Wireless Security for Mobile Computers

A Datalogic Mobile and Summit Data Communications White Paper

Original Version: June 2008
Update: March 2009

DATALOGIC MOBILE

SUMMIT DATA COMMUNICATIONS

Protecting Confidential and Sensitive Information

It is every retailer's nightmare: An attacker exploits weak network security at a retail store to steal information from customers' payment cards (credit cards and debit cards). The theft affects everyone in the retail supply chain, including the retailer, its customers, banks, and payment card companies. The retailer, however, is the one hammered by bad publicity. In addition to costing the retailer business, the bad publicity sullies the retailer's reputation, forever linking its name to the theft.

Retailers are not the only targets. Sensitive data including proprietary technology, employee records, client information, and social security numbers are all potential targets. While scams, phishing and other internet security threats get media airplay, enterprises cannot leave themselves open to any threat that jeopardize data. Any exposure could lead to litigation and media exposure that could ruin the best run company. While most enterprises have implemented strong wired network security protocols and procedures, the advent of wireless devices, such as mobile computers, brings a new challenge.

Many enterprises implement mobile computers as an effective and efficient tool to maximize productivity. The extension of a network through the implementation of a wireless LAN (WLAN) has allowed workers to roam the work space connected with their mobile device. But the radio waves that connect worker and network are not bound by walls and pose a new challenge in network security.

This white paper focuses on client devices, specifically mobile computers, which connect to a network using wireless LAN, or Wi-Fi®, technology. Presented is a robust, approach to Wi-Fi client security for protecting the data that clients transmit and receive and the networks to which they connect.

Wi-Fi and Mobile Computers

WLANs are prevalent in mobile computer applications such as retail stores, warehouses, and distribution centers. Wi-Fi is popular in these applications for two reasons. First, many of the workers in these applications are mobile, meaning that they do their jobs from different locations or while on the move. An increasing number of these mobile workers rely on client devices such as mobile computers to do their jobs, and those devices rely on network connections using Wi-Fi. Second, Wi-Fi gives managers flexibility in configuring their operations. For example, devices such as cash registers can be installed and made operational, then moved or removed without any changes to the store's wired (Ethernet) network. The same is true for other resources such as printers, electronic scales, and other network enabled devices. Because WLANs improve worker productivity and reduce the costs of configuring and reconfiguring operation, most managers consider their WLANs to be a critical part of their information infrastructure.

Threats When Wi-Fi Security Is Weak

Wi-Fi involves communication between radios that use a specific type of radio frequency (RF) technology. Wi-Fi radios send data to each other over the air, using radio waves. In most commercial applications, Wi-Fi radios in computing devices communicate with Wi-Fi radios in infrastructure devices such as access points (APs) that are connected to the wired network. The radio waves that travel between the devices can "bleed" through the walls of the building to adjacent buildings, parking lots, and other nearby public areas. Those RF signals can be viewed by any computing device in the vicinity, provided that the device is equipped with the following:

- A Wi-Fi radio
- An antenna that provides sufficient gain to enable the radio to "hear" the Wi-Fi packets
- A commonly available software application called a Wi-Fi sniffer, which makes the contents of Wi-Fi packets viewable

Without proper Wi-Fi security in place, a hacker can use intercepted Wi-Fi packets to do one or more of the following: view sensitive information, gain access to the WLAN, or trick users into communicating with him instead of the network.

The first threat of weak Wi-Fi security is **data exposure**. Some of the data packets that travel between a Wi-Fi client and a WLAN may contain sensitive information. If the packets are not scrambled, or encrypted, so that they cannot be deciphered by a hacker, then the hacker can view sensitive information, such as credit card information, just by sniffing and viewing the packets.

Weak Wi-Fi security also can lead to **network exposure**. In addition to data packets, control packets travel between Wi-Fi clients and a WLAN. When WLAN access is not governed by a strong authentication mechanism, then a hacker can use the control information in sniffed packets to pose as an authorized user and gain access to the WLAN. Once on the WLAN, the hacker may be able to gain access to sensitive information on the network.

A third threat of weak Wi-Fi security is **man-in-the-middle attacks.** When Wi-Fi clients are not required to use strong authentication methods, a hacker's laptop posing as an AP may be able to trick clients into associating with it instead of a trusted AP. Once a Wi-Fi client associates to a hacker's laptop, the hacker may be able to steal information from the client, including sensitive information and information required to gain access to the trusted network.

Wi-Fi Security Foundation: WPA2-Enterprise

Fortunately, WLAN security threats can be mitigated through good WLAN security practices. The foundation of any WLAN security approach should be the Enterprise version of Wi-Fi Protected Access™ 2, or WPA2.

As Wi-Fi became popular on mainstream client devices such as laptops, it was determined that the original WLAN security mechanism of Wired Equivalent Privacy (WEP) was insufficient for several reasons, including:

- **No access control:** While it defines a means to scramble, or encrypt, transmitted data, WEP provides no means to control access to a WLAN. If you know the WEP encryption key, then you can gain access to the WLAN.

- **Vulnerable keys:** Due to weaknesses in WEP, a hacker can "crack" or decipher a WEP key by collecting WEP-encrypted data packets and running them through a WEP-cracking tool. Today, using sophisticated tools, even a 104-bit WEP key can be cracked in less than an hour.

- **Static keys:** The only way to avoid the use of a WEP key that has been cracked by a hacker is to change all WEP keys regularly, which today means more frequently than every hour. Because the most common way of deploying WEP keys is to define them statically on all devices that used them, changing WEP keys is an administrative nightmare.

The IEEE, which defines the standards for WLANs and how they operate, formed a task group, called the 802.11i task group, to define a standard for stronger WLAN security. The 802.11i task group, like most other IEEE task groups, took several years to define, debate, finalize, and ratify the standard. In the meantime, the market grew increasingly impatient for something better than WEP. The Wi-Fi Alliance®, a non-profit industry association of more than 300 member companies, responded to market pressure by teaming with the 802.11i task group to create WPA, which the Alliance termed "a significant near-term enhancement to Wi-Fi security".

According to the Alliance, WPA is "a specification of standards-based, interoperable security enhancements" that ensures data protection through encryption and WLAN access control through authentication. WPA was designed to be supported in software by Wi-Fi CERTIFIED™ products that previously had supported WEP.

There are two versions of WPA: Personal and Enterprise. Both encrypt and decrypt transmitted data using Temporal Key Integrity Protocol, or TKIP. Like WEP, TKIP uses RC4 encryption, but TKIP is designed to address vulnerabilities of WEP by providing these enhancements:

- Longer initialization vector, which minimizes the chance that a key will be reused during a session

- Key hashing, which results in a different key for each data packet

- Message integrity check, which ensures that the message is not altered in transit between sender and receiver

The key used for TKIP encryption and decryption is derived dynamically from the information exchanged between the Wi-Fi client and the WLAN during the authentication process that proceeds the client's connecting to the WLAN. With WPA-Personal, authentication is done through a four-way handshake using a pre-shared key (PSK) or passphrase. If the PSK on the Wi-Fi client matches the PSK on the AP to which the client is trying to associate, then the authentication succeeds, and an encryption key for that client is derived and stored on the client and the AP.

While PSKs are easy to implement on small networks, a hacker can "guess" a short PSK using a dictionary attack. In such an attack, the hacker captures packets that were created using the PSK and then, using a dictionary of potential PSKs and the published algorithm for WPA, tries to recreate the capture packets. If he is successful, then he has determined the PSK, and he can use it to gain access to the WLAN. The IEEE and various researchers recommend that, if you use a PSK, that PSK should be a random string of at least 20 characters, including characters other than letters and digits.

While WPA-Personal relies on a pre-shared key or passphrase for authentication, WPA-Enterprise relies on IEEE 802.1X, a ratified standard for network access control. 802.1X supports a set of Extensible Authentication Protocol, or EAP, types for mutual authentication of the client device and the network to which it is trying to connect. 802.1X authentication with an EAP type such as PEAP or EAP-TLS is extremely strong.

In July 2004, the IEEE approved the full 802.11i specification. Soon after that, the Wi-Fi Alliance introduced a new interoperability testing certification, called WPA2, that incorporates the key elements of 802.11i. WPA2 is essentially the same as WPA, with TKIP replaced by a stronger encryption method based on the Advanced Encryption Standard (AES) cipher. In March 2006, the WPA2 certification became mandatory for all new equipment certified by the Wi-Fi Alliance.

Figure 1 provides an overview of WPA-Enterprise and WPA2-Enterprise:

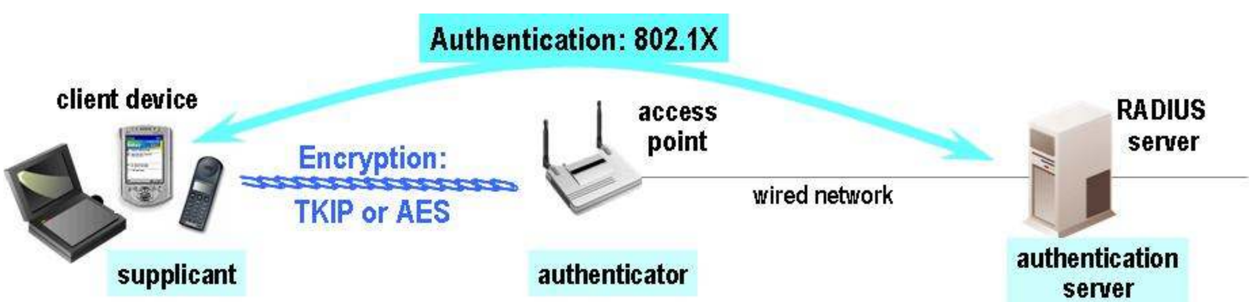

Figure 1: WPA-Enterprise and WPA2-Enterprise

Table 1 below compares popular EAP types that are used with 802.1X authentication.

Type	Credential(s)	Database(s)	Pros and Cons
LEAP	Microsoft password	Active Directory (AD)	No certificates Strong password required
PEAP with EAP-MSCHAP	Microsoft password	AD	Native support in Windows, CE CA certificate on every client device
PEAP with EAP-GTC	Password, one-time password, token	AD, NDS, LDAP, OTP database	Broad range of credentials CA certificate on every client device
EAP-TTLS	Wide variety	Wide variety	Broad range of credentials Not widely supported
EAP-FAST	Microsoft password, others	AD, others	No certificates Complex provisioning process
EAP-TLS	Client certificate	Certificate authority (CA)	Very strong authentication Native support in Windows, CE CA, user certificates on every client device

Table 1: Comparison of popular EAP types

In late 2008, two German researchers reported a vulnerability in TKIP could enable an attacker to decrypt individual packets that are encrypted with TKIP. The same vulnerability does not exist with AES-CCMP, the encryption algorithm used with WPA2. In other words, the researchers confirmed that WPA2-Enterprise offers stronger security than WPA-Enterprise. Given that a broad range of client devices support WPA2-Enterprise, every organization should rely on WPA2-Enterprise instead of WPA-Enterprise.

The use of WPA2-Enterprise addresses the security threats mentioned early in this section:

- **Data exposure:** To prevent the data in Wi-Fi packets from being viewed by a hacker, the sender of those packets must encrypt the data in such a way that only the intended recipient can decrypt the packets and view the data in its unscrambled, clear-text form. WPA and WPA2 provide proven mechanisms for ensuring that all transmitted data is protected from being viewed by a hacker.

- **Network exposure:** When every Wi-Fi client uses WPA or WPA2 with 802.1X authentication to the network, a hacker cannot glean from sniffed packets any information on how to gain access to the network.

- **Man-in-the-middle attacks:** When every Wi-Fi client is configured to use a strong EAP type for mutual authentication to the trusted WLAN, no client will associate inadvertently to a hacker's laptop that is posing as an AP.

The use of WPA2-Enterprise protects all sensitive data, including credit card information, and the networks that house that data. The Payment Card Industry (PCI) Security Standards Council has created a set of guidelines to be used by retailers to protect consumer payment card data. These guidelines known as the PCI Data Security Standard (PCI DSS) provide a strong foundation from which to create a secure wireless network. The guidelines provided in the PCI DSS can provide a foundation for strong WLAN security in environments beyond retail.

Requirements for Wi-Fi Clients

Any organization that stores, processes, or transmits cardholder data must comply with PCI DSS. Four items in PCI DSS have implications for Wi-Fi client device security and how it is configured and managed. Those four items are:

1.2.3: Put a firewall between any WLAN and the cardholder data environment.
2.1.1: Change defaults for WLAN parameters.
4.1: Use strong encryption for all WLAN data.
11.1: Demonstrate the ability to identify and stop unauthorized WLAN access attempts.

These items have direct correlation to the establishment of a secure wireless network for environments that do not handle consumer payment card data. Applying PCI DSS standards will secure sensitive data within a network with wireless devices.

Put Firewalls between WLANs and Confidential Data

You should install a firewall between every WLAN and the confidential data environment. The firewall is to prevent Wi-Fi devices from gaining access to the confidential data environment, unless applications that run on Wi-Fi devices require access to that environment, in which case the firewall is to "control" traffic. It is extremely difficult for a firewall to control traffic unless the firewall knows which devices are authorized to have access and which are not.

The underlying assumption is that every WLAN is an "un-trusted network", which is defined as a network that has one or both of these characteristics:

- Is external to the networks belonging to the entity under review
- Is out of the entity's ability to control or manage

In reality, most organizations manage their WLANs as part of their trusted networks. For all organizations with WLANs, a straightforward approach is to:

- Allow WLAN access only to clients that authenticate to the network in a way that cannot be duplicated by hackers.
- Ensure that all data sent to and from Wi-Fi clients is scrambled using strong encryption, so that a hacker that intercepts the transmitted data cannot decipher it.

In other words, every device on the WLAN that needs access to the confidential data environment must support and use strong WLAN authentication and strong WLAN data encryption. To simplify the configuration and monitoring of Wi-Fi client devices, a best practice is to ensure that **all** Wi-Fi devices support and use strong WLAN authentication and strong WLAN data encryption, even if those devices do not need access to the cardholder data environment. The use WPA2-Enterprise with a strong Extensible Authentication Protocol (EAP) type supports this best practice.

Change WLAN Defaults, and Enable Strong Encryption

Configuration of a secure WLAN requires that access points (AP) not be allowed to broadcast the WLAN network names, called service set identifiers or SSIDs, that are supported by the APs. Disabling SSID broadcast alone does not prevent a malicious user from determining which SSIDs are being used on WLANs. Other encryption, such as AES in WAPA2, and authentication configuration changes are also required.

Wi-Fi client devices must be configured properly. To connect to an AP, a client device must be configured with an SSID supported by that AP and correct credentials for the method of authentication supported by that AP.

Most of today's mobile computers and other business-critical mobile devices run Windows Embedded CE, Windows Mobile, or Windows XP. All three operating systems include a WLAN configuration facility called Windows Zero Config (WZC), which enables a user or administrator to configure the device to associate to an AP, provided that the AP uses one of the authentication methods supported by WZC. WZC supports the configuration of two EAP types, PEAP with EAP-MSCHAPv2 as the inner method (PEAP-MSCHAP) and EAP-TLS. Many organizations, however, rely on other EAP types – such as LEAP, EAP-FAST, and PEAP-GTC – because those types provides a better "fit" with infrastructure and security requirements.

To use an EAP type that is not supported natively by the Windows operating systems, a client device must include a software application called an 802.1X supplicant that supports that EAP type. Commercial supplicants are available for Windows XP but not for Windows CE or Windows Mobile. For the latter two operating systems, the Wi-Fi radio in the client device must include the supplicant.

To simplify administration of Wi-Fi client devices, you should choose devices with software that supports a wide range of EAP types and ensures that the devices are configured to connect only to your trusted WLAN using your chosen EAP type. Ideally, this software will support a means to distribute the same configuration to many devices with minimal intervention.

Use Strong Encryption for All WLAN Data

Using the assumption that every WLAN is an un-trusted network or an open, public network, assumes that the WLAN can be accessed by malicious individuals. Those individuals, can intercept and view data that is transmitted wirelessly, so it is critical to scramble all such data using strong encryption.

The best practice for encrypting WLAN data is to use WPA2-Enterprise because:

- It operates at Layer 2.
- It supports dynamic generation of strong encryption keys.
- It is an industry standard, and testing for it is required for earning the Wi-Fi CERTIFIED seal from the Wi-Fi Alliance.
- Its AES-CCMP encryption is defined as part of the ratified IEEE standard for WLAN security.

Demonstrate Ability to Stop Unauthorized WLAN Access

When Wi-Fi client devices are not required to use strong authentication methods, those clients may associate to un-trusted APs, including those placed in the vicinity of clients to steal information from those clients. Because a rogue AP may be in place only for a few days or even a few hours, periodic use of a wireless analyzer is insufficient. Only a wireless intrusion detection system (IDS) or intrusion prevention system (IPS) that provides constant monitoring is sufficient to detect most rogue APs.

Wireless IDS or IPS tools are no substitute for robust authentication and encryption. When you require every client device to use WPA2-Enterprise to gain access to your trusted WLANs, and when you configure your client devices to gain access only to your trusted WLANs, you minimize the threat posed by rogue APs and other hacker tools. Your tools for WLAN monitoring and wireless IDS/IPS then become ways of demonstrating that your WLAN security policies are implemented properly and are thwarting all attempts to gain unauthorized WLAN access or view sensitive data that is transmitted wirelessly. Those tools may even catch potential attackers in the act.

Summary: Security Best Practices for Wi-Fi Client Devices

The following best practices for Wi-Fi client device security and administration help to ensure protection of confidential and sensitive data in WLAN environment:

- Ensure that a Wi-Fi client device can gain access to your WLANs only using WPA2-Enterprise with a strong EAP type.

- Configure every trusted Wi-Fi client device to connect only to trusted APs.

- Use ongoing monitoring to demonstrate the effectiveness of your WLAN security approach.

Datalogic Mobile is a global manufacturer of rugged mobile computers. We focus on warehousing solutions, field-force automation, and retail applications. Our diverse product range includes pocket-sized mobile computers, pistol grip computers, and industrial PDAs designed to keep workers connected to their enterprise inside or outside their four walls. Our mobile computers use CCX certified radios for maximum security and leverage GSM/GPRS/EDGE for on-the-go connectivity. Datalogic Mobile has engineering and manufacturing facilities in Eugene, Oregon and strong worldwide presence with offices in over 20 countries and over 800 partners worldwide. See us on the web at www.mobile.datalogic.com/americas or call 800-929-7899

Summit Data Communications provides high-performance Wi-Fi radios for mobile computers and other business-critical mobile devices. Summit radios are optimized for the challenging radio environments in which business-critical mobile devices operate, such as factories, warehouses, ports, hospitals, and retail stores. Summit solutions combine hardware, software, and integration and support services