ERNW Newsletter 30b / February 2010

Dear Partners, dear Colleagues,

Welcome to the 30th edition of the ERNW Newsletter with the title:

Some Security Notes on Cisco Enterprise WLAN Solutions

Version 1.0 from 15th of February, 2010
Signed by Friedwart Kuhn

By Enno Rey and Oliver Roeschke, {oroeschke, erey}@ernw.de

[Abstract] This newsletter displays results of on-going research regarding Cisco Enterprise Wireless LAN solutions.

Friedwart Kuhn
15.2.2010 17:27:30

TABLE OF CONTENTS

1 INTRODUCTION

The world of *Enterprise WLAN solutions* is full of obscure and "non-standard" elements and technologies. This also applies for Cisco's solutions.

In this document, we examine potential and practical attacks against network traffic, cryptographic material and/or components in different generations of their offerings. Furthermore we provide some guidelines how to implement the included elements in a secure way.

2 TECHNOLOGY OVERVIEW

The following diagram gives a rough overview of components typically involved in such setups.

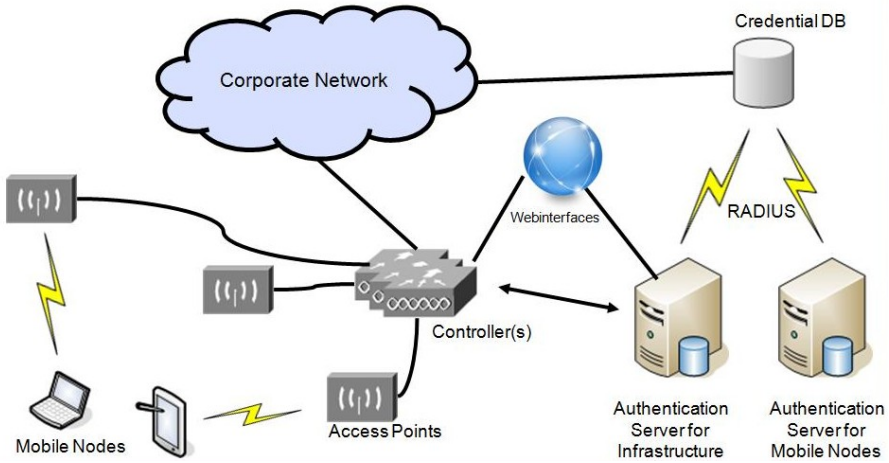


Figure 1: Typical WLAN Setup

Obviously there are Access Points and Mobile Nodes (stations). Furthermore, Authentication Servers (authenticating users and/or devices) as well as entities providing centralized management and configuration capabilities (called "controllers" herein) are part of the overall picture.

2.1 Different generations of Cisco WLAN Solutions

From the authors' perspective three main flavors can be distinguished:

- 1st generation: Structured Wireless-Aware Networks (SWAN).
- 2nd generation: Based on managed AP's & LWAPP, after *Airespace* acquisition in 2005.
- 3rd generation: *Cisco Unified Wireless Network* (CUWN) with CAPWAP as main protocol.

2.2 Cisco Structured Wireless-Aware Networks (SWAN)

"Cisco Structured Wireless-Aware Network (SWAN) solution provides integration for Cisco WLAN access points […], wireless clients […], .and Cisco wired switches and routers. This enables scalability, manageability, reliability and ease of deployment […]. Furthermore the SWAN solution enables end-to-end security, […], and Layer2/ Layer3 mobility. Cisco SWAN solution can scale to manage thousands of AP's and […] WLAN users […]." is stated by [CWLS], page 223[1].

[1] *See [CWLS], page 233.*

Cisco's SWAN solution implements key requirements for enterprise wireless networks, displayed above. All components integrate easily into existing network infrastructure concepts, like identity and accounting services (Authentication, Authorization and Accounting - AAA) and layered network design[2].

2.2.1 SWAN Components

SWAN consists of components at different network layers (see Figure 2), making it possible to integrate within the typical layered network design, recommended by Cisco.
As mentioned in [CWLS] Chapter 9, SWAN can be operated in one of two modes:

- SWAN nonswitching deployment mode
- SWAN central switching deployment mode

Using the central switching deployment mode the Wireless LAN Service Module[3] operates as the central authentication, traffic aggregation and Wireless Domain Services (WDS) master. Within nonswitching deployments, this task is conducted by an AP or Router.

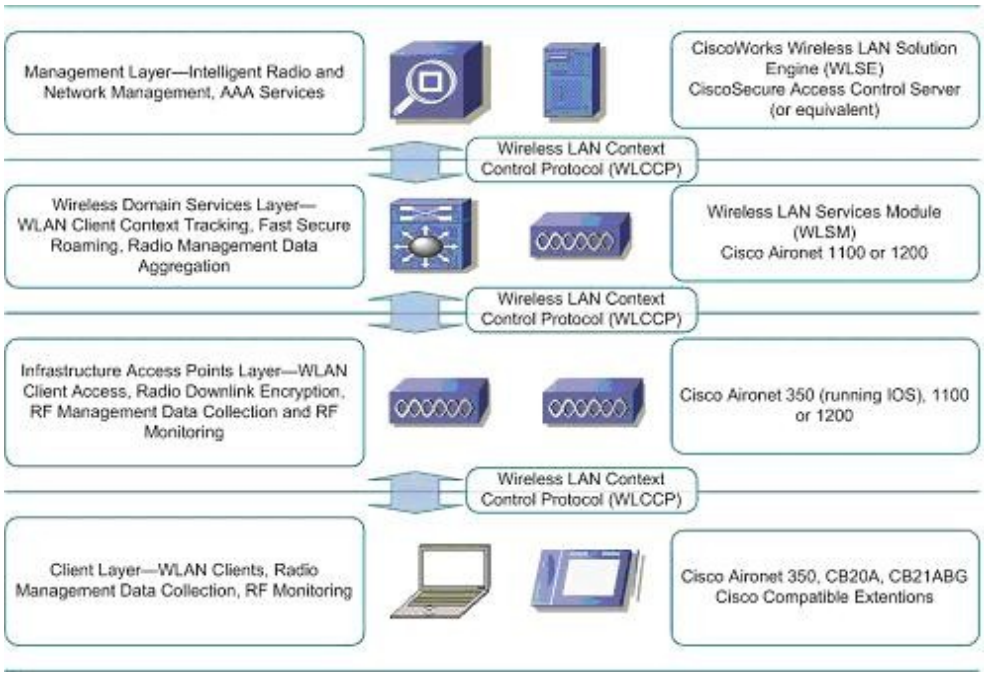


Figure 2: Cisco SWAN Layers (according to [SWANIG])

Both deployment modes depend on a number of common components (which can be found in Figure 3):

- Authentication Server (Cisco Secure ACS): Delivers authentication services by implementing 802.1X and certain EAP methods. Is capable of verifying authentication credentials and is responsible for key derivation during authentication processes.
- Infrastructure Access Points: Assemble the wireless network, which is used by the Mobile Nodes, delivering transit of network traffic between wireless and wired networks.
- Mobile Nodes: Mobile devices, as notebooks, handhelds or Voice-over-IP telephones, which use wireless network cards to transport data into the corporate network.

---

[2] *See [CNHADG], chapter "Hierarchical Campus Network design" for an Introduction into layered network design.*
[3] *WLSM - product details available under http://www.cisco.com/en/US/products/ ps5865/*

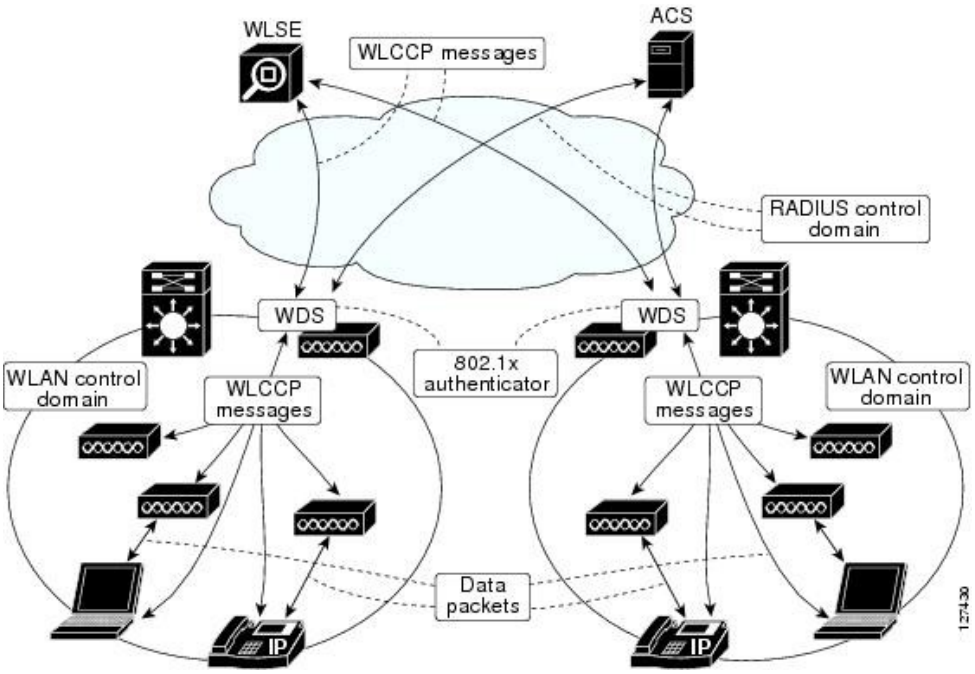


Figure 3: SWAN logical view (according to [SWANIG])

Additionally, both concepts can be expanded using CiscoWorks Wireless LAN Solution Engine[4] appliance, enabling monitoring and optimization of radio coverage, detecting rogue wireless hardware and simplifying management.

Within the SWAN framework, all components are authenticated using EAP and encryption keys are established, enabling secure transport of confidential data. Two modes of authentication must be differentiated:

- Infrastructure Authentication (IA) applies to infrastructure devices like Access Points, WDS Master or WLSE, while
- Client Authentication applies to all Mobile Nodes.

Client authentication can be operated using almost any EAP authentication method that establishes encryption keys and is compatible with Cisco Centralized Key Management (CCKM), while Infrastructure Authentication is determined to use Cisco Lightweight Extensible Authentication Protocol (LEAP).

Functions delivered by the SWAN framework are entitled as Wireless Domain Services (WDS), which represents the technical term to mark up corresponding installations and roles within. As companies may have more than one (e.g. for branch office) wireless network, each segment, that is coordinated by a WDS master, is referred to as a WLAN control domain.

2.2.2 SWAN Protocols

Three protocols map the needed communication processes within SWAN's framework into data packets:

- EAPoL/ EAP: Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) transport authentication messages, produced by EAP methods.
- RADIUS: The Remote Authentication Dial-In User Service (RADIUS) protocol transports EAP method data between WDS Master and Authentication Server.
- WLCCP: All authentication, management and monitoring traffic which is related to SWAN's framework is transported using different message types of Wireless LAN Context Control Protocol (WLCCP).

[4] *WLSE – product details available under http://www.cisco.com/en/US/products /sw/cscowork/ps3915*

RADIUS transports authentication data between WDS Master and Authentication Server and is considered to be beyond the focus of this paper.

2.2.3 SWAN Topology

SWAN's topology is reflected in WLCCP's roles and topology, partially defined by US Patent Application 10/417,653 (available under [USPAP1]) and US Patent Application 11/121,633 (available under [USPAP2]). These define a tree structure, which includes three Context Managers, Campus Context Manager (CCM), Local Context Manager (LCM) and Sub Context Manager (SCM), as well as Access Points and Mobile Nodes. Role impersonation, by network devices, depends on whether switched or non-switched deployment mode is chosen. For non-switched mode CCM and LCM are omitted, so that SWAN's root node is represented by an Access Point claiming SCM's role (denoted by [USPAP2] Section [0067]).

2.2.4 SWAN Key management

Using EAP based authentication, key material is generated dynamically every time Mobile Nodes authenticate successfully to a wireless network. Unfortunately this authentication and key derivation process, does not incorporate with low latency application requirements like Voice over IP (VoIP), as authentication and key derivation processes can take up to several seconds while roaming.

Cisco's Fast Secure Roaming feature resolves this issue by using a modified Reassociation process, involving Cisco Centralized Key Management (CCKM).

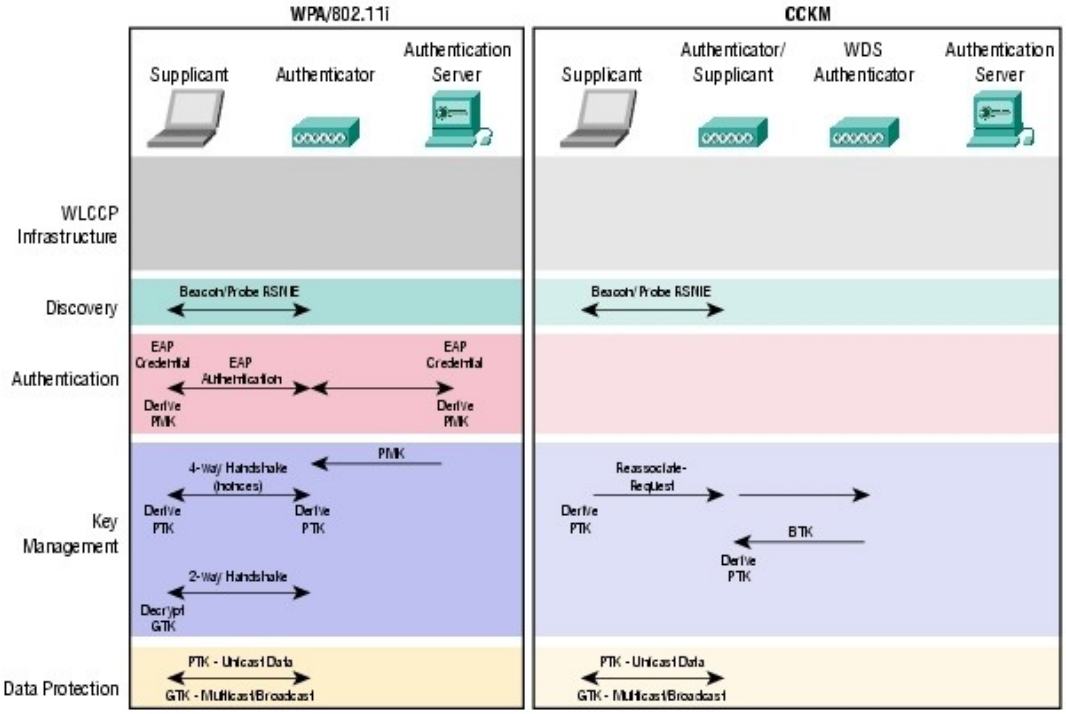


Figure 4: Comparison CCKM and Standard 802.11 Key Management

Significant speed improvements are achieved by caching keying material within the WDS Master node, and therefore skip RADIUS based communication between Authenticator and Authentication Server. As shown in Figure 4, Reassociation defined by the 802.11i standard includes a full authentication scheme, including key derivation, when roaming between Access Points. CCKM capable clients send Reassociation Requests which are authenticated using the Key Refresh Key (KRK), known to the WDS Master.

Assumed that the Reassociation Request can be verified successfully, WDS Masters will forward the Base Transient Key (BTK) to the Access Point the Mobile Node roamed to. This enables Access Points derive encryption keys used to encrypt data on wireless interfaces. As the BTK did not change, MN's are able to derive encryption keys right after deciding which Access Point they will roam to. Finally an AP's Group Transient Key is encrypted and transmitted to the Mobile Node.

Forwarding cryptographic material is considered to be a highly security critical process. Especially when cryptographic keys should are transported. Therefore SWAN establishes so called Context Transfer Keys (CTK) that enable encryption and authentication between Access Points and their corresponding controller.

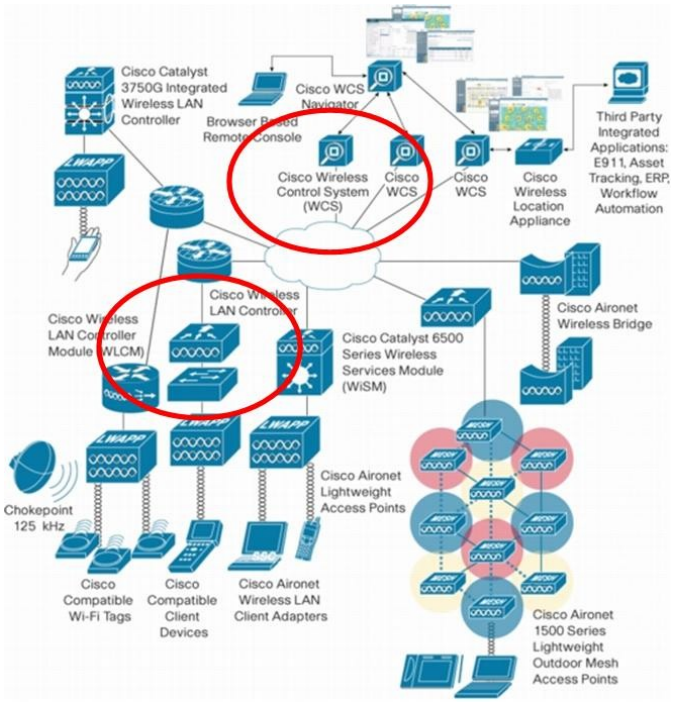
2.3 Short Technical Overview of CUWN world (as of early 2010)

Key features listed by Cisco include the security of transmitted data, ease of deployment and administration as well as advanced RF monitoring. Within the "Cisco Unified Wireless Network Concept" several products leverage certain functionalities. Besides mobile clients these are mainly Access Points (AP), Wireless LAN Controllers (WLC) and the "Cisco Wireless Control System" (WCS). Enabling centralized services within wireless networks furthermore requires certain protocols and corresponding software support. Within a Cisco WLAN installation "Simple Network Management Protocol" (SNMP) and "Control and Provisioning of Wireless Access Points" (CAPWAP) represent the supporting protocols that enable centralized management.

From a conceptual point of view, Access Point functionality is distributed over two devices. Access Points handle all wireless to wired transition of network packets as well as wireless announcement. All management tasks, including association, disassociation, etc. are provided by a Wireless LAN Controller, who handles several Access Points at a time.

CAPWAP is used to transmit Access Point control and status messages, as well as to encapsulate data frames originating or destined to wireless client. This protocol is only spoken between Access Points and Wireless LAN Controllers. Additionally configuration of Access Points is centralized by deployment through the WLC. AP's that operate with WLC's are so-called Lightweight Access Points (LAP).

As companies may need several controllers for performance reasons as well as different locations, unified configuration and centralized monitoring are key features for secure operations. Cisco's "Wireless Control System" is capable of monitoring several WLC's, as well as deploy company wide configuration on all devices. It enables centralized administration and monitoring, including Intrusion Detection and Radio Frequency Monitoring. Communication between WCS and WLC is supported by the use of SNMP.



3 GENERIC ATTACK PATHS AND VULNERABILITIES

The following chapter shows possible attack vectors and associated vulnerabilities in detail. Some of them apply only to the CUWN world.

3.1 Access to wireless transmitted packets

Wireless networks transmit data using radio waves on defined frequencies. Limiting the wireless coverage is a nearly impossible task. Coverage depends highly on the equipment end other environmental factors.

3.1.1 Eavesdropping

Eavesdropping (sniffing) packets belonging to wireless networks is possible as soon as an attacker is within reach of a wireless network. Coverage can generally be increased by using enhanced antennas on receiver side. Therefore eavesdropping of wireless packets is generally regarded as being possible. Critical data should always be encrypted before transmitted over wireless networks.

3.1.1.1 Associated risk: Low

Attackers are able to eavesdrop wireless communication. Eavesdropping on wireless networks is a passive attack; therefore it is impossible to prevent this kind of attack.

As long as the encryption keys are not known by an attacker, she would not able to decrypt the data captured.

3.1.2 Rogue AP's

Wireless networks identify themselves to end user by their configured Extended Service Set Identifier (ESSID). ESSID's are shaped in form of character strings, mostly representing the name of a company/ institute offering wireless network connectivity. ESSID's can be configured as liked, and hence be used by attackers to impose as one certain wireless network. This may trick users to establish connections to rogue Access Points pretending to be a certain corporate wireless network. During this operation users may send valid credentials to rogue AP's, resulting in compromise of these credentials.

3.1.2.1 Associated risk: Low

Rogue Access Points can be placed by attackers in arbitrary locations, some may be visually hidden. Behaviour of associating mobile clients is hardly controllable, as it requires a list of valid Access Points addressed to be deployed prior to authentication.

Cisco WLC and WCS are able to collaborate radio frequency measurement data in order to monitor wireless coverage for rogue devices and warn about new devices. These devices may be Access Points or other kind of wireless devices.

3.1.3 Rogue clients

Analog to the "rogue AP" attack path a "rogue client" attack path exists. In this scenario attackers try to impersonate a legitimate mobile client that tries to establish a wireless connection. During this process credentials may be already known or may be tried to be guessed correctly. Successful attacks may lead to unauthorized usage of wireless networks by attackers and may result in access to critical data or information.

3.1.3.1 Associated risk: Medium

Rogue clients may impose risk on authentication credentials used by mobile clients. Rogue clients may try to brute force these credentials, for example when password authentication for wireless access control is used.

Risk Mitigation can be done by the use of proper authentication schemes that do not involve passwords (e.g. authentication with digital certificates), and limitation of authentication tries within a certain time frame.

3.1.4 Manipulate OTA WLC provisioning

Lightweight Access Points need to know which Controller should be used for authenticating itself with, and where to forward data packages transmitted via the wireless network. One way to announce WLC's IP address is sending CAPWAP neighbor messages over the wireless media. As wireless medium is a shared one, manipulation of these information must be regarded as possible. This may enable attackers to redirect LAPs to a spoofed WLC.

3.1.4.1 Associated risk: None

WLC Over-the-Air provisioning is only available on certain Wireless LAN controllers. For WLC5508 this feature is unavailable.

Using decent hardware (as proposed in this document) renders this information disclosure attack impossible.

3.2 Physical access to Access Points

Access Points mark the border of wireless infrastructure towards the end user. Therefore they have to be placed a relatively close to the end user. This normally includes different types of locations from secure areas to hallways or public buildings.

Physical access may be achieved by un-mounting the Access Points from its carrier. This enables access to Ethernet and Console ports, as well as theft of the device itself.

3.2.1 Determine/ modify configuration

Physical access to Access Points may allow attackers to read configuration that is deployed on to the Access Point if no credentials for login are required. Configuration can be obtained using `show running-config`. This may include sensitive information as username and password.

Additionally configuration can be modified if access to the "enable mode" is not protected by a password. However available configuration commands are limited, as LAPs have less functionality than autonomous.

3.2.1.1 Associated risk: Low

Modification of Access Point configuration is only possible if no authentication for management interfaces is configured. As basic hardening measure authentication should always be configured in a secure fashion. Within Cisco's WLAN infrastructure authentication can be configured to check credentials via RADIUS on centralized authentication servers. Proper configuration leaves this kind of attack very unlikely.

3.2.2 Modify firmware

It must be regarded as possible access to Access Points may include possibilities to modify firmware that is executed on LAPs. Upload of software is typically performed using TFTP, defined by RFC 1350[5]. TFTP does not include any functions that enable verification of connections or transmitted data.

3.2.2.1 Associated risk: Very low

Currently there is no publicly available in-depth knowledge about Cisco IOS internals for Aironet Access Points or Wireless LAN controllers. Therefore it is regarded as unlikely that attackers are able to manipulate AP firmware.

---

[5] *http://tools.ietf.org/html/rfc1350*

3.2.3 Determine cryptographic keys

LAPs contain cryptographic keys as certificates are used to authenticate Access Points and WLCs. Furthermore they are used to establish encrypted communication channels between LAPs and WLCs. Using asymmetric cryptography this is only possible, if every device is equipped with a certificate and corresponding private key.

According to Cisco's documentation, keys are computed during manufacturing process and stored within LAP hardware. It must therefore be regarded as possible that these keys can be retrieved through reverse engineering and/ or disassembling.

3.2.3.1 Associated risk: Low

According to information provided by Cisco, the private key of an AP's cert is stored within a secure area of flash memory. Retrieving this key through IOS commands is impossible. Attackers that are very firm with the hardware platform used in this Access Points may be able to retrieve this key.

Deploying certificates, signed by a designated Certification Authority can easily render this kind of attack ineffective, as Certificate Revocation Lists can be used to declare possibly compromised keys as invalid.

3.3 Access to wireless distribution network

The so called "wireless distribution network" connects Access Points and their corresponding Wireless LAN Controller. This network is commonly wide-spread throughout a campus to provide Access Point's connectivity. Neglecting physical security of LAPs may enable attackers to participate in this network, e.g. by unmounting/un-cabling Access Points. As members of this network are mostly regarded as static, further security measures to control network access are rarely deployed.

3.3.1 Spoofing DHCP Server for APs

Access Points can be configured to obtain IP configuration by the "Dynamic Host Configuration Protocol" (DHCP). It is common to configure DHCP servers to transmit WLC IP addresses during DHCP packet exchange. If no further security measures were deployed, attackers with physical access may impose as DHCP servers within this segment. This way they are able to assign different IP and WLC configurations to Lightweight APs. This can either lead to Denial-of-Service situations, as Access Points are not able to contact their WLC.

3.3.1.1 Associated risk: Medium

Attackers being able to gain access to network segments that connect APs and WLCs are easily able to conduct this attack. Impact is very likely to differ from DoS to possible compromise of the whole environment through introduction of malicious/ rogue wireless infrastructure hardware.

Risk can be mitigated using appropriate authentication methods for network devices, as 802.1X. Attackers being able to gain physical access to network cables originally belonging to Access Points will then be blocked by network infrastructure, rendering the attack impossible.

3.3.2 Manipulate WLC detection

According to Cisco[6] Lightweight Access Points can discover a WLC IP address by certain mechanisms:

- Layer3 CAPWAP discovery
- Locally stored controller IP address
- DHCP server discovery
- DNS discovery
- Over-the-air-provisioning (OTAP)[7]

[6] *http://www.cisco.com/en/US/docs/wireless/wcs/5.2/configuration/guide/5_2ovrv.html#wp1145760*

Assuming access to the wireless distribution network all network based discovery mechanisms can be manipulated, as none of the protocols used includes authentication mechanisms. This includes DNS, DHCP and Layer3 CAPWAP discovery.

3.3.2.1 Associated risk: Medium

As all (except locally stored controller IP address) mechanisms depend on protocols that do not offer authentication and integrity services, manipulation is possible, if attackers are able to inject this kind of traffic

802.1X can mitigate this kind of attack completely, as traffic originating from the attacker is blocked until the attackers has successfully finished authentication.

3.3.3 Redirect traffic with ARP Spoofing/ Routing attacks

Ethernet plus IP is the most wide spread combination of Layer 2 and Layer 3 network protocol. It's also the base set of communication protocols for CAPWAP. As Ethernet and IP use different addressing schemes an automatic translation mechanism needs to be in place. It is called "Address Resolution Protocol" (ARP). ARP does not contain any packet authentication, enabling attackers to spoof ARP answer packets, containing invalid IP to MAC address combinations.

3.3.3.1 Associated risk: Medium

The ARP mechanism depends on a protocol that does not offer authentication and integrity services, so manipulation is possible, if attackers are able to inject this kind of traffic.

802.1X can mitigate this kind of attack completely, as traffic originating from the attacker is blocked until the attackers has successfully finished authentication.

3.3.4 Denial of Service

Attackers may execute Denial-of-Service attacks within the wireless distribution network to interrupt proper functionality. These attacks may be carried out in a variety of different combinations. Mostly these attacks try to interrupt/ disturb communication between AP and WLC, rendering the wireless interface unusable.

3.3.4.1 Associated risk: Low

Denial of Service attacks may be conducted in several ways, leaving the environment unusable. However, these kinds of attacks involve transmission of traffic into network segments that are used for transmission of infrastructure traffic.

802.1X can mitigate these kinds of attack completely, as traffic originating from the attacker is blocked until the attacker has successfully finished authentication.

3.3.5 Read/ send syslog messages

Access Points forward local logging messages to the WLC they are associated with. This way WLCs are capable of receiving status messages from Access Points. Syslog messages are encapsulated using UDP headers. As messages are not authenticated, attackers may read, inject or manipulate these messages.

3.3.5.1 Associated risk: Very Low

Syslog can not be configured to authenticate, nor encrypt messages transported over the network. As no functionality directly depends on Syslog messages impact of spoofed Syslog messages is very unlikely.

---

[7] *Only supported on Cisco 4400 series controllers. Support for this feature has been removed for 5500 series controllers as of release 6.0.188.0 (see http://www.cisco.com/en/US/docs/wireless/controller/release/notes/crn6_0_188.html)*

3.3.6 Man-in-the-Middle attacks on CAPWAP connections

Data exchanged between Access Points and Wireless LAN Controllers can be divided in two groups. The first type is a control channel on which Access Points and WLCs exchange information like current status, configuration changes, cryptographic keys and other information. In combination with ARP spoofing a redirection of this channel may be possible, resulting in access to critical infrastructure information to attackers. Based on this information security of wireless transmitted data may be at risk.

3.3.6.1 Associated risk: Low

CAPWAP authentication is based on digital certificates. This authentication scheme is known to be fairly secure. However infrastructure devices are equipped with a vendor generated certificate. If this certificate is not replaced by company related certificates and/ or 802.1X is not in place attackers may be able to establish CAPWAP connections that can not be declared as rogue in an automated fashion.

3.3.7 Read data transmitted on wireless

The second channel between APs and WLC's is represented by the data channel. Data transmitted to/ from wireless client is encapsulated using CAPWAP. With access to the wireless distribution network attackers may be able to intercept and/ or modify this data. Successful attacks may impact on confidentiality and/ or integrity of data transmitted over the wireless medium.

3.3.7.1 Associated risk: Medium

This scenario will most likely happen in combination with ARP spoofing, decreasing the chance of possible attacks through higher attack complexity. Rendering ARP attacks impossible, also render this kind of eavesdropping impossible.

Through the use of proper mitigating controls, as 802.1X based network authentication and centralized decryption of wireless traffic this kind of attack can be regarded as unlikely.

3.4 Access to WLC management network

Wireless LAN Controllers can be administered by the use of a separate network interface. Communication to web interface as well as communication with WCS is transmitted over this interface. Security of this interface is heavily relevant for the security of the whole wireless infrastructure.

3.4.1 Inject SNMP messages

Management actions are mapped from WCS to each WLC through the use of SNMP. A wide variety of different Management Information Base's (MIB) are available to administer WLC's functions. Some of these have direct impact on Access Point and wireless network configuration options, such as encryption and authentication type.

If SNMP messages are not authenticated (which is the case with SNMP v1 and v2c) attackers that are able to send SNMP messages to either WLC's or WCS are able to change status and configuration of the complete wireless environment. This may result in re-configuration of wireless security algorithms to insecure settings. This would directly impact confidentiality and integrity of data transmitted over wireless interfaces.

3.4.1.1 Associated risk: Medium

This kind of attack depends on SNMP configuration. Version 2c of SNMP protocol does not involve authentication or encryption of transported messages. Community strings can easily be guessed and a wide range of common terms exist. Impact is regarded as fairly high, because all configuration tasks originating from WCS are mapped to SNMP MIBs.

SNMP configuration must be secured separately, as default configuration involves SNMP v2 with community string based authentication, using "public" for read and "private" for read/ write access.

Overall risk is regarded to be medium as WLC and WCS are normally located within secure areas like data centre and network segments connecting these devices are uncommon to be available to attackers.

3.5 Software vulnerabilities

WLC, Access Points, WCS and mobile clients rely on functionality which is implemented in software. Most parts of this software are developed by Cisco and are regarded to be “new”. This is (for example) reflected by the “early deployment” classification of WLC 5508 operating system. This software should be regarded to be not failure proven. These failures may include security relevant impacts, revealing confidential data to attackers.

3.5.1.1 Associated risk: Low

Software vulnerabilities may impose risk of overall security of infrastructure. As hardware for this infrastructure is high-priced, availability to hackers is regarded to be very unlikely. Therefore most software vulnerabilities may be discovered during normal usage by troubleshooting availability issues. Overall risk of unknown software vulnerabilities is therefore regarded as unlikely but not impossible.

4 ATTACKING THE SWAN WORLD: EXPLOITING WLCCP

The following chapter describes attacks against WLCCP, which enables attackers to retrieve encryption keys and break and/or manipulate security mechanisms within the SWAN framework. Implications on these attacks result in the possibility to decrypt protected WLCCP traffic that contains security relevant information such as wireless encryption keys.

4.1 Interfere with election of WDS master

By means of a self-written packet crafting tool (using a higher priority), it was easily possible to take over the WDS master role in a given network.

4.2 Attacks on intra-AP communication – Test environment

For research purposes, a separated environment is used, to reduce side effects on running installations and their stability. This security evaluation took place in a separated, private network segment configured with the address 192.168.88.0/ 24.

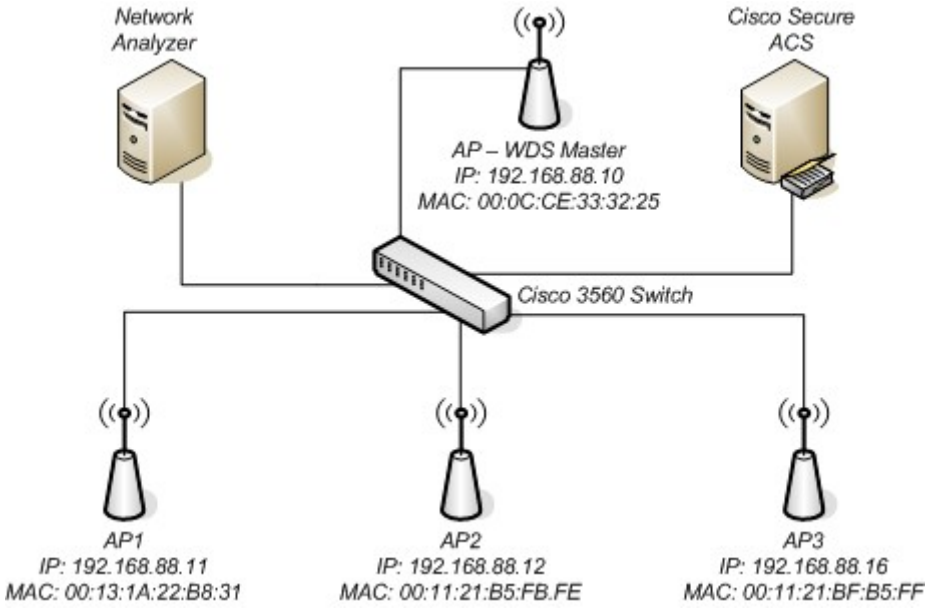


Figure 5: Test environment

The setup is composed of the following components:

- Four Cisco 1231 Access Points, IOS Version 12.3(8) JEC1
- One Cisco Secure Access Control Server (ACS), Version 4.2(0) Build 124
- One Cisco 3560 Switch, IOS Version 12.2 (40) SE
- One Windows XP PC, running Wireshark for Network packet analysis

Using Cisco's Switched Port Analyzer (SPAN) (Configuration Guide as available under [CSPAN]) function, a monitor is configured that copies incoming packets on network ports of Access Points and Secure ACS to the Network Analyzers port[8].

Authentication Server, WDS Master AP and Infrastructure AP's configuration have been extracted from [CWDS], Chapter "Configuring WDS" and been applied using Command Line Interface, where applicable.

[8] *See Appendix C for Configuration Example.*

4.3 Attacks on intra-AP communication – Requirements

The described attacks require network access to the segment that connects Access Points. As Access Points in large environments are spread throughout buildings and campuses, this segment subsists nearly everywhere, having cable ends in mostly unsafe ambiances. Without special precaution steps taken, like security brackets for network and power cables, attackers can use existing cabling to intrude this segment.

Furthermore extended knowledge of the network analyzer Wireshark and the protocol WLCCP is key requirement to lay out successful attacks. This is especially true, as Wireshark can only interpret WLCCP on a rudimentary level[9]. Availability of automated programs that enables attackers to carry out attacks in easier fashion, are regarded as feasible by the author.

4.4 Discovering the WDS Master

According to [USPAP1], Section [0535], a Sub Context Manager is elected "for each subnet […] to advertise network availability and network parameters". Advertisement is facilitated by sending SCM Advertisement Reply Messages with SCM Active Flag set, to the IEEE 802.3 address 01:40:96:FF:FF:C0 in periodic intervals of 5 seconds:

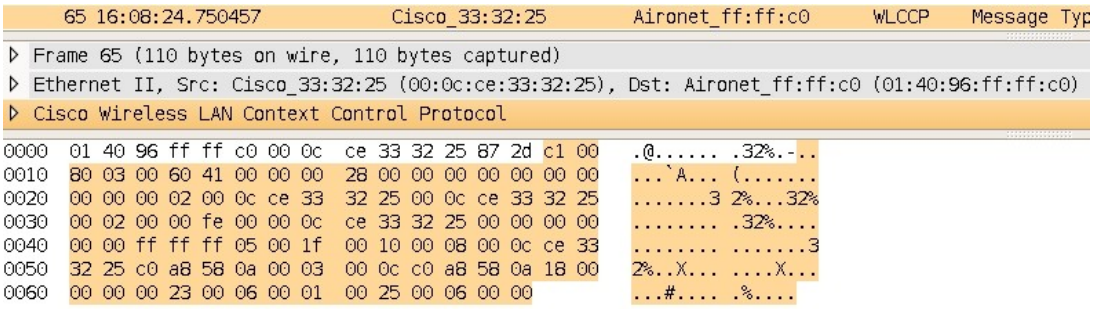


Figure 6: SCM Advertisement Reply examined with Wireshark, Version 1.1.3

Mapping bytes of the shown packet to the WLCCP Advertisement Reply Message format, reveals the MAC address of the active SCM, which is 00:C0:CE:33:32:25 corresponding to the environment setup, and its priority value 0xFE which corresponds to 127[10].

Furthermore four TLV's are appended to the packet in the order of their description:

- WTLV_ROOT_CM_INFO (TLV type 0x001F), starting at byte 0x0046 with a total length of 16 bytes, containing the MAC address 00:C0:CE:33:32:25 and IP address 192.168.88.10 of the Root CM, which is, in case of this setup, equal to SCM's address.
- WTLV_IPV4_SUBNET_ID (TLV type 0x003), starting at byte 0x0056 with a total length of 10 bytes, containing the IPv4 address of SCM and its configured Subnet Mask (0x18 corresponds 255.255.255.0) in the Prefix Length field. This TLV is padded by two 0x00 Bytes.
- An undocumented[11] TLV type of 0x0023 with a total length of 6 bytes, transporting two bytes data: 0x0001. As no Advertisement Reply Messages with different values were observed, this value is assumed to be constant.
- A 6 byte long undocumented TLV of type 0x0025, which is observed to have a constant value of 0x0000.

---

[9] *As at June 2009 only SCM Advertisements and Path Authentication messages can be (partly) dissected using Wireshark.*

[10] *Remember that Bit 0 is the Preferred Flag, which is to 1, leaving Bit 1 – 7 for the priority value.*

[11] *Undocumented represents the fact that this TLV type is neither documented in [USPAP1] nor in [USPAP2].*

4.5 Discovering Infrastructure Access Points

The Sub Context Manager role pictures the direct ancestor within the WLCCP tree for Infrastructure Access Points, who reside in the same Ethernet segment, as shown in [USPAP1] Figure 17. Its existence can be determined as described by Chapter 4.4. With IP address and subnet mask that can be extracted from these packets, it is possible to actively search for Infrastructure Access Points.

This search can be done using several methods. Most obvious would be trying to use the Packet Internet Groper "ping" command[12]. However it is possible to use Access Lists[13] to filter this type of packets and thereby disabling successful discovery. More accurate results will be obtained with a scan technique called ARP scan. This technique benefits from the fact, that network devices communicating via IP must use the ARP mechanism to resolve the MAC address of the packet receiver (Chapter 3 gives an Introduction to ARP). Therefore every networked device must reply to ARP Requests. Checking the aliveness of a certain IP address can therefore be done sending ARP requests. As messages, described by Chapter 4.4, give detailed information about the IP subnet all required parameters for this scan are available.

```
wlccp-logging-server:~/software/arp-scan-1.7# nmap -PR -sU -p2887 192.168.88.0/24

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009-06-30 00:40 CEST
Interesting ports on 192.168.88.1:
PORT     STATE  SERVICE
2887/udp closed unknown (1)
MAC Address: 00:0C:29:A0:F6:1B (VMware)

Interesting ports on 192.168.88.2:
PORT     STATE  SERVICE
2887/udp closed unknown (2)

Interesting ports on 192.168.88.3:
PORT     STATE         SERVICE
2887/udp open|filtered unknown (3)
MAC Address: 00:40:63:E3:19:BC (VIA Technologies)

Interesting ports on 192.168.88.10:
PORT     STATE         SERVICE
2887/udp open|filtered unknown (4)
MAC Address: 00:0C:CE:33:32:25 (Cisco Systems)
```

Figure 7: Results of host discovery via "nmap"

Combining nmap's (available for download at [NMAP]) scan functions enables to search for Infrastructure Access Points. The parameter set shown in Figure 7 specify that nmap should do an ARP scan (parameter "`-PR`") first, followed by an UDP scan on port 2887 (parameter "`-sU -p2887`"). Port 2887 represents the port of the UDP protocol which is used for IP/ UDP encapsulated WLCCP packets.

As the ARP scan may find active network devices which are not Infrastructure Access Points, it is necessary to check every host of the nmap result for the following output:

- Port 2887 must be in state "open|filtered"
- The MAC address must be denoted as "Cisco Systems"

If both checks are true, a found network device is most likely an Infrastructure Access Point[14], compare to result number "(4)".

---

[12] *This command sends an ICMP echo request message to the specified IP address and waits for a corresponding ICMP echo response. Receiving a response indicates that the IP address is reachable. See [RFC1208] for definition.*

[13] *[CIPACL] gives an introduction Cisco's concept of Access Lists and their usage for network infrastructure protection.*

[14] *However it is possible that these results can be identical on some other Cisco devices. Due to the mass of different devices it was impossible for the author to test every combination.*

4.6 ARP Spoofing attack against Cisco IOS

The algorithm for ARP packet handling (see [RFC826], Chapter “Packet Reception”) defines that network devices should update ARP’s Translation Table every time they receive an ARP packet, regardless if they are the requested recipient or type of operation (Request/ Response). Therefore all [RFC826] conforming ARP implementations are vulnerable to arbitrary manipulation of their ARP translation table by any device that is connected to the same Ethernet segment. Crafted ARP packets with spurious IP/ MAC address mappings will result in update to the Translation Table.

Practical attacks can be carried out using the `arpspoof` command, which is included in dsniff’s [DSNIFF] tool collection by Dug Song. Arpspoof implements ARP spoofing attacks, by sending ARP Reply message to the target host (specified with parameter “-t”), claiming that IP address given on command line should be mapped to the MAC address of the network interface card the packets are sent from (parameter “`-i`”). Attackers MAC address during attack shown by Figure 16 is 00:0C:29:9C:3C.CC.

```
wlccp-logging-server:~/software/arp-scan-1.7# arpspoof -i eth1 -t 192.168.88.16 192.168.88.10
0:c:29:9c:3c:cc 0:11:21:bf:b5:ff 0806 42: arp reply 192.168.88.10 is-at 0:c:29:9c:3c:cc
0:c:29:9c:3c:cc 0:11:21:bf:b5:ff 0806 42: arp reply 192.168.88.10 is-at 0:c:29:9c:3c:cc
0:c:29:9c:3c:cc 0:11:21:bf:b5:ff 0806 42: arp reply 192.168.88.10 is-at 0:c:29:9c:3c:cc
0:c:29:9c:3c:cc 0:11:21:bf:b5:ff 0806 42: arp reply 192.168.88.10 is-at 0:c:29:9c:3c:cc
0:c:29:9c:3c:cc 0:11:21:bf:b5:ff 0806 42: arp reply 192.168.88.10 is-at 0:c:29:9c:3c:cc
0:c:29:9c:3c:cc 0:11:21:bf:b5:ff 0806 42: arp reply 192.168.88.10 is-at 0:c:29:9c:3c:cc
```

Figure 8: ARP spoofing attack with "arpspoof"

Verification if a device is vulnerable must be done by examining the ARP translation table before and during spoofing attacks. On Cisco IOS[15] the command “show arp” lists the ARP translation table.

```
ap_kueche#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.88.16           -   0011.21bf.b5ff  ARPA   BVI1
Internet  192.168.88.1            0   000c.29a0.f61b  ARPA   BVI1
Internet  192.168.88.2            0   000c.299c.3ccc  ARPA   BVI1
Internet  192.168.88.10           0   000c.ce33.3225  ARPA   BVI1
Internet  192.168.88.252          0   0018.bab1.8341  ARPA   BVI1
Internet  192.168.88.253          0   0090.270e.a576  ARPA   BVI1
```

Figure 9: ARP translation table before ARP spoofing attack

Figure 9 lists the output before ARP spoofing attack is started, showing that IP address 192.168.88.10 is mapped to MAC address 00:0C:CE33:32:25 which conforms to the environmental setup illustrated in Figure 5. Successful exploitation of this vulnerability results in an updated entry for IP address “192.168.88.10” in the ARP translation table as Figure 10 states.

```
ap_kueche#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.88.16           -   0011.21bf.b5ff  ARPA   BVI1
Internet  192.168.88.1            0   000c.29a0.f61b  ARPA   BVI1
Internet  192.168.88.2            0   000c.299c.3ccc  ARPA   BVI1
Internet  192.168.88.10           0   000c.299c.3ccc  ARPA   BVI1
Internet  192.168.88.252          0   0018.bab1.8341  ARPA   BVI1
Internet  192.168.88.253          0   0090.270e.a576  ARPA   BVI1
```

Figure 10: ARP translation table during ARP spoofing attack

[15] *The operating system Cisco Access Points are executing.*

Interpreting the ARP spoofing test results on Cisco IOS 12.3(8) JEC1 on the Cisco 1231 Access Points reveals that IOS's ARP implementation is vulnerable to ARP translation table manipulation.

4.7 Recovering LEAP password

[USPAP1], Section [0758] states "While MNs can select from any supported 802.1X EAP authentication types, for initial releases, IN nodes shall authenticate using LEAP", limiting authentication of Infrastructure Access Points to Cisco's proprietary authentication method LEAP.

Assuming that no changes have been made to the LEAP process used by WLCCP, vulnerabilities described in [JW03] must be appropriate to WLCCP. Additionally it should be possible to use "asleap" in a similar manner than its original purpose, to retrieve authentication passwords.

4.7.1 LEAP encapsulation

Analyzing Infrastructure Authentication Process revealed, that communication between Infrastructure Access Points and Infrastructure Authenticator[16] is transported by UDP encapsulated WLCCP packets. Most likely this reflects the fact, that Campus Control Manager and Infrastructure Access Points may not share the same Ethernet segment. Interpreting Section [0778] of [USPAP1], LEAP packages that belong to Infrastructure Authentication are encapsulated using EAPoL and WLCCP_AAA headers. Combining these facts LEAP packets are encapsulated by the following cascade of headers:

Figure 11: LEAP encapsulation cascade for Infrastructure Authentication

4.7.2 Packet analysis

Using Wireshark for packet inspection supports the process of finding and understanding data fields, because of its extensive support for dissection of different network protocols. However implementation of WLCCP dissector is incomplete, as reliable results end with the WLCCP Common Context Header[17]. For this reason, packet analysis is done manually by marking parts of the byte stream that belong to certain protocols. The following packet captures are taken from Infrastructure Authentication of Access Point 192.168.88.16 against the SCM (IP address 192.168.88.10) within the test environment, described by Chapter 4.2. Analysis of Ethernet, IP and UDP headers is omitted, as these do not contain relevant information for authentication.

Figure 12 displays the first packet from Authenticator to Supplicant in step 6 of LEAP's message exchange. Protocols are highlighted by the same color mapping as introduced by Figure 11, starting with WLCCP Common Context Header. Two unknown bytes with the value 0x001B reside between WLCCP_AAA and EAPoL header. As WLCCP, WLCCP_AAA, EAPoL and EAP headers build the encapsulation chain for LEAP messages they do not transport relevant data and will therefore not be examined further.

LEAP message starts at byte 0x005C, disclosing the LEAP username "WDSuser" and 8 byte RADIUS Server Challenge Rad_{Chal} = "90 0D 74 BE 3B 38 26 64" [16].

[16] *Located in the CCM, whose role is adopted by SCM in the nonswitched deployment mode.*

[17] *This limitation of Wireshark is true up to version 1.2.0 which marks the most recent stable version as of June 30th, 2009.*

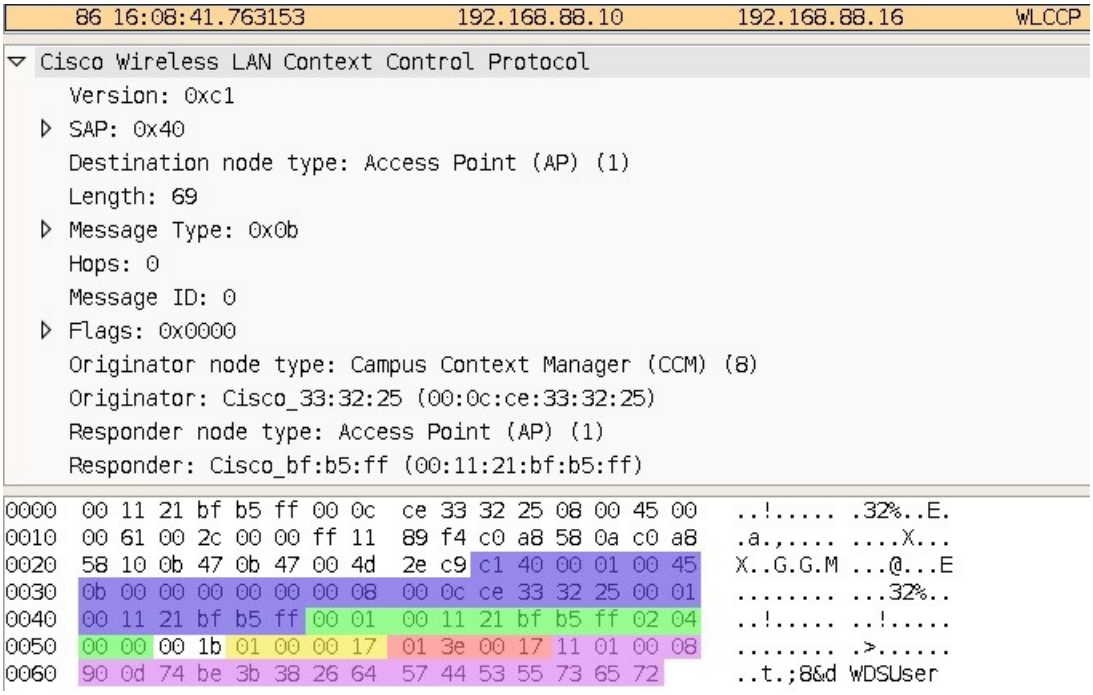


Figure 12: WLCCP encapsulated LEAP packet, transmitting 8 Byte Nonce to Supplicant

Applying LEAP encapsulation cascade to packets 87, 90 and 91 subsequently reveals the Response (Rad_{Resp}) to RADIUS Challenge, as well as Challenge (Sup_{Chal}) and Response (Sup_{Resp}) initiated by the Infrastructure Access Point:

- Rad_{Resp} = "24 AE 72 0F 57 1D DC FD D7 4D F0 FC 85 F9 AA F0 A8 6C 59 4A 95 7B 20 78" $_{16}$
- Sup_{Chal} = "5C 57 0B 03 03 E0 BC 28" $_{16}$
- Sup_{Resp} = "96 F6 25 EB D3 60 F7 1C 1E E1 39 FB AE 33 D9 B1 79 3B 8B C2 9D A3 87 74" $_{16}$

4.7.3 Cracking Infrastructure Authentication passwords by means of *asleap*

Joshua Wright depicts the process of cracking LEAP passwords in [JW03] with the following steps:

- Calculate MD4 hashes for given password lists to create password + NT-Hash mappings.
- Capture LEAP Challenges and Responses.
- The last DES Keys contains 2 byte non-zero data; compute the 2^{16} binary combinations and encrypt the challenge with each.
- Compare all encrypted challenges to the last 8 byte of the Response reveals the binary combination of the last two bytes of the LEAP password hash.
- Compare two byte binary combination to the last two bytes of pre-calculated password hashes. Conformity indicates a password candidate.
- Decrypt Response with all password candidates and compare results to captured Challenge. Corresponding values reveal the LEAP password.

This attack is implemented in the command line utility `asleap` ([ASL]). However as this attack is based on given wordlists, prosperity of an attack is not guaranteed due to limitations in

computing resources[18]. Using the Rad_{Chal} and Rad_{Resp} values from Chapter 4.7.2 in combination with a sufficient wordlist[19] can disclose the Infrastructure Authentication password.

```
22:46:50 #13 > ./genkeys -r wordfile.txt -f wordfile.dat -n wordfile.idx
genkeys 2.2 - generates lookup file for asleap. <jwright@hasborg.com>
Generating hashes for passwords (this may take some time) ...Done.
13 hashes written in 0.21 seconds:  63.31 hashes/second
Starting sort (be patient) ...Done.
Completed sort in 0 compares.
Creating index file (almost finished) ...Done.
dante@phoenix.blechhirn.net> /ablage/documents/ERNW/research/cisco_wlan/coding/asleap-2.2
22:47:12 #14 > ./asleap -C 90:0D:74:BE:3B:38:26:64 -R 24:AE:72:0F:57:1D:DC:FD:D7:4D:F0:FC:85
:F9:AA:F0:A8:6C:59:4A:95:7B:20:78 -f wordfile.dat -n wordfile.idx
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
        hash bytes:        2011
        NT hash:           ad70819c5bc807280974d80f45982011
        password:          123qwe
```

Figure 13: Cracking Infrastructure password with asleap

Figure 13 shows the two steps for cracking LEAP password with asleap. First a password + NT-Hash list is computed using `genkeys` with the wordlist file "wordlist.txt" delivering a hash file ("wordlist.dat") and an index file ("wordlist.idx"). Executing `asleap` with location of hash and index file as well as the Rad_{Chal} and Rad_{Resp} value executes the attack.

4.7.4 Re-Compute EAP Network Session Keys

EAP standard documents require EAP methods to create encryption and authentication keys, in the case they should be used to secure wireless networks. This requirement is also true for Cisco LEAP, which creates the Network Session Key (NSK) by applying the MD5 function to exchanged Challenges, Responses and the double hashed LEAP password. [MCNAL] describes key derivation to work like this:

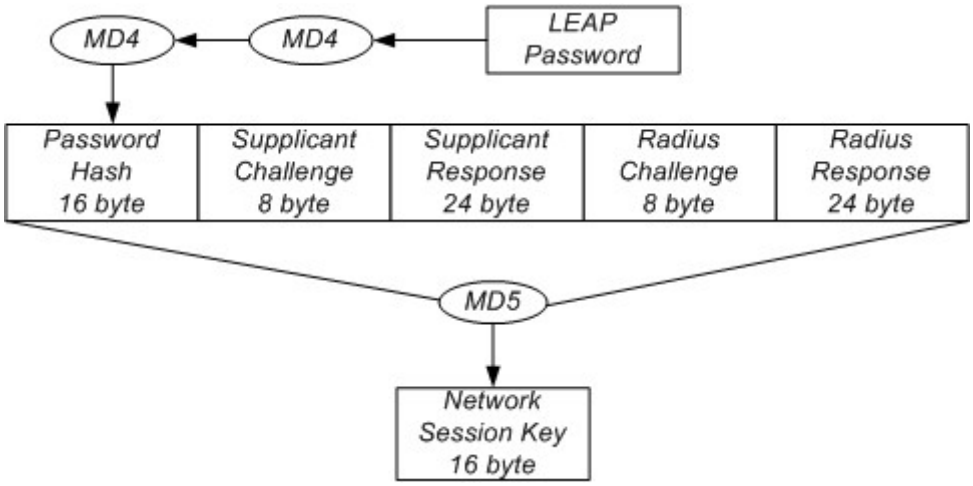


Figure 14: LEAP NSK derivation

LEAP's password is hashed using Rivest's MD4 algorithm two times. The resulting 128 bit value complies with PwHash = MD4(MD4(LEAP-Password)), while LEAP-Password is denoted in its Unicode representation.

The PwHash value is concatenated with the two Challenge and Response values, resulting in an 80 byte value PreNSK defined as:

---

*[18] MD4 produces 128 bit long hash values, therefore the number of different hashes constitutes 2^{128}. Assuming 16 byte for storage of the hash and 16 byte for the corresponding password the required storage for a complete password + NT-Hash list would approximately be (2^{128} * 32 Bytes) / 1024^3 = 10 141 204 801 825 835 211 973 625 643 008 Gigabytes.*

[19] Google can support in wordlist creation, as large wordlists are published on the internet, mostly sorted by topics as names, fictional characters or special subjects.

$$PreNSK = PwHash \,||\, Sup_{Chal} \,||\, Sup_{Resp} \,||\, Rad_{Chal} \,||\, Rad_{Resp}$$

"||" is defined as concatenation of characters. Application of Rivest's MD5 hash algorithm derives the 16 byte long NSK from PreNSK:

$$NSK = MD5(\text{ Pre-NSK})$$

However within WLCCP NSK's are not used for encryption or authentication of security critical messages, but for derivation of a second key type: Context Transfer Keys (CTK).

4.7.5 Re-Compute Context Transfer Keys

[USPAP1], Section [0777] states: "Since LEAP is known to be susceptible to dictionary attacks, as well as good security practice, a CTK must be mutually derived to protect data exchanged between the IN and IN Authenticator". This references work, mentioned above, by Cameron MacNally and Joshua Wright making it possible to break LEAP security and determine LEAP's password, given the Challenge and Response values exchanged during authentication are known.

Furthermore combining [USPAP1] Sections [0095], [0279], [0520], [0829], [0851] and [0870] defines that Path Authentication should be done by Request/ Response message exchange, where Supplicant and Infrastructure Authenticator (IA) supply a 16 byte Nonce value. The general message format is described as:

- WLCCP Common Context Header
- Path-Authentication Header
- WTLV_INIT_SESSION Type-Length-Value container.
- WTLV_IN_SECURE_CONTEXT_REQ TLV container within the Request Message or WTLV_IN_SECURE_CONTEXT_ REPLY embedded in the Response Message.
- WTLV_MIC securing each message with a Message Integrity Check (MIC) value, calculated on the NSK.

Destination-ID (DID) and Supplicant-ID (SID) fields in the WTLV_ IN_SECURE_CONTEXT_REQ and WTLV_IN_SECURE_CONTEXT_REPLY accord to Infrastructure Authenticator and authenticating Access Point. DID additionally maps to SCM-ID field in Figure 15, while SID maps to AP-ID field. The format for all these ID fields corresponds to the 8 byte Node-ID format.

Computation of CTK's is defined as shown in Figure 15.

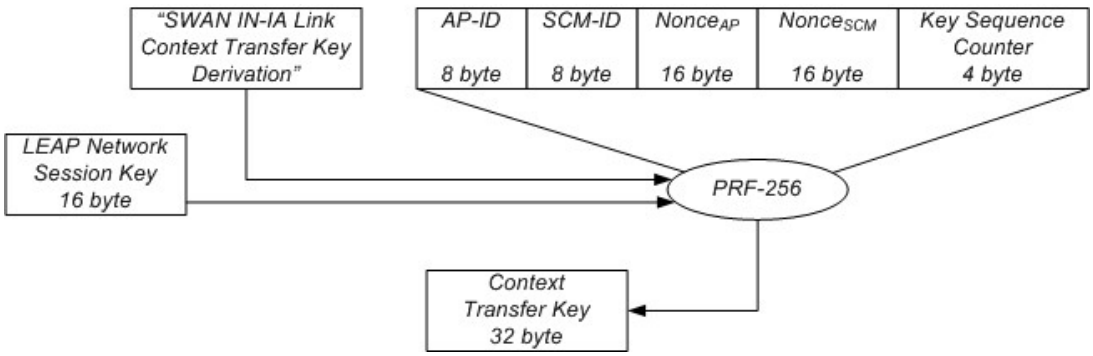


Figure 15: WLCCP Context Transfer Key derivation

"PRF-256" refers to the Pseudo Random Number (RPF) function, defined by [80211I] page 197 and following, returning a pseudo-random encryption key of 256 bit length, using HMAC with SHA-1 (HMAC-SHA1). Within wireless specification this PRF function constitutes the standard for key computation and is defined as:

```
PRF(K, A, B, Len)
    for i = 0 to (Len + 159)/ 160 do
        R = R || HMAC-SHA-1(K, A || Y || B || i)
    return L(R, 0, Len)
```

PRF is able to compute encryption keys for different key sizes, while the desired key length is passed in the Len parameter to the function. "||" is consistent with notation used in Chapter 4.7.4 and refers to the concatenation of values.

Parameter Y is of single octet length, always containing 0x00, while A is a unique label, enabling high randomness between different key types. Infrastructure Authentication in WLCCP uses the text label "SWAN IN-IA Link Context Transfer Key Derivation" as value for parameter A.

A further one byte parameter is used as last parameter in the concatenation of HMAC-SHA-1 parameters. This ensures that return value computed by HMAC-SHA-1 after each single PRF iteration is different. Practically it is mapped to the counter value i of PRF.

Parameter K is passed from the PRF function call without modification to the call of HMAC-SHA-1 and represents the password that is used by HMAC. The NSK (described in Chapter 4.7.4) delivers the value for this key.

According to [USPAP1], Figure 7 the Key Sequence Counter (KSC) value is set to 0x0001 during first Infrastructure Authentication, which can be affirmed when examining the corresponding network packet.

Remaining byte values shown in Figure 15 (AP-ID, SCM-ID, $Nonce_{SCM}$, $Nonce_{AP}$ and Key Sequence Counter) are concatenated in the order shown above, and passed as parameter B. Values for these parameters are taken from the WTLV_IN_SECURE_CONTEXT_REQ and WTLV_IN_SECURE_CONTEXT_ REPLY respectively.

[80211I] page 197 defines L(Str, F, L) as the binary string of Str, "starting from the left, extracting bits F through F+L-1, using the IEEE 802.11 bit conversion […]". Calling this function with a values F=0 and L=Len returns the first Len-1 bits of Str starting at the most left bit.

As PRF defines a pseudo random number function with desired key length as parameter, coherence to PRF-256 is induced by the following definition:

$$PRF\text{-}256(K, A, B) = PRF(K,A, B, 256)$$

Packet 94 displays a Path Authentication request message as described above. However applying the described header structure to this packet reveals inconsistencies.

- Bytes 005E – 005F do not correspond to the WTLV_IN_SECURE_ CONTEXT_REQ TLV header. Their value need to be 0x0102, but is 0x0000. The TLV header for WTLV_IN_SECURE_CONTEXT_REQ is located at bytes 0060 – 0061.
- Bytes 0088 – 0089 are denoted with value 0x2C8F, which does not correspond to the WTLV_MIC TLV header, whose value is 0x0108.
- Bytes 008A – 008B value is 0xCDD5, which, interpreted as integer value for the TLV length field, corresponds to 52693. However this TLV length exceeds maximum packet length for IP of 1500 Bytes.
- In consequence of the two byte padding at 005E, two bytes at the end of WTLV_MIC are missing.
- Byte 0094 – 0095 should contain 0x0008 according to [USPAP1], Section [0829] as this field denotes the MIC length, however the hexadecimal value 0x2395 differs.
- According to [USPAP1] Section [0825] the TLV type value referencing a WTLV_MIC Type-Length-Value container is 0x0108. However this hexadecimal value can not be found beyond byte 0045, which marks the end of the WLCCP Common Context Header.

Applying the header structure for Path Authentication Reply messages described above, reveals additional inconsistencies:

- Length of the WLCCP package, including the WLCCP Common Context Header should be 152 byte, while described package is only 144 bytes long.

- Bytes 005E – 005F show the same discrepancy as described in the Path Authentication Request message.
- Bytes 008C – 008D correspond to the CTK key length, where a hexadecimal value of 0x7D7D (32125 in decimal) is approximately 32KB. Keys of that size can not be used by the RC4 encryption algorithm.
- The following 32 byte corresponding to the CTK (bytes 008E – 00AD) contain 0x00 values which are untypical for encryption keys, as they would reduce the key size.
- Applying the WTLV_IN_SECURE_CONTEXT_REPLY header would result in the WTLV_MIC beginning at byte 00AB. This conflicts with WTLV_MIC's length of 22 bytes, as Packet 95 only contains 14 more bytes.
- Comparing the two byte value 0x5201 at 00AB conflicts with the WTLV_MIC type definition that denotes a value of 0x0108.
- WTLV_MIC's length is represented by hexadecimal value 0xEB7C, corresponding to 60284 in decimal. This value conflicts with the remaining number of bytes in the package being 14.
- [USPAP1] Section [0829] defines a value of 0x0008 for the MIC length field of the WTLV_MIC TLV. However this conflicts with the value taken from byte 00B8 of 0x9978.

These discrepancies can be explained by modifications to WTLV_IN_SECURE_CONTEXT_REQ, WTLV_IN_SECURE_CONTEXT_REPLY and WTLV_MIC putting retrieved byte values back into reasonable context.

- A two byte padding is introduced after WTLV_INIT_SESSION (at bytes 005E – 005F)
- Nonce's, in general, are 32 byte long values.
- MIC values are 16 byte long (Table 3 displays the new WTLV_MIC format). This would correspond when applying the new WTLV_IN_SECURE_ CONTEXT_REPLY message format to packet 95, as byte 00A9 represents the MIC length in WTLV_MIC, whose hexadecimal value of 0x10 maps to 16 in decimal.
- Message structure for WTLV_IN_SECURE_CONTEXT_REQ and WTLV_IN_ SECURE_CONTEXT_REPLY (see Table 1 and Table 2 for revision proposed by author) message formats differ between [USPAP1] and actual implementation.
  - Revisions only differ past the Supplicant-ID (SID) field.
  - WTLV_IN_SECURE_CONTEXT_REQ contains two unknown zero-bytes, followed by 32 bytes representing $Nonce_{AP}$, enclosed by two zero-bytes.
  - No WTLV_MIC is appended to a WTLV_IN_SECURE_CONTEXT_REQ as this does not provide a cryptographically benefit. Modification of the Nonce value during transmission of the WLCCP message would result in MIC mismatches, as the CTK is used to calculate MIC's value. The MIC calculated by the IN Authenticator (who would create a CTK different to the one created on the Infrastructure Access Point) would differ from the transmitted MIC value within the WTLV_IN_SECURE_CONTEXT_RESP message.
  - WTLV_IN_SECURE_CONTEXT_REPLY's new message structure omits the fields CTK Key Length, CTK Key and Optional KEY TLV. From a practical point of view transmission of CTK from IA to IN would be unessential, as the key is derived from two Nonce's. Protection against key manipulation is achieved by append WTLV_MIC which is using the established CTK.

Field name	Size (bytes)	Description
Key Sequence Counter (KSC)	4	Number of times this key has been updated
Destination-ID (DID)	8	Ancestor requesting to share key with SID
Supplicant-ID (SID)	8	Requesting (Supplicant) ID
Unknown	2	Unknown function. Possibly padding. Constant value 0x0000
Nonce	32	Random value
Unknown	2	Unknown function. Possibly padding. Constant value 0x0000

Table 1: Revised WTLV_IN_SECURE_CONTEXT_REQ message format

Field name	Size (bytes)	Description
Key Sequence Counter (KSC)	4	Number of times this key has been updated
Destination-ID (DID)	8	Ancestor requesting to share key with SID
Supplicant-ID (SID)	8	Requesting (Supplicant) ID
Nonce	32	Random value
Session Timeout	4	Remaining session timeout for MN

Table 2: Revised WTLV_IN_SECURE_CONTEXT_REPLY message format

Field name	Size (bytes)	Description
Message Sequence Counter	8	RC4 Initialization Vector providing replay protection
MIC length	2	Length of the MIC in byte, constant value 0x0010
MIC	16	Message Integrity Check value

Table 3: Revised WTLV_MIC message format

Being able to recompute valid CTK's enable attackers to decrypt any information WLCCP is transporting. Knowledge of CTK's is additionally assumed to facilitate arbitrary, valid, MIC protected WLCCP message generation, including WLCCP_CONTEXT messages that are used to transport wireless contexts between APs. Abusing these, access to all PMK's, protecting wireless transmitted traffic is regarded to be possible. Successful compromise leads to disclosure of wireless transmitted data for arbitrary clients, which is neither detectable by Mobile Nodes, nor Access Points.

4.8 Attacks on intra-AP communication – A practical example

A practical attack would include the following steps:

- Obtain network access to a segment in which WLCCP messages are transmitted. A wireless installation can be checked on WLCCP usage by using Wireshark. If so, every Access Point transmits SCM Advertisement Replies on its wireless interface (as defined in [USPAP1] Section [1026]). Unplugging an Access Point illustrates one way to gain access to this network segment.
- Reading network traffic by usage of Wireshark, applying search pattern for SCM Advertisement Reply message's introduced in Section 4.4 provide information on the subnet WLCCP is working in.
- Discovering all Access Points, and thereby Infrastructure Access Point not acting as SCM is characterized in Section 4.5.
- Obtaining Infrastructure Authentication credentials can be done as described in Section
- 4.7.3, by ARP spoofing Access Points (Section 4.6 describes this attack). Admittedly this step involves correct guessing of ARP spoofed Access Point and time when authentication is carried out. However some chances exist to force complete reauthentication. As observed Infrastructure Access Points contact SCM every three minutes with an empty EAP Authentication message, encapsulated by IP/ UDP. ARP spoofing these messages without forwarding them, forces Infrastructure APs to switch back to unauthenticated state and

restart Infrastructure Authentication. It is important to forward all WLCCP EAP Authentication messages after Infrastructure AP authentication started[20].

- Cracking LEAP authentication credentials may take longer time periods, depending on dictionary size. This process may even fail in cases where the password is not included, requiring for expansion on the wordlist. As WLCCP uses mechanisms to rekey CTK's[21] the original CTK may be invalid, repeating actions mentioned one step above will provide attackers with parameters to recompute valid CTK's.
- Extract Nonce's from Authentication Messages, as described in Section 4.7.4 and 4.7.5, to recalculate NSK and CTK.
- Monitor for further WLCCP traffic that includes security relevant information as PMK or further CTK. From the authors perspective it should also be possible to directly request 802.11 Pairwise Master Keys using spoofed WLCCP messages that claim to origin from the ARP spoofed Infrastructure Access Point. However this is beyond the scope of this document.

By means of a self-written tool it was possible to disclose the CTKs used in a given intra-AP communication.
The following listing shows a sample piece of the tool's output:

```
[...]
     =     request node type 1
     =     request node address 0:11:21:bf:b5:ff
     =     request status 0
     === WTLV_INIT_SESSION header ===
     =     path length 1
     === WTLV_IN_SECURE_CONTEXT_REPLY header ===
     =     key sequence counter 00:00:00:01
     =     destination node type 8
     =     supplicant node address 0:c:ce:33:32:25
     =     supplicant node type 1
     =     supplicant node address 0:11:21:bf:b5:ff
           FOUND authenticator nonce:
54:AE:F5:32:A7:EC:8C:83:18:5A:17:21:AD:AE:91:F3:5E:15:D7:03:93:2B:43:E
7:AB:86:1A:33:49:94:94:31
     Starting CTK computation
     ctkSeed:
00:00:01:00:11:21:BF:B5:FF:00:08:00:0C:CE:33:32:25:9B:5C:3F:BA:02:D2:4
C:2D:6A:62:88:E4:D0:99:6B:85:17:30:01:39:2E:42:04:E5:72:08:9A:EC:BA:E0
:F5:2D:54:AE:F5:32:A7:EC:8C:83:18:5A:17:21:AD:AE:91:F3:5E:15:D7:03:93:
2B:43:E7:AB:86:1A:33:49:94:94:31:00:00:00:01:00
```

[20] *Forwarding ARP spoofed packet's on the attacker's machine can be done in several ways, mostly depending on platform and installed software packages.*
[21] *Rekeying is mentioned in [USPAP2], Section [0235] only, without further explanation. However rekeying encryption keys is a security best practice. For the lack of information, analysis of WLCCP's rekeying mechanism is beyond the scope of this thesis.*

CTK:

59:3A:AA:EE:3C:83:BE:D1:97:EE:57:48:45:6D:42:D4:19:EF:6E:8C:EB:07:40:3

8:90:4B:DB:DF:44:B6:CB:86

5 VULNERABILITY ASSESSMENT OF CUWN SETUP

The following chapter describes the assessment process in regard of vulnerabilities that all wireless components had been tested with.

5.1 Description of test environment

All tests described within this chapter were conducted within the following lab environment, consisting of the following devices:

- Cisco Wireless LAN Controller 5508 (IOS Version 6.0.182.0)
- Cisco Aironet Access Point 1242AG-E-K9 (IOS Version 12.4(21a)JA)
- Cisco Aironet Access Point AIR-LAP1142N-E-K9 (IOS Version 12.4(21a)JA)
- Cisco Aironet Access Point AIR-RM1252G-E-K9 (IOS Version 12.4(21a)JA)
- Cisco Wireless Control System (Version 6.0.170.0) on Windows Server 2003 R2 Enterprise Edition

AP to WLC communication is isolated from WLC to WCS communication by the usage of different VLAN's. A single SSID called *wlanlab* using WPA pre-shared key authentication and a separate VLAN was configured.

All devices were connected to a Cisco 3560 Series (WS-C3560-24PS) PoE capable switch. The switch provides power for Access Points and supports network packet capturing using SPAN ports.

Additional machines were connected to conduct special tests like Fuzzing and vulnerability assessment.

5.2 Vulnerability assessment

A common vulnerability assessment involves analysis of network based communication, software components that enable these services and common configuration mistakes.

First overview of network based communication is commonly derived from network scans, involving all TCP and UDP ports. Following are detailed tests on services that analyze the behavior, security critical software vulnerabilities and common configuration mistakes.

5.2.1 Network scan

Network scans were performed using nmap[22] on TCP and UDP ports, including service scan. This scan involves a database of fingerprints that enable nmap to test behaviour of ports, create a fingerprint and map these to known services. The scripting database was updated on 21st of December 2009.

No additional open ports that may impose risk on overall security of the wireless infrastructure could be found.

5.2.2 Security scan of services

Security scans of certain services were accomplished with the help of Tenable Nessus[23] and IBM Rational AppScan, testing with plug-ins updated on 21st of December 2009. NMAP scan policies were configured to test all ports 0 to 65535 on TCP as well as UDP. All plug-ins were enabled, including denial of service tests for NMAP as well as AppScan.

The following results display critical security flaws that were found during security scan.

[22] *http://www.insecure.org*
[23] *http://www.nessus.org*

5.2.2.1 Insecure SSL cipher configuration for WLC Web interface

The Web Interface which enables management of WLC and Access Points uses encryption to protect authentication as well transmitted data. The Transport Layer Security (TLS) protocol is used to setup and operate this encryption.

TLS allows configuring which encryption and signature algorithms can be used to establish a secure communication channel. Several insecure algorithms can generally be chosen, resulting in pour and insecure encryption of the management channel. This can be controlled by configuration, where these insecure algorithms can be disabled.

Analysis of supported algorithms showed, that several WEAK and MEDIUM secure ciphers are enabled. See Appendix B for a list of insecure ciphers supported by WLC.

5.2.2.2 Insecure SSL cipher configuration for WCS Web interface

The Web Interface which enables management of WCS, WLC and Access Points uses encryption to protect authentication as well as transmitted data. The Transport Layer Security (TLS) protocol is used to setup and operate this encryption.

TLS allows configuring which encryption and signature algorithms can be used to establish a secure communication channel. Several insecure algorithms can generally be chosen, resulting in poor and insecure encryption of the management channel. This can be controlled by configuration, where these insecure algorithms can be disabled.

Analysis of supported algorithms showed, that several WEAK and MEDIUM secure ciphers are enabled. See Appendix C for a list of insecure ciphers supported by WCS.

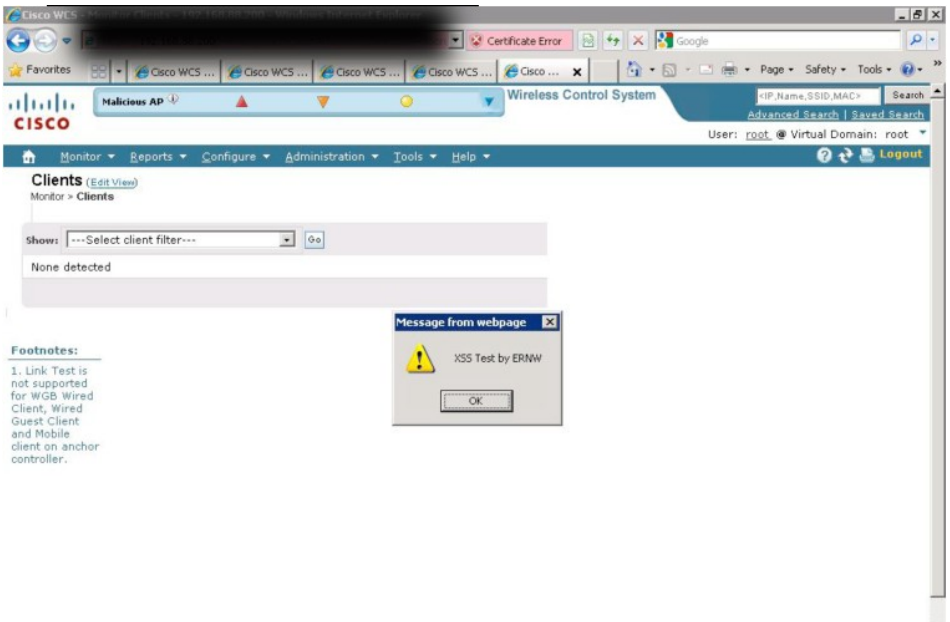
5.2.2.3 Cross-Site Scripting Vulnerability

A Cross-Site-Scripting (XSS) vulnerability within WLC's search function on the Web Interface could be determined. This enables attackers to prepare links for a website that includes code that is executed by the browser visiting this website.

This vulnerability exists due to insufficient input validation of data supplied within the search field. Input validation should generally only allow characters in input, that construct valid search topics. Special characters e.g. as "<" or ">" mark begin and end of HTML Tags, they are not used within valid search topics.

This vulnerability is already reported to Cisco within a responsible disclosure process and should be fixed by the next major release.

It should be assumed that more vulnerabilities may exist.



5.3 Network based attacks

The following chapter details network based attacks that have been engaged on wireless components. These include testing management protocols against abuse patterns that may enable attackers to change status or configuration, as well as fuzzing attacks that are able to reflect software stability in case of malformed/ corrupt packages.

5.3.1 ARP spoofing attacks

In Ethernet networks MAC addresses of interfaces have fixed value, due to vendors setting these during manufacturing process. IP addresses instead can be chosen freely, mostly following network design patterns. A special protocol is used to identify the MAC address of a network interface with a certain IP address configuration. It is called “Address Resolution Protocol” (ARP). ARP uses a simple Ethernet Layer2 based query mechanism to obtain MAC addresses. These packets do not involve any kind of authentication and source verification mechanism. Therefore they are easily spoofable. Spoofing ARP response packets may enable attackers to redirect traffic between two IP communication systems, if these are located within the same subnet.

During tests with a tool called Cain&Abel[24] it showed that Access Points as well as WLC’s are vulnerable to this kind of attack. This enables attackers to redirect traffic between two systems within the same IP subnet. This may lead to different attacks.

If traffic is not authenticated, and/ or encrypted manipulation and eavesdropping of this traffic can easily be done. Denial-of-Service (DoS) attacks are possible as well, by not forwarding redirected data packets to their original destination.

If traffic is authenticated manipulation becomes impossible. However eavesdropping and DoS attacks are still possible to execute.

If traffic is authenticated and encrypted only DoS attacks are possible.

5.3.2 SNMP

A number of security critical parameters accessible via SNMP could be identified. (for details see Appendix D). Special care as for the rigid configuration of SNMP (if at all) must be taken.

5.3.3 Fuzzing

A number of fuzzing tests against some parts for the CAPWAP protocol was performed by means of specially developed scripts for the fuzzing framework sulley (for details see Appendix E). No major impact as for the function of the devices could be observed.

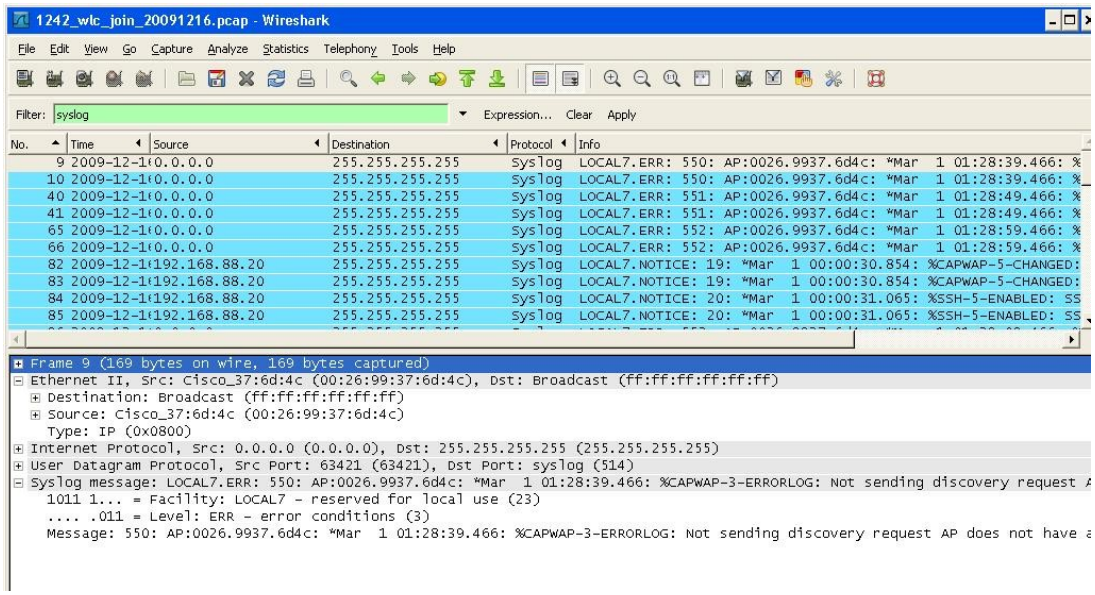
5.3.4 Random Notes

This section presents some miscellaneous findings that are not clearly related to any of the other sections.

5.3.4.1 Syslog to broadcast address

The system sent it’s log files to the broadcast address. This means that anybody on the adjacent network is able to receive these reports. Since log files often contain sensible information about infrastructures, this is a clear case of information disclosure.

[24] *http://www.oxid.it*


1242_wlc_join_20091216.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: syslog
Expression... Clear Apply
No. Time Source Destination Protocol Info
9 2009-12-1(0.0.0.0 255.255.255.255 Syslog LOCAL7.ERR: 550: AP:0026.9937.6d4c: *Mar 1 01:28:39.466: %
10 2009-12-1(0.0.0.0 255.255.255.255 Syslog LOCAL7.ERR: 550: AP:0026.9937.6d4c: *Mar 1 01:28:39.466: %
40 2009-12-1(0.0.0.0 255.255.255.255 Syslog LOCAL7.ERR: 551: AP:0026.9937.6d4c: *Mar 1 01:28:49.466: %
41 2009-12-1(0.0.0.0 255.255.255.255 Syslog LOCAL7.ERR: 551: AP:0026.9937.6d4c: *Mar 1 01:28:49.466: %
65 2009-12-1(0.0.0.0 255.255.255.255 Syslog LOCAL7.ERR: 552: AP:0026.9937.6d4c: *Mar 1 01:28:59.466: %
66 2009-12-1(0.0.0.0 255.255.255.255 Syslog LOCAL7.ERR: 552: AP:0026.9937.6d4c: *Mar 1 01:28:59.466: %
82 2009-12-1(192.168.88.20 255.255.255.255 Syslog LOCAL7.NOTICE: 19: *Mar 1 00:00:30.854: %CAPWAP-5-CHANGED:
83 2009-12-1(192.168.88.20 255.255.255.255 Syslog LOCAL7.NOTICE: 19: *Mar 1 00:00:30.854: %CAPWAP-5-CHANGED:
84 2009-12-1(192.168.88.20 255.255.255.255 Syslog LOCAL7.NOTICE: 20: *Mar 1 00:00:31.065: %SSH-5-ENABLED: SS
85 2009-12-1(192.168.88.20 255.255.255.255 Syslog LOCAL7.NOTICE: 20: *Mar 1 00:00:31.065: %SSH-5-ENABLED: SS
Frame 9 (169 bytes on wire, 169 bytes captured)
Ethernet II, Src: Cisco_37:6d:4c (00:26:99:37:6d:4c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Cisco_37:6d:4c (00:26:99:37:6d:4c)
Type: IP (0x0800)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 63421 (63421), Dst Port: syslog (514)
Syslog message: LOCAL7.ERR: 550: AP:0026.9937.6d4c: *Mar 1 01:28:39.466: %CAPWAP-3-ERRORLOG: Not sending discovery request A
1011 1... = Facility: LOCAL7 - reserved for local use (23)
.... .011 = Level: ERR - error conditions (3)
Message: 550: AP:0026.9937.6d4c: *Mar 1 01:28:39.466: %CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have a

6 RECOMMENDATIONS FOR CUWN SETUPS IN ENTERPRISE ENVIRONMENTS

The following chapter discusses security controls that should be implemented to ensure secure configuration and secure operation of wireless infrastructure.

6.1 General security countermeasures

This chapter includes general security countermeasures that apply to all devices or represent general approaches on how to deploy secure configuration and management of wireless network infrastructures.

6.1.1 Custom PKI

Communication between Access Points and Wireless LAN Controllers is based on the CAPWAP protocol, developed by Cisco. This protocol establishes secure links between APs and WLC's using UDP based communication. Authentication and encryption services rely on the Datagram Transport Layer Security (DTLS) protocol defined by RFC 4347[25]. Credentials used during authentication are individualized certificates, deployed on devices by Cisco during manufacturing[26] process. These certificates are signed by the "Cisco Manufacturing CA", whose certificate is signed by the "Cisco Root CA".

For security reasons it is highly recommended to not use these certificates within productive environments. Authentication certificates should be replaced by custom certificates, whose certificate chain is rooted to an enterprise affiliated Certification Authority. Otherwise attackers who gain access to the segment that connects AP's and WLC's may introduce fully functional rogue WLC's or AP's that are able to authenticate successfully within the infrastructure through their pre-deployed certificates.

Authentication of wireless clients can be based on digital certificates as well. In combination with 802.1x authentication technology, it is possible to configure secure wireless networks enabling reliable authentication services to protect network borders from attackers.

6.1.2 Hardware recommendations

Certain security features as DTLS data encryption are limited to specific hardware platforms. Because of this, only hardware that supports all necessary features should be purchased. Using legacy or hardware that does not support important security features may result in operational issues, as availability impact because feature mismatch or silent breach of defined security policies.

Devices and software that support all necessary features described within this security evaluation are the following:

- Cisco Wireless Control System
- Cisco 5508 Wireless LAN Controller with wplus license
- Cisco Aironet 1130 AG Series Access Point
- Cisco Aironet 1140 Series Access Point
- Cisco Aironet 1240 AG Series Access Point
- Cisco Aironet 1250 Series Access Point

Aironet 1130 and 1240 Access Points only support DTLS data encryption in software, while over models have hardware encryption supporting this feature. If high throughput of wireless data is requested only 1140 and 1250 series Access Points should be deployed in order to prevent denial of service attacks due to high capacity utilization because of encryption.

---

[25] *See http://tools.ietf.org/html/rfc4347*

[26] *Assuming that a device is manufactured before 18th of July 2005 devices produced before this date create a key-pair and certificate on first startup.*

6.1.3 Redundancy

Denial-of-Service attacks against wireless infrastructure may lay foundation for further attacks trying to imitate legitimate wireless infrastructure (e.g. by usage of rogue APs). This may result in clients connecting to wrong wireless infrastructure disclosing critical data like user credentials. Redundancy of critical infrastructure services can mitigate these kinds of attacks and additionally ensures service availability in case of failure or defect scenarios. It is strongly recommended to ensure that Wireless LAN Controllers and Wireless Control System are deployed redundantly. Configuration of every wireless infrastructure device must reflect this redundancy in terms of corresponding configuration that enables fail-over switching on required services.

6.1.4 Time settings

Correct clock values for all incorporated devices plays a critical role within environments using certificates for authentication. Wrong clock values may result in authentication failures, due to misinterpreted validity periods. Clock information can be distributed throughout a network using the Network Time Protocol (NTP). Configuration of valid time sources should always be done statically within configuration. Assigning these value dynamically (e.g. by DHCP options) may enable attackers to spoof these addresses, especially when authentication is not used.

If NTP is used it is strongly advised to evaluate if NTP authentication can be used on all devices. NTP authentication makes it impossible for attackers to spoof valid NTP answers, containing invalid clock information.

6.1.5 Isolate traffic with different security requirements into separate segments

Data transferred over wireless networks may have different security and confidentiality requirements. Typically each category is mapped to a single wireless network, whose configuration may vary, depending on security requirements.

Wireless networks can be mapped onto (existing) VLAN's. This enables easy integration of wireless networks into existing segmentation schemes.

It is strongly recommended to categorize traffic transferred over wireless networks and setup different wireless networks for these categories. If very high security requirements for certain kind of data or services exist, it may be applicable to prevent access to this kind of data via wireless networks to minimize overall risk.

6.1.6 Isolate guest traffic from company traffic

Network access for corporate guests within defined environments as conference rooms may be critical for overall security of the network. Guest computers are most likely covered by different, or even no security policies. This results in greater risks if network access for these kinds of devices is permitted. Best practice recommends complete isolation of network traffic originating from guest devices from corporate networks.

If wireless networks should be used to provide network access to guest users, e.g. in conference rooms, it is strongly advised to separate this traffic from company related traffic. Additionally this traffic should be handled as traffic originating from public networks like the Internet. Transition from this network to corporate network should only be possible using pre-defined, secure mechanisms. It is assumed that these kinds of services are already in operation.

6.1.7 Use strong authentication and encryption for wireless networks

Coverage of wireless networks is hardly controllable. This may result in attackers being able to receive or send data from/ to wireless networks without physical access to company sites. This may enable attackers to participate, manipulate or wiretap data transmitted on wireless networks.

Strong authentication of devices, establishing a connection with wireless networks, enables companies to restrict access to corporate users. Strong encryption of wireless transmitted data prevents wiretapping attacks, which may result in information disclosure of sensitive data.

Strong authentication must be used for limiting network access only to legitimate users. Within company installations it is strongly advised to enable strong authentication based on 802.1x technology in combination with user based authentication. This enables allocation and revocation of wireless usage capabilities for single users.

Strong encryption must be used to mitigate wiretap attacks, as well as secure data during transmission. Wireless networks should in general be encrypted using the Advanced Encryption Standard (AES) algorithm.

6.2 Security of Access Points

In the following chapter security measures for Access Points are discussed. Main goal of this is to keep overall security level of wireless infrastructure high, in case that Access Points are deployed to non-secure areas.

6.2.1 Physical security of Access Points and cabling

Physical security of Access Points and cabling must be regarded as highly critical. Disregarding this issue enables attackers to easily obtain access to Access Points and wireless distribution networks. Cabling should be secured to prevent unplugging network cables or attach serial consoles to Access Points.

It is recommended to use special wall mount kits that secure Access Points from being removed and additionally secure cable ends and cable jacks from removing or inserting cables. During deployment wall mount kits including unique locks should be considered.

Additionally this countermeasure serves theft protection.

6.2.2 Static IP configuration

Access Points can obtain IP address configuration of their wired network interface either by static configuration or dynamic protocols as DHCP. Usage of DHCP may enable attackers with access to the network that connects APs and WLC's to execute DHCP spoofing attacks. These attacks involve a rogue DHCP server, maintained by the attacker, which hands out (partly) wrong configuration data to APs. This is critical for availability of wireless infrastructure. Additionally this may pose an additional security risk, as DHCP address assignments can contain WLC address information. Attackers can therefore be able to redirect Access Points to rogue WLC's by abuse DHCP capabilities.

It is strongly recommended to not use DHCP for IP address configuration of Access Points. Instead IP parameters and WLC addresses should be configured statically to minimize overall risk.

6.2.3 Disable management interfaces

WLC's are capable of managing software and configuration of Access Points from a centralized location. This process utilizes CAPWAP. Access Points can be configured by a range of different protocols as HTTP, HTTPS, SSH, telnet. Each management interfaces is equivalent to a process running on the Access Point. This enlarges network attack surface. It is therefore highly recommended to disable management interfaces which are not in use.

As CAPWAP is used for management all management interfaces except SSH should be disabled. CAPWAP based management can only be conducted as long as APs are associated with at least one WLC. For failure and troubleshooting scenarios SSH will provide a second management interface which is not constrained to the availability of additional services.

6.3 Configuration of intermediate network devices

The following chapter focuses on essential security countermeasures that support overall security of wireless infrastructure and should be deployed to network devices connecting wireless infrastructure devices.

6.3.1 Separate segments

Data flows representing different functionalities with diverse security requirements should be placed into separate network segments. This enables separation and minimizes attack surfaces, as less network devices are connected to a single subnet.

Cisco enterprise wireless infrastructures build on several protocols, whose information are diverse sensitive. Network protocols used to transport these data sets also differ in integrated security mechanisms. Network design should incorporate at least the following segments:

- AP to WLC communication should be placed into a separate segment. During design phase of this network must be considered that his segment will span across all areas of the campus in which WLAN will be deployed. This segment may also be used for simple management connections to APs, e.g. through SSH.
- WLC to WCS communication should be placed into a separate network segment, which is only available where corresponding devices are connected.
- WLC's equipped with separate service ports should be configured to use this port for designated administration tasks. Therefore a separate segment should be configured

6.3.2 Network ACL's

Network traffic within wireless infrastructure should be limited to services necessary for operation and administration. This provides defense-in-depth countermeasures in case of attackers being able to connect to certain segments. Beside infrastructure protocols like ICMP and DNS, access lists must allow protocols used for management. WLC to WCS communication additionally includes RADIUS and SYSLOG communication which must be allowed. AP to WLC communication involves CAPWAP which transports data over UDP port 5246 and 5247.

Network access lists are strongly recommended to be applied to segments transporting data of wireless infrastructure. This results in minimized attack surface and impact in case of attackers being able to connect these network segments.

6.3.3 Enable 802.1x authentication for Access Point

Lightweight Access Points are capable of authentication themselves to the network they are connected to. Authentication is accomplished by the usage of 802.1x and Cisco's EAP-FAST. Authentication credentials are usernames and passwords.

Due to coverage requirements of wireless networks network cables enabling access to wireless infrastructure segments are available where wireless networks are deployed. These may include public areas. This involves certain risks of conducting networks based attacks on existing infrastructure.

It is therefore strongly advised to protect network access by usage of 802.1x authentication for Access Points. This should involve all ports that are designated to connect APs to, regardless if an AP is connected or not. Authentication credentials should additionally be unique for each Access Point.

6.4 WLC configuration

The following chapter discusses security principals that should be applied during configuration of Wireless LAN Controllers, to establish secure configurations.

6.4.1 Administration via encrypted protocols

Access to administrative interfaces should only be able through the usage of protocols that encrypt transported data. Management tasks are considered to be secured appropriately as conducted tasks involve changes that may have impact on overall security of an environment. It is therefore critical that manipulation of management traffic is impossible to conduct. Protocols that involve encryption to protect management traffic are SSH, HTTPS and SNMPv3.

It is strongly recommended to disable all management and administration protocols that do not enable secure administration through the usage of encryption.

6.4.2 Limit access to management interface

Access to management interfaces should in general be limited to certain network segments or machines. This reduces risk of (un-)intentional abuse that may to lead to configuration changes and may have impact on availability of infrastructure devices and services. Limitations can be introduced by usage of filters that either filter network access to management interfaces, as well as allow conduction of management tasks only to certain users.

In general least privilege patterns should be applied, to protect management interfaces. This should be done by allowing network access to these interfaces only to privileged network segments and/ or computers, as well as limiting which users are able to login on management interfaces and what information sets they may be able to retrieve or change.

6.4.3 Secure SNMP configuration

Simple Network Management Protocol (SNMP) is used for centralized configuration and management of WLCs by a WCS. WLCs support SNMP version 1, 2c and 3. Version 1 and 2c do not provide essential security functionality as encryption and authentication. Therefore these protocols are easy to modify and tamper with. Version 3 introduces authentication services based on username and password in conjunction with several HMAC methods. This provides authentication of services as well as SNMP network packets to eliminate certain attack vectors. Additionally SNMP v3 supports encryption of transmitted packets. This is essential in case of sensitive information are transmitted via SNMP. Management via SNMP can be considered as being sensitive data.

It is strongly recommended to only enable SNMP v3 on Wireless LAN Controllers. In addition secure configuration parameters must be set. These involve the usage of HMAC-SHA and AES-128 for authentication and encryption. Algorithms as DES or MD5 should not be used for authentication or encryption services, as these are cryptographically broken. WLC's can use different passwords for authentication and encryption. It is highly recommended to not use the same password for both services, as well as choosing complex passwords.

6.4.4 Enable centralized decryption

Traffic between WLC's and AP's can be grouped in two categories. CAPWAP control traffic and user data traffic. CAPWAP control traffic contains data necessary for AP management as well as wireless management data, e.g. wireless authentication and association frames. This traffic is encrypted and authenticated using DTLS functionality.

Network data sent over wireless networks is encapsulated in CAPWAP and forwarded from AP to WLC. By default configuration this data is only authenticated. Encryption modes configured for wireless networks do not apply for this traffic. Default configuration results in decryption of wireless packets by APs.

This may enable attackers with access to the network that connects AP's and WLC's to read data that is transmitted over wireless interfaces, creating possibilities for information disclosure attacks.

It is therefore strongly recommended to enable DTLS data encryption. Access Points then do not decrypt wireless data packets before encapsulation in CAPWAP. Decryption is done by the Controller, mitigating information disclosure risks.

6.5 WCS configuration

The following chapter contains general security guidelines which should be considered before and during setup and operation of Wireless Control System.

6.5.1 Custom network segment

Wireless Control System enables single point of administration and management for Cisco's wireless infrastructure. Security of this system is therefore highly critical. As network design patterns advise, a distinct segment should be used for highly critical services, as this enables protection by standard Layer 2 and 3 security mechanisms.

WCS should in general be placed into a dedicated network segment. This segment should be protected appropriately. Due to its functions, compromise of WCS may enable attackers to change configuration parameters affecting all wireless infrastructure devices.

6.5.2 Hardening of underlying operating system

Cisco WCS is based on Windows Server operating systems. In comparison to WLC's WCS functionality is not packed into appliance form factor. As this system does heavily depend on availability of network connectivity it may be target to any abuse of security flaws that are eminent on the operating system. Therefore secure configuration and defense in depth hardening of this operating system improve stability, availability and integrity of WCS functionality.

It is strongly recommended, due to WCS's functionality, to implement in-depth hardening countermeasures to the operating system underlying Cisco WCS. This improves overall security of the wireless infrastructure.

6.5.3 Administration via encrypted protocols

Access to administrative interfaces should in general only be able through the usage of protocols that encrypt transported data. Management tasks are considered to be secured appropriately as conducted tasks involve changes that may have impact on overall security of an environment. It is therefore critical that manipulation of management traffic is impossible to conduct. Protocols that involve encryption to protect management traffic are HTTPS and SNMPv3.

It is strongly recommended to disable all management and administration protocols that do not enable secure administration through the usage of encryption.

6.5.4 Limit access to management interface

Access to management interfaces should in general be limited to certain network segments or machines. This reduces risk of (un-)intentional abuse that may to lead to configuration changes and may have impact on availability of infrastructure devices and services. Limitations can be introduced by usage of filters that either filter network access to management interfaces, as well as allow conduction of management tasks only to certain users.

In general least privilege patterns should be applied to protect management interfaces. This should be done by allowing network access to these interfaces only to privileged network segments and/ or computers, as well as limiting which users are able to login on management interfaces and what information sets they may be able to retrieve or change.

6.5.5 Secure SNMP configuration

Simple Network Management Protocol (SNMP) is used for centralized configuration and management of WLC's by a WCS. The WCS supports SNMP version 1, 2c and 3. Version 1 and 2c do not provide essential security functionality as encryption and authentication. Therefore these protocols are easy to modify and tamper with. Version 3 introduces

authentication services based on username and password in conjunction with several HMAC methods. This provides authentication of services as well as SNMP network packets to eliminate certain attack vectors. Additionally SNMP v3 supports encryption of transmitted packets. This is essential in case of sensitive information are transmitted via SNMP. Management via SNMP can be considered as being sensitive data.

It is strongly recommended to only enable SNMP v3 on Wireless Control System. In addition secure configuration parameters must be set. These involve the usage of HMAC-SHA and AES-128 for authentication and encryption. Algorithms as DES or MD5 should not be used for authentication or encryption services, as these are cryptographically broken. WCS can use different passwords for authentication and encryption. It is highly recommended to not use the same password for both services, as well as choosing complex passwords.

7 SUMMARY

Cisco enterprise scale Wireless LAN products are capable of enduring security throughout wireless networks. Mitigation of certain attack vectors, which may be quite feasible, e.g. attackers un-mounting Access Points to gain network access, must be deployed. Manipulation and modification of network traffic, as well as eavesdropping, should be addressed to ensure a high security level.

Security recommendations described in chapter 7 should be deployed in the following prioritized (highest priority first) order:

- Secure SNMP configuration
- 802.1x authentication for Access Points
- Network segmentation
- Custom PKI
- Secure administration (Strong authentication, encryption, limit access to management interfaces)
- Centralized decryption
- Physical security of Access Points

Additionally it should not be discarded that all components heavily depend on complex software. It is necessary do implement an according patching process in case of software vulnerabilities, that may affect overall security of the wireless environment.

Beside mentioned security mechanisms, best practices should additionally be applied to all components. This ensures defense-in-depth configuration, tightening security to make successful attacks less feasible.

8 APPENDIX B: INSECURE TLS ALGORITHMS SUPPORTED BY WLC

The following as weak or medium secure, and therefore cryptographically insecure, stated algorithms for TLS encryption are enabled in WLC's configuration:

- EXP-RC4-MD5
- EXP-RC2-CBC-MD5
- DES-CBC-MD5
- DES-CBC-SHA

9 APPENDIX C: INSECURE TLS CIPHERS SUPPORTED BY WCS

The following as weak or medium secure, and therefore cryptographically insecure, stated algorithms for TLS encryption are enabled in WCS's configuration:

- EDH-RSA-DES-CBC-SHA
- DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

10 APPENDIX D: CRITICAL SNMP MIB'S

The following SNMP MIB's could be extracted from WLC and may impose risk on overall security of environment:

```
1.3.6.1.4.1.14179.2.5.5.1.2.4.101.114.110.119 = STRING: "ernw"
SNMPv2-SMI::enterprises.14179.2.5.5.1.3.4.101.114.110.119 = STRING: "****"
SNMPv2-SMI::enterprises.14179.2.5.5.1.4.4.101.114.110.119 = INTEGER: 1
SNMPv2-SMI::enterprises.14179.2.5.5.1.5.4.101.114.110.119 = INTEGER: 2
SNMPv2-SMI::enterprises.14179.2.5.5.1.6.4.101.114.110.119 = INTEGER: 1
SNMPv2-SMI::enterprises.14179.2.5.5.1.7.4.101.114.110.119 = STRING: " "
SNMPv2-SMI::enterprises.14179.2.5.5.1.26.4.101.114.110.119 = INTEGER: 1



BsnUsersEntry ::= SEQUENCE {
                bsnUserName             OCTET STRING,
                bsnUserPassword         OCTET STRING,
                bsnUserEssIndex         INTEGER,
                bsnUserAccessMode       INTEGER,
                bsnUserType             INTEGER,
                bsnUserInterfaceName    OCTET STRING,
                bsnUserRowStatus        RowStatus
}

bsnUserName OBJECT-TYPE
      SYNTAX     OCTET STRING (SIZE(1..24))
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "User Name"
      ::= { bsnUsersEntry 2 }

bsnUserPassword OBJECT-TYPE
      SYNTAX     OCTET STRING (SIZE(1..24))
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "User Password"
      ::= { bsnUsersEntry 3 }

bsnUserEssIndex OBJECT-TYPE
      SYNTAX     INTEGER (0..17)
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "User WLAN ID. Value 0 implies that this
applies to any
              WLAN ID."
      ::= { bsnUsersEntry 4 }

bsnUserAccessMode OBJECT-TYPE
      SYNTAX     INTEGER { readOnly (1) , readWrite (2)}
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "User Access Mode."
      ::= { bsnUsersEntry 5 }

bsnUserType OBJECT-TYPE
      SYNTAX     INTEGER { management (1),wlan(2),macFilter(3)}
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "User Type."
      ::= { bsnUsersEntry 6 }
```

```
bsnUserInterfaceName OBJECT-TYPE
      SYNTAX     OCTET STRING (SIZE(0..32))
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "Interface Name."
      ::= { bsnUsersEntry 7 }

bsnUserRowStatus OBJECT-TYPE
      SYNTAX     RowStatus
      MAX-ACCESS read-create
      STATUS     obsolete
      DESCRIPTION             "Row Status"
      ::= { bsnUsersEntry 26 }
```

```
SNMPv2-SMI::enterprises.14179.2.5.11.1.1.4.101.114.110.119 = STRING: "ernw"
SNMPv2-SMI::enterprises.14179.2.5.11.1.2.4.101.114.110.119 = STRING: "****"
SNMPv2-SMI::enterprises.14179.2.5.11.1.3.4.101.114.110.119 = INTEGER: 2
SNMPv2-SMI::enterprises.14179.2.5.11.1.23.4.101.114.110.119 = INTEGER: 1
```

```
bsnLocalManagementUserEntry OBJECT-TYPE
      SYNTAX     BsnLocalManagementUserEntry
      MAX-ACCESS not-accessible
      STATUS     current
      DESCRIPTION            "...."
      INDEX      { bsnLocalManagementUserName }
      ::= { bsnLocalManagementUserTable 1 }

BsnLocalManagementUserEntry ::= SEQUENCE {
          bsnLocalManagementUserName            OCTET STRING,
          bsnLocalManagementUserPassword        OCTET STRING,
          bsnLocalManagementUserAccessMode      INTEGER,
          bsnLocalManagementUserRowStatus       RowStatus
}

bsnLocalManagementUserName OBJECT-TYPE
      SYNTAX     OCTET STRING (SIZE(1..24))
      MAX-ACCESS read-create
      STATUS     current
      DESCRIPTION             "User Name"
      ::= { bsnLocalManagementUserEntry 1 }

bsnLocalManagementUserPassword OBJECT-TYPE
      SYNTAX     OCTET STRING (SIZE(1..24))
      MAX-ACCESS read-create
      STATUS     current
      DESCRIPTION             "User Password"
      ::= { bsnLocalManagementUserEntry 2 }

bsnLocalManagementUserAccessMode OBJECT-TYPE
      SYNTAX     INTEGER { readOnly (1) , readWrite (2)}
      MAX-ACCESS read-create
      STATUS     current
      DESCRIPTION             "User Access Mode."
      ::= { bsnLocalManagementUserEntry 3 }
```

```
bsnLocalManagementUserRowStatus OBJECT-TYPE
      SYNTAX     RowStatus
      MAX-ACCESS read-create
      STATUS     current
      DESCRIPTION             "Row Status"
      ::= { bsnLocalManagementUserEntry 23 }



SNMPv2-SMI::enterprises.14179.2.2.1.1.26.0.33.27.235.96.112 = IpAddress:
255.255.255.0
SNMPv2-SMI::enterprises.14179.2.2.1.1.26.0.35.51.141.23.176 = IpAddress:
255.255.255.0
SNMPv2-SMI::enterprises.14179.2.2.1.1.26.0.38.153.34.225.32 = IpAddress:
255.255.255.0
SNMPv2-SMI::enterprises.14179.2.2.1.1.27.0.33.27.235.96.112 = IpAddress:
192.168.88.252
SNMPv2-SMI::enterprises.14179.2.2.1.1.27.0.35.51.141.23.176 = IpAddress:
0.0.0.0
SNMPv2-SMI::enterprises.14179.2.2.1.1.27.0.38.153.34.225.32 = IpAddress:
192.168.88.252
SNMPv2-SMI::enterprises.14179.2.2.1.1.28.0.33.27.235.96.112 = IpAddress:
192.168.88.175
SNMPv2-SMI::enterprises.14179.2.2.1.1.28.0.35.51.141.23.176 = IpAddress:
192.168.88.166
SNMPv2-SMI::enterprises.14179.2.2.1.1.28.0.38.153.34.225.32 = IpAddress:
192.168.88.171


bsnAPNetmask OBJECT-TYPE
      SYNTAX     IpAddress
      MAX-ACCESS read-write
      STATUS     current
      DESCRIPTION            "The Netmask of the IP address of the AP."
      ::= { bsnAPEntry 26 }

bsnAPGateway OBJECT-TYPE
      SYNTAX     IpAddress
      MAX-ACCESS read-write
      STATUS     current
      DESCRIPTION            "The Gateway for the AP."
      ::= { bsnAPEntry 27 }

bsnAPStaticIPAddress OBJECT-TYPE
      SYNTAX     IpAddress
      MAX-ACCESS read-write
      STATUS     current
      DESCRIPTION        "The Static IP-Address configuration for the AP.
         This can only be changed when the LWAPP mode is in Layer-3."
      ::= { bsnAPEntry 28 }
```

11 APPENDIX E: FUZZING

The following script was used to fuzz all parameters on unencrypted CAPWAP packet fields. Details on packet format can be obtained from RFC 5415[27] "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification" chapter 4.

```
from sulley import *

s_initialize("CAPWAP-Header")

s_binary("0x00 24 97 CC 70 41") #ETH Dst
s_binary("0x00 01 02 03 04 05") #ETH Src
s_binary("0x08 00")                          #ETH Type -> IP

s_block_start("IPlength")
s_block_start("IP")
s_binary("0x45")               #IP Version + Len
s_binary("0xc0")               #IP Service Fields -> class 6
s_size("IPlength", length=3D2, endian=3D">", inclusive=3DTrue)  #IP Len
s_binary("0x0000")             #IP ID
s_binary("0x4000")             #IP Flags -> dont fragment, + offset -> 0
s_binary("0xff")                   #IP TTL
s_binary("0x11")               #IP Proto -> UDP
s_checksum("IP", algorithm=3D"ichecksum", endian=3D">")         #IP
Checksum
s_binary("0xc0a8580a")           #IP Src -> 192.168.88.10
s_binary("0xc0a8586f")           #IP Dst -> 192.168.88.111
s_block_end("IP")

s_block_start("UDPlength")
s_binary("0xeb69")             #UDP Src port -> 60265
s_binary("0x147e")             #UDP Dst port -> 5246
s_size("UDPlength", length=3D2, endian=3D">", inclusive=3DTrue) #UDP Len
s_binary("0x0000")             #UDP Csum -> NULL (RFC5415 3.1.)

#~  0                   1                   2                   3
#~  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
#~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#~ |Version|  Type |  HLEN   |   RID   | WBID    |T|F|L|W|M|K|Flags|
#~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#~ |          Fragment ID          |     Frag Offset         |Rsvd |
#~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#~ |                 (optional) Radio MAC Address                  |
#~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#~ |            (optional) Wireless Specific Information           |
#~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
#~ |                         Payload ....                          |
#~ +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

s_block_start("Headerlength", alt_mutate=3DTrue)
```

[27] *http://tools.ietf.org/html/rfc5415*

```
s_byte(0x00)            #Version -> 0 + Type -> 0 (CAPWAP Header)
s_size("Headerlength", length=3D2, endian=3D">", inclusive=3DTrue, math=3D=
lambda x: x << 3)  #HLEN
s_word(0x0210)          #RID + WBID + Flags
s_word(0x0000)          #Frag ID
s_word(0x0000)          #Frag Off
s_dword(0x000000000)    #MAC
s_dword(0x000000000)    #WSI
s_random(0, 0, 30, 1000)


s_block_end("Headerlength")
s_block_end("UDPlength")
s_block_end("IPlength")

sess =3D sessions.session(proto=3D"layer2", iface=3D"eth1")
sess.connect(s_get("CAPWAP-Header"))

target =3D sessions.target("layer2", 1337)
sess.add_target(target)

sess.fuzz()
```

12 REFERENCES

[ASL] ASLEAP, Password Recovery Tool for Cisco LEAP and MS-CHAP-V2 http://asleap.sourceforge.net (As at: June 16, 2009)

[CSPAN] Cisco, *Understanding SPAN and RSPAN*, http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_40_se/configuration/guide/swspan.html#wp1210541 (As at: June 20th, 2009)

[CWDS] Cisco, *Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services*, http://www.cisco.com/en/US/docs/wireless/access_point/12.3_8_JA/configuration/guide/s38roamg.html (As at: June 20th, 2009)

[CWLS] Krishna Sankar, et. Al, *Cisco Wireless LAN Security, Expert guidance for securing your 802.11 networks*, 2005, Cisco Press

[DSNIFF] dsniff, Network auditing and Penetration testing tool collection, http://monkey.org/~dugsong/dsniff (As at: June 30th, 2009; Version 2.3)

[JW03] Joshua Wright, *Weaknesses in LEAP Challenge/ Response*, 2003 http://www.willhackforsushi.com/presentations/asleap-defcon.ppt (As at: June 3rd, 2009)

[MCNAL] Cameron MacNally, *Cisco LEAP protocol description*, E-Mail on Cistron-Radius Mailing List, 2001, http://lists.cistron.nl/pipermail/cistron-radius/2001-September/002042.html (As at: June 1st, 2009)

[NMAP] NMAP, Network Mapper, http://nmap.org (As at July 10th, 2009)

[RFC826] David C. Plummer, RFC 862, *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses*, Request for Comment, 1982

[SWANIG] Cisco, *Cisco Structured Wireless-Aware Network (SWAN) Implementation Guide*, http://www.cisco.com/en/US/docs/wireless/technology/swan/deployment/guide/swandg.html (As at June 03rd, 2009)

[USPAP1] Robert Meier, et. Al, *802.11 Using a compressed Reassociation exchange to facilitate fast handoff*, United States Patent Application Publication No. 10/417,633, 2004