

Closing the Loop: Extending Wireless LAN Security to Wireless Printers



A ZEBRA BLACK&WHITE PAPER





Copyrights

©2006 ZIH Corp. All product names and numbers are Zebra trademarks, and Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. All rights reserved. All other trademarks are the property of their respective owners.

Unauthorized reproduction of this document or the software in the label printer may result in imprisonment of up to one year and fines of up to \$10,000 (17 U.S.C.506). Copyright violators may be subject to civil liability.



Executive Summary

Wireless network security is continually evolving and improving, and the protection available for Zebra wireless printers is keeping pace. Many effective options have been developed to protect wireless LANs since security problems first surfaced several years ago. Loopholes in the original IEEE 802.11b wireless LAN standard have been closed and new protections have been developed to provide protection against other threats. The higher-bandwidth 802.11g wireless networking protocol provides even more opportunities to strengthen security. Zebra Technologies has extended these protections to its mobile printers, so customers using Zebra printers can benefit from the same security used to protect their access points and mobile computers.

Enterprises should not overlook wireless printers when assessing network security. The print jobs and data streams communicated to a wireless printer probably don't include sensitive enterprise data, but an unsecured or under-secured wireless printer could provide hackers with an easy back door into the enterprise network.

This white paper will outline the basics of wireless security and describe how Zebra products support leading standards and protocols. The security methods discussed in the paper are all for 802.11-standard networks except as noted.

Wireless Security Basics

Three things must happen to secure a wireless network: network traffic must be protected during transmission (encryption), unauthorized devices must be prevented from getting on the network (authentication) and authorized devices must be protected against being tricked into transmitting to an unauthorized device.

Encryption protects data in transmission. Data is encrypted by encoding it with an algorithm and it is then decoded with a "key." Matching keys are stored on each device and access point. Encryption keys can be changed frequently. Analyses of successful wireless LAN attacks have found that users increase the vulnerability of their networks by failing to change keys regularly, or by not enabling them at all.

Authentication prevents rogue devices from gaining access to the network, and prevents rogue access points from collecting transmissions from network devices. Authentication can be performed with a simple password or more sophisticated algorithms. The most secure networks employ mutual authentication, where the mobile device and access point must each authenticate themselves with the other before any network transmission can take place.

Some security standards and methods combine authentication and encryption. For example, the IEEE 802.1x framework and 802.11i standard both require authentication and encryption, and define a range of accepted protocols for each. Virtual private networks (VPNs) also combine encryption and authentication.

Dozens of encryption and authentication protocols, standards, techniques and products are available to secure wireless LANs, and there are many ways to combine them, thus creating a confusing array of options. The best way to navigate the choices is to determine how much security is needed, and then to find the solution that best meets the enterprise needs.

Zebra defines the wireless LAN security landscape by different levels, ranging from Level 0 (no or practically no security) to Level 4, which is considered the most secure. Most enterprises consider Level 2 or Level 3 security (see table below) sufficient for their wireless LANs. Unfortunately, many systems are only protected by WEP, the default for 802.11b-standard equipment. WEP has proven vulnerable to hackers and was exploited in several of the highly-publicized wireless LAN security breaches, creating a misperception that wireless LAN technology is inherently insecure. An overview of wireless LAN security levels is presented in Fig. 1 below.

Fig. 1 Wireless LAN Security Levels

Level	Type of Protection	Common protocols
0	Secret service set identifier (SSID)	No security
1	WEP (Wired Equivalency Privacy) encryption only	Basic 40- or 128-bit encryption
2	WPA (Wi-Fi Protected Access) encryption + authentication; WPA2	802.1x authentication – EAP-TLS, EAP-LEAP, EAP-TTLS, EAP-FAST, EAP-PEAP. Supported encryption includes TKIP, MIC and AES (in WPA2).
3	VPN (Virtual Private Network) encryption + authentication	Advanced authentication and encryption
4	802.11i encryption + authentication	Advanced AES encryption plus 802.1x authentication

The following sections provide an overview of common wireless securities, techniques and implementation methods and describe how they can be implemented on Zebra printers. Figure 2 provides a quick reference to security protocols available for Zebra printers as of June, 2006. Zebra wireless printers use radio cards from different manufacturers, including Cisco Systems and Symbol Technologies.

Encryption

Common encryption protocols include Wired Equivalency Protection (WEP), Advanced Encryption Standard (AES), triple-DES (3DES), Temporal Key Integrity Protocol (TKIP) and Secure Socket Layer (SSL).

The original 802.11b standard provided encryption with WEP, which was intended to provide the same level of protection as a wired Ethernet network. In many cases users did not turn on encryption when they originally configured the network. WEP offers up to 128-bit encryption, but most enterprises, if they enabled WEP in the first place, used the default 40-bit encryption setting.

The 802.11 standards committee went back to work to close the security loopholes that were discovered in the original 802.11b standard. One of the results was the creation of Wi-Fi Protected Access (WPA), a standard that is backward compatible with pre-existing 802.11b hardware, and forward compatible with the 802.11i wireless security standard. WPA strengthens security significantly by using TKIP encryption. WPA2 is a follow-up standard that includes even stronger AES encryption. WPA2 is part of the 802.11i standard. Both WPA and WPA2 also add various different authentication protection mechanisms.



Zebra Encryption Support

All Zebra 802.11b and 802.11g wireless printers include 40- and 128-bit WEP encryption support as a standard feature. Zebra QL, QL Plus and RW series mobile printers also offer WPA encryption with TKIP. WPA2 or 802.11i is available on Zebra 802.11g radios for QL Plus and RW series printers. Zebra also supports virtual private network (VPN) technology to provide additional encryption protection for mobile printers.

A u t h e n t i c a t i o n

Numerous protocols are available for wireless devices and access points to authenticate that they are communicating with authorized devices. One of the most important and widespread authentication protocol that has emerged is 802.1x, which was created by the IEEE standards committee. Note that 802.1x does not define a specific form of authentication, rather it is a standardized framework that supports multiple port-level authentication methods.

802.1x requires the use of Extensible Authentication Protocol (EAP). There are several variations of this protocol. Some of the best known are: EAP-LEAP (Lightweight Extensible Authentication Protocol), which was created by Cisco Systems and is used in its wireless networking equipment; EAP-TLS (Transport Layer Security); EAP-PEAP (Protected Extensible Authentication Protocol), supported in Microsoft Windows operating systems; and EAP-TTLS (Tunneled Transport Layer Security). The various types of EAP are not interoperable, which means all the devices used in the network must have the same form of EAP.

Zebra Authentication Support

Zebra supports multiple EAP protocols that enable Zebra printers to be included in 802.1x security systems. LEAP authentication is available throughout Zebra's mobile and stationary product line, so Zebra printers can be included and secured in Cisco wireless networks. EAP-TLS, EAP-TTLS, EAP-FAST and PEAP support are available for QL Plus and RW series printers. PEAP support will aid integration into Windows systems, which support PEAP security.

WPA provides authentication and encryption and is available for QL, QL Plus and RW series mobile printers. WPA2 is available for QL Plus and RW mobile printers with 802.11g radios.

Zebra also supports VPN implementations that offer their own forms of authentication. These will be described in more detail later in this paper.

Symbol Technologies includes Kerberos security in the radio cards it manufactures, therefore Zebra mobile and stationary printers with Symbol radios support Kerberos and can be used in Symbol wireless networks.



802.1x

802.1x is a flexible authentication framework that requires the use of a RADIUS server, enhanced encryption and EAP-based authentication. RADIUS servers provide mutual authentication and block traffic from unauthenticated devices from reaching the wired network. The 802.1x standard permits the use of multiple forms of EAP, but all devices in the system must use the same form. When it was created, the 802.1x framework fixed all known security loopholes in the original 802.11b standard. 802.1x can also be used on 802.11g networks. The 802.11i security standard, which provides even stronger protection, requires the use of 802.1x authentication.

Zebra 802.1x Support

Zebra's QL, QL Plus and RW series printers meet all the criteria for use in 802.1x-protected networks. Refer to Fig. 2 for a list of Zebra's 802.1x-compliant products.

Virtual Private Networks (VPNs)

VPNs were created to provide a secure, private connection over a public network (such as the Internet) and have been adapted to provide very secure wireless LAN communication. Wireless LAN VPNs bundle encryption and mutual authentication into a single system. VPNs are often described as secure “tunnels” that network traffic can pass through without danger of interception. Once everything has been authenticated, communication is encrypted and routed through the “tunnel” created by the VPN.

VPNs are a type of security, not a specific protocol, so there is no interoperability among different brands. Virtual private networks may be standards-based or employ proprietary encryption and authentication methods. Proprietary VPNs are optimized to protect a specific network infrastructure environment. Standards-based VPNs typically feature standardized encryption and authentication protocols, but do not necessarily ensure compatibility or interoperability among all the wireless equipment that share the protocols.

VPNs may use SSL, IPsec or other types of encryption. SSL implementations only enable communication with applications that are coded for SSL, including Web browsers. IPsec VPNs support all applications and network resources.

Zebra VPN Support

Zebra currently offers a TTLS-based Zebra VPN client for QL, QL Plus and RW series mobile printers that work with AirBEAM Safe VPN from Symbol Technologies.

802.11i

The IEEE 802.11i standard was ratified in July, 2004 and provides security for 802.11 networks. 802.11i builds on the WPA standard development and requires the use of 802.1x authentication. A key feature of 802.11i is that it requires the use of the Advanced Encryption Standard (AES), a very powerful encoding algorithm. AES makes 802.11i highly secure, but may be hard to deploy on legacy networks because of processor and bandwidth limitations.

Most 802.11b radios currently deployed in mobile computers and printers lack sufficient processing power to efficiently handle AES encryption. The result is slow performance that is unacceptable for mobile enterprise applications. Newer-generation radios that support the high-speed 802.11g wireless network standard (which is backward-compatible with 802.11b) have processors that can easily handle AES encryption and thus make 802.11i implementation practical.

Zebra 802.11i Support

Zebra supports 802.11i in the optional 802.11g radios available for QL Plus and RW series mobile printers. Figure 2 shows available security protocols for various Zebra wireless printers.

Fig. 2: Quick reference to supported wireless security protocols for Zebra printers

Security Features	Symbol 802.11b radio	Cisco 802.11b radio	Symbol 802.11b radio	Zebra 802.11b radio	Zebra 802.11g radio	Zebra 802.11b radio
WEP	Yes	Yes	Yes	Yes	Yes	Yes
802.1x Authentication						
LEAP	Yes	Yes	Yes	Yes	Yes	Yes
EAP_FAST	Yes	No	Yes	Yes	Yes	Yes
PEAP	No	No	Yes	Yes	Yes	No
EAP-TLS	No	No	Yes	Yes	Yes	No
EAP-TTLS	No	No	Yes	Yes	Yes	No
WPA with TKIP*						
with LEAP	Yes	Yes	Yes	Yes	Yes	Yes
EAP-FAST	Yes	Yes	Yes	Yes	Yes	Yes
PSK	Yes	Yes	Yes	Yes	Yes	Yes
PEAP	No	No	Yes	Yes	Yes	No
EAP-TLS	No	No	Yes	Yes	Yes	No
EAP-TTLS	No	No	Yes	Yes	Yes	No
IEE 802.11i (WPA2)						
with EAP-RLS, EAP-TTLS, LEAP, PEAP or EAP-FAST	No	No	No	No	Yes	No
VPN (AirBEAM Safe)	Yes	Yes	Yes	Yes	Yes	Yes

* WPA-TKIP cannot be ordered standalone. It is included with WPA-PSK and WPA-LEAP authentication.



Managing Security on Zebra Printers

Wireless security is dynamic, with new standards and protocols being developed and gaining support from leading equipment manufacturers. Only a few years ago, WEP was the leading security protocol for 802.11 networks and the AES encryption was intended for top-secret government and military applications. Today, the security on many wireless home computers surpasses WEP protection, and AES is a part of the WPA2 and 802.11i standards intended for enterprise use. Wireless infrastructures—including printers and their management tools—must be flexible enough to facilitate change so users can easily implement the latest upgrades and options to optimize their network security.

Zebra offers powerful management options that make it simple to deploy, monitor, configure and upgrade security protocols on Zebra printers. Zebra's Label Vista software can be used to configure Zebra mobile printers. Select Zebra mobile printers can also be managed with Wavelink Corp.'s Avalanche software, which provides a complete management environment for multiple types of wireless devices from different manufacturers.

Using Wavelink Avalanche, system administrators can remotely implement software updates and security upgrades, configure devices and modify settings for QL Plus and RW series mobile printers, mobile computers, and other wireless devices. Wavelink-enabled wireless Zebra mobile printers enable IT administrators to maintain complete visibility and control over the devices from a single, remote console—without ever having to physically touch the printers. The ability to effectively manage and secure all types of mobile devices from a single point significantly reduces the support costs across an enterprise's wireless network.

Conclusion

There is no reason for a printer to be a weak link in wireless network security. System administrators should not compromise on printer security and should commit to models that support the enterprise's preferred or standard security protocols. Enterprises should also insist on printers and management tools that offer convenient management and upgrades.

Zebra supports many leading encryption, authentication and VPN implementations so users can extend the same safeguards to their printers as they do to the rest of their wireless infrastructure. Custom development to support additional protocols is also available. Zebra's management tools for deploying and configuring printers, status monitoring, and managing downloads and upgrades helps reduce total cost of ownership for the print system and makes it cost-effective to update printers with the latest network security. For more information on Zebra security support, printers, connectivity and management solutions, visit www.zebra.com.



Notes



Notes



Notes



Zebra Technologies

333 Corporate Woods Parkway
Vernon Hills, IL 60061-3109 U.S.A.

T: +1 847 793 2600 or +1 800 423 0442

F: +1 847 913 8766

www.zebra.com

GSA#: GS-35F-0268N

©2006 ZIH Corp.

#13897L (7/06)