WHITE PAPER

Beyond Retail: The Imperative for Ubiquitous Security in Wireless Printers . . .

While the importance of enhanced security and encryption protocols for wireless hardware has long been understood in the retail industry, where identifying theft and credit card fraud are well-known and well-publicized security concerns, the need for protective technology is now pervasive across all industry as the network threat environment has evolved. This concern includes wireless local area networks (WLANs) and associated hardware, such as wireless printers.

According to Forrester Research, the network perimeter has disappeared in the current threat environment. Insiders are as great a danger as outsiders.[1] As such, companies need to include wireless printers when assessing their overall network security, not only because of the data communicated to those printers, but because they can provide vulnerable entry points into the corporate network if not properly secured.

The situation becomes more critical as more enterprises move to WLANs. "We continue to see migration from traditional local area networks with hard-wired data capture devices to wireless networks supported by converged AIDC, including barcode, RFID, voice recognition, video, and powered carts," says Umesh Cooduvalli, senior product manager at Datamax-O'Neil.

CONTENT ■ ■ ■

Söluaðli:

Boðtækni

www.bodtaekni.is

datamax·o'neil™

right by our customers.

While the cost of retrofitting a large warehouse with the latest automatic identification and data capture (AIDC) technology is a major undertaking, and the ROI timeframe may make the barrier to entry rather high for many in the current economic climate, the technology nonetheless is gaining strong momentum. The reasons are clear:

- The technology can lead to improved efficiency and throughput through process automation and coordination, particularly in receiving, picking, packing, staging, and shipping.
- Companies are improving storage utilization and inventory counting by having warehouse operations couple wireless sensors, video monitoring, and task management software designed to improve workflow.
- Faster data entry, improved accuracy, and immediate error correction is being enabled. Since warehouse efficiency is measured in velocity and accuracy, eliminating batch-based scanning and printing solutions addresses these metrics head on.
- Headcount is reduced through the elimination of redundant data entry, while higher productivity levels are achieved through simplified, streamlined task management.
- Travel time is driven down. By enabling data capture and on-demand printing at the point of application, warehouse operators can quantify hourly savings while eliminating mistakes that can have a material impact on operating expenses.[2]

Driven by the need to secure and protect these benefits while preventing the breach of company data, wireless security standards have developed rapidly, as has demand for embedded encryption on wireless devices such as printers. “We knew there would be demand for authentication and encryption i n the retail industry; but demand soon appeared in the automotive industry,” says Cooduvalli. “This was followed by transportation, logistics, and warehousing applications. Wireless security, and specifically 802.11 b/g WLAN with WPA2 security protocols, became a requirement everywhere wireless technology was being applied.”

The Evolution of Wireless Security Standards ■ ■ ■

IEEE 802.11 is a set of standards for implementing WLAN computer communication in the 2.4, 3.6, and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard, IEEE 802.11-2007, has had subsequent amendments. These standards provide the basis for wireless network products using Wi-Fi technology.

Since 1997, 802.11 wireless standards have moved from the embedded native authentication and standard WEP encryption to a veritable alphabet soup of authentication and encryption protocols. Driven by the need to protect against breaches in an ever-more threatened network environment, protocols to protect wireless data have emerged in the market at an exponential pace. Consequently, providers of wireless components must be authoritative experts in the latest wireless security technologies.

Providers must also remain vigilant and knowledgeable about the progress made by hackers and other threat vectors in developing methods to access propriety information contained within wireless networks. It is critical for anyone with a WLAN to work with a partner equipped to address the security concerns associated with wireless business enhancement tools.

Authentication Protocols

Authentication is the process of verifying that someone/something is authentic (i.e., that the claims they make are true). Authentication protocols are used to confirm computers in possession of a cryptographic key and users. Authentication stops rogue devices from obtaining 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. These protocols cover everything from default encryption standards such as 64-bit WEP to a variety of standard and proprietary controls. Common authentication protocols include LEAP, Kerberos, and WPA/WPA2 Enterprise.

Wireless Encryption Protocols

Encryption transforms data from a readable form to a nonreadable form for humans. It prevents eavesdropping of wirelessly transmitted data. The key length is an indicator of the strength of the encryption algorithm. Examples include RC4 (Rivest Cypher 4), Data Encryption Standard (DES), Triple-DES, Blowfish, International Data Encryption Algorithm (IDEA), Software-Optimized Encryption Algorithm (SEAL), RSA (Rivest Shamir Adelman), and RC4.

The most basic wireless networking encryption protocols are Wired Equivalent Privacy (WEP) and the interoperable Wi-Fi Protected Access (WPA). WEP encrypts data before it is transmitted across a wireless network. Only devices that have a valid WEP key can decrypt the data. The Wi-Fi Alliance introduced WPA in 2003 based on Draft 3 of the IEEE 802.11i amendment.

In July 2004, the IEEE approved the full IEEE 802.11i specification, which was quickly followed by a new interoperability testing certification from the Wi-Fi Alliance known as WPA2. WPA2 is based on the Robust Security Network (RSN) mechanism, which provided support for all the mechanisms available in WPA, as well as the following:

- Strong encryption and authentication support for infrastructure and ad-hoc networks (WPA is limited to infrastructure networks)
- Reduced overhead in key derivation during the wireless LAN authentication exchange
- Support for opportunistic key caching to reduce the overhead in roaming between access points
- Support for pre-authentication, where a station completes the IEEE 802.1X authentication exchange before roaming
- Support for the CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) encryption mechanism based on the Advanced Encryption Standard (AES) cipher as an alternative to the TKIP protocol

Mitigating Risk

Unless strong wireless security measures are taken, companies may risk exposing their proprietary information to competitors or having customers' financial data and other sensitive information compromised by breaches. To avoid such disastrous circumstances, it is vital to implement wireless security measures.

In any wireless network, access points give wireless devices, such as scanners, mobile computers, and printers, access to the heart of the operation: the network servers that store and distribute information. Each of these wireless devices, whether sending information (e.g., scanners), receiving information (e.g., printers), or both (e.g., mobile hand held computers and printers with card readers) can associate with the network once it is within range of the access point. It is incumbent on the server to ensure that the device is a trusted part of the store-managed equipment, and authenticate it, before it is allowed access to the network. Finally, to protect the communication links between trusted devices and the network server, the data is encrypted to render it unusable in the unlikely event it is somehow intercepted.

Datamax-O'Neil WLAN Security Support

Datamax-O'Neil H-Class stationary high performance industrial printers and A-Class print engines are offered with 802.11 b/g W-LAN with WPA2 security protocols.

Datamax-O'Neil also provides a W-LAN option DMXrfNet III that replaces the DMXrfNet II version for high performance industrial H-Class printers and A-Class *Mark II* print engines.Users are now able to connect to 802.11 b/g networks right out of the box with a single IP address. The new W-LAN option supports the following security protocols:

A-Class Printer

	WEP	WPA	WPA2
Modes		PSK, Enterprise	PSK, Enterprise
Security / Encryption	64/128	TKIP / RC4	CCMP/AES
Authentication	WEP64, WEP128	PSK, LEAP, LEAP64, LEAP128, PSK64, PSK128, WPA2-PSK, TLS, PEAP, TTLS	

All shipments of H-Class printers and A-Class print engines with the W-LAN option come with the new option card. The new W-LAN option is also available as a field installable kit. (For complete specifications, operation, and installation instructions refer to Datamax-O'Neil technical resource document 92-2573-01, available at www.datamax-oneil.com.)

Field Installable Option Kit - H-Class	
Legacy Kit # OPT78-2657-12	Replaced by New Kit # OPT78-2873-02
Note: New kits are downward compatible.	

H-Class Printer

The H-Class is ideal for high-volume label printing in manufacturing, warehouse, transportation, and high resolution labeling. H-Class reduces the total cost of ownership with its gear-driven design to provide rugged and reliable performance for 24/7 mission-critical services.

Conclusion ■ ■ ■

The need for 802.11-compliant encryption in wireless printers, once a concern essentially in the retail environment, has extended to virtually all markets as more widespread threats to network security have eliminated the traditional network perimeter associated with security.

Wireless in industrial environments poses problems that require multiple solutions and products, but at the same time enables new applications and services that drive down costs. Security is a paramount concern in protecting the competitive benefits available through wireless technology.

Therefore, wireless printers must incorporate the appropriate security technology to keep them from becoming weak outposts in the network environment, vulnerable to internal and external compromise. Reliability and security considerations must be taken into account before deploying printers in wireless networks. Datamax-O'Neil printers provide the industry's leading security protocols to meet today's requirements while the company's security development platform addresses future requirements as well.

Wireless security is a dynamic arena. The expansion of demand for encryption in printers is a vivid example of this changing environment. As requirements continue to evolve, operators of wireless networks will be advised to closely examine the security capabilities of the hardware they plan to implement, including its ability to respond quickly and effectively to an evolving security environment.

NOTES

1. Kindervag, John (January 24, 2011) "Pull Your Head Out of the Sand and Put It on a Swivel: IntroducingNetwork Analysis and Visibility," Forrester Research, Inc.
2. "End Users Increasing AIDC Budgets in 2011," March 2011, VDC Research.