Wireless LAN Security, Policy and Deployment Best Practices

- BRKEWN-2021
- Israel Gonzalez, Security Solutions Architect
- CCIE#15732
Agenda

Security Standards
- Strong Encryption
- Strong Authentication

User-Policy and Device Identification
- Wireless Policy Using ACS and ISE
- Per User VLAN, ACL and QoS
- Device Fingerprinting

Rogue Management, Attack Detection and Threat Mitigation
- Rogue Classification and Containment
- Adaptive wIPS Monitor Mode and ELM
- MFP and Wired IPS Integration
Strong Authentication and Encryption
Authentication Evolution

- MAC Address Authentication
- WEP
- 802.1x / Dynamic WEP
- WPA/WPA2
WPA/WPA2 Breakdown

**WPA**
- A Snapshot of the 802.11i Standard
- Commonly Used with TKIP Encryption

**WPA2**
- Final Version of 802.11i
- Commonly Used with AES Encryption

**Authentication Mechanisms**
- Personal (PSK) – Home Use
- Enterprise (802.1x/EAP) – Office Use
About EAP

- Extensible Authentication Protocol (EAP)

- It is an authentication framework over data link layer
- An authentication framework which supports multiple authentication methods.
- EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.
EAP — Protocol Flow

Authentication conversation is between client and Authentication Server
EAP Authentication Types

- **Tunneling-based** - Common deployments use a tunneling protocol (EAP-PEAP) combined with an inner EAP type such as EAP-MSCHAPv2.
  
  This provides security for the inner EAP type which may be vulnerable by itself.

- **Certificate-based** – For more security EAP-TLS provides mutual authentication of both the server and client.
## EAP Methods Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>EAP-FAST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Secure Roaming (CCKM)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Local WLC Authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OTP (One Time Password) Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server Certificates</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Client Certificates</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PAC (Protected Access Credentials)*</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Deployment Complexity</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
</tbody>
</table>

* PACs can be provisioned anonymously for minimal complexity.
Choosing an EAP Method

- Most clients such as Windows, Mac OS X, Apple iOS devices support EAP-TLS, PEAP (MS-CHAPv2).
  
  Additional supplicants can add more EAP types (Cisco AnyConnect).

- Certain EAP types (TLS) can be more difficult to deploy than others depending on device type.
Encryption Evolution

- WEP (RC4)
- TKIP (RC4 and MIC)
- AES (CCMP)
Encryption Best Practices:
TKIP and AES

TKIP (Temporal Key Integrity Protocol)
- Use only for legacy clients without AES support
- Often a software update for WEP clients
- Can be run in conjunction with AES (mixed-mode)
- Is being discontinued by the WiFi Alliance for certification.

AES (Advanced Encryption Standard)
- Requires hardware support (~2005 chipsets or later)
- Achieves line-rate speeds
- Only encryption standard supported for 802.11n data rates
User-Based Policy and Device Identification
Cisco User-Based Policy Offering

- Cisco ACS (or other RADIUS server which can provide Vendor Specific Attributes) can provide static user-based policy which is assigned upon initial authentication.

- Cisco Identity Services Engine can provide dynamic user-based policy which can be assigned upon initial authentication and changed during a session using CoA (Change of Authorization).
Cisco User-Based Policy Solution with ACS

User Specific Attributes

- **Employees**
  - Employee VLAN
  - Gold QoS

- **Contractors**
  - Contractor VLAN
  - No QoS
  - Restrictive ACL

*This could also be any RADIUS server that supports VSAs.*
Cisco ACS User Policy Steps

Phase 1
User Authentication

- EAP
- ACS

Phase 2
User Policy

- Limited Access
- Allowed User?
- Allowed Access

QoS
- Silver

ACL
- Allow-All

VLAN
- Employee
Cisco Controller User-Based Policy Attributes

Network Access
- “Airespace-Interface-Name”
  - Sets the Interface to which the client is connected.

Network Restrictions
- “Airespace-ACL-Name”
  - Sets the Access Control List used to filter traffic to/from the client.

Quality of Service
- “Airespace-QOS-Level”
  - Sets the maximum QoS queue level available for use by the client (Bronze, Silver, Gold or Platinum).
- “Airespace-802.1p-Tag” and/or “Airespace-DSCP-Tag”
  - Sets the maximum QoS tagging level available for use by the client.
ACLs provide L3-L4 policy and can be applied per interface or per user.

Cisco 5508 and WiSM2 implement line-rate ACLs.

Upto 64 rules can be configured per ACL.

### Implicit Deny All at the End

<table>
<thead>
<tr>
<th>Source IP/Mask</th>
<th>Destination IP/Mask</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>DSCP</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>/</td>
<td>Any</td>
<td>DNS</td>
<td>Any</td>
<td>Inbound</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>/</td>
<td>Any</td>
<td>DNS</td>
<td>Any</td>
<td>Inbound</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>/</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Outbound</td>
</tr>
</tbody>
</table>
Endpoint Access Challenges

- **IT is struggling with:**
  - Classifying managed vs. unmanaged endpoints
  - ID devices that cannot authenticate
  - User <-> Device association

- **But there barriers:**
  - Multiple access mediums
  - Endpoint certainty
  - No automated way to discover new endpoints
New ground up solution
- Multiple sensors – rich profiling
- Complete visibility and tracking
- Holistic (wired + wireless)
- Integrated Authentication, Authorization
- Other services (Guest, Posture, Device Registration)
- Flexible deployment
Integrated, Enhanced Device Profiling with Cisco Identity Services Engine

Visibility for Wired and **Wireless** Devices

Simplified “Device Category” Policy

Create Your Own Device Templates

“iPad Template”

“Custom Template”
### Powerful Policy Deployments with ISE

#### Consolidated Services, SW Packages

- NAC Manager
- ACS
- NAC Profiler
- NAC Server
- NAC Guest

Simplify Deployment and Admin

#### Session Directory

- User ID
- Device (and IP/MAC)
- Location
- Access Rights

Tracks Active Users and Devices

#### Flexible Service Deployment

- All-in-One HA Pair
- Admin Console
- M&T
- Distributed PDPs

Optimize Where Services Run

#### Policy Extensibility

Link in Policy Information Points

#### Manage Security Group Access

<table>
<thead>
<tr>
<th>SGT</th>
<th>Public</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff</td>
<td>Permit</td>
<td>Permit</td>
</tr>
<tr>
<td>Guest</td>
<td>Permit</td>
<td>Deny</td>
</tr>
</tbody>
</table>

Keep Existing Logical Design

#### System-Wide Monitoring and Troubleshooting

Consolidated Data, 3 Click Drill-In
Cisco’s User-Based Policy Solution with ISE

User and Device Specific Attributes

**Employees**
- Employee VLAN
- Gold QoS

**Employee Mobiles**
- Employee VLAN
- Gold QoS
- Restrictive ACL

**Contractors**
- Contractor VLAN
- No QoS
- Restrictive ACL

**Contractor Mobiles**
- No Access

With the ISE, Cisco wireless can support multiple users and device types on a single SSID.
Cisco ISE Device Profiling and Policy Steps

**Phase 1**
Device Authentication

**Phase 2**
Device Identification

**Phase 3**
Device Policy
- **QoS**
  - Silver
- **ACL**
  - Allow-All
- **VLAN**
  - Employee

**EAP**

**MAC, DHCP, DNS, HTTP**

**Limited Access**

**Allowed Device?**

**Allowed Access**
ISE Device Profiling Capabilities

Smart Phones

Gaming Consoles

Workstations

Minimum Confidence for a Match

Multiple Rules to Establish Confidence Level
Once the device is profiled, it is stored within the ISE for future associations:

- Is the MAC Address from Apple?
- Does the Hostname Contain “iPad”?
- Is the Web Browser Safari on an iPad?

### ISE Device Profiling Example - iPad

<table>
<thead>
<tr>
<th>Endpoint Profile</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple-iPad</td>
<td>D8:A2:5E:32:9D:8D</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>00:21:6A:5A:85:3A</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>00:24:E8:E7:7B:93</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>00:21:6A:5A:86:70</td>
</tr>
<tr>
<td>Windows7-Workstation</td>
<td>00:23:5E:9D:BC:C9</td>
</tr>
</tbody>
</table>
Cisco ISE Provides Policy for Wired and Wireless LANs

- Unified wired and wireless policy (ISE) and management (NCS).

Centralized Monitoring of Wired and Wireless Networking, Users and Endpoints

Central Point of Policy for Wired and Wireless Users and Endpoints
Client Type and Policy Visibility with NCS and ISE Integration

### Device Identity from ISE Integration
- **User Name**: Jack
- **IP Address**: 10.20.1.101
- **MAC Address**: 00:21:6a:5a:85:3a
- **Vendor**: Intel
- **Endpoint Type**: Microsoft-Workstation
- **Client Type**: Regular
- **Media Type**: Lightweight
- **Mobility Role**: Local
- **Hostname**: Data Not Available
- **CCX**: V4
- **E2E**: V1
- **Power Save**: OFF

### AAA Override Parameters Applied to Client
- **Security Policy Type**: WPA2
- **EAP Type**: PEAP
- **On Network**: Yes
- **802.11 Authentication**: Open System
- **Encryption Cipher**: CCMP (AES)
- **SNMP NAC State**: Access
- **Radius NAC State**: RUN
- **AAA Override ACL Name**: none
- **AAA Override ACL Applied Status**: N/A
- **Redirect URL**: none
- **ACL Name**: none
- **ACL Applied Status**: N/A
- **H-REAP Local Authentication**: No
- **Policy Management State**: RUN
- **Authenticating ISE**: ISE
- **Authorization Profile Name**: AuthEmp
- **Posture Status**: Not Applicable
- **TrustSec Security Group**: Data Not Available
- **Windows AD Domain**: wlan.local

### Policy Information Including Posture
- **Device Name**: CoreSwitch.wlan.local
- **Vendor**: Dell
- **Endpoint Type**: Microsoft-Workstation
- **Protocol**: 802.3
- **Interface**: GigabitEthernet1/0/40
- **Device Name**: Microsoft-Workstation
- **Vendor**: Intel
- **Endpoint Type**: Microsoft-Workstation
- **Protocol**: 802.11n(5GHz)
- **Interface**: data-contractor
NCS Provides Cross-Linking to ISE Reports on Profiling
Rogue Management, Attack Detection and Threat Mitigation
WLAN Security
Vulnerabilities and Threats

**On-Wire Attacks**
- Ad-Hoc Wireless Bridge: Client-to-Client Backdoor Access
- Rogue Access Points: Backdoor Network Access

**Over-the-Air Attacks**
- Evil Twin/Honeypot AP: Connection to Malicious AP
- Denial of Service: Service Disruption
- Reconnaissance: Seeking Network Vulnerabilities

**Cracking Tools**
- Sniffing and Eavesdropping

**Non-802.11 Attacks**
- Backdoor Access: BLUETOOTH AP
- Service Disruption: MICROWAVE, BLUETOOTH, RF-JAMMERS, RADAR
Cisco Rogue Management Diagram

Multiple Methods

- Wireless Control System (WCS)
- Rogue AP
- Authorized AP
- Rogue AP
- Rogue AP
- Rogue Detector
- ARP Sniffing
- RLDP Scanning
- Switchport Tracing
Listening for Rogues
Two Different AP Modes for RRM Scanning

Local Mode Access Points
- Serves clients with time-slicing off channel scanning
- Listens for 50ms on each channel
- Configurable to scan:
  - All Channels
  - Country Channels (Default)
  - DCA Channels

Monitor Mode Access Points
- Dedicated to scanning
- Listens for 1.2s on each channel
- Scans all channels

Rogue Detection Mechanisms
- Any AP not broadcasting the same RF Group name or part of the same mobility group is considered a rogue
- Automatic white listing for autonomous APs managed by WCS
RRM Channel Scanning
Local Mode AP

### AP on Channel 1 - 802.11 b/g/n – US Country Channels

- Every 16s, a new channel is scanned for 50ms (180sec / 11 channels = ~16s)

```plaintext
1 2 1 3 1 4 1 5 1 6 1 7 1 ...
```

### AP on Channel 36 - 802.11 a/n – US Country Channels (without UNII-2 Extended)

- Every 14.5s, a new channel is scanned for 50ms (180sec / 12 channels = ~14.5s)

```plaintext
36 40 36 44 36 48 36 52 36 56 36 60 36 ...
```
RRM Channel Scanning
Monitor Mode AP

Each channel is scanned a total of \( \sim 10.7 \) seconds \((180 \text{ s} / 1.2 \text{ s}) / 14 \text{ ch}\) within the 180s channel scan duration.

Each channel is scanned a total of \( \sim 6.8 \) seconds \((180 \text{ s} / 1.2 \text{ s}) / 22 \text{ ch}\) within the 180s channel scan duration.
802.11n Rogue Detection

802.11n - Mixed Mode

- Detectable by 11a/g devices
- The most common mode of 11n access points
- Facilitates backwards compatibility with 802.11a/g clients by using 11a/g modulation for management and control frames.

802.11n – Greenfield Mode

- Only detectable by 802.11n devices
- In this case, management, control and data frames are sent using 11n modulation schemes
Rogue Classification Rules

Concept

- Classification based on threat severity and mitigation action
- Rules tailored to customer risk model

Lower Severity

- Off-Network
- Secured
- Foreign SSID
- Weak RSSI
- Distant Location
- No Clients

Higher Severity

- On-Network
- Open
- Our SSID
- Strong RSSI
- On-Site Location
- Attracts Clients
Rogue Classification Rules

Examples

Detected as Rogue

- Rogue Rule: SSID: speedy RSSI: -80dBm
  Marked as Friendly

- Rogue Rule: SSID: Corporate RSSI: -70dBm
  Marked as Malicious

- Rogues Matching No Rule
  Marked as Unclassified

Rules Are Stored and Executed on the Wireless LAN Controller
Rogue Classification Rules

Configuration

Rules Sorted by Priority
WCS Security Dashboard

Security Index

Controller IDS and Adaptive wIPS Alarms

Rogues by Category
Rogue Detector AP Mode

Concept

- **Authorized AP**
- **Rogue AP**
- **L2 Switched Network**
- **Trunk Port**
- **Client ARP**

**Wired Rogue Detector AP**
- Detects all rogue client and Access Point ARP’s.
- Controller queries rogue detector to determine if rogue clients are on the network.
- Does not work with NAT APs.

---

Classify
Rogue Detector AP Mode
Example Deployment Scenario

- Install one rogue detector at each Layer 3 boundary.
- Put more simply - ensure all VLANs are monitored by a rogue detector.
Rogue Detector AP Mode

Operation

Security Alert: Rogue with MAC Address: 00:09:5b:9c:87:68 Has Been Detected on the Wired Network

> debug capwap rm rogue detector
ROGUE_DET: Found a match for rogue entry 0021.4458.6652
ROGUE_DET: Sending notification to switch
ROGUE_DET: Sent rogue 0021.4458.6652 found on net msg
Rogue Detector AP Mode
Configuration

interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk encapsulation dot1q
switchport trunk native vlan 113
switchport mode trunk
spanning-tree portfast

All Radios Become Disabled in This Mode
Rogue Location Discovery Protocol

Concept

RoutedEventArgs (Rogue Location Discovery Protocol)
- Connects to Rogue AP as a client
- Sends a packet to controller’s IP address
- Only works with open rogue access points
Rogue Location Discovery Protocol

Operation

Security Alert: Rogue with MAC Address: 00:13:5f:fa:27:c0 Has Been Detected on the Wired Network

> debug dot11 rldp
Successfully associated with rogue: 00:13:5f:fa:27:c0
Sending DHCP packet through rogue AP 00:13:5f:fa:27:c0
RLDP DHCP BOUND state for rogue 00:13:5f:fa:27:c0 Returning IP 172.20.226.253, netmask 255.255.255.192, gw 172.20.226.193
Send ARLDP to 172.20.226.197 (00:1f:9e:9b:29:80)
Received 32 byte ARLDP message from: 172.20.226.253:52142

%LWAPP-5-RLDP: RLDP started on slot 0.
%LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
%LWAPP-5-RLDP: RLDP stopped on slot 0.
Two automatic modes of operation:

‘AllAPs’ – Uses both local and monitor APs

‘MonitorModeAPs’ – Uses only monitor mode APs

**Recommended: Monitor Mode APs** – RLDP can impact service on client serving APs
Switchport Tracing

Concept

WCS Switchport Tracing
- Identifies CDP Neighbors of APs detecting the rogue
- Queries the switches CAM table for the rogue’s MAC
- Works for rogues with security and NAT

SPT Matches On:
- Rogue Client MAC Address
- Rogue MAC Address
- Rogue MAC +1/-1
- Rogue Vendor OUI
WCS Switchport Tracing
Operation (Cont.)

Switch Port Tracing Details for Rogue AP - Netgear:9c:87:68

- Switch/Ports
  - JB-3750E / 172.20.226.193 (Hop: 0)
  - GigabitEthernet1/0/33 (Admin status: Enabled, MAC count: 1)

- Netgear:9C:87:69 (MAC address +1/-1)

Status: Switch port tracing completed with error(s). Please see status window for more information.

Uncheck to Shut the Port
Match Type
Number of MACs Found on the Port
Rogue Location
On-Demand with WCS

- Allows an individual rogue AP to be located on-demand
- Keeps no historical record of rogue location
- Does not locate rogue clients
Rogue Location
In Real-Time with WCS and MSE Context-Aware

- Track of multiple rogues in real-time (up to MSE limits)
- Can track and store rogue location historically
- Provides location of rogue clients
- Provides location of rouge ad-hoc networks
Rogue AP Containment

- Sends De-Authentication (or Disassociation) Packets to Client and AP
- Can use local, monitor mode or H-REAP APs
- Impacts client performance on local/H-REAP APs
- A temporary solution till the rogue can be tracked down.
Rogue Containment

Local Mode APs

- A local mode AP can contain 3 rogues per radio
- Containment packets sent every 500ms
Rogue Containment
Monitor Mode APs

- A monitor mode AP can contain 6 rogues per radio
- Containment packet sent every 100ms

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Data Rate</th>
<th>Size</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue AP</td>
<td>Ethernet Broadcast</td>
<td>6.0</td>
<td>243</td>
<td>802.11 Beacon</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Rogue Client</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Disassoc</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Rogue Client</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Disassoc</td>
</tr>
<tr>
<td>Rogue Client</td>
<td>Rogue AP</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Disassoc</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Rogue Client</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Deauth</td>
</tr>
<tr>
<td>Rogue Client</td>
<td>Rogue AP</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Deauth</td>
</tr>
</tbody>
</table>
Rogue Containment
Auto-Containment Configuration

• Use auto-containment to nullify the most alarming threats
• Containment can have legal consequences when used improperly

Ability to Use Only Monitor Mode APs for Containment to Prevent Impact to Clients
Cisco’s Attack Detection Mechanisms

**Base IDS**
- Built-In to Controller Software
- Uses Local and Monitor Mode APs

**Adaptive wIPS**
- Requires MSE
- Uses wIPS Monitor Mode and/or Local APs
Adaptive wIPS
Components and Functions

- AP
  - Attack Detection
  - 24x7 Scanning

- WLC
  - Configuration

- MSE
  - Alarm Archival
  - Capture Storage

- WCS / NCS
  - Centralized Monitoring
  - Historic Reporting

- Over-the-Air Detection
- wIPS AP Management
- Complex Attack Analysis, Forensics, Events
- Monitoring, Reporting
Cisco Adaptive wIPS with Dedicated Monitor Mode APs

• Adaptive wIPS monitor mode is available for 1130/1240, 1040/1140/1250, 1260 and 3500 Access Points
Adaptive wIPS Monitor Mode
Deployment Recommendations

• Monitor-mode wIPS APs do not serve clients, thus have greater range
  ▪ Client-serving AP typically covers 914.4-1524 square meters
  ▪ wIPS AP typically covers 4572-10668 square meters

• Ratio of wIPS monitor-mode APs to local-mode traffic APs varies by network design, but 1:5 ratio is reasonable estimate

• wIPS APs can simultaneously run context-aware location in monitor-mode
Cisco Adaptive wIPS with Enhanced Local Mode (ELM)

- Adaptive wIPS scanning in data serving access points, including H-REAP mode APs.
- Provides protection without needing a separate overlay network.
- ELM supported APs: 1040, 1140, 1250, 1260 & 3500

Cisco Adaptive Wireless IPS with Enhanced Local Mode Can Reduce Capital Investment by > 50%
Mobility Services Engine
Support for Cisco Motion Services

<table>
<thead>
<tr>
<th>3310 Mobility Services Engine</th>
<th>3355 Mobility Services Engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports Adaptive wIPS for up to 2000 Monitor Mode APs</td>
<td>Supports Adaptive wIPS for up to 3000 Monitor Mode APs</td>
</tr>
<tr>
<td>Supports Context Aware for up to 2000 Tracked Devices</td>
<td>Supports Context Aware for up to 18000 Tracked Devices</td>
</tr>
</tbody>
</table>

- Services can co-exist on the same MSE, but per-service maximums decrease. For Example, the MSE3310 can handle 1000 wIPS APs + 1000 Context Tracked Items.
- Mobility services may have different WLC/WCS software requirements
- **Adaptive wIPS is licensed on a per-AP basis** (both monitor mode and ELM APs count the same)
## Comparison Between Base IDS and Adaptive wIPS

<table>
<thead>
<tr>
<th>feature</th>
<th>Local</th>
<th>Monitor</th>
<th>wIPS ELM</th>
<th>wIPS Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Service</td>
<td>Yes</td>
<td>X</td>
<td>Yes</td>
<td>X</td>
</tr>
<tr>
<td>Rogue Detection and Containment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Attacks Detected</td>
<td>17</td>
<td>17</td>
<td>39</td>
<td>45</td>
</tr>
<tr>
<td>Attack Encyclopedia</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Forensics</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MSE Required</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WCS Required</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Management Frame Protection

Concept

Problem

- Wireless management frames are 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
Cisco Wired IPS Integration
Unified Intrusion Prevention

Business Challenge
Mitigate Network Misuse, Hacking and Malware from WLAN Clients

- Inspects traffic flow for harmful applications and blocks wireless client connections
- Layer 3-7 Deep Packet Inspection
- Eliminates risk of contamination from wireless clients
- Zero-day response to viruses, malware and suspect signatures

WLAN Security
Vulnerabilities and Threats

**On-Wire Attacks**
- Ad-Hoc Wireless Bridge
- Rogue Detection, Classification and Mitigation Addresses These Attacks
- Backdoor Network Access

**Over-the-Air Attacks**
- Evil Twin/Honeypot AP
- MFP Neutralizes All Management Frame Exploits, Such as Man-in-the-Middle Attacks
- Connection to Malicious AP
- Reconnaissance
- WPA2/802.11i Neutralizes Recon and Cracking Attacks
- Sniffing and Eavesdropping

**Non-802.11 Attacks**
- Backdoor Access
  - BLUETOOTH AP
- Service Disruption
  - MICROWAVE
  - BLUETOOTH
  - RF-JAMMERS
  - RADAR
Interference Also Presents a Security Concern

### End User Impact
- Reduced network capacity and coverage
- Poor quality voice and video
- Potential Denial of Service

### IT Manager Impact
- Potential security breaches
- Support calls
- Increased cost of operation

<table>
<thead>
<tr>
<th>Interference Type</th>
<th>Throughput Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Near (7.6 m)</td>
</tr>
<tr>
<td>Jammer</td>
<td>100%</td>
</tr>
<tr>
<td>Video Camera</td>
<td>100%</td>
</tr>
<tr>
<td>Wi-Fi (busy neighbor)</td>
<td>90%</td>
</tr>
<tr>
<td>Microwave Oven</td>
<td>63%</td>
</tr>
<tr>
<td>Bluetooth Headset</td>
<td>20%</td>
</tr>
<tr>
<td>DECT Phone</td>
<td>18%</td>
</tr>
</tbody>
</table>
CleanAir is Purpose Built to Deal with Interference Issues

Detect and Classify

- Uniquely identify and track multiple interferers
- **Detects security-risk interferers** like RF Jammers and Video Camera.
- Assess unique impact to Wi-Fi performance
- Monitor AirQuality

Cisco CleanAir

High-Resolution Interference Detection and Classification Logic Built-In to Cisco’s 802.11n Wi-Fi Chip Design. Inline Operation with No CPU or Performance Impact.
WLAN Security
Vulnerabilities and Threats

**On-Wire Attacks**
- Ad-Hoc Wireless Bridge
  - Rogue Detection, Classification and Mitigation Addresses These Attacks
  - Client-to-Client Backdoor Access
  - Backdoor Network Access

**Over-the-Air Attacks**
- Evil Twin/Honeypot AP
  - MFP Neutralizes All Management Frame Exploits, Such as Man-in-the-Middle Attacks
  - Connection to Malicious AP
- Reconnaissance
  - WPA2/802.11i Neutralizes Recon and Cracking Attacks
  - Sniffing and Eavesdropping

**Denial of Service**
- Denial of Service

**Service Disruption**
- Service Disruption

**Cisco CleanAir Detects These Attacks**
- Backdoor Access
- BLUETOOTH AP
- Service Disruption
- MICROWAVE
- BLUETOOTH
- RF-JAMMERS
- RADAR

**Non-802.11 Attacks**
- Rogue Access Points
Thank you.