

Securing Enterprise Access via a WIFI Hotspot

By Mark Emmett

Planning The Trip

There is no denying the usefulness of wireless LAN technology, also referred to as WIFI, in the world today. At record speed more and more consumer and business devices continue to go wireless. WIFI hotspots, those free or pay-for-use wireless access points available at cafés, transportation centers, bookstores, conference centers, hotels, and until recently, in some cities, even the payphone down the street, are likewise becoming ubiquitous. Considerable productivity and business enablement gains can be easily attained by using WIFI. Despite WIFI's past growth and acceptance, an almost shameless lack of attention to security had typically been given during the development and implementation of many of the wireless products and systems seen on the market. Accordingly, the use of WIFI in business has come with sizeable risk, primarily because of natively weak security, poor interoperability between vendors, and lack of proper planning prior to moving WIFI into production environments.

Loading Up The Car

Today, there is a better story to tell in regards to WIFI security. Important improvements have increasingly been appearing in the form of new security-enabled products and field upgrades. With the final acceptance of the IEEE 802.11i amendment last year, the stage is set for rapid improvement in open-standards based technology becoming available, bringing secure wireless environments to a much higher level. Enhancements such as port-based access control, dynamic keying, message integrity checks, secure roaming, and AES support are now available to remedy the initial security shortcomings found within the original 802.11 standard.

Helping to push WIFI security awareness to the forefront has been the fact that in the business world the idea of information protection is no longer the distant cousin that no one remembers to invite to the family reunion. The concepts of firewalls, intrusion detection and prevention, VPNs, user and group rights and permissions, data protection, policies, and strong authentication are becoming commonplace throughout industry. While users may not enjoy the corralling of access these security features permit IT organizations to wield, for the most part they have come to accept them as necessary and integral parts of communicating in today's business world. WIFI is no different from most network access methods in that it is made or broken based upon a combined formula blending ease of use and effective security.

The Open Road

Even with these recent advances, the vast majority of WIFI hotspots are void of any safeguarding or policing, mainly because of ease of use

arguments, continuing to make them especially hostile environments to the mobile user. Do not look for this to change significantly in the near term. Yet slowly some hotspot providers are starting to help the situation by introducing a-la-carte security offerings to their patrons, either in the form of a pay-for-security-to-the-access-point service or through an SSL connection to a wired proxy server. As an example, T-Mobile actively promotes optional WPA support, which also incorporates 802.1x authentication, for connecting to its hotspot service. Hopefully, we will continue to see other WIFI service providers following suit with similar offerings and an eye towards securing their services.

Still, these much needed security enhancements, while a boon to consumers, do not address the more stringent requirements of the business community in terms of wireless remote access, specifically from WIFI hotspots. The need to always have a private, authenticated and unabridged transmission path should not be open to compromise. As this requirement cannot be guaranteed from the perspective of a hotspot, it is up to the organization to make sure this requirement is met in other ways that are under its control.

Avoiding Breakdowns

As with similar technological endeavors it is possible to remediate, but not entirely remove, hotspot security weaknesses to create an acceptable risk through a combination of due-diligence, hardened company-managed clients, encryption, authentication, policy adherence, and monitoring. Do not lose sight of the fact that while some changes enhance your overall security posture when using a hotspot, usability of the host can often times be greatly impacted. If wireless modifications or improvements to the client device are unable to be used consistently across the enterprise, look instead at applying them to group or specific service/application types where feasible. At a minimum any organization can create access policies and perform user training, no matter how informal. Many of the recommendations mentioned below also build upon one another. One modification alone may not create a large sway towards better security, yet two or three of them coupled together can create substantial improvement. Finally, while a few of these recommendations are specific to the various Windows clients, the approach can be applied to other operating environments. This list is ordered by importance.

1. **Policy Creation.** It is impossible to effect lasting change without knowing where you are and where you ultimately desire to be. Policies, guidelines, and step-by-step procedures are the road to wireless security salvation in an organization. If company policies addressing remote access—specifically wireless remote access—exist,

then the first and most important step has already been completed. Making sure these policies are enforced and refreshed on a regular basis are requirements for continued usefulness. If such policies do not exist then there is an immediate need for their creation and final acceptance by corporate management. In these cases a remote access policy delineating acceptable client systems or types, password and authentication requirements, privacy, end user training intervals, etc., should be developed. A separate section within the remote access policy or a standalone policy itself referencing wireless access should also be authored. WIFI policy ingredients such as the requirement for a client VPN or SSL enabled access, use of a client-based firewall and anti-virus, company-only systems (if not covered by the remote access policy), and so on could be included. The decision to make two separate policies or one larger encompassing policy is the decision of the team creating them. A good rule of thumb is that the more synoptic and portable the policy, the easier it is to incorporate new information without requiring a considerable rewrite or even one at all. Any subsequent retraining of users is also lessened. Lastly, having a policy for responding to incidents is equally important if and when they occur.

2. **User Education.** Wireless technology still presents a fair amount of complexity even though it is becoming commonplace. Wireless security, with all its initial weaknesses and holes, has been patched, reorganized, and redesigned into a melting pot of old and new protocols and services. This patchwork of methodologies is still in flux at this point in time, but there are sure signs of stability. Fortunately, through a mix of common sense and standard practices, a company can create a capable security foundation upon which to build. The first brick in the foundation was the establishment of published policies dealing with the use of remote access, specifically including wireless networking as the transport. The second step to adding to this foundation is educating and training the organization not only about the policies as they are written but why they are necessary, how to carry them out successfully, how to identify dangerous environments, and the consequences to the company and ultimately themselves for knowingly subverting them. Short, focused, and mandatory training sessions are adequate when delivered in person, in print, or online. Incorporating this training into new employee orientation, especially for mobile staff, would be the most effective method, before bad habits begin. This also forces IT to have its act together by making sure policies and materials are already in existence. Tying policy education to the dissemination of a token or remote access account would be another way to ensure the training was given to the user. With the increased security offerings we are starting to see from hotspot providers, there is going to be an increased burden on the user, and the IT department if vendor specifications are not known in advance, to make those client security changes on the fly. Altering one's wireless network settings, if the company chooses to permit it, may be no cause for concern to the real road warriors, but the casual traveling office worker may encounter a whole host of issues attempting to modify their network settings. Training users in advance and providing one-page cheat sheets for common hotspot scenarios can go a long way in helping users maintain the security of their system, and that of the enterprise, by taking advantage of better security offerings by the hotspot providers.
3. **IPSEC/SSL VPN.** As the link between the client and a hotspot access point is out of a company's control and usually absent of any

capable authentication or protection, the best solution is to provide a secure transport all the way from the client to the enterprise. Using an IPSEC VPN is still the most effective way to accomplish this. Most major VPN vendors also offer special clients for devices running Windows CE. PPTP can also be an option for Windows CE clients beginning with version 3.0 though PPTP does not afford the same benefits as IPSEC. Alternatively, for pocket PCs or PDAs, an organization can look into using Certicom's Movian VPN client, though free downloads of this lightweight client stopped in October 2004. No matter the client, split tunneling, if available, should be disabled, forcing all traffic across the encrypted tunnel. Disabling split tunneling will also reduce the amount of the analyzable traffic being sent over the link should one connect to a rogue access point within the hotspot area. AES encryption is available for most commercial VPN products today to match the encryption level supported by WPA. An SSL-enabled service or application is a viable alternative to a full IPSEC client in the case where a clientless solution is needed or offered.

4. **Client Firewall.** WIFI is a shared medium allowing clients within the same collision domain of the hotspot to be seen and immediately reachable to each other. As mentioned previously, this situation is outside of the auspices of the enterprise. Accordingly a protection mechanism should be provided to the client device, where possible, to protect against potential threats. Client or personal firewalls can provide this capability. An additional option for Windows XP clients is to use the integrated firewall that became available with the release of service pack two. However, commercial firewalls tend to have more features and scale better in a centralized IT environment. Many of the client firewalls today also integrate tightly with anti-virus, security agent, and VPN software. Choosing an integrated application suite can save costs as well as time lost to redundant configurations, vendor incompatibilities, and having to learn more than one application.
5. **Local Administrator Rights.** In many organizations end users are given local administrator rights to their company-assigned laptops and/or desktops. This may be necessary based upon the operational requirements of specific applications or for some other administrative purpose. This need should be evaluated carefully with options for alternative solutions, such as a group policy for changing wireless network properties, investigated at the same time. In established environments the reasoning behind granting users such broad administrative rights is frequently that it has "always been done that way" or "it's easier." From a security standpoint, having users with these rights creates unnecessary or even unacceptable risks. Users are permitted to disable or remove company-mandated software such as firewalls, VPN clients, anti-virus, or other security agents, change important system or network settings, and install with—or without their knowledge in case of malware/spyware—potentially harmful and unauthorized software. These settings and software are all critical elements of maintaining secure hotspot communications. Operating without them in place, or having users change how they function, can have a detrimental effect on the enterprise when this supposedly trusted but now compromised system reconnects to the internal network.
6. **Logfile Auditing.** This activity should really go without saying if the enterprise is at all security conscious. Remote access traffic should be monitored routinely by IT and at a higher level of inspection than normal with interesting traffic entries being investigated.

Correlation with other logs and system activities involving the wireless client(s) should be done in parallel as warranted. An added benefit to analyzing wireless client traffic is that adapter misconfigurations, disabled security applications, and unauthorized software on the client can frequently be detected before they are able to be exploited. Separate Wireless IDS and IPS products also exist which look for traits and footprints unique to WIFI.

7. **Wireless Network Type.** By default a Windows XP/2000 wireless adapter configuration allows the connection to two different types of wireless networks, access point (infrastructure), or computer-to-computer (ad-hoc or peer). The infrastructure network type is the most common, whereby a system associates to an access point which in turn connects into a wired network. This is the only network type that should be selected unless there is a specific and controlled need for computer-to-computer connectivity. The ad-hoc type allows peer-to-peer associations between systems with no access point required, though an SSID is necessary and WEP can still be used. As with the infrastructure network type there is no default authentication requirement. Once two or more systems are connected, which can occur without the other knowing in real time, then the path for file sharing or piggybacking has been created. If ICS or file sharing are enabled, this has become a serious risk to the enterprise.
8. **Automatic Connections.** Another setting that should be verified as disabled within the Windows wireless adapter configuration is the setting to automatically connect to non-preferred wireless networks. Many access points in existence use default or common broadcast SSID's such as "default," "wireless," "public", or in regards to hotspots the hardware or service vendor's name. While using such identifiers are often seen as acceptable in a confined location or controlled setting, it can be very problematic in a malicious situation or in congested airspace with multiple SSID advertisements being broadcasted. As an example, when an SSID of "default" is used with automatic wireless connections enabled, two scenarios could easily arise. First, if the system is out of its normal wireless network environment (such as at a hotel or client office), it would impulsively associate without user intervention to an open wireless network which was configured with the same common SSID. The second situation occurs when the system has been set up in a location where two or more access points with the same SSID, each connected to different backend networks but slightly overlapping in their coverage areas, are active. Assuming these access points are unsecured and using DHCP, which many hotspots are, the casual user would most likely have no idea to which access point they have associated to and, subsequently, whose network they are on or what their system is being subjected to. Malicious tools thrive in this type of environment.
9. **File Sharing.** The sharing of local drives on a system is not recommended and this should be turned off where possible. It is a simple task to have unrestricted file sharing from the root directory down enabled on a system. In many cases sharing could be enabled with active mappings between other systems without the user having any knowledge of it.
10. **IP Forwarding.** This feature is disabled by default in XP/2000 and should remain that way, preventing the routing of traffic through the system itself. This is attainable if a system has a wired adapter and wireless adapter connected simultaneously. It is not usual for a user to forget that their wireless adapter is still

active and possibly associated to an access point even though they believe they have stopped using their wireless connection by "going wired."

11. **Internet Connection Sharing.** ICS should also remain disabled based upon the same reasoning for the disabling of IP forwarding. ICS allows a host system to act as a form of proxy for other systems connected to it, such as with the ad-hoc wireless network type, enabling those systems to route out to the Internet using NAT, or anywhere the hosts default gateway will send the traffic. As long as a system has two network interfaces and access to the Internet, it can act as an ICS host.

Another option if you are not tied to a deadline is to play the waiting game for as long as you can, letting products and technologies mature, become widely deployed (or not) and verify if interoperability has been achieved. Adhering to IEEE standards and IETF recommendations for your wireless hardware and software deployments should aid an organization with this. Getting stuck in the rut of proprietary products and non-standard "enhancements" will can cause incompatibilities, limit flexibility, give life to never-ending support headaches, potentially force the disablement of important security features, and almost certainly result in a loss of user confidence. You'll have invested copious amounts of dollars, time, and resources and be worse off than when you began. If you must be an early adopter then try to stay with one vendor's suite of products though this is improbable in a hotspot scenario.


Arriving At The Destination

The recommendations provided within this article, used to comprise a defense-in-depth approach, should be in place before a company publicly condones hotspot remote access to its user population. Omitting any one of these could result in the eventual failure to reduce the company's risk, letting remote WIFI access remain one of the weakest links in an enterprise's overall security profile. It is the responsibility of the enterprise to protect itself across the entire transmission path when allowing users to connect back into the internal networks and services of the corporation over a wireless medium. The investment an enterprise must make today on managing and controlling its wireless access stance, be it internal or external, allows them to take advantage of all the benefits the freedom WIFI offers in addition to positioning them securely for the future of this burgeoning market. One will also notice that most of the recommendations here are useable, in theory if not in practice, for all types of networked devices, not just those in the wireless arena.

If your client wireless setup does not yet support WPA, you may only need a firmware upgrade for your hardware and/or a software patch or driver to rev up your software. WPA2 may require new hardware to be purchased for both the client and access point ends of the WIFI connection.

Remember that one area in which WIFI still has susceptibility, despite the ratification of 802.11i, is in regards to denial of service attacks. Just about everything else in the networking world is still vulnerable to a DoS, so the fact that WIFI is affected as well should not be much of a standout. Security tools used to squelch DoS or DDOS attacks on wired networks can also be used effectively in the wireless world. However, it is difficult to discern if a hotspot provider has employed any of these countermeasures.

Remember Why You Went In The First Place

At the end of the day the notion that a single breach of the company's security defenses is far more expensive than implementing and maintaining a security plan, of which a wireless remote access is an integral component, is still very much true. Like most things related to information security, the design, purchase, and installation of a product or tool are the easiest and most reasonable pieces of the overall effort. It is in the integration, ongoing support, and monitoring where the challenges can emerge. When considering hotspot remote access, make sure you have planned and prepared in advance of providing the user community the means to connect into the company over public WIFI. Be sure to re-evaluate your approach on a scheduled basis as this technology is rapidly and continually changing. Every environment is different, but WIFI can be secured and the benefits of this technology only continue to grow. 

Mark D. Emmett, CISSP, CISM, is an information security consultant in the Boston area specializing in network and security architecture design. He also holds the CCDP, CCNP, and CCSP certifications.

IEEE 802.11 Standards
<http://standards.ieee.org/getieee802/802.11.html>
IEEE Standard 802.1X-2001
<http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>
IETF RFC 3748—EAP (Used by WPA authentication)
<http://www.ietf.org/rfc/rfc3748.txt>
WIFI Alliance (For WPA/WPA2 information)
<http://www.wifi.org>
Windows XP Update for WPA (Included in service pack 2)
<http://www.microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en>
Windows XP Update for WPA2 (Requires service pack 2 to already be installed)
<http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&DisplayLang=en>
RFC 2196 Site Security Handbook (See section on policies)
<http://www.faqs.org/rfcs/rfc2196.html>
SANS wireless policy template
http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf

