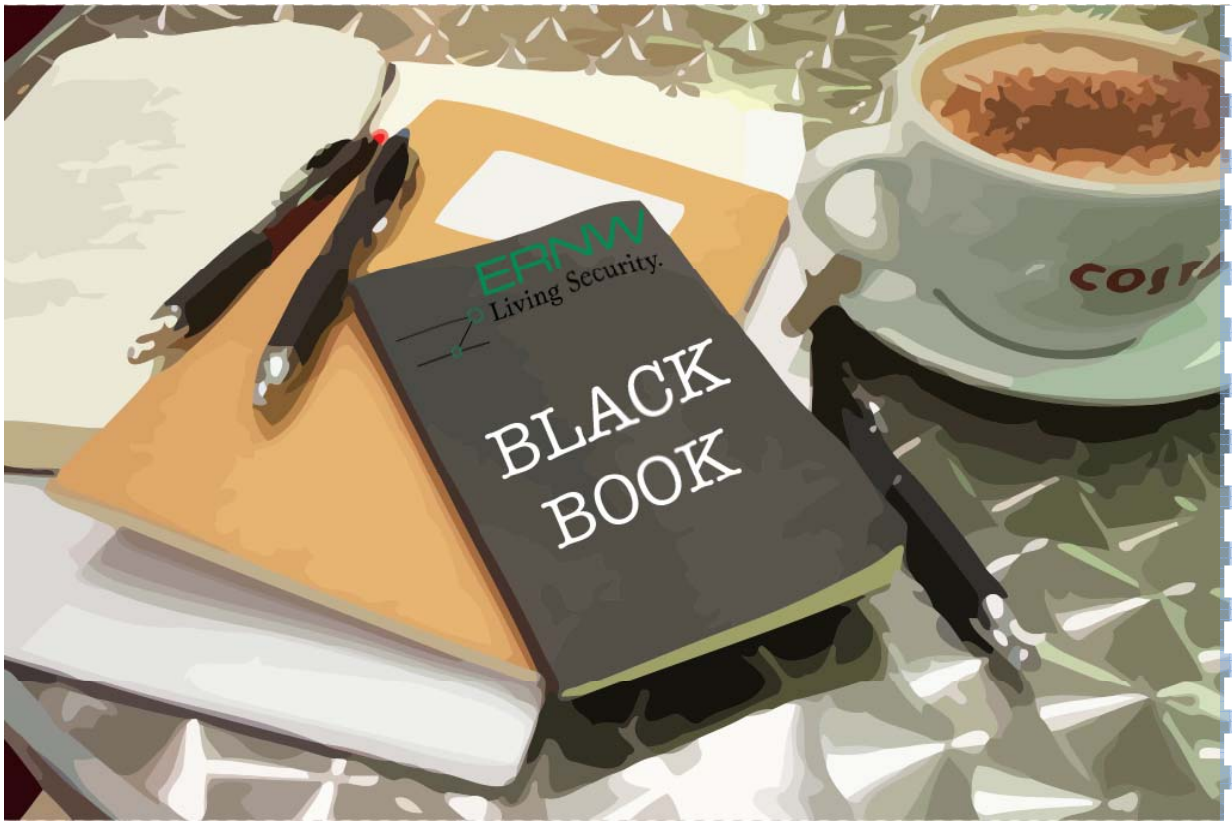
ERNW
Living Security.



TODAY:

Some Security Notes on Cisco Enterprise WLAN Solutions

Daniel Mende, Enno Rey

{dmende, oroeschke, erey}@ernw.de

Who we are

- **Old-school network geeks, working as security researchers for**
- **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**

Agenda

ERNW Living Security.

- **Introduction & Dimensions of this talk**
- **Technology overview & attack paths**
- **Attacks in the SWAN world**
- **Attacks in the CUWN world**
- **Summary & Outlook**

Background of this talk

ERNW Living Security.

- **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 ;-)

Background of this talk

ERNW Living Security.

- **Practically no independent security assessment of this stuff (publicly) available → we built a lab and started fiddling around.**

- **Fortunately some $VERY_LARGE_ENTERPRISE paid some man-days of this work. Thanks for that! (you know who you are…)**

Goals of this talk

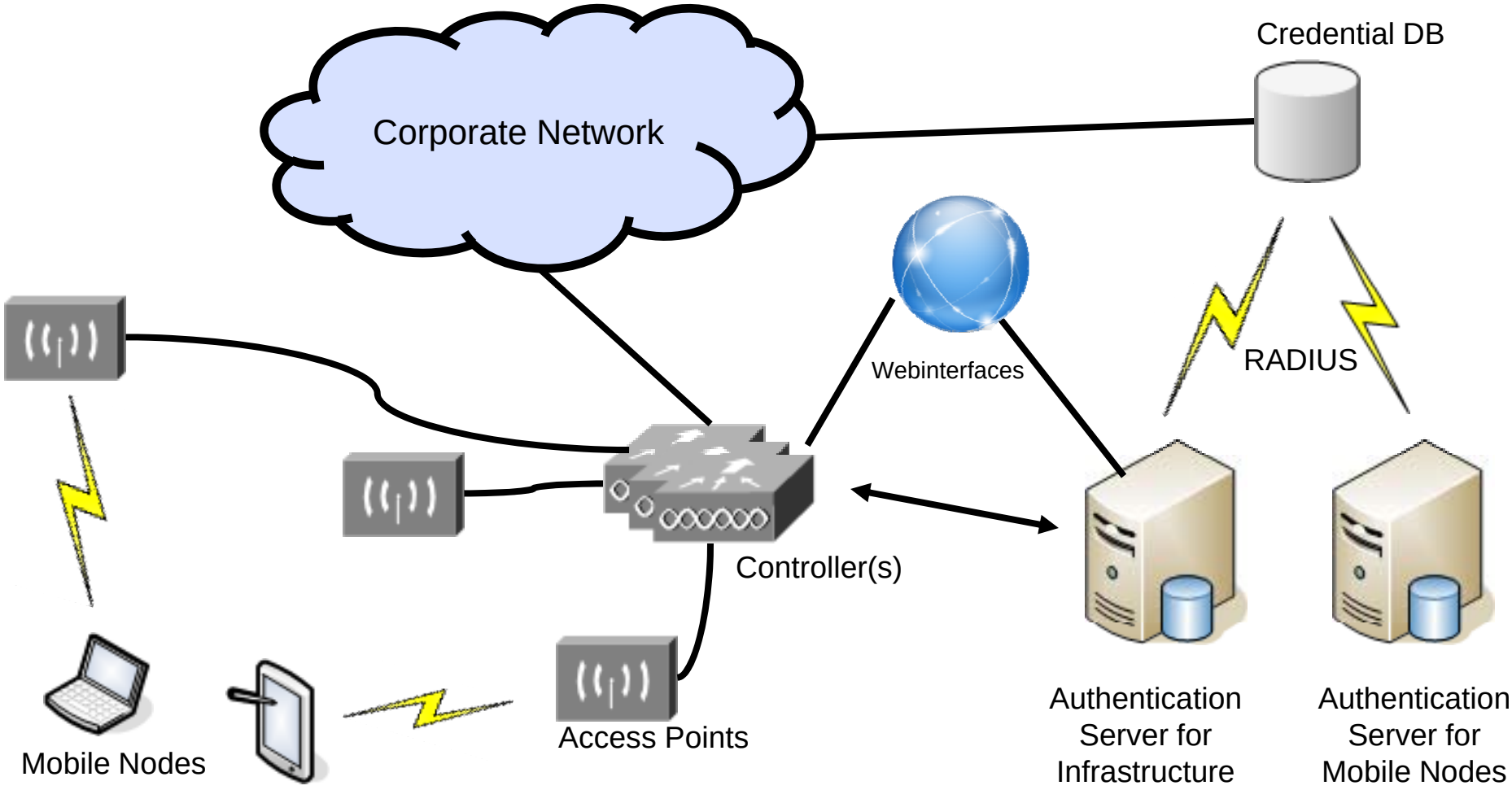
ERNW Living Security.

- **Provide some publicly available security research ;-)**

- **Furthermore we'd like to discuss protocol design considerations in general.**

- **Demonstrate the hidden/obscure vulnerabilities of $SOME_TECH_ENTERPRISE_SOLUTIONS (not just in WLAN space…).**

Overview


Credential DB
Corporate Network
Webinterfaces
RADIUS
Controller(s)
Mobile Nodes
Access Points
Authentication Server for Infrastructure
Authentication Server for Mobile Nodes

Preliminary conclusions for our research

ERNW Living Security.

- **Highly proprietary stuff (including protocols)**
  - → not easy to understand and not too well documented either.
  - → “legal boundaries” when performing security research.

Flavors / Generations

ERNW Living Security.

From our perspective three generations can be identified.

- **Structured Wireless-Aware Networks (SWAN)**

- **Based on managed APs & LWAPP**
  - After *Airespace* acquisition in 2005
  - Still some interesting remnants from *Airespace* age present today…
- ***Cisco Unified Wireless Network* (CUWN) w/ CAPWAP**

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

Main attack paths

ERNW Living Security.

- **Attacks against traffic in transit**

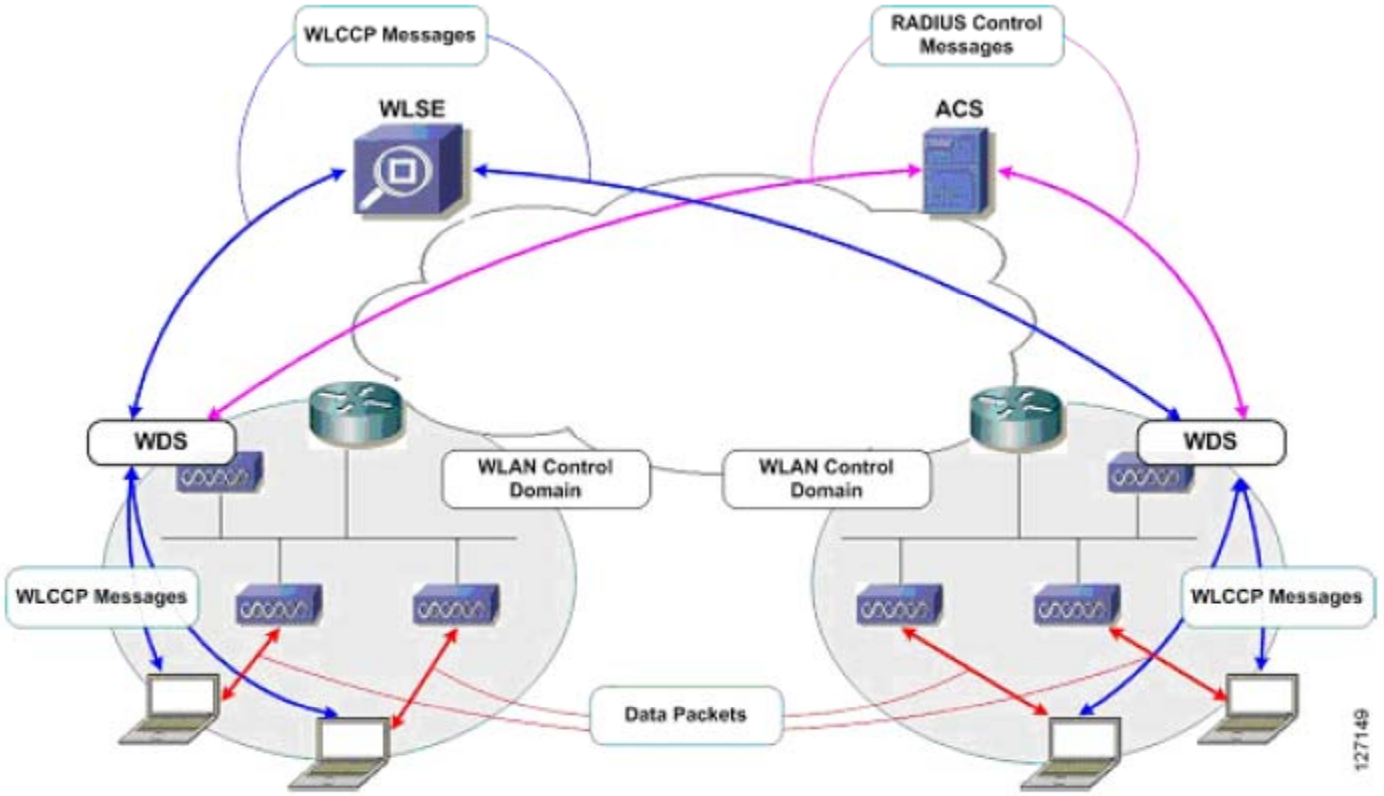
- **Attacks against cryptographic material**
  - Somehow related to attacks against traffic in transit ;-)
  - Might be used of different purposes though
    - E.g. injection of rogue devices

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

Du côté de chez Swan(n)

ERNW Living Security.

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

ERNW Living Security.

- ***Wireless LAN Context Control Protocol***
- **Described essentially in two *US Patents***
  - Wireless local area network context control protocol
  - 802.11 using a compressed reassociation 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 I

ERNW Living Security.

- **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 NSKs and derived CTKs later on…**

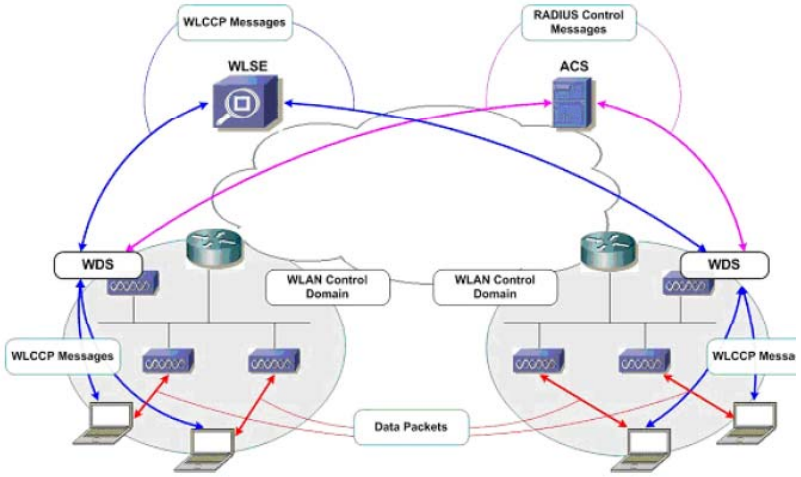
WLCCP internals relevant here II

ERNW Living Security.

- **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).**

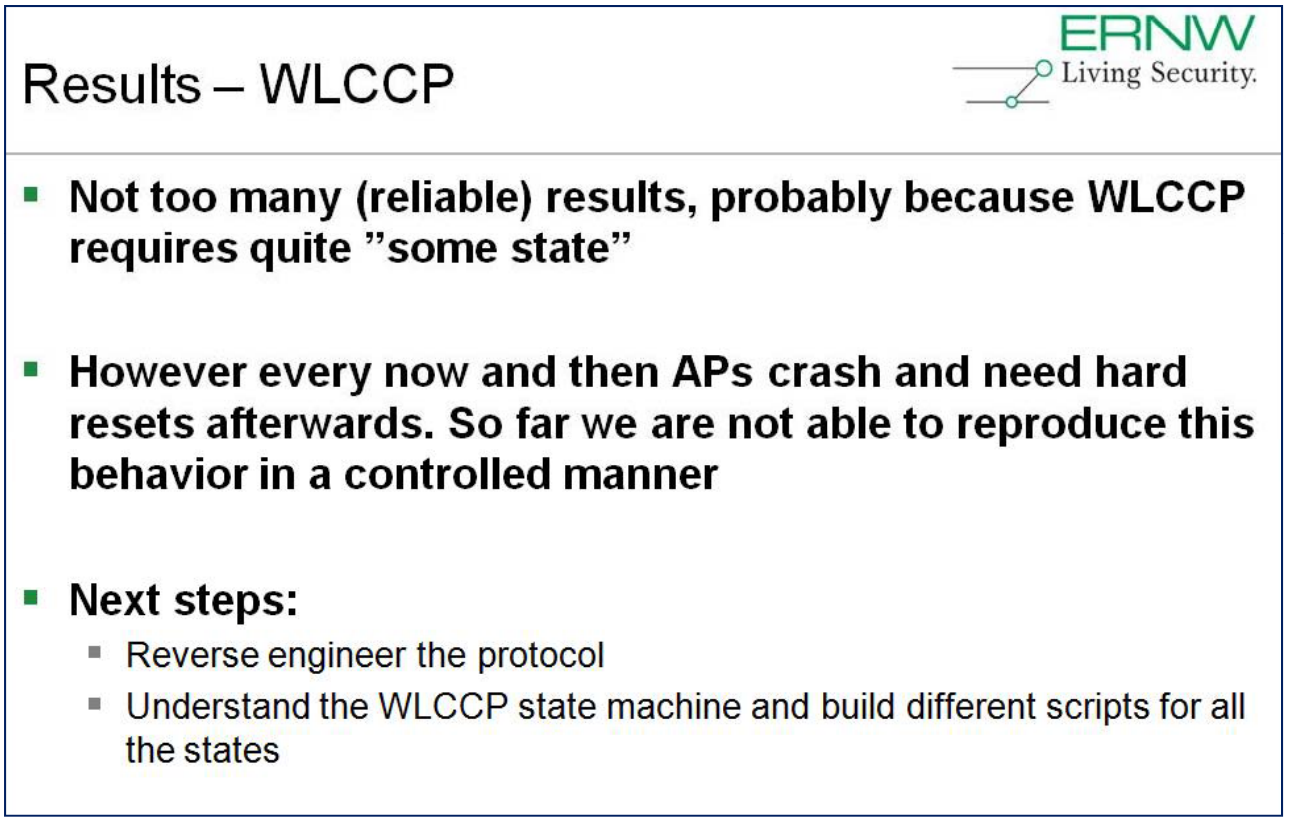
- **CCKM includes the support of exchanging already available crypto-graphic material that is relevant to mobile nodes (e.g. PMKs for WPA) between APs. This exchange is protected by CTKs.**



Before we start hacking WLCCP, some notes from history

ERNW Living Security.

- **At ShmooCon 2008 we gave a talk on *Layer 2 Fuzzing*:**



Results – WLCCP

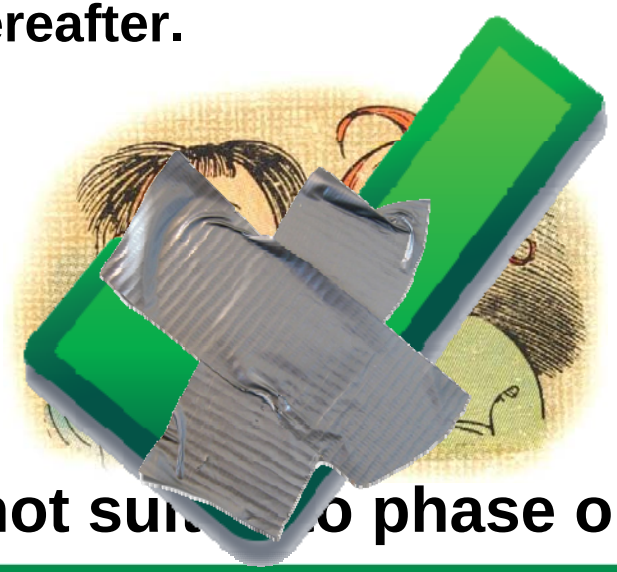
ERNW Living Security.

- **Not too many (reliable) results, probably because WLCCP requires quite "some state"**
- **However every now and then APs crash and need hard resets afterwards. So far we are not able to reproduce this behavior in a controlled manner**
- **Next steps:**
  - Reverse engineer the protocol
  - Understand the WLCCP state machine and build different scripts for all the states

Some notes from history, cont.

ERNW Living Security.

- **Shortly after ShmooCon talk another German security researcher contacted us, for “information exchange on WLCCP”.**
- **Turned out he had some simple *Scapy* scripts, targeting WLCCP and reliably crashing Aps.**
- **We initiated disclosure with Cisco and filed his and our findings. Bugs were silently fixed thereafter.**



→ Still, all this was not sufficient to phase our interest down…

Back on track: two particularly interesting mimics of WLCCP

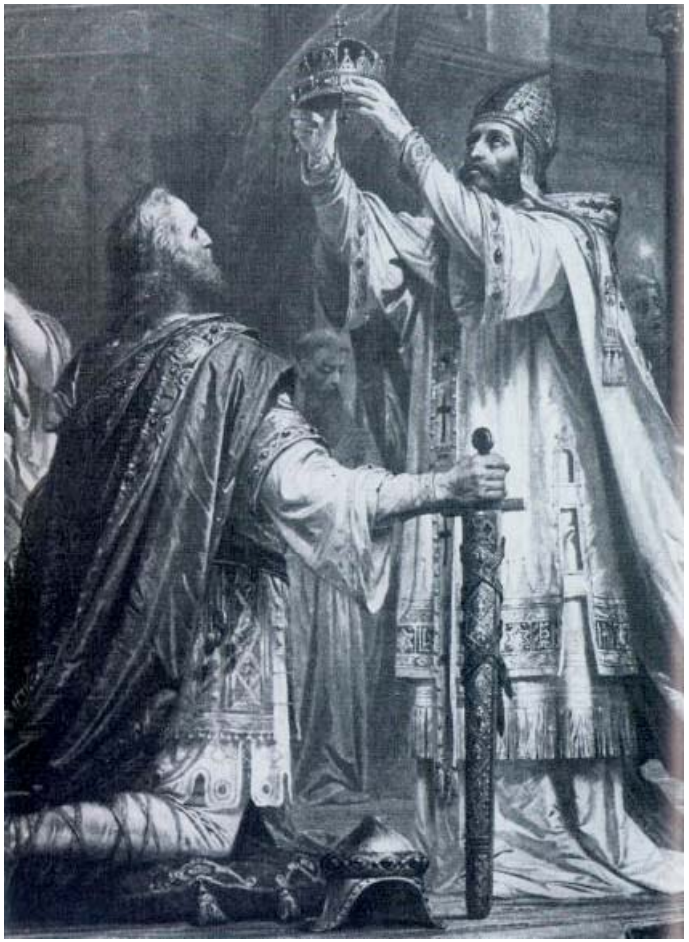
ERNW Living Security.

- **Perform election of WDS master**

- **Intra-AP communication**
  - Authenticated by LEAP

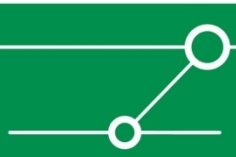
WDS master election

- **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…
  - DEMO



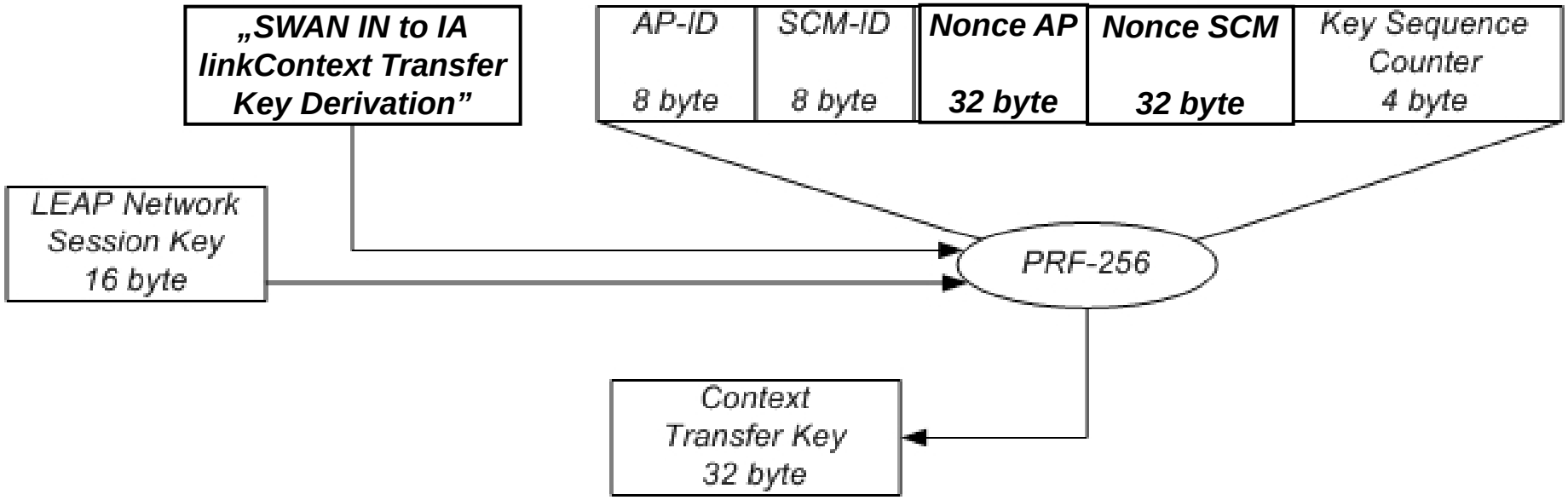
WLCCP intra-AP communication

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



CTK derivation

- **A simple SHA1 using two nonces and IDs**
- **NSK for HMAC**



Practical attack(s) against WLCCP

ERNW Living Security.

- **Get access to "wired AP backbone segment"**
  - We've seen large department stores where everything (WLSE, APs, wired Windows clients, wireless point-of-sale systems etc.) was in *one big flat network* anyway.
- **Identify WLCCP speakers**

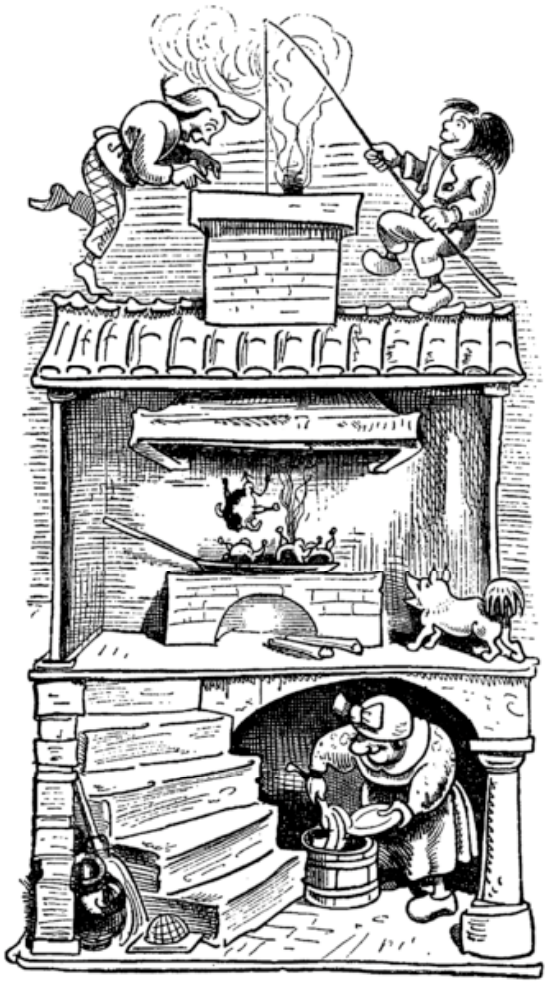
```
Interesting ports on 192.168.88.3:
PORT     STATE         SERVICE
2887/udp open|filtered unknown (3)
MAC Address: 00:40:63:E3:19:BC (VIA Technologies)

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)
```

- **Sniff intra-AP traffic, crack LEAP, extract NSKs/CTKs**
  - Strip current WDS master from it's role if needed ;-)
- **Use CTKs to decrypt PMKs when mobile node roams.**
  - Decrypt mobile node's network traffic afterwards…

WLCCP – Meat

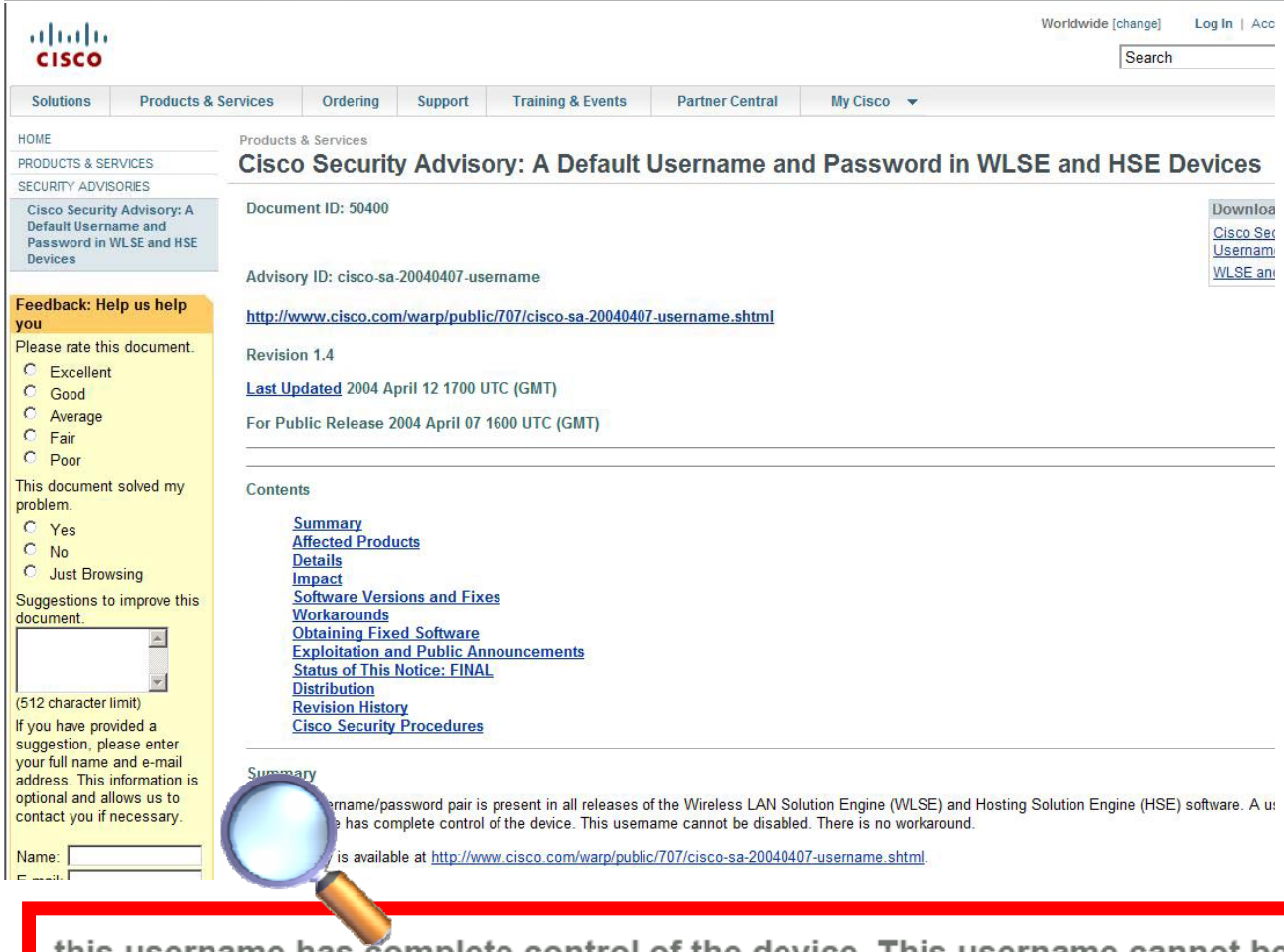
ERNW
Living Security.

DEMO
;)



For completeness' sake: WLSE, Attacks against mgmt

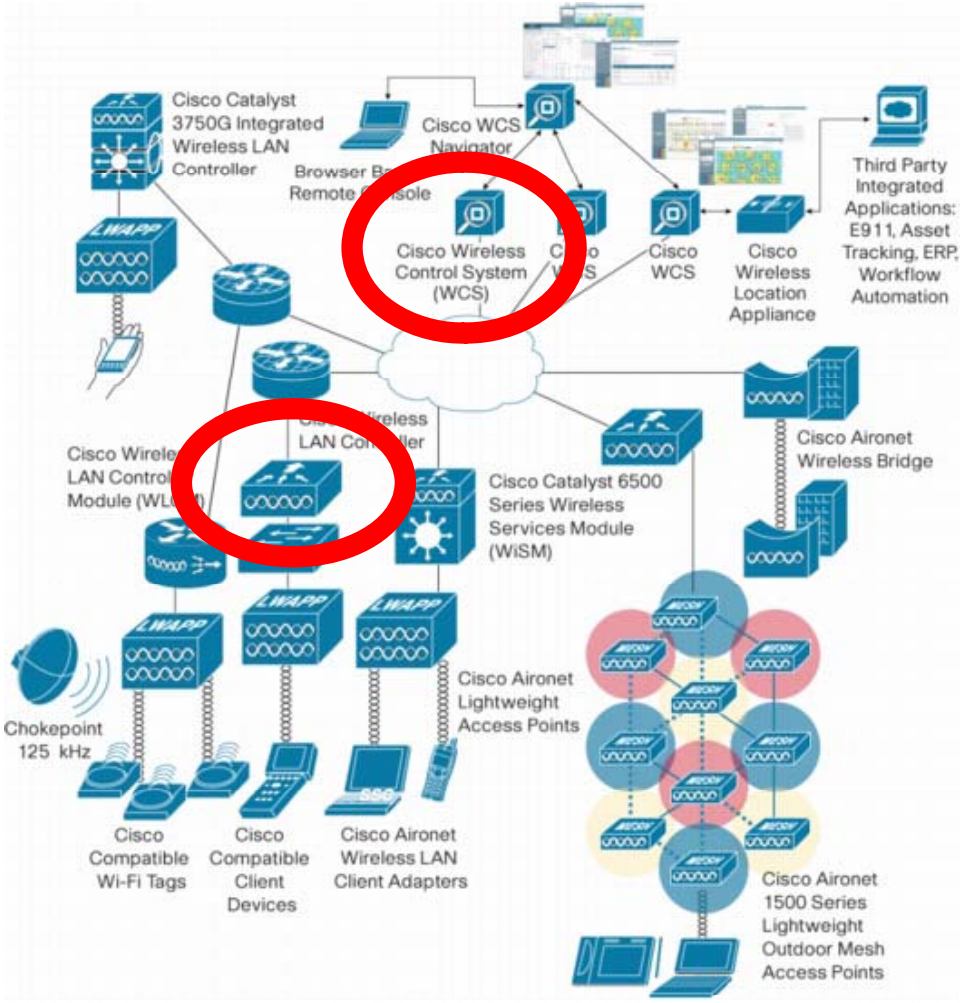
ERNW Living Security.



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

CUWN – A simple overview ;-)

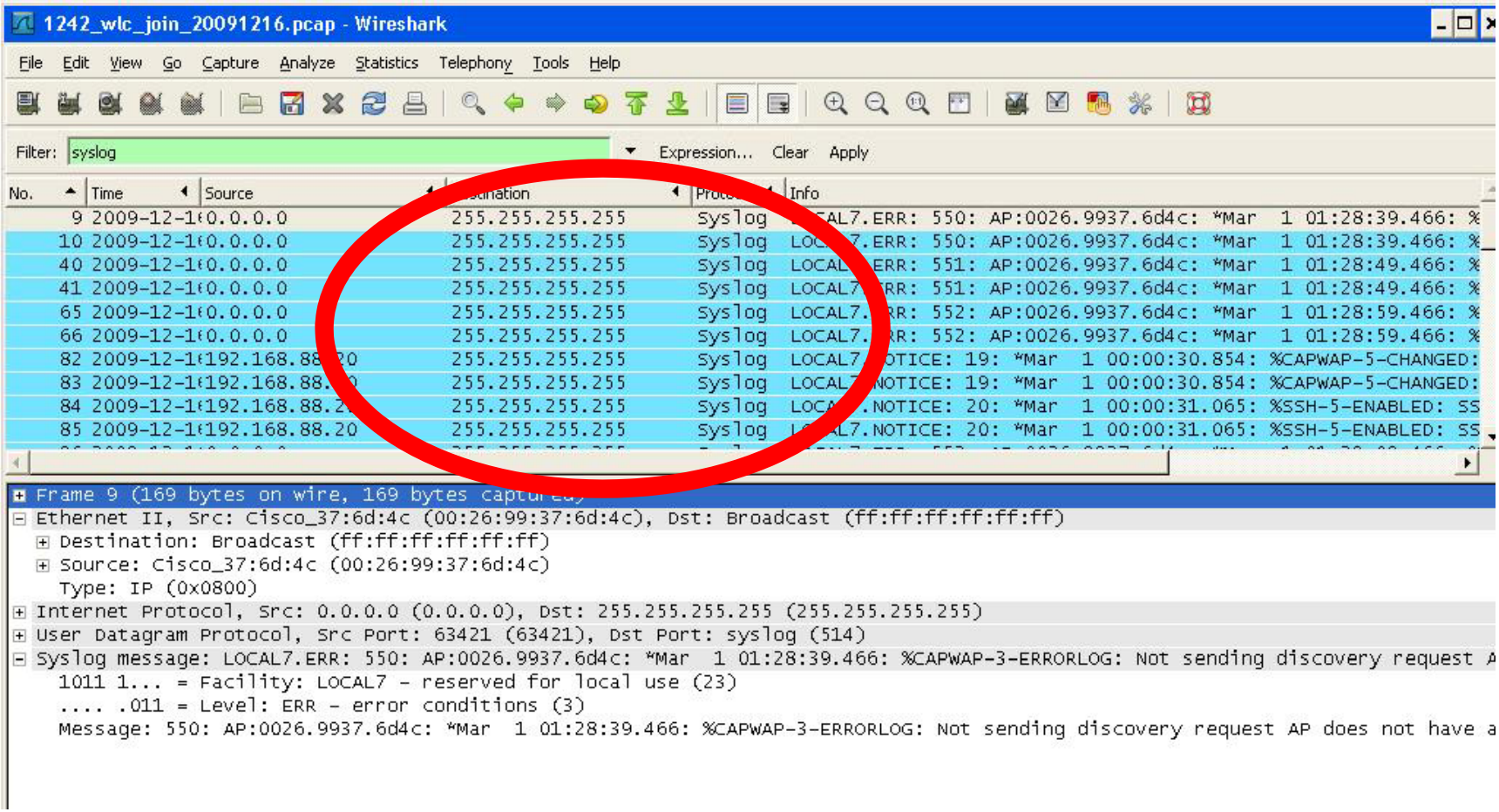
ERNW Living Security.



From: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_brochure09186a0080184925_ns337_Networking_Solution_Solution_Overview.html

Talking about mgmt…what's this?

ERNW Living Security.



CUWN, Protocols & Crypto

ERNW Living Security.

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

CAPWAP

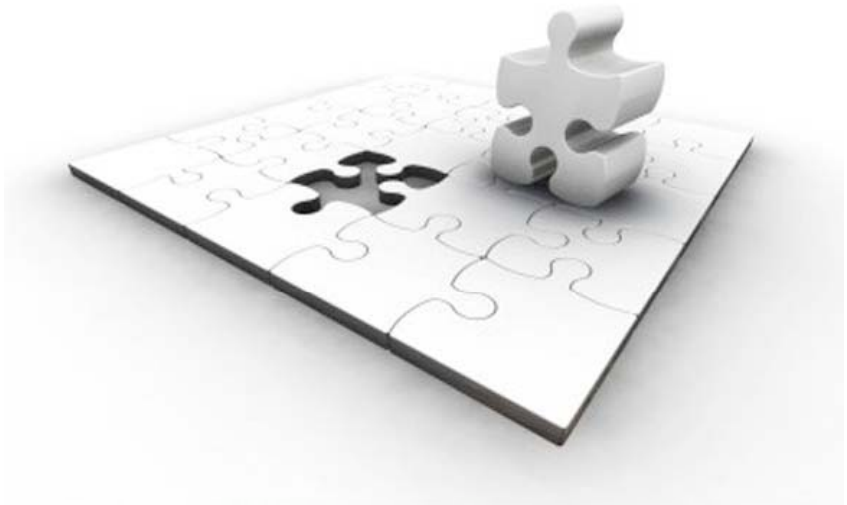
ERNW Living Security.

Bunch of RFCs, 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

ERNW Living Security.

- **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

ERNW Living Security.

- **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 => Troopers 2011 ;-)**

Included software/ bugs…

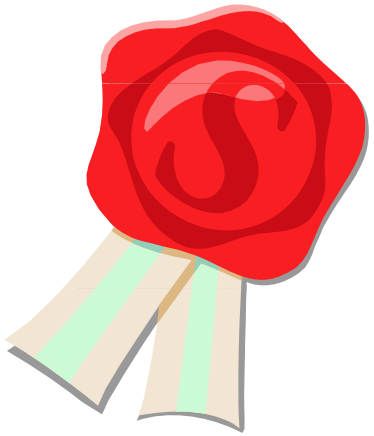
```
bash> strings AP-image |grep "art of OpenSSL"

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

ERNW Living Security.

- **Certificates signed by *Cisco's Manufacturing CA* (MIC) installed in the course of manufacturing process.**
- **Per default every MIC certificate is trusted.**
  - So every 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)

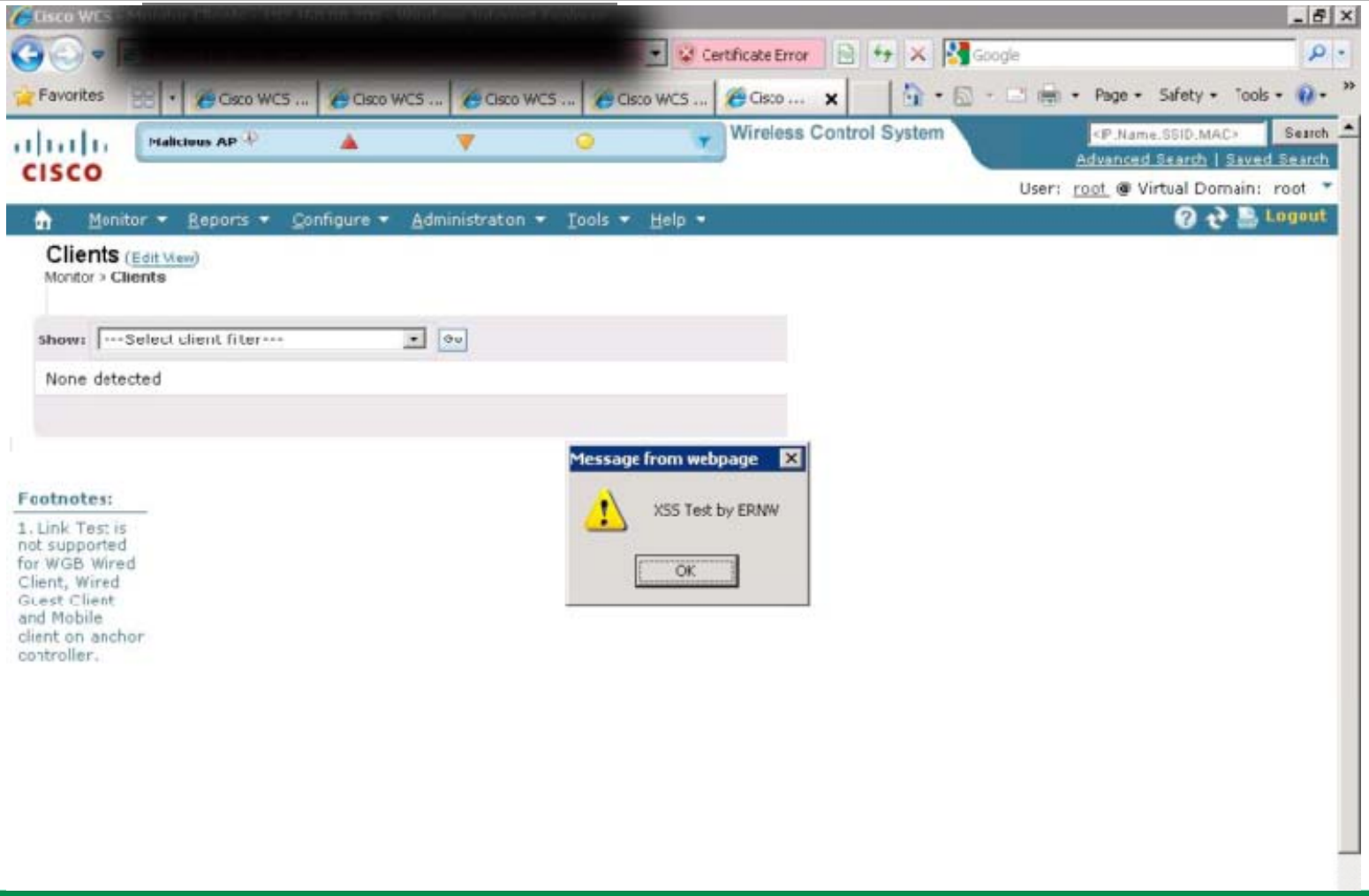
ERNW Living Security.

- **WCS, Webinterface**

- **SNMP … our old friend ;-)**
  - On WLC enabled by default.
  - Heavily used for WLC ⇔ WCS communication.
  - Classic 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"…).

WCS – After all, it's a webinterface…

ERNW Living Security.



SNMP @ WLC

ERNW Living Security.

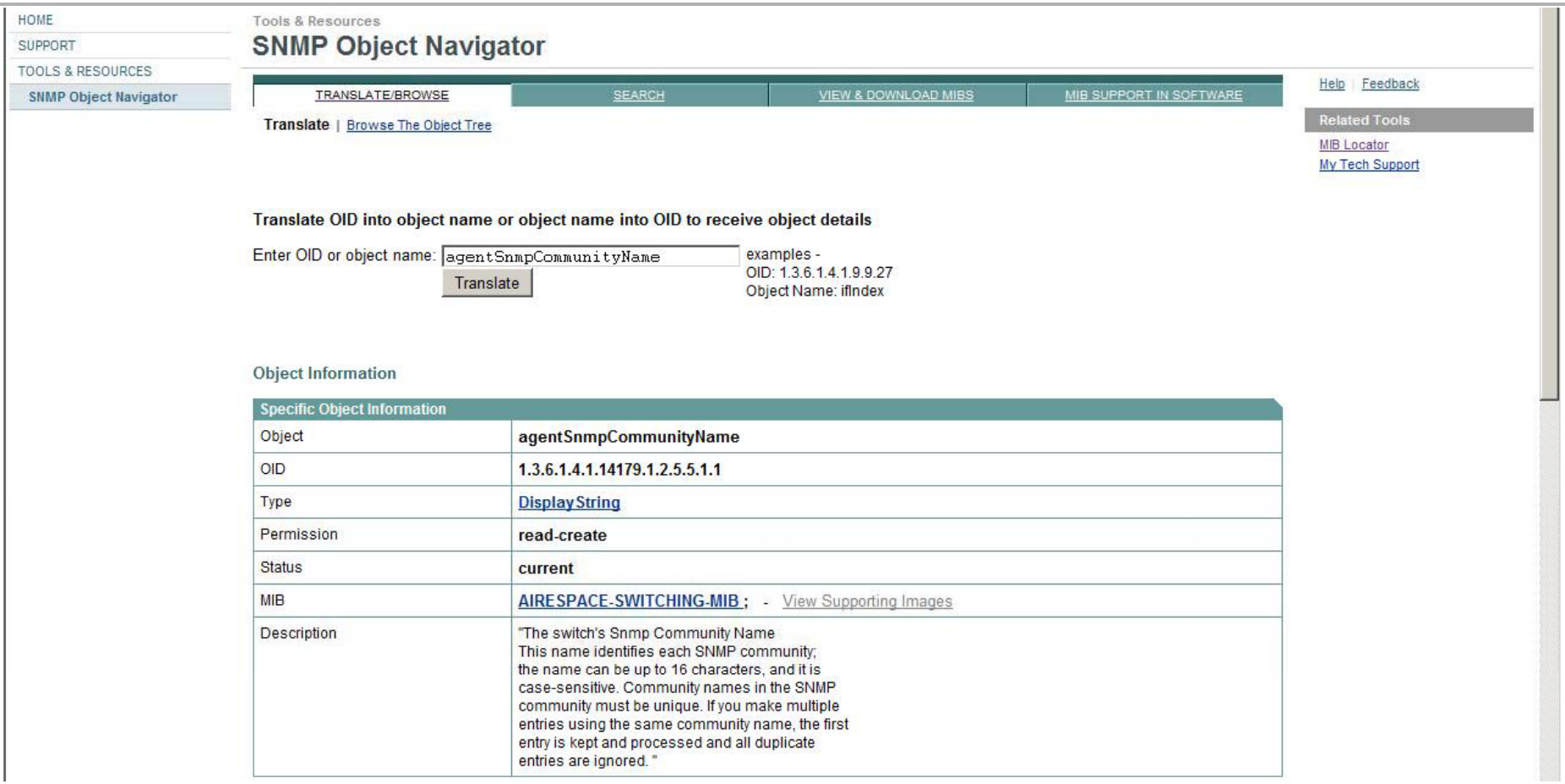
- **Get release number (think “show version”)**
- **Identify APs currently associated (+ some info about)**
- **Get IP configuration of all APs**
  - Can be “set” (on WLC) as well
- **All kinds of key stuff with strange names.**

SNMP @ WLC, Syslog data?

ERNW Living Security.

```
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



Permission: “read-create” => still, access was somehow restricted (views?).

SNMP @ WLC, usernames & passwords

ERNW Living Security.

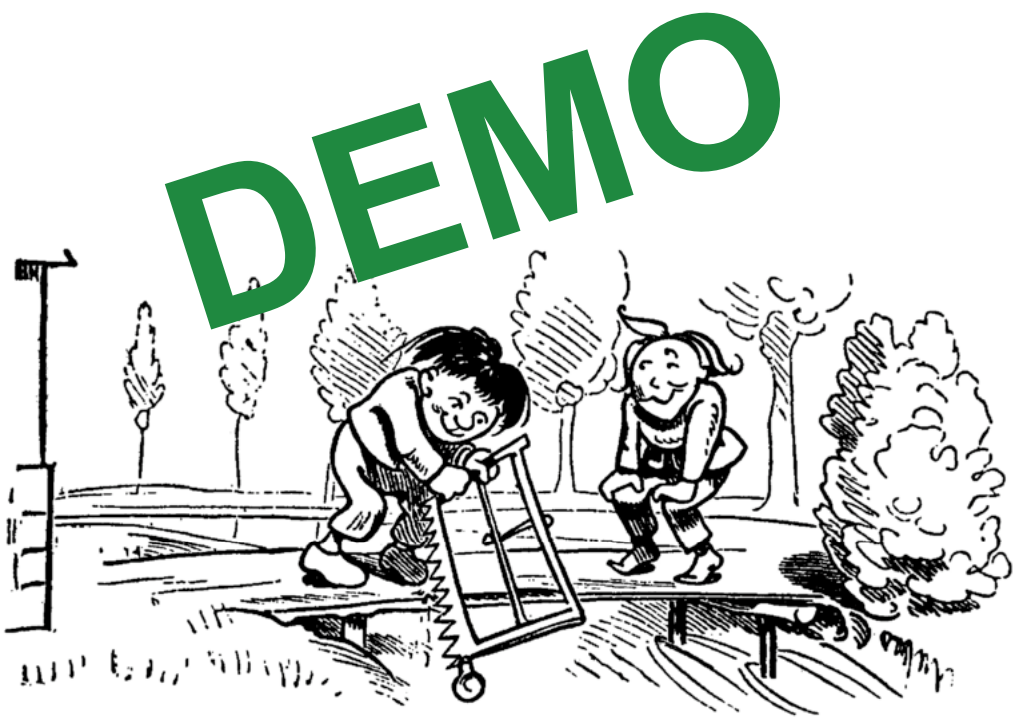
- **Get names of all users, incl. local_admins**

- **Unfortunately, passwords are obfuscated**
  - … and can't be overridden (*read-create* OIDs)

But hey…

ERNW Living Security.

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



Summary & Outlook

ERNW Living Security.

- **“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 Cisco or to WLANs.**

Shameless Announcements

ERNW Living Security.

- **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…

ERNW Living Security.

THANK YOU…

...for yours!