

Network Protection for Design Professionals

Wireless Network Security

Background:

Exploitation of wireless network security weaknesses have been implicated in several high severity security breaches which have recently come to light. The primary difference between wireless networks and wired networks is also the root of the security concerns involved with use of these networks. The radio links used for network communications in a wireless network can be easily covertly intercepted. This makes eavesdropping on or manipulation of these communications by an attacker a much simpler task. To bring these networks to levels of security near that of traditional wired networks, encryption (which makes these intercepted signals unreadable to unauthorized parties) and strong authentication techniques are necessary.

Wired Equivalent Privacy or WEP was the first security specification introduced to address the inherent insecurity of Wireless Local Area Networks (WLANs). Shortly after the introduction of WEP, researchers began to publish papers indicating weaknesses in its encryption and message authentication mechanisms. Attack tools used to exploit these weaknesses are now widely available.

How to implement appropriate controls:

Develop a formal security policy regarding the use and deployment of wireless technology. This policy should address user security awareness, an approval process for adding, monitoring and configuring wireless network hardware, and procedures for registering all wireless Network Interface Cards which are used in devices connecting to the network.

Change WLAN access point Service Set Identifiers (SSIDs) and administrative passwords from factory defaults to unique values for your business. The SSID is a name assigned to a WLAN to allow wireless devices to distinguish one WLAN from another. Administrative passwords allow access point configuration changes which could be used to disable security.

Disable access point SSID broadcast features and enable MAC address filtering. When the broadcast feature is enabled the WLAN's SSID is visible in plain text to anyone with a wireless device. If this SSID has not been carefully chosen to be vague, it may provide information regarding the identity of the network which could be valuable to an attacker. MAC address filtering permits access only to wireless devices with MAC IDs specified by the network administrator.

Do not depend on WEP (Wired Equivalent Privacy) as a primary means of securing wireless networks. At minimum utilize Wi-Fi Protected Access (WPA). Stronger encryption algorithms are available through the use of WPA2 but wireless network hardware, which meets the requirements of IEEE 802.11i must be utilized. A Virtual Private Network (VPN) is also an option for securing wireless links. The VPN should be configured such that it must be used for all WLAN devices and that all wireless traffic is through a VPN device before entering the corporate network.

Resources:

Are Your Company's Wireless Networks Putting Your Sensitive Data at Risk?, CNA Insurance, http://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Network%20Security/CNA%20-%20Wireless%20Technology.pdf

Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

