



Interested in learning more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permitted without express, written permission.

SCORE Security Checklist

Residential Wireless Network Audit Checklist

Prepared by: Dean Farrington

Version: 1.0

References:

1. NIST, Special Publication 800-48, “Wireless Network Security – 802.11, Bluetooth, and Handheld Devices”, 2002
2. Center for Internet Security, “Wireless Networking Benchmark (version 1.0)”, April 2005
3. Planet3 Wireless, “Certified Wireless Network Administrator, Official Study Guide (3rd Edition)”, Berkeley, Ca. Osborne, 2005
4. Planet3 Wireless, “Certified Wireless Security Professional, Official Study Guide”, Berkeley, Ca. Osborne, 2003
5. Gast, Matthew , “802.11 Wireless Networks, the Definitive Guide” 2nd Edition, Sebastopol, Ca. O’Reilly, 2005
6. Potter, Bruce and Fleck, Bob, 802.11 Security”, Sebastopol, Ca. O’Reilly,2002
7. Edney,Jon and Arbaugh,William, “Real 802.11 Security”, Addison-Wesley Professional, 2003
8. Cisco Press, “Cisco Wireless LAN Security”, Cisco Press, Indianapolis, In, 2004

Introduction:

The purpose of this paper is to offer guidance to the residential on creating a secure 802.11 wireless network environment. Today most Wireless Access Point hardware that is sold for the home user is preconfigured in a way to make it extremely simple to get a wireless connection established quickly. Unfortunately for the general population this ease of setup means that most all of the security features available in the Wireless Access Point hardware are turned off by default. This paper cannot document all the possible settings for all vendors of 802.11 Wireless Access Points; however it will attempt to provide guidance on the features that you should be looking to enable or disable to build a more secure Wireless LAN environment. You will need to consult your vendor’s documentation for exact steps to configure these settings.

Since 802.11 wireless networking is a fast developing technology and new risks are being frequently discovered; because of this it is important to employ a Defense-In-Depth strategy when creating security for wireless networks. What this means setting up your security controls so that they overlap so that in the event a new exploit renders one layer of security vulnerable there are others that are still providing you protection.

Many people feel their home network is at a low risk for attack, but if you have an open Wireless Access Point on your network you are inviting unnecessary risk. As wireless technology has seen wider deployment many people have realized that they can transfer the risk of spamming, illicit downloads and illegal activity to someone else by doing it through their open wireless Access Point. If the ISP detects and tracks the illegal activity to the source address, then that address can be that of the unsuspecting homeowner who will have a lot of questions to answer.

These risks can be mitigated by taking the precautions outlined below. None of these settings are going to make you impervious to attack, however the name of the game for the average home user is to make yourself a less attractive target than the folks down the street, who have taken no precautions at all.

Checklist

No.	Control
1	<p><u>Use Anti-Virus</u> – Ensure all systems accessing the wireless network have an Anti-Virus program installed</p> <ul style="list-style-type: none"> • Software should download and apply updated virus signatures at least once a week. • Schedule regular full scans of the system at periods of low activity
2	<p><u>Use Personal Firewall software</u> - Ensure all systems using the wireless network have a personal firewall installed. Use of a firewall is advisable to prevent malicious traffic from one station on the wireless network from reaching other hosts on the wireless network.</p>
3	<p><u>Change the Default SSID of the Access Point</u> - All manufacturers assign a well known default SSID to their access points. If a hacker sees the factory default SSID they commonly expect that it is also likely that many or all of the other settings of the AP are in their default factory configurations, and that the AP will be easy to compromise.</p> <ul style="list-style-type: none"> • Do not use personally identifying information such as your name, address, or phone number in your SSID. The SSID is visible using a packet sniffer or wireless detection tools from any station within radio range. Don't assume no one will ever see what you set your SSID to!
4	<p><u>No SSID Broadcasting</u> – Disabling SSID broadcast means that the SSID of the network will not be sent out in every beacon packet sent by the AP. This screens your SSID from casual viewing by wireless discovery tools that depend on probe responses. It is not however a foolproof security mechanism, when a station associates to the AP it still transmits the SSID so it can still be discovered by tools such as Kismet (http://www.kismetwireless.net/index.shtml).</p>

5	<p><u>Restrict the DHCP pool or use static TCP/IP addressing internally</u> – If an unauthorized user does succeed in penetrating your wireless network restricting the TCP/IP addresses that can be assigned dynamically to the minimum number needed for your own network may deny the attacker the ability to receive an address. Alternately you could use static addressing and disable DHCP altogether so the attacker is forced to attempt to guess what is a valid address range and free address before attempting to make use of your network.</p>
6	<p><u>Lower the AP power to the minimum level needed to support your connectivity needs</u> - for home use, residential quality Access Points often provide more power than is needed. Take a walk with your laptop and see how far away from your access point you can be and still have a connection. If you only need wireless coverage in one or two rooms consider lowering the power levels so that the signal is not broadcast much further than the area you need to cover. Remember a standard AP broadcasts in a 360 degree circle, if you have a requirement for coverage in a long narrow area consider employing a directional antenna to minimize the signal in areas you do not need wireless coverage in. This can be especially important in apartment buildings and multi-family houses.</p> <p>If the signal is not available in an area the hacker can reach, then they cannot attack your wireless network.</p>
7	<p><u>Encryption</u>– Use the strongest encryption practical for your network. It is tempting to think that there is nothing requiring the protection of encryption on a home network, however the use of encryption can serve 2 important roles in your wireless network:</p> <ol style="list-style-type: none"> 1. Take the place of a warning banner to indicate that the network is not free for public access. There have been many arguments over the use of private but unsecured wireless networks for free internet access. So far they have not been tested in a court of law so the exact legal status is unclear. However it seem uncontestable that if the attacker had to break the encryption you have configured in order to make use of your network, then they clearly had to know they where not supposed to be accessing that network. 2. Deter people looking for free internet access. While in some cases these people are simply looking for a place to check their e-mail, many malicious users have discovered that they run a lot less risk being caught sending spam and downloading illicit materials if they use someone else’s network to do it. If their traffic is caught, it will be traced to the account of the person who subscribes to that cable modem or DSL line

	<p>The exact encryption your wireless network can support will depend on the make and model of your access point and wireless cards. The standards are continuing to evolve and new equipment makes its way to the market. The following is a listing of encryption mechanisms in descending order from strongest to weakest:</p> <ul style="list-style-type: none"> • WPA2 • WPA2-PSK • WPA • WPA-PSK • WEP with 802.1x (dynamic WEP) • WEP <p>WPA2 uses Advanced Encryption Standard (AES) encryption; it is only available on newer hardware that supports AES. WPA uses Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC) to address the shortcomings of WEP. Both WPA and WPA2 offer a Pre shared Key (PSK) version which is intended for the homeowner who does not have an authentication server available. The Pre Shared Key is a similar to a WEP key but mechanisms allow for it to be rotated automatically while in use making it harder to break.</p>
8	<p><u>Change Encryption Keys</u> – If you are using WEP or any of the pre-shared key (PSK) variations of WPA, it is advisable to change the encryption keys occasionally to thwart attempts to break the keys. This is most important with WEP which uses a single key for encrypting all traffic from all stations. WPA derives multiple keys from the passphrase you enter and rotates it during use making it more secure. Be sure to use strong pass phrases to make them harder to crack.</p>
9	<p><u>MAC Address Filtering</u> - MAC address filtering is a way to restrict the wireless cards that can connect to your wireless network using their hardware address. This tool has fallen out of favor with many security professionals as hardware addresses are easy to spoof by an attacker, and the authorized addresses are broadcast in the clear when the client is connected so an attacker can easily determine what an allowed address is. There is still value in this setting for a residential user:</p> <ul style="list-style-type: none"> • A residential network may have many hours per day when it is idle. There will be no authorized client traffic for an attacker to gather MAC addresses to spoof from. This is a deterrent to the person looking to make use of a free internet connection. • It is an additional layer in a defense-in-depth strategy. A hacker can identify an authorized MAC address to use, but is it worth his time? Or will he simply move to the next network that doesn't require him to

	<p>jump through the extra hoops?</p> <p>This setting is reasonable for a residential network that is only likely to have a handful of systems connecting to the wireless network since it requires you to track the hardware (MAC) addresses of all wireless cards. It does not scale up well and is seldom used in the corporate world.</p>
10	<p><u>Wireless Client Isolation</u> – The wireless networks is a shared medium similar to a network hub, all stations on the wireless network can see all the traffic on the network. Some AP's offer a feature called Wireless Client Isolation, this feature prevents the stations from communicating with one another through the Access Point. This is a more secure configuration since any station that is infected with a virus or a worm is unable to spread that infection to other stations on the wireless network.</p> <p>This feature is not available on all Access Points check your vendors documentation.</p>
11	<p><u>Enable Logging if possible</u> – Most residential grade access points offer the ability to send logs to another machine. If you have a system that can receive them, this can be important information to collect for troubleshooting network problems and also for identifying security issues. Check your logs periodically for signs of failed associations and unknown clients.</p>
12	<p><u>Power off the Transmitter when not in use</u> – If your wireless network is not going to be used for an extended period of time (While you are at work or away on vacation) it is a good practice to disable the wireless interface. No one can hijack your wireless connection if it is disabled.</p>
13	<p><u>Restrict the addresses allowed to manage the AP</u> – Many residential grade access points have configuration options to allow you to specify if the device can be managed from the Internet side of the router (for routers with integrated wireless capability) and others allow you to restrict to specific machines the ability to change the AP's configuration. It is dangerous to allow configuration changes to be made from the Internet, so this practice should be avoided. It is a good idea to restrict which stations are allowed to make changes to your AP's configuration unless you are in a pure DHCP environment.</p>



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS London 2009	London, United Kingdom	Nov 28, 2009 - Dec 06, 2009	Live Event
SANS WhatWorks in Incident Detection Summit 2009	Washington, DC	Dec 09, 2009 - Dec 10, 2009	Live Event
SANS CDI East 2009	Washington, DC	Dec 11, 2009 - Dec 18, 2009	Live Event
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2010	New Orleans, LA	Jan 07, 2010 - Jan 12, 2010	Live Event
SANS Security East 2010	New Orleans, LA	Jan 10, 2010 - Jan 18, 2010	Live Event
SANS AppSec 2010 and WhatWorks in AppSec Summit	San Francisco, CA	Jan 29, 2010 - Feb 05, 2010	Live Event
SANS Phoenix 2010	Phoenix, AZ	Feb 14, 2010 - Feb 20, 2010	Live Event
SANS Tokyo 2010 Spring	Tokyo, Japan	Feb 15, 2010 - Feb 20, 2010	Live Event
SANS Geneva CISSP at HEG 2009 Autumn	OnlineSwitzerland	Nov 23, 2009 - Nov 28, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced