Componentes y Alcance de la Seguridad en redes Inalámbricas.
## Agenda

- Secure Wireless 2.0 Solution Architecture
- Strong Authentication and Strong Encryption
- Unauthorized Device Management
- Attack Detection and Mitigation
- Adaptive WLAN IPS (Intrusion Protection System)
- NAC review
The State of WLAN Security

Open Air
- No physical barriers to intrusion

Open Protocols
- Well-documented and understood
- The most common attacks against WLAN networks are targeted at management frames

Open Spectrum
- Easy access to inexpensive technology

More Devices
- Over 1.1 billion Wi-Fi devices will enter the market by 2011 (IDC)
- New 802.11 and non-802.11 RF devices
## Regulatory and Business Requirements

### Sarbanes-Oxley

Publicly Traded Companies Must:
- Maintain an adequate internal control structure and procedures for financial reporting
- Assess the effectiveness of internal control structures

### HIPAA

For Patient Information Firms Must:
- Maintain administrative, technical, and physical safeguards to ensure integrity and confidentiality
- Protect against threats or hazards; unauthorized uses or disclosures

### PCI

All Merchants Using Payment Cards Must:
- Build and maintain a secure network
- Protect and encrypt cardholder data
- Regularly monitor and test networks, including wireless

- Business and security compliance is top of mind for executives
- High-profile retail breaches proved issues with improper Wi-Fi security
- Protecting sensitive business and customer data is the key focus of regulatory compliance requirements
Protecting the Network
Key to Business Continuity

- Have Weak or Don’t Know Their Wireless Policies
- Don’t Regularly Scan Their RF Environment
- Do Not Have Intrusion Prevention Deployed

A Majority of Enterprises Are Not Prepared for the Explosive Growth in Mobility
Secure Wireless 2.0 Overview

- Secure wireless 2.0 published on Cisco.com
  Wireless and network security integration

- Focus is on integrating and extending general enterprise network security to an enterprise WLAN
  Defense-in-depth designed and integrated into the end-to-end architecture
  802.11 fundamental and enhanced security features
  General network security elements, plus any WLAN-specific features

- The goal being: consistent security policy enforcement across both the wired and wireless network
  Critical to effective network security
  Not a WLAN overlay
Secure Wireless Solution Architecture

- **Endpoint Protection**
  - Host intrusion prevention
  - Endpoint malware mitigation

- **Traffic and Access Control**
  - Dynamic, role-based network access and managed connectivity
  - WLAN threat mitigation with IPS/IDS
  - (Device posture assessment)

- **WLAN Security Fundamentals**
  - Strong user authentication
  - Strong transport encryption
  - RF monitoring
  - (Secure guest access)
WLAN Security Components

- Strong Authentication
- Strong Encryption
- Unauthorized Device Management
- Attack Detection and Mitigation
Upper Quadrant Best Practices
WPA2-Enterprise

**Strong Authentication**
- Extensible authentication protocol (EAP)
- Outside methods (protective tunnel)
  - PEAP and EAP-FAST
- Inside methods (authentication credentials)
  - EAP-MSCHAPv2 and EAP-GTC

**Strong Encryption**
- AES
Unauthorized Device Management

Rogue Devices

<table>
<thead>
<tr>
<th>What Is a Rogue?</th>
<th>When Is a Rogue Dangerous?</th>
<th>What Needs to Be Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Any device that’s sharing your spectrum, but not managed by you</td>
<td>• When set up to use the same ESSID as your network (honeypot)</td>
<td>• Detect</td>
</tr>
<tr>
<td>• Majority of rogues are set up by insiders (low cost, convenience, ignorance)</td>
<td>• When it’s detected to be on the wired network, too</td>
<td>• Classify (over-the-air and on-the-wire)</td>
</tr>
<tr>
<td></td>
<td>• Ad-hoc rogues are arguably a big threat, too</td>
<td>• Mitigate (shutdown, contain, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Set up by an outsider, most times, with malicious intent</td>
<td></td>
</tr>
</tbody>
</table>
Phases of Rogue Management

**Detect**
- Listen for non-infrastructure access points, clients, and ad-hocs
- 11n rogue considerations

**Classify**
- Rogue rules based on RSSI, SSID, clients, etc.
- Assessing if rogue is on wired infrastructure
- Switch port tracing

**Mitigate**
- Switch port shutting
- Location pin-pointing
- Over the air containment

<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>144</td>
<td>802.11 Beacon</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Ethernet Broadcast</td>
<td>6.0</td>
<td>56</td>
<td>802.11 Desauth</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Ethernet Broadcast</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Desauth</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Rogue Client</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Desauth</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Rogue Client</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Desauth</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Rogue Client</td>
<td>6.0</td>
<td>30</td>
<td>802.11 Desauth</td>
</tr>
</tbody>
</table>
Cisco Rogue Management Diagram

Multiple Methods

Switch Port Tracing

Wireless Control System (WCS)

Network Core

Wireless LAN Controller

Distribution

Managed AP

Access

Rogue AP

RRM Scanning

RLDP

ARP Sniffing

Managed AP

Rogue AP

Rogue Detector

Rogue AP

Unauthorized Device Management

Strong Authentication

Strong Encryption

Attack Detection and Mitigation
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

Nimda, Sasser, TCP Stack Exploit, etc
Cisco Wired IPS Integration

Connect to the IDS Module or Appliance and Go to Sensor Setup > Certificates > Server Certificate

Note the TLS SHA1 “Fingerprint” of the SSM
Cisco Wired IPS Integration

Configuration

Fingerprint Is Generated on Cisco IPS Device

How Often to Check Excluded Client List
Automated Wireless Security Vulnerability Assessment

- Provides networkwide security health summary
- Proactively monitors entire wireless network
  WLCs, APs, and management interfaces
- Identifies vulnerabilities in:
  Encryption
  User/network authentication
  Threat mitigation
  Management
- Reduces configuration errors by recommending optimal security settings
- Increases awareness of potential security issues
WCS Security Dashboard

Controller IDS and Adaptive wIPS Alarms

Security Index

Rogues by Category
Adaptive Wireless Intrusion Prevention System (wIPS)

Unauthorized Device Management

Strong Authentication
Strong Encryption

Attack Detection

and Mitigation
Wireless Intrusion Prevention
Purpose and Components

Threat Management Workflow

- Detect
- Classify
- Notify
- Log
- Mitigate
- Report
- Archive

What Is the Threat?

How Severe Is It?

Alert Staff, Raise System Alarm, or Just Log?

What Action Must Be Taken?

End-to-End Record of Event and Actions
Mobility Services Engine (MSE)

- Extensible platform for rapid delivery of Services and Applications
  Unified API enabling Enterprise 3.0 applications

- Common framework for hosting multiple services
  Ease of deployment and efficient allocation of CapEx
  Separates control and service planes

- Abstraction layer with CAPWAP/NMSP
  Allows Transport and Applications to evolve independently

- Eco-system of application partners
  Accelerate development and deployment of customized solutions

Applications
- Conferencing
- Messaging
- Telemetry Alerting
- SCM
- CRM
- Presence
- Assembly Line Monitoring
- Inventory Management
- ERP

Cisco Mobility Services API (SOAP/XML, SIP/XML)

MSE

Cisco 3300 Series

Network Mobility Services Protocol

Network Infrastructure (Transport)
Adaptive wIPS Difference

Breadth of Alarms Detected

Controller IDS Does 17 Today
Adaptive wIPS: One Alarm per Attack

Controller IDS Has No Correlation
Adaptive wIPS Feature

Forensic Packet Capture

In channel 52, the system has detected 23 CTS frames in the last minute, which matches the traffic pattern of the form of denial-of-service attack, CTS (Clear-To-Send) attack. A wireless denial-of-service attacker may suspend the wireless media for communication by taking advantage of the privilege of CTS frame to reserve RF medium for transmission. By transmitting back to back CTS frames, an attacker can force other wireless devices sharing the RF medium to hold back its transmission until the attacker stops transmitting the CTS frames. The system detects the abuse of CTS frames for denial-of-service attack.
Adaptive wIPS Feature

Forensic Packet Capture
### wIPS Example Alarm

*Click 'Help' for More Info On the Attack*

**Alarms > WIPS AP '1240-mon'**

<table>
<thead>
<tr>
<th>General</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected By</td>
<td>WIPS AP 1240-mon</td>
</tr>
<tr>
<td>WIPS AP IP Address</td>
<td>172.20.225.233</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
</tr>
<tr>
<td>Acknowledged</td>
<td>No</td>
</tr>
<tr>
<td>Category</td>
<td>Security</td>
</tr>
<tr>
<td>Created</td>
<td>Sep 18, 2008 9:09:28 AM</td>
</tr>
<tr>
<td>Modified</td>
<td>Sep 18, 2008 9:09:28 AM</td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Previous Severity</td>
<td>Clear</td>
</tr>
<tr>
<td>Severity Score</td>
<td>0</td>
</tr>
<tr>
<td>First Seen</td>
<td>Sep 18, 2008 9:08:57 AM</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Sep 18, 2008 9:09:01 AM</td>
</tr>
<tr>
<td>Last Disappeared</td>
<td></td>
</tr>
</tbody>
</table>

**Message**

DoS: De-Auth broadcast attack

**Description**

There may have been a denial-of-service attack underway against the 1250 ap [Channel: 11, SSID: wIPSAttack]. The system detected deauthentication frames sent from the 1250-ap [Channel: 11, SSID: wIPSAttack] to the broadcast or multicast address. This traffic pattern matches a form of denial-of-service attack that uses spoofed broadcast/multicast deauthentication frames to break the association between an access point and its client stations.

**Event History**

**Annotations**
wIPS Integrated Attack Encyclopedia

- Available for each alarm
- Accessible from the wIPS Profile page or by clicking ‘Help’ on each attack alarm
Cisco Network Admission Control (NAC)

Features
- Role-based network access control and security policy compliance enforcement
- Full lifecycle: discovery, assessment, enforcement, and remediation

Benefits
- Securing both managed and unmanaged assets
- Providing guest access and preventing unauthorized access
- Reducing vulnerability-based exploits
What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.

- Who is the user?
- Is s/he authorized?
- What role does s/he get?

- Is MS patched?
- Does A/V or A/S exist?
- Is it running?
- Are services on?
- Do required files exist?

- Is policy established?
- Are non-compliant devices quarantined?
- Is remediation required?
- Is remediation available?
The Aironet 1140 Series Access Point

- Integrated Radios
  - 2.4 GHz (b/g/n)
  - 5 GHz (a/n)
- 10/100/1000 Ethernet Port
- Console port
- Security lock
- Plastic over metal design
- Powered via 802.3af PoE
- Retrofit Mounting Kit allows the AP1140 to slide into existing AP1130 mounting brackets (ordered separately)