8.3.2 Wireless Security Facts

Wireless networking uses radio frequencies to transmit data. This means anyone with a wireless receiver can capture data from an improperly secured network.

This lesson covers the following topics:

- Weak configurations
- Cryptographic protocols

Weak Configurations

Proper configuration of a wireless access point (WAP) is the first step in securing the network. The following table explains some important actions to take regarding WAP settings.

Security Configuration Action	Description
Change default login credentials	WAPs typically come configured with a default administrator username and password. Because the administrator username and password is used to configure WAP settings, it's important to reset the defaults. This prevents outsiders from guessing the default username and password and breaking into the system.
Change default service set identification (SSID) and broadcast	The SSID can be a maximum of 32 bytes in length. Since many manufacturers use a default SSID, it's important to change the SSID from the default. The SSID should be unique, but should not contain identifiable information (address, last name, etc.). The SSID broadcast can also be disabled. This is known as SSID suppression or cloaking. A determined hacker can still easily discover hidden SSIDs. Disabling SSID broadcast can cause connection issues for devices.
Enable MAC address filtering	Every network device has a unique media access control (MAC) address. By specifying the MAC addresses that are allowed to connect to the network, unauthorized MAC addresses can be prevented from connecting to the WAP. Configuring a MAC address filtering system is very time consuming and demands upkeep. Attackers can still use tools to capture packets and retrieve valid MAC addresses. An attacker can spoof a wireless adapter's MAC address and circumvent the filter.
Update the firmware	Manufacturers release updates to the firmware on a regular basis to address known issues. It is important to regularly check for updates and apply them to prevent the system from being exposed to known bugs and security vulnerabilities. While it is extremely important to keep devices up-to-date, it's just as important to properly test new updates before pushing them out to the entire network. Proper testing will reduce the number of new bugs or problems on a live network that the update may have introduced.

Enable the WAP firewall	Most wireless APs come with a built-in firewall that connects the wireless network to a wired network. This should be enabled to help prevent unauthorized access to the network.
Wi-Fi signal strength	Data emanation is a significant security problem. By default, the radio signals used by a wireless network are broadcasting omni-directionally and can travel quite a distance from the WAP. An attacker sitting outside the building may be able to connect to the wireless network if the signal is traveling outside. This can be limited by manipulating the WAP antenna placement. Some WAPs also allow the signal strength to be adjusted. Using these settings, reduce the signal strength so the signal stays inside the building.

Cryptographic Protocols

Enabling the proper cryptographic protocol is perhaps the most important way to secure a wireless network. For most users, Wi-Fi Protected Access (WPA) versions 2 or 3 will be the best option. The following table explains these two protocols:

Cryptographic Protocol	Description
Wi-Fi Protected Access 2 (WPA2)	WPA2 is the implementation name for wireless security that adheres to the 802.11i specifications. It was first introduced in 2004 and is still heavily used in today's networks. There are two version of WPA2 available: - WPA2-Personal is also known as WPA2-PSK (pre-shared key). This version uses a pre-shared key, or passphrase, to protect the network. WPA2-PSK: - Uses Advanced Encryption Standard with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)as the encryption algorithm to encrypt all data. AES-CCMP uses a 128-bit key and a 128-bit block size. - Performs a 4-way handshake to authenticate the device when it connects to the access point. The pre-shared key and SSID are used to generate a session key during this process. The handshake does have some vulnerabilities that allow a hacker to intercept data and perform offline password attacks. - WPA2-Enterprise uses a RADIUS server to authenticate users to the network.
Wi-Fi Protected Access 3 (WPA3)	To support the vulnerabilities inherent in the WPA2 handshake and to support newer technologies, WPA3 was implemented. First introduced in 2018, WPA3 implements the Simultaneous Authentication of Equals (SAE) standard instead of using the pre-shared key. SAE uses a 128-bit key and Perfect Forward Secrecy (PFS) to authenticate users. Perfect forward secrecy is a cryptography method that generates a new key for every transmission. This makes the handshake much more secure from hackers. If any portion of the handshake is intercepted, the key is still uncrackable.

Copyright © 2022 TestOut Corporation All rights reserved.