CHAPTER 4

Voice over WLAN Security

The security of a wireless LAN (WLAN) system is always a critical consideration in every WLAN deployment. Control of the WLAN access relies on the principles of Authentication, Authorization, and Accounting (AAA), augmented by encryption to ensure privacy. This chapter focuses on the authentication and encryption aspects of WLAN security, as they relate to VoWLAN deployments. For a more complete and system view of WLAN security, refer to the following guides:

- *Secure Wireless Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg10/secwire_1_0_book.html
- *Mobility Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

WLAN Security Overview

WLAN traffic is visible to any WLAN device within radio frequency (RF) range, and is a shared access medium. This creates a number of security challenges:

- How do you provide privacy for users of your WLAN, from non-users?
- How to provide privacy for users of your WLAN from each other?
- How to support privacy of multicast and broadcast traffic?
- How to identify which user is which on the WLAN?

Each generation of WLAN security have addressed these challenges in slightly different ways. But the key mechanisms are based on the same strategies used to secure communication over an untrusted medium(i.e., Authentication, Authorization and Accounting (AAA) , and encryption). The original 802.11 standard defined an encryption mechanism, Wired Equivalent Privacy (WEP), but did not define a AAA mechanism. The level of authentication offered in the 802.11 standard was at a group level, everyone in the group had to have the same encryption key. This key was used to encrypt unicast and multicast traffic. WLAN security solutions have augmented this group authentication by authenticating the client's MAC address. This is not considered a significant improvement in security as:

- It does not provide any additional per user privacy; the WEP key is still shared by all users.
- Offers a weak level of authentication as the 802.11 MAC addresses are sent unencrypted; the MAC address identifies the WLAN client and not the users.

- MAC address authentication can be difficult to administer for large groups of users, as the database of client MAC addresses must be maintained. The management for WEP keys is difficult, if a WEP needs to be changed all devices must be updated.

802.1X/EAP and Dynamic WEP

In order to provide an enterprise-level WLAN security, Cisco introduced the 802.1X/EAP authentication mechanisms to provide mutual authentication of WLANs and WLAN clients. During the authentication process, a unique per-user per session shared key is also derived and a portion of this key is used as per-session WEP encryption key. The Extensible Authentication Protocol (EAP) mechanism used by Cisco was called LEAP Lightweight Extensible Authentication Protocol (LEAP), which allowed users to perform an MSCHAPv2 authentication against a RADIUS server. Additional EAP mechanisms such as PEAP and EAP-TLS followed LEAP, all providing mechanism for dynamic WEP key generation. However, LEAP is considered the best suited of these for VoWLAN handsets as it requires fewer network transactions for authentication and has lower CPU requirements than the other EAP mechanisms.

Note EAP-FAST, if available, is the recommended EAP type for use of VoWLAN deployments. For more information about EAP-FAST, refer to EAP-FAST, page 4-3.

WEP

While the introduction of a dynamic WEP mechanism was a great improvement upon static WEP key implementations, weakness found in the WEP encryption mechanism means that the security of both static and dynamic WEP are compromised. Dynamic WEP is still the superior security mechanism to static WEP, but the security weaknesses in WEP are such that WEP, either static or dynamic, should not be relied upon to secure a WLAN network.

LEAP

LEAP has been found to have security weakness where weak passwords can be derived through analysis of the LEAP authentication transactions. The security weakness of LEAP is such that it should only be used where the use of strong passwords, a 10-character or higher random string, can be enforced. This means that LEAP may be suitable for VoWLAN handsets as they typically can have a strong passwords policy enforced, as the network administrator would control the handset's passwords. LEAP may be unsuitable for WLAN PCs, as LEAP would typical use the Windows password and these passwords are generally user-generated and a strong password policy can be difficult to enforce.

Note Although LEAP is considered secure for VoWLAN handsets when correctly deployed, it is recommended that a different EAP supplicant, such as EAP-FAST, be used if available.

EAP-FAST

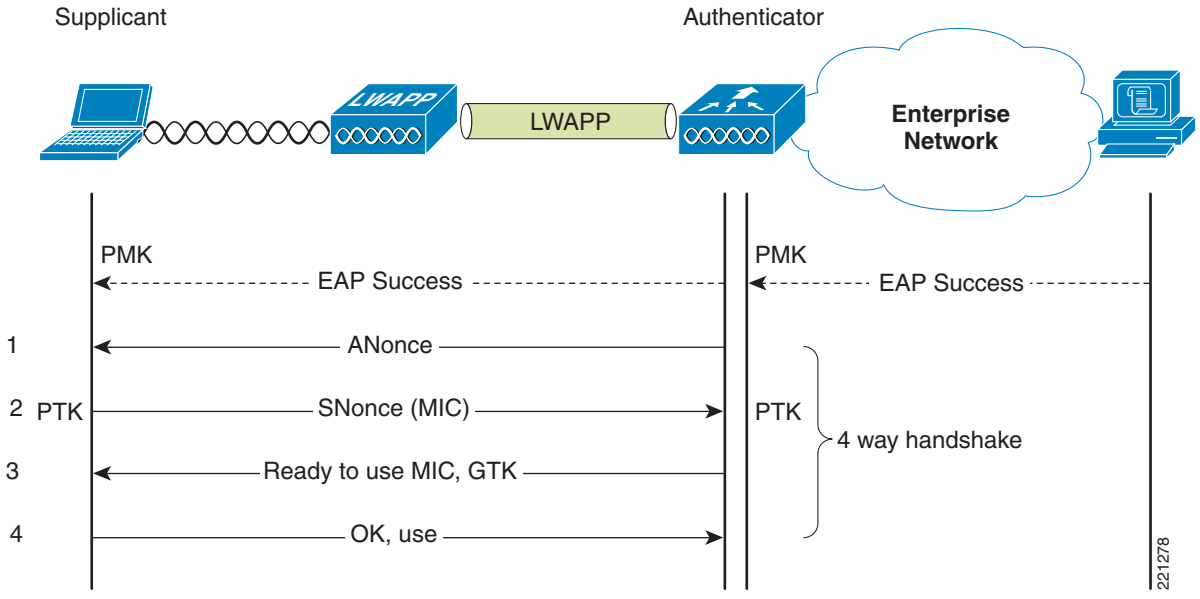
The recommended replacement for LEAP is EAP-Flexible Authentication via Secure Tunneling (EAP-FAST). The EAP-FAST protocol was specifically design to take into account the limited processing power of application specific devices (ASDs) such as VoWLAN handsets. It is designed to

provide the same tunneling protection as a tunneled authentication protocol such as PEAP, without requiring the Public Key Infrastructure (PKI) overhead associated with setting up the TLS tunnel used in PEAP. As a tunneled protocol EAP-FAST is capable of supporting multiple inner authentication mechanism such as MSCHAPv2 or GTC, the supported inner authentication mechanism depends upon the client implementation.

WPA

The weaknesses in WEP and the demand for a solution drove the Wi-Fi Alliance (http://www.wi-fi.org/) to develop WLAN security improvements, based on an 802.11i draft. These improvements are defined as Wi-Fi Protected Access (WPA). WPA addressed the main weakness in WEP encryption by replacing it with the Temporal Key Integrity Protocol (TKIP) which reuses the core encryption engine of WEP (RC4). The reuse of RC4 allowed TKIP to be implemented in the majority of systems through a firmware upgrade, rather than requiring a hardware upgrade. In addition to TKIP, WPA implemented one other major improvement to WEP encryption, an additional message integrity check (MIC) mechanism. In addition to the encryption and message integrity improvements WPA introduced cryptographic improvements where the key shared between the WLAN client and the WLAN AP is not used directly for encryption, but instead it is used as the basis for a 4-way cryptographic handshake, that derives the encryption key, and passes the multicast (group) key. This 4-way handshake is used in both WPA-Personal and WPA-Enterprise. Figure 4-1 shows the basic 4-way handshake mechanism used in WPA-Enterprise. The difference between the WPA-Enterprise behavior and the WPA-Personal behavior is that the 4-way handshake with WPA-Enterprise uses a key derived during the EAP authentication as the base key of the 4-way. Whereas WPA-Personal 4-way handshake users a shared key configured in the WLAN client, Supplicant, and the WLC Authenticator (see Figure 4-1).

Figure 4-1 4-Way Handshake



The keys used for encryption are derived from the PMK that has been mutually derived during the EAP authentication. This PMK is sent to the authenticator in the EAP success message, but is not forwarded to the supplicant because the supplicant has derived its own copy of the PMK:

Step 1 The authenticator sends an EAPOL-Key frame containing an authenticator nonce (ANonce), which is a random number generated by the authenticator).

a. The supplicant generates an supplicant nonce (SNonce), which is a random number generated by the supplicant).

b. The supplicant derives a pair-wise temporal key (PTK) from the ANonce and SNonce (supplicant nonce, which is a random number generated by the client/supplicant).

Step 2 The supplicant sends an EAPOL-Key frame containing an SNonce, the RSN information element from the (re)association request frame, and a MIC (generated from the PMK).

a. The authenticator derives the PTK from the ANonce and SNonce and validates the MIC in the EAPOL-Key frame.

Step 3 If the validation is successful, the authenticator sends an EAPOL-Key frame containing the group temporal key (GTK), the multicast, and the broadcast encryption key.

a. Upon validating the MIC from this frame, the supplicant installs its PTK and the GTK.

Step 4 The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

a. Upon validating the MIC from this frame, the authenticator installs the PTK for this client.

At this point the supplicant and authenticator have verified that they both have a matching PMK, and both share the same PTK and GTK.

WPA-Personal

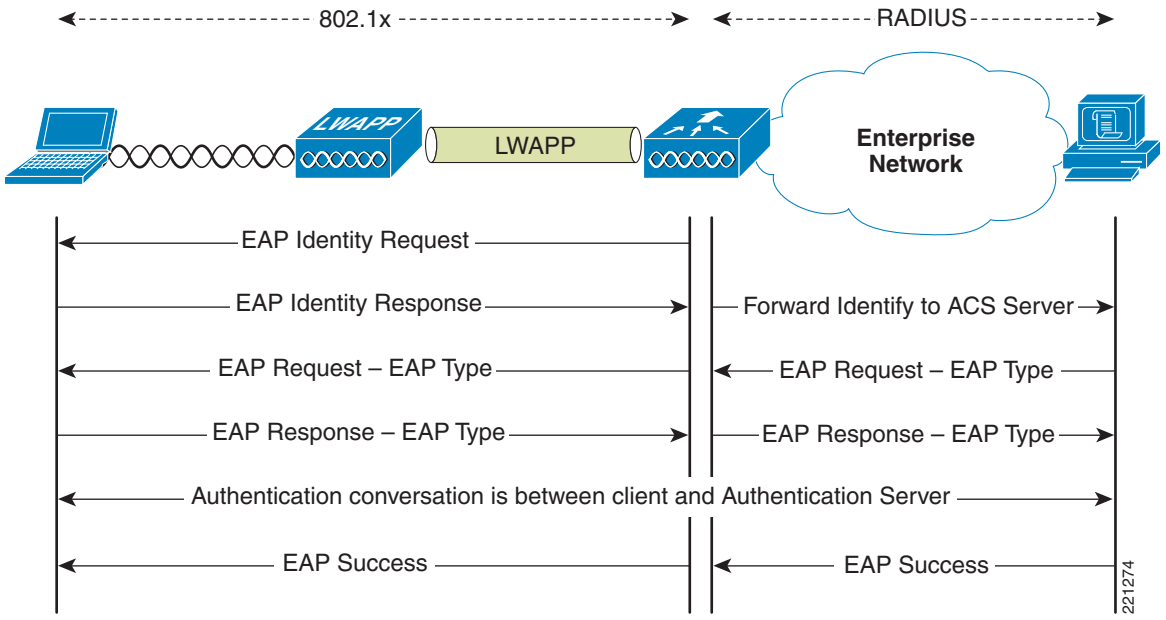
WPA-personal uses the same cryptographic tools, as WPA-Enterprise but uses a shared key to authenticate WLAN clients. This shared key is the key that used in the 4-way handshake that creates the encryption key for that session. The shared key mechanism of authentication used in WPA-Personal does not provide a per-user or per device authentication, every device and every AP that is part of that WLAN uses the same shared key. The key used for encryption is unique per user and per session thanks to the randomizing that occurs during the 4-way handshake, but the shared key used to authenticate is the same for everyone. The primary advantage of WPA-personal in a VoWLAN deployment is that it does not require the use of a AAA server, and this can be an advantage in branch deployments.

Note Strong keys should be used as there are tools available that can successfully perform a dictionary attack on WPA-personal.

WPA-Enterprise

WPA-enterprise uses the base WPA frame protection features, and cryptographic features as WPA-personal, but adds 802.1X/EAP-based authentication to the certification. In WPA-enterprise the shared key that is used to generate the cryptographic key through 4-way handshake is derived during the EAP Authentication. The EAP authentication process provides the AAA features missing in WPA-personal, allowing each user/device to be individually authenticated, a policy based on the authentication ID applied (authorization), and the collection of statistics based on authentication ID (accounting). Figure 4-2 shows an example of EAP protocol flow.

Figure 4-2 EAP Protocol Flow



WPA-Enterprise vs WPA-Personal

Generally, the use of WPA-enterprise is preferred over WPA-personal in enterprise deployments; therefore, the naming convention, WPA-personal is targeted more at the home users. Shared key security systems do not provide the AAA features required for the enterprise, and can introduce operational issues due to the overhead in updating the shared keys if a WLAN client is lost, stolen, or as part of a regular key rotation regime. The reward for successfully cracking, guessing, or stealing the shared key is very high, as it the key for all users. In some deployments WPA personal may be used for VoWLAN deployments, as the enterprise security requirement for AAA need to be balanced against the VoWLAN handset requirements, and characteristics. Voice systems have very high availability requirements, and these may be difficult to achieve in branch and remote environments, when there is a dependency upon a centralized authentication system. This could be addressed by distributing authentication databases to branches through local AAA servers or the embedded AAA services of a WLC; or by deploying a VoWLAN system that does not rely on centralized authentication, such as WPA-personal. The security requirements of VoWLAN also need to be considered in light of the access given to the VoWLAN handsets (i.e., the VoWLAN handset need not be given access to the entire enterprise network) is able to make and receive phone calls, and have limited application access. In addition, a handset such as a Cisco 7921G has application level AAA performed by the UC Manager where the handset is authenticated, authorized, and accounting information is collected.

WPA2

The security features developed in WPA were based on the recommendations of the 802.11i workgroup that was tasked with replacing original security features defined in the 802.11 standard. The market demands for a replacement for WEP, where WPA was released prior to the ratification of the 802.11i standard. There are also slight differences between WPA and the related sections of the 802.11i standard; these differences should be transparent to users. The sections from the 802.11i standard used by WPA primarily addresses the need for a securing the WLAN while maintaining sufficient backward compatibility with WEP for the deployed hardware to be upgraded, though software and firmware

changes. While the security changes from 802.11i adopted by WPA are important, the key component in 802.11i was the incorporation of the Advanced Encryption Standard (AES) into WLAN security this would align its encryption mechanism with the new industry standard for encryption. The underlying mechanism of AES-Counter Mode CBC-MAC (AES-Counter Mode describes the encryption mechanism, and CBC-MAC describes frame protection mechanism) is very different to those of WPA and WEP, and generally requires hardware upgrades to be supported. The hardware requirements to support AES encryption in WPA2 mean that migration from WPA is dependent upon a hardware refreshes. In many cases, updating the network infrastructure is an easier task than updating the WLAN client infrastructure and a complete migration to WPA2 is dependent upon a generational change in the WLAN client infrastructure. The desire to migrate from WPA to WPA2 is also tempered by the knowledge that currently there are no known serious security exposures in WPA.

WPA2-Personal

WPA2-Personal uses the same shared key and 4-way handshake of WPA, but uses the AES-Counter Mode CBC-MAC Protocol to encrypt and protect frames.

WPA2-Enterprise

WPA2-Enterprise uses the same 802.1X/EAP authentication and 4-way handshake of WPA, but uses the AES-Counter Mode CBC-MAC Protocol to encrypt and protect frames.

EAP Timing

The EAP authentication mechanism, its supporting infrastructure and protocols, has to make some assumptions about what is a reasonable amount of time to wait for a WLAN client during the EAP authentication process. These assumptions are based on the typical timing from PC clients, and may not be valid for lower CPU devices such as VoWLAN handsets. For example, an EAP timer adjustment is recommended when using EAP-FAST authentication for the 7921G phone. If not implemented the 7921G is likely to fail authentication even though its credentials are correct.

To adjust the EAP request timeout to 20: [WiSM]]-slot3-1) config advanced eap request-timeout 20 show advanced eap command:

```
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries.............. 20
EAP Key-Index for Dynamic WEP................. 0
EAP Max-Login Ignore Identity Response....... enable
EAP-Request Timeout (seconds)................. 20
EAP-Request Max Retries....................... 2
```

Note Only adjust the EAP timers on the advice of the VoWLAN handset vendor, or when following recommendation from Cisco TAC.

Network Segmentation

The VoIP network shares the base network infrastructure of an enterprise network, but should be separated whenever possible from the general purpose data network. The topic of segmenting and securing the VoIP network is beyond the scope of this design guide, but the VoWLAN network should be separated from the WLAN data network. This can be done in the Cisco Unified Wireless Network,

through the assignment of a VoWLAN interface on the WLC, which is a type of VLAN separation. This should be sufficient to provide integration into the large enterprise VoIP segmentation scheme, whether that be VLAN segmentation, IP address segmentation, or VRF segmentation.