

# Securing the Wireless Network

Because of their nature, wireless networks have no clear boundaries. Securing wireless communications requires strong encryption, authentication, and secure protocols.

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. Wireless networks using WEP or WPA/TKIP are not very secure and are vulnerable to hacking attacks.

WPA2 implements AES, a strong encryption algorithm, and is more secure than WPA. WPA2, an interoperable implementation of 802.11i, is currently the most commonly deployed option in wireless security. Wireless networks using WPA2/AES should have a pass phrase of at least 21 characters. If an IPsec VPN is available, it should be used on any public wireless LANs. WPA2 also has an additional feature called protected management frames. This feature protects unicast and multicast management frames from eavesdropping and forging.

Authentication is now a fundamental component of enterprise wireless policy. The 802.11i architecture specifies 802.1X for authentication, entailing the use of EAP and an authentication server.

Click [here](https://www.youtube.com/watch?v=mW1LCmASQEQ) to watch a video highlighting the vulnerability of using an insecure wireless hotspot in a coffee shop.

When a WiFi-based IoT device or wireless network is being designed, several security considerations should also be kept in mind such as: selecting a secure protocol, protection for management frames, identification of frequency jamming, detecting rogue access points, and using security at the application layer.

One of the most common wireless security threats is the presence of rogue access points. A rogue access point is not approved by administration but is working on the secure network anyway. These rogues can be setup by employees looking for free wireless access or by intruders with more devious intentions in mind. Security administrators should publish and enforce strict rules concerning rogue APs, employ active access point scanning to detect rogues, and use authentication between devices on the network.

Select a wireless protocol with robust, proven security. Many protocols such as LoRoWAN and Bluetooth provide excellent encryption. Although ZigBee is one of the global standards of communication and is very easy to implement, it is not perfect yet. At the time of writing, ZigBee version 1.2 has a number of serious and exploitable security vulnerabilities. Most of these protocol design flaws relate to attempts to make it easier for the end-user to add a ZigBee device to the ZigBee network. Because of these vulnerabilities, ZigBee version 1.2 should not be used on mission critical applications.

Even though most protocols have comprehensive security methods, it is still possible for attacks to be launched against cellular networks. Because user data confidentiality is a cellular carrier responsibility, these attacks would increase the risk of a data breach when data is being transmitted over cellular networks. For this reason it is recommended that security in the form of data authentication and encryption is implemented as part of the application using technologies such as VPNs and TLS/SSL.

        