Wireless security: Say NO to WEP and YES to WPA

If the reports and studies are accurate, a large number of wireless local area networks (WLANs), especially those used in homes, are using outdated and less secure WEP technology. ghost

If the reports and studies are accurate, a large number of wireless local area networks (WLANs), especially those used in homes, are using outdated and less secure WEP technology. Encrypted by yourself.

Back six years ago, when consumer WLAN hardware was first launched, it used a technology called WEP - Wired Equivalent Privacy.

WEP is built to protect a wireless network from eavesdropping. But soon after it discovered thousands of errors in this technology. The security of WEP is not equivalent at all as a wired network. Therefore, not long after, a new technology called WPA (Wi-Fi Protected Access) was born, overcome many disadvantages of WEP.

So far, WPA has become a mainstream technology for many years. But WEP still leaves a standard component in all virtual wireless routers on storage stacks. Although this component is retained only for the purpose of compatibility with the most 'ancient' hardware, but if information on many research reports is accurate, a significant amount of wireless local area network activity (WLAN), especially home wireless networks are still using outdated and less secure WEP techniques for their encryption mechanisms.

The widespread and widespread use of WEP can be interpreted as similar to the abbreviations WEP and WPA. They do not convey any different meaning between the two methods (even implied equivalent). In addition, WEP is always shown first on the security interface of most bandwidth routers, which was preceded by WEP and also preceded in alphabetical order.

Now we will see why we should not use WEP any more, and why WPA is a better choice.

WEP = Weak Encryption Protocol!

The biggest drawback of WEP is the use of static encryption keys. When setting up the WEP mechanism for the router, a key is used for all devices on the network to encrypt all transmission packets. But the truth is that these encoded packets cannot avoid the phenomenon of being blocked. Due to some 'esoteric' technical errors, an eavesdropper can completely block the number of encrypted packets to find out what the decryption key is.

The problem can be solved if you change the WEP key periodically (That's why routers usually allow 4 keys to be stored). But also quite annoying and annoying because changing the WEP key is very inconvenient and time-consuming, not only done on the router but also on all devices connected to it. As a result, most people only set up a single key and continue to use it forever.

A recent development program enhances the ability to change WEP keys regularly but is not effective at protecting WLANs. Hacker can crack WEP keys by blocking millions of packets plus the corresponding amount of time and resources.

But technology changes very quickly. Researchers in the computer science department of German University (Germany) have recently demonstrated the ability to destroy networks using WEP very quickly. After it takes less than a minute to block data (nearly 100,000 packets), they can break the WEP key in just three seconds. Testing was performed on a 1.7GHz Pentium M CPU system, a machine with processors even on low-end laptops is now rare.

Of course, does not mean that anyone who hides outside your home is able to unlock, hack a wireless network. But the ability to unlock easily with popular devices and software is increasing, many people worry. Why should I continue to use WEP while WPA is safer and easier to use?

Switch to WPA

Even if your router has a few years of life, it certainly still supports some WPA forms (if not, upgrading the latest firmware is OK). The easiest and most widely supported version of WPA Personal is now, sometimes called WPA Pre-Shared Key (PSK).

To encrypt a network with WPA Personal (or PSK), you need to provide the router with not an encryption key but a pure English passphrase of 8 to 63 characters. Using a technique called TKIP (Temporal Key Integrity

Protocol), that passphrase and the network SSID are used to create unique encryption keys for each wireless client. These encryption keys are changed frequently. (Although WEP also supports passphrases, it is only intended to make it easier to create a static key, usually including a HEXA character: numbers from 0 to 9 and letters A to F).

Unfortunately, there are still many wireless devices that do not support WPA on the market today (mostly power-consuming devices). Honestly, you should avoid buying these devices. For normal computers, WPA is supported both Windows XP Service Pack 2 and Mac OS X (of course, with Windows Vista). In XP, you will not find WPA options on Data encryption in the Wireless Network Connection properties sheet. Instead, look under Network Authencation and choose the type of Data encrytion that matches the settings on the router (TKIP or AES). (Many routers support AES, which is more powerful than TKIP).

If configured appropriately, WPA will initiate a better protection than WEP, but does not mean WPA is a universal security wall. You should avoid using SSID-related words and WPA passwords in the dictionary (the longer the password, the better). This will provide a better protection program than using your 'link system' or puppy name.

If the router or its base program is fairly new (within the last 18-24 months), WPA2 may be supported. WPA2 provides more advanced features than WPA, including the default setting of AES encryption. However, to use WPA2 on an XP system you need to download an update here.