Wireless traffic security - Part 3

In this article, I will show you the pros and cons of promoting SSID and MAC address filtering.

In this next article, I will show you the pros and cons of promoting SSID and MAC address filtering.

In the previous article of this series, we introduced you to whether or not to change the default password of the wireless access point. In this section, we will continue the discussion by introducing some of the other security settings available in most wireless access points.

SSID

One of the most common security recommendations for wireless networks is to disable SSID promotion. SSID is the abbreviation for the term **Service Set Identifier** . The SSID appears as a word or phrase used to identify a wireless network.

The reason why so many IT experts recommend disabling SSID promotion is because the SSID is almost like a label that you can use to distinguish a wireless network. SSID is actually a secret and is used to restrict access to a wireless network. In other words, unless someone knows the secret, they can't connect to your wireless network.

It should be noted that, although the SSID is a secret, it is different from WEP or WPA keys. We will introduce WEP and WPA in later sections of the series.

At this point, we will go back and learn the concept of SSID secret key. If SSID is actually a cryptographic key used to protect access to a wireless network, why do most access points promote SSID?

We think that the reason why SSID is advertised as such is the development of wireless networking. Although the SSID may initially be created as a security mechanism, it was quickly promoted to become a mechanism for distinguishing between wireless networks from one another. Even the Windows operating system considers the SSID to be the only component of the existence of a wireless network.

So should I promote my SSID or should I disable this promotion? After all, disabling SSID promotion does not bring much to improve network security. When you disable broadcast, the wireless access point will try not to advertise when you encounter packets that require a response. In other words, the SSID will not be displayed on Windows' list of available wireless networks.

This may increase security, but even if you disable SSID broadcast, the SSID is still transmitted in Association and Re-association frames as well as Probe Response frames. This is almost a childish game for anyone with a packet sniffer, who can discover your wireless network SSID because at any time when a legitimate user is connected. If you connect to your wireless network, the SSID is also played in clear text. All the hackers need to do is sit and wait.

Personally, we think it is not right to treat SSID as a security mechanism because doing so only creates a negligible improvement in the security aspect and it can create a security feel. incorrect. More importantly, most older wireless NIC drivers for Windows (even some current drivers) do not work properly when a user tries to connect to a wireless network that does not currently promote its SSID. So, at best, we should consider SSID as just one thing to distinguish wireless networks, not a security mechanism.

Filter MAC address

One of the more effective security techniques for wireless networks at the access point level is to use MAC address filtering. The basic idea below this technique is like a wired network card, all wireless NICs have a unique MAC (Media Access Control) address. MAC address filtering is the process by which you create a whitelist to specify which MAC addresses are authenticated and authorized to connect to the access point.

One advantage of this technique is that even if someone knows your wireless network SSID and WEP or WPA password, they cannot connect to the network unless they use the network card you have authenticated.

Therefore MAC address filtering is a pretty good security mechanism that you may not have heard much about. One reason why MAC address filtering is not widely used on wireless networks is because there are many problems associated with implementing and maintaining this mechanism.

MAC address filtering works only really well in small organizations, it is not practical to use in large enterprise class networks because each time a new network card is used, the card's MAC address that must be added to the MAC address filter. Similarly, whenever a laptop or wireless card does not work, the administrator must specify which MAC address belongs to the device and remove it from the whitelist.

Moreover, in large companies, there are often a lot of experts, appraisers and visitors, who need access over the wireless network. If you use the MAC address filtering technique, this has inadvertently prevented these visitors from accessing the wireless network.

The list management process of the MAC filter is quite elaborate, but these disadvantages are not enough to prevent organizations from using it. There are two problems that can prove to be disadvantages in using MAC address filtering techniques.

One of the two problems is the MAC address filtering technique implemented at the access point level. This will not be a problem for small or medium organizations, but for larger organizations, organizations with multiple physical and virtual wireless access points, managing the whitelist for each device This will be a simple task.

Another drawback in using MAC address filtering techniques is that access points require a reboot each time there is a change to the filter list. These reboots will be very annoying if an organization makes many changes to the filter list.

There are some who argue that these inefficiencies are still worth the advantages of using MAC address filtering.

In general, hackers are often unable to change their NIC to assign it another MAC address. Similarly, hackers are also incapable of changing your filter list if that list prevents them from accessing your network from the beginning. The reason why MAC address filtering is not considered completely reliable is because there are many ways to fake MAC addresses by software. For example, we have seen Windows drivers for wireless NICs come with an option to specify a different MAC address. If the hacker sniffs your wireless network, they can easily get the authenticated NIC's MAC address. Once this address is available, they can configure the computer to fake that address and increase access to your network.

So does this mean we should no longer use MAC address filtering techniques? Not that! You need to know that there is no perfect security feature. Security needs to be multi-layer and deep. In other words, you should have multiple security measures to prevent someone from breaking into your network. It is possible that MAC address filtering is an impractical option for large organizations but it is an option suitable for small and medium organizations.

Conclude

In this article, I have shown you some of the roles of SSID promotion and MAC address filtering in wireless network security. In Part 4 of this series, I will show you some other security options.