



# The Importance of Enhanced Security and Encryption Protocols for Wireless Hardware

In the storefront, at the office, throughout the warehouse, and on the road, wireless technology is a critical tool for conducting and improving business. Yet, despite its ubiquitous presence in business, we still read, almost daily, about hackers breaking into large network databases—heightening concerns about identity theft and credit card fraud. Security risks associated with wireless networks have forced businesses to comply with new, more stringent regulations for network security and data encryption. This document outlines the risks your wireless network faces and summarizes current state-of-the-art wireless hardware security systems. It also highlights critical factors to consider when selecting hardware partners to protect your future investment in wireless technology.

## **CONTENT:**

- > The Business Case for Wireless
- > The Past, Present, and Future of Wireless
  - The Risk
  - Understanding the Basic Wireless Security Process
  - Authentication Protocols
  - Encryption Protocols
  - Certifications
- > O'Neil's Portfolio

O'Neil Product Development, Inc.  
8 Mason, Irvine, CA 92618-2705  
Toll-free: 800.790NEIL  
Phone: 949.458.0500  
Fax: 949.458.0708  
Email: [info@oneilprinters.com](mailto:info@oneilprinters.com)

**WWW.ONEILPRINTERS.COM**

### The Business Case for Wireless

The use of 802.11 wireless devices has been a driving force in the advance of worker efficiency. It has also brought higher levels of service to retail and commercial customers alike. The unassailable benefits of wireless devices are driving the growth of 802.11 technology. According to the Wi-Fi Alliance, chipsets sold on an annual basis to support wireless technology will grow to one billion units by 2012 (Ref. ABI Research). Clearly, companies that ignore the value of wireless technology will be left behind as their competitors benefit from its many advantages. However, the use of wireless technology is not without risks, and astute companies will take measures to mitigate these risks before wholly embracing wireless devices.

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 guard company sensitive data from nosy competitors and ruthless hackers, protocols to protect wireless data have made their way to the market at an exponential pace. With so many protocols coming to market, it is incumbent on providers of wireless components to be authoritative experts in the latest wireless security technologies. Providers must also remain vigilant and knowledgeable about the progress hackers are making in developing methods to access propriety information contained within wireless networks. Today, more than ever, it is critical for anyone with a wireless network to work with a partner equipped to address the security concerns associated with wireless business enhancement tools.



### The Past, Present, and Future of Wireless

#### **The Risk**

Unless strong wireless security measures are taken, you are at risk of exposing your proprietary information to competitors. You are also at risk of having your customers' financial data and other sensitive information compromised by hackers. To avoid such disastrous circumstances, it is critically important to implement wireless security measures.



#### **Understanding the Basic Wireless Security Process**

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.

### **Authentication Protocols**

Authentication consists of a dynamic set of protocols. Authentication protocols cover everything from the default encryption standards such as 64 bit WEP (introduced with the first publishing of the 802.11 standard in the late '90s) to a wide variety of standard and proprietary protocols.

Today's Authentication Protocols include:

- > LEAP
- > Kerberos
- > WPA/WPA2 Enterprise (Wi-Fi Protected Access)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS

### **WPA/WPA2 Pre-Shared Key (PSK) Encryption Protocols**

Encryption also consists of a dynamic set of protocols. Encryption protocols cover everything from WEP, which has been easily breached for many years, to well-known industry protocols.

Today's Encryption Protocols include:

- > WEP (Wireless Equivalent Privacy)
- > TKIP (Temporal Key Integrity Protocol, also referred to as CCMP)
- > AES (Advanced Encryption System, also referred to as RC4)

### **Certifications (Wi-Fi, PCI, CCX)**

Whether you're in retail or manufacturing, Wi-Fi, PCI, and CCX are recognized, commonly used certifications. Certifications apply either to devices or applications.



Certification work is being conducted, as an ongoing process, by such entities as the Wi-Fi Alliance, Cisco Corporation, and the Payment Card Industry's Security Standards Council. The Wi-Fi Alliance and Cisco are known for having created certifications that apply to wireless devices. For instance, the Wi-Fi Alliance created the WPA and WPA2 certification levels, which combine authentication and encryption protocols. Cisco created the CCX, a proprietary certification that is required for wireless hardware components that meet a certain type or "class" of device.

The Payment Card Industry's Security Standards Council has created a Digital Security Standard (PCI-DSS) that defines behaviors required by its members to protect consumer data. The standard dictates practices for managing credit card data, defines minimum security standards for

wireless devices, and as a result, ensures a minimum level of data management security and provides minimum thresholds of wireless security. It is currently at level 1.2 revision released in October 2008. The certifications provided by these entities serve to protect wireless device users from the risks associated with data security. Failure to abide by these standards can result in potentially disastrous security breaches. Unlike other certifications, a hardware product such as a printer or handheld computer cannot be PCI compliant or certified by itself. PCI compliance is about total solutions, not products. It is up to the retailer, or security service provider they employ to validate a secure system with the PCI Security Standards Council. Once certified, a PCI solution is not static but must be managed and maintained on a regular basis to remain compliant.

The mix of industry standards and proprietary certifications is sure to expand over time as the hacker community adjusts its tactics to thwart industry-wide security measures. To sustain the integrity of your business data, it is essential that you choose a partner that can support your wireless security needs today and into the future.

