



TROOPERS10

IT-Security Conference & Workshops



TODAY:



Attacking Cisco Enterprise WLANs

Enno Rey
Daniel Mende
Simon Rich
Oliver Roeschke



{erey, dmende, srich, oroeschke}@ernw.de

Who we are



- **Old-school network geeks, working as security researchers**
- **Germany based ERNW GmbH**
 - Independent
 - Deep technical knowledge
 - Structured (assessment) approach
 - Business reasonable recommendations
 - We understand corporate

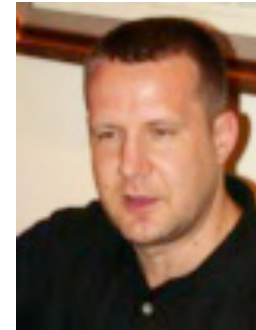


- **Blog: www.insinuator.net**
- **Conference: www.troopers.de**



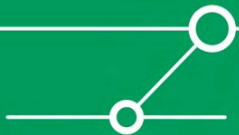
The research team

- **Enno Rey**
 - Project founder & leader
 - “The boss” ;-)
- **Daniel Mende**
 - Coding & tool guru
- **Simon Rich**
 - Hack-IT & PenTesting champion
- **Oliver Roeschke**
 - Protocol analysis & crypto analysis fanatic



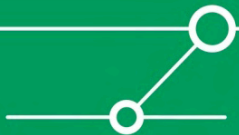
Agenda

- **Introduction & dimensions of this talk**
- **Technology overview & attack paths**
- **Attacks in the SWAN world**
- **Attacks in the CUWN world**
- **Conclusions**



Background of this talk

- Besides being security guys we (still) do some practical network implementation work.
- When occasionally touching Cisco Enterprise WLAN stuff, we couldn't avoid the feeling that security-wise
... it smelled ;-)



mott

- **Even though we did our research (and this talk covers) mainly “vendor C” and the WLAN space, the “main aspects” can be observed as well**
 - In products of other vendors.
 - In other types of “Enterprise Solutions” (e.g. VoIP, storage etc.).



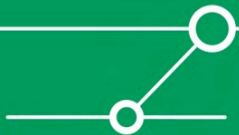
So, it's not only “vendor C” –
others are build on sand, too →



mott

- **The types of problems discussed derive from**
 - Somehow assembled, specific-purpose, multi-component stuff
 - Still, this is usually based on COTS OS's / libraries / applications
 - Put together (at times) without security quality assurance
 - Potentially after acquisition of some niche vendor
- Admin's attitude:

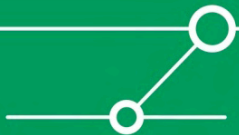
*"thank god it's working,
we can harden it later"*



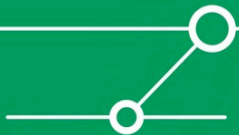
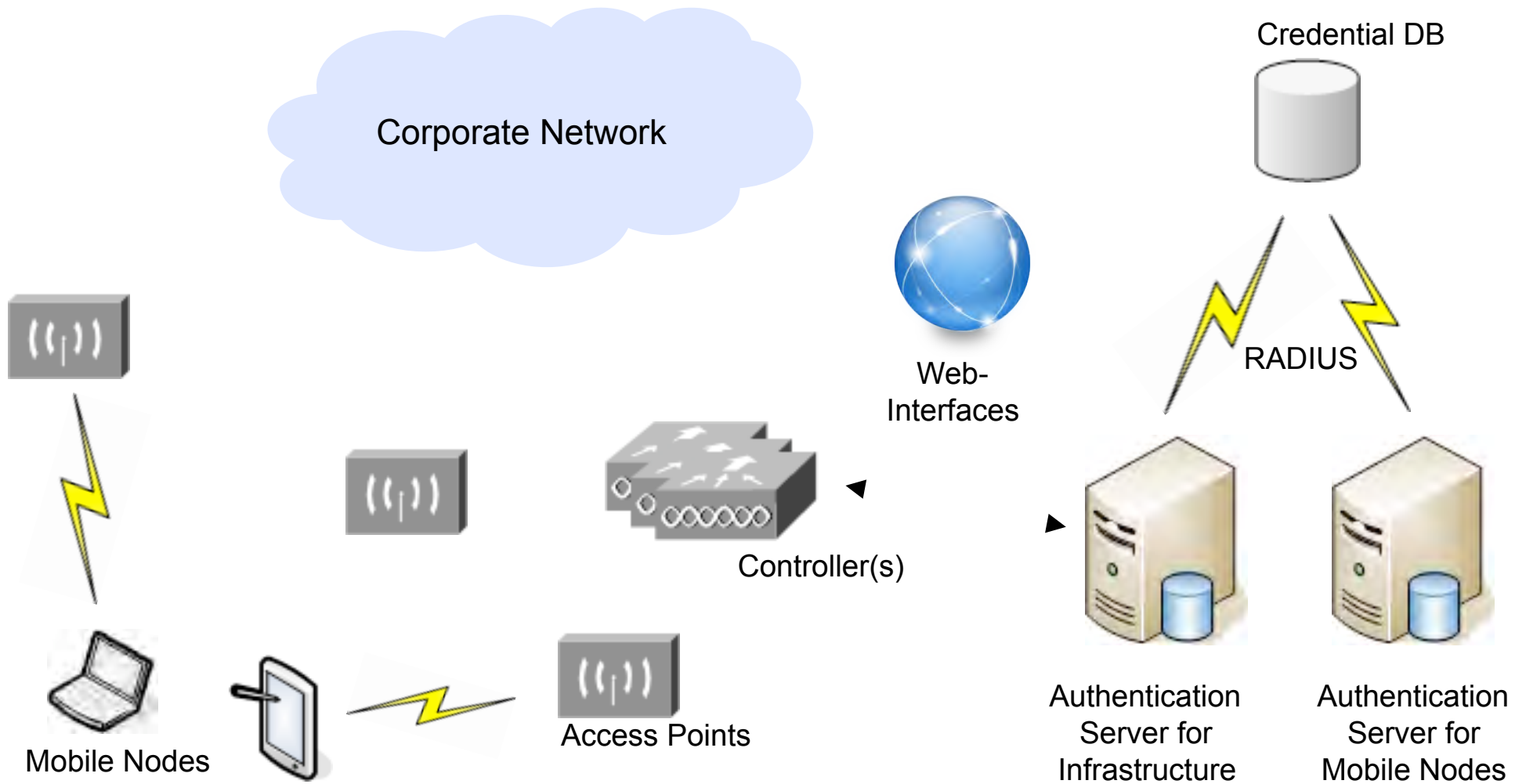
Consequences when performing research

- **Often proprietary stuff (including protocols)**

- not easy to understand and not too well documented either.
- read patents, not RFC's
- “legal boundaries” when performing security research.



WLAN Enterprise Stuff, big picture



Flavors / Generations in C space



From our perspective three generations can be identified.

- **1st: Structured Wireless-Aware Networks (SWAN)**
- **2nd: Based on managed AP's & LWAPP**
 - After *Airspace* acquisition in 2005
 - Still some interesting remnants from *Airspace* age present today...
- **3rd: Cisco Unified Wireless Network (CUWN) w/ CAPWAP**



In this talk, we cover 1st (SWAN) & 3rd (CUWN) generations.



Main attack paths

- **Attacks against traffic in transit**



- **Attacks against cryptographic material**

- Somehow related to attacks against traffic in transit ;-)
- Might be used of different purposes though
 - E.g. injection of rogue devices

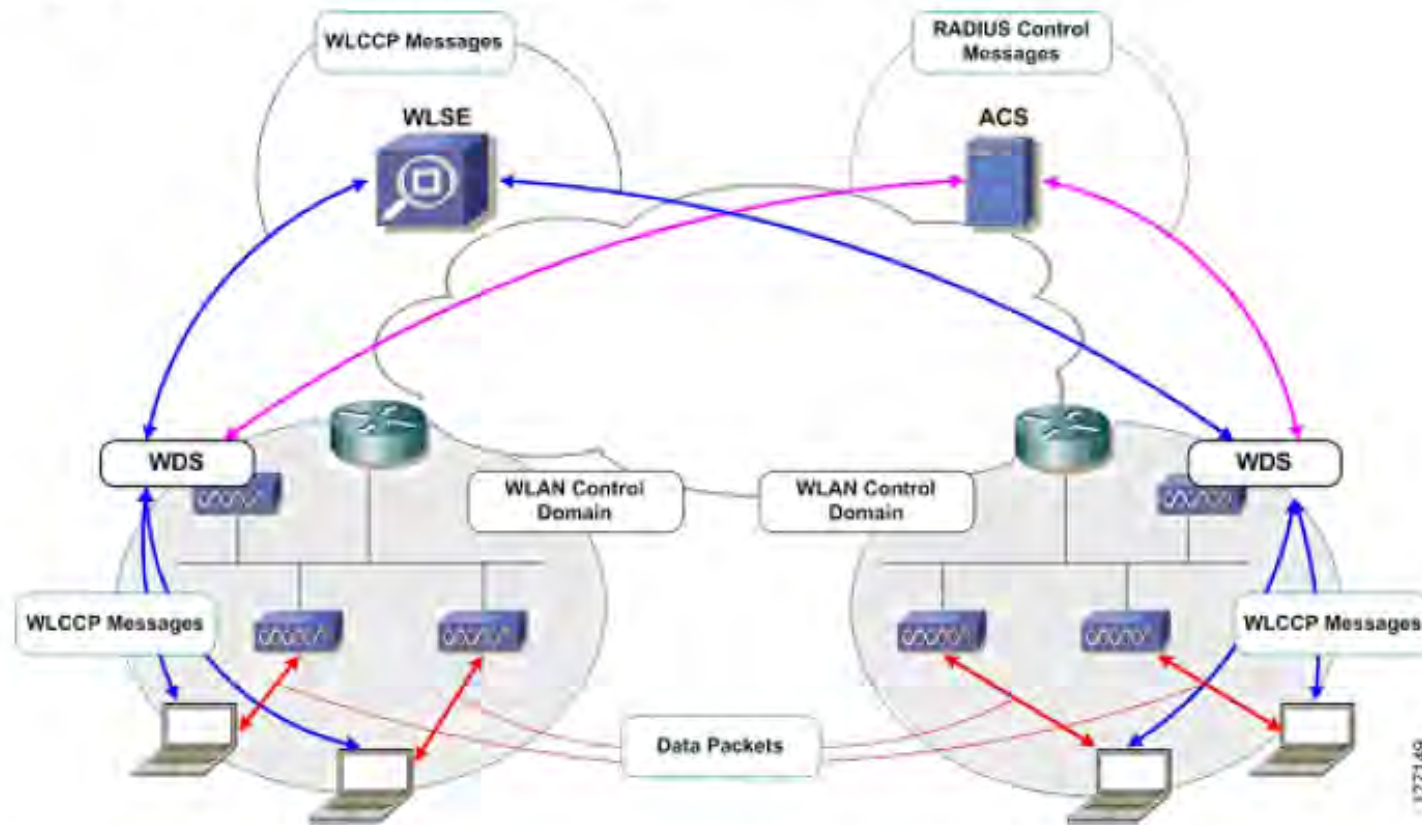
- **Attacks against components**

- Physical removal/replacement
- Mgmt interfaces (SNMP, HTTP[S] et.al.)

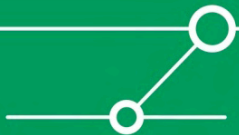


Du côté de chez Swan(n)

Figure 3 Access Point-Based WDS Solution

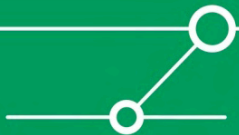
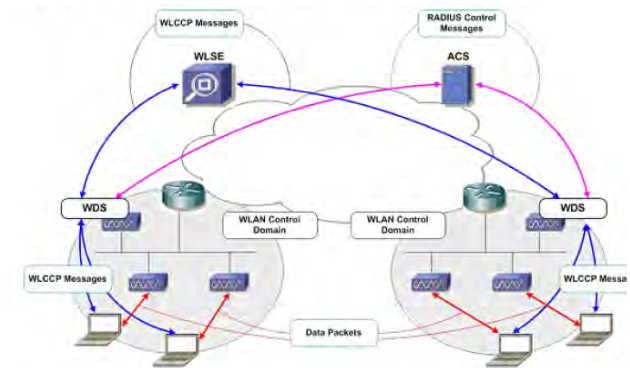


From: <http://www.cisco.com/en/US/docs/wireless/technology/swan/deployment/guide/swandg.html>



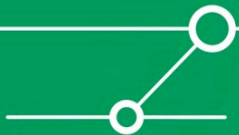
SWAN's way – How things work

- **Access points are autonomous but can be “configured by a central entity”**
 - Wireless LAN Solution Engine (WLSE)
 - Wireless LAN Services Module (WLSM) for Cat65K
- **Framework provides some functions entitled as *Wireless Domain Services (WDS)*.**
- **Intra-AP communication mainly done by means of a proprietary protocol: WLCCP.**



WLCCP

- **Wireless LAN Context Control Protocol**
- **Described essentially in two US Patents**
 - Wireless local area network context control protocol
 - 802.11 using a compressed re-association exchange to facilitate fast handoff
- **Provides functions for central mgmt, authentication, radio frequency measurement etc.**
- **Different encapsulations (Ethernet, UDP 2887) used for different types of traffic (local subnet vs. routed traffic).**
- **Basic *Wireshark* parser for some message types available.**



WLCCP internals relevant here |

■ Two types of authentication

- *Infrastructure Authentication* for Intra-AP communication → LEAP
- Client Authentication
→ potentially all Cisco-supported EAP methods



■ Confidentiality and integrity protection by key material

- NSK = *Network Session Key* established during LEAP authentication.
- *Context Transfer Key* (CTK) derived separately, depends on NSK

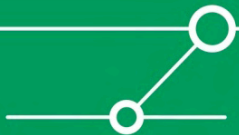
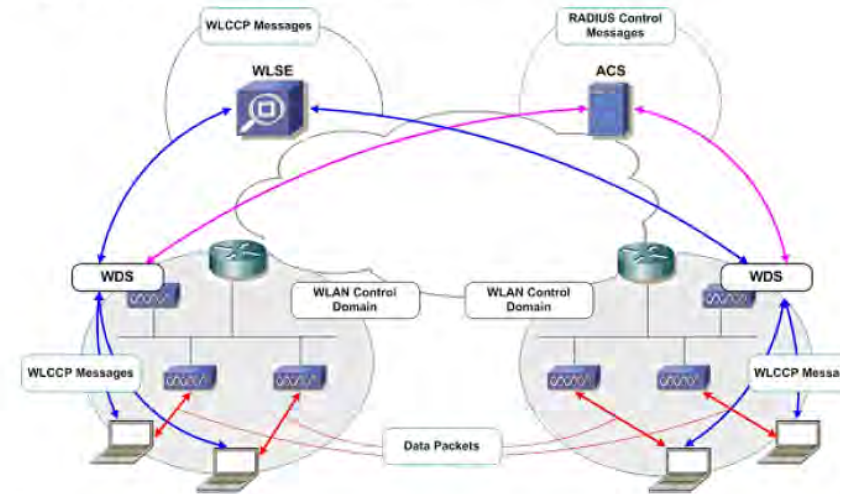
■ We'll go after the NSK's and derived CTK's later on...



WLCCP internals relevant here II

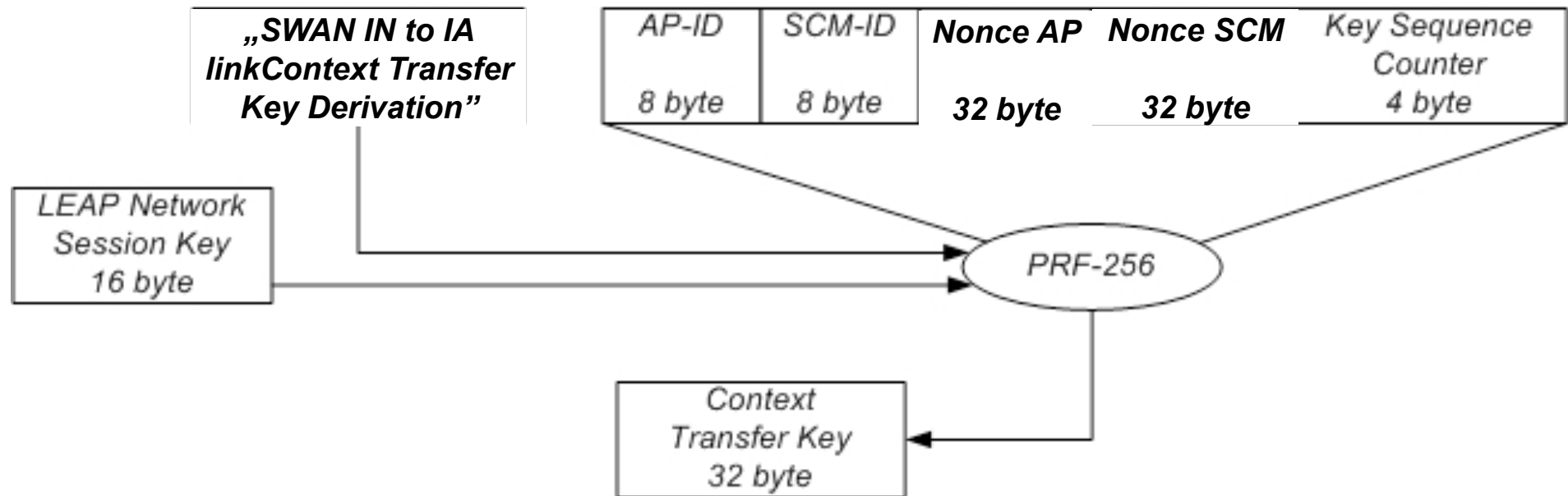


- **As *fast handoff* is an explicit design goal/feature of the SWAN/WDS/ WLCCP architecture, a mobile node associating with a different AP must be saved from undergoing a (new) full EAP exchange with authentication server.**
- **Cisco introduced a proprietary key management frame-work called *Cisco Centralized Key Management (CCKM)*.**
- **CCKM includes the support of exchanging already available cryptographic material that is relevant to mobile nodes (e.g. PMK's for WPA) between AP's. This exchange is protected by CTK's.**



CTK derivation

- A simple SHA1 using two nonce's and IDs
- NSK as the PRF key



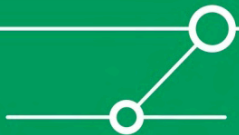
Two particularly interesting mimics of WLCCP

- **Perform election of WDS master**



- **Intra-AP communication**

- Authenticated by LEAP



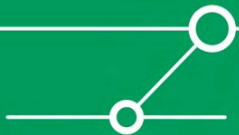
WDS master election

- **WDS master election performed based on \$PRIORITY**
 - Wasn't there another proprietary Cisco protocol with similar behavior?
→ right: HSRP
 - What happens if \$SOME_ENTITY with higher priority shows up?
→ right: DoS/potentially traffic redirection
 - Clever protocol design?
The jury is still out on that...
 - You'll see a DEMO on this in a second.



WLCCP intra-AP communication

- Authenticated by LEAP (“encapsulated in WLCCP”).
- But wait: “isn’t LEAP debatable, security-wise”?
- Cisco: “for additional protection we generate another key”.
- But... that key generation is based on previous LEAP authentication.
- Clever protocol design?
- ➔ The jury is still out on that...



Practical attack(s) against WLCCP



- **Get access to “wired AP backbone segment”**

- We’ve seen large department stores where everything (WLSE, AP’s, wired Windows clients, wireless point-of-sale systems etc.) was in *one big flat network* anyway.

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

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

- **Identify WLCCP speakers**

- **Sniff intra-AP traffic, crack LEAP, generate NSK’s / CTK’s**

- Strip current WDS master from it’s role if needed ;-)

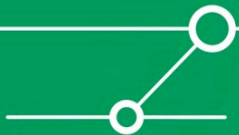
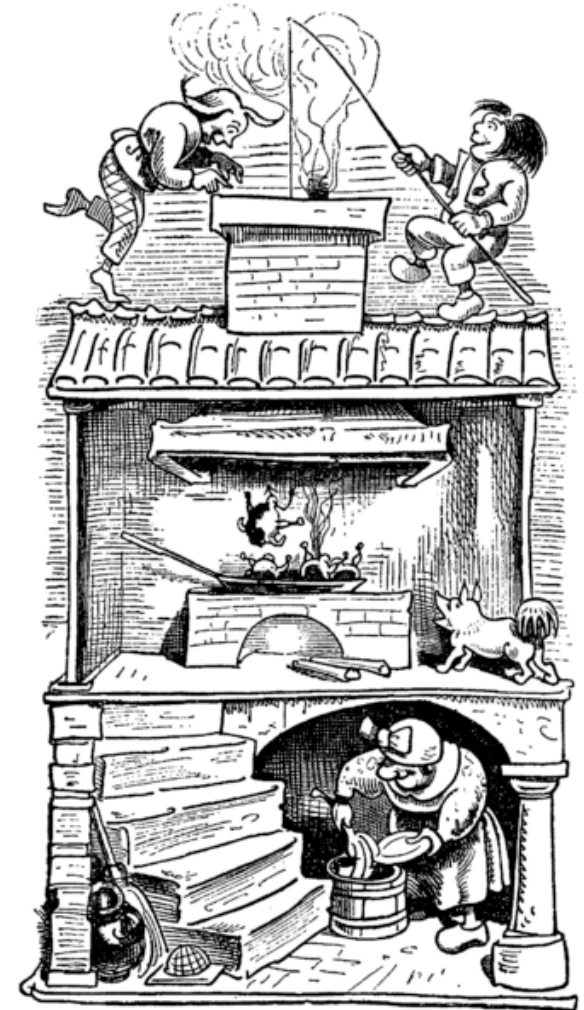
- **Use CTK’s to decrypt PMK’s when mobile node roams.**

- Decrypt mobile node’s network traffic afterwards...

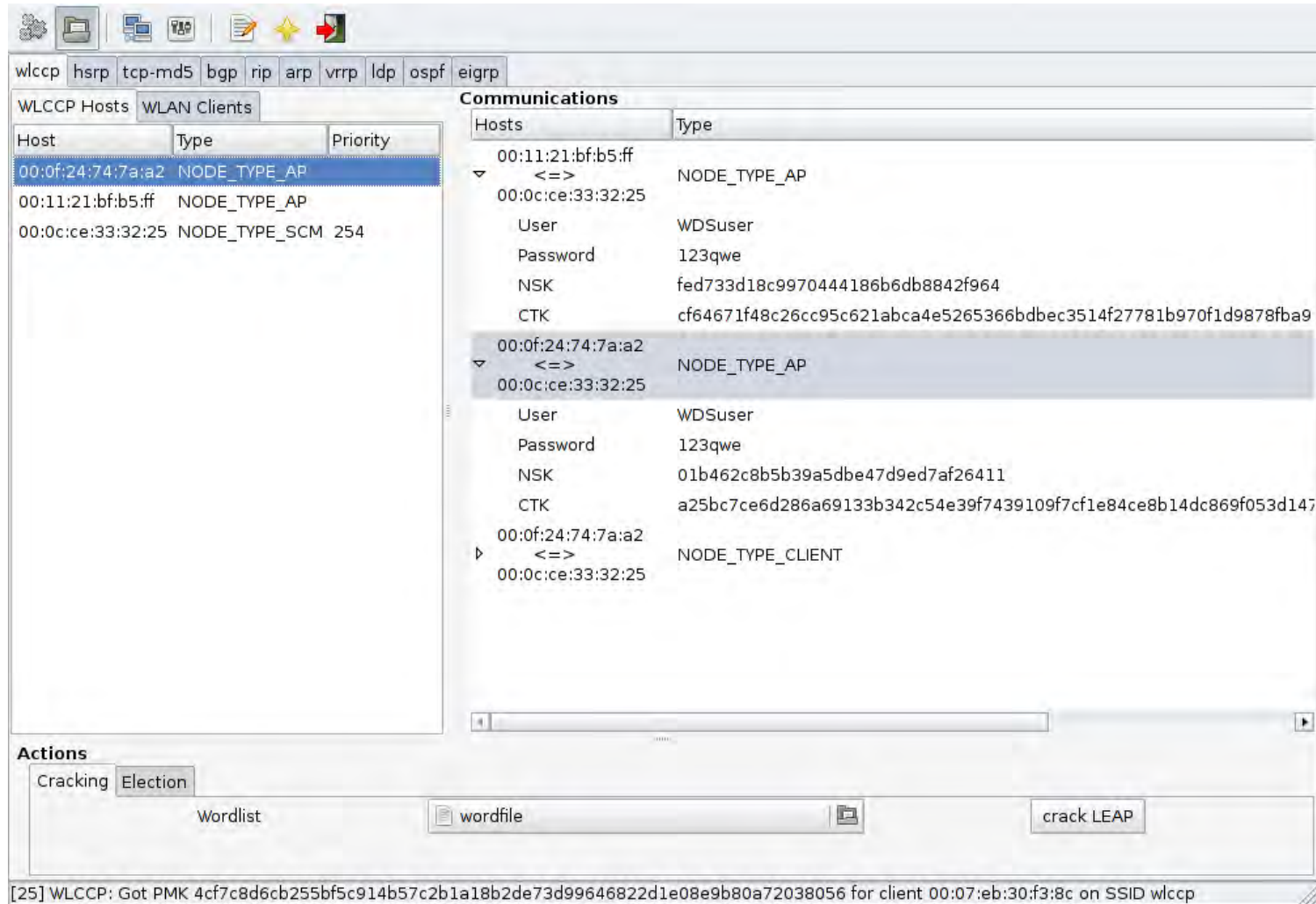


WLCCP – Meat

DEMO
;))



WLCCP – Meat



The screenshot shows the WLCCP software interface. The top menu bar includes protocols: wlccp, hsrp, tcp-md5, bgp, rip, arp, vrrp, ldp, ospf, and eigrp. The main window is divided into two panes: 'WLAN Clients' and 'Communications'.

WLAN Clients

Host	Type	Priority
00:0f:24:74:7a:a2	NODE_TYPE_AP	
00:11:21:bf:b5:ff	NODE_TYPE_AP	
00:0c:ce:33:32:25	NODE_TYPE_SCM	254

Communications

Hosts	Type
00:11:21:bf:b5:ff <=> 00:0c:ce:33:32:25	NODE_TYPE_AP
User	WDSuser
Password	123qwe
NSK	fed733d18c9970444186b6db8842f964
CTK	cf64671f48c26cc95c621abca4e5265366bdbec3514f27781b970f1d9878fba9
00:0f:24:74:7a:a2 <=> 00:0c:ce:33:32:25	NODE_TYPE_AP
User	WDSuser
Password	123qwe
NSK	01b462c8b5b39a5dbe47d9ed7af26411
CTK	a25bc7ce6d286a69133b342c54e39f7439109f7cf1e84ce8b14dc869f053d147
00:0f:24:74:7a:a2 > 00:0c:ce:33:32:25	NODE_TYPE_CLIENT

Actions

Cracking Election

Wordlist wordfile crack LEAP

[25] WLCCP: Got PMK 4cf7c8d6cb255bf5c914b57c2b1a18b2de73d99646822d1e08e9b80a72038056 for client 00:07:eb:30:f3:8c on SSID wlccp



For completeness' sake: WLSE, Attacks against mgmt



The screenshot shows the Cisco Security Advisory page for document ID 50400. The page title is "Cisco Security Advisory: A Default Username and Password in WLSE and HSE Devices". The advisory ID is "cisco-sa-20040407-username". The URL is "http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml". The revision is 1.4, and it was last updated on 2004 April 12 1700 UTC (GMT). The page includes a "Contents" section with links to Summary, Affected Products, Details, Impact, Software Versions and Fixes, Workarounds, Obtaining Fixed Software, Exploitation and Public Announcements, Status of This Notice: FINAL, Distribution, Revision History, and Cisco Security Procedures. A magnifying glass icon is positioned over the "Summary" section, which contains the text: "A default username/password pair is present in all releases of the Wireless LAN Solution Engine (WLSE) and Hosting Solution Engine (HSE) software. A user with this username has complete control of the device. This username cannot be disabled. There is no workaround. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml".



this username has complete control of the device. This username cannot be disabled. There is no workaround.

For completeness' sake:
WLSE, Attacks against mgmt (2010)

- **Lots of “classic web attacks” possible**

- Apache Header XSS
- XSS
- Logfile Download
- XSRF
- Directory Listing
- Response Splitting



- **We won't disclose any details here...**



Preliminary summary on SWAN

- **Excellent example for our thesis**

- Proprietary
- Some components built on COTS stuff (Linux, apache etc.)
- **Complex** and vulnerable.

- **Adding another layer to a weak authentication mechanism (LEAP) does not necessarily help.**

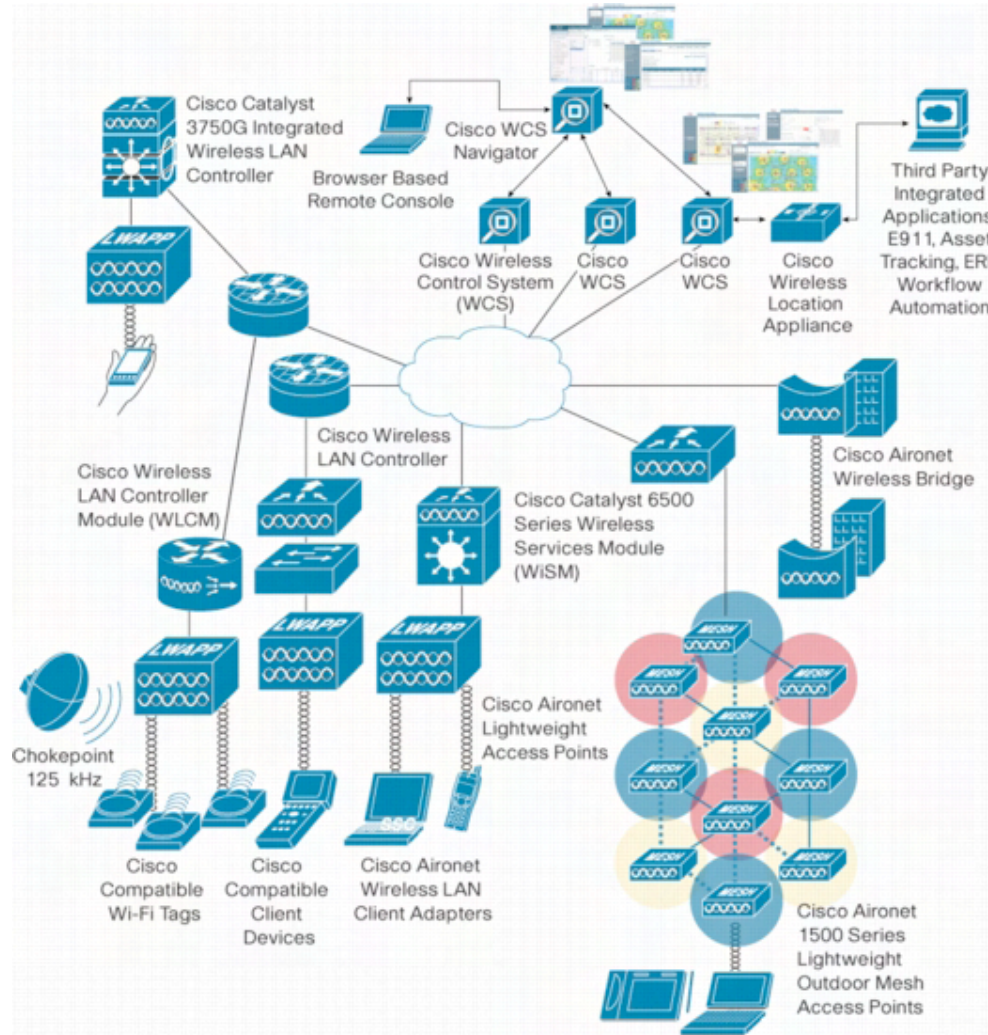
- Overall security depends on passwords. Use `_good_` ones if stuff in use.

- **Following “standard security BCP” would have helped.**

- Isolation / segmentation, strong authentication, yadda yadda yadda



CUWN – A simple overview ;-)



CUWN, Protocols & Crypto



- **Main protocol: CAPWAP**
- **Authentication involves *Datagram TLS* (DTLS, UDP based) with certificates.**
- **All security relevant data is encrypted and authenticated.**



CAPWAP

Bunch of RFC's, mainly

- ***RFC 4118 Architecture Taxonomy for Control and Provisioning of Wireless Access Points***
- ***RFC 5415 Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification***

Some additions to other protocols

- **DHCP**
- **802.11**



RFC 5415 – Mature and stable



- 3.1. UDP Transport

One of the CAPWAP protocol requirements is to allow a WTP to reside behind a middlebox, firewall, and/or Network Address Translation (NAT) device. [...]

When CAPWAP is run over IPv4, the UDP checksum field in CAPWAP packets **MUST** be set to zero.

- **Sure man, why use such annoying checksums at all. I mean UDP is reliable transport anyway, isn't it? ;-)**



CAPWAP – Assessment paths

- **Have a look at the crypto code**
 - Own, proprietary stuff? Re-use of (“open”) libraries?
 - If latter, any known vulnerabilities?
 - Which algorithms in use?
- **Have a look at the certificates**
 - Who trusts who, for which reason (certification path)?
- **We feel there’s some skeletons in the closet
→ TROOPERS2011 ;-)**



Included software/ bugs...

```
bash> strings AP-image |grep "art of OpenSSL"
```

```
Big Number part of OpenSSL 0.9.7b 10 Apr 2003
```

```
AES part of OpenSSL 0.9.7b 10 Apr 2003
```

```
[...]
```

```
SHA part of OpenSSL 0.9.7b 10 Apr 2003
```

```
Stack part of OpenSSL 0.9.7b 10 Apr 2003
```

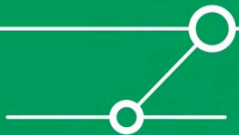
```
SSLv2 part of OpenSSL 0.9.7b 10 Apr 2003
```

```
SSLv3 part of OpenSSL 0.9.7b 10 Apr 2003
```

```
SSLv2/3 compatibility part of OpenSSL 0.9.7b 10 Apr 2003
```

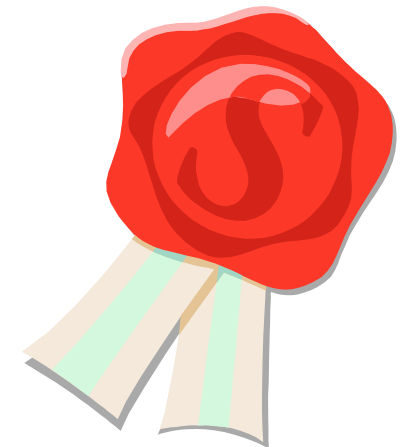
```
TLSv1 part of OpenSSL 0.9.7b 10 Apr 2003
```

Cisco told us they had ported OpenSSL into IOS back in 2003 (and license was reviewed by legal).



CAPWAP – On Certificates

- **Certificates signed by *Cisco's Manufacturing CA (MIC)* installed in the course of manufacturing process.**
 - This is a good thing.
 - We recommend this to every network hardware vendor!
- **Per default every MIC certificate is trusted.**
 - So any piece of Cisco HW might be trusted
 - ... even if it was not deployed by yourselves ;-)
- **One can deploy own certificate chain.**
 - Adds (even) more complexity though.



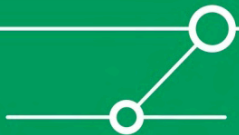
CUWN, Management (Attacks)

- **SNMP ... our old friend ;-)**

- On WLC enabled by default.
- Heavily used for WLC ↔ WCS communication.
- Traditional default communities (`public/private`).
- Yes, sure, those could (& should) be changed.
- Still, given overall complexity → people happy the stuff runs at all (“we’ll harden it later”...).



- **HTTP(S)**



Talking about mgmt...what's this?

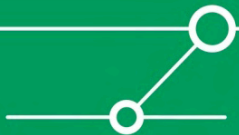
A screenshot of the Wireshark network protocol analyzer interface. The title bar reads "1242_wlc_join_20091216.pcap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, navigation, and analysis. The filter field is set to "syslog". The packet list pane shows several captured packets, with packet 9 selected. The packet details pane for packet 9 shows the following structure:

- 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 AP does not have 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



SNMP @ WLC

- **Get release number (think “show version”)**
- **Identify AP’s currently associated (+ some info about)**
- **Get IP configuration of all AP’s**
 - Can be “set” (on WLC) as well
- **All kinds of key stuff with strange names.**



SNMP @ WLC, Syslog data?



```
SNMPv2-SMI::enterprises.14179.1.1.2.4.1.22.10111 = STRING: " Rogue AP : 00:23:08:65:2a:f8  
removed from Base Radio MAC : 00:21:1b:eb:60:70 Interface no:0(802.11n24) "
```

```
SNMPv2-SMI::enterprises.14179.1.1.2.4.1.22.10112 = STRING: " Rogue AP : 00:23:08:65:2a:f8  
detected on Base Radio MAC : 00:21:1b:eb:60:70 Interface no:0(802.11b/g) with RSSI: -91 and  
SNR: 5 and Classification: unclassified"
```

```
SNMPv2-SMI::enterprises.14179.1.1.2.4.1.22.10113 = STRING: " Rogue AP : 00:23:08:65:2a:f8  
detected on Base Radio MAC : 00:26:99:22:e1:20 Interface no:0(802.11b/g) with RSSI: -89 and  
SNR: 4 and Classification: unclassified"
```

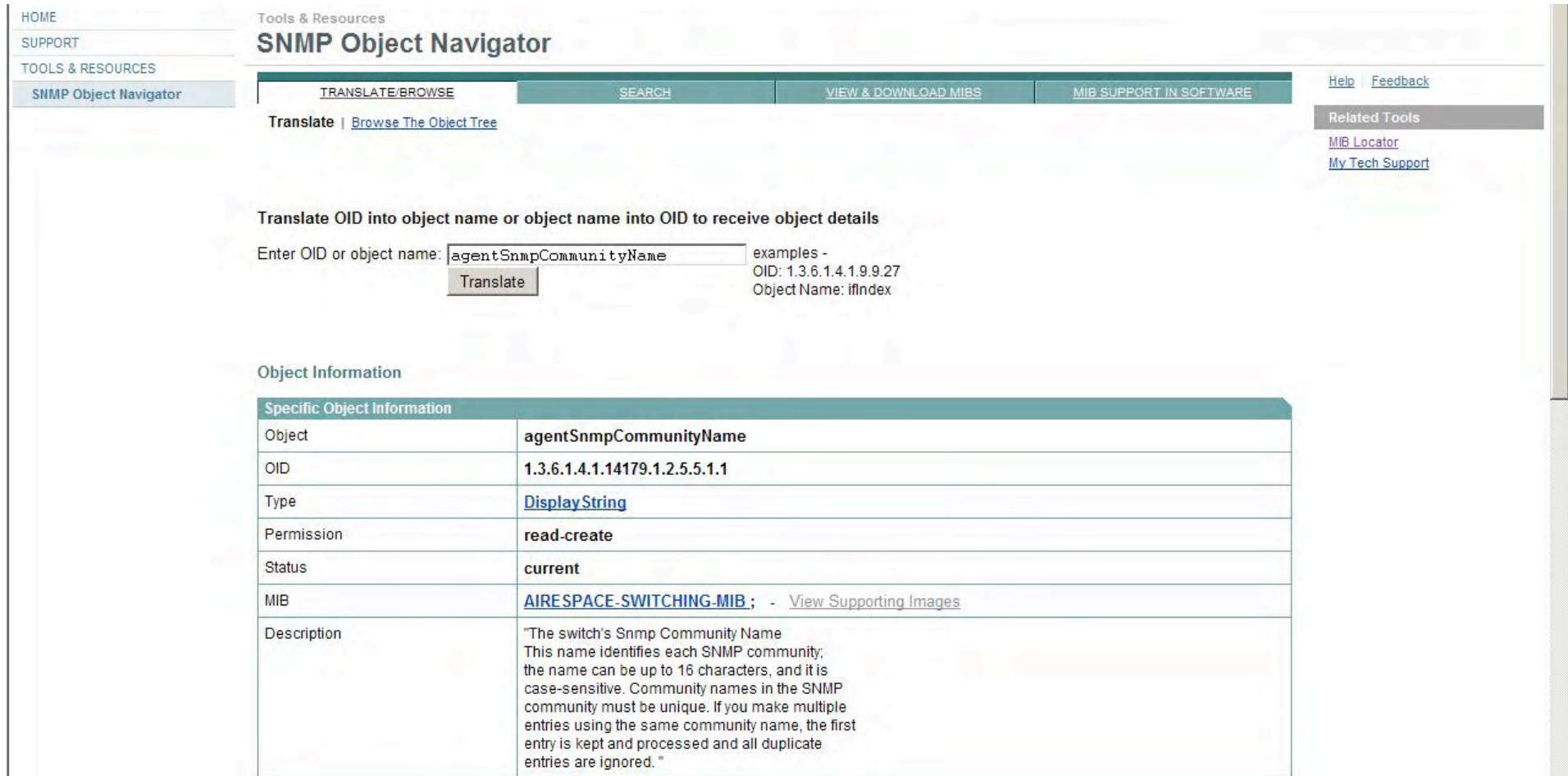
```
SNMPv2-SMI::enterprises.14179.1.1.2.4.1.22.10114 = STRING: " Rogue AP : 00:23:08:2d:9d:1a  
detected on Base Radio MAC : 00:21:1b:eb:60:70 Interface no:0(802.11b/g) with RSSI: -93 and  
SNR: 2 and Classification: unclassified"
```

```
SNMPv2-SMI::enterprises.14179.1.1.2.4.1.22.10115 = STRING: " Rogue AP : 00:1c:4a:02:d9:13  
removed from Base Radio MAC : 00:26:99:22:e1:20 Interface no:0(802.11n24) "
```

```
SNMPv2-SMI::enterprises.14179.1.1.2.4.1.22.10116 = STRING: " Rogue AP : 00:1c:4a:02:d9:13  
removed from Base Radio MAC : 00:21:1b:eb:60:70 Interface no:0(802.11n24) "
```



SNMP @ WLC, SNMP communities



The screenshot shows the 'SNMP Object Navigator' web application. The main heading is 'SNMP Object Navigator' with sub-headings 'TRANSLATE/BROWSE', 'SEARCH', 'VIEW & DOWNLOAD MIBS', and 'MIB SUPPORT IN SOFTWARE'. Below this is a search bar with the text 'agentSnmCommunityName' and a 'Translate' button. To the right of the search bar are examples: 'examples -', 'OID: 1.3.6.1.4.1.9.9.27', and 'Object Name: ifIndex'. Below the search bar is the 'Object Information' section, which contains a table with the following data:

Specific Object Information	
Object	agentSnmCommunityName
OID	1.3.6.1.4.1.14179.1.2.5.5.1.1
Type	Display String
Permission	read-create
Status	current
MIB	AIRESPACE-SWITCHING-MIB ; - View Supporting Images
Description	"The switch's Snmp Community Name This name identifies each SNMP community; the name can be up to 16 characters, and it is case-sensitive. Community names in the SNMP community must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored."

Permission: "read-create" → still, access was somehow restricted (views?).



SNMP @ WLC, usernames & passwords



- **Get names of all users, incl. local_admins**

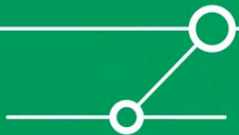
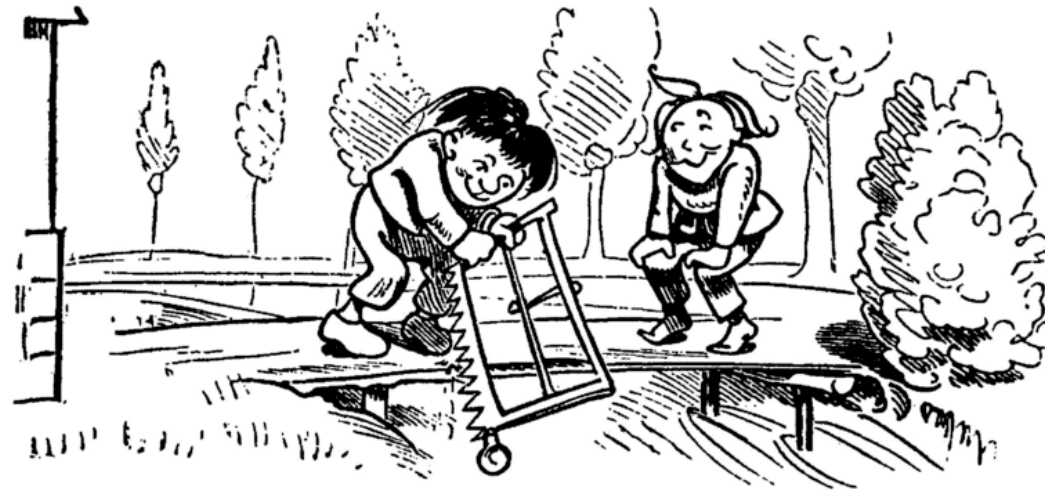


- **Unfortunately, passwords are obfuscated**
 - ... and can't be overridden (*read-create* OID's)

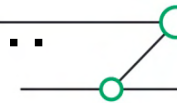


But hey...

- **Why (re-) set password of existing user if new (admin) users can be created? ;-)**



WCS – After all, there’s a webinterface...



The screenshot shows the Cisco WCS web interface. At the top, there is a navigation bar with the Cisco logo, 'WCS' status indicators, and the title 'Wireless Control System'. A search bar is located on the right with the placeholder '<IP,Name,SSID,MAC>' and a 'Search' button. Below the search bar, the user is logged in as 'root @ Virtual Domain: root'. The main navigation menu includes 'Monitor', 'Reports', 'Configure', 'Administration', 'Tools', and 'Help'. The current page is 'Clients', with a sub-menu 'Monitor > Clients'. A search filter is set to 'Associated Clients' and the results show 'None detected'. A modal dialog box titled 'Meldung von Webseite' is displayed in the foreground, containing a warning icon and the text 'get skilled or get owned', with an 'OK' button at the bottom.



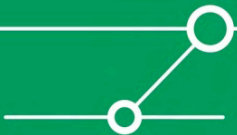
Btw: mod_security ruleset on WCS  ERNW
Living Security.

```
# check incoming request for possible XSS server attacks
```

```
# Look for malicious tags in request
```

```
SecFilter "<(\s)*(script|object|embed|applet|form|meta) "
```

(stripped-down to the essential part)

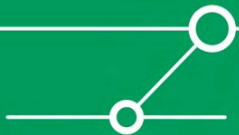


WLC reboot anyone?

```
-----  
Interrupt Status  
-----  
Task Summary  
-----  
Message Logs  
  
Dumping task specific information emWeb  
Crash function not supported by this task  
  
*****  
*           End Cisco Crash Handler           *  
*****  
  
Cisco Crash Handler  
This build was configured to copy this crash information to  
a file called: "/mnt/application/mwar_dump1.crash"  
  
Uploading the core file ...
```

Conclusions

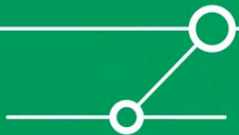
- **“Enterprise WLAN solutions“ might be complex beasts.**
- **Be aware that there might be some obvious or not-so-obvious security vulnerabilities.**
- **Use *common sense* when deploying ;-)**
- **All these kinds of problems are not specific to Vendor C or to WLAN solutions.**



Shameless Announcements

- **Tool “LOKI” to be released in july 2010**
 - Multi function router attack tool with GUI (think: “yersinia on layer 3”)

- **Updated version of this talk + code in the next months.**



There's never enough time...

THANK YOU...



...for yours!

