RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Predatory Hacking of Mobile Devices

SESSION ID: MBS-W03

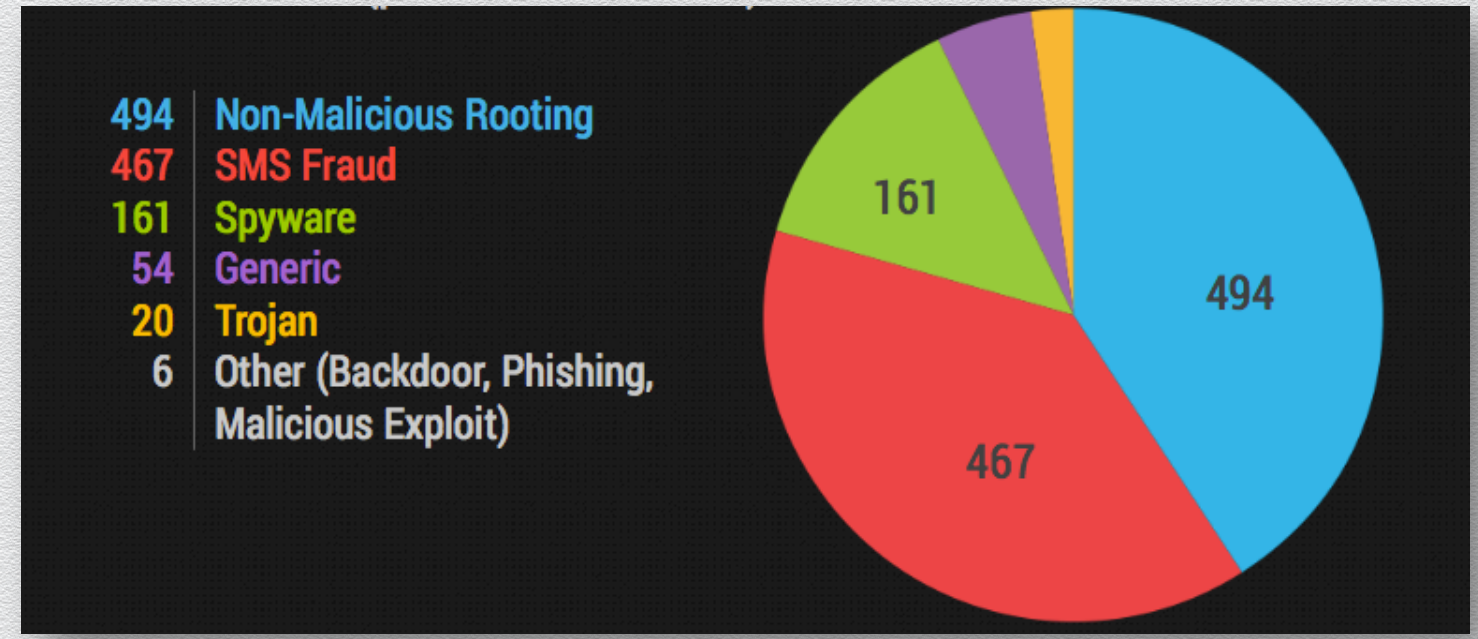
Jeff Forristal

CTO
Bluebox Security
www.bluebox.com

If you haven't heard…

the world has gone mobile.

2013 Q4 shipments:
227.8m smartphones (IDC) vs. 82.6m PCs (Gartner)



Attackers follow opportunity

Credit: Google

This Flashlight Android App Has Been Secretly And Illegally Sharing Your Personal Data With Advertisers

+ Comment Now + Follow Comments

A popular Android flashlight app has been surreptitiously collecting personal data and sharing it with advertisers. The Federal Trade Commission found that Brightest Flashlight, which has been downloaded over fifty million times and which enjoys nearly a million 5-

Data has been leaking for a while

Credit: Forbes

Mobile Device Data & Assets

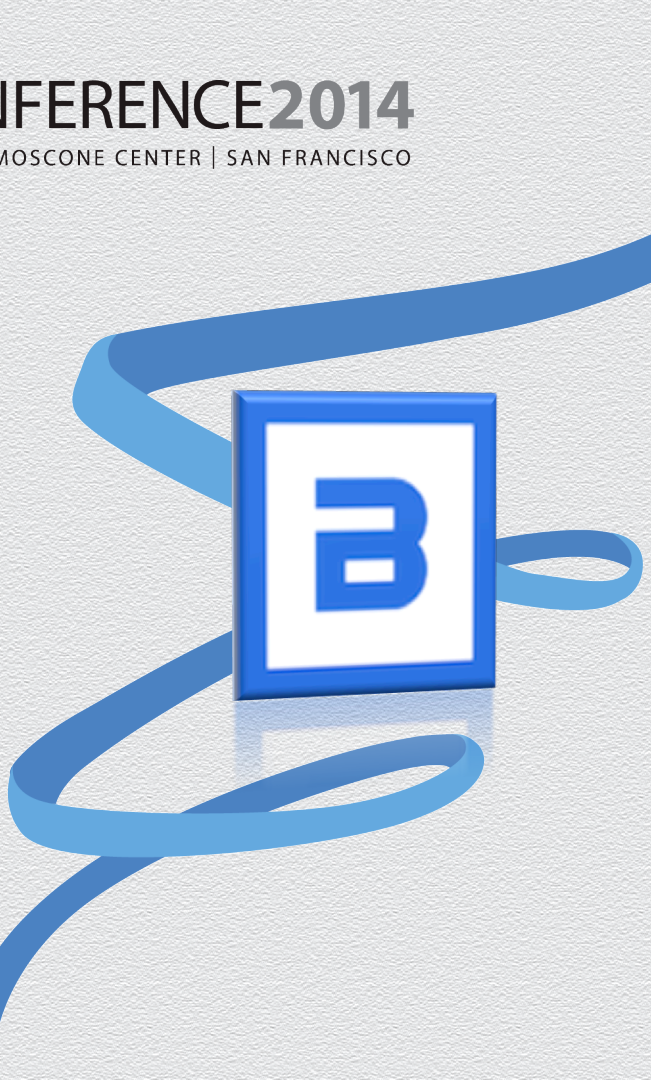
- Account logins & passwords
  - Email
  - VPN
  - Social networks
  - Banking & shopping
- Services / resources
  - Internet & VPN
  - Cellular
  - ***SMS (premium charges)***
- Documents
  - Email & attachments
  - File storage services
- Monitoring
  - Microphone
  - Camera
  - GPS/location
- Soft auth tokens/2FA
- Pivot to PC

Attack Surface

- Communications Networks
  - Cellular
  - Bluetooth
  - Wifi
  - NFC
- Malicious Apps
- Physical Access
  - USB
  - SIM
  - Dock/Accessory Connector
  - Lockscreen
- Other
  - QR Code

Type complex passwords on this?

No thanks.



Data Theft via Malicious Apps

It happens – ask Charlie Miller

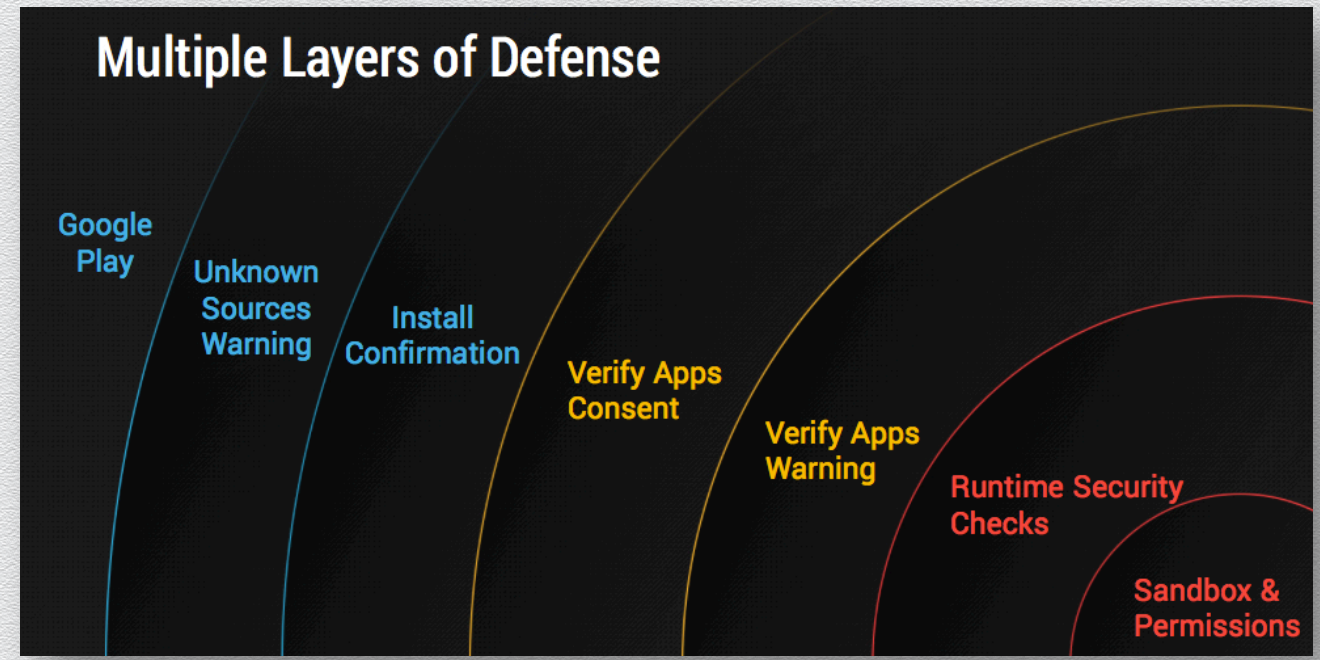
Credit: news.nbc.com

Fake BBM apps, circa Sept 2013

Credit: AndroidCentral.com

Malicious App Sources

- Hosted on Apple/Google stores, missed by reviews
- Jailbreak markets
- Third-party app stores
- Enterprise app stores & app distribution services



Android sandbox & security layers

Credit: Google

Example: Android Masterkey

- Found by Bluebox in 2013
- Code modification without affecting the app cryptographic signature
- Abusing system UID apps to gain system privileges
- System UID access is outside normal app sandbox
- Sub-root data compromise
  - *Will not be detected by normal jailbreak/root detection mechanisms*

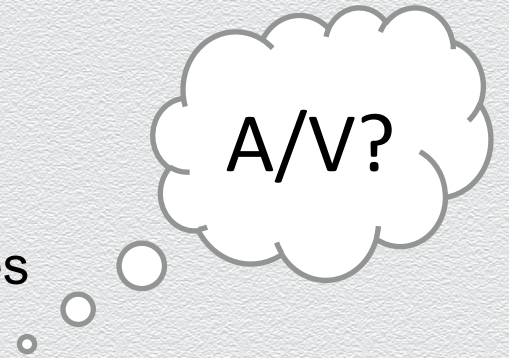
Malicious IOS App Demo

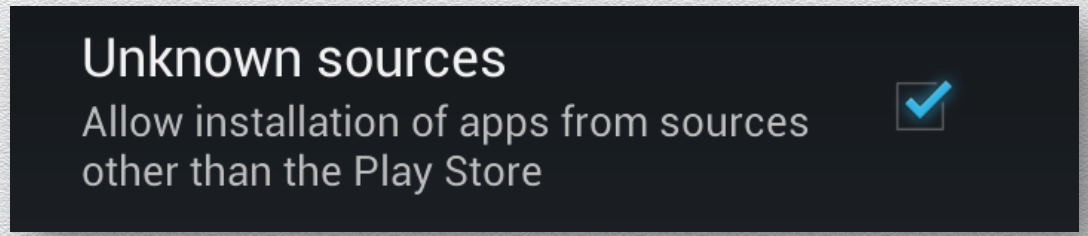
Malicious app steals configuration settings & passwords

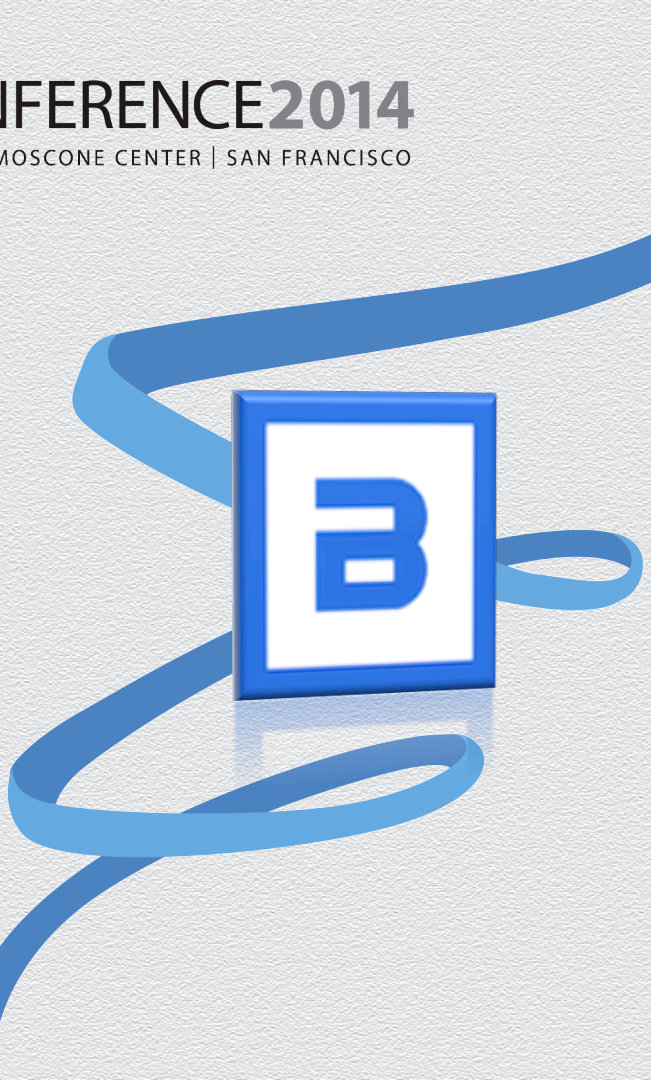
Graphic credit: Iconfactory.com

Mitigations

- Prefer vendors that patch!
- Android: disable installation from unknown sources
- Stick to trusted app sources/markets
- MAM, EMM, VDI can protect on-device data







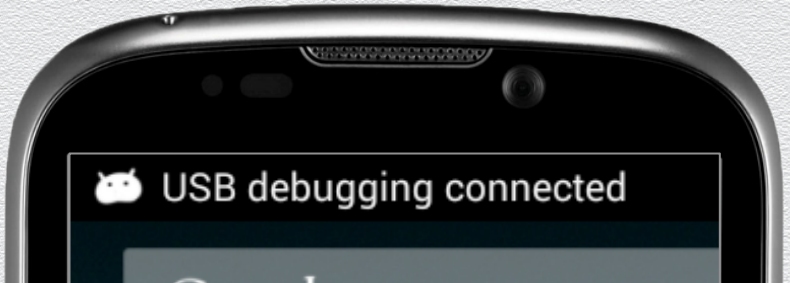
Data Theft via Physical Access

Malicious USB Chargers (“Juice Jacking”)

- Free power charging station is really an exploit host
- Presentation at Blackhat 2013 by Lau et al
  - Targets iPhone
  - Gets UDID over USB
  - Talks to Apple website, gets dev provisioning profile for that UDID
  - Have a malware app signed by dev cert included in provisioning profile
  - Push mobile config to phone to install the malware app
  - Runs code on device, go from there…

USB Debug Access

- Commercial phones with ADB debugging access on by default
  - Blu Dash 4.5 (Android 4.2.1)
  - HTC One (original Android 4.1.2)
- ADB debugging access gives you shell access
- Debugging trust prompt added in Android 4.2.2 (early 2013)



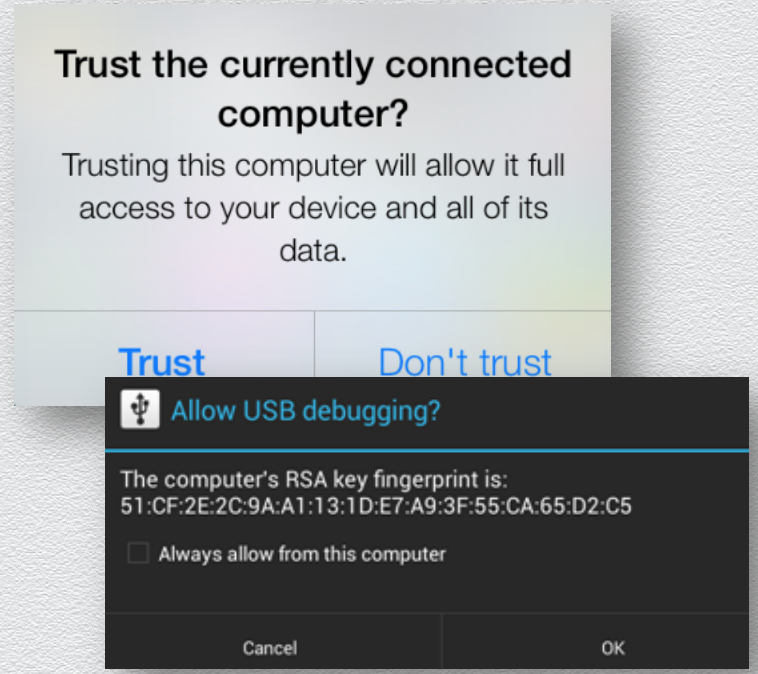
IOS PIN brute force demo

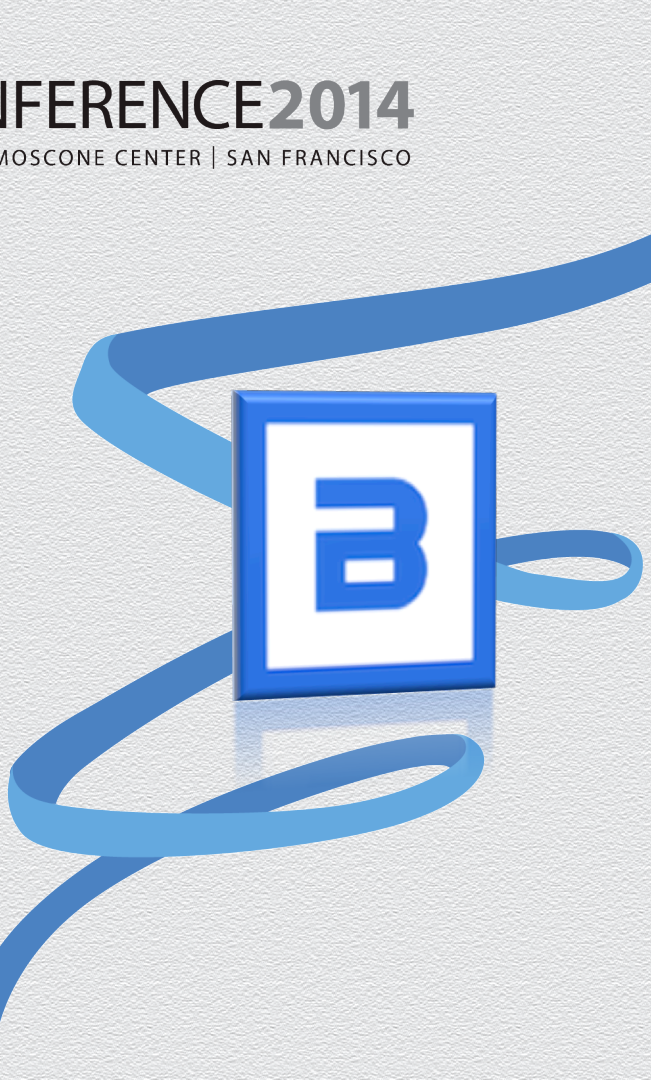
Physical PIN brute force of locked iPhone via USB

Graphic credit: Alexander "PAPO1990" Papadopoulos

Mitigations

- Android: turn off ADB debugging
- Newest IOS, Android prompt you to trust the USB connection
- MAM, EMM, VDI, containers add extra layer of data security





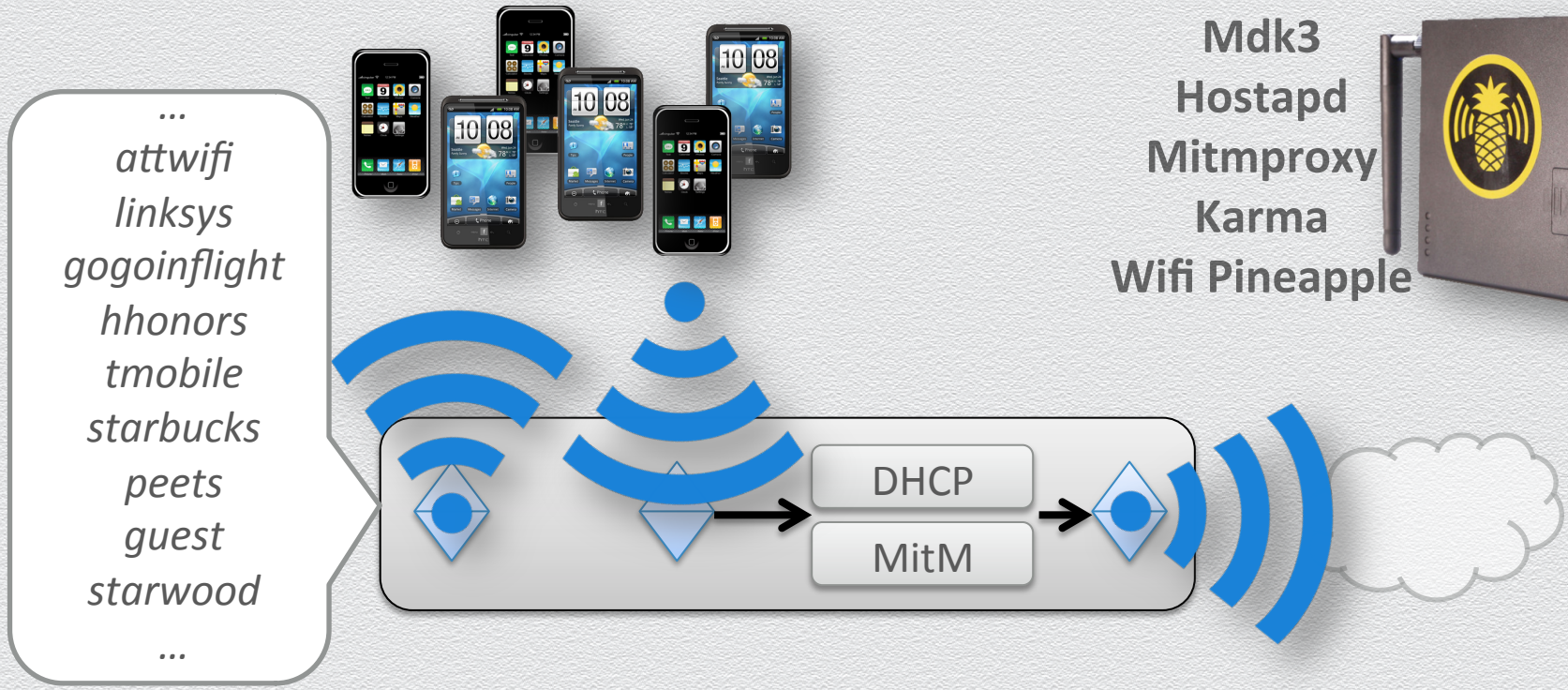
Data Theft via Wifi Networks

SSID spoofing (“WiPhishing”)

- Phones auto-connecting to ‘attwifi’ et al
- Known SSIDs from airports, cafes, etc.
  - Tend to be open auth w/ captive portal, easy to spoof
  - If you used it once, device will remember it for use again later
  - Tools can spoof hundreds of APs, impersonate the ones clients respond to

Non-Secure HTTP Traffic

- Mobile devices & apps sends lots of plaintext traffic
  - This is all observable, subject to MITM
- Interesting data seen in the clear
  - Android device ID
  - IMEI
  - GPS lat/long
- MITM attack vectors
  - Android webview javascript callback
  - IOS SSL verification error



Spoofed APs

Pretending to be everywhere

Photo credit: hak5.org hakshop

Stats

2200 phones

- 53% IOS, 31% Android, 2% Blackberry, 13% other

Top SSIDs

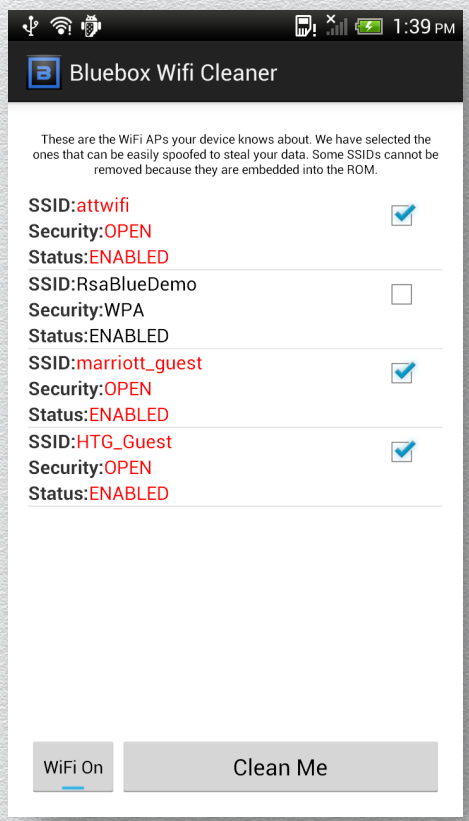
- attwifi (36%)
- Wayport_Access (6%)
- SFO-WiFi (5%)
- United_Wi-Fi (5%)
- linksys (5%)
- gogoinflight (4%)

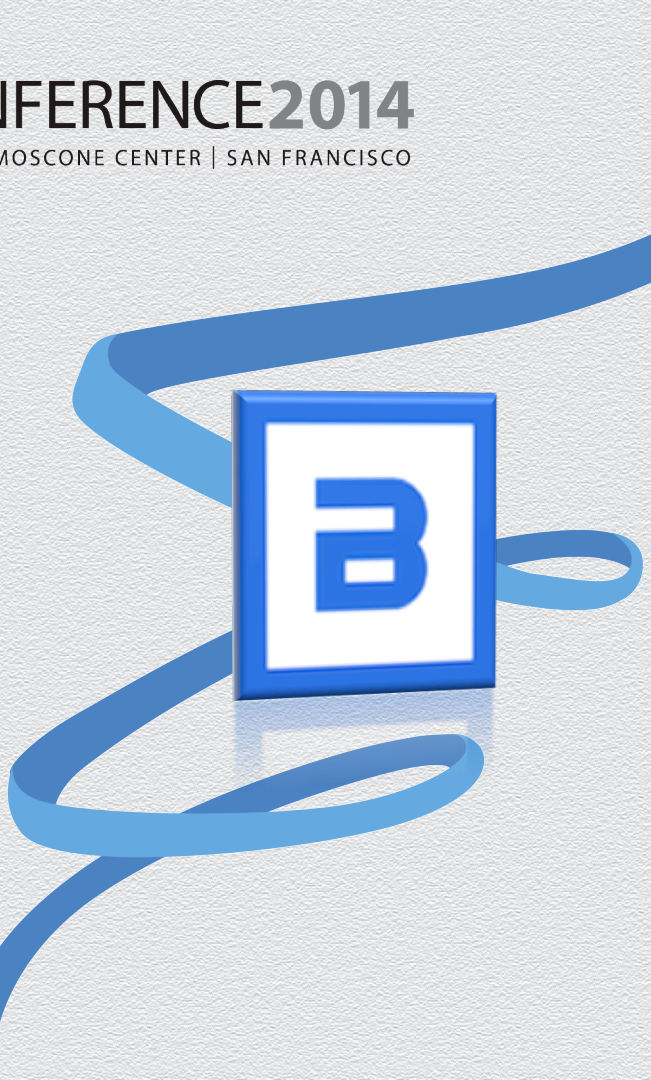
Wifi Demo

Mobile devices connect to spoofed APs, exploited by Android bug

Mitigations

- Purge old prior networks from mobile device wifi list
  - Security apps can automate this
  - Android: Bluebox Wifi Cleaner
- Turn off radios (Bluetooth, Wifi) when not using them
  - Bonus: saves battery!
  - Android: Kismet Smarter Wi-Fi Manager
- Use device VPN & app VPNs to protect traffic on untrusted networks
  - Some capabilities exclusive to MAM, EMM, and containers





Going Forward

Fact:
Mobile vulnerabilities will continue

Challenge:
Keeping data safe; quick detection & recovery

Accepting Reality

- PDAs are finally ubiquitous
- Always on, always connected, *always at risk*
- The form factor makes traditional security controls cumbersome
- Users have minimal incentive to avoid all forms of mobile risk

NIST SP 800-124

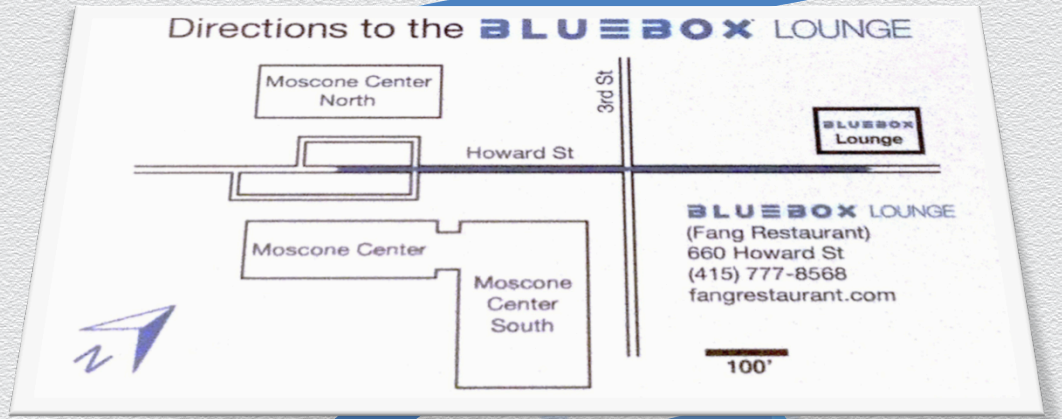
Guidelines for Managing the Security of Mobile Devices in the Enterprise

It’s about the DATA?

Bluebox Security

Securing your mobile data wherever it goes

- **Cloud service** provider of mobile data security
- **Secure what matters most – corporate data** – across devices, apps, and networks
- Unprecedented visibility to inform and tune policies; **take action based on data** usage and movement
- Increase compliance and productivity by providing **security that employees embrace**
- Single pane of glass to manage mobile data security across **fully managed, BYOD, and hybrid environments**



Thank You!

Jeff Forristal

jeff@bluebox.com

bluebox.com/blog/