowsecure.com/>



Ch. 7 - Android app & forensic analysis

"Android Forensics: Investigation, Analysis, and Mobile Security for Google Android"

- TRUE
 - "But data without context and analysis is just noise"
- CHALLENGE ACCEPTED:
 - "Of course, maintaining a complete reference [of key application] would be nearly impossible not only due to the sheer number of applications but also due to the variation between specific devices and Android versions."

Individual mobile app analysis

Works but doesn't scale, not indexed

NowSecure

Introduction ✓

1. Android and mobile forensics ✓

1.1. Android Platform ✓

1.2. Linux, Open Source Software, an... ✓

1.3. Android Open Source Project ✓

1.4. Internationalization ✓

1.5. Android Market ✓

1.6. Android Forensics ✓

1.7. Summary

1.8. References

2. Android hardware platforms ✓

2.1. Overview of Core components ✓

2.2. Overview of Different Device Typ... ✓

2.3. Rom and Boot Loaders ✓

2.4. Manufacturers ✓

Contacts

App Info

This app is the main contacts app provided by Android. While there are many additional apps available, this app provides the core contact functionality.

- App Name: Contacts
- Package name: com.android.providers.contacts
- Version: 2.2
- Device: HTC Incredible
- App developer: Android

Directories, Files, and File Types

In /data/data/com.android.providers.contacts:

```
com.android.providers.contacts    directory
├── databases                      directory
│   └── contacts2.db              SQLite 3.x database, user version 309
├── files                          directory
│   ├── thumbnail_photo_10014.jpg  JPEG image data, JFIF standard 1.01
│   ├── thumbnail_photo_10194.jpg  JPEG image data, JFIF standard 1.01
│   ├── thumbnail_photo_10199.jpg  JPEG image data, JFIF standard 1.01
│   ├── thumbnail_photo_10202.jpg  JPEG image data, JFIF standard 1.01
│   ├── thumbnail_photo_10203.jpg  JPEG image data, JFIF standard 1.01
│   └── thumbnail_photo_12450.jpg  JPEG image data, JFIF standard 1.01
```


Mobile App Analysis

(at scale)

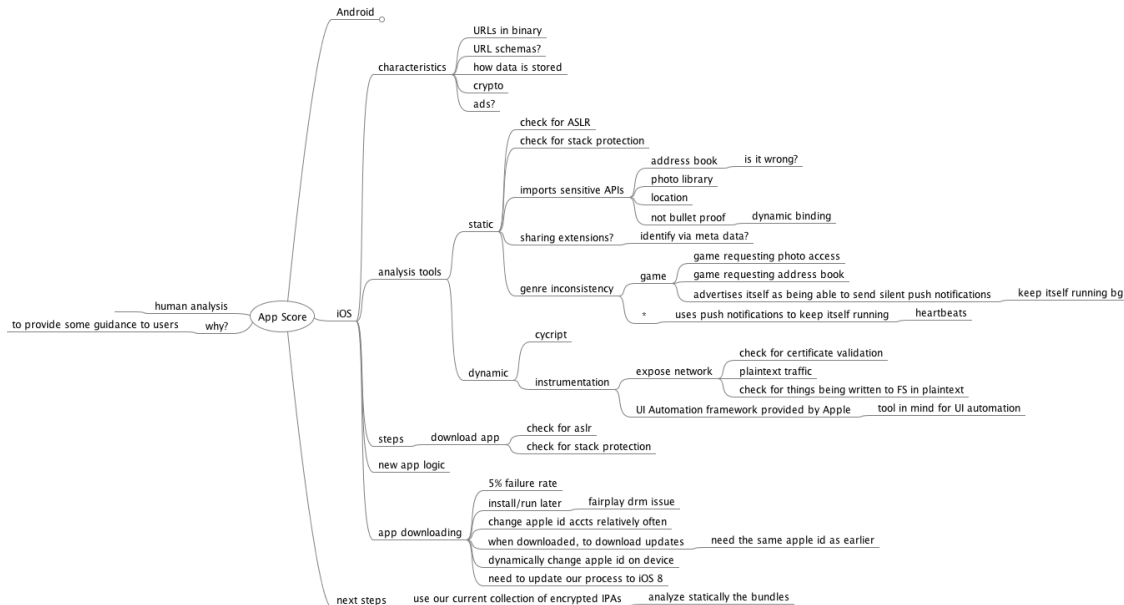
Tools and Techniques

- **App analysis techniques**
 - Static
 - Dynamic
 - Instrument runtime (dalvik) and kernel
 - Store and analyze all artifacts (pcap, file system r/w, ssl session keys)
 - Function tracing (how to decrypt)
- **Tools**
 - Generally command line
 - Manual or automated
 - UI Automator

Data Store and APIs

- **Data store requirements**
 - Simple APIs, scale horizontally and vertically
 - Efficiently store and access significant data (hot, warm and cold storage)
 - Streaming technology with replay capability
 - Data access layer handles indexes
 - Based on [LevelDB](#), @hij1nx began to hire core team members (juliangruber, ralphtheninja, ...)
- **Data store APIs**
 - GET, PUT, DELETE, BATCH

Complex and constantly evolving



Static code analysis

Identify app flaws and characteristics

1. Acquire apk and ipa app files
2. Decompile apps
3. Index source code
4. Identify code of interest (algorithms + manual analysis)
5. Find code of interest in impacted apps

Taint, Exercise, Monitor & Store

Taint

- GPS
- MAC addr
- IMEI
- phone #
- email
- password

Exercise

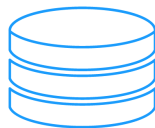
Automatically exercise
the app using UI
Automator

Perform static analysis

Perform dynamic analysis



Internet



File System

Monitor

- raw
- MD5
- xor
- URL encoded
- SHA
- BASE64
- protobuf

Store

- App: com.xyz.abc
- Version: 1.3.9
- GPS
 - File System
 - Encoding: Raw
 - Type: SQLite
 - Column: Location:
- Network
 - Port: 443
 - Format: URLEncoded

UI Automator

Exercising Mobile Apps for Dynamic Analysis

- **Heuristic**

Looks at object hierarchy on the screen to detect login/password/buttons in UI

- **Coverage**

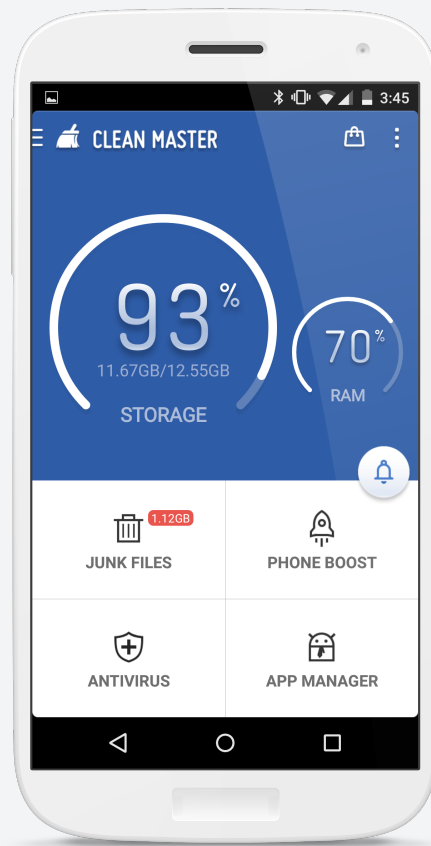
Compare network traffic to crowd sourced netstat

- **Simple yet effective**

Hundreds of automated findings in very short period

- **Portable**

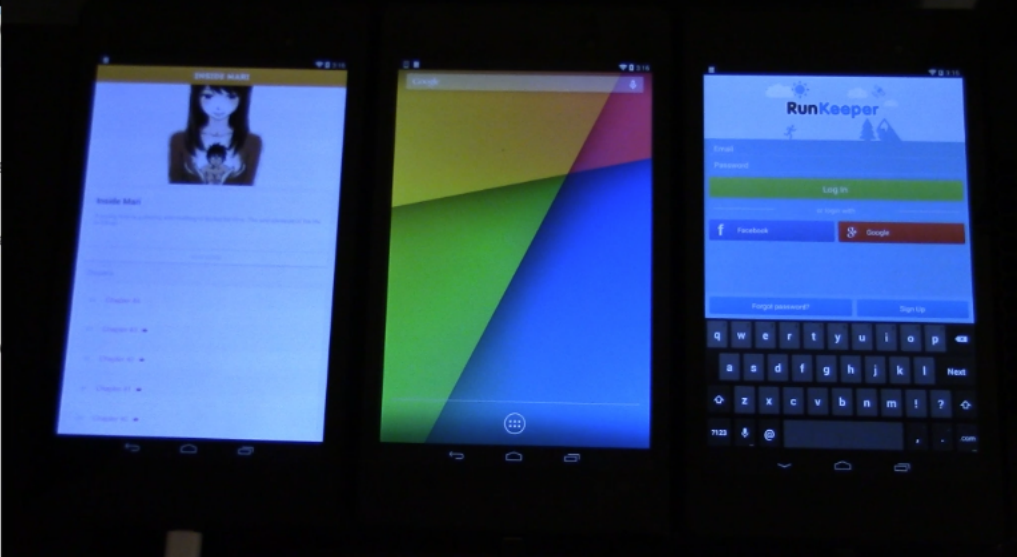
Works for emulator and physical devices via ADB.



```

File Edit View Bookmarks Settings Help
WARNING: linker: app_process has text relocations. This is wasting memory and prevents security hardening.
pkg: /data/local/tmp/com.crunchyroll.crmanga-15-3c43eb8f0114bd873d5bdcda1c89e0e8a168ab5f.apk
5499 KB/s (10092497 bytes in 1.792s)
WARNING: linker: app_process has text relocations. This is wasting memory and prevents security hardening.
WARNING: linker: app_process has text relocations. This is wasting memory and prevents security hardening.
pkg: /data/local/tmp/com.avast.android.mobilesecurity-7875-65d80020c9a66e41478afe9d66fa84a101842ac
5813 KB/s (19534920 bytes in 3.281s)
WARNING: linker: app_process has text relocations. This is wasting memory and prevents security hardening.
WARNING: linker: app_process has text relocations. This is wasting memory and prevents security hardening.
pkg: /data/local/tmp/com.fitnesskeeper.runkeeper.pro-269-c3c6bdb8d7397eac78f8d2d535e4cd1fa9273aee
Success
Starting the activity com.crmanga.misc.SplashActivity...
Running the component com.crunchyroll.crmanga/com.crunchyroll.crmanga.misc.SplashActivity...
Success
Starting the activity com.avast.android.mobilesecurity.app.home.StartActivity...
Running the component com.avast.android.mobilesecurity/com.avast.android.mobilesecurity.app.home.StartActivity...
Success
Starting the activity com.fitnesskeeper.runkeeper.RunKeeperActivity...
Running the component com.fitnesskeeper.runkeeper.pro/com.fitnesskeeper.runkeeper.RunKeeperActivity...
Found button: com.avast.android.mobilesecurity:id/b_dont_agree
Found button: com.avast.android.mobilesecurity:id/b_agree
Found button: com.avast.android.mobilesecurity:id/b_display
Found button: com.avast.android.mobilesecurity:id/b_display
Found button: com.avast.android.mobilesecurity:id/b_dont_agree
Found button: com.avast.android.mobilesecurity:id/b_agree
Found button: com.avast.android.mobilesecurity:id/b_dont_agree text: Don't agree
1433 KB/s (131653 bytes in 0.089s)
Found button: com.crunchyroll.crmanga:id/manga_login
Found button: com.crunchyroll.crmanga:id/manga_login
Found button: com.crunchyroll.crmanga:id/manga_login
Found button: com.crunchyroll.crmanga:id/manga_login
Found button: com.crunchyroll.crmanga:id/main_button_settings
Touching com.crunchyroll.crmanga:id/manga_login text: LOG IN
Found button: com.fitnesskeeper.runkeeper.pro:id/existinguserlogin
Found button: com.fitnesskeeper.runkeeper.pro:id/existinguserlogin
Found button: com.fitnesskeeper.runkeeper.pro:id/existinguserlogin
Found button: com.fitnesskeeper.runkeeper.pro:id/existinguserlogin
Found button: com.fitnesskeeper.runkeeper.pro:id/createaccountwithgooglebutton
Found button: com.fitnesskeeper.runkeeper.pro:id/createaccountwithfacebookbutton
Found button: com.fitnesskeeper.runkeeper.pro:id/createaccountwithemailbutton
Found button: com.fitnesskeeper.runkeeper.pro:id/createaccountwithgooglebutton
Found button: com.fitnesskeeper.runkeeper.pro:id/createaccountwithfacebookbutton
Found button: com.fitnesskeeper.runkeeper.pro:id/createaccountwithemailbutton
Touching com.fitnesskeeper.runkeeper.pro:id/existingUserLogin text: Log In
1278 KB/s (114432 bytes in 0.087s)
6353 KB/s (1946864 bytes in 0.299s)
Swiping left
Attempting to fill in login data
Entering email in: com.fitnesskeeper.runkeeper.pro:id/emailinputbox / email
Swiping left

```



Queue/Analyze, Metadata & Download

Fetch from App/Play, identify metadata

```
± curl -s -XPOST "10.10.171.22:3000/queue/play/pkg/com.insitusec.isthisreallife"?priority=high"  
{ "success": true, "job": 6610 }
```

```
± curl -s '10.10.171.22:3000/reports/apk/pkg/com.insitusec.isthisreallife' | jq -S -C '.metaData|. [0].details.appDetails' | head -n 20  
{  
  "appCategory": "ENTERTAINMENT"  
  "certificateHash": "OKBv0IUqPjIVAs02y6XwmAJ-EWg"  
  "contentRating": 2,  
  "developerEmail": "dweinst+rl+support@insitusec.com",  
  "developerName": "dweinst",  
  "developerWebsite": "http://www.insitusec.com"  
  ...  
}
```

```
± curl "10.10.171.22:3000/download/apk?packageName=com.insitusec.isthisreallife"  
[{"sha1": "ff49f74cb61cb3ec399d99fec773e0b781102cfa", "packageName": "com.insitusec.isthisreallife", "versionCode": 1, "versionName": "1.0", "  
url": "https://vmatrix.s3.amazonaws.com/android/apk/ff49f74cb61cb3ec399d99fec773e0b781102cfa?  
Expires=1425604097&AWSAccessKeyId=AKIAJ4YNT47SPXIVIDHA&Signature=aFF0tUITi%2Bv7d5g3siG7IG42QPs%3D"}]
```

App Properties

Query and return specific app version & properties

```
± curl -s '10.10.171.22:3000/reports/apk/pkg/com.insitusec.isthisreallife' | jq -S -C '.androguardAnalysis|. [0] |  
dexInfo.usedPermissions'  
[  
  {  
    "permissionName": "ACCESS_NETWORK_STATE",  
    "permissionPaths": [  
      "1 Landroid/support/v4/net/ConnectivityManagerCompat$BaseConnectivityManagerCompatImpl;-  
      >isActiveNetworkMetered(Landroid/net/ConnectivityManager;)Z (0x2) --->  
      Landroid/net/ConnectivityManager;->getActiveNetworkInfo()Landroid/net/NetworkInfo;",  
      "1 Landroid/support/v4/net/ConnectivityManagerCompatGingerbread;->isActiveNetworkMetered  
      (Landroid/net/ConnectivityManager;)Z (0x2) ---> Landroid/net/ConnectivityManager;-  
      >getActiveNetworkInfo()Landroid/net/NetworkInfo;",  
      "1 Landroid/support/v4/net/ConnectivityManagerCompatHoneycombMR2;-
```

Finding IMEI

Querying network output for sensitive data

```
± find . -name 'network_issue_summary' | xargs -l{} jq -c '{file: "{}", results: .}' {} | jq -C '.' | head -n 18
```

```
"file": "br.com.easytaxi/66/3ecfdaf270b0b54d192cac72754c12d3b895454e/dynamic_analysis_1424390957.54_603f935/network_issue_summary",  
"results": {  
  "sensitive_data_value": "9988776655443322",  
  "data_value_type": "imei",  
  "encoded_format": "urlEncoded",  
  "issue": "sensitive_data_leak",  
  "full_url": "http://apps.ad-x.co.uk/atrk/andrdapp?udid=9988776655443322&androidID=bef0bbe1371221d6&macAddress=11:22:33:44:55:66&type=&storeAppID=&device_name=Nexus%207&device_type=android&os_version=4.4.4&country_code=US&language=en&app_id=br.com.easytaxi&clientid=rocketinteasytax76895jo&app_version=5.9.7&tag_version=3.1.4&fbattribution=null&uagent=&update=0&idfa=f1002a87-5eed-4faf-b2aa-0260db2c97ab&isLAT=false"
```

Finding MAC Address

Querying network output for sensitive data

```
± find . -name 'network_issue_summary' | barges -l {} jq -c '{file: "{}", results: .}' {} | jq -C '.' | head -n 18
```

```
"file": "br.com.easytaxi/66/3ecfdaf270b0b54d192cac72754c12d3b895454e/dynamic_analysis_1424390957.54_603f935/network_issue_summary",  
"results": {  
  "sensitive_data_value": "11:22:33:44:55:66",  
  "data_value_type": "MAC",  
  "encoded_format": "original",  
  "issue": "sensitive_data_leak",  
  "full_url": "http://apps.ad-x.co.uk/atrk/andrdapp?udid=9988776655443322&androidID=bef0bbe1371221d6&macAddress=11:22:33:44:55:66&type=&storeAppID=&device_name=Nexus%207&device_type=android&os_version=4.4.4&country_code=US&language=en&app_id=br.com.easytaxi&clientid=rocketinteasytax76895jo&app_version=5.9.7&tag_version=3.1.4&fbattribution=null&uagent=&update=0&idfa=f1002a87-5eed-4faf-b2aa-0260db2c97ab&isLAT=false"
```

Finding apps that store passwords

Querying SQLite databases on file system for sensitive data

```
± gfind . -name '*.logcat' | gxargs -l{} grep -H "StealthSpy" {} | grep -i "password TEXT"
```

`./com.apalon.weatherlive.free`

```
D/StealthSpy(26735): {"class": "android.database.sqlite.SQLiteDatabase", "SQLStatement": "CREATE TABLE httpauth (_id INTEGER PRIMARY KEY, host TEXT, realm TEXT, username TEXT, password TEXT, UNIQUE (host, realm) ON CONFLICT REPLACE);", "method": "execSQL"}
```

`./com.appdlab.radarexpress`

```
D/StealthSpy(28243): {"class": "android.database.sqlite.SQLiteDatabase", "SQLStatement": "CREATE TABLE httpauth (_id INTEGER PRIMARY KEY, host TEXT, realm TEXT, username TEXT, password TEXT, UNIQUE (host, realm) ON CONFLICT REPLACE);", "method": "execSQL"}
```

Function tracing

Use this technique to determine how to decrypt data

```
± find . -name '*.logcat' | xargs -l{} grep -H "StealthSpy" {} | grep -i aes | head -n20
```

D/StealthSpy(16281):

./air.com.nbcuni.com.nbcports.liveextra

{"reflectedClassName":"com.android.org.bouncycastle.jcajce.provider.symmetric.AES\$ECB","method":"forName"}

D/StealthSpy(12147):

./se.ace.whatif

1. E/SNOOP (24234): SSL do handshake called
2. D/StealthSpy(24234): {"reflectedClassName":"com.android.org.conscrypt.OpenSSLCipher\$AES\$CBC\$PKCS5Padding","method":"forName"}
3. D/StealthSpy(24234): {"class":"android.database.sqlite.SQLiteDatabase","SQLStatement":"kv_store","method":"update"}
4. E/SNOOP (24234): {"call": "chmod", "args": ["/data/data/se.ace.whatif/shared_prefs/store_prefs.xml", 432], "ret": 0}
5. E/SNOOP (24234): {"call": "remove", "args": ["/data/data/se.ace.whatif/shared_prefs/store_prefs.xml.bak"], "ret": 0}

Extract SSL Session

Decrypt PCAP traffic later

E/SNOOP (24234): RSA Session-ID:

A195965ADB78DB31987C6946BA6BEEDE7EC8A31C0B5D6E8F408820C00A49845E Master-Key:
7C3ED12872AE7B7E17FF0E40207BE8378AC27A84DBA892DD9E0C54A01B5AA3082DE5FD7E1CCF124CBE15E5
905C983A65

E/SNOOP (24234): SSL do handshake called

E/SNOOP (24234): SSL do handshake called

E/SNOOP (24234): RSA Session-ID:

29D73C36D226A91349A19B50EC41C9CA9EC72E0F1D8E9A8A8D76B6E404E92FB8 Master-Key:
3664B0697C19119E6187EABE57B7C42A8E62514D6712510D00CA21EF6CAA4BAEF9253FBAB43A010544B0CF
F89C7773A

E/SNOOP (24234): SSL do handshake called

Sensitive Data Leak

Combine analysis, make human consumable

```
± curl -XGET -s "localhost:9395/issues/?q=path=(type),eq=sensitive-data-leak" | jq -c '[] .value | [.app.package, .app.version,.description]'
```

- ["com.SomeCam","5","Sends PII (password [url-encoded]) to a server in the clear."]
- ["Android.Project1Mgr","27","Sends PII (imei [url-encoded]) to a server in the clear."]
- ["org.CamPhotos","5","Sends PII (username [url-encoded]) to a server in the clear."]
- ["ZZZCatchall2","14","Sends PII (imei [md5]) to a server in the clear."]
- ["YYY.AAACam","5","Sends PII (email [original]) to a server in the clear."]
- ["Android.SomeApp","19","Sends PII (mac [original]) to a server in the clear."]

** package names changed are vulnerabilities not yet disclosed*

Plaintext Zip Download

Combine analysis, make human consumable

```
± curl -XGET -s "localhost:9395/issues/?q=path=(type),eq=plaintext-zip-download" | jq -c '[] .value | [.app.package, .app.version,.description, .url]'
```

- ["aa.bb.tv","20000","Downloads compressed (Zip) files in the clear and may be subject to multiple vulnerabilities.", "http://update2.someurl.net/update2/path/android_armv7a/p1505080.file"]
- ["bb.blitz","37","Downloads compressed (Zip) files in the clear and may be subject to multiple vulnerabilities.", "http://dds.cr.usgs.gov/srtm/version2_1/SRTM3/Africa/N31E035.hgt.zip"]
- ["cc.car.wash","1","Downloads compressed (Zip) files in the clear and may be subject to multiple vulnerabilities.", "http://assets-cdn.cc-car-wash.com/files/mobile/0.9.2/resources/stickeezez/res/anim_present_stamped2.zip"]
- ["dd.TravelWithMe","26","Downloads compressed (Zip) files in the clear and may be subject to multiple vulnerabilities.", "<http://ad.adlibr.com/ext/files/classes.dex.zip>"]

** package names changed are vulnerabilities not yet disclosed*

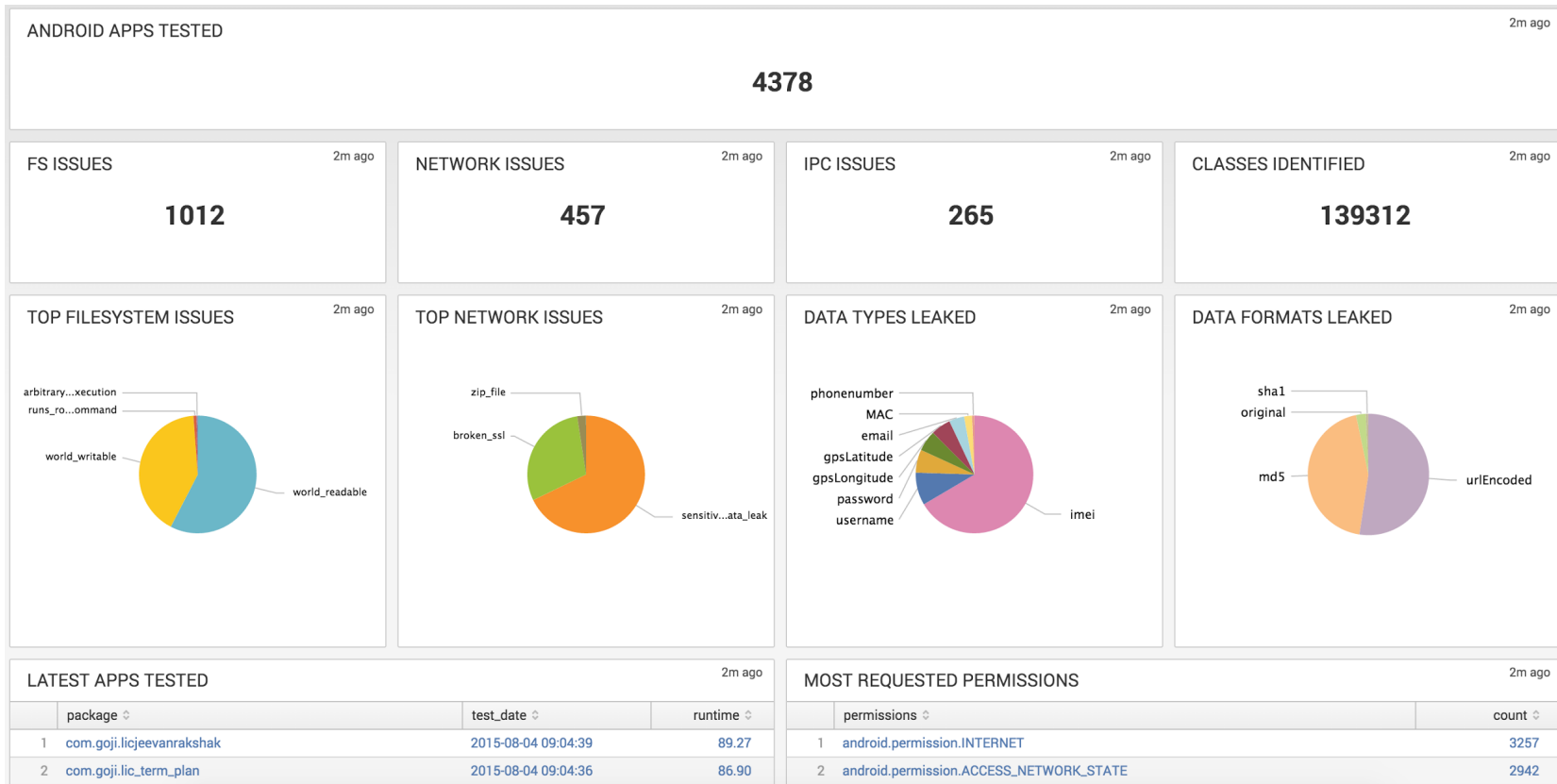
Broken TLS

Combine analysis, make human consumable

```
± curl -XGET -s "localhost:9395/issues/?q=path=(type),eq=broken-tls" | jq -c '[] .value | [.app.package, .app.version, .description, .url]'
```

- ["Com.AAA.Computer.Srsly","465","Has broken transport layer security.", "https://54.1.1./target/target-script-min.js"]

Mobile Intel - Android





On average, popular Android apps request

20 permissions

Top 15 permissions requested on android

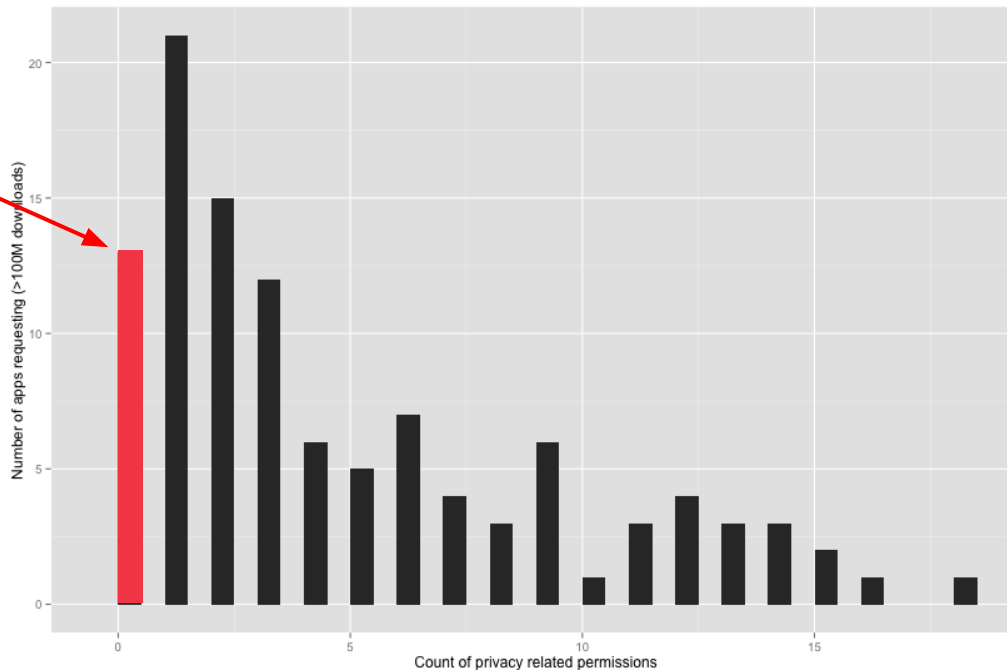
Permission	Apps Request	Dangerous
android.permission.INTERNET	86.830529%	Yes
android.permission.ACCESS_NETWORK_STATE	72.439761%	
android.permission.READ_EXTERNAL_STORAGE	58.710235%	
android.permission.WRITE_EXTERNAL_STORAGE	59.174426%	Yes
android.permission.READ_PHONE_STATE	42.392617%	Yes
android.permission.WAKE_LOCK	31.576694%	
android.permission.ACCESS_WIFI_STATE	28.764068%	Yes (Android M)
android.permission.VIBRATE	26.517248%	
android.permission.ACCESS_FINE_LOCATION	25.101242%	Yes
android.permission.ACCESS_COARSE_LOCATION	24.232722%	Yes
android.permission.GET_ACCOUNTS	19.902901%	
com.google.android.c2dm.permission.RECEIVE	18.859697%	
android.permission.CAMERA	14.934632%	Yes
android.permission.RECEIVE_BOOT_COMPLETED	9.944634%	
com.android.vending.BILLING	8.936366%	

Popular apps and privacy related permissions?

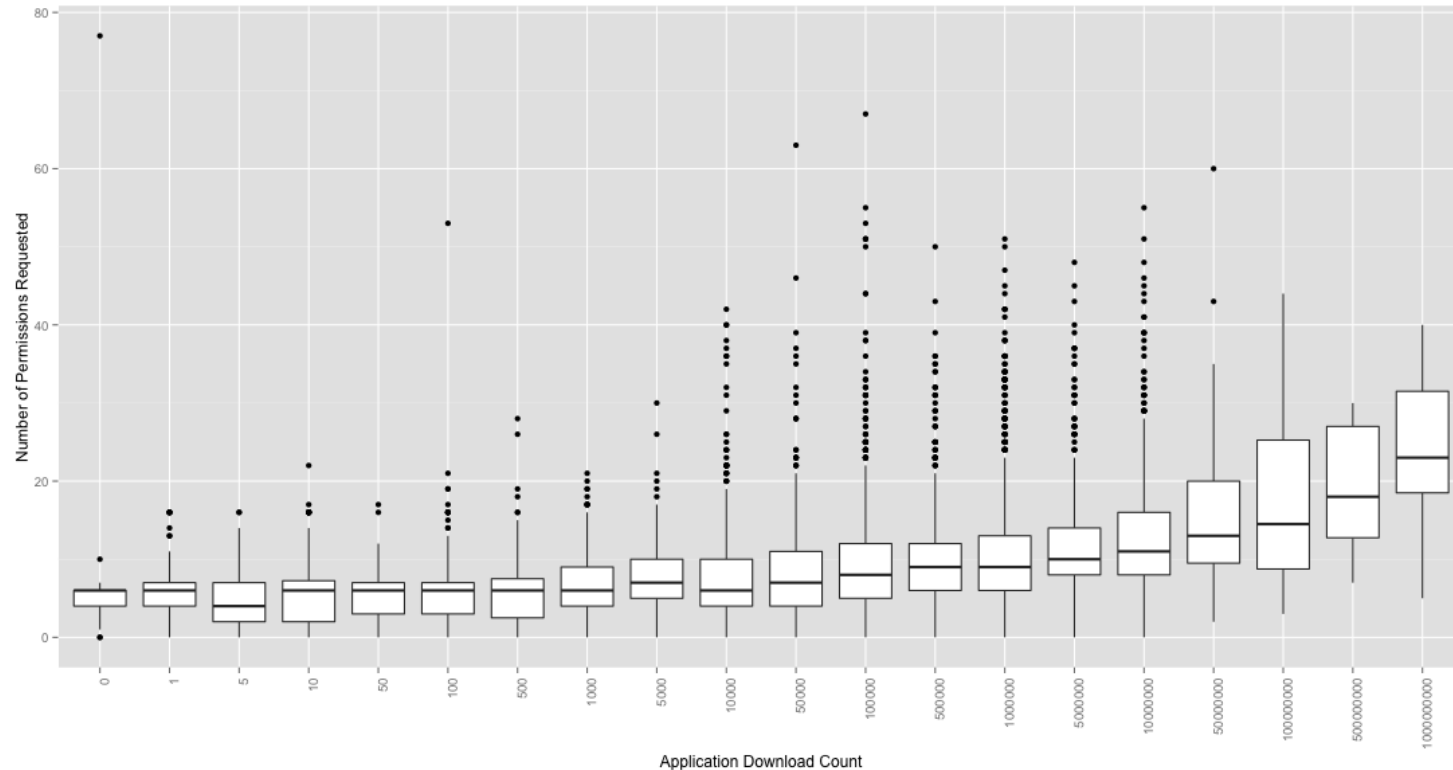
more than 100M downloads

READ_SMS
RECEIVE_SMS
RECEIVE_MMS
READ_PHONE_STATE
READ_CALL_LOG
READ_CONTACTS
WRITE_CONTACTS
READ_HISTORY_BOOKMARKS
WRITE_HISTORY_BOOKMARKS
READ_PROFILE
WRITE_PROFILE
READ_SOCIAL_STREAM
WRITE_SOCIAL_STREAM
READ_CALENDAR
WRITE_CALENDAR
READ_USER_DICTIONARY
WRITE_USER_DICTIONARY
ADD_VOICEMAIL
GET_ACCOUNTS
MANAGE_ACCOUNTS
RECORD_AUDIO
CAMERA
ACCESS_FINE_LOCATION
ACCESS_COARSE_LOCATION

only 13 out of 118 apps
did not ask for any
dangerous permissions

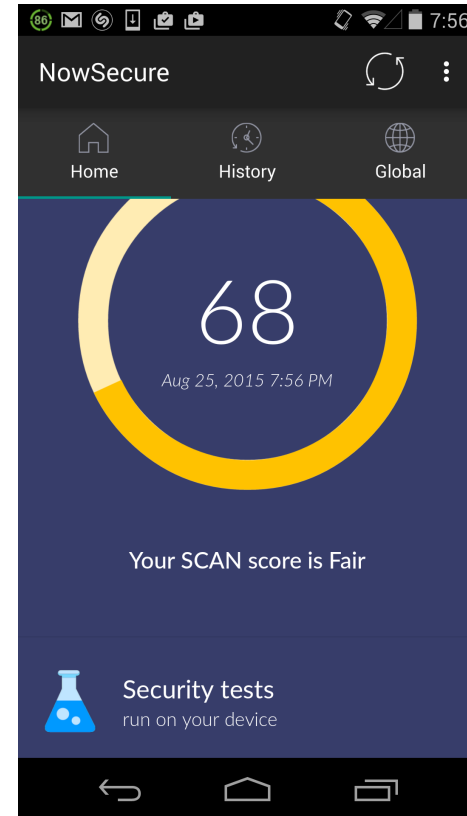


App download count vs # permissions requested



Additional Data Sources

NowSecure Mobile





Data from

188

Countries

United States -	15.06%	India -	2.46%
United Kingdom -	8.10%	Belgium -	2.43%
Iran -	7.97%	Italy -	2.26%
Netherlands -	5.67%	Malaysia -	2.00%
Canada -	4.58%	Mexico -	1.66%
Thailand -	4.42%	Indonesia -	1.66%
Germany -	4.24%	Romania -	1.54%
Brazil -	3.94%	Turkey -	1.17%
Australia -	2.57%	Greece -	1.17%
Vietnam -	2.54%	Russian Federation -	1.11%

A world map with a light blue background. The map shows the outlines of continents and countries. Overlaid on the map is the text 'NowSecure Forensics CE Usage' in a dark grey font, followed by a large black number '44', and then the word 'Countries' in a dark grey font. The map highlights 44 countries in a darker shade of blue, indicating where the software is used. These countries are primarily located in North America, Europe, and Australia, with some scattered locations in South America and Africa.

NowSecure Forensics CE Usage

44

Countries

 NowSecure™

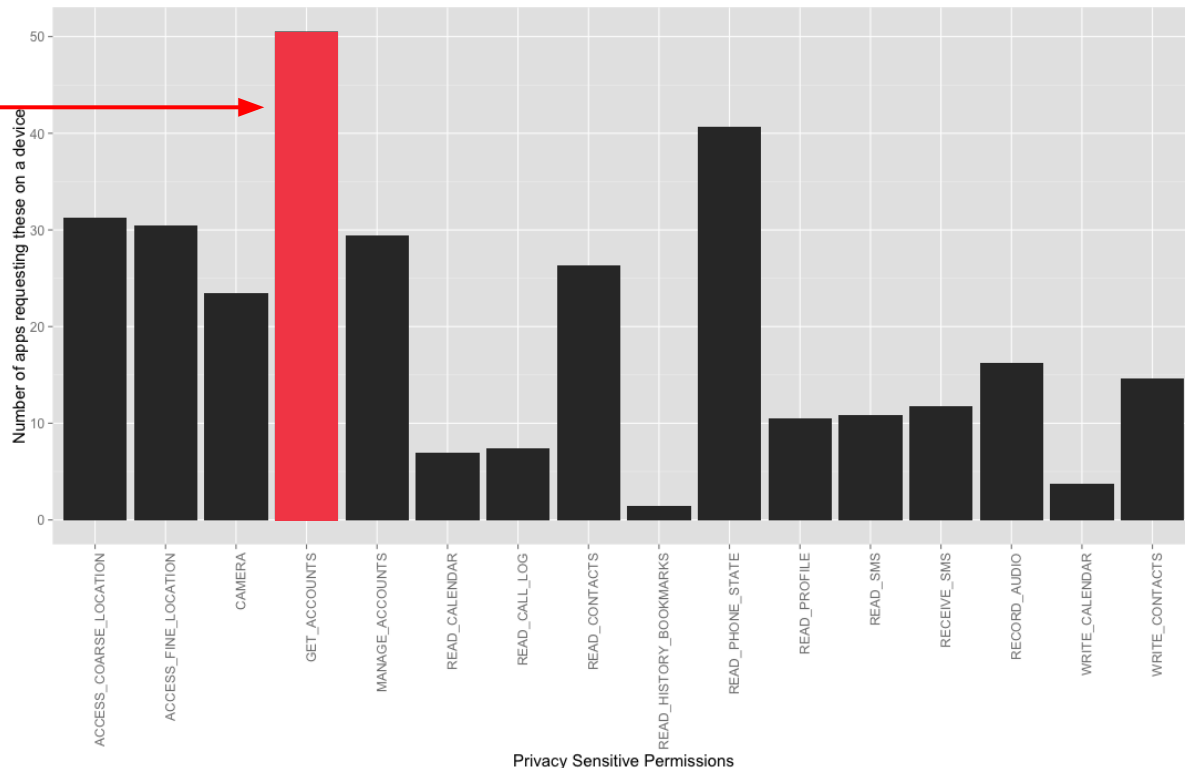
© Copyright 2015 NowSecure, Inc. All Rights Reserved. Proprietary information.

44

Countries

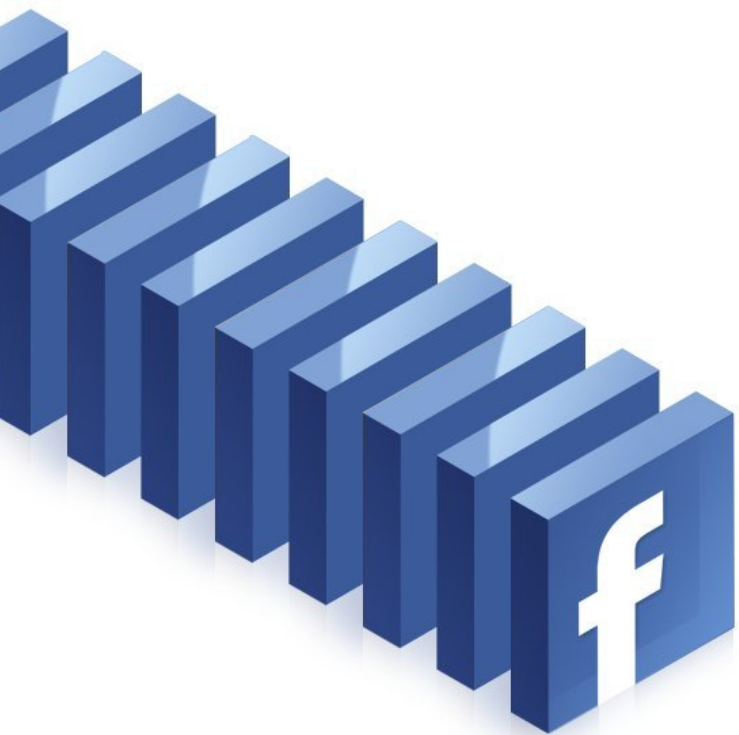
Apps requesting sensitive permissions on a user's device

50 apps per device have access to all the user accounts on the device, including emails, social media handles, etc.



Mobile Device Attributes

	Global
PIN/Pattern/Passcode Enabled	61%
ADB Enabled	20%
Install Unknown Sources	43%
Encryption Enabled	4%
Running Latest O/S	73%



277

versions of the Facebook app
currently in use

Successful root exploits

Samsung

- google/sojus/crespo4g:4.0.4/IMM76D/299849:user/release-keys
- samsung/espressorfxx/espressorf:4.1.2/JZO54K/P3100XXDMC1:user/release-keys
- samsung/m0xx/m0:4.1.2/JZO54K/I9300XXELLA:user/release-keys
- google/soju/crespo:4.1.2/JZO54K/485486:user/release-keys
- samsung/GT-N7000/GT-N7000:4.1.2/JZO54K/N7000XXLT4:user/release-keys
- Verizon/jaspervzw/jaspervzw:4.1.2/JZO54K/I200VRBME1:user/release-keys
- samsung/kona3gxx/kona3g:4.1.2/JZO54K/N5100XXBMD1:user/release-keys
- google/mysid/toro:4.2.2/JDQ39/573038:user/release-keys
- samsung/goldennfcxx/golden:4.1.2/JZO54K/I8190NXXAMG1:user/release-keys
- samsung/GT-I9070/GT-I9070:2.3.6/GINGERBREAD/XXLE2:user/release-keys

HTC

- sprint/htc_shooter/shooter:4.0.3/IML74K/409645.2:user/release-keys
- verizon_wwe/htc_vivow/vivow:2.3.4/GRJ22/\$:user/release-keys
- VERIZON/HTCOneVZW/m7wlv:4.4.2/KOT49H/304035.1:user/release-keys
- htc_asia_india/htc_chacha/chacha:2.3.3/GRI40/77217:user/release-keys
- htc_europe/htc_marvel/marvel:2.3.5/GRJ90/362953.4:user/release-keys

LGE

- lge/e0_open_eur/e0:2.3.6/GRK39F/V10q-DEC-05-2012.2ED92C3F11:user/release-keys

ZTE

- ZTE/P765V20/seanplus:4.1.1/JRO03C/20130719.183904.1197:user/release-keys
- zte/zte_nex/nex:4.1.2/JZO54K/20140605.101842.25315:user/release-keys
- TCT
- TCT/Diablo/Diablo:4.1.1/JRO03C/vPB8-0:user/release-keys
- TCT_MetroPCS/Rav4_MetroPCS/Rav4:4.2.2/JDQ39/vM32-0:user/release-keys

Use Cases

Forensics

- Which forensic technique might work on a device
- What metadata should be collected during a forensics acquisition
 - What apps are popular
 - How do they use device properties to encrypt data
- If you get a device image but not device and/or app metadata
 - Identify app & version by “file system signature”
 - Decrypt data for apps already analyzed

Analysis

- What data leaks out over the network? On the file system?
- If you need to determine all the email aliases for a device, where can you find them?
- What popular Wi-Fi networks are in use:
 - What are the properties of the Wi-Fi (open, WEP, WPA)

Defense

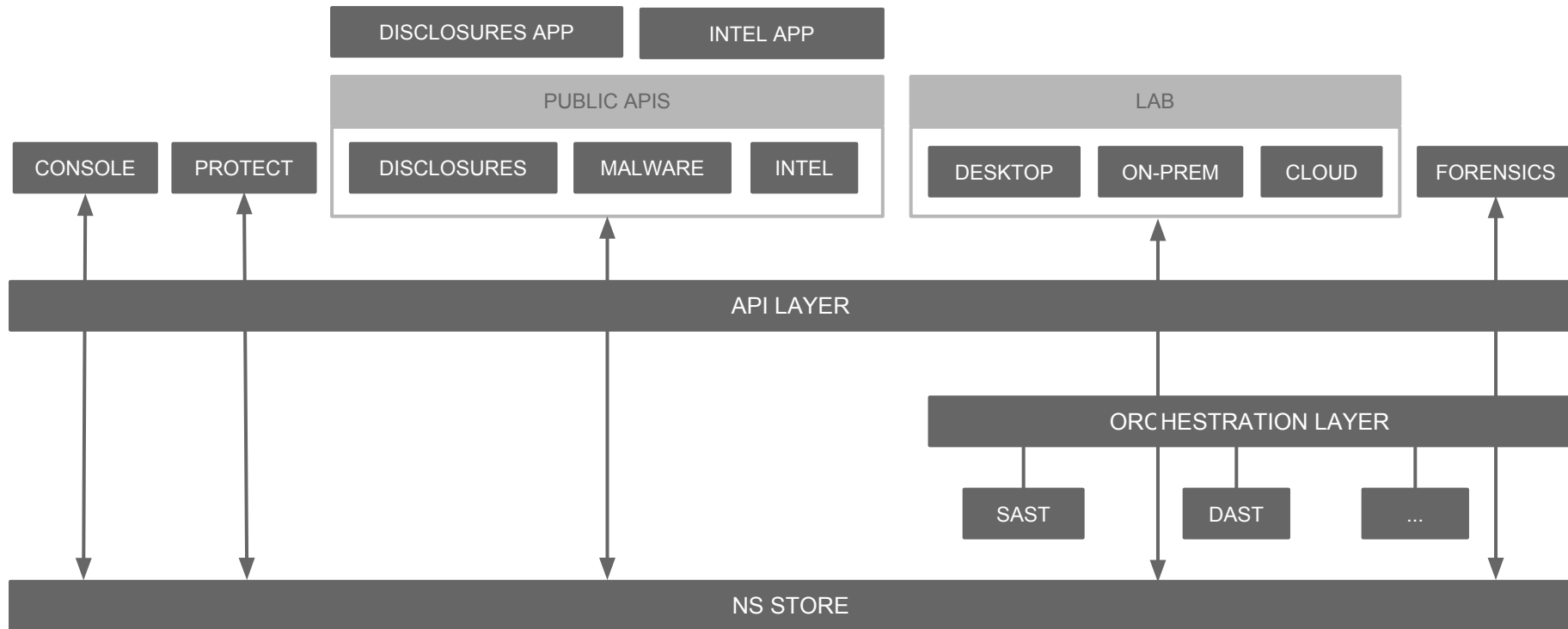
- Which apps leak sensitive data
- Which devices are not susceptible to forensic acquisition
- What apps are popular in a region
- What WiFi or Cellular networks actively poison DNS or attempt to resign SSL

Making Mobile Security Social

Our vision for the future

NowSecure Platform

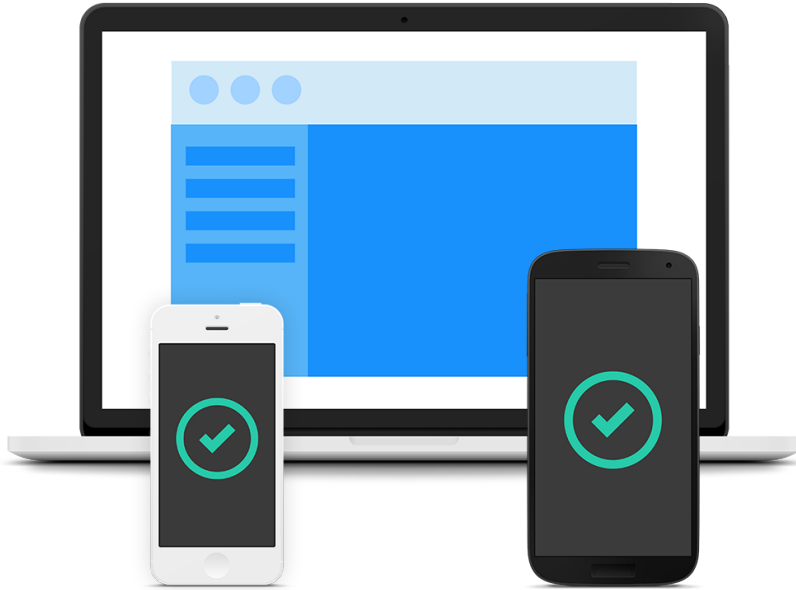
Functional Hierarchy



Key social attributes

- Full API and CLI support, fully documented
- Extensible (apps consuming APIs, plug in new analysis engines to the orchestration layer)
- SaaS supporting web and cross-platform desktop apps (via @electronjs)
- Deep linking
- Free for non-commercial use, including:
 - Security researchers
 - Academia, including professors and students
 - Individuals

The Future of Mobile Security



- Old models (anti-malware signature checking), time consuming human analysis are not effective, don't scale to the problem
- This data-centric approach can be broadly applied, including forensics, analysis and defensive measures
- Mobile security industry must leverage automation, crowdsourced data and analytics to secure the mobile future

Acknowledgements

- Special thanks & greetings to the team at NowSecure who has made all this possible
 - Research team (lead by @insitusec)
 - Engineering team (led by @hij1nx)



DON'T PANIC!

Andrew Hoog // CEO, Co-Founder

ahoog@nowsecure.com

+1 312.878.1100

@ahoog42