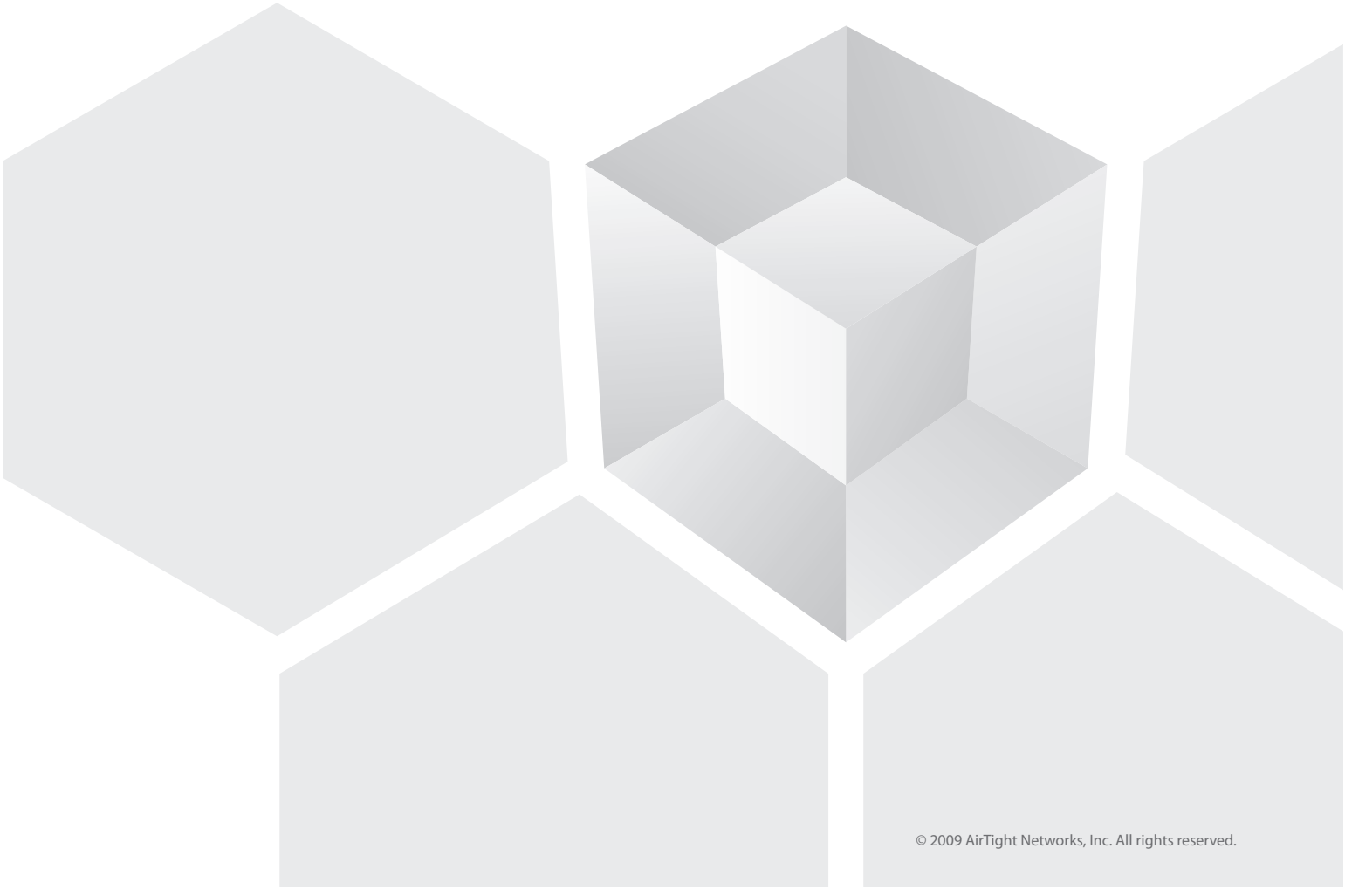
Wireless (In)Security Trends in the Enterprise

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com



WiFi is proliferating fast. The convenience of wireless access, low cost, and plug-and-play nature of the technology have been the major drivers for WiFi's popularity among home Internet users. Lately we are also seeing an increasing adoption of WiFi in the enterprise. More and more businesses are rolling out wireless LANs to cut costs and increase productivity. Today all laptops, PDAs, and smartphones have WiFi built in. WiFi hotspots, spanning coffee shops, hotels, airports, or even cities, are mushrooming to meet the growing demand of WiFi Internet access.

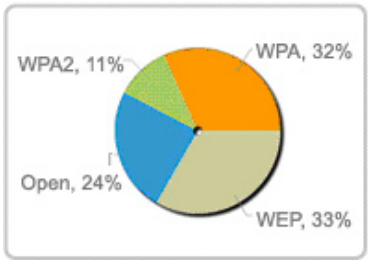
Ironically, the unlicensed frequency spectrum, low cost, and ease of use — the major contributors to WiFi's success — are also promoting its reckless use.

Like any new technology, WiFi brings with it a unique set of security challenges. The prevailing "harden-my-network-perimeter" model of enterprise network security is rooted in the common belief that "being inside (on an enterprise LAN) is safe and outside (the Internet) is unsafe." This model completely breaks down in presence of wireless. The data and the network are now in the air; the invisible radio waves cannot be confined to a building or behind a firewall, blurring the enterprise network perimeter.

A hacker does not need to physically enter a building to bypass the firewall and access an enterprise network. Sitting in the vicinity (e.g., in the parking lot or a coffee shop across the street), the hacker can simply scan the air to discover WiFi vulnerabilities in the network. No special hardware or expertise is needed — just a laptop and a WiFi packet sniffing tool available for free on the Internet.

A series of high-profile security breaches that exploited WiFi vulnerabilities in recent times reflect a serious lack of awareness among WiFi users as well as network administrators. The TJX debacle — largest security breach and identity theft conspiracy in U.S. history — is one example of what such ignorance can cost an enterprise. Other recent instances (e.g., terror email incidents in India, cyber extortion in UK) point to unsecured WiFi becoming a safe haven among cyber criminals for its convenience and the ability to remain anonymous.

To gain a "hacker's eye view" of enterprise WiFi networks and understand the common security gaps, AirTight Networks conducted WiFi security scans across business districts and airports worldwide. What we found was alarming!

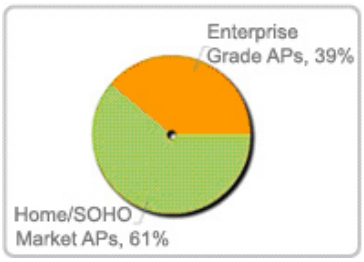


Total APs discovered: 3632

- **Official enterprise WiFi deployments are not properly configured** -- The awareness about using WiFi securely is lagging far behind the rate at which it is being deployed. This is reflected in the high percentage of APs being Open (without encryption) or using the flawed Wired Equivalent Privacy (WEP) encryption. Stronger encryption standards such as the WiFi Protected Access (WPA/WPA2) exist. Yet majority of the discovered APs continue to be vulnerable. Here is the distribution of WiFi security settings on APs discovered in six US financial districts (New York, Chicago, Boston, Wilmington, DE, Philadelphia, San Francisco) and London, UK during a WiFi scan study in early 2009.

  Open and WEP APs serve as wireless backdoors for hackers to enter the enterprise network, access local resources on the LAN, sniff sensitive data traversing the LAN and misuse Internet access without getting detected by firewalls, wired IDS/IPS, and LAN monitoring solutions.

  Often administrators configure their APs with MAC filtering and disable broadcasting SSID (name of their WiFi network). These measures only give a false sense of security. It is very easy to spoof authorized MAC addresses and to discover SSID of a network by passively sniffing over the air data in the vicinity of the WiFi network. This information is sent in clear text and nothing can stop a hacker from finding it.



Distribution of home and enterprise grade Open/WEP APs

- **Presence of home/SOHO grade WiFi APs in enterprise** -- Not only are majority of the APs vulnerable, but we are seeing a growing trend of low cost home APs being used in enterprise environments. Out of the Open/WEP APs discovered in the financial districts, 61% were home/SOHO APs.

  In some cases, IT administrators settle for inexpensive home/SOHO APs to save on costs. These APs are often limited in capabilities (e.g., security, logging) and cannot be managed centrally — increasing the chances of lapse in security. However, more often these APs are "Rogues" connected to enterprise LANs. Rogue APs are unmanaged WiFi APs attached to the corporate network without the knowledge of the administrator. They may be innocently deployed by unwitting employees looking for wireless access, or they could be maliciously placed. Most Rogue APs are unsecured. And it is not difficult to bypass physical security (if any is in place) given how small and inconspicuous (e.g., USB WiFi) many of these APs are.

  So regardless of whether your business uses or bans WiFi, it is risky to discount the presence of unknown or unmanaged WiFi devices on your enterprise network.

- **Mobile workforce is a soft target** -- The number of businesses employing a mobile workforce is growing. Mobile users empowered with WiFi laptops, smartphones, and PDAs can unknowingly expose enterprise security even when they are thousands of miles away from their workplace — waiting for their flight at the airport, sipping a cup of coffee at their favorite cafe, or accessing the Internet from confines of their hotel room.

  A WiFi security scan study of over 30 airports worldwide (US, Canada, Europe, and Asia-Pacific) exposed many inadvertent WiFi malpractices among mobile WiFi users.

  Many users continue to access the Internet over Open WiFi hotspots risking leakage of sensitive data over the air, including their identity.

  The WiFi manager software usually maintains a list of preferred networks or SSIDs — all WiFi networks that a handheld or laptop connected in the past. Unless the unused SSIDs are removed from the list, the WiFi device will continuously broadcast messages in the air searching for those WiFi networks. A hacker can easily set up a fake network with the SSID that a victim device is searching for, and automatically establish a connection. Once a connection is established, the hacker can use a variety of tools to scan the computer for known vulnerabilities and exploit them, possibly gaining access to the hard disk.

  A hacker can similarly exploit a user's computer by tapping into a "Viral WiFi network." Users commonly connect to untrusted WiFi networks, especially with enticing names (SSIDs) such as "Free Internet WiFi." On connecting to these SSIDs, commonly called "Viral SSIDs," the user does not access the Internet, but instead forms an ad-hoc network (direct computer to computer connection) with nearby WiFi computers. The viral SSID gets added to the user's preferred network list and the user's computer starts advertising itself as a WiFi network with that SSID inviting connections from other users. All this happens without the knowledge of the user.

  Group of seven computers found to be part of a Viral WiFi network during a five minute scan at a US airport.

```
-----------------+-------------------+-----------------
 2:19:d2:0:0:2e | 0:13:2:5b:35:8e   | Free Public WiFi
 2:19:d2:0:0:2e | 0:4:23:90:de:6a   | Free Public WiFi
 2:19:d2:0:0:2e | 0:1b:77:a8:b1:88  | Free Public WiFi
 2:19:d2:0:0:2e | 0:16:ce:37:2:28   | Free Public WiFi
 2:19:d2:0:0:2e | 0:9:2d:ce:e6:c8   | Free Public WiFi
 2:19:d2:0:0:2e | 0:17:f2:e8:65:95  | Free Public WiFi
 2:19:d2:0:0:2e | 0:1f:5b:5f:ea:ec  | Free Public WiFi
(7 rows)
```

Wireless (In)Security Trends in the Enterprise

ABOUT AIRTIGHT NETWORKS

AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry's leading wireless intrusion prevention system (WIPS) and the world's first wireless vulnerability management (WVM) security-as-a-service (SaaS). AirTight's award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 11 U.S. patents and two international patents granted (UK and Australia), and more than 25 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit : www.airtightnetworks.com

Wireless Security Recommendations

- Use strong encryption (WPA2) and authentication (802.1x based) for your enterprise WiFi network.
- Conduct periodic WiFi scans to gain visibility into your airspace. Watch out for and get rid of Rogue APs on your network. Use WiFi scanning tools that allow you to automatically detect and physically locate Rogue APs.
- Use a wireless intrusion prevention system (WIPS) if you need automated 24x7 WiFi scanning and complete proactive protection from all types of wireless misuse and hack attacks.
- Educate your mobile workforce about endpoint security best practices such as the use of VPN over Open WiFi hotspots. Consider use of an end-point WiFi security agent for enforcing corporate security policies at work, home, and away.

Conclusions

WiFi has become a mainstream technology offering great benefits and efficiencies but carrying with it unique security challenges. Unsecured WiFi provides an easy target for hit-and-run style attacks allowing hackers to cause severe damage while remaining invisible and undetected. Ignoring the specific requirements for securing their enterprise network and users against WiFi vulnerabilities, businesses risk loss of confidential data, legal fines and penalties, and brand erosion. By following WiFi security best practices and using the right tools, enterprises can reap the benefits of WiFi while protecting their IT infrastructure from WiFi threats.

Interesting links:

http://www.airtightnetworks.com/airport-wifi-study
http://www.airtightnetworks.com/finance-wifi-study
http://www.airtightnetworks.com/secure-wifi-enterprise
http://www.airtightnetworks.com/secure-wifi-home

The Global Leader in Wireless Security Solutions

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 **www.airtightnetworks.com info@airtightnetworks.com**

AirTight® NETWORKS