



Wireless Threats and Practical Exploits

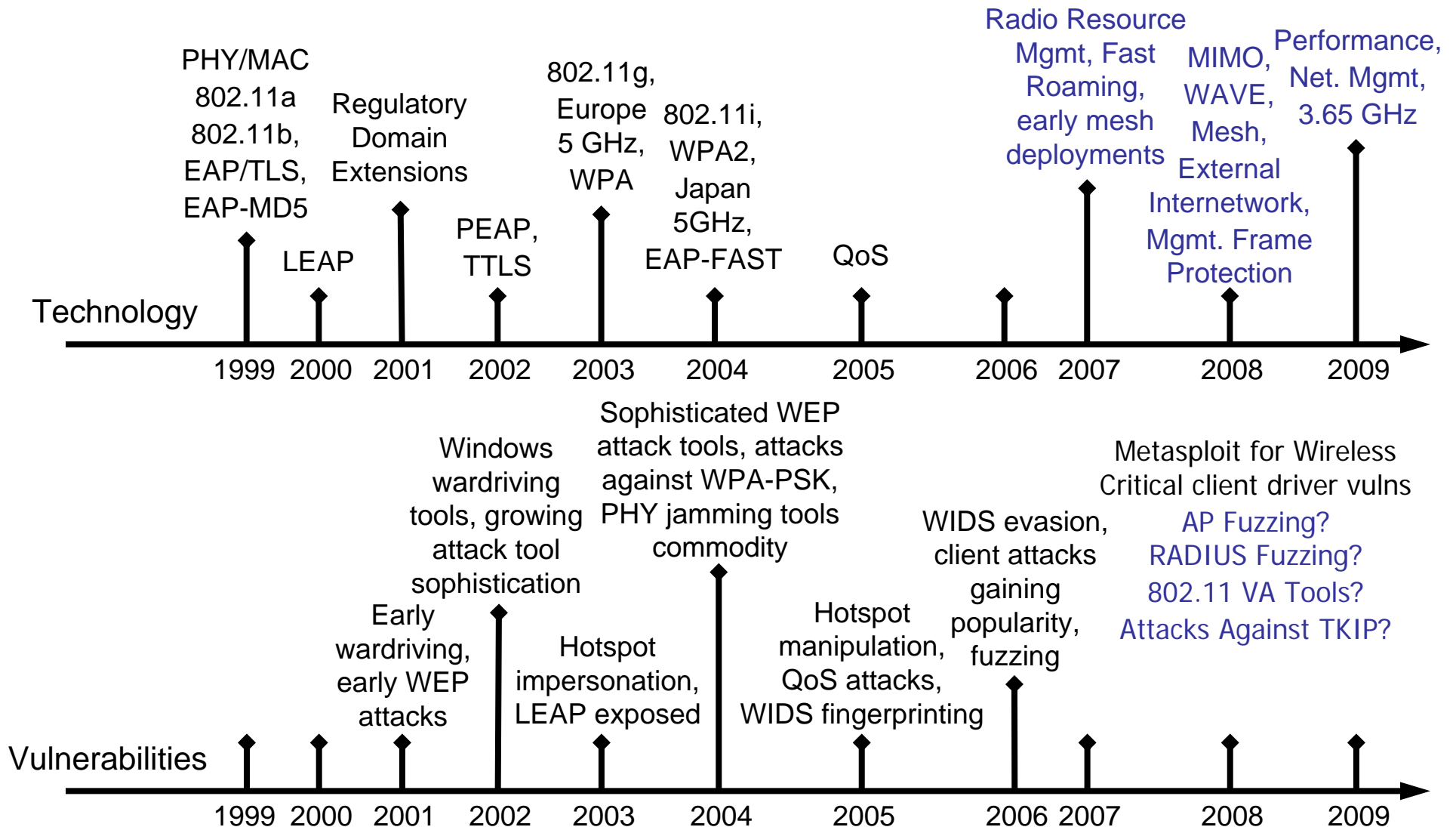
Joshua Wright, Senior Security Researcher



Introduction

- IEEE 802.11 technology and vulnerabilities
- Examining public WLAN attacks and the impact to organizations
- Emerging attack and wireless exploit trends

802.11 Technology and Vulnerabilities



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

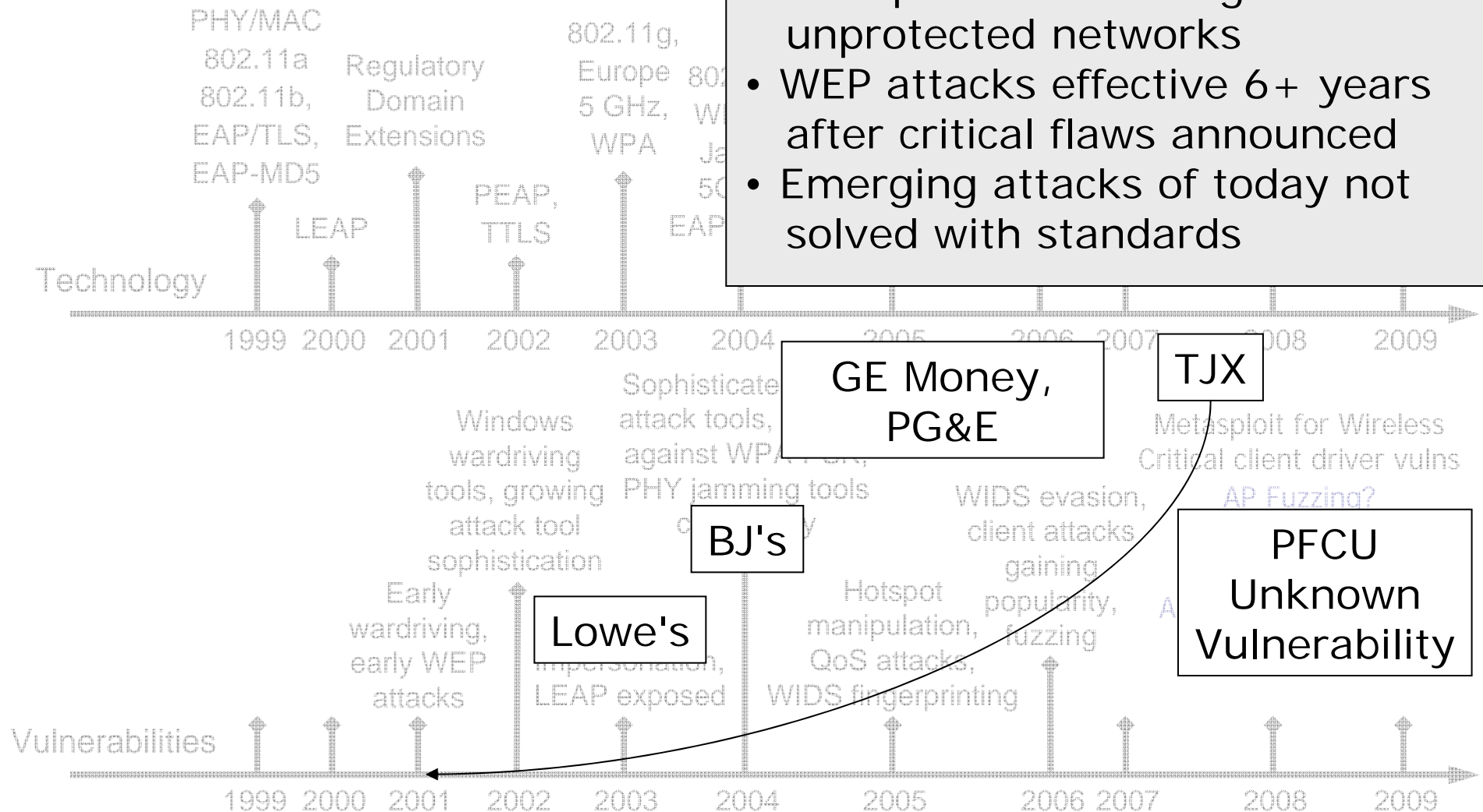
"... Butler moved to various hotel rooms where he would use a high-powered antenna to intercept wireless communications ... He would use the information obtained to hack into the institutions. One witness said Butler gained access to the Pentagon Federal Credit Union, Citibank and a government employee's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



"Bloodhound WiFi Gun"

Timeline and Incidents

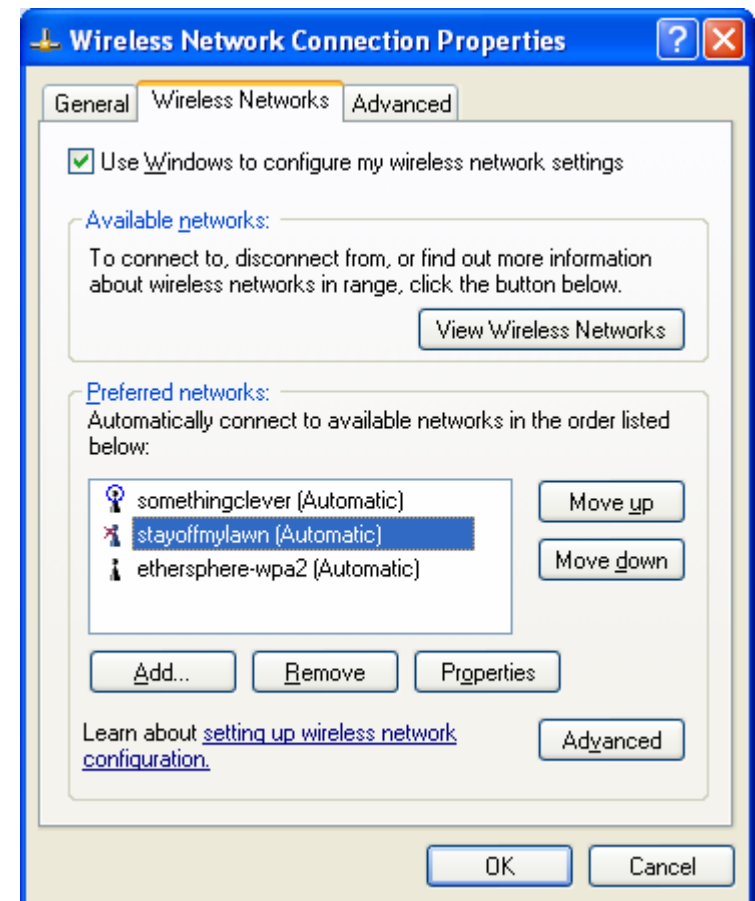
- Most public attacks against unprotected networks
- WEP attacks effective 6+ years after critical flaws announced
- Emerging attacks of today not solved with standards



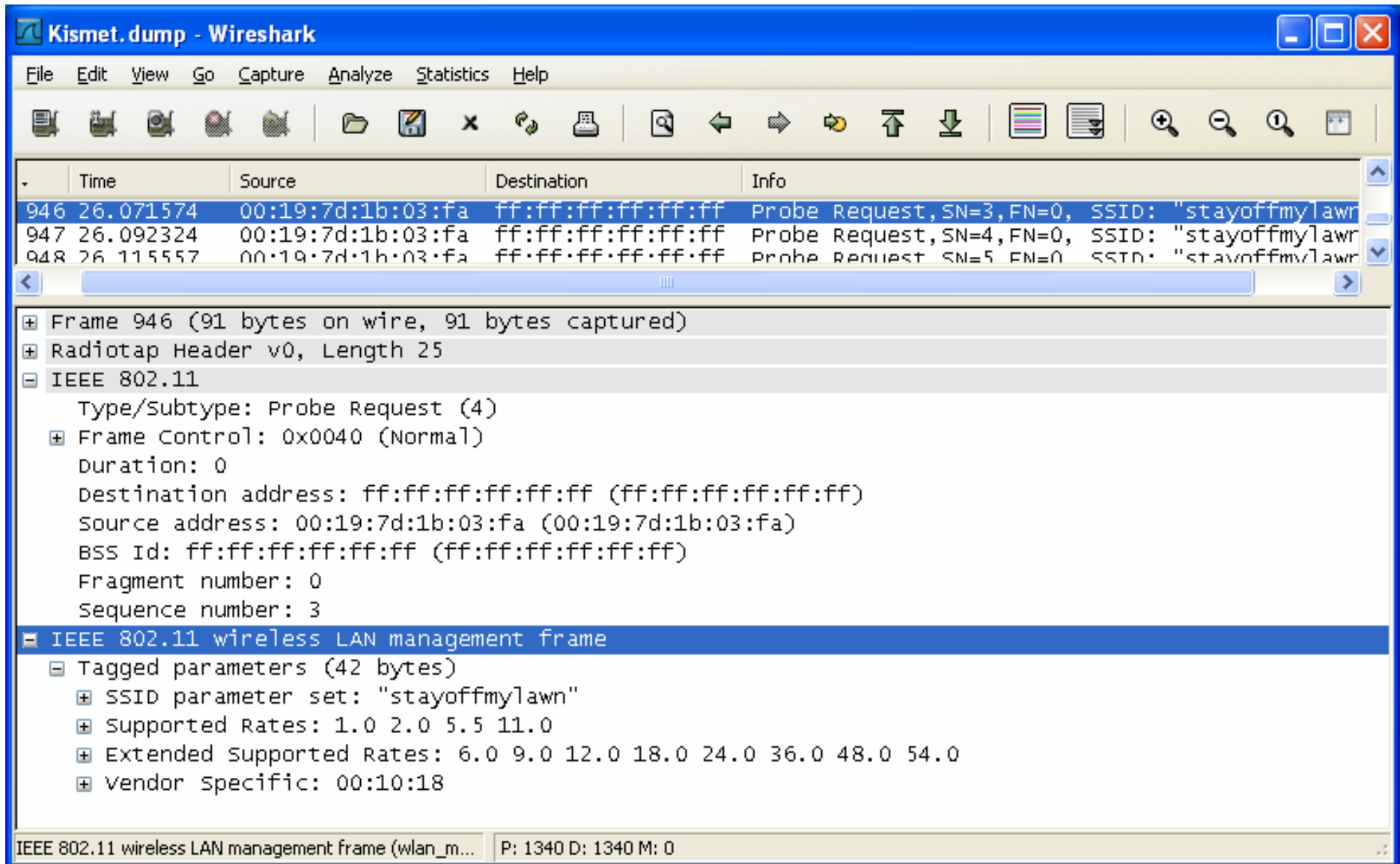
Anonymity Attacks

- 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



Eavesdropping on Broadcast Network Names



The image shows a Wireshark capture window titled "Kismet.dump - Wireshark". The packet list on the left shows three probe requests (frames 946, 947, and 948) all with source address 00:19:7d:1b:03:fa and destination address ff:ff:ff:ff:ff:ff. The selected packet (frame 946) is expanded in the packet details pane, showing the IEEE 802.11 frame structure. The frame control field is 0x0040 (Normal). The destination address is ff:ff:ff:ff:ff:ff, the source address is 00:19:7d:1b:03:fa, and the BSS ID is ff:ff:ff:ff:ff:ff. The frame is an IEEE 802.11 wireless LAN management frame (Type/Subtype: Probe Request (4)). The tagged parameters (42 bytes) include the 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), and vendor specific information (00:10:18).

No.	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: "stayoffmylawn"
947	26.092324	00:19:7d:1b:03:fa	ff:ff:ff:ff:ff:ff	Probe Request, SN=4, FN=0, SSID: "stayoffmylawn"
948	26.115557	00:19:7d:1b:03:fa	ff:ff:ff:ff:ff:ff	Probe Request, SN=5, FN=0, SSID: "stayoffmylawn"

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

http://www.wigle.net/gps/gps/main/confirmquery/

[Home](#) | [Download](#) | [Forums](#) | [Post File](#) | [Query](#) | [Screenshots](#) | [Stats](#) | [Uploads](#) | [Web Maps](#) | [MapPacks/Trees](#) | [Wiki](#) | [Logout](#)

 **Search Results:**

Showing stations 1 through 1 of this query.

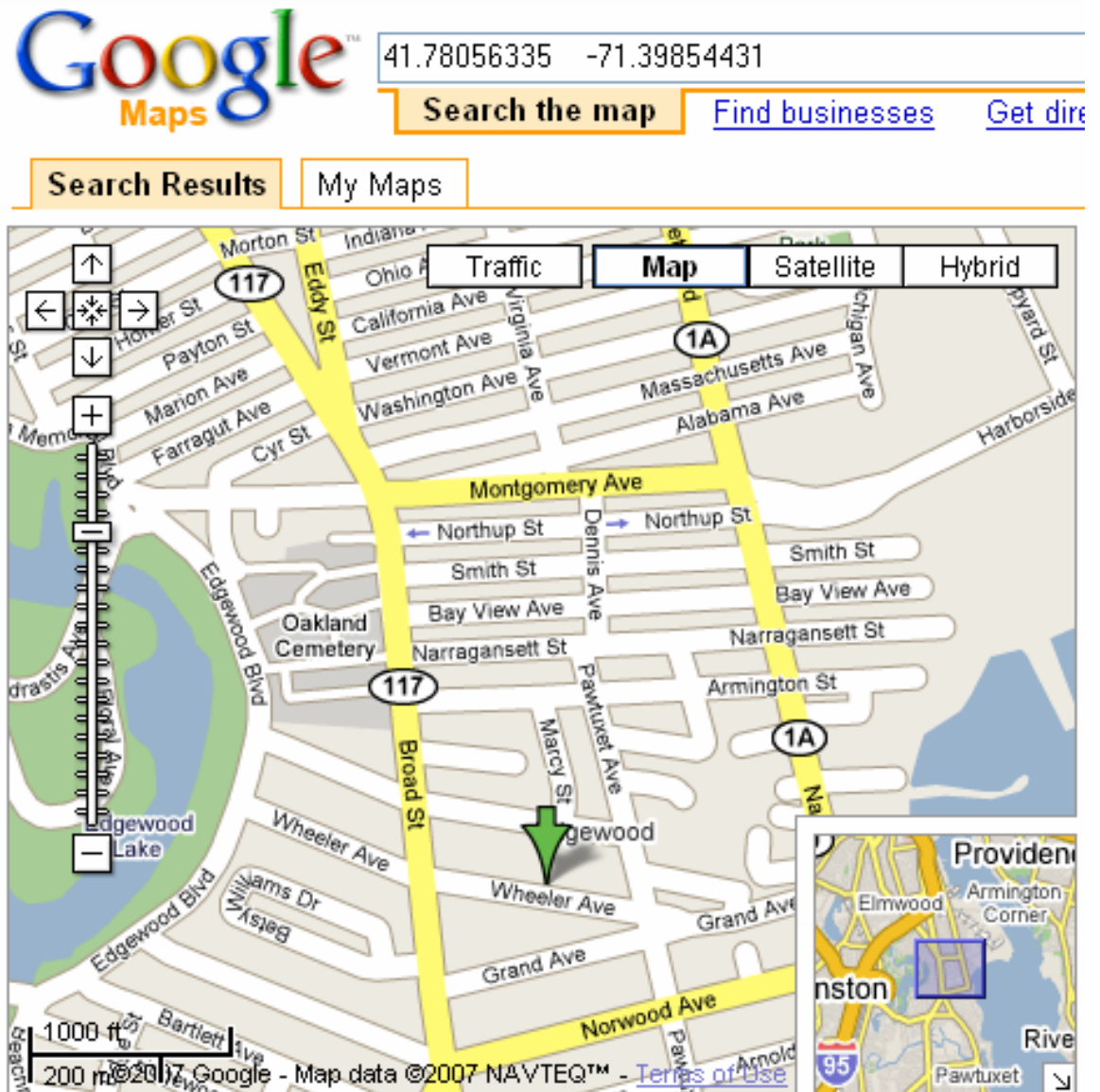
map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp	lastupdt
Get Map	00:0C:41:AC:8A:89	stayoffmylawn			infra	?	?	2007-06-14 08:47:04		N	41.78056335	-71.39854431	?	2007061415

[WiGLE Home](#)

Done

Google Maps

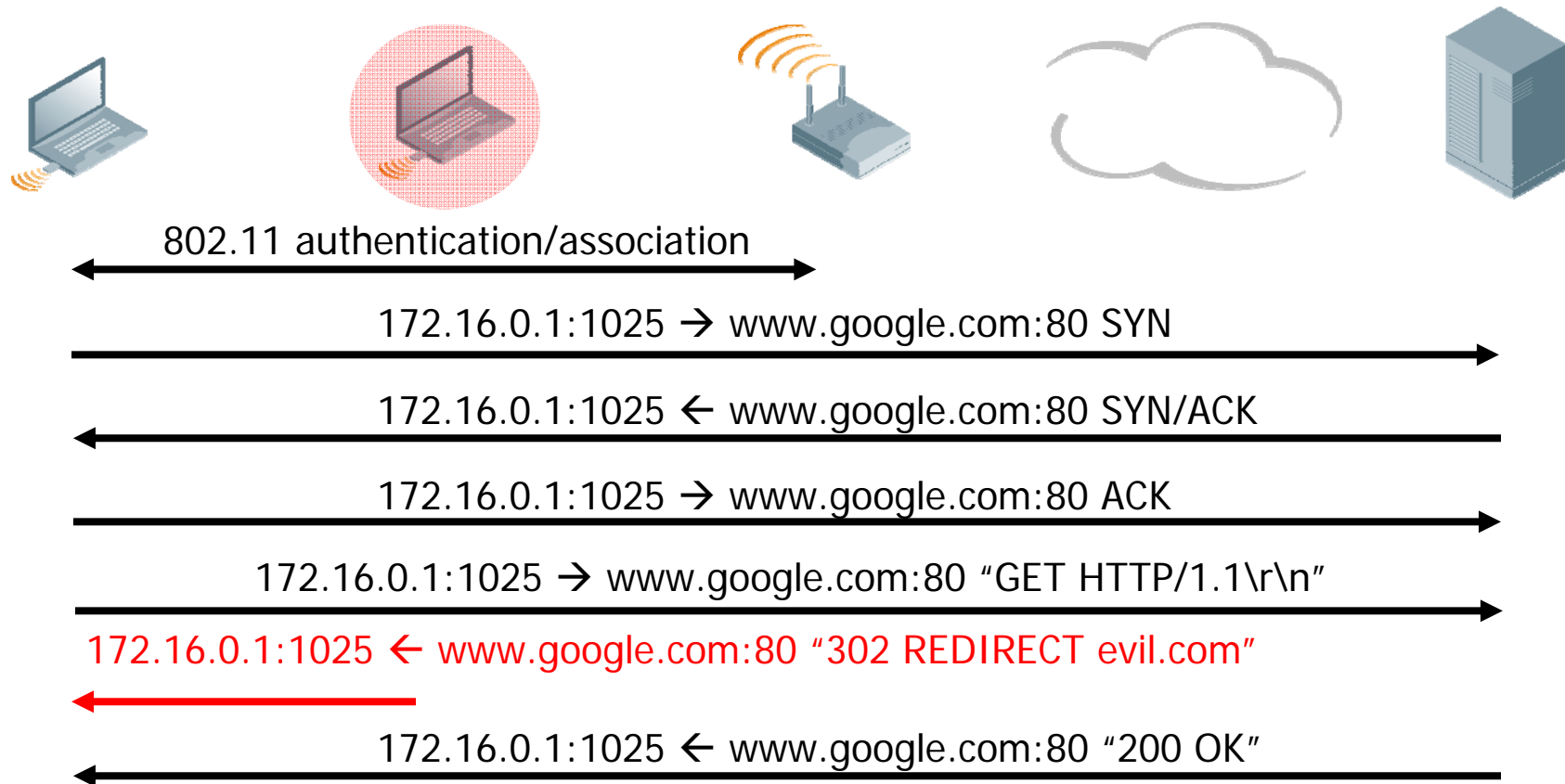
- Attacker knows the network name
- Identifies where you live through public data on wireless network locations
- Directions to your house or place of business



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



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

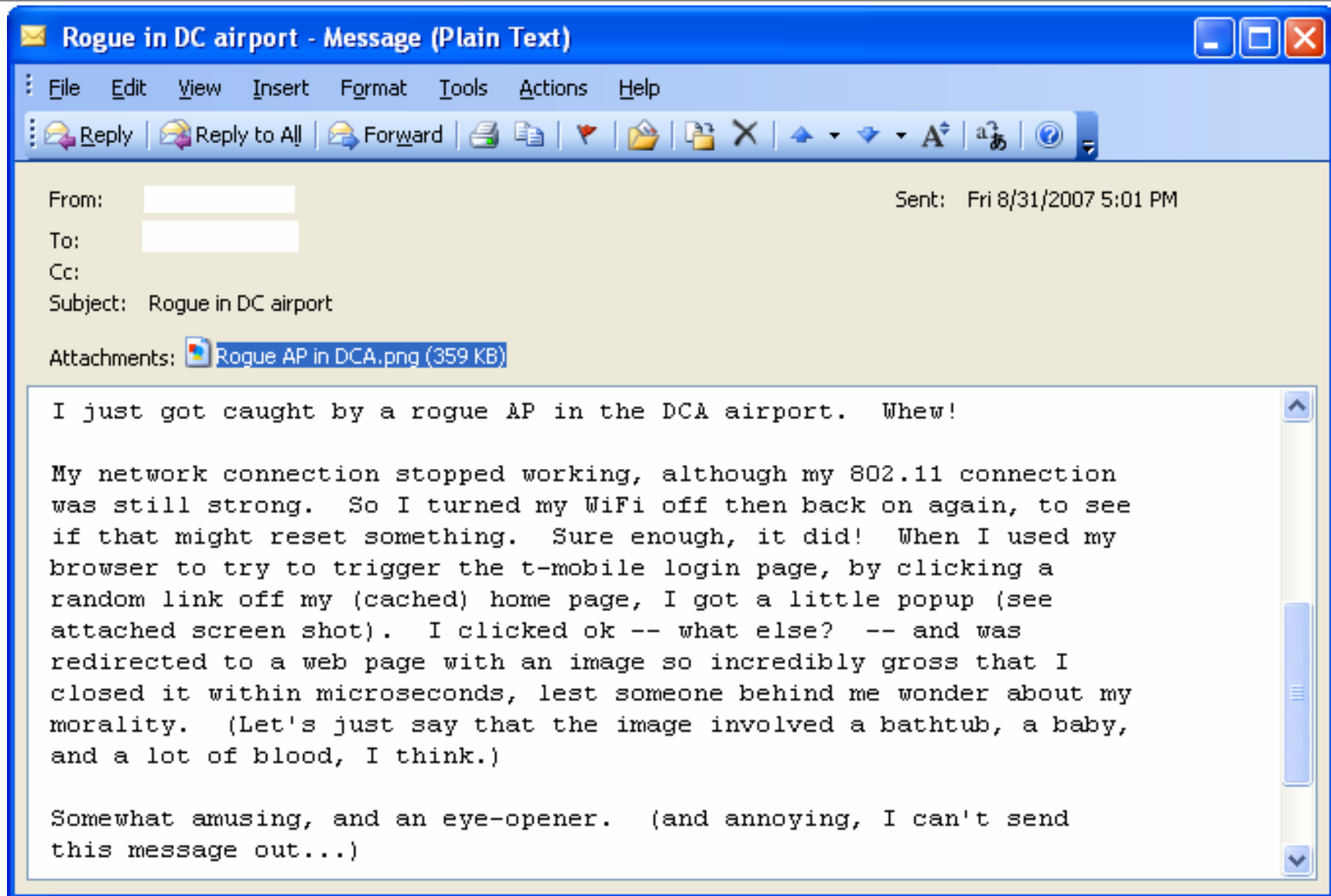
AirPWN: What the User Sees

```
$ 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_html
Listening for packets...
```



AirPWN'd at DCA



AirPWN: Where it Gets Dangerous

- IE 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`ÈAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```


Trends in Driving

- Many states have passed laws requiring hands-free driving
- Many users turn to Bluetooth technology for wireless headsets
 - Also car phone systems, some built-in

CT, NY, NJ and the District of Columbia have enacted laws prohibiting driving while talking on handheld cell phones

Governors Highway Safety Association: www.ghsa.org/html/stateinfo/laws/cellphone_laws.html

Challenge: Eavesdrop On A BT Headset

- Self-imposed challenge to evaluate Bluetooth headset security
- Target: Jawbone Headset
 - Popular headset, often paired with iPhone
 - I already owned one, so it was convenient



"Bluetooth is a short-range technology"

- Common misconception
- Class 1 devices have a range of 100M (328'), comparable to 802.11
- Class 2 devices have a range of 10M
- Possible to extend range with directional antennas
- Linksys USB BT100



Long-Range Bluetooth

- Possible to connect to class 2 device (10M) from over a mile away
- Using class 1 source device and 18 dBi gain antenna



Headset as a Listening Bug

- Limitation: When link key is not known, unable to decrypt active voice call traffic
 - Instead, target headset when not in a call
- Can leverage the audio mic to record audio
 - Can also inject audio into the headphone
- Headset PIN is (almost) always "0000"
 - Only practical security is non-discoverable mode

Not an attack against active Bluetooth conversations.
Connecting to a device when not in a call to
record/inject audio.

CarWhisperer

- Designed to connect to car hands-free Bluetooth device
 - Embedded, or third-party installed
 - Often in discoverable mode by default
- Play or record audio through car speakers, attacks weak PIN selection

"This is the police, stop speeding"



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

"The Good Old Days"



Encryption and Authentication

- Modern networks should leverage WPA2 with AES-based CCMP for encryption
 - Counter 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

Conclusion

- Attacks against wireless networks are costly to organizations
- Many organizations repeat mistakes which have led to visible, high-profile public compromises
- Attacks include privacy/anonymity compromise, hotspot manipulation and BT headset manipulation
- Mitigation strategies include:
 - Deploying strong encryption and authentication protocols
 - Employ rogue monitoring, wireless intrusion detection
 - Protect client systems with patch management, enforcement

Thank you!

Joshua Wright
Senior Security Researcher
Aruba Networks
jwright@arubanetworks.com
Office/Mobile: 401-524-2911

Presentation at www.willhackforsushi.com