Can Wireless LANs Really Be Secured?

Jim Ransome, Ph.D., CISSP, CISM

Senior Director, Secure Wireless Engineering

InfoSec Canada, Toronto, ON, June 14, 2007

About the Speaker

- Ph.D. in information systems specializing in information security
  - Developed/tested a converged wired-wireless network security model for dissertation
- Graduate certificates in international business and international affairs
- Adjunct Professor for a masters-level information security curriculum
- Published 4 books (Elsevier - Digital Press):
  - Operational Wireless Security
  - VoIP Security
  - IM Security
  - Business Continuity and Disaster Recovery for InfoSec Managers
- Certified Information Security Professional (CISSP), Manager (CISM)
- 10 years senior corporate executive information and physical security
- 23 years government service: National Lab computer scientist/national security analyst, NCIS federal special agent, retired naval reserve intelligence officer, former marine corps sergeant

#1 Wireless LAN Concern: Security

Vulnerabilities:

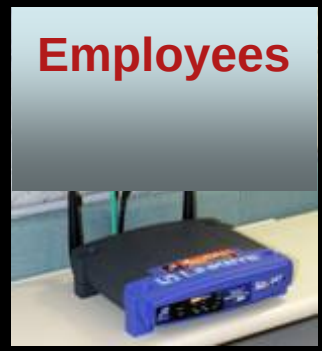

THE WALL STREET JOURNAL.

MONDAY, FEBRUARY 5, 2001 WSJ.com

Hackers Can Penetrate Wireless Network

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

Hackers


Employees

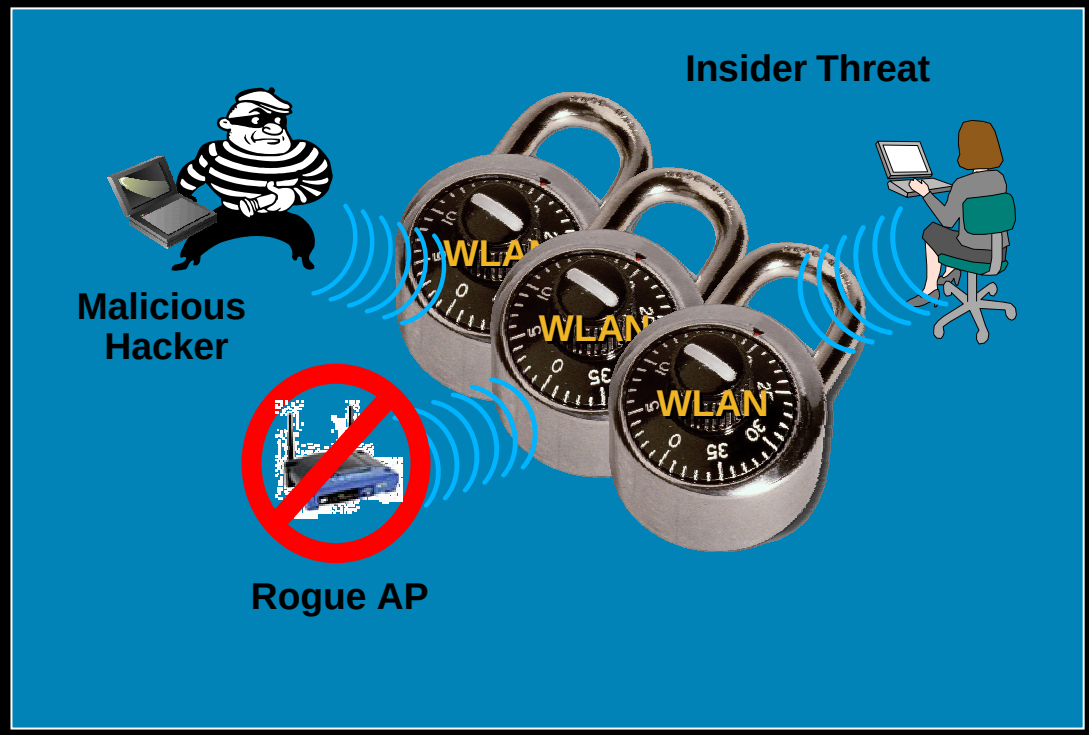

"War Driving"

Lessons:

- Your network is vulnerable if WLAN security is not properly installed and on
- Employees will install WLANs on their own, which comprises the security of your entire network
- Strong security policies must be in place to maintain WLAN security and perform intrusion detection activities

Robust Wireless LAN Security is Needed

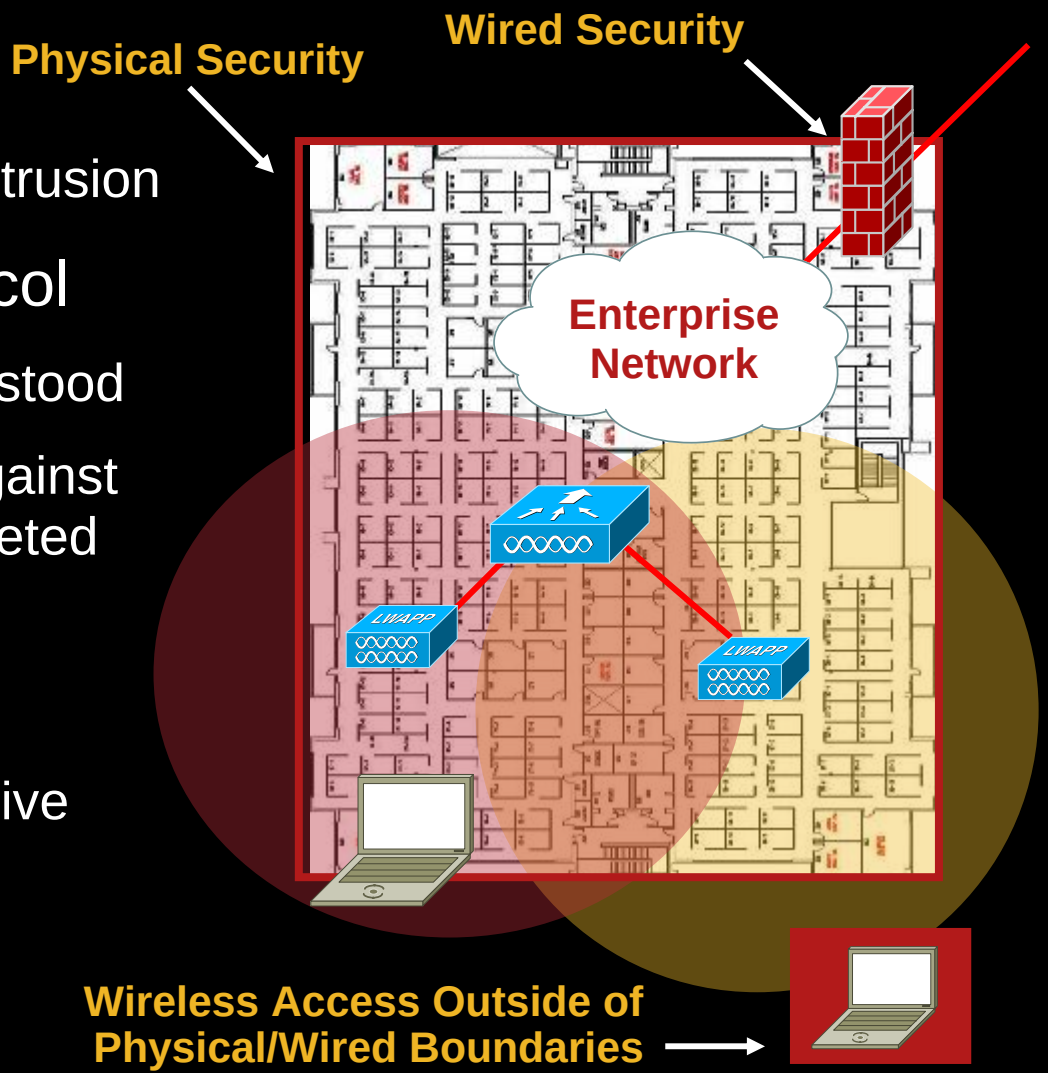
- Each user must be individually authenticated via a unique identifier
- Data must remain uncorrupted throughout the sending-and-receiving transmission process



- Security administration should be scalable, problem-free and not increase the burden on the IT staff
- Unauthorized users, rogue access points and network attacks must be detected and mitigated

Why are Wireless LANs Prone to Attack?

- "Open air"
  - No physical barriers to intrusion
- Standard 802.11 Protocol
  - Well-documented, understood
  - Most common attacks against WLAN networks are targeted at management frames
- Unlicensed
  - Easy access to inexpensive technology



IEEE 802.11 WLAN Security Vulnerabilities

- WLAN Sniffing/War Driving
- Encryption Vulnerabilities

  WEP
- Denial of Service (DoS) Attacks

  Using 802.11 de-authentication/disassociation frames, RF jamming, etc.
- Authentication Vulnerabilities

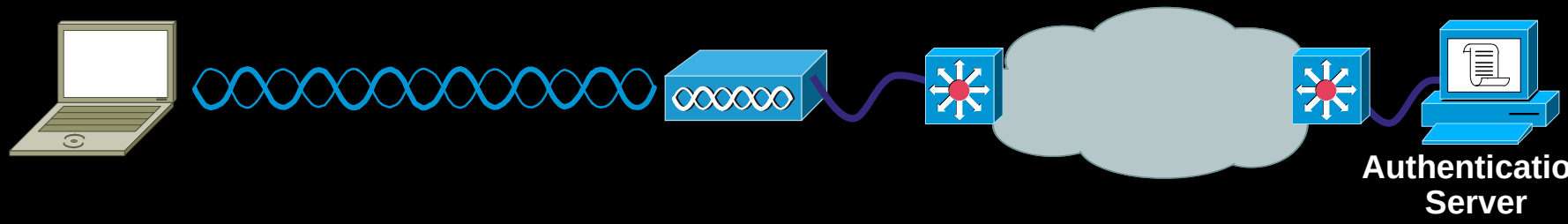
  Dictionary attacks, MITM attacks
- Address Spoofing

  MAC-address spoofing and IP address spoofing (both hostile/outsider attacks and insider attacks)

IEEE 802.11i WLAN Security Improvements

- IEEE 802.11i is an IEEE 802.11 Subcommittee Responsible for WLAN Security Improvements
- Key Components of IEEE 802.11i Standard
  - EAP/802.1x framework-based user authentication
  - TKIP: Mitigate RC4 key scheduling vulnerability and active attack vulnerabilities
  - IV Expansion: 48-bit IVs
  - Key Management: Isolate encryption key management from user authentication
  - AES: Long-term replacement protocol for RC4 (WEP)
- WPA is the Wi-Fi Alliance (WFA) inclusion of 802.11i Security Recommendations

802.11i/WPA Authentication and Key Management Architecture



802.11

UDP/IP

802.1X (EAPoL)

RADIUS

EAP

EAP-TLS

802.11i Specified

WPA Specified

IEEE standards provide device interoperability
WPA guarantees a degree of system interoperability

Protected Access

What are WPA and WPA2?

- Authentication and encryption standards for Wi-Fi clients and APs
- 802.1X authentication
- WPA uses TKIP encryption
- WPA2 uses AES encryption

Which should I use?

- Go for the Gold!
- Silver, if you have legacy clients
- Lead, if you absolutely have no other choice (i.e. ASDs)

Gold

WPA2/802.11i
- **EAP**
- **AES**

Silver

WPA
- **EAP**
- **TKIP**

Lead

dWEP (legacy)
- **EAP/LEAP**
- **VLANs+ACLs**

WiFi Protected Access (WPA)

- Developed to Replace WEP, Improve authC
- Encryption Key Management: TKIP
  - Doubled IV to 48-bits
  - Better protection from replay IV collision attacks
  - Protects against key-recovery attacks (AirSnort)
- Message Integrity: Michael
  - Protects against forgery attacks
- Authentication
  - 802.1x and EAP
  - Mutual authentication
  - So you don't join rogue networks and give up your credentials

Mode	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**

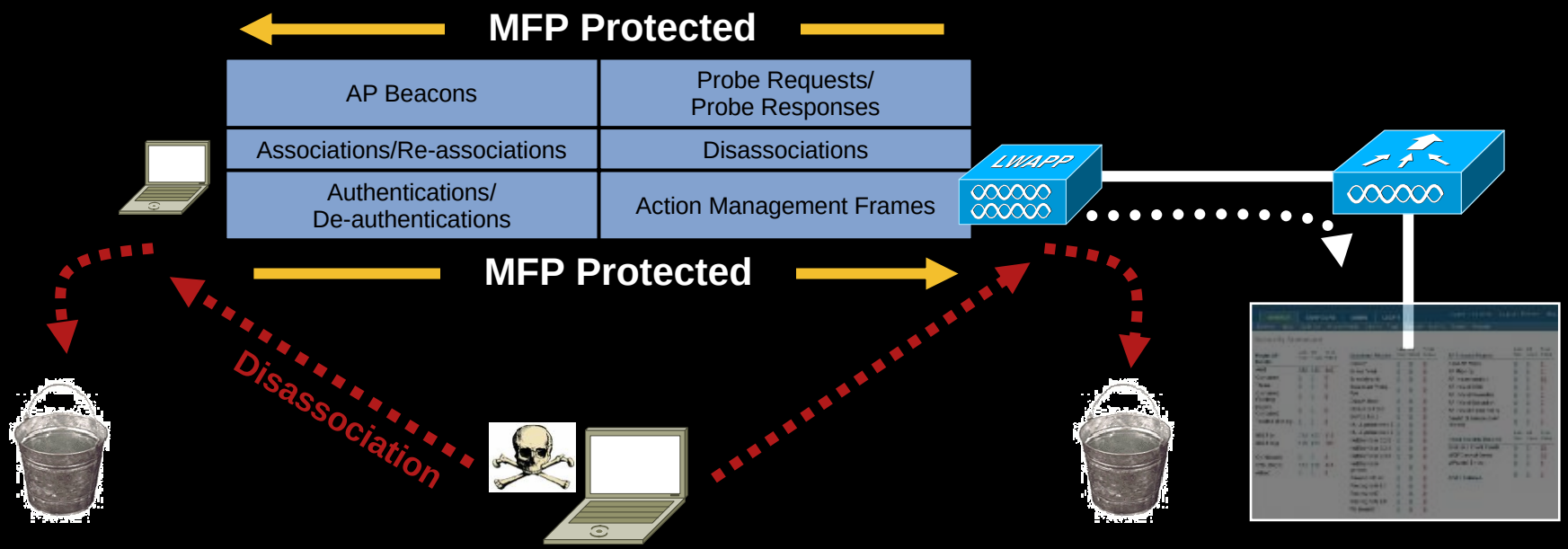
Management Frame Protection (MFP)

Problem

- Wireless management frames not authenticated, encrypted, or signed
- A common vector for exploits

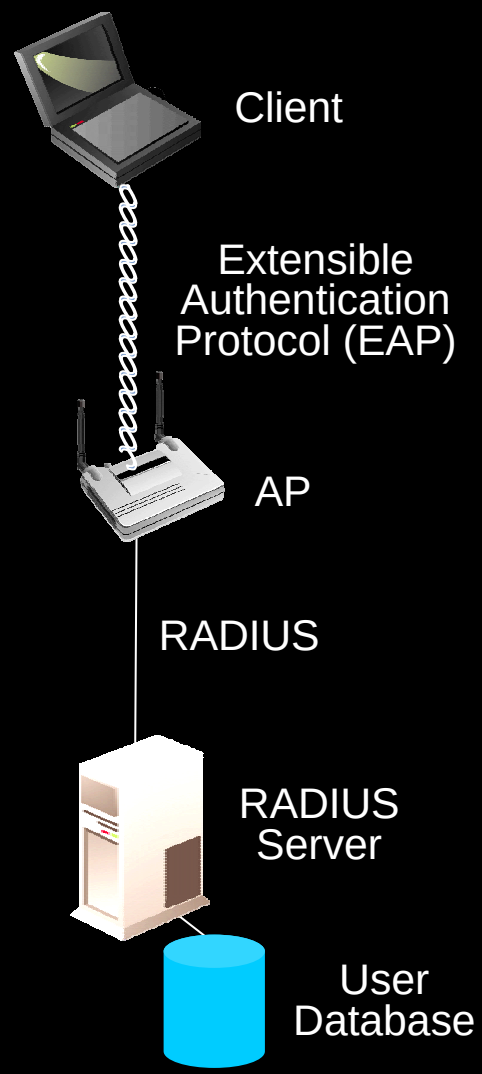
Solution

- Insert a signature (Message Integrity Code/MIC) into the management frames
- Clients and APs use MIC to validate authenticity of management frame
- APs can instantly identify rogue/exploited management frames



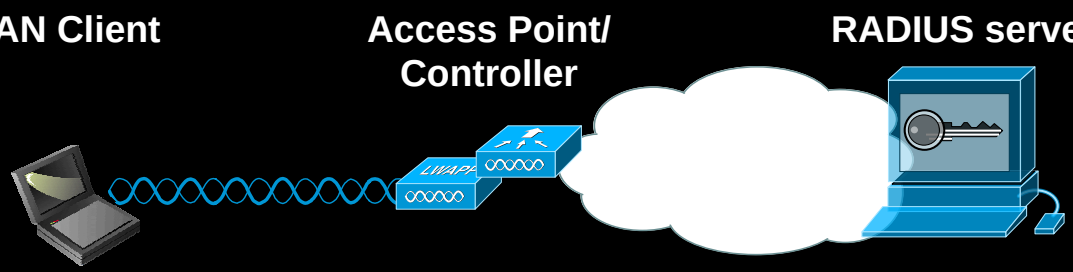
802.1X Authentication Overview

- IEEE 802.11 Task Group i Recommendation for WLAN Authentication
- Supported by Cisco Since December 2000
- Extensible and Interoperable – Supports:
  - Different EAP authentication methods or types
  - New encryption algorithms, including AES as a replacement for RC4
- Key Benefits
  - Mutual authentication between client and authentication (RADIUS) server
  - Encryption keys derived after authentication
  - Centralized policy control, where session timeout triggers re-authentication and new key

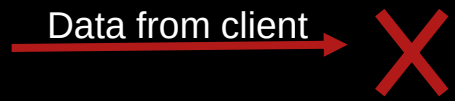


How Does Extensible Authentication Protocol (EAP) Authenticate Clients?

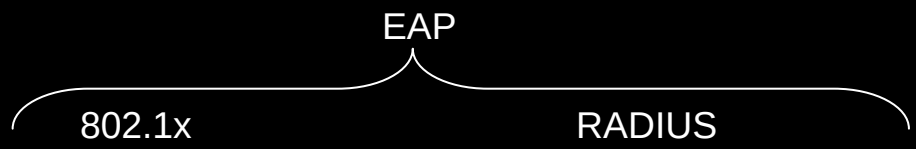
Client associates



Cannot send data until…

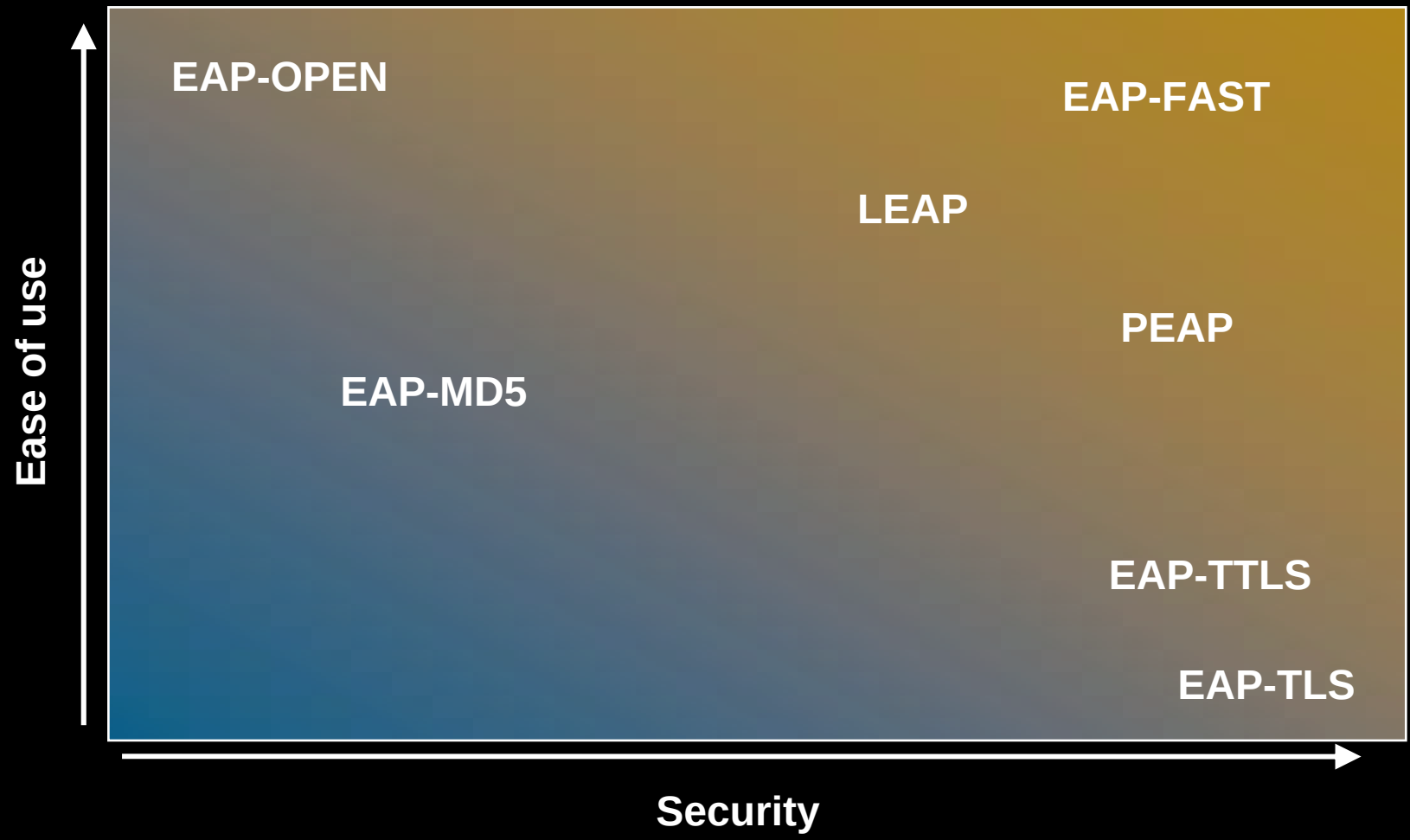


…EAP authentication complete



Client sends data

EAP Mechanisms



For display purposes only
Cisco IT recommends you undertake your own formal security requirements analysis

Wi-Fi Security Myths

No Wi-Fi = Good Security

WRONG!

- A single rogue access point creates enormous risk
- Traditional security measures (firewall, wired IDS/IPS, VPNs, NAC, etc) don't address
- Perpetrated unknowingly by your own employees or contractors

A handheld walk-around survey is sufficient (i.e. AirMagnet)

WRONG!

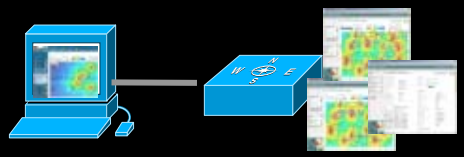
- Would you only turn on your firewall periodically?
- Not practical for branch or remote offices with no local IT personnel
- Laborious and expensive

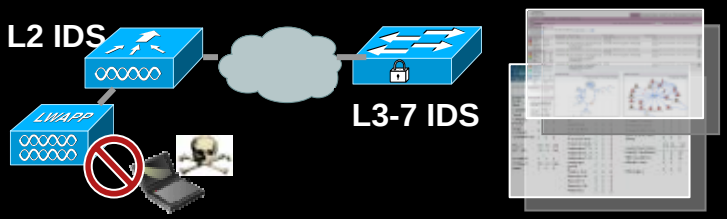
I use 802.11i, WPA or VPN, so my network is secure

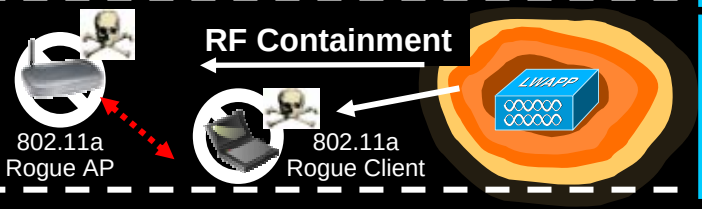
WRONG!

- Only protects authorized clients and infrastructure
- No impact on unauthorized infrastructure (i.e. rogue APs) or unauthorized connections (i.e. ad hoc networks)

Building on 802.11i: A Unified Wireless Security Approach to End-to-End Security







Fine-grained Mapping and Authentication

Location services enable precise mapping of clients and threats, allowing fine-grained authentication and quick removal

Wired IDS Integration

Unified wired and wireless IDS ensures malicious wireless clients are disconnected from the network

Wireless Endpoint Compliance

NAC prevents wireless endpoints from introducing viruses, spyware, malware, etc.

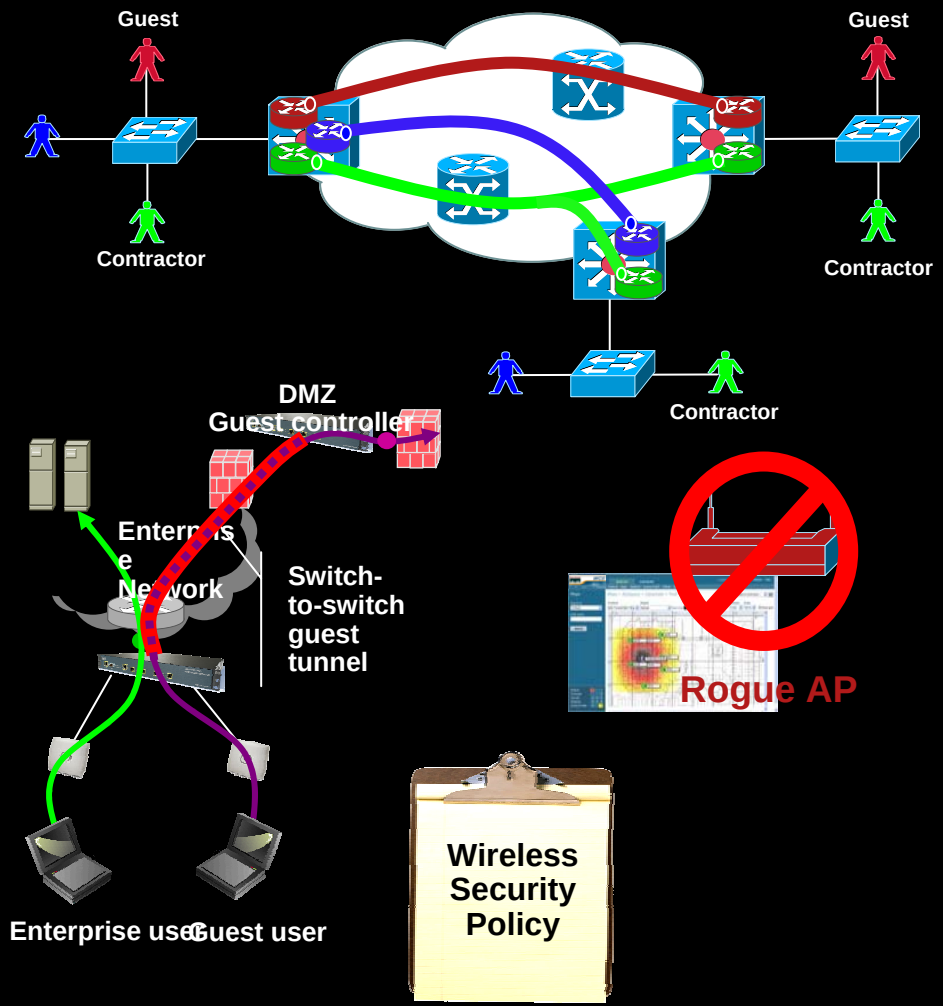
Wireless IDS/IPS

Comprehensive wireless threat identification and over-the-air prevention

Offsite Endpoint Protection

IPS detects and prevents offsite wireless threats such as ad hoc networks

Building on 802.11i: A Unified Wireless Security Approach to End-to-End Security



Network Segmentation

Key to providing Guest Access by controlling and prioritizing access to business resources

Wireless Network Location Services

Quick Location of rogue access points and other wireless threats

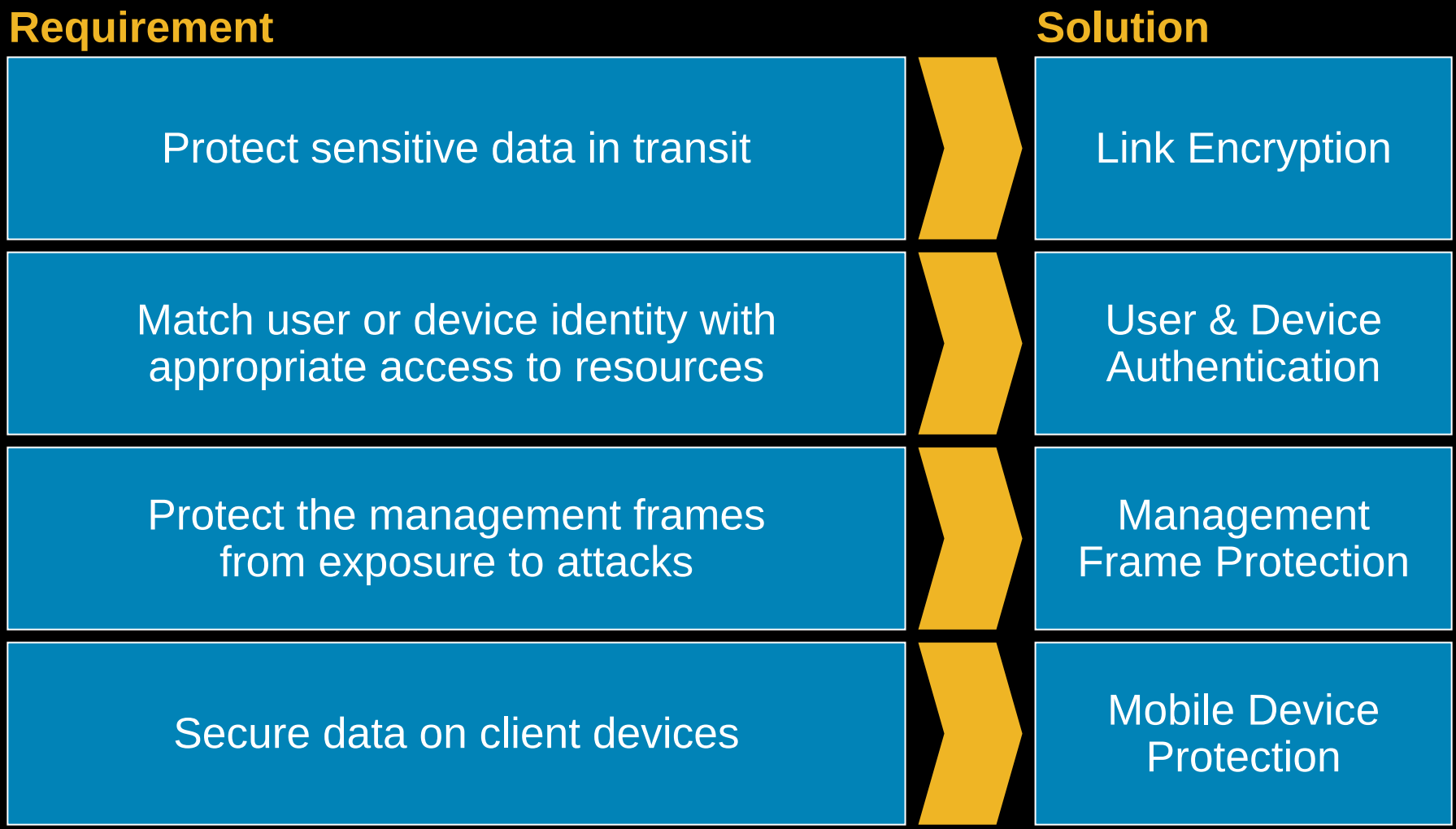
Guest Services

Path Isolation/Guest traffic never mixes with enterprise traffic

Wireless Security Policy

Wireless client connection policy enforcement

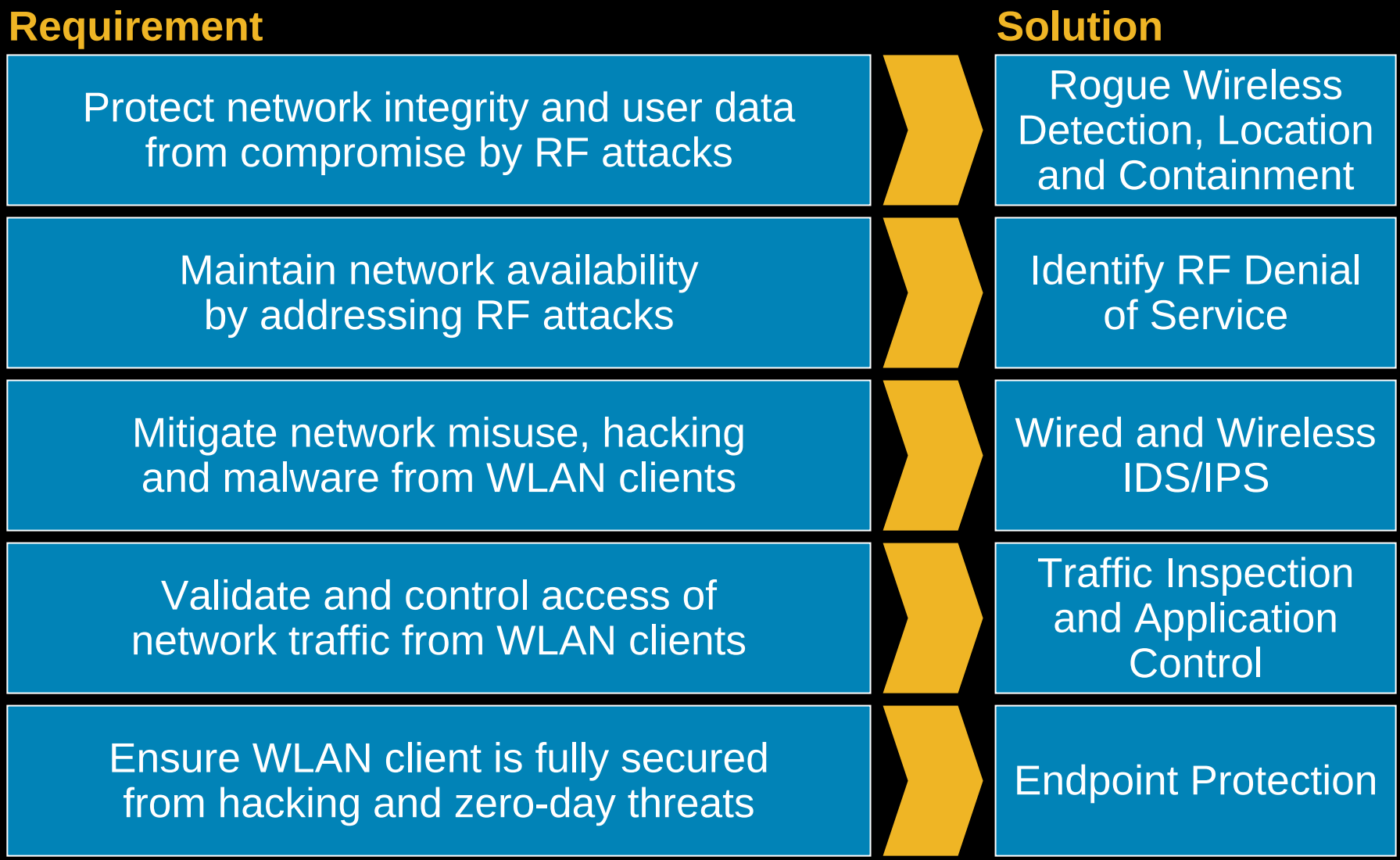
Pulling It All Together: Securing Wireless LAN Confidential Communications



Pulling It All Together: Wireless LAN Operational Control & Policy Management

Requirement	Solution
Determine what is on the network and identify threats	Wireless Security Management
Establish granular policies to minimize risks introduced by users	Wireless Client Connection Policies
Identify who is on the network and enforce granular policies	Network Admission Control
Segregate compliant users and their traffic from non-compliant users	Network Segmentation
Increase security for higher risk locations	Location Based Admission Control

Pulling It All Together: Wireless LAN Threat Control & Containment



Wireless LAN Security Checklist Summary

Endpoint Protection

Keep Clients Safe

- Strong Mutual Authentication
- Strong Encryption
- True Wireless IPS
- Adaptive Client Policies
- Mobile Device Protection

- 802.1X (EAP)
- WPA2 (AES) or WPA (TKIP)
- Management Frame Protection
- Wired/Wireless
- Thin-client applications, Third-party file encryption & remote device locking, User authentication

Admission Control

Keep Clients Honest

- Network Admission Control
- Guest Access

- Network Admission Control (NAC) for wired and wireless
- Wired/Wireless IPS
- Fine Grained
- Network Segmentation
- Guest: Integrated captive portal w/traffic tunneling

Anomaly and IDS/IPS

Protect The Network

- Rogue AP Detection and Containment
- Multilayer Client Exclusions
- Enforceable Policies

- Wireless IDS
- Wireless Network Locations Services/Rogue Detection/Containment
- End-to-end Wired/Wireless Enforceable Security Policies
- Radio Resource Management - Real-Time RF Management