Wi-Fi™ Security – Addressing Concerns

January 2002

Putting Wi-Fi™ Security in Perspective

Before this issue is explained in detail, the reader needs to keep in mind that Wi-Fi™ (IEEE 802.11) only attempts to provide security for the wireless portion of a network. It is not end-to-end security, and it was never intended to do more than prevent casual eavesdropping, which is what un-encrypted wired Local Area Networks (LANs) provide.

The user must, however, keep in mind that wireless networks cannot provide the same level of inherent security at the physical level that wired networks do. Radio waves pass through walls and can be intercepted from a distance. Even though a standard Wireless LAN (WLAN) card in a laptop may indicate a marginal or even non-existent signal, specialized equipment may be able to receive the signal from a much greater distance. By the same token, wired networks, at the physical level, are only as secure as an RJ-45 wall jack. More security is often required, whether the network is wired or wireless.

There are many components to effective network security, including the following:

Authentication - assurance that a packet comes from where it claims

Confidentiality - protection from disclosure to unauthorized persons

Access control - keeping unauthorized users out

Integrity - ensuring that data is error-free

Network security is generally implemented in layers, utilizing all of the above components and built around the seven-layer OSI Reference Model[1]. Unlike the common saying "strong as the weakest link," layered network security is just the opposite. It is as strong as its strongest link. For example, end-to-end security can be achieved by a strong mechanism in the application layer only, even if link-layer security is broken or non-existent. However, that solution only provides security for that particular application. The advantage to applying security at progressively lower levels is that it becomes generally available to more applications.

Also, remember that corporate WLANs are usually attached to a wired LAN. So even if 802.11 link-level security was very strong, it only applies to the wireless portion of the network. Higher-level layers of security may still need to be employed, even if a firewall is utilized for the wired portion. An RJ-45 jack is all it takes to acquire internal access to a wired network without higher layers of security.

Wi-Fi™ Security Options

IEEE 802.11 contains an encryption option intended to provide confidentiality. The Wired Equivalent Privacy (WEP) option is defined in the 802.11 standard as "protecting authorized users of a WLAN from casual eavesdropping." Recently, this security scheme has come under a great deal of criticism, accompanied by a number of papers which uncover weaknesses and outline how WEP can be defeated. Additionally, tools to exploit these weaknesses are now freely available over the Internet.

The Problem with WEP

WEP utilizes RC4[2], a *symmetric algorithm* known as a stream cipher, for encryption. A symmetric algorithm is one that relies on the concept of a single *shared key* (as opposed to a public key) that is used at one end to encrypt *plaintext* (the data) into *ciphertext* (the encrypted data), and at the other end to decrypt it – convert the ciphertext back to plaintext. Thus, the sender and the receiver share the same key, and it must be kept secret.

Stream ciphers encrypt data as it is received, as opposed to *block ciphers* that collect data in a buffer and then encrypt it a block at a time. Stream ciphers are tempting to use for applications requiring hardware implementation (i.e. wireless LAN cards), because they can be implemented very efficiently in silicon. However, care must be taken to ensure that the application is well suited for the proper implementation of a stream cipher, or for that matter, whatever encryption algorithm is being used.

Proper Use of Stream Ciphers

Stream ciphers are very simple and operate in theory by expanding the shared key into an infinite pseudo-random *key stream* which is logically combined (XORed) with the plaintext to produce ciphertext. Being a symmetric cipher, the user employs the shared key at the receiving end to regenerate the identical key stream, which is then XORed with the ciphertext to reproduce the plaintext. In practice, of course, an infinite key stream is never produced; it is only as long as the data stream being encrypted.

Once a key has been used to generate a key stream, the same key can never be reused again because it will generate the same key stream. If an attacker can obtain two different ciphertexts encrypted with the same key stream, the encryption process can be broken and the contents of the shared key determined. An important consequence of this is that if an encrypted transmission is interrupted and the encryption and decryption algorithms lose synchronization, and there is no means to resynchronize the process, then the entire message must be resent again, but with a different key.

The RC4 stream cipher has no mechanism to resynchronize the encryption process if an interruption occurs. Thus, it is not well-suited to applications where there is a possibility of a transmission being interrupted, unless provision is made to restart the session with a new key. For example, the RC4 stream cipher is successfully used to provide encryption for Secure Socket Layer (SSL) services for Internet transactions. An SSL session typically lasts a relatively short period of time and operates over a reliable channel where it is unlikely that a packet will be dropped. If it is, the session is started over, but with a different key. The new key is exchanged during a secure authentication process (using RSA public key cryptography) before the encrypted transaction is begun.

Improper Use of a Stream Cipher by WEP

The problem arises when the RC4 stream cipher is being used to encrypt data being sent over a channel, such as a wireless link, where it is highly likely that packets will be dropped. If there is no provision for key management (802.11 currently has none), then there is no way to create and exchange a new key with an authenticated user so that a packet can be resent.

The designers of WEP tried to get around this by appending a unique initialization vector (IV) consisting of a 24-bit number to the common shared 40-bit key. The effect is that instead of having only one 40-bit shared key available for use, there are now 2^{24} different 64-bit shared keys. The receiver only needs to know the secret shared 40-bit portion which is common to all of them. The unique 24-bit IV vector, which is transmitted unencrypted with each packet, determines which of the keys was used to encrypt a particular packet. The key stream is generated with this unique 64-bit "packet" key and the packet key and the key stream change for every packet.

One of the problems with this scheme is that there are only a finite number of IVs available for use, and there is no mechanism in place for changing the shared key when all of the available unique IVs get used up. Another is that the simple process of concatenating the IV onto the shared key produces unique keys that are too similar.

These fundamental weaknesses proved to be WEP's initial undoing. In the course of a year, a series of papers were published describing how these and other weaknesses could be used to compromise WEP. This has been great fodder for the technology press, which has sometimes showed its lack of understanding of security issues with headlines spelling subsequent doom for 802.11.

Chronology of Papers Revealing 802.11 Security Weaknesses

802.11e task group - As early as summer of 2000, the 802.11e task group began addressing weaknesses in WEP, included a concern that the key-size (then limited to 40 bits by export restrictions) was too small. A modification (WEP2) allowing use of a larger key was proposed.

Walker report[3] - In late October of 2000, Jesse Walker of Intel Corporation published a paper entitled "Unsafe at any key size: An analysis of the WEP encapsulation", in which he showed that WEP's use of a stream cipher was flawed, as explained above, and that increasing key size does not change this situation.

Berkeley report[4] - In February of 2001, a group of researchers at the University of California at Berkeley published a paper entitled "Security of the WEP Algorithm" which outlined various passive and active attacks on WEP. These attacks were considered by critics to be difficult to launch and might take days to get results.

University of Maryland report[5] - In March of 2001, a group of researchers at the University of Maryland published a paper entitled "Your 802.11 Wireless Network has No Clothes", in which they pointed out additional weaknesses in 802.11 security, specifically in the shared key and MAC address authentication procedures. They described an active attack which could get small amounts of data (but not the key) in as little as eight hours.

Fluhrer, Mantin, and Shamir report[6] - In September of 2001, Scott Fluhrer from Cisco Systems, and Itsik Mantin and Adi Shamir from The Weizmann Institute, published a paper entitled "Weaknesses in the Key Scheduling Algorithm of RC4," which outlines a completely passive attack on WEP that scales linearly with key size. Shortly thereafter,

programs appeared on the Internet that utilize this information to completely defeat the WEP key in as little as 15 minutes. (Note: RC4 as implemented in SSL is not able to be broken by this method.[7])

So… WEP is now generally considered to do no more than "discourage casual eavesdropping," which is all it was ever intended to do.

Fixing WEP – long term

The 802.11i TG has taken over security issues that were formerly being considered by the 802.11e TG. It is currently considering all of the issues in the above reports and is working on a draft supplement for 802.11 that will address the protocol or manner in which an encryption algorithm is utilized, as well as the specific encryption algorithm itself. It is felt that a supplement to 802.11 must completely address all components of security in order for the market to have a solution that is absolutely secure. In this respect, it is likely that the supplement will contain a broad and thorough treatment of a solution that ensures that, irregardless of the particular algorithm used for encryption, protocols for proper use of the algorithm are in place.

Fixing WEP – short term

In addition to providing enhancements to the standard 802.11 MAC that will be incorporated into future hardware, it is expected that the information in the supplement will provide manufacturers guidance for designing short-term firmware fixes for legacy 802.11b equipment. Informative text has been included in the draft supplement that describes a key scheduling scheme designed by RSA Security[8] and Hifn[9], called RC4 Fast Packet Keying[10], which addresses known WEP weaknesses.

Both short term and long term solutions will benefit from 802.1x, a higher layer protocol, for authentication and key management.

Providing Additional Security

802.1x is a new supplement to 802.1D (which defines MAC bridges between networks) that provides a port-based mechanism for achieving authentication for all 802 networks, wired or wireless. It defines a process for determining who the user is as soon as he plugs into a port or attempts to acquire access through a wireless AP. This has become an important issue not just because wireless signals leave the building and pass into unsecured space, but also because there needs to be a way to manage which users are authorized to access networks that are available in public spaces such as airports.

802.1x is a transport layer protocol that specifies Extensible Authentication Protocol (EAP), an encapsulated protocol that allows various higher layer authentication methods, referred to as Upper Layer Authentication Protocols (ULAPs), to be used to authenticate a user. ULAP options for authentication include Remote Authentication Dial-In Server (RADIUS), Kerberos, and Transport Layer Security (TLS).

For example, if a RADIUS server was employed for authentication on a WLAN, as soon as a station came within range of an access point, it could request access to the network. The access point would then forward the request to the RADIUS server for verification. If it was determined that the machine was authorized on that network, then a shared key would be sent to the station and network traffic would be allowed to flow. Newly-generated shared keys would be provided on a timely basis, to ensure that a new key was always available when a new key stream needed to be generated.

TLS is a successor to the SSL protocol that is commonly used for secure, web-based transactions. It provides privacy for Internet sessions between an application and an Internet user. For wireless applications, it will allow a client laptop to access a server through an AP for authentication purposes, and then decide on an encryption algorithm and keys to utilize before access is allowed to the network and vital data is exchanged.

Microsoft has embraced 802.1x as a means to bring a new level of manageability to network security. Windows® XP ships with an 802.1x client, which can be utilized for user identification, centralized authentication and dynamic key management. The Windows® RADIUS server has also been enhanced to support wireless device authentication.

Virtual Private Networks (VPNs) provide the most robust security solutions for corporate LANs and are already widely used for intranets and remote access. A VPN typically utilizes a dedicated server that provides both authentication and confidentiality. Wireless Access Points are also beginning to include VPN technologies within their devices, allowing simplified VPN deployment. Internet Protocol Security (IPSec) is the most common security mechanism used by VPNs. It provides a variety of authentication methods, including RADIUS and digital certificates, as well as confidentiality. IPSec provides confidentiality through encryption options such as DES, 3DES, and AES.

HP Recommends

HP recommends the following steps to insure that wireless networks are secure:

For home users and small offices:

- Use all of the 802.11 security options, including WEP.
- Change the default SSID of your product. Disable the “broadcast SSID” on APs if this is an option.
- Use any other security features specific to your vendor’s products.
- Change default passwords.
- Don’t use the default key. Change it immediately and then repeatedly on a regular basis.
- Small office users which require additional security and who do not have access to a VPN may want to consider using TLS to ensure the security of Internet sessions.

Additional steps for corporate users:

- Install the WLAN outside the firewall.

- Use a VPN with a physical authentication token such as a SmartCard or SecureID card.
- Use a tool like NetStumbler[11] to conduct WLAN audits[12] on a regular basis to ensure that there are no rogue access points.
- Consult a wireless integration firm, such as HP Consulting[13], to ensure a secure first installation.

References on the Web

[1]A good explanation of the seven-layer OSI Reference Model, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#xtocid130454
[2] RC4, http://www.rsasecurity.com/rsalabs/faq/3-6-3.html
[3] Walker report, www.dis.org/wl/pdf/unsafe.pdf
[4] Berkeley report, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[5] University of Maryland report, http://www.cs.umd.edu/~waa/wireless.pdf
[6] Fluhrer, Mantin, and Shamir report report, http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf
[7]RC4 in SSL is still secure, http://www.rsa.com/rsalabs/technotes/wep.html
[8] RSA Security, Inc., http://www.rsasecurity.com/
[9] Hifn, Inc., http://www.hifn.com/
[10] RC4 Fast Packet Keying, http://www.rsasecurity.com/rsalabs/technotes/wep-fix.html
[11] NetStumbler is available as shareware from http://www.netstumbler.com
[12] Exploiting and Protecting 802.11b Wireless Networks, http://www.extremetech.com/article/0,3396,apn%253D2%2526s%253D1024%2526a%253D13880%2526ap%253D1,00.asp
[13] HP Consulting, http://www.hp.com/hps/hpc/index.htm