Opening the Kimono: Automating Behavioral Analysis for Mobile Apps

Michael Sutton
Zscaler

Session ID: MBS-108
Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

whois

- Zscaler
  - SaaS based solution for end user web and email security
  - ThreatLabz – security research arm of the company
- Michael Sutton
  - VP, Security Research
  - Previously with SPI Dynamics (HP) and iDefense (Verisign)
  - Frequent speaker at international security conferences including Blackhat, Defcon, CanSecWest, Shmoocon and RSA

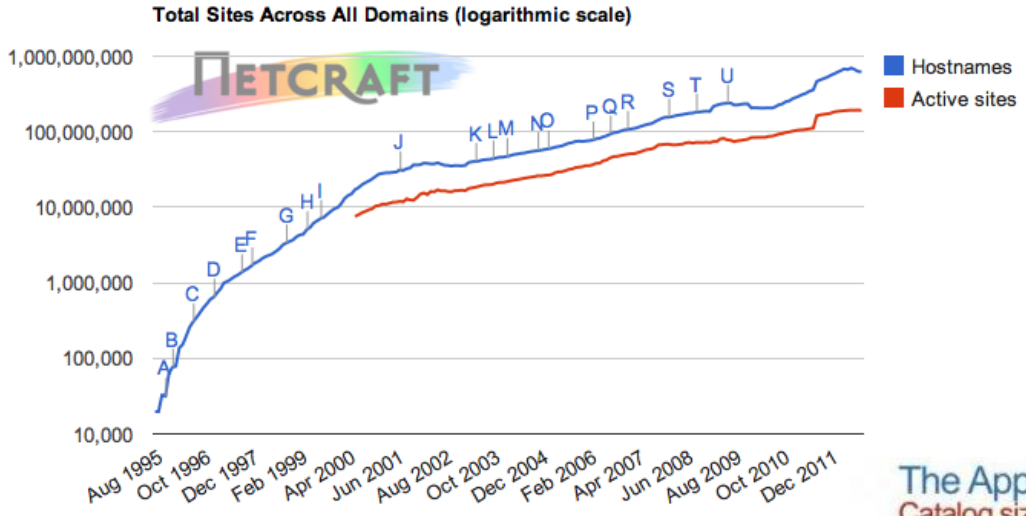
Overview

- Background – How mobile changes the game
  - App stores
  - Analysis – static vs dynamic analysis
- ZAP – Zscaler Application Profiler
  - Goals
  - Architecture
  - Demo
- Findings – Are mobile apps secure?
- Conclusion
  - Where do we go from here?

Background

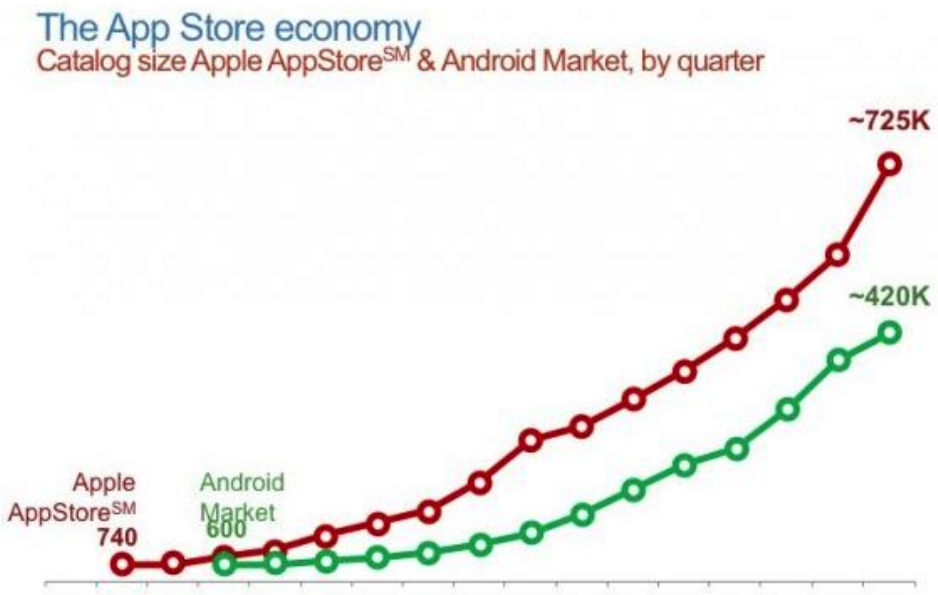
How mobile changes the game

Rapid Growth



- Rapid adoption of web development at the turn of the century ensured that security was an afterthought…

- …history is repeating itself in the mobile space
- Many apps are outsourced to 3rd parties and not properly tested for vulnerabilities and data leakage



Malicious Applications

The Register®

Phone-raiding Trojan slips past Apple's App Store censors

John Leyden
6th July 2012 15:58 GMT

A mobile Trojan that secretly sends the phone's whereabouts and its address book to spammers has slipped into Apple's App Store and Google's Play marketplace.

ZDNet®

Loozfon Android malware targets Japanese female users

By Dancho Danchev for Zero Day
August 27, 2012 -- 14:32 GMT (07:32 PDT)

Security researchers from Symantec have detected a new Android trojan currently circulating in the wild, attempting to socially engineer Japanese female users into downloading and executing the application on their mobile device.

HELP NET SECURITY

Bogus GTA Vice City Android game leads to SMS Trojan

Posted on 11.09.2012

GFI has recently spotted a fictitious Vice City version of Grand Theft Auto being offered on a third-party site that tricks users into downloading a Trojan masquerading as a Flash update. Once the victims download, install and run the bogus app, they are faced with a big button they have to press in order to start the game. But clicking on just makes another message appear, saying ""Flash Player is required" and offering a download link

Differing Approaches to Mobile App Security

		Google
Philosophy	Walled garden	Open
Approval process	Rigid – apps cannot diminish user experience or replicate functionality in native apps	Apps rarely rejected Security via a 'crowdsourcing model'
Rejected applications	Violate SDK (i.e. Path) Censored (i.e. Drones+/Clueful) Content ('over the line') Weak ('amateur hour')	Known malicious applications or copyright violations
App permissions	SDK restricts permissions and users must explicitly allow permissions as needed	SDK permits broad access Users must explicitly allow all necessary permissions at installation

App Store Approval Process

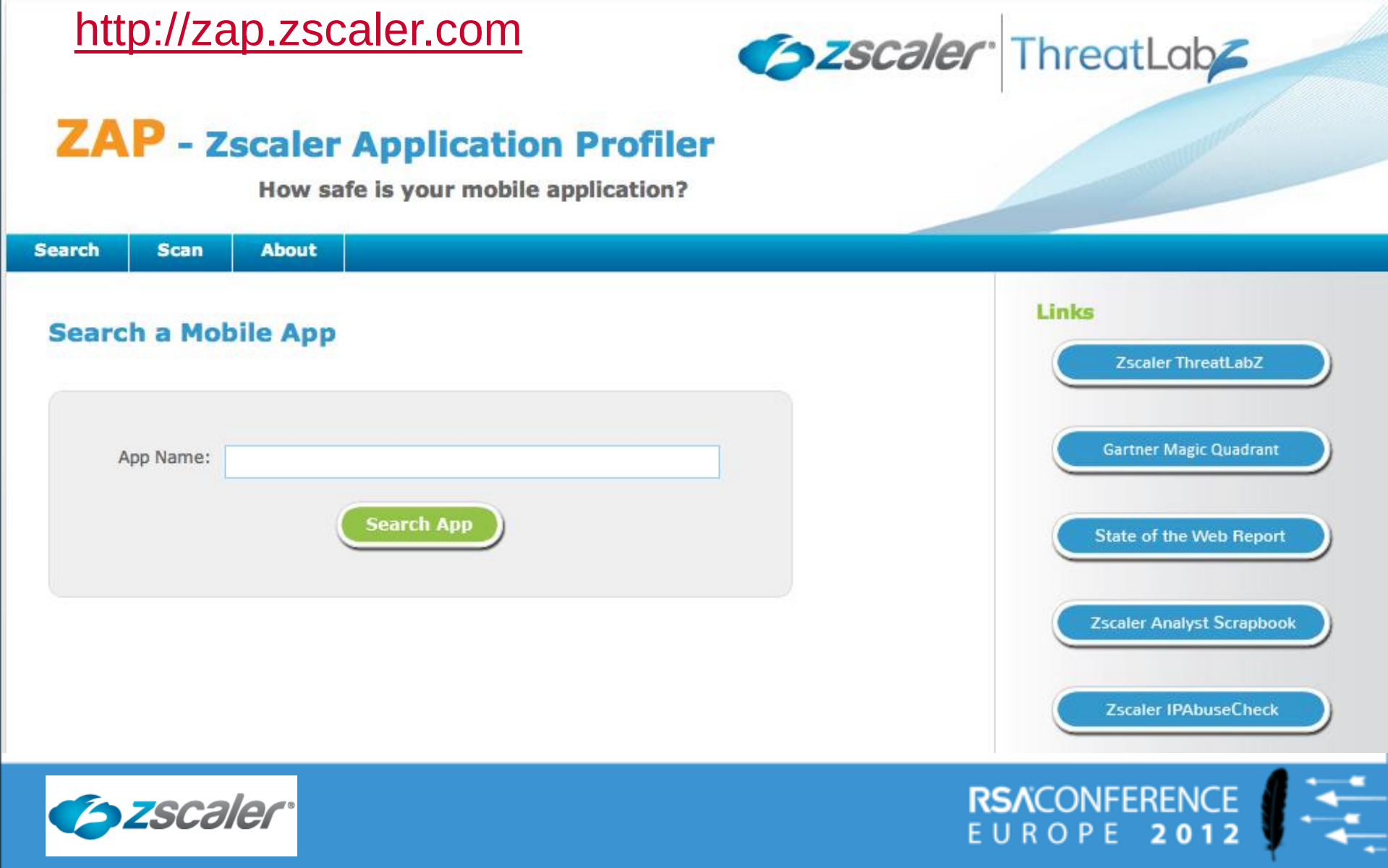
	App Store	Google Play
Process	• Manual review • Automated - private APIs	• Bouncer – homegrown • Crowdsourcing
System	Unknown	Linux, QEMU emulator
Rejected Apps	• Apps that crash • Do not perform tasks described	• Known malware, spyware and Trojans • [bad] behavior
Coverage	???	New and existing apps
Other	???	• Tests originate from known IP address block • 40% drop in malicious apps per Google
Known bypass techniques	???	• Source IP/domain • System properties • Canary data (15555215504)

ZAP

Zscaler Application Profiler

ZAP - Zscaler Application Analyzer

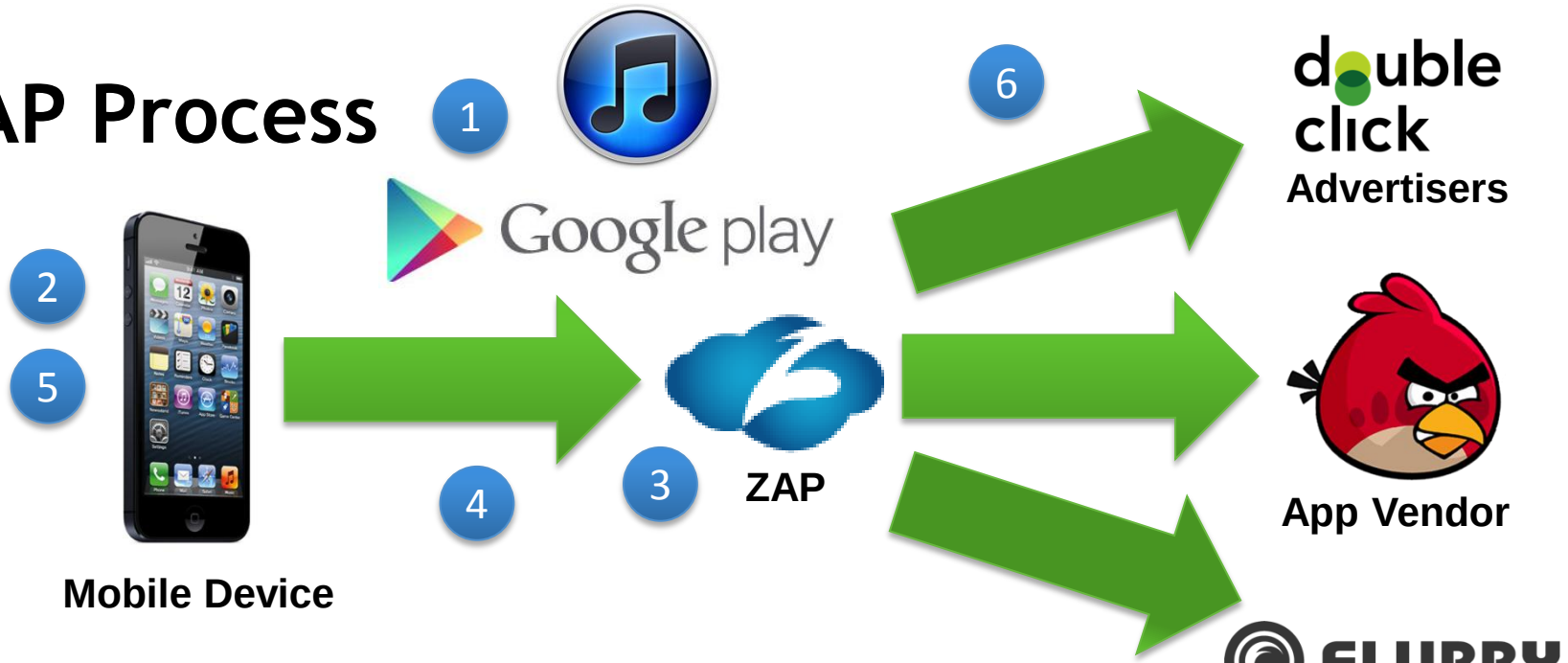
http://zap.zscaler.com



ZAP Goals

- Overall
  - Simple, web based tool to quickly determine the level of risk posed by any iPhone/Android application
- Functionality
  - Scan
    - Capture of mobile app HTTP(S) traffic
    - Automated traffic analysis to identify privacy/security issues
    - Ease of use – security expertise not required
  - Search
    - Query database to view summarized historical results
- Reporting
  - Simple assessment of security/privacy risks
  - Overall risk score

ZAP Process



1. Identify official app URL from iTunes/Google Play, enter into ZAP
2. Install mitmproxy SSL certificate (optional)
3. Enter fake personally identifiable information (PII) (optional)
4. Enter ZAP proxy settings in iOS/Android device (2 minute timeout)
5. Start ZAP proxy, launch app and use all functionality (2 minute timeout)
6. Stop proxy, download MiTM file (optional) and analyze traffic

ZAP Architecture

User Interface

- PHP
- JavaScript

Database

- MySQL

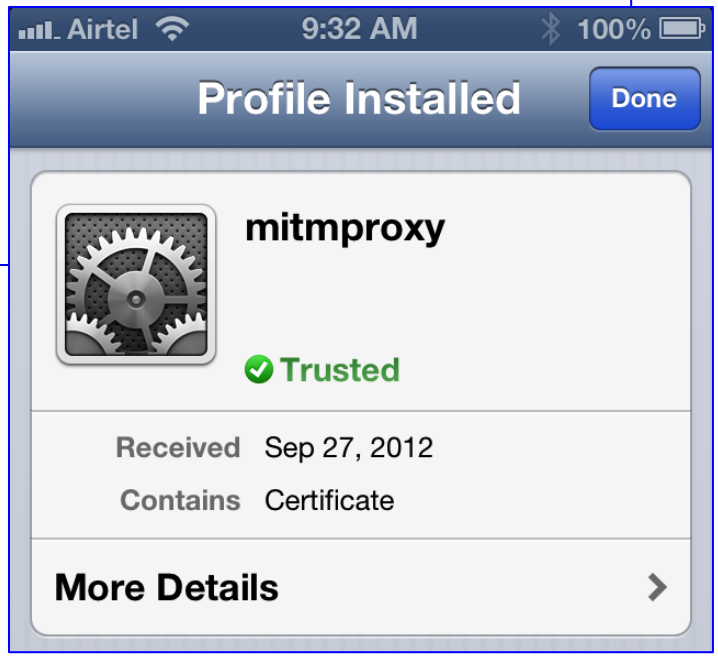
Proxy

- mitmproxy

Scanning Engine

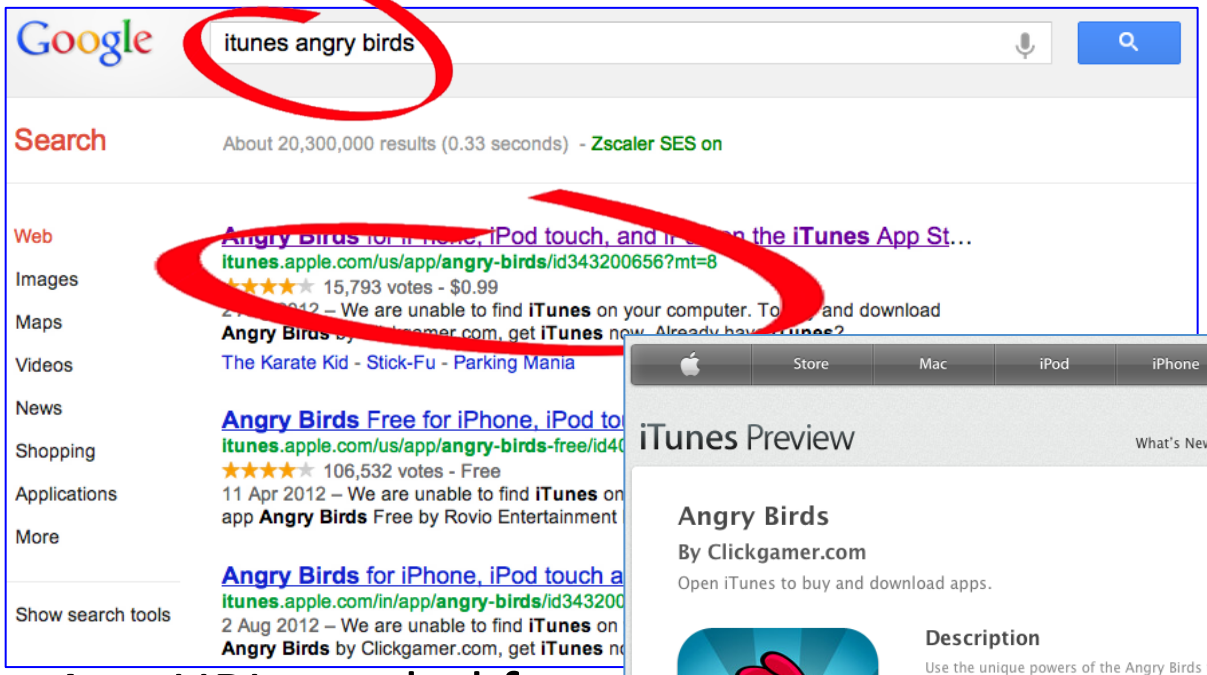
- RegEx based rules identifying:
  - Advertising sites
  - 3rd party sites
  - Shared personally identifiable info. (PII)
  - Shared device info.
  - Weak auth.

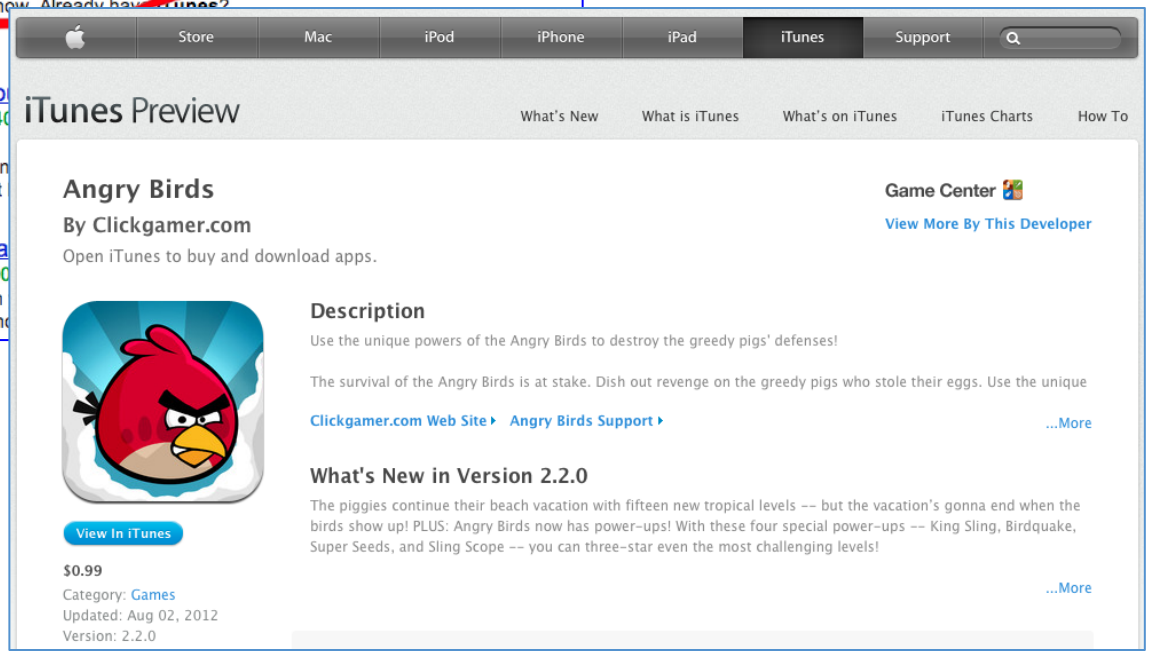
Install SSL Certificate (Optional)



- Optional but ensures complete analysis
- Apps explicitly checking server cert. may fail to communicate

Identify App URL - iTunes





- Other official/unofficial app stores will be supported in future

- App URL needed for meta data
- Pulled from iTunes/Google Play

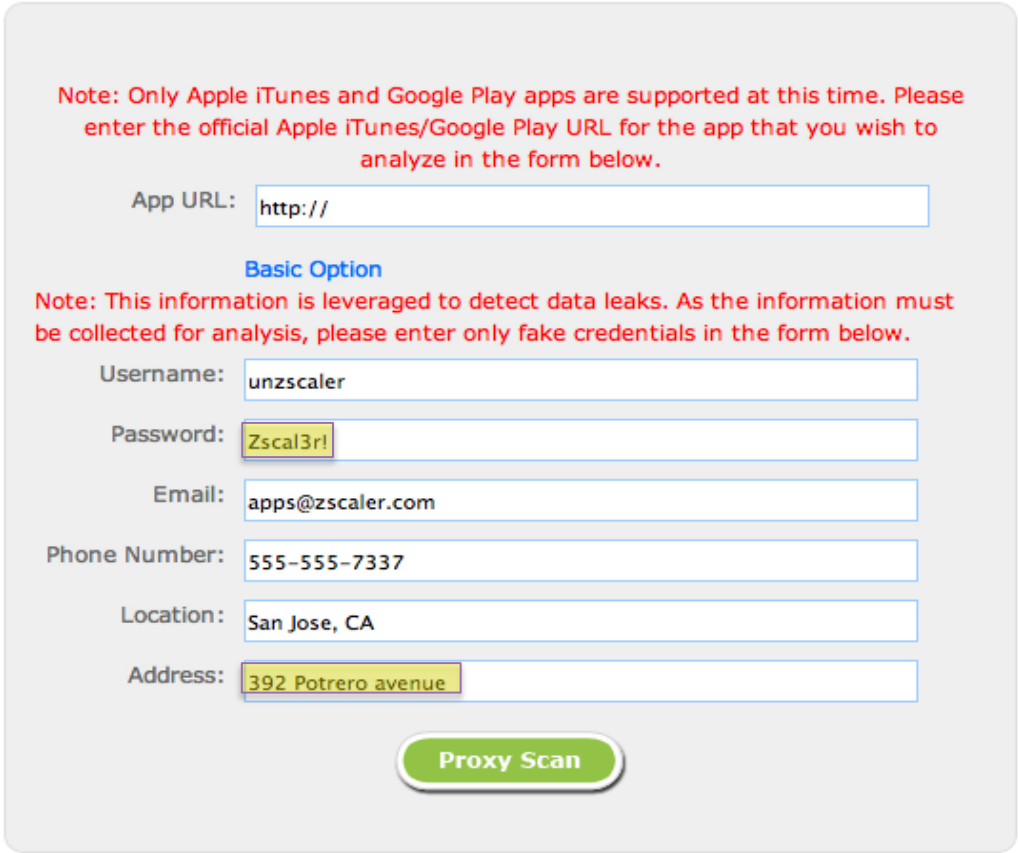
http://itunes.apple.com/us/app/angry-birds/id343200656?mt=8

Enter Personally Identifiable Information (PII)

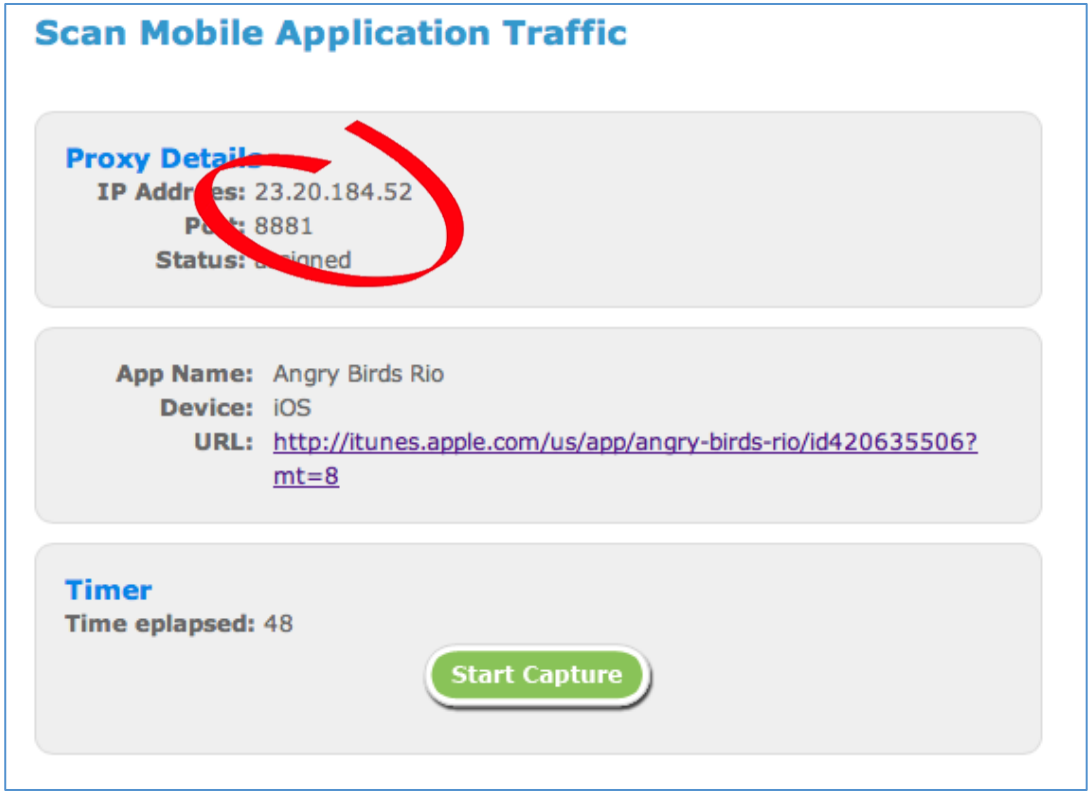
[-]http://www.bligoo.com/bligoo/apiproxy
Method: POST
Host: www.bligoo.com
User-Agent: iGloo/2.0 CFNetwork/548.1.4 Darwin/11.0.0
Request Body: apiKey=81dc9bdb52d04dc20036dbd8313ed055&method=userCreate&address=392 Potrero avenue&birthdate=1980-07-16&password=Zscal3r!&gender=female&email=apps@zscaler.com&singleness=complicated&username=unzscaler
Server Response: Q(K-* , 3PRH ,)J-. ,)

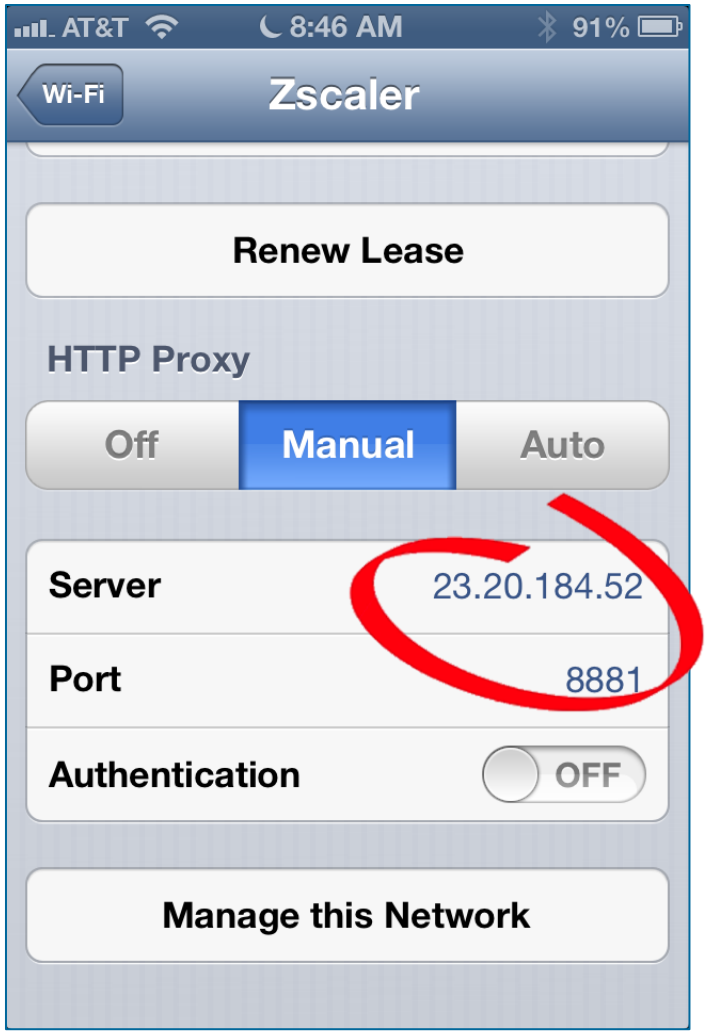
[+]http://www.bligoo.com/bligoo/apiproxy
[+]http://www.bligoo.com/bligoo/apiproxy
[+]http://www.bligoo.com/bligoo/apiproxy
[+]http://www.bligoo.com/bligoo/apiproxy
[+]http://www.bligoo.com/bligoo/apiproxy
[+]http://www.bligoo.com/bligoo/apiproxy

- Adding PII will make leak detection much more accurate
- Fake PII should be entered
- Variables don't matter as long as they're unique



Enter ZAP Proxy Settings - iPhone

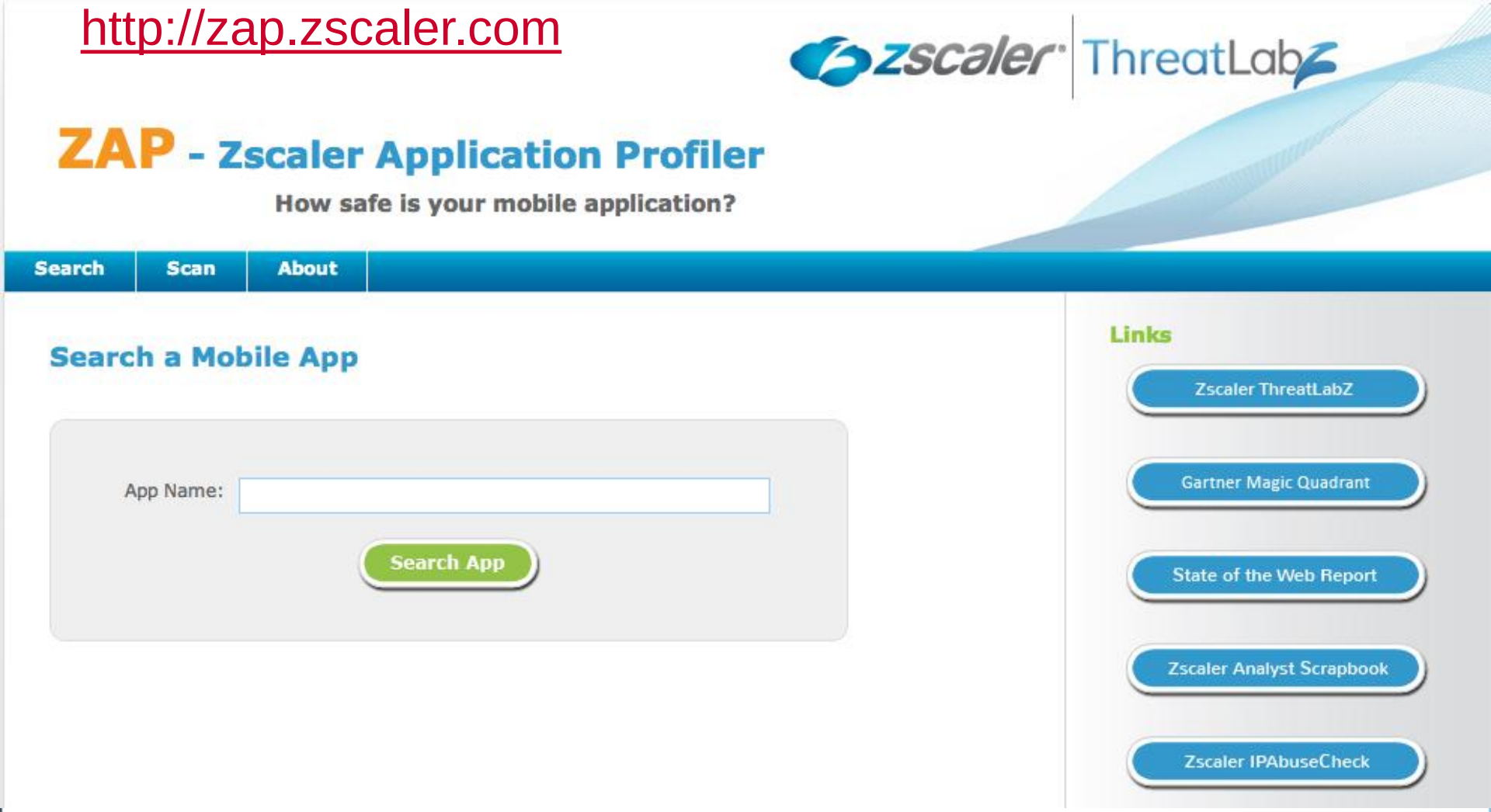




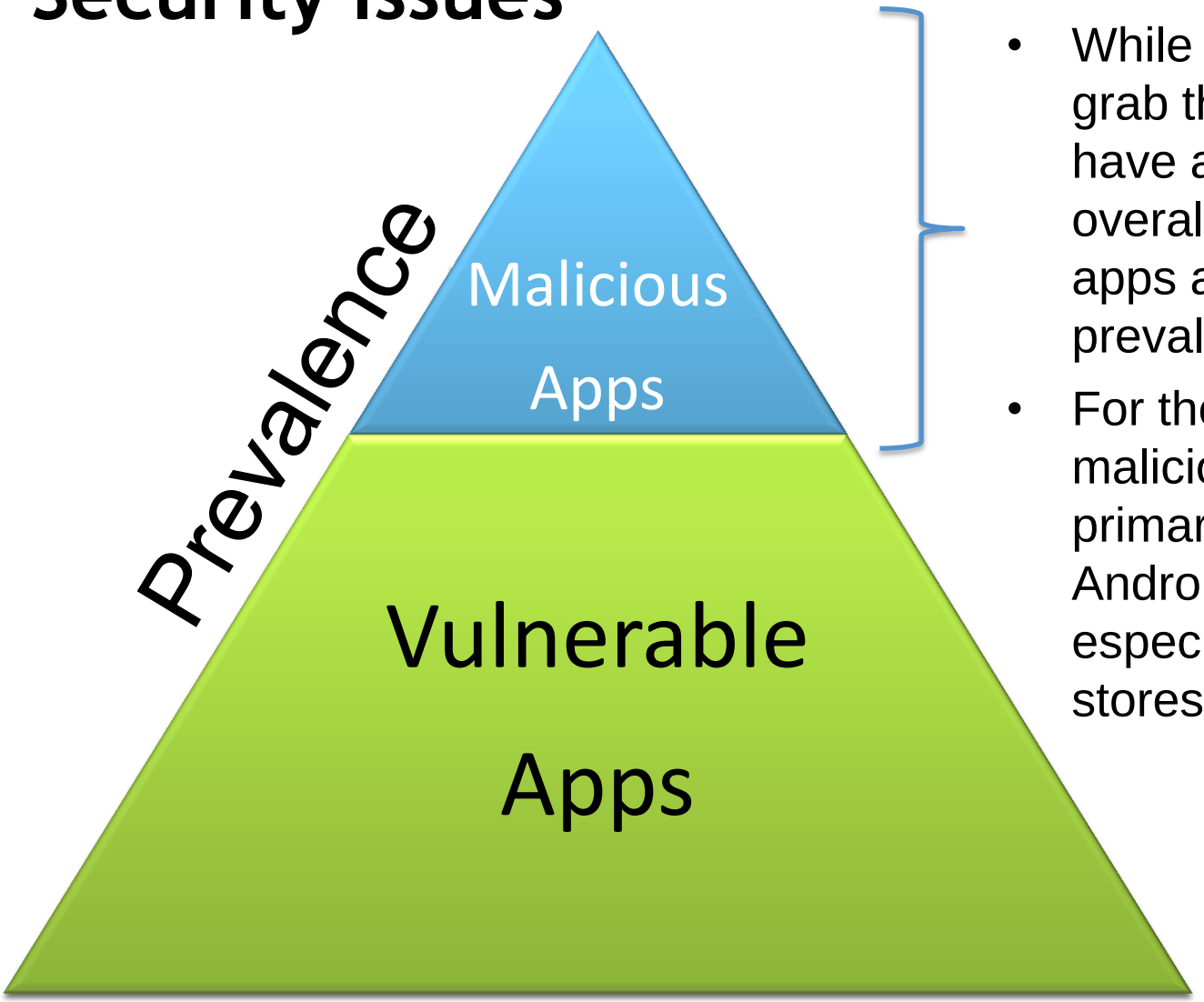
- ZAP Proxy IP/Port set on mobile device
- Timeout after 2 minutes

Demo

http://zap.zscaler.com

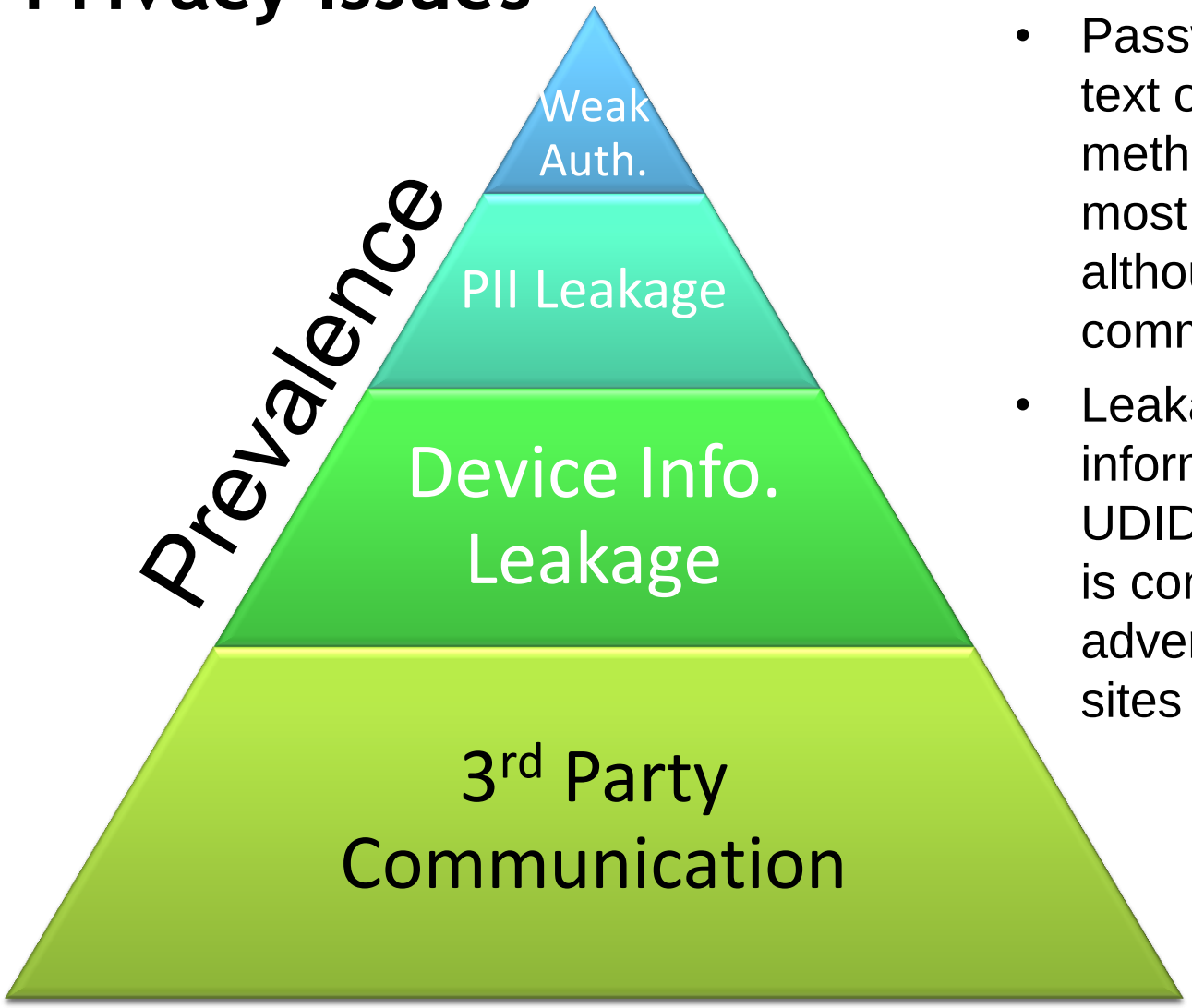


Security Issues



- While malicious apps grab the headlines and have a greater impact on overall risk, vulnerable apps are far more prevalent
- For the most part, malicious apps are primarily an issue in Android app stores, especially non-official stores

Privacy Issues



- Passwords sent in clear text or weak encoding methods represent the most significant risk, although it is the least common threat
- Leakage of device information such as a UDID is very common as is communication with advertising and analytics sites

Weak Authentication - Password Hash

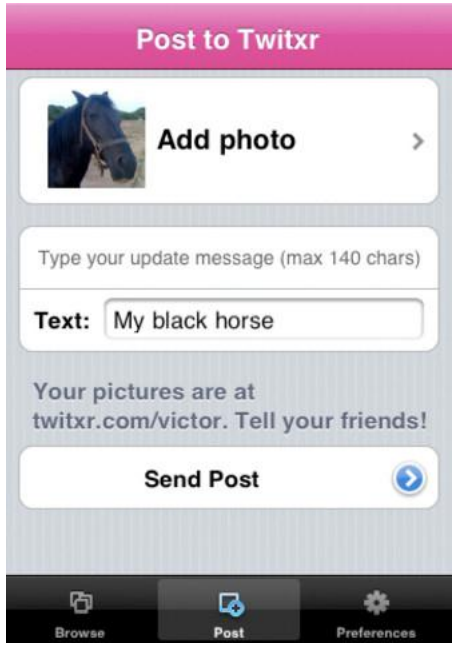
App Name: Twitxr

Version: 0.13 (September 5, 2012)

Category: Social Networking

Ratings: 484

Platform: iOS




```
Michael$ md5 -s Zscal3r!
MD5 ("Zscal3r!") = 42ef56a0090b7b29ab5ee54fc57dc156
```

```
[-
]http://www.twitxr.com/api/rest/registerNewUser?username=unz
scaler&password=42ef56a0090b7b29ab5ee54fc57dc156&email=apps@
zscaler.com
Method: GET
Host: www.twitxr.com
User-Agent: Twitxr/1.3 CFNetwork/548.1.4 Darwin/11.0.0
Server Response: EwNay , 6PvJ
[+]http://www.twitxr.com/api/rest/checkUserData
[+]http://m.twitxr.com/?user=unzscaler&md5pass=42ef56a0090b7
b29ab5ee54fc57dc156
[+]http://m.twitxr.com/unzscaler/with_friends
[+]http://m.twitxr.com/unzscaler/with_friends/
[+]http://m.twitxr.com/style_mobile_v1.0.css
```

Device Info. - MAC Address

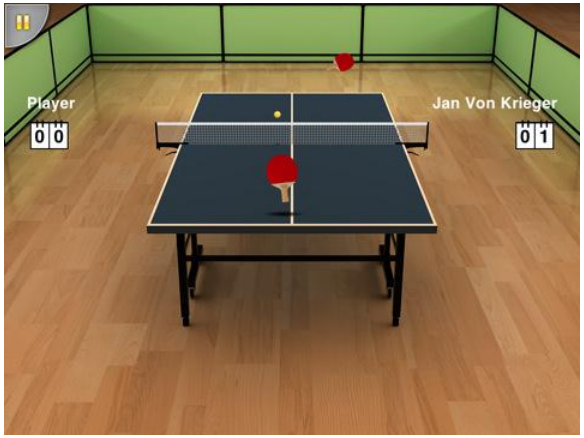
App Name: Virtual Table Tennis 2: Ping Pong Online

Version: 2.2.1 (April, 24 2012)

Category: Games

Ratings: 2,061

Platform: iOS




```
[+]http://met.adwhirl.com/exmet.php?appid=83689b572e784b64b9fb1a676a6e0e37&nid=1bf229998736452a986b4c0e6c44a5fc&type=17&country_code=en_US&appver=310&client=1
[+]https://ws.tapjoyads.com/get_vg_store_items/user_account?country_code=US&device_type=iPod%20touch&app_id=551609c1-da09-4ee2-8568-ed4e860bf845&plugin=native&os_version=5.1.1&library_version=8.1.8&language_code=en&lad=0×tamp=1346237623&sdk_type=offers&platform=iOS&connection_type=wifi&mac_address=00c610c03723&display_multiplier=1.000000&app_version=2.2.1&device_name=iPod4%2C1&publisher_user_id=M00c610c03723_M00c610c03723&verifier=5d63d97fe9a2c3de3066f1ff081745959ce8403f30ce1abdaa8dd98dc1e49143
```

Weak Authentication - Clear Text Username

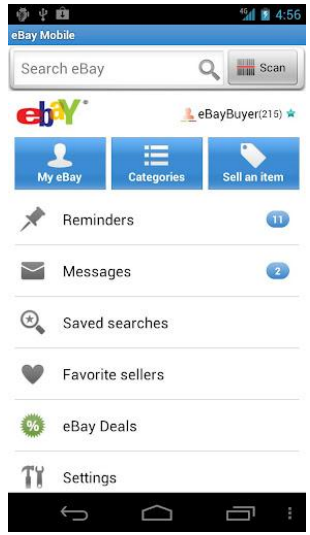
App Name: Official eBay Android App

Version: 1.8.3.5 (September 13, 2012)

Category: Shopping

Ratings: 167,826

Platform: Android




```
[-]http://open.api.ebay.com/shopping
Method: POST
        Host: open.api.ebay.com
        User-Agent: eBayAndroid/1.8.3.5
        Request Body: Details,FeedbackHistoryswap102010
        Server Response: VF}@ , ]Wku , giqL , vBF|1 , f     FzH , W , -kb>i , @mq?
, >%so , %JN. , , v:#{
[+]https://svcs.ebay.com/services/mobile/v1/DeviceConfigurationService
...
[-]https://svcs.ebay.com/services/mobileor/v1/IPhoneApplicationProcessService
Method: POST
        Host: svcs.ebay.com
        User-Agent: eBayAndroid/1.8.3.5
        Request Body: swap102010
        Server Response: B%Rlf , , UUypd , >%WLu , MEi) , ~[vg , , ]/c4 , ] , 3tX@
```

Leaked Device IDs

USA TODAY

Hackers AntiSec claim FBI is collecting Apple IDs

By Scott Martin, USA TODAY | Updated 9/4/2012 8:15 PM

SAN FRANCISCO – The Internet was abuzz Tuesday with charges and countercharges as AntiSec released information on 1 million Apple customers that the Internet hacker collective claims was collected by the FBI.

Slate

FBI Denies It Was Source of Hacked Apple User Information

By Will Oremus | Posted Tuesday, Sept. 4, 2012, at 10:42 AM ET

Update, Sept. 4, 5:32 p.m.: The FBI has issued a statement denying that it was the source of the leaked Apple user information. Or, at least, denying that there's any evidence that it was the source of the leaked Apple user information. Here's the full statement:

CBS NEWS

Anonymous did not get Apple IDs from FBI, Blue Toad CEO says

By Chenda Ngak | September 10, 2012 4:13 PM

NBC News reports that it was actually an Orlando, Fla. publishing company that was hacked, knocking down claims that a group calling themselves Antisec obtained data from an FBI laptop. Blue Toad chief executive officer Paul DeHart told NBC News he is certain that the files released by Antisec were actually from his company. Blue Toad technicians downloaded and compared the files released by Antisec with its own database. The data set was a 98 percent match.

Device Info Leakage - UDID

App Name: Hangman ®SS

Version: 2.2.6 (July 20, 2012)

Category: Games

Ratings: 22,356

Platform: iOS

[+]http://ads.mopub.com/m/open?v=8&udid=sha[redacted]EDC6FBBD41&id=366248637

[+]https://ws.tapjoyads.com/connect?mobile_network_code=&country_code=US&device_type=iPod%20touch&app_id=02aa9e96-7734-47b9-a199-187e294ca557&os_version=5.1.1&library_version=8.1.6&language_code=en&lad=0×tamp=1346830292&platform=iOS&allows_voip=yes&carrier_country_code=&mobile_country_code=&mac_address=00c610c03723&display_multiplier=1.000000&udid=c5a53500780d25743c08f079184903a2d246baad&app_version=1.20&carrier_name=&verifier=37d48f9d34a996dfcda2fd5bb8ee21229afa6f4bfd26d3b2f4edbcd70af81411

[-]https://www.chartboost.com/api/install.json

Method: POST

Host: www.chartboost.com

User-Agent: HangmanFree/1.20 CFNetwork/548.1.4 Darwin/11.0.0

Request Body:

sdk=2.5.11&os=5.1.1&uuid=c5a53500780d25743c08f079184903a2d246baad&app=4ed32026cb6015bd11000000&ui=0&signature=ecf69ddb296fe193d8963e8a12795707&country=US&bundle=1.20&language=en&model=iPod%20touch&

Dijit


TV
ENTER
VOL
CH


Verizon
11:40 AM
89%
TV
My Shows
Netflix
Today
CCHD
745
Futurama
Obsoletely Fabulous
12:22 PM - 12:54 PM
HD
Futurama
Bender Should Not Be Allowed on Tele...
12:54 PM - 1:26 PM
HD
USAHDP
738
House
Need to Know
1:00 PM - 2:00 PM
781
Saturday Night Live
1:00 PM - 2:00 PM
704
30 Rock
The One With the Cast of Night Court
1:30 PM - 2:00 PM
HD
It's Always Sunny in Philadelphia
Guide
Devices
Activities
Rooms
Settings


Verizon
11:41 AM
89%
Guide
30 Rock
14
NBC
Today, 11:30 AM - 12:00 PM
CH703
Watch
On Now!
HD
30 Rock
I Do Do
Liz meets the man of her dreams; Jack's love triangle comes to a head; Kenneth tries to avoid a promotion that would send him to Los Angeles.
Originally aired on 05/20/2010
Liked by 11 Facebook friends and 46 people on Dijit
Check In
Guide
Devices
Activities
Rooms
Settings

PII Leakage - Social Networks

App Name: Dijit Universal Remote and TV Show Guide with Netflix Listings

Version: 3.0.1 (January 08, 2012)

Category: Entertainment

Ratings: 949

Platform: iOS

```
[+]http://www.dijit.com/update_with_udid.json
[+]http://www.dijit.com/phone_states.json
[-]http://www.dijit.com/user_check_ins.jso?user_id=46947
Method: GET
        Host: www.dijit.com
        User-Agent: Dijit 3.0.1 (iPad; iPhone OS 6.0; en_US)
        Server Response: [{"created_at":"2012-03-
04T15:04:59Z","user":{"name":"Michael
Sutton","user_id":46947,"udid":"3b1999a3c15ceda95c918e7cae87d21f15828031","memb
er_since":"2012-03-
04T15:04:59Z","pic_url":"http://graph.facebook.com/100000195781259/picture"},"t
ms_id":"SP002598330000","dijit_id":9101408,"dijit_root_id":9101408,"title":"MLB
Preseason Baseball","comment":"likes this","id":37871,"updated_at":"2012-03-
04T15:04:59Z","episode_title":"Houston Astros at Washington
Nationals","thumb":2,"category":"t"},{"created_at":"2012-02-
17T04:12:09Z","user":{"name":"Michael
Sutton","user_id":46947,"udid":"3b1999a3c15ceda95c918e7cae87d21f15828031","memb
er_since":"2012-02-
17T04:12:09Z","pic_url":"http://graph.facebook.com/100000195781259/picture"},"t
ms_id":"SH000199170000","dijit_id":186674,"dijit_root_id":186674,"title":"Sport
sCenter","comment":"likes this"…
```

PII Leakage - Social Networks (cont'd)

1. [-]http://www.dijit.com/user_check_ins.json?user_id=46947
   - No authentication required for request
   - User_id is an incrementing integer for every user
   - Response often includes user name and link to facebook picture
2. [-]http://www.dijit.com/user_check_ins.json?user_id=46936

Server Response: [{"created_at":"2011-12-26T01:54:02Z","user":{"name":"Julia Ballard","user_id":46936,"udid":"1135edd62cd6962039b666648ce679cbc44e75fd","member_since":"2011-12-26T01:54:02Z","pic_url":"http://graph.facebook.com/762035580/picture"},"tms_id":"EP011583840038","dijit_id":8513643,"dijit_root_id":3561536,"title":"The Good Wife","comment":"likes this","episode_season":"2","episode_number":"14",…

3. [-] http://graph.facebook.com/762035580/

Server Response:

{ "id": "762035580", "name": "Julia Kinningham Ballard", "first_name": "Julia", "middle_name": "Kinningham", "last_name": "Ballard", "link": "https://www.facebook.com/ballardtnn", "username": "ballardtnn", "gender": "female", "locale": "en_US" }

Weak Authentication - Clear Text Password

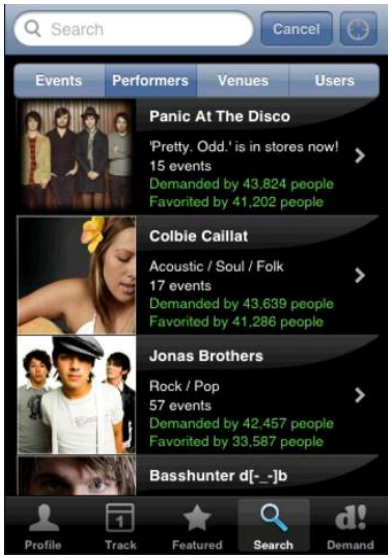
App Name: Eventful

Version: 1.0.4 (Oct 27, 2011)

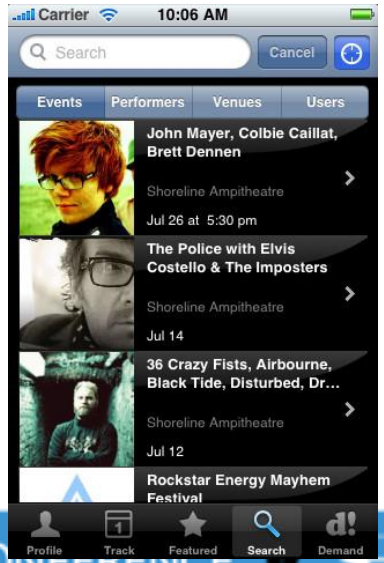
Category: Social Networking

Ratings: 9,415

Platform: iOS




```
[+]http://eventful.com/json/apps/klaxon/star
[-]http://eventful.com/json/apps/klaxon/users/validate
Method: POST
        Host: eventful.com
        User-Agent: Eventful/1.0.4 CFNetwork/548.1.4
Darwin/11.0.0
        Request Body:
password1=Zscal3r!&yob=1980&password2=Zscal3r!&location_id=
&gender=M&email=apps%40zscaler.com&opt_partners=1&location_
type=&username=unzscaler
        Server Response:
{"errors":null,"is_default_eventful_site":"1","home_url":"h
ttp://eventful.com/sanjose/events"}
[+]http://eventful.com/json/apps/klaxon/locations/search?lo
cation=38.951549,-77.333655&stsess=(null)
[+]http://eventful.com/json/apps/klaxon/users/join
[+]http://eventful.com/json/apps/klaxon/users/edit
```



Weak Authentication - Shared Libraries

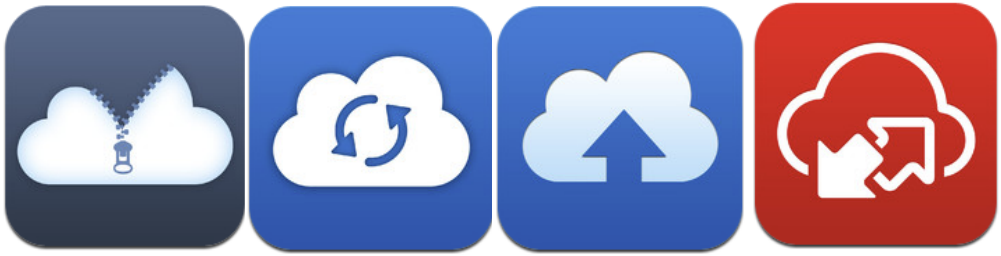
App Names: Zip Cloud, JustCloud, MyPCBackup, Novatech Cloud

Version: 1.1.2 (September 22, 2012)

Category: Productivity

Vendor: JDI Backup Ltd

Platform: iOS



```
[+]http://data.flurry.com/aas.do
[-]http://flow.backupgrid.net/account/create
Method: POST
        Host: flow.backupgrid.net
        User-Agent: ZipCloud 1.0.2 (iPod touch; iPhone OS 5.1.1;
en_US)
        Request Body:
credentials={"app_time":"100","app":"jdi_ios","app_version":"1.0.2","se
cret":"","token":""}&payload={"name":"Fnzscaler","password":"Zscal3r!",
"verify":"1cac4c9b84b77738cb1ede06054ed664","email":"apps@zscaler.com",
"partner_id":"2"}&version=1.0.0
        Server Response: ;;v# , r , '+4f , %eG}
[+]http://flow.backupgrid.net/auth/request
[+]http://flow.backupgrid.net/account/devices
[+]http://flow.backupgrid.net/device/licence
[+]http://flow.backupgrid.net/device/roots
```

Mobile Malware Stats

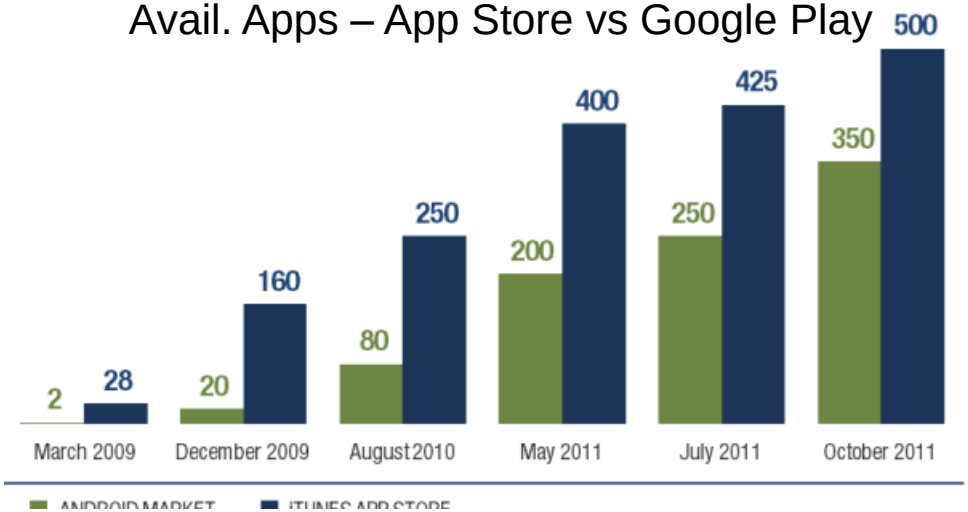
Mobile Threats By Platform

	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL
Android							9	120	129
iOS						2			2
J2ME			2		2	7	2	5	18
PocketPC	1		1	2	7	8	19	2	40
Symbian	24	124	188	44	19	21	50	58	528
	25	124	191	46	28	38	80	185	717

http://www.f-secure.com/weblog/archives/MobileThreatReport_Q1_2012.pdf

- Majority of malware families now target Android
- Malware on iOS apps remains rare
- Malicious apps represent a small fraction of total apps in official stores

Avail. Apps – App Store vs Google Play



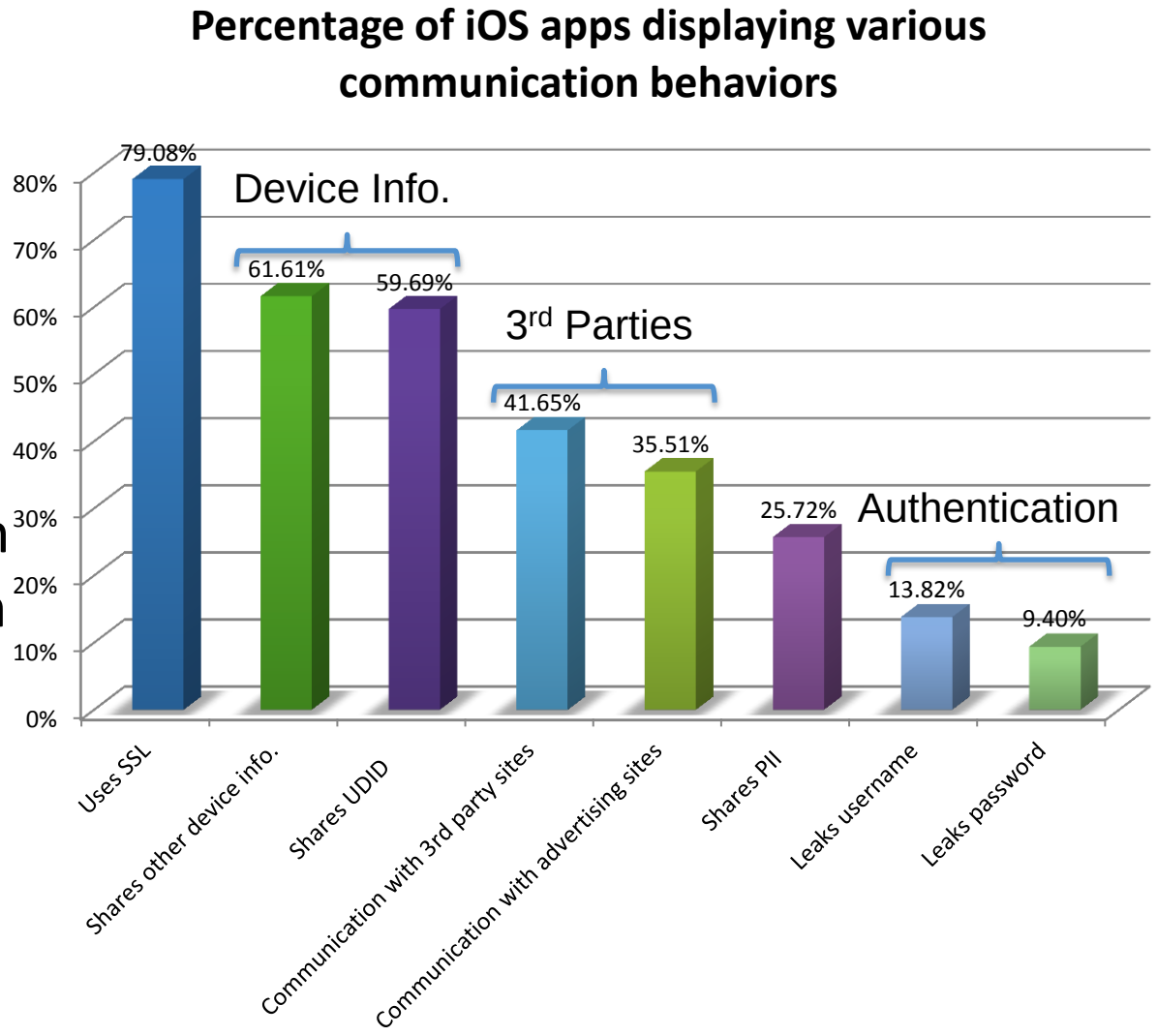
http://blog.flurry.com/default.aspx?Tag=App%20Store

Findings

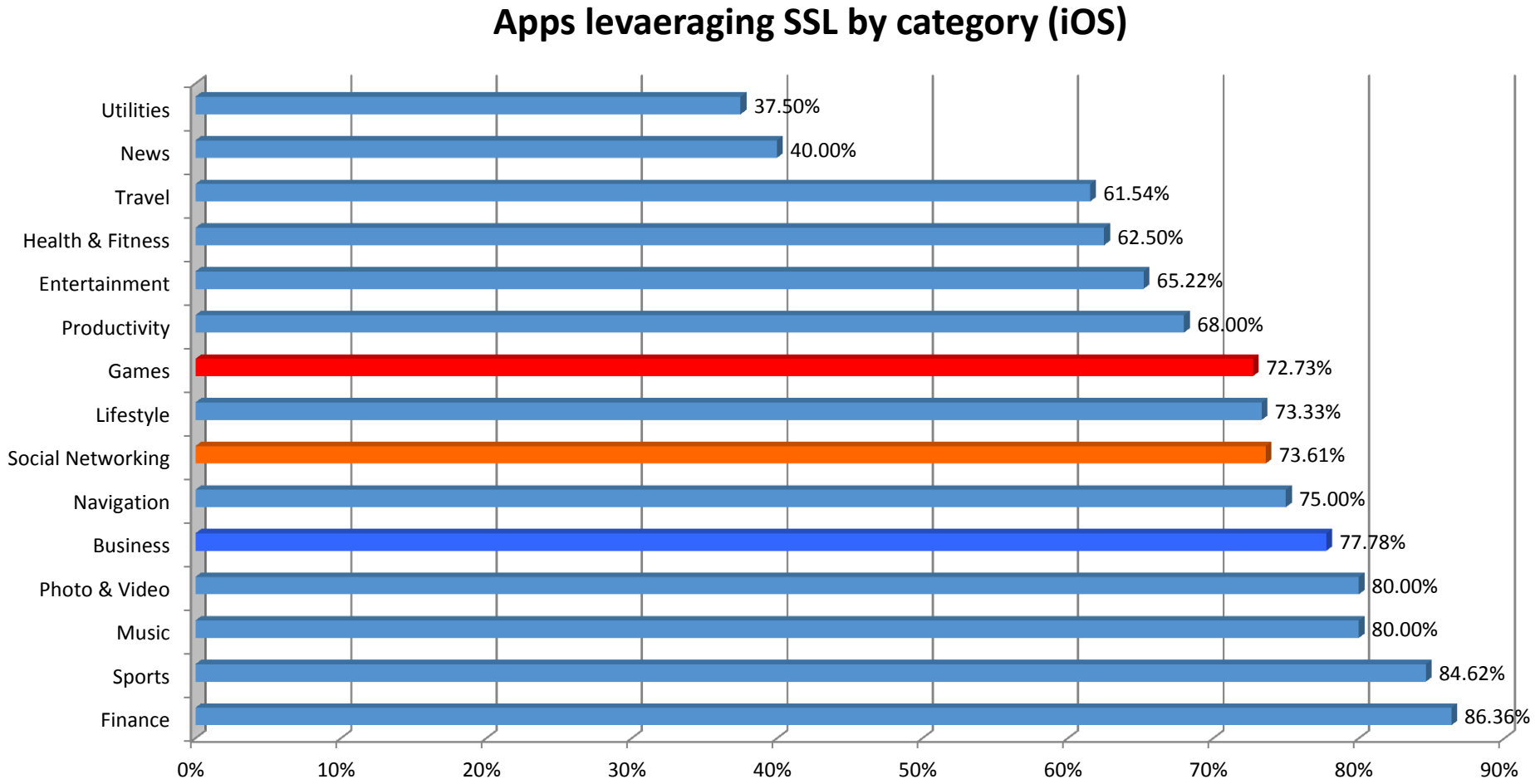
ZAP Results to Date

Mobile Stats - Overall iOS

- Stats cover free apps, therefore advertising/analytics communication common
- Leaked password/username – communication w/out SSL
- Collecting device info. a common practice



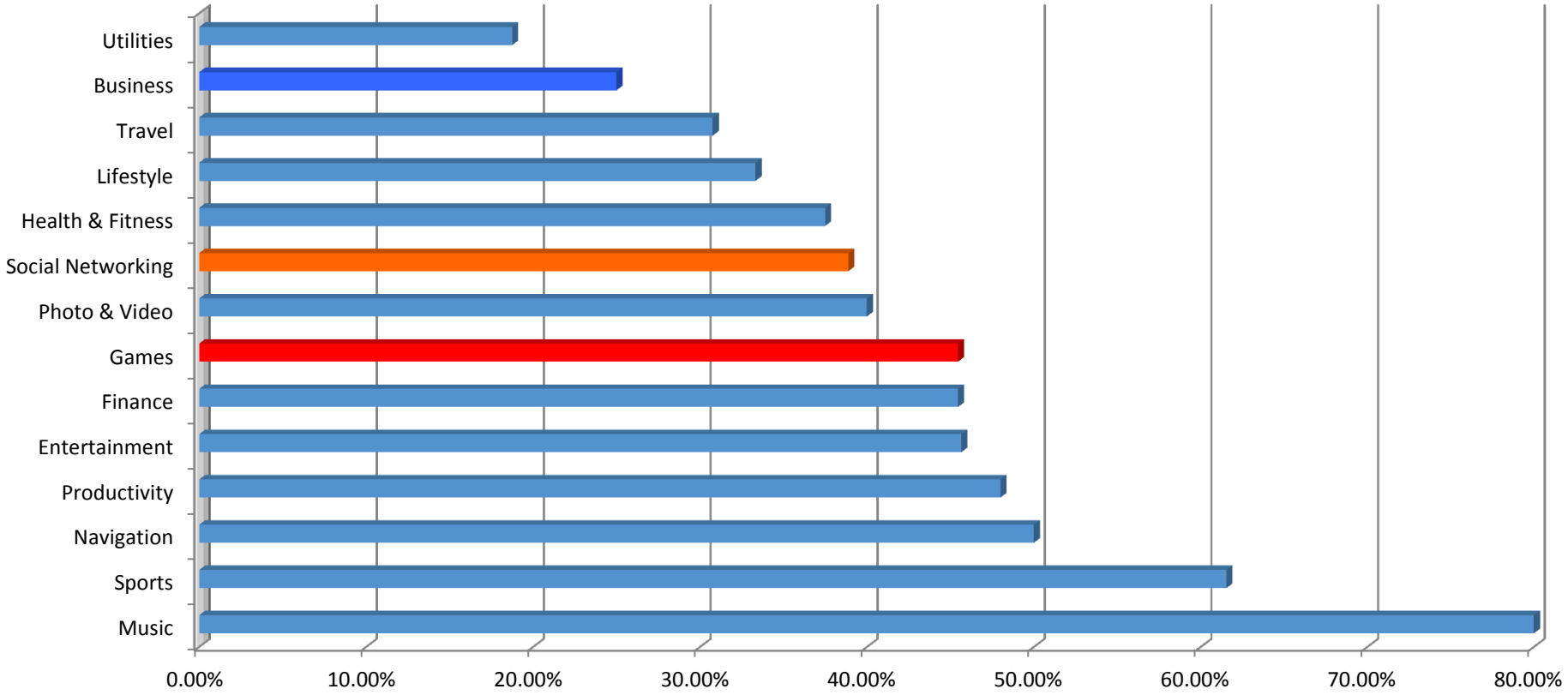
Findings - SSL (iOS)



- SSL commonly employed by apps in for at least some communication

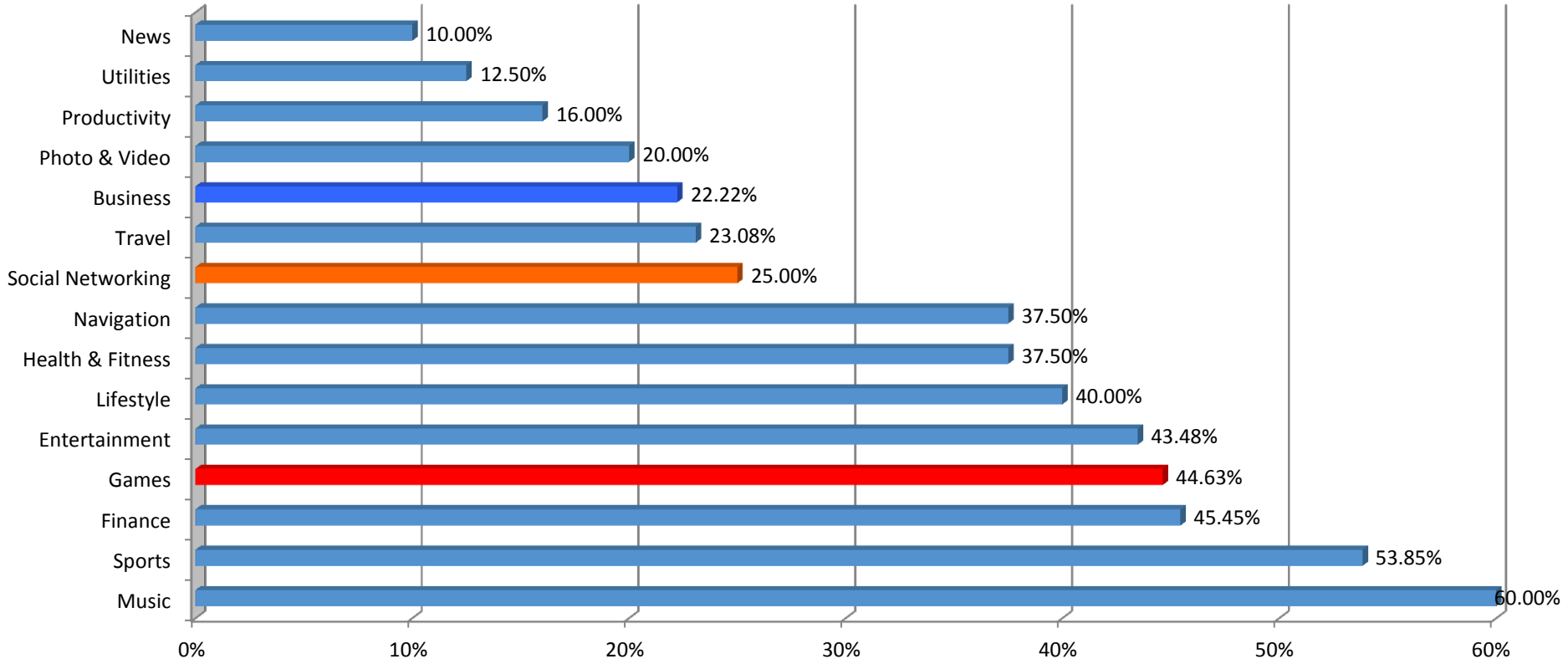
Findings - 3rd Parties (iOS)

Apps Communicating with 3rd party sites by category



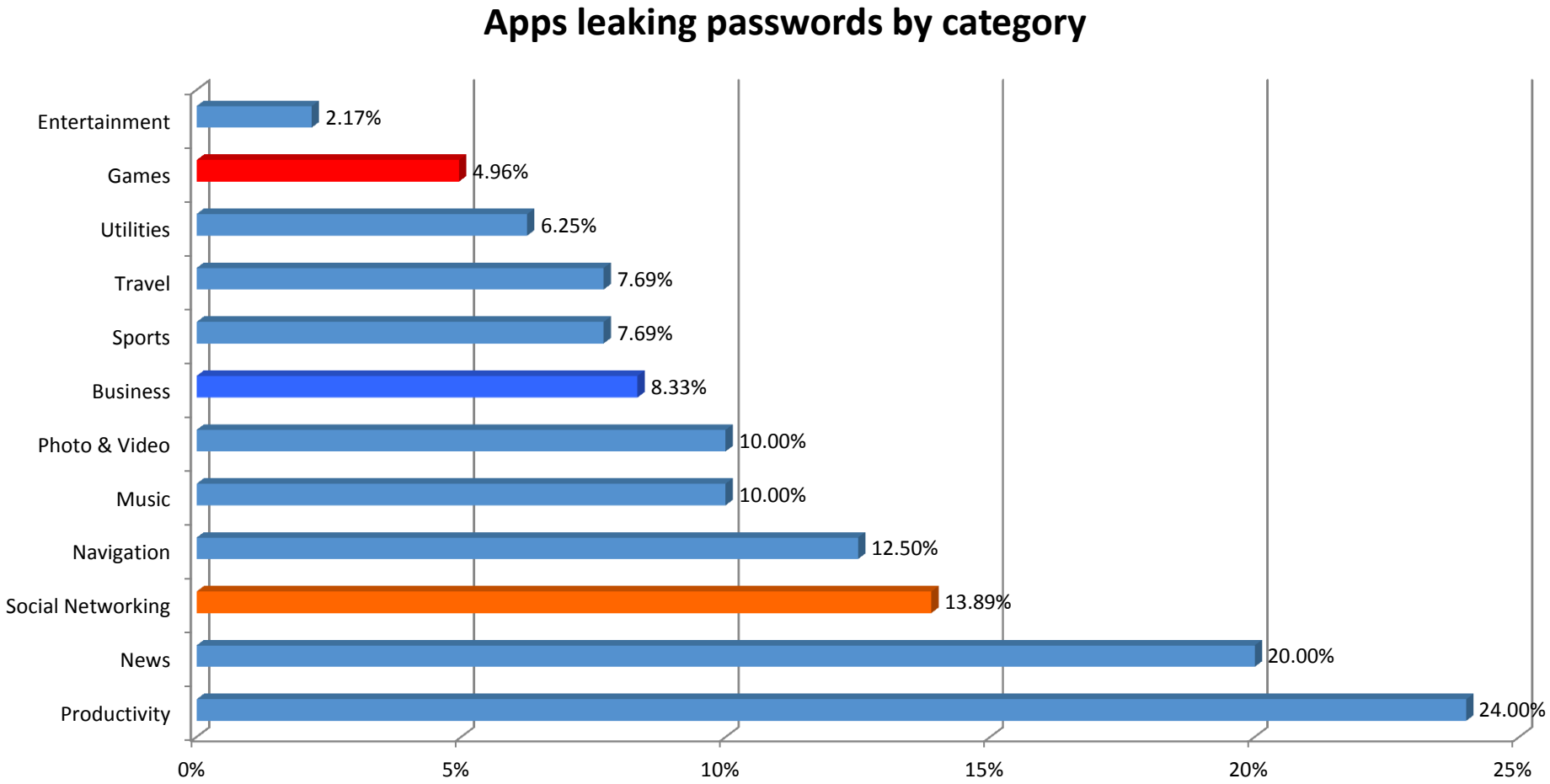
- Business apps less likely to communicate w/ 3rd parties
- 3rd parties include analytics sites and web based content

Findings - Advertising (iOS)



- Business apps less likely to leverage advertising
- Free apps commonly leverage advertising

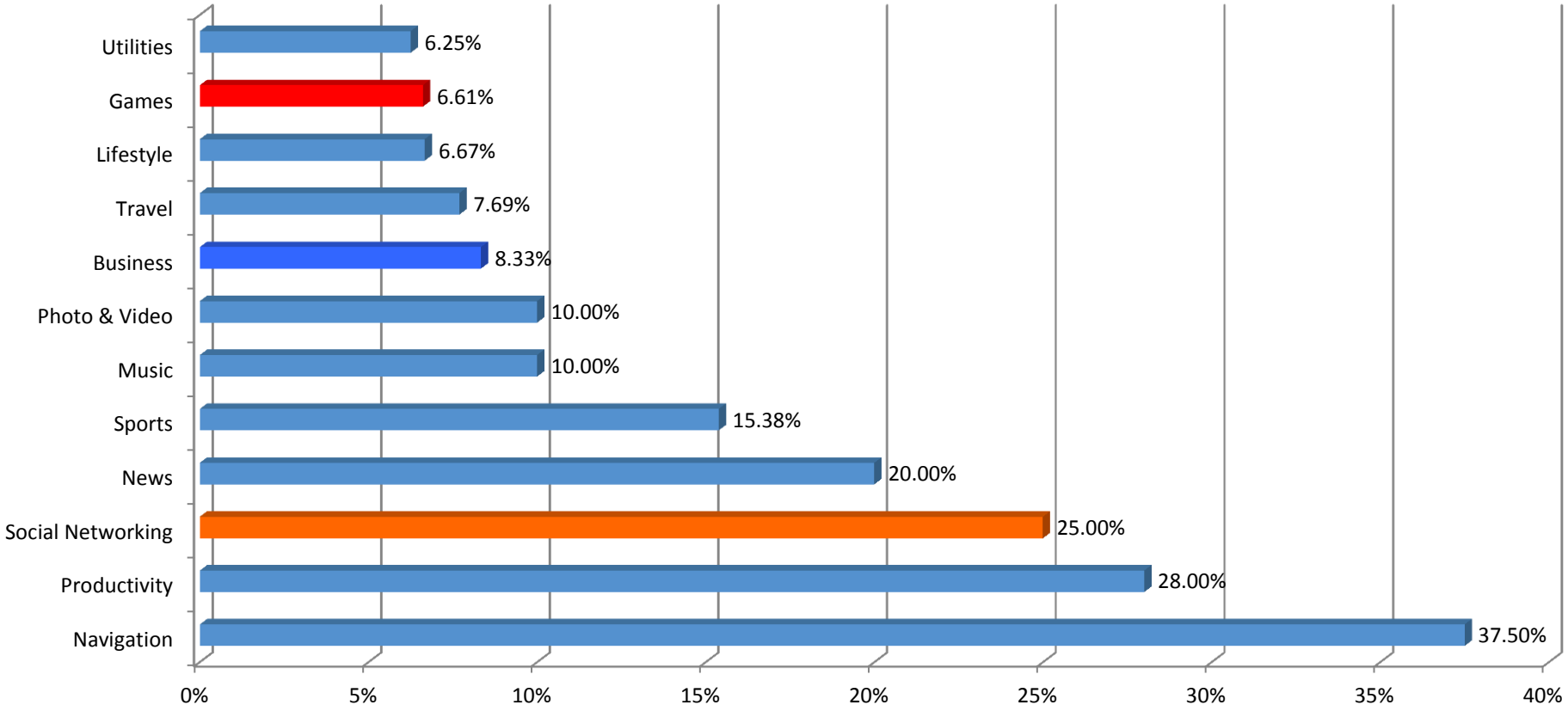
Findings - Passwords (iOS)



- Passwords considered leaked if sent in clear text or with simple encoding (i.e. Base64)

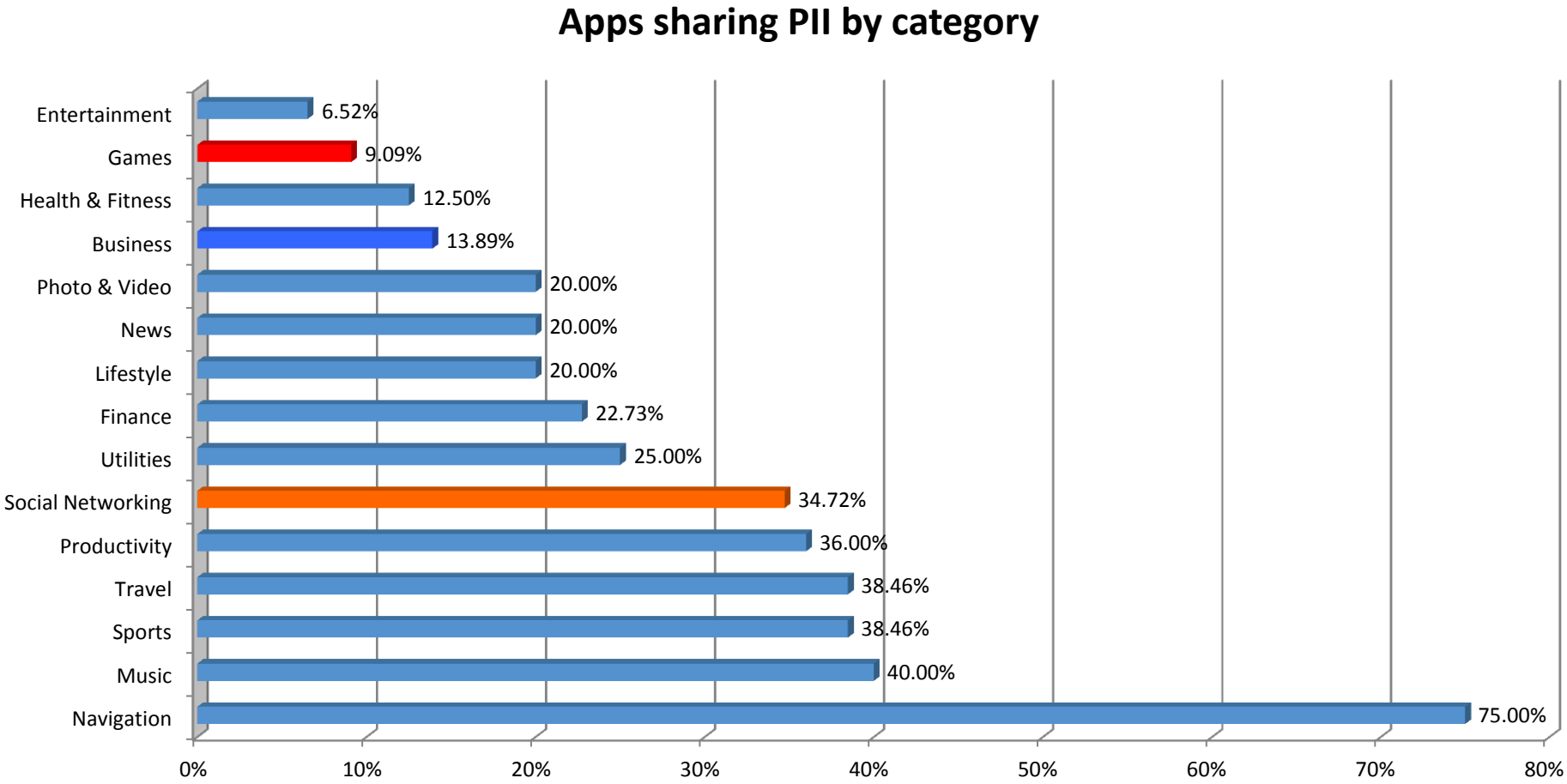
Findings - User Names (iOS)

Apps leaking user names by category Percentage



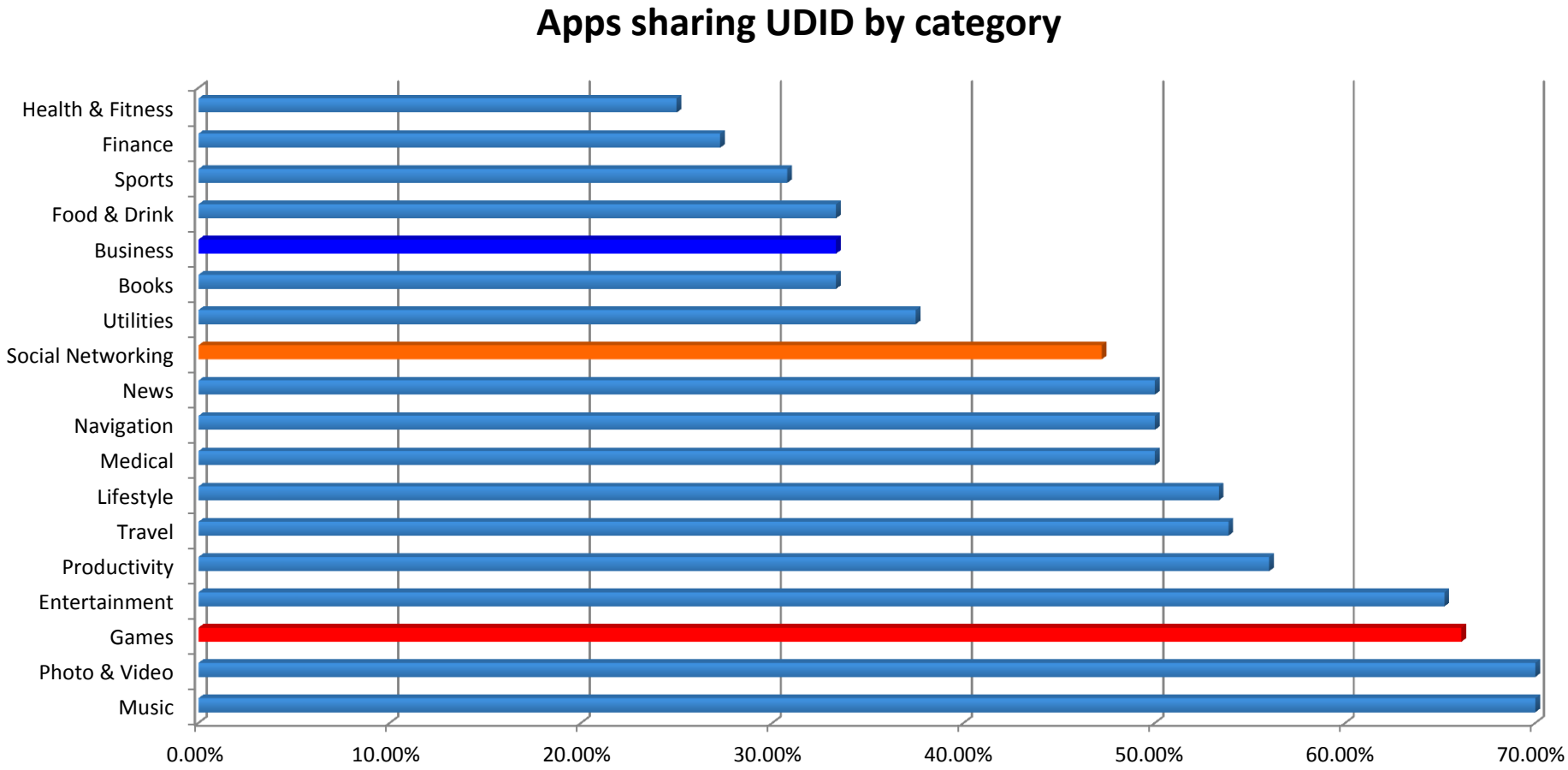
- User names considered leaked if sent in clear text or with simple encoding (i.e. Base64)

Findings - PII (iOS)



- PII consists of canary data - email address, phone number, mailing address, etc.

Findings - UDID (iOS)



- UDID (Unique Device Identifier) allows for activity from a specific smartphone/tablet to be tracked

Conclusion

- Risk
  - Prevalence of privacy risk significantly outweighs security risk
- Android vs iOS
  - Privacy risks are equally prevalent in both platforms
  - Malicious apps remain relatively rare and are primarily a product of Android app stores, especially unofficial stores
  - Although Google has implemented *Bouncer* to scan for malicious apps, it remains imperfect and both Apple/Google fail to filter even basic privacy issues
- Cause
  - Mobile application development is exploding and there are limited tools and expertise available to properly secure applications
- Solution
  - App store gatekeepers are in the best position to conduct basic filtering to limit basic privacy risks

How to Apply What You Have Learned Today

- Identify
  - Assess business needs and risks – establish mobile strategy/policy
  - Implement technology which permits the ability to manage/monitor mobile activity (MDM, SWG, etc.)
- Enforce
  - Mobile devices must not lower overall corporate security posture
  - Monitor and manage mobile app traffic just as you would web traffic
  - Restrict use of apps that expose security/privacy risks

VP, Security Research

Michael Sutton

threatlabz.com

zap.zscaler.com