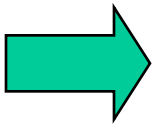
An Intense Look at the Mobile Computing Threat

By Joshua Wright
Senior Instructor, SANS Institute
jwright@willhackforsushi.com

Outline



Mobile Device Proliferation

- Disparity of Mobile Devices
- Mobile Device Encryption
- Malware Threats
- Practical Attacks Against Wireless
- Don't Fight It, Change It

Recognizing the Problem

Many organizations are underprepared to handle the influx of personal mobile devices that lack robust enterprise management functionality while needing to support such a deployment for legitimate business motivators.

This is not your fault. We are underprepared as an industry. Change is required to support secure mobile device deployments.

Mobile Devices and Business

- Mobile devices are a productivity tool
  - Business applications, after-hours use
- Workforce expectations are growing
  - Growth of executive-down mandate
  - Continued employee-up demands, required to employ younger workforce
- Resistance leads to unauthorized devices or WLANs on your network
  - Completely unmanaged

Our Focus Today

1. Examine the disparity of features, controls
2. Dispel commonly held belief regarding device encryption
3. Malware proliferation
4. Examine practical attack techniques against mobile devices
5. Opportunities going forward

Outline

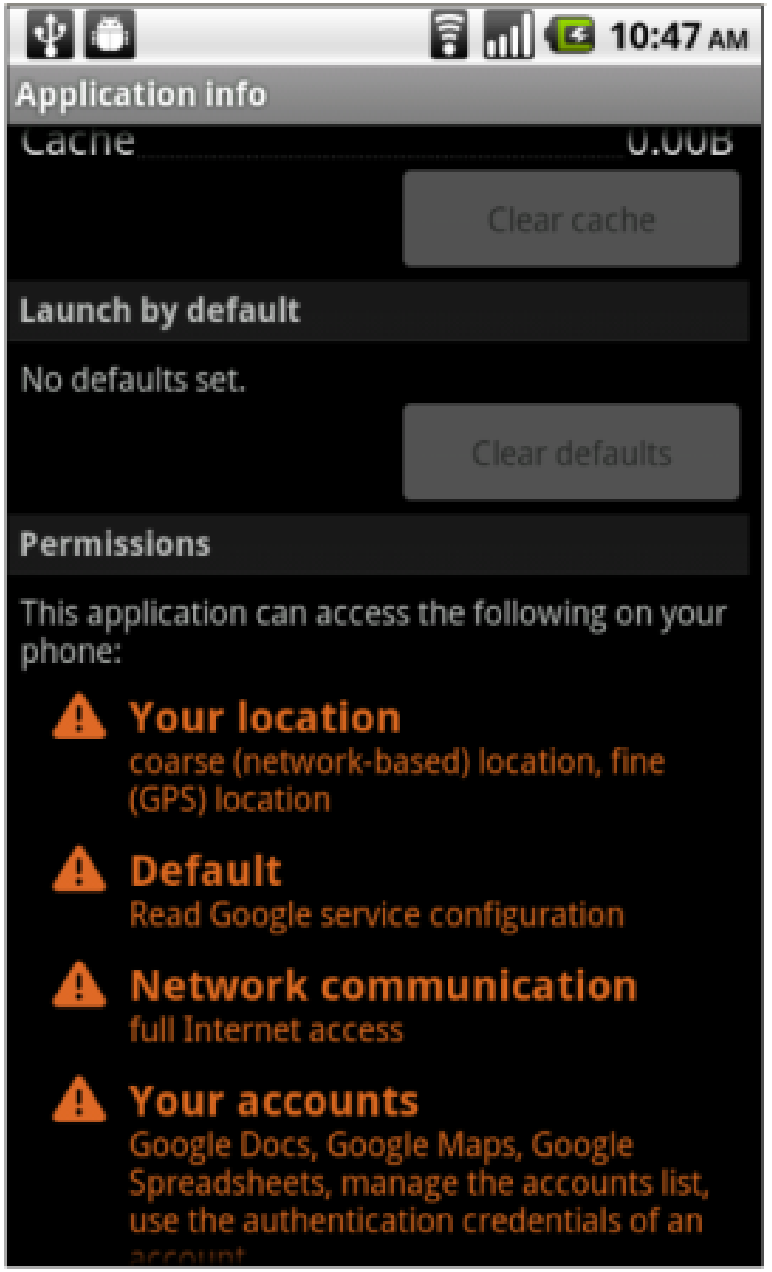
- Mobile Device Proliferation
- Disparity of Mobile Devices
- Mobile Device Encryption
- Malware Threats
- Practical Attacks Against Wireless
- Don't Fight It, Change It

Operating System Sources

- All source code for Android is open and available for public scrutiny
  - Google supports this model for platform transparency and open security scrutiny
  - 20 security vulnerabilities of various criticality since introduction (Sept. 2008)
- Apple does not openly publish platform sources
  - 52 security vulnerabilities of various criticality since introduction (June 2007)

Apple and Android ACL

- Apple vets applications prior to publishing in App Store
  - Little decision in the hands of the end-user
  - Running applications get free access to contact list, calendar, photos, device info. and associated GPS data
- Google permits anything deemed non-malicious
  - End-users permit applications based on required permissions



Vulnerability Resolution

- Apple publishes updates with regular frequency to all customers
  - Free of change, applicable to all platform devices
- Google regularly publishes updates as well
  - Must be vetted by HW platform vendors prior to distribution
  - Commonly, HW vendors do not make updates available (new sales opportunity)
- Android customers leverage vulnerable devices for dangerously long periods

Many Android users are left with no supported options for resolution of identified vulnerabilities.

Enterprise Controls

- Controls for traditional platforms excel at auditing, policy enforcement
  - Supported by native OS controls and third-party add-ons
- Controls for mobile platforms are extremely lacking in functionality
  - No enterprise-tools from Apple*, Google
  - Several third-party tools, SaaS or in-house (MDM's)

The best MDM's are still inadequate security controls due to platform restrictions or limitations.

Outline

- Mobile Device Proliferation
- Disparity of Mobile Devices
- Mobile Device Encryption
- Malware Threats
- Practical Attacks Against Wireless
- Don't Fight It, Change It

Full Device Encryption

- iOS Data Protection encrypts all data using AES-256
- From a lost device, attacker can recover both keys in an offline mode
  - Does not trigger "wipe after 10 failures" lockout
- Unlock-for-use keys are generally very weak since they are entered frequently
- Requires possession of the iOS device

Firefox

Apple loses another unreleased iPhone (...

news.cnet.com/8301-13579_3-20099899-37/apple-loses-another-unreleased-iphone-exclusive/

engadget

Apple loses another unreleased iPhone (exclusive)

By: Greg Sandoval and Declan McCullagh

AUGUST 31, 2011 12:45 PM PDT

Print E-mail

Recommend 10K Tweet 4,453 Share 304 comments

Cava22, the San Francisco bar where another unreleased iPhone apparently went missing. (Credit: James Martin/CNET)

In a bizarre repeat of a high-profile incident last year, an Apple employee once again appears to l unreleased iPhone in a bar, CNET has learned.

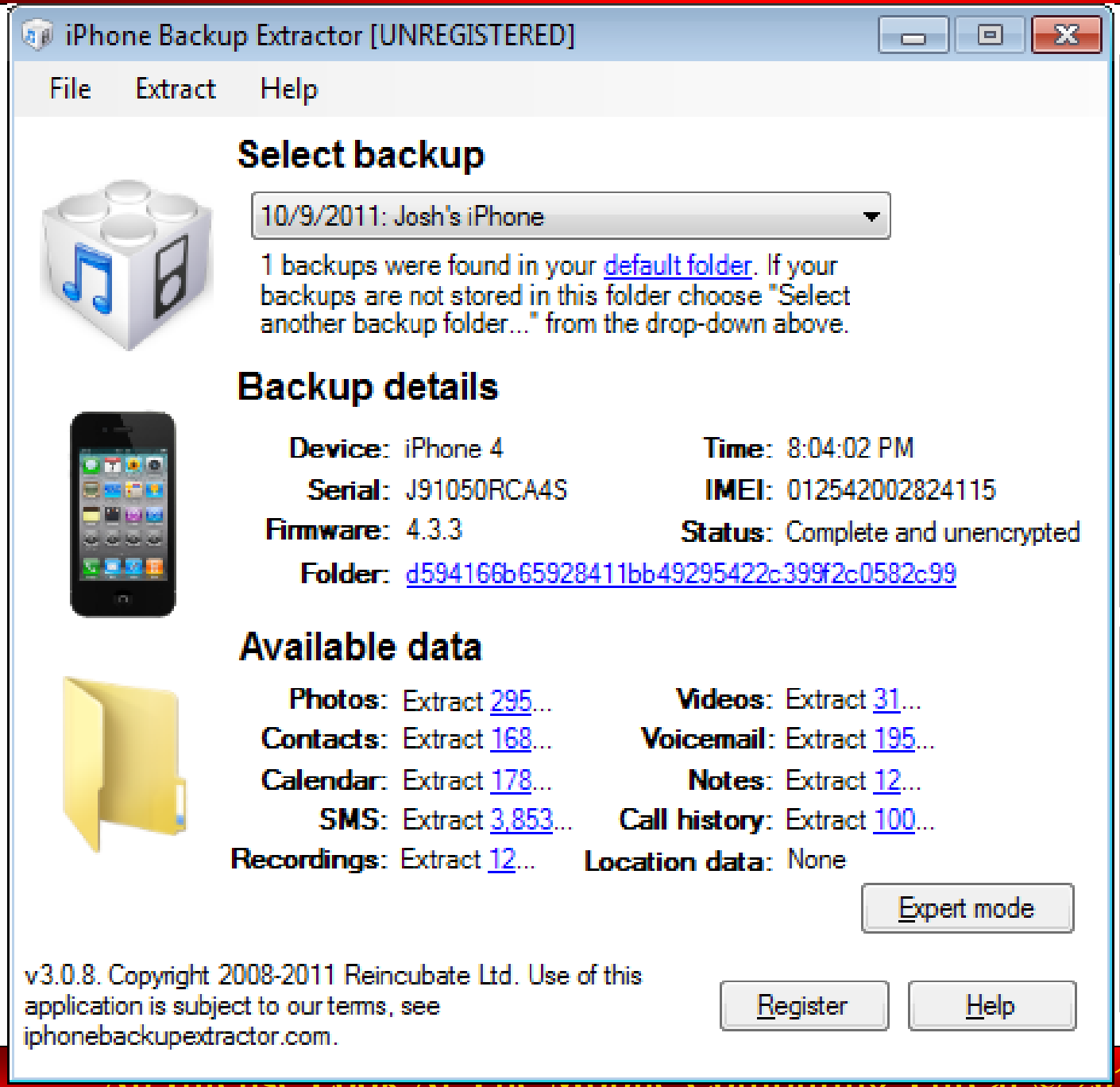
The errant iPhone, which went missing in San Francisco's Mission district in late July, sparked a scramble by Apple security to recover the device over the next few days, according to a source familiar with the investigation.

Apple's iPhone event plus Buzz Out Loud: Join us Tuesday (live blog)
OCTOBER 4, 2011 4:10 AM PDT

3/18/2010 - Gray Powell, Apple SW Engineer, lost his prototype iPhone 4 at Gourmet Haus Staudt (Redwood City).

8/30/2011 - An unnamed Apple employee loses a prototype iPhone 5 at Cava22 (San Francisco), police investigation ensues.

10/4/2011 - Josh considers hanging out at bars in Cupertino upon hearing that there is no iPhone 5 release this year.



Backups are very easy for iOS devices.

Can be encrypted through iTunes configuration settings.

No consistent control on where devices are backed up, or how iTunes is configured.

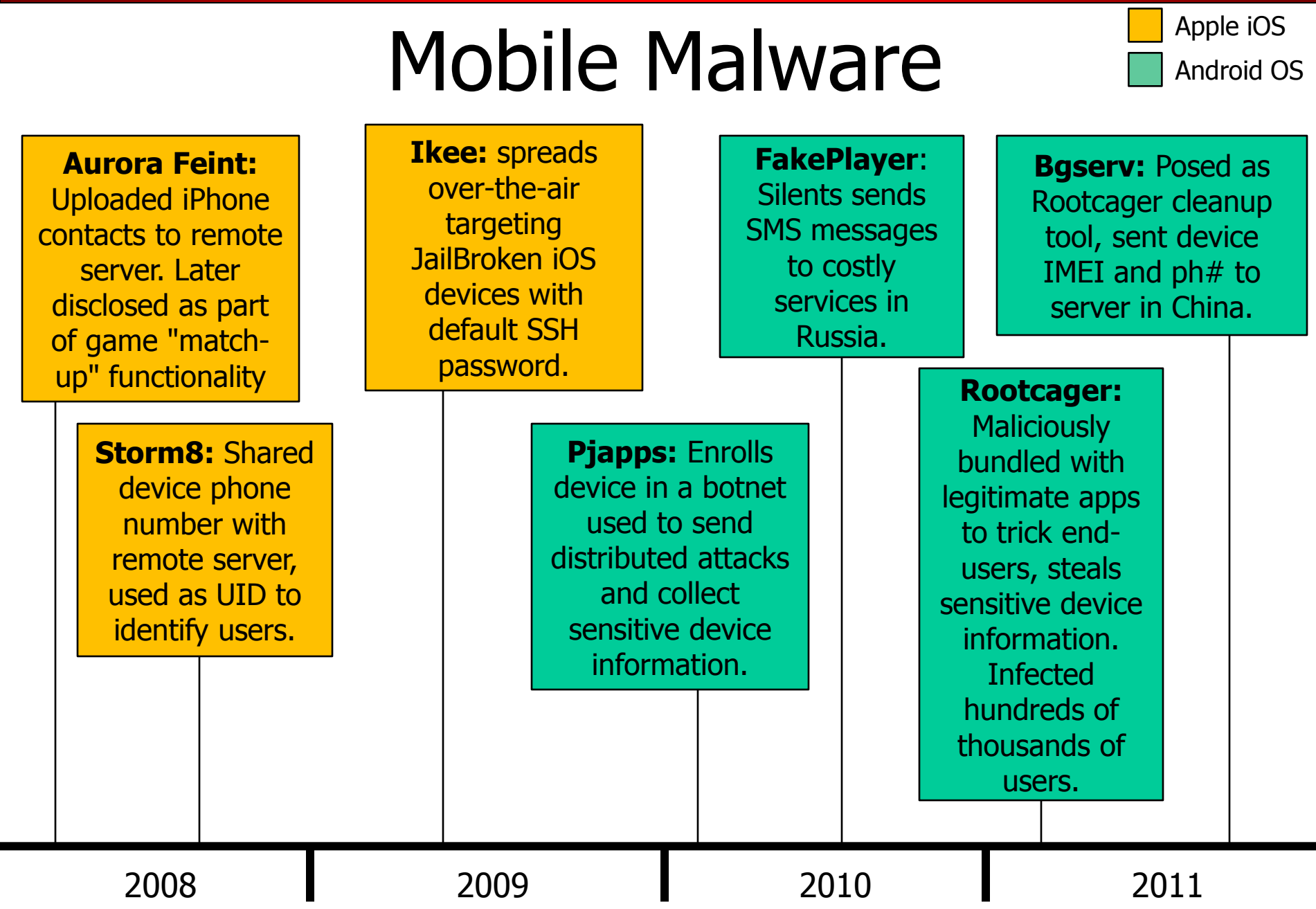
Real Benefit of Disk Encryption

- iOS Data Protection can be bypassed with target device access
- Running applications can access resources
- Disk encryption is very valuable for remote device wipe
  - Overwriting all drive sectors can take a while
  - Overwriting key storage location is very fast
- Requires a policy: Users notify administrators when a device is lost!

Outline

- Mobile Device Proliferation
- Disparity of Mobile Devices
- Mobile Device Encryption
- Malware Threats
- Practical Attacks Against Wireless
- Don't Fight It, Change It

Mobile Malware



Not Really Malware, But Close

- JailbreakMe.com
- Exploits vulnerability in Safari PDF handling
- Installs alternate App Store Cydia
- Not malware (opt-in), but could be similarly leveraged for malicious activity

Mobile Malware Evolution

- To date, most malware has been distributed via app store mechanisms
- A number of vulnerabilities, primarily in iOS have also been disclosed
  - Used by jailbreakme.com
- Reasonably could be used for more malicious activities
- Change influenced by motivators for attackers, financial gain opportunities

Outline

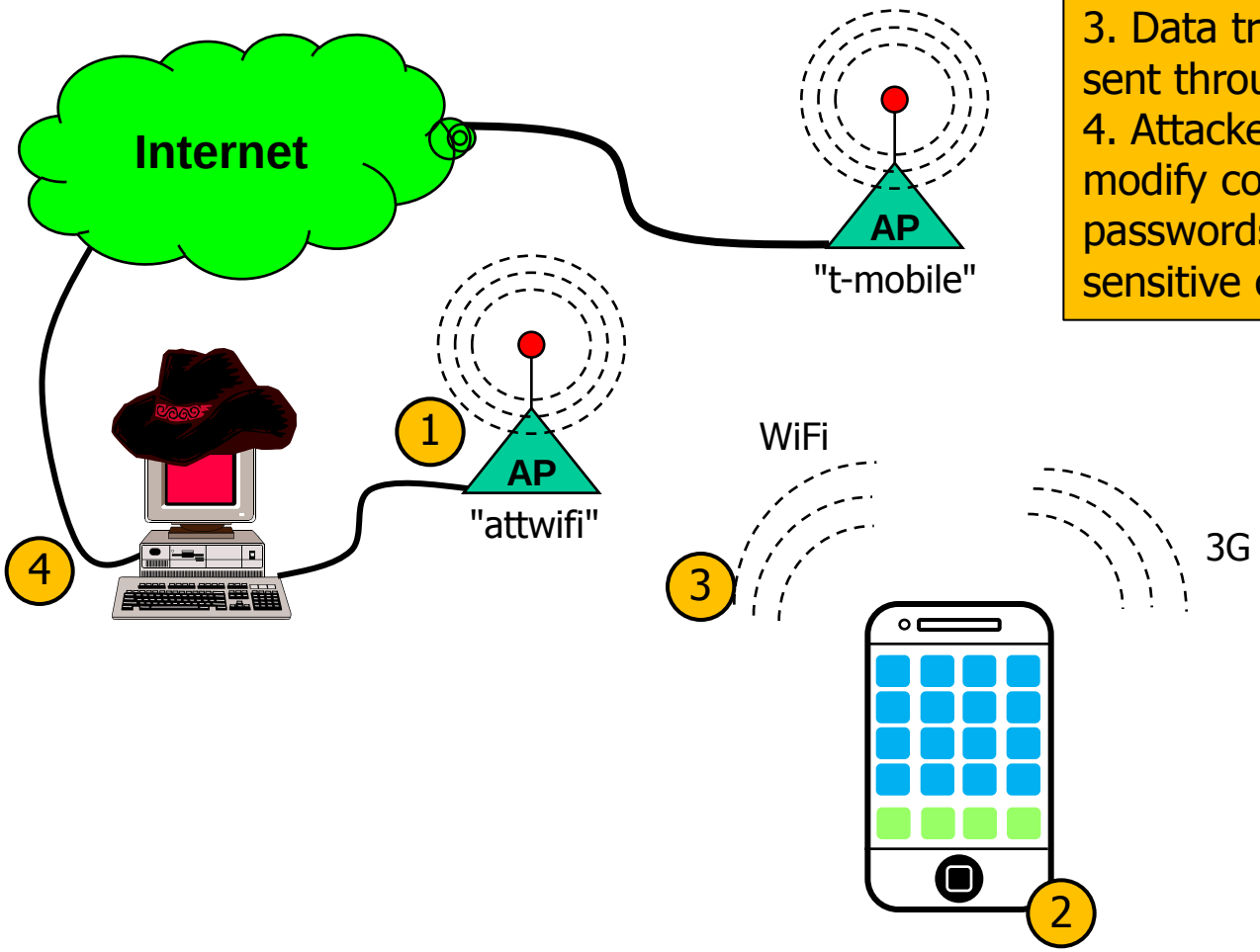
- Mobile Device Proliferation
- Disparity of Mobile Devices
- Mobile Device Encryption
- Malware Threats
- Practical Attacks Against Wireless
- Don't Fight It, Change It

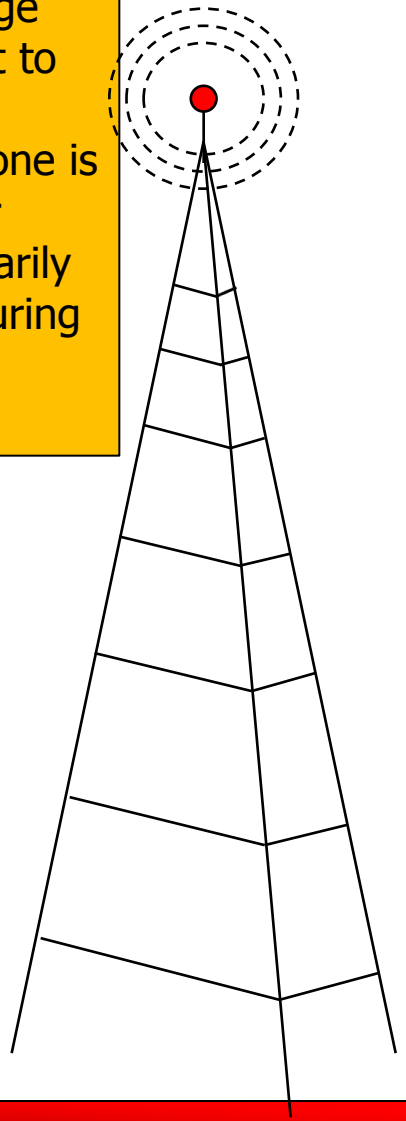
Smartphones and WiFi Hotspots

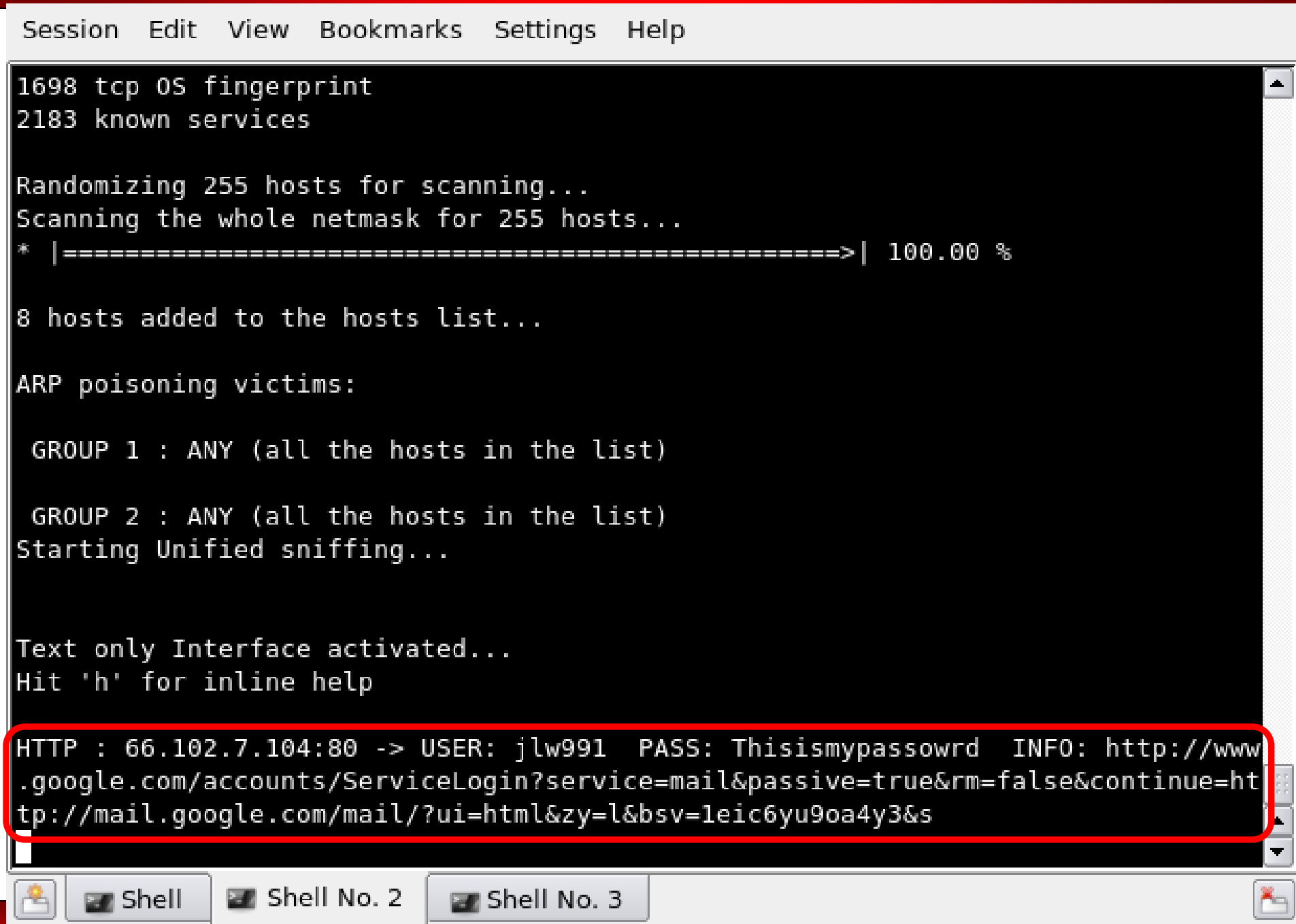
- Many smartphones will automatically connect to WiFi hotspots
  - Carriers are motivated to offload data traffic to a less-expensive medium
- Hotspot networks are unauthenticated
  - Can be impersonated by an attacker
- Once on the attacker's hotspot, multiple attacks are possible

Hotspot Impersonation

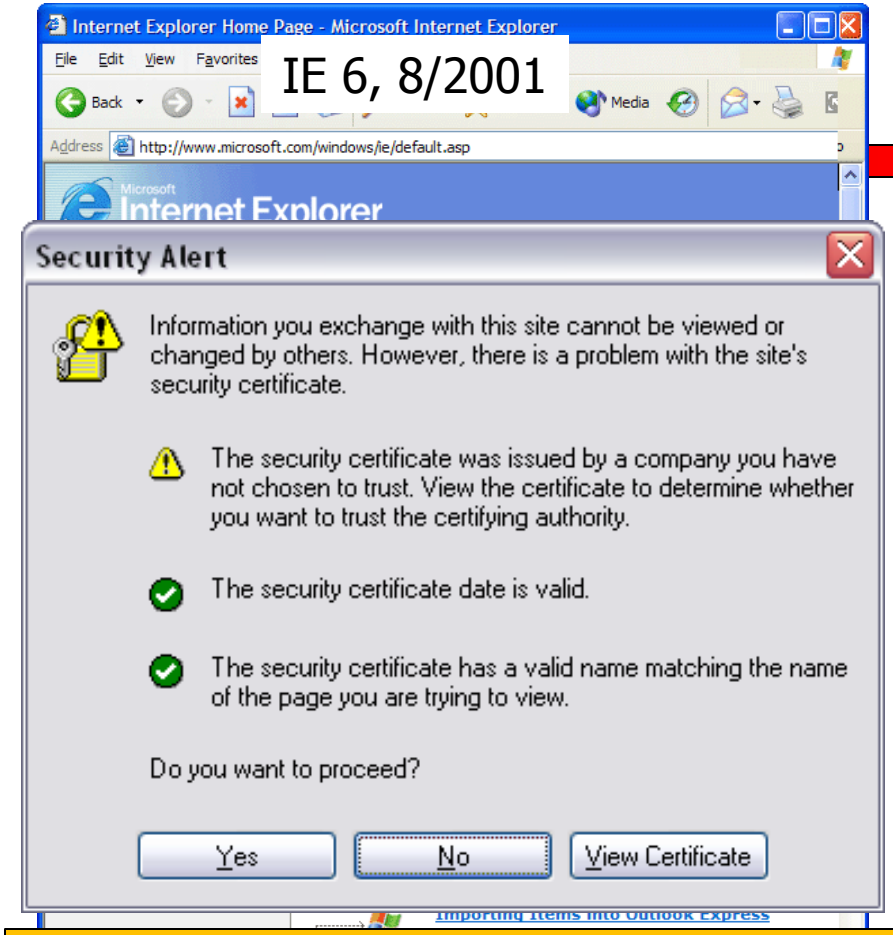
1. Attacker impersonates "attwifi" with mobile AP, connected to the Internet
2. iPhones within range automatically connect to attacker
3. Data traffic on iPhone is sent through attacker
4. Attacker can arbitrarily modify content, capturing passwords and other sensitive content.

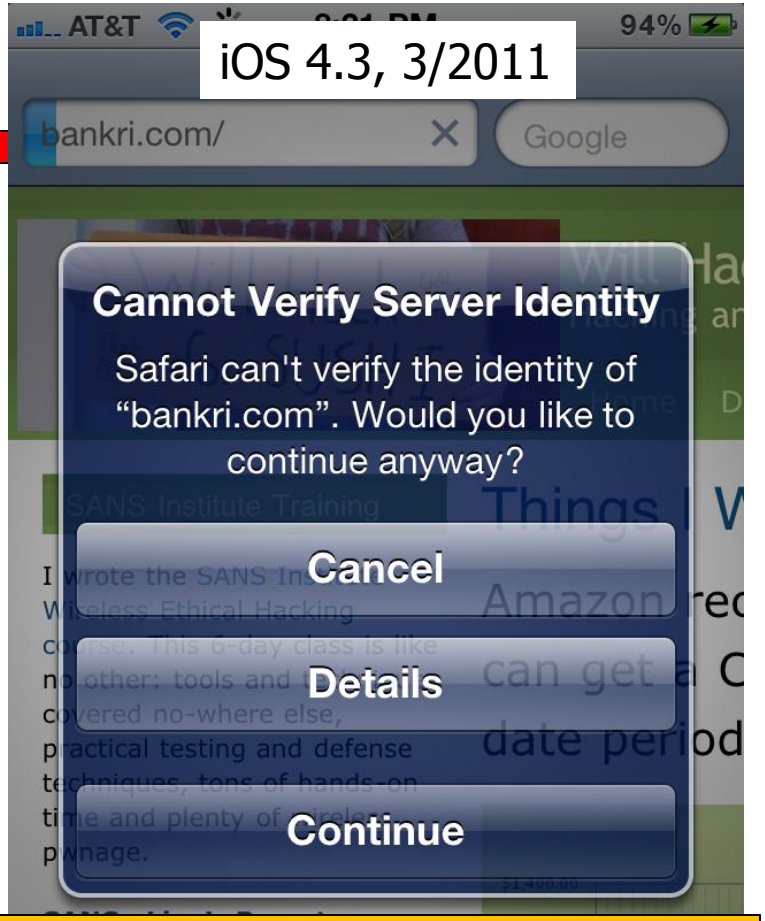





Session Edit View Bookmarks Settings Help
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==>| 100.00 %
8 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help
HTTP : 66.102.7.104:80 -> USER: jlw991 PASS: Thisismypassowrd INFO: http://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/?ui=html&zy=l&bsv=1eic6yu9oa4y3&s
Shell
Shell No. 2
Shell No. 3

SSL Certificate Validation



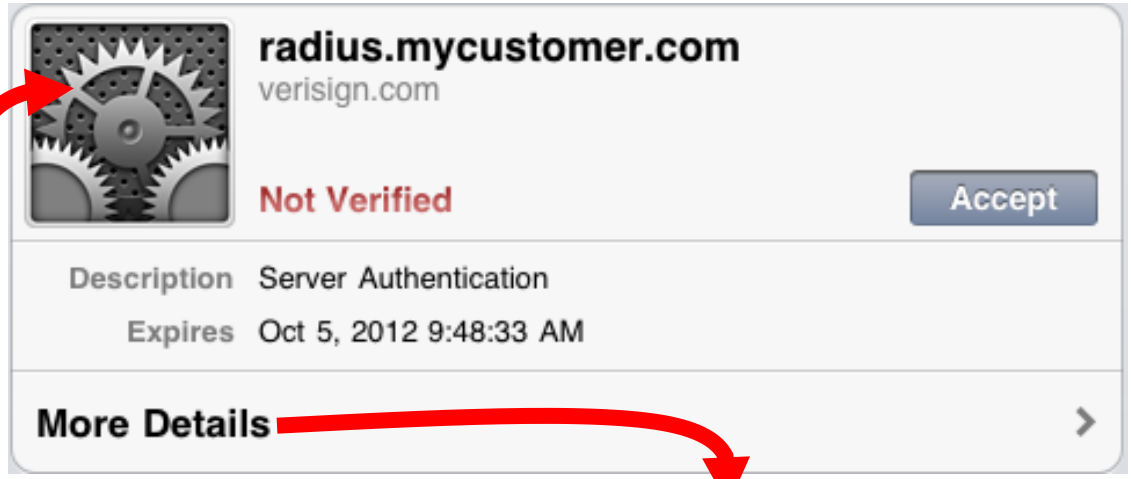


Between IE 6 and IE 9 we've learned that users are too easily tricked into accepting invalid SSL certificates. Mobile devices are not learning from the browser mistakes of the past.

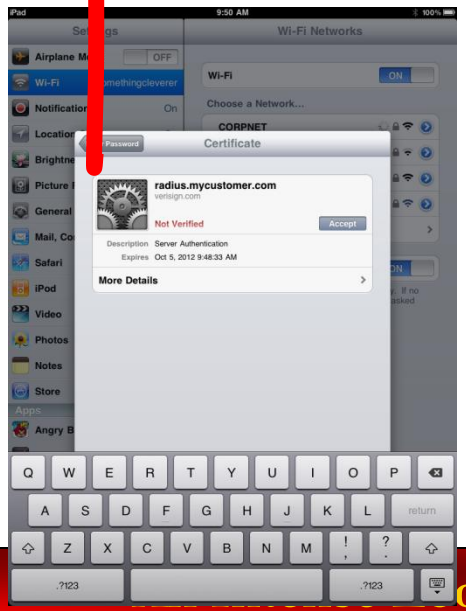
Secure Wireless Impersonation

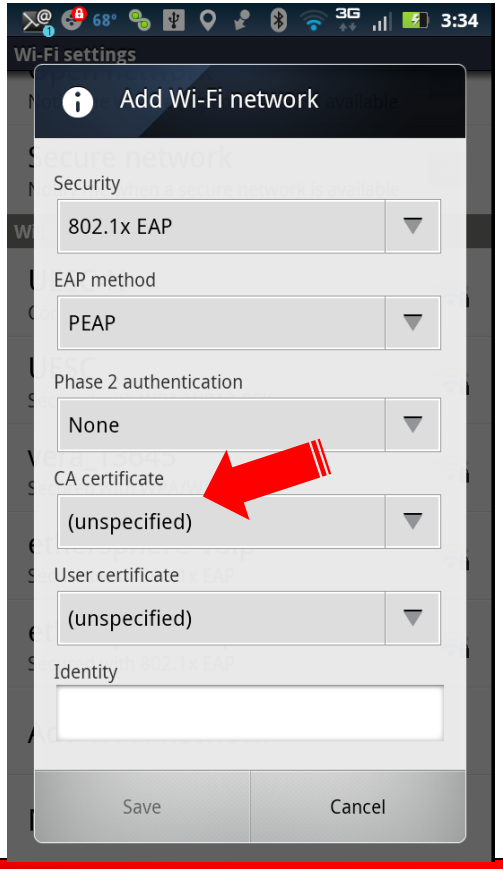
- SSL is used for more than web sites
- Enterprise wireless authentication methods such as PEAP and TTLS
  - Client validates RADIUS server with certificate information
- Creates an opportunity for an attacker to steal credentials

RADIUS Server Cert. Validation



On Android, all WLAN certificates are trusted by default, with no user interaction required.





Recovering PEAP Passwords

```
# tail -f /usr/local/var/log/radius/freeradius-server-wpe.log
mschap: Thu Oct  6 09:50:12 2011

        username: jwright
        challenge: ff:80:4d:52:0a:10:c7:33
        response:
21:77:8a:96:b7:16:e6:ed:e1:c2:19:06:66:ac:78:e9:cb:e1:21:e0:62:86:7d:45

^C
# asleap -C ff:80:4d:52:0a:10:c7:33 -R
21:77:8a:96:b7:16:e6:ed:e1:c2:19:06:66:ac:78:e9:cb:e1:21:e0:62:86:7d:45
-W rockyou.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "rockyou.txt".
        hash bytes:         c2dd
        NT hash:            c80f1ecc1c37905823872cf125d7c2dd
        password:           weloveyouesteban
```

Outline

- Mobile Device Proliferation
- Disparity of Mobile Devices
- Mobile Device Encryption
- Malware Threats
- Practical Attacks Against Wireless
- Don't Fight It, Change It

Policy Development

- Start with a sample policy (SANS Reading Room, bit.ly/ndUouv)
- Reference company data storage policies
  - What data is permitted on devices?
  - How is the data backed up, managed?
- Lost device reporting
- Reference software maintenance and patching policies
  - Minimum compliance for network access

Company or User Owned?

- When smartphones are owned by the company, the company sets policy
  - May leverage enforceable controls to monitor, audit and configure devices
- User owned devices may be forced to comply with some requirements
  - "If you want access to email, you must install our MDM client"
- Privacy requirements and policies

Mobile Device Management

- An MDM is an essential tool for enterprise networks
  - They are lacking, but still offer many security and monitoring benefits
- SaaS or in-house options
- Should offer flexibility to manage all mobile device platforms
- Talk to MDM vendor about controls missing in their platforms
  - They will need to talk to platform vendors

Mobile Devices Today?

I was recently asked if mobile devices could be deployed safely in a high-security environment processing sensitive data resources.

"No."

- This does not mean we can turn our back on mobile device deployments
  - No policy, no enforcement is more risk than embracing with limited controls today
- We need to grow up in security maturity (again)
  - We need to start today.

Conclusion

- A significant disparity exists between traditional and mobile devices
  - Also exists between mobile device vendors
- Technologies such as device encryption are not a panacea
- Malware on mobile devices is a growing market for attackers
- Several attack opportunities exist

The mobile device market needs enterprise maturity so that it can be deployed securely.