4 Hidden Wi-Fi Security Threats

Introduction

By now you likely know WEP security can be cracked and the best Wi-Fi security is provided by WPA2, creating strong passphrases when using the Personal (PSK) mode or using the Enterprise (802.1X) mode for superior protection. Thus in this article we'll look at a few lesser known wireless security vulnerabilities. You'll discover what they are, how they can affect your network, and how to protect against them.

Wi-Fi Protected Setup (WPS) PIN Cracking on Wireless Routers

In late December 2011, a vulnerability was publically discovered with the Wi-Fi Protected Setup (WPS) standard that's built into the majority of wireless routers since 2007. It can potentially allow anyone to gain access to a Wi-Fi network via a wireless router that supports WPS and is using WPA or WPA2 Personal (PSK) security. WPS was ironically developed by the Wi-Fi Alliance to help make securing networks with WPA/WPA2-PSK security easier. Wireless vendors can include a few methods to use WPS, but the only one required, the PIN method, is the root of the vulnerability.

Like pretty much any other password-based protection, the PINs of WPS can be brute force attacked. Meaning you (or a program) can keep guessing the password or combination in hopes of getting it right. What was publically discovered in December 2011 is that the way the PIN queries or guesses are acknowledged can reveal if the first half of the PIN is correct or not without having the full PIN correct. This along with the last digit of the PIN always being given (from the checksum) makes it much quicker and feasible to brute force crack. Using tools like Reaver or WPScrack can reduce the time it takes to just a few hours, which also reveals the network's full WPA or WPA2 passphrase (PSK).

If you have a wireless router that supports WPS you may find an 8-digital PIN printed on the bottom of the router itself or find WPS settings on the web-based control panel. In the settings you might find an option to disable it or turn it off, which you should do. But it's been reported not all routers actually turn off the WPS functionally and respond to PIN queries, thus you still may be vulnerable. You could do your own testing by trying to connect using a WPS compatible computer or device, or give Reaver or WPScrack a try.

Connecting to Other Wi-Fi Networks

One of the most overlooked Wi-Fi security risks is the ability users have to connect to any wireless network. You can have the best security (WPA2 with 802.1X) to protect against outsiders from cracking your security, but you should also think about insiders comprising the security.

For instance, a user may knowingly or unknowing connect to a neighboring (perhaps unsecured) network since it has a better signal. Or they may do it intentionally to bypass content filters you have in place on your network. Once connected to another network, users there might be able to access that computer and snoop on its web traffic, possibly exposing passwords and other sensitive information.

On PCs running Windows Vista or later, network filters can be set via the netsh command-line tool to limit which SSIDs (network names) users see in the list of available networks.

You can block all networks (except those you explicitly allow) with the following command:

```
netsh wlan add filter permission=denyall networktype= infrastructure
```

You should also block all ad-hoc networks:

```
netsh wlan add filter permission=denyall networktype= adhoc
```

Then you can explicitly allow your network:

```
netsh wlan add filter permission=allow
ssid=yournetworkname networktype= infrastructure
```

If you're running a domain network with Group Policy on a Window Server 2008 or later, you can push similar restrictions to the computers. Using the Microsoft Management Console (MMC) snap-in or Group Policy Management Console (GPMC) navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.

Then you can create/edit the **Wireless Network (IEEE 802.11) Policies**. Since you can create policies for specific Windows versions, the settings will vary. But try to add your network as a preferred network and then

review the other settings to find ways to restrict network access. In Windows Server 2008 and later you should see an option, Only use Group Policy profiles for allowed networks, which blocks users from connecting to any network but those you specify on the preferred list.

User Snooping on Enterprise Networks: Hole 196

In mid-2010, a vulnerability mostly applying to the Enterprise (EAP or 802.1X) mode of WPA and WPA2 security was publically discovered. It can potentially allow users (rogue or curious employees) on the wireless network to snoop on each other's wireless traffic, like you can when on a network protected with just the Personal (PSK) mode of WPA/WPA2 security.

The vulnerability has been publically coined as "Hole 196" by many because the weakness is hinted at on the last line of page 196 of the wireless networking standard (Revised IEEE 802.11-2007).

The vulnerability doesn't involve cracking the encryption, but is from an underlying issue with the 802.11 protocol. It enables users to decrypt packets via a man-in-the-middle attack using the ARP cache-poisoning technique, like we've seen on wired networks. It can also potentially allow users to send traffic to others disguised as one of the network's access points (APs) and/or perform denial-of-service attacks.

Some wireless vendors may implement measures to help prevent this vulnerability, but there are also some other steps you can take. If you aren't already, consider segregating Wi-Fi access with VLANs and multiple SSIDs, thus isolating damage to only the attackers VLAN or SSID. If you don't use the native file sharing protocols (SMB, CIFS, etc), consider enabling client (or layer 2) isolation if your APs support it. It's supposed to prevent user-to-user communication and should prevent some of the attacks of this Hole 196 vulnerability.

You should also make sure you keep your APs updated with the latest firmware updates, which may fix this or other security issues. Additionally, consider implementing a wireless intrusion detection system (IDS) and intrusion prevention system (IPS) that may help detect this and other attacks.

Creating Wireless Hosted Networks in Windows 7 and Later

Starting with Windows 7 and Windows Server 2008 R2, Microsoft includes a Wi-Fi feature called Wireless Hosted Networks.

It lets users (with a supported wireless adapter) create a virtual access point (AP), even while connected to a wireless network. It broadcasts the given SSID (network name), appears as an available wireless network to other users nearby, and hands out IP addresses just like any other wireless router or AP. Users can create and manage wireless hosted networks via the netsh command-line tool or use a third-party program like Connectify.

Though users are required to define a WPA2 (AES) security passphrase when creating a Wireless Hosted Network, the feature could be used knowingly or unknowingly to set up backdoor access to the computer and/or the entire network.

If you're running a domain network with Group Policy on a Window Server 2008 R2 or later, you can help prevent users from creating Wireless Hosted Networks with at least the native wireless client of Windows. In the Group Policy Management Console (GPMC) navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**. Right-click **Wireless Network (IEEE 802.11) Policies** and select **Create a New Wireless Network Policy for Windows Vista and Later Releases**, or if you previously created a wireless policy, edit it. Select the **Network Permissions** tab and mark the **Don't allow hosted networks** checkbox.