Deploying Secure 802.11b WLAN's

Cisco.com

Eric Blaufarb
Market Development Manager
Cisco Systems

December 7th, 2002

The #1 Concern for Enterprise about Wireless: Security

Cisco.com

THE WALL STREET JOURNAL.

VOL. CCXXXVII NO. 25 WEPA ★★★ MONDAY, FEBRUARY 5, 2001 WSJ.com ★★★★

Hackers Can Penetrate Wireless Network

By JARED SANDBERG
Staff Reporter of THE WALL STREET JOURNAL

A group of respected security research-

ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the

nel." He adds that the IEEE is working on future versions that won't be vulnerable.

But Mr. Ennis says this type of attack

connect to networks using simple radio antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sold by many vendors but was popularized by Apple Computer Inc. under the name AirPort and is quickly being deployed in networks at a growing number of businesses, college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be deployed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the technology to allow latte guzzlers to noodle around the Internet.

The weakness is another reminder of the difficulty in implementing effective network security.

chief scientist at Zero Knowledge Systems Inc., a privacy-software firm in Montreal. Earlier versions of Wi-Fi were denied

...sses deploy wireless networks, connected to their internal conventional networks, without activating security measures such as WEP. One computer-security consultant in New York, who asked not to be identified, said he was able to access the computer network of his client, a major financial-services firm on Wall Street, while sitting on a bench across the street. Though he didn't have free range of the network, it was as if he walked through the building lobby, past a receptionist and sat down at one of the firm's computers.

Source: WSJ, 2/5/01

News Clip: Hackers hit the Streets

Cisco.com

- **"White Hat Hackers" search for vulnerable wireless LANs**
- **Over 900 companies identified in a single area**

Credit: KNTV San Jose

WEP Under Scrutiny
Weaknesses Unmasked

Cisco.com

University of California, Berkeley
Feb. 2001

University of Maryland
April 2001

Scott Fluhrer, Itsik Mantin, and Adi Shamir
July 2001

Focuses on authentication; identifies flaws in one vendor's proprietary scheme

Focuses on static WEP; discusses need for key management

Focuses on inherent weaknesses in RC4; describes pragmatic attacks against RC4/WEP

* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

- University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

General Sample
I-SEC

Cisco.com

- **I-SEC has been studying levels of wireless security over a number of weeks via a series of controlled drive rounds and has found the following results in its study:**
- **67% of wireless networks were not using WEP (wired equivalent privacy) encryption**
- **32% are still using default SSIDs (service set identifiers) and channel numbers**
- **even though 33% had put in place WEP encryption, this in itself is crackable**

IEEE 802.11 Tgi
Moving Quickly to fix WEP vulnerabilities

Cisco.com

- **TKIP – Temporal Key Integrity Protocol**
  - **Mitigate all know attacks/vulnerabilities to RC4/WEP**
  - **Best cryptologists in the industry within TGi**
  - **Does not require hardware replacement**
  - **Will provide interoperable solution**
- **Vendor specific TKIP becomes Wi-Fi Protected Access adopted throughout the industry expected Q2/Q3 2003**
- **Provides interoperable solution for all Wi-Fi vendors manditory requirement for Wi-Fi certification**

Wi-Fi Alliance
Security & Interoperability

Cisco.com

- **The Wi-Fi Alliance will enforce WPA (Wi-Fi Protected Access) based on final draft from Tgi**
- **Release paper on securing WLAN deployments with current RC4 WEP issues**
  - **All Wi-Fi certified vendors will be required to satisfy TKIP & vendor interoperability**
  - **www.wirelessethernet.org**

Vendor Interim Fixes
WEP Vulnerabilities

Cisco.com

Vendor	Product	Authentication Type	Vulnerability Mitigation	Encryption Enhancements
3 Com	AP-8000	802.1X/EAP-TLS	Fast Rekeying AP/Radius	40-bit/128-bit RC4
Agere*	AP-2000	802.1X/EAP-TLS	Fast Rekeying Radius	128-bit RC4 IV discard WEP PLUS
Cisco	1200	802.1X/EAP-TLS/LEAP	Fast Rekeying Radius	Hash, MIC, BKR or 40-bit/128-bit RC4 Pre-TKIP
Intel	2011/B	802.1X/EAP-TLS	N/A	40-bit/128-bit RC4
Proxim	Harmony 8550/51	Propritary/802.1X (near term)	Controller for Fast Rekey	40-bit/128-bit RC4
Symbol	AP-41X1	Propritary/Kerberos	ticket based certificate	40-bit/128-bit RC4

Vendor Support
Next Generation Security

Cisco.com

- All vendors in support of VPN architectures for WLAN security
- All vendors in support of WPA enhancements for encryption
- All vendors in support of 802.1X for authentication
- All vendors in support of one form of next generation EAP types:
  - EAP-TLS
  - EAP-TTLS
  - EAP-PEAP

Security Issues

Cisco.com

- **Summary of 802.11 RC4 WEP**
- **Vulnerabilities in 802.11 Wireless Security**
- **Technologies for Secure Wireless LANs**
- **Deploying Secure Wireless LANs**
- **What Lies Ahead**

WEP Encryption

Cisco.com

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

Wireless Security in 802.11 Summary

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

Security Issues

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

Authentication Vulnerabilities

Cisco.com

- **Wireless NIC is authenticated, not the user**
- **Unauthorized users can use authorized devices**
  - **Lost or stolen laptop**
  - **Disgruntled employees**

Statistical Key Derivation

Cisco.com

- **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**

Inductive Key Derivation

Cisco.com

- An attacker can derive the key by soliciting info from a wireless LAN
- Common methods
  - IV/WEP key replay
  - Frame bit flipping

IV/WEP Key Reuse Vulnerability

Cisco.com

- Attacker can send a known plaintext to an observable wireless client (i.e. via email)
- Attacker will ‘listen’ to wireless LAN, waiting to see predicted ciphertext
- Once attacker ‘sees’ the ciphertext, key stream is derived
- Key stream is valid only for the specific IV

Bit Flipping Vulnerability

- Attacker captures a frame from a wireless LAN
- The frame is modified by flipping bits
- Attacker predicts a high layer error
- Attacker waits for predicted error ciphertext
- The key stream is derived upon ‘seeing’ predicted ciphertext

802.11 Security Summary

- The security mechanisms in the 1997 802.11 specification are flawed
  - Open authentication
  - Shared key authentication
  - WEP
  - Will NOT secure your wireless LAN!!

Security Issues

Cisco.com

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

Today's Requirements for Secure WLAN

Cisco.com

- **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**

Technologies for Secure Wireless LANs

Cisco.com

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

Secure Authentication Requirements

Cisco.com

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

VPN over 802.11

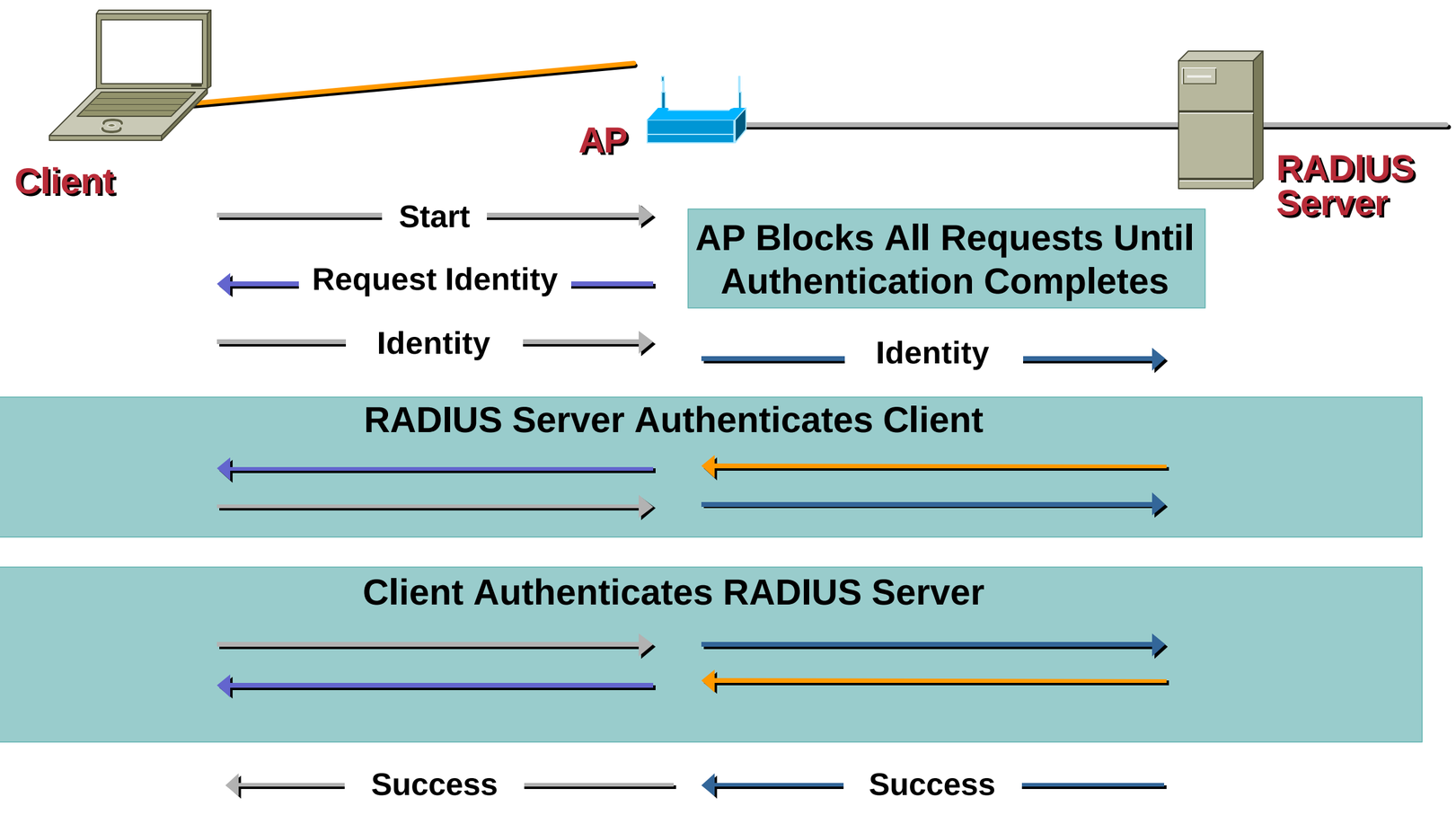
- **Two phase authentication**
  - **Device authentication via pre-shared key or PKI**
  - **User authentication via AAA server**
- **Mutual authentication**
- **Extensible user authentication types**

802.1X for 802.11

- **Layer 2 link layer support for Extensible Authentication Protocol (EAP)**
- **Framework to facilitate authentication between client, AP, and AAA server**
- **Extensible authentication algorithms**
  - **Password-based**
  - **PKI-based**
  - **Biometrics**
  - **More to come…**

802.1X Authentication Process

Cisco.com



EAP Authentication Types for Wireless LANs

Cisco.com

- **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-TLS Authentication

- **Client support**
  - **Windows 2000, XP**
  - **Clients require a local user or machine certificate**
- **Infrastructure requirements**
  - **EAP-TLS supported RADIUS server**
    - **Cisco ACS, Cisco AR, MS IAS**
    - **RADIUS server requires a server certificate**
  - **Certificate Authority Server**
    - **Windows 2000 Server**

Hybrid Authentication's in Development Two new EAP types

- **EAP-TTLS**
  - **Server side authentication with TLS**
  - **Client side authentication with legacy authentication types (CHAP, PAP, etc)**
  - **Developed by Funk & Certicom**
- **EAP-PEAP**
  - **Server side authentication with TLS**
  - **Client side authentication with EAP authentication types (EAP-GTC, EAP-MD5, etc)**
  - **Developed by Microsoft, RSA, Cisco**

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**

Strong Encryption

Cisco.com

- **Temporal Key Integrity Protocol (TKIP) aka WPA**
  - **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

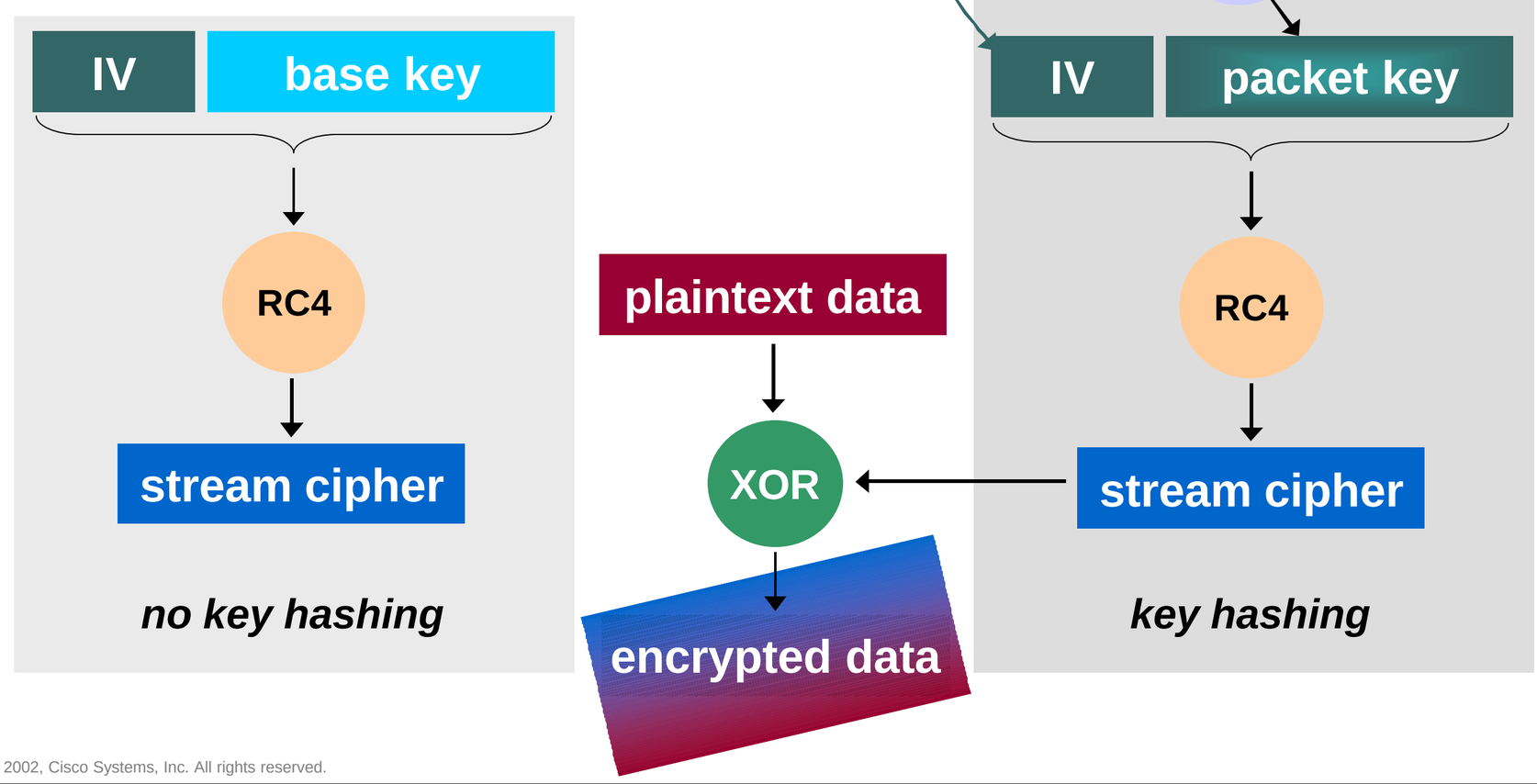
Cisco.com

- **Cisco offers a pre-standards implementation of TKIP**
- **Per packet keying**
- **Message integrity check**
- **Broadcast key rotation**

WEP Key Hashing

Cisco.com

Because packet key is hash of IV and base key, IV no longer gives insight into base key



Message Integrity Check (MIC)

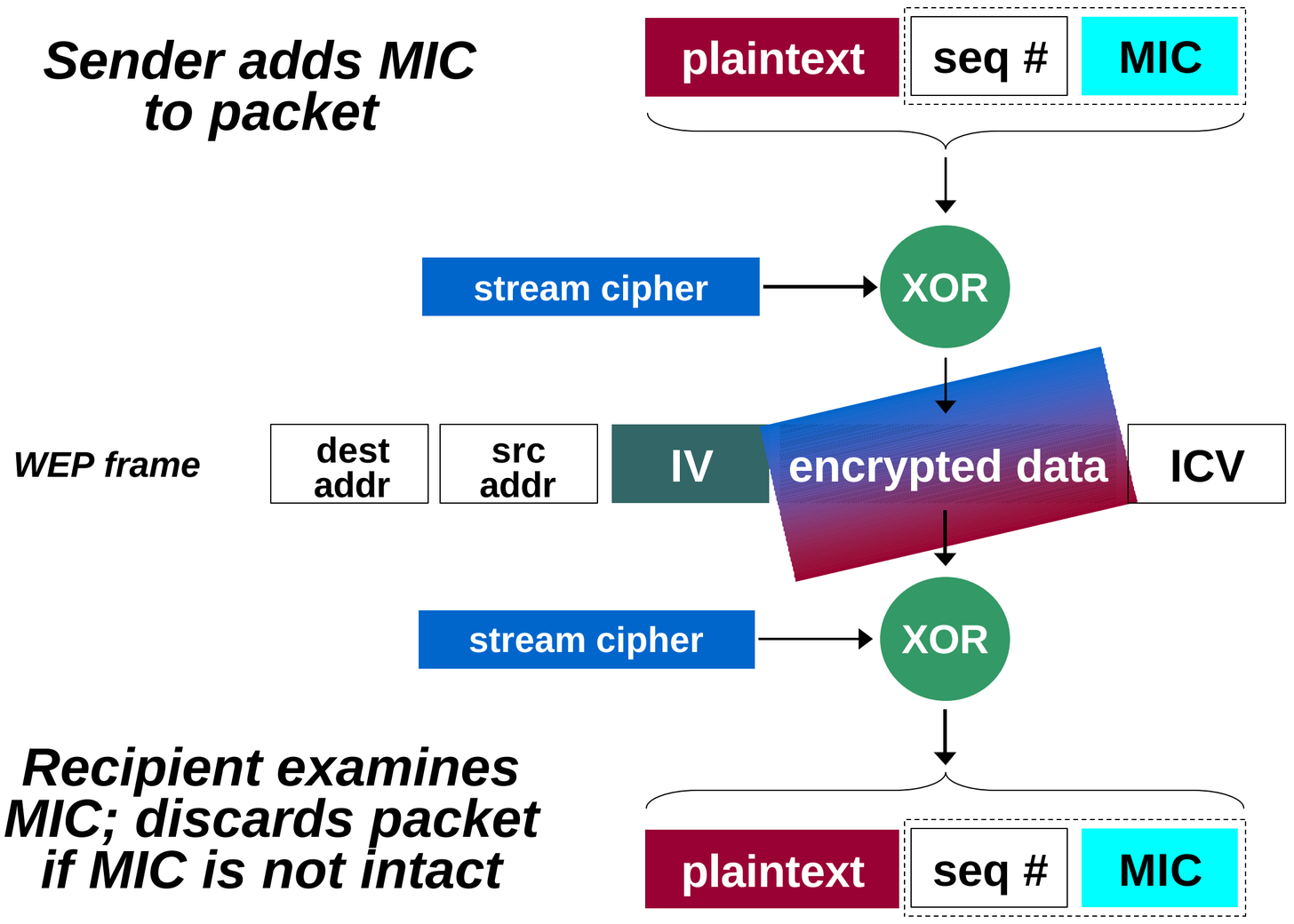
Cisco.com

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

Message Integrity Check

Cisco.com

Sender adds MIC to packet



Recipient examines MIC; discards packet if MIC is not intact

Broadcast Key Rotation

Cisco.com

- **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	WPA	VPN
Bit Flipping		X	X	X
IV Reuse		X	X	X
AirSnort		X	X	X

Security Issues

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

What Lies Ahead

- **Ratification of IEEE 802.11i**
- **WPA in Q2/Q3 2003**
  - **Certifiable vender interoperability Wi-Fi**
- **AES encryption**