Mobile App (in)Security Renaissance 2014

Domingo Guerra
President & co-founder
dguerra@appthority.com
@SundayWar

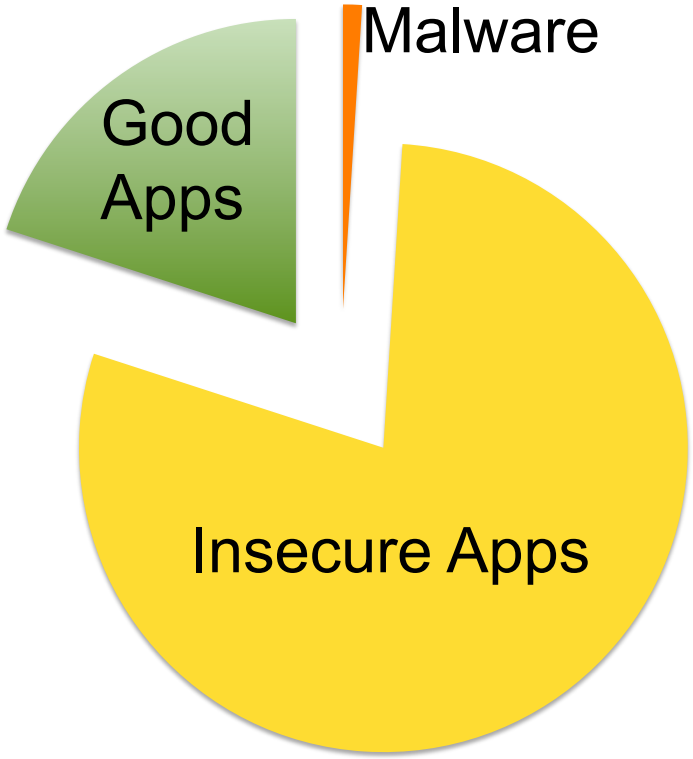
Appthority

- SaaS App Risk Management service
- Identifies hidden risks in mobile apps
- Automates app review, approval, and enforcement
- Analyzed over 2.3 million apps

Appthority enables companies to leverage mobility and empower a smarter, safer, mobile workforce

App Risk: Who's Responsible?

2.3 Million Apps Analyzed



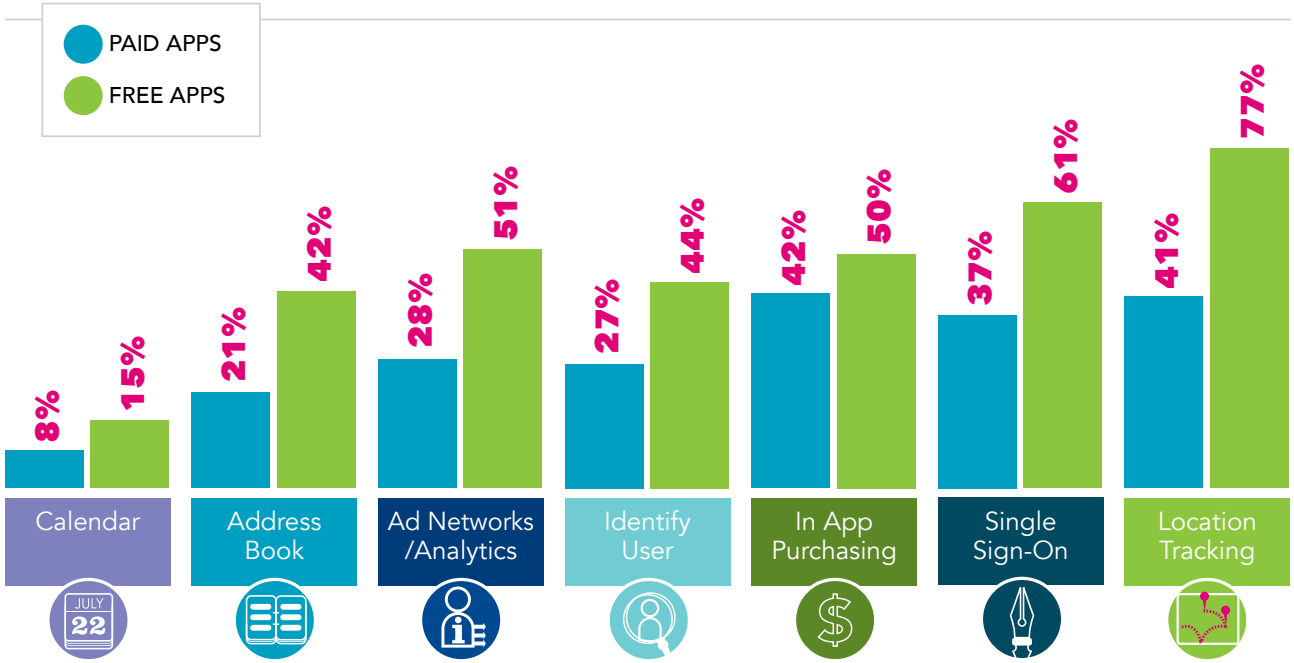
- Malware = Less than 0.4%
  - ***Bad people making bad apps***
  - ***Malicious intent***
- Insecure apps ~ 81%
  - ***Good people making bad apps***
  - ***Insecure programing practices***
  - ***Developer mistakes***
  - ***Bad tools, SDKs, Libraries***

Less than 20% of mobile apps would pass an enterprise grade security test

Appthority®

Fall 2013: App Reputation Report

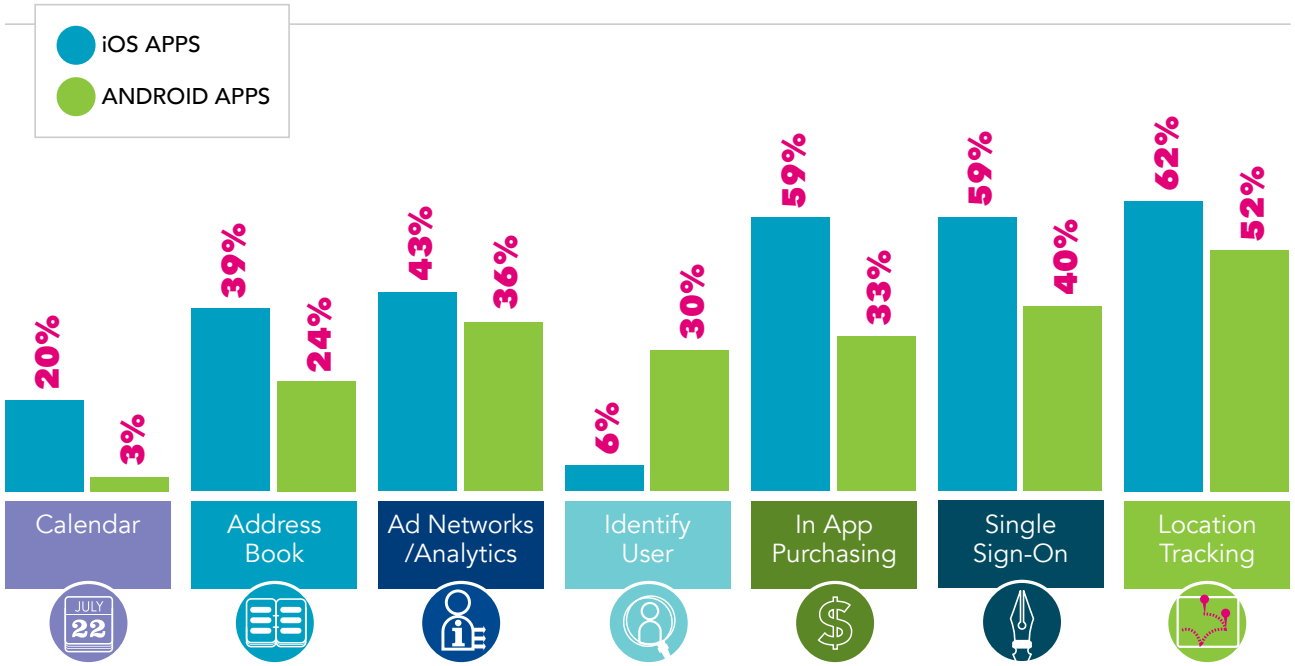
Key Findings: Paid Apps vs. Free Apps



Appthority®

Fall 2013: App Reputation Report

Key Findings: iOS Apps vs. Android Apps



Appthority®

Reputation Report: Summer 2013

Breakdown the Most Popular Apps

DEVELOPERS IN THE TOP 100 FREE APPS

81 DIFFERENT DEVELOPERS

11 DEVELOPERS HAVE MORE THAN 1 APP

5% OF APPS WERE DEVELOPED BY APPLE, FOLLOWED BY GEORGE CL AND GOOGLE WITH 4%, AND DISNEY WITH 3%

85 DIFFERENT DEVELOPERS

13 DEVELOPERS HAVE MORE THAN 1 APP

4% OF APPS WERE DEVELOPED BY GOOGLE

NO ONE ELSE HAD MORE THAN 2%

DEVELOPERS IN THE TOP 100 PAID APPS

79 DIFFERENT DEVELOPERS

11 DEVELOPERS HAVE MORE THAN 1 APP

7% OF APPS WERE DEVELOPED BY DISNEY, FOLLOWED BY ELECTRONIC ARTS WITH 5% AND ROVIO (MAKERS OF ANGRY BIRDS) WITH 4%

88 DIFFERENT DEVELOPERS

8 DEVELOPERS HAVE MORE THAN 1 APP

4% OF APPS WERE DEVELOPED BY DISNEY, CHAINFIRE AND ELECTRONIC ARTS HAD 3% EACH

Appthority®

Risky Application Impact

- **Hurts your user(s)**
  - Users' personal and corporate data & privacy at risk
- **Hurts your brand**
  - App brand and personal/developer brand
- **Impact is broad**
  - Bans from app stores
  - Bans from enterprise use (MDM & BYOD tools)
  - Less downloads
  - Steep fines (FTC & Gov getting serious)

Appthority

Top 5 Developer Fails

1. **Using Risky SDKs**
   Adware/Analytic/3rd party libs

2. **Permissions and Bypassing User Consent**
   accessing device features without user consent, under/over privileged apps
3. **Dirty Laundry**
4. **Improper Handling of Private App Data**
5. **Bad Cryptography**
   weak or no algorithms, predictable seeds

Appthority®

Fail #1: Adware/Analytic SDK

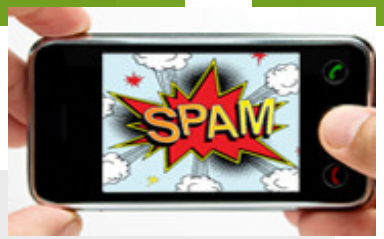
Ad networks introduce external risk!

- Permissions added to app by a popular Adware SDK:
  - *INTERNET, ACCESS_NETWORK_STATE, READ_PHONE_STATE, RECEIVE_BOOT_COMPLETED, LAUNCHER.INSTALL_SHORTCUT, WRITE_EXTERNAL_STORAGE, ACCESS_WIFI_STATE, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, GET_ACCOUNTS, BROWSER.READ_HISTORY_BOOKMARKS*
- These break COPPA, corporate data privacy policies
- Developers may add many Adware SDKs
  - *Potentially aggressive: Apperhand, Vulna/Applovin*

Appthority®

Fail #1: Adware/Analytic SDK (Cont.)

Private data sent by these SDKs…




```
11:31:12 INFORMATIONAL{"TRUDYNAMIC_ID"=>55000,"APPLICATION"=>"com.app.game","CALL"=>"network-ssl-writedata", "ADDRESS"=>"67.222.123.12"}
[POST /dialogad/adclick.php HTTP/1.1
Content-Length: 838
Content-Type: application/x-www-form-urlencoded
Host: api.adnetwork.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/android_game_app (Linux; U; Android 4.2.2; SCH-I545 Build/JDQ39E)
Accept-Encoding: gzip
APIKEY=342343256797 52&appId=94434&imei=528404732124 33&token=b1cb6d3cd29021cfc5eddf&request_timestamp=2013-07-18+18%3A29%3A37_GMT_GMT_GMT&packageName=com.app.game
&version=17&carrier=Verizon&networkOperator=Verizon&phoneModel=Galaxy+Nexus&manufacturer=samsung&longitude=37.783699&latitude=-122.467819&sdkversion=5.0&wifi=0&
useragent=Mozilla%2F5.0+%28Linux%3B+U%3B+Android+4.2.2%3B+en-us%3B+Full+Android+Build%2FJDQ39E%29+AppleWebKit%2F534.30+%28KHTML%2C+like+Gecko%29+Version
%2F4.0+Safari%2F534.30&android_id=507 20 &screenSize=1024_600&deviceUniqueness=IMEI&networkSubType=UMTS&isTablet=true&SD=1.0&isConnectionFast=true&unknownsource=0
&appName=Superman&email=kdawg%40gmail.com&phonenumber=15555215554&language=English&country=US&zip=94110&creativeid=42 0 &campaignid=56303]

13:47:39 INFORMATIONAL{"TRUDYNAMIC_ID"=>55000, "APPLICATION"=>"com.app.game", "CALL"=>"network-ssl-writedata","ADDRESS"=>"67.222.123.12"}
[POST /lp/log_sdk_request.php HTTP/1.1
Content-Length: 2288
Content-Type: application/x-www-form-urlencoded
Host: api.adnetwork.com
Connection: Keep-Alive
User-Agent: pache-HttpClient/android_game_app (Linux; U; Android 4.2.2; SCH-I545 Build/JDQ39E)
Accept-Encoding: gzip
APIKEY=342343256797 52&appId=94434&imei=528404732124 33&android_id=af4e228dddf0377a05e8d941874223ea&inputlist=%22android%22%2C%22com.ubercab%22
%2Ccom.nianticproject.ingress%22%2C%22com.android.calendar%22%2C%22com.amazon.kindle%22%2C%22com.android.contacts%22%2C%22com.android.defcontainer
%22%2C%22com.android.deskclock%22%2C%22com.android.development%22%2C%22com.android.dreams.basic%22%2C%22com.android.dreams.phototable%22%2C%22com.android.email
%22%2C%22com.android.exchange%22%2C%22com.android.galaxy4%22%2C%22com.android.gallery3d%22%2C%22com.android.html...]

13:50:29 INFORMATIONAL{"TRUDYNAMIC_ID"=>50267, "APPLICATION"=>"com.corp.app", "CALL"=>"posix-sendtobytes","ADDRESS"=>"76.200.12.1"}
[GET /jin/ads?v=2.4&platformid=53&pubid=qhpn&apikey=B23234d&placement=bottom&format=html&channel=mobile&ua=Mozilla+SCH-I545+Build%2FJDQ39E%29+ouid=e507929b9&u=35490400
&lat=37.783699&lng=-122.467819&city=San+Francisco&state=CA&country=US&width=320&height=50&gender=&age=34 HTTP/1.1
Host: another.adnetwork.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/android_corp_app (Linux; U; Android 4.2.2; SCH-I545 Build/JDQ39E)
```

APIKEY IMEI TIMESTAMP LAT APP ID LONG PHONE ZIP LAT COUNTRY LONG CITY STATE AGE

Appthority

Which Ad networks to use?

Evaluating an ad network (& other 3rd party tools)

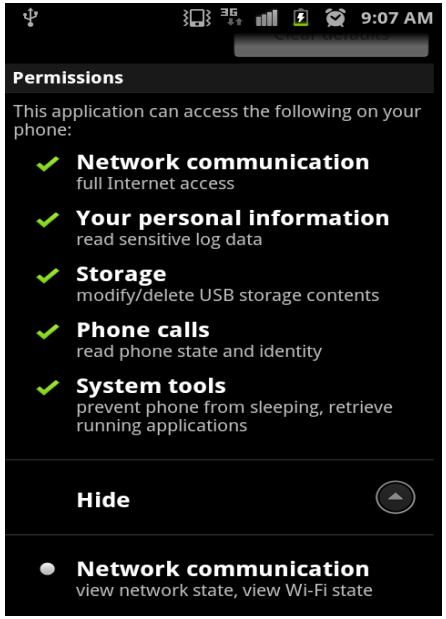
- **Ad network reputation**
  1. Evaluate end-user & developer opinions on privacy & security
  2. Do they treat their developers well? Are there customer complaints?
- **Type of Data Collected**
  1. Read the ad networks T&Cs. (Your users won't)
  2. Discover what kinds of data they collect.
  3. Is it private, potentially sensitive or does it uniquely identify the user?
  4. Does it collect the data in a clandestine manner?
  5. Consider 3rd party testing or certification

Appthority

Fail #2 Permission Abuse & Bypassing Consent

Potential problems with permissions

1. **Under privileged Application** Sidesteps permission system to obtain same behavioral results.
2. **Over privileged Application** Requests permissions that are unneeded.
3. **The Confused Deputy** Perform actions on behalf of another agent. Like sending SMS messages.

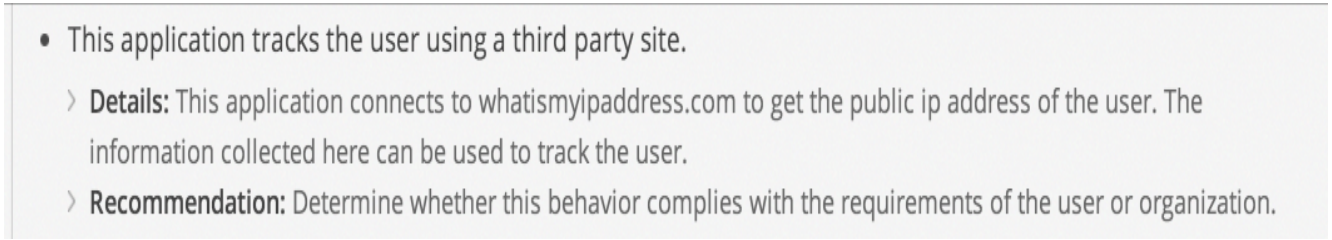


Appthority

Fail #2 Permissions and Bypassing Consent

App behavior must adhere to permissions requested

- Application is underprivileged, side-steps permission system yet is still able to track user
- Yet…



- **ACCESS_COURSE_LOCATION** not in manifest
  - *Doesn't request any permissions to geo-track the app user*

Example: E*trade, iOS & Android

Appthority

Fail #2 Permissions and Bypassing Consent

Application should request the minimal set of permissions necessary to operate correctly.

Frequently unneeded yet requested permissions. Actions can be accomplished with Intents to the target application.

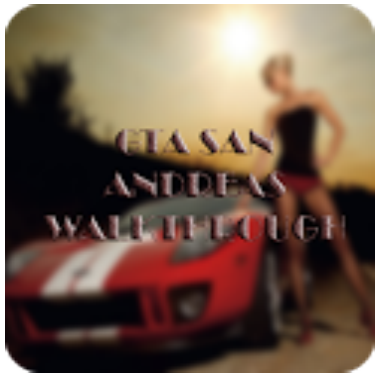
- **CAMERA** – Take picture using default capture.
- **INTERNET** – Open URL in Browser.
- **CALL_PHONE** – Open default phone dialer.

However, autoupdate encourages overprovisioning to make dev lifecycle smoother!

Adrienne Porter Felt, Erika Chin, Steven Hanna, Dawn Song, and David Wagner. Android Permissions Demystified. ACM CCS 2011.

Appthority®

Permission abuse!



Extreme permission abuse!

- Grand Theft Auto Walkthrough Game
- 10k+ Downloads
- Pulled from market
- Requests 50 permissions!

Appthority

More permission abuse!

Extreme permission abuse!

- Joke Screen Melt Wallpaper
- STILL ON MARKET
- Requests 45 permissions!
  - Including:

android.permission.INSTALL_PACKAGES
android.permission.DELETE_PACKAGES
android.permission.RECORD_AUDIO
android.permission.MOUNT_FORMAT_FILESYSTEMS
android.permission.GET_ACCOUNTS
android.permission.SET_WALLPAPER

Aggressive adware!

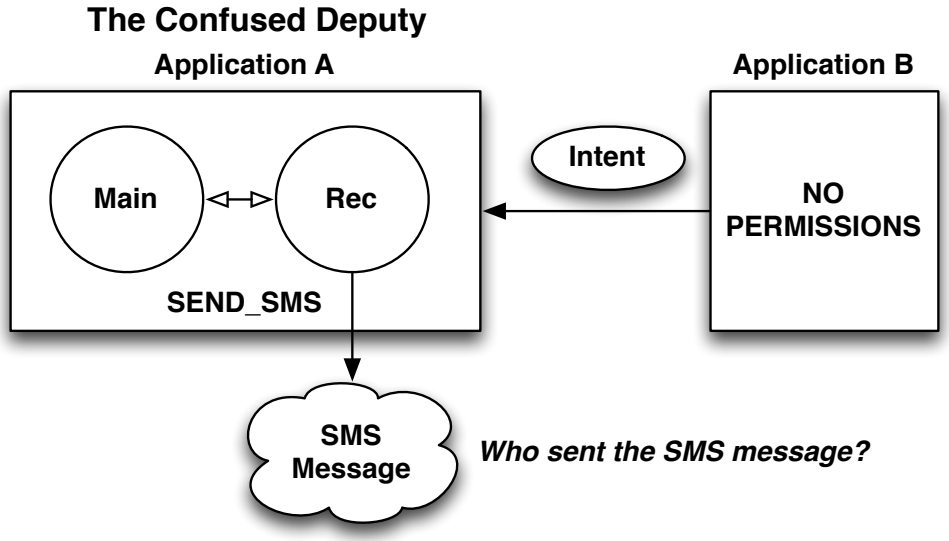
Appthority

Fail #2 Permissions and Bypassing Consent

Apps must check intent permissions and guard its Broadcast Receivers!

Potential for abuse, the confused deputy performs actions on behalf of another agent.

Example: Application A has 2 components: **MainA** main application component, **RecA** broadcast receiver, it has permission SEND_SMS. **Application B** has no permissions.



Appthority

Fail #3 Dirty Laundry & Pandora for iOS

App includes debugging information, giving us a view into the development environment

- This application includes file paths to source code files in debug information stored within the app's executable. These file paths often include usernames or other information related to the developer of the app. This information could be used to assist in targeting the app developer or development company.

```
param27: "/Users/casey/workspace/ios/release/src/iPhone/Classes/AdvertisingController.m",
param28: "/Users/casey/workspace/ios/release/src/iPhone/Classes/../../Twitter+OAuth/SAOAuthTwit
param29: "/Users/casey/workspace/ios/release/src/iPhone/Classes/../../Facebook-iOS-SDK/src/FBRe
param30: "/Users/chrisl/repos/iOS-SDK/sdk/OoyalaSDK/Classes/Internal/JSONKit/OOJSONKit.m",
param31: "/Users/chrisl/repos/iOS-SDK/sdk/OoyalaSDK/Classes/Internal/OOReachability.m",
```

Example: Pandora, iOS

Casey [redacted]

Senior Software Curmudgeon at Pandora

Greater Denver Area · Computer Software

1 shared connection · Similar

Appthority

Fail #4 Improper Handling of Private Data: Tinder

What we Found in the Tinder App…

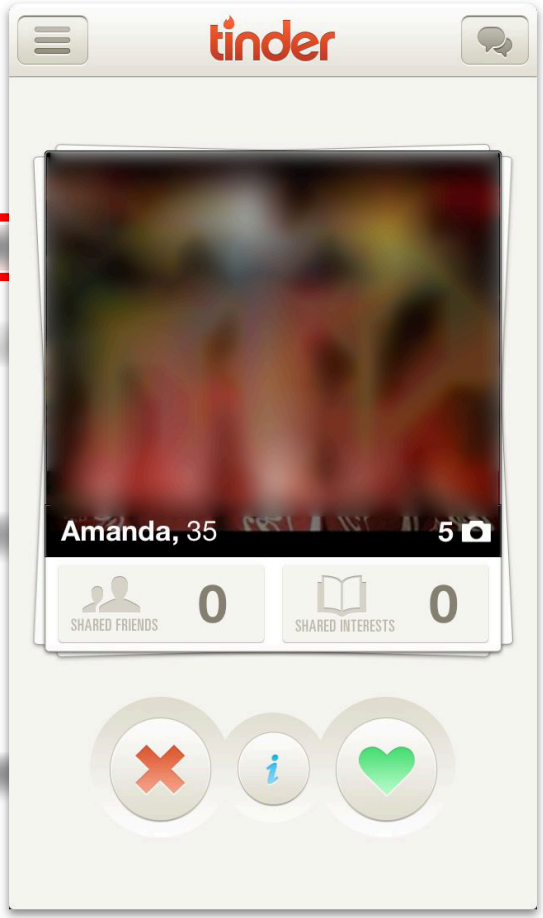
- Our analysis engines alerted us that the App was sending exact geo-location information over the network
- We found much more was being sent over the network – including the full name of all matches, exact birth-date/ age, and Facebook ID profile ID

Appthority®

Fail #4 Improper Handling of Private Data: Tinder

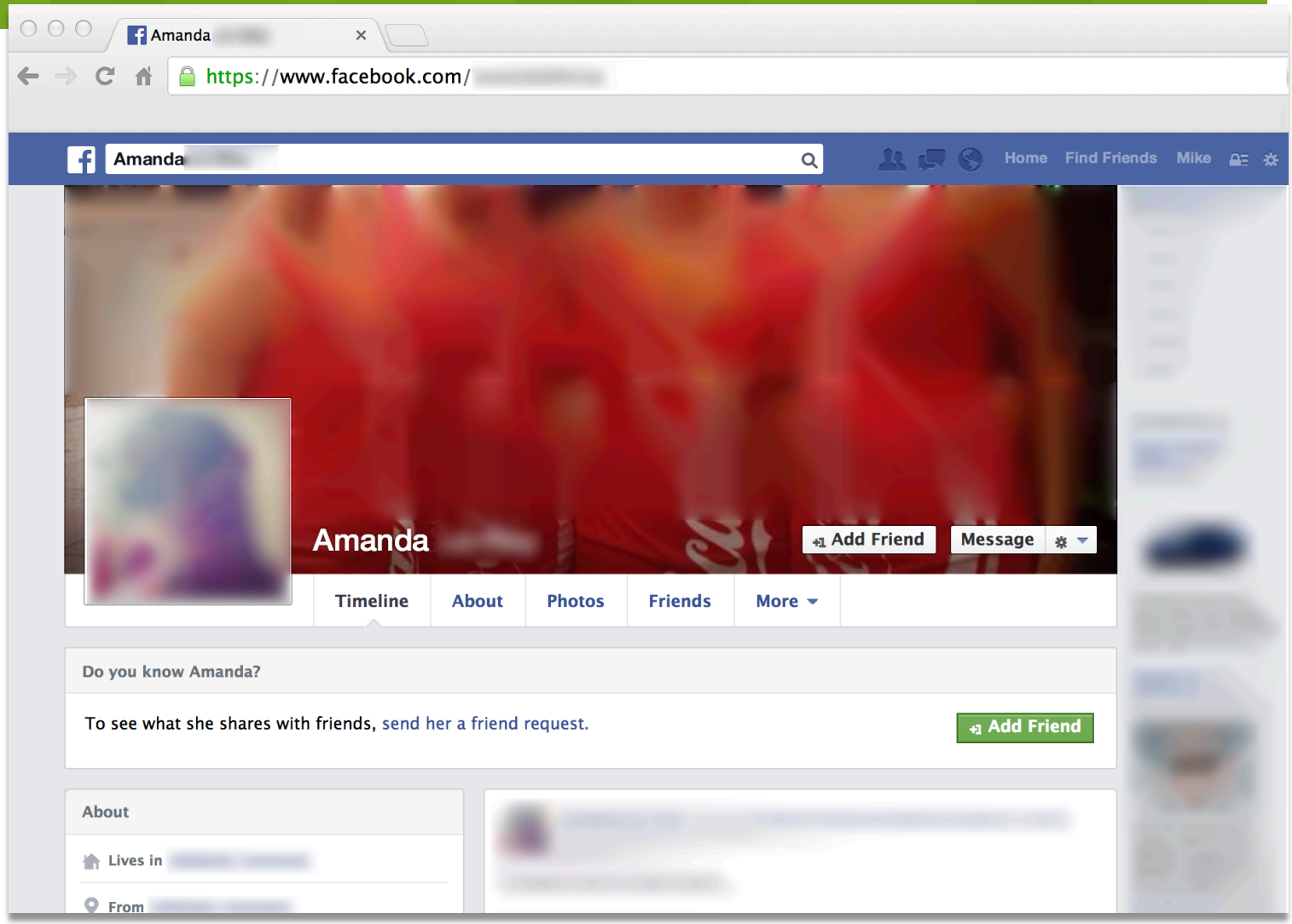
Tinder-2.1.1 — vim — 66×20

```
22 {
23   "status": 200,
24   "results": {
25     "bio": "[redacted]",
26     "name": "Amanda",
27     "birth_date": "1978-[redacted]
28     "gender": 1,
29     "ping_time": "[redacted]
30     "photos": [
31       {
32         "xdistance_percent": 1,
33         "id": "[redacted]
34         "xoffset_percent": 0,
35         "yoffset_percent": 0.2188477,
36         "ydistance_percent": 0.5625,
37         "main": true,
38         "fileName": "[redacted]
   ,
39         "fbId": "1020[redacted]",
```



Appthority

Fail #4 Improper Handling of Private Data: Tinder



Fail #4 Improper Handling of Private Data: Tinder

We made the Tinder report public …

Home > Social Media > There might be more security issues with Tinder…

THERE MIGHT BE MORE SECURITY ISSUES WITH TINDER THAN YOU THOUGHT

By **Jam Kotenko** — July 26, 2013

Tinder found out about the problem and fixed it right away – that's good, right? Unfortunately, the security breach Tinder claims to have under control is a lot more serious than they are admitting. Appthority, which analyzes apps for security issues, found out that the dating app is still putting users' private data at risk. "Through our automated risk analysis engines, we noticed that the dating app Tinder received a very low Appthority Trust Score," says Kevin Watkins, CTO and co-founder of Appthority. "We decided to take a closer look and made some surprising discoveries. We found that Tinder is serving up Facebook IDs and exact birth dates in its API information without the user's knowledge." Their findings also show that although Tinder stopped sharing specific latitudinal and longitudinal user information, the app is still sharing their exact distance away from another users – Watkins believes that anyone with some technical chops could get another user's Facebook ID, birth date, and exact distance, along with the last time that Tinder user submitted their geo-location. "A motivated user could track someone down by spoofing their own location several times to see how far away they are," Watkins explains.

Appthority®

Fail #4 Improper Handling of Private Data: Tinder

The Tinder API "profile" returns a target profile information, including the "distance_mi" away and they did remove the "pos":


```
{
    "distance_mi": 3.683084352674016,
    "common_like_count": 2,
    "common_friend_count": 0,
    "common_likes": 2,
    "0":  6092929747,
    "1":  6459871686,
    "common_friends": 2,
    "_id": "518ca49677ae40da00000a",
    "bio": "Born and raised in Texas",
    "birth_date": "1981-06-05T00:00:00.000Z",
    "gender": 1,
    "name": "Angela Hastings",
    "ping_time": "2013-07-21T16:40:31.389Z",
    "pos":  { "lon":-122.6990317622351,"lat": 37.99630196019288 }
}
```


Exact Distance

STILL A FAIL!

Knowing the Tinder API "ping" sets the geographical position:


```
13:32:11 INFORMATIONAL{"TRUDYNAMIC_ID"=>"55000", "APPLICATION"=>"com.tinder", "CALL"=>"network-ssl-writedata", "fd"=>"0x21500005", "ADDRESS"=>"107.21.48.191"}
[POST /user/ping HTTP/1.1
If-Modified-Since: Thu, 1 Oct 2013 05:52:04 GMT
X-Auth-Token: 5d49c835-407c-4c91-8c0b-060b700f4e25
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; SCH-I545 Build/JDQ39E)
Host: api.gotinder.com

{"lon":-122.4680752,"lat":37.7837377}]
```


How would you use the profile (to get the distance_mi) + ping API (to set the lon, lat) and obtain the exact geo-location of target?

Hint: Shortest path....

Appthority

Fail #4 Improper Handling of Private Data: Tinder

Not limited to just Tinder…

500,000+ Installs


```
15:21:10 INFORMATIONAL{"TRUDYNAMIC_ID"=>"55000", "APPLICATION"=>"com.datingflirty", "CALL"=>"network-ssl-writedata", "fd"=>"0x21500005", "ADDRESS"=>"control.kochava.com"}
[HTTP/1.1 200 OK
Server: nginx/0.7.67
Date: Wed, 31 Jul 2013 07:50:14 GMT
Content-Type: text/html
Connection: keep-alive
P3P: CP="NOI DSP COR CURa ADMa DEVa TAIa OUR BUS IND UNI COM NAV INT"
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Host: control.kochava.com

{"action":"get_homepage_members","result":true,"data":[{"oid":"123432","looking_for_type_id":[1,2,3,4,5],"familystatus_":0,
 "sexuality_":1,"smoker_":0,"drinker_":0,"religion_":0,"education_":0,"occupation":0,"employment_":0,"politics_":0,"user_confirmed":true,
 "screenname":"NaughtyAnnie","age":24,"country_code":"USA","country":"United States","city":"San Jose","post_code":"94xxx","gender": "f",
 "photo":"http:\/\/cdn.imgpict1.com\/static\/_flirt\/i\/photo_placeholders\/no_photo_woman.jpg","desc":" ","online":false, "online_from":null,
 "recently_online":false,"photo_count":1,"winked":false,"distance":2.8189704665892,
 "coordinates":{"latitude":36.12442,"longitude":-115.14637},"blocked":false,"star_sign":"Aries","features":[],"block_communication":false,
 "lifestyle":[[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0]],"personality":[0,0,0,0,0,0,0,0,0,0,0,0]},
 {"oid":"20450162974","looking_for_type_id":[1,2,3,4,5],"familystatus_":6,"sexuality_":1,"smoker_":2,"drinker_":3,"religion_":0,"education_":0, "occupation":0,"employment_"
```


\+

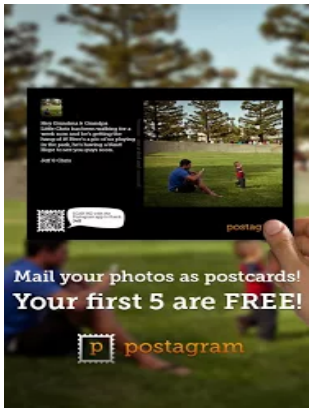
Skout, 10,000,000+ installs

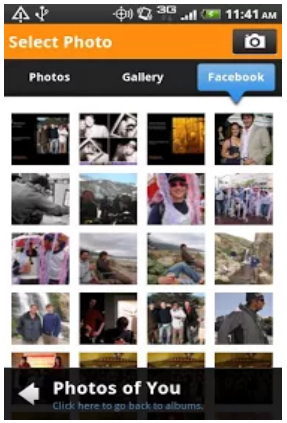
Swoon, 500,000 + installs

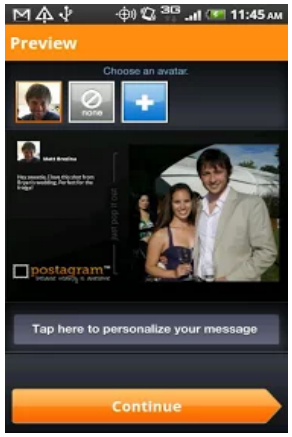
Cheeky, 100,000+ installs

Appthority

Fail #5 Using Bad or No Cryptography







What we Found in the Postogram App…

- Our analysis engines alerted us that the App was uploading private photos
- We found Postogram was sending all private photos to an unprotected server with filenames that were predictable (deterministic)

Appthority

Fail #5 Using Bad or No Cryptography

No encryption - data in motion:

- Our analysis engines alerted us that the App sending Username & Password in clear text

No encryption – data at rest:

- Our analysis engines alerted us that the App was storing Username & Password in clear text

Appthority

Fail #5 Bad Cryptography

Most common crypto mistakes

1. Not using SSL/Encryption for private data
2. Storing passwords/oauth tokens in plaintext
3. Not expiring oauth tokens properly (open to replay attacks)

Appthority®

The Reality is…

These mistakes are easily avoidable

- Best practice guidelines for storing private information do exist
- Tools to help do exist (for bigger dev shops, adding these tools into the SLDC)
- Having a mindset of "What if this was my private information?"
- Have an ***accurate*** & ***current*** privacy policy:

Don't make us call you out ☺

Appthority

Thank You

Domingo Guerra
President & co-founder
dguerra@appthority.com
@SundayWar