



# Six Dumbest Ways to Secure Wireless LAN



George Ou from ZDNet wrote an article a couple of years ago (and [recently updated it](#)) on the “[Six Dumbest Ways to Secure Wireless LAN](#)”. I found it of interest and thought the British Mac listeners may find it of interest too. Doing things such as using WEP encryption, MAC address filtering and “SSID hiding” are not good enough and can lull you into thinking you are secure when you are not. Of course, using WEP is better than nothing (but not *much* better!). As we’ve mentioned in previous British Mac articles, unless you are using WPA encryption with a truly random alpha-numeric minimum 10-character pass-phrase, you are not protecting your wireless network.

“For the last three years, I've been meaning to put to rest once and for all the urban legends and myths on wireless LAN security. Every time I write an article or blog on wireless LAN security, someone has to come along and regurgitate one of these myths. If that weren't bad enough, many "so called" security experts propagated these myths through speaking engagements and publications and many continue to this day. Many wireless LAN equipment makers continue to recommend many of these schemes to this day. One would think that the fact that none of these schemes made it in to the official IEEE 802.11i security standard would give a clue to their effectiveness, but time and time again that theory is proven wrong. To help you avoid the these schemes, I've created the following list of the six dumbest ways to secure your wireless LAN.

## Wireless LAN security hall of shame

**1. MAC filtering:** This is like handing a security guard a pad of paper with a list of names. Then when someone comes up to the door and wants entry, the security guard looks at the person's name tag and compares it to his list of names and determines whether to open the door or not. Do you see a problem here? All someone needs to do is watch an authorized person go in and forge a name tag with that person's name.

The comparison to a wireless LAN here is that the name tag is the MAC address. The MAC address is just a 12 digit long HEX number that can be viewed in clear text with a sniffer. A sniffer to a hacker is like a hammer to a carpenter except the sniffer is free.

Once the MAC address is seen in the clear, it takes about 10 seconds to cut-paste a legitimate MAC address in to the wireless Ethernet adapter settings and the whole scheme is defeated. MAC filtering is absolutely worthless since it is one of the easiest schemes to attack. The shocking thing is that so many large organizations still waste the time to implement these things. **The bottom line is, MAC filtering takes the most effort to manage with zero ROI (return on investment) in terms of security gain.**

**2. SSID hiding:** There is no such thing as "SSID hiding". You're only hiding SSID beaconing on the Access Point. There are 4 other mechanisms that also broadcast the SSID over the 2.4 or 5 GHz spectrum. The 4 mechanisms are: probe requests, probe responses, association requests, and re-association requests.

Essentially, you're talking about hiding 1 of 5 SSID broadcast mechanisms. Nothing is hidden and all you've achieved is cause problems for Wi-Fi roaming when a client jumps from Access Point to Access Point.

Hidden SSIDs also makes wireless LANs less user friendly.

You don't need to take my word for it. Just ask Robert Moskowitz who is the Senior Technical Director of ICSA Labs in his white paper [Debunking the myth of SSID hiding](#).

**3. LEAP authentication:** The use of Cisco [LEAP authentication](#) continues to be the single biggest mistake that corporations make with their wireless LAN because they leave themselves wide open to attack. Cisco still tells their customers that LEAP is fine so long as strong passwords are used. The problem is that strong passwords are an impossibility for humans to deal with.

If you doubt this, try a password audit of all the users in your organization and see how long it takes to crack 99% of all passwords. 99% of organizations will flunk any password audit for most of their users within hours. Any attempt to enforce strong passwords will result in passwords written on sticky notes.

Since Joshua Wright released a tool that can crack LEAP with lightning speed, Cisco was forced to come out with a better alternative to LEAP and they came up with an upgrade to LEAP called EAP-FAST. Unfortunately, [EAP-FAST](#) still falls short in security with its default installation. Although Cisco makes LEAP and EAP-FAST freely available to partners for the client end, the same is not true for Access Points. LEAP and EAP-FAST are essentially two proprietary protocols that Cisco employs as a strategy to monopolize the Access Point market. There are open standards based EAP mechanisms like EAP-TLS, EAP-TTLS, and PEAP which are all much more secure than either LEAP or EAP-FAST and they work on all Access Points and client adapters, not just Cisco. Cisco does support open standard EAPs just like everyone else so you should always use open EAP standards to get better security and avoid the hardware lock-in.

**4. Disable DHCP:** This is much more of a waste of time than it is a security break. DHCP allows the automatic assignment of IP addresses and other configurations. Disabling DHCP has zero security value and just wastes time. It would take a hacker about 10 seconds to figure out the IP scheme of any network and simply assign their own IP address. Anyone who tells you that this is a way to secure your wireless LAN doesn't know what they're talking about.

**5. Antenna placement:** I've heard the craziest thing from so called security experts that actually tell people to only put their Access Points in the center of their building and put them at minimal power. Antenna placement does nothing to deter hackers. Remember, the hacker will always have a bigger antenna than you which can home in on you from a mile away. Making a wireless LAN so weak only serves to make the wireless LAN useless. Antenna placement and power output should be designed for maximum coverage and minimum interference. It should never be used as a security mechanism.

**6. Just use 802.11a or Bluetooth:** Fortunately, I haven't heard this one for a while. There were so called security experts that went around telling people that they simply needed to switch to 802.11a or Bluetooth to secure their wireless LAN. 802.11a refers to a physical transport mechanism of wireless LAN signals over the air, it does not refer to a security mechanism in any way.

**Dishonorable mention:** Some of you might be wondering why I didn't put WEP in as one of the six dumbest ways to secure a wireless LAN.

**In light of recent developments within the last 6 months, it takes only a few minutes to break a WEP based network which makes WEP completely ineffective and a good potential future candidate for the wireless LAN security hall of shame.**

Where it currently fails to be in the hall of shame is that it still holds up for a few minutes, requires a little skill to launch the packet injection attacks, and isn't propagated as an urban legend for a secure wireless LAN.

**The top six require no skills, takes less than a minute to crack, and are propagated as urban legend. However, that doesn't mean you should use WEP in any form or shape.**

This blog wasn't just meant to be funny, it's serious business that so many organizations waste their time and money on worthless security schemes that give them a dangerous false sense of security. If you fall in to any of these six categories, it's time to wake up and implement some real wireless LAN security.

The original blog has probably been read by more than a hundred thousand people, but I still can't kill these nasty urban legends because they are so engrained as "best practice."

I was shocked and infuriated to find that even some security certifications, like the CISSP, and VISA payment processing compliance requirements, like PCI, are recommending most of these methods as "best practice."

Note that I recently attended the official CISSP boot camp training and in spite of this bad wireless LAN advice, I still recommend the CISSP certification and training. It really taught me how to better communicate to management and business people and align security and IT to the business. I have, however, asked them to fix their small section on wireless LAN best practices, and I hope they fix it.

The most common and misguided arguments I hear against my advice and in favor of implementing this nonsense are:

- What's the harm? It's a layered approach to security.
- It makes us harder to see and hack.
- We're a small company, and we can't afford real security.

The problem with these arguments is that they're based on some fundamentally wrong assumptions and an inadequate knowledge of how wireless LAN security works.

- **These aren't layered approaches; they're more like buying overlapping warranty coverage, since any benefit against casual bandwidth thieves is already covered by real security measures. The harm is that people confuse these methods for the real thing, and they spend more money and resources on implementing the wrong security mechanisms and end up skimping on real security.**

- **They don't make you harder to hack. Kismet, which is a free utility, will reveal so-called hidden SSIDs, MAC addresses, and static IP schemes within seconds of scanning the airwaves, sending all that money and time spent on MAC address and static IP management down the toilet.**

- **If you have a limited budget with limited IT staff, it's all the more reason to use real wireless LAN security, because you certainly won't be able to afford the complexities of MAC filtering and static IP configuration. True wireless LAN security is far cheaper to implement and maintain.**

**Rock solid wireless LAN security for the home or small office can be summed up in a single paragraph. All you need to do is use WPA-PSK security with a random alphanumeric pass-phrase that has a minimum of 10 characters.**

I estimated that a truly random alpha-numeric 10-character pass-phrase using modern single-core computers will take one thousand PCs working in parallel 500 years to crack. If your hardware doesn't support WPA mode, you can almost always get a free software/firmware upgrade to support it.

If WPA mode absolutely can't be supported, you can run WEP (104 bit AKA 128) security, which might take a semi-skilled script kiddy using two PCs in an active attack configuration 10 minutes to break.

WEP shouldn't ever be considered effective wireless LAN security, but it's hundreds of times harder to break than any of the myths. WEP can be considered an actual deterrent when nothing better like WPA is available, whereas these myths aren't even worthy of the deterrent title”.

Source: George Wu, ZDNet <http://blogs.zdnet.com/Ou/?p=43>