
By BRUCE POTTER

WIRELESS HOTSPOTS: PETRI DISH OF WIRELESS SECURITY

Laptops and PDAs are so vulnerable in wireless hotspots, users would do well to turn them off.

Achieving a truly secure connection at a public wireless hotspot is an impossible proposition. Despite the lack of security, wireless hotspots using 802.11-based wireless technology have popped up in coffeehouses, bookstores, and restaurants worldwide. The wireless protocol 802.11, better known by the marketing term WiFi, has become the mobile connectivity mechanism of choice for businesspeople, students, and everyone else. Unfortunately, even with the protocol's ease of use and accessibility, WiFi security options remain limited. The threats against wireless networks reflect the variety of users on the network; the only proven tools for adding wireless security are geared toward large-scale enterprise deployments. Smaller networks lack access to the infrastructure

ILLUSTRATION BY JEAN-FRANÇOIS PODEVIN

FOR ALL INTENTS AND PURPOSES, SECURITY AT A HOTSPOT IS UNACHIEVABLE, GIVEN THE CURRENT STATE OF THE TECHNOLOGY.

needed to secure their transmissions. For all intents and purposes, security at a hotspot is unachievable, given the current state of the technology. Fundamental changes to WiFi security protocols are needed to bring effective security to hotspot users.

In order to understand how dangerous the situation is for a typical user, we must first understand the nature of the networks and the related hotspot attacks. Here, I examine the different types of WiFi networks to determine how they are built and maintained, weighing the state of the art in WiFi attacks and defense technology to understand how troubling the situation is for tens of millions of users worldwide. I also examine possible next steps for users, vendors, and WiFi service providers.

Large and complex corporate networks are a great place to begin to understand the inner workings of WiFi security. Corporate networks tend to take security seriously and as such involve some of the best tools and procedures for securing the technology and related communications. Corporations also represent a single point of trust for their employees—a critical point missing from public hotspots. Corporations can exert control over all aspects of their wireless networks—from client software, to users, to system operators—including most of the variables in the wireless security equation.

WiFi networks consist of two major components: access points and clients. Both exist in what can be thought of as a hub-and-spoke architecture. A client “associates” to an access point and sends all its traffic to it. In wired networks an association is analogous to plugging a cable from a computer into a switch or hub. Just as a switch can connect many computers, an access point can have many associated clients. An association is basically a connection at layer 2 of the OSI model (see Figure 1).

A corporate WiFi network consists of many access points, each representing an ingress point into an internal protected network and can be viewed as a

switch waiting for a hacker to connect to in order to attack internal resources. Each one may also have other corporate resources (that is, other wireless users) attached to it that also need protection. Protecting access points and clients spread throughout an enterprise is an important and difficult task.

Networks and their clients can be protected in many different ways. The primary focus for WiFi security is protecting the confidentiality of the data while it is in the air and providing authentication for the client and the infrastructure, so each knows the other is a trusted entity. The first attempt in the original 802.11 protocols (circa 1999) at securing WiFi proved weak in both respects. Developed by the IEEE, the Wired Equivalent Privacy (WEP) protocol sought to do exactly as its name suggests—provide users the same level of security

they would have when plugging into a wired network. Unfortunately, both authentication and encryption provided by WEP proved ineffective in the face of even novice attackers.

Newer wireless security standards offer much better security if set up and used properly. For example, IEEE 802.11i, a suite of three different security mechanisms, describes enhanced authentication and encryption mechanisms for WiFi networks using an authentication mechanism called the Extensible Authentication Protocol (EAP). EAP allows system designers to use whatever manner of authentication they need to secure their system. For some, this may be a simple user-name-and-password combination. Others may need much more assurance of the identity of the actors on the network; bidirectional certificate-based authentication is an option and a key method for creating secure wireless networks (see Figure 2).

With both the client verifying the identity of the access point and the access point verifying the client, attackers have difficulty pretending to be legitimate actors in the network. When a strong-enough signature algorithm and key length are used, attackers find

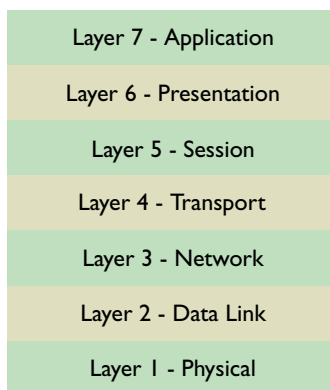


Figure 1.
OSI network
layers.

it almost impossible to impersonate a legitimate device, assuming the software that implements the certificate checking is properly coded.

The drawback of this bidirectional certificate-based authentication architecture is the difficulty of assembling and maintaining it. Clients and access points must have software that understands how to perform certificate-based authentication. An enterprise must run a public key infrastructure (or access an outsourced PKI) to handle the issuance, maintenance, and revocation of certificates. The enterprise must have a server for remote authentication dial-in user service to mediate authentication requests. If all parts are assembled correctly, the end result is that both the infrastructure and the clients are protected. However, it takes a great deal of central control and capital to make this happen. Unfortunately, even when technical expertise and money are available, the hotspot situation ends up being dramatically different.

Many enterprises employ operational procedures and tools that help protect their wireless networks. Since all components of an enterprise wireless network are part of the organization's infrastructure, the operations staff must monitor it all. This important part of enterprise networks does not exist in hotspot networks. Mechanisms like wireless intrusion-detection systems and traffic analysis continuously look for attacks against the network and associated systems. Corporations can impose configuration requirements for laptops connecting to wireless networks, ensuring that wireless clients are not attractive targets for attackers.

HOTSPOT NETWORKS

Unlike the centrally controlled model of an enterprise wireless network, hotspots are much more of a free-for-all. While hotspots use the same basic WiFi technology as enterprise wireless networks, the usage scenarios and security ramifications are completely different. Users of hotspot networks are generally looking for "any port in a storm," or access to any

network that will get them to the Internet. Such open-ended availability and access can lead to problems for both the users and the networks they join.

Unlike the cellular network, there is no common mechanism for users to access networks controlled by different service providers. For example, T-Mobile provides access for a fee to WiFi users in Starbucks coffee shops throughout the U.S. T-Mobile has its own authentication and security infrastructure, as well as its own way of assembling networks. T-Mobile's network and authentication have nothing to do with the small-town independent coffee shops that have set

up hotspots for their customers. Any security mechanisms used to protect the network of one provider generally mean nothing to users of other providers.

Only in so much as it helps keep their networks secure are service providers motivated to focus on the security of their users' systems. The first and foremost concern for providers is to protect their own infrastructure and systems.

They ensure these systems are usable to their customers by employing firewalls, rate-limiting devices, and some monitoring. They may block incoming connections from the Internet to wireless clients in an effort to keep worms and malware from affecting their customers. While this keeps malicious actors from attacking users' machines, it also helps preserve the networks of the service providers by minimizing the amount of traffic they deal with and the potential for malicious activity.

Another central issue for ensuring hotspot security is how to manage layer-2 cryptographic data. In an enterprise environment, the clients and access points are controlled by a central authority. With a hotspot, there is no central point of trust that allows for cryptographic data to be given out in a secure and scalable fashion. The configurations used by the clients connecting to hotspots are variable. Some users may have four-year-old PC laptops, some may have cutting-edge MacBook Pros. Others may be running Linux. There is no guarantee that any of these users will be able to support the most current wireless security.

Some users may have systems infected with malware, including viruses and spyware. Rather than sacrifice revenue for the sake of secure users, many service providers recommend using a virtual private network

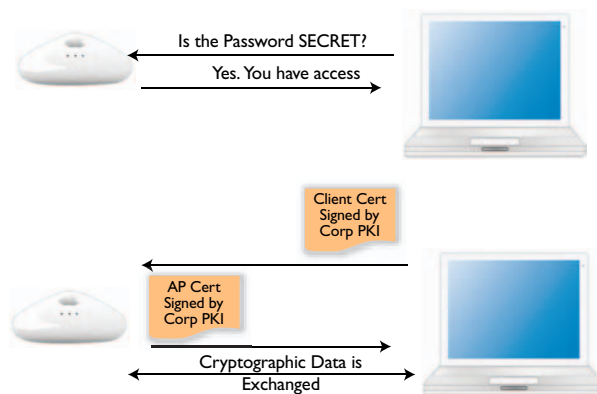


Figure 2. Preshared password and bidirectional certificate authentication.

USERS OF WIRELESS HOTSPOTS ARE ULTIMATELY RESPONSIBLE FOR THEIR OWN SECURITY.

(VPN) to keep traffic secure. Unfortunately, VPNs represent layer-3 solutions to layer-2 problems. A layer-3 solution (such as a firewall or VPN) does not necessarily mitigate attacks against layer 2.

Users of wireless hotspots are ultimately responsible for their own security. Although some tools give them enhanced security functionality when using a hotspot, the situation remains unpredictable and insecure for the majority of users. Operating system vendors and third-party software developers do not provide enough information and direction to users regarding the threats on wireless networks. The attacks against WiFi are not terribly complicated, but without tools for triggering alerts and defensive measures aimed at hotspot users, there's little these users are able to do to protect themselves.

WiFi THREATS

When users use a wireless network, they give up a foundational piece of information security: the physical layer. As outlined in Figure 1, the physical layer forms the base of the OSI model. Similarly, physical access is the core of many of the threat models used in information security. In wired networks lacking physical access to a network, the possible attacks are limited to layer 3 and above. For instance, in a normal office environment using a wired Ethernet network with IP, an attacker is not likely to be able to plug in without risk. So rather than plug in, the attacker might work through the Internet to attempt to gain access to internal systems. However, the attacker cannot execute attacks against layer 2. Even attacks that start at layer 3 (IP-based traffic) are limited due to the use of firewalls and intrusion-detection systems.

Wireless connectivity throws all this architecture

out the window. An attacker has access to layer 1 from beyond the control of a user's physical environment.

Using relatively inexpensive antennas, free software, and personal motivation, an attacker might stealthily access a WiFi network from miles away. What this means in a corporate network is that a hacker could be in the company's parking lot, a neighbor's parking lot, or on the hill across the valley launching attacks against the network.

In hotspot environments, while attackers might act from a distance, they might also act very locally. Much of the software used to attack wireless networks runs on Linux and can be deployed on small devices. Linux can be installed on several different PDAs and mated up with wireless cards. Wireless attack tools can be configured to run automatically, giving an attacker the ability to seem to be completely innocuous. A PDA can be hidden in a backpack or jacket pocket or even carried around without being noticed. However, while attackers are ordering venti lattes and blueberry scones, PDAs in their backpacks are busy intercepting data and exploiting wireless clients.

The most dangerous attack against hotspot networks targets the client computers directly by tricking them into connecting to the attacker's network. An attacker creates a rogue access point that pretends to be a legitimate access point (see Figure 3). When a wireless client attempts to associate with a network, it looks first for all the access points within it. If the client is looking to join the network COFFEE, it sends a probe packet asking to join that network. If multiple access points respond as if they were part of the COFFEE network, the client connects to the access point with the strongest signal.

Attackers wishing to create a rogue access point for the COFFEE network need only ensure that their signal is stronger than the signal of the legitimate access point. This can be accomplished through high-gain

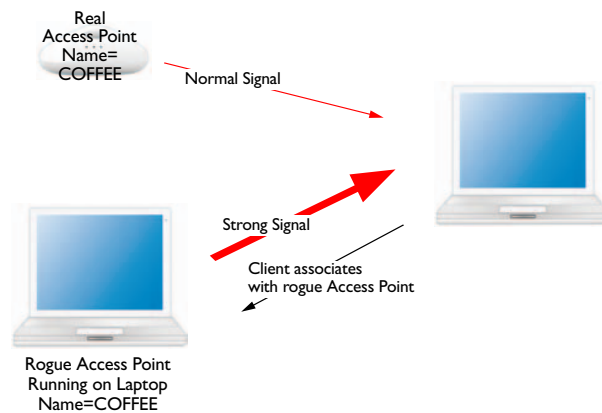


Figure 3. Rogue access point attack.

antennas or through high-power transmitters. In the “PDA in a backpack” scenario, the attacker can use a PC card in the PDA combined with access-point software running Linux to create a stronger signal, even when hidden in a bag or pocket.

Once the client associates to the rogue access point, the attacker then spoofs the rest of the network. The rogue device, having completely subverted the layer-2 connection, can cause undetected havoc at higher layers. The attacker might issue IP addresses to the client, provide bogus DNS responses, and even mask real Web sites with fake ones. Attackers using rogue access points can spoof the login screens of major Web portals (such as Hotmail, Gmail, eBay, and Yahoo) in order to gain usernames and passwords from unwitting victims.

Unfortunately for wireless clients, such an attack is difficult to detect. There is no preestablished trust between the hotspot network and the client. Lacking newer authentication techniques that are not available on many wireless clients, the client has no way to determine if the access point it is being connected to is the right one. Windows (as well as the other operating systems) provide no feedback to the user as to what is happening at layer 2.

The user is not notified if, say, a new access point named COFFEE suddenly pops up and is twice as strong as the previous access point. On the face of it, this scenario should be easy to detect. Unfortunately, few tools are able to identify the situation and send an alert. AirDefense Personal (www.airdefense.net/products/adpersonal/index.php) and other products give users a view of malicious activities at layer 2 and attempt to prevent insecure configurations from being used. Such features need to be included in the operating system to be effective for the vast majority of wireless users.

Several variations on the rogue access point attack are worth mentioning. Most operating systems, including Windows and Mac OS X, keep track of networks to which they’ve previously been connected. When the wireless interface comes online, the client begins looking for these trusted networks. If it finds one of them, the client automatically connects to it. Many users have trusted networks with guessable names (such as “home” and “wireless”). Some users never change their home network name from the default name shipped with their access point. For example, linksys routers use the name linksys by default. Attackers can create rogue access points with the names of common networks (such as “linksys” and “home”) in order to trick clients into connecting automatically. This attack is quite successful and difficult to prevent.

Another problem with using hotspot networks is that attackers can sniff traffic and communicate directly with other client computers. Many users feel that if they are running a VPN connection, they are safe from such attacks. While sniffing and direct communication are more difficult if a user has a VPN, they are not impossible. A VPN can also give a false sense of security if it is used only for communicating with a trusted network (such as a remote office). In this case, known as a “split tunnel,” the client is still sending data across the network in the clear and is likely still accepting connections from other machines.

Modern PCs are very chatty on the network. Attackers sniffing the network are probably able to find usernames, Web sites visited, personal information, and maybe even hashed passwords from instant messaging and mail programs. Rather than sending a password over the network, many applications will create a cryptographic hash of the password and send the hash. Since the hash is a one-way function, application developers feel it is a secure way of transmitting the password across the network. Unfortunately, password hashes are not as resilient to attack as they used to be. Password-guessing programs have become sophisticated, and computers have become powerful enough to quickly guess a great number of passwords. According to [1], a 3.2GHz Xeon processor can sort through more than 9,000 MD5 one-way cryptographic hashed passwords per second and 4.5 million LanMan (Windows authentication) hashes per second. Password guessing is also an easy process to parallelize; it’s so easy that many security experts consider the loss of a password hash equivalent to the loss of the password itself.

PROBLEMS WITH MITIGATION

Mitigating these problems is clearly difficult. First and foremost the 802.11 protocol is designed to make layer-2 transitions transparent to the user. While such transparency is great from a usability perspective, it is terrible from a security perspective. To avoid attacks (such as rogue access points) the core protocol must be violated, a preexisting trust relationship must exist in the form of bidirectional certificate-based authentication; otherwise, security software (such as a wireless intrusion detection system) must be added after the fact.

None of these solutions is particularly useful in normal hotspot environments. Worse, even educated users have no way of knowing if something malicious is happening on the network without using specialized wireless security software. Users have been educated over the years that when using a

secure-sockets-layer-protected Web site they must look at the URL to ensure they are at the right site and to “look for the lock” to ensure the traffic is protected. There is no analog for this activity on wireless networks. The network name is the same whether it is the legitimate network or a rogue; moreover, the user has no visual cue to look for.

Applications are unaware of the network environment in which they run. An instant messaging client or Web browser has no way of knowing if the computer it is running on is within a controlled area with a wired network or if it is at a coffee shop with a random wireless network. Attackers who subvert the wireless connection will then probably try to subvert applications running on the client system. Ideally, the applications are able to recognize differing threat environments and reconfigure themselves accordingly. Conventional wisdom with secure software architectures do not account for these situations.

CONCLUSION

For all their utility and ease of use, hotspots are dangerous places. While every coffeehouse and airport lounge may not include an attacker lying in wait for victim hosts, the fact is attackers are likely to be successful. Users in enterprise environments have the luxury of a single point of control and administration that creates “security of scale” for wireless users. In hotspots, users are on their own. Despite the availability of tools and point solutions, most users represent easy prey for sophisticated attackers.

The state of the art with respect to wireless defense is behind the state of the art with respect to wireless attack. As technologies evolve, users will become better armed to deal with the threat posed in hotspots. In the meantime, it may be better to shut the laptop, enjoy the coffee, and keep an eye on the people nearby using PDAs with wireless cards sticking out. **C**

REFERENCE

1. Amesbury, A. *Password Attack Discussion & Benchmarks*. Technical Report, 2003; www1.umn.edu/oit/security/passwordattackdiscussion.html.

BRUCE POTTER (potter_bruce@bah.com) is a senior associate at Booz Allen Hamilton, Linthicum MD, and founder of the Shmoo Group of security professionals (www.shmoo.com).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.