

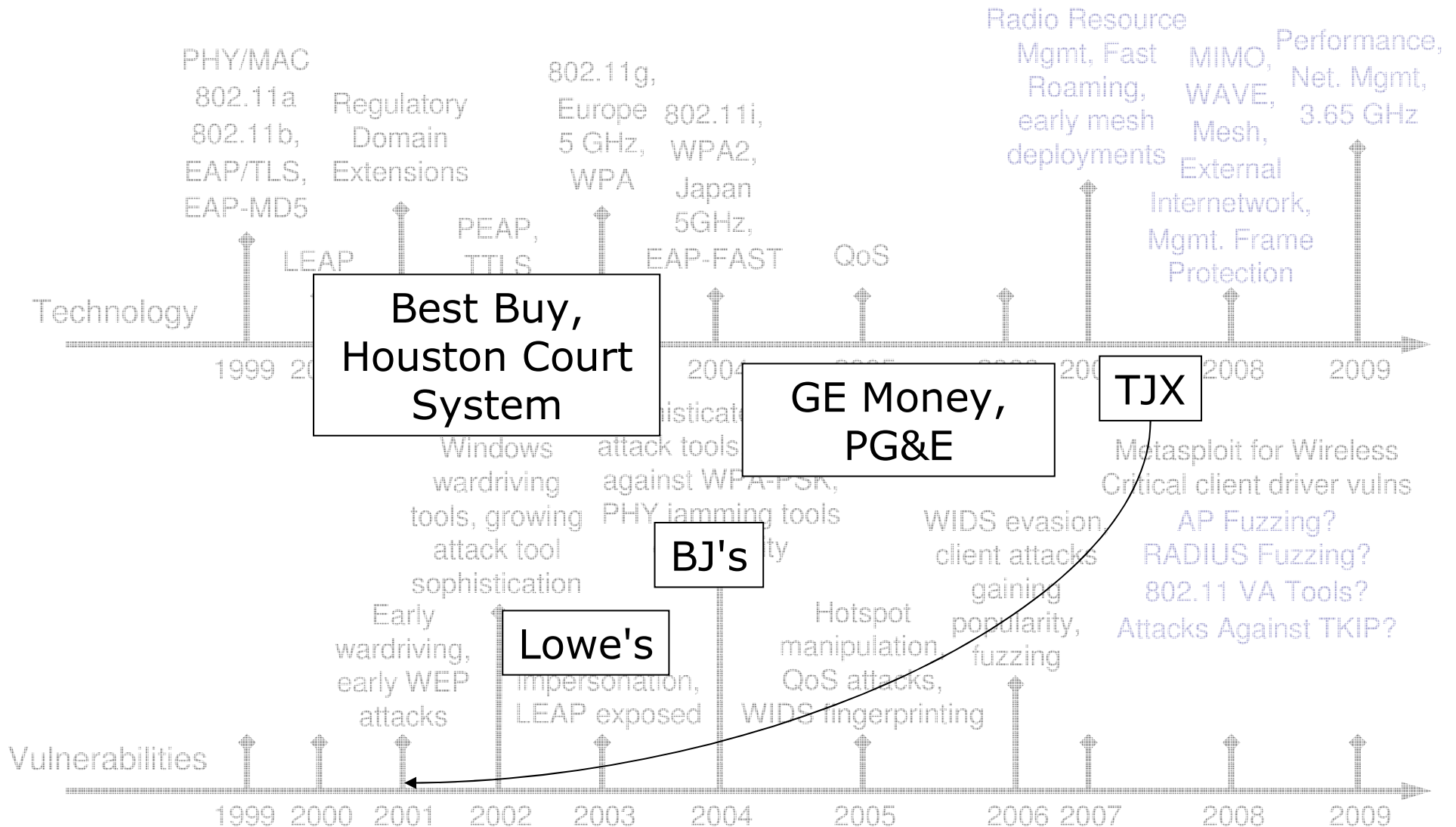


***Wireless Security Strategies that  
Don't Work: Lessons Learned  
Perspective***

Joshua Wright, Senior Security Researcher  
jwright@arubanetworks.com, 401-524-2911



# 802.11 Technology and Vulnerabilities



# 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

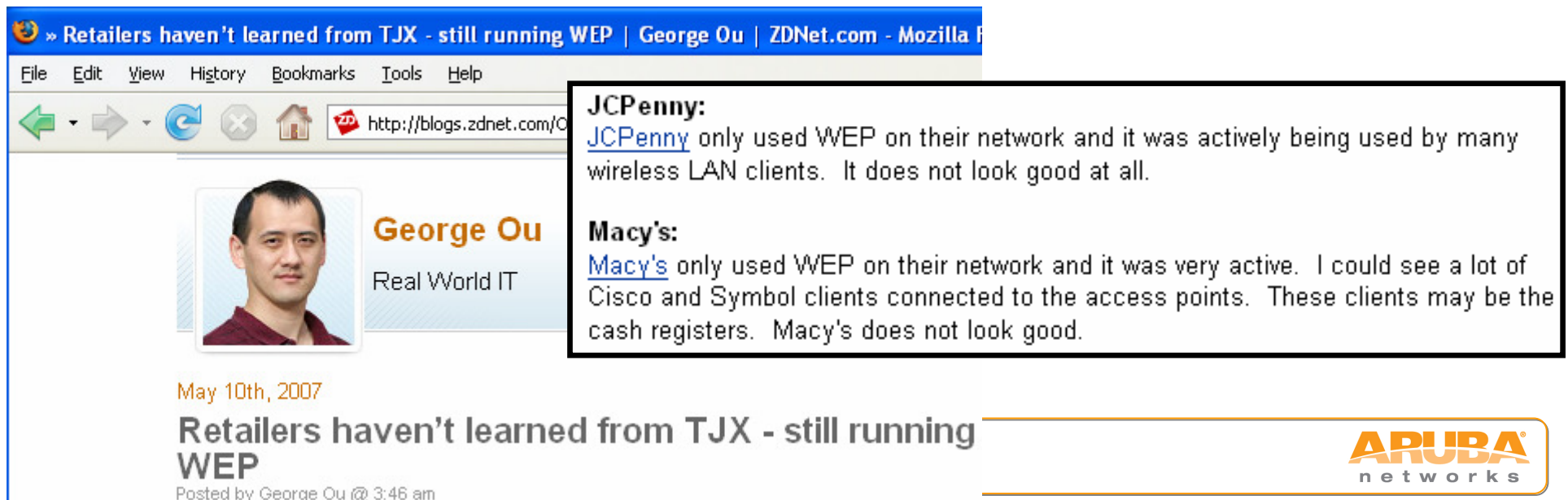
- Often used as an authentication mechanism
  - Especially for legacy devices
- Trivial for an attacker to identify valid MAC addresses and impersonate
- *Strong authentication must involve cryptographic primitives, independently evaluated*

Network List—(Packets desc)—										(-) Up	Info
Name	T	W	Ch	Packets	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	0B	0.0.0.0				0
.	F 00:04:5A:29:51:B6	Linksys		0	0	0B	209.70.174				0
.	F 00:20:78:C7:9A:ED	Unknown		0	0	0B	209.70.122				0
.	F 00:20:78:D3:15:1E	Unknown		0	0	0B	0.0.0.0				0
.	F 00:04:5A:E1:B7:D6	Linksys		0	0	0B	209.70.221				0
.	F 00:04:5A:25:F0:90	Linksys		0	0	0B	0.0.0.0				0
.	F 00:06:28:55:8F:41	Unknown		0	0	0B	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

# "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 Firefox

File Edit View History Bookmarks Tools Help

http://blogs.zdnet.com/O

 **George Ou**  
Real World IT

May 10th, 2007

**Retailers haven't learned from TJX - still running WEP**  
Posted by George Ou @ 3:46 am

**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.

**ARUBA**  
networks

# 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"



## 3 Actionable Steps For WLAN Risk Mitigation

1. Identify schedule and timeline to transition to WPA2 with IEEE 802.1X authentication
  - EAP types EAP/TLS and PEAP or TTLS provide strong security
  - EAP types such as LEAP, EAP-MD5 should never be used
  - WEP cannot be relied upon for any form of data privacy or access control
2. Evaluate wireless monitoring strategies for attack identification and policy enforcement
  - System should identify rogue threats and policy violations (e.g. WEP use with a WPA2-only policy)
3. Leverage user identity authentication with role-based access controls to limit network accessibility

# Conclusion

Thank you!

Joshua Wright

[jwright@arubanetworks.com](mailto:jwright@arubanetworks.com)

Office/Mobile: 401-524-2911

Aruba Networks

[www.arubanetworks.com](http://www.arubanetworks.com)