13.1.4 Wireless Encryption and Authentication Facts

Security is absolutely critical for your wireless networks. As such, network administrators must take the necessary steps to prevent unauthorized access to the network and its data. One way to prevent unauthorized access is to use encryption and authentication.

This lesson covers the following topics:

- Wired Equivalent Privacy
- Wi-Fi Protected Access
- Wi-Fi Protected Access 2
- Extensible Authentication Protocol
- Lightweight Extensible Authentication Protocol
- Protected Extensible Authentication Protocol

Wired Equivalent Privacy

The original encryption protection mechanism developed for wireless networks was *Wired Equivalent Privacy (Wep)*, as specified in the IEEE 802.11b standard.

WEP is based on the Rivest Cipher 4 (RC4) encryption scheme that was designed to provide secure wireless connections equivalent to wired connections. A secret key is created on the access point and sent to all clients using an out-of-band medium (such as email). All clients add this secret key to their systems.

Hackers soon realized that although the relatively small IV changed each time a packet is sent, the secret key was always the same. Knowing this, they learned that they needed to focus only on cracking the IV, which would allow them to crack the rest of the packet. Eventually, hackers were able to crack these types of packets in as little as 10 minutes.

Wi-Fi Protected Access

Wi-Fi Protected Access was developed as an interim solution and delivers a level of security that goes beyond what WEP offered. WPA uses the *Temporal Key Integrity Protocol (TKIP)* and the *Message Integrity Code (MIC)*.

As an integrity check, TKIP lets WPA periodically and dynamically change the keys used by the system. In addition, TKIP uses a much larger initialization vector. With these two changes, the RC4 encryption scheme is able to produce a much longer keystream. This allows WPA to prevent hacking because finding two packets encrypted using the same key sequences is virtually impossible due to the extremely long keystream.

TKIP also uses an algorithm named Michael to produce an authentication code for each message. This message is known as the Message Integrity Code. MIC is designed to protect both the data payload and header on a WEP-encrypted network. WEP only protects the payload. This integrity-checking feature helps the system verify that the keys have not been tampered with.

WPA is still crackable, although the longer the passphrase/secret key is, the harder it is to crack.

Wi-Fi Protected Access 2

Wi-Fi Protected Access 2 improves on the security offered by WPA and is officially known as the IEEE 802.11i standard. WPA2 provides the highest level of wireless security available because it requires the uses of an encryption algorithm called *Advanced Encryption Standard (AES)*.

AES is an encryption algorithm that provides a more complex cipher then older ciphers such as RC4. AES can be used with either TKIP or the *Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)*. CCMP provides a higher level of security than TKIP. CCMP also provides data integrity and authentication. It is an improvement over TKIP because it has a larger block size for encryptions and a larger key size. It also has stronger algorithms that require more resources to run. Using CCMP in conjunction with AES ensures a higher level of security than TKIP and RC4.

When using WPA2, be aware that there are two versions or modes: Personal and Enterprise.

Version/Mode	Encryption Used	Authentication Used
Enterprise	AES - CCMP	IEEE 802.1x - Extensible Authentication Protocol (EAP)
Personal	AES - CCMP	Pre-shared keys (PSK)

Both modes use AES and CCMP to encrypt data. The main difference between these security versions is the authentication used. WPA2 Enterprise was specifically designed for use in organizations. It adheres to the IEEE 802.1x authentication standard, which uses the *Extensible Authentication Protocol (EPA)*, which provides enterprise-grade authentication.

WPA2 Personal uses pre-shared keys and is designed for home use. This means that only one unique global password is used and that everyone will use this same password before connecting to the wireless network. In addition, this password is saved on the device and could be a security hazard if the device is stolen. To ensure security in a business environment, every time a person leaves the company, a new password needs to be created and disseminated throughout the entire company.

The Enterprise version of WPA2 security (if used in conjunction with PEAP or LEAP) lets you assign each user a unique username and password to log into the wireless network. Using this method, an event such as someone losing a device or leaving the company would require a change only to the individual password or username.

Extensible Authentication Protocol

As previously discussed, EAP is used as the authentication protocol for WPA2 Enterprise. This authentication protocol also supports multiple authentication methods, such as smart cards and token cards, Kerberos, one-time passwords, certificates, and public key authentication. EAP can be used with *Remote Authentication Dial-In User Service (RADIUS)* to provide a more secure connection.

The following steps summarize the basic steps used to wirelessly authenticate using EAP and RADIUS:

1. The client requests a connection to a wireless network through an access point.
2. The access point requests the identity of the user and transmits that identity to a RADIUS server.
3. The RADIUS server asks the access point for proof of identity.
4. The access point gets the information from the user and sends it back to the server to complete the authentication process.

Using a RADIUS server with your wireless clients lets you to fortify your security by taking advantage of directory services solutions such as Microsoft Active Directory and OpenLDAP. This allows you to require users to provide their own unique core set of credentials, which are the same credentials they use to log in to the network with their wired connections.

Lightweight Extensible Authentication Protocol

To enhance or strengthen the authentication offered by EAP, Cisco developed its own proprietary wireless LAN authentication method called the *Lightweight Extensible Authentication Protocol*.

Although now depreciated, LEAP provided dynamic WEP keys and mutual authentication between wireless clients and a RADIUS server. LEAP also allowed clients to reauthenticate frequently. Upon each successful authentication, the clients acquired a new WEP key with the hope that the WEP keys wouldn't live long enough to be cracked.

As an alternative, LEAP can be configured to use TKIP instead of dynamic WEP. Although there is no native support for LEAP in any Windows operating system, it is widely supported by the third-party client software most commonly included with wireless LAN devices.

Protected Extensible Authentication Protocol

Despite some of the benefits offered by LEAP, it was still known as a crackable protocol. Therefore, Cisco, working in conjunction with Microsoft and RSA Security, developed the *Protected Extensible Authentication Protocol (PEAP*).

PEAP uses Transport Level Security (TLS), to create an encrypted channel between an authenticating PEAP client, such as a wireless laptop, and a PEAP authenticator, such as Microsoft Internet Authentication Service (IAS) or any RADIUS server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MSCHAPv2, that can operate through the TLS-encrypted channel provided by PEAP.

Depending on its implementation, EAP can use LEAP and PEAP in the following ways:

Service	LEAP	PEAP
Server authentication	Password hash	Public key certificate
Supplicant authentication	Password hash	Any EAP type such as public key certificate
Dynamic key delivery	Yes	Yes
Security concerns	Vulnerable to identity exposure	Vulnerable to man-in-the-middle attack