Financial Districts Wireless Vulnerability Study

A study conducted by AirTight Networks, Inc.

www.aitightnetworks.com
Scan Financial districts for WiFi vulnerabilities
- To assess adoption of WiFi security best practices by organizations in major financial districts

Methodology
- Visited 7 financial districts (6 in US, 1 in UK)
- Scanned WiFi signal for 5 minutes at a randomly selected location
- 3632 APs scanned
- 547 Clients scanned
Financial Districts Covered in this Study

- New York
- Chicago
- Boston
- Wilmington, DE
- Philadelphia
- San Francisco
- London

- A sample WiFi trace tells a lot about network security posture in each location.
View from Wardriver’s Windshield

- Open Aps
- Weak encryption
- Default settings
- Viral SSIDs
- Identity leakage
- Insecure configs
- Flawed practices
- No risk cover!
Key Findings: Widespread Use of Insecure Practices

- 57% of WiFi networks are either OPEN or using weak (WEP) encryption
- Enterprise grade APs were found configured in WEP mode instead of WPA or WPA2
- 39% of threat posing APs (OPEN and WEP) are enterprise grade
- 27% of open APs (non hotspot and non guest) were hiding their SSIDs
Key Findings: Client Vulnerabilities Everywhere

- 61% of threat posing (OPEN and WEP) APs are home/SOHO grade
  - Such devices are operating beyond IT/Security group’s visibility and control
  - Authorized client devices can connect and bypass security controls

- 13% of mobile WiFi clients were found operating in ad hoc mode
  - Actively looking to connect to viral networks such as “Free Public WiFi” & “Free Internet Access”
  - Vulnerable to wi-phishing or honeypotting
A Closer Look at OPEN Access Points
What are OPEN APs being used for?

**Intended Uses**
- Hotspot Access
- Guest Access

**Reality**
- Personal WiFi devices
- Misconfigured APs
- Rogue APs

**Vulnerabilities**
- Backdoor to the wired enterprise network
- Unwitting, impatient employee looking for WiFi access bypass security
Magnified Look at OPEN Access Points

35% Guests/Hotspots APs
- Acadian-Public
- CCCFREE
- tmobile
- eMobile-Zone
- attwifi
- cityhallpublicwireless
- visitor
- WiFi Zone – The Cloud
- WIZ
- XCEWLAN-Guest
- Wayport_Access
- Martiz Guest

65% Non Guests/Hotspots APs
- (null ssid)
- BE11g
- any
- linksys
- monkey
- nikwlan
- WLAN
- kellie
- engineers
- default
- coair722
- copysecure

(1) Hotspot/Guests APs don’t hide SSID
(2) Hotspot SSIDs are well known/published and advertised
(3) Usually signal from multiple hotspot APs is visible at any coverage location
Data Leakage Through Open APs

- Hackers can gain direct access to sensitive data storage – remember TJX breach!
- Hackers can scan all enterprise devices and servers for vulnerabilities and exploit them
- Clients connecting to external APs expose data

Organization identity & executive’s names were visible in clear text in the leaking packets!
We found many instances of packets leaking out of OPEN APs attached to financial network’s internal network!
Practice of SSID Hiding: Security Through Obscurity

**Observations about detected APs**

| Majorit of OPEN APs with hidden SSID are Enterprise grade! |

| So What? |

| There is continued belief among security administrators that SSID hiding adds security. |
A Closer Look at WEP Access Points
Very Low Adoption Rate of WPA2

- 33% WiFi networks in financial districts using WEP!
- No good justification for continued use of WEP
- WEP cracking time reduced to less than 5 minutes!
- APs intended for private applications must use WPA/WPA2

<table>
<thead>
<tr>
<th>Observations about detected WEP APs</th>
<th>So What?</th>
</tr>
</thead>
<tbody>
<tr>
<td>24% of WEP APs are Enterprise grade</td>
<td>These APs are fully capable of supporting stronger encryption such as WPA/WPA2</td>
</tr>
</tbody>
</table>
Wi-Fi Security Footprint in Each Financial District

- New York: Open 60%, WEP 20%, WPA 20%
- Chicago: Open 50%, WEP 30%, WPA 20%
- Boston: Open 55%, WEP 35%, WPA 10%
- Wilmington, DE: Open 40%, WEP 40%, WPA 20%
- Philadelphia: Open 30%, WEP 50%, WPA 20%
- San Francisco: Open 45%, WEP 35%, WPA 20%
- London: Open 35%, WEP 35%, WPA 30%
A Closer Look at WiFi Clients, iPhones, Blackberry’s
Trusted Network Information Leakage By Wi-Fi Users

- Over 56% of clients were broadcasting the name of their trusted Wi-Fi networks
- 34% of them were willing to connect to “HIGHLY INSECURE” Wi-Fi networks

Clients are vulnerable to “Honeypot” / “Caffe Latte” style attacks
Viral Wi-Fi Outbreak Continues

Over 13% laptops found to be infected from Viral SSIDs

Top 3 viral SSIDs found at almost all scan locations are:
- Free Public WiFi
- hpsetup
- Free Internet Access
Conclusions
Weak Wi-Fi Security Policy Definition and Enforcement

- Identity & data leakage from corporate Wi-Fi devices and clients
- Alarming number of mis-configured, unmanaged Access Points
- Clients actively probing for “familiar SSIDs”
- Client ad-hoc connections bypassing security
IT Lacks Wireless Security Expertise

- Not limited to specific WLAN vendor
- No limited to specific locations
- Need to control resources - WiFi infrastructure and clients

**Sample collected in Boston**

- 01:20:51:20:20:01 | WEP | Cisco
- 01:20:51:20:20:02 | WEP | Cisco
- 01:20:51:20:20:03 | WEP | Cisco

**Sample collected in Chicago**

- 02:20:51:20:20:01 | WEP | Motorola
- 02:20:51:20:20:02 | WEP | Motorola
- 02:20:51:20:20:03 | WEP | Motorola

**Sample collected in Boston/San Francisco**

- 03:20:51:20:20:01 | WEP | Nortel
- 03:20:51:20:20:02 | WEP | Nortel
- 03:20:51:20:20:03 | WEP | Nortel
# Five Steps to Protect Against WiFi Security Breaches

<table>
<thead>
<tr>
<th>Recommended Best Practice</th>
<th>WiFi deployed</th>
<th>WiFi not deployed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use strong authentication and encryption:</strong> Use the best standards for authentication and encryption (e.g., WPA/WPA2) when deploying WiFi networks</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Monitor guest WiFi access:</strong> Authenticate guest users and monitor unauthorized access when providing guest access over WiFi networks</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Conduct wireless security audits and scans:</strong> Periodically conduct wireless scans to detect presence of unauthorized WiFi devices and activity in your premises.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Follow endpoint wireless security best practices:</strong> Promote WiFi security best practices among laptop users. Using wireless security endpoint security agent, enforce your enterprise policies seamlessly across all laptops and secure them even when they are away.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Use a Wireless Intrusion Prevention System (WIPS):</strong> Prevent leakage of sensitive data and protect your network from wireless security threats with 24/7 wireless monitoring</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>