U.S.Robotics®

WLAN Security – Networking with Confidence

Introduction

So you've just installed a new wireless local area network (WLAN) in your small business or home. The access point is on and connected, the client PCs are connected to the access point, allowing you to connect to others and the Internet without worrying about wires.

But unlike a wired network, you can't tell if an unauthorised person has accessed your WLAN. With WLANs you are using radio frequencies that in clear air have a range of up to 300 metres, so could somebody else be connecting into your system from the next street?

With many WLANs the default settings make you vulnerable to eavesdropping. But don't worry: by taking a few simple steps, your wireless network can be as secure as a normal, wired LAN. In fact, some security experts even argue that WLANs can be more secure.

Note that a WLAN makes you no more vulnerable to attacks from worms, viruses and other such attacks, since they can be rebuffed by the network edge's defences, usually a firewall.

Online shopping is safe too. When conducting financial transactions over the airwaves, check for a padlock symbol on your browser's status bar. When active, the padlock means there is an encryption tunnel using SSL that scrambles all data between your browser and the remote server. This means that, even if your WLAN is not secure, while SSL is active any data transmitted between you and the remote server remains unreadable by others.

That said, there are steps you can take to reduce the likelihood of your WLAN allowing eavesdropping, and that's what the rest of this white paper is all about.

Why secure the WLAN?

If you only surf the Web and send occasional emails, the risk of being hacked appears low. However, it's not as simple as that. Firstly, if someone manages to hack into your WLAN and piggybacks onto your Internet connection, even if it's only a slow modem link, they are stealing your bandwidth. If they only download the odd email and Web page you might not notice, but if you start a big download and it takes an hour instead of a few minutes, it costs you time and money.

Worse, anyone on your WLAN will be using the same Internet protocol (IP) address as you. To others on the Internet they appear to be you – the intruder has hijacked your identity. This means that they could send spam, fill in forms on Web pages and generally be a nuisance at best or, at worst, conduct criminal acts. And when the authorities trace the IP address, they see yours, potentially rendering you liable for prosecution.

There's a honeypot effect too. A relatively new phenomenon known as warchalking also means that hackers can tell others where there's an accessible Internet connection by chalking marks on the pavement. A "free" Internet connection could entice others to come and piggyback your connection. Most of them do it not to steal data, but simply because they can.

So locking up your WLAN looks like a bright idea, and should help you sleep more soundly.

How much security is enough?

Security involves the application of common sense, bearing in mind the whole risk. The key is to reduce the risk to a level you're comfortable with.

For example, when deciding how much to spend on home security, you calculate how much security you need given the risks involved and balance that against the cost and any inconvenience it might entail.

It's the same when determining the right level of WLAN security. Questions to answer are:

- How valuable is the information you are guarding?
- How much inconvenience are you prepared to tolerate?
- How much are you willing to pay?

Let's examine the risks using a simple example. For a home-based WLAN, the odds are low that anyone will want to steal information since its value to anyone else is likely to be minimal. However, they might want to steal your bandwidth.

This means you need to stop intruders connecting to the AP by using hardware filtering to disallow them from registering a client PC at the AP – see below for details. This is the minimum level of security you should apply. It also makes sense to prevent potential eavesdroppers from spying on your data stream, so a combination of filtering and encryption will provide all the security you need. Best of all, they require no intervention once you've configured the AP and clients, and they're free.

So there's no right or wrong answer to the question of how much security is enough – only you can determine the answer based on your individual circumstances. That said, it makes sense to use whatever security measures that come free with the system if only for your peace of mind.

What security can you get now?

Help is at hand, and it's built into every standard WLAN for free. There's a number of steps you can take to minimise the risk of a WLAN break-in, the first being to change the default settings. That's because hackers can detect your AP's type and will know what the default settings are.

ESSID

Chief among these is the ESSID (Extended Service Set ID), or name of the WLAN. By default it's often "101" but it can be any string of up to 256 characters. Don't be obvious and pick the house or road name. Instead, think of it as a password and use a long name with both letters and numbers, making it harder to hack. Then configure the AP so that it does not broadcast the ESSID. In this way, only authorised clients can connect to your AP.

MAC address filters

Hackers don't have to be particularly determined to find out what WLANs are operational in their immediate vicinity and can often determine the ESSID. So there's a second layer of security you can adopt, the MAC (Media Access Control) address filter. A MAC address is a unique identity burned into every network adapter during manufacture, with no way of changing it.

Using this filter, the AP maintains a list of MAC addresses and only permits those on the list to connect. No connection means no access to the rest of the network, such as the data on servers and client PCs.

What do I do?

Linking the household's two laptops to the broadband connection and the office Ethernet network, I use an access point in the office and another on the ground floor, which allows me to work in front of the TV or in the garden when weather permits. Clients are set up so that only connections to an AP are permitted, not directly to other clients, so rogue clients cannot connect without going through the AP.

I live on a fairly busy street but I can see all round my house so anyone trying to hack into the WLAN by brute force will have to make themselves visible. That doesn't mean it's not worth taking basic precautions though, so the ESSID is changed to a long string of characters connected by numbers and symbols, ESSID broadcast is disabled, and WEP is enabled at full 256-bit strength. Enabling 802.1X would be pointless for a home network so it's switched off.

Other than that, the system is as secure as it both can and needs to be – and I always turn off the AP when leaving the house for a day or more, minimising the chances of an e-burglar gaining access without anyone noticing. Following these simple precautions will keep your WLAN safe and secure too.

The main drawback to MAC address filtering is the need to discover the MAC address of every client's adapter and enter it into the AP's settings fields. As a one-off task, it might take you half an hour from start to finish for say, half a dozen client machines. However, if a PC Card gets lost, you buy new ones, or you add or upgrade an AP, it can make for a lot of extra tedious typing. That said, for a small WLAN where such changes are infrequent, this might be almost all the security you need.

Encryption

Even if hackers can't get past your AP, they may still be able to access data that's traversing your WLAN. The way to protect data in transit is encryption, the WLAN encryption standard being WEP (Wired Equivalence Privacy).

WEP works by encrypting traffic – scrambling it – as it leaves the AP or client PC and decrypting it on arrival. Any encryption method, whether used by the ancient Greeks, the Nazis with their Enigma machine, or today's WLANs, needs a common key at both ends of the link or the result is gobbledegook. The longer the key, the lower the likelihood of someone breaking it through guesswork or, with the huge computing power available today, by brute force by running through all the possibilities.

What this means in practice is that a WEP key must be at least 128 bits long to have a chance of defeating a potential interceptor, with 256 bits being many times more

secure. Just as an example of how adding bits to encryption keys makes a real difference, consider this.

Under WEP, all encrypted packets use the first 24 bits for initialisation, the rest for data. This means that 64-bit encryption – actually 40 bits of which are data – provides just over one trillion combinations which, given today's computing power, would not take too long to crack. However, double the size of the encryption key and the number of combinations jumps exponentially to over 20 million trillion combinations. Double it again to 256 and the number is astronomical – 1.E+69 in scientific notation, a 69-digit number.

If you have a spreadsheet handy, enter the number 2^256 – that's two to the power of 256 – and that's roughly the number of combinations a hacker would need to check to be sure of breaking the encryption.

The chances of anyone doing so are remote since they'd need to capture lots of data over a long period of time. Given WLANs' relatively short range, they would be highly visible for days if not weeks.

An extremely determined individual might feel it was worth the effort though, at which point, the WLAN's security is compromised and a change of key is required. This means tediously typing new keys into every client and AP. Far better to ensure things don't get that far by changing the key frequently, preferably for every packet that's sent over the WLAN. This is where future standards are headed and is the area we'll be exploring in the next section.

Locking down

The next step is to lock down the AP. You'll notice that you can change the AP's settings over the WLAN. This is not a good idea. If a hacker gets into your network, they can also access your AP, altering the settings to suit them, not you. If they're clever, you might not even notice, even though someone else is accessing your connection. If they're not, your WLAN might even stop working.

Either way, make sure you only configure the AP over a wired connection. If you've got Ethernet use that or, better still, use the serial port connection if it's got one. Don't forget to change the default password where possible.

Authentication

The final layer of protection is individual authentication. The standard method of WLAN authentication uses the 802.1X protocol. If the protocol is enabled, unauthenticated users cannot get past the AP to access the rest of the network. It's built into Windows XP already and is embedded in the next-generation WLAN security standard – there's more on this in the Future Standards section below.

Future security standards

If the security technology we've got in WLANs isn't broken, why fix it? Basically, there are two main problems with the current standard. Firstly, with a powerful

At a glance checklist

1. Change the default ESSID
2. Use WEP, with at least 128-bit encryption, 256-bit encryption is many times better
3. Add MAC address filters
4. Turn off ESSID broadcast
5. Lock down the access point's configuration interface
6. Don't worry!

enough computer and enough traffic to analyse, a hacker can determine what your WEP key is and break it, rendering your wireless data stream vulnerable. Secondly, while MAC address filtering is not a bad way of rejecting unwanted intruders, it identifies the computer's WLAN adapter rather than the individual – what happens if someone steals your computer?

So the next generation of security standards, known as the WPA (Wi-Fi Protected Access), improves on what we've got now. Unlike today's static encryption keys, it uses a master password from which the system generates keys that change continuously using a protocol known as TKIP. Keys are never re-used, cutting the risk that a hacker will discover them. WPA also includes 802.1X, discussed earlier, which allows the system to check who's logging in against a central database of known users.

The good news is that you may be able to upgrade to WPA today, as it's designed to be a firmware upgrade. Upload the software into all your AP and client WLAN cards, reboot the AP and you're done!

Further into the future, a new standard known as 802.11i will be finalised, which will strengthen the encryption using a technique known as AES (Advanced Encryption Standard). WLAN hardware will need to be more powerful to run this complex encryption technique so you may need to replace your existing wireless network when AES arrives.

Conclusion

Keeping your WLAN safe from intruders isn't complicated and can be as safe as you need it to be with a few simple precautions. The main thing to remember is that the risk you are willing to tolerate depends on how valuable the data is, balanced against the cost of implementing security measures, cost that's measured in both cash and extra time and inconvenience that security measures may add.

In practice, ensure that you change the defaults. Do just this and you're ahead of a huge number of very highly paid, network security professionals – and that alone should make you feel good about your WLAN.

By Manek Dubash

Manek Dubash is a leading IT journalist, network specialist, former editor-in-chief of PC Magazine and a regular speaker at networking forums and events. With over twenty years industry experience, he is now a director of Webster Buchanan Research, a global media and market intelligence company.

www.usr.com