Wireless LAN attacks

What you need to know or a simple guide to WEP/WPA-PSK cracking

Johannes Greil, SEC Consult, 25.4. 2008

Voraussetzungen

- Linux OS oder LiveCD (z.B. Backtrack)
- bestimmte WLAN-Karte/ Chipsatz
  - Ideal: Ralink, Atheros
  - Vgl. http://aircrack-ng.org/doku.php?id=compatibility_drivers
  - Achtung bei WLAN-Karten-Revision – gleiches Produkt nicht unbedingt gleicher Chipsatz!
  - Beste Ergebnisse: Linksys WUSB54G v4
- Je nach HW gepatchte Treiber für Packet Injection
- Aktuellste aircrack-ng Software Suite
  - airoscript aus SVN
- Wireless Tools (iwconfig, ...)

Voraussetzungen

- Injection Test
  - Neue Funktion bei aireplay-ng – überprüft Packet Injection Unterstützung

```
./aireplay-ng -9 -a 00:18:39:C7:34:D7 -e URANO2 rausb0
10:44:57  Waiting for beacon frame (BSSID: 00:18:39:C7:34:D7) on channel 6
10:44:57  Trying broadcast probe requests...
10:44:59  No Answer...
10:44:59  Found 1 AP

10:44:59  Trying directed probe requests...
10:44:59  00:18:39:C7:34:D7 - channel: 6 - 'URANO2'
10:45:05  Ping (min/avg/max): 8.149ms/14.670ms/21.191ms Power: 0.00
10:45:05   2/30:   6%

10:45:05  Injection is working!
```

  - Mit zwei WLAN-Karten können Angriffsmodi überprüft werden

- Generell: sehr gute Doku auf http://aircrack-ng.org

Aircrack-ng Suite

- Version 1.0beta2 empfohlen
- airmon-ng
  - Generisches Tool zum Aktivieren des Monitor Mode
  - airmon-ng <start|stop> <interface> [channel]
    - für Atheros mit madwifi-ng Treiber: airmon-ng start wifi0 => erzeugt ein neues VAP mit Monitor Mode
- airserv-ng
  - WLAN über TCP => „WLAN-Server“, den man für Angriffe verwenden kann
  - Client benötigt keine WLAN-Karte

Aircrack-ng Suite

- airtun-ng
  - erzeugt Virtual Tunnel Interfaces
  - für wIDS, um verschl. Traffic zu monitoren
  - beliebigen Traffic mit beliebigen Tools(!) injecten
  - Repeater Funktionalität, 2 APs verbinden, Packet Replay, ...
- packetforge-ng
  - beliebige Pakete erzeugen, z.B. ARP

Aircrack-ng Suite

- airolib-ng
  - ESSID + Passwort-Listen importieren => Vorausberechnung Pairwise Master Key (immer gleich für ESSID + Passwort-Kombination)
  - Speicherung in SQLite3 DB
  - Beschleunigung Brute-Force auf WPA
  - Vgl. coWPAtty
  - http://www.renderlab.net/projects/WPA-tables/ => Torrent (bzw. 9 DVDs für 66$) mit 33GB Tabellen
  - Interessant für Kunden wo wir die ESSID im Voraus wissen => Offline berechnen, vor Ort cracken

Aircrack-ng Suite

- aireplay-ng
  - DeAuthentication (DoS)
  - Fake Authentication
  - ARP Replay
  - KoreK ChopChop
  - Fragmentation
  - Caffe Latte (attackiert Clients ohne AP, ebenfalls ARP)
  - Injection Test
  - ...
- airodump-ng, aircrack-ng

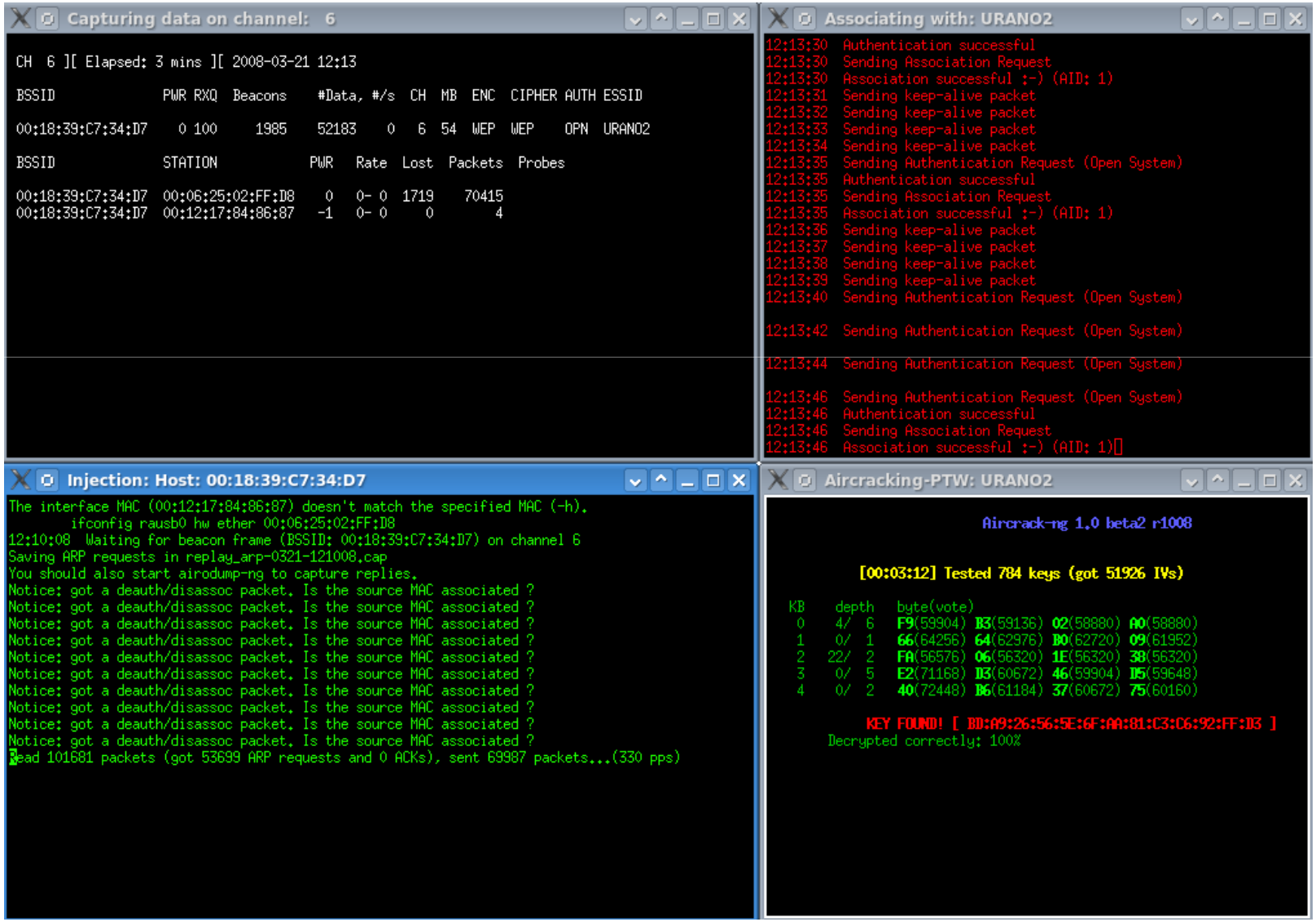
WEP Attacks – ARP Replay

- Für WEP Cracking zahlreiche IV Pakete notwendig
  - Normaler Traffic generiert zu wenig IVs => Injection
- airodump-ng: Sniffen der IV, dumpt ständig im Hintergrund in ein File
- aireplay-ng: Injecten von ARP Request Paketen
  - Legitimer Client muss zumindest 1 ARP Paket verschicken (ping, dhcp-renew), wird mitgesnifft und ständig injected
  - AP re-broadcastet ARP und erzeugt neue IV
- aircrack-ng:
  - PTW Angriff => ca. 40000-50000 IVs reichen zum Cracken (~1-5min)
  - Korek Angriff => ~1,5^6 IVs für 128Bit Keys

WEP Attacks – ARP Replay

- Ergebnis abhängig von WLAN Equipment (sowohl Angreifer, als auch AP), Treiber, Wetterlage, Mondphasen, ...
- Funktioniert (meist) auch ohne assoziertem, legitimen Client (Fake Authentication)

WEP Attacks – ARP Replay

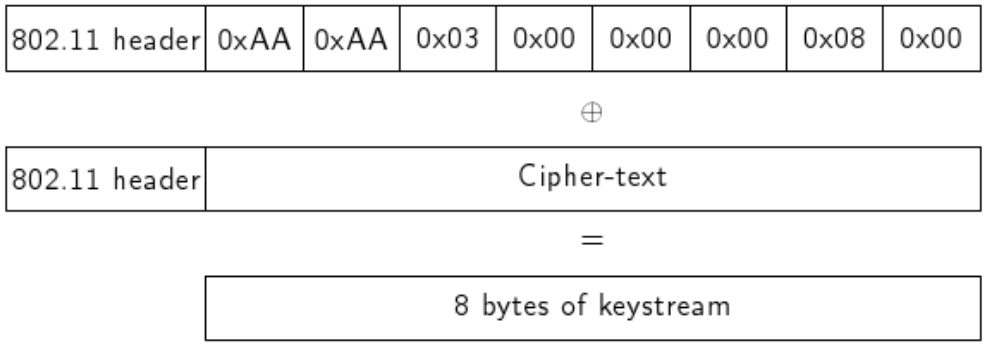


WEP Attacks – ARP Replay

FREE LIVE SHOW!

WEP Attacks – Fragmentation

- Versucht den keystream wiederherzustellen (PRGA), 1500 Bytes
- Um beliebige Daten zu injecten ohne WEP Key zu kennen
- cipher XOR plaintext => keystream
  - Known plaintext => IP Pakete (LLC/SNAP Header immer gleich)
  - Sniffen reicht, um 8 bytes an Daten zu recovern
  - Beliebige Daten in 8 Byte Chunks versendet



WEP Attacks – Fragmentation

- AP erledigt Entschlüsselung für uns
- „Buddy“-Server Konzept
- Mitsniffen eines Payloads
- Anhängen eines neuen Headers mit dest. IP des Buddy Servers
- AP entschlüsselt Paket und schickt an Buddy => known cleartext!

- http://darkircop.org/frag.pdf

WEP Attacks – ChopChop

- Bei erfolgreichem Angriff => WEP Datenpaket ohne KEY entschlüsselbar
- Stark abhängig von AP
- „Chop off the last byte, assume it was 0, correct the packet, send to the AP. If the assumption is correct, the packet is valid hence the AP will broadcast the packet”

WPA Attacks

- Nur Brute-Force / Dictionary
- WPA-PSK: mind. 8 Zeichen, maximal 63
- Passwort gesalted mit ESSID
  - Generierung von „rainbow tables“ immer nur für eine ESSID möglich
- 4-way Handshake mitsniffen => DeAuth
- Danach offline Brute-Force, z.B. Dictionary oder coWPAtty/airolib-ng DB

WPA Attacks

- Dump: airodump-ng -w outfile -c 6 --bssid 00:18:39:C7:34:D7 rausb0
- DeAuth: aireplay-ng -0 1 -a 00:18:39:C7:34:D7 -c 00:1C:BF:55:EF:EE rausb0
- Offline Crack: aircrack-ng –w passwords.lst –b 00:18:39:C7:34:D7 outfile-01.cap

- airolib-ng testdb --import essid $ssidfile
- airolib-ng testdb --import passwd $passwords
- airolib-ng testdb --clean all
- airolib-ng testdb –batch
- airolib-ng testdb --verify all
  - aircrack-ng –r testdb outfile-01.cap

WPA Attacks

URANO VICTIM NEEDED

Ausblick

- wesside-ng
  - „auto-magic tool“ um WEP Key für ein Netzwerk zu erhalten, ohne Benutzerinput
  - noch sehr instabil
- easside-ng
  - „auto-magic tool“ für Kommunikation mit AP, ohne WEP Key zu kennen
  - AP benötigt Internet connectivity, Angreifer benötigt „buddy“ Server im Internet
- airbase-ng
  - Tool, um AP zu simulieren => Clients anzugreifen
  - Z.B. Sniffen von Shared-Key Authentication
- MDK3
  - Bruteforce MAC Filters
  - Bruteforce hidden SSIDs
  - Probe networks for checking if they can hear you
  - Intelligent Authentication-DoS to freeze APs (with checking for success)
  - Beacon Flooding with channel hopping (can crash NetStumbler and some buggy drivers)
  - Disconnects everything found (aka AMOK-MODE) with DeAuth and DisAssoc packets (Don't try this where they can kick your ass! ;D)
  - WPA TKIP Denial-of-Service
  - WIDS/WIPS Confusion

The End

[00:00:00] 19 slides processed (0,1 sl/m)

KEY FOUND! [THE END]

Master Key : 93 35 99 AF 65 B9 CC D7 EA 03 AD 10 8B DD 21 98
CF DD E1 39 12 43 B4 E7 C2 9B 4B 30 81 DF 98 B2

Transcient Key : C1 A8 31 F7 A9 BA 92 A0 43 A0 D3 F2 FD 78 F7 28
9B 7B 2B 6A F7 46 AB 3E 21 96 75 D0 9A 47 7D D2
CE 55 EB 7E C3 DC 76 20 0D 86 66 AE 16 B0 FD 6A
48 2E 8F F4 79 36 38 05 9F D1 63 D9 62 42 12 EF

EAPOL HMAC : 89 BD 0B 10 4E BD EC B9 D5 32 9E A8 C5 48 FA KE