BLACKTHORN SYSTEMS

5921 Shelburne Road
Shelburne, Vermont 05482-6504

(802) 985-2415
(802) 985-1139 FAX
www.blackthornsystems.com
email: info@blackthornsystems.com

Wireless Networking Basic Security Checklist

Home User version

by Frank Thornton

Written with the help and co-operation of the Members and Moderators of the NetStumbler forums and the fine people at WarDriving Central. Additional input was provided by a number of individuals. My thanks to all.

The intended audience for this document is the home owner who currently has, or intends to install a wireless network in the immediate future.

One of the worst mistakes a new user to wireless networking can make is to just set up the equipment and use it right out of the box. By doing so, they have very likely opened their whole network and Internet access to anyone else with wireless connection. In an effort to make wireless networking "user friendly," most WLAN manufacturers have rendered ***consumer-level wireless equipment COMPLETELY UNSECURE out of the box***. Making a home wireless network more secure is possible. However it takes some work, and you MUST read the instructions that are often hidden in the back of the manuals.

You should always assume everything going over the air is open to anyone with the right configuration and equipment. Use wireless as the last viable option.

To help secure your home wireless network you should consider doing all of the following:

1. **Change ALL the default settings on your Access Point, wireless cards, and routers.** These include the SSID, Administrative passwords and User passwords. The default names and passwords are published by the manufacturers on the Internet and are available to anyone.
    - Choose an SSID (Network Name) that will not attract unwanted attention. Do not use your telephone number, family last name, the name of the residence, the address of the residence, etc.
    - Choose a unique SSID.
    - Disable Automatic SSID Broadcast. If you have more than one AP set up to allow roaming, you might not want to do this due to technical considerations. However, most users should consider this option.
    - Change the default channel. While this is not truly a security issue, it may help with radio interference, as many devices use the same channel.
2. **Always use encryption (WEP or WPA) on your wireless network.** If possible, use a 128-bit or higher variation.
    - Whenever possible, use additional encryption such as SSL or VPN.

- Change the encryption key on a periodic basis.
- *NEVER* use the SSID (Network Name) as the Encryption Key.

3. If the following features are part of your AP or router, make sure you use them:
   - **Firewall:** Restrict wireless usage to only the minimum TCP and UPD ports needed. And disable all other ports. For example, you may wish to enable TCP Port 80 (HTTP), and TCP Port 110 (POP) yet disable TCP Port 25 (SMTP) to prevent becoming a wireless mail relay, and TCP Ports 20, 21 (FTP) to prevent unauthorized file transfers. Also, block file sharing ports for programs such as Kaaza.
   - **Address Control List:** The ACL limits the Machine Address Code addresses that may access your AP. Each wireless Network Interface Card has a unique MAC address, so this limits which wireless NICs (and therefore which computers) may access your network.
   - If a fixed number of mobile devices are connecting to the AP, **disable DHCP** and use static IP addresses.
   - If a varying number of devices will be on the wireless network segment, **limit the size of the DHCP address pool** to the absolute maximum number of needed addresses. Many people use DHCP to make it easier on the users. However, there is no need to for the network to give out 254 addresses, or even 30, if you only need 3.
4. Most Access Points have built in logging. Periodically, **review the access logs** and look for any abnormalities.

Glossary:

ACL – Access Control List
AP – Access Point
DHCP- Dynamic Host Configuration Protocol
FTP – File Transfer Protocol
HTTP – HyperText Transfer Protocol
MAC – Machine Address Code
NIC – Network Interface Cards
POP – Post Office Protocol
SMTP – Simple Mail Transfer Protocol
SSID – Service Set Identifier
SSL – Secure Socket Layer
VPN – Virtual Private Networks
WEP – Wired Equivalent Privacy
WPA – WiFi Protected Access
WLAN – Wireless Local Area Network

Copyright © 2003 Blackthorn Systems and Francis J. Thornton, Jr.