



Global Knowledge™

Expert Reference Series of White Papers

WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises

WPA2 Security: Choosing the Right WLAN Authentication Method

Benjamin Miller, Global Knowledge Instructor, CWNE

Introduction

Ask a hundred CIOs what three things about WLANs (wireless LANs) strike fear into their hearts, and the answers are likely to be similar: Security, Security, Security. Sure, you want good coverage. Sure, you want to minimize drops. But the only way an executive is likely to lose their job over a wireless network is if they end up like the folks at The TJX Companies, who saw millions of credit card numbers stolen from an attack that started with a breach of the WLAN.

While the TJX story was an extreme case of faulty wireless encryption, questionable data protection practices, and the Russian mafia combining to create a once-in-a-blue-moon theft, the fact is that many WLANs are vulnerable to intrusion. Even if you don't have a couple hundred million credit card numbers to protect, it's still important to choose the correct WLAN authentication method and configure it properly. This paper will explore the authentication methods available with WPA2 (Wi-Fi Protected Access 2) and identify several important best practices to consider when deploying a wireless network at home or in the enterprise.

What Is WPA2?

To have a reasonable discussion about how you're going to keep intruders off your WLAN, you have to establish an understanding of WPA2.

Those who have followed the aforementioned TJX story know that the initial wireless breach occurred because WEP (Wired Equivalent Privacy) security was in place. WEP security goes all the way back to the original IEEE (Institute of Electrical and Electronics Engineers) 802.11 standard (c. 1997). It's broken. In fact, it's not just broken. It's broken, beaten, dead, and then beaten again posthumously. It's also part of every single Wi-Fi product on the market, be it a, b, g, or n.

The actual problems with WEP are thus:

1. WEP encryption can be broken.
2. After you break WEP encryption, you can attack a network in two ways:
 - a. Use the broken WEP key to sniff data.
 - b. Use the broken WEP key to access the network.

WPA2 is a certification from the Wi-Fi Alliance for 802.11i-compliant products. The 802.11i amendment has a few security protocols that make it a strong replacement for WEP. All Wi-Fi-certified products since 2006 are required to support WPA2 as well.

WPA2 is structured a lot like WEP. When you used WEP (assuming nobody cracked your key), hackers were kept off and data were encrypted. When you use WPA2, both the network and the data are secured as well. Only this time you're using AES-CCMP (Advanced Encryption Standard – Counter-Mode Cipher-Block-Chaining Message-Authentication-Code Protocol) encryption, which has no known flaws. That means no cracking, no sniffing and, most importantly, no network access for hackers.

The Catch

WPA2 sounds great, but as with anything in life, there's a catch. Actually, two catches: You've got to choose the right authentication method that fits the scale of your WLAN. You've got to configure WLAN devices properly to plug potential holes in WPA2.

Security Begins at Home... or Does It?

To begin our look at avoiding these two potential pitfalls of a WPA2 installation, let's first look at the most common type of WLAN: the home network used primarily for wireless Internet access.

One option for security on a home WLAN is the simplest option of all: no security. Sounds radical, sure. But when examined closely, a WLAN with open authentication may be the best option.

On the surface, it seems like allowing any jibroni within RF (radio frequency) signal range to connect to your home WLAN seems like an open invitation to hackers. As the age-old analogy asks: "Would you want an open RJ-45 jack in your parking lot?" But is the answer really, "No," or, "Who cares?" In many cases, the answer is the latter. Consider what a hacker could really do if he had an open RJ-45 jack to connect with:

1. Connect to the Internet.
2. Share your iTunes library.
3. Access guest accounts on networked computers.
4. Access public directories on networked computers.
5. Execute direct peer-to-peer attacks on networked computers.

For many home WLAN users, the first four hacks listed above are somewhat victimless crimes. Sure, your ISP may dislike it if your neighbor is mooching your WLAN for free Internet access rather than ponying up forty bucks a month, but there is little impact on your day-to-day computing life when any of these four things happens. The fact is that most users wade in far more dangerous waters during their everyday Internet activities.

It's the 5th potential hack that home WLAN users have reason to be concerned with: peer-to-peer attacks. While an Internet-based hacker may be dangerous, firewalls on routers typically prevent direct peer-to-peer attacks. When a hacker connects to your WLAN, that barrier between WAN and LAN is no longer present. A hacker looking to execute a peer-to-peer attack after connecting to an open WLAN may have the potential to reach a networked computer. The real question, however, is not whether the hacker can reach your computer, but what can they do once they reach your computer?

Modern operating systems have built-in local firewalls that prevent many intrusions. By simply leaving default settings configured on Windows XP, Windows Vista, or Mac OS X, a strong personal firewall is enabled. That means even if your friendly neighborhood hacker accesses your WLAN and sees your computer on the network, they may not even be able to fire off a net send saying, "Pwned!"

The truth is that I leave my home WLAN open, and I advise all of my non-technical friends to do the same. I've seen unknown computers pop up in my iTunes sharing and I've noticed web sites that my mother wouldn't approve of show up in wireless packet captures when I've been at home, but to me that's less annoying than getting a call from my roommate at 1 a.m. east coast time asking why she can't access YouTube.

Securing the WLAN with WPA2-Personal

Leaving a home WLAN open is often the best choice for non-technical users. But let's face it; the audience of this paper is not non-technical users. Technical users tend to be more adept at handling security on their wireless routers. Therefore, for technical home WLAN users, WPA2-Personal is the security method to choose.

WPA2-Personal provides two important security measures. AES-CCMP encryption protects wireless data and PSK (Pre-Shared Key) authentication keeps hackers off the WLAN.

While it is certainly important that AES-CCMP encryption prevents sniffed packets from being of any use to a hacker, the real meat of WPA2-Personal is PSK authentication. PSK authentication involves configuring a passphrase of 8 to 63 characters on each wireless station (laptop, phone, PDA, etc.) and the AP (access point). There are several aspects of this design that are attractive to home users:

1. **Encryption tied to authentication:** Enabling PSK authentication automatically enables AES-CCMP encryption. There is no separate encryption key to manage.
2. **Security on the AP:** By keeping security on the wireless devices there are no servers to manage.
3. **Single credential security:** Managing a single passphrase is often easier than having to document or remember unique passwords for each user.
4. **Built-in passphrase strength:** 8 characters may not sound like a lot, but it takes a text file of about 1.9 TB just to store all possible lowercase letter combinations.

The Fine Print

Using the PSK as specified in WPA2-Personal is the recommended WLAN authentication method when securing a home WLAN. But there is a catch. If a hacker is sniffing wireless packets at the exact time you connect to the WLAN, they can launch a dictionary attack against your PSK passphrase.

A dictionary attack is where a hacker runs software – in this case, applications like coWPAtty, aircrack-ng and KisMAC – that replicates your PSK authentication offline against a wordlist (text file) of potential passphrases. If your passphrase is in the wordlist, then the attack will be successful.

Though dictionary attacks are a real threat to WPA2-Personal WLANs, it should be emphasized that the hacker's wordlist must contain the correct PSK passphrase. Now, if my passphrase is "wireless," then there are dozens of wordlists that are freely available online that will allow a hacker to crack my passphrase. But if my passphrase is "w1r<le55", then cracking is darn near impossible. Choose "ae\$*&JNjde8(@#JCF(#\$.-*7" as your passphrase, and the hacker has a better chance of walking on the moon than surfing on your WLAN.

The point here is that if you're going to use WPA2-Personal to secure your home WLAN, then do it right by choosing a strong PSK passphrase.

The Enterprise

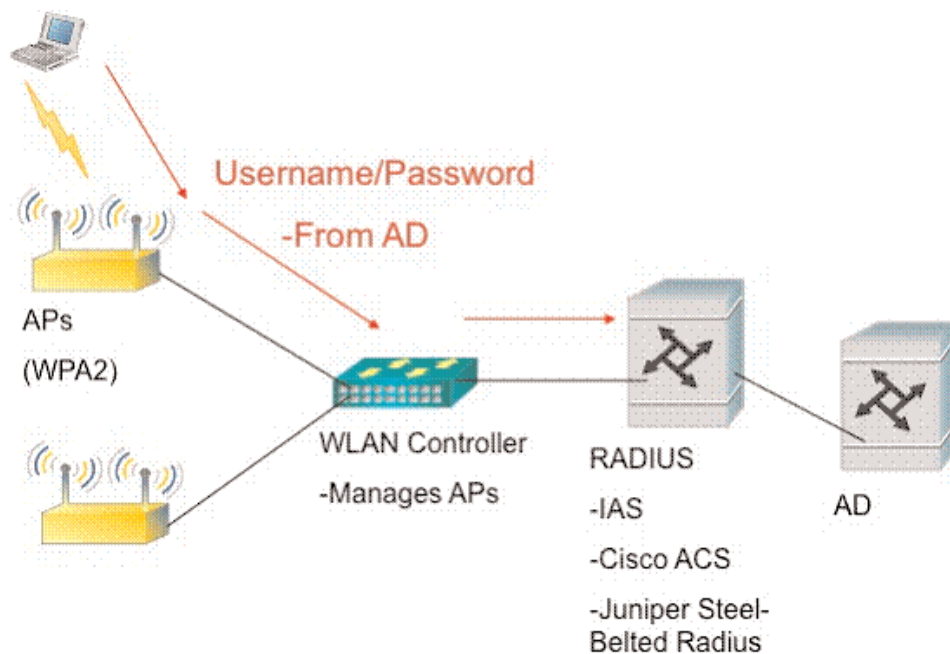
WPA2-Personal is a great security method for home WLANs, but it doesn't fit the enterprise. With WPA2-Personal, there is one passphrase configured on all stations and APs. What if you want to change keys? What if an AP is stolen? What if a laptop is lost? What if someone writes your key on a placard in an office? What if the key is posted on the Internet? In each of these cases, the ideal response is to change the passphrase. But that means changing the configuration settings of every single AP and station on the WLAN.

WPA2-Enterprise solves both the scalability problem of WPA2-Personal. Just like WPA2-Personal, WPA2-Enterprise uses AES-CCMP encryption to protect wirelessly transmitted data. Unlike WPA2-Personal, WPA2-Enterprise uses a server-based authentication method. This eases many of the management headaches that make WPA2-Personal inappropriate for large-scale WLANs. This authentication method is called 802.1X/EAP (Extensible Authentication Protocol).

Using 802.1X/EAP authentication is the ideal choice for the vast majority of enterprise WLANs, but there is a catch. There are several different types of 802.1X/EAP. Not all types of 802.1X/EAP work the same, and to make matters worse, not all WLAN equipment supports the same types of 802.1X/EAP.

WPA2-Enterprise Architecture

To start things off, let's take a look at the general architecture of a WPA2-Enterprise WLAN:



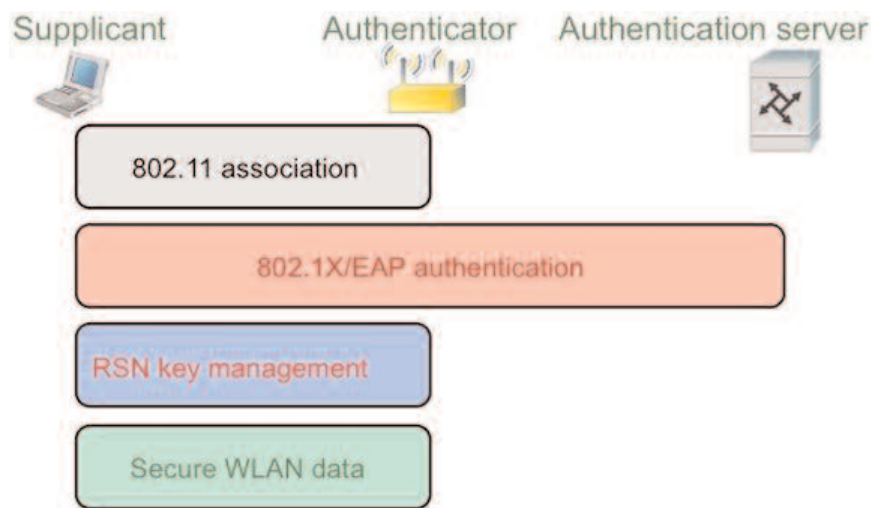
The architecture of WPA2-Enterprise is somewhat straightforward. You install your typical WLAN infrastructure of stations, APs, and antennas. Then you just add a RADIUS server to make things more manageable. Most

enterprises will also leverage their existing database of users by having the RADIUS server act as a proxy for AD (Active Directory) or some other directory service.

The most important part of the basic WPA2-Enterprise architecture is having a RADIUS server to authenticate WLAN users. The RADIUS server allows for centralized WLAN authentication. All of the problems that were cited earlier – stolen APs, lost laptops, posted passwords, etc. – are more easily managed when authentication is centralized. When a security breach happens, a single change is made to the RADIUS server in lieu of having to make individual configuration changes at each AP and station.

The 802.1X/EAP Process

When stations attempt to connect within this basic WPA2-Enterprise architecture, they must go through the 802.1X/EAP process. This process has four basic steps:



After the station (802.1X Supplicant) establishes an association to the AP (802.1X Authenticator), the station completes 802.1X/EAP authentication with the RADIUS server (802.1X Authentication Server). After these first two steps, the station has proven its credentials in order to be allowed on the network.

After authentication is completed, something still must be done to make sure that matching encryption keys are installed on the station and AP. During the 802.1X/EAP authentication process RSN (Robust Security Network) key management information is exchanged. Then after the 802.1X/EAP process is finished, the station and AP use that RSN key management information to negotiate AES-CCMP encryption keys.

Once AES-CCMP encryption keys are installed on both the AP and station, secure data may be transmitted and received across the WLAN.

The name may sound complicated, but 802.1X/EAP authentication is a rather straightforward process. But as was cited long ago in this paper, two catches still remain. Firstly, the right type of EAP must be chosen, and secondly, all devices must be properly configured.

Certificates or Passwords?

Choosing a type of EAP may seem complex at first. There are plenty of types out there. LEAP, PEAP, TLS, TTLS, JUAC, and FAST are all acronyms associated with types of EAP that are currently being used on enterprise WLANs. So how to choose?

Start by asking yourself these two questions:

1. Which type of credential will be used for authentication?
2. Which supplicant and RADIUS software will be chosen?

There are a number of different types of credentials that can be used for EAP authentication. Static passwords, one-time passwords, digital certificates, smart cards and potentially even biometric scans are all possibilities. But when it comes to choosing an EAP type, the question is whether the credential will be controlled by the user (i.e., password) or embedded on the station (i.e., certificate).

If certificates are to be used, then the choice of security over simplicity has been made. Requiring stations to have a verifiable 3rd party certificate present when they authenticate to the WLAN provides great security. Hackers can't crack a certificate with a dictionary attack. Users can't write certificates on Post-It notes. And nobody's going to post your certificate on the Internet. Can the same be said about passwords? Of course not.

Where certificates come up short in comparison to passwords is in ease of management. When passwords are used for WLAN authentication, an existing directory of usernames and passwords can be leveraged. Creating a WPA2-Enterprise network then becomes somewhat of a breeze. Once the RADIUS server and APs are configured to communicate with each other, it just becomes a matter of making sure a properly configured WLAN client utility is installed on each station. When users try to connect, they are prompted for their usual password, and then they are on the WLAN.

Choosing a Type of EAP

As any network admin knows, often times choices like certificates or passwords are out of their control. There may be managers, CIOs, industry standards, or even government regulations that require a certain type of credential for WLAN authentication. But even if the type of WLAN authentication credential is mandated, the network admin still has some work to do. There are several types of EAP. Some support certificates, some support passwords and some support both.

Since this is a paper designed to bring clarity, not calamity, to the minds of networking folks, it's time to get specific.

If you are using certificate-based authentication, choose EAP-TLS.

Every type of EAP that supports certificate-based WLAN authentication is strong. That includes examples such as EAP-TTLS, EAP-PEAP, and EAP-JUAC. But there is one type of certificate-based EAP that stands above all others: EAP-TLS (Transport Layer Security).

EAP-TLS has one major thing going for it that no other certificate-based type of EAP has: it's available everywhere. Every modern Windows machine (starting with Windows XP) comes with an installed client utility that supports EAP-TLS. Same for Windows Mobile and same for Mac OS X. Even if a 3rd party WLAN client utility like the Intel ProSet client, Broadcom client, Dell client, Cisco Secure Services client, or Juniper Odyssey Access client is used, EAP-TLS will be supported.

With that type of broad support, it just makes sense to use EAP-TLS for straightforward WLAN authentication with certificates.¹ Which takes us to our second specific proclamation:

If you are using passwords, choose EAP-PEAP or EAP-TTLS... or both.

All right. That wasn't as specific as the last one. But it's as specific as it can get.

See, the problem here is there just isn't uniform support for one type of password-based EAP in WLAN client utilities. For example, if you want to use EAP-PEAP (Protected EAP) you'll get support from all of the aforementioned client utilities ... but not the Apple Airport client that comes installed with Mac OS X.

The other option is EAP-TTLS (Tunneled Transport Layer Security). If you have a few Macs on the network they'll be able to authenticate using EAP-TTLS. The problem is that you'll lose support from the WZC (Wireless Zero Configuration) client that comes installed with Windows XP and Vista. Kind of frustrating, huh?

There is some good news here, though. First of all, many RADIUS servers will support multiple types of EAP simultaneously. For example, the Juniper Steel Belted Radius server fits that mold. As long as both EAP-TTLS and EAP-PEAP are enabled on the server, stations using either authentication method may access the WLAN.

Another piece of good news is that many computers with internal WLAN adapters ship with more than one client utility installed. That means if you order a fleet of HP laptops because you liked the Jay-Z commercial, you can just enable the Broadcom client instead of the WZC client. That way they'll get on your EAP-TTLS network with the MacBook you were inspired to buy because of John Hodgman's comic genius as "PC" in the Apple commercials.

Not So Fast, My Friend

Seems like we're done, right? We know how WPA2-Personal works on home WLANs, and we know that strong PSK passphrases should be used. We know how WPA2-Enterprise works on enterprise WLANs, and we know that certificates or passwords can be used for authentication. Heck, we even know which types of 802.1X/EAP support which method of authentication and which client utilities support those types of EAP. All that is great, but there is one last major thing to remember:

If passwords are used with EAP, proper client configuration is essential.

At the Schmoocoon hackers convention in 2008, renowned wireless security expert Joshua Wright gave a presentation on flaws in WPA2-Enterprise security. The flaws he described are not intrinsic to the 802.1X/EAP protocol. That's secure. No, the flaws he described deal with the implementation of 802.1X/EAP. In short, Joshua Wright's Schmoocoon presentation pointed out that if client utilities are not configured properly, the possibility of attacks on passwords exists.

There are two configuration settings in WLAN client utilities that could cause securely designed protocols like EAP-TTLS and EAP-PEAP to be vulnerable to attack:

1. Validate server certificate.
2. Specify authentication server.

When the server certificate is validated during the 802.1X/EAP process, it prevents man-in-the-middle attacks. Man-in-the-middle attacks occur when a hacker makes himself part of the network between a client and server. When the client – WLAN station, in this case – authenticates to the server – RADIUS server, in this case – the hacker accepts the server's certificate and creates a phony certificate that is then sent to the client.

Since certificates contain key material that allows for the creation of encryption tunnels, the hacker is effectively building two tunnels. One tunnel goes from the client to the hacker, and a second goes from the hacker to the server. The problem is that the hacker is now able to "see" everything that is passed through these two tunnels.

The good news about man-in-the-middle attacks is that they can be prevented. Since certificates contain information that is specific to a server and a CA (certificate authority), clients have the ability to use certificate errors to identify possible attacks. Therein lies the problem. If the certificate is not going to be validated, then how is the client going to know that there is a certificate error? They won't.

The other good news relating to man-in-the-middle attacks is that server certificate validation is enabled by default on most WLAN client utilities. Not all, but most. So check out your client utility and just make sure that setting is enabled.

Unlike server certificate validation, the second essential client configuration setting is generally not enabled by default. Specifying an authentication server is disabled by default on all of the aforementioned WLAN client utilities.

When a specific authentication server is configured on the WLAN client utility, the station will only complete the 802.1X/EAP process if the RADIUS server is the one specified. Unfortunately, by default WLAN client utilities will allow authentication to any server that supports the correct type of EAP.

Specifying an authentication server prevents Evil Twin RADIUS attacks. A traditional Evil Twin attack (not an Evil Twin RADIUS attack) on a WLAN occurs when a hacker configures an AP with the same SSID (service set identifier) as the legitimate WLAN. This type of attack could potentially draw unsuspecting users into establishing a direct connection to the hacker, thereby opening them up to the type of peer-to-peer attacks that were described earlier.

An Evil Twin RADIUS attack takes things a step further. Traditional Evil Twin attacks are limited because in many cases they are only effective against open WLANs. If a user has security configured for the SSID they are trying to connect to, the user's station will not roam to the hacker's AP that is configured with an open SSID. An Evil Twin RADIUS attack sees the hacker running RADIUS software behind his Evil Twin AP. That way a user's station could potentially roam to the hacker's AP even if WPA2-Enterprise is in place.

The problem for the hacker is that if an authentication server is specified on the WLAN client utility, users' stations will not attempt to authenticate using 802.1X/EAP to the hacker's Evil Twin RADIUS server.

The problem for the network admin is that this type of protection means extra work. Specifying a RADIUS server in every station's WLAN client utility generally takes a bit more effort than validating the server certificate. (Validating the server certificate is typically pretty straightforward if certificates are purchased from a 3rd party like Verisign or created using common CA (certificate authority) software like the Microsoft CA.

An Important Part, But Not the Only Part

So there we have it. Good principles to follow when setting up WLAN authentication for both homes and enterprises. And remember that with WPA2 security, strong encryption comes right along with that strong authentication. The end result is that the WLAN keeps hackers from accessing the LAN wirelessly and protects wireless data from people running a wireless sniffer.

It should always be remembered, though, that WPA2 is intended to be only a part of an overall WLAN security plan. It's an important part, but just a part, nonetheless.

Whether large or small, a properly secured WLAN involves additional considerations as well. How will wireless data be secured when users telecommute? How will the network be protected from rogue APs? How will attacks on stations be prevented when users travel? How will I monitor my environment for vulnerabilities and attacks? When these questions are answered alongside a properly configured WPA2 network, a truly state-of-the-art WLAN security design will be in place.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course:

[Wireless LAN Foundations](#)

For more information or to register, visit www.globalknowledge.com or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Ben Miller is the Course Director for the Global Knowledge wireless curriculum. In addition to his work as an instructor for Global Knowledge, Ben is a wireless services professional based in Los Angeles, CA. He is a CWNE (Certified Wireless Network Expert) and a CWNT (Certified Wireless Network Trainer).