Types Of Wireless Attacks & How To Prevent Them

A wireless attack involves identifying and examining the connections between all devices connected to the business's wifi. These devices include laptops, tablets, smartphones, and any other internet of things (IoT) devices.

Common types of wireless attacks include:

1. **Replay Attacks (Wireless)**
2. **WPS Attacks**
3. **WEP/WPA Attacks**
4. **IV Attack**
5. **TKIP Attack**
6. **WPA2 Attacks**

Replay Attacks (Wireless)

A simple, yet effective strategy for wireless DoS is to replay locally overheard data packets. These packets are then carried by other forwarding nodes resulting in increased levels of congestion on a wider scale. There are variations of the attack, where either control or data packets are replayed.

The objective of the attacker is to make the packet to look like a legitimate unit avoiding at the same time detection. The intelligence of such an attack lies in convincing the MAC level recipient(s) of a packet to accept and forward it and, the final destination into

believing that this was a legitimately retransmitted packet and that no attack is being launched.

You can prevent Replay Attacks (Wireless) by:

- **Placing the access points in separate virtual LANs and implement some type of intrusion detection to help identify when an attacker is attempting to set up a rogue access point or is using a brute force attack to gain access.**
- **Encrypting all data transmitted through your access point.**
- **Setting the access point to accept only Media Access Control (MAC) addresses.**
- **Using firewalls on each network access point.**
- **Disabling the broadcasting of the SSID from all access points.**
- **Implementing EAP-TLS to use different keys for encryption and broadcast traffic.**
- **Setting up a RADIUS server and a certificate authority.**

WPS Attacks

Wi-Fi Protected Setup (WPS) is a wireless standard that enables simple connectivity to "secure" wireless APs. The problem with WPS is that its implementation of registrar PINs make it easy to connect to wireless and can facilitate attacks on the very WPA/WPA2 pre-shared keys used to lock down the overall system.

The WPS attack is relatively straightforward using an open source tool called Reaver. Reaver works by executing a brute-force attack against the WPS PIN.

You can prevent WPS Attacks by:

- **Implementing tools to detect rogue Wireless Access Points (WAPs).**
- **Disabling WPS.**
- **Setting up MAC address controls on your Access Points.**
- **Ensure wireless router is capable of WPS intruder lockout for the WPS PIN.**

WEP/WPA Attacks

WEP, or Wired Equivalent Privacy, was implemented in 1995 to provide the same expectation of privacy as on wired networks for users of Wi-Fi but had security problems that came to light shortly afterwards. It was deprecated in 2004, superseded by the WPA and WPA2 encryption that you see today.

The reason for this was a series of increasingly devastating attacks against the encryption used in WEP, resulting in the ability to recover the password in a matter of minutes.

WEP is a stream cipher which relies on never using the same key twice to provide security. Unfortunately, as demonstrated in several published attacks, an attacker is easily able to force the same key to be used twice by replaying network traffic in a way that forces a tremendous amount of packets to be generated.

This allows an attacker to collect the data needed to determine the encryption key and crack the network password outright. With good

range and a powerful network adapter, anyone can expect to crack WEP networks in only a few minutes.

Unfortunately, WPA (Wi-Fi Protected Access) is susceptible to password-cracking attacks, especially when the network is using a weak PSK or passphrase.

You can prevent WEP/WPA Attacks by:

- **Changing the default SSIDs and passwords.**
- **Updating the firmware of Wi-Fi-enabled devices, routers, and other hardware as soon as updates are available.**
- **Enabling the firewall for added security in devices, or using a virtual private network (VPN) especially when remotely accessing assets.**
- **Raising company awareness on the risks related to unsecure connections and the use of wireless networks at work as well as at home.**
- **Employing network monitoring to oversee connected devices and web traffic.**
- **Regularly reviewing device logs and monitoring results for any suspicious activity.**
- **Using authentication tools, such as two-factor authentication.**

IV Attack

An IV attack is also known as an Initialization Vector attack. This is a kind of wireless network attack that can be quite a threat to one's network. This is because it causes some modifications on the Initialization Vector of a wireless packet that is encrypted during transmission.

After such an attack, the attacker can obtain much information about the plaintext of a single packet and generate another encryption key which he or she can use to decrypt other packets using the same Initialization Vector. With that kind of decryption key, attackers can use it to come up with a decryption table which they and use to decrypt every packet being sent across the network.

You can prevent IV Attacks by:

- **Getting rid of the encrypted nonce.**
- **Initializing a complete block sized 128 bit random value as IV for the packet data encryption.**
- **Encrypting IV separately as a single block.**
- **Adding a 16 bit field for the packet length before encrypting the packet.**

WPA2 Attacks

WPA2 is a type of encryption used to secure the vast majority of Wi-Fi networks. A WPA2 network provides unique encryption keys for each wireless client that connects to it.

Unfortunately, in 2017 an attack method called KRACK (Key Reinstallation AttaCK) was discovered to break WPA2 encryption, allowing a hacker to read information passing between a device and its wireless access point. This technique used a variation of a common – and usually highly detectable – man-in-the-middle attack.

The vulnerability could potentially allow a hacker to spy on your data as well as gain access to unsecured devices sharing the same Wi-Fi network.

In some instances, attackers could also have the ability to manipulate web pages, turning them into fake websites to collect your information or to install malware on your devices.

You can prevent WPA2 Attacks by:

- **Ensuring that Wi-Fi-enabled devices are updated as soon as a software update is made available.**
- **Ensuring wireless router is running up to date firmware.**
- **Implementing a reputable VPN solution on all mobile and computers before connecting to Wi-Fi.**
- **Browsing to only HTTPS URLs when surfing the web over Wi-Fi connection.**