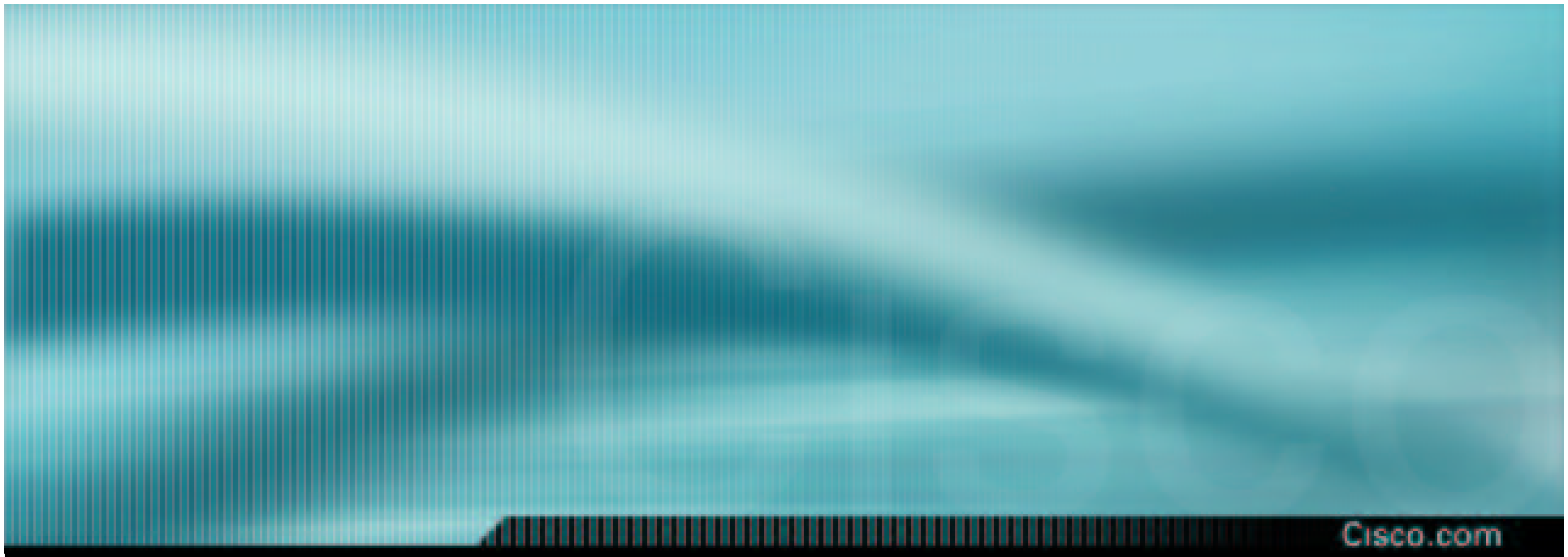


Wireless LAN Security: Ready for Primetime

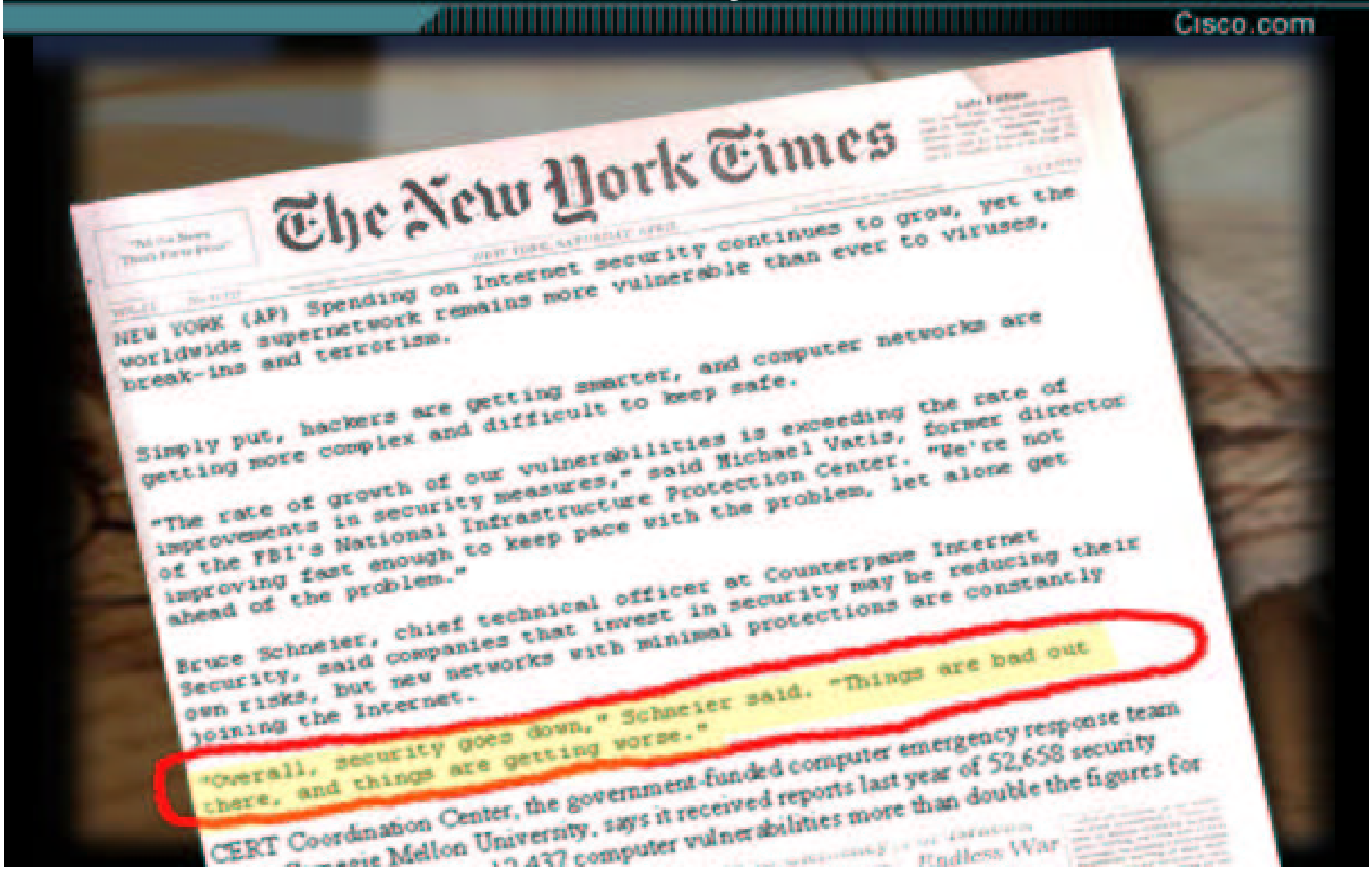
Agenda

- Security Concerns
- Basic security architectures
- How to address security concerns
- Standards update

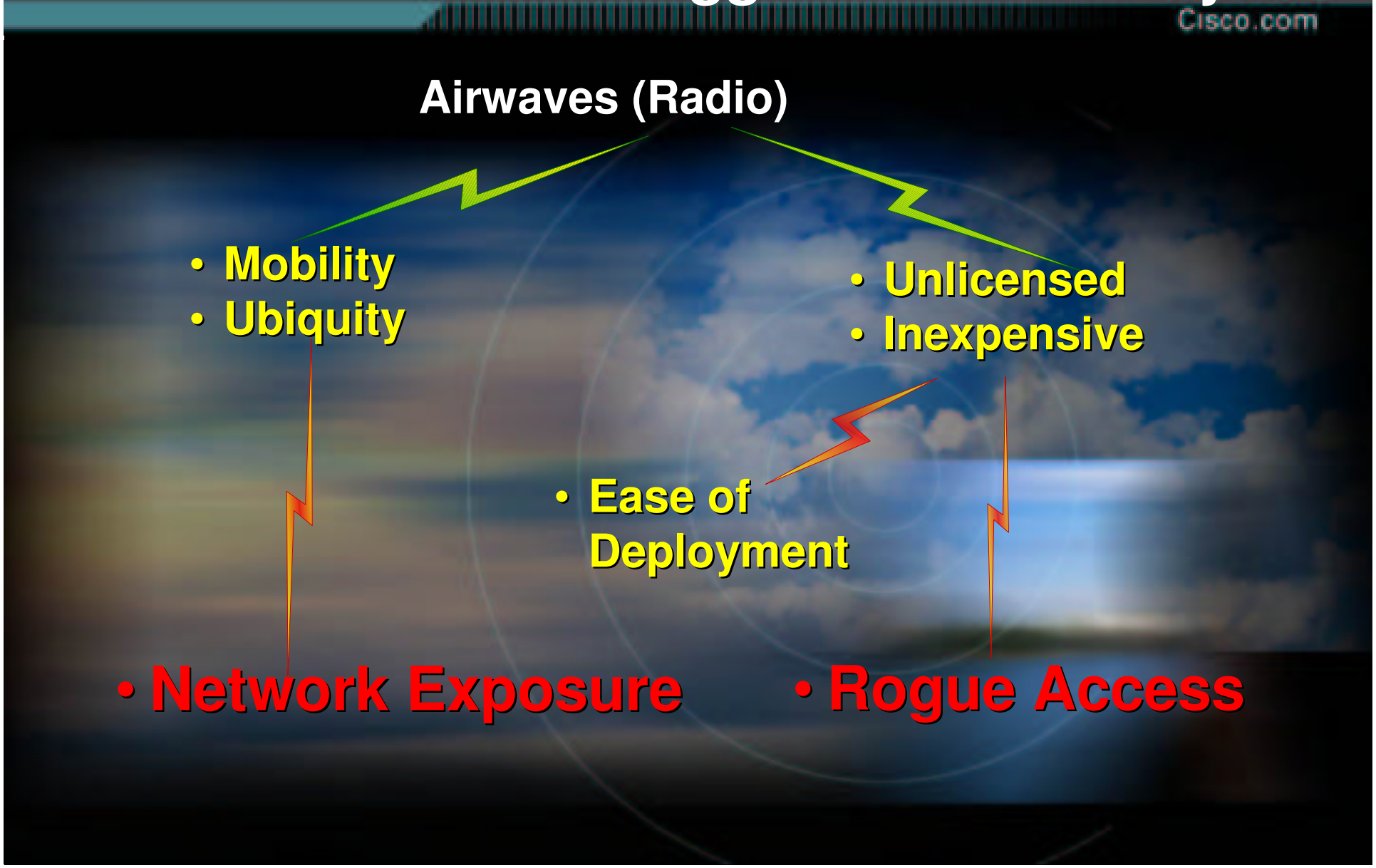
Building a Security solution is a journey, not an end game

- Security was an obstacle, but significant strides have been made!
- Not all security architectures are the same
- Enterprises want flexible, hassle-free, security administration and management

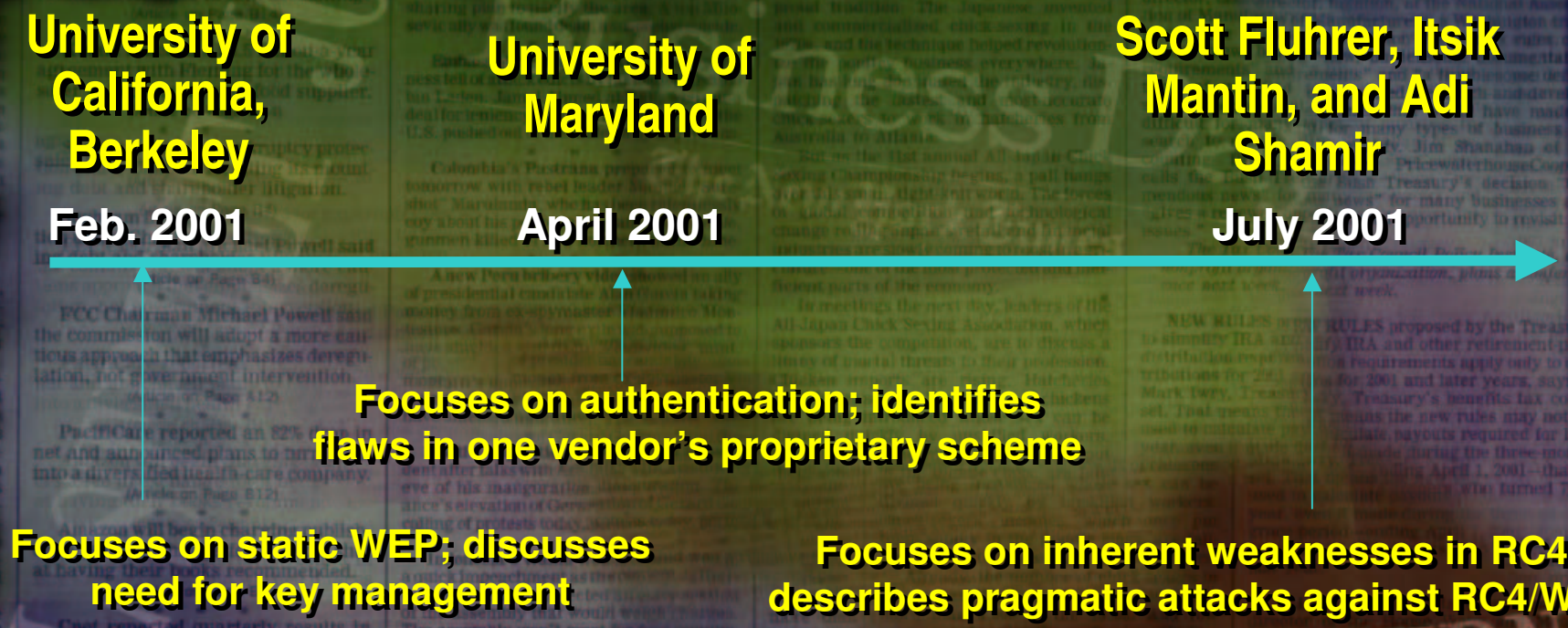
The #1 Concern for Enterprise about Wireless: Security



Problem: The Strength of Wireless LANs Also Creates Their Biggest Vulnerability



Papers on WLAN Security …



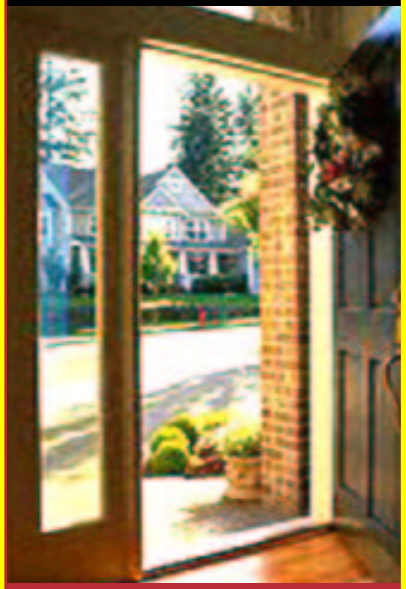
* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

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

First Generation WLAN Security : Not appropriate for Enterprise Deployment

No Security

No WEP and Broadcast Mode



Public Access

Basic Security

Wi-Fi 40-bit, 128-bit Static WEP

Telecommuter and Small Business

Enhanced Security

Dynamic Key Management System, Mutual Authentication, and 802.1x via EAP

Mid-Market and Enterprise

VPN Security

End-to-end security using VPN

Special Apps./ Business Traveler

Issues with First Generation 802.11 Security

- Shared, static WEP keys
- If client adapters are lost or stolen, large-scale re-keying is required
- Lack of integrated user administration
- In 802.11, authentication and encryption are an option (not mandatory)

Early WLAN applications were primarily in the vertical industries (e.g., bar code scanning) and security was not the major driver. Mobility was.

Recommended use of WLAN Security Profiles

Enhanced Security

Dynamic Key Management System, Mutual Authentication, 802.1x via EAP, and 802.11 TKIP

Mid-Market and Enterprise

VPN Security

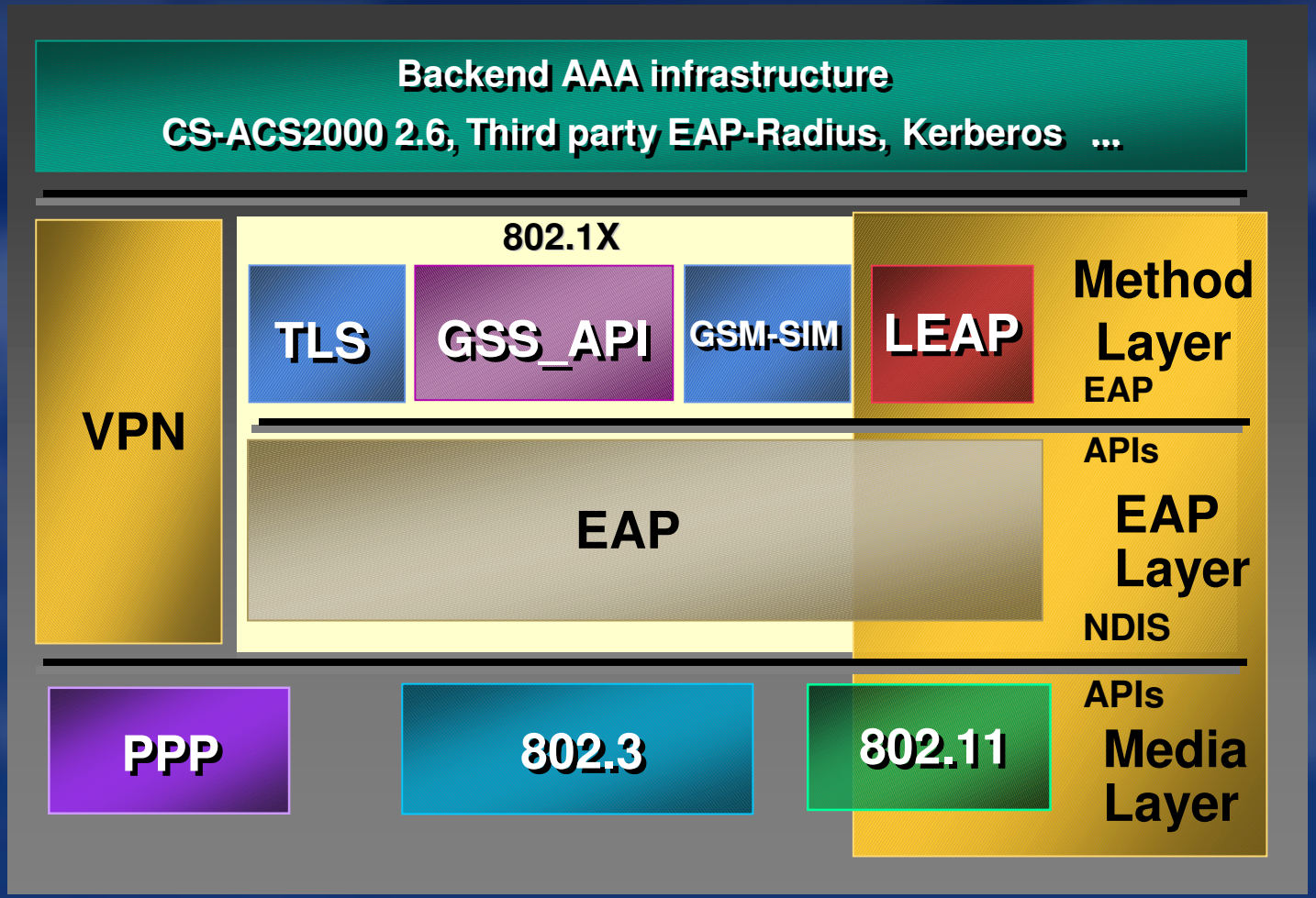
End-to-end security using VPN

Special Apps./ Business Traveler

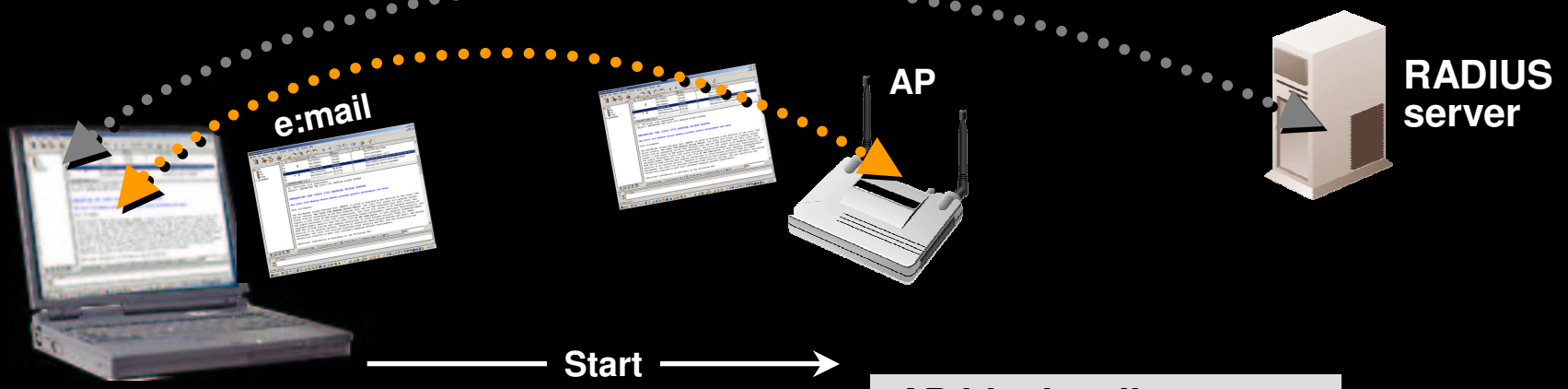
Advantages of 802.1X Framework

- Centralized, scalable, user based authentication
- Mutual authentication
- Various authentication types

IEEE 802.1X as Framework for Security



802.1X Authentication Process



RADIUS server authenticates client

Client authenticates RADIUS server

Derive key

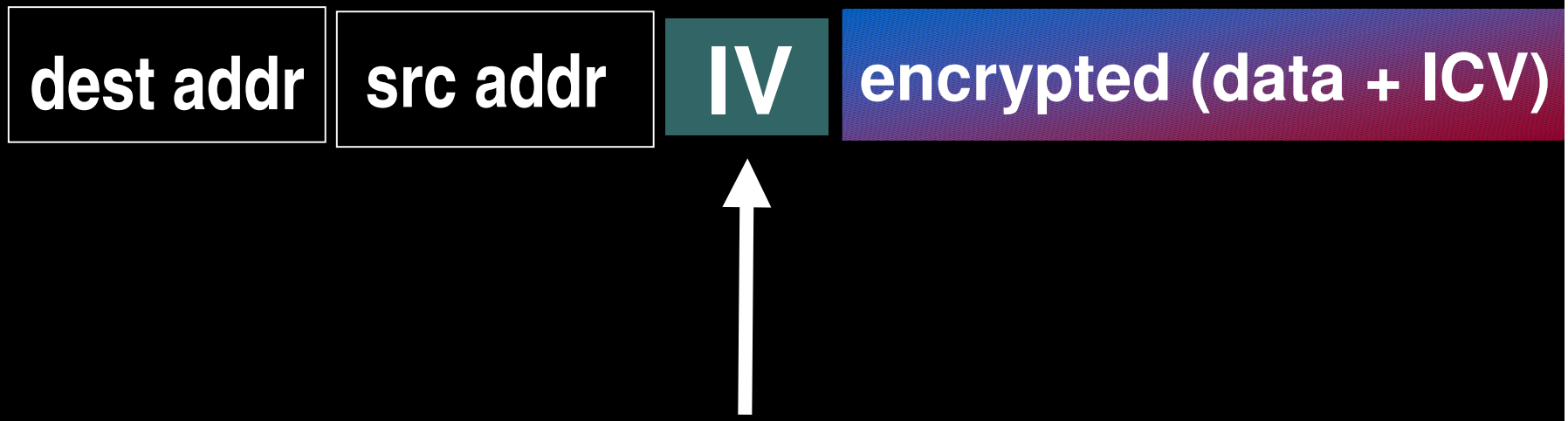
Derive key

The End User's Experience is the Same: Single Sign-On

General 802.11b Packet Structure

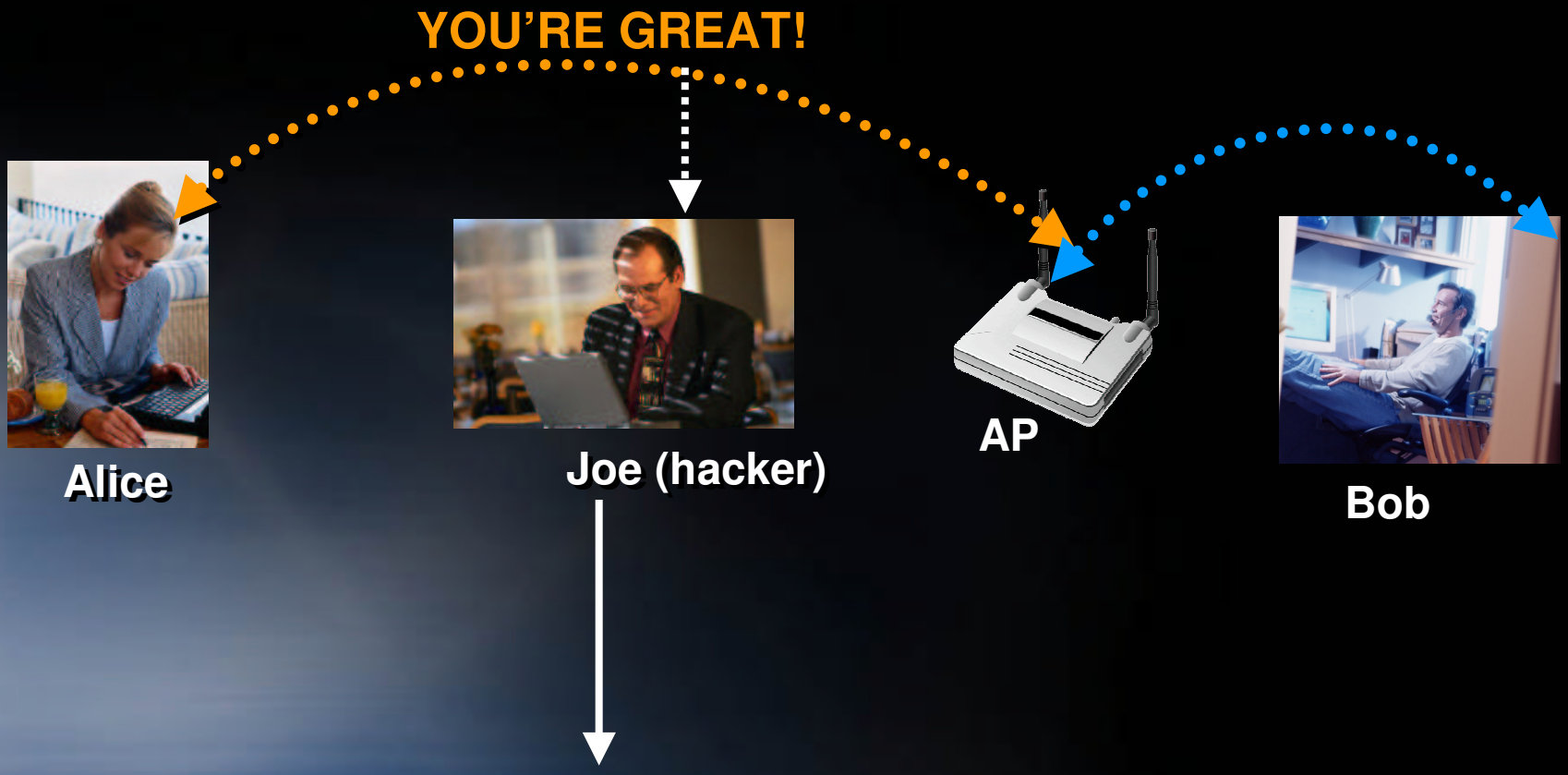
Cisco.com

WEP frame



- Initialization Vector sent in the clear
- Concatenated with base key
- IV collision introduces vulnerabilities

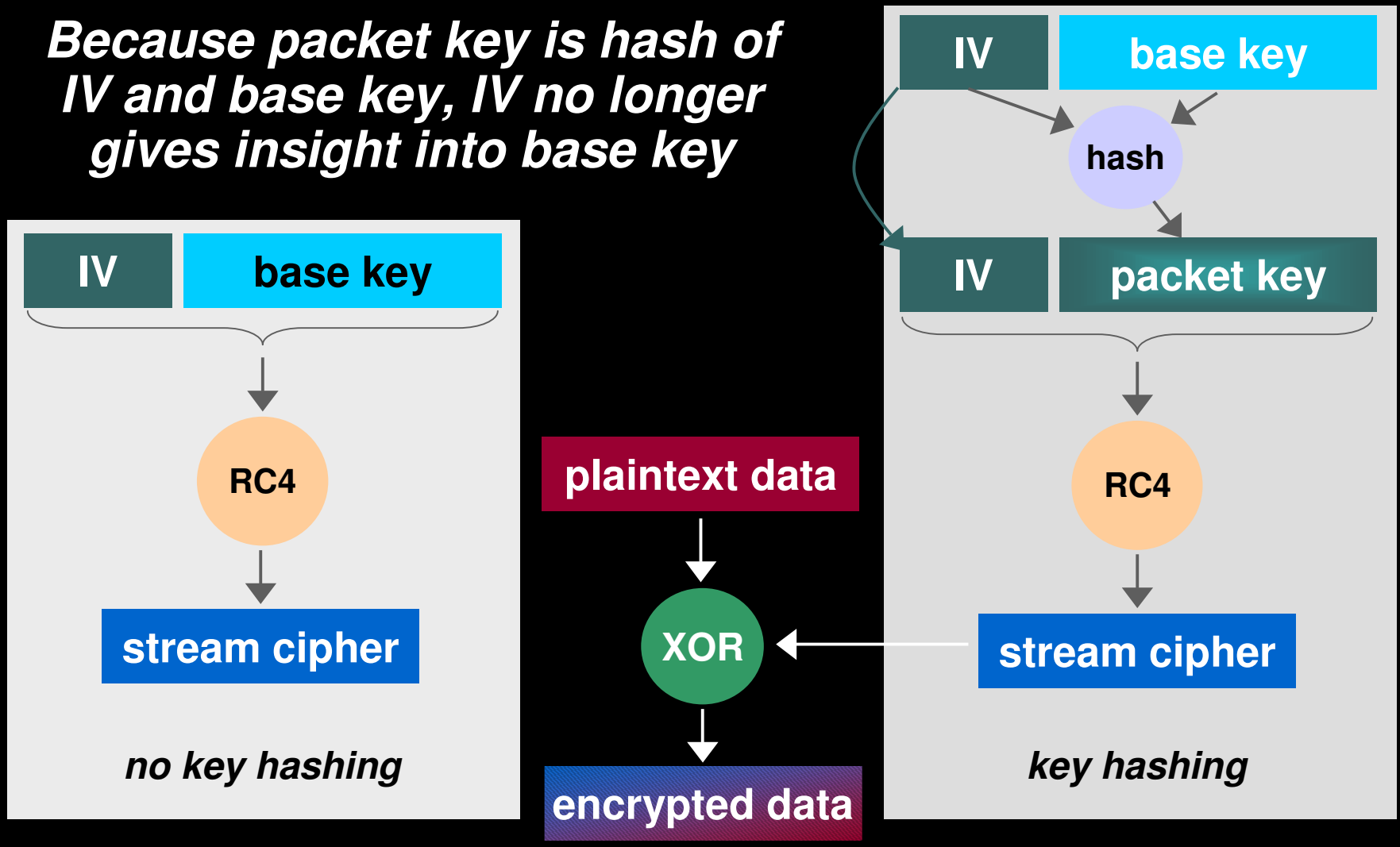
Scenario #1: Passive WEP Attacks



Hacker passively listens and captures enough packets to break WEP key and hence, packet

Solution #1: Change Encryption Keys for Every Packet

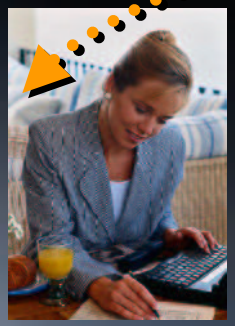
Because packet key is hash of IV and base key, IV no longer gives insight into base key



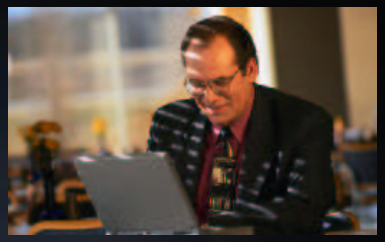
Scenario #2: Bit-Flipping and Replay Attack

Alice -> Bob, YOU'RE GREAT!

Alice -> (Joe) -> Bob YOU'RE AWFUL!



Alice



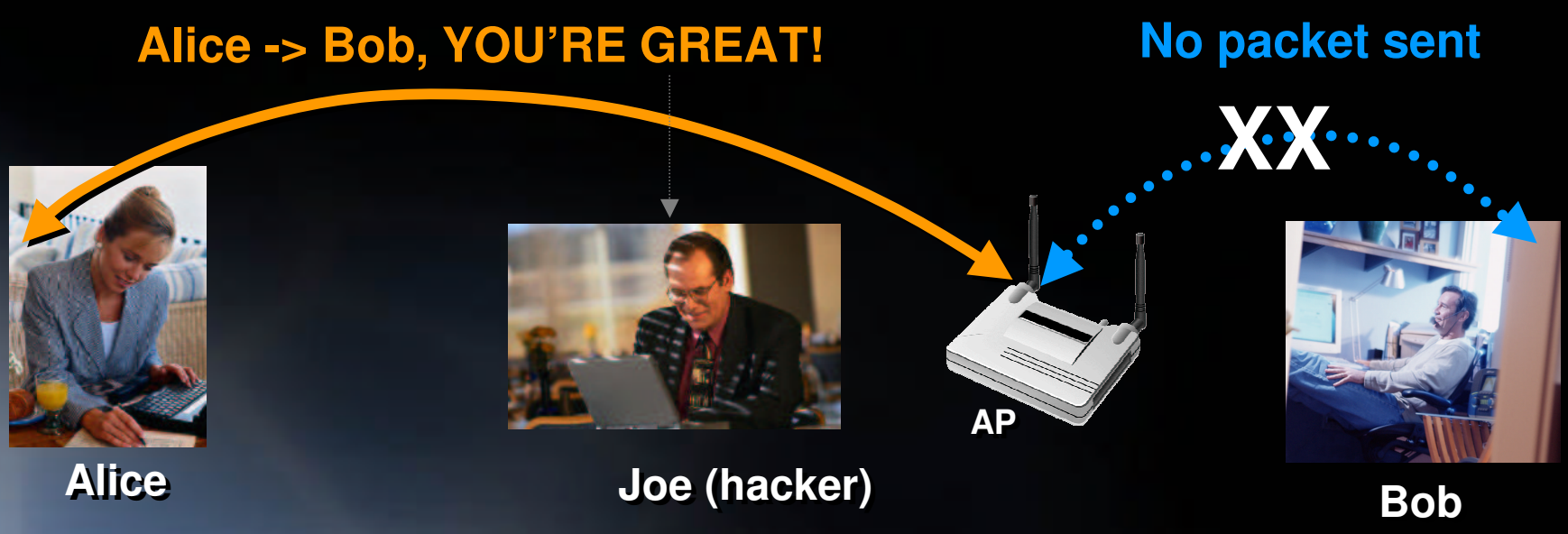
Joe (hacker)

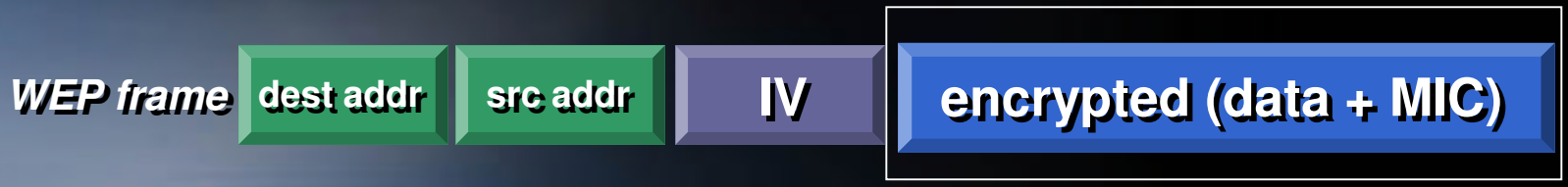
AP

Bob

Packet modified by the hacker gets through to Bob as legitimate packet due to WEP linear CRC

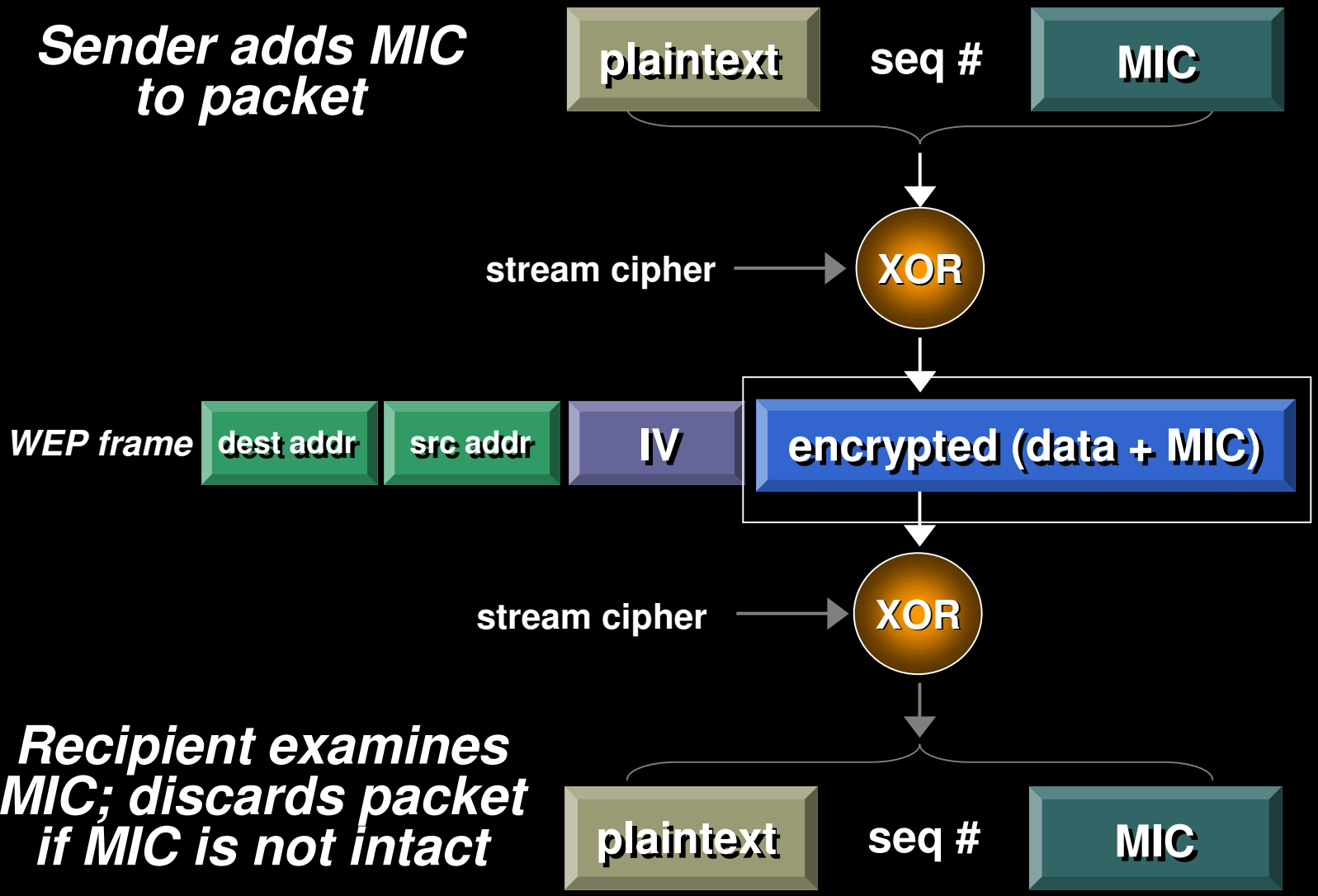
Solution #2: Message Integrity to Fix Bit-Flipping and Replay Attack





Packet is dropped by AP
because of invalid signature (MIC)

Solution #2: Message Integrity Check (MIC)



802.11 Task Group i Security Recommendations

- Mutual Authentication
- Dynamic Session Key
- Message Integrity Check (MIC)
- Temporal Key Integrity Protocol (TKIP)
  - Per-packet Key Hashing
  - Initialization Vector Sequencing
  - Rapid Re-Keying
- Future
  - Stronger encryption schemes such as AES
  - Authentication/security for control and management frames

Summary: Wireless LAN Security

Cisco.com

- Traditional 802.11 security does not address all security issues
- 802.1x for 802.11 addresses many issues and provides a flexible, extensible framework
- Enterprise solutions exist that mitigate WEP key vulnerability to attacks
- Interoperable authentication solutions based on 802.1X available today. However, key management solutions are vendor-specific.
- 802.11 Task Group i recommendations will mitigate most attacks on WEP based implementations. However, do your risk assessment in your application environment.
- Stronger WLAN encryption schemes, such as AES, are expected in the near future

Comprehensive White Paper

Cisco.com

- http://www.cisco.com/warp/customer/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm

NetStumbler Demo

- **http://www.netstumbler.com/**

EMPOWERING THE
INTERNET GENERATION℠