Tutorials

802.11 WEP: Concepts and Vulnerability

By Jim Geier

June 20, 2002

The security of a wireless LAN is very important, especially for applications hosting valuable information. For example, networks transmitting credit card numbers for verification or storing sensitive information are definitely

RELATED ARTICLES

New Wi-Fi Chip Enhances SOHO Security
Intersil Looks Beyond WEP
RSA Security Cuts Staff, Rejiggers Biz
Understanding Basic WLAN Security Issues

candidates for emphasizing security. In these cases and others, proactively safeguard your network against security attacks.

WEP (wired equivalent privacy) is 802.11's optional encryption standard implemented in the MAC Layer that most radio network interface card (NIC) and access point vendors support. When deploying a wireless LAN, be sure to fully understand the ability of WEP to improve security. It's complicated, but here we go.

WEP in action

If a user activates WEP, the NIC encrypts the payload (frame body and CRC) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security. The receiving station, such as an access point or another radio NIC, performs decryption upon arrival of the frame. As a result, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies.

As part of the encryption process, WEP prepares a keyschedule ("seed") by concatenating the shared secret key supplied by the user of the sending station with a random-generated 24-bit initialization vector (IV). The IV lengthens the life of the secret key because the station can change the IV for each frame transmission. WEP inputs the resulting "seed" into a pseudo-random number generator that produces a keystream equal to the length of the frame's payload plus a 32-bit integrity check value (ICV).

The ICV is a check sum that the receiving station eventually recalculates and compares to the one sent by the sending station to determine whether the transmitted data underwent any form of tampering while intransient. If the receiving station calculates an ICV that doesn't match the one found in the frame, then the receiving station can reject the frame or flag the user.

WEP specifies a shared secret 40 or 64-bit key to encrypt and decrypt the data. Some vendors also include 128 bit keys (know as "WEP2") in their products. With WEP, the receiving station must use the same key for decryption. Each radio NIC and access point, therefore, must be manually configured with the same key.

Before transmission takes place, WEP combines the keystream with the payload/ICV through a bitwise XOR process, which produces ciphertext (encrypted data). WEP includes the IV in the clear (unencrypted) within the first few bytes of the frame body. The receiving station uses this IV along with the shared secret key supplied by the user of the receiving station to decrypt the payload portion of the frame body.

In most cases the sending station will use a different IV for each frame (this is not required by the 802.11 standard). When transmitting messages having a common beginning, such as the "FROM" address in an e-mail, the beginning of each encrypted payload will be equivalent when using the same key. After encrypting the data, the beginnings of

these frames would be the same, offering a pattern that can aid hackers in cracking the encryption algorithm. Since the IV is different for most frames, WEP guards against this type of attack. The frequent changing of IVs also improves the ability of WEP to safeguard against someone compromising the data.

What's wrong with WEP?

WEP has been part of the 802.11 standard since initial ratification in September 1999. At that time, the 802.11 committee was aware of some WEP limitations; however, WEP was the best choice to ensure efficient implementations worldwide. Nevertheless, WEP has undergone much scrutiny and criticism over the past couple years.

WEP is vulnerable because of relatively short IVs and keys that remain static. The issues with WEP don't really have much to do with the RC4 encryption algorithm. With only 24 bits, WEP eventually uses the same IV for different data packets. For a large busy network, this reoccurrence of IVs can happen within an hour or so. This results in the transmission of frames having keystreams that are too similar. If a hacker collects enough frames based on the same IV, the individual can determine the shared values among them, i.e., the keystream or the shared secret key. This of course leads to the hacker decrypting any of the 802.11 frames.

The static nature of the shared secret keys emphasizes this problem. 802.11 doesn't provide any functions that support the exchange of keys among stations. As a result, system administrators and users generally use the same keys for weeks, months, and even years. This gives mischievous culprits plenty of time to monitor and hack into WEP-enabled networks. Some vendors deploy dynamic key distribution solutions based on 802.1X, which definitely improves the security of wireless LANs. The problem, however, is that these types of mechanisms won't be part of the 802.11 standard until the end of 2002 at best.

When WEP makes sense to employ

Despite the flaws, WEP is better than nothing, and you should enable WEP as a minimum level of security. Many people have taken to the streets to discover wireless LANs in neighborhoods, business areas, and colleges using protocol analyzers, such as AiroPeek and Airmagnet. Most of these people are capable of detecting wireless LANs where WEP is not in use and then use a laptop to gain access to resources located on the associated network.

By activating WEP, however, you significantly minimize this from happening, especially if you have a home or small business network. WEP does a good job of keeping most people out, at least those that are honest. Beware, though, there are true hackers around who can exploit the weaknesses of WEP and access WEP-enabled networks, especially those with high utilization.

Stay tuned! In the next tutorial, we'll discuss addition security

mechanisms you can deploy to protect wireless LANs beyond what WEP provides.

Jim Geier provides independent consulting services to companies developing and deploying wireless network solutions. He is the author of the book, Wireless LANs (SAMs, 2001), and regularly instructs workshops on wireless LANs.

Got a comment or question? Discuss it in the 802.11 Planet Forums

RELATED ARTICLES

New Wi-Fi Chip Enhances SOHO Security
Intersil Looks Beyond WEP
RSA Security Cuts Staff, Rejiggers Biz
Understanding Basic WLAN Security Issues

Email this article to a colleague
Go to a printable version of this story