Wireless Vulnerability Assessment: Airport Scanning Report

www.airtightnetworks.net

A Study Conducted by AirTight Networks
About this Study

**Background**

- Airports world-wide now provide Wi-Fi Internet access for mobile users
- Use of Wi-Fi hotspots by business users at airports is steadily increasing
- Airports are increasingly using private Wi-Fi networks for baggage handling as well as passenger ticketing

**The Goal**

- To assess adoption of security best practices at Airport Wi-Fi networks
- To assess information security risk exposure of laptop users while they are transiting through airports
**Study Methodology**

- Visited 14 airports world-wide (11 in US; 3 in Asia-Pacific)
- Scanned Wi-Fi signal for 5 minutes at randomly selected location (typically a departure gate or lounge area)
- Traces collected using off the shelf Wi-Fi card and publicly available data collection tools
- Traces collected between 30 Jan 2008 through 8 Feb 2008
- Number of Access Points = 478; Number of Clients = 585
Key Findings & Implications

<table>
<thead>
<tr>
<th>Study Findings</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Critical Airport systems found vulnerable to Wi-Fi threats</td>
<td>~ 80% of the private Wi-Fi networks at Airports are OPEN / WEP!</td>
</tr>
<tr>
<td>2. Data leakage by both hotspot and non-hotspot users</td>
<td>Only 3% of hotspot users are using VPNs to encrypt their data! Non-hotspot users found leaking network information</td>
</tr>
<tr>
<td>3. ‘Viral Wi-Fi’ outbreak continues</td>
<td>Over 10% laptops found to be infected!</td>
</tr>
</tbody>
</table>
Summary of Findings

- We expected to find mostly hotspot networks but we found
  - 77% of the Wi-Fi networks are non-hotspot (i.e., private) Wi-Fi networks
  - 80% of the private Wi-Fi networks are unsecured or are using legacy WEP security
  - There is a high probability some of these Wi-Fi networks are used for logistics, baggage handling, as well as passenger ticketing

- We found considerable data leakage by Wi-Fi hotspot users
  - Only 3% of the users are using VPN to secure their hotspot Wi-Fi connection
  - Sensitive information such as user credentials can be easily captured over the air
  - We found all Wi-Fi users at the airport were leaking their Wi-Fi networking information!

- Users are taking serious risks in connecting to “viral” Wi-Fi networks
  - “Viral” Wi-Fi networks are rapidly spreading...
    - 10% of the laptops are already infected
  - Attackers can take control of victim’s laptop - confidential data theft!
  - We found active “viral” Wi-Fi networks at almost all Airports
Majority of Wi-Fi networks are OPEN
A large number of WEP installations are also visible ~28%
Small % of secure WPA/WPA2 Wi-Fi networks

But are all OPEN Wi-Fi networks Hot-Spots?

A total of 478 Wi-Fi Access Points were analyzed across all Airports!
Wi-Fi Scan Results

**Access Points (APs)**

**Public Wi-Fi Hotspots**

- 123x
- 12x4
- attwifi
- access
- concourse
- default
- free
- flypdx
- flypittsburgh
- golden
tree
- internet
- jwa
- klia-wifi
- linksys
- myr
- netgear
- public
- tmobile
- wireless
- wayport
- wifi

**Private Wi-Fi Networks**

**Open APs**

These don’t look like hotspot APs!
A magnified look at **Unsecured Access Points**

- **41%** Hotspot APs
  - Concourse
  - tmobile
  - Wayport
  - AttWi-Fi
  - FlyPittsburgh
  - Flypdx
  - singaporeair_B
  - singaporeair_F
  - JWA Hotspot
  - Ft.Laud-Hlwd_Airport-Public
  - ACCESS-StarHub

- **59%** Non Hotspot APs
  - (null ssid)
  - Backbone
  - PacGate
  - LGDacom
  - SFOPRIVATE
  - Ice Currency Services
  - IAACCO
  - KIOSKWIRELESS
  - BullPenH1
  - AceRail
  - e-Baggage Trial AP1

  1. **Hotspot 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**
To our surprise, we found –

- 77% of the Wi-Fi networks are non hotspot networks (private Wi-Fi networks)
- 80% of these networks are unsecured or are using legacy WEP security

There is a high probability these networks are being used for:

- Baggage handling
- Passenger ticketing
- By retailers

These networks can be hacked within minutes...
Vulnerability discovered at SFO Airport

- The Wi-Fi Access Points listed below are possibly a part of the airport’s baggage management infrastructure
  - ultratrak is possibly an SSID (Wi-Fi network) for baggage tracking service
    - [http://www.ultra-as.com/products-solutions/ultratrak.html](http://www.ultra-as.com/products-solutions/ultratrak.html) claims their baggage tracking solution “ultratrak” is in use at SFO

<table>
<thead>
<tr>
<th>Vendor</th>
<th>MAC Address</th>
<th>SSID</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>(Hidden)</td>
<td>WEP</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>(Hidden)</td>
<td>Open</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>ultratrak</td>
<td>WEP</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>ultratrak</td>
<td>WEP</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>(Hidden)</td>
<td>Open</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>(Hidden)</td>
<td>WEP</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>44:34:12:</td>
<td>WEP</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>(Hidden)</td>
<td>Open</td>
</tr>
<tr>
<td>Cisco</td>
<td>0:13:1a:38:20:10</td>
<td>ultratrak</td>
<td>WEP</td>
</tr>
</tbody>
</table>

We discovered the “Hidden” SSID of an AP in a mere 5 minute scan!

The “Hidden” WEP-encrypted Access Point was communicating with a “Symbol” card typically used in handheld devices that are likely used in baggage management at SFO. The baggage management system at SFO airport may easily be compromised!

Prevalent Myth – Hiding SSID is more secure than encryption

All APs are Open/WEP!
59% hotspot users are using plain text protocols such as HTTP
Only 3% are using VPN connectivity to secure their data!
Clients sending data without any encryption using HTTP are in serious danger of having their activities spied on and accounts hijacked in some cases.
Data Leakage – By Wi-Fi Users

- Users’ are leaking their Wi-Fi networking information
  - Which networks they have connected to in the past (including security settings, etc)
    - Home networks
    - Office networks
    - Hotspots

- This in turn means these Clients are vulnerable to “Honeypot” / “Caffe Latte” style attacks
“Honeypot” Attack Scenario

(1) Laptop is probing for SSIDs from your preferred list (cached).

(2) Attacker sets up an Access Point with matching SSIDs. Tools for setting this up are easily available (e.g. Karma, Hotspotter).

(3) Laptop connects to the Attacker’s machine.

(4) Attacker launches exploits to download data or gain control of victim’s machine.

- Clients who are not active hotspot user can also be attacked!
- This may already be happening, but nobody will know unless airspace is continuously monitored.
- Airports are good places to find high such high value targets!
Wi-Fi virus outbreak at the Airports

% of total Clients infected by one or more viral SSIDs at various Airports

10% of all mobile users were advertising viral Wi-Fi networks!
What are Viral Wi-Fi networks?

- Viral Wi-Fi networks are Ad-Hoc networks advertising alluring SSIDs
- Typically these SSIDs advertise “free” Internet connectivity
- Natural first choice for most naive users – after all its FREE!!!

- US Airways Free Wi-Fi
- Free Public Wi-Fi
- Free Internet!
How the Infection happens...

- Once the User connects, the Viral SSID ("Free Public Wi-Fi") gets added permanently to the User’s own Wireless Configuration
How the outbreak happens...

- Once infected, a client will broadcast the “Free Public Wi-Fi” SSID to all other clients in its vicinity.
- Thus the infected user further propagates the infection.
- Any laptop which connected to the Viral SSID broadcasted by the user in turn gets infected!
Why are Viral Wi-Fi networks such a big threat?

- Once connected to a Viral SSID network...
- All of the user’s shared folders will be accessible to every other laptop connected to the Viral SSID network
- A hacker can easily access confidential data on your hard disk
Airport authorities and Airlines need to secure their private Wi-Fi networks –

- Secure legacy Wi-Fi enabled handheld devices being used for baggage handling
- Use at least WPA for Wi-Fi enabled ticketing kiosks
- Protect the Airport IT networks against active Wi-Fi attacks
Call to Action – Wi-Fi Hotspot Users

- Do not connect to Unknown Wi-Fi networks (example: “Free Public Wifi”) while at the airport or any other public places
- Be Aware of your Windows Wi-Fi network configuration
  - Periodically inspect your windows Wi-Fi network configuration
  - Remove unneeded Wi-Fi networks from your “preferred” list
- Do not use computer-to-computer (i.e. Adhoc connectivity) while at public places such as Airports
- Business Travelers - Use VPN connectivity while using hotspot Wi-Fi networks
- Turn OFF your Wi-Fi interface if you are not using it!