CISCO SYSTEMS

A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite

1. Introduction

Since the ratification of the IEEE 802.11b standard in 1999, wireless LANs have become more prevalent. Today, wireless LANs are widely deployed in places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even coffeehouses.

These IEEE 802.11-based wireless LANs present new challenges for network administrators and information security administrators alike. Unlike the relative simplicity of wired Ethernet deployments, 802.11-based wireless LANs broadcast radio-frequency (RF) data for the client stations to hear. This presents new and complex security issues that involve augmenting the 802.11 standard.

Security in the IEEE 802.11 specification—which applies to 802.11b, 802.11a, and 802.11g—has come under intense scrutiny. Researchers have exposed several vulnerabilities in the authentication, data-privacy, and message-integrity mechanisms defined in the specification. This white paper:

- Reviews the authentication and data-privacy functions described in Clause 8 of the IEEE 802.11 specification
- Describes the inherent security vulnerabilities and management issues of these functions
- Explains how security issues can be addressed effectively only by augmenting the 802.11 security standard
- Examines Cisco Systems architecture for enhanced security on wireless LANs—including the Cisco Wireless Security Suite
- Looks ahead to long-term security enhancements

2. 802.11 Authentication and Its Weaknesses

Wireless LANs, because of their broadcast nature, require the addition of:

- User authentication to prevent unauthorized access to network resources
- Data privacy to protect the integrity and privacy of transmitted data

The 802.11 specification stipulates two mechanisms for authenticating wireless LAN clients: open authentication and shared key authentication. Two other mechanisms—the Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address—are also commonly used. This section explains each approach and its weaknesses.

The use of Wired Equivalent Privacy (WEP) keys can function as a type of access control because a client that lacks the correct WEP key cannot send data to or receive data from an access point. WEP, the encryption scheme adopted by the IEEE 802.11 committee, provides encryption with 40 bits or 104 bits of key strength. A subsequent section of this paper discusses WEP and its weaknesses in greater detail.

2.1. Service Set Identifier

The SSID is a construct that allows logical separation of wireless LANs. In general, a client must be configured with the appropriate SSID to gain access to the wireless LAN. The SSID does not provide any data-privacy functions, nor does it truly authenticate the client to the access point.
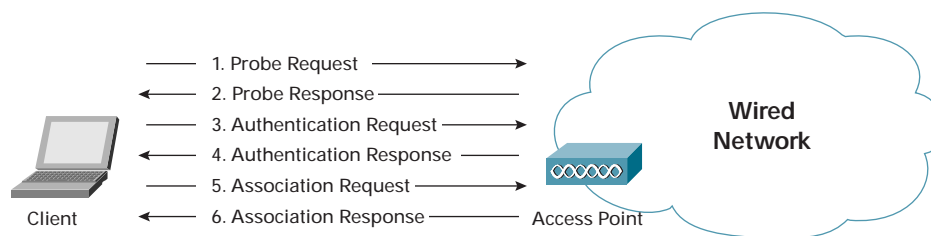
2.2. 802.11 Station Authentication

Authentication in the 802.11 specification is based on authenticating a wireless station or device instead of authenticating a user. The specification provides for two modes of authentication: open authentication and shared key authentication.

The 802.11 client authentication process consists of the following transactions (Figure 1):

1. Client broadcasts a probe request frame on every channel
2. Access points within range respond with a probe response frame
3. The client decides which access point (AP) is the best for access and sends an authentication request
4. The access point will send an authentication reply
5. Upon successful authentication, the client will send an association request frame to the access point
6. The access point will reply with an association response
7. The client is now able to pass traffic to the access point

Figure 1 802.11 Client Authentication Process

The next four subsections will detail each of the individual processes for client authentication.

2.2.1. Probe Requests and Responses

Once the client becomes active on the medium, it searches for access points in radio range using the 802.11 management frames known as probe request frames. The probe request frame is sent on every channel the client supports in an attempt to find all access points in range that match the SSID and client-requested data rates (Figure 2).

All access points that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information and access point load. The client can determine which access point to associate to by weighing the supported data rates and access point load. Once the client determines the optimal access point to connect to, it moves to the authentication phase of 802.11 network access.

Figure 2 Probe Request Frame

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 201 arrived at  10:18:59.4328; frame size is 39 (0027 hex) bytes.
DLC: Signal level             = 100%
DLC: Channel                  = 1
DLC: Data rate                = 2 ( 1.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = 40
DLC:               .... ..00 = 0x0 Protocol Version
DLC:               .... 00.. = 0x0 Management Frame
DLC:               0100 .... = 0x4 Probe request (Subtype)
DLC: Frame Control Field #2 = 00
DLC:               .... ...0 = Not to Distribution System
DLC:               .... ..0. = Not from Distribution System
DLC:               .... .0.. = Last fragment
DLC:               .... 0... = Not retry
DLC:               ...0 .... = Active Mode
DLC:               ..0. .... = No more data
DLC:               .0.. .... = Wired Equivalent Privacy is off
DLC:               0... .... = Not ordered
DLC: Duration                 = 0 (in microseconds)
DLC: Destination Address      = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source Address           = Station Airont500292
DLC: Basic Service Set ID     = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Sequence Control         = 0x6F30
DLC: ...Sequence Number       = 0x6F3 (1779)
DLC: ...Fragment Number       = 0x0  (0)
DLC: Element ID               = 0 (Service Set Identifier)
DLC: ...Length                = 7 octet(s)
DLC: ...Service Set Identity  = "sliders"
DLC:
DLC: Element ID               = 1 (Supported Rates)
DLC: ...Length                = 4 octet(s)
DLC: ...Supported Rates information field = 02
DLC:                          0... .... = Not Basic Service Set Basic Rate
DLC:                          .000 0010 =  1.0 Megabits per second
DLC: ...Supported Rates information field = 04
DLC:                          0... .... = Not Basic Service Set Basic Rate
DLC:                          .000 0100 =  2.0 Megabits per second
DLC: ...Supported Rates information field = 0B
DLC:                          0... .... = Not Basic Service Set Basic Rate
DLC:                          .000 1011 =  5.5 Megabits per second
DLC: ...Supported Rates information field = 16
DLC:                          0... .... = Not Basic Service Set Basic Rate
DLC:                          .001 0110 = 11.0 Megabits per second
DLC:
```

2.2.2. Open Authentication

Open authentication is a null authentication algorithm. The access point will grant any request for authentication. It might sound pointless to use such an algorithm, but open authentication has its place in 802.11 network authentication. Authentication in the 1997 802.11 specification is connectivity-oriented. The requirements for authentication are designed to allow devices to gain quick access to the network. In addition, many 802.11-compliant devices are hand-held data-acquisition units like bar code readers. They do not have the CPU capabilities required for complex authentication algorithms.

Open authentication consists of two messages:

- The authentication request (Figure 3)
- The authentication response (Figure 4)

Figure 3 Open Authentication Request

```
⊟▣ DLC: ----- DLC Header -----
  📄 DLC:
  📄 DLC: Frame 95 arrived at  10:49:47.8255; frame size is 30 (001E hex) bytes.
  📄 DLC: Signal level                = 100%
  📄 DLC: Channel                     = 1
  📄 DLC: Data rate                   = 2 ( 1.0 Megabits per second)
  📄 DLC:
  📄 DLC: Frame Control Field #1 = B0
  📄 DLC:                  .... ..00 = 0x0 Protocol Version
  📄 DLC:                  .... 00.. = 0x0 Management Frame
  📄 DLC:                  1011 .... = 0xB Authentication (Subtype)
  📄 DLC: Frame Control Field #2 = 00
  📄 DLC:                  .... ...0 = Not to Distribution System
  📄 DLC:                  .... ..0. = Not from Distribution System
  📄 DLC:                  .... .0.. = Last fragment
  📄 DLC:                  .... 0... = Not retry
  📄 DLC:                  ...0 .... = Active Mode
  📄 DLC:                  ..0. .... = No more data
  📄 DLC:                  .0.. .... = Wired Equivalent Privacy is off
  📄 DLC:                  0... .... = Not ordered
  📄 DLC: Duration                    = 314 (in microseconds)
  📄 DLC: Destination Address         = Station Airont31669C
  📄 DLC: Source Address              = Station Airont500292
  📄 DLC: Basic Service Set ID        = Airont31669C
  📄 DLC: Sequence Control            = 0x0A40
  📄 DLC: ...Sequence Number          = 0x0A4 (164)
  📄 DLC: ...Fragment Number          = 0x0   (0)
  📄 DLC: Authentication algorithm number = 0 (Open System)
  📄 DLC: Authentication transaction sequence number = 1
  📄 DLC: Status code                 = 0 (Reserved)
```

Figure 4 Open Authentication Response

```
⊟ ■▯ DLC: ----- DLC Header -----
  ─▯ DLC:
  ─▯ DLC: Frame 97 arrived at  10:49:47.8279; frame size is 30 (001E hex) bytes.
  ─▯ DLC: Signal level                 = 81 %
  ─▯ DLC: Channel                      = 1
  ─▯ DLC: Data rate                    = 22 (11.0 Megabits per second)
  ─▯ DLC:
  ─▯ DLC: Frame Control Field #1 = B0
  ─▯ DLC:               .... ..00 = 0x0 Protocol Version
  ─▯ DLC:               .... 00.. = 0x0 Management Frame
  ─▯ DLC:               1011 .... = 0xB Authentication (Subtype)
  ─▯ DLC: Frame Control Field #2 = 00
  ─▯ DLC:               .... ...0 = Not to Distribution System
  ─▯ DLC:               .... ..0. = Not from Distribution System
  ─▯ DLC:               .... .0.. = Last fragment
  ─▯ DLC:               .... 0... = Not retry
  ─▯ DLC:               ...0 .... = Active Mode
  ─▯ DLC:               ..0. .... = No more data
  ─▯ DLC:               .0.. .... = Wired Equivalent Privacy is off
  ─▯ DLC:               0... .... = Not ordered
  ─▯ DLC: Duration                     = 258 (in microseconds)
  ─▯ DLC: Destination Address          = Station Airont500292
  ─▯ DLC: Source Address               = Station Airont31669C
  ─▯ DLC: Basic Service Set ID         = Airont31669C
  ─▯ DLC: Sequence Control             = 0xED50
  ─▯ DLC: ...Sequence Number           = 0xED5 (3797)
  ─▯ DLC: ...Fragment Number           = 0x0  (0)
  ─▯ DLC: Authentication algorithm number = 0 (Open System)
  ─▯ DLC: Authentication transaction sequence number = 2
  ─▯ DLC: Status code                  = 0 (Successful)
```

Open authentication allows any device network access. If no encryption is enabled on the network, any device that knows the SSID of the access point can gain access to the network. With WEP encryption enabled on an access point, the WEP key itself becomes a means of access control. If a device does not have the correct WEP key, even though authentication is successful, the device will be unable to transmit data through the access point. Neither can it decrypt data sent from the access point (Figure 5).

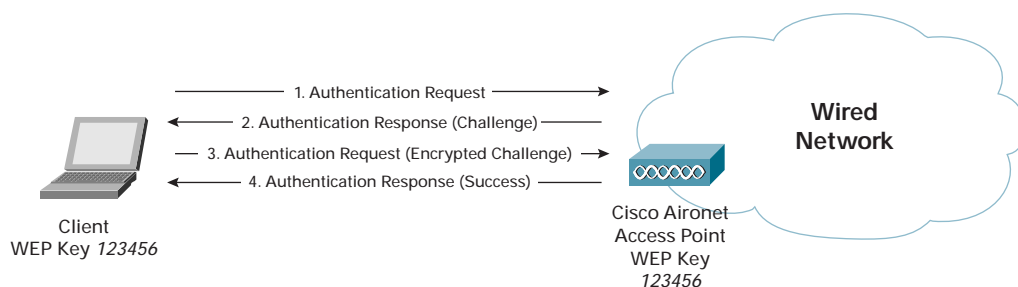**Figure 5** Open Authentication with Differing WEP Keys
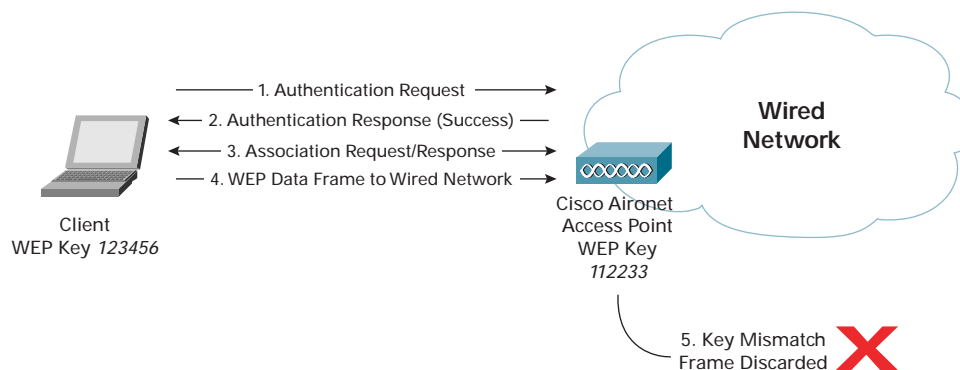
2.2.3. Shared Key Authentication

Shared key authentication is the second mode of authentication specified in the 802.11 standard. Shared key authentication requires that the client configure a static WEP key. Figure 6 describes the shared key authentication process.

1. The client sends an authentication request to the access point requesting shared key authentication

2. The access point responds with an authentication response containing challenge text

3. The client uses its locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request

4. If the access point can decrypt the authentication request and retrieve the original challenge text, then it responds with an authentication response that grants the client access

Figure 6 Shared Key Authentication Process

1. Authentication Request →
← 2. Authentication Response (Challenge)
3. Authentication Request (Encrypted Challenge) →
← 4. Authentication Response (Success)

Client
WEP Key *123456*

Cisco Aironet
Access Point
WEP Key
123456

Wired
Network

2.2.4. MAC Address Authentication

MAC address authentication is not specified in the 802.11 standard, but many vendors—including Cisco—support it. MAC address authentication verifies the client's MAC address against a locally configured list of allowed addresses or against an external authentication server (Figure 7). MAC authentication is used to augment the open and shared key authentications provided by 802.11, further reducing the likelihood of unauthorized devices accessing the network.

Figure 7 MAC Address Authentication Process

1. Association Request →
2. Client MAC Sent as RADIUS Request (PAP) →

Cisco Aironet Access Point   RADIUS

Client
MAC Address ABC
← 4. Association Response (Success)
← 3. RADIUS-ACCEPT
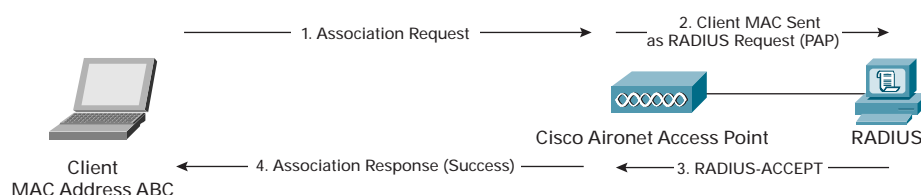
2.3. Authentication Vulnerabilities

2.3.1. Use of SSID

The SSID is advertised in plain-text in the access point beacon messages (Figure 8). Although beacon messages are transparent to users, an eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyzer, like Sniffer Pro. Some access-point vendors, including Cisco, offer the option to disable SSID broadcasts in the beacon messages. The SSID can still be determined by sniffing the probe response frames from an access point (Figure 9).

The SSID is not designed, nor intended for use, as a security mechanism. In addition, disabling SSID broadcasts might have adverse effects on Wi-Fi interoperability for mixed-client deployments. Therefore, Cisco does not recommend using the SSID as a mode of security.

Figure 8 SSID in an Access Point Beacon Frame
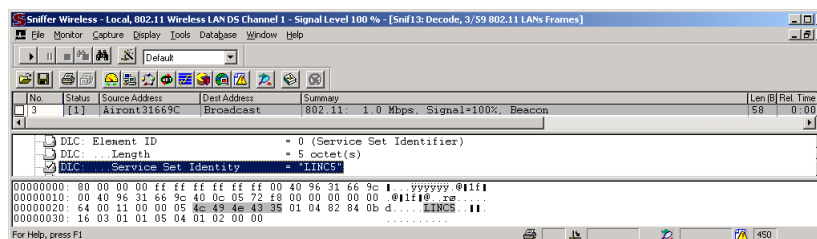
Figure 9 SSID in an Access Point Probe Response Frame
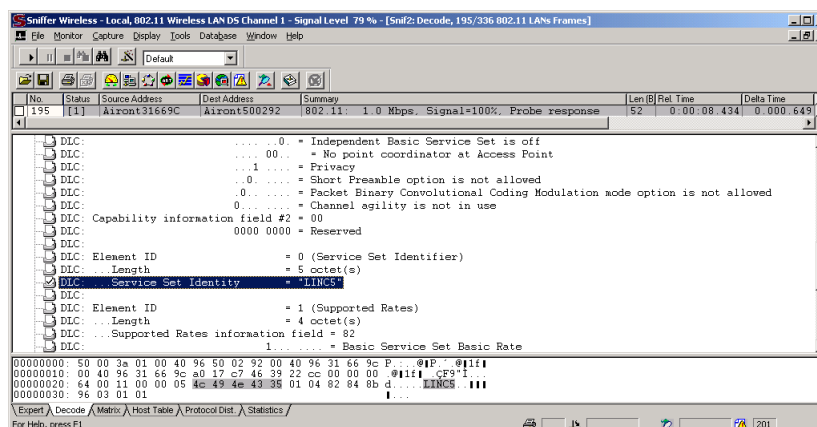
2.3.2. Open Authentication Vulnerabilities

Open authentication provides no way for the access point to determine whether a client is valid. This is a major security vulnerability if WEP encryption is not implemented in a wireless LAN. Cisco does not recommend deploying wireless LANs without WEP encryption. In scenarios in which WEP encryption is not needed or is not feasible to deploy, such as public wireless LAN deployments strong, higher-layer authentication can be provided by implementing a Service Selection Gateway (SSG).
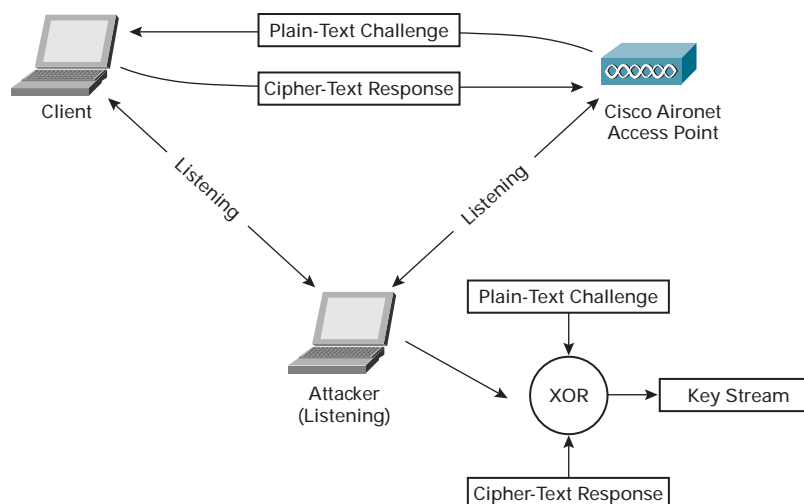
2.3.3. Shared Key Authentication Vulnerabilities

Shared key authentication requires the client use a preshared WEP key to encrypt challenge text sent from the access point. The access point authenticates the client by decrypting the shared key response and validating that the challenge text is the same.

The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack. An eavesdropper can capture both the plain-text challenge text and the cipher-text response. WEP encryption is done by performing an exclusive OR (XOR) function on the plain-text with the key stream to produce the cipher-text. It is important to note that if the XOR function is performed on the plain-text and cipher-text are XORed, the result is the key stream. Therefore, an eavesdropper can easily derive the key stream just by sniffing the shared key authentication process with a protocol analyzer (Figure 10).

Figure 10 Vulnerability of Shared Key Authentication

2.3.4. MAC Address Authentication Vulnerabilities

MAC addresses are sent in the clear as required by the 802.11 specification. As a result, in wireless LANs that use MAC authentication, a network attacker might be able to subvert the MAC authentication process by "spoofing" a valid MAC address.

MAC address spoofing is possible in 802.11 network interface cards (NICs) that allow the universally administered address (UAA) to be overwritten with a locally administered address (LAA). A network attacker can use a protocol analyzer to determine a valid MAC address in the business support system (BSS) and an LAA-compliant NIC with which to spoof the valid MAC address.

3. WEP Encryption and Its Weaknesses

WEP is based on the RC4 algorithm, which is a symmetric key stream cipher. As noted previously, the encryption keys must match on both the client and the access point for frame exchanges to succeed. The following section will examine stream ciphers and provide some perspective on how they work and how they compare to block ciphers.
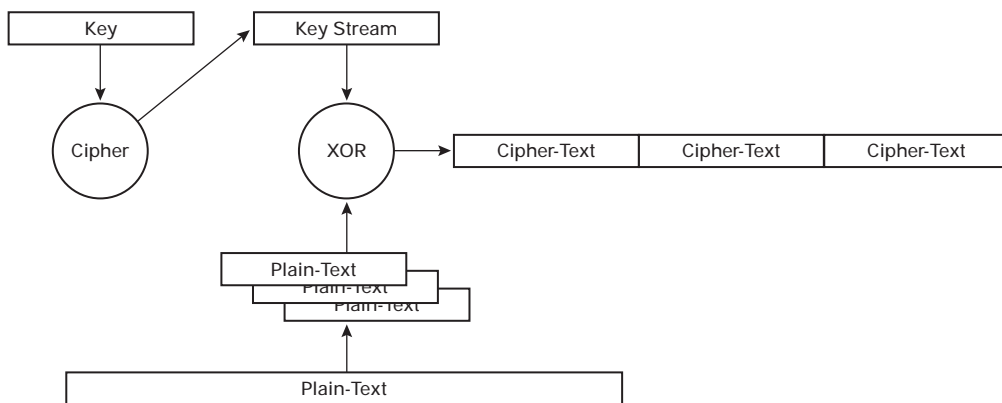
3.1. Stream Ciphers and Block Ciphers

A stream cipher encrypts data by generating a key stream from the key and performing the XOR function on the key stream with the plain-text data. The key stream can be any size necessary to match the size of the plain-text frame to encrypt (Figure 11).

Figure 11 Stream Cipher Operation
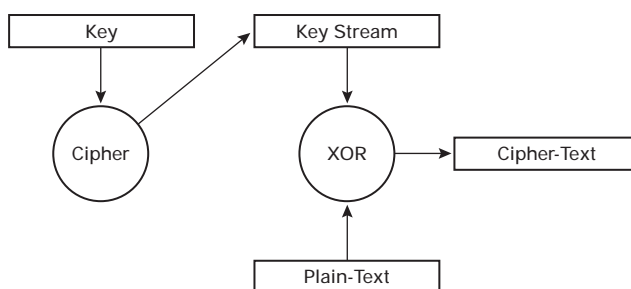
Block ciphers deal with data in defined blocks, rather than frames of varying sizes. The block cipher fragments the frame into blocks of predetermined size and performs the XOR function on each block. Each block must be the predetermined size, and leftover frame fragments are padded to the appropriate block size (Figure 12). For example, if a block cipher fragments frames into 16 byte blocks, and a 38-byte frame is to be encrypted, the block cipher fragments the frame into two 16-byte blocks and one six-byte block. The six-byte block is padded with 10 bytes of padding to meet the 16-byte block size.

Figure 12 Block Cipher Operation

The process of encryption described above for stream ciphers and block ciphers is known as Electronic Code Book (ECB) mode encryption. With ECB mode encryption, the same plain-text input always generates the same cipher-text output. As Figure 13 illustrates, the input text of "FOO" always produces the same cipher-text. This is a potential security threat because eavesdroppers can see patterns in the cipher-text and start making educated guesses about what the original plain-text is.

Figure 13 Electronic Code Book Encryption
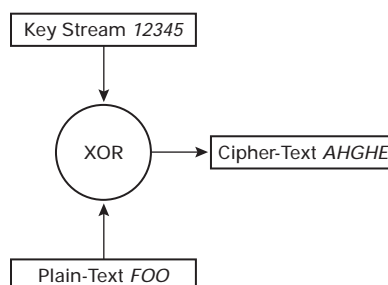
There are two encryption techniques to overcome this issue:

- Initialization vectors
- Feedback modes

3.1.1. Initialization Vectors

An initialization vector (IV) is used to alter the key stream. The IV is a numeric value that is concatenated to the base key before the key stream is generated. Every time the IV changes, so does the key stream. Figure 14 shows the same plain-text "FOO" with the XOR function performed with the IV augmented key stream to generate different cipher-text. The 802.11 standard recommends that the IV change on a per-frame basis. This way, if the same packet is transmitted twice, the resulting cipher-text will be different for each transmission.

Figure 14 Encryption with an Initialization Vector
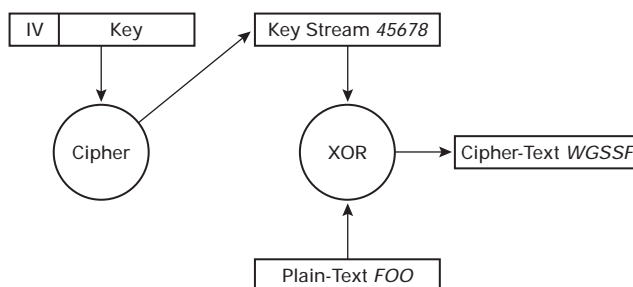
The IV is a 24-bit value (Figure 15) that augments a 40-bit WEP key to 64 bits and a 104-bit WEP key to 128 bits. The IV is sent in the clear in the frame header so the receiving station knows the IV value and is able to decrypt the frame (Figure 16). Although 40-bit and 104-bit WEP keys are often referred to as 64-bit and 128-bit WEP keys, the effective key strength is only 40 bits and 104 bits, respectively, because the IV is sent unencrypted.

Figure 15 Initialization Vector in a WEP-Encrypted Frame

Encrypted

Octets	IV	MAC Service Data Unit (MSDU)	ICV
		0-2304	4

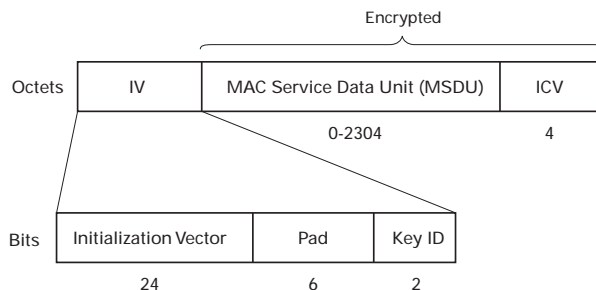| Bits	Initialization Vector	Pad	Key ID
	24	6	2

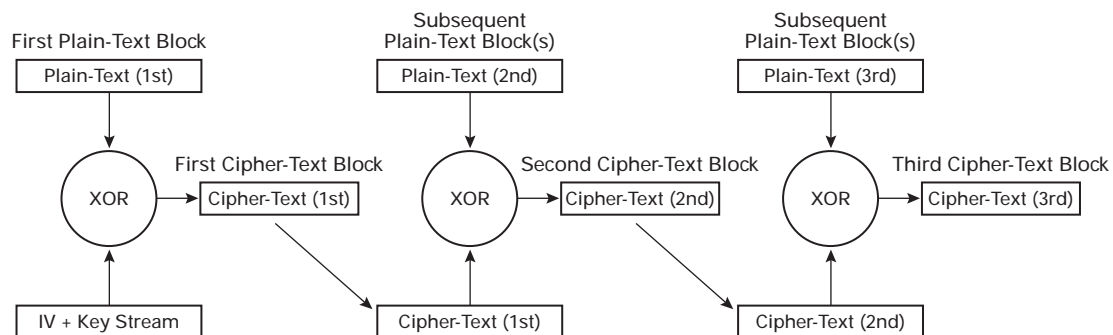**Figure 16** Initialization Vector in an 802.11 Protocol Decode

```
DLC: WEP (Wired Equivalent Privacy) Header
DLC:    ...Initialization Vector #(1-3)= D200F8
DLC:    ...Initialization Vector #4     = C0
DLC:                      11.. .... = 3 (Key ID 4)
DLC:                      ..00 0000 = Pad
DLC:    ...[68 byte(s) of encrypted MSDU]
DLC:    ...Encrypted Integrity Check Value = F9E3F873
```

3.1.2. Feedback Modes

Feedback modes are modifications to the encryption process to prevent a plain-text message from generating the same cipher-text during encryption. Feedback modes are generally used with block ciphers, and the most common feedback mode is known as cipher block chaining (CBC) mode.

The premise behind CBC mode is that a plain-text block has the XOR function performed with the previous block of cipher-text. Because the first block has no preceding cipher-text block, an IV is used to change the key stream. Figure 17 illustrates the operation of CBC mode. Other feedback modes are available, and some will be discussed later in this paper.

Figure 17 CBC Mode Block Cipher

First Plain-Text Block
| Plain-Text (1st) |

Subsequent Plain-Text Block(s)
| Plain-Text (2nd) |

Subsequent Plain-Text Block(s)
| Plain-Text (3rd) |

First Cipher-Text Block
XOR → | Cipher-Text (1st) |

Second Cipher-Text Block
XOR → | Cipher-Text (2nd) |

Third Cipher-Text Block
XOR → | Cipher-Text (3rd) |

| IV + Key Stream |

| Cipher-Text (1st) |

| Cipher-Text (2nd) |

3.2. Statistical Key Derivation—Passive Network Attacks

In August 2001, cryptanalysts Fluhrer, Mantin, and Shamir determined that a WEP key could be derived by passively collecting particular frames from a wireless LAN. The vulnerability is how WEP has implemented the key scheduling algorithm (KSA) from the RC4 stream cipher. Several IVs (referred to as weak IVs) can reveal key bytes after statistical analysis. Researchers at AT&T/Rice University as well as the developers of the AirSnort application implemented this vulnerability and verified that WEP keys of either 40- or 128-bit key length can be derived after as few as 4 million frames. For high-usage wireless LANs, this translates to roughly four hours until a 128-bit WEP key is derived.

This vulnerability renders WEP ineffective. Using dynamic WEP keys can mitigate this vulnerability, but reactive efforts only mitigate known issues. To eliminate this vulnerability, a mechanism that strengthens the WEP key is required.

3.3. Inductive Key Derivation—Active Network Attacks

Inductive key derivation is the process of deriving a key by coercing information from the wireless LAN and is also referred to as an active network attack. As mentioned in the section on stream ciphers, encryption is accomplished by performing the XOR function with the stream cipher to produce the cipher-text. Inductive network attacks work on this premise.

Man-in-the-middle attacks, a form of inductive key derivation attack, are effective in 802.11 networks because of the lack of effective message integrity. The receiver of a frame cannot verify that the frame was not tampered with during its transmission. In addition, the Integrity Check Value (ICV) used to provide message integrity is based on the 32-bit cyclic redundancy check (CRC32) checksum function. The CRC32 value is vulnerable to bit-flipping attacks, which render it ineffective. With no effective mechanism to verify message integrity, wireless LANs are vulnerable to man-in-the-middle attacks, which include bit-flipping attacks and IV replay attacks.

#### 3.3.1. Initialization Vector Replay Attacks

The initialization vector (IV) replay attack is a network attack that has been practically implemented, not just theorized. Although various forms of the network attack exist, the one that clearly illustrates its inductive nature is described below and illustrated in Figure 18:

1. A known plain-text message is sent to an observable wireless LAN client (an e-mail message)
2. The network attacker will sniff the wireless LAN looking for the predicted cipher-text
3. The network attacker will find the known frame and derive the key stream
4. The network attacker can "grow" the key stream using the same IV/WEP key pair as the observed frame

This attack is based on the knowledge that the IV and base WEP key can be reused or replayed repeatedly to generate a key stream large enough to subvert the network.

Figure 18 Initialization Vector Reuse Vulnerability
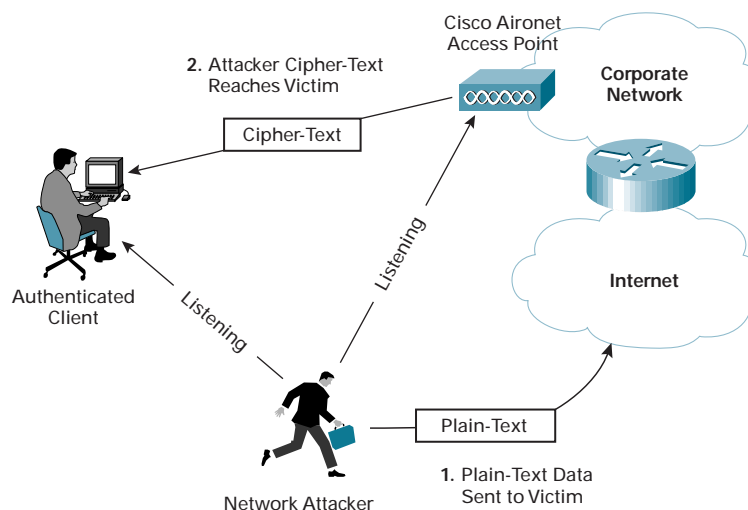
Once a key stream has been derived for a given frame size, it can be "grown" to any size required. This process is described below and illustrated in Figure 19:

1. The network attacker can build a frame one byte larger than the known key stream size; an Internet Control Message Protocol (ICMP) echo frame is ideal because the access point solicits a response

2. The network attacker then augments the key stream by one byte

3. The additional byte is guessed because only 256 possible values are possible

4. When the network attacker guesses the correct value, the expected response is received: in this example, the ICMP echo reply message

5. The process is repeated until the desired key stream length is obtained

Figure 19 "Growing" a Key Stream
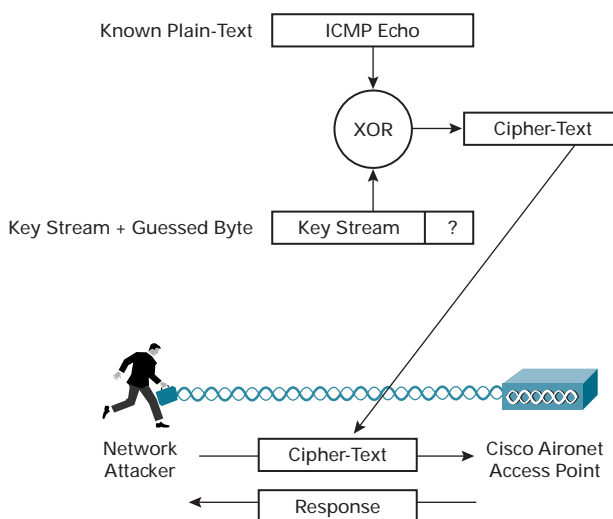
3.3.2. Bit-Flipping Attacks

Bit-flipping attacks have the same goal as IV replay attacks, but they rely on the weakness of the ICV. Although the data payload size may vary, many elements remain constant and in the same bit position. The attacker will tamper with the payload portion of the frame to modify the higher layer packet. The process for a bit-flipping attack is listed below and in Figure 20:

1. The attacker sniffs a frame on the wireless LAN

2. The attacker captures the frame and flips random bits in the data payload of the frame

3. The attacker modifies the ICV (detailed later)

4. The attacker transmits the modified frame

5. The receiver (either a client or the access point) receives the frame and calculates the ICV based on the frame contents

6. The receiver compares the calculated ICV with the value in the ICV field of the frame

7. The receiver accepts the modified frame

8. The receiver de-encapsulates the frame and processes the Layer 3 packet

9. Because bits are flipped in the layer packet, the Layer 3 checksum fails

10. The receiver IP stack generates a predictable error

11. The attacker sniffs the wireless LAN looking for the encrypted error message

12. Upon receiving the error message, the attacker derives the key stream as with the IV replay attack

Figure 20 Bit-Flipping Attack
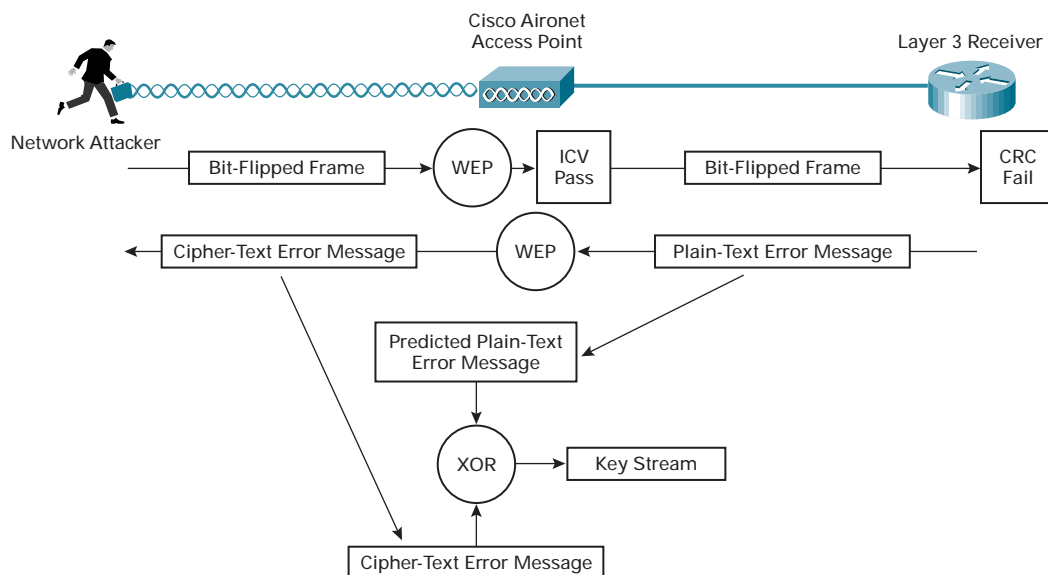
The basis for this attack is the failure of the ICV. The ICV is in the WEP-encrypted portion of the frame, so how is the attacker able to modify it to match the bit-flipped changes to the frame? The process of flipping bits is:

1. A given frame (F1 in Figure 21) has an ICV (C1)

2. A new frame is generated (F2) the same length as F1 with bits set

3. Frame F3 is created by performing the XOR function F1 and F2

4. The ICV for F3 is calculated (C2)

5. ICV C3 is generated by performing the XOR function C1 and C2

Figure 21 ICV Weakness
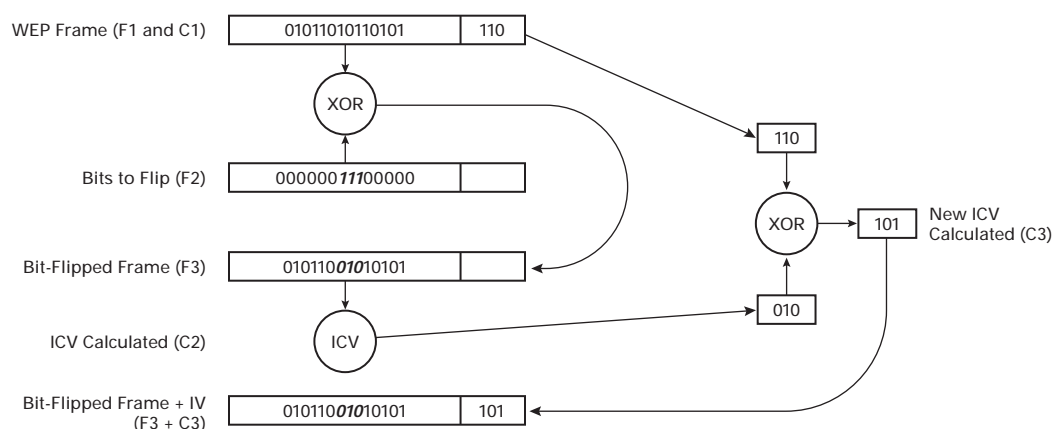
3.4. Static WEP Key Management Issues

The 802.11 standard does not specify key management mechanisms. WEP is defined to support only static, preshared keys. Because 802.11 authentication authenticates a device and not the user of the device, the loss or theft of a wireless adapter becomes a security issue for the network. The loss of an adapter and the compromising of the existing key presents network administrators with the tedious task of manually rekeying all wireless devices in the network.

This task might be acceptable for small deployments but is not realistic in midsize and large deployments in which the number of wireless users can reach into the thousands. Without a mechanism to distribute or generate keys, administrators must watch wireless NICs closely.

4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite

Cisco recognizes the vulnerabilities in 802.11 authentication and data privacy. To give customers a secure wireless LAN solution that is scalable and manageable, Cisco has developed the Cisco Wireless Security Suite. This suite of security enhancements augments 802.11 security by implementing prestandards enhancements to 802.11 authentication and encryption.

Some mistakenly believe WEP to be the only component to wireless LAN security, but wireless security actually consists of three components:

- The authentication framework
- The authentication algorithm
- The data privacy or encryption algorithm

All three of these components are included in the Cisco Wireless Security Suite:

- **802.1X authentication framework**—The IEEE 802.1X standard provides a framework for many authentication types and the link layer
- **Extensible Authentication Protocol (EAP) Cisco authentication algorithm**—The EAP Cisco Wireless authentication type, also called Cisco LEAP supports centralized, user-based authentication with the ability to generate dynamic WEP keys
- **Temporal Key Integrity Protocol (TKIP)**—Cisco has implemented two components to augment WEP encryption:
  - **Message Integrity Check (MIC)**—The MIC function provides effective frame authenticity to mitigate man-in-the-middle vulnerabilities
  - **Per-Packet Keying**—Per-packet keying provides every frame with a new and unique WEP key that mitigates WEP key derivation attacks
  - **Broadcast Key Rotation**—Dynamic key rotation for broadcast and multicast traffic.

4.1. Cisco Wireless Security Suite Components

4.1.1. 802.1X Authentication

The 802.1X authentication framework is included in the draft for 802.11 MAC layer security enhancements currently being developed by the IEEE 802.11 Task Group i (TGi). The 802.1X framework provides the link layer with extensible authentication, normally seen in higher layers (Figure 22).

Figure 22 802.1X Layers
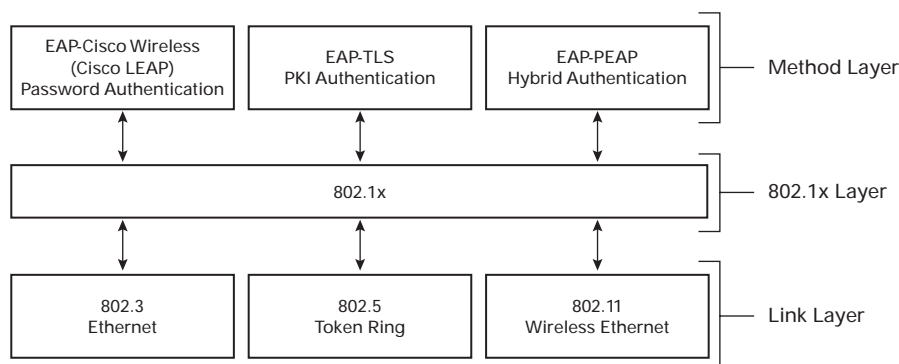
802.1X requires three entities:

- The supplicant—Resides on the wireless LAN client
- The authenticator—Resides on the access point
- The authentication server—Resides on the RADIUS server

These entities are logical entities on the network devices. The authenticator creates a logical port per client, based on the client's association ID (AID). This logical port has two data paths. The uncontrolled data path allows network traffic through to the network. The controlled data path requires successful authentication to allow network traffic through (Figure 23).

Figure 23 802.1X Ports
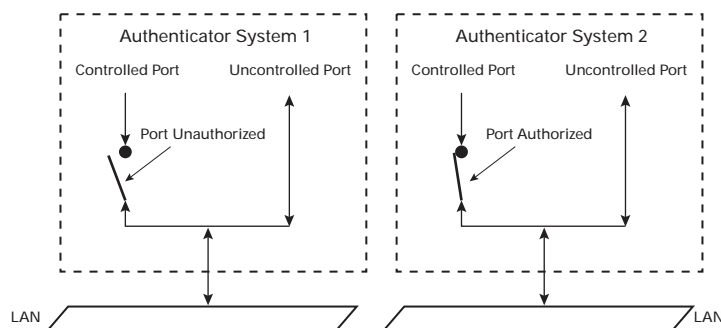
The supplicant becomes active on the medium and associates to the access point. The authenticator detects the client association and enables the supplicant's port. It forces the port into an unauthorized state so that only 802.1X traffic is forwarded. All other traffic is blocked. The client may send an EAP Start message, although client initiation is not required (Figure 24).
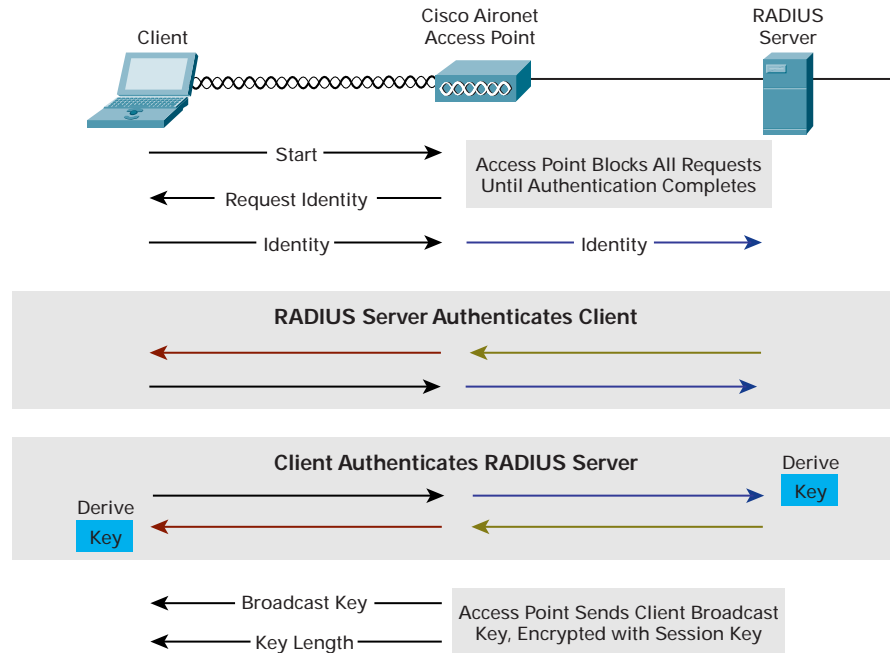
The authenticator replies with an EAP Request Identity message back to the supplicant to obtain the client's identity. The supplicant's EAP Response packet containing the client's identity is forwarded to the authentication server.

The authentication server is configured to authenticate clients with a specific authentication algorithm. Currently, 802.1X for 802.11 LANs does not stipulate a specific algorithm to use. However, this paper focuses on Cisco LEAP authentication and assumes that Cisco LEAP credential verification occurs.

The end result is a RADIUS -ACCEPT or RADIUS-REJECT packet from the RADIUS server to the access point. Upon receiving the RADIUS ACCEPT packet, the authenticator transitions the client's port to an authorized state, and traffic may be forwarded.

Figure 24 802.1X and EAP Message Flow

Client   Cisco Aironet Access Point   RADIUS Server

Start →

Access Point Blocks All Requests Until Authentication Completes

← Request Identity

Identity →   Identity →

RADIUS Server Authenticates Client

Client Authenticates RADIUS Server

Derive
Key

Derive
Key

← Broadcast Key

Access Point Sends Client Broadcast Key, Encrypted with Session Key

← Key Length

802.1X provides the means for a wireless LAN client to communicate with an authentication server to validate the client credentials. 802.1X is extensible and allows a variety of authentication algorithms to operate over it.

4.1.2. The EAP Cisco Authentication Algorithm

Cisco designed the Cisco LEAP authentication algorithm to provide easy-to-implement, strong authentication. Cisco LEAP, like other EAP authentication variants, is designed to function on top of the 802.1X authentication framework. What makes the Cisco LEAP algorithm so compelling is its robust features.

4.1.2.1. Mutual Authentication

Many authentication algorithms exist, each with an ideal use. In the world of wireless LANs, the client needs to be certain that it is communicating with the intended network device. The lack of physical connectivity between the client and the network requires the client to authenticate the network as well as to be authenticated by the network. Therefore, Cisco has designed Cisco LEAP to support mutual authentication.

4.1.2.2. User-Based Authentication

802.11 authentication is device-based. The user of the device is invisible to the authenticator, and so unauthorized users can access the network simply by gaining access to an authorized device. Laptops with 802.11 NICs using static WEP with 802.11 authentication create network vulnerability if the laptop is stolen or lost. Such an event would require the network administrator to rapidly rekey the wireless network and all clients.

The scenario is all too common and is a major barrier to deployment for wireless LANs. Cisco has responded by implementing Cisco LEAP, which is based on authenticating the user rather than the wireless LAN device.

4.1.2.3. Dynamic WEP Keys

User-based mutual authentication provides an easy-to-administer and secure authentication scheme, yet a mechanism is still needed to manage WEP keys efficiently. This need has driven the requirement for the authentication algorithm to generate keying material for dynamic WEP keys. Cisco LEAP employs its user-based nature to generate unique keying material for each client. This relieves network administrators from the burden of managing static keys and manually rekeying as needed.

802.1X session timeouts force the client to reauthenticate to maintain network connectivity. Although reauthentication is transparent to the client, the process of reauthentication in an algorithm that supports dynamic WEP will generate new WEP keys at every reauthentication interval. This is an important feature in mitigating statistical key derivation attacks and is critical for Cisco WEP enhancements (described in detail later).

4.1.3. Data Privacy with TKIP

Previous sections of this paper have highlighted network attacks on 802.11 security and shown WEP to be ineffective as a data-privacy mechanism. Cisco has implemented prestandards enhancements to the WEP protocol that mitigate existing network attacks and address its shortcomings. These enhancements to WEP are collectively known as the Temporal Key Integrity Protocol (TKIP). TKIP is a draft standard with Task Group i of the IEEE 802.11 working group. Although TKIP is not a ratified standard, Cisco has implemented a prestandards version of TKIP to protect existing customer investments in Cisco Aironet® wireless products.

TKIP provides two major enhancements to WEP:

*   A message integrity check (MIC) function on all WEP-encrypted data frames
*   Per-packet keying on all WEP-encrypted data frames

Cisco also adds a third feature not specified in the IEEE 802.11 Task Group i draft: broadcast key rotation.

4.1.3.1. Message Integrity Check

The MIC augments the ineffective integrity check function (ICV) of the 802.11 standard. The MIC is designed to solve two major vulnerabilities:

*   **Initialization vector/base key reuse**—The MIC adds a sequence number field to the wireless frame. The access point will drop frames received out of order.
*   **Frame tampering/bit flipping**—The MIC feature adds a MIC field to the wireless frame. The MIC field provides a frame integrity check not vulnerable to the same mathematical shortcomings as the ICV.

Figure 25 shows an example of a WEP data frame. The MIC adds two new fields to the wireless frame: a sequence number and the integrity check field (Figure 26)

Figure 25 Example of WEP Frame Format

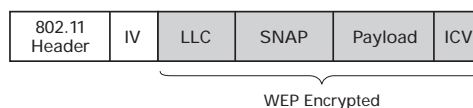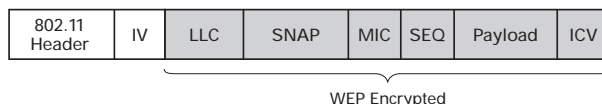| 802.11 Header | IV | LLC | SNAP | Payload | ICV |

WEP Encrypted

Figure 26 Example of WEP Frame Format with MIC Enabled

The sequence number is a sequential counter that increases in value on a per-frame, per-association basis. The access point will discard frames received that have an out-of-order sequence number. The MIC field is calculated based on the fields in Figure 27.

Figure 27 MIC Value Derivation
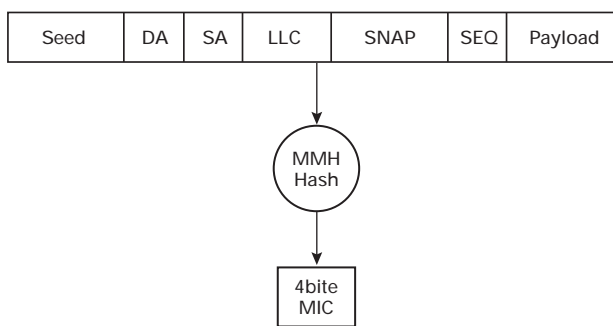
Modifications to any of the fields will result in a discrepancy in the calculated MIC on the receiver. As a result, the receiver will drop the frame.

The MIC is currently a prestandards implementation. Although it is included in the IEEE 802.11 Task Group i draft, all wireless LAN vendors have not adopted it. As a result, the MIC requires the use of Cisco clients and access points.

4.1.3.2. Per-Packet Keying

The vulnerabilities described in the Fluhrer, Mantin, and Shamir, paper as well as the AirSnort tool, which can implement an attack, render WEP ineffective for data privacy and encryption. Using WEP key rotation schemes via 802.1X reauthentication can mitigate the vulnerabilities but does not provide resolution for the weaknesses.

The IEEE has adopted into the Task Group i draft a WEP enhancement that changes the transmit WEP key on a per-packet basis. Cisco was instrumental in devising and co-developing this enhancement and has implemented it on Cisco clients and access points.

In a Cisco implementation of 802.11 WEP encryption, an IV is generated randomly and concatenated with the WEP key. The two values are processed by the WEP algorithm to generate the key stream. The key stream is mixed with the plain-text to generate the cipher-text.

The Cisco implementation of per-packet keying augments the process by hashing the WEP key and the IV to create a new packet key. The original IV is then concatenated with the packet key and processed normally (Figure 28).

Figure 28 Per-Packet Keying
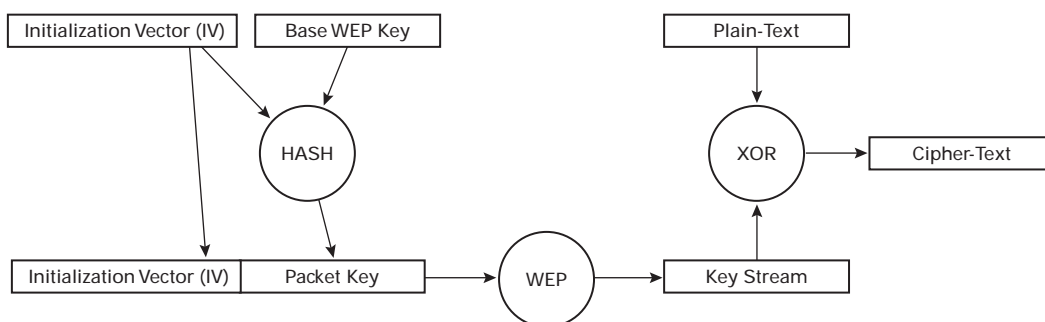
To effectively use the 24-bit IV space, Cisco has also adopted IV sequencing. Cisco client and access points implement IV sequencing by simply starting the IV counter and increasing the IV value by one for each frame. If the client and access point both initiate their IV counters at zero, the client and access point will be sending the same IV/base WEP keys through the hashing algorithm and generating the same packet keys. To overcome this problem, the Cisco IV sequencing is directional. For example, client-to-access-point frames may use an even-numbered IV, and access-point-to-client frames may use an odd-numbered IV.

Per-packet keying will not generate the same packet key as long as unique IV/base WEP key pairs are used. With a static WEP key, this only allows for 224 possible unique packet keys. Because the IV space recycles when it is exhausted, IV/base WEP key pairs will be reused. To get around this limitation, the base WEP key should be changed before the IV space is used. Cisco LEAP session timeouts accommodate this requirement. Once the base WEP key is changed, new IV/base WEP key pairs are used, and unique packet keys will be generated.

4.1.3.3. Broadcast Key Rotation

802.1X authentication types that support user-based WEP keys provide WEP keys for unicast traffic only. To provide encryption for broadcast and multicast traffic, the Cisco Wireless Security Suite requires that one of two options be selected:

- Employ a static broadcast key configured on the access point
- Enable broadcast key rotation for dynamic broadcast key generation

A static broadcast key must be configured on an access point for 802.1X clients to receive broadcast and multicast messages. In wireless LAN deployments in which Cisco TKIP enhancements are implemented, a static broadcast key will go through the per-packet keying process. This reduces the opportunity for statistical key derivation attacks, but because the base broadcast key remains static, the IV space will recycle, causing key streams to be reused. Statistical attacks may take much longer to execute, but they are still possible.

Static broadcast key deployments might be required in some instances. Broadcast keys are sent from the access point to the client encrypted with the client's unicast WEP key. Because the broadcast keys are distributed after authentication, access points do not have to be configured with the same broadcast key.

Cisco recommends enabling broadcast key rotation on the access points. The access point generates broadcast WEP keys using a seeded pseudorandom number generator (PRNG). The access point rotates the broadcast key after a configured broadcast WEP key timer expires. This process should generally be in sync with the timeouts configured on the RADIUS servers for user reauthentication.

Broadcast key rotation is designed for 802.1X-enabled access point deployments. In mixed static WEP/802.1X deployments, broadcast key rotation may cause connectivity problems in static WEP clients. Therefore, Cisco recommends that broadcast key rotation be enabled when the access point services an 802.1X exclusive wireless LAN.

5. Cisco LEAP Architecture

The EAP Cisco Wireless or Cisco LEAP algorithm provides user-based mutual authentication. It also provides keying material to the client and RADIUS server for the generation of WEP keys. This section will examine Cisco LEAP, from protocol message exchanges to how to implement the algorithm on RADIUS servers, access points, and client devices.

5.1. Cisco LEAP Authentication Process

Cisco LEAP is a user-based authentication algorithm that is secure enough to implement in hostile wireless LAN deployments. Based on these user requirements, and the need for single-sign-on (SSO) capabilities, Cisco built Cisco LEAP around the premise of Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

Cisco LEAP is a password-based algorithm. It preserves the integrity of the password during wireless authentication by converting the password to a secret key value so that wireless eavesdroppers cannot sniff Cisco LEAP authentication and see a user's password transmitted across the wireless link. The secret key value is the result of a mathematical function called a hash function. A hash function is an algorithm that one-way encrypts data. The data cannot be decrypted to derive the original input. Cisco LEAP uses secrets in the form of the Microsoft NT key format. The Windows NT key is a Message Digest Algorithm 4 (MD4) hash of an MD4 hash of the user's password (Figure 29).

Figure 29 Windows NT Key
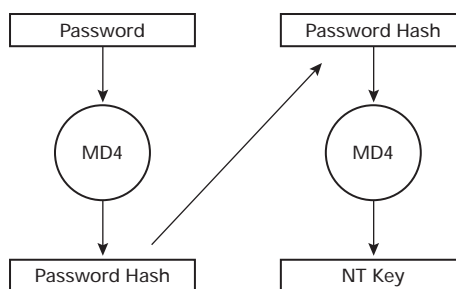
Use of the Windows NT key allows Cisco LEAP to use existing Windows NT Domain Services authentication databases as well as Windows 2000 Active Directory databases. In addition, any Open Database Connectivity (ODBC) that uses MS-CHAP passwords can also be used.

Cisco has developed drivers for most versions of Microsoft Windows (Windows 95, 98, Me, 2000, NT and XP) and uses the Windows logon as the Cisco LEAP logon. A software shim in the Windows logon allows the username and password information to be passed to the Cisco Aironet client driver. The driver will convert the password into a Windows NT key and hand the username and Windows NT key to the Cisco NIC. The NIC executes 802.1X transactions with the AP and the authentication, authorization, and accounting (AAA) server.

Note: Neither the password nor the password hash is ever sent across the wireless medium.

Reauthentication and subsequent WEP key derivation follow a similar process. The transaction WEP-encrypted with the existing client WEP key and client's port on the access point does not transition to a blocking state. It will remain in the forwarding state until the client explicitly sends an EAP Logoff message or fails reauthentication.

5.2. Cisco LEAP Deployment

Cisco designed Cisco LEAP to provide strong, easy-to-deploy, and easy-to-administer wireless security. Cisco offers third-party NIC support and RADIUS support to allow customers to use their existing investments in wireless clients as well as existing RADIUS servers. In addition, Cisco provides deployment best practices guidance to ensure customer success with Cisco Aironet products and the Cisco LEAP algorithm.

5.2.1. Third-Party Support

Cisco offers Cisco LEAP RADIUS support on the:

- Cisco Secure Access Control Server (ACS) Version 2.6 and v3.0 platforms
- Cisco Access Registrar v1.7 or later

To service customers with existing RADIUS servers, Cisco has partnered with Funk Software and Interlink Networks. Cisco LEAP support is available on:

- Funk Steel Belted RADIUS v3.0
- Interlink Merit v5.1

In addition, third-party client support is available from Apple Computers for its AirPort wireless adapters.

5.2.2. Cisco LEAP Deployment Best Practices

Cisco offers deployment guidance for secure wireless LANs with the Cisco SAFE Blueprint for enterprise networks (SAFE), a series of white papers. *SAFE: Wireless Security in Depth* is available at:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml

In addition, here are some salient points for deploying wireless LANs.

5.2.2.1. Use Strong Passwords for LEAP Authentication

Cisco LEAP is a password-based algorithm. To minimize the possibility of a successful dictionary attack, use strong passwords, which are difficult to guess. Some characteristics of strong passwords include:

- A minimum of ten characters
- A mixture of uppercase and lowercase letters
- At least one numeric character or one non-alphanumeric character (Example: !#@$%)
- No form of the user's name or user ID
- A word that is not found in the dictionary (domestic or foreign)

Examples of strong passwords:

- cnw84FriDAY, from "cannot wait for Friday"
- 4yosc10cP!, from "for your own safety choose 10 character password!"

5.2.2.2. Avoid Using MAC and Cisco LEAP Authentication on the Same RADIUS Server

In scenarios where MAC address authentication uses the same ACS as Cisco LEAP, be sure that the MAC address has a separate MS-CHAP strong password.

If a MAC address has been configured on an ACS that supports Cisco LEAP and MAC authentication, the MAC address should use a different strong password for the required MS-CHAP/CHAP field. If not, an eavesdropper can spoof a valid MAC address and use it as a username and password combination for Cisco LEAP authentication.

5.2.2.3. Use RADIUS Session Timeouts to Rotate WEP Keys

Cisco LEAP and EAP Transport Layer Security (TLS) support session expiration and 802.1X reauthentication by using the RADIUS session timeout option (RADIUS Internet Engineering Task Force option 27). To avoid IV reuse (IV collisions), rotate the base WEP key before the IV space is exhausted.

For example, the worst-case scenario for a reauthentication time would be stations in a service set running at maximum packet rate (in 802.11 stations, this is 1000 frames per second).

- 2^{24} frames (16,777,216) / 1000 frames per second ~= 16,777 seconds or 4 hours 40 minutes.

Normal frame rates will vary by implementation, but this example serves as a guideline for determining the session timeout value.

5.2.2.4. Deploy Cisco LEAP on a Separate Virtual LAN (VLAN)

Deploying Cisco LEAP wireless LAN users on a separate VLAN allows Layer 3 access lists to be applied to the wireless LAN VLAN if required, without affecting wired clients. In addition, intrusion-detection systems can be installed on wireless LAN VLANs to monitor wireless LAN traffic.

6. What Lies Ahead

WEP encryption and 802.11 authentication are known to be weak. The IEEE is enhancing WEP with TKIP and providing robust authentication options with 802.1X to make 802.11-based wireless LANs secure. At the same time, the IEEE is looking to stronger encryption mechanisms. The IEEE has adopted the use of the Advanced Encryption Standard (AES) to the data-privacy section of the proposed 802.11i standard.

6.1. AES Overview

The Advanced Encryption Standard (AES) is the next-generation encryption function approved by the National Institute of Standards and Technology (NIST). NIST solicited the cryptography community for new encryption algorithms. The algorithms had to be fully disclosed and available royalty free. The NIST judged candidates on cryptographic strength as well as practical implementation. The finalist, and adopted method, is known as the Rijndael algorithm.

Like most ciphers, AES requires a feedback mode to avoid the risks associated with ECB mode. The IEEE is deciding which feedback mode to use for AES encryption. The two contenders are:

- Offset code book (OCB)
- Cipher block chaining counter mode (CBC-CTR) with cipher block chaining message authenticity check (CBC-MAC), collectively known as CBC-CCM

The two modes are similar but differ in implementation and performance.

6.1.1. AES-OCB Mode

AES-OCB is a mode that operates by augmenting the normal encryption process by incorporating an offset value. The routine is initiated with a unique nonce (the nonce is a 128-bit number) used to generate an initial offset value. The nonce has the XOR function performed with a 128-bit string (referred to as value L). The output of the XOR is AES-encrypted with the AES key, and the result is the offset value. The plain-text data has the XOR function performed with the offset and is then AES-encrypted with the same AES key. The output then has the XOR function performed with the offset once again. The result is the cipher-text block to be transmitted. The offset value changes after processing each block by having the XOR function performed on the offset with a new value of L (Figure 30).

Figure 30 AES-OCB Encryption
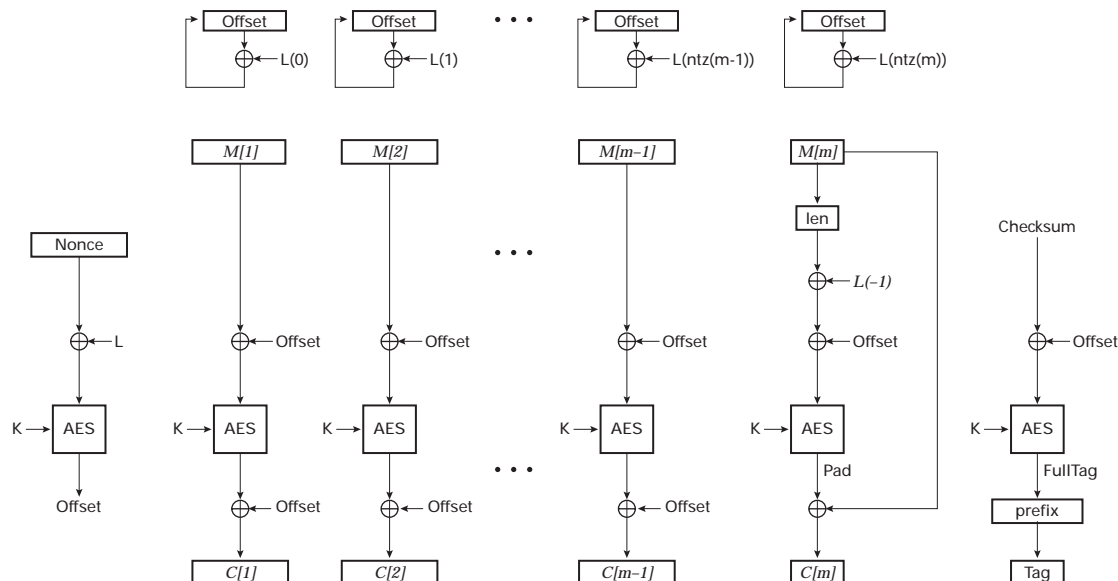
Refer to [OCB Mode](#) for a more detailed description of AES OCB mode.

OCB mode also includes a MIC function. The MIC is calculated by performing the XOR function on the following values:

- All plain-text blocks except the final one
- The final plain-text block with the XOR function performed with the appropriate offset value
- The final cipher-text block
- The final offset value

The result from this XOR function is AES-encrypted using the AES key. The first 64 bits of the resulting 128-bit output is the MIC value inserted into the AES-encrypted frame (Figure 31). Note that the MIC is not included in the encrypted portion of the frame. Encrypting the MIC is not required because MIC itself is the result of AES encryption.

Figure 31 AES-Encrypted Frame
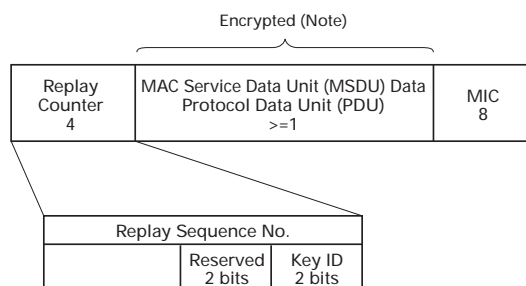
AES-OCB is a new mode, which is an inherent weakness in the eyes of the cryptographic community. But the author of the mode, Phil Rogaway, has cryptographically proven the strength of the mode and is also a well-respected member of the cryptography community. OCB mode is known to be efficient and fast. One major benefit is that the MIC can be calculated in the same processing function as the encryption, minimizing encryption overhead and maximizing data throughput.

6.1.2. AES-CCM Mode

AES-CCM mode is an alternative to OCB mode for AES encryption. CCM mode is the combination of Cipher Block Chaining Counter mode (CBC-CTR mode and CBC Message Authenticity Check (CBC-MAC. The functions are combined to provide encryption and message integrity in one solution.

CBC-CTR encryption operates by using IVs to augment the key stream. The IV increases by one after encrypting each block. This provides a unique key stream for each block (Figure 32).

Figure 32 CBC-CTR Encryption
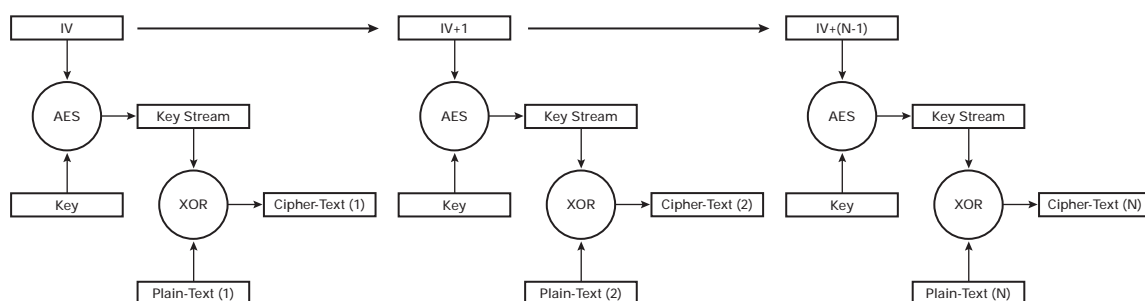
CBC-MAC operates by using the result of CBC encryption over frame length, destination address, source address, and data. The resulting 128-bit output is truncated to 64 bits for use in the transmitted frame.

AES-CCM uses cryptographically known functions but has the weakness of requiring two operations for encryption and message integrity. This is computationally expensive and adds a significant amount of overhead to the encryption process.

7. Summary

Wireless LAN deployments should be made as secure as possible. Standard 802.11 security is weak and vulnerable to numerous network attacks. This paper has highlighted these vulnerabilities and described how the Cisco Wireless Security Suite can augment 802.11 security to create secure wireless LANs.

Some Cisco security enhancement features might not be deployable in some situations because of device limitations such as application specific devices (ASDs such as 802.11 phones capable of static WEP only) or mixed vendor environments. In such cases, it is important that the network administrator understand the potential WLAN security vulnerabilities.

Cisco strives to educate and inform customers and clients about Cisco wireless LAN solutions, and to provide design and deployment guidance to allow them to make decisions that best suit their needs.

Cisco recommends using the Cisco Wireless Security Suite to provide wireless LAN users with the most secure environment possible—abandoning legacy authentication and encryption, wherever possible, in favor of strong authentication and encryption.

Cisco is committed to providing customers with interoperable wireless LAN solutions. The Cisco Wireless Security Suite offers many prestandard features that will be upgradeable to interoperable versions once the standards are ratified. This arrangement allows for deployment of secure wireless LANs today with the prospect of interoperable wireless LANs tomorrow.

8. Appendix A—EAP Authentication Types

8.1. EAP Transport Layer Security

EAP Transport Layer Security (TLS) (RFC2716) is a Microsoft-supported EAP authentication algorithm based on the TLS protocol (RFC2246). TLS is the current version of Secure Socket Layer (SSL) used in most Web browsers for secure Web application transactions. TLS has proved to be a secure authentication scheme and is now available as an 802.1X EAP authentication type. EAP-TLS is supported in the Microsoft XP platform, and support is planned for legacy Microsoft operating systems as well. Including a supplicant on the client operating system eases deployment and alleviates single-vendor constraints.

8.1.1. TLS Overview

EAP-TLS is based on SSL v3.0. To better understand EAP-TLS operation, this section focuses on the operation of TLS with respect to SSL. TLS is designed to provide secure authentication and encryption for a TCP/IP connection. To provide this functionality, TLS comprises three protocols:

- **Handshake protocol**—The handshake protocol negotiates the parameters for the SSL session. The SSL client and server negotiate the protocol version, encryption algorithms, authenticate each another, and derive encryption keys.
- **Record protocol**—The record protocol facilitates encrypted exchanges between the SSL client and the server. The negotiated encryption scheme and encryption keys are used to provide a secure tunnel for application data between the SSL endpoints.
- **Alert protocol**—The alert protocol is the mechanism used to notify the SSL client or server of errors as well as session termination.

TLS authentication is generally split into two methods: server-side authentication and client-side authentication. Server-side authentication uses public key infrastructure (PKI), namely PKI certificates. Client-side authentication can also use PKI certificates, but this is optional. EAP-TLS uses client-side certificates.

8.1.2. PKI and Digital Certificates

PKI encryption is based on asymmetric encryption keys. A PKI user has two keys: a public key and a private key. Any data encrypted with the public key can be decrypted only with the private key, and vice versa. For example: George gives Martha his public key. Martha then sends George an e-mail encrypted with his public key. For George to read the message, he has to decrypt the message with his private key. Because George is the only person with access to his private key, only he can decrypt the message (Figure 33).

**Figure 33** Public Key Encryption
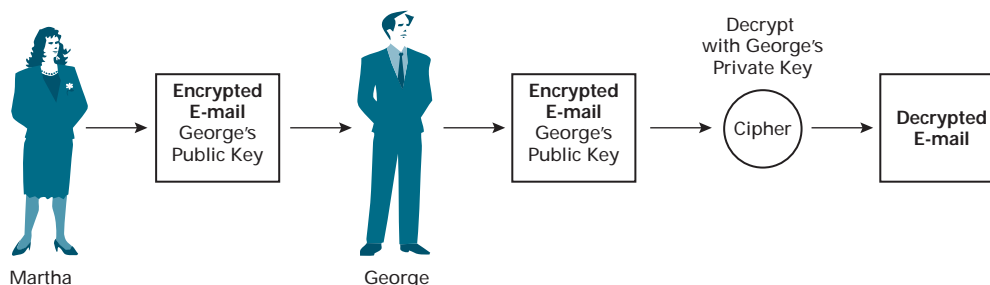
Digital certificates are data structures distributed by a certificate authority that join a public key to a user. A digital certificate is generally made up of the following pieces of information:

- Certificate version
- Serial number
- Certificate issuer
- User
- User's public key
- Validity period
- Optional extensions
- Signature algorithm
- Signature

The digital signature is derived by combining the certificate version, serial number, issuer, user, user's public key, and validity period and running the values through a keyed hash function. The certificate authority keys the hash with its own private key (Figure 34).

Figure 34 Digital Signature
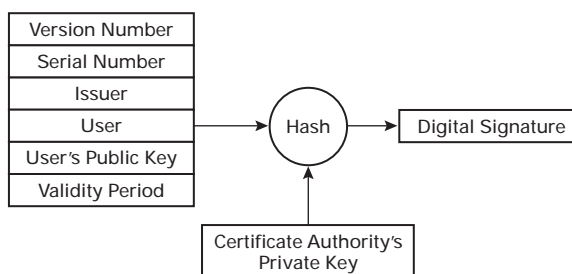
8.1.3. TLS Authentication Process

The TLS process begins with the handshake process:

1. The SSL client connects to a server and makes an authentication request
2. The server sends its digital certificate to the client
3. The client verifies the certificate's validity and digital signature
4. The server requests client-side authentication
5. The client sends its digital certificate to the server
6. The server verifies the certificate's validity and digital signature
7. The encryption and message integrity schemes are negotiated
8. Application data is sent over the encrypted tunnel via the record protocol

8.1.4. EAP-TLS Authentication Process

The EAP-TLS authentication process is as follows (Figure 35):

1. The client sends an EAP Start message to the access point

2. The access point replies with an EAP Request Identity message

3. The client sends its network access identifier (NAI), which is its username, to the access point in an EAP Response message

4. The access point forwards the NAI to the RADIUS server encapsulated in a RADIUS Access Request message

5. The RADIUS server will respond to the client with its digital certificate

6. The client will validate the RADIUS server's digital certificate

7. The client will reply to the RADIUS server with its digital certificate

8. The RADIUS server will validate the client's credentials against the client digital certificate

9. The client and RADIUS server derive encryption keys

10. The RADIUS server sends the access point a RADIUS ACCEPT message, including the client's WEP key, indicating successful authentication

11. The access point sends the client an EAP Success message

12. The access point sends the broadcast key and key length to the client, encrypted with the client's WEP key.

Figure 35 EAP-TLS Authentication Process
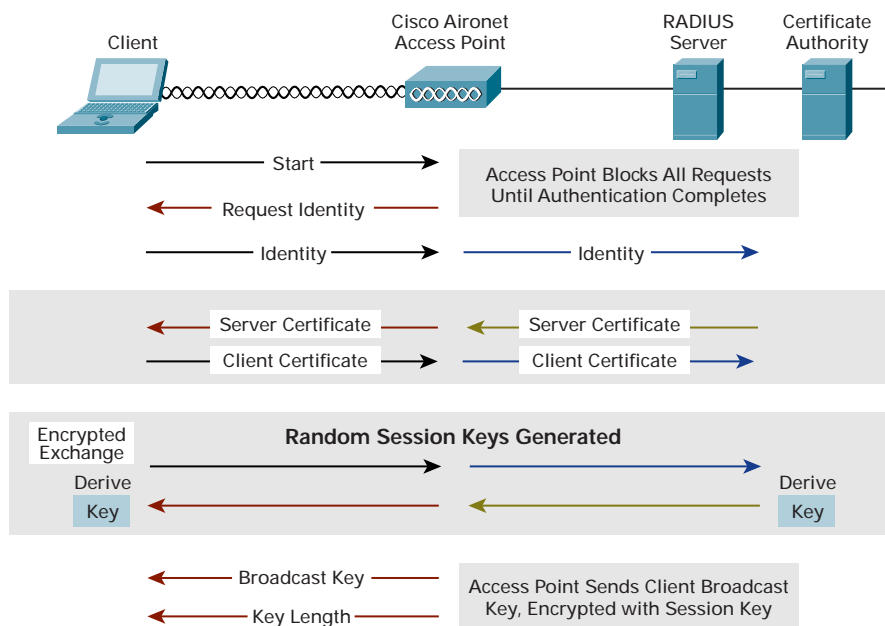
8.2. EAP SIM Architecture

The EAP subscriber identity module (SIM) authentication algorithm is designed to provide per-user/per-session mutual authentication between a wireless LAN (WLAN) client and an AAA server. It also defines a method for generating the master key used by the client and AAA server for the derivation of WEP keys. The Cisco implementation of EAP SIM authentication is based on the most recent IEEE draft protocol. This section will take a closer look at EAP SIM, from protocol message exchanges to how to implement EAP SIM on the AAA servers, access points, and client devices.

8.2.1. Global System for Mobile Communications

EAP SIM authentication is based on the authentication and encryption algorithms stored on the Global System for Mobile Communications (GSM) SIM, which is a Smartcard designed according to the specific requirements detailed in the GSM standards. GSM authentication is based on a challenge-response mechanism and employs a shared secret key, Ki, which is stored on the SIM and otherwise known only to the GSM operator's Authentication Center (AuC). When a GSM SIM is given a 128-bit random number (RAND) as a challenge, it calculates a 32-bit response (SRES) and a 64-bit encryption key (Kc) using an operator-specific confidential algorithm. In GSM systems, Kc is used to encrypt mobile phone conversations over the air interface.

8.2.2. EAP SIM Authentication Process

EAP SIM authentication provides a hardware-based authentication method secure enough to implement in potentially hostile public wireless LAN deployments. It allows GSM mobile operators to reuse their existing authentication infrastructure for providing access to wireless networks, mainly in public access "hot spots." EAP SIM combines the data from several GSM "triplets" (RAND, SRES, Kc), obtained from an AuC, to generate a more secure session encryption key. EAP SIM also enhances the basic GSM authentication mechanism by providing for mutual authentication between the client and the AAA server.

On the client side, the EAP SIM protocol, as well as the code needed to interface with a Smartcard reader and the SIM, is implemented in the EAP SIM supplicant. The supplicant code is linked into the EAP framework provided by the operating system; currently, supplicants exist for Microsoft Windows XP and 2000. The EAP framework handles EAP protocol messages and communications between the supplicant and the AAA server; it also installs any encryption keys provided the supplicant in the client's WLAN radio card.

On the network side, the EAP SIM authenticator code resides on the service provider's AAA server. Besides handling the server side of the EAP SIM protocol, this code is also responsible for communicating with the service provider's AuC. In a Cisco implementation of EAP SIM, the AAA server communicates with a Cisco IP Transfer Point (ITP), which acts as a gateway between the IP and Signaling System 7 (SS7) networks. The Cisco ITP translates messages from the AAA server into standard GSM protocol messages, which are then sent to the AuC.

802.1X authentication using Cisco implementation of EAP SIM proceeds as follows (Figure 36):

1. An EAP-over-LAN (EAPOL) Start message from the client starts the authentication protocol and indicates to the access point that the client wants to authenticate using EAP.

2. In response, the access point sends an EAP Identity Request message to the client. At this point, the client has not yet been assigned an IP address, and the access point blocks all messages from the client except for those necessary for authentication (EAP and EAP SIM protocol messages).

3. The client responds to the access point's request with an EAP Identity Response message containing the user's network identity. This identity is read from the SIM card, using a card reader attached to (or incorporated into) the client. It is of the form 0<IMSI>@<realm>, where <IMSI> is the International Mobile Subscriber Identity (as used in GSM networks) and <realm> is the operator's domain name string (voicestream.com, for example). The network identity is stored on the SIM and determined by the service provider; it may differ from the user's login credentials and is used mainly to authenticate access to the WLAN.

4. The access point forwards the EAP Identity Response to the AAA server using a RADIUS protocol message with Cisco vendor-specific attributes.

5. The AAA server determines that the user intends to use EAP SIM authentication based on its configuration parameters or on the identity passed to it and invokes its EAP SIM extension code. This code then starts the EAP SIM extension protocol by sending an EAP SIM Start request back to the client. It may also generate a GetAuthInfo message to the AuC requesting a (configurable) number of GSM triplets; this step may be delayed until after a response to the EAP SIM Start message is received to ensure that the client indeed supports the EAP SIM protocol.

Note: Depending on the realm (domain) contained in the identity string, the AAA request might need to be proxied from the local AAA server to the service provider's AAA server.

6. The GetAuthInfo message is routed to the Internet Transfer Point Mobile Application Part (ITP MAP) proxy, which acts as a gateway to the service provider's SS7 network. The ITP translates the request into a standard GSM MAP GetAuth request before sending it to the AuC.

7. On receiving the EAP SIM Start request, the client reads a 128-bit (16-byte) random number generated on the SIM and passes it back to the AAA server in the EAP SIM Start response.

8. Once the AAA server has received the client's EAP SIM Start response and the response from the AuC containing a sufficient number of GSM triplets (typically two to three), it then constructs an EAP SIM Challenge message that contains the random numbers (RAND) received from the AuC and a 160-bit (20-byte) message-authentication code (MAC_RAND).

9. The client passes the EAP SIM Challenge request to the SIM card, which first calculates its own MAC_RAND. The AAA server is validated if the result matches the MAC_RAND received from the server. Only in that case, the SIM also calculates the GSM result (SRES) and encryption key (Kc) for each of the RANDs it received, as well as a 160-bit (20-byte) message-authentication code (MAC_SRES) based on these results and the user identity. Only MAC_SRES is returned to the AAA server (and therefore exposed on the radio link) in the EAP SIM Challenge response. The SIM also calculates cryptographic keying material, using a secure hash function on the user identity and the GSM encryption keys, for the derivation of session encryption keys.

10. When the AAA server receives the client's EAP SIM Challenge response, it calculates its own MAC_SRES and compares it to the one received from the client. If both match, the client is authenticated and the AAA server also calculates the session encryption keys. It then sends a RADIUS ACCEPT message to the access point, which contains an encapsulated EAP Success message and the (encrypted) client session key.

11. The access point installs the session key for the client's association ID and forwards the EAP Success message to the client. It then sends its broadcast key, encrypted with the client's session key, in an EAP Key message to the client. It also unblocks the data path for the client so that IP traffic can flow between the client and the rest of the network.

12. Upon receiving the EAP Success message, the EAP SIM supplicant returns the session encryption key calculated by the SIM to the EAP framework, which installs it on the client's WLAN radio card.

13. The client is now able to securely send and receive network traffic.

Figure 36 EAP SIM Authentication
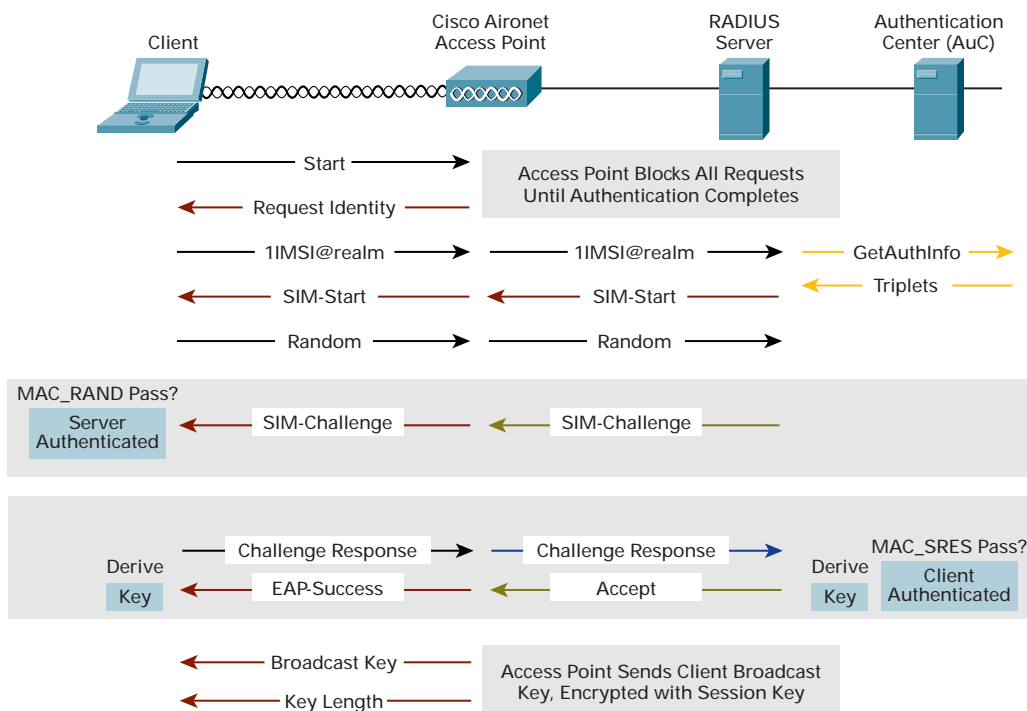
Note: The client's session key is never sent across the radio link and can therefore not be snooped by network attackers listening in on the message traffic. Similarly, the results of the GSM authentication algorithm (SRES, Kc) are never exposed to listeners over the radio link. EAP SIM, therefore, exposes even less information to network attackers than the standard GSM authentication for wireless phones.

All message authentication codes described above are calculated using a secure keyed hashing algorithm, HMAC-SHA1 (steps 4 and 5). A hash function is an algorithm that one-way encrypts data so that it cannot be decrypted to derive the original input data. The algorithm uses the user's identity, the random number generated by the SIM, the GSM encryption keys Kc, and other data to calculate the authentication codes and encryption keys used in EAP SIM.

The Cisco implementation of EAP SIM is particularly secure because the results of the GSM authentication algorithm (SRES, Kc) never leave the SIM and therefore remain inaccessible even if network attackers manage to compromise the EAPSIM supplicant code. This is made possible by a partnership between Cisco and Gemplus, a world leader in Smartcard technology and leading supplier of SIM chips to the GSM industry. Other implementations of EAP SIM, using standard GSM SIM chips or software-based SIM emulators, are possible but are inherently less secure than the Cisco solution.

8.3. Protected EAP

Protected EAP (PEAP), is a draft EAP authentication type that is designed to allow hybrid authentication. PEAP employs server-side PKI authentication. For client-side authentication, PEAP can use any other EAP authentication type. Because PEAP establishes a secure tunnel via server-side authentication, non-mutually authenticating EAP types can be used for client-side authentication, such as EAP generic token card (GTC) for one-time passwords (OTP), and EAP MD5 for password based authentication.

PEAP is based on server-side EAP-TLS, and it addresses the manageability and scalability shortcomings of EAP-TLS. Organizations can avoid the issues associated with installing digital certificates on every client machine as required by EAP-TLS and select the method of client authentication that best suits them.

8.3.1. PEAP Authentication Process

PEAP authentication begins in the same way as EAP-TLS (Figure 37):

1. The client sends an EAP Start message to the access point
2. The access point replies with an EAP Request Identity message
3. The client sends its network access identifier (NAI), which is its username, to the access point in an EAP Response message
4. The access point forwards the NAI to the RADIUS server encapsulated in a RADIUS Access Request message
5. The RADIUS server will respond to the client with its digital certificate
6. The client will validate the RADIUS server's digital certificate

From this point on, the authentication process diverges from EAP-TLS

7. The client and server negotiate and create an encrypted tunnel
8. This tunnel provides a secure data path for client authentication
9. Using the TLS Record protocol, a new EAP authentication is initiated by the RADIUS server
10. The exchange will include the transactions specific to the EAP type used for client authentication
11. The RADIUS server sends the access point a RADIUS ACCEPT message, including the client's WEP key, indicating successful authentication

Figure 37 PEAP Authentication
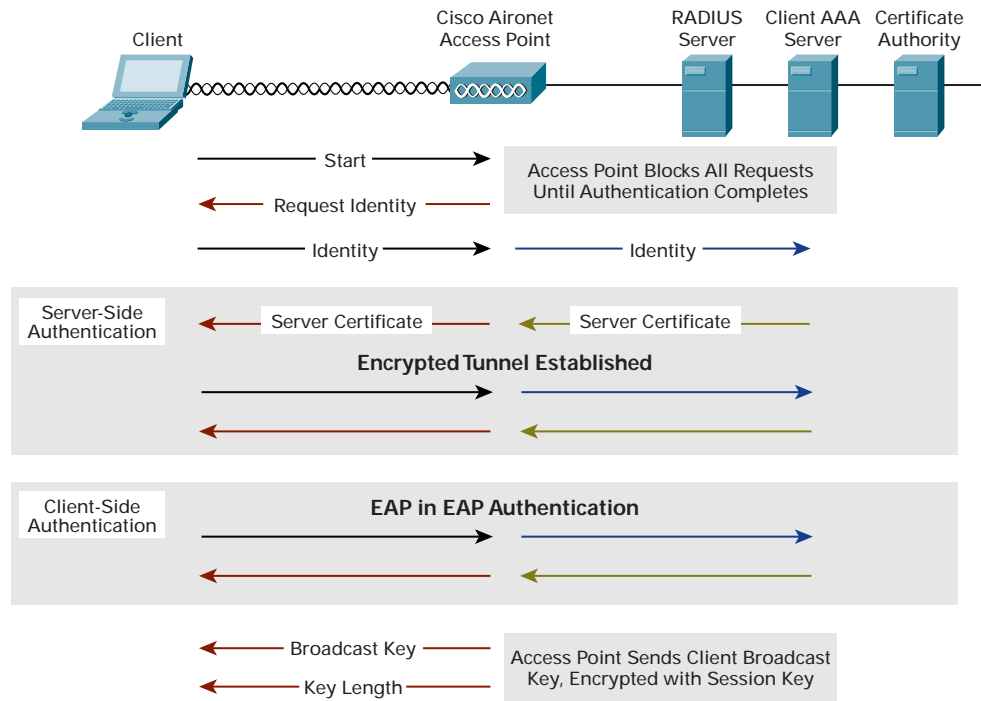
9. Appendix B—Cisco Wireless Security Suite in Bridging Deployments

The authentication and TKIP WEP enhancements are primarily focused on addressing infrastructure basic service sets. Cisco recognizes the need for enhanced security in point-to-point and point-to-multipoint bridging environments and has added features to the bridge firmware to allow wireless bridge links to take advantage of Cisco LEAP authentication and TKIP WEP enhancements.

Figure 38 illustrates a typical point-to-point bridging scenario. The root bridge is configured to support 802.1X authentication and the TKIP WEP enhancements, including per-packet keying, the MIC, and broadcast key rotation.

Figure 38 Cisco LEAP and TKIP and Bridge Links
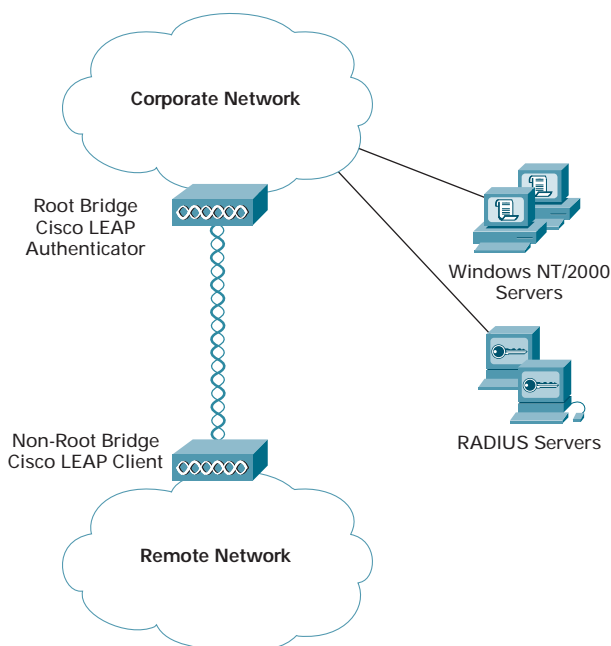
The non-root bridge is statically configured with a username and password. The non-root bridge must also be configured to support per-packet keying and the MIC function. As with a NIC-based client, the broadcast key will be sent via the wireless link to the non-root bridge, encrypted with the dynamic WEP key of the non-root bridge.

Enabling Cisco LEAP and TKIP WEP enhancements allows the wireless bridge link to use dynamic WEP keys with administrator-controlled reauthentication (and WEP rekey) intervals.

10. Appendix C—Useful Links

Cisco Wireless LAN Security Web site

http://www.cisco.com/go/aironet/security

Cisco Aironet Wireless LAN Security Overview

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

SAFE: Wireless LAN Security in Depth

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml

Your 802.11 Wireless Network Has No Clothes

http://www.cs.umd.edu/%7Ewaa/wireless.pdf

Cisco response to *Your 802.11 Wireless Network Has No Clothes*

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246e.html

An Initial Security Analysis of the IEEE 802.1x Standard

http://www.cs.umd.edu/~waa/1x.pdf

Authentication with 802.1x and EAP Across Congested WAN Links

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800a9e8e.shtml

IEEE 802.11 Working Group Web site

http://grouper.ieee.org/groups/802/11/

CISCO SYSTEMS

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe