Network security guide before vulnerability 196

First we need to understand the attacks using this vulnerability must be done within the network. The culprit must have network certificates and need to have a successful connection to your network.

Network Administration - In a recent article, I have shown you a lot of information about the new security vulnerability in WPA / WPA2 encryption for a wireless network. In that article we introduced the weakness and then shared some tips and protections to avoid attacks that use this exploit on your network or when you use public networks.

>>**Learn about vulnerability 196**

First we need to understand the attacks using this vulnerability must be done within the network. The culprit must have network certificates and need to have a successful connection to your network. The attacks are mostly derived from bad employees or someone inside your organization.

The hole 196 also affects Wi-Fi Protected Access's Enterprise (802.1X) and Personal (PSK) modes, but is more significant for wireless networks that use Enterprise mode.

Another important note - some people claim this is a weakness of WPA2, but it really affects two versions of WPA (TKIP) and WPA2 (AES).

To understand this vulnerability, you must realize one of the benefits of using Enterprise mode of WPA / WPA2: Each user or connection receives a private encryption key. So this user cannot decrypt the traffic of the other user - or vice versa. When using Personal mode, users connect to an encryption key, so they can read each other's traffic.

Vulnerability 196 allows users on a protected network in the Enterprise mode to decrypt packets from other users. It's not exactly the same as cracking encryption, but a *man-in-the-middle attack* using the ARP cache-poisoning technique like in wired networks. The problem below is the 802.11 protocol.

Be aware that this vulnerability also affects public networks that secure Wi-Fi hotspots with Enterprise encryption and 802.1X authentication. A hotspot user can snoop on other users' data even though they think their traffic has been protected.

The bottom line is a licensed user who can capture other users' decrypted data traffic, send traffic carrying malicious data (such as malware) to them by disguising them as points. Network access (AP) and perform denial of service attacks.

Protect your network against this vulnerability

While waiting for carriers to make errors and add patches to these security vulnerability standards, here are some things that can be done to limit the vulnerability on your personal network:

- **Isolate access to VLANs and virtual SSIDs: Place rooms or groups on different virtual networks that can isolate attacks. Smaller businesses can use DD-WRT replacement software to set up virtual LANs and receive** SSID **support** .
- **Client isolation:** Some vendors have integrated this feature into their APs and controllers. This feature can prevent user communication with users; so it can help users avoid this vulnerability.
- **Using VPN connections** : If you're really worried, you can tunnel the traffic of each user through the VPN server. So if someone successfully eavesdrop on the traffic of another user, the culprit will only hear the data is not syntactically syntactic. If you don't have a VPN solution, consider the OpenVPN solution.

In the near future, you should:

- **Upgrade AP software** : Firms can provide patches for this problem with a simple software upgrade, so you need to constantly monitor and upgrade APs and other network components.
- **Upgrade wireless IDS / IPS** systems: **Wireless** intrusion detection systems (IDS) and intrusion prevention systems (IPS) are capable of detecting and alerting you to these types of attacks. These solutions have almost been updated on vulnerability 196, so you need to be sure to upgrade it. If you don't have a wireless IDS / IPS system, you should consider it immediately.

Protect yourself from this hole 196 on public networks

As mentioned above, vulnerability 196 can also affect public networks or Wi-Fi hotspots that use WPA / WPA2-Enterprise with 802.1X authentication. Since anyone can connect, these access points will be where we see these attacks the most. Like in a private network, hackers can capture your Internet traffic or encrypted network traffic and can keep you malicious.

However, protecting your traffic on these networks is not difficult. Create a tunnel on the VPN server and your actual traffic will not be captured. If you do not have a VPN server at home or work, consider other paid or free hosting services.

Some tips for general vulnerabilities

Remember, this is just one of many vulnerabilities in the use of wireless networks. Here are some other tips to keep your network safe:

- When using Personal mode (PSK), using complex, long passwords - shorter passwords can be easily guessed by dictionary attacks.

- When using Enterprise mode with 802.1X, properly configure the settings in Windows, otherwise you will be vulnerable to man-in-the-middle attacks.

1. Check the **Validate server certificate** option and select the Trusted Root Certificate Authority from the list.
2. Select the **Connect to these servers option** and enter the domain name or IP address of the RADIUS server.
3. Catalog **Do not prompt the user to authorize new servers or trusted certificates** .

- Wi-Fi networks are used by organizations or businesses that need to use Enterprise mode, so access can be better controlled. Although it requires a RADIUS server, there are some solutions for smaller organizations.

- Do not rely on disabling SSID promotion or MAC address filtering to be secure.