13.9.4 Wireless Network Security Facts

As a system administrator, there are several best practices that you can employ to increase the security of a wireless network. The goal is to make the network more difficult to compromise and accordingly less attractive to an attacker. These best practices are listed in the following table:

Best Practice	Description
Change Default Usernames and Passwords	You should change the default username and password used on wireless access points. The default username and password assigned to a device by the manufacturer are widely known and posted on the internet.

Manage the SSID	There are several practices you can implement regarding your wireless network's SSID to increase the security of the wireless network:
	▪ Change the SSID from the default. Lists of default SSIDs assigned by manufacturers are posted on the internet. If you use the default SSID, an attacker can quickly determine the make and model of your access point. Using this information, an attacker can:
	  ▪ Identify the default username and password used by that device.
	  ▪ Research known security weaknesses associated with that device, making it easier to compromise your wireless network.
	▪ Use a network name that is not easily associated with your organization.
	▪ Disable SSID broadcast. If SSID broadcast is enabled, then the name of the network is advertised to all wireless devices within range of your wireless access points. Disabling SSID makes your wireless network harder to locate.

Implement Encryption and Authentication	You should implement encryption and authentication on your wireless network using the strongest algorithms available:
	▪ Avoid implementing an open (unencrypted) network.
	▪ Avoid using WEP to protect the network. A WEP key can be cracked quickly with software available on the internet.
	▪ Use one of the following versions of WPA2 to implement wireless encryption and authentication:
	  ▪ WPA2-PSK is best suited for wireless networks used by home or small business users. WPA2-PSK requires the same pre-shared key to be configured on the access point and on each wireless client. This key is used to both authenticate the host to the wireless network and to encrypt transmissions.
	  ▪ WPA2-Enterprise is a best suited for wireless networks that are part of a large corporate network. WPA2-Enterprise requires a separate authentication process to access the wireless network. Whenever a host wants to connect, credentials are forwarded to a RADIUS server for authentication.

Implement MAC Address Filtering	MAC address filtering restricts access to the wireless network to hosts that have specific MAC addresses. This can be done in two different ways: ▪ Use a whitelist, which defines a list of MAC addresses that are allowed to connect. ▪ Use a blacklist, which defines a list of MAC addresses that are not allowed to connect. With MAC address filtering enabled, the access point checks a computer's MAC address when it connects to the wireless network. If the access point has been configured to use a whitelist, it will compare the computer's MAC address to the whitelist. If its address is listed in the whitelist of allowed MAC addresses, then the access point will allow the host to connect to the network. If the computer's MAC address is not in the whitelist, then the host will be denied access. If the access point is configured to use a blacklist, the opposite occurs. If the computer's MAC address is on the blacklist, the access point will not allow the host to connect to the network. If its MAC address is not listed in the blacklist, the access point will allow the computer to connect to the network. For security reasons, whitelists are usually the preferred option. This configuration locks out all hosts except for those specifically allowed in the whitelist. However, MAC address filtering provides only a basic level of network security and can be defeated by determined attackers. However, it does make the network harder to compromise and hopefully less attractive to

	attackers.
Implement Static IP Addressing	Most wireless access points provide a DHCP server function within the firmware of the device. Using DHCP makes it very easy for wireless hosts to connect to the wireless network. However, it also decreases the security of the network. With DHCP is enabled, the access point provides any wireless client with the appropriate information needed to communicate with other hosts on your network. If you implement static IP addressing, then wireless hosts must be statically configured with this information. This increases security because it makes it more difficult for attackers to connect to your wireless network. Even if they manage to associate with the access point, they still have to figure out what IP addressing information is required. This won't stop determined attackers, but it does make their job more difficult..
Manage Antenna Placement	You need to reduce data emanation as much as possible. If your network's radio signal emanates outside your facility, an attacker can intercept that signal and potentially gain access to your organization's computer network. You can minimize data emanation by doing the following: ▪ Consider where wireless access points are placed and where their antennae are transmitting the wireless network's radio signal. Be aware that omni-directional wireless access points transmit in all directions with equal signal strength. If placed near an exterior wall, these antennae will transmit the wireless network's radio signal outside the structure. ▪ Implement directional antennas, which can be aimed in a certain direction. Use these antennae to ensure your wireless network's radio signal is aimed only towards the interior of your facility.
Manage Power Levels	Most wireless access points are set to run at maximum power by default. However, this can result in the wireless network's radio signal being transmitted outside of your facility. Usually you can decrease an access point's signal strength to reduce emanation. However, this will require additional access points to be deployed because the reduced signal strength can create areas of poor coverage. Usually, directional antennae are used in conjunction with customized power levels to provide the best coverage while reducing data emanation. You should use a site survey tool to measure the strength of the wireless signal at various locations both inside and outside the structure to customize the configuration of each access point. This ensures appropriate wireless coverage with minimal emanation.
Disable Wi-Fi Protected Setup (WPS)	While WPS makes wireless networks easier to manage, it also introduces security issues. For example, devices that support the PIN number method have been found to be susceptible to brute-force attacks. An attacker can simply send one PIN number after another to an access point until the correct one is identified. If the access point is not physically secured (which is common in small business and in homes) then attackers can use the push-button or NFC methods to associate their device with the access point. Because of these issues, a best practice is to disable WPS functionality on the access point.