Wireless LAN Endpoint Security Fundamentals

BRKAGG-2014
Session Scope

- This session is intended to serve as an introduction to Wireless LAN Endpoint Security Fundamentals.

- The session briefly highlights:
  - Wireless Security Evolution
  - 802.11i
  - Simple WLAN Security Case studies

- The session is not designed to be a detailed guide for any of the features or services described and it is recommended that the audience attend the Techtorial and/or the detailed feature-specific breakout sessions.

What You Should Already Know

- Cisco networking basics (routing and switching)
- Campus network design concepts
- 802.11 WLAN fundamentals
- Cisco Unified Wireless Network concepts
- RF basics
- WLAN security basics – not a theory class
Session Agenda

- WLAN Security Vulnerabilities and Threats
- Cisco Unified WLAN & WLAN Security Review
- WLAN Client and Data Plane Security
  - Authentication & Encryption
  - Fast Secure Roaming
  - Network Access Control – Cisco Clean Access
  - Cisco Secure Agent
  - CS-MARS Integration
  - Cisco Firewall Integration
- Case Study
- Summary
WLAN Security Vulnerabilities and Threats
Why Are Wireless LANs Prone to Attack?

- Open air,
- Propagation Control is difficult
  - No physical barriers to intrusion
- Standard 802.11 protocol
  - Well-documented and understood
  - The most common attacks against WLAN networks are targeted at management frames
- Unlicensed
  - Easy access to inexpensive technology
Risk Assessment

- **Sensitive data**
  
  Different for companies
  
  Determined at all levels of an organization what data must be protected from both a legal and business viewpoint
  
  Appropriate data is being protected with proper protection. Intellectual property, trade secrets, identity information, credit card information, health information, and customer databases
  
  Possibility that some data is too high a security risk

- **Network services**
  
  Availability of a company's network, and such actions would cause damage to the company's productivity and affect sales.
  
  Services: E-mail services, file servers, database services, directory services, Internet connectivity, Web-based applications, virus and intrusion detection services, and custom application services.
Why Is WLAN Security Important?

Vulnerabilities:

- Hackers/Criminal
- Employees

Lessons:

- Do not rely on basic WEP encryption; requirement for enterprise class security (WPA, EAP/802.1x protocols, Wireless IDS, VLANs/SSIDs, etc.)
- Employees often install WLAN equipment on their own (compromises security of your entire network)
- Business impact due to stolen data: Potential financial and legal consequences (laws to protect data confidentiality; example: healthcare, retail, financial, government)

“War Driving”
WLAN Security “Visibility”

- Prevalence of technology
  PWLAN (Public Wireless LAN) and other public 802.11 networks

- Other security fears—identity theft, phishing, etc.
  “Hackers target Xbox Live players”, Feb 20, 2009
  “Crime to boom as downturn blooms” Dec 30, 2008
  [http://news.bbc.co.uk/2/hi/technology/7797946.stm](http://news.bbc.co.uk/2/hi/technology/7797946.stm)

Public availability of tools
- Aircrack—WEP key exploit
- coWPAtty—WPA-PSK exploit
- Kismet—MAC-based implementation of Kismet
WLAN Security Vulnerabilities and Threats

Examples of Existing Vulnerabilities and Threats

- 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 as well as insider attacks)
An Example: How Does a Wireless Exploit Take Place?

- Probe response “listening” (to get SSID)
- Passive WEP key sniffing
- Initial phases of WLAN security exploit
  
  Discovery of WLAN networks by monitoring for probe/probe responses
  
  Collection of sufficient encrypted packets, offline processing and attempt to calculate WEP key
An Example: How Does a Wireless Exploit Take Place?

Active De-Auth to Induce Clients to Probe (Reduces Time to Overcome SSID “Cloaking”

- For example, “Kismac” tool: offers a “suite” of exploit tools with a easy-to-use GUI


- Authentication exploits can then be undertaken, once a client has been provoked to re-authenticate

- Or, if client may be induced to negotiate unauthenticated/unencrypted connection, a direct exploit on client may be undertaken
The Simplest Type of WLAN Exploit

- However, given the “open” characteristics of 802.11 association behavior, one that is not easily fixed
- Disabling SSID “broadcast” simply overcomes passive sniffing; SSID is easily discovered by observing probe responses from clients
- Thus, SSID “cloaking” shouldn’t be considered a security mechanism
802.11 WEP Vulnerabilities

- **802.11 Static-WEP is flawed: encryption passive attacks**
  
  RC4 Key Scheduling algorithm uses 24-bit Initialization Vector (IV) and does not rotate encryption keys

  Practical tools that have implemented FMS attack (example: AirSnort) can uncover the WEP key after capturing 1,000,000 packets

  This is about ~ 17 minutes to compromise the WEP key in a busy network; this attack is passive and all the attack tool needs to do is “listen” to the WLAN network (i.e., sniff WLAN packets)

- **802.11 Static-WEP is flawed: encryption active attacks**
  
  Does not protect the WLAN user data integrity

  Several forms of attacks possible: Replay attacks, bit-flipping attacks, etc.

- **802.11 Static-WEP shared key authentication is flawed**
  
  AP challenges (plaintext challenge) the WLAN user to ensure possession of valid encryption key

  Attacker can obtain key stream \( \Rightarrow \) plaintext challenge \( \text{XOR} \) ciphertext = Key Stream
WLAN Denial of Service (DoS) Attacks

- **RF jamming**
  A simple RF jamming transmitter (example: microwave or chordless phone next to an AP)

- **DoS attacks using 802.11 management frames**
  In current implementations, 802.11 management frames are **not** authenticated between the AP and the clients
  Anyone can spoof a client’s MAC address and send an 802.11 management frame on behalf of that client

- **802.1x authentication flooding**
  An attacker can send a flood of 802.1x authentication requests to the AP
  This causes the AP to process unnecessary authentication frames
Man-in-the-Middle Exploits

Man-in-the-Middle Exploits Are Attacks by Which the Attacker Poses as the Network to Clients and as a Client to the Network

- Attacker must first force client off of intended network in order to lure wireless station to associate to “rogue network”

- Attacker attempts to obtain security credentials or security key by intercepting credentials
Rogue AP Vulnerability: Both Internal and External Sources

Frustrated insider
- User that installs wireless AP in order to benefit from increased efficiency and convenience it offers
- Common because of wide availability of low cost APs
- Usually ignorant of AP security configuration, default configuration most common

Malicious hacker
- Penetrates physical security specifically to install a rogue AP
- Can customize AP to hide it from detection tools
- Hard to detect—more effective to prevent via 802.1x and physical security
- More likely to install LINUX box than an AP
What Is a Dictionary Attack Tool?

- What is a dictionary?
  - Contains variations of passwords
  - Weak passwords can be cracked using standard dictionaries (found easily in various Internet discussion forums and web sites)

- Success factors for this tool depend on:
  - Variation of the user’s password must be found in the dictionary used by the attacker
  - Attacker’s experience and knowledge in generating dictionaries
  - Password strength
    - A weak six character password will be easily compromised compared to a strong ten letter password
    - Attacker’s dictionary strength determines whether the password can be compromised
Address Spoofing

- As with wired networks, MAC address and IP address spoofing are possible in WLAN Networks

- Outsider (hostile) attack scenario
  - Does not know key/encryption policy
  - IP Address spoofing is not possible if Encryption is turned on (DHCP messages are encrypted between the client and the AP)
  - MAC Address spoofing alone (i.e., without IP Address spoofing) may not buy much if encryption is turned on

- Insider attack scenario:
  - Seeking to obtain other’s secure info
  - MAC address and IP Address spoofing will not succeed if EAP/802.1x authentication is used (unique encryption key is derived per user (i.e., per MAC address))
Exploits Using 802.11 as a Launchpad

- Standard Layer 2 exploits, e.g., Dsniff, Nmap
- Penetration test—server and service vulnerabilities:
  - Metasploit project—open source RPC injector [http://metasploit.com](http://metasploit.com)
  - Immunity CANVAS
  - Core security technology impact
- Application security—exploit/malware
- Specific examples that have been launched:
  - Installation of various viruses, worms, and other malware, thereby complicating detection—Security Conference, Canfield University, UK
  - Simple sniffing of unencrypted user ID, passwords, account nos., etc.—Wi-Fi hotspots
Wireless LANs have become easy targets for both “traditional” network exploits, as well as criminal element.

Passive SSID probe sniffing and WEP key attacks are just the first stage in WLAN exploits.

More sophisticated WLAN exploits are likely to employ management frames, as there is currently no encryption capable for these 802.11 media management packets.

If an attacker can gain access to a WLAN, it is possible to launch a variety of higher-layer exploits over this media.
Cisco Unified WLAN & WLAN Security Review
802.11 Security Fundamentals: Setting up a secure 802.11 link

- **Association**
  
  Establish a virtual port for the link

- **Authentication**
  
  Enforce strong, mutual authentication of client & server
  
  Recommendation is 802.1X/EAP
  
  802.1X blocks user access until authentication successful

- **Encryption**
  
  Enforce strong encryption to provide data privacy over the 802.11 link
  
  Recommendation is AES or TKIP
Securing 802.11
Authentication Phase

WPA/WPA2 802.1x Authentication

- 802.1x from client through AP to Controller
- EAP from client to RADIUS
- Encrypted link from client to AP
Look for the 802.11 Security Standards

- Key 802.11 Security Standards
  - WPA (Wi-Fi Protected Access)
    - Wi-Fi Alliance standard for WLAN authentication and encryption prior to 802.11i
    - Developed to address the known WEP issues while supporting legacy hardware
    - Uses 802.1X/EAP + TKIP encryption
  - WPA2 or 802.11i
    - 802.11i is the IEEE standard for WLAN security
    - WPA2 is the Wi-Fi Alliance standard for WLAN authentication and encryption which includes the 802.11i security recommendations
    - Uses 802.1X/EAP + AES encryption
- IEEE 802.11i defines WLAN security standard
- WPA certifies standards compliance for system interoperability
Use CCX for Client Interoperability

- CCX can help with general client interoperability on Cisco & non-Cisco platforms
- Independent testing of devices for standards **compliance**
  - Including WPA, WPA2, 802.11i
- Independent testing of devices for **compatibility** with Cisco infrastructure
  - Including Cisco proprietary and other additional features
- **Variety** of devices/OSs supported with Cisco infrastructure
  - e.g. Windows CE, Symbian

<table>
<thead>
<tr>
<th>Security</th>
<th>v1</th>
<th>v2</th>
<th>v3</th>
<th>v4</th>
<th>ASD</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11i</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>LEAP</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PEAP with EAP-GTC (PEAP-GTC)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAP-FAST</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PEAP with EAP-MSCHAPv2 (PEAP-MSCHAP)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAP-TLS ASD requires either LEAP, EAP-Fast, or EAP-TLS</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco TKP (encryption)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>WPA Protected Access (WPA), 802.1X + WPA TKIP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>With LEAP (ASD requires either LEAP, EAP-Fast, or EAP-TLS)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>With PEAP-GTC</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>With EAP-FAST (ASD requires either LEAP, EAP-Fast, or EAP-TLS)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>With PEAP-MSCHAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>With EAP-TLS (ASD requires either LEAP, EAP-Fast, or EAP-TLS)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>802.11i – WPA2: 802.1X + AES</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>With LEAP</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>With PEAP-GTC</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>With EAP-FAST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>With EAP-FAST and EAP-TLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Cisco driven Wireless Standards

Over the Air

CCX
- 802.11k Radio Measurement
- 802.11r Fast Roaming
- 802.11u External Networks
- 802.11v Client Management
- 802.11w Mngmt Security

Over the Wire

LWAPP
- 802.11j Japan Radios
- 802.11n Next-gen Radios
- 802.11s Mesh Networks

IETF
CAPWAP
WLAN Client & Data Plane Security

Authentication & Encryption
IEEE 802.11i (WLAN Security) Improvements

- 802.11i is the IEEE 802.11 subcommittee responsible for WLAN security improvements

- Key components of IEEE 802.11i standard are:
  
  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
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 block cipher encryption

Which should I use?

Gold, for supporting NIC/OSs
Silver, if you have legacy clients
Lead, if you absolutely have no other choice (i.e., ASDs)
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—mitigation for unauthorized clients/rogue AP
  - Encryption keys derived after authentication—no requirement to manually manage keys
  - Centralized policy control—autonomic encryption policy/user access to authorized resources
How Does Extensible Authentication Protocol (EAP) Authenticate Clients?

Client Associates

Cannot Send Data Until…

…EAP Authentication Complete

Client Sends Data

Data from Client Blocked by Controller/AP

EAP

Data From Client Passed by Controller/AP
EAP-FAST—Simple, Versatile, and Secure

- EAP-FAST: Flexible authentication via secure tunneling
- Strong authentication without the requirement for cert management
- Simple to deploy
- Open standard—latest draft published October 2005
- Robust support
  - Fast roaming (CCKM)
  - Fallback authentication via Cisco IOS® Access Point Local Authentication server
  - Multiple NAC supplicants are available which employ EAP-FAST authentication
- EAP-FAST establishes an encrypted tunnel between the client and the AAA server
  - The client and AAA can then securely use any credentials within the tunnel
  - Client stacks from Meetinghouse Data Communications and others
  - CCX versions 3 and 4 specify EAP-FAST support
EAP-FAST Authentication

Start --> Request Identity

Identity --> Identity

AP Blocks All Requests Until Authentication Completes

Server Authentication

A-ID <--> A-ID
PAC-Opaque <--> PAC-Opaque

Establish a Secure Tunnel (PAC and TLS)

Server Authentiﬁes Client

Key Management <--> Client Authentication
Protected Data Session

WPA or CCKM Key Management Used
Cisco LEAP

- Client support
- RADIUS server
  - Cisco ACS and Cisco Access Registrar
  - Local RADIUS on AP (12.2(13)), ISR (12.3(11), and WLSM)
  - Juniper (Funk) Steel Belted RADIUS or Odyssey server products
  - Interlink RAD-series
- Microsoft Domain or Active Directory database (optional) for back end authentication
- Device support
  - Cisco WLCM, WiSM, 2100 and 4000 Series controllers
    Deprecated
EAP-PEAP

- PEAP: “Protected EAP”
- Hybrid authentication method
  - Server side authentication with TLS
  - Client side authentication with EAP authentication types (EAP-GTC, EAP-MSCHAPv2, etc.)
- Clients do not require certificates
  - Simplifies end user/device management
- RADIUS server requires a server certificate
  - RADIUS server self-issuing certificate capability may be used
  - Purchase a server certificate per server from public PKI entity
  - Setup a simple PKI server to issue server certificates
- Allows for one way authentication types to be used
  - One-time passwords
  - Proxy to LDAP, UNIX, NT/AD, OTP, etc.
EAP-TLS

- Client support
  Windows 2000, XP, and Windows CE (natively supported)
  Non-Windows platforms: third-party supplicants (Meetinghouse and Funk)
  Each client requires a user certificate

- Infrastructure requirements
  EAP-TLS supported RADIUS server
    Cisco ACS, Cisco AR, MS IAS, Funk, Interlink
  RADIUS server requires a server certificate
  Certificate Authority Server (PKI infrastructure)

- Certificate management
  Both client and RADIUS server certificates to be managed
## EAP Protocols: Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>LEAP</th>
<th>EAP-FAST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign-on</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Login Scripts (MS DB)</td>
<td>Yes(^1)</td>
<td>Yes(^1)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Password Expiration (MS DB)</td>
<td>N/A</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Client and OS Availability</td>
<td>XP, 2000, CE, and Others(^2)</td>
<td>XP, 2000, CE, CCXv2 Clients(^3), and Others(^2)</td>
<td>Cisco/CCXv1 or Above Clients and Others(^2)</td>
<td>Cisco/CCXv3 Clients(^4) and Others(^2)</td>
</tr>
<tr>
<td>MS DB Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAP DB Support</td>
<td>Yes</td>
<td>Yes(^5)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>OTP Support</td>
<td>No</td>
<td>Yes(^5)</td>
<td>No</td>
<td>Yes(^6)</td>
</tr>
</tbody>
</table>

\(^1\) Windows OS supplicant requires machine authentication (machine accounts on Microsoft AD)

\(^2\) Greater operating system coverage is available from Meetinghouse and Funk supplicants

\(^3\) PEAP/GTC is supported on CCXv2 clients and above

\(^4\) Almost all CCX clients support EAP-FAST on MSFT XP

\(^5\) EAP-FAST supported on CB21AG/PI21AG clients with ADU v2.0 and CCXv3 clients

\(^6\) Supported by PEAP/GTC only

\(^5\) Supported with 3\(^{rd}\) party supplicant
## EAP Protocols: Feature Support

<table>
<thead>
<tr>
<th></th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>LEAP</th>
<th>EAP-FAST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off-Line Dictionary Attacks?</td>
<td>No</td>
<td>No</td>
<td>Yes¹</td>
<td>No</td>
</tr>
<tr>
<td>Local Authentication</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WPA Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Specific Device (ASD) Support</td>
<td>No</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>
<td>No</td>
</tr>
<tr>
<td>Client Certificates?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Deployment Complexity</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>RADIUS Server Scalability Impact</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low/Medium</td>
</tr>
</tbody>
</table>

802.11i/WPA Authentication and Key Management Overview

Controller/Access Point

RADIUS

Capabilities
Discovery

802.1X Authentication

Key Management

Key Distribution

Data Protection
802.11i/WPA Capabilities Discovery

- **Probe Request**
- **Probe Response + WPA IE (AP Supports WEP Mcast, TKIP Ucast, 802.1X Auth)**
- **802.11 Open System Auth**
- **802.11 Open Auth (Success)**
- **Association Req + WPA IE (STA Requests WEP Mcast, TKIP Ucast, 802.1X Auth)**
- **Association Response (Success)**
Four-Way Handshake

- ANonce
- SNonce (MIC)
- Ready to Use (MIC)
- OK, Use

Temporal Keys

- The four WPA/TKIP temporal keys are:
  - Data Encryption key (128 bits)
  - Data Integrity key (128 bits)
  - EAPOL-Key Encryption key (128 bits)
  - EAPOL-Key Integrity key (128 bits)

- The three WPA2/AES-CCMP temporal keys are:
  - Data Encryption/Integrity key (128 bits)
  - EAPOL-Key Encryption key (128 bits)
  - EAPOL-Key Integrity key (128 bits)
WLAN Client & Data Plane Security

Fast Secure Roaming
Roaming Requirements

- Roaming must be fast… Latency can be introduced by:
  - Client channel scanning and AP selection algorithms
  - Re-authentication of client device and re-keying
  - Refreshing of IP address

- Roaming must maintain security
  - Open auth, static WEP – session continues on new AP
  - WPA/WPAv2 Personal – New session key for encryption derived via standard handshakes
  - 802.1x, 802.11i, WPA/WPAv2 Enterprise – Client must be re-authenticated and new session key derived for encryption
Fast Secure Roaming

- Client channel scanning and AP selection algorithms—Improved via CCX features
- Refreshing of IP address—Irrelevant in controller-based architecture!
- Re-authentication of client device and re-keying

**Cisco Centralized Key Management (CCKM)** – Cisco proprietary, supported via CCX

**Proactive Key Caching (PKC)**—extension of optional component of 802.11i (PMK Caching)

Coming soon: Standardization via 802.11r
Client embeds PMKID in (re)association request

PMKID = HMAC-SHA1-128 (PMK, “PMK Name” || BSSID || STA Mac)

Controller validates PMKID, if it checks out, bypass full RADIUS auth and go directly to 4-Way Handshake.

If it does not match, controller sends EAP Identity request to client and proceeds with full authentication

PMK and Four-Way Handshake

Group Key Two-Way Handshake Sends GTK from Controller/AP to STA

Benefits:
- Standards-based
- Very fast roam times with supported supplicants
- Requires WPAv2
Cisco Centralized Key Management (CCKM) — Initial Key Derivation

RADIUS Pushes “NSK” from AS to Controller/AP

Controller starts “Re-key” counter (RN)

Four-Way Handshake yields 2 additional keys (BTK, KTK)

Client hashes BTK, RN, BSSID to derive PTK

Controller hashes BTK, RN, BSSID to derive PTK

Group Key (GTK) encrypted and handed to client
Cisco Centralized Key Management (CCKM)—Client Roam

Client embeds MIC based on hash of RN++ and KRK, updates internal RN

Controller increments RN, validates MIC using RN++ and KRK
If MIC checks out, controller hashes BTK, RN++, new BSSID to derive new PTK

Client hashes BTK, RN++, new BSSID to derive new PTK

Group Key (GTK) encrypted and handed to client

Controller increments RN, validates MIC using RN++ and KRK

Benefits:
- Supported since CCXv2—large supplicant base including voice handsets and ASDs
- Extremely fast roam times
- Supported with TKIP, not AES
WLAN Client & Data Plane Security

Network Access Control – Cisco Clean Access
Cisco Unified Wireless with NAC Appliance

Cisco NAC Summary:

- Cisco NAC appliance is an easily deployed NAC product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources.

- The Cisco NAC appliance identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with network security policies, and repairs any vulnerabilities before permitting access to the network.

- Cisco’s NAC solution is a natural complement to a Unified Wireless deployment and enhances overall wireless security by enforcing end station policy compliance.
Cisco Unified Wireless with NAC Appliance

- NAC Appliance accommodates several deployment scenarios:
  - Centralized and Distributed
  - In-band and Out-of-Band
  - Virtual Gateway or Real IP Gateway

- Unified Wireless and Campus Virtualization best practices currently recommend a centralized deployment
  - Should be logically in-band, L2 adjacent with wireless topology
  - Virtual G/W mode with VLAN Mapping is preferred over IP GW mode for wireless deployments
  - Real IP G/W mode is compatible with wireless deployment, but with caveats.
Cisco Unified Wireless with NAC Appliance
Cisco Unified Wireless with NAC Appliance

In-band Virtual Gateway

VLAN 10

VLAN 900

VLAN 10

VLAN 110

Posture Assessment

Authenticated Access

NAC MGR

VLAN Mapping

WLAN Controller

LAP

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public
Cisco Unified Wireless with NAC Appliance

User Authentication:

- NAC appliance authentication doesn’t replace wireless 802.1x/EAP
- Both are necessary for strongest security
- NAC Authentication by default is un-aware of wireless authentication.
  
  Can be addressed by implementing NAC VPN SSO authentication with WLC RADIUS accounting
  
  Best user experience achieved when used with Clean Access Agent.
Cisco Unified Wireless with NAC Appliance

Assessment and Remediation:

- Two Methods:
  - Agent – Clean Access Agent software on client PC
  - Network Scan – Web Based

- Both are compatible with Unified Wireless Deployment
  - Agent based offers best user experience and solution performance.
Cisco Unified Wireless with NAC Appliance

Client Roaming with NAC:

- Layer 2 Roaming – Supported with NAC In-band Virtual Gateway.
  - Between AP’s same controller
  - Between AP’s on different controllers, same VLAN/subnet per controller.
  - Between AP’s in different AP groups, same controller
Cisco Unified Wireless with NAC Appliance

Client Roaming with NAC:

- **Layer 3 Roaming – Supported with NAC In-band Virtual Gateway**
  
  Between AP’s on different controllers, different VLAN/subnets per controller
  
  Between AP’s in different AP groups on different controllers.
  
  Symmetrical roaming tunnel is enabled.
WLAN Client & Data Plane Security

Cisco Security Agent
CSA for WLAN Security Overview

- CSA Overview
  - Key element of integrated end-to-end, defence-in-depth approach to security
  - Identifies and prevents malicious or unauthorized behavior
  - Offers endpoint threat protection, often referred to as Host-based IPS (HIPS)

- CSA for WLAN Security
  - Threat detection and mitigation on a WLAN, along with policy enforcement
    - General client protection
    - WLAN-specific scenarios
Cisco Self-Defending Network

- LWAPP Access Point
- Wireless LAN Controller
- NAC Appliance Server
- CS-MARS
- ASA IPS Edition
- Wired Client
- CSSC
- CSA NAC Agent
- CS-ACS
- CSA Manager
- NAC Manager
- DHCP Server
Cisco Security Agent

- Wired Client
- Wireless Client
- CSA
- LWAPP Access Point
- Wireless LAN Controller
- NAC Appliance Server
- ASA IPS Edition
- CS-MARS
- Wired Client
- CSSC
- CSA
- NAC Agent
- CS-ACS
- CSA Manager
- NAC Manager
- DHCP Server

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public
Wireless Ad-Hoc Connection Security Concerns

- Typically little or no security
  - Generally, unauthenticated, unencrypted connection
- High risk of connectivity to unauthorized or rogue device
- Risk of bridging a rogue wireless ad-hoc device into a secure, wired network
  - Simultaneous wireless ad-hoc & wired connections
- Microsoft Windows native WLAN client vulnerability
  - Microsoft Wireless Auto Configuration default behavior creates high risk of connectivity to a rogue device, particularly as a user may not even be aware that an 802.11 radio is enabled
## CSA Wireless Ad-Hoc Pre-Defined Rule Module

### Management Center for Cisco Security Agents V5.2

**Configuration** » Rule Modules » Windows Rule Modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Filter</th>
<th>Version</th>
<th>Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent Wireless Adhoc communications</td>
<td>adhoc</td>
<td>5.2 r203</td>
<td>1 rule</td>
<td>Prevents all communications over 802.11 when the wireless connection is in Adhoc mode (i.e., peer to peer)</td>
</tr>
</tbody>
</table>
CSA Wireless Ad-Hoc Pre-Defined Rule Module Considerations

- Wireless ad-hoc connections continue to be initiated, accepted, and remain active and connected

- Only UDP and TCP traffic over a wireless ad-hoc connection is dropped
  
  Additional CSA security measures should be in place to protect clients from non-UDP and non-TCP threats

- ICMP pings that route over a wireless ad-hoc interface are not filtered and remain a threat
  
  Incoming ICMP packets may be filtered by enforcing a CSA Network Shield rule module
  
  No current solution to filter outgoing ICMP packets
Simultaneous Wired & Wireless Security Concerns

- Risk of bridging a rogue device into a secure wired network
- Risk of bridging an authorized device into the wired network, bypassing network security measures and policies
- User may not be aware of 802.11 network connectivity

Active insecure or wireless ad-hoc profile may be used by rogue device, e.g. public hotspot or unauthenticated home WLAN profile
Location-Based Security Concerns

- Are you on the corporate network?
- Are you connected to a rogue device?
- Is your VPN up?
- Is your data secured?
- Whose network are you on?
- Are you bridging unauthorized devices into your VPN?

Wireless Ad-Hoc Networks
- Office
- Airplane
- Shared Building e.g. home or office
- Customer or Partner Site

Simultaneous Wired & Wireless
- Home
- Hotspot

Rogue WLAN

Insecure WLAN
CSA Location-Aware Policy Enforcement

- CSA v5.2 introduced the ability to enforce different security policies based on the location of a client
  
  Enables stronger security protection measures to be enforced when a client is on an insecure or non-corporate network

- CSA v5.2 also introduced a pre-defined location-aware Windows rule module
  
  “Roaming - Force VPN”
  
  Leverages system state conditions and interface sets to apply rules that force the use of VPN if a client is out of the office
CSA v5.2 introduced a pre-defined Windows rule module to module to force connectivity to the corporate network if a network connection is active

“Roaming - Force VPN”

If a network connection is active but the CSA MC is not reachable, all UDP or TCP traffic over any interface is denied, except HTTP/HTTPS for a period of 300 seconds

May be used to protect the roaming client itself, local data, and data in transit when on insecure, non CORPORATE networks
### CSA Force VPN When Roaming Pre-Defined Rule Module

#### Management Center for Cisco Security Agents V5.2

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Rules</th>
<th>Description</th>
<th>Target OS</th>
<th>Syntax</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming - Force VPN</td>
<td>5.2 r203</td>
<td>5 rules</td>
<td>Force VPN connection if MC unreachable</td>
<td>All</td>
<td></td>
<td>Windows</td>
</tr>
</tbody>
</table>

*Configuration > Rule Modules > Windows Rule Modules*
Session Agenda

- WLAN Security Vulnerabilities and Threats
- Cisco Unified WLAN & WLAN Security Review
- WLAN Client and Data Plane Security
  - Authentication & Encryption
  - Fast Secure Roaming
  - Network Access Control – Cisco Clean Access
  - Cisco Secure Agent
  - CS-MARS Integration
  - Cisco Firewall Integration
- Case Study
- Summary
WLAN Client & Data Plane Security

CS MARS Integration
CS-MARS
Monitoring Analysis and Response System

LWAPP Access Point  →  Wireless LAN Controller  →  NAC Appliance Server

Guest Anchor Controller  →  ASA IPS Edition

CS-MARS

Wired Client
CSSC
CSA
NAC Agent

CS-ACS
CSSC
CSA Manager
NAC Manager
DHCP Server
Wireless and CS MARS: Integrated with WLC and MARS 5.3.2

- **Device Discovery:**
  - Add WLC's IPs in MARS
  - Initiate MARS Discovery to WLCs to Learn APs

- **Event parsing:**
  - SNMP Trap from WLC to MARS
  - MARS Parses SNMP Trap and Presents “Event Type” and “AP Name” in MARS Incident Table

- **Event Manipulation:**
  - MARS Searches Raw SNMP Message to Create Incidents

- **Mitigation Assistance:**
  - MARS Suggests Mitigation Actions (WLC and AP) in Common MARS Format

- **Real-time Notification:**
  - MARS Performs Incident Notification Based on Current MARS Framework

- **Report and Query:**
  - MARS Performs Reporting Based on Current MARS Framework
Wireless MARS Integration: Deployment Example

1. Wireless Attack Launched

2. Wireless IDS Fires

3. WLC Takes Action AND Sends Event to MARS

4. MARS Presents Consolidate Incident View and Mitigation Suggestion
WLAN Client & Data Plane Security

Cisco Firewall Integration
Cisco Firewall Integration

- Cisco offers range of fully featured firewalls that can be integrated into the Secure Wireless solution
  - Enables a consistent firewall platform deployment across the wired and wireless network
  - Enables consistent policy enforcement across both the wired and wireless network
  - Provides lower TCO and easier management
- Can be used to enforce policy on traffic between the WLAN and the wired network
  - Policies may be applied on layers L2-L7
  - Enables stateful firewall, network access restrictions, etc.
- Integrated and extended features on common platforms
  - Including SSL VPN, IPS, content security, security contexts
Cisco Firewall Integration Scenario: User Group Access Policy Enforcement

- User group access policy enforcement
  
  Different firewall policies for different classes of users sharing the same WLAN infrastructure
Cisco Firewall Integration Scenario: User Group Access Policy Enforcement

- Restricts user group access to permitted network resources only
- 802.1X allows a common WLAN but different user group VLAN assignment based upon AAA policy
  
  Single SSID with RADIUS-assigned VLAN upon successful 802.1x/EAP authentication
- VLAN mapped to different firewall VLANs and subject to different firewall policy
  
  VLAN mapped to a specific virtual context (user group) in the firewall
  
  Firewall policy enforced per user group
Cisco Firewall Integration Considerations

- Transparent or Routed Mode
  
  Both transport and routed mode can be used with WLAN

  Transparent mode was used for testing due to its ease of integration

- Single or Multiple Context Mode
  
  Both single and multiple context modes can be used with WLAN

  Multiple context mode was used for testing to enable use of multiple virtual firewalls and load sharing

- Cisco Firewall Platform
  
  Any Cisco firewall platform or module can be used with WLAN

  FWSM was used for testing to leverage the Cat6K integration
Case Study
This case study is just for training purpose. This has no reference to any of Cisco Customers.
Design Considerations

- Size of the Company – 750 employees
- Location of the Company - One location, x floors, y remote branches (15~20 employees)
- Wireless Infrastructure - Off the shelf wireless devices, decentralized, No Management
- Wireless Security - Primitive, Difficult to manage,
- Client devices - Desktops, Laptops, Handheld scanners
- Guest Access - Not available
Customer Requirement

- Easy to Manage, Control and handle
- Centralized management, Little remote management
- Reliable, robust & Scalable network design
- Compliance with Standards
- Compatible with existing Wireless clients
- Easily Integrate with Cisco wired architecture
Case Study - Discussion
Q & A
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.