lookout™

App Attack

Surviving the explosive growth of mobile apps.

Kevin Mahaffey
CTO, Lookout

John Hering
CEO, Lookout

Hi.

- Kevin Mahaffey → @dropalltables
- John Hering
- We like to think about Mobile Security, RFID, Privacy

  Blackhat, Defcon, Bluehat

Vuln

Android Logging Subsystem

- Android has a system log for debugging

  Accessible by applications via logging APIs or /dev/log device

  Requires READ_LOGS permission.

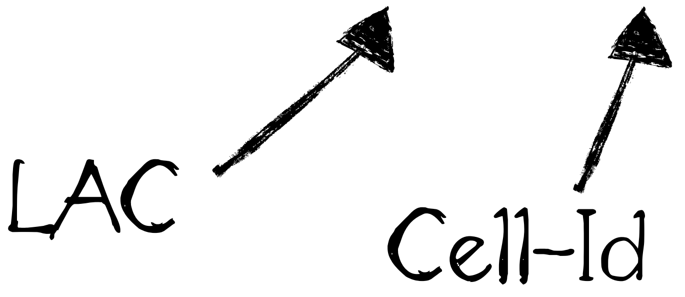
Location Disclosure Vuln

- LocationManager discloses Cell-Id and LAC into system logs

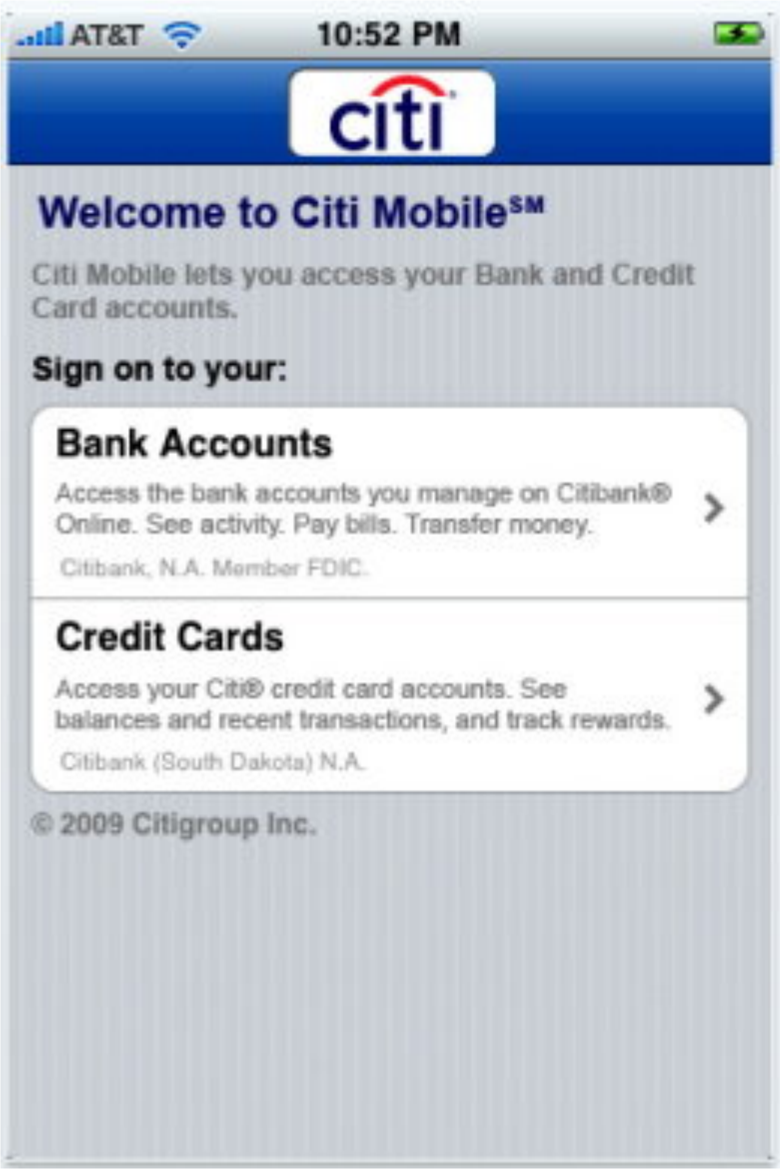
  This gives approximate location to any apps that bother to look in the logs

- Fixed in 2.2/Froyo

```
D/NetworkLocationProvider(71): onCellLocationChanged [6044,1006]
```



Information Leakage Example: Citibank



Welcome to Citi Mobile℠

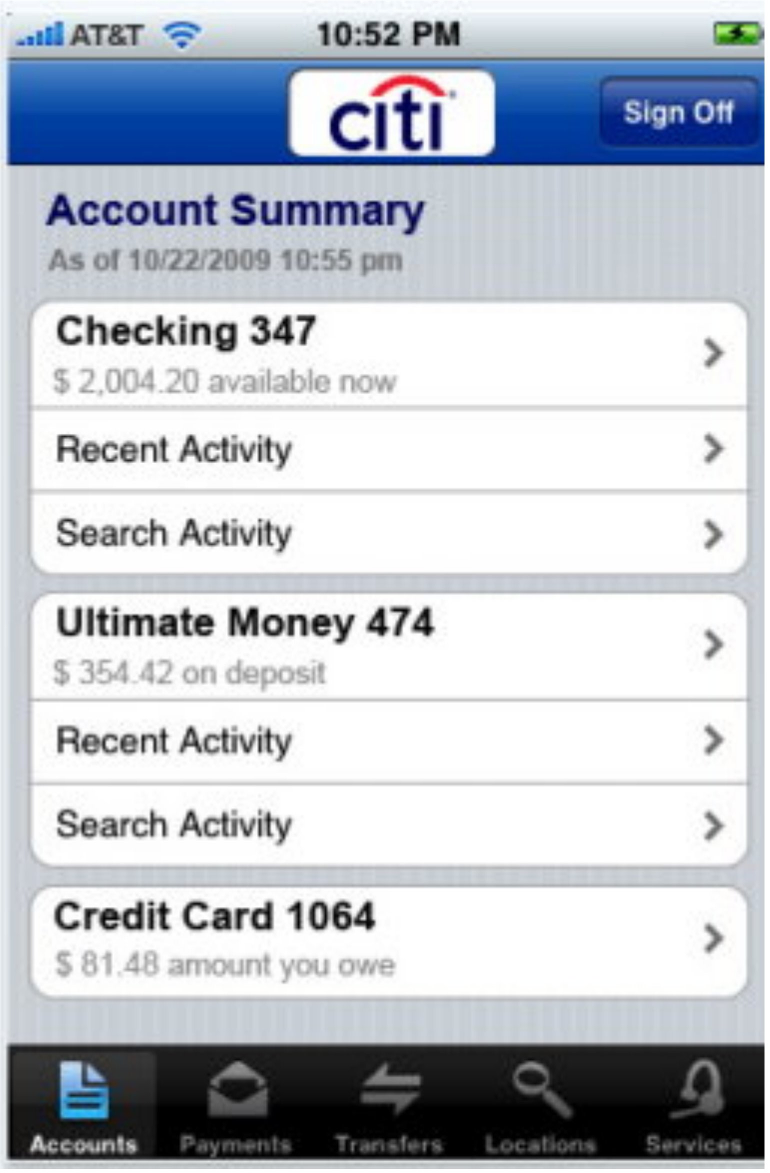
Citi Mobile lets you access your Bank and Credit Card accounts.

Sign on to your:

Bank Accounts
Access the bank accounts you manage on Citibank® Online. See activity. Pay bills. Transfer money.
Citibank, N.A. Member FDIC.

Credit Cards
Access your Citi® credit card accounts. See balances and recent transactions, and track rewards.
Citibank (South Dakota) N.A.

© 2009 Citigroup Inc.



Account Summary
As of 10/22/2009 10:55 pm

Checking 347
$ 2,004.20 available now
Recent Activity
Search Activity

Ultimate Money 474
$ 354.42 on deposit
Recent Activity
Search Activity

Credit Card 1064
$ 81.48 amount you owe

Account Hijacking

- Many applications log URLs they hit to the system log

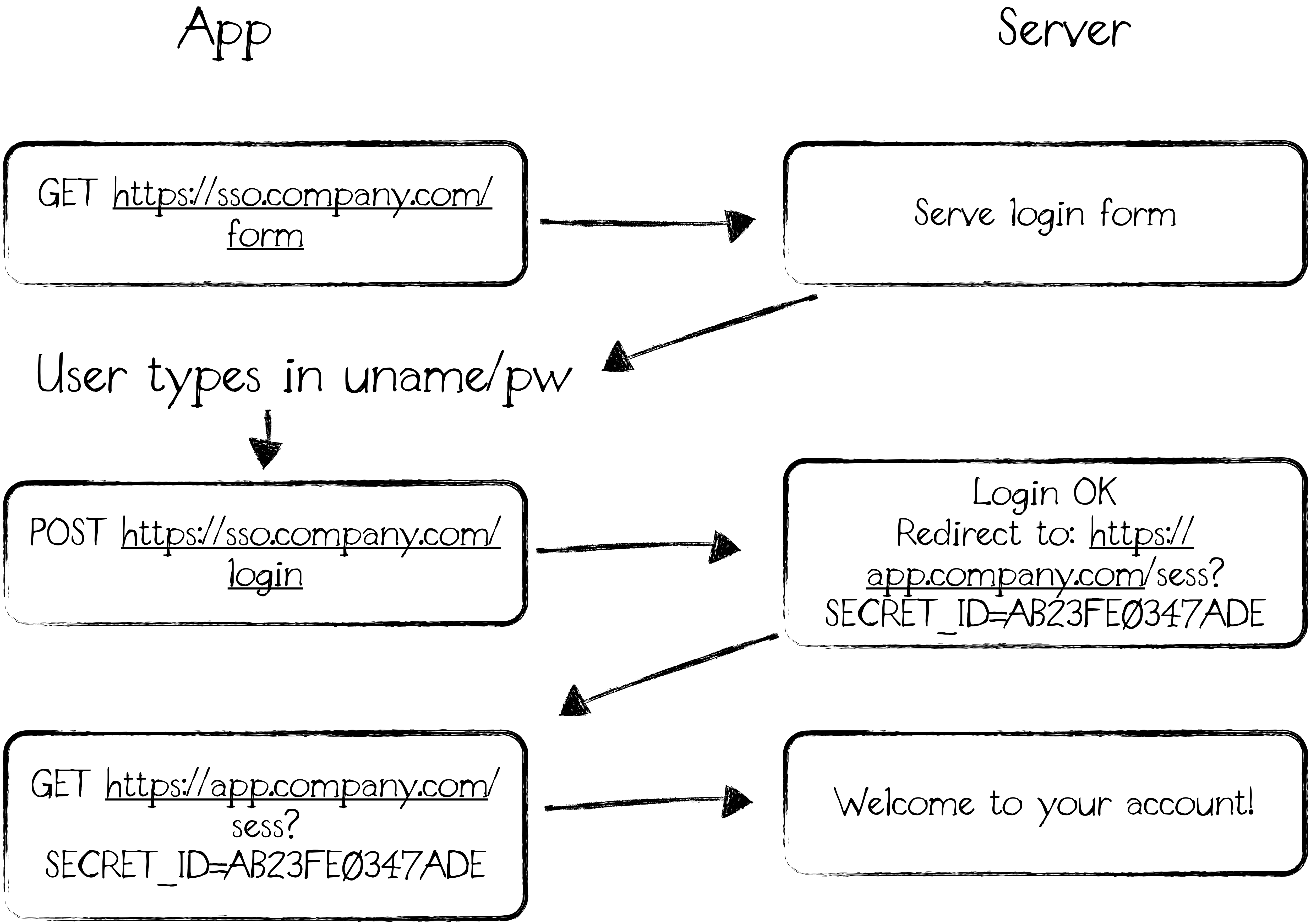
  Including the android browser in certain circumstances

```
I/SearchDialog: Starting (as ourselves)
#Intent;action=android.intent.action.SEARCH;launchFlags=0x
10000000;component=com.android.browser/.BrowserActivity;S.
query=www.blackhat.com;S.user_query=www.blackhat.com;end
```

Browser

Another app

```
D/com.company.app(1): getUrl = https://
onlineservice.company.com/login/LoginForm
```



App

Server

GET https://sso.company.com/form

Serve login form

User types in uname/pw

POST https://sso.company.com/login

Login OK
Redirect to: https://app.company.com/sess?SECRET_ID=AB23FE0347ADE

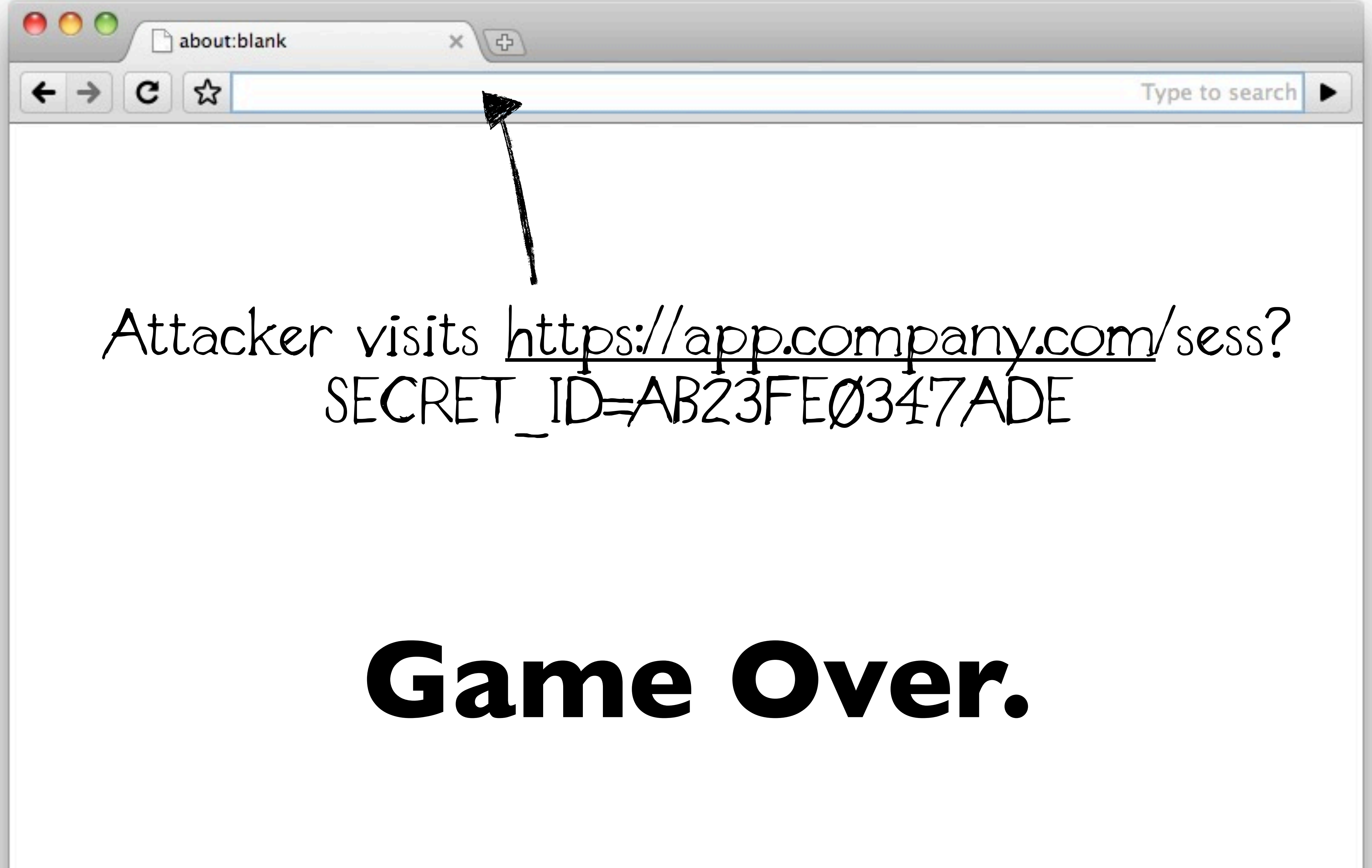
GET https://app.company.com/sess?SECRET_ID=AB23FE0347ADE

Welcome to your account!

What do the logs say?

```
D/com.company.app(1): getUrl = https://sso.company.com/form

...

D/com.company.app(1): postUrl = https://sso.company.com/login

...

D/com.company.app(1): getUrl = https://app.company.com/sess?
SECRET_ID=AB23FE0347ADE
```

Malicious application reads logs from device and transmits them to attacker.



Attacker visits https://app.company.com/sess?SECRET_ID=AB23FE0347ADE

Game Over.

Lessons Learned

- App developers: don't log anything confidential.
- Web developers: don't put sensitive parameters in GET query strings.

  Especially if an application may log it or the URL is being sent between apps.

What if you could ask questions about every app in the world?

App Genome Project

Largest-ever Mobile App Dataset.

- Nearly 300,000 apps encountered.
- iPhone App Store + Android Market.
- Analyzed nearly 100,000 free apps.
- Metadata + application binaries.

Agenda

- Why care about mobile apps?
- Why build the App Genome Project?
- How did we build it?
- What did we find?
- Using the App Genome Project for security response.
- What apps may come?

Why care about mobile Apps?

Mobile Apps Matter.

- Smartphones are becoming the computing platform.

  54.3 million devices shipped in Q1 2010. (Gartner)

- People who use apps, use a lot of them.

  22 apps per smartphone in US. (Nielsen)

- Apps access sensitive information and can charge $$$.

  Bank accounts, location, SMS billing, premium phone calls, email, text messages, etc.

Why care about Apps?

- What enables attacks

  Standardized APIs (e.g. contact list on a computer is complicated)

  Capabilities (e.g. browser history, dialing)

- What incentivizes attackers

  $$$ (direct or indirect)

  Sensitive information

Why mobile threats won't matter?

- Isn’t mobile fragmented

  There are 3 windows.

- Isn’t there a sandbox?

  Sandbox != safe.

- Isn’t there a small attack surface?

  Apps, push services, messaging services, etc.

  App stores are a choke-point for distribution

Why did we build the App Genome Project?

Why?

- Ultimately, to keep people safe.

  Good data helps everyone make good security decisions.

- Identify threats in the wild.

  Analytics to identify high-risk apps based on behavior.

- Understand platform differences.

  Compare Android vs. iPhone.

- See what apps are ***actually*** doing.

  Is this the same as what they ***say*** they're doing?

How did we build the App Genome Project?

Overview

- Distributed crawler

  Speaks Android Market and Apple App Store

- Data store

  Keep metadata and downloads around for offline analysis

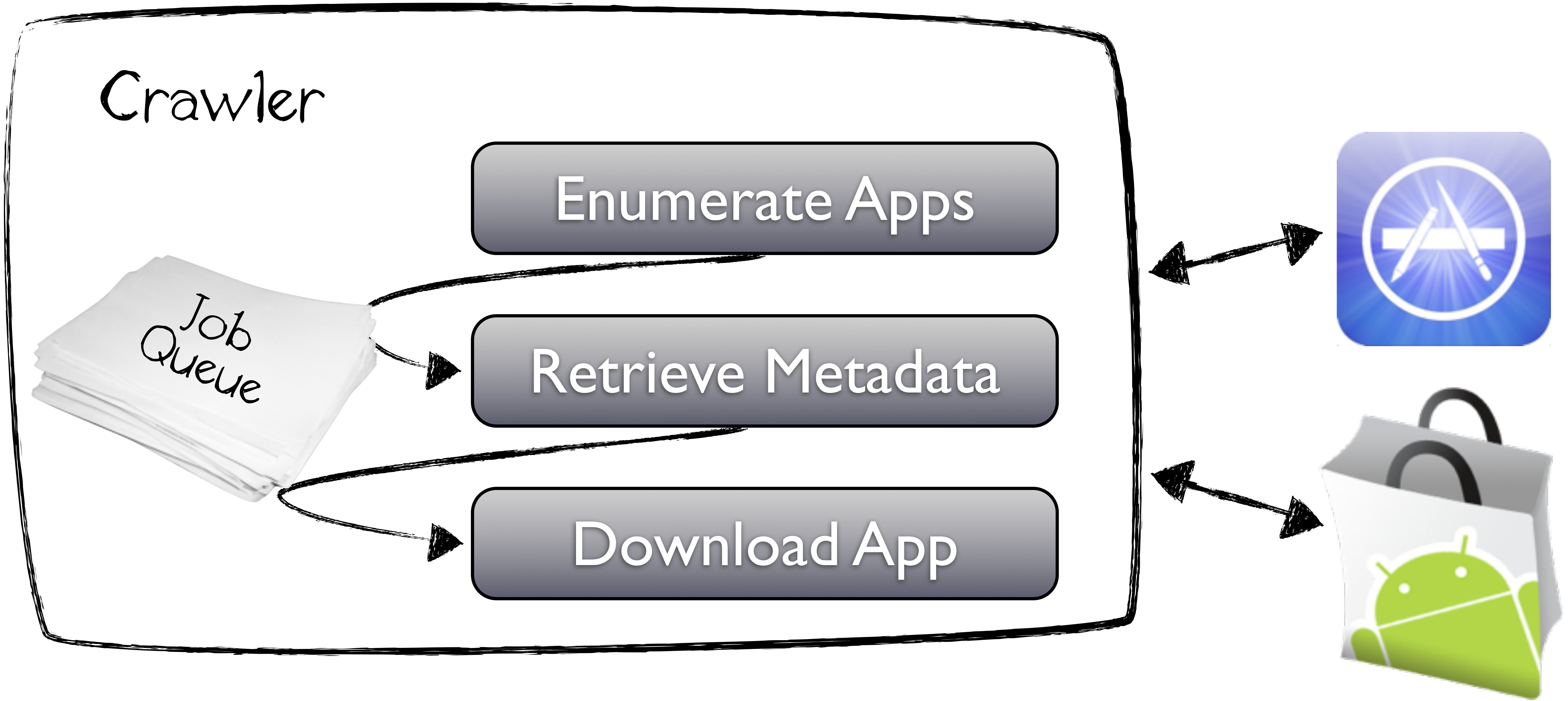
- Custom analysis tools

  OS-specific analysis to sequence capabilities

- The crawler is a series of jobs.

  It's not like a truck.

- Each job queues other jobs using a job queue.



Data Store

- Application Metadata → MySQL

  Description, Ratings, Version, Creator, Permissions (Android)

- Application Binaries → Filesystem

  For free applications only

- Changes tracked over time

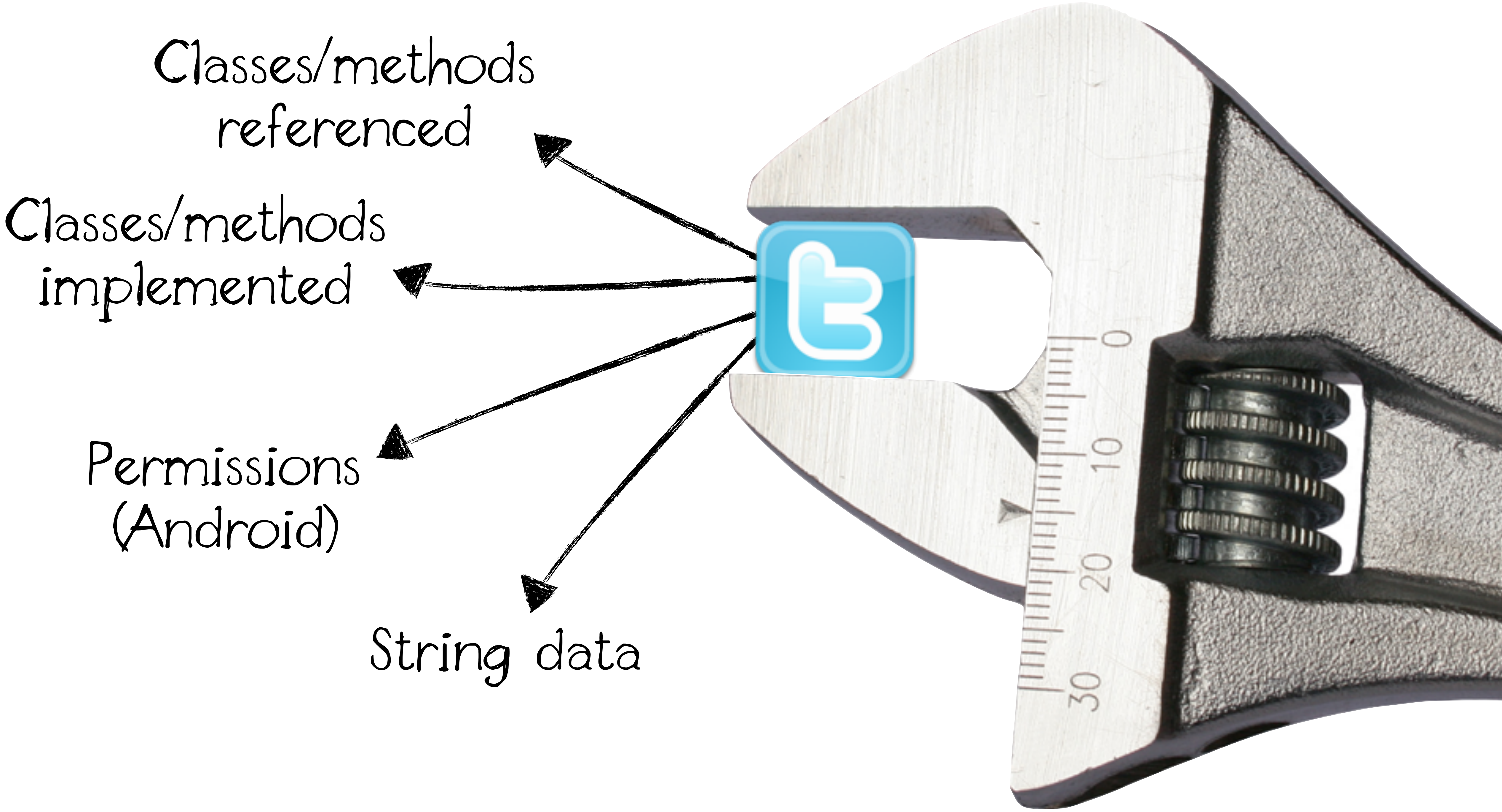
  Both metadata and binaries

1. Download ~100k mobile apps

2. ???

3. Profit!

We built custom static analysis tools to automate feature extraction



Classes/methods referenced

Classes/methods implemented

Permissions (Android)

String data

Analyzing Android

Dalvik is here

Anatomy of an Android App

- Applications run in a virtual machine called Dalvik.
- APK file format - very similar to a Java JAR.

  Just a zip archive
- “classes.dex” is the main Dalvik executable.
- “AndroidManifest.xml” is a binary XML document describing permissions, application components, etc.

Android Security Model

- Granular permissions for specific capabilities.

  Read Contacts, Send SMS, Read Logs, Internet, etc.

- Apps declare permissions at install.

  Acceptance is before download on the Android Market.

- Enforcement at process level.

  Common misconception: enforcement by the VM.

Analysis Methodology

- Package permissions + DEX (Dalvik executable) static analysis

  e.g permission requested + API referenced by “classes.dex”

- Define heuristics for features we want to extract

  e.g. reading the device’s phone number =>
  READ_PHONE_STATE permission + reference to
  TelephonyManager#getLine1Number

- ...or run arbitrary analysis queries against all apps

Analysis Constraints

- Apps ~~are not~~ shouldn't be able to exceed declared permissions.

  We look for vulnerability exploitation as special features.

- Capabilities can be implemented outside of Dalvik.

  Native code can interact directly with Binder, network, etc.

  Apps can dynamically pull code from the internet.

- Currently, we're not looking for:

  Code downloaded at runtime

  Evasive code (e.g. encrypted, obfuscated)

  Raw IPC calls or dynamic linkage

Analyzing iPhone

iPhone Security Model

- Process-level sandboxing.
- App-store API enforcement.

  Private/undocumented APIs prohibited, though technically accessible.
- User acknowledgement for certain capabilities

  e.g. location, push

Anatomy of an iPhone App

- IPA file

  Just a zip archive

- Application binary typically in "/Payload/AppName.app/AppName"

- Mach-O executable

Mach-O

- Header contains a series of load commands.

  Specify segmentation, runtime linkage, encryption, etc.

- A Mach-O file contains multiple segments, e.g.

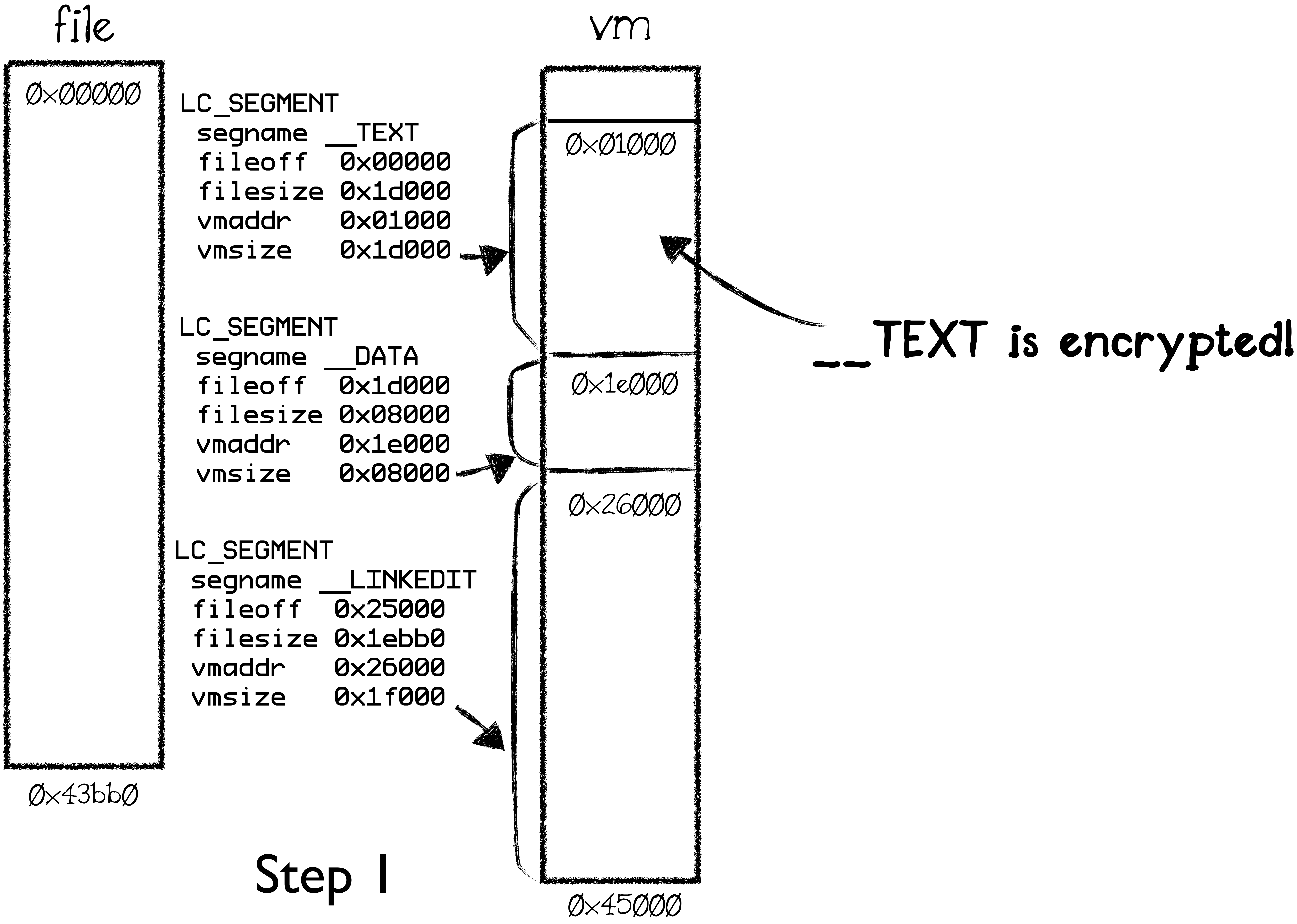
  __TEXT (executable code/read-only data)

  __DATA (writable data)

  __LINKEDIT (dynamic linker data)

- Each segment *has many* sections.

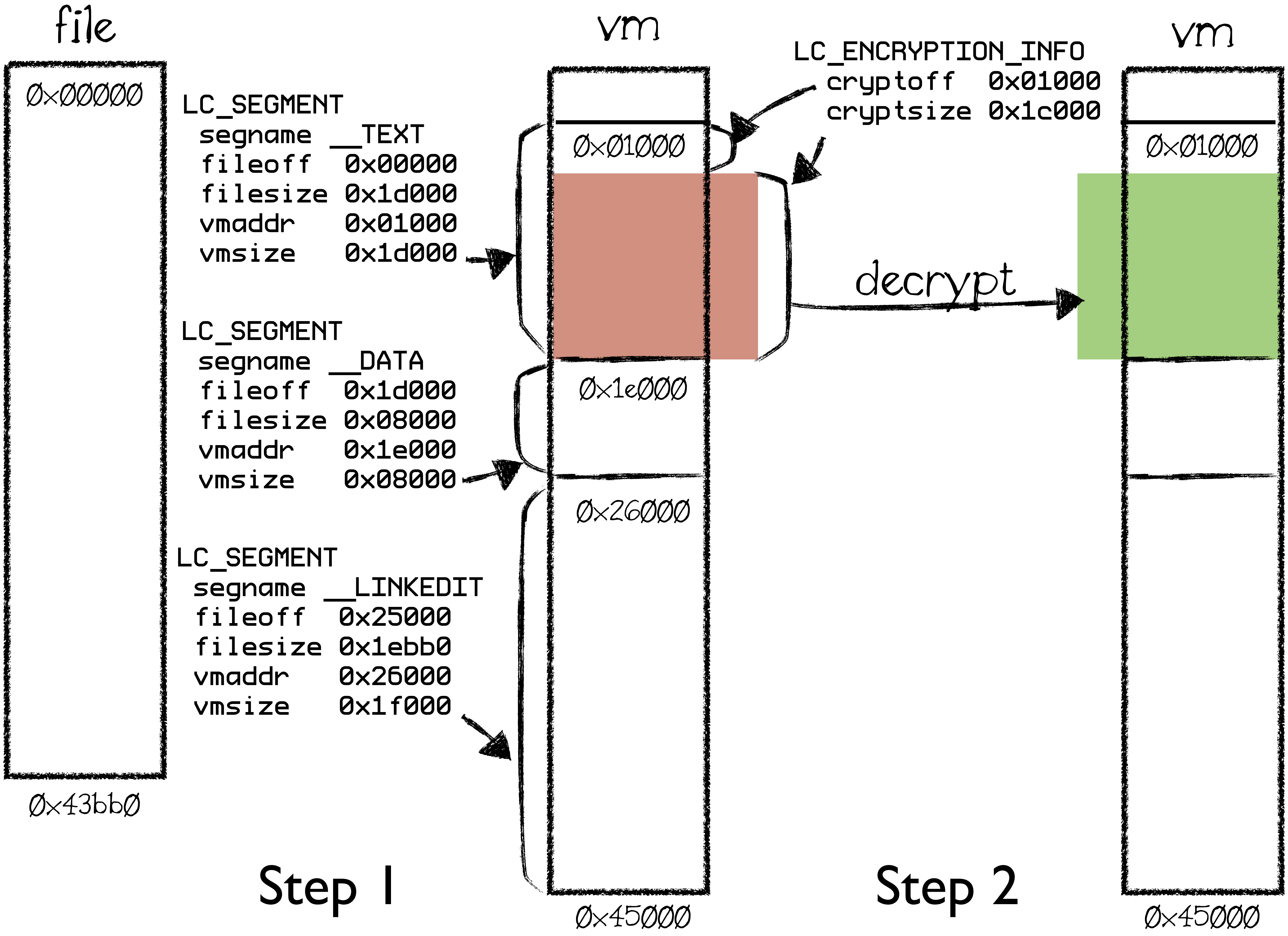
- iPhone apps are encrypted!



```
LC_SEGMENT
 segname  __TEXT
 fileoff   0x00000
 filesize 0x1d000
 vmaddr   0x01000
 vmsize   0x1d000

LC_SEGMENT
 segname  __DATA
 fileoff   0x1d000
 filesize 0x08000
 vmaddr   0x1e000
 vmsize   0x08000

LC_SEGMENT
 segname  __LINKEDIT
 fileoff   0x25000
 filesize 0x1ebb0
 vmaddr   0x26000
 vmsize   0x1f000
```

__TEXT is encrypted!

Step 1



```
LC_SEGMENT
 segname  __TEXT
 fileoff   0x00000
 filesize 0x1d000
 vmaddr    0x01000
 vmsize    0x1d000

LC_SEGMENT
 segname  __DATA
 fileoff   0x1d000
 filesize 0x08000
 vmaddr    0x1e000
 vmsize    0x08000

LC_SEGMENT
 segname  __LINKEDIT
 fileoff   0x25000
 filesize 0x1ebb0
 vmaddr    0x26000
 vmsize    0x1f000
```

```
LC_ENCRYPTION_INFO
 cryptoff   0x01000
 cryptsize 0x1c000
```

Step 1

Step 2

```
#if CONFIG_CODE_DECRYPTION

static load_return_t
set_code_unprotect(
         struct encryption_info_command *eip,
         caddr_t addr,
         vm_map_t map,
         struct vnode  *vp)
{
   int result, len;
   char vpath[MAXPATHLEN];
   pager_crypt_info_t crypt_info;
   const char * cryptname = 0;

   size_t offset;
   struct segment_command_64 *seg64;
   struct segment_command *seg32;
   vm_map_offset_t map_offset, map_size;
   kern_return_t kr;

   if (eip->cmdsize < sizeof(*eip))
      return LOAD_BADMACHO;
```

Go here for the juicy details

http://www.opensource.apple.com/source/xnu/xnu-1504.7.4/bsd/kern/mach_loader.c

```
      case 1:
         cryptname="com.apple.unfree";
         break;
      case 0x10:
         /* some random cryptid that you could manually put into
          * your binary if you want NULL */
         cryptname="com.apple.null";
         break;
```

What can we see?

- We're not currently decrypting the __TEXT segment.

- Symbol tables are stored in the __LINKEDIT segment.

  Not encrypted. ← Yay!

- Runtime framework linking implemented by Mach-O load commands.

  Also not encrypted. ← Again, yay!

Analysis Methodology

- Symbol table includes defined (implemented) and undefined (referenced) symbols.

  C functions, Obj-C classes/methods/ivars

- Mach-O load commands specify frameworks imported at runtime.

- Define heuristics for each feature we extract

  e.g. Accessing a device's contacts => reference to any of the AddressBook API data access methods.

- ...or run arbitrary analysis queries against all apps.

Analysis Constraints

- We’re not decrypting the __TEXT segment of apps.

- Currently, we’re not looking for:

  Dynamically loaded code (constants stored in __TEXT).

  Bypassing frameworks to access data via private APIs.

  Code downloaded at runtime.

So...

- We downloaded free Android + iPhone binaries.

  Lots of them.

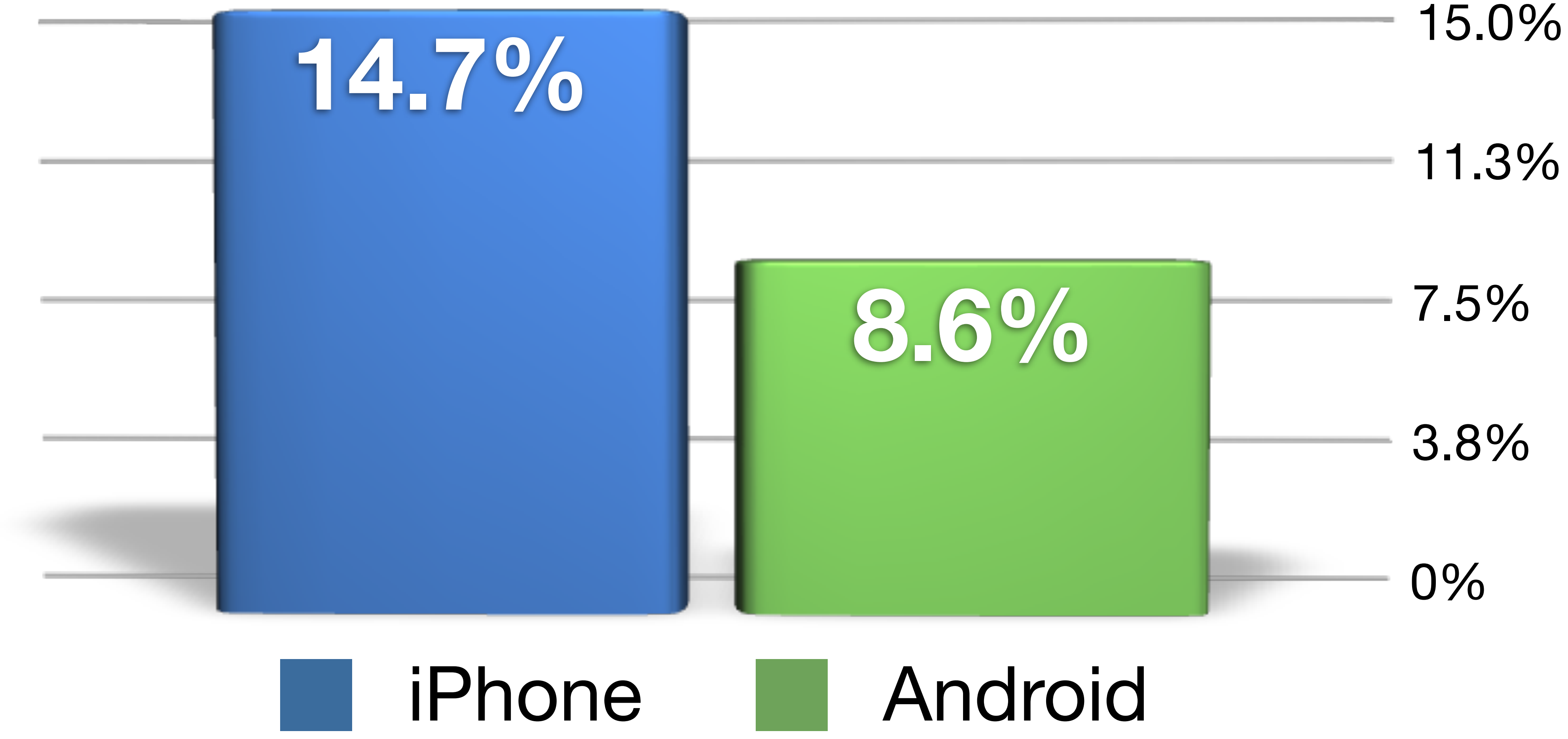
- We built analysis tools that allow us to ask questions of the apps *en masse.*

  ...so we don't have to do it manually.

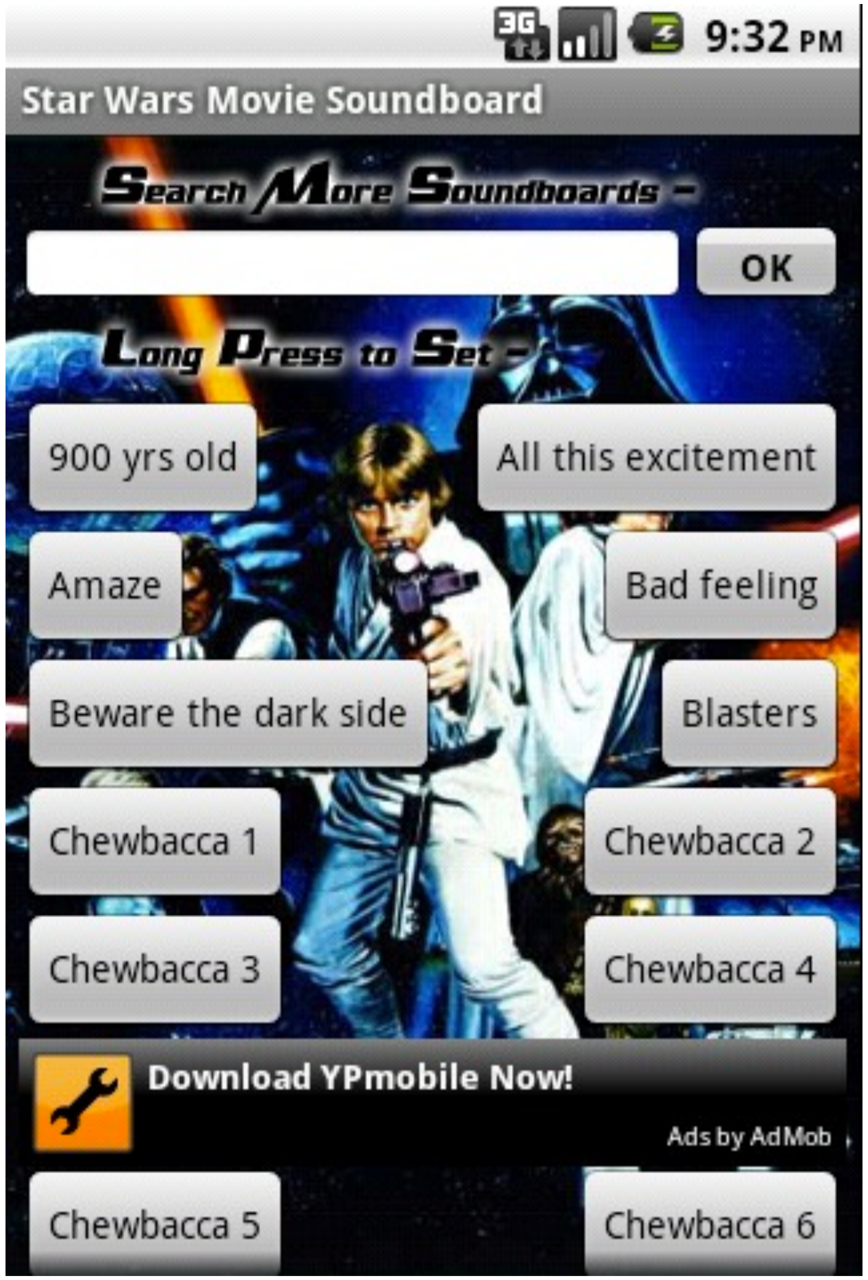
What did we find?

Story #1:
In the beginning there was data.

Free Apps Reading Contacts



- Are there any apps accessing my contacts that shouldn’t be?



- We found a seemingly suspicious series of sound boards on Android

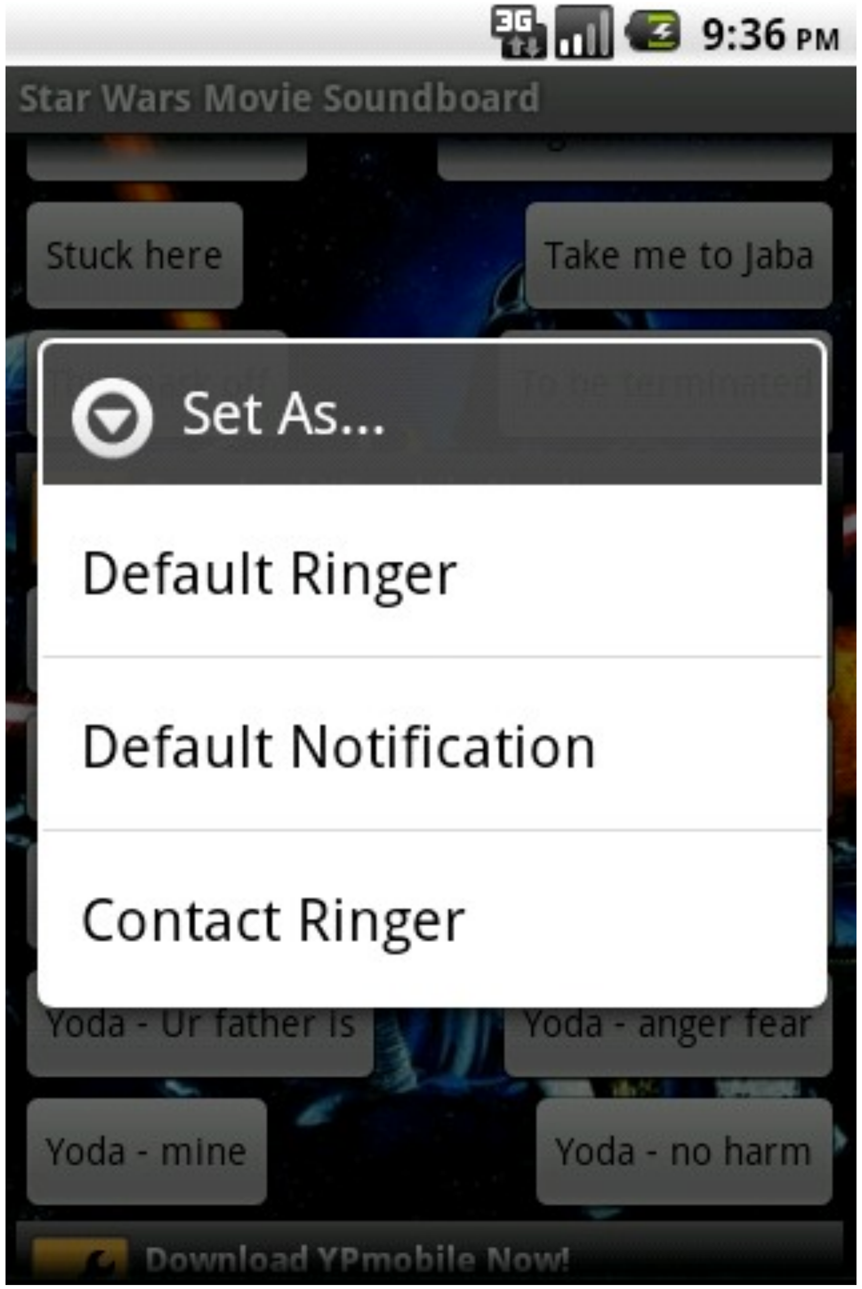
- Requests WRITE_CONTACTS

- References Contact API

```
sget-object v7, android/provider/ContactsContract$Contacts;-
>CONTENT_URI
```

- Accesses contacts to set custom ringers.

  Totally legitimate



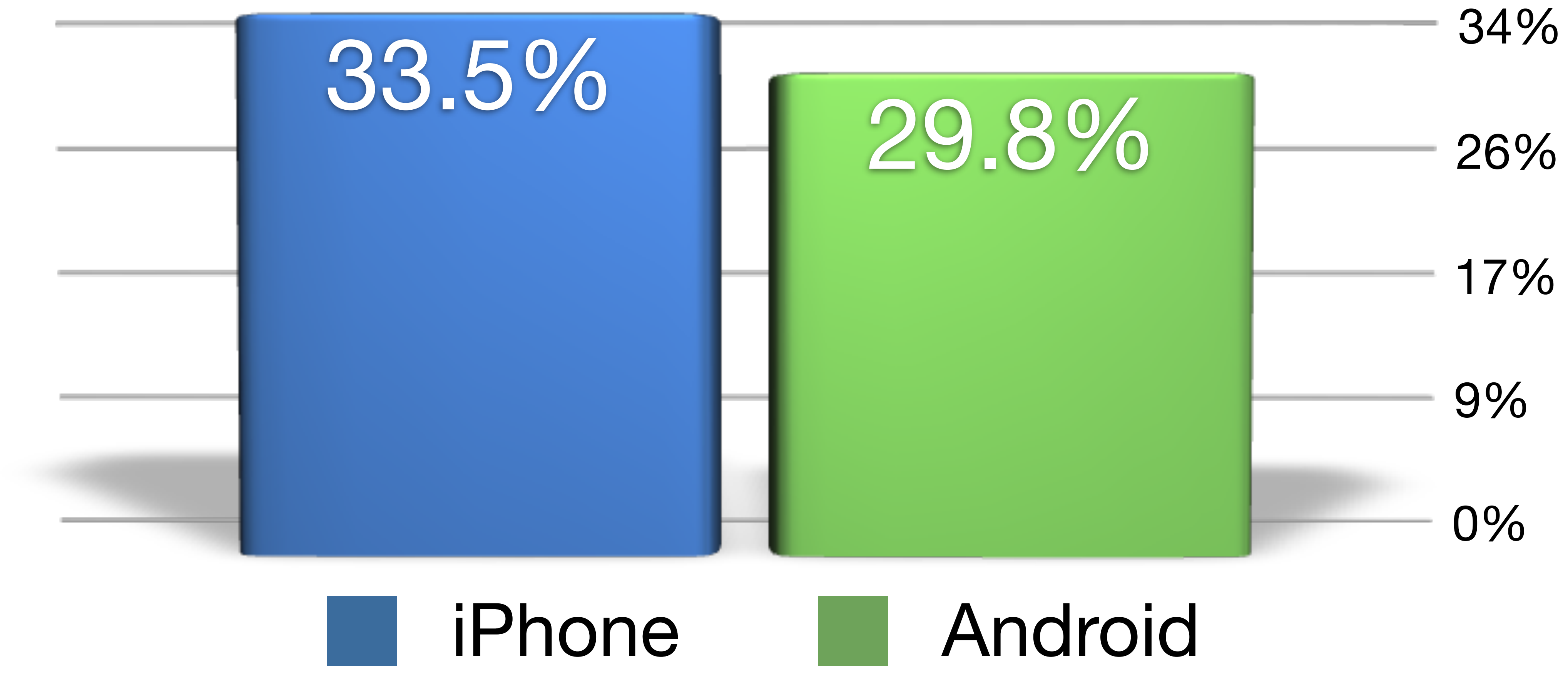
```
class droidsounds/StarWarsMovieSoundboard/ChooseContactActivity {
   ...
   assignRingtoneToContact ( );
   ...
}
```

Lesson Learned:

Not all apps that access sensitive data are bad.

Story #2:
Three’s Company

Free Apps Accessing Location



- Are there any applications accessing my location that shouldn't be?

The Search

- We started going through Android and iPhone Apps that looked accessed location but didn't seem to need it.

  There were a lot.

- We found a huge number of apps on both iPhone and Android that included 3rd party advertising SDKs.

Looking Closer

- Tested one Android application that has the QuattroWireless SDK in an emulator

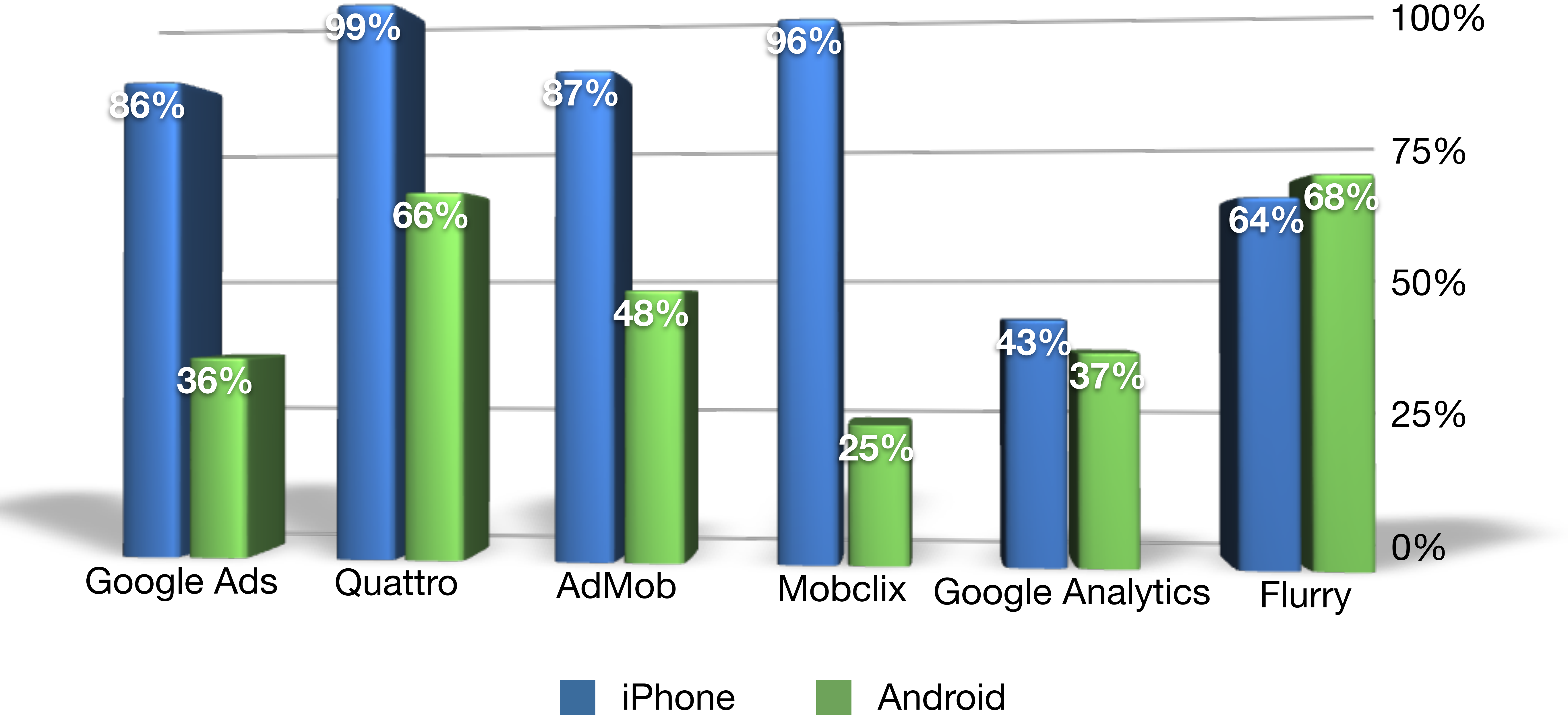
  Simulated Lat/Lon to -3.1337, 3.1337

- Wireshark caught the details

  Plain HTTP request to “ad.qwapi.com”

```
GET /adserver/render
    udid=ANDROID_SIMULATOR_0
    lat=-3.1336999999999997
    lon=3.1336999999999997
    ua=Android_US_generic_google_sdk_google_sdk_3_QuattroWirelessSDK
    ...
```

Conditional Likelihood to Access Location



Key Insights

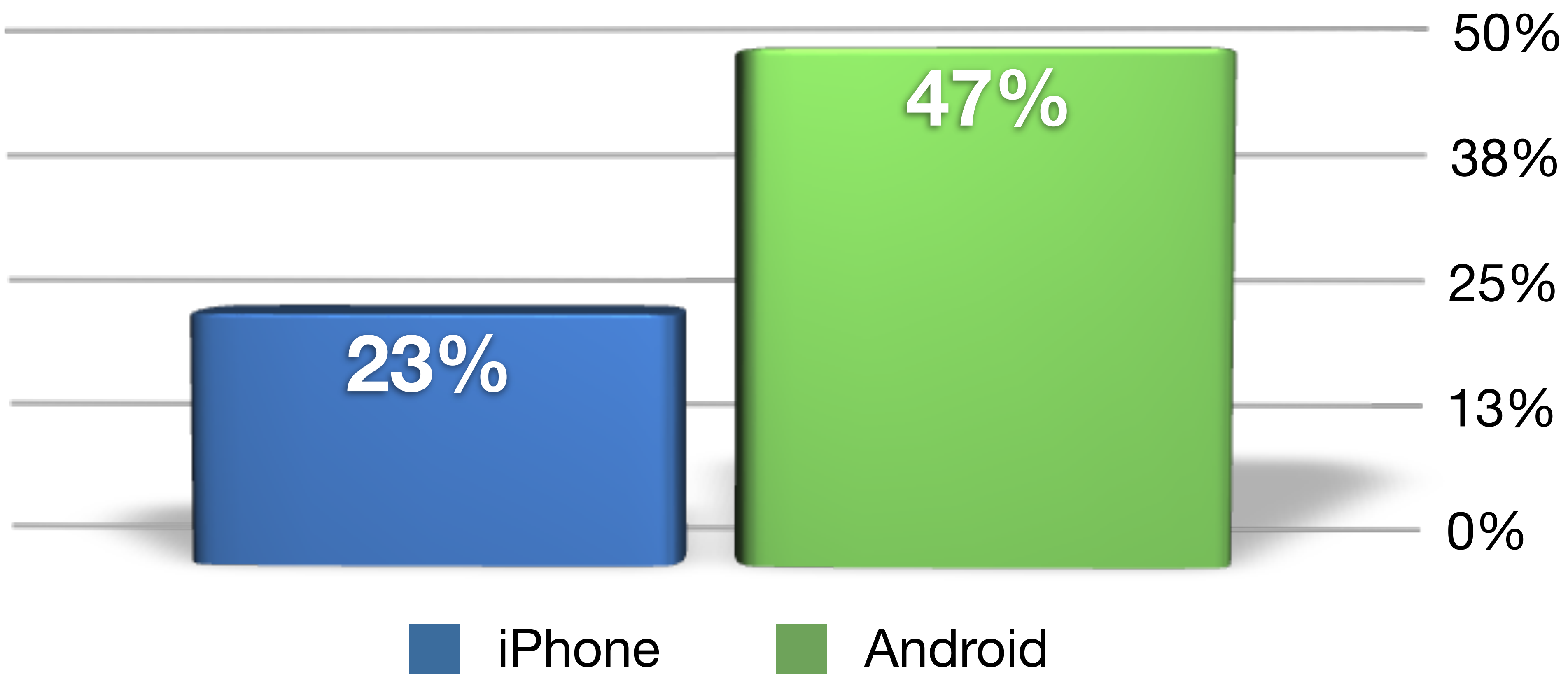
- On Android, if a developer brings in an ad SDK but doesn’t request location permissions, the app doesn’t access location.

  Our analysis takes this into account.

- On iPhone, an application will only be allowed to use location if Apple deems it appropriate.

  “If your app uses location-based information primarily to enable mobile advertisers to deliver targeted ads based on a user's location, your app will be returned to you by the App Store Review Team for modification before it can be posted to the App Store."

3rd Party Code Prevalence



- Presence of 8 popular 3rd party SDKs in free apps

Responsibility: Developers

- Many novice developers are developing mobile applications.

- When developers bring in 3rd party code, they don’t always know what’s going on.

  SDKs are closed source.

  It’s not always obvious what data SDKs collect.

- Developers need to be responsible with the data their app collects and inform users.

Responsibility: SDK Providers

- SDK Providers need to make sure developers know what data is being collected about their users.

- AdMob encourages developers to consider their users privacy.

Excerpt from AdMob iPhone SDK

```
// Whether AdMob may request location information from the phone. Defaults
to NO.
// We ask that you respect your users' privacy and only enable location requests
// if your app already uses location information.
...
- (BOOL)mayAskForLocation;
```

Lesson Learned:

Developers don’t always know what’s in their apps.

Story #3:
I Spy.

Finding the spies

- Are there apps that gather more than contacts/ location?

- We looked for applications that accessed a ton of data.

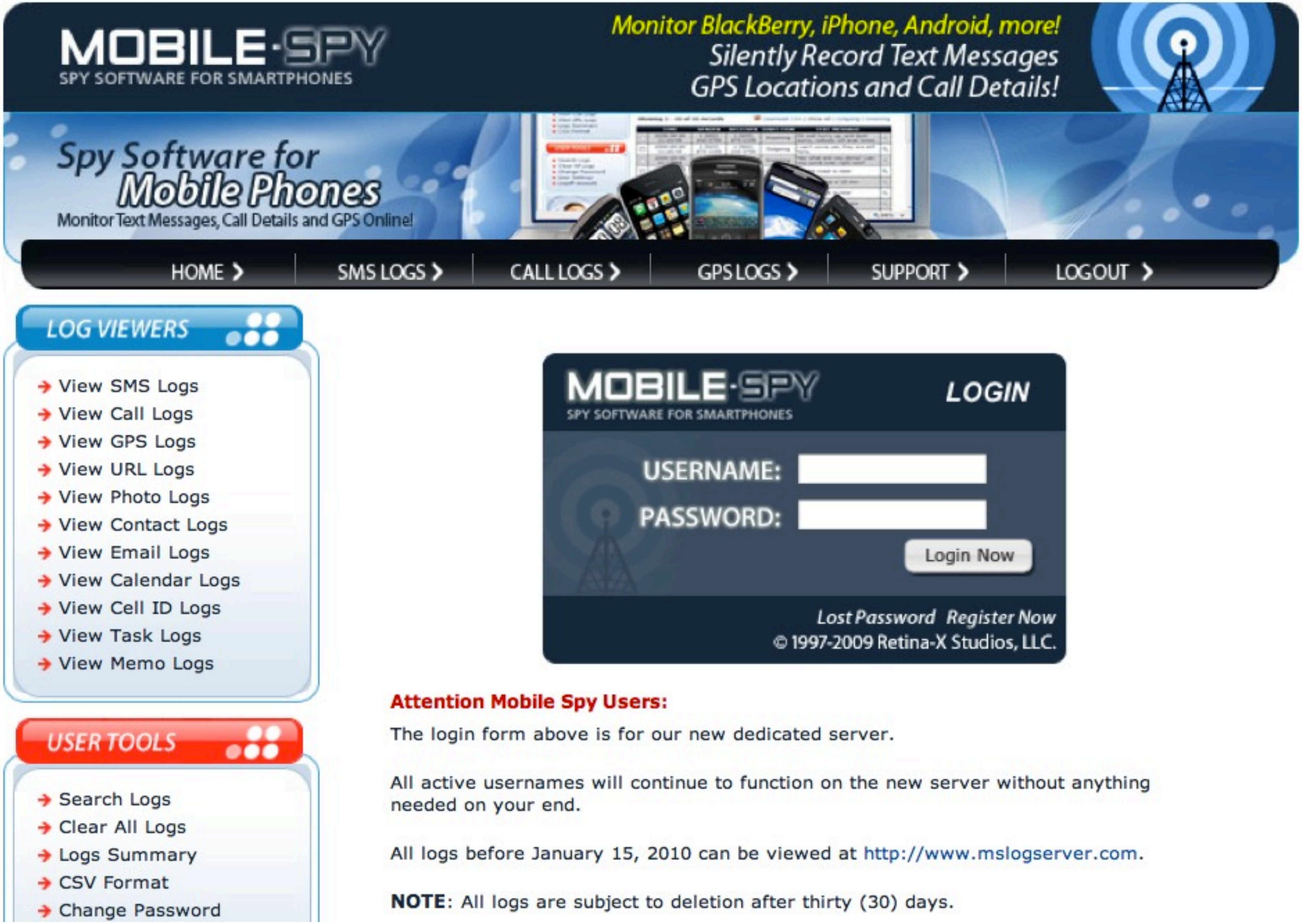
  e.g. IMEI, IMSI, browser history, contacts, location

A "System Utility" eh?

- Lots of applications by developer "RXS" accessed very sensitive data.
- Many had innocuous names and described themselves as a "System Utility"

  Android 15x, Android 16x, Android 20x, Android 21x
- Inside we see code shuttling data to: http://www.mobilespylogs.com/webapi

```
invoke-virtual {v0, v1, v2, v3}, Lcom/rxs21a/android/
SavePreviousData;->getSmsDetails(Landroid/content/
Context;Ljava/lang/String;I)V

invoke-virtual {v0}, Lcom/rxs21a/android/SavePreviousData;-
>getContactDetails()V

invoke-virtual {v0}, Lcom/rxs21a/android/SavePreviousData;-
>getURLDetails()V

invoke-static {}, Lcom/rxs21a/android/DatabaseHandler;-
>getCallContents()Ljava/lang/String;

// and more
```



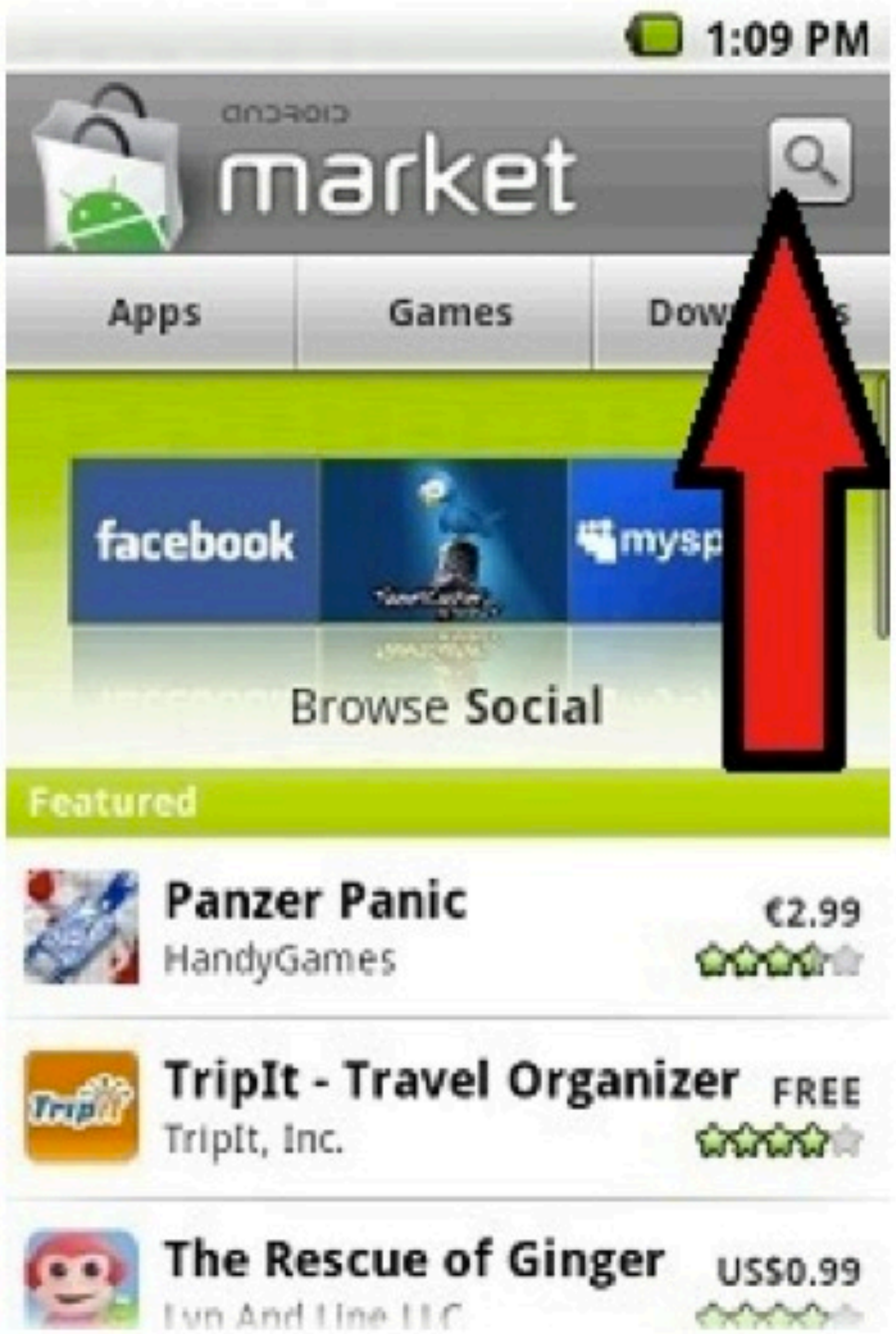
Attention Mobile Spy Users:

The login form above is for our new dedicated server.

All active usernames will continue to function on the new server without anything needed on your end.

All logs before January 15, 2010 can be viewed at http://www.mslogserver.com.

NOTE: All logs are subject to deletion after thirty (30) days.



4. Now you will need to search for the version of Mobile Spy that is designed for your version of the Android operating system.

For Android OS version 1.5, search for: **Android 15x**

For Android OS version 1.6, search for: **Android 16x**

For Android OS version 2.0, search for: **Android 20x**

For Android OS version 2.1, search for: **Android 21x**

iPhone SpyPhone App

- Nicholas Seriot, Blackhat DC

- PoC SpyPhone Application that only uses permitted APIs.

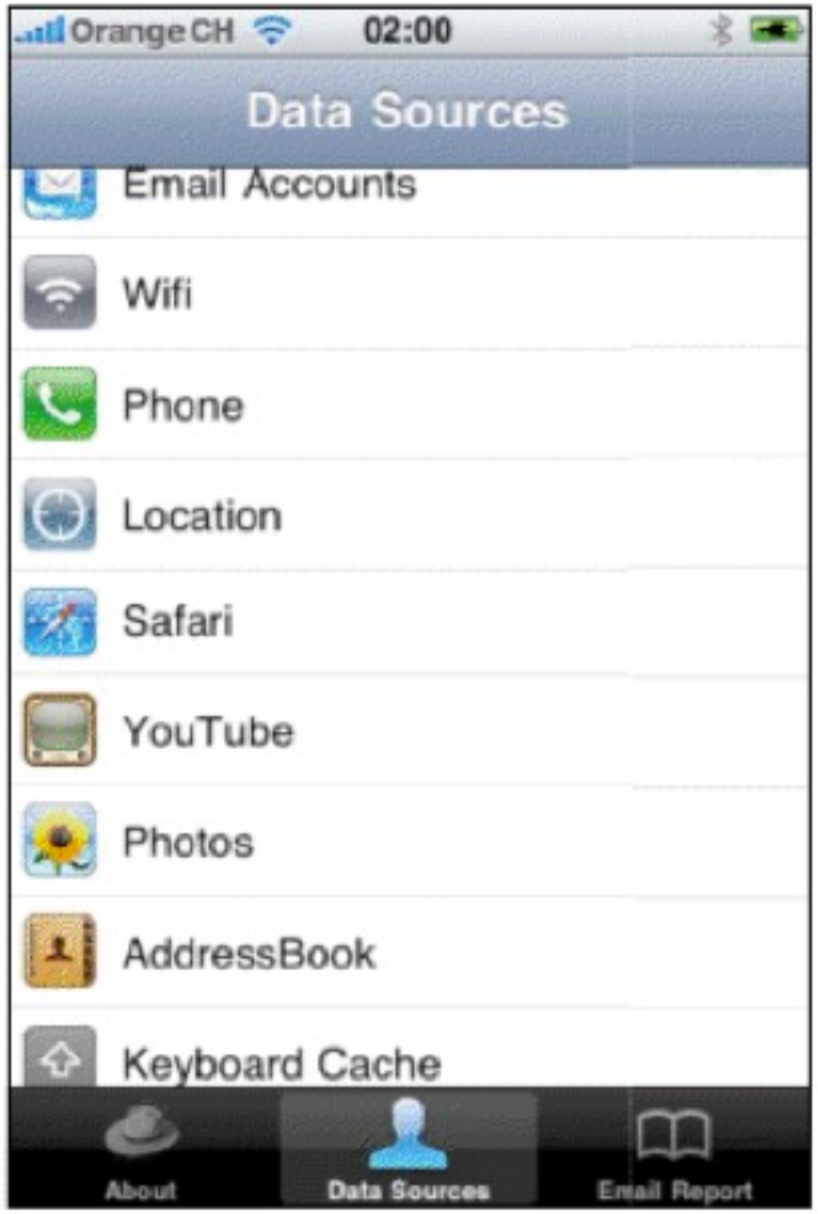
  Search History

  Keyboard Cache

  Contacts

  Email addresses

- On iPhone, users don't know what data is accessed (except location).



iPhone Flashlight App

- 15-year old developer

  SRSLY

- Created a flashlight app

  ...that also had a functional SOCKS proxy for tethering

- Accepted into the App Store

  Once the internets found out, Apple removed it.

- If a 15 year old can sneak code into the App Store...

Lesson Learned:

Apps aren’t always upfront about what they do.

Story #4:
The Orange Wallpaper

More sensitive data

- What about apps that access a device's Phone Number + IMEI + IMSI?

  Only a few hundred in the Android Market

- Any patterns?

  "jackeey,wallpaper" => 76 apps

  "IceskYsl@1sters!" => 8 apps

NBA Wallpapers

WWE Wallpapers

NationalGeographic Wallpapers

Quotes Wallpapers

Michael Jackson Wallpapers

Wallpapers,Pro

Harrypotter Wallpapers

WarCraft Wallpapers

Lost Wallpapers

Game CG Wallpapers

Forever Friends Wallpapers

Windows7 Wallpapers

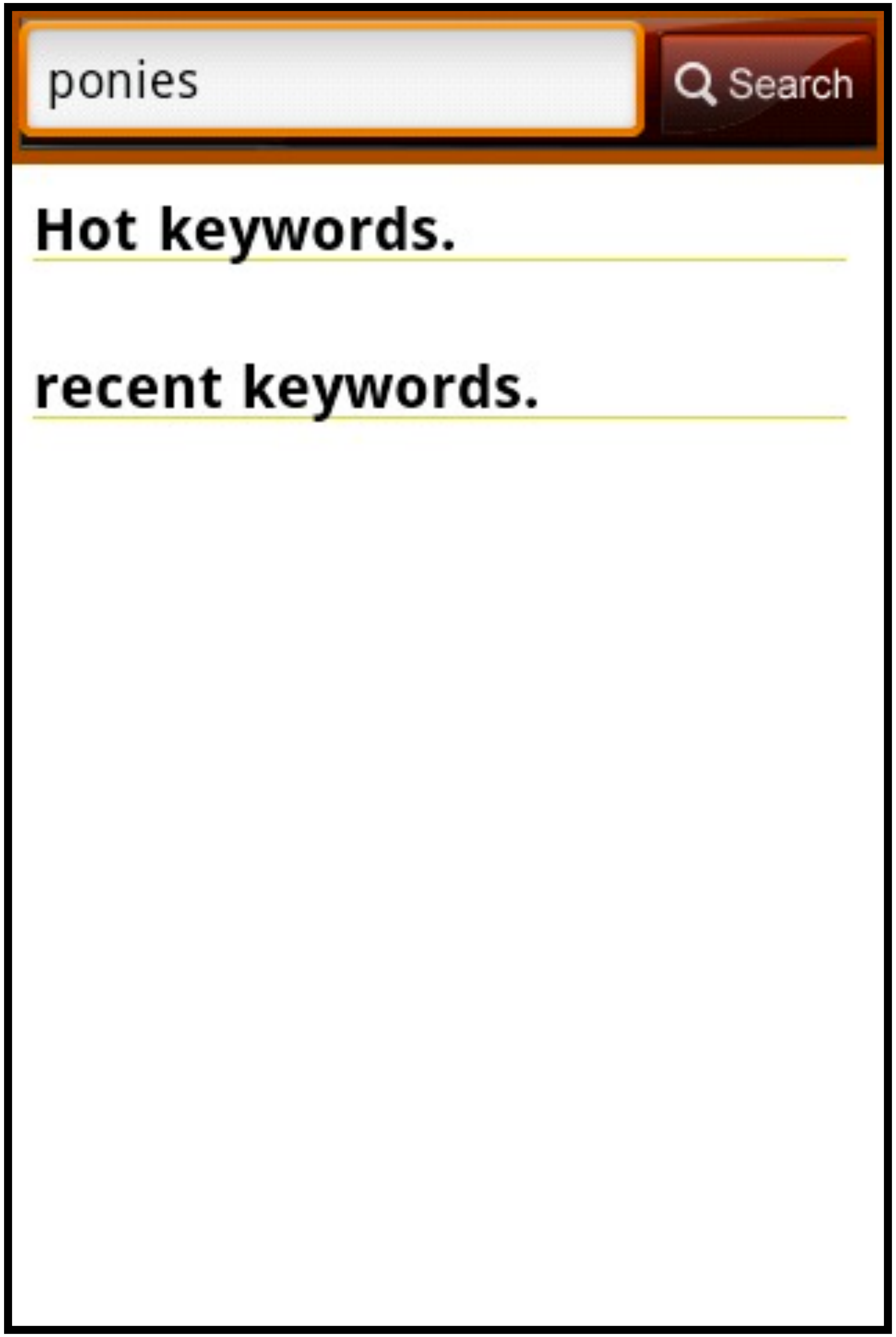
eWallpapers, phone backgrounds

Nature Wallpapers

Sex women Wallpapers series2

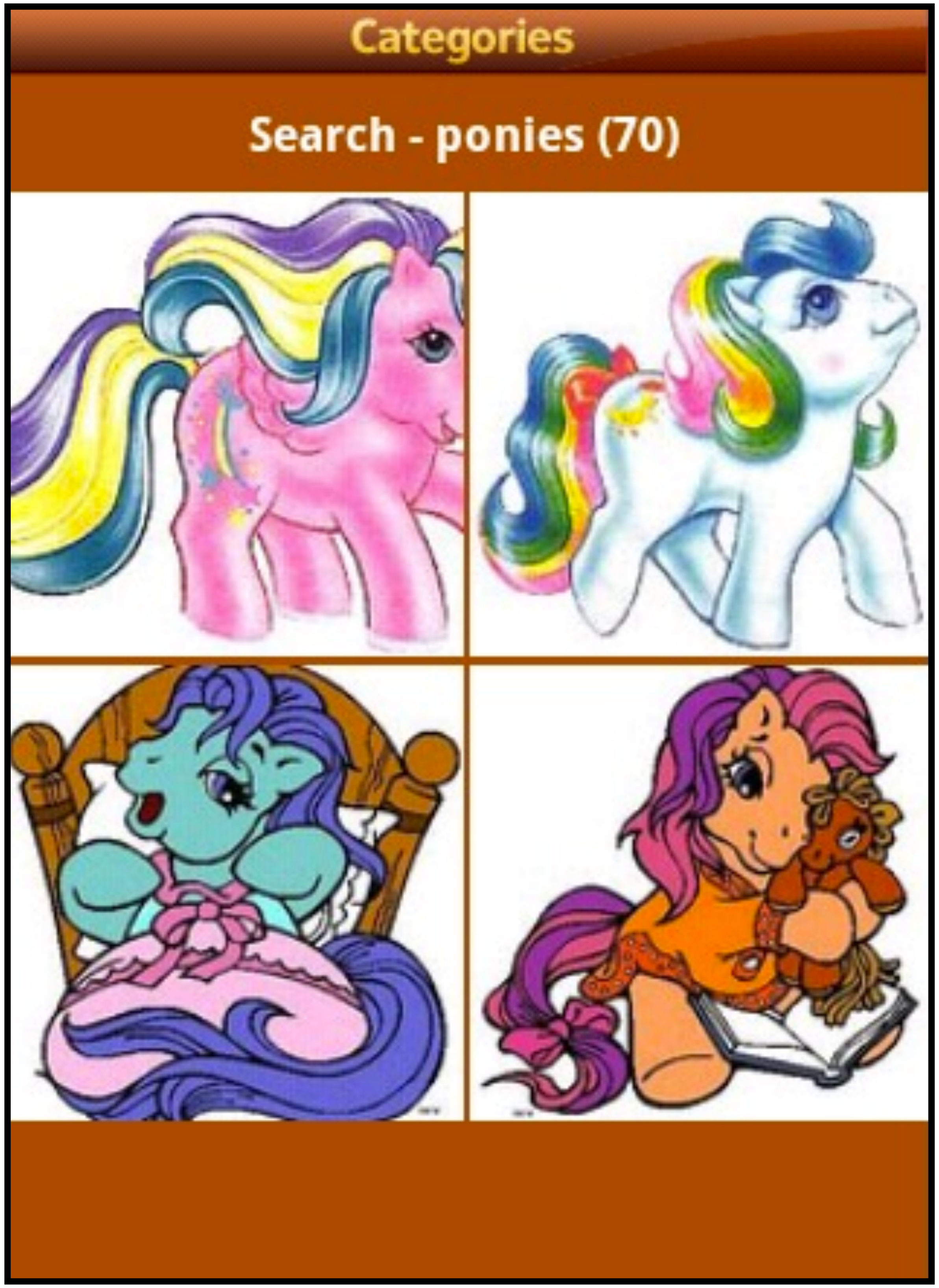
Nature Wallpapers, beautiful.

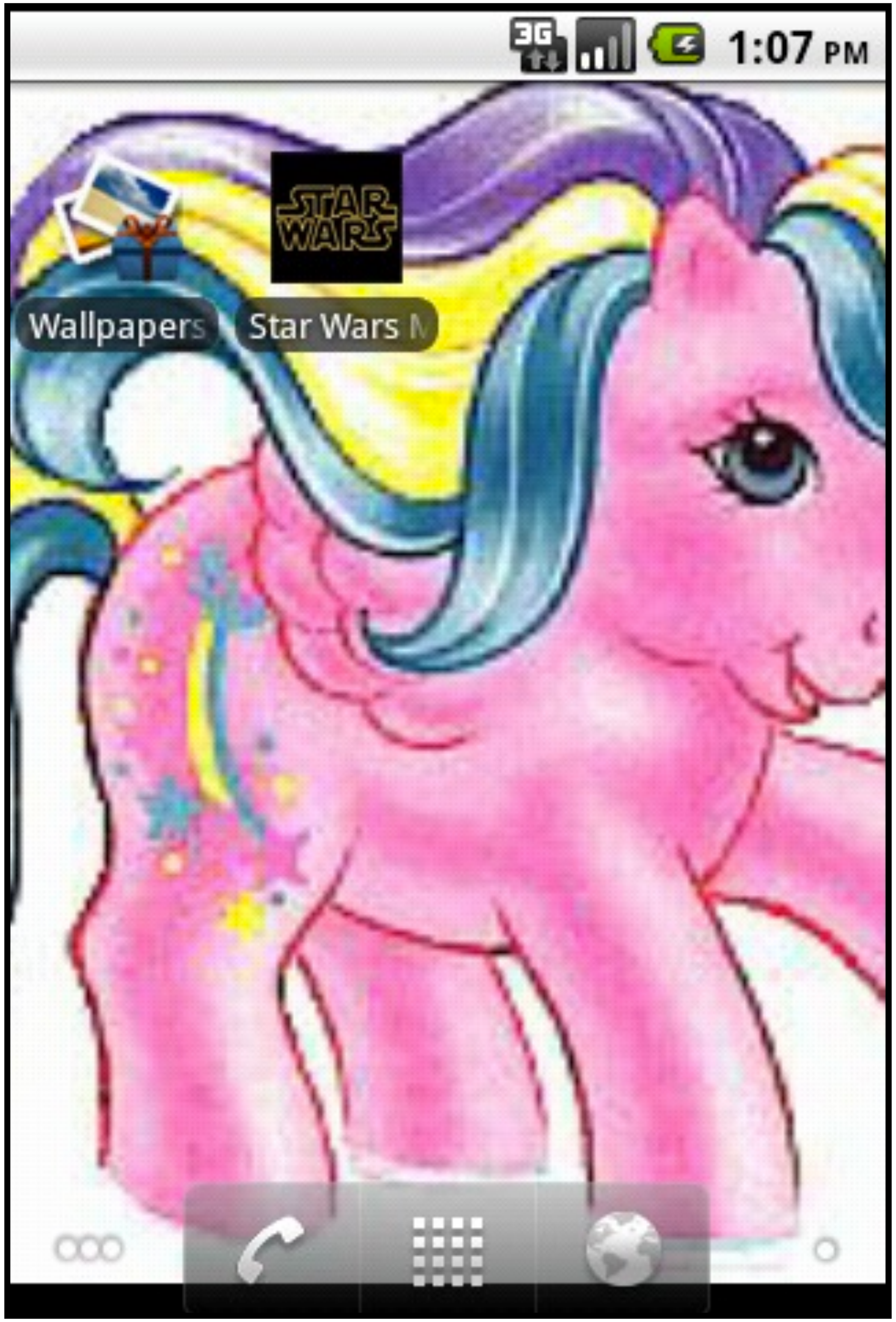
Arts Wallpapers



Hot keywords.

recent keywords.


Categories
Search - ponies (70)


1:07 PM
3G
Wallpapers
STAR WARS
Star Wars M

Why are wallpaper apps accessing my phone number, IMSI, IMEI?

Wiresharked

```
POST /api/wallpapers/log/device_info?locale=en-
rUS&version_code=422&w=320&h=480&uniquely_code=000000000000000&api_key=CIEhu15fY4bO4SGcGTq6g&nonc
e=9fe79a6119a9c650eb8f9615e2b88a8d&timestamp=1279591671671&api_sig=11404ee56654c3ad52649fb1e0589e5f
HTTP/1.1
Content-Length: 1146
Content-Type: application/x-www-form-urlencoded
Host: www.imnet.us
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
Expect: 100-Continue

HTTP/1.1 100 Continue

uniquely_code=000000000000000&device_info=device_id%3D000000000000000%26device_software_version%3Dnull
%26build_board%3Dunknown%26build_brand%3Dgeneric%26build_device%3Dgeneric%26build_display%3Dsdk-eng
+2.2+FRF42+36942+test-keys%26build_fingerprint%3Dgeneric%2Fsdk%2Fgeneric%2F
%3A2.2%2FFRF42%2F36942%3Aeng%2Ftest-keys%26build_model%3Dsdk%26build_product%3Dsdk%26build_tags
%3Dtest-keys%26build_time%3D1273720406000%26build_user%3Dandroid-build%26build_type%3Deng%26build_id
%3DFRF42%26build_host%3De-honda.mtv.corp.google.com%26build_version_release%3D2.2%26build_version_sdk_int
%3D8%26build_version_incremental%3D36942%26density%3D1.0%26height_pixels%3D480%26scaled_density
%3D1.0%26width_pixels%3D320%26xdpi%3D160.0%26ydpi%3D160.0%26line1_number
%3D15555218135%26network_country_iso%3Dus%26network_operator%3D310260%26network_operator_name
%3DAndroid%26network_type%3D3%26phone_type%3D1%26sim_country_iso%3Dus%26sim_operator
%3D310260%26sim_operator_name%3DAndroid%26sim_serial_number%3D89014103211118510720%26sim_state
%3D5%26subscriber_id%3D310260000000000%26voice_mail_number%3D%2B15552175049%26imsi_mcc
%3D310%26imsi_mnc%3D260%26total_mem%3D35885056
```

You probably can't read this

What just happened?

- We installed a wallpaper app.

  Ponies!

- The app sent this HTTP request in the clear.

```
POST /api/wallpapers/log/device_info
...
Host: www.imnet.us
...

sim_serial_number=89014103211118510720
subscriber_id=310260000000000
line1_number=15555218135
voice_mail_number=+15552175049
```

Digging in.

- Applications from each developer have a suspicious service

```
com/eoeandroid/wallpapers/nature/service/
SyncDeviceInfosService

com/jackeey/wallpapers/all1/orange/
SyncDeviceInfosService
```

- What does this service do?

```
invoke-virtual {v7}, Landroid/telephony/TelephonyManager;
->getDeviceId()Ljava/lang/String;

...

invoke-virtual {v7}, Landroid/telephony/TelephonyManager;
->getLine1Number()Ljava/lang/String;

...

invoke-virtual {v8}, Landroid/telephony/TelephonyManager;
->getSimSerialNumber()Ljava/lang/String;

...

invoke-virtual {v8}, Landroid/telephony/TelephonyManager;
->getSubscriberId()Ljava/lang/String;

...

invoke-virtual {v8}, Landroid/telephony/TelephonyManager;
->getVoiceMailNumber()Ljava/lang/String;

...
```

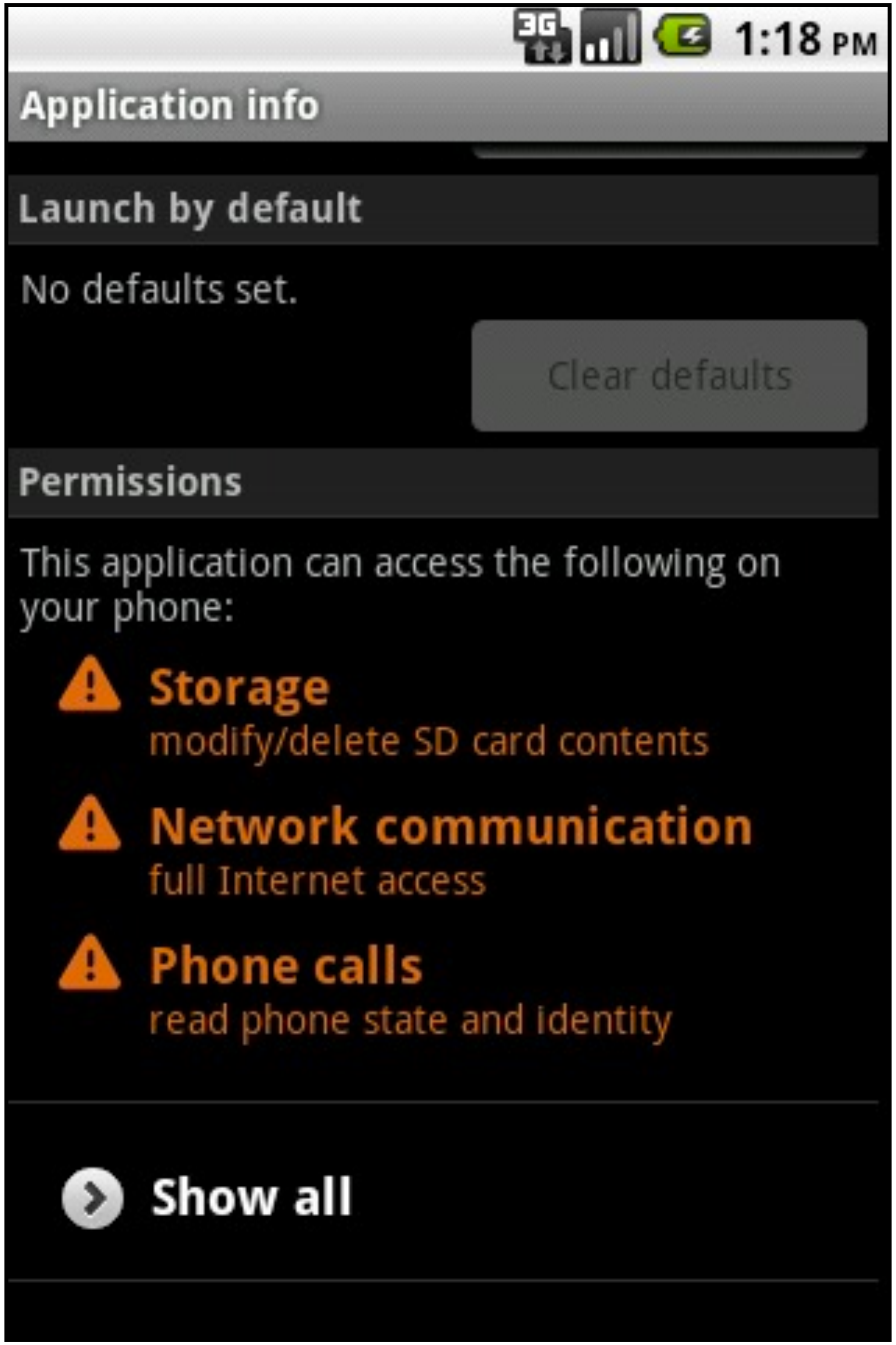
Who Owns imnet.us?

- Whois says:

```
Administrative Contact City: shenzhen
Administrative Contact State/Province: guangdong
Administrative Contact Country: China
Registrant Email: iceskysl@__REMOVED__.com
```

Surely nobody would download a wallpaper app that wanted to access identity information about my phone.

right?



Application info

Launch by default

No defaults set.

Permissions

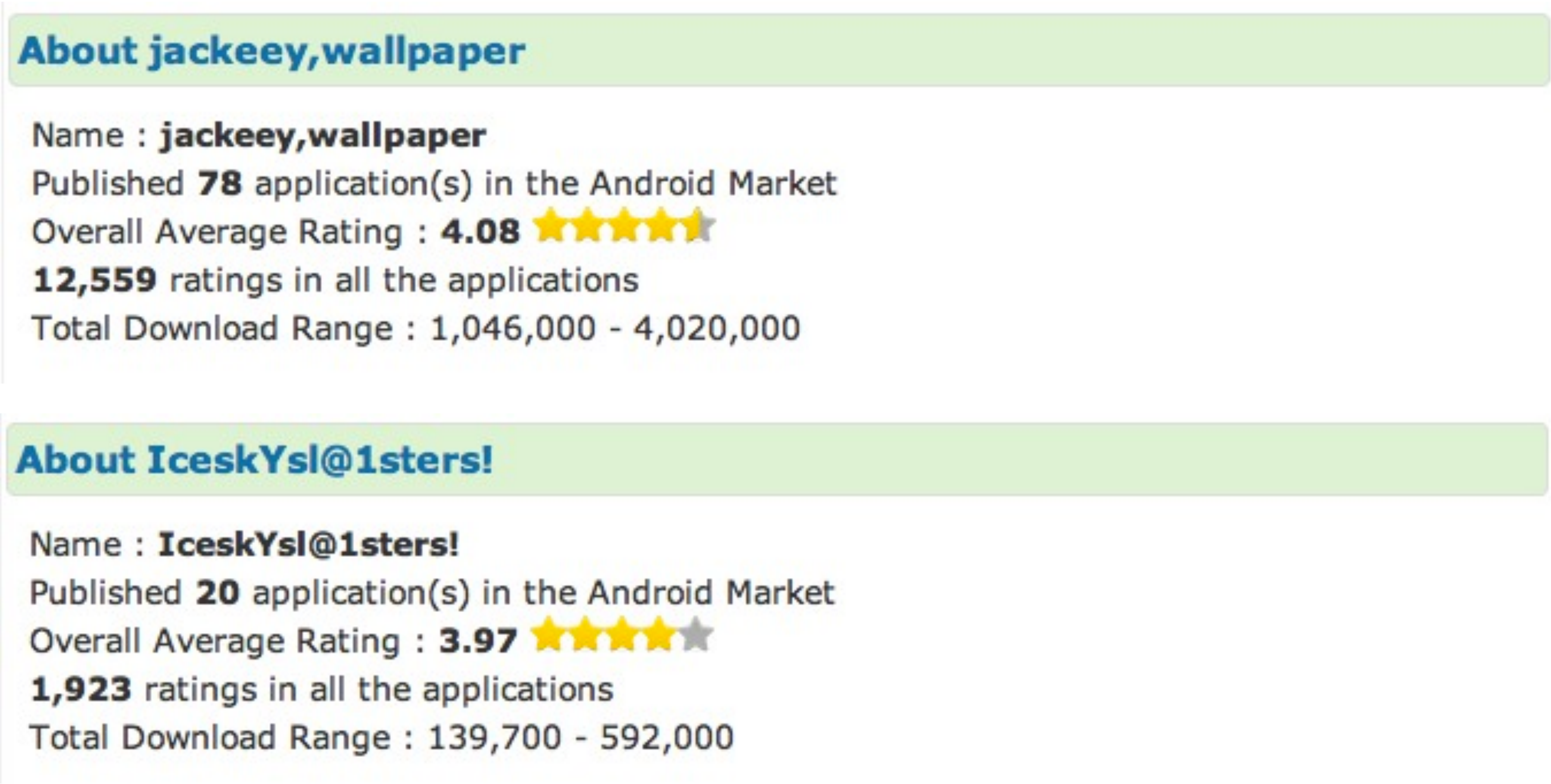
This application can access the following on your phone:

⚠ **Storage**
modify/delete SD card contents

⚠ **Network communication**
full Internet access

⚠ **Phone calls**
read phone state and identity

Together, these apps are estimated to have between 1.1 and 4.6 MILLION downloads!



About jackeey,wallpaper

Name : **jackeey,wallpaper**
Published **78** application(s) in the Android Market
Overall Average Rating : **4.08**
12,559 ratings in all the applications
Total Download Range : 1,046,000 - 4,020,000

About IceskYsl@1sters!

Name : **IceskYsl@1sters!**
Published **20** application(s) in the Android Market
Overall Average Rating : **3.97**
1,923 ratings in all the applications
Total Download Range : 139,700 - 592,000

Source: http://www.androlib.com

What’s next?

- Developer claims that information gathering is to preserve favorites when users switch devices.

- Google has taken the apps down from the Android Market while they investigate.

Lesson Learned:

Apps take advantage of their capabilities.

Summary of Findings

- Not all apps that access sensitive data are bad.

- Developers don't always know what's in their apps.

  A lot of apps include 3rd party code.

- Apps aren't always upfront about what they do.

  Do you trust app descriptions?

- Apps take advantage of their capabilities.

  Be careful what you download.

What’s in the wild?

- Imagine a hypothetical vulnerability
- We can use the App Genome project to ask:

  Are there any apps in the wild exploiting it?

  Are there any vulnerable apps in the wild?
- This is a very powerful tool during security response.

e.g. Account Hijacking

- On Android, apps shouldn't be able to get around permissions

  If they root the device, account hijacking is the least of our problems.

- Find all applications with READ_LOGS permissions.

  Only a couple hundred

- Automate static analysis to identify code that accesses log data.

  Does any of it target a vulnerable app?

What’s to come?

Finding bad apps in the future

- App store distribution model will minimize obviously bad apps.

- More prevalent: apps that seem good, but...

  have hidden functionality

  turn bad dynamically

e.g. iPhone Flashlight,
Android Wallpapers

- Probably can't remove all "context-dependent" apps from app stores.

e.g. Spy apps

Takeaways:

- Users: Pay attention to the apps you download

- Developers: Be responsible with the data you collect and how you use it.

  And don't put sensitive data into logs.

- Administrators: Don't ban apps or smartphones

  Do you force people to go back to typewriters if there's an MS Word vuln?

Thanks.

References

- http://www.dalvikvm.com/

- http://www.opensource.apple.com/source/xnu/xnu-1504.7.4/bsd/kern/mach_loader.c

- http://seriot.ch/resources/talks_papers/iPhonePrivacySlides.pdf