Wireless network traffic security - Part 4

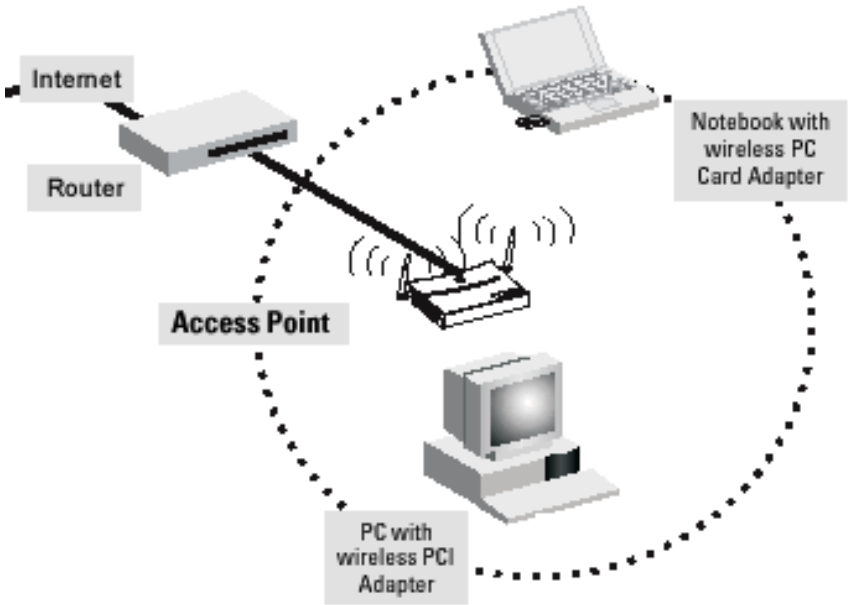
In the next part of this series, I will show you some of the security mechanisms available in wireless hardware.

Network Administration - In the next part of this article series, I will show you some of the security mechanisms available in wireless hardware.

In the previous article of this series, I talked about the importance of the SSID of a wireless access point, besides MAC address filtering. In this section, we will introduce some of the security features that are usually included in wireless access points. Here is a point to note that not all wireless access points have the features introduced here.

Encode

When it comes to securing wireless networks, a security feature seems to attract the most attention, encryption. It is for this reason that we want to start by providing you with some basic information about some general encryption options. Note here that we only introduce encryption mechanisms available in wireless hardware, OS-level encryption features will be introduced in the following sections.



No coding

In the first part of this series, we asked a question about what happens if the wireless network is not encrypted. The reason we ask this question is because in most access points, the configuration of connections is usually set to the unencrypted state by default.

If you're going to use OS-level encryption such as IPSec or if you will use an access point to provide public Wi-Fi access, not encrypting or encrypting is not a problem. However, in other cases, using one of the encryption options introduced below will be better for your network.

WEP

WEP (Wired Equivalent Privacy) is the first encryption algorithm of wireless networks. Today, most wireless access points still provide this WEP encryption mechanism, but their purpose is only to solve some compatibility issues. WEP encryption has shown many shortcomings in recent years and is currently considered unsafe.

WPA-PSK [TKIP]

WPA (Wi-Fi Protected Access) is designed as a mechanism to overcome the shortcomings of WEP. There are several formats of WPA, but the most well known is WPA-PSK, which uses pre-shared key encryption.

Some other WPA formats use a protocol called TKIP, which is the abbreviated name for the Temporal Key Integrity Protocol. TKIP will generate a 128-bit key for each data packet.

WPA2-PSK

WPA2-PSK is the next version of WPA. Although still using pre-shared keys, WPA2 replaced the TKIP encryption protocol with CCMP to enhance security. CCMP is based on the Advanced Encryption Standard (AES) algorithm using 10 encryption ciphers to generate 128-bit keys. WPA2 is currently the preferred encryption mechanism.

Other issues to pay attention to

Although encryption is a key security mechanism on any wireless access point, there is one important point we need to remember here that encryption will not secure the wireless network security. Comprehensive security can only be achieved by implementing deep defense, which also means that we must take full advantage of the existing security mechanisms. We will introduce some other security mechanisms available in some access points.

Record

Many access points have the ability to record what happens. For example, the access point we use has a logging mechanism, which allows creating log entries every time a connection is made. More importantly, the access point allows you to know where the connection originates (wired network, wireless network or Internet), the IP address of the device that wants to make the connection, the number of connection ports made through there.

The logs on our access point also allow tracing to logins that want to access the access point administrative interface. This feature allows us to easily detect non-authenticated access attempts.

Black list

Some access points have different blacklist types. For example, many access points provide this list so that users can use it for blocking access to certain websites. Although this feature is designed to block access to incompatible content, you can also use the blacklist as a way to prevent accidental access to websites that contain malicious code. In fact, there are many websites that provide a list of malicious sites and it is possible to use such a list in combination with the access point's blacklist feature to reduce user access errors. site like that.

Easy blacklist cannot solve all via URL. Some access points also allow users to make black lists through ports and services. For example, if the company's privacy policy restricts the use of e-mail software, you can use the access point blacklist to block instant messaging traffic. This way, even if the user can install instant messaging client software to the workstation, the client is useless.
If you decide to use a blacklist to prevent certain types of traffic from passing through your network, it is best to use both the port list and the list of services if available.

Warning

Some more advanced wireless access points also have warning mechanisms. When used, this mechanism will be a valuable asset for securing your wireless network.

The basic idea behind the warning is that users can define certain conditions that they want to know. These conditions can be any. For example, you might want to know when a user tries to access a website that is blocked or you might want to know when someone tries to log into the administration interface. Some wireless access points can even be configured to alert an administrator if someone tries to connect to an access point outside of the official business hours of the business.

Once you have defined the conditions for creating an alert, you must manually configure your alert. The warning options in each wireless access point are very different, but in general you can configure the access point so that it can email you when an event occurs.

Wireless signal

Another aspect of wireless security that we want to cover here is related to the signal generated by the access point. Some access points allow users to adjust signal strength. If your access point has such a feature, what you should do is reduce the signal strength so that it only covers a certain area you need.

Controlling the wireless signal so that its coverage does not extend beyond the periphery of the company is an essential action. This method will make your network safer from unfriendly eyes of someone on the street.

Conclude

So far, we've introduced some of the security aspects that come with wireless hardware. However, the security issue is not only in hardware but also has many useful features in Windows operating system. In the next part of the series, we will introduce you to those features.

tips and guides. Thank you for reading and for following us regularly.