

Technological Trends

Wi-Fi Client Device Security Part 1: The Need for Wi-Fi Security

This is the first of three articles on Wi-Fi client security. The first article explains the need for strong Wi-Fi security. The second article explains why WPA2-Enterprise is required for solid Wi-Fi security. The third article provides three best practices for ensuring strong Wi-Fi client security.

Long before wireless LAN (WLAN), or Wi-Fi[®], technology became popular in homes, offices, airports, and coffee shops, it was in widespread use in retail stores, distribution centers, manufacturing facilities, and other business locations. In fact, some businesses have been using WLANs since before the first Wi-Fi standard was ratified by the 802.11 Committee of the IEEE, or the Institute of Electrical and Electronics Engineers, in 1997.

Wi-Fi is popular in businesses for two reasons. First, many workers 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 businesses flexibility in configuring their networks. For example, retail store 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. Because WLANs improve worker productivity and reduce the costs of configuring and reconfiguring networks, many businesses consider their WLANs to be a critical part of their information infrastructure.

The convenience of WLANs brings a challenge: providing reliable network security when the network literally extends into the air and sensitive data can travel hundreds of meters outside the perimeter of the business location. The failure to meet this challenge has led to information theft, costing businesses huge amounts of money and, in some cases, damaging their reputations almost beyond repair.

An Example from the Retail World

Wireless network breaches at two Miami-area stores of a U.S.-based discount retailer gave hackers undetected access to the retailer's central databases for 18 months, exposing over 45 million credit and debit cards to potential fraud. Fraudulent purchases occurred around the world, including in Hong Kong and Sweden. The breaches cost the retailer at least USD150 million, and experts estimate that, because of litigation, the final cost could be several times more.

In response to security threats and security breaches related to payment cards, or credit cards and debit cards, major payment card companies established the Payment Card Industry (PCI) Security Standards Council to create a common set of guidelines for how retailers must protect payment card information and thereby prevent credit card and debit card fraud and identity theft. Those guidelines are codified as requirements in the PCI Data Security Standard (PCI DSS).

If a retailer processes, stores, or transmits information for payment cards issued by any of the major payment card companies, then that retailer must comply with the requirements of PCI DSS. A retailer that fails to comply may risk stiff penalties from the payment card companies and may be denied the ability to accept credit and debit cards from those companies. Of course, potential penalties for noncompliance pale in comparison to the damage from payment card information being stolen.

Other industries have established their own requirements for securing WLANs and the information that travels over them. These efforts are a recognition that, without strong security, WLANs are vulnerable to information theft and network breaches.

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 in computing devices such as mobile computers send data to and receive data from Wi-Fi radios in infrastructure devices such as access points (APs) that are connected to a wired network. The radio waves that travel between the devices can “bleed” through the walls of a facility to adjacent facilities, 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:

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

When proper Wi-Fi security is not 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.

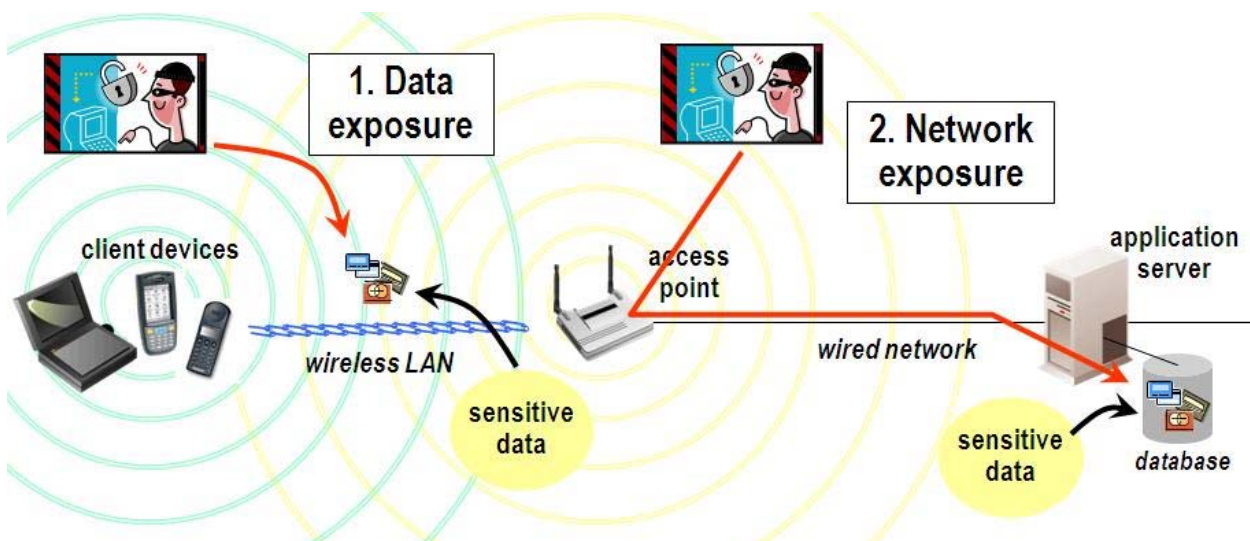


Figure 1: Two threats of weak Wi-Fi security are data exposure and network exposure.

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.

The next article will explain how these threats can be mitigated through the use of WPA2-Enterprise security on your WLANs.