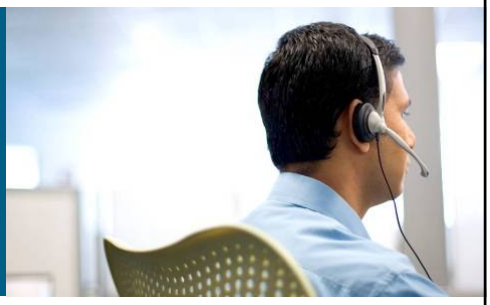
Introducing Wireless Security



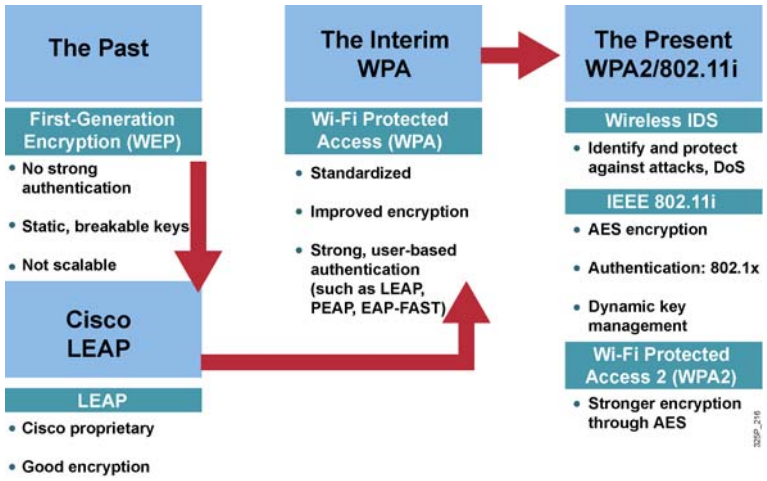
Objectives

- Describe the need for WLAN security.
- Describe the evolution of WLAN security methods.
- Identify common authentication and encryption technologies used in WLANs.
- Explain the benefits and weaknesses of the common security methods used in WLANs.

The Need for WLAN Security

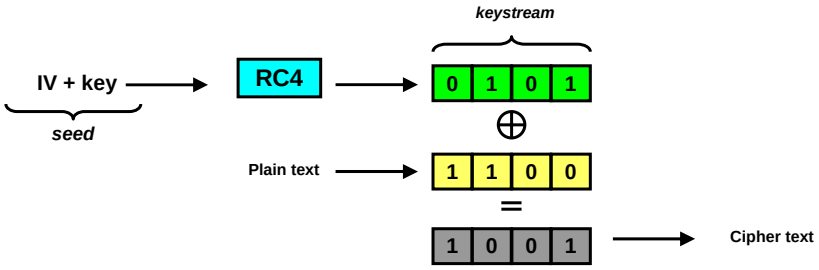
- Vulnerabilities:
  - War driving
  - Non-secret SSID
  - MAC filtering
  - Automatic DHCP
  - Man-in-the middle attacks
  - Cracking WEP
  - Initialization Vector attacks
  - Password Cracking
  - DoS attacks
- WLAN Security requires:
  - Authentication: Proves the user belongs on the network
  - Encryption: Protects the data traversing the network

Evolution of WLAN Security



802.11 WEP

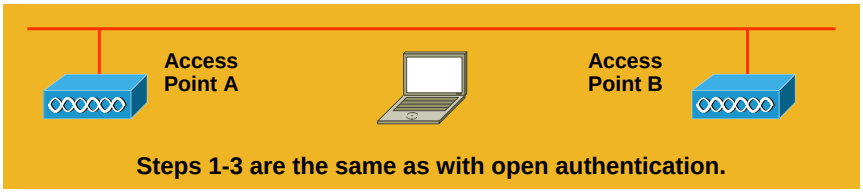
- WEP aims at providing Wired Equivalent Privacy
- WEP is an optional IEEE standard for encryption
- Keys can be static and shared among many clients
- Uses RC4 algorithm—known vulnerabilities
- Keys can be dynamic and unique for each client (as with 802.1x) per session



802.11 Open Authentication

1. Client sends probe request.
2. Access points (A/B) send probe response. Client evaluates access point response and selects the best access point.
3. Client sends authentication request to selected access point (A).
4. Access point A confirms authentication and registers client.
5. Client sends association request to selected access point (A).
6. Access point A confirms association and registers client.

802.11 Shared Key Authentication



4. **Access point A sends authentication response containing the unencrypted challenge text.**
5. **Client encrypts the challenge text using one of its WEP keys and sends it to access point (A).**
6. **Access point A compares the encrypted challenge text to its copy of the encrypted challenge text. If the text is the same, access point A will allow the client onto the WLAN.**

Cisco Enhanced 802.11 WEP Security

- Cisco prestandard enhancements
- Implemented in 2001 and 2002
- Authentication:
  - 802.1x and Extensible Authentication Protocol (EAP) protocols
  - User, token, and machine credentials
  - Dynamic encryption key generation
- Encryption:
  - CKIP
  - CMIC

Enhanced 802.11 Security

- Authentication:
  - 802.1x and Extensible Authentication Protocol (EAP) protocols
  - User, token, and machine credentials
  - Dynamic encryption key generation
  - IEEE 802.11i
- Encryption:
  - TKIP and MIC
  - Wi-Fi Protected Access (WPA)—TKIP encryption
  - WPA2—Advanced Encryption Standard (AES)

Encryption—TKIP and MIC

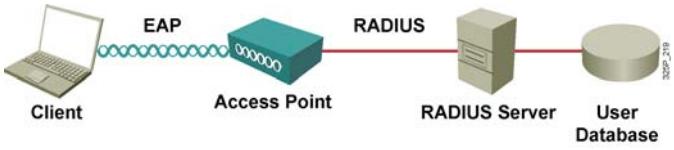
- TKIP:
  - Key hashing for unique seed values per packet to protect against WEP initialization vector vulnerabilities
  - MIC from Michael algorithm
  - Broadcast key rotation
- MIC:
  - Provides more protection than Integrity Check Value (ICV) by protecting the header and the payload
  - Protects against man-in-the-middle or replay attacks

WPA2 and AES

- WPA2 offers the following:
  - Authenticated key management
  - Key validation mechanisms for unicast and broadcast keys
  - TKIP is used, which for WPA includes both per-packet keying and MIC
  - Expanded IV (defeats AirSnort)
  - Broadcast key rotation
- AES Encryption:
  - 128-bit block cipher—cryptographically more robust than RC4
  - Requires new radio cards on clients and access points because more CPU power is required

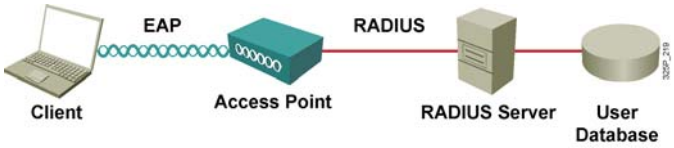
802.1x Authentication Overview

- The wireless client must be authenticated before it gains access to the network
- Extensible and interoperable supports:
  - Different EAP authentication methods or types
  - May be used with multiple encryption algorithms
  - Depends on client capability
- Supported by Cisco since December 2000



802.1x Authentication Key Benefits

- Mutual authentication between client and authentication (RADIUS) server
- Encryption keys derived after authentication
- Centralized policy control

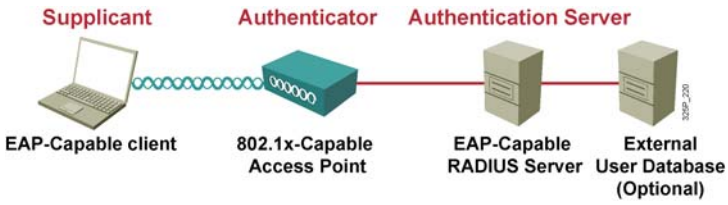


802.1x and EAP Authentication Protocols

- LEAP—EAP Cisco Wireless
- EAP-FAST
- EAP-TLS
- PEAP:
  - PEAP-GTC
  - PEAP-MSCHAPv2

Components Required for 802.1x Authentication

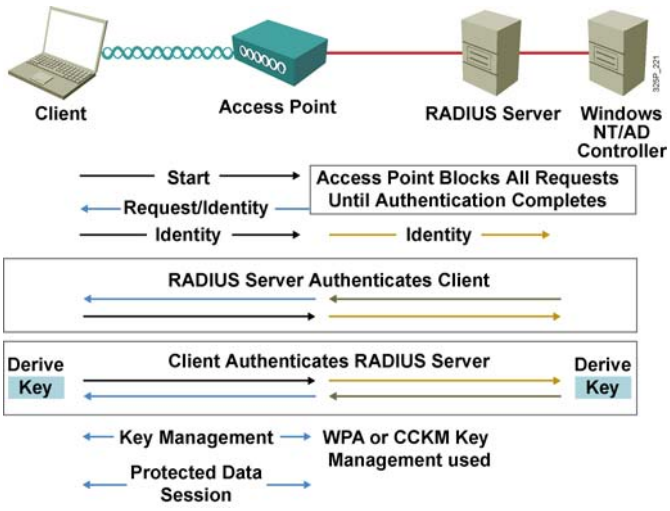
- Authentication server is an EAP-capable RADIUS server:
  - Cisco Secure ACS, Microsoft IAS, Meetinghouse Aegis
  - Local authentication service on Cisco IOS access point
  - May use either local RADIUS database or an external database server such as Microsoft Active Directory or RSA SecurID
- Authenticator is an 802.1x-capable access point.
- Supplicant is an EAP-capable client:
  - Requires 802.1x-capable driver
  - Requires an EAP supplicant—either available with client card, native in operating system, or from third-party software



Cisco LEAP

- Client support:
  - Windows 98-XP-Vista, Windows CE, Macintosh OS 9.X or 10.X, and Linux Kernel 2.2 or 2.4
  - Cisco Compatible Extensions Clients (CCXv1)
- RADIUS server:
  - Cisco Secure ACS and Cisco Access Registrar
  - Meetinghouse Aegis
  - Interlink Merit
- Microsoft domain or Active Directory (optional) for back-end authentication (must be Microsoft format database)
- Device support:
  - Cisco autonomous access points and bridges
  - Cisco lightweight access points and WLAN controllers
  - Cisco Unified Wireless IP Phone 7920 (VoIP) handset

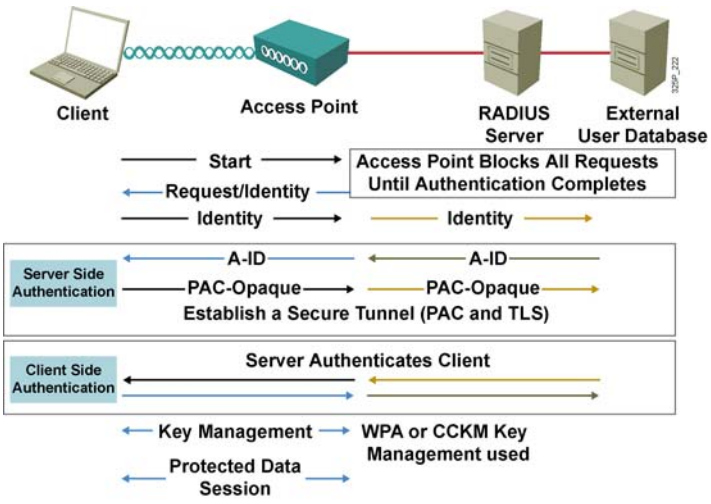
Cisco LEAP Authentication



EAP-FAST: Flexible Authentication via Secure Tunneling

- Considered in three phases:
  - Protected access credential is generated in Phase 0 (Dynamic PAC provisioning):
    - Unique shared credential used to mutually authenticate client and server
    - Associated with a specific user ID and an authority ID
    - Removes the need for PKI
  - A secure tunnel is established in Phase 1.
  - Client is authenticated via the secure tunnel in Phase 2.

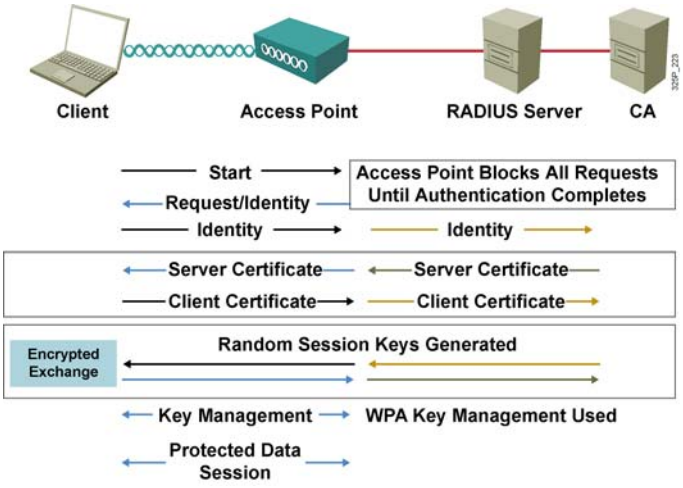
EAP-FAST Authentication



EAP-TLS

- Client support:
  - Windows 2000, XP, and Windows CE (natively supported)
  - Non-Windows platforms: Third-party supplicants (Meetinghouse)
  - User certificate required for each client
- Infrastructure requirements:
  - EAP-TLS-supported RADIUS server
    - Cisco Secure ACS, Cisco Access Registrar, Microsoft IAS, Aegis, Interlink
  - RADIUS server requires a server certificate
  - Certificate authority server (PKI)
- Certificate management:
  - Both client and RADIUS server certificates to be managed

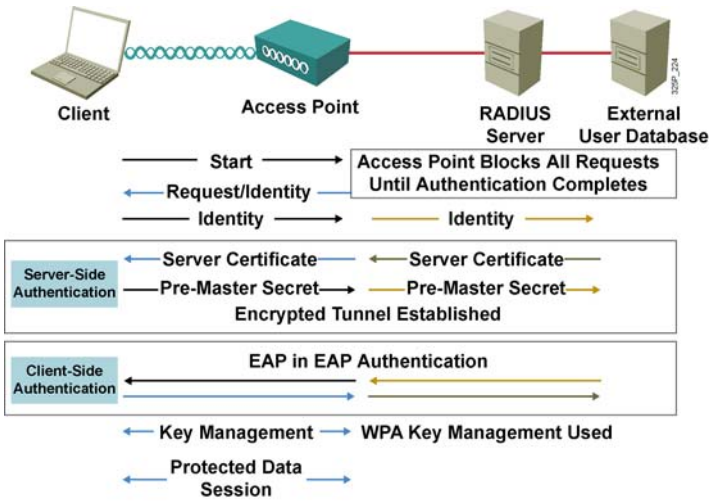
EAP-TLS Authentication



EAP-PEAP

- Hybrid authentication method:
  - Server-side authentication with TLS
  - Client-side authentication with EAP authentication types
    - EAP-GTC
    - EAP-MSCHAPv2
- Clients do not require certificates.
- RADIUS server requires a server certificate:
  - RADIUS server has self-issuing certificate capability.
  - Purchase a server certificate per server from PKI entity.
  - Set up a simple PKI server to issue server certificates.
- Allows for one-way authentication types to be used:
  - One-time passwords
  - Proxy to LDAP, Unix, Microsoft Windows NT and Active Directory, Kerberos

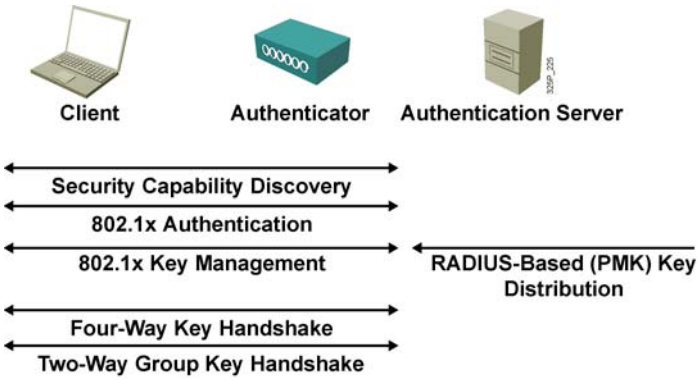
EAP-PEAP Authentication



Wi-Fi Protected Access

- WPA introduced in late 2003
- Prestandard implementation of IEEE 802.11i WLAN security
- Addresses currently known security problems with WEP
- Allows software upgrade on deployed 802.11 equipment to improve security
- Components of WPA:
  - Authenticated key management using 802.1x: EAP authentication and preshared key authentication
  - Unicast and broadcast key management
  - Standardized TKIP per-packet keying and MIC protocol
  - Initialization vector space expansion: 48-bit initialization vectors
  - Migration mode—coexistence of WPA and non-WPA devices (optional implementation that is not required for WPA certification)

802.11i and WPA Authentication and Key Management Overview



WPA Issues

- WPA uses TKIP, which uses the same base encryption algorithm, RC4, as WEP.
- WPA cannot entirely avoid the design flaws of WEP.
- WPA is a compromise solution.
- Software upgrade is required for clients and access points, which gives no guarantee that all vendors will support the solution.
- Operating system support or a supplicant client is required.
- WPA is susceptible to a new type of DoS attack.
- WPA is susceptible to a recently discovered weakness when preshared keys are used.

IEEE 802.11i—WPA2

- 802.11i:
  - Ratified in June 2004
  - Standardizes:
    - 802.1x for authentication
    - AES encryption—Facilitates U.S. government FIPS 140-2 compliance
    - Key management
- WPA2:
  - Supplement to WPA “version 1”—Wi-Fi Alliance interoperable implementation of 802.11i
  - Provides for AES encryption to be used
  - Proactive Key Caching
  - Third-party testing and certification for WLAN device compatibility

Wireless Intrusion Detection Systems

- Address RF-related vulnerabilities:
  - Detect, locate, and mitigate rogue devices
  - Detect and manage RF interference
  - Detect reconnaissance if possible
- Address standards-based vulnerabilities:
  - Detect management frame and hijacking-style attacks
  - Enforce security configuration policies
- Complementary functionality:
  - Forensic analysis
  - Compliance reporting

WPA and WPA2 Modes

	WPA	WPA2
Enterprise mode (business, education, government)	Authentication: IEEE 802.1x/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1x/EAP Encryption: AES-CCMP
Personal mode (SOHO, home, personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

WPA2 Issues

- Client (supplicant) must have a WPA2 driver that supports EAP.
- RADIUS server must understand EAP.
- PEAP carries EAP types within a channel secured by TLS and so requires a server certificate.
- WPA2 is more computationally intensive with optional AES encryption.
- WPA2 may require new WLAN hardware to support AES encryption.

Summary

- With increased reliance on WLANs, businesses are becoming more concerned about network security. Network managers need to provide end users with freedom and mobility without offering intruders access to the WLAN or the information sent and received on the wireless network.
- Authentication and encryption are the two primary facilities for securing the WLAN. While encryption using static WEP keys is very vulnerable, WLANs can now be configured to support EAP and the 802.1x standards including LEAP, EAP-FAST, EAP-TLS, PEAP, WPA, and WPA2.