

Access on the Road: Putting Hotspot Security to the Test

*A Core Competence/Farpoint Group
Technical Note*

Document FPG 2006-328.1
August 2006



Executive Summary

We recently went into the field to test security on a number of public-access wireless-LAN (WLAN) systems. Our objective was to evaluate how well different networks provision security, and to evaluate the real-world information-security threats that business travelers face today. Our key findings include:

- The risks of using public-access networks, wired and wireless, at a hotel or similar venue are significantly greater than those experienced at home or in an enterprise setting, warranting additional precautions and procedures.
- We tested and evaluated these risks by visiting more than two dozen hotels and examining the security behavior of their public-access network installations. A large variety of operators was tested.
- The quality of security implementations varied widely. All of the top-performing sites were operated by either iBAHN or T-Mobile.

We outline a number of steps that users can take to protect themselves in the *Conclusions* section, below.

Introduction

Like most business travelers, we enjoy the convenience and speed of (especially wireless) broadband Internet access at hotels, and would be hard-pressed to do without them. But, as network and security professionals, we also appreciate the risks associated with open wireless hotspots and unsecured Ethernet connections. While appropriate safeguards can render hospitality broadband connections safe for business, many users unfortunately place their systems and data at risk through careless use of hotel and other public-access broadband services. Via a set of field tests conducted during February 2006, we attempted to assess that risk from a number of directions, and our findings and recommendations are the subject of this Tech Note.

Risks: Known and Unexpected

Vulnerabilities associated with hospitality-provided broadband services run the gamut from common Internet pitfalls to more subtle exposures that put unsuspecting users at risk. Many hotspot visitors know about Wi-Fi eavesdropping, for example, and some protect their data using convenient SSL and other VPN tunnels. These measures are extremely helpful, but unfortunately incomplete. Devices that use shared LANs -- whether wired or wireless -- leak many unencrypted packets, including LAN broadcast and multicast traffic (e.g., NetBIOS announcements, DHCP and ARP queries) and Wi-Fi management frames (e.g., Deauthenticates, Disassociates). Login and VPN set-up messages may also expose values of interest, including company names, portal URLs, gateway addresses, and user identities. This infor-

mation can be used to attack LAN users and corporate resources.

For example, hotel broadband users often expose server applications and stored data to other devices connected to the same wired or wireless LAN. Sharing folders, printers, desktops, and other services can be useful on private home or office LANs, but doing so is inappropriate on a public access LAN, where unseen peers could be colleagues, competitors, or outright attackers. Many notebooks fail to differentiate between these environments, announcing themselves to everyone on the LAN and replying to stranger's requests. Hotels can thus be excellent venues for those interested in stealing confidential data from business travelers.

Most private LANs use network firewalls to defend trusted insiders against Internet-borne attacks. This is not necessarily true in hotel broadband LANs, where topologies and security practices vary widely. For example, some use private IP addressing, while others assign each user their own public IP address to facilitate VPN tunneling. Users may assume they are insulated from outsiders, but really have no idea whether any firewall lies between their notebook and the Internet. Notebooks that do not firewall themselves or that use certain applications that open holes in firewalls could thus be exposed to intrusions from the far side of the Internet.

User carelessness and Wi-Fi promiscuity also make hotels an obvious target for stealthy wireless attacks. By default, Wi-Fi devices will connect to any access point or ad-hoc peer. Those configured to seek out preferred networks will automatically connect to any device with the specified network name (SSID), authentic or not. Attackers can thus lure hotspot visitors into automatically connecting to phony "honeypots" – sometimes called "evil twins" – that advertise common residential or hotspot SSIDs. Users who fail to detect a honeypot may fall victim to look-alike login portals that steal credit cards or man-in-the-middle attacks that intercept supposedly-protected SSL or SSH sessions. Business travelers willing to connect to any network that offers "free Internet access" are especially vulnerable to such attacks – it is literally impossible to tell the good from the bad in this case.

Road Tested

While these challenges can appear on any hotel broadband network, security measures and best practices can mitigate these risks. To more concretely assess the current state of hotel broadband security, and what countermeasures are most appropriate, we decided to test the broadband services at two dozen hotels that offer both wired and wireless Internet access to business travelers.

Venues in three large cities (Philadelphia, New York, and Washington DC) were selected to yield a representative mix of business hotels and network operators. We focused on hotels that make Internet access available to visitors in public areas: typically lobby Wi-Fi and business center Ethernet. We also used guest room Ethernet, increasingly common in business hotels, in one-quarter of our venues.

Our primary goal was to determine whether a notebook computer connected to a hotel Wi-Fi hotspot is:

- Necessarily vulnerable to Wi-Fi eavesdropping
- Accessible to other local Wi-Fi users
- Accessible to remote Internet intruders, and
- Accessible to other local Ethernet users, and vice versa.

To answer these questions, we ran identical tests at each hotel, covering the four scenarios illustrated in Figure 1 - (Test #1) Wi-Fi to Wi-Fi, (2) Remote to Wi-Fi, (3) Ethernet to Wi-Fi, and (4) Wi-Fi to Ethernet.

All tests were conducted between our own tester and target notebooks. We did not probe other users, nor did we explicitly try to analyze their data. Our tester used standard Windows XP clients (e.g., ping, arp, net use, ftp, telnet, mstsc, Internet Explorer, Network Neighborhood) and popular shareware (e.g., nmap, Super-

print.). To find Access Points and analyze our own traffic, we used Ethereal, AirMagnet, and AiroPeek. These readily-available, easy-to-use tools were chosen to represent common threats - - if our target proved vulnerable to these simple probes, more sophisticated attacks (many easily available as freeware on the Internet) could no doubt leverage those exposures.

We applied a similar rationale when outfitting our target. Standard Windows XP and IIS services opened listening ports probed by our tester. Files, web pages, interactive prompts, and PC attributes returned to our tester indicated when the target was accessible. Although we hope that hotspot users configure their own notebooks to counter such threats, our goal was to quantify the security capabilities provided by hotspot and business-center LANs. In hotspots with Wi-Fi Protected Access (WPA), we analyzed target sessions with and without WPA to assess the traffic exposed to eavesdroppers in both cases.

To ensure meaningful results, target and tester logged in as required by each network, paying for service, confirming Internet access, and determining IP addresses. Where tester and target shared a subnet, we probed the target's private address (bound to the target's MAC address where needed to bypass ARP filters.) Otherwise, we aimed our tester at the target's unique, routable public address where available. We used these known addresses to avoid probing other users, but could have easily analyzed LAN captures and scanned IP ranges to identify potential targets.

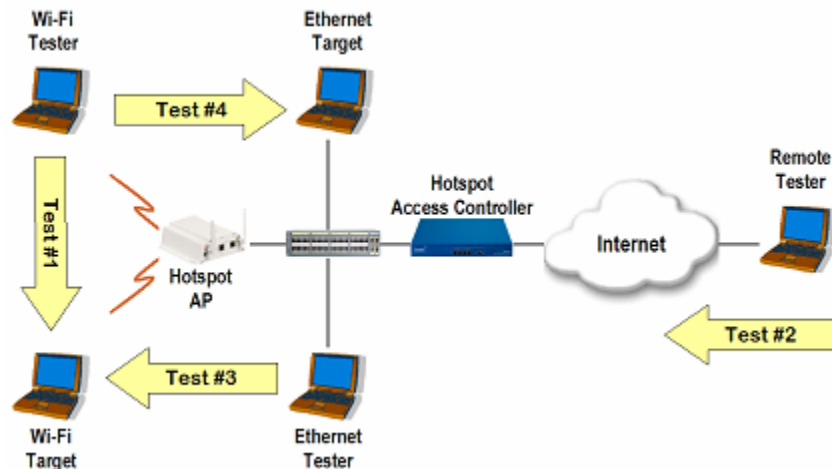


Figure 1 - The four test scenarios explored at each venue. *Source:* Core Competence/ Farpoint Group.

Lessons Learned

We ran tests to completion in 24 of 27 hotels that we visited, including six free Wi-Fi hotspots. We tested three independent hotspots. The rest were operated by Guest-Tek, iBAHN, Passsym, Starwood, TurboNet, StayOnline, T-Mobile, or Wayport. Guest room Ethernet access was provided by iBAHN, Passsym, and Wayport. Business center and lobby Ethernet access ranged from self-service kiosks to staffed cubicle cable drops, and were frequently unaffiliated with the hotel's Wi-Fi hotspots.

After digesting test results, we rated each site, based on whether tester access to our target's exposed files and services had been blocked in all, some, or none of our tests. As expected, wireless eavesdropping was possible everywhere. But we reserved our highest grade for those sites that blocked all notebook probes *and* offered a WPA option.

Overall, hotel broadband security varied quite a bit, from wide open to relatively tight. Just one in four sites could prevent wireless eavesdropping and block all notebook probes. At three more hotels, the only vulnerability encountered was NetBIOS browsing in an unaffiliated business center. All of the top nine sites were operated by iBAHN or T-Mobile.

Our bottom nine hotels left Wi-Fi users largely on their own for security, with extensive or complete notebook file and service exposure. Contrary to conventional wisdom, our Wi-Fi notebook was just as likely to be reachable from the Internet or Ethernet as it was to be reachable over Wi-Fi. This may be due in part to attention paid to Wi-Fi security over the past few years, as well as lax security in business centers. Although our sample size is limited, our results suggest that external reachability is not uncommon.

We easily reached our Wi-Fi notebook's files and services from the Internet at four hotspots, including one where our target chose to be assigned a public IP. When given the option, many VPN users choose public IPs to facilitate tunnel establishment and receive keep-alive or re-key messages. Fortunately, VPN clients are routinely paired with host firewalls to deflect Internet attacks. But other hotspot users might be unpleasantly surprised to discover they are reachable from the Internet.

We accessed our Wi-Fi notebook's files and services from a local Ethernet connection at five hotels. Given our Internet results, this is not surprising. Where Wi-Fi users have unique public IPs, there may be little difference between Ethernet and Internet hosts. But we also encountered cases where Wi-Fi and Ethernet users were located behind the same gateway or firewall, protected from the Internet but not from each other.

We accessed our own notebook's fileshares at eleven sites. At several, NetBIOS browsing was the only noteworthy notebook access. However, Wi-Fi NetBIOS access was not as common as anticipated. Ethernet LANs were more likely to expose NetBIOS shares, including many with names that suggested local ownership (e.g., business center printers, staff PCs).

We expected paid networks would protect users from each other or Internet attacks more often

than free hotspots, but this was not the case. Several free hotspots had noteworthy exposures, but so did paid networks, including the most expensive sites. As expected, we did encounter more diversity among free hotspots than paid networks. We never knew what to expect from a free hotspot -- each was a new adventure. Networks operated by known providers were not identical, but they were largely consistent.

We also found that WPA support is growing, but is far from common. iBAHN and T-Mobile were the only hotspots we could find that offered this option. VPNs and SSL can also prevent eavesdropping, but WPA does so while avoiding multicast / broadcast leakage and helping users identify honeypot APs. WPA is *not* a substitute for VPN or SSL; rather, it fills in these local LAN security gaps, and we consistently recommend it as the base-level wireless security that should be used by everyone, all the time.

At every hotspot, we saw our target send Wi-Fi data as cleartext, including DHCP requests, DNS queries, NetBIOS name broadcasts, SSDP discovery broadcasts, IGMP multicasts, and unicast application messages. At every hotspot where we were able to use WPA, all Wi-Fi data was encrypted after 802.1X authentication. We did not see our target leak any of the above-mentioned traffic. We also saw our tester verify the hotspot server's certificate using EAP-PEAP (iBAHN) or EAP-TTLS (T-Mobile.)

On the other hand, we observed that user error can cause leakage. When using Windows XP to connect automatically to iBAHN hotspots, our target occasionally connected to the hotspot's open SSID instead of the WPA SSID. When using T-Mobile's connection manager, prompts made it easy to re-connect to that hotspot's open SSID, and there is no option to disable open connections. Users must be aware of WPA and exercise care when connecting to stay safe.

Conclusions

From Wi-Fi eavesdropping to Ethernet fileshare browsing to Internet probes from afar, we found it all too easy to steal our target's documents and data. Clearly, many hotel broadband networks are still not inherently secure. These tests, while sampling just a small fraction of US hotels offering Internet access, demonstrate that consumers should take pro-active steps to protect themselves when using such networks, and to look for services that provide the security protections we have discussed in this report.

We firmly believe that users can protect themselves against these and other attacks through sound notebook configuration, personal firewalls, VPNs, SSL-protected websites, and host intrusion detection. Users who take steps to defend their notebook and data should also use secure hotel broadband networks. Doing so can help avoid accidental file sharing, LAN broadcast announcements, and man-in-the-middle honeypot attacks. To get started, we recommend the following hotspot security measures:

- Disable or block file sharing (and all other network services) on interfaces used for broadband access

- Enable Windows Firewall or (preferably) install a third-party personal firewall
- Use file encryption, available in Windows XP Professional and other products
- Choose non-obvious passwords to deter notebook, data, and server access
- Use a VPN or encrypted mobile application, ideally with two-factor (hardware or biometric) authentication
- Choose public Wi-Fi access that provides enhanced security services
- Connect only to known SSIDs, using WPA/802.1X to verify the server's certificate
- Disable ad-hoc mode and automated connection to non-preferred SSIDs
- Use a host intrusion detection agent to detect/prevent risky connections, including bridging between wireless and wired interfaces.

In summary, "free broadband" isn't a good value if it is insecure; the potential risk – and resulting cost – to business travelers can be significant. Our tests demonstrated that risks inherent in (likely most) hospitality broadband services are very real and must be taken seriously. Fortunately, users can mitigate these risks through defense in depth: look for inherently-secure networks, take advantage of security options where offered, and always defend yourself with remote-access security measures.



Chester Springs, PA 19425
610-458-7106
www.corecom.com
lisa@corecom.com



Ashland MA 01721
508-881-6467
www.farpointgroup.com
info@farpointgroup.com

The information and analysis contained in this document are based upon direct research and publicly-available information sources that are believed to be correct as of the date of publication. Core Competence and Farpoint Group assume no liability for any inaccuracies which may be present herein. Revisions to this document may be issued, without notice, from time to time.

Copyright 2006 — All rights reserved

Permission to reproduce and distribute this document is granted provided this copyright notice is included and no modifications are made to the original.