



Risks & Rewards of WiFi and WiMax

BITS Wireless Security Forum

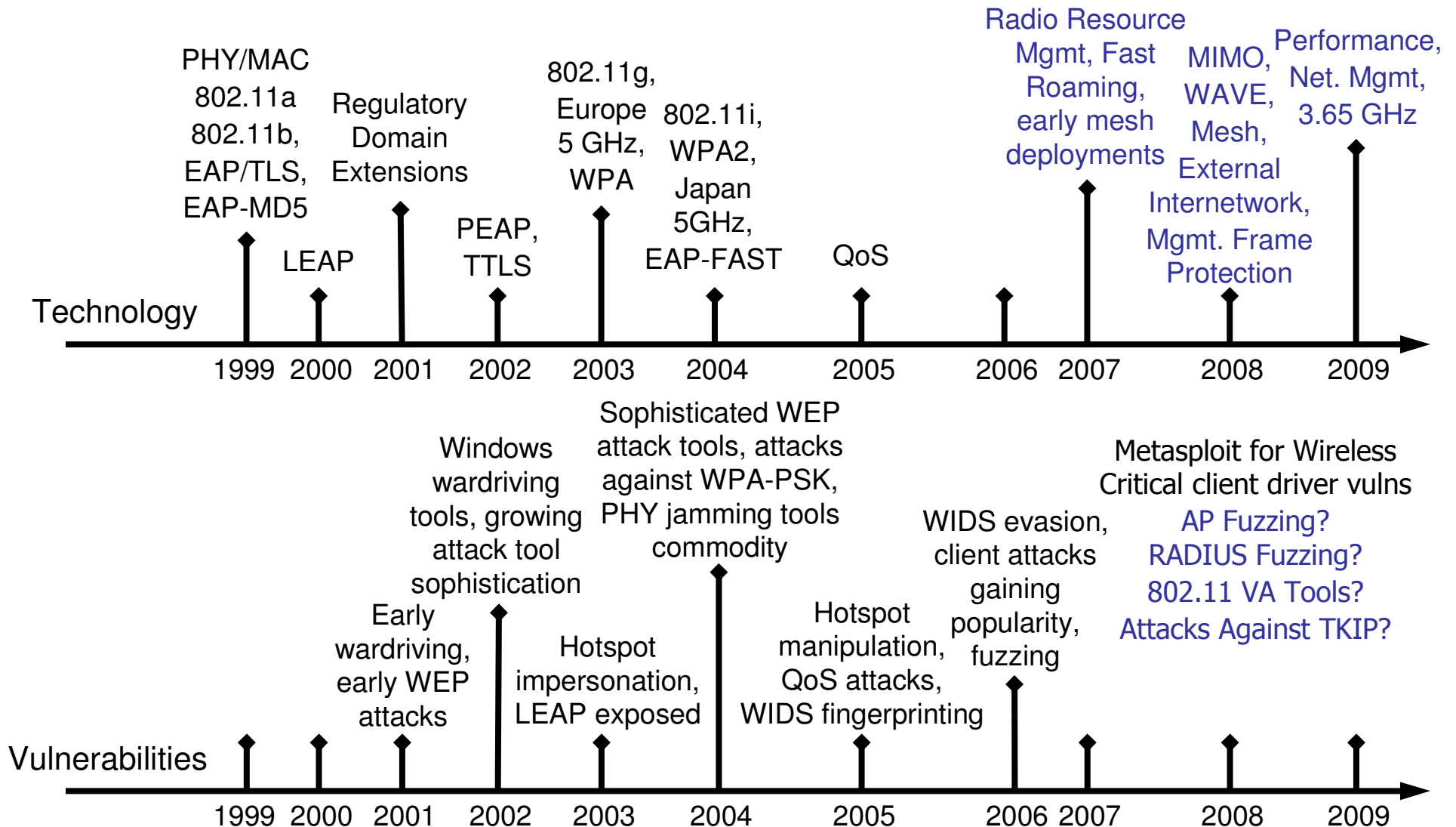
Joshua Wright, Senior Security Researcher



Introduction

- IEEE 802.11 technology and vulnerabilities
- Examining public WLAN attacks and the impact to organizations
- Anonymity threats and wireless networks; an example

802.11 Technology and Vulnerabilities



Review of Public WLAN Security Attacks (1)

- 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 (2)

- 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 (3)

- 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."

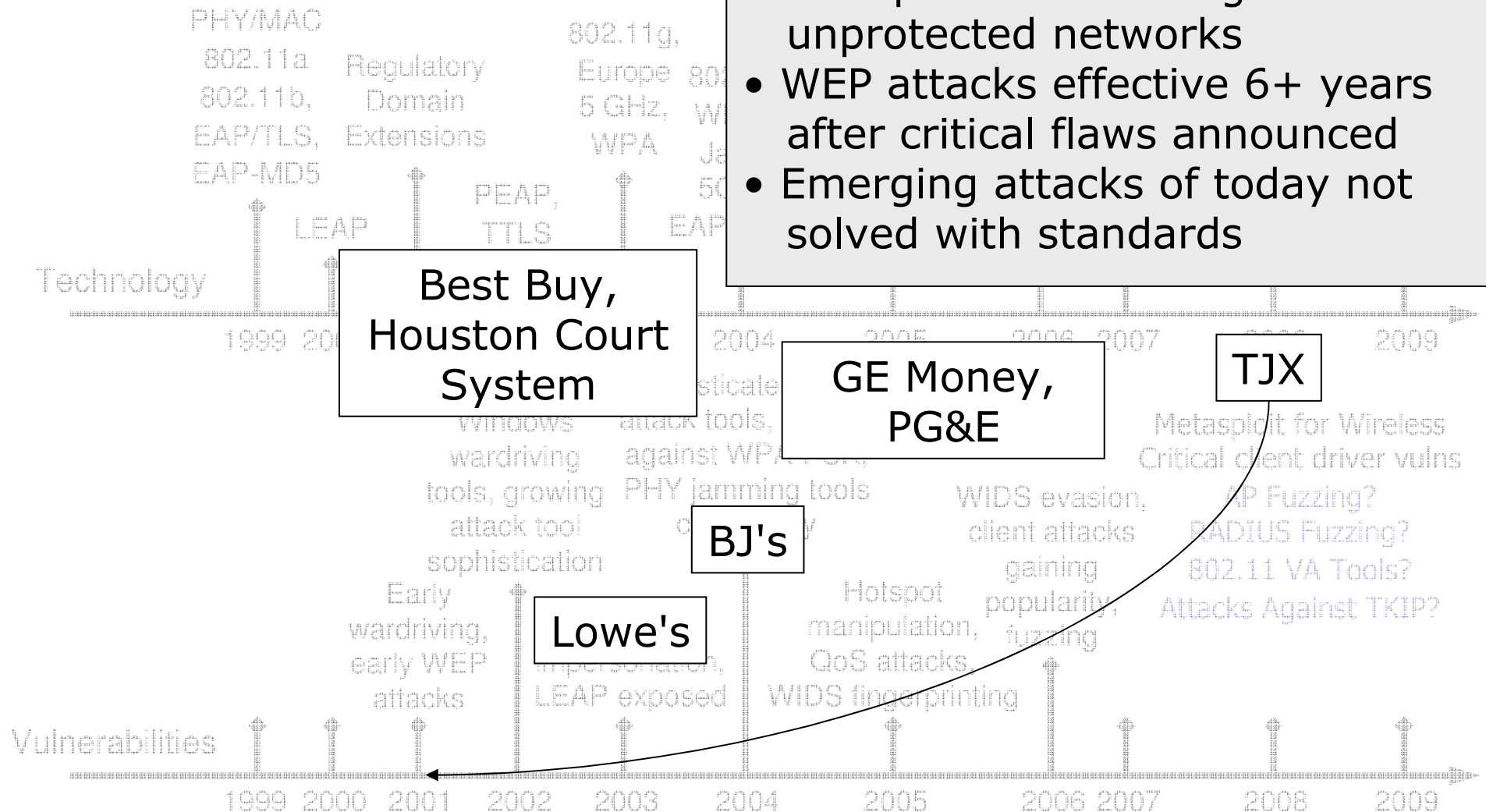
Review of Public WLAN Security Attacks (4)

- 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."

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

The image shows a Wireshark capture window titled 'Kismet.dump - Wireshark'. The packet list at the top shows three frames (946, 947, 948) all being Probe Requests for the SSID 'stayoffmylawn'. The details pane for frame 946 is expanded, showing the IEEE 802.11 structure. The frame control field indicates a normal probe request to the broadcast address (ff:ff:ff:ff:ff:ff) from the source address 00:19:7d:1b:03:fa. The management frame body contains tagged parameters including the SSID 'stayoffmylawn', supported rates, and a vendor-specific field with the value 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	dhc	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



41.78056335 -71.39854431

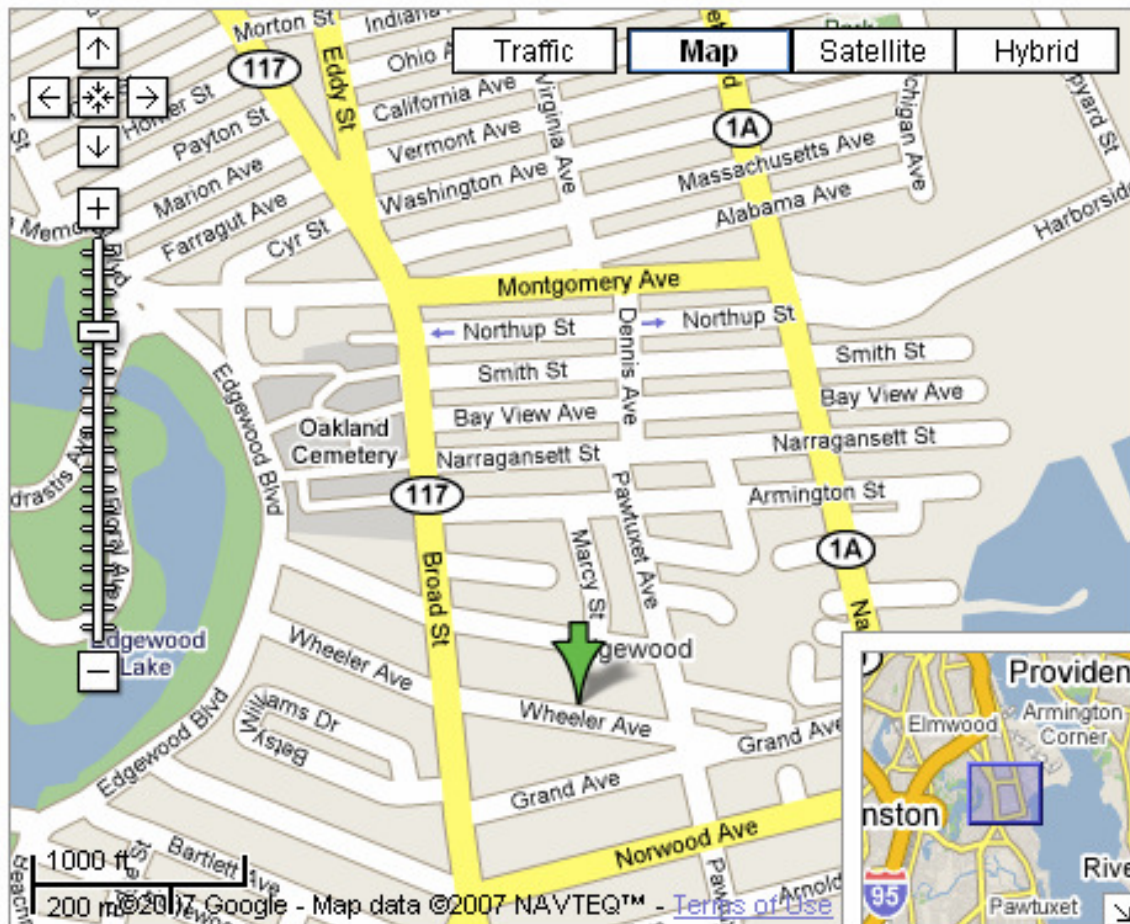
[Search the map](#)

[Find businesses](#)

[Get directions](#)

Search Results

My Maps



↑
Nick DePetrillo

Conclusion

Thank you!

Joshua Wright

Office/Mobile: 401-524-2911

Aruba Networks

www.arubanetworks.com