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

Small Business 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 small business 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 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 most wireless networking equipment ***COMPLETELY UNSECURE out of the box***. Making a 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 business' 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 that will not attract unwanted attention. For example, an SSID of "Rm125" is less apt to attract criminals as opposed to "Accounting Department Wireless".
    - 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. WLAN isolation: Treat all APs as UNTRUSTED and as such, locate the wired network connection of any AP on its own firewall or firewall interface. This firewall should have rules for both the WLAN and internal LAN access.

3. Always use encryption (WEP or WPA) on your wireless network. If possible, use a 128-bit or higher variation. If WPA is available for your equipment, then update all firmware and switch to WPA.

    - 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.Use proven security measures such as VPN, SSL, etc.
    - If using WEP, run the systems as an Open Key rather than Shared Key. While this may seem counterintuitive due to the names, Open Key systems are actually the more secure of the two types of key systems. In a Shared Key network, the data exchange is easily attackable, revealing the key. Also, do not use common words as a key. Create keys as you would a strong password, mixing alpha and numeric characters.

4. Design the WLAN to limit RF propagation to only those areas needed for coverage. Choosing the correct antenna and RF power levels can also help limit the RF footprint. Limiting the RF footprint to only needed areas will help minimize access to the WLAN by unauthorized persons who are outside the building or grounds.
5. Consider disabling Automatic SSID Broadcast. This may cause performance problems for those with a multiple AP setup for fast roaming. This may also cause problems for businesses running VoIP on 802.11. However, this will help make your WLAN less likely to be discovered to the casual wireless user.

6. Restrict wireless usage to only the minimum TCP and UPD ports needed by the users to meet job requirements. 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.

7. Use a MAC based ACL. Maintain an updated list of current MAC addresses.

8. If a fixed number of mobile devices are connecting to the AP(s), disable DHCP and use static IP addresses.

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

9. If a floating number of devices will be on the wireless network segment, do not size of the DHCP pool to the absolute maximum number of needed addresses, and use proper subnetting to limit the determine the number of clients

    - Limiting the DHCP pool limits the amount of leases handed out.
    - The subnet mask determines the limit of the amount of clients.
    - Limiting the subnet will add a little tighter security, although if an attacker knows subnets, it will just slow him down. There is nothing to prevent someone who understands subnetting to manually entering an IP address and submask within the proper range.
    - Part of the idea of this Security checklist is to give a little balance on the security side. Many people use DHCP to make it easier on the users. This just helps even that out. i.e. Don't hand out 254 addresses, or even 30, if you only need 3.

10. Authenticate users via a system such as RADIUS or NoCat. Restrict access to the network until the user is authenticated.
11. Perform regular network scans on both the LAN and WLAN for "rogue" APs.
12. Perform regular audits and review LAN and WLAN logs:

    - Check the DHCP logs for rogue APs.
    - Check the DHCP logs for rogue clients; odd MAC addresses that have associated and de-associated.
    - Maintain and regularly audit AP access logs
    - AP logs for exception alarm (SNMP) messages.

13. As a standard policy, restrict the use of wireless NICs to authorized personnel only.
14. Integrate the Network User/Security Policies for both wireless and wired networks.

Not all of the above may apply to your situation, depending on the systems and network. For example, the hand-held wireless terminals used by many popular warehouse management systems are incapable of several of using Virtual Private Networking. The hardware used by these systems only has enough processing power to run the built-in firmware.

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

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
RF - Radio Frequency
SMTP – Simple Mail Transfer Protocol
SSID – Service Set Identifier
SSL - Secure Socket Layer
VoIP – Voice over IP
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.