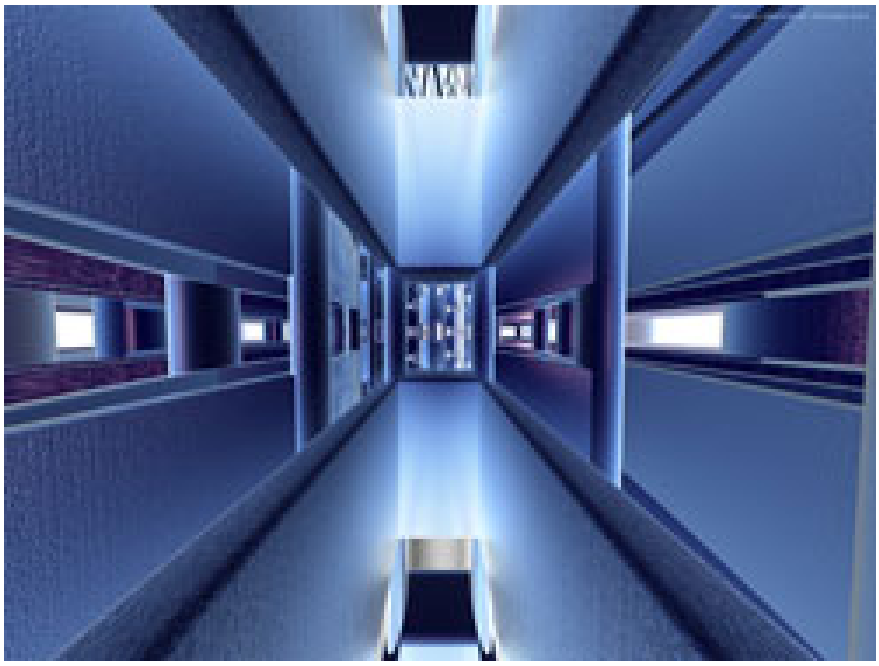
WEP - Security for wireless networks

In recent years, the information technology industry has witnessed a boom in the wireless network industry. Wireless communication capabilities are almost inevitable in handheld devices (PDAs), laptops, mobile phones and mobile phones.



In recent years, the information technology industry has witnessed a boom in the wireless network industry. Wireless communication capabilities are almost inevitable in handheld devices (PDAs), laptops, mobile phones and other digital devices.

With preeminent features for flexible connectivity, fast deployment capabilities, reduced costs, wireless networks have become one of the competitive solutions that can replace traditional Ethernet LAN networks. . However, the convenience of wireless networks also poses a great challenge on network security for network administrators. The advantage of the convenience of wireless connectivity can be reduced due to difficulties arising in network security.

When designing technical requirements for wireless networks, IEEE's 802.11 standard took into account the security of transmission data through WEP encryption. This method is supported by most wireless device manufacturers as a default security method. However, recent findings on weaknesses of the 802.11 WEP standard have raised doubts about the safety of WEP and the development of 802.11i. However, most of the current wireless devices are already using WEP and it will last long before the 802.11i standard is accepted and widely deployed.

Within the scope of this article, the author would like to present a brief overview of the concept and method of operation of WEP protocol, weaknesses and prevention, and provide an optimal WEP configuration method for the system. Small and medium network.

WEP protocol

WEP (*Wired Equivalent Privacy*) means security equivalent to a wired network (Wired LAN). This concept is part of the IEEE 802.11 standard. By definition, WEP is designed to ensure the security of wireless networks to the same degree as traditional cable networks. For LANs (defined by IEEE 802.3 standard), data security on the line for external attacks is ensured through physical limit measures, ie hackers cannot access the system directly. cable transmission line. Therefore, the 802.3 standard does not pose a problem of data encryption against unauthorized access. For the 802.11 standard, the problem of data encryption is a top priority because the characteristics of wireless networks are that it is not possible to physically limit access to the line, anyone within the coverage area can access it. data if not protected.

TERMS

Stream cipher method: The method of encrypting data in bits. In contrast to the block cipher method (block cipher), encrypting data according to each block of data (usually 64 bits). Thus, WEP provides security for data on the wireless network via encryption using RC4 symmetric algorithm, developed by Ron Rivest - of RSA Security Inc -. RC4 algorithm allows the length of the lock to change and can be up to 256 bits. The 802.11 standard requires mandatory WEP devices to support a minimum key length of 40 bits, while ensuring the option of supporting longer keys. Currently, most wireless devices support WEP with three key lengths: 40 bits, 64 bits and 128 bits.

With the RC4 encryption method, WEP provides security and integrity of information on the wireless network, and is considered as a method of access control. A wireless network connection without a WEP key will not be able to access the Access Point (AP) and will not be able to decode and change the data on the line. However, recent security analyst findings have shown that if the largest number is captured, specify encrypted data using WEP and use the appropriate, detectable tool. WEP key authentication in a short time. This weakness is due to a flaw in the way WEP uses RC4 encryption.

Restrictions of WEP

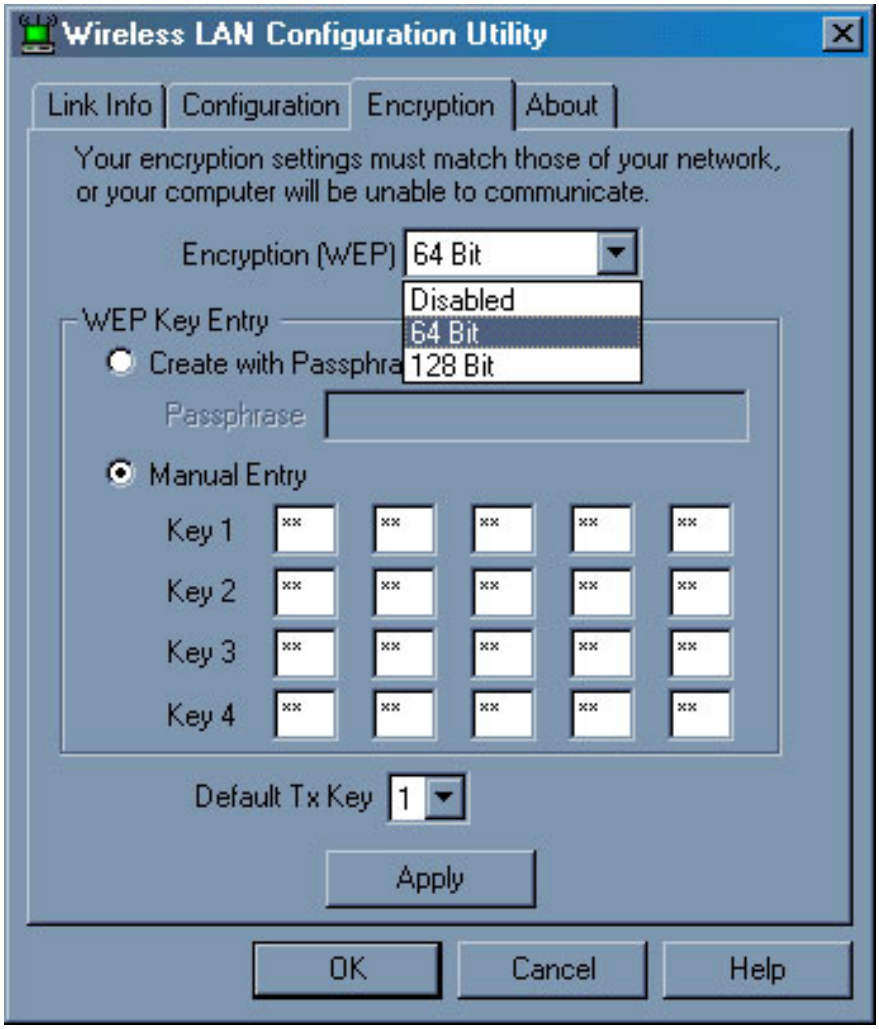
Because WEP uses RC4, an algorithm that uses stream cipher method, it is necessary to have a mechanism to ensure that the same two data will not produce the same result after being encoded twice. This is an important factor in data encryption to limit hackers' speculation. To achieve this goal, a value named Initialization Vector (IV) is used to add to the key to create a different key each time it is encrypted. IV is a value of 24 bits in length and recommended by the IEEE 802.11 standard (optional) must change according to each data packet. Since the sending machine creates IV not according to the law or standard, IV is required to be sent to the receiver in unencrypted form. The receiver will use the IV value and the key to decrypt the packet.

The use of value IV is the source of most problems with WEP. Since the value of IV is transmitted in unencrypted form and placed in the header of 802.11 data packets, anyone who "catches" the data on the network is visible. With a length of 24 bits, the value of IV ranges from 16,777,216 cases. Security experts at the University of California-Berkeley have discovered that when the same IV value is used with the same key on an encrypted packet (this concept is known as an IV collision), the hacker has Can capture the packet and find the WEP key. In addition, three coders Fluhrer, Mantin and Shamir (FMS) have discovered the weaknesses of the IV creation algorithm for RC4. FMS has outlined a method to detect and use error IVs to find WEP keys.

In addition, one of the biggest dangers is the attacks using the two methods mentioned above are passive. This means that the attacker only needs to receive data packets on the line without contacting the Access Point. This makes it difficult and almost undetectable to detect WEP key attack attacks.

Currently, the Internet is available with tools for finding WEP keys like AirCrack (Figure 1), AirSnort, dWepCrack, WepAttack, WepCrack, WepLab. However, to use these tools requires a lot of in-depth knowledge and they also have limitations on the number of data packets to capture.

Optimal WEP solution



With the serious weaknesses of WEP and the widespread spread of WEP key detection tools on the Internet, this protocol is no longer the security solution chosen for networks with high levels of information sensitivity. However, in many wireless networking devices today, the popular supported data security solution is still WEP. Anyway, WEP vulnerabilities can be mitigated if configured correctly, and use other security measures that are supportive.

To increase the level of security for WEP and make it difficult for hackers, the following measures are recommended:

• *Using WEP key with 128 bit length:* Usually WEP devices allow configuration of keys in three lengths: 40 bits,

64 bits, 128 bits. Using a 128-bit key increases the number of hacker packets that must be available to analyze IV, making it difficult and prolong the WEP key decryption time. If your wireless device only supports WEP at 40 bit level (common in older wireless devices), you need to contact the manufacturer to download the latest firmware update.

• *Implement policy to change the WEP key periodically:* Because WEP does not support the automatic lock change method, the periodic lock change will make it difficult for users. However, if you do not change the WEP key regularly, you should do it at least once a month or when it is suspected that it will be exposed.

• *Use data tracking tools on wireless links:* Because WEP lockers need to capture large numbers of data packets and hackers may have to use data generation tools so a sudden increase in data traffic may be a sign of a WEP attack, provoking network administrators to detect and apply timely preventive measures.

The future of WEP

As mentioned in the previous sections, WEP (802.11) does not provide the necessary security for most wireless applications that require high security. Due to the use of fixed keys, WEP can be easily cracked using the available tools. This motivates network administrators to find non-standard WEP solutions from manufacturers. However, since these solutions are not standardized, it makes it difficult to integrate devices between different manufacturers.

Currently, the 802.11i standard is being developed by IEEE with the aim of overcoming weaknesses of WEP and becoming a complete replacement for WEP when widely adopted and implemented. But the officially approved 802.11i standard has yet to be announced. Therefore, the wireless manufacturers association WiFi has proposed and widely popularized WPA (WiFi Protected Access) standard as a stepping stone before officially implementing 802.11i. Technically, WPA is the latest copy of 802.11i and ensures compatibility between devices from different manufacturers. To date, a number of new WiFi devices that support WPA and WPA2 address WEP security issues.

Conclude

Although there are serious disadvantages, WEP security is better than no encryption mechanism for wireless networks! WEP can be viewed as a security mechanism at the lowest level, necessary to be deployed when better methods cannot be used. This is suitable for situations where old wireless devices that do not support WPA are available, or situations that require low security such as home wireless networks, community wireless networks .