

CISCO SYSTEMS



Wireless LAN Security

Marco Misitano, CISSP

Enterprise Consulting, Security
misitano@cisco.com

Agenda

- **Wireless Security in 802.11**
- **Vulnerabilities in 802.11 Wireless Security**
- **Technologies for Secure Wireless LANs**
- **What Lies Ahead**

Agenda

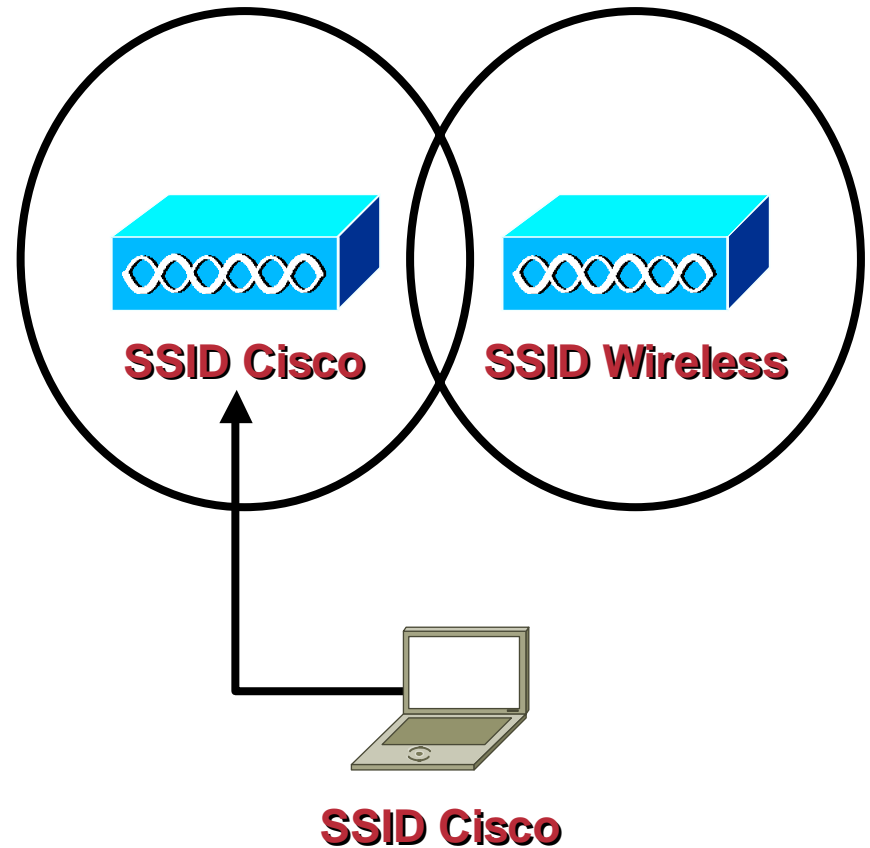
- **Wireless Security in 802.11**
- **Vulnerabilities in 802.11 Wireless Security**
- **Technologies for Secure Wireless LANs**
- **What Lies Ahead**

802.11 Wireless Security

- **Service Set Identifier (SSID)**
- **Wired Equivalent Privacy (WEP)**
- **Open Authentication**
- **Shared Key Authentication**
- **MAC Address Authentication**

The Service Set Identifier (SSID)

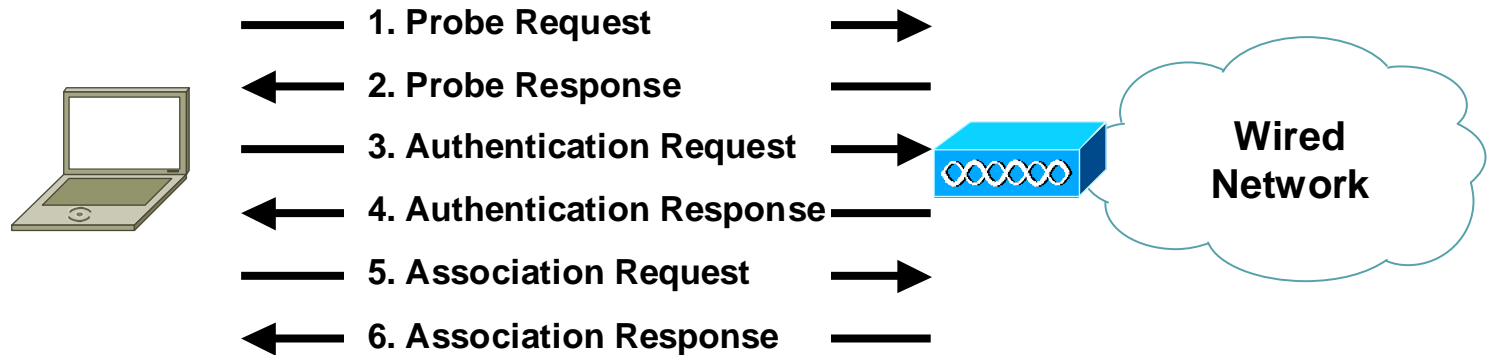
- Used to logically separate wireless LANs



WEP Encryption

- **Wired Equivalent Privacy**
- **Based on the RC4 symmetric stream cipher**
- **Static, pre-shared, 40 bit or 104 bit keys on client and access point**

802.11 Authentication

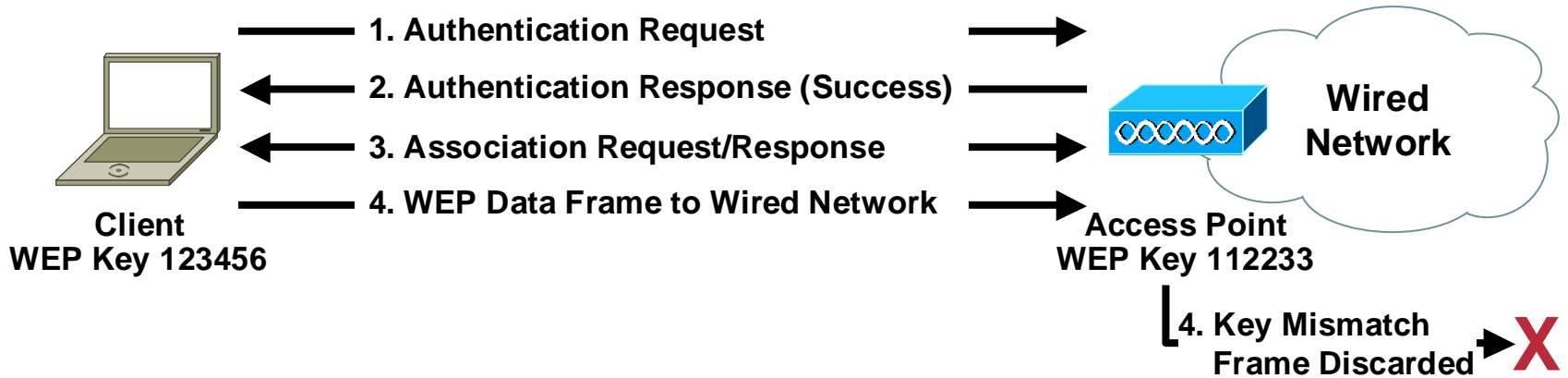


- **Client probes for an AP**
- **Client requests authentication**
- **Client requests association**
- **Client can begin data exchange**

802.11 Open Authentication

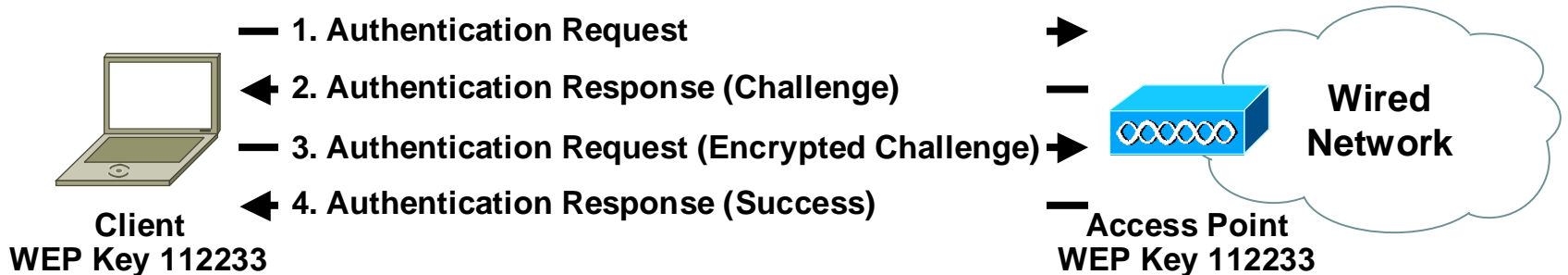
- **Device oriented authentication**
- **Uses null authentication—All requests are granted**
- **With no WEP, network is wide open to any user**
- **If WEP encryption is enabled, WEP key becomes indirect authenticator**

802.11 Open Authentication



- Client send authentication request
- AP sends Success response
- WEP keys must match for data to traverse AP

802.11 Shared Key Authentication



- **Client and AP must use WEP with pre-shared keys**
- **Client requests shared key authentication**
- **AP sends plaintext challenge**
- **Client encrypts challenge with WEP key and responds**
- **If the AP can decrypt the response, client is valid**

Wireless Security in 802.11 Summary

- **Authentication is device oriented**
- **Static, pre-shared WEP for encryption**
- **No key management specified**

Agenda

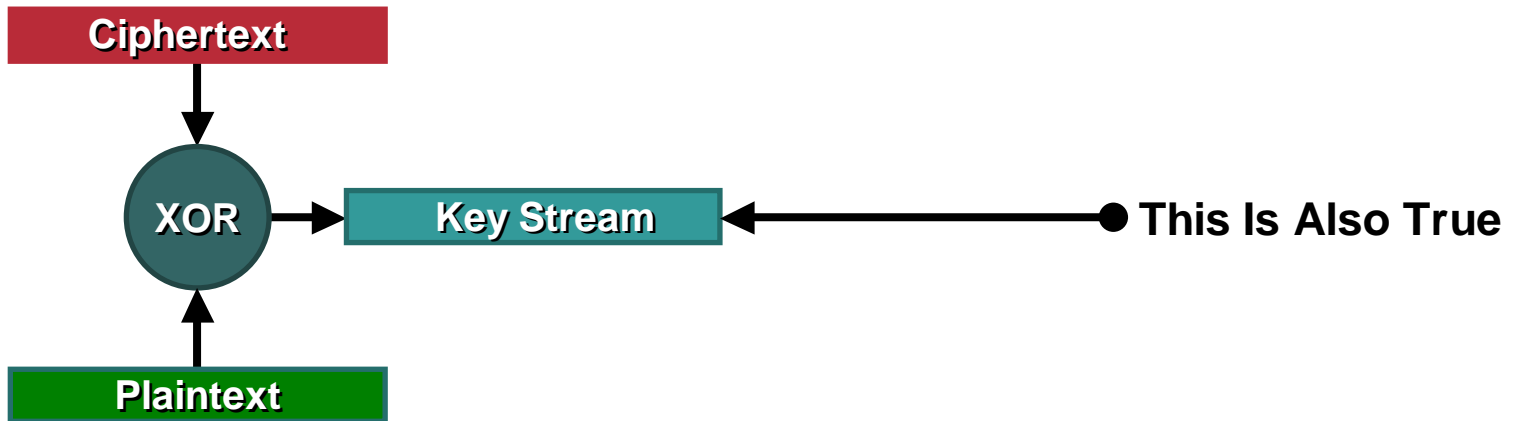
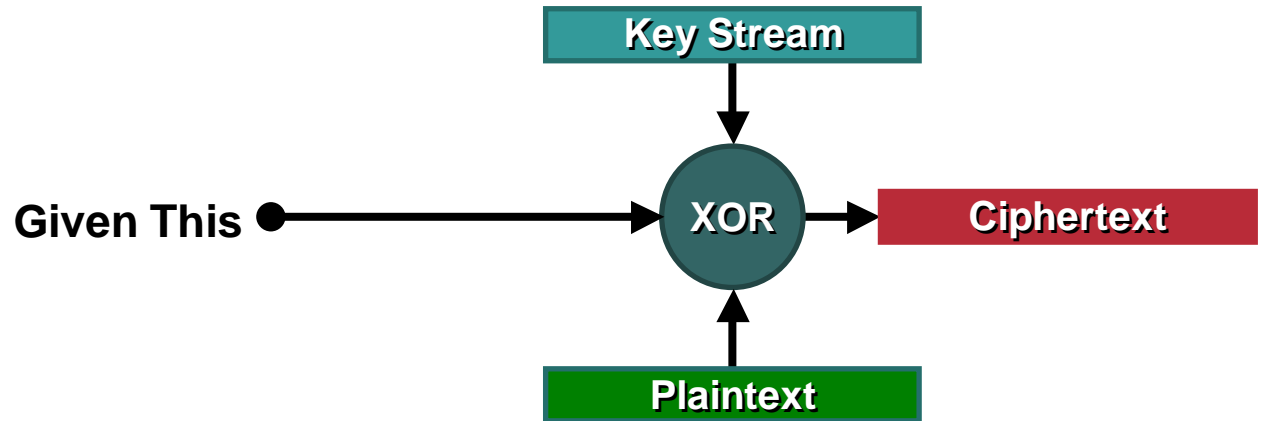
- **Wireless Security in 802.11**
- **Vulnerabilities in 802.11 Wireless Security**
- **Technologies for Secure Wireless LANs**
- **What Lies Ahead**

Vulnerabilities in 802.11 Wireless Security

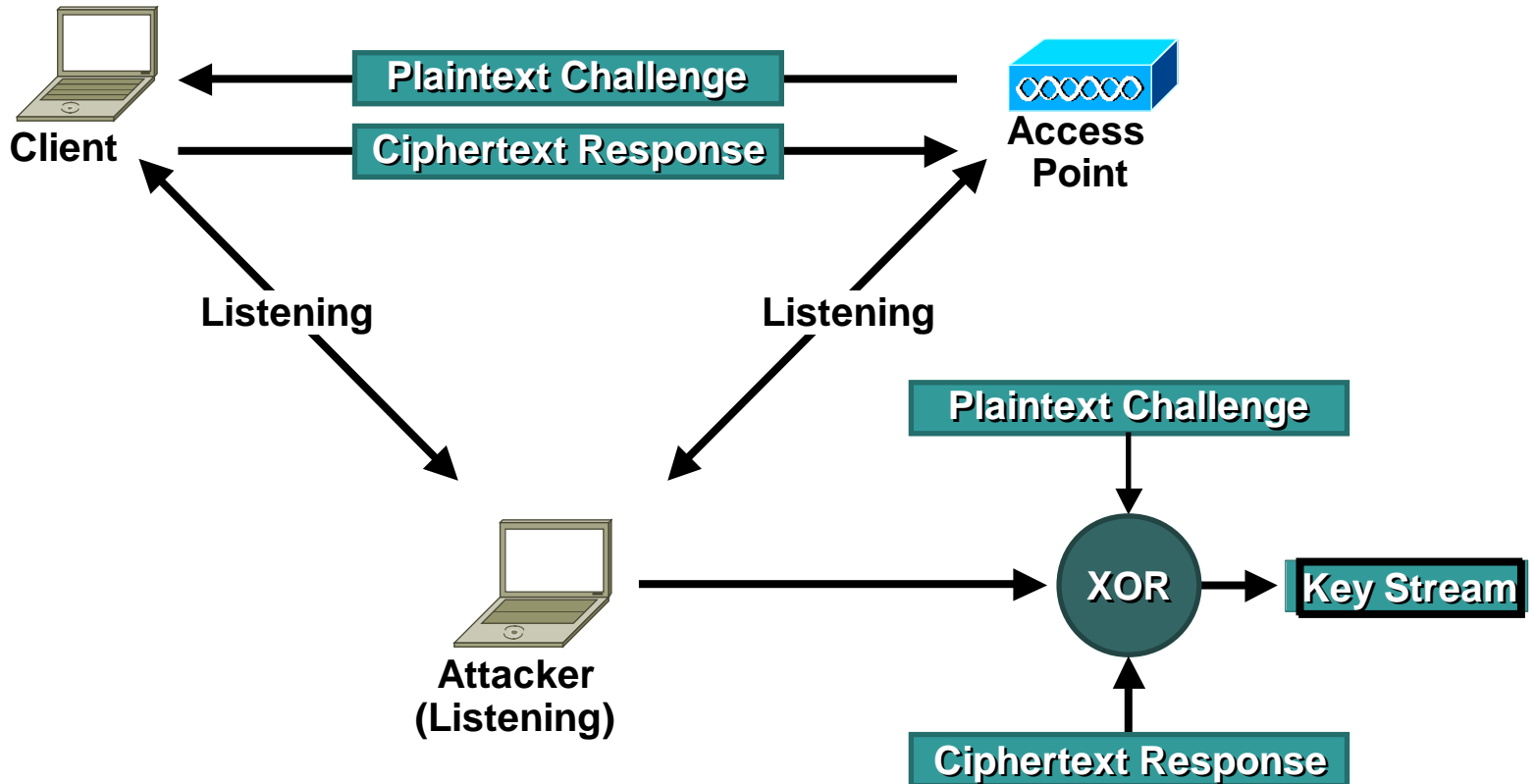
Cisco.com

- **Authentication Vulnerabilities**
- **Statistical WEP Key Derivation**
- **Inductive WEP Key Derivation**

Authentication Vulnerabilities



Authentication Vulnerabilities



- **Shared Key is vulnerable to Man in the Middle Attack**

Authentication Vulnerabilities

- **MAC Authentication is weak**
- **MAC addresses are sent in the clear**
- **MAC addresses can be sniffed and spoofed**

Statistical Key Derivation

- **802.11 WEP is flawed**
- **A WEP key can be derived in 1M to 4M frames using statistical analysis**
- **Attacker is passive, and 'listens' to wireless LAN**
- **Implemented in the AirSnort application**

802.11 Security Summary

- **The security mechanisms in the 1997 802.11 specification are flawed**
 - Open authentication**
 - Shared Key authentication**
 - WEP**
- **These will **NOT** secure your wireless LAN!!**

802.11 Security Summary

- **Requirements for wireless authentication**
 - User-based, centralized, strong authentication**
 - Mutual authentication of client and network**
- **Requirements for wireless privacy**
 - Strong, effective encryption**
 - Effective message integrity check**
 - Centralized, dynamic WEP key management**

Agenda

- **Wireless Security in 802.11**
- **Vulnerabilities in 802.11 Wireless Security**
- **Technologies for Secure Wireless LANs**
- **What Lies Ahead**

Secure Wireless LANs

User Considerations

- **Single sign on**
- **Extensible authentication support**
- **Minimal security overhead**

Secure Wireless LANs Infrastructure Considerations

- **Cost**
 - Additional Server Hardware**
 - Additional Network Infrastructure**
- **Rapid Deployment**
- **Maintenance and Support**
 - Impact to client and infrastructure**
- **Future 802.11 Enhancements**
 - Interoperability with enhancements**

Technologies for Secure Wireless LANs

- **VPN**
- **802.1X with TKIP encryption**

Secure Authentication Requirements

- **Centralized authentication via AAA server**
- **Mutual authentication of client and network**
- **Support for dynamic, user-based encryption keys**
 - Optional capability to change keys**

- **Two phase authentication**
 - Device authentication via pre-shared key or PKI**
 - User authentication via AAA server**
- **Mutual authentication**
- **Extensible user authentication types**

802.1x Standard

Port-Based Network Access Control

- Falls under 802.1 **not** 802.11
- This is a **network** standard, not a wireless standard
- Is part of the 802.11i draft
- Provides network authentication, **not** encryption
- Incorporated as part of LEAP

802.1x Overview

- Standard set by the IEEE 802.1 working group
- Describes a standard **link layer protocol** used for transporting higher-level authentication protocols
- Works between the **supplicant** (client) and the **authenticator** (network device)
- Maintains backend communication to an **authentication (RADIUS) server**

EAP Overview

- **EAP—The Extensible Authentication Protocol**
- **A flexible protocol used to carry arbitrary authentication information**
- **Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)**
- **Specified in RFC 2284**
- **Support multiple “authentication” types:**
 - Plain password hash (MD5) (not mutual)**
 - OTP Tokens (not mutual)**
 - TLS (based on X.509 certificates)**
 - And EAP-Cisco Wireless!!**

802.1x and EAP

- **802.1x Transport authentication information in the form of Extensible Authentication Protocol (EAP) payloads**
- **The authenticator (AP or switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information**
- **Three forms of EAP are specified in the 802.1x standard**
 - EAP-MD5—MD5 Hashed Username/Password**
 - EAP-OTP—One-Time Passwords**
 - EAP-TLS—Strong PKI Authenticated Transport Layer Security (TLS)**

802.1x Header

EAP Payload

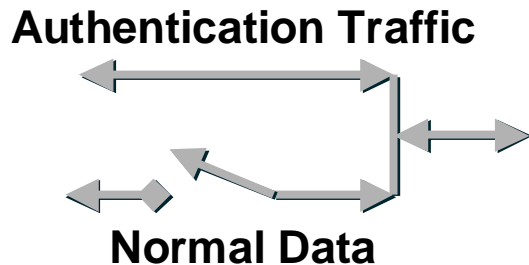
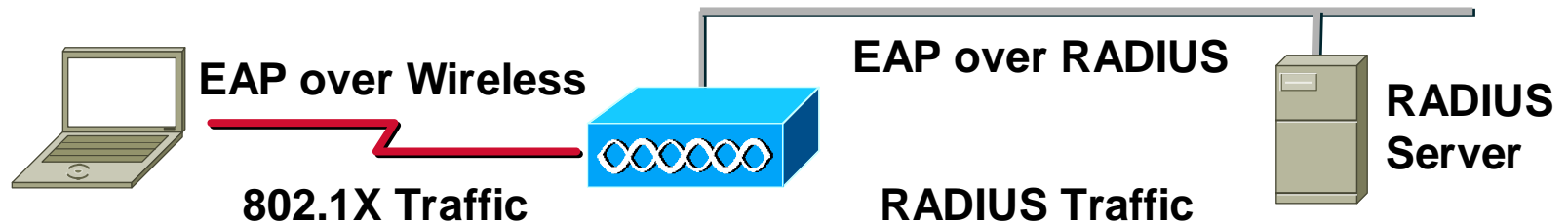
802.1x, EAP and RADIUS

- **RADIUS—The Remote Authentication Dial In User Service**
- **A protocol used to communicate between a network device and an authentication server or database**
- **Allows the communication of login and authentication information; i.e., username/password, OTP, etc.**
- **Allows the communication of arbitrary value pairs using “Vendor Specific Attributes” (VSAs)**
- **Can also act as a transport for EAP messages**



802.1x / EAP Authentication

802.11 Association Complete; Data Blocked by AP



AP “Encapsulates” 802.1x Traffic into RADIUS Traffic, and Visa Versa

AP Blocks Everything but 802.1x-to-RADIUS Authentication Traffic

802.1x for Wireless LANs

- **Multiple wireless vendors have adopted 802.1x for WLANs**
- **802.1X authentication protocols include EAP-Cisco Wireless, EAP-TLS, EAP-MD5, TTLS, and PEAP**
- **Microsoft has integrated support for EAP-TLS and EAP-MD5 into Windows XP operating system**

Also has announced support for EAP on native platforms (Windows 2000, Windows NT 4, Windows 98 and Windows ME)

EAP Authentication Types for Wireless LANs

- **EAP-Cisco (aka LEAP)**
Password-based
- **EAP-TLS (Transport Layer Security)**
Certificates-based
- **EAP-PEAP (Protected EAP)**
Hybrid—Certificate/Password
- **EAP-TTLS (Tunneled TLS)**
Hybrid—Certificate/Password
- **EAP-SIM (SIM Card)**
Authentication by SIM Cards

Authentication Attack Mitigation

	EAP-MD5	EAP-Cisco	EAP-TLS	EAP-TTLS/PEAP	VPN
Rogue APs		X	X	X	X
Session Hijacking		X	X	X	X
Man in the Middle		X	X	X	X
Dictionary Attack	X*	X*	X	X	X

X: Mitigates Vulnerability

***Requires the Use of Strong Passwords**

Strong Encryption Requirements

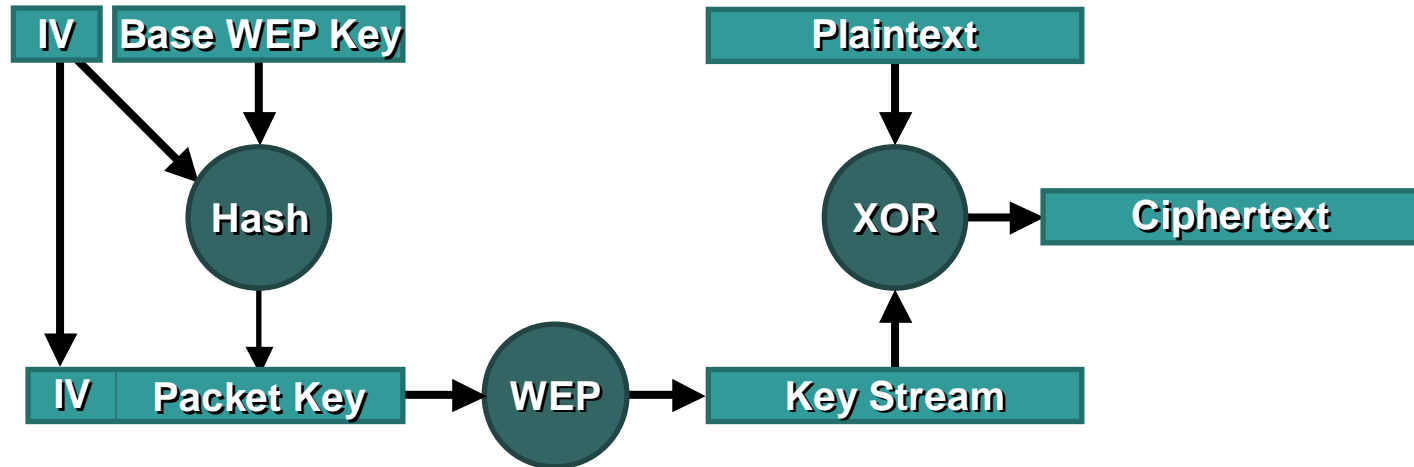
- **Cryptographically sound encryption algorithm**
- **Effective message integrity**

- **Temporal Key Integrity Protocol (TKIP)**
 - Enhances WEP encryption**
 - Per Packet Keying**
 - Message Integrity Check**
- **VPN over Wireless**
 - 3DES encryption—Tried and true**
 - HMAC-SHA1 or HMAC-MD5 message authentication**

TKIP Encryption

- **Cisco offers a pre-standards implementation**
- **Per Packet Keying**
- **Message Integrity Check**
- **Broadcast Key Rotation**

Per Packet Keying Operation

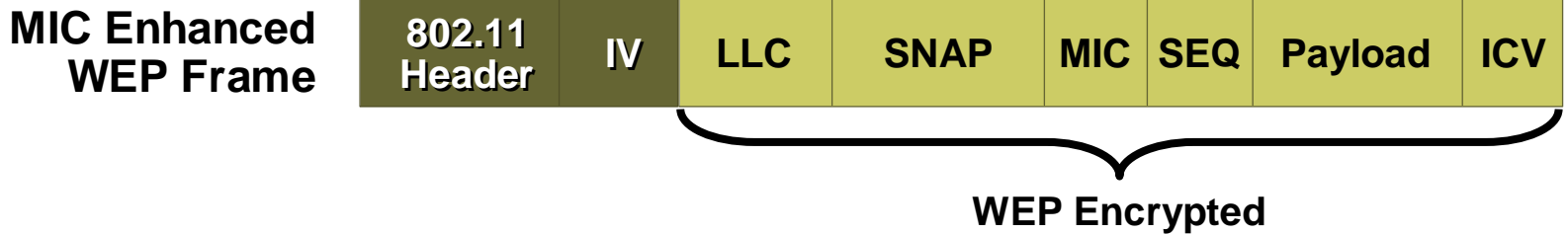
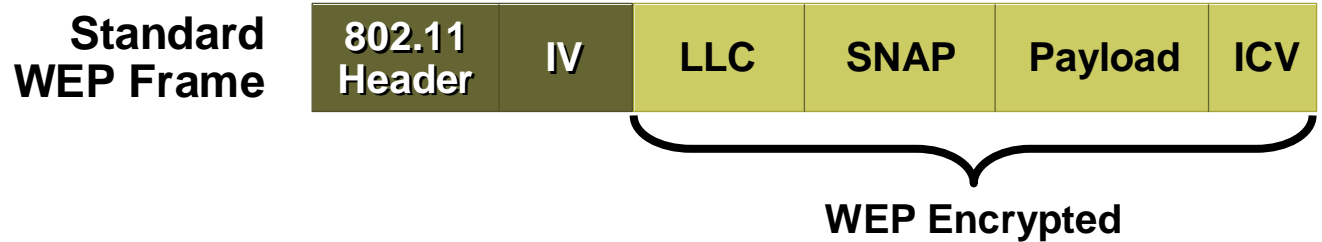


- **IV Sequencing—IVs increment by one**
- **Per Packet IV is hashed with base WEP key**
- **Result is a new ‘Packet’ WEP key**
- **The Packet WEP key changes per IV**

Message Integrity Check (MIC)

- **Prevents IV/WEP key reuse**
- **Prevents frame tampering**

Message Integrity Check (MIC)



Broadcast Key Rotation

- **Broadcast key is required in 802.1X environments**
- **Broadcast key is vulnerable to same attacks as static WEP key**
- **Broadcast key needs to rotate, as with unicast key**

Encryption Attack Mitigation

	WEP	TKIP	VPN
Bit Flipping		X	X
IV Reuse		X	X
AirSnort		X	X

Agenda

- **Drivers for Wireless Security**
- **Wireless Security in 802.11**
- **Vulnerabilities in 802.11 Wireless Security**
- **Technologies for Secure Wireless LANs**
- **What Lies Ahead**

What Lies Ahead

- **Ratification of IEEE 802.11i**
- **Adoption of TKIP encryption**
Certifiable vendor interoperability (WiFi)
- **AES encryption**
3DES successor

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION