Chapter 9:
Wireless Security

9.1 Overview

Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using specialist equipment.

To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels.

9.2 Security of 802.11 Wireless LANs

This section discusses the built-in security features of 802.11. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. The IEEE 802.11 specification identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection as shown in Figure 9.1.

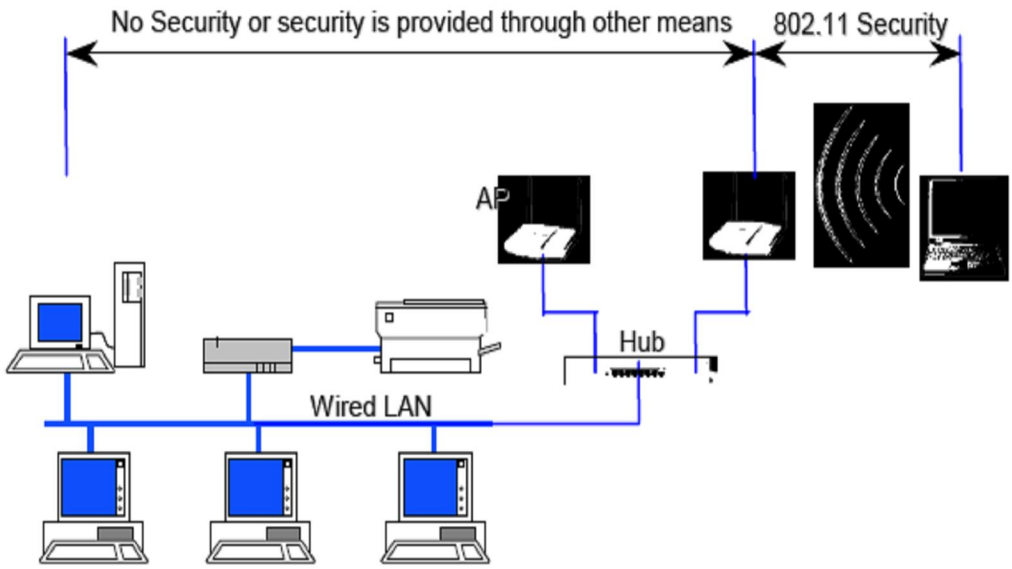

Figure 9.1 Wireless Security of 802.11 in Typical Network

Encryption is the process of transforming information to make it unreadable to anyone except those possessing special knowledge, usually referred to as a Key. The result of the process is **encrypted** information In many contexts, the word **encryption** also implicitly refers to the reverse process, **decryption** , to make the encrypted information readable again (i.e. to make it unencrypted).

Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as computers and networks, mobile telephones, and bank automatic teller machines. Encryption is also used in digital rights management to restrict the use of copyrighted material and in software copy protection to protect against reverse engineering and software piracy.

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to verify the integrity and authenticity of a message; for example, a message authentication code (MAC) or digital signatures. Standards and cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security is a challenging problem. A single slip-up in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption.

9.2.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (**WEP**) is a security protocol, specified in the IEEE Wireless Fidelity (WI-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms

(controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

How does it work?

WEP uses secret keys to encrypt data. Both AP and the receiving stations must know the secret keys.

There are two kinds of WEP with keys of either 64bits or 128bits. The longer key gives a slightly higher level of security (but not as much as the larger number would imply). In fact the user keys are 40bits and 104bits long, the other 24bits in each case being taken up by a variable called the Initialization Vector (IV).

When a packet is to be sent it is encrypted using a combination of the IV and the secret key. The IV is different (in theory) for each packet, while the secret key is fixed. The resulting packet data looks like random data and therefore makes the original message unreadable to an outsider not knowing the key. The receiving station reverses the encryption process to retrieve the message in clear text.

What is wrong with WEP?

- **Values can be reused**

  In fact the standard does not specify that the value needs to change at all. Reusing keys is a major cryptographic weakness in any security system.

- **Length is too short**

  24 bit keys allow for around 16.7 million possibilities. Sounds a lot, but on a busy network this number can be achieved in a few hours. Reuse is then unavoidable.

  Some manufacturers use 'random' keys. This is not the best way to ensure against reuse. A better solution is to start with a key and increment by one for each subsequent key. Unfortunately many devices revert to the same value at start up and then follow the same sequence providing lots of duplicate values for hackers to work on.

- **Weak keys are susceptible to attack**

  Certain keys value combinations, 'Weak IVs', do not produce sufficiently random data for the first few bytes. This is the basis of the highly publicized attacks on WEP and the reason that keys can be discovered.

Manufacturers often deliberately disallow Weak IV values. This is good in that it reduces the chances of a hacker capturing weak keys, but also has the effect of reducing the already limited key possibilities further, increasing the chance of reuse of keys.

- **Master keys are used directly**

  From a cryptographic point of view using master keys directly is not at all recommended. Master keys should only be used to generate other temporary keys. WEP is seriously flawed in this respect.

- **Key Management and updating is poorly provided for**

  Administration of WEP keys is not well designed and difficult to do on large networks. Users tend to change keys very infrequently which gives a potential hacker lots of time to collect enough packets to launch an attack.

- **Message integrity checking is ineffective**

  WEP does have a message integrity check but hackers can change messages and recompute a new value to match. This makes the checking ineffective against tampering.

9.2. 2 Wi-Fi Protected Access (WPA)

WPA is an encryption algorithm that takes care of a lot of the vunerablities inherent in WEP. WEP is, by design, flawed. No matter how good or crappy, long or short, your WEP key is, it can be cracked. WPA is different. A WPA key *can* be made good enough to make cracking it unfeasible. WPA is also a little more cracker friendly. By capturing the right type of packets, you can do your cracking offline. This means you only have to be near the AP for a matter of seconds to get what you need. Advantages and disadvantages.

WPA basically comes in two flavours RADIUS or PSK. PSK is crackable, RADIUS is not so much.

PSK uses a user defined password to initialize the TKIP, temporal key integrity protocol. There is a password and the user is involved, for the most part that means it is flawed. The TKIP is not really crackable as it is a per-packet key but upon the initialization of the TKIP, like during an authentication, we get the password (well the PMK anyways). A robust dictionary attack will take care of a lot of consumer passwords.

Radius involves physical transferring of the key and encrypted channels blah blah blah, look it up to learn more about it but 90% of commerical APs do not support it, it is more of an enterprise solution then a consumer one.

WPA Key Management

Rekeying of unicast encryption keys is optional with 802.1x. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key that is used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. The Temporal Key Integrity Protocol (TKIP) changes the unicast encryption key for every frame and each change is synchronized between the wireless client and the wireless AP. For the global encryption key, WPA includes a facility for the wireless AP to advertise changes to the connected wireless clients.

Temporal Key Integrity Protocol (TKIP)

WEP encryption is optional for 802.11. For WPA, encryption using TKIP is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, yet can be performed using the calculation facilities present on existing wireless hardware. TKIP also provides for:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each pre-shared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit ICV that is appended to the 802.11 payload and encrypted with WEP. AIthough the ICV is encrypted, it is possible through cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as Michael specifies a new algorithm that calculates an 8-byte message integrity code (MIC) with the calculation facilities available on existing wireless hardware. The MIC is placed between the data portion of the 802.11 frame and the 4-byte ICV. The MIC field is encrypted with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the 802.11 frame is used to prevent replay attacks.

Advanced Encryption Standard (AES) Support

WPA defines the use of AES as an additional optional replacement for WEP encryption. Because adding AES support through a firmware update might not be possible for existing wireless equipment, support for AES on wireless network adapters and wireless APs is not required.

Supporting a Mixture of WPA and WEP Wireless Clients

To support the gradual transition of a WEP-based wireless network to WPA, it is possible for a wireless AP to support both WEP and WPA clients simultaneously. During the association, the wireless AP determines which clients are using WEP and which are using WPA. The disadvantage

to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. All other security enhancements for WPA clients are preserved.

9.3 Authentication

The IEEE 802.11 specification defines two means to “validate” wireless users attempting to gain access toa wired network: open-system authentication and shared-key authentication. One means, shared-keyauthentication, is based on cryptography, and the other is not. The open-system authentication techniqueis not truly authentication; the access point accepts the mobile station without verifying the identity of thestation. It should be noted also that the authentication is only one-way: only the mobile station isauthenticated. The mobile station must trust that it is communicating to a real AP. A taxonomy of thetechniques for 802.11 is depicted in Figure 9.2.

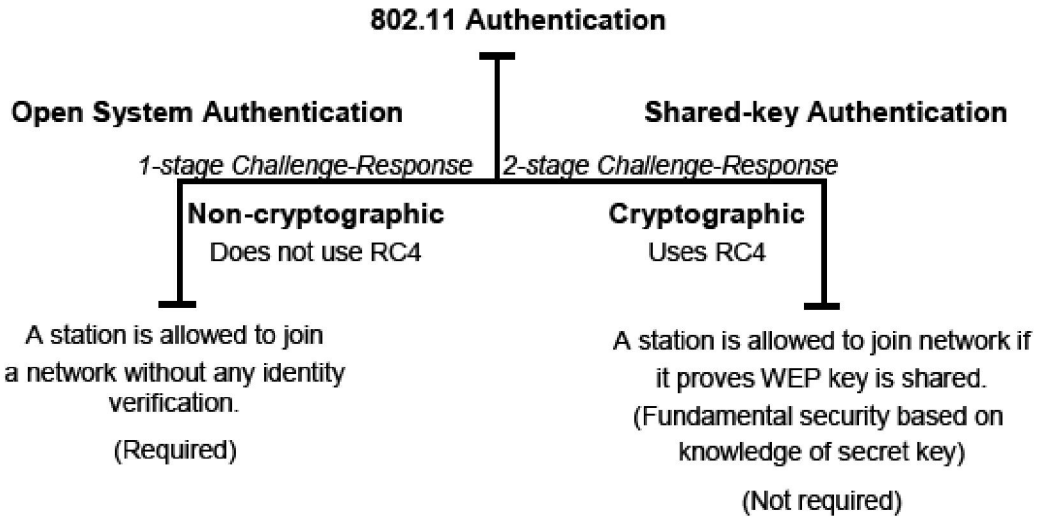

Figure 9.2 Taxonomy of 802.11 Authentication Techniques

With Open System authentication, a client is authenticated if it simply responds with a MAC addressduring the two-message exchange with an access point. During the exchange, the client is not trulyvalidated but simply responds with the correct fields in the message exchange. Obviously, with out cryptographic validatedation, open-system authentication is highly vulnerable to attack and practically invites unauthorized access. Open-system authentication is the only required form of authentication by the802.11 specification.

Shared key authentication is a cryptographic technique for authentication. It is a simple “challenge response ”scheme based on whether a client has knowledge of a shared secret. In this scheme, as depicted conceptually in Figure 2-5, a random challenge is generated by the access point and sent to the wireless client. The client, using a cryptographic key that is shared with the AP, encrypts the challenge (or“ nonce,” as it is called in security vernacular) and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if

the decrypted value is the same as the random challenge transmitted. The algorithm used in the cryptographic computation and for the generation of the 128-bit

challenge text is the RC4 stream cipher developed by Ron Rivest of MIT. It should be noted that the authentication method just described is a rudimentary cryptographic technique, and it does not provide mutual authentication. That is, the client does not authenticate the AP, and therefore there is no assurance that a client is communicating with a legitimate AP and wireless network. It is also worth noting that simple unilateral challenge-response schemes have long been known to be weak. They suffer from numerous attacks including the infamous "man-in-the-middle" attack. Lastly, the IEEE 802.11specification does not require shared-key authentication.

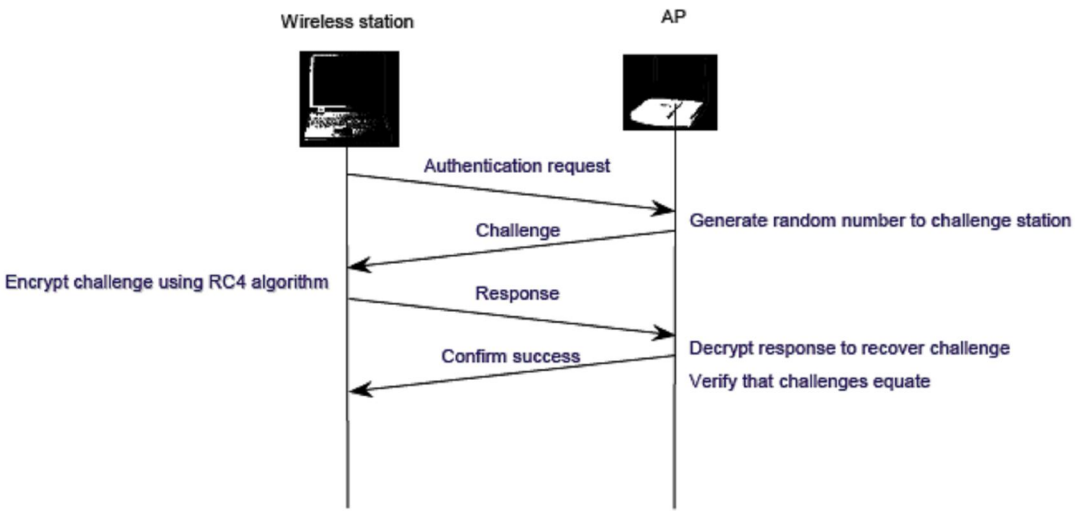

Figure 9.3 Shared-key Authentication Message Flow