# Wi-Fi security: Choose which solution?

Security is a very important issue and is especially concerned by businesses. Moreover, security is also the reason why businesses are afraid of installing wireless LAN (wireless LAN). They are concerned about security in WEP (Wire

**Security is a very important issue and is especially concerned by businesses. Moreover, security is also the reason why businesses are afraid of installing *wireless LAN* ( *wireless LAN* ). They are concerned about security in WEP ( *Wired Equivalent Privacy* ), and are interested in safer new security solutions.**

IEEE and Wi-Fi Alliance have developed a more secure solution: WPA ( *Wi-Fi Protected Access* ) and IEEE 802.11i *Wi-Fi protection* (also called "WPA2 Certified" under Wi-Fi Alliance). ) and another solution called VPN Fix also enhances wireless network security.

According to Webtorial, WPA and 802.11i are 29% and 22% respectively. On the other hand, 42% is used for other "situational solutions" such as: securing VPNs ( *Vitual Private Network* ) over wireless local area networks.

So, what security solution should we choose for wireless networks?

**WEP: Security is too bad**

WEP (Wired Equivalent Privacy) means wireless security equivalent to wired.In fact, WEP has brought both user authentication and data security to the same unsafe method.WEP uses an unchanged encryption key with a length of 64 bits or 128 bits, (minus 24 bits used for the encryption key initialization vector, so the key length is only 40 bits or 104 bits) used to authenticate devices that are allowed to access the network, and also used to encrypt data transmission.

Quite simply, these encryption keys are easily "broken" by brute-force algorithms and *trial-and-error* attacks.Free software like Airsnort or WEPCrack will allow hackers to break the encryption key if they collect between 5 and 10 million packets on a wireless network.128-bit encryption keys are also no better: 24 bits for encryption initialization, so only 104 bits are used for encryption, and the same way as 64-bit encryption, 128-bit encryption is also easily unlocked.In addition, the weaknesses in encryption key initialization vectors allow hackers to find passwords faster with a lot more information packages.

Without predicting errors in the encryption key, WEP can be created more robust security using an authentication protocol that provides each new encryption key for each session.The encryption key will change on each session.This will make it more difficult for hackers to gather all the necessary data packets to break the security key.

**Situation solution: VPN (Vitual Private Network) Fix**

Recognizing the weakness of WEP, business users have discovered an effective way to protect their WLAN wireless network, called VPN Fix.The basic idea of ??this method is to treat WLAN users as users of remote access services.

In this configuration, all WLAN access points, and also computers connected to these access points, are defined in a virtual LAN ( *Vitual LAN* ). In the security infrastructure, these devices are treated as "unreliable". Before any WLAN devices are connected, they will have to get permission from the LAN security component. The data as well as the connection of devices will have to run through an authentication server such as RADIUS, etc. The connection will then be established as a secure connection route encrypted by a protocol. Security such as IPSec, like when using remote access services over the Internet.

However, this solution is also not perfect, VPN Fix needs larger VPN traffic for the firewall, and need to create initialization procedures for each user. Moreover, IPSec does not support devices with many separate functions such as handheld devices, barcode scanners . Finally, from the network architecture point of view, configuration according to VPN is just a situation solution. not a combination with WLAN.

**Security solution with authentication**

The truth is that when it comes to security flaws in wireless LANs, the industry has spent a lot of effort to solve this problem. One thing to remember is that we need to deal with two issues: authentication and information security. Authentication ensures that legitimate users can access the network. Security keeps data transmission safe and not stolen on the line.

One of the advantages of authentication is that IEEE 802.1x uses EAP ( *Extensible Authentication Protocol* ) extension *authentication* .EAP is really a good base for authentication, and can be used with several other authentication protocols.These protocols include MD5, Transport Layer Security (TLS), Tunneled TLS (TTLS), Protected EAP (PEAP) and Cisco's Lightweight EAP (LEAP).

Fortunately, the choice of authentication protocol requires only a few basic elements.First of all, a mechanism only needs to provide one or two authentication methods, which can be called *mutual authentication* , meaning that the network will authenticate the user and the user will also authenticate. network. This is very important for WLANs, because hackers can add certain unauthorized access points between network devices and legitimate access points ( *man-in-the-middle* attacks *)* , to block and change packets on data transmission. And the MD5 encryption method does not provide cross-authentication, so it is not recommended to use WLAN.

**Standard 802.11i or WPA2 encryption**

A long-term solution is to use 802.11i equivalent to WPA2, certified by the Wi-Fi Alliance.This standard uses strong encryption algorithm and is called *Advanced Encryption Standard* (AES). AES uses symmetric encryption algorithm according to the Rijndael block, using a 128-bit encryption block, and 192 bits or 256 bits.

To evaluate this coding standard, the National Institute of Standards and Technology, NIST (National Institute of Standards and Technology), adopted this symmetric code algorithm. And this encryption standard is used for US government agencies to protect sensitive information. If you want to know more about how Rijndael algorithm works, you can visit http://en.wikipedia.org/wiki/Rijndael

While AES is considered much better security than WEP 128 bit or 168 bit DES (Digital Encryption Standard).To ensure performance, the encryption process needs to be performed in hardware devices such as integrated into the chip.However, very few WLAN cards or access points support hardware encryption at the present time.Furthermore, most Wi-Fi handsets and barcode scanners are not compatible with 802.11i standards.

**WPA (Wi-Fi Protected Access)**

Realizing the difficulties of upgrading to 802.11i, the Wi-Fi Alliance introduced another solution called Wi-Fi Protected Access (WPA).One of the most important improvements of WPA is the use of the TKIP ( *Temporal Key Integrity Protocol* ) key change function. WPA also uses RC4 algorithms like WEP, but fully encodes 128 bits. And another feature is that WPA changes the key for each packet. The tools to collect packets to break the encryption key are not possible with WPA. Because WPA changes the key continuously, the hacker never collects enough sample data to find the password. Not only that, WPA also includes information integrity checking (Message Integrity Check). Therefore, the data cannot be changed while on the line.

One of the biggest attractions of WPA is that there is no hardware upgrade required. Free software upgrades for most network cards and access points using WPA are easy and available. However, WPA does not support handheld devices and barcode scanners. According to the Wi-Fi Alliance, about 200 devices have been granted WPA compatibility certificates.

WPA has two options: WPA Personal and WPA Enterprise. Both of these options use the TKIP protocol, and the difference is only the initial encryption key initialized. WPA Personal is suitable for home and small office networks, initialization keys will be used at access points and workstation devices. Meanwhile, WPA for businesses needs an authentication server and 802.1x to provide initialization keys for each session.

While the Wi-Fi Alliance has launched WPA, it is considered to eliminate all vulnerable vulnerabilities of WEP, but users still do not really trust WPA. There is a flaw in WPA and this error only occurs with WPA Personal. When using a TKIP key change function is used to create the encrypted keys, if the hacker can guess the initialization key or part of the password, they can identify the entire password, therefore it is possible to decrypt the data. However, this vulnerability will also be removed by using non-predictable initialization keys (do not

use words like "PASSWORD" as a password).

This also means that WPA's TKIP technique is only a temporary solution, not providing the highest security method. WPA is only suitable for companies that do not transmit "confidential" data about commerce, or sensitive information . WPA is also suitable for day-to-day and technology-testing activities.

**Conclude**

While using VPN Fix over WLAN connections can be a good idea and will also be a right direction.But the inconvenience as well as the price and the increase in network traffic are also barriers to overcome.The transition to 802.11i and AES encryption provides the highest security.But organizations and agencies are still using thousands of WLAN cards that do not support this standard.Moreover, AES does not support handheld devices and barcode scanners or other devices . These are limitations when selecting 802.11i.

The shift to WPA is still challenging.Although, there are still security holes and maybe new vulnerabilities will be discovered.But at this point, WPA is a good choice.

**Minh Phuc** *(According to Newsfactor)*