

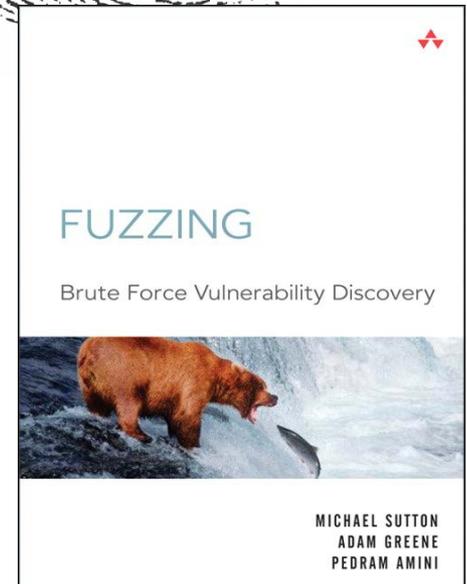


Future Shock: How mobility is forcing enterprises to completely rethink security

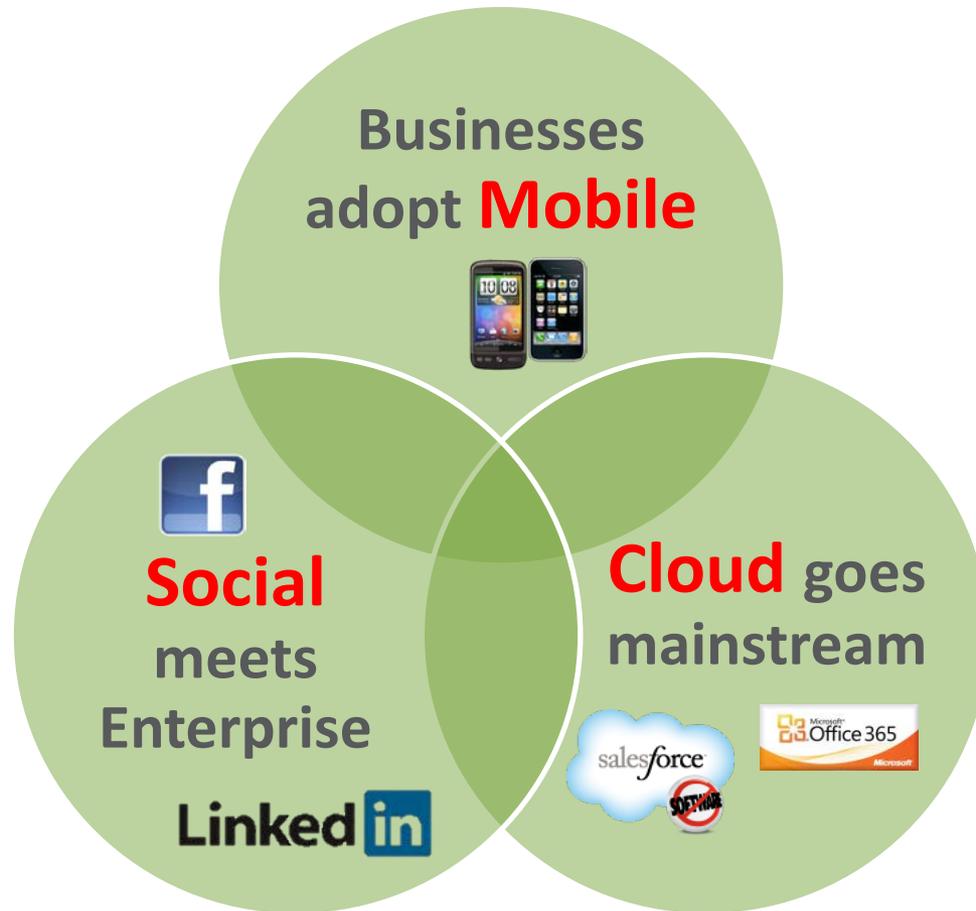
Michael Sutton
VP, Security Research
May 3, 2013

whois

- Zscaler
 - VP, Security Research
 - SaaS based solution for end user web security
 - ThreatLabZ – security research arm of the company
- Background
 - Founding Member – Cloud Security Alliance
 - SPI Dynamics – acquired by HP
 - iDefense – acquired by VeriSign
- Research
 - Web security
 - Client-side vulnerabilities
 - Book – Fuzzing: Brute Force Vulnerability Discovery



Three Mega Trends in IT



This turns traditional security & networking upside down

The evolving threat landscape

2003



Enterprises

Sedentary Workforce

- PCs and laptops
- Corporate network
- VPN connectivity required for remote employees
- Corp. owned devices

Attackers

Rogue Individuals

- Motivated by the challenge
- No financial gain

Attacks

Loud and Noisy

- Server side vulns
- Attacks were obvious, for a brief duration
- Damage could be costly but easy to clean up

Security

- URL filtering
- Anti-virus

2013



Dynamic Workforce

- Smartphones and tablets
- Working from free wifi networks and 3G/4G connections
- BYOD

Organized Criminals/Nation States

- Well funded
- Highly skilled
- Financial gain
- Political advantage

Quiet and stealthy

- Exploiting client-side vulns and social engineering
- Leveraging end users as a catalyst
- Goal - data exfiltration

- URL filtering
- Anti-virus

Enterprise security has failed to keep pace with the evolving threat landscape

Is this the Year?

Forbes

2013: The Year Android Users Get Pwned

Mark Gibbs, Contributor

CIO NETWORK | 4/24/2013 @ 10:43PM | 124 views

To date, mobile devices such as smartphones and tablets have been pretty safe from malware. This era may well have come to end.

The reason mobile devices have been immune is arguably because **in many ways the opportunities to capitalize on weaknesses and flaws in the relatively young operating systems of these new products have been scarce** in comparison to the millions of machines running, for example, Windows.

Is this the Year?

PCWorld

Report: **2011** Is the 'Year of Mobile Malware'

By Tony Bradley, PCWorld | Nov 21, 2011 5:55 AM

Smartphones and tablets continue to rise in popularity--among both consumers and malware developers. Traditional malware is still a large and growing threat as well, but **mobile platforms represent fertile ground** with less awareness and limited defenses. A new report from McAfee illustrates that **malware developers are anxious to exploit mobile devices.**

Is this the Year?



Will **2010** Be the Year of Mobile Malware?

By Larry Seltzer February 16, 2010 04:15pm EST

One of the perennial predictions for security is that **it will be the year of mobile malware. This year just might.**

Two important factors have kept malware off of mobiles (or "phones" as Microsoft calls them):

Mobile network operators, OS vendors and handset manufacturers all have code signing programs to control what code is run on the phone...

The market is fragmented; there's **nothing like Windows running on the overwhelming majority of devices...**

Is this the Year?



2006: Year of the mobile malware

December 19, 2005 4:43 PM PST

By Dawn Kawamoto

Staff Writer, CNET News

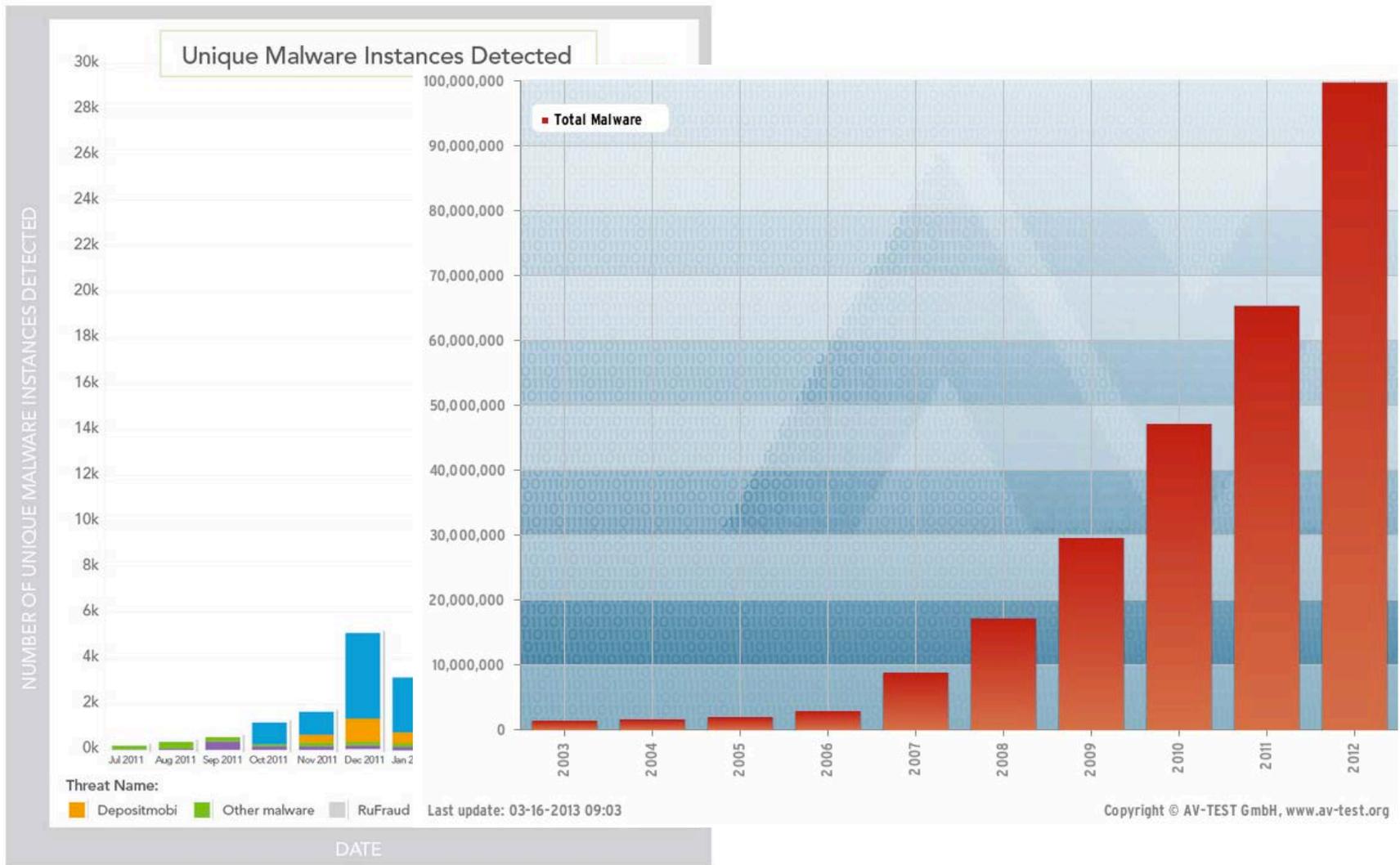
Mobile security **threats are expected to triple** in 2006 as smart phones and other mobile devices become more prevalent, according to a study released Monday by McAfee Avert Labs.

The number of malicious software programs created for mobile devices is expected to **reach 726 by the end of 2006, up from an estimated 226 at the end of 2005**, according to McAfee.

Is Mobile Malware on the Rise?

Mobile

PC



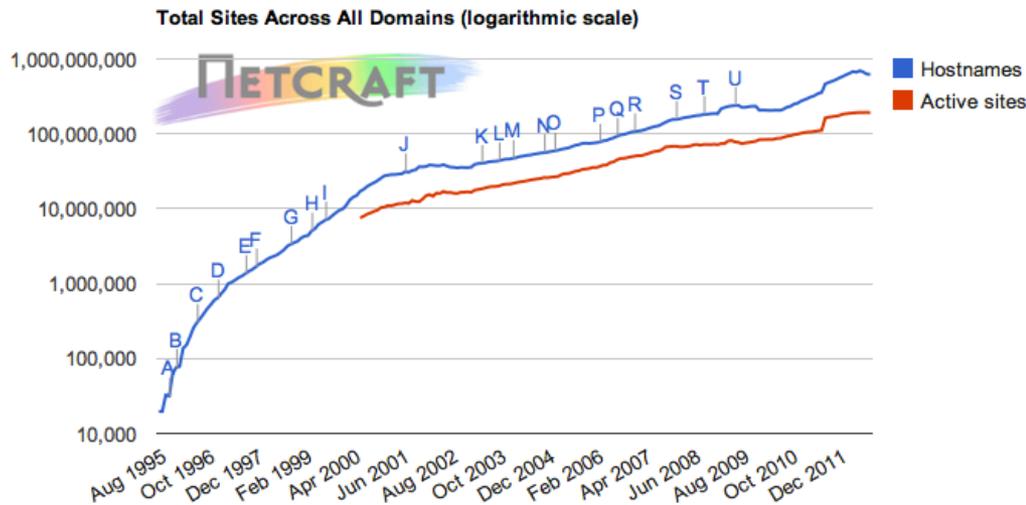
Lookout Mobile Security

All Devices Are Not Created Equal



- PCs often run numerous server side services such as RDP, RPC, HTTP, FTP, etc.
- Mobile app stores provide a validation layer
- Mobile fragmentation (among both vendors and O/S versions) limits total exposure
- PC browser plugin framework a significant malware entry point
- Malicious apps can be revoked via official app stores

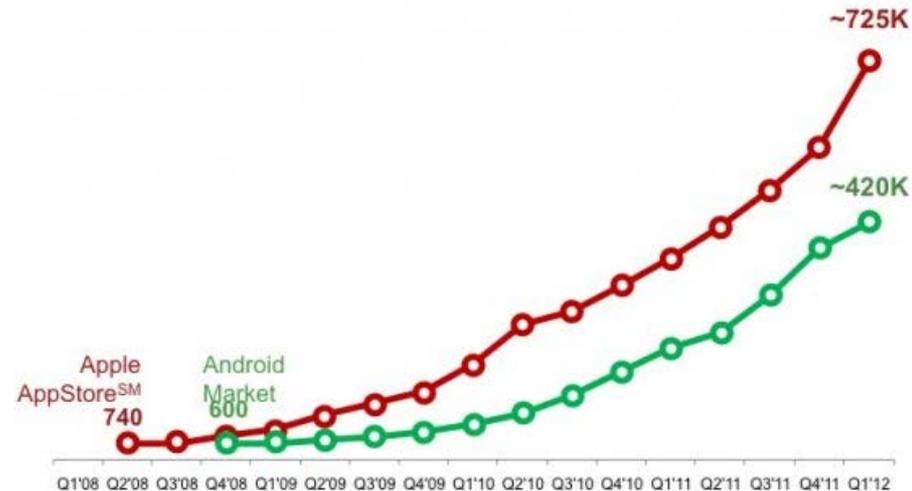
Rapid Growth



- 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

the App Store economy
Catalog size Apple AppStoreSM & Android Market, by quarter



Source: Apple, Google, Xylogix; Chart created and compiled by Accenture, 2012.
Copyright © 2012 Accenture. All rights reserved.

Mobile Challenges

■ Ownership

- BYOD, cloud and social are forcing CISOs to lose control of the devices and data that they are tasked with managing

■ Visibility

- Enterprises have significant blind spots and are no longer able to understand total risk and exposure
 - » Remote users bypass appliances
 - » Reporting not consolidated

■ Hyper-growth

- Lack of security tools and skills to fully understand security/privacy
- Blind trust of App Store gatekeepers

■ Traditional endpoint security is dead

- Host based – Resource constraints and restrictive O/S ecosystem
- Appliance Based – Can't protect what it can't see

Malicious Applications

The Register

John Leyden
6th July 2012 15:58 GMT

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

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.



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



| 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 | <ul style="list-style-type: none">• Manual review• Automated identifies use of private APIs | <ul style="list-style-type: none">• Bouncer – homegrown• Crowdsourcing |
| System | Unknown | Linux, QEMU emulator |
| Rejected Apps | <ul style="list-style-type: none">• Apps that crash• Do not perform tasks described | <ul style="list-style-type: none">• Known malware, spyware and Trojans• [bad] behavior |
| Coverage | ??? | New and existing apps |
| Other | ??? | <ul style="list-style-type: none">• Tests originate from known IP address block• 40% drop in malicious apps per Google |
| Known bypass techniques | ??? | <ul style="list-style-type: none">• Source IP/domain (android-test-2.mtc/corp.google.com)• System properties• Canary data (15555215504) |

Phishing and Mobile

| Phishing | Mobile |
|--|---|
| Attacks are short lived and taken down or blocked frequently | Always online and therefore always a viable attack target |
| Social engineering often requires spoofing portions of a legitimate web page | Limited screen real estate prevents many visual security indicators |
| Links are often sent via social networking applications | Browsers embedded within apps often do not show the URL at all |
| Attacks are constantly adapting and blacklisting alone is ineffective | Mobile browsers have fewer embedded security controls iOS ecosystem prevents any 3 rd party security controls running in the background |



How iOS is Forcing Enterprises to Rethink Security



| | Yesterday | Tomorrow |
|--------------|------------------------------------|---|
| Malware | Host based AV | Background apps/services prohibited |
| Network | Controlled while on-premises | 3G connectivity bypasses network controls |
| Traffic | Most HTTP(S) traffic browser based | Most HTTP(S) traffic app driven |
| Data leakage | Appliance based DLP | Device regularly off-premises |
| Ownership | Corporate owned asset | Personal asset |

Mobile Data Loss

What exactly does your smartphone know about you and who does it share it with?



Do you know what your app is doing behind your back?

Security

Productivity

Privacy

Passwords
Pers. Ident. Info.
Device ID (IMEI)
No SSL
Contacts
...

XSS
Command injection
Insecure permissions
Data theft
Race condition
...

Games
Social Networking
...



ZAP – Zscaler Application Analyzer

<http://zap.zscaler.com>



ZAP - Zscaler Application Profiler

How safe is your mobile application?

Search

Scan

About

Search a Mobile App

App Name:

Search App

Links

Zscaler ThreatLabZ

Gartner Magic Quadrant

State of the Web Report

Zscaler Analyst Scrapbook

Zscaler IPAbuseCheck

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

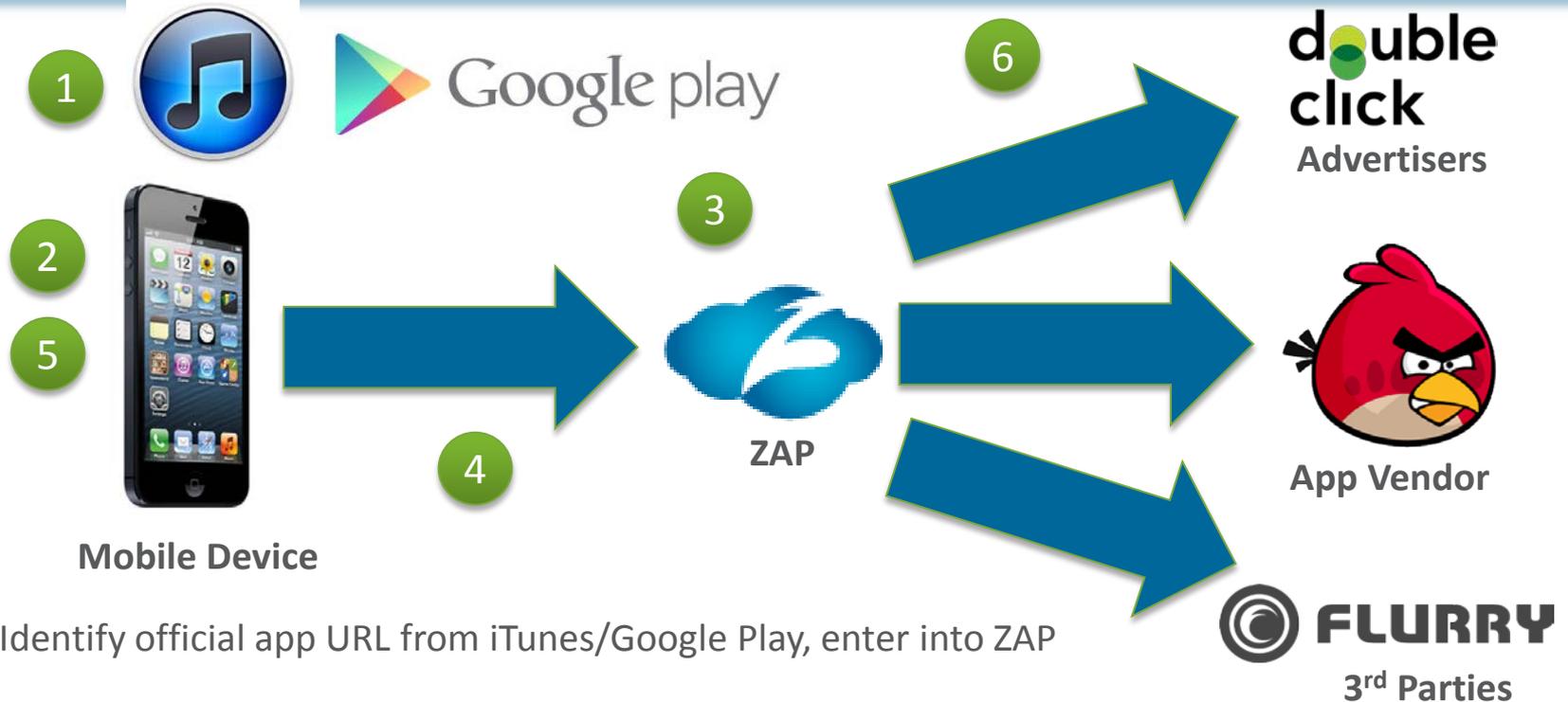
- Search

- » Query database to view summarized historical results

- Reporting

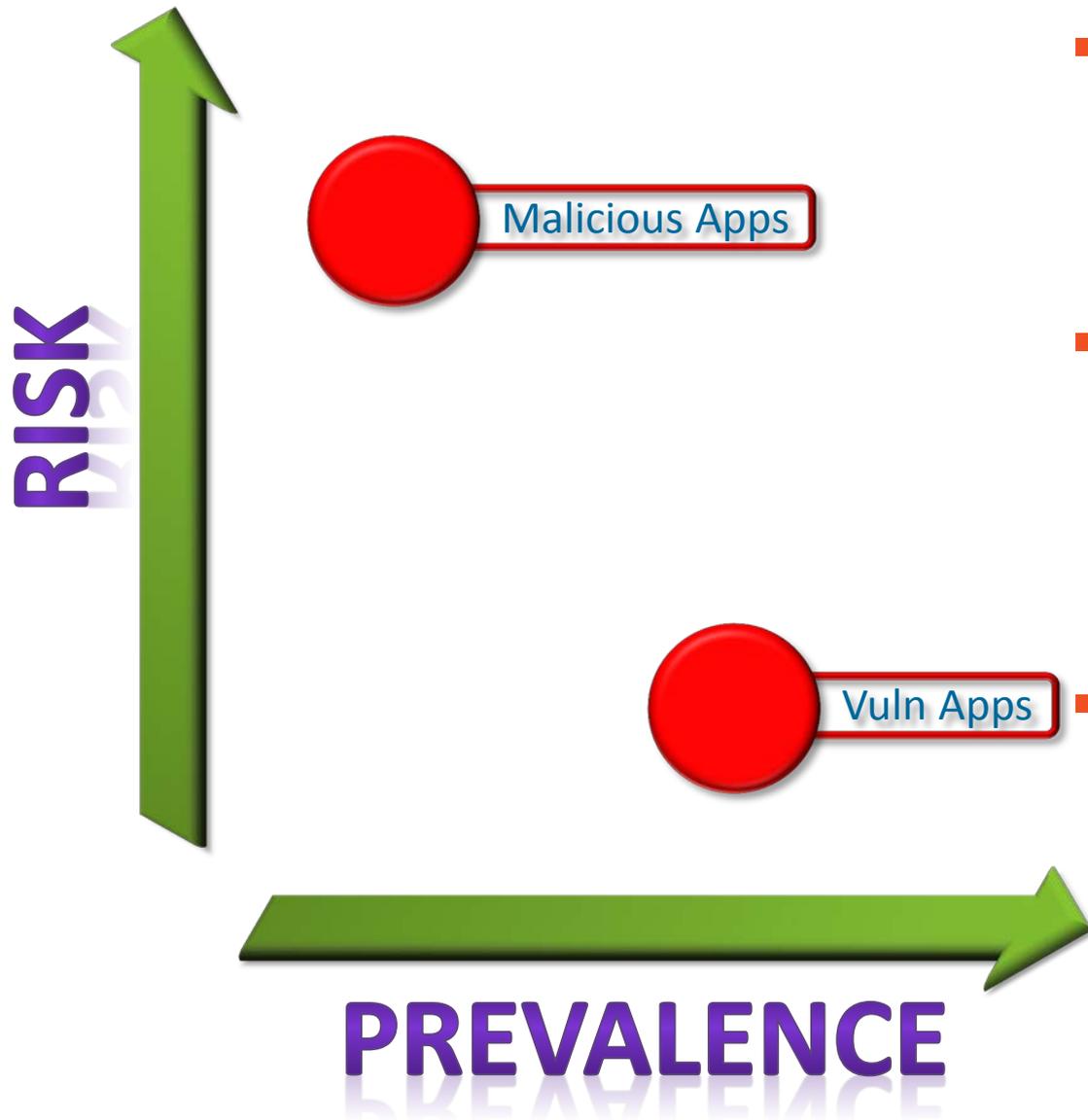
- Simple assessment of security/privacy risks
- Overall risk score

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

Mobile App Security



- Malicious apps grab the headlines but are a fraction of overall apps
- Given the hyper-growth of mobile app development, vulnerable apps are far more common
- App store gatekeepers are not weeding vuln apps out

Mobile App Privacy



- Given advertising driven model of app ecosystem, 3rd party comm., device ID tracking and collecting PII is very common
- Poorly coded apps often leak auth. credentials
- App store gatekeepers doing little to limit privacy issues

Weak Authentication – Password Hash

App Name: Twitxr

Version: 0.13 (September 5, 2012)

Category: Social Networking

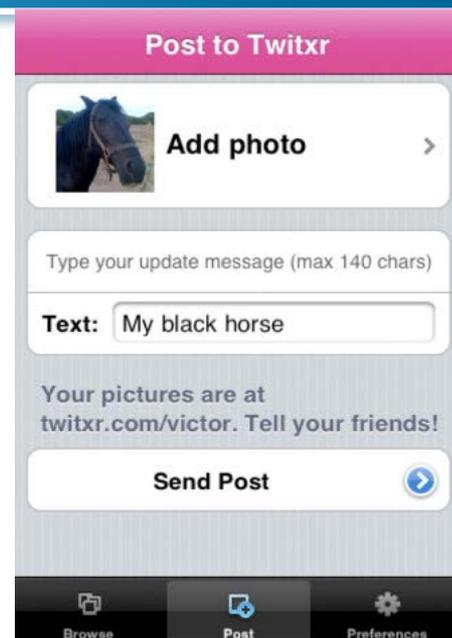
Ratings: 484

Platform: iOS



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

```
[-  
] http://www.twitxr.com/api/rest/registerNewUser?username=unzscaler&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=42ef56a0090b7b29ab5ee54fc57dc156  
[+] http://m.twitxr.com/unzscaler/with_friends  
[+] http://m.twitxr.com/unzscaler/with_friends/  
[+] http://m.twitxr.com/style_mobile_v1.0.css
```



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/DeviceConfigu  
rationService
```

```
...
```

```
[ -  
] https://svcs.ebay.com/services/mobile/v1/IpHoneApplica  
tionProcessService
```

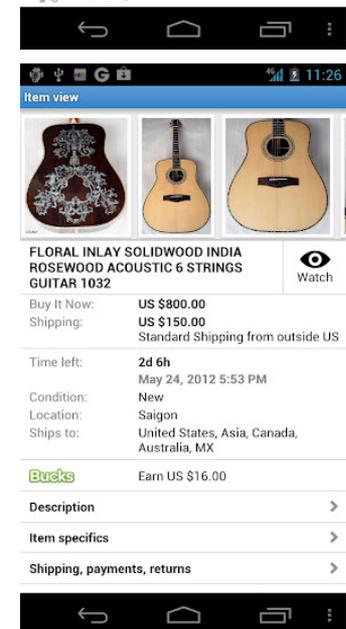
```
Method: POST
```

```
Host: svcs.ebay.com
```

```
User-Agent: eBayAndroid/1.8.3.5
```

```
Request Body: swap102010
```

```
Server Response: B%Rlf , , UUypd , >%WLu , MEi) ,  
~[vg , , ]/c4 , ] , 3tX@
```



Device Info Leakage – UDID

App Name: Hangman ®®®

Version: 2.2.6 (July 20, 2012)

Category: Games

Ratings: 22,356

Platform: iOS



[+] <http://ads.mopub.com/m/open?v=8&udid=sha:C6D279823C0BB1FBBD41&id=366248637>

[+] https://ws.tapjoyads.com/connect?mobile_network_code=&e_type=iPod%20touch&app_id=02aa9e96-7734-47b9-a199-187e294ca557&os_version=5.1.1&library_version=8.1.6&language=en&p=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



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.json?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", "member_since":"2012-03-04T15:04:59Z", "pic_url":"http://graph.facebook.com/100000195781259/picture"}, "tms_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", "member_since":"2012-02-17T04:12:09Z", "pic_url":"http://graph.facebook.com/100000195781259/picture"}, "tms_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", ...
```

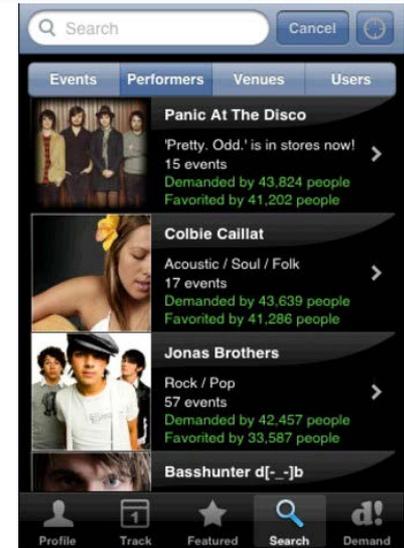
3 [-] **http://graph.facebook.com/762035580/**

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/start?stsess=(null)
[-]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","secret":"","token":""}&payload={"name":"Fnzscaler","password":"Zscal3r!","verify":"1cac4c9b84b77738cb1ede06054ed664","email":"apps@zscaler.com","partner_id":"2"}&version=1.0.0
```

```
Server Response: ;iv# , r , '+4f , %eG}
```

```
[+]http://flow.backupgrid.net/auth/request
```

```
[+]http://flow.backupgrid.net/account/devices
```

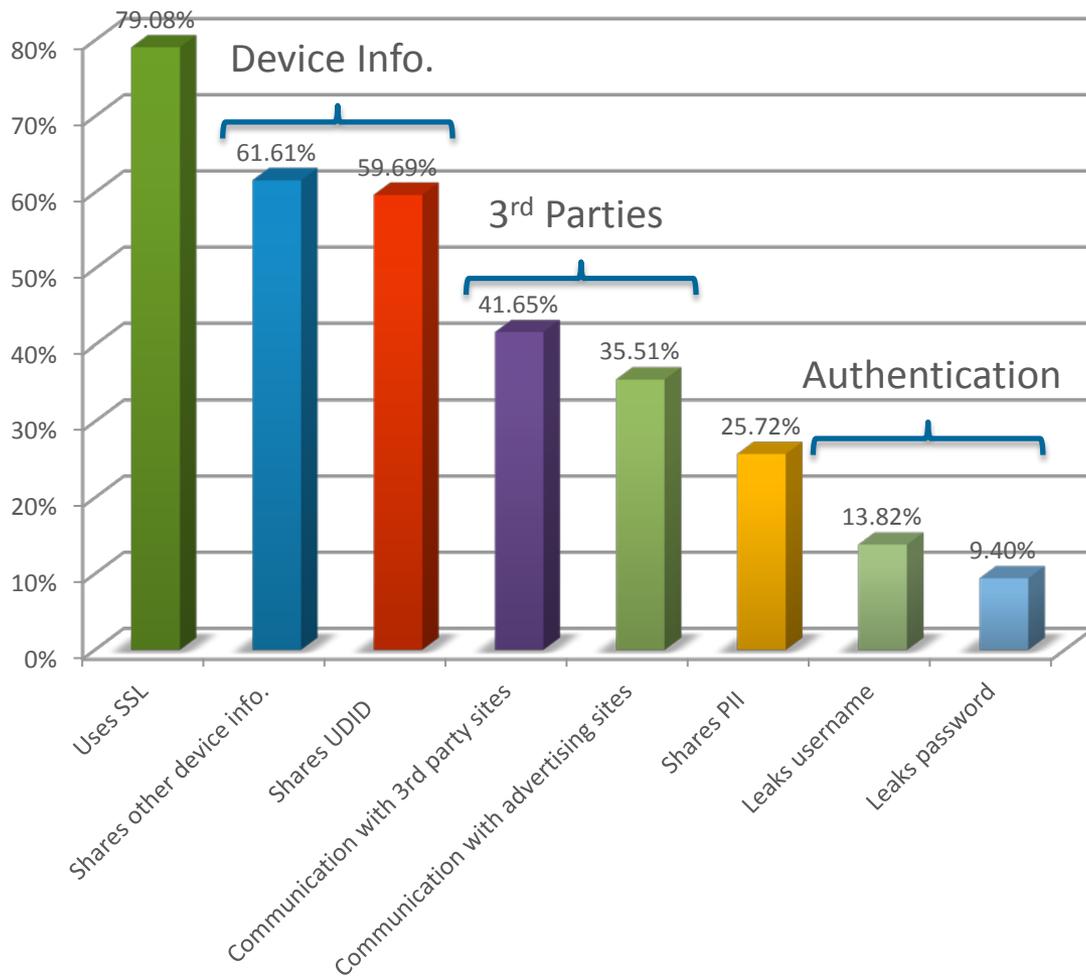
```
[+]http://flow.backupgrid.net/device/licence
```

```
[+]http://flow.backupgrid.net/device/roots
```

Mobile 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

Percentage of iOS apps displaying various communication behaviors



Securing Mobile

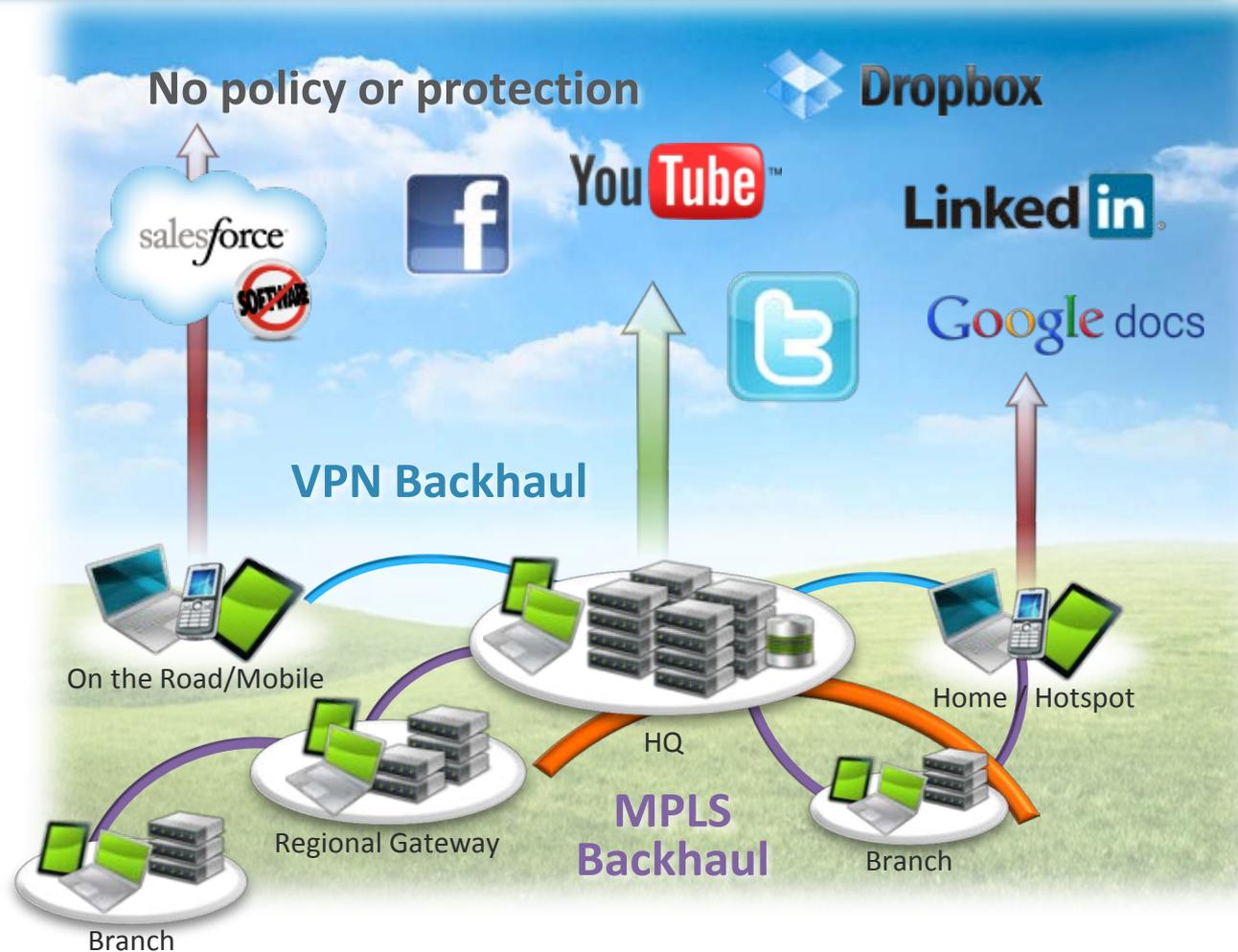
How enterprises must adapt in a mobile world



How Mobility turns Enterprise Security Upside Down

Yesterday

- Devices, applications & Data at Corp HQ or DC
 - Owned and controlled by the enterprise
- Traffic backhaul
 - Branch offices - MPLS
 - Road warriors – VPN
- Protect users with appliances
 - On-prem gateway proxies (URL, AV, DLP) enforce policies for users accessing Internet



Today

- Mobility
 - Users go direct
 - Data, networks and devices no longer owned/controlled by the enterprise

Ltd. protection and visibility for the mobile workforce

Zscaler Secure Cloud Gateway



“Zscaler was the only one that truly delivered an ultra-low latency experience along with exceptional protection from threats. And best of all, it works exactly as advertised.”

Consider Three Users...



| | Office | Coffee Shop | Airport |
|------------|------------------------------|----------------------------|-------------------|
| Device | PC | Laptop | Tablet/smartphone |
| Protection | IDS, IPS, FW, SWG, DLP, etc. | Host based AV and firewall | Nothing |
| Visibility | Location based reporting | | Nothing |

- *We must seek security solutions that ensure consistent policy, protection and visibility, regardless of device or location.*
- Cloud provides the opportunity to level the playing field.



zscaler.com
threatlabz.com

Michael Sutton
VP, Security Research