## Introduction

Corporations, government agencies, the military, and enterprises – in fact all medium to large scale wireless LANs have a different set of security requirements compared to the wireless LAN used in your home or in small offices. Enterprise wireless security requires advanced mutual authentication and strong encryption solutions. But what is needed to properly secure a home wireless network? Below is a list of ten simple steps the average home user can take to secure their own home wireless network.

David Coleman of AirSpy Networks (www.airspy.com), a wireless LAN consultant and CWNP Program Trainer compiled the following wireless LAN SOHO security checklist to assist you in securing your network.

## Table of Contents

## 1. No Default Settings

The relatively small home wireless market, 8.7 million households in 2004, will climb to 28 million in 2008

– Jupiter Research

The first and biggest mistake that most users of home wireless networks make is that they just power up the box and leave all the default configuration settings enabled on the home wireless gateway device. The two most obvious default settings would be the SSID and the administrator login name/password. The SSID (Service Set Identifier) is the "name" of your wireless network comparable to a Windows workgroup name.

For example, Linksys, the SOHO WiFi market leader, uses an SSID of "linksys". Another leading vendor D-Link uses the SSID of "default". A simple Google search will generate links to numerous sites that have compiled lists of all the default settings for the products of many wireless vendors. Any individual can also simply download the PDF manual with the same information from the vendor's web site.

Amateur hackers, Wardrivers and script-kiddies will always target the wide open wireless systems first. Using the vendors default settings is analogous to leaving the front door of your house always open. A conservative estimate of SOHO users that do not change the default settings is about 70%. So do not use the default settings. Pick a different SSID. Change the device's administrator login name and change the admin login password. Also, if the device allows you... change the default IP address.

## 2. Cell Sizing

SOHO wireless access points and wireless gateways/routers extend the network into the "air". Every device uses 2.4 GHz and/or 5 GHz radios card to transmit and receive the data. Despite low power, radio waves travel at the speed of light and can penetrate most construction materials. It is not uncommon that a very strong and usable signal can still be received from the street outside your home or small business. Other than putting a chain link fence completely covering your home, there is no way to completely contain an RF signal.

**FIGURE 1** Oversized WLAN cell

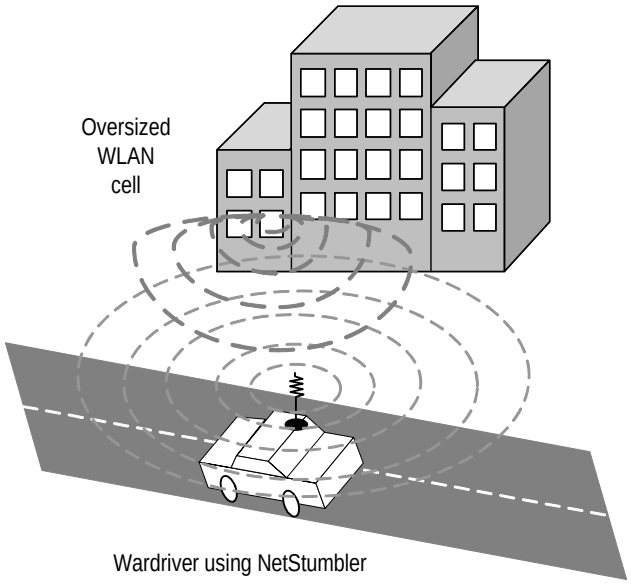
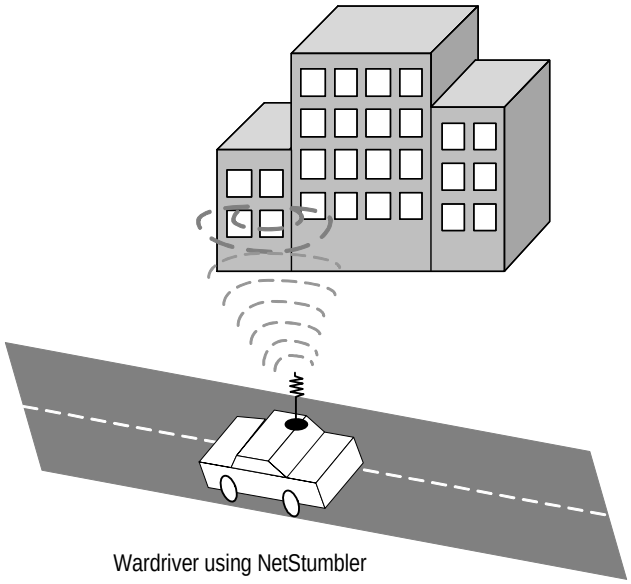



**FIGURE 2** Correctly sized WLAN cell that is still vulnerable




However, today many SOHO WiFi manufacturers give you the ability to adjust the power settings of your wireless gateway. Lower power settings mean shorter range. If your vendor provides the option, lower your power settings so that your neighbor three houses down is not using your wireless network. But still make sure your power settings are enough to properly provide signal coverage for your mobility needs. Some vendors have a setting called "adjust antenna transmit power". In reality you are not adjusting the antenna but are in fact lowering the transmit power of the radio card. If your wireless router does not have the ability to adjust the power settings, physically locate the unit in the center of the house and away from the windows.

## 3. SSID Naming

Do not use a network name (SSID) that can clearly identify who you are. Do not use a family surname, your street address, or your dog's name. Choose a network name with no meaning. Something such as Rhj18YT89. Please be aware that SSID's are "case sensitive" and must match on both the wireless gateway and on the software client utilities of your computers using wireless cards.

## 4. Cloaking

Remember in Star Trek when the Enterprise was "cloaked" but somehow the Klignons found the ship anyway? Well there is a way to "cloak" your wireless network. Your SOHO wireless device should have a setting called "Closed Network" or "Broadcast SSID". By either enabling a closed network or disabling the broadcast SSID feature you can hide or cloak your network. The SSID (network name) is transmitted in the air by your device in a broadcast called a "Beacon". Also, many wireless cards client utilities transmit empty "Probe Requests" looking for your device.

**Cloaking is a great way to hide your network, but any experienced hacker will still find the SSID.**

There is a very popular and freely available software program called Network Stumber that is used by individuals to discover wireless networks. Network Stumbler also sends out blank Probe Requests looking for wireless access points. When you implement a closed network, the SSID is no longer in the BEACON and your wireless gateway will not respond to blank Probe Requests. Effectively, your wireless network is temporarily invisible.

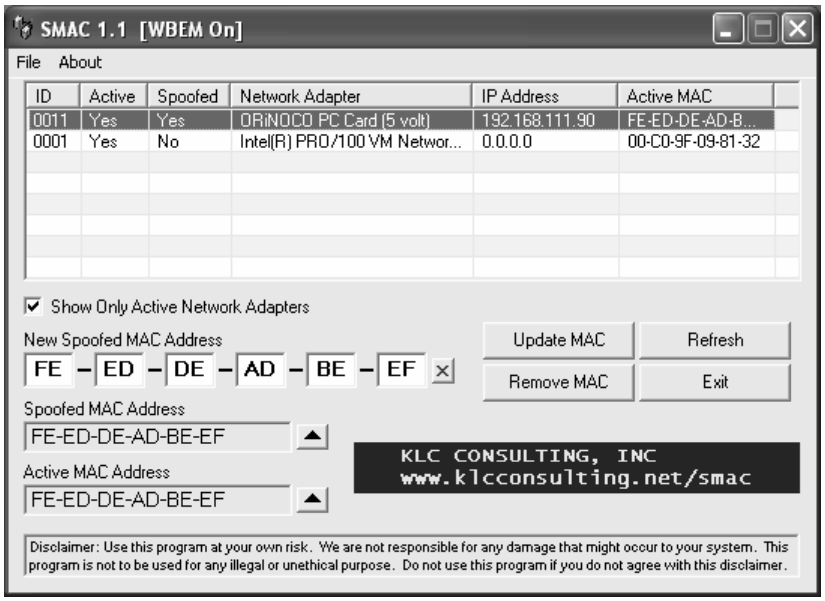
It should be noted that more professional tools can still discover your network because there are other transmissions from your home device that will eventually expose your SSID. Cloaking is a great way to hide your network, but any experienced hacker will still find the SSID.

## 5. Mac Filters

Every network card has a physical address called a MAC address. This address is a twelve digit hexadecimal number that can usually be found on the back of your wireless card. All SOHO wireless gateway/routers should have a configuration setting to apply MAC filters. By entering in all the "allowed" MAC addresses of your wireless cards and enabling the MAC filter, any cards with other addresses will be denied access.

It should be noted that MAC addresses can be "spoofed" and any amateur hacker can still bypass any MAC filter by spoofing. However, implementing MAC filters will add another reasonable layer of security to your wireless network.

**FIGURE 3** Sample MAC Spoofing Software Utility




## 6. Encryption

All the data that you transmit is radiated into the air for anyone to see. Hacking tools exist where an individual can reassemble all your data even if they were not the intended recipient. This means that someone can read all your e-mail, watch the web pages you are surfing, read your instant messages and steal passwords. It is imperative that any SOHO wireless network deploy encryption.

By default, all WiFi devices support an encryption technology called WEP (Wired Equivalent Privacy). Newer units should support an encryption protocol called TKIP (Temporal Key Integrity Protocol) which is basically an improved and more secure version of WEP. Even better, the newest wireless cards support an encryption protocol called AES (Advanced Encryption Standard) which the United States Government mandates for use in wireless networking at many government agencies. If your device supports WEP, enter a matching static 128-bit WEP "Key" on both your wireless gateway and wireless cards. The keys must match otherwise you will lock yourself out of your own wireless network. If you enable WEP all your data will be encrypted as it transverses through the air.

Be aware that WEP encryption has been cracked. It used to take about a month to generate enough traffic in the average SOHO network to crack WEP. Please be warned that the newest hacking utilities can crack WEP encryption in about five minutes. Because WEP has been cracked, it is a good idea to use TKIP or AES encryption if your vendor supports it.

If your vendor is WPA (Wi-Fi Protected Access) certified, then the wireless equipment you have supports TKIP encryption. Both the access unit and the wireless cards must be WPA certified. Implementing TKIP usually means enabling a security setting called WPA-Personal. This security setting is sometimes known under other vendor names including WPA Passphrase, WPA-Pre-Shared Key and WPA-PSK. Entering a matching passphrase on both the

wireless router and your cards will enable TKIP encryption. Also be aware that your older cards and devices that only support WEP may have a WPA firmware upgrade available. Check your vendor's website to see if a WPA/TKIP firmware upgrade is available for download.

If your vendor is WPA2 (Wi-Fi Protected Access - version 2) certified, then the wireless equipment you have supports AES-CCMP encryption. Both the access unit and the wireless cards must be WPA2 certified. Implementing AES-CCMP usually means enabling a security setting called WPA2-Personal. This security setting is sometimes known under other vendor names including WPA2 Passphrase, WPA2-Pre-Shared Key and WPA2-PSK. Entering a matching passphrase on both the wireless router and your cards will enable AES encryption. Older cards will probably not be able to be upgraded via firmware to use AES-CCMP encryption. However, check your vendor's website to see if a WPA2/AES-CCMP firmware upgrade is available for download.

Using a matching passphrase on your wireless router and your wireless cards provides a simple form of authentication and dynamically generates the encryption keys that are used to encrypt your data. Be advised that hacking tools currently exist that can capture and discover your passphrase. If your passphrase was compromised, a hacker could obtain access to your wireless network as well as potentially decrypt your data. Because these hacking tools exist, it is imperative that the passphrase you choose be a "strong" passphrase. The strong passphrase should consist of at least eight characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.). The passphrase is case-sensitive and should contain letters in both uppercase and lowercase. The passphrase also becomes stronger and harder to crack as you use more characters in a passphrase. An example of a twenty character strong passphrase would be M$8ni3y0tKde&P4Ad8@2.

## 7. Static IP

Your wireless gateway will issue out IP dynamic IP address to your wireless network cards. Why freely hand out IP addresses to potential bad guys? Consider disabling DHCP settings on your gateway and manfully entering static IP addresses on all your wireless cards. If you still want to use DHCP, at the very least change the range of IP addresses that are used and do not use the default scope of IP addresses.

## 8. Common Security Practices

Implement common sense security practices on all your computers that will have wireless access:

- Install virus protection software and download the virus signature files on a regular basis
- Disable file sharing on your computers unless you absolutely have a need
- Although most wireless routers also have firewalls, consider installing personal firewalls on every computer as well.

## 9. Document your settings

Record all your configuration settings for SSID, WEP keys, TKIP passphrases, IP settings, MAC filters, channel and power settings in a document that you can save and refer to later. Print a copy of this document and store it in a safe place. You never know when you might have to reset your device to the default settings and start over.

## 10. Turn it off

Here is a novel idea: If you are not using your wireless network, turn it off! An intruder cannot access your wireless network ever if it is not in use.

**About the Author**


David Coleman is a Wireless Security/Networking Trainer and Consultant. He teaches the CWNP classes that are recognized throughout the world as the industry standard for wireless networking certifications as well as vendor-specific Wi-Fi training. He has also taught numerous "train the trainer" classes and "beta" classes for the CWNP Program. He has instructed IT professionals from around the globe in wireless networking administration, wireless security, and wireless frame analysis. His company, AirSpy Networks (www.airspy.com), specializes in corporate training and recently instructed numerous employees at SpectraLink and Dell Computers. AirSpy Networks also specializes in government classes and has trained numerous computer security employees from various law enforcement agencies, the Department of Defense, US Army, US Navy, and other federal and state government agencies. David Coleman is also the co-author of Sybex Publishing's "CWNA : Certified Wireless Network Administrator Study Guide" - ISBN # 0471789526. Contact David Coleman via e-mail: david@airspy.com.

**About the CWNP Program**

The CWNP Program is the industry standard for wireless LAN training and certification. IT professionals in 86 countries have achieved CWNP certification in how to make wireless LANs more secure, cost-effective, and reliable. The CWNP Program is operated by Planet3 Wireless, Inc., a privately-held Georgia corporation. For more information about the CWNP Program, visit www.cwnp.com

**Corporate Headquarters**
CWNP Program
P.O. Box 20063
Atlanta, GA 30325
USA

Tel: 404.305.0555
866.438.2963
Fax: 866.422.8354

**www.cwnp.com**