TOMORROW starts here
Secure Wireless LAN Design and Deployment

BRKEWN-2664

Mark Krischer
CTO, Enterprise Networks – Asia Pacific, Japan and Greater China
Abstract

The proliferation of mobile devices and the rise of BYOD has raised the profile of the enterprise wireless network and the challenges associated with secure and scalable wireless network design.

In this session we will explore the threats associated with wireless networks and consider the 802.11 standards and Cisco solutions which address them. This will include an understanding of enforcing policies based on authentication and authorisation; the implications of fast secure roaming in voice and video deployments; and more advanced topics such as rogue AP detection, wireless intrusion detection and prevention, and spectrum intelligence.
Session Objectives

- What this session will cover
  - Wireless Threats
  - Wireless Security Fundamentals
    - Authentication
    - Encryption
    - Authorisation
  - Wireless Security Standards
  - Advanced Wireless Security
  - Network Design Implications

- And what it won’t
  - Configuration Details
  - Version Discrepancies
  - Roadmap

- Except when it does…
Wireless Threats and Vulnerabilities

- Wireless propagates beyond the traditional physical boundaries of the wired network

- Attack from anywhere within the bounds
  - Passive scanning attacks
  - Active spoofing attacks
  - Active jamming or DoS attacks

- Rogue APs can be a source of different vulnerabilities
  - Honeypot APs
  - Unsecured backdoor access

- Wireless Clients themselves can introduce vulnerabilities as well
  - Bridge wireless to wired network
  - Unsecured Hot-Spot usage
  - Data Exposure
Wireless Protected Access

**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 – Pre-Shared Key)
- Enterprise (802.1X/EAP)
**802.11 Fundamentals**

**Beacons and Probes**

- Beacon: SSID = blizzard, Security = WPA2-Enterprise
- Beacon: SSID = ciscolive, Security = Open
- Probe Request: SSID = blizzard
- Probe Response: SSID = blizzard, Security = WPA2-Enterprise
- Probe Request: SSID = ciscolive
- Probe Response: SSID = ciscolive, Security = Open
### 802.11 Fundamentals

#### Association

- **Association Request**
- **Association Response**
- **Disassociation Request**
- **Disassociation Response**
- **Reassociation Request**
- **Association Response**

- SSID = blizzard
- SSID = blizzard, Security = WPA2-Enterprise
- SSID = blizzard
- SSID = blizzard
- SSID = blizzard
- SSID = blizzard, Security = WPA2-Enterprise
802.11 Fundamentals

Authentication

Supplicant -> CAPWAP -> Wireless LAN Controller -> RADIUS -> Identity Services Engine

Authenticator

802.1x

RADIUS -> EAP
802.11 Fundamentals

Authentication

Association Response
Identify Request
Identity Response
EAP Type Negotiation
Authentication Sequence Between Supplicant and Authentication Server
EAP Success
Identity Response
Identity Response
EAP Success
WPA-Enterprise
802.1x and Extensible Authentication Protocols

Tunnel-Based

Outer Methods
- EAP-PEAP
- EAP-FAST

Inner Methods
- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS

Certificate-Based

- EAP-TLS
802.11 Fundamentals

Encryption

PTK = SHA(PMK + ANonce + SNonce + AP MAC + STA MAC)
NOTE: Pairwise key support with TKIP or CCMP allows a receiving STA to detect MAC address spoofing and data forgery. The RSNA architecture binds the transmit and receive addresses to the pairwise key. If an attacker creates an MPDU with the spoofed TA, then the decapsulation procedure at the receiver will generate an error. GTKs do not have this property.

- When enabled, GTK should be randomised for each client
- Clients will not be able to decrypt the Broadcast and Multicast packets received from other clients
- Consider the implications for certain applications
  - IGMP membership report queries are send as “broadcast”
  - Downstream IGMP client membership report queries will not be decipherable by all clients
Secure Fast Roaming

Challenges

- Client channel scanning and AP selection
- Re-authentication of client device and re-keying
Secure Fast Roaming
Cisco Compatible Extensions

- Client channel scanning and AP selection
  - Improved via Cisco Compatible Extensions (CCX) Neighbour Lists
- Re-authentication of client device and re-keying
  - Cisco Centralised Key Management (CCKM)
- In *highly controlled test environments*, CCKM roam times measure 5-8ms

- Available in CCX enabled clients
Secure Fast Roaming
Voice-Enterprise and 802.11k and 802.11r

- Client channel scanning and AP selection
  - Improved via 802.11k Neighbour Lists
- Re-authentication of client device and re-keying
  - 802.11r based on CCKM
- Available in Voice-Enterprise certified clients
  - Due to changes to 802.11 management frames, older client drivers may not understand the 11r response frame
Management Frame Protection

- Infrastructure Management Frame Protection
  - Detection

- Client Management Frame Protection
  - Prevention
Management Frame Protection

802.11w and Protected Management Frames

- Unicast Management Frames
  - Confidentiality and Integrity Protection

- Multicast Management Frames
  - Integrity Protection
Security Association Teardown Protection

802.11w and Protected Management Frames
Security Association Teardown Protection
802.11w and Protected Management Frames

Reassociation Request → Reassociation Response
SA Query Request → SA Query Request
SA Query Request → SA Query Request
Reassociation Request → Association Response

Reject: Try again later
SA Query Timeout
Comeback Timer
Reassociation Request Accepted
Security Association Teardown Protection
802.11w and Protected Management Frames

802.11w Protected

Reassociation Request ➔
Reassociation Response ←
SA Query Request ←
SA Query Response ➔

Reject: Try again later
Reassociation Request Ignored
WPA Personal
Pre-Shared Key

- Offline Attack
  - Dictionary
  - Rainbow Table

- Strong Passwords Matter

PSK

PTK

PTK = SHA(PSK + ANonce + SNonce + AP MAC + STA MAC)
Wi-Fi Protected Setup
Brute Force Attack Feasibility

- Online Attack
  - Brute force

<table>
<thead>
<tr>
<th>PIN</th>
<th>➔ Identity Request ➔</th>
<th>PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>➔ Identity Response ➔</td>
<td>WFA-SimpleConfig</td>
</tr>
<tr>
<td></td>
<td>➔ EAP-NACK</td>
<td>Key Space $10^8 = 100,000,000$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prove Possession of 1\textsuperscript{st} half of the PIN</td>
</tr>
<tr>
<td></td>
<td>➔ EAP-NACK</td>
<td>Key Space $10^4 = 10,000$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prove Possession of 2\textsuperscript{nd} half of the PIN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Space $10^4 + 10^4 = 20,000$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Space $10^4 + 10^3 = 11,000$</td>
</tr>
</tbody>
</table>
Wi-Fi Direct

- Wi-Fi Direct allows devices to make direct connection groupings to enable printing, syncing and content sharing
- Wi-Fi Direct leverages both WPA2 for security and WMM for QoS
- *But*, WPS is used to enable the quick and easy connection
- *Worse*, Wi-Fi Direct supports simultaneous connections to both infrastructure networks and Wi-Fi Direct groups
Data Exposure
AnyConnect

Desktop
- Microsoft Windows
- Mac OS X
- Linux

Mobile
- Apple iOS
  - iPhone and iPad
- Android
  - Smartphones
  - Tablets
  - BB10 (future)
  - Smartphones
  - Playbook

Clientless
- HTC
- Motorola
- Samsung
- Version 4.0+
Advanced Security Capabilities

- Rogue AP Detection and Containment
- Layer 1 active jamming attacks
- Layer 2 active spoofing attacks
Rogue AP Detection

Rogue Location Discovery Protocol

RLDP Packet
Rogue AP Detection
Switch Port Tracing

- Show CDP Neighbours
- SNMP CAM Table Lookup
- MSE
- Prime Infrastructure
Integrated IDS and Adaptive wIPS

- Monitor Mode AP / WLC Integrated IDS
  - Rogue AP and Client Detection
  - 17 Common Attack Signatures

- Enhanced Local Mode
  - Enables Client Serving APs to periodically go off-channel for IDS scanning

- Adaptive wIPS
  - Alarm Aggregation, Consolidation and False Positive Reduction
  - Enhanced DoS Attack Behaviour Analysis
  - Coordinated Rogue Containment
  - Anomaly Detection
  - Forensic, Blacklisting, Auto Containment, and Auto Immunity responses
Alarm Consolidation
MDK3 Secret Destruction Mode

- MDK3 is a wireless penetration test tool

- Beacon Flooding Attack
  - Fills the environment with fake APs

- EAPOL Flooding Attack
  - Generates multiple authentication requests from spoofed MAC addresses

- Deauthentication/Disassociation Attacks

- Michael MIC Countermeasure DoS Exploit
Wireless Security and Spectrum Intelligence

Deployment Modes

**Enhanced Local Mode**
- Data, wIPS & CleanAir

**Monitor Mode**
- Data
- wIPS & CleanAir

**AP3600/3700 with WSSI**
- Data, wIPS & CleanAir

- **AP Mode**
  - local
  - monitor

- **AP Sub Mode**
  - wIPS
  - WIPS

- Data with wIPS & CleanAir “On Channel”
- Data with CleanAir “On Channel”
- Best Effort wIPS coverage “Off Channel”
- wIPS & CleanAir “All Channels”
Wireless Security and Spectrum Intelligence

Off Channel Scanning

- **Dwell time**
  - ELM: 50ms per-channel
  - MM: 1.2s per channel

- **Monitor Mode**
  - 1 Monitor Mode AP : 5 Local Mode

- **WSSI Module**
  - 1:5 Clean Air
  - 2:5 wIPS
Wireless Security and Spectrum Intelligence

CleanAir Integration

- Detection and location of RF layer DoS attacks
- Non-standard channel threat detection
- Detection and mitigation of non-Wi-Fi device interference
Authorisation
Network Segmentation
Authorisation

Static VLAN Assignment

- VLAN based on SSID
- VLAN segregation based on security policy

Dynamic VLAN Assignment

- VLAN based on authentication credentials
- VLAN segregation based on role

TrustSec – Secure Group Access

- Security based on TAGs instead of source and destination addresses
- ACLs applied at the packet level
Network Design Implications

Centralised Wireless Deployment

- WLC acts as a chokepoint
- ASA provides policy enforcement and threat detection on wireless traffic before bridging onto the Enterprise network

- Wireless traffic tunneled to the network core
- Wireless traffic treated differently to wired traffic
Network Design Implications
Converged Access Deployment

- Wireless traffic bridged at the access layer
- Wireless traffic treated the same as wired traffic

Wireless
- wIPS
  - Rogue AP Detection
  - Containment
  - Switch Port Tracing
  - WSSI support pending
- ACLs
  - Airespace
  - Downloadable
  - SGACL

Wired
- Security Features
  - Storm Control
  - Protected Ports
  - IP Source Guard
  - IPv6 First Hop Security
- Flexible Netflow
- Wireshark
- EEM
Q & A
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. [www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)