TECH TIP

A division of Chatsworth Products

The Payment Card Industry – Why Physical Protection is the Key to Securing the Wireless Network

In today's digital world, consumer preference for both online and in-person payment card purchasing is on the rise. Payment cards are commonly referred to as credit or charge cards, debit or ATM cards, gift cards, and pre-paid cards.

Additionally, mobile wallet adoption is also expected to advance the growth of payment card use. Market segments could include Hospitality, Retail, Utilities & Telecommunication, as well as others. In North America, the use of a credit card is the primary method of payment preferred by customers for both point-of-sale (POS) and online methods, driven by rewards programs offered by the issuers. Payment card issuers are leveraging this momentum by focusing on adding new cards and broadening the rewards program to stay competitive. Global in-store payment card usage is expected to grow at expeditious rates. Given the accelerated increase of in-person payment card usage, safeguarding the personal payment data of customers is of the utmost importance to both financial organizations and customers.

sales@oberonwireless.com
877-867-2312

Retailers, suppliers, and resellers who accept payment cards from customers, must comply with the Payment Card Industry Data Security Standard (PCI DSS.) This comprehensive guideline is designed to safeguard the personal payment data of customers when it's stored, processed, and transmitted by the companies they do business with.

The widespread use of wireless networks for processing and transmitting cardholder data has become a top priority in data protection. Given the critical nature of physical protection, the PCI Security Standards Council Special Interest Group Implementation team has issued a supplement called PCI DSS Wireless Guideline. This guideline explains how PCI DSS applies to the wireless environment and how to secure wireless network components with practical methods for deployment in the payment card environment. Below are examples of sections outlining the physical security of the wireless devices.

4.1. Physical Security of Wireless Devices

PCI DSS Wireless Guideline promotes the need for physical security surrounding wireless access points, gateways, and handheld devices. The focus of this requirement is to prevent unauthorized persons from using unattended wireless devices to gain access to network resources or connecting their own devices to the wireless network to gain unauthorized access. The security of devices that are publicly accessible or provide access to critical components are of particular concern. For example, the use of a physical cage may not be necessary for access points (APs) that are in a secure data center but may be justified for APs in public or semi-public areas, or that are otherwise deemed to be a high risk. An obvious risk associated with insufficient physical security (other than theft) is the ability for an unauthorized person to reset an AP to its factory

default settings. The reset function is particularly problematic because returning the AP to its default factory settings allows individuals to negate any security settings that administrators have configured in the AP. The default settings generally do not require an administrative password and may disable encryption. Resetting the configuration to the default settings can be done simply by inserting a pointed object, such as a pen, into the reset hole. If a malicious user gains physical access to the device, it is easy to exploit the reset feature and cancel any security settings on the device. Additionally, an AP reset can be invoked over the management interface or by using a serial console interface on the AP. An attacker with physical access could connect to a physical port on the device and bypass network access controls, which is why PCI DSS requires that adequate mechanisms be in place to prevent unauthorized physical access to wireless devices.

PCI DSS Requirement 9.1.3

Although PCI DSS does not mandate how wireless devices are to be secured, there are many ways to implement physical security. Options for securing wireless devices may include physically restricting access (e.g., by mounting APs or base stations high up on the ceiling) and disabling the console interface and factory reset options through use of a tamper-proof chassis. Many enterprise APs are equipped with special mounting brackets that prevent access to the network cable. Securing handheld wireless devices and laptops may be more difficult since physical access to these devices is typically needed to perform job functions. Such devices should be physically secured when not in use or if left unattended in a public area.

Restrict physical access to wireless access points, gateways, handheld devices, networking/ communications hardware, and telecommunication lines.

Verify that physical access to wireless access points, gateways, handheld devices, networking/ communications hardware, and telecommunication lines is appropriately restricted.

4.1.1 Recommendations

A. Mount APs on (or in) ceilings and walls that do not allow easy physical access, or locate in secure areas, such as locked closets or server rooms. (Figures 1, 2 and 3)

B. Use APs with tamper-proof chassis and mounting options that prevent physical access to ports and reset features. (Figures 1, 2 and 3)

C. Review signal settings and physical placement of APs to provide maximum coverage for the desired service area while minimizing broadcast

D. Secure handheld devices with strong passwords and always encrypt pre-shared keys (PSKs) if cached locally.

E. Enable automatic lockouts on handheld devices after a defined idle period and configure devices to require a password when powering on.

F. Use a wireless monitoring system that can track and locate all wireless devices and report if one or more devices are missing.

Figure 1: Oberon Hi-BarTM series. Secure locked enclosure painted by the customer to match the surroundings meeting aesthetic requirements

Robust wireless network connectivity requirements in the payment card industry continue to progress. The proper installation and protection of wireless access points is key to ensuring that the Wi-Fi network can deliver stability, reliability, and performance. In an evolving Wi-Fi landscape continuously shaped by rapidly emerging technologies, wireless professionals must navigate not only the complexities of optimizing the network performance, but also streamline their critical operational objectives. This means implementing physical AP deployment methods that should:

- Offer quick and easy serviceability of the AP and cabling components
- Provide a consistent look and maintenance functionality throughout the facility
- Offer a cost-effective migration path to next-generation technologies

Turn to the experts at Oberon Wireless for more options.

Figure 2: Oberon H-Plane™ series. Secure locked right angle surface mount. Permits horizontal mounting of the AP by recessing the AP into the bracket for additional security. Provides interchangeable trims for easy migration path to next-generation APs.

Figure 3: Oberon locked Wi-Tile™ series. Provides an aesthetic ceiling mount solution with interchangeable doors for quick and easy migration path to next-generation APs.

oberonwireless.com
sales@oberonwireless.com
877-867-2312

Source: PCI_DSS_v2_Wireless_Guidelines.pdf